OPEN ACCESS

Volume 9 (1), January-March 2025, 327-333

E-ISSN:2580-1643

Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

DOI: https://doi.org/10.35870/jtik.v9i1.3183

Pengaruh *Ping of Death* pada Perangkat dengan Sistem Keamanan Jaringan NIDS dan HIPS

Faisal Hakim Indrayana [1*], Erwien Christianto [2]

[1,2] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Kota Salatiga, Provinsi Jawa Tengah, Indonesia.*

a r t i c l e i n f o

Article history:
Received 13 September 2024
Received in revised form
30 September 2024
Accepted 25 October 2024
Available online January
2025.

Keywords:
Ping of Death; Network-Based Intrusion Detection System; Host Intrusion Prevention System; OpenvSwitch.

Kata Kunci:
Ping of Death; Network-Based Intrusion Detection System; Host Intrusion Prevention System; OpenvSwitch.

a b s t r a c t

This research will create a virtual network security simulation on OpenvSwitch using the Network-Based Intrusion Detection System (NIDS) method to determine the effect of Ping of Death attacks and the Host Intrusion Prevention System (HIPS) to prevent Ping of Death attacks. The security system on the network was created virtually via OpenvSwitch using the NIDS and HIDS methods designed using SNORT. The results of the Ping of Death attack cause the CPU performance to be very high, so that the computer works optimally due to the large number of packets going to the Server computer. This Ping of Death attack causes CPU performance to reach approximately 90%, the performance of the device's memory card reaches 80% and the Network receives 2.5 MiB packets per second and the use of HIDS is able to limit and prevent the Ping of Death attack from continuing.

a b s t r a k

Penelitian ini akan membuat sebuah simulasi keamanan jaringan virtual pada OpenvSwitch dengan menggunakan metode Network-Based Intrusion Detection System (NIDS) untuk mengetahui pengaruh dari serangan Ping of Death dan Host Intrusion Prevention System (HIPS) untuk mencegah serangan Ping of Death. Sistem keamanan pada jaringan dibuat secara virtual melalui OpenvSwitch dengan menggunakan metode NIDS dan HIDS yang dirancang menggunakan SNORT. Hasil dari serangan Ping of Death ini menyebabkan kinerja dari CPU sangat tinggi, sehingga komputer bekerja dengan maksimal dikarenakan banyaknya paket yang menuju komputer Server. Serangan dari Ping of Death ini menyebabkan kinerja CPU mencapai kurang lebih 90 %, kinerja dari kartu memori perangkat mencapai 80 % dan Network menerima paket sebanyak 2,5 MiB per detik dan penggunaan HIDS ini mampu membatasi dan mencegah serangan Ping of Death tetap berjalan.

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

Corresponding Author. Email: 672018167@student.uksw.edu [1].

1. Pendahuluan

Menjaga keamanan jaringan komputer sangat penting untuk memastikan data tetap utuh, valid, serta layanan selalu tersedia bagi pengguna. Hal ini memerlukan sistem keamanan jaringan yang efektif guna mencegah dan melindungi dari serangan peretas sehingga operasional jaringan komputer tidak terganggu. Mariusz Stawiwski dalam jurnal *The Principles of Network Security Design* menekankan bahwa tujuan utama dari keamanan jaringan adalah melindungi sumber daya sistem dari ancaman eksternal. Keamanan jaringan komputer mencakup berbagai aspek, termasuk perangkat keras sebagai elemen penting (Stawiwski, 2020). Keamanan perangkat keras berkaitan dengan perlindungan alat fisik yang digunakan dalam jaringan komputer. Meskipun sering diabaikan, keamanan perangkat keras sangat esensial dalam menjaga stabilitas jaringan. Server, tempat penyimpanan data, serta perangkat jaringan seperti hub dan switch, harus menjadi prioritas utama dalam pembatasan akses fisik. Sistem keamanan yang dapat memantau aktivitas jaringan serta mendeteksi percobaan serangan seperti *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) sangat diperlukan (Dietrich, 2021). Peretas dapat melakukan berbagai jenis serangan untuk mengakses sistem komputer yang ditargetkan. Salah satu serangan umum yang digunakan adalah *Denial of Service* (DoS), termasuk serangan *Ping of Death* (PoD).

