INTRUSION DETECTION PREVENTION SYSTEM (IDPS) PADA LOCAL AREA NETWORK (LAN)

Oleh:
Didit Suhartono[1], Andi Dwi Riyanto[2],
Yogi Widy Astomo[3]
Dosen Program Studi Sistem Informasi, STMIK Amikom Purwokerto
Dosen Program Studi Teknik Informatika, STMIK Amikom Purwokerto
Mahasiswa Program Studi Teknik Informatika, STMIK Amikom Purwokerto

ABSTRAK

Penelitian ini berjudul "Intrusion Detection Prevention System Local Area Network (LAN)" yang bertujuan untuk memproteksi jaringan dari usaha- usaha penyusupan yang dilakukan oleh seorang intruder. Metode yang digunakan pada penelitian ini adalah menggunakan metode kerangka pikir sebagai acuan dari tahap- tahap penelitian yang penulis lakukan. IDS difungsikan sebagai pendeteksi adanya serangan sesuai rule yang ada kemudian pesan peringatan disimpan dalam database dan dikirim via sms kepada seorang network administrator, sedangkan Firewall digunakan sebagai packet filtering dengan cara menentukan security policy yang dinilai penting. Hasilnya adalah ketika IDS memberikan pesan peringatan ketika ada serangan, seorang network administrator dapat memblok adanya serangan tersebut dengan cara manual dengan firewall, ataupun firewall akan memblok sendiri serangan tersebut sesuai dengan security policy yang diterapkan oleh network adminisrator sebelumnya.

Kata kunci : *IDS, Firewall, Perkembangan Teknologi*

A. PENDAHULUAN

Pada era globalisasi sekarang kemajuan teknologi dan tingkat kebutuhan masyarakat akan teknologi semakin tinggi. Sebab dengan adanya teknologi, informasi dan komunikasi manusia dapat memperoleh dan memberi informasi dari atau kepada orang lain. Teknologi pada era sekarang tidak lagi menjadi kebutuhan sekunder melainkan menjadi sebuah kebutuhan primer yang mendukung banyak sisi aspek kehidupan. Dengan berkembang pesatnya teknologi, proses pertukaran informasi menjadi semakin cepat, dengan faktor tersebut, keamanan sebuah teknologi jaringan menjadi taruhannya

Pada sisi lain timbul masalah serius yaitu faktor keamanannya, namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun. Ini disebabkan karena kepedulian masyarakat yang sangat kurang terhadap sistem keamanan jaringan.

Dalam perkembangan teknologi sekarang yang sudah semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat *free* dan ada pula yang dikomersilkan. Kemudian dari sisi *software* pendukung pun sudah banyak *tool-tool* yang bersifat *free* yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan *intruder* dan *attacker.*

Network security is an extremely important today. The more complex and the number of computers connected together yield gaps that vulnerable on a network. Administrator is a subject that plays an important role in protecting the web server. However, administrator have the parameters that may limited by humane limitations to protect web servers, such as, illness, limit working hours, negligence, etc (Ariewijaya, 2011).

Keamanan jaringan lokal ini bergantung sepenuhnya terhadap bagaimana seorang network administrator merespon dengan cepat sebuah serangan yang terjadi. Tapi network administrator hanyalah seorang manusia yang terbatas akan waktu. Seorang network administrator tidak dapat mengawasi seluruh jaringan secara terus- menerus. Maka dari itu dibutuhkan sebuah sistem yang dapat membantu network administrator untuk digunakan sebagai monitor trafik jaringan dengan memanfaatkan IDS (*intrusion detection system*).

B. TINJAUAN PUSTAKA

1. INTRUSION DETECTION SYSTEM

Menurut Ariyus (2007) Intrusion Detection System (IDS) adalah suatu perangkat lunak (software) atau suatu sistem perangkat keras (hardware) yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan. Serangan yang terjadi terhadap jaringan komputer selalu meningkat pada infrastruktur keamanan

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

perusahaan dan organisasi yang menggunakan komputer sebagai alat bantu untuk menyelesaikan pekerjaan. Tipe dasar dari IDS adalah :

a. *Rule based system*

Berdasarkan pada *signature* dan *rule* yang tersimpan di *database*. Jika IDS mencatat lalu-lintas yang sesuai dengan *rule* dan *signature* yang ada, maka langsung dikategorikan sebagai serangan.

b. *Adaptive system*

Mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan *database* yang ada,tetapi juga membuka kemungkinan untuk mendeteksi bentuk-bentuk serangan baru.

