**Journal of Applied Informatics and Computing (JAIC)**
Vol.8, No.2, December 2024, pp. 326~331
e-ISSN: 2548-6861 

# Implementation of IDS and IPS for Detecting and Preventing TCP Port Scanning and ICMP Flooding Attacks

**Iqbal Maqdum Razzanda [1]*, Muhammad Koprawi [2]***
* Teknik Komputer, Universitas Amikom Yogyakarta
iqbalmr.528@students.amikom.ac.id [1], koprawi@amikom.ac.id [2]

**Article Info**

***Article history:***

Received 2024-07-06
Revised 2024-07-19
Accepted 2024-08-12

***Keyword:***

*IDS,*
*IPS,*
*TCP Port Scanning,*
*ICMP Flooding,*
*Telegram.*

**ABSTRACT**

The implementation of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) is a crucial step in maintaining network security. This research aims to test the effectiveness of IDS and IPS in detecting and preventing TCP port scanning attacks and ICMP flooding attacks and also providing real-time notifications using Telegram. The methodology used includes configuring a test environment that reflects real network scenarios, where various attacks are initiated to test the IDS and IPS responses. The experimental results show that IDS is able to detect suspicious activity with a high degree of accuracy, while IPS is effective in blocking identified attacks, thereby reducing potential damage to the system. Proper implementation of IDS and IPS can significantly improve network security by early detecting and preventing cyberattacks.



## I. PENDAHULUAN

Intrusion Detection System (IDS) merupakan suatu perangkat lunak atau aplikasi yang dapat digunakan untuk mendeteksi aktivitas berbahaya dan kerentanan di seluruh jaringan. Tujuan IDS adalah untuk memantau aktivitas terkait aplikasi, yaitu lalu lintas masuk dan keluar, dan untuk memantau ancaman atau serangan yang berasal dari jaringan lain [1]. Sistem Deteksi Intrusi (IDS) mengambil peran utama dalam mendeteksi dan memantau serangan siber eksternal dan internal melalui semua teknologi internet. Namun, seiring dengan peningkatan pesat data di internet setiap tahunnya, beberapa intrusi tingkat lanjut dan tidak diketahui juga meningkat secara dramatis. Oleh karena itu, tugas sistem deteksi intrusi akan menjadi lebih menantang menghadapi masalah keamanan saat ini [2].

Sistem Pencegahan Intrusi (IPS) telah dikenal luas sebagai alat yang ampuh dan elemen penting IT sebagai salah satu perlindungan keamanan. IPS adalah perangkat yang memiliki kemampuan untuk mendeteksi serangan, baik yang diketahui maupun tidak, serta cara mencegahnya agar serangan gagal masuk. Teknologi IPS dibedakan dari teknologi IDS berdasarkan satu karakteristik. IPS dapat merespons ancaman yang terdeteksi dengan berupaya mencegahnya agar tidak berhasil. IPS juga dapat beroperasi pada tingkat jaringan atau host dan dapat digunakan untuk melindungi terhadap berbagai macam serangan, termasuk serangan penolakan layanan (DoS), buffer overflows, dan serangan injeksi SQL. IPS juga diklasifikasikan menjadi tiga jenis utama: IPS berbasis jaringan (NIPS), IPS berbasis host (HIPS), dan IPS Hibrid (HIPS/NIPS). Perbedaan utama antara IDS dan IPS adalah IDS dirancang untuk mendeteksi dan memperingatkan aktivitas mencurigakan, sedangkan IPS dapat mendeteksi dan juga mencegah serangan secara real-time. Selain mendeteksi potensi ancaman keamanan, IPS juga dapat mengambil tindakan segera untuk mencegah atau memblokir ancaman tersebut, seperti memblokir lalu lintas, mengakhiri, atau mengatur ulang koneksi [3].

Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) adalah teknologi keamanan yang memantau lalu lintas jaringan atau aktivitas host untuk mencari tanda-tanda akses tidak sah atau aktivitas jahat. IDS biasanya terdiri dari beberapa komponen yang bekerja sama untuk memantau, menganalisis, dan merespons potensi ancaman keamanan atau pelanggaran dalam jaringan atau sistem. Mereka secara umum dapat diklasifikasikan menjadi tiga jenis utama: IDS berbasis jaringan (NIDS), IDS berbasis host (HIDS), dan IDS Hibrida (HIDS/NIDS). NIDS memantau lalu lintas jaringan untuk mencari tanda-tanda aktivitas jahat, sementara HIDS memantau aktivitas host untuk mencari tanda-tanda upaya

intrusi. Pentingnya IDS dan IPS dalam keamanan jaringan tidak dapat dipandang sebelah mata. Dengan semakin canggihnya ancaman dari dunia maya, penting bagi suatu Lembaga atau organisasi untuk menerapkan langkah-langkah keamanan yang efektif untuk melindungi jaringan dan data mereka. Peretas dan penjahat cyber terus-menerus mengembangkan teknik dan alat baru untuk menembus sistem keamanan yang sifatnya tradisional/terdahulu, sehingga penting bagi suatu Lembaga atau organisasi untuk memiliki teknologi keamanan canggih seperti IDS dan IPS [4].

Akhir-akhir ini penggunaan internet, jumlah data penting, data sensitif, rahasia baik individu maupun perusahaan yang melewati internet semakin bertambah. Dengan adanya celah dalam sistem keamanan, penyerang berusaha menyusup ke jaringan, sehingga mendapatkan akses ke informasi penting dan rahasia, yang dapat membahayakan pengoperasian sistem, dan juga mempengaruhi kerahasiaan data [5]. Untuk mengatasi kemungkinan serangan ini, sistem deteksi intrusi (IDS), yang merupakan cabang penting dari keamanan siber, digunakan untuk memantau dan menganalisis lalu lintas jaringan sehingga dapat mendeteksi dan melaporkan aktivitas berbahaya [6].

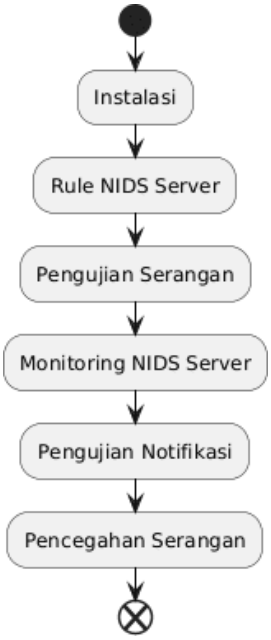
Menempatkan seorang administrator jaringan adalah tindakan pencegahan yang umum dilakukan. Karena membutuhkan waktu, administrator tidak dapat melakukan pengawasan tanpa henti. Masalah tersebut dapat diatasi dengan sistem deteksi ancaman atau gangguan jaringan (NIDS). Sistem ini merupakan suatu teknik yang dapat digunakan sebagai pemantau lalu lintas masuk dan keluar serta lalu lintas bagian jaringan lokal atau biasa disebut lalu lintas antar host [7]. Sistem deteksi intrusi jaringan (NIDS) dapat terdiri dari perangkat keras atau sensor dan perangkat lunak atau konsol untuk mengontrol dan memantau paket lalu lintas jaringan di beberapa lokasi untuk potensi intrusi atau anomali.

Aplikasi Telegram dipilih sebagai metode untuk menerima notifikasi dalam penelitian ini. Ini disebabkan oleh fakta bahwa aplikasi Telegram memiliki fitur bot telegram dengan fitur Application Programming Interface (API), yang memungkinkan pengguna untuk menjalankan proses otomatisasi pada sistem. Selain itu, bot telegram sebagai suatu media aplikasi tambahan memiliki berbagai fungsi unik dan pengguna dapat menggunakannya untuk mengirimkan perintah dalam format yang berbeda. Oleh karena itu, administrator jaringan yang menggunakan smartphone Android dapat mengoptimalkan notifikasi pemantauan NIDS dengan menggunakan bot telegram ini.

