Hacking & PC Security

Kosasih Iskandarsjah & Onno W. Purbo
Graha Santika, Semarang
Kamis, 29 Agustus 2002

Komputer sebagai alat produktivitas pada dasarnya memanfaatkan perangkat-perangkat lunak word processor, spreadsheet, database, dan alat untuk berkomunikasi. Alat untuk berkomunikasi ini ada karena adanya Internet, terutama dalam bentuk email dan web browser.

Kemudahan komunikasi melalui Internet bukan tidak ada bahayanya. Dengan terhubung ke Internet, berarti komputer anda masuk menjadi bagian dari Internet itu sendiri, suatu jaringan yang menghubungkan jutaan komputer di seluruh dunia. Dan di dunia maya yang begitu luas terdapat bermacam karakter dengan bermacam perilaku pula. Sama seperti di dunia nyata, kita harus mempunyai kemampuan untuk 'hidup' di dunia maya ini.

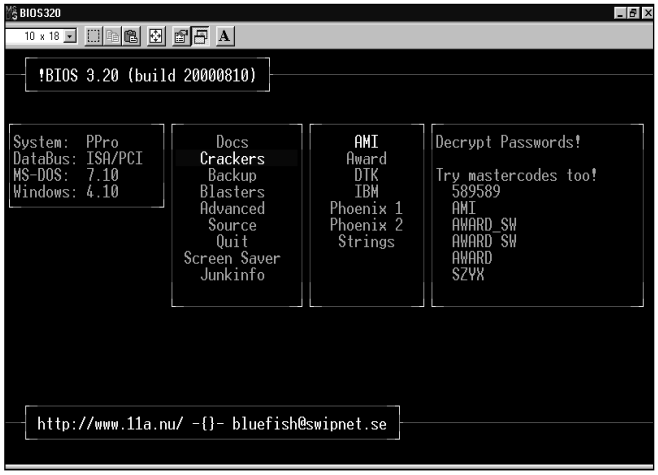
Salah satu pengetahuan yang harus dikuasai adalah cara mempertahankan diri (tepatnya mempertahankan komputer anda) sewaktu terhubung ke Internet. Pada bahasan ini, diasumsikan bahwa anda terhubung ke Internet melalui komputer yang paling lazim digunakan oleh para pemakai pribadi, yaitu menggunakan sistem operasi Windows 9x/ME. Walau demikian, sebagian besar bahan-bahan bahasan berlaku pula untuk sistem operasi lain.

Ancaman Terhadap Komputer Anda

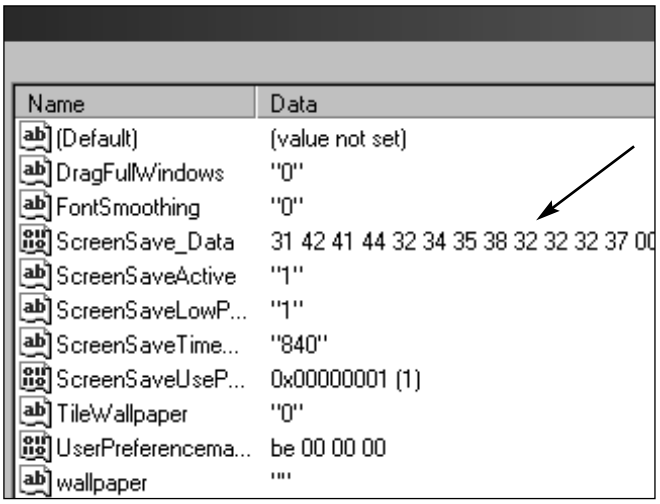
Ada tiga jenis ancaman pada komputer anda:

- *Local attack*
- Bahaya berinternet
- *Hacker attack*

Local attack atau *console hacking* adalah usaha rekan anda sendiri untuk mengakses data anda secara tidak sah. Jadi si penyerang dapat mengakses komputer anda secara fisik dan berusaha masuk ke dalam penyimpanan data. Apabila komputer anda tidak diproteksi dengan password, maka data anda dapat dilihat oleh siapa saja.



• *!BIOS dapat menghapus password pada berbagai macam BIOS*



• *Informasi screen saver password terdapat pada registry, di bawah segmen HKEY_USERS\.DEFAULT\Control Panel\Desktop*

• *Ekspor bagian registry ang ada komponen password screen saver-nya, lalu crack dengan 95sscrk. Screen saver password langsung kelihatan!*

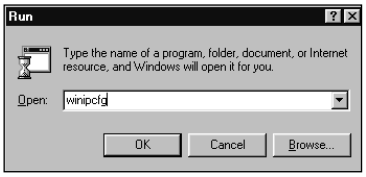
Ada beberapa lapis pengamanan terhadap *console hacking*:

- Men-set BIOS password
- Men-set screen saver password
- Men-set password pada folder
- Men-enkripsi dokumen-dokumen penting

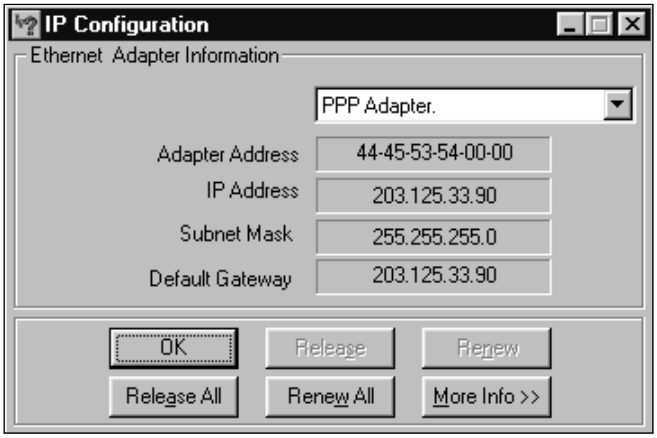
Seperti maling dan polisi, ada saja teknik untuk membobol pertahanan anda. BIOS password dapat di-reset dengan mengangkat baterai yang terpasang pada motherboard atau menggunakan BIOS password cracker seperti misalnya **!BIOS** yang mampu menghapus password pada macam-macam jenis BIOS. Screen saver password juga dapat di-crack dengan 95sscrk (Screen Saver Cracker). Keduanya mudah digunakan dan dapat diperoleh gratis di Internet.

Tinggal mengamankan dokumen dengan melindungi folder dan file itu sendiri yang relatif lebih sulit dibongkar oleh hacker amatiran. Itupun belum seratus persen aman.

Identitas Komputer Anda di Internet



Sebelum membahas bahaya berinternet dan *hacker attack*, kita bahas dulu identitas komputer anda di Internet. Anda dapat kena bahaya dalam berinternet di antaranya karena komputer anda dapat diakses. Komputer anda dapat diakses, sebab di Internet komputer anda ini mendapatkan identitas tersendiri berupa IP address.



• *Identitas komputer anda di Internet ditetapkan dalam bentuk IP address yang dapat dilihat dengan mengetikkan winipcfg.*

Begitu anda terhubung ke Internet melalui ISP (Internet Service Provider) anda, maka anda akan mendapatkan identitas berupa IP address. IP address pada pemakai Internet biasa (*dial up*) biasanya merupakan IP dinamis, yaitu berubah-ubah setiap kali terhubung ke Internet.

IP address komputer lokal yang tidak terhubung ke Internet adalah 127.0.0.1, sedangkan apabila terhubung ke Internet akan mendapatkan lagi satu IP address, misalnya 203.125.33.90 (atau lainnya tergantung ISP anda).

Untuk mengetahui berapa IP address anda, pilih **Start > Run** dan pada kotak dialog Run ketikkan **winipcfg** dan akan tampil kotak informasi IP Configuration. Pilih PPP Adapter dan di situ terlihat berapa IP address komputer anda. IP address ini terlihat oleh pihak lain di luar, sehingga dapat menjadi obyek serangan.

Apabila komputer anda merupakan bagian dari LAN (*local area network*), dan koneksi ke Internet secara bersama-sama melalui satu komputer (disebut *proxy server*), maka IP address komputer anda ditetapkan secara lokal oleh administrator, biasanya IP address lokal ini formatnya 192.168.x.x atau sejenisnya. IP address ini tidak terlihat oleh pihak luar, sehingga komputer anda terlindung oleh *proxy server* tadi.

Bahwa komputer anda menggunakan Windows 9x/ME atau Windows NT ataupun yang lain dapat pula diketahui dari luar, sebab setiap sistem operasi mempunyai 'sidik jari'-nya sendiri-sendiri. Khusus untuk Windows 9x/ME terlihat dari terbukanya port 139 (pada NT port 135 dan 139). Port lain yang lazim terbuka pada komputer anda (ini hal biasa sebab untuk mengirim dan menerima email) adalah port 25 (SMTP, mengirim email) dan 110 (POP3, menerima email).

• *Scan komputer anda sendiri untuk melihat port-port apa saja yang terbuka. Dapatkan port-port ini sebelum hacker yang mendapatkannya!*

Mengenal Internet Port Number

Service pada Internet diakses melaui port-port tertentu. Pada setiap IP address dapat diaktifkan port dengan nomor 0 sampai 65535 (didapat dari 2 pangkat 16). Port ini bersifat logis (bukan fisik seperti halnya serial port atau parallel port pada komputer anda), tapi seperti juga port fisik, digunakan untuk mengakses servis-servis tertentu pada Internet.