Ping of Death adalah jenis serangan DoS di mana penyerang mengirimkan paket data yang rusak atau melebihi ukuran maksimal, sehingga perangkat target mengalami kerusakan atau malfungsi. Untuk meningkatkan keamanan jaringan komputer, diperlukan sistem yang mampu mendeteksi intrusi, dikenal sebagai *Intrusion Detection System* (IDS). Salah satu jenis IDS yang digunakan dalam mendeteksi serangan jaringan adalah *Network-Based Intrusion Detection System* (NIDS), sementara metode *Host Intrusion Prevention System* (HIPS) digunakan untuk mencegah serangan (Ohyver & Chandra, 2023). *Network-Based Intrusion Detection System* (NIDS) memiliki kemampuan memantau serangan serta lalu lintas di seluruh jaringan yang menggunakan sistem ini. NIDS menganalisis semua lalu lintas yang masuk untuk mendeteksi percobaan serangan atau intrusi. NIDS sangat efektif dalam memantau lalu lintas antara host dan bagian jaringan lokal lainnya. Biasanya, NIDS ditempatkan sebelum atau sesudah firewall serta pada gateway VPN untuk mengevaluasi efektivitas interaksi sistem keamanan, sehingga meningkatkan keamanan jaringan secara keseluruhan (Yuliandari *et al*., 2023). *Host Intrusion Prevention System* (HIPS) adalah sistem keamanan yang dipasang pada perangkat endpoint individu untuk memantau dan mencegah aktivitas mencurigakan atau berbahaya, termasuk perlindungan dari malware, eksploitasi, serta aktivitas lain yang mengancam keamanan sistem. HIPS mampu menghentikan serangan secara langsung, seperti memutus koneksi jaringan, menghentikan proses serangan, atau memblokir akses penyerang ke file tertentu (Wijaya *et al*., 2023). Penelitian terdahulu yang menjadi landasan penelitian ini mencakup studi oleh Ohyver dan Chandra (2023) dalam *Simulasi Keamanan Jaringan pada DPDK OpenvSwitch Berbasis Network-Based Intrusion Detection System (NIDS)*. Mereka menyimpulkan bahwa peretasan jaringan komputer sering dilakukan oleh kelompok yang ingin menembus keamanan sistem untuk mencari, mengubah, atau bahkan menghapus data. Penggunaan OpenvSwitch serta penerapan NIDS terbukti membantu dalam melindungi jaringan virtual. Simulasi yang dilakukan menunjukkan bahwa tingkat keberhasilan NIDS dalam mendeteksi serangan DoS mencapai sekitar 75%.

Penelitian oleh Adam, Alwi, dan As'ad (2022) dalam *Analisis Forensik Terhadap Serangan DDoS Ping of Death pada Server* mengidentifikasi masalah saat banyak paket data terkumpul dan memerlukan analisis lebih lanjut. Penelitian ini mensimulasikan serangan *DDoS Ping of Death* pada web server dan menggunakan perangkat lunak Snorby untuk merekam data serangan yang kemudian dianalisis mengikuti metode forensik NIST. Penelitian ketiga oleh Wijaya, Kalsum, dan Riska (2023) dalam *Penerapan OPNsense Sebagai Sistem Keamanan Web Server Menggunakan Metode Host Intrusion Prevention System* menunjukkan bahwa OPNsense efektif dalam melindungi web server di jaringan LAN. Metode yang digunakan mencakup pencegahan berlapis melalui filter paket dan inspeksi sistem secara real-time. Dalam penelitian ini, dilakukan simulasi virtual keamanan jaringan menggunakan OpenvSwitch. Pada jaringan virtual tersebut, diterapkan sistem keamanan berupa *Network-Based*

