PENCEGAHAN SERANGAN LAYANAN JARINGAN INTERNET MENGGUNAKAN METODE KEAMANAN INTRUSION PREVENTION SYSTEM

Disusun Oleh

H. Heru Abrianto

PROGRAM STUSI TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS TAMA JAGAKARSA
JAKARTA
2023

ABSTRAK

Metode pendeteksian terhadap paket serangan Finger_Bomb dan PWL_Access serta sistem IPS mendeteksi serangan tersebut sebagai jenis serangan ***Denial of Services (DoS)*** dan sistem akses tanpa kewenangan (*Unauthorized Access attempt*).

Monitoring berhasil mendeteksi adanya sistem dari luar yang melakukan serangan berupa ***Port_scan*** dan ***TCP_Flood*** ke jaringan internal dengan IP address tujuan 192.168.8.11. Sistem IPS juga berhasil melakukan penghentian paket signature dengan pula serangan tipe ***Open.SSL..Bleed.Attack*** dan ***Data BashFunction*** berhasil dihentikan oleh sistem sebelum mengakses server internet banking dengan IP address 192.168.8.3 port 443.

Kata Kunci : IPS, IDS, DoS, TCP_flood, Signature

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

ACK	Acknowldgement
ARP	Address Resolution Protocol
ASII	American Standard Code for Information
BNC	Bayonet Neill–Concelman
CPU	Computer Proccesing Unit
DoS	Denial of Service
FTP	File Transfer Protocol
HTTP	Hypertet Transfer Protocol
HIPS	Host-base Intrusion System
ICMP	Internet Control Management Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NIPS	Network-base Intrusion Prevention System
NIC	Network Interface Card
OS	Operating System
OSI	Open System Interconnection
PC	Personal Computer

QoS	Quality of Services
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
SYN	Synchronize
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLS	Transport Layer Protocol
UDP	User Diagram Protocol
UTP	Unshield Twisted Pair
VPN	Virtual Private Network
WAN	Wide Area Network
www	World Wide Web

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemudahan akses layanan internet yang dapat diakses dimanapun dan kapanpun menjadi faktor utama bagi para pengguna layanan internet, tetapi dilain sisi ada resiko didalamnya yang harus diwaspadai yaitu faktor keamanan saat penggunaannya.

Dengan hanya mengandalkan penggunaan internet protocol, yang secara teknologi telah terbukti rendah atau lemah dalam tingkat keamanaannya. Sehingga dibutuhkan suatu sistem yang dapat melakukan perlindungan sistem terhadap resiko serangan yang terjadi. Penggunaan *Intrusion Prevention System* (*IPS*) merupakan salah satu cara untuk mencegah terjadinya serangan dengan lebih proaktif.

IPS mempunyai fungsi utama seperti mengindetifikasi serangan, menyimpanan (log) serangan, melakukan pencegahan (memblok) terhadap serangan dan menyampaikan peringatan (alert) pada administrator. Beberapa metode digunakan pada sistem *IPS* yang antara lain metode network base intrusion dan Host base intrusion. Penggunan metode signature (aturan khusus/spesifik) sangat diperlukan dalam mengantisipasi berbagai tipe serangan yang terjadi sehingga sistem dapat melakukan langkah-langkah yang tepat.

1.2 Pokok Permasalahan

Penggunaan sistem keamanan dengan metode deteksi tidak cukup sehingga metode baru dalam penanganan terhadap serangan pada sistem seperti pengamanan menggunakan *IPS* sangat dibutuhkan. Hal ini diperlukan agar sistem melakukan pencegahan lebih cepat dan secara otomatis mencegah serangan terhadap system.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini pada pengamanan jaringan akses internet yang dilakukan dengan mengunakan *IPS* dengan metode signature

1.4 Metode Pendekatan

Metode pendekatan yang digunakan dalam penyusunan penelitian ini adalah dengan melakukan :

1. Studi pustaka yang menunjang pada penelitian ini
2. Studi lapangan pihak-pihak terkait yang memahami pada penelitian ini
3. Simulasi dan

1.5 Sistematika Penulisan

Pembahasan penelitian ini terdiri dari (lima) bab dimana setiap bab saling berhubungan satu dengan yang lain tetapi membahas masalah masing–masing. Pembahasan pada masing-masing bab memberikan penjelasan dan maksud pembahasan.

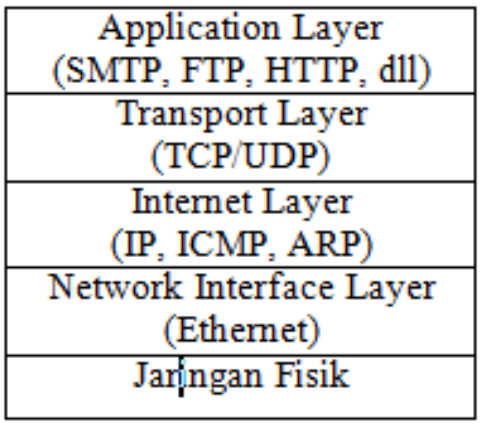
Sistematika penulisan disusun meliputi Bab I Pendahuluan yang berisi latar belakang penyusunan penelitian, pokok permasalahan, batasan masalah, ruang lingkup masalah dan sistematika penulisan. Bab II Teori penunjang . Bab III *Metodologi*. Bab IV Analisa dan Pembahasan, Bab V berisi Kesimpulan.

