Implementasi Intrusion Detection System (IDS) Suricata Untuk Mendeteksi Serangan DDoS Menggunakan Metode TAARA Pada Jaringan Internet di Pixel Esport Arena Samarinda

Zailani Abdillah[1)], Pitrasacha Adytia[2)] dan Muhammad Fahmi [3)]
Program Studi Teknik Informatika, STMIK Widya Cipta Dharma
Jalan M. Yamin No. 25, Samarinda, 75123
E-mail: zailaniabdillah@gmail.com

ABSTRAK

Keamanan jaringan sangat penting untuk melindungi data dari akses ilegal, termasuk serangan DDoS. Penelitian ini menggunakan sistem deteksi intrusi Suricata dengan metode TAARA untuk mengelola keamanan jaringan di Pixel Esport Arena Samarinda. Penelitian dilakukan di Game Center Pixel Esport Arena dengan metode pengumpulan data melalui wawancara dan observasi langsung. Metode pengembangan sistem yang digunakan adalah *Network Development Life Cycle* (NDLC), bersama dengan penerapan kerangka kerja TAARA dan perangkat lunak seperti *Virtual Machine*, *Suricata, Cisco Packet Tracer*, dan *Wireshark*. Implementasi IDS *Suricata* memudahkan *monitoring* keamanan jaringan melalui notifikasi *bot* Telegram dan kustomisasi *rules*. Analisis *file* .pcap meningkatkan akurasi bukti forensika terhadap serangan DDoS, sementara kerangka kerja TAARA efektif dalam investigasi pasca serangan.

Kata Kunci: Keamanan Jaringan, Suricata, Deteksi Intrusi, TAARA

Implementation of Suricata Intrusion Detection System (IDS) for Detecting DDoS Attacks Using the TAARA Method on the Internet Network at Pixel Esport Arena Samarinda

ABSTRACT

Network security is crucial for protecting data from unauthorized access, including DDoS attacks. This research employs the Suricata intrusion detection system with the TAARA method to manage network security at Pixel Esport Arena Samarinda. The study was conducted at the Pixel Esport Arena Game Center using data collection methods such as interviews and direct observation. The system development methodology applied is the Network Development Life Cycle (NDLC), along with the implementation of the TAARA framework and supporting software including Virtual Machine, Suricata, Cisco Packet Tracer, and Wireshark. The implementation of the Suricata IDS facilitates network security monitoring through Telegram bot notifications and rule customization. .pcap file analysis enhances the accuracy of forensic evidence against DDoS attacks, while the TAARA framework is effective in post-attack investigation.

Keywords*: Network Security, Suricata, Intrusion detection, TAARA*

1. PENDAHULUAN

Kemanan jaringan merupakan suatu sistem yang bertujuan untuk mencegah aktivitas yang tidak diinginkan dengan cara mengidentifikasi pengguna yang tidak memiliki hak akses dalam jaringan. Saat menghubungkan komputer ke dalam jaringan, baik menggunakan kabel maupun nirkabel, hal ini memungkinkan orang lain untuk mengakses, mengubah, atau bahkan menghapus data yang ada dalam jaringan tersebut. Dengan pentingnya sebuah keamanan pada jaringan, maka hal ini menjadi aspek krusial dalam teknologi informasi saat ini.

Kejahatan *cyber* selalu terkait dengan penggunaan teknologi informasi dan komputer. Kejahatan *cyber* dilakukan dengan memasuki sistem jaringan komputer secara ilegal atau tanpa sepengetahuan pemilik sistem jaringan tersebut. Serangan *Distributed Denial of Service* (DDoS) adalah salah satu jenis serangan dan kejahatan internet yang paling umum. Serangan *Distributed Denial of Service* (DDoS) memiliki tujuan yang negatif, yaitu menghabiskan sumber daya dari server sehingga server menjadi tidak dapat digunakan dengan optimal.

Banyak sistem pertahanan server yang masih dioperasikan secara manual oleh administrator, sehingga

integritas sistem bergantung pada seberapa cepat administrator dapat merespon gangguan. Apabila gangguan telah berhasil membuat server *down* atau jaringan tidak berfungsi, administrator tidak dapat lagi mengakses sistem secara remote, yang berarti mereka tidak dapat memperbaikinya. Suricata adalah sistem deteksi intrusi yang memiliki kemampuan untuk mendeteksi aktivitas serangan pada jaringan yang dibantu oleh *rules* yang telah dibuat. Ketika terjadi serangan, suricata akan mengecek paket atau serangan yang ada melalui *rules* yang telah dibuat, dan jika serangan terdeteksi, suricata akan membuat log serangan yang dilakukan.

