Analisis Keamanan Jaringan Menggunakan *Intrusion Prevention System* (IPS) Dengan Metode *Traffic Behavior*

Andhika Kurniawan[1], Lukman Medriavin Silalahi[2]

Jurusan Teknik Elektro Universitas Mercu Buana, Jakarta Selatan
Jl Raya Warung Buncit No. 98 Jakarta Selatan 12510
[1]andhikur14@gmail.com
[2]lukman.medriavin@mercubuana.ac.id

Intisari — **Riset ini mengangkat masalah tentang celah keamanan jaringan untuk disusupi oleh peretas jaringan internet, diantaranya yang saat ini diteliti adalah *Port Scanning*, DDoS (*Distribute Denial of Service*), *Bruteforce*. Tujuan penelitian ini adalah mendeteksi setiap serangan yang terjadi dan melakukan blokir akses masuk ke server. Hipotesis riset ini adalah mendeteksi dan melakukan pencegahan terhadap serangan menggunakan *default rules* yang dimiliki oleh Suricata 6.0.4. Metode yang diusulkan adalah penelitian eksperimen yang bersifat kuantitatif untuk dapat mengamankan suatu sistem jaringan menggunakan *Intrusion Prevention System* (IPS) yang dikombinasikan antara fitur *blocking* dari *Firewall* dan fitur *detection capabilities* dari *Intrusion Detection System* (IDS) berdasarkan *traffic behavior* atau anomali yang ditemukan selama dalam pengamatan dan pengujian yang telah dilakukan. Perancangan sistem keamanan ini membutuhkan sistem jaringan yang sudah yang terpasang aplikasi pfSense yang memiliki *service* Suricata sebagai IPS. Hasil riset ini menunjukan bahwa IPS dapat melakukan deteksi dan blokir terhadap serangan *Scanning Port*, *Bruteforce* dengan 3 kali pengujian dan DDoS dengan pengujian selama durasi waktu 30 detik, 1 menit dan 3 menit.**
Kata kunci — **Intrusion Prevention System, Intrusion Detection System, Port Scanning, Distributed Denial of Service, Bruteforce**

Abstract — **This research explains the problem of network security gaps to be infiltrated by internet network hackers, including those currently being studied are Port Scanning, DDoS (Distribute Denial of Service), Bruteforce. The purpose of this research is to detect every attack that occurs and block access to the server. This research hypothesis is to detect and prevent attacks using the default rules owned by Suricata 6.0.4. The proposed method is a quantitative experimental research to be able to secure a network system using intrusion prevention system (IPS) combined between the blocking feature of the Firewall and the detection capabilities feature of intrusion detection system (IDS) based on traffic behavior or anomalies found during observations and tests that have been done. The design of this security system requires a network system that is already installed pfSensei application that has suricata service as IPS. The results of this study showed that IPS can detect and block scanning port attacks, bruteforce with 3 times tests and Ddos with testing for a duration of 30 seconds, 1 minute and 3 minutes.**
Keywords— **Letakkan kata kunci Anda di sini dalam bahasa inggris, kata kunci dipisahkan dengan koma.**

I. PENDAHULUAN

Perkembangan teknologi saat ini sudah sangat membantu berbagai kegiatan masyarakat baik dalam pekerjaan, rumah tangga, dan lainnya. Namun, hal tersebut menimbulkan banyak celah keamanan jaringan internet yang ditemukan. Beberapa yang sering terjadi adalah *Port Scanning*, DDoS (*Distributed Denial of Service*), *Sniffer*, *Spoofing*, *Bruteforce* dan sebagainya. Masalah tersebut merupakan ancaman bagi sistem keamanan jaringan yang menyebabkan data didalam server dapat diubah/diganti/dirusak oleh peretas (*attacker*) [1]. Banyak metode yang telah dilakukan agar dapat mengamankan sebuah sistem jaringan. Salah satunya yang diusulkan didalam riset ini adalah penggunaan *Intrusion Prevention System* (IPS). IPS sendiri merupakan kombinasi antara fasilitas *blocking capabilities* dari *Firewall* dan kedalaman inspeksi paket data dari *Intrusion DetectionSystem* (IDS). Pada saat kondisi aktif, IPS akan membuat akses kontrol dengan cara melihat konten aplikasi sehingga IPS mampu mencegah serangan yang datang dengan bantuan administrator dan akan menghalangi suatu serangan sebelum terjadi

