Sistem Pengamanan Komputer

Disampaikan: WAN HENDRA M, M.SI

LOGO

Keamanan Komputer

1. Keamanan Komputer
2. Penyerangan
3. Keamanan dan kerahasian data
4. Tugas

KEAMANAN KOMPUTER

- Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab
- Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam system komputer. Jadi bisa disimpulkan keamanan komputer adalah: Suatu usaha pencegahan dan pendeteksian penggunaan komputer secara tidak sah atau tidak diizinkan Usaha melindungi aset dan menjaga privacy dari para cracker yang menyerang

Mungkinkah aman?

Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini Hukum alam keamanan komputer Tidak ada sistem yang 100% aman.

Apa Itu Sistem Yang Aman

Kalau sebuah sistem atau komputer hanya kita matikan, masukkan ke ruangan yang tidak berpintu dan dijaga sepasukan militer, maka tentu sistem atau komputer tersebut tidak ada gunanya lagi bagi kita

Ukuran sebuah sistem yang aman diarahkan ke beberapa parameter dibawah:

Mengorbankan banyak waktu, tenaga dan biaya besar dalam rangka penyerangan Resiko yang dikeluarkan penyerang (intruder)

(perimbangan antara keamanan dan biaya (cost)) : Semakin aman sebuah sistem (tinggi levelnya), maka semakin tinggi biaya yang diperlukan untuk memenuhinya. Karena itu dalam kenyataan, level sistem yang aman boleh dikatakan merupakan level optimal (optimal level) dari keamanan. Artinya titik dimana ada perimbangan antara biaya yang dikeluarkan dan tingkat keamanan yang dibutuhkan

Tahapan Penyerangan

1. Spying & Analyzing (finger printing)
2. Initial Access to The Target (gaining access)
3. Full System Access (rooting)
4. Covering Track & Installing Backdoor (sweeping & backdooring)

1. Spying & Analyzing (finger printing)

Pada tahapan ini, penyerang akan berusaha mempelajari target yang akan diserang, mengumpulkan data termasuk didalamnya teknik-teknik atau hal-hal apa saja yang berkaitan dengan target. Penyerang juga akan menganalisa setiap perubahan yg terjadi baik secara internal maupun eksternal target.

Penyerang menetapkan tujuan penyerangan dari data-data yang telah terkumpul. Penyerang akan menggunakan segala sumber informasi dan pengetahuan anda tentang lingkungan target, tak peduli akan seberapa cepat atau lamakah serangan akan dilakukan. Inti dari tahapan ini adalah analisa dari data dan informasi yang didapat

2.Initial Access to The Target (gaining access)

Mendapatkan akses ke target sistem. Tidak diragukan lagi, inilah bagian yang paling menyenangkan para penyerang. Akses tidak perlu harus root atau user biasa, bisa berupa apa saja, dari akses FTP sampai Sendmail, pokoknya sekedar untuk dapat login sebagai user dalam sistem.

3. Full System Access (Rooting) Tujuan tahapan ini adalah untuk mendapatkan akses penuh dalam target sistem. Pada level ini, dapat dikatakan bahwa para penyerang telah mecapai apa yang mereka harapkan dari rencana-rencana yang telah dijalankan sebelumnya. Mendapatkan password untuk dicrack, memasang trojan, mengambil dokumen atau apa saja.

4. Covering Track & Installing Backdoor (Sweeping Backdooring)

Tujuan tahapan ini adalah untuk menghilangkan jejak dan emasang backdoor. Menghapus log dalam target sistem merupakan langkah yang bagi para penyerang wajib dilakukan untuk menghilangkan jejak. Sedangkan pemasangan backdoor tentu saja tujuannya agar penyerang dapat tetap dengan mudah masuk dalam target sistem.

KEAMANAN DAN KERAHASIAAN DATA

Masalah keamanan dan kerahasiaan data

Merupakan salah satu aspek penting dari suatu sistem informasi. informasi tidak akan berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang

Informasi dikategorikan sebagai berikut :

Sangat Rahasia (Top Secret)

Konfidensial (Confidential)

Terbatasan (Restricted)

Internal Use

Public

1.Sangat Rahasia (Top Secret)

Apabila informasi ini disebarluaskan maka akan berdampak sangat parah terhadap keuntungan berkompetisi dan strategi bisnis organisasi.

Contoh : rencana operasi bisnis, strategi marketing, strategi bisnis.

2. Konfidensial (Confidential), apabila informasi ini disebarluaskan maka ia akan merugikan privasi perorangan, merusak reputasi organisasi.

Contoh : Konsolidasi penerimaan penerimaan, biaya, keuntungan beserta informasi lain yang dihasilkan unit kerja keuangan organisasi, strategi marketing, teknologi, rencana produksi, gaji karyawan, informasi pribadi karyawan, promosi.

3. Terbatasan (Restricted)

Informasi ini hanya ditujukan kepada orang-orang tertentu untuk menopang bisnis organisasi.

Contoh : informasi mengenai bisnis organisasi, peraturan organisasi, strategi marketing yang akan diimplementasikan, strategi harga penjualan, strategi promosi.

4. Internal use, informasi ini hanya boleh digunakan oleh pegawai perusahaanuntuk melaksanakan tugasnya.

Contoh : prosedur, buku panduan, pengumuman/memo organisasi.

5. Public. Informasi ini dapat disebarluaskan kepada umum melalui jalur yang resmi.

Contohnya : informasi di web. Internal korespondensi yang ridak perlu melalui pengontrolan/screening.

TUGAS

Kejahatan siber atau kerap dikenal dengan *cyber crime* merupakan tindak perilaku kejahatan berbasis komputer dan jaringan internet.

Berikut empat jenis tindak kejahatan siber:

- **Penipuan *Phising***
- **Peretasan**
- ***Cyber Stalking***
- ***Cyber Bullying***

Yang ditanyakan?

Buat kajian berdasarkan kasus yang anda pilih dalam bentuk

1. ***Dokumen (makalah)***
2. ***Langkah kejadian (alur kejadian boleh disajikan dalam flowchat dll)***
3. ***Videos (bisa cari di internet)***

- ***Contoh topik (Cyber Crime dalam penipuan Phising)***
- ***4 jenis topik cyber diatas dibagi menjadi 4 kelompok***
- ***Hasil dijelaskan di depan Kelas dengan waktu 2 minggu dari sekarang***
- ***Tolong nama topik dan anggota kelompok di send di grup***