

# MODUL 3

## INTRUSION DETECTION SYSTEM DG SNORT

### TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep IDS dg snort di linux
2. Mahasiswa memahami cara membuat rule pada snort
3. Mahasiswa mampu menggabungkan snort dengan base dan mySQL

### DASAR TEORI

#### Deteksi Penyusupan (Intrusion Detection)

Deteksi penyusupan adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus yang otomatis. Program yang dipergunakan biasanya disebut sebagai Intrusion Detection System (IDS).

Tipe dasar dari IDS adalah:

- Rule-based systems - berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalu lintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
- Adaptive systems - mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada, tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk bentuk penyusupan yang baru.

Bentuk yang sering dipergunakan untuk komputer secara umum adalah rule-based systems.

Pendekatan yang dipergunakan dalam rule-based systems ada dua, yakni pendekatan pencegahan (preemptory) dan pendekatan reaksi (reactionary). Perbedaannya hanya masalah waktu saja. Pendekatan pencegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan, maka program akan melakukan tindakan yang perlu. Pendekatan reaksi, program pendeteksi penyusupan hanya mengamati file log. Jika ditemukan paket yang mencurigakan, program juga akan melakukan tindakan yang perlu.

### Snort

#### *Mengoperasikan Snort*

Tiga (3) buah mode, yaitu

1. **Sniffer mode**, untuk melihat paket yang lewat di jaringan.
2. **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
3. **Intrusion Detection mode**, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai rules / aturan yang akan membedakan

sebuah paket normal dengan paket yang membawa serangan.

### **Sniffer Mode**

Untuk menjalankan snort pada sniffer mode tidaklah sukar, beberapa contoh perintah-nya terdapat di bawah ini,

```
#snort -v  
#snort -vd  
#snort -vde  
#snort -v -d -e
```

dengan menambahkan beberapa switch `-v`, `-d`, `-e` akan menghasilkan beberapa keluaran yang berbeda, yaitu

- v, untuk melihat header TCP/IP paket yang lewat.
- d, untuk melihat isi paket.
- e, untuk melihat header link layer paket seperti ethernet header.

### **Packet Logger Mode**

Tentunya cukup melelahkan untuk melihat paket yang lewat sedemikian cepat di layar terutama jika kita menggunakan ethernet berkecepatan 100Mbps, layar anda akan scrolling dengan cepat sekali susah untuk melihat paket yang di inginkan. Cara paling sederhana untuk mengatasi hal ini adalah menyimpan dulu semua paket yang lewat ke sebuah file untuk di lihat kemudian, sambil santai ... Beberapa perintah yang mungkin dapat digunakan untuk mencatat paket yang ada adalah

```
./snort -dev -l ./log  
./snort -dev -l ./log -h 192.168.0.0/24  
./snort -dev -l ./log -b
```

perintah yang paling penting untuk me-log paket yang lewat adalah

```
-l ./log
```

yang menentukan bahwa paket yang lewat akan di log / di catat ke file `./log`. Beberapa perintah tambahan dapat digunakan seperti `-h 192.168.0.0/24` yang menunjukkan bahwa yang di catat hanya packet dari host mana saja, dan `-b` yang memberitahukan agar file yang di log dalam format binary, bukan ASCII.

Untuk membaca file log dapat dilakukan dengan menjalankan snort dengan di tambahkan perintah `-r` nama file log-nya, seperti,

```
./snort -dv -r packet.log  
./snort -dvr packet.log icmp
```

### **Intrusion Detection Mode**

Mode operasi snort yang paling rumit adalah sebagai pendeteksi penyusup (intrusion detection) di jaringan yang kita gunakan. Ciri khas mode operasi untuk pendeteksi penyusup adaah dengan menambahkan perintah ke snort untuk membaca file konfigurasi `-c` nama-file-konfigurasi.conf. Isi file konfigurasi ini lumayan banyak, tapi sebagian besar telah di set secara baik dalam contoh `snort.conf` yang dibawa oleh source snort. Beberapa contoh perintah untuk mengaktifkan snort untuk melakukan pendeteksian penyusup, seperti

```
./snort -dev -l ./log -h 192.168.0.0/24 -c snort.conf
```

```
./snort -d -h 192.168.0.0/24 -l ./log -c snort.conf
```

Untuk melakukan deteksi penyusup secara prinsip snort harus melakukan logging paket yang lewat dapat menggunakan perintah `-l` nama-file-logging, atau membiarkan snort menggunakan default file logging-nya di directory `/var/log/snort`. Kemudian menganalisa catatan / logging paket yang ada sesuai dengan isi perintah `snort.conf`.

Ada beberapa tambahan perintah yang akan membuat proses deteksi menjadi lebih efisien, mekanisme pemberitahuan alert di Linux dapat di set dengan perintah `-A` sebagai berikut,

- A fast, mode alert yang cepat berisi waktu, berita, IP & port tujuan.
- A full, mode alert dengan informasi lengkap.
- A unsock, mode alert ke unix socket.
- A none, mematikan mode alert.

Untuk mengirimkan alert ke syslog UNIX kita bisa menambahkan switch `-s`, seperti tampak pada beberapa contoh di bawah ini.

```
./snort -c snort.conf -l ./log -s -h 192.168.0.0/24
```

```
./snort -c snort.conf -s -h 192.168.0.0/24
```

Untuk mengirimkan alert binary ke workstation windows, dapat digunakan perintah di bawah ini,

```
./snort -c snort.conf -b -M WORKSTATIONS
```

Agar snort beroperasi secara langsung setiap kali workstation / server di boot, kita dapat menambahkan ke file `/etc/rc.d/rc.local` perintah di bawah ini

```
/usr/local/bin/snort -d -h 192.168.0.0/24 -c /root/snort/snort.conf -A full -s -D
```

atau

```
/usr/local/bin/snort -d -c /root/snort/snort.conf -A full -s -D
```

dimana `-D` adalah switch yang menseset agar snort bekerja sebagai Daemon (bekerja dibelakang layar).

## TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep logging ?
2. Sebutkan fasilitas logging yang ada di linux !
3. Sebutkan beberapa software yang biasa dipakai untuk melakukan monitoring log di linux.

## PERCOBAAN

1. Siapkan 3 file source
  - o Snort
  - o snortrules-pr
2. Copikan Semua File Tadi Ke `/usr/local/src`
3. Langkah Insallasi Snort

```
# tar -xvzf <snort.....tar.gz> --dir=/usr/local
# ./configure
# make
# make install
```

4. Buat user dan grup snort
  - # groupadd snort
  - # useradd -g snort snort -s /sbin/nologin
5. Unzip snort-rules source file
  - # tar -xvzf <snort-rules-..tar.gz> --dir=/usr/local
  - # cd /usr/local/snort-rules
6. Buat direktori dan kopikan /snort-2.7.0.1 ke /etc/snort
  - # mkdir /etc/snort
  - # mkdir /etc/snort/rules
  - # mkdir /var/log/snort
  - # cd /usr/local/snort-2.6/etc
  - # cp \* /etc/snort
7. Copikan rules dari direktori /rules (hasil unzip snort rules) ke /etc/snort/rules
8. Edit file snort.conf. Ubahlah baris-baris berikut :

```
var HOME_NET 10.252.102.0/24
var EXTERNAL_NET !$HOME_NET
var RULE_PATH /etc/snort/rules
```

9. Manjalankan snort

Menjalankan snort dengan mode sniffer

- a. Bekerjalalah dengan teman anda, salah satu menjalankan snort yang satunya menjalankan aplikasi yang lain.
- b. Jalankan perintah ping dari komputer lain ke komputer snort, buka terminal yang lain dan jalankan nmap.
- c. Jalankan snort dengan menggunakan mode sniffer
  - snort -v
  - #snort -vd
  - #snort -vde
  - #snort -v -d -e

Jelaskan perbedaan hasil dari option di atas.

Menjalankan snort untuk melihat paket dari dan menuju host tertentu :

```
# snort -h 10.252.102.0/24 -d -v host 10.252.102.33
```

Coba lakukan scanning dg nmap dari komputer lain dan lihat apakah terekam oleh snort anda

Menjalankan snort dengan mode logger.

- d. Untuk mempermudah pembacaan masukkan hasil snort ke dalam file, jalankan perintah berikut :
  - snort -dev -l /root/snort-2.7.0.1/log
- e. Untuk membaca file snort berikan option -r pada snort
  - Buka direktori /root/snort-2.7.0.1/log. Pilih log mana yang hendak anda lihat.

- `snort -dev -r <nama-log-file> | more`

Menjalankan snort dengan mode NIDS (Network Intrusion Detection System)

- f. Opsi e, dihilangkan karena kita tidak perlu mengetahui link layer MAC. Opsi v dihilangkan juga

```
snort -d -h 192.168.1.0/24 -l /var/log/snort -c /etc/snort/snort.conf
```

10. Bekerjasamalah dengan rekan anda. Sekarang coba jalankan scanning dari komputer lain dengan nmap menuju komputer yang anda pasang snort. Terlebih dulu jalankan snort dengan mode NIDS, kemudian lakukan scanning dengan perintah :

```
# snort -d -h 192.168.1.0/24 host <no_ip_snort> -l /var/log/snort -c
/etc/snort/snort.conf
#nmap -sS -v <no_ip_snort>
```

11. Lihatlah apakah scan anda terekam oleh snort. Jika iya, copy paste hasil snort pada bagian scanning SYN. Untuk melihat, gunakan perintah :

```
# snort -dev -r <nama-log-file> | more
```

Apakah scanning ini ditandai sebagai alert ? Coba lihat di /var/log/snort

12. Jalankan snort. Buka halaman web. Apakah ini terdeteksi sebagai alert?
13. Sekarang coba ubah rule snort. Buat rule baru yaitu alltcp.rules.

```
alert tcp any any -> any any (msg:"TCP Traffic";sid:9000000;rev:0;)
```

Apa artinya ?

14. Coba lihat snort.conf. Beri tanda # pada semua rule lain kecuali rule anda yaitu : alltcp.rules.
15. Bukalah halaman web, lihatlah apakah ada tanda sebagai alert atau tidak
16. Coba lakukan scanning seperti perintah 11. Lihatlah apakah ada tanda sebagai alert atau tidak
17. Apa yang dapat anda simpulkan dari langkah diatas ? Have fun with snort.

## LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Intrusion Detection System [Snort]

Dasar Teori :

Tugas Pendahuluan :

Daftar Pertanyaan

Berikan kesimpulan hasil praktikum yang anda lakukan.

Download rule terbaru di snort dan bandingkan dengan rule yang lama, apa saja perubahan yang ada !

Jelaskan rule apa saja yang bisa dideteksi oleh snort !

Untuk mempermudah pembacaan data snort dimungkinkan dimasukkan dalam database, carilah artikel tentang konfigurasi snort menggunakan database

Jelaskan juga aplikasi yang bisa dipakai untuk membaca database snort!