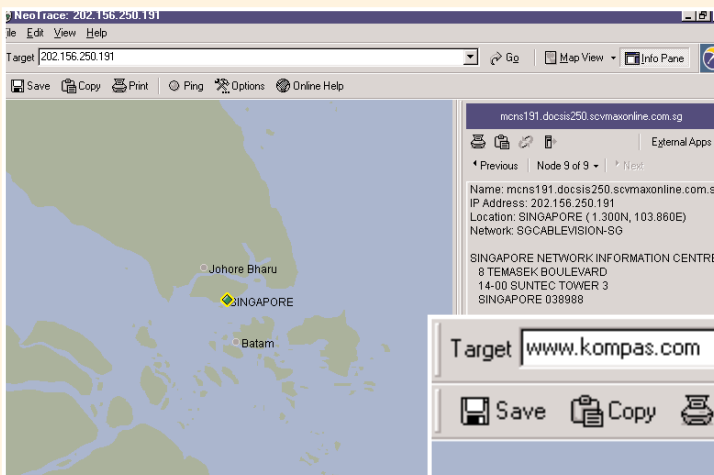
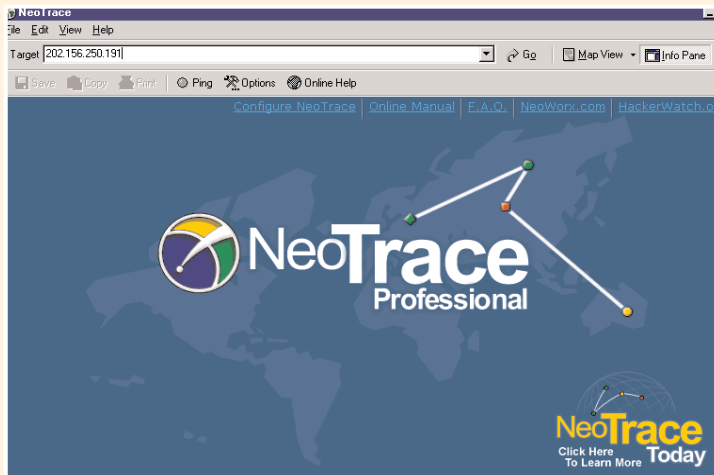


Kulacak Kau sampai ke 'ujung dunia'



Nah!

Mau sembunyi kemana kamu penyusup?

NeoTrace dapat juga digunakan untuk mencari lokasi geografis suatu server dari URL-nya.

Pada contoh ini kita mencari di mana server situs harian Kompas (www.kompas.com) terletak. Cukup ketikkan www.kompas.com pada kolom isian Target dan klik Go; NeoTrace akan menampilkan secara grafis perjalanan paket data dari komputer kita sampai ke server harian ini, yang ternyata di-hosting di Houston, Texas.

Selain **map view**, terdapat pula **list view** dan **node view**

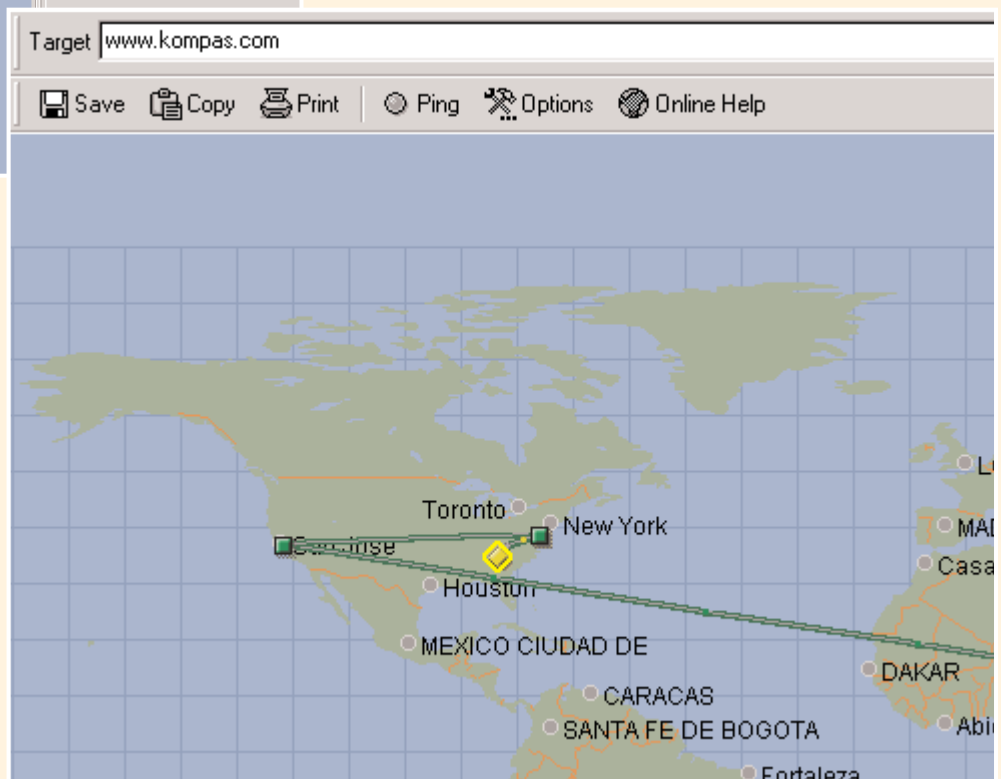
Melacak Si Iseng

Dengan Snort kita dengan mudah dapat mengenali 'si iseng' yang coba-coba men-scan komputer kita (apa maunya ya?) dengan melihat IP Address mesin 'si iseng' pada alert log-nya Snort.

Dari IP Address itu dengan mudah kita bisa dapatkan lokasi komputer 'si iseng' dengan trace-route yang merupakan salah satu tool footprinting (dibahas di NeoTek Vol. II No. 3)

Kali ini dikemukakan dua tool traceroute grafis, yaitu NeoTrace dan VisualRoute (dapatkan di CD NeoTek). Dengan NeoTrace, cukup ketikkan IP Address 'si iseng' dan klik Go, maka akan ditampilkan di mana secara geografis mesin yang melakukan scanning tadi dan di mana hosting-nya.

Pada contoh ini karena komputer yang men-scan dan kena scan sama-sama di Singapore maka yang tampak adalah peta Singapore itu saja.



NEOTEK

Pendamping Berselancar
www.neotek.co.id

Daripada anda men-download...

NeoTek menyediakan CD yang berisi program-program yang dibahas pada NeoTek nomor ini:

- ScreenSaver Crack
- 007PwRec
- Dripper20
- PWLCrack
- L0phtcrack
- NTPassword
- WindowsCrack
- ExcelCrack
- Jigsaws Galore
- Paintshop Pro 7
- Psychostats
- NetBuster

Dapatkan CD-ROM-nya dalam satu paket dengan majalah NeoTek:

Majalah + CD Rp19.500
CD saja Rp15.000

Hubungi

Bagian Sirkulasi
Majalah NeoTek

Tel. (021) 548 1457

Faks. (021) 532 9041

email:

pemasaran@neotek.co.id

Kontak: Elvi R. Nainggolan

PENAWARAN KHUSUS

Dapatkan koleksi 8 CD NeoTek

- CD NEOTEK 2-1
- CD NEOTEK 2-2
- CD NEOTEK 2-3
- CD NEOTEK 2-4
- CD NEOTEK 2-5
- CD NEOTEK 2-6
- CD NEOTEK 2-7
- CD NEOTEK 2-8

Dengan harga Rp95.000,-

Salam!

Belajar menembus password agar tidak menjadi sewot.



• Cain & Abel disebutkan oleh pembuatnya sebagai 'password recovery utility'. Utilitas ini dapat anda gunakan untuk memperoleh kembali kata sandi komputer yang anda lupa.

Password cracking dapat anda gunakan ketika suatu saat anda lupa kata sandi yang pernah anda masukkan di komputer. Dengan password cracking, anda dapat 'memancing' kembali kata sandi yang terlupakan itu dan mendapatkannya kembali. Password cracking, dengan demikian, dapat membantu anda untuk menembus kebuntuan yang terjadi karena terlupakannya kata sandi pada komputer. Anda, dengan kata lain, tidak menjadi sewot.

NeoTek nomor ini menyajikan seluk beluk cara menembus password pada komputer lengkap dengan perangkat atau utilitas yang anda butuhkan untuk melakukan hal itu. Dan kami, seperti biasa, menyajikan perangkat itu di CD bulan ini.

Redaksi

redaksi@neotek.co.id

Bagaimana menghubungi NEOTEK?

KONTRIBUSI ARTIKEL

redaksi@neotek.co.id

SURAT PEMBACA

support@neotek.co.id

WEBMASTER

webmaster@neotek.co.id

PEMASARAN

pemasaran@neotek.co.id

CHATROOM DI DALNET

#neoteker

MILIS PARA NEOTEKER

http://groups.yahoo.com/group/majalahneotek

ADMINISTRASI IKLAN

Tel. 021-5481457 Fax. 021-5329041

SIRKULASI NEOTEK

Tel. 021-3854764

ALAMAT REDAKSI

Gedung Cahaya Palmerah Suite 506
Jl. Palmerah Utara III No. 9
Jakarta 11480

Daftar Isi

NeoTek Vol. II No. 12

NeoStart

- 7 Nge-crack Password**
Bagaimana menembus alat pengaman utama komputer?



- 8 Screen Saver Password**
Kata sandi 'screen saver' pun dapat di-crack lewat segmen pada registry.

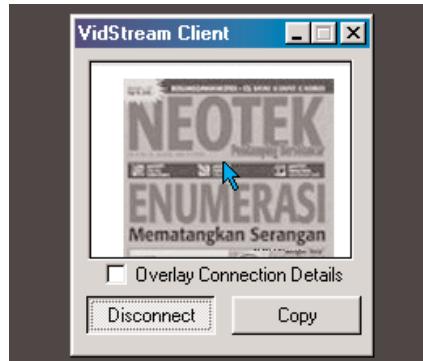
- 9 Password Revealer**
Kenali utilitas-utilitas yang dapat dengan mudah dapat memunculkan password yang terlupa.

- 11 Cracker untuk NT**
Untuk Windows NT anda, di antaranya, dapat menggunakan LOphtcrack sebagai password cracker.

NeoTekno



- 33 BO & Deep BO**
Cara mudah hacking dengan menggunakan trojan legendaris dari Cult of the Dead Cow.



- 36 Konfigurasi BO2K**
BO2K mewarisi fitur-fitur BO plus kemampuannya untuk dikonfigurasi dengan sangat fleksibel.

- 38 BO2K Client Mengendalikan BO2K Server**
Sekali suatu komputer terinfeksi BO2K Server, maka menjadi bulan-bulanan pengendalinya yaitu BO2K Client.

- 40 BO Peep**
Ketangguhan BO2K ditambah dengan banyaknya plug-in. Salah satunya adalah BO Peep untuk mengintip melalui video streaming.

- 42 NetBuster**
Hati-hati hacking dengan trojan NetBus. Bisa-bisa anda sendiri yang kena hack.

- 45 BlackICE Defender**
Suatu network-based IDS yang mudah digunakan. Lebih dari sekedar firewall.

NeoGame

- 46 Psychostats**
Begitu populernya Counter Strike sehingga banyak sekali situs pendukungnya. Psychostats adalah dukungan statistik untuk game multi-user melalui Internet ini. Jangan anggap remeh dengan game. Anda perlu paham Perl, PHP, dan scripting.

- 48 Puzzle Elektronik**
Obat bete yang ampuh dan mudah digunakan. Anda dapat memanfaatkan foto pribadi atau si dia untuk dijadikan puzzle.



NeoTutor

- 12 Pasangan Pencuri**
Dalam password cracking, Cain dan Abel adalah pasangan pencuri yang ampuh.

- 14 Kendali Remote**
Cain juga dapat berfungsi sebagai Abel Client, pengendali komputer yang telah terpasang Abel.

- 16 LOphtcrack untuk NT**
Gunakan LOphtcrack untuk membuka password pada komputer dengan sistem operasi Windows NT.

- 18 Advanced Office 2000**
Utilitas yang dapat digunakan untuk memancing kembali password pada program Microsoft Office.

- 20 Password Winzip**
Advanced Archive Password Recovery dapat digunakan untuk memulihkan password Winzip.

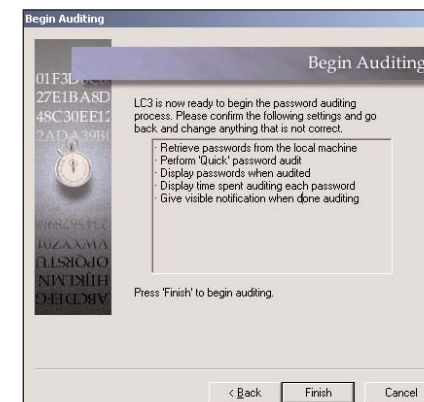
22

Password OE

Anda dapat menggunakan registry editor untuk membongkar password OE.

- 26 Perulangan JavaScript**
Perulangan digunakan untuk mengefisienkan penulisan program pada JavaScript.

- 28 Polling dengan ASP**
Bagaimana membuat polling di situs Web anda dengan menggunakan ASP?



Situs NeoTek

www.neotek.co.id
neotek.kpone.com.sg

Jadikan situs NeoTek sebagai pangkalan Anda berselancar

Link Langsung

Kunjungi situs-situs yang dibahas di majalah NeoTek dengan sekali klik lewat situs NeoTek.

NeoTek versi PDF

Kehabisan NeoTek di kota Anda? Dapatkan saja versi PDF-nya. Gratis!

Download

Tersedia juga download di situs NeoTek selain dari situs aslinya

Layanan Rupa-rupa NeoTek

Dapatkan perlengkapan awal dalam berinternet dari situs web NeoTek HumanClick

Hotline langsung ke redaksi NeoTek untuk menyampaikan saran dan pesan.

Chat Room

Kini tidak usah jauh-jauh untuk ngobrol langsung dengan sesama Neoteker

Mailing List

Ini yang paling ramai. Segera ikutan berbagi pengalaman berinternet!

NeoSoft

- 0 NeoTrace**
Merunut paket data dari satu mesin ke mesin lain dalam LAN dan/atau Internet. Semuanya secara grafis!

RealProfil

- 3 Kru NeoTek**
Bermarkas di Gedung Cahaya Palmerah 503 Jl. Palmerah Utara III No. 9 Jakarta 11480
Telp. 021-5481457
Fax. 021-5329041

Pemimpin Umum
Fachri Said

Pemimpin Redaksi
Kosasih Iskandarsjah

Redaktur Ahli
Onno W. Purbo
Michael S. Sunggiardi

Pemimpin Usaha
Fahmi Oemar
Ridwan Fachri

Redaktur Pelaksana
Gianto Widiyanto
Dadi Pakar

Sekretaris Redaksi
Elvy Risma Nainggolan

Dewan Redaksi
David Sugianto
Stanley

Webmaster
Supriyanto

Pemasaran
Hedhi Sabaruddin
Tuti Sundari

Iklan dan Promosi
Stanley
Elvy Risma Nainggolan

Kuangan
Aswan Bakri

Bank

Bank BNI
a.n. PT NeoTek Maju Mandiri
No. rekening 070.001709720.001

Bank BCA KCP Rawamangun
a.n. Aswan Bakri
No. rekening 0940544131

Inbox

- 6 NmN**
Neoteker menjawab Neoteker dalam forum milis NeoTek

NeoRagam

- 4** Ada Apa di CD NeoTek?
PC Security
Enkripsi Menjaga Privasi Anda
Terdeteksi Sebagai Virus

- 5** Daftar Isi CD NeoTek

NeoTek Oktober 2002

Remote Password Cracking
Setelah memahami cara meng-crack password secara offline, kita teruskan dengan meng-crack password HTTP, POP3, dan FTP secara online.

PHP dan PostNuke

Bersamaan dengan berakhirnya tutorial JavaScript, NeoTek memulai tutorial PHP serta instalasi server PostNuke.

Arabic Word Processor

MS Arabic keyboard mapping cocok untuk keyboard asli Arabic. Tetapi bagaimana menggunakan keyboard Latin untuk Arabic word processing.

Ada Apa di CD NeoTek?

CD NeoTek
September 2002



Password adalah teknik pengamanan yang paling lazim digunakan.

Kelehaman password salah seorang user dalam jaringan dapat dijadikan batu pijakan untuk hacking lebih lanjut ke dalam jaringan.

NeoTek kali ini membahas bagaimana **segala macam password pada dasarnya dapat di-crack**. Pertanyaannya tinggal seberapa sulit atau seberapa mudah?

Enkripsi password bukan berarti password tidak dapat di-crack, melainkan membuat proses cracking menjadi begitu lama sehingga tidak menarik lagi untuk dilakukan.

Selain itu pada CD NeoTek disediakan pula berbagai macam **kamus dan word generator** untuk kegiatan password attack maupun brute force attack. Uji password anda sendiri sebelum 'diuji' orang lain.

Khusus untuk scripting, selain bahasan konvensional mengenai ASP dan JavaScript, terdapat juga **Psychostats**, suatu pendukung statistik untuk game Counter Strike. Anda harus memahami Perl dan PHP untuk dapat memanfaatkannya.

Fokus NeoTek bulan ini adalah pada **password cracking**, khususnya untuk memahami **local security** dan memulihkan password milik anda sendiri yang terlupa. Namun dibahas juga Cain 2.0, suatu **password stealing trojan**.

PASSWORD CRACKING

1. BIOS Password

- ▶ **AMI BIOS Cracker**
- ▶ **AMI BIOS Decoder**
- ▶ **Kill CMOS**

Password BIOS dapat diatasi dengan mengangkat baterai komputer atau dengan BIOS password decoder

2. Screen Saver Pw.

- ▶ **Screen Saver Crack**

Perlindungan berikutnya adalah screen saver password yang dapat pula diatasi dengan Screen Saver Password Recovery.

3. Cached Password

- ▶ **007 Password Recovery**
- ▶ **DialUp Ripper**
- ▶ **Dripper 2.0**
- ▶ **DUNRipper**
- ▶ **Rev**
- ▶ **Revelation NT PW Crack**
- ▶ **Showin 2.0**
- ▶ **Snadboy's Revelation**
- ▶ **Unhide**

Menyimpan password di komputer memang berbahaya sebab dapat diintip dengan tool-tool di atas.

4. PWL Cracker

- ▶ **Deelam PwLeecher**
- ▶ **PWDump2**
- ▶ **PWDump2 Original**
- ▶ **PWDump for NT**
- ▶ **PWL Crack**
- ▶ **PWL Hack 3.20**
- ▶ **PWL Hack 4.02**
- ▶ **PWL Hack 4.10**
- ▶ **PWL Tool**
- ▶ **PWL View**
- ▶ **Make PWL**

Windows menyimpan password dalam file PWL yang dapat anda copy ke disket dan tenang-tenang meng-cracknya di rumah.

5. NT Password

- ▶ **L0phtcrack 1.0**
- ▶ **L0phtcrack 2.01 Src**
- ▶ **L0phtcrack 2.01**
- ▶ **L0phtcrack 3.0**
- ▶ **L0phtcrack 3.0 v 02**
- ▶ **L0phtcrack 1.5**
- ▶ **NT Crack**
- ▶ **NT Password**
- ▶ **NT Sweep**
- ▶ **NTU Crack NT**

Dibandingkan dengan Linux, NT Password lebih mudah di-

crack sebab tidak membedakan huruf besar dan huruf kecil serta password hashnya lebih pendek sebab diusahakan backward compatible.

6. Application Pw.

- ▶ **Advanced Office 2000**
- ▶ **Advanced Archive**
- ▶ **ARJ Cracker**
- ▶ **ARJ Hack**
- ▶ **Break ARJ**
- ▶ **Crack Eudora**
- ▶ **Advanced Zip**
- ▶ **Eudora Pw Decoder**
- ▶ **Excel Crack**
- ▶ **Glide Brute Force**
- ▶ **Hotmail Hack**
- ▶ **Windows Crack**
- ▶ **Windows Pw Cracker**
- ▶ **Word Decrypt**
- ▶ **WP Crack**

What do you want to crack today? Segala macam password dapat di-crack.

7. Pw. Stealing Trojan

- ▶ **Cain 2.0**
- Selain mencuri password, Cain juga berperan sebagai remote admin trojan.

TROJAN DAN ANTI-TROJAN

Melanjutkan bahasan tentang infeksi digital, kali ini NeoTek kembali membahas beberapa trojan yang terkenal:

- ▶ **Back Orifice**

Trojan legendaris dari Cult of the Dead Cow.

- ▶ **Deep Back Orifice**

BO Client yang memanfaatkan BO Server dari BO yang asli pada port yang berbeda.

- ▶ **Back Orifice 2000**

Mewarisi ketangguhan BO plus kemudahan konfigurasi server maun client-nya.

- ▶ **BO Peep**

Plugin BO2K yang mampu memonitor server dengan streaming video.

- ▶ **BO Butt Trumpet 2000**
- ▶ **BO Cast-256 Encryption**
- ▶ **BO Rattler**
- ▶ **BO Serpent Encryption**
- ▶ **BO STCPPIO**
- ▶ **BO Tool**

Macam-macam plugin BO yang sebagian besar dari pihak ketiga.

- ▶ **NetBus 1.70**

- ▶ **SubSeven**

Remote access trojan yang tidak kalah ganas dibandingkan Back Orifice.

- ▶ **NetBuster 1.31**

Jebakan untuk pemakai Netbus sehingga dapat kena counter-hack.

Terdeteksi Sebagai Virus

Pada CD NeoTek kali ini ada beberapa program yang akan terdeteksi sebagai virus.

Trojan dan Anti-Trojan

- bo.exe
- bo2k_1_0-full.exe
- NetBus170.zip
- s7a.zip
- alt_bopeep_1-0.zip
- srv_bt2k_1_2.zip
- enc_cast_2.3.zip
- srv_rattler_1-10.zip
- enc_serpent-1.4.zip
- io_stcpio_2-10.zip
- cli_botool_1-10.zip
- deepBO.zip
- netbuster1_31.zip

Password Stealing Trojan

- cain20.exe

daftar isi cd neotek

SCRIPTING & SERVER

JavaScript Editor 2.5	jse2em
PWS (web server)	setup
ASP Edit	aspedit
PHPEasy Windows Installer	php404
PHPedit	phpedsetup3x
PHPTriad	phptriadsetup2-11
Psychostats 1.8	psychostats1.8

TROJAN & ANTI TROJAN

Back Orifice (trojan)	bo
Back Orifice 2000 (trojan)	bo2k_1_0_full
NetBus 1.70 (trojan)	netbus170
SubSeven	s7a
BO Peep	alt_bopeep_1-0
BO Butt Trumpet 2000	srv_bt2k_1-2
BO Cast 256 Encryption	enc_cast-2.3
BO Rattler	srv_rattler_1-10
BO Serpent Encryption	enc_serpent-1.4
BO STCPPIO	io_stcpio_2-10
BO Tool	cli_botool_1-10
Deep BO	deepBO
NetBuster 1.31	netbuster1_31

NETWORK-BASED IDS FOR WINDOWS

AntiSniff1021	as-1021
BlackIce Defender 3.0	defeval
Snort 1.7 Windows	snort-1.7-win32-static
Snort 1.8.3 Windows	snort_1.8.3_win32_release
Win PCap	WinPcap_2_3
IDS Center 1.08	idscenter

GAME

Jigsaws Galore 4.2	jigsawgalore42
--------------------	----------------

NEOSOFT

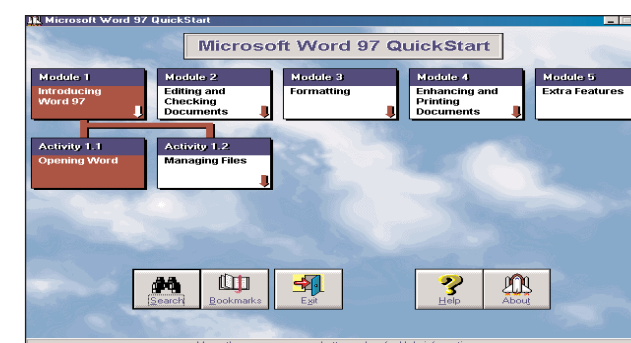
NeoTrace	NeoTraceProTrial325
Visual Route	vr
Word 97 Quick Start	setup

PROGRAM UMUM BERSELANCAR

Acrobat Reader	ar500enu
CuteFTP	cuteftp
GoZilla	gozilla
ICQ	icq2000b
Internet Explorer 6	ie6setup
mIRC	mirc591t
Quick Time	QuickTimeInstaller
RealPlayer	rp8-standard-setup
WinAmp	winampful
Windows Media Player	mp71
WinZip	wzbeta32
PaintShop Pro 7	PaintShopPro7_04
WS FTP	ws_ftple

DICTIONARY

Dictionary
Dictionary Generator
Dictionary Creator
Dictionary Maker
PassList Generator
PassWord Dictionary
WordList



BIOS PASSWORD CRACKER

AMIBIOSCracker	ami-crack
AMIBIOSDecoder	amidecod
KillCMOS	killcmos

SCREEN SAVER PASSWORD CRACKER

ScreenSaverCrack	95sscrk
------------------	---------

CACHED PASSWORD REVEALER

007PwRec	PasswordRecovery
DialUpRipper	dialrip
Dripper20	dripper2.0
DUNRipper	dripper
Rev	Rev
RevelationNTPwCrack	revelation_1_1
Showin20	showin
Snadboy_Revelation	RevelationV2
Unhide	unhide

PWL FILE CRACKER

DeelamPwLeecher	depl
pwdump2	pwdump2
pwdump2orig	pwdump2-orig
PWDumpUsewithNTCrack	pwdump
PWLcrack	Pwlcrack
PwlHack3.20	pwlhck32.rar
PwlHack402	pwl_h402.rar
Pwlhack410	pwl_h410.rar
Pwltool	pwltool
Pwlview	pwlview
MakePWL	makepwl

NT PASSWORD CRACKER

L0phtCrack10	l0hptcrack
L0phtCrackNT	lc201src
L0phtCrack 2.01	lc201.exe
L0phtCrack 3.0	lc3setup
Lc3	lc3setup02
L0phtCrack15	lc15.exe
NTCrack	ntcrack20
NTPassword	ntpsw
NTSweep	ntsweep
NTUCrack NT	ntucrack

APPLICATION PASSWORD CRACKER

Adv Mailbox Pw Rec	ambpr
ao20pr	ao20pr_s
Archpr21	archpr
ARJCracker	breakarj
ARJHack	arjcrack
BrkArj	brkarj10
CrackEudora	CrackPk18
Elcomsoft_AZPR	azpr
EudoraPwDecoder	eudpass
ExcelCrack	excelcrack
GlideBFPwl	glide
HotmailHack	hotmhack
WindowsCrack	windows_crack
WindowsPwCracker	windows_passwd
WordDecrypt	wwprt11d
WPCrack	wpcrackb

PASSWORD STEALING TROJAN

Cain20	cain20
--------	--------

Microsoft Word 97 Quick Start

Microsoft Word merupakan alat bantu kerja sehari-hari yang paling lazim. Namun masih banyak yang belum memahami keseluruhan fungsinya. Dalam CD NeoTek kali ini terdapat tutorial interaktif lengkap tentang Microsoft Word 97.



NmN

NeoTekr menjawab NeoTekr

Forum ini dimaksudkan sebagai bentuk *offline* dari *mailing list* NeoTek di <http://groups.yahoo.com/group/majalahneotek>.

Aman IE atau Netscape? T: Posted July 21

Mau tanya untuk versi yang sekelas-artinya untuk tahun releasenya sama misalnmnya ie.50 dengan netscape 4.75-aman mana ie dengan netscape. juga untuk versi sekelas apakah eudora lebih aman drpada outlook express

Apakah ada site untuk online scanner gratis selain di trendmicro.com (house call antivirus)

Devi RQ
devi_rq@yahoo.com

J: Posted July 21

Pengalaman saya dulu,Netscape Messenger (CMIIW, pokoknya ada dalam paket Netscape Communicator) lebih aman dibanding produknya MS (baik Outlook Express maupun MS Outlook) dalam masalah daya tahan terhadap virus. Tapi saat ini, kayaknya Netscape Messenger udah mulai rentan juga kok... CMIIW.

Bagi saya, selama antivirus yg terpasang selalu uptodate virus definitions-nya, Outlook Express maupun MS Outlook-pun sudah cukup kebal thd serangan2 virus. Oleh karenanya, sering2lah meng-update virus definitions

Btw, Netscape Messenger versi berapa yag yg udah bisa multi eMail account ??? AFAIK mulai versi 6.0 seh... Ada yg pernah make ???

Mat Gemboel
gemboel@ToughGuy.net

J: Posted July 21

Balasan email untuk Mat Gemboel. Kayaknya kerentanan suatu s/w atau OS sangat tergantung dari jumlah pemakai s/w bersangkutan,

bila jumlahnya banyak maka secara otomatis para cracker/hacker akan berusaha mencari kelemahan s/w atau OS tersebut untuk membuat bencana yang lebih besar...

Cock Wirawan
decock@dps.centrin.net.id

Tutorial VPN

T: Posted July 17

Ada neotekker yg bisa ngasih tutorial singkat tentang implementasi VPN? dan ada yg bisa ngasih referensi yg bagus soal VPN ditunggu jawabannya yaa

Rony Adriyanto
ronnie@pertamina.co.id

J: Posted July 18

VPN intinya adalah membentuk jaringan pribadi (private network) dengan memanfaatkan jaringan public (misalnya Internet). Itu sebabnya disebut "Virtual". Tujuan utama adalah menekan biaya seminimal mungkin, tanpa menghilangkan keamanan/security.

Perbedaan PN (Private Network) dan VPN (Virtual Private Network) kurang lebih sbb:

Private Network (Contoh A)

LAN di Jakarta-->Router-->leased-line/vsat<---
Router<--LAN di Surabaya

Dengan cara di atas, dibutuhkan biaya besar untuk koneksi leased-line antar kota.

Private Network (Contoh B)

PC di rumah-->Modem--->Telkom<---Modem Server
<--HUB<--LAN di kantor

Dengan cara diatas, proses dial dari rumah ke kantor, harus dilakukan secara langsung, baik menggunakan pulsa lokal, SLJJ, bahkan SLI, tergantung lokasi.

Virtual Private Network (Contoh A)

LAN di Jakarta-->Sesi VPN-->Router-->Internet<---
Router<--Sesi VPN<--LAN di Surabaya

Virtual Private Network (Contoh B)

PC di rumah-->sesi VPN-->Modem-->Internet<---
Router<--Sesi VPN<--HUB<--LAN di kantor

Dengan menggunakan VPN, maka masing-masing pihak cukup konek ke ISP dengan biaya lokal, dan tetap bisa bertukar informasi dengan aman.

Sesi VPN (VPN Session) ini adalah gabungan dari otentikasi dan encrypt/decrypt atau "tunnel/terowongan" Internet dengan menggunakan protokol network (misalnya TCP/IP).

Implementasi VPN bisa dimulai dari yang sederhana, misalnya di Windows sudah ada fasilitas VPN. Untuk perusahaan besar, proses VPN bisa dilakukan oleh firewall atau box khusus untuk VPN. Semua tergantung berapa tinggi tingkat keamanan yang ingin dicapai.

Albert Siagian
asiagian@gmx.net

VOIP

T: Posted July 23

Jaringan Cabang dan pusat seperti ini, terhubung ke internet

[komputer ---- LAN ---- Server] ---- [LAN ---- komputer] cabang | pusat | Server ---- Internet
Saya ingin menambah VOIP di jaringan cabang dan pusat, bisakah VOIP ikut jaringan tsb ataukah memakai jaringan tersendiri.

Wahyu Budi
wbudi@satelindo.co.id

J: Posted July 23

VOIP bisa ikut jaringan tersebut, dengan catatan bandwidthnya berbagi pakai. Seingat saya 1 line sekitar 8Kbps. Misalnya anda pakai leased-line 64Kbps, dan dipakai oleh 1 line, maka untuk data akan turun jadi 56Kbps (+ VOIP 8Kbps). Dengan catatan router anda support VOIP.

Albert Siagian
asiagian@gmx.net

DLL Ditaruh di Mana?

T: Posted July 22

Sorry berhubung engga pernah ngutak-ngatik windows file DLL di taro dimana ya? Lagi mau mainan openh323 di windows bentuknya DLL engga tahu di taro dimana ..

Onno W. Purbo
onno@indo.net.id

J: Posted July 22

Terserah pak Onno saja deh :) karena pada OS Windows file DLL itu tidak tergantung dimana dia diletakan jadi cukup taruh di sembarang tempat yang diinginkan. Lalu register file DLL tersebut dengan menggunakan RegSvr32 <nama_file_dll> tujuannya agar properties file DLL terdaftar di registry, Termasuk no IDL dan juga method2x yang dalamnya shg aplikasi dapat memakainya cuman ada beberapa org mengumpulkan dalam satu direktori tertentu misal file DLL untuk system OS Windows, akan disimpan di folder windows dalam bagian folder system32 atau system, tujuannya supaya rapi saja :)

Agus Kurniawan
akurniawan@balicamp.com

Password Cracking

Seni dan Tekniknya

Password adalah alat pengamanan komputer yang paling lazim digunakan. **Password yang mudah ditebak** merupakan **mata rantai yang paling lemah** dalam sistem keamanan suatu sistem. NeoTek membawakan serangkaian tulisan untuk mengenal password dan betapa password yang lemah mudah ditembus oleh penyusup.

DENGAN HANYA MENEBAK *PASSWORD* YANG LEMAH, penyerang dapat dengan mudah mendapatkan akses ke dalam sistem, mendapatkan informasi penting, atau menghentikan suatu sistem.

Banyak yang mengelola *password* dengan tidak hati-hati, seperti misalnya menggunakan kata 'password' untuk password-nya atau password yang sama dengan user name-nya. Sekali penyerang masuk dengan menggunakan user name yang password-nya lemah, maka tahap berikutnya adalah mencari password administrator network untuk meningkatkan privilege-nya dalam network itu.

Mem-bypass Password

Windows 9x/ME tidak mempunyai konsep logon multi-user, sehingga setiap orang dapat dengan mudah mengakses komputer yang menggunakan Windows 9x dengan cara mematikan dan menghidupkan kembali komputer itu atau dengan Ctrl-Alt-Del. Permintaan memasukkan password pada saat logon ke Windows 9x semata-mata hanya kosmetik saja. Pada Windows 95 versi awal, Ctrl-Alt-Del bahkan dapat mengatasi *screen-saver password*! Teknik ini dikenal sebagai *console hacking*.

BIOS Password

Cara tradisional untuk mengatasi console hacking adalah dengan menerapkan BIOS password. BIOS (Basic Input

Output System) terpasang secara *hardware* pada motherboard dan menjalankan fungsi *boot* pada komputer PC. BIOS dengan demikian merupakan komponen pertama yang harus dilewati untuk masuk ke dalam sistem.

