SISTEM PENCEGAH PENYUSUPAN

Andika Agus Slameto[1]

Abstraksi

Berkembangnya teknologi sistem informasi yang demikian pesat, sangat membantu pekerjaan-pekerjaan manusia. Di satu sisi manusia menjadi sangat terbantu (dan juga tergantung), tetapi di sisi lain jumlah insiden keamanan sistem informasi meningkat tajam sehingga pada hakekatnya sisi-sisi kehidupan manusia berada dalam posisi yang terancam.

Teknik-teknik pencegahan terhadap serangan pada sistem informasi terus dikembangkan sehingga integritas, availibilitas dan confidentialitas pada sebuah sistem informasi menjadi lebih terjamin. Salah satunya adalah dengan sistem pencegahan penyusupan. Dalam tulisan ini, penulis membangun sebuah sistem pencegahan penyusupan dengan menggunakan Snort IDS dan IPTables Firewall. Sistem ini bekerja dengan membangun sebuah mesin yang membaca parameter IP asal penyerang pada alert yang kemudian memerintahkan firewall untuk memblok akses dari IP penyerang tersebut. Untuk mempermudah manajemen rule digunakan Webmin sedangkan untuk menganalisa log (history serangan) digunakan ACID *(Analysis Console for Intrusion Databases).*

Pengujian dilakukan pada jaringan berteknologi hub dan PC Router dengan sistem operasi Linux Slackware 10 sebagai tempat implementasi sistem ini. Hasil pengujian memberikan hasil yang memuaskan sesuai dengan yang diharapkan, yakni dengan mampunyai sistem untuk memblok (menutup) akses terhadap usaha-usaha penyerangan.

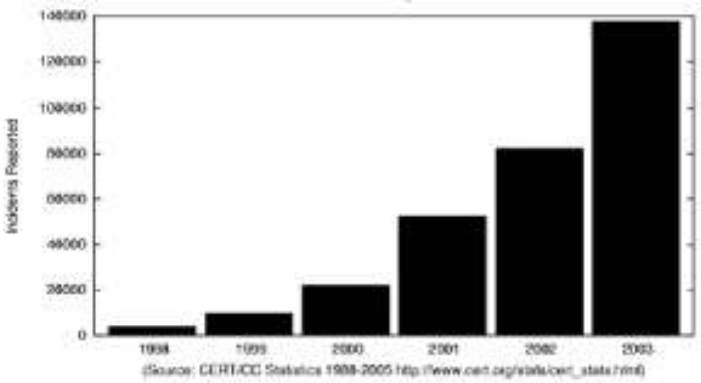
Kata kunci : IDS, IPTables, Firewall, snort, snort rules, webmin, ACID.

[1] Staff Pengajar STMIK AMIKOM Yogyakarta

1. Pendahuluan

Berkembangnya teknologi informasi khususnya jaringan komputer dan layananlayanannya di satu sisi mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan sistem informasi, akan tetapi di sisi lain statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang. Berikut ini statistik insiden keamanan yang dilaporkan oleh CERT (*Community Emergency Response Team*).

.



Gambar 1. Statistik insiden keamanan komputer yang dilaportkan CERT dari 1998-2003

Untuk mencegah insiden keamanan perlu dilakukan langkah-langkah pencegahan baik teknis maupun non teknis.

- Pencegahan dengan non teknis seperti membuat *security policy* yang baik dan terkendali.
- Pencegahan secara teknis dilakukan dengan langkah-langkah *hardening* di sistem operasi, aplikasi, infrastruktur jaringan, implementasi Sistem Pencegahan Penyusupan dan lain sebagainya.

Tujuan dan Ruang Lingkup Pembahasan

Berdasarkan latar belakang di atas, tulisan ini akan membahas pencegahan penyusupan secara teknis yang secara khusus berupa *hardening* sistem dengan IPS berbasis Snort IDS dan IPTables Firewall, yakni sebuah sistem yang mampu melakukan deteksi dan kemudian pencegahan terhadap usaha penyusupan yakni dengan memblok (menutup) akses paket data yang berasal dari penyusup tersebut.

Implementasi sistem pencegahan penyusupan ini dalam sebuah PCRouter dengan yang terkoneksi ke konsentrator berupa HUB dengan kabel UTP sebagai media koneksinya. Dalam tulisan ini tidak dibahas bagaimana implementasi teknis jika sistem pencegahan penyusupan ini diimplementasikan dengan konsentrator berupa switch ataupun jika diimplementasikan pada jaringan dengan traffic yang sangat padat.

