Implementation of Intrusion Detection System With Suricata on Ubuntu 22.04 LTS

Wahyat Wahyat [1,a] , ***Parlindungan Kudadiri*** [2,b]
[1] Informatics Engineering, Politeknik Negeri Bengkalis, Bengkalis, Indonesia
[2] Departemen of Information System,Universitas Sains dan Teknologi Indonesia, Pekanbaru, Indonesia
[a] wahyat@polbeng.ac.id, [b] parlindungan@usti.ac.id

Abstract—This study seeks to put into action and assess the effectiveness of a Suricata based Intrusion Detection System (IDS), on a Linux Ubuntu 22 04 operating system setup. Suricata was selected as the IDS for its features and strong performance, in identifying types of cyber threats. The execution procedure involves setting up Suricata through installation configuring it and conducting tests in a controlled setting. The efficiency assessment entails studying the detection accuracy alarm rate and response time of Suricata when confronted with attack scenarios. The findings, from the research are anticipated to enhance the protection of information systems that operate using Linux as their base platform.

Keywords : intrusion detection system, suricata, linux ubuntu

I. Introduction

In todays age, with its complexities rising each day rapidly and posing new challenges to information system security. The stakes are higher than ever before! The evolving landscape of cyber threats has put individuals and organizations at risk. Even poses a threat to nations! To tackle this issue head on we need a system that can proactively identify and thwart access attempts into the system. A key player, in this field is the Intrusion Detection System (IDS) (Syamsuddin & Barukab, 2022).

Intrusion Detection Systems (IDS) are created to observe network and system behavior to spot any signs of access or suspicious actions in order to give system administrators a heads up and enable them to take precautions before any serious harm is done by an attack.It's worth noting that Suricara is a used open source IDS that stands out for its adaptability and strong performance, in identifying a range of attacks – from basic ones, to more intricate security breaches (Nam & Kim, 2018)

Linux Ubuntu 22.04, as one of the most popular Linux distributions, provides a stable and secure environment for running applications, including Suricata. The combination of Suricata and Ubuntu 22.04 offers a reliable and easy-to-manage IDS solution (Fadhilah & Marzuki, 2020)

There has been a lot of research on Suricata-based IDS in the Linux environment (Santoso et al., 2022) shows that Suricata is able to detect various types of attacks with a high level of accuracy. compared Suricata's performance with other IDSs and showed Suricata's superiority in terms of detection speed. Discusses the customization of Suricata's detection rules to improve its ability to detect specific attacks. Examines the integration of Suricata with other security systems to form a more comprehensive defense. Evaluates Suricata's effectiveness in protecting systems from evolving attacks.

Tests will be carried out using Linux times with 3 test scenarios, including ICMP Ping attack, Port Scanning Attack and DDos Attack, intrusion detection system testing is successful if suricata is able to provide notification when an attack occurs (Anis et al., 2022)

II. Research Methodology

A. *Place and time of research*

This research was conducted in the computer network laboratory of the informatics engineering department of the Bengkalis state polytechnic, located at Jl. Bathin Alam, Sungai Alam Bengkalis Riau - 28711.

B. *SDLC Method*

The method used in this research is the *NDLC (Network Development Life Cycle)* method, while the cycle of stages is started by *Analysis, design, simulation, prototyping, implementation, monitoring* and *management*, the chart can be seen in the following figure.

.

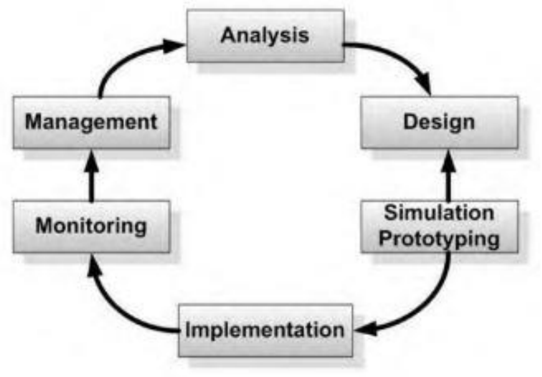


Figure 1. Method SDLC

C. Research stages

In order for the research implementation process to be directed and structured, the research stages start from data collection, analyzing the needs and design of the *Intrusion Detection System* (IDS), making the Intrusion *Detection* System, integration and implementation of the *Intrusion Detection System*, testing and analyzing test results, documenting and reporting research results. The research stages can be seen in the figure.

