JURNAL MEDIA APLIKOM
ISSN : 2086 - 972X
Vol. 2, No. 2, Mei 2012

KEAMANAN SISTEM INFORMASI

Yosef Murya Kusuma Ardhana
Jurusan Komputerisasi Akuntansi STIKOM Yos Sudarso Purwokerto
Jl. SMP 5 Karang Klesem Purwokerto Telp (0281)-6845088
e-mail: yosefmurya@yahoo.com

Abstrak

Pada era pertumbuhan sistem informasi yang sangat cepat saat ini keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan, karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

Pada dasarnya suatu sistem yang aman akan melindungi data didalamnya seperti identifikasi pemakai (user identification), pembuktian keaslian pemakai (user authentication), otorisasi pemakai (user authorization). Beberapa kemungkinan serangan (Hacking) yang dapat dilakukan, seperti Intrusion , denial of services. joyrider, vandal, hijacking, sniffing, spoofing dan lain-lain. Ancaman terhadap sistem informasi banyak macamnya, antara lain : pencurian data, penggunaan sistem secara ilegal, penghancuran data secara ilegal, modifikasi data secara ilegal, kegagalan pada sistem, kesalahan manusia (SDM-sumber daya manusia), bencana alam.

Tujuan dari keamanan sistem informasi yaitu mencegah ancaman terhadap sistem serta mendeteksi dan memperbaiki kerusakan yang terjadi pada sistem.

Keyword: *Sistem informasi, user identification, user authentication, user authorization, hacking.*

1. PENDAHULUAN

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan, karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

2. TINJAUAN PUSTAKA

Ada banyak cara mengamankan data atau informasi pada sebauh sistem. Pada umumnya pengamanan data dapat dikategorikan menjadi dua jenis, yaitu : penecegahan *(presentif*) dan pengobatan (*recovery*). Pencegahan dilakukan supaya data tidak rusak, hilang dan dicuri, sementara pengobatan dilakukan apabila data sudah terkena virus, sistem terkena worm, dan lubang keamanan sudah diexploitasi.

3. METODE PENELITIAN

Pengertian dasar keamanan informasi.

Sistem keamanan informasi (*information security*) memiliki empat tujuan yang sangat mendasar, yaitu :

a) Kerahasiaan (*Confidentiality*).
   Informasi pada sistem komputer terjamin kerahasiaannya, hanya dapat diakses oleh pihak-pihak yang diotorisasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga. Sehingga upaya orang-orang yang ingin mencuri informasi tersebut akan sia-sia.
b) Ketersediaan (*Availability*).
   Menjamin pengguna yang sah untuk selalu dapat mengakses informasi dan sumberdaya yang diotorisasi. Untuk memastikan bahwa orang-orang yang memang berhak untuk mengakses informasi yang memang menjadi haknya.
c) Integritas (*Integrity*)
   Menjamin konsistensi dan menjamin data tersebut sesuai dengan aslinya, sehingga upaya orang lain yang berusaha merubah data akan segera dapat diketahui.
d) Penggunaan yang sah (*Legitimate Use*).
   Menjamin kepastian bahwa sumberdaya tidak dapat digunakan oleh orang yang tidak berhak.

Masalah keamanan dalam sistem informasi
Ancaman terhadap sistem informasi dibagi menjadi 2 macam, yaitu ancaman aktif dan ancaman pasif.

Ancaman aktif mencakup:

1. Pencurian data
   Jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang maka hasilnya dapat kehilangan informasi atau uang. Misalnya, mata-mata industri dapat memperoleh informasi persaingan yang berharga, penjahat komputer dapat mencuri uang bank.

2. Penggunaan sistem secara ilegal
   Orang yang tidak berhak mengakses informasi pada suatu sistem yang bukan menjadi hak-nya, dapat mengakses sistem tersebut. Penjahat komputer jenis ini umumnya adalah hacker yaitu orang yang suka menembus sistem keamanan dengan tujuan mendapatkan data atau informasi penting yang diperlukan, memperoleh akses ke sistem telepon, dan membuat sambungan telepon jarak jauh secara tidak sah.