eksekusi dalam memori.Perancangan sistem jaringan ini menggunakan VMware Workstation, pfSense, Suricata, dan DVWA (*Damn Vulnerable Web Application*), dengan scenario pengujian adalah mensimulasikan kondisi saat server akan diserang menggunakan ancaman *Port Scanning, Bruteforce,* DDos [6-11]. Sehingga, judul riset ini adalah "Analisis Keamanan Jaringan Menggunakan *Intrusion Prevention System* (IPS) Dengan Metode *Traffic Behavior*" bertujuan untuk memantau lalu lintas jaringan (*Traffic network*), mendeteksi aktivitas mencurigakan, dan melakukan pencegahan awal terhadap intrusi atau ancaman pada sistem jaringan komputer. Manfaat yang didapat dari riset ini adalah dapat mendeteksi serangan, dapat melakukan blokir otomatis pada *Attacker* dan mampu menangkal *Attacker* saat terjadi akses masuk ke dalam server. Implementasi hanya sebatas pada pembuktian bahwa aplikasi dapat berjalan di atas sistem yang dibangun. Metode *Traffic behavior* bertujuan untuk memantau kegiatan yang dianggap normal dan untuk mendeteksi adanya penyimpangan. Pada metode ini, IPS memiliki profil yang mewakili perilaku yang normal dari user, host, koneksi jaringan dan aplikasi.

II. METODE PENELITIAN

A. Tinjauan Pustaka

Kajian riset ini menelaah pada beberapa jurnal yang digunakan sebagai acuan dalam melakukan melakukan perancangan system keamanan jaringan. Pada riset [1] membahas mengenai implementasi *Intrusion Prevention System (IPS)* untuk keamanan jaringan PT. Grahamedia Informasi. Penelitian ini menggunakan Suricata sebagai IPS untuk mengetahui adanya anomali pada jaringan. Selain itu, hasil dari penelitian ini ditemukan beberapa anomali antara lain SQL *Injection* dan *login* SSH sebagai *admin* dengan perangkat lain Riset [3] membahas tentang implementasi *Intrusion Prevention System* (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram. Pada penelitian ini menggunakan mikrotik sebagai IPS yang di konfigurasikan pada menu *firewall* dengan menggunakan Telegram sebagai notifikasi jika IPS mendeteksi serangan *bruteforce*.

Pada riset [5] membahas tentang keamanan jaringan menggunakan *Network Intrusion Detection* and *Prevention System.* Pada penelitian ini menggunakan Suricata sebagai IPS dengan mengaktifkan *rules* yang berhubungan dengan *protocol* ftp dan *telnet*, pada penelitian ini juga merancang *interface web* untuk melihat notifikasi *alert.* Penelitian ini menggunakan simulasi penyerangan dengan mendeteksi adanya proses percobaan *port scanning*

Sehingga, kebaruan pada penelitian ini adalah pengembangan system keamanan jaringan menggunakan pfSense sebagai *platform security* yang memiliki *services* Suricata sebagai IPS sehingga dapat melakukan *detection*, *blocking* dan menghasilkan tampilan pemberitahuan terhadap 3 (tiga) serangan diantaranya *Port Scanning*, DDoS, *Bruteforce*.

B. Perancangan Sistem

Gambar 1 menunjukkan diagram alir yang menjelaskan tentang awal mula dari serangan masuk hingga selesai. Paket masuk kemudian akan dilakukan pengecekan pada sistem IPS kemudian dicocokan menggunakan *rules*, apabila sebuah paket terindikasi ancaman akan keluar *alert* yang berisikan informasi dari setiap indikasi serangan tersebut, jika paket tersebut memiliki *behavior* ancaman tetapi IPS tidak mendeteksi, maka harus dilakukan penambahan *rules manual* sehingga IPS dapat mendeteksi ancaman tersebut dan melakukan *blocking.*