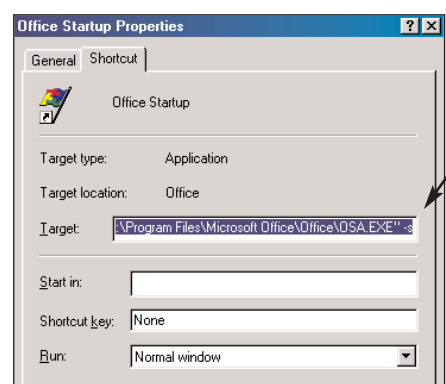
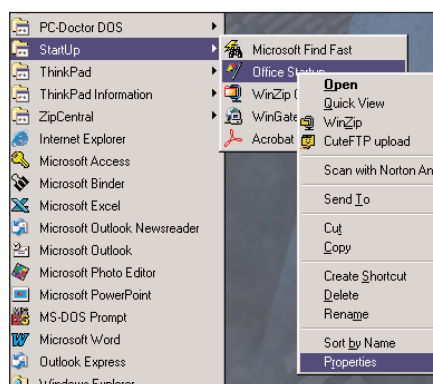
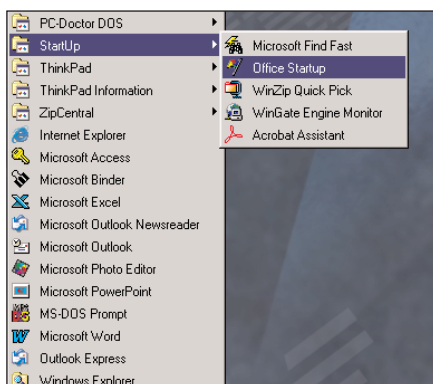
Hampir semua pembuat *motherboard* menyediakan fasilitas BIOS password untuk mencegah masuknya penyusup amatiran ke dalam sistem komputer. Penyusup yang lebih canggih tentunya dapat saja mematikan BIOS password dengan mengangkat baterai yang terpasang pada *motherboard* atau bahkan 'meminjam' *hard disk* anda dan memasangnya pada komputer lain. Selain itu terdapat pula berbagai jenis BIOS password cracking, sehingga BIOS password tetap saja tidak aman. Namun BIOS password sudah memadai untuk mencegah masuknya penyusup amatiran.

Screen Saver Password

Selain BIOS password, pertahanan lapis kedua adalah *screen saver password*. Screen saver password dipasang lewat Display Properties pada Control Panel. Screen Saver tidak bisa diaktifkan secara manual, melainkan hanya akan diaktifkan setelah beberapa waktu komputer tidak aktif (dapat ditetapkan mulai dengan satu menit).

Apabila pada sistem anda terpasang juga Microsoft Office, maka screen saver dapat diaktifkan dengan jalan memodifikasi Office Startup Application (OSA) dengan mengganti switch -b menjadi -s pada menu Startup.

Mengaktifkan Screen Saver pada Saat Startup



1

START UP MICROSOFT OFFICE

Melalui Start → Programs → Startup, cari entri Office Startup (pada MS Office 97) atau Microsoft Office (pada Office 2000) yang mengaktifkan Microsoft Office setiap kali komputer dijalankan.

2

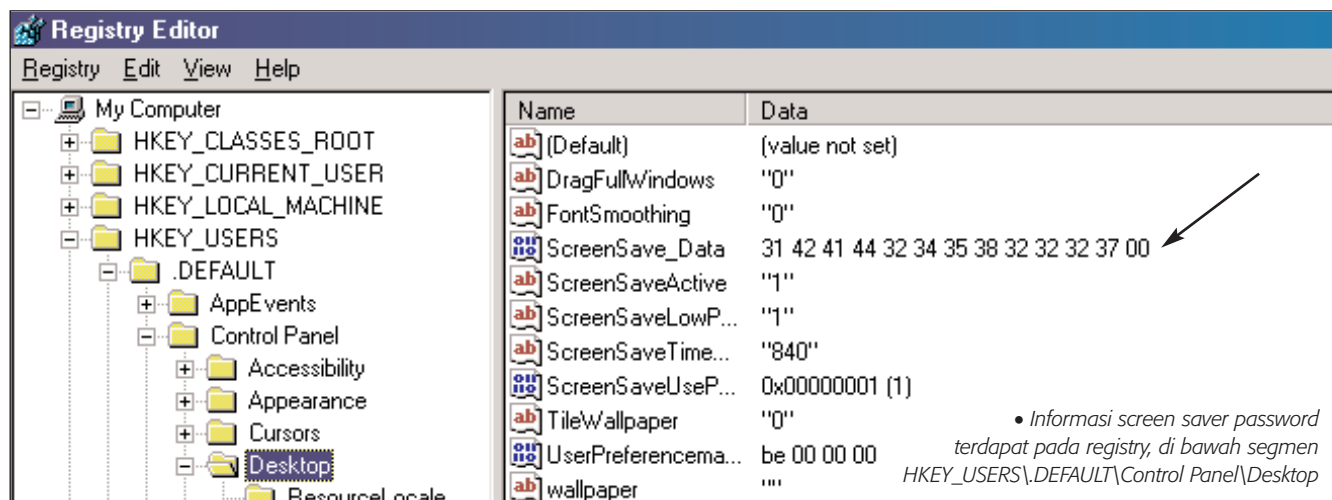
PROPERTY

Klik kanan pada ikon Office Startup (atau Microsoft Office) untuk menampilkan pilihan menu selanjutnya. Pilih Properties untuk menampilkan jendela dialog Microsoft Office Properties.

3

UBAH PARAMETER

Akan tampak pada target bahwa untuk menjalankan MS Office pada waktu Startup, yang dijalankan adalah file OSA.EXE (atau OSA9.EXE pada MS Office 2000). Ubah parameter -b menjadi -s. Kini setiap kali Start, screen saver akan dijalankan.



Screen saver password juga dapat di-bypass. Hal ini dimungkinkan karena kelemahan yang ada pada sistem Windows 9x/ME.

Kelemahan pertama adalah bahwa sistem Windows 9x/ME yang menggunakan CD ROM akan menjalankan file Autorun.inf walaupun screen saver sedang dijalankan. Jadi sementara anda diminta memasukkan password screen saver untuk dapat mengakses sistem, sebenarnya sistem sudah diakses apabila anda memasukkan CD yang mempunyai autorun ke CD ROM drive. Hal ini dapat dimanfaatkan untuk menjalankan program apa saja, terutama trojan seperti NetBus atau Back Orifice.

Kelemahan kedua adalah bahwa data mengenai screen saver password disimpan dalam registry, tepatnya di bawah segmen HKEY_USERS\DEFAULT\Control Panel\Desktop serta dalam file USER.DAT pada direktori Windows. Screen saver password dengan demikian dapat di-bypass ataupun di-crack.

Untuk mem-bypass screen saver password dapat digunakan SSBypass, yang CD-nya dapat dibeli seharga US\$39.95 lewat <http://www.amecisco.com/ssbypass.htm>. Anda akan mendapatkan CD yang bila dipasang pada CD ROM drive

akan segera mengakses sistem dengan mem-bypass layar yang meminta anda memasukkan password screen saver. Software ini pada dasarnya menarik data dari registry dan/atau USER.DAT, men-dekripsi file ini untuk mendapatkan password-nya, dan memasukkan password ini ke sistem Windows 9x/ME.

Untuk mengatasi screen saver bypass pada Windows 9x/ME (pada NT/2000 kelemahan ini telah diatasi oleh Microsoft) non-aktifkan fitur CD ROM Autorun dengan:

- Pada Control Panel, double click System
- Klik tab Device Manager
- Double click CD ROM lalu double click entri CD ROM driver
- Pada tab Setting, pastikan check box Auto Insert Notification kosong.
- Klik OK lalu Close untuk kembali ke Control Panel. Bila diminta untuk me-restart komputer, klik Yes.

Ada juga freeware untuk men-dekripsi screen saver password ini, yaitu 95sscrk.exe yang dapat men-dekripsi screen saver password baik lewat USER.DAT maupun lewat segmen registri yang diekspor menjadi namafire.reg.

Password Cracking

Apa yang dimaksud dengan password cracking? Password cracking adalah kegiatan menebak suatu password dengan menggunakan *encrypted password*-nya. Ada banyak cara untuk melaksanakannya. Cara yang paling sederhana adalah menebak password dan meng-input-kannya sampai didapat password yang diterima. Untuk itu yang perlu diketahui adalah user ID dan akses ke *prompt* logon pada network.

Password cracking secara manual mengikuti langkah-langkah sebagai berikut:

- Dapatkan user ID yang absah
- Ciptakan daftar password yang mungkin
- Susun password-password ini mulai dari yang paling besar peluangnya
- Ketikkan setiap password
- Bila sistem mengizinkan anda masuk, maka sukses!
- Bila tidak, coba lagi dengan memperhatikan *password lockout* (berapa kali boleh memasukkan password yang keliru sampai sistem menutup dan tidak mengizinkan anda mencoba lagi).

Pada prinsipnya caranya sangat mudah, hanya saja memakan waktu. Maka lebih banyak digunakan cara untuk mengotomatisasi kegiatan *password cracking*. Untuk cara otomatis ini, diperlukan satu hal lagi, yaitu file password yang terenkripsi.

Langkah-langkah yang digunakan untuk otomatisasi password cracking adalah sebagai berikut:

- Dapatkan user ID yang absah
- Dapatkan algoritma enkripsi yang digunakan
- Dapatkan password yang terenkripsi
- Ciptakan daftar password yang mungkin
- Enkrip setiap kata yang akan dicobakan
- Periksa apakah cocok untuk setiap user ID
- Ulangi langkah a sampai f

Langkah b (mendapatkan algoritma enkripsi) sudah diketahui untuk berbagai macam sistem. Windows 9x/ME menggunakan enkripsi sederhana untuk screen saver password, sehingga screen saver password dapat dengan mudah di-crack. Windows NT/2000 dan Unix menggunakan algoritma yang lebih sulit ditembus, namun tetap saja terdapat *tool* untuk meng-crack password baik pada NT/2000 maupun Unix.

Telah tersedia perbagai macam tool untuk meng-crack password mengikuti cara otomatisasi di atas. Apabila untuk meng-crack password yang terdapat dalam bentuk file terenkripsi masih diperlukan *password attack*, maka untuk password yang tersimpan dalam *cache memory* akan dengan mudah diungkapkan oleh *password revealer*.

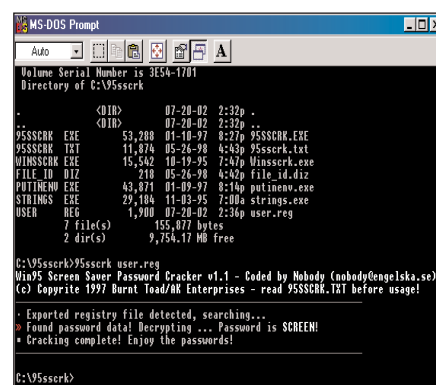
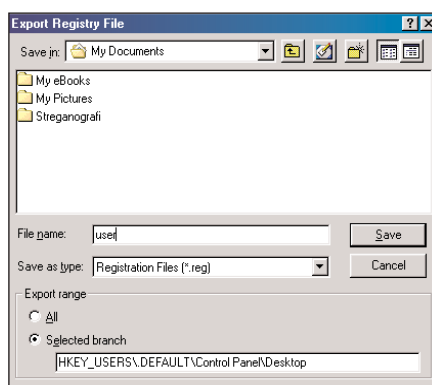
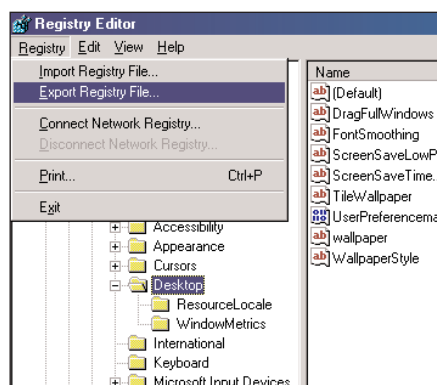
Dengan demikian, apabila anda meminta Windows menyimpan password anda, maka password itu dengan sangat mudah dapat terungkap.

Mengungkap Cached Password

Bila penyusup sudah dapat mematahkan pertahanan BIOS password dan screen saver password, maka tahap berikutnya adalah mengungkap password yang tersimpan dalam memori sistem yang 'terlindung' dengan tanda asterisk sebagai *******. Tanda asterisk ini menandakan bahwa password tersimpan dalam sistem, hanya ditutup dengan tanda asterisk tadi. Fasilitas yang ditawarkan Windows untuk mengingat password kita memang nyaman, namun masalah dapat timbul apabila kita lupa akan password kita sendiri. Untuk itulah fungsi dari software pengungkap password, yang mengungkap password dari password yang tersimpan dalam sistem (cached).

Salah satu pengungkap password yang terkenal adalah **Snadboy's Revelation** (www.snadboy.com) yang cara kerjanya begitu mudah dalam mengungkap password yang disembunyikan di bawah tanda asterisk. Software lain yang serupa di antaranya **007 Password Recovery**, **ShoWin**, **Unhide**, **Pwlttool**, **Pwlview**, dan Dial-up Ripper (**dripper**). Semua software ini pada dasarnya digunakan untuk mengungkapkan password kita sendiri apabila kita lupa akan password itu, sebab semuanya hanya dapat digunakan setelah melewati sesi logon.

Mengekspor Segmen Registry yang Berisi Screen Saver Password



1

EKSPOR SEGMENT REGISTRY

Setelah menjalankan regedit (Start → Run lalu ketikkan regedit), pada segmen yang terdapat screen saver password pilih menu Registry lalu pilih Export Registry File...

2

SAVE REGISTRY SEGMENT

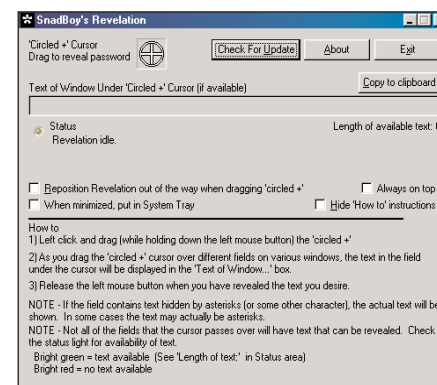
Akan tampil jendela dialog Export Registry File yang akan men-save segmen registry yang anda buka ke file dengan ekstensi .REG. Dalam contoh kita namakan file ini USER.REG disimpan pada folder yang sama dengan 95sscrk.exe

3

CRACK PASSWORD-NYA

Crack screen saver password yang ada pada USER.REG ini dengan mengaktifkan DOS prompt, masuk ke folder C:\95sscrk dan ketikkan: C:\>95sscrk user.reg dan screen saver password pun ditampilkan!

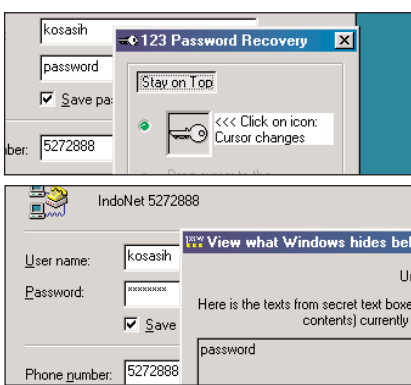
Berbagai Macam Password Revealers



1

SNADBOY'S REVELATION

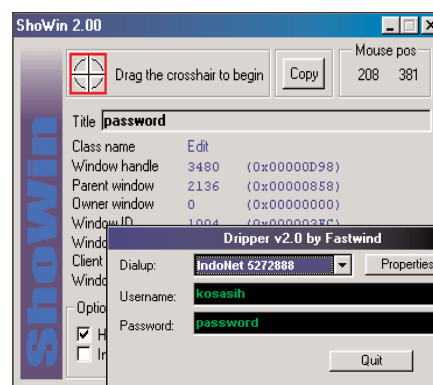
Cache password dengan mudah diungkapkan oleh Snadboy's Revelation dengan membuka tirai asterisk ******* yang menyembunyikan password sebenarnya yang tersimpan dalam sistem atas permintaan anda sendiri.



2

007 PASSWORD RECOVERY

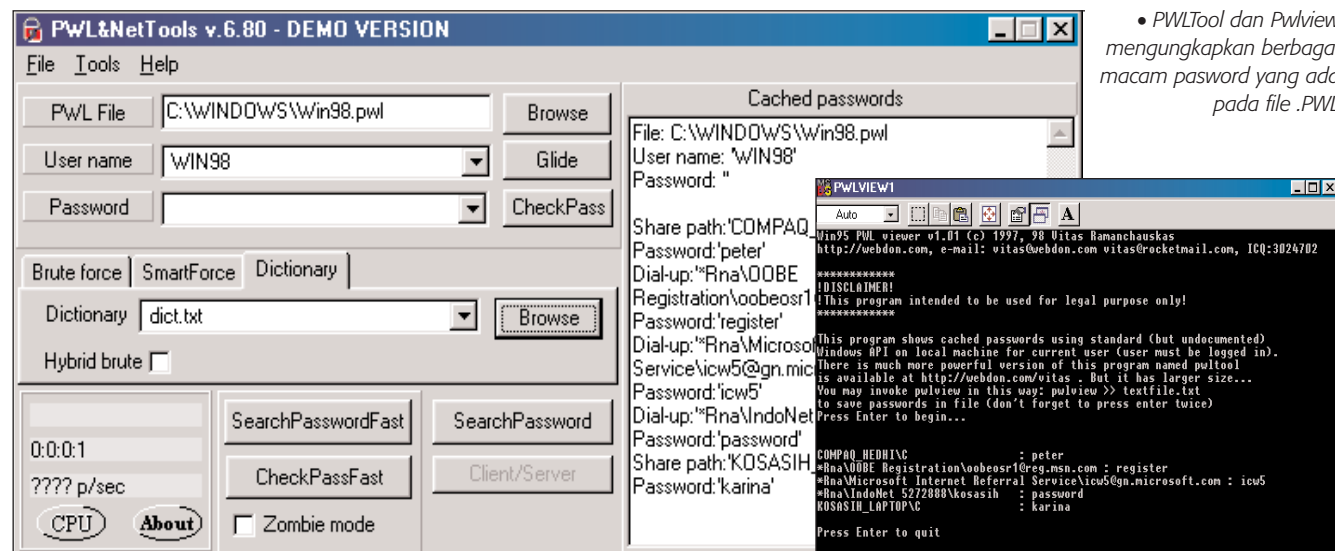
007 Password Recovery dijalankan dengan menggeret ikon anak kunci ke tempat *boxed password* yang akan menampilkan password dari yang sebelumnya tanda asterisk ******* Unhide dijalankan dengan mengklik Refresh List.



3

SHOWIN 2.0 DAN DRIPPER

ShoWin 2.0 mengungkapkan boxed password seperti Snadboy's Revelation. Dial Up Ripper (dripper) mengungkapkan cached password khusus untuk dial up networking.



• PwLTool dan PwLview mengungkapkan berbagai macam pasword yang ada pada file .PWL

File Password pada Windows 9x/ME

Password pada sistem Windows tersimpan dan terenkripsi dalam file .PWL di direktori C:\WINDOWS. File-file ini diberi nama berdasarkan setiap user profile. File-file .PWL dapat di-copy ke disket dengan perintah sederhana:

C:\>copy C:\Windows*.pwl a:

Sekali seseorang telah mendapatkan file-file .PWL maka kini dengan sabar dia dapat mencoba meng-crack-nya. Windows 95 edisi awal menggunakan algoritma enkripsi sederhana sehingga file-file .PWL dapat dengan mudah di-crack. Algoritma yang digunakan pada file .PWL yang sekarang lebih kuat, namun tetap berdasarkan nama yang digunakan sewaktu user logon.

File .PWL pada dasarnya adalah daftar password yang di-cached untuk mengakses *network resource* sebagai berikut:

- Resource yang dilindungi oleh share-level security
- Aplikasi yang menggunakan *password caching* seperti Dial-Up Networking

- Komputer-komputer Windows yang berada di luar domain
- Password logon ke Windows yang bukan merupakan logon primer pada network.
- Server NetWare.

PwL cracking pada dasarnya dilakukan dengan cara melakukan *dictionary attack* atau *brute-force attack* terhadap file .PWL bersangkutan.

Pwltool melakukan dictionary attack terhadap file .PWL yang kehebatannya tergantung pada besarnya ukuran kamus yang digunakan. Agar suatu kamus dapat digunakan oleh Pwltool, kata-kata pada kamus tersebut harus diubah menjadi huruf kapital semua.

Tool lain yang juga bagus untuk meng-crack file .PWL adalah Cain (versi 2.0 untuk Windows 9x/ME dan versi 2.5 untuk Windows NT/2000). Cain menggunakan dictionary attack maupun brute-force attack untuk meng-crack password yang terdapat pada file .PWL. Cain akan dikenali sebagai virus oleh antivirus.

File Password pada Windows NT

Pada Windows NT, password untuk setiap *account* (disebut *password hash*) pada security database yang seringkali disebut sebagai SAM atau *security account manager*. Lokasi file di \Windows\system32\config\SAM. File ini dapat dibaca namun tidak dapat diakses sebab dikunci oleh *kernel system*.

Sewaktu instalasi NT, password database disalin ke direktori Windows/repair. File ini belum berisi *account* apa-apa selain *default account*. Tetapi jangan lupa, biasanya *default account* adalah account tingkat administrator.

User NT memasukkan password sebagai teks biasa, lalu NT menjalankan dua algoritma. Yang pertama untuk NT hash biasa dan satunya lagi untuk LANMAN hash. Untuk menghitung NT hash biasa, Microsoft mengubah password itu ke Unicode dan kemudian menjalankannya pada algoritma hash MD4 untuk mendapatkan nilai 16-byte.

Untuk menghitung LAN Manager hash, Microsoft mengisi password yang bersangkutan dengan angka-angka 0 sampai 14 karakter panjangnya. Lalu diubah ke huruf kapital dan memecahnya menjadi dua potong yang masing-masing panjangnya 7 karakter. Untuk setiap potongan itu dihitung kunci-kunci untuk 8-byte odd parity DES-nya (data encryption standard), lalu kunci-kunci ini dienkripsi dan dikombinasikan menjadi suatu nilai hash 16-byte.

Pada dasarnya semua password dapat di-crack. Hanya pertanyaannya adalah dalam waktu berapa lama? Fungsi enkripsi adalah membuat proses password cracking menjadi begitu lama sehingga tidak layak untuk dilakukan. Namun demikian, dibandingkan Unix, password pada Windows NT dapat lebih cepat di-crack karena adanya kelemahan desain dalam enkripsinya yang tidak membedakan huruf kapital dari huruf kecil. Kemudian memecah password menjadi dua bagian juga menyebabkannya lebih mudah di-crack.

Program untuk meng-crack password pada Windows NT di antaranya L0phtcrack, NTSweep, NTCrack, dan PWDump2. L0phtcrack adalah NT password cracking yang paling baik sekarang ini, sedangkan PWDump2

sebenarnya bukanlah password cracker, melainkan hanya mengekstrak password hashes. PWDump2 masih diperlukan karena ukurannya yang kecil dan ada beberapa password hashes pada NT yang tidak dapat diekstrak sendiri oleh L0phtcrack.

Mengenal L0phtcrack

Mengapa L0phtcrack begitu terkenal dan berharga? Kebanyakan program password cracking mengandalkan kamus dan berasumsi bahwa administrator jaringan mempunyai password yang sudah dienkripsi yang bisa dicuri untuk kemudian di-crack. L0phtcrack tidak mengandalkan kerjanya pada asumsi-asumsi di atas dan menyertakan beberapa feature sebagai berikut:

- Password cracking
- Ekstrak hashes dari password registry
- Loading password dari suatu file
- Sniffing password pada network
- Menjalankan *dictionary*, *hybrid*, *brute force attack* atau kombinasinya.

L0phtcrack hanya berjalan pada lingkungan Windows NT/2000.

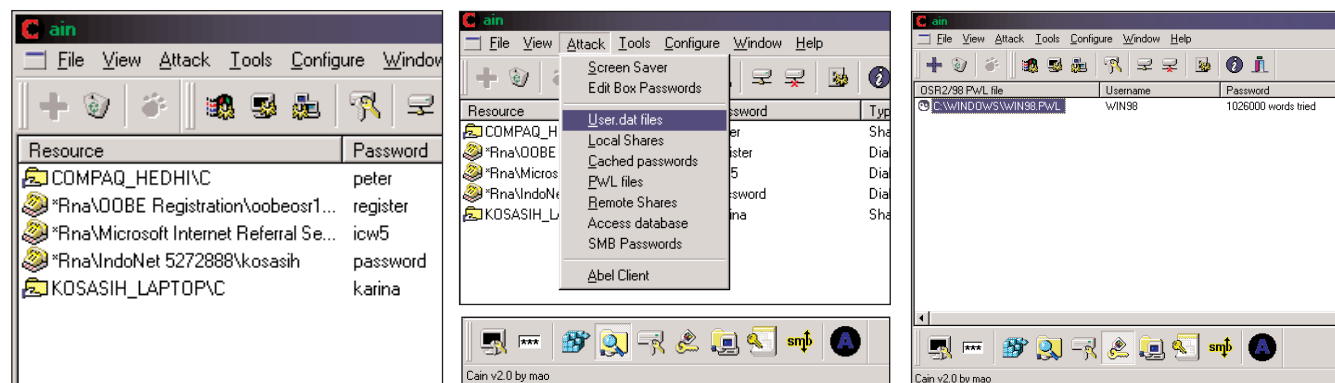
NTCrack dan NTSweep

NTCrack serupa dengan UNIX password cracking program dan berjalan di lingkungan DOS pada semua sistem Windows. Baik NTCrack maupun NTSweep memerlukan user ID yang absah dan kombinasi-kombinasi password untuk dicoba.

What Do You Want to Crack Today?

Selain file .PWL kini segala macam password dapat diungkap (di-crack), mulai dari file .PST pada Microsoft Outlook sampai password pada Microsoft Word, Excel, dan Powerpoint. Bahkan terdapat juga *password cracker* untuk file .ZIP seperti misalnya Advanced Zip Password Recovery (AZPR) dari Elcomsoft, Russia. Pelbagai password cracker dari Elcomsoft menggunakan teknik dictionary, plain text, maupun brute-force attack dan berlangsung amat cepat dengan lebih dari 500.000 tebakan password tiap detiknya.

Cain Password Stealer



1 CACHED PASSWORD

Begitu Cain 2.0 dijalankan langsung semua *cached password* yang ada ditampilkan, baik itu *cached password dial up networking*, *local resource*, maupun *remote resource* yang pernah diakses.

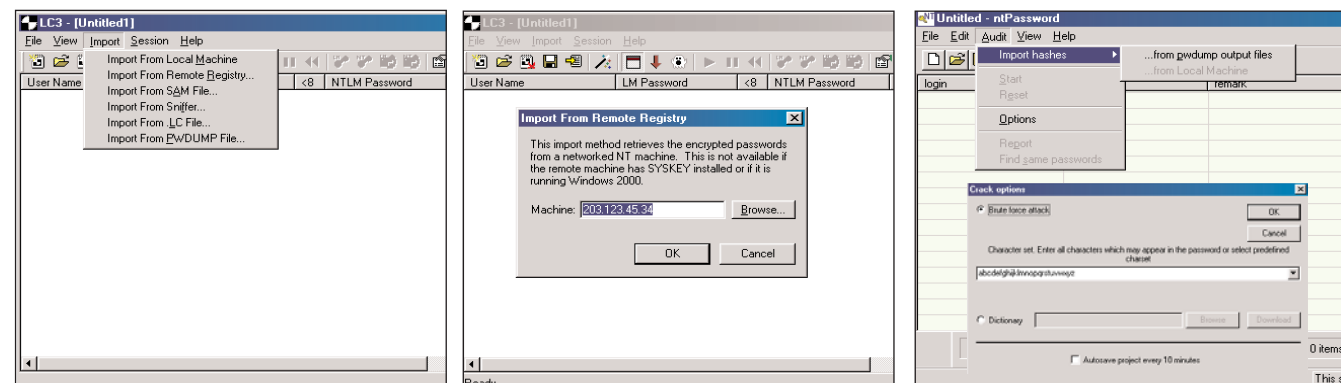
2 PASSWORD ATTACK APA SAJA?

Membuka *cached password* hanya salah satu dari banyak kemampuan Cain 2.0: *user .DAT files*, *local shares*, *cached password*, *.PWL files*, *remote share*, *Access database*, sampai *SMB Password*. Juga terdapat *Abel client* yang memonitor *Abel server*.

3 BRUTE FORCE

Bila anda meng-klik .PWL files attack, maka tampil file-file .PWL yang ada. Dengan mengkliknya, serangan brute force langsung dilaksanakan.

Berbagai Macam NT Password Cracker



1 LOPHTCRACK

L0phtcrack merupakan NT password cracker yang sangat tangguh. Mempunyai kemampuan mengimpor file password baik dari local machine, remote registry, SAM file, sniffer, LC file, maupun PWL file.

2 IMPORT REMOTE REGISTRY

Salah satu kehebatan L0phtcrack adalah kemampuannya mengimpor remote registry. Cukup masukkan IP address dari suatu mesin NT dan dengan mudah passwod terenkripsi dari mesin NT itu akan diperoleh untuk kemudian di-crack.

3 NTPASSWORD

NT password cracker yang juga mudah digunakan adalah ntpassword. Menu Audit-nya terdiri dari impor hashes serta Option untuk melakukan crack berdasarkan brute force (karakter yang disertakan dapat ditentukan) serta dictionary attack.

CAIN & ABEL 2.0

PASANGAN

PENCURI PASSWORD

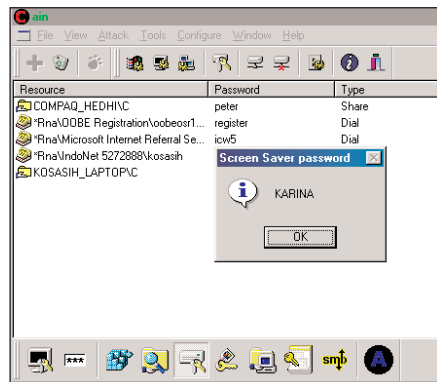
Untuk lebih memahami aspek-aspek password cracking, akan kita bahas 'software terbaik' untuk keperluan ini **Cain** (lengkapnya adalah Cain & Abel), yang terdapat dalam dua versi. **Versi 2.0** yang berjalan pada **Windows 9x/ME** dan versi 2.5 yang berjalan pada Windows NT/2000.

Fasilitas password cracking lengkap dengan fasilitas remote control terhadap komputer lain.

Karena sangat lengkap dan mudah digunakan, Cain 2.0 sangat baik untuk memahami konsep password cracking, baik untuk komputer lokal milik sendiri maupun komputer lain.

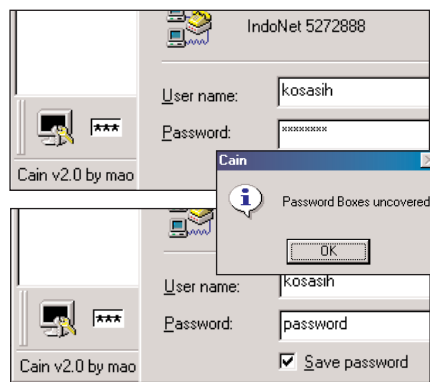
Cain dapat mengakses komputer lain yang ada pada LAN maupun Internet, terutama apabila komputer tersebut mempunyai *share* yang dapat diakses. Apabila terdapat *cached password*, maka share segera dapat diakses, bila tidak, gunakan fasilitas *dictionary* atau *brute force attack*.

Abel server akan terinstalasi bersama Cain. Server ini harus anda nonaktifkan, sebab bila tidak anda sendiri akan menjadi target komputer lain yang menjalankan Cain yang juga merupakan Abel client.



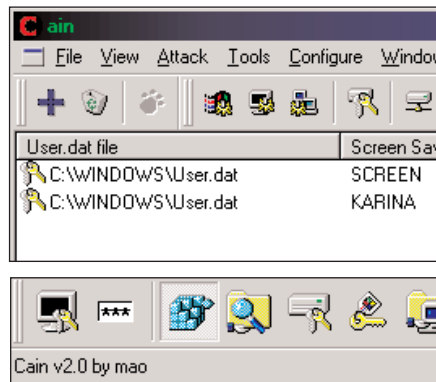
4 SCREEN SAVER PASSWORD

Klik ikon yang terletak paling kiri bawah (atau menu Attack > Screen Saver) maka akan tampil informasi mengenai screen saver password pada komputer lokal anda. Ini mudah dilakukan mengingat screen saver password terdapat di registry dengan enkripsi sederhana saja.



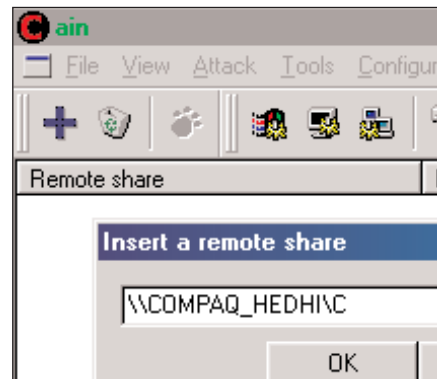
5 BOXED PASSWORD

Boxed password (yang tampak sebagai *****) dapat diungkap dengan mengklik ikon kedua dari ujung kiri bawah (Attack > Boxed Passwords) setelah terlebih dahulu boxed password itu ditampilkan. Pada contoh ini adalah password dial up networking.



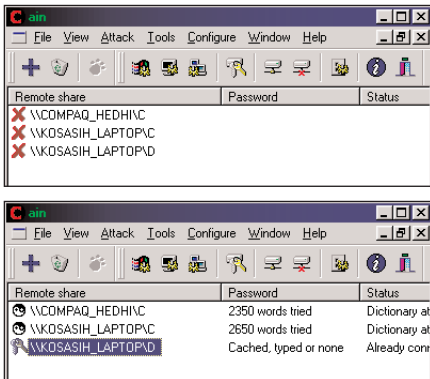
6 DARI USER.DAT FILE

Klik ikon ke-3 (Attack > User.dat files); klik tanda + (kiri atas, atau File > Add to List); cari file user.dat yang terdapat di bawah direktori Windows. Screen saver password yang pernah dipakai akan tampil. Terlihat ada dua screen saver password, yang sekarang dan sebelumnya.



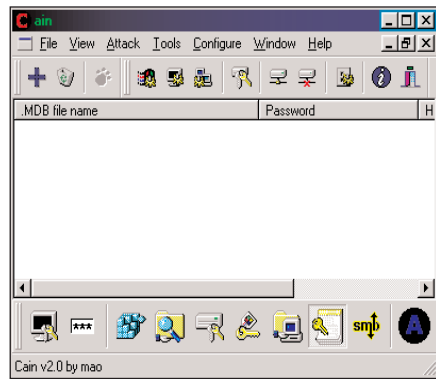
10 INSERT REMOTE SHARE

Ini yang paling seru, mencari password di komputer orang! Dapatkan IP dari komputer yang dapat diakses (dapat menggunakan Legion 2.1) atau dalam contoh ini dalam LAN yang sama. Klik ikon ke-7 lalu klik tanda + untuk menampilkan menu dialog 'Insert a remote share'.



11 REMOTE SHARES PASSWORD

Pada LAN contoh ini terdapat tiga remote share pada dua komputer. Untuk meng-crack password di masing-masing share cukup double click pada masing-masing share dan apabila terdapat cached password (baru diketik atau tidak ada) maka anda langsung terhubung ke share tersebut.



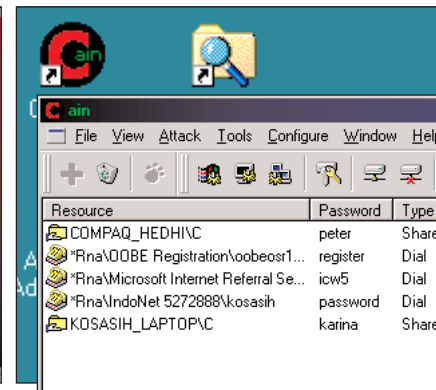
12 ACCESS PASSWORD MANAGER

Microsoft Access menggunakan sistem password yang amat lemah dan dengan Cain anda dapat langsung mendapatkan password dari suatu file .MDB serta dapat pula mengubahnya melalui Cain. Telah teruji pada Microsoft Access 97.



