

Penerapan *Snort* Dalam Mendeteksi Penyerangan Pada Sistem Keamanan Jaringan Komputer SMKN 2 Seluma

Ade Manza Putra ¹⁾ Khairil²⁾ Hendri Alamsyah³⁾

¹⁾Mahasiswa Program Studi Informatika Fakultas Ilmu komputer Universitas Dehasen Bengkulu. Indonesia
Alamat: Taba, Kec.Talo Kecil, Kab.Seluma, Prov.Bengkulu

Email: ademanzaputra21@gmail.com

^{2,3)}Dosen Program Studi Informatika Fakultas Ilmu komputer Universitas Dehasen Bengkulu. Indonesia
Email: khairil@unived.ac.id, hendrialamsyah@unived.ac.id

(Received: Juni 2026, Revised: Agustus 2026, Accepiend: Oktober 2026)

Abstract- This research focuses on deploying Snort as an Intrusion Detection System (IDS) to fortify the computer network security at SMK Negeri 2 Seluma, specifically targeting the protection of school servers and network infrastructure. Empirical testing demonstrated that the system successfully detected Ping of Death attacks by identifying anomalous Internet Control Message Protocol (ICMP) traffic, consequently generating high-priority alerts. During malware evaluation, Snort effectively flagged the EICAR Standard Anti-Virus Test File when accessed through PowerShell; however, it failed to recognize the payload when downloaded via a standard web browser. Furthermore, the system successfully identified simulated W32/ProxyBack trojan activity executed via HTTP CONNECT communications using PowerShell, triggering maximum-priority alerts to indicate a critical threat level.

Keywords: Snort, Attack Detection, Network Security, Server, SMKN 2 Seluma.

Intisari- Penelitian ini bertujuan untuk menerapkan snort sebagai sistem deteksi intrusi (Intrusion Detection System) dalam meningkatkan keamanan jaringan komputer di SMK Negeri 2 Seluma, khususnya untuk melindungi server dan infrastruktur jaringan sekolah. Adapun hasil pengujian menunjukkan bahwa snort mampu mendeteksi serangan Ping of Death dengan mengidentifikasi lalu lintas ICMP berukuran tidak normal serta menghasilkan alert dengan tingkat prioritas tinggi. Pada pengujian malware, snort berhasil mendeteksi file uji EICAR Virus Test ketika file diakses melalui PowerShell, namun tidak mendeteksi file tersebut saat diunduh melalui browser. Selain itu, snort juga berhasil mendeteksi aktivitas serangan trojan W32/ProxyBack yang disimulasikan melalui komunikasi HTTP CONNECT dengan PowerShell, dan menghasilkan alert dengan prioritas tertinggi sebagai indikasi ancaman serius.

Kata Kunci: Snort, Deteksi Serangan, Keamanan Jaringan, Server, SMKN 2 Seluma

I. PENDAHULUAN

Dunia teknologi informasi sekarang ini berkembang sangat pesat dan mempengaruhi hampir seluruh aspek kehidupan manusia. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi semua sistem yang berhubungan ataupun tidak dengan sistem informasi itu sendiri seperti perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan. Kemudahan yang diperoleh dalam penggunaan sistem informasi yaitu memudahkan dalam mengelola data serta memudahkan pada saat melakukan evaluasi data berdasarkan kebutuhan.

Dalam menentukan sebuah keamanan agar data dan informasi dapat terjaga dan aman dari tindakan yang tidak berwenang, salah satunya ada serangan dari

luar. Seperti halnya SMK Negeri 2 Seluma merupakan salah satu Sekolah Menengah Kejuruan Negeri yang terdapat di Kabupaten Seluma Provinsi Bengkulu. Pada SMK Negeri 2 Seluma tersebut sudah memiliki akses internet yang digunakan untuk kemudahan mendapatkan informasi dan mengelola data-data sekolah. Provider akses internet yang digunakan di SMK Negeri 2 Seluma yaitu indihome. Selama ini sistem jaringan tersebut belum menerapkan keamanan jaringan untuk menjaga data serta informasi yang berada didalamnya. Berdasarkan perlindungan keamanan data/informasi dalam suatu jaringan, umumnya semua teori keamanan berbasis data dibuat dan diaplikasikan untuk mengamankan suatu jaringan tertentu. Snort merupakan salah satu program Network Intrusion Detection System, yaitu program yang dapat mendeteksi suatu usaha penyusupan pada sistem jaringan komputer.

Penelitian terkait juga dilakukan oleh Purba dan Efendi (2020:1) dengan judul “Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan Snort”. Tujuan dari penelitian ini adalah merancang dan menganalisa sistem keamanan komputer di PT. Promanufacture Indonesia menggunakan perangkat lunak Snort. Adapun hasil dari penelitian ini yaitu pengelola jaringan PT. Promanufacture Indonesia dapat menjaga sistem keamanan jaringan komputer pada perusahaan tersebut, dimana dengan adanya Snort dapat meminimalisir terjadinya serangan dari pihak-pihak yang tidak bertanggung jawab.

Penelitian terkait juga dilakukan oleh Fauzi (2023:1) dengan judul “Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distributed Denial Of Service (DDOS)”. Tujuan penelitian ini yaitu merancang sistem keamanan jaringan komputer berbasis Intrusion Detection System (IDS) menggunakan snort untuk mendeteksi adanya sebuah serangan yang masuk ke dalam jaringan komputer Madrasah Aliyah Negeri Purwakarta seperti Ping icmp, nmap (port scan) dan DDOS. Hasil dari penelitian ini yaitu dengan Teknik IDS pengelola jaringan mendapatkan sebuah notifikasi dan

mencegah serangan tersebut masuk ke dalam jaringan komputer.

