|  |  |
| --- | --- |
| **11** | **INTRUSION DETECTION** |
| **SYSTEM (IDS)** |

1. **POKOK BAHASAN**
   1. IDS menggunakan snort pada komputer/server berbasis Linux.
   2. Perintah-perintah snort dan rules pada komputer/server.
2. **TUJUAN**

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

* 1. Mengenalkan pada mahasiswa tentang konsep IDS di linux
  2. Mahasiswa memahami konsep IDS : Snort yang ada di linux
  3. Mahasiswa mampu melakukan konfigurasi dan analisa terhadap aplikasi snort

1. **PERALATAN**
   1. Sistem Operasi Linux Penestrasi Kali dan Server Linux
2. **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 lalulintas 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.

84

1. **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari.
2. **Intrusion Detection mode**, pada mode ini snort akan berfungsi untuk mendeteksiserangan 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 menunjukan 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.

85

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 effisien, 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 menset agar snort bekerja sebagai Daemon (bekerja dibelakang layar).

**E. PERCOBAAN**

1. Lakukan instalasi snort pada server linux:

root@server:~# apt-get install snort

Masukkan range network yang akan dianalisa :

Address range for the local network :

192.168.20.0/24

1. Manjalankan snort
   1. Bekerjalah dengan teman anda, salah satu menjalankan snort yang satunya menjalankan aplikasi yang lain.
   2. Jalankan perintah ping dari komputer lain ke komputer snort, buka terminal

86

yang lain dan jalankan nmap.

c. Jalankan snort dengan menggunakan mode sniffer

root@server:~# snort –v

root@server:~# snort –vd

root@server:~# snort –vde

root@server:~# snort –v –d –e

Ket : Running in packet dump mode

Jelaskan perbedaan hasil dari option di atas.

d. Untuk mempermudah pembacaan masukkan hasil snort ke dalam file, jalankan perintah berikut :

root@server:~# snort –dev –i eth0 –L /var/log/snort/snort.log

Ket : Running in packet logging mode

Akan menghasilkan sebuah file di folder /var/log/snort, lihat dengan perintah :

root@server:~# ls /var/log/snort

* 1. Untuk membaca file snort (misal : snort.log.1234) berikan option –r pada snort

root@server:~# snort -dev -r /var/log/snort/snort.log.1234

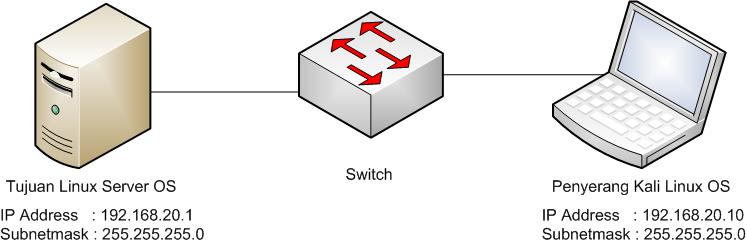
* 1. Jalankan perintah ping dan nmap dari komputer lain ke komputer snort.

1. Menjalankan snort dengan mode NIDS (Network Intrusion Detection System)
   1. Opsi e, dihilangkan karena kita tidak perlu mengetahui link layer MAC. Opsi v dihilangkan juga

root@server:~# snort -d -h 192.168.20.0/24 -l /var/log/snort -c /etc/snort/snort.conf

Ket : Running in IDS mode

1. Sekarang coba jalankan scanning dari komputer lain dengan nmap menuju komputer yang anda pasangi snort. Terlebih dulu jalankan snort dengan mode NIDS, kemudia lakukan scanning dengan perintah :



root@server:~# snort -d -h 192.168.20.0/24 host <no\_ip\_snort> -l /var/log/snort –c /etc/snort/snort.conf

root@kali:~# #nmap -sS -v <no\_ip\_snort>

87

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

root@server:~# snort –dev –r <nama-log-file> | more

Apakah scanning ini ditandai sebagai alert ? Coba lihat di /var/log/snort, gunakan perintah :

root@server:~# vim /var/log/snort/alert

1. **TUGAS**
   1. Lakukan monitoring dengan menggunakan tools tcpdump dari terhadap server.adapun command yang di lakukakan sebagai berikut :

root@server:~# tcpdump –i eth0

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?