Port yang lazim digunakan adalah:

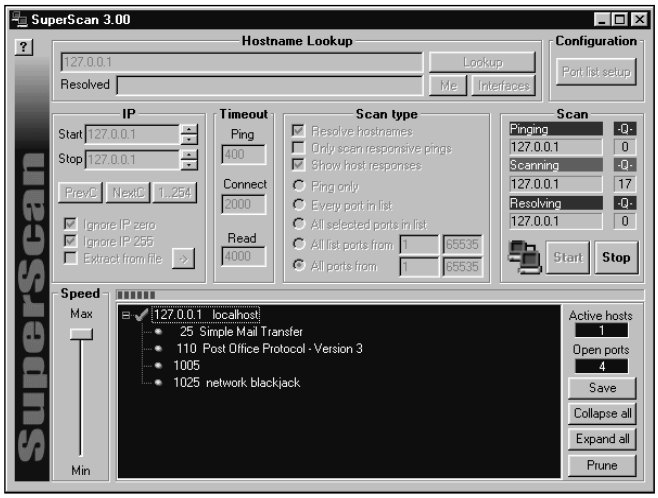
Port 21	FTP (File Transfer Protocol)
Port 22	SSH (Secure Shell)
Port 23	Telnet
Port 25	SMTP (Simple Mail Transfer Protocol)
Port 80	HTTP (Hypertext Transfer Protocol)
Port 110	POP3 (post office protocol, version 3)
Port 119	NNTP (Network News Transfer Protocol)
Port 139	NetBIOS session service
Port 143	IMAP (Internet Message Access Protocol)
Port 194	IRC (Internet Relay Chat Protocol)

Bila kita mengakses suatu servis di Internet, maka port-port di atas yang digunakan, tergantung pada jenis servicenya. Bila kita berselancar (*browsing*), maka kita mengakses port 80 pada situs yang kita akses. Bila kita mengambil email, maka digunakan port 110. Mengirim email menggunakan port 25. Web email menggunakan port 143. Membaca newsgroup lewat ISP anda menggunakan port 119. Chatting menggunakan port 194, dan lain sebagainya.

Adapun pada komputer kita sendiri sebagai yang mengakses service, seharusnya tidak banyak port yang terbuka. Pada umumnya hanya port 25, 110, dan 139 yang terbuka (diaumsikan menggunakan Windows 9x/ME yang membuka port 139). Khusus untuk port 139 perlu mendapat perhatian khusus, sebab dapat merupakan celah untuk masuknya penyerang ke komputer Windows 9x/ME anda.

Apabila ada lagi port-port lain yang terbuka, anda perlu waspada. Misalnya bila yang terbuka port 21. Apakah anda pernah menginstalasi program FTP server dan sekarang sedang berjalan? Juga bila port 23 terbuka, apakah anda menjalankan service Telnet? Kedua port ini tidak lazim terbuka pada komputer yang hanya dipakai mengakses Internet (bukan memberi service pada komputer lain).

Untuk mengetahui mana port-port yang terbuka, gunakan scanner seperti SuperScan atau UltraScan dan scan IP lokal anda (127.0.0.1) seperti contoh di bawah ini:



Di sini tampak bahwa ada 4 port yang terbuka. Port 25 dan 110 biasa terbuka, tetapi apa itu port 1005 dan 1025?

Dengan mencari informasi di Internet melalui *search engine* (misalnya Google, **www.google.com**) akan didapat bahwa port 1005 adalah port Theef Trojan dan port 1025 adalah port Network Blackjack. Port-port apa ini?

Dari mana port ini bisa terbuka? Port 1005 kemungkinan secara tidak sengaja kita men-*download* suatu program, menjalankannya dan diam-diam Trojan Theef diaktifkan, membuka port ini, dan menjadikan komputer kita suatu server bagi komputer orang lain yang mempunyai pengendalinya! Adapun port 1025 tampaknya terbuka sewaktu secara tidak sengaja kita mengunjungi situs judi di Internet.

Bahaya Berinternet

Bahaya sewaktu berinternet sudah dimulai sewaktu anda berselancar dan dapat dibagi atas dua bagian besar:

- *Remote Controlled PC*
- Infeksi Digital: Virus dan Trojan

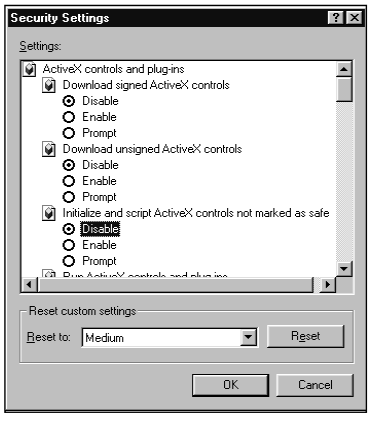
Remote Controlled PC

Pada awalnya situs web hanya berisi teks dan gambar dan ini merupakan kemajuan pesat sejak adanya Internet. Namun hal ini tidak berlangsung lama, sebab web menjadi lebih dinamis dengan menyertakan komponen-komponen aktif kedalamnya. Komponen-komponen ini selain membuat web lebih menarik, juga menyimpan potensi bahaya dari penyalahgunaannya. Ada empat active component yang sedang marak, yaitu **ActiveX**, **Java applet**, **JavaScript**, dan **VBScript.**

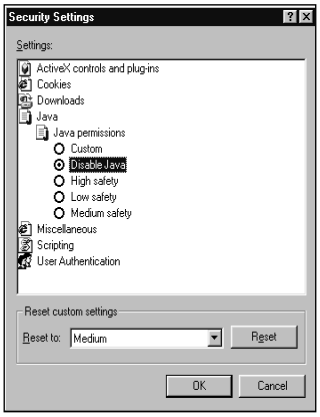
Apabila *static content* disajikan dari server, maka *active content* dijalankan pada komputer pengguna. Pada Windows, *active content* yang paling berbahaya adalah milik Microsoft sendiri, yaitu ActiveX. Suau komponen ActiveX adalah *executable program* yang *built-in* pada suatu situs web. Bila anda masuk ke situs web ini, maka *browser* akan me-*load* halaman web ini beserta *built-in component*-nya, dan menjalankannya pada komputer anda.

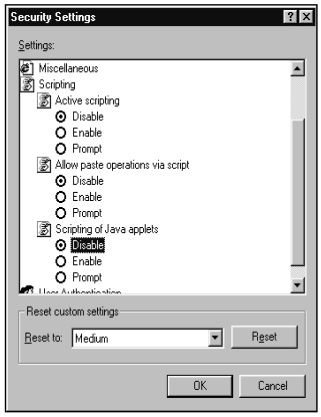
Komponen ActiveX yang dapat dibuat dengan Visual Basic ini (juga dari Microsoft) mempunyai beberapa sifat sebagai berikut:

- Sebagai suatu program Visual Basic, dapat mengakses semua fungsi pada PC anda. Browser anda tidak dapat mengendalikan fungsi apa yang akan dijalankan dan apa yang tidak.
- Hanya *programmer*-nya yang tahu fungsi apa pada PC anda yang akan dijalankannya. Bisa saja misalnya suatu situs web menawarkan suatu game, yang bila anda mainkan akan menginstalasi Trojan pada komputer anda (atau lebih gawat lagi langsung mem-format hard disk anda!) sewaktu anda menjalankannya.



Untuk melindungi komputer anda dari bahaya ActiveX, paling baik dengan me-non-aktifkannya. Caranya pada browser pilih **Tools > Internet Options** untuk masuk ke jendela **Internet Options**. Disini pilih **tab Content** dan klik tombol **Custom Level.** Pilih *disable* terhadap ActiveX.





Walaupun tidak seberbahaya ActiveX, Java applet juga patut diwaspadai. Java lebih memperhatikan keamanan data pemakai dibandingkan ActiveX. Ada beberapa aturan yang harus diikuti oleh suatu program Java:

- Hanya mengakses daerah tertentu pada sistem file komputer lokal.
- Tidak menjalankan program lain pada komputer lokal.
- Dijalankan hanya pada PC yang terhubung ke Internet
- Hanya mengakses sistem file lokal atau melakukan pertukaran data melalui jaringan dan tidak bisa dua-duanya.
- Tidak dapat mengakses memori dari program.

Walaupun demikian, bisa saja terjadi kesalahan pemrograman. Misalnya port tertentu setelah digunakan oleh Java applet tetap terbuka sehingga dapat dimanfaatkan oleh hacker. Namun hal ini memerlukan keterampilan khusus, sehingga dalam hal ini Java applet boleh dikatakan aman.

Namun untuk memastikan pengamanan PC anda, boleh saja anda men-*disable* Java pada browser anda. Pilih **Tools > Internet Options**. Pilih **tab Security** pada jendela **Internet Options**, klik **Custom Level** untuk mendapatkan jendela **Security Setting** dan tick pada Disable Java.

Apabila Java applet bersifat lebih aman, maka tidak demikian dengan **JavaScript** dan **VBScript**. Banyak hal mengenai software yang terinstal pada komputer anda dapat diintip dengan JavaScript maupun VBScript. Mereka juga dapat berulang-ulang membuka window baru pada komputer anda, suatu hal yang menjengkelkan yang mungkin pernah anda alami juga.

Baik JavaScript maupun VBScript dapat di-nonaktifkan pada browser anda. Kali ini pada pilihan Scripting tick pada Disable.

Infeksi Digital: Virus dan Trojan

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 jaringan (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 selalau 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, McAffee, dan PC Cillin, terdapat pula anti virus *freeware* yang tidak kalah kemampuannya dalam melindungi anda terhadap virus. Ada 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 *server*-nya yang akan dikendalikan penyerang lewat versi *client*-nya.

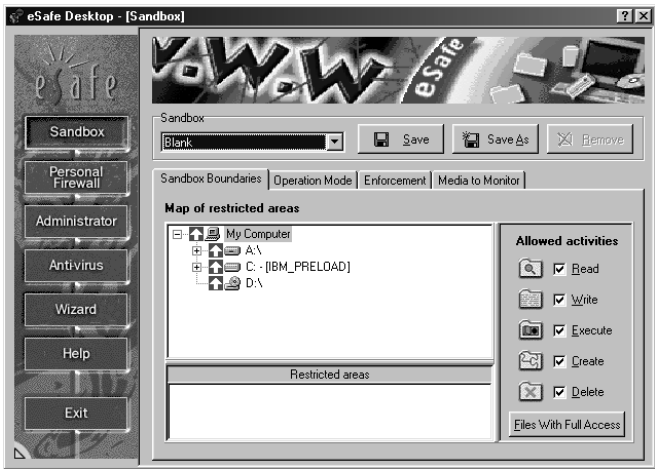
Antivirus kini mampu juga mendeteksi adanya trojan, tetapi paling baik menggunakan *scanner* yang ditujukan untuk mendeteksi trojan. Berbeda dengan antivirus yang mendeteksi trojan hanya dari file-nya, maka *trojan scanner* mendeteksi trojan juga dengan melakukan scan terhadap port-port yang terbuka 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



• eSafe mempunyai fasilitas Sandbox untuk mengkarantina hasil download dan menjalankannya di bawah lingkungan terkendali

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 partisi 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.