Penelitian ini menjelaskan langkah-langkah yang diperlukan untuk mengimplementasikan IDS dan IPS di lingkungan jaringan komputer, termasuk memilih perangkat keras dan perangkat lunak yang sesuai. Selain itu, kami akan menjelaskan proses mengintegrasikan notifikasi Telegram ke dalam sistem keamanan ini. Dengan menganalisis keamanan jaringan komputer, tujuan penelitian ini adalah memahami bagaimana teknologi IDS dan IPS bekerja sama untuk melindungi jaringan, dan bagaimana penggunaan notifikasi Telegram dapat meningkatkan respons terhadap potensi ancaman. Kami berharap penelitian ini akan memberikan panduan yang berguna bagi para profesional keamanan jaringan dan administrator sistem dalam menjaga keamanan dan integritas jaringan komputer.

## II. METODE PENELITIAN

Metode pada penelitian ini menggunakan metode eksperimen. Adapun alur penelitian yang digunakan untuk membimbing dalam menyelesaikan masalah penelitian. Berbagai langkah yang dapat diuraikan sebagai berikut.




Gambar 1. Alur Penelitian

Dengan merujuk pada alur penelitian diatas, dapat dijelaskan sebagai berikut.

*1) Instalasi*: Langkah pertama dalam implementasi Network Intrusion Detection System (NIDS) adalah instalasi. Pada tahap ini, perangkat lunak NIDS (seperti Snort) diinstal pada server yang akan digunakan untuk memonitor jaringan.

*2) Pembuatan Rule NIDS Server*: Setelah instalasi selesai, langkah berikutnya adalah pembuatan rule (aturan) untuk NIDS. Rules ini digunakan untuk menentukan pola atau tanda-tanda serangan yang harus dideteksi oleh NIDS.

*3) Pengujian Serangan*: Tahap berikutnya adalah pengujian serangan. Ini adalah langkah untuk memastikan bahwa IDS dapat mendeteksi aktivitas yang mencurigakan. Adapun rancangan pengujian yang dapat dilihat pada Tabel I.

TABEL I
RANCANGAN PENGUJIAN SERANGAN

| No | Jenis Serangan | Parameter | Kriteria |
|---|---|---|---|
| 1 | TCP Port Scanning | Scan Type | Pemantauan NIDS Server |
| | | Port Range | Notifikasi Bot Telegram |
| 2 | ICMP Flooding | Packet Size | Pemantauan NIDS Server |
| | | Ping Count | Notifikasi Bot Telegram |

*4) Monitoring NIDS Server*: Setelah pengujian scanning, langkah berikutnya adalah monitoring NIDS server secara terus-menerus. Monitoring ini penting untuk memastikan bahwa NIDS berfungsi dengan baik dan mendeteksi ancaman secara real- time.

*5) Pengujian Notifikasi*: Selanjutnya adalah pengujian notifikasi. Sistem NIDS biasanya dilengkapi dengan fitur notifikasi untuk memberi tahu administrator tentang potensi ancaman atau serangan dengan menggunakan bot telegram.

*6) Pencegahan Serangan*: Langkah terakhir adalah pencegahan serangan. Untuk mencegah serangan jaringan dengan menggunakan Snort sebagai Intrusion Prevention System (IPS).

Dalam menunjang penelitian ini, ada beberapa komponen terdiri dari perangkat keras dan dan perangkat lunak. Laptop merupakan perangkat keras yang digunakan pada penelitian ini dan perangkat lunak yang digunakan yaitu sistem operasi linux.

Intrusion Detection System atau IDS merupakan kerangka kerja yang berfungsi memfilter lalu lintas pada jaringan untuk mengenali berbagai aktivitas yang mencurigakan [8]. IDS berfungsi untuk memantau dan menganalisis lalu lintas jaringan atau sistem, kemudian memberikan peringatan jika ditemukan ancaman atau aktivitas yang tidak biasa. Terdapat dua jenis utama IDS:

- Network-based IDS (NIDS): Memantau lalu lintas jaringan untuk mendeteksi serangan. NIDS ditempatkan pada berbagai titik strategis dalam jaringan untuk dilakukan analisis lalu lintas yang masuk dan keluar.
- Host-based IDS (HIDS): Memantau aktivitas pada perangkat atau host individual. HIDS beroperasi dengan cara memeriksa log sistem, log aplikasi, dan file sistem untuk mendeteksi aktivitas yang mencurigakan [9].

