e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 5 No. 1, Juni, 2021, **Hal. 60-69**
DOI: 10.29408/edumatic.v5i1.3278

Perancangan *Security Network Intrusion Prevention System* Pada PDTI Universitas Islam Raden Rahmat Malang

Farid Wahyudi[*1], Listanto Tri Utomo[2]
[1]Program Studi Sistem Informasi, Universitas Islam Raden Rahmat
[2]Program Studi Teknik Informatika, Universitas Islam Raden Rahmat
email: faridstifler@gmail.com*[1], listantotri@gmail.com[2]

(Received: 31 Maret 2021/ Accepted: 28 April 2021 / Published Online: 20 Juni 2021)

Abstrak

Keamanan sangat penting dalam jaringan komputer, dimana banyak perangkat yang terhubung satu sama lain untuk berinteraksi dan bertukar data tanpa batas. Keamanan jaringan juga merupakan masalah yang sangat penting untuk diprioritaskan keberadaannya salah satunya adalah dengan menggunakan sistem pencegahan intrusi. Pada PDTI UNIRA sering terjadi ada masalah-masalah keamanan jaringan, salah satu yang sering adalah ketika musim ujian, server banyak mengalami masalah intrusi. Tujuan dari penelitian ini adalah untuk mengembangkan sebuah sistem IPS berdasarkan analisis pada PDTI Universitas Islam Raden Rahmat Malang. Metode Penelitian ini menggunakan pendekatan pengembangan keamanan komputer yaitu *Intrusion Prevention System* (IPS), dengan menggabungkan metode rekayasa *firewall* dan *Intrusion Detection System* (IDS). Hasil dari penelitian ini adalah teknologi yang dapat digunakan untuk mencegah serangan yang akan masuk ke kejaringan lokal mengecek dan merekam semua paket data serta mengenali paket sensor, saat serangan telah teridentifikasi, IPS akan menolak akses (blokir) dan mencatat (log) semua paket data yang teridentifikasi. Jadi IPS berperan sebagai *firewall* yang akan mengijinkan dan memblokir digabungkan dengan IDS yang dapat mendeteksi paket secara detail. Dengan adanya sebuah system keamanan jaringan tersebut server PDTI Unira malang lebih aman dan dapat terhindar dari intrusi.

Kata kunci: IPS, *Intrusion Prevention System*, *Early detection*, Keamanan Jaringan

Abstract

Security is very main in computer networks, where many devices are connected to each other to interact and exchange data without limits. Network security is also a very important issue to prioritize, one of which is to use an intrusion prevention system. At PDTI UNIRA there are often network security problems, one of which is that during the test season, the server experiences many intrusion problems. The purpose of this research is to develop a social science system based on the analysis at PDTI of Raden Rahmat Islamic University Malang. This research method uses a computer security development approach, namely the Intrusion Prevention System (IPS), by combining firewall engineering methods and Intrusion-Detection System (IDS). The result of this research is a technology that can be used to prevent attacks that will enter the local network checking and recording all data packets and recognizing sensor packets, when the attack has been identified, IPS will deny access (block) and record (log) all data packets. identified. So IPS acts as a firewall that will allow and block combined with IDS that can detect packets in detail. With a network security system, the Unira PDTI server is safer and can avoid intrusion.

Keywords: *IPS, Intrusion Prevention System, Early detection, Network Security*

PENDAHULUAN

Keamanan jaringan pada era digital sekarang ini sangat diperukan, karena semua kegiatan yang dilakukan untuk operasional kampus sehari-hari saling terkoneksi satu sama lain. Hal ini dapat menimbulkan manfaat yang banyak dan juga bisa menimbulkan suatu

celah negatif yang dapat merugikan kampus, salah satu diantaranya jika terjadi intrusi yang dapat mengakibatkan data hilang atau kejadian yang lebih parah lagi. Pada PDTI Universitas Islam Raden Rahmat akibat semakin banyak aplikasi yang saling terintegrasi dengan situs kampus dan juga aplikasi ujian yang sangat penting mendukung proses pembelajaran, sehingga banyak juga pihak-pihak yang tidak bertanggung jawab ingin merusak sistem yang sudah ada dengan tujuan tertentu, salah satu diantaranya adalah meminta uang jaminan dengan meretas halaman utama dari situs. Hal tersebut merupakan masalah yang harus segera ditangani, maka penelitian ini untuk memberikan solusi atas permaslahan tersebut dikembangkan sebuah keamanan jaringan menggunakan pendekatan *Intrusion Prevention System* (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer. Sampai saat ini IPS telah menjadi "*The New Brand*" bagi para vendor, mereka berlomba – lomba untuk membuat solusi IPS, begitu pula dengan PDTI Universitas Islam Raden Rahmat Malang.