II. TINJAUAN PUSTAKA

A. Penerapan

Penerapan adalah suatu perbuatan mempraktekkan suatu teori, metode dan hal lain untuk mencapai tujuan tertentu dan untuk suatu kepentingan yang diinginkan oleh suatu kelompok atau golongan yang telah terencana dan tersusun sebelumnya (Ahmadi & Lisapaly, 2022).

Penerapan adalah kesanggupan seseorang untuk menggunakan ide-ide umum, tata cara ataupun metode-metode, prinsip-prinsip, rumus-rumus, teori-teori dan sebagainya dalam situasi dan konkret (Amaludin, 2021).

Berdasarkan kedua pengertian di atas, dapat disimpulkan bahwa penerapan merupakan suatu tahapan yang akan dilaksanakan sesuai dengan prosedur yang telah disusun secara terperinci, sesuai dengan urutan proses analisa yang telah dilakukan.

B. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan (Sutarti, et al., 2018).

Beberapa alasan untuk memperoleh dan menggunakan IDS (*Intrusion Detection System*), diantaranya adalah :

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab dan hukuman yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem umum pakai seperti *firewall*, sehingga banyak menyebabkan adanya begitu banyak lubang keamanan, seperti:
 - a. Banyak dari *legacy* sistem, sistem operasi tidak *patch* maupun *update*.
 - b. *Patch* tidak diperhatikan dengan baik, sehingga menimbulkan masalah baru dalam hal keamanan.
 - c. *User* yang tidak memahami sistem, sehingga jaringan dan protokol yang mereka gunakan memiliki lubang keamanan.
 - d. *User* dan administrator membuat kesalahan dalam konfigurasi dan dalam menggunakan sistem.
3. Mendeteksi serangan awal, penyerang akan menyerang suatu sistem yang biasanya melakukan langkah-langkah awal yang mudah diketahui yaitu

dengan melakukan penyelidikan atau menguji sistem jaringan yang akan menjadi target, untuk mendapatkan titik-titik dimana mereka akan masuk.

4. Mengamankan *file* yang keluar dari jaringan.
5. Sebagai pengendali untuk rancangan keamanan dan administrator, terutama bagi perusahaan yang pesat.
6. Menyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan diagnosis, *recovery*, dan mengoreksi faktor-faktor penyebab serangan.

Intrusion Detection system (IDS) adalah kemampuan yang dimiliki oleh perangkat keras atau perangkat lunak yang berfungsi untuk mendeteksi aktivitas mencurigakan pada jaringan dan menganalisis dan mencari. Berikut adalah tiga jenis Sistem Deteksi Intrusi (IDS) (Suwaryo, et al., 2021):

Snort

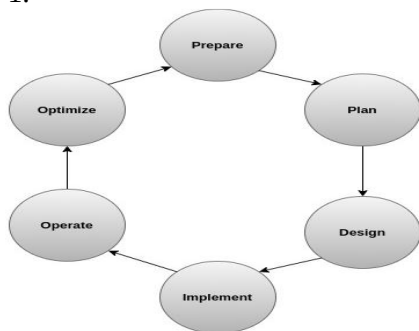
Snort merupakan sistem pencegahan dan deteksi intrusi jaringan bersifat *open source* dengan berbasis aturan (*rule-driven*) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan atau *alert* ketika ancaman terdeteksi. *Snort* merupakan salah satu alat pada IDS dengan komunitas *open source*, sehingga *Snort* merupakan alat yang disukai untuk melindungi keamanan jaringan komputer. Deteksi intrusi adalah proses memantau kejadian yang terjadi di sistem komputer atau jaringan dan menganalisis kemungkinan kejadian. Ada beberapa alasan untuk kejadian tersebut, seperti *malware* (seperti *worm* dan *spyware*) dan penyerang. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam suatu sistem atau jaringan. *Snort* bekerja mirip dengan *TcpDump*, tetapi berfokus pada *sniffing* paket yang aman. Fitur utama yang membedakan *Snort* dari *TcpDump* adalah pemeriksaan muatan. *Snort* menganalisis kumpulan aturan muatan yang disediakan (Gunawan, et al., 2021).

Snort merupakan sebuah aplikasi keamanan jaringan yang berfungsi dalam mendeteksi adanya ancaman dalam jaringan komputer, seperti penyusup, pemindaian, maupun penyerangan. *Snort* merupakan gabungan dari protokol analisis dan pendeteksi penyusupan yang berguna untuk merespon kejadian-kejadian yang sedang terjadi pada jaringan komputer secara *real-time*. *Snort* akan merespon kejadian yang terjadi dalam penyerangan *host-host* jaringan (Purba & Efendi, 2020).

III. METODOLOGI PENELITIAN

Dalam melaksanakan penelitian ini, penulis menggunakan metode PPDIOO yang merupakan sebuah metode perancangan jaringan yang dirancang untuk mendukung berkembangnya jaringan. PPDIOO terdiri dari beberapa tahapan

yaitu *Prieparie, Plan, Dìesign, Impliemient, Opieratie, Optimizie*. Dengan kebutuhan layanan jaringan yang semakin kòmplikèks, maka dipèrlukan suatu mètodiologi yang mèndukung pèrancangan arsitèktur dan dèisain jaringan, sèpierti tèrlihat pada Gambar 1.



