

Anti-Trojan 5.5

(bukan cuma file scan)



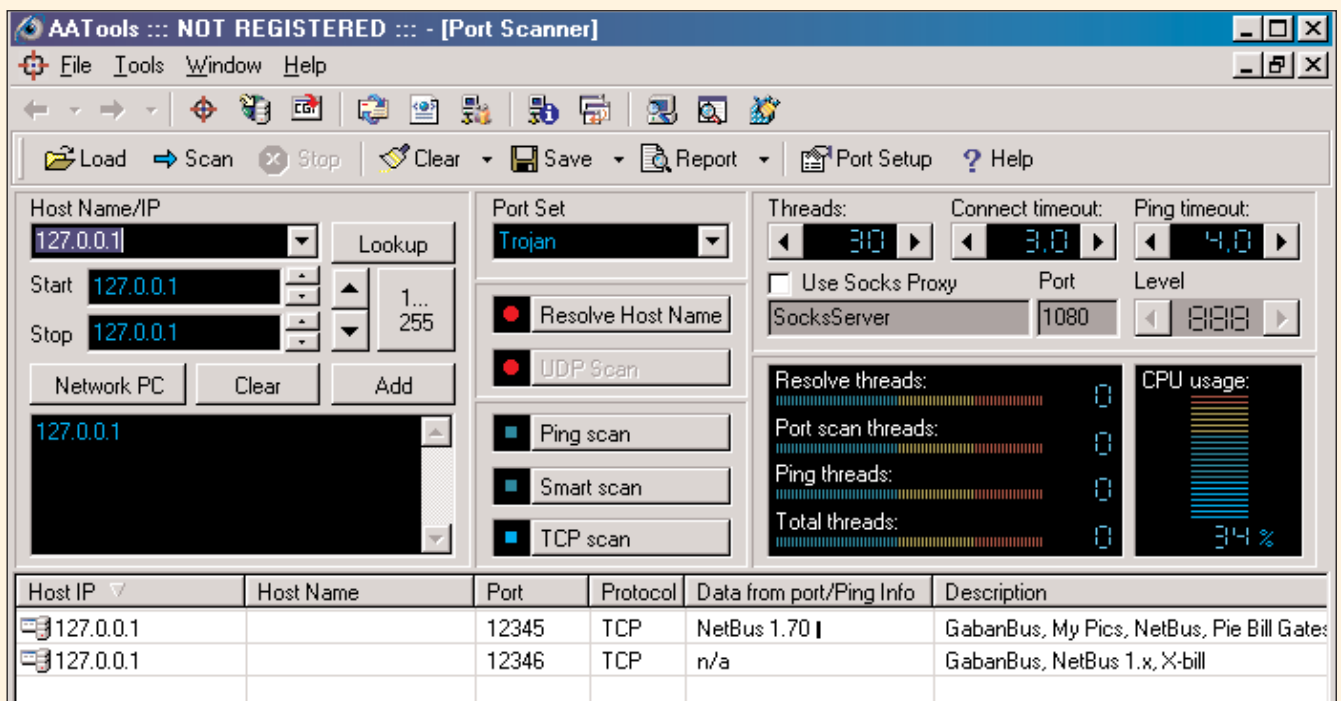
Scan Port dan Registry

Trojan sesuai fungsinya akan membuka pintu belakang berupa port pada nomor tertentu. Adanya port dengan nomor tidak lazim yang terbuka mengindikasikan adanya kegiatan aktif trojan.

Informasi mengenai port-port yang lazim digunakan oleh pelbagai macam trojan dapat diperoleh di situs GLock software:

<http://www.glocksoft.com>

Adanya trojan memang tidak membawa masalah langsung seperti halnya virus, namun potensi bahayanya dapat jauh lebih besar. Bagaimana tidak bila penyusup dapat melakukan hard disk anda seperti miliknya sendiri: termasuk memformatnya!



AATools menyediakan fasilitas port scan khusus untuk port-port yang umum digunakan oleh trojan. Pada contoh di atas ditunjukkan adanya kegiatan trojan NetBus 1.70 di komputer lokal (127.0.0.1) yang mengaktifkan port nomor 12345.

NEOTEK

Pendamping Berselancar
www.neotek.co.id

Daripada anda men-download...

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

- Walrus Macro Virus Gen
- VB Morm Generator
- NetBus 2.0
- Anti Klez
- McAfee Virus Scan
- Protect X
- @Guard
- PC Spy
- Cookie Pal
- iCQ Password Grabber
- Port Sentry
- SMB Scanner

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

Majalah + CD Rp19.500
CD saja Rp15.000

Hubungi

Bagian Sirkulasi

Majalah NeoTek

Tel. (021) 548 1457

Faks. (021) 532 9041

email:

pemasaran@neotek.co.id

Kontak: Elvi R. Nainggolan

PENAWARAN KHUSUS

Dapatkan koleksi 8 CD NeoTek

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

Dengan harga Rp95.000,-

Salam!

Virus merajalela tidak menjadi masalah jika tahu menangkalnya.



• Kisah epik kuda Troya yang dikirim oleh bangsa Yunani untuk menyusupkan pasukannya ke kota Troya telah mengilhami hacker untuk menciptakan 'penyusup' ke komputer orang lain. Maka terciptalah yang namanya Trojan Horse.

Virus komputer, terlepas dari efeknya terhadap para pengguna komputer, adalah juga hasil reka kreatif yang dalam perkembangannya jadi tidak terkendalikan. Maka jika anda intensif menggunakan komputer, dapat dikatakan anda wajib mempelajarinya dan mengetahui 'mahluk' yang seringkali merugikan para pengguna komputer ini.

Pada nomor ini NeoTek menggelar informasi mengenai virus komputer. Isinya bukan hanya pengetahuan mengenai apakah itu virus, apakah itu Trojan Horse, tetapi juga cara menggunakan, membuat dan menangkalnya. Dengan demikian, kami berharap anda mempunyai bekal yang cukup lengkap untuk menghadapi 'mahluk' merepotkan 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

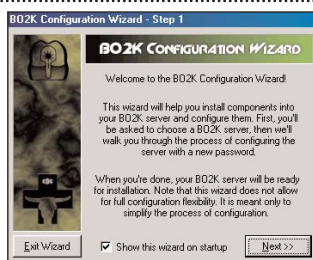
Gedung Cahaya Palmerah Suite 506
Jl. Palmerah Utara III No. 9
Jakarta 11480

Daftar Isi

NeoTek Vol. II No. 11

NeoStart

- 7 Registry Tweak**
Gunakan Windows Registry Guide agar mahir nge-tweak



- 8 Virus Komputer**
Mengetahui bermacam-macam virus, penyebaran, dan cara kerjanya. Mencakup juga trojan.

- 16 Trojan Horse**
Bagaimana umumnya serangan trojan terjadi? Dibahas pula tiga trojan populer yang ganas.

- 19 Infeksi Digital**
Bagaimana melindungi PC anda dari virus dan trojan? Selain dengan tools, juga harus disiplin.

NeoTutor

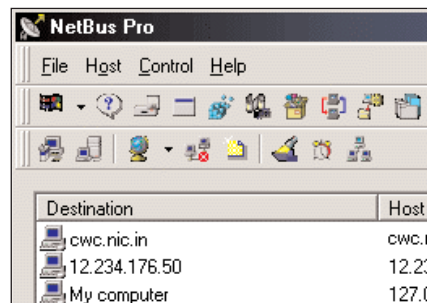
- 10 Membasmi Virus**
Gunakan dua antivirus free-ware yang tidak kalah ampuhnya: AVG Antivirus dan Antivir

- 12 Membuat Virus Macro**
Kini anda dapat dengan mudah membuat virus macro sendiri dengan Walrus Macro Virus Generator.

- 14 Visual Basic Worm**
Worm instan yang dapat anda buat dengan mudah ini sama berbahayanya dengan worm lain yang berkeliaran di Internet.

- 20 Trojan Pilihan: NetBus**
Setelah Back Orifice, kali ini diperkenalkan trojan serba-bisa lain yang telah berevolusi sampai versi NetBus Pro 2.10.

- 23 Trojan untuk Hacking**
Gunakan NetBus 1.70 untuk melakukan hacking dengan mudah terhadap komputer terinfeksi.



- 32 Program Siluman**
Anda suka chat dan belakangan ini komputer anda agak aneh?

Bagaimana mengenali adanya program siluman seperti trojan di komputer anda?

- 37 Menjalankan Program Setiap Kali Start**

Trojan dan program-program siluman lain sering kali ikut dijalankan sewaktu kita men-start komputer. Bagaimana hal itu dapat terjadi?

- 38 JavaScript: Percabangan**
Tutorial JavaScript bagian empat yang membahas alur logika bersyarat pada JavaScript.

- 40 PGPFreeware 7.0.3**

Pahami konsep gembok dan kunci pada konsep enkripsi dengan contoh langkah demi langkah yang jelas.



- 42 PGPFreeware 7.0.3: Impor Keyring & Email**

Penerima 'gembok' dapat mengirimkan email terenkripsi kepada pengirim 'gembok' dengan pop mail client seperti Outlook, Outlook Express, ataupun Eudora.

- 44 PGPFreeware 7.0.3: Aplikasi Web Mail**

Dengan PGPTay, bukan hanya pop mail yang dapat memanfaatkan enkripsi, melainkan juga web mail maupun file attachment.

Situs NeoTek

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

Jadikan situs NeoTek sebagai pangkalan Anda berselancar

Link Langsung

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

NeoTek versi PDF

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

Download

Tersedia juga download di situs NeoTek selain dari situs aslinya

Layanan Rupa-rupa NeoTek

Dapatkan perlengkapan awal dalam berinternet dari situs web NeoTek HumanClick

Hotline langsung ke redaksi NeoTek untuk menyampaikan saran dan pesan.

Chat Room

Kini tidak usah jauh-jauh untuk ngobrol langsung dengan sesama NeoTeker Mailing List

Ini yang paling ramai. Segera ikutan berbagi pengalaman berinternet!

FOKUS BULAN INI

Infeksi Digital: Virus dan Trojan

NeoTekno



24 Mendeteksi Penyusup dengan Snort

Network-based Intrusion Detection System (IDS) seperti Snort ini lebih aktif melacak penyusup dibandingkan firewall yang sifatnya pasif.

28 Snort dan IDScenter

Kini instalasi IDS pada Windows menjadi sangat mudah dengan menggunakan IDScenter, interface grafis untuk Snort.

30 PortSentry: Menjaga Serangan Port Scan

Bila IDS memonitor paket data pada jaringan, maka PortSentry menjaga port-port tertentu yang memang dijaga.

Inbox

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

NeoRagam

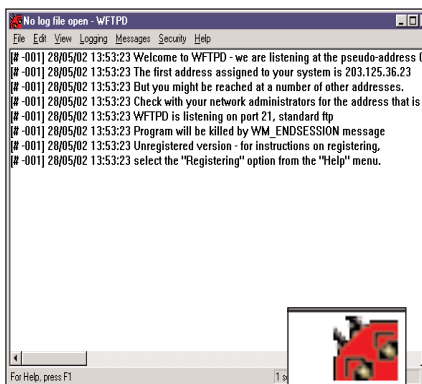
- 4** Ada Apa di CD NeoTek?
PC Security
Enkripsi Menjaga Privasi Anda
Terdeteksi Sebagai Virus

- 5** Daftar Isi CD NeoTek

NeoEdu

46 FTP Server wFTPD

Kesulitan mentransfer file-file besar yang diperlukan dalam proses belajar-mengajar? Pasang sendiri FTP server untuk kepentingan internal. Namun jangan lupa menyeting security-nya agar tidak diganggu tangan-tangan jahil.



48 NetBeans, FSL, OpenUSS

Proses belajar-mengajar dengan memanfaatkan NetBeans untuk menyiapkan bahan pengajaran.

NeoTek September 2002

Password Cracking

Password dapat dengan mudah dicuri dengan tool yang ada di Internet. Password yang kuat pun dapat dibuka dengan brute force attack.

PHP dan PostNuke

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

Tip & Trick Outlook Express

Sudahkan anda memanfaatkan sepenuhnya fitur-fitur yang ada pada email client yang populer ini?

Daftar Isi

NeoSoft

0 Anti-Trojan 5.5

Memang antivirus dapat untuk mendeteksi trojan, tetapi dengan antr-trojan yang di-sac termasuk juga port yang terbuka.

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 Widianto

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
Agustus 2002



Karena terfokus pada keamanan PC (*PC security*), maka CD NeoTek kali ini dapat dikatakan 'lengkap' untuk keperluan pengamanan PC secara umum. Untuk memahami cara kerja rekan yang usil (*local attack*), disediakan BIOS password decoder, screen saver password stealer, dan cache password eavesdropper, yang dapat diatasi dengan **PassKeeper**.

Akses ke Internet membuka ancaman baru baik berupa virus dan trojan maupun ancaman terhadap privasi anda. Selain virus dan trojan serta antinya, disediakan penangkal berupa **firewall** maupun **virtual sandbox** untuk menguji program yang belum dikenal.

Untuk menghadapi serangan hacker disediakan **IDS** (*intrusion detection system*) baik yang network-based maupun host-based.

Pahami juga cara hacker menghindari dari pengamanan 'radar' IDS dengan **packet fragmenter** seperti FragRouter maupun **CGI evasion** seperti Whisker dan SideStep.

Untuk tujuan pendidikan disajikan juga pelbagai **server** yang amat mudah digunakan, baik itu FTP, SMTP, maupun web server.

Kali ini CD NeoTek terfokus pada **keamanan PC** anda, baik secara **stand alone** maupun terhubung ke **network** dan **Internet**. Selain membahas ancaman yang ada, juga disajikan cara menanggulangnya.

PC SECURITY

Security Level 1: Local Attack

Amankan PC anda dari rekan kerja yang iseng atau ceroboh:

- ▶ **AMI BIOS Decoder**
- ▶ **Award BIOS PassCalc**

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

- ▶ **Screen Saver Password**
- Perlindungan berikutnya adalah screen saver password yang dapat pula diatasi dengan Screen Saver Password Recovery

- ▶ **SnadBoy's Revelation**
- ▶ **Password Recovery**
- ▶ **PWL View**

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

- ▶ **PassKeeper**

Manfaatkan PassKeeper sebagai *master key* untuk semua password yang ada di komputer anda.

Security Level 2: Bahaya Internet

Selain dengan men-set *security feature* pada browser anda, lindungi juga komputer anda dari virus dan trojan.

- ▶ **AntiVir**
- ▶ **AVG AntiVirus**

Dua antivirus versi freeware yang efektif melindungi komputer anda dengan fasilitas *guard*.

- ▶ **AntiTrojan 5.5**
- ▶ **NetCommando**
- ▶ **Cleaner 3**
- ▶ **LockDown 2000**

Berbeda dengan anti-virus, anti-trojan men-scan juga port yang terbuka serta mengecek registry untuk memeriksa adanya kegiatan trojan.

- ▶ **eSafe**

Software ini bukan sekedar *firewall*, melainkan juga anti-virus dan anti-trojan yang mempunyai fasilitas *sandbox* untuk menguji program yang belum jelas keamanannya.

Security Level 3: Hacker Attack

Dengan begitu mudahnya informasi dan hacking tool diperoleh, semua orang dapat menjadi penyusup (*intruder*) ke komputer anda. Jaman *hacker* yang digambarkan sebagai *computer nerds* sudah lewat. Kini hacking sudah menjadi kegiatan favorit untuk melewatkan waktu luang.

- ▶ **ZoneAlarm 2.6**
- ▶ **Protect X**
- ▶ **BlackICE 3.0 Defender**
- ▶ **Snort dan IDSCenter**

Firewall sederhana seperti ZoneAlarm sudah memadai untuk mencegah penyusupan. Atau gunakan *hacker security suite* seperti Protect X atau network-based IDS seperti BlackICE atau Snort. Semuanya tersedia pada Windows.

- ▶ **Salus**
- ▶ **PC Spy**

Monitor PC anda terhadap adanya kegiatan yang mencurigakan.

ENKRIPSI: MENJAGA PRIVASI ANDA

Melanjutkan pengenalan tentang enkripsi, kali ini disajikan PGPFreeware dan Streganos Suite sebagai dua metode enkripsi.

▶ PGPFreeware

Tool enkripsi paling populer karya Phil Zimmerman yang dapat merupakan plug-in pada Outlook, OE, dan Eudora, maupun dipakai tersendiri untuk web mail dan enkripsi file.

▶ Streganos 3 Suite

Berbeda dengan PGPFreeware yang mengenkripsi file menjadi teks acak, maka streganografi men-enkripsi teks dengan menyembunyikannya pada file gambar atau suara.

Berikut adalah public key milik kosasih@indo.net.id. Tolong kirim file yang telah dienkripsi.
Salam,
kosasih@indo.net.id
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPFreeware 7.0.3 for non-cc
<<http://www.pgp.com>>

```
mQG1BDzwgEKRBDTS3S4inhv1rJq9Fb8GzOC:
jvdIauL7FFOnNKQsdfzIqV0W0yTQ5792o6E+
B54XgBUw+YzeQTkyxRz/ldRmRSqh26adUhw
ISguac+JTGxy38UzKjW+xeUD/RklorF5XL+g
7nVdR40OuFHzwIFwQe1Q6bcwyCfc548dXDzz:
```

• Enkripsi dengan PGPFreeware



File .BMP sebelum disisipkan teks



Setelah disisipkan teks. Tak tampak bedanya, hanya diketahui dari tanggal file creation

• Enkripsi dengan streganografi

Terdeteksi Sebagai Virus

Pada CD NeoTek kali ini ada beberapa program yang akan terdeteksi sebagai virus bila menggunakan anti-virus. Hal ini biasa sebab trojan memang dimonitor oleh anti-virus. Juga terdapat VB Worm Generator yang juga dianggap sebagai virus. Berikut file-file yang dianggap berbahaya:

- bo2k_1_0-full.exe
- dv1.zip
- NetBus170.zip
- netbus20.zip
- nb2pro.zip
- s7a.zip
- sub7_server_2.zip
- sub7_1_8.zip
- vbswg200b.zip
- vbswg200f.zip

daftar isi cd neotek

SCRIPTING & SERVER

| | |
|-------------------------|----------|
| JavaScript Editor 2.5 | jse2em |
| Mdaemon (mail server) | mdsetup |
| PWS (web server) | setup |
| Sambar 5.0 (web server) | sambar50 |
| wFTPD (FTP server) | 32wfd310 |
| WinGate (mail server) | wgsetup |
| WinSMTP (mail server) | sts07b4 |
| Xitami (web server) | bw3224d9 |

VIRUS & TROJAN

| | |
|-----------------------------|---------------|
| Walrus Macro Virus Gen | wmvg |
| VB Worm Generator 2.0b | vbswg200b |
| VB Worm Generator 2.0f | vbswg200bf |
| Back Orifice (trojan) | bo |
| Back Orifice 2000 (trojan) | bo2k_1_0_full |
| DeepThroat (trojan) | dtv1 |
| NetBus 1.70 (trojan) | netbus170 |
| NetBus 2.0 (trojan) | netbus20 |
| NetBus 2.0 Pro (trojan) | nb2pro |
| NetBus 2.0 Pro Reg (trojan) | nbpro20breg |
| SubSeven | s7a |
| SubSeven Update | sub7_server_2 |
| SubSeven 1.8 | sub7_1_8 |

ANTI VIRUS

| | |
|------------------------|------------------|
| Anti Klez | AntiKlez |
| Anti MyParty | AntiMyparty |
| AntiVir | avwin9xp |
| AVG Anti Virus | avg6362fu |
| F-CIH | f-cih |
| Fix CIH | fix-cih |
| McAfee Virus Scan 6.02 | McAfeeVscan6_0_2 |
| McAfee Virus Upgrade | McAfeeVSupgrade |
| Norton Anti Virus 2002 | setup |
| Panda Titanium 2 | PandaTitanium2 |
| PC Cillin 2000 | pc2k |

ANTI TROJAN

| | |
|------------------|--------------|
| Anti Trojan 5.5 | AntiTrojan55 |
| Cleaner 3 | cleaner3 |
| Net Commando | NCLINST |
| LockDown 2000 | Lockdown2000 |
| Jammer (anti BO) | jammer |
| NetBus Detective | Detect52 |

FIREWALL

| | |
|----------------|-------------|
| Zone Alarm 2.6 | zonalnm26 |
| @Guard | atgd322u |
| IFW 2000 | ifq21s |
| ConSeal | cpf9x209 |
| eSafe | esd31b36 |
| Protect X | protectxstd |

NETWORK SECURITY

| | |
|----------------------------|-----------|
| Black Ice 3.0 (evaluation) | Defeval |
| Essential Net Tools | ent3 |
| Salus | Salus |
| PC Spy | PCSpy |
| Scotty WinPatrol | wpsetup |
| Anti Sniff 1021 | as-1021 |
| Cookie Pal | CookiePal |
| WinDump | WinDump |

LOCAL SECURITY

| | |
|--------------------------|-------------------|
| AMI BIOS Decoder | amidecod |
| Award BIOS PassCac | aw |
| Folder Guard | fg95 |
| Pass Keeper | PassKeeper |
| TweakUI | tweakui |
| Handy Backup | HandyBackup3_0 |
| Password Recovery | PasswordRecovery |
| PWL View | Pwlview1 |
| iCQ Password Grabber | iCQ pwGrabber |
| Screen Saver Password | sspwrecovery_demo |
| Snadboys Revelation | RevelationV2 |
| AATools Registry Cleaner | aatools |

NETWORK-BASED IDS FOR LINUX

| | |
|-------------------------|--------------------------------------|
| Snort 1.8.6 Linux | snort-1.8.6.tar.gz |
| Snort User Manual | snort.pdf |
| Analysis Console for ID | acid-0.9.6b21tar.gz |
| ADO Database Linux | adodb200 |
| Apache Server Linux | httpd-2.0.36.tar.gz |
| Log Snorter Linux | logsnorter-0.2.tar.gz |
| MySQL RedHat | MySQL-3.23.49a-1.i386.rpm |
| MySQL tarball | mysql-3.23.49a-pc-linux-gnu-i686.tar |
| MySQL Cygwin | cygwin-1.3.9-1.tar.gz |
| PHP 4.21 Source | php-4.2.1.tar.bz2 |
| PHP Plot Linux | phplot-4.4.6.tar.gz |
| Postgre SQL tarball | postgresql-7.2.1.tar.gz |
| Postgre SQL Mandrake | postgresql-7.2.1-2PGDG.i586.rpm |
| Postgre SQL RedHat | postgresql-7.2.1-2PGDG.i386.rpm |
| Shoki tarball | shoki-0.1.2.tar.gz |
| Tamandua tarball | tamandua_gpl-1.0.tar.gz |

NETWORK-BASED IDS FOR WINDOWS

| | |
|-----------------------|---------------------------|
| Snort 1.7 Windows | snort-1.7-win32-static |
| Snort 1.8.3 Windows | snort_1.8.3_win32_release |
| Win PCap | WinPcap_2_3 |
| IDS Center 1.08 | idscenter |
| ADO Database Windows | adodb200 |
| Apache Server Windows | httpd-2.0.36.win32 |
| MySQL Windows | mysql-3.23.49-win |
| PHP 4.21 Windows | php-4.2.1.win32 |
| Postgre SQL Windows | psqlodbc-07_02_0001 |
| SolarWinds Std Ed Eva | SolarWinds2001-SE-Eval |

HOST-BASED IDS (LINUX)

| | |
|------------------|-----------------------------|
| Port Sentry 1.1 | portsentry-1.1.tar.gz |
| Port Sentry 2.0 | portsentry-2.0b1.tar.gz |
| Log Sentry 1.1.1 | logsentry-1.1.1.tar.gz |
| Host Sentry | hostsentry-0.02.tar.gz |
| AIDE 0.8 | aide-0.8.tar.gz |
| Hummer 3.4 | Hummer_3_4_bin |
| IDA | ida-plugin0.82.tar.gz |
| LIDS | lids-0.11.0r2-2.2.20.tar.gz |
| Shadow | SHADOW-1.7.tar.gz |
| Tripwire tarball | tripwire-2.3-47.bin.tar.gz |
| Tripwire RedHat | tripwire-2.3-47.i386.tar.gz |

IDS EVASION

| | |
|------------------------|------------------------|
| FragRouter 1.2 Linux | fragroute-1.2.tar.gz |
| FragRouter 1.6 Linux | fragrouter-1.6.tar.gz |
| Library for FragRouter | libpcap-0.7.1.tar.gz |
| Nikto 1.1.0 Linux | nikto-1.1BETA3.tar.gz |
| Whisker Linux | whisker-2.0.tar.gz |
| Nessus 1.3.3 Windows | nessuswx-1.3.3-install |
| Side Step Windows | sidestep |
| ZCGI Scan Windows | zcgiscan |

ENKRIPSI

| | |
|--------------------|-------------------|
| PGPFreeware 7.0.3 | PGPF703 |
| Sreganos Suite | streganos3suite |
| Private Idaho | PrivatIdoho |
| Stealth Anonymizer | StealthAnonymizer |

NETBIOS SCANNER

| | |
|---------------|-------------|
| Shares Finder | Find shares |
| SMB Scanner | SMB Scanner |
| Legion | legion |

TOOLS & LIBRARY

| | |
|---------------------------|---------------------|
| DivX 4.12 Bundle | DivX412Bundle |
| DirectX 8.1 | DirectX8_1 |
| WinDissassembler | Windis |
| WS_FTP LE | ws_ftple |
| POPmail | Popmail |
| Visual Basic Runtime 5.0 | vbrun500 |
| Visual Route | vr |
| NeoTrace 325 Trial | NeoTraceProTrial325 |
| Teleport Pro | pro12 |
| Norton Utilities 2002 | Nu2002 |
| LapLink Technical | Setup |
| mIRC 6.01 | mirc601 |
| GIF Animation Collections | |



NmN

NeoTeker menjawab NeoTeker

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

Konflik IRQ

T: Posted July 1

Saya ingin tanya bagaimana membagi atau menentukan IRQ agar tidak konflik. Saya pake Win2000-server. Saya liat di System yang konflik yaitu Micro-soft ACPI-Compliance System. VGA Card, Sound Card, Lan Card, USB PCI Controller yg semuanya memakai IRQ 9. Mobo saya Asus.

Wendy
w.tech@hotmail.com

J: Posted July 1

Settingnya di BIOS setup, di Advanced-PCI Configuration -> nah kelihatan kan? Slot 1 pake IRQ berapa, dst. Kalo kamu nggak pake perangkat USB, mending disable aja USB-nya.

Settingnya juga di Advanced dan Advanced-PCI Configuration-USB Function. Tujuan disable di sini supaya lebih hemat IRQ.

Resist Arie
resistarie@softhome.net

T: Posted July 1

1. Saya pernah instal WinXP pro terus semua hardware terdeteksi kecuali Modem Motorola sm56 speakerphone. Apa ada driver khusus modem tsb untuk winxp pro? Kalo ada yang tau tolong dong saya harus download dimana? Kalo pake winxp home bisa ngga?

2. Rekan2 ada yang tau softwarenya gratis buat sms ke handphone? kecuali icq, download dimana?

Dreamer Boyz
rscript@telkom.net

J: Posted July 1

Cobain ke mtsn.com atau sms.ac tapi sehari cuma dapet 5 free. Bikin aja ID banyak-banyak. Tapi pengalamannya saya sih ICQ is the best.

Shamdi
shamdi@stelab.nagoya-u.ac.jp

J: Posted July 1

Kenapa nggak cobain Istwap sehari bisa 25x
www.1stwap.com

Ban Rachmat
Rahmatn@oto.co.id

J: Posted July 2

Daripada itu mending make <http://www.1stwap.com/parters/go.to/1stwap> atau <http://www.1stwap.com/parters/go.to/gsm-club> cuman ya itu harus regis dulu n' ada no hp soale confirm regisnya dikirim lewat sms daripada sms.ac ini lebih cepetan tapi skr dibatesi 15 sms/minggu.

Agus Budi
agus_budi@yahoo.com

Ganti Nama Menu Start

T: Posted July 1

Ada yang tau gak cara ganti tulisan start di start menu tanpa melalui program bantu spt tweak ui. Jadi yang saya hendak tanyakan yaitu langkah-langkah mengganti tulisan tersebut melalui regedit.

Jiu Jujitsu
alberd@bdg.centrin.net.id

J: Posted July 3

Untuk masalah ini ada artikel yang saya tulis sendiri di NeoTek edisi April atau Mei 2002 atau aja situs Neotek dan <http://come.to/digitalworks> ada artikel pdf-nya.

Cakrabirawa
cakrabirawa@mail.ru

Format NTFS & FAT32

T: Posted July 2

Tolong terangin cara ngeformat system NTFS dong.

Gini, saya punya 2 harddisk, di Master dan di Slave. Yang master saya isi WIN XP (2 partisi, NTFS dan FAT32) danyang Slave saya isi WIN-2K (juga NTFS dan FAT32). Tapi saya sering make yang Slave untuk uprak oprek. Jadi yang Master saya matiin.

WIN2K NTFS yang di Slave saya format melalui WINXP. Terus saya mau instal WIN 98 di slave itu, kok drive C yang di Slave nggak kebaca yah, alias drive yang format NTFS itu, yang kebaca malah data yang tadinya di drive D yang format FAT32 itu. Jadi bingung deh saya. Tolong dong caranya ngeformat NTFS biar kebaca. Untung saya nggak langsung format di DOS-nya, kalo nggak kan data di D bisa ilang semua.

Gunwan
neotek@zapo.net

J: Posted July 2

Setahu saya kalo dari fat32 emang ndak isa baca ntfs jadi kalo di win98 emang ndak isa liat drive yang make ntfs. itu kayak'e emang gitu. Kelebihan dari sistem ntfs. ndak tau kalo emang bisa baca ntfs dari fat32 soale dari dulu aku nyoba ya ndak isa, kecuali itu antar komp di jaringan, itupun harus setting dulu.

Agus Budi
agus_budi@yahoo.com

J: Posted July 2

FAT32 nggak bisa baca NTFS kecuali pake software tambahan seperti dari www.sysinternals.com. Kalau

mau gampang, XP dan W2K ubah jadi FAT32 juga.

Albert Siagian
asiagian@gmx.net

J: Posted July 3

Cobain captain nemo deh... bisa buat baca ntfs maupun linux... search di Google.

Wahyu Budi
wbudi@satelindo.co.id

Dari Win 98 ke Win 95

T: Posted July 3

Kenapa yaah kalo komputer udah diinstal win 98 terus mao dibalikin instal win 95 selalu nggak bisa? Ada yang punya kiat mbalikin dari win 98 ke win 95.

Cakrabirawa
cakrabirawa@mail.ru

J: Posted July 2

Emang ndak isa, kalo aku dulu ya format ulang dulu setelah data2nya di pindah, karena sistem yang berjalan berlainan, sistem windows ndak isa baca versi yang lebih tinggi, gitchuuu.

Agus Budi
agus_budi2@yahoo.com

J: Posted July 3

Kalo anda upgrade Win95 ke Win98 maka saat instalasi Win98 akan diminta untuk men-SAVE win95 yang lama. Apabila kita gak jadi install win98 maka bisa diuninstall. Settingan makan tempat sekitar 50 MB. Tapi kalo anda install langsung Win98 atau saat diminta untuk save tsb dtidak di-save maka harus diformat tuh HD kalo mau install win95 (downgrade).

mbUdh
mbudh@centrin.net.id

MEN-TWEAK REGISTRY DENGAN WINDOWS REGISTRY GUIDE

Windows Registry Guide adalah tuntunan yang sangat berguna jika anda ingin belajar lebih jauh tentang cara *men-tweak* dan mengoptimalkan *registry* Windows anda. Di dalamnya tersimpan segudang tip dan trik, tetapi anda membutuhkan program lain untuk mengedit *registry* itu.

Windows Registry Guide sebenarnya adalah file Help Windows yang memberikan tip, trik, dan *tweak* untuk *registry* di Windows 95, 98, NT dan 2000.

Registry adalah basisdata yang digunakan untuk menyimpan setting dan opsi untuk Windows versi 32 bit. Basisdata ini berisi informasi dan setting untuk perangkat lunak, perangkat keras, pengguna, dan preferensi pada suatu PC. Setiap kali pengguna membuat perubahan di setting Control Panel, kaitan file, system policies, atau perangkat lunak yang diinstal, maka perubahan itu terekam dan disimpan di Registry Windows itu.

Mengais informasi di gudang arsip NeoTek

Windows Registry Guide 2002

Download Now
Free download 939K
Download options

Downloads:
Publisher:
Date added:
File size:
License:
Minimum req
Uninstaller in

Description
The Windows Registry Guide is a Windows 98, NT, and 2000 Registries. The Registry is Microsoft Windows. It contains information ar

le Install Program - Directory

Windows Registry Guide's files will be installed in the following directory:
C:\Program Files\WinGuides\Registry

Disk space needed : 1 Mb
Available disk space : 2048 Mb

Microsoft Access
Microsoft Excel
Microsoft FrontPage
Microsoft Outlook
Microsoft PowerPoint
Microsoft Word
Outlook Express
Windows Media Player
WinGuides

1

TEMPAT SANG GUIDE

Untuk mendapatkan **Windows Registry Guide 2002 (WRG)**, arahkan *browser* anda ke situs ZD Net di <http://downloads-zdnet.com.com/3000-2251-10027292.html>. Atau dapatkan di CD NeoTek bulan ini.

2

FOLDER TEMPAT INSTALASI

Setelah anda *men-download* file sebesar 939Kb ini dan menginstalnya, WRG akan ditempatkan di folder seperti tertera pada gambar di atas.

3

MEMANGGIL WRG

Untuk menjalankan WRG, klik tombol Start > Programs > WinGuides > Windows Registry Guide.

Windows Registry Guide 2002

Contents | Search | Favorites

Index Page
Hardware
Network
Security
Software
Tips and Tricks
Windows
WinGuides Home Page
WinGuides Tweak Manager
Book List
Support Forums
Newsletter
Download Updates
Subscribe

The Windows Registry Guide provides an extensive range of registry tips, tricks & tweaks for optimizing, enhancing and securing the Windows operating system. Get started by exploring the categorized tweaks below or visit us online at <http://www.winguides.com/>

Categories

Hardware
Hardware and Peripheral Enhancements

Software
Enhancements for Windows Applications

Network
Network and Connectivity Enhancements

Tips and Tricks
Windows Tips, Tricks and Shortcuts

Security
Security Restrictions and System Policies

Windows
Windows Operating System Enhancements

Documents and Resources

Disk Drives
Fixed and Removable Disk Drives

Input Devices
Mice, Keyboards and Joysticks

Modems and Communications
Modems, Fax and ISDN Enhancements

Registry tweaks, tricks & hacks to optimize Windows

Disable Print Job Notification in Event Viewer (Win98)
Category: Home > Hardware > Printers and Plotters
Download: WinGuides Tweak Manager

By default Windows NT server adds an entry in the event log which quickly fill up the event log with redundant information.

To disable this function, change the DWORD value for EventLog to 0.

Registry Editor Example

| Name | Type |
|--|-----------|
| (Default) | REG_SZ |
| EventLog | REG_DWORD |
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ | |

4

TAMPILAN PERTAMA WRG

Inilah tampilan pertama WRG yang penuh dengan tuntunan yang menarik seputar cara mengedit dan *men-tweak* *registry* Windows anda. Pada kolom kiri anda dapat menjumpai menu-menu yang berkaitan dengan pengoptimalan *registry*.

5

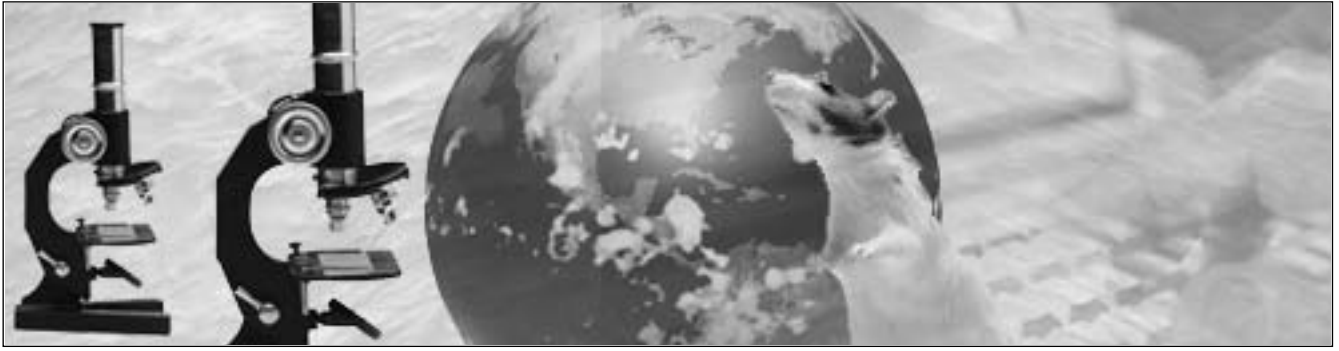
MENGATUR HARDWARE

Jika anda mengklik menu 'Hardware,' misalnya, maka kolom di sisi kanan akan berubah menampilkan beberapa hardware yang dapat anda atur cara kerjanya dengan *men-tweak* *registry*.

6

ISI 'PELAJARAN'

Jika anda mengklik link salah satu hardware, WRG akan menampilkan isi 'pelajaran' untuk *men-tweak* hardware bersangkutan, seperti contoh di atas. Uraian disertai contoh *screen shot* *registry* yang akan anda ubah.



Mengenal Infeksi Digital: Virus Komputer

Siapa yang tidak kenal virus? Sekarang virus telah menjadi bagian sehari-hari dalam berkomputer. **Odyxb** (odyxb@chat-plus.org) mencoba memberi penjelasan awal mengenai jenis dan cara kerja virus.

Anda yang telah terjun atau mengenal komputer tentu pernah mendengar tentang virus komputer. Hanya saja informasi mengenai virus komputer di Indonesia masih sangat kurang sekali, berbeda dengan di luar negeri seperti Amerika yang sudah mempunyai media massa khusus yang memuat informasi mengenai virus bahkan sampai pembuatan virus komputer itu. Lalu apa dampaknya terhadap kita yang di Indonesia? Kita hanya bisa menjadi penonton dan menjadi korban penyebaran virus komputer tanpa mampu menanggulangnya.

Virus komputer pertama kali dikemukakan oleh Dr. Fred Cohen melalui makalahnya pada seminar internasional mengenai keamanan komputer, 1984, di Universitas Cincinnati, USA, di Fakultas Teknik Elektro dan Komputer. Dan pada tahun 1989 beliau mengeluarkan program software antivirus yaitu "Advance System Protection" untuk platform PC, komputer, dan LAN.

Karakteristik

Seiring kemajuan zaman, virus komputer dalam perkembangannya juga mengalami kemajuan sehingga memiliki efek yang semakin mengerikan dengan sifat merusak. Beberapa karakteristik virus komputer itu adalah:

- Memiliki kemampuan untuk melakukan penulisan pada file-file eksekusi program secara ilegal.
- Dapat bergerak berpindah-pindah dari satu komputer yang satu ke komputer yang lain dengan menggunakan media yang dimiliki komputer itu sendiri; floppy disk, hardisk, dan cdrom. Bahkan juga dapat melalui e-mail atau melalui file hasil download melalui internet.
- Dapat melakukan fungsi ilegal; mengacaukan waktu, merusak, sukar dilacak, dan lain-lain.

Aturan Main Program

Virus komputer adalah program yang unik yang memiliki aturan main program, di antaranya berupa:

Check of Information

Dilakukan pada operasi baca-tulis pada media penyimpan; disket atau *hard disk*. Virus akan mengecek ukuran kapasitas media penyimpanan, jenis penyimpanan, proteksi yang ada pada media penyimpanan, panjang file/*boot sector*.

Check of Other Viruses

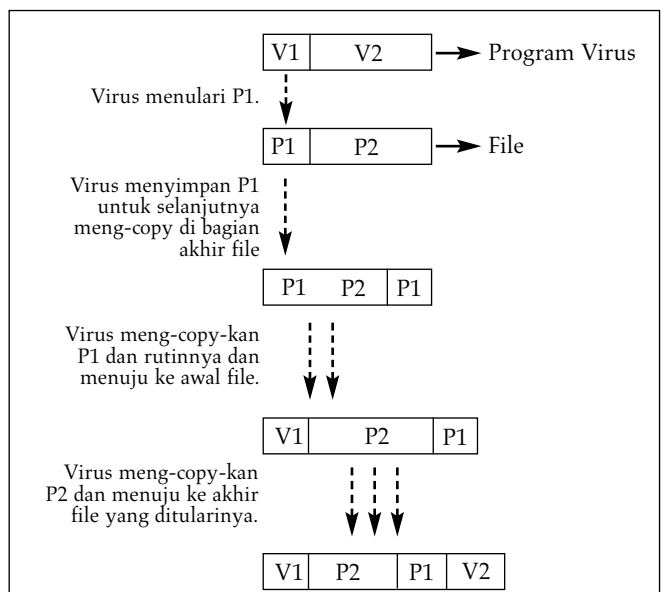
Memeriksa program virus yang lebih dahulu ada dan menyingkirkannya.

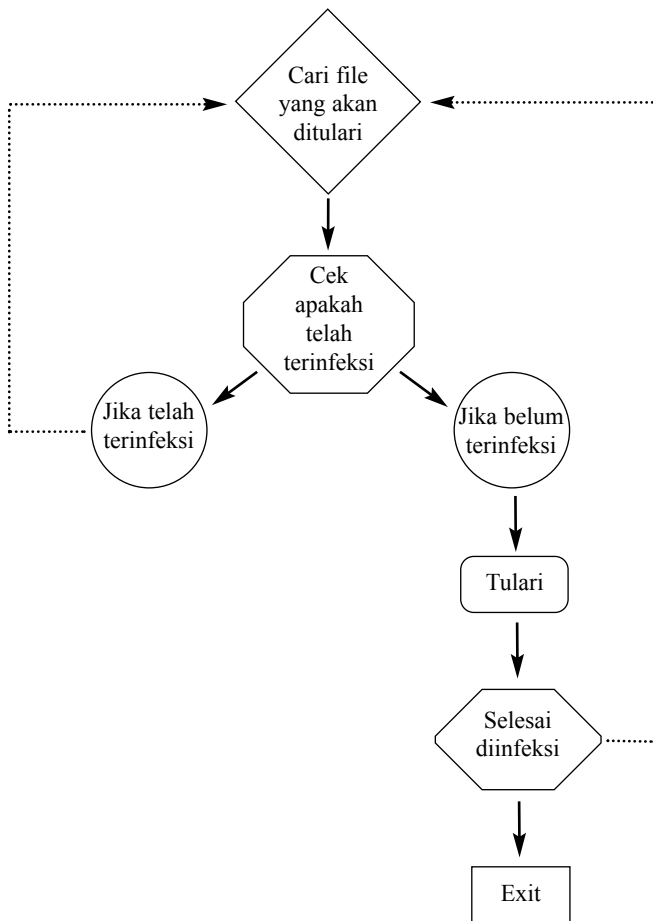
Interception

Menyusup pada media penyimpanan agar tidak terlacak atau terdeteksi oleh sistem.

Self Replicating/Self Duplicating

Menggandakan diri untuk membuat koloni-koloni baru untuk menunjang eksistensinya. Di sini virus komputer menggunakan karakteristik penulisan, seperti terlihat pada bagan di bawah ini.





• Langkah-langkah proses kerja virus untuk melakukan penularan secara umum

Stealth, Hidden, dan Manipulation

- *Stealth*, menghindari deteksi antivirus dan sekuriti komputer (menghilangkan jejak).
- *Hidden*, bersembunyi untuk menon-aktifkan dirinya untuk sementara jika eksistensinya terancam dan kembali melakukan aktivitasnya jika telah aman.
- *Manipulation*, memanipulasi atau memutasi diri jika virus ingin mengacaukan program pendeteksi seperti CHKDSK.COM, MEM.COM, atau file deteksi *hardware* dan *software* komputer lain.

Cara Kerja

Dalam melakukan operasi menyusupkan kode programnya, ada beberapa cara kerja virus komputer itu, yaitu:

Virus Overwriting Target File

Menindas file program eksekusi sasaran dan menggantinya dengan program virusnya.

Virus Non-Overwriting Target File

Kemampuan menyusup tanpa merusak program file sasaran, hanya memindahkan lokasi program asli dan menggantikan header program file target dengan programnya sendiri.

Virus Resident

Melakukan penularan dengan menggunakan memori RAM komputer. Virus akan bercokol di dalam memori sampai komputer dimatikan.

Virus Call and Document

Virus ini aktif pada program-program tertentu dengan jalan ditempelkan pada file dokumen untuk dieksekusi dengan menggunakan software pengolah kata. Contoh dari virus ini adalah virus Makro.

Virus Stealth

Ini merupakan virus yang sangat berbahaya karena memiliki kemampuan untuk *defense*, *stealth*, *interception*, *destroyer*, dan penularan yang mengagumkan. Sukar dideteksi karena dapat melakukan mutasi. Contoh virus ini adalah Diehard, Ambulan, dan virus Mutan Dark Avenger.

Virus Boot Sector

Virus ini berdiam pada *boot sector* media penyimpanan dan aktif saat dilakukan booting. Cara kerjanya adalah menempel pada sistem *booting* sehingga sulit dideteksi kehadirannya dan melakukan pembelokan alamat pada awal *booting*. Contoh virus ini adalah virus Have a Nice Day.

Bahasa, Compiler, dan Utilitas

- *Virus* komputer banyak dibuat dengan bahasa Assembly karena kekhasan, kemudahan, kecepatan, dan keefisiennya untuk operasi rutin virus komputer. Program virus komputer selalu melakukan akses langsung maupun tidak langsung terhadap *interrupt-interrupt* yang dapat dilakukan dengan menggunakan bahasa Assembly.
- *Compiler* yang digunakan untuk membuat virus, dapat digunakan Borland Turbo Assembler atau Microsoft Micro Assembler yang terbukti handal dalam mengkompilasi kode program virus.
- Utilitas lain yang dibutuhkan dalam membuat program virus adalah perangkat lunak manajemen memori seperti MEM.EXE, MAPMEM, PMAP, dan MARK RELEASE Software.

Tipe

Virus yang ada sekarang memiliki tiga tipe yaitu:

Virus Kecil

Ukurannya kecil, di bawah 500 byte. Kode-kodenya pendek dan dibuat begitu agar tidak mudah dideteksi.

Virus Besar

Ukurannya lebih dari 1500 byte, memiliki kode yang rumit yang memiliki teknik *stealth* atau menghilangkan jejak.

Virus Trojan

Virus ini meyebar melalui file-file yang di-copy secara ilegal.

Bagian Rutin

Program virus komputer memiliki 3 bagian rutin utama dalam menjalankan aksinya, yaitu :

Replikator

Menyebarkan virus ke seluruh sistem yang ditularinya tanpa menghancurkan file yang terinfeksi.

Pengaman

Melindungi virus dari pelacakan/pendektesian *scanning* antivirus. Salah satu cara yang digunakan pada program virus dalam menghindari deteksi adalah dengan teknik enkripsi.

Time Bomb

Waktu-waktu yang ditentukan dalam program virus untuk melakukan aksinya.

MEMBASMI VIRUS DENGAN ANTIVIR DAN AVG ANTIVIRUS

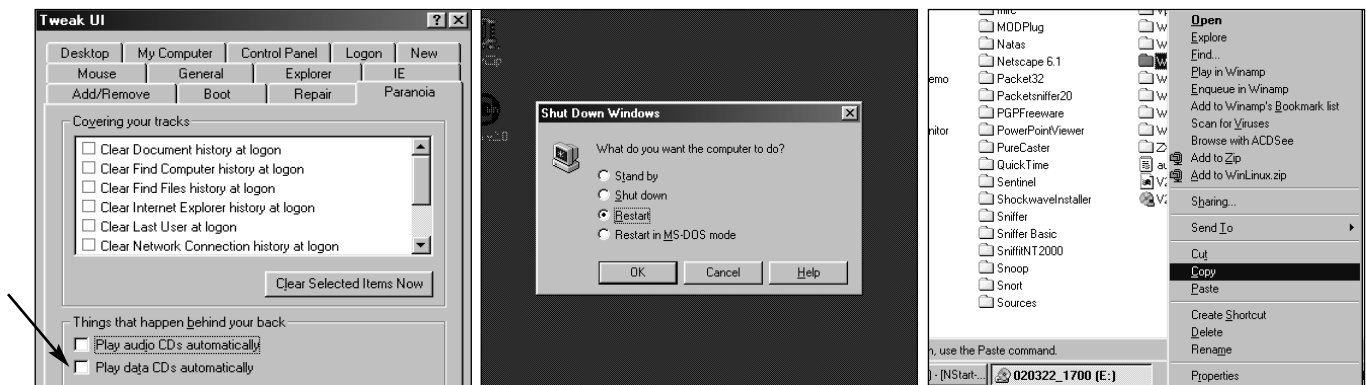
I Putu Edy Budiarsa punya kiat sendiri untuk membasmi virus yang menginfeksi file-file komputernya. Ikuti caranya yang mudah dipraktikkan dan *cespleng*.

CD NeoTek April 2002 betul-betul merupakan paket kejutan. Bagaimana tidak? Di CD tersebut *ngendon* seabrek virus CIH dan Trojan BackOrifice.

Peristiwa tidak sengaja tersebut bisa merupakan bencana, bisa pula merupakan hal yang menguntungkan tergantung dari sudut mana kita memandangnya.

Kejadian ini saya gunakan untuk belajar mengevaluasi beberapa antivirus yang tersedia secara cuma-cuma. Alhasil saya dapatkan dua pilihan karena keduanya berhasil mendeteksi jumlah dan jenis virus yang sama.

Cara mengatasi virus gaya Edy Budiarsa



1

PENGAMANAN AWAL

Jalankan TweakUI, pilih tab Paranoia. Hilangkan tanda cawang pada Play data CD automatically. Tujuannya agar tidak ada file yang terinfeksi yang dijalankan secara tidak sengaja. Instalasi TweakUI pernah dibahas di NeoTek Februari 2002.

2

BOOT KE SAVE MODE

Boot-lah komputer dalam safe mode. Sebelumnya jangan lupa menonaktifkan antivirus residen melalui menu Run, msconfig ataupun melalui menu yang disediakan.

3

COPY FILE YANG TERINFEKSI

Anda dapat membackup keseluruhan CD NeoTek, salin seluruh isinya ke folder tertentu di hard disk. Tapi jika ingin membersihkan program tertentu yang hendak Anda install maka program itu saja yang disalin. Hanya dicopy, jangan sekali-sekali dijalankan!

Mengintip 'Isi Perut' Virus dengan Debugger

Program virus yang ada dapat di-*debug* atau untuk melihat kode program sebuah virus, anda dapat menggunakan program TASM (Turbo Assembler) Debugger atau sejenisnya.

TASM Debugger Borland dapat anda download gratis dari www.borland.com/bcppbuilder/turbodebugger/

Untuk melakukan debug terhadap sebuah virus, terlebih dahulu cari file yang telah terjangkiti virus dan gunakan program debugger seperti di atas untuk melihat kode programnya.

Di bawah ini adalah contohnya. Kurang lebih seperti di bawah inilah sebuah virus yang di-debug untuk melihat kode programnya.

Kode program contoh ini adalah kode program The Funky Bob Ross Virus, tetapi tidak dalam kode lengkapnya.

```

traverse_fcn proc    near
    push    bp
    mov     bp,sp
    sub     sp,44
    call    infect_directory
    mov     ah,1Ah
    lea     cx,word ptr [bp-44]
    int     21h
    mov     ah,4Ah
    mov     cx,16
    lea     cx,[si+of fset_dir_mask] ; *.*
    int     21h
    jmp     short isdirk
gonow:
    cmp     byte ptr [bp-14], '.'
    je      short doneit
    lea     cx,word ptr [bp-14]
    mov     ah,3Ah

```


Antivirus tersebut adalah AVG Anti-Virus Free Edition dan AntiVir 9x Personal Edition. Keduanya bisa diperoleh cuma-cuma untuk kepentingan pribadi. (kedua antivirus ini tersedia pada CD NeoTek bulan ini).

Sebelum mengulas secara singkat kedua antivirus tersebut, inilah langkah-langkah penyelamatan yang penulis lakukan agar program-program dalam CD NeoTek tersebut bisa dimanfaatkan dengan baik dan steril.

Bagi yang berdomisili di Denpasar dan ingin memperoleh antivirus tersebut dapat menghubungi penulis di e_budiasa@mailpuppy.com

Catatan Redaksi:

CD NeoTek Vol. II No. 7, April 2002 itu sendiri telah ditarik dari peredaran dan diganti dengan edisi Revisi (ada tulisan 'Revisi' pada CD pengganti).

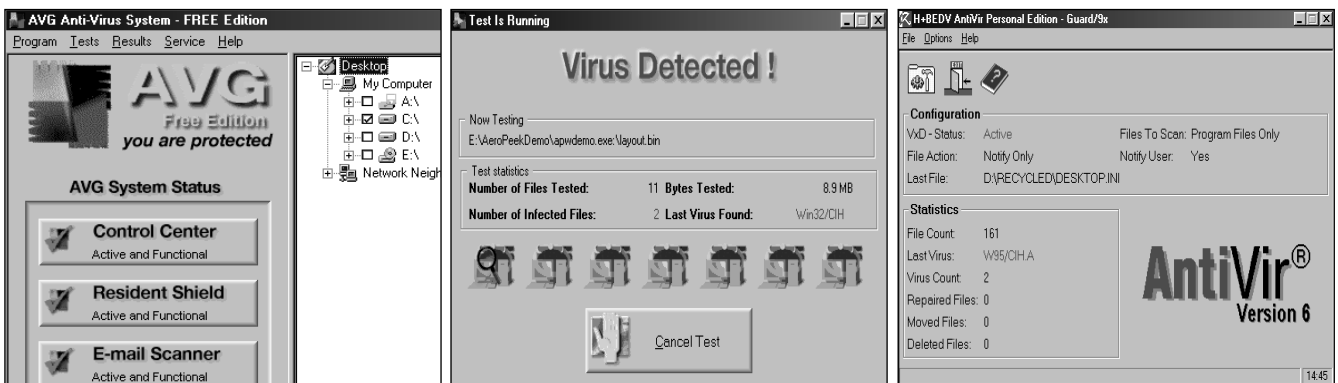
Sebelum sempat beredar luas, adanya virus pada CD NeoTek April 2002 sempat diketahui, segera ditarik, dan diganti dengan edisi Revisi. Namun ada saja kemungkinan CD yang bervirus terlanjur beredar.

Terima kasih atas kerja sama dari TB Gramedia serta rekan-rekan pada channel #neoteker di Dalnet yang ikut aktif mengatasi masalah ini.

Redaksi menganjurkan untuk sama sekali tidak menggunakan CD NeoTek edisi April 2002 yang bervirus. Apabila artikel ini hendak dipraktikkan, harap lakukan dengan sangat hati-hati.

Apabila anda masih belum mendapatkan CD pengganti, hubungi TB Gramedia terdekat untuk menukarkannya, atau email ke redaksi@neotek.co.id dan informasikan alamat pos anda. CD pengganti akan dikirim ke alamat anda tanpa biaya apapun.

NeoTek menyadari bahwa peristiwa ini dapat mengakibatkan bencana dan untuk itu kami mohon maaf yang sebesar-besarnya.



4

JALANKAN ANTIVIRUS

Kini aktifkan lagi antivirus yang bersifat residen (AVG atau AntiVir). Pada AVG Anti-Virus Free Edition: Pilih **Test, Custom Test, My Computer**. Berikan tanda cawang pada folder tempat program terinfeksi tersebut disimpan. Klik **Start** dan...

5

Hopla virus Win32/CIH-pun dilenyapkan. AVG bisa Anda download di www.grisoft.com Ukurannya sekitar 5 Mb. Jangan lupa mendownload updatenya sekalian, yang diperbaharui seminggu sekali. Daftarkan secara cuma-cuma dan untuk mendapatkan kode registrasinya.

6

ANTIVIR

Kemampuan antivirus buatan Jerman ini setara dengan AVG, dengan pilihan pengoperasian AVG lebih banyak, misalnya dapat men-scan folder tertentu saja. Antivir dan updatenya bisa diperoleh di www.free-av.com dan berukuran sekitar 4 Mb.

```

int     21h
jc      short dnext
inc     word ptr [si+of fset nest]
call    near ptr traverse_fcn
lea     dx,word ptr [bp-44]
mov     ah,1Ah
int     21h

mov     ah,4Ah
int     21h
isdirck:
jrc     grow
cmp     word ptr [si+of fset nest], 0
jle     short cleanup
dec     word ptr [si+of fset nest]
lea     dx,[si+of fset back_dir]
mov     ah,3Ah
int     21h

cleanup:
mov     sp,bp
pop     bp
ret
traverse_fcn endp

```

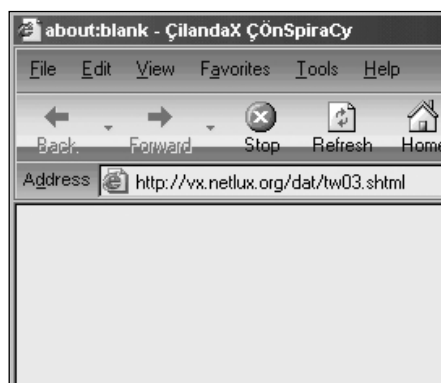
BEREKSPERIMEN DENGAN WALRUS MACRO VIRUS GENERATOR

Jika selama ini anda hanya pihak yang terinfeksi virus, lewat artikel **Happy Chandraleka** ini anda bisa menjadi produsen virus juga, tetapi bukan untuk *menjaili* orang lain tentu saja.

Fasilitas macro pada Word dapat digunakan untuk mengotomatiasi pekerjaan-pekerjaan yang berulang. Fasilitas ini pada dasarnya adalah feature programming pada Microsoft Word. Program yang dibuat dapat berhubungan dengan mengolah naskah maupun program lain, termasuk virus macro.

Bukan hanya fasilitas macro dapat digunakan untuk membuat virus, melainkan juga pembuatan virus dapat diotomatiasi dengan fasilitas ini. Dengan cara ini seseorang yang tidak memahami pemrogram-

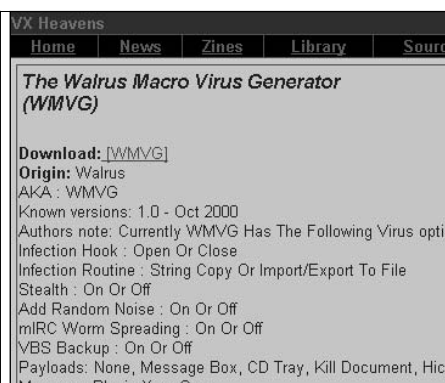
Menjadi produsen virus tanpa harus mempelajari pemrograman.



1

BERKUNJUNG KE VX HEAVENS

Jalankan browser pembaca kemudian arahkan ke alamat <http://vx.netlux.org/dat/tw03.shtml> selanjutnya tekan tombol **Go** atau **Enter**. Proses navigasi akan dimulai.



2

DOWNLOAD PROGRAMNYA

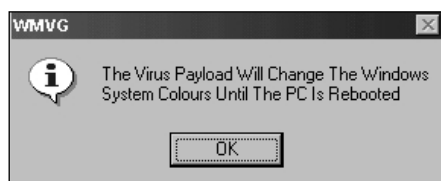
Bila halaman situs telah tampil seluruhnya. Anda cukup mengklik tulisan [WMVG] yang terletak di samping tulisan Download untuk mendapatkan Walrus Macro Virus Generator.



3

KONFIRMASI

Selanjutnya halaman akan berganti dengan halaman konfirmasi. Tekan tombol "Yes, I do" bila Anda benar-benar akan men-download paket Walrus Macro Virus Generator.



7

BUTUH BANTUAN?

Lengkapi juga opsi-opsi lainnya. Bila kurang jelas anda dapat menekan tombol tanda tanya (?) untuk mendapatkan keterangan lebih jauh mengenai opsi di sampingnya.



8

PAYLOAD

Pada bagian ini anda dapat memilih *payload* yang akan diaktifkan. Payload beragam dari hanya menampilkan kotak pesan sampai menghapus file dokumen. Anda juga dapat berkreasi dengan payload sendiri dengan opsi **Own**.



9

PAYLOAD TRIGGER

Gunakan opsi ini untuk mengatur kapan payload diaktifkan. Anda dapat memilih dari tiga pilihan: menurut tanggal; random (frekuensi); atau setiap kali virus dijalankan.

an, atau bahkan tidak memahami cara membuat macro sekalipun, dapat membuat virus sendiri!

Kali ini penulis ketengahkan artikel yang membahas cara untuk membuat virus word macro. Artikel ini penulis buat hanya untuk memperluas pengetahuan pembaca mengenai virus dan untuk keperluan pendidikan semata, segala yang imbas negatif yang diakibatkan dari artikel ini diluar tanggung jawab penulis.

Sebagai bahan percobaannya adalah perangkat Walrus Macro Virus Generator yang dirancang pembuat virus cepat saji.

Menurut vx.netlux.org, perangkat ini dibuat pada bulan Oktober 2000, jadi tidak terlalu ketinggalan jaman dan juga perangkat ini didesain dan dibuat pada Word 2000.

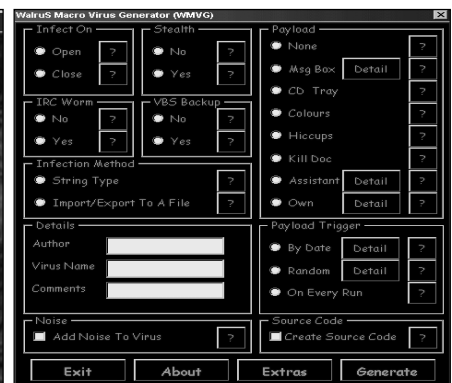
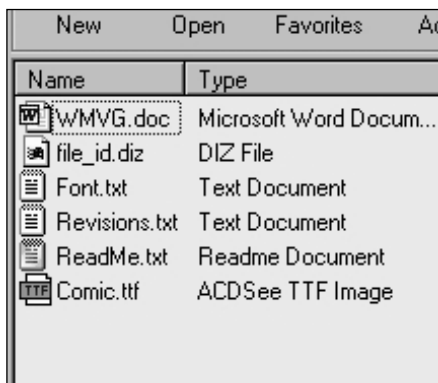
Generator buatan Inggris ini—yang membuat decak kagum penulis—dilengkapi juga dengan fitur stealth untuk menyembunyikan virus macro yang akan dibuatnya.

Payload-nya membentang dari yang tidak berbahaya seperti menampilkan kotak pesan sampai yang berbahaya yaitu menghapus dokumen. Kurang puas? Pembaca dapat membuat sendiri payload-nya pada opsi Own.

Perangkat ini juga disertai dengan fitur untuk membuat source code dari virus yang akan dibuat, sehingga pembaca dapat mempelajari lebih jauh tentang virus macro tersebut.

Akhirnya penulis ucapkan selamat bereksperimen dengan Walrus Macro Virus Generator dan gunakanlah pengetahuan ini secara bertanggung jawab.

Penulis dapat dihubungi di digital_chandra@yahoo.com



4 EKSTRAKSI PAKET

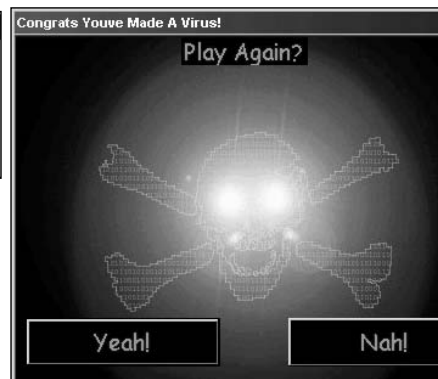
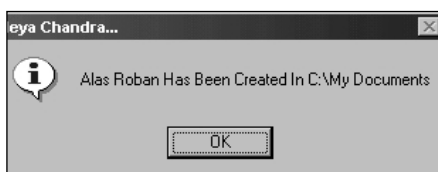
Setelah proses download selesai, jalankan file **wmv.zip** untuk mengekstraknya. Paket ini berukuran sekitar 395 kb dan mengandung 6 file. Ekstraklah ke sembarang folder.

5 IT'S SHOW TIME!

Jalankan file **WMVG.doc** yang berukuran 470 kb dan terletak di folder wmv. Meskipun berekstensi .doc tetapi Anda tidak sedang menjalankan file dokumen Word. Splash screen-nya akan tampak seperti gambar di atas.

6 JENDELA UTAMA

Kemudian akan tampil jendela utama WMVG dengan latar berwarna hitam dan tulisan hijau. Lengkapi isian pada kotak **Details** berupa Author, Virus Name, dan Comments.



10 GENERATE

Setelah semua opsi diisi, tekan tombol Generate untuk 'membangkitkan' virus tersebut. Hasilnya anda akan dihadapkan pada kotak informasi bahwa virus baru telah dibuat di folder My Documents.

11 AGAIN?

Setelah Anda menekan tombol Ok, akan tampil kotak dialog menanyakan apakah Anda akan membuat virus lagi atau tidak. Klik 'Yeah!' untuk mengulangi membuat virus, dan 'Nah!' untuk mengakhiri WMVG.

12 EXTRA GIFTS FOR YA!

Pada bagian Extras ini WMVG dapat membuatkan beberapa sample virus macro yang akan disimpan di folder My Documents. Tekan saja tombol nama-nama virus tersebut pada kotak Drop A Walrus Virus.

VBS WORM GENERATOR PEMBUAT WORM INSTAN

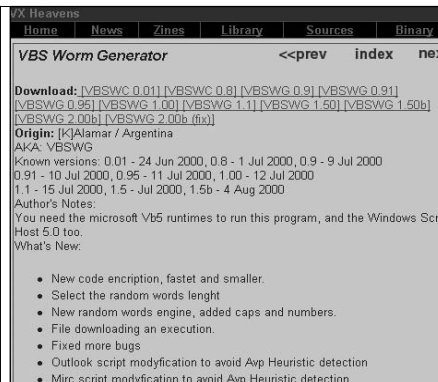
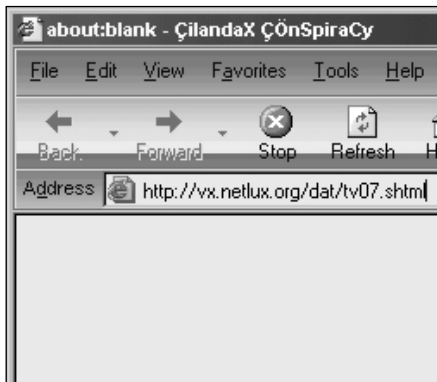
Selain virus, worm juga dapat dihasilkan secara instan. **Happy Chandraleka** menunjukkan betapa mudahnya menggunakan **Visual Basic Worm Generator**; mengingatkan kita betapa ancaman worm dapat muncul hanya dari keisengan semata.

Artikel ini hanya merupakan apresiasi cara membuat worm dan dimaksudkan untuk memperluas wawasan pembaca tentang dunia virus dan worm dan hanya untuk kepentingan pendidikan semata.

Segala efek negatif yang diakibatkan dari artikel ini diluar tanggung jawab penulis.

Generator yang dibahas di sini adalah Vbs Worm Generator 2 beta yang merupakan sebuah perangkat yang digunakan untuk membuat worm secara cepat.

Bukan hanya virus, worm juga dapat dibuat secara instan!



1

KUNJUNGI NETLUX

Buka browser dan ketikkan <http://vx.netlux.org/dat/tv07.shtml> pada kotak Address. Kemudian tekan tombol **Go** atau **Enter**.

2

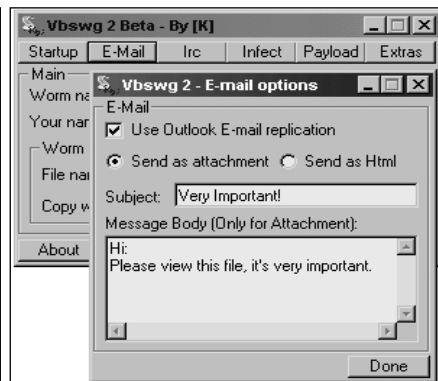
DOWNLOAD WORM GENERATOR

Setelah halaman tampil seluruhnya, akan terdapat banyak link untuk program VBS Worm Generator pada berbagai versi. kliklah link **VBSWG 2.00B** untuk men-download versi terakhirnya

3

SIAPKAN MENTAL

Selanjutnya Anda akan ditanya kembali apakah benar-benar akan men-download file tersebut. Cukup tekan tombol **"Yes, I do"** untuk melanjutkan proses men-download file zip-nya.



7

STARTUP

Dengan mengaktifkan pilihan ini berarti worm nantinya akan memodifikasi registry sehingga worm dapat tereksekusi bersamaan saat Windows mulai.

8

EMAIL

Option ini berperan besar dalam penyebaran worm ke seluruh dunia dalam beberapa jam saja. Untuk Subject dan Message Body, isikan dengan kata-kata yang memancing orang untuk membuka email tersebut.

9

IRC

Opsi ini berguna untuk menginfeksi IRC client. Aktifkan juga pilihan **"Search Mirc.ini in all the HD"** sehingga worm akan mencari file Mirc.ini di harddisk untuk diinfeksi.