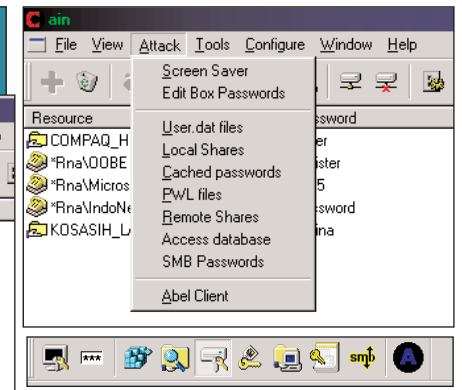
1 INSTAL CAIN 2.0

Instal Cain 2.0 dari CD NeoTek atau dapat juga di-download dari <http://www.oxid.it>. Akan tampil layar awal instalasi Cain 2.0, klik **Next** dan ikuti langkah-langkahnya sampai selesai.



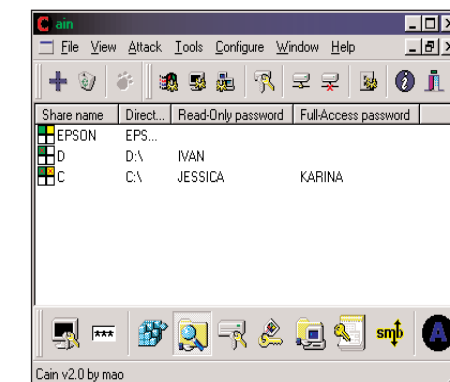
2 ICON CAIN PADA DESKTOP

Akan tampak ikon Cain v2.0 pada desktop komputer anda. Double click ikon ini untuk menjalankan Cain. Langsung Cain akan menunjukkan semua cache password yang terdapat pada komputer anda.



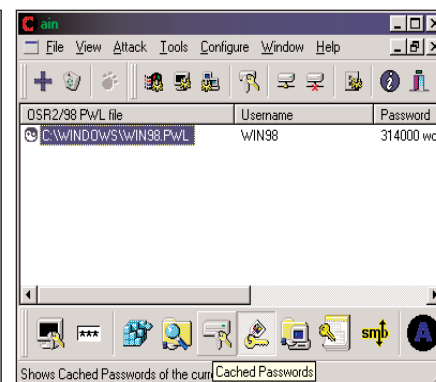
3 FITUR-FITUR CAIN 2.0

Dari menu Attack atau ikon di bagian bawah terlihat secara berurutan fitur-fitur: screen saver, edit box password, user .dat files, local shares, cache passwords, PWL files, remote shares, SMB passwords, dan Abel client.



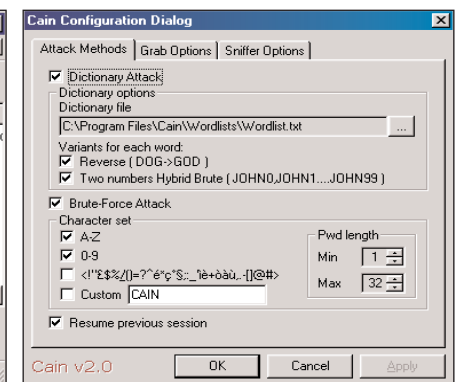
7 LOCAL SHARE

Untuk menunjukkan share yang terdapat pada komputer anda, klik ikon keempat (Attack > Local Shares) dan akan tampil tiga shares yaitu printer dan dua hard disk. Hard disk D hanya read-only sedangkan hard disk C bisa full atau read-only, tergantung password-nya.



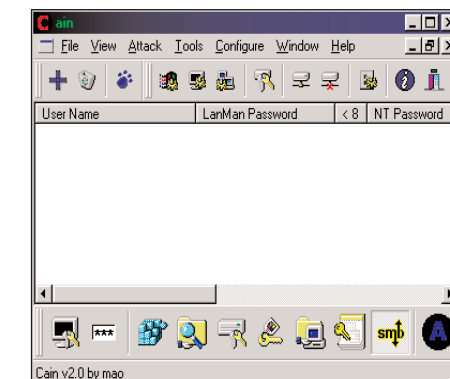
8 PWL FILE

Untuk mendapatkan password yang tersimpan pada PWL file klik ikon kelima. Terlihat bahwa PWL tersebut dibentuk oleh Windows 98 release 2 (OSR2/98) yang lebih sulit di-crack. Untuk meng-crack-nya dengan dictionary attack dan brute force, double click padanya.



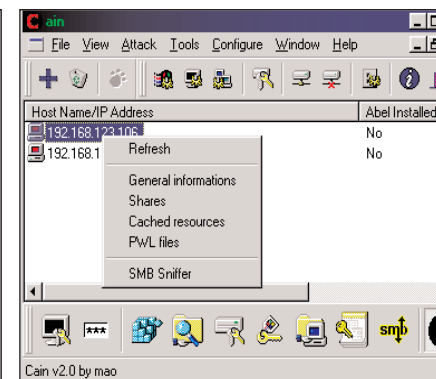
9 CAIN CONFIGURATION

Dictionary dan brute force attack di Langkah 8 dapat dikonfigurasi dengan klik menu Configure yang akan menampilkan Cain Configuration Dialog. Anda dapat men-set apakah karakter-karakter di luar abjad dan angka akan dipakai dalam brute force dan kamus apa yang akan dipakai.



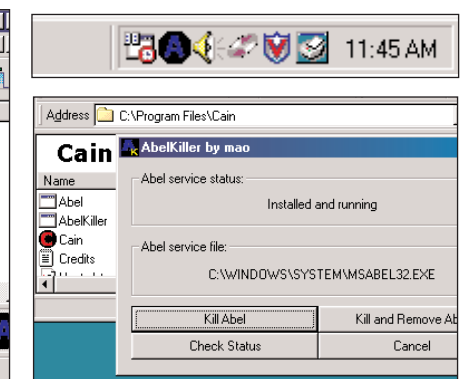
13 SMB PASSWORD RECOVER

Cain memungkinkan anda mendapatkan Windows 9x/ME/NT dan Samba password dengan jalan mendekripsi MD4 hash-nya. MD4 hash dapat diperoleh dari file SAM pada NT serta melalui tool seperti Pwdump, Pwdump2, L0phtcrack, serta melalui sniffing.



14 ABEL CLIENT

Cain juga merupakan client dari Abel. Klik ikon paling kanan bawah dan klik + serta masukkan IP address dari komputer yang diketahui dapat diakses (pada LAN atau di luar dengan Legion). Klik kanan dan pilih Refresh. Tampak bahwa Abel server belum terpasang.



15 KILL ABEL DI KOMPUTER LOKAL

Pada komputer anda sendiri terdapat Abel server (artinya anda dapat diserang dari luar). Matikan Abel dengan menjalankan killabel.exe yang terdapat pada direktori \Program Files\Cain (diakses melalui Windows Explorer dan double click pada killabel.exe).

CAIN & ABEL 2.0 MENGENDALIKAN REMOTE COMPUTER

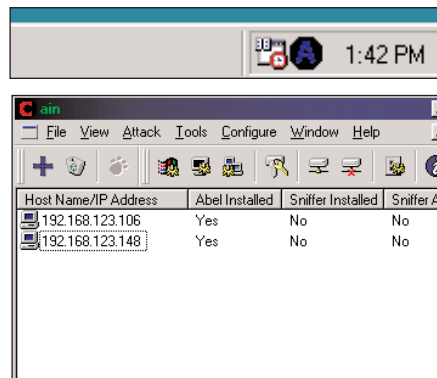
Selain password cracking terhadap local computer, kelebihan Cain adalah fungsinya sebagai **Abel client**, yang memonitor dan mengendalikan *remote computer* yang telah terpasang Abel server. Abel server akan secara terotomatis terpasang juga sewaktu anda menginstal Cain. Jadi hati-hati!

Abel server yang terpasang pada suatu komputer membuatnya dapat diakses lewat Internet.

Sewaktu instalasi Cain, akan terbentuk pula abel.exe yang apabila komputer di-boot akan mengaktifkan Abel server dengan menjalankan Abel.exe tadi. Abel server hanya dapat di-nonaktifkan lewat Cain.

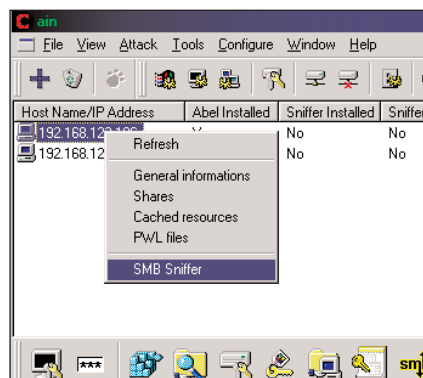
Walaupun abel server sudah dinonaktifkan dan abel.exe sudah dihapus, namun sewaktu boot tetap saja abel server dijalankan (tanpa sepengeahuan kita) sebab dengan menjalankan abel.exe akan terbentuk msabel32.exe pada direktori Windows\system serta registri khusus yang akan menjalankan Abel server setiap kali boot.

Karena berbahaya, abel.exe dan msabel32.exe akan dikenali sebagai virus PWL. Cain Password Stealer oleh kebanyakan antivirus.



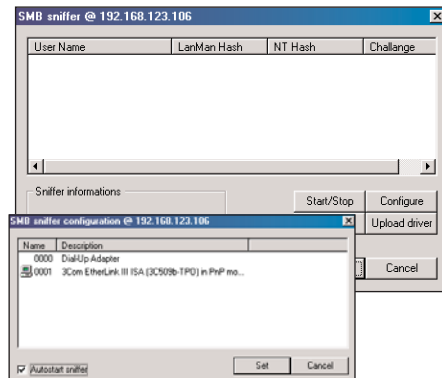
4 ABEL.EXE AKTIF

Kini, pada remote computer, abel.exe sudah aktif, terlihat dari tanda A pada toolbar. Pada komputer remote yang lain sebenarnya Cain sudah dihapus, tetapi tunggu... abel server tetap aktif tanpa disadari. Jadi di komputer anda sekarang pun ada abel server yang berjalan.



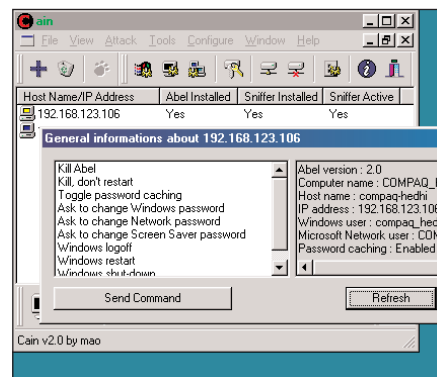
5 BISA APA SAJA?

Apa saja yang bisa dilakukan terhadap remote computer yang sudah terpasang abel server? Klik kanan pada Host name dan di bawah Refresh terdapat: General Information, Shares, Cached Resources, PWL files, dan SMB Sniffer.



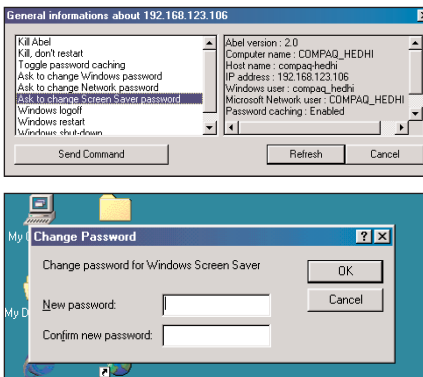
6 SMB SNIFFER

Cain dapat meng-crack password yang diperoleh dengan melakukan sniffing melalui network card yang tersedia. Klik SMB Sniffer dan jendela dialog SMB Sniffer @192.168.123.106 klik tombol Configure dan tetapkan (Set) adapter LAN pada remote computer sebagai sniffer. Tick autostart sniffer.



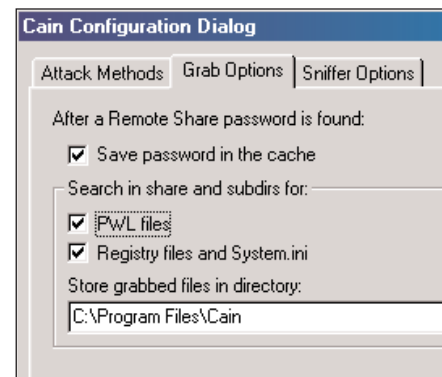
10 GENERAL INFORMATION

Pilihan General Information sebenarnya lebih dari sekedar informasi. Memang terdapat informasi tentang remote host di window pane kanan, namun di window pane kiri terdapat command untuk remote host. Salah satunya adalah Toggle Password Caching. Pilih lalu klik Send Command.



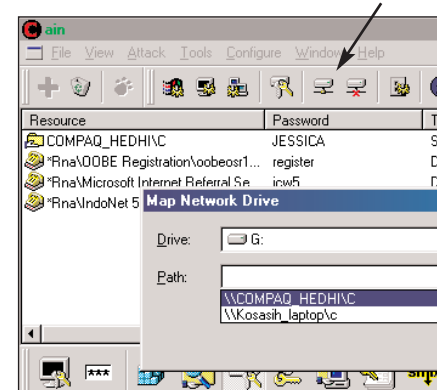
11 SEND COMMAND YANG LAIN

Masih banyak perintah lain yang dapat dikirim ke remote host. Di antaranya mematikan Abel (Abel server tidak dapat dimatikan dari host itu sendiri) atau dapat juga kita meminta pemakai komputer host mengganti password windows, network, atau screen saver. Semuanya akan di-sniffing tentu.



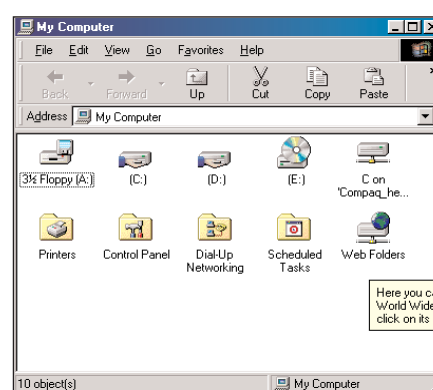
12 CAIN CONFIGURATION

Klik menu Configure pada Cain dan pilih tab Grab Option. Tampak apa saja yang dipilih untuk diambil: cache password, PWL files, atau registry file serta system.ini. Semuanya disimpan secara default di C:\Program Files\Cain



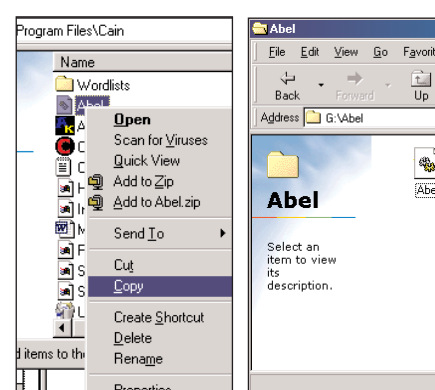
1 MAP NETWORK DRIVE

Terhadap remote resource yang sudah connected, kita bisa lakukan mapping sebagai local resource. Klik icon Map Network Drive dan tetapkan suatu share (di sini \\COMPAQ_HEDHI\C) ke G: di komputer lokal anda.



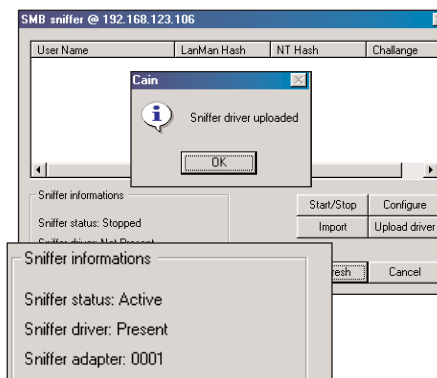
2 DRIVE G; PADA MY COMPUTER

Klik icon My Computer pada desktop dan di dalamnya akan tampak drive G: yang merupakan network drive yang di-mapping menjadi drive G: di komputer anda. Anda bisa perlakukan drive ini sebagai drive anda sendiri.



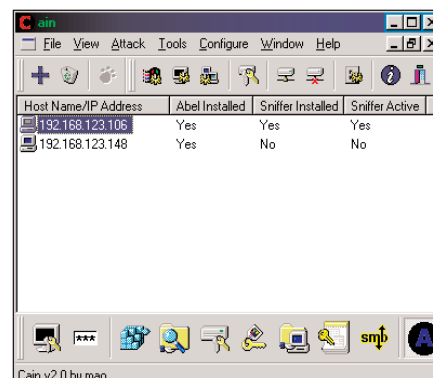
3 COPY-KAN ABEL.EXE

Copy-kan abel.exe dari C:\Program Files\Cain ke drive G: ini. Pada contoh dibuatkan direktori Abel pada network drive tersebut. Misalkan pemilik drive itu terjebak menjalankan abel.exe.



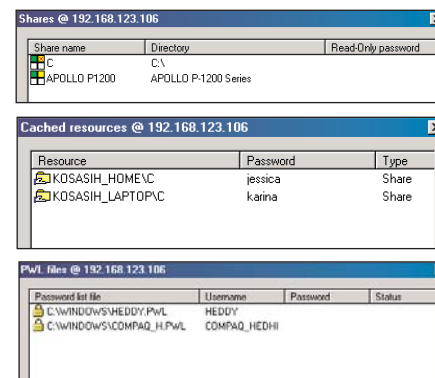
7 UPLOAD DRIVER & AKTIFKAN

Selanjutnya klik tombol Upload driver untuk meng-upload sniffer driver (Klik OK), lalu klik tombol Start/Stop untuk mengaktifkan atau menonaktifkan kegiatan sniffing pada remote computer tadi. Terakhir klik tombol Refresh untuk melihat status terakhir, yaitu Sniffer diaktifkan.



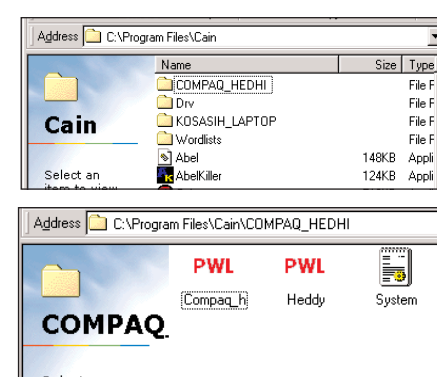
8 REFRESH STATUS REMOTE

Pada Host Name/IP Address klik kanan dan pilih Refresh dan status kedua remote host di-update. Tampak pada kedua host abel server telah terinstal, tetapi hanya pada yang pertama sniffer telah terpasang dan diaktifkan.



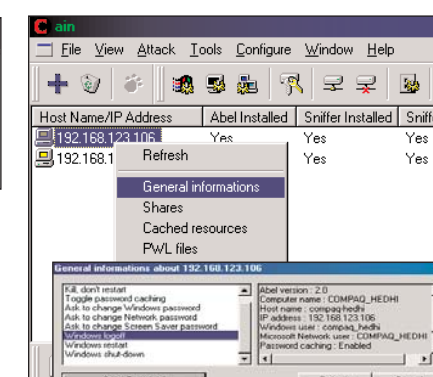
9 FASILITAS REMOTE LAIN

Selain mengaktifkan SMB Sniffer, terdapat fasilitas-fasilitas lain terhadap remote host, yaitu: menampilkan Shares, Cache Resources, dan PWL files. Semua ini adalah informasi yang ada pada remote host, bukan yang ada pada local computer anda.



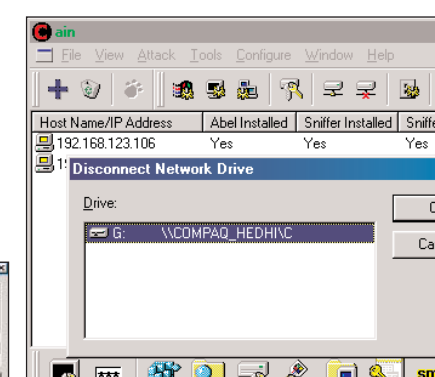
13 DIREKTORI UNTUK TIAP HOST

Tampak pada direktori itu terbentuk dua subdirektori yang masing-masing untuk host yang diakses oleh Cain. Di dalam setiap subdirektori terdapat file-file PWL dan system.ini yang diperoleh dari masing-masing host. Waktu untuk meng-crack kini di pihak anda.



14 MAU ISENG JUGA?

Perintah lain yang dapat dikeluarkan pemakai di komputer host adalah Windows Logoff, Windows restart, dan Windows shutdown. Tapi ini juga ada fungsinya sebab dengan cara ini pemakai yang tidak sadar dirinya dikendalikan akan mengetikkan password kembali.



15 DISCONNECT NETWORK DRIVE

Bila kegiatan sudah selesai, anda dapat memilih opsi Disconnect Network Drive. Ini bukan berarti akses terhadap host terhenti. Abel server akan terus bekerja apabila host berjalan dan bila terhubung ke Internet (atau LAN) akan mengirimkan hasil sniffing ke Abel client.

LOPHTCRACK 3 NT PASSWORD CRACKER

Pada dasarnya semua password dapat di-crack, yang membedakan suatu password cracker dari lainnya adalah kecepatan dalam melakukan dictionary attack atau brute force attack. Salah satu password cracker yang tangguh adalah **Lophthcrack**. **David Sugianto** memperkenalkannya untuk anda.

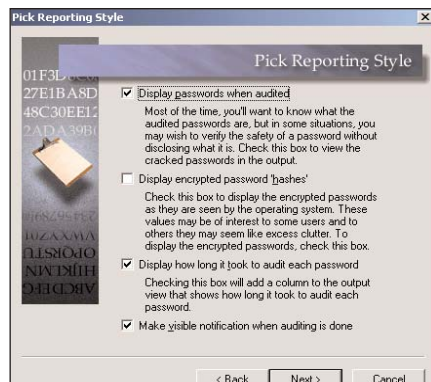
Lophthcrack yang menggunakan kamus dalam proses cracking, dilengkapi juga dengan sniffer.

Lophthcrack dibuat oleh suatu kelompok administrator ahli yang menamakan diri mereka dengan sebutan "Lophth." Program ini banyak digunakan oleh para administrator NT/2000 untuk menguji password komputer maupun password user mereka.

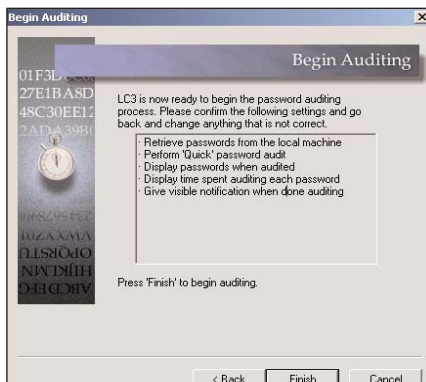
LophthCrack mengaudit dan memulihkan password dengan berbagai cara. Pada dasarnya menggunakan kamus untuk menemukan password. Jika kata dalam kamus tersebut sesuai dengan password, maka akan ditampilkan pada layar.

Karena itu janganlah bosan mengkoleksi kamus kata-kata, yang bisa anda dapatkan di situs internet.

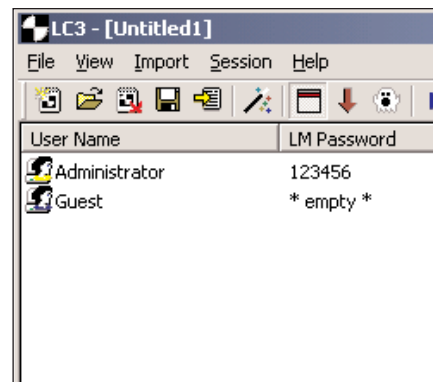
david_sugianto2002@yahoo.com



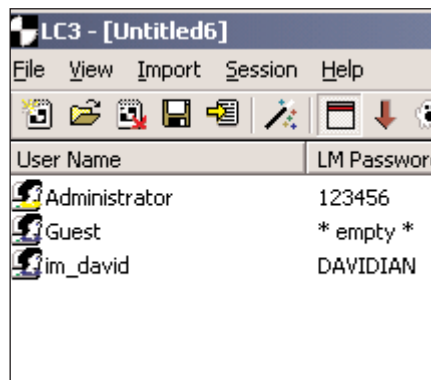
4 TAMPILAN LAPORAN
Bentuk laporan pun dapat dipilih: menampilkan password sewaktu audit, menampilkan password hashed terenkripsi, menampilkan lamanya audit, dan menampilkan proses audit.



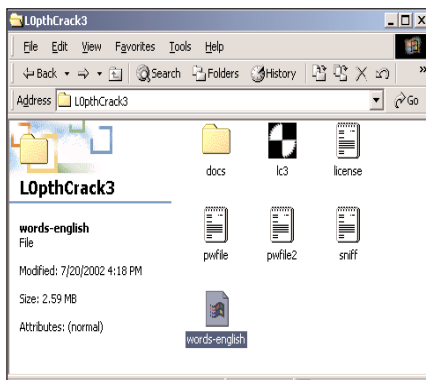
5 Konfirmasi
Sebelum proses audit dilakukan, anda diberi kesempatan untuk memeriksa kembali pengaturan yang anda buat sebelumnya, jika sudah sesuai, klik **Finish**.



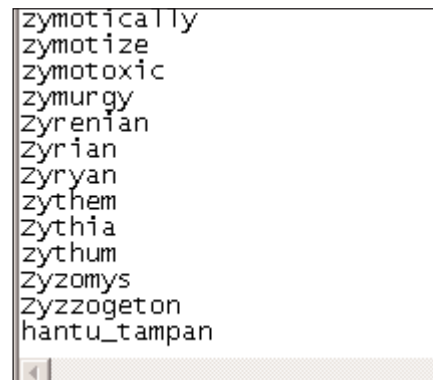
6 TAMPILAN PASSWORD
Aha... ternyata password administrator pada komputer yang sedang digunakan adalah **123456** dan password untuk Guest kosong (*** empty ***).



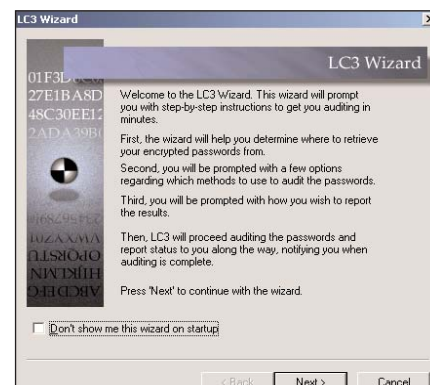
10 TAMPILAN PASSWORD
Lakukan seperti langkah 1–6, kemudian hasilnya pun akan segera keluar. Password user yang baru anda buat juga dapat di-crack dan ditampilkan. Buatlah user baru lagi dengan username **Anton** dan password **hantu_tampan**.



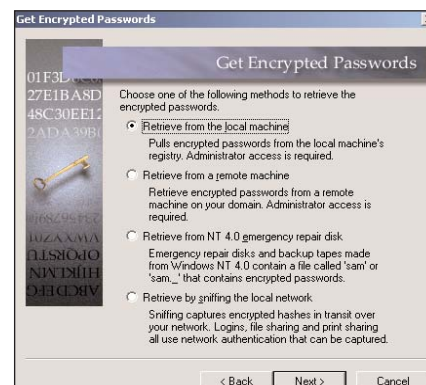
11 BUKA KAMUS
Dengan Windows Explorer masuk ke folder tempat program LophthCrack disimpan dan klik dua kali pada file **word-english**. Pada waktu kotak dialog **Open With...** tampil, pilih **Notepad** untuk membukanya.



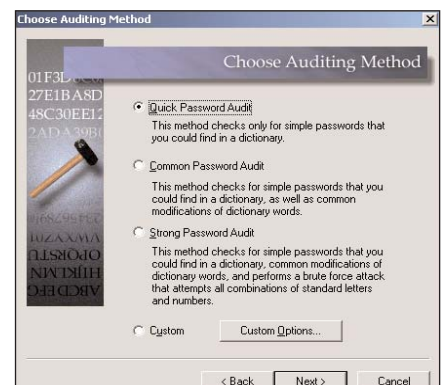
12 MENAMBAH KATA
Tambahkan **hantu_tampan** pada daftar kata yang ada di dalam file word-english dan kemudian simpan dengan nama yang sama.



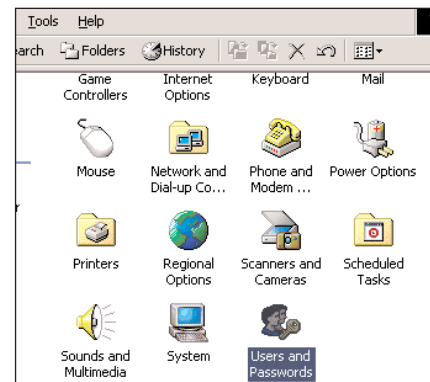
1 LAYAR WIZARD
Tampilan wizard akan muncul ketika anda menjalankan program Lophthcrack. Jika anda ingin agar layar wizard selalu muncul, silahkan langsung klik **Next**.



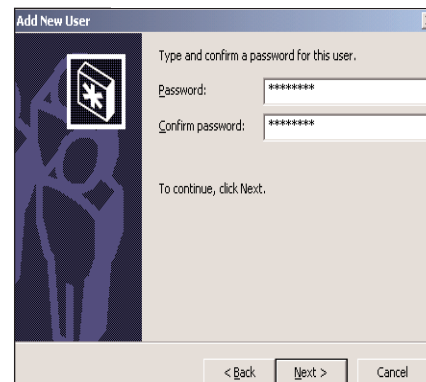
2 SUMBER PASSWORD
Lophthcrack mendapatkan password yang akan di-crack dari empat macam sumber: local machine, remote machine, NT 4.0 repair disk, dan hasil sniffing pada network. Kali ini kita coba pilihan pertama.



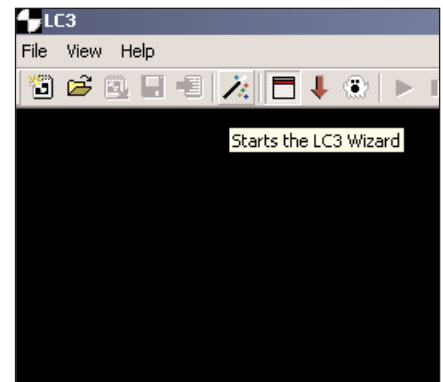
3 METODE AUDIT
LophthCrack juga dapat melakukan empat macam cara dalam meng-crack password. Pilihlah pilihan pertama yaitu **Quick Password Audit** dan klik **Next**.



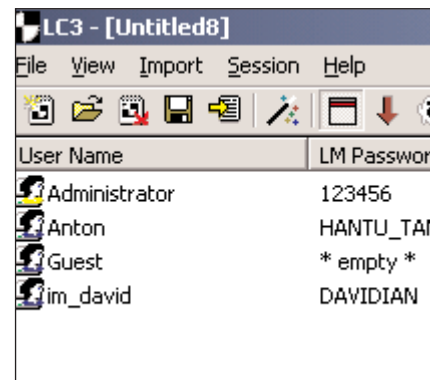
7 BUKA CONTROL PANEL
Buka Control Panel dan klik dua kali pada ikon **Users and Password** untuk menampilkan kotak dialog **User and Password**.



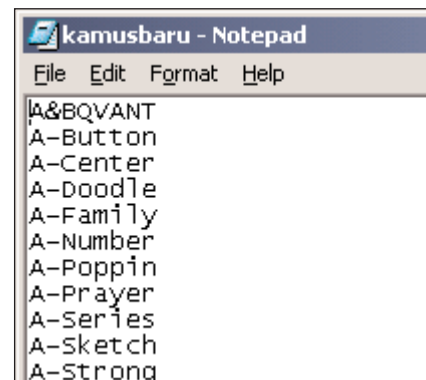
8 MEMBUAT USER BARU
Klik tombol **Add** untuk membuat user baru dan kotak dialog **Add New User** akan muncul. Isikan Username dengan **im_david** lalu klik **Next** dan isi password dengan **dauidian**. Lalu daftarkan sebagai group **Guest**.



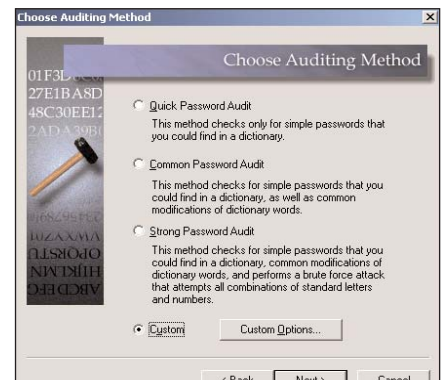
9 MEMBUKA LAYAR WIZARD
Klik ikon bergambar tongkat sulap pada toolbar atau pilih menu **File > LC3Wizard** untuk menampilkan layar wizard



13 TAMPILAN PASSWORD
Berhasil... password pada user Anton kini dapat di-crack serta ditampilkan. Hal ini menunjukkan bahwa Lophthcrack bekerja berdasarkan file kamus yang tersedia.



14 BUAT KAMUS
Buatlah kamus kata anda sendiri yang terdiri atas kata-kata yang umum untuk dijadikan password. Atau anda dapat juga mendapatkannya dari internet melalui situs yang menyediakan. Simpanlah pada folder tempat program LophthCrack disimpan.



15 MENGGANTI KAMUS
Kembali ke layar wizard dan ketika tiba pada layar seperti diatas, silahkan pilih **Costum** kemudian klik **Costum Option...** Ubah kamus yang akan digunakan untuk melakukan audit password dengan mengisi nama file kamus anda pada kotak teks.

ADVANCED OFFICE 2000 PASSWORD RECOVERY MEMULIHKAN PASSWORD WORD DAN EXCEL

Kebiasaan gonta-ganti password kadang menjadi bumerang bagi kita sendiri. **Happy Chandraleka** menguraikan cara mengatasi password yang terlupa lewat artikel di bawah ini.

Praktik memulihkan password pada dokumen Word dan Excel.

Membuat *password* merupakan solusi yang jitu untuk mencegah orang-orang yang tidak berkepentingan mendapatkan informasi dari dokumen yang telah kita simpan.

Rasa was-was akan terbongkarnya data-data penting pada dokumen kita menyebabkan kita sering kali mengganti-ganti password. Namun tidak jarang upaya proteksi itu malah menjadi bumerang bagi kita sendiri yaitu jika kita lupa akan password yang telah masukkan pada dokumen yang kita buat tersebut.

Kali ini penulis akan menjelaskan satu cara untuk mengetahui password pada dokumen kita sendiri. Tujuannya hanya satu yaitu mengembalikan password

kita yang hilang yang kebanyakan disebabkan oleh karena anda lupa akan password itu.

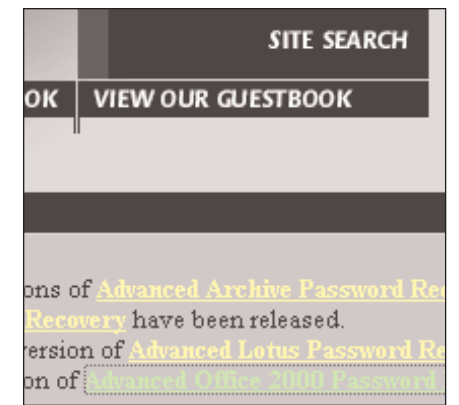
Program yang digunakan untuk tujuan ini adalah Advanced Office 2000 Password Recovery. Program ini bekerja dengan metode Brute Force. Dengan metode ini, Advanced Office 2000 melakukan pencarian password dengan membandingkannya pada kombinasi teks yang terbentuk dari karakter-karakter.

