ANALISIS SISTEM PENDETEKSIAN DAN PENCEGAHAN PENYUSUP PADA JARINGAN KOMPUTER DENGAN MENGGUNAKAN SNORT DAN *FIREWALL* PADA SISTEM OPERASI DISTRIBUSI *LINUX IPCOP FIREWALL*

Kundang Karsono Juman
Fasilkom - Universitas INDONUSA Esa Unggul, Jakarta
Jl. Arjuna Utara Tol Tomang Kebon Jeruk, Jakarta 11510
Kundang.karsono@indonusa.ac.id

Abstract

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses,trojan horses, and worms). An IDS can be composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

Keywords: *Acess Open Data, Intruder, Intrusion Detection System (IDS)*

Pendahuluan

Dalam era teknologi informasi saat ini, hampir seluruh informasi yang penting bagi suatu institusi seperti organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintah maupun individiual (pribadi) dapat diakses oleh para penggunanya dari mana dan kapan saja. Keterbukaan akses tersebut memunculkan berbagai masalah baru antara lain adalah pemeliharaan validitas dan integritas data atau informasi tersebut, jaminan ketersediaan informasi bagi pengguna yang berhak, pencegahan akses informasi dari yang tidak berhak serta pencegahan akses sistem dari yang tidak berhak.

Sistem pertahanan terhadap aktivitas gangguan saat ini umumnya dilakukan secara manual oleh para *administrator*. Hal ini mengakibatkan integritras sistem bergantung pada keterasediaan dan kecepatan *administrator* dalam me-*respons* gangguan. Apabila gangguan tersebut berhasil membuat suatu jaringan mengalami malfungsi, *administrator* tidak dapat lagi melakukan pemulihan sistem dengan cepat.

Oleh karena itu dibutuhkan sistem yang dapat menaggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan. Salah satu cara yang dapat digunakan untuk menanggulangi atau mengatasi hal tersebut adalah dengan menggunakan *Intrusion Detection System* (IDS). IDS adalah sistem pendeteksian dan pencegahan penyusup dengan menggunakan suatu perangkat lunak (*software*) atau perangkat keras (*hardware*) yang bekerja secara otomatis untuk memonitor keadaan pada jaringan

komputer dan dapat menganalisis masalah keamanan jaringan

Jaringan Komputer

Sebuah jaringan komputer biasanya terdiri dari dua buah atau lebih komputer yang saling berhubungan. Keadaan ini didesain untuk memfasilitasi ide *sharing resources* seperti *printer, CD ROM, file,* dll. (Tanenbaum, Andrew S, 2007). Jaringan komputer juga memungkinkan terjadinya komunikasi secara elektronik. Hubungan antara komputer yang satu dengan komputer yang lainnya untuk membentuk suatu jaringan dimungkinkan dengan menggunakan suatu media baik itu berupa kabel maupun media lainnya. Secara umum terdapat 4 jenis jaringan /*network* yaitu :

1. *Local Area Network* (LAN)
2. *Wide Area Network* (WAN)
3. *Metropolitan Area Network* (MAN)
4. *Inter Network.*

Pengertian *Security System*

Security sistem merupakan sebuah konsep dimana suatu sistem komputer dilindungi sedemikian rupa untuk menghindari gangguan-gangguan *internal* maupun *eksternal* yang bersifat destruktif (baik pada sistem operasi maupun sistem jaringan) yang dapat mengakibatkan sistem berjalan lambat, mengurangi *bandwidth,* kebocoran data, dan bahkan menghancurkan perangkat keras.

Aspek Dasar Keamanan Sistem

Dalam perencanaan keamanan sistem yang baik hendaknya memperhatikan 4 aspek dasar keamanan sistem yang sangat fundamental bagi jaringan. Keempat aspek tersebut adalah *Privacy/Confidentialy, Integrity, Authentication, dan Availability.* (Agus Fanar Syukuri, 2003)

Security Sistem Jaringan

Security sistem jaringan merrupakan suatu konsep perlindungan sistem jaringan yang dirancang sedemikian rupa sehingga dapat melindungi sistem jaringan dari gangguan baik dari *internal* maupun *eksternal* sistem jaringan (Agus Fanar, 2007). Perlindungan ini mencakup perlindungan dari gangguan yang bersifat destruktif yang dapat mengakibatkan melambatnya proses, pengurangan *bandwidth*, kebocoran data, dan bahkan penghancuran perangkat keras.

Pengenalan *Firewall*

Dalam terminologi *internet*, istilah *firewall* didefinisikan sebagai sebuah titik diantara dua/lebih jaringan dimana semua lalu lintas (*traffic*) harus melaluinya (*chooke point*), trafik dapat dikendalikan oleh dan diautentifikasi melalui sautu perangkat, dan seluruh *traffic* selalu dalam kondisi tercatat (*logged*). Dengan kata lain, *firewall* adalah penghalang (*barrier*) antara "kita" dan "mereka" dengan nilai yang di atur (*arbitrary*). (Chesswick, W & Bellovin, S., 1994)

Fungsi *Firewall*

Terdapat 4 fungsi *firewall* dalam keamanan sistem jaringan dimana 3 poin pertama masih dalam konteks dimana komunikasi antara *server* dan *client* secara langsung. (Ahmad Muammar, 2004). Keempat fungsi tersebut adalah:

1. *Static packet filtering*
   Firewall mem-*filter* paket – paket berupa:
   - IP address
   - Port
   - Flag
2. *Dynamic packet filtering*
   Pada *dynamic packet filtering firewall* akan membuat suatu *list* koneksi yang mencatat *log-log* yang nantinya akan diperiksa untuk memvalidasi hak akses. Kelemahan sistem ini adalah *user* harus selalu melakukan *login* untuk membuka sesi padahal ketika *login user* harus memasukan *username* dan *password*. Untuk menanggulanginya digunakan poin berikut (poin 3).
3. *State Full Filtering*
   Untuk menanggulangi kelemahan pada *dynamic packet filtering* maka *firewall* tidak membuat *list* koneksi melainkan *list* aplikasi.
4. *Proxy*
   Pada fungsi terakhir ini komunikasi antara *server* dan *client* tidak dilakukan secara langsung tetapi melewati *proxy server*.

Intrusion Detection System

Intrusion Detection system (IDS) adalah sistem pencegahan penyusup dengan menggunakan suatu perangkat lunak (*software*) atau perangkat keras (*hardware*) yang bekerja secara otomatis untuk memonitor keadaan pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan. (Dony Ariyus, 2007).

Intrusion Detection system (IDS) dapat didefinisikan sebagai *tools*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaingan komputer.

Kemampuan dari IDS adalah memberikan peringatan kepada administrator server saat terjadinya sebuah aktivitas tertentu yang tidak diinginkan *administrator* sebagai penanggung jawab sebuah sistem, selain memberikan peringatan, IDS juga mampu melacak aktivitas yang merugikan sebuah sistem. Suatu IDS dapat melakukan pengamatan (*monitorring*) terhadap paket – paket yang melawati jaringan dan berusaha menemukan apakah terdapat paket – paket yang berisi aktivitas – aktivitas mencuruigakan.

Fungsi *Intrusion Detection system* (IDS)

Intrusion Detection system (IDS) berfungsi melakukan pengamatan (*monitoring*) kegiatan – kegiatan yang tidak lazim pada jaringan sehingga awal dari langkah para penyerang bisa diketahui. Dengan demikian administrator bisa melakukan tindakan pencegahan dan bersiap atas kemungkinan yang akan terjadi. (Dony Ariyus, 2007).

Ada beberapa alasan untuk memperoleh dan menggunakan *intrusion detection system*, diantaranya adalah :

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang – orang yang tidak bertanggung jawab.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem yang umum dipakai, seperti *firewall*.
3. Mendeteksi serangan awal (biasanya *network probe* dan aktifitas *doorknob ratting*). Penyerang yang akan menyerang biasanya melakukan langkah – langkah awal yang dapat diketahui oleh IDS.
4. Mengamankan file yang keluar dari jaringan.
5. Sebagai pengendali untuk *security design* dan *administrator*, terutama bagi perusahaan yang besar.
6. Menyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan diagnosis, *recovery* dan mengkoreksi faktor – faktor penyebab serangan.