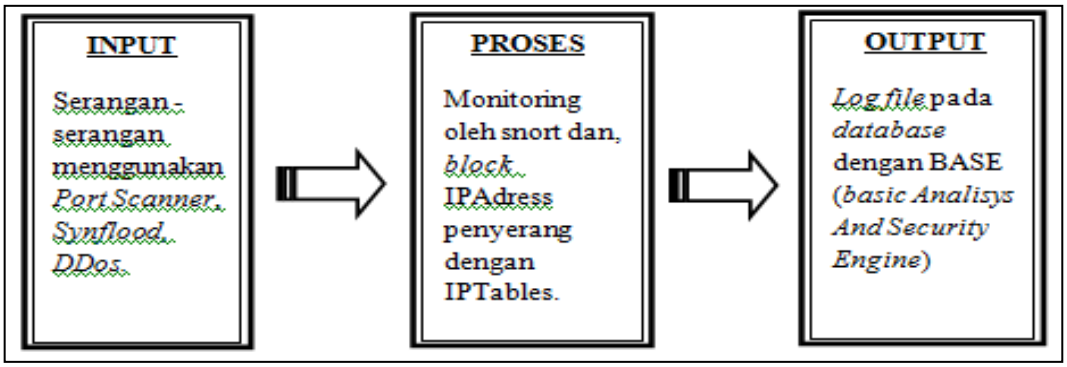
IPS adalah sistem yang dapat mendeteksi aktivitas yang mencurigakan pada sistem atau jaringan (Panggabean, 2018; Riadi, Fadlil, & Hafizh, 2020; Suhartono, Riyanto, & Astomo, 2015). Perangkat lunak ini menganalisis semua lalu lintas di *firewall* mencari serangan dan anomali yang diketahui (Mentang, Sinsuw, Najoan, & Elektro-ft, 2015). *Intrusion Prevention System* dapat memberikan peringatan saat berhasil mendeteksi suatu aktivitas mencurigakan kepada administrator dan kemudian perangkat lunak ini akan melakukan pencegahan secara langsung.*Intrusion Prevention System* (IPS) memberikan kemampuan untuk mengenali, mengidentifikasi, dan mencegah serangan yang terjadi secara otomatis (Prakosa, Hendrawan, & Apriana, 2015). Integrasi IPS ke dalam jaringan *Software Defined Network* (SDN) memberikan keuntungan bahwa administrator dapat mengatur dan memonitor keamanan jaringan secara terpusat, karena serangan yang dicegah adalah di level perangkat bukan host (Nugroho & Suwastika, 2018). Sistem yang dibangun yaitu *intrusion detection system* menggunakan *snort* yang mempunyai fungsi untuk memonitoring trafik jaringan wireless, mencari paket data atau tingkah pola yang mencurigakan untuk dicatat kedalam log dan memberitahukan peringatan kepada administrator jaringan (Sobari, 2015). *Firewall* sangat rentan akan usaha penyusupan (intrusi) yang dilakukan oleh pengguna yang tidak punya hak akses atau *intruder*, yang menyebabkan sistem jaringan tidak dapat menjalankan tugas pelayanan terhadap pengguna dengan optimal (Gozali & Setiaji, 2013). Berdasarkan penelitian – peneltian terdahulu yang sudah dilakukan menggunakan salah satu metode saja untuk membangun keamanan system jaringannya (Akbar, Widiartha, Pada, & Ips, 2015; Arsin, Yamin, & Surimi, 2017; Gozali & Setiaji, 2013). Pada penelitian ini mengkombinasikan pendekatan IPS dengan teknik *firewall* dan *Intrusion Detected System* (IDS) serta menggunakan *snort*.

Tujuan dari penelitian ini adalah mengembangkan sebuah keamanan jaringan menggunaan pendekatan IPS khususnya pada PDTI Universitas Islam Raden Rahmat Malang, karena banyak pengakses yang mengunjungi situs kampus baik intranet maupun internet sehingga sebagai unit pengelola jaringan kampus ingin memberikan keamanan yang maksimal. Tercatat kurang lebih 1000 pengunjung situs kampus perharinya membuat rawan terhadap intrusi. Oleh karena itu perancangan monitoring dan *security network* IPS diharapkan bisa memberikan jaminan keamanan jaringan khusunya PDTI Universitas Islam Raden Rahmat Malang.

