



S'to

C | E | H

Certified | Ethical Hacker

100% illegal



Jika Anda ingin menghentikan Hacker, Anda harus bisa berlaku dan bertindak seperti Hacker



CEH

Certified Ethical Hacker



S'to

CEH : 100% illegal

Hak Cipta © 2009 pada penulis

Hak Cipta dilindungi Undang-Undang. Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apapun, baik secara elektronis maupun mekanis, termasuk memfotocopy, merekam atau dengan sistem penyimpanan lainnya, tanpa izin tertulis dari Penulis dan Penerbit.

ISBN 978-979-1090-21-6

Cetakan pertama : Maret 2009

Publisher

Jasakom

Email

admin@jasakom.com

Web Site

<http://www.jasakom.com/penerbitan>

Ketentuan pidana pasal 72 UU No. 19 tahun 2002

1. Barang siapa dengan sengaja dan tanpa hak melakukan kegiatan sebagaimana dimaksud dalam pasal 2 ayat (1) atau pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp. 1.000.000 (satu juta rupiah) atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).
2. Barang siapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu Ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait sebagaimana dimaksud pada ayat (1), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)

DAFTAR ISI

Module 1. Pemahaman Dasar Ethical Hacker.....	1
Kenapa keamanan komputer menjadi penting.....	1
Terminologi-Terminologi Dasar.....	4
Element-element keamanan	5
Tahapan aktifitas Hacking	6
1. Reconnaissance.....	7
2. Scanning	8
3. Gaining access	8
4. Maintaining access	9
5. Covering Tracks	9
Pengelompokan Jenis serangan.....	9
1. Level Sistem Operasi	10
2. Level Aplikasi	10
3. Shrink Wrap Code.....	10
4. Kesalahan konfigurasi.....	11
Hacktivism.....	11
Pengelompokan Hacker.....	12
1. Black Hat Hacker	12
2. White Hat Hacker	12
3. Grey Hat Hacker	12
4. Suicide Hacker	12
Ethical Hacking atau Hacking beretika.....	13
Vulnerability Research dan Tools	14
National Vulnerability Database (http://nvd.nist.gov/).....	14
Securitytracker (http://www.securitytracker.com/)	15
Securiteam (http://www.securiteam.com).....	16

Secunia (http://secunia.com/)	17
Hackerstorm (www.hackerstorm.com)	18
Hackerwatch (http://www.hackerwatch.org)	18
SecurityFocus (http://www.securityfocus.com)	19
SCMagazine (http://scmagazine.com)	20
Zone-h (http://zone-h.org)	21
Milw0rm (http://www.milw0rm.com/)	22
Jasakom (http://www.jasakom.com)	22
Bagaimana Ethical Hacker Bekerja	23
Jenis Testing	24
Metodologi Testing	25
Module 2. Footprinting	27
1. Menggali Informasi Awal	29
1.1. Mendapatkan informasi dari website resmi	29
1.2. Mendapatkan informasi dari nama domain atau alamat IP	30
1.3. Netcraft, mendapatkan informasi domain	33
1.4. Mendapatkan arsip website	34
1.5. Mencari Sub Domain, Email dan informasi lainnya	34
1.6. Survei Lokasi	37
1.7. Mengetahui Rute Perjalanan	38
1.8. Melacak email	41
1.9. Melacak Aktivitas Penerima Email	44
1.10. Lebih Mengenal Korban	46
2. Mencari Informasi Range Alamat IP	52
Module 3. Google Hacking	73
Google Cache	74
Proxy Google	75
Menampilkan Direktori Listing	78
Mencari File Tertentu	80
Mencari Type File	81
Pencarian Pada Domain Tertentu	82
Mencari “Target” Toko Online	83
Mendapatkan File “Biang Kerok”	84
Mencari Pesan Kesalahan	85

Module 4.Scanning	91
1. Port Scanning.....	92
2. Network Scanning	93
3. Vulnerability Scanning	93
Metodologi Scanning.....	94
1. Mencari System yang aktif	95
2. Mencari Port yang terbuka	98
Apa itu TCP dan Sequence Number dalam TCP ?	98
Three Way Handshake.....	100
Saatnya Mencari Port Yang Terbuka.....	102
1. TCP Connect scan	103
2. TCP SYN scan	103
3. TCP FIN scan	103
4. TCP NULL scan	104
5. TCP ACK scan	104
6. TCP XMAS scan	104
7. IDLE Scan.....	104
War Dialing.....	119
Bagaimana War Dialing Bekerja	121
3. Mengidentifikasi Services	124
4. Banner grabbing/OS Fingerprinting.....	131
OS Fingerprinting berdasarkan Implementasi TCP/IP ..	133
Active Fingerprinting	134
Passive Fingerprinting.....	137
Menipu Hacker Melalui Banner	141
5.Vulnerability Scanning.....	145
6. Menggambarkan diagram network dari host yang bermasalah (Vulnerable hosts)	162
7. Menyiapkan proxy	165
Kegunaan Proxy Server	166
Anonymous proxy dan Free Proxy Server	168
Mencari Free Proxy Server	170
Teknik HTTP Tunneling	181

Penutup (FAQ)	189
Kenapa tidak semua modul dibahas didalam buku ini?	189
Apakah Anda Akan Membahas Semua Modul ini ?	191
Apa judul buku berikutnya ?	191
Apakah training CEH mengajarkan semua modul?	192
Katanya 4 modul pertama,	
kenapa ada yang di'lewatkan'?	192
Apakah semua tools didalam modul CEH	
dibahas juga dibuku Anda ?	192

Module 1

Pemahaman Dasar Ethical Hacker

Kenapa keamanan komputer menjadi penting

Helen terburu-buru ke airport untuk membeli tiket menuju korea, tempat dimana ia harus memberikan presentasi untuk sebuah pertemuan yang sangat penting. Sesampainya di airport, tampak orang-orang yang hiruk pikuk diluar biasanya, ada yang marah-marah, ada yang kebingungan dan ada pula yang menangis.

Karena terdesak oleh waktu, Helen tidak memperdulikan situasi diluar kebiasaan tersebut dan langsung menuju mesin ATM *Bank of America Corp* untuk menarik uangnya. Ketika ia memasukkan kartu ATM-nya, ternyata mesin tersebut mati dan tidak bisa digunakan. Untunglah, airport dengan kelas internasional ini cukup bonafit dan masih banyak mesin ATM lain yang bisa digunakan. Dengan tergesa-gesa Helen mencari mesin ATM lain dan betapa terkejutnya ia karena semua ATM bernasib sama dan Helen tidak bisa menarik uang-nya sama sekali !

Untuk mengantisipasi keadaan yang sudah berantakan ini, Helen berfikir cepat dan memutuskan mengirimkan bahan presentasi kepada keleganya di korea menggunakan internet namun nasib sedang tidak memihak padanya. Internet di korea selatan sedang mengalami gangguan hebat sehingga kiriman tersebut tidak bisa dilakukan. Helen memutar otaknya sekali lagi dan teringat akan "uang lipat" ! yah, Helen memang suka menyimpan beberapa ratus dolar dalam dompet yang diselipin diantara kartu namanya yang tersembunyi di dalam dompet untuk digunakan dalam keadaan terdesak semacam ini.

Uang keramat tersebut dikeluarkan dan setelah dihitung-hitung, ternyata masih memungkinkan untuk membeli tiket kelas ekonomi. Dengan terburu-buru, Helen segera kembali ke loket penjualan tiket pesawat. Terlihat petugas dengan keringat dan muka murung sedang kelabakan melayani penumpang yang hendak membeli tiket karena komputer sedang tidak bisa digunakan, semuanya dikerjakan manual dan petugas tidak bisa memastikan ketersediaan tempat duduk !

Kini Helen menyadari keadaan yang sedang dihadapi oleh orang-orang disekitarnya ! Cerita ini bukanlah cerita di dalam sebuah film yang dibesar-besarkan seperti *Die Hard 4.0* atau *Swordfish* yang mampu meng-crack password sembari di "service" namun adalah sebuah kondisi yang terjadi ketika serangan worm yang dinamakan *SQL Slammer* terjadi pada tahun 2003 walaupun Helen hanyalah sebuah tokoh fiktif.

Selain ratusan ribu mesin ATM yang mati, penerbangan pesawat mengalami gangguan, *Korea Telecom Freetel* dan *SK Telecom service* tidak bisa digunakan, pelanggan tidak bisa menghubungi website resmi Microsoft karena gangguan hebat yang terjadi, situs-situs internet banyak yang tumbang, bahkan media cetak mengalami keterlambatan penerbitan.

• Sumber: <http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/>

Perkembangan komputer yang sedemikian pesatnya dan ketergantungan manusia terhadap komputer sudah tidak perlu diperdebatkan lagi. Kini, sudah bukan suatu hal yang aneh atau ajaib lagi bila sebuah bank menolak melayani nasabahnya karena jaringan komputernya rusak.

Perkembangan komputer yang pesat juga semakin hari menuntut kompleksitas yang semakin tinggi namun dengan penggunaan yang mudah oleh pengguna. Para developer berlomba-lomba membuat produk yang mudah untuk digunakan namun keamanan sering menjadi anak tiri. Atas nama waktu dan target, developer seringkali hanya melakukan pengetesan terhadap fungsi suatu program dan masalah keamanan kurang mendapatkan perhatian.

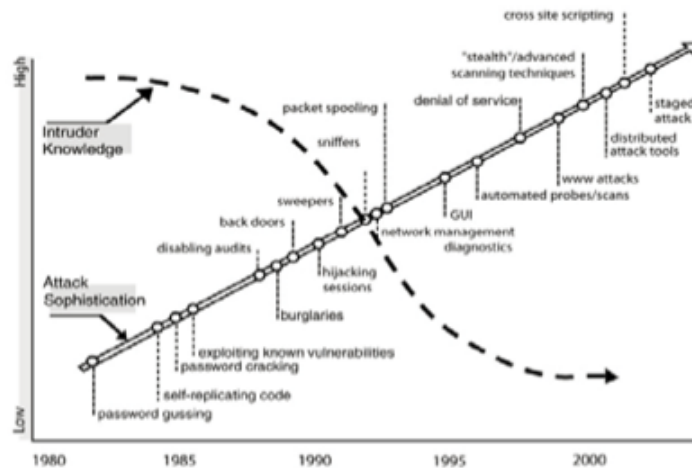
Tidak heran bila kita sering melihat banyaknya tambalan yang perlu dilakukan terhadap sebuah software yang sudah digunakan, ini artinya proses pengetesan atau *Quality Control* tidak berjalan

dengan baik karena tidak bisa mendeteksi permasalahan secara dini. Ancaman terhadap keamanan komputer semakin hari semakin berbahaya seiring dengan semakin kompleksnya sebuah software.

Sebagai contoh, jika Anda perhatikan *MS Word* versi awal, tombol dan menu-menu yang tersedia tidaklah terlalu banyak namun saat ini terdapat ratusan menu, ratusan fungsi yang bahkan sebagian besar tidak diketahui kegunaannya oleh para pengguna. Virus dan worm mulai menyebar memanfaatkan "otomatisasi" yang tidak disadari oleh pengguna dan memanfaatkan otomatisasi ini tidaklah sulit.

Di dalam negeri Anda bisa melihat banyaknya buku-buku mengenai membuat virus dan worm yang hanya memanfaatkan *auto startup* tersembunyi di dalam windows. Celaknya, dengan metode sederhana, korban yang jatuh ternyata sangat besar !

Mudahnya melakukan hacking juga diakibatkan oleh semakin tersedianya peralatan-peralatan untuk melakukan hacking dimana seseorang hanya tinggal mengklik tombol mousenya untuk mendapatkan hasil yang diinginkan. Akibatnya adalah secara umum kemampuan orang-orang yang dikenal sebagai hacker semakin menurun namun ancaman yang ditimbulkan justru semakin naik. Artinya dengan kemampuan yang rendah, seorang hacker bisa menjadi sebuah ancaman yang tinggi dan berbahaya bagi kepentingan umum.



(Source: The Cert® Guide to System and Network Security Practices)

Akibat langsung dari anomali ini sudah bisa diprediksi, korban berjatuhannya yang semakin banyak dari hari ke hari. Kerugian akibat dari serangan hacker inipun mengalami kenaikan menurut survei dari beberapa lembaga keamanan komputer sedangkan pengetahuan rata-rata dari pengguna komputer yang ternyata masih sangat rendah karena kemudahan yang ditawarkan oleh berbagai software.

Terminologi-Terminologi Dasar

Setiap menangani diskusi dip perusahaan, permasalahan pertama yang selalu saya hadapi adalah perbedaan istilah yang membuat diskusi ibarat ayam berbicara dengan kodok. Untuk sesuatu yang sama, setiap perusahaan menggunakan istilahnya masing-masing. Pengeluaran uang dari bank misalnya, ada yang menggunakan istilah BBK (bukti bank keluar), ada yang menggunakan kata Voucher, ada yang menggunakan istilah KK (Keluar kas).

Sedikit perbedaan saja dalam istilah membuat diskusi selama beberapa jam menjadi sia-sia karena itu sebelum kita melanjutkan, tahap pertama adalah menyamakan istilah-istilah yang akan digunakan di dalam buku ini, agar “ayam” yang saya maksudkan sama dengan “ayam” yang ada didalam pikiran Anda.

Kelemahan dalam sebuah sistem baik program, design ataupun implementasi dinamakan sebagai **Vulnerability**. Akibat dari Vulnerability ini adalah timbulnya suatu ancaman atau yang dikenal dengan **Threat**. Threat atau ancaman belum tentu akan menimbulkan kerusakan pada suatu sistem dan ini yang sering disalah artikan. Misalnya ancaman bencana alam, yang belum tentu akan terjadi tapi ancaman tersebut jelas ada dan tidak bisa dihilangkan dimanapun dimuka bumi ini. Berdasarkan ancaman atau Threat yang ada, ada kemungkinan terjadinya serangan atau **Attack** yang mengancam elemen keamanan dari sistem.

Software, tools ataupun teknik yang bisa digunakan untuk melakukan serangan terhadap salah satu elemen keamanan suatu sistem dinamakan sebagai **exploit**. Jadi exploit tidak hanya berupa software yang tinggal dijalankan namun juga termasuk tuntunan langkah demi langkah bagaimana suatu sistem bisa diserang / dimanfaatkan /

diperdaya. Banyak sekali situs-situs yang memberikan informasi mengenai exploit ini seperti *milworm*, *securiteam* dan dari dalam negeri yang terkenal saat buku ini ditulis adalah komunitas jasakom (*www.jasakom.com*) dan *echo*.

Element-element keamanan

Topik utama dalam sertifikasi CEH adalah keamanan dan saya sudah membicarakan mengenai berbagai macam istilah yang mengancam keamanan, lalu apa yang dimaksud dengan keamanan itu sendiri? Apanya yang terancam? Keamanan terdiri atas tiga elemen yang sering disingkat menjadi CIA (*confidentiality*, *integrity* dan *availability*). Serangan hacker adalah serangan terhadap salah satu elemen CIA dan mengancam salah satu elemen CIA ini.

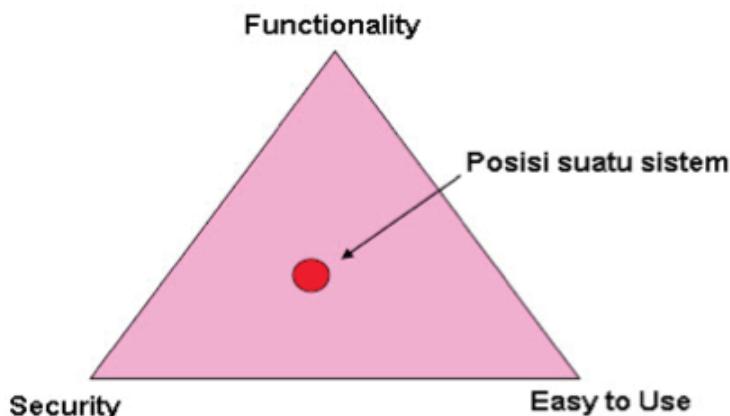
Anda tidak akan suka bila email Anda bisa dibaca oleh setiap orang dan Anda juga tidak suka jika rekening bank Anda bisa dilihat oleh semua orang, inilah elemen *Confidentiality* atau kerahasiaan.

Ketika Anda mengirimkan email, tentu akan menjadi masalah besar bila isi email Anda ternyata telah dirubah isinya oleh seseorang, dari memuji seorang karyawan menjadi memecat karyawan. Inilah contoh dari elemen *integrity* atau integritas.

Suatu data, tidak boleh dirubah oleh orang yang tidak berhak. Baik, Anda khawatir dengan keamanan email dan mematikan komputer Anda. Apa yang terjadi? Anda menjadi tidak bisa dihubungi, inilah elemen *Availability* (tersedia/keberadaan) yang sangat penting.

Sistem bagaimanakah yang seharusnya dibangun dan terbaik untuk digunakan? Keamanan yang tinggi, kemudahan pakai untuk semua pengguna dan fungsi yang tinggi tentunya. Kenyataannya, Anda tidak bisa mendapatkan ketiga hal ini ! Hubungan antara keamanan, fungsi dan kemudahan penggunaan digambarkan dalam bentuk segitiga (*triangle*).

Ketika Anda memintahkan posisi sistem ke arah *security*, fungsi dan kemudahan pemakaian harus Anda korbankan. Ketika Anda memindahkan sistem agar mudah digunakan (*easy to use*), Anda akan menjauhi fungsi dan juga masalah keamanan.



Menentukan dimana letak sebuah sistem bukanlah perkara mudah dan sangat tergantung pada situasi dan kondisi yang ada. Yang harus Anda lakukan adalah menentukan suatu keseimbangan antara keamanan, kemudahan dan fungsi. Komputer Anda dijamin aman 100% bila Anda mematikan komputer Anda namun tindakan demikian membuat komputer Anda tidak bisa digunakan dan tidak berfungsi sebagaimana mestinya.

Tentu ini bukan suatu ide yang bagus. Anda bisa menaruh komputer disetiap ruangan, tanpa password, setiap orang bisa langsung menggunakannya. Nyaman dan mudah namun tentu saja menjadi tidak aman karena sangat mungkin komputer tersebut disalah gunakan.

Dengan melihat gambaran mengenai posisi sebuah sistem, bisa disimpulkan bahwa kondisi terbaik untuk meletakkan suatu sistem tidaklah bisa ditentukan dan sangat tergantung pada setiap kebutuhan yang berbeda-beda. Untuk sistem perbankan, Anda perlu menaruhnya mendekati Security dan mungkin untuk kebutuhan dirumah Anda, posisinya akan lebih tepat dengan posisi mendekati *Easy to Use* (kemudahan penggunaan).

Tahapan aktifitas Hacking

Semakin Anda mengenal korban, semakin dekat Anda pada kemenangan. Semakin mengenal musuh Anda, semakin Anda

mengenal kelemahannya karena itu tidaklah heran, musuh dalam selimut adalah musuh yang paling berbahaya.

Anda memang bisa menjadi koboi, berjalan dengan gagah berani, masuk ke bank, menodongkan pistol dan merampok uang yang ada kemudian kabur namun kemungkinan keberhasilan dan keselamatan Anda mungkin hanya 0.00001%.

Perampok biasanya mengamati terlebih dahulu bank yang akan dirampok, menyusun rencana, dan bahkan menggambarkan peta untuk kabur dengan kondisi lalu lintas yang macet. Semakin matang dan semakin rinci perencanaan yang dilakukan, keberhasilan perampokan akan semakin tinggi, demikian juga halnya dengan aksi hacking. Seorang hacker dalam melakukan penyerangan terhadap target-nya. Berikut adalah 5 tahapan yang didefinisikan dalam sertifikasi CEH, yaitu :



1. Reconnaissance

Reconnaissance adalah tahap mengumpulkan data dimana hacker akan mengumpulkan semua data sebanyak-banyaknya mengenai target. Data apa saja? Semuanya ! tanggal lahir, nomor plat kendaraan, jenis komputer, nama anak, hobi, bahkan sampai nama istri simpanan dari orang penting, semuanya bisa berguna. Tidak percaya? Apa yang Anda gunakan untuk password Anda? apa yang Anda gunakan untuk pin ATM Anda? Ketika hacker mendapatkan form login atau semacamnya, ia bisa mencoba informasi yang didapatkan ini sebagai password. Ini hanyalah salah satu contoh kecil kegunaan dari tahapan *Reconnaissance*.

Reconnaissance masih dibagi lagi menjadi 2 yaitu *Active* dan *Passive Reconnaissance*. Ketika Anda mencari berita mengenai perusahaan tersebut dari berita-berita di koran atau dengan *search engine*, Anda sedang melakukan *Passive Reconnaissance*. *Passive Reconnaissance* bisa dikatakan sebagai *Reconnaissance* yang tanpa berhubungan secara

langsung dengan korban. Anda tidak akan terdeteksi oleh korban ketika melakukan *Passive Reconnaissance*.

Sebaliknya, *Active Reconnaissance* adalah *Reconnaissance* yang dilakukan secara aktif, dimana hacker melakukan aktifitas terhadap korban untuk mendapatkan data tersebut. Hacker bisa menginjeksi paket, hacker bisa membohongi karyawan perusahaan agar mendapatkan data yang dikehendaki, dlsb. *Active Reconnaissance* merupakan langkah yang lebih berbahaya dibandingkan dengan *Passive Reconnaissance* dan Anda sangat mungkin berurusan dengan polisi akibat dari tindakan Anda.

2. Scanning

Scanning merupakan tanda dari dimulainya sebuah serangan hacker (*pre-attack*). Melalui *scanning* ini, hacker akan mencari berbagai kemungkinan yang bisa digunakan untuk mengambil alih komputer korban. Melalui informasi yang didapatkan pada tahapan *scanning*, hacker bisa mencari “jalan masuk” untuk menguasai komputer korban. Berbagai tools biasanya digunakan oleh hacker dalam membantu proses pencarian ini namun seorang hacker profesional tidak hanya mengandalkan sebuah tools, mereka juga bisa mencari secara manual untuk hal-hal yang tidak bisa dilakukan oleh sebuah tools.

3. Gaining access

Melalui semua informasi yang didapatkan, hacker akan mulai menyerang komputer korban untuk menguasainya. Tahapan ini merupakan tahapan penerobosan (*penetration*) setelah hacker berhasil mengetahui kelemahan yang ada pada komputer atau system korban melalui tahapan *scanning*. Tahapan ini tidak harus selalu sebuah tahapan yang “canggih” karena hacker bisa saja memanfaatkan seorang staff IT yang telah diketahui mempunyai sifat “takut atasan”. Hacker bisa berpura-pura menjadi orang yang disewa oleh bos (dengan menyebut nama bos berdasarkan informasi yang didapatkan pada tahap *Reconnaissance*) dan menanyakan password kepadanya melalui telp serta berbagai trik kotor lainnya.

4. Maintaining access

Setelah mendapatkan akses ke komputer korban, hacker biasanya ingin tetap menguasai komputer tersebut. Ketika korban mengganti passwordnya atau ketika korban memperbaiki kelemahan yang ada, hacker biasanya tidak ingin kehilangan kekuasaannya terhadap komputer tersebut.

Untuk itu, biasanya seorang hacker akan berusaha mempertahankan kekuasaannya terhadap komputer korban dengan berbagai cara seperti dengan menanamkan backdoor, rootkit, trojan, dll. Untuk mempertahankan kekuasaannya, hacker bahkan bisa memperbaiki beberapa kelemahan yang ada pada komputer korban agar hacker lain tidak bisa memanfaatkannya untuk mengambil alih komputer yang sama.

5. Covering Tracks

Apakah Anda berminat merasakan sejujunya tidur dibalik terali besi? Atau merasakan bagaimana aksi sodomi di dalam penjara? Hacker juga tidak ingin merasakan hal-hal semacam ini karena ancaman yang sangat nyata terhadap aksi mereka, apalagi di negara yang sudah mempunyai hukum yang jelas.

Tidak heran, biasanya hacker akan berusaha menutup jejak mereka dengan cara menghapus log file serta menutup semua jejak yang mungkin ditinggalkan karena itu tidak mengherankan, ketika hacker membuat file atau direktory di dalam komputer korban, mereka seringkali membuatnya dalam modus tersembunyi (*hidden*).

Pengelompokan Jenis serangan

Untuk menguasai komputer korban, hacker hanya perlu mengeksploitasi salah satu elemen yang bermasalah pada komputer korban. Elemen-elemen atau jenis serangan ini bisa dikelompokkan menjadi beberapa bagian yaitu :

1. Level Sistem Operasi

Seberapa banyaknya patch yang harus Anda install dalam sebulan? pernahkah Anda diminta agar menginstall patch sesegera mungkin agar tidak diserang oleh worm, virus atau hacker? ini adalah contoh dari kelemahan sistem operasi yang umumnya bisa diperbaiki bila Anda rajin-rajin mengupdate komputer Anda dengan tambahan atau patch yang disediakan oleh vendor sistem operasi seperti windows atau linux.

2. Level Aplikasi

Aplikasi yang Anda gunakan seperti Office, Acrobat, mp3 player, games, dll menyimpan permasalahan yang sama dengan sistem operasi Anda. Kelemahan pada satu aplikasi yang Anda gunakan saja bisa membawa implikasi yang sangat besar karena hacker bisa masuk dan menguasai komputer Anda dari situ.

3. Shrink Wrap Code

Untuk apa menemukan kembali roda yang sudah ditemukan? Anda tinggal menggunakan roda tersebut bukan? ini adalah sebuah ungkapan untuk menunjukkan bahwa Anda seharusnya memanfaatkan peralatan atau alat bantu yang sudah ada (seperti film Mac Gyver) daripada selalu memikirkan membuat yang baru. Di dalam pemrograman, banyak sekali fungsi-fungsi yang sudah dibuat dan siap digunakan, ketika Anda menginstall sistem operasi, berbagai script contoh yang bisa digunakan untuk memudahkan pekerjaan Anda sudah siap digunakan.

Banyak orang yang menggunakan kode-kode program ini atau membiarkannya diaktifkan apa adanya tanpa melakukan sedikitpun perubahan atau konfigurasi. Akibatnya bisa Anda duga, program ini bisa dimanfaatkan oleh hacker untuk menguasai komputer Anda. Microsoft 2000 dan NT misalnya, menyediakan berbagai script contoh yang bisa digunakan untuk membantu sistem administrator maintenance aplikasi mereka namun script ini ternyata juga dengan mudah bisa dimanfaatkan oleh hacker untuk menguasai komputer korban.

4. Kesalahan konfigurasi

Semakin hari, aplikasi dan sistem operasi semakin rumit dengan tambahan berbagai feature yang terus berubah. Masalahnya adalah sebagian besar orang-orang tidak memahami semua teknologi baru ini. Administrator hanya membuat konfigurasi sederhana dengan prinsip “yang penting program bisa dijalankan”.

Hacker seringkali memanfaatkan kesalahan konfigurasi ini untuk mengambil alih sebuah komputer. Apakah Anda membutuhkan web server di komputer Anda? Apakah menggunakan UPS? apakah Anda men-sharing file Anda dengan komputer lain di rumah Anda? atau Anda hanya mempunyai 1 komputer? apakah registry di komputer Anda perlu di akses oleh orang luar? lalu kenapa Anda membiarkan service-service tersebut aktif di komputer Anda?

Hacktivism

Seringkali kita melihat sebuah situs di hack dan halaman utama dari website tersebut diganti oleh hacker dengan pesan-pesan politik tertentu. Ketika malaysia memenangkan sengketa pulau dengan Indonesia, hacker indonesia beramai-ramai melakukan serangan ke situs malaysia. Halaman utama berbagai situs diganti dengan kata-kata dari yang sopan sampai yang tidak senonoh. Aksi ini dikategorikan sebagai *hacktivism*, suatu gerakan hacker dengan motif politik tertentu. Mereka ingin menyampaikan pesan agar didengar oleh orang-orang didunia ini.

Contoh lain dari aktifitas cyber dengan tujuan politik ini pernah dilakukan oleh hacker portugal dengan menyerang ke situs indonesia dan menampilkan pesan “Free East Timor” yang marak dilakukan pada tahun 1998, dan hacker Indonesia yang memprotes orde baru yang marak dilakukan pada saat era presiden soeharto berkuasa. Tidak semua aksi deface ini dikategorikan sebagai *hacktivism*. Sebagai contoh, banyak sekali orang-orang yang mendeface hanya untuk menyampaikan salam kepada pacarnya, atau hanya menyampaikan salam kepada kelompoknya agar mereka dikenal sebagai seorang hacker. Aksi semacam ini terkadang dibungkus dengan pesan politik agar mendapatkan perhatian dan pemberitaan dari media massa.

Pengelompokan Hacker

Hacker bisa dikelompokkan berdasarkan aktifitas yang mereka lakukan. Pengelompokan ini memang tampak agak aneh bagi Anda yang pertama kali mendengarnya karena menggunakan istilah hat (topi), yaitu :

1. Black Hat Hacker

Black Hat Hacker adalah jenis hacker yang menggunakan kemampuan mereka untuk melakukan hal-hal yang dianggap melanggar hukum dan merusak. Ini adalah type hacker yang selalu digambarkan dan mendapatkan berita dari media massa akibat ulah mereka. Kelompok ini juga disebut sebagai *cracker*.



2. White Hat Hacker

White Hat Hacker adalah jenis hacker yang menggunakan kemampuan mereka untuk menghadapi *Black Hat Hacker*. Umumnya mereka adalah profesional-profesional yang bekerja pada perusahaan keamanan dan umumnya juga disebut sebagai *security analys*, *security consultant*, dlsb

3. Grey Hat Hacker

Grey Hat Hacker adalah jenis hacker yang bergerak diwilayah abu-abu, terkadang mereka adalah *White Hat Hacker* namun mereka juga bisa berubah menjadi *Black Hat Hacker*.

4. Suicide Hacker

Terorisme cyber sejauh ini masih lebih banyak mitos daripada kenyataan. Film-film seperti *Die Hard 4.0* memberikan gambaran tentang hal semacam ini dimana hacker menguasai jaringan semua komputer dari sebuah negara sehingga ia bisa melakukan banyak hal untuk berbuat kekacauan. Ledakan gas terjadi dimana-mana, listrik dan air dimatikan sehingga negara menjadi kacau balau dan

porak poranda (chaos). Kejadian ini memang hanya terjadi difilm dan belum pernah terjadi di dalam dunia nyata, namun bukan tidak mungkin hal tersebut bisa dilakukan. Hacker jenis ini tidak takut dengan ancaman penjara 100 tahun sekalipun dan hanya mempunyai tujuan membuat kekacauan yang sebesar-besarnya. Suicide hacker, bisa disetarakan dengan tindakan bom bunuh diri yang marak di jaman modern ini atau berbagai tindakan terror dari teroris.

Ethical Hacking atau Hacking beretika

Hacker beretika? Apakah itu mungkin dilakukan? Saya mendapatkan sebuah email dari seorang pembaca buku **Seni Teknik Hacking 2** yang mengatakan telah melakukan *Ethical Hacking* :

Maaf saya sebenarnya ingin bertanya, apabila kita melakukan ethical hacking, memberitahu kelemahan dari IT suatu instansi, apakah pihak instansi tersebut dapat menuduh kita melakukan hal yang tidak seharusnya terhadap server mereka?

Beberapa waktu yang lalu saya melakukan serangan MITM pada Melsa hotspot di Bandung Supermall, saya mendapatkan cukup banyak user dan paswd (friendster, plasacom, webmail, dll). Di mana salah satunya adalah user dan paswd admin dari melsa sehingga saya dapat menambahkan user hotspot berapapun dan tentu saja dengan data pribadi yang dikarang. Aplikasi Cain yang Anda berikan melalui cd buku Anda sangat bermanfaat pada MITM ini.

Sebenarnya saya ingin memberitahu pihak Melsa tentang hal ini, tetapi yang saya takutkan adalah apabila mereka berlaku tidak bijaksana.

Apakah tindakan semacam ini termasuk *Ethical Hacking*? apakah hacker ini bersalah? bisakah dijebloskan ke penjara? Tentu saja! Saya katakan kepadanya bahwa "*seharusnya*" Melsa berterima kasih sebelum jatuh korban yang lebih banyak lagi dan sangat kecil kemungkinan mereka akan menuntutnya tapi hal tersebut bukan jaminan dan pihak Melsa bisa saja melakukan hal yang sebaliknya.

Aksi semacam ini, tidak bisa dikategorikan sebagai *Ethical Hacking*! Ketika Anda mencari kelemahan pada sebuah situs dan

memberitahukannya kepada pemilik website, tindakan Anda juga bukan termasuk *Ethical Hacking* walaupun Anda mempunyai niat yang sangat mulia.

Ethical Hacking adalah hacking yang dilakukan dengan ijin dan sepengetahuan dari pemilik. Hacking yang dilakukan tanpa sepengetahuan dan ijin dari pemilik, walaupun bertujuan baik tetap tidak bisa dikategorikan sebagai *Ethical Hacking* dan beresiko mendapatkan ancaman hukuman sesuai dengan negaranya masing-masing apabila sang korban merasa tidak senang dengan tindakan hacker.

Agar terbebas dari sangsi hukum, *Ethical Hacker* perlu mendapatkan persetujuan tertulis dan menandatangani perjanjian mengenai apa saja yang boleh dilakukan dan apa saja yang tidak boleh dilakukan oleh hacker.

Vulnerability Research dan Tools

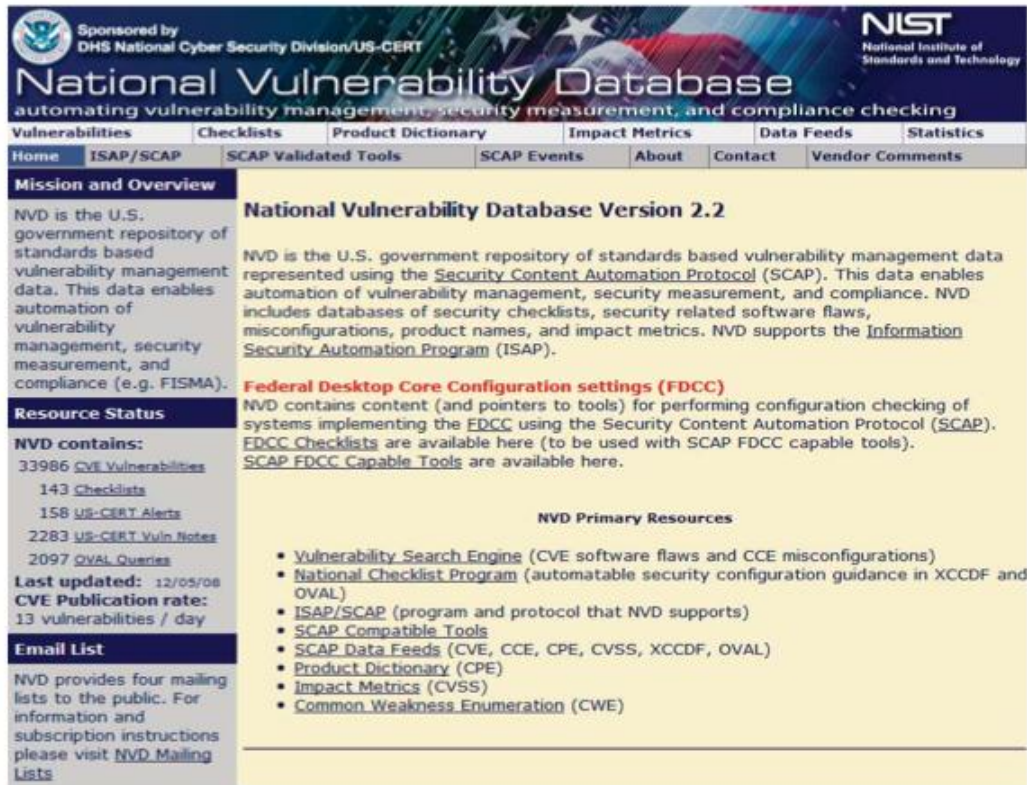
Seorang *Ethical Hacker*, haruslah mempunyai kemampuan dan pengetahuan yang sama dengan seorang hacker. Untuk itu, *Ethical Hacker* harus terus mengasah kemampuannya agar tidak ketinggalan kereta dibandingkan dengan hacker yang melakukan kerusakan. Seorang *Ethical Hacker* misalnya, juga harus mengetahui perkembangan dunia keamanan dan berbagai issue yang telah dipublikasikan kepada publik karena pengetahuan semacam ini seringkali digunakan oleh para hacker untuk melakukan eksploitasi terhadap korbannya.

Salah satu cara mengasah dan mengikuti perkembangan dalam dunia jebol menjebol ini adalah melalui *Vulnerability Research*. *Vulnerability Research* adalah proses menemukan dan mencari kelemahan yang memungkinkan suatu system di-hack. Beberapa situs sangat membantu dalam hal ini karena melaporkan berbagai permasalahan pada berbagai software.

National Vulnerability Database (<http://nvd.nist.gov/>)

Ini adalah situs milik pemerintah Amerika Serikat yang mendokumentasikan berbagai informasi kelemahan/vulnerability

dalam bentuk sebuah database.



National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | **Checklists** | **Product Dictionary** | **Impact Metrics** | **Data Feeds** | **Statistics**

Home | **ISAP/SCAP** | **SCAP Validated Tools** | **SCAP Events** | **About** | **Contact** | **Vendor Comments**

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the Information Security Automation Program (ISAP).

Federal Desktop Core Configuration settings (FDCC)

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- ISAP/SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)

Resource Status

NVD contains:

- 33986 CVE Vulnerabilities
- 143 Checklists
- 158 US-CERT Alerts
- 2283 US-CERT Vuln Notes
- 2097 OVAL Queries

Last updated: 12/05/08
CVE Publication rate: 13 vulnerabilities / day

Email List


NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Dengan adanya database ini, software-software keamanan bisa menggunakan data ini untuk berbagai kebutuhan seperti otomatisasi pengecekan kelemahan suatu sistem, otomatisasi pengecekan kesalahan konfigurasi dan lain sebagainya.

Securitytracker (<http://www.securitytracker.com/>)

SecurityTracker mengumpulkan informasi vulnerabilities dari berbagai sumber yang ada dan menginformasikannya kepada Anda sehingga Anda akan selalu mendapatkan informasi mengenai kelemahan terbaru yang ditemukan.

Anda bisa mendapatkan informasi ini dalam bentuk laporan per-minggu melalui email atau Anda juga bisa mendapatkan laporan seketika ketika suatu kelemahan ditemukan namun untuk layanan yang satu ini, Anda harus rela mengeluarkan sedikit uang.



Keep Track of the Latest Vulnerabilities with SecurityTracker!

[Home](#) | [View Topics](#) | [Search](#) | [Contact Us](#) | [Help](#)

Sunday
December 7 2008

Get Our Premium Vulnerability Notification Service

Expert Analysis

Get Free Weekly
E-Mail Updates
Subscribe to
SecurityTracker

View All

View a Listing of All Recent Vulnerabilities

Sign Up

Sign Up for Your **FREE** Weekly SecurityTracker E-mail Alert Summary

Instant Alerts

Buy our **Premium Vulnerability Notification Service** to receive customized, instant alerts

Affiliates

Put SecurityTracker Vulnerability Alerts on Your Web Site - It's **Free!**

Partners

Become a Partner and **License** Our Database or Notification Service

Report a Bug

Report a vulnerability that you have found to SecurityTracker

[Join](#)
[@](#)
[securitytracker.com](#)

TWiki Input Validation Flaw in %SEARCH{}% Parameter Lets Remote Users Execute Arbitrary Commands

A vulnerability was reported in TWiki. A remote user can execute arbitrary commands on the target system.

Impact: Execution of arbitrary code via network, User access via network

TWiki Input Validation Flaw in %URLPARAM{}% Parameter Permits Cross-Site Scripting Attacks

A vulnerability was reported in TWiki. A remote user can conduct cross-site scripting attacks.

Impact: Disclosure of authentication information, Disclosure of user information, Execution of arbitrary code via network, Modification of user information

NetWare Bug Lets Remote Users Access the ApacheAdmin Console

A vulnerability was reported in NetWare. A remote user can access the target ApacheAdmin console.

Impact: User access via network

Trillian Buffer Overflow in Processing AIM XML Tags May Let Remote Users Execute Arbitrary Code


A vulnerability was reported in Trillian. A remote user can execute arbitrary code on the target user's system.

Impact: Execution of arbitrary code via network, User access via network

Trillian Buffer Overflow in Creating Tooltips Lets Remote Users Execute Arbitrary Code

A vulnerability was reported in Trillian. A remote user can cause arbitrary code to be executed on the target user's system.

Impact: Execution of arbitrary code via network, User access via network



Our Sponsors

Ads by Google

Remote Spying Keylogger
Find out email passwords and chats. Spy on a computer in minutes!
[www.viewsecret.com](#)

GFI Languard Security
Network Security Analyzer Detect security vulnerabilities
[www.gfi.nordic.dk](#)

RedView GPS
GPS Tracker, GPS Tracking Solution ODM Meet your specific requirement
[www.redview.net](#)

Layanan berbayar ini juga memungkinkan Anda untuk memilih atau memonitor informasi-informasi produk tertentu saja sehingga Anda bisa memilih hanya mendapatkan informasi dari produk yang Anda gunakan karena informasi kelemahan semua produk akan membuat Anda banjir informasi.

Securiteam (<http://www.securiteam.com>)

Sama seperti dengan *securitytracker*, *securiteam* juga berusaha mengumpulkan semua informasi mengenai *vulnerabilities* secara terpusat sehingga Anda tidak perlu lagi repot-repot mengikuti berbagai mailing list, situs, dan komunitas hacker.

SecuriTeam
Free // Accurate // Independent

Security News - Security Reviews - Exploits - Tools - UNIX Focus - Windows Focus - Blogs - CVEs

SecuriTeam Home
Ask the Team
Writing Tools
Advancing Info
Advancing Info
Blogs

Mark Bui Testing
Vulnerability Assessment
Vulnerability Scanner

SecuriTeam in Your Inbox

New vulnerability?
New tool?
Tell us
(Our RSS key)

SECURITY
CHECKED
TESTED Dec-08

Featured Articles:

Hacking SOHO Routers
The purpose of this paper is to outline the security measures being taken by vendors to prevent such attacks in their home routing products, what those security measures accomplish, and where they fall short. [More >>>](#)

LibSPF2 DNS TXT Record Parsing Bug
A relatively common bug parsing TXT records delivered over DNS, dating at least back to 2003 in Sendmail 8.3.0 and almost certainly much earlier, has been found in LibSPF2, a library frequently used to retrieve SPF (Sender Policy Framework) records and apply policy according to those records. [More >>>](#)

Vulnerability in Server Service Allows Code Execution (MS08-067)
This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. [More >>>](#)

Latest Articles:

Frame Pointer Overwrite Demonstration (Linux)
8 Dec. 2008

Format String Exploitation Demonstration (Linux)
8 Dec. 2008

JSP dba_replace() Arbitrary File Destruction
20 Nov. 2008

Google Chrome MetaCharacter URI Obfuscation Vulnerability (1 Comment)
20 Nov. 2008

iPhone Configuration Web Utility for Windows Directory Traversal
20 Nov. 2008

Streamripper Multiple Buffer Overflows
20 Nov. 2008

Amaya URL Bar Stack Overflow Vulnerability
20 Nov. 2008

Microsoft Windows Active Directory LDAP Server Information Disclosure Vulnerability
18 Nov. 2008

Checkpoint VPN-1 RAT Information Disclosure
12 Nov. 2008

Vulnerability in SMB Allows Code Execution (MS08-068)
12 Nov. 2008

Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08-069)
12 Nov. 2008

VMware Emulation flaw x84 Guest Privilege Escalation (3RET)
11 Nov. 2008

GlanVW get_unccode_name() Off-By-One Buffer Overflow
11 Nov. 2008

Wlogs
17 Dec. 2008

Exploits
18 Nov. 2008

Tools
1 Dec. 2008

Salah satu kelebihan situs ini adalah update informasi yang cepat, rinci dan terdapat bagian tutorial/artikel buat Anda yang suka mempelajari masalah keamanan.

Secunia (<http://secunia.com/>)

What's on your PC?
Secure? **Vulnerable!**
Updated!

Personal Software Inspector 1.0
Out now! Free!

Search here

Vulnerability Intelligence | Vulnerability Scanning | Community | Blog **new entry!** | Corporate Information | Online Shop | Customer Login

Home

Welcome to Secunia.com

Vulnerability Database

- Covering all products and vulnerabilities
- 23,915 Secunia advisories published to date
- Get the latest vulnerability intelligence

[Secunia Advisories](#)

In-depth Analysis

- Detailed analysis of vulnerabilities
- Proof of concept and exploit code
- Restricted to certain companies and organisations

[Binary Analysis](#)

Secunia News

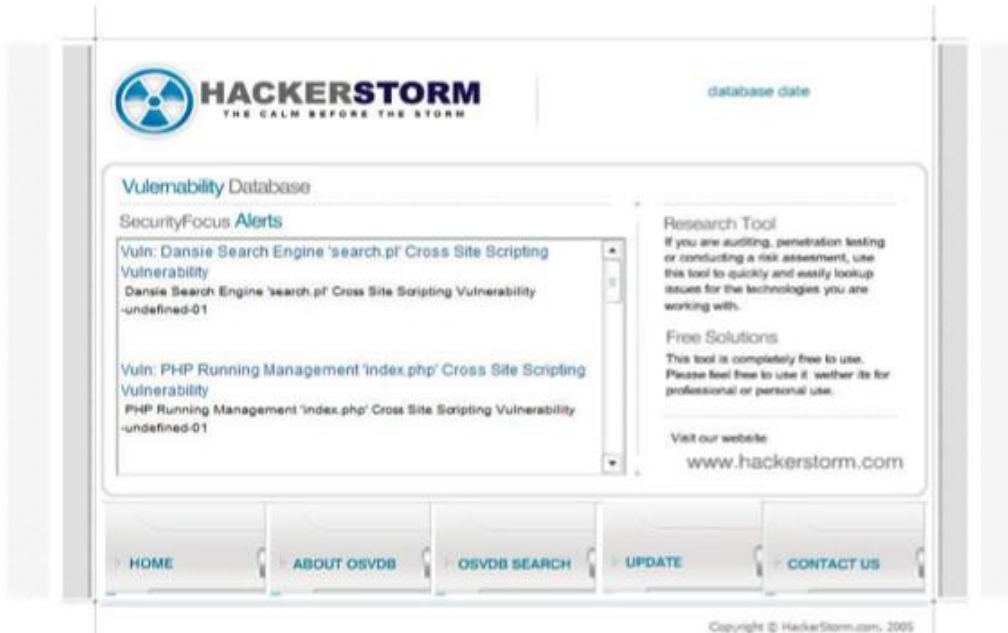
3rd Dec, 2008 - new!
1-91% of all PCs are fully patched! [Read more](#)

2nd Dec, 2008 - new!
Monthly Binary Analysis Update. [Read more](#)

25th Nov, 2008
Secunia BSI 1.0 Beta Review

Secunia membuat security scanner bernama *Internal Vulnerability Scanner – Secunia NSI* yang selain menjual produk dan jasa, juga mengeluarkan banyak informasi mengenai kelemahan produk. Walaupun tidak selengkap *securiteam* atau *securitytracker*, situs ini pantas juga menjadi rujukan karena banyak informasi kelemahan produk yang diinformasikan oleh secunia berdasarkan research yang dilakukan oleh team mereka.

Hackerstorm (www.hackerstorm.com)

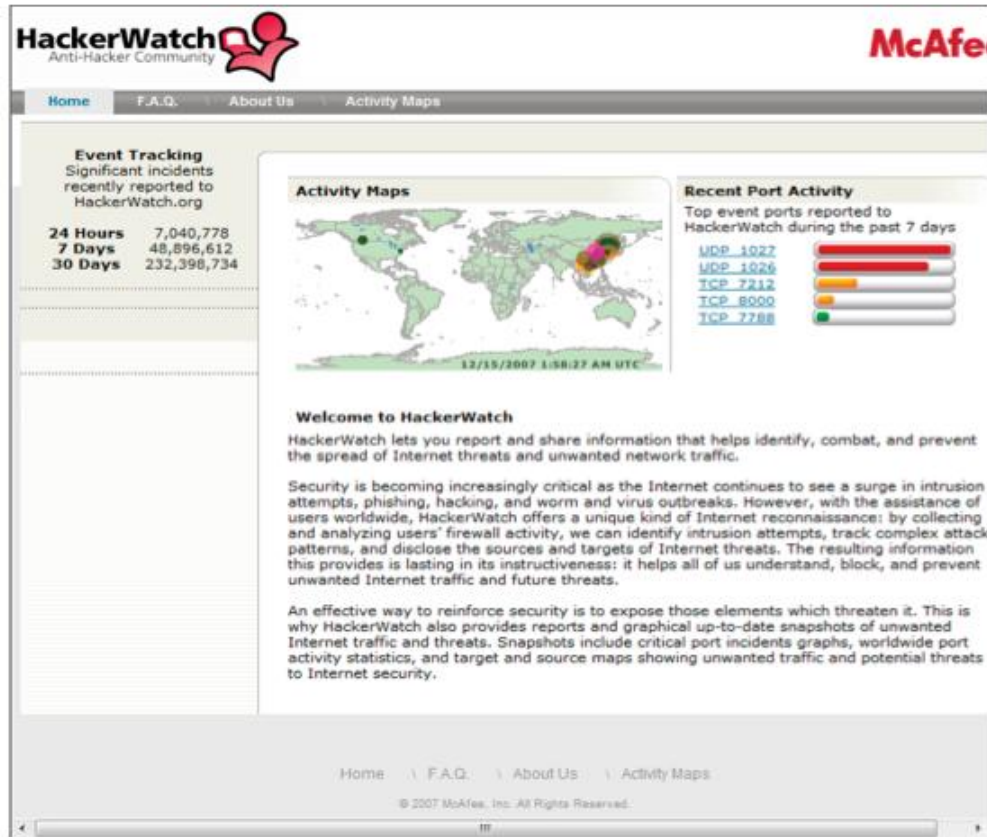


Situs ini menyediakan informasi kelemahan lebih dari 1500 vendor. Keunggulannya adalah Anda bisa mendownload program kecil yang disediakan untuk mencari informasi kelemahan suatu produk baik secara online maupun offline secara gratis.

Hackerwatch (<http://www.hackerwatch.org>)

Situs ini melaporkan traffic atau lalu lintas data yang dicurigai sebagai ancaman terhadap keamanan internet. Laporan yang dihasilkan sangatlah menarik karena berbentuk grafik dengan warna-warna yang sangat mudah untuk dipahami dan menarik.

Anda bisa melihat ancaman yang sedang terjadi secara global di internet dalam bentuk animasi, misalnya gerakan penyebaran dari worm/virus dari satu daerah ke daerah lainnya.



SecurityFocus (<http://www.securityfocus.com>)

Securityfocus adalah situs yang menjadi sumber informasi yang terpercaya dan dihormati. *Securityfocus* terkenal dengan netralitasnya dan juga informasi-informasi yang berbobot. Situs ini juga mengelola mailinglist security paling terkenal didunia, yaitu *bugtraq*.

Mailing list yang dikelola oleh *securityfocus* ini diikuti oleh para ahli dari berbagai perusahaan seperti Microsoft, Cisco, dll. Selain para ahli dari vendor, anggota dari mailinglist *bugtraq* juga berasal dari para administrator, hobbies, konsultan, end user, dll.

Karena topik security yang begitu luas, *securityfocus* membagi mailinglist yang dikelolanya ini menjadi bagian yang lebih kecil dan terfokus pada bidang tertentu seperti mailinglist khusus produk Microsoft dan linux, mailing list khusus masalah forensics, dll.

Jika Anda ingin mengikuti mailinglist securityfocus, ikutilah mailinglist yang Anda butuhkan saja, dan sebaiknya jangan mengikuti semua mailing list yang ada karena terdapat ratusan email setiap harinya dari sebuah mailing list yang ramai.

SCMagazine (<http://scmagazine.com>)

Anda bisa mendapatkan banyak informasi mengenai masalah keamanan melalui situs SC Magazine. Situs ini mengkhususkan dirinya

pada pemberitaan masalah keamanan yang terjadi didunia, selain itu SC Magazine juga melakukan review produk-produk keamanan. Bila Anda mau, Anda juga bisa berlangganan tabloit gratis yang akan dikirimkan ke email Anda dua kali dalam seminggu.

Zone-h (<http://zone-h.org>)

The screenshot shows the Zone-h website interface. At the top, there's a banner that says "THIS SPACE IS FOR RENT" with a "CLICK ON THIS BANNER TO KNOW MORE" link. Below the banner, there's a search bar and a date display "Monday, 06 December 2006".

LAST WEEK ATTACKS

O.S.	Defns.	%
Linux	6002	70.65%
Win 2003	1672	19.69%
Solaris 8/10	311	3.66%
FreeBSD	228	2.69%
Win 2000	155	1.82%
Other	130	1.53%

Total attacks: 8496 of which 3101 single ip and 5395 mass defacements

HIGHLIGHT ON MOST RECENT ATTACKS

LATEST ADVISORIES

- IBM Security Advisory: AIX 6.1 multiple security vul

LATEST ON DIGITAL WARFARE

- Derp's "Insect in IC": a smart article and our comments
- ICANN and SIDA domains hijacked by Turkish crackers
- Systemic wars of the third millennium
- Phoenix Lander project website defaced: UPDATED
- G.O.B group members arrested

LATEST ON GEOPOLITICS

- Bloggers blogs, Olympic blogs the Chinese way
- Internet security becomes the real threat
- War 2.0
- New C&M world war
- Snake Oil

CERN'S LHC HIT WITH THE SAME CERN TECHNOLOGY BY GREEK HACKERS

ITsec News

Written by Sy884738 (Roberto Preadoni)
Monday, 15 September 2008

The phantom Higgs boson still has no face, as the Cern's LHC (Large Hadron Collider) didn't produce yet the planned proton collisions. Meanwhile Cern's website lost his own face, due to a Greek group of defacers called GST (Greek Security Team).

The defacers left a homepage message in Greek language. While when we learned about the CERN defacement everybody here was thinking about a politically, etically or scientifically motivated attack, once translated, the message left by the defacers embraces the usual topics so much loved by true script kiddies: we are the best, you are the worst, we are left, you are lame, we are 2500 (I wonder if these guys actually know what 2500 means in the hacker world...), we wars... blah blah blah.

WIRELESS HACKING

Nov. 10th-14th Special session Bratislava - SK private
Nov. 11th-12th Hott Unlimited Johannesburg - ZA Telospace
Nov. 18th-19th Wireless Hacking Roma - IT Domatec
Nov. 17th-18th Wireless Hacking Warsaw - PL Clixu
Nov. 19th-20th Wireless Hacking Bratislava - SK SAT
Nov. 26th-27th Wireless Hacking Oslo - NO Watchcom
Nov. 27th-28th Wireless Hacking Carosno Port - IT Plug in
Nov. 25th-26th Wireless Hacking Roma - IT Domatec
Nov. 27th-28th Hot WebApp Tokyo - JP Ruchu
Dec. 19th 20th Hott Unlimited Rocho - JP Ruchu

MAIN MENU

- Home
- Digital Warfare
- Geopolitics
- ITsec News
- ITsec Advisories
- Test Drive
- 360°
- Digital Attacks Archive
- Zone-H events
- Publications
- Zone-H Friends/Partners
- Contact Us
- Search
- Download Area

Selain menyediakan berita dan artikel mengenai masalah keamanan, zone-h terkenal dengan pencatatan halaman deface yang dilakukan oleh hacker. Zone-h melakukan mirroring terhadap website yang telah dideface oleh hacker sehingga Anda bisa melihat dokumentasi dari aksi hacker ini. Situs ini juga seringkali menjadi rujukan statistik serangan hacker seperti pada saat buku ini dibuat, terlihat mesin linux paling banyak mendapatkan serangan yang diikuti oleh mesin windows 2003 dan Solaris.