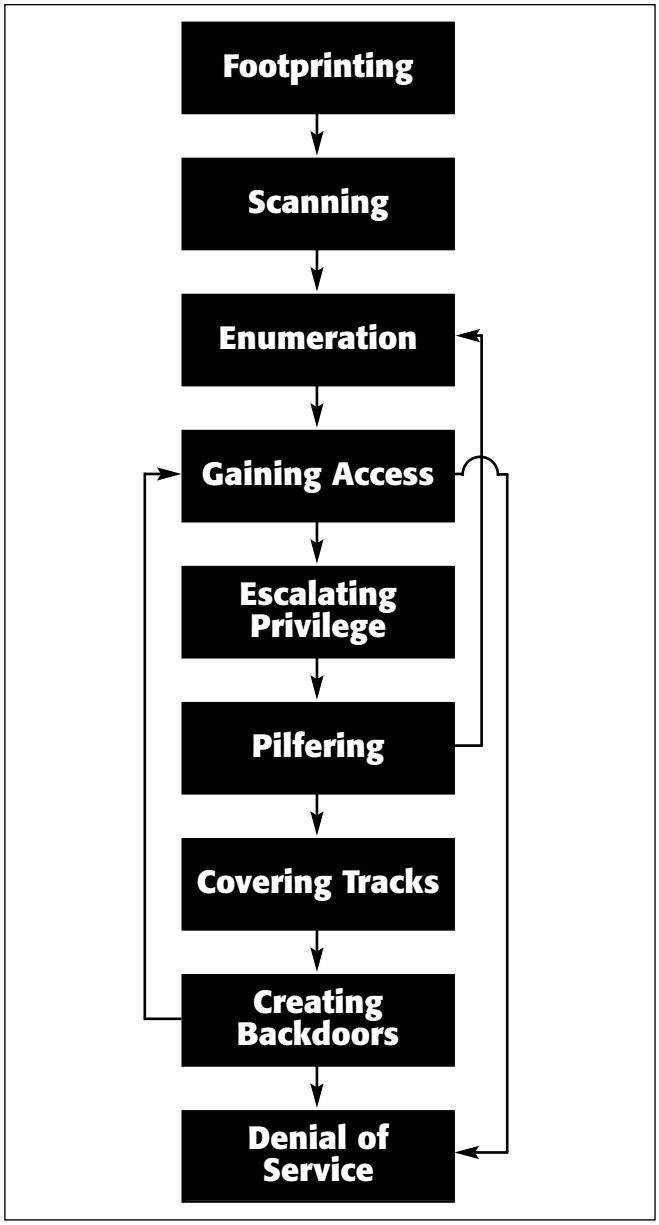
Sandbox pada eSafe dapat dikonfigurasi, namun sudah terdapat aturan tinggal pakai untuk kebanyakan proses pengujian software:

- **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 mecegah penciptaan *script file* berbahaya.

Hacker Attack

Gambaran mengenai *hacker* yang berupa orang gila komputer yang lusuh, kini sudah tidak tepat lagi. Dengan adanya Internet siapa pun dengan sedikit kemauan dan kegigihan bisa menjadi *hacker*. *Hacking* kini sudah menjadi kegiatan untuk memanfaatkan waktu luang, terutama oleh para hacker amatir yang dikenal sebagai *script kiddies*.

Untuk melindungi komputer anda sewaktu berinternet, anda perlu mengetahui cara kerja *hacker* mengakses suatu sistem, yang secara sederhana dapat digambarkan sebagai berikut:



Hacking merupakan 'seni' tersendiri yang melibatkan proses mencari serpihan-serpihan informasi yang bertebaran di mana-mana dan seolah-olah tidak ada hubungannya satu sama lainnya. Untuk memberi gambaran tentang keseluruhan proses hacking, di bawah ini disajikan langkah-langkah logisnya.

1. **Footprinting**. Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan *search engine*, whois, dan DNS zone transfer.
2. **Scanning**. Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan *ping sweep* dan *port scan*.
3. **Enumeration**. Telaah intensif terhadap sasaran, yang mencari *user account* absah, *network resource and share*, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.
4. **Gaining Access**. Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, serta melakukan *buffer overflow*.
5. **Escalating Privilege**. Bila baru mendapatkan *user password* di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan *password cracking* atau *exploit* sejenis getadmin, sechole, atau lc_messages.
6. **Pilfering**. Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke *trusted system*. Mencakup evaluasi *trust* dan pencarian *cleartext password* di registry, config file, dan *user data*.
7. **Covering Tracks**. Begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan *network log* dan penggunaan *hide tool* seperti macam-macam *rootkit* dan *file streaming*.
8. **Creating Backdoors**. Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk *user account* palsu, menjadwalkan *batch job*, mengubah *startup file*, menanamkan servis pengendali jarak jauh serta *monitoring tool*, dan menggantikan aplikasi dengan trojan.
9. **Denial of Service**. Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trincoo, smurf, dan lain-lain.

Pada tahap 1 (footprinting), *hacker* baru mencari-cari sistem mana yang dapat disusupi. *Footprinting* merupakan kegiatan pencarian data berupa:

- Menentukan ruang lingkup (*scope*) aktivitas atau serangan
- Network enumeration
- Interogasi DNS
- Mengintai jaringan

Semua kegiatan ini dapat dilakukan dengan *tools* dan informasi yang tersedia bebas di Internet. Kegiatan footprinting ini diibaratkan mencari informasi yang tersedia umum melalui buku telepon. *Tools* yang tersedia untuk ini di antaranya

- **Teleport Pro:** Dalam menentukan ruang lingkup, *hacker* dapat men-download keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon, contact person, dan lain seagainya.
- **Whois for 95/9/NT:** Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (*domain hijack*).
- **NSLookup:** Mencari hubungan antara *domain name* dengan IP address.
- **Traceroute 0.2:** Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

Tahap 2 atau scanning lebih bersifat aktif terhadap sistem-sistem sasaran. Di sini diibaratkan *hacker* sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya.

Kegiatan *scanning* dengan demikian dari segi jaringan sangat 'berisik' dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali menggunakan *stealth scanning*.

Scanning tool yang paling legendaris adalah **nmap** (yang kini sudah tersedia pula untuk Windows 9x/ME maupun DOS), selain **SuperScan** dan **UltraScan** yang juga banyak digunakan pada sistem Windows.

Untuk melindungi diri anda dari kegiatan scanning adalah memasang firewall seperti misalnya **Zone Alarm**, atau bila pada keseluruhan network, dengan menggunakan IDS (Intrusion Detection System) seperti misalnya **Snort**.

Tahap 3 atau enumerasi sudah bersifat sangat intrusif terhadap suatu sistem. Di sini penyusup mencari *account name* yang absah, *password*, serta *share resources* yang ada.

Pada tahap ini, khusus untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk *resource sharing* antar-pemakai dalam jaringan.

Anda mungkin berpikir bahwa hard disk yang di-*share* itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian. **NetBIOS session service** dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia! Tools seperti Legion, SMBScanner , atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka *resource share* tanpa *password*).

Tahap 4 atau gaining access adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai *user* biasa. Ini adalah kelanjutan dari kegiatan enumerasi, sehingga biasanya di sini penyerang sudah mempunyai paling tidak *user account* yang absah, dan tinggal mencari *password*-nya saja.

Bila *resource share*-nya diproteksi dengan password, maka *password* ini dapat saja ditebak (karena banyak yang menggunakan *password* sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui **dictionary attack** (mencobakan kata-kata dari kamus sebagai password) atau **brute-force attack** (mencobakan kombinasi semua karakter sebagai password). Dari sini penyerang mungkin akan berhasil memperoleh logon sebagai *user* yang absah.

Tahap 5 atau Escalating Privilege mengasumsikan bahwa penyerang sudah mendapatkan *logon access* pada sistem sebagai *user* biasa.

Penyerang kini berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi *dictionary attack* atau *brute-force attack* yang memakan waktu itu, melainkan mencuri *password file* yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem.

Pada sistem Windows 9x/ME password disimpan dalam file .PWL sedangkan pada Windows NT/2000 dalam file .SAM.

Bahaya pada tahap ini bukan hanya dari penyerang di luar sistem, melainkan lebih besar lagi bahayanya adalah 'orang dalam' yaitu *user* absah dalam jaringan itu sendiri yang berusaha 'naik kelas' menjadi admin atau root.

Pada tahap 6, 7, dan 8 penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan (**pilfering**), menutupi jejak penyusupannya (**covering tracks**), dan menyiapkan pintu belakang (**creating backdoor**) agar lain kali dapat dengan mudah masuk lagi ke dalam sistem.

Adanya Trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri.

Terakhir, denial of service, bukanlah tahapan terakhir, melainkan kalau penyerang sudah frustrasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu *crash*.

Denial of service attack sangat sulit dicegah, sebab memakan habis *bandwidth* yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para *script kiddies* yang pengetahuan *hacking*-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

Bagaimana Hacker Mendapatkan Password?

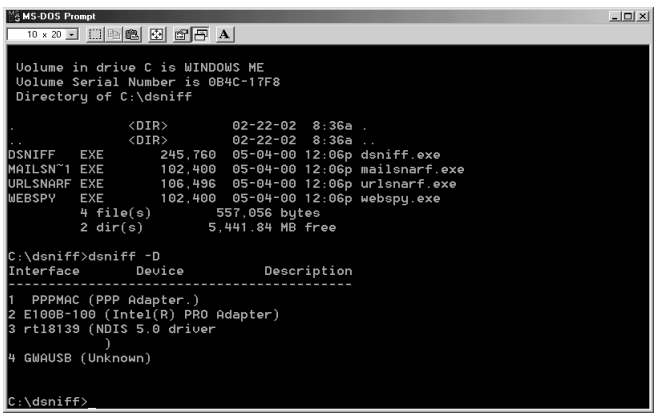
Dari langkah-langkah yang dibahas di atas, paling tidak ada tiga langkah yang melibatkan kegiatan mendapatkan *password*, pada *enumeration*, *gaining access*, dan *escalating privileg*e. Password dapat diperoleh dengan banyak cara.

