BAB XI
EVALUASI KEAMANAN SISTEM INFORMASI

11.1 Penyebab Masalah Dalam Sistem

Sebab masalah keamanan harus selalu dimonitor, yaitu :

a. 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.
b. 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.
c. 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).

Ada dua penyebab dan masalah dalam sistem keamanan jaringan:

Serangan yang berasal dari luar

1. DoS (Denial of Service), merupakan serangan yang dilancarkan melalui paket-paket jaringan tertentu, biasanya paket-paket sederhana dengan jumlah yang besar dengan maksud mengacaukan keadaan jaringan
2. IP Spoofing, juga dikenal sebagai Source Address Spoffing, yaitu pemalsuan alamat IP attacker
3. Malware, serangan yang dilakukan ketika attacker menaruh program-program penghancur, seperti virus
4. FTP Attack, adalah serangan buffer overflow yang diakibatkan oleh perintah malformed. Tujuannya adalah untuk mendapatkan command shell, yang akhirnya user tersebut dapat mengambil source di dalam jaringan tanpa adanya otorisasi.
5. Sniffer, Adalah usaha untuk menangkap setiap data yang lewat dari suatu jaringan (dapat berupa password).

Serangan dari dalam

1. Password Attack, usaha penerobosan suatu sistem jaringan dengan cara memperoleh password dari jaringan tersebut.
2. Merusak file server
3. Deface web server,

Kerawanan yang terdapat dalam web server adalah :

1. Buffer overflow, hal ini terjadi karena attacker menambah errors pada port yang digunakan untuk web trafic
2. Httpd,
3. Bypasses,
4. Cross scripting
5. kode vulnerabilities
6. floods

11.2 Sumber lubang keamanan jaringan

Lubang keamanan (security hole) dapat terjadi karena beberapa hal yaitu salah disain (design flaw), salah implementasi, salah konfigurasi, dan salah penggunaan.

1. Salah Disain (design flaw)

Umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.

Contoh :

a. 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.
b. Kesalahan disain 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 engamati urutan paket dari host yang hendak diserang).

2. Implementasi kurang baik

Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibat tidak adanya cek atau testing implementasi suatu program yang baru dibuat.

Contoh:

a. Tidak memperhatikan batas (“bound”) dari sebuah “array” tidak dicek sehingga terjadi yang disebut out-of-bound array atau buffer overflow yang dapat dieksploitasi (misalnya overwrite ke variable berikutnya).
b. Kealpaan memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

3. Salah konfigurasi

Meskipun program sudah diimplementasikan dengan baik, masih dapat terjadi lubang keamanan karena salah konfigurasi.

Contoh :

a. 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.

b. Adanya program yang secara tidak sengaja diset menjadi “setuid root” sehingga ketika dijalankan pemakai memiliki akses seperti super user (root) yang dapat melakukan apa saja

4. Salah menggunakan program atau sistem

Salah penggunaan program dapat juga mengakibatkan terjadinya lubang keamanan.

Contoh:

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

11.3 Pengujian Keamanan sistem

Dikarenakan banyaknya hal yang harus dimonitor, administrator dari sistem informasi membutuhkan “automated tools”, perangkat pembantu otomatis, yang dapat membantu menguji atau meng-evaluasi keamanan sistem yang dikelola. Untuk sistem yang berbasis UNIX dan Windows NT ada beberapa tools yang dapat digunakan, antara lain:

Contoh Tools Terintegrasi:

Tabel 11.1 Tools yang terintegrasi

Perangkat lunak bantu	Sistem Operasi
Cops UNIX	Cops UNIX
Tripwire UNIX	Tripwire UNIX
Satan/Saint UNIX	Satan/Saint UNIX
SBScan: localhost security scanner UNIX	SBScan: localhost security scanner UNIX
Ballista <http://www.secnet.com> Windows NT	Ballista <http://www.secnet.com> Windows NT

Penetration Test *(pentest*) merupakan kegiatan yang dilakukan untuk melakukan pengujian terhadap keamanan sebuah sistem. Pengujian ini dilakukan untuk menemukan celah keamanan yang terdapat pada sistem tersebut. Hasil pengujian ini digunakan untuk memperbaiki sisi keamanan dari sistem. Yang dicari dari Pentest ini adalah apakah terdapat celah keamanan yang dapat disalahgunakan (*exploitable vulnerability*). (Ismail 2014)