Milw0rm (<http://www.milw0rm.com/>)

[\[home \]](#)
[\[contents \]](#)
[\[platforms \]](#)
[\[shellcode \]](#)
[\[search \]](#)
[\[cracker \]](#)
[\[links \]](#)
[\[rss \]](#)
[\[archive \]](#)

MILW0RM

[remote]

DATE	DESCRIPTION	HITS		AUTHOR	
2008-12-05	NULL FTP Server 1.1.0.7 SITE Parameters Command Injection Vuln	2354	R	D	Tan Chew Keong
2008-11-23	Microsoft XML Core Services DTG Cross Domain Scripting PoC MS08-069	10232	R	X	Jerome Athias
2008-11-21	vsftpd <= 0.9.9-RC2 Remote Command Execution Vulnerability	5300	R	D	valkyrieux
2008-11-21	KVirc 3.4.2 Shing (url handler) Remote Command Execution Exploit	4359	R	X	NineSituationsGroup
2008-11-20	Eondux 0.10 (url handler) Arbitrary Parameter Injection Exploit	2267	R	X	NineSituationsGroup
2008-11-18	Net-IP DCC <= 2.1.7 Remote Code Execution Exploit	9393	R	D	XenoHula

[local]

DATE	DESCRIPTION	HITS		AUTHOR	
2008-12-05	PGD <= 0.91 Malformed PE File Universal Buffer Overflow Exploit	1448	R	D	S&D
2008-12-03	RadAssn <= 2.2.1.4 (.RAP File) WindowsCallProcA Pointer Hijack Exploit	1411	R	D	DATA_SNIPER
2008-12-03	Cain & Abel 4.9.23 (vdp file) Buffer overflow Exploit	1849	R	D	Encrypt3d.Hnd
2008-12-01	Dubius GNU/Linux (symlink attack in login) Arbitrary File Ownership PoC	3870	R	D	Paul Szabo
2008-11-30	Cain & Abel <= v4.9.24 .RDP Stack Overflow Exploit	2942	R	D	S&D
2008-11-28	Apache Tomcat runtime.getRuntime().exec() Privilege Escalation (win)	2680	R	D	Abysssec

[web apps]

DATE	DESCRIPTION	HITS		AUTHOR	
2008-12-07	ASP Talk (SQL/CSO) Multiple Remote Vulnerabilities	201	R	D	Blackw0rd
2008-12-07	PHPMyGallery Gold 1.31 (index.php) Directory Traversal Vulnerability	182	R	D	sAs
2008-12-07	Qmail Mailbox List Manager 1.2 Database Disclosure Vulnerability	172	R	D	Ghost Hacker
2008-12-07	Mini-CMS 1.0.1 (index.php) Multiple Local File Inclusion Vulnerabilities	152	R	D	c0ndemned
2008-12-07	Mini Blog 1.0.1 (index.php) Multiple Local File Inclusion Vulnerabilities	148	R	D	c0ndemned
2008-12-07	ASPManga Banners (RFU/DD) Multiple Remote Vulnerabilities	144	R	D	Z0RLLa
2008-12-07	Ikoon AdManager 2.1 Remote Database Disclosure Vulnerability	129	R	D	Ghost Hacker
2008-12-07	Professional Download Assistant 0.1 Database Disclosure Vulnerability	127	R	D	Ghost Hacker
2008-12-07	Nettachat 1.12 (nettachat112.mdb) Database Disclosure Vulnerability	118	R	D	OffensiveTrack
2008-12-07	WebBlog CMS 3.0.3 Arbitrary File Upload & LFI Exploit	124	R	D	DNX
2008-12-07	Product Sale Framework 0.15 (forum_topic_id) SQL Injection Vulnerability	124	R	D	h3h4dd
2008-12-07	PayPal eStore Admin Password Changing Exploit	204	R	D	G4H0K
2008-12-07	Samza Cart <= 1.10 Admin Password Changing Exploit	149	R	D	G4H0K
2008-12-07	DL PayCart <= 1.24 Admin Password Changing Exploit	128	R	D	G4H0K
2008-12-07	1980v3 <= 1.44 Admin Password Changing Exploit	128	R	D	G4H0K
2008-12-06	phpPgAdmin <= 4.2.1 (.language) Local File Inclusion Vulnerability	1069	R	D	dan

Milw0rm adalah situs favorit para hacker karena situs ini memberikan informasi dan juga berbagai code yang bisa digunakan untuk melakukan eksploitasi atau hacking. Selain itu, situs milw0rm juga menyediakan tutorial dalam bentuk video mengenai hacking. Informasi diupdate setiap harinya yang terkadang bisa mencapai lebih dari 10 informasi kelemahan beserta code-code eksploitasinya yang siap digunakan.

Jasakom (<http://www.jasakom.com>)

Ini adalah situs lokal satu-satunya yang terus diupdate dengan berbagai informasi mengenai keamanan komputer dalam bahasa indonesia. Selain artikel-artikel teknis keamanan, terkadang juga

terdapat artikel teknis mengenai penerobosan situs seperti kejadian penerobosan situs kebudayaan malaysia dan informasi mengenai penerobosan situs KPU pada saat pemilu berlangsung.



Bagaimana Ethical Hacker Bekerja

Seorang *Ethical Hacker* harus mengetahui dengan pasti bagaimana pekerjaan dan juga apa yang harus dilakukan sebagai seorang profesional. Seorang *Ethical Hacker* misalnya, tidak boleh menyebarkan informasi yang didapatkannya kepada publik karena informasi tersebut bisa disalah-gunakan atau dimanfaatkan untuk tujuan yang merugikan.

Seorang *Ethical Hacker*, ibarat seorang dokter yang memeriksa penyakit pasien, harus bisa menjaga rahasia dan juga harus mengetahui dengan pasti bagaimana bekerja dengan “nyawa” pasiennya.

Sebelum melakukan hal-hal teknis, *Ethical Hacker* akan membicarakan terlebih dahulu kepada client mengenai kebutuhan dan juga tujuan yang hendak dicapai. Setelah mendapatkan semua informasi tersebut, *Ethical Hacker* akan menyiapkan dokumen NDA (*NonDisclosure Agreement*) untuk di tanda-tangani bersama dengan client.

Tujuan dari dokumen ini sangatlah penting karena merupakan dokumen hukum tentang rahasia yang harus dijaga dan pekerjaan yang dilakukan. Dokumen inilah yang akan melindungi *Ethical Hacker* dari tuntutan hukum dan merupakan bukti hitam diatas putih yang berlaku di pengadilan.

Banyak contoh dari dokumen NDA ini di internet yang bisa Anda pelajari atau jika Anda memahami hukum, Anda juga bisa membuatnya sendiri. Dokumen NDA bisa dikatakan sebagai tiket keluar penjara seandainya terdapat kasus hukum, karena itu jangan mengabaikannya ketika Anda diminta untuk melakukan *penetration testing*.

Setelah menandatangani NDA, *Ethical Hacker* bisa segera menyiapkan hal-hal teknis maupun non teknis sebelum memulai usaha percobaan penerobosan ke dalam sistem komputer client seperti *schedule* dan juga tim yang akan melakukannya.

Setelah selesai melakukan tugasnya, *Ethical Hacker* harus menyiapkan laporan kepada client mengenai apa saja yang telah dilakukannya dan permasalahan apa yang telah ditemukan. Biasanya juga terdapat rekomendasi tentang bagaimana memperbaiki permasalahan yang berhasil ditemukan. Pekerjaan ini umumnya dikenal dengan *Penetration Testing*.

Jenis Testing

Perusahaan menghadapi ancaman dari berbagai sisi. Hacker yang diantisipasi berasal dari luar perusahaan namun kenyataannya, lebih banyak penerobosan dilakukan oleh karyawan sendiri. Karena itu, *Ethical Hacker* menggunakan beberapa pendekatan dalam melakukan security testing yaitu :

1. **Black-box Hacking** : Metode ini memposisikan hacker sebagai orang dari luar perusahaan yang tidak mengetahui apapun mengenai perusahaan tersebut. Hacker akan mencoba mencari informasi dari segala sumber informasi yang bisa didapatkan dan mencoba menerobos ke dalam perusahaan.
2. **White-box Hacking** : Metode ini memposisikan hacker sebagai orang yang telah mengetahui segala hal tentang perusahaan baik teknis maupun non teknis, bahkan seorang yang memiliki akses kedalam source code program dan segala informasi penting lainnya. Jadi hacker telah mengetahui bagaimana jaringan perusahaan dibentuk, sistem operasi yang digunakan, pertahanan yang dimiliki, prosedur dan segalanya. Dengan informasi detail semacam ini, *Ethical Hacker* akan mencoba menerobos ke dalam perusahaan untuk melihat kelemahan yang ada pada sistem pertahanan.
3. **Gray-box Hacking** : Metode ini dikenal juga dengan internal testing atau penetrasi/pengujian yang dilakukan didalam jaringan perusahaan. Metode testing mengasumsikan hacker mengetahui informasi sistem yang digunakan namun dalam tahap yang terbatas. Contoh kasus semacam ini adalah karyawan didalam perusahaan itu sendiri yang tentunya mengetahui prosedur dan sistem yang digunakan namun pengetahuan itu masih terbatas karena data super sensitif seperti source code program dll tidak diketahui.

Metodologi Testing

Jika Anda diminta untuk melakukan *security testing* ataupun *security audit* terhadap sebuah perusahaan, apa yang Anda lakukan terlebih dahulu? apa saja yang Anda test? apa yang Anda periksa? pertanyaan ini tidak hanya menghinggapi orang-orang yang berniat memulai bisnis *security testing* dan jawaban atas pertanyaan ini memang tidak mudah.

Berbagai metode digunakan dan umumnya perusahaan besar memiliki check list tentang apa yang harus dilakukan dan apa yang akan diperiksa. Cara kerja yang sama bisa Anda lihat di WC-WC yang umumnya mempunyai lembaran check list yang harus dicek

oleh petugas WC, apakah tissue masih tersedia? apakah air berjalan dengan lancar? apakah lantai sudah dibersihkan? dlsb.

Membuat check list semacam ini adalah pekerjaan mudah saat Anda membayangkannya namun ketika Anda mulai mengetik dan mulai mengerjakannya, Anda akan mengetahui betapa sulitnya membuat security check list semacam ini. Tidak percaya? Silahkan mencobanya dan lihat sendiri hasilnya.

Jika Anda kesulitan membuatnya, jangan khawatir karena Anda tidak sendirian. Banyak orang mengalami hal yang sama dengan Anda dan sudah banyak organisasi yang mencoba membantu orang-orang seperti Anda, termasuk pemerintah suatu negara. NIST (*National Institute of Standard and Technology*) menyediakan banyak sekali dokumen-dokumen yang bisa dijadikan panduan dalam mengamankan komputer, network, mail server dan tentu saja panduan dalam melakukan security test. Anda bisa mengunjungi situs NIST di <http://csrc.nist.gov/publications/PubsSPs.html>. Saya telah mendownload dokumen **NIST-SP800-42.pdf** yang berjudul "*Guideline on Network Security Testing*" untuk Anda didalam CD yang disertakan bersama dengan buku ini.

Metodologi yang lebih terkenal lagi dan banyak disukai adalah *Open Source Security Testing Methodology Manual (OSSTMM)*. Dokumen OSSTMM ini banyak sekali digunakan oleh *White Hat Hacker* dalam melakukan tugasnya karena memberikan checklist dan panduan yang sangat jelas.

Pada saat buku ini dibuat, versi terakhir dari dokumen OSSTMM adalah **OSSTMM_3.0_LITE.pdf** yang bisa Anda dapatkan melalui situs OSSTMM di <http://www.isecom.org/osstmm/> atau Anda bisa mendapatkannya pada CD yang disertakan bersama dengan buku ini.

Module 2

Footprinting

Penipu

Bapak Joe mendapatkan telpon dari orang yang mengaku dari rumah sakit. Orang tersebut mengatakan bahwa anak-nya si Joe kecil mendapatkan kecelakaan yang sangat serius, kepalanya bocor karena tertabrak oleh bis yang ngebut dan harus segera dioperasi namun dibutuhkan uang jaminan untuk itu karena rumah sakit tidak mau melakukan operasi tanpa uang jaminan. Dengan panik bapak Joe berusaha menenangkan dirinya dan mencoba menghubungi anaknya melalui HP berkali-kali tapi HP si anak ternyata mati dan tidak bisa dihubungi! Tanpa ragu-ragu lagi, Bapak Joe percaya 100% dengan informasi yang diterimanya dan segera mentransfer uang yang dibutuhkan sebelum buru-buru berangkat ke rumah sakit. Ternyata.... semua ini penipuan!

Aksi penipuan ini kabarnya memakan banyak korban. Berbagai isu-pun bertebaran. Si keparat adalah penipu ulung yang melakukan aksinya dengan perencanaan yang sangat baik sehingga korban yang rata-rata adalah orang kaya, yang mempunyai pengetahuan cukup luas dan tinggi, tetap bisa tertipu. Penipu mengumpulkan segala informasi yang dibutuhkan seperti nomor telepon rumah, nama orang tua, alamat, dlsb sebelum melancarkan aksi penipuannya. Selain mengumpulkan informasi yang sangat detail mengenai korbannya ini, sang penipu juga mempunyai kemampuan teknis cukup yaitu "mematikan telp si anak" agar tidak bisa dihubungi oleh orang tuanya.

Penipu menggunakan beberapa cara untuk mematikan HP sang korban. Pertama, penipu akan menghubungi si anak dan mengaku berasal dari kepolisian atau operator seluler yang sedang menyelidiki pembengkakan pulsa yang terjadi dan meminta agar HP si anak dimatikan terlebih dahulu namun Informasi lain menyebutkan bahwa mereka tidak pernah mematikan handphonenya namun yang aneh adalah signal handphone mereka tiba-tiba tidak bisa digunakan pada waktu itu. Kecurigaan-pun tertuju pada operator handphone yang ikut bermain namun saya tidak percaya karena permainan ini terlalu "kasar" dengan jumlah uang yang terlalu kecil (kecuali ada anggota komplotan yang juga bekerja di operator seluler).

Mematikan handphone atau membuat sebuah handphone tidak bisa dihubungi bisa dilakukan dengan cara yang sangat mudah yaitu dengan teknik Jamming! Jika Anda pernah mendengar siaran radio yang terganggu oleh siaran radio lainnya, maka Anda akan mudah memahami hal ini. Sebuah alat Jamming bisa dibuat dengan biaya yang cukup murah. Alat ini bisa mengeluarkan frekwensi yang sama dengan frekwensi handphone, akibatnya adalah signal handphone yang berada di daerah jangkauan alat Jamming ini akan menjadi rusak dan tidak bisa digunakan. Saya pernah mencoba alat Jamming yang dibuat secara khusus untuk mengacaukan frekwensi handphone, berbentuk seperti HT dan dijual dengan harga dibawah 6 juta rupiah.

Jasakom bisa dikatakan sebagai komunitas keamanan yang paling berkembang pada tahun 2000 silam. Karena 'prestasi' ini, bukan lagi hal yang aneh bila banyak hacker yang mencoba melakukan serangan dan mencoba men-deface situs Jasakom. Pada tahun 2001, seorang hacker berinisial FC (*Fabian Clone*) yang cukup terkenal pada jaman tersebut akhirnya berhasil masuk dan melakukan perubahan pada halaman muka jasakom. Waktu itu FC hanya menaruh sebuah "tulisan kecil" agar tidak terlalu "memalukan" bagi situs Jasakom. Walaupun demikian, hal ini tentunya sudah cukup membuktikan bahwa tindakan yang lebih brutal dengan mudah bisa dilakukan.

Hacker yang masuk ke situs Jasakom, tidak melakukan penyerangan langsung atau mengeksploitasi kelemahan yang ada pada situs Jasakom. Masalahnya ternyata terletak pada salah satu server Brinskter, web hosting tempat dimana web jasakom bernaung. Dengan mengeksploitasi salah satu server di brinkster dan menjadikannya sebagai "pintu masuk" ke situs Jasakom, akhirnya aksinya bisa berhasil. Ini adalah contoh bagaimana seorang hacker tidak selalu menyerang dari pintu depan, namun juga bisa menyerang dari pintu samping, pintu belakang, cerobong asap dan bahkan rumah tetangga seperti kejadian yang menimpa situs jasakom ini.

Kenali musuh Anda, maka Anda akan memenangkan ribuan berperangan, ini adalah kata-kata Sun Tzu yang sangat terkenal. Sebelum melakukan serangan, seorang hacker akan mengenali terlebih dahulu siapa calon korbannya dengan mengumpulkan informasi sebanyak mungkin. Pengumpulan informasi ini bertujuan untuk menemukan sebanyak mungkin "pintu masuk" yang mungkin bisa dilakukan.

Jika Anda tidak bisa masuk dari pintu depan, cobalah pintu samping, jika tidak bisa, cobalah terobos dari jendela atau dari bawah tanah sekalian ! Jadi, mengumpulkan data tentang kemungkinan "jalan masuk" yang bisa digunakan sangatlah penting. Metodologi pengumpulan data (*Information Gathering*) dalam sertifikasi CEH dibagi menjadi 7 tahap yaitu :

1. Menggali informasi awal
2. Mencari Informasi Range Jaringan yang digunakan
3. Mencari komputer yang aktif
4. Mencari port yang terbuka dan keberadaan Access Point

5. OS Fingerprinting
6. Fingerprinting services
7. Network Mapping.

Tahapan pertama dan kedua, yaitu menggali informasi awal dan mencari informasi range jaringan yang digunakan termasuk dalam kategori *Footprinting* yang akan kita bicarakan pada bab ini sedangkan selebihnya termasuk dalam Scanning yang akan dibicarakan pada bab selanjutnya.

1. Menggali Informasi Awal

Banyak cara yang bisa digunakan untuk mendapatkan informasi sebuah perusahaan atau jaringan yang ada didalamnya.

1.1. Mendapatkan informasi dari website resmi

Website resmi perusahaan, misalnya www.apasaja.co.id, merupakan sumber yang sangat berharga dan mudah untuk mendapatkan informasi mengenai sebuah perusahaan. Anda bisa membaca berbagai berita mengenai perusahaan. Dari situ, Anda bisa mengetahui petinggi dari perusahaan, anak perusahaan dan terkadang perusahaan mempublikasikan informasi mengenai komputer atau pertahanan yang mereka gunakan kepada publik.

Anda juga bisa melihat informasi mengenai lowongan kerja yang biasanya terdapat pada situs perusahaan. Untuk apa melihat lowongan kerja ? Tidak, tentu saya tidak meminta Anda melamar kerja ditempat tersebut namun Anda bisa melihat orang-orang yang kualifikasi yang dibutuhkan. Misalnya, Anda melihat informasi lowongan seperti berikut :

Dibutuhkan : Network Administrator

Syarat :

- *Pengalaman min 2 tahun*
- *Mampu menangani Network dengan sistem operasi Windows dan Linux*
- *Menguasai switch dan router cisco*
- *Menguasai ISA 2006 dan Microsoft Exchange server 2005*

Dari informasi kerja ini, hacker bisa mengetahui bahwa perusahaan tersebut menggunakan sistem operasi Windows dan Linux dengan switch dan router cisco. Hacker bisa mencari informasi kelemahan pada sistem tersebut dan mencoba melakukan eksploitasi terhadapnya.

Karena perusahaan tersebut juga menggunakan ISA 2006, hacker bisa mengetahui bahwa perusahaan cukup peduli dengan masalah keamanan dan memiliki firewall. Email server yang digunakan adalah Exchange Server 2007, jadi bisa diperkirakan bahwa sebagian besar, produk Microsoft yang digunakan dengan versi terbaru. Tanpa perlu bersusah payah, hacker sudah mendapatkan sedikit gambaran mengenai jaringan dan infrastructure yang digunakan oleh perusahaan tersebut.

1.2. Mendapatkan informasi dari nama domain atau alamat IP

Hanya melalui nama domain atau alamat IP dari sebuah perusahaan, hacker bisa mendapatkan banyak informasi darinya. Setiap nama domain, didaftarkan dan mempunyai nama penanggung jawab serta berbagai informasi penting lainnya seperti email, nomor telp, dll yang tersedia kepada publik.



Di Internet, terdapat 4 penguasa yang bertugas mengalokasikan dan administrasi penggunaan alamat IP. Penguasa ini disebut sebagai *Regional Internet Registries* (RIR). Kok disebut sebagai Regional? karena daerah kekuasaan mereka dibagi-bagi berdasarkan *regional* (daerah) dan ke-empat penguasa tersebut adalah :

1. ARIN (www.arin.net), penguasa daerah North America dan sub-Sharan Afrika
2. APNIC (www.apnic.net), penguasa Asia Pacific
3. LACNIC (www.lacnic.net), penguasa Southern dan Central America dan Carribean
4. RIPE NCC (www.ripe.net), penguasa Europe dan northern Africa

Untuk mendapatkan pemilik alamat IP, Anda bisa mencarinya berdasarkan masing-masing regional. Saya sama sekali tidak mengetahui lokasi pemilik IP, lalu harus menggunakan situs yang mana? Pertanyaan bagus, gunakan saja ARIN yang akan memberikan referensi lanjut kepada Anda. Kenapa harus ARIN? Karena alasan sejarah. Perhatikan informasi dari APNIC (*For historical reasons, the ARIN Whois Database is generally the starting point for searches. If an address is outside of ARIN's region, then that database will provide a reference to either APNIC or RIPE NCC*)

Jika ada yang mencari bos dari ke-empat penguasa regional, dia adalah IANA (Internet Assigned Numbers Authority). IANA bertanggung jawab terhadap keseluruhan manajemen dan koordinasi DNS serta pendelegasian nama domain di dunia ini.

Sebagai contoh, saya mendapatkan alamat IP orang yang telah mengancam saya adalah 202.53.255.221. Karena saya tidak mengetahui lokasi, atau apapun tentang alamat IP ini, saya mencarinya melalui whois-nya ARIN (www.arin.net). Dari ARIN, terlihat bahwa alamat IP 202.53.255.221 dibawah kekuasaan APNIC.

Berdasarkan informasi ini, saya-pun ke situs APNIC untuk mengetahuinya lebih lanjut. Situs APNIC akhirnya menginformasikan bahwa pemilik IP tersebut adalah ISP IndoInternet. Langkah selanjutnya yang bisa saya lakukan adalah menghubungi IndoInternet dan menanyakan pengguna alamat IP 202.53.255.221.

Pencarian informasi mengenai sebuah domain juga bisa dilakukan dengan tools yang akan lebih memudahkan pengguna karena tidak perlu mengunjungi alamat RIR. Salah satunya adalah dengan perintah *Whois*. Fasilitas whois ini juga banyak tersedia secara online seperti samspace.org, centralops.net, www.allwhois.com, www.betterwhois.com, www.dnsstuff.com dan masih banyak lagi yang lainnya. Pada contoh, saya memasukkan nama domain bhineka.com pada situs centralops.net dan mendapatkan hasil :

Registrant:

Garputala Komunika Tujuh
Nicholas Tio
Jl. Gunung Sahari Raya 73C # 5-6
Jakarta, 10610

ID
Email: nicholas@bhinneka.com

Registrar Name.....: REGISTER.COM, INC.
Registrar Whois....: whois.register.com
Registrar Homepage: www.register.com

Domain Name: bhineka.com

Created on.....: Tue, Mar 14, 2000
Expires on.....: Sat, Mar 14, 2009
Record last updated on..: Thu, Nov 29, 2007

Administrative Contact:
Bhinneka Mentari Dimensi PT.
Nicholas Tio
Jl. Gunung Sahari Raya 73C # 5-6
Jakarta, 10610
ID
Phone: +62 (21) 4261617
Email: nicholas@bhinneka.com

Technical Contact:
Bhinneka Mentari Dimensi PT.
Nicholas Tio
Jl. Gunung Sahari Raya 73C # 5-6
Jakarta, 10610
ID
Phone: +62 (21) 4261617
Email: **nicholas@bhinneka.com**

DNS Servers:

dns229.c.register.com
dns249.d.register.com
dns131.a.register.com
dns133.b.register.com


bhineka.com IN MX exchange: relay2.exodus.net

Berdasarkan informasi yang didapatkan dari centralops ini, bisa diketahui alamat dari [bhineka](http://bhineka.com), orang yang bertanggung jawab (nicholas@bhineka.com), DNS server yang digunakan yang menunjukkan [bhineka](http://bhineka.com) meregister domainm mereka di register.com dll. Melalui centralops ini, hacker juga bisa melihat MX record atau alamat email server yang digunakan serta informasi lainnya. Semua informasi ini bisa menjadi "pintu masuk" alternatif bagi hacker.


1.3. Netcraft, mendapatkan informasi domain

Netcraft.com, adalah sebuah situs yang melakukan memonitoring terhadap website-website yang ada di internet. Situs ini menganalisa sistem operasi dan web server yang digunakan. Selain itu, netcraft juga mencatat informasi yang sangat berharga lainnya yaitu sejarah hosting sebuah website lengkap dengan informasi alamat IP beserta webserver dan sistem operasi yang digunakan.

Pada gambar berikut, saya memasukkan nama domain dari *www.bhineka.com* dan terlihat informasi terakhir mengenai web server bhineka diambil pada tanggal 12 Oktober 2007. Pada saat itu, Bhineka.com diketahui menggunakan sistem operasi Windows Server 2003 dengan Web Server IIS 6.0 dan servernya berada di ISP CBN. Dengan mengetahui secara jelas lingkungan yang digunakan oleh korban, hacker akan lebih mudah melakukan aksinya.



Every Rack Is Private
100GigE Cisco Network
Public & Private Networks



do it faster. do it better. do it in private.

Site Search

Toolbar

Netcraft

Site report for www.bhineka.com

Site	http://www.bhineka.com	Last reboot	5 days ago
Domain	bhineka.com	Netblock owner	Network Operations Center
IP address	202.158.49.178	Site rank	158011
Country	ID	Nameserver	dns131.a.register.com
Date first seen	December 1999	DNS admin	root@register.com
Domain Registry	register.com	Reverse DNS	ip49-178.cbn.net.id
Organisation	Garputala Komunika Tuguh, Nicholas Tio, Jl. Gunung Sahari Raya 73C # 3-6, Jakarta, 10610, Indonesia	Nameserver Organisation	Register.Com, Inc., 375 Eighth Avenue, 11th Floor, New York, 10018, United States
Check another site:	<input type="text"/>	Netcraft Site Report Gadget	[More Netcraft Gadgets]

Automated OS Reloads

100GigE
Cisco Network
Public & Private
Networks

Every Rack Is A Private Rack

Hosting History

Netblock Owner	IP address	OS	Web-Server	Last changed
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.178	Windows Server 2003	Microsoft-IIS/6.0	12-Oct-2007
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.178	Windows Server 2003	Microsoft-IIS/6.0	10-Jul-2007
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.178	Windows Server 2003	Microsoft-IIS/6.0	16-Apr-2007
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.178	Windows Server 2003	Microsoft-IIS/6.0	10-Apr-2007
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.178	Windows Server 2003	Microsoft-IIS/6.0	9-Jan-2007
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH	203.130.232.112	Windows 2000	Microsoft-IIS/5.0	21-Dec-2006

1.4. Mendapatkan arsip website

INTERNET ARCHIVE
Wayback Machine

Enter Web Address: All Adv. Search Compare Archive Pages

<http://www.jasakom.com> 282 Results

site was updated.
y becomes available here 6 months after collection. [See FAQ](#).

Search Results for Jan 01, 1996 - Jun 22, 2007

1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
0 pages	0 pages	0 pages	4 pages	13 pages	26 pages	37 pages	114 pages	70 pages	18 pages
			Feb 02, 2001 Feb 05, 2001 Mar 01, 2001 May 17, 2001	Mar 28, 2002 May 23, 2002 Jun 03, 2002 Jun 06, 2002 Jul 21, 2002 Aug 02, 2002 Sep 22, 2002 Sep 27, 2002 Sep 29, 2002 Nov 25, 2002 Nov 26, 2002 Nov 30, 2002 Dec 01, 2002	Jan 22, 2003 Jan 24, 2003 Feb 19, 2003 Feb 20, 2003 Mar 31, 2003 Apr 05, 2003 Apr 05, 2003 Apr 07, 2003 Apr 19, 2003 May 25, 2003 Jun 05, 2003 Jun 08, 2003 Jun 09, 2003 Jun 19, 2003 Jul 19, 2003 Sep 29, 2003 Sep 29, 2003 Oct 02, 2003 Oct 09, 2003 Oct 25, 2003 Nov 27, 2003 Dec 01, 2003	Feb 24, 2004 Mar 04, 2004 Mar 16, 2004 Apr 06, 2004 May 18, 2004 May 18, 2004 Jun 05, 2004 Jun 08, 2004 Jun 11, 2004 Jun 14, 2004 Jun 18, 2004 Jun 28, 2004 Jun 29, 2004 Jul 04, 2004 Jul 05, 2004 Jul 12, 2004 Jul 14, 2004 Jul 15, 2004 Jul 18, 2004 Aug 08, 2004 Aug 18, 2004 Aug 18, 2004 Aug 18, 2004	Jan 04, 2005 Feb 04, 2005 Feb 10, 2005 Feb 12, 2005 Mar 04, 2005 Mar 11, 2005 Mar 18, 2005 Mar 31, 2005 Apr 02, 2005 Apr 17, 2005 May 08, 2005 May 12, 2005 May 13, 2005 May 19, 2005 May 24, 2005 May 26, 2005 May 27, 2005 May 29, 2005 May 30, 2005 May 31, 2005 Jun 01, 2005 Jun 01, 2005 Jun 01, 2005 Jun 01, 2005	Jan 01, 2006 Jan 01, 2006 Jan 01, 2006 Jan 01, 2006 Jan 02, 2006 Jan 02, 2006 Jan 02, 2006 Jan 02, 2006 Jan 02, 2006 Jan 06, 2006 Jan 06, 2006 Jan 07, 2006 Jan 07, 2006 Jan 07, 2006 Jan 07, 2006 Jan 07, 2006 Jan 07, 2006 Jan 07, 2006 Jan 08, 2006 Jan 08, 2006 Jan 08, 2006 Jan 12, 2006 Jan 27, 2006	Jan 02, 2007 Jan 07, 2007 Jan 12, 2007 Jan 17, 2007 Jan 28, 2007 Feb 02, 2007 Feb 05, 2007 Feb 10, 2007 Feb 17, 2007 Feb 25, 2007 Mar 05, 2007 Mar 14, 2007 Mar 23, 2007 May 06, 2007 May 09, 2007 Jun 01, 2007 Jun 03, 2007 Jun 04, 2007

Melalui situs *www.archive.org*, hacker bisa mendapatkan dan melihat halaman website sebuah domain semenjak pertama kali diaktifkan serta mendapatkan informasi-informasi yang mungkin telah dihilangkan.

Situs ini mencatat dan menyimpan perubahan-perubahan yang terjadi pada sebuah domain/situs. Pada contoh diatas, saya memasukkan nama domain *www.jasakom.com* dan hasilnya sangat mengagetkan. Saya tidak percaya bagaimana jeleknya situs *jasakom* waktu pertama kali online dan berapa banyak perubahan yang telah terjadi.

1.5. Mencari Sub Domain, Email dan informasi lainnya

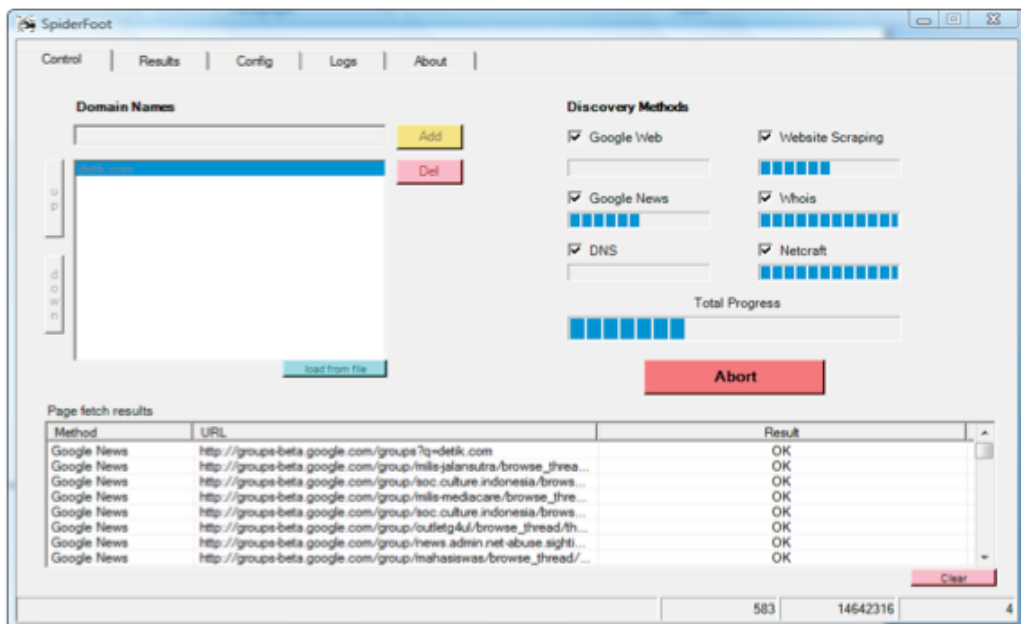
Mendapatkan informasi detail dari seseorang bisa dilakukan dengan melihat blog yang saat ini sedang trend atau melalui situs seperti friendster, facebook, dan situs-situs lainnya. Tentu, hacker juga bisa mencarinya dengan bantuan search engine seperti google.

Web site *people.yahoo.com* bahkan menawarkan fasilitas khusus dalam melakukan pencarian informasi mengenai seseorang seperti alamat tinggal dan lain sebagainya. Dengan informasi semacam ini, hacker bisa lebih mengenal korbannya dan bisa meluncurkan serangan *social engineering* (penipuan) dengan lebih meyakinkan.

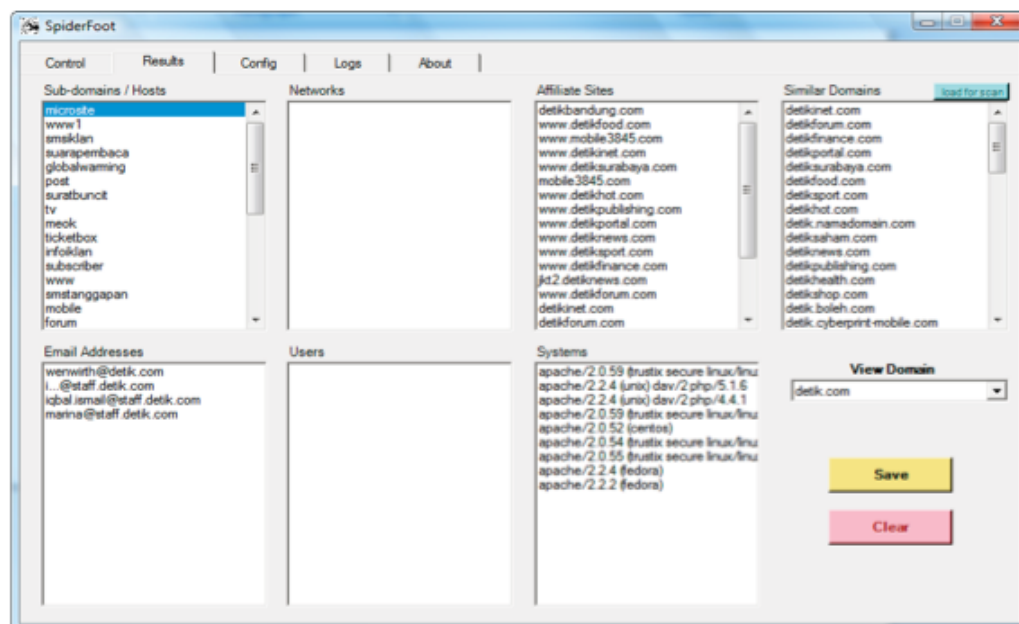
SpyderFoot

Tools yang dibuat oleh *Steve Micallef* ini merupakan sebuah tools untuk melakukan footprinting yang bisa Anda dapatkan pada situs *www.binarypool.com/spiderfoot*. Tools ini akan mencari berbagai informasi termasuk juga informasi yang berhubungan mengenai sebuah domain. *SpyderFoot* menggunakan beberapa teknik untuk melakukan pencarian ini seperti memanfaatkan search engine google, memanfaatkan Netcraft, memanfaatkan database *www.whois.net*, website spidering dll.

Informasi yang mampu diberikan oleh *SpyderFoot* inipun sangat beragam, seperti alamat email, subdomain, domain yang berhubungan, system yang digunakan, dll. Berikut adalah hasil percobaan *SpyderFoot* yang dilakukan terhadap domain *detik.com* :



Anda bisa melihat hasil yang didapatkan oleh *SpyderFoot* pada tabulasi *Result*:



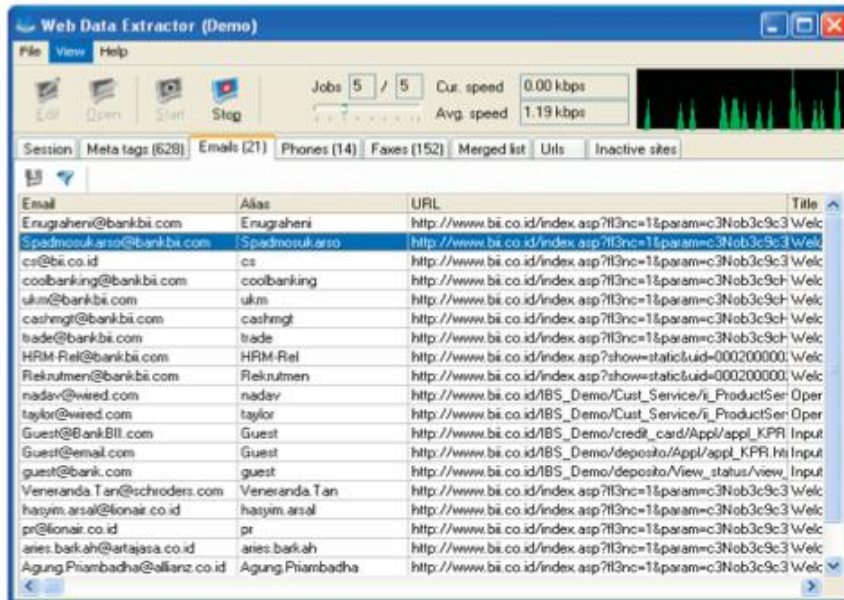
Dari hasil yang didapatkan ini, saya baru mengetahui bahwa ternyata banyak sekali sub domain dari situs detik.com seperti microsite.detik.com, globalwarming.detik.com, smsiklan.detik.com, dst. Anda juga bisa meng-klik dua kali pada item hasil pencarian ini untuk melihat darimana SpyderFoot mendapatkan informasi ini.

Sebagai contoh, dengan mengklik dua kali pada alamat email marina@staff.detik.com, saya dibawa ke beberapa halaman situs suara pembaca. Jadi bisa diperkirakan bahwa marina adalah salah satu staff detik yang mengurus bagian suara pembaca.

Web Data Extractor

Tools lainnya yang sangat membantu dalam mencari informasi mengenai alamat email, nomor telepon dan fax serta informasi lainnya pada sebuah domain adalah Web Data Extractor (www.webextractor.com).

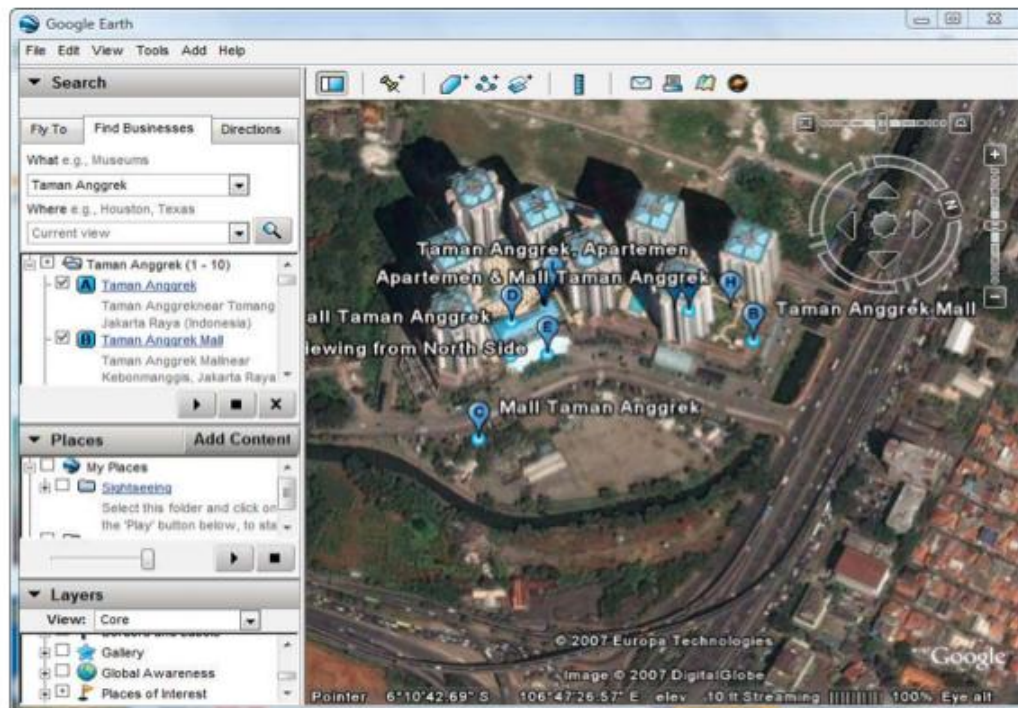
Saya memasukkan alamat domain bii.co.id ke dalam tools ini dan lihatlah, saya berhasil mengumpulkan 21 alamat email, 14 nomor telp dan 152 nomor fax dalam waktu 1 menit !



1.6. Survei Lokasi

Dunia memang sudah gila, dengan kemajuan teknologi yang tidak pernah terpikirkan bahkan tidak pernah pula diimpikan. Dengan Google Earth (<http://earth.google.com/>), kini Anda bisa melihat sebuah lokasi melalui satelit. Anda bisa melihat sebuah lokasi secara jelas tanpa perlu menginjakkan kaki ataupun membeli tiket pesawat. Pada contoh, saya menggunakan Google Earth untuk melihat Mall dan Apartemen Taman Angrek.

Fasilitas yang dimiliki oleh Google Earth ini bahkan menjadi kekhawatiran negara adikuasa seperti Amerika karena di takutkan teknologi ini digunakan oleh para teroris dalam merencanakan tindakan terror.



1.7. Mengetahui Rute Perjalanan

Mengetahui rute yang dilalui sebuah paket sampai di tempat komputer korban memberikan suatu kelebihan tersendiri. Terkadang Anda bisa mengetahui alamat IP penjaga (firewall) yang digunakan dengan melihat komputer terakhir yang dilalui sebelum sampai ditujuan. Lalu bagaimana melakukan hal ini semua tanpa perlu menelusuri satu persatu komputer yang ada? *Traceroute* adalah jawabannya!

Traceroute memanfaatkan flag TTL di dalam paket TCP. Saya akan menjelaskan cara kerja dari protokol TCP yang digunakan dalam jaringan internet agar Anda bisa memahami fungsi dari flag TTL didalam paket TCP ini.

Anda tentu sudah mengetahui bahwa komputer yang terhubung di dalam jaringan internet ini berjumlah sangat-sangat banyak. Komputer yang hendak mengirimkan data ke tujuan, biasanya tidak bisa melakukannya secara langsung namun paket tersebut akan melalui beberapa komputer dan router perantara (peralatan

yang melakukan proses routing agar paket bisa berpindah dari satu network ke network yang lain).

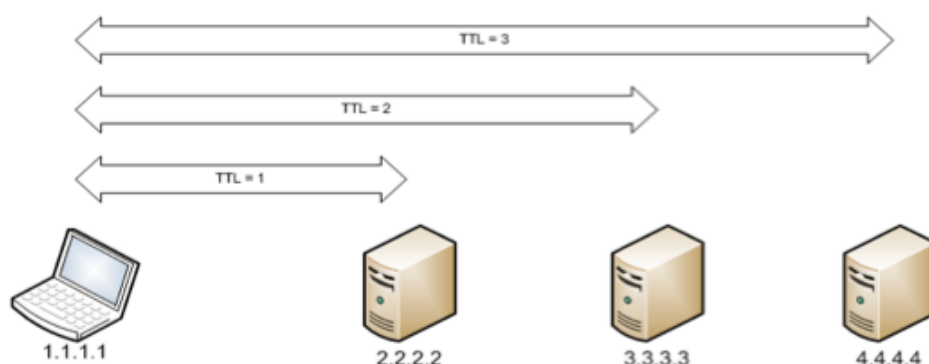
Misalnya, Anda mengirimkan email ke teman Anda yang berada di makassar. Email Anda akan mengalir dari komputer Anda, berpindah ke komputer/router ISP Anda, kemudian berpindah lagi ke komputer ISP yang digunakan oleh teman Anda dan akhirnya diambil oleh komputer teman Anda. Kenyataannya, komputer dan peralatan yang terlibat bahkan selalu lebih banyak daripada ini karena sebelum email Anda sampai ke mail server ISP, masih ada komputer atau peralatan lain di tempat ISP yang harus dilalui seperti firewall, router, dll.

Nah, karena internet adalah jaringan yang sangat kompleks dan ada banyak jalan menuju roma, ada kemungkinan paket yang tidak terkirim dengan satu jalan akan mencari jalan yang lain. Akibatnya adalah mungkin saja paket tersebut akan terus mencari dan mencari jalan walaupun sebenarnya sudah tidak ada jalan lagi sehingga paket tersebut menjadi paket abadi (*immortal*) yang menghabiskan bandwidth semua orang karena terus bergerak.

Untuk itulah, diciptakan sebuah flag TTL yang membatasi jarak yang bisa ditempuh oleh sebuah paket. Dengan nilai TTL sebesar 30, artinya kita mengatakan kepada komputer "Apabila setelah melalui 30 komputer, paket masih belum sampai ketempat tujuan, musnahkan saja paket data ini".

Bagaimana cara kerjanya? Nilai TTL ini akan dikurangi dengan 1 oleh setiap router atau komputer yang dilalui oleh setiap paket dan apabila nilai pengurangan ini hasilnya sama dengan nol, router atau komputer akan mengabaikan paket ini dan mengembalikan nilai error "*TTL Exceeded*".

Van Jacobson kemudian membuat program yang dinamakan sebagai *traceroute* untuk mengetahui jalannya sebuah paket dari sumber menuju tujuan. Bagaimana cara kerjanya? Dengan sangat licik, *Van Jacobson* memanfaatkan flag TTL untuk mengetahuinya. Misalkan Anda ingin mengirimkan paket ke komputer dengan alamat IP 4.4.4.4. Anda ingin mengetahui komputer mana saja yang dilalui oleh paket data ini agar bisa sampai ke tujuannya.



Untuk itu, *traceroute* akan mengirimkan paket dengan nilai TTL 1. Paket data kemudian mengalir dari komputer 1.1.1.1 ke 2.2.2.2. Komputer 2.2.2.2 akan mengurangi nilai TTL dengan 1, akibatnya adalah nilai TTL menjadi 0! Komputer 2.2.2.2 kemudian akan mengirimkan error kepada komputer 1.1.1.1. Ok! sekarang komputer 1.1.1.1 sudah mengetahui bahwa komputer pertama yang dilalui adalah 2.2.2.2.

Kini komputer 1.1.1.1 mengirimkan paket yang sama lagi namun sekarang dengan nilai TTL 2. Proses ini berlangsung terus sampai paket tersebut sampai ke tujuan sehingga *traceroute* bisa mengetahui komputer atau router mana saja yang dilalui oleh sebuah paket.

Sebagai contoh, saya menjalankan perintah *traceroute* ke alamat *www.jasakom.com* (Karena kata *traceroute* melebihi 8 karakter dan pada awalnya sistem operasi windows hanya mengenali nama file dengan maksimum 8 karakter, maka program *traceroute* di windows diberi nama *tracert*. Pada contoh ini saya menggunakan Windows Vista):

```
C:\> tracert www.jasakom.com
Tracing route to www.jasakom.com [202.67.9.82]
over a maximum of 30 hops:
```

```
 1  3 ms    1 ms    2 ms    192.168.1.1
 2 39 ms   44 ms   21 ms   10.16.40.1
 3 28 ms   53 ms   23 ms   6.96.73.202.fast.net.id [202.73.96.6]
 4 38 ms   38 ms   22 ms   5.96.73.202.fast.net.id [202.73.96.5]
 5 63 ms   96 ms   13 ms   dhecyber.openixp.net [218.100.27.155]
 6 61 ms   74 ms   35 ms   dhe.dhecyber.net.id [202.67.8.18]
 7 64 ms   62 ms   55 ms   iix2.rumahweb.com [202.67.9.82]
```


Dengan memahami komputer atau alamat IP mana saja yang dilalui oleh sebuah paket sebelum sampai ke tujuannya, hacker bisa menggambarkan perkiraan infrastructure yang digunakan termasuk alamat IP dari firewall yang digunakan.

Visual Route

Tidak hanya menampilkan alamat IP yang dilalui oleh sebuah paket dalam bentuk text, *Visual Route* (www.visualroute.com) juga menampilkan lokasi dari alamat IP secara visual dalam bentuk peta yang sangat menarik. Pada contoh, saya menjalankan *Visual Route* dari komputer dirumah saya ke situs www.jasakom.com. Terlihat perjalanan paket semenjak meninggalkan komputer rumah dengan alamat IP lokal, menuju alamat IP dari ISP yang saya gunakan, sampai akhirnya tiba ditujuan :

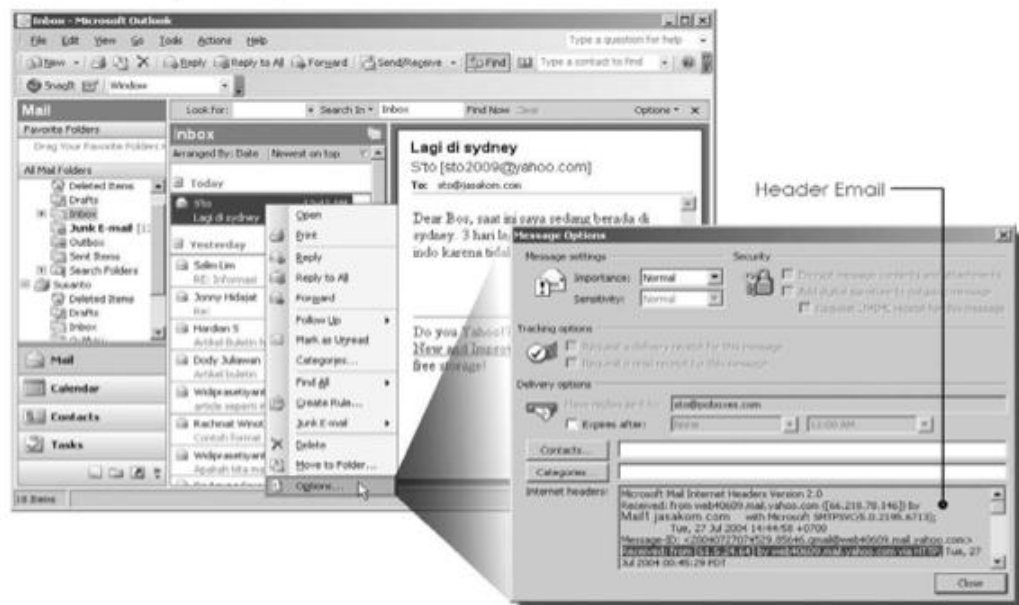


1.8. Melacak email

Pada saat Anda mengirim email, mail server akan memasukkan informasi tambahan ke dalam email yang Anda kirim tersebut. Dan salah satu informasi tersebut adalah alamat Anda! Bila Anda berfikir bahwa mengirim email dengan alamat palsu adalah aman, itu adalah suatu kesalahan besar yang banyak dilakukan oleh orang-

orang. Pada saat Anda mengirim email, server email Anda termasuk situs seperti yahoo juga akan menambahkan alamat IP Anda di header email. Benar, alamat IP Anda akan tercatat walaupun Anda mengirimnya melalui web.

Bagaimana melihat header sebuah email? Program seperti outlook, web mail yahoo, google, dlsb biasanya menyembunyikan header sebuah email karena takut membingungkan pengguna awan namun sebenarnya Anda tetap bisa melihatnya. Untuk Anda yang menggunakan Outlook, klik kanan pada email yang hendak dilihat kemudian pilih *Options*.



Berikut adalah contoh header email yang saya dapatkan :

```
Microsoft Mail Internet Headers Version 2.0
Received: from web40609.mail.yahoo.com ([66.218.78.146]) by
mail.Jasakom.com SMTPSVC(5.0.2195.6713) ;
Tue, 27 Jul 2004 14:44:58 +0700
Message-ID: <20040727074529.85646.qmail@web40609.mail.yahoo.com>
Received : from [61.5.24.64] by web40609.mail.yahoo.com via
HTTP; Tue, 27 Jul 2004 00:45:29 PDT
Date: Tue, 27 Jul 2004 00:45:29 -0700 (PDT)
```

```
From: S'to <sto2009@yahoo.com>
Reply-To: sto@poboxes.com
Subject: Lagi di sydney
To: bos@Jasakom.com
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="0-838722002-1090914329=:85546"
Return-Path: sto2009@yahoo.com
X-OriginalArrivalTime: 27 Jul 2004 07:44:58.0796 (UTC)
FILETIME=[9DD86EC0:01C473AD]
```

Berdasarkan informasi yang didapatkan dari header email, terlihat bahwa email ini berasal dari server mail lokal, *mail1.Jasakom.com*. Email server ini menginformasikan bahwa email tersebut diterima dari email server yahoo, *web40609.mail.yahoo.com* yang menggunakan alamat IP 66.218.78.146 (*Received: from web40609.mail.yahoo.com ([66.218.78.146]) by mail1.Jasakom.com*). Message ID merupakan sebuah nomor unik yang mengidentifikasikan sebuah email dan seringkali digunakan untuk troubleshooting perjalanan sebuah email.

Kini, bagian yang paling penting, "*Received: from [61.5.24.64] by web40609.mail.yahoo.com via HTTP*" memberikan informasi bahwa mail server yahoo, *web40609.mail.yahoo.com* menerima pengiriman email dari seseorang yang mempunyai alamat IP 61.5.24.64 melalui HTTP (web).

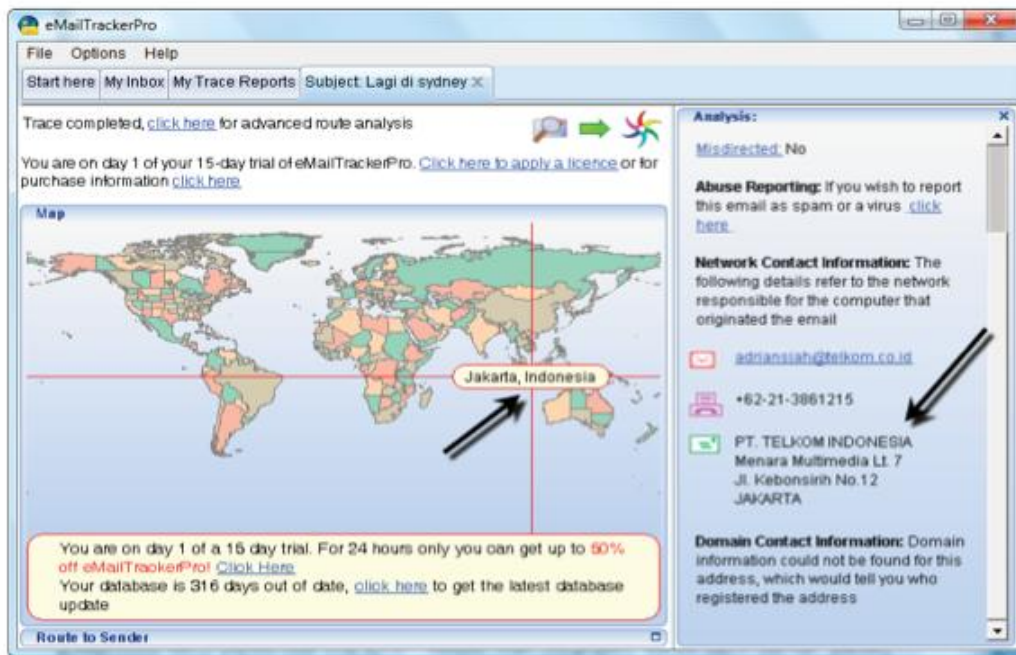
Lalu siapakah 61.5.24.64? Berdasarkan penelusuran melalui situs whois untuk melihat siapakah pemilik alamat IP ini, ternyata pemiliknya adalah Telkom. Dengan kata lain ternyata email yang katanya dikirim dari Sydney sebenarnya berasal dari Indonesia dengan Telkomnet Instan.

Email Tracker Pro

Membaca header email terkadang menjadi sulit karena tidak ada standarisasi baku tentang bagaimana email server harus menambahkan header ini. Bila Anda menginginkan kemudahan, Anda bisa menggunakan tools *Email Tracker Pro* yang bisa didownload dari situs *www.visualware.com*.

Email tracker Pro akan menunjukkan lokasi asal suatu email secara visual beserta dengan informasi pemilik IP. Anda tinggal mengklik menu *File* → *Trace an Email* → kemudian meng-copy dan paste header

email diatas ke dalam program *Email Tracker Pro* untuk melihat hasilnya :



Selain menyediakan tools yang bisa diinstall, situs *Email Tracker Pro* juga menyediakan fasilitas pelacakan email ini secara online. Anda bisa mengunjungi situs <http://emailtrackerpro.visualware.com/> untuk menggunakan fasilitas ini secara online. Selain *Email Tracker Pro*, masih banyak tersedia program lainnya untuk kebutuhan yang sama seperti *McAfee Neotrace Profesional*, dll.

1.9. Melacak Aktivitas Penerima Email

Email yang telah terkirim, ibarat surat yang sudah dikirimkan oleh burung merpati. Anda tidak akan mengetahui apakah surat tersebut telah sampai ditujuan, sudah dibaca atau bahkan hilang dijalan. Merpati tidak bisa diajak diskusi, demikian juga halnya dengan server email yang Anda gunakan.

Read Notify

www.readnotify.com, menyediakan layanan yang bisa digunakan

untuk melacak status dari sebuah email. Situs ini bisa melacak status sebuah email dan mengetahui banyak hal seperti jam dan tanggal email tersebut dibaca, lokasi korban saat membaca email, alamat IP waktu membaca email, berapa kali email tersebut dibuka, dan apakah email Anda diforward ke orang lain. Untuk menggunakan fungsi dari *ReadNotify* ini, Anda tidak perlu mengganti alamat email yang saat ini sedang digunakan.



Bagaimana *ReadNotify* bekerja? sangat menarik untuk mengetahui bagaimana layanan ini bisa bekerja karena pada situsnya, cara kerja dari *ReadNotify* ini dirahasiakan alias tidak ada informasinya.