METODE

Metode penelitian yang digunakan pada penelitian ini adalah metode penelitian pengambangan keamanan sistem jaringan menggunakan pendekatan IPS (*Intrusion Detected System*) dimana tahap pertama yang dilakukan adalah melakukan perancangan server yang kemudian dilanjutkan dengan perancangan sistem, dibutuhkan 1 buah server IPS yang telah

di install *Ubuntu Server*, *Snort Inline*, MySQL sebagai *database* dari *Snort* untuk mencegah sebuah serangan. Pada *Attacker* terinstal *tools* serangan diantaranya DDoS yang akan digunakan untuk menyerang server IPS. Skema proses secara umum sistem *Intrusion Prevention System* (IPS) pada sebuah jaringan ini memiliki beberapa tahapan seperti pada gambar 1 berikut.



Gambar 1. Skema Proses IPS

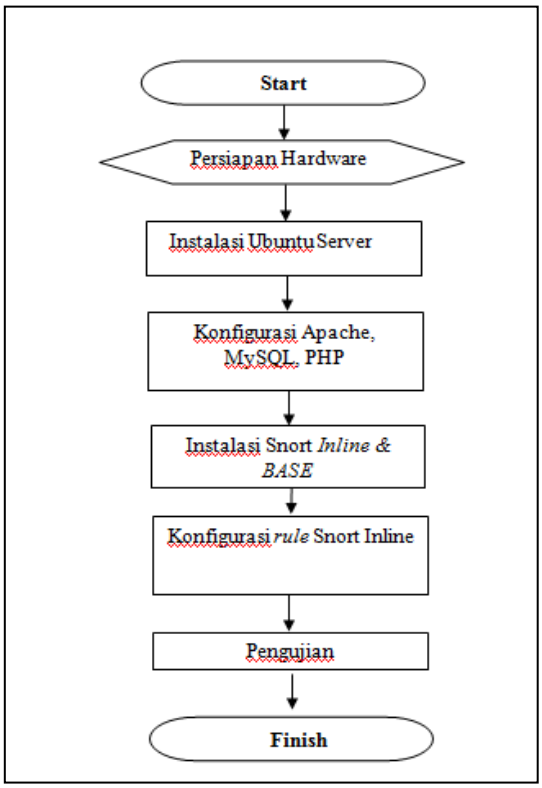
Metodologi Perancangan Server

Ubuntu Server merupakan sistem operasi yang mendukung banyak sekali aplikasi-aplikasi server yang handal. Karena Ubuntu mempunyai sebuah *repository* (Dahlan & Zulianto, 2019; Tambunan, Raharjo, & Purwadi, 2013). PuTTY adalah sebuah program klien untuk protokol jaringan SSH, Telnet, dan Rlogin. Semua protokol ini digunakan untuk menjalankan sebuah *remote session* pada sebuah komputer, menggunakan sebuah jaringan (Tambunan et al., 2013). *Snort* merupakan *software open source* yang berfungsi sebagai *Intrusion Detected System* (IDS) yang mampu mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi (Alamsyah, -, & Al Akbar, 2020). Pola atau *rules* tersimpan berkas atau files yang dapat dikonfigurasikan sesuai kebutuhan. *Snort* dikonfigurasikan menggunakan *comment lines switches* atau *optional Berkeley packet* (BPF) *commands* (Sutarti, Pancaro, & Saputra, 2018). *Snort Inline* adalah kombinasi dari snort dan IPtables yang berlaku sebagai *firewall* untuk mencegah terjadinya serangan lebih dini karena mampu allow atau block paket yang lewat (Siregar, Dwiputra Purba, Seniman, & Fahmi, 2018).

BASE (*Basic Analisys And Security Engine*) berfungsi untuk menampilkan hasil deteksi snort agar dapat ditampikan dalam bentuk grafik, digunakan untuk mengelola data - data *security event*, keuntungan menggunakan BASE diantaranya, log - log yang tadinya susah dibaca menjadi mudah dibaca, serta data - data dapat dicari dan difilter sesuai dengan kriteria tertentu (Siregar et al., 2018). *Software* pendukung untuk aplikasi diperlukan adalah Mysql, PHP dan Apache webserver. Apache berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP. Sama seperti web server lainya *apache* bertanggung jawab pada *request-response* HTTP, serta untuk menjalankan PHP dan mySQL (Arsin et al., 2017). Fungsi PHP-MYSQL adalah suatu fungsi yang menjembatani antara PHP sebagai Programing web server (Kusrini, Fathurrahmani, & Sayyidati, 2020; Sabirin, Sulistiyarini, & Zulkarnain, 2020), dan MySQL sebagai database (Ramadhan & Santika, 2020), sehingga data - data yang terdapat pada database MySQL dapat ditampilkan pada *browser* (Fadhlurrahman & Capah, 2020; Mentang et al., 2015; Ulfa & Megawaty, 2015).