2. SECURITY, OTENTIKASI DAN METODE AKSES

Otentikasi dan pengaturan mode akses merupakan dua buah metode yang lazim digunakan untuk mengamankan jaringan komputer. Setiap user yang akan mengakses jaringan komputer harus menyatakan identitas diriya melalui proses yang disebut otentikasi. Proses otentikasi yang paling lazim yaitu dengan mengetikkan login dan password. Teknik otentikasi yang lebih canggih yaitu dengan pengenalan sidik jari, retina mata, pengenalan suara dan lain-lain.

a. Firewall

Menurut Marco Van Basten (2009) Firewall merupakan alat untuk mengimplementasikan kebijakan security (security policy). Sedangkan kebijakan security, dibuat berdasarkan pertimbangan antara fasilitas yang disediakan dengan implikasi security-nya. Semakin ketat kebijakan security, semakin komplekskonfigurasi layanan informasi atau semakin sedikit f.asilitas yang tersedia di jaringan.

Firewall mempunyai beberapa tugas:

1. Harus dapat mengimplementasik an kebijakan security di jaringan (site security policy). Jika aksi tertentu tidak di perbolehkan oleh kebijakan ini, maka firewall harus meyakinkan bahwa semua usaha yang mewakili operasi tersebut harus gagal atau digagalkan. Dengan

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

demikian, semua akses ilegal antar jaringan (tidak diotoritaskan) akan ditolak.

2. Melakukan *filtering* yaitu dengan mewajibkan semua trafik yang ada untuk dilewatkan melalui *firewall* bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam konteks ini, aliran paket data dari/menuju *firewall* bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam nomor port, atau arahnya, dan disesuaikan dengan kebijakan *security*.
3. *Firewall* juga harus dapat merekam/mencatat even-even mencurigakan serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan *security*.

b. Intrusion Prevention System

Menurut Deris Setiawan, *Intrusion Prevention System* (IPS) adalah pendekatan yang sering digunakan *system* keamanan komputer, IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket semua paket dan serta mengenali paket dengan sensor, disaat *attack* telah teridentifikasi, IPS akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak seperti layaknya *firewall* yang akan melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan *signatures* untuk mendeteksi di aktifitas trafik di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound- outbound*) dapat di cegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal.

Secara umum, ada dua pendekatan yang dapat digunakan untuk mendeteksi ancaman *attack* ini yaitu *Host-based approach*, *Network-based approach*. *Host-based approach* adalah teknologi terkini yang dipakai dan sangat popular, dapat melakukan mengecekan untuk aktifitas

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

yang mencurigakan langsung dari *host computer* tersebut di level *operating system*nya, dan *Network- based approach* sangat terfokus pada *network- based*, dengan gabungan komponen keamanan lainnya dapat menjadi solusi yang menyeluruh pada *system* keamanan. Namun implementasi IPS pada jaringan *internetwork* sangat dipengaruhi oleh beberapa faktor lainnya. Faktor teknis menjadi kendala utama dalam implementasi ini, karena IPS adalah salah satu bagian dalam *system* keamanan yang dibangun, hendaknya memperhatikan isu-isu yang ada dalam jaringan komputers.

C. HASIL PENELITIAN SEBELUMNYA

Hasil penelitian sebelumnya yang bertema Keamanan jaringan yang menjadi acuan dan referensi penyusunan dalam menyusun laporan ini penulis mengambil dari jurnal dan penelitian IT, antara lain :

1. Penyusunan yang dilakukan oleh Micky Sandy Pratama (2012) Teknik Informatika Universitas Pembangunan Nasional Veteran Jawa Timur yang mengambil judul "PENGAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE IPS (*INTRUSION PREVENTION SYSTEM*) TERHADAP SERANGAN BACKDOOR DAN SYNFLOOD BERBASIS SNORT INLINE". Tujuan penelitian ini adalah untuk mampu mengaplikasikan pendeteksian dan pencegahan serangan-serangan dengan metode IPS (*Intrusion Prevention System*).Penelitian ini ditujukan untuk mendeteksi dan mencegah serangan- serangan *backdoor* dan *synflood*. Pengujan dilakukan dengan memanfaatkan VMWare sebagai simulasi jaringan komputer.
2. Penyusunan yang dilakukan oleh Ariewijaya (2011) Teknik informatika STMIK Amikom Yogyakarta yang mengambil judul "OPTIMALISASI NETWORK SECURITY DENGAN MENGKOMBINASIKAN *INTRUSION DETECTION SYSTEM* DAN *FIREWALL* PADA WEB SERVER". Tujuan penelitian ini adalah untuk membantu mengawasi jaringan server, utomatisasi tindakan serta memberikan informasi yang tepat dan cepat

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

mengenai serangan dan ancaman dari scanning port dan DOS attack.Pengujian dilakukan sebanyak empat (4) kali dengan pengklasifikasian pengujian sebelum implementasi dan pengujian setelah implementasi sistem. Skenario pengujian dilakukan dengan menghubungkan kedua komputer dengan kabel UTP, dimana komputer *client* sebagai penyerang dan satunya sebagai komputer *server*. Komputer *client* akan mencoba melakukan serangan ke komputer *server*, dengan kondisi *server* dengan IDS yang aktif dan non-aktif untuk membuktikan apakah IDS benar-benar mampu melindungi *server* atau tidak.

