Evaluasi Keamanan Sistem Informasi

Budi Rahardjo

ID-CERT
PPAU Mikroelektronika ITB
PT INSAN KOMUNIKASI – PT INDOCISC

Pentingnya Evaluasi

- Lubang keamanan diketemukan hampir setiap hari.
- Kesalahan konfigurasi bisa terjadi.
- Penambahan perangkat baru yang mengubah konfigurasi yang sudah ada.

Sumber Lubang Keamanan

- Disain kurang baik
  - TCP/IP sequence numbering, IP spoofing
  - Algoritma enkripsi yang lemah
- Implementasi kurang baik
  - Implementasi terburu-buru
  - Bad programming, out-of-bound array
  - sloppy programming

Sumber Lubang Keamanan

- Kesalahan konfigurasi
  - Berkas yang esensial menjadi *writeable for all.* Contoh: berkas password, aliases, log.
  - Default account masih aktif
  - False sense of security
- Kesalahan menggunakan program.
  - **`rm -rf /`**
  - **`del *,*`**

Penguji Keamanan Sistem

- Automated tools berbasis informasi tentang security hole
  - Crack: memecahkan password
  - Tripwire: integritas berkas dan direktori
  - Satan/Saint: Menguji keamanan sistem melalui Web
  - Cops

Probing Services

- Melihat servis yang diberikan oleh sebuah server
- Servis diberikan melalui TCP atau UDP dengan port tertentu.
  - telnet, port 23
  - SMTP, port 25
  - HTTP/WWW, port 80
  - POP, port 110

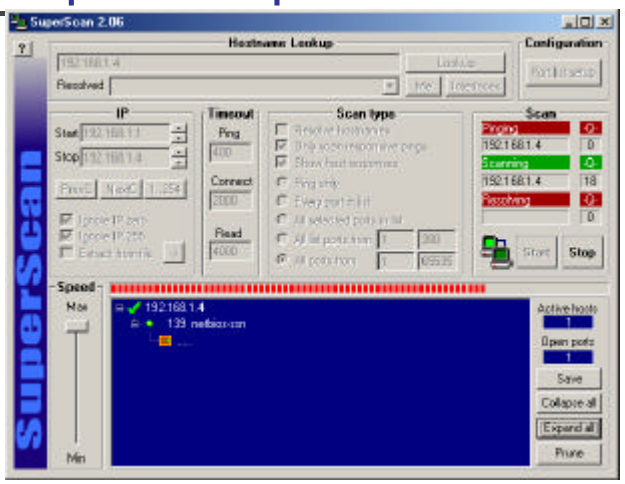
Probing Services (cont.)

- Menguji secara manual lewat telnet
- Menguji SMTP:
  `telnet localhost 25`

Program Probe

- Proses probing secara otomatis
- UNIX:
  - nmap, strobe, tcpprobe
- Windows 95/98/NT
  - SuperScan, Netlab, Ogre
- Deteksi melalui
  - Unix: Courtney, Portsentry
  - Windows: attacker

Tampilan SuperScan



Penggunaan Attack

- Menyerang diri sendiri untuk melihat security hole.
- Jangan menyerang sistem milik orang lain
- Memperolah program attack
  - http://www.rootshell.com
  - http://www.antionline.com
  - http://packetstorm.securify.com
  - http://www.technotronic.com

Contoh Program Penyerang

- Denial of Service (DoS) Attack
  - land, latierra, winnuke, jolt & variasinya
  - ping-o-death
  - mail server attack: MS Exchange, Netscape
  - mail bombing
  - mail attachment attack: rockme.c
  - Distributed DoS attack: trinoo, TFN

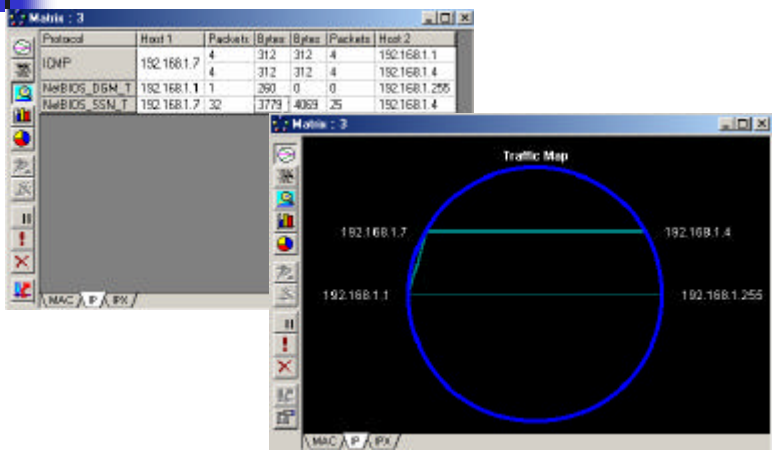
Network Monitoring

- Network monitoring untuk melihat trafik yang tidak normal.
- Dapat digunakan oleh lawan untuk menganalisa trafik sistem anda.
- Dapat digunakan untuk menangkap data (sniffer)!

Network Traffic Analysis Tools

- Etherman, packetman
- Etherboy, packetboy
- sniffit, tcpdump
- iptraf, netwatch, ntop

Contoh peragaan Sniffer



Langkah Selanjutnya

- Setelah melakukan evaluasi, dapat diketahui bagian mana saja yang dapat ditingkatkan keamanannya.
- Tingkatkan keamanan.