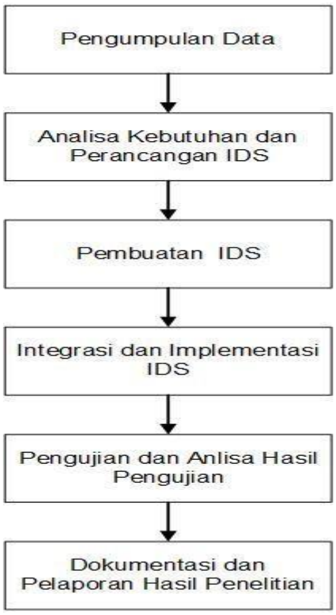

Pengumpulan Data
Analisa Kebutuhan dan Perancangan IDS
Pembuatan IDS
Integrasi dan Implementasi IDS
Pengujian dan Anlisa Hasil Pengujian
Dokumentasi dan Pelaporan Hasil Penelitian

Figure 2. *Research stages*

The stages of this research will be divided into several stages of research, namely, the initial stage is to collect the data needed to conduct research, in this case, looking for what data is needed to create an Intrusion Detection System design. Analyzing functional and non-functional requirements followed by the design of the *Intrusion Detection System*. After making the *Intrusion Detection System* design, the next step is installation and configuration, then testing and analyzing the results of the *Intrusion Detection System* design that has been made so that it functions properly when it will be implemented. Integrate and implement the *Intrusion Detection System* design on the local network.

D. Network topology

The *Intrusion Detection System (IDS)* topology applies the concept of *Client - Server* Network, the attacker's computer is connected to the *Suricata IDS server computer*.

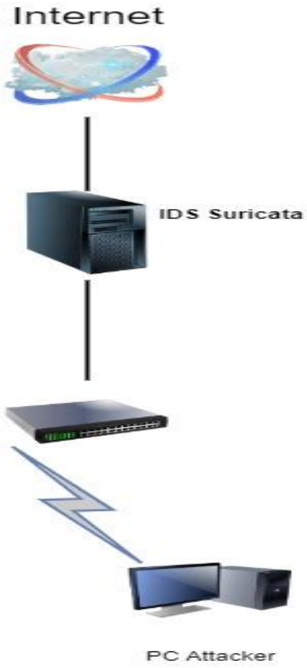


Figure 3. Network topology

III. Results and Discussion

A. Test scenario

in intrusion detection system research with suricata on linux ubuntu using 3 test scenarios namely:

1. ping attacks

2. port scanning

3. DDos attack

B. Rules Intrusion Detection System suricata

The following 3 rules are used in testing the intrusion detection system with suricata on linux ubuntu 22.04 LTS,

1. ICMP rules

```
alert icmp any any -> $HOME_NET any (msg:"Penyerangan ICMP Packets"; sid:123; rev:1;)
```

2. Scanning Port

```
alert tcp any any -> any [21,22,23,25,53,80,88,110,135,137,138,139,143,161,389,443,445,465,514,587,636,853,993,995,1194,1433,1720,3306,3389,8080,8443,11211,27017,51820](msg:"POSSBL PORT SCAN (NMAP -sS)"; flow:to_server,stateless;flags:S;window:1024; tcp.mss:1460; threshold:type threshold, track by_src, count 20, seconds 70; classtype:attempted-recon; sid:3400001; priority:2; rev:1;)

alert tcp any any -> any ![21,22,23,25,53,80,88,110,135,137,138,139,143,161,389,443,445,465,514,587,636,853,993,995,1194,1433,1720,3306,3389,8080,8443,11211,27017,51820](msg:"POSSBL PORT SCAN (NMAP -sS)"; flow:to_server,stateless;flags:S;window:1024;tcp.mss:1460;threshold:type threshold, track by_src, count 7, seconds135; classtype:attempted-recon; sid:3400002; priority:2; rev:2;)
```

