

Intrusion Detection System (IDS) Pada Snort Dengan Bot Telegram Sebagai Sistem Notifikasi Terhadap Serangan Syn Flood dan Ping Of Death

Zuriati Ardila Safitri¹, Elin Haerani², Rometdo Muzawi³, Muhammad Affandes⁴, Pizaini⁵

¹Universitas Islam Negeri Sultan Syarif Kasim Riau, 12050126277@students.uin-suska.ac.id, Jl. H.R Soebrantas, Pekanbaru, Indonesia

²Universitas Islam Negeri Sultan Syarif Kasim Riau, elin.haerani@uin-suska.ac.id, Jl. H.R Soebrantas, Pekanbaru, Indonesia

³STMIK Amik Riau, rometdomuzawi@stmik-amik-riau.ac.id, Jl. H.R Soebrantas, Pekanbaru, Indonesia

⁴Universitas Islam Negeri Sultan Syarif Kasim Riau, affandes@uin-suska.ac.id, Jl. H.R Soebrantas, Pekanbaru, Indonesia

⁵Universitas Islam Negeri Sultan Syarif Kasim Riau, pizaini@uin-suska.ac.id, Jl. H.R Soebrantas, Pekanbaru, Indonesia

Informasi Makalah

Submit : Juni 27, 2024

Revisi : Juni 29, 2024

Diterima : Juni 30, 2024

Kata Kunci :

Snort IDS;
Bot Telegram;
Artificial Intelligence (AI);
Syn Flood;
Ping of Death;
Keamanan Jaringan.

Abstrak

Keamanan jaringan menjadi prioritas penting dalam era digital. Penelitian ini mengembangkan sistem *Intrusion Detection System (IDS)* berbasis Snort yang terintegrasi dengan bot Telegram untuk notifikasi real-time dan menggunakan kecerdasan buatan (AI) untuk mendeteksi serta mengelompokkan jenis serangan *Syn Flood* dan *Ping of Death*. Snort dikonfigurasi dengan aturan khusus untuk mendeteksi kedua jenis serangan ini. Bot Telegram digunakan untuk mengirimkan notifikasi langsung kepada administrator jaringan saat serangan terdeteksi. Hasil penelitian menunjukkan bahwa sistem ini mampu mendeteksi serangan dengan cepat, memberikan notifikasi *real-time*, dan mengelompokkan jenis serangan dengan tingkat keberhasilan mengirimkan notifikasi 100% dalam waktu rata-rata 5 detik setelah mendeteksi serangan. Integrasi ini meningkatkan efektivitas deteksi dan respons terhadap serangan jaringan, menawarkan solusi yang lebih aman dan efisien bagi organisasi.

Abstract

Network security is an important priority in the digital era. This research develops a Snort-based Intrusion Detection System (IDS) system that is integrated with Telegram bots for real-time notifications and uses artificial intelligence (AI) to detect and classify types of Syn Flood and Ping of Death attacks. Snort is configured with specific rules to detect both types of attacks. Telegram bots are used to send notifications directly to network administrators when attacks are detected. The research results show that this system is able to detect attacks quickly, provide real-time notifications, and classify attack types with a success rate of sending notifications of 100% within an average of 5 seconds after detecting an attack. This integration increases the effectiveness of detection and response to network attacks, offering organizations a more secure and efficient solution.

1. Pendahuluan

Keberadaan Internet dapat memudahkan kehidupan sehari-hari jika digunakan dengan bijak (Azzahra, 2008). Internet banyak dimanfaatkan untuk berkomunikasi, mencari informasi, memudahkan transaksi digital, sarana belajar dan lainnya (Hapsari & Pamungkas, 2019). Maka tidak mengherankan jika pengguna internet meningkat dari tahun ke tahunnya. Berdasarkan laporan terbaru dari We Are Social dan Hootsuite, Jumlah pengguna internet di seluruh dunia mencapai 5,16 miliar pada Januari 2023 (Hapsari & Pamungkas, 2019),(Hardianti et al., 2023). Jumlah ini mencapai 64,4% dari total populasi dunia yaitu 8,01 miliar jiwa dan meningkat jika dibandingkan dengan jumlah pengguna di periode sama tahun sebelumnya yaitu 5,01 miliar pengguna (Rahmatullah, 2021). Dengan pesatnya perkembangan internet ini, maka tidak mengherankan jika terdapat celah yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan aksi kejahatan di dunia maya. Salah satu ancaman yang masih sering terjadi di dunia maya adalah *Denial of Service*.

DoS merupakan jenis serangan yang membebani server dengan mengirimkan paket dalam jumlah besar dalam jangka waktu yang lama atau dengan mengirimkan paket dalam jumlah besar secara bersamaan (Prasetya, 2016). Dalam skenario serangan DoS, server akan menerima jumlah permintaan yang tiba-tiba dalam waktu singkat, mengakibatkan server menjadi terbebani secara berlebihan dan kehilangan kemampuan untuk melayani permintaan yang sah (Dr. Ir. Martoono Anggusti. et al., 2016). Penyerang biasanya memanfaatkan berbagai teknik, seperti membanjiri jaringan dengan permintaan palsu atau memanfaatkan kerentanan dalam perangkat lunak server (Butarbutar, 2023). Hal ini memunculkan tantangan serius bagi organisasi dan

perusahaan yang bergantung pada server untuk menjalankan bisnis mereka.

