

Implementation of Intrusion Detection System (IDS) and Snort Community Rules to Detect Types of Network Attacks

Tri Widodo

Department of Information Technology Education
Universitas Teknologi Yogyakarta
Yogyakarta of Indonesia

Adam Sekti Aji

Department of Informatics
Universitas Teknologi Yogyakarta
Yogyakarta of Indonesia

ABSTRACT

Intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered. Administrators can certainly implement firewalls on managed networks, but not necessarily implement IDS. IDS has a detection function, so administrators will get notifications when there are activities that are prohibited based on IDS rules. IDS rules can be set by the administrator from scratch, one by one, but administrators can also use IDS rules provided by some security sites. In this study, a network topology that is integrated with IDS will be used and implemented various rules on the IDS. The operating system used is Ubuntu and the IDS used is Snort. The IDS rules are taken from the community rules on www.snort.org. Based on the tests and simulations on the IDS, the conclusions are: IDS is effective in detecting the activity of network attacks aimed at the server and Community rules provided by the official Snort website contain rules that can be used to anticipate network attacks. Further research is expected to be able to collaborate on network security applications with artificial intelligence or machine learning applications. Research that combines computer network security applications and artificial intelligence or machine learning can improve computer network security because it is able to analyze computer network attacks or malware based on certain patterns

Keywords

Keywords Intrusion detection system (IDS), Snort Community Rule, Network Attack

1. INTRODUCTION

Intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered [1]. implementation of IDS (Intrusion Detection System) as part of computer network protection is still little used. Administrators can certainly implement firewalls on managed networks, but not necessarily implement IDSs. This is because IDS is more passive, in contrast to a firewall that actively blocks various activities that are considered harmful to computer networks. IDS has a detection function, so administrators will get notifications when there are activities that are prohibited based on IDS rules. This IDS rule is the basis for IDS in identifying allowed activities and activities that are not allowed. IDS in addition to providing notifications will also record all activities through the network. IDS logs or records are very important and useful for administrators to find out client behavior and security vulnerabilities in managed networks. IDS rules can be set by the administrator from scratch, one by one, but administrators can also use IDS rules provided by some security sites. In this

study, researchers will use the IDS rule provided by <https://www.snort.org/downloads/community/community-rules.tar.gz>. Researchers will analyze the IDS rules so that it can be seen what types of rules and violations can be detected based on the IDS rules. This research is very important to be done to ensure that the IDS rules are used effectively and efficiently to prevent and detect network attacks.

2. STUDY LITERATURE

2.1 Previous Study

Previous study conducted by (Suhartono and Patta, 2017) with the title Server Admin Network Security System with the Snort Intrusion Detection System (IDS) Method Using the ClearOS Operating System. This study tries to simulate the installation of Snort as an IDS to detect network attacks through two network ports, namely, SSH and FTP [2].

Previous research was conducted by (Jacob and Wanjala, 2017) with the title A Review of Intrusion Detection Systems. This study reviews IDS starting from the definition, types of IDS and how effective the use of IDS is in general. This study also discusses in detail how IDS can detect network attacks [3].

Previous research was conducted by (Taasneem, Kumar, and Sharma, 2018) with the title Intrusion Detection Prevention System using SNORT. In general, this research only discusses IDS and IPS. This study also discusses how IDS can identify network attacks either through Anomaly based Methodology and Signature based Methodology [4].

Previous research was conducted by (Sandi and Arrofiq, 2018) with the title Implementation of Snort-Based NIDS Analysis Using the Fuzy Method to Overcome LoRaWAN Attacks. This research focuses on Snort testing to detect network attacks on Long Range Wide Area Network (LoRaWAN) [5].

Previous research was conducted by (Alamsyah, Riska and Akbar 2020) with the title Network Security Analysis Using a Network Intrusion Detection and Prevention System. This study uses IDS Suricata to detect computer network attacks. This study also provides examples of simulated attacks detected on existing IDS interfaces [6].

Previous research was conducted by (Ardiyasa, 2019) with the title Network Forensic Analysis Application for Analysis of Attacks on Syslog Servers [7].