Intrusion Prevention System (IPS)

Intrusion Prvention System (IPS) merupakan bentuk pengembangan dari IDS. IPS mampu mencegah serangan yang datang dengan bantuan *administrator* secara minimal atau bahkan tidak sama sekali. (Dony Ariyus, 2007). Secara logika IPS akan menghalangi suatu serangan sebelum terjadi eksekusi pada memori, metode lain dari IPS adalah dengan membandingkan *file checksum* yang tidak semestinya dengan *file checksum* yang semestinya mendapatkan izin untuk di eksekusi dan juga bisa menginterupsi sistem *call*. Secara khusus IPS memiliki empat komponen utama :

- Normalisasi *traffic*
- *Service Scanner*
- *Detection engine*
- *Traffic Shaper*

Snort

Snort adalah *Intrusion Detection System* jaringan *open source* yang mampu menjalankan analisis *real-time* dan paket *logging* pada IP *network.* (Tom Thomas, 2004)

Snort dapat menjalankan analisis protokol, *content searching* atau *maching*, dan dapat digunakan untuk mendeteksi berbagai serangan dan penyusupan.

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup maupun menganalisa paket yang melintasi jaringan computer secar *realtime traffic* dan *logging* ke dalam *database* serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort dapat digunakan pada *platform* sistem operasi Linux, BSD, Solaris, Windows dan sistem operasi lainnya.

Snort merupakan suatu *intrusion detectiom system* yang dipakai oleh banyak orang. www.snort.org menyediakan layanan untuk *update rule* dan *signature*, *mailing list*, forum diskusi, komunitas *project* dan layanan lain yang memudahkan user untuk mendapatkan informasi.

Snort dapat dioperasikan dengan tiga mode:

1. *packet sniffer:* untuk melihat paket yang lewat di jaringan.
2. *packet logger:* untuk mencatat semua paket yang lewat di jaringan untuk dianalisis di kemudian hari.
3. *NIDS, deteksi pemyusup pada jaringan:* pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

Linux

Saat ini ada tujuh distribusi Linux paling terkenal, yaitu :

1. *RedHat Linux, distributor* paling populer di AS dan salah satu yang paling mudah digunakan.
2. *Mandrake Linux, distributor* yang menambahkan *update* dan *patch* untuk *RedHat Linux*.
3. *Caldera Open Linux*, distibrusi Linux dengan instalasi dan lingkungan pengguna berbasis grafis yang bagus.
4. *Suse Linux*, distribusi Linux paling populer di Eropa yang juga menyediakan perangkat instalasi dan panduan berbahasa Indonesia.
5. *Slackware Linux*.
6. *Debian GNU/Linux.*
7. *TurboLinux*, distribusi Linux paling populer di Asia yang menyediakan dukungan untuk set karakter khusus Asia.

IPCop *Firewall*

IPcop *Firewall* adalah distro Linux untuk aplikasi *firewall* yang menyediakan kemudahan dalam me-*manage* (*simple-to-manage*) berbasis *hardware* PC. IPCop dibangun berdasarkan kerangka Linux *netfilter*. Pada dasarnya IPCop merupakan pengembangan dari *SmoothWall Linux firewall*, selanjutnya project ini berkembang secara signifikan dan berdiri sendiri. IPCop sangat mudah dalam mengatur *security update* yang diperlukan. Selain itu, IPCop dapat diimplementasikan oleh pengguna yang baru belajar linux sekalipun.

Dengan penerapan teknologi yang ada bersama teknologi baru beorientasi pada *'secure programmin*g', IPCop dapat digunakan sseperti distribusi Linux lainnya bagi mereka yang serius ingin menjaga keamanan komputer dan jaringannya.

Beberapa hal berikut dapat dijadikan pertimbangan dalam kita memilih IPCop *Firewall* sebagai aplikasi *firewall* ;

1. Kemudahan instalasi dan *free license under GPL.*
2. Kemudahan dalam mengkonfigurasi.
3. Banyaknya *support* dari kalangan komunitas maupun perseorangan.
4. *Add ons* sebagai tambahan *tools* yang disesuaikan dengan kebutuhan.
5. *Autocheck* untuk *Security Update*.
6. Kebutuhan *hardware PC* yang disesuaikan dengan kondisi *network* kita.
7. Berfungsi sebagai *Proxy Server.*

Pembahasan

Pada analisis ini, pemilihan tipe IDS dimaksudkan untuk memilih tipe apa yang sebaiknya digunakan untuk kegiatan *monitoring* pada jaringan komputer. Pemilihan dimaksudkan untuk keamanan dalam melakukan implementasi serta fungsionalitasnya sebagai pendeteksi penyusup dalam jaringan komputer. Pada sistem pendeteksian penyusup yang berdasarkan sumber infomasinya terdapat dua jenis tipe IDS, yaitu :

1. HIDS *(Host Intrusion Detection System)*
   Bekerja pada *host* yang akan dilindungi. IDS dengan tipe ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada host tersebut.
2. NIDS *(Network Intrusion Detection System)*
   IDS tipe ini akan mengumpulkan paket – paket data yang terdapat pada jaringan dan kemudian menganalisisnya serta menentukan apakah paket – paket itu berupa suatu

paket yang normal atau suatu serangan atau berupa aktifitas yang mencurigakan.

Berikut adalah tabel perbandingan dari kedua jenis tipe sistem pendeteksian penyusup berdasarkan sumber informasinya.

Tabel 1
Perbandingan HIDS dan NIDS

Keterangan	HIDS	NIDS
Sumber Informasi	Dari data yang dihasilkan oleh sistem pada sebuah komputer yang diamati.	dari paket – paket jaringan komputer yang diamati.
Monitoring	Memonitor aktifitas sistem tertentu	Memonitor aktifitas jaringan komputer.
Sistem Operasi	Bergantung Pada Sistem Operasi	tidak tergantung pada sistem operasi.
Respons Deteksi	Secara *realtime*	*Secara realtime*
Cakupan Sumber Informasi	Hanya Pada *Host* itu sendiri.	Multi – *host*
Konfigurasi	Rumit (konfigurasi untuk setiap host)	Mudah (konfigurasi pada pusat IDS)
Tingkat keamanan IDS	beresiko (*Host* merupakan target)	Tidak beresiko (*host* bukan target)
Deteksi serangan	Lebih baik mendeteksi serangan yang berasal dari dalam jaringan.	Lebih baik untuk mendeteksi serangan yang berasal dari luar jaringan
Kinerja	Memverifikasi sukses atau gagalnya suatu serangan	Mendeteksi usaha dari serangan yang gagal
Cost	Lebih mahal untuk diimplementasikan	Lebih murah untuk diimplementasikan

Sumber: Hasil Olahan Data

Berdasarkan tabel 1, penggunaan tipe IDS yang dimaksudkan untuk melakukan monitoring pada jaringan komputer yang baik untuk analisis ini adalah NIDS (*Network Intrusion Detection System*). Dikarenakan cakupan yang luas yang dapat memantau jaringan komputer yang ada, tingkat keamanan yang dimiliki NIDS yang tidak beresiko dikarenakan sistem yang digunakan untuk melakukan *monitoring* bukan merupakan sistem yang menjadi target penyusup, sehingga sistem pendeteksian dapat bekerja secara optimal serta biaya pengimplementasiannya yang lebih murah dibandingkan dengan HIDS.