Password cracking hanyalah salah satu cara yang digunakan hacker untuk mendapatkan password anda. Ada banyak lagi cara lain, termasuk **social engineering**, yaitu kata lain dari menipu.

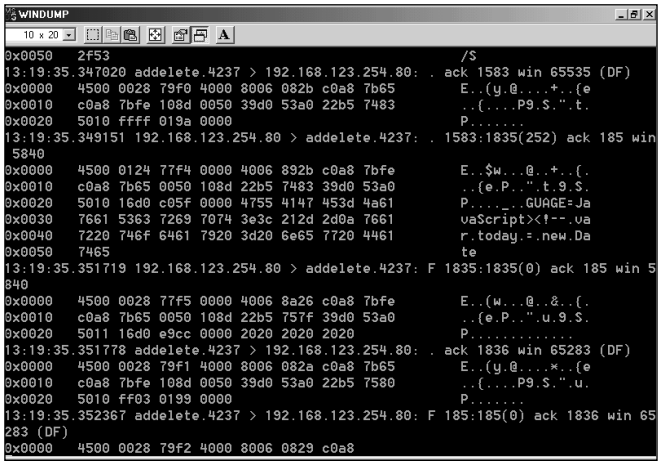
Pada dasarya ada empat cara untuk mendapatkan *password* secara 'lebih terhormat,' yaitu:

- Menghadang email yang mengirimkan *password* pada anda.
- Menggunakan *password cracker* untuk mendapatkan *password* anda.
- Menggunakan *web spoofing* untuk melihat apa yang anda ketikkan secara *online*, termasuk *password* anda.
- Menggunakan Java applet dan ActiveX untuk mengakses hard disk dan mencari *password* yang tersimpan di dalamnya.

Menghadang Email



• Dsniff dan mailsnarf adalah utilitas yang 'mengendus' paket-paket data yang melewati suatu network card dan menganalisanya untuk mengeluarkan password (dsniff) maupun isi emailnya (mailsnarf).

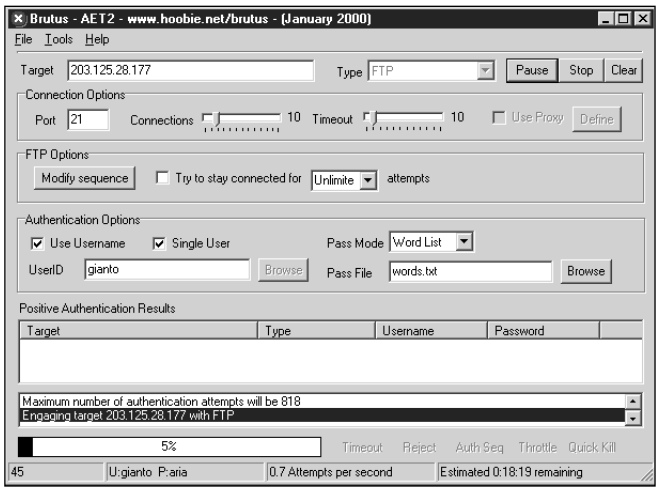


• *Seperti inilah paket-paket data yang melewati suatu network card. Di sini paket-paket data itu di-capture dengan WinPCap dan ditampilkan dan disimpan dalam file log oleh Windump.*

Pada dasarnya tidak sulit untuk menghadang email. Salah satunya adalah menggunakan **mailsnarf** yang terdapat pada utility **dsniff**. Mailsnarf menghadang paket data yang lewat di Internet dan menyusunnya menjadi suatu email utuh.

Dsniff dan mailsnarf merupakan software yang bekerja atas dasar **WinPcap** (setara dengan **libcap** pada Linux) yaitu suatu library yang menangkap paket-paket data. Paket-paket yang ditangkap ini akan disimpan dalam bentuk file oleh Windump, sedangkan Dsniff dan Mailsnarf bertindak lebih jauh lagi, yaitu menganalisa paket-paket data ini dan menampilkan password (dsniff) atau isi email (mailsnarf).

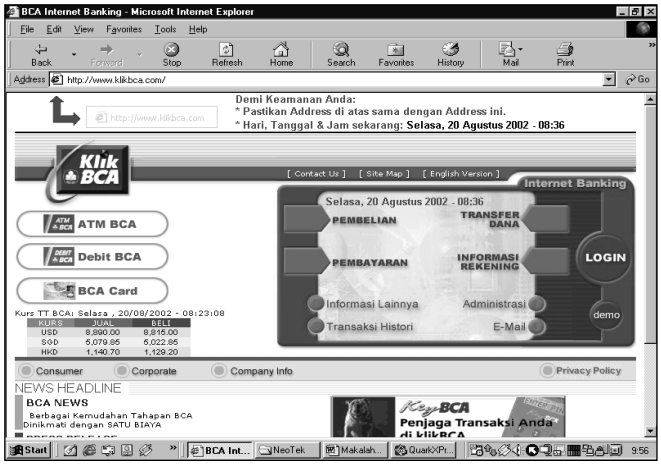
Password Cracking



• *Brutus, salah satu jenis remote password cracker yang bekerja dengan teknik dictionary attack atau brute-force attack terhadap port-port http, POP3, ftp, telnet, maupun NetBIOS.*

Ada dua macam *password cracker*. Cara lama adalah dengan mencoba kombinasi password satu per satu sampai didapat password yang cocok. Cara ini dikenal sebagai **dictionary attack** (bila mencobakan kata-kata yang ada dalam kamus) atau **brute-force attack** (mencobakan semua kombinasi huruf, angka, dan karakter). Cara ini sangat lambat dan banyak situs yang menutup akses terhadap usaha login yang secara berturut-turut tidak berhasil.

Cara lain adalah **mencari password anda dari dalam** dan cara ini hacker harus masuk ke dalam sistem anda. Ini bisa karena kelemahan sistem atau merupakan kenakalan 'orang dalam' sendiri.



• *Situs BCA sampai memberi peringatan bahwa URL yang benar untuk Internet Banking-nya adalah http://www.klikbca.com. Hal ini untuk mencegah web spoofing yang memperdaya nasabahnya.*

Web Spoofing

Web spoofing pada dasarnya adalah usaha menipu anda agar anda mengira bahwa anda sedang mengakses suatu situs tertentu, padahal bukan. Cara yang pernah dilakukan terhadap situs web BCA adalah dengan membuat situs mirip BCA yang membuat orang terkecoh sehingga tanpa curiga mengetikkan nama dan *password*-nya dan nama dan *password* itupun direkam di server palsu tadi.

Cara lain adalah dengan menjadi situs web perantara anda dengan situs yang anda akses. Dengan kata lain menjadi *proxy server* untuk anda dalam berselancar. Ada contoh *proxy server* yang tidak berbahaya, yaitu **Anonymizer** (http://www.anonymizer.com/), yang membuat identitas anda tidak diketahui oleh situs yang anda kunjungi. Tetapi seluruh identitas anda (dan juga apa yang anda lakukan justru diketahui oleh *proxy server* ini).

• *Anonymizer adalah servis untuk berselancar secara anonim. Memang identitas anda tidak akan diketahui oleh situs yang anda kunjungi, tetapi segala hal mengenai diri anda justru dketahui oleh servis ini. Teknik yang digunakan oleh servis ini dapat ditiru untuk membuat situs curang yang tujuannya mengintip semua informasi anda.*

Java applet dan ActiveX

Suatu applet Java atau ActiveX dapat diciptakan untuk mengakses hard disk anda dan melakukan apa saja terhadapnya, termasuk membaca *password* yang tersimpan dalam program penyimpan *password*.

Fasilitas Windows yang menawarkan untuk mengingat *password* anda sangat berbahaya, sebab membuat *password* itu tersimpan di *cache memory* dan dapat diakses dengan mudah dengan pelbagai *password revealer* seperti **Snadboy's Revelation** atau **007 Password Recovery**.

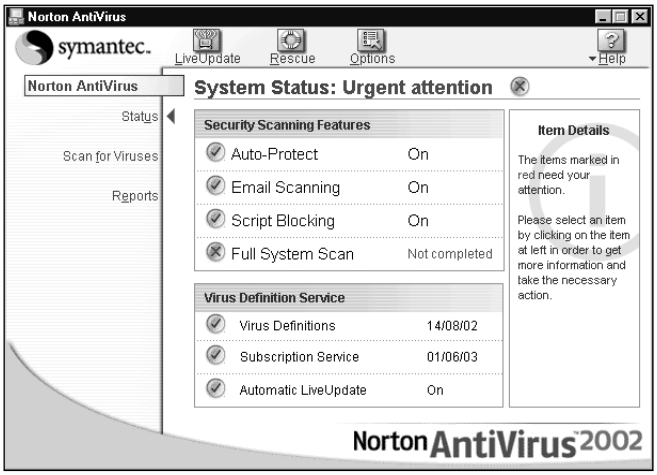
Lebih aman menyimpan password anda di secarik kertas. Tidak juga dalam zip file yang juga bisa di-*crack*.

Melindungi Komputer Anda

Untuk menghadapi sebagian besar bahaya di Internet, paling tidak komputer anda harus dilengkapi oleh dua hal berikut ini; adapun yang ketiga boleh juga digunakan untuk lebih melindungi komputer anda serta untuk menyimpan bukti adanya serangan.

- **Antivirus** yang di-*update* secara berkala. Dapat pilih Norton Antivirus, McAffee, PCCillin, Panda Anti Virus, dan Norman Anti Virus. Dapat juga gunakan versi *freeware* seperti AVG Anti Virus dan AntiVir.
- **Personal Firewall.** Yang banyak digunakan adalah Zone Alarm yang amat mudah digunakan dan cukup efektif memonitor dan mencegah akses dari Internet ke komputer anda atau sebaliknya.
- **IDS.** Menggunakan software yang mencatat (*logging*) serangan ke komputer anda. Hal ini dapat dilakukan dengan IDS (Intrusion Detection System) seperti Salus, Snort, atau BlackICE Defender.

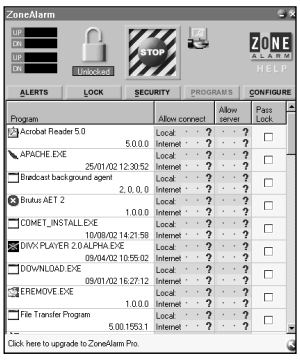
Antivirus



• *Norton Anti Virus (seperti juga McAffee dan lainnya) meng-upate data yang paling mutakhir mengenai virus yang ada secara berkala*

Antivirus akan sekaligus juga mencegah masuknya trojan ke dalam komputer anda seperti telah dibahas sebelumnya.