Previous research was conducted by (Lukman and Suci, 2020) with the title Comparative Analysis of the Performance of Snort and Suricata as Intrusion Detection Systems in Detecting Syn Flood Attacks on Apache Web Servers [8].

Previous research was conducted by (Purba and Efendi, 2021), with the title Design and Analysis of Computer Network Security Systems using SNORT. This research also

focuses on DDOS attacks (Purba & Efendi, 2021). The fourth study is almost the same as the second study, namely using IDS to detect DDOS attacks [9].

This study aims to determine the effectiveness of IDS in identifying and recognizing network attacks. In addition, this study also aims to find out how the IDS rules work developed by the community on the official Snort website page. This community-based rule can make it easier for IDS Snort users without having to create their own rules.

2.2 Intrusion Detection System

An intrusion detection system (IDS) are devices or software's that are used to monitors networks for any unkind activities that bridge the normal functionality of systems hence causing some policy violation [3].

2.3 Snort

Snort is that the form of the Intrusion Detection System that's used for scanning databases flowing on the network [10]. Snort logically divided into multiple components. Snort logically divided into multiple parts. These parts work along to find specific attacks and generate output into a needed format from the detection system [10]. Snort's components are: packet decoder, preprocessors, detection engine, logging and alerting systems, and output modules [10].

2.4 Snort Rule

Snort utilizes existing rules, which are patterns of known attacks for searching and matching the network traffic data[11]. If an abnormal behavior pattern is detected it generates an alert. The structure of Snort rules consists of two

logical parts. The first part is the rule header, while the second is the rule option [11].

3. METHODOLOGY

3.1 Research Tools

The research tools used for this research are

1. Virtual Box
2. Ubuntu Operating System
3. Snort Intrusion Detection System
4. Snort Community rules

3.2 Research Stages

The research methodology used in writing this research is as follows:

3.2.1 Analysis

Analysis is used to find and collect material from various references related to IDS and network attacks. This analysis stage is also used to identify the network topology used to perform simulations and experiments.

3.2.2 Network design

Design a network topology that integrates IDS and implements various rules on IDS. In this study, the operating system used is Ubuntu and the IDS used is Snort. IDS rules are taken from <https://www.snort.org/downloads/community/community-rules.tar.gz4> [12]. The network topology that will be used in the research is as shown in the Figure 1.

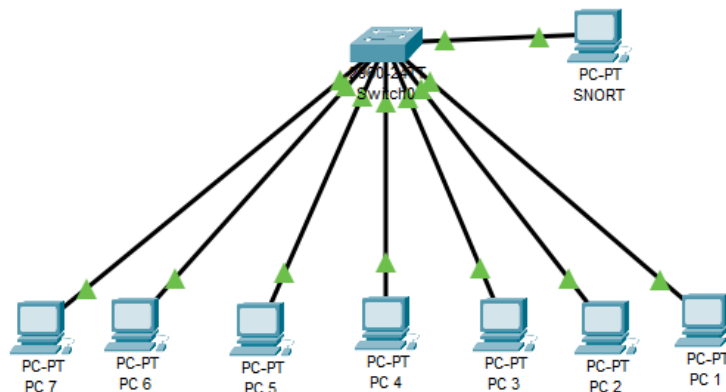


Fig 1: Network topology for research

3.2.3 Implementation

The network topology design is implemented on a virtual box virtual machine using the Ubuntu operating system. then install IDS Snort on Ubuntu. Snort Community rules are then added to the installed Snort IDS. The community rules used are the community rules provided on the Snort IDS official website.

3.2.4 Simulation and testing

Simulating various attacks on the IDS-integrated server. Then testing is done to determine the effectiveness of the IDS based on the rules that have been configured on the IDS.