3. Penyusunan yang dilakukan oleh Abraham Nethanel Setiawan Junior,Agus Harianto, Alexander (2009) yang mengambil judul "PERANCANGAN DAN IMPLEMENTASI *INTRUSION DETECTION SYSTEM* PADA JARINGAN NIRKABEL BINUS *UNIVERSITY*".Tujuan penelitian ini adalah sebagai solusi yang dapat digunakan untuk membantu pengatur jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut.

D. METODE PENELITIAN

1. Metode Pengumpulan Data

Metode pengumpulan data yang dipakai adalah penelitian kepustakaan dan dokumentasi

a. Studi Pustaka

Menurut Moh. Nazir (2011), Studi pustaka merupakan teknik engumpulan data dari sumber-sumber seperti buku, dokumen, publikasi atau internet. Sumber tersebut yang selanjutnya menjadi referensi penulis dalam pembuatan sistem.

b. Dokumentasi

Menurut Sugiyono (2011), Dokumentasi merupakan catatan peristiwa yang sudah berlalu. Dokumen ini bisa berbentuk tulisan, gambar, atau karya-karya dari seseorang.

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

2. Alat dan Bahan Penelitian

Adapun alat dan bahan yang digunakan untuk penelitian ini baik itu *hardware* maupun *software* adalah sebagai berikut :

1. Perangkat keras (*hardware*)
   a. 3 unit laptop
   b. 2 kabel *crossover*, 1 kabel *straightover*
   c. 1 buah *wireless access point*
2. Perangkat lunak (*software*)
   a. Sistem Operasi Ubuntu Desktop 12.04 LTS
   b. Sistem Operasi
   c. Backtrack 5R3
   d. Sistem Operasi
   e. Windows 7
   f. Iptables
   g. Snort
   h. Gammu

E. KONSEP PENELITIAN

1. ANALISIS

Tahap awal dari kerangka piker ini adalah analisi. Pada tahap ini penulis mengidentifikasi konsep snort IDS, Barnyard, BASE, dan Firewall. Kemudian mengumpulkan dan mengidentifikasi seluruh kebutuhan dari system tersebut sehingga dapat diperjelas dan terperinci. Tahap-tahap ini meliputi :

a. Identifikasi yaitu untuk mengidentifikasi permasalahan yang dihadapi sehingga dibutuhkan proses pengembangan sistem.
b. Pemahaman yaitu untuk memahami struktur dan mekanisme kerja sistem yang akan dibangun atau dikembangkan.
c. Analisis yaitu untuk menganalisis dan menyimpulkan elemen-elemen atau komponen dan kebutuhan sistem yang akan dibangun atau dikembangkan

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

2. PERANCANGAN

a. Perancangan arsitektur sistem Perancangan arsitektur sistem bertujuan untuk menggambarkan interaksi antar komponen tersebut.
b. Komponen aplikasi Komponen aplikasi merupakan detail dari komponen yang ada pada sistem baik perangkat lunak maupun perangkat keras..

3. IMPLEMENTASI

a. Penerapan rule digunakan untuk menerapkan rule pada sistem operasi yang nantinya digunakan sebagai mesin sensor.
b. Penerapan Iptables Penerapan Iptables digunakan untuk menerapkan security policy bersamaan pada mesin sensor.

F. HASIL DAN PEMBAHASAN

METODE PENGEMBANGAN

1. ANALISIS

Pada bagian ini dijelaskan bagaimana cara melakukan konfigurasi snort IDS dan firewall. Pada tahap anaalisis ini dibagi menjadi empat yaitu identifikasi, pemahaman, analisis dan laporan.

a. Identifikasi

Tujuan diikembangkannya sistem proteksi dari penyusup yang terdiri dari dua komponen yaitu:

a) Intrusion detection system (IDS) digunakan untuk mencatat atau mengetahui jenis serangan, IDS sendiri memiliki banyak perbedaan berdasarkan pada kemampuan yang dimiliki masing- masing pendeteksi penyusup. Dalam penelitian ini, penulis membahas tentang Network intrusion detection system (NIDS) dimana NIDS akan memantau semua trafik jaringan pada segmen dimana sensor terpasang aktif sehingga dapat memberi peringatan secara cepat jika menemui sebuah trafik/aktifitas-aktifitas berdasarkan rule/aturan yang telah dibuat.
b) Firewall dapat digunakan untuk mengatur mekanisme pencegahan serangan dengan cara memblok sebuah aktifitas. Kedua komponen diatas