ReadNotify menggunakan teknik yang dikenal dengan *webbug*, yaitu dengan menyisipkan sebuah link gambar yang sangat kecil di dalam email yang dikirimkan. Berikut adalah contoh script yang disisipkan oleh *ReadNotify* :

```
<Img moz-do-not-send="true" border=0 height=1 width=3 alt="" lowsrc=""
Src=http://www.rlbj5e0krvy8.ReadNotify.com/nocache/rlbj5e0krvy9/
footer0.gif><Img moz-do-not-send="true" Border=0 Height=1 Width=2 Alt=""
Lowsrc=http://www.readnotify.com/ca/rspr47.gif >
```

Ketika korban membaca email, secara otomatis email client biasanya akan membuka link yang telah disediakan oleh *ReadNotify*. *ReadNotify* kemudian akan mencatat alamat IP, mencatat waktu, dan informasi lainnya yang menandakan bahwa email tersebut telah dibaca.

Masalahnya adalah email client sekarang seperti outlook 2007, sudah mulai memblokir otomatisasi pembukaan link gambar. Akibat dari kebiasaan baru dari email client ini, *ReadNotify* tidak akan mampu melacak status sebuah email apakah sudah dibuka atau belum dan informasi lainnya. Tentu ini menjadi tantangan bagi *ReadNotify* apakah masih terus bertahan atau sudah waktunya untuk tutup toko.

1.10. Lebih Mengetahui Korban

Semakin Anda mengetahui korban atau musuh, semakin dekat pula kemenangan yang bisa Anda dapatkan. Mengetahui yang saya maksudkan disini, bukanlah dalam artian kuno yang artinya Anda mengetahui orang tersebut dan berteman dengannya.

Sebagai contoh, Anda mungkin mengetahui idola Anda melebihi siapapun didunia ini dan apakah idola Anda mengetahui Anda?

Biasanya tidak, karena Anda bisa mencari informasi mengenai idola Anda dari banyak sumber seperti berita gosip, televisi, radio, konser dan lain sebagainya. Target Anda mungkin bukanlah seorang artis yang selalu masuk berita namun pada jaman sekarang ini, masyarakat biasa-pun bisa ditelusuri dengan berbagai cara.

© Yahoo! People Search

YAHOO! PEOPLE SEARCH

U.S. Phone & Address

First Name/Initial: Last Name: (required)

City/Town: State:

Reverse Phone #

Phone Number:

Ex: 408-555-1212

Email Search

First Name/Initial:

Last Name: (required)

© 2008 Yahoo! [Privacy](#) / [Legal](#) - [Submit Your Site](#)

Situs *Yahoo! People Search* (people.yahoo.com) memungkinkan Anda melakukan berbagai pencarian seperti pencarian alamat, pencarian pemilik telepon dan pencarian alamat email seseorang.

BestPeopleSearch.com
Our Name says it all!

Home | Articles | Help | Login | Checkout

Quick Search

Home
All Searches
Our Guarantee
FAQs
About Us
Contact Us
Link Exchange

Search Categories

- Search by Name
- Search by Address
- Search by Phone
- Search by Cell
- Search by SSN
- Criminal check
- Background check
- DMV

Have a Phone Number?
Need a Name and Address?
[Click Here!](#)

Need Assistance?
[View Cart](#)

People Search by Name

- People Search by Name
- Comprehensive People Search
- Guaranteed Current Address Search
- Find Address and Phone number (w/SSN)
- Find Address and Phone numbers (w/out SSN)
- How can I find cell phone numbers
- Locate Cell Phone Number (exclude known numbers)
- Search for cell phone numbers
- Locate Mobile Number (exclude known numbers) no SSN
- Verified Current Employer Search w/SSN (POE)
- Verified Current Employer Search w/o SSN (POE)
- Financial Due Diligence Report (w/out SSN)

Bank Account & Assets Searches

- Bank Account Search
- Bank Account Search without SSN
- Deluxe Bank Account Search
- Brokerage Bank - Investment Account Search
- Real Estate Property Search

Credit Reports

- Credit Report for Judgment
- Credit Report for Judgment without SSN
- Credit Checks for Tenant Screening

Search for Wages or Employer

- Verified Current Employer Search w/SSN (POE)
- Verified Current Employer Search w/o SSN (POE)
- Employment Wages Search w/SSN
- Employment Wages Search w/o SSN

Background Checks

- Preemployment Screening (Standard)
- Pre-Employment Screening (Deluxe)
- Skip Trace (Exhaustive People Search Report)
- Subveter Background Check - Nanny Background Screening
- Professional License Verification
- Comprehensive Background Check

Most Popular Searches

- FREE Social Security Number Verification
- Find Someone's Cell phone number (Cell phone lookup)
- Bank Account Search
- Basic People Search
- Nationwide Criminal Records Search
- Comprehensive Background Check
- Reverse Address Lookup (phone, P.O. address)
- Phone of Employment Search
- Find someone from License, Photo, Records
- Verified Current Address Search

Live Private Investigators
Search for Current and Accurate Information

Point to Verify

Berbeda dengan Yahoo yang memberikan layanannya secara gratis, situs *BestPeopleSearch* melakukan pencarian informasi seseorang secara komersial. Situs ini menawarkan layanan pencarian informasi yang sangat lengkap seperti informasi mengenai catatan kriminal, alamat, finansial/keuangan, dan lain sebagainya.

People-Search-America

Seperti halnya dengan *BestPeopleSearch*, situs *People-Search-America* juga menawarkan layanan komersial yang hampir sama namun jauh lebih sederhana. Saking sederhananya, beberapa bagian dari situs ini terkesan kurang diperhatikan seperti munculnya error ketika mengklik link yang disediakan.

People-Search-America menawarkan pencarian informasi dan latar belakang seseorang termasuk latar belakang kriminal. Anda juga bisa mencari pemilik dari sebuah nomor telepon dan pencarian informasi berdasarkan nomor 'social security' (nomor jaminan sosial di Amerika Serikat)

People-Search-America.com

HOME
SUPPORT
FAQS
MEMBER LOGIN
REGISTER
PRIVACY
TERMS AND CONDITIONS

PEOPLE SEARCH

Find information on any phone, mobile cell phone, business, pager, pay phone and even unlisted numbers. Reverse phone number search includes name, address service provider and other details.

* Name :

* City :

* State : All States Search

BACKGROUND CHECK

Investigate your boyfriend. View criminal, finance, court and other records. Get the scoop on your daughter's coach or new acquaintance.

* Name :

* City :

* State : Select State Search

REVERSE PHONE LOOKUP

Find information on any phone, mobile cell phone, business, pager, pay phone and even unlisted numbers. Reverse phone number search includes name, address service provider and other details.

Search

SOCIAL SECURITY

Investigate your boyfriend. View criminal, finance, court and other records. Get the scoop on your daughter's coach or new acquaintance.

Search

Switchboard

Your Digital Directory

Find a Business
Find a Person
Maps & Directions
Search by Phone
Area & Zip Codes
Web Search

White Pages

First Name: Last Name:

City or Zip/Area Code:

State: Select a State Search

Public Records Search

First Name:

Last Name:

State: Select a State Search

Reverse Phone Lookup

Phone Number:

(e.g. "206-555-1212")

Search

Additional Resources

- [People Search - Find Anyone](#)
Current & Verified Phone Number, Address, Age & Relatives.
- [Comprehensive Background Check](#)
Criminal Check, Address History, Assets, Lawsuits & more.
- [Email and Unlisted Phone Lookup](#)
Current Name, Address and Phone for any Email address.

Bila Anda pernah mencari informasi seseorang melalui buku *yellow pages*, maka situs *switchboard* adalah solusi pengganti dalam bentuk online. Situs ini ditujukan untuk memudahkan konsumen dan pedagang saling berhubungan. Tentu saja, Anda juga bisa memanfaatkan situs ini untuk menemukan informasi mengenai seseorang.

 Yellow Pages

merry christmas
selamat hari natal



Sun, 28 Dec 2008

City Guide Career Business Yellow Map
Search Advanced Search Web Search Category

Keyword Category City
Phone Address Brand/Product

Tips Pencarian

At least one of keyword or category must be specified!
Search example:

- Keyword = Infomedia, Category = Directory, City = Jakarta
- Keyword = Infomedia, City = Jakarta
- Category = Directory, City = Jakarta

LIVE CHAT
CUSTOMER CARE
Not online

Situs yellowpages di Indonesia sendiri bisa dilihat melalui alamat www.yellowpages.co.id yang juga memberikan layanan pencarian walaupun pencarian yang dilakukan masih sangat terbatas karena situs ini hanya ditujukan bagi masyarakat yang ingin mencari tempat bisnis atau tempat belanja, bukan melakukan pencarian orang.

 Skippease & 411x411

WhitePages.com™
search. find. connect.

 **STAY** close to family and friends in Mexico & Latin America for \$15 more a month!

 **CLICK HERE!**

Home People Search Business Search Reverse Lookup Area & ZIP Codes Add Your Listing

Quick Search | WhitePages Anywhere | International Resources

People Search **Business Search** **Quick Links**

Basic Search Advanced Search
First Name
Last Name
City or ZIP/Postal State/Prov
*required Search

Business Ad Categories
*Name or Category
City or ZIP/Postal State/Prov
Save as default location
*required Search

- Add Your Work Listing
- Join WhitePages today!
- Mobile Carrier Lookup
- WhitePages for iPhone

the Spotlight
Add WhitePages to your favorites. Find out how


HOW DO THEY GET THEIR ATTRACTIVE STOMACHS?
THEY USE THE FDA APPROVED FLEX BELT®
WHICH TONES THEIR ABS
WITHOUT NEEDING TO EXERCISE!
Advertise with Us

Selain situs yang direkomendasikan oleh CEH ini, ada lagi beberapa situs yang memberikan layanan pencarian orang secara gratis seperti <http://skipease.whitepages.com> dan <http://www.411x411.com>.

411 x 411.com

411 x 411.com Free People Finder & Person Search

>> [411 & People Searches](#) << [Reverse Lookups](#) • [Yellow Pages](#) • [SSN Search](#) • [Public Records](#) • [Maps](#) •
• [Auction Searches](#) • [Job Searches](#) • [Specialty Search Engines](#) • [News Feeds, Blogs & Message Boards](#) •

[about us](#) | [bookmark us !](#) | [disclaimer](#) | [link to us](#) | [submit links](#)

411 x 411.com Person Locator & People Search Engine

411 People Finder, People Search

First Name ☒ Begins with

Last Name* ☐ Begins with

City, ZIP or Postal Code

State or Province

Select a State

Search

🕒 Situs Pertemanan

Situs pertemanan atau social networking juga bisa menjadi tempat yang sangat empuk untuk mendapatkan informasi detail mengenai seseorang, bahkan termasuk hobi, teman-temannya, tanggal lahir dan informasi lainnya yang seharusnya rahasia. Situs pertemanan yang terkenal dan bisa dimanfaatkan contohnya adalah www.myspace.com, www.friendster.com, www.facebook.com dan www.linkedin.com.

[myspace invite](#)
[Click here!](#)

invite your friends to MySpace!
Watch your network grow as your friends add friends!

[Home](#)
[Browse People](#)
[Find People](#)
[Forums](#)
[Music](#)
[Video](#)
[More ▾](#)
[MaRiA ▾](#)
[Log In](#)
[Sign Up](#)

MaRiA

"@->-HaPpInEs
LiEs In YoU-<-@"

Female
23 years old
SiNgApOrE, NoNe
Singapore

Last Login:
11/10/2004

MaRiA is in your extended network

MaRiA's Latest Blog Entry [\[Subscribe to this Blog\]](#)

My Valentine - Martina McBride (feat. Jim Brickman) [\(view more\)](#)

Sweden iD [\(view more\)](#)

DREAMING OF YOU - Selena [\(view more\)](#)

Chalet @ Sentosa... [\(view more\)](#)

SAF Commander's Camp Site [\(view more\)](#)

[\[View All Blog Entries\]](#)

View My: [Pics](#) | [Videos](#)

Contacting MaRiA

Send Message	Forward to Friend
Add to Friends	Add to Favorites
IM / call	Block User
Add to Group	Rank User

MaRiA's Blurbs

About me:
ORdiNaRy, SiMple, QuiET, LaZy, InNoCeNt, SiLLy, BlUrRr, CrAZY & MaD
OcCaSiOnAlLy...LeVe SpOrTs BuT NoT GoOd At SpOrTs...

friendster. powered by Google

Home Profile Apps Connections Explore Search Messages Settings Help Log In

Classifieds Find Friends

I'm dona




"bingongg ah... mo mong apeh..."

female, 14, single
interested in: dating men and women, relationship men and women, friends, activity partners
member since: jan 2009
location: jakarta, id
hometown: jkt...
last login: 2 weeks
i'm's url:
<http://profiles.friendster.com/95793617>
"mdu tau koda gmn jdang shayv... it lat jd primarycity... tau lu trawong aj andi koda gmn idag daku... tam jnat shayv..."

how you're connected: view all
you → i'm is in your extended network → i'm

i'm's friends



view all (2)

more about i'm

facebook

Remember Me Forgot your password?

Email Password Login

Facebook helps you connect and share with the people in your life.



Sign Up
It's free and anyone can join

Full Name:
Your Email:
New Password:
I am: Select Sex:
Birthday: Month: Day: Year:
Why do I need to provide this?
Sign Up

By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.

LinkedIn

Home | What is LinkedIn? | Join Today | Sign In | Language

Over 30 million professionals use LinkedIn to exchange information, ideas and opportunities

- Stay informed about your contacts and industry
- Find the people & knowledge you need to achieve your goals
- Control your professional identity online

Join LinkedIn Today

First Name:
Last Name:
Email:
Continue
Already on LinkedIn? Sign in.

Please enter a last name.

Search for someone by name: First Name Last Name Go

People directory: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z more

Hanya bermodalkan informasi dari situs pertemanan (*social networking*) yang sedang populer saat ini, hacker mampu membajak account seseorang dan hal ini sudah sering terjadi karena itu.

Sebagai contoh, beberapa webmail atau account lainnya memberikan fasilitas recovery password dengan memasukkan informasi tempat dan tanggal lahir, nama sekolah atau informasi lainnya yang bisa didapatkan dengan mudah melalui profil yang tersedia secara bebas di situs pertemanan ini.

Penyerangan yang lebih berbahaya bisa terjadi seperti melakukan transaksi melalui phone banking karena transaksi ini biasanya hanya melakukan verifikasi dengan menanyakan nama orang tua, tempat dan tanggal lahir, dan informasi lainnya juga juga sering tersedia di situs pertemanan.

2. Mencari Informasi Range Alamat IP

Sebuah perusahaan besar, biasanya mendapatkan alokasi alamat IP oleh ISP. Alamat-alamat IP ini kemudian bisa digunakan oleh beberapa server seperti web server, mail server, remote access server dan server-server lainnya. Seorang hacker, akan mencoba mencari informasi alamat-alamat IP yang dimiliki oleh sebuah perusahaan atau range alamat IP yang digunakan oleh perusahaan. Cara mencarinya sebenarnya sudah saya tunjukkan sebelumnya, yaitu pada penjelasan mengenai *whois* dan *RIR* (*Regional Internet Registries*).

Pada hasil pencarian *whois*, Anda akan mendapatkan sebuah record yang biasanya dinamakan dengan **NetRange**. Dari sini, hacker bisa melihat alamat-alamat IP yang digunakan perusahaan target.



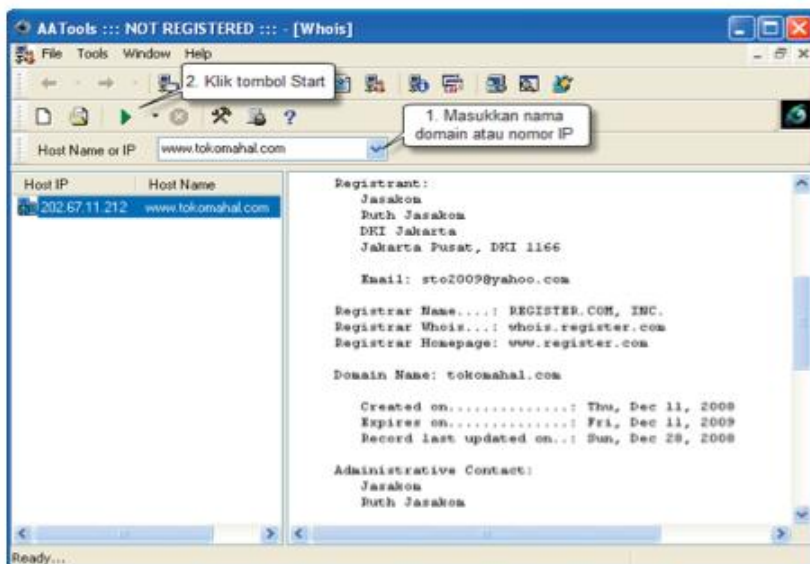
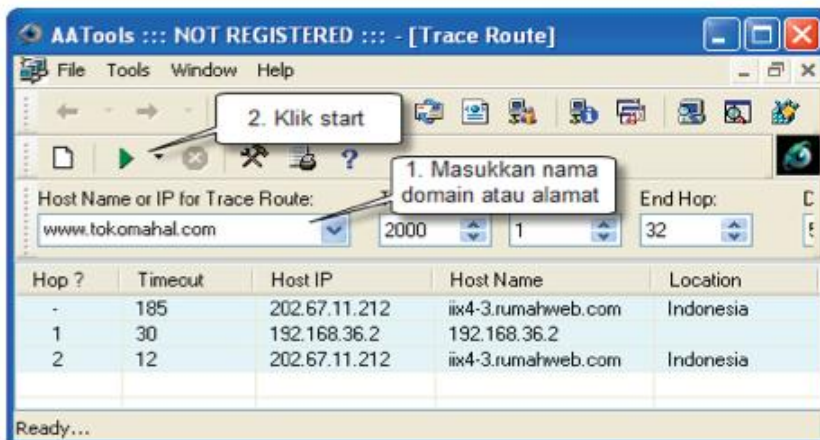
Informasi yang diberikan oleh NetRange, tidak sepenuhnya bisa dijadikan patokan karena mungkin saja provider atau ISP tidak mendaftarkan pemilik range IP sehingga hacker masih akan mendapatkan range alamat IP yang dimiliki oleh ISP. Tentu saja, walaupun tidak 100% benar, informasi ini tetap merupakan informasi yang berharga untuk dicoba.

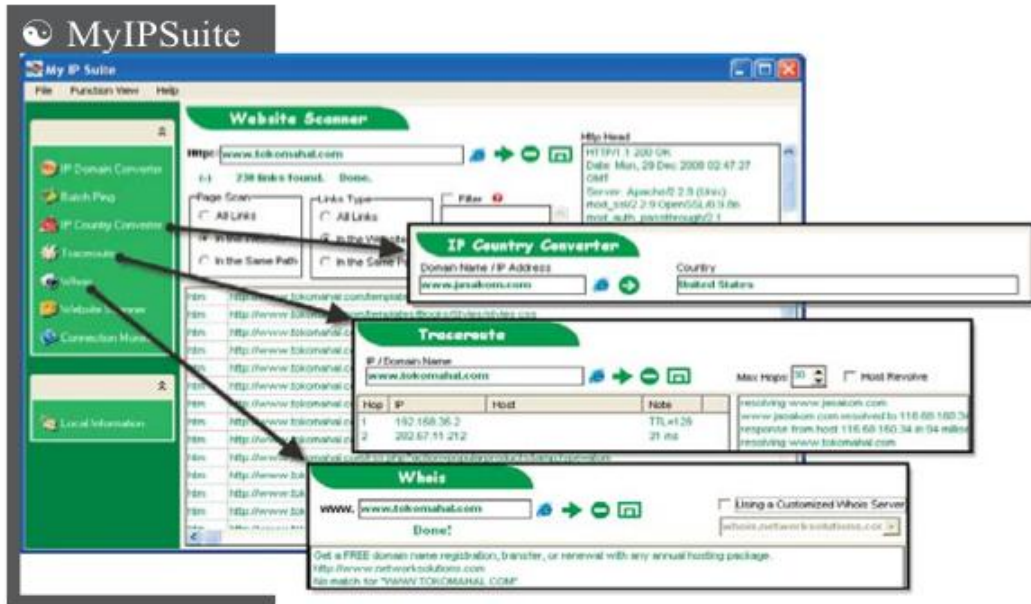
Hacker juga bisa memanfaatkan tool seperti traceroute untuk mendapatkan alamat-alamat IP yang dimiliki oleh sebuah perusahaan. Hacker juga bisa melakukan percobaan-percobaan terhadap alamat IP yang berurutan. Misalnya alamat website target menggunakan alamat IP 1.1.1.1, maka hacker bisa mencoba melihat alamat IP 1.1.1.2, 1.1.1.3, dst. Ini adalah cara yang tidak 'high tech' namun terkadang sangat efektif.



Untuk menggali informasi awal, banyak tools yang bisa digunakan untuk memudahkan pekerjaan ini. Salah satunya adalah, *Advanced Administrative Tools (AA Tools)*, yang merupakan kumpulan berbagai tools seperti port scanner, proxy analyzer, Trace Route, Whois, Network Monitor dan lain sebagainya.

Tools yang berguna untuk kebutuhan kita untuk menggali informasi awal adalah *Trace Route* yang bisa digunakan untuk mengetahui perjalanan paket dari komputer kita menuju komputer target. *Trace Route* secara otomatis juga akan menampilkan informasi negara pemilik alamat IP yang dilewati. Tools lainnya adalah *whois* yang bisa digunakan untuk menampilkan informasi mengenai sebuah domain seperti informasi pemilik domain, informasi DNS dan informasi lainnya.





MyIPSuite (www.sabsoft.com) merupakan program komersial yang cukup sederhana dengan harga yang cukup murah (sekitar 400 ribuan). Tools ini menyediakan fasilitas mencari alamat IP, informasi negara asal sebuah IP, pelacakan paket (trace route), whois, website scanner dll. Saya tidak merekomendasikan software ini kecuali ada perbaikan yang signifikan dari pembuatnya apalagi untuk sebuah program komersial.

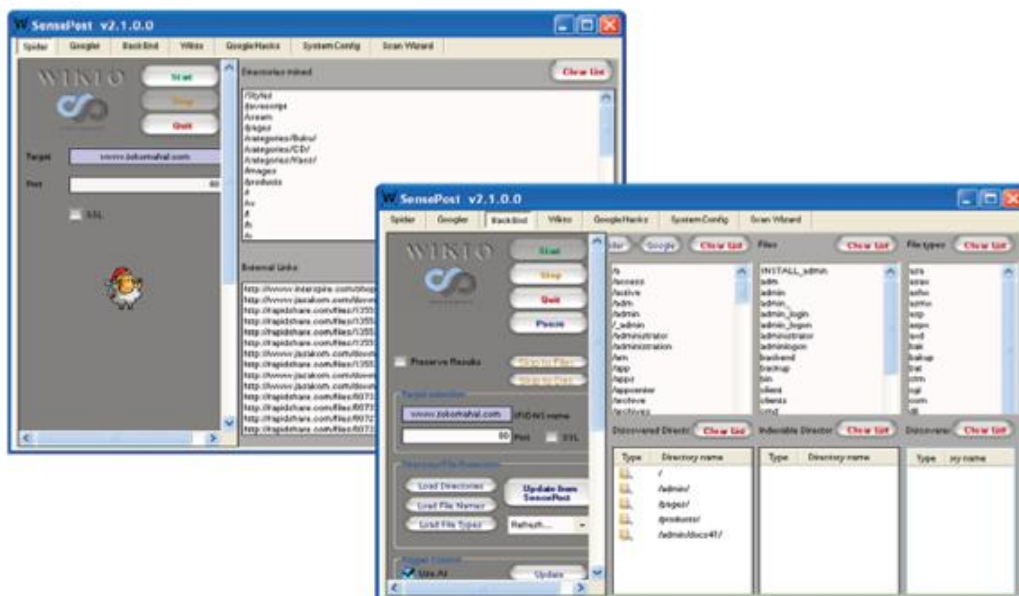
Fungsi *IP Country converter* memberikan hasil yang keliru ketika dicoba, Fungsi *Trace Route* memberikan hasil yang sama dengan fungsi *tracert* bawaan dari sistem operasi tanpa ada kelebihan, fungsi whois tidak bisa dijalankan dengan baik. Satu-satunya fungsi yang berjalan dengan baik dan memberikan hasil yang cukup memuaskan hanyalah *Website Scanner* yang melakukan pencarian link pada sebuah website secara otomatis.

Wikto

Wikto (*Web Server Assessment Tool*), bisa didownload secara gratis melalui situs www.sensepost.com/research/wikto/. Dengan Wikto, Anda bisa mencari link-link eksternal yang terdapat didalam sebuah website melalui fungsi 'Spyder'.

Fungsi lainnya yang sangat berguna untuk kegiatan awal bisa didapatkan dari fungsi yang dinamakan 'Back End'. Fungsi ini akan mencari direktory, file dan type file tertentu yang bisa dikonfigurasi sesuai dengan kebutuhan.

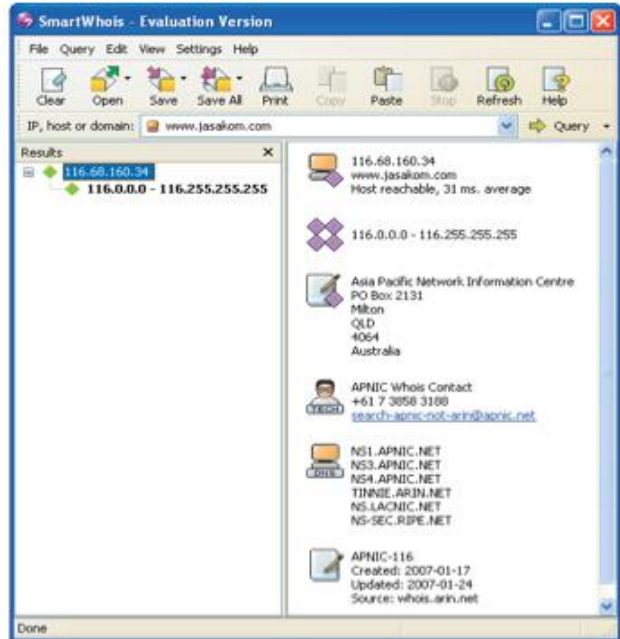
Terkadang administrator (dan saya juga sering melakukannya) merasa aman dengan menyembunyikan file atau direktory penting tertentu dengan nama dan extension yang tidak biasa atau 'aneh'. Wikto akan mencari file dan direktory semacam ini karena file atau direktory yang disembunyikan, biasanya mempunyai fungsi yang sangat penting bahkan terkadang merupakan sebuah pintu masuk yang tidak terkunci.



SmartWhois

SmartWhois dari Tamos (www.tamos.com) merupakan tools whois yang sangat bisa dipercaya (*reliable*) dan memberikan informasi whois dengan format yang mudah dan nyaman untuk dilihat. Tools ini akan memudahkan Anda dalam menggunakan fungsi whois dan memudahkan Anda dalam mencari informasi mengenai sebuah nama domain atau alamat IP, termasuk informasi dari network blok yang digunakan.

Anda juga bisa memberikan keterangan yang Anda butuhkan kedalam hasil query *SmartWhois* dengan klik kanan dan memilih menu 'My Notes'. Hasil pencarian dan dokumentasi Anda juga bisa disimpan sehingga Anda tidak perlu mengulangi pekerjaan yang telah Anda lakukan.



Tools ini juga memiliki fasilitas lainnya yaitu fasilitas integrasi dengan browser seperti IE dan Email. Fasilitas ini memungkinkan Anda menjalankan program whois hanya dengan mengklik menu tambahan yang tersedia didalam browser Anda yang akan membuka program SmartWhois secara otomatis.

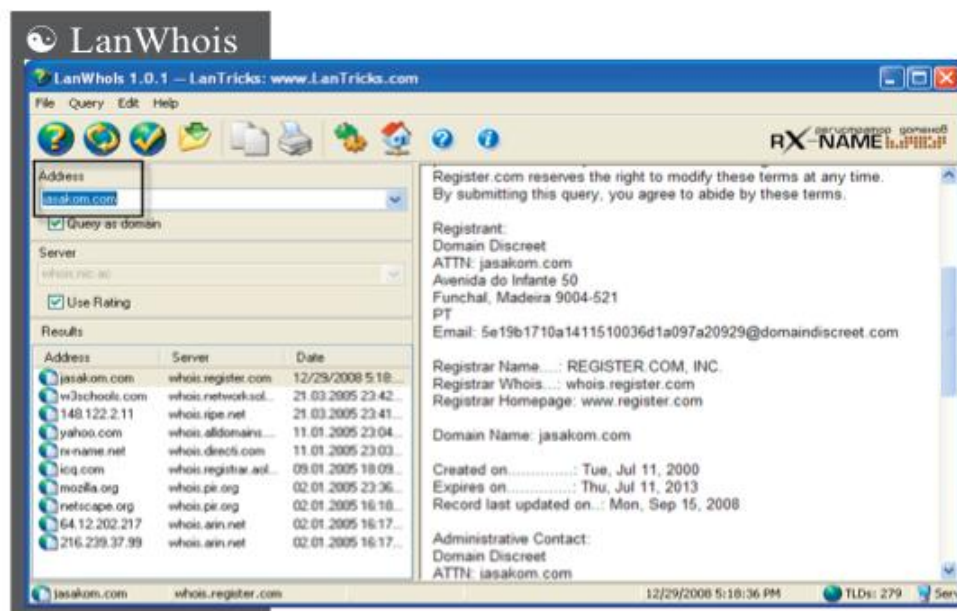


ActiveWhois (www.johnru.com/active-whois/), Seperti tools whois yang

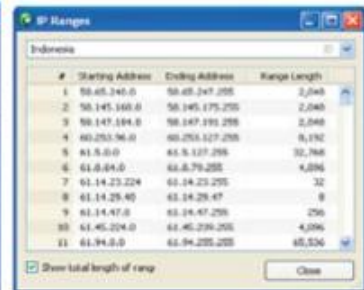
lain, ActiveWhois ini akan mencari informasi berdasarkan nama atau alamat IP yang diberikan.

Hasil query whois ditampilkan dengan format tampilan yang sangat sederhana namun mudah untuk dipahami. Bila Anda tidak suka dengan modus pencarian server otomatis, Anda juga bisa menentukan server whois yang akan digunakan secara manual walaupun pilihan ini jarang digunakan.

Salah satu kelebihan dari ActiveWhois adalah kemampuannya yang bisa bekerja dalam modus Offline, artinya untuk nama domain yang sudah pernah dilakukan pencarian, ActiveWhois akan menggunakan ingatannya kembali ketika tidak ada koneksi internet yang tersedia.



LanWhois, merupakan program Whois yang sederhana yang bisa Anda dapatkan dari situs *lantricks.com*. Program ini akan mencari server whois secara otomatis dan menampilkan kepada Anda hasil pencarian yang Anda lakukan. Program *LanWhois* tidak mempunyai kelebihan yang berarti dibandingkan dengan program Whois lainnya yang telah dibahas.



CountryWhois (www.tamos.com) merupakan program komersial yang dikhususkan untuk mencari lokasi negara dari sebuah domain atau alamat IP. Perlu Anda perhatikan bahwa domain yang berada pada suatu negara, belum tentu milik warga di negara tersebut, bisa saja pemilik domain meng-hosting situsnya pada negara yang berbeda dan hal ini sangat umum dilakukan.

Bila Anda penasaran dengan kemampuan dari *ContryWhois* ini, tekanlah tombol F7 dan Anda akan melihat tabel range alamat IP dari setiap negara. Dengan mencari alamat IP dari sebuah domain dan menggunakan tabel inilah, program *ContryWhois* menentukan lokasi server dari sebuah domain.



WhereIsIP (www.jufsoft.com), program ini menggunakan interface yang sangat sederhana dan mudah untuk digunakan. Anda bisa memasukkan alamat IP atau nama domain pada tabulasi IP Address/Web Site. Anda juga bisa memasukkan alamat email yang ingin diperiksa melalui tombol 'Email Address' dan *WhereIsIP* secara

otomatis akan mengecek alamat IP dari email server yang digunakan dan menampilkan informasi whois dari alamat IP tersebut.



Ip2country (www.olej.com) ini sesuai dengan namanya berfungsi sebagai pencari lokasi dari sebuah alamat IP. Software ini benar-benar hanya berfungsi sesuai dengan namanya, tidak ada lainnya. Anda bahkan tidak bisa memasukkan nama domain dan hanya bisa memasukkan alamat IP. Berita bagusnya adalah software ini bisa didapatkan secara gratis.

CallerIP

CallerIP, program yang bisa didapatkan dari situs www.callerippro.com merupakan program yang sangat menarik dan berguna. *CallerIP* akan menampilkan koneksi-koneksi yang terjadi pada komputer Anda, baik koneksi keluar maupun koneksi masuk dan menampilkannya bersama dengan peta lokasi.

Anda bisa melihat waktu terjadinya koneksi dan jenis koneksi apakah koneksi yang dilakukan dari komputer ke luar (Out) atau koneksi dari komputer luar ke komputer Anda (In). Selain itu jenis aplikasi yang melakukan koneksi juga ditampilkan pada kolom '*Application*' dan kolom '*State*' akan menampilkan informasi status dari koneksi tersebut.

Bila status koneksinya adalah '*Established*' artinya koneksi sedang terjadi, status koneksi '*Closed*' artinya koneksi telah terputus dan status koneksi '*Listening*' artinya belum ada koneksi dan komputer sedang dalam keadaan menunggu koneksi dari luar. Anda bisa mengetahui informasi atau arti dari setiap kolom dengan mengklik header dari kolom tersebut yang akan memunculkan sebuah window penjelasan.



Program *CallerIP* bisa dikatakan sebagai versi 'canggih' dari program *netstat* yang disertakan secara gratis oleh sistem operasi. Dengan program *netstat*, Anda juga bisa mengetahui koneksi yang terjadi namun tanpa informasi negara asal koneksi dan tanpa informasi aplikasi yang membuat koneksi.



Web Data Extractor (www.webextractor.com) akan mencari dan mengumpulkan informasi berharga dari sebuah website dengan cara menelusuri semua link yang ada. Langkah pertama menggunakan

program ini adalah menentukan alamat URL dan informasi yang ingin didapatkan dari URL tersebut melalui konfigurasi yang terdapat didalam 'Session Settings'. Setelah selesai melakukan konfigurasi, langkah selanjutnya adalah mengklik tombol *Start* yang akan membuat program ini segera melakukan tugasnya.

Pada contoh, saya mencoba mendapatkan informasi dari situs *klikbca.com*. Terlihat, dari situs yang ada didalam *klikbca.com*, saya berhasil mendapatkan 6 buah email, 16 nomor telepon, 52 nomor fax, dan berbagai informasi lainnya. Salah satu kekurangan program ini adalah tidak adanya pengecekan informasi yang double. Sebagai contoh, dari 52 nomor fax yang saya dapatkan, sebagian besar isinya sama persis sehingga nomor fax yang sebenarnya saya dapatkan, tidaklah sebanyak itu.

☪ Expired Domains

Expired Domains, tools gratis dari *www.domainsoftware.org* akan memudahkan Anda dalam mencari nama-nama domain menarik yang akan segera kadaluarsa. Domain yang akan segera kadaluarsa ini terkadang bukanlah nama domain yang benar-benar sudah tidak diinginkan lagi oleh pemiliknya.

Beberapa kasus besar pernah terjadi dimana pemilik nama domain lupa memperpanjang nama domainnya sehingga diambil oleh orang lain dan kehidupan demokratis di internet memperbolehkan hal ini untuk terjadi walaupun masih memungkinkan pemiliknya untuk melakukan komplain, namun prosesnya akan rumit dan panjang.



Nama Domain ini telah habis masa berlakunya dikarenakan hal-hal berikut:

- Pemakai/pengelola nama domain ini mengetahui bahwa nama domainnya telah habis masa berlakunya tetapi memilih untuk tidak memperpanjang masa berlaku nama domain tersebut.
- Pemakai/pengelola nama domain ini tidak menerima email informasi mengenai habis masa berlakunya nama domain melalui alamat email yang terdaftar pada sistem registrasi. Hal ini dapat disebabkan oleh tidak aktif/validnya alamat email tersebut.

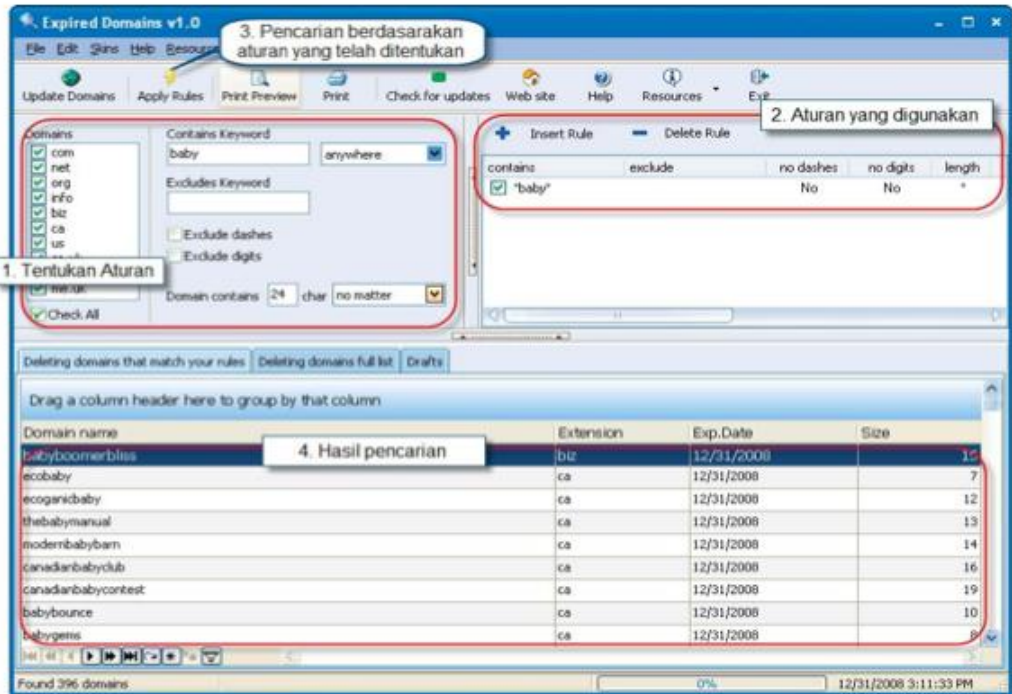
Bila nama domain ini masih ingin dipergunakan maka pihak pemakai/pengelola nama domain ini dapat melakukan proses perpanjangan agar nama domain dapat diaktifkan kembali.

Untuk informasi mengenai proses perpanjangan silahkan menghubungi pengelola domain anda atau dapat langsung menghubungi:

PANDI (Pengelola Nama Domain Internet Indonesia)

Gedung ArthaBhika, Lantai 11
Jalan Jenderal Sudirman Kav 2 Jakarta 10220

Telepon +622157929151 (hunting), +6221 98290955
Fax +62 21 570 30132
Email: info@pandi.or.id
website: www.pandi.or.id

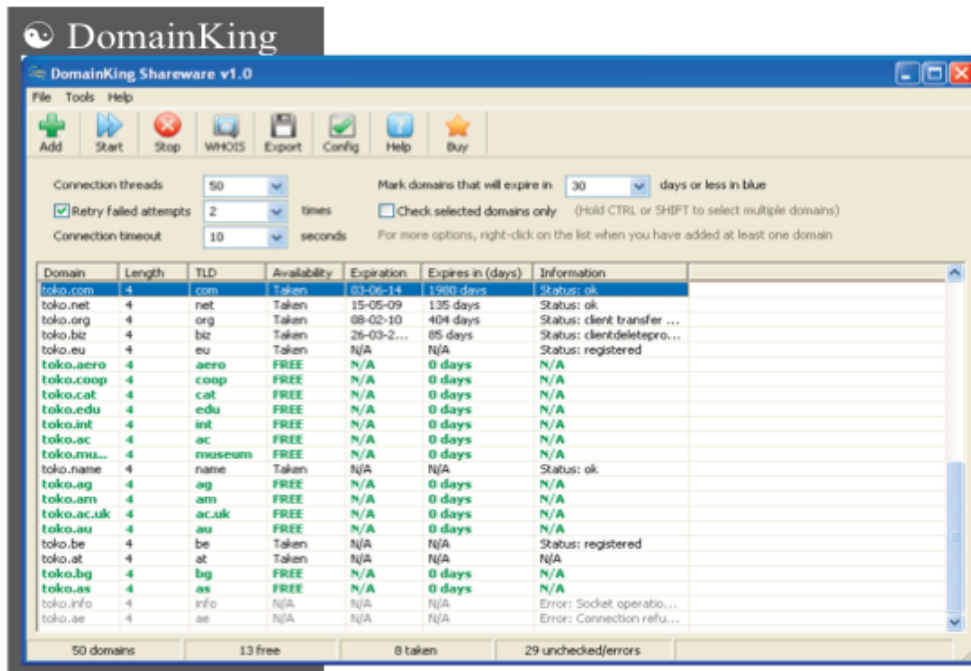


Untuk menggunakan program *Expired Domains* ini, caranya sebenarnya cukup mudah namun karena interfacenya yang cukup rumit, membuat banyak pemakai merasa kebingungan.

Anda bisa mengklik tombol *Update Domains* untuk mendownload semua nama domain yang akan segera habis masa berlakunya yang biasanya sangat banyak. Karena terlalu banyak, mencari satu persatu menjadi sulit untuk dilakukan. Untuk itu, Anda bisa membuat rules atau filter dan menampilkan hanya nama domain yang Anda sukai.

Sebagai contoh, saya membuat aturan yang akan menampilkan nama domain yang mengandung kata *baby*. Untuk itu, langkah pertama (1) yang saya lakukan adalah menentukan jenis domain yang akan ditampilkan, kata yang terdapat didalam domains, jumlah karakter dan aturan lainnya.

Setelah aturan ditetapkan, langkah selanjutnya (2) adalah memasukkan aturan yang telah ditetapkan ini dengan mengklik tombol *Apply Rules* (3). Hasil pencarian nama domain akan ditampilkan pada kolom bagian bawah (4).

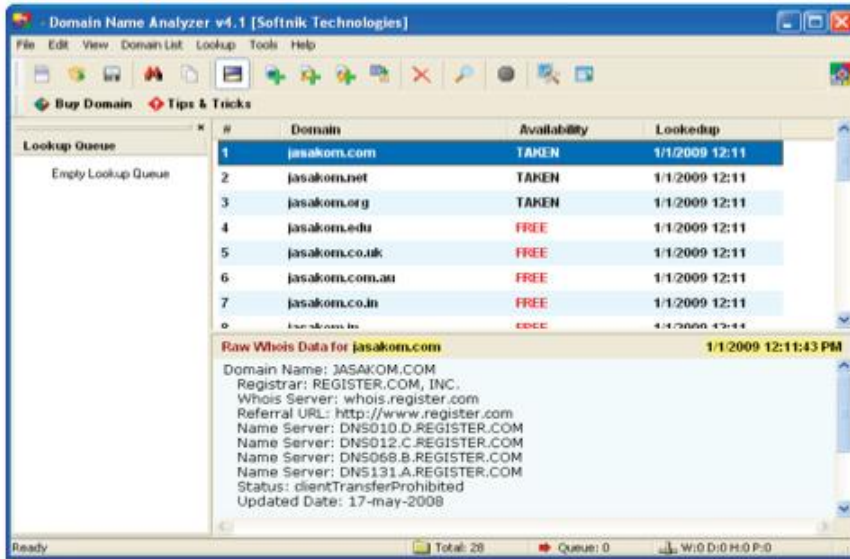


DomainKing (www.twotails.biz), shareware ini akan membantu Anda dalam melakukan pengecekan nama domain secara masal. Anda bisa memasukkan nama domain secara manual atau menciptakan nama domain sesuai dengan kata kunci yang Anda inginkan dan *DomainKing* akan melakukan pengecekan secara otomatis terhadap semua nama domain tersebut.

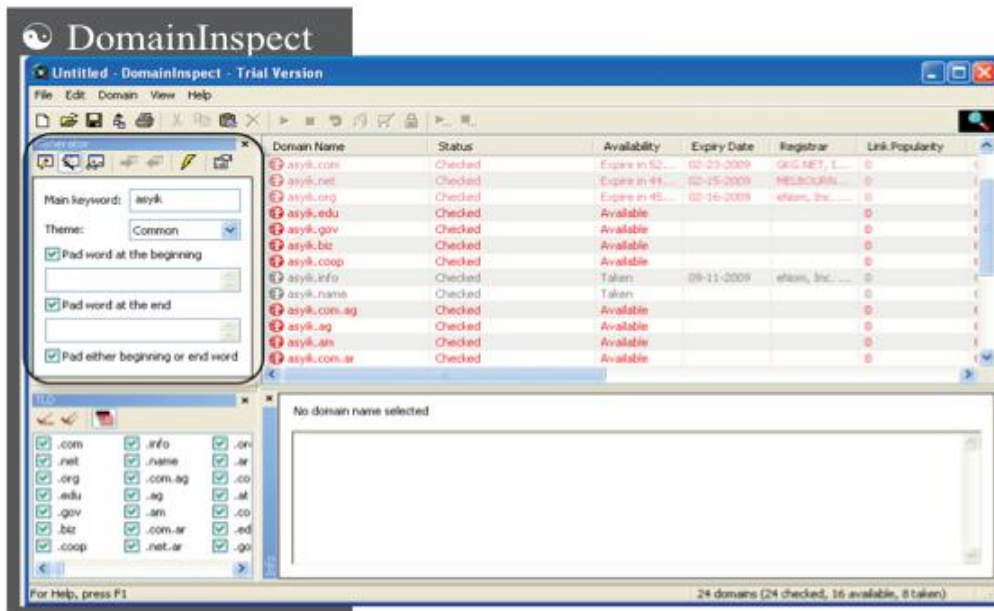
Anda bisa melihat domain mana saja yang telah diregistrasi beserta informasi lainnya dan Anda juga bisa melihat nama domain mana saja yang masih tersedia secara bebas. Pada contoh, saya mengecek nama domain *toko* dengan ratusan extensions domain yang berbeda-beda yang bahkan sebagian besarnya baru saya ketahui seperti .cat, .ag, .at, .dlsb.

Domain Name Analyzer

Domain Name Analyzer (www.domainpunch.com), software gratis ini akan sangat membantu untuk Anda yang ingin melakukan pencarian *whois* secara masal. Anda bisa memasukkan nama domain yang ingin diperiksa secara manual atau memasukkan kata kunci tertentu dan *Domain Name Analyzer* akan menciptakan nama domainnya untuk Anda.

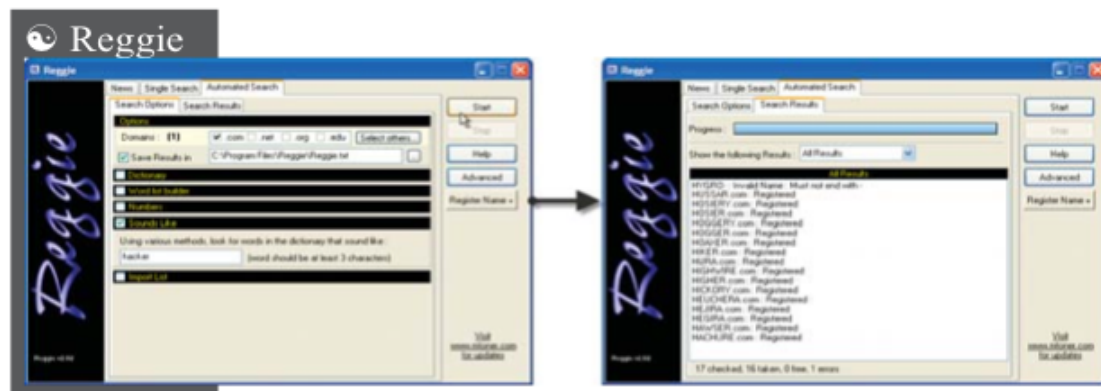


Setelah memasukkan daftar domain yang ingin diperiksa, selanjutnya Anda tinggal memilih menu 'Lookup'. Domain Name Analyzer akan memperlihatkan kepada Anda nama-nama domain yang masih belum dan sudah bertuan.



DomainInspect (www.antssoft.com) akan sangat membantu bagi Anda yang ingin melakukan pengecekan atau melakukan whois terhadap

domain secara masal seperti halnya yang dilakukan oleh software *Domain Name Analyzer* dan *DomainKing*. Anda bisa memasukkan nama domain yang Anda inginkan secara manual atau Anda juga bisa memasukkan kata kunci dan membiarkan *DomainInspect* menciptakan nama domain untuk Anda.

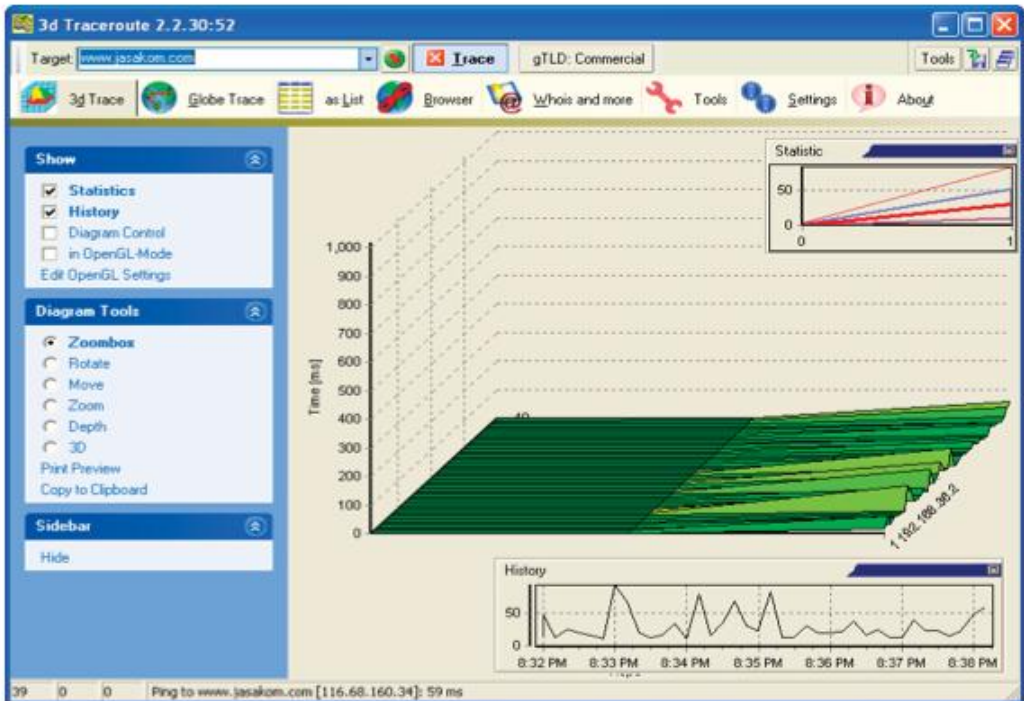


Reggie (www.mtoner.com), program komersial seharga \$29.95 ini memang sejenis dengan program *whois* yang telah dibahas. Anda bisa mengecek banyak domain sekaligus dan melihat apakah domain tersebut sudah ada pemiliknya atau belum. Satu keunikan yang ada pada program Reggie ini adalah fungsi 'Sounds Like'. Fungsi ini akan membuat daftar nama domain yang lafalnya (cara pengucapan) hampir sama dengan kata kunci yang Anda masukkan.

Sebagai contoh, pada tabulasi *Search Options*, saya memilih pilihan *Sounds Like* dan memasukkan kata kunci *hacker*. Selanjutnya, saya tinggal mengklik tombol *Start* dan Reggie akan segera membuat dan sekaligus mengecek domain-domain yang cara pengucapannya hampir sama dengan kata *hacker*.

3D Traceroute

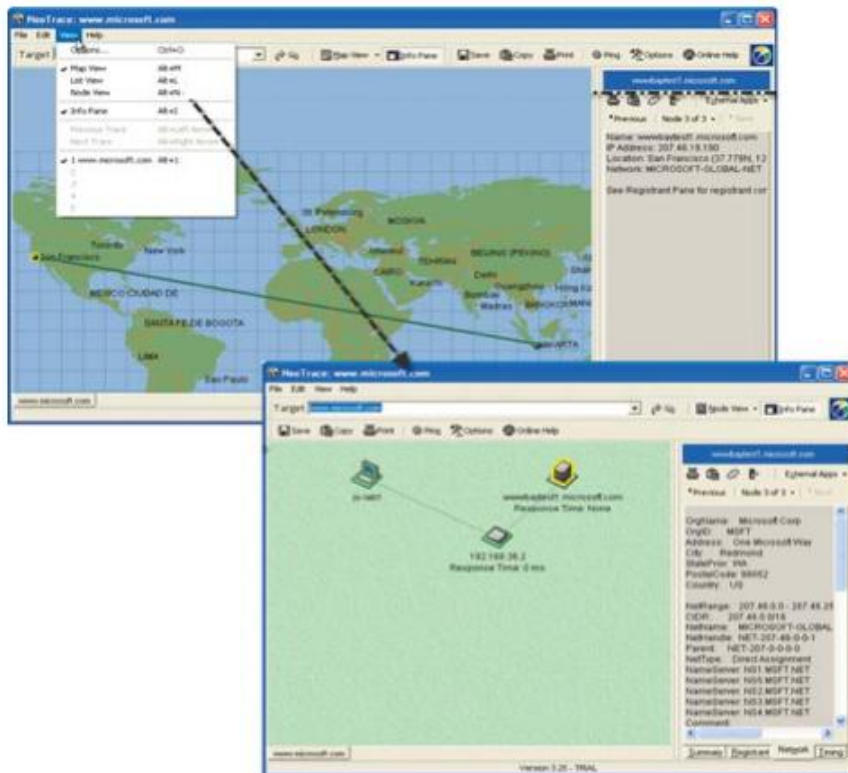
3D Traceroute (www.d3tr.de), menampilkan hasil traceroute secara visual berupa grafik dalam bentuk tiga dimensi. Grafik tiga dimensi ini, masih bisa Anda tentukan sesuai dengan kebutuhan Anda. Tampilan dalam bentuk visual memang bagus, namun untuk analisa yang lebih tajam terkadang agak menyulitkan sehingga program ini tetap dilengkapi dengan tampilan dalam bentuk tabel (tombol *as List*).



Versi berbayarnya yang diberikan tambahan kata 'Pro' menjadi '**3D Traceroute Pro**', memiliki fungsi *Globe Trace* dimana Anda bisa melihat rute-rute yang dilewati oleh paket traceroute dalam bentuk peta visual. Selain fungsi utamanya dalam memperlihatkan paket traceroute, software ini juga dilengkapi dengan beberapa utility tambahan seperti whois, port scanner, dll.

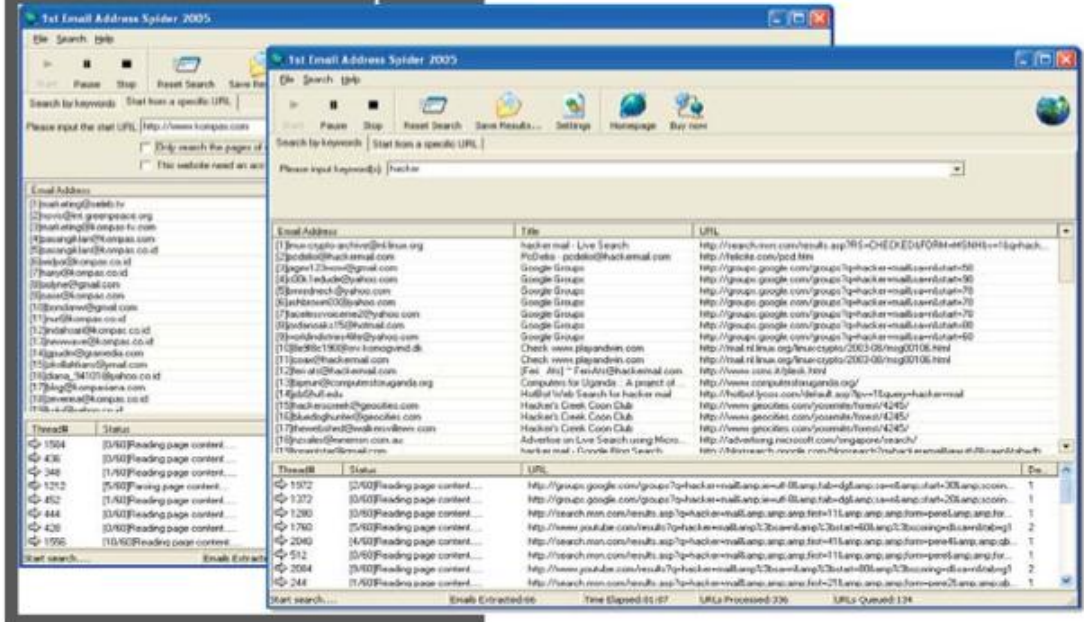
NeoTrace

Neotrace, setelah bergabung dengan McAfee, mengganti namanya menjadi *McAfee Visual Trace*. *McAfee Visual Trace* adalah sebuah tools traceroute visual yang sangat mudah dan nyaman untuk digunakan. Anda bisa melihat lokasi-lokasi yang dilewati oleh paket data Anda dalam bentuk peta dunia dan Neotrace secara otomatis juga meng-whois alamat IP tujuan yang bisa dilihat pada kolom sebelah kanan. Selain tampilan dalam bentuk peta, Anda juga bisa melihat tampilan dalam bentuk yang dinamakan sebagai '*Node View*' (gambar bawah).



Path Analyzer Pro (www.pathanalyzer.com) merupakan tools yang sangat berguna untuk Anda yang ingin melihat dan menganalisa perjalanan paket traceroute. Selain berupa peta, Anda juga bisa melihat perjalanan dan performance dari paket-paket yang dikirimkan menuju tujuan dalam bentuk grafik.

1st Email Addrss Spider



1st Email Address Spider (www.123hiddensender.com), merupakan tools pengumpul alamat email yang bertebaran di internet. Anda bisa mengumpulkan alamat email yang terdapat pada sebuah situs tertentu saja atau Anda juga bisa meminta software ini mencari alamat email berdasarkan kata kunci tertentu.

