semanTIK, Vol.4, No.2, Jul-Des 2018, pp. 11-20
ISSN: 2502-8928 (Online)
DOI : 10.5281/zenodo.1407864

IMPLEMENTASI KEAMANAN *SERVER* PADA JARINGAN *WIRELESS* MENGGUNAKAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) (STUDI KASUS : TECHNO'S STUDIO)

Muh. Sadam Husain S.S[1], LM. Fid Aksara[*2], Natalis Ransi[*3]
[1,*2,*3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail : [1]sadamsaranani3692@gmail.com, [*2]**fid.laode@uho.ac.id**, [*3]**natalis.ransi@uho.ac.id**

Abstrak

Penerapan jaringan komputer menggunakan media *wireless* saat ini memberikan dampak perubahan yang cukup signifikan yang memungkinkan orang-orang bisa memperluas akses kerja karena tidak terikat pada penggunaan kabel. Techno's Studio adalah perusahaan yang bergerak dibidang teknologi dan merupakan perusahaan yang menggunakan teknologi *wireless* sebagai salah satu komponen penting dalam aktifitas pegawai sehari-hari. Oleh karena itu, masalah keamanan *server* pada jaringan *wireless* menjadi sangat penting, karena tanpa adanya dukungan keamanan dapat menimbulkan kegagalan sistem dan dapat menjadi celah terjadinya tindakan *hacking*.

Metode IDPS *(Intrusion Detection & Prevention System)* digunakan sebagai sistem pendeteksi dan pencegahan serangan dengan cara pemblokiran terhadap *Internet Protocol* (IP) penyerang. Hasil yang diperoleh dari penelitian ini yaitu penggunaan *Snort* dan *IPTables* sebagai sistem keamanan *server* pada jaringan *wireless* berhasil mengatasi jenis serangan pada *port* ICMP, FTP, SSH, TELNET, dan HTTP menggunakan berbagai macam *tools* penyerang seperti *Angry IP Scanner, Filezilla, Putty, Mozila Firefox* dan *Zenmap*.

Kata Kunci—*Server, Wireless, Intrusion Detection & Prevention Sytem* (IDPS), *Snort, IPTables*

Abstract

The use of computer networks uses the current wireless media that provides significant information that allows others to access the connection because they do not use cables.Techno's Studio is a company engaged in technology and is a company that uses wireless technology as one of the important components in the activities of everyday employees. Therefore, server security issues on wireless networks become very important, because without any security support can lead to system failure and can be a gap in the occurrence of hacking.

The IDPS method (Intrusion Detection & Prevention System) is used as an attack detection and prevention system by blocking Internet Protocol (IP) attackers. The results obtained from this research is the use of Snort and IPTables as a server security system on the wireless network successfully overcome the type of attack on ICMP ports, FTP, SSH, TELNET, and HTTP using various tools of attackers such as Angry IP Scanner, FileZilla, Putty, Mozilla Firefox, and Zenmap.

Keywords— *Server, Wireless, Intrusion Detection & Prevention Sytem (IDPS)*, *Snort, IPTables*

1. PENDAHULUAN

Perkembangan teknologi informasi kini mengalami kemajuan yang semakin pesat, dengan adanya perkembangan tersebut keamanan jaringan komputer menjadi sangat penting dan patut untuk diperhatikan. Penerapan jaringan komputer menggunakan media *wireless* saat ini memberikan dampak perubahan yang cukup signifikan yang memungkinkan orang-orang bisa memperluas akses kerja karena tidak terikat pada penggunaan kabel. Penerapan jaringan *wireless* walaupun baik, namun bukan berarti tidak memunculkan masalah baru yaitu mengenai keamanan *server* yang terhubung pada jaringan *wireless*.

Keamanan jaringan sebagai sebuah bagian dari sistem sangat penting untuk menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunanya, baik yang berupa organisasi komersial (perusahaan), lembaga pemerintahan, perguruan tinggi, instansi, maupun individual [1]. Pentingnya nilai dari sebuah informasi menjadikan informasi tersebut dibatasi hanya untuk orang-orang tertentu. Bocornya suatu informasi kepihak yang tidak bertanggung jawab dapat menimbulkan kerugian bagi pemilik informasi.

Techno's Studio adalah perusahaan yang bergerak dibidang teknologi dan merupakan perusahaan yang menggunakan teknologi *wireless* sebagai salah satu komponen penting dalam aktifitas pegawai sehari-hari. Oleh karena itu, masalah keamanan *server* pada jaringan *wireless* menjadi sangat penting, karena tanpa adanya dukungan keamanan dapat menimbulkan kegagalan sistem dan dapat menjadi celah terjadinya tindakan *hacking*. Belum adanya sistem yang dapat mengawasi *server* pada jaringan *wireless*, menginformasikan serangan, dan mengambil tindakan tepat untuk pencegahan terhadap keamanan *server* pada jaringan *wireless,* membuat admin sulit dalam mengatasi berbagai bentuk serangan yang dilakukan *hacker*.