BAB II

TEORI PENUNJANG

2.1. Teori Dasar TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) adalah sekelompok protocol yang mengatur komunikasi data komputer di internet. Komputer-komputer yang terhubung ke internet berkomunikasi dengan protocol TCP/IP. TCP/IP terdiri dari 4 lapisan (layer) kumpulan protokol yang bertingkat. Lapisan lapisan tersebut adalah Layer 1 yaitu *Network Interface Layer*, bertanggung jawab mengirim dan menerima data ke dan dari media fisik. Layer 2 yaitu Internet Layer, bertanggung jawab dalam proses pengiriman data ke alamat yang cepat. Layer 3 yaitu Transport Layer, bertanggung jawab untuk mengadakan komunikasi antar host. Layer 4 yaitu Application, tempat aplikasi aplikasi yang menggunakan protokol TCP/IP.



Gambar 2.1 Layer TCP/IP [1]

2.2 Network Interface

Layer/lapisan ini bertanggung jawab mengirim dan menerima data ke dan dari media fisik. Media fisik dapat berupa kabel, serat optik, atau gelombang

radio. Peralatan yang diperlukan untuk menghubungkan jaringan salah satunya Ethernet.

2.3 Internet Layer

Layer ini bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat 3 macam protocol yaitu :

a. Internet Protocol (IP)

b. Internet Control Massage Protocol (ICMP)

c. Address Resolution Protocol (ARP)

2.4 Transport Layer

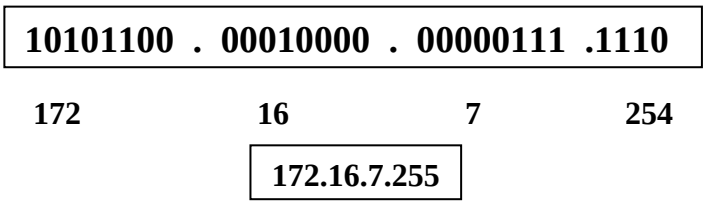
Transport Layer merupakan layer komunikasi data yang mengatur aliran data, untuk keperluan aplikasi ini, ada 2 buah protokol pada layer ini yaitu :

a. Transmisission Control Protocol (TCP)

b. User Datagram Protocol (UDP)

2.5 Pembagian Kelas-kelas Alamat IP.

Alamat IP merupakan bilangan biner 32 bit yang dipisahkan oleh tanda pemisah berupa tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai *oktet*, yang masing-masing bit tersebut dapat diganti dengan angka 0 dan 1. Nilai terbesar dari bilangan biner 8 bit adalah 255 yaitu $2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$. Karena Alamat IP terdiri dari 4 buah bilangan 8 bit maka jumlah Alamat IP yang tersedia adalah 255.255.255.255.



Gambar 2.2 Pengalamatan TCP/IP [1]

2.5.1 Network ID dan Host ID

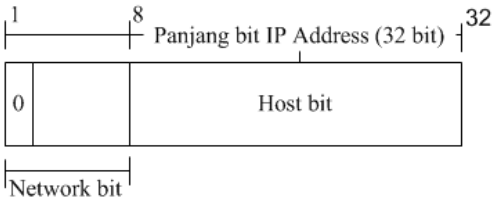
Pembagian kelas-kelas Alamat IP didasarkan pada 2 hal yaitu : Network ID dan Host ID dari suatu Alamat IP

Setiap Alamat IP selalu merupakan sebuah pasangan dari network ID (Indentitas jaringan) dan host ID (indentitas host dalam jaringan tersebut). Network ID ialah bagian dari Alamat IP yang digunakan untuk menunjukkan jaringan tempat komputer itu berada. Sedangkan host ID adalah bagian dari Alamat IP yang digunakan untuk menunjukan Komputer, router dan semua host TCP/IP lainnya dalam jaringan tersebut. Dalam satu jaringan, host ID ini harus unik (tidak diperbolehkan ada yang sama).

Untuk mempermudah pendistribusian pendaftaran Alamat IP maka dikelompokkan dalam kelas kelas IP sebagai berikut :

a. IP Kelas A

Alamat IP kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar. Bit pertama dari Alamat IP kelas A adalah di set 0 (nol) sehingga byte yang terdepan dari Alamat IP kelas A, selalu bernilai antara 0 dan 127. Pada Alamat IP kelas A, network ID ialah 8 bit pertama, sedangkan host ID ialah 24 bit berikutnya. Dengan panjangan host ID yang 24 bit, network dengan Alamat IP kelas A ini dapat menampung sekitar 16 juta host. Hal ini seperti terlihat pada gambar 2.3.

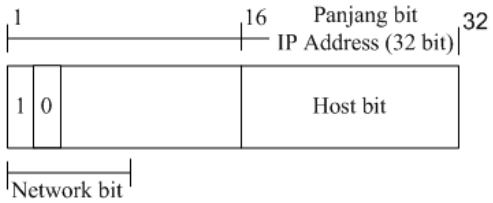


Gambar 2.3 Format Alamat IP Kelas A [1]

b. IP kelas B

IP kelas B biasanya dialokasikan untuk jaringan berukuran sedang dan besar. 2 bit pertama dari Alamat IP kelas B selalu diset 10 (satu nol). Sehingga byte terdepan dari Alamat IP kelas B selalu bernilai antara 128

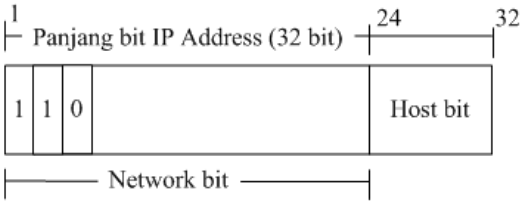
hingga 191 pada Alamat IP kelas B, network ID ialah 16 bit pertama sedangkan host ID ialah 16 bit berikutnya dengan panjang host ID yang 16 bit, network dengan Alamat IP kelas B ini dapat menampung 65000 host. Hal ini seperti terlihat pada Gambar 2.4.