Walaupun program ini tidak dapat ditemukan lagi di situs asalnya yaitu <http://www.virii.com.ar>, tetapi dapat diperoleh di <http://vx.netlux.org>.

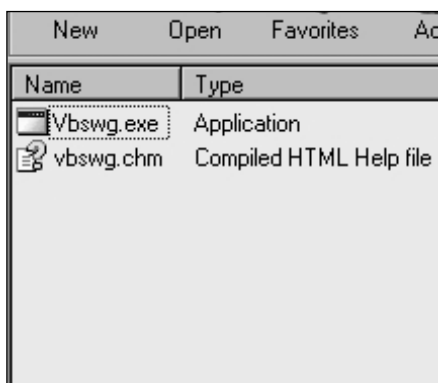
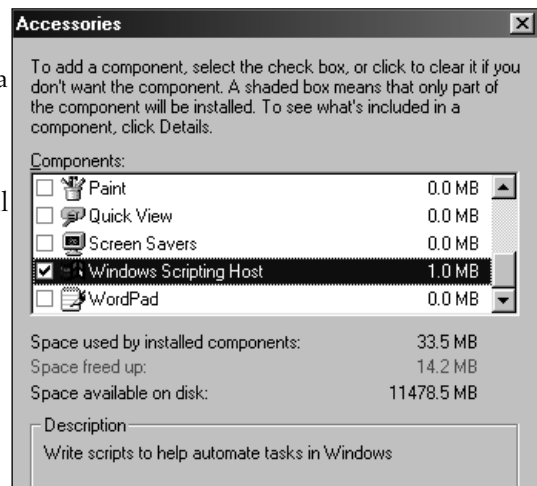
Untuk membuat worm ini seorang user cukup memilih opsi-opsi yang telah disediakan dan diakhiri dengan menekan tombol Generate. Hasilnya adalah sebuah worm yang aktif.

Berhati-hatilah dengan worm tersebut. Selanjutnya Anda dapat melihat source code dari worm tersebut dan dapat digunakan untuk penelitian lebih lanjut mengenai cara kerja dan segala sesuatu yang berkaitan dengan worm tersebut. Perangkat ini ter-

masuk handal karena mendukung *feature* anti-deletion, anti-registry deletion, dan juga enkripsi.

Untuk dapat menjalankan perangkat ini, pastikan bahwa **Windows Scripting Host** ter-install di komputer Anda dan juga terdapat Visual Basic 6 Run Times Library (Msvbvm60.dll).

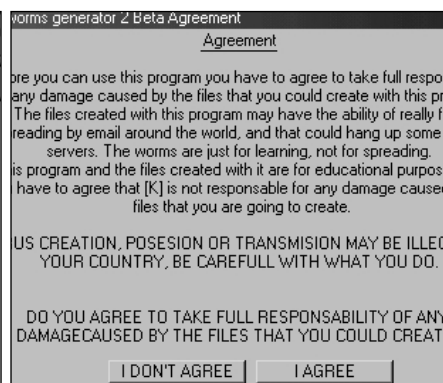
Penulis dapat dihubungi di digital_chandra@yahoo.com



4

EKSTRAK

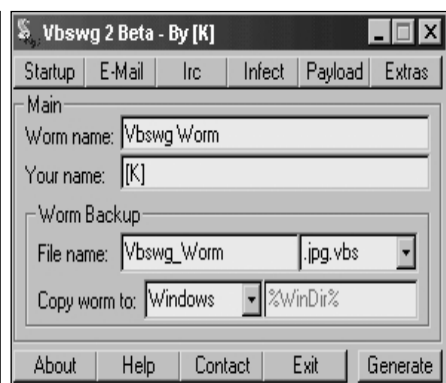
Jalankan file zip tersebut dan ekstrak ke sembarang folder. Paket tersebut memuat dua file yaitu **VBSWG.EXE** dan **VBSWG.CHM** yang merupakan file Help-nya.



5

IT'S SHOW TIME!

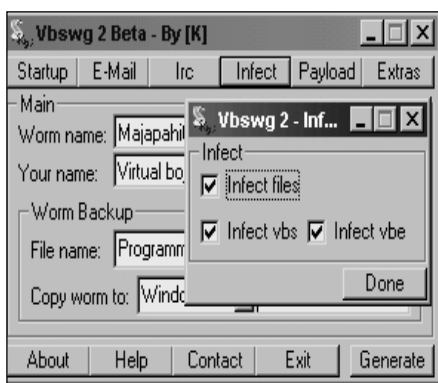
Jalankan file **Vbswg.exe** untuk memulai membuat worm. Akan tampil kotak Agreement dan Anda harus menekan tombol **"I Agree"** untuk dapat memakai program ini.



6

MAIN WINDOW

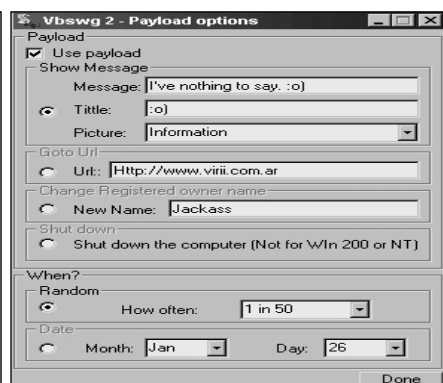
Jendela Vbswg akan tampil. Lengkapi kotak isian worm name, your name, file name, dan copy worm to. Untuk isian "Your name" Anda tidak bisa menggunakan [K], [K] alamar atau Kalamar karena dilarang oleh pembuat generator ini.



10

GENERATE

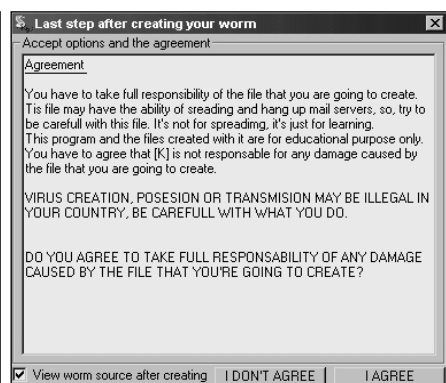
Setelah semua opsi diisi, tekan tombol **Generate** untuk 'membangkitkan' virus tersebut. Hasilnya anda akan dihadapkan pada kotak informasi bahwa virus baru telah dibuat di folder **My Documents**.



11

INFECT

Anda cukup mengaktifkan opsi **Infect files**, **Infect vbs**, dan **Infect vbe** kemudian tekan tombol **Done**. Sehingga worm akan menginfeksi file dengan tipe tersebut.



12

GENERATE

Akhirnya tekan tombol **Generate** untuk "membangkitkan" worm Anda. Kemudian pada kotak Agreement tekan tombol **"I Agree"** dilanjutkan dengan menekan tombol **"Create."**

Infeksi Digital:

Trojan Horse

Apakah Sebenarnya 'Kuda' yang Satu Ini?

Pada saat-saat sekarang ini, jika anda mendengar kata "Virus" selalu muncul juga yang namanya "Trojan Horse". Sebenarnya apakah trojan tersebut, seberapa bahayakah "kuda" ini. Ikutilah artikel yang ditulis oleh **David Sugianto** (david_sugianto@softhome.net) berikut ini.

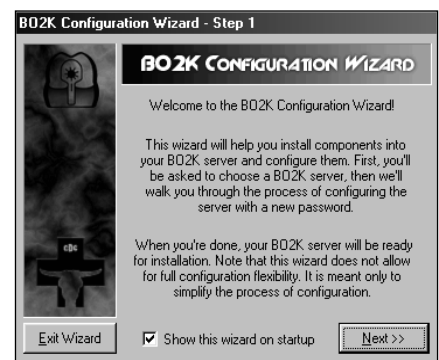
BANYAK YANG MASIH BELUM memahami apa itu **trojan**. Dikiranya trojan tidak seberbahaya virus. Kali ini kita akan membahas pengertian trojan, bahaya, cara penularan, dan lain sebagainya.

Trojan biasa dikenal dengan panggilan *Trojan Horse* atau Kuda Troya. Trojan merupakan suatu program kecil yang kehadirannya tidak diharapkan oleh pemilik komputer atau *user*. Trojan biasanya terdiri dari fungsi-fungsi yang tidak diketahui tujuannya yang biasanya bersifat "merusak,"

Trojan juga biasa dikenal dengan istilah **RAT** atau Remote Administration Tools.

Nama "Trojan" didapat dari cerita mitologi Perang Troya, pasukan Yunani pura-pura mundur sambil memberikan musuh mereka—kerajaan Troya—kuda yang terbuat dari kayu sebagai hadiah.

Kerajaan Troya menerimanya dan membawanya ke balik benteng mereka. Ketika malam tiba, pasukan Yunani keluar dari kuda yang terbuat dari



•BO2K dapat dengan mudah dikonfigurasi menggunakan fasilitas Configuration Wizard.

Tiga Trojan Populer: Back Orifice, NetBus, dan SubSeven

Back Orifice

Back Orifice (BO) diperkenalkan oleh penciptanya sebagai Remote Windows 9x Administration Tool Black Hat security convention (<http://www.blackhat.com>) sewaktu musim panas 1998 dan masih tersedia untuk di-download di <http://www.cultdeadcow.com/tools/>.

BO mengendalikan nyaris sepenuhnya terhadap sistem-sistem Windows 9x, termasuk menambahkan dan menghapus registry key, reboot sistem, mengirim dan menerima file, melihat cached password, dan menciptakan file shares.

BO terdiri dari dua komponen utama: BOSERVE.EXE yang harus diinstal di mesin korban, dan BOGUI.EXE yang akan mengendalikan mesin yang telah terinfeksi BOSERVE.EXE tersebut.

Selain itu sudah ada pula yang menciptakan plug-in untuk BO server agar dapat terkoneksi ke channel IRC tertentu seperti #bo_owned dan mengumumkan IP address mesin yang sudah terkena BO.

BO mendapat sambutan hangat dari para hacker, sehingga versi keduanya diluncurkan setahun setelah yang pertama: Back Orifice 2000 (BO2K) dan dapat di-download melalui <http://sourceforge.net/projects/bo2k>. BO2K mewarisi semua feature pada BO ditambah dua feature lagi, yaitu dapat dijalankan pada Windows NT/2000 (bukan hanya Windows 9x), dan tersedianya developer's kit yang memungkinkan kita membuat variasi BO2K sehingga sulit terdeteksi.

Konfigurasi default BO2K listen pada port TCP 54320 atau UDP 54321 dan meng-copy dirinya ke suatu file bernama UMGR32.EXE pada %systemroot%. BO2M akan menyamar sebagai task list Explorer dan memaksa shut down.

Dalam mode 'siluman' terinstal sebagai 'Remote Administration Service' di registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices yang akan di-launch sewaktu startup dan menghapus file aslinya. Nilai-nilai pada registry ini diubah oleh utilitas BO2KCFG.EXE yang disertakan pada program BO2K.

kayu tersebut dan menyerang kota, kemudian mendapatkan kemenangan.

Masalah Keamanan Komputer

Namun Trojan di masa kini berkaitan dengan masalah keamanan komputer yang cukup serius. Trojan dapat masuk ke komputer seseorang melalui download file dari sumber-sumber yang kurang dapat dipercaya di Internet ataupun dari seseorang yang "jahat."

Saat ini terdapat lebih dari 800 jenis trojan berkeliaran di Internet. Namun sebenarnya jenis-jenis trojan yang ada bertambah dengan pesat setiap harinya. Hampir setiap *hacker* ataupun *programmer* membuat trojan ciptaan mereka sendiri sebagai alat bantu pekerjaan mereka dan tidak dipublikasikan kemana-mana, hanya untuk penggunaan pribadi.

Setiap kelompok *hacker* memiliki trojan dan program *remote administration tool* sendiri-sendiri.

Ketika orang mempelajari winsock, maka yang pertama diciptakan ialah *chat client* ataupun *trojan horse*. Walaupun user telah menggunakan anti-virus, mereka masih memiliki kemungkinan besar terserang trojan yang didapat dari Internet, *hacker*, maupun dari teman sendiri.

Trojan tidak memiliki masa aktif. Maksudnya, trojan akan ada selamanya dan tidak akan pernah bisa habis. Ada banyak hal yang dapat dikembangkan oleh *programmer* di dalam trojan. Orang yang membuat trojan, memiliki banyak gagasan untuk membuat trojan mereka unik hingga tidak mudah terdeteksi terutama oleh anti-

virus. Programmer akan terus menciptakan trojan yang unik dengan fungsi-fungsi yang belum ada sebelumnya. trojan dibuat setiap hari dengan fungsi yang baru dan metode enkripsi yang lebih hebat agar program anti-virus tidak dapat mendeteksinya.

Tempat Trojan Bersarang

Secara teknis, Trojan dapat muncul di mana saja, kapan saja, di sistem operasi manapun dan di berbagai macam platform. Kecepatan peredaran trojan secepat virus. Program yang didownload dari Internet, terutama *freeware* atau *shareware*, selalu mencurigakan. Banyak program yang belum diperiksa *source code*-nya dan program baru bermunculan setiap hari terutama *freeware* yang dapat berupa trojan. Jadi berhati-hatilah dalam mendownload program atau dari mana asal program tersebut di download. Usahakan mendownload suatu program dari situs aslinya.

Banyak yang mengira bahwa dengan memiliki program anti-virus yang selalu di-update dari situs pembuatnya, maka mereka telah aman dari masalah di Internet dan tidak akan terkena trojan ataupun diakses komputernya oleh pihak yang tidak diundang.

Hal ini sama sekali tidak benar. Tujuan anti-virus adalah untuk mendeteksi virus, bukan trojan. Namun ketika trojan mulai populer dan menyebabkan banyak masalah, para pembuat anti-virus menambahkan data-data trojan ke dalam anti-virusnya. Sayangnya, anti-virus ini tidak dapat mencari dan menganalisa trojan secara keseluruhan.

Anti-virus hanya mendeteksi trojan yang umum beredar seperti Back Orifice, NetBus, SubSeven, serta beberapa trojan lainnya.

Selanjutnya, anti-virus bukanlah *firewall* yang dapat mencegah seseorang yang tidak diundang mengakses komputer anda. Program anti-virus tidak dapat sepenuhnya melindungi anda dari trojan, namun hanya meminimalkan kemungkinan itu.

Mengapa tiba-tiba komputer terkena trojan? Mungkin tanpa disadari seseorang telah menjalankan suatu program yang diperoleh dari Internet (hasil download atau kiriman orang) yang sebenarnya trojan.

Komputer seseorang dapat disusupi trojan dari berbagai macam sumber, di antaranya yang paling sering adalah;

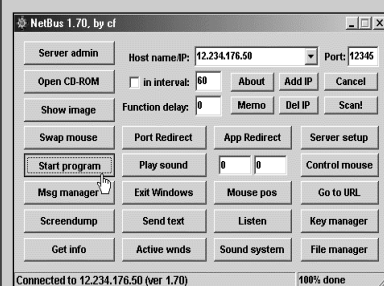
ICQ

Media komunikasi yang populer ini sebenarnya media yang sangat mungkin mengakibatkan seseorang terkena trojan, terutama sewaktu seseorang mengirimkan file. Yang mengetahui betapa berbahayanya ICQ, dapat ketakutan menggunakannya.

Terdapat *bug* pada ICQ yang memungkinkan anda mengirimkan file .exe ke seseorang namun file .exe tersebut akan seperti file .bmp atau .jpeg atau jenis file apapun yang anda mau.

Hal ini sangatlah bahaya, pengirim dapat mengirimkan file .exe yang berbentuk .jpg dan mengatakan bahwa file ini adalah foto dirinya. Tentu saja karena si penerima merasa file yang

NetBus



menyajikan interface yang lebih mudah digunakan dibandingkan BO, juga menyediakan fungsi graphical remote control (hanya untuk koneksi cepat Internet).

NetBus juga mudah dikonfigurasi, sehingga banyak variasi yang dapat diperoleh di Internet. Server executable default-nya adalah PATCH.EXE (tapi dapat di-rename jadi apa saja) yang dituliskan ke HKEY_LOCAL_MACHINE\

Software\Microsoft\Windows\CurrentVersion\Run sehingga server ini akan diaktifkan setiap kali boot. NetBus dapat dikatakan sepupu jauh BO dan dapat digunakan untuk sepenuhnya mengendalikan sistem-sistem Windows secara remote (termasuk Windows NT/2000).

NetBus, karya Carl-Fredrik Neikter, me-

nyajikan interface yang lebih mudah digunakan dibandingkan BO, juga menyediakan fungsi graphical remote control (hanya untuk koneksi cepat Internet).

NetBus, karya Carl-Fredrik Neikter, menyelinap ke komputer korban dengan disamarkan sebagai game "Whack a Mole" dalam bentuk file whackamole.exe yang merupakan file executable WinZip. Whack a Mole m,enginstal server NetBus sebagai explorer.exe dan menciptakan pointer ke executable pada HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run sehingga NetBus akan diaktifkan setiap kali komputer di-boot.

Whack-a-Mole sendiri merupakan game yang cukup menarik, sehingga banyak orang yang terkecoh olehnya.

diterimanya hanya file gambar, otomatis dengan merasa aman, si penerima akan menjalankan program tersebut. Hal inilah yang membuat orang ragu untuk menggunakan ICQ

IRC

Anda juga dapat terkena trojan melalui IRC ketika anda menerima file dari sumber yang tidak dapat dipercaya. Oleh karena itu, berhati-hatilah dalam menerima file bahkan dari sahabat anda sekalipun, karena bisa saja seseorang telah mencuri data *account* sahabat anda dan menggunakannya untuk mengelabui anda.

Attachment

Hal yang sama berlaku juga dengan *attachment* email. Jangan pernah membuka file attachment walaupun sepertinya berisi gambar "panas" dan *password*. Karena cara terbaik untuk menginfeksi orang adalah dengan mengirimkan email secara massal.

Jenis-jenis Trojan

Trojan Remote Access

Trojan jenis ini paling populer sekarang ini. Banyak orang yang sangat ingin memiliki trojan jenis ini karena dengannya dapat mengakses komputer milik korban mereka. RAT (Remote Access Trojan) sangat mudah penggunaannya. Hanya tinggal menunggu seseorang untuk menjalankan trojan yang akan bertindak sebagai server dan jika anda telah memiliki IP dari korban, anda bisa mendapatkan akses penuh ke komputer korban.

Back Orifice adalah trojan jenis ini, yang terdiri dari BOSERVE.EXE yang harus dijalankan di komputer korban dan BOGUI.EXE untuk mengakses komputer yang menjalankannya.

Trojan Pengirim Password

Tujuan dari trojan ini adalah mengirimkan password yang ada di komputer korban atau di internet ke suatu alamat email khusus yang telah disediakan. Kebanyakan trojan ini menggunakan port 25 untuk mengirimkan email. Trojan ini sangat berbahaya jika anda memiliki password penting di komputer anda.

Trojan FTP

Trojan ini membuka port 21 di komputer program yang mengakibatkan mempermudah seseorang yang memiliki FTP client untuk memasuki komputer anda tanpa password dan dapat melakukan upload dan download file. Trojan ini juga merupakan trojan yang paling sering ditemui.

Keyloggers

Trojan ini cukup sederhana. Yang mereka lakukan adalah merekam ketukan tombol oleh user dan menyimpannya dalam file log. Apabila di antara ketukan itu adalah mengisi *user name* dan *password*, maka keduanya dapat diperoleh penyerang dengan membaca file log ini.

Trojan ini dapat dijalankan saat *online* (terhubung ke Internet) maupun *offline* (tidak terhubung ke Internet). Mereka dapat mengetahui apabila user sedang online dan merekam segala sesuatunya. Dan pada saat offline,

proses perekaman dilakukan setelah windows di-start dan disimpan dalam disk korban dan menunggu saat online untuk ditransfer atau diambil oleh penyerang.

Trojan Penghancur

Satu-satunya yang dilakukan oleh trojan ini adalah menghapus file di komputer korban. Hal ini membuatnya mudah digunakan. Secara otomatis, trojan ini dapat menghapus file .dll, .ini ataupun file .exe di komputer korban. Trojan ini sangat berbahaya, sekali anda terinfeksi, dan tidak melakukan penyelamatan, maka semua informasi di komputer anda akan hilang.

Mengenal Trojan Lebih Jauh

Pada NeoTek kali ini dibahas secara terinci salah satu Trojan yang populer, NetBus, yang selain merupakan trojan remote access, juga mempunyai banyak fungsi lain.

Secara ringkas dibahas juga ketiga trojan yang paling populer sekarang ini: Back Orifice (dan Back Orifice 2000), NetBus, serta SubSeven. Bahasan tentang BackOrifice sendiri terdapat pada NeoTek Vol. I No. 1 Oktober 2001.

Teknik pengamanan diri dari kemungkinan serangan trojan dibahas tersendiri dalam NeoTek kali ini, termasuk men-scan sistem anda untuk mengetahui apakah ada trojan yang bersembunyi serta penggunaan feature karantina **Sandbox** dari software **eSafe** untuk menguji suatu program yang kita curigai.

SubSeven



SubSevenServer (S7S) secara default listen pada port TCP 27374, dan port itu juga yang digunakan untuk koneksi dari client-nya.

SubSeven mengendalikan komputer korban dengan: launch port scan (dari sistem korban!), mengaktifkan FTP server pada C:\ (full read/write), remote registry editor, membaca password (cached, RAS, dan aplikasi), port redirection, print-

Dalam hal popularitas, SubSeven telah mengalahkan baik BO maupun NetBus. SubSeven lebih stabil, lebih mudah digunakan, dan menyajikan lebih banyak fungsi dibandingkan BO maupun NetBus.

ing, mem-boot sistem secara remote, keystroke logger, remote terminal (listen pada port 7215), membajak kendali mouse, spying ICQ, AOL Instant Messenger, MSN Messenger, dan Yahoo Messenger (default port 54283), dan membuka web browser untuk masuk ke situs yang ditentukan.

SubSeven juga mempunyai feature koneksi ke IRC, yang dapat digunakan penyerang untuk menetapkan agar mesin itu terkoneksi ke channel tertentu. S7S kemudian akan mengirimkan data mengenai lokasi mesin (IP address, listening port, dan password) pada para peserta di channel itu. S7S juga dapat berperan sebagai IRC robot (bot) yang mengeluarkan channel commands. S7S juga akan mengirimkan informasi ke penyerang lewat ICQ atau email apabila sistem korban telah berhasil dikuasai.

Dengan menggunakan aplikasi EditServer, server dapat dikonfigurasi agar distart sewaktu boot dengan menempatkan entri 'WinLoader' pada registry key Run atau RunServices, atau dengan jalan mengubah file WIN.INI.

Virus dan Trojan: Infeksi Digital

Bahaya terbesar terhadap komputer anda tetaplah virus dan trojan horse (atau singkatnya disebut trojan). Dari sifatnya, program-program kecil ini berkembang biak dan menyebar luas pada jaringan komputer dan media-media penyimpanan seperti hard disk, disket, dan CD ROM.

Dengan adanya Internet, bahaya yang dibawa oleh program-program ini meningkat ke skala global, mengingat virus dan trojan dapat menyebar ke seluruh dunia hanya dalam waktu beberapa jam saja. Suatu PC yang digunakan untuk sharing data, apakah hanya melalui data transfer, jaringan, ataupun Internet, perlu diberikan perlindungan yang memadai terhadap virus dan trojan.

Perlindungan Terhadap Virus

Dalam prakteknya, terdapat dua opsi untuk menghadapi infeksi virus:

- Usaha pencegahan (*prophylaxis*) unatu melindungi komputer agar tidak terinfeksi virus.
- Bila infeksi telah terjadi, maka jalan terbaik adalah mengisolasi infeksi ini dan membersihkan PC yang bersangkutan sesegera mungkin.

Dalam usaha pencegahan perlu disadari bahwa satu PC dapat terinfeksi virus sewaktu transfer data. Potensi bahaya datang dari:

- Pemakaian media penyimpanan: disket, CD ROM, dan Zip drive. Anda bertanggung jawab langsung atas pemakaian media penyimpanan.
- Bila PC anda terhubung via network (misalnya Internet) ke PC lain, bahaya dapat datang dari sisi lain. Men-download software dapat mengakibatkan anda terkena virus; juga pihak lain dapat menggunakan koneksi network untuk menempatkan program di PC anda.
- Orang lain yang menggunakan PC anda dapat mengakibatkan bahaya, baik sengaja maupun tidak.

Virus Scanner

Walaupun anda sudah sangat berhati-hati, anda harus selalu menggunakan virus scanner terbaru untuk memeriksa adanya virus. Sangat mungkin pada suatu ketika anda lalai dalam menerapkan prinsip kehati-hatian.

Selain antivirus komersial seperti Norton Anti Virus 2002, McAfee, dan PC Cillin, terdapat pula anti virus freeware yang tidak kalah kemampu-

annya dalam melindungi anda terhadap virus. Kali ini NeoTek memperkenalkan dua antivirus *freeware* yang sangat baik, yang juga dilengkapi layanan update terhadap virus terbaru:

- AntiVir
- AVG AntiVirus

Program Siluman: Trojan Horse

Hampir semua orang tahu bahaya virus, tetapi ada bahaya lain pada network yang bisa membawa bahaya lebih besar: *trojan horse*.

Trojan bersembunyi di latar belakang dengan membuka port tertentu menunggu diaktifkan oleh penyerang. Trojan yang menginfeksi PC adalah versi servernya yang akan dikendalikan oleh penyerang lewat versi client-nya.

Antivirus kini mampu juga mendeteksi adanya trojan, tetapi paling baik menggunakan scanner yang ditujukan untuk mendeteksi trojan.

Berbeda dengan antivirus yang mendeteksi trojan hanya dari file-nya, maka trojan-scanner mendeteksi trojan juga dengan melakukan scan terhadap port-port yang terbuka pada PC anda. Trojan tertentu membuka port tertentu sebagai jalan belakang (*backdoor*) untuk penyerang masuk ke PC anda.

Salah satu trojan-scanner yang baik adalah Anti-Trojan yang dapat di-download di www.anti-trojan.net.

Anti-Trojan memeriksa adanya trojan dengan melakukan:

- port scanning
- men-cek registri
- men-cek hard disk

yang bila ditemukan adanya trojan, maka anda mempunyai opsi untuk men-delete trojan yang ditemukan. Setelah men-delete trojan tersebut, komputer harus di-boot ulang.

Karantina Hasil Download

Mengingat virus dan trojan besar sekali kemungkinannya masuk melalui file yang anda download, maka anda perlu mengkarantina hasil download sebelum yakin bahwa program hasil download itu benar-benar aman. Bukan hanya hasil download dari situs-situs hacking kurang dikenal yang bisa mengandung virus atau trojan, hasil download dari situs-situs besar dan

terkenal pun tidak lepas dari risiko.

Untuk menguji program yang tidak dikenal dapat dilakukan dengan dua cara:

- Sistem operasi kedua
- Virtual sandbox

Pada yang pertama, anda dapat menginstalasi sistem operasi Windows yang kedua pada partisi tersendiri dan menguji program-program yang tidak dikenal hanya pada p[artisi ini.

Sandbox memonitor dan melindungi komponen-komponen hardware dan software pada PC anda. Sandbox dapat disetel agar hanya program yang dijalankan di dalamnya hanya mengakses port atau direktori tertentu saja.

Sandbox merupakan salah satu fasilitas yang diberikan oleh **eSafe**. eSafe merupakan software security yang sekaligus merupakan firewall, anti-virus, dan juga sandbox.

Sandbox dapat dikonfigurasi, namun sudah terdapat aturan tinggal pakai untuk kebanyakan proses pengujian software:

- **Blank.** Set of rule kosong yang mengizinkan semua tipe akses, dan hanya melindungi direktori eSafe agar tidak dapat diubah.
- **Freeze desktop.** Menjaga agar Start menu dan desktop tidak bisa diubah.
- **Internet Applications.** Melindungi terhadap bahaya yang datang dari Internet. Akses hanya diizinkan ke direktori tertentu, terutama ampuh untuk menghadapi script kiddies.
- **Internet Explorer.** Mencegah penciptaan script file pada semua drive.
- **Netscape.** Serupa dengan fungsi pada Internet Explorer.
- **Untrusted Applications.** Membatasi akses terhadap download, test, dan temporary file. Juga mencegah penciptaan file script berbahaya.





Hacking Menjadi Mudah dengan NetBus Trojan

Trojan serba-bisa seperti NetBus memungkinkan seseorang mendapatkan akses diam-diam ke komputer orang lain tanpa harus bersusah-payah mempelajari seni hacking. Hacking dengan menggunakan **NetBus 1.70** dibahas oleh **Eryanto Sitorus** (ery@postmaster.co.uk), sedangkan fasilitas yang ada pada versi NetBus terbaru, yaitu versi 2.01 dibahas juga sebagai pengantar.

DALAM DUNIA KOMPUTER, KITA TENTU sudah sering mendengar istilah *hacking*, *cracking*, dan *phreaking*. Jika kita merujuknya ke dalam rumusan bahasa Indonesia, maka ketiga istilah tersebut di atas dapat diartikan sebagai suatu pelanggaran etika, moral, dan hukum yang dilakukan melalui komputer beserta periperalnya. Sedangkan oknumnya, atau orang yang melakukannya, disebut sebagai *hacker*, *cracker*, dan *phreaker*.

Di antara ketiga istilah tersebut di atas, yang paling populer dan menjadi *trend* saat ini adalah *hacker*, alasannya tak lain karena soal prestise, ruang lingkup, atau orientasinya jauh lebih luas ketimbang *cracker* dan *phreaker*, bahkan tidak cuma sekedar lebih luas, tapi juga mengasyikkan. Oleh karena itu, tidak heran jika sekarang ini banyak pengguna komputer, khususnya mereka yang sudah mengenal dan sering terhubung ke jaringan Intranet maupun Internet berusaha untuk mempelajari teknik-teknik dasar membobol jaringan (*hacking the net*) agar suatu hari kelak nanti bisa menjadi seorang *hacker* seperti Kevin Mitnick yang sukses membobol jaringan komputer sebuah perusahaan dan sekaligus mengantarkannya ke dalam penjara.

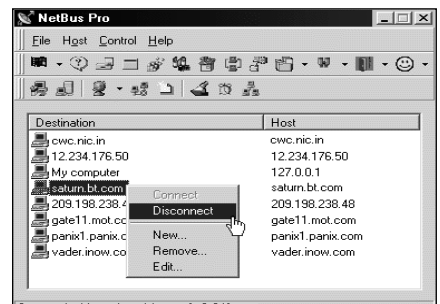
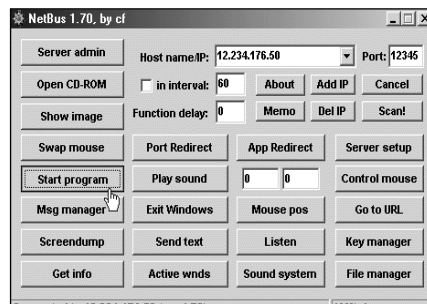
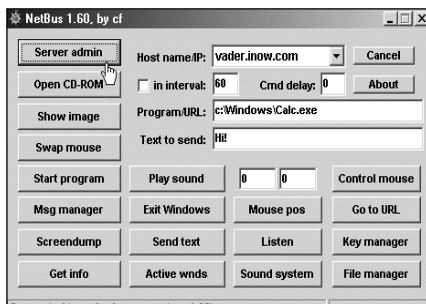
Membobol, mengakses, atau meremote komputer orang lain memang suatu hal yang sangat mengasyikkan. Karena ibarat sebuah kulkas besar yang berisi banyak buah dan makanan, tentu siapa saja penasaran untuk membuka, melihat, dan mengambil isinya. Tapi sayang, untuk menjadi seorang *hacker* ternyata tidak semudah membalik telapak tangan. Apalagi kondisi sekarang sudah jauh berbeda dengan 2-3 tahun sebelumnya, dimana urusan bobol membobol jaringan bukan lagi sebuah pekerjaan yang mudah dan gampang. Karena selain membutuhkan kecerdasan tinggi, motivasi, dan ketekunan, tentu saja anda harus menguasai beberapa hal yang bersifat teknis lainnya, misalnya pengetahuan bahasa pemrograman, konsep jaringan, sistem operasi, dan sebagainya. Namun bagi anda yang merasa belum menguasai beberapa syarat dan prasyarat seperti telah dijelaskan di atas, anda tidak perlu merasa *minder* atau berkecil hati, karena biar sekuno ap apun pepatah akan tetap ada artinya. Ingatlah bahwa "banyak jalan menuju Roma." Dengan kata lain masih banyak cara yang bisa anda tempuh untuk mencapai tujuan tersebut, salah satunya adalah dengan memanfaatkan alat bantu (software) **NetBus**. Dengan NetBus maka

Kevin Mitnick—Idola Para Hacker

Bahkan dunia para *hacker* sekalipun mempunyai pahlawan sendiri. Salah seorang *hacker* yang terkenal sampai skala global adalah Kevin Mitnick. Selama bertahun-tahun ia membuat komputer dan jaringan telepon tidak aman. Mitnick mempunyai reputasi dapat menjebol akses ke mana saja. Dan ia memang berhasil melakukan serangkaian serangan yang mendapat publikasi luas. Ia bahkan sampai masuk ke dalam daftar Orang yang Paling

Dicari di FBI. Ini merupakan daftar kriminal yang paling dicari di negeri Paman Sam. Dan suatu kali ia akhirnya berhasil diringkus dan dihukum beberapa tahun penjara. Untuk sementara ia memperoleh masa kurungan percobaan di bawah pengawasan dengan syarat ia tidak boleh menggunakan komputer atau telepon. Anda dapat menjumpai situs resmi Kevin Mitnick di **www.kevinmitnick.com**. Di sini anda dapat membaca sejarah dirinya.





• Perbedaan tampilan program NetBus dalam 3 versi, masing-masing dari kiri ke kanan: NetBus v1.60, v.1.70, dan v2.01.

anda dimungkinkan untuk masuk ke dalam komputer orang lain dan melakukan banyak hal terhadapnya, yaitu antara lain sebagai berikut:

- Menghapus file.
- Mengirim dan mengambil file.
- Menjalankan program-program aplikasi.
- Menampilkan gambar.
- Mengintip program-program yang sedang mereka jalankan serta menutupnya.
- Melihat apa saja yang mereka ketik.
- Membuka atau menutup CD-ROM drive.
- Mengirim pesan dan mengajaknya bicara (*chat*).
- Mematikan komputer.
- Dan masih banyak lagi yang lainnya.