Salah satu solusi yang dapat diterapkan dalam meningkatkan keamanan *server* pada jaringan *wireless* yaitu dengan menggunakan *Intrusion Detection and Prevention System* (IDPS). IDPS mampu mendeteksi penyusup atau paket-paket berbahaya dalam jaringan dan memberikan laporan berupa *log* tentang aktivitas dan kondisi jaringan sekaligus melakukan *drop packet* terhadap upaya penyusupan dan dapat digunakan untuk membantu *administrator* dalam memantau dan menganalisa paket berbahaya yang terdapat dalam sebuah jaringan.

2. METODE PENELITIAN

2.1 Jaringan Komputer

Jaringan komputer adalah bentuk telekomunikasi yang memungkinkan antar komputer untuk saling bertukar data. Tujuan dari jaringan komputer adalah agar setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan. Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut *server*. Desain ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer [2].

2.2 Wireless Local Area Network (WLAN)

Wireless Local Area Network (disingkat *Wireless* LAN atau WLAN) adalah jaringan komputer yang menggunakan frekuensi radio dan *infrare*d sebagai media transmisi data. *Wireless* LAN sering disebut sebagai jaringan nirkabel atau jaringan *wireless* [3].

Proses komunikasi tanpa kabel ini dimulai dengan bermunculannya peralatan berbasis gelombang radio, seperti *walkie talkie*, *remote control*, *cordless phone*, telepon selular, dan peralatan radio lainnya.

2.3 Intrusion Detection System (IDS)

IDS atau *Intrusion Detection System* adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan di dalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau *administrator* jaringan [4].

Dalam banyak kasus IDS juga merespon terhadap *traffic* yang tidak normal/ anomali melalui aksi pemblokiran seorang *user* atau alamat IP (*Internet Protocol*). IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda yang intinya berfungsi untuk mendeteksi *traffic* yang mencurigakan di

dalam sebuah jaringan. Beberapa jenis IDS adalah : yang berbasis jaringan (NIDS) dan berbasis *host* (HIDS).

2.4 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem 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 data 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 sepeti layaknya *Firewall* yang akan melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan *signatures* untuk mendeteksi di aktivitas trafik di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat dicegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi *early detection* dan *prevention* menjadi penekanan pada IPS ini [5].

2.5 Server

Server merupakan sebuah tempat yang dipenuhi dengan berbagai macam informasi, dimana *server* memiliki tugas utama untuk memberikan sebuah *service* atau layanan bagi para klien yang terhubung dengannya. Terdapat berbagai macam jenis *server* yang ada dengan fungsi yang berbeda-beda, misalnya saja web *server* yang digunakan untuk menyimpan data dalam sebuah web, FTP *server* yang menangani perpindahan file (transfer file), mail *server* yang melayani urusan email para klien, database *server* untuk menyimpan berbagai macam data atau file dan lain sebagainya [6].

2.6 Snort

Snort merupakan IDS yang gratis dan berbasis *open source* yang diciptakan oleh Martin Roesch pada tahun 1998. Snort dikembangkan oleh Sourcefire dengan Roesch sebagai pendiri sekaligus CTO dari Sourcefire. Snort sebagai IDS berbasis jaringan *open source* memiliki kemampuan untuk menganalisa lalu lintas jaringan secara *real time* dan pendataan paket pada IP jaringan [7].

Snort bekerja dengan melakukan analisa protokol, pencarian dan pencocokan konten, dan digunakan secara aktif untuk mendeteksi suatu serangan.

2.7 IPTables

IPTables adalah *Intrusion Prevention System* (IPS) dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalu lintas data dalam komputer, baik yang masuk ke komputer, keluar dari komputer, maupun sekedar melewati komputer. Secara sederhana digambarkan sebagai pengatur lalu lintas data.

IPTables merupakan *Firewall*, yang default di-install hampir semua distribusi Linux, seperti, Ubuntu, Kubuntu, Xubuntu, Fedora Core, dan lain-lain. IPTables sudah terinstall, tapi defaultnya mengizinkan semua trafik untuk lewat [8].

2.8 Security Policy Development Life Cycle (SPDLC)

Security Policy Development Life Cycle (SPDLC) adalah suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tiada awal dan akhirnya. Dalam membangun sebuah jaringan komputer mencakup lima tahap, yaitu *analysis, design, implementation, enforcement dan enhancement* [9].