Sistem Pencegah Penyusupan

Sistem Pencegahan Penyusupan *(Intrusion Preventing System* atau *IPS)* adalah suatu tools yang digunakan untuk mencegah adanya penyusupan. Ada 2 fungsi dalam IPS yakni kemampuan mendeteksi penyusupan dan kemampuan untuk mencegah akses penyusupan. Kemampuan mendeteksi penyusupan secara umum disebut IDS (*Instrusion Detection System*) dan kemampuan untuk mencegah akses dikenal dengan Firewall.

Komponen Sistem Pencegahan Penyusupan

Sistem pencegahan penyusupan harus dapat mendeteksi dan merespon terhadap penyusupan yakni dengan mengkonfigurasi ulang rule firewall yang ada. Untuk itu komponen-komponen yang harus ada pada sistem pencegahan penyusupan meliputi:

• IDS (*Intrusion Detection System*).

Dilihat dari cara kerja dalam menganalisa apakah paket data dianggap sebagai penyusupan atau bukan, IDS dibagi menjadi 2:

knowledge based atau *misuse detection* dan *behavior based* atau *anomaly based*.

Knowledge-based IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan data-base rule IDS (berisi catatan paket serangan). Jika paket data mempunyai pola yang sama dengan salah satu atau lebih pola di database rule IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di database rule IDS, maka paket data tersebut dianggap bukan serangan.

Sedangkan *behavior based (anomaly)* dapat mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan-kejanggalan pada sistem, atau adanya penyimpangan-penyimpangan dari kondisi normal, sebagai contoh ada penggunaan memori yang melonjak secara terus menerus atau ada koneksi parallel dari 1 buah IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi-kondisi diatas dianggap kejanggalan yang kemudian oleh IDS jenis *anomaly based* dianggap sebagai serangan.

Sedangkan dilihat dari kemampuan mendeteksi penyusupan pada jaringan, IDS dibagi menjadi 2 yakni: *host based* dan *network based*. Host based mampu mendeteksi hanya pada host tempat implementasi IDS, sedangkan *network based IDS* mampu mendeteksi seluruh host yang berada satu jaringan dengan host implementasi IDS tersebut. Tulisan ini secara khusus menggunakan IDS jenis *knowledge based* dan *network based*.

• Packet Filtering Firewall.

Packet Filtering Firewall dapat membatasi akses koneksi berdasarkan parameter-parameter: protokol, IP asal, IP tujuan, port asal, port tu-juan, chain (aliran data) dan code bit sehingga dapat diatur hanya akses yang sesuai dengan policy saja yang dapat mengakses sistem. Packet filtering firewall ini bersifat statik sehingga fungsi untuk membatasi aksespun statik, misalnya akses ke web server (port 80) di-ijinkan oleh policy, maka dari manapun dan apapun aktifitas terhadap webserver diijinkan walaupun merupakan usaha

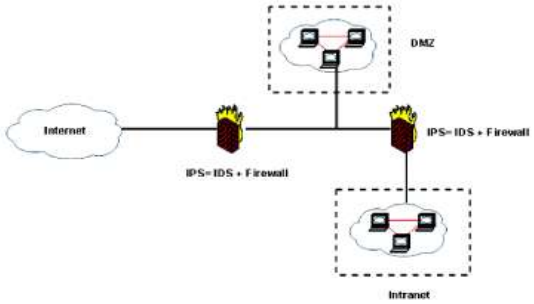
penetrasi oleh craker. Untuk itulah packet filtering firewall tidak dapat mengatasi gangguan yang bersifat dinamik sehingga harus dikombinasikan dengan IDS untuk membentuk sistem hardening yang maksimal.

• Engine Sistem Pencegahan Penyusupan (IDS-Firewall).

Engine ini bertugas untuk membaca alert dari IDS (antara lain berupa jenis serangan dan IP Address penyusup) untuk kemudian memerintahkan firewall untuk memblok akses koneksi ke sistem dari enyusup tersebut.

Dimana diletakkan Sistem Pencegahan Penyusupan?