Melihat pentingnya keamanan jaringan, maka diperlukan pemantauan selama 24 jam. Namun pemantauan ini sangat tidak memungkinkan jika dilakukan secara manual oleh administrator (Sokibi, 2017). Untuk itu, diperlukan dukungan sistem yang dapat terus memantau guna mencegah atau mengendalikan serangan terhadap server. Sistem fisik atau non fisik dapat memberikan langkah keamanan pada jaringan komputer (Hasibuan, 2016). Sistem fisik dirancang untuk memberikan perlindungan pada server dan perangkat, mencegah pencurian, bencana alam, dan kesalahan manusia (Irmayani, 2019). Sistem operasi server mungkin mengalami gangguan, aplikasi mungkin mengalami kerusakan, dan gangguan eksternal seperti serangan hacker, virus, atau trojan horse juga dapat mengakibatkan kerusakan fisik (Eriana, 2022).

Gangguan yang disebabkan oleh serangan DDoS pada jaringan server merupakan masalah umum (Sutarti & Khairunnisa, 2017). Gangguan ini dapat mencakup sistem crash, shutdown, kesalahan query, dan bahkan kerusakan perangkat keras pada server. Sejak tahun 1990, serangan DDoS menjadi lebih sering dan menantang. Cara serangan yang paling umum adalah serangan DDoS, seperti yang dilaporkan pada akhir tahun 2014 (Putri & Munawar, 2020). Oleh karena itu, DDoS merupakan salah satu ancaman siber utama dan masalah keamanan siber utama.

Teknik yang membantu mendeteksi dan melaporkan aktivitas jaringan komputer dikenal sebagai *intrusion detection system* (IDS) (Ramadhan et al., 2024). IDS akan melakukan melakukan pengawasan terhadap aktivitas yang mencurigakan dan traffic jaringan. Sistem akan memberikan sebuah peringatan guna memberitahu apakah aktivitas tersebut berbahaya atau tidak. Salah satu aplikasi yang digunakan sebagai IDS adalah *Snort*. *Snort* adalah contoh *tools* IDS

yang bersifat *open source* (Puji Insani et al., 2023). *Snort* dapat digunakan untuk mendeteksi apakah ada serangan yang menembus sistem.

Berbagai penelitian telah dilakukan untuk memperkenalkan mekanisme IDS pada keamanan jaringan, salah satunya adalah pemanfaatan bot telegram API untuk mengirimkan pemberitahuan akan adanya serangan (Wikantama & Puspitasari, 2023). Menurut Supratman, mengungkapkan bahwa IDS dengan *Snort* dapat mendeteksi intrusi serangan pada jaringan komputer, dan sistem dapat mengirimkan peringatan *real-time* dari *Snort* ke *administrator* melalui *bot Telegram* (Supratman, 2021). Dalam penelitiannya menunjukkan bahwa sistem berhasil mendeteksi serangan *DDOS Attack*, *FTP Bruteforce Attack*, serta *SSH Bruteforce Attack*, dan mengirimkan notifikasi secara otomatis melalui bot Telegram sehingga administrator dapat mengetahui kondisi server saat terjadinya serangan tersebut (Supratman, 2021).

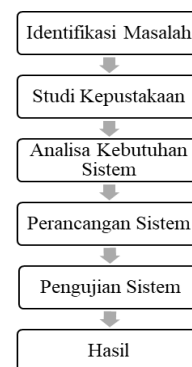
Salah satu perangkat *mobile* yang bisa dijadikan media menerima notifikasi adalah bot Telegram (Fahana et al., 2017). Bot Telegram ini merupakan salah satu fitur API (*Application Programming Interface*) pada aplikasi Telegram (Fahana et al., 2017). Fitur ini memudahkan pengguna untuk mengotomatiskan sistemnya karena bot Telegram ini merupakan platform aplikasi tambahan dengan berbagai fitur. Telegram digunakan oleh pengguna untuk mengirim perintah dalam format berpemilih. Karena bot Telegram dapat memberikan informasi berupa data serangan pada jaringan Mikrotik, maka notifikasi bot Telegram dapat sangat berguna bagi administrator jaringan untuk memberikan peringatan ketika terjadi serangan *DDoS* (Arif Gunawan Simanjunta, Naikson Fandier Saragih, 2021).

Berdasarkan uraian permasalahan diatas, maka tujuan penelitian ini untuk merancang dan mengimplementasikan *intrusion detection system* (IDS) berbasis *Snort* yang

dapat mengidentifikasi serangan *Syn Flood* dan *Ping of Death*, sekaligus memanfaatkan bot Telegram untuk memberikan notifikasi *real-time*.

2. Metode Penelitian

Dijelaskan bahwa penelitian ini menggunakan celah kemajuan teknologi berdampak pada keamanan server dan jaringan dan desain pengujian system skenario serangan *Syn Flood* dan *Ping Of Death*. Metodologi yang diterapkan dalam pengembangan sistem *Intrusion Detection System* (IDS) ini melibatkan beberapa langkah terintegrasi yang mencakup konfigurasi alat deteksi, pengiriman notifikasi *real-time*, serta pendeteksian dan pengelompokan serangan menggunakan kecerdasan buatan (AI). Metodologi ini membuktikan bahwa penggabungan *Snort*, bot Telegram, dan AI dapat menghasilkan sistem IDS yang kuat dan responsif. Dengan konfigurasi yang tepat dan integrasi teknologi yang efektif, sistem ini mampu memberikan deteksi serangan yang akurat, notifikasi *real-time*, serta pengelompokan serangan dan system tanya jawab yang memberikan jawaban relevan dan akurat.