2.9 Analisis Sistem yang Diajukan

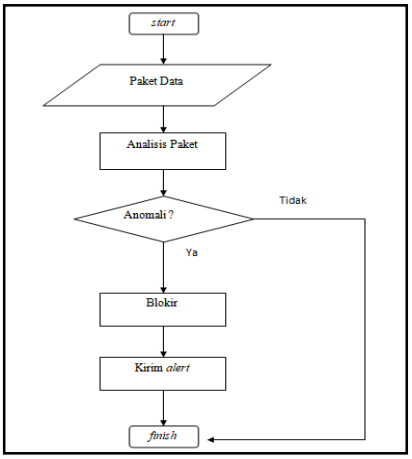
Sistem ini digunakan untuk mendeteksi dan mencegah gangguan/serangan yang terjadi pada *server* yang terhubung di jaringan *wireless* dan dapat memberi notifikasi kepada administrator.

Berikut alur kerja dari sistem yang diajukan:

1. Sistem IDPS menganalisa lalu lintas paket data pada *server* yang terhubung pada jaringan *wireless* sesuai dengan *rule*/aturan yang telah di terapkan pada sistem.
2. Apabila gangguan/serangan terdeteksi, sistem IDPS akan menyimpan *log* serangan dan mencegah serangan yang terjadi.
3. *Administrator* dapat memantau detail serangan yang terjadi pada *web* BASE.

2.10 Gambaran Umum Sistem

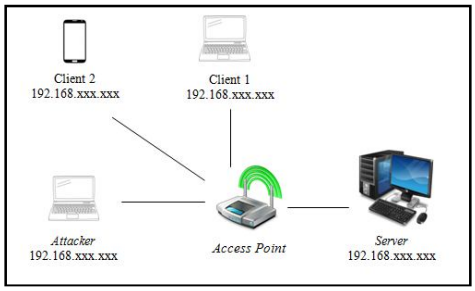
Gambaran umum sistem merupakan penjelasan umum dari proses sistem yang akan dibangun. Berdasarkan gambar 1, paket-paket data yang ada dalam lalu lintas jaringan akan diperiksa dan dianalisa oleh sistem. Jika paket tersebut tidak berisi anomali/serangan/ gangguan maka paket tersebut akan dilewati. Namun saat sistem mendeteksi suatu paket berisi anomali/serangan/gangguan maka proteksi menggunakan IDPS akan aktif, dimana IPS akan memblokir paket-paket yang berisi anomali/serangan/gangguan sebagai tindakan untuk menahan serangan dan IDS akan mengirimkan *alert* kepada *administrator* bahwa *server* yang terhubung pada jaringan *wireless* sedang mengalami serangan yang ditunjukkan oleh Gambar 1.



Gambar 1 Gambaran Umum Sistem

2.11 Rancangan Pengujian Sistem

Rancangan usulan *topologi* untuk pengujian sistem ditunjukkan oleh Gambar 2.



Gambar 2 Topologi Pengujian

Topologi yang akan digunakan pada pengujian sistem ini adalah *topologi star*, dimana dalam *topologi* tersebut ada PC (*Personal Computer*) yang akan berperan sebagai *attacker* untuk mengirimkan paket-paket berisi anomali/serangan/gangguan terhadap *server* melalui jaringan *wireless*, *access point* yang berperan sebagai penghubung, *client* 1 dan *client* 2 berperan sebagai *host* yang memiliki izin untuk mengakses *server*, kemudian *server* sebagai PC (*Personal Computer*) yang akan diserang dan berfungsi sebagai pendeteksi dan pencegah intrusi/serangan dari *attacker*. Pemilihan *topologi* star ditujukan untuk membuat simulasi menjadi lebih mudah dilakukan karena tipe serangan yang digunakan adalah *direct attack* atau serangan langsung yang terarah kepada *server*.

3. HASIL DAN PEMBAHASAN

3.1 Perintah Menjalankan IDS

Snort menjadi *tools* IDS dalam membangun sistem keamanan berbasis IDPS (*Intrusion Detection and Prevention System*). Alasan pemilihan snort sendiri dikarenakan snort lebih fleksibel untuk dikombinasikan dengan bahasa pemrograman mananpun. Selain snort ada *tools* tambahan yang digunakan yaitu barnyard2. Barnyard2 bertugas sebagai penghubung antara *log* snort dan *database mysql*, karena snort tidak lagi mendukung *mysql* di dalam paket instalasinya.