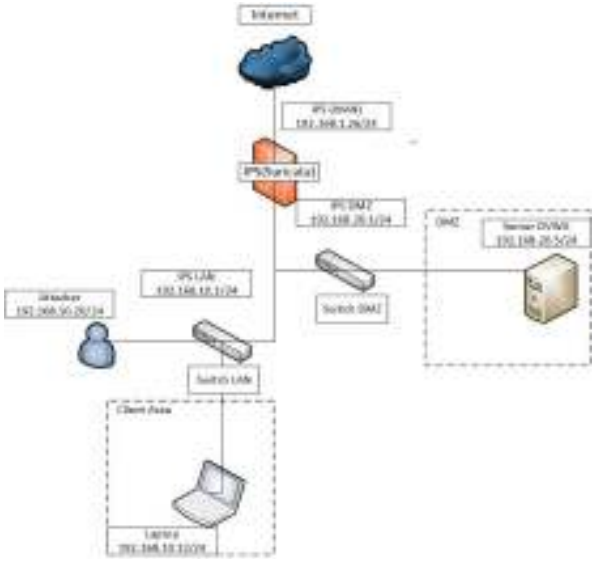
Gambar 2 menunjukkan topologi yang digunakan dalam implementasi sistem keamanan jaringan menggunakan IPS. Pada topologi tersebut dapat diketahui bahwa *Attacker* akan melakukan penyerangan ke arah server DVWA yang nantinya akan diproteksi dan dimonitor oleh Suricata sebagai IPS. Untuk scenario pengujian dapat dilihat pada Gambar 3.

Gambar 3 menjelaskan sebagai berikut:

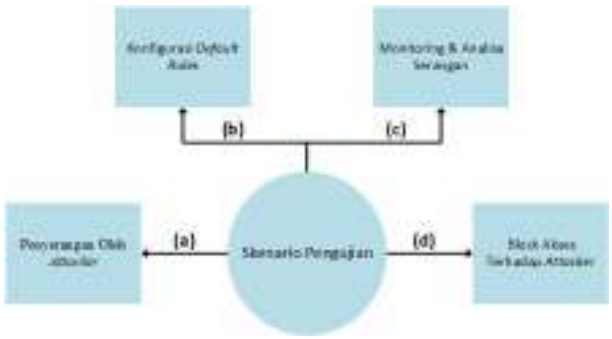
- Penyerangan oleh *Attacker*
  Dalam pengujian ini, *Attacker* akan melakukan serangan ke Server DVWA, jenis serangan yang di simulasikan adalah *Port Scanning*, DDoS dan Bruteforce.

- Konfigurasi Default Rules
  Skenario pengujian ini menggunakan *default rules* atau aturan untuk konfigurasi IPS yang digunakan untuk mendeteksi tiap jenis serangan yang dilakukan oleh *Attacker*.
- Pemantauan serangan
  Pada pengujian ini akan dilakukan pemantauan terhadap jenis serangan yang berjalan. Tujuannya adalah untuk menganalisa jenis serangan yang terjadi dan *behavior* dari serangan tersebut. Setelah mendapatkan *alert* dari fungsi *detection* IPS kemudian dilakukan analisa sehingga langkah selanjutnya dapat melakukan blokir serangan yang dilakukan oleh *Attacker*.
- Melakukan blokir akses server terhadap *Attacker*
  Pada skenario pengujian ini melakukan blokir terhadap *Attacker* agar tidak dapat melakukan penyerangan terhadap server dan menyatakan bahwa fungsi *blocking* yang dimiliki oleh IPS telah terbukti.

Gbr. 1 Diagram alir perancangan IPS



Gbr. 2 Topologi usulan sistem keamanan jaringan



Gbr. 3 Skenario pengujian

Dapat dilihat pada Gambar 2 Pada pengujian Bruteforce, dilakukan penambahan *rule* secara *custom* ke *rules* IPS serangan tersebut dan dapat mengirimkan *alert*, karena secara *default rule*, IPS tidak mengenali ada nya serangan Bruteforce, sehingga harus dilakukan *custum rule*, dan setelah menambahkan *rule* tersebut, IPS berhasil mendeteksi serangan dari 3 kali pengujian yang telah dilakukan dan menghasilkan sebanyak 9 *alert* untuk setiap pengujian yang dilakukan. Dapat dilihat pada Gambar 3.