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

dapat digabungkan sebagai langkah pencegahan terhadap serangan yang dapat dideteksi sedini mungkin oleh sistem IDS ketika seorang intruder melakukan penyerangan dari jaringan luar ke jaringan internal

b. Pemahaman

Hasil identifikasi diatas membutuhkan pemahaman yang teliti agar dapat menghasilkan sebuah rancangan yang tepat dan baik untuk digunakan. Dengan menggunakan penelitian kepustakaan dan dokumentasi, penulis memanfaatkan perpustakaan dan internet untuk mengumpulkan data-data serta informasi- informasi dari berbagai sumber baik itu dalam bentuk buku, makalah, literatur, artikel, jurnal dan situs-situs web yang ada kaitannya mengenai topik yang dibahas oleh penulis sehingga hasilnya dapat digunakan untuk memahami permasalahan yang terjadi untuk merumuskan solusi efektif dalam menyelesaikan berbagai perumusan permasalahan.

c. Analisa

Hasil pemahaman akan digunakan sebagai masukan untuk menganalisis sistem solusi yang dapat mengatasi rumusan permasalahan. Hasilnya adalah :

1) Penulis menggunakan Snort, Barnyard, BASE, Firewall, Gammu yang di integrasikan agar antar komponen tersebut dapat menghasilkan sebuah sistem proteksi sistem keamanan jaringan. Penulis menggunakan sistem operasi Linux yaitu Ubuntu 12.04 LTS. Snort bertugas untuk melakukan pencatatan dan pemberitahuan saat mendeteksi aliran paket data yang dianggap mencurigakan atau illegal didasarkan pada rule yang telah dibuat. Jika diketahui ada paket data ilegal maka Snort akan memicu sebuah alert atau peringatan.

a) Jika terjadi aktifitas yang dianggap ilegal, Barnyard bertugas untuk menangani file output dari snort, sehingga snort dapat berfokus untuk melakuakan sensor terhadap lalu lintas jaringan. Barnyard juga bertugas memformat *output file* snort agar dapat di manfaatkan untuk keperluan analisis. Base (*Basic analysis security engine*) bertugas

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

untuk merepresentasikan *log file* Snort kedalam format berbasis GUI (*Graphical user interface*) yaitu dalam bentuk web yang lebih *user friendly* sehingga mudah untuk proses analisis. Gammu berfungsi sebagai pengirim notifikasi via sms kepada seorang *network administrator* ketika Snort mendeteksi adanya aktifitas illegal *Firewall* digunakan untuk memblok paket data baik secara manual oleh *network administrator* maupun secara otomatis setelah diatur *security policy*nya.

Berikut adalah kesimpulan dari sistem yang akan dibangun :

Tabel 1 Spesifikasi sistem

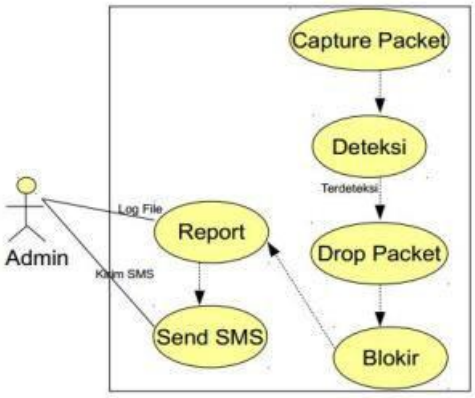
Sistem	**Keterangan**
Intrusion Detection Prevention System	Terdiri dari NIDS yang berfungsi untuk memonitor trafikdalam jaringan lokal dan *Firewall* digunakan
Client	Difungsikan sebagai penyerang untuk menguji apakah IDS dan *Firewall* tersebut

2. Perancangan

a. Perancangan arsitektur system

a) Use Case System Perancangan sistem yang digunakan untuk membangun sistem menggunakan UML (Unified Modeling Language). Perancangan dengan UML ini akan mempermudah dalam menganalisis sistem yang dibangun, dan yang paling penting UML merupakan bahasa grafik (Graphical Language) yang memudahkan untuk proses perancangan sistem.