Gambar 1. Metodologi Penelitian

2.1 Analisa Kebutuhan Sistem

Pada analisa kebutuhan ini akan dilakukan untuk mengetahui spesifikasi kebutuhan sistem. Spesifikasi kebutuhan melibatkan analisa perangkat keras (*Hardware*) dan perangkat lunak (*Software*).

2.1.1 Analisa Kebutuhan Perangkat Keras

Kebutuhan perangkat keras yang digunakan dalam penelitian ini adalah:

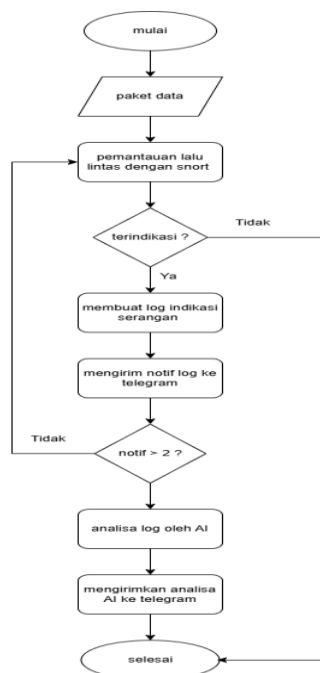
1. Processor Intel Core i5 2.3 Ghz
2. Random Access Memory (RAM) DDR3 6GB.
3. Harddisk 500 GB.

2.1. Analisa Kebutuhan Perangkat Lunak

1. Virtualbox
2. Linux kubuntu
3. Snort IDS
4. Hping3
5. Telegram
6. *Service API Open AI*

2.2 Alur Pendeteksi Serangan

Sistem yang akan dibangun pada penelitian ini adalah *Intrusion Detection System* sebagai pendeteksi yang akan mengirimkan notifikasi terhadap peringatan melalui bot telegram. Untuk melakukan pendeteksian, digunakan *database snort* yang telah dikonfigurasi sebelumnya yang akan dijadikan sebagai laporan untuk administrator. Model AI dilatih untuk mendeteksi dan mengelompokkan jenis serangan berdasarkan data yang dikumpulkan.



Gambar 4. Flowchart Alur Pendeteksi Serangan

2.3 Server

Jaringan mencakup perangkat atau komputer yang terhubung ke komputer atau perangkat lain melalui server, yang pada dasarnya memberikan satu atau lebih layanan (Riska et al., 2018). Menghosting konten dan mengendalikan akses ke perangkat keras, perangkat lunak, dan sumber daya lainnya di jaringan adalah beberapa di antara kemampuan.

Server hadir dalam berbagai jenis, ukuran, dan fitur. Misalnya, server menyimpan file secara terpusat yang dapat diakses oleh banyak pengguna melalui jaringan. Spesifikasi berskala besar dan beragam bervariasi untuk jenis server, termasuk memori, prosesor (eksekutif di Internet), media penyimpanan atau media lainnya (seperti fasilitas konferensi video), kemampuan perangkat lunak, dan koneksi melalui internet.

2.4 Denial of Service

Serangan pada sistem internet dapat mengakibatkan penipisan sumber daya, yang mengarah ke Penolakan Layanan (DoS), yang menyebabkan pengguna lain yang tidak berwenang menggunakan layanan sistem untuk menjalankan fungsinya dengan baik.

Serangan DoS tersebut menargetkan kelemahan sistem sehubungan dengan sumber daya yang tersedia seperti penggunaan bandwidth, kebutuhan penyimpanan, dan kerentanan terkait sumber daya lainnya yang dieksploitasi di server. Pada dasarnya, para penyerang bertujuan untuk mengganggu sistem ini namun terkadang meminta uang tebusan untuk menghentikannya.

Serangan *Denial of Service* (DoS) cukup kuat untuk merusak infrastruktur organisasi. Tujuan dari serangan ini adalah untuk mencegah pengguna menggunakan layanan yang disediakan oleh server dan pada akhirnya menjatuhkannya. Karena serangan DoS adalah serangan satu lawan satu, maka diperlukan host untuk membanjiri lalu lintas

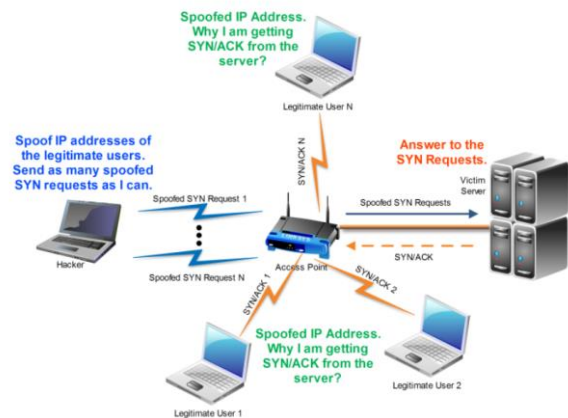
host target untuk mencegah klien mengakses layanan jaringan di server yang diserang oleh penyerang. Pada penelitian ini, dilakukan simulasi serangan terhadap server dengan 2 cara, yaitu *Syn flooding* dan *Ping of death*.