III. HASIL DAN PEMBAHASAN

Berdasarkan skenario yang telah dilakukan maka diperoleh hasil Analisa sebagai berikut:

A. Pengujian Skenario 1

Pengujian skenario 1 (pertama) adalah melakukan pengecekan fungsi dari *detection* yang dimiliki oleh IPS. Pengujian ini

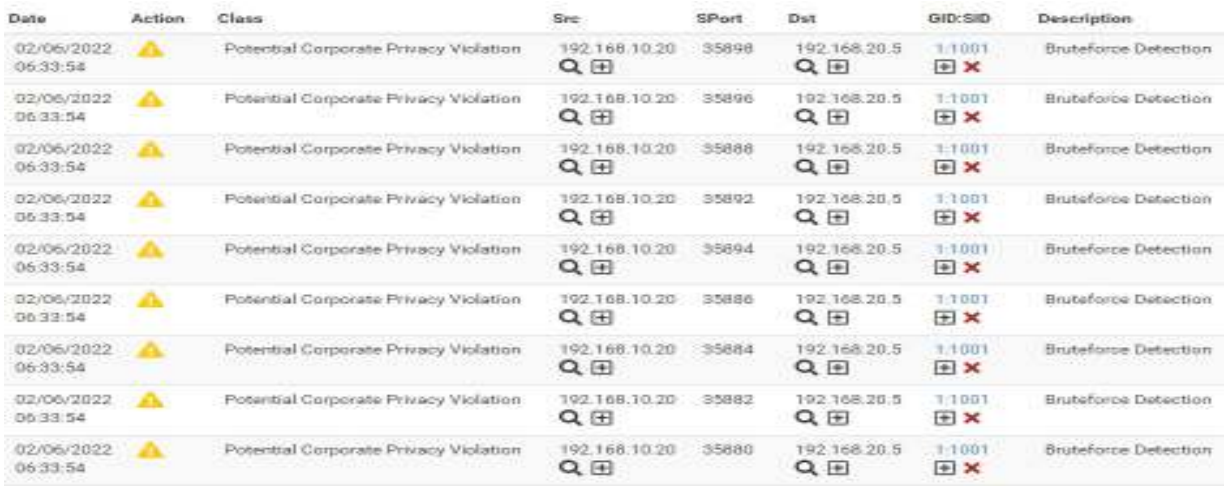
dilakukan menggunakan 3 jenis penyerangan, Pada pengujian *Port Scanning*, *Attacker* berhasil mendapatkan informasi mengenai port yang terbuka didalam server DVWA tersebut seperti port 21=ftp, 22=ssh & 80=http dan IPS berhasil mendeteksi serangan dari 3 kali pengujian yang telah dilakukan sehingga menghasilkan sebanyak 4 *alert* untuk setiap pengujian, dapat dilihat pada Gambar 4. sehingga dapat membantu untuk mengenali Pada pengujian Ddos, *Attacker* berhasil membuat kinerja dari sistem server tersebut menjadi lambat dan IPS berhasil berhasil mendeteksi dan menghasilkan *alert* sebanyak 29 *alert* dengan penyerangan selama 30 detik, 38 *alert* dengan penyerangan selama 1 menit dan 243 *alert* untuk penyerangan selama 3 menit.

Date	Action	Class	Src	SPort	Dst	GID:SID	Description
02/06/2022 05:36:01	⚠	Misc Attack	42.172.14.182	43716	192.168.20.5	1:2400001	ET DROP Spamhaus DROP Listed Traffic Inbound group 2
02/06/2022 05:35:59	⚠	Misc Attack	150.25.243.128	15802	192.168.20.5	1:2400014	ET DROP Spamhaus DROP Listed Traffic Inbound group 15
02/06/2022 05:35:59	⚠	Misc Attack	196.15.104.135	15750	192.168.20.5	1:2400027	ET DROP Spamhaus DROP Listed Traffic Inbound group 28
02/06/2022 05:35:59	⚠	Misc Attack	134.33.43.229	15574	192.168.20.5	1:2400011	ET DROP Spamhaus DROP Listed Traffic Inbound group 12
02/06/2022 05:35:59	⚠	Misc Attack	180.237.75.189	15524	192.168.20.5	1:2400021	ET DROP Spamhaus DROP Listed Traffic Inbound group 22
02/06/2022 05:35:59	⚠	Misc Attack	42.163.172.87	15148	192.168.20.5	1:2400001	ET DROP Spamhaus DROP Listed Traffic Inbound group 2
02/06/2022 05:35:59	⚠	Misc Attack	106.95.163.155	15059	192.168.20.5	1:2400010	ET DROP Spamhaus DROP Listed Traffic Inbound group 11