3. Penghancuran data secara ilegal
   Orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu sistem operasi komputer. Penjahat komputer ini tidak perlu berada ditempat kejadian. Ia dapat masuk melalui jaringan komputer dari suatu terminal dan menyebabkan kerusakan pada semua sistem dan hilangnya data atau informasi penting. Penjahat komputer jenis ini umumnya disebut sebagai cracker yaitu penjebol sistem komputer yang bertujuan melakukan pencurian data atau merusak sistem.

4. Modifikasi secara ilegal
   Perubahan-perubahan pada data atau informasi dan perangkat lunak secara tidak disadari. Jenis modifikasi yang membuat pemilik sistem menjadi bingung karena adanya perubahan pada data dan perangkat lunak disebabkan oleh progam aplikasi yang merusak (*malicious software*). Program aplikasi yang dapat merusak tersebut terdiri dari program lengkap atau segemen kode yang melaksanakan fungsi yang tidak dikehendaki oleh pemilik sistem. Fungsi ini dapat menghapus file atau menyebabkan sistem terhenti. Jenis aplikasi yang dapat merusak data atau perangkat lunak yang paling populer adalah virus.

Ancaman pasif mencakup:

1. Kegagalan sistem
   Kegagalan sistem atau kegagalan software dan hardware dapat menyebabkan data tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. Selain itu, tegangan listrik yang tidak stabil dapat membuat peralatan-peralatan menjadi rusak dan terbakar.

2. Kesalahan manusia
   Kesalahan pengoperasian sistem yang dilakukan oleh manusia dapat mengancam integritas sistem dan data.

3. Bencana alam
   Bencana alam seperti gempa bumi, banjir, kebakaran, hujan badai merupakan faktor yang tidak terduga yang dapat mengancam sistem informasi sehingga mengakibatkan sumber daya pendukung sistem informasi menjadi luluhlantah dalam waktu yang singkat.

Klasifikasi metode penyerangan
Pada dasarnya suatu sistem yang aman akan mencoba melindungi data didalamnya, beberapa kemungkinan serangan yang dapat dilakukan antara lain :

1. *Intrusion.*
   Pada metode ini seorang penyerang dapat menggunakan sistem komputer yang dimiliki orang lain. Sebagian penyerang jenis ini menginginkan akses sebagaimana halnya pengguna yang memiliki hak untuk mengakses sistem.

2. *Denial of services.*
   Penyerangan jenis ini mengakibatkan pengguna yang sah tak dapat mengakses sistem karena terjadi kemacetan pada sistem. Contoh dari metode penyerangan ini adalah *Distributed Denial of Services* (DDOS) yang mengakibatkan beberapa situs Internet tak bisa diakses. Banyak orang yang melupakan jenis serangan ini dan hanya berkonsentrasi pada intrusion saja.

3. *Joyrider.*
   Pada serangan ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem. Mereka masuk ke sistem karena beranggapan bahwa mungkin didalam sistem terdapat data yang menarik. Rata-rata mereka hanya terbawa rasa ingin tahu, tapi hal tersebut menyebabkan terjadinya kerusakan atau kehilangan data.

4. *Vandal.*
   Jenis serangan ini bertujuan untuk merusak sistem, namun hanya ditujukan untuk situs-situs besar.

5. *Hijacking.*
   Seseorang menempatkan sistem monitoring atau spying terhadap pengetikan yang dilakukan pengguna pada PC yang digunakan oleh pengguna. Biasaya teknik penyerangan ini membutuhkan program khusus seperti program keylog atau sejenisnya. Saat ini semakin banyak perusahaan yang memanfaatkan jasa dari seseorang yang memiliki kemampuan ini.