Contoh Tools Pengujian yang dibuat para hacker

Tabel 11.2 Tools pengujian para hacker

Tools	Kegunaan
Crack	program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (dictionary). Program crack ini melakukan brute force cracking dengan mencoba mengenkripsikan sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan.
land dan latierra	sistem Windows 95/NT menjadi macet (hang, lock up). Program ini mengirimkan sebuah paket yang sudah di"spoofed" sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka
Ping-o-death	sebuah program (ping) yang dapat meng-crash-kan Windows 95/NT dan beberapa versi Unix.
Winuke	program untuk memacetkan sistem berbasis Windows

11.4 Probing Services

Probing yaitu "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.[18]

Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:

1. SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
2. DNS, untuk domain, UDP dan TCP, port 53
3. HTTP, web server, TCP, port 80
4. POP3, untuk mengambil e-mail, TCP, port 110

Contoh di atas hanya sebagian dari servis yang tersedia. Di sistem UNIX, lihat berkas /etc/services dan /etc/inetd.conf untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan. Berkas /etc/services berisi daftar servis dan portnya, sementara berkas /etc/ inetd.conf berisi servis-servis yang di jalan di server UNIX tersebut. Jadi tidak semua servis dijalankan, hanya servis yang dibuka di /etc/inetd.conf saja yang dijalankan. Selain itu ada juga servis yang dijalankan tidak melalui inetd.conf melainkan dijalankan sebagai daemon yang berjalan di belakang layar.[5]

Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan. Sayangnya seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai "default". Kadang-kadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker. Untuk itu ada beberapa program yang dapat digunakan untuk melakukan "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.

Untuk beberapa servis yang berbasis TCP/IP, proses probe dapat dilakukan dengan menggunakan program telnet. Misalnya untuk melihat apakah ada servis e-mail dengan menggunakan SMTP digunakan telnet ke port 25.

```
unix% telnet target.host.com 25
Trying 127.0.0.1...
Connected to target.host.com.
Escape character is '^]'.
220 dma-baru ESMTP Sendmail 8.9.0/8.8.5; Mon, 22 Jun 1998 10:18:54
+0700
```

Dalam contoh di atas terlihat bahwa ada servis SMTP di server tersebut dengan menggunakan program Sendmail versi 8.9.0. Adanya informasi tentang sistem yang digunakan ini sebetulnya sangat tidak disarankan karena dengan mudah orang dapat mengetahui kebocoran sistem (jika software dengan versi tersebut memiliki lubang keamanan).[5]

Program penguji probing (penguji semua port otomatis) :

1. Paket probe untuk sistem UNIX
   - nmap
   - strobe
   - tcpprobe

2. Probe untuk sistem Window 95/98/NT
   - NetLab
   - Cyberkit
   - Ogre

Program yang memonitor adanya probing ke system

Probing biasanya meninggalkan jejak di berkas log di system anda. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing. Selain itu, ada juga program untuk memonitor probe seperti paket program courtney, portsentry dan tcplogd.[19]

11.5 OS FINGERPRINTING

Mengetahui operating system (OS) dari target yang akan diserang merupakan salah satu pekerjaan yang dilakukan oleh seorang cracker. Setelah mengetahui OS yang dituju, dia dapat melihat database kelemahan sistem yang dituju. Fingerprinting merupakan istilah yang umum digunakan untuk menganalisa OS sistem yang dituju.

Fingerprinting dapat dilakukan dengan berbagai cara. Cara yang paling konvensional adalah melakukan telnet ke server yang dituju. Jika server tersebut kebetulan menyediakan servis telnet, seringkali ada banner yang menunjukkan nama OS beserta versinya.

```
unix% telnet 192.168.1.4
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'. Linux 2.0.33 (rock.pau-mikro.org) (ttyp0) login:
```

Apabila sistem tersebut tidak menyediakan servis telnet akan tetapi menyediakan servis FTP, maka informasi juga sering tersedia. Servis FTP tersedia di port 21. Dengan melakukan telnet ke port tersebut dan memberikan perintah “SYST” anda dapat mengetahui versi dari OS yang digunakan seperti contoh di bawah ini.

```
unix% telnet ftp.netscape.com 21
Trying 207.200.74.26...
Connected to ftp.netscape.com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

Jika server tersebut tidak memiliki FTP server akan tetapi menjalankan Web server, masih ada cara untuk mengetahui OS yang digunakan dengan menggunakan program netcat (nc) seperti contoh di bawah ini (dimana terlihat OS yang digunakan adalah Debian GNU):

```
$ echo -e "GET / HTTP/1.0\n\n" | nc localhost 80 | \ grep "^Server:"
Server: Apache/1.3.3 (Unix) Debian/GNU
```

Cara fingerprinting yang lebih canggih adalah dengan menganalisa respon system 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:

1. nmap
2. queso

Berikut ini adalah contoh penggunaan program queso untuk mendeteksi OS dari sistem yang menggunakan nomor IP 192.168.1.1. Kebetulan sistem ini adalah sistem Windows 95.