Gbr. 4 Peringatan serangan *port scanning*

Date	Action	Class	Src	SPort	Dst	GID:SID	Description
02/06/2022 05:18:10	⚠	Web Application Attack	192.168.10.20	35700	192.168.20.5	1:2024364	ET SCAN Possible Nmap User-Agent Observed
02/06/2022 05:18:10	⚠	Web Application Attack	192.168.10.20	35698	192.168.20.5	1:2024364	ET SCAN Possible Nmap User-Agent Observed
02/06/2022 05:18:10	⚠	Web Application Attack	192.168.10.20	35686	192.168.20.5	1:2024364	ET SCAN Possible Nmap User-Agent Observed
02/06/2022 05:18:10	⚠	Web Application Attack	192.168.10.20	35690	192.168.20.5	1:2024364	ET SCAN Possible Nmap User-Agent Observed

Gbr. 5 Peringatan serangan DdoS



Date	Action	Class	Src	SPort	Dst	GID:SID	Description
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35898	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35896	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35888	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35892	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35894	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35886	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35884	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35882	192.168.20.5	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	Potential Corporate Privacy Violation	192.168.10.20	35880	192.168.20.5	1:1001	Bruteforce Detection

Gbr. 6 Peringatan serangan *bruteforce*

Untuk keseluruhan pengujian skenario 1 maka didapatkan hasil yang ditunjukan pada Tabel 1.

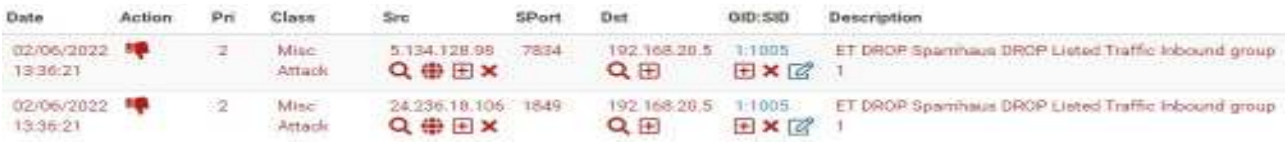
Tabel 1. Hasil Pengujian Skenario 1

No	Jenis Serangan	Status Serangan	Status IPS
1	Port Scanning (Nmap)	Serangan berhasil dilakukan	IPS mengirimkan *alert*
2	Ddos (hping3)	Serangan berhasil dilakukan	IPS mengirimkan *alert*
3	Bruteforce (Hydra)	Serangan berhasil dilakukan	IPS mengirimkan *alert* setelah *add rule*

B. Pengujian Skenario 2

Pengujian skenario 2 (kedua) adalah melakukan pengecekan fungsi dari pemblokiran yang dimiliki oleh IPS. Pengujian ini dilakukan menggunakan 3 (tiga) jenis serangan. Pada pengujian *Port Scanning*, *Attacker* tidak berhasil mendapatkan informasi mengenai *port* yang terbuka didalam server DVWA tersebut dan pada pengujian ini IPS berhasil melakukan *blocking* terhadap *Attacker* dari 3 kali pengujian yang telah dilakukan sehingga menghasilkan sebanyak 4 *blocking alert* untuk setiap pengujian. Hasil pengujian dapat dilihat pada Gambar 7. Pengujian DDoS, *Attacker* tidak berhasil melakukan penyerangan dan IPS berhasil melakukan *blocking* dan menghasilkan alert sebanyak 27 *blocking alert* dengan penyerangan selama 30 detik, 41 *blocking alert* dengan penyerangan selama 1 menit dan 241 *blocking alert* untuk penyerangan selama 3 menit. Hasil pengujian dapat dilihat pada Gambar 8. Pengujian Bruteforce, *Attacker* tidak berhasil mendapatkan *username & password* login ke *web server*, dan pada pengujian ini IPS berhasil melakukan *blocking* terhadap *Attacker* dari 3 kali pengujian yang telah dilakukan dan menghasilkan sebanyak 9 *blocking alert* untuk setiap pengujian yang dilakukan. Hasil pengujian dapat dilihat pada Gambar 9.

