NASKAH PUBLIKASI (*MANUSCRIPT)*

PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGGUNAKAN *INSTRUSION DETECTION SYSTEM* (IDS) SURICATA

NETWORK ATTACK DETECTION AND PREVENTION USING INSTRUSION DETECTION SYSTEM (IDS) SURICATA

Khaerunnisa Marda Tillah, Faldi, Muhammad T Sumadi

DISUSUN OLEH:

KHAERUNNISA MARDA TILLAH

1911102441070

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

SAMARINDA

2023

Naskah Publikasi (*Manuscript)*

Pendeteksi dan Pencegahan Serangan Jaringan menggunakan *Instrusion Detection System* (IDS) Suricata

Network Attack Detection and Prevention using Instrusion Detection System (IDS) *Suricata*

Khaerunnisa Marda Tillah, Faldi, Muhammad T Sumadi

Disusun Oleh:

Khaerunnisa Marda Tillah

1911102441070

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

SAMARINDA

2023

HALAMAN PENGESAHAN

PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGGUNAKAN *INSTRUSION DETECTION SYSTEM* (IDS) SURICATA

NASKAH PUBLIKASI

DISUSUN OLEH :

KHAERUNNISA MARDA TILLAH

1911102441070

Dosen Pembimbing	Penguji
Faldi, S.Kom.,M,Ti	Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom
NIDN. 1121079101	NIDN. 1111089501

Dekan	Ketua Program Studi
Prof. Ir. Sarjito, MT., Ph.D	Asslia Johar Latipah, M.Cs
NIDN. 0610116204	NIDN. 1124098902

PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGGUNAKAN *INSTRUSION DETECTION SYSTEM* (IDS) SURICATA

Khaerunnisa Marda Tillah[1*], Faldi[2], Muhammad Taufiq Sumadi[3].
[1]*Teknik Informatika, Indonesia*
[2]*Teknik Informatika, Indonesia*
[3]*Teknik Informatika, Indonesia*

[*]*1911102441070@umkt.ac.id*

Abstract

Network attacks pose a serious threat in academic environments. To protect the network from such attacks, a system capable of detecting and preventing them is needed. This research aims to develop and implement Suricata Intrusion Detection System (IDS) to detect and prevent network attacks. The research utilizes the Security Policy Development Life Cycle (SPDLC) method, involving stages such as requirement analysis, IDS system design, IDS implementation on the network, and testing and evaluation of the developed IDS system. The analysis results of this research show that Suricata IDS is capable of detecting Slowloris, Nmap Scan, Denial of Service (DoS), and PingFlood attacks. The detection time for Slowloris attack is 3 minutes, while real-time detection is achieved for Nmap Scan, DoS, and PingFlood attacks. Suricata IDS performs well in detecting threat packets, and the variation in detection time for different attacks is due to their distinct characteristics.

Keywords: IDS, SLowloris, Nmap Scan, DoS, PingFlood.

Abstrak

Serangan jaringan merupakan ancaman yang serius dalam lingkungan akademik. Untuk melindungi jaringan dari serangan, diperlukan sistem yang mampu mendeteksi dan mencegah serangan tersebut. Penelitian ini bertujuan mengembangkan dan mengimplementasikan *Intrusion Detection System* (IDS) Suricata untuk mendeteksi dan mencegah serangan jaringan. Penelitian ini menggunakan metode *Security Policy Development Life Cycle* (SPDLC) dengan tahapan analisis kebutuhan, perancangan sistem IDS, implementasi IDS pada jaringan, serta pengujian dan evaluasi sistem IDS yang dikembangkan. Hasil analisis dari penelitian ini menunjukkan bahwa IDS Suricata mampu mendeteksi serangan *Slowloris, Nmap Scan, Denial of Service* (D0S), dan *PingFlood*. Waktu yang diperlukan untuk mendeteksi serangan *Slowloris* adalah 3 menit, sedangkan untuk serangan *Nmap Scan,* DoS, dan *PingFlood* terdeteksi *real-time.* IDS Suricata bekerja dengan baik dalam mendeteksi paket-paket ancaman, perbedaan waktu dalam deteksi serangan bervariasi dikarenakan setiap serangan memiliki karakteristik yang berbeda.

Kata kunci : IDS, *SLowloris, Nmap Scan,* DoS, *PingFlood.*

1. Pendahuluan

Dalam lingkungan akademik yang semakin berkembang, jaringan komputer menjadi infrastruktur yang sangat penting dalam menghubungkan berbagai sistem dan pengguna di seluruh dunia. Namun, dengan meningkatnya kompleksitas jaringan dan jumlah serangan yang dilakukan oleh pihak yang tidak bertanggung jawab, keamanan jaringan telah menjadi salah satu tantangan terbesar dalam dunia teknologi informasi.

