



Aspek Keamanan Dan Kerahasiaan SI



Agenda

- Evaluasi Keamanan Sistem Informasi
- Sumber Lubang Keamanan
- Penguji Keamanan Sistem
- Probing Services
- Penggunaan Program
- Program Pemantau Jaringan



Evaluasi Keamanan SI

Meski sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah keamanan harus selalu dimonitor. Hal ini disebabkan oleh beberapa hal, antara lain:

- Ditemukannya lubang keamanan (security hole) yang baru.
Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Terkadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.



Evaluasi Keamanan SI

- Kesalahan konfigurasi.

Terkadang karena lalai atau lupa, 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



Evaluasi Keamanan SI

- Penambahan perangkat baru (hardware dan/atau software) Menyebabkan menurunnya tingkat security atau berubahnya metode untuk mengoperasikan system

Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang masih menjadi masalah, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).



Sumber Lubang Keamanan

- Lubang keamanan (security hole) dapat terjadi karena beberapa hal:
 - Salah desain (design flaw)
 - Salah implementasi
 - Salah konfigurasi
 - Salah penggunaan



Sumber Lubang Keamanan

- Salah desain (design flaws)

Lubang keamanan yang ditimbulkan oleh salah desain umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat desain yang salah, maka meskipun ia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.



Sumber Lubang Keamanan

Contoh:

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

- Salah implementasi

Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibatnya cek atau testing yang harus dilakukan menjadi tidak dilakukan.



Sumber Lubang Keamanan

Contoh:

Lupa (tidak tahu?) memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program (misalnya input dari HTML Script) sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses



Sumber Lubang Keamanan

- Salah konfigurasi

Contoh:

Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi "writeable".

phpmyadmin?



Sumber Lubang Keamanan

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



Sumber Lubang Keamanan

- Contoh:

Administrator baru yang teledor dalam menjalankan perintah "rm -rf" di system UNIX (yang menghapus berkas atau direktori beserta sub direktori di dalamnya).



Penguji Keamanan Sistem

Karena banyaknya hal yang harus dimonitor, administrator dari sistem informasi membutuhkan “automated tools”, perangkat pembantu otomatis, yang dapat membantu menguji atau mengevaluasi keamanan sistem yang dikelola.



Penguji Keamanan Sistem

Untuk sistem yang berbasis UNIX ada beberapa tools yang dapat digunakan, antara lain:

- Tripwire
- SAINT
- COPS
- ?



Probing Services

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

- HTTP; TCP port 80
- FTP; TCP port 21



Probing Services

- Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan.
- Seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai "default". Terkadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker.



Probing Services

- Ada beberapa tools 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.



Probing Servis

- Beberapa tools probing:
 - Nmap
 - Strobe
 - Tcpprobe



Penggunaan Program

- Salah satu cara untuk mengetahui kelemahan sistem informasi anda adalah dengan menyerang diri sendiri.
- Jangan menggunakan program-program tersebut untuk menyerang sistem lain (sistem yang tidak anda kelola).



Penggunaan Program

Dua jenis program penyerang :

- Aktif

Program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju.

- Pasif

Program penyerang yang sifatnya melakukan pencurian atau penyadapan data.



Penggunaan Program

- Contoh program:
 - Pcapture
 - Tcpdump
 - Wireshark

Penggunaan Program

Capturing from wlan0 [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
9	6.765544000	173.194.38.176	10.7.10.29	ICMP	98	Echo (ping) reply id=0x0f3a, seq=2/512, ttl=57
10	6.765797000	10.7.10.29	10.7.10.1	DNS	87	Standard query 0x6544 PTR 176.38.194.173.in-addr.arpa
11	6.769947000	10.7.10.1	10.7.10.29	DNS	126	Standard query response 0x6544 PTR sin04s02-in-f16.1e100.net
12	7.745158000	10.7.10.29	173.194.38.176	ICMP	98	Echo (ping) request id=0x0f3a, seq=3/768, ttl=64
13	7.766137000	173.194.38.176	10.7.10.29	ICMP	98	Echo (ping) reply id=0x0f3a, seq=3/768, ttl=57
14	7.766341000	10.7.10.29	10.7.10.1	DNS	87	Standard query 0xe792 PTR 176.38.194.173.in-addr.arpa
15	7.770423000	10.7.10.1	10.7.10.29	DNS	126	Standard query response 0xe792 PTR sin04s02-in-f16.1e100.net
16	10.760748000	(Routerbo_af:45:43)	LiteonTe_93:a8:19	ARP	60	Who has 10.7.10.29? Tell 10.7.10.1
17	10.760780000	(LiteonTe_93:a8:19)	Routerbo_af:45:43	ARP	42	10.7.10.29 is at 1c:65:9d:93:a8:19
18	28.474271000	(Routerbo_0c:03:3f)	LenovoMo_f7:76:5c	LLC	38	I, N(R)=16, N(S)=0; DSAP SNAP Individual, SSAP NULL LSAP Command
19	30.835322000	(Routerbo_0c:03:3f)	LiteonTe_93:a8:19	IPv4	14	[Malformed Packet]
20	49.676035000	(Cisco_f7:d0:82)	PVST+	STP	64	Conf. Root = 32768/710/00:11:92:f7:d0:80 Cost = 0 Port = 0x800
21	50.910485000	(Routerbo_0c:03:3f)	LiteonTe_93:a8:19	IPv4	14	[Malformed Packet]