Fungsi pencarian alamat email berdasarkan kata kunci tertentu yang bisa dijalankan dengan mengklik tabulasi *Search by keywords* ini memungkinkan Anda mencari alamat email yang berhubungan dengan kata kunci yang Anda masukkan. Sebagai contoh, Anda bisa memasukkan kata kunci 'hacker' atau 'security' untuk menemukan alamat email yang berhubungan dengan bidang keamanan komputer atau Anda bisa memasukkan kata 'asuransi jiwa' untuk menemukan alamat email orang-orang yang berhubungan dengan bidang asuransi jiwa.

Tools ini mampu mengumpulkan alamat email dalam jumlah ribuan dalam waktu singkat bila Anda memiliki bandwidth internet yang besar. Tidak disangkal lagi, ini adalah salah satu program pengumpul alamat email yang sangat baik dan mudah untuk disalah gunakan.



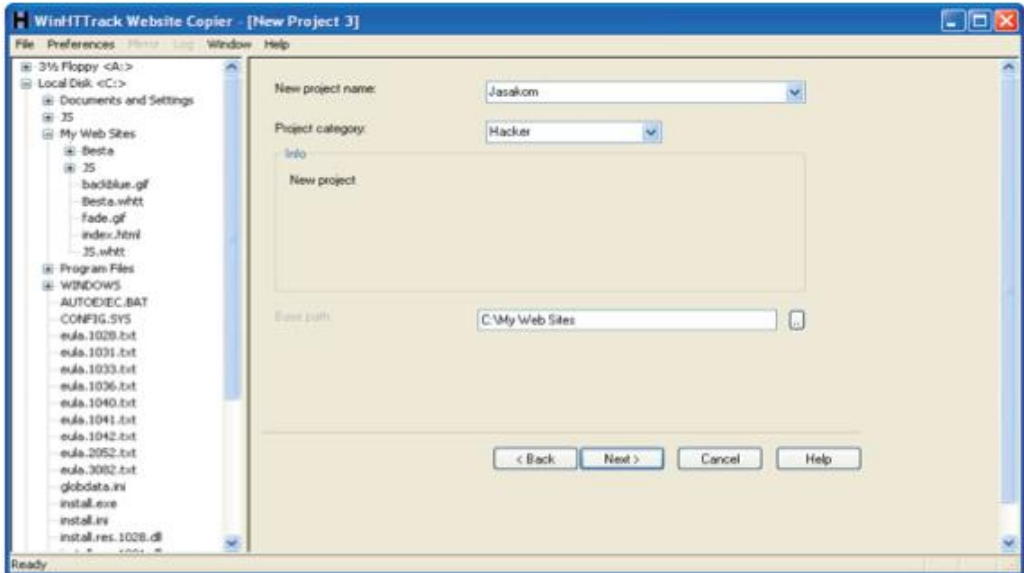
Power Email Collector (www.tecsoftware.biz), merupakan tools pengumpul alamat email yang jauh lebih sederhana dibandingkan dengan *1st Email Address Spider*. Tools ini akan mengumpulkan alamat email dari nama domain yang Anda berikan kepadanya dan tidak bisa melakukan pencarian berdasarkan kata kunci atau keyword seperti yang dilakukan oleh *1st Email Address Spider*.

Untuk mempercepat proses pencarian email, *Power Email Collector* akan membuat koneksi-koneksi secara bersamaan (default setting untuk *Connections* adalah 20) sehingga kecepatan yang didapatkannya bisa Anda sesuaikan sesuai dengan besarnya bandwidth yang Anda miliki.

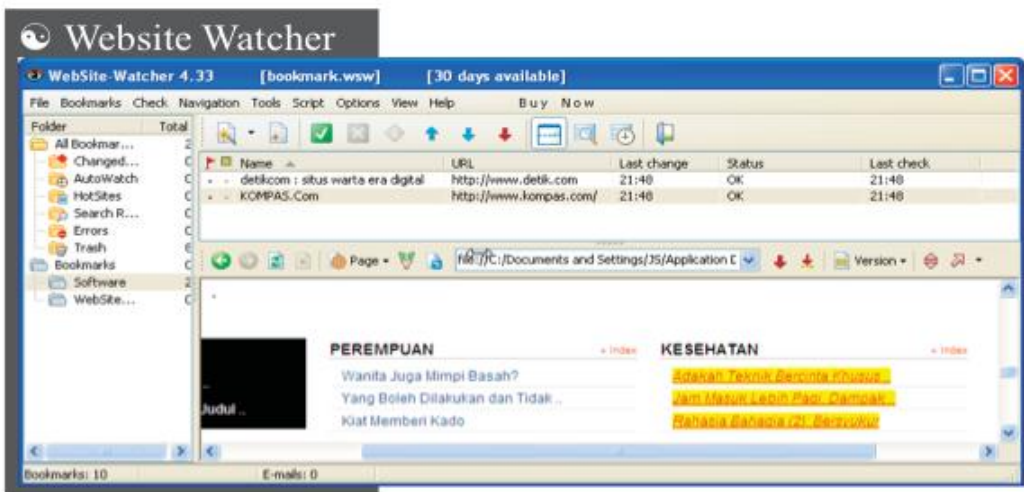
HTTrack Web Site Copier

HTTrack Web Site Copier (<http://www.httrack.com>), software gratis ini memungkinkan Anda mengcopy halaman website kedalam komputer Anda. Dengan memindahkan isi situs kedalam komputer lokal, Anda bisa menelusuri halaman demi halaman suatu website tanpa harus terhubung ke internet. Dengan browsing secara offline, tentunya lebih cepat dan mudah melakukan analisa.

Tidak semua situs bisa dipindahkan kedalam komputer lokal. Sebagai contohnya, situs yang penuh dengan halaman flash, tidak bisa dipindahkan secara sempurna. Untuk memindahkan situs kedalam kompute lokal, Anda tinggal membuat project baru dengan mengklik menu *File* → *New Project* atau dengan menekan tombol *Ctrl+N*.



Setelah itu, isilah nama project dan kategori yang bisa Anda isi dengan apa saja. Anda juga menentukan lokasi tempat penyimpanan website secara offline di komputer Anda yang secara default ada di 'C:\My Web Sites'. Setelah proses pengcopyan selesai dilakukan, Anda tinggal masuk ke folder lokal di komputer Anda dan mengklik file *index.html* untuk melihat website secara offline.



Website Watcher(www.aignes.com), adalah jawaban untuk Anda yang telah menghabiskan sebagian besar waktu Anda untuk mengecek

situs-situs di internet. Software ini akan membantu Anda melakukan pemantauan terhadap website-website yang telah Anda tentukan sebelumnya sehingga Anda bisa segera mengetahui ketika terdapat perubahan pada situs yang Anda pantau atau biasa Anda kunjungi. Kelebihannya adalah, semuanya bisa dikerjakan dalam waktu singkat.

Bila terdapat perubahan pada situs yang Anda awasi, alamat website akan berubah menjadi warna merah dan ketika Anda melihat website yang telah terjadi perubahan tersebut, bagian yang berubah akan disorot oleh *Website Watcher*. Suatu feature yang sangat berguna sehingga Anda tidak perlu mencari lokasi dari informasi baru tersebut.

Website Watcher mampu melakukan hal ini karena pada saat Anda memasukkan alamat situs yang hendak dipantau, *Website Watcher* akan menyimpan halaman yang akan diawasi ke dalam komputer lokal Anda dan menggunakannya sebagai pembanding ketika melakukan pengecekan selanjutnya.

Software ini tidaklah sempurna dan mempunyai satu kekurangan yang sangat disayangkan. Anda tidak bisa menentukan bagian mana saja yang tidak perlu dipantau. Sebagai contoh, saat ini banyak sekali situs-situs yang menampilkan bagian yang dinamis seperti iklan yang akan selalu berubah ketika Anda masuk ke situs tersebut. Sifat semacam ini akan bermasalah karena *Website Watcher* akan selalu menganggap terdapat sesuatu yang baru pada website yang dipantau.

Module 3

Google Hacking

Perkembangan internet yang sangat mengagumkan dan diluar perkiraan semua orang, telah membuat hampir semua informasi bisa didapatkan dari internet. Masalahnya adalah mencari informasi dari sekian milyar situs yang ada didalam dunia internet ini tidaklah mudah dan bahkan bisa dikatakan tidak memungkinkan bila dilakukan secara manual dengan mengunjungi satu persatu situs yang ada. Solusi yang paling cerdas adalah dengan memanfaatkan mesin pencari (*search engine*) seperti google, yahoo, msn, dan lain lain.

Untuk memudahkan pencarian, *search engine* akan menyimpan informasi penting yang didapatkan dari situs internet kedalam server internal mereka sendiri dan melakukan indexing sehingga proses pencarian bisa berlangsung dengan cepat, tanpa harus menghubungi satu persatu web server yang ada di dunia ini.

Tugas maha berat dari *search engine* adalah mengumpulkan inti dari halaman-halaman yang tersebar didalam hutan belantara internet yang dipercayakan kepada robot. Robot? Benar, namun bukan robot seperti yang Anda kira. Robot *search engine* yang seringkali disingkat menjadi bot dan juga seringkali disebut dengan nama *Crawler* atau *Spider* ini adalah sebuah software khusus yang bertugas menelusuri setiap halaman web yang ada didunia ini dan bot yang digunakan oleh Google dinamakan dengan *Googlebot*.

Baik, lalu apa yang dimaksud dengan *Google Hacking*? *Google hacking* adalah teknik mencari informasi dengan mesin pencari sehingga bisa didapatkan informasi-informasi berharga yang terdapat didalam mesin pencari. Teknik yang pelopori oleh *Johnny Long* ini menjadi sangat terkenal karena ternyata sangatlah mudah mendapatkan

berbagai informasi berharga seperti password, nomor kartu kredit, serta berbagai informasi yang seharusnya rahasia dari mesin pencari ini.

Google hacking juga digunakan oleh para hacker dalam mencari korbannya sehingga jangan heran bila situs

Anda yang jarang pengunjungnya dan tidak punya musuh bisa tiba-tiba di-hack oleh hacker. Seperti yang Anda perkirakan, situs mesin pencari *google.com* adalah senjata utama dari *Google Hacking*.

Catatan: Sebagian dari isi bab ini diambil berdasarkan teknik yang dijabarkan oleh Johnny Long

ARTIKEL COMMUNITY

Analisa Bug VP-ASP

Oleh Dr' Ponds

Published: Juli 19, 2003

Print

Meskipun bug ini sudah lama, masih tetap ada saja beberapa situs shopping yang vulnerable dengan bug vp-asp ini

Hal itu dikarenakan kecerobohan dari si pemilik situs. Kenapa bisa begitu? Ok, akan saya jelaskan. ;)

[Exploit]

1. Buka browser kesayangan kamu terserah mo make IE atau Netscape. Abis itu lo buka situs Search Engine macam kayak www.google.com atau situs search engine lainnya.

2. Setelah itu lo isi keyword di search engine dengan beberapa type sbt:

```
- allinurl:shopdisplaycategories.asp
[shopdisplaycategories.asp apaan tuh? :), itu merupakan main page nya vp-asp]

- allinurl:shopadmin.asp
[shopadmin.asp apa lagi neh?, ye.. itu kan utk masukin log ma pasword adminnya :)]

- allinurl:shopdbtest.asp
[shopdbtest.asp mmm... i like it :), shopdbtest.asp merupakan Diagnostic Tool for VP-ASP Shopping Cart
berguna untuk test database access and mail access di VP-ASP]
```

Google Cache

Seperti yang telah saya jelaskan sebelumnya, google mencari dan menyimpan informasi-informasi berharga pada setiap halaman web di internet kedalam server mereka. Selain itu, google juga menyimpan halaman penting ke dalam server mereka. Halaman penting yang tersimpan didalam server google dinamakan sebagai *cache memory*. Google.co.id juga memberikan fasilitas untuk melihat halaman cache ini yang bisa Anda lakukan dengan mengklik link *Tembolok* atau link *Cached* bila Anda menggunakan Google dalam bahasa inggris.

Dengan melihat dan mengambil data dari *cache memory*, artinya hacker tidak perlu berhubungan secara langsung dengan server korban. Karena tidak berhubungan dengan komputer korban, artinya segala proteksi dan segala alat deteksi yang terpasang tidak akan berguna, bahkan korban tidak akan mengetahui bahwa data penting mereka telah diambil oleh hacker.

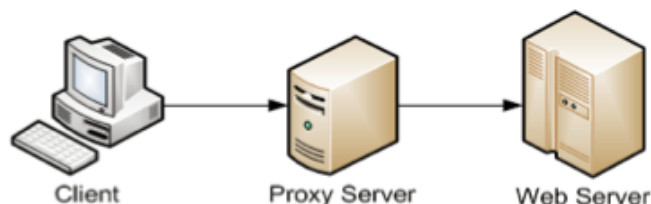


Pada bagian atas dari setiap halaman cache yang ditampilkan, Google menginformasikan tentang kapan halaman tersebut diambil oleh google. Pada contoh, halaman situs jasakom yang saya lihat pada tanggal 8 Januari, diambil oleh Google pada tanggal 7 Januari 2008 yang artinya hanya berbeda 1 hari.

Karena halaman yang ditampilkan adalah data terakhir yang diambil oleh google, ada kemungkinan halaman sebenarnya dari situs jasakom.com telah berubah dan cache google tidak akan berubah sampai Googlebot mengambil data terbaru. Hal ini berarti pula bahwa apabila Anda membuang informasi penting dari situs Anda, ada kemungkinan informasi tersebut masih tersimpan didalam cache google dan hacker masih bisa mendapatkannya dari situ.

Proxy Google

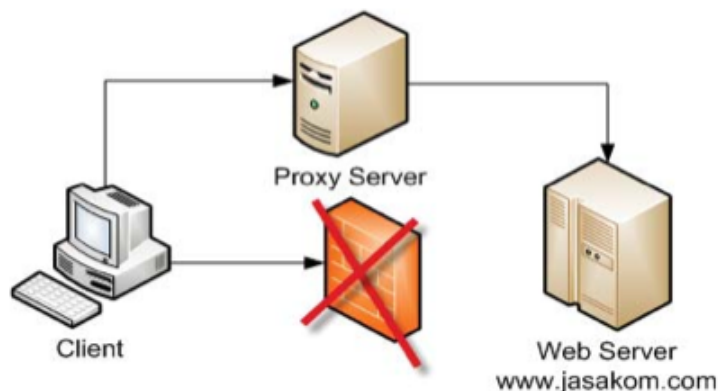
Sebelum menjelaskan penggunaan google sebagai proxy server, saya akan menjelaskan kepada Anda secara singkat fungsi dari proxy server dan apa yang dilakukan oleh sebuah proxy server terlebih dahulu. Proxy server bisa dikatakan sebagai calo, orang yang berfungsi sebagai perantara. Sebagai contoh, bila Anda mengunjungi sebuah website dengan memanfaatkan proxy server maka yang terjadi adalah komputer Anda menghubungi proxy server dan proxy server yang akan mengambil data dari web server untuk Anda (masalah proxy akan banyak dibahas lebih lanjut pada module 4).



Dengan adanya proxy server ini, artinya Anda tidak berhubungan secara langsung dengan Web Server dan artinya Web server hanya mengetahui proxy server yang melakukan permintaan. Karena Anda tidak berhubungan secara langsung, keberadaan Anda tidak akan terdeteksi oleh Web Server karena itu, proxy server seringkali dimanfaatkan oleh orang-orang yang tidak ingin keberadaannya diketahui seperti yang seringkali dilakukan oleh seorang hacker!

Selain masalah privasi, proxy server juga bisa digunakan untuk melewati proteksi baik yang dilakukan oleh sisi client maupun dari sisi server. Sebagai contoh, kantor Anda melarang Anda browsing ke situs www.jasakom.com karena dianggap sebagai situs yang menyebarkan informasi berbahaya.

Untuk melewati proteksi semacam ini, Anda bisa memanfaatkan perantara yaitu proxy server untuk browsing ke situs Jasakom. Dengan adanya proxy server ini, alat proteksi didalam kantor Anda hanya akan mengetahui bahwa Anda melakukan koneksi ke proxy server, bukan ke situs www.jasakom.com.



Kondisi yang sama juga terjadi ketika koneksi diproteksi dari server. Sekarang andaikan webserver www.jasakom.com melarang Anda untuk browsing ke situs mereka karena Anda pernah meng-hack situsnya.

Dengan memanfaatkan proxy server, *jasakom.com* mengira yang melakukan permintaan adalah proxy server, bukan Anda. Contoh nyata lainnya adalah proteksi alamat IP oleh situs *rapidshare.com* yang bisa dilewati dengan memanfaatkan proxy sehingga Anda tidak perlu menunggu berjam-jam hanya untuk mendownload file dari situs mereka.

Sekarang waktunya kembali lagi pada pembahasan utama kita tentang Google (masih ingat?). Dimana layanan proxy dari google? Google tidak menyediakan layanan ini sama sekali! namun google mempunyai sebuah layanan 'penerjemah' pada alamat "*http://translate.google.com/translate_t#*" yang bekerja mirip dengan proxy.

Sebagai contoh, bila Anda tidak paham dengan bahasa inggris, Anda bisa meminta google melakukan penerjemahan halaman tersebut dan menampilkannya dalam bahasa indonesia. Google akan membaca halaman yang Anda inginkan dan membuat halaman baru untuk Anda dengan bahasa yang Anda inginkan.

Pada contoh, saya meminta google menerjemahkan halaman *www.jasakom.com* ke dalam bahasa inggris dan secara tidak langsung, google mengakses halaman yang saya minta dan bayangkan bila halaman yang saya minta sebenarnya adalah sebuah kode berbahaya. Apa yang terjadi? Google melakukan penyerangan dengan perintah saya dan didalam log file webserver, yang tercatat adalah server google.



Didalam modul CEH, Anda diajarkan melakukan penerjemahan dengan bahasa yang sama untuk memfungsikan google sebagai proxy. Sebagai contoh, Anda bisa meminta google menerjemahkan halaman dalam bahasa indonesia ke bahasa indonesia, akibatnya adalah google berfungsi sebagai proxy murni. Teknik ini bisa digunakan dulunya tapi itu dulu, sekarang sudah tidak bisa lagi karena google mulai menyadari kesalahan mereka dan memperbaiki masalah semacam ini.

Teknik lain yang saya gunakan dulunya adalah membohongi google seperti menerjemahkan halaman www.jasakom.com yang aslinya berbahasa indonesia. Saya meminta google menerjemahkan halaman tersebut yang saya katakan menggunakan bahasa inggris menjadi bahasa indonesia dan google-pun akan melakukannya dengan senang hati. Teknik ini juga sudah tidak berlaku lagi karena adanya pendeteksian otomatis dari google tentang bahasa yang digunakan oleh sebuah halaman website.

Menampilkan Direktory Listing

Direktory listing adalah halaman website yang menampilkan isi file yang ada didalam webserver layaknya file explorer. Dengan menampilkan file-file yang ada didalam webserver, pengunjung akan dengan mudah melakukan navigasi dan melihat file-file yang ada didalam webserver. Masalahnya adalah direktory listing ini terlalu terbuka dan memungkinkan pengunjung melihat dan mengambil file-file yang ada didalamnya yang sangat mungkin terdapat file penting yang tidak seharusnya dilihat apalagi diambil.

Beberapa setting webserver secara default mengaktifkan direktory listing ini apabila file default tidak tersedia seperti *index.html*, *index.asp*, *index.php*, *default.html*, *default.php*, dan lain sebagainya. Masalahnya adalah terkadang, file default ini hilang atau terhapus secara tidak sengaja dan akibatnya adalah setiap pengunjung yang mengunjungi situs ini, akan bisa melihat semua file yang ada didalam webserver ini termasuk file-file yang seharusnya sangat rahasia.

Masalah file default ini menjadi sangat umum terjadi karena setiap direktory yang ada didalam webserver, diharuskan memiliki file default agar webserver tidak menampilkan direktory listing dan

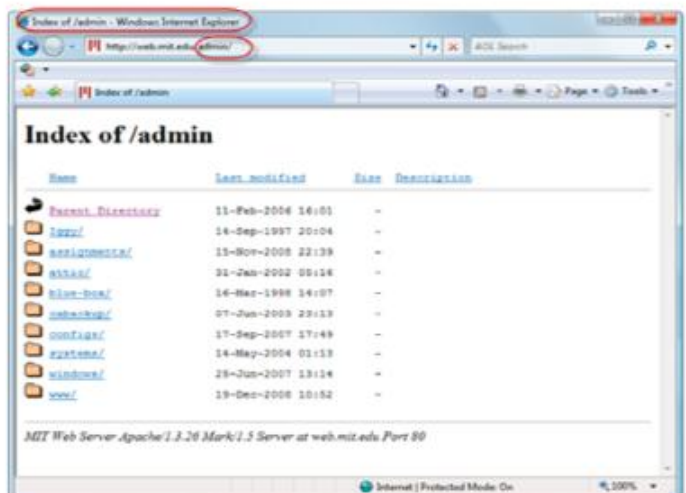
akibatnya, banyak yang lalai dalam hal ini karena tidak menyadari direktory listing diaktifkan dalam webserver mereka.

Sebagai contoh pada saat buku ini dibuat, pada situs <http://web.mit.edu>. Pada halaman depan situs ini, halaman utamanya ditampilkan dengan baik namun ketika saya mengetikkan secara langsung direktory didalamnya, <http://web.mit.edu/admin/> yang kebetulan tidak ada file default yang tersedia dimana direktory listing pada webserver ini sendiri diaktifkan, yang terjadi adalah saya bisa melihat semua file dan direktory yang ada didalamnya.

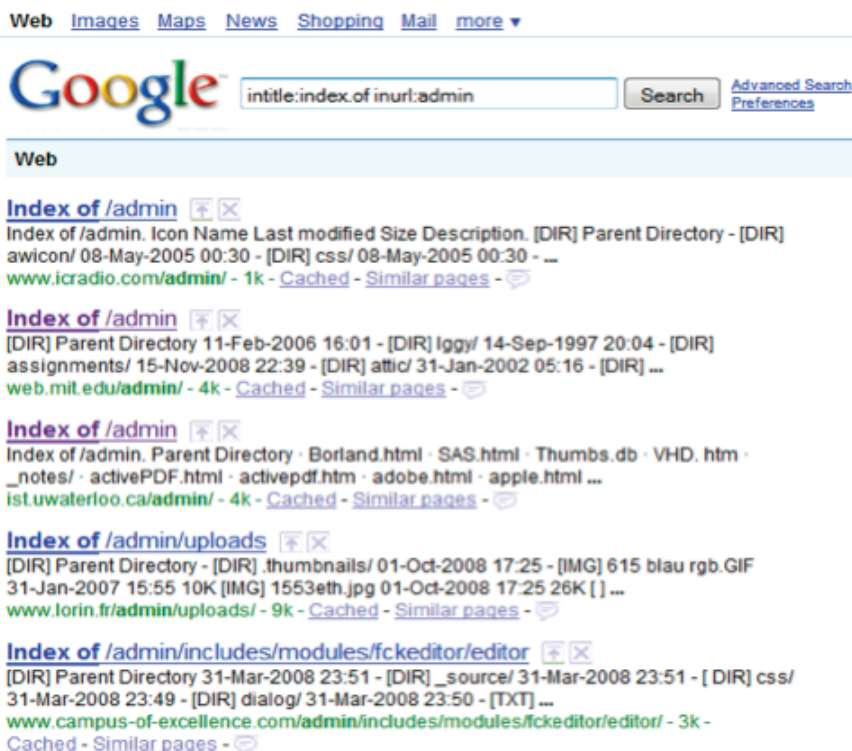


Inti dari teknik google hacking adalah mencari keunikan karena tanpa adanya keunikan ini, Anda akan mendapatkan terlalu banyak hasil dan celaknya adalah sebagian besar hasil pencarian Anda tidak ada hubungannya sama sekali dengan yang Anda inginkan. Sebagai contoh, mari kita lihat kembali halaman admin dari situs web.mit.edu ini.

Pada bagian title terdapat kata "Index of" yang cukup unik dan untuk melakukan pencarian kata yang ada

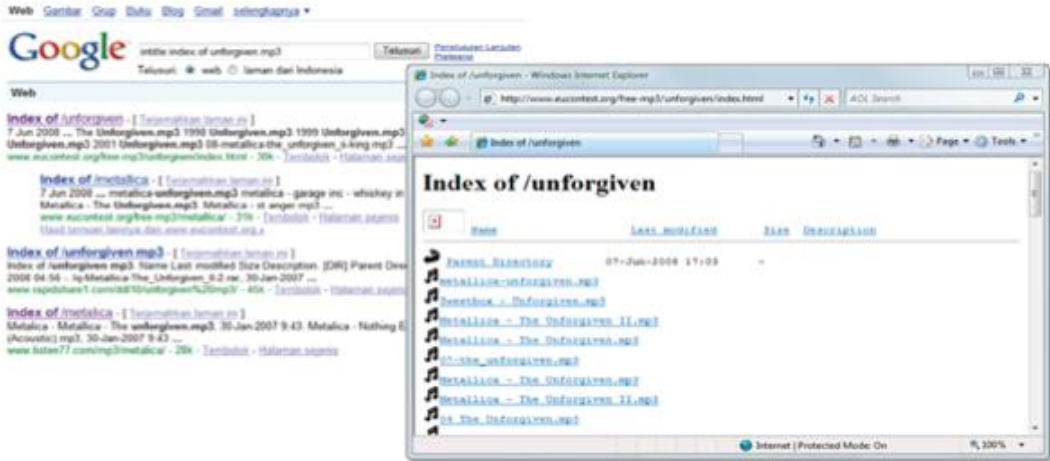


didalam title, Anda bisa menggunakan operator “**intitle:**”. Karena direktory `/admin` sangat umum digunakan dan umumnya file-file didalam direktory ini adalah file penting, maka pencarian direktory ini menjadi sangat menarik. Untuk mencari berdasarkan direktory tertentu, Anda bisa menggunakan operator “**inurl:**”. Jadi, perintah lengkap yang digunakan adalah “**intitle:index.of inurl:admin**”



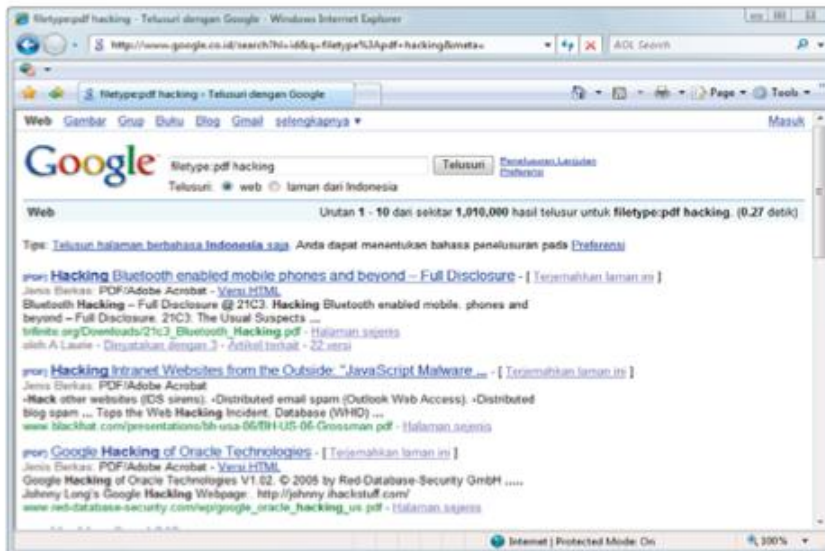
Mencari File Tertentu

Untuk melakukan pencarian file tertentu yang ada didalam direktory listing, Anda tinggal memasukkan nama file yang hendak dicari. Sebagai contoh, untuk mencari file lagu *unforgiven.mp3*, kata kunci yang Anda gunakan adalah “**intitle:index.of unforgiven.mp3**”. Dengan kata kunci ini, terlihat dengan mudah saya bisa mendapatkan file .mp3 dari metallica ini. Dengan teknik yang sama, Anda bisa mencari file lainnya seperti boot.ini, ws_ftp.log, dlsb.



Mencari Type File

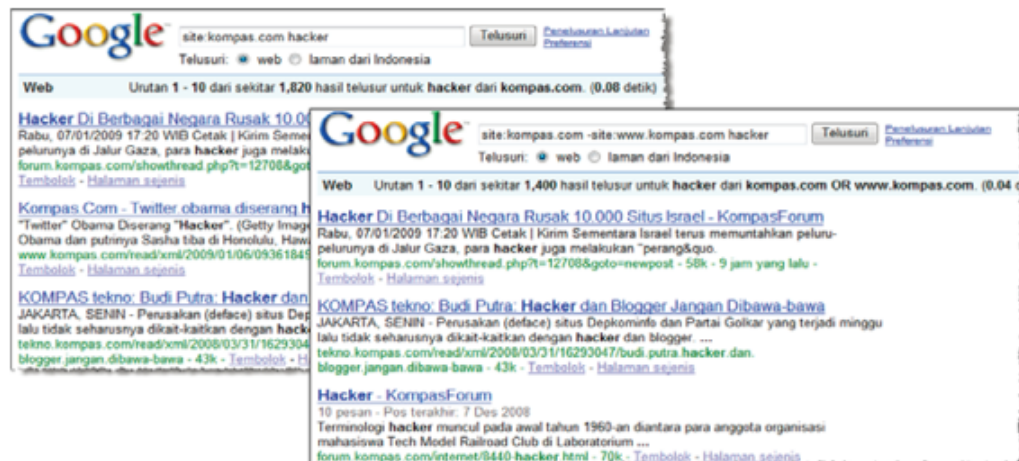
Dengan google, Anda juga bisa melakukan pencarian jenis file tertentu seperti file mp3, doc, pdf dan lain sebagainya. Dokumentasi, panduan, manual, ebook dan berbagai dokumen lainnya biasa disajikan dalam bentuk pdf karena pdf mampu menawarkan tampilan dan bentuk yang lebih profesional, selain itu, dokumen pdf bisa dicetak pada berbagai lingkungan yang berbeda dengan hasil cetakan yang sama persis.



Untuk mencari jenis dokumen tertentu, Anda bisa menggunakan operator **filetype:** yang diikuti dengan type file yang diinginkan seperti pdf, doc, txt atau jenis file lainnya. Operator ini membutuhkan parameter tambahan karena Anda tidak bisa meminta google mencari type file tertentu tanpa memasukkan kata kunci tambahan sama sekali, misalnya meminta google menampilkan semua file .pdf. Sebagai contoh, untuk meminta google mencari file pdf yang berhubungan dengan kata *hacking*, perintah yang digunakan adalah **filetype:pdf hacking**. Dengan teknik yang sama, Anda bisa mencari type-type file lainnya.

Pencarian Pada Domain Tertentu

Selain mencari di hutan belantara Internet, Anda bisa meminta agar google hanya melakukan pencarian pada situs tertentu. Google mendukung pencarian pada situs yang Anda tentukan dengan operator **"Site:"** yang disertai dengan alamat domain yang hendak Anda lakukan pencarian. Sebagai contoh, dengan perintah **"Site:kompas.com hacker"**, google akan menampilkan semua artikel yang memiliki kata hacker didalamnya pada semua situs berdomain kompas.com.



Bila Anda ingin salah satu sub domain tidak dimasukkan, misalnya karena memberikan hasil tidak relevan yang terlalu banyak, Anda bisa menggunakan operator **"-site:"**. Pada contoh, saya memasukkan

perintah **"site:kompas.com –site:www.kompas.com hacker"**. Arti dari perintah ini adalah meminta agar google melakukan pencarian pada semua situs berdomain **kompas.com** kecuali sub domain **www.kompas.com**. Pada contoh, terlihat bahwa google akan menampilkan semua artikel yang berhubungan dengan kata **hacker** namun domain **www.kompas.com** akan diabaikan atau tidak dilakukan pencarian.

Operator Site juga bisa digunakan tanpa parameter tambahan. Misalnya Anda bisa memasukkan perintah **"site:kompas.com"**, maka google akan menampilkan semua direktory dan subdomain dari **kompas.com**. Cara ini sangat efektif dan efisien untuk menelusuri struktur direktory dan sub domain yang ada pada suatu domain.

Mencari "Target" Toko Online

Seperti yang pernah saya sampaikan pada awal bab ini, hacker memanfaatkan google hacking dalam mencari korban-korbannya. Sebagai contoh, andaikan terdapat permasalahan pada program shopping card bernama **cube cart 2.0.1**. Hacker yang sebelumnya tidak memiliki pengecetahan tentang software ini bisa mencari informasi dari situs resmi **cube card** dan mempelajari keunikan dari program yang dibuat berdasarkan **cube card 2.0.1** ini.

The screenshot shows a Google search interface with the query "powered by cube cart 2.0.1". The search results list several websites, including "CubeCart - Free & Commercial Online Shopping Cart Software", "Google Hacking for Penetration Testers: For Penetration Tester", "Generations Cross Stitch (powered by CubeCart)", "Clay From: Metal Sculpture (powered by CubeCart)", "Down For Five Web Shop (powered by CubeCart)", and "Marshwood Gardens (powered by CubeCart)".

The preview of the "Down For Five" website shows a banner with the text "DOWN FOR FIVE" and a skull icon. The website content includes a welcome message, a list of products, and a section for "Powered by CubeCart 2.0.1".

Biasanya terdapat situs contoh yang disediakan oleh pembuat software untuk mendemonstrasikan pemakaian softwrenya kepada calon pelanggan dan hacker bisa memanfaatkan hal ini. Cara lainnya, hacker juga bisa mendownload program trial yang biasa disediakan secara gratis.

Sebagai contoh, untuk program Cuber Cart 2.0.1 ini terlihat adanya sebuah text yang bertuliskan *"Powered by CubeCart 2.0.1"*. Tulisan ini rasanya cukup unik sehingga pencarian sederhana dengan memasukkan tulisan ini saja, hacker dengan mudah bisa mendapatkan puluhan bahkan ratusan calon korban.

Mendapatkan File "Biang Kerok"

Penjahat hanya membutuhkan sebuah pintu masuk untuk menguasai seluruh rumah Anda. Hanya dengan modal permasalahan pada sebuah file, hacker bisa menguasai seluruh jaringan komputer yang Ada. Masalah semacam ini kerap terjadi karena itu, teknik yang populer digunakan dari dulu sampai sekarang adalah menemukan keberadaan file yang bermasalah ini.

Sebagai contoh, andaikan file `/cgi-bin/userreg.cgi` diketahui mempunyai permasalahan yang memungkinkan hacker memasukkan perintah kedalamnya sehingga bisa menguasai komputer korban, hacker bisa memanfaatkan google dalam menemukan file ini. Dengan perintah seperti *"inurl:/cgi-bin/userreg.cgi"*, google akan menemukan file `userreg.cgi` yang berada didalam direktory `/cgi-bin/`.

Tentu saja, keberadaan file yang dicari ini belum tentu menunjukkan file yang sama seperti yang Anda cari. Bisa saja, nama file yang sama namun isinya berbeda atau ternyata file yang dimaksud



ternyata telah memiliki versi update yang telah memperbaiki permasalahan yang ada. Anda tidak bisa mengharapkan google dalam hal ini karena google tidak bisa membedakan versi file.

Mencari Pesan Kesalahan

Pesan kesalahan atau yang dikenal dengan *error message* biasanya menunjukkan adanya permasalahan serius, yang tidak tertangani dengan baik oleh web developer yang artinya pula ada kemungkinan terbukanya pintu yang bisa digunakan oleh hacker dalam melakukan penerobosan. Tidak jarang, pesan kesalahan yang tidak dikonfigurasi dengan baik akan menampilkan informasi-informasi penting yang tidak seharusnya diketahui oleh umum. Selain itu, pesan kesalahan juga bisa digunakan untuk mencari sebuah sistem tertentu karena setiap aplikasi, biasanya memiliki ciri khas pesan kesalahan yang berbeda dengan aplikasi lainnya.

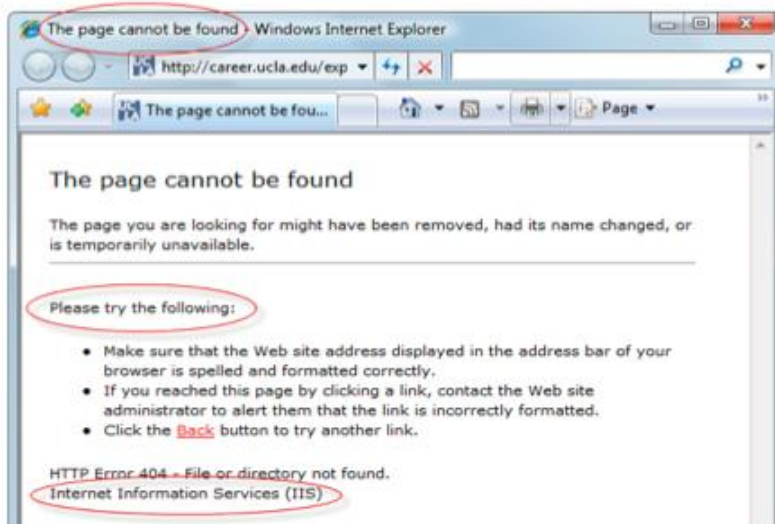
Sebagai contoh, IIS (*Internet Information Services*), web server buatan Microsoft secara default akan menampilkan sebuah pesan kesalahan bila halaman yang diminta oleh pengunjung ternyata tidak tersedia. Pesan kesalahan yang ditampilkan ini sebenarnya diambil oleh IIS dari file html yang telah disediakan secara default saat instalasi IIS dilakukan dan sangat jarang dirubah oleh web admin.

File yang ditampilkan saat error terjadi ini disimpan didalam direktory `%systemroot%\help\iishelp\common\` dan diberikan nama sesuai dengan kode error yang terjadi seperti file `400.htm` untuk menampilkan kode error 400 yang menandakan '*File not found*', file `401.1.htm` untuk menampilkan kode error 400.1 yang menandakan '*You are not authorized to view this page*', dan lain sebagainya.

Seperti yang telah saya jelaskan sebelumnya, inti dari google hacking adalah menemukan keunikan dari setiap halaman yang hendak dicari, suatu tanda yang tidak dimiliki oleh halaman yang tidak berhubungan lainnya. Semakin Anda mampu menemukan keunikan dari halaman yang hendak Anda cari, semakin tepat pula google menampilkan hasil pencariannya.

Sekarang, mari kita lihat contoh halaman error yang ditampilkan oleh web server IIS dari Microsoft ini (Anda juga bisa melihat halaman

error ini langsung dengan membuka file kode error yang berada didalam direktory `%systemroot%\help\iishelp\common\`). Pada title terdapat tulisan *The page cannot be found* yang tampaknya cukup unik untuk digunakan. Pada halaman error, kata *Please try the following* dan adanya tulisan *Internet Information Services* yang bila digunakan bersama-sama tentunya akan semakin membuat pencarian halaman error ini semakin tepat.



Syntax lengkap untuk melakukan pencarian halaman error untuk menemukan webserver IIS ini bisa ditulis dengan `intitle:"The page cannot be found" "please * * following" "Internet * Services"`.



Memfaatkan halaman error untuk menemukan jenis webserver

yang digunakan hanyalah satu dari sekian banyak teknik yang digunakan. Hacker juga bisa menemukan aplikasi yang bisa dimasuki berdasarkan pesan kesalahan yang ditampilkan. Cara atau teknik yang digunakan tetaplah sama. Amati keunikan dari error yang hendak dimanfaatkan dan gunakan keunikan ini untuk melakukan pencarian. Sebagai contoh, untuk melakukan pencarian pesan kesalahan yang ditampilkan oleh database oracle, bisa dilakukan dengan syntax **"ORA-00921: unexpected end of SQL command"**.

Mmm'mm Apakah kode-kode yang saya masukkan sudah semakin membingungkan Anda? Perlu penjelasan lebih lanjut atau membutuhkan syntax lainnya? Masih ingat dengan yang saya katakan pada awal bab ini? Google hacking diperkenalkan secara luas oleh Johny Long. Johny juga membuat sebuah database yang berisi kumpulan teknik-teknik pencarian yang telah dikelompokkan dengan sangat rapih. Anda bisa melihat syntax-syntax yang digunakan untuk mendapatkan password, informasi rahasia, jenis webserver, jenis aplikasi, situs yang bermasalah dengan SQL injection, XSS dan lain sebagainya. Silahkan kunjungi situs Johny Long di <http://johnny.ihackstuff.com/ghdb.php>

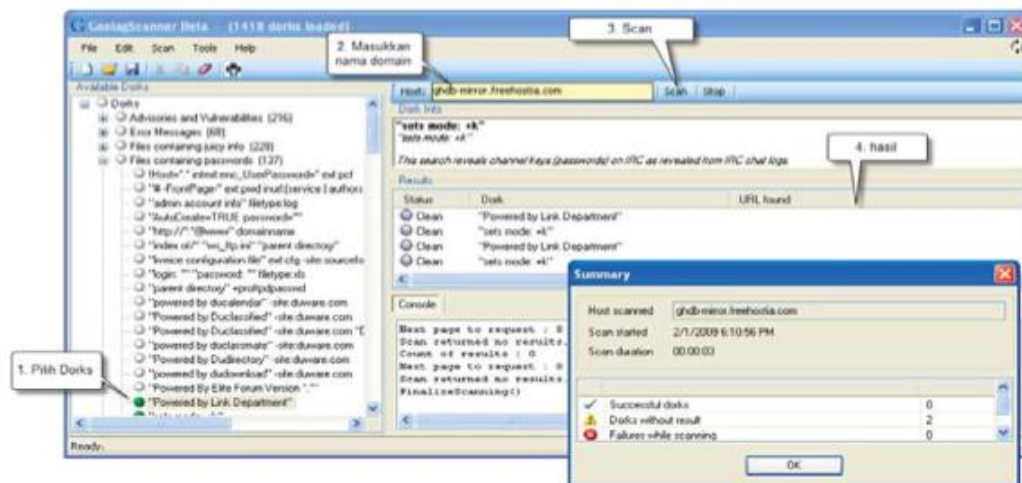


Google Hacking Database (GHDB) yang dikelola oleh Johny Long ini, selain digunakan oleh manusia, juga digunakan oleh program. Dengan bantuan dari program-program ini, proses *Google Hacking* menjadi semakin mudah dan cepat.

☯ Goolag Scanner

Group hacker yang sempat membuat heboh dengan software trojan *Back Orifice* kini kembali membuat sebuah software yang sangat menarik yang dinamakan dengan nama *GoolagScanner*. *GoolagScanner* adalah software pencari informasi berharga atau kelemahan situs dengan memanfaatkan teknik *Google Hacking*.

Software yang tampaknya kurang mendapatkan perhatian dan update ini membutuhkan *.Net Framework 2.0* untuk bekerja. Jadi bila Anda menggunakan sistem operasi dibawah windows Vista, Anda perlu mendownload *.Net Framework* dari situs Microsoft dan menginstalnya terlebih dahulu sebelum bisa menggunakan software ini. Untuk menggunakan software ini, caranya cukup mudah. Anda tinggal memilih *Dorks* yang tersedia pada kolom sebelah kiri (1), kemudian memasukkan nama domain yang hendak dicek pada kolom *host* (2) dan mengklik tombol *Scan*.

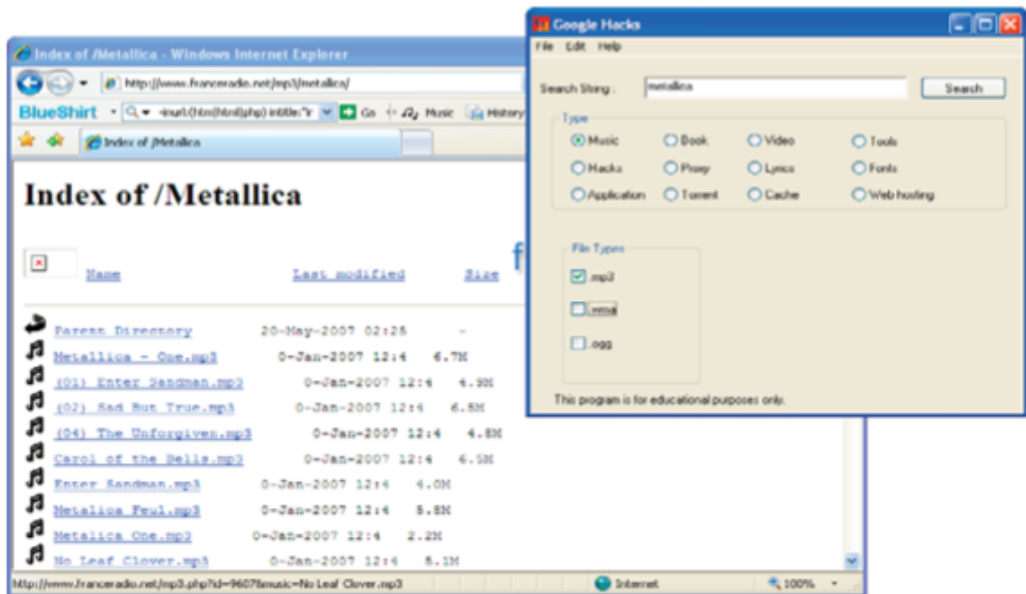


Pada saat saya mencoba menggunakan software ini, hasil yang didapatkan sangat mengecewakan karena software ini ternyata tidak mampu memanfaatkan teknik *google hacking* dengan baik. Walaupun secara manual google mampu menemukan informasi berharga dari sebuah website, dengan tools ini ternyata informasi tersebut tidak ditemukan. Bisa jadi, hal ini terjadi karena software yang masih dalam versi beta. Selain itu, bila Anda melakukan pencarian dengan memilih *Dorks* yang terlalu banyak, google akan melakukan proteksi

terhadap pencarian Anda karena dianggap Anda memiliki maksud jahat (tidak benar bukan?)

☾ Google Hack

Anda pasti menyukai tools yang satu ini. Dengan memanfaatkan teknik google hacking, tools yang diberikan nama *Google Hacks* ini bisa Anda dapatkan secara gratis melalui situs *code.google.com/p/googlehacks/* atau Anda juga bisa mendapatkannya di dalam CD yang disertakan bersama dengan buku ini. Tools ini akan membantu Anda dalam melakukan pencarian “barang-barang” berharga di Internet seperti buku, musik, video, dan lain sebagainya. Anda tinggal memasukkan kata kunci dan memilih apa yang akan Anda cari kemudian mengklik tombol *Search*.



Sebagai contoh, saya memasukkan kata group band rock *Metallica* dan memilih type music dengan type file *.mp3*. Setelah mengklik tombol *Search*, browser yang saya gunakan segera menampilkan ratusan link ke alamat-alamat URL yang memiliki file lagu mp3 dari group band *Metallica*. Dengan mudah, saya bisa mendapatkan lagu-lagu kenangan yang saya inginkan dengan mudah (ingat, tindakan ini adalah illegal karena file mp3 dilindungi oleh hak cipta).

Type file yang ditampilkan oleh tools *Google Hacks* ini tidaklah selalu sama karena tergantung pada apa yang Anda cari. Misalnya, Anda melakukan pencarian *Aplikasi*, maka jenis file yang akan ditampilkan sebagai pilihan adalah “.exe”, “.zip”, “.rar”, dll. Bahkan, terdapat juga jenis pencarian yang tidak memerlukan informasi type file seperti Fonts. Dengan tools ini, mencari file-file menarik bisa dilakukan dengan mudah tanpa harus menghafal syntax pencarian google hacking yang terkadang membingungkan.

Module 4

Scanning

Setelah mendapatkan informasi awal dari proses *Footprinting*, hacker akan melanjutkan aksinya dengan mencari informasi yang lebih detail lagi mengenai korban. Pada tahapan ini, hacker akan menggunakan berbagai cara untuk memastikan berbagai informasi teknis mengenai korban seperti sistem operasi yang digunakan, port apa saja yang terbuka, software yang digunakan, dlsb. Dengan mengetahui berbagai informasi yang lebih detail ini, hacker akan memiliki banyak pilihan yang bisa digunakan untuk melakukan penerobosan. Tentu saja, hacker akan memilih jalan yang paling mudah dan aman untuk digunakan.

Scanning adalah proses lanjutan dari *Information gathering* atau pengumpulan informasi dimana pada bagian ini, kita akan membahas tentang tahapan ke 3 sampai dengan tahapan ke 7 yaitu Mencari komputer yang aktif, Mencari port yang terbuka dan keberadaan Access Point, OS Fingerprinting, Fingerprinting services dan Mapping the network.

Setelah melalui proses scanning, hacker sudah memahami informasi teknis mengenai korban. Dengan informasi teknis ini, pintu-pintu yang ada sudah diketahui, apakah bisa dimasuki atau tidak. Bila terdapat kelemahan, hacker tinggal melakukan langkah kecil saja untuk menguasai komputer korban. Scanning bisa dibagi menjadi 3 jenis yaitu :

1. Port Scanning
2. Network Scanning
3. Vulnerability Scanning

1. Port Scanning

Port ibaratnya adalah pintu. Anda harus membuka pintu agar bisa keluar ataupun agar tamu bisa masuk ke rumah Anda. Tidak mungkin membuka sebuah toko yang pintunya tertutup, demikian juga halnya, tidak mungkin memberikan suatu layanan publik seperti web server, ftp server, mail server, dll tanpa membuka suatu port.

Untuk mencari ataupun melihat apakah suatu port terbuka atau tidak sangatlah mudah. Anda bisa menggunakan cara setengah manual ataupun menggunakan cara yang lebih otomatis dan cepat. Cara manual yang saya maksudkan di sini adalah menggunakan program telnet.

Telnet adalah sebuah program emulasi terminal. Jadi seakan-akan Anda menggunakan sebuah terminal, yang berbentuk hanya berupa monitor dan keyboard pada jamannya AS400. Terminal yang dinamakan dump terminal ini terkoneksi ke mesin lain seperti AS400 dan menjalankan perintah-perintah yang disediakan oleh sang server.

Sebagai contoh, untuk memeriksa apakah port 80 terbuka atau tidak pada sebuah komputer, Anda bisa menjalankan perintah :

```
C:\>Telnet www.Jasakom.com 80
```

Jika Anda mendapatkan layar hitam, artinya port 80 tersebut terbuka. Jika port yang Anda telnet tidak terbuka, Anda akan mendapatkan pesan time out atau pesan kegagalan koneksi seperti berikut ini :

```
C:\>telnet www.Jasakom.com 80
Connecting To www.Jasakom.com...Could not open connection to
the host, on port 8
1: Connect failed
```

Untuk mencari port-port lain, misalkan Anda ingin melihat apakah trojan yang menggunakan port 12345 terbuka atau tidak, Anda tinggal mengetikkan perintah **telnet www.Jasakom.com 12345**. Mencari port yang terbuka dengan telnet memang mudah dan sederhana karena bisa dikatakan semua sistem operasi telah mengikut sertakan program telnet ini sehingga Anda tidak perlu lagi melakukan instalasi ataupun mencarinya kemana-mana.

Lalu bagaimana jika Anda ingin mencari semua port yang mungkin terbuka pada sebuah komputer atau pada banyak komputer sekaligus? Telnet ke semua port satu persatu (antara 1-65535) memang memungkinkan, namun melelahkan terlebih ada cara yang lebih mudah untuk dilakukan yaitu dengan program *Port Scanner*.

2. Network Scanning

Masih ingat dengan kasus yang pernah terjadi pada situs Jasakom? Hacker menyerang dari komputer lain sebagai perantara untuk mengakses server yang digunakan oleh situs Jasakom. Sebuah jaringan biasanya saling terkait dan komputer didalam jaringan ini biasanya saling percaya dengan keamanan yang lebih rendah. Bila dirumah Anda memiliki 2 komputer yang saling terhubung, password apa yang Anda gunakan untuk sharing folder? Sebagian besar mengatakan mereka tidak akan menggunakan password sama sekali. Dengan memasuki salah satu komputer didalam jaringan ini, hacker bisa mendapatkan komputer yang lain dengan lebih mudah. Jadi daripada mendobrak pintu utama yang terbuat dari baja, kenapa tidak mencari pintu tetangga yang terbuat dari kertas ?

Network Scanning akan mencari host atau komputer-komputer yang aktif pada sebuah jaringan. Semakin banyak komputer aktif yang bisa diketahui, akan semakin memudahkan hacker dalam melakukan penyerangan karena hacker hanya membutuhkan 1 pintu masuk sementara korban harus menjaga beberapa, puluhan atau bahkan ratusan pintu yang terbuka.

3. Vulnerability Scanning

Vulnerability Scanning merupakan scanning yang bertujuan menemukan kelemahan dari sebuah sistem. Dengan mengetahui *Vulnerability* atau kelemahan yang ada, hanya tinggal langkah kecil untuk memiliki atau memasuki komputer korban. Jika Anda lihat ke situs-situs yang meng-informasikan kelemahan software yang berhasil ditemukan seperti *secunia.com/product*, *www.hackerstorm.com*, *www.securiteam.com*, dll, terdapat ribuan kelemahan yang ada dan setiap harinya terdapat tambahan puluhan informasi baru.

Hacker bisa mencoba satu-persatu permasalahan yang diketahui namun mencoba satu-persatu dengan jumlah kelemahan yang mencapai ribuan ini, akan menjadi pekerjaan yang maha berat dan membutuhkan waktu yang lama sekali. Dengan software *Vulnerability Scanning*, pekerjaan pengecekan ini hanya membutuhkan waktu yang sangat singkat, dan mudah.

Hampir semua konsultan security memanfaatkan software *Vulnerability Scanning* untuk membantu pekerjaan mereka. Beberapa software *Vulnerability Scanning* ini juga mampu menghasilkan laporan dengan format yang sangat bagus sekali sehingga disukai oleh para top manager perusahaan.

IDS (Intrusion Detection System) merupakan software yang digunakan untuk mendeteksi usaha serangan hacker dan produk ini biasanya mampu mendeteksi aktifitas scanning, baik port, network maupun vulnerability scanning. IDS juga bisa memblok host yang melakukan aktifitas yang dianggap bisa membahayakan jaringan yang dijaga, walaupun tidak semua serangan bisa dicegah oleh IDS namun setidaknya software ini sangat membantu dalam hal pencegahan serangan hacker.

Metodologi Scanning

Ada beberapa bentuk scanning, mana yang sebaiknya dilakukan terlebih dahulu? Apa yang dilakukan oleh hacker setelah melakukan scanning? Sertifikasi CEH mendeskripsikan 7 tahapan scanning atau metodologi scanning sebelum hacker melakukan penyerangan yaitu:

1. Mencari System Yang Aktif
2. Mencari Port yang Terbuka
3. Mengidentifikasikan Services
4. Banner grabbing / OS Fingerprinting
5. Vulnerability Scanning
6. Menggambarkan diagram network dari host yang bermasalah (Vulnerable hosts)
7. Menyiapkan proxy

1. Mencari System yang aktif

Cara yang paling mudah untuk mencari host atau komputer yang aktif adalah dengan perintah *ping* yang tersedia di semua sistem operasi yang saya kenal. *Ping* yang dibuat pertama kali oleh *Mike Muuss* pada akhir tahun 1983 ini akan mengirimkan sebuah paket ICMP *Echo Request* dan komputer yang menerima paket ping ini kemudian akan mengirimkan paket ICMP *Echo Response* kembali.

Apabila komputer yang dikirimkan paket tidak ada atau tidak dihidupkan, komputer tidak akan mendapatkan respon apa-apa atau terjadi time out. Perintah ping bisa dijalankan dengan parameter nama komputer seperti XYZ, nama domain seperti *www.jasakom.com* atau dengan alamat IP seperti 116.68.160.34.

Mike Muuss, penulis program ping pertama kali pada tahun 1983 menamakan programnya dengan *ping* karena terinspirasi dengan cara kerja sonar kapal selam yang akan memberikan bunyi ping ketika menemukan suatu benda. Belakangan, *David L. Mills* memberikan backronym, dengan menyatakan Ping sebagai singkatan dari *Packet InterNet Grouper (Groper)* yang terkadang juga dikenal sebagai *Packet Inter-Network Groper*.

Sebagai contoh, untuk memeriksa apakah situs *www.jasakom.com* sedang aktif atau tidak dengan perintah ping (Start⇒Run⇒cmd) :

```
C:\>ping www.jasakom.com
Pinging www.jasakom.com [116.68.160.34] with 32 bytes of data:
Reply from 116.68.160.34: bytes=32 time=63ms TTL=58
Reply from 116.68.160.34: bytes=32 time=76ms TTL=58
Reply from 116.68.160.34: bytes=32 time=95ms TTL=58
Reply from 116.68.160.34: bytes=32 time=57ms TTL=58
Ping statistics for 116.68.160.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 57ms, Maximum = 95ms, Average = 72ms
```

Terlihat bahwa situs *jasakom* memberikan reaksi berupa adanya reply yang menunjukkan bahwa situs atau server *jasakom* ini dalam kondisi aktif/hidup. Hasil yang sama saya dapatkan ketika mengecek situs *www.kompas.com*.

Perintah ping memang efektif untuk mengecek aktif atau tidaknya sebuah komputer namun menjalankan perintah ping untuk memeriksa banyak komputer sekaligus, akan menghabiskan banyak waktu dan tidak efisien.