Intrusion Detection System (NIDS) dan *Host Intrusion Prevention System* (HIPS). NIDS diuji menggunakan serangan *Ping of Death* (PoD) untuk mengevaluasi kemampuan deteksi serta mengamati dampaknya terhadap perangkat. HIPS digunakan untuk mencegah serta mengamankan perangkat dari serangan PoD. Tujuan pengujian ini adalah mengevaluasi efektivitas NIDS dan HIPS dalam mendeteksi serta mengantisipasi serangan, serta memahami dampak serangan PoD terhadap kinerja perangkat komputer.

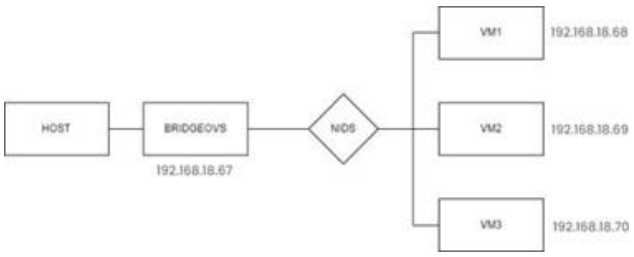
2. Metodologi Penelitian

Gambar 1. Tahapan Penelitian

Penjelasan Tahapan Penelitian (Gambar 1):

1) Merencanakan skenario simulasi dengan merujuk pada jurnal dan referensi terkait untuk memastikan keakuratan serta relevansi penelitian, serta mempersiapkan perangkat keras dan perangkat lunak yang diperlukan untuk simulasi sistem keamanan jaringan yang melibatkan NIDS pada OpenvSwitch.
2) Langkah berikutnya adalah melakukan proses simulasi, yang mencakup sejumlah tugas penting seperti perancangan jaringan, instalasi perangkat lunak, konfigurasi OpenvSwitch, dan penyiapan NIDS.
3) Pada tahap pengujian, kegiatan utama adalah melakukan serangkaian pengujian. Komputer yang bertindak sebagai penyerang akan melancarkan serangkaian serangan terhadap komputer atau server dalam jaringan. Sementara itu, komputer yang telah diimplementasikan dengan NIDS akan mendeteksi setiap serangan yang dilakukan oleh komputer penyerang dan mencatat dampak serangan tersebut terhadap sistem, seperti penggunaan CPU dan memori. Selanjutnya, sistem HIPS yang telah diimplementasikan akan mencegah serangan tersebut.
4) Setelah menyelesaikan proses pengujian, langkah berikutnya adalah melakukan analisis hasil pengujian simulasi. Hasil analisis ini akan digunakan sebagai dasar untuk menyusun kesimpulan. Kesimpulan akan mencakup ringkasan hasil pengujian, temuan signifikan, evaluasi kinerja NIDS, penggunaan CPU dan memori, serta rekomendasi untuk perbaikan atau peningkatan keamanan jaringan.

Pada Gambar 2 ditampilkan topologi jaringan yang digunakan dalam penelitian ini. Perangkat yang berperan sebagai pengelola *OpenvSwitch* (OVS) adalah host utama. Host ini juga menjadi tempat penerapan sistem keamanan jaringan, yaitu *Network-Based Intrusion Detection System* (NIDS) dan *Host Intrusion Prevention System* (HIPS). Jaringan virtual yang dibuat terdiri dari tiga mesin virtual (VM), yaitu VM 1, VM 2, dan VM 3. Setiap VM dihubungkan ke bridge OVS melalui *Virtual Interface* (vport1–vport3).
Komputer yang digunakan memiliki satu *Virtual Interface*, yaitu enp1s0, yang berfungsi sebagai penghubung antara host, OVS, VM, dan internet.