Sistem pencegahan penyusupan akan maksimal jika diletakkan di router sehingga daerah kerja sistem ini dapat mencakup semua host yang berada dalam 1 jaringan dengan router tempat mengimplementasikan Sistem Pencegahan Penyusupan. Masalah timbul ketika konsentrator menggunakan switch dimana proses penyadapan yang harus dilakukan dalam proses deteksi penyusupan menjadi tidak berfungsi, salah satu cara yang mudah untuk mengatasi masalah ini adalah dengan melakukan spoofing MAC address terhadap host-host yang akan diamati. Posisi sistem pencegahan penyusupan untuk menghasilkan hasil yang maksimal dijelaskan dalam gambar berikut.



Gambar 2. Penempatan sistem pencegahan penyusupan untuk mendapatkan hasil maksimal

Sistem Pencegahan Penyusupan berupa IDS dan Firewall yang diimplementasikan di router/gateway antara internet-DMZ digunakan untuk melindungi server-server yang berada di wilayah DMZ dari kemungkinan serangan dari internet, sedangkan yang diimplentasikan antara jaringan DMZ-intranet digunakan untuk melindungi kemungkinan serangan dari intranet ke wilayah DMZ maupun internet.

Snort IDS dan IPTables Firewall

Seperti dijelaskan sebelumnya, sistem pencegahan penyusupan dibangun dari 2 komponen utama yakni IDS dan Firewall. Dalam pembahasan ini, IDS yang digunakan adalah Snort (www.snort.org) sedangkan firewall yang digunakan adalah Iptables yang merupakan firewall bawaan Linux.

Snort IDS

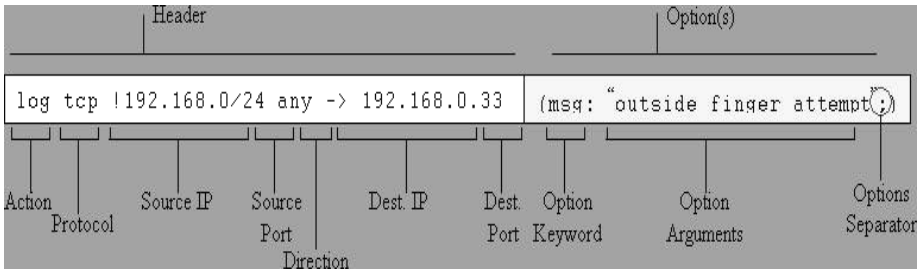
Snort IDS merupakan IDS open source yang secara defacto menjadi standar IDS di industri. Snort dapat didownload di situs www.snort.org. Snort dapat diimplementasikan dalam jaringan yang multiplatform, salah satu kelebi-hannya adalah mampu mengirimkan alert dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui SMB. Snort dapat berkerja dalam 3 mode: *sniffer mode* (penyadap), *packet logger* dan *network intrusion detection mode*. Tentunya mode kerja yang akan digunakan dalam membangun sistem pencegahan penyusupan dalam mode kerja *network intrusion dection.* Penyusupan (*intrusion*) didefinisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect* atau *inappropriate* yang terjadi di jaringan atau di host.

Komponen-komponen Snort IDS meliputi:

• Rule Snort

Rule Snort merupakan database yang berisi pola-pola serangan berupa signature jenis-jenis serangan. Rule Snort IDS ini, harus diup-date secara rutin agar ketika ada suatu teknik serangan yang baru, serangan tersebut dapat terdeteksi. Rule Snort dapat didownload di www.snort.org.

Sebagai contoh rule pada Snort sebagai berikut



Gambar 3. Contoh rule pada snort.

Dari rule-rule seperti di ataslah IDS Snort menentukan apakah sebuah paket data dianggap sebagai penyusupan/serangan atau bukan, paket data dibandingkan dengan rule IDS, jika terdapat dalam rule, maka paket data tersebut dianggap sebagai penyusupan/serangan dan demikian juga sebaliknya jika tidak ada dalam rule maka dianggap bukan penyusupan/serangan.

