Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 8, No. 2, Juni 2023 (330-340) **10.32493/informatika.v8i2.33685**

Implementasi Anti-DDOS Menggunakan *Intrusion Prevention System* (IPS) terhadap Serangan DDOS

Kevin Jorenta Surbakti[1], Rohmat Tulloh[2], and Muhammad Nazel Djibran[3]

[1,2]Teknologi Telekomunikasi, Telkom University, Jalan Telekomunikasi, Bojongsoang, Bandung, Jawa Barat, 40257
e-mail: [1]kevinjorentas@student.telkomuniversity.ac.id, [2]rohmatth@telkomuniversity.ac.id

[3]IT Security Implementation, PT Datacomm Diangraha, Jalan Kapten Tendean, Mampang Prapatan, Jakarta Selatan, DKI Jakarta 12790
e-mail: [3]nazel.djibran@datacomm.co.id

Submitted Date: June 16th, 2023 Reviewed Date: June 22nd, 2023
Revised Date: June 27th, 2023 Accepted Date: June 30th, 2023

Abstract

Distributed Denial of Service (DDoS) is a type of attack that can exhaust server resources. This attack results in a decrease in server quality so that it cannot be accessed by authorized users. Servers that are commonly victimized by this attack belong to companies from various sectors. PT Datacomm Diangraha provides solutions to these problems. As PT Datacomm Diangraha will do to Company X, which is to implement an Intrusion Prevention System (IPS) device as Anti-DDoS on its customers according to the customer's needs. This paper will test IPS devices in preventing DDoS attacks such as TCP Flood, UDP Flood, and ICMP Flood. The test is conducted by connecting the attacker and victim to the IPS device in the local network. The analysis will be done by comparing the network traffic and throughput of the victim when the attack is carried out when protected by IPS, no protection, and when traffic is normal. Experiments were conducted by performing a one-minute attack. The results of the experiments show that the traffic when protected by an IPS is similar to that during normal traffic. In addition, tests were conducted to prevent XSS malware to prove that IPS can prevent other attacks besides DDoS. From the test results, it was found that IPS can prevent DDoS attacks with 100% accuracy. The throughput data obtained when a DDoS attack occurs without IPS protection is 260978.9 - 1080732.32 bps. Throughput data when a DDoS attack occurs with IPS protection of 42.55 - 49.95 bps, which shows similarity in value with throughput during normal traffic which is 43.43 bps.

Keywords: DDoS; IPS; Anti-DDoS; malware; XSS

Abstrak

Distributed Denial of Service (DDoS) merupakan jenis serangan yang dapat menghabiskan sumber daya *server*. Serangan ini mengakibatkan penurunan kualitas *server* sehingga tidak bisa diakses oleh pengguna yang sah. *Server* yang biasa menjadi korban serangan ini adalah milik perusahaan dari berbagai sektor. PT Datacomm Diangraha menyediakan solusi dari permasalahan tersebut. Seperti yang akan dilakukan PT Datacomm Diangraha kepada Perusahaan X, yaitu mengimplementasikan perangkat *Intrusion Prevention System* (IPS) sebagai Anti-DDoS pada pelanggannya sesuai dengan kebutuhan pelanggan tersebut. Makalah ini akan melakukan pengujian perangkat IPS dalam mencegah serangan DDoS seperti *TCP Flood, UDP Flood, dan ICMP Flood*. Pengujian dilakukan dengan menghubungkan penyerang dan korban ke perangkat IPS dalam jaringan lokal. Analisis akan dilakukan dengan membandingkan lalu lintas jaringan serta *throughput* korban ketika dilakukan penyerangan saat dilindungi IPS, tidak ada perlindungan, serta saat lalu lintas normal. Eksperimen dilakukan dengan melakukan penyerangan selama satu menit. Hasil dari eksperimen menunjukkan bahwa lalu lintas ketika dilindungi IPS menunjukkan

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

kesamaan dengan saat lalu lintas normal. Sebagai tambahan, dilakukan pengujian untuk mencegah *malware* XSS untuk membuktikan IPS dapat mencegah serangan lain selain DDoS. Dari hasil pengujian didapatkan bahwa IPS dapat mencegah serangan DDoS dengan akurasi 100%. Didapatkan data *throughput* ketika terjadi serangan DDoS tanpa perlindungan IPS sebesar 260978.9 - 1080732.32 bps. Data *throughput* ketika terjadi serangan DDoS dengan perlindungan IPS sebesar 42.55 – 49.95 bps, yang menunjukkan kemiripan nilai dengan *throughput* saat lalu lintas normal yaitu sebesar 43.43 bps.

Kata Kunci: DDoS; IPS; Anti-DDoS; *malware*; XSS

1. Pendahuluan

Teknologi informasi pada saat ini sudah berkembang pesat terutama dalam layanan internet. Internet tidak hanya digunakan dalam lingkup individu untuk bertukar informasi, tetapi sudah digunakan untuk keperluan komersial perusahaan dalam menyediakan layanan untuk pelanggannya (Saini, Behal, & Bhatia, 2020). Dengan meningkatnya permintaan layanan melalui jaringan internet, hal ini yang dimanfaatkan oleh *cyberattacker* untuk menyusup ke dalam jaringan tersebut dan mengirimkan serangan untuk menghabiskan sumber daya *server* yang dituju. Hal ini menyebabkan penurunan kualitas layanan internet perusahaan yang dialami oleh pelanggannya. Serangan ini disebut dengan serangan *Distributed Denial of Service* (DDoS).

Serangan DDoS merupakan sebuah teknologi yang dapat menggabungkan beberapa komputer yang sudah terinfeksi virus sehingga dapat dikendalikan jarak jauh, untuk menyerang sebuah *server* secara bersamaan untuk menaikkan jumlah lalu lintas jaringan *server* tersebut(Pei et al., 2019). DDoS terdiri dari beberapa jenis serangan yang berbeda menurut protokolnya, seperti *TCP Flood, UDP Flood, dan ICMP Flood*.

Intrusion Prevention System (IPS) adalah sebuah sistem yang dapat mengenali aktifitas mencurigakan dalam sebuah jaringan (Wahyudi & Utomo, 2021). IPS dapat menganalisis tiap permintaan yang masuk dan mengenali permintaan yang anomali atau sah. IPS memiliki *database signature* yang membantu proses identifikasi jaringan. Jika terdapat lalu lintas jaringan yang ditandai sebagai anomali, maka IPS akan memberikan peringatan serta langsung memitigasinya. Hasil mitigasi ini kemudian akan ditampilkan dalam *log*.

