The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 4, August 2024
https://doi.org/10.33022/ijcs.v13i4.4212

Implementasi IDS dan IPS terhadap Serangan *TCP Port Scanning* dan ICMP *Flooding*

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

Informasi Artikel

Diterima : 28 Jun 2024
Direview : 16 Jul 2024
Disetujui : 8 Agu 2024

Kata Kunci

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

Abstrak

Implementasi Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) merupakan langkah penting dalam menjaga keamanan jaringan. Penelitian ini bertujuan untuk menguji efektivitas IDS dan IPS untuk mendeteksi dan mencegah serangan TCP Port Scanning dan serangan ICMP Flooding serta memberikan notifikasi secara real-time dengan menggunakan Telegram. Metodologi yang digunakan termasuk mengkonfigurasi lingkungan pengujian yang mencerminkan skenario jaringan nyata, di mana berbagai serangan diinisiasi untuk menguji respon IDS dan IPS. Hasil percobaan menunjukkan bahwa IDS mampu mendeteksi aktivitas yang mencurigakan dengan tingkat akurasi yang tinggi, sedangkan IPS efektif dalam memblokir serangan yang teridentifikasi, sehingga mengurangi potensi kerusakan pada sistem. Implementasi IDS dan IPS yang tepat dapat secara signifikan meningkatkan keamanan jaringan dengan mendeteksi dan mencegah serangan siber .

Keywords

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.

A. Pendahuluan

Intrusion Detection System (IDS) merupakan suatu aplikasi atau perangkat lunak yang dapat dipakai untuk mendeteksi kerentanan serta berbagai aktivitas yang berbahaya 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 terbentuk melalui beberapa komponen yang saling bekerja sama untuk memantau, menganalisis, dan merespons potensi ancaman keamanan atau pelanggaran dalam jaringan atau sistem. Mereka pada umumnya 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, dan dipakai untuk memantau serta 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 bisa membuat pengguna dapat 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.

Berdasarkan penelitian yang dilakukan Shah dkk., (2021) trafik protokol ICMP lebih mudah dikenali sehingga rule filtering yang diterapkan pada firewall secara otomatis mendrop paket flood tersebut. Hanya saja dalam penelitian ini belum dikembangkan Sistem Filtering yang memfilter protokol-protokol yang dapat menyebabkan serangan flood selain TCP, UDP, dan ICMP sehingga untuk meningkatkan Kinerja Firewall Berbasis Filtering ini dibutuhkan sistem monitoring serangan flood yang lain seperti IDS dan IPS [8]. Selain itu, pada penelitian Abuswhereb dkk., (2020) yang mempelajari mengenai berbagai serangan DOS penting didapatkan hasil bahwasannya sensitifitas serangan terbesar dipegang oleh TCP-SYN dengan serangan jenis SYN yang paling bertanggung jawab atas 79,70% dari semua serangan DoS pada jaringan sehingga apabila dilakukan penelitian yang dapat mendeteksi serangan TCP-SYN nantinya akan sangat berguna di masa mendatang oleh karena itu dibutuhkan sistem monitoring seperti IDS dan IPS untuk mendeteksi serangan tersebut [9]. Hal ini didukung oleh penelitian Roslan (2023) yang mengemukakan bahwa alat terbaik untuk melakukan pemindaian port menggunakan teknik scan TCP SYN dan scan TCP Connect adalah Nmap. Teknik pemindaian port yang terbaik adalah pemindaian TCP SYN karena memiliki waktu respons paling rendah dan dengan demikian paling tidak berdampak pada host target. Pemindaian TCP SYN juga dikenal sebagai teknik pemindaian port yang paling tersembunyi [10].