Pixel Esport Arena merupakan salah satu *game center* terbesar di kota Samarinda yang memiliki banyak sekali pelanggan, mulai dari pelajar, mahasiswa, bahkan masyarakat pada umumnya. Dengan komposisi 115 unit PC untuk *Clients* dengan spesifikasi komputer yang cukup tinggi. Kegiatan yang dipaparkan diatas merupakan kegiatan penggunaan internet yang membutuhkan peningkatan keamanan pada jaringan. Hanya saja sistem pertahanan pada server yang digunakan masih bergantung secara manual kepada *administrator*. Salah satu metode yang digunakan dalam manajemen keamanan jaringan adalah metode TAARA, yang merupakan singkatan dari *Trigger, Acquire, Analysis, Report,* dan *Action.* TAARA digunakan untuk pendekatan investigasi forensik yang selanjutnya akan di evaluasi berdasarkan serangan DDoS. Pada penelitian ini peneliti akan menggunakan metode TAARA untuk mengimplementasikan IDS *suricata* pada jaringan internet di *game center Pixel Esport Arena.*

2. RUANG LINGKUP

Dalam penelitian ini permasalahan mencakup:

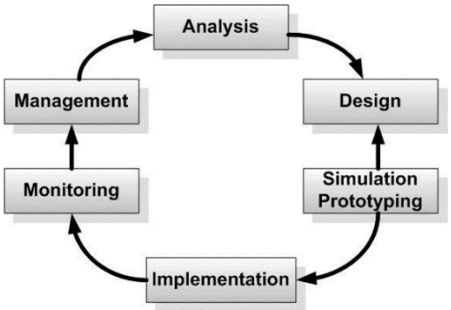
1. Hanya mengimplementasikan IDS pada jaringan *internet Pixel Esport Arena.*
2. Penelitian ini berfokus pada deteksi serangan DDoS dan optimalisasi forensik pasca serangan.
3. Proses pengujian dilakukan menggunakan jenis serangan *port scanning, syn flood,* dan *ping of death.*
4. Proses implementasi digital forensik menggunakan metode *framework* TAARA.

3. BAHAN DAN METODE

Main Adapun bahan dan metode yang digunakan dalam aplikasi ini adalah :

3.1 Metode *Network Development Life Cycle*

Menurut (Afrianto dan Hendrawan, 2019) metode NDLC merupakan sebuah kerangka logis yang memungkinkan desain jaringan untuk bersifat dinamis dan dapat berkembang. Dalam NDLC, pendekatan yang digunakan adalah mempertimbangkan perubahan yang mungkin terjadi dalam lingkungan jaringan serta kebutuhan dan persyaratan yang berubah dari waktu ke waktu.Dengan menggunakan NDLC, perancangan jaringan dapat lebih adaptif dan fleksibel, sehingga mampu mengikuti perkembangan teknologi



Gambar 1. Prosedur Penelitian NDLC

3.2 Keamanan Jaringan

Keamanan jaringan adalah merupakan upaya untuk melindungi jaringan komputer dari berbagai ancaman dan kerentanan. Fungsinya meliputi melindungi aset digital, menjaga privasi pengguna, menjamin integritas data, dan memastikan ketersediaan layanan (Rahman *et al.*, 2024).

Keamanan jaringan merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data dan informasi dalam jaringan komputer yang dikenal dengan *confidentiality*, *integrity*, dan *availability* (CIA) Triad. Menurut (Hermawan *et al.*, 2022), CIA Triad adalah indikator keamanan informasi yang digunakan oleh para ahli sebagai alat ukur keamanan *cyber*, dimana CIA Triad terdiri atas *confidentiality* atau kerahasiaan, *integrity* atau integritas, serta *availability* atau ketersediaan, dimana hal tersebut dapat dijelaskan dibawah :

1. *Confidentiality*

Confidentiality atau kerahasiaan adalah suatu langkah-langkah yang perlu dilakukan untuk memastikan kerahasiaan atau privasi suatu sistem agar tidak diakses oleh orang yang tidak memiliki kewenangan.

