JISAMAR (Journal of Information System, Applied, Management, Accounting and Research **ISSN: 2598-8700 (Printed)**
ISSN: 2598-8719 (Online)

Volume 1 Nomor 1 November 2017

SISTEM PENDETEKSIAN DAN PENCEGAHAN PENYUSUP PADA JARINGAN KOMPUTER DENGAN MENGUNAKAN SNORT DAN FIREWALL

Budi Sudradjat
Akademi Bina Sarana Informatika/AMIK BSI Jakarta
e-mail: budi.bst@bsi.ac.id

Abstrak

Di era teknologi informasi saat ini, hampir seluruh informasi yang penting bagi suatu institusi 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. Oleh karena itu dibutuhkan sistem yang dapat menanggulangi 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) dan *firewall*. Salah satu aplikasi yang mendukung *intrusion detection system* (IDS) adalah Snort. Snort mampu melakukan analisis terhadap bentuk serangan *intruder* yang menyalahgunakan protokol jaringan.

Kata kunci : Keterbukaan akses data, *Intruder*, *Intrusion Detection System* (IDS), *firewall*, *Snort*, protokol jaringan, *IPCop Firewall*.

1. PENDAHULUAN

Keterbukaan akses informasi memunculkan berbagai masalah 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 system pendeteksian dan pencegahan penyusup dengan menggunakan perangkat lunak (*software*) atau perangkat keras (*hardware*) yang bekerja secara otomatis untuk memonitor keadaan pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan.

Atas dasar latar belakang tersebut dapat dirumuskan antara lain :

Bagaimana pola penyerangan yang dilakukan oleh *intruder*, sejauh mana peranan *Intrusion Detection System* dan *Firewall* pada keamanan jaringan komputer.

Untuk mencegah meluasnya pembahasan masalah diatas maka ruang lingkup masalah akan dibatasi sebagai berikut :

Pengenalan pola penyerangan yang dilakukan oleh *Intruder*, konfigurasi *IPCop Firewall*, teknik dan metode penggunaan *Network Intrusion Detection System* (NIDS) dan *Firewall* pada *IPCop Firewall*.

1.1. Jaringan Komputer

a. Pengertian

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*, dan lain-lain. 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),** merupakan jenis dari jaringan computer yang paling sederhana, tidak terlalu luas umumnya dibatasi oleh suatu lingkungan seperti perkantoran disebuah gedung atau universitas. Jarak maksimal antara satu titik komputer dengan yang lainnya hanya 100 meter dan kecepatan transmisi data berkisar dari 10 Mbps sampai 100 Mbps
2. ***Metropolitan Area Network (MAN)***, bisa dikatakan gabungan dari beberapa *Lokal Area Network* yang ada dan pemanfaatan teknologinya pun hampir sama dengan yang ada di *Lokal Area Network*. Luas dari *Metropolitan Area Network* ini biasanya mencakup jaringan antar gedung atau kantor secara sekaligus untuk dapat saling bertukar data.
3. ***Wide Area Network (WAN)***, biasanya WAN telah menggunakan sarana satelit ataupun kabel bawah laut sebagai media transmisinya. Luas jangkauan dapat mencapai 50 km. Kecepatan transmisi pada WAN tergantung pada media transmisi yang digunakan.
4. ***Inter Network***, lebih dikenal dengan nama internet merupakan jaringan terbesar yang ada didunia. *Internet* menjangkau seluruh negara di dunia dengan memanfaatkan media transmisi kabel telepon, satelit, dan media lainnya.

1.2 Komponen Jaringan

Perangkat pada sistem jaringan meliputi media transmisi secara fisik untuk menghubungkan beberapa komponen jaringan (*hub, switch, router*, dll) berupa peralatan *input output*, peralatan pemrosesan media penyimpanan, dan peralatan fisik lainnya yang dapat digunakan untuk mendukung kerja jaringan komputer.

a. Server, komputer yang berada pada satu jaringan dimana komputer ini mempunyai banyak fungsi sebagai penyedia jasa bagi perangkat yang terkoneksi dengan jaringan, menentukan hak akses bagi client untuk mengakses resources yang tersedia dalam jaringan, mengatur dan mengawasi kegiatan dalam jaringan.
b. Work Station / Client, Semua komputer/*host* yang terhubung dalam jaringan selain *server* disebut dengan *client* dimana masing-masing client mempunyai komponen *input output* (keyboard, mouse, monitor) dan *Central Processing Unit* (CPU) untuk mengolah *input* dan menghasilkan *output* dari *input* yang dimasukan.
c. Hub, merupakan sebuah perangkat yang menyatukan berbagai kabel-kabel *network* dari tiap-tiap *host*/komputer , server, dan perangkat lain dalam jaringan. *Hub* sering juga disebut *multiport repeater*. *Hub* sering dipertimbangkan untuk dipakai dalam jaringan karena *hub* dapat membuat koneksi terpusat pada jaringan dan meningkatkan reliabilitas jaringan. *Hub* juga disebut sebagai *share device* karena jika hub tersebut mempunyai kemampuan transmisi data sebesar 100 Mbps dan mempunyai 10 *port* misalnya maka masing masing *port* hanya mempunyai kecepatan transmisi data 10 Mbps, hub akan membagi rata untuk semua *port* yang ada.
d. Bridge, digunakan untuk mensegmentasi jaringan menjadi dua buah segmen jaringan. Jika sebuah jaringan menggunakan bridge untuk membuat segmentasi maka masing-masing jaringan yang tersegmentasi mempunyai masing-masing satu *collision domain*.