▶ Frame 1: 14 bytes on wire (112 bits), 14 bytes captured (112 bits) on interface 0

▶ Ethernet II, Src: Routerbo_0c:03:3f (00:0c:42:0c:03:3f), Dst: LiteonTe_93:a8:19 (1c:65:9d:93:a8:19)

▶ [Malformed Packet: IPv4]

0000 1c 65 9d 93 a8 19 00 0c 42 0c 03 3f 08 00 .e.....B..?..

wlan0: <live capture in progress> Fil Packets: 21 Displayed: 21 Marked: 0 Profile: Default



Program Pemantau Jaringan

- Sistem pemantau jaringan (network monitoring) dapat digunakan untuk mengetahui adanya lubang keamanan.
- Dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan system dengan melalui denial of service attack (DoS) dengan mengirimkan paket yang jumlahnya berlebihan.
- Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol).



Program Pemantau Jaringan

- Contoh-contoh program network monitoring / management antara lain:
 - Etherboy (Windows), Etherape (Unix)
 - HP Openview (Windows)
 - Packetboy (Windows), Packetman (Unix)
 - SNMP Collector (Windows)
 - Webboy (Windows)

Program Pemantau Jaringan

The screenshot displays the EtherApe network monitoring application. It features a 'Protocols' window on the left and a main network graph window on the right. The terminal window at the bottom shows the execution of ping commands to various hosts.

EtherApe: Protocols

Protocol	Port	Inst Traffic	Accum Traffic	Last Heard	Packets
BOOTPS	67	0 bps	2.338 Kbytes	32" ago	7
DOMAIN	53	0 bps	11.402 Kbytes	16" ago	115
HTTPS	443	0 bps	8.121 Kbytes	10" ago	113
ICMP	-	0 bps	5.551 Kbytes	16" ago	58
IP_UNKNOWN	-	0 bps	14 bytes	1'46" ago	1
NETBIOS-NS	137	0 bps	92 bytes	1'46" ago	1
WWW	80	0 bps	2.256 Kbytes	1'9" ago	40

EtherApe Network Graph

The graph shows a central node '10.7.10.29' connected to several other nodes:

- 202.92.198.146
- 255.255.255.255
- sin04s02-in-44.1e100.net
- sin04s02-in-44.1e100.net
- sin01s05-in-8.1e100.net
- 0.0.0.0
- 10.7.10.1
- sin01s05-in-6.1e100.net
- 10.7.10.29
- edge-star-ecmp-12*pm1.facebook.com

Terminal Output:

```
root@bt: ~
l=244 time=191 ms
^C
--- star.c10r.facebook.com ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 2002ms
rtt min/avg/max/mdev = 191.032/243.335/295.639/52.305 ms
root@bt: # ping localhost
PING localhost (127.0.0.1): 56(84) bytes of data:
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.041 ms
^C
--- localhost ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.041/0.041/0.041/0.000 ms
root@bt: # ping secureit.com
PING secureit.com (202.92.198.146) 56(84) bytes of data:
64 bytes from 202.92.198.146: icmp_seq=1 ttl=64 time=1.78 ms
64 bytes from 202.92.198.146: icmp_seq=3 ttl=64 time=1.77 ms
64 bytes from 202.92.198.146: icmp_seq=4 ttl=64 time=1.78 ms
64 bytes from 202.92.198.146: icmp_seq=5 ttl=64 time=1.75 ms
^C
--- secureit.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4011ms
rtt min/avg/max/mdev = 1.756/1.775/1.786/0.032 ms
root@bt: #
```