Biasanya Brute Force membutuhkan waktu lama sebab menggunakan semua kombinasi yang mungkin untuk membentuk password dari karakter-karakter yang ada.

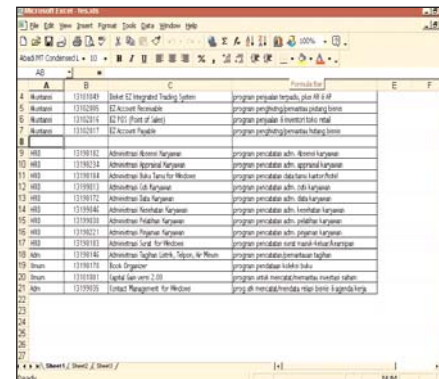
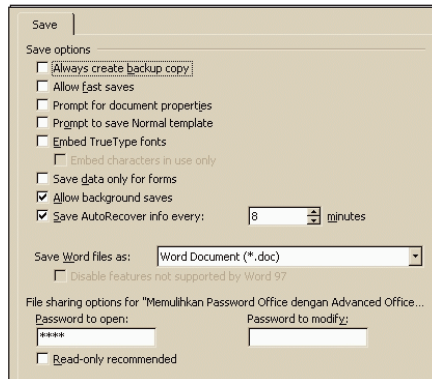
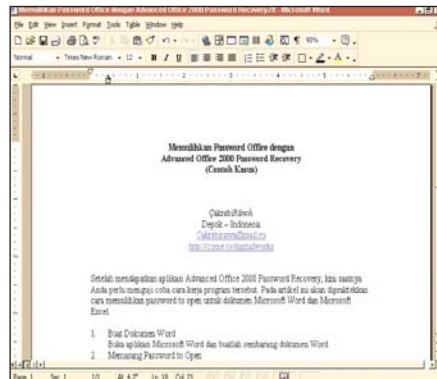
Versi *un-registered* program Advanced Office 2000 Password Recovery bisa diperoleh gratis dari **Elcomsoft** (www.elcomsoft.com/ao2000pr.html) atau dari CD NeoTek bulan ini.

Aplikasi ini kemudian dapat anda instal di komputer anda. Setelah itu anda dapat menggunakannya untuk memulihkan atau mencari kembali password yang telah anda masukkan pada dokumen Office anda dan anda telah lupa. Pada artikel ini akan dipraktikkan cara memulihkan "Password to Open" untuk dokumen Microsoft Word dan Excel.

Apabila ada pertanyaan, penulis dapat dihubungi di hchandreka@telkom.net



• Advanced Office 2000 Password Recovery dapat diperoleh di www.elcomsoft.com/ao2000pr.html atau pada CD Neotek bulan ini.



1 MEMBUAT DOKUMEN WORD

Buka aplikasi Microsoft Word dengan memilih Start → Programs → Microsoft Word. Setelah bidang kerja jendela Microsoft Word tampil, buatlah sembarang dokumen Word untuk percobaan.

2 MEMASANG PASSWORD TO OPEN DI WORD

Selanjutnya pilih File → Save As. Lalu pilih Tools → General Options. Isikan kata "pass" pada bagian "Password to Open" dan tekan tombol Ok. Isikan lagi kata "pass" pada kotak dialog "Confirm Password." Simpan dokumen Word tersebut.

3 MEMBUAT DOKUMEN EXCEL

Buka aplikasi Microsoft Excel dengan memilih Start → Programs → Microsoft Excel. Bila bidang kerja Microsoft Excel telah tampil, buat saja sembarang dokumen Excel untuk percobaan.

4 MEMASANG PASSWORD TO OPEN DI EXCEL

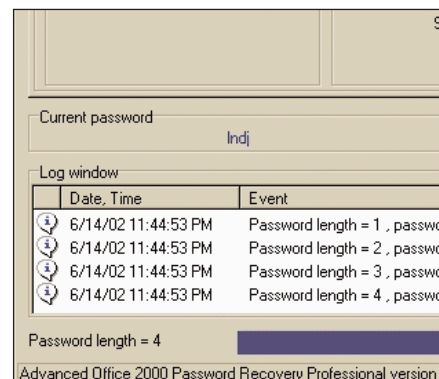
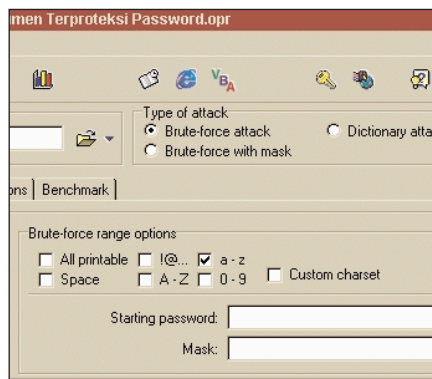
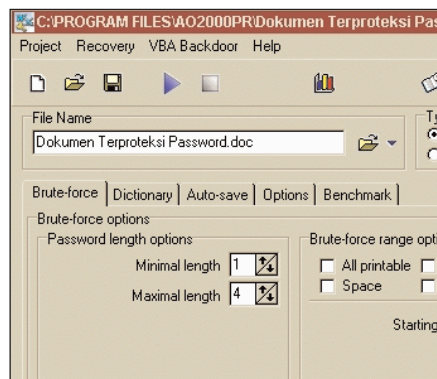
Kemudian pilih File → Save As, dan lanjutkan dengan Tools → General Options. Pada Save Options, isikan "piss" pada "Password to Open." Tekan OK dan isikan lagi kata "piss" pada Confirm Password. Simpan dokumen Excel tersebut.

5 THE SHOW BEGINS

Jalankan aplikasi Advance Office 2000 Password Recovery yang telah Anda instal dengan memilih menu Start → Programs → Advanced Office 2000 Password Recovery → Advanced Office 2000 Password Recovery.

6 PILIH DOKUMEN WORD

Pilihlah dokumen Word yang terproteksi password yang telah anda buat pada Langkah 1 dan 2. Anda cukup mengklik ikon folder pada kotak "File Name." Pada kotak dialog "Open," cari file dokumen Word tersebut.



7 PASSWORD LENGTH OPTIONS

Kotak "Brute-force options" mempunyai dua bagian yaitu Password Length dan range options. Pada kotak Password length options, pastikan Minimal length-nya berisi '1' dan Maximal length-nya berisi '4', yang merupakan nilai tertinggi untuk versi *trial* ini.

8 BRUTE-FORCE RANGE OPTIONS

Kursor akan berpindah ke offset 28172 yang merupakan awal tulisan Log Off yang dimaksud. Tuliskan memanjang dari offset 28172 sepanjang F h offset. Inilah yang akan kita ganti.

9 MEMULAI PENCARIAN

Setelah semua setting-nya siap, anda dapat langsung memulai pencarian password. Gunakan menu Recovery → Start. Lama pencarian password tergantung dari panjang password dan pilihan jangkauannya.

10 DITEMUKAN!

Proses pencarian password berlangsung beberapa lama. Dan bila ditemukan akan tampil kotak dialog statistik. Pada baris keempat di kotak "Password for this file" akan berisi password untuk dokumen Word ini yaitu "pass."

11 JUGA PADA DOKUMEN EXCEL

Ulangi langkah 6 sampai 10 untuk dokumen Excel. Bila berhasil akan tampil kotak dialog yang akan memberitahukan password dokumen tersebut yaitu "piss." Anda dapat bereksperimen dengan dokumen yang lain.

12 HELP!

Kurang jelas? Atau ingin tahu lebih jauh tentang keandalan program ini? Anda dapat memanfaatkan file bantuannya dengan memilih menu Help → Help Contents. Ingin tahu lebih jauh lagi? Kunjungi situs Web-nya.

ADVANCED ARCHIVE PASSWORD RECOVERY MEMULIHKAN PASSWORD WINZIP

Lupa password yang anda berikan pada file winzip yang anda buat? **Happy Chandraleka** memberi jalan keluar dengan utilitas Advanced Archive Password Recovery.

Setelah dijelaskan cara memulihkan password yang terlupakan pada dokumen Microsoft Office, kali ini disajikan cara mendapatkan kembali password yang terlupakan pada file dokumen lain di luar Microsoft Office, dengan menggunakan program Advanced Archive Password Recovery.

Seperti Advanced Office 2000 Password Recovery, program ini pun adalah produk dari Elcomsoft dan versi *unregistered*-nya dapat di-download gratis lewat situs Elcomsoft (www.elcomsoft.com/archpr.html) atau didapatkan dari CD NeoTek bulan ini.

Program ini pun menggunakan metode Brute-Force dalam operasinya. Pada ba-

gian terdahulu sudah dijelaskan, karena cara kerjanya, Brute-Force kadang kala membutuhkan waktu lama untuk bisa menyelesaikan pekerjaannya yaitu memperoleh password yang anda cari.

Untuk menjelaskan cara kerja Advanced Archive Password Recovery, pada artikel ini dipraktikkan cara kerjanya mendapatkan kembali password pada sebuah file percobaan yang dibuat dengan menggunakan utilitas kompresi yaitu WinZip.

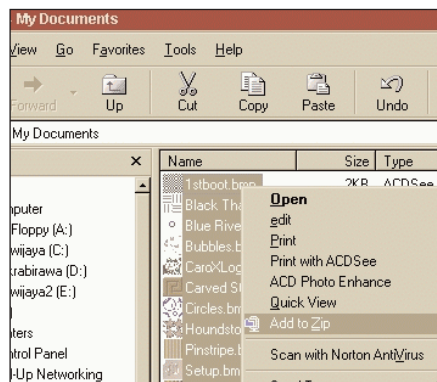
Anda sudah tentu dapat menggunakan utilitas pencari password ini untuk dokumen-dokumen yang dibuat dengan program lain. Dan seperti yang anda

akan jumpai pada artikel ini, penggunaan Advanced Archive Password Recovery ini sederhana dan mudah.

Apabila ada pertanyaan mengenai artikel ini, penulis dapat dihubungi di hchandreleka@telkom.net

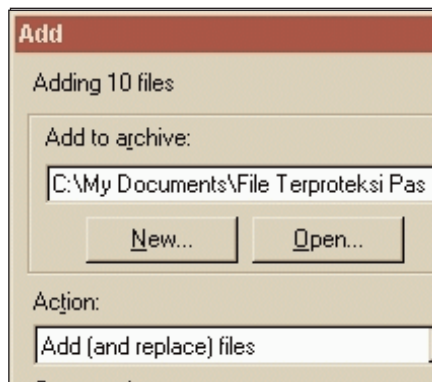


Praktik memulihkan password yang hilang pada archive file



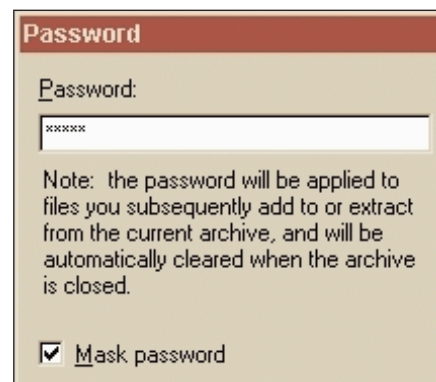
1 FILE KELINCI PERCOBAAN

Copy-kan beberapa file percobaan ke direktori "My Documents." Pada contoh ini di-copy-kan beberapa file bitmap dari direktori Windows. Sorot seluruh file tersebut dan klik kanan kemudian pilih menu "Add to Zip."



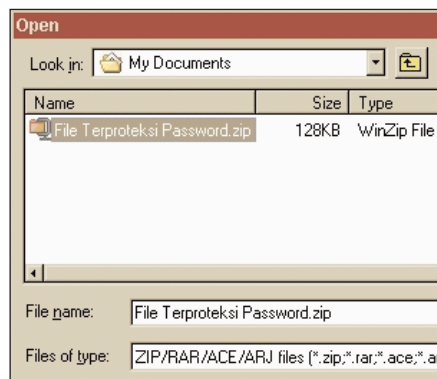
2 KOTAK DIALOG ADD

Akan tampil kotak dialog "Add." Pada kotak "Add to archive," beri nama filenya dengan "File Terproteksi Password," sehingga lengkapnya menjadi "C:\My Documents\File Terproteksi Password." Biarkan pilihan-pilihan lainnya.



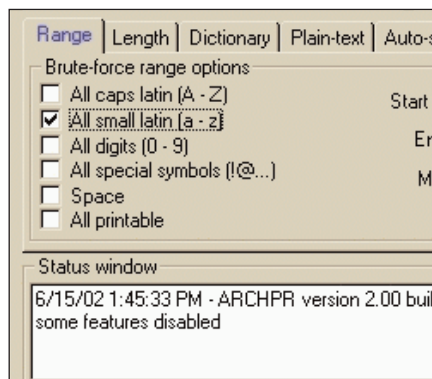
3 MEMBERI PASSWORD

Pada kotak dialog "Add" tersebut, selanjutnya tekan tombol "Password" di pojok kanan bawah. Kotak dialog "Password" akan tampil. Isikan kata 'sandi' pada kotak Password dan tekan tombol OK. Ulangi pengisian pada kotak dialog yang tampil dan tekan OK.



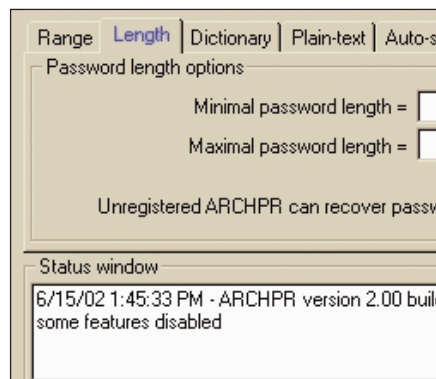
7 MENENTUKAN FILE

Tentukan file yang akan dicari password-nya. Anda cukup menekan ikon folder pada kotak Encrypted ZIP/RAR/ACE/ARJ-file. Kotak dialog "Open" akan tampil. Carilah file yang terproteksi password tersebut.



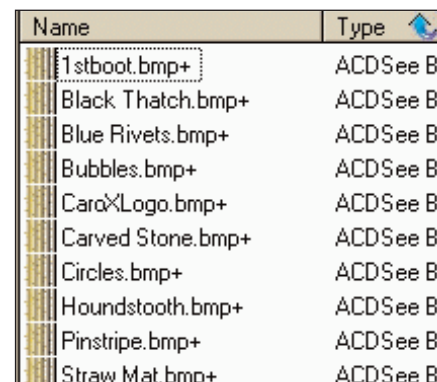
8 MENENTUKAN RANGE

Pada tab "Range," tentukan pilihan opsinya. Pilihan opsi ini menentukan kecepatan dan akurasi program dalam mencari password. Pilih saja opsi "All Small." Bisa saja anda memilih opsi "All printable," tetapi akan memakan waktu yang lama.



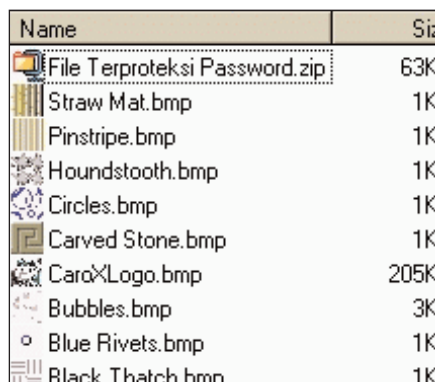
9 PASSWORD LENGTH

Pada tab "Length," tentukan juga panjang minimal dan maksimal password-nya. Untuk minimal, isikan nilai '1' dan untuk maksimal, isikan nilai '5', yang merupakan nilai tertinggi untuk versi *unregistered* ini.



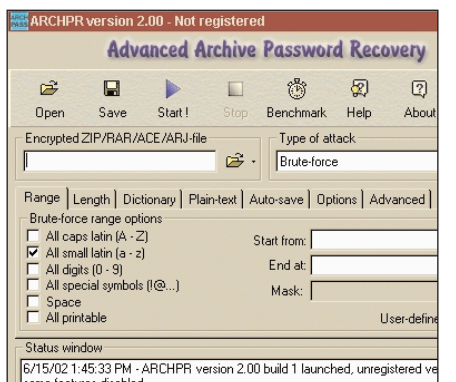
4 PROSES PENGEPAKAN

Kemudian tulisan di title bar akan berganti dengan "Add with Password." Lanjutkan proses dengan menekan tombol "Add" di pojok kanan atas. Winzip akan melakukan proses pengepakan. Setelah selesai, di akhir nama file akan terdapat tanda plus.



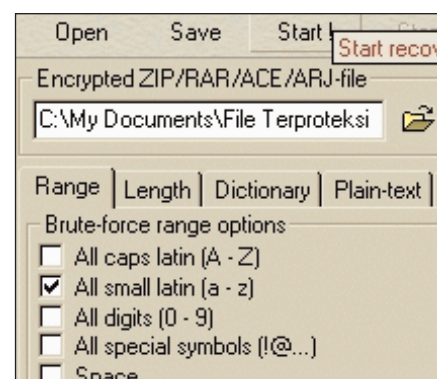
5 FILE TERPROTEKSI PASSWORD

Buka jendela Windows Explorer dan anda akan melihat hasil file zip-nya pada direktori "My Documents." File ini diproteksi dengan password yang akan dicari dengan Advanced Archive Password Recovery.



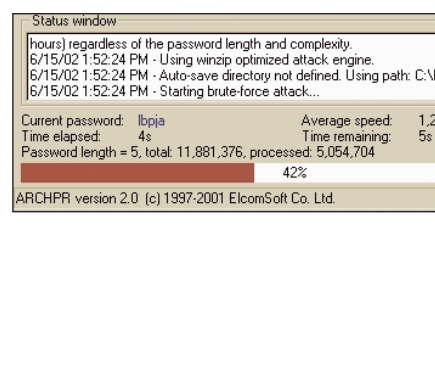
6 JALANKAN ADVANCED ARCHIVE PASSWORD RECOVERY

Jalankan program Advanced Archive Password Recovery dari Start menu kemudian Programs → Advanced Archive Password Recovery → Advanced Archive Password Recovery.



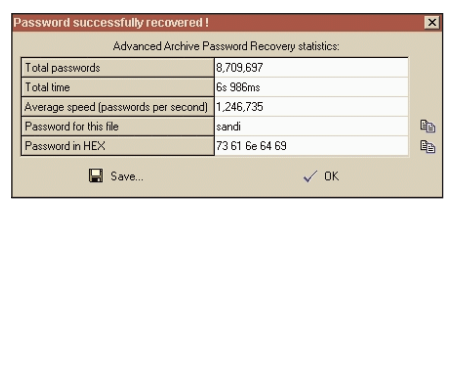
10 MEMULAI PENCARIAN

Setelah semua setting siap, anda dapat memulai pencarian password dengan menekan tombol "Start" yang berwarna biru pada toolbar aplikasi.



11 PROSES PENCARIAN

Proses pencarian password akan berlangsung beberapa waktu, bergantung pada panjang password-nya dan pilihan jangkauan Brute-Force. Anda dapat memantau proses pencarian yang diperlihatkan pada "Status Window."



12 INI DIA PASSWORD-NYA!

Proses pencarian berakhir dengan tampilnya kotak dialog yang memberi informasi mengenai statistik pencarian. Pada baris keempat tabel statistiknya diperlihatkan password untuk untuk file ini yaitu "sandi."



Menembus Password ID pada Outlook Express

Produk-produk dalam lingkungan Microsoft Office memang kurang tangguh pengamanannya. Setelah membahas betapa mudahnya mendapatkan password file Access dengan Cain dan password-password Word dan Excel dengan produk-produk Elcomsoft, kini **Fitrianto Halim** membahas betapa **lemahnya pengamanan** pada **Outlook Express**.

SALAH SATU FASILITAS YANG MENARIK pada Outlook Express (OE) sejak versi 5.0 adalah Multiple Identities, dimana dengan fasilitas tersebut setiap pemakai dapat mengkonfigurasi program OE pada identitasnya masing-masing. Konfigurasi yang dimaksud meliputi tampilan (view), account, dan lain-lain.

Selain itu, seorang pemakai dapat menambahkan password pada identitasnya, sehingga jika pemakai akan memasuki identitas tersebut akan ditanyakan password terlebih dahulu.

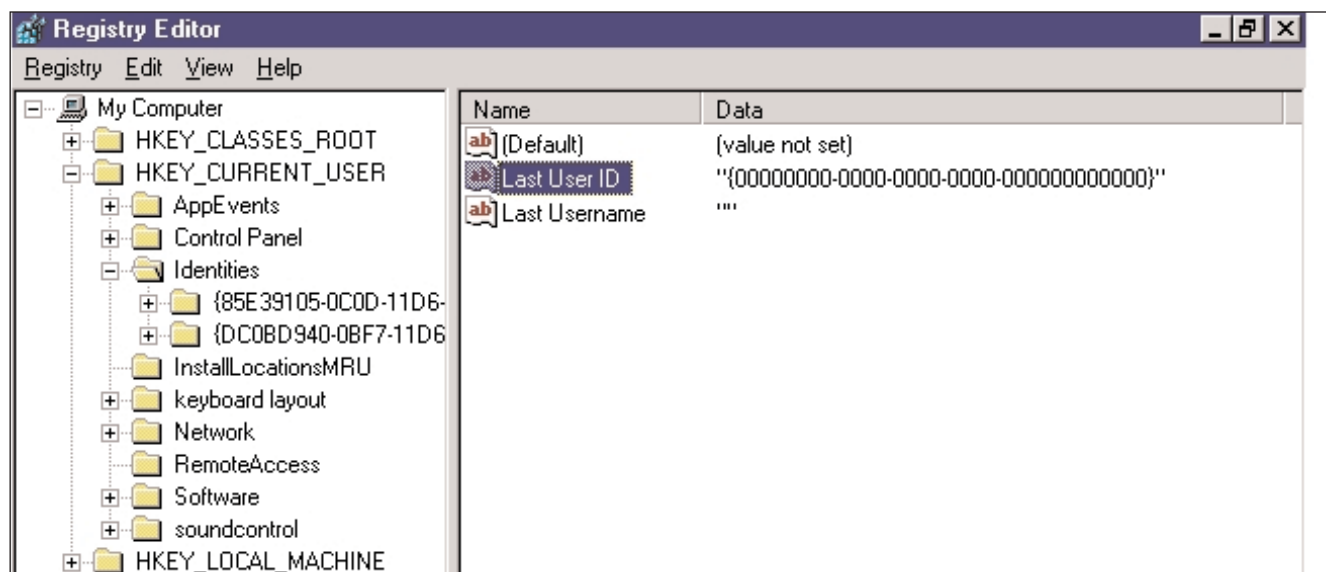
Hal ini dimaksudkan jika pemakai tersebut ingin menambahkan faktor keamanan sehingga e-mail-nya tidak dibaca dan/atau account-nya tidak di-copy oleh orang lain.

Namun, salah satu kekurangan program OE ini adalah jika pemakai tersebut lupa melakukan log off, maka ketika program OE dijalankan lagi akan langsung menuju pada identitas terakhir sekalipun pada identitas tersebut terpasang password.

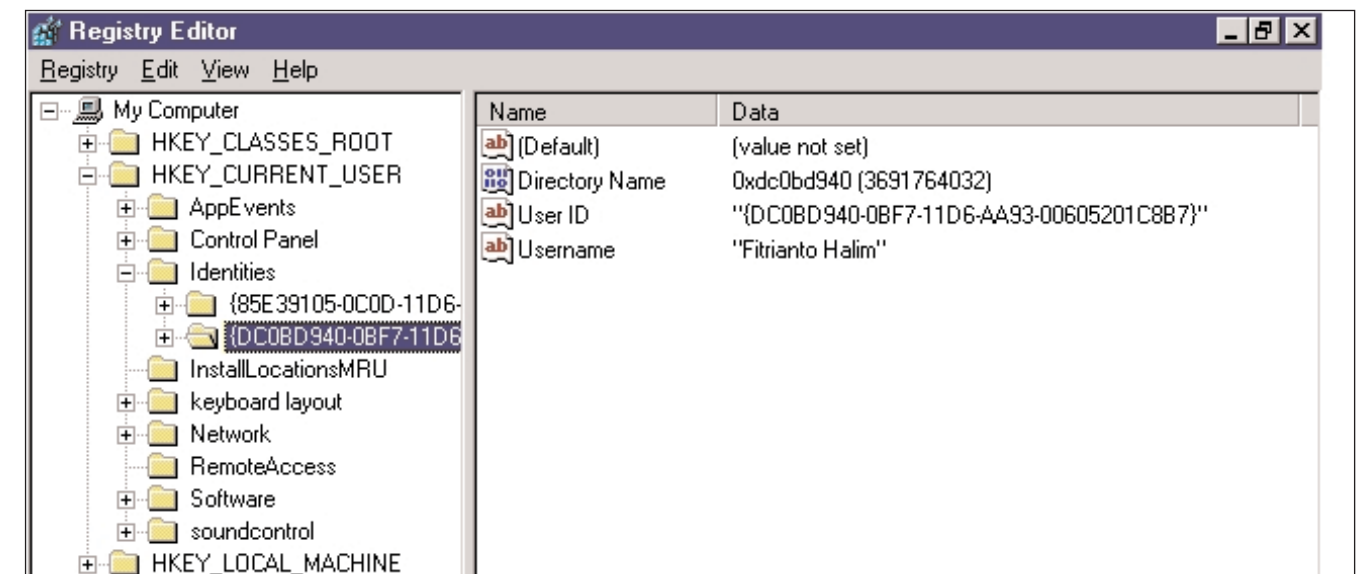
Dengan demikian, kunci untuk menerobos masuk pada suatu identitas yang terpasang password adalah membuat seolah-olah sang pemakai lupa melakukan log off pada identitas tersebut.

Melakukan hal tersebut ternyata cukup mudah, yaitu dengan memanfaatkan Registry Editor (regedit). Dibawah ini dibahas langkah-langkahnya.

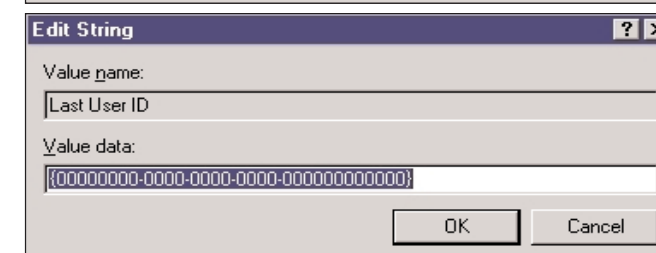
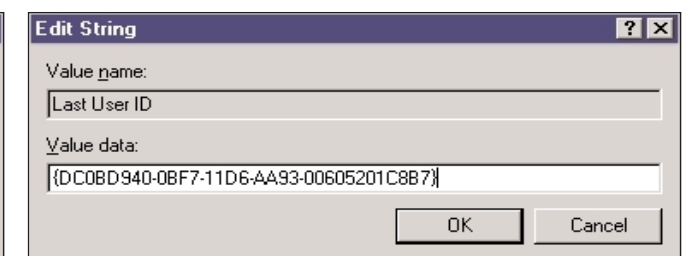
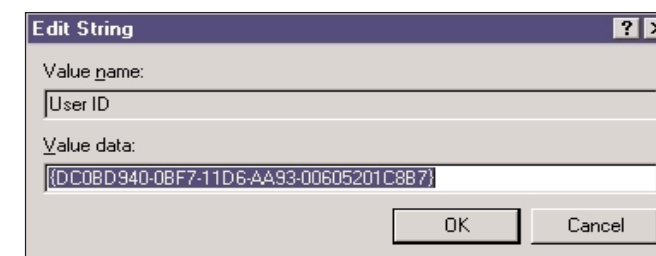
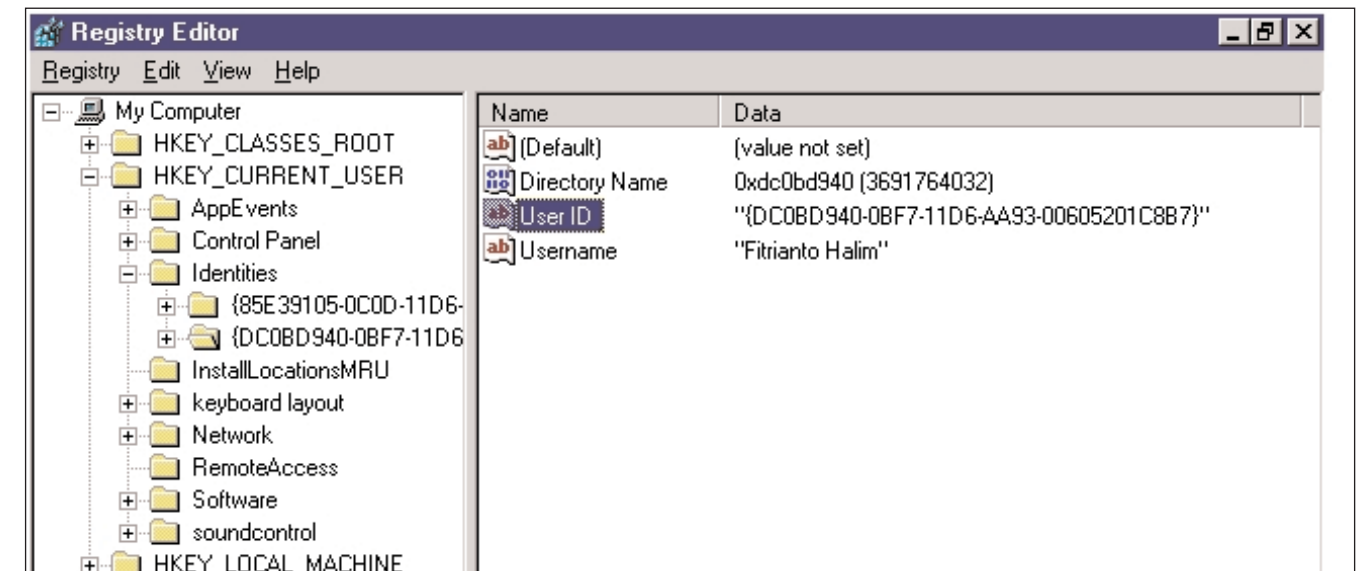
1 Jika anda telah *log off*, maka nilai registry-nya sama dengan yang diperlihatkan pada gambar di atas. Dari hasil percobaan, untuk menerobos masuk pada suatu identitas yang terpasang password adalah cukup dengan mengganti nilai Last User ID dengan ID yang anda inginkan.



2 Untuk mendapatkan ID yang anda inginkan, anda dapat mencarinya pada *subkey* dari Identities seperti yang terlihat pada gambar di bawah ini.



3 Untuk memudahkan penggantian nilai Last User ID, anda dapat melakukan Copy/Paste, seperti terlihat pada gambar-gambar di bawah ini.



Kesimpulan

Keamanan pada OE 5.x tidak baik. Oleh karena itu, jangan menyimpan *password* pada *account* anda, agar *account* anda tersebut tidak disalahgunakan oleh orang lain.

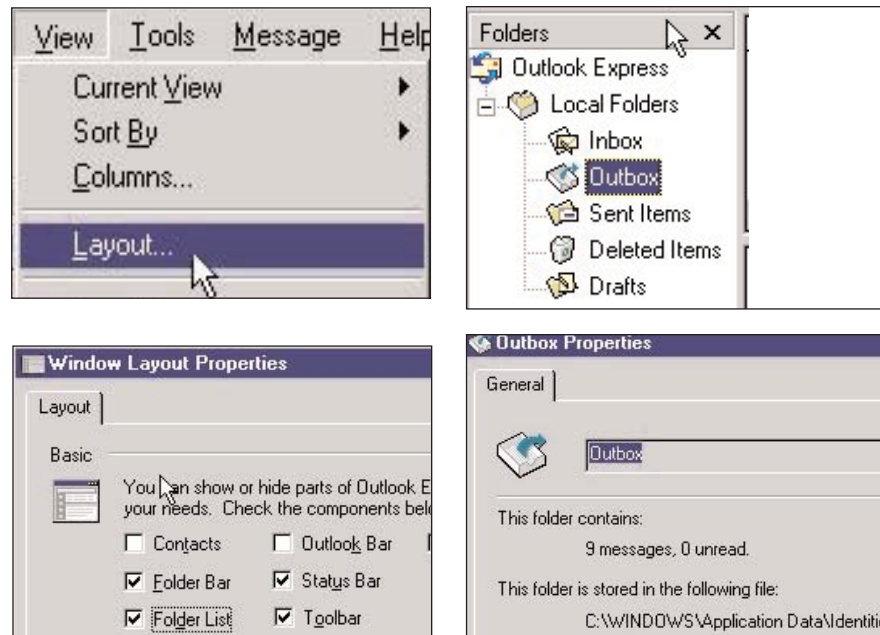
Apabila ada pertanyaan mengenai artikel ini maupun artikel lainnya mengenai Outlook Express, hubungi penulis di fitriantoh@hotmail.com

Tip Lain Seputar Outlook Express

Dimana folder Outlook Express 5.x disimpan?

Ada cara mudah untuk mengetahui dimana folder Outlook Express 5.X (OE) disimpan.

- 1 Pertama-tama masuk ke Folder List. Caranya, pada menu **View** pilih **Layout...**
- 2 Kemudian, aktifkan Folder List (ditandai dengan adanya tanda centang).
- 3 Pilih folder yang akan dilihat (misalnya Outbox); lihat property-nya (misal dengan menekan **Alt+Enter**).
- 4 Kini terlihat tempat folder tersebut disimpan pada **This folder is stored in the following file:**



Mengubah Letak Penyimpanan Folder-folder Outlook Express 5.x

Folder-folder pada Outlook Express 5.x disimpan pada file-file DBX yang bersesuaian dengan nama folder-nya. File-file tersebut secara default akan terdapat pada **C:\WINDOWS\Application Data\Identities\ID Anda\Microsoft\Outlook Express**

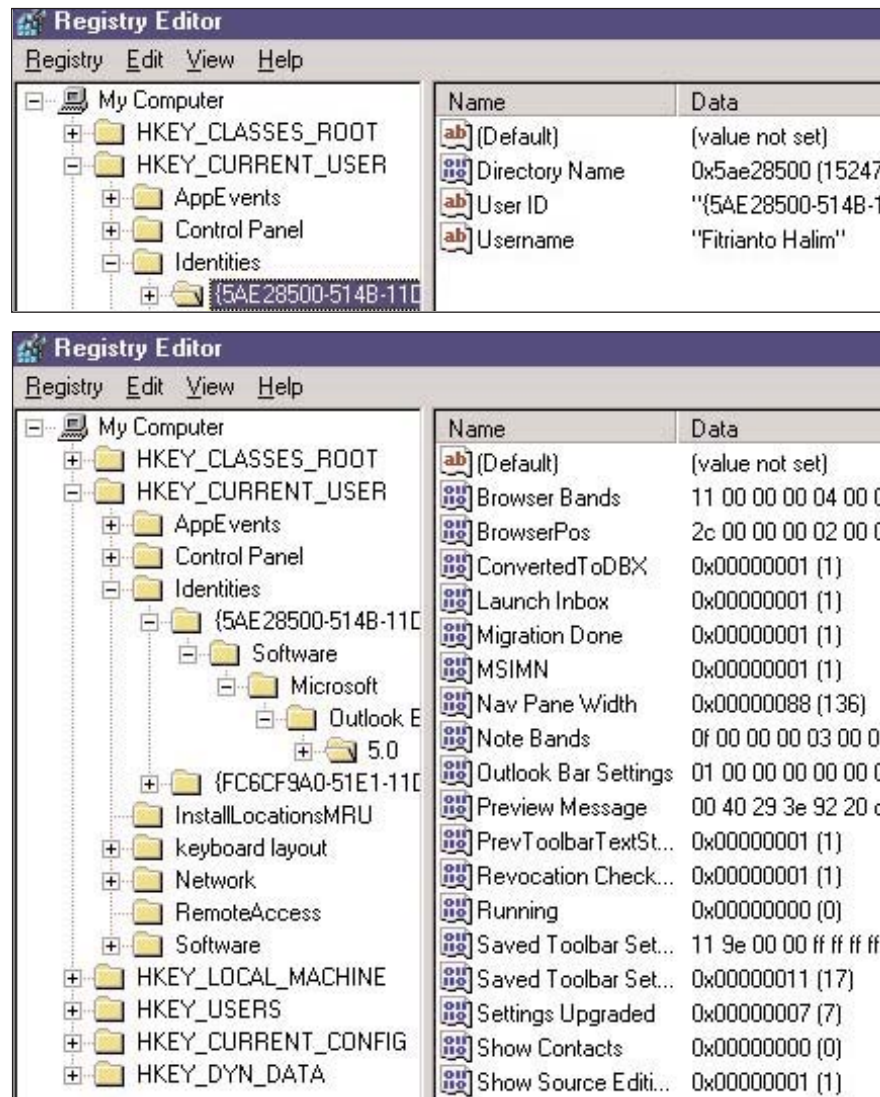
Untuk mengubahnya, kita menggunakan *registry editor* (regedit).