Skema Perancangan Sistem

Membangun jaringan tidak terlepas dari IP *Address* untuk menghubungkan perangkat satu dengan lainnya. Untuk pengalamatan pada pembuatan radius *server* ini menggunakan alamat IP versi 4 dengan panjang 32 bit, karena pembuatan server Intrusion *Prevention system* masih dalam skala kecil. TCP/IP menggunakan *address class* untuk memutuskan mengetraksi *network part* dan *host* part. Berdasarkan aturan, *address* paling rendah dalam range digunakan sebagai *address* jaringan yang nantinya memudahkan penentuan *address* jaringan untuk digunakan dalam kode keputusan *routing* pada pembuatan sytem menggunakan IP Addresss kelas C, IP Address standar jaringan. Untuk alamat server yang didalamnya terdapat *snort Inline*, dan *firewall* digunakan *mode bridging* diamana *interface* dari eth0 dan eht1 dijembatani oleh br0.



Gambar 2. Skema Perancangan Sistem

HASIL DAN PEMBAHASAN

Hasil

Perancangan Sistem

Sebelum melakukan pengujian terhadap IPS (*Intrusion Prevention System*) yang telah dibuat, terlebih dahulu harus menyiapkan beberapa *software* / *tools attacker* yang nantinya akan digunakan sebagai melihat nilai acuan yang akan digunakan sebagai batasan agar suatu serangan dapat terdeteksi oleh IPS (*Intrusion Prevention System*), sekaligus sebagai sarana untuk menentukan jenis dari serangan tersebut

Instalasi Ubuntu Server

Proses instalasi sistem operasi dilakukan melalui CD-Drive dengan CD Ubuntu Server 12.04 LTS. Setelah proses instalasi selesai, maka penulis melakukan perintah update pada sistem, yang berfungsi untuk melakukan pembaharuan terhadap data *repository* :

```
# apt-get install update
```

Konfigurasi IP *Address*

Sebelum mengkonfigurasi IP server IPS terlebih dahulu menginstal `#apt-get install bridge-utils`. Pada gambar 3 merupakan *setting mode bridge* pada IP *address server* untuk menjembatani *interface* eth0 dan eth1 dalam satu *network*.

```
# Vi /etc/network/interface
```

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto eth0
#iface eth0 inet static
auto br0
iface br0 inet static
        address 192.168.91.136
        netmask 255.255.255.0
        broadcst 192.168.91.0#
        gateway 192.168.91.1
##port you want to add to your bridge
bridge_ports eth0 eth1
#time to wait before loading the bridge
bridge_maxwait 0
```

Gambar 3. Konfigurasi IP addres

Instalasi *Snort Mode Inline*

Berikut sedikit tampilan dari proses instalasi *Snort Mode Inline*, dimana menunjukkan bahwa instalasi *snort* dengan *mode inline* telah berhasil (lihat gambar 3).

```
root@Mr:~# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.0.1 (Build 72) inline
   ''''    By Martin Roesch & The Snort Team:
http://www.snort.org/team.html
           (C) Copyright 1998-2007 Sourcefire
Inc., et al.
           Using PCRE version: 8.12 2011-01-15

root@Mr:~#
```

Gambar 4. *Snort Mode Inline*

Konfigurasi *Snort* IPS

Berikut merupakan konfigursi *snort* dengan database *mysql* sehingga *log* dari *snort* bisa disimpan di *database* yang terlihat pada gambar 5.