• Snort Engine

Snort Engine merupakan program yang berjalan sebagai daemon proses yang selalu bekerja untuk membaca paket data dan kemudian mem-bandingkannya dengan rule Snort. Dalam sistem Linux, untuk mende-teksi apakah snort engine dalam keadaan aktif atau tidak dengan melihat prosesnya seperti contoh di bawah ini:

```
[root@localhost rules] # ps  aux   |   grep snort
root  3060 0.0  1.3 9188 820  ?    S  Jun03 0:04   [snort]
```

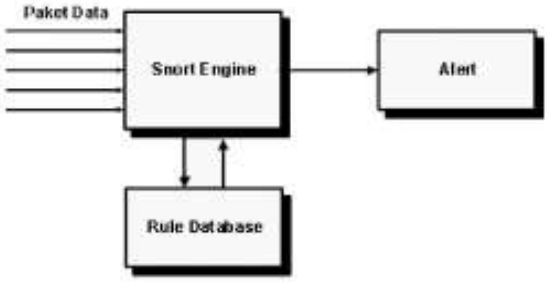
Contoh diatas menunjukkan bahwa snort engine dalam keadaan aktif dengan proses ID 3060 dan dijalankan oleh user "root"

• Alert

Alert merupakan catatan serangan pada deteksi penyusupan. Jika snort engine menghukumi paket data yang lewat sebagai serangan, maka snort engine akan mengirimkan alert berupa log file. Untuk kebutuhan analisa, alert dapat disimpan di dalam database, sebagai contoh ACID (*Analysis Console for Intrusion Databases*) sebagai modul tambahan pada Snort.
Contoh alert sebagai berikut:

[**] [1:499:3] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] 05/09-20:15:14. 895348 10.1.4.113 -> 10.1.3.126 ICMP TTL:128 TOS:0x0 ID:6316 IpLen:20 DgmLen:65528 Type:8 Code:0 ID:512 Seq:3072 ECHO [Xref => http://www.whitehats.com/info/IDS246]

Contoh alert di atas merupakan alert ketika terdapat paket data dalam ukuran besar dari IP Address 10.1.4.113 ke 10.1.3.126 yang dianggap sebagai serangan oleh Snort karena pola paket data tersebut terdapat dalam rule Snort.
Hubungan ketiga komponen IDS dijelaskan dalam gambar berikut:



Gambar 4. Bagian-bagian IDS

IPTables Firewall

IPTables merupakan firewall bawaan Linux. Iptables mampu melakukan filtering dari layer transport sampai layer fisik. Sebagai contoh rule dalam sebuah firewall akan menutup semua koneksi kecuali ke port 80 protokol TCP, atau sebuah rule firewall mendefiniskan bahwa yang dapat melakukan koneksi hanya paket data yang berasal dari MAC address 00-80-48-24-3b-e5. Variabel-variabel dalam Iptables Firewall meliputi:

- Protokol, contoh: tcp, udp, icmp
- Port asal, contoh: port yang lebih besar dari 1023
- Port tujuan, contoh: port 21, 22, 80
- IP asal/Jaringan asal: contoh 202.91.8.112, 202.62.9.216/28
- IP tujuan/Jaringan tujuan: contoh 202.91.8.112, 202.62.9.216/28
- Chain (aliran), contoh: INPUT, OUTPUT, FORWARD (khusus router)
- Code bit (flag), contoh: SYN, ACK.

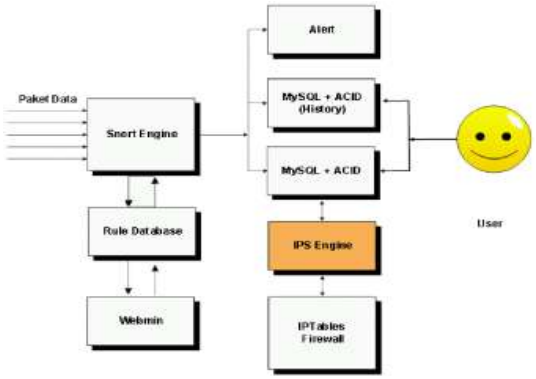
Contoh rule firewall pada Iptables sebagai berikut:
iptables -A FORWARD -p tcp -d 202.91.8.112 —dport 80 –j ACCEPT
iptables -A FORWARD -p tcp -d 202.91.8.112 -j DROP

Rule di atas mendefinisikan bahwa semua paket data dengan protokol tcp dari manapun yang menuju 202.91.8.112 ditolak semua kecuali yang menuju ke port 80.