2.4.1 Serangan *Syn Flood*

Serangan *Syn flooding* adalah serangan penolakan layanan (DoS) yang dilakukan dengan mengirimkan permintaan koneksi SYN dalam jumlah besar ke server atau sistem jaringan. Permintaan ini dibuat dengan sengaja oleh penyerang menggunakan alamat IP yang dipalsukan. Tujuan utama dari serangan ini adalah untuk menghabiskan sumber daya sistem jaringan, membuat sistem tidak dapat beroperasi, dan membuat layanan yang disediakan tidak tersedia.

Serangan *Syn flooding* dimulai ketika penyerang mengirimkan beberapa permintaan koneksi SYN ke server atau sistem jaringan. Untuk membuat koneksi, sistem jaringan harus merespon setiap permintaan SYN dengan permintaan ACK (*acknowledgement*). Namun, dalam serangan *Syn flooding*, penyerang tidak mengirimkan permintaan ACK (*Acknowledgement*) kembali ke sistem jaringan, sehingga sistem jaringan terus menunggu dan membuang sumber daya komputasi. Hal ini menyebabkan sistem jaringan berhenti merespons dan layanan menjadi tidak tersedia (Bagian Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat - BSSN, 2020).

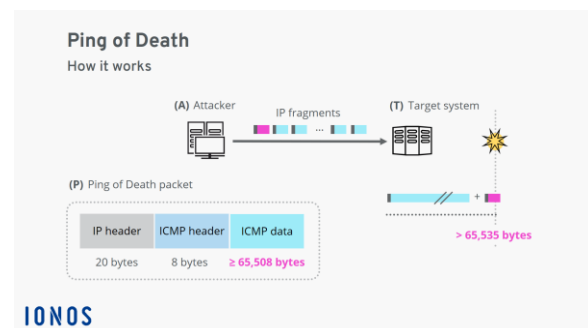
Serangan *Syn flooding* merupakan salah satu jenis serangan DoS yang paling berbahaya karena dapat mematikan atau bahkan merusak sistem jaringan secara permanen. Selain itu, serangan ini dapat menyebabkan kerugian finansial yang signifikan bagi korbannya, terutama jika korbannya adalah bisnis atau organisasi yang memerlukan layanan jaringan untuk operasional bisnis.



Gambar 2. Simulasi Serangan *Syn Flood* (Bogdanoski, 2013)

2.4.2 Serangan *Ping Of Death*

Ping of death adalah serangan *Denial of Service* (DoS). Serangan ini dimulai dengan mengirimkan paket data berbahaya ke target. Ketika sistem target memproses paket data, terjadi kesalahan yang menyebabkan sistem crash. Untuk melakukan serangan *ping-of-death*, penyerang mengirimkan paket data *Internet Control Message Protocol* (ICMP) yang berisi data palsu atau melebihi batas yang diizinkan ke sistem target. Paket data ini mungkin terlihat seperti permintaan ping standar, namun ukurannya jauh lebih besar. Ketika sistem target menerima paket data ini, ia mencoba memprosesnya secara normal. Namun, jika ukuran paket data melebihi batas yang diizinkan, sistem target mungkin tidak dapat memprosesnya dan pada akhirnya berhenti merespon atau mengalami *crash*.



IONOS

Gambar 3. Simulasi Serangan *Ping Of Death* (Tim Penulis IONOS, 2020)

2.5 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan salah satu metode untuk mendeteksi serangan. Cara ini mampu mengatasi serangan yang masuk. Dari segi penggunaan, fungsi IDS hanya sebagai pendeteksi dan bukan digunakan untuk pengambilan keputusan ketika terjadi serangan. Tidak hanya itu, IDS juga mampu mengklasifikasikan apakah serangan berasal dari luar ataupun dalam organisasi sehingga dapat membantu dalam pengambilan keputusan ketika mengalokasikan sumber daya keamanan jaringan .

2.6 Snort

Alat pemantauan perilaku daring seperti Snort dirancang untuk mendeteksi dan menganalisis aktivitas mencurigakan. Melalui penangkapan dan dokumentasi paket data jaringan, program ini dapat mengidentifikasi berbagai serangan eksternal. Dari segi keunggulan, Snort adalah salah satu pilihan yang lebih baik dibandingkan produk IDS lainnya, termasuk Cisco IDN dan ISS *Real Secure*.

2.7 Telegram Bot

Telegram merupakan aplikasi yang menggunakan teknologi cloud yang memungkinkan pengguna mengakses akun Telegram dari beberapa perangkat secara bersamaan. Nikolai Durov dan Pavel Duriv, dua bersaudara Rusia, mengembangkan perangkat lunak yang memungkinkan pengguna untuk berbagi file hingga 1,5 GB Telegram dengan mudah. Nikolai bertanggung jawab atas pengembangan aplikasi, termasuk pembuatan protokol MTPProto, yang merupakan inti dari Telegram. Di sisi lain, Pavel fokus pada aspek finansial dan infrastruktur melalui *Digital Fortress* .

Dengan Telegram, pengguna dapat membuat bot yang dapat diintegrasikan ke dalam sistem informasi. Salah satu hal menarik tentang Telegram adalah tersedianya

client source code yang dapat dikompilasi oleh pengguna. Oleh karena itu, dimungkinkan untuk mengintegrasikan aplikasi Telegram ke dalam sistem informasi yang dikembangkan secara terpisah. Selain menyediakan *client source code*, Telegram juga menyediakan API untuk pengembangan bot yang merupakan sebuah sistem terprogram dengan antarmuka penjawab pertanyaan sederhana yang dapat diintegrasikan pengguna.