PT Datacomm Diangraha merupakan salah satu penyedia layanan teknologi informasi terkemuka di Indonesia (About - Datacomm Diangraha, 2023). Salah satu layanan yang disediakan oleh PT Datacomm Diangraha adalah pada bidang *IT Security* yang menyediakan jasa pengamanan jaringan pada perusahaan. Implementasi IPS sebagai Anti-DDoS ini dilakukan PT Datacomm Diangraha untuk memenuhi kebutuhan Perusahaan X dalam menangani serangan DDoS. PT Datacomm Diangraha memberikan solusi untuk memasang perangkat keamanan sesuai dengan spesifikasi perangkat permintaan pelanggannya.

Beberapa penelitian yang sudah dilakukan sebelumnya seperti yang dilakukan oleh Firmansyah, Negara, dan Sanjoyo (Firmansyah, Negara, & Sanjoyo, 2019), IPS diimplementasikan dalam jaringan *Software Defined Network* (SDN) untuk menjadi pengaman jaringan tersebut. SDN memiliki kelebihan dalam meningkatkan efisiensi dalam mengelola sebuah jaringan komputer, yang dapat memisahkan antara *control plane* dan *data plane*. IPS diterapkan berbasis *software* yaitu dengan mengintegrasikan fungsi *Intrusion Detection System* (IDS) pada *Snort*. Setelah sistem ini diterapkan, akan dilakukan penyerangan seperti *ICMP Flood* dan *Ping of Death*. Makalah ini akan menerapkan IPS berbasis perangkat pada jaringan perusahaan untuk melakukan pencegahan *TCP Flood, UDP Flood, ICMP Flood*, serta *malware* XSS.

Penelitian lain yang dilakukan oleh Aditya (Aditya, 2020), menampilkan cara mencegah serangan DoS dan DDoS menggunakan *Host Intrusion Prevention System* (HIPS) *Snort*. HIPS Snort akan diterapkan pada *router* untuk menjadi sistem pengaman yang mengamankan data atau *file* yang tersimpan dalam *router*. HIPS Snort akan mendeteksi aktifitas yang tidak normal akibat serangan DoS dan DDoS kemudian memitigasinya. Makalah ini mengimplementasikan perangkat IPS untuk mencegah serangan DDoS. Hasilnya serangan DDoS dapat dicegah dengan menganalisis nilai lalu lintas jaringan serta *throughput server*.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

Selanjutnya penelitian dari Wahyudin (Wahyudin, 2023), IPS Suricata diintegrasikan dengan *Blockchain* untuk mendistribusikan IP yang dianggap anomali kepada semua IPS yang terdapat dalam jaringan. IP anomali tersebut merupakan IP dari penyerang yang akan dicegah selanjutnya. Terdapat tiga buah IPS Suricata yang digunakan untuk mengamankan jaringan. IPS tersebut akan memblokir serangan *SYN Flood* yang dilakukan dalam beberapa metode. Hasil yang didapatkan merupakan perbandingan jumlah paket yang diterima dan dikirimkan berbeda pada tiap metode. Makalah ini mengimplementasikan sebuah perangkat IPS pada jaringan perusahaan. Pada pengujian akan membandingkan lalu lintas jaringan normal dengan kata lain ketika tidak terdapat serangan dan ketika terjadi serangan saat dilindungi IPS. Hasil yang didapatkan adalah lalu lintas jaringan saat terjadi serangan ketika dilindungi IPS menunjukkan kesamaan dengan lalu lintas jaringan normal dilihat dari jumlah paket yang diterima dan paket yang dikirim.

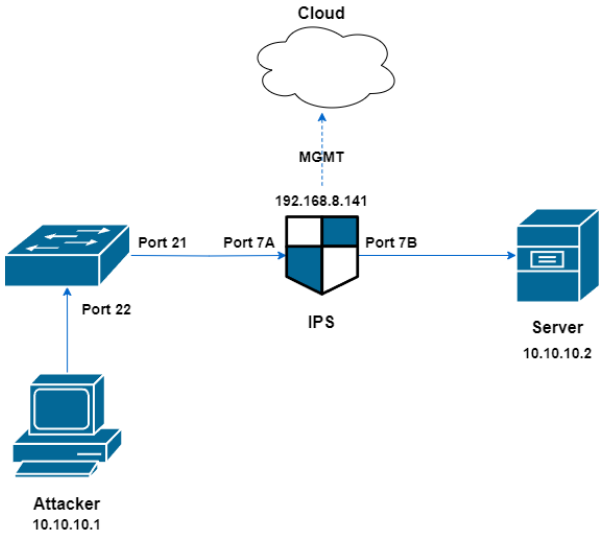
Berikutnya penelitian dari Nugraha (Nugraha, 2023), pencegahan DDoS menggunakan *Self Organizing Map* (SOM) diterapkan pada SDN. SOM berguna untuk mengklasifikasikan lalu lintas jaringan normal dan lalu lintas jaringan saat terjadi serangan DDoS berdasarkan dari dataset. Hasilnya SOM dapat memitigasi serangan DDoS dengan akurasi terbaik mencapai 76,3%. Makalah ini menggunakan perangkat IPS untuk memitigasi DDoS sehingga didapatkan tingkat keberhasilan mitigasi mencapai 100% berdasarkan perbandingan dari lalu lintas jaringan normal dan lalu lintas jaringan saat terjadi serangan DDoS dengan perlindungan IPS. Perangkat yang digunakan pada makalah ini memiliki spesifikasi yang lebih mumpuni daripada (McAfee & LLC, 2019). *Trellix NS9500* memiliki kemampuan *IPS throughput* mencapai 30 Gbps. Makalah ini menggunakan perangkat sesuai dengan yang dibutuhkan perusahaan. *IPS throughput* yang dibutuhkan perusahaan sebesar 40 Gbps, sehingga perangkat yang digunakan pada makalah ini adalah perangkat yang memiliki *IPS throughput* sebesar kebutuhan tersebut.

Berdasarkan permasalahan serta penelitian yang telah dilakukan sebelumnya, maka penelitian ini mengajukan solusi mengatasi serangan DDoS menggunakan perangkat IPS. Perangkat IPS yang digunakan ditentukan sesuai dengan spesifikasi yang dibutuhkan oleh Perusahaan X. Hasil dari penelitian ini, perangkat IPS dapat menangani serangan DDoS dengan akurasi 100% dan sebagai tambahan dapat menangani serangan *malware* XSS.

