IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS) MENGGUNAKAN SNORT, IP TABLES, DAN *HONEYPOT* PADA ROUTER MIKROTIK

Adhitya Kurniawan*[1], Sayyidah Nabiila Putri[2], Dedy Hermanto[3]
[1,2]STMIK GI MDP; Jl. Rajawali No. 14 Palembang, Telp: (0711) 376400, Fax: (0711) 376360
[3] Program Studi Informatika, STMIK GI MDP, Palembang
e-mail: *[1]adhitya@mhs.mdp.ac.id, [2]sayyidahnabiilaputri@mhs.mdp.ac.id, [3]dedy@mdp.ac.id

Abstrak

Keamanan jaringan ialah kunci utama yang menunjukkan kinerja dan ketersediaan intranetwork. Untuk itu perlu dilakukan peningkatan keamanan jaringan secara terus menerus, seiring dengan makin banyak bermunculannya ancaman keamanan jaringan seperti hacker,cracker, virus, malicious, trojan, worm, dos, spoofing, sniffing, spamming, dan lainnya. Sehingga pengembang sistem membuat sebuah sistem keamanan jaringan dengan berbagai macam metode. Terdapat beberapa metode yang dapat digunakan untuk mengamankan sebuah sistem jaringan diantaranya adalah IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System). Pada pengembangan sistem ini penulis menggunakan metode IPS yang merupakan penyempurnaan dari metode IDS. Sistem ini akan diterapkan pada Router Mikrotik dengan menggunakan IPS yang berbasis pada software Snort, IP Tables, dan Honeypot. Dalam melakukan penerapan ini metodologi penelitian yang digunakan adalah model action research. Action research memiliki tahapan yaitu study literature, diagnosing, action planning, action taking, evaluating, dan learning. Sistem keamanan Intrusion Prevention System (IPS) menggunakan snort, ip tables, dan honeypot, dapat membantu pengguna dalam mengamankan sistem jaringan (lokal / internet) yang digunakan dari ancaman pencurian dan perusakan data serta dapat mengetahui jenis – jenis serangan yang mengancam sistem.

Kata kunci— Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Snort, IP *Tables, Honeypot*, Mikrotik, *Action Research.*

Abstract

Network security is the main of key that indicate performance and availability of intranetwork. Therefore need to do development of network security as constantly, along with more popping out of the threats of network security likes hacker, cracker, virus, malicious, trojan, worm, dos, spoofing, sniffing, spamming, and etcetera. So that developer of system make a network security system with variety of methods. There are some methods that can use for secure network system including IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) . On development of this system the author used IPS method that is the refinement of IDS method. This system will applied on Mikrotik Router with use IPS and based on Snort, IP Tables, and Honeypot softwares. In doing this implementation the research of methodology that used is action research model. Action research model have steps that are study literature, diagnosing, action planning, action taking, evaluating and learning. Network security of Intrusion Prevention System (IPS) for snort, ip tables and honeypot, can help user to secure network system (local / internet) that used from the threat of theft and data destruction and will be able to know the types of threats that will threaten system.

Keywords— *Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Snort, IP Tables, Honeypot, Mikrotik, Action Research.*