Pemilihan Sistem Operasi

Pada analisis ini, pemilihan sistem operasi dimaksudkan untuk mempermudah dalam pengimplementasian sistem pendeteksian penyusup pada jaringan komputer serta sebagai pertimbangan keamanan dari sistem penyusup itu sendiri. Sistem operasi yang digunakan untuk melakukan perbandingan adalah :

1. Windows *XP Profesional Service Pack 2*
2. Distribusi Linux *Red Hat 9.0*
3. Distribusi Linux IPCop *Firewall* Versi 1.4.18

Berikut adalah tabel perbandingan antara sistem operasi yang digunakan untuk pengimplementasian sistem pendeteksian penyusup pada jaringan komputer (dengan spesifikasi hardisk 4 Gb memori 256Mb menggunakan VMware 6.0). (Tabel 2).

Pada sistem operasi Windows XP dan Red Hat tingkat kesulitan dalam melakukan konfigurasi sangat tinggi dikarenakan banyaknya aplikasi yang harus dikonfigurasikan. Seperti snort.conf pada aplikasi snort, penyesuaian database pada mysql dan SQL server, penggabungan konfigursi untuk PHP, Adodb dan Apache. Serta konfigurasi ACID dan BASE agar terhubung ke sistem database masing – masing sistem operasi. Kesulitan yang paling besar adalah kesulitan dalam melakukan penggabungan snort dengan komponen – komponen tambahan seperti BASE, ACID, PHPlot, Zlib dll, dikarenakan tidak semua versi snort sesuai dengan komponen yang digunakan untuk mengembangkan IDS lebih lanjut.

Berdasarkan tabel 2, sistem operasi yang digunakan untuk analisis ini adalah IPcop *Firewall* dikarenakan kemudahan instalasi, yang untuk orang awam memerlukan waktu kurang dari 20 menit, kemudian *space hardisk* yang digunakan kurang dari 300 Mb (tanpa penggunaan aplikasi tambahan seperti *addons*) serta kemudahan konfigurasi untuk sistem pendeteksi penyusup dan tingkat kea-

manan dari IPcop yang merupakan *secure programming*. Serta tidak perlu lagi melakukan konfigurasi dan penggabungan komponen – komponen pendukung snort karena pada Ipcop *firewall* semua komponen untuk melakukan monitoring sudak terkonfigurasi dengan baik.

Tabel 2
Perbandingan System Operasi untuk Implementasi

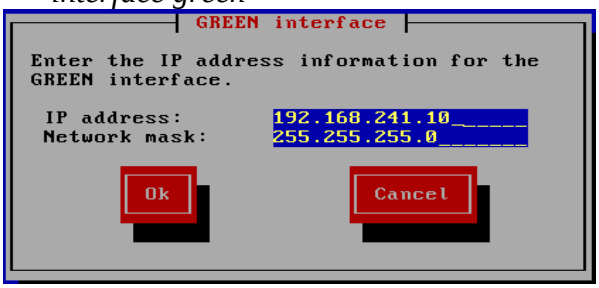
Keterangan	XP	Red Hat 9.0	IPcop *Firewall*
Waktu Instalasi	40 – 50 menit	50 – 60 menit	< 20 menit
Space Hardisk	> 700 Mb	> 1,1 Gb	< 300 Mb
Sofware Pendukung IDS	WinPcap, Snort, SQL server, PHP, Apache, Adodb, PHPlot, BASE	Snort, MySQL, apache, PHP, ADODB, ACID, Zlib, LibPcap	Snort, Apache, Cron, LibPcap
Konfigurasi	Sulit	Sulit	Mudah
keberhasilan konfigurasi	Rendah	Rendah	Tinggi
Keamanan	tidak ditunjukan untuk keamanan jaringan	tidak ditunjukan untuk keamanan jaringan	*Secure Programming*

Sumber: Hasil Olahan Data

Instalasi IPCop *Firewall*

Ipcop Firewall pada penulisan ini menggunakan tiga NIC, satu berfungsi sebagai *adapter local area network*, yang lain berfungsi sebagai koneksi keluar jaringan. Berikut adalah langkah – langkah instalasi *Ipcop Firewall* :

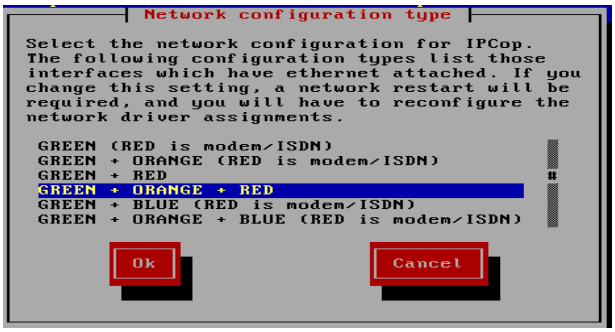
- *Booting* dengan CD *bootable* melalui CD Rom
- Sesaat akan muncul *command pro*mpt dan muncul tampilan selamat datang dari *Ipcop Firewall* tekan *ENTER*
- Pilih bahasa yang akan digunakan pilih *english*.
- Pilih media instalasi konfirmasi partisi *hardisk* pilih OK.
- Pilihan untuk melakukan *back up*, pilih *skip*.
- Masukan *IP address* untuk *network interface green*



Sumber: Hasil Olahan Data

Gambar 1
green interface

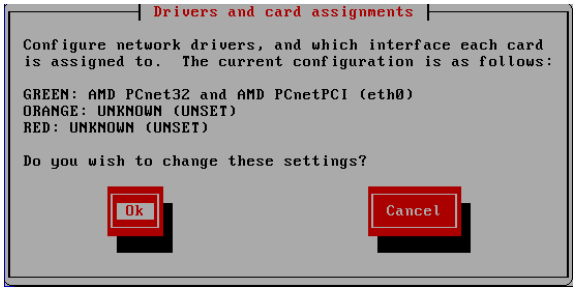
- Konfirmasi instalasi tekan OK.
- Pilihan *keyboard* mapping pilih US.
- Pilihan *Time Zone* pilih Asia/Jakarta.
- Menu pemberian nama untuk *hostname*, *domain name*
- Menu konfigurasi ISDN
- Setelah terkonfigurasi maka akan muncul tampilan *network configuration menu*. Pilih *network configuration type*. Pilih *green*, *orange* dan *red.*



Sumber: Hasil Olahan Data

Gambar 2
Network Configuration Type

- Dikarenakan pada instalasi *Ipcop firewall* menggunakan tiga buah NIC, maka setiap NIC harus di konfigurasi agar sesuai dengan setiap *network interface* yang ada. Untuk menyesuaikan setiap NIC pilih pilihan *Driver and Card assignments*. Dikarenakan *network interface green* sudah maka pada sesi sebelumnya maka pada menu ini hanya melakukan penyesuaian untuk *network interface orange* dan *red* saja.



Sumber: Hasil Olahan Data

Gambar 3

Drivers and Card Assignments

- Setiap *network interface* harus memiliki *ip address*, untuk memberikan *ip address* pilih pilihan *Address Settings*. Dikarenakan *network interface green* sudah maka pada sesi sebelumnya maka pada menu ini hanya melakukan pengalamatan untuk *network interface orange* dan *red* saja.

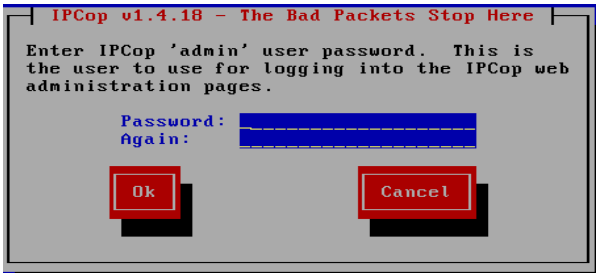
Sumber: Hasil Olahan Data

Gambar 4

address settings

- Pilih menu *DNS and Gateway* settings untuk melakukan konfigurasi *primary* dan *secondary domain name server* dan *default gateway*.
- Pilih menu *DHCP Server Configuration* untuk melakukan konfigurasi *dynamic host control protocol*
- Setelah semua terkonfigurasi dengan baik maka pilih *done* untuk menyelesaikan konfigurasi.
- Masukan password minimal enam *character* untuk root
- Masukan password untuk admin yang akan diggunakan untuk login

Pada autentikasi pada tampilan *web Ipcop* dengan menggunakan user name admin. Pastikan password ini memiliki tingkat keamanan yang cukup tinggi.