Bot adalah aplikasi pihak ketiga yang dapat berjalan di dalam Telegram. Pengguna dapat mengirim pesan, perintah dan *inline request*. Pengguna dapat memanfaatkan API Telegram untuk mengontrol bot melalui HTTPS.

2.8 Artificial Intelligence (AI)

AI adalah singkatan dari "*Artificial Intelligence*" atau kecerdasan buatan. Ini merujuk pada bidang ilmu komputer yang berfokus pada pengembangan sistem komputer yang mampu melakukan tugas-tugas yang membutuhkan kecerdasan manusia. Tujuan utama dari AI adalah untuk membuat komputer atau sistem cerdas yang mampu belajar, merencanakan, memecahkan masalah, dan mengambil keputusan dalam situasi yang kompleks.

Kecerdasan buatan (AI) digunakan sebagai bagian integral dari sistem Intrusion Detection System (IDS) untuk meningkatkan kemampuan deteksi dan pengelompokan jenis serangan yang terjadi dalam jaringan. Peran utama AI adalah untuk menganalisis data serangan yang terdeteksi oleh IDS, mengidentifikasi pola-pola yang mungkin sulit dikenali oleh metode deteksi tradisional, dan memberikan klasifikasi yang lebih akurat tentang jenis serangan yang terjadi.

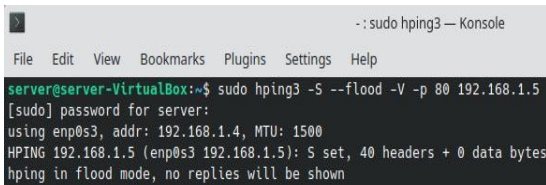
3. Hasil dan Pembahasan

3.1 Pengujian System

3.1.1 Serangan *Syn Flood*

Pengujian ini dilakukan dengan melakukan serangan bertipe *Syn Flood*

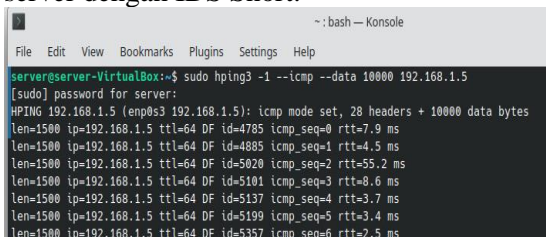
Attack kepada server menggunakan tool hping3 sebagai bahan uji dari computer attacker. Berikut tampilan perintah untuk melakukan serangan bertipe Syn Flood kepada server dengan IDS Snort



Gambar 10. Serangan Syn Flood

3.1.2 Serangan Ping Of Death

Pengujian ini dilakukan dengan melakukan serangan bertipe Ping Of Death Attack kepada server menggunakan tool hping3 sebagai bahan uji dari computer attacker. Berikut adalah tampilan perintah serangan bertipe Ping Of Death kepada server dengan IDS Snort.



Gambar 11. Serangan Ping Of Death

3.2 Source Code bot-tele.sh

Buat file bot-tele.sh pada directory /home/username/telegram dan masukkan script sesuai token dan chat id yg sudah didapatkan, berikut source code file bot-tele.sh :

```
#!/bin/bash

#init
initCount=0
logs=/home/server/telegram/log-tele.txt
notif_count=0

#File
msg_caption=/tmp/telegram_msg_captio
n.txt

#Chat ID dan bot token Telegram
chat_id="1100838603"
token="7033534624:AAG3okO2Jt375q0
atCWMkX4qqb7gTuz4SKE"
```

```
chatgpt_api_key="sk-
J8rHqnLTLjW4cawWHQ59T3B1bkFJU
S2M6PhHKFsE7mLUM9uc"

#kirim
function sendAlert
{
    curl -s -F chat_id=$chat_id -F
text="$caption"
https://api.telegram.org/bot$token/sendM
essage
}

#Ask ChatGPT
function askChatGPT
{
    local log_msg=$1
        local request_body=$(jq -n \
            --arg model "gpt-4" \
            --arg content "Apakah ini jenis
serangan ping of death atau syn flood?
Log: $log_msg. Dan berikan tips
menanganinya. jika bukan dua dari itu ,
itu ciri ciri serangan apa? dan
bagaimana cara kerjanya serta
penanganannya?" \
            {
                model: $model,
                messages: [{role: "user",
content: $content}]
            })

    local response=$(curl -s -X POST
"https://api.openai.com/v1/chat/complet
ions" \
        -H "Authorization: Bearer
$chatgpt_api_key" \
        -H "Content-Type:
application/json" \
        -d "$request_body")

    echo "Response from ChatGPT:
$response" # Debug line to see the raw
response

    local answer=$(echo $response | jq -r
'.choices[0].message.content // "null"')
```



```
if [ "$answer" == "null" ]; then
    answer="Maaf, saya tidak dapat
mengidentifikasi serangan dari log ini.
Silakan periksa log secara manual."
fi

echo -e "Halo Ipit\n\nBerikut adalah
analisa dari log terbaru:\n\n$answer" |
curl -s -F chat_id=$chat_id -F
text="$(</dev/stdin)"
https://api.telegram.org/bot$token/send
Message
}

#Monitoring Server
while true
do
    lastCount=$(wc -c $logs | awk '{print
$1}') #getSizeFileLogs

    if (( lastCount > initCount ));
    then
        msg=$(tail -n 2 $logs)
#GetLastLineLog
        echo -e "Halo Ipit\n Terjadi ada
nya Penyerangan pada Server
!!!\n\nServer Time : $(date +"%d %b
%Y %T")\n\n$msg" > $msg_caption
#set Caption / Pesan
        caption=$(<$msg_caption) #set
Caption
        sendAlert #Panggil Fungsi di
function
        echo "Alert Terkirim"
        initCount=$lastCount
        rm -f $msg_caption
        sleep 1
        notif_count=$((notif_count + 1))

        if ((notif_count % 3 == 0)); then
            askChatGPT "$msg"
        fi
    fi
    sleep 2 #delay if Not Indication
done
```