```
#   output alert_syslog: LOG_AUTH LOG_ALERT
output database: log, mysql, dbname=snort user=root password=toor  host=localhost
# }
```

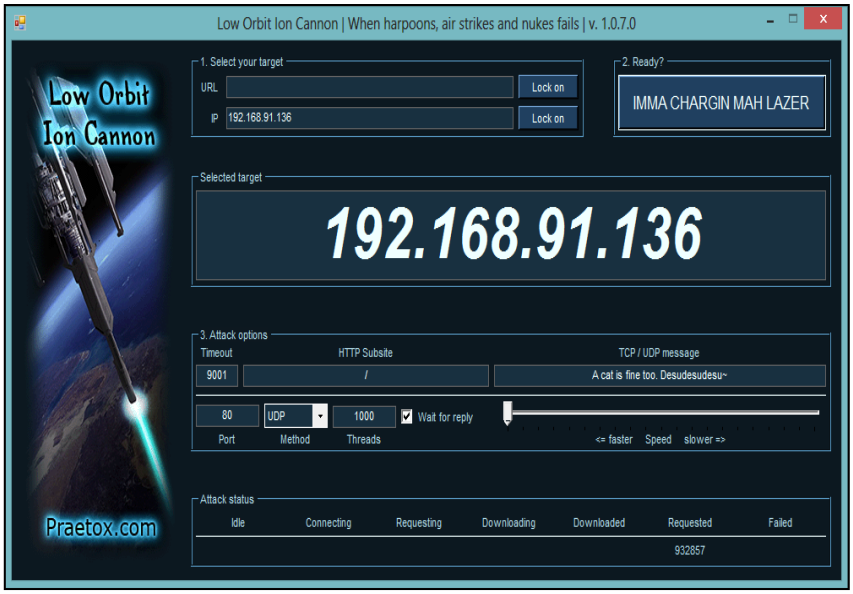
Gambar 5. Konfigurasi *database snort*

Pengujian Sistem

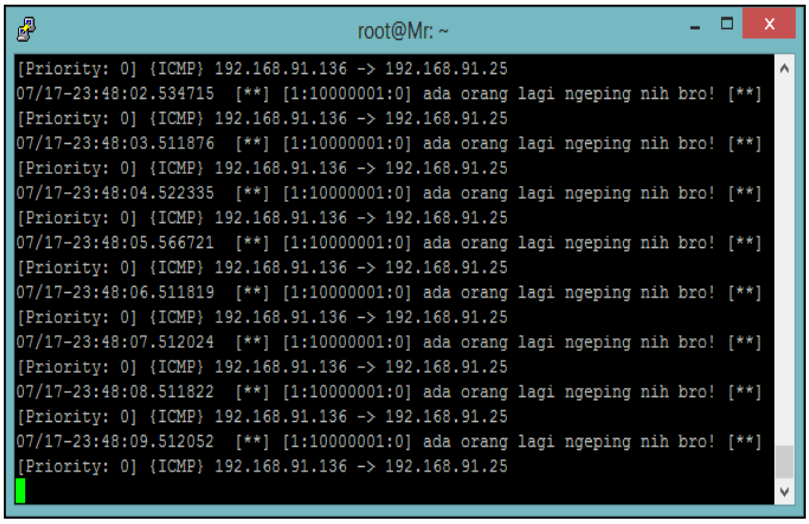
Pengujian sistem dilakukan dengan melakukan serangan DDos, *Portscan* dan performa *server* IPS.

DDos

Melakukan DDos *flooding* menggunakan LOIC terhapda server IPS. Pada gambar 6. menunjukkan proses serangan ke IP address server di 192.168.91.136 dengan menggunakan DDos. Sementara itu pada gambar 7 merupakan proses dari IPS yang mendeteksi adanya serangan DDos.



Gambar 6. DDos dengan LOIC

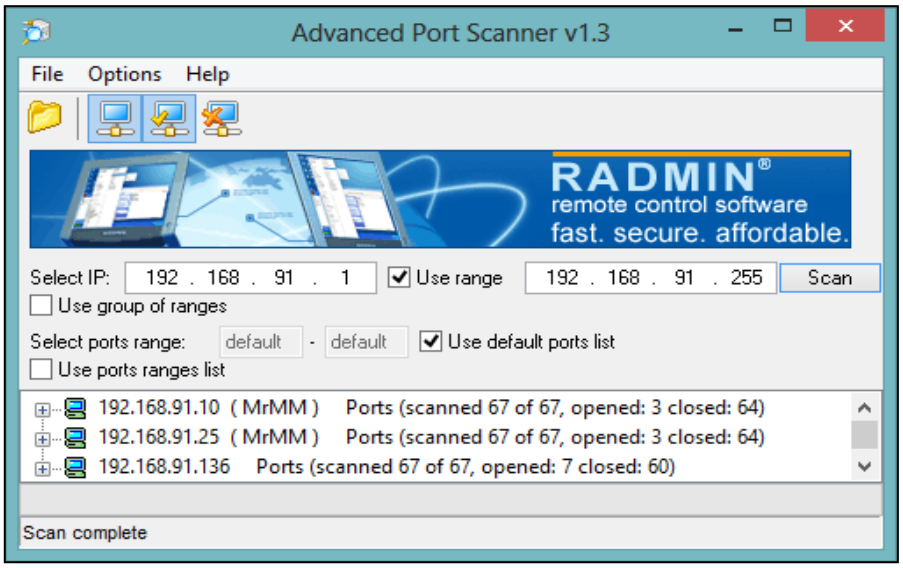


Gambar 7. Hasil serangan DDos

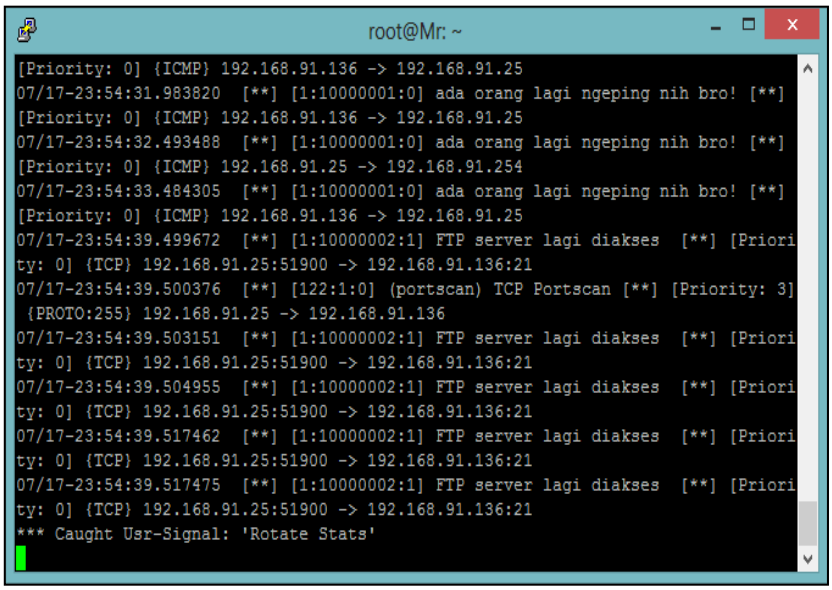
Port Scanning

Scanning port pada server IPS menggunakan *software Advanced Port Scanner* v1.3 untuk mencari beberapa informasi penting pada *server* yang mungkin dapat digunakan oleh *attacker* atau penyerang untuk menentukan kelemahan yang miliki suatu sistem. *Advanced Port Scanner* v1.3 memiliki fungsi sebagai *scan* terhadap *port*, *ping scan* secara *default*. *Advanced Port Scanner* v1.3 melakukan sebuah ping scan untuk mengetahui *port* yang dalam

keadaan terbuka. Pada gambar 8 merupakan tampilan dari penyerangan terhadap *port scanning*. Sementara itu, Pada gambar 9 merupakan proses dari IPS yang mendeteksi adanya *port scanning*. Dengan adanya *port scanning* tersebut dapat diketahui bahwa adanya penyerang yang masuk terhadap situs, sehingga dapat dilakukan pencegahan oleh sistem IPS. Selain itu kita juga perlu melakukan ceking terhadap performa dari server IPS apakah berjalan dengan baik atau tidak dalam mendeteksi dan mencegah terjadinya penyerangan terhadap situs.



Gambar 8. *Port Scaning*

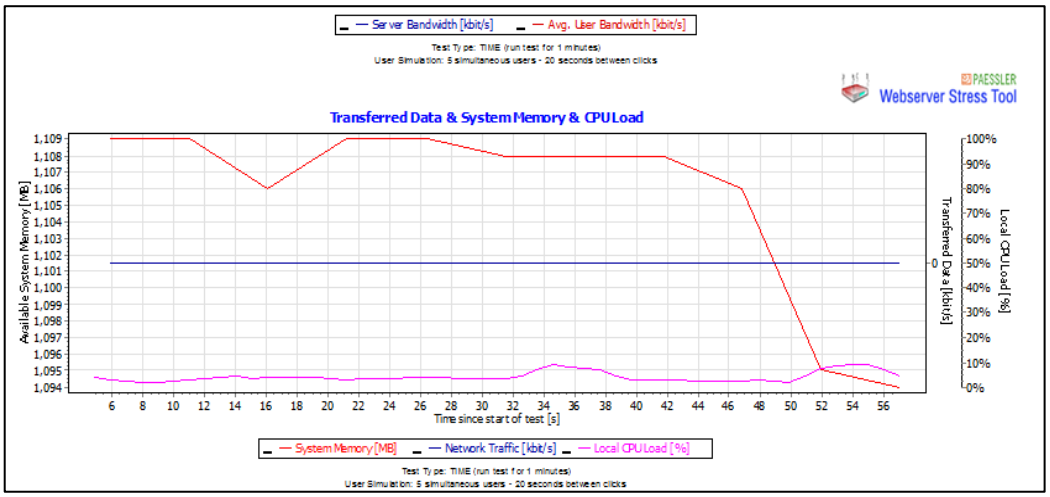


Gamabr 9. Hasil *Port Scaning*

Performa server IPS

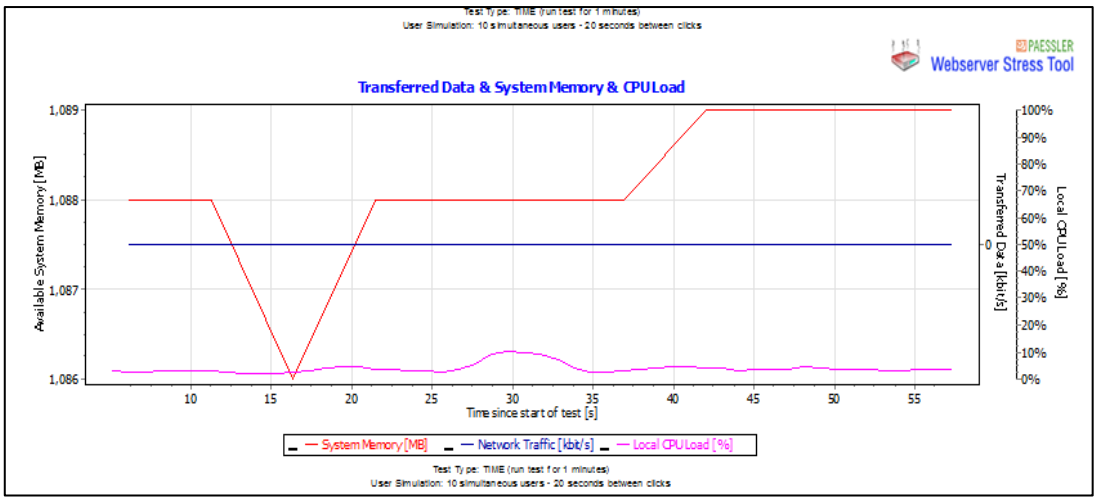
Untuk mengetahui seberapa performa *Server* IPS maka digunakan aplikasi *Webserver Strees* Tool dengan perbandingan 5 dan 10 user dan kemudian akan ditampilkan dalam bentuk grafik.