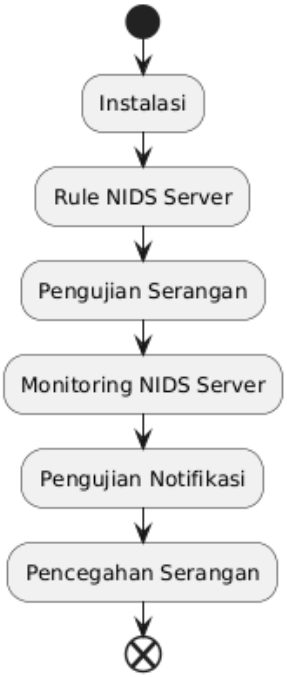
Pada penelitian ini akan di bahas prosedur yang diperlukan untuk menginstal IDS dan IPS pada jaringan komputer beserta saran mengenai pemilihan perangkat lunak dan perangkat keras yang dapat digunakan. Kemudian dibahas cara

memasukkan notifikasi menggunakan Telegram ke dalam sistem IDS. Penelitian ini bertujuan untuk mengetahui bagaimana cara teknologi IDS dan IPS bekerja sama dalam melindungi jaringan dan penggunaan notifikasi pada Telegram dapat meningkatkan respon terhadap kemungkinan ancaman dengan memeriksa keamanan jaringan komputer. Selain itu, pada penelitian ini diharapkan dapat menjadi panduan untuk membantu administrator sistem dan pakar keamanan jaringan dalam menjaga keamanan jaringan komputer.

B. Metode Penelitian

1. Alur Penelitian

Metode yang digunakan pada penelitian ini adalah metode eksperimen. Pemecahan masalah pada penelitian kali ini berpedoman pada alur penelitian. Uraian langkah penelitian dapat dilihat pada gambar berikut.



Gambar 1. Alur Penelitian

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

a. 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.
b. 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.
c. 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 1.

Tabel 1. Rancangan Pengujian Serangan

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

d. 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*.
e. 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.
f. Pencegahan Serangan
   Langkah terakhir adalah pencegahan serangan. Untuk mencegah serangan jaringan dengan menggunakan Iptables sebagai *Intrusion Prevention System* (IPS)

2. Intrusion Detection System

Intrusion Detection System atau IDS merupakan kerangka kerja yang memiliki fungsi memfilter lalu lintas pada jaringan untuk mengenali berbagai aktivitas yang mencurigakan [11]. 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:

a. 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.
b. 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 berbagai aktivitas mencurigakan [12].

3. Intrusion Prevention System

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 [13].

4. Snort

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 [14].

5. Telegram

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 [15]. 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 [16] .

6. Nmap

Nmap atau Network Mapper merupakan tool open source yang berguna 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 ada pada jaringan, layanan dengan nama aplikasi beserta versinya, sistem operasi dengan versinya, pemakaian jenis firewall/filter paket, 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 [17].

7. TCP Port Scanning

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 [18].

8. ICMP Flooding

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 [19].

C. Hasil dan Pembahasan

1. Konfigurasi Sistem

Pada tahapan ini akan dijelaskan langkah-langkah dimulai dari proses instalasi hingga konfigurasi yang diperlukan dalam penelitian ini.

a. Instalasi Snort

Melakukan instalasi Snort menggunakan konfigurasi $ 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

b. Pembuatan *Rule* NIDS Server

Pembuatan *rule Network Intrusion Detection System* (NIDS) merupakan proses menciptakan aturan yang memungkinkan sistem dapat mendeteksi dan merespon terhadap aktivitas jaringan yang mencurigakan atau berbahaya [20]. Melakukan pembuatan *rule* memilki fungsi untuk menampilkan notifikasi serangan yang akan dideteksi oleh snort dan bot telegram menggunakan *script code* seperti dibawah ini :

```
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 sebagai berikut :

a. 'alert' menunjukkan bahwa *rule* ini akan menghasilkan sebuah peringatan jika kondisi terpenuhi.
b. 'tcp' menunjukkan bahwa *rule* ini hanya berlaku untuk paket TCP.
c. 'any any' menunjukkan bahwa *rule* ini berlaku untuk paket TCP dari semua alamat IP dan port sumber.
d. '$HOME_NET' any menunjukkan bahwa *rule* ini berlaku untuk paket TCP yang menuju ke alamat IP dalam variabel '$HOME_NET' pada semua port tujuan.

e. ‘msg : “TCP Port Scanning”’ menyediakan pesan yang akan ditampilkan jika aturan ini aktif dan pesannya adalah “TCP Port Scanning”.
f. ‘detection_filter’ menunjukkan bahwa filter deteksi diterapkan.
g. ‘track by_src’ menunjukkan bahwa filter ini akan melacak berdasarkan alamat IP sumber.
h. ‘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.
i. ‘seconds 60’ menunjukkan bahwa jangka waktu yang dipantau adalah 60 detik.
j. ‘sid’ adalah *identifier* unik untuk aturan ini, dalam hal ini ‘sid’ adalah 1000006.
k. ‘rev’ menunjukkan revisi dari aturan ini, dalam hal ini revisi dari aturan ini adalah 2.

c. Instalasi Iptables IPS

Instalasi Iptables dengan script code $ sudo apt-get install iptables ditunjukkan 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

2. Pengujian Serangan TCP Port Scanning

a. Pengujian TCP Port Scanning

Port Scanning adalah teknik yang digunakan untuk menemukan layanan jaringan yang tersedia pada mesin atau perangkat dengan memeriksa status port Transmission Control Protocol (TCP) [21]. 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 -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 disabl
ed. 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