Sumber: Hasil Olahan Data

Gambar 5

Password untuk *admin*

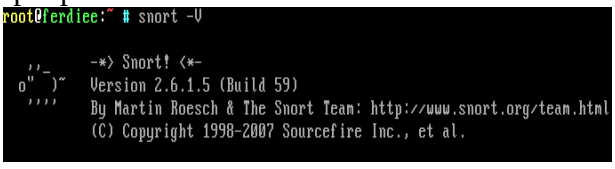
- Masukkan *password* untuk *back up key*. Password ini digunakan untuk menyimpan konfigurasi *Ipcop firewall* serta menyimpan *log – log* yang telah tersimpan pada sistem *Ipcop firewall*.
- Secara otomatis *Ipcop* akan melakukan *reboot*.

Selesai melakukan *reboot Ipcop Firewall* akan masuk ke dalam sistem utama dimana semua konfigurasi dapat dapat di *setting* kembali.

- Setelah *reboot* sistem *Ipcop firewall* akan meminta *username* dan *password* untuk bisa masuk ke dalam sistem. Gunakan *username root* serta *password* yang telah di masukan pada sesi instalasi sebelumnya.
- Pastikan semua services pada sistem *Ipcop Firewall* berjalan dengan semestinya dan jangan lupa untuk memastikan setiap *interface* terkonfigurasi dengan baik.

Snort Pada Ipcop *Firewall*

Pada IPCop *Firewall* terdapat aplikasi perangkat lunak yang mendukung sistem pendeteksi penyusup yaitu Snort, snort pada Ipcop *Firewall* 1.4.18 adalah versi 2.6.1.5.



Sumber: Hasil Olahan Data

Gambar 6

Snort Version

File – file konfigurasi snort berada pada direktori **/etc/snort** di dalamnya berisi file local.rules, ruleslist.conf, rulestags, snort.conf, threshold.conf, vars serta direktori rules.

```
root@ferdiee:/etc/snort # ls -l
total 60
-rw-r--r-- 1 root  root    143 2007-12-02 01:07 local.rules
drwxr-xr-x 2 snort snort  4096 2008-02-19 03:44 rules
-rw-r--r-- 1 root  root   1602 2007-12-02 01:07 ruleslist.conf
-rw-rw-r-- 1 snort nobody  157 2008-02-20 07:30 rulestags
-rw-r--r-- 1 root  root  34763 2007-12-02 01:07 snort.conf
-rw-r--r-- 1 snort snort  2319 2007-12-02 01:07 threshold.conf
-rw-r--r-- 1 root  root    120 2008-02-24 00:20 vars
```

Sumber: Hasil Olahan Data

Gambar 7

direktori snort

Direktori yang sangat penting pada snort adalah direktori ules, karena pada direktori ini signature – signature serangan berasal. Rules sangat diperlukan untuk menganalisis serangan yang masuk kedalam network interface pada ipcop.

```
root@ferdiee:/etc/snort/rules # ls -a
.                         info.rules           smtp.rules
..                        local.rules          snmp.rules
attack-responses.rules    misc.rules           snort.conf
backdoor.rules            multimedia.rules     sql.rules
bad-traffic.rules         mysql.rules          telnet.rules
cgi-bin.list              netbios.rules        tftp.rules
chat.rules                nntp.rules           threshold.conf
classification.config     oracle.rules         unicode.map
ddos.rules                other-ids.rules      virus.rules
deleted.rules             p2p.rules            VRT-License.txt
dns.rules                 policy.rules         web-attacks.rules
dos.rules                 pop2.rules           web-cgi.rules
experimental.rules        pop3.rules           web-client.rules
exploit.rules             porn.rules           web-coldfusion.rules
finger.rules              reference.config     web-frontpage.rules
ftp.rules                 rpc.rules            web-iis.rules
generators                rservices.rules      web-misc.rules
gen-msg.map               scan.rules           web-php.rules
icmp-info.rules           shellcode.rules      x11.rules
icmp.rules                sid
imap.rules                sid-msg.map
```

Sumber: Hasil Olahan Data

Gambar 8

snort rules directory

Untuk memastikan keadaan snort aktif atau tidak dapat di periksa dengan perintah **ps –ef|grep snort**, dengan perintah ini service snort pada Ipcop dapat diperlihatkan, perintah ini akan menampilkan service setiap interface network yang dipantau oleh snort.berikut adalah tampilan setelah menggunakan perintah **ps –ef|grep snort**.

```
root@ferdiee:~ # ps -ef|grep snort
snort      348     1  0 03:28 ?        00:00:00 /usr/sbin/snort -c /etc/snort/sn
ort.conf -D -u snort -g snort -d -e -o -p -b -A fast -m 022 -i eth2
snort      370     1  0 03:28 ?        00:00:00 /usr/sbin/snort -c /etc/snort/sn
ort.conf -D -u snort -g snort -d -e -o -p -b -A fast -m 022 -i eth1
snort      379     1  0 03:28 ?        00:00:00 /usr/sbin/snort -c /etc/snort/sn
ort.conf -D -u snort -g snort -d -e -o -p -b -A fast -m 022 -i eth0
root@ferdiee:~ # _
```

Sumber: Hasil Olahan Data

Gambar 9

ps-ef|grep snort

Pada akhir baris pada service snort, terdapat perintah service –i eth0, -i eth1, -i eth2, itu menandakan snort bekerja dan melakukan monitoring terhadap *interface network* 0 (*green*), *interface network* 1(*orange*), *interface network* 2 (*red*) dengan *alert mode fast.* Snort bekerja dengan menggunakan sintaks – sintaks tertentu, sintaks – sintaks berikut yang biasanya digunakan pada pantauan jaringan komputer pada ipcop :

-A *set alert mode: fast, full, console, or none (alert file alerts only)*

-b *log pakets in tcdump format*

-d *dump the application layer*

-e *display the second layer header info*

-i *listen on interface*

-I *add interface name to alert output*

-*o change the rule testing order to pass|alert|log*

-p *disable promiscuous mode sniffing*

-P *set explicit snaplen of packet*

-q *quit.*

Berikut adalah tampilan penggunaan sintaks – sintaks yang digunakan pada ipcop *firewall* dengan menggunakan mode packet sniffer.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/27-23:04:42.462204 0:50:56:C0:0:1 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x102
192.168.241.9:138 -> 192.168.241.255:138 UDP TTL:128 TOS:0x0 ID:828 IpLen:20 Dgm
Len:244
Len: 216
11 0A 80 76 C0 A8 F1 09 00 8A 00 CA 00 00 20 45  ...v.......... E
4F 46 4A 45 50 45 4F 46 4A 45 42 46 50 45 4A 46  OFJEPEOFJEBFPEJF
44 45 4C 45 42 45 4F 45 45 45 42 46 43 41 41 00  DELEBEOEEEBFCAA.
20 41 42 41 43 46 50 46 50 45 4E 46 44 45 43 46   ABACFPFPENFDECF
43 45 50 46 48 46 44 45 46 46 50 46 50 41 43 41  CEPFHFDEFFPFPACA
42 00 FF 53 4D 42 25 00 00 00 00 00 00 00 00 00  B..SMB%.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 11 00 00 30 00 00 00 00 00 00 00 00 00 E8  .....0..........
03 00 00 00 00 00 00 00 00 30 00 56 00 03 00 01  .........0.V....
00 01 00 02 00 41 00 5C 4D 41 49 4C 53 4C 4F 54  .....A.\MAILSLOT
5C 42 52 4F 57 53 45 00 0C 00 60 EA 00 00 57 4F  \BROWSE...`...WO
52 4B 47 52 4F 55 50 00 E8 DA 90 02 00 E0 03 0A  RKGROUP.........
00 10 00 80 00 E0 F8 7F 4E 59 4F 4E 59 41 5F 49  ........NYONYA_I
53 4B 41 4E 44 41 52 00                          SKANDAR.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Sumber: Hasil Olahan Data