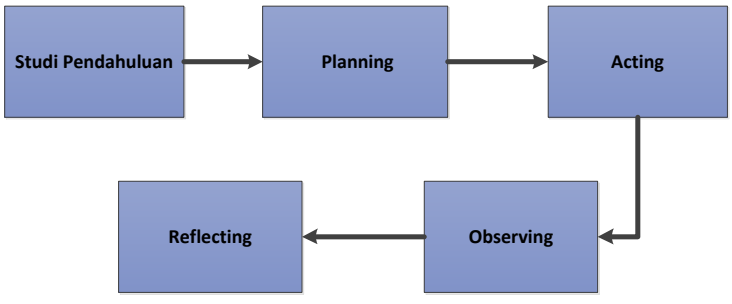
1. PENDAHULUAN

Perkembangan teknologi yang sangat pesat menuntut meningkatnya kualitas keamanan jaringan. Terutama dengan semakin terbukanya pengetahuan tentang *hacking* dan *cracking* yang didukung oleh *tools* - *tools* yang bisa didapatkan dengan mudah dan gratis. Selain itu ancaman keamanan jaringan komputer juga datang dari virus, *malicious*, trojan, *worm*, dos, *spoofing*, *sniffing*, *spamming*, dan lainnya. Hal – hal inilah yang akan mengancam keamanan sebuah sistem jaringan dimana data dapat dengan mudah diambil bahkan dirusak oleh *intruder* atau *attacker*. Keamanan jaringan ialah kunci utama yang menunjukkan kualitas kinerja dan ketersediaan *intranetwork*. Banyak metode yang bisa dilakukan untuk dapat mengamankan sebuah sistem jaringan. Salah satunya adalah dengan menggunakan *Intrusion Prevention System* (IPS). IPS sendiri merupakan kombinasi antara fasilitas *blocking capabilities* dari Firewall dan kedalaman inspeksi paket data dari *Intrusion Detection System* (IDS). Pada saat bekerja, IPS akan membuat akses kontrol dengan cara melihat konten aplikasi sehingga IPS mampu mencegah serangan yang datang dengan bantuan administrator dan akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, selain itu IPS juga akan membandingkan *file checksum* yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga bisa menginterupsi *sistem call*.

Untuk dapat mengimplementasikan IPS maka dibutuhkan routerOS karena untuk dapat membuat sebuah topologi jaringan dibutuhkan setidaknya satu buah routerOS. Terdapat banyak pilihan routerOS diantaranya Vyatta, Mikrotik, Cisco dan lain – lain. Namun, yang dikenal memiliki kualitas tinggi hanyalah Cisco dan Mikrotik. Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang digunakan untuk menjadikan komputer biasa menjadi router *network* yang handal,mencakup berbagai fitur yang dibuat untuk ip *network* dan jaringan *wireless*. MikroTik RouterOS, merupakan sistem operasi Linux *base* yang diperuntukkan sebagai *network* router yang *user-friendly* dan murah. Banyak ISP (*Internet Service Provider*) yang menggunakannya sebagai *Limit bandwidth*, router pada warnet, *gateway* pada kantor, hingga pada kafe sebagai *hotspot*. Diantara kelebihan serta tingkat keamanan yang ditawarkan oleh Mikrotik routerOS akan tetap ada kemungkinan untuk menjadi sasaran para *attacker* atau *intruder.*

2. METODE PENELITIAN

2.1 Metodologi



Gambar 1 Diagram Blok Metode Penelitian

2. 1.1 Studi Pendahuluan (Study Literature)

Tahapan ini merupakan metode pengumpulan data dimana penulis melakukan pencarian dokumen, jurnal, buku, dan majalah serta data dari penelitian sebelumnya yang berkaitan dengan sistem jaringan yang akan dibangun (*intrusion prevention system*, snort, ip *tables*, *honeypot*, dan lain – lain), kemudian mempelajari teori pendukung tersebut [1].

2. 1.2 Model *Action Research* (Penelitian Tindakan)

Pada penelitian ini penulis menggunakan metode penelitian model *action research* (penelitian tindakan) yang memiliki tahapan [1] :

a. *Planning*
   Pada tahap ini, penulis akan mengamati dan mengidentifikasi masalah yang mengancam keamanan jaringan, kemudian menganalisa kelemahan sistem dari penelitian serupa yang pernah dilakukan sebelumnya. Dan dilanjutkan dengan menganalisis kebutuhan sistem serta merancang topologi sistem jaringan yang akan dibangun.
b. *Acting*
   Selanjutnya penulis melakukan penerapan serta pengujian terhadap rancangan topologi sistem yang telah dibuat.
c. *Observing*
   Setelah sistem selesai diterapkan dan telah diuji, pada tahap ini penulis melakukan pengamatan dan mengevaluasi hasil penerapan serta pengujian yang telah dilakukan dengan cara membandingkan hasil penerapan yang dilakukan dengan penelitian sebelumnya. Kemudian menelaah apakah hasil yang didapatkan mampu menyelesaikan permasalahan yang mengancam jaringan khususnya pada router mikrotik yang belum terselesaikan pada penelitan – penelitian sebelumnya.

d. *Reflecting*
   Tahap akhir dari metode ini adalah penulis akan kembali mempelajari proses kerja dari sistem tahap demi tahap, dan hasil penerapan yang telah didapatkan. Kemudian menentukan kesimpulan, kelebihan, serta kekurangan dari sistem yang telah dibangun.