Intrusion Prevention System atau IPS merupakan alat keamanan jaringan yang dirancang untuk mendeteksi dan mencegah potensi ancaman dan aktivitas berbahaya. Alat ini berfungsi dengan memantau lalu lintas jaringan untuk mengetahui perilaku yang mencurigakan, menganalisis data, dan mengambil Tindakan proaktif untuk menghentikan ancaman secara real-time. Dalam penelitian alat yang digunakan untuk melakukan IPS yaitu Iptables [10].

Snort sebagai NIDS adalah program intrusi dan penginderaan jaringan sumber terbuka (IDS/IPS). Snort adalah yang paling banyak digunakan sebagai teknologi IDS/IPS di dunia dan menyatukan manfaat protokol, tanda tangan, dan spesifikasi berdasarkan pengecualian. Alat ini adalah IDPS (Sistem Deteksi dan Pencegahan Intrusi) yang menggunakan serangkaian aturan/kebijakan yang membantu menguraikan atau menggambarkan aktivitas jaringan berbahaya dan manfaatkan aturan/kebijakan. tersebut untuk menemukan paket yang tidak cocok dan membuat peringatan bagi pengguna. Pengguna telah menulis aturan/kebijakan ini dalam file teks yang terkait dengan file snort.conf yaitu tempat semua konfigurasi snort ditempatkan. Untuk menjalankan Snort, ada beberapa perintah yang dapat dilakukan untuk memeriksa perilaku jaringan [11].

Telegram tidak hanya menyediakan fitur untuk chatting online tetapi juga dapat digunakan untuk membuat alat yang dipersonalisasi dengan bantuan platform bot. Bot Telegram dapat di program sehingga memiliki fungsi tertentu yang beroperasi secara otomatis sebagai respons terhadap perintah atau permintaan pengguna [12]. Pengoperasian chatbot pada Aplikasi Telegram melibatkan pengguna yang memasukkan perintah relevan dan nantinya bot secara otomatis akan memberikan tanggapan berdasarkan database yang ada. Jika perintahnya tidak sesuai, bot tidak akan mengirimkan respon apa pun [13].

Nmap atau Network Mapper merupakan tool open source yang digunakan untuk melakukan analisis dan eksplorasi pada keamanan jaringan. Alat tersebut dirancang untuk memeriksa secara cepat jaringan besar dan dapat bekerja dengan host tunggal. Dengan memakai paket IP raw, Nmap dapat mengidentifikasi berbagai karakteristik, termasuk berbagai host yang tersedia pada jaringan, layanan dengan nama aplikasi dan versinya, sistem operasi dengan versinya, jenis firewall/filter paket yang digunakan, dan lain sebagainya. Banyak administrator jaringan dan sistem yang menganggap Nmap dapat digunakan untuk tugas biasa seperti melacak uptime host atau layanan, mengelola jadwal upgrade layanan, dan menyimpan inventori jaringan, meskipun Nmap pada umumnya digunakan untuk melakukan proses audit keamanan [14].

TCP Port Scanning adalah teknik mendasar dalam keamanan jaringan, yang digunakan untuk mengidentifikasi port dan services yang terbuka. Setiap metode pemindaian memiliki kelebihan dan kekurangannya, tergantung pada kemampuan, kecepatan dan deteksi yang diperlukan. Dengan menggunakan alat seperti Nmap, para profesional keamanan jaringan bisa melakukan pemindaian ini untuk memastikan keamanan jaringan dan mengidentifikasi potensi kerentanan [15].

ICMP (Internet Control Message Protocol) flooding adalah jenis serangan Denial of Service (DoS) yang di mana penyerang membanjiri korban dengan paket ICMP Echo Request (ping). Tujuannya adalah membanjiri jaringan atau server target dengan lalu lintas ICMP yang sangat banyak sehingga server tersebut menjadi kewalahan, yang

mengakibatkan penurunan kinerja atau tidak tersedianya layanan yang ditargetkan [16].