Untuk menjalankan sistem keamanan dengan mode IDS maka membutuhkan perintah seperti yang ditunjukkan oleh Gambar 3.

```
sudo /usr/local/bin/snort -q -u
snort -g snort -c
```

Gambar 3 Perintah Menjalankan Mode IDS

Berdasarkan Gambar 3, -q digunakan untuk melakukan mode *sniffing* paket yang berada dalam lingkup lalu lintas jaringan *server*, –u digunakan untuk menandakan *user* yang menggunakan, -g menandakan *group* dari *user* yang menggunakan sistem, -c digunakan untuk mengaktifkan konfigurasi , -i digunakan untuk inisialisasi *interface* jaringan yang digunakan untuk diamati oleh sistem dan -D digunakan untuk menjalankan sistem dalam mode *daemon*. Agar IDS dapat membuat *alert* maka dibutuhkan lagi satu baris perintah seperti yang ditunjukkan oleh Gambar 4.

```
sudo barnyard2 -c
/etc/snort/barnyard2.conf -d
/var/log/snort -f snort.u2 -
w/var/log/snort/barnyard2.waldo -g
snort -u snort
```

Gambar 4 Perintah Membuat *Alert*

Gambar 4 memilih perintah yang mirip dengan perintah sebelumnya namun ada beberapa fungsi tambahan dimana sistem akan membaca log dan me-*record* data ke *log snort*. Untuk –d digunakan untuk melihat isi paket pada *log*, -f digunakan untuk menentukan nama *file* yang akan dibaca dan –w digunakan untuk membuat *file waldo* yang nantinya akan dihubungkan dengan *database*.

3.2 Perintah Menjalankan IPS

IPTables menjadi *tools* IPS dalam membangun sistem keamanan berbasis IDPS (*Intrusion Detection and Prevention System*). Alasan pemilihan IPTables sendiri dikarenakan IPTables adalah *Intrusion Prevention System* (IPS) dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalu lintas data dalam komputer.

Untuk menjalankan sistem dalam *mode* IPS, dengan mengizinkan *client* tertentu agar dapat masuk ke *server* yang terhubung pada jaringan *wireless* maka digunakan perintah seperti yang ditunjukkan oleh Gambar 5.

```
iptables -A INPUT -s 192.168.43.36 -j
ACCEPT
iptables -A INPUT -s 192.168.43.1 -j
ACCEPT
iptables -A INPUT -s 192.168.43.72 -j
ACCEPT
```

Gambar 5 Perintah Menjalankan Mode IPS

Kemudian untuk memblokir *port* agar *client* yang tidak terdaftar sebelumnya tidak dapat mengakses *server* maka digunakan perintah seperti yang ditunjukkan oleh Gambar 6.

Perintah terakhir ini membuat tiap *client* yang tidak terdaftar dan memberikan paket yang mencurigakan akan diblokir.

Pada 2 perintah tersebut, IPTables digunakan untuk menjalankan tools IPTables, -A digunakan untuk menambahkan aturan yang telah dibuat. –p digunakan untuk mengecek tipe *protocol* tertentu, -s digunakan untuk mencocokkan paket berdasarkan alamat IP sumber, -dport digunakan untuk menentukan spesifik *port* yang akan diamati oleh sistem, -j digunakana untuk menentukan paket apakah akan diterima (ACCEPT) atau ditolak (DROP).

```
iptables -A INPUT -p icmp -s
192.168.43.0/24 -j DROP
iptables -A INPUT -p tcp -s
192.168.43.0/24 --dport 21 -j DROP
iptables -A INPUT -p tcp -s
192.168.43.0/24 --dport 22 -j DROP
iptables -A INPUT -p tcp -s
192.168.43.0/24 --dport 23 -j DROP
iptables -A INPUT -p tcp -s
192.168.43.0/24 --dport 80 -j DROP
iptables -A INPUT -j DROP
```

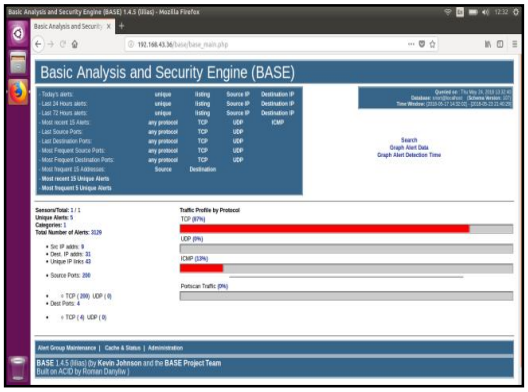
Gambar 6 Perintah Memblokir *Port*

3.3 Implementasi

Implementasi antarmuka (*interface*) *web* (BASE) ditunjukkan oleh Gambar 2 dan 3.

1. Tampilan Halaman Beranda

Pada halaman beranda berisi mengenai informasi jumlah serangan yang telah terjadi terhadap *server* berdasarkan *protocol* yang diserang seperti yang ditunjukkan oleh Gambar 7.



