MAKALAH

PENGANTAR ILMU KOMPUTER
"KEAMANAN KOMPUTER"

D
I
S
U
S
U
N
oleh:

1. Aisyah
2. Alvin Daffa Hutajulu
3. Alvina Tansy Pulungan
4. Ayu Mahriza Agusitn Efendi
5. Hadzrul Ananta Fazri Lubis
6. Henni Novita Sari Hasibuan
7. Ahmad Fadhly Sani Saragih
8. Khairunnisa

UNIVERSITAS ISLAM NEGERI SUMATERA UTARA

T.A 2018/2019

Latar Belakang Perlunya Sebuah Keamanan

Keamanan komputer (computer security) atau dikenal juga dengan sebutan cybersecurity atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Computer security atau keamanan komputer bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Informasinya sendiri memiliki arti non fisik.

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 terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan.

Sistem kemanan komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja dan proses komputer. Penerapan computer security dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi, interupsi, dan diganggu oleh orang yang tidak berwenang. Keamanan bisa diidentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis. Computer security akan membahas dua hal penting yaitu Ancaman/Threats dan Kelemahan sistem/Vulnerability.

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 menjadi lebih menantang karena sudah cukup sulit untuk membuat program komputer melakukan segala apa yang sudah dirancang untuk dilakukan dengan benar.

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.

Klasifikasi Kejahatan Komputer

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (annoying). Menurut David Icove 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. Beberapa bekas penjahat komputer (crackers) mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan. Misalnya pernah diketemukan coretan password atau manual yang dibuang tanpa dihancurkan. Wiretapping atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini. Denial of service, yaitu akibat yang ditimbulkan sehingga servis tidak dapat diterima oleh pemakai juga dapat dimasukkan ke dalam kelas ini. Denial of service dapat dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya

jumlah pesan). Beberapa waktu yang lalu ada lubang keamanan dari implementasi protokol TCP/IP yang dikenal dengan istilah Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (hang).

2. **Keamanan yang berhubungan dengan orang** (personel): termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Seringkali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai dan pengelola). Ada sebuah teknik yang dikenal dengan istilah "social engineering" yang sering digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi. Misalnya kriminal ini berpura-pura sebagai pemakai yang lupa passwordnya dan minta agar diganti menjadi kata lain.
3. **Keamanan dari data dan media serta teknik komunikasi**(communications). Yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang virus atau trojan horse sehingga dapat mengumpulkan informasi (seperti password) yang semestinya tidak berhak diakses.
4. **Keamanan dalam operasi**: termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (post attack recovery)

Aspek-Aspek Keamanan Komputer

Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Keamanan komputer sendiri meliputi beberapa aspek , antara lain :

1. Privacy, adalah sesuatu yang bersifat rahasia(provate). Intinya adalah pencegahan agar informasi tersebut tidak diakses oleh orang yang tidak berhak. Contohnya adalah email atau file-file lain yang tidak boleh dibaca orang lain meskipun oleh administrator. Pencegahan yang mungkin dilakukan adalah dengan menggunakan teknologi enksripsi, jadi hanya pemilik informasi yang dapat mengetahui informasi yang sesungguhnya.

2. Confidentiality(kerahasiaan), merupakan data yang diberikan ke pihak lain untuk tujuan khusus tetapi tetap dijaga penyebarannya. Contohnya data yang bersifat pribadi seperti : nama, alamat, no ktp, telpon dan sebagainya. Confidentiality akan terlihat apabila diminta untuk membuktikan kejahatan seseorang, apakah pemegang informasi akan memberikan infomasinya kepada orang yang memintanya atau menjaga clientnya.

3. Integrity(integritas), penekanannya adalah sebuah informasi tidak boleh diubah kecuali oleh pemilik informasi. Terkadang data yang telah terenskripsipun tidak terjaga integritasnya karena ada kemungkinan chpertext dari enkripsi tersebut berubah. Contoh :

Penyerangan Integritas ketika sebuah email dikirimkan ditengah jalan disadap dan diganti isinya, sehingga email yang sampai ketujuan sudah berubah.