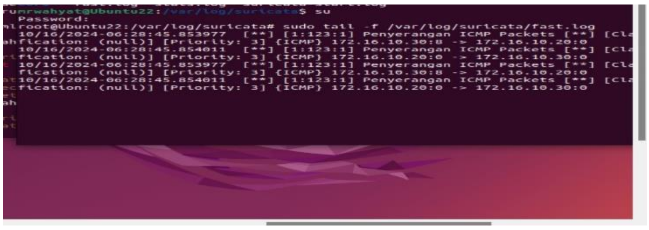
3. DDos Attack

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Attack DDoS SYN packet flood inbound, Potential DDoS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:5;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Attack DDoS SYN packet flood outbound, Potential DDoS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:6;)
```

C. Instrusion detection system suricata results

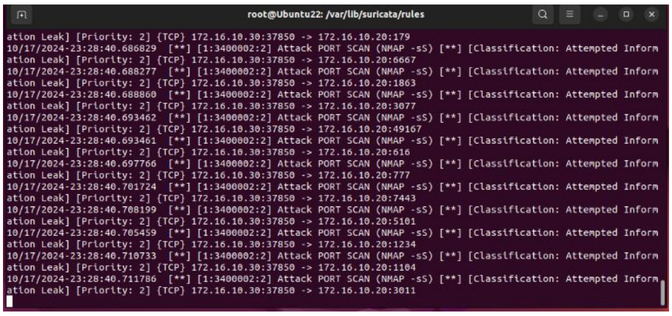
1. Ping Attack ICMP



```
mrwahyat@Ubuntu22:/var/log/suricata$ su
 Password:
root@Ubuntu22:/var/log/suricata# sudo tail -f /var/log/suricata/fast.log
 10/16/2024-06:28:45.853977  [**] [1:123:1] Penyerangan ICMP Packets [**] [Cla
fication: (null)] [Priority: 3] {ICMP} 172.16.10.30:8 -> 172.16.10.20:0
 10/16/2024-06:28:45.854011  [**] [1:123:1] Penyerangan ICMP Packets [**] [Cla
fication: (null)] [Priority: 3] {ICMP} 172.16.10.20:0 -> 172.16.10.30:0
 10/16/2024-06:28:45.853977  [**] [1:123:1] Penyerangan ICMP Packets [**] [Cla
fication: (null)] [Priority: 3] {ICMP} 172.16.10.30:8 -> 172.16.10.20:0
 10/16/2024-06:28:45.854011  [**] [1:123:1] Penyerangan ICMP Packets [**] [Cla
fication: (null)] [Priority: 3] {ICMP} 172.16.10.20:0 -> 172.16.10.30:0
```

Figure 4. Alert Ping ICMP Attack

2. Port Scanning

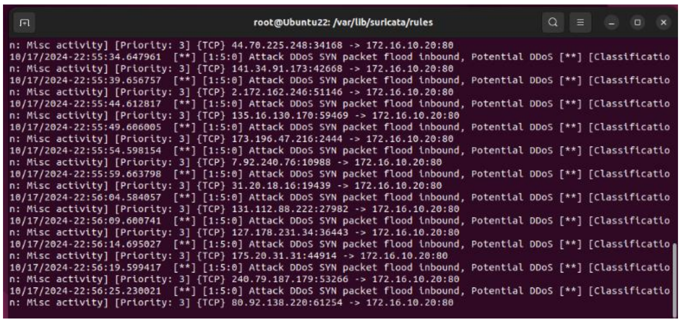


root@Ubuntu22: /var/lib/suricata/rules