Firewall



• *Personal Firewall seperti Zone Alarm amat mudah digunakan.*

Firewall bertindak bahkan sebelum serangan terjadi. *Firewall* dapat berupa *software* atau *hardware* atau keduanya yang melindungi komputer anda dengan memonitor dan menyaring semua paket data yang keluar masuk komputer anda dengan Internet. *Firewall* menganalisa paket data dan mempelajari:

- Sumber paket data
- Komputer yang dituju oleh paket data
- Protokol yang digunakan
- Isi paket data

Dengan demikian, bila anda menggunakan *firewall*, maka anda dapat:

- Memblokir paket data dari alamat-alamat tertentu
- Memblokir pertukaran data antara satu PC dengan lainnya sesuai dengan yang ditentukan
- Mencegah pemakaian protokol tertentu
- Menolak paket data dengan kata-kata tertentu di dalamnya.

Snort Intrusion Detection System

Snort adalah suatu **NIDS** (**Network-based Intrusion Detection System**). Sebuah NIDS akan memperhatikan seluruh segmen jaringan tempat dia berada, berbeda dengan host-based IDS yang hanya memperhatikan sebuah mesin tempat 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 ditempelkan pada *interface* ISDN ppp0, maka sebaiknya di mesin yang sama dipasang *firewall* dan *router* sambungan *dial-up*-nya.

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

Mengoperasikan Snort

Secara umum Snort dapat dioperasikan dalam tiga mode, yaitu

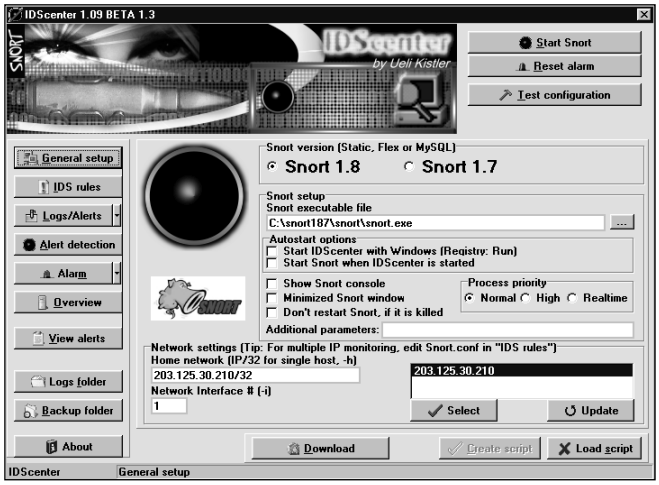
- **Sniffer mode**, untuk melihat paket yang lewat di jaringan.
- **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari.
- **Intrusion Detection mode**, pada mode ini Snort berfungsi mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk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

Snort for Windows

Snort selain terdapat pada Linux, kini terdapat pula pada Windows lengkap dengan GUI (Graphical User Interface) IDS Center yang amat memudahkan penggunaannya.

Snort memanfaatkan WinPCap untuk menangkap paket-paket data yang lalu-lalang melalui jaringan. *Download* WinPCap di **http://winpcap.polito.it/install/default.htm.**

Selanjutnya *download* Snort di **http://www.silicondefense.com/techsupport/downloads.htm**.



• *Adanya IDS Center sebagai GUI untuk Snort pada Windows membuatnya menjadi mudah digunakan.*

Download dan instal Snort for Windows versi 1.7 dan versi 1.8.7. Misal pada direktori snort.

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.

Port yang Terbuka: Mengundang Hacker

Seperti telah dibahas di awal makalah ini, anda dapat memeriksa komputer anda sendiri apakah ada port-port yang terbuka. Anda dapat menggunakan Supercan yang sangat mudah penggunaannya atau dapat juga menggunakan Nmap yang merupakan tool sangat berharga bagi seorang hacker. Sebelum hacker menemukan port terbuka pada komputer anda, dapatkan dulu sendiri hal itu sehingga anda dapat mengambil tindakan yang perlu.

Port-port yang Perlu Dicurigai

Jumlah port semuanya 65536 (0 sampai 65535). Port-port yang terkenal adalah port nomor 0 sampai 1023, port-port terdaftar dari 1024 sampai 49151, dan *dynamic* dan/atau *private port* dari 49152 sampai 65535.

Dari sekian banyak port, mana yang biasa dan aman terbuka dan mana yang tidak? Seperti dibahas sebelumnya, komputer pribadi yang hanya dipakai untuk mengakses Internet pada umumnya hanya membuka port 25 dan 110, serta 139 apabila menggunakan Windows 9x/ME. Namun online game menggunakan port-port nomor tertentu seperti 1025 untuk Network Blackjack serta Microsoft Gaming Zone menggunakan port 28800 agar para pemain dapat saling mengirim ping satu sama lain.

Untuk mempelajari apakah suatu port yang terbuka pada komputer perlu dicurigai, anda dapat dilihat di situs-situs berikut:

http://www.glocksoft.com/trojan_port.htm

atau situs serupa lain lain.

Di bawah ini beberapa port Trojan horse yang popular:

Back Orifice/Back Orifice 2000	54320, 54321
NetBus 1.60, 1.70	12345
NetBusPro 2.01	20034
SubSeven	27374

PortSentry: Menjaga Port yang Terbuka

Bahasan berikut bukanlah untuk komputer pemakai biasa, melainkan untuk komputer yang bertindak sebagai server. Apabila suatu port memang harus terbuka karena memang memberi servis tertentu pada Internet, maka untuk menjaga port tersebut dari serangan *port scan* dapat digunakan **PortSentry**. PortSentry hanya ada pada Linux, sedangkan pada sistem Windows hanya tersedia versi komersial dari **Host-based IDS** ini.

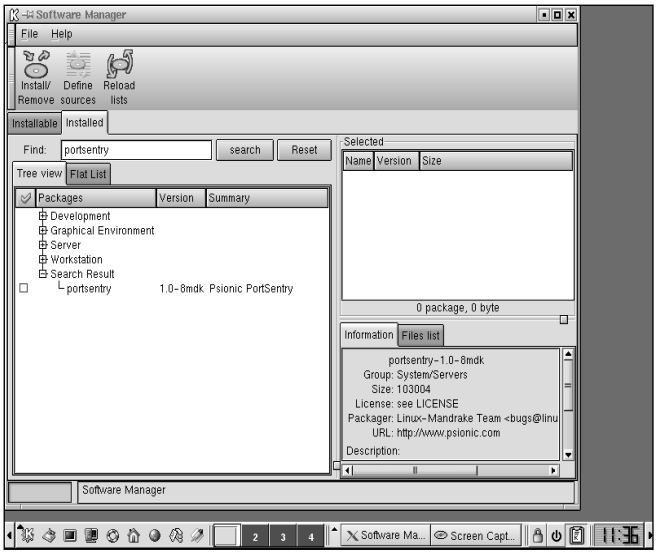
Mengapa kita perlu mendeteksi *port scan*? Jawaban versi hebohnya kira-kira sebagai berikut, *port scan* adalah awal dari masalah besar yang akan datang melalui jaringan. *Port scan* merupakan awal serangan dan hasil *port scan* membawa beberapa informasi kritis yang sangat penting untuk pertahanan mesin dan sumber daya yang kita miliki. Keberhasilan untuk menggagalkan port scan akan menyebabkan penyerang 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 dirancang untuk mendeteksi dan menanggapi kegiatan *port scan* pada sebuah mesin secara *real-time*.

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.



• *PortSentry dengan mudah dapat di-instal dari Linux Mandrake 8.0 Installation CD. Sayang pada versi 8.2 sudah tidak disertakan.*

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

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 tersamar/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 **nmap** yang merupakan salah satu *port scan software* terbaik yang ada.
- PortSentry akan bereaksi terhadap usaha *port scan* dari lawan dengan cara memblokir 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 didampingkan 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 acak (*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 acak. 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.

Email Sebagai Senjata

Bahwa virus dan worm sering dikirim melaui *attachment* email, sudah banyak diketahui orang. Setelah Nimda, sekarang ada worm Klez sampai sekarang masih saja berkeliaran, membuatnya menjadi worm yang paling sulit dibasmi. Untunglah antivirus yang ada memberi juga perlindungan dengan jalan men-scan email yang diterima (dan juga dikirim terhadap kemungkinan adanya virus). Bahkan servis web email gratis Yahoo! Memberikan juga pelayanan scan terhadap virus.

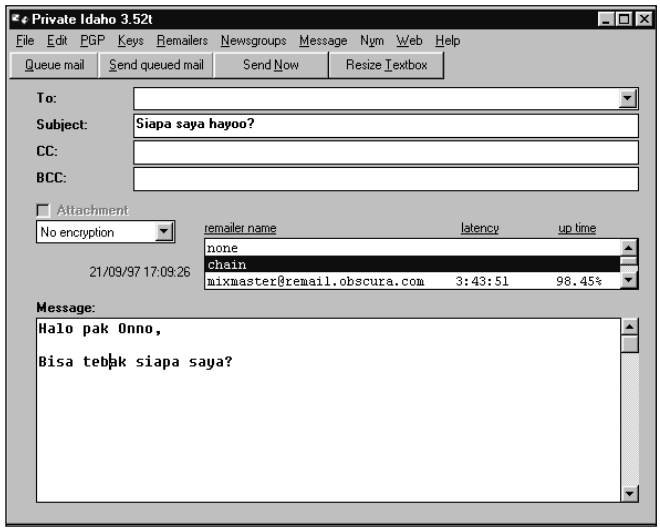
Namun selain sebagai media penyebaran virus dan worm, email itu sendiri dapat dijadikan senjata dalam perang di dunia cyber.