2. 2 Jaringan Komputer

Jaringan komputer dapat diartikan sebagai koneksi antara dua komputer atau lebih yang bisa saling berkomunikasi dan bisa saling berbagi sumber daya. Pada jaringan komputer terdapat model atau cara pembagian *resource*. Berikut model jaringan yang terdapat pada jaringan komputer [2] :

a. *Client – server*
b. *Peer to Peer*

Sedangkan berdasarkan area jangkauannya, jaringan komputer dibedakan menjadi beberapa jenis [2] :

a. *Local Area Network* (LAN)
b. *Campus Area Network* (CAM)
c. *Metropolitan Area Network* (MAN)
d. *Wide Area Network* (WAN)

Selain itu pembagian jaringan juga dibedakan berdasarkan bagaimana jaringan tersebut dihubungkan secara fisik (topologi). Ada beberapa topologi pada jaringan komputer [2] :

a. Topologi *Bus*
b. Topologi *Ring*
c. Topologi *Star*
d. Topologi *Hybrid*

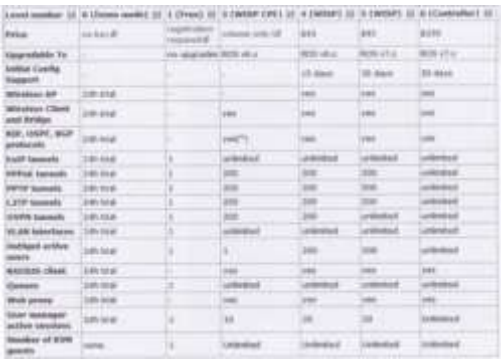
2. *3 Mikrotik*

MikroTik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router *network* yang handal, mencakup berbagai fitur yang dibuat untuk ip *network* dan jaringan *wireless*, cocok digunakan oleh ISP dan *provider hotspot* [3] Router Mikrotik memiliki banyak fitur [4] :

1. Sebagai Internet *Gateway* bagi LAN
2. Sebagai *Access Point (indoor / outdoor)*

3. Sebagai *Intermediary device (routing)*

MikroTik RouterOS ialah sistem operasi router berlisensi, yang mana lisensi tersebut dibagi menjadi beberapa level mulai dari 0 (versi *demo* / *trial*) sampai dengan level 6 yakni level tertinggi dan dapat berperan sebagai *controller*. Berikut gambaran perbedaan setiap level yang dapat dilihat pada Gambar 2 [4]:



Gambar 2 Level dari RouterOS

2. 4 Winbox

Winbox merupakan sebuah *utility* yang digunakan untuk melakukan *remote* ke *server* mikrotik dalam mode GUI. Untuk melakukan konfigurasi pada router mikrotik dengan menggunakan *winbox* dapat dilakukan dengan 2 cara, yakni melalui GUI ataupun *CommandLine*. Berikut ini adalah beberapa fungsi dari *winbox* [5] :

1. Melakukan pengaturan mikrotik router
2. Mengatur *bandwidth* pada jaringan internet
3. Melakukan pemblokiran terhadap situs
4. Dan lain – lain.

2.5 Intrusion Prevention System

Intrusion Prevention System (IPS) adalah *host* yang berbasis aplikasi yang melindungi sistem dari serangan luar dengan menganalisa pesan yang melewatinya. IPS bekerja dengan beberapa cara [6] :

1. Analisis pesan yang masuk.
2. Mencocokan pesan masuk dengan *signature*.
3. Mencocokan data yang melanggar aturan domestik / internasional.
4. Mens*can* perangkat jaringan.
5. Penolakan layanan serangan
6. Pengintaian aktivitas komputer dan jaringan.

IPS memiliki 2 cara untuk menangkal serangan [6] :

1. *Host-Based Approach*
   Melakukan pengecekan untuk aktivitas yang mencurigakan yang datang langsung dari *host* komputer yang terletak di operator *operating system*.
2. *Network Based Approach*
   Memfokuskan pada jaringan dengan cara menggabungkan keamanan jaringan sehingga menghasilkan keamanan jaringan dan *clients*.