Gambar 7 Halaman Beranda

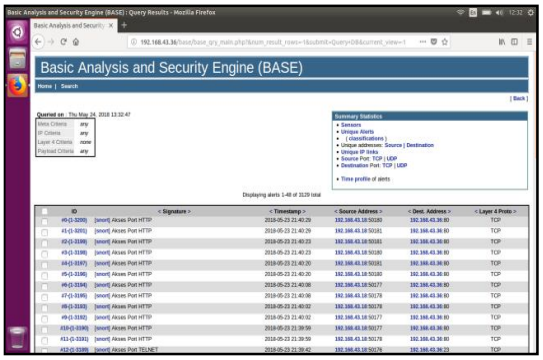
2. Tampilan Halaman Log Serangan

Halaman *log* serangan merupakan halaman yang menampilkan detail serangan yang terjadi terhadap *server*. Dimana pada halaman ini *log* serangan akan ditampilkan berdasarkan *timeline* waktu serangan terbaru seperti yang ditunjukkan oleh Gambar 8.

3.4 Pengujian Sistem

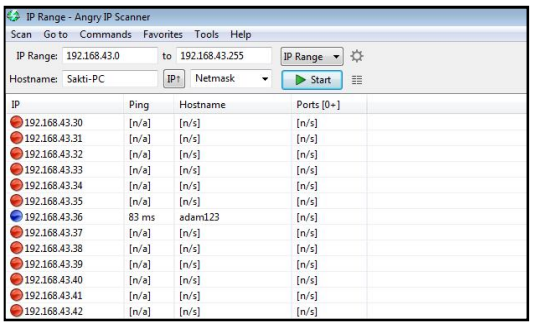
Pengujian sistem keamanan menggunakan IDPS (*Intrusion Detection and Prevention System*) dilakukan dengan menguji 5 port yaitu ICMP, FTP, SSH, *Telnet* dan HTTP. Pengujian dilakukan 2 kondisi pada masing-masing *port*, yaitu kondisi *server* yang

terhubung pada jaringan *wireless* dalam keadaan tidak terlindungi dan saat terlindungi dengan sistem IDPS.



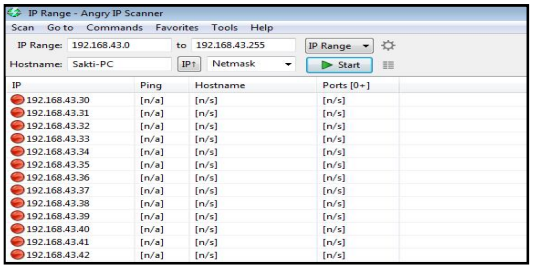
Gambar 8 Halaman *Log* Serangan

Pengujian terhadap *port* ICMP (*port* 138) dilakukan dengan mencoba mencari IP *Address server* menggunakan *Angry IP Scanner*. Saat keadaan *server* tidak mengaktifkan sistem IDPS, PC penyerang mampu mendeteksi IP *Address server* seperti yang ditunjukkan oleh Gambar 9.



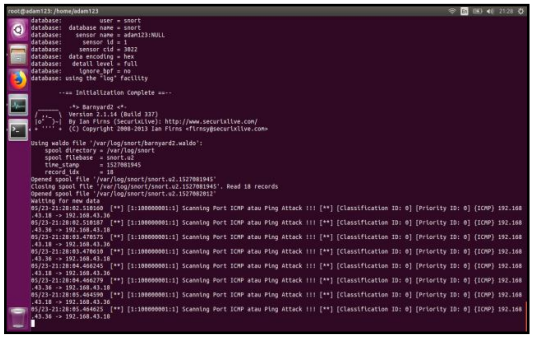
Gambar 9 *Scanning* IP *Server* Tanpa Perlindungan

Setelah sistem keamanan IDPS diterapkan terhadap *port* ICMP (138) dengan perintah *drop*, maka setiap percobaan pencarian IP *Address server* akan di blokir pada saat yang sama ditunjukkan oleh Gambar 10.

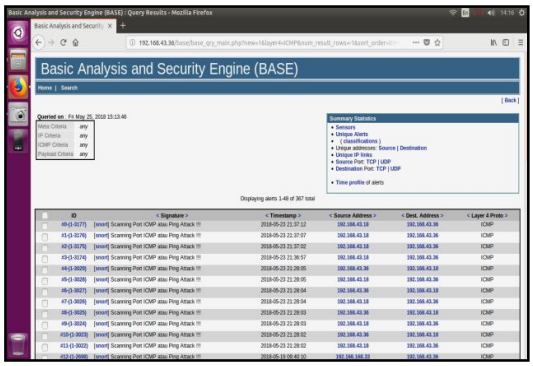


Gambar 10 *Scanning* IP *Server* dengan Perlindungan

Pada Gambar 10 terlihat bahwa percobaan mencari IP *Address server* diblokir sehingga penyerang tidak dapat mengetahui IP *Address server*. Setelah proses pemblokiran dilakukan oleh *server* maka notifikasi akan terkirim pada *administrator* seperti yang ditunjukkan oleh Gambar 11 dan 12.