Gambar 2. Topologi Penelitian

3. Hasil dan Pembahasan

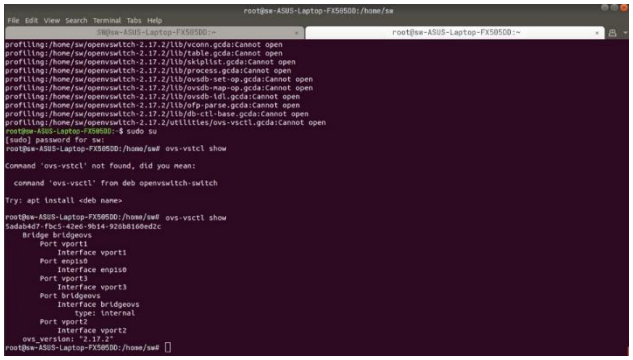
Hasil

Setelah menyelesaikan persiapan yang meliputi topologi jaringan, perangkat keras, dan perangkat lunak seperti *OpenvSwitch*, *Snort*, serta perangkat lunak lain yang diperlukan, serta menginstal alat *Ping of Death* pada VM penyerang untuk melakukan serangan terhadap *OpenvSwitch*, langkah selanjutnya adalah melakukan simulasi serangan. Serangan yang disimulasikan adalah serangan *Ping of Death* yang ditujukan kepada *OpenvSwitch*. Tujuan simulasi ini adalah untuk menguji apakah sistem *Network Intrusion Detection System* (NIDS) dari *Snort* dapat mendeteksi serangan tersebut secara efektif dan menganalisis

dampak serangan terhadap perangkat. Setelah itu, dilakukan pencegahan serangan *PoD* menggunakan sistem *Host Intrusion Prevention System* (HIPS). Hasil yang diharapkan dari penelitian ini adalah mengetahui sejauh mana sistem *Network Intrusion Detection System* (NIDS) yang diimplementasikan pada *OpenvSwitch* dapat berfungsi secara efektif dalam mendeteksi serangan yang dilancarkan oleh penyerang terhadap *OpenvSwitch*. Selain itu, sistem *Host Intrusion Prevention System* (HIPS) diharapkan mampu mengantisipasi serangan tersebut. Penelitian ini juga bertujuan untuk menganalisis dampak dari serangan tersebut pada kinerja perangkat jaringan yang diserang.

Instalasi dan Konfigurasi OpenvSwitch

Setelah mengunduh *OpenvSwitch* dari https://www.openvswitch.org/download/ dan melakukan instalasi, langkah pertama yang dilakukan adalah membuat sebuah *bridge* dan tiga port untuk menghubungkan ketiga mesin virtual (VM) agar dapat terhubung dalam jaringan. Dalam penelitian ini, *bridge* tersebut diberi nama "bridgeovs", sementara ketiga port-nya diberi nama "Vport1", "Vport2", dan "Vport3".



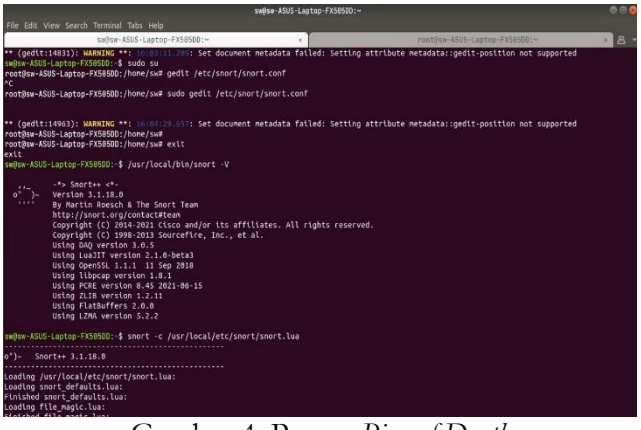
Gambar 3. *Bridge* dan *Port* pada *OpenvSwitch*

Bridge dan ketiga VM tersebut memiliki alamat IP sebagai berikut: *bridgeovs*: 192.168.18.67, VM1 yang terhubung melalui *vport1*: 192.168.18.68, VM2 yang terhubung melalui *vport2*: 192.168.18.69, dan VM3 yang terhubung melalui *vport3*: 192.168.18.70.