2. *Integrity*

Integrity atau integritas adalah kepercayaan data atau keaslian data dimana data tidak boleh diubah oleh orang yang tidak memiliki kewenangan untuk mengakses data didalam nya sehingga perlu tindakan tidak hanya memfilter data namun juga memfilter penguna yang ada didalam web app tersebut agar orang yang tidak memiliki kewenangan tidak dapat mengakses data tersebut

3. *Availability*

Availability atau ketersediaan data ialah serangkaian langkah-langkah yang digunakan untuk memberikan jaminan autentikasi kepada pengguna bahwa data didalam nya tidak dapat diakses oleh orang yang tidak memiliki kewenangan,

3.3 *Intrusion Detection System*

Intrusion Detection System (IDS) adalah sistem yang memiliki kemampuan untuk mendeteksi aktivitas yang mencurigakan dalam sistem atau jaringan. (IDS) dapat

mengawasi lalu lintas jaringan yang mencurigakan dan memberikan peringatan kepada sistem dan administrator agar mereka segera melakukan analisis jaringan. Proses mengamati dan mengidentifikasi aktivitas jaringan dari berbagai anomali yang mungkin terjadi dan dapat mengganggu jalannya sistem adalah definisi lain dari *intrusion detection system*.(Syani, 2020)

3.4 Suricata

Suricata merupakan IDS yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan rules yang telah ada. Cara kerja dari suricata adalah ketika adanya penyerangan, suricata akan melakukan pengecekan paket/serangan yang ada melalui rules yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat log serangan yang dilakukan.(Stephani *et al.*, 2020)

3.5 DDoS

Menurut (Haris *et al.*, 2022) *Denial of Service* (DoS) adalah jenis serangan siber di mana penyerang berusaha membuat sumber daya atau layanan yang disediakan oleh sebuah sistem komputer tidak tersedia bagi pengguna yang sah. Tujuan utama dari serangan DoS adalah untuk mengganggu operasi normal dari layanan atau situs web yang ditargetkan, biasanya dengan membanjiri target dengan lalu lintas berlebih atau mengirim permintaan yang merusak.

3.6 TCP *Syn Flood*

TCP *syn flood* adalah jenis serangan yang dilakukan dengan mengirimkan permintaan sambungan TCP (*Transmission Control Protocol*) ke server dengan menggunakan alamat IP palsu. Server akan membuka sesi sambungan dan menunggu pengiriman data dari pengirim, tetapi data tidak akan pernah dikirimkan. Server akan terus menunggu hingga batas waktu tertentu, sehingga menyebabkan sumber daya server terpakai untuk sesi yang tidak valid (Ayuningtyas, 2023).

3.7 *Port Scanning*

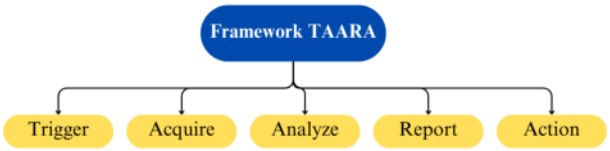
Menurut (Valianta *et al.*, 2016) *Port Scanning* adalah salah satu serangan yang cukup berbahaya, teknik ini dapat memetakan karakteristik, mendeteksi *port* yang terbuka bahkan mendapatkan informasi penting pada suatu jaringan atau host untuk kemudian diteruskan ke serangan lebih lanjut. *TCP Connect Scan* merupakan salah satu teknik *port* scanning yang sukar untuk dideteksi pada kondisi realtime. Permasalahan yang sering diungkapkan pada proses deteksi gangguan secara *real-time* yaitu kapasitas sensor terhadap trafik data, efisiensi volume data serta pemilihan metode yang dapat mengatasi besarnya lalu-lintas data.

3.8 *Ping of Death*

Ping of death yaitu serangan paling lama dan sering digunakan orang pada serangan ini dengan menggunakan *utility ping* disebuah sistem operasi. saat fragmentasi dilakukan, setiap fragmen IP perlu membawa informasi tentang bagian mana dari paket IP asli yang dikandungnya (Walad, 2020).