- 1 Pertama-tama, masuklah ke **HKEY_CURRENT_USER\Identities**. Pada *key Identities*, anda akan mendapatkan satu atau lebih *subkey* (tergantung pada banyaknya identitas yang ada) yang berisi ID. Dari *subkey* inilah, anda dapat melihat identitas yang sesuai.

- 2 Expand *subkey* tersebut hingga anda menuju **HKEY_CURRENT_USER\Identities ID Anda\Software\Microsoft\Outlook Express\5.0** (Di sini penulis menggunakan OE 5.0). Pada bagian kanan, cari name **Store Root** yang berisi letak penyimpanan folder-folder pada OE.

Ganti isinya sesuai kehendak anda, misal **C:\My Documents\My Mails**

Manfaat dari artikel ini akan terasa jika anda bekerja pada network, karena anda tidak perlu lagi meng-copy file-file DBX milik rekan anda.



Memanfaatkan "Move to Folder" dan "Copy to Folder"

Pada menu **Edit** kita akan menemukan pilihan **Move to Folder...** dan **Copy to Folder...**

Mungkin anda bertanya-tanya, apa kegunaannya. Maka jawabannya adalah bergantung pada kreativitas anda.

- 2 Sedangkan **Move to Folder...** dapat Anda manfaatkan untuk sinkronisasi email. Misalkan anda memiliki komputer dengan Outlook Express 5.x, tetapi tidak memiliki koneksi ke Internet.

Jika anda sudah memiliki *account* email jenis POP3 (atau yang mirip

- 1 Misalkan anda ingin membuat beberapa surat lamaran kerja dan dikirim lewat email, maka anda cukup membuat sebuah *draft* lalu manfaatkan **Copy to Folder...** untuk meng-copy *draft* tersebut.

Kini, anda hanya perlu mengedit sedikit email tersebut.

Animasi Slide pada Outlook Express

Jika anda senang mengutak-atik Java Script, mungkin anda pernah membuat animasi *slide*, artinya gambar bisa berpindah sendiri dalam rentang waktu tertentu.

Tapi, bagaimana jika kita ingin menampilkan animasi slide pada Outlook Express 5.x dan dapat disajikan secara *offline*?

Ternyata, cara membuatnya tidak sukar jika anda pernah mempelajari teknik penyatuan teks dan gambar yang ada pada OE—disebut *Stationery*.

Kuncinya adalah header content-type utama diisi dengan multipart/related dan tiap-tiap gambar memiliki header content-id yang unik. Isi dari header content-id inilah yang digunakan sebagai pengganti nama file gambar.

Apakah sudah cukup? Masih belum,

Utak-atik Header email Outlook Express

Umumnya, orang mengirim *anonymous mail* melalui telnet, itupun coba-coba.

Pada trik ini, kita akan mencoba mengutak-atik header email dengan cara yang gampang, dengan email yang dibuat dengan Outlook Express 5.x.

Secara garis besar, folder-folder yang ada pada OE akan dinyatakan sebagai sebuah file DBX. File ini berisi index dan isi. Nah, bagian isi adalah bagian yang terpenting, karena bagian ini yang akan dikirim ke SMTP server.

File kuncinya adalah Outbox.DBX. Untuk mengutak-atik header-nya anda

karena semua gambar harus ditampilkan. Sebab jika anda tidak melakukannya, maka gambar-gambar yang tidak ditampilkan akan dianggap sebagai *attachment*. Agar gambar-gambar tersebut tidak tampak, maka anda dapat mengatur atribut *height* dan *width* dari tag *img* ke 0.

Penulis sarankan untuk mencobanya dalam format EML (Microsoft Internet Mail Message). Sebagai tambahan, format EML sebenarnya berupa *plain text*, sehingga anda dapat mengeditnya dengan *text editor*.

Untuk menampilkannya, ada beberapa cara yang bisa digunakan.

Pertama, anda bisa menyimpan isi EML tersebut ke e-mail dalam format plain text (*default* dari isi header Content-Transfer-Encoding adalah 7 bit).

Kedua, Anda bisa menyisipkan file EML tersebut.

membutuhkan suatu editor yang mampu mengedit data *binary* (penulis sendiri menggunakan Norton Utilities).

Ada baiknya, anda memadatkan file Outbox.DBX terlebih dahulu dengan memilih menu **File → Folder → Compact** (Anda sedang berada di folder Outbox).

Header awal dari OE adalah From, sehingga jika editor yang anda pakai menyediakan fasilitas search, anda dapat mengisikannya dengan From: sebagai kata yang dicari.

Silahkan berkreasi... Sebagai contoh, penulis paling suka mengosongkan header Date (akan diisi oleh SMTP server) dan mengganti header X-Mailer.

POP3, yaitu *account* dari Hot Mail), maka email yang anda terima di warnet dapat anda baca pula di rumah.

Caranya, setelah selesai men-download email, "pindahkan" isi yang ada pada **Local Folders\Inbox (Hotmail\Inbox** untuk HotMail) ke folder yang tidak terpakai (misal, **Local Folders\Drafts**).

Setelah keluar dari OE, *copy* file **Drafts.DBX** ke disket.

Di rumah, *copy* file **Drafts.DBX** yang berasal dari disket ke *harddisk* anda. Setelah OE dijalankan, masuk ke **Local Folders\Drafts** lalu "pindahkan" isinya ke **Local Folders\Inbox**.

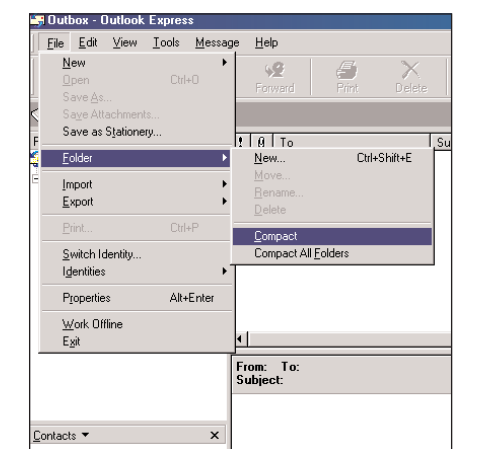
Kini anda dapat membaca e-mail yang anda download di Warnet dengan tenang di rumah.



Tentunya, kedua cara tadi masih memerlukan revisi header dari e-mail tersebut (lihat artikel terakhir).

Sebagai contoh, anda dapat melihat file "Happy Birthday.EML" yang disertakan.

Di sini anda dapat melihat sebuah foto album sederhana. Pada contoh ini, hanya sebuah format yang didukung, yaitu text/html.



Ada baiknya anda membuat *back-up* terlebih dahulu.

Mengenal JavaScript Perulangan

Pada bagian kelima dari tutorial JavaScript ini kami memperkenalkan **Perulangan**. Perulangan membuat penulisan program dengan JavaScript menjadi lebih efisien karena dengan fitur yang satu ini penulisan *listing* program kadang tidak perlu diulang sehingga bisa lebih efektif dan efisien.

Perulangan adalah pengeksekusian secara berulang terhadap kelompok statement sebanyak yang ditetapkan. Prinsip perulangan sering digunakan, karena dapat mengurangi panjang *listing* program, sehingga penulisan *scripting* lebih efektif dan efisien.

Contoh kasus yang dapat diselesaikan dengan perulangan banyak sekali, misalnya saja perhitungan nilai faktorial, nilai rataan sejumlah data, dan masih banyak lagi (lihat beberapa contoh kasus pada akhir pembahasan).

Dalam javascript, alur perulangan dapat dilakukan dengan menggunakan:

1. Statement for
2. Statement while
3. Statement do... while

Statement for

Digunakan untuk melakukan proses perulangan yang telah diketahui berapa kali jumlah perulangan yang akan dilakukan. Sintaksnya sebagai berikut:

Keterangan:

```
for(inisialisasi; kondisi; konter)
{
  ---statement javascript
  ---statement javascript
  ---statement javascript
}
```

a. Inisialisasi

Yaitu untuk memberi inisial terhadap variabel konter secara sederhana dapat dikatakan sebagai nilai awal dari variabel konter. Komponen ini merupakan kondisi awal dari proses dan hanya akan dieksekusi sekali saja pada awal proses.

b. Kondisi

Yaitu untuk menentukan batas akhir dari perulangan, di mana jika kondisi sudah tidak lagi terpenuhi, maka perulangan akan dihentikan, sebaliknya jika kondisi masih terpenuhi maka perulangan masih akan terus dilakukan.

c. Konter

Yaitu untuk menaikkan nilai variabel konter. Komponen ini menjadi penting, karena penaikan nilai variabel konter terkait dengan batas akhir dari proses perulangan. Jika variabel konter nilainya tetap maka secara otomatis batas akhir tidak akan pernah tercapai sehingga proses perulangan tidak akan pernah berhenti.

Contoh penggunaan:

```
<!-contoh 5.1 -->
<!-- simpan dalam format html -->
<html>
<head>
<title>Perulangan dengan statement for</title>
</head>
```

```
<body>
<script language="javascript">
<!--
var x
for(x=1;x<8;x++)
{
  document.write("<font face='arial' size='''+ x +'\">Javascript")
  document.write("</font><br>")
}
//-->
</script>
</body>
</html>
```

Contoh skrip yang menggunakan perulangan dengan for

Keterangan:

Pada contoh di atas, kita melakukan perulangan terhadap penulisan kata Javascript dengan urutan besar *font* naik. Coba jalankan di browser anda!

Catatan:

Jika dalam bagian komponen terdapat lebih dari satu *statement* maka masing-masing statement dipisahkan dengan tanda koma (,). Perhatikan contoh skrip berikut:

```
<!-- contoh 5.2 -->
<!-- simpan dalam format html -->
<html>
<head>
<title>Perulangan dengan statement for</title>
</head>
<body>
<script language="javascript">
<!--
var x,y
for(x=1,y=1,x<8;x++,y+=2)
{
  document.write("<font face='arial' size='''+ x +'\">"+ y)
  document.write("</font><br>")
}
//-->
</script>
</body>
</html>
```

Keterangan:

Pada contoh di atas, *output* akan berupa bilangan ganjil dengan penulisan yang semakin membesar. Coba di browser anda!

Statement while

Digunakan untuk perulangan yang hanya diketahui kondisi akhir dari perulangan tersebut tanpa diketahui berapa kali jumlah perulangan akan dilakukan. Sintaksnya sebagai berikut:

```
while(kondisi yang diuji)
{
  ---statement javascript
  ---statement javascript
  ---statement javascript
  variabel konter
}
```

Cara kerja:

Pertama kali *statement while* akan menguji kondisi dari ekspresi yang diberikan, jika kondisi terpenuhi maka statement-statement dalam blok akan dieksekusi. Kemudian nilai variabel konter akan dinaikkan pada bagian akhir blok.

Selanjutnya *statement while* akan memeriksa kembali kondisi, apakah masih terpenuhi? Jika ternyata masih terpenuhi maka statement-statement dalam blok akan kembali dieksekusi, sebaliknya jika sudah tidak terpenuhi maka perulangan akan dihentikan. Demikian proses ini terjadi berulang-ulang sampai kondisi yang disyaratkan tidak lagi terpenuhi.

Contoh:

Berikut (contoh 5.3) adalah contoh script yang menggunakan perulangan dengan statement while.

```
<!-- contoh 5.3 -->
<!-- simpan dalam format html -->
<html>
<head>
<title>Perulangan dengan statement while</title>
</head>
<body>
<script language="javascript">
<!--
var x
x=1
while(x<8)
{
  document.write("<font face='arial' size='''+ x +'\">Javascript")
  document.write("</font><br>")
  x++
}
//-->
</script>
</body>
</html>
```

Keterangan:

Contoh di atas akan memberikan hasil yang sama dengan contoh perulangan dengan menggunakan *statement for*. Bandingkan hasilnya dengan Contoh 5.1!

Statement do ... while

Pada dasarnya perulangan dengan *statement do ... while* sama saja dengan perulangan yang menggunakan *statement while*. Perbedaananya terletak pada letak dari kondisi yang diuji.

Pada *statement do ... while*, kondisi ditempatkan pada akhir perulangan, sedangkan pada *statement while* kondisi diletakkan pada awal perulangan.

Konsekuensinya, pada *statement do ... while*, akan terjadi minimal sekali proses eksekusi terhadap blok *statement*, meskipun kondisi awal tidak terpenuhi.

Sebaliknya pada *statement while* dimungkinkan tidak adanya eksekusi sama sekali terhadap blok statement, karena pemeriksaan dilakukan di awal.

Sintaksnya sebagai berikut:

```
do
{
  ---statement javascript
  ---statement javascript
  ---statement javascript
  variabel konter
}
while(kondisi yang di uji)
```

Contoh:

Berikut adalah Contoh 5.1 yang dimodifikasi dengan menggunakan *statement do ... while*.

```
<!-- contoh 5.4 -->
<!-- simpan dalam format html -->
<html>
<head>
<title>Perulangan dengan statement do ... while</title>
</head>
<body>
<script language="javascript">
<!--
var x
x=1
do
{
  document.write("<font face='arial' size='''+ x +'\">Javascript")
  document.write("</font><br>")
  x++
}
while(x<8)
//-->
</script>
</body>
</html>
```

Statement break

Statement break digunakan untuk menghentikan perulangan meskipun secara kondisional perulangan masih harus dilakukan. Perhatikan contoh berikut:

```
<!-- contoh 5.5 -->
<!-- simpan dalam format html -->
<html>
<head>
<title>Statement break</title>
</head>
<body>
<script language="javascript">
<!--
var x
x=1
while(x<8)
{
  if(x==4)
  {
    break
  }
  document.write("<font face='arial' size='''+ x +'\">Javascript")
  document.write("</font><br>")
  x++
}
while(x<8)
//-->
</script>
</body>
</html>
```

Keterangan:

Pada contoh di atas perulangan akan dihentikan pada saat nilai variabel x mencapai nilai 4. Artinya perulangan hanya akan dilakukan sebanyak tiga kali.

Statement continue

Statement continue digunakan untuk mengarahkan proses eksekusi kembali ke awal proses perulangan, tanpa mengeksekusi statement-statement di bawahnya.



Polling dengan ASP

Polling adalah fitur yang dapat ditambahkan pada halaman Web anda. Fitur ini banyak manfaatnya bagi anda sebagai pengelola situs. **David Sugianto** menyajikan cara membuat fasilitas *polling* atau jajak pendapat sendiri sehingga lebih sesuai dengan keperluan anda.

Dengan Format Data File .txt

APLIKASI *POLLING* SERING SEKALI KITA TEMUKAN pada halaman-halaman Web di Internet. *Polling* atau jajak pendapat berguna untuk mengumpulkan pendapat para pengunjung Web anda mengenai sesuatu hal. Misalnya, anda ingin mencari tahu perbandingan antara pengunjung situs anda yang berminat mempelajari HTML, PHP, dan ASP. Setiap kali seorang pengunjung memilih salah satu opsi, maka jumlah dari pilihan pada opsi tersebut akan bertambah. Dan dengan nilai tersebut, anda dapat melihat berapa persen atau suara yang berpartisipasi, atau opsi mana yang paling diminati pengunjung. Menarik bukan?

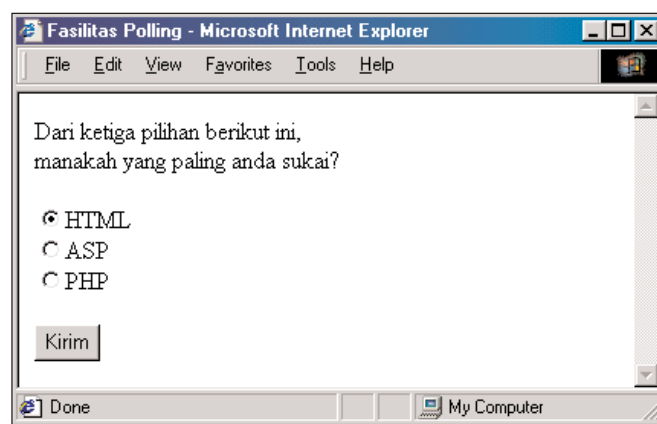
Jika selama ini anda mendapatkan fasilitas polling dari situs portal yang menyediakan, anda sebenarnya dapat membuatnya sendiri sesuai dengan keinginan dan keperluan anda. Dalam membuat artikel ini, saya berasumsi bahwa anda telah menguasai atau memahami HTML walaupun yang mendasar. Oleh karena itu, kode yang tidak memerlukan skrip ASP, tidak saya bahas mengingat ruang dan tempat. Dan untuk dasar ASP anda dapat membacanya di majalah NeoTek edisi Mei 2002.

Marilah kita memulai pembuatan polling-nya. Pertama-tama yang harus kita buat terlebih dahulu adalah tampilan polling tersebut. Untuk itu, kita akan membuat file pertama dengan nama form.asp. Sebenarnya, jika anda ingin menggunakan nama file form.htm juga bisa, namun untuk menyeragamkan, maka saya menggunakan nama form.asp. Ketikkan skrip pada kotak di kolom sebelah ini ke dalam teks editor kesayangan anda.

Kode-kode yang diberikan murni merupakan HTML statis. Dalam kode tersebut kita membuat form dengan menggunakan tag <form> yang diikuti oleh radio button dengan tag <input type="radio"> dengan nama "polling" dan *value* masing-masing yang berbeda satu dengan yang lain.

```
<html>
<head>    <title>Fasilitas Polling</title>
</head>
<body>
<form method="POST" action="terima.asp">
  <p>Dari ketiga pilihan berikut ini, <br>
    manakah yang paling anda sukai?</p>
  <p><input type="radio" value="html" checked
    name="polling">HTML<br>
    <input type="radio" name="polling" value="asp">ASP<br>
    <input type="radio" name="polling" value="php">PHP</p>
  <p><input type="submit" value="Kirim" name="Kirim"></p>
</form>
</body>
</html>
```

Jika anda buka di browser, akan tampil gambar berikut:



Setelah tampilan form selesai kita buat, kini kita memerlukan sebuah file khusus yang berfungsi untuk menyimpan data-data. Untuk itu, buka teks editor kesayangan anda, ketikkan:

```
0
0
0
```

Simpanlah dengan nama **data.txt**.

Kini saatnya kita membuat halaman Web yang bertugas menerima masukan dari pengunjung dan menyimpannya ke file data.txt. Kodenya akan terlihat sebagai berikut:

```
<html><head>
  <title>Fasilitas Polling</title>
</head><body>
<H2>Terima Kasih Atas Partisipasi Anda</H2><HR><p>
<center> Hasil Sementara Hingga Tanggal <%=date()%> </center><p>
<%
  Dim objBuka, objFSO, Path, nilai(3), pilihan
  pilihan = Request.Form("polling")
  Path = Server.MapPath("data.txt")
  Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
  set objBuka = objFSO.OpenTextFile(Path, 1)

  varA = 0
  Do While varA < 3
    nilai(varA) = objBuka.ReadLine
    varA = varA + 1
  Loop

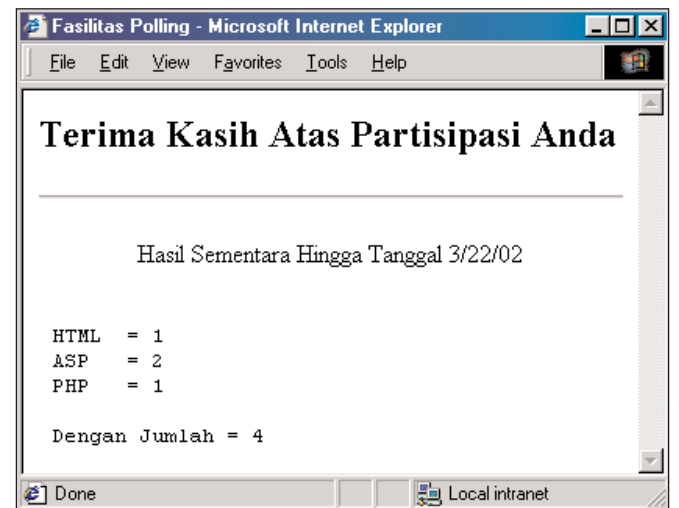
  %>
  <%
    Select Case pilihan
      Case "html"
        nilai(0) = nilai(0) + 1
      Case "asp"
        nilai(1) = nilai(1) + 1
      Case "php"
        nilai(2) = nilai(2) + 1
    End Select
    Jumlah = nilai(0) + nilai(1) + nilai(2)
  %><pre>
    HTML = <%=nilai(0)%>
    ASP  = <%=nilai(1)%>
    PHP  = <%=nilai(2)%>

    Dengan Jumlah = <%=jumlah%>
  </pre>
  <%
    Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
    set objBuka = objFSO.OpenTextFile(Path, 2)
    varA = 0
    Do While varA < 3
      objBuka.WriteLine nilai(varA)
      varA = varA + 1
    Loop
  %>
  </body></html>
```

Hasilnya akan seperti pada gambar di kolom sebelah atas.

Penjelasan file terima.asp:

```
<H2>Terima Kasih Atas Partisipasi Anda</H2><HR><p>
<center> Hasil Sementara Hingga Tanggal <%=date()%>
</center><p>
```



Skrip di atas berfungsi untuk menampilkan ucapan terima kasih serta menampilkan tanggal hari ini yang didapat dari fungsi <%=date()%>.

Dim objBuka, objFSO, Path, nilai(3), pilihan
Semua variabel yang akan digunakan di aplikasi polling ini dideklarasikan

pilihan = Request.Form("polling")
Value hasil kiriman yang radio button yang dipilih disimpan di dalam variabel pilihan

Path = Server.MapPath("data.txt")
Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
set objBuka = objFSO.OpenTextFile(Path, 1)
Kita menggunakan tiga variabel, yaitu Path untuk menyimpan lokasi file data.txt, objFSO yang merupakan *unsure* yang harus diikutsertakan, dan yang terakhir objBuka untuk membuka file data.txt dan men-setnya menjadi mode "1", yaitu mode membaca.

```
varA = 0
Do While varA < 3
  nilai(varA) = objBuka.ReadLine
  varA = varA + 1
Loop
```

Ini merupakan struktur kontrol perulangan ASP yang kita gunakan untuk mengisi variabel nilai yang bersifat "array." Karena kita hanya menggunakan tiga macam pilihan, yaitu "html," "asp," dan "php," maka perulangan pun cukup sebanyak tiga kali. Dan dalam perulangan ini, terdapat "objBuka.ReadLine" untuk membaca file per baris dan disimpan ke dalam variabel nilai (indeksnya mengikuti varA).

```
Select Case pilihan
  Case "html"
    nilai(0) = nilai(0) + 1
  Case "asp"
    nilai(1) = nilai(1) + 1
  Case "php"
    nilai(2) = nilai(2) + 1
End Select
```

Jika di atas kita menggunakan struktur kontrol perulangan, kini kita menggunakan struktur kontrol perbandingan dengan variabel *pilihan* yang menjadi fokusnya. Ingat *pilihan* didapat dari "pilihan=Request.Form("polling")"

```
Jumlah = nilai(0) + nilai(1) + nilai(2)
```

Tentunya kita ingin untuk menampilkan jumlah suara yang telah ikut berpartisipasi di polling kita. Untuk itu, kita menggunakan variabel *jumlah* untuk menyimpan

jumlah dari variable nilai dari semua indeks.

```
<pre>
HTML = <%=nilai(0)%>
ASP  = <%=nilai(1)%>
PHP  = <%=nilai(2)%>
```

Dengan Jumlah = <%=jumlah%>

```
</pre>
```

Merupakan perintah/tag HTML biasa yang digabung dengan kode ASP untuk menampilkan status pilihan dan jumlah seluruh suara.

Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
set objBuka = objFSO.OpenTextFile(Path, 2)
Jika waktu pertama kali kita membuka file data.txt dengan mode membaca ("1"), maka kini kita membuka file tersebut kembali namun dengan mode menulis ("2"). Karena kita akan mengupdate file penyimpanan data kita.

```
varA = 0
Do While varA < 3
    objBuka.WriteLine nilai(varA)
    varA = varA + 1
```

Loop

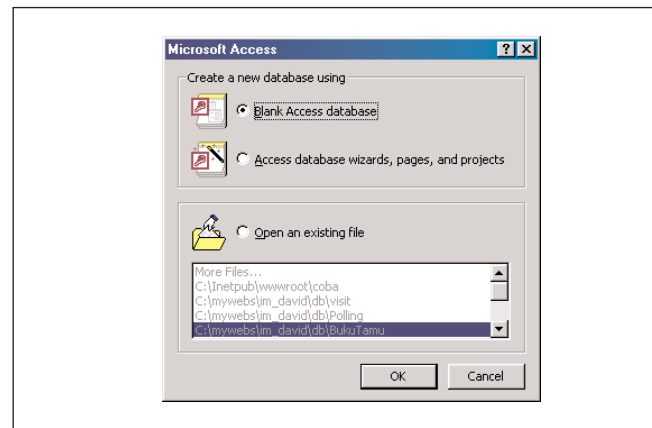
Langkah terakhir yang harus dilakukan adalah menuliskan isi dari variabel nilai yang telah kita lakukan pertambahan data/nilai. Dengan menggunakan perulangan dan "objBuka.WriteLine" untuk menuliskan di file data kita per baris.

Kini anda telah selesai dalam membuat fasilitas Polling yang dapat anda masukkan ke dalam halaman Web anda. Semua nama variabel yang digunakan di atas, tidaklah mutlak. Maksudnya jika anda berniat untuk mengganti nama variabel-variabel di atas, silakan saja. Namun harap hati-hati dalam mengganti namanya. Karena jika satu variabel diganti, maka semua variabel yang namanya sama juga harus diganti.

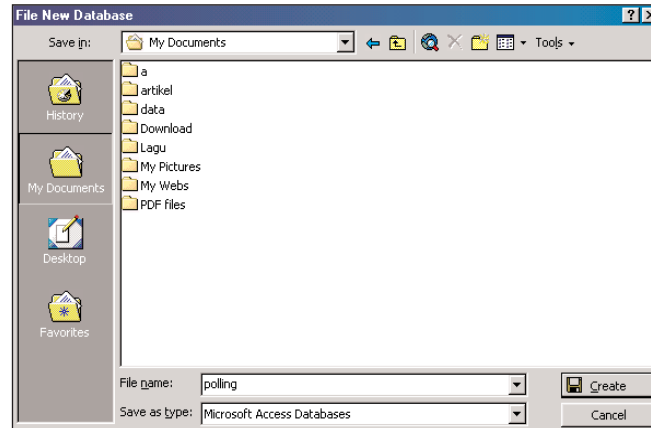
Dengan Format Data Access

Polling merupakan suatu fasilitas yang biasanya disediakan oleh para webmaster dari suatu situs untuk mengetahui pendapat dari para pengunjung situs atas suatu hal. Jika pada artikel sebelumnya, kita telah membuat fasilitas polling dengan menggunakan

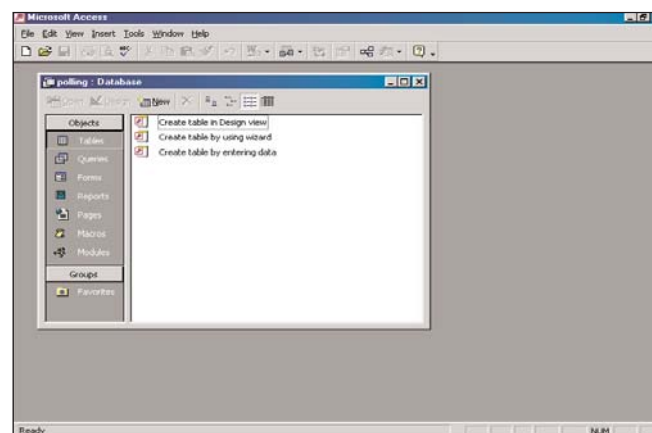
file yang berbentuk *.txt sebagai bentuk penyimpanan data, kini kita akan membuat fasilitas polling dengan menggunakan basisdata dari Microsoft Access untuk menyimpan data. Untuk itu, kita memerlukan file database dari MS Access dengan cara pembuatannya



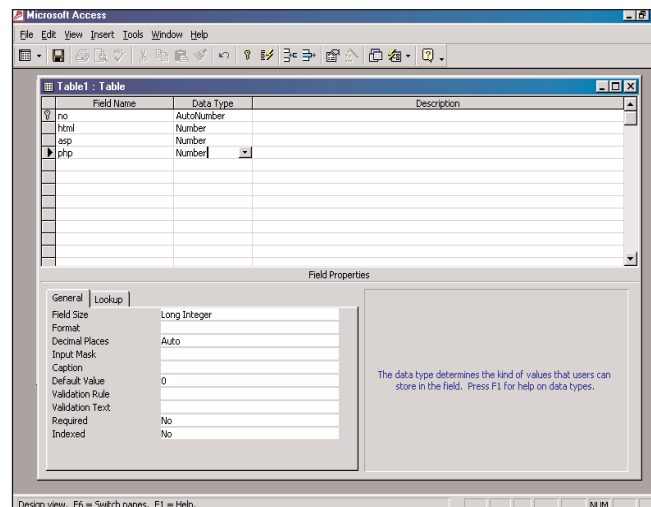
1 Buka Ms.Access anda, lalu pada File > New, pilih "Blank Access database."



2 Simpanlah dengan nama "Polling," lalu klik "Create."



3 Double klik "Create Table in Design View"



Pada window Design View, isilah field-field yang akan kita gunakan.

Field Name	Data Type
no	AutoNumber
html	Number
asp	Number
php	Number

Simpan table tersebut dengan nama **tbldata**.

Setelah kita selesai dengan pembuatan database-nya, kini kita akan mulai membuat halaman-halaman web yang kita perlukan. Halaman yang kita akan buat terlebih dahulu ialah halaman formnya yang juga akan menampilkan jumlah suara telah yang masuk ke database kita

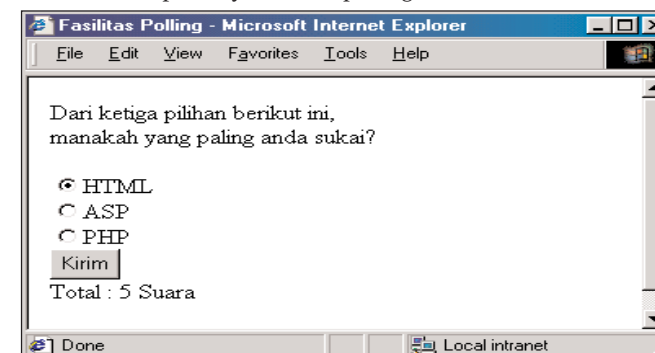
Ketikkan kode berikut ini ke dalam teks editor anda.

```
<html><head>
<title>Fasilitas Polling</title>
</head>
<body>
  <!--#Include File=adovbs.inc-->
  <table border="0" width="100%">
    <tr>
      <td>Dari ketiga pilihan berikut ini, <br>
        manakah yang paling anda sukai?<br>
      <form method="POST" action="voting.asp">
        <input type="radio" value="html" checked name="polling">HTML<br>
        <input type="radio" name="polling" value="asp">ASP<br>
        <input type="radio" name="polling" value="php">PHP<br>
        <input type="submit" value="Kirim"><br>
        Total:
      </form>
    </td>
  </tr>
</table>

<%
filePath = Server.MapPath("Polling.mdb")
strSQL = "SELECT * FROM data"
Set objConn = Server.CreateObject("ADODB.Connection")
objConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
  filePath
Set objRset = Server.CreateObject("ADODB.Recordset")
objRset.Open strSQL, objConn, adOpenStatic
Response.Write(objRset.RecordCount & " Suara")
ObjRset.Close
Set ObjRset = Nothing
objConn.Close
Set objConn = Nothing
%>

</font></form></td></tr></table>
</body></html>
```

Simpanlah dengan nama **form.asp**. dan jika anda buka dari browser, tampilannya akan seperti gambar di bawah ini:



Penjelasan singkat mengenai script ASP tersebut:

<!--#Include File=adovbs.inc-->
Jika kita berhubungan dengan basisdata, maka file adovbs.inc harus diikutsertakan. Karena file ini berisi konstanta yang diperlukan oleh metode ADO. File ini dapat anda temukan di C:\program Files\Common Files\System\ADO

Path = Server.MapPath("Polling.mdb")

Pada *statement* ini, kita menentukan lokasi dari basisdata Access yang telah kita buat dan disimpan ke dalam variabel Path.

strSQL = "SELECT * FROM data"

Select merupakan perintah dari SQL yang berfungsi membaca baris per baris. Kerena kita menggunakan karakter *, maka dianggap kita membaca seluruh baris yang ada di tabel data

Set objConn = Server.CreateObject("ADODB.Connection")
objConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & filePath
Set objRset = Server.CreateObject("ADODB.Recordset")
objRset.Open strSQL, objConn, adOpenStatic
Kini kita harus membuka koneksi ke basisdata agar isi dari basisdata dapat kita manipulasi baik membaca, menambah, meng-*update*, dan sebagainya.

Response.Write objRset.RecordCount & " Suara"

Jika anda mengikuti artikel tentang ASP dari pertama, maka anda pasti mengetahui bahwa fungsi Response.Write digunakan untuk menampilkan ke layar monitor. Sedangkan objRset.RecordCount & "Suara" untuk menghitung jumlah *record* yang tersimpan dalam basisdata kita, yang diikuti dengan kata "Suara"

ObjRset.Close

Set ObjRset = Nothing

objConn.Close

Set objConn=Nothing

Blok skrip di atas berfungsi untuk menutup basisdata yang telah kita buka.