## III. HASIL DAN PEMBAHASAN

### A. *Konfigurasi Sistem*

1) Instalasi Snort : Melakukan instalasi snort dengan script code $ sudo apt-get install snort yang dapat dilihat pada gambar 2.

```
iqbalmr@iqbalmr-VirtualBox:~$ sudo apt-get install snort
[sudo] password for iqbalmr:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.20-0+deb11u1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 88 not upgraded.
```

Gambar 2. Instalasi Snort

2) Pembuatan Rule NIDS Server: Pembuatan rule Network Intrusion Detection System (NIDS) adalah proses menciptakan aturan yang memungkinkan sistem untuk mendeteksi dan merespon terhadap aktivitas jaringan yang mencurigakan atau berbahaya [17]. Melakukan pembuatan rule berfungsi untuk memunculkan notifikasi serangan yang dideteksi snort dan bot telegram dengan script berikut.

```
Alert icmp any any -> $HOME_NET any (msg:"ICMP Test"; sid:10000016; rev:1; classtype:icmp-event;)

Alert tcp any any -> $HOME_NET any (msg:"TCP Port Scanning"; detection_filter:track by_src, count 30, seconds 60; sid:1000006; rev:2;)
```

Dari script code diatas dapat dijelaskan setiap rule atau parameter yang dapat dilihat pada Tabel II.

TABEL II
RULES

| Rule | Penjelasan |
|---|---|
| 'alert' | menunjukkan bahwa rule ini akan menghasilkan sebuah peringatan jika kondisi terpenuhi. |
| 'tcp' | menunjukkan bahwa rule ini hanya berlaku untuk paket TCP. |
| 'any any' | menunjukkan bahwa rule ini berlaku untuk paket TCP dari semua alamat IP dan port sumber. |
| '$HOME_NET' | any menunjukkan bahwa rule ini berlaku untuk paket TCP yang menuju ke alamat IP dalam variabel '$HOME_NET' pada semua port tujuan. |
| 'msg: "TCP Port Scanning"' | menyediakan pesan yang akan ditampilkan jika aturan ini aktif dan pesannya adalah "TCP Port Scanning". |
| 'detection_filter' | menunjukkan bahwa filter deteksi diterapkan. |
| 'track by_src' | menunjukkan bahwa filter ini akan melacak berdasarkan alamat IP sumber. |
| 'count 30' | menunjukkan bahwa jika 30 atau lebih percobaan koneksi TCP dari alamat IP sumber yang sama terjadi dalam jangka waktu yang ditentukan aturan ini akan aktif. |
| 'seconds 60' | menunjukkan bahwa jangka waktu yang dipantau adalah 60 detik. |
| 'sid' | identifier unik untuk aturan ini, dalam hal ini 'sid' adalah 1000006. |
| 'rev' | menunjukkan revisi dari aturan ini, dalam hal ini revisi dari aturan ini adalah 2. |

3) Instalasi Iptables IPS: Instalasi Iptables dengan script code $ sudo apt-get install iptables yang dapat dilihat pada gambar 3.

```
iqbalmr@iqbalmr-VirtualBox:~$ sudo apt-get install iptables
[sudo] password for iqbalmr:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 126 not upgraded.
```

Gambar 3. Instalasi Iptables

### B. *Pengujian*

Port Scanning adalah teknik yang digunakan untuk menemukan layanan jaringan yang tersedia pada mesin atau perangkat dengan memeriksa status port Transmission Control Protocol (TCP) [18].

```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 12:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:42:48:01 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

Gambar 4. Scan Type

Pada pengujian serangan ini menggunakan dua parameter yaitu scan type dan port range. Tool yang digunakan dalam pengujian ini adalah Nmap yang dilakukan kepada alamat Ip 192.168.56.101 dan diperoleh port yang terbuka 80/tcp.

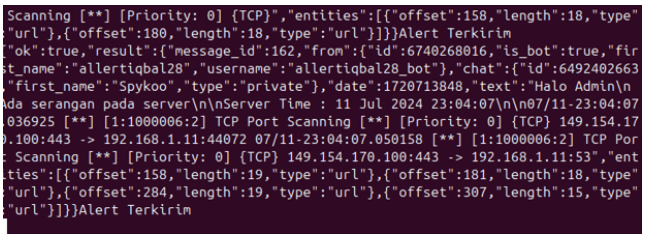
```
┌──(root㉿kali)-[~]
└─# nmap -p 80 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 12:13 EDT
Nmap scan report for 192.168.56.101 (192.168.56.101)
Host is up (0.0012s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