Gbr. 7 Blokir serangan *port scanning*



Gbr. 8 Blokir serangan DDoS

Gbr. 9 Blokir serangan *bruteforce*

Untuk keseluruhan pengujian skenario 2 maka didapatkan hasil yang ditunjukan pada Tabel 2.

Tabel 2. Hasil Pengujian Skenario 2

No	Jenis Serangan	Status Serangan	Status IPS
1	Port Scanning (Nmap)	Serangan tidak berhasil	IPS blokir IP
2	Ddos (hping3)	Serangan tidak berhasil	IPS blokir IP
3	Bruteforce (Hydra)	Serangan tidak berhasil	IPS blokir IP

IV. KESIMPULAN

Berdasarkan pengujian dan analisa hasil pengujian yang telah dilakukan, sehingga kesimpulan riset ini adalah :

1. IPS berhasil mendeteksi dan melakukan blokir terhadap *Port Scanning* menggunakan Nmap dengan 3 kali pengujian yang telah dilakukan dan menghasilkan sebanyak 4 *blocking alert* untuk setiap pengujian.
2. IPS berhasil mendeteksi dan melakukan *blocking* terhadap serangan DDoS yang menghasilkan sebanyak 27 *blocking alert* dengan penyerangan selama 30 detik, 41 *blocking alert* dengan penyerangan selama 1 menit dan 241 *blocking alert* dengan penyerangan selama 3 menit.
3. IPS berhasil mendeteksi dan melakukan *blocking* terhadap serangan Bruteforce dengan 3 kali pengujian yang telah dilakukan dan menghasilkan sebanyak 9 *blocking alert* untuk setiap pengujian.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada Universitas Mercu Buana yang telah mendukung riset ini hingga selesai. Serta, semoga riset ini bermanfaat bagi kalangan akademisi dan praktisi.

REFERENSI

[1] Anggoro, B. S., & Sulistyo, W. (2019, November). Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi. In *SEMINAR NASIONAL APTIKOM (SEMNASTIK) 2019* (pp. 280-288).

[2] Pradipta, Y. W. (2017). Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IP Tables Berbasis Linux. *Jurnal Manajemen Informatika*, *7*(1).

[3] Rahmatillah, A., Firdaus, A., & Laila, E. (2021). Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer. *Jurnal Laporan Akhir Teknik Komputer*, *1*(1), 10-17.

[4] Gozali, F., & Setiaji, A. L. (2017). Perancangan Dan Analisis Sistem Pendeteksi Intrusi Berbasis Network Intrusion Detection System (Nids) Pada Sistem Keamanan Jaringan Komputer. *Jetri: Jurnal Ilmiah Teknik Elektro*, *11*(1), 1-16.

[5] Alamsyah, H., & 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.

[6] Hartono, H. (2019). *Perancangan Keamanan Jaringan Menggunakan firewall Pfsence* (Doctoral dissertation, Universitas Internasional Batam).

[7] Monoarfa, M. N., Najoan, X. B., & Sinsuw, A. A. (2016). Analisa dan Implementasi Network Intrusion Prevention System di Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro dan Komputer*, *5*(4), 34-45.

[8] Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., & Ma, M. (2019). Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. *IEEE Access*, *7*, 158481-158491.

[9] Sylvester, A., Asante, M., & Twum, F. An Improved Computer Network Access Control using Free BSD PFSENSE: A Case Study of UMaT Local Area Network.

[10] Alturfi, S. M., Muhsen, D. K., Mohammed, M. A., Aziz, I. T., & Aljshamee, M. (2021, February). A Combination Techniques of Intrusion Prevention and Detection for Cloud Computing. In *Journal of Physics: Conference Series* (Vol. 1804, No. 1, p. 012121). IOP Publishing.

[11] Swetha, K. V., & Dara, R. (2018). Deployment of intrusion prevention system on multi-core processor based security hardware. *Int J Comput Netw Commun*, *10*(3), 13-25.