4. RESULTS AND DISCUSSION

4.1 Implementation of Snort Community Rules on IDS

The configuration and addition of community rules is done after all the IDS installation and network configuration processes have been completed. Community rules are then installed and added to Snort IDS. Rules configuration results can be seen in Figure 2

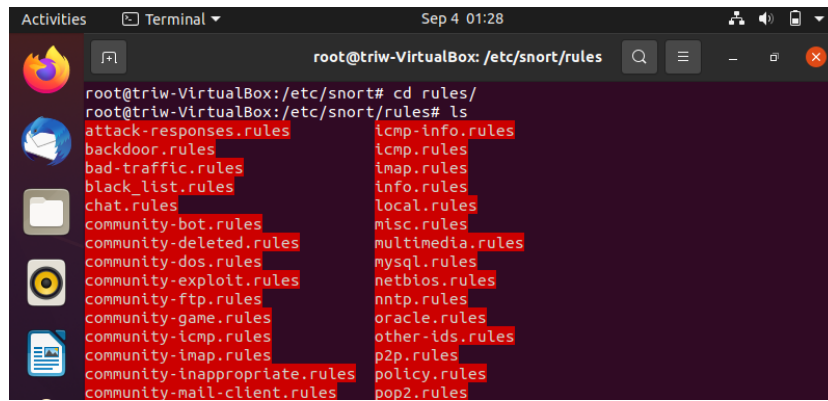


Fig 2: IDS community rules installed on snort

The community rules provided on the official page of the snort website show number of very complete rules to anticipate various attack models on the server. Various rules

to detect these attacks are specifically set in each section of the rule file. In detail these rules can be grouped into several types of attacks as shown in Table 1.

Table 1. IDS rules design by community

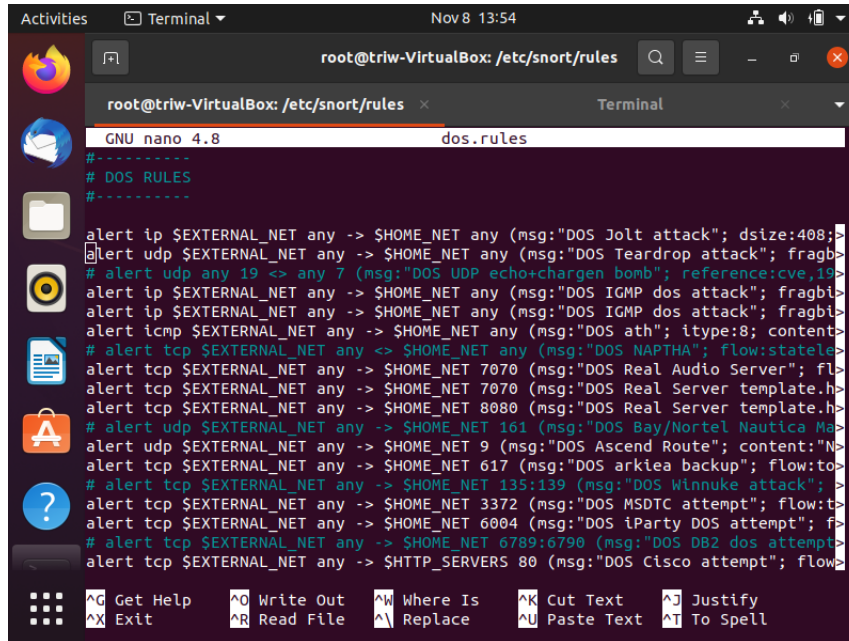
Rules by category		
Rules for detecting attacks via network protocols	Rules to detect Virus and Malware attacks	Rules for detecting attacks via web services
attack-responses.rules icmp-info.rules icmp.rules bad-traffic.rules p2p.rules community-dos.rules community-ftp.rules nntp.rules community-icmp.rules other-ids.rules community-imap.rules pop2.rules pop3.rules rpc.rules rservices.rules scan.rules smtp.rules snmp.rules telnet.rules tftp.rules ddos.rules ftp.rules dos.rules dns.rules community-nntp.rules community-sip.rules imap.rules community-smtp.rules	community-virus.rules backdoor.rules virus.rules exploit.rules	info.rules chat.rules local.rules community-bot.rules misc.rules community-deleted.rules multimedia.rules community-exploit.rules netbios.rules community-game.rules oracle.rules community-inappropriate.rules policy.rules community-mail-client.rules community-misc.rules porn.rules community-oracle.rules community-policy.rules shellcode.rules community-sql-injection.rules black_list.rules mysql.rules community-web-attacks.rules sql.rules community-web-cgi.rules community-web-client.rules community-web-dos.rules community-web-iis.rules web-attacks.rules community-web-misc.rules web-cgi.rules community-web-php.rules web-client.rules web-coldfusion.rules deleted.rules web-frontpage.rules web-iis.rules web-misc.rules experimental.rules web-php.rules white_list.rules finger.rules x11.rules