Instalasi dan Konfigurasi SNORT

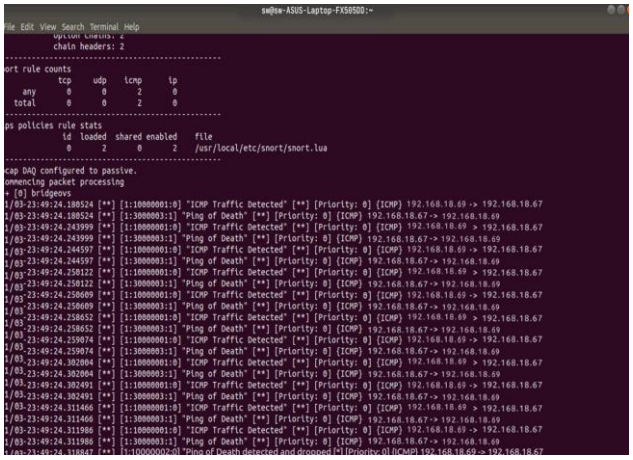
Snort dapat diunduh pada website *https://www.snort.org/downloads*. Pengguna harus mengunduh perangkat lunak Snort beserta aturan (rules) yang diperlukan dari situs tersebut. Setelah instalasi Snort selesai, langkah selanjutnya adalah melakukan konfigurasi agar Snort dapat menangkap dan menganalisa paket-paket yang ditujukan kepada *OpenvSwitch*. Konfigurasi ini mirip dengan konfigurasi pada network cards untuk memberikan alamat IP pada Snort sehingga Snort dapat mengidentifikasi alamat IP yang perlu dipantau. Selain itu, *rules* juga perlu dibuat pada direktori Snort. Penambahan aturan ini sangat penting untuk memungkinkan Snort membedakan paket-paket yang ditujukan kepada OpenvSwitch dan menentukan apakah paket tersebut berpotensi berbahaya atau tidak. Rules yang perlu ditambahkan yaitu "*alert icmp any any ->$HOME_NET any (msg:"Ping of Death"; dsize:>1500; sid:3000003; rev:1;)" untuk mengetahui jika ada serangan Ping of Death dan, "alert icmp any any -> any any (msg:"ICMP Traffic Detected"; sid:10000001; metadata:policy security-ips alert;)*" untuk mengetahui jika ada yang melakukan *Ping*.

Lalu pada *rules* HIPS agar dapat mencegah dan mengantisipasi serangan *Ping of death*, perlu untuk menambahkan rules "*drop icmp any any -> any any (msg:"Ping of Death detected and dropped"; dsize:>65535; sid:1000002;)*". *Rules* ini akan mendeteksi paket ICMP yang terlalu besar dan menjatuhkannya untuk mencegah serangan *Ping of Death*. Setelah konfigurasi telah selesai, Snort perlu dijalankan untuk memungkinkannya membaca paket-paket yang dikirim ke OpenvSwitch. Untuk menjalankan Snort, perlu memasukkan perintah berikut ke terminal: */usr/local/bin/snort -v*. Perintah ni akan menghasilkan output seperti yang terlihat pada Gambar 4 yang menunjukkan bahwa Snort telah diaktifkan dan siap untuk melakukan deteksi dan pencegahan pada *OpenvSwitch*.



Gambar 4. Proses *Ping of Death*

Pada gambar 4 dapat dilihat bahwa Snort telah mendeteksi serangan Ping of Death dari VM 2. Snort akan menampilkan pesan terkait serangan "*Ping of Death*" yang ditujukan kepada OpenvSwitch, serta menampilkan waktu serangan, *port*, dan alamat IP penyerang yang menyerang OpenvSwitch. Lalu sistem HIPS yang telah di konfigurasi pada Snort akan mengehentikan serangan *Ping of Death* tersebut. dapat dilihat pada alert "*[1:10000002:0] "Ping of Death detected and dropped [**] [Priority: 0] {ICMP} 192.168.18.69 -> 192.168.18.67*" menandakan bahwa *Ping of Death* telah terdeteksi dan dicegah oleh sistem HIPS.