ISSN : 1979 – 925X e-ISSN : 2442 - 4528



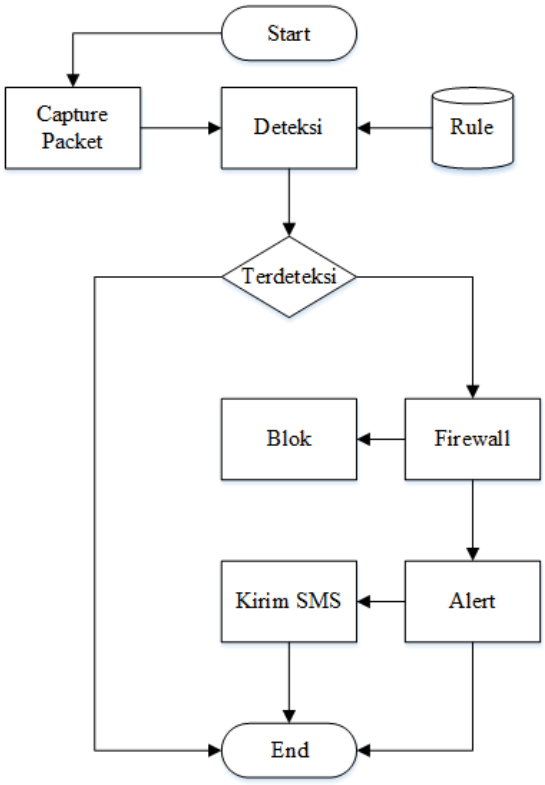
Gambar 2. Use Case System

Penjelasan Use Case

1) Use Case diagram yang digambarkan diatas merupakan tampilan kerja Intrusion Detection Prevention System (IDPS). Awalnya Packet Capture menangkap sebuah paket dalam trafik jaringan, lalu terjadi proses pendeteksian yang akan dilakukan oleh snort engine. Setelah terjadi proses pendeteksian, apabila paket tersebut terdeteksi sebagai sebuah serangan, maka IDS akan men drop paket dan firewall akan melakukan blok terhadap sumber serangan. Setelah itu IPS akan mengirimkan report yang akan disimpan di dalam log dan dikirim ke admin melalui layanan sms.
2) Diagram alur

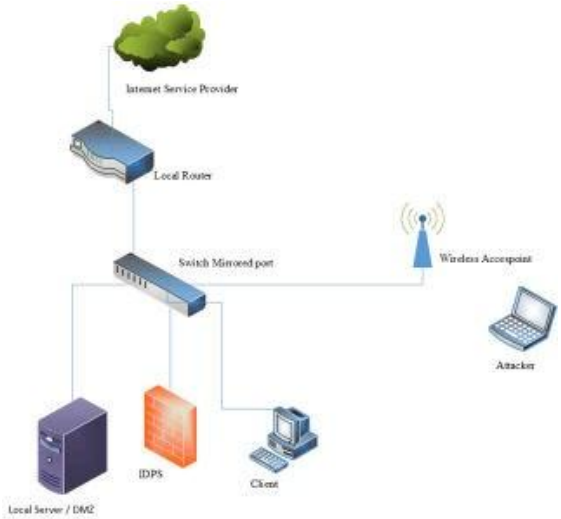
   Diagram alur atau flowchart menggambarkan bagaimana jalannya sebuah sistem dalam melakukan deteksi dan pencegahan. Pada awalnya paket akan di capture lalu dideteksi oleh IDS berdasarkan rule yang tersedia. Kemudian apabila tidak terdeteksi maka proses berakhir, sedangkan apabila terdeteksi, maka firewall akan melakukan blokir terhadap paket dan mengirimkan alert. Kemudian dengan memanfaatkan sms gateway, pesan serangan akan diterima oleh network administrator.

ISSN : 1979 – 925X e-ISSN : 2442 - 4528



Gambar 3 Flowchart System

3) Perancangan topologi Perancangan topologi dimaksudkan untuk merancang topologi yang kiranya sesuai dengan sistem yang dikembangkan, sehingga gambaran topologi berikut dapat memberikan gambaran secara jelas tentang sistem yang hendak dibangun.



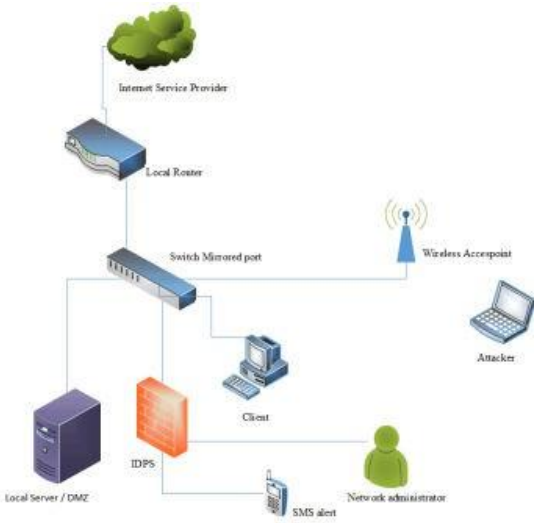
Gambar 3 Topologi

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

Pada gambaran topologi diatas, attacker memanfaatkan koneksi wifi yang dapat digunakan untuk masuk kedalam jaringan lokal.