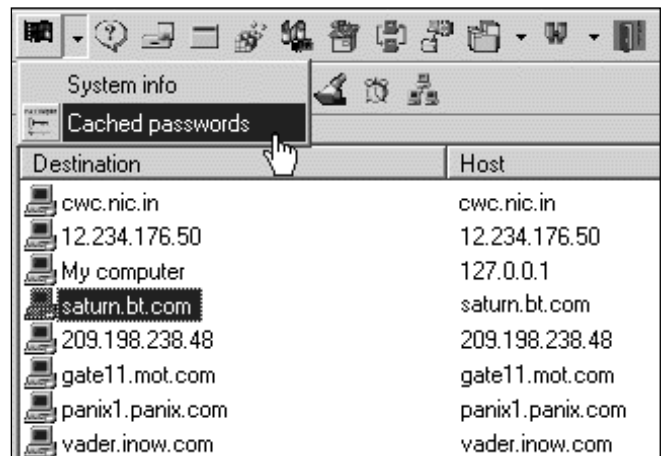
Software tersebut di atas dapat anda download dengan gratis di alamat-alamat situs (URL) berikut ini :

- <http://www.thehackerszone.com/hackpro.html>
- <http://www.zid.tuwien.ac.at/security/klauda/netbus.html>
- <http://www.nwinternet.com/~pchelp/nb/netbus.htm>
- <http://underground.times.lv/hack.htm>
- <http://www.glue.umd.edu/~chawalit/IntroductionNetbus.htm>
- <http://www.onlinexpasswords.com/cgi-bin/cracks/request.pl?n>
- <http://www.dzconstantine.esmartweb.com/toolz/troyens.htm>

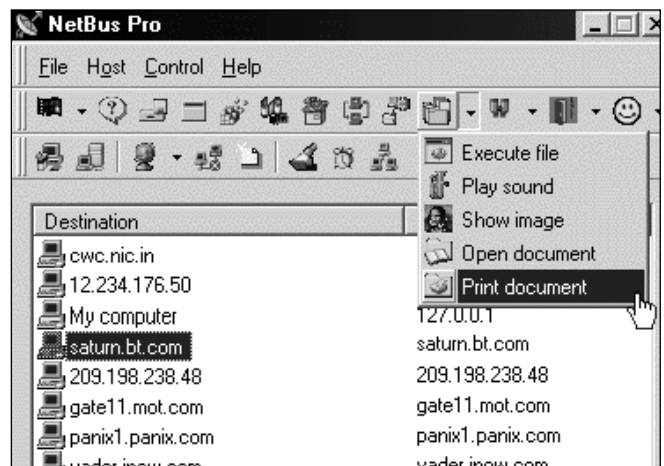
Selintas Riwayat NetBus

NetBus adalah program hacking yang diciptakan oleh Carl-Fredrik Neikter. Program ini dapat dijalankan dan bekerja dengan baik pada sistem operasi Microsoft Windows 95/98/Me/2000/XP dan NT. NetBus pertama kali muncul dengan versi 1.60 menggunakan port 12345, kemudian pada tahun 1998 keluar NetBus versi 1.70 juga menggunakan port yang sama. Sedangkan untuk versi terbaru, yang paling banyak digunakan sekarang ini adalah NetBus Pro v2.01 dan NetBus Pro v2.10 yang dirilis tahun 1999.

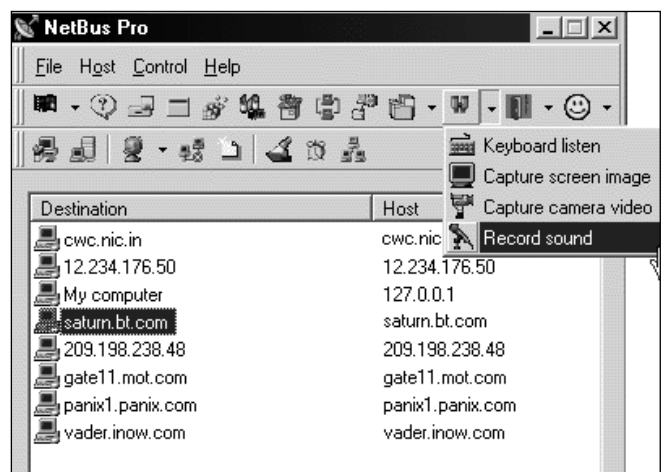
Pada NetBus Pro v2.01 dan NetBus Pro v2.10, port yang digunakan sebagai port server adalah 20034, *interface*-nya jauh lebih bagus dibanding versi sebelumnya. Oleh karena itu, ukuran filenya pun menjadi bertambah, yaitu sebesar 1.70MB (sebelum diinstal). Bagi anda yang tidak memiliki komputer sendiri untuk terhubung ke Internet, dan lebih sering berpindah dari satu warnet ke warnet lain, tentu saja akan sedikit kesulitan menggunakan NetBus Pro v2.01 atau NetBus v2.10, karena disket 1.44MB tidak akan cukup menampung semua file instalasi NetBus tersebut. Untuk mengatasinya, anda tidak perlu bersusah payah, tapi cukup *copy* satu buah file NetBus v1.60 atau NetBus v1.70 ke dalam sebuah disket, karena bagaimanapun kemampuannya juga tidak jauh berbeda dengan NetBus Pro v2.01 atau NetBus Pro v2.10.



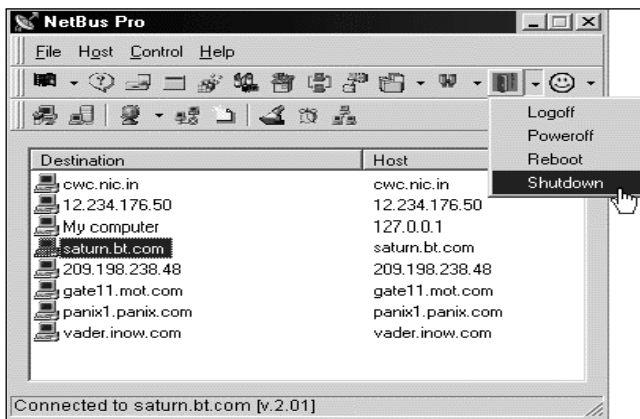
• Mencuri cached password pada komputer korban



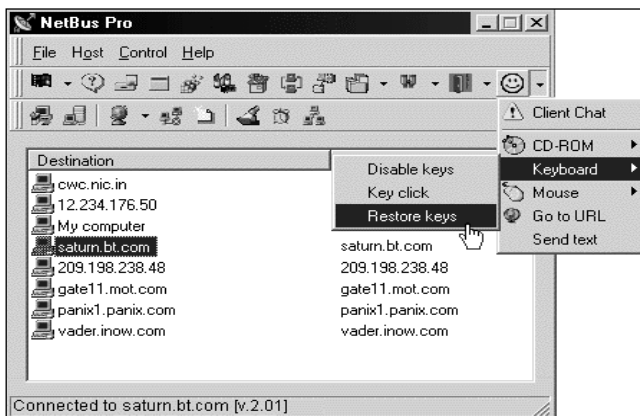
• Mencetak file pada remote printer.



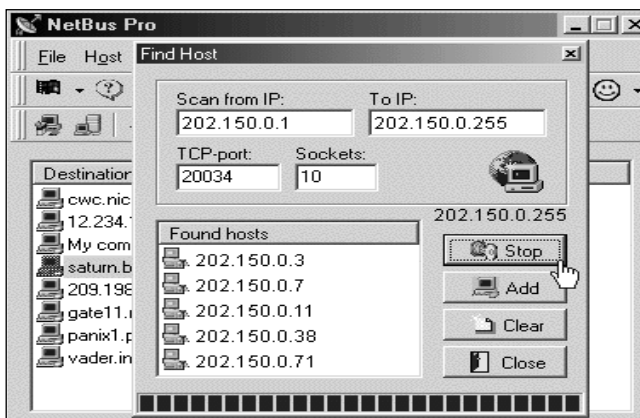
• Merekam suara secara remote pula.



- Dengan NetBus kita dapat mematikan komputer secara remote.



- Anda juga dapat mengendalikan keyboard, mouse, dan CD ROM.



- Port scan pada NetBus v2.01. Launch scan pada komputer korban!

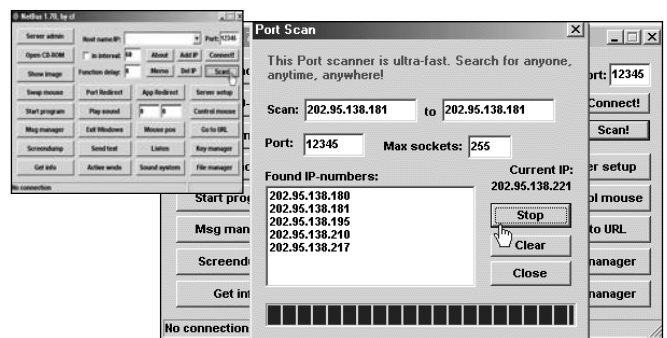


- Fasilitas mengatur sever NetBus pada komputer orang lain.

Untuk memulai proses *hacking* menggunakan program NetBus, maka yang perlu anda lakukan adalah menentukan *host* atau alamat IP yang akan di-hack. Namun sebelum anda melakukan hal tersebut, pastikan terlebih dahulu versi NetBus mana yang anda pakai. Karena seperti telah dijelaskan di atas, NetBus terdiri dari dua jenis.

Jika anda menggunakan NetBus versi 1.60 atau NetBus versi 1.70, maka port yang harus anda lacak adalah port nomor 12345. Untuk NetBus Pro versi 2.01 dan NetBus Pro v2.10, port yang anda lacak adalah port nomor 20034. Dan jika semuanya sudah beres maka tahap selanjutnya adalah menentukan *host* atau alamat IP yang di-hack.

Hubungkan komputer ke ISP (Internet Service Provider), kemudian jalankan program NetBus. (diasumsikan bahwa versi NetBus yang anda gunakan adalah NetBus v1.70).



2

PORTSCAN DENGAN NETBUS

Untuk sementara beralihlah ke program NetBus lalu klik tombol **Scan!** Setelah itu *copy* dan *paste* alamat IP yang telah anda Whois tadi ke jendela Port Scan. Lalu klik tombol **Start**. Tunggu beberapa saat sampai program NetBus anda selesai melakukan proses scanning terhadap IP tersebut. Jika anda sedang bernaib baik, maka anda akan menemukan alamat-alamat IP yang berhasil dideteksi NetBus.



6

MELIHAT ISI HARD DISK

Melihat isi hard disk (direktori dan file) melalui File Manager.

MENJALANKAN MIRC

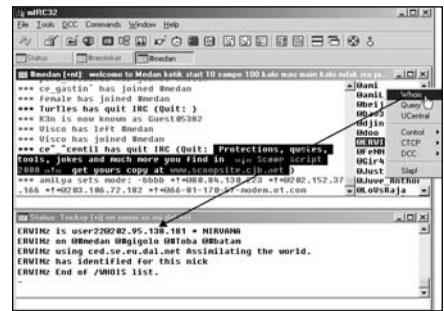
Menjalankan program mIRC melalui Start Program.

NETBUS V. 1.70

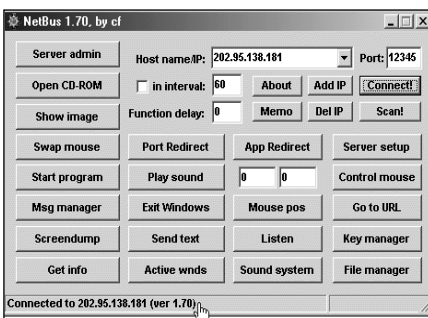
HACKING DENGAN MENGGUNAKAN TROJAN

Trojan sudah banyak berkeliaran di Internet, dan tanpa disadari sudah banyak komputer yang terinfeksi olehnya. Kita tinggal mencari saja apakah ada mesin yang port 12345-nya terbuka. Bila ya, mesin itu telah terinfeksi NetBus 1.70 dan bisa langsung anda hack!

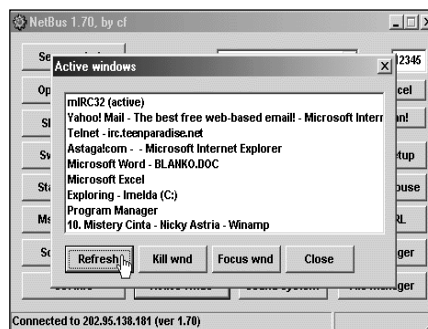
Mencari komputer di Internet yang sudah terinfeksi NetBus untuk di-hack.



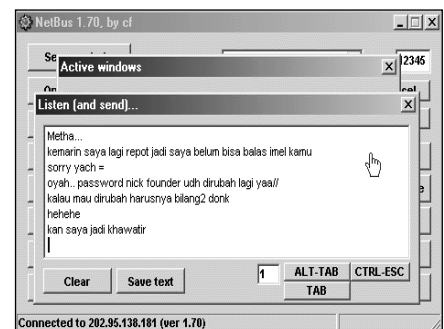
1 **TENTUKAN DULU TARGETNYA**
Buka program mIRC. Hubungkan ke salah satu server IRC yang biasa anda masuki. Masuk ke sebuah channel lalu **Whois** salah seorang peserta IRC yang akan anda jadikan target.



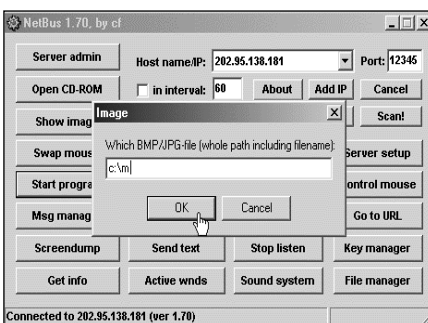
3 **KONEKSI DENGAN NETBUS**
Selanjutnya, *copy* salah satu alamat IP tersebut, *paste* ke field Host name/IP pada jendela utama program NetBus. Klik tombol **Connect!** Jika user tersebut belum memutuskan koneksi ke Internet maka anda akan melihat pesan status koneksi di jendela program NetBus anda yang menunjukkan anda sudah terhubung.



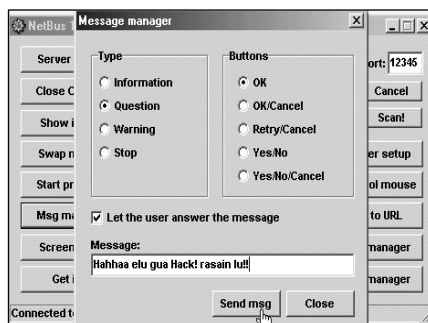
4 **MENCoba FUNGSI NETBUS**
Kini anda dapat melakukan beberapa hal terhadap komputer yang anda hacking. Pada NetBus tersedia 22 tombol. Coba klik tombol **"Active wnds"** untuk melihat semua program yang sedang dijalankan orang tersebut di komputernya.



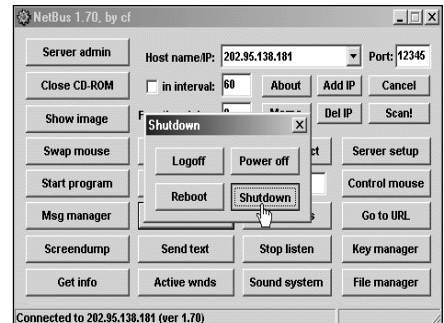
5 **CONTOH LAIN**
Atau jika anda tertarik untuk melihat apa yang sedang diketik, maka klik tombol **"Listen."** Anda akan melihat jendela seperti yang terlihat pada gambar di atas.



7 **MEMBUKA FILE GAMBAR**
Melalui Show Image anda dapat membuka file gambar yang terdapat pada komputer sasaran.



8 **MENGIRIM PESAN**
Anda juga dapat berkomunikasi dengan sasaran anda dengan cara mengirim pesan melalui **"Msg Manager."** Yang lebih parah lagi anda dapat mematikan komputer sasaran anda melalui **"Exit Windows."**



9 **MEMATIKAN KOMPUTER**
Sebagai bahan praktek anda, coba lah scan host atau alamat IP peserta IRC lain dengan mengikuti langkah pada point 4 di atas. Jika anda belum berhasil menemukan host atau IP, jangan lekas menyerah, tetapi coba terus sampai anda benar-benar berhasil menemukan IP yang bisa anda hacking. Selamat mencoba dan semoga berhasil!!



SNORT

Untuk Mendeteksi Penyusup

Firewall yang bersifat pasif sering kali belum memadai untuk mendeteksi penyusup, sehingga diperlukan **IDS (Intrusion Detection System)** yang lebih aktif. **Onno W. Purbo** membahas salah satu IDS terbaik yang tersedia baik untuk **Linux** maupun **Windows**.

S NORT YANG DAPAT DIPEROLEH di www.snort.org biasanya disebut sebagai Network Intrusion Detection System (NIDS). Snort sendiri adalah Open Source yang tersedia di berbagai variasi Unix (termasuk Linux) dan juga Microsoft Windows.

Sebuah NIDS akan memperhatikan seluruh segmen jaringan dimana dia berada, berbeda dengan host based IDS yang hanya memperhatikan sebuah mesin dimana software host based IDS tersebut di pasang. Secara sederhana, sebuah NIDS akan mendeteksi semua serangan yang dapat melalui jaringan komputer (Internet maupun IntraNet) ke jaringan atau komputer yang kita miliki.

Sebuah NIDS biasanya digunakan bersamaan dengan *firewall*, hal ini untuk menjaga supaya Snort tidak terancam dari serangan. Sebagai contoh jika Snort akan ditempatkan pada *interface* ISDN ppp0, maka sebaiknya di mesin yang sama dipasang *firewall* dan *router* sambungan *dial-up*-nya. Untuk selanjutnya ada baiknya membaca-baca tentang Firewall-HOWTO atau Firewalling + Masquerading + Diald + dynamic IP-HOWTO, biasa dapat ditemukan di directory `/usr/share/doc` di Linux, atau ambil sendiri ke www.linuxdoc.org.

Bagi pengguna yang memasang Snort pada mesin yang sering sekali diserang, ada baiknya memasang ACID (Analysis Console for Intrusion Databases), yang merupakan bagian dari AIR-CERT project. ACID menggunakan PHPlot, sebuah *library* untuk membuat grafik

| File | Checksum | Readme | Last Modified |
|------------------------------------|---------------------|------------------------|--------------------------|
| snort-1.8.6.tar.gz | md5 | README | Mon Apr 8 16:50:25 2002 |
| snort-1.8.5.tar.gz | md5 | | Wed Apr 3 08:44:43 2002 |
| snort-1.8.4.tar.gz | md5 | README | Sat Mar 16 01:32:36 2002 |
| snort-1.8.3.tar.gz | md5 | README | Thu Nov 29 20:46:01 2001 |
| snort-1.8.2.tar.gz | md5 | | Fri Nov 2 12:06:17 2001 |
| snort-1.8.1.tar.gz | md5 | | Fri Nov 2 12:14:23 2001 |

yang baik di PHP, dan ADODB, sebuah library abstraksi untuk menggabungkan PHP ke berbagai database seperti MySQL dan Postgre SQL.

The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of incidents generated by security-related software such as IDSes and firewalls.

ACID dapat diperoleh di www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html. Terus terang instalasi ACID sangat mudah. Mungkin yang agak membingungkan adalah menghubungkan Snort-PHP-ACID-MySQL-Apache Web server, pada kesempatan lain akan dijelaskan.

Mengoperasikan Snort

Secara umum snort dapat dioperasikan dalam tiga mode, yaitu

- **Sniffer mode**, untuk melihat paket yang lewat di jaringan.
- **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari.
- **Intrusion Detection mode**, pada mode ini Snort berfungsi mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai aturan (*rules*) yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Instalasi Snort di Linux

Secara umum teknik instalasi snort di Linux sangat mudah. Bagi pemula mungkin ada baiknya menggunakan file RPM yang jauh lebih mudah instalasinya. Pada kesempatan ini saya gunakan file tar.gz yang sedikit lebih sulit, walaupun sebetulnya tidak terlalu sulit juga. Beberapa langkah persiapan yang perlu dilakukan,

- Ambil *source snort*. Saya biasanya mengambil *source snort* yang terakhir langsung dari www.snort.org. Biasanya file *source* tersebut berbentuk *snort-*.tar.gz*.
- Copykan file *tar.gz* tersebut ke directory `/usr/local/src/`
- Buka file *snort-*.tar.gz* menggunakan perintah `# tar zxvf snort-*.tar.gz`
- Biasanya *source code* *snort* akan terlihat di folder `/usr/local/src/snort-*`
- Pastikan library untuk *capture packet (libpcap)* terinstal, jika tidak yakin dapat menggunakan *software manager* melihat apakah *libpcap* terinstal. Jika belum, instal library *libpcap* tersebut. jika anda menggunakan *Mandrake 8.0* hal ini cukup mudah dilakukan karena library tersebut terdapat pada CD *Mandrake tsb*.

Setelah semua persiapan selesai dilakukan, langkah yang perlu dilakukan untuk menginstal tidak banyak, yaitu:

- Masuk ke direktori `/usr/local/src/snort-*`
`cd /usr/local/src/snort-*`
- Konfigurasi snort menggunakan `./configure`

Untuk konfigurasi standar, praktis tidak perlu di apa-apakan. Biasanya pada saat konfigurasi ini kita akan diberitahukan jika ada modul yang kurang yang perlu diinstal, seperti libpcap dll. Usahakan untuk mencari modul tersebut di CD distribusi Linux yang anda miliki yang biasanya berbentuk RPM dan mudah di-install.

- Selanjutnya mengcompile source code menggunakan
`# make`
Pastikan pada saat di install Linux di konfigurasi untuk melakukan *development*. Jika Linux tidak diinstall untuk melakukan *development*, *compiler gcc* biasanya tidak terinstall dan kita tidak dapat menjalankan perintah `make` di atas.
- Setelah source di compile kita menginstall software `snort` menggunakan
`# make install`

Snort akan diinstal di direktori yang sebenarnya. *Default directory* tempat instalasi snort adalah `/usr/local/bin`, `/usr/local/man` dll. Tentunya kita dapat meletakkannya di direktori lain selain `/usr/local`, dengan cara memberikan pilihan `-prefix=PATH` pada saat melakukan `./configure`.

Untuk konfigurasi yang agak aneh-aneh misalnya ingin menggunakan ACID dll, maka kita perlu menambahkan beberapa switch / perintah setelah ./configure, beberapa switch yang mungkin akan digunakan seperti,

- with-snmp
Menggunakan SNMP *alerting code*.
- with-mysql=DIR
Mendukung mysql, perlu di-*on*-kan jika anda menggunakan ACID dengan MySQL.
- with-odbc=DIR
Mendukung *database* ODBC, perlu di-*on*-kan jika kita menggunakan ACID dengan *database* yang tidak ada di daftar.
- with-postgresql=DIR
Mendukung *database* Postgresql, perlu di-*on*-kan jika kita menggunakan ACID dengan PostgreSQL.
- -with-oracle=DIR
Mendukung *database* Oracle, perlu di-*on*-kan jika kita menggunakan ACID dengan Oracle.
- with-libcap-includes=DIR
Jika skrip konfigurasi gagal memperoleh directory libcap, maka anda dapat men-set secara manual melalui *switch* ini.
- with-libcap-libraries=DIR
Jika skrip konfigurasi gagal memperoleh direktori libcap, maka kita dapat men-set secara manual melalui *switch* ini.

Setelah selesai di instal, Snort dapat langsung digunakan untuk melakukan *sniffing* dan *logging*, hanya untuk Network Intrusion Detection System (NIDS) kita perlu melakukan setup atau konfigurasi Snort. Proses konfigurasi akan sangat ditolong dengan membaca manual *SnortUsersManual.pdf* yang ada di file `snort-*.tar.gz`. atau menjalankan perintah `./snort -h`

Sniffer Mode

Untuk menjalankan snort pada sniffer mode tidaklah sukar, beberapa contoh perintah-nya terdapat di bawah ini,

```
./snort -v
./snort -vd
./snort -vde
./snort -v -d -e
```

dengan menambahkan beberapa switch -v, -d, -e akan menghasilkan beberapa keluaran yang berbeda, yaitu

- v untuk melihat header TCP/IP paket yang lewat.
- d untuk melihat isi paket.
- e untuk melihat header link layer paket seperti ethernet header.

Contoh hasil sniffing paket di jaringan menggunakan perintah `/usr/local/bin/ snort -v` dapat dilihat di bawah ini:

```
[root@gate onno]# /usr/local/bin snort -v
Log directory = /var/log/snort
Initializing Network Interface eth0
```

```
--== Initializing Snort ==--
```

```
Checking PID path...
PATH_VARRUN is set to /var/run/ on this operating system
PID stat checked out ok, PID set to /var/run/
Writing PID file to "/var/run/"
Decoding Ethernet on interface eth0
```

```
--== Initialization Complete ==--
```

```
-> Snort! <-  
Version 1.8.3 [Build 88]  
By Martin Roesch (roesch@sourcefire.com, www.snort.org)  
04/18-11:32:00.261488 192.168.120.232:2757 -> 192.168.120.255:8859  
UDP TTL:64 TOS:0x0 ID:1735 IpLen:20 DgmLen:38  
Len: 18  
  
==+=+=====  
04/18-11:32:10.261514 192.168.120.232:2758 -> 192.168.120.255:8859  
UDP TTL:64 TOS:0x0 ID:1736 IpLen:20 DgmLen:38  
Len: 18  
  
==+=+=====  
04/18-11:32:20.261518 192.168.120.232:2759 -> 192.168.120.255:8859  
UDP TTL:64 TOS:0x0 ID:1737 IpLen:20 DgmLen:38  
Len: 18  
  
==+=+=====
```

Tampak bahwa antar paket selalu dibatasi tanda +=+=+=+=. Karena sniffer diaktifkan hanya menggunakan switch -v, maka hanya *header network* dan *transport protocol* yang diperlihatkan. Dalam contoh di atas protokol yang digunakan adalah Internet Protocol (IP) dan User Datagram Protocol (UDP). Kalimat pertama berisi *header IP*, beberapa informasi yang penting yang dapat dilihat di atas dari kalimat pertama adalah,

04/18-11:32:20.261518 192.168.120.232:2759 -> 192.168.120.255:8859

| | |
|-----------------|------------------------------------|
| 04 | = versi protokol IP yang digunakan |
| 192.168.120.232 | = IP address sumber paket |
| 192.168.120.255 | = IP address tujuan |
| 2759 | = port sumber |
| 8859 | = port tujuan |

Beberapa contoh perintah untuk mengaktifkan snort untuk melakukan pendeteksian penyusup, seperti

```
./snort -dev -l ./log -h 192.168.0.0/24 -c snort.conf
./snort -d -h 192.168.0.0/24 -l ./log -c snort.conf
```

Untuk melakukan deteksi penyusup secara prinsip snort harus melakukan *logging* paket yang lewat dapat menggunakan perintah `-l nama-file-logging`, atau membiarkan snort menggunakan *default* file *logging*-nya di direktori `/var/log/snort`. Kemudian menganalisa catatan atau *logging* paket yang ada sesuai dengan isi perintah `snort.conf`.

Ada beberapa tambahan perintah yang akan membuat proses deteksi lebih efisien, mekanisme pemberitahuan *alert* di Linux dapat di-set dengan perintah `-A` sebagai berikut:

- A fast, mode alert yang cepat berisi waktu, berita, IP & port tujuan.
- A full, mode alert dengan informasi lengkap.
- A unsock, mode alert ke unix socket.
- A none, mematikan mode alert.

Untuk mengirimkan *alert* ke syslog UNIX, kita bisa menambahkan switch `-s`, seperti tampak pada beberapa contoh di bawah ini.

```
./snort -c snort.conf -l ./log -s -h 192.168.0.0/24
./snort -c snort.conf -s -h 192.168.0.0/24
```

Untuk mengirimkan *alert* binari ke *workstation* Windows, dapat digunakan perintah di bawah ini:

```
./snort -c snort.conf -b -M WORKSTATIONS
```

Agar snort beroperasi secara langsung setiap kali *workstation* atau *server* di-*boot*, kita dapat menambahkan perintah di bawah ini ke file `/etc/rc.d/rc.local`

```
/usr/local/bin/snort -d -h 192.168.0.0/24 -c /root/snort/snort.conf -A full -s -D
```

atau

```
/usr/local/bin/snort -d -c /root/snort/snort.conf -A full -s -D
```

dimana -D adalah switch yang menset agar snort bekerja sebagai Daemon (bekerja dibelakang layar).

Setup snort.conf

Secara umum ada beberapa hal yang perlu di set pada `snort.conf`, yaitu:

- Set konfigurasi dari jaringan kita.
- Konfigurasi pemrosesan sebelum dilakukan proses deteksi penyusup.
- Konfigurasi output.
- Konfigurasi *rule* untuk mendeteksi penyusup.

Secara umum kita hanya perlu men-set konfigurasi jaringan saja, sedang *setting* lainnya dapat dibiarkan menggunakan *default* yang ada. Khususnya konfigurasi *rule* jika ingin mudah kita ambil saja contoh file *.rules yang ada di snort.tar.gz.

Konfigurasi jaringan yang perlu dilakukan sebetulnya tidak banyak, hanya mengisi

```
var HOME NET 192.168.0.0/24
```

memberitahukan snort IP jaringan lokal-nya adalah 192.168.0.0/24 (satu kelas C). Sisanya dapat didiamkan saja menggunakan nilai *default*-nya.

Bagian konfigurasi *output* dapat kita mainkan sedikit untuk men-set ke-mana *alert* dan informasi adanya *portscan* di-

rim, secara *default* akan dimasukkan ke `/var/log/snort`. Sedikit modifikasi perlu dilakukan jika kita ingin menggunakan ACID untuk menganalisa *alert* yang ada. *Output* perlu dimasukkan ke *database*, seperti MySQL.

Rules biasanya terdapat pada file *.rules. Untuk mengedit sendiri *rules* agak lumayan, anda membutuhkan pengetahuan yang dalam tentang protokol, *payload* serangan dll. Untuk pemula sebaiknya menggunakan contoh *.rules yang disediakan oleh snort yang dapat langsung dipakai melalui perintah *include* pada snort.conf.