Gambar 11 Notifikasi serangan *Port* ICMP pada Terminal



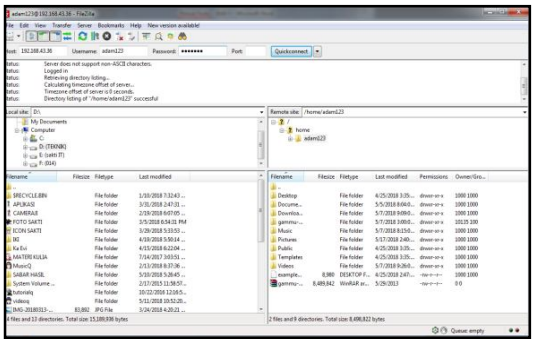
Gambar 12 Notifikasi serangan *Port* ICMP pada *web* (Base)

Pada Gambar 11 dan 12 dapat terlihat bahwa notifikasi penyerangan berhasil di terima. Dimana notifikasi yang diterima berisi informasi IP Address penyerang, IP *Address Server*, nama serangan, dan waktu serangan.

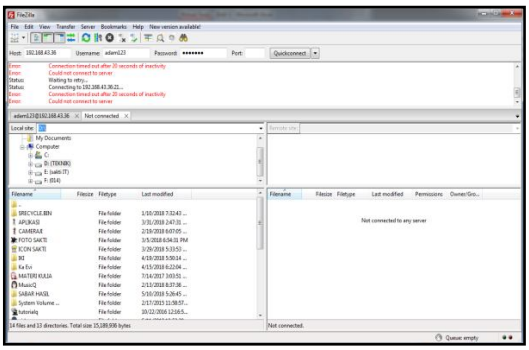
Pengujian terhadap *port* FTP (*port* 21) dilakukan dengan mencoba akses FTP ke IP *Address server* menggunakan aplikasi *Filezilla*. Saat keadaan *server* tidak mengaktifkan sistem IDPS, PC penyerang mampu melakukan *remote* FTP ke IP *Address server* seperti yang yang ditunjukkan oleh Gambar 13.

Saat melakukan akses *server* dengan login menggunakan akun "adam123" terlihat bahwa proses *remote server* menggunakan FTP berhasil dilakukan. Setelah sistem keamanan IDPS diterapkan terhadap *port* FTP

(21) dengan perintah *drop*, maka setiap akses *login* FTP yang ditujukan ke *server* akan di blokir dan memutuskan setiap kali mencoba *reconect* ke *server* seperti yang yang ditunjukkan oleh Gambar 14.

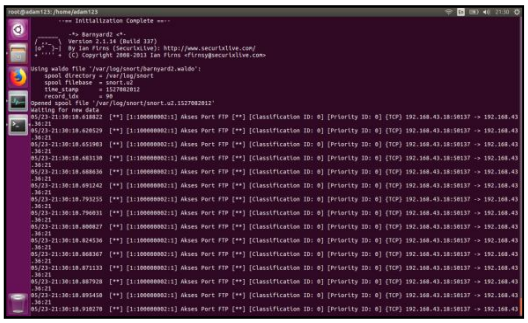


Gambar 13 *Remote* FTP Tanpa Perlindungan



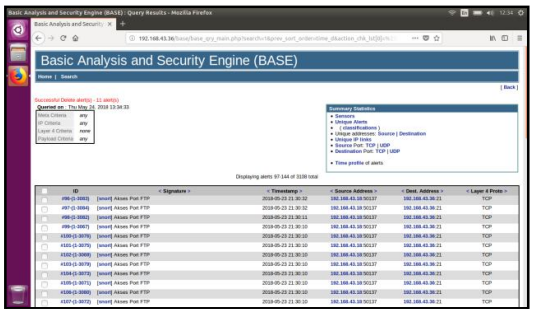
Gambar 14 *Remote* FTP dengan Perlindungan

Pada Gambar 14 terlihat bahwa kegiatan *login* FTP ke *server* akan mengalami *timeout* dan tidak diijinkan masuk meski memasukkan *username* dan *password* yang benar. Setelah proses pemblokiran dilakukan oleh *server* maka notifikasi akan terkirim pada *administrator* seperti yang ditunjukkan oleh Gambar 15 dan 16.



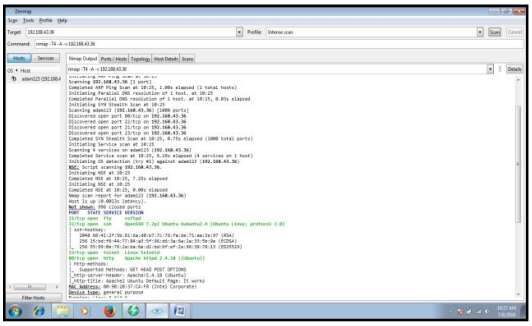
Gambar 15 Notifikasi Serangan *Port* FTP pada Terminal

Pada Gambar 15 dan 16 dapat terlihat bahwa notifikasi penyerangan berhasil di terima. Dimana notifikasi yang diterima berisi informasi IP Address penyerang, IP *Address Server*, nama serangan, dan waktu serangan.