3.9 TAARA

Framework TAARA digunakan untuk memfasilitasi proses analisis forensik jaringan komputer. *Framework* ini menyediakan berbagai fitur untuk analisis forensik jaringan komputer, seperti analisis paket, analisis log, dan visualisasi data. *Framework* TAARA juga digunakan dalam analisis investigasi, yang dikembangkan berdasarkan Metodologi Threat Assessment & Remediation Analysis (TARA) dan standar ISO SAE 21434 serta NIST SP-800-30 dan ISO IEC 31010. (Suprihadi dan Magfira, 2023)



Gambar 2. *Framework* TAARA

3.10 *Virtual Machine*

Menurut (Hakim, 2022) *Virtual Machine* (VM) adalah sebuah perangkat lunak yang bekerja di dalam sistem operasi komputer yang berfungsi sebagai komputer berbasis perangkat lunak. menciptakan sebuah lingkungan komputasi yang dihasilkan dari perangkat lunak yang memungkinkan pengguna menjalankan sistem operasi dan aplikasi seolah-olah mereka berjalan pada perangkat keras fisik yang sebenarnya

4. IMPLEMENTASI

4.1 Konfigurasi

Pertama-tama lakukan penginstalan IDS suricata pada server dengan melakukan perintah sudo apt-get install suricata -y pada terminal. Bisa dilihat pada gambar 3.

```
root@pixel:/home/zai# apt-get install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:6.0.10-1).
```

Gambar 3. Installasi IDS suricata

Langkah selanjutnya adalah memeriksa apakah IDS suricata sudah terinstall pada server dengan melakukan perintah systemctl status suricata. Perintah systemctl adalah singkatan daripada *system control* yang berfungsi sebagai keterangan perintah untuk menjalankan sebuah aplikasi. Installasi IDS suricata. Perintah sudo pada terminal menandakan bahwa perintah dilakukan oleh *superuser* atau biasa dikenal dengan *administrator* Bisa dilihat pada gambar 4.

```
root@pixel:/home/zai# sudo systemctl start suricata
root@pixel:/home/zai# sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-07-30 23:09:56 +08; 1h 21min ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata-ids.org/docs/
    Process: 648 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml
   Main PID: 695 (Suricata-Main)
      Tasks: 9 (limit: 4622)
     Memory: 855.5M
        CPU: 1min 44.407s
     CGroup: /system.slice/suricata.service
             └─695 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfi

Jul 30 23:09:56 pixel systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Jul 30 23:09:56 pixel suricata[648]: 30/7/2024 -- 23:09:56 - <Notice> - This is Suricata v
Jul 30 23:09:56 pixel systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

Gambar 4. Status Suricata

Langkah selanjutnya membuka *file* suricata.yaml untuk mengkonfigurasi *IP address, interface, rules* dan integrasi *file .pcap.* lakukan perintah sudo nano /etc/suricata/suricata.yaml, bisa dilihat pada gambar 5.

```
# more specific is better for alert accuracy and performance
address-groups:
  HOME_NET: "[192.168.1.11/24]"
  #HOME_NET: "[192.168.0.0/16]"
  #HOME_NET: "[10.0.0.0/8]"
  #HOME_NET: "[172.16.0.0/12]"
  #HOME_NET: "any"
```

Gambar 5. Konfigurasi *IP address* server

Pada gambar 5 diatas adalah *IP* address server berada pada bagian HOME_NET dimana bagian tersebut menjadi *IP address* internal utama untuk deteksi intrusi. Langkah selanjutnya adalah mengkonfigurasikan *rules*, bisa dilihat pada gambar 6.

```
default-rule-path: /etc/suricata/rules

rule-files:
  - suricata.rules
```

Gambar 6. Konfigurasi *rules* suricata

Selanjutnya untuk memastikan apakah fungsi keamanan jaringan dengan implementasi suricata sudah berjalan dengan normal dan sesuai rencana. Setelah mengaktifkan aplikasi IDS suricata dengan systemctl start suricata lalu kemudian melakukan perintah tail -f /var/log/suricata/suricata.log untuk memantau lalu lintas paket pada jaringan server.