4. Autentication(otentikasi), ini akan dilakukan sewaktu user login dengan menggunakan nama user dan passwordnya, apakah cocok atau tidak, jika cocok diterima dan tidak akan ditolak. Ini biasanya berhubungan dengan hak akses seseorang, apakah dia pengakses yang sah atau tidak.

5. Availability(ketersediaan), aspek ini berkaitan dengan apakah sebuah data tersedia saat dibutuhkan/diperlukan. Apabila sebuah data atau informasi terlalu ketat pengamanannya akan menyulitkan dalam akses data tersebut. Disamping itu akses yang lambat juga menghambat terpenuhnya aspe availability. Serangan yang sering dilakukan pada aspek ini adalah denial of service (DoS), yaitu penggagalan service sewaktu adanya permintaan data sehingga komputer tidak bisa melayaninya. Contoh lain dari denial of service ini adalah mengirimkan request yang berlebihan sehingga menyebabkan komputer tidak bisa lagi menampung beban tersebut dan akhirnya komputer down.

KONSEP KEAMANAN KOMPUTER

Konsep Keamanan

Sistem komputer bisa dikatakan sebagai suatu sistem yang aman jika telah memenuhi beberapa syarat tertentu untuk mencapal suatu tujuan keamanan. Secara garis besar, persyaratan keamanan sistem komputer dapat dibedakan menjadi tiga, yaitu :

a. Kerahasiaan (secretcy)

Secrecy berhubungan dengan hak akses untuk membaca data atau informasi dan suatu sistem komputer

b. Integritas (integrity)

Integrity berhubungan dengan hak akses untuk mengubah data atau informasi darl suatu sistem komputer

c. Ketersediaan (availability)

Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan

Lingkup Pengamanan

Lingkup keamanan adalah sisi-sisi jangkauan keamanan komputer yang bisa dilakukan. Pada prinsipnya pengamanan sistem komputer mencakup empat hal yang sangat mendasar, yaitu:

a. Pengamanan Secara Fisik

Komputer secara fisik adalah wujud komputer yang bisa dilihat dan diraba, sepertl monitor, CPU, keyboard, dan lain-lain. jika komputer memang perlu untuk diamankan karena fungsl dan data di dalamnya yang penting, maka pengamanan secara fisik dapat dilakukan dengan menempatkan sistem komputer pada tempat atau lokasi yang mudah diawasi dan dikendalikan, pada ruangan tertentu yang dapat dikunci, dan sulit dijangkau orang lain. Kebersihan ruangan juga menjadi faktor pengamanan fisik, hinda-ri ruangan yang panas, kotor, lembab. Usahakan ruangan tetap dingin jika perlu ber-AC tetapi tidak lembab.

b. Pengamanan Akses

Ini dilakukan untuk PC yang menggunakan sistem operasi loggin dan system operasi jaringan dilakukan untuk mengantisi kejahatan yang sifatnya disengaja atau tidak disengaja, seperti kelalaian atau keteledoran pengguna yang sering kali meninggalkan komputer dalam keadaan masih menyala, atau jika berada pada jaringan komputer tersebut masih berada dalam logon user.

c. Pengamanan data

Pengamanan data dilakukan dengan menerapkan sistem tingkatan atau hierarki akses di mana seseorang hanya dapat mengakses data tertentu saja yang menjadi haknya

d. Pengamanan komunikasi jaringan

Jaringan di susun berkaitan erat dengan pemanfaatan jaringan publik seperti Internet. Pengamanan jaringan dapat dilakukan dengan menggunakan kriptografi di mana data yang sifatnya sensitif dienkripsi atau disandikan terlebih dahulu sebelum ditransmisikan melalui jaringan tersebut.