Selain itu, pada IPS terdapat tiga pola pengenalan *signature* [6]:

a. *Pattern- Based Prevention*
   Mengenali *pattern* yang direpresentasikan dengan *text* atau *binary string*.
b. *Anomaly – Based Prevention*
   Pengguna harus membuat sebuah profil yang mendefinisikan dengan jelas bagaimana digolongkan sebagai aktivitas normal dan sebaliknya.

c. *Behavior – Based Prevention*
Model yang menjelaskan tegas aktivitas dalam beberapa kelas untuk mengenali *malicious threat*.

2.6 Snort

Snort ialah sebuah aplikasi atau *tool* keamanan yang berfungsi mendeteksi *intrusi – intrusi* jaringan (penyusupan, penyerangan, pemindaian dan beragam bentuk ancaman lainnya) sekaligus melakukan pencegahan. Snort sangatlah handal dalam membentuk *logging* paket – paket dan analisis trafik – trafik secara *real time* dalam jaringan berbasis TCP/IP yang sangat berguna dalam merespon insiden penyerangan terhadap *host-host* jaringan [7].

Gambar 3 *Output* Snort

Secara prinsip snort memerankan 3 fungsi utama [7] :

1. Sebagai penangkal program – program *sniffer* (seperti tcpdump).
2. Sebagai *packet logger* (berguna men-*debug* trafik – trafik jaringan).
3. Sebagai sistem pencegah penyusupan untuk sistem jaringan.

Snort bekerja menganilisis protokol, pencocokan / pencarian konten, dan secara aktif digunakan untuk menangkal dan secara pasif mendeteksi ancaman tertentu seperti [7]:

1. *Buffer overflow*
2. *Stealth port scan*
3. Serangan aplikasi berbasis *web*
4. SMB *probe*
5. Usaha – usaha *fingerprint* OS
6. Dan lain – lain.

2.7 Honeypot

Honeypot merupakan sumber sistem informasi yang didesain dengan tujuan untuk mendeteksi, menjebak usaha percobaan penetrasi kedalam [8]. *Honeypot* memiliki fitur monitoring untuk memantau aktivitas penyerang ketika masuk ke dalam sistem *honeypot.* Aktivitas yang bisa diketahui diantaranya adalah ketika *port* yang diserang, *command* yang diketik oleh penyerang, dan perubahan yang dilakukan penyerang di *server* palsu *honeypot.* Hal ini dapat dimanfaatkan oleh *Network* Administrator untuk melakukan pencegahan dini [8].
Honeypot memiliki 2 macam tipe berdasarkan fungsi peletakkannya [8], yaitu:

a. *Production Honeypot*, *honeypot* tipe ini diletakkan dalam jaringan produksi.
b. *Research Honeypot*, *honeypot* tipe ini didesain untuk mendapatkan informasi mengenai aktivitas - aktivitas penyerang atau penyusup.

Honeypot juga diklasifikasikan berdasarkan tingkat interaksi yang dimilikinya, diantaranya [8]:

a. *Low-Interaction Honeypot*
Honeypot yang didesain untuk mensimulasikan *service* (layanan) seperti pada *server* yang asli dengan layanan - layanan tertentu (misal SSH, HTTP, FTP) .

b. *High-Interaction Honeypot,*
Pada sistem operasi dimana penyerang berinteraksi langsung dan tidak ada batasan yang membatasi interaksi tersebut.

Sebuah *honeypot* biasanya akan ditempatkan pada lokasi berikut [8]:

a. Penempatan berhadapan langsung dengan Internet.
b. Penempatan di belakang *firewall* .
c. Penempatan pada DMZ (*Demiliterized Zone).*

2.8 IP Tables Firewall

IP *Tables Firewall* adalah suatu *tools* dalam operasi linux yang berfungsi sebagai alat untuk melakukan penyaringan terhadap lalu lintas data. *IP tables firewall* digunakan untuk melakukan seleksi terhadap paket – paket yang datang baik itu *input* ataupun *output* maupun *forward* berdasarkan IP *address*, identitas jaringan, *port, source* (asal), *destination* (tujuan), protokol yang digunakan bahkan berdasarkan koneksi pada paket data yang diinginkan [9]. IP *Tables Firewall* memiliki 3 aturan *filtering dan target*, diantaranya [9] :