```
user@Pixel:~$ sudo tail -f /var/log/suricata/fast.log
```

Gambar 9. Pantauan *fast.log* suricata

Kemudian penulis menintegrasikan isi dari setiap peringatan dalam *file* fast.log pada aplikasi telegram. Pada saat penulis menjalankan serangan DoS *Syn Flood* dan *port* scanning, maka disaat itu juga notifikasi telegram masuk. Maka dari itu Penulis melakukan pembuatan *shell script* untuk *server* agar dapat memberikan notifikasi ke telegram mengenai adanya serangan yang dideteksi suricata.

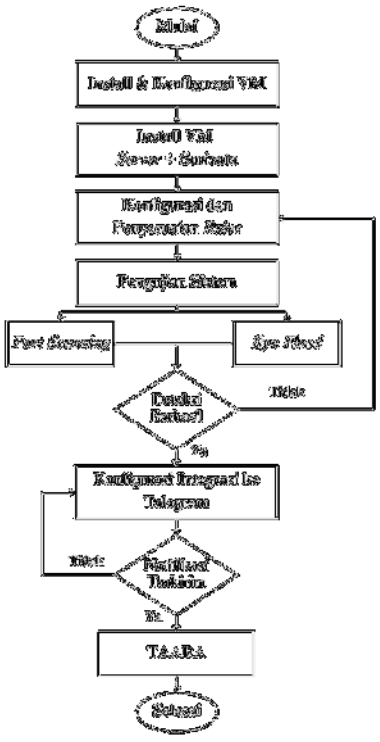
```
 GNU nano 7.2                          suricata-telegram-notifier.sh
#!/bin/bash

# Konfigurasi Telegram
BOT_TOKEN="6745045828:AAFlfnc-VSWEgiYA8hzbSuQ-Ucr89U1i3_E"
CHAT_ID="622644113"

# Path ke file fast.log
LOG_FILE="/var/log/suricata/fast.log"

# File sementara untuk menyimpan log yang telah dibaca
TEMP_LOG="/tmp/fastlog.tmp"

# Cek apakah file sementara sudah ada, jika tidak buat
if [ ! -f "$TEMP_LOG" ]; then
    touch "$TEMP_LOG"
fi

# Membaca log baru dari fast.log
tail -n0 -F "$LOG_FILE" | while read -r line; do
    # Mengirim pesan ke Telegram
    MESSAGE="Suricata Pixel Alert: $line"

    curl -s -X POST "https://api.telegram.org/bot$BOT_TOKEN/sendMessage" \
        -d chat_id="$CHAT_ID" \
        -d text="$MESSAGE"