Serangan jaringan dapat mencakup berbagai bentuk, termasuk pencurian data sensitif, penghancuran sistem, dan gangguan pada ketersediaan layanan. Untuk melindungi jaringan komputer dari serangan ini, dibutuhkan sistem yang efektif dalam mendeteksi dan mencegah serangan tersebut.

Salah satu solusi yang digunakan secara luas adalah Sistem Deteksi Intrusi (Intrusion Detection System/IDS). IDS adalah sebuah mekanisme yang dirancang untuk mengidentifikasi aktivitas yang mencurigakan atau serangan yang sedang terjadi pada jaringan komputer. Dengan mengamati lalu lintas jaringan, IDS dapat memantau dan menganalisis aktivitas yang tidak normal, seperti usaha masuk yang tidak sah atau eksploitasi kerentanan sistem.

Dalam penelitian ini, kami fokus pada penggunaan Suricata sebagai sistem deteksi intrusi untuk mendeteksi dan mencegah serangan jaringan. Suricata adalah salah satu IDS open-source yang sangat powerful dan sering digunakan dalam lingkungan jaringan yang kompleks. Suricata memiliki kemampuan untuk memantau lalu lintas jaringan secara real-time, menganalisis paket jaringan, dan mendeteksi pola serangan yang diketahui.

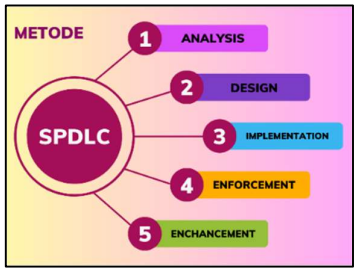
Penelitian ini bertujuan untuk menganalisis efektivitas Suricata dalam mendeteksi dan mencegah serangan jaringan. Kami akan menguji Suricata pada skenario serangan yang umum dan mengukur tingkat deteksi yang dicapai serta jumlah serangan yang berhasil dicegah. Selain itu, kami juga akan mempertimbangkan faktor-faktor lain seperti performa sistem, keandalan, dan efisiensi dalam penerapan Suricata.

Hasil dari penelitian ini diharapkan dapat memberikan wawasan yang berharga dalam penggunaan Suricata sebagai alat yang efektif dalam mengamankan jaringan komputer dari serangan. Diharapkan penelitian ini dapat membantu organisasi dan profesional keamanan dalam memilih dan mengimplementasikan solusi IDS yang tepat untuk melindungi jaringan mereka.

Penelitian ini terdiri dari beberapa bagian, termasuk tinjauan pustaka tentang serangan jaringan, sistem deteksi intrusi, dan Suricata. Metodologi penelitian yang digunakan juga akan dijelaskan secara rinci. Selanjutnya, kami akan menyajikan hasil eksperimen dan menganalisis data yang diperoleh. Terakhir, kami akan menyimpulkan penelitian ini dengan menyoroti temuan utama dan memberikan rekomendasi untuk pengembangan lebih lanjut.

Dengan melakukan penelitian ini, diharapkan bahwa kita dapat melangkah lebih maju dalam upaya meningkatkan keamanan jaringan dan melindungi informasi penting dari serangan yang berpotensi merugikan.

2. Metode Penelitian



Gambar 1 : Security Policy Development Life Cycle

Metode yang digunakan dalam penelitian ini adalah Security Policy Development Life Cycle (SPDLC) atau siklus pengembangan kebijakan keamanan. SPDLC adalah pendekatan yang terstruktur dan berurutan dalam mengembangkan kebijakan keamanan yang efektif dan sesuai dengan kebutuhan organisasi. Rancangan SPDLC mencakup langkah-langkah yang diperlukan untuk mengidentifikasi,merancang,mengimplementasikan, dan memantau kebijakan keamanan. Proses Pengolahan dan Analisis Data/Informasi:

a. Pengumpulan Data: Data dan informasi yang diperlukan dalam setiap tahap SPDLC akan dikumpulkan menggunakan berbagai metode seperti wawancara, tinjauan dokumen, observasi, dan proses pengumpulan data yang relevan. Data dan informasi ini dapat berupa kebutuhan keamanan, standar industri, kebijakan yang ada, dan laporan keamanan.

b. Analisis Data: Data yang dikumpulkan akan dianalisis untuk memahami kebutuhan keamanan, menganalisis kebijakan yang ada, dan mengevaluasi keberhasilan implementasi kebijakan keamanan. Analisis data melibatkan pengidentifikasian tren, perbandingan dengan praktik terbaik, dan pengukuran keberhasilan implementasi kebijakan keamanan.

c. Interpretasi Hasil: Hasil analisis data akan diinterpretasikan untuk menghasilkan rekomendasi dan rencana aksi yang sesuai. Hasil ini akan membantu dalam pengembangan kebijakan keamanan yang efektif dan peningkatan kebijakan keamanan yang ada. Interpretasi hasil juga dapat

melibatkan konsultasi dengan ahli keamanan dan pemangku kepentingan terkait.