Tabel 1 Aturan *Filtering* IP *Tables Firewall*

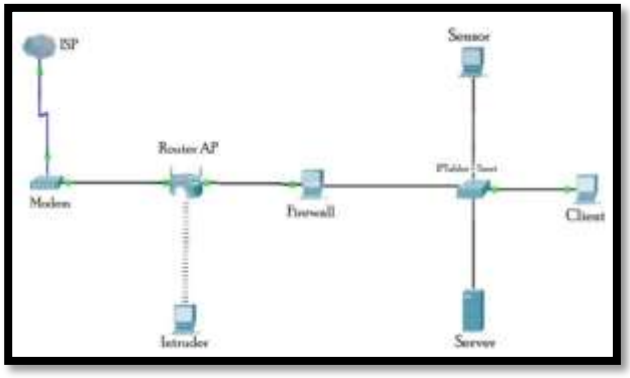
1.	***Input***	Mengatur paket data yang memasuki *firewall* dari arah intranet ke internet.
2.	***Output***	Mengatur paket data yang keluar dari *firewall* baik dari arah intranet ke internet.
3.	***Forward***	Mengatur paket data yang melintasi *firewall* dariarah intranet internet atau sebaliknya.

Tabel 2 Target IP *Tables Firewall*

1.	***Accept***	Akses diterima dan diizinkan melewati *firewall.*
2.	***Reject***	Akses ditolak dan koneksi dari *client* yang melewati *firewall* akan terputus.
3.	***Drop***	Akses diterima tapi paket data akan langsung dibuang oleh kernel sehingga pengguna tidak mengetahui koneksinya dibatasi *firewall*

2.9 Analisis Kebutuhan Sistem Jaringan

Penulis mengidentifikasi masalah-masalah pokok yang berkenaan dengan ancaman jaringan yang ada serta menganalisa kekurangan sistem dari penelitian sebelumnya. Akan tetapi peneliti sebelumnya menggunakan metode yang berbeda yakni *Intrusion Detection System* (IDS) [10]. Berikut ini merupakan rancangan topologi yang telah dibuat pada penelitian sebelumnya.



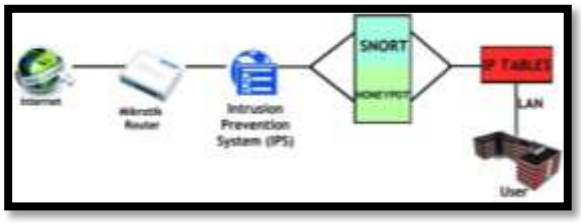
Gambar 4 Rancangan Topologi IDS

Pada tahap implementasi yang dilakukan oleh peneliti sebelumnya terhadap topologi diatas, maka didapatkan beberapa kekurangan, yaitu [10] :

1. Sistem yang telah dibuat berdasarkan topologi tersebut tidak terlalu sensitif terhadap serangan - serangan yang memasuki sistem.
2. Dari sisi pencegahan serangan, sistem tersebut tidak memiliki kinerja yang terlalu baik sehingga serangan terhadap sistem masih bisa lolos.

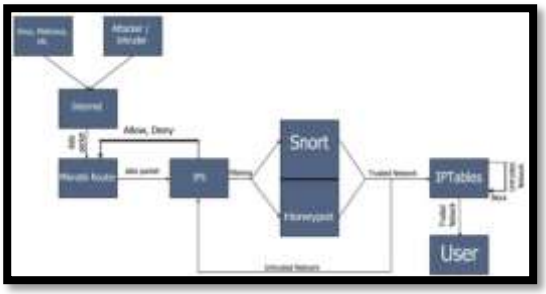
2.10 Perancangan Sistem

Berdasarkan kekurangan dari rancangan topologi pada Gambar 4 , maka penulis membuat rancangan topologi baru dengan menggunakan kekurangan tersebut sebagai acuan. Berikut ini merupakan rancangan topologi yang dibuat penulis untuk melakukan implementasi IPS pada router mikrotik dengan menggunakan snort, *honeypot,* dan ip*tables* :



Gambar 5 Rancangan Topologi

Selanjutnya penulis akan membuat rancangan urutan proses kerja dari sistem tersebut dan menggambarkan kinerja IPS pada sistem keamanan jaringan di router mikrotik yang akan dibantu penggunaan *snort,* IP t*ables,* dan juga *honeypot* dalam bentuk diagram blok.