3.3 Notifikasi Telegram

File *bot.tele.sh* yang mendeteksi adanya *log* baru, meneruskan hasil *log* tersebut menjadi pesan yang diterima oleh *bot telegram* dan diubah menjadi bentuk notifikasi yang masuk ke dalam bot telegram yang sudah dibuat sebelumnya.

```
Halo Ipit
Terjadi ada nya Penyerangan pada Server !!!

Server Time : 26 Jun 2024 07:35:25

06/26-07:35:13.433746 [**] [1:499:4] ICMP Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.1.5
-> 192.168.1.4
06/26-07:35:14.462352 [**] [1:499:4] ICMP Larg                                07:35
```

Gambar 5. Notifikasi Telegram

3.4 Respon AI

Dengan membuat *script* untuk mengirimkan notifikasi melalui bot telegram yang telah menghubungkan IDS dengan snort sehingga setiap kali ada serangan yang terdeteksi dan diklasifikasikan oleh AI.

Implementasi AI dalam sistem deteksi intrusi memberikan keuntungan signifikan dalam hal akurasi dan efisiensi. Dengan kemampuan untuk mengelompokkan jenis serangan.

3.1 Respon Otomatis AI Pada Serangan *Syn Flood*

```
Halo Ipit

Berikut adalah analisa dari log terbaru:

Dari log yang disediakan, tampaknya ini bukan serangan ping of
death maupun SYN flood. Log tersebut menunjukkan lalu lintas TCP
yang tidak biasa dengan port 0, yang diklasifikasikan sebagai "Misc
activity" atau aktivitas tidak biasa. Port 0 dalam protokol TCP/UDP
biasanya tidak digunakan dan seringkali ditandai sebagai tanda dari
aktivitas yang mencurigakan.

Ini bisa saja merupakan tanda dari serangan seperti port scanning
(mencoba mengidentifikasi port mana yang terbuka untuk
komunikasi), atau lainnya - tetapi sejujurnya sulit untuk
menentukan dengan pasti tanpa informasi lebih lanjut.

Beberapa tips untuk mengatasi atau mencegah serangan ini
meliputi:

1. Install dan konfigurasi firewall dengan baik. Firewall akan
membatasi dan mengendalikan lalu lintas yang masuk dan keluar
dari sistem atau jaringan anda.

2. Lakukan patch dan pembaruan secara regular pada sistem anda.
Ini akan memastikan bahwa sistem anda memiliki perlindungan
terkini terhadap berbagai jenis serangan.

3. Gunakan sistem deteksi intrusi (Intrusion Detection System - IDS).
IDS akan membantu mendeteksi aktivitas yang tidak biasa dalam
jaringan anda.
```


Gambar 6. Respon AI terhadap serangan *Syn Flood*

3.2 Respon AI Pada Serangan *Ping Of Death*

Halo Ipit

Berikut adalah analisa dari log terbaru:

Dari log tersebut tampak seperti serangan Ping of Death, yang merupakan jenis serangan DoS (Denial of Service) yang mana pengguna mengirimkan paket ICMP yang sangat besar ke sistem target dengan tujuan antara lain memperlambat sistem atau bahkan membuatnya tidak responsif.

Namun, harus dipastikan lanjutan dari log tersebut. Biasanya, "large ICMP packet" merujuk pada paket yang lebih besar dari 65.535 bytes, yaitu ukuran paket maksimum untuk IPv4.

Cara menanganinya:

1. Gunakan alat deteksi penetrasi. Ada banyak alat yang dapat mendeteksi dan mencegah serangan Ping of Death, seperti Wireshark, tcpdump, dan banyak lainnya.
2. Cek konfigurasi firewall. Pastikan bahwa firewall Anda hanya mengizinkan ICMP yang diperlukan dan memblokir yang lain.
3. Gunakan sistem operasi dan perangkat yang telah mengupdate patch. Paket besar seharusnya tidak menyebabkan masalah pada sistem operasi dan perangkat modern karena mereka biasanya telah memperbaiki bug ini.

Jika bukan Ping of Death, itu bisa merupakan serangan ICMP flood dimana serangan tersebut mengirim sejumlah besar paket ICMP ke target, menguras bandwidth dan sumber daya, dengan tujuan membuat jaringan atau sistem tidak dapat diakses. Penanganannya mirip dengan penanganan untuk Ping of Death yang melibatkan keamanan jaringan yang baik, pembaruan perangkat, dan pencegahan banjir ICMP.

Gambar 7. Respon AI terhadap serangan *Ping Of Death*

3.5 Bot Telegram Manual

Menggunakan bot manual dalam sistem IDS untuk notifikasi adalah pendekatan di mana bot berinteraksi dengan pengguna secara langsung untuk memberikan informasi tentang serangan yang terdeteksi dan memungkinkan pengguna untuk merespons atau menanyakan lebih lanjut tentang insiden tersebut.