```
┌──(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

b. Monitoring NIDS Server

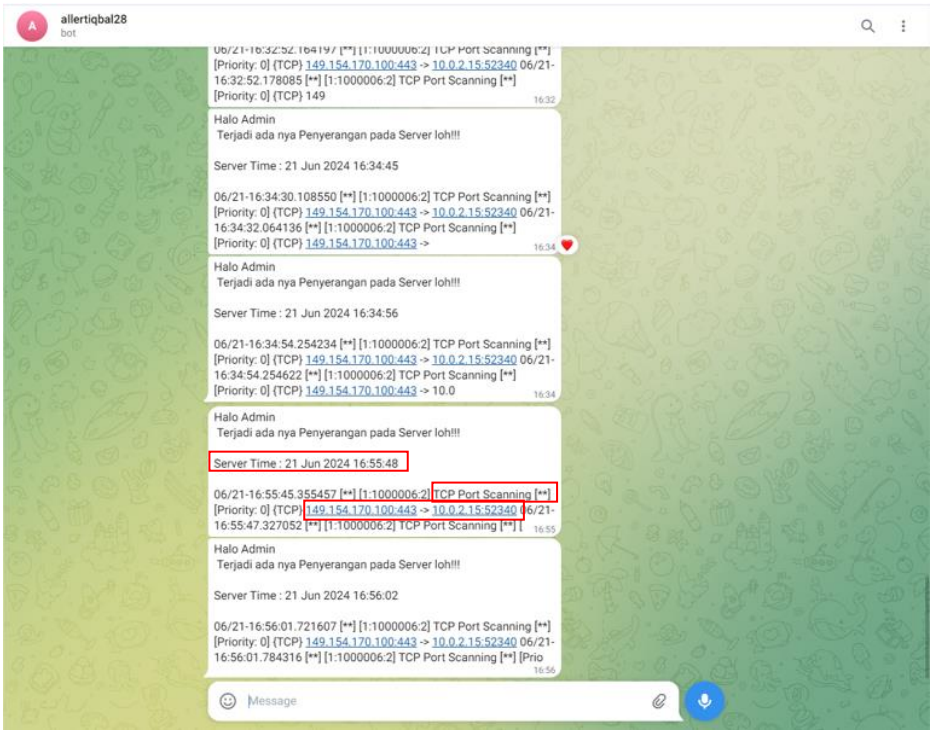
Setelah melakukan pengujian TCP Port Scanning dilakukan pada laptop penyerang, server NIDS dapat digunakan untuk memantau serangan tersebut dengan cara menjalankan script bot telegram pada server NIDS dan hasilnya ditunjukkan pada Gambar 6.

```
iqbalmr@iqbalmr-VirtualBox:~$ ./bot-tele.sh
{"ok":true,"result":{"message_id":101,"from":{"id":6740268016,"is_bot":true,"first_name":"allertiqbal28","username":"allertiqb
l28_bot"},"chat":{"id":6492402663,"first_name":"Spykoo","type":"private"},"date":1718963749,"text":"Halo Admin\n Terjadi ada
ya Penyerangan pada Server loh!!!\n\nServer Time : 21 Jun 2024 16:55:48\n\n06/21-16:55:45.355457 [**] [1:1000006:2] TCP Port
canning [**] [Priority: 0] {TCP} 149.154.170.100:443 -> 10.0.2.15:52340 06/21-16:55:47.327052 [**] [1:1000006:2] TCP Port Sca
ning [**] [","entities":[{"offset":180,"length":19,"type":"url"},{"offset":203,"length":15,"type":"url"}]}}Alert Terkirim
{"ok":true,"result":{"message_id":102,"from":{"id":6740268016,"is_bot":true,"first_name":"allertiqbal28","username":"allertiqb
al28_bot"},"chat":{"id":6492402663,"first_name":"Spykoo","type":"private"},"date":1718963763,"text":"Halo Admin\n Terjadi ada
nya Penyerangan pada Server loh!!!\n\nServer Time : 21 Jun 2024 16:56:02\n\n06/21-16:56:01.721607 [**] [1:1000006:2] TCP Port
Scanning [**] [Priority: 0] {TCP} 149.154.170.100:443 -> 10.0.2.15:52340 06/21-16:56:01.784316 [**] [1:1000006:2] TCP Port Sca
nning [**] [Prio","entities":[{"offset":180,"length":19,"type":"url"},{"offset":203,"length":15,"type":"url"}]}}Alert Terkirim
^C
```