1. Pengetesan dengan *User* 5
   Pada gambar 10 merupakan proses pengetesan performa sistem IPS dengan menggunakan 5 *user* dan *sistem memory*, *traffic network* dan *local* CPU *load*.



Gambar 10. Hasil Grafik dengan *user* 5

2. Pengetesan dengan *User* 10
   Pada gambar 11 merupakan proses pengetesan performa sistem IPS dengan menggunakan 10 *user* dan *sistem memory*, *traffic network* dan *local* CPU *load*.



Gambar 11. Hasil Grafik dengan *user* 10

Pembahasan

Hasil *port scanning* yang dilakukan menggunakan *software Advanced Port Scanner v1.3* dideteksi adanya beberapa serangan terhadap *web* yang terbaca pada log file *port scanner*, Serangan tersebut jika tidak segera diatasi dapat menyebabkan kerusakan yang fatal terhadap web maka dari itu dilakukan pengujian performa server IPS terhadap beberapa serangan pada pengujian di atas menggunakan 10 *user*, dengan hasil *Server* IPS menunjukan kinerja memori yang tinggi sehingga menyebakan *neck bottle*, sedangkan kinerja CPU *load* tidak terlalu tinggi. Dari proses percobaan *port scanning* dan pengujian performa server IPS, maka dapat diperoleh bahwa keamanan sistem jaringan yang menggunakan pendekatan IPS berjalan dengan baik, yaitu dapat mendeteksi dan mencegah terjadinya penyerangan terhadap situs yang dapat mengakibatkan intrusi. Dengan pengujian maksimal 8 user *server* IPS

menunjukan kinerja yang mulai menurun dan mengakibatkan serangan yang dilakukan *attacker* dapat berhasil (Alamsyah et al., 2020). Pada penelitian ini dengan mengkombinasikan *Intrusion Prevention System* mengkombinasi teknik *firewall* dan *Intrusion Detected System* (IDS), maka walaupun melebihi 8 *user* yaitu pengujian sampai 10 *user* sistem *server* IPS masih dapat bertahan bekerja dengan baik dan mencegah terjadinya serangan yang mengakibatkan kerusakan pada web.

SIMPULAN