   Terdapat beberapa jenis macam mata-mata, yaitu :
   a) *The curious* (Si ingin tahu)
      Tipe penyusup yang pada dasarnya tertarik menemukan jenis sistem dan data yang dimiliki orang lain.
   b) *The malicious* (Si perusak)
      Tipe penyusup yang berusaha untuk merusak sistem, atau merubah halaman web site.
   c) *The high profile intruder* (Si profil tinggi)
      Penyusup yang berusaha menggunakan sistem untuk memperoleh popularitas dan ketenaran.
   d) *The competition* (Si Pesaing)
      Penyusup yang tertarik pada data yang terdapa dalam sebuah sistem.

6. *Sniffing*
   Sesorang yang melakukan monitoring atau penangkapan terhadap paket data yang ditransmisikan dari komputer client ke web server pada jaringan internet (saluran komunikasi).

7. *Spoofing*
   Seseorang berusaha membuat pengguna mengunjungi sebuah halaman situs yang salah sehingga membuat pengunjung situs memberikan informasi rahasia kepada pihak yang tidak berhak. Untuk melakukan metode penyerangan ini seseorang terlebih dahulu membuat situs yang mirip namanya dengan nama server eCommerce asli. Contoh dari kasus yang pernah terjadi dan menimpa pada salah satu nasabah bank bca, ketika itu ada seseorang membuat situs palsu yang hampir sama dengan situs asli dengan nama www.klik_bca.com, www.klikbca.org, www.klik-bca.com, www.klikbca.co.id, www.clickbca.com, www.clicbca.com, www.clikbca.com. Dengan demikian ketika salah satu nasabah atau pengguna membuka alamat situs palsu yang sekilas terlihat sama akan tetap menduga bahwa situs yang dikunjungi adalah situs klikbca yang benar. Tujuan dari metode ini adalah menjebak nasabah atau pengunjung situs agar memasukkan inforasi yang penting dan rahasia, seperti data kartu kredit, id dan nomor pin atau password.

8. *Website Defacing*
   Seseorang melakukan serangan pada situs asli (misalkan www.stikomyos.ac.id) kemudian mengganti isi halaman pada server tersebut dengan halaman yang telah dimodifikasi. Dengan demikian pengunjung akan mengunjungi alamat dan server yang benar namun halaman yang asli telah berubah. Tujuan dari seseorang yang menggunakan metode penyerangan ini yaitu agar instansi, perusahaan, pemerintahan dan organisasi tertentu yang memiliki situs sebagai sarana untuk memberikan kemudahan bagi masyarakat terkait menjadi tidak berfungsi dengan sebagaimana mestinya.

9. *Virus*
   Virus adalah kode program yang dapat mengikatkan diri pada aplikasi atau file, di mana program tersebut bisa menyebabkan komputer bekerja di luar kehendak pemakai sehingga file yang berkestensi

terntentu menjadi terinfeksi yangmengakibatkan file menjadi hilang karena disembunyikan (*hide*), termodifikasi (*encrypt*) bahkan terhapus (*delete*).

10. *Trojan Horse*
    Salah satu metode penyerangan yang sangat ampuh dan sering digunakan dalam kejahatan-kejahatan di internet. Seseorang memberikan program yang bersifat free atau gratis, yang memiliki fungsi dan mudah digunakan (*user friendly*), tetapi di dalam program tersebut terdapat program lain yang tidak terlihat oleh user yang berfungsi menghapus data. Misalnya program untuk cracking password, credit-card generator dan lain-lain.

11. *Worm*
    Program yang dapat menduplikasikan dirinya sendiri dengan menggunakan media komputer yang mengakibatkan kerusakan pada sistem dan memperlambat kinerja komputer dalam mengaplikasi sebuah program.

Keamanan sistem informasi
Ada banyak cara mengamankan data atau informasi pada sebauh sistem. Pada umumnya pengamanan data dapat dikategorikan menjadi dua jenis, yaitu : penecegahan (*presentif*) dan pengobatan (*recovery*).