2. Metode Penelitian

2.1 Topologi Jaringan

Gambar 1 merupakan topologi jaringan yang diujikan pada makalah ini. Dalam topologi terdapat dua buah laptop, sebuah *switch*, dan perangkat IPS. Laptop 1 digunakan sebagai *Attacker* dengan OS Windows 10 dan terinstal *Virtual Machine* (VM). Di dalam VM terdapat *Raptor* yang berguna untuk menjalankan serangan DDoS. Laptop 2 digunakan sebagai *server* dengan OS Ubuntu-Server 22. Dalam *server* sudah terinstal *Damn Vulnerable Web Application* (DVWA) yang berguna sebagai korban pengujian penyerangan.



Gambar 1. Topologi Pengujian IPS

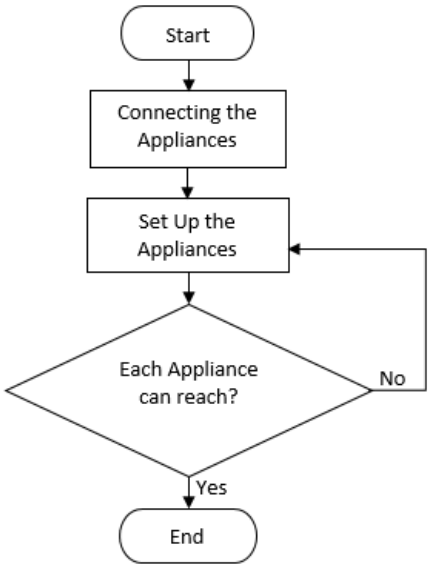
Penelitian dilakukan di Laboratorium PT Datacomm Diangraha. *Attacker* yang akan menyerang *server* terhubung ke *switch*, yang berguna sebagai penghubung ke perangkat IPS. *Server* kemudian terhubung ke perangkat IPS, yang berfungsi untuk mencegah setiap serangan yang masuk melalui *switch*. Setiap permintaan yang telah lolos dari IPS kemudian akan diteruskan ke *server*. Semua perangkat yang terhubung menggunakan IP dalam jaringan lokal. *Port Management* IPS terhubung ke jaringan internet agar perangkat memiliki *IP Public* sehingga

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

perangkat dapat diakses secara *remote*. *Server* nantinya akan diukur besar lalu lintas jaringannya sebagai bahan analisis makalah ini.

Setelah membuat topologi jaringan, selanjutnya melakukan perancangan sistem. Gambar 2 merupakan *flowchart* perancangan sistem. Perancangan sistem dilakukan dengan menghubungkan tiap perangkat sesuai dengan topologi yang sudah dibuat. Perangkat *attacker* diinstal OS Widows 10 serta diberikan IP 10.10.10.1. Pada *attacker* diinstal VM yang bernama Raptor, yang berguna untuk meluncurkan serangan DDoS. Perangkat *server* diinstal OS Ubuntu-Server 22 serta diberikan IP 10.10.10.2. Pada *server* diinstal DVWA yang berfungsi untuk menguji serangan-serangan yang ditujukan ke *server*. Pada *Switch*, *attacker* akan diatur dalam *vlan* yang sama agar dapat terhubung dengan perangkat IPS. Selanjutnya *switch* dicolokkan pada *port* 7A dan *server* dicolokkan pada *port* 7B pada perangkat IPS. *Port-port* tersebut sudah termasuk dalam satu *interface* sehingga antar *port* dapat saling berkomunikasi. Setelah semua tahap dilakukan, antar perangkat akan coba melakukan *ping*. *Attacker* akan *ping* ke *server* dan juga sebaliknya. Jika antar perangkat berhasil *reach*, dapat lanjut ke tahap pengujian penyerangan.

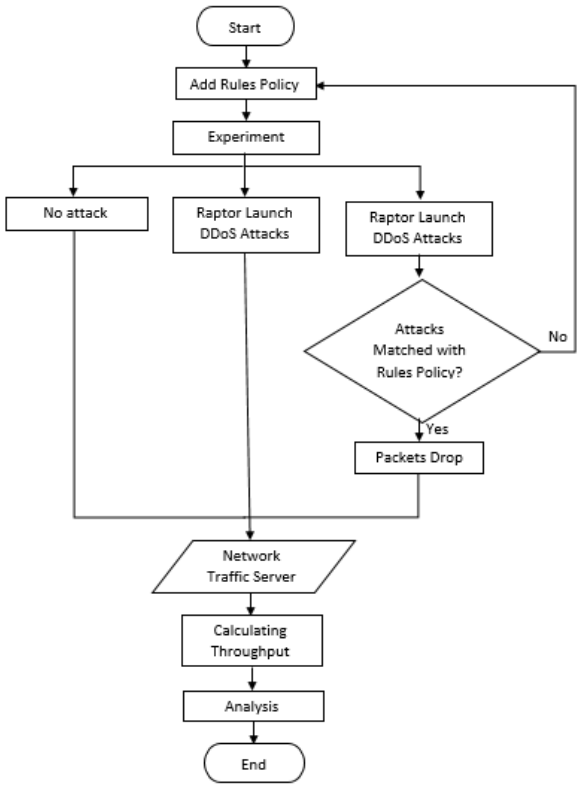
2.2 *Flowchart* Perancangan Sistem



Gambar 2. *Flowchart* Perancangan Sistem

2.3 *Flowchart* Pengujian IPS

Gambar 3 merupakan *flowchart* pengujian yang dilakukan dalam makalah ini. Pengujian dilakukan dalam beberapa metode yaitu, tidak meluncurkan serangan, meluncurkan serangan DDoS tanpa dilindungi IPS, dan meluncurkan serangan DDoS dengan dilindungi IPS. Metode tidak meluncurkan serangan bertujuan untuk melihat lalu lintas normal jaringan dari *server* yang menandakan aktifitas normal *server*. Metode meluncurkan serangan DDoS tanpa dilindungi IPS bertujuan untuk melihat peningkatan lalu lintas jaringan *server* yang disebabkan oleh serangan DDoS, yang menandakan aktifitas tidak normal dari *server*. Metode yang terakhir berguna untuk menguji kemampuan perangkat IPS dalam melindungi *server* dari serangan DDoS yang menunjukkan lalu lintas jaringan dalam keadaan normal walaupun terserang serangan DDoS.