Gambar 6. NIDS Server

c. Pengujian Notifikasi Bot Telegram

Selain dapat memonitoring NIDS Server, notifikasi serangan juga secara otomatis akan terkirim pada telegram bot yang sudah dikonfigurasi sebelumnya, hasilnya ditunjukkan pada Gambar 7.



Gambar 7. Notifikasi Serangan pada Bot Telegram

Dari pengujian serangan TCP *Port Scanning* yang telah dilakukan didapatkan hasil seperti yang tertera pada tabel 2.

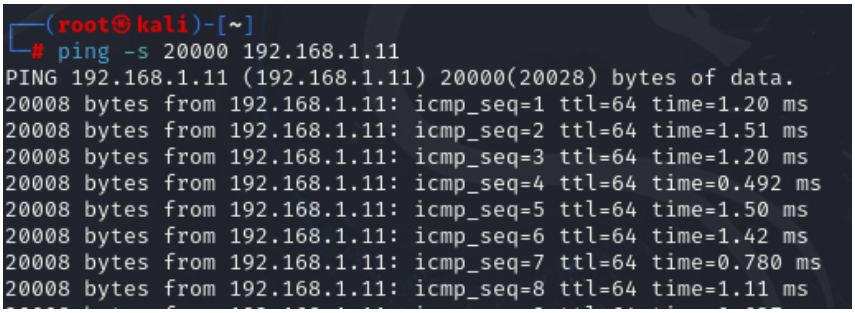
Tabel 2. Hasil Pengujian TCP *Port Scanning*

No	Parameter	Snort	Telegram
1	Scan Type	Berhasil	Berhasil
2	Port Range	Berhasil	Berhasil