Gambar 10

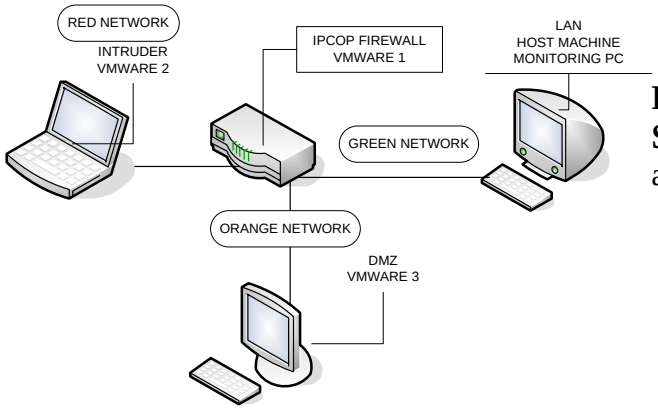
report snort mode sniffer

isis *Network Intrusion Detection* *em*

ema Analisis NIDS

Sebelum melakukan analisis pengujian *Intrusion Detection System* dalam hal ini analisis *network intrusion detection system (NIDS)*, terlebih dahulu membuat skema analisis *Network Intrusion Detection System* pada lingkungan implementasinya, skema ini digu-

nakan untuk mempermudah melakukan analisis pada lingkungan implementasinya. Skema analisis tersebut sebagai berikut :



Sumber: Hasil Olahan Data

Gambar 11
Skema pengujian NIDS

Keterangan :

- *Ipcop Firewall* (VMWare 1)
  - Processor Intel Core 2 duo 1.85 Ghz
  - Memori 256 Mb
  - Hardisk 4 Gb
  - Virtual CD room,3 NIC (Network Interface Card)
  - Operasi sistem *Ipcop* v.1.4.18 Distribusi Linux
  - *IP Address* :
  - ✓ Green : 192.168.241.10
  - ✓ Orange : 192.168.242.10
  - ✓ Red : 192.168.243.10
- Intruder (VMWare 2)
  - Processor Intel Core 2 duo 1.85 Ghz
  - Memori 128 Mb
  - Hardisk 2 Gb
  - Virtual CD Room, 1 NIC
  - Operasi Sistem Windows XP professional SP 2
  - *IP Address* : 192.168.242.100
- *DMZ* (VMWare 3)
  - Processor Intel Core 2 duo 1.85 Ghz
  - Memori 128 Mb
  - Hardisk 2 Gb
  - Virtual CD Room, 1 NIC
  - Operasi Sistem Windows XP professionnal SP 2
  - *IP Address* : 192.168.242.11
- Host Machine
  - Processor Intel Core 2 duo 1.85 Ghz
  - Memori 1 Gb
  - Hardisk 160 Gb
  - DVD Combo, 1 NIC
  - Operasi Sistem Windows XP professionnal SP 2
  - *IP Address* : 192.168.241.11

Pengujian NIDS

Skenario pengujian

a) Terdapat tiga *virtual* komputer sebagai *intruder*, *Ipcop Firewall* dan PC untuk *DMZ* dan satu buah *host machine* untuk melakukan *monitoring*.
Vmware pertama sebagai *Ipcop Firewall* yang berada ditengah koneksi jaringan yang akan memantau semua lalu lintas jaringan yang masuk dan keluar.
VMWare ke dua sebagai intruder digunakan untuk menjalankan berbagai cara eksploitasi
Host Mchine akan bertindak sebagai PC *monitoring*, digunakan untuk melihat tampilan *Ipcop* berupa *web GUI*.

b) *Intruder* akan menggunakan *Ping of Death* menggunakan *ICMP protocol* kemudian menggunakan beberapa *tools hacker* yang bertujuan untuk menciptakan *Denial Of Service* pada sistem yang dapat mengakibatkan sistem menjadi *crash* atau *hank*.

c) Selanjutnya diamati pada Host Machine apakah *Ipcop* mampu menjalankan snort dan fungsi *logging* snort terhadap serangan dari *intruder*.

d) Mencocokan *signature* yang terekam pada *Ipcop* terhadap *signature* yang ada pada snort *signature*.

e) Mencoba untuk menanggulangi menggunakan *Firewall* yang ada pada *Ipcop*.

Pengujian

Monitoring

Host melakukan *monitoring* dengan masuk ke dalam tampilan *Ipcop* yang berupa *Web GUI*, dengan membuka *browser* dan arahkan ke alamat *IP Address Monotoring Interface* (https://192.168.241.10 dengan menggunakan *port* 445 atau 81).

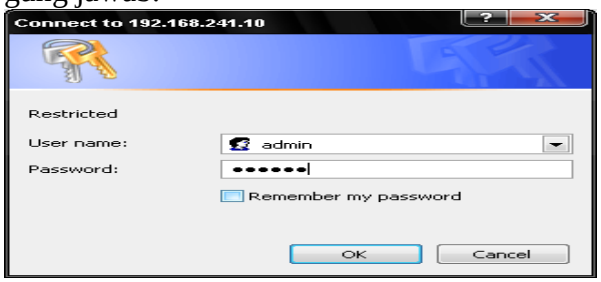
Anda akan mendapatkan *Security Alert* bahwa anda melihat halaman melalui koneksi yang memiliki keamanan, tekan OK untuk

melanjutkan. Setelah itu akan dapat peringatan bahwa *browser* tidak dapat mengenali sertifikat yang terpasang, untuk melanjutkan tekan YES.

Sumber: Hasil Olahan Data

Gambar 12
security alert

Setelah melewati tahap keamanan maka untuk dapat mengakses *Ipcop*, harus login terlebih dahulu dengan *user name admin* lalu masukan *password. Password* didapat dari akhir proses instalasi. Autentikasi ini dibutuhkan untuk menghindari pengguna yang tidak bertanggung jawab.

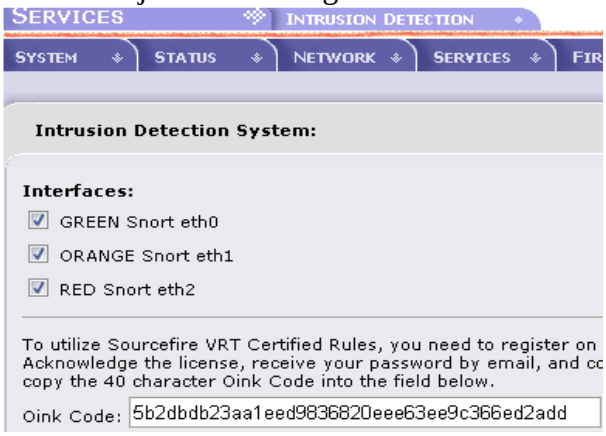


Sumber: Hasil Olahan Data

Gambar 13 *login*

Kemudian Setelah *login* maka harus melakukan konfigurasi untuk mengaktifkan IDS pada *Ipcop firewall* karena IDS tidak terkonfigurasi secara default pada *Ipcop firewall*. Konfigurasi dapat dilakukan dengan mengikuti *link services/intrusion detection* lalu *ceklist* pada jaringan / *interface* yang ingin di pantau (saat pengujian kondisi yang digunakan adalah *red, green, orange*).