Gambar 3. *Flowchart* Pengujian IPS

Setelah tiap perangkat dipastikan dapat berkomunikasi satu dengan yang lain, perangkat IPS diberikan *rules policy*. *Rules policy* berguna sebagai pengaturan yang akan melakukan aksi terhadap serangan yang masuk. Pengujian dilakukan menggunakan *Raptor* yang akan

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

mengirimkan serangan DDoS ke *server*. Metode tanpa serangan dan meluncurkan serangan tanpa perlindungan DDoS akan langsung memperhatikan lalu lintas jaringan *server*. Metode meluncurkan serangan dengan perlindungan DDoS akan melewati proses pengecekan pada perangkat IPS. Jika serangan *match* dengan *rules policy* IPS, maka serangan langsung dimitigasi. Jika masih ada serangan yang lolos, maka diatur kembali *rules policy* IPS. Setelah itu akan memperhatikan lalu lintas jaringan *server*, dengan mencatat besar paket yang diterima dan paket yang dikirimkan. Lalu lintas jaringan tersebut yang akan menjadi bahan perhitungan *throughput*. Hasil dari pengukuran *throughput* tiap metode akan menetukan keefektifan IPS dalam menangani serangan DDoS. Tiap metode tersebut akan dilakukan selama 1 menit.

2.4 Perhitungan *Throughput*

Throughput adalah ukuran sebenarnya banyak jumlah data yang dikirimkan dalam satuan waktu tertentu. *Throughput* biasa memiliki satuan *bits per second* (bps) (Vanny Andini et al., 2020). Ukuran ini biasa digunakan sebagai parameter kualitas sebuah jaringan. Kualitas sebuah jaringan dilihat dari berbagai faktor seperti kemampuan jaringan melakukan sebuah beban kerja, waktu respon jaringan, dan yang lainnya. Peningkatan nilai *throughput* atau penurunan nilai dari nilai yang normal dapat menjadi bahan analisis terhadap masalah yang terjadi. Persamaan dari *throughput* adalah sebagai berikut:

$$Throughput\ (bps) = \frac{Packet\ received\ (bits)}{Total\ time\ attack\ (seconds)}$$

Persamaan tersebut merupakan perhitungan *throughput* yang merupakan perbandingan dari jumlah paket yang diterima dalam satuan bit dengan jumlah waktu serangan yang terjadi. Perhitungan *throughput* ditujukan untuk mengetahui kualitas jaringan *server*. Dari hasil pengukuran dapat dilihat jika *server* tiba-tiba mendapatkan serangan ditandai dengan peningkatan nilai *throughput* yang tiba-tiba meningkat dari keadaan normal yang dapat mengakibatkan penurunan kinerja *server* akibat banyaknya data yang masuk.

2.5 Spesifikasi Perangkat

Perangkat yang digunakan dalam makalah ini ditentukan berdasarkan kebutuhan Perusahaan X. Adapun kebutuhan spesifikasi yang ditetapkan oleh perusahaan adalah seperti pada Tabel 1.

Tabel 1. Kebutuhan Spesifikasi Perusahaan X

Kebutuhan Spesifikasi dari Perusahaan X
IPS throughput upgradable up to 40 Gbps
Latency less than 40 microseconds
Concurrent sessions at least 56 Million
Connections per Second at least 650,000 new sessions per second
Network connectivity 2 x 2-segment SFP+ 10G Fiber SR Bypass perDevice/IPS Sensor

Perusahaan X menetapkan spesifikasi-spesifikasi tersebut untuk menambah sistem keamanannya. Berdasarkan beberapa kebutuhan spesifikasi tersebut, didapatkan perangkat yang sesuai dengan spesifikasi tersebut yaitu "Trend Micro TippingPoint Threat Protection System 8400TX". Diambil dari (• DATASHEET • TIPPINGPOINT THREAT PROTECTION SYSTEM FAMILY KEY FEATURES, 2023), spesifikasi perangkat tersebut ditunjukkan pada Tabel 2.

Tabel 2. Spesifikasi Trend Micro TPS 8400TX

Features	**8400TX**
Supported IPS Inspection Throughput	3/5/10/15/20/30/40 Gbps
Latency	<40 microseconds
Concurrent Sessions	120,000,000
New Connections per second	650,000
Network Connectivity	Fiber Bypass 2-Segment 10GE SR/LR

3. Hasil dan Pembahasan

Eksperimen pada makalah ini dilakukan dalam tiga metode pengujian. Metode pertama tidak meluncurkan seragan apapun, metode kedua meluncurkan serangan DDoS tanpa dilindungi IPS, dan metode ketiga meluncurkan serangan DDoS dengan dilindungi IPS. Jenis serangan DDoS yang diluncurkan adalah *TCP Flood, UDP Flood, dan ICMP Flood*. Sebagai tambahan, dilakukan penyerangan *malware* XSS untuk menguji

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

kemampuan perangkat dalam menangani serangan lain selain DDoS. Pengujian beberapa metode tersebut nantinya akan memperhatikan lalu lintas jaringan *server*. Jumlah paket yang diterima dan paket yang dikirim akan dicatat sebagai bahan analisis pengukuran *throughput*. Pencatatan jumlah paket tersebut diukur tiap interval 10 detik. Tiap metode akan diujikan selama 1 menit.

3.1 Tidak diluncurkan serangan

Pada pengujian pertama, dilakukan tanpa meluncurkan serangan. Hal ini bertujuan untuk melihat aktifitas normal dari lalu lintas jaringan *server* ketika tidak ada permintaan apapun yang masuk ke *server*.

Tabel 3. Lalu Lintas Jaringan Normal

Time (s)	Paket Diterima (bits)	Paket Dikirimkan (bits)
10	312	0
20	3600	0
30	0	0
40	4064	0
50	3600	0
60	4064	0
Rata-rata	**2606**	**0**

Tabel 3 merupakan rata-rata besar paket yang diterima serta dikirimkan dalam waktu 1 menit. Pada tabel tersebut dapat dilihat besar paket yang diterima dalam kurun waktu 1 menit berada pada rentang 0 bits – 4064 bits. Didapatkan rata-rata dari data tersebut, paket yang diterima selama 1 menit sebesar 2606 bits. Pada besar paket yang dikirimkan juga dapat dilihat jumlah nilai yang dikirimkan konstan, yaitu 0 bits, yang berarti tidak ada paket yang dikirimkan. Hasil tersebut menandakan jumlah paket yang dikirimkan serta paket yang diterima dalam keadaan lalu lintas jaringan normal.

3.2 Diluncurkan Serangan DDoS Tanpa Perlindugan IPS

Pada metode kedua, dilakukan peluncuran serangan DDoS tanpa dilindungi IPS. Hal ini bertujuan untuk melihat peningkatan lalu lintas jaringan *server* ketika adanya serangan DDoS.