Switch, mempunyai fungsi sama dengan Hub hanya saja *switch* mempunyai beberapa

keunggulan dibandingkan dengan hub yakni *switch* tidak membagi sama rata kecepatan transmisi datanya pada masing-masing *port*. Jika switch tersebut mempunyai kecepatan transfer data sebesar 100 Mbps dan terdapat 12 *port*, maka masing-masing *port* juga mempunyai kecepatan transfer data sebesar 100 Mbps. Satu lagi keunggulan *switch* dibanding alat-alat sejenis yakni *switch* dapat membuat *collision domain* untuk masing-masing *port* yang terhubung padanya

e. *Repeater*, merupakan alat yang digunakan untuk menguatkan kembali sinyal transmisi data jika terdapat perangkat jaringan yang berada diluar jangkauan media sehingga sinyal yang dikirimkan akan melemah bahkan rusak.
f. *Router*, merupakan microcomputer yang mempunyai lebih dari satu NIC. *Router* juga digunakan untuk mentransmisikan data dari suatu jaringan lokal ke jaringan luar. *Router* hampir sama seperti *bridge* hanya router lebih pintar karena dapat mem-*filter packet* data yang keluar dan masuk. Router terdiri dari dua macam yaitu PC router dan *Hardware* router. PC router mempunyai sistem operasi *network* yang *built-in* dengan sistem operasi PC sedangkan *hardware* router hanya terdapat *processor* didalamnya dan menggunakan *Internet Operating System* (IOS).
g. *Network Interface Card (NIC)*, sebuah hardware berupa electric card yang terpasang pada slot *motherboard* komputer yang terhubung pada jaringan. NIC terdiri dari RAM, ROM, dan *Tranceiver* (*Transmitter* & *Receiver*). RAM digunakan sebagai *buffer* dan terdapat *flow control* supaya data yang ditampung pada *buffer* tidak terlalu berlebihan. Pada ROM terdapat *access method* dan *code* (MAC *Address*) yang *burn-in*. *Tranceiver* digunakan sebagai alat *transmisi* dan *receiver* data dari dan ke komputer.
h. Kabel merupakan media transmisi tentunya tidak sembarangan dan setiap kabel berpengaruh terhadap kualitas transmisi yang dilakukan. Jenis-jenis kabel yang biasa untuk transmisi jaringan adalah :
    1. Twisted Pair, kabel yang digunakan Kabel ini terbuat dari tembaga yang terpilin (*twisted*) bersama dalam satu pasang (*pair*). Sebuah kabel bisa terdiri dari dua hingga delapan pasang kabel. Kabel ini terbagi menjadi dua jenis yaitu *Shielded* dan *Unshielded*. *Shielded Twisted Pair* (STP) memiliki lapisan tembaga dan *foil* disekeliling kabel dalam bungkus plastik untuk melindunginya dari sinyal listrik yang berlebihan. Kabel ini relatif lebih mahal dan sulit mengkonfigurasinya karena lebih berat dan kurang fleksibel.
    2. *Coxial Cable (10Base2)*, media ini banyak digunakan sebagai media LAN, meskipun mahal kabel ini memiliki bandwith yang lebar sehingga bisa digunakan untuk komunikasi *broadband*. Dapat menjangkau jarak 500 m bahkan 2500 m dengan menggunakan *repeater*. Kabel ini proses pemasangannya menggunakan konektor BNC, untuk menyambung kemasing-masing computer menggunakan konektor T (*T-connector*) dan setiap ujungnya menggunakan terminator atau penutup jika tidak menggunakan *Hub*.
    3. *Fiber Optic* (Serat Optik), mempunyai kemampuan mentransmisi sinyal melewati jarak yang jauh dari pada kabel *coaxial* maupun kabel *twisted pair* dan mempunyai kecepatan yang baik. Hal ini sangat baik digunakan ketika digunakan untuk fasilitas konferensi Radio atau layanan interaktif. 10baseF adalah merujuk ke spesifikasi untuk kabel *fiber optic* dengan membawa sinyal *Ethernet*.
j. Protocol, merupakan suatu aturan main yang harus diikuti untuk menjamin keberlangsungan suatu kejadian dalam hal ini merupakan suatu bahasa yang terstandarisasi untuk komunikasi dalam jaringan maupun antar jaringan. Protocol yang dikenal secara luas antara lain :
    1. *Novell*, merupakan *network operating system* yang dirancang utnuk mengaitkan PC kedalam jaringan yang dapat memungkinkan media *storage (hardisk)*

dari server atau client yang ada menjadi transparan bagi satu dengan yang lain.

2. *TCP/IP, Transmission Control Protocol* dalam jaringan internet yang *compatible* dengan semua *platform*. Dengan TCP/IP interaksi antara satu komputer dengan komputer lainnya dapat terjadi tanpa dibatasi satu *platform* tertentu. Protokol ini merupakan hasil pengembangan DoD (*Department of Defence*) Amerika Serikat.
3. *IPX/SPX*, merupakan protocol standar untuk jaringan Novell (Netware) untuk mengatasi masalah *internetworking* pada jaringan PC yang menggunakan Novell. Pada prakteknya IPX dijalankan berkaitan dengan TCP karena lebih menguntungkan.
4. *Protocol* komunikasi *peer to peer*, *protocol* ini diimplementasikan pada *Windows for Group*.

1.3 *Security System*

Security system merupakan sebuah konsep dimana suatu 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.

a. *Privacy / Confidentialy*, pada system informasi jaringan merupakan usaha untuk mencegah akses terhadap informasi-informasi yang tidak seharusnya diakses oleh yang tidak berkepentingan. Konsep *privacy* lebih mengarah kepada data-data yang bersifat private sedangkan *confidentiality* cenderung mengarah kepada kerahasiaan data-data yang yang saling berkomunikasi. Kebocoran pada konsep ini dapat berakibat kepada bocornya informasi-informasi rahasia perusahaan.
b. *Integrity*, memastikan bahwa modifikasi data tidak dilakukan oleh *user* yang tidak memiliki izin untuk mengakses data dan tidak berwenang melakukan modifikasi data, modifikasi data yang tidak diperbolehkan dilakukan oleh *user* bahkan oleh *user* yang memiliki akses terhadap data, data konsisten baik secara internal maupun eksternal. Kebocoran konsep ini dapat menyebabkan pihak lain diluar sistem jaringan dapat merubah informasi-infornmsi yang krusial bagi perusahaan.
c. *Authentication*, merupakan metode atau cara yang diterapkan untuk memvalidasi terhadap keaslian data maupun user yang mengakses jaringan, apakah data maupun user yang dimaksud terdaftar dalam sistem jaringan. Kebocoran pada konsep ini dapat menyebabkan terbaginya atau terekploitasinya *resource* dalam jaringan internal perusahaan oleh user yang tidak terdaftar dalam jaringan. Adapun elemen untuk memastikan konsep ini adalah *Network Authentication Service*.
d. *Availability*, memastikan bahwa akses terhadap data-data yang dilakukan oleh user yang berwenang dapat dilakukan secara *reliable* dan terjadi pada saat itu juga. Dengan kata lain konsep ini memastikan bahwa sistem selalu siap dan berjalan ketika dibutuhkan. Kebocoran pada konsep ini menyebabkan kegagalan sistem jaringan (*down*) yang dapat mengakibatkan menurunnya kinerja elemen-elemen dalam perusahaan.

1.4 Teknik yang digunakan Firewall

Kebocoran pada konsep ini menyebabkan kegagalan sistem jaringan (*down*) yang dapat mengakibatkan menurunnya kinerja elemen-elemen dalam perusahaan. Berikut merupakan teknik-teknik yang digunakan dalam jaringan :

a. Service Control, Teknik ini ditekankan pada tipe-tipe layanan yang dapat dan yang tidak dapat digunakan baik kedalam maupun keluar *firewall*. Biasanya *firewall* akan memeriksa IP address dan nomor *port* yang digunakan pada protocol TCP ataupun UDP.
b. *Direction Control*, Teknik ini ditekankan pada arah *traffic* dari permintaan layanan yang akan dikenali dan diijinkan melewati *firewall* baik *inbound* maupun *outbound*.
c. *Behaviour Control*, Teknik ini ditekankan pada perilaku mengenai seberapa banyak suatu layanan telah digunakan
d. *User Control*, Teknik ini ditekankan pada *user* untuk dapat meminta dan menjalankan suatu layanan dimana terdapat *user* yang boleh dan

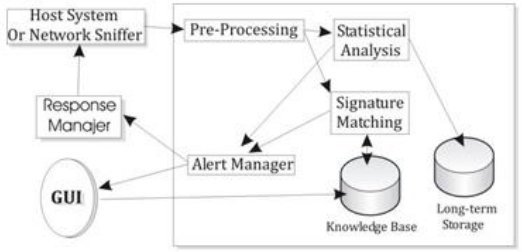
tidak boleh meminta dan menjalankan layanan tersebut. Teknik ini biasanya digunakan untuk membatasi *user* jaringan lokal untuk mengakses keluar.

e. *Host Control*, Teknik ini ditekankan pada *host* untuk dapat meminta dan menjalankan suatu layanan dimana terdapat *host* yang boleh dan tidak boleh meminta dan menjalankan layanan tersebut.
f. *Time Control*, Teknik ini ditekankan pada waktu dimana suatu layanan dapat diminta dan dijalankan. Teknik ini digunakan untuk mencegah terjadinya akses keluar disaat yang tidak diijinkan misalkan pada saat jam kerja, dan sebagainya.
g. *Transmission Line Control*, Teknik ini ditekankan pada jalur transmisi yang digunakan sistem. Jalur transmisi ini dapat berupa *private* maupun *public transmission line*.

1.5 *Intrusion Detection System*

Intrusion Detection System 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. *Intrusion Detection system* (IDS) dapat didefinisikan sebagai *tools*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan 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 meberikan peringatan, IDS juga mampu melacak aktivitas yang merugikan sebuah sistem. Suatu IDS dapat melakukan pengamatan (*monitoring*) terhadap paket – paket yang melawati jaringan dan berusaha menemukan apakah terdapat paket – paket yang berisi aktivitas – aktivitas mencuruigakan. *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.



Sumber : Dony Ariyus (2007)

Gambar 1.1 *Intrusion Detection System*

1.6 *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. 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*.

1.7 *Snort*

Snort adalah *Intrusion Detection System* jaringan *open source* yang mampu menjalankan analisis *real-time* dan paket *logging* pada IP *network*. 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.

Sumber : *www.snort.org*

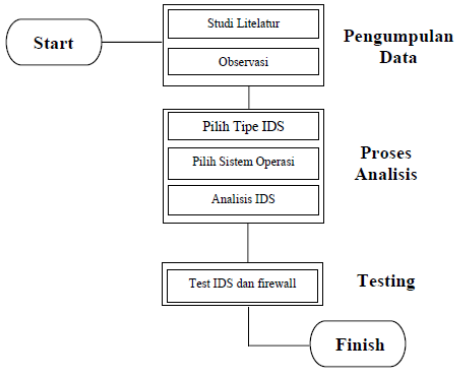
Gambar1.2. *Support Snort*

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 dijaringan untuk dianalisis dikemudian hari.

NIDS deteksi penyusup pada jaringan, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

2. Metode Penelitian

Tahapan penelitian dapat dilihat dari workflow diagram berikut :



Workflow diagram

Metode peneitian yang digunakan sebagai berikut :
1. Studi *literature*, data didapatkan dari buku-buku, artikel, jurnal yang mendukung.
2. Observasi, melakukan observasi mengenai aspek-aspek objek penelitian dan mendapatkan data perbandingan yang diperoleh melalui studi *literature*.

Tahapan analisis yang dilakukan sebagai berikut :
1. Pemiliihan tipe *Intrusion Detection System*, digunakan sebagai pertimbangan disesuaikan dengan kebutuhan administrator karena tipe yang ada pada *Intrusion Detection System* memiliki kelebihan dan kekurangan masing-masing.
2. Pemilihan sistem operasi, yang digunakan untuk menjalankan *Intrusion Detection System*. Sistem operasi yang digunakan harus mempertimbangkan tingkat kemudahan, keamanan dari sistem operasi.
3. Analisis *Intrusion Detection System*, peran serta kapabilitas dengan keamanan jaringan komputer.
4. Testing *Intrusion Detection System* dan *Firewall* untuk mendapatkan pembuktian seperti yang diharapkan.

Hardware dan *Software* yang digunakan adalah :
1. *Hardware* :
   a. PC Intel Pentium IV Core 2 duo 2 GHz
   b. RAM DDR3 2Gb
   c. Hardisk 160 GB
   d. CD/DVD Rom
2. Sistem Operasi
   a. Microsoft Windows 7 Profesional.
   b. IPCop *Firewall* Ver 1.4.18
3. *Software*
   a. VMWare Workstation 6 ACE Edition
   b. Snort IDS
   c. IPCop Firewall
   d. Nessus
   e. Inferno Hack Tools.

3. Pembahasan

3.1 Pemilihan Tipe IDS

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 .

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.

3.2 Pemilihan Sistem Operasi

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 7 Profesional
2. Distribusi Linux *Red Hat* 9.0
3. Distribusi Linux IPCop *Firewal*l Versi 1.4.18.

Berikut tabel perbandingan antara system operasi yang digunakan untuk pengimplementasian system pendeteksian penyusup pada jaringan computer.

Perbandingan Sistem Operasi untuk implementasi IDS :

Keterangan	Win 7	Red Hat 9	IPcop
Waktu Instalasi	40-50 mnt	50-60 mnt	<20 mnt
Space HD	>700 MB	>1.1 GB	<300 MB
SW Pendukung IDS	WinPcap, Snort, SQL Server, PHP, Apache, adodb, PHPlot, BASE	Snort, Mysql, Apache, PHP, Adodb, ACID, Zlib, LibPcab	Snort Apache, Cron, LibPcab
Konfigurasi	Sulit	Sulit	Mudah
Keamanan	Tidak ditujukan untuk keamanan jaringan	Tidak ditujukan untuk keamanan jaringan,	Secure Program

Pada sistem Win7 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 uraian diatas 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 keamanan 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 sudah terkonfigurasi dengan baik.

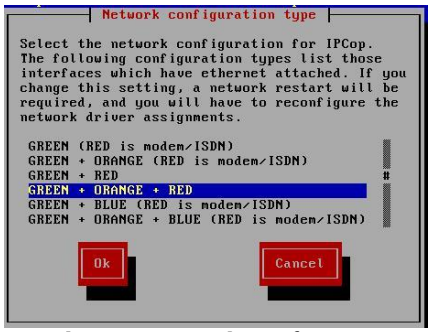
3.3 Instalasi IPCop *Firewall*

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

a. *Booting* dengan CD *bootable* melalui CD Rom.
b. Sesaat akan muncul *command prompt* dan muncul tampilan selamat datang dari Ipcop *firewall*.
c. Pilih bahasa yang akan digunakan pilih e*nglish*.
d. Pilih media instalasi konfirmasi partisi hardisk pilih Ok.
e. Pilihan untuk melakukan backup, pilih skip
f. Masukan IP address untuk network interface green.

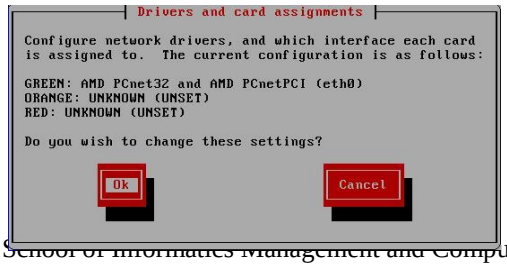
Gambar 3.1 *green interface*

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



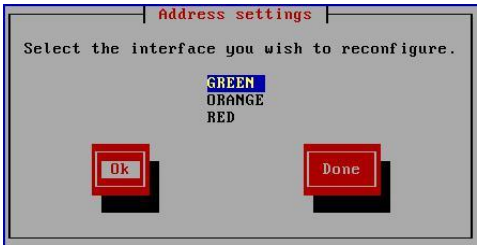
Gambar 3.2 *Network Configuration Type*

m. 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.



Gambar 3.3 *Drivers and Card Assignments*

n. Setiap *network interface* harus memiliki *iaddress*, 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.



Gambar 3.4 *address settings*

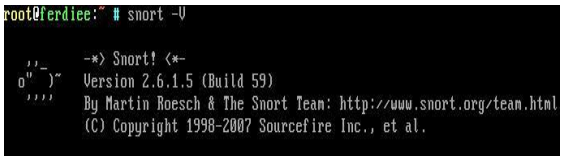
o. Pilih menu *DNS and Gateway* settings untuk melakukan konfigurasi *primary* dan *secondary domain name server* dan *default gateway.*
p. Pilih menu *DHCP Server Configuration* untuk melakukan konfigurasi *dynamic host control protocol.*
q. Setelah semua terkonfigurasi dengan baik maka pilih *done* untuk menyelesaikan konfigurasi
r. Masukan password minimal enam *character* untuk root.
s. 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.

Gambar 3.5 *Password* untuk *admin*

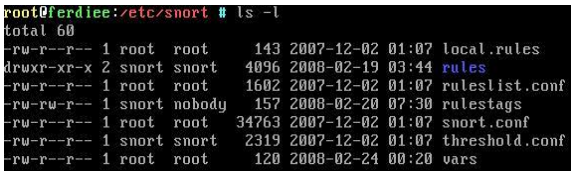
t. Masukkan *password* untuk *back up key*. Password ini digunakan untuk menyimpan konfigurasi *Ipcop firewall* serta menyimpan *log – log* yang telah tersimpan pada sistem *Ipcop firewall.*
u. Secara otomatis *Ipcop* akan melakukan *reboot.*Selesai melakukan *reboot Ipcop firewall* akan masuk kedalam sistem utama dimana semua konfigurasi dapat di *setting* kembali.
v. 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
w. Pastikan semua sevices pada sistem *Ipcop Firewall* berjalan dengan semestinya dan jangan lupa untuk memastikan setiap interface terkonfigurasi dengan baik

3.3 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.



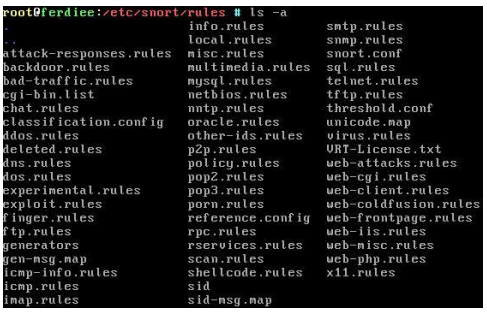
Gambar 3.6 Snort Version

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



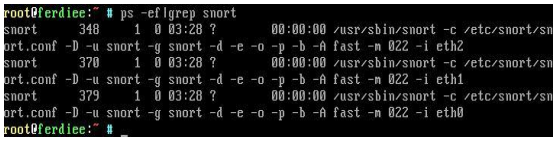
Gambar 3.7 Direktori Snort

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



Gambar 3.8 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**.

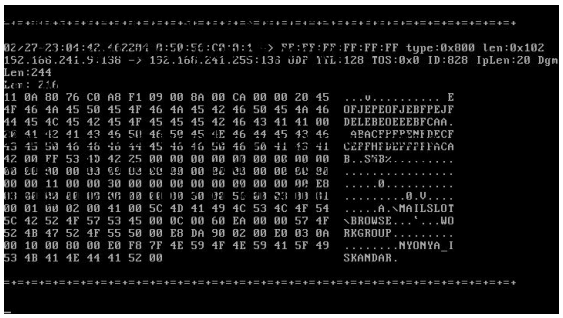


Gambar 3.9 ps-ef|grep snort

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

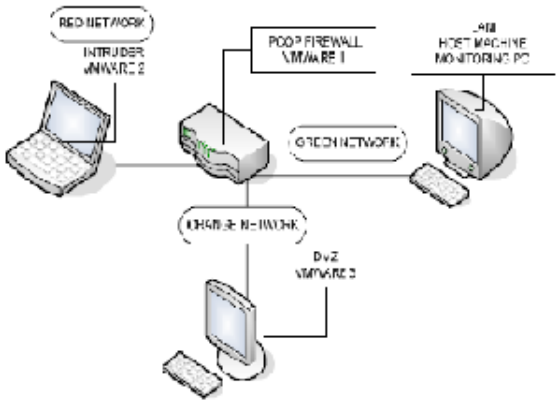


Gambar 3.10. *report snort mode sniffer*

3.4 Analisis Network Intrusion Detection System

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



Gambar 3.11 Skema pengujian NIDS

3.4.2 Pengujian NIDS

A. Skenario Pengujian

1. 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.

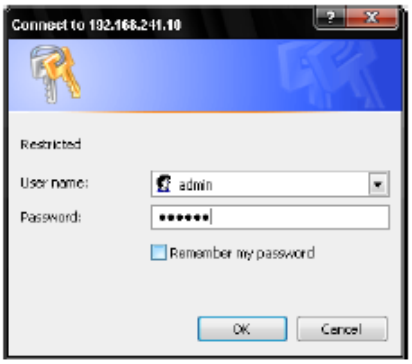
   VMWare ke dua sebagai intruder digunakan untuk menjalankan berbagai cara eksploitasi *Host Mchine* akan bertindak sebagai PC *monitoring*, digunakan untuk melihat tampilan *Ipcop* berupa *web GUI*.
2. Intruder akan menggunakan *Ping of Death* menggunakan *ICMP protocol* kemudian menggunakan beberapa *tools hacker* yang bertujuan untuk menciptakan *Denial Of Service* pada sistem yang dapat mengakibatkan sistem menjadi *crash* atau *hank*.
3. Selanjutnya diamati pada Host Machine apakah *Ipcop* mampu menjalankan snort dan fungsi *logging* snort terhadap serangan dari *intruder*.
4. Mencocokan *signature* yang terekam pada *Ipcop* terhadap *signature* yang ada pada snort *signature*.
5. Mencoba untuk menanggulangi menggunakan *Firewall* yang ada pada *Ipcop*.

B. Pengujian

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

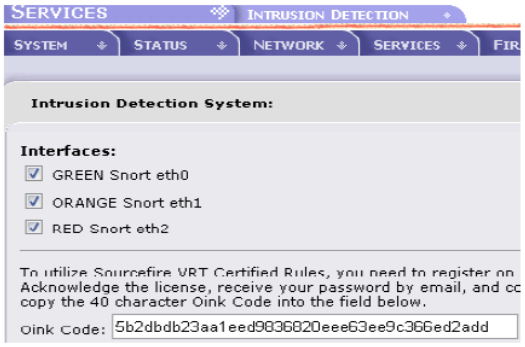
Gambar 3.12 Security Alert

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.



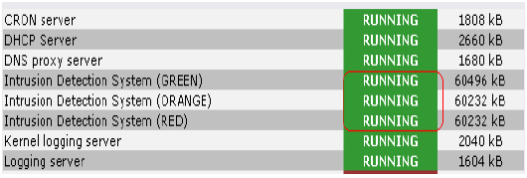
Gambar 3.13 Login

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.



Gambar 3.14 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.



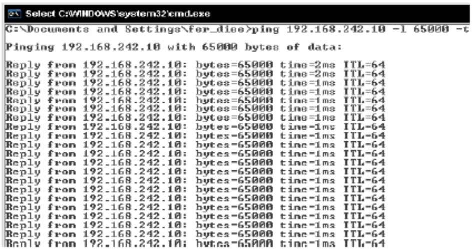
Gambar 3.15 *status of intrusion detection system*.

2. SERANGAN

Pada pengujian 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 :

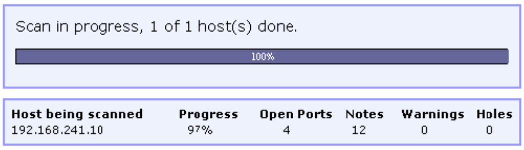
a. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datangnya dari pengguna yang terdaftar menjadi tidak dapat masuk kedalam system jaringan. Teknik ini dinamakan *traffic flooding*.

b. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga request yang datang dari pengguna. terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini dinamakan sebagai *request flooding.*
c. Meningkatkan kinerja sistem sampai batas maksimal sehingga terjadi *buffer overlow* yang dapat mengakibatkan sistem menjadi *hank* atau *crash.* Intruder menggunakan perintah ping dengan size 65000. Berikut gambar untuk eksploitasi *ping atack* yang dilancarkan di sistem operasi *windows* dengan *time to life* 64.



Gambar 3.16 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 system* 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*.

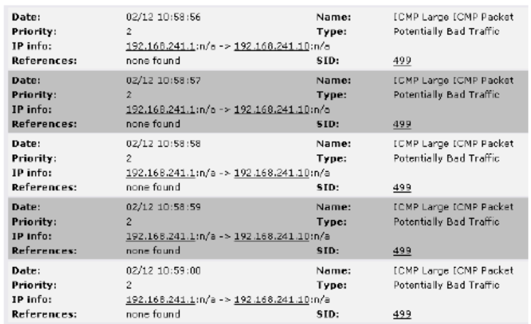


Gambar 3.17 hasil port scanning

3. PANTAUAN *IPCOP FIREWALL*

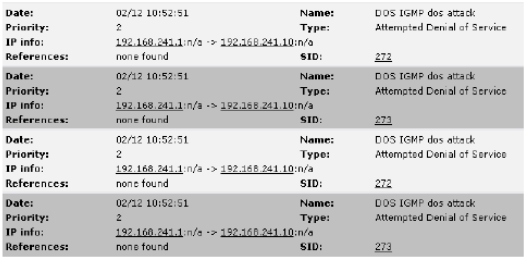
Pada tampilan *web administrator Ipcop Firewall* untuk memantau *Intrusion Detection System* biasanya *administrator* memperhatikan :

a. Status pada *system Ipcop* yaitu, *CPU Usage, Memory Usage, Swap Usage, Disk Access.*
b. Status pada *Traffic Ipcop* yaitu, *Traffic on Green, Traffic on Red, Traffic on Orange*.
c. 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*.



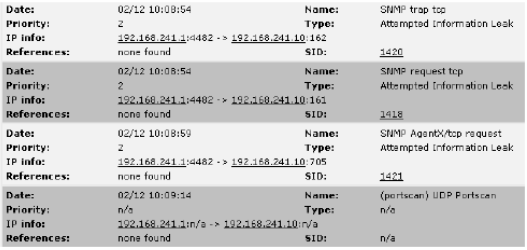
Gambar 3.18. Report Serangan Ping Attack

Berikut adalah hasil report serangan dengan menggunakan tools hackers inferno



Gambar 3.19 Report serangan menggunakan tools hackers inferno

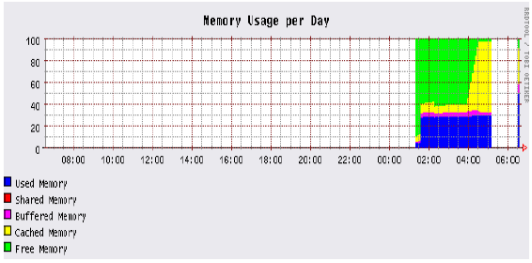
Berikut hasil report menggunakan Port Scanning menggunakan tools Nessus.



Gambar 3.20 Report serangan menggunakan Nessus

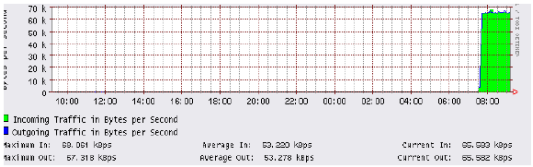
4. DAMPAK SERANGAN

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.



Gambar 3.21 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*.

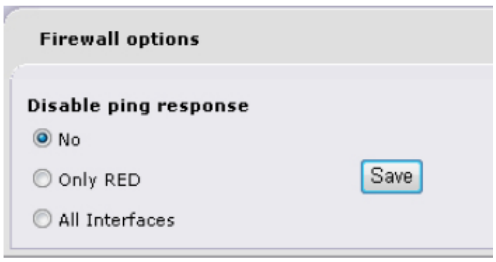


Gambar 3.22 Traffic pada Interface

3.4.3 Pencegahan Menggunakan Firewall

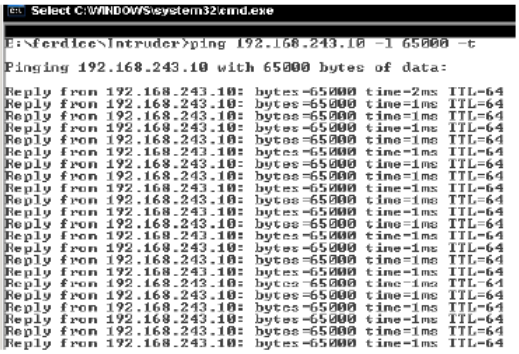
Pada Sistem operasi Ipcop telah tersedia system keamanan jaringan berupa *firewall*. *Ipcop firewall* merupakan distribusi linux dengan kernel 2.4.x yang didukung dengan *iptables.* Pada analisis ini *firewall* pada *Ipcop* digunakan untuk mem-*blok* usaha penyusup untuk masuk kedalam jaringan.

Berdasarkan pantauan dari sisi penyerang, penyusup biasanya diawali dengan melakukan *ping request* pada sistem korban dimaksudkan untuk mengetahui ada atau tidaknya *respons* system 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*.



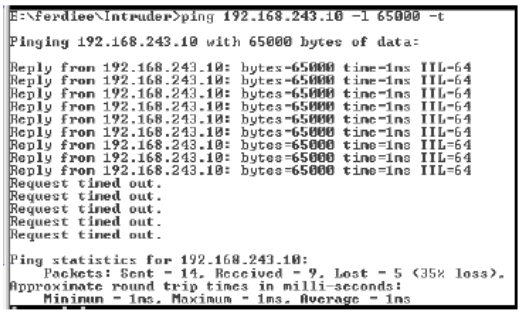
Gambar 3.23 *Firewall Option*

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.*



Gambar 3.24 Ping Attack

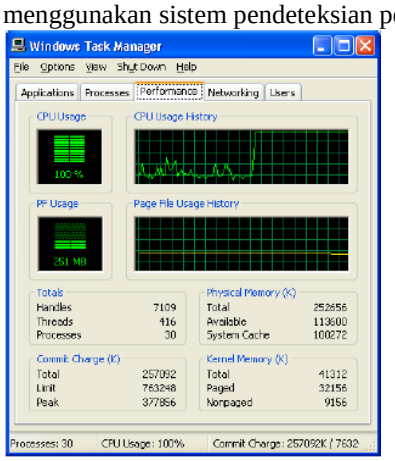
Berikut adalah gambar setelah *disable ping response* yang berada pada *firewall* options diaktifkan dengan menggunakan pilihan *Only RED*.



Gambar 3.25 Hasil *Block* menggunakan *Firewall*

3.4.4 Sebelum dan sesudah system deteksi

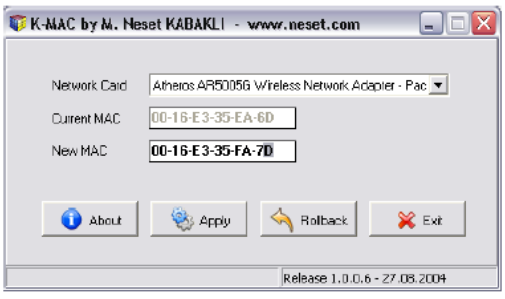
Pada bagian ini, system operasi yang digunakan windows 7 profesional sebagai sistem yang belum menggunakan sistem pendeteksian penyusup. Terbukti sistem operasi yang belum menggunakan sistem pendeteksian penyusup kinerja pada CPU-nya menigkat. Berikut adalah tampilan proses CPU sistem operasi yang tidak menggunakan sistem pendeteksian penyusup.



Gambar 3.26 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 4.27 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.

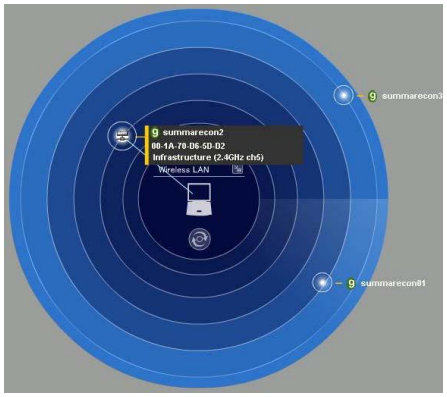
Namun setelah penggunaan Ipcop *firewall* pada jaringan komputer, keadaan ini dapat dihindari dengan mengawasi *traffic* yang ada pada jika terjadi sesuatu yang mencurigakan pada IDS *logs* pada Ipcop *firewall* maka *administrator* dapat mengaktifkan *firewall* pada bagian jaringan yang mengalami serangan. Keadaan dengan firewall aktif pada *network interface red* terbukti dapat menyulitkan intruder untuk melancarkan serangan seperti ping request.brikut adalah sambungan yang dibuat untuk melakukan eksploitasi pada jaringan. 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.



Gambar 3.27 K-Mac

Berikut adalah gambar dimana MAC address penyerang telah berubah menjadi MAC address yang terdaftar pada akses jaringan.

Gambar 3.28 Adapter Information



Gambar 3.29 Jangkauan Wireless

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

4. Penutup

4.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan di ruang kerja, maka dapat diambil beberapa kesimpulan mengenai Sistem Pendeteksian dan Pencegahan Penyusup pada Jaringan Komputer mengunakan SNORT dan Firewall sebagai berikut :

a. Pemilihan teknologi *Intrusion Detection System* sangat tepat untuk diterapkan pada satu jaringan sebagai keamanan jaringan yang dapat menjaga integritas data dan informasi
b. Keamanan teknologi dengan menggunakan teknologi Intrusion Detection System dapat dibuktikan dangan mengoperasikan sistem operasi pendukung yaitu *IPCop Firewall* yang mampu memantau paket-paket data yang lewat melalui koneksi jaringan komputer.
c. Dengan menggunakan IPCop Firewall bukan hanya dapat memantau paket – paket data yang lewat tapi juga dapat mem-*blok* paket – paket data yang dicurigai sebagai bentuk eksploitasi serta memutuskan koneksi.

4.2 Saran

Saran-saran yang dapat disampaikan untuk penelitian ini adalah :

a. Untuk meningkatkan keamanan pada suatu jaringan komputer dibutuhkan *intrusion detection system* dan *firewall* yang lebih baik untuk mem-*filter* IP *address* yang lewat.
b. Selalu *update signature database* agar dapat metode dan cara serangan yang terbaru yang pernah terjadi.
c. Sebaiknya *intrusion detection system* digunakan untuk kalangan menengah kebawah dengan asumsi keadaan *traffic* yang ada tidak terlalu padat.
d. Dikarenakan sistem pendeteksian penyusup berbasis snort memiliki kekurangan yaitu tidak dapat bekerja secara optimal pada kondisi *traffic* yang padat atau berada pada sistem jaringan *backbone* (mengakibatkan *false positives*) sebaiknya gunakan *IPS machine* yang mampu menanggulangi keadaan tersebut.

REFERENSI

[1] Ariyus, Doni 2007. *Intrusion detection system*, Penerbit ANDI, Yogyakarta
[2] Muammar,Ahmad (2015) .Firewall ,www.ilmukomputer.com, search : 25 Januari 2015
[3] Tanenbaum, Andrew S. (2008), Jaringan Komputer Edisi Bahasa Indonesia Penerbit Pregalindo, Jakarta.
[4] Thomas, Tom (2004). *Network Security First-Step*, Cisco