Beberapa contoh rules dari serangan atau eksploit dapat dilihat berikut ini:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"EXPLOIT ssh CRC32
overflow /bin/sh"; flags:A+; content:"/bin/sh"; reference:bugtraq,2347;
reference:cve,CVE-2001-0144; classtype:shellcode-detect; sid:1324; rev:1;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"EXPLOIT ssh CRC32
overflow NOOP"; flags:A+; content:"90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90";
reference:bugtraq,2347; reference:cve,CVE-2001-0144;
classtype:shellcode-detect; sid:1326; rev:1)
```

Cukup pusing bagi pemula, rincian berbagai parameter *rules* terdapat di SnortUsersManual.pdf yang juga di sediakan bersama source snort.tar.gz.

Melihat Hasil Deteksi Penyusup

Default snort hasil deteksi penyusup atau paket yang mencurigakan akan disimpan pada folder `/var/log/snort`. Catatan kemungkinan serangan portscan akan disimpan pada file `/var/log/snort/portscan.log`, sedang untuk alert akan diletakkan pada folder-folder berdasarkan alamat IP sumber serangan karena saya menggunakan mode alert `-A full`.

Contoh cuplikan isi portscan.log dapat dilihat berikut ini,

```

Apr 4 19:00:21 202.159.32.71:110 -> 192.168.120.114:2724 NOACK 1*U*P*S*
Apr 4 20:47:43 168.143.1174:80 -> 192.168.120.114:2916 NOACK 1*U*P*S*
Apr 5 06:04:04 216.136.171.200:80 -> 192.168.120.114:3500 VECNA 1*U*P***
Apr 5 17:28:20 198.64.9.225:80 -> 192.168.120.114:1239 NOACK 1*U*P*S*
Apr 6 09:35:56 202.153.120.158:80 -> 192.168.120.114:3628 NOACK 1*U*P*S*
Apr 6 17:44:06 205.166.76.243:80 -> 192.168.120.114:1313 INVALIDACK *2*A*R*F
Apr 6 19:55:03 213.244.183.211:80 -> 192.168.120.114:43946 NOACK 1*U*P*S*
Apr 7 16:07:57 202.159.32.71:110 -> 192.168.120.114:1655 INVALIDACK *2*A*R*F
Apr 7 17:00:17 202.158.2.4:110 -> 192.168.120.114:1954 INVALIDACK *2*A*R*F
Apr 8 07:35:42 192.168.120.1:53 -> 192.168.120.114:1046 UDP
Apr 8 10:23:10 192.168.120.1:53 -> 192.168.120.114:1030 UDP
Apr 8 10:23:49 192.168.120.1:53 -> 192.168.120.114:1030 UDP
Apr 20 12:03:51 192.168.120.1:53 -> 192.168.120.114:1077 UDP
Apr 21 01:00:11 202.158.2.5:110 -> 192.168.120.114:1234 INVALIDACK *2*A*R*F
Apr 21 09:17:01 66.218.66.246:80 -> 192.168.120.114:42666 NOACK 1*U*P*S*
Apr 21 11:00:28 202.159.32.71:110 -> 192.168.120.114:1800 INVALIDACK *2*A*R*F

```

Secara umum anda akan dapat membaca tanggal dan jam serangan, IP address dan port sumber, IP address dan port tujuan, protokol yang digunakan, kesalahan yang terjadi beserta *pointer* pada protokol TCP-nya seperti,

U = Urgent
A = Acknowledge
P = Push
F = Final

Rincian dari berbagai *pointer* TCP tersebut dapat diketahui dengan membaca detail protokol TCP.

Contoh *alert* dapat dilihat berikut ini:

```

[**] INFO - Possible Squid Scan [**]
04/20-14:06:49.953376 192.168.0.33:1040 -> 192.168.0.1:3128
TCP TTL:128 TOS:0x0 ID:393 IpLen:20 DgmLen:48 DF
*****S* Seq: 0x60591B9 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) ==> MSS: 1460 NOP NOP SackOK

```

Pada contoh alert di atas, ada usaha menscan keberadaan Squid proxy server pada 192.168.0.1 port 3128 dari workstation 192.168.0.33 port 1040. Workstation 192.168.0.33 mengirimkan paket Sinkronisasi TCP terlihat dari *****S*.

SNORT & IDSCENTER

CARA MUDAH MENGENALI PENYUSUP

Selama ini **IDS** untuk sistem Windows hanyalah untuk organisasi besar yang mempunyai anggaran untuk itu, sedangkan sistem IDS yang murah hanya ada pada Unix/Linux. Tapi kini tidak lagi dengan adanya **Snort for Windows**. Lebih jauh lagi **IDSCenter** membuat semuanya lebih mudah.

Snort for Windows seperti juga windump dan dsniiff (dibahas di NeoTek Vol. II No. 7) memerlukan WinPCap untuk dapat berjalan.

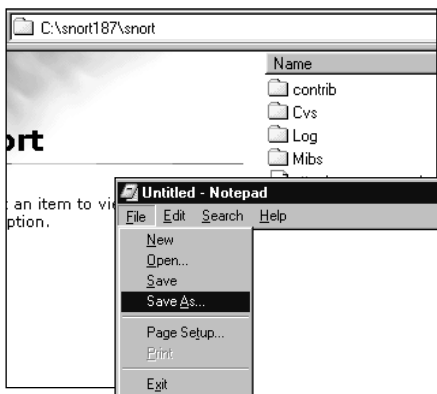
Snort for Windows bersama WinPCap saja sudah dapat berjalan di latar belakang melalui perintah command line:

C:\>snort -A full -c snort.conf -D

Tapi kini sudah ada IDSCenter yang merupakan GUI bagi Snort for Windows yang menjadikan Snort for Windows mudah dan nyaman digunakan.

Untuk studi lanjutan, Snort dapat juga dikonfigurasi bersama database MySQL dan ACID (Analysis Console for Intrusion Databases) pada NT.

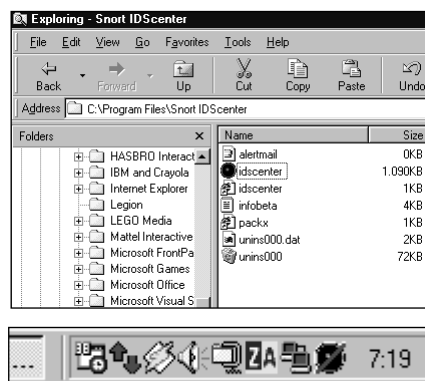
Dengan adanya IDSCenter, menjalankan Snort pada Windows amatlah mudah



4

SIAPKAN FOLDER LOG

Di direktori \snort187\snort terdapat tiga folder: contrib, Cvs, dan Mibs. Buat folder baru dengan nama **Log** dan di dalam folder itu buat file kosong bernama **alert.ids.txt**. Caranya buka Notepad dan file kosong di-save sebagai nama itu pada folder tersebut.



5

JALANKAN IDSCENTER

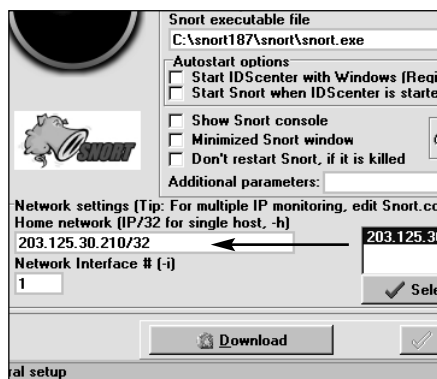
Double click pada ikon **idcenter** di direktori \Program Files\Snort IDSCenter dan pada bagian kanan bawah layar akan terlihat ikon loudspeaker (lingkaran hitam) yang dicoret garis merah. Ini menunjukkan IDSCenter sudah di-load tetapi belum di-Start.



6

MENAMPILKAN IDSCENTER

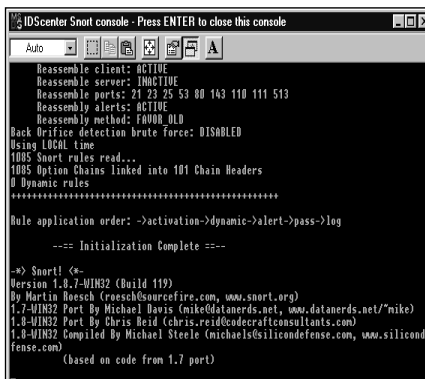
Double click pada ikon loudspeaker di bagian kanan bawah window itu dan panel IDSCenter akan ditampilkan. Kini kita akan mengkonfigurasi **IDSCenter** untuk berjalan **bersama** program intinya yaitu **Snort for Windows**.



10

NETWORK SETTING

Pada keadaan komputer terhubung ke Internet, kita kembali ke General Setting dan perhatikan di kolom kanan bawah Snort sudah mengenali IP Address komputer kita. Klik **Select** untuk memilih IP Address ini sebagai pos penjagaan kita dan IP Address itu diisikan di kolom kiri.



11

MENGUJI KONFIGURASI

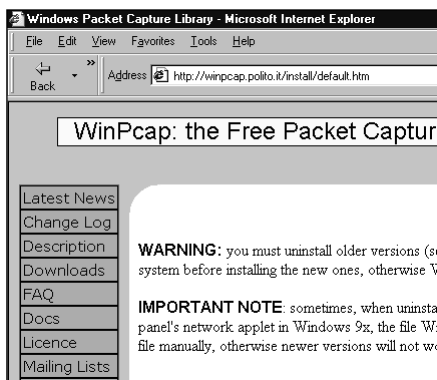
Uji konfigurasi ini apakah sudah berjalan baik, pertama kali klik tombol **Create Script**. Script adalah ringkasan informasi lokasi-lokasi snort.exe, snort.conf, dan alert.ids.txt yang kita tetapkan sebelumnya. Klik **Test Configuration**. Bila berhasil tidak ada pesan error.



12

START SNORT

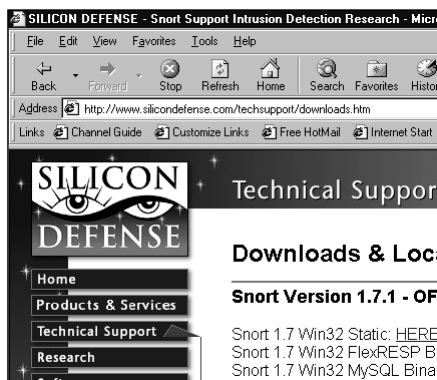
Semua di atas dijalankan sewaktu Snort tidak berjalan. Untuk menjalankan Snort klik tombol **Start Snort** dan kini network anda sudah dilengkapi network-based IDS. Tampak di bagian kanan bawah ikon loudspeaker sudah tidak lagi dicoret



1

DOWNLOAD WINPCAP

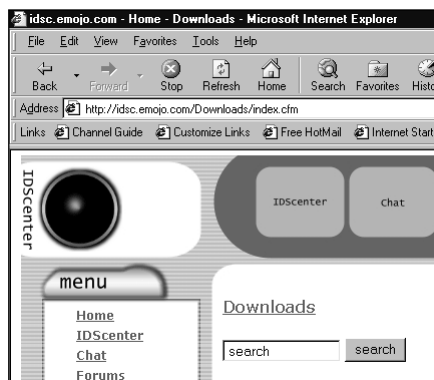
Snort memanfaatkan **WinPcap** untuk menangkap paket-paket data yang lalu-lalang melalui network. Download WinPcap di <http://winpcap.polito.it/install/default.htm> atau dapat juga menginstalnya dari CD NeoTek.



2

DOWNLOAD SNORT

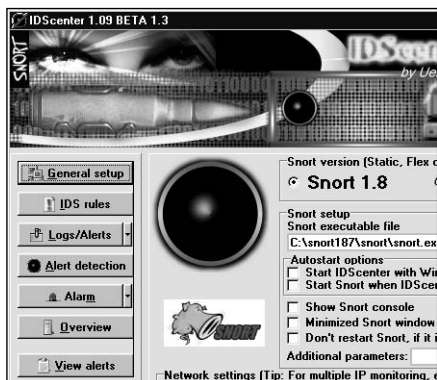
Selanjutnya download **Snort** di <http://www.silicondefense.com/techsupport/downloads.htm>. Ada beberapa versi Snort yang tersedia. Download dan instal Snort for Windows versi 1.7 dan versi 1.8.7. Misal pada direktori C:\snort187.



3

DOWNLOAD IDSCENTER

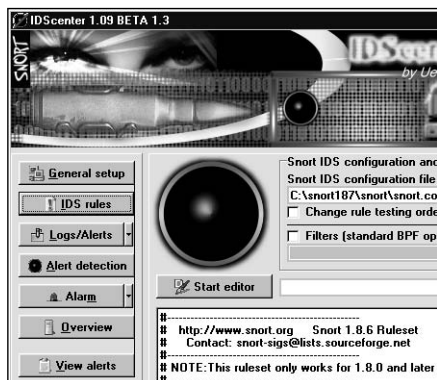
Download **IDSCenter 1.09beta 1.3** di <http://idsc.emojo.com/Downloads/index.cfm>. Setelah itu instal IDSCenter ini. Kini kita siap untuk menggabungkan ketiga software ini menjadi network-based IDS di Windows.



7

GENERAL SETUP

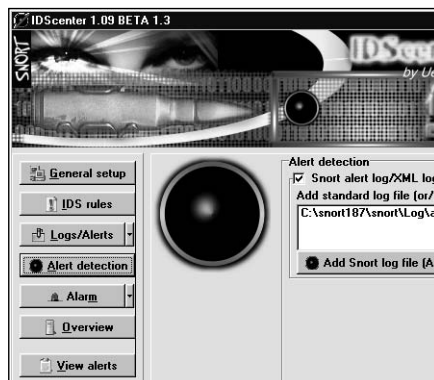
Pada General Setup terdapat pilihan akan menggunakan Snort 1.8 atau 1.7. Karena kita menginstal salah satu versi 1.8, pilih **Snort 1.8** dan pada kolom Snort executable file browse dan open snort.exe yang ada. Pada contoh ini pada C:\snort187\snort\snort.exe



8

IDS RULES

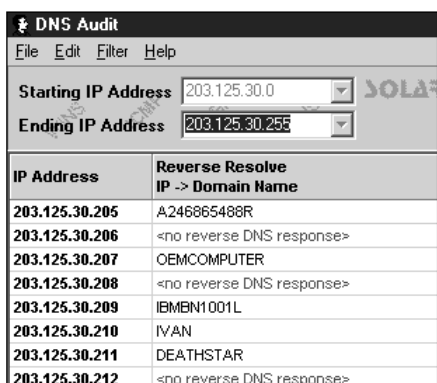
Pada IDS Rules, kita menetapkan di mana terdapat file **snort.conf** yang dalam contoh ini terdapat di C:\snort187\snort\snort.conf. File ini dapat diedit untuk menetapkan aturan-aturan yang diinginkan dalam melakukan deteksi. Untuk kali ini gunakan yang ada saja.



9

LOGS/ALERTS

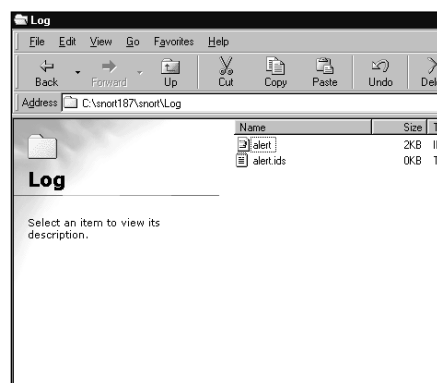
Pada Logs/Alerts kita menetapkan di mana kita akan menyimpan file log dari hasil monitoring lalu-lintas paket data pada sistem kita ini. Dalam hal ini pada file **alert.ids.txt** yang telah kita siapkan sebelumnya di C:\snort187\snort\Log>alert.ids.txt



13

KOMPUTER PENYERANG

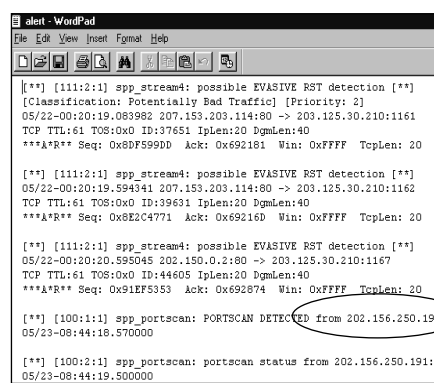
Pada contoh ini dilakukan scan dengan fasilitas **DNS Audit** dari **Solarwinds**. Dari hasil scan IP Address 203.125.30.0 sampai 203.125.30.255 terlihat bahwa IP Address 203.125.30.210 adalah komputer dengan nama **IVAN** (komputer dengan Snort ini)



14

FILE ALERT.TXT TERBENTUK

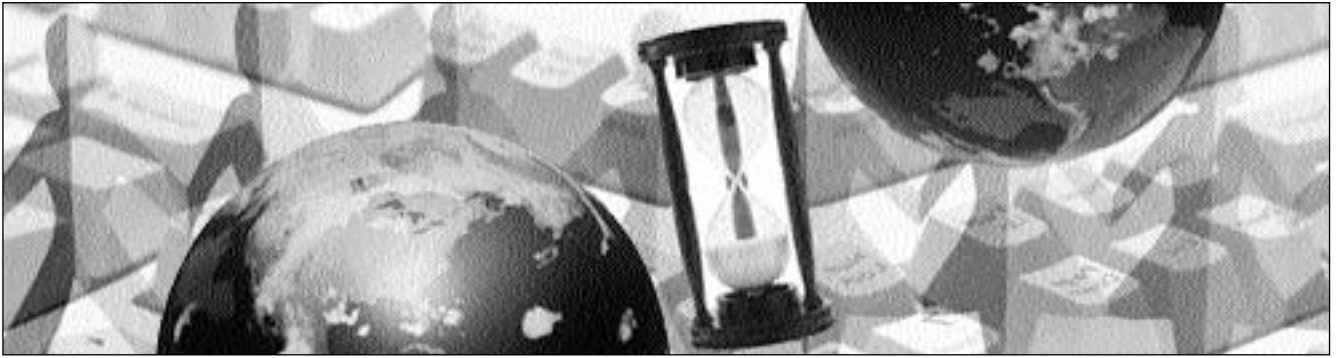
Di folder C:\snort187\snort\Log ini selain file alert.ids.txt yang kita buat tadi, telah terbentuk pula file **alert.txt** yang ukurannya tidak nol (2 kbyte). Ini tentunya hasil capture Snort terhadap lalu-lintas paket data. Buka file ini dengan Notepad atau Wordpad.



15

SIAPA YA SI ISENG?

Dari file file alert.txt terlihat adanya intrusi berupa port scanning yang berasal dari mesin dengan IP Address 202.156.250.151. Gunakan **tracert**, **nslookup**, serta **whois** untuk melacak siapa si iseng ini.



PORTSENTRY

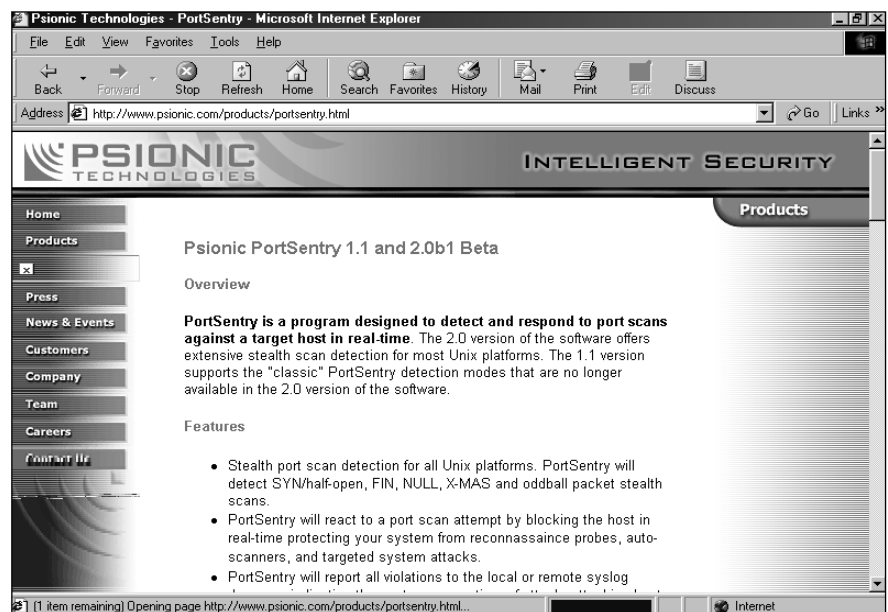
Penjaga Serangan Portscan di Jaringan

Apabila Network-based IDS seperti Snort memonitor paket data yang lalu-lalang di jaringan dan mengamati adanya pola-pola serangan, maka **PortSentry** dikhususkan untuk menjaga port yang memang dibuka oleh sistem kita. **Onno W. Purbo** membahasnya untuk kita.

Mengapa kita perlu mendeteksi Port Scan? Jawaban versi hebohnya kira-kira sebagai berikut, Port Scan adalah awal dari masalah besar yang akan datang melalui jaringan. Port Scan merupakan awal serangan dan hasil Port Scan membawa beberapa informasi kritis yang sangat penting untuk pertahanan mesin & sumber daya yang kita miliki. Keberhasilan untuk menggagalkan Port Scan akan menyebabkan kita tidak berhasil memperoleh informasi strategis yang dibutuhkan sebelum serangan yang sebetulnya dilakukan.

PortSentry dapat di terjemahkan ke bahasa Indonesia sebagai Penjaga Gerbang/Pelabuhan. Sentry berarti penjaga, Port dapat diterjemahkan gerbang atau pelabuhan. Sekedar latar belakang informasi, pada jaringan komputer (Internet), masing-masing server aplikasi akan stand-by pada port tertentu, misalnya, Web pada port 80, mail (SMTP) pada port 25, mail (POP3) pada port 110. PortSentry adalah program yang di disain untuk mendeteksi dan merespond kepada kegiatan port scan pada sebuah mesin secara real-time.

PortSentry tersedia untuk berbagai platform Unix, termasuk Linux, OpenBSD & FreeBSD. Versi 2.0 dari PortSentry memberikan cukup banyak fasilitas untuk mendeteksi scan pada berbagai mesin Unix. Versi 1.1 mendukung mode deteksi PortSentry yang klasik yang tidak lagi digunakan pada versi 2.0. PortSentry 2.0 membutuhkan library libpcap untuk dapat di jalankan,



biasanya sudah tersedia berbentuk RPM dan akan terinstall secara otomatis jika anda menggunakan Linux Mandrake. Bagi yang tidak menggunakan Linux Mandrake dapat mengambilnya dari situs tcpdump.org.

Pembaca dapat mengambil PortSentry langsung dari sumbernya di <http://www.psionic.com/products/portentry.html>. Source portsentry terdapat dalam format tar.gz atau .rpm.

Bagi pengguna Mandrake 8.0, PortSentry telah tersedia dalam CD-ROM dalam format RPM. Instalasi PortSentry menjadi amat sangat mudah dengan di bantu oleh program Software Manager. Yang kita lakukan tinggal:

- Mencari PortSentry dalam paket program.
- Pilih (Klik) PortSentry.
- Klik Install maka PortSentry.

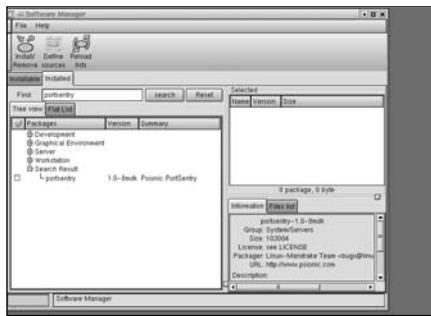
Secara automagic anda akan memperoleh PortSentry.

Bagi pengguna Mandrake 8.2 ternyata PortSentry tidak dimasukan dalam CD ROM Mandrake 8.2, jadi anda harus menggunakan CD Mandrake 8.0 untuk mengambil PortSentry dan menginstallnya.

Beberapa fitur yang dimiliki oleh PortSentry, antara lain:

- Mendeteksi adanya Stealth port scan untuk semua platform Unix. Stealth port scan adalah teknik port scan yang tersa-

- Instalasi PortSentry pada Linux Mandrake 8.0 sangat mudah.



mar/tersembunyi, biasanya sukar di deteksi oleh sistem operasi.

- PortSentry akan mendeteksi berbagai teknik scan seperti SYN/half-open, FIN, NULL dan X-MAS. Untuk mengetahui lebih jelas tentang berbagai teknik ini ada baiknya untuk membaca-baca manual dari software nmap yang merupakan salah satu software portscan terbaik yang ada.
- PortSentry akan bereaksi terhadap usaha port scan dari lawan dengan cara membolkiir penyerang secara real-time dari usaha auto-scanner, probe penyelidik, maupun serangan terhadap sistem.
- PortSentry akan melaporkan semua kejanggalan dan pelanggaran kepada software daemon syslog lokal maupun remote yang berisi nama sistem, waktu serangan, IP penyerang maupun nomor port TCP atau UDP tempat serangan di lakukan. Jika PortSentry di-dampingkan dengan LogSentry, dia akan memberikan berita kepada administrator melalui e-mail.
- Fitur cantik PortSentry adalah pada saat terdeteksi adanya scan, sistem anda tiba-tiba menghilang dari hadapan si penyerang. Fitur ini membuat penyerang tidak berkutik.
- PortSentry selalu mengingat alamat IP penyerang, jika ada serangan Port Scan yang sifatnya random PortSentry akan bereaksi.

Salah satu hal yang menarik dari PortSentry adalah bahwa program ini dirancang agar dapat dikonfigurasi secara sederhana sekali dan bebas dari keharusan memelihara.

Beberapa hal yang mungkin menarik dari kemampuan PortSentry antara lain: PortSentry akan mendeteksi semua hubungan antar-komputer menggunakan protokol TCP maupun UDP. Melalui file konfigurasi yang ada PortSentry akan memonitor ratusan port yang di scan secara berurutan maupun secara random. Karena PortSentry juga memonitor protokol UDP, PortSentry akan memberitahukan kita jika ada orang yang melakukan probing (uji coba) pada servis RPC, maupun servis UDP lainnya seperti TFTP, SNMP dll.

Setup Parameter PortSentry

Setup Parameter PortSentry dilakukan secara sangat sederhana melalui beberapa file yang berlokasi di

/etc/portsentry

adapun file-file tersebut adalah

```
always_ignore
portsentry.blocked.atcp
portsentry.blocked.audp
portsentry.conf
portsentry.history
portsentry.ignore
portsentry.modes
```

dari sekian banyak file yang ada, yang perlu kita perhatikan sebetulnya tidak banyak hanya

- Always_ignore—yang berisi alamat IP yang tidak perlu di perhatikan oleh PortSentry.
- Portsentry.conf—yang berisi konfigurasi portsentry, tidak terlalu sukar untuk di mengerti karena keterangannya cukup lengkap.

Mengedit portsentry.conf tidak sukar & dapat dilakukan menggunakan teks editor biasa saja. Sebetulnya portsentry dapat langsung bekerja hampir tanpa perlu mengubah file konfigurasi yang ada. Beberapa hal yang perlu diperhatikan dalam mengedit konfigurasi file portsentry.conf adalah:

- Konfigurasi Port—disini di set port mana saja di komputer yang kita gunakan yang perlu di perhatikan. Pada konfigurasi port ini

tersedia juga pilihan untuk menghadapi advanced stealth scan.

- Pilihan untuk melakukan respons (Reponds Options—seperti Ignore options yang memungkinkan kita mengacuhkan serangan, menghilang dari tabel routing yang mengakibatkan paket dari penyerang tidak diproses routingnya, setting untuk TCP Wrappers yang akan menyebabkan paket dari penyerang tidak akan masuk ke server.
- Serang balik—ini adalah bagian paling berbahaya dari PortSentry, pada file konfigurasi PortSentry telah disediakan link untuk menyambungkan / menjalankan script untuk menyerang balik ke penyerang. Bagian ini sebaiknya tidak digunakan karena akan menyebabkan terjadinya perang Bharatayudha.

Dari sekian banyak parameter yang ada di konfigurasi file portsentry.conf, saya biasanya hanya menset bagian routing table saja untuk menghilangkan semua paket dari penyerang yang mengakibatkan paket tidak di proses. Kebetulan saya menggunakan Mandrake 8.0 yang proses paket dilakukan oleh iptables, kita cukup menambahkan perintah di bagian Dropping Routes: dengan perintah iptables.

```
# PortSentry Configuration
```

```
# $Id: portsentry.conf,v 1.13 1999/11/09 02:45:42 crowland Exp
crowland $
```

```
# IMPORTANT NOTE: You CAN NOT put spaces between your port
arguments.
```

```
# The default ports will catch a large number of common probes
```

```
# All entries must be in quotes.
```

```
#####
```

```
# Dropping Routes:#
```

```
#####
```

```
# For those of you running Linux with ipfwadm installed you may
like
```

```
# this better as it drops the host into the packet filter.
```

```
# You can only have one KILL_ROUTE turned on at a time though.
```

```
# This is the best method for Linux hosts.
```

```
#
```

```
#KILL_ROUTE="/sbin/ipfwadm -I -i deny -S $TARGET$ -o"
```

```
#
```

```
# This version does not log denied packets after activation
```

```
#KILL_ROUTE="/sbin/ipfwadm -I -i deny -S $TARGET$"
```

```
#
```

```
# New ipchain support for Linux kernel version 2.102+
```

```
# KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -I"
```

```
#
```

```
# New iptables support for Linux kernel version 2.4+
```

```
KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"
```

Cek Adanya Serangan

Untuk mengecek adanya serangan, ada beberapa file dan perintah yang dapat dilihat, yaitu:

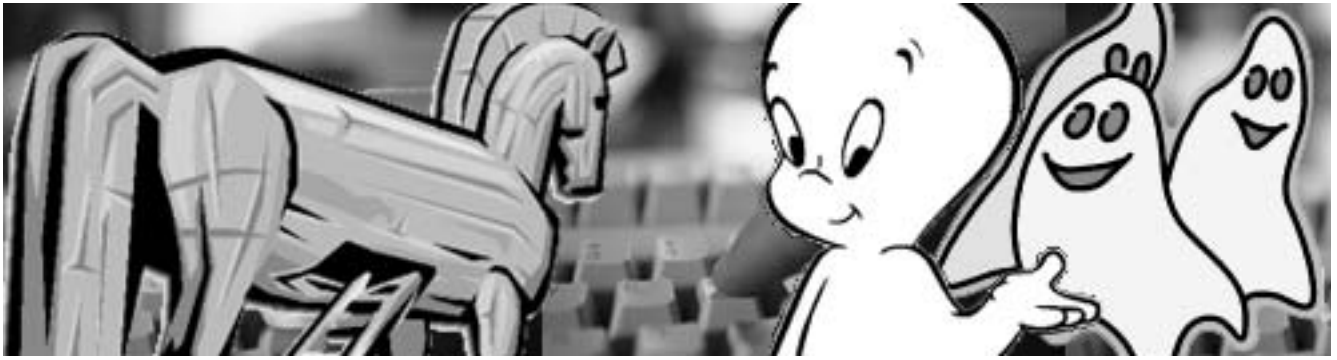
- /etc/hosts.deny—berisi daftar IP mesin yang tidak diperkenankan untuk berinteraksi ke server kita. Daftar ini di gunakan oleh TCP Wrappers & di hasilkan secara otomatis oleh PortSentry pada saat serangan di lakukan.
- /etc/portsentry/portsentry.blocked.atcp—daftar alamat IP mesin yang di blok akses-nya ke semua port TCP.
- /etc/portsentry/portsentry.blocked.audp—daftar alamat IP mesin yang di blok akses-nya ke semua port UDP.
- /etc/portsentry/portsentry.history—sejarah serangan yang diterima oleh mesin kita.

Pada Mandrake 8.0 dan Mandrake 8.2, untuk melihat paket yang di tabel paket filter oleh PortSentry dapat dilakukan menggunakan perintah:

```
# iptables -L
```

Jika hanya PortSentry yang digunakan maka tabel filter iptables seluruhnya secara otomatis di hasilkan oleh PortSentry. Untuk membuang semua tabel filter dapat dilakukan dengan perintah:

```
# iptables -F
```

PROGRAM SILUMAN

Mewaspadaai Penyusup di PC Anda

Trojan dapat menyelinap dan dijalankan tanpa anda ketahui. Berbagai **program siluman** dapat saja masuk ke komputer anda melalui jaringan, sewaktu anda berinternet seperti chatting, browsing, ataupun men-download program tertentu. **Eryanto Sitorus** membahas cara mensiasatinya.

Menghubungkan komputer ke jaringan Internet adalah suatu aktifitas yang paling menyenangkan dan sekaligus mengasyikkan, terutama setelah anda terhubung ke dalam server tempat di mana anda biasa ngobrol (chatting), belanja (shopping), melihat-lihat informasi (surfing), mengirim dan membaca email, men-download atau mengupload file, melakukan eksperimen, mengutak-atik BNC, PsyBNC, Eggdrop, dan sebagainya.

Akan tetapi jika anda tidak berhati-hati atau waspada, apalagi sampai tidak memperdulikan program-program aplikasi yang terinstal di dalam hard disk anda, maka itu adalah awal dari bencana yang akan menimpa komputer anda sebagai konsekuensi dari hubungan tersebut. Karena bukan tidak mungkin di saat anda sedang mengakses Internet, atau sedang asyik ngobrol di IRC, tanpa anda sadari ada orang lain yang juga sedang asyik mengakses file-file dan semua sumber daya di dalam komputer anda, dan hal itu terjadi akibat adanya salah satu aplikasi atau program yang aktif tanpa sepengetahuan anda dan secara tidak sengaja telah membuat pintu khusus bagi orang lain untuk memasuki sistem komputer anda.

Oleh karena itu pemahaman dan pengetahuan dalam konteks keamanan (*security*) mutlak anda miliki agar komputer anda luput dari bahaya. Dan di sisi lain, anda pun akan merasa aman (*secure*) saat terhubung dan berselancar di Internet. Sebaliknya, jika Anda tidak memiliki dua hal pokok tersebut,



yakni pemahaman dan pengetahuan untuk mengantisipasi dan mengatasi bahaya, maka yang anda rasakan adalah kekhawatiran, gelisah, dan rasa takut seperti yang di alami seorang kenalan saya di Internet yang mengaku sering terkejut ketika mendengar hard disk komputernya berbunyi pertanda sedang sibuk (*busy*) dalam waktu yang cukup lama setiap kali terhubung ke Internet, padahal dia cuma memeriksa mail menggunakan Internet Explorer sambil sesekali ngobrol di IRC dan tidak sedang menjalankan program-program aplikasi besar atau sedang mendownload sesuatu yang meng-



haruskan piringan hard disknya berputar selama itu. Akhirnya, karena khawatir ada orang lain yang telah masuk dan sedang mengakses komputernya, maka dia pun buru-buru memutuskan koneksi ke ISP (Internet Service Provider) tanpa melakukan investigasi terlebih dahulu untuk mencari tahu apa penyebabnya dan dari mana sumbernya. Dan satu hal lagi yang membuat saya juga merasa *surprise* adalah, ternyata bukan cuma kenalan saya yang mengalami keanehan seperti itu, hal senada juga sering ditanyakan oleh para peserta *chat* di IRC yang mengaku pernah mengalami kejadian-kejadian aneh di komputer mereka.

Dari penjelasan dan alasan-alasan yang dikemukakan tersebut di atas, dapat kita simpulkan bahwa ternyata faktor keamanan itu juga penting, khususnya bagi anda yang mengakses Internet melalui sistem operasi Microsoft Windows 95/98/ME/2000/XP atau NT. Karena sudah bukan rahasia umum lagi, bahwa sistem operasi yang paling gampang disusupi oleh para hacker atau cracker adalah sistem operasi yang diproduksi oleh Microsoft (Bill Gates).

Namun anda tidak perlu terlalu khawatir, apalagi sampai buru-buru mengambil keputusan untuk segera mengganti sistem operasi Microsoft Windows anda dengan sistem operasi lain yang sama sekali tidak anda pahami. Karena selain cara itu, masih ada solusi atau cara lain yang bisa anda implementasikan dalam rangka mengatasi kelemahan-kelemahan yang ada pada sistem anda, misalnya dengan memasang perangkat sistem keamanan seperti **proxy**, **firewall**, **router**, atau **gateway**. Tujuannya adalah untuk memfilter dan mengontrol semua lalu-lintas data (*packet*) yang masuk pada tingkat aplikasi maupun pada jaringan *transport layer* yang selama ini cukup dipercaya mampu melindungi komputer dari gangguan hacker atau cracker.

Jika anda memilih cara tersebut, maka anda bisa memulainya dengan menginstal program-program proxy berbasis firewall seperti **Zone Alarm** atau **Blackice** di komputer anda. Software-software ini bisa anda peroleh dengan gratis di alamat (URL) berikut ini :

Zone Alarm

<http://www.webmasterfree.com>
<http://www.zone-alarm-pro.com>
<http://www.webattack.com>
<http://www.softseek.com>
<http://www.pcworld.com>

Blackice

<http://www.lml.se/blackice.htm>
<http://www.securelab.com>
<http://www.iss.net>
<http://www.aragoza.com>
<http://www.infowar.com>

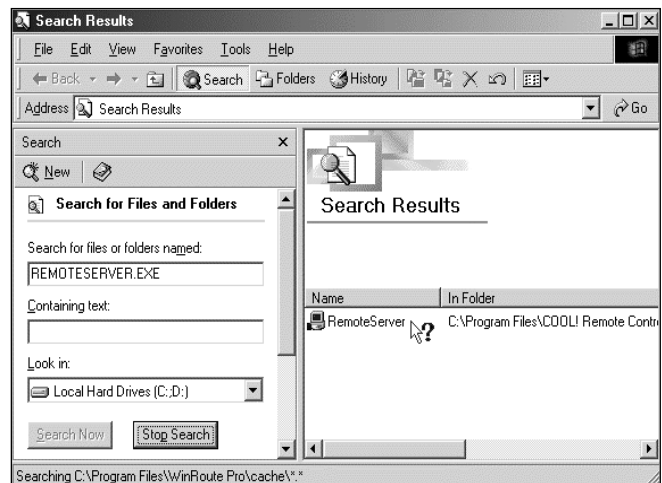
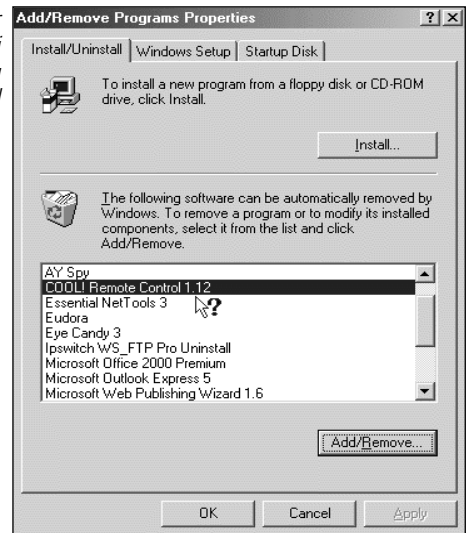
Namun sebelum anda menginstal perangkat lunak seperti yang disebutkan di atas, saya ingin menjelaskan bahwa sebenarnya masih ada cara lain yang jauh lebih sederhana dan praktis tapi cukup ampuh untuk melindungi komputer anda, yaitu dengan cara mewaspadai dan memeriksa semua program aplikasi yang terinstal dan yang sedang aktif di sistem komputer anda. Karena seperti yang sudah dijelaskan di atas, salah satu faktor yang menyebabkan orang lain bisa masuk ke dalam komputer adalah terjadi akibat aplikasi atau program yang secara tidak sengaja telah membuat pintu khusus bagi orang lain untuk memasuki sistem komputer anda. Adapun prosedur atau langkah-langkah pemeriksaannya dapat dijelaskan sebagai berikut:

1. Masuk lah ke dalam jendela **Control Panel**, lalu klik menu icon **Add/Remove Programs** untuk memeriksa semua daftar program atau aplikasi yang terinstal pada sistem komputer anda. Jika anda menemukan suatu program yang sama sekali tidak anda ketahui apa manfaat dan fungsinya, maka usahakan lah untuk menemukan direktori atau folder tempat program itu terinstal terlebih dahulu. Kemudian buka file README.TXT atau file-file yang lain di mana anda bisa membaca deskripsi

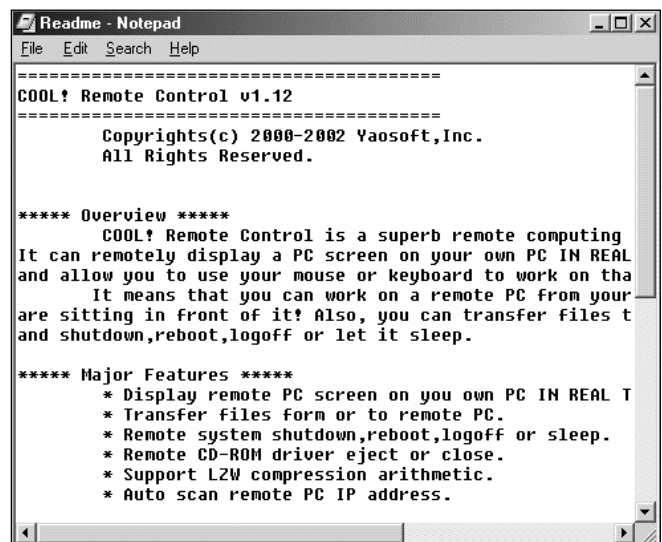
•Melihat daftar program/aplikasi yang sudah diinstal

tentang program tersebut. Apabila anda kesulitan menemukan direktori atau program tersebut, anda bisa memanfaatkan fungsi "search" dengan mengklik menu

Start > Find > Files or Folders, lalu ketik nama program yang ingin anda cari. Dan setelah anda menemukan dan membacanya, tapi anda masih tetap tidak tahu apa manfaat serta fungsi program tersebut, maka lakukanlah proses uninstall dengan mengklik tombol **Add/Remove** pada jendela **Add/Remove Program Properties**.

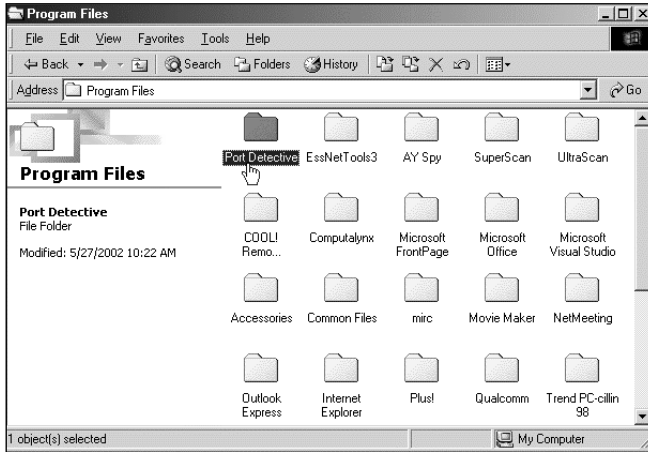


•Mencari letak direktori/program dengan menggunakan Find.



•Membaca deskripsi program/aplikasi dengan Notepad

2. Buka Windows Explorer, lanjutkan investigasi dengan memeriksa setiap direktori atau folder yang terdapat pada semua drive hard disk komputer anda. Tapi agar waktu anda tidak terlalu banyak tersita, maka anda cukup memprioritaskan pemeriksaan pada program-program yang ada dalam folder C:\PROGRAM FILES atau pada direktori-direktori yang anda curigai saja. Dan jika anda menemukan sesuatu yang aneh dan mencurigakan, maka lakukanlah hal yang sama seperti yang disarankan pada butir 1.

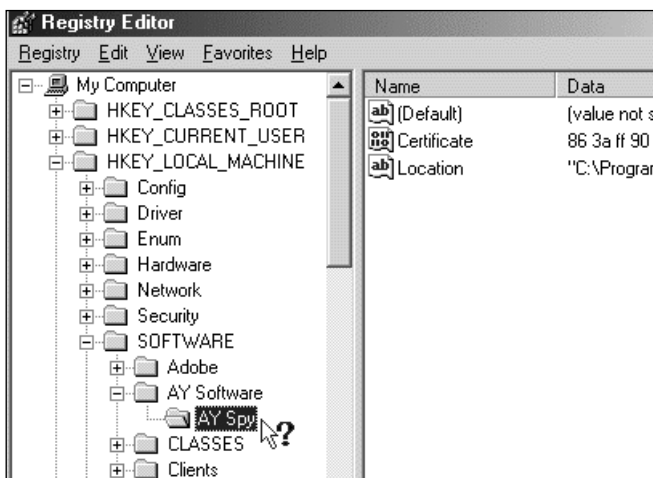


•Memeriksa program/aplikasi menggunakan Windows Explorer

3. Klik tombol **Start > Run**, lalu ketik **regedit** untuk menjalankan program Registry Editor (REGEDIT.EXE) yang akan kita pakai untuk memeriksa folder HKEY_CURRENT_USER dan HKEY_LOCAL_MACHINE.

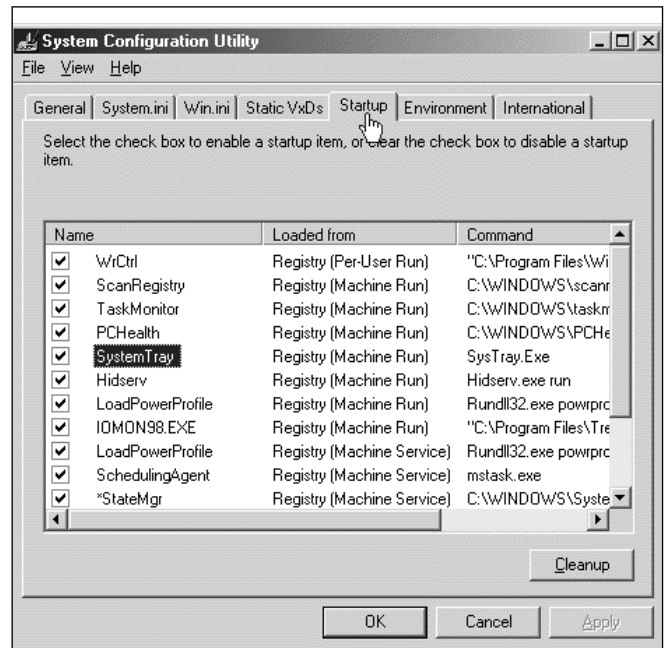


•Menjalankan program Regedit dari menu Run



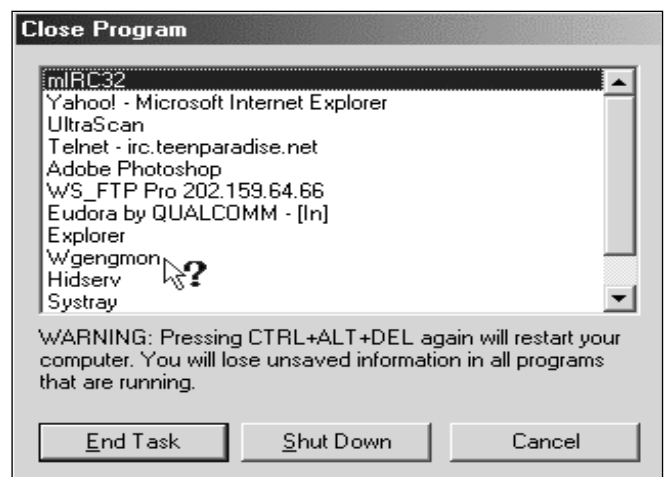
•Memeriksa program/aplikasi menggunakan Regedit

Jika anda masih tidak menemukan sesuatu yang mencurigakan, maka lanjutkan pemeriksaan ke tahap berikutnya.



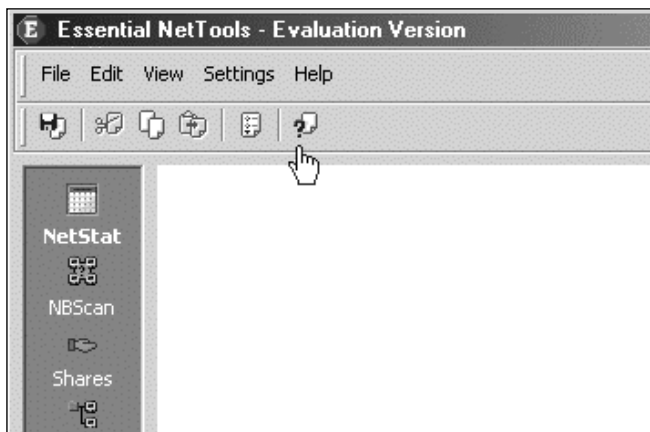
•Memeriksa program/aplikasi yang load secara otomatis (Startup)

4. Klik tombol **Start > Run**, lalu jalankan program **System Configuration Utility** (MSCONFIG.EXE) untuk memeriksa semua setting dan konfigurasi yang terdapat pada tab Startup. Pada tahap ini, pastikan bahwa tidak ada program atau aplikasi yang sama sekali tidak anda kenal aktif secara otomatis (startup). Dan jika anda menemukan sesuatu (program) yang aneh, dan anda tidak tahu apa fungsi dan kegunaannya, maka usahakanlah mencari dan membaca informasinya terlebih dahulu sebelum anda menghilangkan symbol [✓].



•Memeriksa program/aplikasi yang sedang aktif

5. Tekan tombol **Ctrl-Alt-Del** untuk memeriksa daftar program aplikasi yang sedang aktif saat itu, termasuk program-program lain yang sifatnya TSR (*terminate-and-stay-resident*). Jangan lupa, pada tahap ini anda sudah melakukan pemeriksaan yang jauh lebih teknis dari pada sebelumnya, oleh karena itu waspada lah, karena akan sangat besar kemungkinan bagi anda untuk melihat program-program aneh yang sedang aktif di komputer anda. Jika anda mencurigai sesuatu, maka klik lah tombol End Task untuk menutup atau menonaktifkannya dari memory komputer. Namun sebelum anda melakukannya, pastikan bahwa anda sudah melacak lokasi dimana program tersebut tersimpan dan membaca deskripsinya.



•Tampilan utility Essential NetTools.

Selain cara tersebut di atas, anda juga bisa mengandalkan program (*utility*) untuk membantu anda melakukan pemeriksaan dengan cara yang lebih mudah, singkat, praktis, namun juga akurat. Salah satu utility yang bisa anda pakai adalah Essential NetTools, yang diproduksi oleh TamoSoft, Inc. Jika anda tertarik menggunakannya, download software tersebut di alamat situs berikut ini:

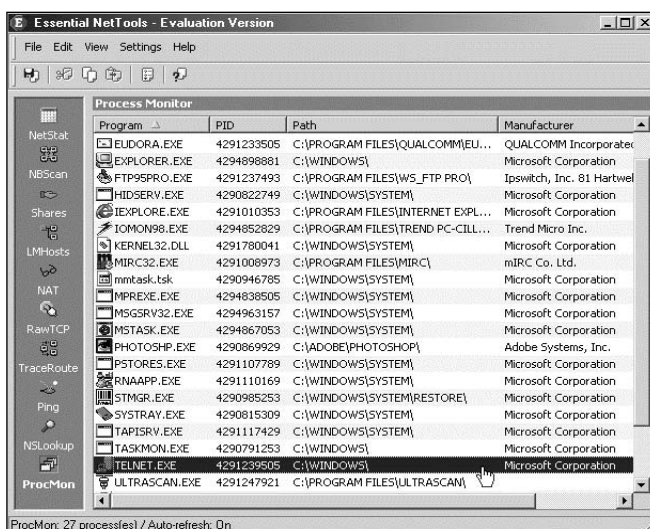
Essential NetTools

<http://www.tamofiles.com/ent3.zip>

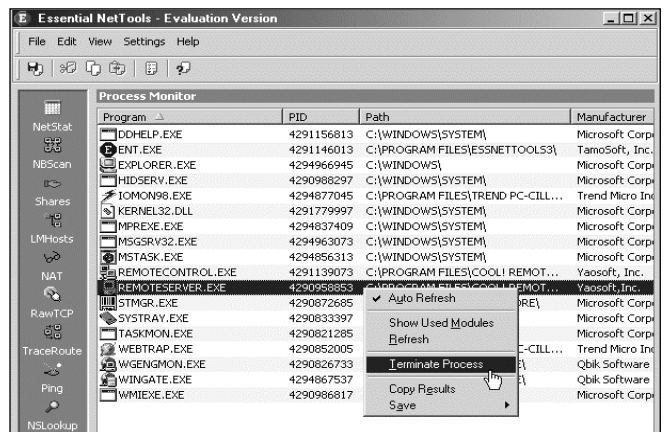
<http://www.all-nettools.com/ent3.zip>

Secara teknis, Essential NetTools adalah utility jaringan paling lengkap yang dirancang khusus untuk membantu anda melakukan diagnosa serta memonitor seluruh aktifitas dan hubungan yang berasal dari dan ke jaringan komputer (Intranet maupun Internet). Disebut paling lengkap, karena memang Essential NetTools memiliki fitur-fitur yang cukup penting.

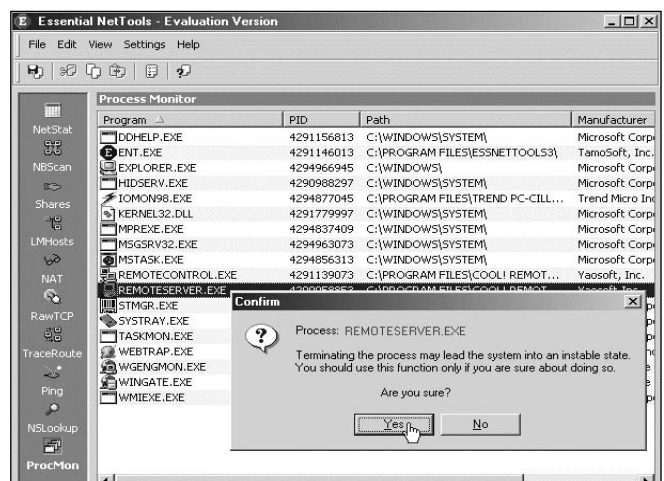
Salah satu fitur yang dimiliki Essential NetTools adalah **ProcMon** (Process Monitor). Dengan ProcMon anda dapat mengidentifikasi semua program atau aplikasi yang bekerja secara tersembunyi berikut informasi lain yang menyertainya, misalnya seperti nama program, nama lokasi atau direktori tempat program tersebut di instal, nomor PID (Process ID), modul yang ikut di load, serta nama perusahaan pembuatnya. Dan jika anda ingin menonaktifkannya dari sistem komputer anda (kill), maka anda cukup mengklik tombol mouse kanan dan memilih menu Terminate Process.



•Memeriksa program/aplikasi menggunakan Essential NetTools.



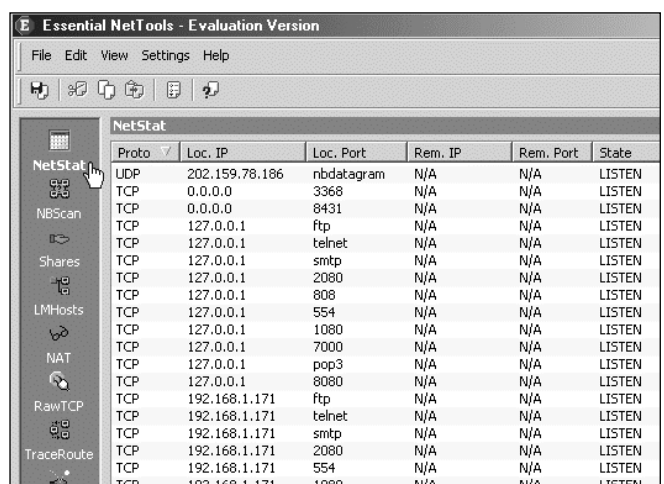
•Meng-kill program yang sedang aktif menggunakan Essential NetTools.



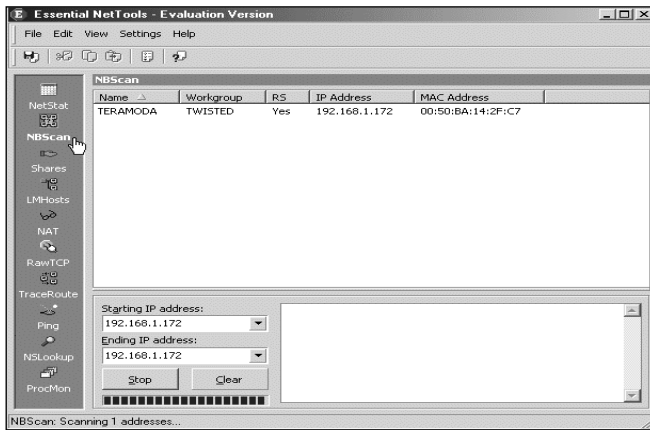
•Meminta konfirmasi sebelum perintah kill (terminate) dilaksanakan.

Adapun fitur-fitur lain yang bisa anda gunakan pada utility Essential NetTools antara lain:

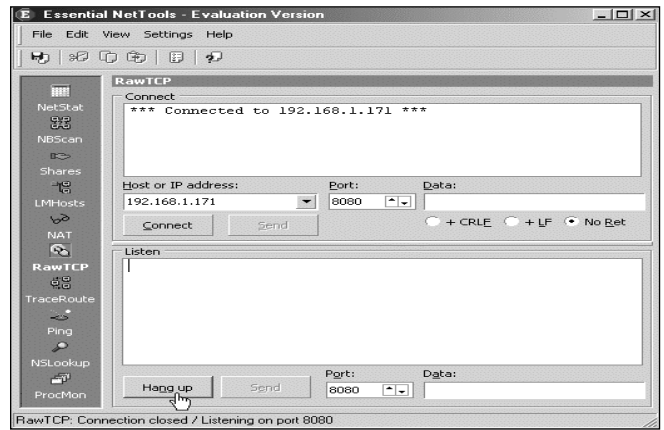
NetStat
NBScan (NetBIOS Scan)
Shares
LMHosts
NAT (NetBIOS Auditing Tool)
RawTCP
TraceRoute
Ping
NSlookup



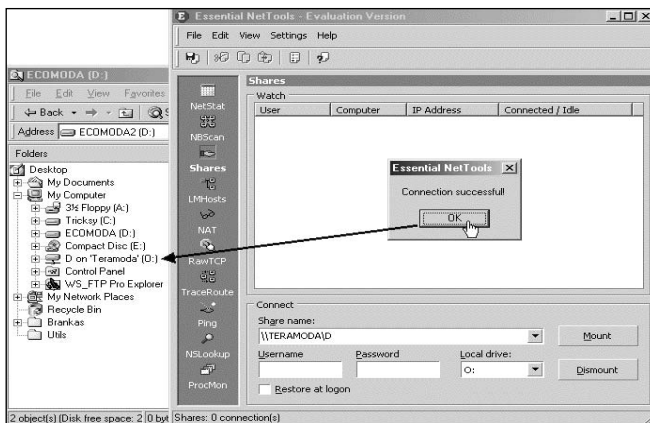
•Contoh tampilan utility NetStat.



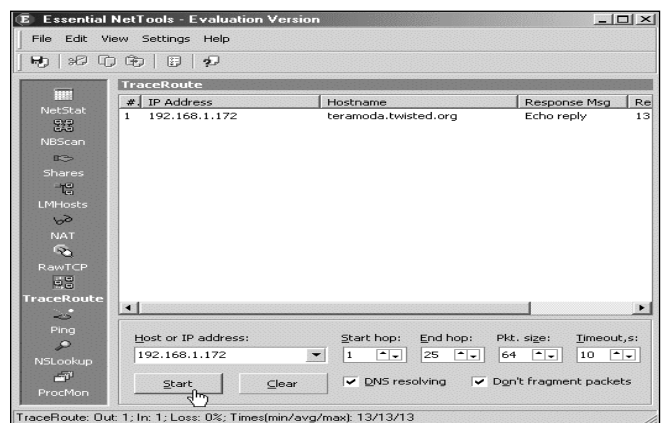
•Contoh tampilan utility NBScan (NetBIOS Scan)



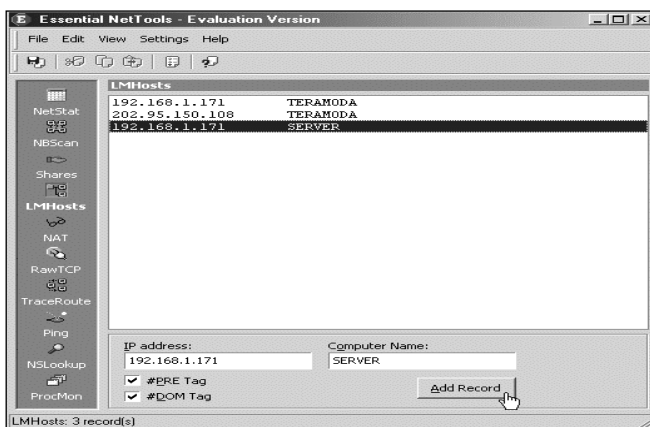
•Contoh tampilan utility RasTCP.



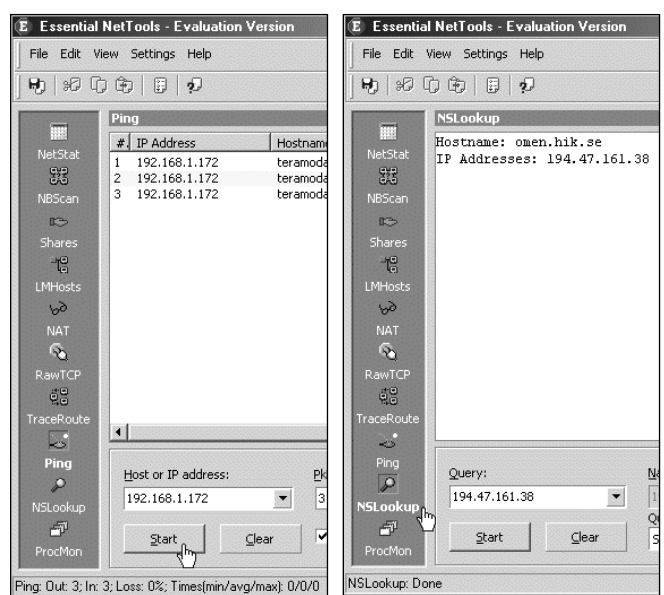
•Contoh tampilan utility Shares



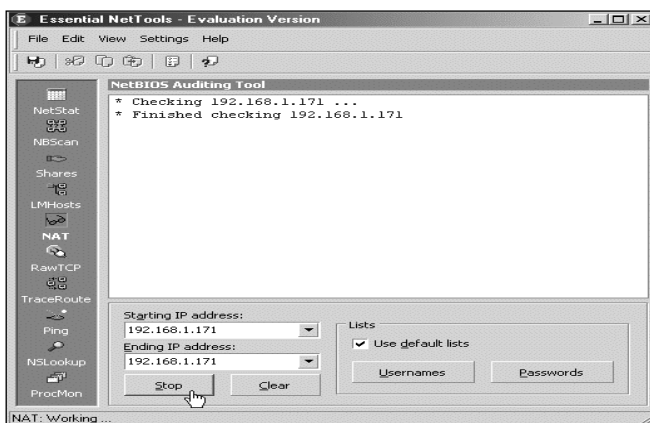
•Contoh tampilan utility TraceRoute.



•Contoh tampilan utility LMHost



•Contoh tampilan utility Ping dan NSLookup.



•Contoh tampilan utility NAT (NetBOS Auditing Tool)

Akhir kata saya ingin mengingatkan anda sekali lagi, bahwa meskipun anda sudah menginstal perangkat sistem keamanan untuk melindungi atau mengamankan sistem komputer anda, namun seyogyanya anda juga harus tetap waspada dan tanggap terhadap semua yang terjadi pada komputer anda, karena sebaik apa pun sistem operasi yang ada pakai, atau sebgas apa pun perangkat sistem keamanan yang anda gunakan tetap saja akan memiliki kendala, kelemahan, dan kekurangan. Itu adalah kunci atau solusi yang paling jitu untuk menghindari PC anda dari serangan hacker.

Menjalankan Program Saat Pertama Kali Windows Dijalankan

Untuk melengkapi artikel-artikel mengenai trojan dan kegiatan susup-menyusup serta cara mengatasinya, disajikan pula artikel tentang 'Menjalankan Program Saat Pertama Kali Windows Dijalankan.'

Ada beberapa cara untuk menjalankan program saat Windows pertama kali Start. Hal ini bisa kita gunakan untuk kemudahan dan efisiensi kita dalam bekerja, namun dalam banyak kasus hal ini sering digunakan oleh virus atau trojan untuk meng-execute dirinya di komputer kita.

Cara menjalankan program secara otomatis ini adalah sebagai berikut:

1. Pada start up folder

Semua Program yang ada di folder ini akan dijalankan secara otomatis ketika Windows di jalankan.

C:\windows\start menu\programs\startup

Direktori diatas tersimpan di registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell

2. Win.ini

```
[windows]
load=file.exe
run=file.exe
```

Pada load dan run bisa kita isikan nama program yang kita inginkan berjalan pada saat pertama windows dijalankan.

3. System.ini [boot]

Shell=Explorer.exe file.exe

Nama Program dapat diletakan setelah explorer.exe pada system.ini(dipisahkan dengan spasi)

4. c:\windows\winstart.bat

Program yang dapat berjalan di winstart.bat hanya yang berperilaku seperti bat file, missal, copy, del, dll.

5. Pada Registry

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
```

Program yang terdapat pada registry key diatas semuanya dijalankan saat pertama windows start.

6. c:\windows\wininit.ini

Biasa digunakan oleh Setup-Programs. filenya akan dijalankan hanya sekali lalu akan di hapus oleh windows

Contoh: (isi bagian dari wininit.ini)

```
[Rename]
NUL=c:\windows\file.exe
```

Perintah diatas akan mengirim c:\windows\file.exe ke proses NUL, yang berarti dihapus. Hal ini tidak membu-

tuhkan interaksi dari user dan berjalan sepenuhnya di background.

7. Autoexec.bat

Akan menjalankan program secara otomatis dalam dos level.

8. Registry Shell Spawning

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\comfile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\batfile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\piffile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] @="\"%1\" \"%*"
```

Value key yang sesungguhnya adalah "%1 %*", jika dirubah menjadi "file.exe %1 %*", maka

file.exe akan di jalankan setiap program yang berekstensi exe/pif/com/bat/hta dijalankan.

Dan biasa digunakan oleh trojan SubSeven.

9. Icq Inet

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
```

```
"Path"="test.exe"
"Startup"="c:\\test"
"Parameters"=""
"Enable"="Yes"
```

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\
```

Registry key diatas termasuk semua program yang akan dijalankan jika ICQNET mendeteksi adanya koneksi internet.

10. Lain-lain

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap]
```

```
@="Scrap object" "NeverShowExt"=""
```

Bagian " NeverShowExt " key mempunyai fungsi untuk menyembunyikan ekstensi asli dari file.shs, yang berarti jika kita mempunyai file bernama "Girl.jpg.shs" yang akan terlihat adalah "Girl.jpg" di semua program termasuk Explorer.

Jika registri anda terdapat NeverShowExt keys, delete key tersebut agar ekstensi yang sesungguhnya dapat terlihat...

Penulis dapat dihubungi di Prayana1@yahoo.com

Menjalankan Program Saat Pertama Kali Windows Dijalankan

Untuk melengkapi artikel-artikel mengenai trojan dan kegiatan susup-menyusup serta cara mengatasinya, disajikan pula artikel tentang 'Menjalankan Program Saat Pertama Kali Windows Dijalankan.'

Ada beberapa cara untuk menjalankan program saat Windows pertama kali Start. Hal ini bisa kita gunakan untuk kemudahan dan efisiensi kita dalam bekerja, namun dalam banyak kasus hal ini sering digunakan oleh virus atau trojan untuk meng-execute dirinya di komputer kita.

Cara menjalankan program secara otomatis ini adalah sebagai berikut:

1. Pada start up folder

Semua Program yang ada di folder ini akan dijalankan secara otomatis ketika Windows di jalankan.

C:\windows\start menu\programs\startup

Direktori diatas tersimpan di registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell

2. Win.ini

```
[windows]
load=file.exe
run=file.exe
```

Pada load dan run bisa kita isikan nama program yang kita inginkan berjalan pada saat pertama windows dijalankan.

3. System.ini [boot]

Shell=Explorer.exe file.exe

Nama Program dapat diletakan setelah explorer.exe pada system.ini(dipisahkan dengan spasi)

4. c:\windows\winstart.bat

Program yang dapat berjalan di winstart.bat hanya yang berperilaku seperti bat file, missal, copy, del, dll.

5. Pada Registry

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
```

Program yang terdapat pada registry key diatas semuanya dijalankan saat pertama windows start.

6. c:\windows\wininit.ini

Biasa digunakan oleh Setup-Programs. filenya akan dijalankan hanya sekali lalu akan di hapus oleh windows

Contoh: (isi bagian dari wininit.ini)

```
[Rename]
NUL=c:\windows\file.exe
```

Perintah diatas akan mengirim c:\windows\file.exe ke proses NUL, yang berarti dihapus. Hal ini tidak membu-

tuhkan interaksi dari user dan berjalan sepenuhnya di background.

7. Autoexec.bat

Akan menjalankan program secara otomatis dalam dos level.

8. Registry Shell Spawning

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\comfile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\batfile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command]
@="\"%1\" \"%*"
```

```
[HKEY_CLASSES_ROOT\piffile\shell\open\command]
@="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] @="\"%1\" \"%*"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] @="\"%1\" \"%*"
```

Value key yang sesungguhnya adalah "%1 %*", jika dirubah menjadi "file.exe %1 %*", maka

file.exe akan di jalankan setiap program yang berekstensi exe/pif/com/bat/hta dijalankan.

Dan biasa digunakan oleh trojan SubSeven.

9. Icq Inet

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
```

```
"Path"="test.exe"
"Startup"="c:\\test"
"Parameters"=""
"Enable"="Yes"
```

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\
```

Registry key diatas termasuk semua program yang akan dijalankan jika ICQNET mendeteksi adanya koneksi internet.