4) Perancangan sistem

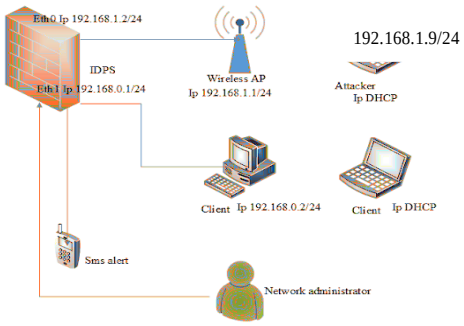
Perancangan sistem merupakan sebuah rancangan / gambaran tentang sistem yang hendak dibangun.



Gambar 4 Rancangan sistem

Ketika attacker melakukan penyerangan, maka switch mengirimkan Salinan paket data yang lewat ke port dimana IDPS terkoneksi. Untuk selanjutnya akan muncul pesan alert, dan kemudian pesan alert tersebut disimpan pada log file dan dikirimkan kepada nomor ponsel network administrator.

5) Perancangan Pengujian



Gambar 5 Perancangan Pengujian

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

Dari gambar diatas, attacker mendapatkan IP secara DHCP, IDPS diatas berfungsi juga sebagai local router.

b. Komponen Aplikasi

Pada bagian ini akan dibahas mengenai rincian dari komponen yang dibutuhkan.

1) Spesifikasi perangkat lunak yang digunakan

Tabel 2 Spesifikasi perangkat lunak

No	Perangkat lunak	Keterangan
Sistem operasi mesin IDPS		
1	Ubuntu 12.04 LTS	Sistem operasi IPS yang digunakan.
Sistem operasi clients		
1	Backtrack 5R3	Sistem operasi client yang difungsikan sebagai attacker penguji IPS.
No	**Perangkat lunak**	**Keterangan**
2	Microsoft Windows 7 SP 1	Sistem operasi client normal.
No	**Perangkat lunak**	**Keterangan**
Perangkat lunak perancang topologi		
1	Microsoft office visio	Perangkat lunak aplikasi yang digunakan untuk merancang
Mesin IPS (intrusion prevention system)		
1	Snort 2.9.6.0	Aplikasi perangkat lunak IDS.
2	Barnyard 2-2.10	Aplikasi pengelola output dari snort.
3	BASE (basic analysis and security engine) 1.4.5	Aplikasi perangkat lunak analisis dan keamanan berbasis web

No	Perangkat lunak	Keterangan
Sistem operasi mesin IDPS		
4	Iptables	Bagian dari Firewall untuk memfilter paket data
5	Gammu	Aplikasi perangkat lunak untuk notifikasi serangan yang dikirim via sms
Perangkat lunak penguji IPS		
1	Ettercap	Program untuk penguji sistem IPS dengan jenis serangan MITM
2	Hping3	Program untuk penguji sistem IPS dengan jenis serangan dos

3. Implementasi

a. Penerapan rule pada IDS. Pada tahap penerapan IDS langkah pertama yang dilakukan adalah menginstall paket-paket yang berkaitan dengan IDS baik berupa plugin seperti nmap, nbtscan, lamp-server^, php5- mysql, libpcap0.8-ev, libpcre3-dev, g++, bison, flex, libpcap-ruby, make, autoconf,

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

libtool, libmysql-client-dev, dan perangkat lunak IDS serta pendukung IDS seperti snort-2.9.6.0, Snortrules- snapshot-2956, snortreport-1.3.4, daq-2.0.2, base-1.4.5, barnyard2-2.10, adodb518. Setting snort sesuai dengan kebutuhan

Tabel 3 Snort Conf

```
var WHITE_LIST_PATH
/usr/local/snort/rules
var BLACK_LIST_PATH
/usr/local/snort/rules

dynamicpreprocessor directory
/usr/local/snort/lib/snort_dyn amicpreprocessor/ dynamicengine
/usr/local/snort/lib/snort_dyn amicengine/libsf_engine.so dynamicdetection directory
/usr/local/snort/lib/snort_dyn amicrules

output unified2: filename snort.u2, limit 128
```

Penulis menggunakan output handler yaitu barnyard2 sebagai perangkat lunak pengatur output dari snort dengan menambahkan syntax output unified2: filename snort.u2, limit 128 sebagai trigger dari snort ke barnyard2. Penulis juga menggunakan database sebagai tempat menampung log file snort yang sudah di atur oleh barnyard2. Untuk database penulis juga menggunakan schema sql kepunyaan barnyard2. Berikut konfigurasi barnyard agar bisa men-store log file kedalam database.