Hasil dari implementasi dan pengujian yang telah dilakukan dapat diambil kesimpulan yaitu dengan anasila topologi jaringan di PDTI Universitas Islam Raden Rahmat Malang didapatkan topologi perancangan untuk pembuatan server IPS, untuk menjembatani dua buah *interface* jaringan maka digunakan *bridging* untuk konfigurasi jaringannya. Sistem IPS (*Intrusion Prevention System*) dapat membantu administrator (pengelolah jaringan) dalam memonitoring terhadap suatu jaringan ketika terjadi sebuah *intruder*. Dari segi pengola jaringan atau administrator dengan adanya *port scanning* dapat melihat *log file intruder* pada *log file* yang di integrasikan dengan BASE. Sistem IPS mampu bekerja seperti yang diharapkan dalam hal menangani intruder dalam bentuk DDos dan Portscan serta performa CPU server IPS saat menjalankan IPS tidak terlalu tinggi sedangkan kinerja dari sistem memori sangat tinggi.

REFERENSI

Akbar, S. I., Widiartha, I. B. K., Pada, A., & Ips, S. (2015). *Intrusion Prevention System Pada Server*. *2*(1), 27–31.

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, *5*(1), 17–24. https://doi.org/10.31328/jointecs.v5i1.1240

Arsin, F., Yamin, M., & Surimi, L. (2017). Implementasi Security System Menggunakan Metode IDPS (Intrusion Detection and Prevention System) Dengan Layanan Realtime Notification. *SemanTIK*, *3*(2), 39–48.

Dahlan, & Zulianto, A. (2019). Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) yang Diintegrasikan dengan Access Control List (ACLs). *Scientia Regendi*, *I*(1), 86–96.

Fadhlurrahman, M., & Capah, D. (2020). Aplikasi Penyewaan Lapangan Futsal Berbasis Web. *Edumatic: Jurnal Pendidikan Informatika*, *4*(2), 30–39. https://doi.org/10.29408/edumatic.v4i2.2412

Gozali, F., & Setiaji, A. L. (2013). Perancangan Dan Analisis Sistem Pendeteksi Intrusi Berbasis Network Intrusion Detection System (Nids) Pada Sistem Keamanan Jaringan Komputer. *Jetri*, *11*(1), 1–16.

Kusrini, W., Fathurrahmani, F., & Sayyidati, R. (2020). Sistem Pakar untuk Diagnosa Penyakit Ayam Pedaging. *Edumatic: Jurnal Pendidikan Informatika*, *4*(2), 75–84.

Mentang, R., Sinsuw, A. A. E., Najoan, X. B. N., & Elektro-ft, J. T. (2015). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *Jurnal Teknik Elektro Dan Komputer*, *4*(7), 35–44.

Nugroho, M. A., & Suwastika, N. A. (2018). Perancangan Intrusion Prevention System pada Jaringan Software Defined Networks. *Jumanji*, *02*(01), 1–16.