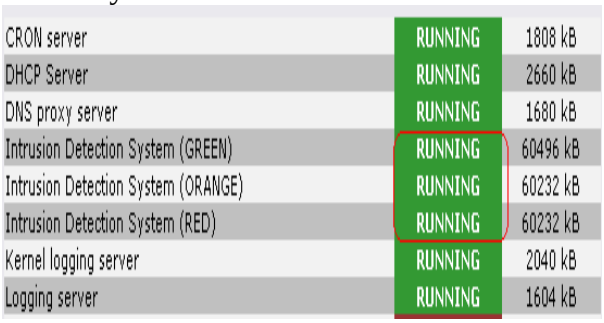
Agar snort bisa mendeteksi penyusup maka snort membutuhkan *rules*. Rules yang terdapat pada *Ipcop Firewall* versi 1.4.18 adalah rules dengan versi 2.6.1.5. Untuk mendapatkan *rules* yang terbaru pada *Ipcop* menyediakan fasilitas untuk bisa terus melakukan *update*, namun untuk mendapatkan *update*-an terbaru harus terdaftar pada situs resmi snort di www.snort.org. Setelah terdafatar akan mendapatkan 40 *character oink code*. Masukan 40 *Charater Oink Code*, setelah memasukkan *code* klik *save*, kemudian *apply now* untuk menjalankan konfigurasi.



Sumber: Hasil Olahan Data

Gambar 14
konfigurasi NIDS

Periksa hasil konfigurasi NIDS pada menu *status – system status* kemudian lihat pada *services* apakah *intrusion detecsion system* pada *network interface green, network interface red, network interface orange* sudah berjalan atau tidak. Jika tidak ulangi langkah sebelumya.



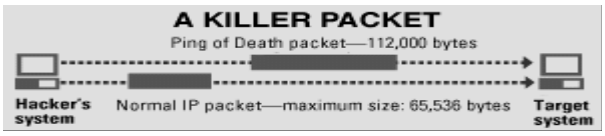
Sumber: Hasil Olahan Data

Gambar 15
status of intrusion detetion system

Serangan

Pada penggujian ini, PC *intruder* melakukan *ping attack* yang merupakan teknik serangan DoS *(Denail of Service)* dengan mengirimkan beberapa paket *ICMP (Internet Control Message Protocol)* dalam ukuran yang besar dan terus menerus ke *interface Network Orange* dan *Inreface Network Green* pada *Ipcop* dengan tujuan sebagai berikut :

1. membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datangnya dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam system jaringan. Teknik ini dinamakan *traffic flooding*.
2. membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah *host* sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini dinamakan sebagai *request flooding.*
3. meningkatkan kinerja sistem sampai batas maksimal sehingga terjadi *buffer overlow* yang dapat mengakibatkan sistem menjadi *hank* atau *crash.*

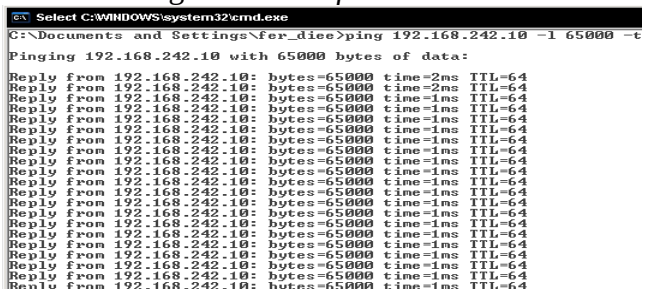


Sumber: Hasil Olahan Data

Gambar 16

denial of sevice

Intruder menggunakan perintah ping dengan size 65000. Berikut gambar untuk eksploitasi *ping atack* yang dilancarkan di sistem operasi *windows* dengan *time to life* 64



Sumber: Hasil Olahan Data

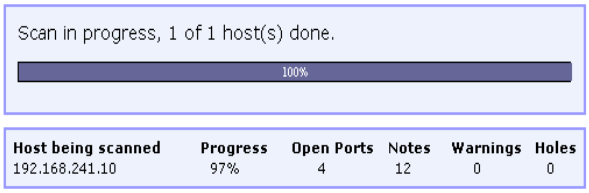
Gambar 17

Ping attack

Dari gambar diatas *intruder* berhasil melakukan *ping attack* terhadap *interface Network Orange* sehingga *traffic* pada jaringan tersebut menjadi penuh dikarenakan *size* yang digunakan merupakan *size* yang sangat besar.

Serangan dilanjutkan kembali menggunakan *tool hacker inferno* yang berfungsi sebagai DoS (*Denail of Service*) *attack*. Tools ini juga mampu melakukan *scanning port* pada sistem penyedia layanan jaringan sebagai awal dari bentuk serangan sehingga jika terdapat lubang pada *port* sistem maka *inferno* akan terus melancarkan pada *port* tersebut.

Selain menggunaan *ping attack* menggunakan aplikasi Nessus yang berfungsi untuk melakukan *scanning* terhadap *port – port* yang ada pada *Ipcop* dan melihat lubang – lubang yang memungkinkan untuk dapat disusupi oleh *intruder*. Dari hasil *port scanning* terdapat 4 *port* yang terbuka yaitu *port* 81, 53, 445, *general port.*



Sumber: Hasil Olahan Data

Gambar 18

hasil *port scanning*

Pantauan *Ipcop Firewall*

Pada tampilan *web administrator Ipcop Firewall* untuk memantau *Intrusion Detection System* biasanya *administrator* memperhatikan :

- Status pada system *Ipcop* yaitu:
  - *CPU usage*
  - *Memory Usage*
  - *Swap Usage*
  - *Disk Access*
- Status pada *Traffic Ipcop* yaitu :
  - *Traffic on Green*
  - *Traffic on Red*
  - *Traffic on Orange*
- IDS *Logs*

  Hasil dari serangan *intruder* terekam pada IDS *logs* berupa *report* serangan. *Ipcop* menyimpan *log – log* yang melewati

interface pada *Ipcop* kemudian disimpan pada *data*base snort. IDS *logs* berfungsi sebagai penterjemah hasil matching antara *logs* dengan signature snort yang ada pada rules. IDS *logs* menjelaskan darimana asal serangan,kemana arah tujuan serangan dan bentuk dari serangan. Berikut adalah laporan serangan yang menggunakan *ping attack.*

Date:	02/12 10:58:56	**Name:**	ICMP Large ICMP Packet
Priority:	2	**Type:**	Potentially Bad Traffic
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	499
Date:	02/12 10:58:57	**Name:**	ICMP Large ICMP Packet
Priority:	2	**Type:**	Potentially Bad Traffic
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	499
Date:	02/12 10:58:58	**Name:**	ICMP Large ICMP Packet
Priority:	2	**Type:**	Potentially Bad Traffic
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	499
Date:	02/12 10:58:59	**Name:**	ICMP Large ICMP Packet
Priority:	2	**Type:**	Potentially Bad Traffic
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	499
Date:	02/12 10:59:00	**Name:**	ICMP Large ICMP Packet
Priority:	2	**Type:**	Potentially Bad Traffic
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	499

Sumber: Hasil Olahan Data

Gambar 19

report serangan *ping attack*

Berikut adalah bentuk hasil *report* serangan yang menggunakan *tools hacker inferno*.

Date:	02/12 10:52:51	**Name:**	DOS IGMP dos attack
Priority:	2	**Type:**	Attempted Denial of Service
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	272
Date:	02/12 10:52:51	**Name:**	DOS IGMP dos attack
Priority:	2	**Type:**	Attempted Denial of Service
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	273
Date:	02/12 10:52:51	**Name:**	DOS IGMP dos attack
Priority:	2	**Type:**	Attempted Denial of Service
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	272
Date:	02/12 10:52:51	**Name:**	DOS IGMP dos attack
Priority:	2	**Type:**	Attempted Denial of Service
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	273

Sumber: Hasil Olahan Data

Gambar 20

report serangan menggunakan *tools hacker Inferno*

Berikut adalah hasil re*port* menggunakan *Port Scanning* menggunakan *tools Nessus*.