Kini saatnya kita membuat halaman yang terakhir, yaitu halaman yang mengucapkan terima kasih kepada pengunjung dan bertugas untuk memasukkan data ke dalam basisdata kita. Ketikkan kode berikut ini di dalam teks editor kesayangan anda.

```
<html><head>
<title>Fasilitas Polling</title>
</head>
<body><center>
  <H2>Terima Kasih Atas Partisipasi Anda</H2><HR>
  <H2>Hasil Sementara Hingga Tanggal <%=date()%></h2>
</center>
  <!--#Include File=adovbs.inc-->
  <%dim objConn, objRset, array(3)
  dim Path, total, field(3), persen(3)
  array(0) = "html"
  array(1) = "asp"
  array(2) = "php"
  pilihan = Request.Form("polling")
  Path=Server.MapPath("Polling.mdb")
  Set objConn = Server.CreateObject("ADODB.Connection")
  objConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" +
    Path
  set objRset = Server.CreateObject("ADODB.Recordset")
  objRset.Open "data", objConn, adOpenStatic, adLockOptimistic, adCmdTable
  objRset.AddNew
  Select Case pilihan
```

```

Case "html"
  objRset("html")=1
Case "asp"
  objRset("asp")=1
Case "php"
  objRset("php")=1
End Select
objRset.Update
total = objRset.RecordCount
objRset.MoveFirst

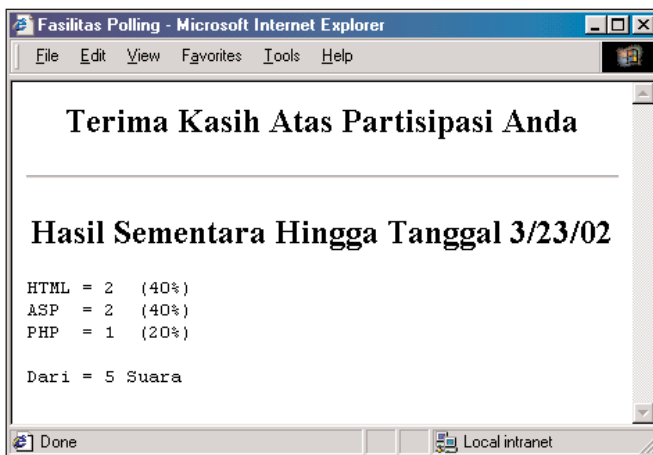
For a=1 to total
  For b=1 to 3
    field(b)=field(b)+objRset(b)
  Next
  objRset.MoveNext
Next

For a=1 to 3
  persen(a) = (field(a)/total)*100
Next
t%>
<pre>
HTML = <%=field(1)%> (<%=int(persen(1))%>%%)
ASP  = <%=field(2)%> (<%=int(persen(2))%>%%)
PHP  = <%=field(3)%> (<%=int(persen(3))%>%%)
Dari = <%=total%> Suara
</pre></body></html>

```

Simpanlah dengan nama **voting.asp**.

Dan hasilnya di browser akan seperti berikut



Penjelasan singkat mengenai kode ASP di atas:

```

array(0) = "html"
array(1) = "asp"
array(2) = "php"

```

Kita menggunakan variabel array yang terdapat tiga indeks, dan mengisi masing-masing indeks dengan "html," "asp," "php"

```

pilihan = Request.Form("polling")

```

Untuk menerima value dari form yang dikirimkan dan disimpan di variabel pilihan

```

objRset.AddNew
Select Case pilihan
Case "html"
  objRset("html")=1
Case "asp"

```

```

  objRset("asp")=1
Case "php"
  objRset("php")=1
End Select

```

Skrip ini untuk memasukkan data ke dalam basisdata dengan melakukan perbandingan terlebih dahulu terhadap variabel pilihan.

```

For a=1 to total
  For b=1 to 3
    field(b)=field(b)+objRset(b)
  Next
  objRset.MoveNext
Next

```

For merupakan struktur kontrol perulangan dalam ASP, yang kali ini kita gunakan untuk mengisi field-field yang kita punya dengan jumlah dari data yang ada dalam field tersebut. Field(1) mewakili html, field(2) mewakili asp, dan field(3) mewakili php

```

For a=1 to 3
  persen(a) = (field(a)/total)*100
Next

```

Jika tadi kita mengisi jumlah masing-masing field, kini kita akan menghitung persentase dari field-field yang ada.

```

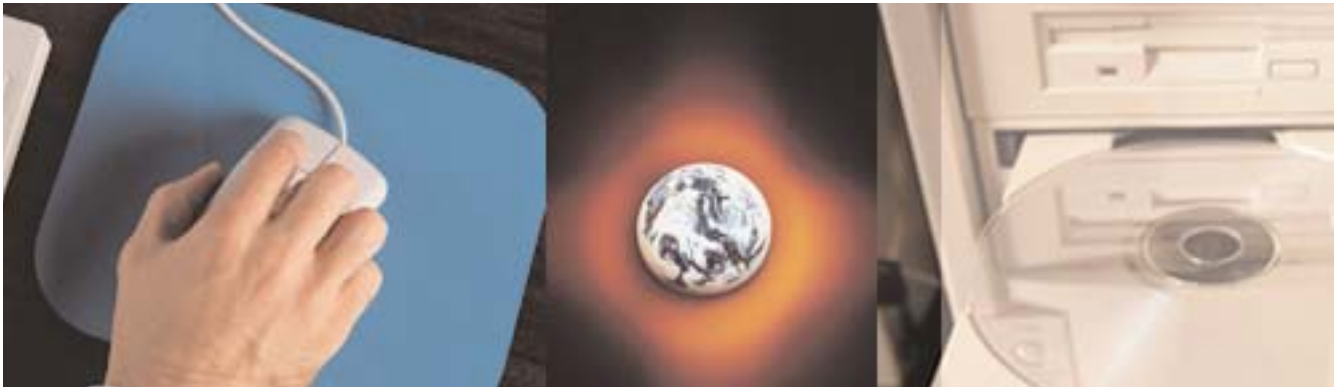
<pre>
HTML = <%=field(1)%> (<%=int(persen(1))%>%%)
ASP  = <%=field(2)%> (<%=int(persen(2))%>%%)
PHP  = <%=field(3)%> (<%=int(persen(3))%>%%)
Dari = <%=total%> Suara
</pre>

```

Dan terakhir kita menampilkan data masing-masing field beserta keterangan, persentase, dan jumlah seluruh suara yang ada di basisdata kita.

Kini anda telah membuat fasilitas *polling* sendiri dengan memanfaatkan Microsoft Access sebagai media penyimpanan data. Setiap metode, baik penyimpanan melalui teks maupun basisdata memiliki kekurangan dan kelebihan masing-masing. Adalah yang menentukan sendiri apakah lebih baik menggunakan teks atau basisdata. Halaman Web yang telah kita buat di atas, dapat anda ubah sesuai dengan kebutuhan anda. Selama tidak mengganggu skrip ASP-nya.

Jika ada pertanyaan seputar tutorial ini anda dapat mengirim email ke david_sugianto2002@yahoo.com



Hacking dengan Menggunakan BO & Deep BO

Walaupun sudah banyak dikenal orang dan juga dikenali oleh berbagai anti-virus, trojan Back Orifice tetap menarik untuk dipelajari. **Eryanto Sitorus** membahas **Back Orifice** dan **Deep Back Orifice** untuk melengkapi bahasan serupa mengenai NetBus yang telah dimuat di NeoTek Agustus 2002.

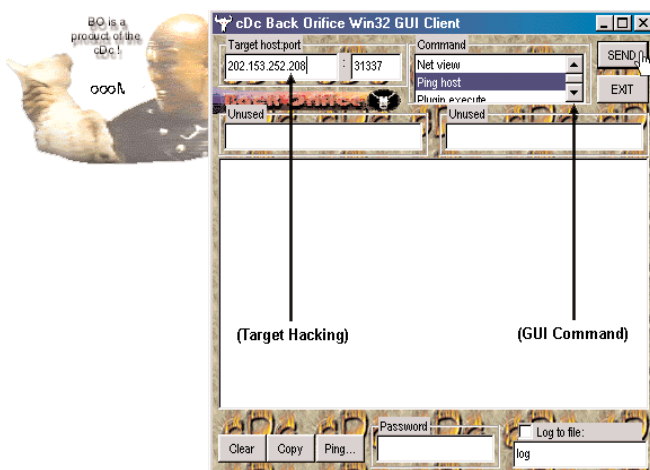
JIKA PADA EDISI SEBELUMNYA KAMI telah memperkenalkan pada anda salah satu perangkat lunak bertajuk Remote Administration System yang sangat "vulgar" dan bersifat user friendly, yaitu NetBus, rasanya kurang *sreg* jika kami tidak menyertakan aplikasi sejenis sebagai pelengkapannya. Hal ini kami lakukan karena kami menyadari bahwa tidak semua software mampu *handle* semua yang kita inginkan, secanggih apa pun suatu *software*, pasti memiliki kelemahan dan kekurangan. Nah, agar "perangkat hacking" anda makin lengkap, anda perlu mencoba dua buah perangkat hacking yang akan kami bahas dalam artikel ini, yakni **Back Orifice** dan **Deep Back Orifice**.

Back Orifice dan Deep Back Orifice adalah dua buah aplikasi berbasis *client/server* yang dapat dijalankan pada sistem operasi UNIX dan Microsoft Windows 95/97/98/ME/2000/XP, atau NT. Jika sebelumnya dikatakan bahwa NetBus beroperasi pada *port* 12345 dan *port* 20034, maka

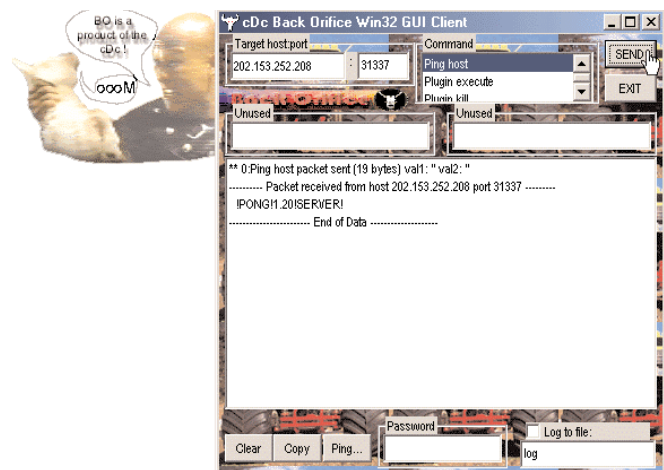
Back Orifice dan Deep Back Orifice beroperasi pada *port* 31337, inilah salah satu alasan yang membuat kami merasa perlu untuk memperkenalkannya pada anda. Tentunya semakin banyak alternatif nomor *port* yang bisa disusupi, maka akan semakin besar pula kemungkinan anda berhasil melakukan hacking.

Sama seperti program Remote Administration System lainnya, kedua buah aplikasi ini (Back Orifice dan Deep Back Orifice) juga dilengkapi dengan sebuah program yang berfungsi untuk menjembatani *client* agar dapat masuk dan mengakses semua sumber daya pada komputer lain, yang dalam hal ini disebut sebagai "server," yaitu BOSERVE.EXE. Jika program tersebut sedang aktif di komputer orang lain, maka dapat dipastikan bahwa anda akan leluasa mengakses semua isi *hard disk* komputer orang lain tanpa mengalami kesulitan sedikit pun.

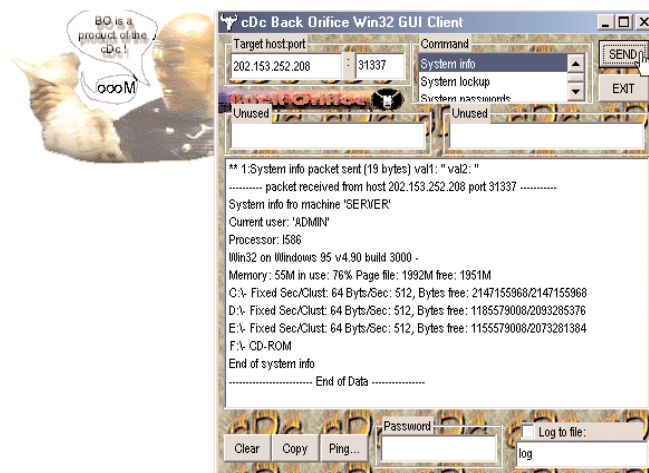
Dan satu hal lagi yang perlu anda ketahui dari kedua aplikasi tersebut, jika BOSERVE.EXE sudah aktif di PC



• Gambar 1: Menentukan target yang akan di-hack.



• Gambar 2: Memeriksa IP/host yang akan di-hack.



• Gambar 3: Melihat spesifikasi komputer.

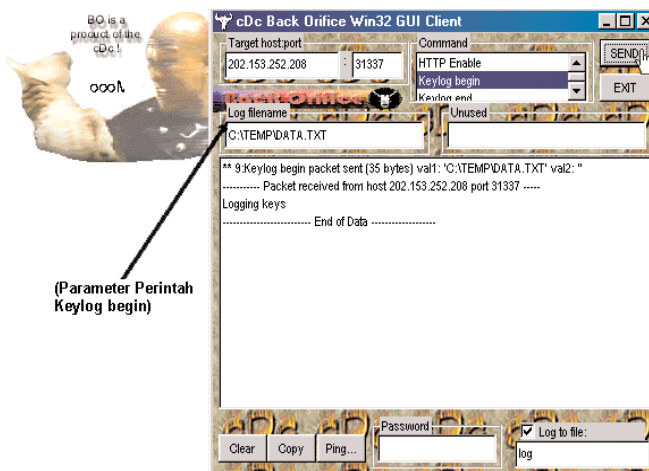
seseorang, maka sangat kecil kemungkinan program tersebut dihapus, dinonaktifkan, atau dideteksi oleh anti virus, penyebabnya karena memang BOSERVE.EXE sudah tidak dapat lagi ditemukan dalam *hard disk*. Pada saat program tersebut aktif, maka secara otomatis dia langsung berubah menjadi sesuatu yang misterius dan tidak berwujud. Berbeda dengan PATCH.EXE milik NetBus yang bisa dilihat atau dideteksi oleh anti virus, dan jika pemilik PC yang anda hacking berhasil menemukannya dalam direktori C:\WINDOWS dan menghapusnya, maka saat itu juga anda akan kehilangan akses. (Inilah salah satu kelemahan NetBus).

Sebelum kita mulai membahas bagaimana cara mengoperasikan kedua aplikasi itu, sebaiknya anda men-download-nya lebih dahulu dari alamat berikut ini:

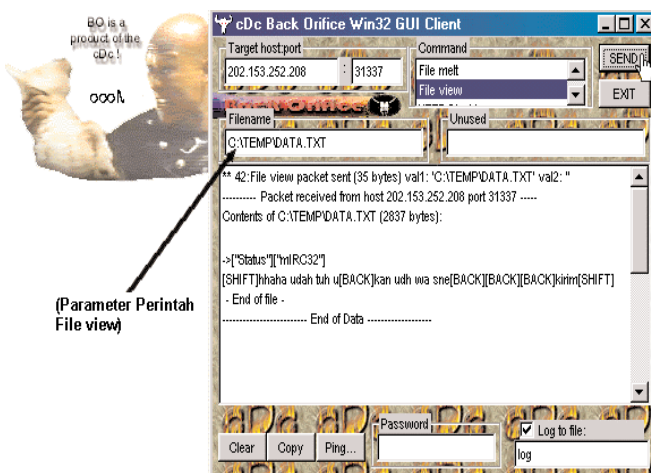
- www.cultdeadcow.com
- www16.brinkster.com/erytricksy/Software/bo120.zip
- www16.brinkster.com/erytricksy/Software/deep_bo.zip

Memulai Hacking dengan Back Orifice

1. Masuklah ke dalam folder di mana anda meletakkan aplikasi Back Orifice, lalu klik BOGUI.EXE.
2. Kemudian masukkan IP atau host orang yang akan anda remote ke dalam field **Target host:port**.
3. Untuk memastikan apakah IP atau host tersebut bisa anda remote, maka anda harus memeriksanya terlebih dahulu. Caranya, pilih **Ping host** pada *form Scrolling Text*



• Gambar 4: Membuat parameter untuk perintah keylog begin.



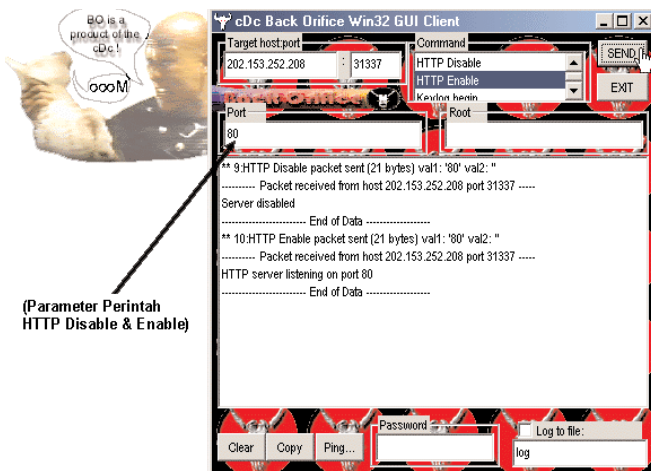
• Gambar 5: Membaca file log menggunakan perintah File View.

Box, lalu klik tombol **SEND**. Kemudian perhatikan pesan yang muncul setelah itu, jika anda hanya memperoleh pesan seperti yang terlihat di bawah ini:

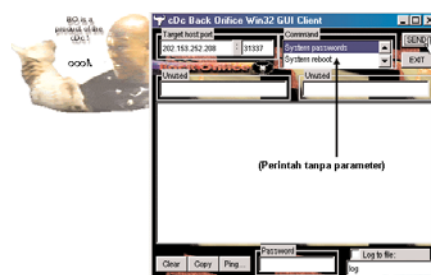
**** 0:Ping host packet sent (19 bytes) val1: " val2: "**

Artinya aplikasi Back Orifice anda gagal mendeteksi program BOSERVE.EXE pada IP atau host tersebut. Namun jika Back Orifice anda melaporkan hasil seperti yang terlihat pada Gambar 2, saya ucapkan selamat! Itu artinya anda telah berhasil menemukan IP atau host yang bisa anda *remote*. Selanjutnya terserah anda. Pada form Scrolling Text Box, selain Ping host, tersedia 51 perintah *hack-ing* untuk anda gunakan. Sebagai contoh, anda ingin agar PC yang anda *hack* tidak bisa mengakses situs Web, maka anda tinggal memilih perintah **HTTP Disable**, lalu klik tombol **SEND**. Untuk mengaktifkannya kembali, pilih perintah **HTTP Enable**, lalu klik tombol **SEND**. Jika anda ingin mengetahui informasi spesifikasi PC yang anda hack, pilih perintah **System info**, lalu klik tombol SEND, bentuk laporannya akan tampak seperti pada Gambar 3.

Namun anda juga harus teliti, karena tidak semua perintah Back Orifice bersifat toggle (disable/enable), beberapa perintah lain membutuhkan parameter agar bisa bekerja. Tetapi sebagai petunjuk bagi anda untuk mengetahui kapan saatnya sebuah perintah bersifat *toggle* atau yang memerlukan parameter, maka anda cukup melihat pesan tampilan yang berada tepat di bawah **field Target host:port**. Sebagai contoh, misalnya anda ingin menggunakan perintah **Key-log begin**, yaitu perintah yang berfungsi untuk mengintip



• Gambar 6: Menutup dan membuka port HTTP (home page).

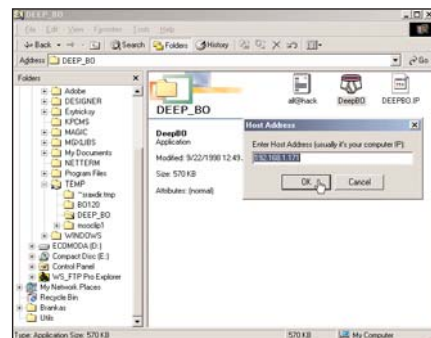


• Gambar 7: Perintah-perintah Back Orifice tanpa parameter.

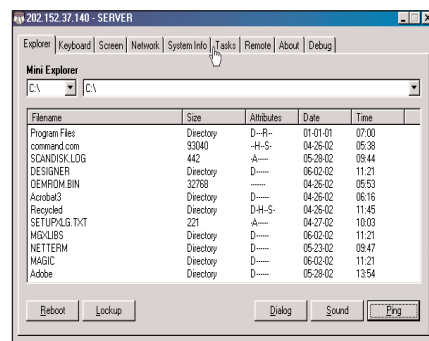
(*listening*) teks yang diketik oleh orang yang anda *hack*. Agar perintah tersebut bisa anda gunakan, maka anda harus mengetikkan sebuah nama file sebagai parameter untuk perintah tersebut ke dalam **field Log filename**, kemudian klik tombol **SEND**. Dan jika anda ingin melihat isi dari file tersebut, pilihlah perintah **File view**, lalu klik tombol SEND, namun sebelumnya pastikan bahwa anda sudah memasukkan nama file yang akan anda baca sebagai parameter untuk perintah tersebut ke dalam **field Filename**.

Cara yang sama juga berlaku untuk perintah **MM Capture screen** atau yang lainnya, anda harus menentukan nama file beserta ekstensi sebagai parameter terhadap apa yang akan anda capture, ekstensi untuk file tersebut misalnya GIF, JPG, BMP, atau yang lainnya. Setelah proses *capture* selesai dan anda ingin melihat hasilnya, carilah file tersebut dalam direktori C:\TEMP, atau C:\WINDOWS\TEMP di hard disk PC anda. Jika anda kesulitan menemukan file tersebut, manfaatkan fasilitas Find → Files or Folders dari menu Start. Demikian seterusnya, dan untuk mengetahui fungsi-fungsi perintah yang lain selain perintah yang sudah saya jelaskan, silakan anda mencobanya sendiri. Saya yakin itu akan jauh lebih bermanfaat daripada anda berlama-lama membaca artikel ini.

Memulai Hacking dengan Deep Back Orifice



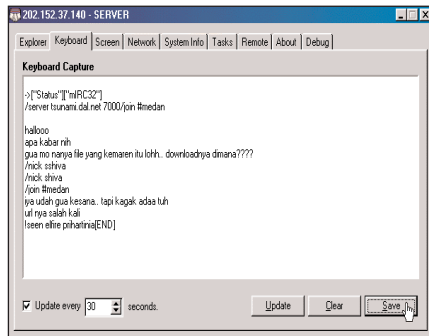
• Gambar 8: Tahap awal menjalankan aplikasi Deep Back Orifice.



• Gambar 9: Informasi yang menyiratkan bahwa proses hacking berhasil.

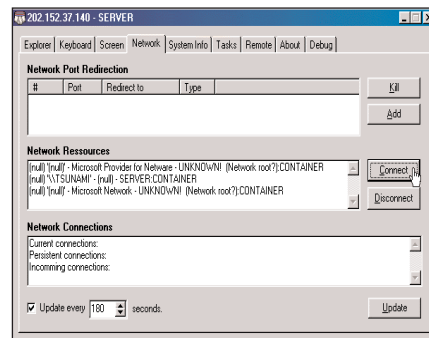
Berikut adalah petunjuk untuk mengoperasikan aplikasi Deep Back Orifice:

1. Masuklah ke dalam folder tempat di mana anda menyimpan program aplikasi Deep Back Orifice, lalu klik file DeepBO.exe. Sesaat kemudian akan muncul pesan seperti yang tampak pada Gambar 8. Jika IP yang muncul di komputer anda tidak sama seperti yang terlihat pada di bawah ini, abaikan saja, karena itu bukan merupakan suatu masalah, lalu lanjutkan dengan mengklik tombol OK.

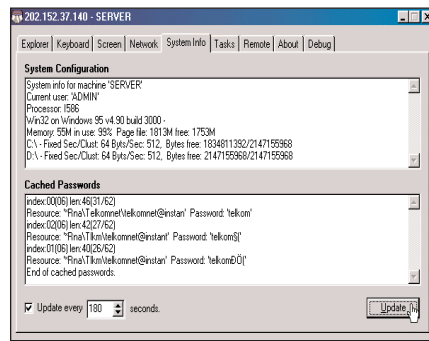


• Gambar 10: Contoh tampilan teks yang berhasil di-listen.

2. Masukkan IP atau host orang yang akan anda remote ke dalam field Quick Connect to IP, lalu klik tombol Connect. Dan sebagai petunjuk apakah IP atau host yang anda masukkan tadi dapat di-remote, periksalah jendela tab Explorer. Jika jendela tersebut benar-benar kosong, maka itu berarti aplikasi Deep Back Orifice gagal menemukan program



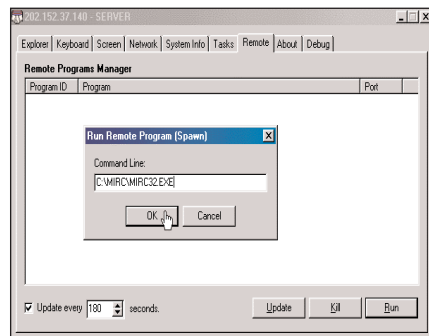
• Gambar 11: Contoh tampilan informasi network yang berhasil dideteksi.



• Gambar 12: Contoh informasi spesifikasi PC dan password yang berhasil di-cache.

BOSERVE.EXE. Tapi jika pada jendela tab Explorer aplikasi Deep Back Orifice anda terlihat informasi seperti pada Gambar 9, maka sekali lagi saya ucapkan selamat karena anda berhasil menemukan IP atau host yang bisa anda remote (hack).

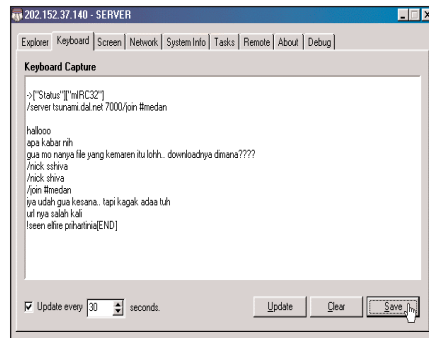
3. Untuk melanjutkan proses hacking, kliklah satu per satu tab (fitur) sebagaimana yang terlihat pada Gambar 9, misalnya tab Keyboard untuk me-listen teks yang diketik pada PC yang anda remote, tab Screen untuk meng-capture



• Gambar 13: Menjalankan program menggunakan fungsi remote.

layar, tab Network untuk melihat informasi jaringan, tab System Info untuk melihat informasi spesifikasi PC termasuk untuk mendapatkan password yang terdapat pada PC tersebut, tab Task untuk melihat informasi program yang sedang aktif, tab Remote, dan sebagainya.

ery@postmater.co.uk

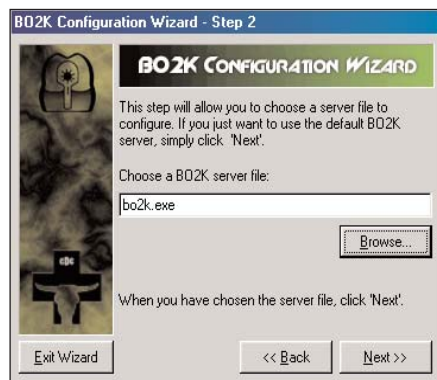


• Gambar 14: Contoh informasi program-program yang sedang aktif.

BACK ORIFICE 2000 MENGKONFIGURASI BO2K SERVER

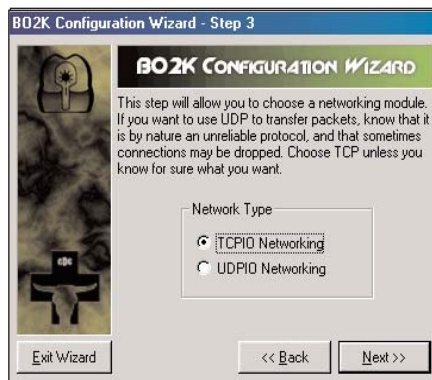
Keberhasilan Back Orifice memotivasi anggota Cult of the Dead Cow lain untuk menyempurnakannya menjadi Back Orifice 2000 (BO2K). Kelebihan BO2K adalah sifatnya yang dapat dikonfigurasi sepenuhnya. **Diovan** membahasnya untuk anda.

Konfigurasi BO2K server yang akan dikirim ke komputer sasaran.



1 INSTALASION WIZARD BO2K

Selesai instalasi dan memilih launch software, maka anda akan mendapatkan layar BO2K Configuration Wizard yang disebut Step 1 (atau setelah menjalankan file bo2kcfg.exe). Klik Next untuk masuk ke Step 2 di atas. Anda diminta memilih BO server file. Biarkan bo2k.exe



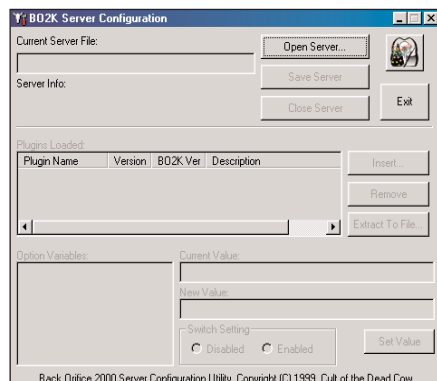
2 TCP ATAU UDP?

Anda dapat memilih networking module TCP atau UDP. Bila tidak yakin apa yang mesti dipilih, biarkan TCP sebab UDP sifatnya kurang bisa diandalkan dibandingkan TCP.



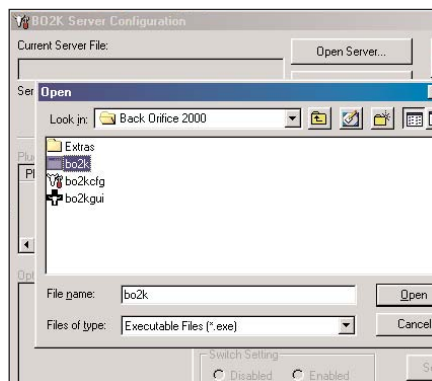
3 MEMILIH NOMOR PORT

Masukkan nilai port yang diinginkan. Untuk kompatibilitas penuh sebaiknya gunakan port di atas 1024, untuk memastikan tidak ada konflik dengan port-port yang sudah digunakan. Klik Next.



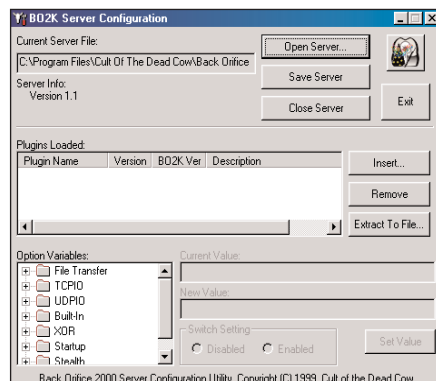
7 BO2K SERVER CONFIGURATION

Anda akan mendapatkan jendela konfigurasi BO2K Server Configuration. Di sini anda dapat mengubah konfigurasi server lebih lanjut. Bila menggunakan opsi-opsi standar pada Wizard, anda tidak harus mengkonfigurasi lebih lanjut. Klik Open Server.



8 OPEN FILE BO2K

Akan tampil jendela dialog Open yang langsung menuju direktori Back Orifice 2000. Ada tiga file: bo2k.exe, bo2kcfg.exe, dan bo2kgui.exe. Pilih bo2k.exe dan klik tombol Open. **Perhatian:** Jangan membuka BO2K.exe dengan double-click, sebab anda akan terinfeksi sendiri!



9 FLEKSIBILITAS KONFIGURASI

Tampak demikian banyaknya opsi yang dapat dikonfigurasi. Konfigurasi TCP misalnya, yang secara default beroperasi pada port 54320 dapat anda ubah menjadi port berapa saja. Pelajari opsi-opsi yang demikian banyak itu.

Sekali BO menginfeksi sistem, dia tidak akan tampil dalam list process (CTRL-ALT-DEL), dan akan berjalan secara otomatis setiap kali komputer dijalankan. Nama file yang berjalan sesuai dengan yang kita tentukan sebelumnya pada BO Server.

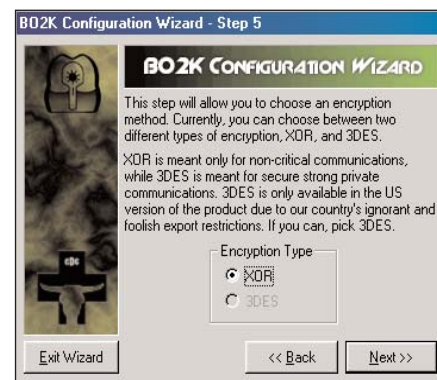
Pada kenyataannya, BO membuka jalan kepada para hacker, jika tidak mengeksplotasi setidaknya melakukan 'pelanggaran.'

Pada rilis ke-2 BO, Back Orrifice 2000 (BO2K) terdapat beberapa peningkatan. BO2K mempunyai semua kapabilitas dari versi rilis yang pertama, dengan beberapa perkecualian; server dan client

yang berjalan di NT/2000 dan Unix; tersedianya developer kit.

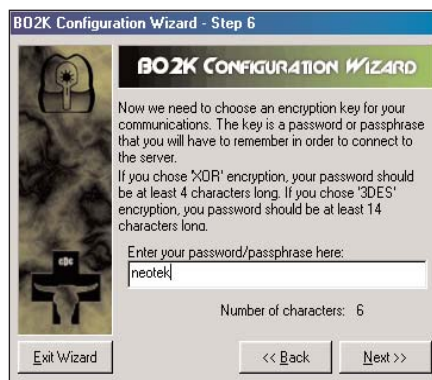
Konfigurasi dasar BO2K berpatokan pada TCP port 54320 atau UDP 54321, dan mengkopinya jadi umgr32.exe dalam folder system, menyamarkan dalam task list sebagai EXPLORER dan memerintahkan untuk mematikan sistem.

Jika disebar dengan Stealth Mode, maka akan terinstal dalam entry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices yang akan secara otomatis jalan pada Startup dan menghapus file yang asli. Semua setting ini dapat diatur menggunakan bo2kcfg.exe.



4 METODE ENKRIPSI

Ada dua metode enkripsi: XOR atau 3DES. XOR untuk komunikasi yang tidak terlalu kritis, sedangkan 3DES untuk komunikasi privat yang kuat dan secure. 3DES hanya tersedia untuk di US, jadi kita lanjutkan dengan meng-klik Next.



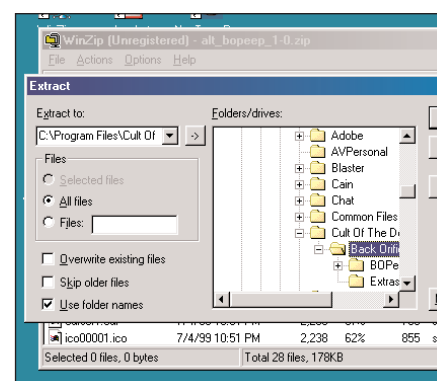
5 PASSWORD

Masukkan password, lalu klik Next. Password (atau passphrase) akan diperlukan sewaktu anda terhubung ke server. Bila menggunakan enkripsi XOR, panjang password minimal 4 karakter, sedangkan pada 3DES minimal 14 karakter.



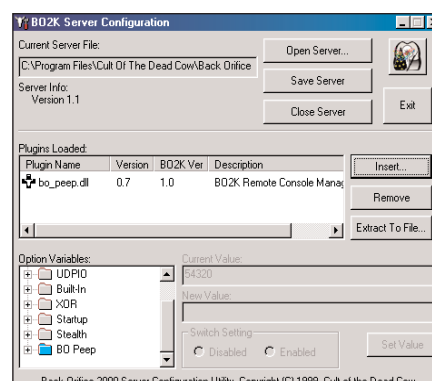
6 FINISH

Konfigurasi server selesai. Klik Finish. Selanjutnya anda harus mengkonfigurasi BO2K client dengan opsi yang sama. Bila anda akan menghubungkan server dengan komputer yang anda pakai ini, maka client akan secara otomatis di-setup sewaktu meng-klik 'Finish'.