Implementasi AI dalam sistem menjawab pertanyaan pengguna, sistem ini tidak hanya meningkatkan keamanan jaringan tetapi juga menyediakan alat edukasi bagi pengguna untuk memahami lebih baik tentang ancaman yang ada. Integrasi dengan bot Telegram memastikan bahwa pengguna mendapatkan notifikasi real-time dan dapat berinteraksi dengan sistem secara langsung, menjadikan respons terhadap insiden lebih cepat dan tepat.

tolong dibantu saya untuk mengelompokkan jenis serangan pada DDoS Attack ? 14:08 ✓

Gambar 8. Pertanyaan Manual Bot Telegram

Jawaban AI : Serangan pada DDoS Attack (Distributed Denial of Service Attack) umumnya dapat dikelompokkan menjadi tiga kategori utama, yaitu:

1. Volume-based Attacks
Serangan jenis ini bertujuan untuk membanjiri bandwidth sebuah situs atau jaringan dengan data yang besar. Contoh dari serangan ini antara lain UDP flood, ICMP flood, dan spoofing IP lainnya.
2. Protocol Attacks
Serangan jenis ini berfokus pada menghabiskan sumber daya server secara langsung atau infrastruktur jaringan dengan menerapkan prosedur tertentu yang diatur oleh protocol-protocol tertentu. Contoh dari serangan ini antara lain SYN flood, Ping of Death, Smurf DDoS dan lainnya.

3. Application Layer Attacks
Jenis serangan ini menyerang aplikasi, sistem operasi, dan server-situs web dengan tujuan untuk mematikan layanan. Contoh dari serangan ini antara lain GET/POST flood, Low-and-Slow attack, dan serangan Zero-day DDoS.

Itu merupakan cara umum untuk mengelompokkan serangan DDoS tetapi penting untuk diingat bahwa penyerang sering menggabungkan berbagai jenis serangan untuk mencapai tujuannya. Jadi, serangan DDoS bisa sangat kompleks dan sulit untuk dihentikan atau dicegah.

14:0

Gambar 9. Respon AI

07:35

3.6 Hasil Pembahasan Pengujian

Pengujian Serangan *Syn Flood* dan *Ping Of Death* menunjukkan bahwa sistem keamanan dengan menggunakan simulasi serangan *Syn Flood* dan *Ping of Death* memiliki tingkat deteksi yang tinggi dan respons cepat terhadap ancaman yang terdeteksi. Integrasi sistem AI dan notifikasi melalui Telegram memungkinkan pengelola sistem untuk merespons serangan dengan efisien, meminimalkan waktu tanggap terhadap serangan, dan memberikan solusi yang tepat waktu kepada pengguna. Evaluasi ini juga menunjukkan bahwa penggunaan teknologi ini dapat meningkatkan keandalan sistem keamanan secara keseluruhan, mendukung upaya perlindungan data dan infrastruktur dari serangan *cyber* yang semakin kompleks dan berbahaya.

Tabel 2. Pengujian Sistem

Pengujian Sistem	
Tipe Serangan	Deskripsi
<i>Syn Flood Attack</i>	Serangan dilakukan menggunakan Tool hping3 dari komputer

Pengujian Sistem	
Tipe Serangan	Deskripsi
Ping Of Death Attack	Attacker, dideteksi oleh ids snort. Serangan <i>ping of death</i> dilakukan Menggunakan tool hping3 dari Komputer attacker, terdeteksi Oleh ids snort.
Respon AI	Sistem ai merespons dengan Mengelompokkan jenis serangan Dan memberikan informasi serta Tips penanganannya.
Notifikasi Telegram	File bot-tele.sh mendeteksi log baru dari serangan, mengirimkan notifikasi ke bot Telegram untuk tindakan lanjut.
Tanya Jawab Bot Telegram	Sistem ai mampu memberikan informasi serta tips untuk penanganannya kepada pengguna.

4 Simpuln

Pengembangan sistem *Intrusion Detection System* (IDS) berbasis Snort yang terintegrasi dengan bot Telegram berhasil menunjukkan kemampuan untuk mendeteksi dan memberikan notifikasi secara real-time terhadap serangan seperti *Syn Flood* dan *Ping of Death* pada jaringan komputer. Implementasi ini memperkuat keamanan sistem dengan memanfaatkan teknologi *open-source* yang efektif dalam menghadapi ancaman keamanan *cyber* yang semakin kompleks. System tanya jawab menggunakan AI memberikan jawaban yang relevan dan akurat terhadap pertanyaan pengguna tentang keamanan jaringan.

Dengan demikian, sistem ini memberikan kontribusi signifikan dalam meningkatkan responsibilitas administrator terhadap serangan yang dapat mengganggu operasional jaringan. Untuk penelitian selanjutnya dapat meningkatkan keamanan jaringan secara keseluruhan dan AI dapat menangani serangan DoS secara otomatis.