Gambar 16 Notifikasi Serangan *Port* FTP pada *Web* (BASE)

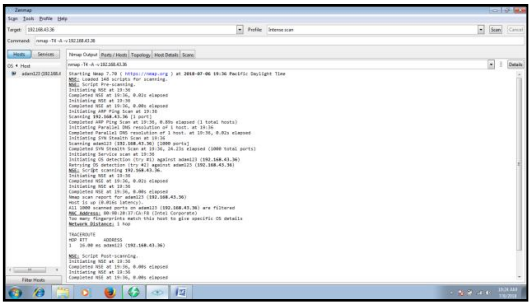
Pengujian terhadap *port scanning* dilakukan dengan mencoba mencari port yang dapat di akses melalui IP *Address server* menggunakan aplikasi *Zenmap*. Saat keadaan *server* tidak mengaktifkan sistem IDPS, PC penyerang dapat mendeteksi *port server* yang terbuka seperti yang ditunjukkan oleh Gambar 17.



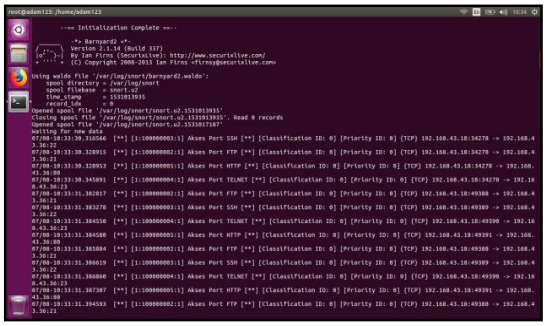
Gambar 17 *Port Scanning* Tanpa Perlindungan

Saat melakukan akses *server* terlihat bahwa proses *port scanning* pada *server* berhasil dilakukan. Setelah sistem keamanan IDPS diterapkan terhadap *server* dengan perintah *drop*, maka aktifitas *port scanning* yang ditujukan ke *server* akan di blokir dan memutuskan setiap kali mencoba *reconect* ke *server* seperti yang ditunjukkan oleh Gambar 18.

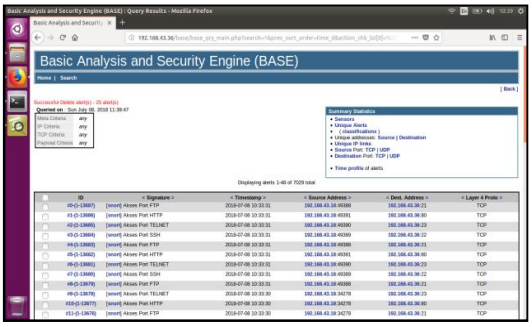
Pada Gambar 18 terlihat bahwa kegiatan *port scanning* ke *server* akan mengalami *timeout*. Setelah proses pemblokiran dilakukan oleh *server* maka notifikasi akan terkirim pada *administrator* seperti yang ditunjukkan oleh Gambar 19 dan 20.



Gambar 18 *Port Scanning* dengan Perlindungan



Gambar 19 Notifikasi Serangan *Port Scanning* pada Terminal

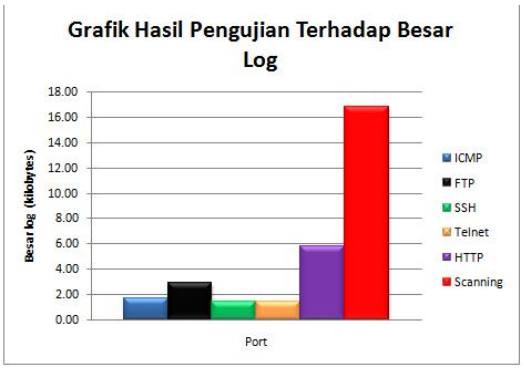


Gambar 20 Notifikasi serangan *Port Scanning* pada *web* (Base)

Pada Gambar 19 dan 20 dapat terlihat bahwa notifikasi penyerangan berhasil di terima. Dimana notifikasi yang diterima berisi informasi IP Address penyerang, IP *Address Server*, nama serangan, dan waktu serangan.

Setelah melakukan pengujian terhadap 5 *port*, hasil pengujian terhadap besar *log* yang dihasilkan dengan percobaan serangan sebanyak 5 kali menggunakan 3 penyerang secara bersamaan. Hasil pengujian seperti yang ditunjukkan oleh Gambar 21.