4.2 Intrusion Detection System (IDS) Detects Network Attacks

Based on the community rules in table 1, it can be seen that Snort can detect a variety of different attack techniques, such as port scanning, smurf attacks, UDP flooding, spoofing, DoS (Denial of Service), DDoS (Distributed Denial of Service),

DNS poisoning, trojan horses, SQL injection, PHP injection, script kiddies, viruses and malware, pornography and various cyber attacks.

Snort rules can also prevent access to certain websites that are included in the black list website .

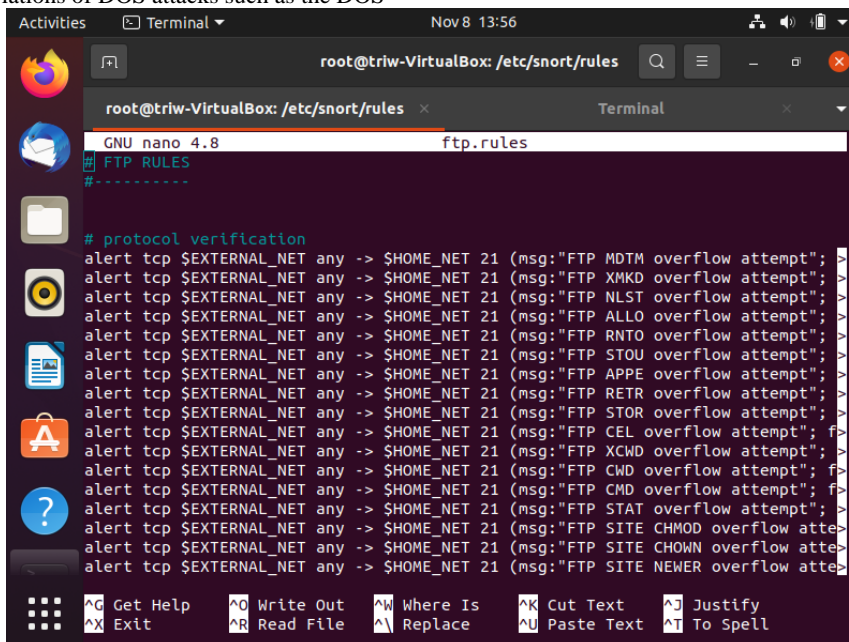


```
root@triv-VirtualBox: /etc/snort/rules
GNU nano 4.8 dos.rules
#-----
# DOS RULES
#-----
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Jolt attack"; dsize:408;
alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Teardrop attack"; fragb
# alert udp any 19 <-> any 7 (msg:"DOS UDP echo+chargen bomb"; reference:cve,19
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS IGMP dos attack"; fragbt
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS IGMP dos attack"; fragbt
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS ath"; itype:8; content
# alert tcp $EXTERNAL_NET any <-> $HOME_NET any (msg:"DOS NAPTHA"; flow:statele
alert tcp $EXTERNAL_NET any -> $HOME_NET 7070 (msg:"DOS Real Audio Server"; fl
alert tcp $EXTERNAL_NET any -> $HOME_NET 7070 (msg:"DOS Real Server template.h
alert tcp $EXTERNAL_NET any -> $HOME_NET 8080 (msg:"DOS Real Server template.h
# alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"DOS Bay/Nortel Nautica Ma
alert udp $EXTERNAL_NET any -> $HOME_NET 9 (msg:"DOS Ascend Route"; content:"N
alert tcp $EXTERNAL_NET any -> $HOME_NET 617 (msg:"DOS arkiea backup"; flow:to
# alert tcp $EXTERNAL_NET any -> $HOME_NET 135:139 (msg:"DOS Winnuke attack"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 3372 (msg:"DOS MSDTC attempt"; flow:to
alert tcp $EXTERNAL_NET any -> $HOME_NET 6004 (msg:"DOS iParty DOS attempt"; f
# alert tcp $EXTERNAL_NET any -> $HOME_NET 6789:6790 (msg:"DOS DB2 dos attempt
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"DOS Cisco attempt"; flow
```