Date:	02/12 10:08:54	**Name:**	SNMP trap tcp
Priority:	2	**Type:**	Attempted Information Leak
IP info:	192.168.241.1:4482 -> 192.168.241.10:162		
References:	none found	**SID:**	1420
Date:	02/12 10:08:54	**Name:**	SNMP request tcp
Priority:	2	**Type:**	Attempted Information Leak
IP info:	192.168.241.1:4482 -> 192.168.241.10:161		
References:	none found	**SID:**	1418
Date:	02/12 10:08:59	**Name:**	SNMP AgentX/tcp request
Priority:	2	**Type:**	Attempted Information Leak
IP info:	192.168.241.1:4482 -> 192.168.241.10:705		
References:	none found	**SID:**	1421
Date:	02/12 10:09:14	**Name:**	(portscan) UDP Portscan
Priority:	n/a	**Type:**	n/a
IP info:	192.168.241.1:n/a -> 192.168.241.10:n/a		
References:	none found	**SID:**	n/a

Sumber: Hasil Olahan Data

Gambar 21

report serangan menggunakan *Nessus*

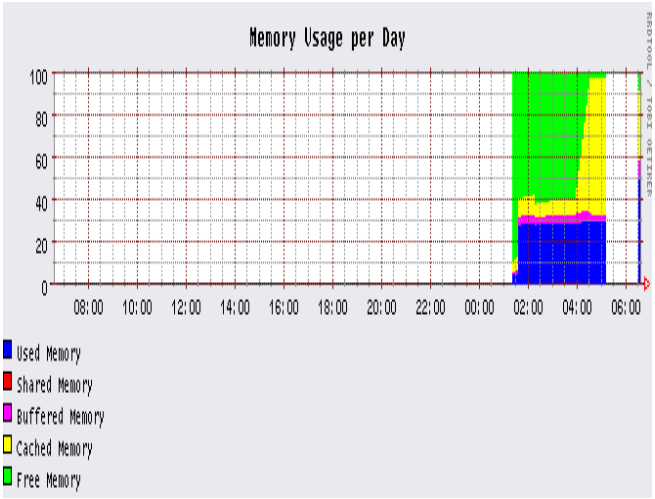
Dampak Serangan

Dampak serangan yang terjadi pada *Ipcop* dengan berbagai serangan adalah meningginya proses pada prosesor, memori dan *swap*.

Perubahan yang cukup signifikan pada pengunaan memori dari keadaan yang stabil dengan penggunaan memori sebesar sepuluh persen melonjak beberapa menit menjadi tiga puluh persen.

Begitu juga pada *cache memory* yang meningkat tajam dari empat puluh persen melonjak menjadi Sembilan puluh persen.

Berikut adalah grafik yang dhasilkan oleh *Ipcop firewall* berdasarkan memori yang digunakan.

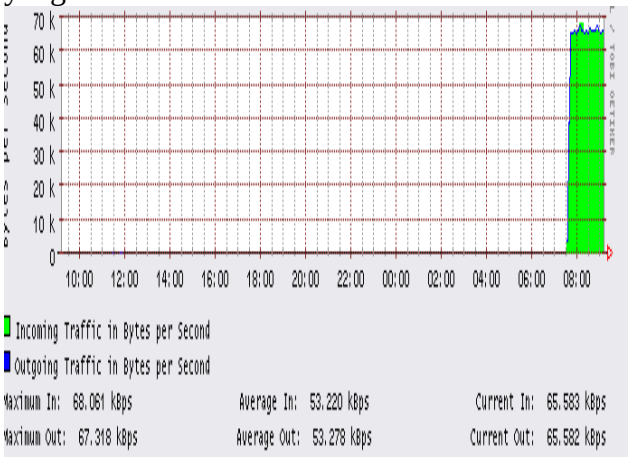


Sumber: Hasil Olahan Data

Gambar 22

memory usage

Selain memiliki dampak terhadap kinerja CPU, memori fisik, *swap* dan *cache*, dampak serangan yang dilancarkan dapat memadati *traffic*. *Traffic* akan dipenuhi oleh ping request yang dilancarkan oleh *intruder.*



Sumber: Hasil Olahan Data

Gambar 23

traffic pada *interface*

Pencegahan Menggunakan *Firewall*

Pada sistem operasi *Ipcop* telah tersedia sistem keamanan jaringan berupa *firewall*. *Ipcop firewall* merupakan distribusi linux dengan kernel 2.4.x yang didukung dengan *iptables.* Pada analisis ini *firewall* pada *Ipcop* digunakan untuk mem-*blok* usaha penyusup untuk masuk kedalam jaringan.

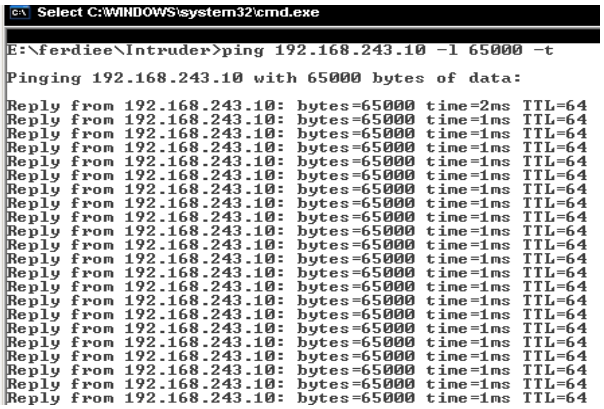
Berdasarkan pantauan dari sisi penyerang, penyusup biasanya diawali dengan melakukan *ping request* pada sistem korban dimaksudkan untuk mengetahui ada atau tidaknya *respons* sistem korban, kemudian mencoba membuat sistem menjadi *crash* atau *hank*. Pada *Ipcop* hal tersebut dapat ditanggulangi dengan menggunakan fitur *Disable Ping Response*. Fitur *Disable Ping Response* berada pada *firewall option.*

Sumber: Hasil Olahan Data

Gambar 24

Firewall Options

Penggunaanya adalah dengan memastikan terlebih dahulu darimana asal serangan terjadi, jika terjadi pada *network interface red*, pilih *only RED* pada *firewall options* kemudian klik *save*. Atau jika terjadi pada *interface* lainnya seperti *network interface green* maka pilih *All Interfaces.*berikut adalah serangan dari sisi intruder pada *network interface red* dengan menggunakan *ping attack.*

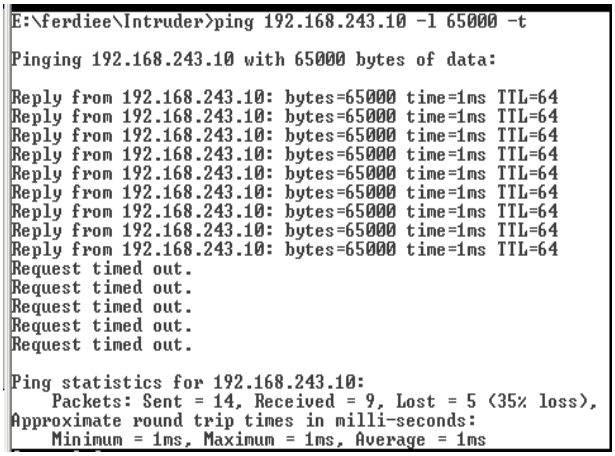


Sumber: Hasil Olahan Data

Gambar 25

ping attack

Berikut adalah gambar setelah *disable ping response* yang berada pada *firewall* options diaktifkan dengan menggunakan pilihan *Only RED.*



Sumber: Hasil Olahan Data

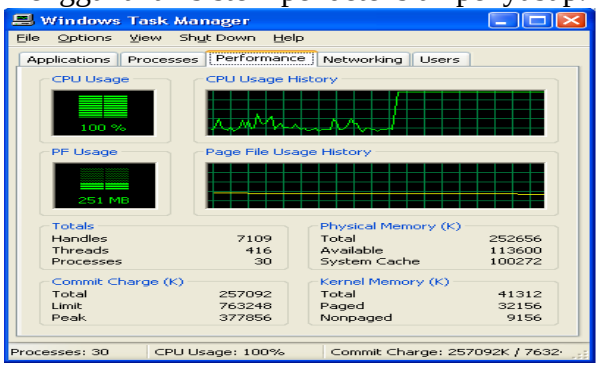
Gambar 26

hasil *block* menggunakan *firewall*

Sebelum dan sesudah sistem pendeteksian penyusup berjalan

Pada analisis ini, sistem operasi yang digunakan adalah windows XP *profesional service pack* 2 sebagai sistem yang belum