Tabel 4 Banyard2.conf

```
config reference_file:
/usr/local/snort/etc/reference. config
config classification_file:
/usr/local/snort/etc/classificat ion.config
config gen_file:
/usr/local/snort/etc/gen- msg.map
config sid_file:
/usr/local/snort/etc/sid- msg.map
config hostname: localhost config interface: eth1 output database: log, mysql, user=snort password=root dbname=snort host=localhost
```

Penulis membuat *user* tersendiri yang bisa fungsi CRUD *database*.

1) Implementasi *rule* IDS *Rule* untuk icmp flood : alert icmp $EXTERNAL _NET any -> $HOME_NET any (msg:"ICMP Large ICMP Packet"; dsize:>800; reference:Arab hnids,246; classtype:bad-unknown; sid:499;).

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

2) *Rule* untuk scan SYN, ACK, FIN, alerttcp $EXTERNA L_NET any - >$HOME_NE T any (msg:"SCAN SYN FIN";flow:stateless; flags:SF,12; reference:arac hnids,198; classtype:atte mpted-recon; sid:624;). Alert tcp $EXTERNAL_NET any - > $HOME_NET any (msg:"SCAN NULL"; flow:stateless; ack:0; flags:0; seq:0; reference:arac hnids,4; classtype:atte mpted-recon; sid:623;)
3) Preprocessor arpspoof Preprocessor arpspoof untuk mendeteksi adanya upaya- upaya serangan dengan tipe arp spoofing. Edit file di snort.conf pada bagian preprocessor, tambahkan Preprocessor arpspoof <ipaddress>< mac address>
4) Penerapan Iptables Penerapan Iptables bermaksud untuk menentukan security policy firewall Iptables untuk memblok address Iptables –A INPUT – s <ipaddress>-j DROP Iptables synflood Iptables –A INPUT – p tcp ! –syn –m state –state NEW –j DROP Iptables fragment Iptables – A INPUT – f –j DROP Iptables xmas paket Iptables –A INPUT – p tcp --tcp-flags ALL ALL –j DROP Iptables null paket Iptables –A INPUT – p tcp --tcp-flags ALL NONE –j DROP

4. Hasil

a. Pengujian IDS dan Iptables Deteksi dan drop icmp flood dos Serangan dilakukan dengan sistem operasi backtrack 5 dengan console. Syntax : ping 192.168.1.9 –l 10000 (Ip mesin IDPS) yaitu mengirimkan paket icmp kepada alamat ip 192.168.1.9 dengan *buffer size* sebesar 10000 berhasil dilakukan.
b. Deteksi dan drop ping of death Serangan dilakukan dengan sistem operasi backtrack 5 dengan console. Syntax : ping –l 1000 192.168.1.9 –n 1000000 –w 0.0001. Yaitu mengirimkan paket icmp dengan buffer size 1000, dos attempt 1000000, waiting time 0.0001 detik, berhasil dilakukan.
c. Deteksi dan drop Hping3 DoS Serangan dilakukan dengan sistem operasi backtrack 5 dengan console. Syntax : Hping3 –x 192.168.1.9, berhasil dilakukan

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

d. Deteksi proses mitm Syntax: ettercap –G pada console backtrack, berhasil dilakukan

G. KESIMPULAN DAN SARAN

a. Kesimpulan

Rumusan kesimpulan keseluruhan dari proses penelitian ini setelah diuraikan pada bab-bab sebelumnya adalah :

1. Sistem IDS (*Intrusion Detection System*) yang diterapkan telah berhasil dibangun dan dikembangkan. Keseluruhan sistem mesin sensor IDS dapat bekerja dengan efektif sebagai pemberi peringatan dini adanya aksi-aksi penyusupan dalam jaringan.
2. IDS (*Intrusion Detection System*) yang diterapkan adalah mekanisme kerja dari Snort dan BASE. Dalam pengujian sistem Snort dan BASE yaitu dengan seranagan tipe Dos (*Denial of Service*) dan MITM (*Man In The Middle*).
3. IDPS (*Intrusion Detection Prevention System*) yang diterapkan adalan mekanisme kerja dari IDS dan *Firewall*.
4. Fungsionalitas atas komponen yang sedemikian rupa dapat untuk mengetahui adanya serangan pada jaringan lokal dan setelah itu melakukan aksi blok terhadap paket yang dinilai mencurigakan.