```
unix# queso 192.168.1.1
192.168.1.1:80 * Not Listen, Windoze 95/98/NT[5]
```

11.6 Penggunaan Program Penyerang

Salah satu cara untuk mengetahui kelemahan sistem informasi anda adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet. Dengan menggunakan program ini anda dapat mengetahui apakah sistem anda rentan dan dapat dieksploitasi oleh orang lain. Perlu diingat bahwa jangan menggunakan program-program tersebut untuk menyerang sistem lain (sistem yang tidak anda kelola). Ini tidak etis dan anda dapat diseret ke pengadilan.

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.[19]

Contoh program penyadap (sniffer) antara lain:

- pcapture (Unix)
- sniffit (Unix)
- tcpdump (Unix)
- WebXRay (Windows)

11.7 Penggunaan Sistem Pemantau Jaringan

Sistem pemantau jaringan (network monitoring) dapat di gunakan untuk mengetahui adanya lubang keamaman. Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat di akses 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 di lihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan packet yang jumlahnya berlebihan.

Network monitoring biasanya di lakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol). Tingkat keamanan dari SMNP versi 1 sangat rendah sehingga memungkinkan penyadapan oleh orang yang tidak berhak.

Contoh-contoh program network monitoring atau management antara lain :

1. Etherboy (Windows), Etherman (Unix).
2. HP Openview (Windows).
3. Packetboy (Windows), Packetman (Unix).
4. SNMP Collector (Windows).
5. Webboy (Windows).

Contoh program pemanatu jaringan yang tidak menggunakan SNMP antara lain :

1. iplog, icmplog, updlog, yang merupakan bagian dari paket iplog untuk memantau paket IP, ICMP, UDP.
2. iptraf, sudah termasuk dalam paket Linux Debian netdiag.
3. netwatch, sudah termasuk dalam paket Linux Debian netdiag.
4. ntop, memantau jaringan seperti program top yang memantau proses di sistem Unix (lihat contoh gambar tampilannya).
5. trafshow, menunjukkan traffic antar hosts dalam bentuk text-mode.

Server dan network monitoring merupakan sebuah sistem yang berfungsi untuk memonitoring kondisi dari suatu jaringan. sistem ini akan melakukan proses monitoring secara terus menerus pada saat sistem jaringan aktif sehingga jika terjadi masalah maka akan mudah untuk mengetahuinya. Semisal, jika ada perangkat hardware atau software yang ada dalam NMS

menjadi down atau bahkan mati maka NMS akan memberi tanda kepada administrator. Dan salah satu fungsi dari sistem ini yaitu berguna untuk menganalisa apakah server masih cukup layak untuk digunakan atau perlu tambahan kapasitas.

Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol). Kebutuhan akan Simple Network Management Protocol pada sebuah sistem monitoring disebabkan oleh kebutuhan akan pemerolehan data monitoring dari sumber daya komputer lain.

Pentingnya setiap perusahan memiliki sistem untuk memonitoring sebuah server atau jaringan akan memudahkan kerja admin dalam memelihara server-server yang terdapat pada perusahaan tersebut.

Berikut ini sistem kerja pada server dan network monitoring :

1. Memastikan bahwa DNS Server telah tersetting sebagaimana mestinya.
2. Mengawasi server apakah berfungsi dengan baik atau tidak.
3. Menganalisa trafik terhadap server.
4. Mengambil tindakan secepatnya bisa terjadi kesalahan dalam server
5. Mengawasi pemakaian space server

Ada beberapa keuntungan melakukan sistem monitor yang baik untuk jaringan anda:

1. Tool monitor akan memperlihatkan tentang infrastruktur jaringan dan dapat menangani kebutuhan pengguna jaringan.
2. Dengan melihat trafik jaringan, akan dapat mendeteksi dan mencegah penyerang yang ingin mengakses ke server dan layanan yang penting.
3. Virus jaringan dengan mudah dideteksi.
4. Jika ada masalah pada jaringan, sistem akan segera memberitahukan masalah secara spesifik. Beberapa masalah bahkan bisa diperbaiki secara otomatis.
5. Kinerja pada jaringan dapat di optimisasikan.
6. Perencanaan untuk kapasitas jaringan lebih mudah. (Softbless n.d.)

Soal

1. Jelaskan apa itu Salah Desain?
2. Apa itu Probing Sevices ?