1. Pengendalian akses.
   Pengendalian akses dapat dicapai dengan tiga langkah, yaitu:
   a) Identifikasi pemakai (*user identification*).
      Mula-mula pemakai mengidentifikasikan dirinya sendiri dengan menyediakan sesuatu yang diketahuinya, seperti kata sandi atau password. Identifikasi tersebut dapat mencakup lokasi pemakai, seperti titik masuk jaringan dan hak akses telepon.

   b) Pembuktian keaslian pemakai (*user authentication*).
      Setelah melewati identifikasi pertama, pemakai dapat membuktikan hak akses dengan menyediakan sesuatu yang ia punya, seperti kartu id (*smart card, token* dan *identification chip*), tanda tangan, suara atau pola ucapan.

   c) Otorisasi pemakai (*user authorization*).
      Setelah melewati pemeriksaan identifikasi dan pembuktian keaslian, maka orang tersebut dapat diberi hak wewenang untuk mengakses dan melakukan perubahan dari suatu file atau data.

2. Memantau adanya serangan pada sistem.
   Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya penyusup yang masuk kedalam sistem (*intruder*) atau adanya serangan (*attack*) dari hacker. sistem ini biasa disebut "*intruder detection system*" (IDS). Sistem ini dapat memberitahu admin melalui e-mail atau melalui mekanisme lain. Terdapat berbagai cara untuk memantau adanya penyusup. Ada yang bersifat aktif dan pasif. IDS cara yang pasif misalnya dengan melakukan pemantauan pada logfile.
   Berbagai macam software IDS antara lain, yaitu:
   a) *Autobuse* yaitu mendeteksi *port scanning* dengan melakukan pemantauan pada logfile.
   b) *Port blocker* yaitu memblok port tertentu terhadap serangan. Biasanya untuk melakukan port blok memerlukan software tertentu, seperti NinX atau sejenisnya.
   c) *Courtney* dan *portsentry* yaitu mendeteksi *port scanning* dengan melakukan pemantauan paket data yang sedang lewat.
   d) *Snort* yaitu mendeteksi pola pada paket data yang lewat dan mengirimkan instruksi siaga jika pola tersebut terdeteksi. Pola disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

3. Penggunaan enkripsi .
   Salah satau mekanisme untuk meningkatkan keamanan sistem yaitu dengan menggunakan teknologi enkripsi data. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah diketahui oleh orang lain yang tidak berhak.

   Ada tiga kategori enkripsi, yaitu:
   a) Enkripsi rahasia.
      Terdapat sebuah kunci yang dapat digunakan untuk meng-enkripsi dan men-dekripsi datadata.

b) Enkripsi publik.
Terdapat dua kunci yang digunakan, satu kunci digunakan untuk melakukan enkripsi dan kunci yang lain digunakan untuk melakukan proses dekripsi.

c) Fungsi one-way.
Suatu fungsi dimana informasi di enkripsi untuk menciptakan "signature" dari data asli yang dapat digunakan untuk keperluan autentifikasi.

Enkripsi dibentuk berdasarkan algoritma yang dapat mengacak data kedalam bentuk yang tidak bisa dibaca atau rahasia, sedangkan dekripsi dibentuk berdasarkan algoritma yang sama untuk mengembalikan data yang teracak menjadi bentuk asli atau dapat dibaca.

Ada beberapa metode enkripsi yaitu:

a) DES (*Data Encryption Standard*)
DES merupakan nama dari sebuah algoritma untuk mengenkripsi data yang dikeluarkan oleh Federal Information Processing Stadard (FIPS) Amerika Serikat. DES memiliki blok kunci 64-bit, tetapi yang digunakan dalam proses eksekusi adalah 54 bit. Algoritma enkripsi ini termasuk algoritma yang tidak mudah untuk diterobos.