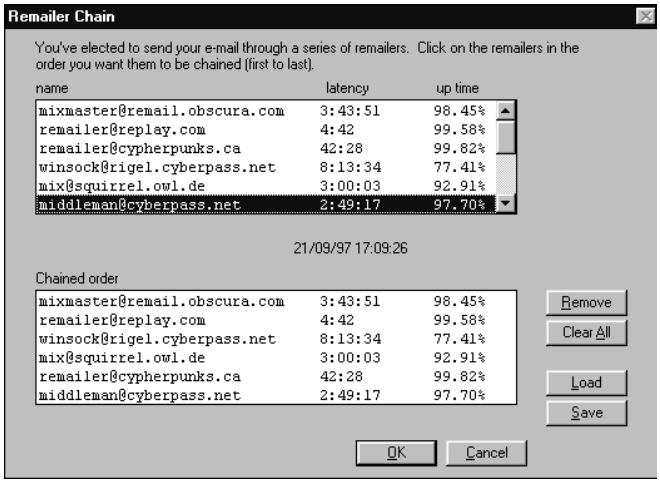
Surat Kaleng di Internet

Dengan pos biasa setiap orang bisa mengirim surat tanpa alamat si pengirim (surat kaleng); tapi bagaimana dengan email? Apakah bisa kita mengirim 'email kaleng'?

Anda dapat mengirim *anonymous email* dengan *software* seperti **Private Idaho** dengan menggunakan fasilitas **remailer** yang ada pada software ini. Private Idaho dapat di-download di **http://www.lynagh.demon.co.uk/pidaho** dan untuk menjalankannya diperlukan **VBRun300.dll** di **C:\Windows\System**. Download VBRun300.dll di sini: **http://www.bodgers.clara.net/vbrun.htm**

Gambar di bawah menunjukkan cara Private Idaho bekerja, yaitu mengirimkan email anda ke tujuan melewati beberapa kali remailer yang akan mengirimkan *anonymous email* dari satu remailer ke yang lain sebelum email itu sampai di tujuan.



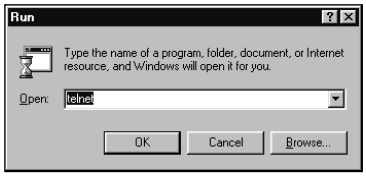


• Private Idaho memanfaatkan remailer secara berantai untuk menyembungikan identitas pengirim email.

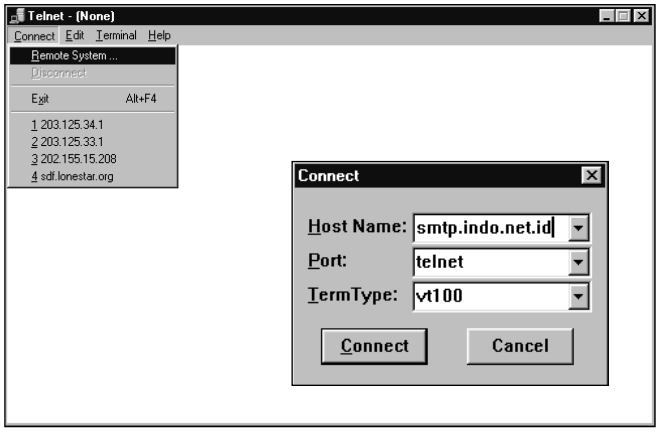
Email dengan Alamat Pengirim Palsu

Mengirim email kaleng artinya email tanpa alamat pengirim, tapi bagaimana dengan alamat palsu? Dalam pos biasa kita tinggal menulis saja alamat palsu dan memposkannya. Pada email sebenarnya juga hampir semudah itu, yaitu dengan mengakses SMTP server kita dengan telnet dan sewaktu komunikasi dengan SMTP server kita tinggal ketikkan saja email address kita (sebagai pengirim) sesuka-suka kita.

Fasilitas telnet terdapat pada setiap mesin Windows dengan menjalankan **Start > Run** lalu ketikkan **telnet**. Akan tampil jendela Telnet. Pilih menu **Connect > Remote System** dan masukkan SMTP mail anda pada Host Name dan anda akan mengakses server ini melalui fasilitas Telnet. Akses



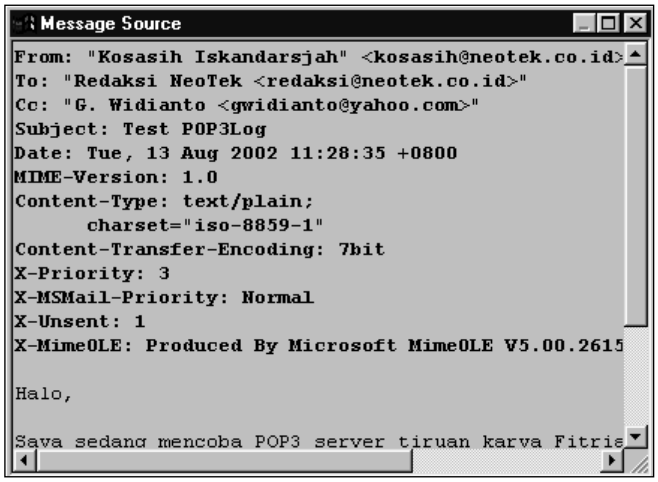
telnet ke server SMTP biasanya hanya disediakan apabila anda sebagai pelangan ISP tersebut sudah *logon* ke langsung ke server-nya melalui fasilitas *dial up*.



• *Mengakses SMTP server melalui telnet. Selanjutnya dalam komunikasi dengan server anda dapat mengirim email dengan header yang diubah sesuai keinginan anda.*

Bagaimana anda melindungi diri dari kebohongan email palsu ini? Bila anda merasa curiga terhadap email tertentu, anda harus melihat *header*-nya. Sayangnya hampir semua *mailer* secara *default* menyembunyikan data ini.

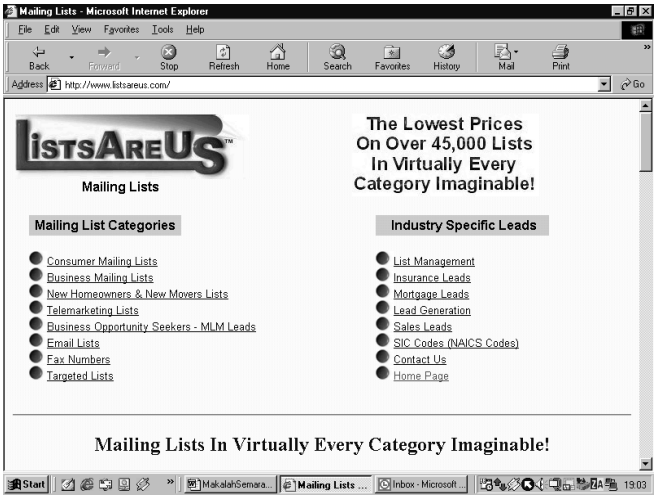
Pada Outlook Express anda dapat melihat rincian header email yang anda curigai dengan memilih email itu, lalu pilih **File > Properties** lalu pilih tab **Detail** serta tombol **Message Source**. Bandingkan isi **From:** dengan **X-Sender.** Bila berbeda, maka paling tidak anda tahu siapa pengirim sebenarnya. X-Sender berasal dari mail server pengirim dan lebih sukar dimanipulasi.



• *Apabila From: berbeda dengan X-Sender, maka palimng tidak anda tahu siapa pengitrim email yang sebenarnya.*

Email Bomb

Email dapat digunakan untuk melumpuhkan komputer yang terhubung ke Internet, bahkan seluruh jaringan komputer perusahaan dapat dilumpuhkan dengan *email bomb*. Untuk melakukan hal ini jumlah email dan ukurannya harus cukup besar untuk melumpuhkan sasarannya.



• *Mendaftarkan email korban pada banyak mailing list adalah salah satu teknik untuk mengirim email bomb.*

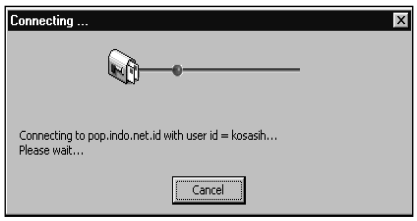
Metode paling sederhana dari *email bomb* adalah dengan mengirimkan sejumlah besar email ke alamat email korban. Jumlah email yang dikirim tidak harus ratusan, ribuan, atau lebih, namun dapat juga lebih sedikit, asalkan isinya besar, misalnya dengan memberikan *attachment* berupa file yang besar.

Email pribadi dapat saja menjadi serangan *email bomb*. Sebagai contoh bila seseorang mengirimkan anda email dengan ukuran *attachment* 10 Mbyte satu saja setiap hari, akan membuat *mailbox* anda penuh dan membuat email dari pihak lain ditolak oleh *mail server* anda.

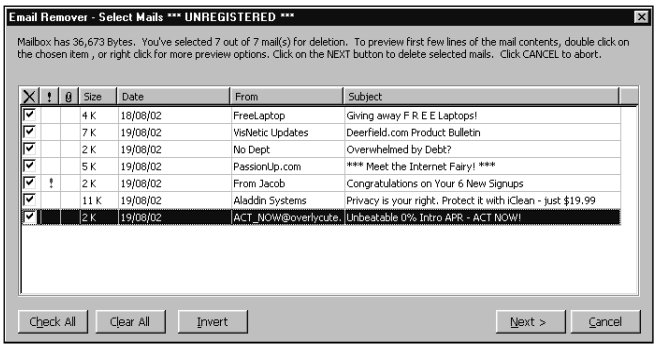
Lebih parah lagi kalau anda sebagai korban dibuat berlangganan pada sejumlah besar mailing list. Daftar mailing list dari segala macam jenis dapat dilihat di sini:

http://www.listsareus.com/

Untuk melindungi komputer anda dari *email bomb*, anda dapat menggunakan **Email Remover**, yang dapat di-*download* di **http://eremover.bizhosting.com/**



• *Dengan Email Remover anda dapat memeriksa email melalui header-nya dulu, dan email dapat dihapus tanpa harus men-download-nya.*



Dengan Email Remover anda tidak perlu men-*download* keseluruhan email, melainkan cukup *header*-nya saja. Dengan daftar email dan ukurannya anda dapat memperkirakan email mana yang tidak anda inginkan dan langsung anda hapus di sini.

Enkripsi Email

Kerahasiaan email anda terancam bukan oleh para hacker ataupun agen-agen rahasia, melainkan para *system administrator* sendiri. Para *system administrator* kadang-kadang bosan tidak tahu apa yang harus dikerjakan selain membaca-baca email orang. Mereka dapat melakukannya tampa sedikit pun meninggalkan jejak.