Gambar 2.4 Format Alamat IP Kelas B [1]

c. IP kelas C

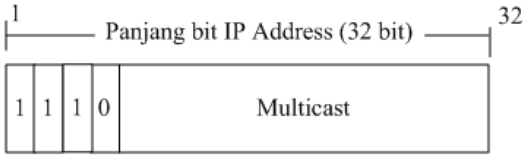
Alamat IP kelas C terdiri dari 3 bit pertama selalu berisi 110, bersama 21 bit berikutnya, angka ini membentuk network ID 24 bit. Host ID ialah 8 bit terakhir. Dengan konfigurasi ini, bisa dibentuk sekitar 2 juta network dengan masing-masing network memiliki 256 Alamat IP seperti terlihat pada Gambar 2.5



Gambar 2.5 Format Alamat IP Kelas C [1]

d. IP kelas D

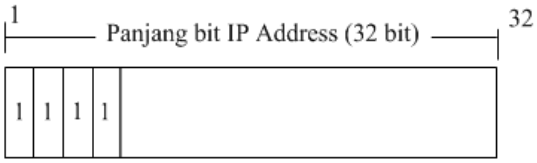
Alamat IP kelas D digunakan untuk keperluan IP multicasting 4 bit pertama Alamat IP kelas D diset 1110 seperti terlihat pada Gambar 2.6.



Gambar 2.6. Format Alamat IP Kelas D [1]

e. IP kelas E

Alamat IP kelas E dicadangkan untuk kegiatan riset dan eksperimental, 4 bit pertama Alamat IP ini diset 1111. seperti terlihat pada Gambar 2.7



Gambar 2.7. Format Alamat IP Kelas E [1]

2.5.2 Subnetting

Dalam *subnetting* proses yang dilakukan ialah memakai sebagian bit *host ID* untuk membentuk subnet ID. Dengan demikian jumlah bit yang digunakan untuk host ID menjadi lebih sedikit.

Suatu alasan perlunya dibentuk subnetting antara lain :

1. Menghindari limitasi jumlah simpul dalam satu segmen
2. Mereduksi trafik yang disebabkan oleh broadcast maupun benturan (*collision*).

Subnet mask ialah angka biner 32 bit yag digunakan untuk :

a. Menunjukkan letak suatu host, apakah berada dijaringan local atau jaringan luar/lain.

b. Membedakan network ID dan host ID

Secara default subnet mask untuk tiap kelas Alamat IP sebagai berikut :

- Kelas A : 255.0.0.0
- Kelas B : 255.255.0.0
- Kelas C : 255.255.255.0

Pada *subnet mask,* seluruh bit yang berhubungan dengan network ID diset 1 sedangkan bit yang berhubungan dengan host ID diset 0. Alamat IP kelas A

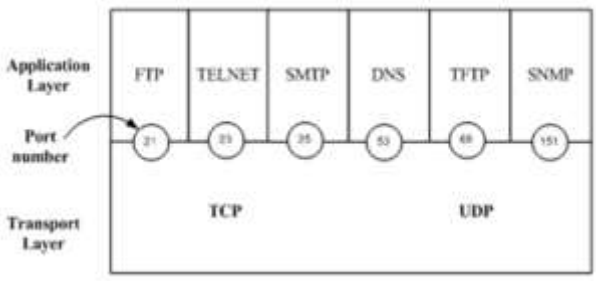
misalnya secara default memiliki subnet 255.0.0.0 yang menunjukkan batas antara network ID dari Alamat IP kelas A.

Subnet mask juga digunakan untuk menentukan letak suatu host, apakah dijaringan local atau dijaringan luar. Hal ini diperlukan untuk operasi pengiriman paket IP. Dengan melakukan operasi AND antara subnet mask dengan Alamat IP tujuan paket IP tersebut. Jika kedua hasil operasi tersebut sama maka host tujuan terletak dijaringan local dan paket IP dikirimkan langsung ke host tujuan. Jika hasilnya berbeda, host tujuan terletak diluar jaringan local sehingga paket pun dikirimkan ke default router.

Dalam *subnetting,* proses yang dilakukan ialah memakai sebagian bit host ID untuk membentuk subnet ID. Dengan demikian jumlah bit yang digunakan untuk host ID menjadi lebih sedikit. Semakin panjang subnet ID maka jumlah subnet yang dapat dibentuk semakin banyak juga namun jumlah host tiap subnet menjadi semakin sedikit.

2.5.3 Port

Port digunakan untuk memetakan koneksi antara 2 host, antara layer TCP/UDP dan aplikasi aktual yang berjalan pada host. Port dengan range 0 – 1023 dinamai *"reserved"* atau *"privillage"* port. Artinya port-port tersebut digunakan untuk berbagai aplikasi yang khas. Seperti telnet, mail, web, ftp, dan sebagainya. Sedangkan sisanya yaitu 1024 – 65535 disebut sebagai *"dynamic"* atau *"privillage"* port. Pada Gambar 2.8 TCP port menjelaskan pembagian atau alokasi dari nomor port dari setiap lajur aplikasi & lajur transport.