Gambar 5. Snort yang mendeteksi dan menghentikan serangan

Hasil serangan *ping of death* pada *openvswitch* dan pencegahan serangan dengan HIPS

Pada gambar 6 dapat dilihat bahwa serangan *Ping of Death* ini menyebabkan kinerja dari CPU sangat tinggi, maka komputer akan bekerja dengan maksimal dikarenakan banyaknya paket yang menuju komputer Server. Dapat dilihat pada gambar 6, serangan dari *Ping of Death* ini menyebabkan kinerja CPU mencapai kurang lebih 90%. Lalu untuk kinerja dari memori perangkat mencapai 80 % dan *Network* menerima paket sebanyak 2,5 MiB per detik. Pada gambar 6 dapat dilihat bahwa setelah HIPS menghentikan serangan Ping of Death, kinerja dari CPU, memori, dan *network* kembali normal. Hal ini dapat dilihat pada grafik kinerja perangkat yang turun secara signifikan dimana kinerja CPU turun menjadi kurang lebih 13%, memori 16.6% dan network 0 MiB per detik.

Gambar 6. Grafik performa komputer saat serangan *Ping of Death*

Gambar 7. Grafik performa komputer saat normal

Pembahasan

Hasil penelitian ini menunjukkan bahwa sistem keamanan yang mengombinasikan *Network Intrusion Detection System* (NIDS) menggunakan *Snort* dan *Host Intrusion Prevention System* (HIPS) pada *OpenvSwitch* efektif dalam mendeteksi serta mencegah serangan *Ping of Death*. Berdasarkan konfigurasi yang dilakukan, *Snort* mampu mengidentifikasi paket ICMP berukuran besar yang berpotensi menjadi serangan. Hal ini sesuai dengan penelitian Dietrich (2021) dan Ilham *et al.* (2023) yang menunjukkan efektivitas *Snort* sebagai NIDS dalam mendeteksi serangan *Denial of Service* (DoS). Ohyver dan Chandra (2023) juga mencatat keberhasilan NIDS berbasis *Snort* dalam mendeteksi serangan dengan tingkat akurasi sekitar 75%. Pada simulasi ini, setelah NIDS mendeteksi serangan, HIPS yang diterapkan berhasil menghentikan serangan dengan memblokir paket ICMP yang berukuran besar. Hasil ini sejalan dengan temuan Wijaya *et al.* (2023) yang menyatakan bahwa HIPS efektif dalam melindungi perangkat dari serangan berbahaya, serta penelitian Suwanto *et al.* (2019) yang menunjukkan pentingnya penggunaan sistem pencegahan intrusi untuk meningkatkan keamanan jaringan. Dampak serangan *Ping of Death* terhadap kinerja jaringan juga

terukur secara jelas dalam penelitian ini. Sebelum serangan dihentikan oleh HIPS, penggunaan CPU meningkat hingga 90%, memori mencapai 80%, dan lalu lintas jaringan naik menjadi 2,5 MiB per detik. Kondisi ini mengindikasikan bahwa serangan *Ping of Death* dapat menurunkan kinerja perangkat secara signifikan, mendukung hasil analisis Walad (2020) tentang dampak negatif serangan DoS pada stabilitas sistem. Namun, setelah HIPS aktif menghentikan serangan, kinerja perangkat kembali normal dengan penggunaan CPU turun menjadi 13% dan memori menjadi 16,6%, serta lalu lintas jaringan yang stabil tanpa adanya paket ICMP berbahaya. Temuan ini menguatkan studi Alwi *et al.* (2022) yang mencatat bahwa sistem pencegahan intrusi seperti HIPS mampu mengurangi dampak serangan pada server dan memperbaiki kondisi jaringan.