b. Saran

Pada penelitian ini penulis menerapkan dan mengimplementasikan sistem IDPS (Intrusion Detection Prevention System). Penulis menemukan saran-saran yang menurut penulis perlu untuk dikembangkan bagi pengembang selanjutnya yaitu :

1) Penulis menyarankan untuk mengembangkan sistem IDPS ini agar dapat mendeteksi aktivitas penyusupan pada komputer Server Public.
2) Penulis menyarankan untuk mengembangkan sistem IDPS ini dilakukan atau diterapkan pada jaringan lebih cepat yakni 1/1000 Mbps.
3) Penulis menyarankan untuk mengembangkan sistem IDPS ini agar dapat melakukan pendeteksian pada trafik jaringan yang terenkripsi. Akan jauh

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

lebih baik, jika sistem IDPS selanjutnya dapat mendeteksi serangan yang dilancarkan tidak hanya pada sistem jaringan normal (non-enkripsi) tetapi juga pada sistem jaringan terenkripsi.

DAFTAR PUSTAKA

Ariyadi, T. Kunang, Y. N. Santi, R. 2009 Implementasi intrusion prevention system pada jaringan komputer B universitas bina darma.

http://blog.binadarma.ac.id/yesinovariakunang/wp-content/uploads/2012/IMPLEMENTASI-INTRUSION-PREVENTION-SYSTEMIPS-PADA-JARINGAN-KOMPUTER-KAMPUS-B-UNIVERSITAS-BINA-DARMA.pdf diakses tanggal 19 mei 2014)

Ariyus, Dony. 2007. Intrusion detection system.Yogyakarta: Penerbit Andi

Basten, M. V. 2009. Optimalisasi firewall pada jaringan skala luas. http://www.unsri.ac.id/upload/arsip/Optimalisasi%20Firewall%20Pada%20Jaringan%20Skala%20Luas.pdf (diakses tanggal 20 mei 2014)

Harianto, A. Junior, S.N.A., Alexander. 2009. *Perancangan dan Implementasi Intrusion Detection System pada jaringan Nirkabel Binus University.* From http://ict.binus.edu/metamorph/file/re search/MAID_JOURv2.0.pdf (diakses tanggal 21 Mei 2014)

Lukas, Jonathan. 2006. Jaringan Komputer:Yogyakarta:Graha Ilmu

Nazir, Moh.v 2011 "Metode Penelitian" Jakarta : Ghalia Indonesia Networks, Arbor. 2013. "Arbor Special Report". Worldwide Infrastructure Security Report. Volume IX.

Pratama, Mick Sandy. 2012. Pengamanan jaringan komputer menggunakan metode IPS (Intrusion Prevention System) terhadap serangan Backdoor dan Synflood berbasis snort inline. *http://eprints.upnjatim..ac.id/3696/1/file1.pdf (diakses tanggal 17 Mei 2014)*

Sofana, Iwan. 2011. *Teori dan Modul Praktikum Jaringan Komputer*.Bandung:Modula

Sofana, Iwan. 2013. *Membangun Jaringan Komputer* . Bandung: Informatika

ISSN : 1979 – 925X e-ISSN : 2442 - 4528

Sutanto, Imam, 2010. *Penerapan easy intrusion detection system (EASY IDS) sebagai pemberi peringatan dini kepada administrator system jaringan.* http://repository.uinjkt.ac.id/dspae/bitstream/123456789/1/Imam%20SutantoFST.pdf

Sugiyono. 2011. *"Metode Penelitian (Pendekatan Kuantitatif, kualitatif, dan R&D"* Bandung: Alfabeta

Syafrizal, Melwin. 2005. *Pengantar Jaringan Komputer.* Yogyakarta : Penerbit Andi

Wagito. 2007. *Jaringan Komputer Teori dan Implementasi Berbasis Linux.*Yogyakarta:Gava Media

Wijaya, Arie. 2011. *Optimalisasi network security dengan mengkombinasikan intrusion detection system dengan firewall pada web server.* http://repository.amikom.ac.id/files/Publikasi_06.11.1181.pdf (diakses tanggal 19 Mei 2014)

Yunos, Aziz Kasmir. 2006. *Intrusion notification via sms. http://eprints.uitm.edu.my/846/1/AZIZ_KASMIR_BIN_MAT_YUNOS_06_24.pdf (diakses tanggal 19 Mei 2014)*

ISSN : 1979 – 925X e-ISSN : 2442 - 4528