Gambar 2.8 port TCP [1]

BAB III

METODOLOGI

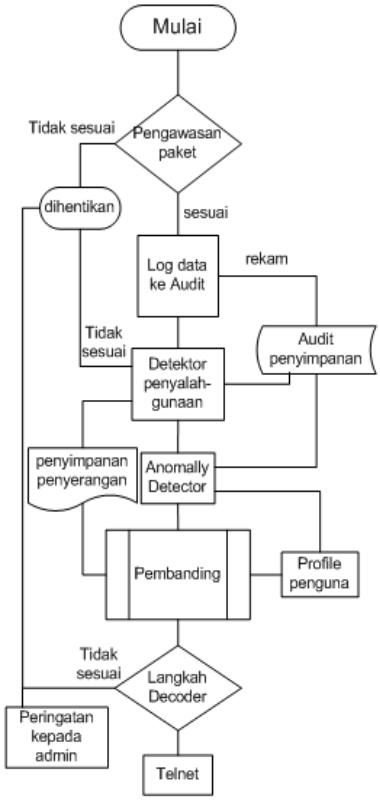
3.1 Intrusion Prevention System

Perkembangan yang sangat cepat dari internet serta potensi kehilangan data yang sensitif sehingga deteksi saja tidak cukup tetapi kebutuhan pencegahan menjadi perlu. *IPS* melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *ports* atau Alamat IP seperti *firewall* umumnya. *IPS* Selain dapat memantau dan monitoring, IPS dapat juga mengambil kebijakkan dengan pencegahan (block) paket yang lewat.

3.2 Diagram Alir *IPS*

Alur data pada *IPS* seperti dijelaskan pada gambar 3.1 dapat disampaikan sebagai berikut : paket monitor melakukan analisa pengontrolan data pada paket yang akan dikirim atau diterima dari semua jaringan. Jika pada paket yang ditemukan ada sesuatu yang tidak normal maka *IPS* akan merespon dengan mematikan system. Namun jika paket yang ditemukan adalah normal maka Paket yang normal tersebut akan di-log ke dalam audit trail.

Extractor melakukan pemilah dan memisahkan masing-masing data audit pada masing-masing detector, baik itu *misuse detector* maupun *anomaly detector* selanjutnya pendeteksian penyalahgunaan (misuse detection) melakukan pengecekan serangan statis berdasarkan skenario serangan dari *intrusion log*. Jika ditemukan aktifitas yang sesuai dengan log tersebut maka dinyatakan sebagai serangan dan *IPS* akan merespon dengan mematikan (Shutdown) sistem, sementara aktifitas yang tidak sesuai dilanjutkan dengan menentukan ‘k” (*Misuse detection)*, yaitu aktifitas yang diindikasikan sebagai serangan. Nilai ini kemudian diberikan ke pembanding (*comparator*). Anomaly detector menentukan ‘b’, yakni dengan mengindikasikan aktifitas yang terjadi pada kebiasaan normal sebagai user profile. Nilai ini kemudian diberikan ke komparator.



Gambar 3.1 Diagram Alir IPS [6]

Komparator akan membandingkan nilai ‘b’ dan ‘k’ untuk mengklasifikasikan aktifitas yang terjadi secara tepat, menjadi 4 tingkatan tertentu yakni : Strongly Intrusive (SI), Strongly Normal (SN), Weakly Intrusive (WI) dan Weakly Normal (WN)

Output dari *comparator* kemudian diberikan *action decorder sehingga* action decorder akan mengubah *output comparator* menjadi respon yang tepat seperti pada tabel .3.1

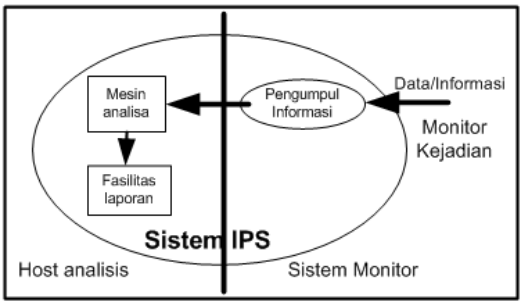
Tabel 3.1 Respon terhadap Serangan

Tingkatan Aktifitas	Respon
SI	**A**
WI	**B**
WN	**C**
SN	**D**

3.3 Proses *IPS*

IPS terdapat 3 fungsi yang merupakan proses utama dalam *IPS* yaitu :

1. Pengambilan Data (Information Source)
2. Analisis Pendeteksian serangan (Detection Attact Analyst)
3. Respon terhadap Serangan (Attact Respond)



Gambar 3.2 Sistem *IPS* [11]

3.4 Tipe Intrusion Prevention System

IPS dapat diklasifikasi menjadi 4 type berdasarkan fungsi dan perannya sebagai berikut :

1. Network-Base Intrusion Prevention System (NIPS)
2. Wireless Intrusion Prevention System (WIPS)
3. Network Behavior Analysis
4. Host-Base Intrusion Prevention System (HIPS)