Symmetric Encryption

Cara mengatasi hal ini adalah dengan mengenkripsi email anda. Ada dua macam enkripsi, **Symmetric Encryption** dan **Asymmetric Encryption**. Pada *symmetric encryption*, pengirim dan penerima menggunakan kunci yang sama (simetrik). Yang menjadi masalah adalah bahwa kunci ini harus dikirim pada penerima agar dapat membuka file yang dienkripsi tadi. Kunci ini harus dikirim lewat jalur yang aman, baik lewat telepon, disket, atau format penyimpan data lainnya. Dan tentunya jangan dikirin lewat pos biasa.

Standard yang terkenal dalam hal *symmetric encrytion* ini adalah DES (Data Encryption Standard) yang dikembangkan oleh IBM dan NSA (National Security Agency) pada awal tahun 70-an. Sekarang ini DES digunakan dalam banyak sistem di Internet seperti *secure web protocol* (HTTPS) dan SSL selain juga pada *home banking standard* (HBCI). Salah satu variasi DES adalah Triple DES (3DES) yang memproses tiga proses sehingga mencapai panjang kunci total 192 bit.

Asymmetric Encryption

Untuk mengatasi masalah pengiriman kunci seperti yang terdapat pada *symmetric encryptrion*, dikembangkan asymmetric encryption, yang di sini kedua belah pihak memegang satu dari pasangan kunci.

Personal key hanya untuk pemakaian sendiri dan harus tetap rahasia dan tidak diberikan pada orang lain. Kunci ini dapat men-enkrip dan men-dekrip pesan yang dienkripsi dengan *public key*.

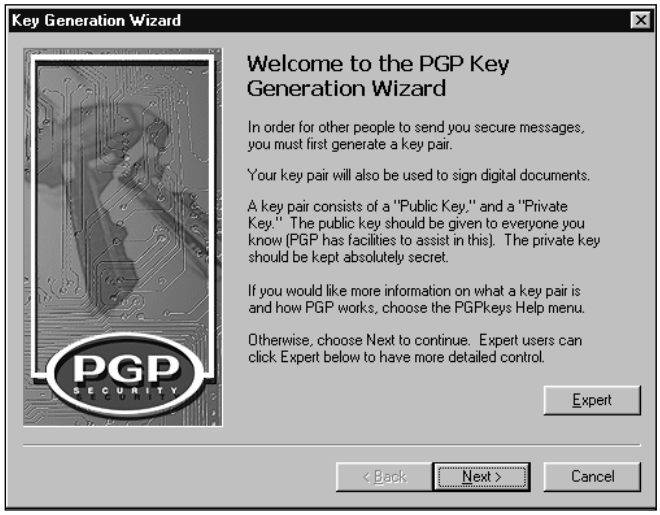
Public key ditujukan untuk didistribusikan pada rekan komunikasi dari pemegang *private key*. *Public key* akan digunakan untuk mengirimkan pesan terenkripsi yang hanya dapat dibuka menggunakan *private key*.

Untuk memudahkan pengertian, bayangkan bahwa *public key* adalah gembok sedangkan *private key* adalah anak kuncinya. Pemilik anak kunci mengirim gembok pada rekanannya dan meminta agar pesan yang dikirim digembok dulu sebelum dikirim. Pesan itu aman dalam perjalanan sebab pesan yang sudah digembok tidak bisa dibuka sebab kunci untuk membukanya hanya ada di pihak penerima pesan (yang juga pengirim gembok tadi).

Proses enkripsi asimetrik yang paling terkenal adalah RSA (dari nama penciptanya Rivest, Shamir, dan Adleman). RSA menggunakan proses matematis yang lebih kompleks dibandingkan dengan DES. Hal ini membuatnya memerlukan waktu lebih lama untuk membentuk enkripsi yang lebih aman. Anda harus memilih antara keamanan dengan efisiensi.

Personal Encryption

Kriptografi yang mudah digunakan namun tangguh baru ada semenjak Phil Zimmerman memperkenalkan programnya PGP (Pretty Good Privacy) pada tahun 1991. PGP memanfaatkan *public key cryptography* untuk enkripsi dan *digital signing* terhadap file-file umum seperti email. PGP



dengan cepat menjadi standar *de facto* untuk *personal cryptography*, walaupun PGP masih merupakan produk yang dibatasi ekspornya oleh pemerintah AS, sehingga Zimmerman bolak-balik diperiksa oleh pejabat bea cukai AS selama tiga tahun.

PGP adalah sistem enkripsi hybrid, yang memanfaatkan baik *public key* maupun algoritma enkripsi konvensional. Untuk meng-enkrip suatu pesan, suatu kunci rahasia diciptakan dan digunakan untuk mengenkripsi pesan itu. Kunci ini kemudian dienkripsi dengan *public key* dari penerima pesan dan di-*attach* bersama pesan yang dienkripsi tadi.

PGP juga digunakan sebagai *digital signature* yang memastikan bahwa suatu pesan memang pesan asli dari pengirimnya.

PGP dapat diperoleh bebas untuk pemakaian pribadi dan bentuknya yang paling populer adalah seri v2.6.x menggunakan algoritma IDEA (lisensi gratis untuk pemakaian pribadi pada PGP) untuk *key encryption* rahasianya dan algoritma RSA untuk bagian *public key*-nya.

Steganografi

Berbeda dengan PGP yang mengenkripsi file menjadi teks acak, maka steganografi men-enkripsi teks dengan menyembunyikannya pada file gambar atau suara. Steganografi adalah salah satu jenis enkripsi yang menggunakan **symmetric key**.

Penutup

Masih ada lagi beberapa aspek yang sejalan dengan topik **Hacking dan PC Security**, di antaranya adalah *web site hacking* yang sering terjadi sekarang ini. *Web site hacking* banyak terjadi pada sistem-sistem yang menggunakan IIS (dengan Windows NT/2000) mengingat cukup banyak kelemahan-kelemahan pada sistem ini.

Namun demikian, karena titik berat bahasan ini adalah untuk keamanan pemakai komputer, topik ini tidak dibahas dalam makalah ini. *Remote hacking* terhadap server Windows NT dengan memanfaatkan kelemahan Unicode-nya dapat dibaca di NeoTek Desember 2001.

Bacaan Lanjutan

Daftar bacaan lanjutan di bawah ini khusus hanya merujuk pada artikel-artikel yang pernah dibahas di majalah NeoTek dan disusun secara tematik sesuai dengan urutan bahasan pada makalah ini.

Pengantar Hacking dan PC Security

- Hacker Riwayatmu Kini...
  NeoTek Vol. II/1 (Oktober 2001), hlm. 22–24
- Masyarakat Hacker
  NeoTek Vol. II/1 (Oktober 2001), hlm. 26–28
- New Order: Situsnya para Hacker
  NeoTek Vol. II/1 (Oktober 2001), hlm. 29
- Remote Hacking: Bagaimana langkah-langkahnya?
  NeoTek Vol. II/2 (November 2001), hlm. 22–25
- Anatomi Proses Hacking
  NeoTek Vol. II/8 (Mei 2002), hlm. 45 (box)

Local Attack

- Software Cracking: Memacu Belajar Assembly Language
  NeoTek Vol. II/4 (Januari 2002), hlm. 21–23
- Password Cracking dengan Disassembler dan Hex Editor
  NeoTek Vol. II/4 (Januari 2002), hlm. 24–27
- SoftICE untuk Serial Fishing: Memancing Serial Number
  NeoTek Vol. II/6 (Maret 2002), hlm. 18–23
- Memulihkan Password: Office 2000
  NeoTek Vol. II/12 (September 2002), hlm. 18–19
- Memulihkan Password: Archive File
  NeoTek Vol. II/12 (September 2002), hlm. 20–21
- Menembus Password ID pada Outlook Express
  NeoTek Vol. II/12 (September 2002), hlm. 22–23
- Kalau Hacker-nya Orang Dalam (Legion 2.1)
  NeoTek Vol. II/8 (Mei 2002), hlm. 6

Bahaya Berinternet: Virus, Trojan, Malicious Codes

- Hacking Itu Gampang: Pakai Saja Back Orifice
  NeoTek Vol. II/1 (Oktober 2001), hlm. 30–31
- Hacking dengan Bac orifice dan Deep Back Orifice
  NeoTek Vol. II/12 (September 2002), hlm. 20–23
- Hacking Menjadi Mudah dengan NetBus Trojan
  NeoTek Vol. II/11 (Agustus 2002), hlm. 33–35
- BO2K Client Mengendalikan BO2K Server
  NeoTek Vol. II/12 (September 2002), hlm. 38–39
- BO Peep: Mengintip Korban Secara Streaming Video!
  NeoTek Vol. II/12 (September 2002), hlm. 40–41
- Konfigurasi BO2K
  NeoTek Vol. II/12 (September 2002), hlm. 36–37
- Berduel dengan Virus Makro & Trojan Horse
  NeoTek Vol. II/1 (Oktober 2001), hlm. 32–34
- Membasmi Virus CIH
  NeoTek Vol. II/8 (Mei 2002), hlm. 7
- Mengenal Infeksi Digital: Virus Komputer
  NeoTek Vol. II/11 (Agustus 2002), hlm. 8–9
- Bereksperimen dengan Walrus Macro Virus Generator
  NeoTek Vol. II/11 (Agustus 2002), hlm. 12–13
- VBS Worm Generator: Pembuat Worm Instan
  NeoTek Vol. II/11 (Agustus 2002), hlm. 14–15
- Infeksi Digital: Trojan Horse
  NeoTek Vol. II/11 (Agustus 2002), hlm. 16–17
- Virus dan Trojan: Infeksi Digital
  NeoTek Vol. II/11 (Agustus 2002), hlm. 10