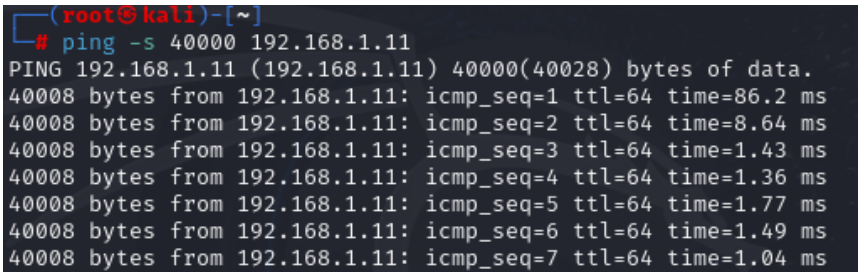
3. Pengujian Serangan ICMP Flooding

a. Pengujian ICMP Flooding

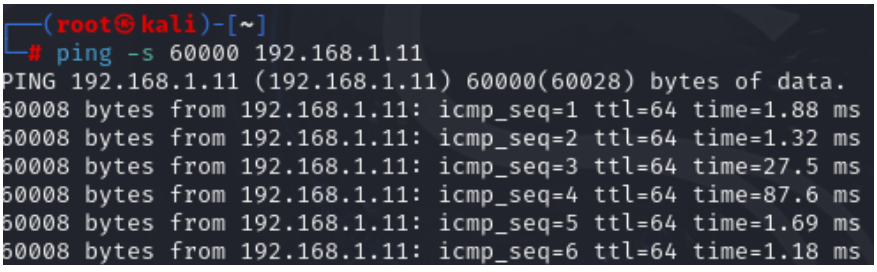
Pengujian ICMP Flooding atau yang biasa disebut ping of death ini bertujuan untuk memenuhi lalu lintas jaringan dengan byte tinggi, pada pengujian serangan ini akan menggunakan dua parameter yaitu packet size dan ping count.



Gambar 8. Packet Size 20000 bytes



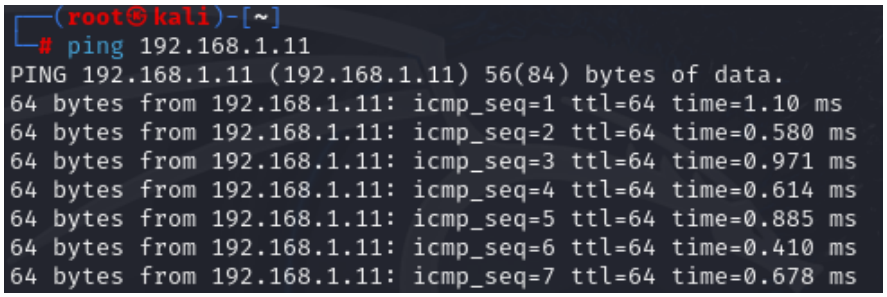
Gambar 9. Packet Size 40000 bytes



Gambar 10. Packet Size 60000

Pada gambar 8, 9, dan 10 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.

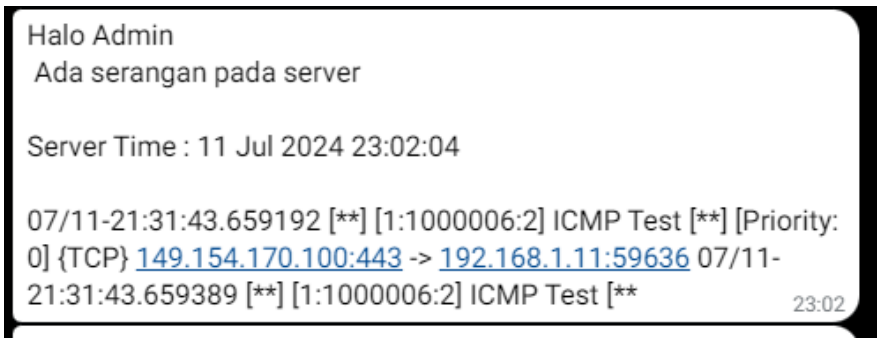


Gambar 11. Ping Count

Perintah 'ping' digunakan untuk melakukan pengujian *ping count* jaringan antar perangkat. Perintah ini mengirimkan paket ICMP *Echo Request* dan didapatkan dari hasil ping menunjukkan bahwa perangkat [22] dengan alamat IP 192.168.1.11 merespon dengan paket ICMP *Echo Reply*

b. Notifikasi Bot Telegram

Melakukan pengecekan pada notifikasi bot telegram ketika terjadi serangan ICMP *flooding* dapat dilihat pada Gambar 12.



Gambar 12. Notifikasi Serangan ICMP *Flooding*

c. Monitoring NIDS Server

Setelah melakukan pengujian serangan ICMP flooding, server NIDS dapat memantau serangan serangan tersebut yang ditunjukkan pada gambar 13.

Gambar 13. Monitoring NIDS Server

Dari pengujian serangan ICMP *Flooding* yang telah dilakukan didapatkan hasil seperti yang tertera pada tabel 3.