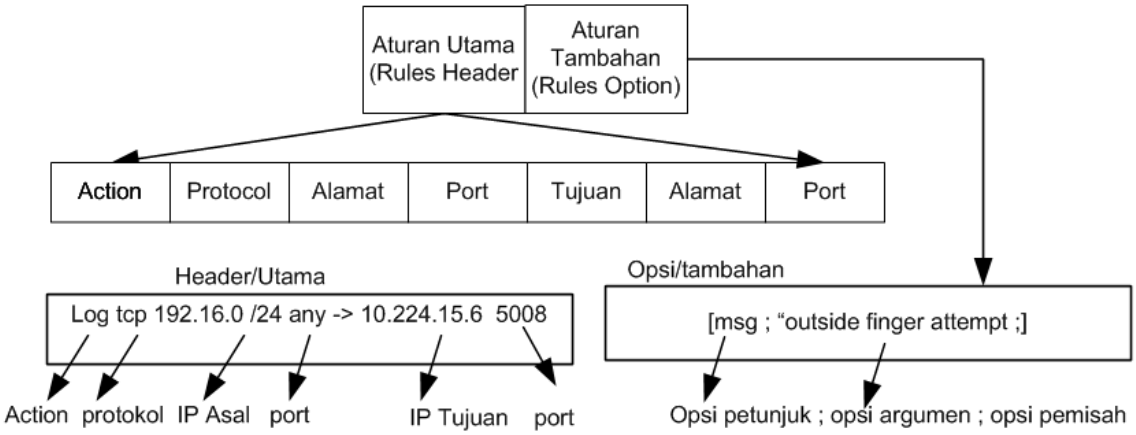
3.5 Metode Deteksi *IPS*

Berikut ini adalah beberapa metode dalam *IPS* yang melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan. Metode deteksi yang digunakan pada *IPS* terdiri dari :

1. Signature-base Detection
2. Anomaly-base Detection
3. Stateful Protocol Analysis Detection

3.6. Metode pengecekan Paket TCP

Metode pengecekan paket TCP yang diterlihat pada gambar 3.10 dilakukan oleh *IPS* berdasarkan Header rules dan option rules. Pengecekan terhadap paket dilakukan dibawah ini :



Gambar 3.3 Pengecekan packet TCP [12]

Rules option harus dibuat sehingga setiap paket yang lewat setelah dilakukan pengecekan TCP header akan dilanjutkan ke option Rules (aturan tambahan). Berikut contoh rules yang digunakan sebagai berikut :

a. Pengecekan terhadap paket yang mengandung sub seven Tojan

Alert tcp $ETERNAL_NET 27374 -> 4HOME_NET any (msg:"BACKDOOR subseven 22"; flags: A+; content: "I 0d0a5b52504c5d3030320d0a I "; reference:arachnids, 45;Clastype:misc-activity; rev:4😉.

Penjelasan terhadap message diatas sebagai berikut : ***Alert*** langkah yang diambil terhadap paket data; serta log. ***Tcp*** merupakan protocol, *$EXTERNAL_NET* alamat asal (source address), *ini merupakan variable 12yst juga Alamat IP*. ***27374*** merupakan port asal (source port), dapat pula ***any. ->*** *petunjuk,* ***$HOME_NET****, alamat tujuan (variable), any* port tujuan (destination port). *Msg:'BACKDOOR SUBSEVEN";* tampilan yang akan muncul pada log. ***Flag:*** **A**; merupakan tcp flags/tanda, ***content***: "(0d0….0a'; merupakan binary data yang akan dicheck pada paket. ***Reference***…; merupakan penjelasan sumber atau latar belakang dari aturan/rules. ***Sid:103*** merupakan rule ID (indentitas aturan), ***classtype:***

misc-activity; merupakan tipe aturan dan tambahan aktifity, ***rev:4:*** merupakan nomer revisi aturan (rule revision number). ***Other rule option*** dimungkinkan seperti offset, depth ataupun nocase

b. Aturan (Rules) dalam pengecekan HTTP signature :

F-SBID(--name “FrontPage.Fp30reg.Chunked.Overflow”; --protocol tcp; --service HTTP; --flow from_client; --parsed_type HTTP_POST; --pattern “/_vti_bin/_vti_aut/fp30reg.dll”; --context uri; --no_case; --parsed_type HTTP_CHUNKED;)

c. Aturan (Rules) dalam pengecekan DHCP FLOOD :

F-SBID(--name **DHCP.FLOOD**; --protocol TCP; --service DHCP; --dhcp_type 1; --rate **100,10**; --track DHCP_CLIENT;)

signature menunjukan bahwa IPS melihat atau menemukan DHCP request discover requests (--dhcp_type 1😉 melebihi 100 x dalam 10 detik ***(--rate 100,10***😉 dari DHCP client yang sama ***(--track dhcp_client***😉, maka alert akan di berikan/13ystem13ate.

d. Berikut ini merupakan contoh dari Custome signature yang melakukan pengecekan terhadap ip_flag Header pada paket TCP

F-SBID(--name testflag; --protocol tcp; --ip_flag D😉

Contoh trafik paket yang dibuat (Custom) :

sendip –p ipv4 –p tcp –is 192.168.5.37 –ifd 1 –ts 5566 –td 1234 –tfs 1 ***192.168.5.40 .***

Jika Log diaktifkan maka signature akan membandingkan paket yang lewat dengan database IPS custome signature :

1 2004-09-02 01:19:52 log_id=0420070000 type=ips subtype=signature pri=alert attack_id=113770497 src=192.168.5.37 dst=***192.168.5.40*** src_port=5598 dst_port=1234 src_int=ha dst_int=dmz status=detected proto=6 service=1234/tcp msg=”custom: testflag”

Dalam hal ini 14ystem *IPS* melihat ada kesamaan dari tujuan Alamat IP yang dituju. Proses yang dilakukan terhadap paket tersebut adalah paket data **Dihentikan/Stop**.