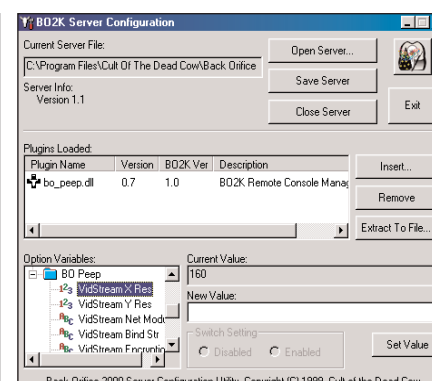
10 MEMASUKKAN PLUG-INS

Pada BO2K distribution standar tidak terdapat plug-in. BO2K plugin terdapat lengkap di CD NeoTek Vol. II/1 Oktober 2001. Pada contoh ini ekstrak BO Peep dari ke folder C:\Program Files\Cult of the Dead Cow\Back Orifice 2000



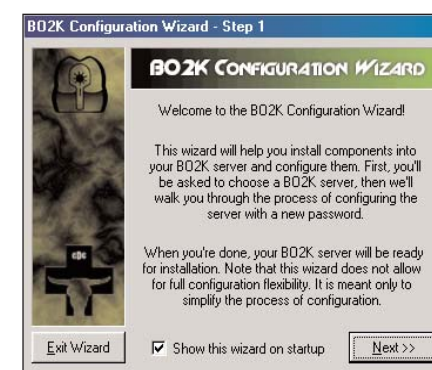
11 FOLDER BARU: BO PEEP

Buka folder yang BO Peep yang baru terbentuk dan pilih file plug-in yang berupa file .DLL. Dalam contoh ini adalah file bo_peep.dll yang merupakan BO2K Remote Console Manager.



12 NILAI DEFAULT FOLDER

Kita bisa mengubah default nilai dalam folder yang tertera, sesuai keinginan dan tujuan. Pada contoh ini tidak gunakan saja dulu nilai default-nya. Klik Save Server dan konfigurasi BO2K server selesai.



Apabila ada pertanyaan mengenai artikel ini, penulis dapat dihubungi di wiz_wuz@telkom.net

BACK ORIFICE 2000 MENJALANKAN PADA MESIN TARGET DAN MENGENDALIKANNYA

Sekali BO2K server telah dieksekusi pada suatu komputer, maka BO2K Server akan dijalankan setiap kali komputer tersebut dijalankan, dan menjadi sasaran empuk BO2K Client.

Mengendalikan remote computer yang dijadikan BO2K server.

Fungsi-fungsi standar yang ada pada BO2K sudah begitu kaya, sehingga akan mengasyikkan anda mengeksplorasinya.

Menjalankan BO2K pada mesin sasaran caranya mudah saja. Cukup meng-copykan file bo2k.exe dan jalankan software ini (dapat dengan *double click*, dan ingat jangan sekali-kali lakukan itu di komputer anda sendiri) maka secara otomatis file ini akan meng-copy dirinya sendiri menjadi umgr32.exe ke Windows\System. Nama ini dapat anda ganti sewaktu konfigurasi server.

Setelah itu anda tinggal menjalankan saja BO2K client yang akan menjadi pengendali terhadap remote computer yang

telah terpasang BO2K server. Untuk itu anda harus terhubung dulu ke server itu dengan menetapkan IP Address dan port untuk koneksi. Nomor port ini ditetapkan sewaktu konfigurasi server.

Sekali BO menginfeksi sistem, dia tidak akan tampil dalam list process (CTRL-ALT-DEL), dan akan berjalan secara otomatis setiap kali komputer dijalankan. Nama file yang berjalan sesuai dengan yang kita tentukan sebelumnya pada BO Server.

Dengan sekali klik pada tombol 'Connect to Server' anda sudah dapat mengendalikan remote computer itu sepenuhnya, termasuk me-*restart* komputer itu.

Selain fungsi-fungsi standar, BO2K dapat dibuat lebih tangguh lagi dengan menambahkan plug-in.

Berikut ini beberapa plug-in yang tersedia untuk BO2K:

BO_Peep Plugin

Memungkinkan anda mengintip apa saja yang sedang dikerjakan pada komputer sasaran dengan sistem real-time streaming video!

Butt Trumpet 2000

Remote e-mail tool

Rattler v.1.0

BO2K plug-in yang mengirim email ke user tertentu walaupun IP address-nya berubah

STCPIO Stealthy TCP IO

Plugin 'asli' dari Cult of the Dead Cow untuk menghindari IDS

Cast-256 Encryption Plugin

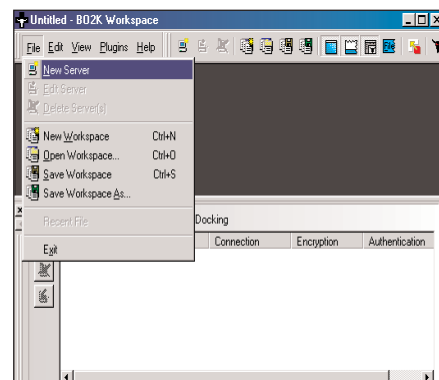
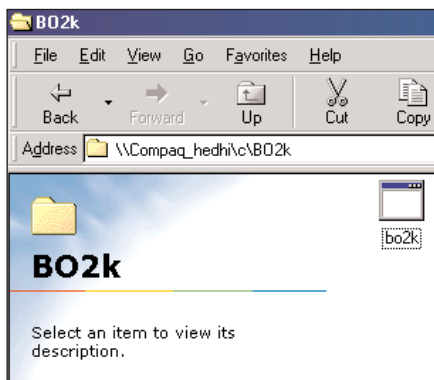
Enkripsi yang lebih kuat (256 bit) dari 3DES (168 bit) maupun IDEA (128 bit)

Serpent Strong Encryption

Sekuat Cast-256 tetapi lebih cepat.

BOTool

Remote Filesystem Browser & Registry Editor



1 MENJALANKAN BO2K

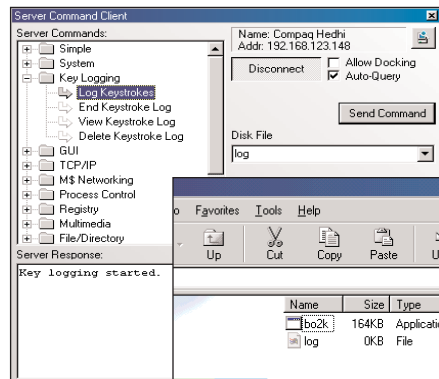
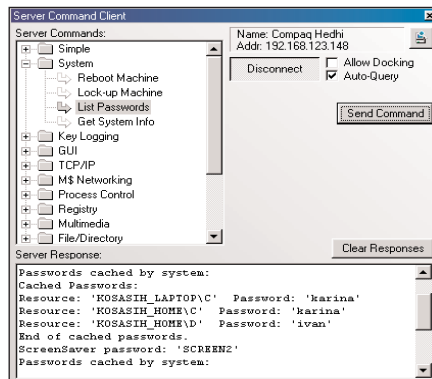
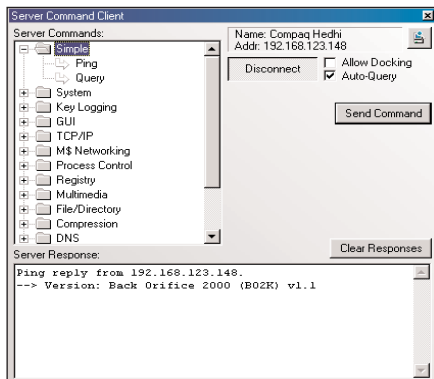
Copy BO2K.EXE ke mesin sasaran dan *double-click*, BO2K Server akan berjalan di latar belakang. Pada contoh ini dipasang pada mesin lain pada LAN (untuk mesin lain di Internet, anda harus menjebak pemakainya agar mau menjalankan BO2K.EXE ini).

2 JALANKAN BO2K CLIENT

Dari **Start > BO2K** jalankan **BO2K Client**. Akan tampil layar BO2K Workspace yang diawali oleh logo BO2K: '**Show Some Control**'.

3 BO2K WORK SPACE

Beginilah bentuk BO2K wok space. Pada ruang kerja inilah kita akan mengendalikan remote computer yang telah kita jadikan BO2K Server. Kita akan mencoba menghubungi komputer yang telah kita pasangkan BO2K.EXE tadi. Pilih menu **File > New Server**.



7 MENGIRIM PERINTAH KE SERVER

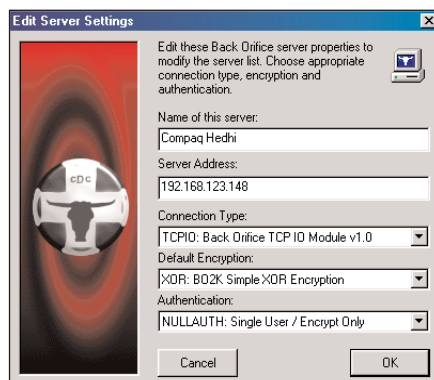
Dari pilihan-pilihan command yang ada, anda tinggal pilih lalu klik tombol **Send Command** dan respons dari server akan terlihat pada windows pane bawah. Kita mulai dengan dua **Simple** command: *ping* dan *query* seperti tampak pada gambar di atas.

8 MENCURI CACHED PASSWORD

Anda bisa mencuri *cached password* dengan perintah **List Passwords** pada **System**. Perintah pada System lainnya sudah cukup jelas: Reboot Machine, Lock-up Machine, dan Get System Info. Anda coba saja sendiri ketiga perintah 'iseng' ini.

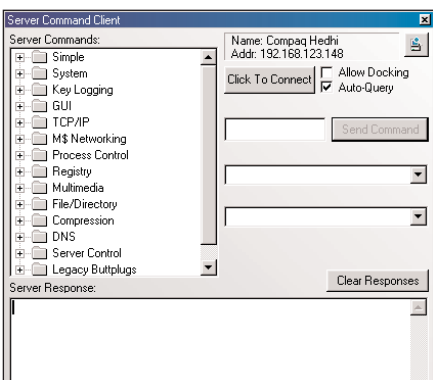
9 KEYSTROKE LOGGING

BO2K dapat juga berfungsi sebagai *keylogger*. Tetapkan nama file untuk menampung *keystroke* ini, misalkan nama file itu **log**. Pilih **Log Keystroke** pada Key Logging dan klik tombol **Send Command**. Tampak informasi Key logging started. Pada komputer target file log segera terbentuk.



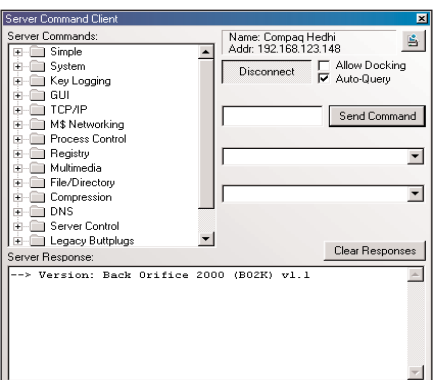
4 EDIT SERVER SETTING

Akan tampil jendela dialog **Edit Server Setting**. Namakan server ini (pada contoh: Compaq Hedhi) dan server address-nya (dalam hal ini 192.168.123.148). Adapun connection type, default encryption, dan authentication sudah ditetapkan sewaktu konfigurasi sebelumnya. Klik **OK**.



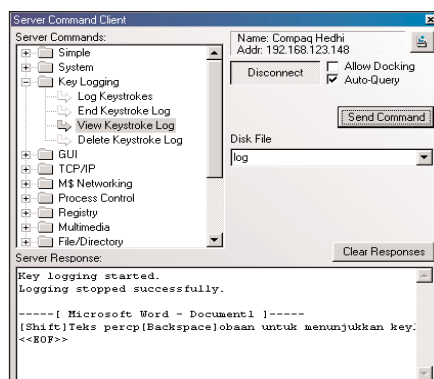
5 SERVER COMMAND CLIENT

Akan tampil jendela dialog **Server Command Client**. Dari sini kita dapat mengirimkan perintah-perintah ke server. Untuk dapat mengirimkan perintah, anda harus terhubung dulu ke server tersebut. Klik tombol **Click to Connect**.



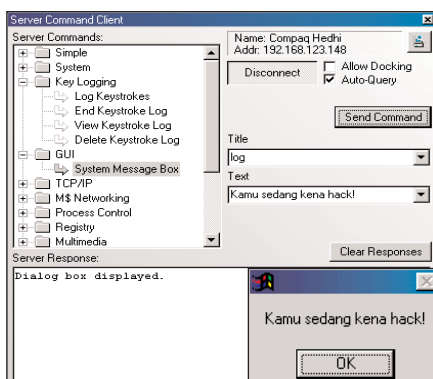
6 TERHUBUNG!

Akan tampil jendela dialog **Server Command Client**. Klik tombol **Connect** dan server yang kita hubungi memberi respons yang ditunjukkan pada window pane bagian bawah. Terlihat bahwa server menginformasikan bahwa di mesin ini terpasang BO2K versi 1.1.



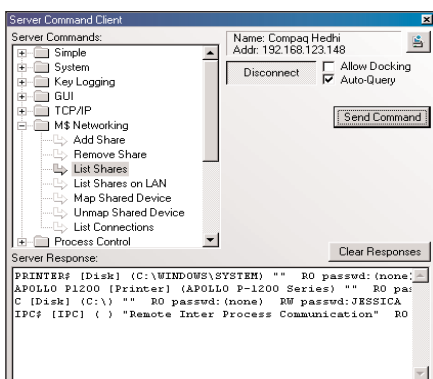
10 MELIHAT HASIL KEYLOGGING

Pada komputer target seseorang membuka Microsoft Word dan mengetikkan suatu teks dan menyimpannya. Semua itu dapat terlihat dengan jelas dengan **View Keystroke Log** dan klik **Send Command**.



11 MENGIRIM PESAN

Anda dapat mengirim pesan ke komputer sasaran dengan memilih **GUI > System Message Box** dan ketikkan pesannya, lalu klik **Send Command**. Pesan itu akan tampil di komputer sasaran.



12 PERINTAH-PERINTAH LAIN

Masih banyak perintah-perintah lain yang menarik yang dapat anda coba sendiri yang berhubungan dengan TCP/IP, MS Networking, Process Control, Multimedia, File/Directory, Compression, DNS, Server Control, dan Legacy Backup.

BACK ORIFICE 2000 INSTALASI BO PEEP DAN MENGINTIP SECARA REAL-TIME

Big brother is watching you! Itulah kira-kira yang terjadi pada komputer yang telah terinfeksi Back Orifice 2000 Server. Tanpa disadari, apa yang dilakukan di komputer itu dapat diamati orang lain.

Ada banyak plugin untuk BO2K, termasuk *plugin* untuk *anonymous email*, menghindari Intrusion Detection System (IDS), enkripsi, serta remote registry editor.

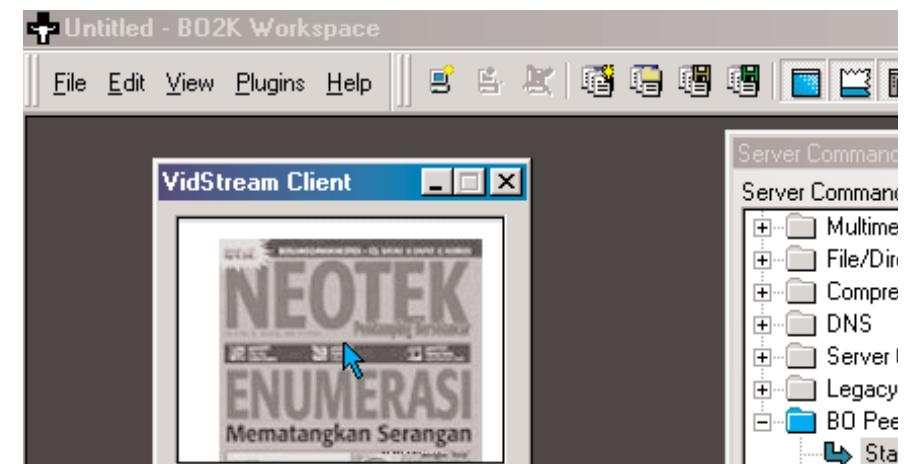
Kali ini kita membahas BO2K plugin yang paling standar, yaitu BO Peep. Walaupun standar, plugin ini merupakan yang paling menarik. Bagaimana tidak, kita seolah-olah memasang televisi untuk memonitor apa saja yang dikerjakan remote computer, lewat layar dengan video streaming!

Untuk menjalankan itu, baik pada BO2K server yang kita kirim ke komputer sasaran maupun BO2K client yang kita gunakan, harus terpasang BO Peep

plugin dengan konfigurasi yang sama. Apabila anda menggunakan komputer yang sama untuk *client* dan yang dipakai untuk menyiapkan BO2K server, maka konfigurasinya sudah sama, termasuk konfigurasi plugin-nya.

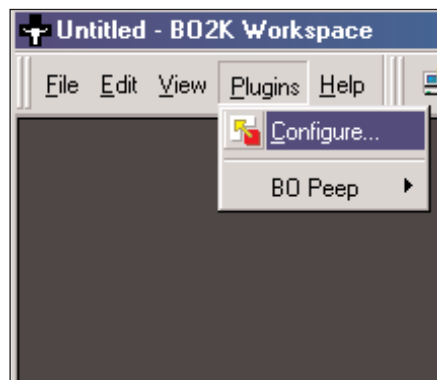
Apabila BO2K server terhubung pada port yang kita tetapkan sebelumnya (dalam contoh pada port 54320), maka Video Streaming ini akan terhubung secara default ke port 15151 pada IP Address yang sama.

Selain Video Streaming, terdapat pula fungsi untuk meng-Hijak remote mouse dari *rwemote* computer pada port 14141 di IP Address yang sama.

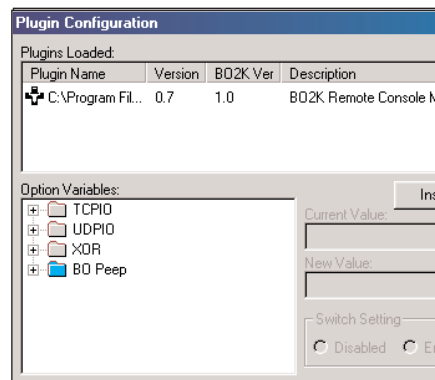


• Tampilan layar BO2K client yang sedang memonitor apa yang dikerjakan BO2k server.

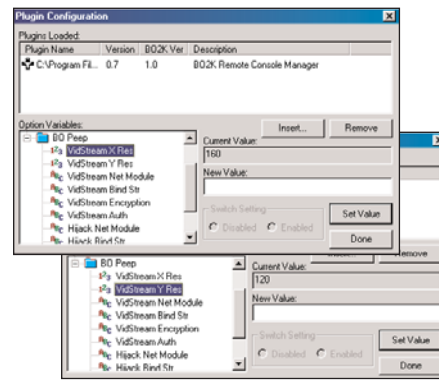
Memonitor secara real time apa yang dikerjakan dengan teknik video stream.



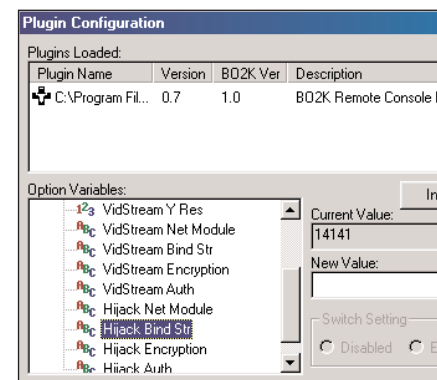
1 KONFIGURASI BO2K CLIENT
Jalankan **bo2kgui.exe** untuk mendapatkan BO2K Workspace. Pilih menu **Plugins > Configure...** untuk menampilkan jendela dialog **Plugin Configuration**.



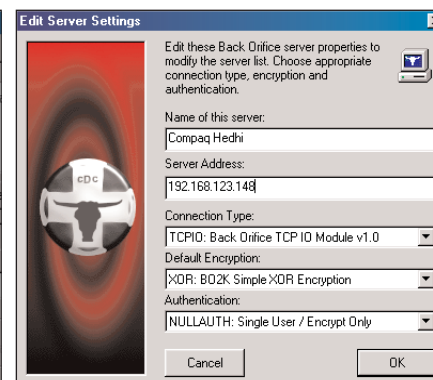
2 APAKAH BO_PEEP TERPASANG?
Pastikan bahwa plug-in BO_PEEP telah terpasang. Apabila komputer yang anda gunakan ini adalah komputer yang sama dengan yang digunakan untuk mengkonfigurasi plug-in untuk BO2K server, maka konfigurasi client-nya akan sama. Pilih folder **BO Peep** (warna biru).



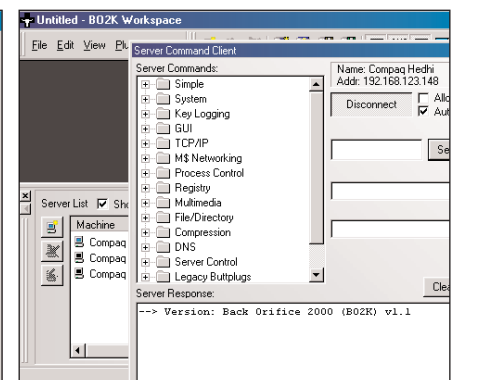
3 SETTING BO-PEEP
Catat setting BO Peep. Di antaranya: VidStream X Res: 160
VidStream Y Res: 120
VidStream Net Module: TCPIO
VidStream Bid Str: 15151
VidStream Encryption: XOR
VidStream Auth: NULLAUTH
Semua ini parameter video streaming.



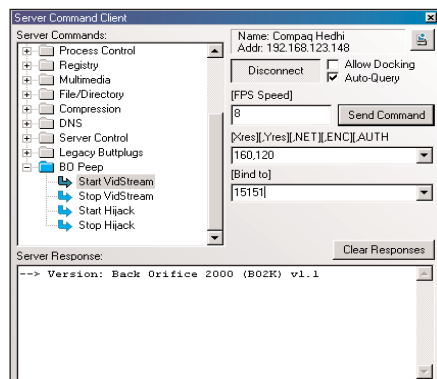
4 PARAMETER UNTUK HIJAK
Parameter untuk meng-hijak remote computer terdapat pada: Hijack Net Module: TCPIO
Hijack Bind Str: 14141
Hijack Encryption: XOR
Hijack Auth: NULLAUTH
Klik **Done** untuk kembali ke BO2K Workspace.



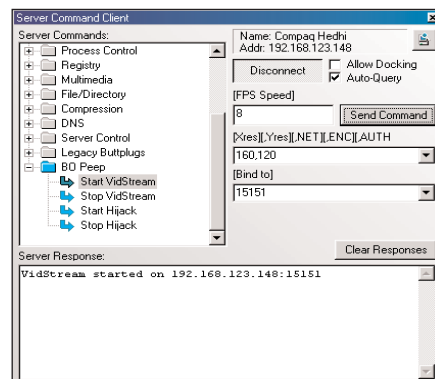
5 CONNECT TO SERVER
Pilih **File > New Server** dan masukkan setting dari server yang akan dihubungi. Beri nama untuk server ini dan masukkan IP Address-nya. Klik **OK** untuk menghubungkan server tersebut.



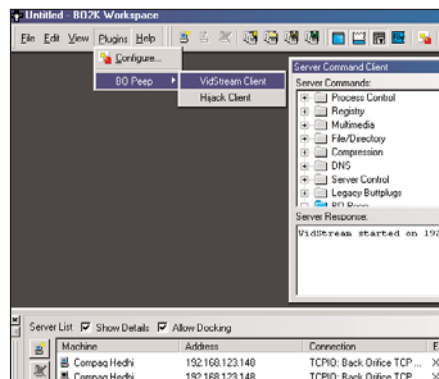
6 TERHUBUNG!
Akan tampil jendela dialog **Server Command Client**. Klik tombol **Connect** dan server yang kita hubungi memberi respons yang ditunjukkan pada window pane bagian bawah. Terlihat bahwa server menginformasikan bahwa di mesin ini terpasang BO2K versi 1.1.



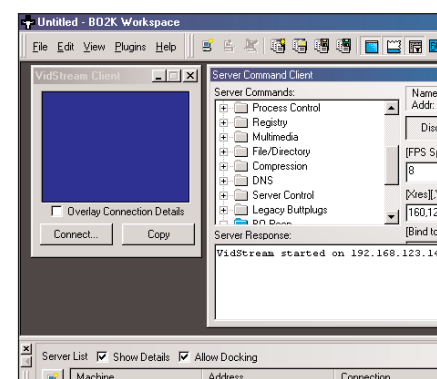
7 PERINTAH BO PEEP KE SERVER
Jalankan VidStream dengan parameter-parameternya. Pilih **Start VidStream** pada folder BO Peep, lalu masukkan FPS: 8
[XRes][YRes][NET][ENC][AUTH: 160,120
[Bind To]: 15151
lalu klik tombol **Send Command**



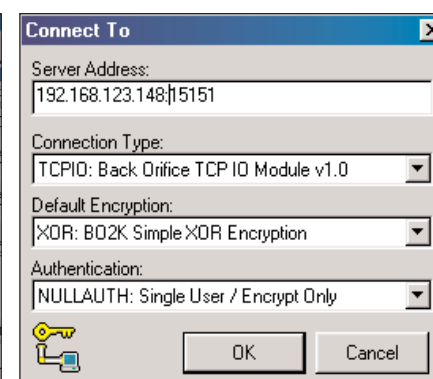
8 VISTREAM DIJALANKAN
Pada windows pane bawah terlihat pesan bahwa VidStream sudah dijalankan: VidStream started on 192.168.123.148:15151



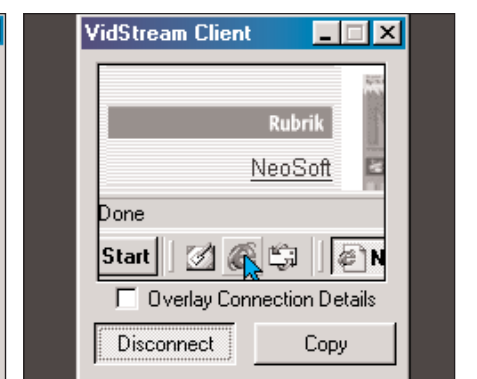
9 JALANKAN VIDSTREAM CLIENT
Untuk menjalankan VidStream Client, pilih menu **Plugin > BO Peep > VidStream Client** dari BO2K Workspace.



10 VIDSTREAM CLIENT SCREEN
Akan tampil layar biru dengan ukuran 160x120 pixel yang akan menjadi jendela kita untuk mengintip apa yang ditampilkan pada layar remote computer (yang menjalankan BO2K server) dan sedang kita kendalikan dengan BO2K Client.



11 KE VIDSTREAM SERVER
Klik **Connect** pada tombol di bawah layar dan anda akan masuk ke jendela dialog Connect to. Pada server address telah tertera nomor port 15151. Lengkapi dengan IP Address menjadi 192.168.123.148:15151 dan klik **OK**.



12 MONITOR REAL TIME
Segera akan tampil potongan yang penting-penting dari layar monitor remote computer seperti bagian Taskbar yang di-klik serta sebagian dari apa yang terlihat pada desktop. Kebetulan di sini remote computer sedang masuk ke situs NeoTek.

NetBuster Menjebak Para Penyusup

Jengkel karena pernah di-hack? Jangan tinggal diam, gunakan **NetBuster** untuk menjebak para penyusup seolah-olah sudah berhasil menguasai komputer anda, padahal andalah yang menguasai komputer si iseng itu. **Eryanto Sitorus** membahasnya untuk anda.

JIKA ANDA TERMASUK SALAH satu dari sekian banyak pengguna Internet, yang (mungkin) pernah di-“terror” *hacker*, tentunya anda pernah memikirkan bagaimana cara menjebak dan mempermainkan mereka biar kapok! Bagi saya pribadi, yang pernah *dikerjai* mereka, itulah salah satu yang menjadi obsesi setiap kali akan terhubung ke Internet. Ya! saya ingin balas dendam.

Kejadiannya persis terjadi kira-kira dua bulan yang lalu, ketika saya sedang asyik chatting pada salah satu channel IRC (Internet Relay Chat). Tidak tahu dari mana sumbernya dan apa penyebabnya, tiba-tiba dua buah program yang sedang saya jalankan saat itu (mIRC dan Internet Explorer) lenyap begitu saja dari pandangan mata, dan disusul kemudian dengan Shut Down. Pada awalnya saya cuma mengira bahwa penyebabnya adalah karena *operating system* Microsoft Windows ME (Millennium Edition) saya yang sedang “kacau,” namun setelah beberapa kali saya mengetik ulang kata sandi (*password*) email dan nick IRC, yang muncul selalu tulisan “Invalid Password” — “Incorrect Password.” Akhirnya saya baru sadar bahwa kejadian tersebut tadi bukan karena kerusakan pada sistem, tetapi lebih tepat disebut “malapetaka,” karena saya benar-benar telah di-*hack* seseorang yang tidak tahu siapa orangnya dan di mana dia berada.

Dengan perasaan dongkol dan geram, kemudian saya periksa komputer saya dan melakukan uji coba. Ketemu! Rupanya selama ini, tanpa saya sadari, komputer saya telah berubah menjadi “server” bagi seseorang yang berhasil memasukkan dan mengaktifkan PATCH.EXE ke dalam sistem saya. PATCH.EXE adalah file trojan milik program NetBus, yang jika dia aktif atau diaktifkan ke dalam komputer seseorang, maka secara otomatis kita akan dengan mudah masuk dan melakukan apa saja di komputer orang

tersebut, termasuk melihat kata sandi (*password*), meng-kill (*close*) program yang sedang aktif dan men-*shut down* komputernya melalui program yang disebut NetBus, NetHacker, Back Orifice atau Deep Back Orifice. Itulah satu kesimpulan yang saya peroleh. Oleh karena itu, saya juga ingin mengingatkan anda, agar waspada dan selalu berhati-hati pada saat terhubung ke Internet. Karena di Internet tidak ada yang tidak mungkin.

Nah, sekarang kita kembali ke persoalan semula, yaitu bagaimana cara menjebak dan mempermainkan mereka yang mendeklarasikan dirinya sebagai hacker, yang kerjanya sehari-hari mungkin hanya ingin mengintimidasi dan mempermainkan anda, saya, dan pengguna Internet lain.

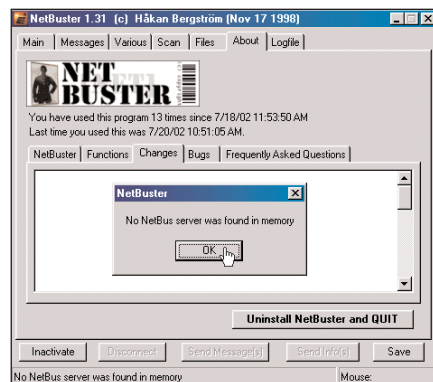
Salah satu cara yang paling gampang untuk melakukan hal itu adalah dengan menggunakan program **NetBuster**, yang dibuat oleh Hakan Bergstrom. Program tersebut bisa anda peroleh gratis di alamat berikut:

- <http://surf.to/netbuster>
- www16.brinkster.com/erytricksy/Software/netbuster_v131.zip

Secara teknis, NetBuster adalah program anti NetBus, yang selain berfungsi untuk mempermainkan para penyusup yang masuk ke dalam komputer kita, juga dimungkinkan untuk melakukan serangan balik ke komputer orang tersebut. Bisa melalui program NetBuster itu sendiri atau program hacking lain seperti NetHacker, Back Orifice, Deep Back Orifice, dan sebagainya. README file menyebutkan “NetBuster is Win 95/97/98/ME/2000/XP/NT tool to fool with the people trying to fool you with NetBus. It also removes any NetBus server from your system if found. NetBuster emulates the NetBus server so that the intruder THINKS he’s fooling around with you. But instead all his actions will be logged, and you will be able to fool him instead.”

Nah, setelah anda membaca deskripsi singkat cara kerja NetBuster (secara teori), maka sekarang kita akan mempraktikkannya secara langsung. Perlu anda ketahui, bahwa semua proses yang diperlihatkan pada beberapa gambar yang penulis sertakan dalam artikel ini, adalah gambar dari kejadian “nyata” yang penulis tangkap pada saat seseorang masuk ke dalam komputer penulis. Langkah-langkahnya adalah sebagai berikut:

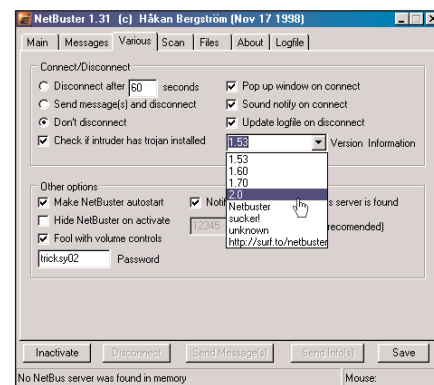
1. Pertama masuk ke folder atau direktori tempat anda meletakkan program NetBuster, lalu klik dua kali file NET-BUSTER.EXE. Sesaat kemudian NetBuster akan memeriksa apakah NetBus *server* sedang aktif di memori komputer anda, seperti terlihat pada Gambar 1. Jika NetBuster menemukan-nya, maka NetBuster akan menonaktifkan dan menghapusnya.



• Gambar 1: Menjalankan program NetBuster.

Sebagai informasi, setelah anda menginstal NetBuster, program tersebut akan dijalankan secara otomatis setiap kali anda meng-ON kan komputer anda. Namun jika anda tidak menginginkan itu terjadi, anda bisa mengubahnya dengan menghilangkan opsi [v] pada Make NetBuster autostart dalam tab Various.

2. Klik tab Various, lalu pastikan bahwa anda sudah mengaktifkan opsi “Check if intruder has trojan installed.” Ke-

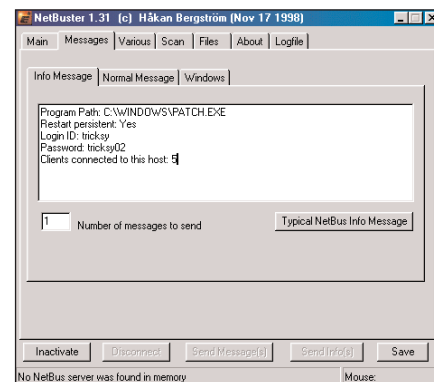


• Gambar 2: Memilih versi Trojan yang akan dideteksi.

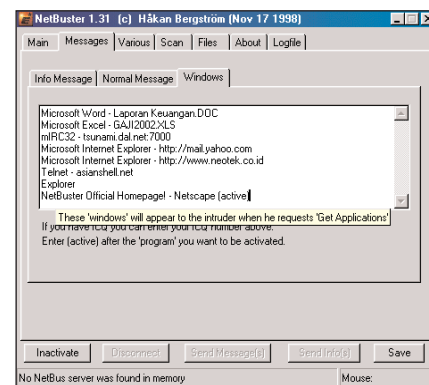
mudian klik “Version Information” untuk memilih versi trojan yang nantinya akan dideteksi NetBuster ketika penyusup mencoba masuk ke dalam komputer anda, seperti yang tampak pada Gambar 2.

3. Mungkin, katakanlah ketika seorang penyusup berhasil masuk ke dalam komputer anda melalui program NetBus, NetHacker, Back Orifice, atau yang lainnya, maka orang tersebut tentunya pasti ingin mengetahui informasi versi trojan yang aktif di sistem komputer anda, termasuk informasi semua program yang sedang anda aktifkan. Nah, khusus untuk yang satu itu, kita bisa mengelabui mereka dengan memberikan informasi palsu. Caranya, masuklah ke tab Messages, lalu ketikkan beberapa informasi palsu ke dalam tab Info Message, Normal Message dan tab Windows, seperti yang terlihat pada Gambar 3-4.