Security Policy Development Life Cycle (SPDLC) adalah serangkaian tahapan yang dirancang untuk membantu organisasi dalam mengembangkan kebijakan keamanan jaringan yang lebih efektif [1]. Berikut adalah 5 tahapan yang ada pada metode SPDLC [2] :

1. Analysis : Pada tahapan ini dilakukan perumusan masalah dan pengumpulan data berupa informasi IDS dalam peningkatan keamanan jaringan dan serangan yang terjadi. Hasil informasi yang di dapatkan dijadikan sebagai landasan dalam pemecehan masalah.
2. Desain : Pada tahapan ini dilakukan perancangan berupa

topologi jaringan yang akan dibangun dan rancangan sistem operasi yang akan digunakan.

3. Implementation : Pada tahapan ini dilakukan implementasi dari rancangan topologi yang sudah dibangun pada tahapan sebelumnya yaitu dengan melakukan instalasi perangkat yang dibutuhkan dan melakukan konfigurasi Software yang diperlukan.
4. Enforcement : Pada tahapan ini akan dilakukan pengujian sistem dimana akan dilakukan pengamatan terhadap sistem yang sudah dibangun dan diterapkan apakah sistem sudah berjalan dengan baik dan benar.
5. Enchancement : Pada tahapan ini dilakukan perbaikan sistem yang telah dibangun meliputi peningkatan fungsional atas komponen dan spesifik dan melakukan pembaruan sistem.

3. Hasil Penelitian

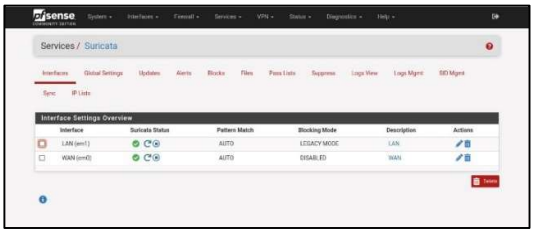
3.1. Konfigurasi

Tahapan awal dari konfigurasi Suricata adalah dengan mengunduh paket Suricata dari repositori paket pfSense. Untuk melakukannya, buka *interface web* pfSense dan navigasikan ke menu "*System*" dan pilih

opsi "*Package Manager*". Cari suricata dalam daftar paket yang tersedia lalu lakukan proses instalasi.

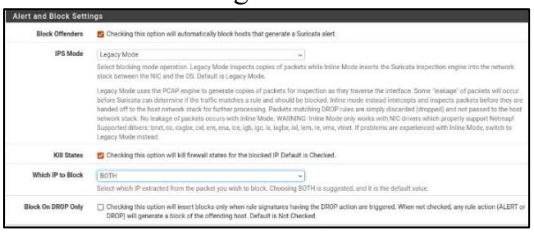
Gambar 2 : Instalasi Suricata pada PfSense

Setelah tahapan instalasi selesai, selanjutnya dilakukan tahapan konfigurasi pengaturan dasar dari IDS Suricata. Pada bagian pfSense pilih menu "*Service*" dimenu utama kemudian pilih opsi "Suricata" untuk membuka *interface* konfigurasinya. Pada bagian ini juga dapat dilakukan konfigurasi *interface* jaringan yang akan dimonitoring oleh Suricata, mengkonfigurasi aturan (*rules*) dan pemilihan mode operasi yang diinginkan misalnya IDS atau IPS.



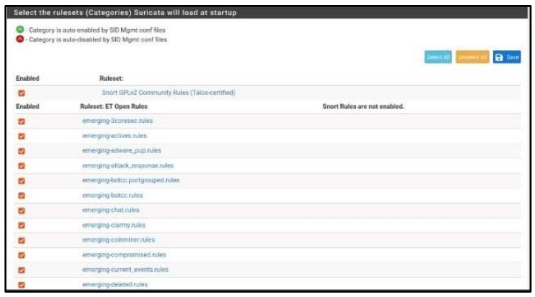
Gambar 3 : Interface Jaringan Suricata pada PfSense

Setelah tahapan pengaturan *interface* jaringan selesai, selanjutnya dilakukan tahapan pengaturan pada bagian "*Global Settings*". Pada bagian "*Alert and Block Settings*", aktifkan "*Block Offenders*" untuk mendeteksi dan memblokir pengguna yang melanggar kebijakan. Dengan mengaktifkan mode ini suricata berada dalam mode IPS, dimana artinya Suricata mampu mendeteksi dan memblokir serangan.