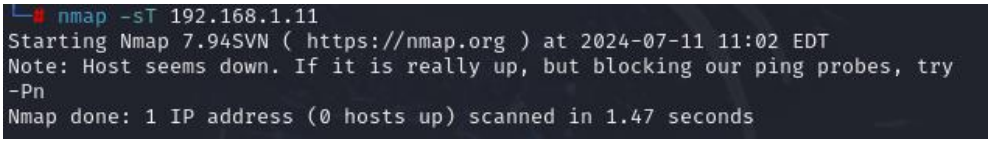
Tabel 3. Pengujian ICMP *Flooding*

No	Parameter	Respon Snort	Respon Telegram
1	Scan Type 20000 Bytes	Berhasil	Berhasil
2	Scan Type 40000 Bytes	Berhasil	Berhasil
3	Scan Type 60000 Bytes	Berhasil	Berhasil
4	Ping Count	Berhasil	Berhasil

4. Pencegahan Serangan Jaringan

a. Mencegah Serangan TCP Port Scanning

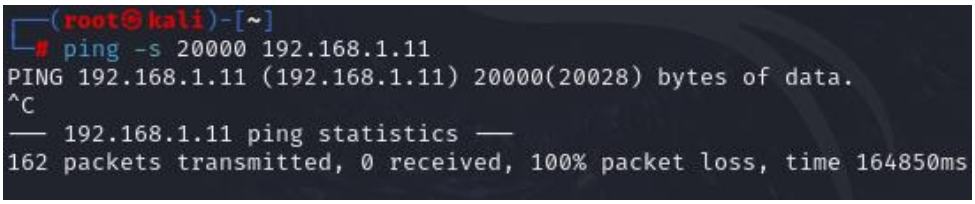
Serangan TCP Port Scanning dapat diatasi menggunakan Iptables dengan perintah : sudo apt iptables -A INPUT -p tcp –dport 80 -m state –state NEW -m recent --set. Kemudian dilakukan penyerangan ulang dan hasilnya adalah host sedang tidak aktif atau host memblokir probe ping.



Gambar 14. Hasil dari Pencegahan TCP *Port Scanning*

b. Mencegah Serangan ICMP Flooding

Serangan yang terjadi pada gambar 8, 9, dan 10 dapat diatasi menggunakan Iptables dengan perintah : iptables -A INPUT -p icmp –icmp-type echo-request -j DROP. Kemudian dilakukan penyerangan ulang dan hasilnya ditunjukkan pada gambar 15.



Gambar 15. Hasil dari Pencegahan ICMP *Flooding*

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

D. Simpulan

Dari penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa Network Intrusion Detection System (NIDS) menggunakan Snort mampu bekerja secara efektif memberikan peringatan terhadap 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 dari pengujian membuktikan bahwa IDS dan IPS dapat memberi pertahanan yang kuat terhadap berbagai serangan tersebut terutama pada ICMP *Flooding*. Karena ICMP *Flooding*

sekedar mengirimkan serangan berbentuk packet yang banyak dan proses penyerangan melalui protocol dan tidak masuk ke port secara langsung. IDS dan IPS adalah solusi yang efektif untuk menghadapi serangan tersebut.

E. Ucapan Terima Kasih

Terima kasih kepada Universitas Amikom Yogyakarta, dosen, orang tua, dan teman teman atas arahan, saran, bantuan dan dukungannya dalam menyelesaikan penelitian ini.

F. Referensi

[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] A. Trisolino, "Analysis of Security Configuration for IDS/IPS," *Diss. Politecnico di Torino*, 2023.

[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] S. Q. A. Shah, F. Z. Khan, and M. Ahmad, "The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network," *Computer Networks*, vol. 187, p. 107825, 2021.

[9] M. Abushwereb, M. Mustafa, M. Al-Kasassbeh, and M. Qasaimeh, "Attack based DoS attack detection using multiple classifier," *arXiv preprint arXiv:2001.05707*, 2020.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] A. Fathurrozi and F. Karimah, "Pelayanan Dan Informasi Customer Service Berbasis Bot Telegram Dengan Algoritma Forward Chaining Pada CV. PRIMGUARD INDONESIA," *Journal of Informatic and Information Security*, vol. 2, no. 2, 2021.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.