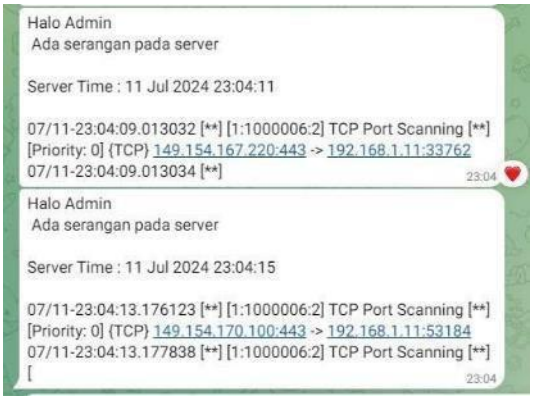
Gambar 5. Port Range

Monitoring NIDS Server: Setelah melakukan pengujian TCP Port Scanning dilakukan pada laptop penyerang, server NIDS dapat digunakan untuk memantau serangan tersebut dengan cara menjalankan script bot telegram pada server NIDS dan hasilnya dapat dilihat pada gambar 6.




Gambar 6. NIDS Server

Pengujian Notifikasi melalui Bot Telegram: Selain dapat memonitoring NIDS Server, notifikasi serangan juga secara otomatis akan terkirim pada telegram bot yang sudah dikonfigurasi sebelumnya, hasilnya dapat dilihat pada gambar 7.




Gambar 7. Notifikasi Serangan TCP Port Scanning

Dari pengujian serangan TCP Port Scanning yang telah dilakukan didapatkan hasil yang dapat dilihat pada Tabel III.

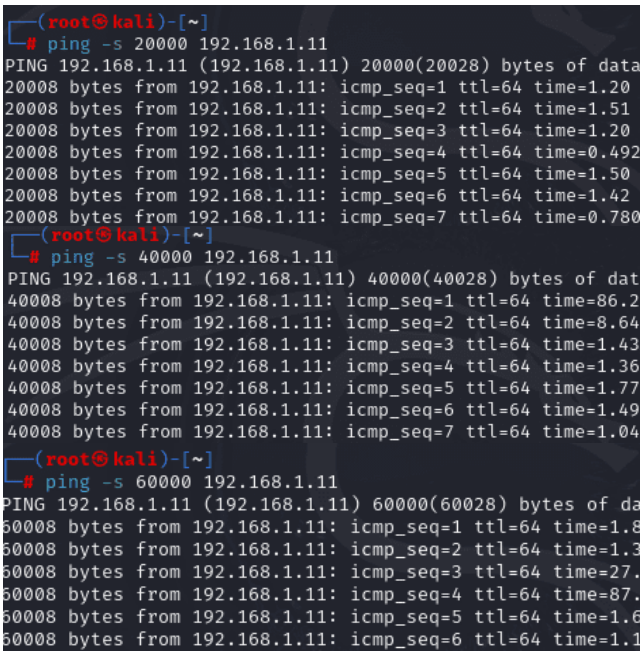
TABEL III
TCP PORT SCANNING

| Parameter | Respon Snort | Respon Telegram |
|---|---|---|
| Scan Type | Berhasil | Berhasil |
| Port Range | Berhasil | Berhasil |

Pengujian ICMP Flooding atau yang biasa disebut ping of death ini bertujuan untuk membanjiri lalu lintas jaringan dengan byte tinggi, pada pengujian serangan ini akan menggunakan dua parameter yaitu packet size dan ping count.

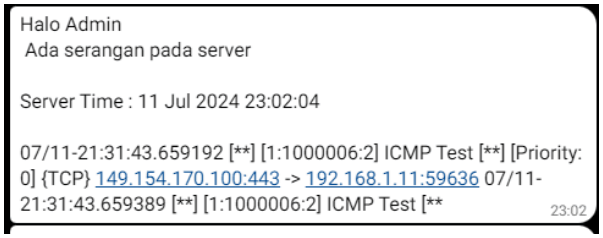
Pada gambar 8 melakukan penyerangan ICMP Flooding menggunakan parameter packet size atau mengirimkan packet dengan bytes yang tinggi. Mengirimkan packet dengan bytes tinggi berfungsi untuk menguji kinerja dan kapasitas jaringan.