Fig 3: Example rule to detect DOS attack

In the Figure 3, it can be seen that the DOS rule has anticipated various variations of DOS attacks such as the DOS

Jolt attack, DOS teardrop attack and others.



```
root@triv-VirtualBox: /etc/snort/rules
GNU nano 4.8 ftp.rules
#-----
# FTP RULES
#-----
# protocol verification
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MDTM overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XMKD overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP NLST overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP ALLO overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNTD overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOU overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP APPE overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RETR overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOR overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CEL overflow attempt"; f
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XCWD overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CMD overflow attempt"; f
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CMD overflow attempt"; f
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STAT overflow attempt"; >
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHMOD overflow atte
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHOWN overflow atte
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE NEWER overflow atte
```

Fig 4: Example rule to detect FTP attack

The Figure 4 also shows a complete FTP rule to anticipate various variations of FTP-based attacks. The FTP rule has been configured to detect FTP attacks that use MTDM overflow, XMKD overflow, NSLT overflow and various other attacks.

after implementing the rules on snort, then an experiment was carried out for some initial attacks on the server. IDS Snort detects various attacks based on predefined rules. Snort provides alerts or warnings to administrators regarding certain attacks or access to the network as shown in Figure 5

```

root@triw-Vi... x root@triw-Vi... x root@triw-Vi... x root@triw-Vi... x
ty: 0] [ICMP] 192.168.56.103 -> 192.168.56.1
09/04-01:42:46.620316 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Att
empted Information Leak] [Priority: 2] [TCP] 192.168.56.1:45697 -> 192.168.56.1
03:22
09/04-01:42:46.722807 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Att
empted Information Leak] [Priority: 2] [TCP] 192.168.56.1:45697 -> 192.168.56.1
03:22
09/04-01:42:46.825562 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Att
empted Information Leak] [Priority: 2] [TCP] 192.168.56.1:45697 -> 192.168.56.1
03:22
09/04-01:42:46.842373 [**] [1:1000002:0] Ada yang ECHO PING [**] [Priority: 0]
[ICMP] 192.168.56.104 -> 192.168.56.103
09/04-01:42:46.842452 [**] [1:1000003:0] Ada yang ECHO REPLY PING [**] [Priori
ty: 0] [ICMP] 192.168.56.103 -> 192.168.56.104

```

Fig 5: Alert Message from IDS

When the administrator receives an alert or alarm from the IDS. Administrators can follow up with some Actions, such as

blocking ports as shown in figure 6, Blocking IP, or disabling some protocols.

```

root@triw-VirtualBox:/home/triw# ufw deny 23/tcp
Rule updated
Rule updated (v6)

```

Fig 6: Firewall configuration changes to block certain ports

Administrators can also follow up by changing some rules to

optimize network security, as shown in Figure 7.

```

root@triw-VirtualBo... x root@triw-VirtualBo... x root@triw-VirtualBo... x
GNU nano 4.8 local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
#percobaan rule baru
log tcp any any -> 192.168.56.0/24 !6000:6010
alert tcp any any -> 192.168.56.103 23 (msg: "Ada yang telnet ke mesin!"; sid:>
alert icmp any any <> 192.168.56.103 any (msg:"Ada yang ECHO PING"; icode:0; i>
alert icmp any any <> 192.168.56.103 any (msg:"Ada yang ECHO REPLY PING"; icod>