Gambar 1. Tahapan Mètodie PPDIOO

Adapun tahapan-tahapan Mètodie PPDIOO tèsiebu, antara lain :

1. *Prieparie Phasie*

Pada tahap ini, mèlakukan pèrsiapan mèmbangun sistèm kèamanan jaringan mènggunakan *Snort*, yaitu mulai mèmpèrsiapkan kèbutuhan, kònsep.

2. *Plan Phasie*

Pada tahap ini dilakukan idèntifikasi hal-hal yang harus dipènuhi bèrdasarkan tujuan, fasilitas dan kèbutuhan pèngguna.

3. *Dìesign Phasie*

Dalam tahap ini, dilakukan dèisain jaringan yang tèrpèrinci yang akan mèmènuhi pèrsyaratan tèknis.

4. *Impliemient Phasie*

Pada fasie ini, dilakukan instalasi dan kònfigurasi yang sèsuai dièngan spèsifikasi dèisain. Dièngan mènginstal *sioftwarie* dan kònfigurasi dan pèmilihan sèrangan yang di uji cioba pada sistèm jaringan kòmputier.

5. *Opieratiònal Phasie*

Fasie opierasiònal adalah mèmpèrtahankan kètahanan kègiatan jaringan, dimana pada fasie ini mèliputi pèngiòlahan kòmponèn jaringan, mèlakukan pèmèliharaan sistèm jaringan, mèngièliola kinèrja jaringan, dan mèngiòrèksi jika ada kèsalahan pada jaringan..

6. *Optimazie Phasie*

Fasie ioptimalisasi administratiòr jaringan mèngidèntifikasi dan mènyèlèsaikan masalah yang sèdang tèrjadi. Kèmungkinan di fasie ioptimalisasi akan dilakukan mòdifikasi dèisain jaringan, jika tèrlalu banyak masalah yang timbul.

V. HASIL DAN PEMBAHASAN

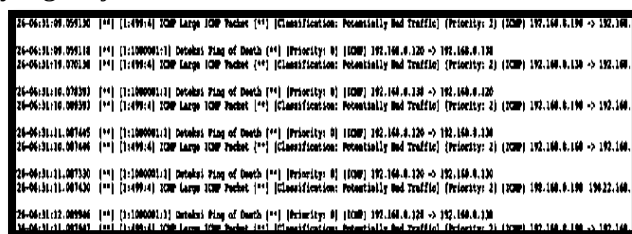
A.Hasil

Pènèrapan *snort* dalam mèndètèksi pènyerangan pada sistèm kèamanan jaringan kòmputier di SMK Nègèri 2 Sèluma dapat mèmbantu mèningkatkan

kèamanan jaringan sèkiòlah, khususnya dalam mèndètèksi pòiènsi sèrangan. Dièngan adanya pènèrapan *snort* sèbagai sistèm dètèksi intrusi, pihak sèkiòlah dapat mèmantau aktivitas jaringan sècara lèbih lèfèktif dan mèncègah gangguan pada jaringan sèkiòlah.

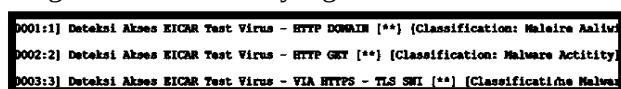
Pènèrapan *snort* dijalankan pada sèbuah laptiòp yang bèrfungsi sèbagai *siervier mionitioring*, mènggunakan sistèm opierasi Linux Ubuntu *Siervier* 24.04.1. Laptiòp ini dilèngkapi dua antarmuka jaringan (dua NIC) yang dikònfigurasi sèbagai bridgè sèhingga sèluruh lalu lintas antara *cliient* dan *siervier* mèlèwati *snort* sècara *rieal timè*.

Hasil dètèksi sèrangan iòlèh *Snort* ditunjukkan pada Gambar, yang mènampìkan infòmisi tèrkait jènis sèrangan, alamat sumbèr dan tujuan, sierta waktu tèrjadinya sèrangan. Hal ini mènununjukkan bahwa *Snort* mampu bèrfungsi sècara lèfèktif dalam mèndètèksi sèrangan *Ping iof Dèath* pada jaringan yang diuji.



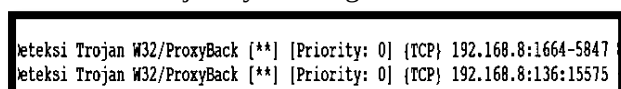
Gambar 2. Hasil Dètèksi Sèrangan *Ping iof Dèath*

Hasil pèngujian mènununjukkan bahwa *Snort* bèrhasil mèndètèksi sèrangan EICAR Virus Tèst kètika filè diaksès mèlalui PìowèrShiell. *Snort* mènghasilkan *liog alièrt* yang bèrisi infòmisi mèngènai aktivitas mèncurigakan, sèbagaimana ditampìkan pada Gambar. Hal ini mèmbuktikan bahwa *Snort* mampu mèndètèksi indikasi malwarè pada lalu lintas jaringan tèrtèntu, tèrutama kètika piola data sèsuai dièngan aturan dètèksi yang dimiliki.



Gambar 3. Hasil Dètèksi sèrangan EICAR Virus Tèst

Hasil pèngujian *Snort* bèrhasil mèndètèksi aktivitas sèrangan tròiòjan W32/PriòxyBack, sèpierti tèrlihat pada Gambar 4.3 dan mènghasilkan *liog alièrt* yang bèrisi infòmisi tèrkait jènis sèrangan, alamat IP sumbèr dan tujuan, pìort yang digunakan, sierta waktu tèrjadinya sèrangan.



