MODUL 6
INTRUSION DETECTION SYSTEM [PORTSENTRY]

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep portsentry di linux
2. Mahasiswa memahami sistem blocking portsentry di linux
3. Mahasiswa mampu melakukan analisa terhadap portsentry yang ada di linux

DASAR TEORI

Dari sekian banyak hal yang paling banyak di takuti orang pada saat mengkaitkan diri ke Internet adalah serangan virus & hacker. Penggunaan Software Firewall akan membantu menahan serangan dari luar. Pada kenyataan di lapangan, menahan serangan saja tidak cukup, kita harus dapat mendeteksi adanya serangan bahkan jika mungkin secara otomatis menangkal serangan tersebut sedini mungkin. Proses ini biasa disebut dengan istilah Intrusion Detection.

PortSentry adalah sebuah perangkat lunak yang di rancang untuk mendeteksi adanya port scanning & meresponds secara aktif jika ada port scanning. Port scan adalah proses scanning berbagai aplikasi servis yang dijalankan di server Internet. Port scan adalah langkah paling awal sebelum sebuah serangan di lakukan.

Cara kerja port sentry dengan melakukan melihat komputer yang melakukan scan dan secara aktif akan memblokir mesin penyerang agar tidak dapat masuk & melakukan transaksi dengan Server kita.

PortSentry dapat di download secara pada http://www.psionic.com.

Beberapa fitur utama dari PortSentry:

- Berjalan di atas soket TCP & UDP untuk mendeteksi scan port ke sistem kita.
- Mendeteksi stealth scan, seperti SYN/half-open, FIN, NULL, X-MAS.
- PortSentry akan bereaksi secara real-time (langsung) dengan cara memblokir IP address si penyerang. Hal ini dilakukan dengan menggunakan ipchains/ipfwadm dan memasukan ke file /etc/host.deny secara otomatis oleh TCP Wrapper.
- PortSentry mempunyai mekanisme untuk mengingat mesin / host mana yang pernah connect ke dia. Dengan cara itu, hanya mesin / host yang terlalu sering melakukan sambungan (karena melakukan scanning) yang akan di blokir.
- PortSentry akan melaporkan semua pelanggaran melalui syslog dan mengindikasikan nama system, waktu serangan, IP mesin penyerang, TCP / UDP port tempat serangan dilakukan. Jika hal ini di integrasikan dengan Logcheck maka administrator system akan memperoleh laporan melalui e-mail.

Dengan adanya berbagai fitur di atas maka system yang kita gunakan tampaknya seperti hilang dari pandangan penyerang. Hal ini biasanya cukup membuat kecut nyali

penyerang.

Penggunaan PortSentry sendiri sangat mudah sekali, bahkan untuk penggunaan biasa saja praktis semua instalasi default tidak perlu di ubah apa-apa dapat langsung digunakan.

Yang mungkin perlu di tune-up sedikit adalah file konfigurasi portsentry yang semuanya berlokasi di /etc/portsentry secara default. Untuk mengedit file konfigurasi tersebut anda membutuhkan privilige sebagai root. Beberapa hal yang mungkin perlu di set adalah:

- file /etc/portsentry/portsentry.conf merupakan konfigurasi utama portsentry. Disini secara bertahap diset port mana saja yang perlu di monitor, responds apa yang harus di lakukan ke mesin yang melakukan portscan, mekanisme menghilangkan mesin dari routing table, masukan ke host.deny. Proses setting sangat mudah hanya dengan membuka / menutup tanda pagar (#) saja.
- pada file /etc/portsentry/portsentry.ignore.static masukan semua IP address di LAN yang harus selalu di abaikan oleh portsentry. Artinya memasukan IP address ke sini, agar tidak terblokir secara tidak sengaja.
- Pada file /etc/default/portsentry kita dapat menset mode deteksi yang dilakukan portsentry. Semakin baik mode deteksi yang dipilih (advanced stealth TCP/UP scanning), biasanya PortSentry akan semakin sensitif & semakin rewel karena sedikit-sedikit akan memblokir mesin.

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep portsentry ?
2. Sebutkan fasilitas portsentry yang ada di linux !