2. Pembahasan

Perancangan Sistem Pencegahan Penyusupan

Untuk memenuhi kebutuhan fungsional sistem pencegahan penyusupan dibutuhkan modul-modul utama dan modul pendukung. Modul utama berupa: snort engine, rule snort, engine IPS dan firewall. Sedangkan modul pendukung berupa: ACID (manajemen event) dan Webmin (manajemen rule). Target implementasi IPS di sistem Linux Slackware 10. Diagram blok sistem pencegahan penyusupan yang dirancang sebagai berikut.



Gambar 5. Blok diagram Sistem Pencegahan Penyusupan

Rule Snort

Modul ini menyediakan rule-rule berupa pattern jenis serangan. Rule ini berupa file text yang disusun dengan aturan tertentu.

Snort Engine

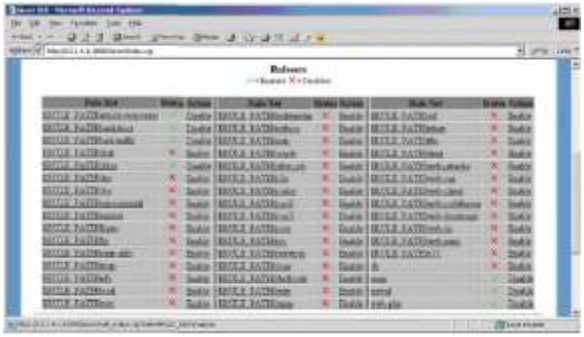
Modul ini berfungsi untuk membaca paket data dan membandingkannya dengan rule database, jika paket data dihukumi sebagai penyusupan/serangan, maka Snort engine akan menuliskannya ke alert (berbentuk file log) dan ke database (yang digunakan dalam eksperimen ini adalah database MySQL).

Alert

Bagian ini merupakan catatan serangan pada sebuah file log.

Webmin

Webmin (http://www.webmin.com) yang telah ditambahkan module snort rule (http://msbnetworks.com/snort/) digunakan untuk mengelola rule. Rule mana saja yang akan di menable dan disable dapat diatur melalui Webmin, bahkan dapat digunakan untuk menambahkan rule-rule secara manual dengan editor berbasis web. Berikut contoh tampilan Webmin untuk mengelola rule Snort.



Gambar 6. Webmin dengan plugin snort digunakan untuk mengelola rule

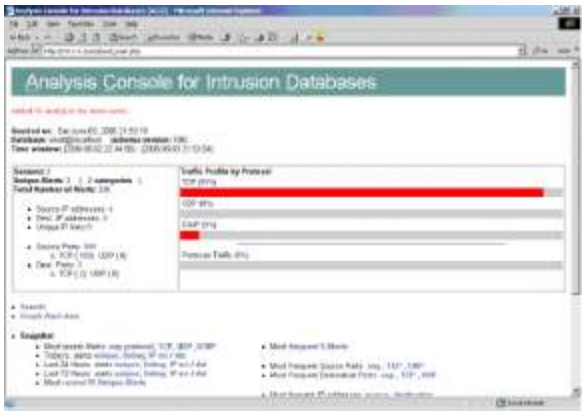
ACID (Analysis Console for Intrusion Databases)

ACID (http://www.cert.org/kb/acid) digunakan untuk mengelola data-data security event, keuntungan menggunakan ACID diantaranya:

- Log-log yang tadinya susah dibaca menjadi mudah di baca.
- Data-data dapat dicari dan difilter sesuai dengan kriteria tertentu.
- Managing Large Alert Databases (Deleting and Archiving).

Untuk kasus-kasus tertentu dapat merujuk alert pada situs database security seperti Securityfocus, CVE, arachNIDS.

Berikut contoh tampilan ACID.



Gambar 7. ACID digunakan untuk mengelola *security event*

ACID (Analysis Console for Intrusion Databases) History

ACID history ini digunakan untuk menganalisa catatan-catatan IDS. Database dalam history ini tidak dihapus karena bersifat seperti arsip-berbeda dengan database pada ACID yang akan dihapus catatan serangannya jika pengelola IPS ini berkehendak untuk membuka akses bagi IP address yang pernah ditutupnya.

Firewall

Firewall digunakan untuk membuka dan menutup akses sesuai dengan rule yang dibuat, dalam hal ini rule akan dinamis sesuai dengan kondisi yang dideteksi oleh IDS. Firewall yang digunakan dalam eksperimen ini adalah Iptables yang merupakan firewall bawaan Linux.