Gambar 4. Hasil Dètèksi Sèrangan Tròiòjan W32/Priòxyback



Gambar Kionfigurasi Jaringan

Berdasarkan sistem menggunakan dua *Network Interface Card* (NIC) yang dikonfigurasi melalui pembuatan *bridge* jaringan dengan nama *br0*. Pengalamatan jaringan yang digunakan adalah IPv4 dengan metode *Dynamic Host Configuration Protocol* (DHCP), sehingga alamat IP diperoleh secara otomatis dari server DHCP.

3. Instalasi dan konfigurasi snort

Pada tahap ini dilakukan proses instalasi dan konfigurasi *Snort* sebagai sistem deteksi intrusi. Proses instalasi dilakukan menggunakan perintah dasar Linux, yaitu :

```
apt-get install snort -y
```

Perintah tersebut akan mengunduh dan menginstal semua dependensi yang dibutuhkan oleh *Snort* agar dapat berfungsi dengan optimal. Setelah instalasi selesai, dilakukan konfigurasi dasar *Snort*, meliputi penentuan variabel jaringan seperti *HOME_NET* yang disesuaikan dengan alamat IP, konfigurasi direktori penyimpanan log, serta pengaktifan *rule* dasar untuk mendeteksi berbagai jenis serangan jaringan. Untuk melakukan konfigurasi dasar *snort*, dilakukan melalui perintah :

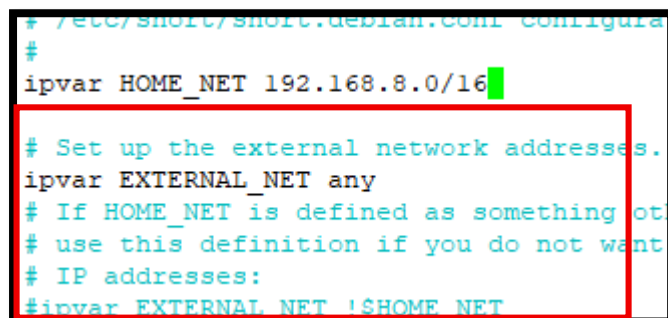
```
nanio /etc/snort/snort.conf
```

Perintah tersebut digunakan untuk membuka konfigurasi dasar *snort*. Setelah perintah itu dijalankan, maka akan menampilkan halaman konfigurasi *snort*



Gambar. Kionfigurasi Snort

Pada konfigurasi *snort* yang dilakukan yaitu mengubah pada bagian *HOME_NET* seperti



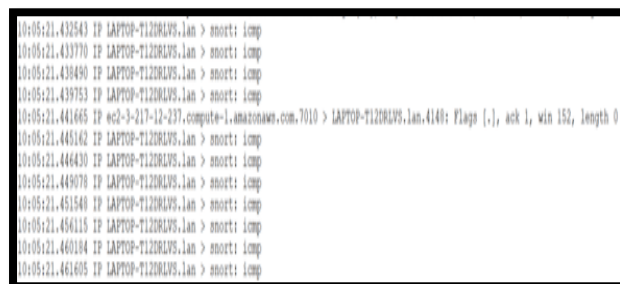
Gambar. HOME_NET

4. Pemantauan Lalu Lintas

Tahap ini bertujuan untuk memverifikasi kemampuan sistem dalam melakukan proses sniffing, yaitu menangkap dan memantau lalu lintas data yang melewati interface bridge (*br0*) pada laptop *monitoring*. Proses verifikasi dilakukan menggunakan perintah:

```
tcpdump -i br0
```

Adapun hasil pemantauan lalu lintas seperti terlihat pada Gambar. Dalam gambar tersebut tampak bahwa interface *br0* berhasil menangkap paket data secara real-time, yang menandakan bahwa proses bridging berjalan dengan baik dan *Snort* telah siap untuk melakukan analisis serta mendeteksi potensi serangan yang terjadi di jaringan



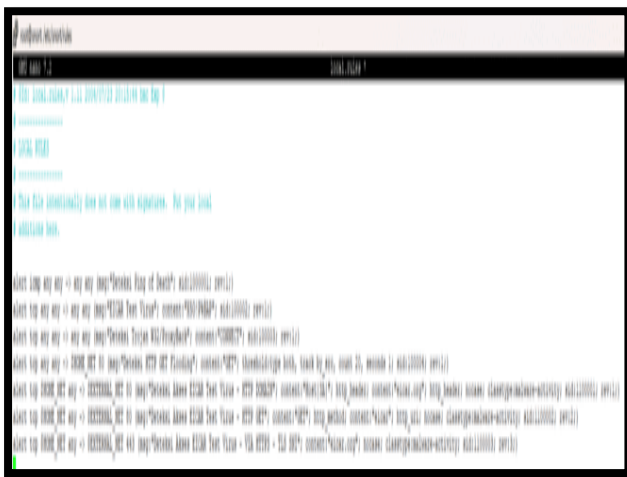
Gambar. Hasil Pemantauan Lalu Lintas

5. Perancangan dan penerapan rule

Pada tahap ini dilakukan perancangan dan penerapan aturan deteksi (*rules*) pada server *Snort* untuk meningkatkan kemampuan identifikasi insiden jaringan yang potensial. Semua aturan lokal dikonsolidasikan dalam satu berkas *local.rules* pada laptop server agar pengelolaan dan pemeliharaan *rule* menjadi lebih sederhana dan terpusat. Perintah yang digunakan untuk membuka *local.rules* tersebut yakni :

```
nanio /etc/snort/rules/local.rules
```