Tabel 4. Lalu Lintas Jaringan Saat Serangan DDoS Tanpa Perlindungan

Waktu (s)	Serangan DDoS	Paket Diterima (bits)	Paket Terkirim (bits)
10	TCP Flood	50331648	614400
	UDP Flood	51170508	51170508
	ICMP Flood	18454937	16777216
20	TCP Flood	66941091	615526
	UDP Flood	52009369	52009369
	ICMP Flood	19293798	18454937
30	TCP Flood	66270003	617779
	UDP Flood	76336332	76336332
	ICMP Flood	8388608	1003520
40	TCP Flood	63753420	599654
	UDP Flood	67947724	67947724
	ICMP Flood	20132659	18454937
50	TCP Flood	64592281	633241
	UDP Flood	51170508	51170508
	ICMP Flood	11744051	10066329
60	TCP Flood	77175193	630169
	UDP Flood	85563801	85563801
	ICMP Flood	15938355	14260633
Rata-rata	**TCP Flood**	**64843939**	**618461**
	UDP Flood	**64033040**	**64033040**
	ICMP Flood	**15658734**	**13169550**

Tabel 4 merupakan hasil pengukuran dari penyerangan DDoS tanpa dilindungi IPS. Nilai-nilai tersebut menunjukkan peningkatan yang sangat jauh dibandingkan dengan lalu lintas normal. Tiap jenis serangan menunjukkan nilai yang berbeda-beda tiap waktunya. Pada jenis serangan *TCP Flood*, jumlah paket yang diterima

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

berada pada rentang 50331648 bits – 77175193 bits, lalu jumlah paket yang terkirim berada pada rentang 599654 bits – 633241 bits. Nilai rata-rata dari jenis serangan *TCP Flood* adalah paket yang diterima sebanyak 64843939 bits selama 1 menit, dan paket yang dikirim sebanyak 618461 bits selama 1 menit. Lalu jenis serangan *UDP Flood* menunjukkan nilai yang berbeda dengan serangan sebelumnya. Terlihat dari tabel, jumlah paket yang diterima dan dikirimkan menunjukkan jumlah yang sama. Jumlah paket yang diterima dan terkirim sama-sama berada pada rentang 51170508 bits – 85563801 bits. Nilai rata-rata dari jenis serangan *UDP Flood* adalah menerima dan mengirim sebanyak 64033040 bits selama 1 menit. Terakhir, pada jenis serangan *ICMP Flood* terlihat jumlah paketnya lebih sedikit daripada dua serangan sebelumnya. Paket yang diterima menunjukkan nilai pada rentang 8388608 bits – 20132659 bits dan paket yang terkirim menunjukkan nilai pada rentang 1003520 bits – 18454937 bits. Rata-rata dari serangan *ICMP Flood* adalah menerima sebanyak 15658734 bits dalam 1 menit dan mengirimkan 13169550 bits dalam 1 menit. Berdasarkan tabel tersebut dapat dilihat bahwa jumlah paket diterima terbanyak berasal dari jenis serangan *TCP Flood* dan jumlah paket terkirim terbanyak berasal dari jenis serangan *UDP Flood*.

3.3 Diluncurkan Serangan DDoS dengan Perlindungan IPS

Pada pengujian terakhir dilakukan metode peluncuran serangan DDoS dengan dilindungi IPS. Hal ini bertujuan untuk melihat kemampuan perangkat dalam mengambalikan nilai lalu lintas jaringan menjadi normal kembali walaupun saat terserang DDoS.

Tabel 5. Lalu Lintas Jaringan Saat Serangan DDoS dengan Perlindungan IPS

Waktu (s)	Serangan DDoS	Paket Diterima (bits)	Paket Terkirim (bits)
10	TCP Flood	472	0
	UDP Flood	3120	0
	ICMP Flood	3120	0
20	TCP Flood	0	0
	UDP Flood	3600	0
	ICMP Flood	3120	0
30	TCP Flood	3120	0
	UDP Flood	4064	0
	ICMP Flood	0	0
40	TCP Flood	4064	0
	UDP Flood	3600	0
	ICMP Flood	3600	0
50	TCP Flood	3600	0
	UDP Flood	0	0
	ICMP Flood	4064	0
60	TCP Flood	4064	0
	UDP Flood	3600	0
	ICMP Flood	3600	0
Rata-rata	**TCP Flood**	**2553**	**0**
	UDP Flood	**2997**	**0**
	ICMP Flood	**2917**	**0**

Tabel 5 merupakan hasil pengukuran setelah diluncurkan serangan DDoS dengan perlindungan IPS. Nilai-nilai pada tabel tersebut menunjukkan penurunan jumlah paket yang diterima serta dikirimkan dari semua jenis serangan DDoS. Pada serangan *TCP Flood*, jumlah paket yang diterima dalam 1 menit menunjukkan pada rentang 0 – 4064 bits dan jumlah paket yang terkirim menunjukkan nilai 0 bits. Rata-rata besar paket yang terkirim adalah 2553 bits dalam 1 menit dan tidak ada paket yang terkirim. Kemudian pada serangan *UDP Flood*, jumlah paket yang diterima dan dikirim juga menunjukkan penurunan. Jumlah paket yang diterima berada pada rentang 0 – 4064 bits dan jumlah paket yang terkirim sebanyak 0 bits. Rata-rata paket yang diterima saat serangan *UDP Flood* terjadi adalah 2997 bits serta tidak ada paket yang dikirimkan. Pada jenis serangan terakhir, *ICMP*

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

Flood, jumlah paket yang diterima berada pada rentang 0 – 4064 bits dan paket yang dikirimkan sebesar 0 bits. Rata-rata jumlah paket yang diterima ketika serangan ini terjadi sebanyak 2917 bits dan tidak ada paket yang dikirim.

3.4 Perhitungan *Throughput* Lalu Lintas Jaringan

Setelah dilakukan pengujian dalam beberapa metode, akhirnya didapatkan nilai-nilai paket yang diterima serta paket yang dikirimkan dalam kurun waktu 1 menit. Nilai-nilai tersebut akan menjadi bahan analisis berikutnya untuk menghitung nilai *throughput*. Perhitungan *throughput* dilakukan menggunakan persamaan yang sudah disebutkan sebelumnya. Perhitungan *throughput* dibedakan menurut beberapa metode yang telah dilakukan sebelumnya.

3.5 Throughput Lalu Lintas Jaringan Normal

Pada bagian ini akan menghitung nilai *throughput* ketika keadaan tidak terjadi serangan apapun, atau dengan kata lain ketika keadaan lalu lintas normal.

$$Throughput\ (bps) = \frac{Packet\ received\ (bits)}{Total\ time\ attack\ (seconds)} = \frac{2606}{60} = 43.43\ bps$$

Dari perhitungan di atas didapatkan nilai *throughput* saat lalu lintas normal sebesar 43,43 bps. Nilai ini menjadi patokan yang menunjukkan nilai ketika keadaan *server* sedang normal.

