


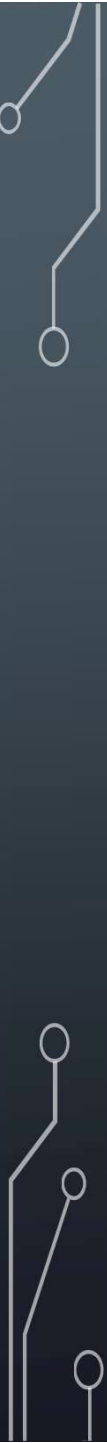


EVALUASI KEAMANAN SISTEM INFORMASI

PERTEMUAN 12



SEBAB MASALAH KEAMANAN HARUS SELALU DIMONITOR (1)

- Lubang Keamanan
 - Ditemukannya lubang keamanan (security Hole) yang baru
 - Biasanya akibat kecerobohan implementasi.
 - Ditemukannya lubang keamanan (security hole) yang baru.
 - Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen.
 - Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.
- 

SEBAB MASALAH KEAMANAN HARUS SELALU DIMONITOR (2)

- Kesalahan konfigurasi : Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan.
 - Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.
- Penambahan perangkat baru (hardware dan/atau software) yang menyebabkan menurunnya tingkat security atau berubahnya metoda untuk mengoperasikan sistem.
 - Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

SUMBER LUBANG KEAMANAN (1)

Salah Design

- Akibat desain yang salah, walaupun implementasinya baik, kelemahan dari sistem akan tetap ada
- Contoh : kesalahan desain urutan nomor (sequence numbering) dari paket TCP/ IP, kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama 'IP Spoofing' (Sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah mengamati urutan paket dari host yang hendak diserang)
- Contoh lain: lemah disainnya algoritma enkripsi ROT13 atau Caesar cipher, dimana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.

SUMBER LUBANG KEAMANAN (2)

Salah implementasi/ implementasi kurang baik

- Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean
- Tidak adanya pemeriksaan dan pengujian implementasi suatu program yang baru dibuat.
- Contoh: lupa memfilter karakter-karakter aneh yang dimasukkan sebagai input dari sebuah program sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

SUMBER LUBANG KEAMANAN (3)

Salah konfigurasi

- Contoh : Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi “writeable”. Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan. Kadangkala sebuah Komputer dijual dengan konfigurasi yang sangat lemah.
- Adanya program yang secara tidak sengaja diset menjadi “setuid root” sehingga ketika dijalankan pemakai memiliki akses seperti superuser (root) yang dapat melakukan apa saja.

Salah menggunakan program / sistem

- Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal

PENGUJIAN KEAMANAN SISTEM (1)

- Untuk memudahkan administrator dari sistem informasi membutuhkan “automated tools”, perangkat pembantu otomatis, yang dapat membantu menguji atau evaluasi keamanan sistem yang dikelola
- Pengujian fungsi, kinerja, aksesibilitas, kompatibilitas dan kegunaan aplikasi tersebut bisa ditemukan dengan cara melakukan pengujian sebelum aplikasi tersebut dirilis ke publik.

Alat Penguji:

- Apache JMeter: Sebuah alat pengujian loading web aplikasi berbasis open source yang support semua platform dan ditulis dengan Java 6+. Biasanya, JMeter digunakan untuk menguji beban dan untuk mengukur dan menganalisa kinerja aplikasi.
- Webt: Merupakan load testing tool yang bekerja semua Windows, menyediakan cara yang mudah dan murah untuk menguji website. Alat ini bekerja pada HTTPS, aplikasi RIA, dan konten yang dinamis.

PENGUJIAN KEAMANAN SISTEM (2)

- **Load Impact:** Ini adalah alat pengujian yang bisa dilakukan secara online untuk menguji aplikasi web, situs web, aplikasi mobile, dan API dibawah beban yang cukup besar untuk semua platform.
- **Sahi:** Sebuah open-source, alat penguji aplikasi web cross-platform, yang ditulis dalam JavaScript dan Java. Hal ini dapat digunakan untuk menguji beberapa aplikasi browser.
- **Watir (Web Application Testing di Ruby):** Ini adalah open source, alat penguji yang cross-platform untuk menguji aplikasi web. Watir termasuk alat penguji yang fleksibel untuk otomatisasi. Mendukung aplikasi yang ditulis dalam semua bahasa walaupun dia dibuat dengan Ruby.
- **Ranorex:** Alat untuk menguji berbasis GUI di Windows yang digunakan untuk menguji web, mobile dan aplikasi berbasis desktop. Sangat cocok untuk skala besar maupun kecil.
- **LoadRunner:** LoadRunner adalah alat untuk menguji loading buatan HP yang digunakan untuk Linux dan Windows, dibuat untuk menguji web aplikasi secara efisien sebelum dirilis ke publik. Alat ini membantu dalam menentukan kinerja web aplikasi.
- **OWASP:** Open Web Application Security Project merupakan sebuah yang bisa cross-platform yang sudah cukup terkenal, fokusnya adalah pada keamanan aplikasi web, dan menciptakan teknik yang free, serta dilengkapi dokumentasi juga lho.

PROBING SERVICE

- Definisi Probing : “probe” (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.
- Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP.
- Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:
 - SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
 - POP3, untuk mengambil e-mail, TCP, port 110
- Contoh di atas hanya sebagian dari servis yang tersedia. Di system UNIX, lihat berkas `/etc/services` dan `/etc/inetd.conf` untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan.

OS FINGERPRINTING

- Fingerprinting : Analisa OS sistem yang dituju agar dapat melihat database kelemahan sistem yang dituju.
- Metode Fingerprinting Cara yang paling konvensional :
 - Service telnet ke server yang dituju, jika server tersebut kebetulan menyediakan servis telnet, seringkali ada banner yang menunjukkan nama OS beserta versinya.
 - Service FTP di port 21. Dengan melakukan telnet ke port tersebut dan memberikan perintah "SYST" anda dapat mengetahui versi dari OS yang digunakan.
 - Melakukan finger ke Web server, dengan menggunakan program netcat (nc).
 - Cara fingerprinting yang lebih canggih adalah dengan menganalisa respon sistem terhadap permintaan (request) tertentu. Misalnya dengan menganalisa nomor urut packet TCP/IP yang dikeluarkan oleh server tersebut dapat dipersempit ruang jenis dari OS yang digunakan. Ada beberapa tools untuk melakukan deteksi OS ini antara lain:
 - nmap
 - queso

PENGGUNAAN PROGRAM PENYERANG

- Untuk mengetahui kelemahan sistem informasi adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet.
- Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data.
- Untuk penyadapan data, biasanya dikenal dengan istilah “sniffer”. Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakan untuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.
- Contoh program penyadap (sniffer) antara lain:
 - pcapure (Unix)
 - sniffit (Unix)
 - tcpdump (Unix)
 - WebXRay (Windows)

PENGGUNAAN SISTEM PEMANTAU JARINGAN

- Sistem pemantau jaringan (network monitoring) dapat digunakan untuk mengetahui adanya lubang keamanan.
- Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat diakses oleh orang dari dalam, akan tetapi dari pemantau jaringan dapat terlihat bahwa ada yang mencoba mengakses melalui tempat lain. Selain itu dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan packet yang jumlahnya berlebihan.
- Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol).