MENGANALISA SISTEM KEAMANAN JARINGAN BERBASIS INTRUSION PREVENTION SYSTEM DAN HONEYPOT SEBAGAI PENDETEKSI DAN PENCEGAH MALWARE
(STUDI KASUS PT. KARYA MITRA NUGRAHA)

Johanes Indra Homenta[1], Rissal Efendi[2]
[1,2,] Program Studi Teknik Informatika STMIK ProVisi Semarang
[1]**johanes@gmail.com,** [2]**rissal@gmail.com**

Abstract

Current internet technology is growing, the exchange of information easily done with other people anywhere and anytime. But the ease of communication is not accompanied by a security to secure any information that is interchangeable. The high-level offenses such as burglary attempt by a person who is not responsible to prove the lack of security in computer networks. The use of firewalls is also deemed to be lacking in securing network security, it is necessary for a tool that helps enhance network security capable of monitoring network traffic by using Honeyd and snort IDS. This study aims to monitor network traffic patterns in PT. Mitra Karya Nugraha, the results showed that the application of Honeyd and Snort IDS can be used to monitor the network in real-time.

Keywords : computer network, IDS, network security, Honeyd, Snort.

1. Pendahuluan

A. Latar Belakang

Seiring berkembangnya Teknologi Informasi kejahatan komputer berkembang melalui jaringan internet, maupun media komputer lainnya. Jenis kejahatan yang dilakukan diantaranya berupa penyebaran *Malware* yang tentunya dapat merugikan pengguna komputer. *Malware* merupakan perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, atau jejaring komputer tanpa izin dari pemilik (Prayitno (2010:8)). Penyebaran dari *Malware* bisa melalui berbagai macam cara diantaranya melalui penggunaan jaringan internet, USB flashdisk, maupun melalui aplikasi yang terinfeksi *Malware*.

Ada pula beberapa kasus penyerangan *Malware* terhadap perusahaan melalui jaringan komputer yang pernah terjadi diantaranya :

1. 7 Februari 2000. Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E-Trade.
2. Adrian Lamo adalah seorang analis ancaman virus. Dia pertama kali mendapat perhatian media adalah saat merusak beberapa profil jaringan komputer menggunakan virus, termasuk The New York Times, Yahoo, dan Microsoft.

Berdasarkan kasus yang pernah terjadi penyerangan *Malware* ini memiliki resiko kerugian yang besar, karena dapat merugikan suatu perusahaan yang diserangnya. Kerugian yang dialami dapat berupa kerusakan data perusahaan, hilangnya data perusahaan, ataupun pencurian data perusahaan yang terbilang penting. Maka dari itu perlunya perlindungan yang dapat mencegah penyerangan *Malware* terjadi.

Beberapa perusahaan pada umumnya meggunakan jaringan komputer sebagai pendukung kinerja para karyawannya, seperti halnya PT. KARYA MITRA NUGRAHA menggunakan jaringan komputer sebagai pendukung kerja karyawannya. Berdasarkan hasil pengamatan beberapa perangkat komputer yang terdapat di PT. KARYA MITRA NUGRAHA didapati terinfreksi *Malware* diantaranya adalah *Trojan Horse, Virus, Worm, Exploit,* dan *Backdoor* yang tentunya dapat merugikan perusahaan

B. Rumusan Masalah

Berdasarkan latar belakang diatas, maka penulis merumuskan masalah yaitu bagaimana menerapakan *Honeypot* dan juga *Intrusion Prevention System* sebagai sistem proteksi dan sistem pendeteksi penyusup yang membantu mendeteksi dan mencegah aktifitas penyerang khususnya *Malware* dalam sebuah sistem jaringan komputer pada PT. KARYA MITRA NUGRAHA.

D. Tujuan Penelitian

Adapun tujuan penelitian yang dibuat oleh penulis yaitu :

1. Menganalisa keamanan jaringan di PT. KARYA MITRA NUGRAHA untuk mengetahui kelemahan pada sistem keamanan jaringan.
2. Menerapkan *Intrusion Prevention System* dan *honeypot* pada server bayangan.
3. Mengkonfigurasi *honeypot* dan *Intrusion Prevention System* sebagai sistem keamanan jaringan

II. Landasan Teori

A. Intrusion Prevention System / IPS

Menurut Scarfone (2007:9) merupakan sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya.

Intrusion Prevention System merupakan kombinasi antara fasilitas *blocking capabilities* dari Firewall dan kedalaman inspeksi paket data dari *Intrusion Detection System* (IDS). IPS diciptakan pada awal tahun 1990-an untuk memecahkan masalah serangan yang selalu melanda jaringan komputer. IPS membuat akses kontrol dengan cara melihat konten aplikasi, dari pada melihat *IP address* atau port, yang biasanya dilakukan oleh firewall. Sistem setup IPS sama dengan sistem setup IDS. IPS mampu mencegah serangan yang datang dengan bantuan administrator secara minimal atau bahkan tidak sama sekali. Secara logis IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, selain itu IPS membandingkan file yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga bisa menginterupsi sistem call (Scarfone (2007:9)).

Ada beberapa metode IPS melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut, diantaranya :

a. *Signature-based Intrusion Detection System*, pada metode ini tersedia daftar sgnature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data signature yang ada harus tetap ter-update (Scarfone (2007:9)).

b. *Anomaly-based Intrusion Detection System* Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS dan IPS sehingga IDS dan IPS dapat mengatahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS dan IPS menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau akan menolak paket tersebut untuk diteruskan (IPS) (Scarfone (2007:9)).

Intrusion prevention system mengkombinasikan kemampuan *network based* IDS dengan kemampuan firewall, sehingga selain mendeteksi adanya penyusup juga bisa menindaklanjuti dengan melakukan pemblokiran terhadap IP yang melakukan serangan.

B. Intrusion Detected System / IDS

Menurut Scarfone (2007:9) Intrusion Detection Systems merupakan sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatankegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/ anomali melalui aksi pemblokiran seorang user atau alamat IP (Internet Protocol) sumber dari usaha pengaksesan jaringan.

IDS juga memiliki cara kerja dalam menganalisa apakah paket data yang dianggap sebagai intrusion oleh intruser. Cara kerja IDS dibagi menjadi dua, yaitu :

a. *Knowledge Based* adalah cara kerja IDS dengan mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule pada IDS tersebut. Database rule tersebut dapat berisi signature – signature paket serangan. Jika pola paket data tersebut terdapat kesamaan dengan rule pada database rule pada IDS, maka paket data tersebut dianggap sebagai serangan dan demikian juga sebaliknya, jika paket data tersebut tidak memiliki kesamaan dengan rule pada database rule pada IDS, maka paket data tersebut tidak akan dianggap serangan (Scarfone (2007:14)).
b. *Anomaly Based* adalah cara kerja IDS dengan mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan – kejanggalan pada sistem, aatu adanya keanehan dan kejanggalan dari kondiri pada saat sistem normal, sebagai contoh : adanya penggunaan memory yang melonjak secara terus menerus atau terdapatnya koneksi secara paralel dari satu IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi tersebut dianggap kejanggalan yang selanjutnya oleh IDS Anomaly Based ini dianggap sebagai serangan (Scarfone (2007:14)).

Intrusion itu sendiri didefinisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect*, *inappropite* yang terjadi di jaringan atau di host tersebut. *Intrusion* tersebut kemudian akan diubah menjadi "rules" ke dalam IDS. Oleh karena itu IDS ditujukan untuk meminimalkan kerugian dari *intrusion* (Scarfone (2007:14)).

C. Honeypot

Menurut Diebold, et all (2005: 4) Honeypot dapat berguna untuk membuang – buang sumber daya penyerang atau mengalihkan penyerang dari sesuatu yang berharga.

Honeypot adalah komputer yang sengaja " dikorbankan" untuk menjadi target serangan hacker. Oleh sebab itu setiap interaksi dengan honeypot patut diduga sebagai sebagai aktivitas penyusupan. Honeypot memang hanya mempunyai manfaat kecil pada pencegahan, tetapi sangat berguna untuk mendeteksi serangan. Perlu diingat bahwa firewall juga tidak bisa menghilangkan serangan *Mallware*, tetapi hanya memperkecil resiko serangan. honeypot bisa menangkap aktivitas dari *script kiddies* sampai elite hacker baik dari dunia luar maupun yang berasal dari jaringan internal (Diebold, et all (2005: 6)).

D. Malware

Menurut Prayitno (2010:10) perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer atau jejaring komputer tanpa izin dari pemilik.

Dapat disimpulkan bahwa *Malware* merupakan aplikasi komputer yang khusus dibuat dengan tujuan mencari celah dan kelemahan software. *Malware* dirancang untuk menggangu atau menolak *software* dengan tujuan mengumpulkan informasi yang mengarah pada hilangnya privasi atau eksploitasi dari dalam sumber daya sistem.

III. Metode Penelitian Dan Perancangan

A. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam laporan skripsi ini adalah :

1. Interview : Menanyakan gejala – gejala malware beserta kerugian yang pernah dialami kepada Teknisi komputer di PT. KARYA MITRA NUGRAHA.
2. Observasi : Mengamati dan mencatat *Malware* apa saja yang menginfeksi komputer di PT. KARYA MITRA NUGRAHA.
3. Dokumen : Mengambil dokumen berupa gambar *malware*

B. Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah PPDIOO dimana mencakup tahapan sebagai berikut (Teare (2008:11)) :

1. *Prepare* (Persiapan)

Kebutuhan akan sebuah *tools* (alat) untuk mendukung peningkatan keamanan dalam sebuah jaringan sangatlah penting. Berbagai alat telah digunakan untuk meningkatkan keamanan jaringan computer dari segala ancaman, gangguan, atau serangan. Masih banyak perusahaan yang menggandalkan *firewall* sebagai alat keamanan dalam jaringan komputer dengan berfungsi sebagai

tembok yang menyaring semua objek data yang akan dilewatkan. Tetapi dengan hanya menggunakan *firewall* tersebut jaringan komputer masih belum aman dari segala ancaman, gangguan, dan serangan dikarenakan *firewall* tidak dapat memberikan *report* secara *real time* mengenai aktivitas pada jaringan.

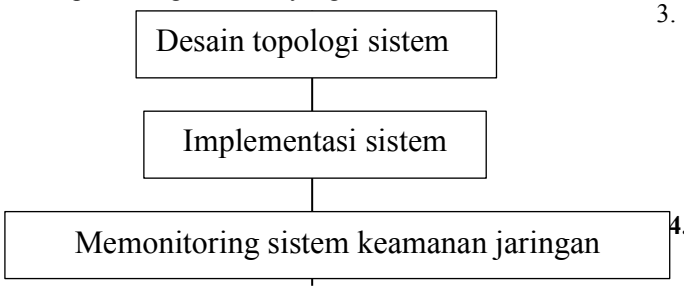
Maka dari itu perlunya meningkatkan kemanan jaringan dengan menggunakan beberapa *tools* keamanan jaringan yang mampu merekam dan mengidentifikasi akitvitas jaringan, diantaranya menggunakan *tools* tambahan berupa honeyd, *snort*, dan Ufw *firewall*. Dimana honeyd berfungsi sebagai server bayangan yang mendeteksi dan merekam aktivitas jaringan, *snort* digunakan sebagai sistem keamanan jaringan yang mendeteksi sekaligus mencegah paket data yang dianggap ancaman, dan ufw *firewall* yang merupakan *firewall* dengan fitur mengatur dapat lalu lintas jaringan secara manual.

2. . ***Plan*** **(Perencanaan)**

Dalam meningkatkan sistem keamanan jaringan yang akan dibuat, dibutuhkan sebuat *tools* (alat) yang sistem kerjanya mampu merekam semua aktivitas jaringan secara *real time* dan menampilkan hasil rekamanan aktivitas jaringan yang sudah dikelola tersebut kepada *administrator*, sehingga *administrator* dapat denan mudah memahami setiap hasil laporan yang ditampilkan. Dengan demikian, *administrator* akan lebih cepat mengambil tindakan apabila terjadi, ancaman, gangguan, atau serangan terhadap jaringan tanpa melakukan analisis

3. ***Design*** **(Desain)**

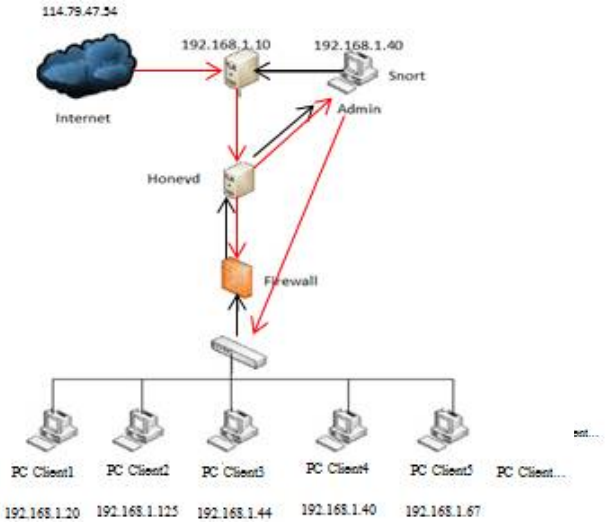
Sebelum melakukan penelitian, penulis membuat bagan desain perancangan sistem. Berikut merupakan gambaran bagan perancangan sistem yang akan dibuat :



Gambar 3.4 Bagan perancangan sistem

Gambar 3.4 menunjukan bagan perancangan sistem yang akan dibuat.

Mendesain topologi sistem yang akan di bangun, dimana bertujuan agar dapat memudahkan kita ketika sistem tersebut di implementasikan secara nyata karena akan diketahui tahap – tahap pengerjaan apa saja yang di perlukan dalam penelitian, teknologi seperti apa yang akan dibutuhkan, dan gambaran mengenai cara memperbaiki konfigurasi yang tepat. Berikut merupakan gambaran desain topologi sistem yang akan dibuat :



Gambar 3.5 Design topologi sistem

Gambar 3.5 menunjukan desain topologi sistem yang akan dibuat, berikut merupakan penjelasan dari gambar diatas :

1. Honeyd berguna sebagai server bayangan yang memonitoring dan mendeteksi aktivitas jaringan yang terjadi, diletakan setelah server utama.
2. *Firewall* berguna untuk mengatur *traffic* jaringan mana saja yang boleh keluar atau masuk sistem jaringan.
3. *Snort* yang berguna untuk memonitoring aktivitas jaringan dimana akan menganalisis paket yang diterima sekaligus mencegah paket data jika paket data dianggap mencurigakan, *Snort* diletakan sesudah *firewall*.

4. ***Implement*** **(Implementasi)**

Dalam melakukan implementasi hal pertama yang dilakukan adalah instalasi ubuntu versi backtrack 3 R5,

mengkonfigurasikan *honeyd*, Instalasi *Intrusion Prevention System* yang mencakup IDS (*Snort* IDS) dan *Ufw Firewall* (*Packet Filtering Firewall*), dan melakukan konfigurasi keamananan jaringan secara keseluruhan baik *Honeyd*, *Intrusion Prevention System* yang mencakup *Snort* IDS dan *Ufw firewall* sebagai Packet Filtering *Firewall*.

5. ***Operate*** **(operasional)**

Mengimplementasikan bentuk penelitian secara nyata diantaranya melakukan monitoring dan menganalisis aktivitas jaringan pada server bayangan *Honeyd*, *Intrusion Prevention System* yang mencakup *Snort* IDS dan *Ufw firewall* sebagai *Packet Filtering Firewall*. Hasil dari monitoring akan disimpan dalam file catatan yang berupa file log *Honeyd*, *Intrusion Prevention System* yang mencakup log *Snort* IDS dan Log *Ufw firewall* sebagai *Packet Filtering Firewall*.

6. ***Optimize*** **(Optimalisasi)**

mengoptimalkan sistem keamanan jaringan dibuat dengan memonitoring dan juga memperbaiki sistem keamanan jaringan jika terjadi kesalahan baik pada konfigurasi maupun pada implementasi tools penelitian.

IV. Hasil Dan Pembahasan

A Implementasi

Mengimplementasikan sistem secara nyata, melakukan installasi sistem operasi *backtrack 5 r3*, mengkonfigurasikan *honeyd*, *snort*, beserta *ufw firewall* yang nantinya akan digunakan untuk memonitoring sistem keamanan jaringan

1. **Installasi Bactrack 5 r3**

Melakukan instalasi sistem operasi yang akan digunakan dalam menunjang penelitian, diantaranya adalah sistem operasi backtrack 5 r 3. Backtrack 5 r3 ini dugunakan karena sistem operasi ini sangatlah menunjang penelitian dalam hal jaringan keamanan komputer.

2. **Konfigurasi Honeyd Pada Backtrack 5 r3**

Buatlah file pengaturan untuk honeyd dengan menuliskan perintah dan isikan pengaturan *honeyd* seperti berikut :

```
#gedit honeyd.conf
```

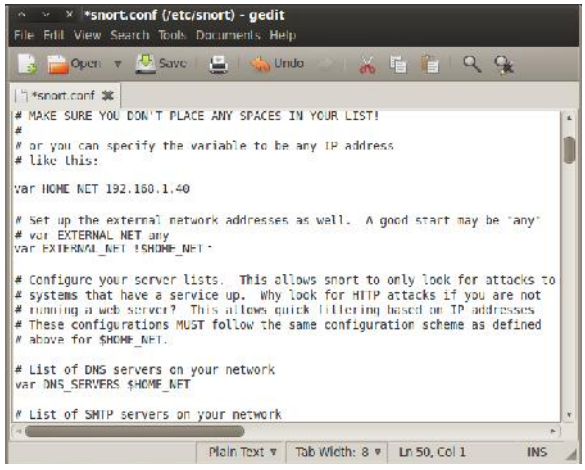
```
create windows
set windows personality “Microsoft Windows XP Proffesional SP1
add windows tcp port 23 open
add windows tcp port 25 open
add windows tcp port 80 open

set windows ethernet “aa:bb:cc:ee:ff”
bind 192.168.1.40 windows
```

3. Konfigurasi Snort Pada Backtrack 5 r3

Mengimplementasikan snort pada *backtrack 5 r3* hal yang harus dilakukan terlebih dahulu adalah mengkonfigurasi *network* yang akan diawasi dengan cara mendaftarkan *network* yang akan diawasi ke dalam pengaturan snort. Buka jendela terminal *pada backtrack 5 r3* dan tuliskan perintah

```
# gedit /etc/snort/snort.conf
```



Gambar 4.13 Gedit snort.conf

Gambar 4.13 Dalam snort.conf sebenarnya sudah terdapat pengaturan tersendiri, namun kita harus menambahkan pengaturan sesuai dengan kebutuhan. Keterangan dari gambar diatas adalah :

- Tuliskan "192.168.1.40" pada VAR_HOME_NET. Hal ini diartikan, *network* yang diawasi adalah 192.168.1.10
- Hilangkan tanda "#" pada VAR_EXTERNAL_NET !$HOME_NET yang artinya *network* lain yang terhubung dengan *network* 192.168.1.40 juga bisa diawasi melalui *Ethernet*.

3. Konfigurasi Ufw firewall Pada Backtrack 5 r3

Ufw firewall merupakan *firewall* tambahan yang kompatible dengan sistem operasi *open source*, yang berguna memberi perintah keluar masuknya paket data.

```
#apt-get install ufw
```

```
#apt-get install gufw
```

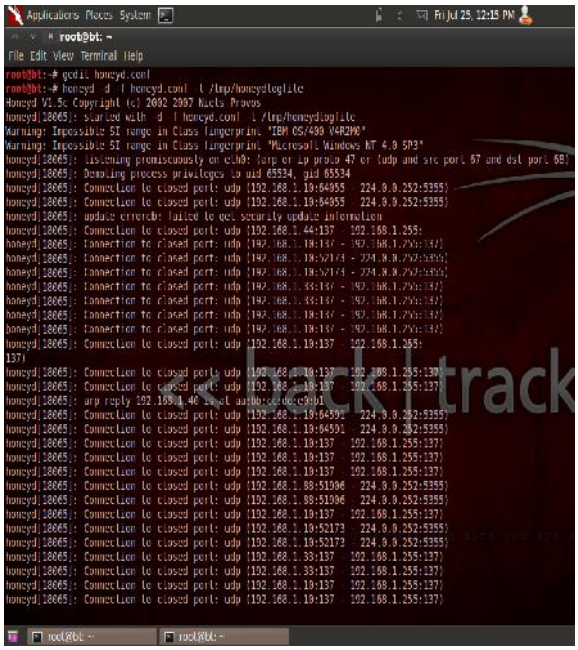
Perintah diatas adalah perintah installasi *ufw firewall* beserta dengan *graphic* yang merupakan tampilan *user interface* dari *ufw firewall*.

B. Operasional

1. Menjalankan Dan Memonitoring Honeyd

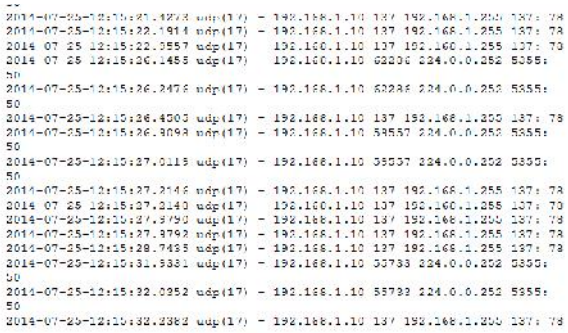
Jalankan *honeyd* pada jendela terminal *Backtrack 5 r3* dengan perintah sebagai berikut

```
# honeyd –d –f honeyd.conf –l /tmp/honeydlogfile
```



Gambar 4.17 Proses monitoring honeyd

Gambar 4.17 menunjukan hasil proses monitoring yang dilakukan oleh *honeyd* yang berperan sebagai server bayangan. *Honeyd* memiliki peranan sebagai server bayangan yang dikorbankan dan memanipulasi penyerang bahwa server yang diserang berstatus aktif atau *up*.



Gambar 4.18 File log Honeyd

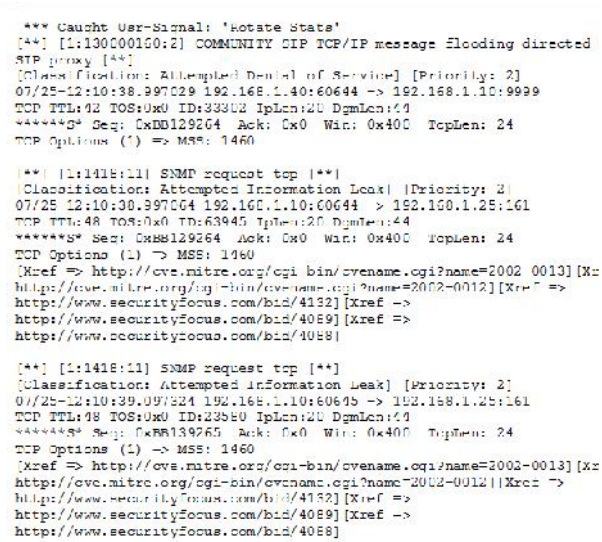
Gambar 4.18 menunjukan *capture screen* yang terdapat pada logfile *honeyd*

2. Menjalankan Dan Memonitoring Snort

Untuk menjalankan *snort* yang digunakan sebagai sistem keamanan jaringan yang memonitoring aktivitas pada jaringan gunakan perintah pada jendela terminal seperti berikut

```
# snort –q –A console –i eth0 –c etc/snort/snort.conf –L ./log
```

Jika *snort* mendeteksi adanya gejala *anomaly* dalam jaringan yang diawasinya, maka snort akan menampilan *alert* ke jendela terminal dan juga merekam semua *alert* ke dalam filelog *snort*. Di saat melakukan monitoring aktivitas jaringan dalam waktu yang sudah ditentukan, *snort* menunjukan hasil kerjanya dengan menunjukan beberapa paket *anomaly* yang di terdeteksi. *Snort* menampilkan penjelasan mengenai paket *anomaly* yang terdeteksi ke dalam jendela terminal pada *backtrack 5 r3* secara detail.



Gambar 4.34

Gambar 4.34 menunjukan hasil monitoring *snort* yang di simpan ke dalam filelog *snort.* Dari hasil monitoring yang didapat terbukti sistem keamanan jaringan pada *snort* mampu mengidentifikasi dan mencegah paket yang bersifat *anomaly* masuk ke dalam sistem jaringan.

C. Optimalisasi

Mengoptimalkan sistem keamanan jaringan yang dibuat dengan memonitoring dan memperbahatui sistem keamanan jaringan yang telah dibuat dengan cara:

1. Mengupdate *honeyd* dengan versi yang terbaru, hal ini dimaksudkan agar *honeyd* yang digunakan tidak ketinggalan jaman.
2. Melakukan *update* pada *snort* jika tersedia. Hal ini dimaksudkan agar database keamanan pada *snort* diperbaharui, sehingga jenis *malware* yang terbaru dapat dideteksi oleh *snort*.
3. Melakukan *update rules* dalam *snort* agar *snort* terupdate dengan *rule – rule* yang terbaru.
4. Menambahkan *tools* keamanan jaringan yang kiranya bisa memperketat sistem keamanan pada jaringan.
5. Melakukan *update* pada *antivirus* yang digunakan, sehingga penyebaran *malware* pada jaringan dapat diminimalisir.

Kiranya itulah beberapa cara dalam mengoptimalkan sistem keamanan jaringan yang telah dibuat, ini dimaksudkan agar sistem keamanan jaringan yang dibuat dapat mengikuti perkembangan jaman yang ada.

V. KESIMPULAN DAN SARAN

A. Kesmipulan

Hasil dari Penelitan yang berjudul menganalisa sistem keamanan Jaringan berbasis intrusion prevention system dan honeypot sebagai pendeteksi dan pencegah malware pada PT, Karya Mitra Nugraha perlu disimpulkan :

1. Honeypot dapat digunakan untuk membantu firewall dan intrusion detection system (IDS) mendeteksi usaha intrusi terhadap sistem jaringan komputer.
2. Honeypot merupakan sebuah sistem yang digunakan hanya untuk mendeteksi adanya serangan yang masuk dalam jaringan tetapi tidak bisa mengatasinya, honeypot hanya mencatat semua aktivitas jaringan tetapi tidak bisa membalas serangan *Bad traffic, dos, ddos,* dan *Attempted recon.*
3. Snort sebagai sistem deteksi yang berhasil mendeteksi dan mencegah serangan yang masuk ke dalam sebuah sistem keamanan jaringan , diantaranya : *Bad traffic, dos, ddos,* dan *Attempted recon.*
4. Ufw firewall yang berguna membantu mengatur lalu lintas pada jaringan, sehingga keamanan pada jaringan lebih ketat.
5. Sistem keamanan yang dibuat dirasa cukup untuk mendeteksi dan juga mencegah serangan yang terjadi dalam sistem keamanan jaringan, diantaranya mampu mencegah serangan berupa : *Bad traffic, dos, ddos,* dan *Attempted recon*

B. SARAN

Perlunya pengembangan lebih lanjut dalam mengoperasikan dan pemeliharan sistem keamanan jaringan pada PT. Karya Mitra Nugraha antara lain :

1. Keamanan jaringan dapat ditingkatkan dengan menambahkan *local rules* pada *snort* sesuai dengan kebutuhan yang dibutuhkan dan mengupdate *rule* yang berasal dari *vendor snort*.
2. Peningkatan performa dengan melakukan *upgrade* pada *hardware server*.
3. Perlunya peningkatan statistik pengunaan grafik untuk mempermudah dalam

menganalisis hasil dari monitoring *honeyd* dan juga *snort*.

Daftar Pustaka

Diebold, P., A. Hess, and G. Schafer. 2005. *A honeypot architecture for detecting and analyzing unknown network attacks.14th Kommunikation in Verteilten Systemen.*

Disky, Sulkarnaen. 2010. Implementasi Honeypot Sebagai Alat Bantu Deteksi Kemanan Jaringan Pada Kantor Pengawasan Bea Dan Cukai. STMIK PalComTech, Palembang.

Hendro, Onno. 2005. *Mahir Administrasi Server dan Router dengan Linux*. Jakarta : PT Elex Media Komputindo.

O'Brien. 2007. *Network Warior*. Springler London Dordereicht New York.

Prayitno , Indra. 2010. *Kupas Tuntas Malware.* Jakarta : Elex Media Komputindo

Rusyamsi. 2011. *Menjadi Dokter Spesialis Komputer.* Jakarta : Kawan Pustaka.

Sukamanji, Anjik dan Rianto. 2008. *Jaringan Komputer*. Yogyakarta : Andi.

Teare, Diane. 2008. *Designing for Cocp internetwork Solutions (DESGN)*. Cisco Press. USA

Scarfone, Karen and Peter Mell.2007. *Guide to Intrusion Detection and Prevention Systems (IDPS).*

Setiawan, Deris. 2005.*Sistem Keamanan Komputer*.Jakarta: PT Elex Media Komputindo.

Utdirartatmo, Firrar. 2005. *Trik Menjebak Hacker dengan Honeypot*. Yogyakarta: Andi.

Verdian, Kimin. 2005. Perancangan Sistem Keamanan Jaringan Komputer Berbasis Intrusion Detection System Dan IpTable Firewall. Universitas Sumatra Utara.