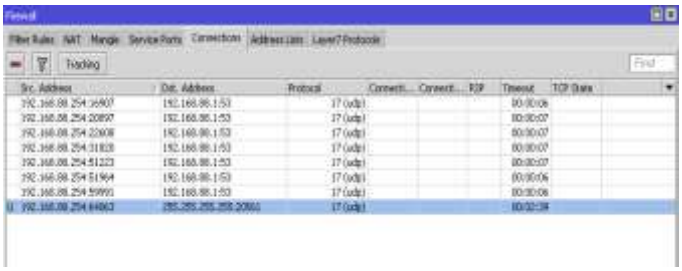


Gambar 6 Diagram Blok Proses Kerja

3. HASIL DAN PEMBAHASAN

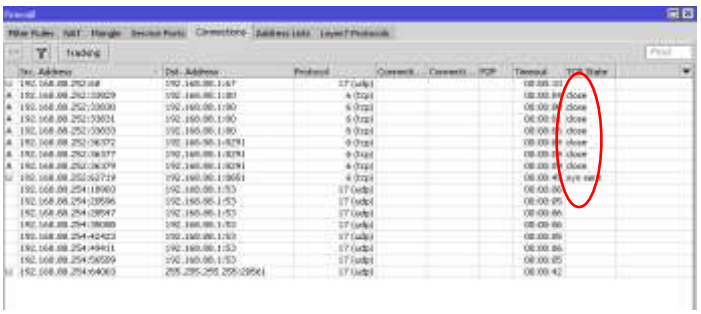
3.1 Pengujian Mikrotik

Pengujian pada mikrotik akan dilakukan dengan melakukan pengujian *scan* ip mikrotik melalui nmap untuk mengetahui *port – port* mana saja yang memungkinan dapat diakses oleh *intruder*. Berikut ini adalah tampilan dari *submenu firewall* sebelum dilakukan pengujian.



Gambar 7 Tampilan *Submenu Firewall*
pada Mikrotik

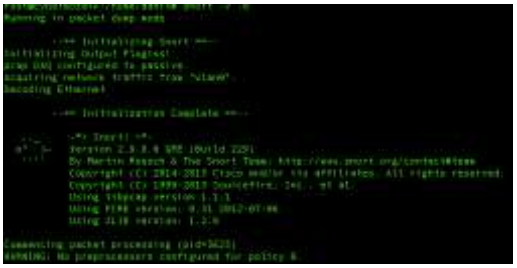
Selanjutnya penulis akan melakukan pengujian *scan* ip mikrotik melalui nmap. pada Gambar 8 adalah tampilan *sub menu firewall* pada saat dilakukan proses *scanning* ip mikrotik melalui nmap maka *firewall* mikrotik melakukan beberapa pemblokiran ip yang mencoba mengakses melalui *port – port* tersebut dengan cara meng-*close* setiap paket data yang melewatinya.



Gambar 8 Tampilan *Submenu Firewall* ketika
Proses S*canning IP* melalui Nmap

3.2 Pengujian Snort

Pada snort penulis melakukan pengujian *ping flood server*. Serangan *ping flood server* dapat menyebabkan *server* yang menjadi target tidak dapat lagi melakukan pengiriman paket kembali ke dalam jaringan, hal itu disebabkan karena *server* dipenuhi oleh paket – paket ICMP. Berikut ini merupakan tampilan snort tanpa adanya serangan :

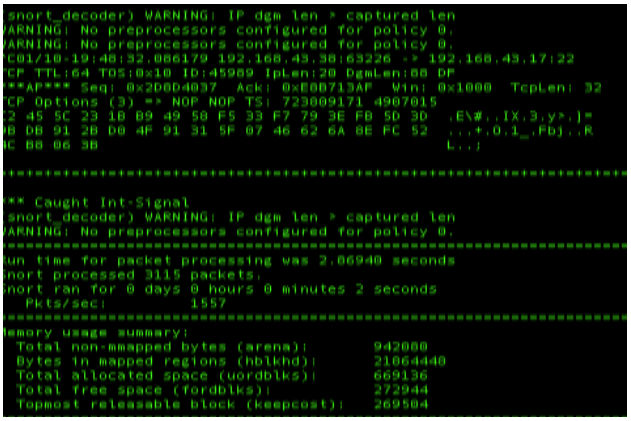


Gambar 9 Tampilan Snort Tanpa Serangan

Kemudian penulis melakukan pengujian *test ping replay* pada snort dengan menggunakan ip 192.168.43.17 maka snort akan memberitahukan bahwa ip 192.168.43.38 mendapatkan respon *echo replay* dari ip 192.168.43.17. Gambar 10 merupakan tampilan saat proses *test ping reply* dilakukan.