b) 3DES (*Triple* DES)
Triple DES dikembangkan untuk mengatasi kelemahan ukuran kunci yang digunakan pada proses enkripsi-deskripsi DES sehingga teknik kriptografi ini lebih tahan terhadap exhaustive key search yang dilakukan oleh kriptoanalis. Penggunaan triple DES dengan suatu kunci tidak akan menghasilkan pemetaan yang sama seperti yang dihasilkan oleh DES dengan kunci tertentu. Hal itu disebabkan oleh sifat DES yang tidak tertutup (*not closed*). Sedangkan dari hasil implementasi dengan menggunakan modus *Electronic Code Book* (ECB) menunjukkan bahwa walaupun memiliki kompleksitas atau notasi O yang sama (O(n)), proses enkripsi-deskripsi pada DES lebih cepat dibandingkan dengan *triple* DES.

c) Kerberos.
Kerberos adalah suatu sistem keamanan berdasarkan enkripsi yang menyediakan pembuktuan keaslian (*mutual authentication*) bersama-sama antara komponen client dan komponen server dalam lingkungan computing terdistribusi. Kerberos juga menyediakan hak-hak layanan yang dapat digunakan untuk mengontrol client mana yang berwenang mengakses suatu server.

4. Melakukan backup secara rutin.
Dengan adanya backup data yang dilakukan secara rutin merupakan sebuah hal yang esensial, sehingga apabila ada penyusup yang mencuri, menghapus, bahkan melakukan modifikasi seluruh isi berkas penting dapat diatasi dengan cepat.

Sejarah Hacker

Hacker muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka beroperasi dengan sejumlah komputer mainframe. Kata hacker pertama kali muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik dari yang telah dirancang bersama. Kemudian pada tahun 1983, analogi hacker semakin berkembang untuk menyebut seseorang yang memiliki obsesi untuk memahami dan menguasai sistem komputer. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer The 414s yang berbasis di Milwaukee AS. 414 merupakan kode area lokal mereka.

Kelompok yang kemudian disebut hacker tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Salah seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Para hacker mengadakan pertemuan setiap setahun sekali yaitu diadakan setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan hacker terbesar di dunia tersebut dinamakan Def Con. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas hacking.

- Tokoh-tokoh Hacker ternama

a. Dennis M. Ritchie

Dennis (nama handle "dmr") lahir di Bronxville, New York pada tanggal 09 September 1941. Ia memperoleh gelar BSc di bidang fisika dan gelar PhD matematika terapan di Havard University. Pada tahun 1967 atau tepatnya setahun sebelum doktoral selesai, ia mengikuti jejak ayahnya bekerja di Bell Laboratories. Proyek komputer pertamanya di Bell adalah sistem operasi multics, yang merupakan proyek kerjasama Bell Laboratories, MIT dan General Electric.

Dennis kemudian bekerjasama dengan Ken Thompson, dan menulis sistem operasi UNIX yang kemudian diketahui sebagai sistem operasi pertama yang dapat digunakan diberbagai jenis komputer. Untuk menghasilkan sistem operasi ini, Dennis dan Ken menyempurnakan bahasa pemrograman B karya Ken, kemudian menghasilkan bahasa C, yang digunakan untuk menulis UNIX dan program bantuannya. Sampai sekarang Dennis dan Ken masih aktif di Bell Labs. Proyeknya yang sudah diselesaikan antara lain sistem operasi Plan9 dan inferno.

b. Ken Thompson

Ken Thompson adalah mitra kerja Dennis M. Ritchie yang bisa dibilang paling dekat, mulai dari proyek penyempurnaan bahasa pemrograman B, yang kemudian menghasilkan bahasa C, lalu membuat sistem operasi UNIX, dan lainnya.

Kerjasama Ken dan Dennis yang kompak ini terlihat dari hasil dan beberapa penghargaan yang mereka terima. Bahkan semua penghargaan yang pernah Ken dan Dennis adalah hasil kerjasama mereka. Penghargaan-penghargaan tersebut antara lain ACM Award (1974), IEEE Emmanuel Piore Award(1982), Bell Laboratories Fellow(1983), Association for Computing Machinery Turing Award(1983), U.S.National Medal of Tecknology(1999) dan masih banyak lagi.

c. Richard M. Stallman

R.M. Stallman lahir ditahun 1953 dan merupakan salah seorang hacker generasi pertama yang paling terkenal. Ia pertama kali menggunakan komputer pada saat berumur 16 tahun, di IBM Scientific Center. Tahun 1971, setelah lulus undergraduate (S1) Havard, ia bekerja di laboratorium kecerdasan buatan Massacusets Institute of Technology. Handle dengan nama sebutannya saat itu adalah "RMS".