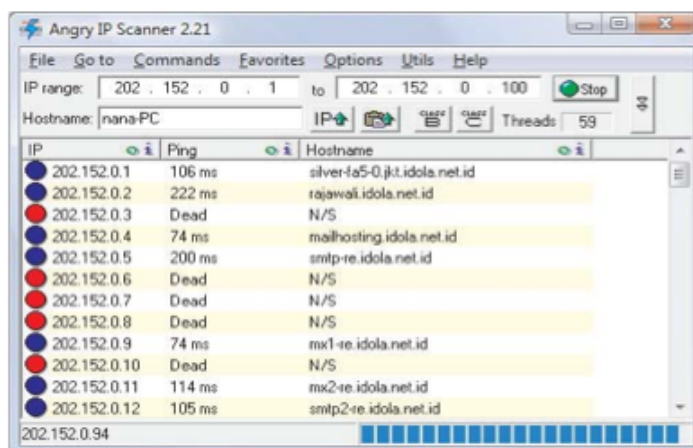
Ping Sweep atau yang sering dinamakan juga dengan **ICMP Sweep** adalah proses pengecekan alamat IP dalam jumlah banyak untuk menentukan host yang aktif. Caranya adalah dengan mengirimkan paket ICMP sama seperti perintah ping namun dilakukan dalam jumlah banyak dan dalam waktu bersamaan agar proses pengecekan menjadi jauh lebih cepat dan efisien.

Beberapa program yang mampu melakukan *Ping Sweep* ini diantaranya adalah *Ping Sweep* dari *www.solarwinds.net*, *Angry IP Scanner*, *fping*, *gping*, *nmap*, *pinger*, *WS_Ping_ProPack*, *Network scan tools*, *Super Scan*, dll.

☯ Angry IP Scanner

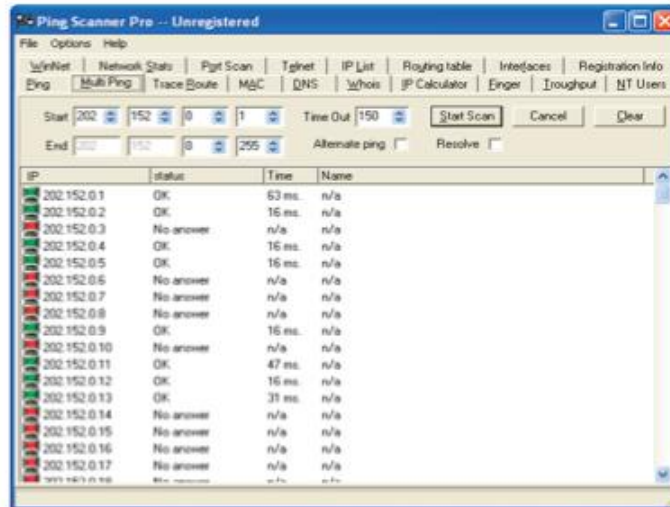
Angry IP Scanner misalnya, mampu mengecek ratusan komputer dalam waktu beberapa detik saja. Anda tinggal memasukkan alamat IP awal dan alamat IP akhir yang ingin dicek dan *Angry IP Scanner* akan melakukan pengecekan secara berurutan dimana alamat IP yang aktif akan ditandai dengan icon warna biru tua sedangkan alamat host yang tidak aktif akan ditandai dengan icon warna merah.

Angry IP Scanner juga menunjukkan kepada Anda waktu yang dibutuhkan untuk melakukan Ping sehingga Anda bisa menentukan kualitas koneksi Anda, selain itu, *Angry IP Scanner* juga akan me-resolve secara otomatis Hostname dari alamat IP yang bisa Anda lihat pada kolom 'Hostname'.



🕒 Ping Scanner Pro

Software ping sweep lainnya adalah *Ping Scanner Pro* (www.digilextechnologies.com) yang mempunyai banyak utility kecil lainnya selain fungsi ping sweep yang bisa didapatkan dari tabulasi *Multi Ping*. Fungsi ping sweep yang ditawarkan oleh *Ping Scanner Pro* bisa dikatakan sama dengan *Angry IP Scanner* dimana Anda bisa melihat *hostname* dari suatu alamat IP namun Anda perlu memberikan tanda centang pada pilihan *Resolve* terlebih dahulu.



Sebelumnya saya katakan bahwa icon merah yang ditunjukkan oleh *Angry IP Scanner* maupun *Ping Scanner Pro* menunjukkan bahwa alamat IP tersebut tidak aktif. Sebenarnya, hal ini tidaklah sepenuhnya benar. Ketika saya mencoba ping ke alamat *www.Microsoft.com*, ternyata hasil negatif yang diberikan padahal, jelas situs *www.Microsoft.com* sedang aktif :

```
C:\>ping www.Microsoft.com
Pinging lb1.www.ms.akadns.net [207.46.19.254] with 32 bytes of
data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 207.46.19.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Apa yang terjadi ? Beberapa penjahat cyber, mengganggu komputer yang ada di internet dan membuat komputer yang aktif tumbang tak berkutik. *Worm Welchia* misalnya, memanfaatkan ping (paket ICMP) untuk melakukan gangguan host yang ada di Internet. Akibatnya, banyak yang mulai melakukan pemblokiran terhadap paket ICMP sehingga perintah ping tidak bisa dijalankan lagi. Akibatnya seperti yang Anda lihat pada situs detik.com, dimana komputer tidak akan merespon perintah ping walaupun komputer tersebut aktif.

Windows XP Service Pack 1 dan Windows Vista misalnya, secara default juga telah memblokir paket ICMP sehingga perintah ping tidak bisa digunakan lagi untuk menentukan aktif tidaknya sebuah komputer. Metode lain yang bisa digunakan untuk menentukan apakah sebuah komputer sedang aktif atau tidak adalah dengan port scanning yang akan kita bahas selanjutnya.

IDS biasanya digunakan untuk mendeteksi kemungkinan serangan dari hacker termasuk aktifitas Ping Sweep yang merupakan tanda-tanda adanya kemungkinan serangan. Snort adalah salah satu IDS Open Source yang sangat terkenal dan mampu mendeteksi adanya aktifitas Ping Sweep ini.

2. Mencari Port yang terbuka

Sebelum menjelaskan lebih detail tentang metodologi yang digunakan ini, akan sangat membantu bila Anda memahami sedikit komunikasi protokol TCP. Penjelasan ini memang sedikit “low level” dan teknis namun tanpa memahami ini, Anda tidak akan mungkin bisa memahami bermacam-macam teknik yang digunakan dalam metodologi ini.

Penjelasan mengenai komunikasi TCP ini sebenarnya telah saya lakukan pada buku “**Seni Teknik Hacking 2**” dan karena tidak semua orang yang membeli buku ini memiliki buku STH-2, saya akan menjiplak sebagian isi buku tersebut disini :

Apa itu TCP dan Sequence Number dalam TCP ?

Pada saat komputer A melakukan komunikasi dengan komputer B,

maka secara otomatis akan ada pengiriman data dari komputer A ke B dan sebaliknya. Pengiriman data ini menggunakan kurir yang dinamakan TCP. TCP-lah yang mengatur dan membuat aturan tentang bagaimana paket-paket tersebut harus diantar ke komputer tujuan dan memastikan data yang dikirim bisa diterima dengan baik.

Kamar tidur saya adalah kamar yang cukup kecil, pintunya pun cukup imut. Ketika saya membeli sebuah meja belajar, meja tersebut terlalu besar untuk dimasukkan melalui pintu yang ada. Akhirnya apa yang terjadi? tidak, saya tidak bisa mengembalikan meja tersebut karena bentuknya yang saya sukai dan terlebih lagi saya pula yang merancangnya. Akhirnya, meja tersebut dilepaskan menjadi bagian-bagian kecil, kemudian diberi nomor. Bagian-bagian kecil ini, saya memasuk satu persatu ke dalam kamar dan merakitnya kembali menjadi meja.

Bagaimana saya merakitnya kembali? berdasarkan penomoran yang telah saya berikan sebelumnya. Saya juga memberikannya nomor secara berurutan agar saya bisa mengetahui apabila ada bagian yang kurang atau hilang.

Paket TCP, bekerja dengan cara yang sama seperti yang telah saya lakukan. Suatu data yang besar, tidak bisa dikirim secara sekaligus, namun harus dipecah menjadi beberapa paket yang lebih kecil. Paket kecil ini kemudian diberikan nomor urut yang dinamakan *sequence number*. Tujuan dari *sequence number* ada dua yaitu *reliability* dan *error recovery*. Dikatakan *reliable* atau bisa dipercaya karena adanya konfirmasi penerimaan.

Misalnya komputer A mengirimkan paket dengan *sequence number* 10 kepada komputer B. Pada saat paket tersebut telah diterima, komputer B akan mengatakan kepada komputer A "hei komputer A, saya telah menerima paket dengan *sequence number* 10".

Dengan cara seperti ini, komputer A akan mengetahui bahwa paket nomor 10 yang dikirimkannya telah tiba dengan selamat di komputer tujuan.

TCP juga dikatakan memiliki kemampuan *error recovery* atau memperbaiki permasalahan yang terjadi karena TCP mampu mendeteksi paket yang hilang atau rusak.

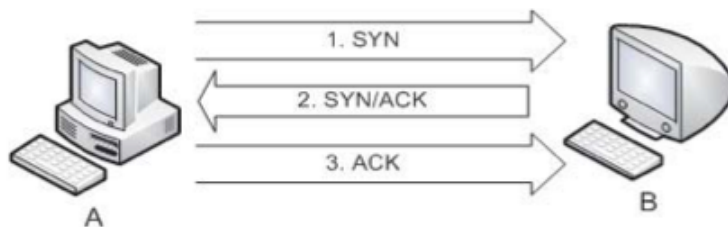
Misalnya, komputer A mengirimkan paket dengan *sequence number* 10 kepada komputer B. Setelah ditunggu-tunggu, komputer B tidak menginformasikan bahwa dirinya telah menerima paket dengan *sequence number* 10. Oleh karena itu, komputer A mengetahui bahwa paket dengan *sequence number* 10 telah rusak atau hilang diperjalanan sehingga perlu di kirim ulang ke komputer B.

Dengan bantuan *sequence number* inilah, tidak perlu dilakukan pengiriman ulang semua paket namun hanya paket yang hilang atau rusak. Paket-paket yang telah diterima oleh komputer B, selanjutnya akan dirakit kembali menjadi sebuah data yang utuh berdasarkan *sequence number* sama seperti saya merakit potongan-potongan kayu menjadi sebuah meja kembali.

Mungkin dulu waktu TCP di rancang, idenya juga berasal dari merakit meja. who knows?

Three Way Handshake

Jangan pikir sopan santun hanya milik manusia. Protokol komunikasi-pun menggunakan konsep sopan santun agar komunikasi bisa berjalan dengan baik dan lancar. Pada saat komputer yang menggunakan protokol TCP / IP hendak memulai komunikasi, terdapat tahapan awal yang sangat penting yang harus dilakukan yaitu yang dinamakan sebagai *three way handshake* atau jabatan tangan tiga kali. Perhatikan ilustrasi berikut :



Sebelum komputer “A” dan komputer “B” bisa berkomunikasi, mereka harus membuat beberapa kesepakatan terlebih dahulu yang dikenal dengan *Three Way Handshake*. Kesepakatan apa yang dilakukan oleh kedua mesin itu ?

1. Paket pertama yang dikirimkan oleh komputer A adalah paket yang dinamakan sebagai paket SYN, yang berasal dari singkatan

'synchronize sequence numbers'. Tujuan dari paket SYN, sesuai dengan namanya adalah men-sinkronkan atau menyamakan nomor Sequence Number. Jadi komputer A membuat sebuah nomor secara acak, misalnya 1000 dan memberitahukannya kepada komputer B. Komputer A mengatakan kepada komputer B, "Hei komputer B, paket dari saya akan dimulai dari kode 1000. Jangan lupa yah". Jadi pada tahap ini, komputer B sudah mengetahui penomoran paket yang dikirim oleh komputer A dan mereka sepakat !

2. Komputer B yang mendapatkan paket dari komputer A, akan mengirimkan paket balasan ke komputer A yang dinamakan paket SYN/ACK. Dengan paket ACK (*Acknowledgement*) ini, komputer B mengatakan kepada komputer A "Hei komputer A, kata-kata Anda sudah saya terima dan saya mengerti, thanks ya". Lalu selain flag ACK, di dalam paket ini flag SYN juga diaktifkan. Dengan flag SYN ini, komputer B mengatakan kepada komputer A "Hei komputer A, paket kiriman dari saya akan dimulai dari angka 2000 deh". Angka 2000 ini ditentukan oleh komputer B secara acak, sama seperti penomoran pertama yang dilakukan oleh komputer A. Penomoran paket pertama ini dinamakan sebagai ISN atau *Initial Sequence Number*.
3. Selanjutnya, komputer A juga akan memberikan konfirmasi juga kepada komputer B agar komputer B yakin bahwa pesannya bisa diterima dengan baik. Komputer A akan mengirimkan paket ACK yang mengatakan "Ok komputer B, pesan Anda sudah saya terima dan saya juga sudah tau kalo paket dari kamu akan dimulai dari nomor 2000. Sip deh... "

Selanjutnya, komunikasi antara komputer A dan komputer B sudah bisa dilakukan. Ok, saya sudah menjelaskan sedikit mengenai fungsi dari flag SYN dan ACK dalam paket TCP namun sebenarnya tidak hanya flag SYN dan ACK yang ada. Flag di dalam paket TCP masih ada beberapa seperti FIN, RST, PSH dan URG.

Flag FIN (*Finish*) digunakan untuk mengakhiri komunikasi TCP, RST (*Reset*) digunakan untuk menutup koneksi yang abnormal, PSH (*Push*) bersama dengan URG (*Urgent*) biasanya digunakan untuk menandakan paket penting yang harus didahulukan.

Saya tidak menjelaskan dengan detail konsep komunikasi dan flag di dalam TCP ini karena membutuhkan banyak sekali penjelasan yang bakalan menghabiskan seluruh isi halaman buku ini. Bila Anda tertarik dengan penjelasan detail dari komunikasi ini, saya sarankan Anda untuk mempelajari khusus komunikasi paket TCP yang sangat menarik ini.

Saatnya Mencari Port Yang Terbuka

Saya telah menjelaskan kepada Anda bagaimana mencari port yang terbuka dengan program telnet. Mencari port yang terbuka dengan telnet memang mudah dan sederhana namun terkadang Anda tidak bisa melakukannya karena terproteksi oleh firewall dan lagipula, tindakan Anda mungkin akan dicatat oleh IDS yang bisa membahayakan nyawa/hidup Anda.

Hacker tidak kehilangan akal dan mencari berbagai teknik untuk mengalahkan firewall maupun IDS sehingga tetap bisa melakukan scanning.

Sebelum membahas lebih lanjut mengenai port scanner, masih ingatkah Anda dengan konsep *Three Way Handshake* bukan? Telnet akan membuat koneksi ke port yang terbuka dan pada saat itu, *Three Way Handshake* akan terjadi dengan sempurna. Ibaratnya, telnet akan mengetuk pintu komputer yang terbuka dan bersalaman dengan pemiliknya.

Cara ini tidak ada salahnya namun menimbulkan kecurigaan besar dan diketahui oleh satpam(IDS/Firewall). Karena itu, terdapat beberapa teknik yang digunakan oleh port scanning dalam melakukan pengecekan port agar tidak terdeteksi oleh korban dan agar bisa melewati proteksi firewall maupun IDS.

Pada saat menjelaskan tentang *Three Way Handshake*, saya telah menjelaskan kepada Anda tentang keberadaan flag di dalam paket TCP yaitu flag SYN dan flag ACK. Didalam paket TCP, terdapat total flag sebanyak 6 buah dan 2 buah flag yang belum digunakan jadi grand totalnya ada 8.

Dengan mempermainkan flag-flag inilah bisa tercipta berbagai teknik yang bisa digunakan untuk memperdaya firewall maupun

IDS. Jika Anda perhatikan, dengan total flag yang sebanyak 8, artinya bisa diciptakan 256 kombinasi. Pada bagian ini, saya hanya akan menjelaskan beberapa kombinasi yang sering digunakan.

1. TCP Connect scan

Ini adalah teknik yang digunakan oleh program telnet dimana koneksi dengan komputer korban terjadi dengan sempurna (*Three Way Handshake*) sehingga paling mudah terdeteksi.

2. TCP SYN scan

Teknik ini dikenal juga dengan nama *Half Open* karena *Three Way Handshake* tidak terjadi dengan sempurna. Anda mengetuk pintu namun buru-buru kabur ketika pemiliknya membuka pintu. Walaupun Anda kabur pada saat tuan rumah keluar, namun Anda sudah mengetahui bahwa ada orang dirumah.

Teknik ini akan mengirimkan paket SYN dan menunggu paket balasan dari komputer korban. Seandainya dijawab dengan paket SYN/ACK, artinya port komputer korban terbuka sedangkan paket RST/ACK menandakan port tertutup.

Pada koneksi normal (*Three Way Handshake*), komputer sumber harus mengirimkan lagi paket ACK namun paket ini tidak pernah dikirimkan sehingga dinamakan sebagai *Half Open*. Teknik ini sudah dikenal oleh IDS dan rata-rata IDS sudah mampu mendeteksinya namun biasanya tidak tercatat ke dalam log aplikasi.

3. TCP FIN scan

Teknik ini tidak memanfaatkan momen saat terjadinya koneksi TCP (*Three Way Handshake*) namun malah memanfaatkan momen saat suatu hubungan TCP diputuskan. Teknik ini akan langsung mengirimkan paket FIN (Finish) ke port korban. Anda mengatakan putus kepada seorang perempuan yang bukan pasangan Anda, aneh bukan? Tentu saja, tanpa mempunyai koneksi, permintaan pemutusan hubungan (Finish) sangatlah aneh namun ternyata teknik ini bisa digunakan.

Port yang tertutup akan mengembalikan paket RST sedangkan port yang terbuka akan mengabaikan paket ini dan dari sifat inilah, bisa diketahui apakah sebuah port sedang terbuka atau tertutup. Teknik

ini tidak berguna pada sistem operasi Windows karena Windows mengimplementasikan TCP dengan sifat yang berbeda dan baik port itu terbuka ataupun tertutup, Windows akan mengirimkan kembali paket RST (Teknik ini bisa juga digunakan untuk menentukan apakah sistem operasi korban adalah windows atau bukan).

4. TCP NULL scan

Paket TCP mempunyai flag atau kode-kode didalam paket TCP namun apa jadinya bila sebuah paket dikirimkan tanpa flag apapun? Jika sistem operasi mengimplementasikan aturan dari RFC 793, maka port yang tertutup akan mengembalikan paket RST sedangkan port yang terbuka tidak akan mengembalikan apa-apa.

5. TCP ACK scan

Teknik ini menggunakan TCP ACK untuk menentukan apakah sebuah server aktif atau tidak dengan cara mengirimkan paket TCP dengan flag ACK yang diset dengan nomor port. Teknik ini terutama digunakan terhadap host yang tidak merespon ping. Jika komputer korban aktif, paket TCP RST akan dikirimkan oleh komputer korban sebagai balasan.

6. TCP XMAS scan

Apa yang Anda temui ketika natal tiba? Benar, gemerlap lampu natal dimana-mana. Teknik ini akan mengirimkan paket TCP dengan menyalakan flag FIN, URG dan PSH. Port yang tertutup akan mengembalikan paket RST sedangkan port yang terbuka akan mengabaikan paket ini. Dari sifat inilah, bisa diketahui apakah sebuah port sedang terbuka atau tertutup. Teknik ini tidak berguna pada sistem operasi Windows karena Windows mengimplementasikan TCP dengan sifat yang berbeda dan baik port itu terbuka ataupun tertutup, Windows akan mengirimkan kembali paket RST.

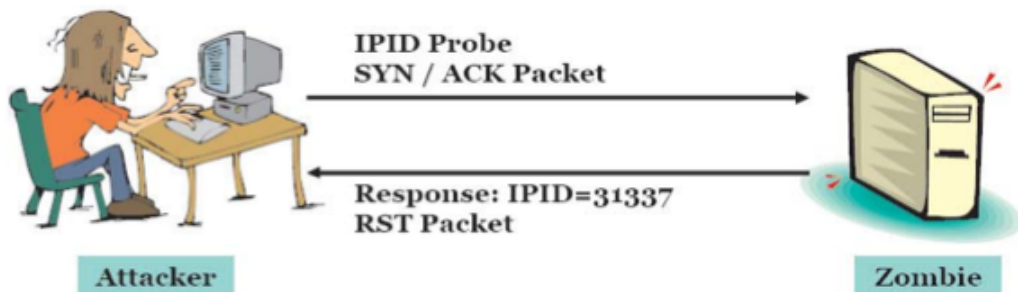
7. IDLE Scan

Teknik yang sangat menarik dan inovatif ditemukan oleh seorang peneliti bernama *Antirez*. Teknik ini dikatakan menarik karena memungkinkan hacker melakukan scanning tanpa meninggalkan jejak-nya sendiri, hanya jejak komputer yang dijadikan kambing

hitam. Saya akan menjelaskan ini dengan ilustrasi yang saya dapatkan dari slide presentasi CEH dari EC-Council (EC-Council sendiri tampaknya mengambil keterangan dan mempercantik gambar dari situs <http://insecure.org/nmap/idlescan.html>)

Langkah pertama, hacker akan mencari sebuah komputer zombie atau sebuah komputer yang akan dijadikan sebagai “kambing hitam”. Hacker kemudian akan mengirimkan sebuah paket SYN/ACK kepada komputer zombie (perantara) dan karena tidak ada permintaan komunikasi sebelumnya, komputer zombie akan mengirimkan paket RST.

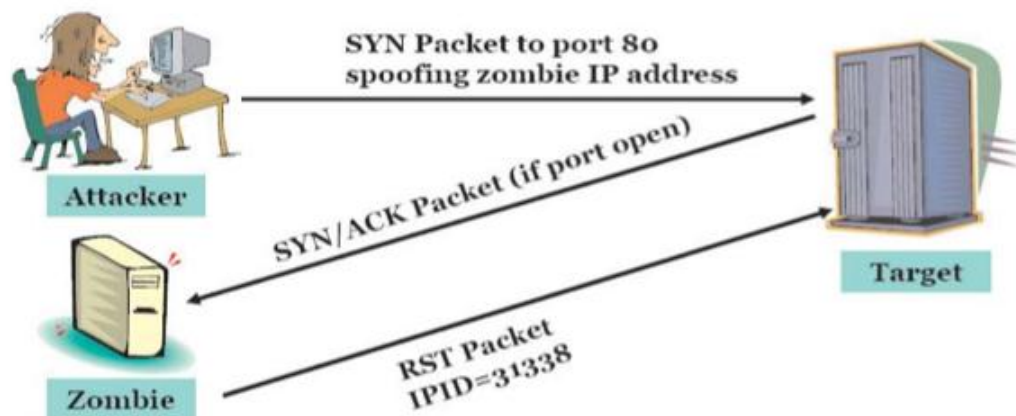
Didalam paket RST ini terdapat nomor IPID yang memberikan kode setiap paket yang dikirimkan. Hacker akan mencatat nomor IPID yang didapatkan ini. Sekarang kita asumsikan nomor ini adalah 31337.



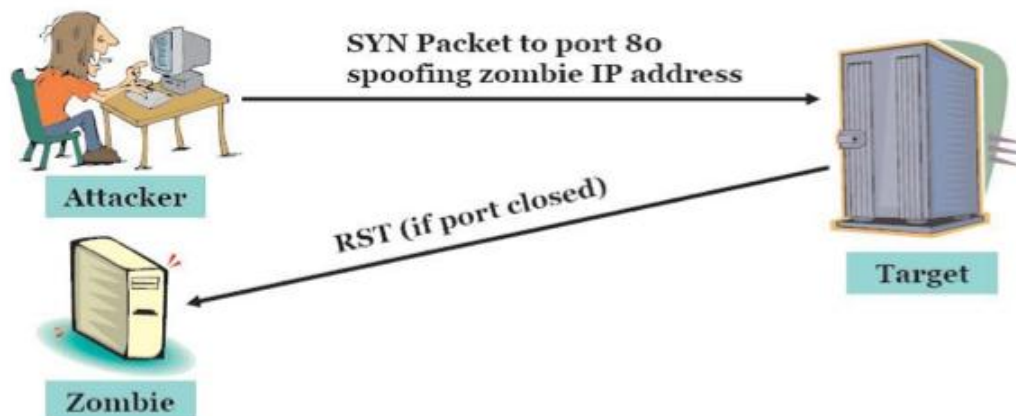
Tahap berikutnya, hacker akan mengirimkan paket TCP SYN kepada komputer korban pada port 80 namun dengan memalsukan alamat IP tersebut seakan-akan paket tersebut berasal dari komputer zombie (dengan merubah source IP dalam paket TCP). Komputer korban yang mendapatkan paket ini tidak akan menyadari bahwa paket yang diterimanya adalah paket palsu dan akan mengirimkan balasan berupa paket SYN/ACK ke komputer zombie.

Apabila port 80 pada komputer korban terbuka (open), maka komputer korban akan mengirimkan paket SYN/ACK kepada komputer zombie. Tentu saja komputer zombie akan kaget karena dirinya tidak pernah melakukan koneksi ke komputer korban sehingga ia akan mengirimkan paket RST kepada komputer korban yang akan mengatakan kepada komputer korban “Hei, apa-apaan sih kamu ? saya tidak mempunyai koneksi apapun dengan Anda.

Nih saya kirimkan paket reset untuk memutuskan hubungan ini". Di dalam paket RST ini terdapat kode IPID yang akan bertambah untuk setiap paket TCP yang dikirimkan. Sebelumnya nomor IPID ini adalah 31337 karena itu, diasumsikan sekarang nilainya akan bertambah dan menjadi 31338.

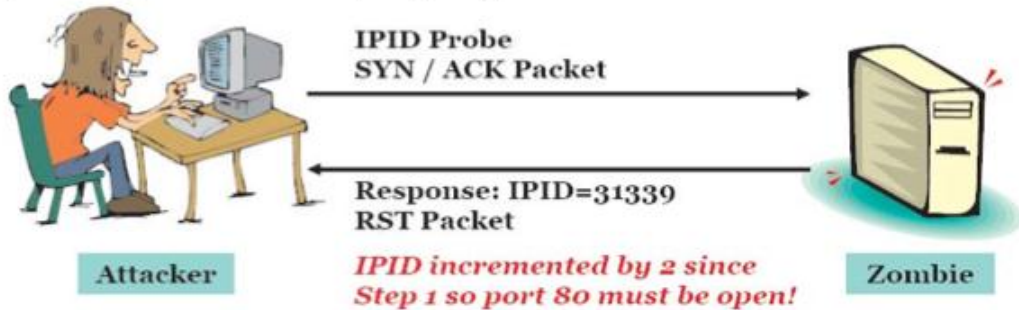


Lalu bagaimana bila komputer korban tidak membuka port 80 atau port 80-nya dalam keadaan tertutup (closed)? Komputer korban yang menerima paket SYN akan kebingungan dan mengembalikan paket RST (reset) kepada komputer zombie.



Kini, hacker tinggal mengecek nilai IPID dari komputer zombie untuk menentukan apakah port 80 pada komputer korban terbuka atau tidak. Jika nilai IPID bertambah 2, artinya port 80 pada komputer korban pastilah terbuka. Untuk mengecek nilai IPID pada komputer zombie, sekali lagi hacker akan mengirimkan paket TCP SYN/ACK

dimana hal ini akan menyebabkan komputer mengirimkan paket RST yang didalamnya terdapat nilai IPID (sama dengan langkah pertama). Suatu teknik yang sangat licik bukan ?



Banyak yang meragukan teknik yang dipaparkan oleh Antirez dan menganggapnya hanya teori belaka sehingga tidak mendapatkan banyak perhatian namun pada tahun 1999, teknik ini dibuktikan oleh LiquidK. Salah satu tools saat ini yang bisa digunakan untuk melakukan serangan ini adalah Nmap.

TCP adalah protokol yang reliable artinya dengan TCP, komputer bisa memastikan bahwa data yang ditransfer dari sumber ke tujuan, bisa berjalan dengan baik atau tidak. Sebelum berkomunikasi, TCP harus mengadakan ritual *three way handshake* dan pada saat pemutusan, juga harus melakukan ritual untuk itu. Hal ini tentu memberikan beban tambahan karena itu, ada protokol lain lagi yang digunakan yaitu UDP.

Protokol UDP adalah protokol yang tidak reliable karena protokol jenis ini tidak mengenal *three way handshake* dan bla..bla..bla lainnya. Akibatnya adalah UDP tidak menjamin data yang dikirimkan oleh komputer sumber, akan diterima atau tidak oleh komputer tujuan. Lalu untuk apa menggunakan protokol UDP? Karena kecepatan dan kesederhanaannya! Contoh penggunaan protokol ini adalah DNS.

Karena perbedaan sifat ini, untuk mengecek apakah port UDP terbuka atau tidak, mempunyai teknik yang berbeda dengan TCP yang telah kita bahas. Jika dengan TCP hacker banyak memainkan flag yang ada didalam paket TCP, tidak demikian halnya dengan UDP karena UDP tidak memiliki flag semacam ini. Satu-satunya harapan atau respon yang bisa digunakan adalah pesan kesalahan atau pesan penolakan.

Masih ingat dengan cara kerja UDP? Sebuah paket akan dikirimkan oleh komputer sumber setelah itu, masalahnya selesai. Komputer sumber tidak mengetahui apakah paket yang dikirimkan tersebut diterima atau tidak oleh komputer tujuan.

Satu-satunya harapan yang bisa digunakan adalah pesan kesalahan *Port Unreachable* yang terjadi ketika UDP komputer tujuan dalam keadaan tertutup (closed) namun apabila komputer tujuan memblokir paket ICMP dengan firewall, komputer sumber tidak akan mendapatkan pesan kesalahan apapun karena itu, men-scan port UDP menjadi lebih sulit.

Nmap

Teknik hacking yang sulit, ternyata tidak sulit untuk dilakukan berkat alat bantu yang tersedia di dalam dunia internet. Hal yang sama juga terjadi pada teknik scanning port yang telah kita bahas ini. Salah satu tools andalan dari para hacker ini adalah *nmap* yang dibuat oleh *Fyodor Yarochkin*.

Anda bisa mendapatkan nmap dari situsnya di *nmap.org* secara gratis. Sampai saat ini, tools andalan para hacker ini selalu di update dan untuk versi terbaru pada saat buku ini dibuat adalah 4.76. Nmap tersedia dalam berbagai versi, baik untuk windows, linux, Mac dan sistem operasi lainnya. Untuk melihat parameter apa saja yang ada pada nmap, Anda bisa mengetikkan perintah nmap tanpa menggunakan parameter dan menekan tombol [ENTER].

```
C:\nmap
Nmap 4.76 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, Microsoft.com/24, 192.168.0.1, 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO [protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
```

```
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
--traceroute: Trace hop path to each host
--reason: Display the reason a port is in a particular state
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
  directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in milliseconds, unless you append 's'
(seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T[0-5]: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <time>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
  probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
```

```
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP checksum

OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
    and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use twice or more for greater effect)
-d[level]: Set or increase debugging level (Up to 9 is meaningful)
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to
HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:
-6: Enable IPv6 scanning
-A: Enables OS detection and Version detection, Script scanning and
Traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.

EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

Seperti yang Anda lihat dari parameter-parameter yang ditampilkan, nmap adalah tools serbaguna dengan kemampuan yang sangat luas. Sebagai contoh, untuk melakukan scanning port dengan teknik *TCP Connect*, Anda tinggal menggunakan parameter **-sT** sedangkan untuk menggunakan teknik *Xmas Tree*, Anda tinggal menggunakan parameter **-sX**. Pada contoh ini, saya men-scan port-port yang terbuka pada host 192.168.0.1 dengan teknik TCP connect.

```
C:\>nmap -sT 192.168.0.1
Starting Nmap 4.75 ( http://nmap.org ) at 2008-09-11 15:04 SE
Asia Standard Time

Interesting ports on 192.168.0.1 (192.168.0.1):
Not shown: 978 closed ports
```



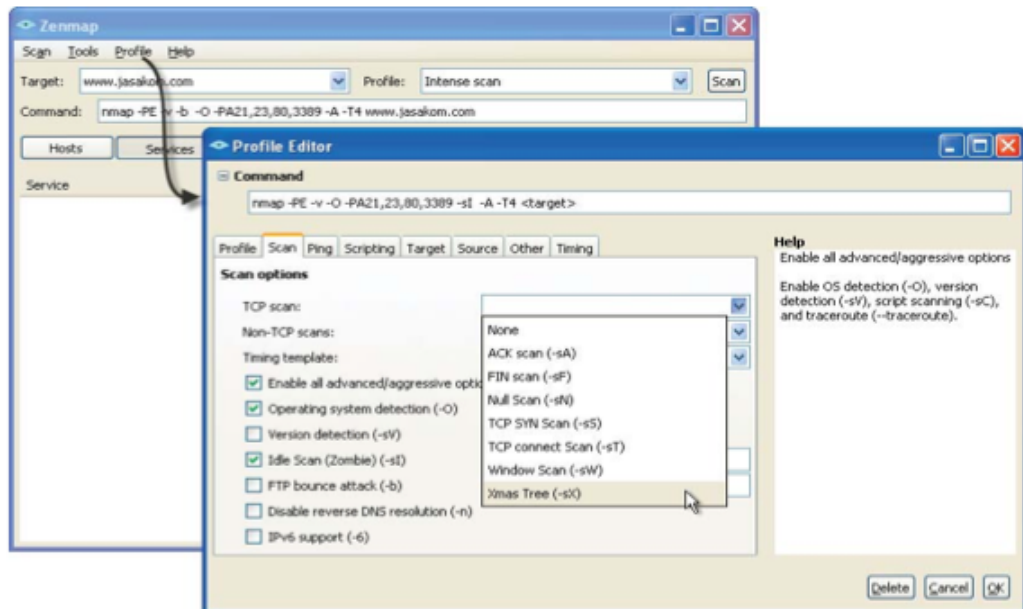
```

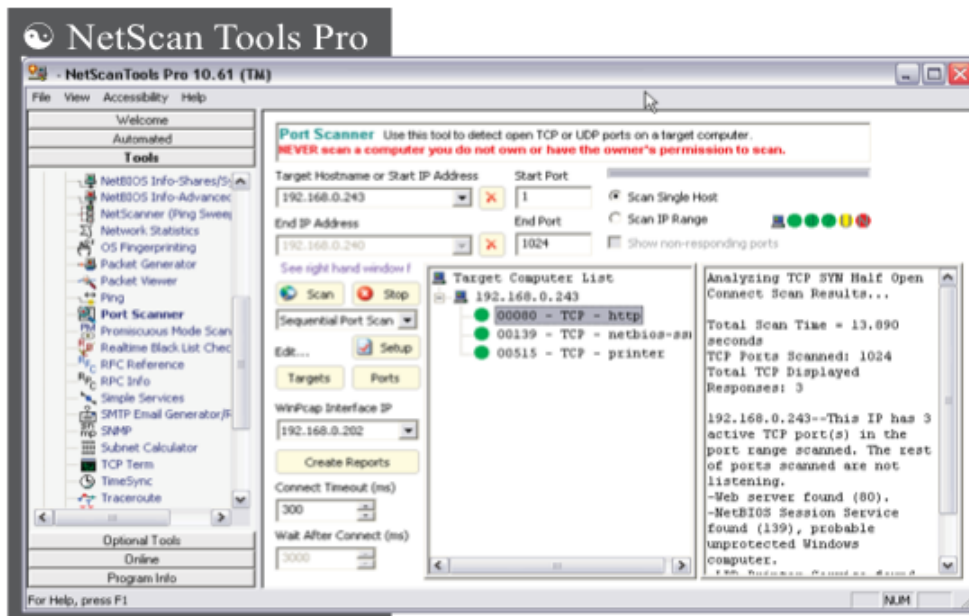
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
366/tcp   open  odmr
445/tcp   open  Microsoft-ds
1000/tcp  open  cadlock
MAC Address: 00:11:95:63:6B:61 (D-Link)
Nmap done: 1 IP address (1 host up) scanned in 223.31 seconds

```

Pada contoh, beberapa port yang terbuka diperlihatkan oleh nmap seperti port 21, 25, 80, 110, dst. Buat Anda yang tidak suka dengan baris perintah, tersedia juga interface GUI untuk Nmap yang membuatnya menjadi lebih mudah untuk digunakan.

Pada situs nmap, terdapat interface GUI nmap yaitu *ZenMap* yang membuat penggunaan Nmap menjadi lebih mudah. Anda bisa membuat profile dan menentukan jenis scanning yang hendak dilakukan dan secara otomatis ZenMap akan memperlihatkan baris perintah yang sesuai dan tentu saja Anda bisa juga langsung mengklik tombol scan untuk melakukan scanning dan melihat hasilnya dari.





NetScan Tools Pro (www.netscantools.com), selain bisa digunakan untuk mencari port yang terbuka juga bisa melakukan banyak hal seperti mengecek keabsahan alamat email, mencari lokasi dari sebuah alamat IP, mencari sharing di dalam jaringan, mendeteksi keberadaan sniffer didalam jaringan, mendeteksi komputer-komputer didalam jaringan dan lain sebagainya.

FloppyScan

FloppyScan, sebenarnya bukanlah sebuah tools namun sebuah paket program yang didesign untuk melakukan pencurian scanning. Tahapan pencurian dilakukan dengan cara :

1. Secara diam-diam, hacker memasukkan floppy disk yang telah dipersiapkan dengan tools *FloppyScan* sebelumnya ke komputer korban. Dalam kasus ini, hacker harus memiliki akses fisik.
2. Reboot komputer korban sehingga sistem operasi dijalankan dari floppy disk
3. *FloppyScan* akan menjalankan nmap dan melakukan port scanning pada jaringan komputer korban
4. Hasil scanning akan dikirimkan melalui email yang telah ditentukan oleh hacker.

Untuk menggunakan tools ini, hacker harus berada didepan komputer korban secara fisik atau menipu korban untuk menjalankan disket yang diberikan dan berharap komputer korban memiliki floppy disk yang sudah semakin langka dewasa ini. Selain itu, hacker juga harus berdoa agar komputer korban telah disetting untuk booting melalui floppy disk agar tools ini bisa berjalan.

Ketika tools ini dijalankan, dilayar komputer akan tampak *Blue Screen of Death* yang tampak seakan-akan windows mengalami crash, padahal tentu saja tidak karena dibalik layar ini, FloppyScan sedang bekerja.

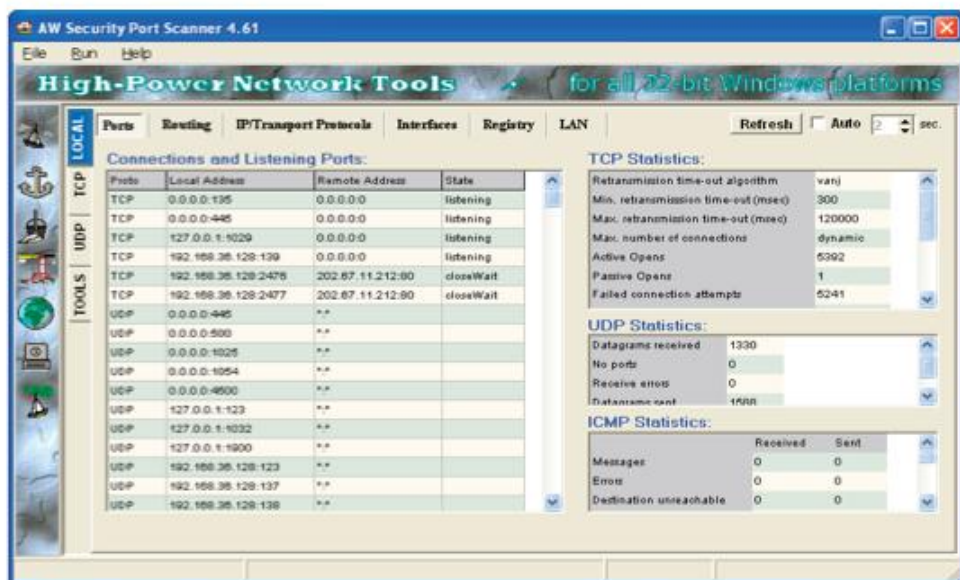
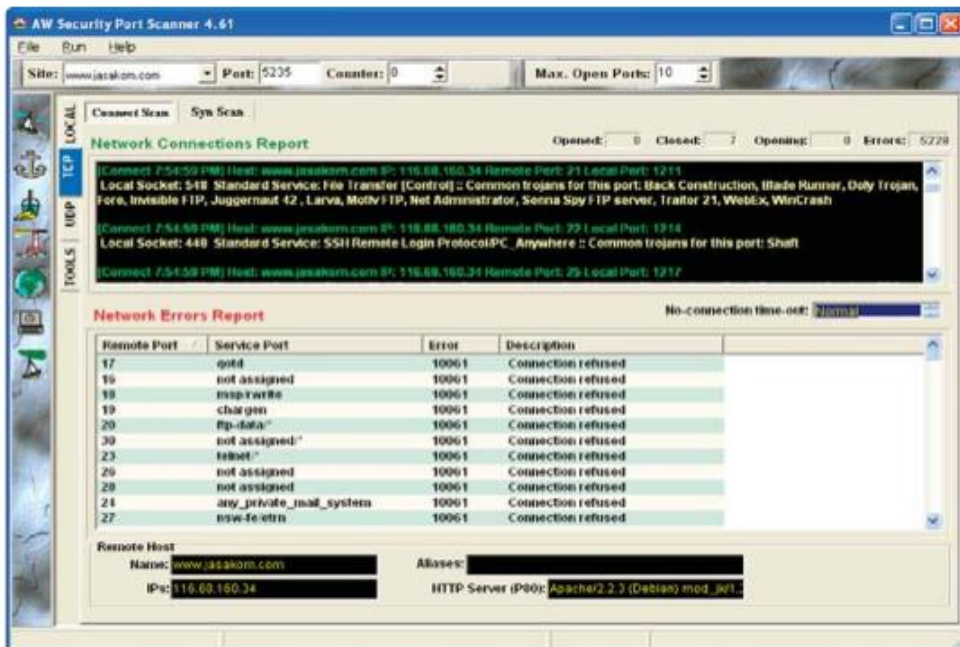
Dengan menekan tombol Alt+F4, hacker bisa melihat layar scanning yang sedang terjadi. Ketika scanning telah selesai dilakukan dan hasilnya telah dikirim ke email hacker, FloppyScan bisa menghapus dirinya sendiri.

FloppyScan disediakan dalam bentuk file image dengan nama **dosdisc.img**. Untuk memindahkan file ini kedalam floppy disk, Anda bisa menggunakan tools rawrite atau bila Anda menggunakan linux, Anda bisa menjalankan perintah **dd if=dosdisc.img of=/dev/fd0**. Setelah memindahkan FloppyScan kedalam disket, selanjutnya Anda bisa mengkonfigurasi FloppyScan melalui file *config.cfg* yang ada didalamnya seperti menentukan alamat email, dan lain sebagainya.

☯ Atelier Web Security Port Scanner

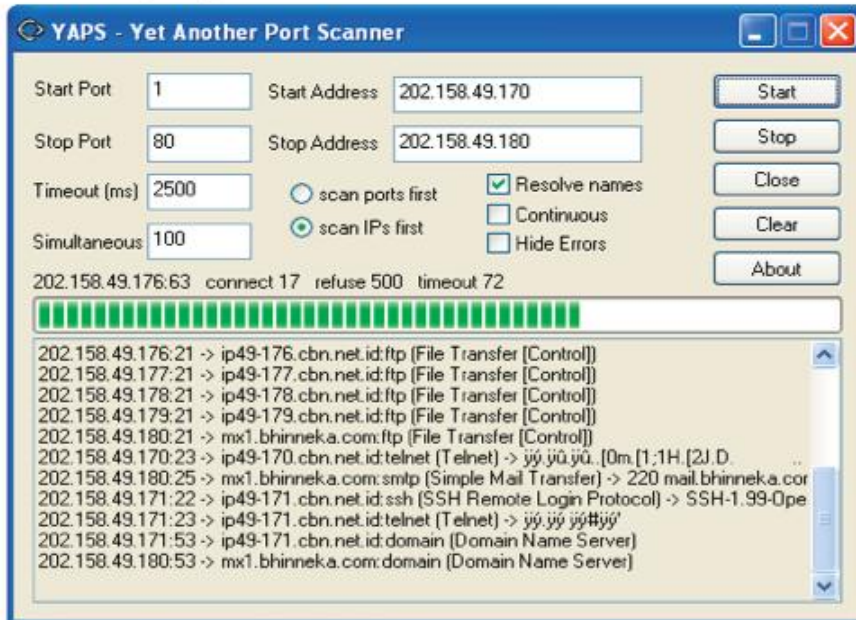
Atelier Web Security Port Scanner(www.atelierweb.com), tools ini menyediakan dua jenis port scanning yaitu *Connect Scan* dan *SynScan*. Selain scanning port TCP, tools ini juga bisa melakukan scanning port UDP. Anda tinggal memasukkan alamat host yang ingin diperiksa dan mengklik icon *Scan* yang berada pada kolom sebelah kiri.

Barangkali yang lebih menyenangkan dari tools ini adalah kemampuan memonitor port yang terbuka dan koneksi yang terjadi pada komputer lokal. Dengan tools ini, Anda bisa memonitor seandainya terdapat koneksi yang aneh dan mencurigakan baik dari maupun ke komputer Anda.



YAPS , Yet Another Port Scanner (www.steelbytes.com) adalah tools yang sederhana namun berguna. Tools ini sedikit berbeda dengan

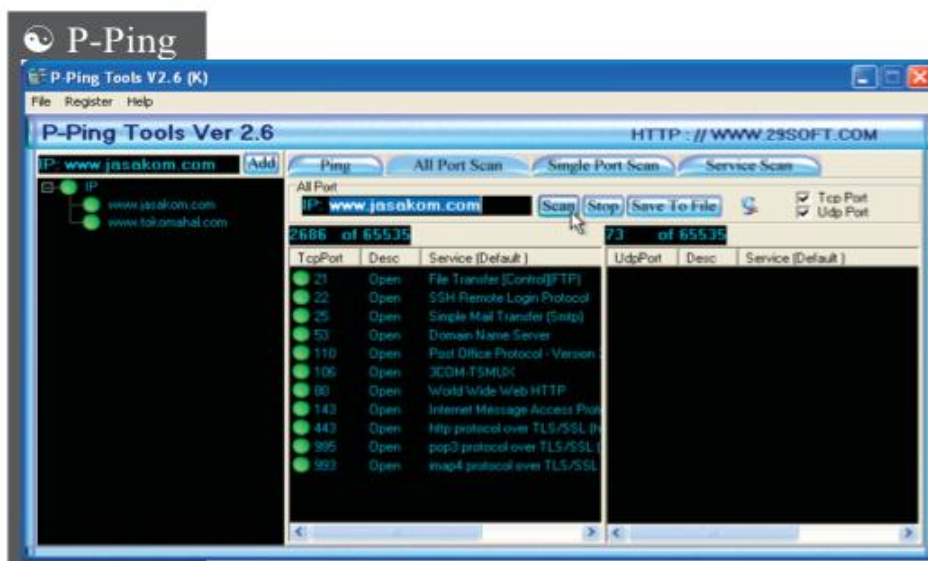
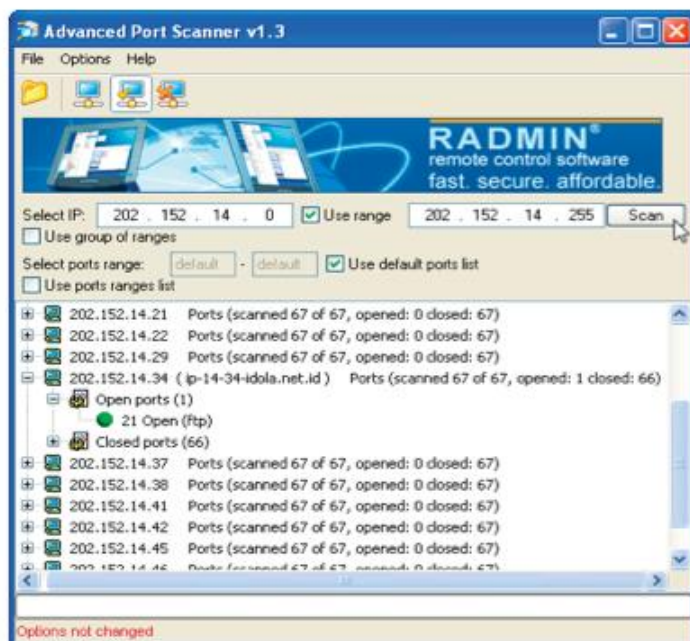
tools lainnya. Biasanya, sebuah tools bisa memeriksa banyak alamat IP sekaligus namun tidak melakukan pengecekan port yang terbuka dan biasanya program yang memeriksa port yang terbuka, hanya bisa melakukan pada satu host saja. YAPS bisa melakukan pengecekan pada banyak host sekaligus dan Anda juga sekaligus bisa menentukan pemeriksaan open port.



🕒 Advanced Port Scanner

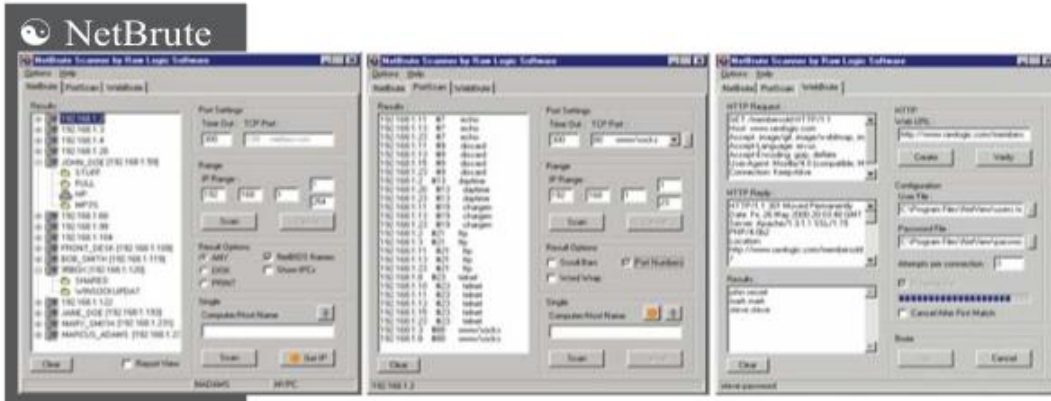
Advanced Port Scanner, tools gratis yang disediakan oleh www.radmin.com ini mempunyai ukuran file yang kecil namun dengan fungsi utama yang bisa dijalankan dengan baik. Seperti halnya dengan YAPS, dengan tools ini, Anda bisa menentukan range alamat IP dan juga port-port yang akan diperiksa untuk setiap host.

Selain bisa menggunakan port-port yang sudah umum digunakan, Anda juga bisa melakukan konfigurasi sendiri agar port-port yang Anda inginkan juga ikut diperiksa. Misalkan Anda menyebarkan trojan dan membuka port rahasia, maka Anda bisa menambahkan nomor port ini ke dalam scanner ini agar ikut diperiksa.



P-Ping (www.29soft.com), menyediakan port scanner yang mudah untuk digunakan namun tidak ada kelebihan dibandingkan dengan software lainnya. P-Ping hanya memungkinkan Anda untuk melakukan scanning terhadap satu host pada satu waktu sehingga akan merepotkan bila Anda harus melakukan scanning terhadap

banyak host sekaligus. Salah satu keunggulan dari program ini adalah ukurannya yang kecil dan kemampuannya menyimpan hasil scanning ke dalam file.



NetBrute Scanner (www.rawlogic.com) merupakan kumpulan dari 3 tools yang berbeda. Tabulasi *Netbrute* memungkinkan Anda melakukan scanning terhadap beberapa komputer secara sekaligus untuk menemukan file dan Print sharing. Banyak kasus terjadi dimana users atau pengguna awam tidak menyadari bahaya yang ada dan mereka melakukan sharing tanpa menggunakan password ataupun dengan password yang sangat lemah. Dengan tools ini, sharing dengan nama yang aneh dan panjang sekalipun bisa ditemukan dengan mudah.

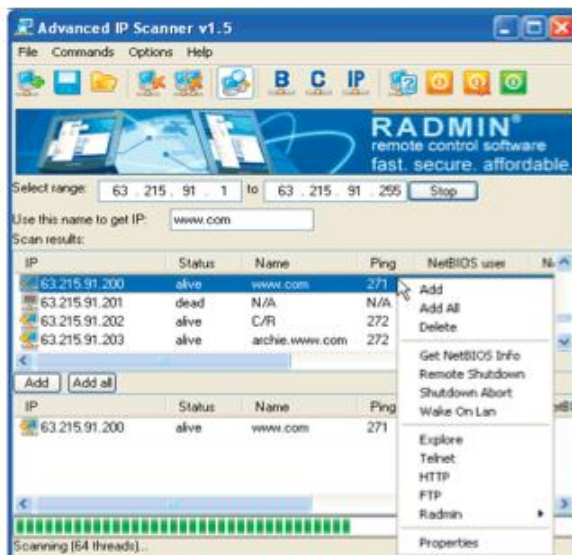
Tabulasi *PortScan*, memungkinkan Anda melakukan scanning port terhadap banyak host secara sekaligus. Interface yang disediakan juga sangat sederhana sehingga mudah untuk digunakan baik untuk pengguna awam sekalipun namun hasil scanning yang tidak ditampilkan dalam bentuk tree seperti pada tabulasi *NetBrute* dan pengurutan berdasarkan services/port sehingga host yang sama bisa tampil pada baris yang berbeda-beda membuat hasil pemeriksaan kurang nyaman untuk dilihat.

Tabulasi ketiga yaitu *WebBrute* memungkinkan Anda mencari direktory yang diproteksi pada sebuah situs dan menariknya program ini memungkinkan Anda untuk melakukan penerobosan dengan cara brute force (teknik yang akan kita pelajari pada buku ke-2 CEH).

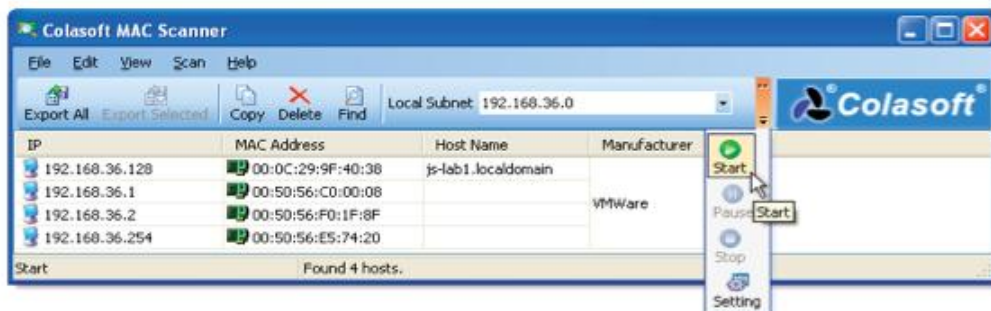
Advanced IP Scanner

Advanced IP Scanner (www.radmin.com) Tool gratis ini menyediakan fasilitas pengecekan alamat IP yang aktif. Tools ini akan lebih berguna bila digunakan didalam jaringan karena bisa juga menampilkan nama komputer serta bisa mematikan komputer secara remote.

Tentu saja, untuk mematikan komputer secara remote, Anda harus mengetahui username dan password yang digunakan. Apa gunanya? tentu saja, remote shutdown disini dilakukan secara sah dan bukan dengan cara illegal. Fungsi semacam ini dibutuhkan oleh admin yang biasanya perlu mematikan komputer yang lupa dimatikan oleh user ataupun komputer yang perlu direstart setelah melakukan instalasi patch.

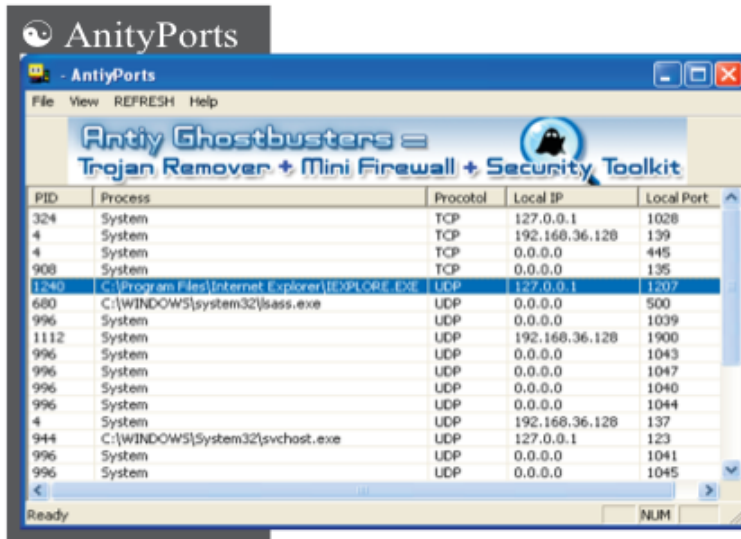


Colasoft MAC Scanner



Colasoft MAC Scanner (www.colasoft.com), tools gratis ini menyediakan fasilitas pengecekan komputer-komputer didalam jaringan lokal. Dengan tools ini Anda bisa mengetahui alamat IP mana saja yang aktif, digunakan oleh komputer yang mana dan alamat MAC atau alamat ethernet card yang digunakan. Bila Anda menggunakan versi

gratis, pada kolom isian 'Local Subnet' akan terisi secara otomatis berdasarkan alamat IP dari komputer Anda yang artinya Anda hanya diperkenankan melakukan scanning pada jaringan yang Anda gunakan. Bila Anda menggunakan versi Pro, atau versi berbayar, Anda bisa menentukan dengan bebas subnet yang hendak discan. Selanjutnya, Anda tinggal mengklik icon *Start* untuk memulai proses scanning.