Gambar 10 Tampilan Snort saat *Test Ping Reply*

Selanjutnya adalah melakukan pengujian *ping flood server*, dan penulis akan mendapatkan *log / pemberitahuan* bahwa ip 192.168.43.38 melalui *port* 63226 melakukan serangan dengan IP dmg len yang termasuk dalam snort *rules* snort_decode.



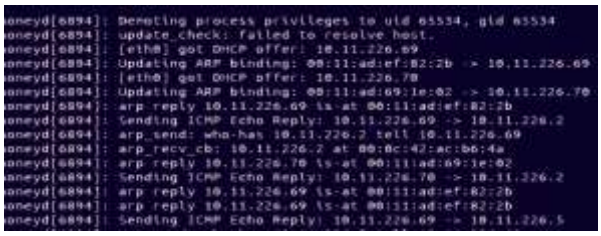
Gambar 11 Tampilan Snort saat *Ping Flood Server*

3.3 Pengujian Honeypot

Pada pengujian *honey*pot penulis melakukan salah satu pengujian sesuai dengan *rule* yang telah dibuat sebelumnya yaitu *test ping replay* . Berikut tampilan dari sisi *attacker* dimana IP 10.11.226.69 dan 10.11.226.70 telah berhasil melakukan *test ping* terhadap sistem.

Gambar 12 Tampilan dari sisi A*ttacker* pada
saat *Test Ping Reply*

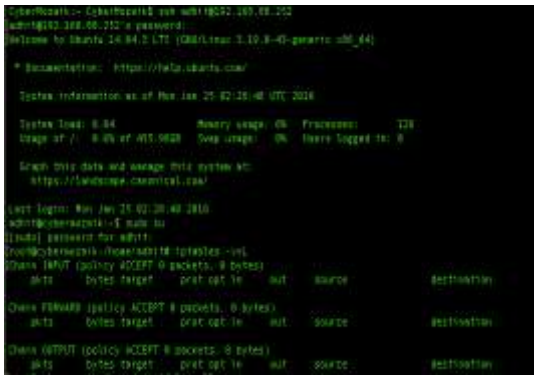
Disaat yang bersamaan, ketika *attacker* melakukan kegiatan *test ping replay* maka honeypot akan memberikan laporan kepada administrator *server*. Pada *honeypot* akan terlihat bahwa arp_send dengan IP 10.11.226.5 ke IP 10.11.226.69 dan *honeypot* memberikan respon *replay* dari IP 10.11.226.69 ke IP 10.11.226.5 agar *attacker* berfikir bahwa ip *server up*.



Gambar 13 Tampilan dari sisi Administrator
Server saat *Test Ping Reply*
dilakukan A*ttacker*.

3.4 Pengujian IP *Tables*

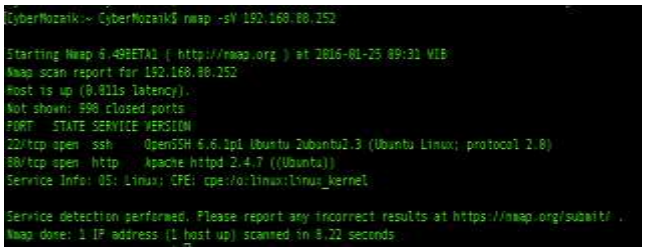
Gambar 14 adalah tampilan ip*tables* ketika dijalankan dengan menggunakan salah satu konfigurasi yang telah dibuat oleh penulis. Pada pengujian ipt*ables* penulis akan melakukan pengujian *scan* ip melalui nmap.