IPS Engine

IPS engine merupakan sistem yang akan membaca alert kemudian memerintahkan firewall untuk menutup akses paket data dari penyerang. Cara kerja IPS engine digambarkan dalam flowchart berikut ini:

Gambar 8. Flowchart IPS engine

IPS akan menutup akses bagi penyerang ketika aktivitas tersebut terdeteksi oleh IDS. Dalam eksperimen ini, proses pembacaan *alert* dan *update rule* pada firewall dilakukan secara periodik dengan meletakkan program IPS engine (yang ditulis dalam bahasa PHP) di crontab (*scheduling task*). Jadi, ketika terjadi usaha penyusupan dan terdeteksi oleh IDS, maka IPS akan memerintahkan firewall untuk menutup akses dari IP address penyerang, adapun jika pada waktu yang lain pengelola IPS akan membuka IP address. IP address yang telah melakukan penyerangan, hal ini dapat dilakukan dengan menghapus isi alert pada serangan dari IP yang dimaksud pada database ACID.

Pengujian

Untuk menguji rancangan sistem pencegahan penyusupan dengan cara melancarkan paket serangan ke sistem yang dilindungi oleh IPS.

Sebagai contoh disini IPS diimplementasikan pada jaringan router yang menghubungkan jaringan intranet dan DMZ. Pada pengujian ini dikirimkan paket ICMP dalam ukuran besar sehingga dikategorikan oleh IDS sebagai DOS attack (*denial of service*).
Berikut contoh pengujian yang dilakukan melalui client di jaringan internal:

```
ping 202.91.8.112  -l   10000  -t
Pinging 202.91.8.112 with  10000 bytes of  data:
Reply from 202.91.8.112:bytes=10000 time=10ms TTL=63
Reply from 202.91.8.112:bytes=10000 time=10ms TTL=63
Reply from 202.91.8.112:bytes=10000 time=10ms TTL=63
Ping statistics for 202.91.8.112:
Packets:Sent=3,Received=3,Lost=0(0Approximate
round trip times  in milli-seconds:
Minimum = 0ms,   Maximum =  10ms,  Average = 3ms
```

DOS attack ini akan segera terdeteksi oleh snort engine yang kemudian snort engine akan mengirimkan alert ke alert log, MySQL ACID dan MySQL ACID history. IPS engine membaca alert pada ACID MySQL dan kemudian memerintahkan firewall untuk mengupdate rulenya dengan menambahkan rule untuk memblok akses dari IP penyerang yang terdeteksi. Pengamatan eksperimen ini dilakukan pada 2 tempat: di client tempat melancarkan serangan dan di sistem IPS.

• *Pengamatan di client penyerang*

Pengamatan dilakukan dengan cara melakukan pengiriman paket ICMP dengan perintah ping ke komputer target seperti berikut ini:

```
ping 202.91.8.112 -t Pinging 202.91.8.112 with 32 bytes of  data:
Reply from 202.91.8.112:bytes=32 time<10ms TTL=63
Reply from 202.91.8.112:bytes=32 time<10ms TTL=63
Reply from 202.91.8.112:bytes=32 time<10ms TTL=63
Request timed out.
```

Request timed out.
Request timed out.
Ping statistics for 202.91.8.112:
Packets: Sent = 6, Received =3, Lost =35 (50Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Dari pengamatan di atas terlihat bahwasanya IPS telah bekerja dengan baik, hal ini ditunjukkan dengan tertutupnya akses ke komputer target serangan dengan munculnya pesan "*Request Time Out*" yang sebelumnya "*Repply*".

• *Pengamatan di Sistem Pencegahan*

Penyusupan Adapun pengamatan di sistem pencegahan penyusupan dilakukan dengan mengamati rule firewall yang telah berubah, yakni ips engine memasukkan IP address penyerang sebagai sebuah rule dimana akses dari komputer tersebut harus diblok (tidak diijinkan). Berikut pengamatan di sistem:

Chain INPUT (policy ACCEPT) target prot opt source destination
Chain FORWARD (policy ACCEPT) target prot opt source destination DROP all — 10.1.4.161 anywhere
Chain OUTPUT (policy ACCEPT) target prot opt source destination