Ia bersama hacker-hacker generasi pertama MIT membuat berbagai program bantu untuk komputer-komputer raksasa yang digunakan di lab MIT saat itu. Pada tahun 1980, ia secara resmi keluar dari MIT. Ia juga membuat sistem operasi GNU. Pengalamannya selama di MIT digunakannya untuk membantu Steven Levy menulis bukunya yang berjudul Hackers: Heroes of the Computer Revolution, tahun 1984.

Belakangan, ia menentang anggapan bahwa perangkat lunak adalah hak milik pribadi, dan mendirikan free software foundation. Modul-modul program buatan free software foundation-lah yang kemudian menolong Linus Torvalds dalam menciptakan Linux. Selain itu, Stallman juga menyatakan ketidak puasannya terhadap trend hacker dewasa ini, dan secara pribadi menolak penggunaan kata hacker untuk menunjuk kepada orang-orang yang memasuki sistem orang lain.

d. Steve Wozniak

Steve tumbuh di Sunnyville, di saat masih muda steve becita-cita ingin memiliki komputer sendiri. Semasa sekolah, ia sering membuat desain-desain dengan menggunakan komputernya sendiri. Kepandaian dan kecerdasannya dalam bidang matematik berkembang secara pesat berkat bantuan sang ayah, yang merupakan seorang insinyur. Hingga pada pertengahan tahun 1975, Steve berhasil merancang komputer pribadinya. Saat itu konsep komputer pribadi steve diremehkan oleh perusahaan-perusahaan besar seperti IBM, yang memilih untuk memproduksi komputer-komputer berkemampuan besar yang berukuran raksasa dan harganya sangat mahal. Steve kemudian bekerjasama dengan rekannya yaitu Steve Jobs, dan mendirikan Apple Computer. Produk pertama dari perusahaan dengan dua karyawan itu adalah Apple I, tetapi produk yang benar-benar membuat Apple Computer terkenal adalah Apple II, yang keluar pada tahun 1977. Setelah produk Apple II muncul, Apple Computer go public dan Steve Wozniak, saat itu berusia 30 tahun, menjadi jutawan baru.

Setelah beberapa lama menikmati kesuksesan Apple Computer, Steve Wozniak memutuskan untuk keluar dari Apple Computer. Tetapi pada tahun 1996, ia kembali lagi keperusahaan tersebut dengan jabatan sebagai penasihat.

e. Robert Morris

Robert Tappan Morris lahir pada tahun 1966, yang merupakan putra seorang ilmuan National Computer Security Center atau bagian dari National Security Agency Amerika Serikat, yaitu Robert Morris senior, ia dikenal karena telah mengacaukan internet dengan program Worm ciptaannya.

Pertemuan Robert Morris muda dengan komputer sebenarnya berawal ketika ayahnya membawa salah satu komputer penyandi pesan "Enigma" (yang digunakan jerman semasa perang) dari tempat kerjannya. Pada saat remaja, Robert Tappan Morris sudah berhasil menghack sistem komputer Bell Labs dan memperoleh akses superuser. Nama handlenya adalah "rtm".

Pada tanggal 02 November 1988, saat masih kuliah di Cornell University, Robert Morris menulis sebuah program Worm yang menurutnya ditujukan untuk penelitian. Worm yang dibuat Morris memiliki kemampuan untuk menyebar di Internet secara otonom, memanfaatkan kelemahan yang umum pada sistem UNIX, mengeksploitasi sendmail dan berbagai kemampuan lainnya.