AnityPorts, tools gratis yang sederhana dari AnityLabs ini akan menampilkan proses-proses yang ada didalam komputer Anda layaknya *Task Manager* namun dengan informasi yang lebih detail. *AnityPorts* misalnya, juga menampilkan program beserta folder dari program yang aktif disertai dengan alamat IP lokal beserta port yang dibuka. Program ini bisa membantu Anda dalam mencari koneksi mencurigakan yang terjadi seperti oleh koneksi yang dilakukan oleh hacker ataupun oleh virus/spyware.

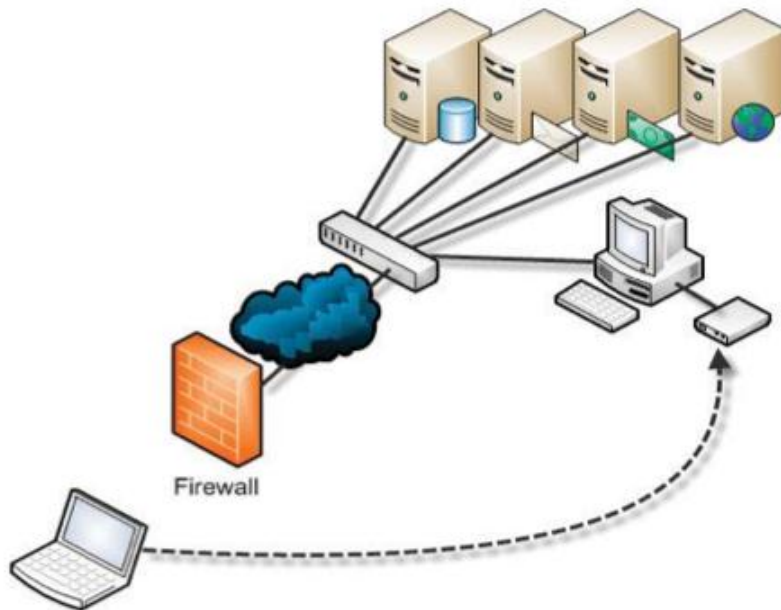
War Dialing

Jaringan perusahaan biasanya mendapatkan perhatian utama dalam hal pengamanan terhadap serangan dari luar. Firewall, IDS, Antivirus dan bermacam bentuk proteksi dilakukan untuk mencegah hacker melakukan penetrasi ke dalam perusahaan. Tentu saja hal semacam ini menyulitkan hacker namun banyak jalan menuju roma.

Di dalam jaringan sebuah perusahaan, terkadang ada saja yang entah dengan sengaja atau tidak, memasang modem untuk diremote dari luar dengan software semacam PC AnyWhere, RAS, dan lain sebagainya.

Alasannya, banyak. Ada yang karena ingin bekerja dari rumah dengan memanfaatkan komputer kantor, ada yang ingin memantau kondisi jaringan perusahaan dari luar perusahaan, ada yang ingin menggunakan internet gratis dari rumah, dan seribu alasan lainnya.

Masalahnya adalah komputer yang digunakan untuk remote access ini biasanya berada didalam jaringan yang tidak diproteksi yang artinya apabila ada yang masuk ke komputer ini, proteksi firewall menjadi tidak berguna. Masalah yang jauh lebih serius lagi adalah banyak yang menganggap hal ini sebagai sesuatu yang remeh dan merasa bahwa koneksi yang mereka sediakan ini tidak diketahui oleh siapapun.



War Dialing adalah proses pencarian akses masuk dengan menghubungi satu persatu daftar nomor telepon yang ada. Daftar nomor telepon perusahaan sendiri bisa didapatkan pada tahapan *information gathering* atau pengumpulan informasi mengenai perusahaan yang dilakukan pada tahap awal hacking.

Bila remote access atau modem yang digunakan oleh jaringan komputer korban ternyata tidak menggunakan password atau menggunakan password yang lemah, hacker dengan mudah bisa memasuki jaringan yang ada.

Mungkin Anda berfikir tentang siapa yang begitu tidak ada kerjaannya yang bersedia melakukan *war dialing* ini dengan menghubungi semua nomor telepon yang ada. Didalam bukunya, Team Security Microsoft yang menulis buku *Assessing Network Security*, diceritakan Peter Shipley yang melakukan aksi War Dialing ini dengan menghubungi jutaan nomor telepon di San Francisco untuk mendapatkan akses kedalam jaringan secara illegal yang dilakukan antara tahun 1997 sampai dengan 2000.

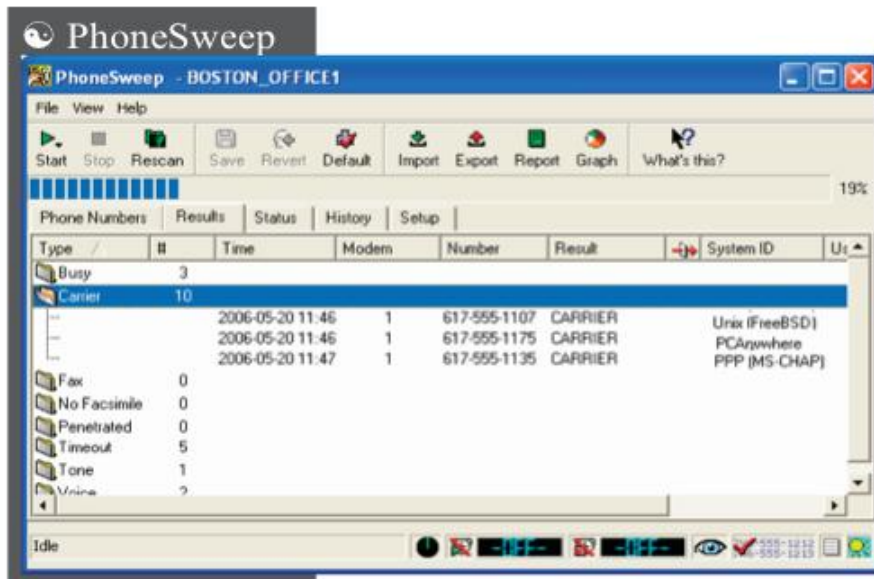
Shipley berhasil mendapatkan berbagai informasi rahasia seperti data kartu kredit, informasi kesehatan, dan berbagai informasi lainnya. Anda mungkin tidak akan pernah berfikir bahwa ada orang seperti Shipley yang mau melakukan hal semacam ini namun kenyataannya memang ada. Jadi, jangan pernah berfikir bahwa tidak akan ada orang iseng (dan sedikit gila) yang akan mencoba menelpon ke nomor telepon modem Anda yang rahasia.

Nama *War Dialing* berasal dari film *War Games* pada tahun 1983. Didalam film tersebut, seorang pemain menghubungi semua nomor telepon yang ada di Sunnyvale, California menggunakan komputernya.

Bagaimana War Dialing Bekerja

War Dialing dilakukan dengan cara menghubungi satu persatu nomor telepon yang ada dan menunggu beberapa kali nada telepon (biasanya adalah 2 kali nada telepon). Jika setelah beberapa kali nada telepon berbunyi dan tidak didapatkan nada sambung seperti fax, secara otomatis hacker akan memutuskan koneksi dan mencoba lagi nomor berikutnya. Kondisi yang sama juga terjadi jika nomor telepon yang dihubungi ternyata dijawab oleh manusia.

Dengan menggunakan program khusus, War Dialing bisa dilakukan tanpa memerlukan interaksi manusia sama sekali dan dengan mudah bisa didapatkan nomor-nomor telepon yang digunakan oleh fax maupun modem.



PhoneSweep(www.sandstorm.net), tools ini tidak hanya mencari nomor-nomor telepon yang menggunakan modem namun juga bisa mencoba melakukan penerobosan. Setelah menemukan modem, *PhoneSweep* akan mencatat nomor telepon yang didapatkan dan juga mencoba mengidentifikasi sistem yang digunakan.

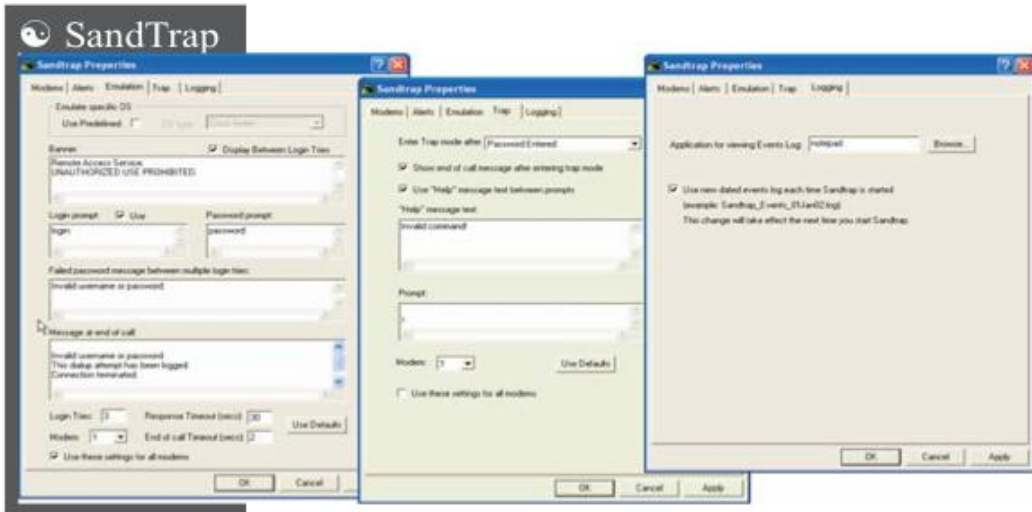
Pada versi 5.5, sandstorm menyatakan bahwa software mereka mampu mengenali 460 system yang berbeda. Dengan software ini, Anda juga bisa memasang beberapa line modem sekaligus sehingga proses phonesweep yang umumnya memakan waktu lama untuk setiap nomor telepon yang di periksa, bisa dikurangi.



THCSan(www.thc.org), tools gratis ini dibuat oleh Van Hauser dari

group hacker/phreaker eropa bernama THC (*The Hacker's Choice*). THCSan dibuat pada tahun 1995 dengan interface yang sangat sederhana namun banyak digunakan oleh kalangan hacker.

Saat ini, versi terbarunya adalah 2.01 yang dibuat pada tahun 2005. Keunikan dari program ini selain gratis adalah tersedia juga source code-nya sehingga Anda yang jago dalam hal programming, bisa saja merubahnya agar sesuai dengan kebutuhan Anda.



Populernya teknik war dialing ini tidak membuat semua orang menjadi senang. Perusahaan-perusahaan yang benar-benar peduli dengan masalah keamanan misalnya, selain memastikan tidak adanya modem liar didalam perusahaannya, juga bisa melakukan aksi balasan. *SandTrap* merupakan jawabannya untuk Anda. *SandTrap* dibuat oleh perusahaan yang sama dengan *PhoneSweep* yaitu *SandStorm* dan seperti halnya dengan *PhoneSweep*, *SandTrap* juga produk komersial yang harus dibeli untuk bisa menggunakannya.

Untuk memanfaatkan *SandTrap* secara maksimal, sebaiknya Anda mengaktifkan layanan Caller ID pada telepon yang digunakan. Dengan adanya Caller ID, *SandTrap* akan mampu mencatat nomor telepon hacker yang melakukan war dialing sehingga Anda bisa mengetahui siapa yang melakukannya. Selain mencatat *war dialing* yang terjadi, *SandTrap* juga bisa menciptakan terminal palsu, dengan menampilkan form untuk memasukkan username dan password

untuk menipu pelaku war dialing. Apa yang diketikkan oleh pelaku, akan dicatat oleh *SandTrap* sehingga Anda bisa mengetahui lebih banyak lagi mengenai pelaku *War Dialing*.

3. Mengidentifikasi Services

Tahapan ketiga dalam metodologi scanning yaitu *mengidentifikasi services yang berjalan pada komputer korban* mempunyai hubungan yang sangat erat dengan tahapan kedua metodologi scanning yaitu *port scanning*. Dengan mengetahui port mana saja yang terbuka pada komputer korban, hacker bisa menebak services atau layanan apa saja yang dijalankan. Misalnya, hacker menemukan bahwa port 80 dalam kondisi terbuka, maka hampir bisa dipastikan bahwa komputer tersebut menjalankan web server.

Contoh port yang umum digunakan beserta dengan services yang menggunakannya bisa Anda lihat pada tabel dibawah ini (ingat, tabel ini tidaklah lengkap karena tabel yang lebih lengkap bisa menghabiskan lebih dari 100 halaman buku ini) :

Keyword	Decimal	Description
echo	7/tcp	Echo
echo	7/udp	Echo
ftp-data	20/tcp	File Transfer [Default Data]
ftp-data	20/udp	File Transfer [Default Data]
ftp-data	20/sctp	FTP
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
ftp	21/sctp	FTP
ssh	22/tcp	SSH Remote Login Protocol
ssh	22/udp	SSH Remote Login Protocol
ssh	22/sctp	SSH
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer

time	37/tcp	Time
time	37/udp	Time
name	42/tcp	Host Name Server
name	42/udp	Host Name Server
nameserver	42/tcp	Host Name Server
nameserver	42/udp	Host Name Server
nickname	43/tcp	Who Is
nickname	43/udp	Who Is
tacacs	49/tcp	Login Host Protocol (TACACS)
tacacs	49/udp	Login Host Protocol (TACACS)
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
bootps	67/tcp	Bootstrap Protocol Server
bootps	67/udp	Bootstrap Protocol Server
bootpc	68/tcp	Bootstrap Protocol Client
bootpc	68/udp	Bootstrap Protocol Client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	Gopher
gopher	70/udp	Gopher
finger	79/tcp	Finger
finger	79/udp	Finger
http	80/tcp	World Wide Web HTTP
http	80/udp	World Wide Web HTTP
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
http	80/sctp	HTTP
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
rtnet	107/tcp	Remote Telnet Service
rtnet	107/udp	Remote Telnet Service

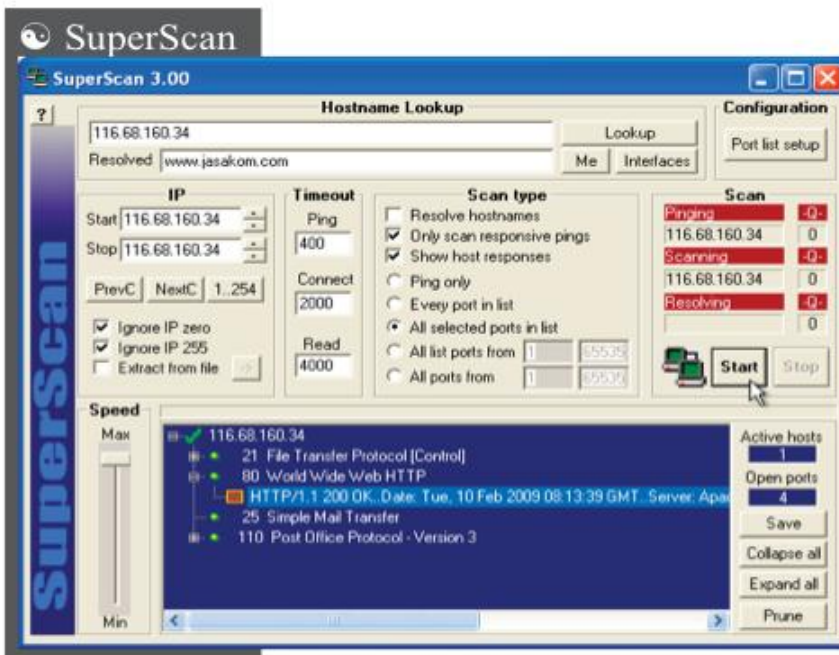
pop2	109/tcp	Post Office Protocol - Version 2
pop2	109/udp	Post Office Protocol - Version 2
pop3	110/tcp	Post Office Protocol - Version 3
pop3	110/udp	Post Office Protocol - Version 3
sunrpc	111/tcp	SUN Remote Procedure Call
sunrpc	111/udp	SUN Remote Procedure Call
ident	113/tcp	
auth	113/tcp	Authentication Service
auth	113/udp	Authentication Service
sftp	115/tcp	Simple File Transfer Protocol
sftp	115/udp	Simple File Transfer Protocol
sqlserv	118/tcp	SQL Services
sqlserv	118/udp	SQL Services
nntp	119/tcp	Network News Transfer Protocol
nntp	119/udp	Network News Transfer Protocol
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
profile	136/tcp	PROFILE Naming System
profile	136/udp	PROFILE Naming System
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol
imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	SNMP
snmp	161/udp	SNMP

snmptrap	162/tcp	SNMPTRAP
snmptrap	162/udp	SNMPTRAP
bgp	179/tcp	Border Gateway Protocol
bgp	179/udp	Border Gateway Protocol
bgp	179/sctp	BGP
irc	194/tcp	Internet Relay Chat Protocol
irc	194/udp	Internet Relay Chat Protocol
ldap	389/tcp	Lightweight Directory Access Protocol
ldap	389/udp	Lightweight Directory Access Protocol
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
https	443/tcp	http protocol over TLS/SSL
https	443/udp	http protocol over TLS/SSL
https	443/sctp	HTTPS
Microsoft-ds	445/tcp	Microsoft-DS
Microsoft-ds	445/udp	Microsoft-DS
login	513/tcp	remote login a la telnet;
who	513/udp	maintains data bases showing who's
shell	514/tcp	cmd
syslog	514/udp	
printer	515/tcp	spooler
printer	515/udp	spooler
timed	525/tcp	timeserver
timed	525/udp	timeserver
tempo	526/tcp	newdate
tempo	526/udp	newdate
irc-serv	529/tcp	IRC-SERV
irc-serv	529/udp	IRC-SERV
courier	530/tcp	rpc
courier	530/udp	rpc
uucp	540/tcp	uucpd
uucp	540/udp	uucpd
uucp-rlogin	541/tcp	uucp-rlogin

uucp-rlogin	541 / udp	uucp-rlogin
klogin	543 / tcp	
klogin	543 / udp	
kshell	544 / tcp	krcmd
kshell	544 / udp	krcmd
dhcpcv6-client	546 / tcp	DHCPv6 Client
dhcpcv6-client	546 / udp	DHCPv6 Client
dhcpcv6-server	547 / tcp	DHCPv6 Server
dhcpcv6-server	547 / udp	DHCPv6 Server
dsf	555 / tcp	
dsf	555 / udp	
remotefs	556 / tcp	rfs server
remotefs	556 / udp	rfs server
nnntp	563 / tcp	nnntp protocol over TLS/SSL (was snntp)
nnntp	563 / udp	nnntp protocol over TLS/SSL (was snntp)
whoami	565 / tcp	whoami
whoami	565 / udp	whoami
ms-shuttle	568 / tcp	Microsoft shuttle
ms-shuttle	568 / udp	Microsoft shuttle
ldp 646 / tcp	LDP	
ldp 646 / udp	LDP	
dhcp-failover	647 / tcp	DHCP Failover
dhcp-failover	647 / udp	DHCP Failover
kerberos-adm	749 / tcp	kerberos administration
kerberos-adm	749 / udp	kerberos administration
kerberos-iv	750 / udp	kerberos version iv
ftps-data	989 / tcp	ftp protocol, data, over TLS/SSL
ftps-data	989 / udp	ftp protocol, data, over TLS/SSL
ftps	990 / tcp	ftp protocol, control, over TLS/SSL
ftps	990 / udp	ftp protocol, control, over TLS/SSL
telnets	992 / tcp	telnet protocol over TLS/SSL
telnets	992 / udp	telnet protocol over TLS/SSL
imaps	993 / tcp	imap4 protocol over TLS/SSL

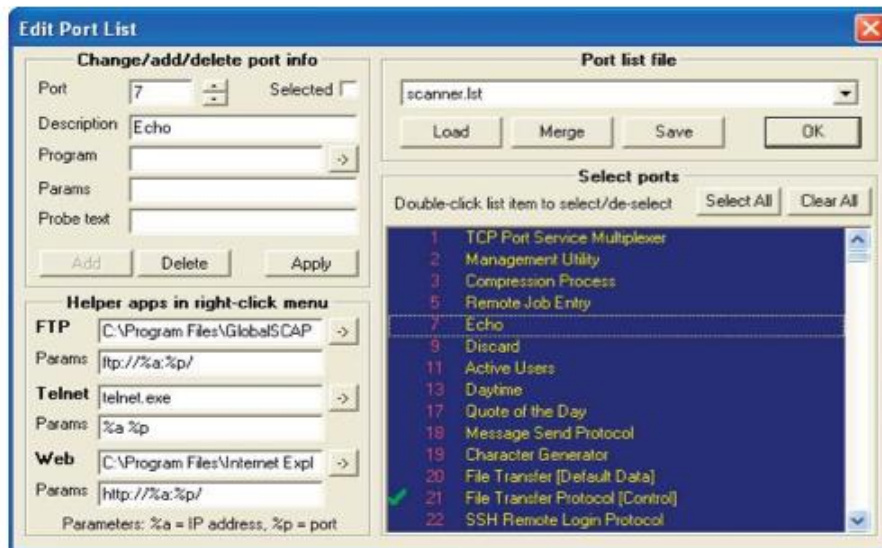
imaps	993/udp	imap4 protocol over TLS/SSL
ircs	994/tcp	irc protocol over TLS/SSL
ircs	994/udp	irc ptocol over TLS/SSL
pop3s	995/tcp	pop3 protocol over TLS/SSL (was spop3)
pop3s	995/udp	pop3 protocol over TLS/SSL (was spop3)

Anda bisa melihat port yang digunakan oleh services-services pada alamat http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

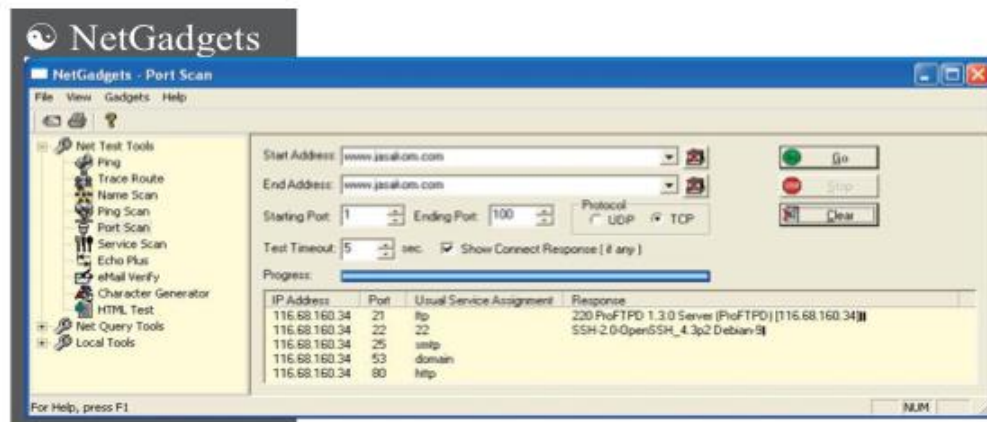


SuperScan yang dibuat oleh FoundStone (www.foundstone.com) ini cukup menarik karena memiliki beberapa fungsi seperti bisa mencari system yang aktif, mencari port terbuka, mengidentifikasi services sampai banner grabbing. Dari metodologi scanning yang dideskripsikan oleh CEH, SuperScan bisa melakukan tahapan 1 sampai dengan tahapan 4.

Untuk menggunakan SuperScan, Anda tinggal memasukkan alamat IP atau hostname yang hendak dicek kemudian mengklik tombol *Start* untuk menggunakan software ini.



Pengecekan yang dilakukan oleh *SuperScan* ini secara default cukup cepat karena hanya port-port TCP/UDP yang umum saja yang akan dicek. Anda bisa merubah port-port TCP/UDP mana saja yang akan diperiksa oleh tools ini dengan mengklik tombol 'Port List Setup'. Pada form ini, Anda juga menentukan bagaimana *SuperScan* mengambil banner dari layanan yang ditemukan.



NetGadgets (www.noticeware.com/netgadgets.htm), tools komersial ini menyediakan banyak fungsi yang bisa digunakan. Dengan program ini, Anda bisa mencari sistem yang aktif dengan ping walaupun harus dilakukan satu persatu, mencari port yang terbuka dan

mengidentifikasi services pada beberapa host sekaligus. Selain itu, tools ini juga menyiakan banyak informasi mengenai komunikasi yang terjadi pada komputer lokal yang bisa Anda lihat pada bagian *Local Tools*.

4. Banner grabbing/OS Fingerprinting

Mengetahui jenis sistem operasi yang digunakan oleh komputer korban, sangatlah penting untuk dilakukan. Sebagai contoh, bila hacker telah mengetahui bahwa sistem operasi komputer korban adalah Microsoft Windows Server 2008, hacker tinggal mencari informasi mengenai kelemahan pada sistem operasi ini dan tidak perlu lagi mencoba ribuan exploit yang tidak ada hubungannya. Mencari tahu jenis sistem operasi yang digunakan inilah yang dinamakan dengan *OS Fingerprinting*.

Pada awalnya, teknik untuk mengetahui sistem operasi komputer korban ini dilakukan dengan teknik yang dinamakan dengan *Banner Grabbing*. *Banner Grabbing* adalah teknik mencari informasi dengan melihat 'kalimat selamat datang' yang ditayangkan ketika melakukan koneksi ke layanan atau services tertentu. 'Kalimat selamat datang' atau yang dikenal dengan banner ini biasanya menunjukkan banyak hal seperti software yang digunakan, versi, dan bahkan informasi-informasi terkait lainnya. Sebagai contoh, bila Anda melihat web server yang digunakan adalah IIS, maka kemungkinan besar server yang digunakan juga dari keluarga Microsoft.

Secara default, Windows Vista tidak menginstall program Telnet. Hal ini kemungkinan dikarenakan program telnet dianggap tidak aman karena komunikasi yang dilakukan dengan telnet tidak menggunakan enkripsi namun Windows Vista tetap menyediakan program yang sangat sering digunakan ini. Untuk mengaktifkan program Telnet pada Windows Vista, lakukan langkah-langkah berikut ini :

1. Klik *Start* kemudian pilih *Control Panel*.
2. Pilih *Programs and Features*.
3. Pilih *Turn Windows features on or off*.
4. Berikan tanda centang pada *Telnet Client*.
5. Klik *OK*.

Sebagai contoh, Anda bisa mendapatkan banner dari sebuah web server (bila tidak diproteksi) dengan program telnet. Pada contoh kali ini, saya akan menggunakan program telnet dan menghubungi situs www.klikbca.com :

```
C:\>telnet www.klikbca.com 80 (Tekan [ENTER] 2 KALI)
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 06 Feb 2009 16:03:05 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is
incorrect. </body>
</html>
Connection to host lost.
C:\>
```

Pada contoh ini, terlihat banner yang ditampilkan oleh www.klikbca.com menginformasikan bahwa web server yang digunakan adalah IIS versi 5. Melalui banner yang ditampilkan ini, bahkan hacker bisa mengetahui versi dari web server IIS yang digunakan. Apakah itu penting ? Sangat penting. Bila web server yang digunakan adalah IIS, seperti yang saya katakan maka kemungkinan besar sistem operasi yang digunakan juga dari keluarga windows. Pada kasus ini, bahkan diketahui versi dari IIS yang digunakan yaitu versi 5.0 dan dengan mengetahui versi ini, bahkan bisa diprediksi lebih jauh tentang sistem operasi yang digunakan yaitu Windows Server 2000! Bagaimana hal tersebut bisa terjadi ?

Web Server IIS disediakan secara default oleh sistem operasi Windows dan setiap versi sistem operasi, menyediakan versi IIS yang berbeda. Berikut adalah tabel versi IIS dan sistem operasi yang menyediakannya :

- IIS 1.0, Windows NT 3.51
- IIS 2.0, Windows NT 4.0
- IIS 3.0, Windows NT 4.0 Service Pack 3
- IIS 4.0, Windows NT 4.0 Option Pack
- IIS 5.0, Windows 2000
- IIS 5.1, Windows XP Professional, Windows MCE
- IIS 6.0, Windows Server 2003 dan Windows XP Professional x64 Edition
- IIS 7.0, Windows Server 2008 dan Windows Vista
- IIS 7.5, Windows Server 2008 R2 (Beta) dan Windows 7 (Beta)

OS Fingerprinting berdasarkan Implementasi TCP/IP

Teknik *Banner Grabbing*, tidaklah selalu bisa diandalkan. Korban yang cerdas bisa mengelabui *banner grabbing* dengan mengganti banner default yang ada sehingga hacker yang melihat banner akan tertipu (akan dibahas pada bagian khusus). Selain itu, ada juga services yang tidak menampilkan banner sama sekali sehingga teknik *banner grabbing* menjadi tidak berguna.

Teknik lainnya yang digunakan oleh Hacker dalam menentukan sistem operasi adalah dengan mempelajari keunikan masing-masing sistem operasi dalam implementasi protokol TCP/IP. Protokol TCP/IP yang sudah menjadi standard protokol memang memiliki panduan yang bisa digunakan oleh setiap sistem operasi dalam memimplementasikannya namun panduan ini tidaklah mencakup semua kemungkinan yang bisa terjadi dan tidak semua detail dari panduan ini diikuti oleh semua vendor sistem operasi.

Sebagai contoh, sebelumnya saya sudah menjelaskan fungsi dari flag dan adanya 2 flag yang masih belum digunakan. Apa yang akan dilakukan oleh sistem operasi seandainya mendapatkan paket dengan flag yang belum terpakai namun diaktifkan? atau bagaimana bila flag yang diaktifkan dengan tidak seharusnya? paket dengan flag aneh? paket yang tidak normal atau paket rusak? sistem operasi meresponnya dengan cara yang berbeda-beda.

Contoh lainnya, pada saat terjadi komunikasi TCP, masing-masing sistem operasi ternyata menggunakan penomoran paket yang berbeda-beda sehingga dengan mengamati penomoran paket TCP ini bisa ditebak sistem operasi yang digunakan. Contoh lain lagi, yaitu pengiriman paket reply ping yang ternyata membawa data yang berbeda-beda (karena data yang dibawa sebenarnya tidak digunakan).

Berdasarkan keunikan-keunikan inilah, para hacker bisa menebak sistem operasi komputer nun jauh disana dengan keakuratan yang tinggi. Teknik menebak sistem operasi target dengan mengamati paket-paket unik dari masing-masing sistem operasi dibagi menjadi 2 yaitu : *Active Fingerprinting* dan *Passive Fingerprinting*.

Active Fingerprinting

Active Fingerprinting adalah fingerprinting yang dilakukan secara aktif. Hacker secara aktif membuat hubungan dengan komputer korban dengan mengirimkan paket-paket yang telah dimanipulasi maupun tidak dan mengamati respon dari komputer korban. Berdasarkan respon ini, hacker kemudian mempelajari keunikan yang ada dan menentukan sistem operasi dari komputer korban. Salah satu contoh *Active Fingerprinting* adalah dengan menggunakan telnet seperti yang telah kita bahas sebelumnya.

Xprobe2

Tools gratis buatan *fyodor* akan sangat membantu Anda dalam menentukan sistem operasi komputer target. Tools ini akan mengirimkan berbagai macam paket ke komputer korban dan mempelajari reaksi dari komputer korban untuk menentukan sistem operasi yang digunakan.

Tools yang dijalankan dari sistem operasi linux ini bisa Anda dapatkan pada sistem operasi BackTrack 3 tanpa perlu lagi melakukan instalasi atau jika Anda menggunakan sistem operasi linux lainnya, silahkan mendownload program xprobe2 dari situs <http://www.net-security.org/software.php?id=231>. Untuk mengetahui sistem operasi komputer korban, Anda hanya perlu menjalankan perintah xprobe2 disertai dengan nama domain atau alamat IP tujuan.

```
bt ~ # xprobe2 www.jasakom.com
```

```
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu
```

```
[+] Target is www.jasakom.com
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping - ICMP echo discovery module
[x] [2] ping:tcp_ping - TCP-based ping discovery module
[x] [3] ping:udp_ping - UDP-based ping discovery module
[x] [4] infogather:ttl_calc - TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan - TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module
```

```
[x] [12] fingerprint:smb - SMB fingerprinting module
[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 116.68.160.34. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 116.68.160.34. Module test failed
[-] No distance calculation. 116.68.160.34 appears to be dead or no ports known
[+] Host: 116.68.160.34 is up (Guess probability: 50%)
[+] Target: 116.68.160.34 is alive. Round-Trip Time: 0.05597 sec
[+] Selected safe Round-Trip Time value is: 0.11195 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.19" (Guess probability: 100%)
[+] Other guesses:
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.20" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.21" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.22" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.23" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.24" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.25" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.26" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.27" (Guess probability: 100%)
[+] Host 116.68.160.34 Running OS: "Linux Kernel 2.4.28" (Guess probability: 100%)
[+] Modules deinitialized
[+] Execution completed.
```

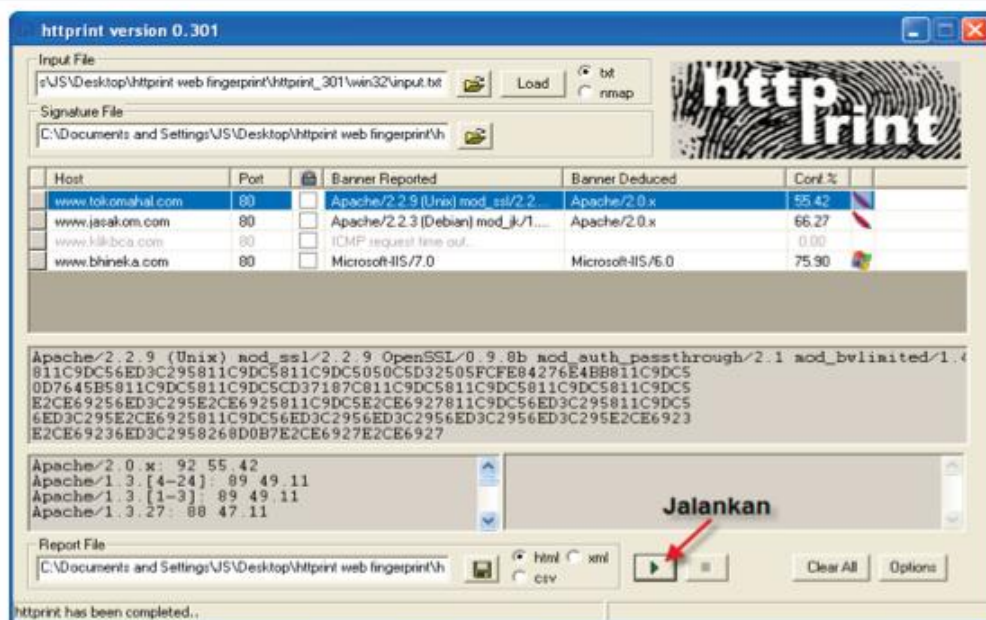
Httpprint

Contoh program *Active Fingerprinting* lainnya adalah *Httpprint* (<http://net-square.com/httpprint/>) yang bisa didapatkan secara gratis. Berbeda dengan *OS Fingerprinting* yang menggunakan keunikan implementasi protokol TCP/IP dalam menebak sistem operasi, *Httpprint* menggunakan keunikan protokol HTTP dalam menentukan jenis web server.

Konsep yang sama juga berlaku pada teknik web server fingerprinting ini yaitu dengan memanfaatkan keunikan dari setiap web server dalam menangani berbagai paket seperti paket permintaan penghapusan data, paket rusak, paket yang tidak normal dan lain-lain. Berdasarkan respon dari web server, *Httpprint* menebak jenis web server komputer korban. Sebagai contoh, tabel berikut menunjukkan perbedaan respon dari 3 jenis webserver yang berbeda yang saya ambil dari situs http://net-square.com/httpprint/httpprint_paper.html.

Server	Field Ordering	DELETE Method	Improper HTTP version	Improper protocol
Apache/1.3.23	Date, Server	405	400	200
Microsoft-IIS/5.0	Server, Date	403	200	400
Netscape-Enterprise/4.1	Server, Date	401	505	no header

Httpprint tidak mengandalkan banner seperti yang telah saya jelaskan sebelumnya karena dua sebab. Pertama, ada services-services yang tidak menampilkan banner dan kedua adalah banner bisa dipalsukan ! Benar, Anda bisa memalsukan banner sehingga IIS akan memberikan banner yang sama dengan Apache. Dengan mata telanjang, Anda jelas akan tertipu. Teknik ini akan dibahas lebih lanjut pada bab ini juga namun tidak disini.



Untuk menggunakan Httpprint, Anda tinggal memasukkan host atau alamat URL yang hendak dicek beserta port yang digunakan. Webserver yang umumnya menggunakan port 80 yang juga akan terisi secara otomatis ketika Anda memasukkan alamat URL walaupun Anda tetap bisa menggantinya dengan port yang lain.

Setelah selesai, Anda tinggal mengklik tombol *Play/Execute*, maka httpprint akan segera menjalankan tugasnya dan melaporkan kepada Anda jenis webserver yang digunakan oleh komputer korban beserta berapa persen keyakinan dari httpprint ini.



MiArt HTTP Header Info (www.miart.co.uk), tools gratis ini memungkinkan Anda melihat header sebuah host dengan sekali klik. Anda tinggal memasukkan nama host yang hendak dilihat kemudian klik tombol "Get Header".

MiArt HTTP Header Info sangat mudah untuk digunakan namun karena korban yang cerdas bisa saja mengganti header web server yang digunakan, Anda tidak bisa 100% mengandalkan informasi dari tools ini saja untuk menentukan web server yang digunakan oleh komputer korban.

Passive Fingerprinting

Berbeda dengan *Active Fingerprinting*, *Passive Fingerprinting* tidak berhubungan secara langsung dengan komputer korban. Hacker mengamati paket-paket komunikasi yang terjadi pada kondisi normal dengan metode sniffing dan berdasarkan paket komunikasi yang terjadi, hacker menentukan sistem operasi yang digunakan oleh komputer korban.

Karena hacker tidak berhubungan langsung dengan komputer korban dan karena pada komunikasi normal paket-paket yang terjadi juga terbatas, *Passive Fingerprinting* menjadi kurang akurat dibandingkan dengan *Active Fingerprinting*. Walaupun *Passive Fingerprinting* kurang akurat dibandingkan dengan *Active Fingerprinting*, *Passive Fingerprinting* tidak bisa terdeteksi oleh IDS.

P0f

P0f, tools banner grabbing yang dibuat oleh *M. Zalewski* ini termasuk *Passive Fingerprinting*. *p0f* menjalankan dirinya dengan modus sniffer dan mengamati paket komunikasi yang terjadi kemudian menebak sistem operasi yang digunakan secara otomatis. Anda bisa melihat parameter-parameter yang didukung oleh *p0f* dengan parameter *-h*.

Karena *p0f* menjalankan modus sniffer, Anda harus menentukan kartu jaringan yang akan diamati dengan parameter *-i* disertai dengan nomor kartu jaringan yang Anda gunakan. Bagaimana menentukan penomoran dari kartu jaringan yang ada saat ini?

Anda bisa melihatnya dengan parameter *-L*. Selanjutnya, *p0f* akan dijalankan dalam modus listening dan ketika terjadi koneksi misalnya ada komputer lain yang melakukan koneksi ke komputer Anda misalkan dengan telnet, ftp, browsing (bila komputer Anda menjalankan webserver), *p0f* akan memprediksi sistem operasi yang digunakan oleh pengunjung tersebut dan menampilkannya kelayar. Bila Anda melakukan browsing ke luar, *p0f* akan menampilkan prediksi dari sistem operasi yang Anda gunakan.

```
C:\p0f>p0f -h
```

```
Usage: p0f [ -f file ] [ -i device ] [ -s file ] [ -o file ]
        [ -w file ] [ -XVNDUKASCMLRqtpdlrx ]
        [ -c size ] [ -T nn ] [ 'filter rule' ]
-f file   - read fingerprints from file
-i device - listen on this device
-s file   - read packets from tcpdump snapshot
-o file   - write to this logfile (implies -t)
-w file   - save packets to tcpdump snapshot
-c size   - cache size for -Q and -M options
-M        - run masquerade detection
-T nn     - set masquerade detection threshold (1-200)
-V        - verbose masquerade flags reporting
-F        - use fuzzy matching (do not combine with -R)
-N        - do not report distances and link media
-D        - do not report OS details (just genre)
-U        - do not display unknown signatures
-K        - do not display known signatures (for tests)
-S        - report signatures even for known systems
-A        - go into SYN+ACK mode (semi-supported)
-R        - go into RST/RST+ACK mode (semi-supported)
-r        - resolve host names (not recommended)
-q        - be quiet - no banner
```

- p - switch card to promiscuous mode
- d - daemon mode (fork into background)
- l - use single-line output (easier to grep)
- x - include full packet dump (for debugging)
- X - display payload string (useful in RST mode)
- C - run signature collision check
- L - list all available interfaces
- t - add timestamps to every entry

'Filter rule' is an optional pcap-style BPF expression (man tcpdump).

C:\p0f>p0f -L

Interface	Device	Description
1	\Device\NPF_GenericDialupAdapter	Adapter for generic dialup and VPN capture
2	\Device\NPF_{4298C4AB-6488-4E7A-919B-022AC62EB104}	VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler)

C:\p0f>p0f -i 2

```
p0f - passive os fingerprinting utility, version 2.0.4
(C) M. Zalewski <lcantuf@dione.cc>, W. Stearns <wstearns@pobox.com>
WIN32 port (C) M. Davis <mike@datanerds.net>, K. Kuehl <kkuehl@cisco.com>
p0f: listening (SYN) on '\Device\NPF_{4298C4AB-6488-4E7A-919B-022AC62EB104}', 22
3 sigs (12 generic), rule: 'all'.
192.168.36.128:1134 - Windows XP Pro SP1, 2000 SP3
-> 207.46.250.101:80 (distance 0, link: ethernet/modem)
192.168.36.128:1135 - Windows XP Pro SP1, 2000 SP3
-> 66.77.197.150:80 (distance 0, link: ethernet/modem)
```

Bila Anda adalah pengguna linux, Anda bisa mendownload versi terbaru versi 2.08(pada saat buku ini dibuat) atau Anda bisa langsung menggunakan sistem operasi BackTrack yang sudah menyertakan p0f versi 2.08. Berbeda dengan versi windowsnya, versi 2.08 ini tidak memiliki parameter -L untuk melihat kartu jaringan yang ada didalam komputer Anda. Hal ini terjadi karena Anda bisa melihat kartu jaringan yang ada dengan mudah melalui perintah dari linux sendiri yaitu *ifconfig*.

Selanjutnya, Anda bisa menggunakan parameter -i disertai dengan nama kartu jaringan yang digunakan. Apabila komputer Anda hanya memiliki satu kartu jaringan, Anda tidak perlu menggunakan parameter -i, karena p0f secara otomatis akan menggunakan kartu jaringan yang tersedia tersebut.

```

Shell - Konsole
bt ~ # ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:40:34:5C
      inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:364 errors:0 dropped:0 overruns:0 frame:0
      TX packets:285 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:274295 (267.8 KiB) TX bytes:36530 (35.6 KiB)
      Interrupt:16 Base address:0x2000

lo Link encap:Local Loopback
   inet addr:127.0.0.1 Mask:255.0.0.0
   UP LOOPBACK RUNNING MTU:16436 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:0
   RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # p0f -i eth0
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcantuf@diode.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0', 262 sigs (14 generic, cksum 0F1F5CA2), rule: 'all'
192.168.1.100:53549 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
      Signature: [8192:128:1:52:M1460,N,W2,N,N,S:::Windows:?]
      -> 192.168.1.101:21 (distance 0, link: ethernet/modem)
192.168.1.100:53549 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
      Signature: [8192:128:1:52:M1460,N,W2,N,N,S:::Windows:?]
      -> 192.168.1.101:21 (distance 0, link: ethernet/modem)
192.168.1.100:53549 - Windows 2000 SP2+, XP SP1+ (seldom 98)
      -> 192.168.1.101:21 (distance 0, link: ethernet/modem)
192.168.1.101:52801 - Linux 2.6 (newer, 1) (up: 1 hrs)
      -> 202.6.211.8:80 (distance 0, link: ethernet/modem)
192.168.1.101:49320 - Linux 2.6 (newer, 1) (up: 1 hrs)
  
```

Netcraft

Netcraft (www.netcraft.com), situs riset yang berbasis di Inggris ini mengumpulkan informasi mengenai jenis web server dan juga sistem operasi yang digunakan oleh sebuah web secara berkala. Dengan memanfaatkan web ini, hacker bisa dengan mudah mengetahui informasi mengenai sistem operasi dan juga web server yang digunakan beserta history atau sejarah perubahan yang pernah terjadi.

Misalnya, komputer korban sebelumnya menggunakan sistem operasi linux, kemudian berubah menjadi windows, netcraft akan melaporkan hal ini kepada Anda juga. Dengan memanfaatkan netcraft, hacker tidak perlu berhubungan sama sekali dengan komputer korban sehingga tidak akan terdeteksi.



Menipu Hacker Melalui Banner

Seperti yang telah saya katakan sebelumnya, pemeriksaan informasi berdasarkan banner bisa saja menipu karena banner bisa diganti walaupun masih sedikit yang melakukan hal ini dan masih sedikit administrator yang mengetahui hal ini bisa dilakukan. Untuk mengganti banner dari sebuah services, tentunya sangat tergantung dari services yang digunakan.

Terkadang, ada services yang telah menyediakan banner yang dengan mudah bisa diganti seperti router cisco namun services yang lain mungkin membutuhkan sedikit editing pada file text seperti apache dan yang lain mungkin membutuhkan sedikit kerja keras seperti web server IIS. Dengan IIS, Anda harus mengedit file `%SYSTEMROOT%\system32\inetsrv\w3svc.dll` dengan hex editor yang beresiko besar.

Iislockdown

Iislockdown (<http://www.Microsoft.com/technet/Security/tools/locktool.msp>) yang telah menggabungkan *URLscan* adalah tools gratis buatan Microsoft yang akan membantu Anda mengamankan web server IIS Anda. Dengan tools ini, Anda bisa menghapus banner dari IIS versi 4 & 5. Tools ini tidak mendukung IIS versi 6 ke atas yang disertakan

oleh sistem operasi Windows Server 2003. Hal ini dikarenakan keamanan IIS versi 6 ke atas telah mendapatkan perhatian yang jauh lebih baik dari Microsoft sehingga dianggap tidak membutuhkan iislockdown lagi.

Walaupun telah mendapatkan perhatian yang lebih ketat, IIS versi 6 tidak memberikan fasilitas membuang header web server karena dianggap bukan sebagai sebuah ancaman. Alasan lainnya adalah karena adanya tools semacam httpprint yang tidak mengandalkan respon dari header HTTP dalam menentukan jenis web server yang digunakan (<http://technet.microsoft.com/en-au/security/cc242650.aspx#ECAA>).

ServerMask

Salah satu produk pengganti banner yang sangat menarik adalah *Server Mask* (www.port80software.com/products/servermask). *Server Mask* mendukung web server IIS 5.0 (Windows 2000 Server), IIS 5.1 (Windows XP) dan IIS 6.0 (Windows Server 2003) dan memungkinkan Anda memalsukan web server yang Anda gunakan sehingga tampak seperti apache, sun, atau web server lainnya.

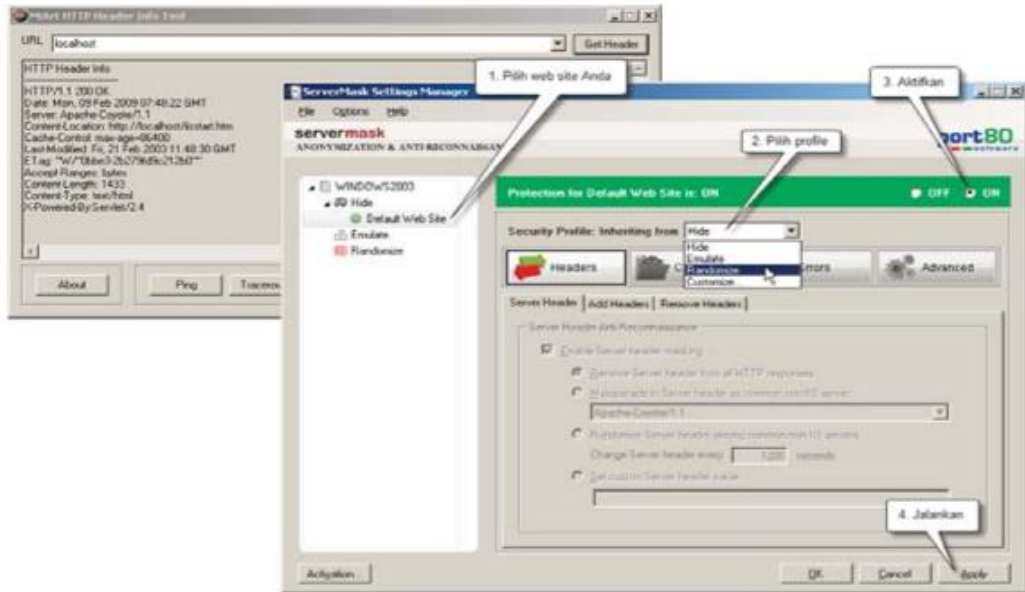
ServerMask menyediakan 3 profile default yaitu *Hide*, *Emule* dan *Randomize*. Profile *Hide* akan membuang header HTTP dari web server Anda sedangkan profile *Emule* akan memalsukan web server Anda dengan web server lainnya.

Profile ketiga yaitu *Randomize* akan memalsukan web server yang Anda gunakan secara acak, jadi terkadang akan mirip dengan apache, terkadang mirip dengan WebSphere, terkadang mirip dengan Lotus Domino dan lain sebagainya.

ServerMask adalah program yang sangat menarik untuk mengamankan web server Anda dan bisa mengelabui hacker namun dengan interface dan rancangan navigasi yang buruk dan membingungkan. Perhatikan penjelasan berikut bila Anda ingin menggunakan ServerMask.

Pertama kali, *ServerMask* akan menampilkan 3 profile yang disediakan pada kolom sebelah kiri. Web server Anda akan berada didalam profile '*Hide*' yang pada contoh ini nama web servernya

adalah 'Default Web Site', nama default yang diberikan oleh IIS 6. Klik 'Default Web Site' (1) dan kini perhatikan form yang ditampilkan.

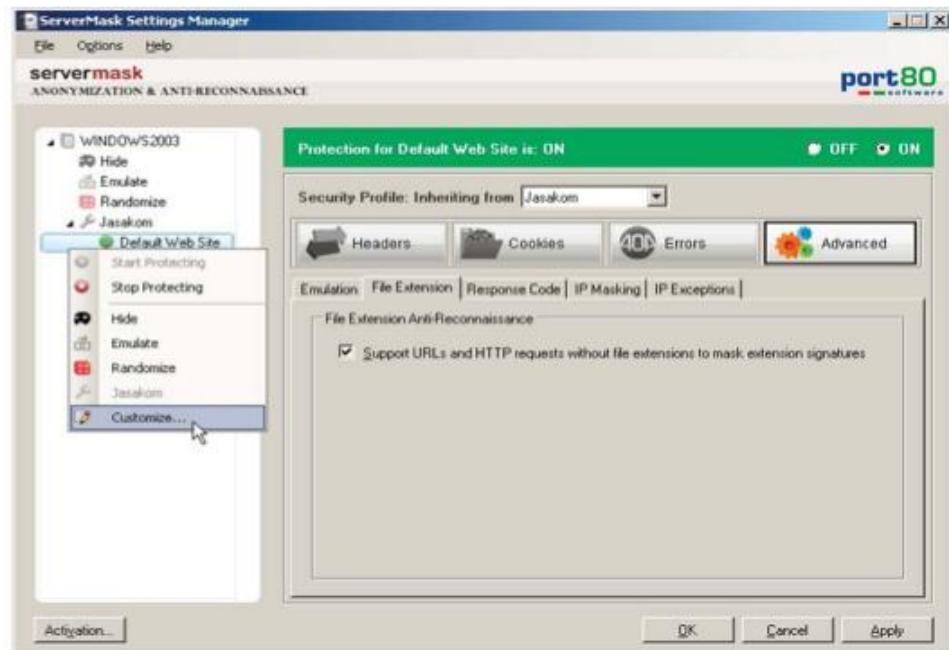


Pada form yang ditampilkan, terdapat settingan "Security Profile: Inheriting from:". Pada kolom isian inilah Anda memilih 'profile' yang hendak digunakan. Ketika Anda milih profile 'Randomize' misalnya (2), tiba-tiba saja (karena itu saya katakan interface yang buruk) posisi dari 'Default Web Site' akan berubah dan berada didalam direktory tree 'Randomize'. Tahapan berikut, Anda tinggal mengklik radio button 'On' (3) dan mengklik tombol 'Apply' (4).

Selain dengan profile yang telah ada, Anda juga bisa membuat profile baru. Untuk itu, Anda tinggal memilih web site Anda, klik kanan dan pilih 'Customize'.

Pada contoh, saya telah membuat sebuah profile baru bernama 'Jasakom'. Dengan profile baru ini, Anda bisa menentukan secara bebas bagaimana akan melindungi web server Anda dan mengaktifkan berbagai setting 'penipuan' untuk hacker.

Pada settingan 'Advanced', tabulasi 'File Extention' terdapat pilihan 'Support URL and HTTP requests without file extensions to mask extension signatures' yang memungkinkan Anda menghilangkan extensions file.



Menghilangkan extensions file yang digunakan sangatlah penting karena dengan melihat jenis file Anda saja, hacker bisa menebak jenis web server yang digunakan. Sebagai contoh, bila web server Anda menggunakan file dengan extensions asp atau aspx, maka bisa diperkirakan web server yang digunakan adalah IIS sedangkan bila web server Anda menggunakan file dengan extensions php, maka bisa diperkirakan web server yang digunakan adalah Apache.

PageXchaner

PageXchanger(www.port80software.com/products/pagexchanger) memungkinkan Anda menghilangkan extensions file sehingga pengunjung tidak mengetahui jenis file yang Anda digunakan.

Tentu saja, untuk memanfaatkan software ini secara maksimal, di dalam source code program Anda, extensions file juga harus Anda hilangkan. Software ini mendukung web server IIS 6.0 / Windows Server 2003, IIS 5.1 / Windows XP, IIS 5 / Windows 2000 dan IIS 4 / Windows NT.



Seperti halnya dengan *ServerMask*, Anda memilih terlebih dahulu web site yang hendak disetting pada kolom sebelah kiri, sedangkan settingan ada di form sebelah kanan. Pada tabulasi '*Dynamic Negotiation*', terdapat daftar extensions file. Daftar ini memegang peranan yang sangat penting karena menentukan urutan pencarian file oleh PageXchanger dan Anda bisa menambahkan, menghapus ataupun merubah urutan file yang ada.

Sebagai contoh, misalkan ada pengunjung yang mengakses situs Anda dengan URL <http://www.xxx.com/test>, maka PageXchanger akan mencari file `test.asp` terlebih dahulu. Bila file `test.asp` ada didalam server, PageXchanger akan menjalankan file tersebut namun apabila file tersebut tidak ada didalam server, PageXchanger akan mencari file selanjutnya yaitu file `test.asmx`, dan seterusnya berdasarkan daftar extensions yang ada didalam tabulasi '*Dynamic Negotiation*' ini.

5.Vulnerability Scanning

Barangkali, inilah bagian paling menarik bagi sebagian pembaca buku pertama ini karena pada tahapan inilah, hacker bisa mengetahui secara jelas pintu masuk ke komputer korban tanpa harus bekerja

keras. Setiap hari, informasi tentang kelemahan produk, terus bermunculan. Bayangkan saja bila terdapat satu permasalahan saja setiap hari, dalam setahun sudah terdapat 365 macam permasalahan yang ada di dunia ini.

Bila Anda harus melakukan pengecekan permasalahan yang ada satu persatu secara manual, berapa lama waktu yang Anda butuhkan? Anggap saja untuk memeriksa satu permasalahan dibutuhkan waktu 10 menit maka waktu yang dibutuhkan untuk memeriksa kemungkinan 365 permasalahan saja dibutuhkan waktu 3.650 menit atau 60 jam.

Itu untuk satu komputer saja, belum lagi jika Anda harus memeriksa 10 komputer ! oh, dan saya mengasumsikan hanya terdapat 365 macam permasalahan yang ada padahal yang sebenarnya adalah terdapat ribuan vulnerabilities yang beredar saat ini dan terus bertambah dengan pesat seiring dengan banyaknya software-software baru yang beredar.



Dan Farmer dan Wietse Venema

Pada tahun 1995, *Dan Farmer* dan *Wietse Venema* membuat geger dunia security karena kedua pemberontak ini membuat sebuah tools yang dinamakan dengan SATAN (setan) yang merupakan singkatan dari *Security Administrator Tool for Analyzing Networks*.

SATAN merupakan network based vulnerability scanners yang pertama didunia dan beredar secara luas kepada masyarakat umum. Dengan tools ini, pengguna awam sekalipun bisa mencari kelemahan didalam suatu produk dan menggunakan informasi yang didapatkan dari produk ini untuk menerobos masuk kedalam suatu komputer.

Hacking menjadi mudah untuk semua orang, banyak yang senang dan banyak pula yang khawatir. *Dan Farmer* sendiri dipecat dari pekerjaannya di Silicon Graphics Inc namun ternyata hal tersebut tidak membuat *Dan Farmer* lama menjadi pengacara (pengangguran banyak acara) karena ia segera dipekerjakan oleh Sun Microsystems Inc. Selamat!

Kini, SATAN memang sudah tidak dikembangkan lagi namun akibat dari beredarnya SATAN sangatlah luas dan memicu software-software sejenis lainnya yang kini telah mencapai lebih dari seratus tools yang melakukan hal yang sama.