4. Setelah anda selesai mengisi informasi atau keterangan palsu ke dalam semua tab Messages, kemudian simpan lah semua perubahan tersebut dengan mengklik tombol Save, kemudian klik Minimize. Demi keamanan dan kenyamanan anda ketika berselancar atau chatting di Internet, saya sarankan sebaiknya biarkanlah program tersebut selalu aktif di komputer

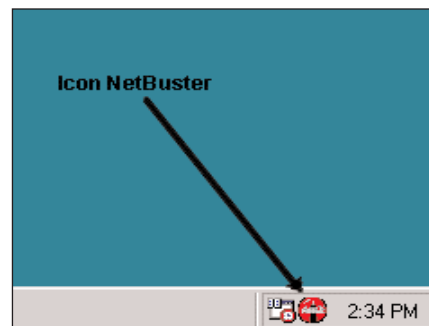


• Gambar 3: Mengisi informasi palsu ke dalam tab Info Message.



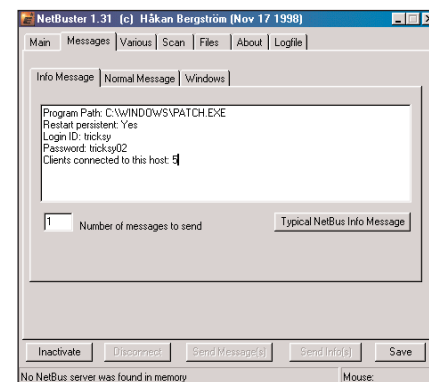
• Gambar 4: Mengisi informasi palsu ke dalam tab Windows.

anda. Dengan begitu maka anda akan selalu siap menjebak dan mempermainkan para penyusup (intruder) jika sewaktu-waktu mereka mencoba mengusik kenyamanan anda.

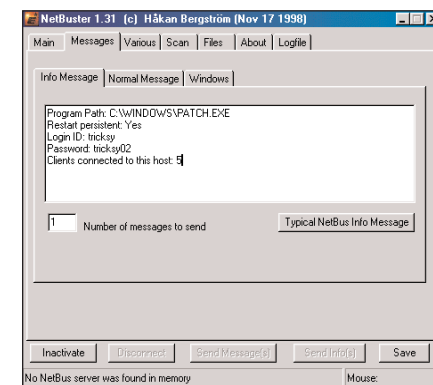


• Gambar 5: Tampilan ikon program NetBuster yang sedang aktif.

5. Setelah melakukan dialup, masuklah ke dalam beberapa channel IRC yang anda anggap sebagai channel “rawan” hacker, dimana semua para peserta yang ada di dalam channel-channel tersebut berpotensi untuk melakukan intrusi ke komputer orang lain. Dan jika anda sedang bernasib baik, tidak lama setelah itu program NetBuster anda yang tadinya mungkin sedang “tidur,” tiba-tiba “terbangun” dan melaporkan sinyal bahaya kepada anda, seperti terlihat pada Gambar 6.



• Gambar 6: NetBuster melaporkan sinyal bahaya.

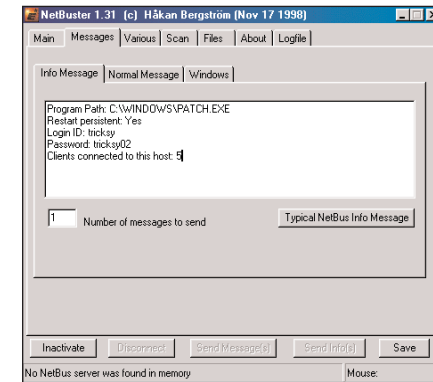


• Gambar 7: Mengirim pesan kepada penyusup.

Dalam Gambar 6 terlihat bahwa seorang penyusup yang menggunakan alamat IP 202.159.28.171 sudah berhasil masuk ke dalam perangkat anda. Tapi sayangnya nasib baik anda ternyata nilainya tidak mencapai 100%, mungkin hanya 50% saja. Karena pada jendela Logged events and actions terbaca pesan “No NetBus server found on remote host.” Artinya anda tidak bisa menyerang penyusup tersebut secara total. Namun demikian anda masih bisa “menggertak” penyusup tersebut dengan mengirim pesan seperti yang terlihat pada Gambar 7 melalui tombol “Send Message(s).” Dan jika anda tidak terlalu *mood* untuk mempermainkan penyusup itu, segera putuskan koneksinya dengan mengklik tombol Disconnect.

Setelah memutuskan koneksi si penyusup tadi yang kehadirannya tidak begitu membuat kita surprise, mungkin tidak lama setelah itu NetBuster anda kembali melaporkan sinyal bahaya, seperti terlihat pada Gambar 8.

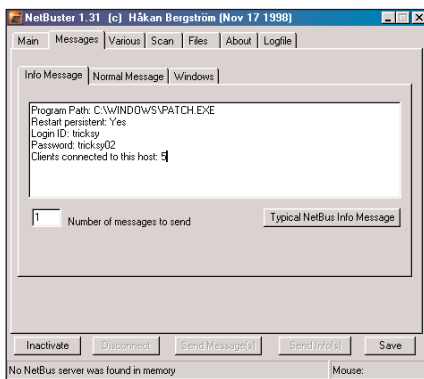
Apa yang dilaporkan NetBuster seperti terlihat dalam Gambar 8 tentunya adalah merupakan “good news” buat kita. Kerena dengan begitu, maka apa yang kita harapkan sejak awal kini sudah terkabul.



• Gambar 8: Sinyal bahaya yang dilaporkan NetBuster.

Perhatikan, pada program NetBuster anda tersedia tujuh tombol penting yang kini sudah dapat anda pakai untuk memukul balik si penyusup tadi, yaitu: Open CD, Swap Mouse, Key Click On, Set Password, Disconnect, Send Message(s) dan Send Info(s).

Hal ini berbeda dengan apa yang diperlihatkan pada Gambar 7, yang hanya menyediakan tiga buah tombol. Namun jika anda merasa tidak cukup puas hanya menggentak si penyusup tadi dengan mengirim pesan-pesan "angker," atau membuka dan menutup CD ROM komputer-nya. Anda bisa menjalankan program-program hacking lain, seperti NetBus, atau Back Orifice misalnya, yang memiliki banyak tombol-tombol penting seperti yang tampak pada Gambar 9.



• Gambar 9: Menyerang si penyusup dengan NetBus.

Akhirnya, sebagai penutup, saya ucapkan selamat pada anda!. Karena dengan mencoba menerapkan apa yang sudah saya bahas dalam artikel ini, maka secara langsung maupun tidak langsung anda telah ikut berpartisipasi dalam memberantas narkoba. Eeh maksud saya dalam memberantas hacker. Good luck!

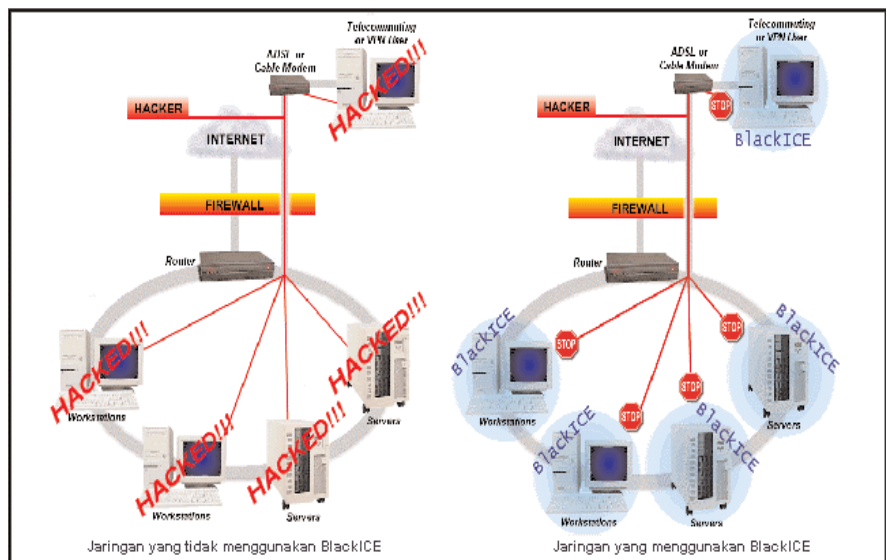
Apabila ada pertanyaan mengenai artikel ini, hubungi penulisnya di ery@postmaster.co.uk.

INTERNET ADALAH SESUATU YANG SANGAT FENOMENAL, DIA TUMBUH DAN berkembang dengan cepat, dibutuhkan karena bermanfaat sebagai media komunikasi dan sumber informasi, diminati dan digemari banyak orang dari semua lapisan masyarakat, baik yang kaya, setengah kaya, laki-laki, perempuan, tua, dan muda. Namun, tanpa kita sadari, ternyata Internet juga dapat membuat kita menjadi boros, ketagihan, merasa curiga, gelisah, dan selalu khawatir, yang pada akhirnya lama-kelamaan dapat merubah diri kita menjadi seorang paranoid.

Mungkin, salah satunya, hal itu lah yang dirasakan oleh rekan sekantor saya. Akibat ketagihan "ngakses" Internet, dia kaget bukan main setelah membayar rekening listrik dan telepon yang jumlahnya nyaris sama dengan jumlah gaji yang diperolehnya di kantor.

Sementara itu, masalah-masalah lain yang juga kerap membuat kita gelisah adalah kehadiran dan aktifitas para hacker, yang secara langsung maupun tidak langsung berhasil membuat kita merasa khawatir dan menjadi tidak leluasa ketika mengakses Internet. Kehadiran mereka di dunia Internet telah menjadi ancaman besar buat kita (pengguna Internet). Akibatnya, kita pun menjadi merasa tidak aman setiap kali mengetik kata sandi (password) email, kita curiga jangan-jangan ada pihak lain menangkap apa yang kita ketik pada saat akan meng-indentify nick IRC (Internet Relay Chat) ke NickServ, atau kata sandi channel IRC yang sudah saatnya untuk kita indentify sebelum di drop oleh ChanServ. Kita juga merasa khawatir ketika akan mengetik kata sandi shell account, account Web, GuestBook, serta account-account lainnya. Jika itu yang terus menerus kita alami setiap kali terhubung ke Internet, maka bukan tidak mungkin hal itu akan memberikan implikasi buruk pada kesehatan kita.

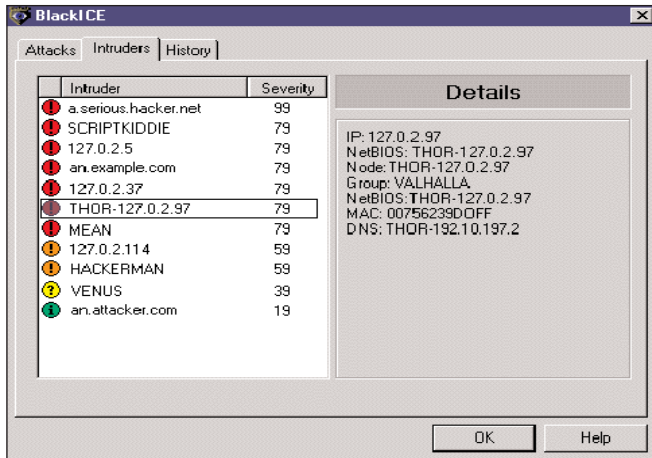
Nah, daripada kesehatan kita terganggu karena selalu merasa khawatir, gelisah, dan curiga tidak menentu seperti itu, lebih baik kita amankan sistem komputer kita. Salah satu cara yang paling efektif yang dapat kita lakukan, tentunya adalah dengan menginstal software yang benar-benar bisa diandalkan dan dapat dipercaya untuk melindungi komputer dari serangan hacker. Dalam hal ini anda perlu selektif, saya katakan sekali lagi pilihlah *software* yang keandalannya sudah tidak diragukan lagi.



BlackICE

Pelindung terhadap Network Intrusion

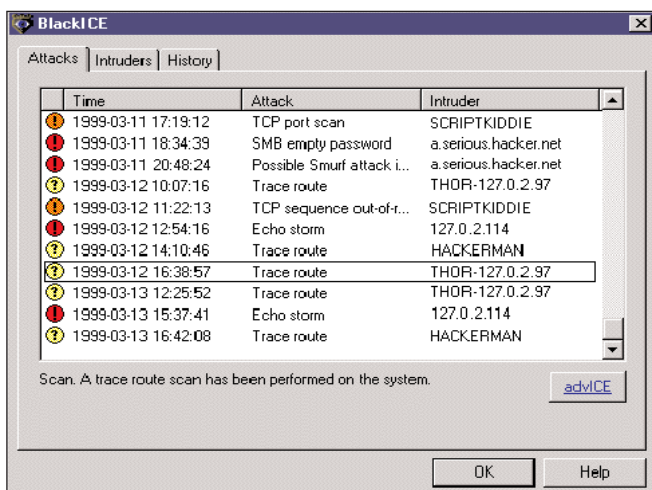
Untuk melengkapi tulisan mengenai Intrusion Detection System (IDS) sebelumnya (Snort dan PortSentry), kali ini **Eryanto Sitorus** membahas salah satu Intrusion Detection System yang mudah digunakan, yaitu **Black ICE**.



• Gambar 1: Informasi para pengguna (intruder).

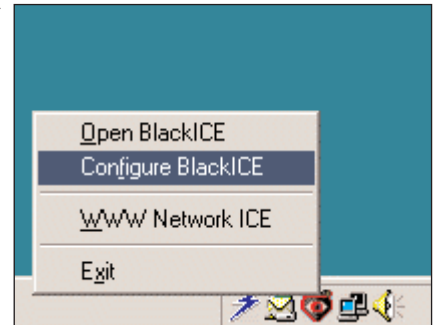
Salah satu dari sekian banyak software yang layak untuk anda pertimbangkan adalah BlackICE Defender. Alasan penulis merekomendasikan software tersebut untuk anda pakai adalah karena memang penulis telah membuktikan sendiri, BlackICE Defender adalah software anti hacker yang terbaik dan sangat handal. Dengan BlackICE Defender, maka dapat dipastikan bahwa komputer atau jaringan komputer anda akan selamat dan terhindar dari hacker, yang selain bermaksud ingin mengusik kenyamanan anda ketika berselancar di Internet, juga ingin mencuri data, dan men-celakakan komputer anda.

Disebutkan bahwa BlackICE terbuat dari alat pelacak yang kekuatannya sangat luar biasa dan sekaligus sebagai mesin analisis yang dapat memvisualisasikan semua lalu-lintas port



• Gambar 2: Informasi jenis serangan yang dilakukan para pengganggu.

• Gambar 3: BlackICE Defender yang sudah terinstal dan aktif.



jaringan dan protokol yang dicurigai. Jika BlackICE mendeteksi adanya kemungkinan serangan, maka BlackICE akan langsung mengirim dan merekam

aktifitas tersebut ke dalam file log. Kemudian informasi tentang penyerang tersebut akan dilaporkan ke dalam tab Intruders, seperti yang terlihat pada Gambar 1. Sedangkan informasi tentang jenis serangan yang dilakukan para pengganggu tersebut akan di coba divisualisasikan ke dalam tab Attacks, seperti yang tampak pada Gambar 2.

BlackICE mengumpulkan informasi dari setiap serangan yang sudah dianalisis dengan menggunakan algoritma jaringan yang dibuat secara khusus. Jika serangan tersebut nantinya dianggap berpotensi menjadi intrusi, maka BlackICE akan secara otomatis memblokir setiap akses yang dilakukan dari komputer (alamat IP) hacker tersebut. Dan asal anda tahu saja, biar bagaimana gigihnya pun hacker tersebut mencoba meng-crack sistem anda, dijamin orang tersebut tidak akan pernah berhasil masuk ke dalam lingkungan BlackICE.

Secara teknis, BlackICE dapat bekerja dengan baik pada sistem operasi Microsoft Windows 95/97/98/ME/2000/XP serta Windows NT. Sedangkan spesifikasi hardware yang dibutuhkan, antara lain adalah:

1. Menggunakan prosesor Pentium.
2. Sedikitnya memiliki RAM sebesar 16 MB.
3. Kapasitas hard disk yang tersisa sedikitnya harus ada sebesar 6.5 MB. Jumlah tersebut sudah termasuk persiapan tempat sebesar 2.5 MB untuk mengalokasikan semua file logging trace.

Jika anda tertarik untuk menginstal software tersebut, anda dapat menginstalnya langsung dari dalam CD Neotek yang disertakan pada majalah ini. Namun bagi anda yang (mungkin) hanya meminjam majalah ini dari teman anda (alias tidak membeli), anda bisa mendownloadnya dari beberapa alamat situs tersebut di bawah ini:

1. www.black-ice-firewall.com
2. www.lml.se/blackice.htm
3. www.aragoza.com/download/blackice/defender/
4. www16.brinkster.net/erytricksy/Software/
5. www.downloadstore.com/

ery@postmaster.co.uk

PSYCHOSTATS

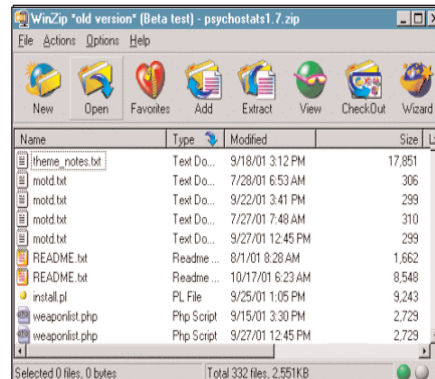
DUKUNGAN STATISTIK GAME COUNTER-STRIKE

Begitu populernya **Counter Strike** sebagai game First Person Shooter yang dimainkan secara multiplayer di Internet memunculkan banyak situs-situs pendukung bagi game ini. Selain pengayaan seperti peta permainan, terdapat pula **psychostats**, dukungan untuk statistik permainan. **William** menyajikannya untuk anda.

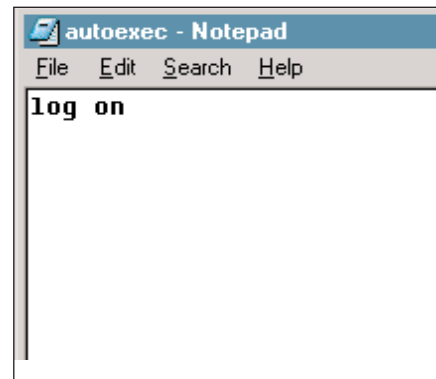
Instalasi support untuk game Counter Strike membutuhkan pengetahuan mengenai Perl and PHP.



1 MASUK KE SITUS PSYCHOSTATS
Arahkan browser anda ke alamat <http://www.psychostats.com/download.php> Pilih Windows Distribution versi 1.7 dengan ukuran 2MB file zip.



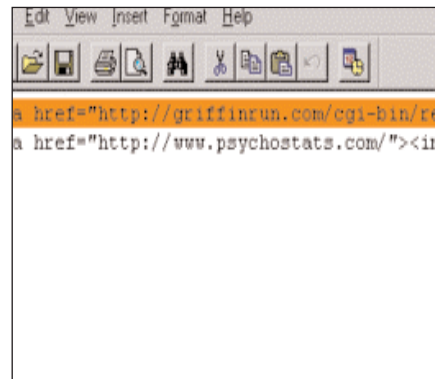
2 UNZIP FILE PSYCHOSTATS
Anggaphlah anda telah memiliki game Counter Strike yang diinstal di folder **C:\Sierra\Counter-Strike** (default). Unzip semua file **psychostats1.7.zip** yang telah anda download ke folder **C:\Sierra**. Jangan gunakan Notepad untuk mengubah setting, melainkan Wordpad.



3 BUAT AUTOEXEC.CFG
Buka Notepad dan tuliskan **log on**. Kemudian **Save as** autoexec.cfg dan simpan di folder **C:\Sierra\Counter-Strike\cstrike**. Kemudian mainkan game Counter Strike dengan bot anda agar terbentuk direktori logs di folder **cstrike**. Semua kemenangan dan kekalahan akan dicatat.



7 LIHAT DENGAN BROWSER
Ketikkan <http://localhost/cgi-bin/stats> untuk melihat status permainan anda. Ada sesuatu yang mengganggu yaitu adanya banner tanpa gambar di bagian paling atas halaman. Ini karena file gambarnya hanya tersedia online. Yang harus dilakukan adalah **rename** direktori PsychoStats ke **Psycho**



8 MENGHILANGKAN BANNER
Hilangkan dengan menghapus banner codenya. Masuk ke **C:\Sierra\Psycho\themes\cstrike1.7** atau **cstrike1.7.php** untuk membuka PHP theme dan cari banner.html. Buka dengan Notepad dan hapus kode mulai tag **<a>** pertama sampai ****, kemudian **Save**. Jalankan **stats.pl**. Banner pertama hilang.



9 PHP THEME
Psychostats dengan PHP theme lebih unggul karena mempunyai fungsi **Search pemain** (yang telah memenuhi syarat kemenangan). Theme yang tersedia terdiri dari 4 bagian, 2 bagian untuk versi cstrike.html dan 2 untuk PHP. Versi html telah selesai dibahas. Langkah selanjutnya untuk PHP theme.

mengenai kemenangan, kekalahan, senjata yang dipakai, sampai status peta yang digunakan.

Pada awalnya, psychostats berjalan pada sistem operasi Linux, namun kini psychostats berjalan juga pada Windows.

Script yang diciptakan Stormtrooper masih memiliki kekurangan, terutama kesalahan penggunaan variabel dalam salah satu script PHP-nya. Namun kekurangan tersebut bukanlah kesalahan yang fatal dan masih dapat di atasi.

Konsep kerja psychostats sangat sederhana. Psychostats dalam bentuk script Perl berfungsi memproses kata-kata yang dihasilkan oleh Server

Counter-Strike

Game Counter Strike yang kemudian disajikan dalam bentuk diagram dalam Layout Table yang mudah dibaca dan dipahami.

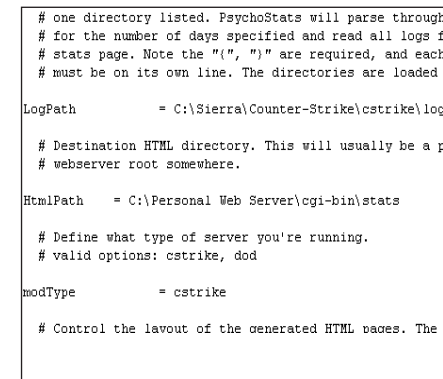
Agar dapat menggunakan Psychostats, pada komputer yang merupakan server Counter Strike terlebih dahulu sudah harus terinstal Active Perl, PWS (Personal Web Server), dan PHP.

Setelah ketiga pendukung tersebut telah terinstal, selanjutnya tinggal menginstal psychostat itu sendiri.

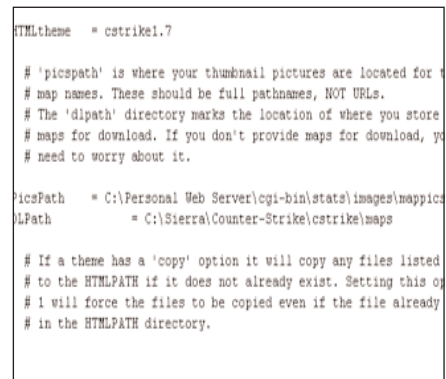
Untuk jelasnya, ikuti langkah-langkah dalam artikel ini berikut ini.

Untuk mengetahui informasi lebih dalam mengenai psychostats, kunjungi **www.psychostats.com** Di situs tersebut terdapat forum bagi yang ingin bertanya seputar psychostats.

Apabila ada pertanyaan mengenai artikel ini, penulis dapat dihubungi di ascii255@telkom.net



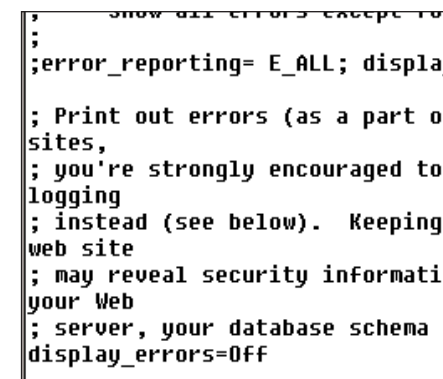
4 UBAH SETTING STATS.CFG
Cari **stats.cfg** di direktori **C:\Sierra\psychostats** kemudian buka file tersebut dengan Wordpad. Cari baris: **LogPath** dan ubah persis menjadi **LogPath = C:\Sierra\Counter-Strike\cstrike\logs**. Kemudian Cari baris **HtmlPath** dan ubah ke **C:\Personal Web Server\cgi-bin\stats**



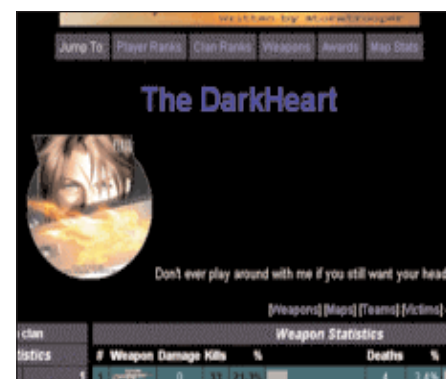
5 UBAH SETTING STATS.CFG
Kemudian carilah baris **PicsPath** ubah ke **C:\Personal Web Server\cgi-bin\stats\images\mappics**. Cari **DLPath** ubah ke **C:\Sierra\Counter-Strike\cstrike\maps**. Anda juga perlu memodifikasi baris tertentu seperti Admin name, admin e-mail sesuai data diri anda. Terakhir **Save**.



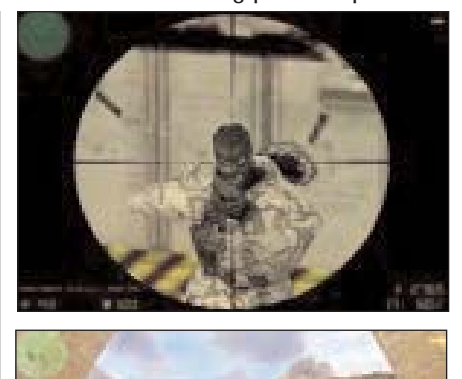
6 JALANKAN FILE INSTALASI
Sekarang jalankan file **install.pl**. Anda akan ditanya apakah settingnya telah benar, ketik **Yes**. Dengan begitu akan terbentuk **stats.pl** dan folder images di folder **stats**. Kemudian jalankan **stats.pl** maka semua log file akan di-scan dan terbentuk file html di PWS. File **stats.pl** perlu dijalankan berulang kali untuk mengupdate status pemain.



10 SETTING PHP.INI
Untuk menggunakan PHP Theme, set **php.ini**. Buka dengan Notepad; cari dan ubah setting barisnya. Cari **display_error**, set ke **Off** dan tambahkan ; (titik koma) ke **error_reporting** yang belum mempunyai ; PHP programmer harus mengembalikan settingnya ke semula. Jalankan **stats.pl**, buka browser dan uji.



11 PLAYER LOGO
Untuk memakai **player logo** pada file **playerlogos.cfg** perlu ditambahkan tag. Tulis seperti seperti yang dicontohkan. Boleh juga menghapus line Default kalau anda bukan server admin di Internet. Untuk mengotomatisasi pekerjaan update status, bisa gunakan **Scheduled Wizard** pada Windows.





Membuat & Bermain Puzzle Elektronik

Karena rutinitas sehari-hari dalam berkomputer, anda mungkin memerlukan sesuatu yang bersifat *entertainment*. **Eryanto Sitorus** mengajak anda berekreasi membuat game *puzzle* sendiri. dengan menggunakan program gratis bernama **Jigsaws Galore**.

SETIAP HARI NONGKRONG DI DEPAN KOMPUTER terkadang bisa membuat kita merasa sumpek, jenuh, bosan, atau bete. Jika sudah bosan, maka akhirnya kita pun jadi bingung dan agak sedikit malas-malasan. Bahkan, saking sumpeknnya, kadang-kadang *chatting* saja pun rasanya malas, mau *browsing* malas, 'nyetel MP3' malas, main *game* malas, sementara jelas-jelas kita tahu bahwa saat itu (mungkin) PC kita masih dalam keadaan terhubung (*connected*) ke Internet. Nah, dari pada kita uring-uringan tidak karuan, dan menghabiskan pulsa telepon untuk sesuatu yang tidak dinikmati, lebih baik kita bermain *puzzle*, yah tentunya *puzzle* elektronik yang dibuat dengan program dan dimainkan di komputer. Asyik!

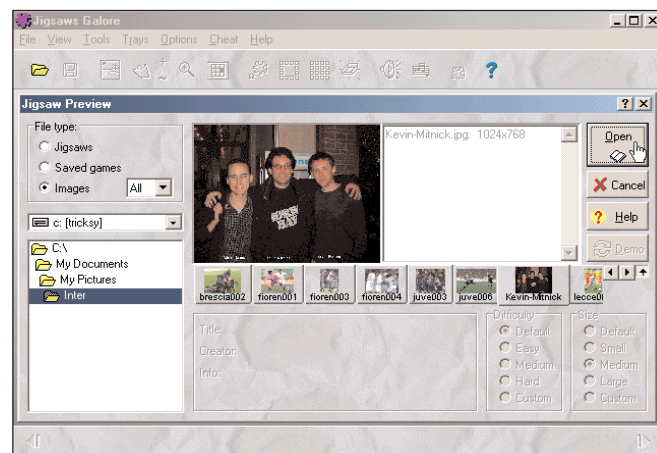
Program yang akan kita gunakan untuk membuat puzzle bernama **Jigsaws Galore v4.2**, yang diciptakan David P. Gray tahun 1996. Jika anda berminat menggunakan program tersebut, anda bisa menginstalnya langsung dari CD NeoTek yang disertakan dalam majalah ini, atau downloadnya dari:

- www.dgray.com
- www16.brinkster.com/erytricksy/Software/jigsaw_v42.zip

Proses Pembuatan Puzzle

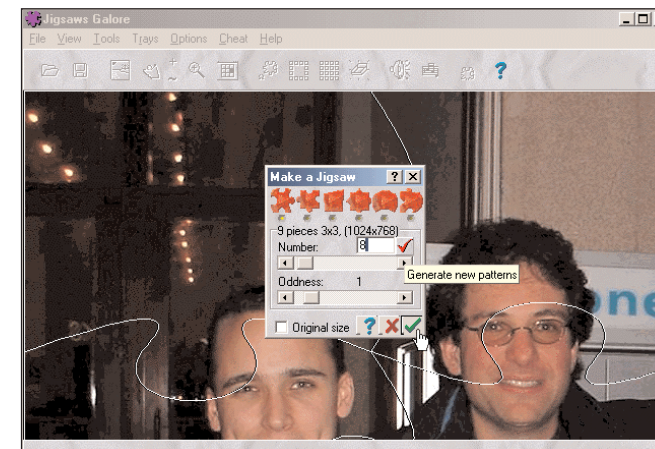
Untuk membuat *puzzle* elektronik, yang pertama-tama anda lakukan adalah menyediakan beberapa gambar, yang tentunya menurut anda cukup menarik dan cocok dijadikan puzzle. Namun jika stok gambar anda tidak begitu lengkap atau menarik, program Jigsaws Galore juga menyertakan beberapa gambar yang bisa anda pilih untuk dijadikan puzzle. Adapun format file gambar yang didukung oleh program Jigsaws Galore untuk dijadikan puzzle antara lain adalah BMP, JPG, PCX, TGA, WME, EMF.

Nah, setelah anda berhasil menemukan/mengumpulkan gambar-gambar, maka sekarang kita akan membuatnya sebagai puzzle. Proses pembuatannya sangat gampang, caranya adalah sebagai berikut:



- Menentukan folder/direktori gambar.

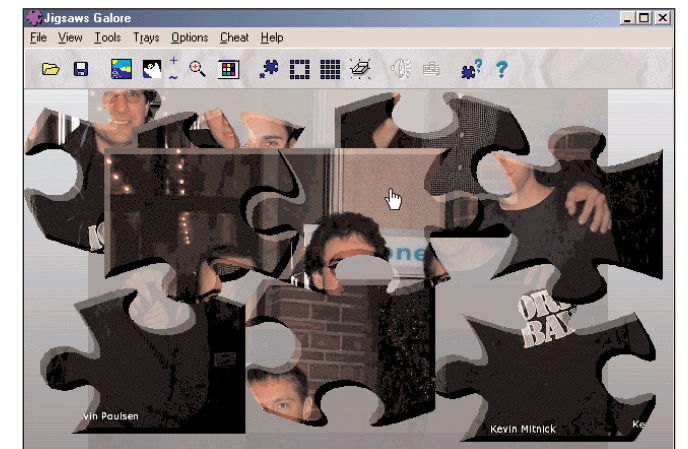
1. Jalankan program Jigsaws Galore.
2. Dari jendela Jigsaws Preview (File → Open), pada bagian "File type," pilih "Images." Kemudian tentukan nama *folder* atau direktori tempat anda akan menyimpan file-file gambar anda.
3. Setelah gambar di-load ke dalam mode Preview, klik tombol "Open," sesaat kemudian akan muncul jendela "Make a jigsaw."
4. Pada jendela "Make a jigsaw," pilih model atau bentuk potongan gambar yang anda inginkan. Model atau bentuk-potongan gambar yang bisa dipilih adalah: Classic, Blip, Squares, Stars, Bubbleless, dan Mixture. Kemudian tentukan berapa banyak gambar yang akan anda potong (*cut*). Banyaknya potongan gambar yang diizinkan adalah berkisar antara 4 sampai 16 potong. Dan setelah itu tentukanlah tingkat ketidakteraturan (*Oddness*) potongan-potongan gambar tersebut. Tingkat ketidakteraturan gambar yang diizinkan untuk kita set ialah mulai 0 hingga 10.



- Memilih model potongan, tingkat kesulitan, dan ketakteraturan puzzle.

5. Setelah selesai, simpanlah puzzle tersebut dengan mengklik "Save jigsaw." Namun sebelum anda menyimpannya, program akan meminta anda untuk membuat terlebih dahulu deskripsi tentang puzzle yang baru saja anda ciptakan tadi. Beberapa deskripsi yang dapat anda isikan ke dalam puzzle tersebut antara lain adalah: Title, Creator). Selain itu anda juga bisa memasukkan komentar anda sendiri pada field "Description." Setelah selesai, klik tombol OK, lalu simpan file tersebut ke dalam folder atau direktori yang anda inginkan.
6. Selamat! Puzzle sudah jadi. Untuk memainkan puzzle tersebut, caranya adalah sebagai berikut:

- Klik menu File → Open. Kemudian pada jendela Jigsaw Preview, pilih Jigsaws.



- Puzzle yang siap untuk dimainkan.

- Kemudian tentukan nama folder atau direktori tempat anda menyimpan puzzle yang tadi anda buat. Beberapa saat kemudian anda akan segera melihat gambar puzzle yang siap untuk anda mainkan. Sebelum anda mengklik tombol "Open," pilihlah tingkat kesulitan yang sesuai dengan keinginan anda. Misalnya, tingkat Default, Easy, Medium, Hard, atau Custom, dan termasuk ukuran potongan masing-masing gambar.
- Klik tombol "Open." Nah, sekarang cobalah susun potongan-potongan puzzle tersebut hingga menjadi gambar utuh. Jika anda berhasil, anda akan mendapat ucapan selamat dari Jigsaws Galore.

Apabila ada pertanyaan mengenai artikel ini, penulis dapat dihubungi di ery@postmaster.co.uk

Iklan visionnet
17,6 x 12,3