Dari pengamatan di dua sisi, sisi penyerang dan sisi sistem pencegahan penyusupan, dapat disimpulkan bahwa fungsional sistem ini telah berjalan dengan yang diharapkan. Serangan-serangan jenis yang lain juga akan bernasib sama yakni diblok, hal ini tentunya tergantung dari ketelitian dan kelengkapan rule snort. Rule snort begitu lengkap sehingga mampu mende-teksi banyak jenis serangan. Berikut contoh rule Snort.

attack-responses.rules, dos.rules, local.rules, oracle.rules, scan.rules, web-cgi.rules, backdoor.rules, experimental.rules, Makefile other-

ids.rules, shellcode.rules, web-client.rules, bad-traffic.rules, exploit.rules, Makefile.am p2p.rules, smtp.rules, web-coldfusion.rules, chat.rules, finger.rules, Makefile.in policy.rules, snmp.rules, web-frontpage.rules, db.config ftp.rules, misc.rules, pop2.rules, sql.rules, web-iis.rules, db.timestamp icmp-info.rules, multimedia.rules, pop3.rules, telnet.rules, web-misc.rules, ddos.rules, icmp.rules, mysql.rules, porn.rules, tftp.rules, web-php.rules, deleted.rules, imap.rules, netbios.rules, rpc.rules, virus.rules, x11.rules, dns.rules, info.rules, nntp.rules, rservices.rules, webattacks.rules.

3. Penutup

Sebuah sistem pencegahan penyusupan haruslah mempunyai fungsi: deteksi (IDS) dan memberikan respon berupa update rule firewall, untuk memper-mudah pengelolaan IPS dibutuhkan module-module tambahan selain IDS dan Firewall.

Kesimpulan

Secara keseluruhan eksperimen ini, dapat disimpulkan bahwa:

- Serangan/penyusupan dapat dicegah dengan implementasi Sistem Pencegahan Penyusupan.
- Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam rule IDS atau tidak. Oleh karena itu, pengelola IDS harus secara rutin mengupdate rule terbaru.
- Implementasi IPS pada jaringan berbasis switch memerlukan penanganan khusus (oleh karena itu, karena keterbatasan waktu,dalam eksperimen ini digunakan hub sebagai konsentratornya).
- Untuk mempermudah pengelolaan rule perlu user interface (*front end*) yang lebih "manusiawi" seperti Webmin yang ditambahkan plugin snort rule.
- Untuk mempermudah analisa terhadap catatan-catatan IDS *(security event)* perlu ditambahkan module tambahan seperti ACID.

Saran

Sistem yang kami bangun masih terdapat banyak kekurangan, karena keterbatasan waktu dan sarana. Saran-saran yang dapat

diberikan bagi yang ingin mendalami lebih lanjut sistem ini antara lain:

- Update rule pada firewall seharusnya dalam bentuk daemon proses sehingga proses bekerja secara realtime, yang kami bangun masih dalam bentuk script yang dieksekusi secara periodik (1 menit sekali).
- Implementasi IPS dalam jaringan yang menggunakan switch perlu penambahan module MAC *address spoofing.*
- Manajemen rule sebaiknya dibuat tersendiri, dapat dilakukan dengan pemrograman aplikasi berbasis web, bukan diletakkan di Webmin, dikarenakan Webmin merupakan administrasi secara keseluruhan sistem Linux dan hanya dilindungi dengan format utentification sehingga jika suatu saat Webmin dapat dikuasai, maka keseluruhan sistem akan dikuasasi juga.
- Perlu diuji pada jaringan dengan traffic yang sangat tinggi sehingga kinerja IDS dapat terukur tidak hanya fungsionalitasnya saja yang mampu mendeteksi penyusupan .

4. Daftar Pustaka

Avudz Syah Putra, "*Monitoring Serangan Hacker Ke Jaringan Dengan Snort*", http://www.jasakom.com/haking/avudz.html, 17 Juni 2003.

Kerry J. Cox & Christopher Gerg, "*Managing Security With SNORT and IDS Tools"*, O'RIELLY, July 2003.

Martin Roesch, *"Snort – Lightweight Intrusion Detection for Networks*",http://www.clark.net/~roesch/lisapaper.txt, November, 2003.

Nalneesh Gaur, *"Snort: Planning IDS for Your Enterprise"*, http://www.linuxjournal.com, July, 2004.

Puji Hartono, "*Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall"*, http://budi.insan.co.id, 2005

Rebecca Bace, "*An Introduction To Instrussion Detection And Assesment*", http://www.SecurityFocus.com, 2004.