Saat ini vulnerability scanner digunakan oleh semua pihak, baik setan maupun malaikat, baik Anda maupun saya (yang jelas, bukan saya setannya).


Pada bagian ini, Anda akan melihat beberapa security scanner yang beredar saat ini dan Anda bisa menggunakan referensi ini untuk kebutuhan Anda yang berbeda-beda (maksud saya, sebagai ethical hacker tentunya :)

Saint

Saint (*Security Administrator's Integrated Network Tool*), adalah tiruan dan salah satu pengganti dari program SATAN yang sudah tidak dikembangkan lagi. Tools yang kini dikomersilkan (www.saintcorporation.com) ini bisa dijalankan dari lingkungan Linux, Sun Solaris, FreeBSD dan Mac OS X ini akan melakukan pengecekan kelemahan yang ada dan melaporkannya kepada Anda dalam bentuk laporan yang menarik.

Untuk melakukan scanning, Anda hanya perlu menentukan alamat IP yang akan dicek, selanjutnya, SAINT akan melakukan pengecekan secara otomatis.

Karena setiap harinya kelemahan produk selalu bertambah dan berubah, Anda perlu mengupdate database yang digunakan oleh SAINT untuk memanfaatkan secara maksimal produk ini.



Examine. Expose. **Exploit.**

Vulnerability Scanning

Penetration Testing

Home

Sessions

Scan Set-Up

Data Analysis

Configuration

Schedule

Documentation

Vulnerabilities – Danger Levels

Critical Problems ▶

- Root Shell
- User Shell
- Unprivileged Shell
- User File Write
- Root Access via Buffer Overflow
- Evidence of Penetration
- Denial of Service

Areas of Concern ▶

- Information Gathering
- Privilege Elevation
- Use as an Intermediary
- Susceptibility to Malicious Content

Potential Problems ▶

- Possible Vulnerabilities
- Limit Internet Access?
- Poor Security Policy

Hosts may appear in multiple categories.

Show excluded records

Confirmed Vulnerability

Inferred Vulnerability

Included Vulnerability

Excluded Vulnerability

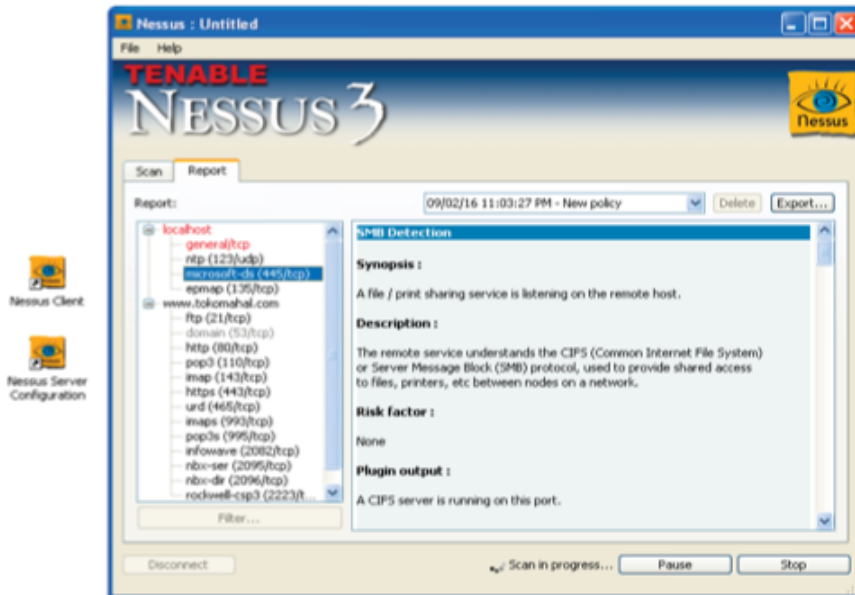
Root Access via Buffer Overflow

Host	Vulnerability	CVE	Include/Exclude	Include All/Exclude All
host1.domain.com	vulnerability in Windows Media Services (nslislog.dll)	CVE-2003-0227 CVE-2003-0349		
host1.domain.com	MS FrontPage Server Extension Vulnerability: /_vti_bin/shtml.dll	CVE-2003-0824		
host1.domain.com	MS FrontPage Server Extension Vulnerability: remote_debug	CVE-2003-0822 EXPLOIT		
host1.domain.com	Windows 2000 ASN1 buffer overflow	CVE-2003-0818		
host1.domain.com	Windows 2000 RPC buffer overflow	CVE-2003-0352 EXPLOIT		
host1.domain.com	TOP 20 Windows SMB Transaction response buffer overflow	CVE-2005-0045		
host2.domain.com	Win2003 RPC buffer overflow	CVE-2003-0352 EXPLOIT		

Nessus

Nessus (www.nessus.org), bisa dikatakan sebagai security scanner paling populer, open source dan gratis... sampai tahun 2005 ketika pembuatnya berubah pikiran dan menutup source code-nya dan

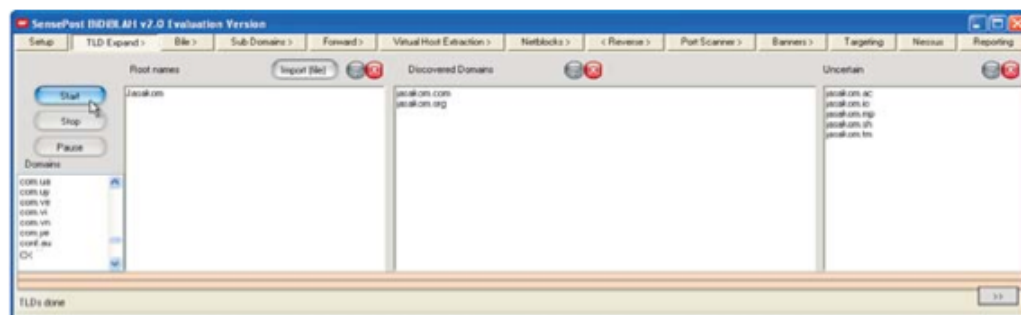
pada tahun 2008 menarik biaya untuk softwarenya sebesar 1.200 dolar per tahun walaupun masih tersedia versi gratis untuk pengguna rumahan/personal.



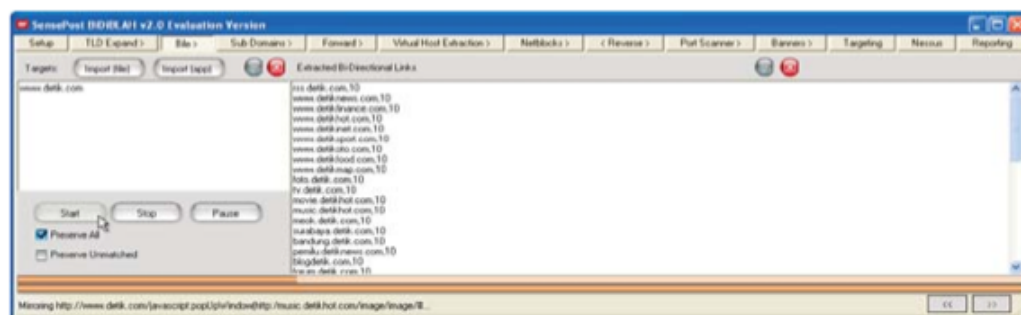
Software ini terdiri dari dua bagian yaitu *server* dan *client*. Anda bisa menjalankan server dan client Nessus dari komputer yang berbeda dan untuk melakukan scanning, yang Anda jalankan adalah program client namun client ini hanyalah berupa interface untuk pengguna, tanpa server Nessus, client yang Anda jalankan tidak ada gunanya. Untuk itu, Anda harus membuat koneksi ke Nessus Server dari client Nessus. Setelah koneksi tercipta, Anda baru bisa menggunakan Nessus dalam melakukan *vulnerabilities scanning*.

Bidiblah

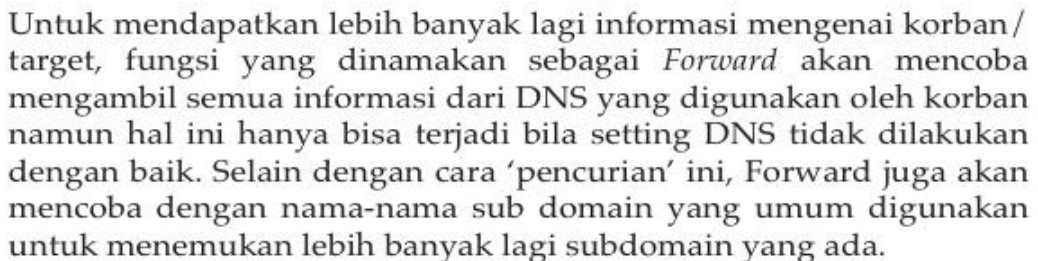
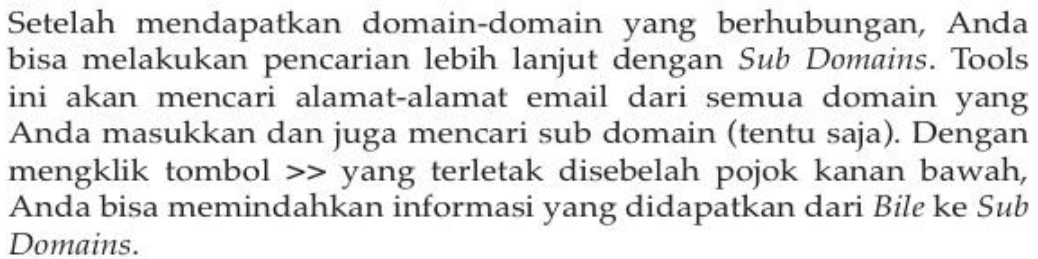
Bidiblah Automated Scanner, Tools dari SensePost ini merupakan gabungan dari beberapa tools yang mencakup tahapan menggali informasi sampai dengan penetration testing (percobaan penerobosan). Tools yang tercakup didalam paket ini dari TLD Expand, Bile, SubDomains, Forward, Netblocks, Reverse, Port Scanner, Banners, Targeting, Nessus sampai Reporting.



Tolos pertama, TLD Expand akan mencari domain-domain berdasarkan kata yang Anda masukkan dan memisahkannya berdasarkan domain digunakan dan domain yang belum digunakan secara aktif (misalnya sudah dimiliki namun belum diaktifkan). Misalnya, Anda memasukkan kata 'Jasakom', maka TLD Expand akan mencari Jasakom.com, Jasakom.net, Jasakom.tw dan seterusnya. Informasi mengenai domain-domain yang akan dicoba ini didapatkan dari file `C:\Program Files\SensePost\BiDiBLAH\misc\known-tlds.txt` sehingga dengan merubah file ini, Anda bisa menambahkan atau mengurangi domain yang ada.



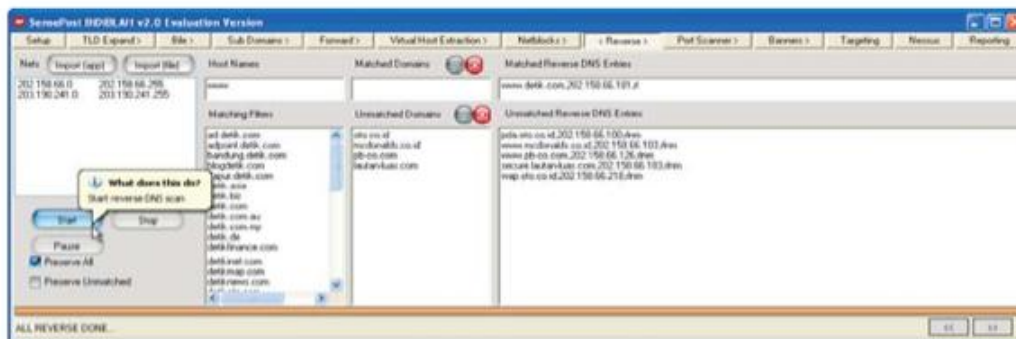
Pada awal buku ini, saya katakan kepada Anda bahwa hacker akan mencari sebanyak mungkin pintu masuk yang ada, termasuk melalui pintu tetangga seperti kasus situs Jasakom.com. Situs-situs yang saling berhubungan, biasanya juga memiliki hubungan fisik yang kuat, termasuk server yang sama atau server yang saling percaya dan bisa saling akses. *Bile* (Bi-directional Link Extraction), adalah tools yang digunakan untuk mencari link atau hubungan antar domain. Dengan memasukkan sebuah nama domain, Bile Akan mencari situs-situs lainnya yang dianggap mempunyai hubungan yang kuat.



Sebuah alamat IP dan sebuah server yang sama bisa digunakan oleh beberapa web server yang berbeda. Dengan memanfaatkan salah satu web yang bermasalah saja, hacker bisa menguasai semua web yang terletak pada server yang sama. *Virtual Host Extraction*, akan mencari domain-domain lain yang menggunakan alamat IP yang sama karena hal ini bisa diartikan beberapa web server menggunakan server fisik yang sama. Dengan mengetahui domain-domain ini, hacker bisa mencoba melakukan penetrasi berdasarkan pintu yang paling lemah pertahanannya dan menguasai seluruh web server yang ada.



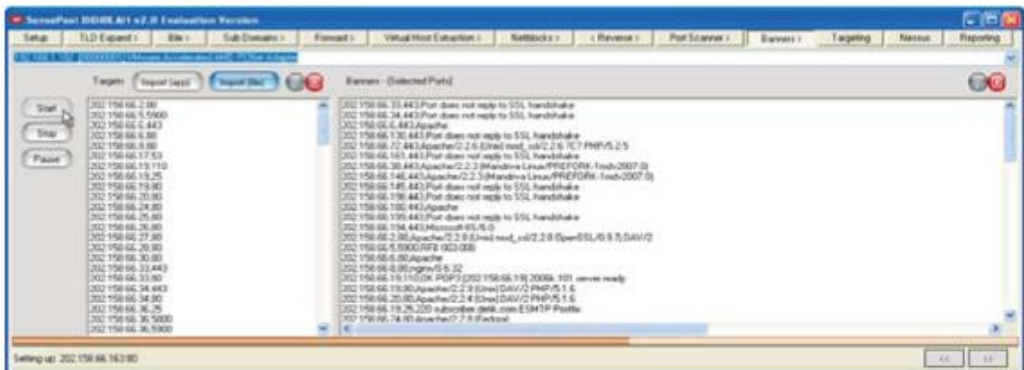
Berdasarkan alamat IP yang telah diketahui, hacker bisa mencari range alamat IP yang dimiliki oleh korban dan juga melihat informasi mengenai pemilik alamat IP tersebut (whois) dengan tools *Netblocks*. Selain mendapatkan informasi range alamat IP dari proses sebelumnya, Anda juga bisa memasukkan range alamat IP secara manual pada bagian ini karena informasi yang dimasukkan disini, akan digunakan pada proses selanjutnya. Berdasarkan range alamat IP yang dimasukkan, *Netblocks* juga akan mencari informasi negara asal alamat IP tersebut.



Reverse menggunakan teknik *Reverse Lookup* (pencarian terbalik, dari alamat IP ke nama domain) untuk mendapatkan nama host berdasarkan alamat IP yang ada. Pada bagian ini, Anda tidak bisa menambahkan range alamat IP dan hanya bisa menggunakan tombol *Import(app)* yang akan mengambil range alamat IP yang telah ada pada tabulasi *Netblocks*.

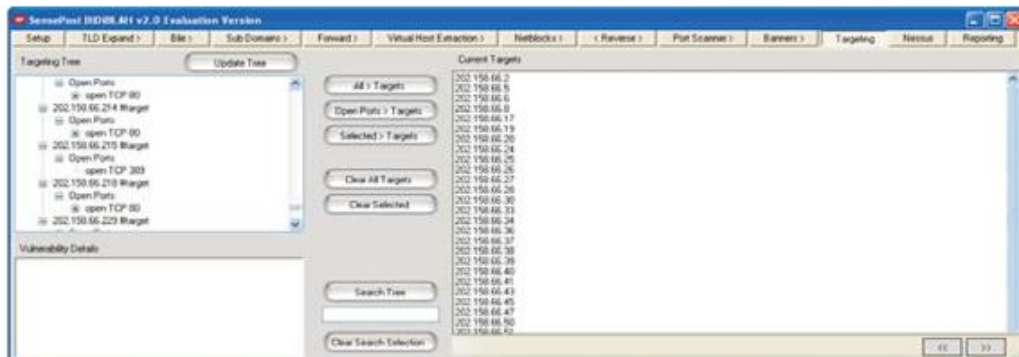


Port Scanner, akan memeriksa port-port mana saja yang terbuka pada setiap alamat IP yang ada. Anda juga bisa menentukan port-port mana saja yang akan diperiksa disini. Memeriksa semua port yang ada memakan waktu yang terlalu lama karena itu pemeriksaan biasanya dilakukan hanya pada port yang umum digunakan seperti 21,22,25,80, dst. Jika Anda menggunakan windows XP, firewall Anda akan di-nonaktifkan sementara waktu secara otomatis agar program bisa dijalankan dengan baik.

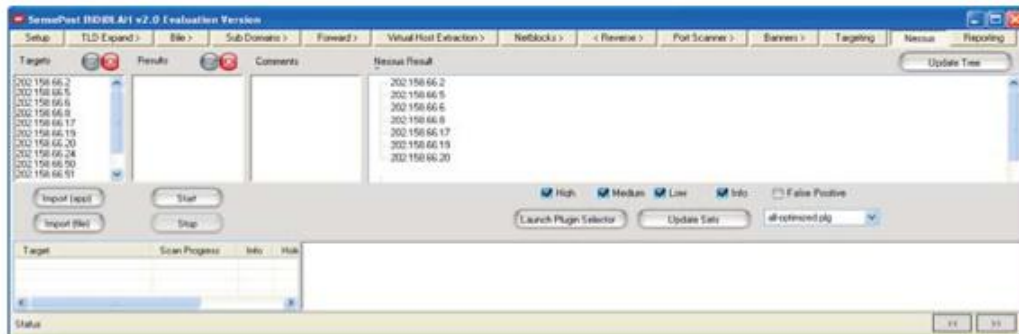


Setelah mengetahui port-port yang terbuka, tools *Banners*, akan mencoba melakukan koneksi ke port tersebut untuk mendapatkan

banner yang mungkin saja menarik untuk Anda. Melalui banner yang ditampilkan ini, biasanya bisa diketahui banyak hal seperti jenis software yang digunakan, versi, dan informasi menarik lainnya. Sama seperti dengan fungsi *Port Scanner*, jika Anda menggunakan XP, firewall komputer Anda juga akan di-nonaktifkan untuk sementara waktu secara otomatis.



Targeting, digunakan untuk menentukan komputer target atau korban yang akan diperiksa kelemahannya. Komputer korban dengan port-port yang terbuka beserta dengan bannernya yang didapatkan pada proses sebelumnya akan ditampilkan dalam bentuk tree yang mudah dan nyaman untuk dilihat pada kolom sebelah kiri.



Pada tabulasi *Nessus*, Bibiblah akan memanfaatkan security scanner Nessus dalam melakukan penetrasi atau pengecekan kelemahan yang ada pada komputer korban karena itu, mutlak dibutuhkan adanya *Server Nessus*. Alamat IP yang ada disini, didapatkan pada tabulasi *Targeting* yang telah Anda tentukan sebelumnya. Dengan mengetahui kelemahan-kelemahan yang ada melalui laporan yang diberikan oleh Nessus, hacker bisa menguasai komputer korban .



Terakhir, *Reporting* akan menghasilkan laporan yang nyaman untuk dilihat. Dengan laporan ini, Anda bisa melihat segala informasi yang didapatkan dari proses awal sampai dengan akhir.

Qualys

Qualys Web Based Scanner (<http://www.qualys.com>), adalah perusahaan yang menawarkan jasa *vulnerability scanning* dengan cara yang unik dan cerdas. Berbeda dengan produk-produk *vulnerability scanner* yang lain, Qualys tidak menjual software namun menjual services atau layanan yang diberikan secara online melalui web/internet.

Qualys akan melakukan penetrasi secara otomatis ke jaringan client untuk mencari kelemahan yang ada dan melaporkannya dalam format yang mudah untuk dilihat serta disertai pula dengan penjelasan detail mengenai kelemahan yang ada beserta akibat dan solusi yang perlu dilakukan.

Berbeda dengan produk lainnya, Qualys juga menawarkan *Vulnerability Management*. *Vulnerability Management* memudahkan Anda dalam menangani dan menyelesaikan permasalahan-permasalahan yang didapatkan pada tahapan *vulnerability scanning*. Anda bisa melihat komputer dan permasalahan apa saja yang telah diselesaikan, bagian mana yang belum diselesaikan, bagian mana yang perlu mendapatkan prioritas dan lain sebagainya.

Kemampuan ini membuat Qualys banyak digunakan oleh perusahaan-perusahaan besar di dunia. Selain itu, Qualys juga unik karena

layanannya diberikan secara online melalui web, sehingga tidak diperlukan instalasi yang rumit pada sisi client dan juga tidak perlu adanya pemeliharaan software seperti update database vulnerability dan lain sebagainya yang ujung-ujungnya tentu saja mengurangi biaya dan pekerjaan yang harus dilakukan oleh perusahaan.




[Print](#)
[Download](#)
[Quick Help](#)

FreeScan Report

Detailed Results
09/30/2004

64.41.134.60 (demo02.qualys.com, DEMO02)
Windows 2000/XP

Vulnerabilities Total 34
 Security Risk 5.0

Vulnerabilities (34)

- MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability**
port 1434/udp
- Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability**
port 80/tcp
- Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability**
port 10080/tcp
- Microsoft Windows Media Services NSISlog.DLL Remote Buffer Overflow Vulnerability**
port 10080/tcp
- Microsoft SQL Server 2000 SP1 Not Installed**
port 1433/tcp
- Microsoft SQL Server 2000 SP2 Not Installed**
port 1433/tcp
- Microsoft SQL Server Service Pack 3 Not Installed**
port 1433/tcp
- Remote Windows User List Disclosure Vulnerability**
- Microsoft Windows Task Scheduler Code Execution (MS04-022)**
- Microsoft IIS Administrative Pages Cross-Site Scripting Vulnerability**
port 80/tcp
- Microsoft IIS Malformed HTR Request Buffer Overflow Vulnerability**
port 80/tcp

OID: 10577 **Category:** CGI **CVE ID:** [CVE-2002-0071](#)

Vendor Reference: N/A

THREAT:

It's been reported that a heap overflow condition exists in the HTR ISAPI extension in Microsoft Internet Information Server (IIS) Versions 4.0 and 5.0.

By sending a series of specially malformed HTR requests, it could be possible for a malicious user to cause the IIS service to fail. Additionally, under a very difficult operational scenario, it could be possible to cause code to run on the server.

IMPACT:

If this vulnerability is successfully exploited, a malicious user could cause a denial of service condition or execute arbitrary instructions on the vulnerable host.

SOLUTION:

Microsoft released an IIS cumulative patch to address several vulnerabilities, including this one. For more information regarding these IIS vulnerabilities and for patch download locations and instructions, read [Microsoft Security Bulletin MS02-018](#).

There are reports of problems with the cumulative patch for users who are running Microsoft IIS Site Server. A hotfix to address problems caused as a side effect of installing the cumulative patch has been released by Microsoft. Any users who have experienced difficulties as a result of installing the cumulative patch are advised to contact Microsoft support and request hotfix Q317915.

RESULT:

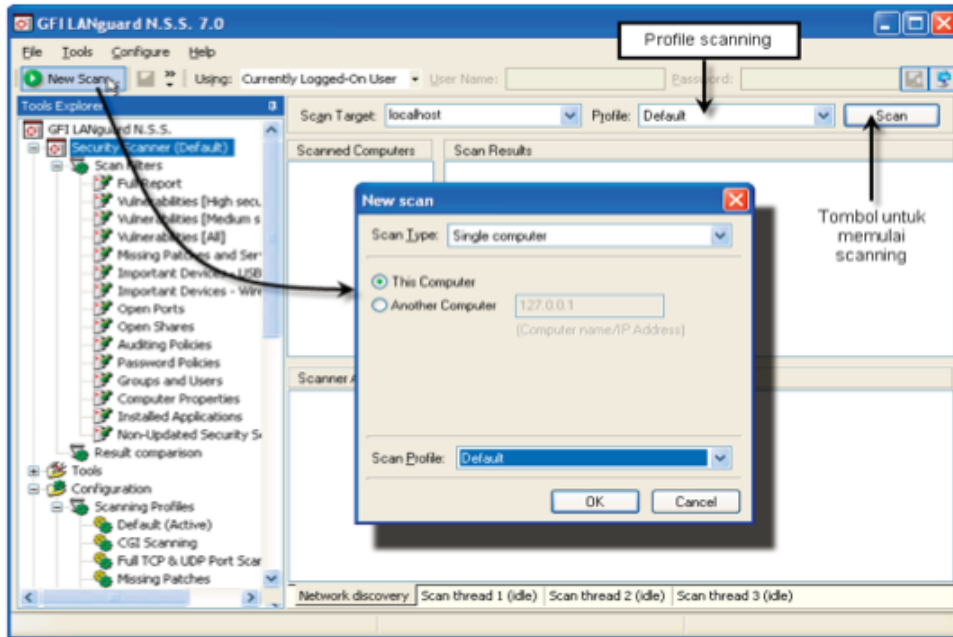
No results available

- Microsoft IIS HTR ISAPI Extension Heap Overflow Vulnerability**
port 80/tcp
- Null Session/Password NetBIOS Access**

Contoh Laporan Vulnerabilities yang dilaporkan oleh Qualys.



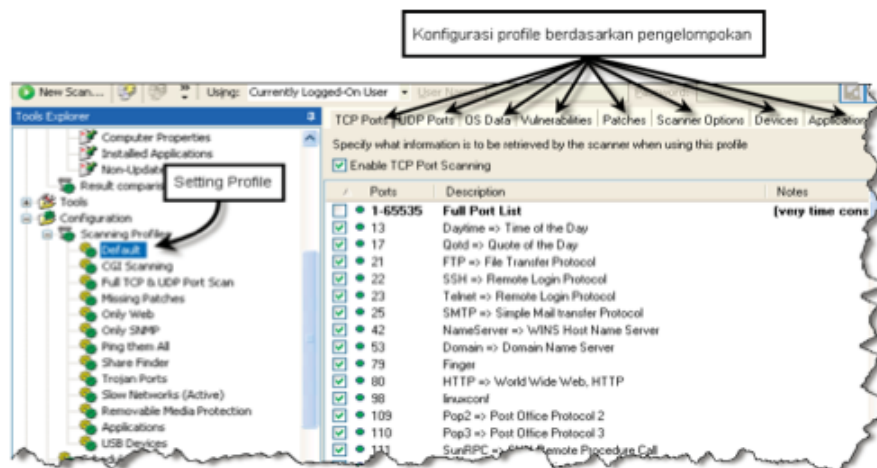
Vulnerability Scanner *GFI LANguard* (www.gfi.com/lannetscan) merupakan salah satu scanner yang cukup kompleks dengan banyak kemampuan.



Untuk melakukan scanning, Anda hanya perlu mengklik tombol wizard “New Scan” yang akan menuntun Anda dengan pilihan pertama berupa penentuan host atau komputer yang hendak di scan. Pada bagian ini, yang perlu Anda perhatikan adalah profile yang digunakan untuk melakukan scanning. Profile ini menentukan bagaimana proses scanning akan dijalankan terhadap komputer target.

Sebagai contoh, saya menggunakan profile dengan nama “Default” yang merupakan setting yang paling umum digunakan. Jika Anda klik menu *Configuration* → *Scanning Profiles* → *Default* pada Tools Explorer yang berada di kolom sebelah kiri, Anda bisa melihat konfigurasi untuk profile Default ini.

Setting pada profile Default ini akan ditampilkan pada kolom sebelah kanan yang terbagi atas beberapa tabulasi, diantaranya TCP Ports, UDP Ports, OS Data, Vulnerabilities, Patches, Scanner Options, dll.



Setting Default pada tabulasi TCP Ports terlihat hanya meminta scanner untuk melakukan pengecekan terhadap port-port yang sudah umum digunakan seperti port 13, 17, 21, dst. Andaikan komputer target ternyata membuka sebuah port 10, maka scanner tidak akan menemukannya. Anda bisa merubah setting ini apabila Anda menginginkan scanner memeriksa semua port yang ada (1-65535).

Scanner tidak melakukan pengecekan terhadap semua port yang ada karena hal tersebut akan memakan waktu yang cukup lama. Bayangkan saja apabila pengecekan 1 port membutuhkan waktu sekitar 6 detik, maka Anda harus siap-siap menunggu untuk waktu yang cukup lama ($6 \times 65.535 = 393.210$ detik atau 6.553,5 menit). Dan ini hanya pengecekan TCP port, belum lagi pengecekan UDP Ports, Pengecekan kelemahan, dll.

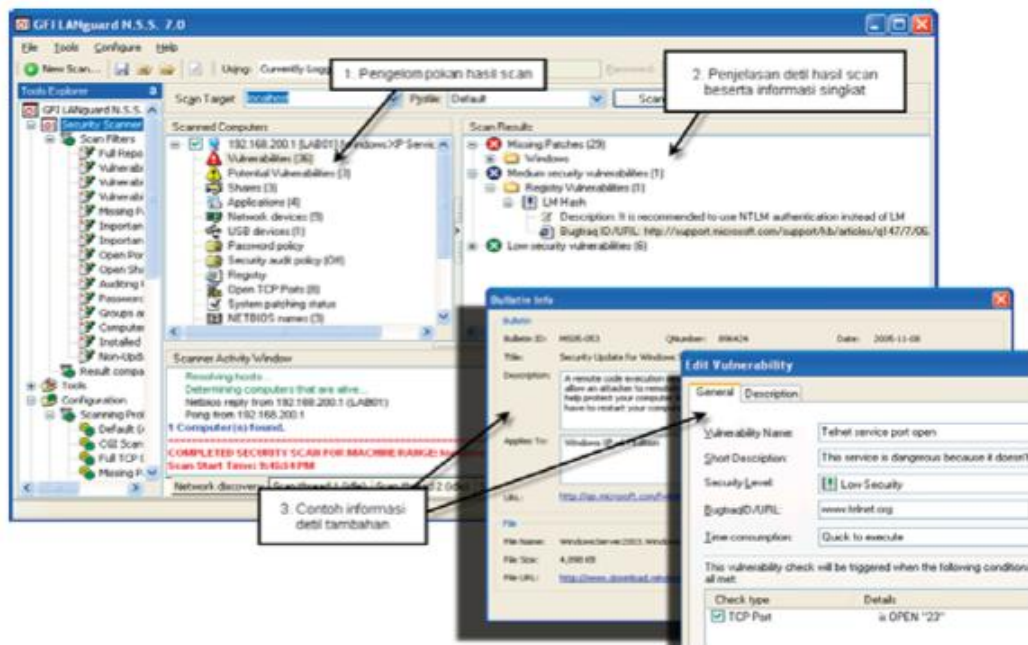
Profile *Default*, bukanlah profile yang cocok untuk segala kondisi. Terkadang Anda harus merubah setting ini atau menggunakan profile yang cocok dengan lingkungan yang Anda hadapi. Misalnya Anda melakukan pengecekan komputer yang ada di internet dengan koneksi yang cukup lambat. Untuk itu, Anda sebaiknya menggunakan profile *Slow Networks* yang memberikan waktu yang lebih lama kepada scanner untuk melakukan pemeriksaan.

Sebagai contohnya, pada setting *Default*, scanner akan mencoba melakukan koneksi ke port dan mengharapkan adanya balasan dalam waktu 3 detik. Apabila dalam 3 detik tidak ada respon dari

target, maka scanner akan menganggap bahwa port tersebut tertutup dan pemeriksaan akan dilanjutkan pada port berikutnya.

Waktu 3 detik mungkin tidak cukup bila Anda memeriksa komputer yang berada di internet apalagi Anda menggunakan koneksi Dial Up yang lambat. Belum sempat komputer target memberikan jawaban, scanner Anda sudah menganggap tidak ada jawaban. Akibatnya adalah kesalahan yang membuat proses scanning menjadi tidak akurat.

Pada profile *Slow Networks*, waktu yang diberikan untuk memeriksa sebuah port TCP adalah 6 detik yang diharapkan sudah merupakan angka yang bisa diterima. Tentu saja, apabila koneksi Anda ternyata masih terlalu lambat, Anda bisa merubah setting semacam ini pada profile yang Anda gunakan atau Anda bisa juga membuat sebuah profile baru yang sesuai dengan kebutuhan Anda.



Setelah proses scanning selesai dilakukan, Anda bisa melihat hasil scan (1) yang dikelompokkan berdasarkan jenis informasi atau kelemahan yang ditemukan. Misalnya, Anda akan mendapatkan laporan service pack mana saja yang belum terinstall (terutama jika Anda melakukan scanning terhadap komputer lokal) dan juga

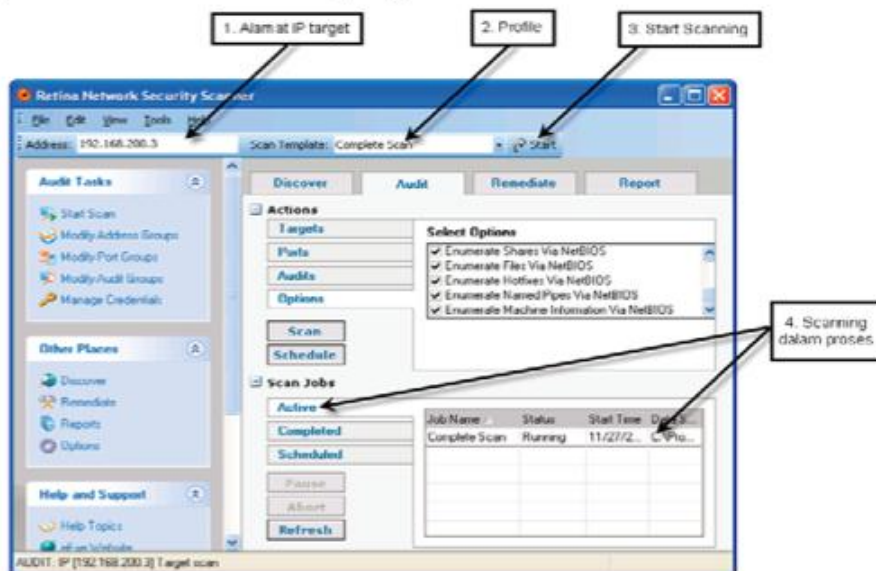
berbagai potensi kelemahan yang mungkin terjadi dimasa mendatang dan lain sebagainya.

Anda bisa melihat lebih detail informasi yang didapatkan dari hasil scanning ini di kolom sebelah kanan (2). Informasi yang lebih detail lagi bisa Anda lihat dengan cara mengklik keterangan tersebut (3). GFI LANguard bahkan menyertakan rekomendasi untuk Anda tentang apa yang bisa Anda lakukan untuk mengatasi kelemahan yang berhasil ditemukan. Jadi dengan cara yang sangat mudah, Anda sudah bisa menjadi seorang auditor security.

🌀 Retina

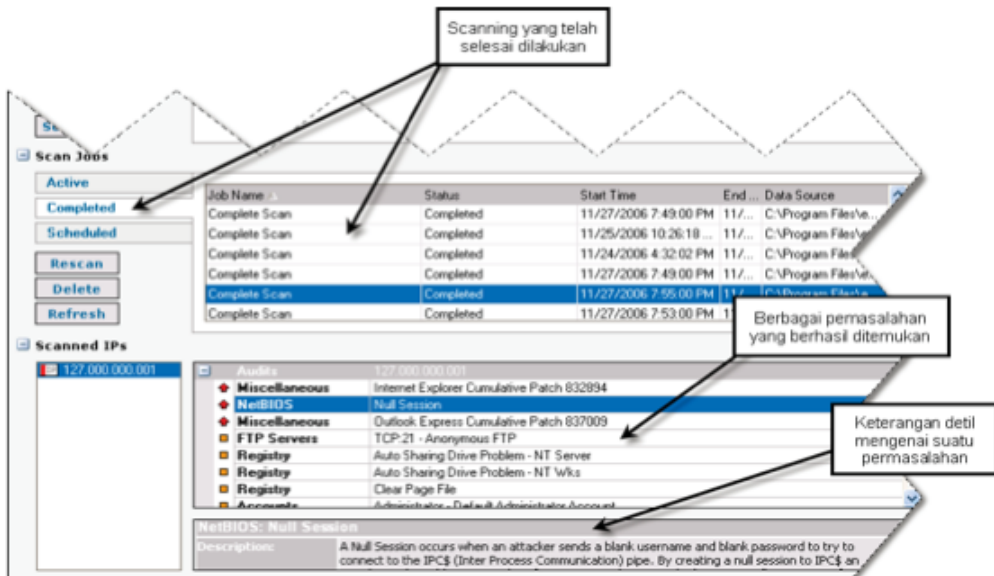
Security Scanner lainnya yang cukup terkenal ada Retina yang dibuat oleh perusahaan www.eeye.com. Perusahaan yang memang bergerak dibidang keamanan komputer ini cukup dikenal di dunia ini karena banyak kelemahan kritis windows ditemukan oleh pekerja-pekerja dari eEye ini.

Mungkin karena pekerja yang terlalu pintar dan teknis, software Retina yang dihasilkan perusahaan ini merupakan produk yang sangat bagus namun interface yang sangat buruk. Tidak mudah untuk bisa menggunakan produk ini dengan nyaman tanpa melihat dengan teliti tombol mana yang harus diklik.



Dengan sedikit kebiasaan, Anda tidak akan mengalami kesulitan menggunakan program Retina ini karena pada dasarnya, penggunaan scanner semacam ini tidak jauh berbeda. Anda tinggal memasukkan alamat IP komputer target (1), menentukan profile yang akan digunakan untuk proses scanning (2), dan mengklik tombol scan (3) untuk memulai proses scanning.

Scanning yang sedang terjadi bisa Anda lihat pada bagian *Scan Jobs* (4). Setelah proses scanning selesai, scanning yang terlihat di kotak sebelah kanan bawah akan segera hilang tanpa adanya peringatan ataupun informasi apapun. Satu lagi yang membingungkan !

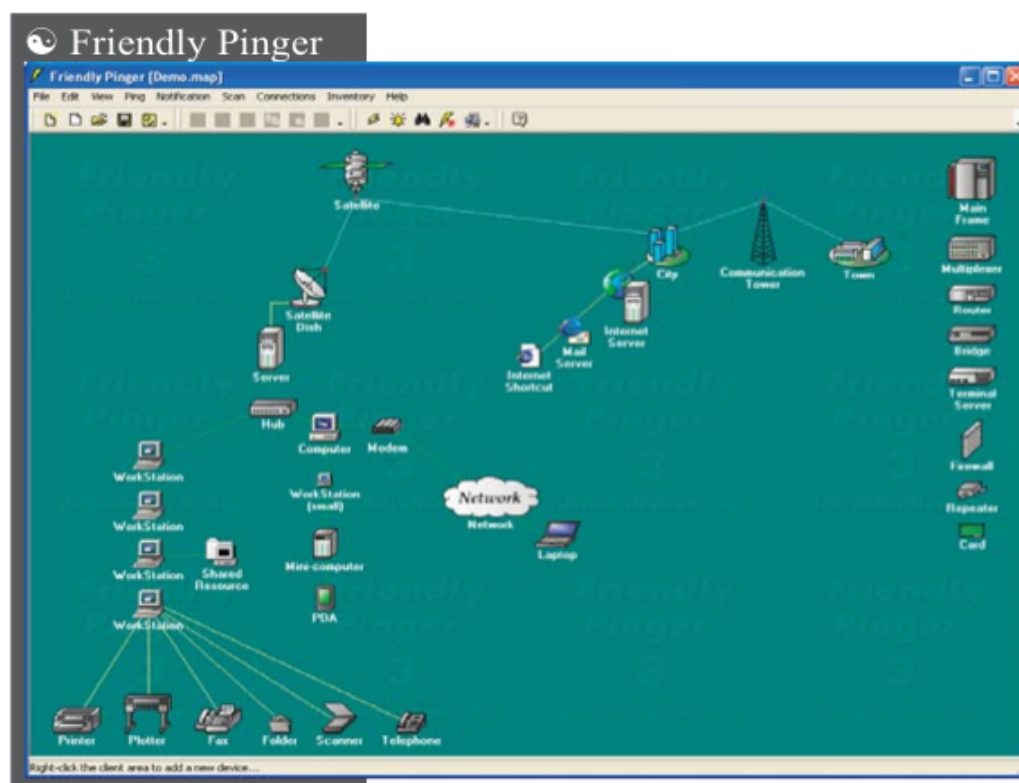


Untuk melihat hasil scanning, Anda bisa mengklik tombol *Completed* yang akan memperlihatkan semua tugas scan yang telah diselesaikan. Anda bisa mengklik tugas (job) yang sudah selesai ini untuk melihat secara detail apa yang ditemukan oleh scanner ini.

Anda bisa mengunjungi situs <http://sectools.org/> yang melaporkan tools-tools favorit yang digunakan oleh hacker ataupun para security profesional.

6. Menggambarkan diagram network dari host yang bermasalah (Vulnerable hosts)

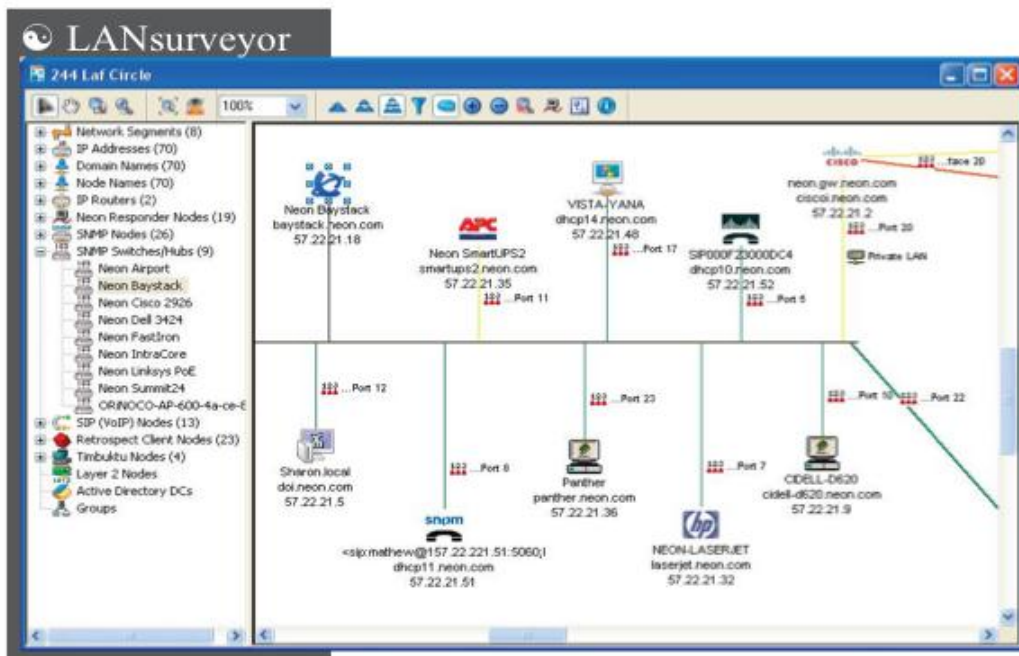
Sebuah gambar setara dengan seribu kata, hal ini karena manusia lebih mudah menangkap dalam bentuk visualisasi. Dengan menggambarkan jaringan dari jaringan korban berdasarkan informasi yang didapatkan dari proses awal, hacker bisa menganalisa dengan lebih mudah untuk menemukan titik lemah yang bisa dijadikan sebagai pintu masuk. Pemetaan jaringan ini bisa dilakukan secara manual seperti dengan visio namun beberapa tools bisa membantu dalam hal pemetaan jaringan ini. Umumnya software ini digunakan oleh administrator jaringan.



Friendly Pinger, software komersial buatan *Andrey Kilievich* (www.kilievich.com) yang dijual dengan harga \$68 ini memungkinkan Anda membuat pemetaan jaringan secara visual yang tampak cantik sekali.

Pemetaan awal bisa dilakukan secara otomatis melalui pengecekan yang dilakukan secara software namun Anda jangan berharap software ini bisa menggambarkan seluruh jaringan Anda dengan baik dan benar karena Anda akan lebih banyak melakukannya secara manual dengan menambahkan setiap peralatan yang ada.

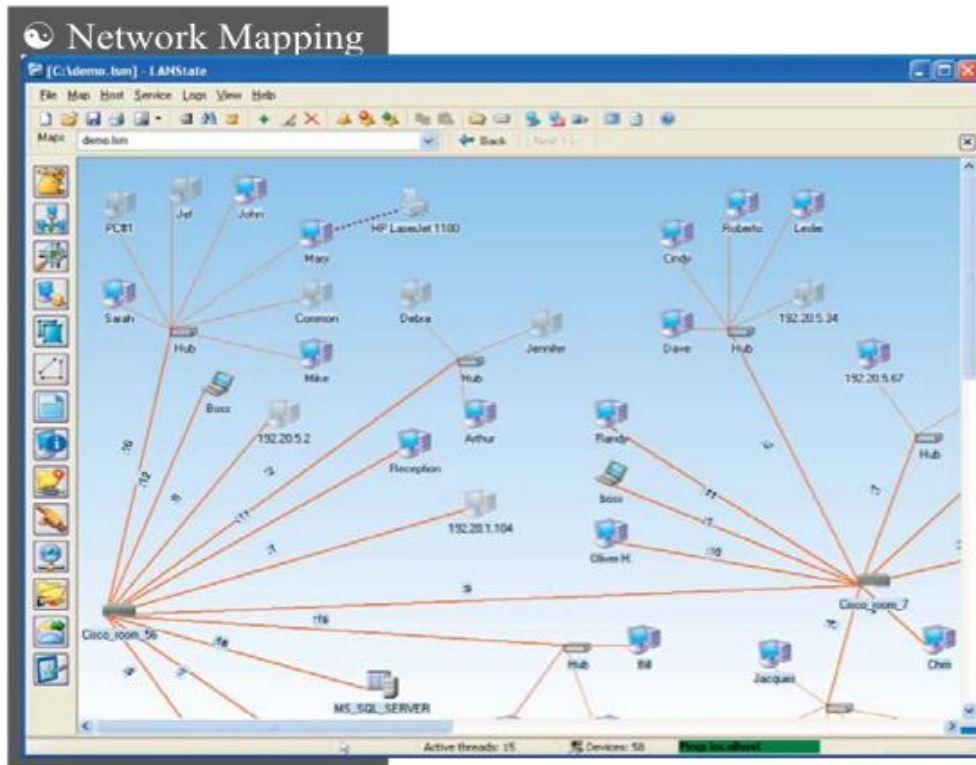
Dari pemetaan yang telah dilakukan, Anda bisa mengklik komputer yang ada didalam gambar dan menjalankan perintah seperti ping, traceroute, dan lain sebagainya. Selain itu, Anda juga bisa memberikan informasi detail dari setiap peralatan yang ditunjukkan oleh Friendly Pinger seperti nama komputer, merk, jenis prosesor, sistem operasi yang digunakan, dan lain sebagainya.



LANsurveyor (www.solarwinds.com) Pada saat pertama kali dijalankan, LANsurveyor akan mencari informasi komputer-komputer yang ada pada jaringan Anda kemudian menggambarkan devices yang ditemukan ini menjadi peta jaringan.

LANsurveyor lebih kompleks dan menggunakan banyak metode untuk menemukan komputer-komputer yang ada didalam jaringan dibandingkan dengan Friendly Pinger sehingga keakuratannya jauh lebih tinggi.

Selain membuat peta jaringan, dengan LANsurveyor, Anda juga bisa memantau performance dari komputer-komputer yang ada didalam jaringan serta menjalankan berbagai perintah remote seperti shutdown, telnet, VNC, Remote Desktop, Mengirim file, pesan dan lain sebagainya. Dengan software ini, infrastruktur yang rumit tampak menjadi lebih sederhana. Seperti halnya dengan *Friendly Pinger*, Anda juga bisa menambahkan, merubah ataupun menghapus secara manual peralatan yang ada.



Seperti software Network Mapping lainnya, LANState (www.10-strike.com/lanstate/) ini juga bisa mendeteksi secara otomatis komputer-komputer yang ada didalam jaringan dengan metode yang hampir sama dengan Friendly Pinger.

Software ini juga menawarkan administrasi komputer-komputer yang ada dalam peta. Anda bisa melihat secara realtime komputer yang aktif maupun tidak. Anda bisa mematikan ataupun merestart komputer dari jarak jauh dan Anda juga bisa memberikan informasi

tentang komputer yang sedang dimonitor dan menambahkan devices secara manual.

Selain software yang telah diinformasikan, masih banyak software Network Mapping lainnya yang sangat berguna misalnya Insightix Visibility (www.insightix.com), SolarWinds Toolset, Queso, Cheops, dll.

7. Menyiapkan proxy

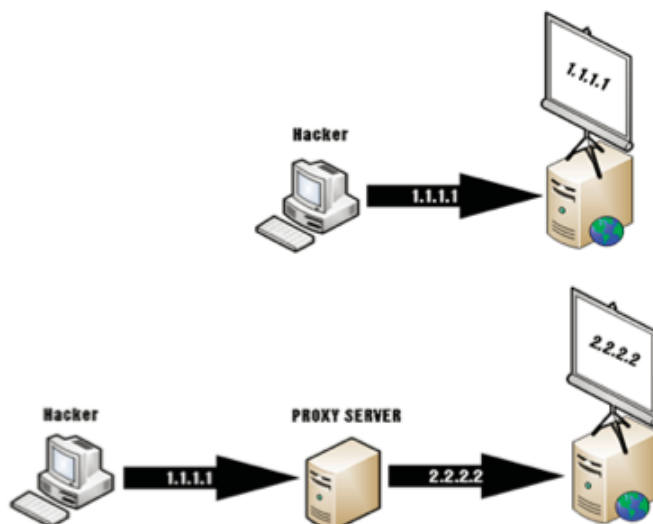
Setelah semua informasi, termasuk kelemahan dan pintu masuk yang bisa digunakan terhadap korban diketahui, hacker kini sudah bisa menerobos ke dalam jaringan korban namun hacker biasanya tidak akan terburu-buru melakukannya. Hotel gratis dibalik jeruji besi tentu bukan pilihan yang menarik, apalagi ada kabar burung yang mengatakan banyak kasus pelecehan seksual disitu. Hacker perlu menyembunyikan dirinya dan Proxy adalah jawabannya !

Proxy bisa diartikan sebagai perantara, sebuah aplikasi atau server yang berdiri ditengah-tengah antara client (hacker) dan server tujuan. Ketika hacker melakukan permintaan, permintaan tersebut tidak langsung disampaikan kepada server tujuan namun disampaikan kepada proxy server yang akan menyampaikannya kepada server tujuan mewakili hacker.

Jika hacker mengakses sebuah server secara langsung, alamat IP dari sang hacker akan tercatat pada komputer server. Dengan bantuan dari whois server, berdasarkan alamat IP yang ada bisa dicari pemilik alamat IP yang biasanya adalah alamat IP perusahaan atau alamat IP suatu ISP. Pihak berwenang, selanjutnya tinggal mencari perusahaan atau ISP untuk mengetahui secara pasti siapa penggunaanya dan tamatlah sudah cerita untuk sang hacker.

Dengan bantuan proxy server, keadaannya menjadi berbeda. Untuk mengakses server korban, hacker memanfaatkan proxy server. Secara teknis, semua permintaan dari hacker akan diberikan kepada proxy dan proxy akan menyampaikan permintaan ini kepada server korban. Server korban, hanya mengetahui proxy server karena itu, alamat IP dari proxy server akan tercatat oleh server korban namun

alamat IP dari hacker tidaklah diketahui oleh server korban. Hacker menjadi aman? Tergantung.



Dengan adanya proxy server, menangkap hacker menjadi jauh lebih sulit karena komputer korban hanya mengetahui alamat IP dari proxy server. Untuk mengetahui alamat IP dari hacker, informasi dari proxy server adalah satu-satunya cara.

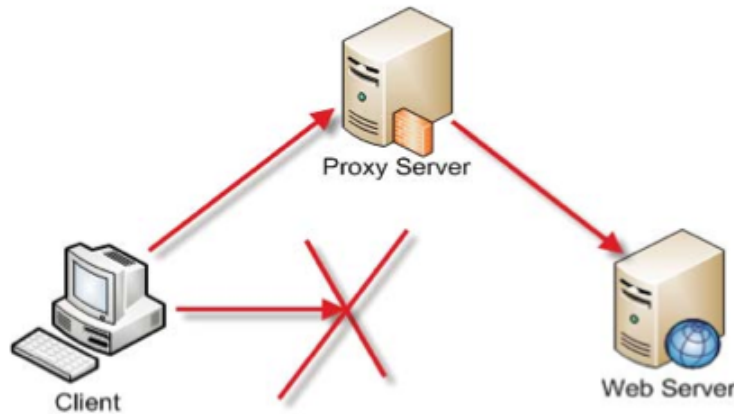
Apabila proxy server mencatat penggunaanya atau komputer-komputer yang menggunakan layanannya, maka identitas atau alamat IP dari komputer hacker bisa diketahui. Hal ini biasanya sulit dilakukan karena ada saja server yang tidak melakukan pencatatan dengan baik, ada pula yang pencatatannya sudah dihapus dan ada pula yang karena berada pada negara yang berbeda dengan hukum yang berbeda, sehingga pemeriksaan secara legal tidak bisa dilakukan.

Kegunaan Proxy Server

Proxy server mempunyai banyak kegunaan dan tentu saja bukan teknologi yang sengaja diciptakan untuk urusan hacking. Sebagai contoh, proxy sever bisa menghemat bandwidth karena proxy server bisa menyimpan halaman web site yang sering diakses kemudian menyediakan halaman tersebut kepada pengguna lain secara langsung dengan memanfaatkan halaman yang telah disimpan

sebelumnya. Jenis proxy ini banyak diimplementasikan oleh perusahaan-perusahaan dan ISP.

Proxy server juga bisa menjadi media sensor. Proxy server bisa memfilter informasi-informasi atau situs-situs yang tidak diinginkan. Hal ini tentu saja bisa dilakukan karena semua permintaan dari client, melalui proxy server sehingga proxy server bisa memutuskan apa yang akan dilakukan terhadap permintaan tersebut.



Fungsi yang lain, proxy server juga bisa digunakan untuk melewati proteksi. Sebagai contoh, ketika pemerintah china melakukan proteksi terhadap situs google, banyak pengakses dari china memanfaatkan proxy untuk melewatinya. Kasus yang sama ketika perusahaan membatasi Anda mengakses situs tertentu, misalnya situs *jasakom.com*, Anda bisa melewati proteksi semacam ini dengan proxy server.

Kasus lain lagi yang seringkali terjadi adalah proteksi dari webserver terhadap alamat IP tertentu seperti situs *rapidshare.com* yang bisa diatasi dengan memanfaatkan proxy server sehingga Anda tidak perlu menunggu batasan waktu yang diberikan. Fungsi ini memang saling berlawanan dimana proxy server bisa digunakan untuk melakukan proteksi namun proteksinya sendiri juga bisa dilewati dengan memanfaatkan proxy server yang lain.

Fungsi yang akan banyak kita bahas pada bagian ini adalah kegunaannya dalam menyembunyikan identitas asli penggunanya.

Anonymous proxy dan Free Proxy Server

Banyak yang menyamakan *Free Proxy Server* dengan *Anonymous proxy* yang sebenarnya berbeda. *Free Proxy Server* adalah proxy server yang tersedia dan bisa digunakan secara gratis oleh semua orang.

Proxy semacam ini ada yang memang sengaja disediakan untuk digunakan secara bebas namun ada juga yang tersedia karena salah konfigurasi sehingga menyebabkan semua orang bisa menggunakan proxy tersebut secara bebas. Selain itu, ada juga proxy server yang tersedia karena diaktifkan oleh hacker / worm / virus. *Free Proxy* bisa saja menyembunyikan identitas penggunanya namun ada yang juga tidak.

Proxy server yang tidak menyembunyikan identitas pemakainya (client), dinamakan sebagai *transparent proxy*. Karena proxy ini tidak menyembunyikan identitas pemakainya, server yang Anda akses akan mengetahui bahwa Anda masuk ke situs mereka melalui proxy dan alamat IP Anda juga diketahui.

Fungsi utama dari proxy semacam ini adalah agar Anda bisa browsing dengan lebih cepat, karena proxy ini menyimpan halaman-halaman yang pernah diakses oleh client-nya, dan menampilkan halaman yang sama tanpa menghubungi web server lagi ketika ada permintaan yang sama dilakukan. Proxy jenis ini banyak digunakan oleh perusahaan-perusahaan untuk menghemat bandwidth.

Anonymous Proxy adalah proxy yang menyembunyikan identitas penggunanya seperti alamat IP sehingga server yang diakses tidak mengetahui alamat IP dari client yang sebenarnya. Di dalam dunia cyber, jenis proxy ini masih dibedakan lagi.

Anonymous Proxy biasanya menunjukkan proxy yang menyembunyikan alamat IP penggunanya namun server yang diakses, tetap bisa mendeteksi bahwa pengaksesnya menggunakan proxy server dengan mudah.