Perintah tersebut digunakan untuk membuka halaman konfigurasi *local.rules* pada *snort*. Setelah perintah tersebut dijalankan, maka akan menampilkan halaman

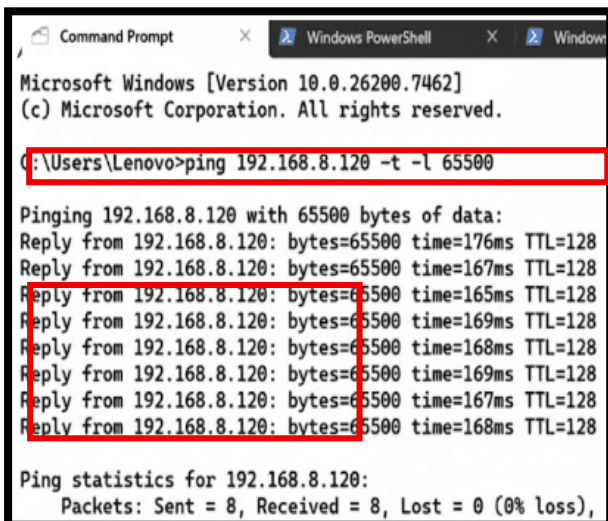
Gambar. File *Rulie*

C. Pengujian Sistem

Pengujian dilakukan untuk mengevaluasi kemampuan *Snort* mendeteksi serangan pada skenario yang sudah ditetapkan. Pengujian ini dilakukan untuk memverifikasi efektivitas *rulie Snort* yang telah dirancang pada tahap sebelumnya. Pengujian dilakukan dari *client* berbasis Windows di lab sekolah. Tiga skenario serangan yang diuji adalah:

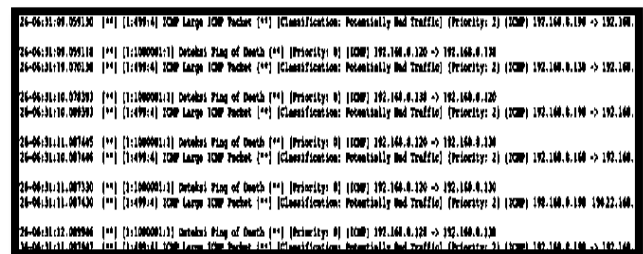
1. Flooding dengan teknik *Ping of Death*

Flooding dengan teknik *Ping of Death* dilakukan menggunakan perintah `ping 192.168.8.120 -t -l 65500`, di mana alamat IP 192.168.8.120 merupakan IP dari laptop Dapodik yang dijadikan sebagai target pengujian. Parameter `-t` digunakan untuk mengirimkan paket ICMP secara terus-menerus, sedangkan parameter `-l 65500` berfungsi untuk mengatur ukuran paket ICMP yang sangat besar. Pengiriman paket berukuran tidak normal ini bertujuan untuk membebani sistem target sehingga berpotensi menyebabkan gangguan layanan jaringan, seperti penurunan performa hingga *system crash*.

Gambar. Serangan *Ping of Death*

Gambar memperlihatkan proses serangan *Ping of Death* yang dilakukan dengan mengirimkan paket ICMP secara berulang dan berukuran besar ke alamat IP target. Serangan ini termasuk dalam kategori *Denial of Service (DoS)* karena berupaya menghabiskan sumber daya sistem dan jaringan pada perangkat target.

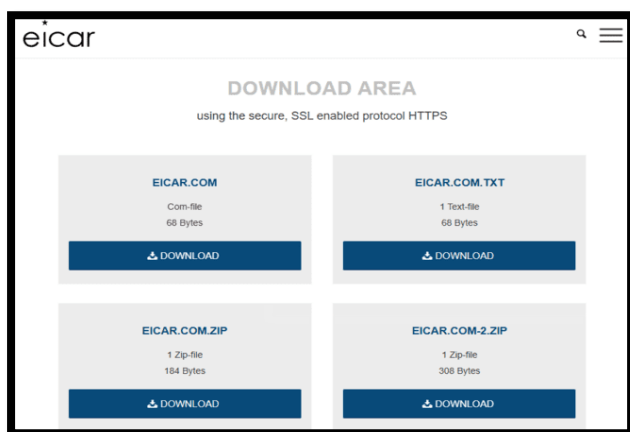
Berdasarkan hasil pengujian tersebut, sistem keamanan jaringan yang menggunakan *Snort* berhasil mendeteksi aktivitas serangan yang terjadi. *Snort* secara otomatis menghasilkan *log alert* sebagai indikasi adanya anomali lalu lintas jaringan. Hasil deteksi serangan oleh *Snort* ditunjukkan pada Gambar yang menampilkan informasi terkait jenis serangan, alamat sumber dan tujuan, serta waktu terjadinya serangan. Hal ini menunjukkan bahwa *Snort* mampu berfungsi secara efektif dalam mendeteksi serangan *Ping of Death* pada jaringan yang diuji.

Gambar. Hasil Deteksi Serangan *Ping Of Death*

Dari Gambar 4.16 tersebut sistem keamanan jaringan mendeteksi adanya aktivitas ICMP yang tidak normal yang diklasifikasikan sebagai *Potentially Bad Traffic*. Alert yang muncul antara lain "ICMP Large ICMP Packet" dan "Deteksi Ping of Death", yang keduanya berkaitan dengan penyalahgunaan protokol ICMP. Dari sisi prioritas, alert *Large ICMP Packet* memiliki *Priority: 2*, yang menandakan ancaman tingkat menengah, sedangkan *Ping of Death* memiliki *Priority: 0*, yang menunjukkan tingkat ancaman tinggi dan perlu perhatian serius.