Pada Gambar 21, *bar* biru menunjukan besarnya *file log* yang dihasilkan saat penyerangan terhadap *port* ICMP dengan rata-rata *file log* sebesar 1,7 *kilobytes*, *bar* hitam menunjukan besarnya *file log* yang dihasilkan saat penyerangan terhadap *port* FTP dengan rata-rata *file log* sebesar 2,9 *kilobytes*, *bar* hijau menunjukan besarnya *file log* yang dihasilkan saat penyerangan terhadap *port* SSH dengan rata-rata *file log* sebesar 1,4 *kilobytes*, *bar* jingga menunjukan besarnya *file log* yang dihasilkan saat penyerangan terhadap *port Telnet* dengan rata-rata *file log* sebesar 1,4 *kilobytes, bar* ungu menunjukan besarnya *file log* yang dihasilkan saat penyerangan terhadap *port HTTP* dengan rata-rata *file log* sebesar 5,8 *kilobytes,* dan *bar* merah menunjukan besarnya *file log* yang dihasilkan saat penyerangan menggunakan *port Scanning* dengan rata-rata *file log* sebesar 16,8 *kilobytes*.



Gambar 21 Grafik Hasil Pengujian Terhadap Besar Log

4. KESIMPULAN

Berdasarkan penelitian dan hasil pengujian yang dilakukan pada penelitian ini, maka dapat disimpulkan:

1. Pembuatan sistem keamanan *server* pada jaringan *wireless* menggunakan IDPS (*Intrusion Detection and Prevention System*) dapat mendeteksi dan mencegah adanya upaya-upaya penyerangan atau penyusupan yang terjadi terhadap *server* yang terhubung pada jaringan *wireless.*
2. Sistem keamanan *server* pada jaringan *wireless* menggunakan IDPS (*Intrusion Detection and Prevention System*) telah berhasil mendeteksi dan mencegah upaya-upaya penyerangan atau penyusupan yang menggunakan berbagai macam *tools* seperti *Angry IP Scanner, Filezilla, Putty, mozila firefox* dan *Zenmap.*

3. Sistem keamanan *server* pada jaringan *wireless* menggunakan IDPS (*Intrusion Detection and Prevention System*) yang dikembangkan juga telah dapat memberikan *alert* atau pesan peringatan sedini mungkin ketika terjadinya upaya-upaya penyerangan atau penyusupan pada s*erver* yang terhubung pada jaringan *wireless*.
4. Rata-rata besar file log pada *port* ICMP adalah 1,7 kb, pada *port* FTP adalah 2,9 kb , pada *port* SSH adalah 1,4 kb, pada *port* TELNET adalah 1,4 kb, pada *port* HTTP adalah 5,8 kb dan pada *port Scanning* adalah 16,8 kb.

5. SARAN

Saran yang dapat diberikan untuk pengembangan lebih lanjut terhadap penelitian ini yaitu penambahan fitur notifikasi agar dapat memberikan informasi secara *realtime* terhadap gangguan yang terjadi pada *server* dan dapat menggunakan *tools* IDPS lain untuk membandingkan besar *log* serangan yang dihasilkan.

DAFTAR PUSTAKA

[1] L. Putri, "Implementasi Intrusion Detection System Menggunakan Snort Pada Jaringan Wireless (Studi Kasus : SMK Triguna Ciputat)," Universitas Islam Negeri, 2011.

[2] Irawan, *Jaringan Komputer untuk Orang Awam*. Palembang: Maxikom, 2013.

[3] M. Rajab, "Analisa dan Perancangan Wireless LAN Security Menggunakan WPA2-RADIUS," Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2010.

[4] D. Ariyus, *Intrusion Detection System*. Yogyakarta: Andi, 2007.

[5] G. P. Digdo, "Simulasi Ancaman Keamanan pada Aplikasi Berbasis Web," Universitas Komputer Indonesia, 2012.

[6] N. Aliya, "Pengertian Server, Fungsi Server Beserta Cara Kerja dan Jenis-jenis Server," 2018. [Online]. Available: http://nesabamedia.com/pengertian-server-dan-fungsi-server/. [Accessed: 10-May-2018].

[7] B. Y. Pradana, "Membandingkan Kemampuan Deteksi Intrusion Detection System (IDS) Snort dan Suricata Berbasis Aturan/Rules Standar Pengembang," Universitas Sanata Dharma, 2016.

[8] O. W. Purbo, *Workshop Onno : Panduan Mudah Merakit Dan Menginstall Server Linux*. Jakarta: Andi Publisher, 2008.

[9] L. A. Wahsheh and J. A. Foss, "Security Policy Development : Towards a Life-Cycle and Logic-Based Verification Model," *Am. J. Appl. Sci.*, Vol. 5, No. 9, pp. 1117–1126, 2008.