Program Worm tersebut kemudian menyebar secara tak terkendali, dan akhirnya memacetkan ribuan komputer di Internet. Kasus ini akhirnya mendorong pembentukan CERT (*Computer Emergency Response Team*) yaitu badan yang menangani kasus-kasus keamanan di Internet. Robert Morris sendiri dikenakan denda sebesar US$10.000, dan menjadi orang yang paling terkenal karena membuat virus.

f. Linus Torvalds

Linus Benedict Torvalds lahir di Helsinki, Finlandia pada tahun 1970. Pada saat linus masih muda, komputer pribadi berkembang pesat. Saat menjadi seorang mahasiswa, ia bercita-cita menulis sistem operasi yang lebih bagus dari MS-DOS, dan gratis. Pada masa itu ia masih menggunakan MINIX, klon UNIX yang berukuran kecil, dan fasilitasnya masih terbatas. Mahasiswa Ilmu Komputer University of Helsinki ini lalu mendiskusikan idenya dengan rekan-rekannya.

Dengan bantuan rekan-rekannya itu, ia berhasil merancang sistem operasi Linux, sistem operasi yang mirip UNIX yang fasilitasnya jauh diatas MS-DOS. Dalam waktu sekitar tiga tahun, mereka berhasil menyelesaikan Linux, dan mendistribusikannya secara cuma-cuma. Linux lalu berkembang menjadi berbagai versi.

Pada tahun 1997, linus dan keluarganya pindah ke Santa Clara, California, AS. Mereka dikaruniai dua orang putri, Patricia Miranda Torvalds dan Daniela Torvalds. Linus sendiri sekarang bekerja di perusahaan TransMeta.

g. Kevin Poulsen

Komputer pribadi Kevin Poulsen adalah Trash atau sering disebut TRS-80, komputer yang sama dengan yang digunakan tokoh film "War Games". Poulsen pada akhir tahun 1980-an berurusan dengan FBI karena berhasil membobol sistem komputer mereka. Dengan aksesnya itu, ia berhasil medapatkan seluruh data perusahaan yang dijalankan oleh agen-agen FBI. Dicari dengang tuduhan membahayakan keamanan nasional, Kevin Polsen menyembunyikan diri.

Pada tahun1990, Kevin Poulsen berhasil memenangkan kontes telpon yang diselenggarakan oleh sebuah radio di Los Angeles. Caranya cukup menarik, yakni mengambil alih sistem komputer perusahaan LA, dengan memblokir semua telepon ke stasiun radio tersebut dan membuat dirinya sendiri menjadi penelepon ke 102 dan secara otomatis menjadi pemenang dalam kontes tersebut. Sebagai hadiah, ia memperoleh sebuah Porsche 944 S2 dan juga liburan gratis ke Hawaii.

Setelah Kevil Poulsen tertangkap, ia dihukum lima tahun atas tuduhan pencucian uang dan kejahatan telepon. Pada tahun 1998 lalu, ia kembali kemasyarakat, dan menjadi penulis tetap pada perusahaan berita ZDTV. Rubrik yang diasuhnya adalah Chaos Theory, yaitu sebuah rubrik yang membahas kejahat komputer yang ditayangkan setiap hari jumat.

h. Kevin Mitnick

Kevin David Mitnick merupakan hacker paling banyak dipublikasikan karena terlibat perkara-perkara kriminal. Lahir di tahun 1963, Kevin Mitnick memulai karir hackingnya semasa masih remaja di Los Angeles, sekitar tahun 1970-an. Orang tuanya bercerai dan ia tinggal bersama ibunya. Dimasa remaja, karena tidak mampu untuk membeli sebuh komputer, ia menghabiskan waktunya disebuah toko Radio Shack dan bermain-main dengan komputer disana.

Belakangan, Mitnick meneruskan kegiatan hackingnga, dan menimbulkan konflik dengan penegak hukum di AS. Aksinya antara lain adalah WELL (*Whole Earth 'Lectronic Link*), dan dikomputer-komputer pakar keamanan komputer dan Farmer, Eric Allman, dsb. Akhirnya ia ditangkap untuk kelima kalinya pada bulan februari 1995 setelah pelacakan FBI dibantu pakar keamanan Tsutomu Shimo-mura. Tuduhannya antara lain pemilikan 20.000 kartu kredit curian, menyalin sistem operasi Digital Equepment Corporation secara ilegal dan menggunakan komputernya untuk mengambil alih seluruh hub jaringan telepon New York dan California.