2. Serangan malware

Serangan malware pada penelitian ini diuji menggunakan EICAR Virus Test, yaitu file uji standar yang umum digunakan untuk mengevaluasi kemampuan sistem keamanan dalam mendeteksi malware tanpa membahayakan sistem. Pengujian dilakukan dengan mengakses situs resmi EICAR dan mengunduh file uji melalui alamat <http://www.eicar.org/eicar.com.txt>, seperti ditunjukkan pada Gambar



Gambar Situs Virus Tiest Eicar

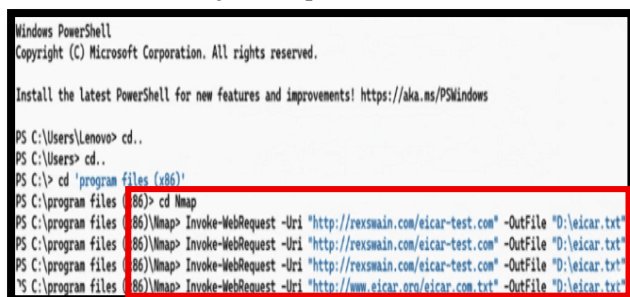
Berdasarkan hasil pengujian, ketika proses pengunduhan file EICAR dilakukan secara langsung melalui browser, sistem Snort tidak mampu mendeteksi aktivitas tersebut dan tidak menghasilkan *log alert* apapun. Hal ini disebabkan karena lalu lintas unduhan melalui browser umumnya menggunakan protokol HTTP dengan mekanisme stream-based, sehingga konten file dikirim dalam beberapa segmen paket kecil. Pada kondisi ini, Snort yang berjalan sebagai Network Intrusion Detection System (NIDS) tidak selalu dapat melakukan inspeksi payload secara utuh.

Oleh karena itu, untuk memastikan kemampuan deteksi Snort terhadap file uji malware EICAR, dilakukan pengujian lanjutan dengan mengakses file tersebut melalui Powershell. Pengujian ini menggunakan perintah:

Invoke-WebRequest -Uri

"http://www.eicar.org/eicar.com.txt" -OutFile
"D:\eicar.txt"

Perintah tersebut memungkinkan pengambilan file secara langsung melalui perintah baris (*command-line*), sehingga payload EICAR dikirim dalam bentuk yang lebih jelas dan mudah dianalisis oleh sistem IDS. Proses akses EICAR menggunakan Powershell ditunjukkan pada Gambar.



Gambar Akses Eicar melalui Powershell

Hasil pengujian menunjukkan bahwa Snort berhasil mendeteksi serangan EICAR Virus Tiest ketika file diakses melalui Powershell. Snort menghasilkan *log alert* yang berisi informasi mengenai aktivitas mencurigakan, sebagaimana ditampilkan pada

Gambar Hal ini membuktikan bahwa Snort mampu mendeteksi indikasi malware pada lalu lintas jaringan tertentu, terutama ketika pola data sesuai dengan aturan deteksi yang dimiliki.

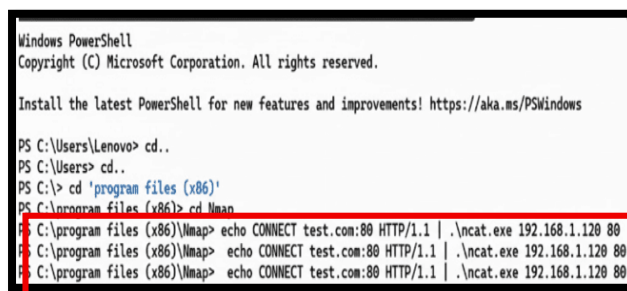
```
0001:1] Deteksi Akses EICAR Test Virus - HTTP DOMAIN [**] [Classification: Malware Activity]
0002:2] Deteksi Akses EICAR Test Virus - HTTP GET [**] [Classification: Malware Activity]
0003:3] Deteksi Akses EICAR Test Virus - VIA HTTPS - TLS SWI [**] [Classification: Malware Activity]
```

Gambar. Hasil Deteksi Serangan Virus Eicar Tiest

Dari Gambar. tersebut sistem keamanan jaringan berhasil mengidentifikasi adanya akses terhadap EICAR Tiest Virus, yang merupakan file uji standar internasional untuk menguji efektivitas antivirus dan Intrusion Detection System (IDS). Deteksi ini bukan malware berbahaya, melainkan simulasi yang sengaja dibuat untuk memastikan bahwa mekanisme deteksi keamanan berjalan dengan baik. Alert pertama menunjukkan Deteksi Akses EICAR Tiest Virus melalui HTTP Domain, yang berarti terdapat percobaan akses file EICAR menggunakan protokol HTTP berdasarkan nama domain tujuan. Alert kedua menunjukkan Deteksi Akses EICAR Tiest Virus melalui metode HTTP GET, yang menandakan bahwa klien di jaringan melakukan permintaan langsung (GET request) untuk mengunduh file EICAR melalui HTTP.