Gambar 4 : Alert dan Block Setting

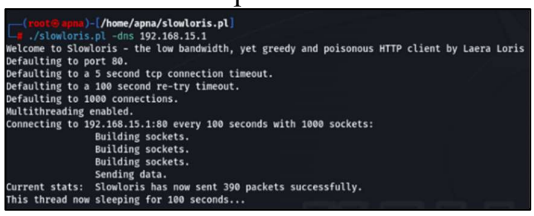
Tahapan selanjutnya adalah melakukan seleksi *rules* yang dibutuhkan. Pilih tab "*Categories*" dan pilih *rules* yang perlu diaktifkan. Selanjutnya pada tab "*Files*" periksa opsi "*Enable Automatic Rule File Updates*" untuk kemudian diaktifkan. Tahapan ini akan memastikan bahwa aturan Suricata diperbarui secara otomatis. Kemudian selanjutnya pilih tab "*Update Rules*" untuk memperbarui aturan Suricata secara manual.



Gambar 5 : Rules Suricata

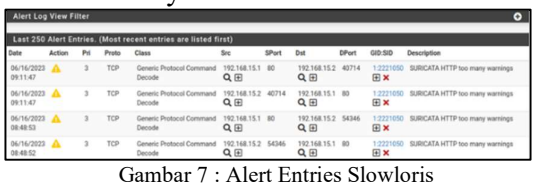
3.2. Pengujian Suricata

Pada bagian ini akan dilakukan evaluasi terhadap kinerja IDS Suricata. Metode evaluasi kinerja IDS yang digunakan berupa pengujian menggunakan metode serangan Slowloris dan Nmap Scan.



Gambar 6 : Serangan Slowloris

Gambar 6 diatas merupakan metode penyerangan slowloris Dalam serangan Slowloris, penyerang menggunakan sejumlah besar koneksi atau klien palsu untuk mengirim permintaan HTTP yang tidak lengkap atau sangat lambat. Permintaan-permintaan tersebut akan mempertahankan koneksi terbuka dengan server dan mengkonsumsi sumber daya yang ada, seperti slot koneksi atau thread pemrosesan. Dengan mempertahankan banyak koneksi terbuka secara simultan, server akhirnya kehabisan sumber daya untuk melayani koneksi baru dari pengguna yang sah, sehingga menyebabkan penurunan kinerja atau bahkan keruntuhan layanan web.

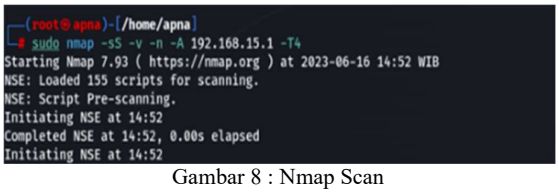


Gambar 7 : Alert Entries Slowloris

Berdasarkan gambar 7 pada tanggal 16 Juni 2023, terjadi beberapa kejadian jaringan yang melibatkan protokol TCP (*Transmission Control Protocol*). Kejadian ini terdeteksi oleh perangkat yang menggunakan program pengendalian Intrusi (*Intrusion Detection System*) bernama SURICATA. Detail kejadian tersebut adalah sebagai berikut:

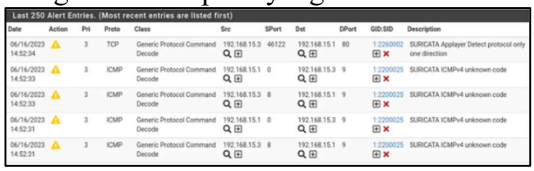
1. Pada pukul 09:11:47, terjadi pertukaran paket antara alamat IP sumber 192.168.15.1 dan alamat IP tujuan 192.168.15.2. Paket tersebut menggunakan protokol TCP dengan nomor port sumber 80 dan nomor *port* tujuan 40714. Dalam analisis lebih lanjut, paket ini diklasifikasikan dengan ID "1:2221050". Pesan yang diberikan adalah "*SURICATA HTTP too many warnings*" yang mengindikasikan adanya banyak peringatan terkait protokol HTTP.
2. Pada pukul 09:11:47, terjadi pertukaran paket lainnya antara alamat IP sumber 192.168.15.2 dan alamat IP tujuan 192.168.15.1. Paket ini juga menggunakan protokol TCP dengan nomor *port* sumber 40714 dan nomor port tujuan 80. Klasifikasi paket dan pesan yang diberikan sama dengan kejadian sebelumnya, yaitu "1:2221050" dan "*SURICATA HTTP too many warnings*".
3. Pada pukul 08:48:53, terjadi pertukaran paket antara alamat IP sumber 192.168.15.1 dan alamat IP tujuan 192.168.15.2. Paket menggunakan protokol TCP dengan nomor *port* sumber 80 dan nomor port tujuan 54346. Dalam analisis lebih lanjut, paket ini diklasifikasikan dengan ID "1:2221050". Pesan yang diberikan adalah "*SURICATA HTTP too many warnings*".
4. Pada pukul 08:48:52, terjadi pertukaran paket lainnya antara alamat IP sumber 192.168.15.2 dan alamat IP tujuan 192.168.15.1. Paket ini juga menggunakan protokol TCP dengan nomor *port* sumber 54346 dan nomor port tujuan 80. Klasifikasi paket dan pesan yang diberikan sama dengan kejadian sebelumnya, yaitu "1:2221050" dan "*SURICATA HTTP too many warnings*".