Efektivitas kombinasi NIDS dan HIPS dalam menjaga keamanan jaringan juga tercermin dari hasil simulasi ini. NIDS berperan sebagai detektor yang mengidentifikasi potensi serangan dan memberikan peringatan dini, sementara HIPS bertindak sebagai penghalang yang menghentikan serangan sebelum menyebabkan kerusakan lebih lanjut. Integrasi kedua sistem ini terbukti memberikan perlindungan yang lebih kuat, seperti yang telah disarankan dalam penelitian oleh Yuliandari *et al.* (2023) serta Fachri dan Harahap (2020), yang menekankan pentingnya penerapan sistem keamanan berlapis untuk menghadapi ancaman jaringan yang kompleks. Hasil penelitian ini memperkuat pandangan bahwa implementasi kombinasi NIDS dan HIPS pada jaringan komputer dapat memberikan perlindungan yang efektif terhadap serangan berbahaya seperti *Ping of Death*, menjaga stabilitas perangkat, dan meningkatkan keamanan jaringan secara keseluruhan.

4. Kesimpulan

Hasil pengujian menunjukkan bahwa OpenvSwitch dapat memanfaatkan Snort dalam untuk menerapkan sistem keamanan jaringan *Network-Intrusion Detection System* (NIDS) dan *Host Intrusion Prevention System* (HIPS), serta memungkinkan akses internet dari jaringan lokal pada *Virtual Machine* yang terhubung dengan baik ke OpenvSwitch. Sistem NIDS yang menggunakan Snort ini dapat mengidentifikasi jenis serangan *Ping of Death* yang dilancarkan oleh penyerang dan menunjukkan waktu, *port*, dan alamat IP penyerang dan sistem HIPS dapat menghentikan serta mencegah serangan *Ping of Death*. Pengaruh yang diterima oleh perangkat pada serangan *Ping of Death* ini menyebabkan kinerja dari CPU sangat tinggi, maka komputer akan bekerja dengan maksimal dikarenakan banyaknya paket yang menuju komputer Server. Serangan dari *Ping of Death* ini menyebabkan kinerja CPU mencapai kurang lebih 90 %. Lalu untuk kinerja dari kartu memori perangkat mencapai 80 % dan *Network* menerima paket sebanyak 2,5 MiB per detik. Lalu ketika HIPS menghentikan serangan *Ping of Death*, kinerja dari perangkat menurun dari CPU menjadi kurang lebih 13%, memori 16,6%, dan *network* 0 MiB per detik.

Saran yang dapat diberikan ialah bahwa penggunaan sistem keamanan jaringan *Network-Intrusion Detection System* (NIDS) sangat berguna untuk mengetahui apabila ada serangan pada perangkat. Akan tetapi NIDS hanya memberikan peringatan berupa *Alert* jika ada serangan yang masuk namun NIDS tidak dapat mengantisipasi serangan tersebut. Agar sistem keamanan jaringan bekerja dengan maksimal, sangat disarankan untuk menambahkan sistem *Intrusion Prevention System* (IPS). Pada penelitian ini, digunakan sistem *Host Intrusion Detection System* yang dimana sistem ini hanya mencegah serangan pada host individu tidak secara universal. Ada banyak jenis sistem IDS yang dapat digunakan sesuai dengan kebutuhan dan fokus keamanan yang diingnakan. Contoh nya seperti *Network-based Intrusion Prevention System* (NIPS) yang Memonitor dan mencegah serangan pada seluruh jaringan atau *Wireless Intrusion Prevention System* (WIPS) yang memonitor dan mencegah serangan pada jaringan nirkabel. Sistem IPS sendiri mampu menyingkirkan dan mengantisipasi apabila ada serangan yang masuk ke perangkat. Dengan menggabungkan kedua sistem keamanan tersebut, ketika NIDS mendeteksi serangan yang masuk ke perangkat secara otomatis sistem IPS mampu memblokir dan menyingkirkan serangan tersebut sehingga keamanan jaringan yang dimiliki pada perangkat dapat berjalan dengan maksimal.