3.7. *IPS* Signature Database

Merupakan tabel database aturan yang digunakan sebagai referensi untuk menganalisa terhadap paket. Hal ini sangat diperlukan untuk dapat memahami metode dari serangan.

IPS metode Signature terdiri dari 2 jenis yaitu Official Signature dan Custom Signature. Official Signature merupakan paket database aturan yang dikeluarkan atau dibuat oleh pembuat produk hardware/software dan akan memberikan update secara berkala untuk perkembangan signature. Sedangkan Custom Signature merupakan paket aturan yang dibuat berdasarkan ke khusus aplikasi dikarenakan setiap aplikasi mempunya spesifikasi terhadap port atau parameter yang digunakan. Hal ini diperlukan untuk menghindari false alarm (peringkatan keliru/salah) yang diberikan oleh sistem *IPS*.

3.8 Jenis Jenis serangan dalam internet

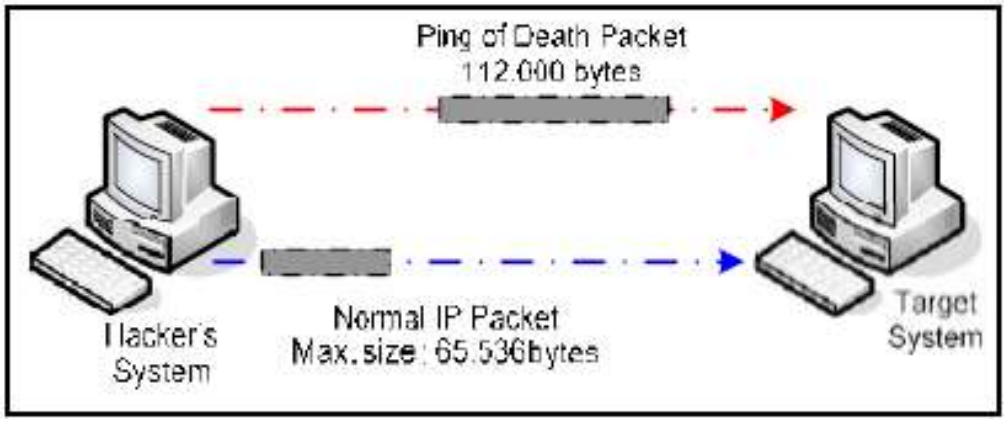
Teknologi internet yang digunakan saat ini bergantung kepada teknologi Internet Protokol (IP) versi 4, IPv4 memiliki beberapa kelemahan : Paket protocol IP tidak memiliki enkripsi sehingga dapat dibaca dan diganti isi packetnya. Membaca paket tersebut dapat dilakukan dengan cara menyadap yang biasa disebut dengan istilah *wire-tapping atau packet sniffing*. Menyamarkan Alamat IP menggunakan alamat IP lain sehingga berhasil mendapatkan paket yang seharusnya ditunjukan ke host tersebut.

Serangan yang sering terjadi muncul karena kelemahan dari TCP/IP adalah Denial of Service (DoS), yakni serangan diinternet yang menyebabkan mesin/server tidak dapat beroperasi sama sekali dan tidak memberikan service.

Beberapa serangan yang sering digunakan adalah :

a. Ping of Death

Ping digunakan untuk mengecek berapa lama waktu yang dibutuhkan untuk mengirimkan sejumlah data tertentu dari satu komputer ke komputer lain. Panjang maksimum data yang dikirim menurut spesfikasi protocol IP adalah 6536 byte. Pada Ping of Death data yang dikirimkan melebihi maksimum paket sehingga sistem yang tidak siap akan crach atau hang, atau system akan reboot pada saat menerima paket yang demikian panjang. Serangan ini dapat diatasi dengan memperbaiki sistem operasi. Berikut ini gambar 3.4 menjelaskan pola serangan Ping of Death.

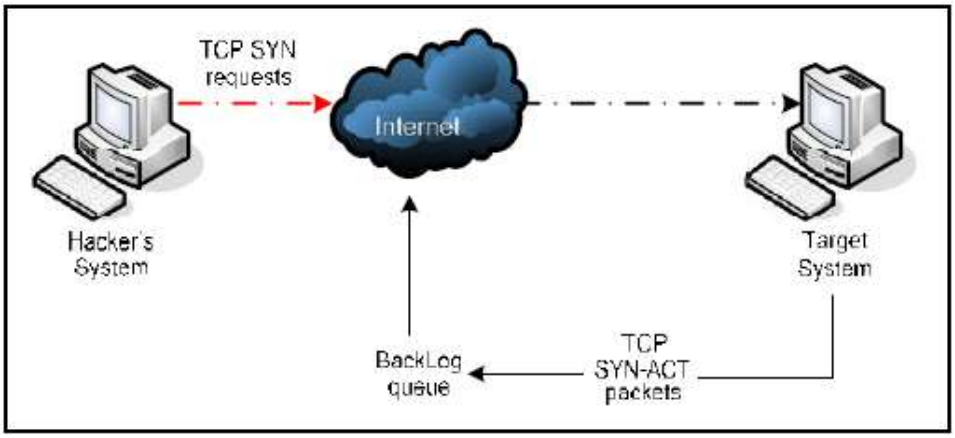


Gambar 3.4 Serangan Ping of Death [13]