    # Menyimpan log yang telah dibaca ke file sementara
    echo "$line" >> "$TEMP_LOG"
done
```

Gambar 10. *Shell script* telegram

Secara garis besar, cara kerja dari *script* pada gambar 4.30 adalah jika pada *file log* suricata yakni *fast.log* terdeteksi adanya baris baru yang mana itu menandakan adanya percobaan serangan, maka *file* tersebut dan selanjutnya dikirimkan ke telegram.

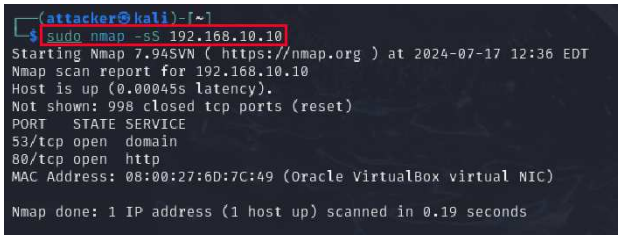
4.2 Pengujian

Agar tahap pengujian ini mampu dipahami dengan mudah sesuai dengan maksud dari penulis, maka alur pengujian dibuat agar mendapat kesesuaian dari metode pengembangan penelitian yang dijalankan



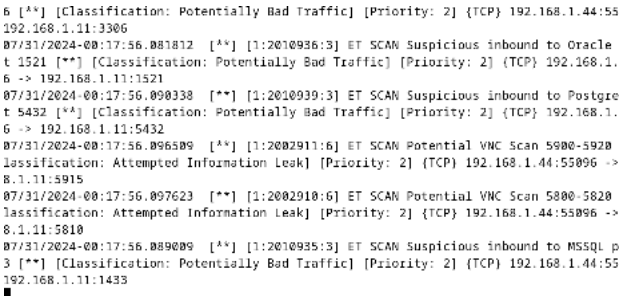
Gambar 11. *Flowchart* alur pengujian

Dalam pengujian ini *port scanning* dilakukan menggunakan dan memanfaatkan utilitas aplikasi nmap yang sudah diinstall di komputer yang digunakan sebagai penyerang. Karena menggunakan sistem operasi linux maka pengujian lewat terminal atau *command prompt* seperti pada gambar dibawah :



Gambar 12. Pengujian *Port Scanning* menggunakan Nmap

IDS suricata akan menampilkan hasil intrusi port scanning via terminal atau command prompt seperti pada gambar dibawah.

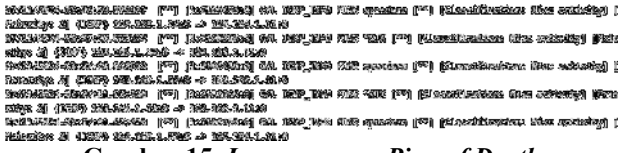


Gambar 13. *Log* seragan *Port Scanning* pada suricata

Pada Gambar 13 diatas menunjukkan *log* serangan dari *port scanning* yang dimana memiliki pesan "*ET SCAN Suspicious in bound*" yang berarti ET adalah singkatan dari *emerging threats* yaitu sebuah ancaman, *SCAN* menunjukkan kategori aktivitas pemindaian, sedangkan *Suspicious inbound* mengidentifikasikan bahwa lalu lintas mencurigakan datang dari luar jaringan. Selanjutnya pengujian dengan menggunakan metode serangan *ping of death* dengan **menggunakan** utility ping disebuah sistem operasi

Gambar 14. *Command* serangan *Ping of Death*

IDS suricata akan menampilkan hasil intrusi *ping of death* dengan menggunakan utilitas ping via terminal atau command prompt seperti pada gambar dibawah.

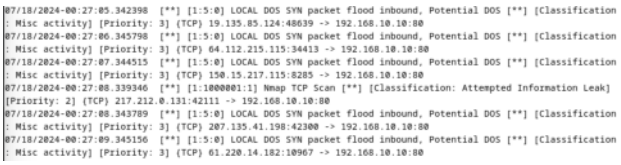


Gambar 15. *Log* serangan *Ping of Death*

Pengujian dengan menggunakan metode serangan *syn flood* dengan menggunakan tools hping.

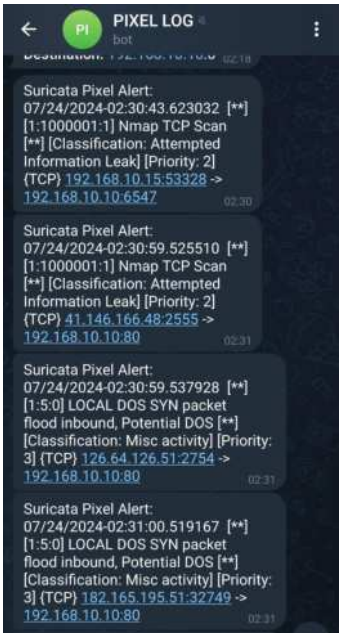
Gambar 16. Perintah serangan *Syn Flood*

IDS suricata akan menampilkan hasil serangan *syn flood* dengan menggunakan tools hping via terminal atau command prompt seperti pada gambar dibawah.



Gambar 17. *Log* serangan *Syn Flood*

Pada log peringatan diatas terdapat pesan "*LOCAL DOS SYN packet flood inbound, Potential DOS"* yang berarti indikasi serangan lokal yang sedang berlangsung, bahwa terdapat potensi serangan DOS paket syn yang bertujuan untuk membanjiri koneksi dan mencegah koneksi yang sah.



Gambar 18. Pemberitahuan di telegram

Tabel 1. Hasil pengujian Sistem

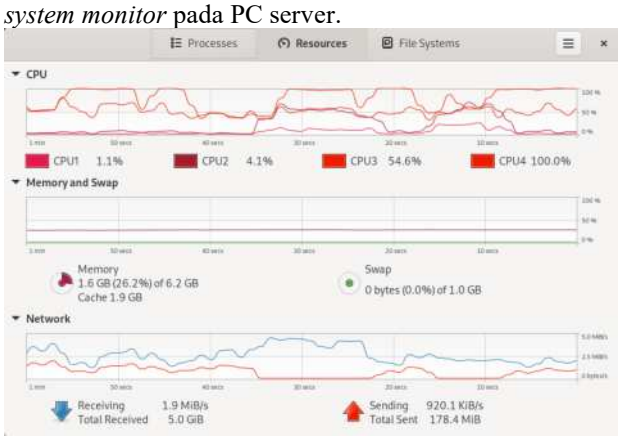
Serangan	Status
Port Scanning	Terdeteksi
Ping of Death	Terdeteksi
Syn Flood	Terdeteksi

4.3 TAARA

1. *Trigger*

Trigger merupakan tahapan awal dalam metode TAARA yakni sebagai pemicu untuk segera dilakukannya investigasi. Dalam skenario kasus

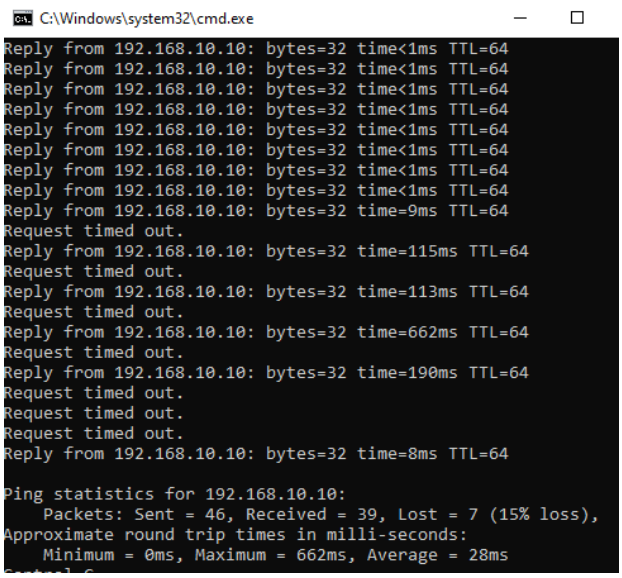