5 Referensi

- Arif Gunawan Simanjunta, Naikson Fandier Saragih, M. J. P. (2021). Pengamanan Mikrotik Routerboard Dari Serangan Keamanan Dengan Notifikasi Bot Telegram. *Majalah Ilmiah Methoda*, 11(3), 241–246. <https://doi.org/10.46880/Methoda.Vol11no3.Pp241-246>
- Azzahra, A. (2008). Pemanfaatan Teknologi Dalam Meningkatkan Mutu Pendidikan. *Jurnal Pendidikan Dan Sastra Indonesia*, 5.
- Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Danperkembangannya. *Technology And Economics Law Journal*, 2(2), 299–317. https://www.google.com/search?q=Kejahatan+Siber+Terhadap+Individu%3a+Jenis%2c+Analisis%2c+Dan+Perkembangannya&rlz=1c5chfa_Enid876id882&Oq=Kejahatan+Siber+Terhadap+Individu%3a+Jenis%2c+Analisis%2c+Dan+Perkembangannya&Gs_Lcrp=Egzjahjvbwuybggaeuyotigcaeqrg
- Dr. Ir. Martoono Anggusti., S. M. . H. H., Manda Dwipayani Bhastary, S. S. . M. S., & Sumi Khairani, S. T. . M. K. (2016). Sistem Informasi Manajemen. *Buku*.
- Eriana, S. F. & E. S. (2022). Keamanan Sistem Informasi. In *Seminar Nasional Informatika 2008 (Semnasif 2008) Upn "Veteran" Yogyakarta, 24 Mei 2008* (Vol. 2008, Issue Semnasif).
- Fahana, J., Umar, R., & Ridho, F. (2017). Pemanfaatan Telegram Sebagai Notifikasi Serangan Untuk Keperluan Forensik Jaringan. *Jurnal Sistem Informasi*, 5341(6), 2.
- Hapsari, S. A., & Pamungkas, H. (2019). Pemanfaatan Google Classroom Sebagai Media Pembelajaran Online Di Universitas Dian Nuswantoro. *Wacana: Jurnal Ilmiah Ilmu Komunikasi*, 18(2),

- 225–233.
<https://doi.org/10.32509/Wacana.V18i2.924>
- Hardianti, F., Kumorotomo, W., & Setianto, W. A. (2023). Sosialisasi Child Grooming: Cyber Crime Yang Mengintai Anak-Anak Di Era Digital. *Jurnal Pengabdian Literasi Digital Indonesia*, 2(2), 85–96. <https://doi.org/10.57119/Abdimas.V2i2.45>
- Hasibuan, M. S. (2016). Keylogger Pada Aspek Keamanan Komputer. *Teknovasi*, 3(1), 8–15.
- Irmayani, D. (2019). Penerapan Physical Security. *Jurnal Informatika*, 1(2), 1–16. <https://doi.org/10.36987/Informatika.V1i2.105>
- Prasetya, N. I. (2016). Mereduksi Serangan Denial Of Services Terdistribusi Pada Linux Virtual Server Menggunakan HoneyPot. *Scan, Xi*(3), 33–47.
- Puji Insani, P., Kanedi, I., Al Akbar, A., & Dehasen Bengkulu, U. (2023). Implementation Of Snort As A Wireless Network Security Detection Tool Using Linux Ubuntu Implementasi Snort Sebagai Alat Pendeteksi Keamanan Jaringan Wireless Menggunakan Linux Ubuntu. *Jurnal Komitek*, 3(2), 443–458. <https://doi.org/10.53697/Jkomitek.V3.2>
- Putri, N. I., & Munawar, Z. (2020). Deep Learning Dan Teknologi Big Data Untuk Keamanan Iot. *Jurnal Informatika – Computing*, 7(1), 48–73.
- Rahmatullah, T. (2021). Teknologi Persuasif: Aktor Penting Media Sosial Dalam Mengubah Sikap Dan Perilaku Pengguna. *Jurnal Soshum Insentif*, 4(1), 60–78. <https://doi.org/10.36787/Jsi.V4i1.509>
- Ramadhan, M. R., Santoso, J. D., Mulyatun, S., Komputer, T., Amikom Yogyakarta, U., Utara, J. R., & Corresponding Author, Y. (2024). Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikasi Dengan Menggunakan Snort. *Bhatara: Jurnal Multidisiplin*, 1(1), 31–40. <https://doi.org/.....Ijccs>
- Riska, P., Sugiartawan, P., & Wiratama, I. (2018). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. *Jurnal Sistem Informasi Dan Komputer Terapan Indonesia (Jsikti)*, 1(2), 53–64. <https://doi.org/10.33173/Jsikti.12>
- Sokibi, P. (2017). Perancangan Sistem Monitoring Perangkat Jaringan Berbasis Icmp Dengan Notifikasi Telegram. *Itej (Information Technology Engineering Journals)*, 2(2), 1–11. <https://doi.org/10.24235/Itej.V2i2.16>
- Supratman, I. (2021). Analisa Keamanan Jaringan Lan Menggunakan Snort Dengan Metode Penetration Test Di Labor Teknik Informatika Universitas Islam Riau. *Thesis*. <http://repository.uir.ac.id/id/eprint/11032>
- Sutarti, & Khairunnisa. (2017). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial Of Service) Berbasis HoneyPot. *Jurnal Prosisko*, 4(2), 8.
- Wikantama, P. T., & Puspitasari, R. (2023). Perancangan Perangkat Pengukur Ketinggian Banjir Dengan Esp32 Dan Telegram Berbasis Iot. *Elektriase: Jurnal Sains Dan Teknologi Elektro*, 13(02), 107–114. <https://doi.org/10.47709/Elektriase.V13i02.3108>.