Perintah ‘ping’ digunakan untuk melakukan pengujian ping count jaringan antar perangkat [19]. Perintah ini mengirimkan paket ICMP Echo Request dan didapatkan dari hasil ping menunjukkan bahwa perangkat dengan alamat IP 192.168.1.11 merespon dengan paket ICMP Echo Reply.




Gambar 8. Packet Size 20000, 40000, 60000 bytes

Notifikasi Bot Telegram: Melakukan pengecekan pada notifikasi bot telegram ketika terjadi serangan ICMP flooding dapat dilihat pada gambar 9.




Gambar 9. Notifikasi Serangan ICMP flooding

Monitoring NIDS Server: Setelah melakukan pengujian serangan ICMP flooding, server NIDS dapat memantau serangan serangan tersebut yang dapat dilihat pada gambar 10.


Gambar 10. Monitoring NIDS Server

Dari pengujian serangan ICMP Flooding yang sudah dilakukan didapatkan hasil yang dapat dilihat pada Tabel IV.

TABEL IV
PENGUJIAN ICMP FLOODING

| Parameter | Snort | Notifikasi Telegram |
|---|---|---|
| Scan Type 20000 bytes | Berhasil | Berhasil |
| Scan Type 40000 bytes | Berhasil | Berhasil |
| Scan Type 60000 bytes | Berhasil | Berhasil |
| Ping Count | Berhasil | Berhasil |

*C. Pencegahan Serangan Jaringan*

Mencegah serangan TCP Port Scanning: Serangan TCP Port Scanning dapat diatasi menggunakan Iptables dengan perintah:

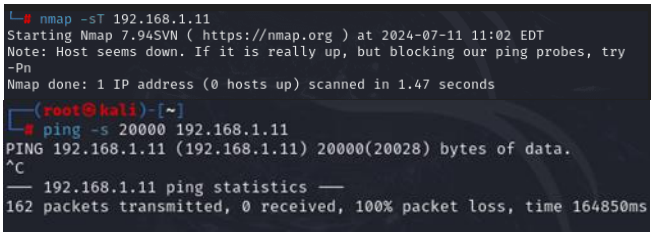
```
$sudo apt iptables -A INPUT -p tcp –dport 80 -m
state –state NEW -m recent --set.
```

Kemudian dilakukan penyerangan lagi dan hasilnya adalah host sedang tidak aktif atau host memblokir probe ping.

Mencegah serangan ICMP Flooding: ICMP Flooding yang terjadi pada gambar 7, 8, dan 9 dapat diatasi menggunakan Iptables dengan perintah:

```
iptables -A INPUT -p icmp – icmp-type echo-
request -j DROP
```

Kemudian dilakukan penyerangan lagi dan hasilnya dapat dilihat pada gambar berikut.




Gambar 14. Hasil Pencegahan

Dari gambar diatas, hasilnya adalah tidak ada paket yang diterima atau 100 % packet loss setelah mengirimkan 162 packet.

## V. KESIMPULAN

Dari penelitian yang telah dilakukan, dapat ditarik kesimpulan bahwa Network Intrusion Detection System (NIDS) menggunakan snort terbukti mampu bekerja efektif sebagai pemberi peringatan pada serangan TCP Port Scanning dan ICMP flooding. Selain itu, sistem notifikasi menggunakan bot telegram juga terbukti dapat menerima notifikasi serangan secara real-time. Pada penelitian ini juga telah dibuktikan bahwa system Iptables yang dirancang efektif dalam pencegahan serangan TCP Port scanning dan ICMP Flooding. Oleh karena itu, hasil pengujian menunjukkan bahwa kedua sistem tersebut mampu memberikan pertahanan yang kuat terhadap serangan-serangan tersebut terutama pada ICMP Flooding. Karena ICMP Flooding hanya mengirimkan serangan dalam paket banyak dan menyerang melalui protocol bukan masuk ke port, IDS dan IPS adalah solusi yang efektif untuk menghadapi serangan tersebut.