3.6 Throughput Lalu Lintas Jaringan Saat Terserang DDoS Tanpa Perlindungan IPS

Bagian ini akan menghitung nilai *throughput* ketika keadaan sedang diserang serangan DDoS namun tidak dilindungi oleh IPS.

Tabel 6. *Throughput* Lalu Lintas Jaringan Terserang DDoS Tanpa Perlindungan IPS

Serangan DDoS	*Throughput* (bps)
TCP Flood	1080732.32
UDP Flood	1067217.33
ICMP Flood	260978.9

Tabel 6 merupakan hasil perhitungan *throughput* ketika terjadi serangan DDoS tanpa perlindungan IPS. Nilai *throughput* dari serangan *TCP Flood* sebesar 1080732,32 bps. Nilai *throughput* dari serangan *UDP Flood* sebesar 1067217,33 bps. Nilai *throughput* dari serangan *ICMP Flood* sebesar 260978,9 bps. Nilai-nilai tersebut menunjukkan peningkatan yang drastis jika dibandingkan dengan nilai *throughput* saat keadaan normal. Tingginya nilai *throughput* menunjukkan adanya serangan yang masuk ke dalam *server* sehingga *server* tidak berada dalam keadaan normal.

3.7 Throughput Lalu Lintas Jaringan Saat Terserang DDoS dengan Perlindungan IPS

Bagian ini akan menghitung nilai *throughput* ketika keadaan sedang diserang serangan DDoS dengan dilindungi oleh IPS.

Tabel 7. Throughput Lalu Lintas Jaringan Saat Terserang DDoS dengan Perlindungan IPS

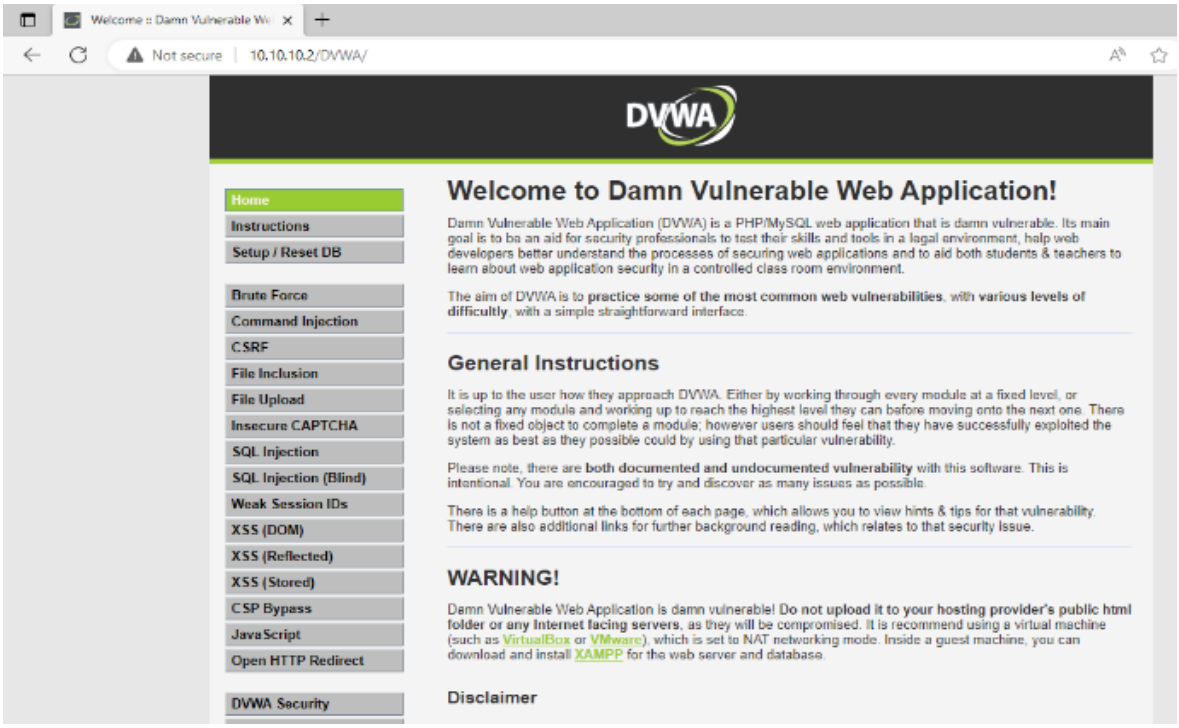
Serangan DDoS	*Throughput* (bps)
TCP Flood	42.55
UDP Flood	49.95
ICMP Flood	48.62

Tabel 7 merupakan hasil perhitungan *throughput* ketika terjadi serangan DDoS dengan perlindungan IPS. Nilai *throughput* dari serangan *TCP Flood* berkurang menjadi 42,55 bps. Nilai *throughput* dari serangan *UDP Flood* berkurang menjadi 49,95 bps. Nilai *throughput* dari serangan *ICMP Flood* berkurang menjadi 48,62 bps. Nilai-nilai tersebut menunjukkan penurunan dari perhitungan nilai *throughput* saat terjadi serangan sebelumnya. Nilai *throughput* ini menunjukkan kemiripan dengan nilai *throughput* saat keadaan normal.