Pesan "*SURICATA HTTP too many warnings*" menunjukkan bahwa ada banyak peringatan terkait protokol HTTP yang terdeteksi oleh SURICATA pada pertukaran paket-paket tersebut.



Gambar 8 : Nmap Scan

Gambar 8 diatas merupakan pengujian sistem menggunakan metode *Nmap scan*. *Nmap scan* bekerja dengan mengirimkan paket-paket ke *host*-target dalam jaringan dan menganalisis respons yang diterima.

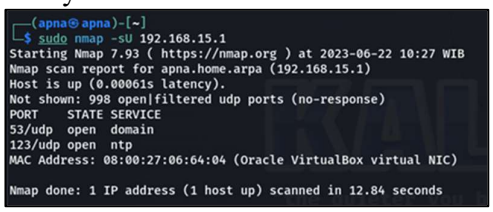


Gambar 9 : Alert Entries Nmap Scan

Berdasarkan gambar 9 dapat dijelaskan bahwa pada tanggal 19 Juni 2023, pukul 09:50:53, terjadi sebuah kejadian jaringan yang melibatkan protokol TCP (*Transmission Control Protocol).* Kejadian ini terdeteksi oleh perangkat yang menggunakan program pengendalian Intrusi SURICATA. Detail kejadian tersebut adalah sebagai berikut:

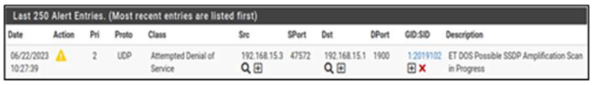
1. Sumber alamat IP (IP address) dari paket yang diterima adalah 192.168.15.3.
2. Paket tersebut memiliki nomor port (port number) 38170.
3. Tujuan alamat IP dari paket adalah 192.168.15.1.
4. Paket ini menggunakan protokol HTTP dengan nomor port 80.
5. Pada analisis lebih lanjut, paket ini diklasifikasikan sebagai "1:2260002" yang mungkin merujuk pada sebuah tanda pengenal atau kategori serangan yang spesifik.

Pesan tambahan yang diberikan adalah "SURICATA *Applayer Detect protocol only one direction*". Pesan ini mengindikasikan bahwa perangkat SURICATA hanya mendeteksi protokol aplikasi pada satu arah saja, artinya kemungkinan ada lalu lintas jaringan yang tidak terdeteksi pada arah lainnya.



Gambar 10 : Serangan DoS

Serangan DoS bertujuan untuk membanjiri sumber daya sistem yang ditargetkan, seperti bandwidth jaringan, kapasitas pemrosesan server, memori, atau sumber daya lainnya. Dengan membebani sistem secara berlebihan, serangan ini dapat menyebabkan kelambatan, kegagalan, atau penolakan akses bagi pengguna yang sah.



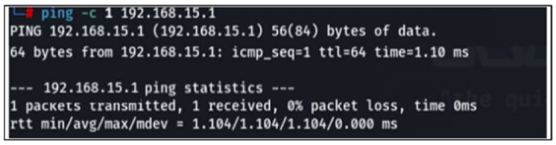
Gambar 11 : Alert Entries DoS

Berdasarkan gambar 11 pada tanggal 22 Juni 2023 pukul 10:27:39, terjadi sebuah kejadian yang tercatat dalam log jaringan. Kejadian tersebut terkait dengan protokol UDP (User Datagram Protocol) dan diklasifikasikan sebagai "Attempted Denial of Service" (Upaya Penolakan Layanan). Informasi lebih lanjut tentang kejadian tersebut adalah sebagai berikut:

1. Sumber IP (IP address) yang mencoba melakukan serangan adalah 192.168.15.3.
2. Port sumber yang digunakan adalah 47572.
3. IP tujuan (destination IP) yang menjadi target adalah 192.168.15.1.
4. Port tujuan yang dituju adalah 1900.
5. ID aturan yang terkait dengan kejadian ini adalah 1:2019102.