## DAFTAR PUSTAKA


[1] C. Anilkumar, D. Paul Joseph, V. Madhu Viswanatham, A. Karrothu, and B. Venkatesh, “Experimental and comparative analysis of packet sniffing tools,” in Proceedings of the 2nd International Conference on Data Engineering and Communication Technology: ICDECT 2017, Springer, 2019, pp. 597–605.

[2] S. Ennaji, N. El Akkad, and K. Haddouch, “A powerful ensemble learning approach for improving network intrusion detection system (nids),” in 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), IEEE, 2021, pp. 1–6.

[3] H. Kılıç, N. S. Katal, and A. A. Selçuk, “Evasion techniques efficiency over the ips/ids technology,” in 2019 4th International Conference on Computer Science and Engineering (UBMK), IEEE, 2019, pp. 542–547.

[4] D. E. Kurniawan, H. Arif, N. Nelmiawati, A. H. Tohari, and M. Fani, “Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator,” in Journal of Physics: Conference Series, IOP Publishing, 2019, p. 012031.

[5] D. Ghelani, “Cyber security, cyber threats, implications and future perspectives: A Review,” Authorea Preprints, 2022.

[6] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, “A systematic literature review for network intrusion detection system (IDS),” Int J Inf Secur, vol. 22, no. 5, pp. 1125–1162, 2023.

[7] L. Ashiku and C. Dagli, “Network intrusion detection system using deep learning,” Procedia Comput Sci, vol. 185, pp. 239–247, 2021.

[8] P. S. Fat, K. Khairil, and E. P. Rohmawan, “Design and Implementation of Intrusion Detection System (IDS) for Wireless Local Area Network (WLAN) Security at SMKN 5 Bengkulu City,” Jurnal Media Computer Science, vol. 2, no. 1, pp. 1–8, 2023.

[9] S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T. M. Ghazal, and S. Sakib, “A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis,” Journal of Engineering, vol. 2024, no. 1, p. 3909173, 2024.

[10] P. F. De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, “An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform,” IEEE Access, vol. 9, pp. 166855–166869, 2021.

[11] G. Jain, “Application of snort and wireshark in network traffic analysis,” in IOP Conference Series: Materials Science and Engineering, IOP Publishing, 2021, p. 012007.

[12] B. Pasaribu and W. Susanti, “Sistem Informasi Pengajuan Rancangan Usulan Penelitian Menggunakan PHP Native dan Bot Telegram,” Jurnal Mahasiswa Aplikasi Teknologi Komputer dan Informasi (JMApTeKsi), vol. 3, no. 1, pp. 29–38, 2021.

[13] D. E. Kurniawan, M. Iqbal, J. Friadi, R. I. Borman, and R. Rinaldi, “Smart monitoring temperature and humidity of the room server using raspberry pi and whatsapp notifications,” in Journal of Physics: Conference Series, IOP Publishing, 2019, p. 012006.

[14] S. Liao et al., “A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments,” in 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2020, pp. 64–71. doi: 10.1109/CyberC49757.2020.00020.

[15] F. H. Roslan, “A Comparative Performance of Port Scanning Techniques,” Journal of Soft Computing and Data Mining, vol. 4, no. 2, pp. 43–51, 2023.

[16] W. Yunus and M. E. Lasulika, “Security system analysis against flood attacks using tcp, udp, and icmp protocols on mikrotik routers,” International Journal of Advances in Data and Information Systems, vol. 3, no. 1, pp. 11–19, 2022.

[17] İ. Gündoüdu and A. A. Selçuk, “Effectiveness analysis of public rule sets used in snort intrusion detection system,” in 2021 29th Signal Processing and Communications Applications Conference (SIU), IEEE, 2021, pp. 1–4.

[18] C. Yuan, J. Du, M. Yue, and T. Ma, “The design of large scale IP address and port scanning tool,” Sensors, vol. 20, no. 16, p. 4423, 2020.

[19] F. H. M. B. Lima, L. F. M. Vieira, M. A. M. Vieira, A. B. Vieira, and J. A. M. Nacif, “Water ping: ICMP for the internet of underwater things,” Computer Networks, vol. 152, pp. 54–63, 2019.