Hacker Attack

- Footprinting: Intelijen Awal Hacking
  NeoTek Vol. II/3 (Desembar 2001), hlm. 38–39
- Port Scanning: Melihat Kondisi Target di Internet
  NeoTek Vol. II/2 (November 2001), hlm. 26–27
- Hacking & Keamanan Jaringan: Scanning & Scanning Tool
  NeoTek Vol. II/8 (Mei 2002), hlm. 34–39
- SuperSCAN: Tool Scanning Jarngan di Windows
  NeoTek Vol. II/8 (Mei 2002), hlm. 40–42
- Nmap kini Tersedia untuk Window 9x/ME dan DOS
  NeoTek Vol. III/1 (Oktober 2002), hlm. 0
- Password untuk Folder dengan JavaScript
  NeoTek Vol. III/1 (Oktober 2002), hlm. 28–29
- Enumerasi: Mematangkan Serangan
  NeoTek Vol. II/10 (Juli 2002), hlm. 26–32
- Legion v2.1: Gampang Kok Jalan-jalan ke Komputer Orang
  NeoTek Vol. II/10 (Juli 2002), hlm. 34–35
- Gaining Acess: Remote Password Cracking
  NeoTek Vol. III/1 (Oktober 2002), hlm. 46–48
- Password Cracking: Seni dan Tekniknya
  NeoTek Vol. II/12 (September 2002), hlm. 7–11
- PWL View: cache password revealer
  NeoTek Vol. II/10 (Juli 2002), hlm. 5 (box)
- Intip Password ! (lagi): Snadboy's Revelation
  NeoTek Vol. II/10 (Juli 2002), hlm. 0
- Cain & Abel: Pasangan Pencuri Password
  NeoTek Vol. II/12 (September 2002), hlm. 12–15
- L0phtCrack: Password Cracker untuk NT
  NeoTek Vol. II/12 (September 2002), hlm. 16–17
- Packet Sniffing dengan Tcpdump
  NeoTek Vol. II/7 (April 2002), hlm. 31–35
- Dsniff: Cara Mudah Mengintip Password
  NeoTek Vol. II/7 (April 2002), hlm. 38–39
- Password, Nih! (ICQ Password Grabber)
  NeoTek Vol. II/8 (Mei 2002), hlm. 0

Melindungi Komputer Anda

- Belajar Jadi Hacker? Coba Dulu AATools
  NeoTek Vol. II/1 (Oktober 2001), hlm. 24–25
- Lindungi Diri Anda dari Para Packet Sniffer
  NeoTek Vol. II/7 (April 2002), hlm. 37
- Policy Editor sebagai Pelindung MS Windows
  NeoTek Vol. II/10 (Juli 2002), hlm. 36–39
- Mengganti Ikon, Nama & Tooltip Folder Khusus
  NeoTek Vol. II/10 (Juli 2002), hlm. 8–9
- Password untuk Folder dengan JavaScript
  NeoTek Vol. III/1 (Oktober 2002), hlm. 28–29
- Proteksi Folder: Folder Guard
  NeoTek Vol. II/9 (Juni 2002), hlm. 34–36
- Proteksi Folder: Modifikasi Registri
  NeoTek Vol. II/9 (Juni 2002), hlm. 38–39
- Proteksi Folder: Cara Sederhana
  NeoTek Vol. II/9 (Juni 2002), hlm. 40
- Privasi da Interne Explorer 6
  NeoTek Vol. II/7 (April 2002), hlm. 8–9

- Proteksi Folder: Folder Guard
  NeoTek Vol. II/9 (Juni 2002), hlm. 34–35
- Anti-Trojan 5.5 (bukan cuma file scan)
  NeoTek Vol. II/11 (Agustus 2002), hlm. 0
- Snort untuk Mendeteksi Penyusup
  NeoTek Vol. II/11 (Agustus 2002), hlm. 24–27
- NetBuster: Menjebak para Hacker Pemakai NetBus
  NeoTek Vol. II/12 (September 2002), hlm. 42–43
- BlackICE Defender
  NeoTek Vol. II/12 (September 2002), hlm. 45
- Snort & IDS Center: Cara Mudah Mengenali Penyusup
  NeoTek Vol. II/11 (Agustus 2002), hlm. 28–29
- Port Sentry: penjaga Serangan Portscan di Jaringan
  NeoTek Vol. II/11 (Agustus 2002), hlm. 30–31
- Program Siluman: Mewaspadai penyusup di PC Anda
  NeoTek Vol. II/11 (Agustus 2002), hlm. 32–37

Email Sebagai Senjata

- Hushmail: Cara Aman Berkirim Surat Elektronik
  NeoTek Vol. II/7 (April 2002), hlm. 22–23
- Sekilas Tentang Enkripsi
  NeoTek Vol. II/7 (April 2002), hlm. 30
- PGPFreeware: Instalasi dan Mengirim Gembok
  NeoTek Vol. II/11 (Agustus 2002), hlm. 40–41
- PGPFreeware: Impor Keyring da Email Terenkripsi
  NeoTek Vol. II/11 (Agustus 2002), hlm. 42–43
- PGPFreeware: Enkripsi/Dekripsi untuk Web Mail
  NeoTek Vol. II/11 (Agustus 2002), hlm. 44–45

Web Hacking

- Remote Hacking: Memanfaatkan Unicode Bug pada NT
  NeoTek Vol. II/5 (Februari 2002), hlm. 34–36

Chatting dan Telephony

- Chatting di Room #neoteker di Dalnet
  NeoTek Vol. II/6 (Maret 2002), hlm. 10–11
- Channel #neoteker Akses Melalui Situs NeoTek
  NeoTek Vol. II/7 (April 2002), hlm. 7
- Warna di Chat Room
  NeoTek Vol. II/9 (Juni 2002), hlm. 7
- Mengatur mIRC
  NeoTek Vol. II/9 (Juni 2002), hlm. 8–9
- Bermain Skrip mIRC
  NeoTek Vol. II/9 (Juni 2002), hlm. 10–11
- Membuat Skrip mIRC
  NeoTek Vol. II/9 (Juni 2002), hlm. 12–13
- Address Book mIRC
  NeoTek Vol. III/1 (Oktober 2002), hlm. 17–28
- Fasilitas pada Dalnet: NickServ
  NeoTek Vol. II/7 (April 2002), hlm. 7–9
- Fasilitas pada Dalnet: ChanServ dan MemoServ
  NeoTek Vol. II/8 (Mei 2002), hlm. 14–19
- EggDrop untuk Proteksi Channel mIRC
  NeoTek Vol. II/9 (Juni 2002), hlm. 16–17
- Menggunakan PsyBNC Saat Chat di IRC
  NeoTek Vol. II/10 (Juli 2002), hlm. 10–11
- Nguping Pembicaraan di IRC
  NeoTek Vol. II/10 (Juli 2002), hlm. 12–15
- Fasilitas & 'Wajah Baru' mIRC (Resource Hacker)
  NeoTek Vol. III/1 (Oktober 2002), hlm. 219–20
- Mengintip Kinerja GSM: Hacking Ponsel
  NeoTek Vol. III/1 (Oktober 2002), hlm. 36–37

Pengetahuan Dasar Networking

- Mengenali IP Address di Komputer Anda
  NeoTek Vol. II/2 (November 2001), hlm. 22 (box)
- TCP/IP Header
  NeoTek Vol. II/9 (Juni 2002), hlm. 29–31
- Menggunakan Telnet untuk Email Secara Manual
  NeoTek Vol. II/4 (Januari 2002), hlm. 28–29
- Pine: Email dengan Telnet pada Unix Shell Account
  NeoTek Vol. II/4 (Januari 2002), hlm. 30–31
- Menciptakan Unix Shell Account
  NeoTek Vol. II/2 (November 2001), hlm. 24 (box)
- PuTTY: Telnet dan SSH Client
  NeoTek Vol. II/2 (November 2001), hlm. 25 (box)
- Mencari Situs yang Menggunakan IIS
  NeoTek Vol. II/5 (Februari 2002), hlm. 36 (box)
- Meng-Compile Exploit dalam Bahasa C
  NeoTek Vol. II/2 (November 2001), hlm. 28
- Miracle C untuk Memahami C Compiler
  NeoTek Vol. II/2 (November 2001), hlm. 29
- Yang Sedang Trendi: Home Networking
  NeoTek Vol. II/2 (November 2001), hlm. 30–31
- Menghubungkan Dua Komputer dengan DCC
  NeoTek Vol. II/2 (November 2001), hlm. 32–33
- Menghubungkan Dua Komputer dengan Ethernet Card
  NeoTek Vol. II/2 (November 2001), hlm. 34–35
- Berbagi Akses Internet Menggunakan Router
  NeoTek Vol. II/2 (November 2001), hlm. 36–39
- Konfigurai Komputer Klien dengan Router
  NeoTek Vol. II/2 (November 2001), hlm. 40–43
- Mengenal Kabel Network
  NeoTek Vol. II/2 (November 2001), hlm. 44–45
- Utak-atik Windows dengan Tweak UI
  NeoTek Vol. II/5 (Februari 2002), hlm. 26–29
- Tweaking Sistem Windows dan Koneksi Internet
  NeoTek Vol. II/5 (Februari 2002), hlm. 31
- CaroX: Program Tweaking Buatan Anak Bangsa
  NeoTek Vol. II/5 (Februari 2002), hlm. 30
- Men-Tweak Registry dengan Windows Registry Guide
  NeoTek Vol. II/11 (Agustus 2002), hlm. 7
- Membuat Mail Server di Linux
  NeoTek Vol. II/6 (Maret 2002), hlm. 24–28
- Memanfaatkan Cookie agar Situs Menjadi Interaktif
  NeoTek Vol. II/7 (April 2002), hlm. 24–25
- Dengan Windows Membuat Router Sederhana
  NeoTek Vol. II/7 (April 2002), hlm. 42–45
- Teknik Routing Internet
  NeoTek Vol. II/8 (Mei 2002), hlm. 43–45
- Tool Networking TCP/IP Sederhana pada Windows 9x
  NeoTek Vol. II/10 (Juli 2002), hlm. 33
- Menjalankan Program Saat Pertama Kali Win Dijalankan
  NeoTek Vol. II/11 (Agustus 2002), hlm. 12–13
- FTP Sever wFTPd: Instalasi Mudah pada Win 9x/ME
  NeoTek Vol. II/11 (Agustus 2002), hlm. 46–47
- Mail Server Tiruan dengan Java
  NeoTek Vol. III/1 (Oktober 2002), hlm. 30–34
- Web Server Sederhana dengan Java
  NeoTek Vol. III/1 (Oktober 2002), hlm. 35