Keterangan dari ID aturan tersebut adalah "ET DOS Possible SSDP Amplification Scan in Progress" yang dapat diartikan sebagai kemungkinan adanya pemindaian SSDP (Simple Service Discovery Protocol) yang menggunakan teknik amplifikasi. SSDP adalah protokol jaringan yang digunakan untuk mendeteksi dan menemukan perangkat di dalam jaringan. Amplifikasi adalah teknik yang digunakan oleh penyerang untuk memperbesar ukuran paket yang dikirimkan agar dapat membanjiri sasaran yang rentan, dengan tujuan mengganggu atau menolak akses ke layanan jaringan yang dituju.

Pada kejadian ini, sistem mendeteksi bahwa ada kemungkinan sedang terjadi pemindaian SSDP amplifikasi yang dapat menunjukkan adanya upaya penolakan layanan (Denial of Service) yang sedang dilakukan.



Gambar 12 : Serangan PingFlood

Pada gambar 12 merupakan pengujian dengan serangan pingflood, penyerang mengirimkan sejumlah besar permintaan ping ke alamat IP target secara berulang-ulang. Setiap permintaan ping meminta balasan dari target dengan mengirimkan paket echo request dan menunggu balasan echo reply. Dengan mengirimkan sejumlah besar permintaan ping dalam waktu singkat, penyerang membanjiri kapasitas jaringan target dan membuatnya tidak mampu menangani permintaan secara efisien.

Gambar 13 Alert Entries PingFlood

Berdasarkan gambar 13 pada tanggal 7 Juli 2023. Berikut adalah penjelasan untuk setiap elemen kejadian tersebut:

1. Date: Menunjukkan tanggal kejadian terjadi, dalam format 07/07/2023, yang mewakili tanggal 7 Juli 2023.
2. Pri: Merupakan prioritas kejadian jaringan. Dalam kejadian jaringan diatas skala prioritasnya berada pada level 3
3. Proto: Merupakan singkatan dari "Protocol" (Protokol), dan dalam konteks ini, ICMP (Internet Control Message Protocol) adalah protokol yang digunakan. ICMP digunakan untuk mengirim pesan kendali dan kesalahan dalam jaringan.
4. Class: Menunjukkan kelas kejadian jaringan. Dalam hal ini, kelasnya adalah "Generic" (Umum), yang mungkin menunjukkan bahwa kejadian ini adalah kejadian umum yang tidak secara spesifik terkait dengan satu jenis serangan atau anomali jaringan tertentu.
5. Protocol: Menunjukkan protokol yang digunakan dalam kejadian ini, yaitu ICMP (ICMPv4 dalam konteks ini).
6. Command: Merupakan perintah yang didekode dari paket yang dikirim atau diterima dalam kejadian ini. Dalam informasi yang diberikan, perintahnya tidak ditentukan.
7. Decode: Menunjukkan hasil dekode paket atau pesan jaringan yang terkait dengan kejadian ini. Dalam informasi yang Anda berikan, pesan "SURICATA ICMPv4 unknown code" muncul, yang mungkin menunjukkan bahwa Suricata (sebuah perangkat lunak IDS/IPS) mendeteksi pesan ICMPv4 dengan kode yang tidak dikenal atau tidak valid.
8. Src: Menunjukkan sumber (source) alamat IP dalam kejadian ini. Dalam hal ini, alamat IP sumber adalah 192.168.15.3.
9. Dst: Menunjukkan tujuan (destination) alamat IP dalam kejadian ini. Dalam hal ini, alamat IP tujuan adalah 192.168.15.1.
10. Dport: Merupakan singkatan dari "Destination Port" (Port Tujuan), yang menunjukkan nomor port tujuan yang terkait dengan kejadian ini. Dalam informasi yang diberikan, port tujuan adalah 9. Port 9 umumnya digunakan untuk protokol TFTP (Trivial File Transfer Protocol).
11. GID:SID: Merupakan singkatan dari "Generator ID: Signature ID" (ID Pembangkit: ID Tanda Tangan). GID dan SID digunakan dalam sistem deteksi intrusi (IDS) untuk mengidentifikasi dan mengelompokkan peraturan atau aturan deteksi spesifik. Dalam hal ini, GID adalah 1 dan SID adalah 2200025.

12. Description: Merupakan deskripsi singkat tentang kejadian ini. Dalam informasi yang diberikan, deskripsinya adalah "SURICATA ICMPv4 unknown code", yang menunjukkan bahwa Suricata mendeteksi pesan ICMPv4 dengan kode yang tidak dikenal atau tidak valid.