```
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:179
10/17/2024-23:28:40.686829  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:6667
10/17/2024-23:28:40.688277  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:1863
10/17/2024-23:28:40.688860  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:3077
10/17/2024-23:28:40.693462  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:49167
10/17/2024-23:28:40.693461  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:616
10/17/2024-23:28:40.697766  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:777
10/17/2024-23:28:40.701724  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:7443
10/17/2024-23:28:40.708199  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:5101
10/17/2024-23:28:40.705459  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:1234
10/17/2024-23:28:40.710733  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:1104
10/17/2024-23:28:40.711786  [**] [1:3400002:2] Attack PORT SCAN (NMAP -sS) [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 172.16.10.30:37850 -> 172.16.10.20:3011
```

Figure 5. Alert Port Scanning Attack

3. DDos Attack



root@Ubuntu22: /var/lib/suricata/rules

```
n: Misc activity] [Priority: 3] {TCP} 44.70.225.248:34168 -> 172.16.10.20:80
10/17/2024-22:55:34.647961  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 141.34.91.173:42668 -> 172.16.10.20:80
10/17/2024-22:55:39.656757  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 2.172.162.246:51146 -> 172.16.10.20:80
10/17/2024-22:55:44.612817  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 135.16.130.170:59469 -> 172.16.10.20:80
10/17/2024-22:55:49.606005  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 173.196.47.216:2444 -> 172.16.10.20:80
10/17/2024-22:55:54.598154  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 7.92.240.76:10988 -> 172.16.10.20:80
10/17/2024-22:55:59.663798  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 31.20.18.16:19439 -> 172.16.10.20:80
10/17/2024-22:56:04.584057  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 131.112.88.222:27982 -> 172.16.10.20:80
10/17/2024-22:56:09.600741  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 127.178.231.34:36443 -> 172.16.10.20:80
10/17/2024-22:56:14.695027  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 175.20.31.31:44914 -> 172.16.10.20:80
10/17/2024-22:56:19.599417  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 240.79.187.179:53266 -> 172.16.10.20:80
10/17/2024-22:56:25.230021  [**] [1:5:0] Attack DDoS SYN packet flood inbound, Potential DDoS [**] [Classificatio
n: Misc activity] [Priority: 3] {TCP} 80.92.138.220:61254 -> 172.16.10.20:80
```

Figure 6. Alert DDoS Attack

D. Test scenario results table

The following are the results of 3 Intrusion detection system test scenarios with Suricata on linux ubuntu 22.04 LTS

Table 1. Test results of 3 scenarios

No	Type Of Attack	Alert	Date
1.	Attack Ping ICMP	It works	October 16, 2024
2.	Attack Scanning Port	It works	October 16, 2024
3.	DDoS Attack	It works	October 16, 2024

IV Conclusion

From the results of system design and testing, it can be concluded that:

1. Implementation of intrusion detection system with suricata on linux ubuntu 22.04 LTS successfully testedIn this part suggestions can also be included

2. Accuracy Rate Suricata generally shows a high accuracy rate in detecting various types of network attacks, ranging from simple to complex attacks.

3. Suricata is able to detect various types of attacks such as : Ping ICMP attack, Port Scanning Attack and DDoS Attack.

Acknowledgement

Thank you to the Bengkalis State Polytechnic computernetwork laboratory team for their support so that the Intrusion Detection System research with Suricata on linux Ubuntu 22.04 is complete.

References

[1] Anis, M., Hilmi, A., & Khujaemah, E. (2022). Network Security Monitoring With Intrusion Detection System. *Jurnal Teknik Informatika (JUTIF)*, *3*(2), 249–253. https://doi.org/10.20884/1.jutif.2022.3.2.117

[2] Fadhilah, D., & Marzuki, M. I. (2020). Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines against Dos/DDoS Attacks. *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering, BCWSP 2020*, *March 2015*, 157–162. https://doi.org/10.1109/BCWSP50066.2020.9249449

[3] Nam, K., & Kim, K. (2018). A Study on SDN security enhancement using open source IDS/IPS Suricata. *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*, 1124–1126. https://doi.org/10.1109/ICTC.2018.8539455

[4] Santoso, D., Noertjahyana, A., & Andjarwirawan, J. (2022). Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS. *Jurnal Infra*, *10*(1), 1–6.

[5] Syamsuddin, I., & Barukab, O. M. (2022). SUKRY : Suricata IDS with Enhanced kNN Algorithm on. *Electronics*, *11*(737).