PERCOBAAN

1. Jalankan perintah berikut untuk installasi
   # apt-get install portsentry

2. Edit file konfigurasi untuk bloking serangan dengan TCPWrapper:
   # vim /etc/portsentry/portsentry.conf
   Edit bagian berikut

```
#Edit bagian HISTORY_FILE dan BLOCKED_FILE menjadi:
#
IGNORE_FILE=”/etc/portsentry/portsentry.ignore”
HISTORY_FILE="/var/lib/portsentry/portsentry.history"
BLOCKED_FILE="/var/lib/portsentry/portsentry.blocked"
#
#
################################
# Misc. Configuration Options #
################################
RESOLV_HOST="0"
######################Ini diperlukan utk memblok TCP dan UDP
BLOCK_UDP=”1”
BLOCK_TCP=”1”
```

```
######################
# TCP Wrapper #
###################### Perintah ini untuk memblok ip di /etc/hosts.deny
KILL_HOSTS_DENY=”ALL: $TARGET$ : DENY”
######################
#EOF
```

3. Edit File /etc/portsentry/portsentry.ignore.static, isi dengan IP yang tidak terblokir, misal :

```
# Format : <Ip Address>/<Netmask>
# Misalnya: Konfigurasi Ip di Router initrd@vmlinuz.unixminix.com
# eth0 : 202.212.77.99/30
# eth1 : 192.168.1.1/24
#
# Maka Daftar Hosts-nya menjadi :
#
# Exclude all local interface
192.168.50.1/32
192.168.50.10
127.0.0.1

# Exclude default Gateway
202.212.77.98
#
# Exclude nameserver
202.212.77.1
#
# Catatan: jika kita tidak mencantumkan nilai mask_length-nya
# maka diasumsikan bernilai 32 bits.
# Jadi 192.168.1.1 sama dengan 192.168.1.1/32
```

4. File /etc/default/portsentry

```
TCP_MODE=”atcp”
UDP_MODE=”audp”
```

NB:
Pilihan TCP_MODE dan UDP_MODE :
tcp : deteksi portscan sesuai yang ditentukan di TCP_PORT di portsentry.conf
atcp : advanced tcp / udp port
stcp : adanya tambahan deteksi stealth scan

5. Bukalah port sebanyak mungkin untuk persiapan portsentry.
   Misal : http (80), ftp (21), ssh (22), telnet (23)
   # nmap localhost

   NB : Jika belum ada dapat dilakukan instalasi terlebih dahulu
   # apt-get install apache2 proftpd openssh-server telnetd

6. Insialisasi Daemon
   #/etc/init.d/portsentry restart
7. Jika sudah jalan, jalankan **# tail -f /var/log/syslog**, akan keluar hasil spt berikut :
   Nov 20 08:35:27 localhost portsentry[2192]: adminalert: PortSentry is now active and listening.
8. Pada komputer lain (PC penyerang) jalankan nmap ke komputer yang diinstal portsentry (PC target) apa yang terjadi.
   # nmap –sT –v no_IP_komputer_portsentry
   NB: Scanning yang pertama biasanya masih diterima oleh target, baru scanning berikutnya akan diblok.

   a. Lakukan scanning dari ip yang akan diblok
   b. Lakukan scanning dari daftar ip dari poin 3
9. Cek ip yang terblokir di PC target
   # vim /etc/hosts.deny
10. Blocking menggunakan iptables
    a. Hapus ip yang diblok (uncomment) pada file /etc/hosts.deny : **# vim /etc/hosts.deny**
       `#ALL: ip_penyerang : DENY`
    b. Edit file konfigurasi : **# vim /etc/portsentry/portsentry.conf**
       Uncomment pada perintah tcpwrapper berikut
       `# KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"`
       Buka comment pada perintah berikut untuk iptables
       `KILL_ROUTE="/sbin/iptables –I INPUT –s $TARGET$ -j DROP"`
    c. Jalankan lagi portsentry
       #/etc/init.d/portsentry restart
    d. Ulangi langkah 8.

11. Cek informasi pada IGNORE_FILE, HISTORY_FILE, BLOCKED_FILE pada step 2.
    a. # vim /etc/portsentry/portsentry.ignore
    b. # vim /var/lib/portsentry/portsentry.history
12. Selanjutnya tutup/matikan service portsentry dan jalankan nmap lagi, apa yang terjadi

LAPORAN RESMI

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Dengan bekerja hanya mendeteksi port dimana sebaiknya portsentry ditempatkan ?
3. Jelaskan arsitektur portsentry sehingga bisa melakukan blok menggunakan firewall jika ada yang dicurigai!

LEMBAR ANALISA

Praktikum Network Security (IDS - portsentry)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

A. Gambar topologi jaringan beserta dengan IP Addressnya

B. Catat ip yang tidak terblokir pada poin 3

C. Catat hasil nmap pada poin 5

D. Catat hasil log pada poin 7

E. Catat proses scanning dari PC penyerang ke PC target menggunakan tcpwrapper, catat juga ip yang diblok dan yang tidak (poin 8 & 9)

F. Catat proses scanning dari PC penyerang ke PC target menggunakan iptables (poin 10)

G. Catat informasi pada IGNORE_FILE DAN HISTORY_FILE (poin 11)

H. Catat proses pada poin 12.