Gambar 14 Tampilan IP *Tables* dengan
Salah Satu *Rules*

Pada Gambar 15 merupakan tampilan ip*tables* yang belum dikonfigurasi ketika dilakukan pengujian *scan* ip melalui nmap. Dapat dilihat pada gambar tersebut, ip *tables* menampilkan informasi mengenai *operating system* serta *port – port* yang terbuka. Hal ini dapat menyebabkan

penyerang menemukan celah untuk melakukan penyerangan dan masuk ke server melalui *port – port* tersebut.



Gambar 15 Tampilan IP *Tables* yang belum Dikonfigurasi

Untuk mencegah hal itu pada tahap pengujian selanjutnya, penulis melakukan konfigurasi pada ip*tables* sehingga ketika penyerang mencoba melakukan *scan* ip melalui nmap pada ip*tables.* Informasi yang akan didapat oleh si penyerang hanyalah informasi tentang *port – port* yang tertutup. Gambar 16 adalah tampilan dari proses konfigurasi yang dilakukan penulis pada ip*tables.*

Gambar 16 Tampilan IP *Tables* saat Dikonfigurasi

4. KESIMPULAN

Kesimpulan yang didapatkan penulis dari implementasi dan pengujian sistem adalah sebagai berikut :

1. Penerapan *intrusion prevention system* (IPS) pada router mikrotik yang dikombinasikan dengan snort, *honeypot*, dan ip *tables* dapat berjalan dengan baik untuk mengamankan sebuah sistem jaringan.
2. Aktivitas – aktivitas yang mengancam keamanan sistem akan terdeteksi dengan cepat dan mudah, sehingga tindakan pencegahan dapat dilakukan sedini mungkin.
3. *Server* Administrator dapat mengecek ulang *log – log* paket data yang berusaha mengakses sistem, sehingga apabila terdapat intrusi yang belum terdefinisi di sistem *server* administrator dapat meng-*update signature* / konfigurasi sistem.

5. SARAN

Dalam pembuatan sistem keamanan ini belum sempurna. Sehingga masih terdapat banyak kekurangan. Adapun saran yang dapat direkomendasikan oleh penulis adalah sebagai berikut :

1. Pengembangan sistem ini dapat diimplementasikan ke sistem operasi yang berbeda selain ubuntu *server*.
2. Melakukan pengembangan menggunakan metode pengamanan jaringan selain metode *Intrusion Prevention System* (IPS).
3. Melakukan pengembangan sistem keamanan jaringan dari satu arah menjadi dua arah yaitu sistem keamanan yang tidak hanya mengamankan jaringan publik ke jaringan lokal, akan tetapi juga mampu melindungi jaringan lokal ke jaringan publik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu dalam proses pembuatan jurnal ini, terutama kepada Bapak Dedy hermanto, S.Kom, M.T.I yang telah banyak membimbing penulis dalam pengerjaan skripsi hingga selesai.

DAFTAR PUSTAKA

[1] Arikunto, Suharsimi 2010, *Prosedur Penelitian Suatu Pendekatan Praktik*, PT Rineka Cipta, Jakarta

[2] Sto 2014, *100% Networking+ Ilegal*, Jasakom, Jakarta.

[3]Mikrotik.co.id 2005, *MikroTik RouterOS*, Diakses 04 Agustus 2015 , dari http://mikrotik.co.id/

[4] Towidjojo, Rendra 2013, *Mikrotik Kung Fu*, Jasakom, Jakarta

[5] Delhendro.com 2012, *Pengertian dan Fungsi Winbox*, Diakses 25 Januari 2016, dari http://www.delhendro.com/

[6] Suhindra, Denys, dan M Bagas Syarafah 2013, *IPS*, Politeknik Telkom Indonesia, Bandung

[7] Rafiudin, Rachmat 2010, *Mengganyang Hacker dengan SNORT* , Andi Offset, Yogyakarta.

[8] Tambunan, Bosman; dan Willy Sudiarto Raharjo, dan Joko Purwadi 2013, *Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System*, Teknik Informatika, Universitas Kristen Duta Wacana

[9] Firdaus, Muhammad Fajar 2014, *Pengertian Firewall, NAT dan Proxy Server*, Diakses 03 Agustus 2015, dari http://www.slideshare.net/

[10] Satria, Muhammad Nugraha 2010, *Implementasi Intrusion Detection System untuk Filtering Paket Data*, Teknik Informatika, Universitas Islam Negri Syarif Hidayatullah Jakarta.