b. SYN Attach

Paket SYN dikirim disaat memulai handsake antara 2 aplikasi sebelum transaksi/pengiriman data dilakukan. Pada kondisi Normal, aplikasi pengguna akan mengirimkan paket TCP SYN untuk mensinkronisasi paket pada aplikasi di server. Server akan mengirimkan respon berupa acknowldgement pada TCP SYN ACK. Setelah paket TCP SYN ACK diterima dengan baik oleh pengguna maka pengguna akan mengirimkan paket ACK sebagai tanda transaksi/pengiriman data akan dimulai. Dalam serangan SYN Flood (banjir Paket SYN) , pengguna akan membanjiri server dengan banyak paket TCP SYN. Setiap paket TCP SYN yang dikirim akan menyebakan server menjawab dengan paket TCP SYN ACK. Server akan terus mencatat (membuat antrian backlog) untuk menunggu respond TCP ACK dari pengguna yang mengirimkan paket TCP SYN. Tempat antrian backlog yang terbatas akan menyebabkan antrian backlog ini penuh sehingga system tidak dapat merespon paket TCP SYN lain yang masuk dengan kata lain sistem akan hang. Pada SYN attach ini pengguna membanjiri server dengan paket TCP SYN

ACK. Dengan cara ini sistem akan berhenti/hang dan tidak dapat memproses respon dalam waktu yang sama. Pertahanan terhadap SYN attach dapat dilakukan mengunakan IPS sementara itu program pada firewall juga disetting agar tidak ada paket dengan alamat IP sumber yang kacau Gambar 3.5 ini menunjukkan serangan TCP SYN ACK.

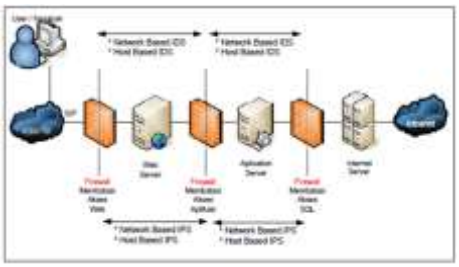


Gambar 3.5 TCP SYN Flood [8]

BAB IV

ANALISA DAN PEMBAHASAN

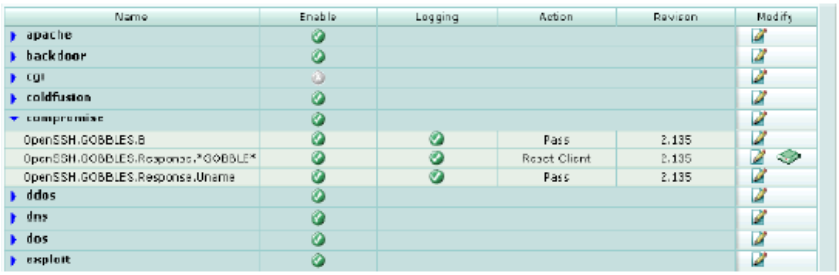
Teknologi keamanan layanan internet menggunakan *IPS* memiliki kemampuan lebih baik dari metode deteksi dimana hanya mampu mendeteksi adanya penyusup dalam jaringan lalu mengaktifkan peringatan kepada pengguna untuk segera mengambil langkah-langkah mitigasi sementara IPS langsung melakukan fungsinya mengatasi penyusup tersebut.



Gambar 4.1 Diagram Network Internet [12]

4.1. Konfigurasi *IPS*

Konfigurasi yang digunakan pada perangkat seperti pada daftar *IPS* Signature gambar 4.2 konfigurasi standar *IPS* Signature yang sudah terdeteksi metode penyerangan.



Gambar 4.2 Konfigurasi IPS signature standar

4.2. Pengujian Penerapan IPS

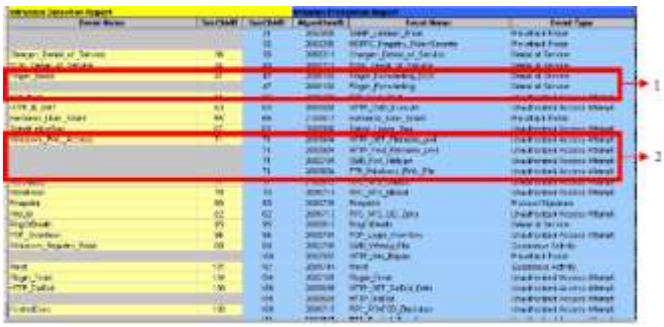
Konfigurasi Penerapan IPS digunakan dalam memonitoring trafik dan paket data yang masuk kedalam sistem layanan internet seperti pada Gambar 4.3 dan 4.4.

Gambar 4.3 Console layanan Internet

Gambar 4.4 Console protekci Server Analisis

Pada gambar 4.3 dan 4.4 terlihat bahwa serangan yang ditampilkan merupakan hasil dari pendeteksian dari perangkat sensor. Console site protector juga menampilkan status serangan yang terdeteksi, apakah sudah ditutup ataupun dikenali oleh perangkat, banyak atau seringnya serangan yang terjadi dan IP asal serta ke IP tujuan.

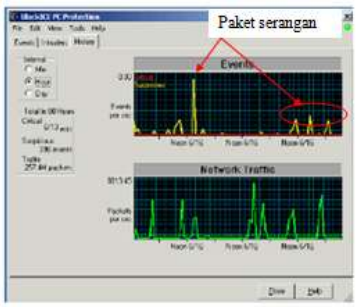
Log hasil dari serangan yang terdeteksi dapat dilihat pada gambar 4.5 selanjutnya dimana merupakan perbandingan log dari perangkat *IPS* & deteksi.