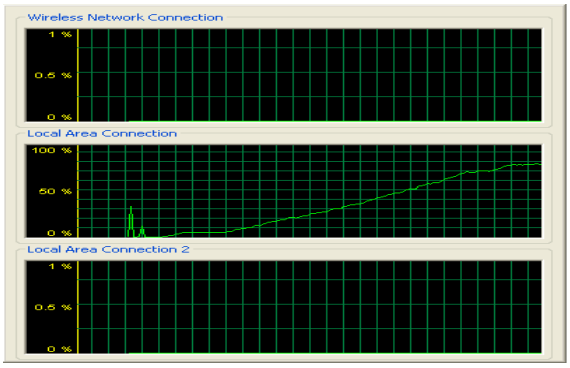
menggunakan sistem pendeteksian penyusup. Terbukti sistem operasi yang belum menggunakan sistem pendeteksian penyusup kinerja pada CPU-nya menigkat. Berikut adalah tampilan proses CPU sistem operasi yang tidak menggunakan sistem pendeteksian penyusup.



Sumber: Hasil Olahan Data

Gambar 27
proses CPU

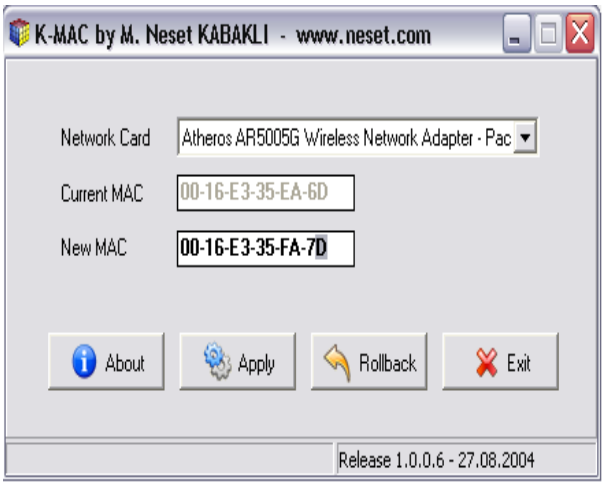
Dari serangan yang terjadi, hal yang menjadi perhatian adalah lalu lintas yang terekam pada *network connection* sistem operasi yang tidak menggunakan sistem pendeteksian penyusup. Grafik yang ada pada gambar 27 melonjak secara signifikan dan presentasi penggunaan traffic pada jaringan komputer dari 100Mbps yang mencapai 99 persen. Keadaan tersebut jika dibiarkan terus menerus akan mengakibatkan keadaan sistem operasi akan lama kelamaan akan crash atau hank dan akan sangat mengganggu konektifitas ke jaringan lainnya. Berikut adalah gambar dari penggunaan *network connection* pada sistem operasi widows XP profesional.



Sumber: Hasil Olahan Data

Gambar 28
network connection

Namun setelah penggunaan Ipcop *firewall* pada jaringan komputer, keadaan ini dapat dihindari dengan mengawasi *traffic* yang ada pada jika terjadi sesuatu yang mencurigakan pada IDS *logs* pada Ipcop *firewall* maka *administrator* dapat mengaktifkan *firewall* pada bagian jaringan yang mengalami serangan. Hal ini sudah diimplementasikan oleh mall baru yang ada di Serpong, Tangerang (mengaktifkan *firewall* pada *network interface* tertentu). Yaitu Summarecon Mall Serpong. Keadaan dengan firewall aktif pada *network interface red* terbukti dapat menyulitkan intruder untuk melancarkan serangan seperti ping request. Berikut adalah sambungan yang dibuat untuk melakukan eksploitasi pada jaringan summarecon. Eksploitasi dilancarkan dengan cara melakukan MAC *spoofing*, namun sebelumnya sudah mendapatkan MAC *address* yang telah terdaftar pada jaringan *wireless* pada summarecon. MAC *spoofing* diakukan menggunakan tools K-Mac, berikut adalah gambar pemalsuan MAC *address* pada PC penyerang.



Sumber: Hasil Olahan Data

Gambar 29
K-MAC

Berikut adalah gambar dimana MAC address penyerang telah berubah menjadi MAC address yang terdaftar pada akses jaringan summarecon dan jangkauan wireless pada summarecon mall.

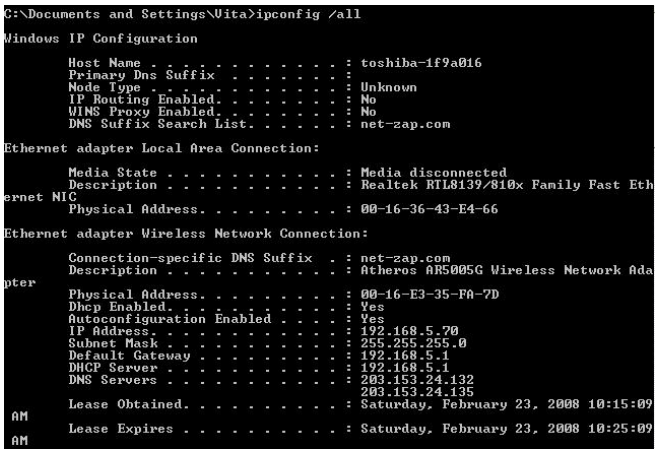
Sumber: Hasil Olahan Data

Gambar 30 *Adapter Information*

Sumber: Hasil Olahan Data

Gambar 31 jangkauan wireless

Setelah melakukan konektifitas terhadap jaringan summarecon, penyerang melakukan DoS dengan mengirimkan paket ICMP dengan jumlah besar, namun hal ini telah diantisipasi dengan baik.



Sumber: Hasil Olahan Data

Gambar 32 konektifitas

Kesimpulan

Dari beberapa hasil analisis dan re*port* diatas, snort pada *Ipcop* berjalan dengan sangat baik. *Snort* pada *Ipcop* mampu dapat mencocokan pola – pola serangan pada *signature – signature* yang ada pada sistem snort kemudian diterjemahkan oleh *Ipcop* ke dalam bentuk *report* berupa IDS *logs*. Kemudian dengan adanya *firewall* pada *Ipcop*, bentuk serangan menggunakan *ping request*, *port scanning* dapat di cegah dengan baik.

Daftar Pustaka

Ariyus, Doni, *"Intrusion detection system"*, Penerbit ANDI, Yogyakarta, 2007.

http://www.bondanmanajemen.blogspot.com, search : 25 Januari 2008

http://www.gajahmada .edu, search 10 Januari 2008

http://www.google.co.id, search: 25 Desember 2007

http://www.gudanglinux.net,search: 1 Februari 2008

http://www.ipcop.org, search: 1 Desember 2007

http://www.kamii_yogyakarta.tripod.com, search : 15 Januari 2008

http://www.mhaddons.tk, search: 28 Januari 2008

http://www.snort.org, search: 11 November 2007

Muammar, Ahmad, *"Firewall"*, www.ilmu komputer.com, search: 25 Januari 2008

Sutabri, Tata, "Karakteristik Sistem", www.google.co.id, search: 20 Desember 2007

Syukuri, Agus Fanar, ”Masa Depan Sekuriti Informasi”, www.ilmukomputer.com, search : 23 Desember 2007.

Tanenbaum, Andrew S, ”Jaringan Komputer Edisi Bahasa Indonesia”, Penerbit Pregalindo, Jakarta, 1997.

Thomas, Tom, “*Network Security First-Step”*, Cisco, 2004.