Laporan Pendahuluan Praktikum Kemanan Data

Network IDS – Snort

Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

**Network IDS**

*Network IDS (NIDS)* adalah intrussion detection system yang berjalan pada jaringan atau network. Intrussion detection sendiri adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus yang otomatis.

Ada beberapa tipe dasar dari IDS diantaranya 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.

Jenis yang sering digunakan adalah rule-based system. Rules-based system juga memiliki odua pendekatan, yaitu penceganan (preemptory) dan reaksi (reactionary) yang perbedaannya ada di masalah waktu.

Network IDS memiliki tiga jenis IDS, yaitu

* Signature Based
* Anomaly Based
* Hybrid Based

Program signature based yang terkenal adalah Snort, sedangkan program IDS anomaly-based yang sering digunakan adalah BRO-IDS. Hybrid based merupakan gabungan antara keduanya, program yang terkenal adalah suricata

**Snort**

Snort merupakan signature based IDS yang bekerja pada network dengan cara menginspeksi packet yang melewati sensor nya dan akan memeberitahu network administrator jika ada packet yang mencurigakan atau yang menyalahi rule.

Snort memiliki tiga buah mode yaitu,

* **Sniffer Mode**, untuk melihat packet yang lewat di jaringan

Untuk menjalankan snort pada sniffer mode tidaklah sukar, beberapa contoh perintahnya

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**, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari

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

* **Instrusion Detection Mode**, untuk mendeteksi serangan yang dilakukan melalui jaringan komputer

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

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).