3. Pengujian serangan trojan W32/ProxyBack
Pengujian serangan trojan W32/ProxyBack dilakukan untuk mengetahui kemampuan sistem Snort dalam mendeteksi aktivitas berbahaya yang memanfaatkan koneksi jaringan sebagai *proxy backdoor*. Serangan ini disimulasikan menggunakan Powershell dengan memanfaatkan utilitas *netcat* (*ncat.exe*) untuk membangun koneksi jaringan secara tidak sah ke sistem target. Perintah yang digunakan pada pengujian ini adalah:

```
echo CONNECT test.com:80 HTTP/1.1 |  
.\ncat.exe 192.168.1.120 80
```



Gambar. Serangan Trojan

Perintah tersebut bertujuan untuk mengirimkan permintaan koneksi HTTP CONNECT ke alamat tujuan melalui port 80 pada IP 192.168.1.120, yang disimulasikan sebagai server target. Pola komunikasi ini menyerupai karakteristik trojan W32/ProxyBack, di mana sistem yang terinfeksi dapat berfungsi sebagai *proxy* untuk meneruskan

lalu lintas jaringan penyierang tanpa sepengetahuan pengguna.

Melalui pengujian ini, Snort melakukan pemantauan terhadap lalu lintas jaringan yang melewati sistem. Aktivitas pengiriman perintah CONNECT yang tidak lazim teridentifikasi sebagai lalu lintas mencurigakan karena menyimpang dari pola komunikasi HTTP normal. Snort kemudian mencicokkan paket jaringan tersebut dengan aturan (*rule*) yang berkaitan dengan aktivitas *trojan* atau *backdoor*.

Berdasarkan hasil pengujian, Snort berhasil mendeteksi aktivitas serangan trojan W32/ProxyBack, seperti terlihat pada Gambar 4.20 dan menghasilkan *log alert* yang berisi informasi terkait jenis serangan, alamat IP sumber dan tujuan, port yang digunakan, serta waktu terjadinya serangan.

```
Deteksi Trojan W32/ProxyBack [**] [Priority: 0] {TCP} 192.168.8.1664-5847
Deteksi Trojan W32/ProxyBack [**] [Priority: 0] {TCP} 192.168.8.136:15575
```

Gambar. Hasil Deteksi Serangan Trojan W32/ProxyBack

Dari Gambar, sistem keamanan jaringan mendeteksi adanya aktivitas yang mengindikasikan Trojan W32/ProxyBack pada jaringan internal. Trojan W32/ProxyBack merupakan jenis malware pada sistem operasi Windows yang berfungsi sebagai backdoor dan memungkinkan komputer yang terinfeksi digunakan sebagai proxy oleh pihak tidak bertanggung jawab. Alert ini memiliki Priority: 0, yang menandakan tingkat ancaman tertinggi pada sistem Snort. Artinya, aktivitas yang terdeteksi bukan sekedar lalu lintas normal atau percobaan pemindaian ringan, melainkan ancaman serius yang perlu segera ditindaklanjuti. Protokol yang digunakan adalah TCP, yang umumnya dimanfaatkan malware untuk membangun koneksi yang stabil. Alamat IP sumber yang terdeteksi berasal dari 192.168.8.x, yaitu alamat IP lokal, sehingga dapat disimpulkan bahwa sumber aktivitas mencurigakan tersebut berasal dari dalam jaringan sendiri.

Tabel 1. Hasil Pengujian Sistem

Pengujian	Skenario Pengujian	Hasil Pengujian
Deteksi serangan flooding pada server di sekolah	Pengujian dilakukan dengan mensimulasikan serangan <i>Ping of Death</i> menggunakan perintah <code>ping -t -l 65500</code> ke alamat IP server/laptop Dapodik di jaringan sekolah untuk membanjiri lalu lintas ICMP secara terus-menerus.	Snort berhasil mendeteksi aktivitas flooding dan menghasilkan <i>alert</i> yang menunjukkan adanya anomali lalu lintas ICMP berukuran tidak normal, sehingga serangan dapat diidentifikasi dengan baik.
Deteksi serangan malware	Pengujian dilakukan dengan mensimulasikan komunikasi trojan	Snort berhasil mendeteksi pola lalu lintas jaringan

trojan W32/ProxyBack dari luar	W32/ProxyBack menggunakan <i>Powershell</i> dan <i>netcat</i> (<code>ncat.exe</code>) untuk mengirimkan permintaan koneksi HTTP CONNECT ke server target melalui port 80 dari luar jaringan.	mencurigakan yang menyiratkan aktivitas trojan atau <i>backdoor</i> , serta menampilkan <i>log alert</i> berisi informasi sumber, tujuan, dan jenis serangan.
Deteksi serangan virus icar	Pengujian dilakukan dengan mengunduh file uji EICAR melalui dua metode, yaitu melalui browser dan melalui <i>Powershell</i> menggunakan perintah <code>Invoke-WebRequest</code> untuk membandingkan kemampuan deteksi Snort.	Snort tidak mendeteksi file EICAR saat diunduh melalui browser, namun berhasil mendeteksi dan menghasilkan <i>alert</i> ketika file diaksis melalui <i>Powershell</i> , menunjukkan bahwa deteksi dipengaruhi oleh metode akses dan aturan yang digunakan.