serangan DDoS, data log dari suricata menjadi pemicu untuk perlu dilakukannya investigasi, seperti yang terlihat pada gambar *resources* pada jendela *system monitor* pada PC server.



Gambar 19. Jendela *system monitor*

2. *Aqcquire*

Observasi lapangan berkaitan dengan *trigger* yang terjadi sehingga pendalaman terkait informasi apa saja yang dapat dikumpulkan. Dalam kasus ini beberapa informasi yang diberikan terkait dengan *trigger* yang terjadi pada server yang terindikasi mendapatkan serang DDoS. Berdasarkan informasi yang didapatkan dari beberapa PC Client, bahwa kecepatan jaringan dilaporkan ada penurunan bahkan sampai didapati terkendala RTO (*request time out)*.



Gambar 20. Trafik jaringan pada *Client*

3. *Analyze*

Analyze adalah tahap penyelidikan mendalam berdasarkan data akusisi. Dalam penelitian ini, data yang berhasil dikumpulkan dari tahapan sebelumnya menunjukkan terdapat beberapa file dalam bentuk .pcap yang dapat dianalisa baik menggunakan suricata atau alat bantu wireshark. Selanjutnya dengan dukungan pemberitahuan peringatan pada *tools* suricata, penulis melakukan analisis selanjutnya dengan file .pcap yang ada di dalam *directory* log.

Tabel 2. Total paket serangan

Time Stamp		Protokol	Jumlah Paket
First packet	Last packet		
18-07-2024 20:25:16	18-07-2024 20:37:49	ICMP	28961
18-07-2024 20:25:16	18-07-2024 21:09:35	SYN(80)	1055436

4. *Report*

Report adalah tahap penyusunan hasil analisis dan penyelidikan terhadap bukti-bukti dalam jaringan server. Tahapan ini akan menyajikan semua kegiatan yang dilakukan dari proses sebelumnya dalam bentuk laporan. Laporan memberikan informasi mengenai serangan, termasuk detail penyerang dan korban, dan dapat merekontruksi serangan saat insiden terjadi. Penulisan laporan mengenai serangan DDoS menggunakan kerangka kerja TAARA menjadi tujuan yang tidak kalah serius pada penelitian ini. Untuk memudahkan pemahaman isi laporan tahapan, maka temuan laporan paparan berdasarkan bukti penyerangan akan coba ditampilkan pada tabel dibawah.

Tabel 3. Report hasil investigasi

No.	Timestamp	Jenis serangan	Catatan
1	07/18/2024-00:25:16	Port Scanning	Terdapat Bukti peringatan pada log rules [Nmap TCP Scan]
2	07/18/2024-20:25:16	ICMP Flood	Bukti pada .pcap didukung dengan peningkatan kinerja pada CPU server
3	07/18/2024-21:09:35	Syn Flood	Bukti pada log serangan yang sebelumnya melakukan serangan port scanning pada port yang sama.

5. *Action*

Tahapan investigasi terakhir *Action*, dengan berdasarkan laporan investogator dapat melakukan evaluasi guna memperbaiki kerentanan dan mencegah adanya potensi serangan yang akan datang serta memberikan pernyataan untuk menjawab serangkaian insiden yang terjadi bahwa, telah terjadi sebuah insiden berupa serangan *Distributed Denial of*

Service dengan perangkat server sebagai target utama.

5. KESIMPULAN

Berdasarkan proses implementasi IDS Suricata dan hasil serta pembahasan dari proses forensika jaringan terhadap serangan *Distributed Denial of Service* menggunakan tahapan yang ada pada kerangka kerja TAARA, maka dapat ditarik kesimpulan yaitu :