10. Lain-lain

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap]
```

```
@="Scrap object" "NeverShowExt"=""
```

Bagian " NeverShowExt " key mempunyai fungsi untuk menyembunyikan ekstensi asli dari file.shs, yang berarti jika kita mempunyai file bernama "Girl.jpg.shs" yang akan terlihat adalah "Girl.jpg" di semua program termasuk Explorer.

Jika registri anda terdapat NeverShowExt keys, delete key tersebut agar ekstensi yang sesungguhnya dapat terlihat...

Penulis dapat dihubungi di Prayana1@yahoo.com



Percabangan pada JavaScript

Pada bagian keempat dari tutorial JavaScript ini kami memperkenalkan **percabangan**, yang mengatur eksekusi program mengikuti **alur logika bersyarat** dengan **if**, **if ... else**, dan **switch**

DALAM KEADAAN NORMAL, ALUR program JavaScript adalah berurutan (*sequence*), artinya baris *statement* yang di atas akan terlebih dahulu dikerjakan, kemudian berurutan ke baris *statement* di bawahnya dan seterusnya demikian sampai semua baris dieksekusi.

Akan tetapi mungkin saja suatu saat alur seperti ini menjadi kurang efektif, misalnya saja jika kita dihadapkan pada pilihan apakah akan mengerjakan ini atau mengerjakan itu, atau mungkin ketika ada beberapa *statement* yang harus dikerjakan secara berulang-ulang sekian kali.

Dalam JavaScript, dan umumnya semua bahasa pemrograman yang terstruktur, ada tiga macam alur dasar yang mendasari semua jenis aplikasinya yakni:

1. Urutan (Sequence)
2. Percabangan (Branch)
3. Perulangan (Looping)

Semua aplikasi yang dibuat mengacu pada ketiga alur dasar tersebut, mungkin salah satunya saja, atau kombinasi ketiganya.

Percabangan

Definisi

Alur yang bercabang, terdapat kondisi yang diuji untuk menentukan cabang mana yang akan dikerjakan dan cabang mana yang tidak. Intinya adalah adanya pemilihan apakah suatu kelompok *statement* (dalam satu cabang) akan dieksekusi atau tidak, bergantung pada kondisi disyaratkan.

Dalam Javascript, alur percabangan ini dapat dibuat dengan :

- a. If statement
- b. If ... else statement
- c. Switch statement

If statement

Digunakan untuk melakukan pilihan, apakah suatu kelompok *statement* akan

dieksekusi atau tidak dengan kondisi yang diuji. Jika kondisi benar maka eksekusi akan dikerjakan, jika kondisi salah, kelompok *statement* tersebut akan dilewati begitu saja tanpa ada eksekusi.

Sintaksnya adalah sebagai berikut:

```
if(kondisi yang diuji)
{
  ---statement javascript
  ---statement javascript
  ---statement javascript
}
```

Contoh penggunaan

Perhatikan contoh berikut:

```
<!-- contoh 4.1 -->
<!-- simpan dalam format .html -->
<html>
<head>
<title>Percabangan dengan if</title>
</head>
<body>
<script language="javascript">
<!--
var jam = new Date()
var sekarang = jam.getHours()
if(sekarang < 10)
{
  document.write("Selamat Pagi!")
}
document.write("<br>Sekarang waktu sekitar jam "+
sekarang)
//-->
</script>
</body>
</html>
```

Pada contoh di atas, **If statement** akan mencek apakah jam yang diperoleh adalah lebih kecil dari 10? Jika ya, maka akan dituliskan dalam dokumen HTML ucapan "Selamat Pagi" kemudian diikuti dengan penulisan kalimat penunjuk waktu. Akan tetapi jika tidak, maka ucapan "Selamat Pagi" tidak akan dituliskan.

Dalam percabangan **If statement**, hanya ada dua kemungkinan, yaitu apakah suatu kelompok *statement* akan diekse-

kusi ataukah tidak, jika tidak maka akan dilewati begitu saja. Ingat yang dieksekusi hanya satu kelompok *statement* saja. Jika kita memiliki lebih dari satu kelompok *statement*, yang satu akan dieksekusi ketika kondisi terpenuhi, dan yang lain ketika kondisi tidak terpenuhi, maka kita harus menggunakan **If ... else statement**.

If ... else statement

Digunakan untuk melakukan pemilihan, kelompok *statement* mana yang akan dieksekusi dengan menguji suatu kondisi. Jika kondisi terpenuhi, maka satu kelompok *statement* akan dieksekusi, jika kondisi tidak terpenuhi, maka kelompok *statement* lain yang akan dieksekusi. Sintaksnya adalah sebagai berikut:

```
if(kondisi yang diuji)
{
  ---statement javascript
  ---statement javascript
  ---statement javascript
}
else
{
  ---statement javascript
  ---statement javascript
  ---statement javascript
}
```

Contoh penggunaan

Perhatikan contoh berikut:

```
<!-- contoh 4.2 -->
<!-- simpan dalam format .html -->
<html>
<head>
<title>Percabangan dengan if ... else</title>
</head>
<body>
<script language="javascript">
<!--
var jam = new Date()
var sekarang = jam.getHours()
if(sekarang < 10)
{
  document.write("Selamat Pagi!")
}
else
{
  document.write("Selamat Datang!")
}
```



```

}
//-->
</script>
</body>
</html>

```

Pada contoh di atas, setelah kondisi diuji, maka If statement akan mengeksekusi blok statement yang pertama (setelah if) jika kondisi terpenuhi, dan akan mengeksekusi blok statement yang kedua (setelah else) jika kondisi tidak terpenuhi.

Perbedaan pokok dari statement if dengan statement if ... else adalah pada statement if ada dua kemungkinan yaitu dieksekusi atau tidaknya satu kelompok statement, sedangkan pada if ... else ada satu kemungkinan yaitu eksekusi terhadap kelompok statement yang satu atau kelompok statement yang satunya lagi.

Nested If

Yaitu If ... else statement yang berada di dalam If ... else statement.

Suatu kali mungkin kita kondisi yang diuji tidak hanya satu kondisi saja, dalam hal ini maka dapat digunakan nested If.

Perhatikan contoh berikut:

```

<!-- contoh 4.3 -->
<!-- simpan dalam format .html -->
<html>
<head>
<title>Percabangan dengan nested if</title>
</head>
<body>
<script language="javascript">
<!--
var jam = new Date()
var sekarang = jam.getHours()
if(sekarang < 10)
{
document.write("Selamat Pagi!")
}
else
{
if(sekarang > 20)
{
document.write("Selamat Malam!")
}
else
{
document.write("Selamat Datang!")
}
}
//-->
</script>
</body>
</html>

```

Secara ringkas contoh di atas dapat dijelaskan sebagai berikut: pertama kali statement if ... else akan menguji kondisi, jika kondisi terpenuhi maka blok statement setelah statement if akan dieksekusi, sedangkan jika kondisi tidak terpenuhi maka blok statement setelah else yang akan dieksekusi, akan tetapi ternyata blok statement setelah statement else adalah suatu percabangan lagi yang akan diproses seperti statement if sebelumnya. Demikian seterusnya.

Switch Statement

Digunakan jika ingin dipilih satu saja dari sekian banyak kelompok statement yang memiliki nilai label yang berbeda-beda.

Sintaks umumnya sebagai berikut:

```

switch (ekspresi)
{
case label1 :
... statement javascript
break
case label2 :
... statement javascript
... statement javascript
break
default :
... statement javascript
... statement javascript
}

```

Cara kerja statement switch adalah sebagai berikut. Pertama kali satu ekspresi (sering kali adalah suatu variabel) dimasukkan ke dalam statement switch. Kemudian oleh ekspresi tersebut akan dilihat nilainya satu kali saja. Selanjutnya switch statement akan membandingkan nilai variabel dengan label pada masing-masing *case*. Jika sama maka statement pada *case* tersebut akan dieksekusi demikian seterusnya. Jika ternyata tidak ada yang cocok maka statement pada bagian *default* yang akan dikerjakan.

Statement Break

Statement break digunakan untuk menghentikan proses eksekusi. Penggunaan statement break pada syntax *case* diatas adalah untuk mencegah kemungkinan eksekusi terhadap *case* sesudahnya, karena itu statement break ditempatkan pada baris akhir dari kelompok statement pada masing-masing *case*. Perhatikan contoh penggunaan statement switch berikut :

```

<!-- contoh 4.4 -->
<!-- simpan dalam format .html -->
<html>
<head>
<title>Percabangan dengan switch</title>
</head>
<body>
<script language="javascript">
<!--
var hari = new Date()
var sekarang = hari.getDay()
switch(sekarang)
{
case 1:
document.write("Hari ini adalah Hari Senin!")
break
case 2:
document.write("Hari ini adalah Hari Selasa!")
break
case 3:
document.write("Hari ini adalah Hari Rabu!")
break
case 4:
document.write("Hari ini adalah Hari Kamis!")
break
case 5:
document.write("Hari ini adalah Hari Jumat!")
break
case 6:
document.write("Hari ini adalah Hari Sabtu!")
break
default:
document.write("Hari ini adalah Hari Minggu!")
}
//-->
</script>
</body>
</html>

```

Pada contoh-contoh di atas kita telah menggunakan objek tanggal yang akan kita pelajari lebih detail pada bagian yang lain.

Operator Kondisional

Selain operator-operator yang kita pelajari pada bagian sebelumnya, dalam JavaScript dikenal juga adanya operator kondisional, yang akan memberikan satu nilai jika kondisi yang diuji benar dan memberikan nilai yang lain jika kondisi yang diuji salah.

Sintaksnya adalah sebagai berikut:

```
namavariabel = (kondisi yang diuji)? nilai1 : nilai2
```

Perhatikan contoh berikut ini:

```

<!-- contoh 4.4 -->
<!-- simpan dalam format .html -->
<html>
<head>
<title>Percabangan dengan switch</title>
</head>
<body>
<script language="javascript">
<!--
var jam = new Date()
var sekarang = jam.getHours()
var x
x = (sekarang < 10)? "Selamat Pagi!" : "Selamat Datang!"
document.write(x)
//-->
</script>
</body>
</html>

```

Seminar Hacking dan Keamanan Jaringan

Majalah NeoTek
dengan CV Hujunggaluh
menyelenggarakan seminar

'Hacking dan Keamanan Jaringan'

29 Agustus 2002
Grand Candi Jotel
Semarang

Pemrasaran:
Onno W. Purbo
(Redaktur Ahli Majalah NeoTek)

yang ditujukan untuk karyawan yang dalam pekerjaan sehari-harinya menggunakan komputer serta jaringan (termasuk Internet) Dibahas tiga macam bahaya ang mengancam komputer dan data pekerjaan:

- Serangan lokal
- Bahaya dari Internet
- Serangan hacker terhadap jaringan

Undangan dapat diperoleh di CV Hujunggaluh, Jl. Nakula I/48-50, Semarang. Telp. 024-3521458

PGP FREEWARE 7.0.3

INSTALASI DAN MENGIRIM 'GEMBOK'

Melanjutkan bahasan ringkas enkripsi pada NeoTek Vol. II No. 7 (April 2002), kali ini kita bahas **PGPfreeware** (Pretty Good Privacy) karya Phil Zimmermann yang dapat digunakan sebagai plugin di Outlook, OE, Eudora. maupun ICQ dan Virtual Personal Network. Dapat juga untuk **web mail**.

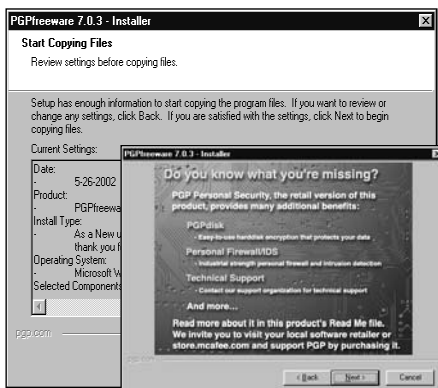
Konsep PGP sederhana namun brilian. Seseorang membentuk public key (gembok) dan private key (anak kunci) sekaligus. Public key dikirim ke rekan korespondensi sedangkan private key disimpan sendiri.

Rekan kita nanti akan mengirim email yang di-encrypt menggunakan public key kita (calon penerima) dan setelah diterima oleh kita baru bisa dibuka oleh penerima dengan private key-nya.

Setelah di-encrypt, pengirim asli pun tidak dapat membukanya kembali (decrypt) karena tidak memiliki private key-nya.

Bayangkan bahwa kita mengirim gembok untuk dipakai mengirim barang untuk kita tapi anak kuncinya tidak kita kirimkan.

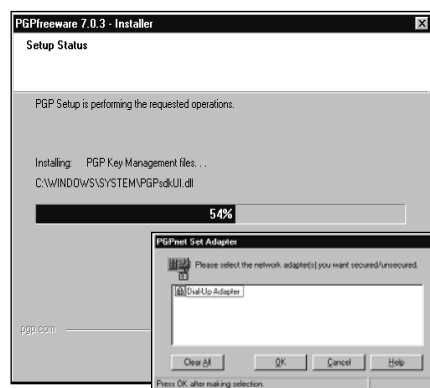
Konsep gembok dan anak kunci akan memudahkan memahami konsep PGPfreeware



4

COPYING FILES

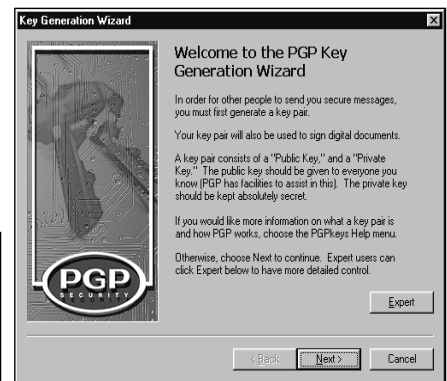
File-file yang diperlukan untuk instalasi akan di-copy ke hard disk anda. Sebelum melanjutkan akan tampil 'iklan' yang menunjukkan apa kelebihan versi komersial dari PGPfreeware, yaitu PGP Personal Security.



5

SETUP SYSTEM

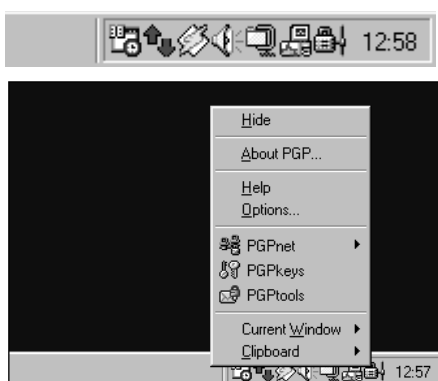
PGPfreeware akan otomatis di-setup sesuai konfigurasi komputer anda. Pada contoh ini komputer yang digunakan mengakses Internet melalui dial-up adapter sehingga adapter itu yang akan diamankan. Bila ada LAN card, LAN card itu yang akan ditampilkan.



6

PGP KEY GENERATION WIZARD

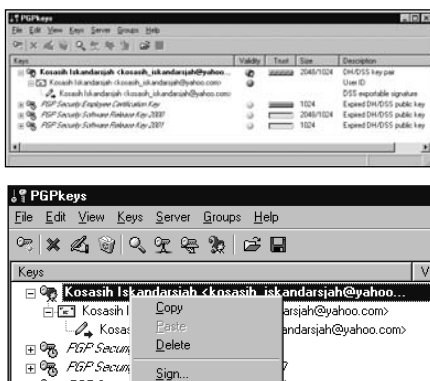
Kini saatnya membentuk 'anak kunci' (**private key**) dan 'gembok' (**public key**). Akan tampil jendela PGP Key Generation Wizard. Klik **Expert** untuk melihat opsi-opsinya. Bila klik Next, akan secara otomatis dipilih opsi-opsi default.



10

PGP TERPASANG

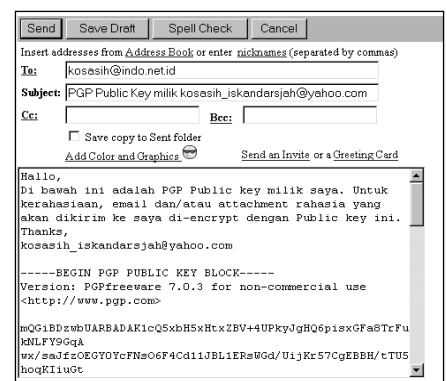
Setelah boot ulang, pada start up tray sebelah kanan bawah terlihat ikon berbentuk **gembok dengan anak kunci**, yang bila diklik akan menampilkan pull up menu. Pilih **PGPkeys** untuk melihat key yang sudah kita buat. Akan tampil jendela berisi key yang baru terbentuk. Hijau artinya secure.



11

COPY 'GEMBOK' KE CLIPBOARD

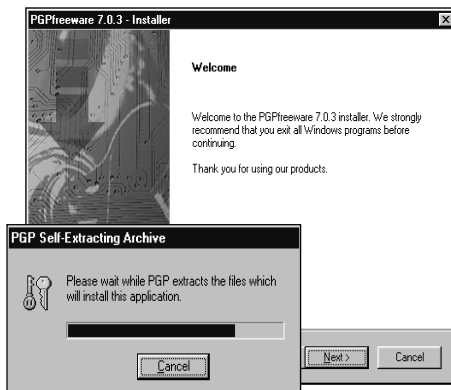
Klik **kanan** pada key paling atas yang akan menampilkan menu. Klik kiri pada opsi **Copy** dan public key (gembok) akan di-copy ke Clipboard. Selanjutnya buka program email (dalam hal ini web mail Yahoo di **mail.yahoo.com**) dan pilih **Compose**.



12

MENGIRIM 'GEMBOK'

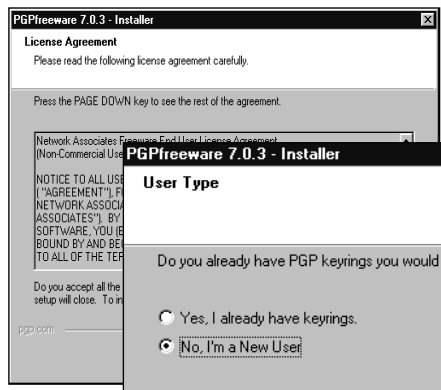
Tulis surat pengantar bahwa anda mengirim public key dan agar sang penerima nanti men-encrypt dulu email rahasianya dengan public key ini sebelum mengirimkannya pada anda. Dalam contoh ini public key dikirim ke **kosasih@indo.net.id** oleh **kosasih_iskandarsjah@yahoo.com**



1

INSTAL PGPFREWARE 7.03

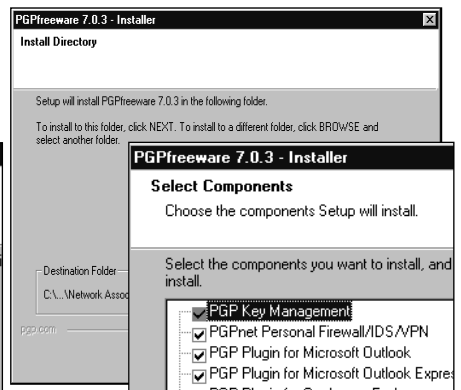
Instal PGPfreeware 7.03 dari CD NeoTek atau dapat juga dari hasil download di <http://www.cnet.com/software/0-806183-8-4792641-1.html>. Setelah self-extracting dan install shield wizard, klik **Next**.



2

USER TYPE

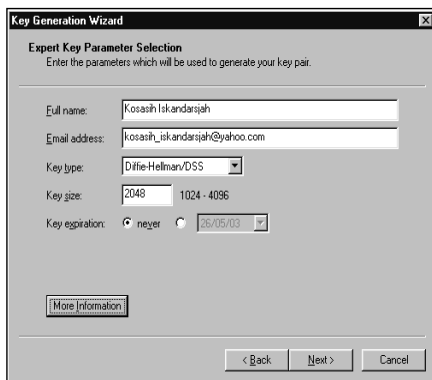
Setelah menyetujui lisensinya, anda diminta memasukkan user type. Karena belum pernah mempunyai keyring (anak kunci) sebelumnya, maka pilih opsi kedua yaitu **No, I'm a New User**. Teruskan dengan **Next**.



3

INSTALASI PLUG-IN

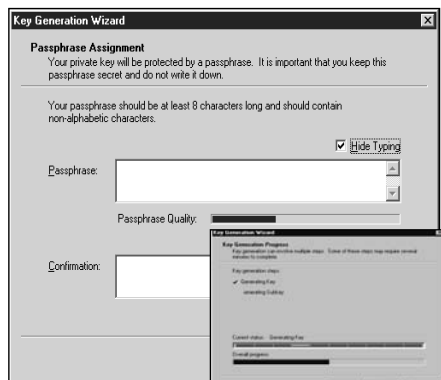
PGPfreeware akan diinstal pada default directory di bawah folder Program Files. Kita ikuti saja ini dan selanjutnya akan ditampilkan jendela plug-in untuk apa saja yang akan di-install. Di antaranya untuk Outlook dan Outlook Express.



7

PARAMETER-PARAMETERNYA

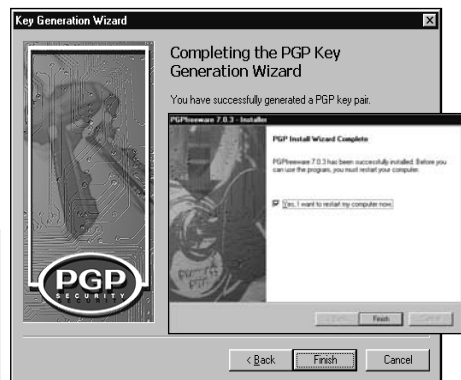
Masukkan Full name dan Email address. Selanjutnya **Key Type**. Pilih Diffe-Hillman/DSS yang didukung terus pada versi-versi PGP berikutnya. RSA dan RSA Legacy adalah key model lama. **Key size** jangan terlalu besar (lama prosenya) atau kecil (kurang aman). pilih 2048.



8

MASUKKAN PASSPHRASE

Key expiration pilih never. Selanjutnya anda diminta untuk memasukkan **passphrase** (seperti password) tapi dalam bentuk frasa kata dan minimum 8 karakter). Klik **Next** dan Key dan Subkey akan terbentuk. Klik **Next** untuk menyelesaikan proses pembentukan key.



9

PGP KEY TERBENTUK

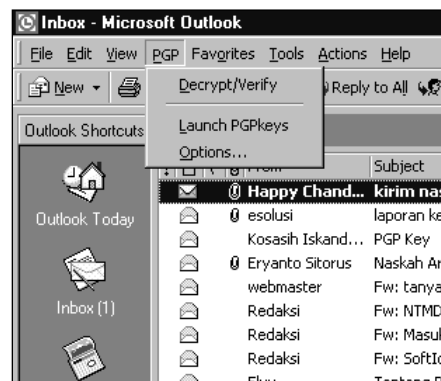
Tampil pesan bahwa PGP Key telah terbentuk dan anda kini dapat mengirim dan menerima secure message. Juga diinformasikan bahwa public key anda dapat 'diterbitkan' di server yang disiapkan. Selanjutnya komputer perlu di-boot ulang. Klik **Finish** untuk itu.



13

PIHAK PENERIMA 'GEMBOK'

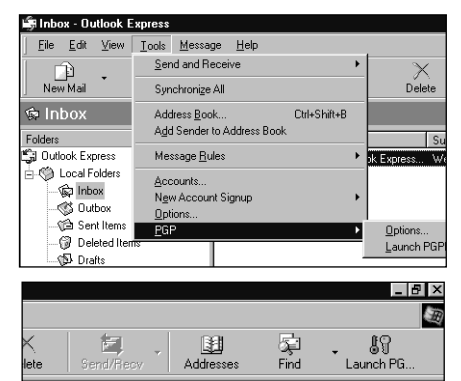
Di pihak penerima beginilah email yang diterimanya. Public key itu diawali dengan -----BEGIN PGP PUBLIC KEY BLOCK----- dan diakhiri dengan -----END PGP PUBLIC KEY BLOCK-----



14

PLUG-IN PADA OUTLOOK

Pada contoh sebelumnya digunakan web mail untuk mengirim public key. Selanjutnya untuk encrypt dan decrypt banyak menggunakan clipboard. Bila memakai email client Outlook, terlihat bahwa pada Outlook sudah ada menu PGP-nya.



15

PLUGIN PADA OE

Pada Outlook Express tampilan menu setelah instal PGPfreeware terpasang agak berbeda, terdapat di bawah menu Tools maupun berupa logo sendiri yaitu Launch PGPfreeware.

PGP FREEWARE 7.0.3

IMPORT KEYRING DAN EMAIL TERENKRIPSI

Kini bahasan dari sisi **pemakai komputer lain** yang menerima kiriman PGP public key. Public key yang didapatnya itu adalah 'gembok' yang akan digunakan untuk mengirim email terenkripsi ke pemilik 'gembok' tadi. Kalau tidak hati-hati si pengirim tidak bisa membuka arsip emailnya sendiri.

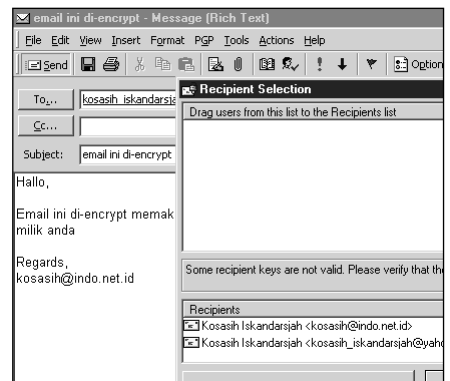
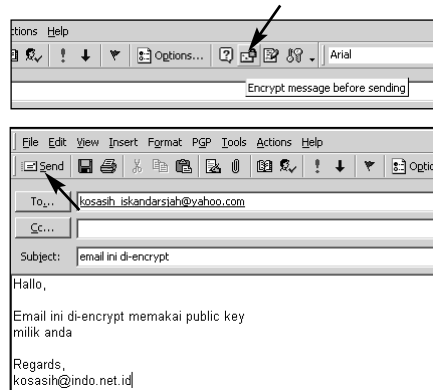
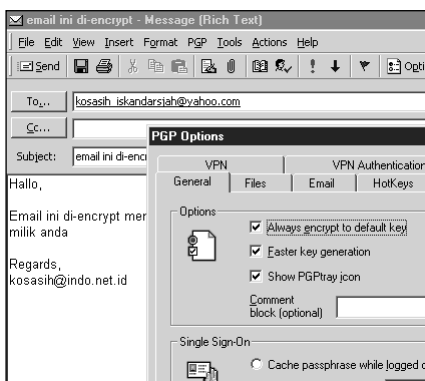
Pada contoh ini penerima public key menggunakan email client Outlook dan bukan menggunakan web mail seperti halnya pengirim public key (gembok).

Penerima public key kini dapat mengirim email terenkripsi ke pemilik public key, yang diibaratkan mengembok barang dengan gembok kiriman (yang tidak disertakan anak kuncinya).

Plug-in PGPfreeware pada Outlook, OE, dan Eudora membuat berbagai email client ini mendapatkan fungsi enkripsi secara terpadu sehingga sangat memudahkan.

Sekali konsep gembok dan anak kunci ini dipahami, wnkripsi dan dekripsi (serta verify signature) menjadi begitu mudah.

Konsep gembok dan anak kunci akan memudahkan memahami konsep PGPfreeware



4

MENGIRIM ENCRYPTED EMAIL

Kini kosasih@indo.net.id dapat mengirim email yang akan di-enkripsi dengan public key milik kosasih Iskandarsjah@yahoo.com. Namun sebelum mengirimkannya pastikan pilih **Always encrypt to default key** dari menu **PGP > Options**.

5

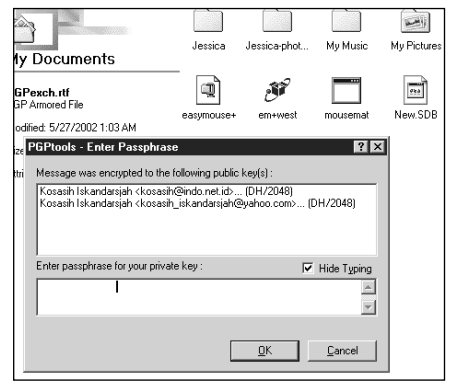
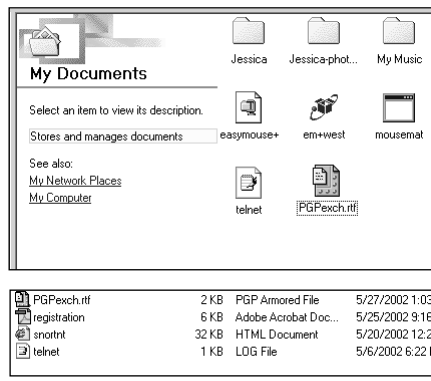
SIAP DI-ENCRYPT

Setelah mengetikkan isi email (biasa saja), klik icon Encrypt sebelum di-kirim. Setelah itu baru klik tombol Send. PGPfreeware yang aktif sebagai plug-in akan meng-encrypt email ini dengan **dua public key** sekaligus. Dengan public key milik penerima dan pengirim.

6

RECIPIENT SELECTION

Tampil jendela **Recipient Selection** yang menunjukkan nama-nama email yang ada pada public keyring pada komputer pengirim. Di sini ada kosasih Iskandarsjah@yahoo.com dan milik pengirim email ini, yaitu kosasih@indo.net.id. Pilih entri yang kedua, yaitu email yang di Yahoo!



10

SAVE DI FOLDER ANDA

Save file yang lengkapnya bernama **PGPexch.rtf.asc** ini pada folder pilihan anda. Pada contoh ini disimpan pada folder MyDocuments.

11

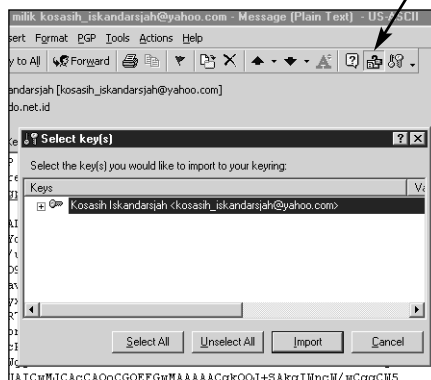
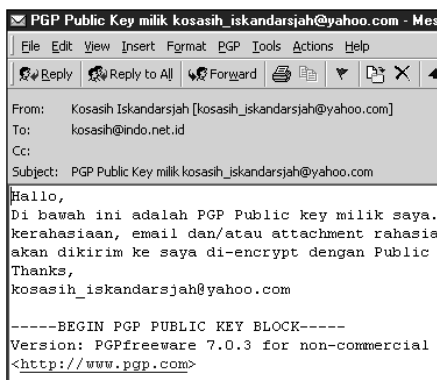
FILE TERPROTEKSI

Dengan Windows Explorer kita dapatkan bahwa file ini termasuk kategori **PGP Armored File**. Double click pada icon file ini untuk membukanya.

12

BUKA DENGAN PRIVATE KEY

Terlihat informasi bahwa file ini di-enkripsi dengan menggunakan dua macam public key. Untuk membukanya pengirim perlu menggunakan private key milik pengirim itu sendiri yang meminta pengirim memasukkan passphrase-nya sendiri.



1

MENERIMA PUBLIC KEY

Di contoh ini kosasih@indo.net.id mendapatkan email yang berisi public key (gembok) milik kosasih_iskandarsjah@yahoo.com dan dibaca dengan menggunakan Microsoft Outlook.

2

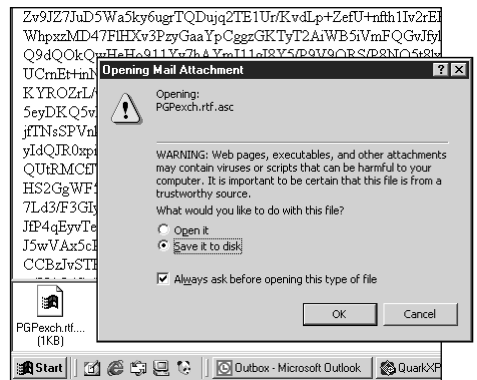
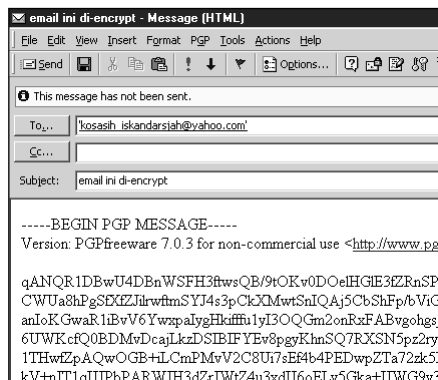
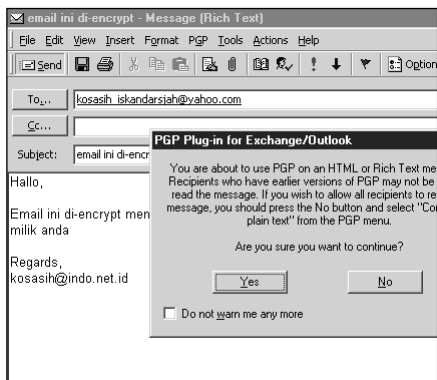
IMPORT KE KEYRING FILE

Untuk meng-import public key ini ke keyring file milik penerima email, pada Outlook klik icon **Decrypt/Verify** dan akan tampil public key yang ada pada email itu, yaitu public key milik pengirim. Klik **Import**.

3

TAMBAHAN ENTRI

Selanjutnya klik start-up tray dan pilih PGPKeys dari pull-up menu. Akan tampak bahwa kini telah terdapat tambahan entri pada keyring milik penerima email (entri yang kedua). Entri pertama adalah entri default milik kosasih@indo.net.id



7

PGP ON HTML/RTF

Ada pesan bahwa pesan yang akan dienkripsi ini berbentuk HTML atau RTF dan pemakai PGP versi lama mungkin tidak dapat membacanya. Karena pada contoh ini kedua belah pihak menggunakan PGPFreeware 7.0.3, kita lanjutkan saja. Klik **Yes**.

8

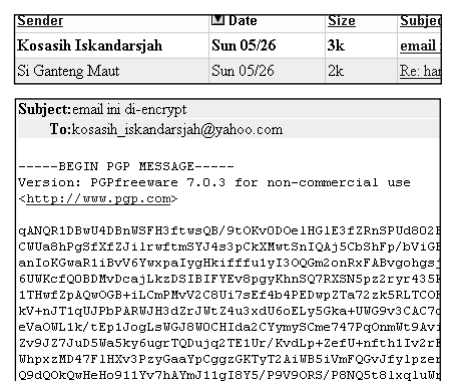
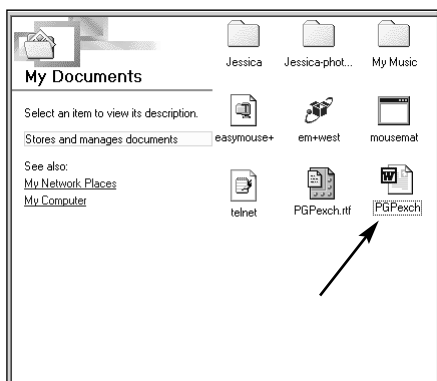
MASUK KE OUTBOX

Karena akses Internet belum dijalankan, email akan masuk Outbox pada Outlook. Kita bisa lihat apa yang akan dikirim ini. Nah sudah terenkripsi, dan tidak terbaca lagi apa isinya. Bagaimana untuk arsip pengirim? Body text ini dienkripsi dengan public key penerima.

9

PGPEXCH.RTF

File yang akan kita kirim itu ada lampirannya yaitu **PGPexch.rtf** yang dienkripsi dengan public key pengirim sesuai setting agar selalu dienkripsi juga dengan default key. Double click pada icon ini dan pada jendela **Opening Mail Attachment**, pilih **Save to Disk**.



13

TERBUKA MENJADI FILE RTF

Terlihat proses konversi berjalan dan tak lama kemudian file ini telah terbuka menjadi file yang tidak dienkripsi dan sudah dapat dibuka dengan word processor.

14

BUKA ARSIP DENGAN WORD

Arsip email yang dienkripsi tadi telah terbuka kembali dengan memasukkan public key milik pengirim. Pengirim kini dapat melihat kembali arsip email yang dikirimkannya.

15

DITERIMA DI WEB MAIL

kosasih_iskandarsyah@yahoo.com yang mempunyai account web mail di mail.yahoo.com kini mendapatkan adanya email yang baru masuk yang dikirimkan oleh kosasih@indo.net.id. Buka file ini seperti biasa dan akan diperoleh bahwa email ini terenkripsi. Bagaimana membukanya?

PGP FREWARE

ENKRIPSI/DEKRIPSI

UNTUK WEB MAIL

Plugin PGPfreeware tersedia untuk Outlook, Outlook Express, dan Eudora. Bagaimana dengan email client lain? Atau web mail? PGPfreeware mendukung enkripsi/dekripsi/verify pada teks yang ada di **clipboard**. Dengan demikian praktis mendukung segala macam aplikasi pada Windows.

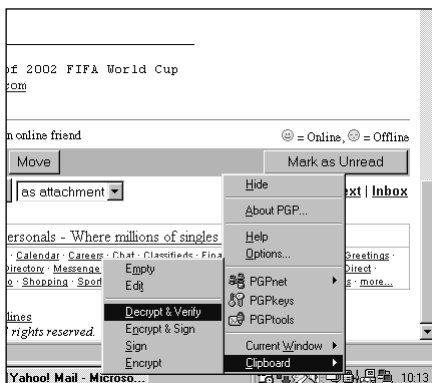
Fasilitas memproses teks yang ada dalam clipboard, yang dapat diaktifkan lewat PGPTray amat praktis, membuat segala macam aplikasi pada Windows dapat memanfaatkan PGPfreeware.

Lewat PGP Tray kita dapat mengaktifkan fasilitas untuk clipboard selain menu-menu utama PGPNet, PGPKeys, dan PGPTools.

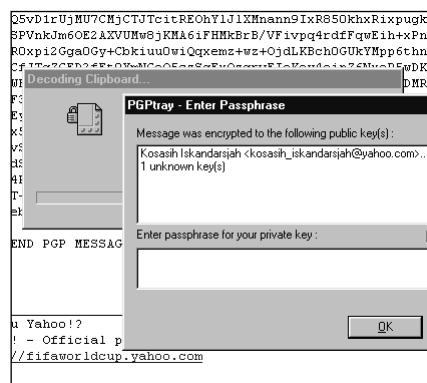
Khusus PGPTools untuk mengenkripsi file yang akan dikirim sebagai attachment. Adapun PGPNet merupakan VPN client yang memungkinkan anda melakukan transaksi secara aman melalui Internet.

PGPNet dan cara menerbitkan public key anda pada server yang disediakan belum dibahas pada NeoTek kali ini. Silakan eksplorasi sendiri!

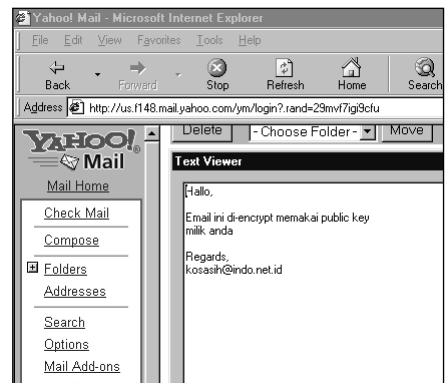
PGPfreeware untuk web mail ataupun aplikasi lain yang tidak mendukung PGPfreeware plugin



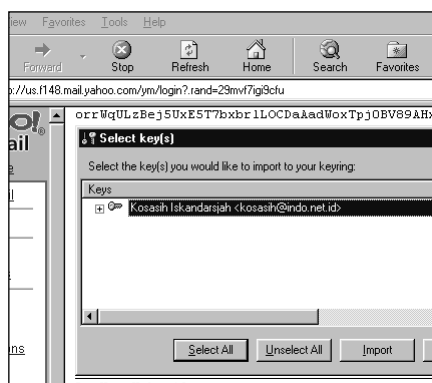
- 4 DECRYPT/VERIFY ISI CLIPBOARD**
Klik PGP tray yang terdapat pada startup bar dan pilih **Clipboard > Decrypt/Verify** untuk mendekripsi teks yang kini ada di clipboard. Akan tampil jendela dialog yang menyatakan bahwa teks yang ada di clipboard itu di-encrypt dengan menggunakan dua public key.



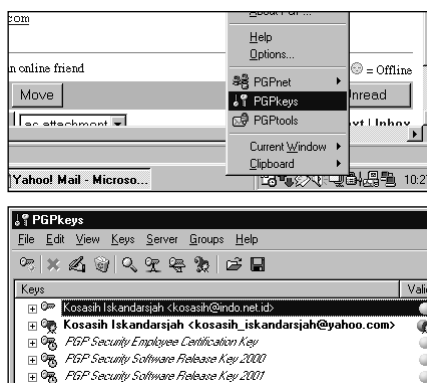
- 5 ENTER PASSPHRASE**
Yang pertama milik penerima, yaitu kosasih_iskandarsjah@yahoo.com dan yang kedua tidak diketahui siapa. Masukkan passphrase milik penerima dan klik **OK**.



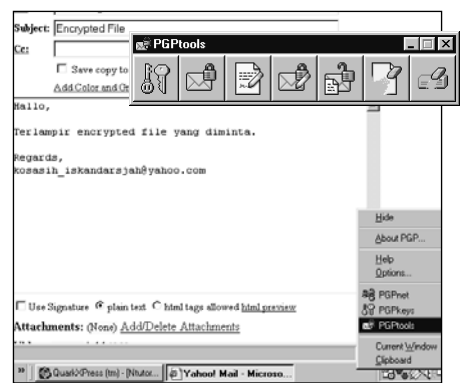
- 6 TEKS TERDEKRIPSI**
Akan tampil jendela Text Viewer yang menampilkan versi asli pesan sebelum di-enkripsi.



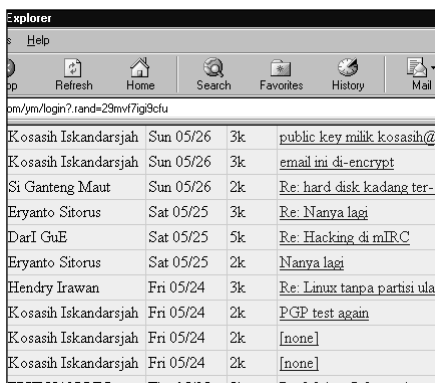
- 10 IMPORT PUBLIC KEY**
Akan tampil jendela Select key(s) yang berisi satu public key, dalam hal ini milik kosasih@indo.net.id. Klik Import untuk memasukkan public key ini ke file keyring.



- 11 PERIKSA PUBLIC KEY YANG ADA**
Untuk memeriksa apakah public key tersebut sudah masuk ke dalam file keyring, dari PGP Tray pilih **PGPKeys** dan akan tampil PGP keys yang ada. Tampak public key yang baru di-impor sudah ada (baris pertama). Adapun yang kedua (bold) adalah public key default.



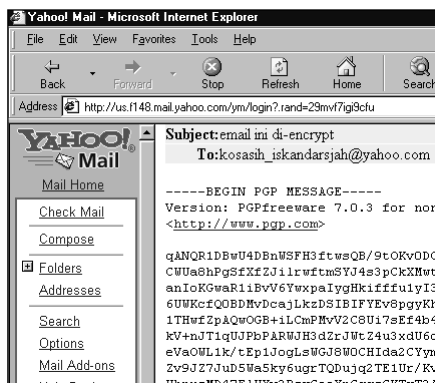
- 12 MENGIRIM FILE TERENKRIPSI**
Sesuai permintaan, suatu file terenkripsi akan dikirim sebagai attachment. Tulis email pada web mail Yahoo! seperti biasa. Setelah selesai, dari PGP Tray pilih **PGPTools** yang akan menampilkan jendela icon-icon PGP Tools.



1

MEMBACA WEB MAIL

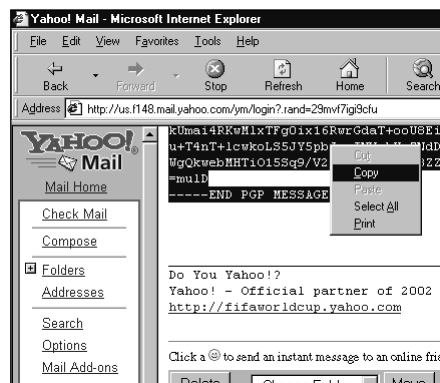
Buka mail.yahoo.com dan pilih Inbox. Terlihat ada dua email dari kosasih@indo.net.id yang dikirim ke kosasih_iskandarsjah@yahoo.com. Pilih email yang lebih awal dikirim yaitu dengan subject 'email ini di-encrypt' dengan mengklik-nya.



2

ENCRYPTED EMAIL

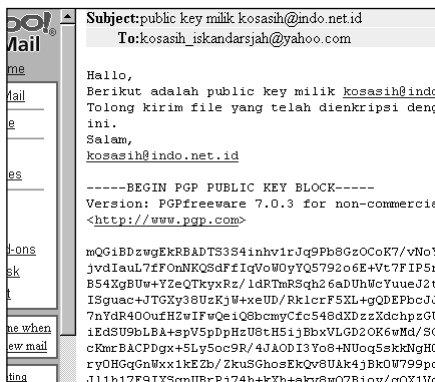
Terlihat email yang di-encrypt yang diawali dengan teks
-----BEGIN PGP MESSAGE-----
dan diakhiri dengan
-----END PGP MESSAGE-----



3

HIGHLIGHT DAN COPY

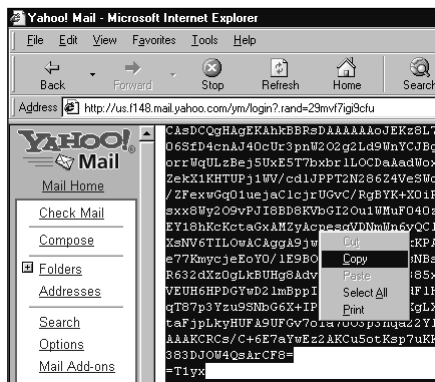
Highlight teks yang berada di antara kedua pembatas itu dan klik kanan untuk memunculkan opsi terhadap teks yang di-highlight. Pilih **Copy** untuk menyalin teks tersebut ke clipboard.



7

EMAIL KEDUA

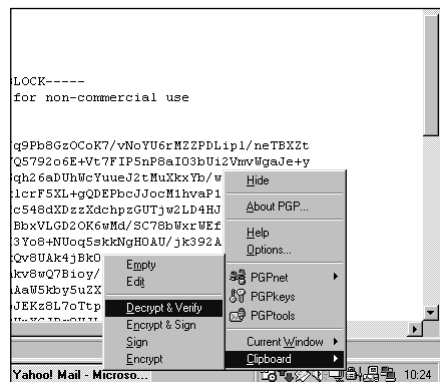
Buka email kedua, yang ternyata berisi PGP public key milik pengirim, yaitu kosasih@indo.net.id dan pesan agar mengirimkan file yang sebelumnya harap di-encrypt dengan public key pengirim email ini.



8

HIGHLIGHT DAN COPY

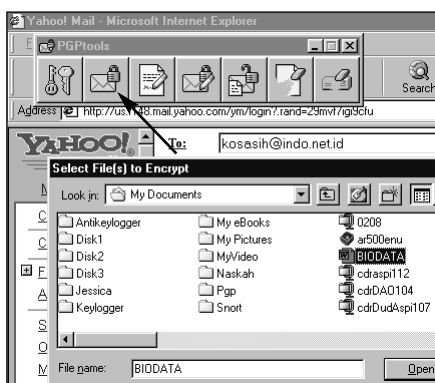
Untuk menambahkan public key yang baru dikirim ini ke keyring penerima, highlight teks ini mulai dari awal sampai akhir seperti yang ditandai oleh
-----BEGIN PGP PUBLIC KEY BLOCK-----
sampai
-----END PGP PUBLIC KEY BLOCK-----



9

KEMBALI KE PGP TRAY

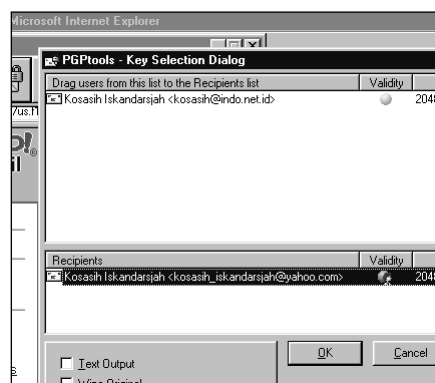
Sama seperti mendeskripsi pesan yang di-encrypt, untuk menambahkan public key ini ke file keyring penerima, yang perlu dilakukan adalah pilih icon PGP Tray pada startup bar dan pilih **Clipboard > Decrypt Verify**.



13

PILIH ICON ENCRYPT

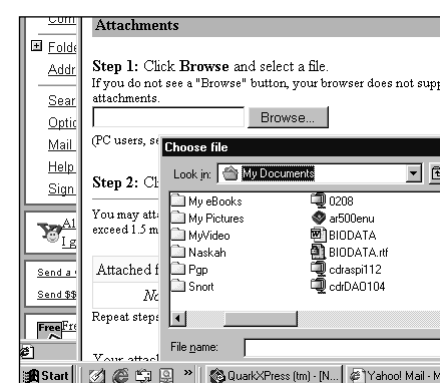
Pilih **icon encrypt** (icon kedua) dan akan tampil jendela dialog **Select File(s) to Encrypt** dan anda dapat mem-browse komputer anda untuk memilih file yang hendak di-encrypt. Misalkan file BIODATA.RTF yang terdapat pada folder MyDocuments.



14

SIAPA PENERIMANYA?

Akan tampil **Key Selection Dialog** yang menanyakan mana lagi penerima file ini selain yang ada di penerima. Karena tidak ada lagi, klik **OK** untuk mulai menenkripsi file ini.



15

ARMORED FILE SIAP DIKIRIM

Maka dari file BIODATA.RTF akan terbentuk file BIODATA.RTF.ASC yang mempunyai icon yang khas. File ini siap di-attach seperti biasa melalui fasilitas attachments pada web mail Yahoo! Kelak penerima harus membuka dengan memasukkan passphrase miliknya.

FTP SERVER wFTPD INSTALASI MUDAH PADA WINDOWS 9x/ME

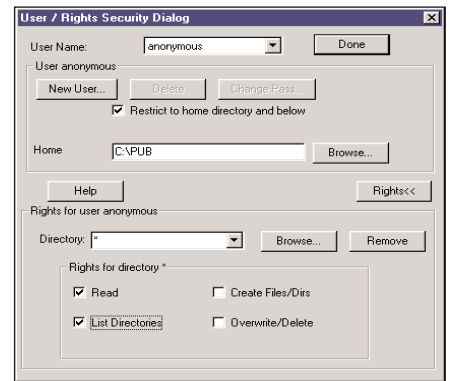
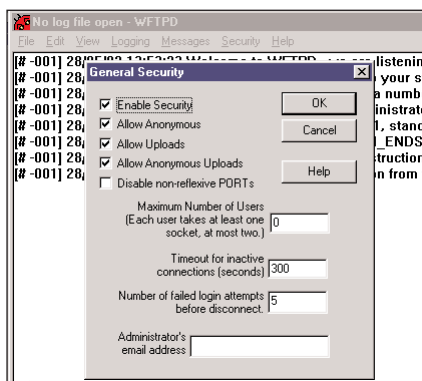
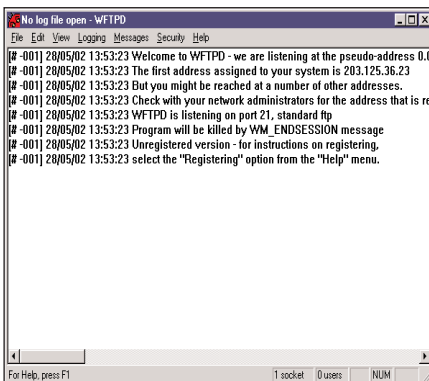
Perlu **transfer file** antara sistem yang berbeda: PC dengan macintosh, misalnya? Atau kesulitan meng-attach file yang besar sebab web mail anda (misalnya Yahoo mail) membatasi besar attachment 1,5 Mbyte? Pasang saja **FTP server** pada salah satu komputer anda yang terhubung ke Internet.

Menyiapkan FTP server untuk sekolah-sekolah hanya dengan komputer biasa dengan akses Internet.

Bila web server yang diakses lewat web browser sudah cukup dikenal (misalnya Apache, IIS, Xitami, atau Sambar), maka FTP server yang sebenarnya 'lebih tua' dari web server malah kurang terkenal.

Kebutuhan akan FTP server mungkin hanya dalam LAN saja (namun antara sistem yang berbeda, misalnya PC dengan Macintosh), atau dapat juga untuk sharing file dalam komunitas terbatas seperti rekan kerja ataupun keperluan pendidikan.

NeoTek kali ini menyajikan wFTPD, suatu FTP server yang sangat mudah penggunaannya dan disarankan untuk dipakai oleh sekolah-sekolah dasar atau menengah untuk sharing file antara guru dan murid



4

FTP SERVER ANDA

FTP server anda kini telah berjalan. Perhatikan pesan yang menunjukkan bahwa wFTPD mendapatkan IP Address pada komputer anda (pada contoh 203.125.36.23 dan dapat berubah lagi setiap kali akses lagi ke Internet) serta listen pada port 21, standar ftp.

5

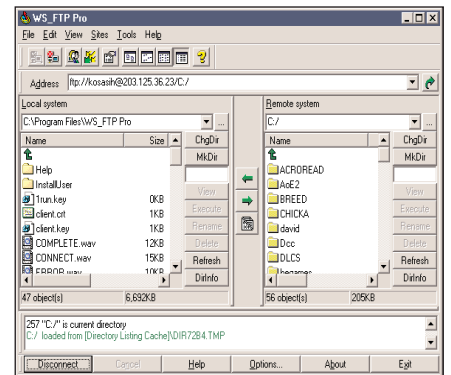
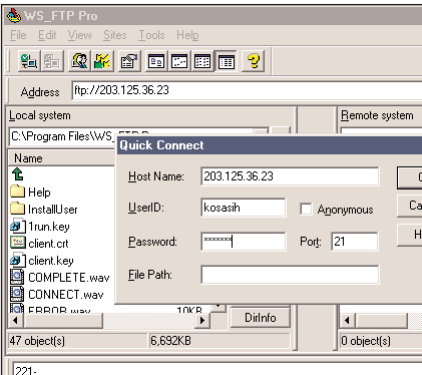
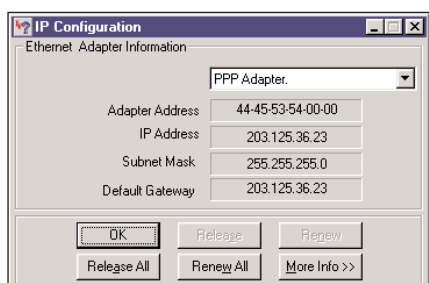
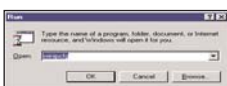
MENU SECURITY

Pilih **Security > General** dan di sini tampil opsi yang dapat ditetapkan. Bila ftp server anda membolehkan anonymous access, klik kotak di depan Allow Anonymous. Demikian juga apakah membolehkan upload serta anonymous upload.

6

USER/RIGHTS ANONYMOUS

Pilih **Security > User/Rights** dan di sini kita akan menetapkan sejauh mana anonymous user boleh mengakses ftp server kita. Tetapkan Home di C:\PUB (jangan lupa buat dulu direktori ini) dan batasi hanya akses pada direktori ini dan apakah boleh Read, List, atau lainnya.



10

MEMASTIKAN IP ADDRESS

Pada wFTPD diketahui bahwa IP Address komputer yang menjadi FTP server ini adalah 203.125.36.23 serta listen di port 21. IP Address ini dapat juga dilihat dengan mengetikkan **winipcfg** dari **Start > Run**. FTP server kita belum diberi nama domain, jadi memakai IP Address saja.

11

AKSES DARI KOMPUTER LAIN

FTP server anda kini dapat diakses dari komputer lain di seluruh dunia. Jalankan ftp client (di sini WS_FTP) dan pada kotak address ketikkan **ftp://203.125.36.23** dan klik **Go**. Dapat juga tanpa ftp:// yang artinya cukup 203.125.26.23 dan akan tampil jendela **Quick Connect**.

12

AKSES SELURUH KOMPUTER

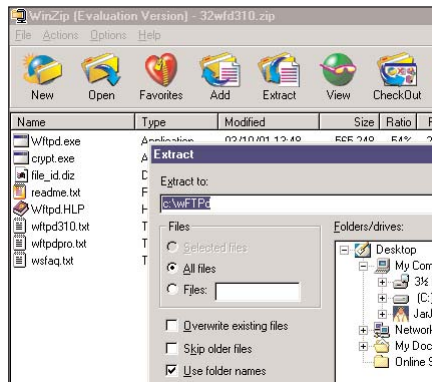
Masukkan **user id** kosasih dan **password**-nya maka koneksi ke FTP server terjadi. Window pane sebelah kiri menunjukkan **komputer lokal** sedangkan yang kanan adalah remote **FTP server**. Upload dan download cukup dengan memilih file dan klik tanda panah yang sesuai.



1

DOWNLOAD WFTPD

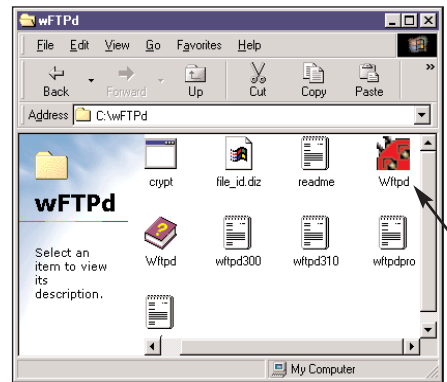
Download wFTPD dari sumbernya di <http://www.wftpd.com/>. Versi terakhir adalah wFTPD 3.10.



2

EKSTRAK DENGAN WINZIP

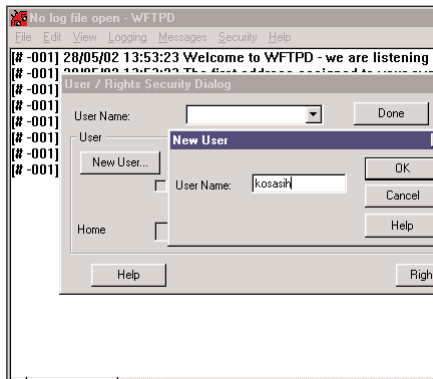
Kemudian buka dengan WinZip dan ekstrak ke direktori pilihan anda. Misalkan diekstrak ke folder C:\wFTPD. Sebelum menjalankan wFTPD jangan lupa untuk menjalankan koneksi ke Internet.



3

JALANKAN WFTPD

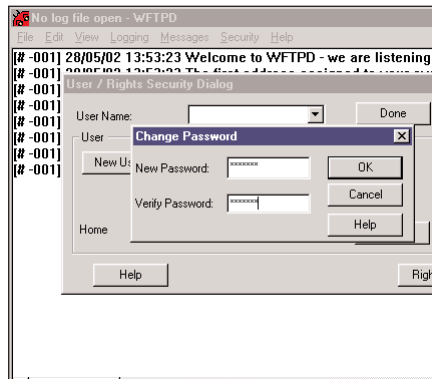
Untuk menjalankan wFTPD cukup klik dua kali pada icon Wftpd yang bentuknya khas dan berwarna merah. FTP server anda akan langsung berjalan.



7

NEW USER

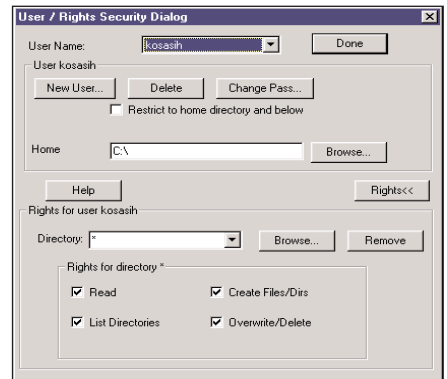
Masih pada jendela dialog yang sama pilih **New User** dan masukan nama user baru. Pada contoh ini new user-nya **kosasih** yang akan kita berikan akses yang lebih luas daripada anonymous user. Klik **OK** untuk melanjutkan.



8

PASSWORD

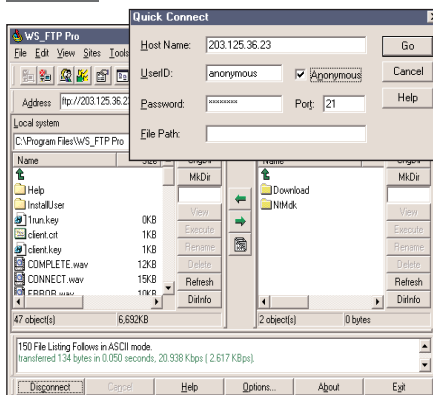
Untuk user baru ini anda diminta memasukkan **password** serta **verifikasinya** (dua kali), klik **OK** untuk melanjutkan.



9

USER/RIGHTS

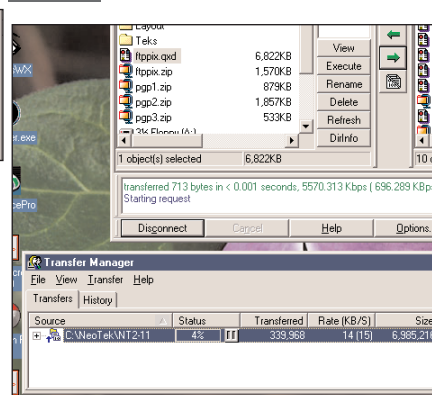
Untuk user ini tidak diberikan batasan. Dapat masuk mulai dari root di C:\ serta dapat Read, List Directories, Create Files/Dirs, serta Overwrite/Delete. Ini adalah rights dari si pemilik komputer itu sendiri.



13

ANONYMOUS ACCESS

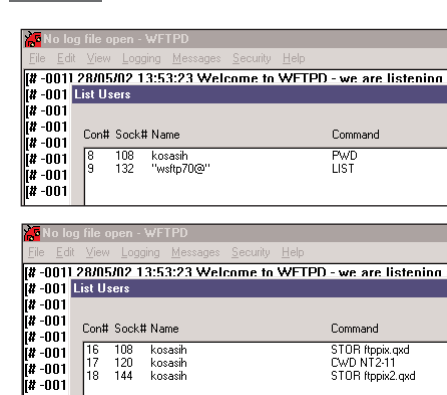
Untuk sembarang orang di seluruh dunia (anonymous access), akses ke FTP server ini menggunakan UserID **anonymous** dan biasanya sebagai password adalah **email address** yang mengakses. Klik **Go** untuk anonymous access.



14

UPLOAD FILE

Pada contoh ini user kosasih melakukan file upload dari komputer lokal ke FTP server (ada dua file yang di-upload, namun yang ditunjukkan pada gambar cuma satu), sedangkan user anonymous baru mem-browsing direktori C:\pub saja.



15

CONNECTED USER

Di sisi FTP server pilih **View > Connected Users** dan akan tampil jendela yang menunjukkan hal itu. Gambar atas menunjukkan user kosasih dan anonymous yang baru saja akses. Yang kedua menunjukkan user kosasih mengakses direktori dan upload dua file.

NetBeans, FSL & OpenUSS dalam Proses Teaching & Learning

Dengan perangkat lunak open source yang ada, dosen dapat menempatkan bahan-bahan kuliah pada server yang dapat diakses mahasiswa. Demikian juga dengan ujian dan kemudian hal-hal administratif.

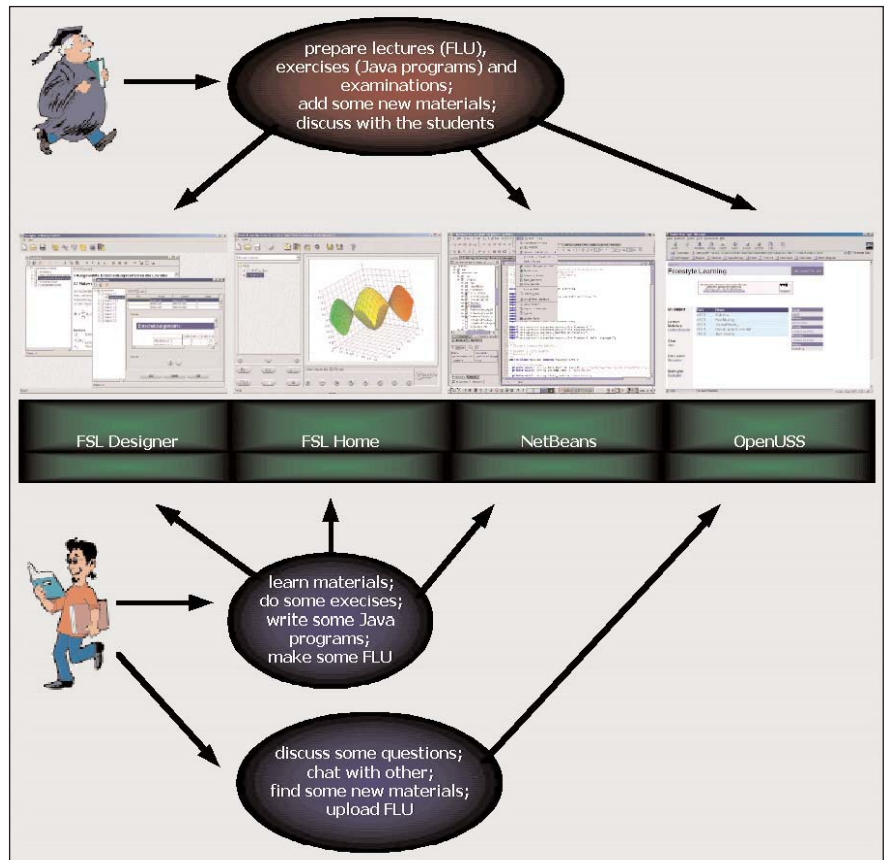
Marilah sekarang kita melihat peran piranti lunak *open source* dalam proses pengajaran dan pembelajaran. Pada kesempatan ini kita akan memfokuskan perhatian kita pada produk *open source* yang berbasis Java yang dapat digunakan dalam bidang ini.

Kita akan menganalisa perbedaan kemampuan NetBeans, FSL, dan OpenUSS dilihat dari dua perspektif. Perspektif pertama adalah dari segi pengguna atau user, yang akan diperlihatkan bagaimana hebatnya ketiga produk di atas secara bersama-sama untuk mendukung "teaching and learning Java." Sedangkan perspektif kedua adalah dari segi pengembang atau *developer*-nya. Dengan kekuatan dan kehebatan Java, pengembang secara independen (*independent developers*) dapat menambahkan sebuah kemampuan (*functionality*) baru kedalam ketiga produk ini. Sebuah paradigma Java yaitu: "learn once use everywhere" membuat para Java *developer* sangat mudah untuk kemudian mengembangkan sebuah proyek open source seperti halnya pada NetBeans, FSL dan OpenUSS untuk menjadi sebuah pasar yang sangat besar.

Pengintegrasian NetBeans, FSL, dan OpenUSS dengan sangat hebat meningkatkan siklus pendidikan bagi Java sebagai bahasa pemrograman.

Sebuah skenario CAT+CAL yang sangat khas adalah dapat kita lihat pada gambar di samping.

- Pengajar menciptakan beberapa materi pembelajaran untuk sebuah kuliah Java dengan menggunakan FSL Designer. Materi ini dinamakan Freestyle Learning Units (FLU).
- Kemudian pengajar menggunakan NetBeans untuk mempersiapkan berbagai contoh dan latihan dalam pemrograman bahasa Java.
- Dosen juga dapat menggunakan atau menggabungkan FLU yang sudah ada tadi untuk dikembangkan mahasiswa dan instruktur.
- Para mahasiswa kemudian mendownload FLU-nya melalui OpenUSS dan mempelajarinya secara offline dari komputer mereka dari homepage FSL. Selain itu FLU juga tersedia pada CD ROM untuk mahasiswa yang tidak memiliki koneksi internet untuk men-download pelajaran tersebut.
- Mahasiswa kemudian meringkas apa yang mereka dipelajari dengan menuliskan beberapa program Java menggunakan NetBeans.



• Proses teaching and learning bahasa Java dengan NetBeans, FSL, dan OpenUSS.

- Selain itu mahasiswa juga dapat mendiskusikan beberapa bahan dan memberikan pertanyaan yang mereka punyai kepada para pengajar dan tentu saja dengan rekan sejawatnya yakni mahasiswa lain dengan menggunakan fasilitas chat dan mailing list pada OpenUSS.
- Dosen dapat kemudian memberikan informasi tambahan lainnya dan latihan-latihan pada bagian/seksi pada OpenUSS yang namanya bahan-bahan kuliah.
- Sedangkan mahasiswa lainnya dan instruktur dapat membuat FLU mereka masing-masing dengan FSL Designer dan menempatkannya pada komunitas yang ada sehingga dapat diakses oleh seluruh anggota komunitas.

Seluruh produk yang digunakan dalam skenario ini adalah open source, sehingga tidak ada keharusan bagi para dosen dan mahasiswa untuk membayar lisensi dari piranti-piranti lunak diatas. Hal ini membuat para dosen dan mahasiswa lebih

mudah untuk segera bergerak dan berlari untuk mengejar ketinggalan dalam ilmu ini terutama bahasa pemrograman Java. Banyak hal yang dapat dilakukan dengan menggunakan teknologi CAT+CAL yang dapat diintegrasikan dalam siklus pendidikan, dari bahan-bahan kuliah yang ditawarkan secara eksklusif melalui online hingga mengirimkan bahan-bahan kuliah tambahan pada situs sebuah institusi pendidikan. Satu-satunya batasan yang ada adalah kemampuan imajinasi anda.

Apa lagi? Para mahasiswa tingkat lanjut dapat segera menunjukkan kemampuan Java-nya untuk digunakan menolong mengembangkan NetBeans, FSL, dan OpenUSS. Partisipasi dalam sebuah proyek open source juga memberikan pada para mahasiswa sebuah situasi dan pengalaman yang benar-benar realistik (*real-world*) dan bernilai tinggi dalam proyek-proyek pemrograman skala besar.

Open Source dan Java untuk Pendidikan?

Ketika Java menjadi lebih populer dan menyebar secara cepat, dimana makin banyak para pemrogram berluncuran kedalam 'kereta Java'. Sebuah kenyataan bahwa pada saat ini dan dimasa depan Java menjadi bahasa pemrograman paling populer adalah salah satu alasan utama mengapa banyak piranti lunak pendidikan yang dituliskan dalam bahasa Java. Perangkat piranti lunak yang dituliskan dalam bahasa Java ini juga mendukung gerakan open source dengan membiarkan para pengguna untuk memilih penggunaan Linux namun juga Windows tanpa membatasi para pemirsanya hanya menuliskan piranti lunak dalam Linux.

Artikel ini menunjukkan kekuatan piranti lunak open source dalam bidang pendidikan. Dengan menggunakan NetBeans, FSL dan OpenUSS untuk matakuliah Java hanya sebuah contoh dari banyak kemungkinan lain yang terdapat di dalam bidang pendidikan. Apa yang dapat sekarang kita lakukan untuk menolong dan mendukung pengembangan piranti lunak open source dan integrasinya untuk tetap membuat proyek open source menjadi pelopor terdepan di bidang teknologi piranti lunak. Anda tidak perlu memulai sebuah proyek open source dari awal, anda tinggal memi-

lih salah satu dari proyek yang ada dan cocok bagi anda dan segera bergabung dengan dengan proyek itu! Untuk anda yang berminat dan tertarik dengan penggunaan Java dibidang pendidikan maka NetBeans, FSL dan OpenUSS adalah beberapa proyek besar yang cukup menarik untuk memulainya. Sukses sebuah proyek open source di bidang pendidikan dapat membawa "equality of knowledge to the Internet." Pertanyaannya sekarang apakah anda memiliki kemauan dan inisiatif dalam menggunakannya?

Kontak dan Status Proyeknya

NetBeans

NetBeans (<http://www.netbeans.org>) adalah sebuah proyek open source, modular IDE, dan dituliskan dalam bahasa pemrograman Java. Saat ini mendukung pengembangan Java namun arsitekturnya sendiri mendukung untuk pemrograman bahasa lain. NetBeans juga merupakan sebuah extensible tools platform dimana tools yang lainnya dan juga functionality-nya dapat seamlessly diintegrasikan dengan menuliskan dan mengintegrasikan modul-modulnya. Core dari the NetBeans dapat digunakan dalam generic application framework untuk mempermudah penulisan aplikasi non-IDE. Karena dituliskan dalam bahasa pemrograman Java, maka akan beroperasi pada setiap plat-

form dengan sebuah virtual machine.

Freestyle Learning dan OpenUSS

OpenUSS (<http://openuss.sourceforge.net>) dibuat sebagai proyek open source sejak dari awalnya. FSL (<http://www.wi.uni-muenster.de/aw/freestyle-learning/english/eindex.htm>) adalah sebuah mature product dan telah tersedia pada Universitas Muenster. Proyek ini akhirnya dijadikan sebuah proyek open source dan dalam beberapa minggu mendatang akan dirilis dibawah lisensi GPL pada SourceForge.

Blasius Lofi Dewanto
(dewanto@uni-muenster.de)

- *asisten riset di Westfälische Wilhelms- Universität Muenster, Jerman, Institut für Wirtschaftsinformatik Lehrstuhl für Wirtschaftsinformatik und Controlling*
- *arsitek pengembangan OpenUSS (Open University Support System).*

Referensi:

Pdf documents about Freestyle Learning and OpenUSS.
<http://edu.netbeans.org/support/fsl.pdf>
<http://edu.netbeans.org/support/openuss.pdf>