3.3. Hasil Data Serangan

Setelah melakukan pengujian untuk mengetahui kinerja dari Suricata pada pfSense untuk mengidentifikasi, mendeteksi, dan mengambil Tindakan yang tepat kedepannya. Berdasarkan hasil uji coba yang dilakukan pada jaringan Universitas Muhammadiyah Kalimantan Timur diperoleh data sebagai berikut :

Table 1 : Hasil Data Serangan

Slowloris	
Protokol	TCP
Waktu Serangan (WIB)	08:45
Waktu Notifikasi Diterima	08:48
Waktu Proses (Menit)	3
Nmap Scan	
Protokol	TCP
Waktu Serangan (WIB)	14:52
Waktu Notifikasi Diterima	14:52
Waktu Proses (Menit)	0
Denial of Service (DoS)	
Protokol	UDP
Waktu Serangan (WIB)	10:27
Waktu Notifikasi Diterima	10:27
Waktu Proses (Menit)	0
PingFlood	
Protokol	ICMP
Waktu Serangan (WIB)	16:31
Waktu Notifikasi Diterima	16:31
Waktu Proses (Menit)	0

Pada Tabel 1 adalah hasil pengujian menggunakan metode slowloris dan *Nmap scan* yang diujikan pada jaringan Universitas Muhammadiyah Kalimantan Timur. Berdasarkan hasil uji coba menunjukkan Suricata mampu mendeteksi adanya serangan slowloris dan *Nmap scan* yang artinya suricata bekerja dengan baik mendeteksi serangan pada server.

Berdasarkan pengujian yang dilakukan waktu yang diperlukan suricata untuk mendeteksi serangan slowloris adalah 3 menit sedangkan waktu yang diperlukan suricata untuk mendeteksi *Nmap scan,* DoS, dan *PingFlood* adalah 0 detik (real time). Alert pada suricata bekerja dengan baik dan mengirimkan notifikasi kedalam data base dengan tepat.

4. Kesimpulan

Setelah melakukan hasil dan pembahasan penelitian yang telah dilakukan, maka diperoleh hasil kesimpulan sebagai, berikut;

1. Berdasarkan hasil pengujian yang telah dilakukan IDS Suricata memperoleh hasil yaitu Sistem mampu mendeteksi serangan berupa Slowloris, Nmap scan, DoS, dan PingFlood.
2. IDS Suricata bekerja dengan baik dalam mendeteksi paket-paket ancaman untuk waktu yang dibutuhkan kurang lebih 4 menit tergantung dari koneksi internet yang digunakan.
3. Intrusion Detection System bersifat pasif, Sistem ini hanya akan bekerja jika terjadi serangan saja.

5. Saran

Untuk pengembangan penelitian ini, ada beberapa saran yang dapat diberikan :

1. Penting untuk menganalisis kinerja sistem IDS Suricata dalam skenario yang melibatkan jaringan yang lebih besar dan lebih kompleks. Uji coba yang melibatkan beban lalu lintas yang tinggi dan berbagai jenis serangan akan memberikan wawasan tentang skalabilitas sistem dan bagaimana itu mempengaruhi waktu respons dan kehandalan deteksi.
2. Melakukan perbandingan yang lebih luas antara Suricata dan sistem deteksi intrusi lainnya akan membantu dalam memahami keunggulan dan kelemahan masing-

masing sistem. Ini dapat dilakukan dengan mengimplementasikan beberapa IDS populer dan membandingkan kinerja, akurasi, dan kemudahan penggunaannya. Perbandingan semacam ini akan memberikan wawasan yang berharga dalam memilih dan mengembangkan solusi IDS yang optimal.

6. Daftar Pustaka

[1] J. D. Santoso, "Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," *Infos*, vol. 1, no. 3, pp. 44–50, 2019.

[2] M. Jufri and H. Heryanto, "Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 5, no. 2, pp. 98–108, 2021, doi: 10.35145/joisie.v5i2.1759.

[3] M. A. -, E. I. Alwi, and I. As'ad, "Analisis Forensik Terhadap Serangan Ddos Ping of Death Pada Server," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 1, pp. 23–31, 2022, doi: 10.14421/csecurity.2022.5.1.3423.

[4] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[5] A. Nurhayati, "Monitoring Sistem Keamanan Jaringan Berbasis Telegram Bot Pada Local Area Network," *J. Informatics Commun. Technol.*, vol. 1, no. 2, pp. 45–53, 2020, doi: 10.52661/j_ict.v1i2.41.

[6] G. E. Yogiswara, S. Nita, and N. R. Hidayati, "Aplikasi Sistem Pakar Diagnosa Kegagalan Koneksi TCP / IP Menggunakan Metode Forward Chaining," pp. 453–462, 2022.

[7] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[8] A. V. Mananggel, A. Mewengkang, and A. C. Djamen, "Perancangan Jaringan Komputer Di Smk Menggunakan Cisco Packet Tracer," *Edutik J. Pendidik. Teknol. Inf. dan Komun.*, vol. 1, no. 2, pp. 119–131, 2021, doi: 10.53682/edutik.v1i2.1124.