5. Daftar Pustaka

Abdurrohman, M., Suharto, N., & Mas' udia, P. E. (2023). Overcoming Network Security on Host-Based Intrusion Detection System (HIDS) With IP and PORT Blocking Methods. *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)*, *13*(3), 208-213.

ANam, M. K., Sudyana, D., Ulfah, A. N., & Lizarti, N. (2020). Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru. *J-PEMAS-Jurnal Pengabdian Masyarakat*, *1*(2), 39-44.

As' ad, I. (2022). Analisis Forensik Terhadap Serangan DDoS Ping of Death Pada Server. *Cyber Security dan Forensik Digital (CSFD)*, *5*(1), 23-31.

Dietrich, N. (2021). Snort 3.1. 18.0 on Ubuntu 18 & 20. *Configuring a Full NIDS & SIEM*.

Fachri, B., & Harahap, F. H. (2020). Simulasi penggunaan intrusion detection system (IDS) sebagai keamanan jaringan dan komputer. *Jurnal Media Informasi Budidarma*, 4(2), 413. DOI: https://doi.org/10.30865/mib.v4i2.2037.

Gassais, R., et al. (2020). Multi-level host-based intrusion detection system for Internet of Things. *Journal of Cloud Computing*, 9(1). DOI: https://doi.org/10.1186/s13677-020-00206-6.

Ilham, K. F. I., Alwi, E. I., & Fattah, F. (2023). Penerapan dan analisis network security Snort menggunakan intrusion detection system pada serangan UDP flood. *Informal*, 8(1), 94. DOI: https://doi.org/10.19184/isj.v8i1.34003.

Ohyver, J. T. (2022). *Simulasi Keamanan Jaringan pada DPDK OpenvSwitch Berbasis Network-Based Intrusion Detection System (NIDS)* (Doctoral dissertation).

OpenvSwitch. (2022). *Open vSwitch, Release 2.17.90*.

Silalahi, L. M., & Kurniawan, A. (2023). Analisis keamanan jaringan menggunakan intrusion prevention system (IPS) dengan metode traffic behavior. *Electrician: Jurnal Rekayasa dan Teknologi Elektro*, 17(1), 71–76. DOI: https://doi.org/10.23960/elc.v17n1.2296.

Suwanto, R., Ruslianto, I., & Diponegoro, M. (2019). Implementasi intrusion prevention system (IPS) menggunakan snort dan IPTABLE pada monitoring jaringan lokal berbasis website. *Coding Jurnal Komputer dan Aplikasi*, *7*(01). DOI: https://doi.org/10.26418/coding.v7i01.3269.

Team, S. (2017). Snort–Network Intrusion Detection & Prevention System.

Wahyudi, F., & Utomo, L. T. (2021). Perancangan security network intrusion prevention system pada PDTI Universitas Islam Raden Rahmat Malang. *Edumatic*, 5(1), 60–69. DOI: https://doi.org/10.29408/edumatic.v5i1.3278.

Walad, I. (2020). *Analisis Denial Of Service Attack Pada Sistem Keamanan Web* (Doctoral dissertation, Universitas Sumatera Utara).

Wijaya, A. W. A., Kalsum, T. U., & Riska. (2023). Penerapan OPNsense sebagai sistem keamanan web server menggunakan metode host intrusion prevention system. *Jurnal Amplifier: Jurnal Ilmiah Bidang Teknik Elektro dan Komputer*, 13(2), 91–100. DOI: https://doi.org/10.33369/jamplifier.v13i2.31514.

Yuliandari, D., Walim, W., Raja, B. K., Ningsih, R., & Wahidin, A. J. (2023). Simulasi Penerapan Sistem Monitoring Jaringan Snort NIDS Pada Web Server Menggunakan Metode SPDLC. *Jurnal Infortech*, *5*(2), 133-138. DOI: https://doi.org/10.31294/infortech.v5i2.17338.