3.8 Penyerangan *Malware* XSS

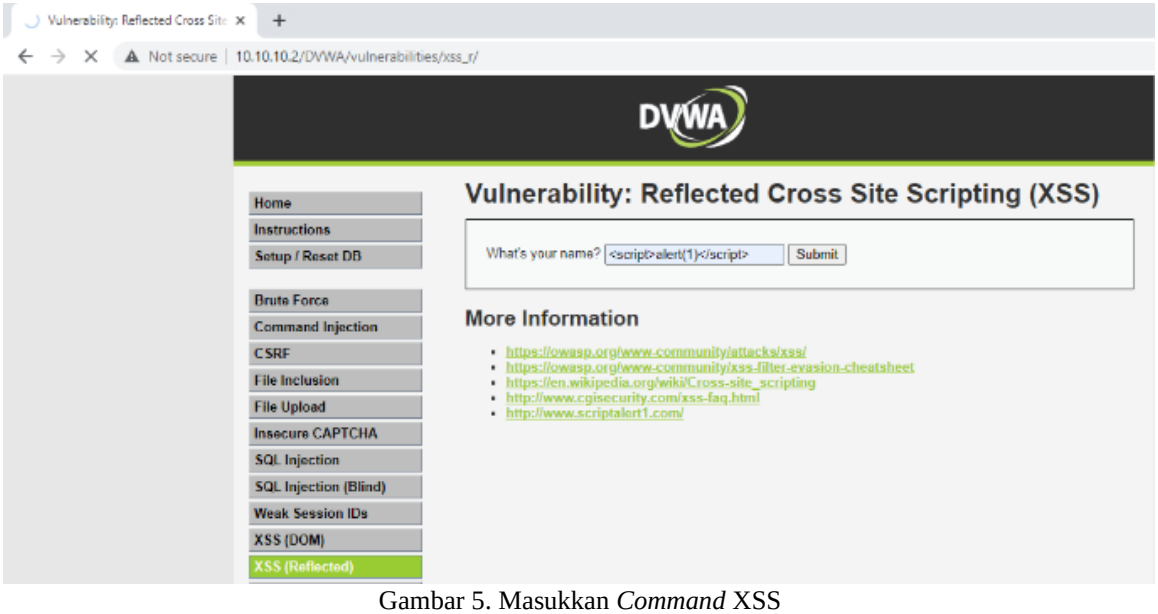
Sebagai tambahan dari pengujian perangkat IPS, dilakukan juga penyerangan selain serangan DDoS yaitu XSS. XSS merupakan serangan yang ditujukan ke *website* dengan memasukkan kode-kode atau *script* berbahaya (Hakim et al., 2020). Penyerangan *malware* ini dilakukan untuk melihat kemampuan perangkat dalam mencegah serangan selain DDoS. Penyerangan XSS dilakukan melalui DVWA yang telah terinstal pada perangkat *server*. Penyerangan dilakukan dengan mengakses DVWA dari perangkat *attacker* lalu mengirimkan serangan *malware* berupa XSS.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran



Gambar 4. Halaman Awal DVWA

Sebelum melakukan penyerangan, terlebih dahulu *attacker* mengakses IP *server* melalui peramban yang mana IP tersebut sudah terintegrasi dengan DVWA. Seperti pada Gambar 4, *attacker* dapat mengakses IP *server* dan memunculkan halaman utama dari DVWA. Hal ini menunjukkan bahwa *attacker* dapat berkomunikasi dengan *server*. Setelah dipastikan *attacker* dapat berkomunikasi dengan *server*, maka dilanjutkan dalam peluncuran serangan.

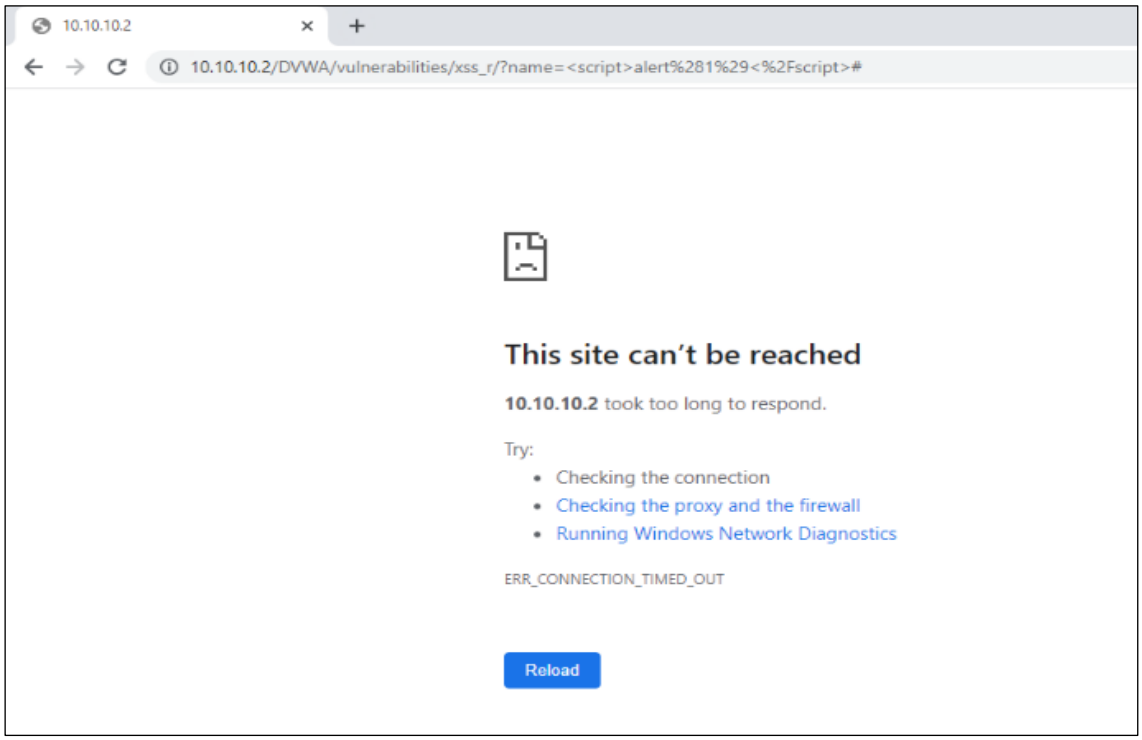


Gambar 5. Masukkan *Command* XSS

Berikutnya *attacker* memasukkan *command* XSS pada DVWA. Seperti pada Gambar 5, *command* XSS yang dimasukkan adalah "<script>alert(1)</script>". Ketika di-*submit*,

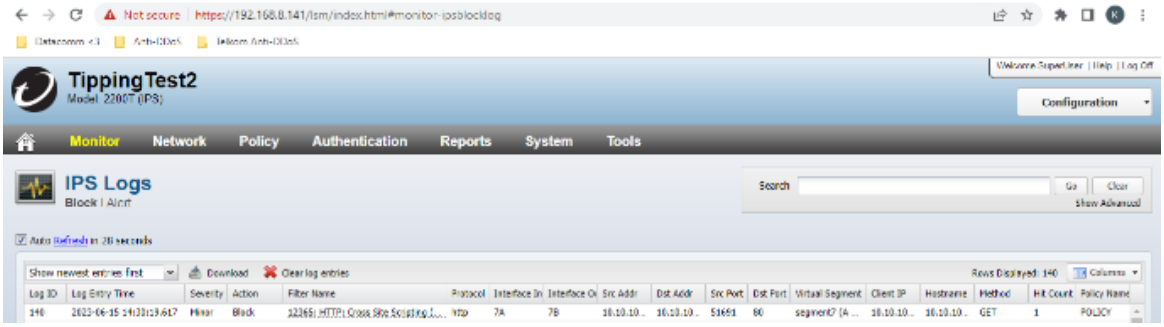
This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

command ini nantinya akan memunculkan sebuah *pop-up* berupa *alert* pada peramban dengan menampilkan angka "1". Jenis serangan ini memanfaatkan *bug* yang terdapat pada *web* dengan memberikan perintah yang seharusnya tidak dapat terjadi. Hal ini dapat dilakukan pada *web* ini karena memang dirancang untuk mempunyai celah keamanan.