1. Implementasi IDS suricata di server *Pixel Esport Arena* Samarinda mampu memberikan kemudahan dalam monitoring keamanan jaringan yang sebelumnya manual menjadi otomatis dengan notifikasi *bot* telegram.
2. IDS suricata pada server terbukti mampu meningkatkan keamanan jaringan dengan kustomisasi fitur *rules* sesuai dengan keinginan *administrator*.
3. Penggunaan alat bantu untuk menganalisa file .pcap dalam mendapatkan informasi tambahan pada serangan DDoS juga mampu menambah akurasi serta kekuatan bukti forensika terhadap serangan pada sistem jaringan.
4. Kerangka kerja TAARA digunakan dalam proses investigasi terhadap serangan DDoS menunjukkan bahwa TAARA dapat digunakan untuk membantu dalam proses investigasi pasca serangan terjadi.

6. SARAN

1. Penelitian selanjutnya diharapkan dapat lebih banyak mengkonfigurasikan *rules* pada pengujian serangan, dikarenakan ada beberapa *default rules* yang tidak mampu mendeteksi serangan ICMP flood dari sistem jaringan DHCP server.
2. Framework TAARA dapat dikembangkan kolaboratif dengan teknik-teknik AI untuk menjadi alat investigasi jaringan komputer yang dapat menangani berbagai jenis serangan selain DDoS.
3. Penelitian selanjutnya diharapkan dapat mengmbangkan potensi fitur *intrusion prevention system* (IPS) pada suricata guna memberikan solusi tepat agar dapat mengatasi dan mencegah serangan DDoS dengan optimal.

7. DAFTAR PUSTAKA

Afrianto, Y. dan A. H. Hendrawan. 2019. Implementasi Data Center Untuk Penempatan Host Server Berbasis Private Cloud Computing. *Krea-Tif*. Vol. 7, No. 1, h. 50.

Ayuningtyas, A. D. 2023. Deteksi Serangan Distributed Denial of Service (Ddos) Menggunakan Catboost Classifier. *Journal of Engineering Research*.

Hakim, Z. Al. 2022. Apa itu Virtual Machine (VM)? Dan Mengapa Harus Menggunakan VM? https://btech.id/en/news/apa-itu-virtual-machine-vm-dan-mengapa-harus-menggunakan-vm/, diakses 8 Mei 2024.

Haris, A. I., B. Riyanto, F. Surachman dan A. A. Ramadhan. 2022. Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika : Jurnal Sistem Komputer*. Vol. 11, No. 1, h. 67–76.

Hermawan, A., T. Hartati dan Y. A. Wijaya. 2022. Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. *Jurnal Informatika: Jurnal Pengembangan IT*. Vol. 7, No. 3, h. 125–130.

Rahman, R., M. S. Ariantini, A. Hadi, N. Hayati dan P. W. Gunawan. 2024. *Buku Ajar Keamanan Jaringan Komputer*. Efitra, ed. Jambi: PT. Sonpedia Publishing Indonesia.

Stephani, E., Fitri Nova dan E. Asri. 2020. Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*. Vol. 1, No. 2, h. 67–74.

Suprihadi, D. dan I. Magfira. 2023. Forensik Pada Jaringan Komputer Lokal Dengan Klasifikasi Svm Berbasis Framework Taara Universitas Kebangsaan Republik Indonesia. *Jurnal Review Pendidikan dan Pengajaran*. Vol. 7, No. 1, h. 666–673.

Syani, M. 2020. Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps). *Jurnal Inkofar*. Vol. 1, No. 1.

Valianta, S. A., T. Salim dan D. Stiawan. 2016. Identifikasi Serangan Port Scanning dengan Metode String Matching. *Annual Research Seminar (ARS)*. Vol. 2, No. Fakultas Ilmu Komputer Unsri, h. 466–471.

Walad, I. 2020. "Analisis Denial Of Service Attack Pada Sistem Keamanan Web". Universitas Sumatra Utara.