Gambar 4.5 Data deteksi & IPS serangan report

Deteksi serangan dan trafik serangan dari penggunaan *IPS*, pada gambar 4.6 terdeteksi adanya paket UDP & pada gambar 4.7 terlihat terjadinya serangan pada sistem yang terdeteksi oleh IPS pada monitoring :

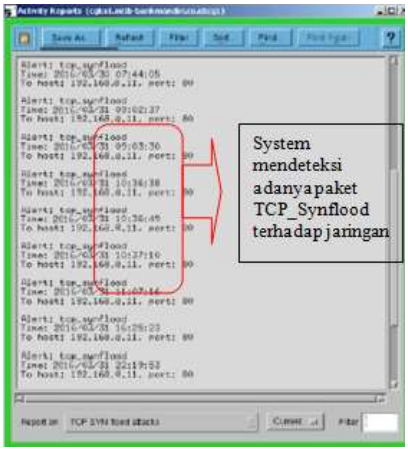
Gambar 4.6 Serangan/paket UDP terdeteksi pada laporan HIPS



Gambar 4.7 Trafik serangan pada HIPS Report

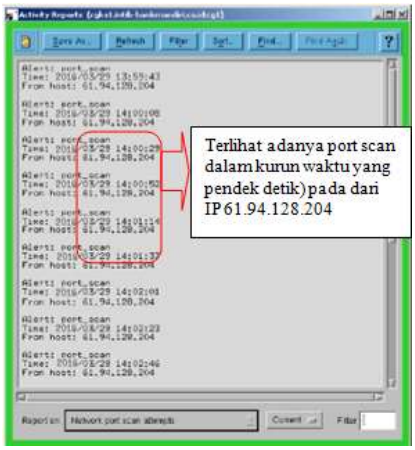
Tampilan aktifitas pada laporan yang mendeteksi adanya serangan berupa TCP_Flood menuju jaringan IP 192.168.8.11 terlihat gambar 4.8 yang

memberikan laporan aktifitas dari serangan yang masuk dan terdeteksi oleh sistem monitoring.



Gambar 4.8 Activity Report Alert Serangan TCP SYNC Flood

Tampilan aktifitas pada laporan yang mendeteksi adanya serangan berupa port_scan dari jaringan IP 61.94.128.204 terlihat gambar 4.9 yang melakukan aktifitas scan port pada jaringan internal.



Gambar 4.9 Activity Report Alert Serangan Port scan

4.3. Pencegahan Serangan

Sistem melakukan pencegahan serangan yang dicurigai seperti terlihat pada gambar 4.10 dan gambar 4.11, dapat terlihat juga dari report yang ada tingkat dari serangan (severity), protocol yang digunakan TCP) yang terjadi dan

tipe dari serangan. Dalam hal ini sistem IPS menangkap dan sekaligus menghentikan paket data yang menggandung pola serangan ***Open.SSL..Bleed.Attack.*** Pada laporan dapat terlihat bahwa paket dari Alamat IP 46.4.94.230 mencoba mengakses IP server 192.168.8.3 dengan port 443 dengan tipe serangan sesuai dengan data signature. Pada laporan tersebut dapat terlihat beberapa paket data dari IP 192.168.23.21 yang menggunakan protokol tidak sesuai dengan rules atau aturan signature yang digunakan berhasil dihentikan oleh sistem IPS.

Gambar 4.10 Data serangan *Open.SSL..Bleed.Attack*

Gambar 4.11 Data Bash Function

BAB V

Kesimpulan

Suatu keamanan merupakan hal yang sangat penting dalam jaringan baik keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar. Perkembangan *IPS* (Pencegahan) berkembang mengikuti pola serangan pada sistem.

1. Monitoring berhasil mendeteksi adanya sistem dari luar yang melakukan serangan berupa ***Port_scan*** dan ***TCP_Flood*** ke jaringan internal dengan Alamat IP tujuan 192.168.8.11.
2. Sistem IPS juga berhasil melakukan pencegahan serangan dengan pula serangan tipe ***Open.SSL..Bleed.Attack*** dan ***Data BashFunction*** berhasil dihentikan oleh sistem sebelum mengakses server internet banking dengan Alamat IP 192.168.8.3 port 443.

DAFTAR PUSTAKA

1. Behrouz A. Forouzan – TCP/IP Protocol Suite, Four Edition
2. Daryanto, “Teknologi Jaringan Internet” 2010
3. Steve Piper, CISSP, SFCP, “Intrusion Prevention System for Dummies”
4. Fortinate Inc, Fortigate IPS Guide ver 1.0
5. Bilal Maqbool Beigh, 2 Prof.M.A.Peer, Intrusion Detection and Prevention System: Classification and Quick Review
6. H. Jadidoleslamy, Jurnal Designing a New Security Architecture for Online-Banking: A Hierarchical Intrusion Detection Architecture and Intrusion Detection System.
7. Karen Scarfone, Peter Mell, National Institute of Standards and Technology- Gaithersburg Guide to Intrusion Detection and Prevention Systems (IDPS)
8. International Conference on Computer Communication and Management, Pitcher Flow: Unified Integration for Intrusion Prevention System, 2011
9. Fortinate Inc , IPS Signature Syntax Guide, May 22, 2014
10. International Journal of Advance Research in Computer Science and Management Studies RafatRana S.H. Rivi, A Review on Intrusion Detection System,
11. International Journal of Computer Application, Abdul Hanan Abdullah, Characterizing Network Intrusion Prevention System, 2011
12. Stonesoft Corp, Intrusion Detection and Analysis for Active Response - Version 1.2, 2005