Panggabean, P. (2018). Analisis Network Security Snort Metode Intrusion Detection System Untuk Optimasi Keamanan Jaringan Komputer. *Jursima*, *6*(1), 1–12. https://doi.org/10.47024/js.v6i1.107

Prakosa, B. A., Hendrawan, A. H., & Apriana, W. (2015). Perancangan Sistem Remote IP

Table dan Instrusion Detection System (IDS) dengan Snort Pada Jaringan LAN. *Krea-TIF*, *3*(2), 1–10.

Ramadhan, A. G., & Santika, R. R. (2020). AHP dan WP: Metode dalam Membangun Sistem Pendukung Keputusan (SPK) Karyawan Terbaik. *Edumatic : Jurnal Pendidikan Informatika*, *4*(1), 141–150. https://doi.org/10.29408/edumatic.v4i1.2163

Riadi, I., Fadlil, A., & Hafizh, M. N. (2020). Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology. *Edumatic : Jurnal Pendidikan Informatika*, *4*(1), 21–29. https://doi.org/10.29408/edumatic.v4i1.2046

Sabirin, F., Sulistiyarini, D., & Zulkarnain, Z. (2020). Pengembangan Sistem Informasi Seminar dan Skripsi Mahasiswa. *Edumatic: Jurnal Pendidikan Informatika*, *4*(1), 73–82.

Siregar, B., Dwiputra Purba, R. F., Seniman, & Fahmi, F. (2018). Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm. *IEEE International Conference on Communication, Networks and Satellite, Comnetsat*, 55–59. https://doi.org/10.1109/COMNETSAT.2018.8684039

Sobari, I. A. (2015). Rancangan Wireless Intrusion Detection System Menggunakan Snort. *Jurnal Techno Nusa Mandiri*, *12*(1), 1–9.

Suhartono, D., Riyanto, A. D., & Astomo, Y. W. (2015). Intrusion Detection Prevention System (IDPS) pada Local Area Network (LAN). *Telematika*, *8*(1), 24–42.

Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, *5*(1), 1–8.

Tambunan, B., Raharjo, W. S., & Purwadi, J. (2013). Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System. *Jurnal ULTIMA Computing*, *5*(1), 1–7. https://doi.org/10.31937/sk.v5i1.283

Ulfa, M., & Megawaty. (2015). Perancangan dan Implementasi Sistem Keamanan Berbasis IDS di Jaringan Internet Universitas Bina Darma. *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, *4*(2), 45–49. https://doi.org/10.23887/janapati.v4i2.9773