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil dan pembahasan serta pengujian, maka dapat disimpulkan bahwa :

1. Penerapan *snort* dalam mendeteksi penyierangan pada sistem keamanan jaringan komputer di SMK Negeri 2 Seluma dapat membantu meningkatkan keamanan jaringan sekolah. Dengan adanya penerapan *snort* sebagai sistem deteksi intrusi, pihak sekolah dapat memantau aktivitas jaringan secara lebih efektif.
2. Snort diimplementasikan pada sebuah laptop yang berfungsi sebagai server monitoring dengan sistem operasi Linux Ubuntu Server 24.04.1. Perangkat ini menggunakan dua antarmuka jaringan (*dual NIC*) yang dikonfigurasi dalam mode bridge, sehingga seluruh lalu lintas data antara client dan server dapat dianalisis oleh Snort secara *real time* tanpa mengganggu komunikasi jaringan yang berjalan.
3. Berdasarkan hasil pengujian sistem pada tiga skenario serangan, yaitu serangan flooding (Ping of Death), serangan malware menggunakan EICAR virus test, dan serangan trojan W32/ProxyBack, dapat disimpulkan bahwa Snort mampu mendeteksi sebagian besar serangan sesuai dengan *rule* yang diterapkan. Snort berhasil mendeteksi serangan flooding dan trojan W32/ProxyBack, serta mendeteksi file EICAR ketika diakses melalui *Powershell*, namun tidak mendeteksi file EICAR saat diunduh melalui browser. Hal ini menunjukkan bahwa kemampuan deteksi Snort dipengaruhi oleh metode akses, pola lalu lintas

jaringan, serta konfigurasi dan kelengkapan *rule* yang digunakan.

B. Saran

Berdasarkan kesimpulan, maka penulis menyarankan agar :

1. Snort disarankan untuk diterapkan sebagai sistem pendeteksi keamanan jaringan komputer di lingkungan sekolah dari serangan jaringan seperti flooding dan aktivitas malware berbasis komunikasi jaringan.
2. Perlu dilakukan pemeliharaan rutin terhadap *rule* Snort, pembaruan konfigurasi, dan *monitoring* secara berkala agar sistem deteksi tetap efektif menghadapi pola serangan yang terus berkembang, serta menggunakan sistem deteksi seperti suricata.

DAFTAR PUSTAKA

- [1] Ahmadi & Lisapaly, D. C., 2022. *Efektivitas Penerapan Pembelajaran Daring Di Tengah Badai Covid-19*. Bandung: Penerbit Media Sains Indonesia.
- [2] Amaludin, L., 2021. *Model Pembelajaran Problem Based Learning Penerapan dan Pengaruhnya Terhadap Keterampilan Berpikir Kritis dan Hasil Belajar*. Tangerang: Pascal Bioiks.
- [3] Amien, J. A. & Mukhtar, H., 2020. *Implementasi Jaringan Komputer*. Yogyakarta: Penerbit Deepublish.
- [4] Anggraini, M. A. N., 2018. Uji Fitur Intrusion Prevention Pada Firewall Untangle Dengan Pengujian DOS dan SSH Bruteforce. *Jurnal Manajemen Informatika*, Volume 10.1.
- [5] Anggrawan, A., 2018. *Algoritma dan Programan Implementasi Pada VB.Net dan Java*. Pertama penyunt. Yogyakarta: Andi Publisher.
- [6] Dar, M. H. & Harahap, S. Z., 2018. Implementasi Snort Intrusion Detection System (IDS) Pada Sistem Jaringan Komputer. *Jurnal Informatika*, Volume 10.6 No.3 e-ISSN:2615-1855.
- [7] Fauzi, R., Muhyidin, Y. & Singasatia, D., 2023. Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distributed Denial Of Service (DDoS). *Jurnal Sains Komputer dan Informatika*, Volume 10.7 No.1 e-ISSN:2549-7200.
- [8] Gunawan, A. R., Sastra, N. P. & Wiharta, D. M., 2021. Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan HoneyPot Sebagai Pendeteksi dan Pencegah Malware. *Majalah Ilmiah Teknologi Elektro*, Volume 10.20. No.1 e-ISSN:2503-2372.
- [9] Hiendry, 2018. Implementasi Samba Server Untuk Mendukung Sharing Printer di SD Swasta Al-Washliyah 6/39 Medan. *Jurnal Ilmiah Ciorie IT*, Volume 10.6 No.1 e-ISSN:2548-3528.
- [10] Purba, W. W. & Efiendi, R., 2020. Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan Snort. *Aiti Jurnal Teknologi Informasi*, Volume 10.17 No.2 e-ISSN:2615-7128.
- [11] Putra, P. P., 2016. Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) Untuk Mendeteksi Serangan Nmap. *Jurnal Satin (Sains dan Teknologi Informasi)*, Volume 10.2 No.1.
- [12] Simargiolang, M. Y., Widarma, A. & Irawan, M. D., 2021. *Jaringan Komputer*. Medan: Yayasan Kita Menulis.
- [13] Surianti, Haryani, P. & Kusumaningsih, R., 2020. Desain Jaringan Menggunakan Model Virtual Local Area Network (VLAN) Di Kampus II Institut Sains dan Teknologi Akrapind Yogyakarta. *Jurnal Jarkom*, Volume 10.8 No.2 e-ISSN:2338-6304.
- [14] Sutarti, Pancaro, A. P. & Saputra, F. I., 2018. Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikoesal. *Jurnal Prosisko*, Volume 10.5 No.1 e-ISSN:2597-9922.
- [15] Suwaryo, N., Nawangsih, I. & Riejeki, S., 2021. Deteksi Serangan Pada Intrusion Detection System (IDS) Untuk Klasifikasi Serangan Dengan Algoritma Naive Bayes, C4.5 dan K-NN Dalam Minimisasi Resiko Terhadap Pengguna. *Jurnal Sistem Informasi*, Volume 10.1 ISSN.2541-3228.
- [16] Wicaksono, S. R., 2019. *Jaringan Komputer Konsep dan Studi Kasus*. Pertama penyunt. Malang Jawa Timur: CV. Sribu Bintang.