Namun perlakuan tidak adil para penegak hukum antara lain penahanan sejak tahun 1995 tanpa uang jaminan dan tanpa proses peradilan dan media masa telah menimbulkan gelombang pro-Mitnick. Ini ditunjukkan antara lain dengan aksi protes, pembuata home page yang dikhususkan untuk mendukung Mitnick, dan pemasangan logo "Free Kevin" diperbagai situs bawah tanah yang mendukung.

Ciri-ciri seorang Hacker

Menurut Eric Raymond, pengarang buku The New Hacker's Dictionary mendefinisikan hacker sebagai programer yang cerdas. "Hacker yang baik memberikan solusi terhadap masalah pemrograman yang timbul," tulisnya. Lebih jauh, Raymond memberikan lima kriteria tentang seorang hacker. Pertama, mereka adalah orang yang menyukai pemrograman ketimbang hanya sekadar berteori. Kedua, mereka adalah orang yang jeli mengutak-atik detail pemrograman, dan ketiga, hacker selalu menangkap bahasa pemrograman dengan cepat. Keempat, mereka biasanya adalah orang-orang yang jago dalam bahasa pemrograman atau sistem tertentu seperti UNIX atau Windows. Dan terakhir, hacker adalah seorang yang mampu menginterpretasi dan mengapresiasi tindakan hacking yang dilakukan.

Target yang diserang oleh Hacker

Hacker menyerang suatu sistem dengan bermacam-macam target, antara lain:

a. Database kartu kredit (*credit card*).
b. Database account bank, berupa ID dan nomor PIN.
c. Database informasi pelanggan.
d. Mengacaukan sistem pada komputer.

Cara Hacker Berinteraksi

Para hacker melakukan interaksi dengan sesama hacker melalui:

a. *Internet Relay Chat* (IRC)
b. *Voice over* IP (VoIP)
c. ICQ
d. Online forums
e. Encryption

Yang Dilakukan Hacker Setelah Menembus Keamanan Sistem.

a. Menginstall Backdoors, Trojan Horses, dan Rootkits dengan tujuan:
    - Memudahkan akses masuk kembali
    - Memperdayai sysadmin untuk mendapatkan akses penuh (root)
    - Menginstal sekumpulan tools untuk menjadi invisible ketika login
b. Menghapus jejak dengan cara memodifikasi logfiles sehingga tidak menimbulkan kecurigaan sysadmin.
c. Menyalin /etc/passwd dan /etc/shadow atau /etc/master passwd sehingga dapat diperlukan sewaktu-waktu jika semua backdoor terhapus.

4. HASIL DAN PEMBAHASAN

Dengan mengetahui bagaimana seorang penerobos atau penyusup (*hacker*) melakukan penerobosan pada sebuah sistem (*hacking*) dan melakukan pencurian, penghapusan atau melakukan modifikasi suatu data atau informasi maka seorang administrator atau user dapat mencegah terjadinya *hacking*, sehingga data atau informasi dapat tersimpan dengan aman.

5. KESIMPULAN

- Mengerti dan memahami bagaimana aksi hacker dalam menerobos sistem, sehingga kegiatan hacking dapat dikontrol dan dicegah.
- Dapat mengetahui dan mengerti bagaimana melakukan teknik pengamanan data dan bagaimana menjaga kerahasiaannya.

6. DAFTAR PUSTAKA

- Kadir Abdul, Pengenalan Sistem Informasi, Penerbit Andi, 2003.
- Sutedjo Dharma Oetomo Budi, Perencanaan dan Pengembangan Sistem Informasi, Penerbit andi, 2002.
- Yosef Murya Kusuma Ardhana, Paryati, Sistem Informasi, Ardana Media, 2008.