



KEAMANAN SISTEM INFORMASI

**Evaluasi Keamanan Sistem
Pertemuan III**

Rianto, S.Kom., M.Eng.

Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : me@rianto.com Website : <http://www.rianto.com>

Mobile : 0815 787 02873

Daftar Isi

- Sumber lubang keamanan
- Penguji keamanan Sistem
- Melakukan Probing pada Network
- Penggunaan program penyerang
- Penggunaan Sistem pemantau jaringan

Monitoring

Beberapa hal yang menyebabkan perlu monitoring

1. Ditemukannya lubang keamanan (security hole) yang baru.
2. Kesalahan konfigurasi.
3. Penambahan perangkat baru (hardware dan/atau software)

Security Hole dapat terjadi karena :

- Salah Design
- Salah Konfigurasi
- Salah Implementasi
- Salah Penggunaan

Probing

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
- DNS, untuk domain, UDP dan TCP, port 53
- HTTP, web server, TCP, port 80
- POP3, untuk mengambil e-mail, TCP, port 110

Untuk beberapa servis yang berbasis TCP/IP, proses *probe* dapat dilakukan dengan menggunakan program telnet.

Paket *probe* untuk sistem UNIX : *nmap* , *strobe*, *tcpprobe*

Probe untuk sistem Window 95/98/NT : *NetLab*, *Cyberkit*, *Ogre*

Probing

- **Mendeteksi Probing**

Untuk mendeteksi adanya probing ke sistem informasi dapat dipasang suatu program yang memonitornya.

Probing biasanya meninggalkan jejak di berkas log di sistem. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing.

Program Probe lain : *courtney*, *portsentry* dan *tcplogd*.

Probing

- **OS FINGERPRINTING**

Fingerprinting merupakan istilah yang umum digunakan untuk menganalisa OS sistem yang dituju.

Fingerprinting dapat dilakukan dengan berbagai cara. Cara yang paling konvensional adalah :

1. Melakukan telnet ke server yang dituju.
2. Servis FTP. Servis FTP tersedia di port 21.
Dengan melakukan telnet ke port tersebut dan memberikan perintah “SYST” anda dapat mengetahui versi dari OS yang digunakan.
3. Menggunakan program *netcat* (*nc*)

Probing

- **Aplikasi Berbasis Web**

Dapat menggunakan aplikasi berbasis web untuk melihat data-data domain. Misalnya dengan Menggunakan <http://www.domainwhitepages.com>

Sistem Pemantau Jaringan

Sistem pemantau jaringan (*network monitoring*) dapat digunakan untuk mengetahui adanya lubang keamanan.

- Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (*Simple Network Management Protocol*).
- Contoh-contoh program network monitoring / management antara lain:
 - *Etherboy* (Windows), *Etherman* (Unix)
 - *HP Openview* (Windows)
 - *Packetboy* (Windows), *Packetman* (Unix)
 - *SNMP Collector* (Windows)
 - *Webboy* (Windows)

Sistem Pemantau Jaringan

Contoh program pemantau jaringan yang tidak Menggunakan SNMP antara lain:

- *iplog, icmplog, updlog*, yang merupakan bagian dari paket *iplog* untuk memantau paket IP, ICMP, UDP.
- *iptraf*, sudah termasuk dalam paket Linux Debian *netdiag*
- *netwatch*, sudah termasuk dalam paket Linux Debian *netdiag*
- *ntop*, memantau jaringan seperti program *top* yang memantau proses di sistem Unix
- *trafshow*, menunjukkan traffic antar hosts dalam bentuk text-mode

Pemantau Serangan

- Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tak diundang (*intruder*) atau adanya serangan (*attack*).
- Nama lain dari sistem ini adalah “*intruder detection system*” (IDS).
- Sistem ini dapat memberitahu administrator melalui e-mail maupun melalui mekanisme lain seperti melalui pager.

Pemantau Serangan

- *Autobuse*, mendeteksi probing dengan memonitor logfile.
- *Courtney* dan *portsentry*, mendeteksi *probing* (*port scanning*) dengan memonitor packet yang lalu lalang. *Portsentry* bahkan dapat memasukkan IP penyerang dalam filter *tcpwrapper* (langsung dimasukkan kedalam berkas */etc/hosts.deny*)
- *Shadow* dari SANS
- *Snort*, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi.

Honeypot

- Merupakan sebuah sistem yang digunakan untuk memancing dan memantau hacker
- Berupa kumpulan software (server) yang seolah-olah merupakan server yang hidup dan memberi layanan tertentu
- SMTP yang memantau asal koneksi dan aktivitas penyerang (misalnya penyerang berniat menggunakan server tersebut sebagai mail relay)
- Beberapa honeypot digabungkan menjadi honeynet

Daftar Pustaka

- Keamanan Sistem Informasi
Dr. Budi rahardjo
- Materi Kuliah Keamanan Jaringan
Bina Sarana Informatika