Lapisan Keamanan

Ada 8 lapisan keamanan komputer :

1) Keamanan Fisik

Membatasi akses fisik ke mesin dengan cara :

– Akses masuk keruangan komputer

– Penguncian komputer secara hardware

– Keamanan BIOS

2) Kemanan Bootloader

Dengan cara :

– Back-up data

– Pemilihan piranti back-up

– Penjadwalan back-up

3) Keamanan Lokal

Berkaitan dengan user dan hak-haknya yaitu dengan cara :

– 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

4) Keamanan Root/Administrator

Selalu perlahan dan berhati-hati ketika menjadi root/administrator. Tindakan anda dapat mempengaruhi banyak hal. Gunakan akses root/administrator jika memang benar-benar dibutuhkan

5) Keamanan File/Sistem File

Directory home user tidak boleh mengakses perintah,mengubahsystem seperti partisi, perubahan device dan lain-lain.

Lakukan setting limit system file.

Atur akses dan permission file : read, write, execute bagi user maupun group.

Selalu cek program-program yang tidak dikenal.

6) 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.

7) Keamanan Kernel

– Selalu update kernel system operasi.

– Ikuti review bugs dan kekurangan-kekurangan pada system operasi.

8) Keamanan Jaringan

– Waspadai paket sniffer yang sering menyadap port Ethernet.

– Lakukan prosedure untuk mengecek integritas data.

– Verifikasi informasi DNS.

– Lindungi network file system.

– Gunakan firewall untuk barrier anara jaringan privat dengan jaringan eksternal.

Macam-Macam Bentuk Serangan Komputer

1.Intrusion

Pada penyerang jenis ini , seseorang penyerang akan bisa menggunakan system computer yang kita miliki , sebagaian penyerang jenis ini menginginkan akses sebagaimana halnya pengguna yang mempunyai hak untuk mengakses system.

2.Intelligence

Intelligence ialah para hacker atau Cracker yang melakukan suatu kegiatan guna mengumpulkan segala informasi yang berkaitan dengan system target, berbagai cara bisa ditempuh guna mendapatkan informasi tersebut , baik melalui internet , mencari buku –buku maupun jurnal.

3.Land Attack

LAND attack ialah salah satu macam serangan terhadap suatu server/komputer yang terhubung dalam suatu jaringan yang bertujuan guna menghentikan layanan yang diberikan oleh server tersebut sehingga terjadi gangguan pada layanan ataupun jaringan komputer tersebut.

4.Logic Bomb

Logic Bomb adalah Program yang dimasukan ke dalam sebuah computer yang bekerja guna memeriksa kumpulan kondisi di system , apabila kondisi – kondisi yang dimaksud ditemukan oleh program tersebut , maka program akan mengeksekusi perintah – perintah yang terdapatdi dalamnya .

5.Operation System Fingerprinting

Istilah ini mengacu kepada kegiatan menganalisis sistem operasi pada sistem yang akan diserang. Ada beberapa cara yang bisa dilakukan. CAra yang paling umum ialah melakukan telnet ke server. Jika server yang dituju mempunyai fasilitas telnet, biasaya ada banner yang menunjukkan sistem operasi yang dipakai.

6.Smurf Attack

Smurf Attack ialah serangan yang dilakukan dengan mengubah alamat IP dari datangnya request atau (IP Spoofing). Penggunaan IP Spoofing jenis ini memungkinkan respon dari ping tadi yang dialamatkan ke kompute yang alamatnya dipalsukan. Akibatnya, komputer akan dibanjiri paket data. Hal tersebut akan mengakibatkan pemborosan bandwith jaringan. Komputer bisa juga menjadi hang karena terus dibanjiri dengan paket data.

7.Scanning

Scanning merupakan kegiatan para hacker atau cracker untuk mengidentifikasi sistem yang menjadi target serangan dan juga mencari celah keamanan yang akan digunakan untuk menembus suatu sistem. Kegiatan scanning dari sisi jaringan sangat berisik dan juga mudah dikenali, kecuali apabila menggunkan stealth scanning. Scanning tool yang paling terkenal ialah nmap. Selain itu ada juga SuperScan dan UltraScan yang banyak dipakai pada sistem Windows.

8.Back door

Seperti namanya, Backdoor adalah suatu akses “pintu belakang” yang diciptakan hacker setelah berhasil menjebol suatu sistem. Hal tersebut dimaksudkan agar para hacker mudah mendapat akses kembali ke dalam sistem yang sudah diserangnya tadi.