[9] S. Ramadhani, U. Sultan Syarif Kasim Alamat, J. Koto Kociak Kecamatan Latina Payakumbuh Sumatera Barat, J. H. Soebrantas Kelurahan Simpang Baru No, and K. Tampan, "Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata," *Semin. Nas. Teknol. Inf. Komun. dan Ind.*, vol. 0, no. 0, pp. 308–317, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368

[10] M. A. Anas, Y. Soepriyanto, and Susilaningsih, "PENGEMBANGAN MULTIMEDIA TUTORIAL TOPOLOGI JARINGAN UNTUK SMK KELAS X TEKNIK KOMPUTER DAN JARINGAN Muchammad Azwar Anas, Yerry Soepriyanto, Susilaningsih," *Multimed. Tutor.*, vol. 1, no. 4, pp. 307–314, 2018.

[11] I. P. A. E. Pratama and P. A. Dharmesta, "Implementasi Wireshark Dalam Melakukan Pemantauan Protocol Jaringan (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)," *Mantik Penusa*, vol. 3, no. 1, pp. 94–99, 2019.

[12] A. Saputra, "Implementasi Intrusion Detection System (Ids) Suricata Dan Management Log Elk Stack Untuk Pendeteksian Kegiatan Mining," vol. 22, no. 1, pp. 23–29, 2019.

[13] L. Lukman and M. Suci, "Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache," *Respati*, vol. 15, no. 2, p. 6, 2020, doi: 10.35842/jtir.v15i2.343.

[14] M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 4, pp. 244–247, 2021, doi: 10.32672/jnkti.v4i4.3098.

[15] M. Fakhmi and L. M. Gultom, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis)," *Semin. Nas. Ind. dan Teknol.*, pp. 260–277, 2021.

[16] M. D. S. Antariksa and A. Aranta, "Analisis Jaringan Komputer Local Area Network (LAN) Di Rumah Sakit UNRAM," *J. Begawe Teknol. Inf.*, vol. 3,

no. 2, pp. 201–212, 2022, doi: 10.29303/jbegati.v3i2.748.
[17] J. Buttu, “Analisis Kinerja Jaringan Wlan pada Sekolah Menengah Pertama Negeri 6 Palopo,” *J. Inform. dan Teknol. Komput.*, vol. 01, no. 01, pp. 20–27, 2023.
[18] O. E. S. L. Aprilyano Ekklesia Tangkowit, Verry Ronny Palilingan, “Fakultas teknik pendidikan teknologi informasi dan komunikasi universitas negeri manado 2014,” vol. 1, pp. 69–82, 2021.
[19] M. Syani, “Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps),” *J. Inkofar*, vol. 1, no. 1, pp. 13–20, 2020, doi: 10.46846/jurnalinkofar.v1i1.155.
[20] A. J. Alhasan and N. Surantha, “Evaluation of Data Center Network Security based on Next-Generation Firewall,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 9, pp. 518–525, 2021, doi: 10.14569/IJACSA.2021.0120958.
[21] Adam Dwi Ralianto and S. Cahyono, “Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan,” *Info Kripto*, vol. 15, no. 2, pp. 69–75, 2021, doi: 10.56706/ik.v15i2.10.
[22] H. Alamsyah, R. -, and A. Al Akbar, “Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System,” *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.
[23] E. Stephani, Fitri Nova, and Ervan Asri, “Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server,” *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.
[24] Z. Munawar, M. Kom, and N. I. Putri, “Keamanan Jaringan Komputer Pada Era Big Data,” *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 14–20, 2020.

UMKT
UNIVERSITAS MUHAMMADIYAH
Kalimantan Timur

Kampus 1 : Jl. Ir. H. Juanda, No.15, Samarinda
Kampus 2 : Jl. Pelita, Pesona Mahakam, Samarinda
Telp. 0541-748511 Fax.0541-766832

بسم الله الرحمن الرحيم

SURAT KETERANGAN ARTIKEL PUBLIKASI

Assalamu'alaikum Warahmatullahi wabarakatuh

Saya yang bertanda tangan dibawah ini:

Nama	:	Faldi, S.Kom.,M,Ti
NIDN	:	1121079101
Nama	:	Khaerunnisa Marda Tillah
NIM	:	1911102441070
Fakultas	:	Sains dan Teknologi
Progam Studi	:	Teknik Informatika

Manyatakan bahwa artikel ilmiah yang berjudul "*Network Attack Detection and Prevention Using Instrusion Detection System* (IDS) Suricata" telah di submit pada Media Teknologi Informasi dan Komputer Jurnal.
https://journal.universitasmulia.ac.id/index.php/metik

Demikian surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Warahmatullahi wabarakatuh

Samarinda, 31 Juli 2023

Mahasiswa	Dosen Pembimbing
Khaerunnisa Marda Tillah	Faldi, S.Kom.,M,Ti
NIM. 1911102441070	NIDN. 1121079101