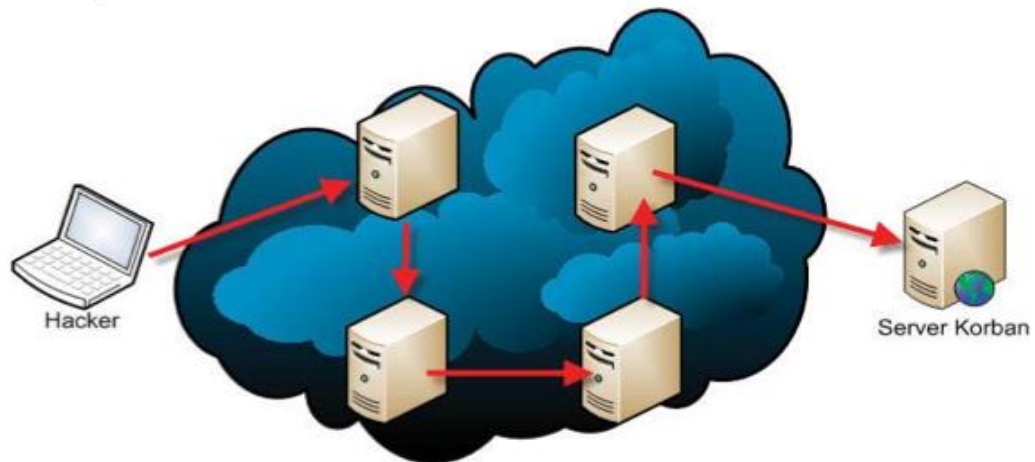
Level anonymous proxy yang lebih tinggi lagi sering dikategorikan sebagai *High Anonymous Proxy Server*. Jenis proxy ini selain menyembunyikan alamat IP dari client-nya, juga membuang berbagai informasi lainnya yang bisa digunakan untuk mengidentifikasi adanya proxy server sehingga web server menjadi sulit untuk

mengetahui keberadaan proxy server dan menganggap client mengakses secara langsung.

Banyak yang salah pengertian dengan level anonymous suatu proxy server. Server anonymous bukan berarti server ini akan menjaga identitas Anda yang (mungkin) tercatat didalam server mereka. Pemilik proxy, mungkin saja memberikan informasi mengenai Anda kepada teman-temannya atau kepada siapapun yang meminta informasi ini. Bukan suatu yang aneh, sebuah proxy gratis yang sengaja dibuat untuk mencuri data-data dari penggunanya karena itu, penggunaan proxy secara sembarangan bisa berbahaya.

Beberapa layanan dari Anonymous proxy berbayar, memberikan jaminan tidak akan mencatat segala informasi tentang apa yang Anda lakukan. Anda boleh percaya dan boleh saja tidak terhadap layanan semacam ini karena tidak ada cara untuk membuktikannya.

Untuk meningkatkan tingkat anonymous dan juga tingkat keamanan pemakai, termasuk menghindari pelacakan yang mungkin dilakukan oleh pihak berwajib, ada teknik lain lagi yang sering digunakan oleh hacker yaitu dengan menggunakan beberapa proxy server sekaligus.



Sebagai contoh, permintaan Anda akan diberikan kepada Proxy A, selanjutnya Proxy A akan memberikan permintaannya kepada Proxy B, dan Proxy B ke Proxy C yang kemudian diteruskan lagi ke Proxy D. Dari proxy terakhir yang dalam kasus ini adalah Proxy D, barulah permintaan benar-benar disampaikan kepada server korban.

Dengan teknik ini, untuk melacak hacker sangatlah sulit dan biasanya sudah tidak memungkinkan lagi karena berbagai kesulitan, baik teknis (pencatatan log) maupun non-teknis (batas negara, aturan, undang-undang, dlsb). Rangkaian proxy-proxy ini kita namakan sebagai *proxy chains*.

Anda mungkin tidak akan pernah percaya bila tidak melihatnya sendiri. Terdapat ribuan proxy server di dunia ini dan hebatnya lagi proxy-proxy ini mirip dengan ikan lele, timbul dan tenggelam dengan cepat. Anda bisa mencari proxy server gratis dengan search engine seperti google dengan mengetikkan kata kunci sederhana seperti *"Free Proxy servers"*.

Dari hasil pencarian, Anda bisa melihat banyak sekali situs-situs yang menampilkan daftar proxy server yang terdeteksi dan bisa digunakan. Situs ini bahkan secara berkala melakukan pengecekan apakah proxy-proxy masih bisa digunakan atau tidak dan selalu berusaha mencari proxy yang baru muncul ke permukaan.



Sebagai contoh, Anda bisa melihat situs *www.proxy4free.com*, *www.proxiz.com*, *www.multiproxy.org*, *www.publicproxyservers.com*, *www.anonymitychecker.com*, dan lain sebagainya. Situs seperti *proxy4free* bahkan juga menyediakan menu yang akan membantu Anda mengecek level anonymous sebuah proxy.

Ribuan proxy server yang Anda dapatkan pada situs-situs ini tampaknya memang sangat menyenangkan dan mudah namun Anda akan sadar ketika mulai mencoba menggunakan satu persatu proxy ini. Sebagian besar ternyata tidak bisa digunakan!

Waktu Anda mungkin akan terbuang berjam-jam hanya untuk menemukan satu saja proxy yang bisa digunakan dan itupun mungkin berlangsung tidak terlalu lama sampai Anda harus mencari lagi proxy pengganti.

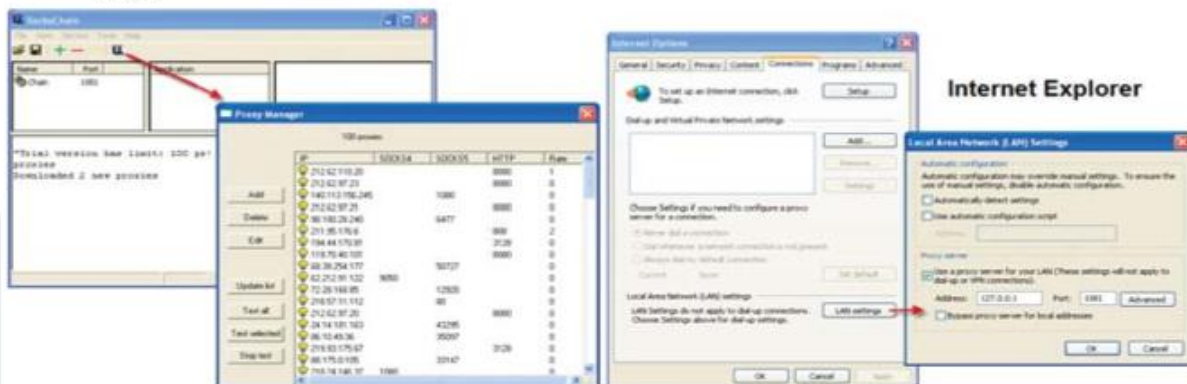
Tidak heran, akhirnya banyak aplikasi dibuat untuk memudahkan pekerjaan pengecekan dan pemanfaatan proxy ini agar bisa berlangsung dengan lebih otomatis. Ada program yang secara otomatis mengambil daftar proxy yang sudah disediakan oleh situs-situs seperti *proxy4all*, dkk-nya namun ada juga yang manual. Artinya, Anda harus mengambil sendiri daftar yang ada kemudian memasukkan kedalam program pembantu ini. Sebagian besar program yang akan kita bahas selanjutnya memungkinkan Anda memasukkan daftar proxy untuk diperiksa secara otomatis.

SocksChains

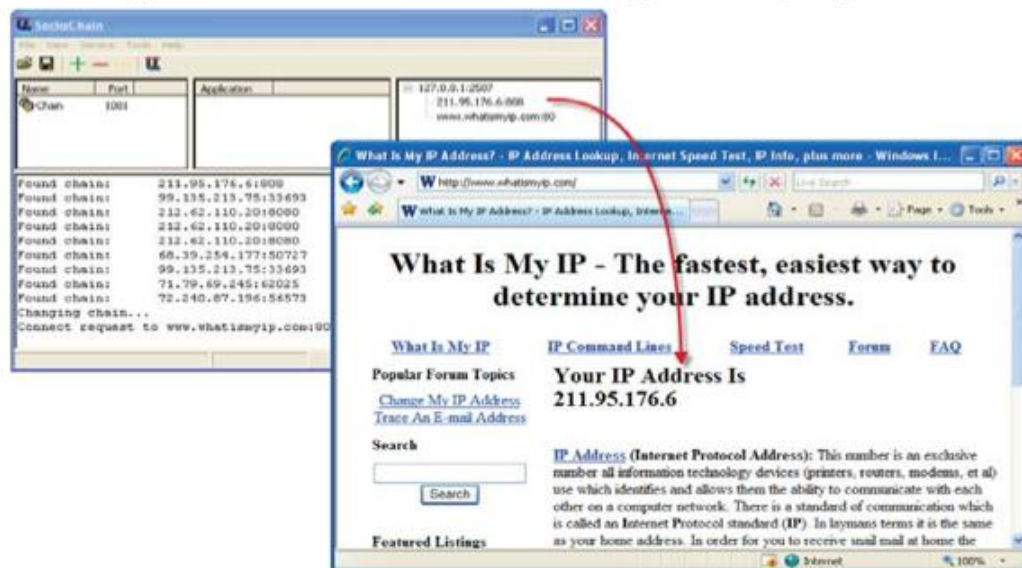
SocksChains (*www.ufasoft.com/socks*), menawarkan koneksi kedalam jaringan *proxy chains* yang diambil dari proxy-proxy yang tersebar didunia ini. Anda bisa menentukan jumlah chain (proxy) yang akan digunakan yang akan semakin meningkatkan keamanan Anda namun akibat sampingannya adalah koneksi yang Anda dapatkan akan semakin lambat.

Pada saat pertama kali dijalankan, program *SocksChains* secara otomatis akan membuat sebuah proxy di lokal komputer Anda pada port 1081 yang bisa dilihat pada kolom kiri atas. Anda juga bisa melihat proxy-proxy yang digunakan oleh proxy chains dengan mengklik icon *Proxy Manager*. Kecepatan yang Anda dapatkan, sangatlah tergantung pada proxy-proxy ini.

Selanjutnya, Anda perlu melakukan perubahan pada aplikasi yang akan memanfaatkan proxy chains ini. Sebagai contoh, bila Anda menggunakan Internet Explorer, Anda bisa merubahnya pada menu *Tools* → *Internet Options* → *Connections* → *LAN Settings* → *Proxy Server*. Isilah dengan alamat *sockschains* yaitu *Address* 127.0.0.1 dengan *Port* 1081.



Setelah melakukan setting, kini Anda bisa menjalankan aktifitas browsing seperti biasa. Semua koneksi yang Anda lakukan kini akan melalui proxy chains yang menjamin keamanan Anda. Untuk memastikan bahwa koneksi Anda benar-benar telah menggunakan proxy ini, Anda bisa mengecek alamat IP Anda pada situs *www.whatismyip.com* sebelum dan setelah menggunakan proxy chains.



Sebagai penutup untuk *proxychains* ini, perlu saya ingatkan sekali lagi bahwa kecepatan koneksi Anda sangatlah tergantung pada proxy server yang Anda dapatkan. Seringkali, koneksi ini sangat lambat yang mengakibatkan gagalnya koneksi.



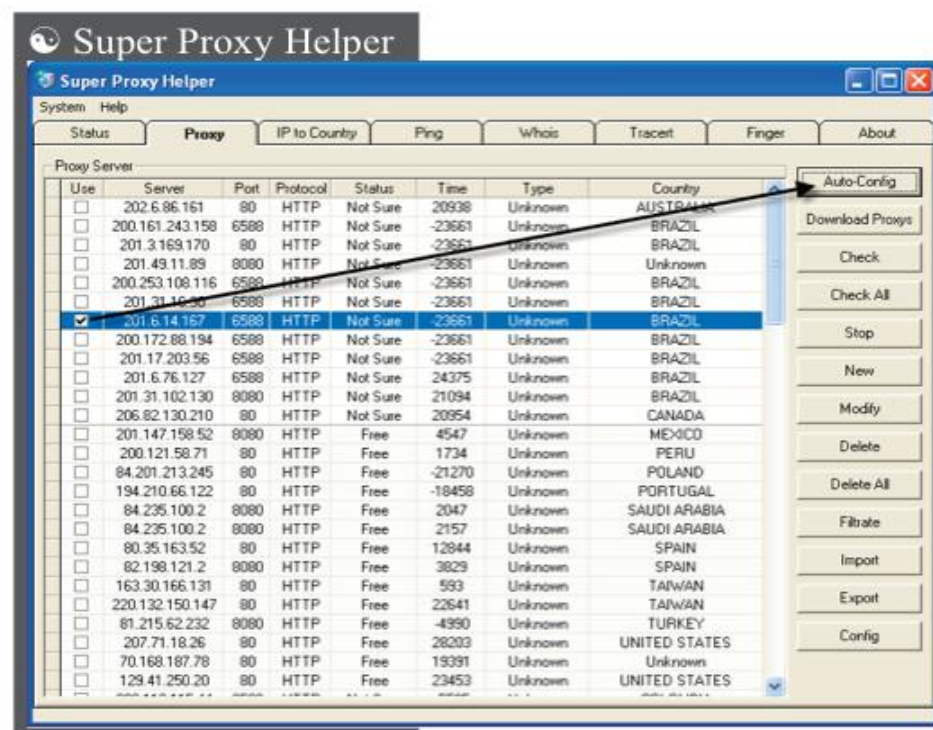
Anonymizer (*anonymizer.com*), bisa dikatakan sebagai pioner yang memberikan layanan browsing secara anonymous di internet. *Anonymizer* yang dibuat oleh *Lance Cottrell* pada tahun 1997 dan sampai saat ini tetap menjadi layanan yang populer.

Anonymizer akan membuang semua informasi pribadi dari penggunaanya dan menjamin segala informasi dari client agar tetap rahasia walaupun tidak disebutkan apa yang akan terjadi apabila terdapat masalah hukum atau tuntutan hukum terhadap client *anonymizer*.

Dulu, untuk menggunakan layanan anonymizer, Anda mengunjungi website *anonymizer.com* kemudian memasukkan alamat URL yang hendak Anda kunjungi. Selanjutnya, anonymizer akan menampilkan website tersebut untuk Anda namun kini, layanan anonymizer jauh lebih mudah untuk digunakan dan nyaman.

Anda hanya perlu mendownload dan menjalankan software dari *anonymizer* pada komputer Anda. Setelah itu, Anda bisa menjalankan web browser Anda seperti biasa, tanpa perlu setting apa-apa lagi.

Program dari *anonymizer* ini akan mengalihkan panggilan Anda ke proxy server yang dikelola oleh *anonymizer*. Anda bisa melihat bahwa kini, Anda akan dikenal dengan alamat IP yang berbeda dengan alamat IP Anda yang sebenarnya.



Super Proxy Helper (www.igoodsoft.com), akan membantu Anda dalam melakukan pengecekan proxy-proxy yang ada. Anda juga bisa memasukkan daftar proxy yang Anda dapatkan dari situs-situs pengecek proxy seperti www.multiproxy.org, dtt (dan teman-temannya). *Super Proxy Helper* juga akan menampilkan tingkat anonymous yang ada, adapakah termasuk *Transparent*, *Anonymous* atau *High Anonymous*.

Salah satu keunggulan program ini adalah fasilitas konfigurasi otomatis yang sangat membantu Anda dalam aksi gonta-ganti proxy pada browser Anda. Dengan memilih salah satu proxy yang ada didalam daftar kemudian mengklik tombol 'Auto-Config', browser Anda secara otomatis akan dikonfigurasi dengan proxy yang Anda pilih.

Dengan otomatisasi ini, proses gonta-ganti proxy menjadi jauh lebih mudah daripada harus melakukannya secara manual.

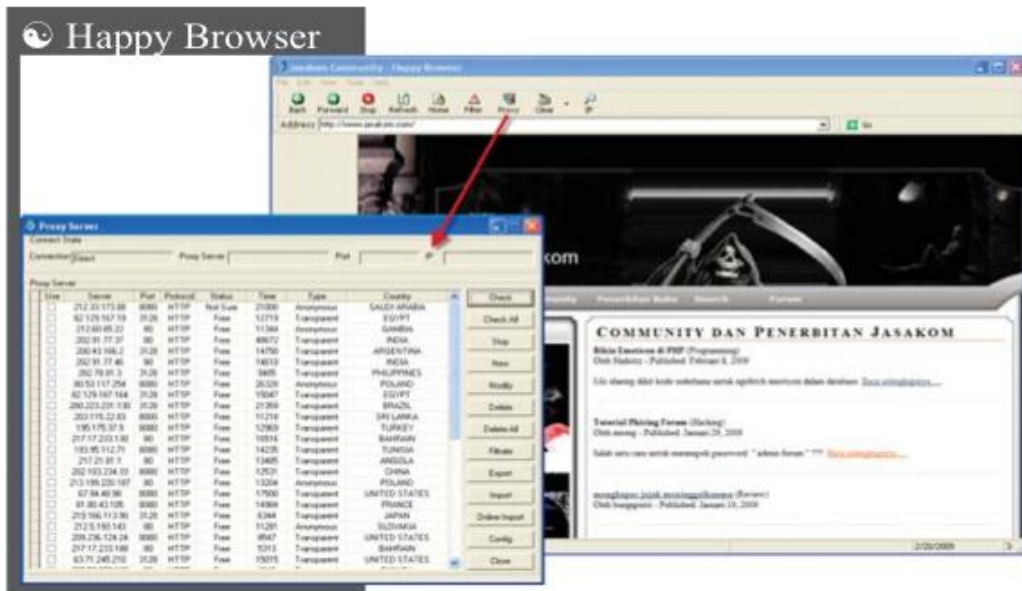


ProxySwitcher (www.proxyswitcher.com), sangat mudah dan nyaman untuk digunakan. Yang paling saya sukai dari program ini adalah adanya video tutorial saat melakukan instalasi sehingga Anda bisa langsung memahami bagaimana menggunakan program ini.

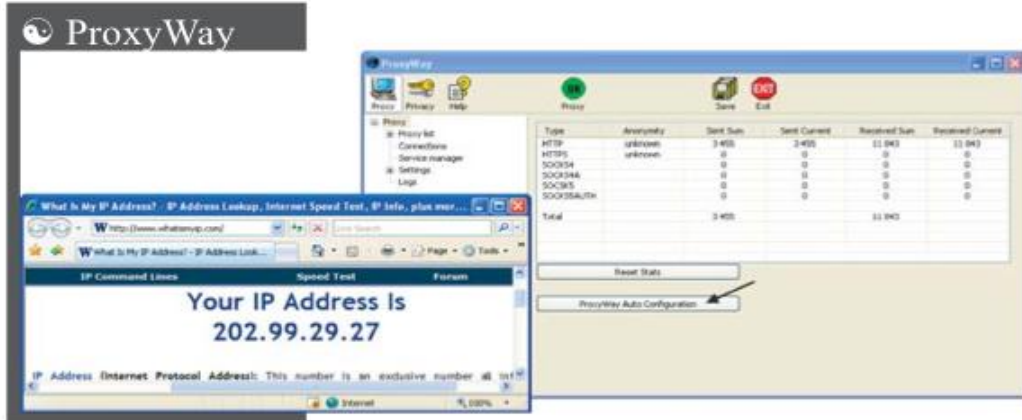
Pada saat pertama kali dijalankan, Anda memerlukan daftar proxy server yang ada di internet dan seperti biasa, daftar ini bisa Anda masukkan secara manual namun ProxySwitcher juga bisa melakukannya secara otomatis. Dengan sekali klik saja (1), daftar proxy akan segera didownload kedalam komputer Anda, sekaligus akan dilakukan pengecekan status dari proxy tersebut.

Untuk menggunakan proxy server yang ada didalam daftar, caranya juga sangat mudah dengan bantuan dari *Proxy Switcher*. Anda hanya perlu double klik proxy server yang ingin Anda gunakan dan secara otomatis, Internet Explorer akan disetting untuk menggunakan proxy tersebut.

Untuk berpindah dan menggunakan proxy yang lainnya, caranya juga sangat mudah. Anda tinggal mengklik dua kali proxy tersebut dan konfigurasi proxy di browser Anda secara otomatis akan berubah mengikuti pilihan Anda.



Happy Browser (www.igoodsoft.com), menawarkan web browser yang mudah dan nyaman dalam menggunakan dan gonta-ganti proxy. Dengan browser ini, Anda juga bisa mendownload daftar proxy server dari internet secara langsung yang tentunya bisa menghemat banyak waktu Anda yang berharga.



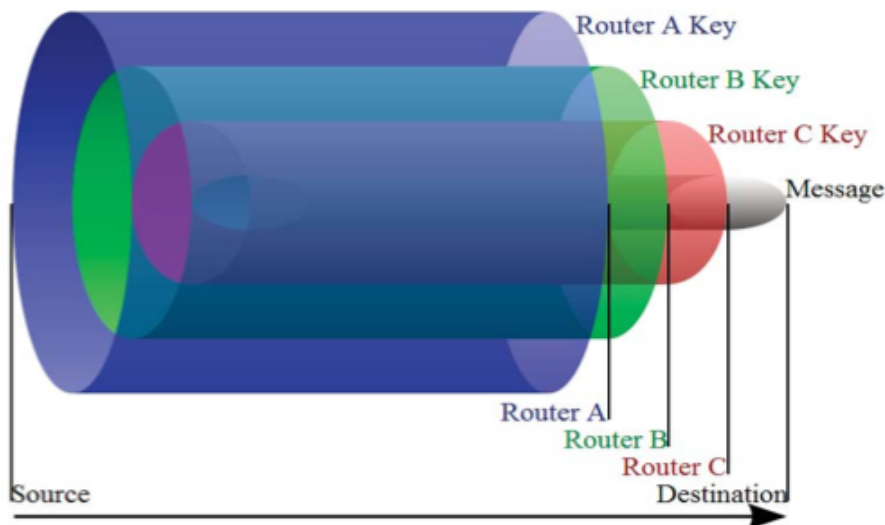
ProxyWay (www.proxyway.com), menyediakan program yang sangat mudah untuk menggunakan proxy server. Banyak hal bisa dilakukan dengan otomatis sehingga pengguna awam bisa menggunakan program ini dengan sangat mudah. Dengan mengklik tombol 'ProxyWay Auto Configuration' saja misalnya, download daftar proxy,

pengecekan proxy serta konfigurasi penggunaan proxy pada web browser akan dilakukan secara otomatis.

Tor

Tor (www.torproject.org), merupakan proyek open source yang dibuat pada tahun 2001 dan sampai sekarang masih terus dikembangkan. Tujuan utama dari tor adalah menjaga privasi Anda selama Anda berada di internet, artinya informasi mengenai Anda seperti alamat IP dan lain sebagainya akan terjaga dengan baik. Lalu apa bedanya dengan sistem proxy lainnya? Sangat berbeda.

Apakah Anda masih ingat dengan apa yang saya katakan sebelumnya? Proxy server yang Anda gunakan untuk menyembunyikan identitas Anda mungkin saja sebuah jebakan, yang akan mengintip data-data Anda ketika melewati proxy mereka. Tor menggunakan konsep proxy yang dinamakan sebagai *Onion Proxy* (proxy bawang) dimana data yang dikirimkan ke tempat tujuan, akan melalui beberapa proxy (*onion*) yang berbeda-beda setiap waktu dan dipilih secara acak. Lalu bagaimana jaringan Tor menjaga keamanan dari data yang melalui proxy tor?



Teknik 'bawang' adalah jawabannya. Sebuah paket akan dibungkus dengan beberapa lapis enkripsi berdasarkan router yang dilalui oleh sebuah paket. Setiap router yang menerima paket ini, akan melakukan

dekripsi berdasarkan kunci yang diketahuinya namun paket lapisan dalam masih terenkripsi yang hanya diketahui oleh proxy selanjut. Hal ini terus berlangsung sampai paket sampai ditujukan.

Analoginya begini. Si A ingin mengirimkan paket ke si B dan paket tersebut harus melalui si X, Y dan Z. Untuk menghindari agar si X, Y dan Z mengintip paket yang ada kirimkan, Anda membuat kotak didalam kotak sebanyak 3 buah. Kunci dari kotak paling luar (yang paling besar tentunya) Anda berikan kepada si X, sedangkan kunci kotak kedua diberikan kepada si Y dan kunci kotak paling kecil diberikan kepada si Z.

Pada awalnya, X tidaklah mengetahui kemana paket tersebut harus dikirimkan sampai ia membuka kotak yang Anda berikan kepadanya dan membuka kotak tersebut dengan kunci yang Anda berikan pula. Selanjutnya, kotak tersebut diberikan kepada si Y sesuai petunjuk didalam kotak terluar yang telah terbuka

Si Y yang menerima paket dari X, membuka kotak yang diberikan kepadanya dengan kunci yang Anda berikan dimana didalam kotak tersebut masih terdapat kotak terkecil yang harus disampaikan kepada si Z yang memiliki kunci kotak terkecil ini.

Akhirnya Z membuka kotak yang diberikan kepadanya dan bisa melihat data yang harus disampaikan kepada B. Nah lho, bukannya tadi saya katakan dengan teknik ini, router tidak bisa mengintip data yang melaluinya? Ternyata pada router terakhir, data tersebut bisa dilihat. Kenapa tidak membuat satu kotak lagi? Hal ini terjadi karena tujuan akhir (si B) biasanya adalah sebuah layanan akhir yang tidak bisa dikontrol dan diluar kendali Anda.

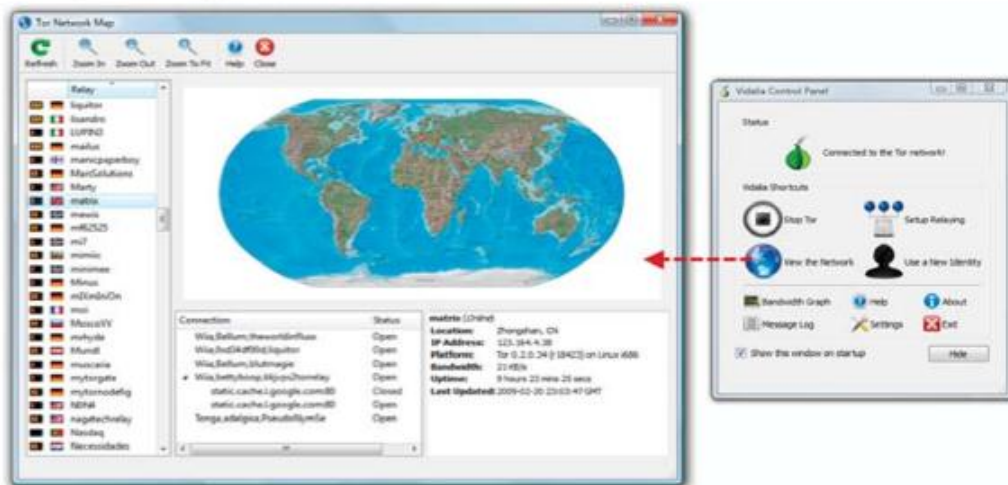
Anda tidak bisa memberikan kunci kepada si B karena ia tidak mengerti dengan enkripsi yang Anda ciptakan. Jadi teknik ini mempunyai sedikit kelemahan dimana router terakhir bisa melihat data yang melaluinya.

Lalu apa gunanya semua kesulitan ini kalau begitu? Masih ingat ketika saya katakan bahwa data yang dikirimkan akan diberikan kepada beberapa router? maksud saya adalah beberapa jaringan router yang berbeda! Jadi walaupun si Z bisa melihat paket datanya, namun data ini hanyalah sebagian data yang ada. Dimana data selengkapnya ? ada pada jaringan onion yang lain.

Kenapa menggunakan nama 'Onion' atau bawang seharusnya sudah jelas sekarang. Anda sudah melihat bagaimana si X, Y dan Z membuka atau mengupas satu persatu lapisan kotak yang ada dan karena itulah, teknik ini dinamakan sebagai teknik bawang karena mirip dengan mengupas bawang (mungkin yang menciptakannya adalah seorang koki dulunya).

Sekarang mari kita kembali pada program Tor yang bisa Anda dapatkan dari situs www.torproject.org secara gratis ini. Untuk memudahkan penggunaan tor, disediakan paket all-in-one yang bisa dijalankan secara langsung tanpa diperlukan lagi instalasi yang tentunya sangat menarik.

Feature yang jarang dilakukan oleh pengembang lainnya ini memungkinkan Anda menyimpan tor didalam flash disk dan menggunakannya setiap waktu dengan browser bawaan berupa Mozilla Firefox. Anda juga bisa melihat jaringan onion dari Tor ini dengan mengklik menu 'View the Network'.



Ketika menjalankan firefox portable bawaan dari paket Tor ini, Anda bisa melihat informasi mengenai alamat IP 'palsu' Anda. Untuk membuktikannya, Anda bisa mengunjungi situs seperti www.whatismyip.com. Pada task bar yang terletak di bagian pojok kanan bawah, Anda juga bisa melihat tulisan 'Tor Enabled'. Kini, selamat berselancar dengan aman dan nyaman di internet karena jaringan dari Tor ini cukup bisa diandalkan.



Stealthsurfer

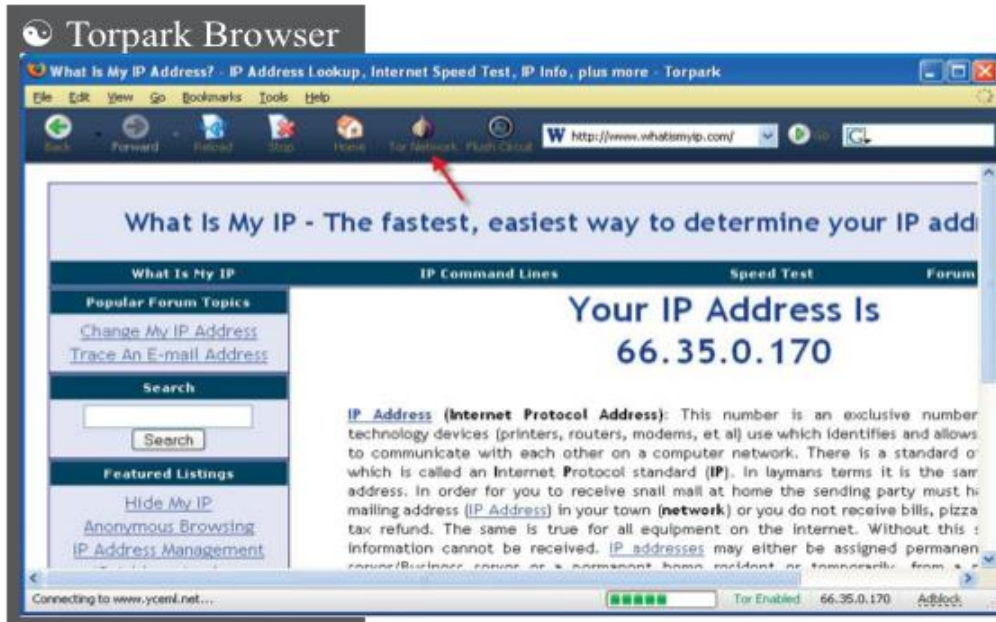
Stealthsurfer (www.stealthsurfer.com), perusahaan yang menyadari akan kebutuhan privasi pengguna dengan cara yang praktis membuat paket software yang disimpan kedalam flashdisk.

Penjualan flashdisk beserta isinya ini dijual dengan harga yang bervariasi antara \$99 untuk kapasitas 4GB sampai dengan \$199 untuk kapasitas 16GB.



StealthSurfer memanfaatkan program *Tor*, *Mojopac*, *Hushmail Premium*, *Roboform*, *Firefox* dan *Thunderbird* untuk menjaga privasi Anda.

Ketika Anda menggunakan *StealthSurfer*, informasi sensitif seperti cookies, internet history, dan cache akan tersimpan didalam *StealthSurfer* USB flashdisk sehingga Anda tidak akan meninggalkan jejak pada komputer yang Anda gunakan.



Torpark Browser, adalah browser yang memanfaatkan jaringan Onion Proxy secara otomatis sehingga Anda tidak perlu lagi menjalankan Tor secara terpisah. Jika Anda merasa aktifitas browsing Anda terlalu lama karena jaringan Tor atau ketika Anda merasa Anda tidak perlu menyembunyikan diri Anda, Anda bisa mengklik toolbar 'Tor Network' untuk mematikan penggunaan *Onion Network*.

Menariknya, program ini bisa digunakan secara bebas alias gratis dan bisa dijalankan tanpa perlu melakukan instalasi sehingga sangat cocok disimpan didalam flashdisk Anda dan digunakan sewaktu-waktu. Kode inti dari browser Torpark ini dibuat dari browser Firefox sehingga Anda akan melihat banyak feature dan kemiripan dengan mozilla firefox.

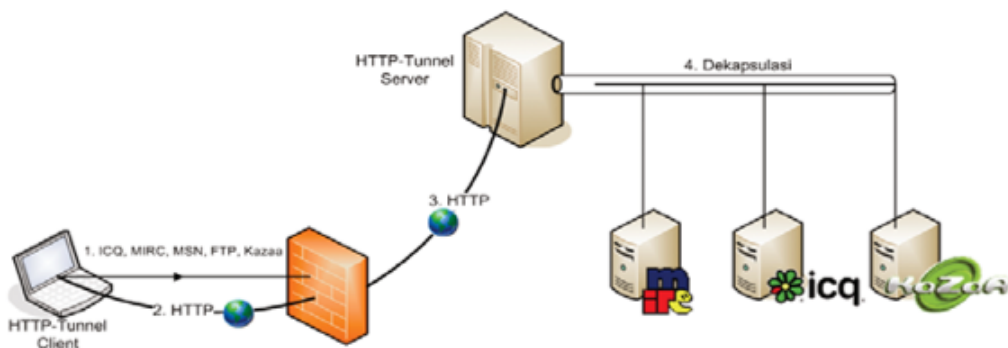
Teknik HTTP Tunneling

Protokol ibaratnya adalah bahasa dan hanya dengan berbahasa yang sama, suatu komunikasi bisa terjadi. Saat Anda berselancar di web misalnya, Anda menggunakan protokol HTTP dan semua browser menggunakan protokol yang sama baik itu Internet Explorer, Mozilla Firefox, Opera dan lain-lain. Aplikasi seperti mIRC, menggunakan protokol IRC yang terhubung dalam jaringan IRC sehingga Anda

bisa chatting dengan teman Anda yang berada dibelahan bumi yang lain. Walaupun sama-sama sebagai program chatting, ICQ misalnya menggunakan protokol yang berbeda lagi, dan program P2P yang merupakan program sharing file juga menggunakan protokol yang berbeda.

Karena keunikan protokol, pembatasan terhadap layanan tertentu bisa dilakukan dengan memblokir protokol yang digunakan. Hal inilah yang seringkali terjadi dan dilakukan oleh perusahaan-perusahaan dalam membatasi kegiatan yang tidak diinginkan. Banyak perusahaan misalnya, mencegah karyawannya bermain selama dikantor dengan memblokir protokol chatting dengan harapan agar produktifitas bekerja tidak terganggu.

Pemblokiran ini bisa berjalan sangat efektif sampai diperkenalkannya teknik *tunneling* (terowongan). *Tunneling* adalah teknik membungkus suatu protokol dengan protokol lainnya sehingga protokol asli bisa disembunyikan. *HTTP Tunneling*, adalah teknik membungkus protokol lain kedalam protokol HTTP. Sebagai contoh, bila perusahaan Anda membatasi karyawan dalam menggunakan internet sehingga hanya bisa digunakan untuk browsing (protokol HTTP) dan tidak untuk aplikasi lainnya, termasuk chatting, Anda bisa melewatinya dengan teknik *HTTP Tunneling*. *HTTP Tunnel* ini selalu terdiri atas dua bagian, yaitu Server dan Client.



Dengan HTTP Tunnel, proteksi terhadap protokol ICQ, MIRC, FTP, Kazaa, dll oleh firewall (1) bisa menjadi tidak berguna. Dengan menggunakan HTTP Tunnel pada komputer client, paket-paket terlarang ini bisa di-enskapsulasi ke dalam HTTP (2) sehingga bisa melewati proteksi firewall (3). Paket yang telah melewati firewall ini

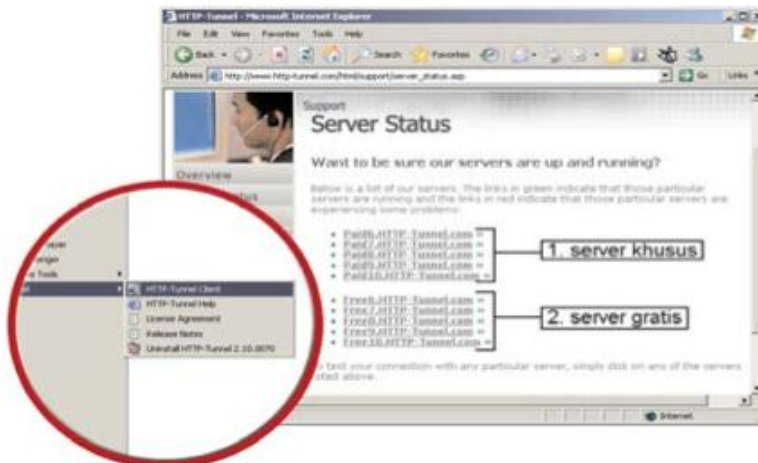
akan dirubah kembali oleh HTTP-Tunnel Server dan di-dekapsulasi (4) kembali ke bentuk aslinya seperti MIRC, ICQ, FTP, Kazaa, dll. Dengan teknik ini, proteksi chatting atau aplikasi lainnya bisa dilewati asalkan akses browsing diperbolehkan.

Karena semua komunikasi melalui HTTP-Tunnel ini, maka server-server HTTP Tunnel yang disediakan atau yang akan digunakan ini sangat berpengaruh terhadap performance aplikasi. Artinya, jika server HTTP Tunnel ini lambat, otomatis pengguna aplikasi ini juga akan mengalami kelambatan.

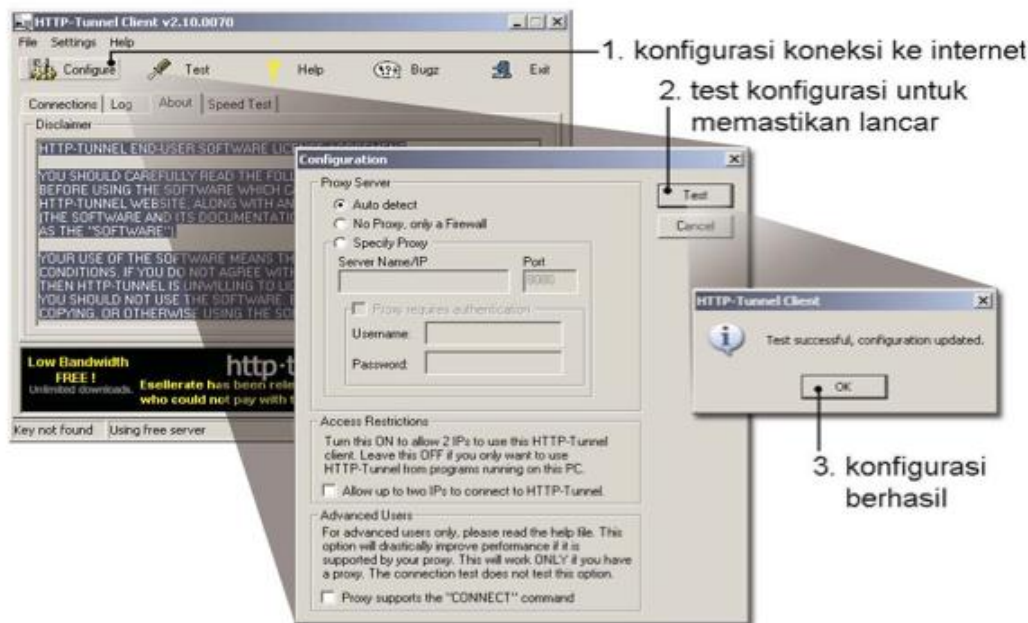
HTTP-Tunnel (www.http-tunnel.com), merupakan program HTTP tunneling yang terkenal dan banyak digunakan. Untuk menggunakan program ini, ada 4 tahap yang perlu dilakukan, yaitu :

1. Melakukan instalasi HTTP-Tunnel Client (hanya mengklik tombol next sehingga tidak dibahas)
2. Memastikan server-server HTTP-Tunnel aktif
3. Melakukan konfigurasi HTTP-Tunnel client
4. Melakukan konfigurasi program seperti Mirc, ICQ dan YM! agar melakukan koneksi melalui HTTP-Tunnel.

Sebelum kita memulai menjalankan program *HTTP-Tunnel Client* yang telah terinstalasi, pastikan server-server gratis yang digunakan ini dalam keadaan aktif. Untuk itu, Anda bisa mengeceknya secara online, www.http-tunnel.com/html/support/server_status.asp (link ini mungkin berubah sewaktu-waktu) yang akan memperlihatkan dua kelompok server yaitu kelompok khusus pelanggan (1) dan kelompok gratis (2).



Tentu saja, server-server gratis mempunyai keterbatasan yaitu bandwidth yang disediakan sangat terbatas sedangkan server untuk pelanggan yang bayar, bandwidth yang disediakan jauh lebih besar.



Selanjutnya, *HTTP-Tunnel Client* yang telah terinstall harus di konfigurasi sebelum bisa digunakan. Langkah pertama konfigurasi adalah menentukan bagaimana komputer yang terinstall *HTTP-Tunnel Client* ini terkoneksi ke internet.

Untuk itu, klik tombol *Configure* (1). Dari form *Configuration* ini, Anda bisa mengisi pilihan *proxy server* atau memilih *Auto Detect* agar program mencarinya sendiri. Jika Anda tidak mengetahui konfigurasi ini, tapi selama ini bisa IE Anda berjalan lancar, conteklah konfigurasi dari IE melalui menu *Tools* → *Internet Options* → *Connections* → *LAN Settings*.

Setelah pengisian *Proxy Server* selesai dilakukan, klik tombol *Test* (2). Jika tombol *Test* memberikan informasi berhasil atau "*Test successful, configuration updated*" (3) maka *HTTP-Tunnel* Anda sudah siap di gunakan. Mudah bukan ?

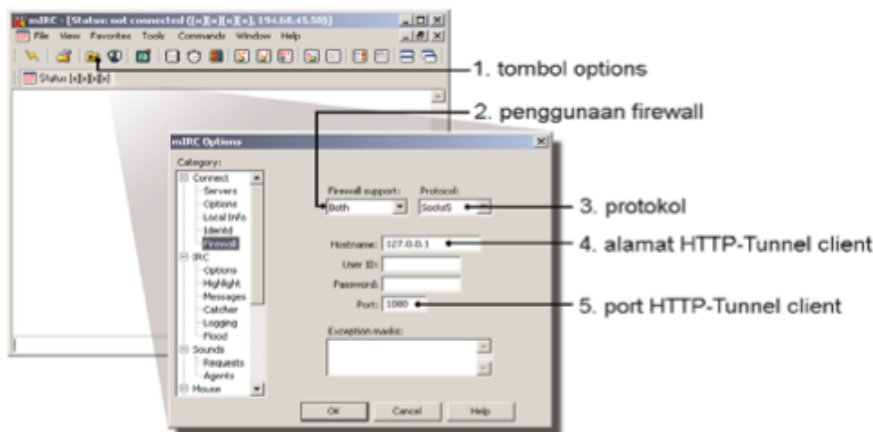
Setelah konfigurasi selesai, pada tabulasi Log Anda akan melihat status dari HTTP-Tunnel. Baru pertama menampilkan *"Starting HTTP-Tunnel, waiting for client to connect"*.



Baris kedua menampilkan *"Retrieving HTTP-Tunnel server's IP Address"* yang berarti HTTP-Tunnel Anda sedang mencari server HTTP-Tunnel yang aktif di internet.

Baris ketiga menampilkan *"Please do not start any applications until this is complete"*. Baris selanjutnya yang akan ditampilkan adalah *"IP Address successfully retrieved"* yang disertai dengan *"Socks 4/5 Server Started"*. Kini, HTTP-Tunnel Client Anda sudah siap digunakan oleh aplikasi-aplikasi yang telah dilarang.

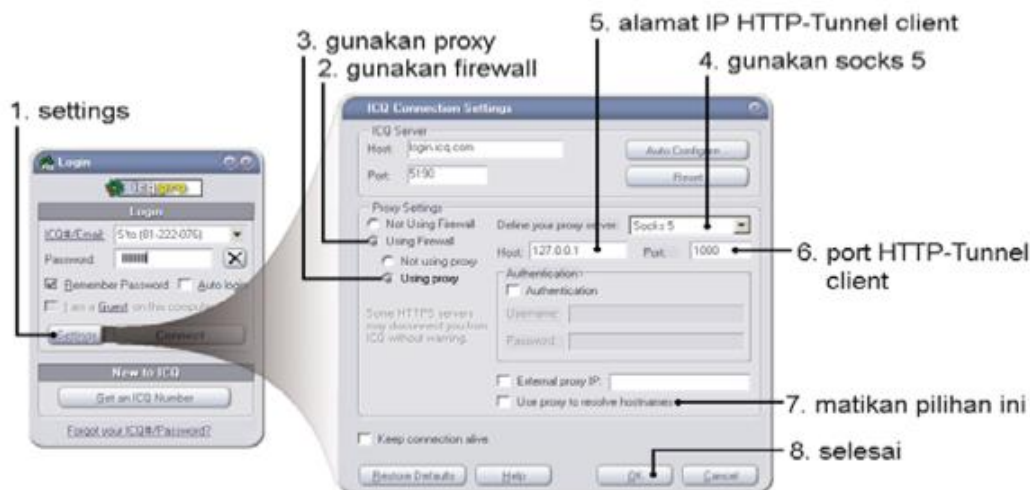
Langkah selanjutnya adalah melakukan setting pada aplikasi client, baik itu mIRC, FTP, ICQ, dll agar menggunakan HTTP-Tunnel ini. Pada dasarnya Anda melakukan setting pada bagian firewall/proxy agar menunjuk ke alamat HTTP-Tunnel Client. Sebagai contoh, saya akan melakukan setting di mIRC agar menggunakan program HTTP-Tunnel Client di komputer saya yang telah dijalankan dan di konfigurasi.



Pada program mIRC (saya menggunakan versi 6.16), klik tombol Options (1), pilih kategori *Connect* → *Firewall*. Pada bagian Firewall support (2), pilih *Both* (2) agar mIRC Anda selalu menggunakan HTTP-Tunnel sedangkan pada Protocol (3), gunakan *Socks5*. Pada kolom Hostname (4), isilah alamat IP dari komputer yang menjalankan HTTP-Tunnel ini. Karena saya menjalankan HTTP-Tunnel Client dengan mIRC pada komputer yang sama, maka saya mengisikan alamat localhost, yaitu 127.0.0.1. Port yang digunakan oleh HTTP-Tunnel adalah 1080 sehingga Anda harus mengisi bagian Port (5) dengan angka 1080.



Setelah setting mIRC selesai dilakukan, kini chatting melalui mIRC bisa dilakukan seperti biasa. Pada saat mIRC terkoneksi ke server IRC, program HTTP-Tunnel Client segera akan menampilkan koneksi yang terjadi ini pada tabulasi *Connection*.



Untuk aplikasi ICQ (saya menggunakan versi 2003b), Anda bisa melakukan setting dengan mengklik tombol *Settings* (1) yang akan menampilkan konfigurasi tata cara koneksi ke internet. Pada pilihan *Proxy Settings*, pilihlah pilihan *Using Firewall* (2) dan *Using proxy* (3).

Untuk *Define your proxy server* (4), gunakan *Socks 5* sedangkan *Host* (5) diisi dengan alamat IP dari *HTTP-Tunnel Client* Anda. Jika ICQ dan *HTTP-Tunnel Client* berada pada komputer yang sama, Anda bisa mengisi dengan alamat 127.0.0.1 yang berarti "komputer lokal".

Port (6) yang digunakan oleh *HTTP-Tunnel Client* adalah 1080 jadi isilah dengan angka ini. Jangan lupa Anda harus mematikan pilihan *Use proxy to resolve hostnames* (7). Setelah mengklik tombol OK (8), maka ICQ Anda telah siap menggunakan *HTTP-Tunnel* untuk melewati proteksi dari admin IT yang angkuh (atau Anda?).

Penutup (FAQ)

Kenapa tidak semua modul dibahas didalam buku ini?

Sebelum Anda protes kepada saya, berikan saya sedikit waktu untuk menjelaskan kepada Anda sedikit mengenai buku ini dan sertifikasi CEH. Pertama, buku ini memang tidak lengkap dan karena tidak mungkin membuat sebuah buku CEH dalam beberapa ratus halaman buku. Agar Anda paham dengan kata 'luas' yang saya maksud, berikut adalah modul lengkap CEH versi terbaru saat buku ini dibuat :

- Module 1 : Introduction to Ethical Hacking
- Module 2 : Hacking Laws
- Module 3 : Footprinting
- Module 4 : Google Hacking
- Module 5 : Scanning
- Module 6 : Enumeration
- Module 7 : System Hacking
- Module 8 : Trojans and Backdoors
- Module 9 : Viruses and Worms
- Module 10 : Sniffers
- Module 11 : Social Engineering
- Module 12 : Phishing
- Module 13 : Hacking Email Accounts
- Module 14 : Denial-of-Service
- Module 15 : Session Hijacking
- Module 16 : Hacking Web Servers
- Module 17 : Web Application Vulnerabilities
- Module 18 : Web-Based Password Cracking Techniques
- Module 19 : SQL Injection
- Module 20 : Hacking Wireless Networks
- Module 21 : Physical Security
- Module 22 : Linux Hacking
- Module 23 : Evading IDS, Firewalls and Detecting Honey Pots
- Module 24 : Buffer Overflows
- Module 25 : Cryptography

Module 26 : Penetration Testing
Module 27 : Covert Hacking
Module 28 : Writing Virus Codes
Module 29 : Assembly Language Tutorial
Module 30 : Exploit Writing
Module 31 : Smashing the Stack for Fun and Profit
Module 32 : Windows Based Buffer Overflow Exploit Writing
Module 33 : Reverse Engineering
Module 34 : MAC OS X Hacking
Module 35 : Hacking Routers, cable Modems and Firewalls
Module 36 : Hacking Mobile Phones, PDA and Handheld Devices
Module 37 : Bluetooth Hacking
Module 38 : VoIP Hacking
Module 39 : RFID Hacking
Module 40 : Spamming
Module 41 : Hacking USB Devices
Module 42 : Hacking Database Servers
Module 43 : Cyber Warfare- Hacking, Al-Qaida and Terrorism
Module 44 : Internet Content Filtering Techniques
Module 45 : Privacy on the Internet
Module 46 : Securing Laptop Computers
Module 47 : Spying Technologies
Module 48 : Corporate Espionage- Hacking Using Insiders
Module 49 : Creating Security Policies
Module 50 : Software Piracy and Warez
Module 51 : Hacking and Cheating Online Games
Module 52 : Hacking RSS and Atom
Module 53 : Hacking Web Browsers (Firefox, IE)
Module 54 : Proxy Server Technologies
Module 55 : Data Loss Prevention
Module 56 : Hacking Global Positioning System (GPS)
Module 57 : Computer Forensics and Incident Handling
Module 58 : Credit Card Frauds
Module 59 : How to Steal Passwords
Module 60 : Firewall Technologies
Module 61 : Threats and Countermeasures
Module 62 : Case Studies
Module 63 : Botnets
Module 64 : Economic Espionage

Module 65 : Patch Management
Module 66 : Security Convergence
Module 67 : Identifying the Terrorist

Terdapat 67 modul! Untuk setiap modul, terdapat lebih dari 100 halaman slide, bahkan banyak yang melebihi 200 slides. Jadi membutuhkan waktu yang sangat lama untuk membuat semua modul ini dan dibutuhkan ribuan halaman untuk membuat versi lengkap dari CEH yang juga belum tentu mampu saya lakukan. Akhirnya, saya mencoba membuatnya secara bertahap dan menerbitkannya secara berseri.

Apakah Anda Akan Membahas Semua Modul ini ?

Saya tidak bisa menjawab pertanyaan ini, karena tergantung pada banyak hal. Sertifikasi CEH sendiri sebenarnya hanya mencakup modul 1 sampai dengan modul 26 (<http://www.eccouncil.org/Exam/312-50.htm>). Lalu modul yang lain bagaimana? self study alias Belajar sendiri ! Anda boleh mempelajarinya sendiri ataupun tidak karena topik ini hanyalah topik tambahan yang tidak digunakan pada oleh ujian CEH.

Apa judul buku berikutnya ?

Judulnya masih sama... mm'mm, hampir sama maksud saya, yaitu "**CEH: 200% illegal**" yang akan dilanjutkan dengan "**CEH: 300% illegal**" dan seterusnya. Saya sangat berharap bisa menyelesaikan topik CEH ini, minimal topik intinya namun semua itu sangat tergantung pada pembaca juga. Sebagai penulis, penghargaan paling tinggi adalah ketika banyak pembaca yang tertarik dengan tulisan Anda yang selama ini saya rasakan dan memacu saya untuk terus menulis.

Untuk buku CEH ini, masalahnya adalah saya terikat dengan kurikulum dan 'pendapat' dari EC-Council yang terkadang berlawanan dengan pendapat pribadi dan saya harus mengalah untuk itu. Jadi style yang ada di buku ini, cukup berbeda dengan style di buku saya lainnya. Jika ternyata tidak ada pembaca yang menyukai atau sangat sedikit yang menyukai modul CEH ini, akan sangat berat untuk menyelesaikan misi ini.

Apakah training CEH mengajarkan semua modul?

Apakah menurut Anda training CEH yang hanya 5 hari mampu menjelaskan semua topik yang ada ? Tidak ! Hampir tidak mungkin menjelaskan semua modul dalam waktu 5 hari kecuali trainer Anda hanya membacakan slide yang ada untuk Anda.

Katanya 4 modul pertama, kenapa ada yang di'lewatkan'?

Saya tidak membuat versi yang sama persis dengan modul CEH ini. Saya mempertimbangkan hal-hal yang saya temui di lapangan dan berdasarkan kemampuan saya juga. Sebagai contoh, untuk modul 2, seharusnya adalah modul hukum namun tidak saya bahas dan diganti dengan modul berikutnya. Jadi pembahasan saya sebenarnya sampai saat ini adalah modul 1,3,4 dan 5.

Kenapa modul hukum dilewatkan ? karena isinya adalah undang-undang cyber dari setiap negara tanpa negara indonesia didalamnya. Bahasa yang digunakan juga bahasa hukum yang tidak mungkin saya ringkas dan akibatnya adalah sekitar seratus halaman yang terbuang untuk itu. Saya tidak bisa melakukan apapun karena kemampuan yang sangat terbatas selain menerjemahkan kata-kata yang ada didalamnya dan hal tersebut menghabiskan lebih dari seratus halaman ? saya memilih melewatkannya.

Apakah semua tools didalam modul CEH dibahas juga dibuku Anda ?

Hampir ! Ada beberapa alasan kenapa sebuah tools tidak saya bahas. Pertama, tools tersebut saya anggap tidak relevan alias tidak nyambung dengan topik yang dibahas. Kedua, tools tersebut sudah tidak bisa digunakan lagi karena sudah terlalu kuno. Sebagai contoh, saya tidak memperlihatkan Anda tools SATAN dibuku ini karena tools ini jelas sudah berumur lebih dari sepuluh tahun, tidak dikembangkan lagi dan tidak bisa digunakan lagi untuk jaman sekarang, jadi untuk apa membuang-buang halaman yang ada, waktu Anda dan waktu saya ? Ketiga, tools tersebut terlalu buruk untuk dibahas dan terakhir, saya anggap tidak penting dan yang terakhir, saya tidak mampu menjelaskannya kepada Anda.

Seiring dengan semakin pentingnya keamanan komputer, kebutuhan akan profesional dibidang keamanan komputer semakin dibutuhkan. Melihat kebutuhan tersebut, International Council of E-Commerce Consultants (EC-Council) membuat sebuah sertifikasi keamanan komputer yang diakui secara internasional dengan nama CEH (**Certified Ethical Hacker**).

Tujuan dari sertifikasi ini adalah menciptakan orang-orang yang paham dan mengerti cara kerja serta kemampuan yang sama dengan hacker. Filosofi yang digunakan adalah untuk menangkap seorang maling, Anda harus mampu berfikir dan bertindak seperti maling.

Di Indonesia, beberapa lembaga kursus bekerjasama dengan EC-Council dalam menyelenggarakan kursus ini dengan biaya sekitar \$990 (dengan kurs Rp.12.000, artinya sekitar Rp.11.880.000) dengan waktu training sekitar 5 hari. Banyak yang tertarik dengan topik CEH namun terkendala dengan masalah waktu dan biaya yang tidak bisa dikompromi.

Buku **CEH : 100% illegal** mencoba memberikan Anda alternatif lain dalam mempelajari topik CEH secara mandiri dengan cara yang lebih mudah dan murah. Buku ini disusun dengan kurikulum terbaru CEH yaitu CEH versi 6 yang baru dikeluarkan sehingga Anda bisa melihat penggunaan tools dan teknik terbaru yang berjumlah ratusan. Selain itu, salah satu keunggulan dari buku ini adalah penjelasan konsep yang mendalam untuk beberapa topik penting agar pembaca tidak hanya mengetahui dan menggunakan tools yang diberikan.

Buku **CEH : 100% illegal** merupakan seri pertama yang membahas 4 modul pertama dari topik CEH.

Buku-buku berikutnya yang membahas modul-modul lanjutan CEH bisa dipelajari secara terpisah namun modul awal yang dibahas dibuku pertama ini merupakan modul wajib untuk memahami modul-modul berikutnya.

Tentang Penulis :

S'to adalah konsultan dan praktisi independen dibidang keamanan komputer. Ia merupakan pendiri dan salah satu pengelola situs beserta milis Jasakom yang merupakan milis keamanan terbesar di tanah air. Buku-buku yang ditulisnya selama ini merupakan buku dengan predikat Best Seller. Penulis bisa dihubungi di : Sto@jasakom.com

~~Rp. 11.880.000,-~~

Rp. 59.000,-