```

Fig 7: Rule update to detect network attacks

All network activity will be recorded by IDS Snort on logs as shown in Figure 8. network administrators can perform analysis on IDS logs to view details of network activity as

well as view details of network attacks. IDS log analysis results can be used by administrators to improve the security of managed computer networks.

```

root@triw-VirtualBox:/var/log/snort/snortlogs# ls -l
total 308184
-rw-r--r-- 1 root snort 0 Sep 4 01:21 alert
-rwsrwxr-t 1 root snort 787 Sep 1 17:16 snort.log.1630491357
-rw----- 1 root snort 1899 Sep 1 17:43 snort.log.1630492975
-rw----- 1 root snort 50641079 Sep 2 17:07 snort.log.1630566064
-rw----- 1 root snort 129963719 Sep 4 01:23 snort.log.1630689641
-rw----- 1 root snort 134216566 Sep 4 01:52 snort.log.1630694117
-rw----- 1 root snort 730999 Sep 4 02:55 snort.log.1630695145

```

Fig 8: Snort IDS Log that records network activity

5. CONCLUSION

Based on the tests and simulations on the IDS, the conclusions are:

1. IDS is effective in detecting the activity of network attacks aimed at the server
2. Community rules provided by the official Snort website contain rules that can be used to anticipate network attacks
3. Further research is expected to be able to collaborate on network security applications with artificial intelligence or machine learning applications. Research that combines computer network security applications and artificial intelligence or machine learning can improve computer network security because it is able to analyze computer network attacks or malware based on certain patterns.

6. REFERENCES

- [1] Lutkevich, B. (2021, October 7). *What is An Intrusion Detection System (IDS)? Definition from Searchsecurity*. SearchSecurity. Retrieved November 9, 2021, from <https://searchsecurity.techtarget.com/definition/intrusion-detection-system>
- [2] Suhartono, S., & Patta, A. R. (2017). Admin Server Network Security System with The Snort Intrusion Detection System (IDS) Method Using the ClearOS Operating System. *Teknologi Elekerika Journal*, 14(2), 145. <https://doi.org/10.31963/elekerika.v14i2.1220>
- [3] Jacob, N.M, & Wanjala, M.Y. (2017). A Review of Intrusion Detection Systems. *Global Journal of Computer Science and Technology*, 17(3), 10.

- [4] Tasneem, A., Kumar, A., & Sharma, S. (2018). Intrusion Detection Prevention System Using Snort. *International Journal of Computer Applications*, 181(32), 21–24. <https://doi.org/10.5120/ijca2018918280>
- [5] Sandi, D. V., & Arrofiq, M. (2018). Implementation of Snort-Based NIDS analysis with the Fuzy Method To Overcome Lorawan Attacks. *RESTI Journal (Rekayasa Sistem Dan Teknologi Informasi)*, 2(3), 685–696. <https://doi.org/10.29207/resti.v2i3.504>
- [6] Alamsyah, H., -, R., & Al Akbar, A. (2020). Network Security Analysis Using a Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, 5(1), 17. <https://doi.org/10.31328/jointecs.v5i1.1240>
- [7] Ardiyasa, I. W. (2019). Forensic Network Analysis Application for Attack Analysis on Syslog Server. *RESEARCH: Computer, Information System & Technology Management*, 2(2), 59. <https://doi.org/10.25273/research.v2i02.5220>
- [8] Lukman, L., & Suci, M. (2020). Comparative Analysis of the Performance of Snort and Suricata as an Intrusion Detection System in Detecting SYN Flood Attacks on the Apache Web Server. *Respati*, 15(2), 6. <https://doi.org/10.35842/jtir.v15i2.343>
- [9] Purba, W. W., & Efendi, R. (2021). Design and Analysis of Computer Network Security Systems Using Snort. *AITI*, 17(2), 143–158. <https://doi.org/10.24246/aiti.v17i2.143-158>
- [10] Erlansari, A., Coastera, F. F., & Husamudin, A. (2020). Early Intrusion Detection System (IDS) Using Snort and Telegram Approach. *SISFORMA*, 7(1), 21. <https://doi.org/10.24167/sisforma.v7i1.2629>
- [11] Khamphakdee, N., Benjamas, N., & Saiyod, S. (2015). Improving Intrusion Detection System Based on Snort Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining. *Journal of ICT Research and Applications*, 8(3), 234–250. <https://doi.org/10.5614/itbj.ict.res.appl.2015.8.3.4>
- [12] Snort rules and IDS software download. (n.d.). Retrieved November 9, 2021, from <https://www.snort.org/downloads>.