Gambar 6. *Malware* XSS di-*block* oleh IPS

Setelah *command* tersebut di-*submit*, *web* akan memproses *command* tersebut. Namun, karena *web* sudah terlindungi oleh IPS, maka *command* tersebut tidak dapat dijalankan. Seperti pada Gambar 6, *website* akan menampilkan halaman yang tidak bisa diakses dengan tertulis "*This site can't be reached*". Hal ini menunjukkan bahwa *command* XSS yang dimasukkan berhasil dicegah oleh XSS sehingga tidak dapat masuk ke *server*.



Gambar 7. Tampilan *Block* XSS pada *Log* IPS

Setiap serangan yang berhasil dicegah oleh IPS, akan tercatat pada *log* perangkat. Informasi yang ditampilkan oleh *log* beragam, seperti tanggal dan waktu ketika serangan masuk, nama serangan, IP penyerang, IP tujuan, dan yang lainnya. Seperti pada Gambar 7, merupakan tampilan *log* perangkat IPS yang berhasil mencegah serangan XSS yang dimasukkan sebelumnya. Perangkat akan melakukan aksi terhadap serangan yang masuk berdasarkan IP yang didaftarkan untuk dilindungi.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License
Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran

IPS mengenali tiap jenis serangan yang masuk melalui *signature based malware* yang sudah dimiliki dalam *database* perangkat. Jika serangan yang masuk *match* dengan *database* tersebut, maka perangkat menandainya dengan serangan berbahaya dan langsung melakukan aksi *block*.

4. Kesimpulan

Berdasarkan penelitian yang sudah dilakukan dapat disimpulkan bahwa perangkat IPS dapat digunakan sebagai Anti-DDoS untuk mencegah serangan DDoS. Dari beberapa metode yang telah diujikan didapatkan hasil yang menunjukkan kemampuan IPS dalam mencegah serangan DDoS serta *malware* XSS. Dari metode pertama, ditunjukkan data yang menampilkan nilai ketika lalu lintas normal dari *server* dalam 1 menit dengan rata-rata sebesar 2606 bits paket yang diterima dan tidak ada paket yang dikirimkan. Lalu pada metode kedua, data menampilkan lalu lintas jaringan *server* yang terkena serangan DDoS tanpa perlindungan IPS dalam 1 menit dengan rata-rata sebesar 15658734 – 64843939 bits paket yang diterima dan sebesar 618461 – 64033040 bits paket yang dikirimkan. Pada metode terakhir, data yang didapatkan ketika terjadi serangan DDoS dengan perlindungan IPS dalam 1 menit dengan rata-rata sebesar 2553 – 2997 bits paket yang diterima dan tidak ada paket yang dikirimkan. Dari perhitungan *throughput* juga menunjukkan penurunan nilai ke kondisi normal. Ketika tidak dilindungi IPS, rata-rata nilai *throughput* sebesar 260978,9 – 1080732,32 bps. Ketika dilindungi IPS rata-rata nilai *throughput* sebesar 42,55 – 49,95 bps. Nilai *throughput* ketika dilindungi IPS menunjukkan kemiripan dengan nilai *throughput* ketika lalu lintas normal, yaitu sebesar 43,43 bps. Berdasarkan penurunan *throughput* tersebut, berarti *server* dapat berjalan dalam aktifitas normal kembali saat terlindungi IPS. Dengan data-data tersebut dapat disimpulkan bahwa akurasi keberhasilan perangkat dalam mencegah serangan DDoS adalah 100%. Pengujian tambahan juga menunjukkan keberhasilan IPS dalam mencegah serangan *malware* XSS yang membuktikan IPS dapat mencegah serangan lain selain DDoS. Berdasarkan kesimpulan yang diambil, menunjukkan bahwa perangkat "Trend Micro TippingPoint Threat Protection System 8400TX" dianggap mampu dalam memperkuat sistem keamanan Perusahaan X.

Referensi

(2023). • *DATASHEET • Tippingpoint Threat Protection System Family Key Features*.

Retrieved from https://www.datacomm.co.id/about/

Aditya, R. (2020). *Implementasi dan Analisis Pertahanan dari Serangan DOS dan DDoS pada Virtual Server dengan Menggunakan HIPS SNORT*. Bandung: Telkom University.

Firmansyah, M., Negara, R., & Sanjoyo, D. (2019). *Mengimplementasikan Sistem Keamanan Jaringan Intrusion Prevention System Berbasis SNORT pada Arsitektur Software Defined Network Implementing SNORT Based Intrusion Prevention System as Network Security in Software Defined Network*. Bandung.

McAfee, & LLC. (2019). *Revision A McAfee Network Security Platform (NS9500 Sensor Product Guide) Trademark Attributions License Information License Agreement the Place of Purchase for a Full Refund. 2 McAfee Network Security Platform*.

Nugraha, M. (2023). *Sistem Deteksi dan Mitigasi Serangan DDoS pada Jaringan Software Defined Network Menggunakan Self Organizing MAP*. Bandung: Telkom University.

Wahyudin, M. (2023). *Sistem Pendistribusian Blacklisted IP untuk Menangani Serangan DDoS Menggunakan Intrusion Prevention System (IPS) Suricata Berbasis Blockchain*. Bandung: Telkom University.

Hakim, A. S., Cahyanto, T. A., & Azizah, H. (2020). Serangan cross-site scripting (XSS) berdasarkan base metric CVSS V.2. *Jurnal Smart Teknologi*, *2*(1).

Pei, J., Chen, Y., & Ji, W. (2019). *A DDoS Attack Detection Method Based on Machine Learning*. *1237*(3). https://doi.org/10.1088/1742-6596/1237/3/032040

Saini, P. S., & Behal. (2020). *Detection of DDoS Attacks using Machine Learning Algorithms*. 16–21.

Vanny Andini, Lipur Sugiyanta, & Bachren Zaini. (2020). Analisis Kinerja Parameter Throughput Dan Delay Akses Inetrnet Di Smk Karyaguna Jakarta Selatan. *PINTER : Jurnal Pendidikan Teknik Informatika Dan Komputer*, *4*(2), 41–44. https://doi.org/10.21009/pinter.4.2.8

Wahyudi, F., & Utomo, L. T. (2021). *Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang*. *5*(1), 60–69. https://doi.org/10.29408/edumatic.v5i1.3278

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License

Copyright © 2023 Kevin Jorenta Surbakti, Rohmat Tulloh, Muhammad Nazel Djibran