Deployment of Snort Intrusion Detection System on Usmanu Danfodiyo University Network

Muazu Dalhatu Sifawa
Management Information SystemDepartment, UsmanuDanfodiyo University , Sokoto-, Nigeria
Email: dalhatu.muazu@udusok.edu.ng
Bello Alhaji Buhari
Department of Computer Science, Usmanu Danfodiyo University, Sokoto - Nigeria
Email: buhari.bello@udusok.edu.ng
Lawal Sulaiman
Department of Computer Science, Usmanu Danfodiyo University, Sokoto - Nigeria
Email: lawal.sulaiman@udusok.edu.ng

---**ABSTRACT**---

The increasingly frequent attacks on Internet visible systems are attempts to breach or compromise the security of those systems. Network security issues have been a major challenge on Usmanu Danfodiyo University networks for a long time. Intrusion detection system allows organizations to protect themselves from losses associated with network security challenges. The aim and objectives of this project is to deploy and evaluate the performance of SNORT-IDS system in safeguarding demilitarize zone network segment of Usmanu Danfodiyo University. SNORT-IDS were implemented using some various tools such as Snort Application, Pulledpork, Barnyard, Apache, MySQL, PHP, BASE, and ADODB. The result obtained from the system evaluation indicates that Snort-ids system is able to detect suspicious trafficby 97%.

Keywords – **Intrusion detection system, Snort, Network Security, University, Usmanu Danfodiyo University.**

Date of Submission: Jun 18, 2022 Date of Acceptance: Aug 29, 2022

I. INTRODUCTION

Systems and networks are subject to electronic attacks. Today's information systems in government and commercial sectors are distributed and highly interconnected via local area and wide area networks. While indispensable, these networks provide potential avenues of attack by hackers, international competitors, and other adversaries. The increasingly frequent attacks on Internet visible systems are attempts to breach or compromise the security of those systems. Intrusion detection technology allows organizations to protect themselves from losses associated with network security problems. Intrusion Detection System (IDS) are Hardware and Software Systems that monitor events which occurred on computers and computer networks in order to analyze security problems. IDS have become a key component in ensuring the safety of systems and networks. Intrusions to computer networks are called ''attacks" and these attacks threaten the security of networks by violating privacy, integrity and accessibility mechanisms. Attacks can originate from users who login to the computer using Internet trying to gain administrator rights and other users who misuse the rights they have. IDSs automate monitoring and analyzing the attacks [1]. Intrusion detection systems are classified as either signature-based or anomaly-based. Signature-based schemes (also called as misuse-based) seek to defined patterns, or signatures, within the analyzed data. Anomaly-based IDSs analyses abnormal activities and flag these activities as attacks.

Snort intrusion detection system (IDS) combines both the benefits of signature-based and anomaly-based inspection. Snort is an open-source network intrusion detection and prevention system (IDS/IPS) developed by Sourcefire. It is the most widely deployed IDS/IPS technology worldwide because it is free and open-source application. With over 4 million of downloads and over 500,000 registered users; It has become the de facto standard for IDS/IPS. Snort's network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. With the vast features of Snort and the meager university budget on IT infrastructure and software, Usmanu Danfodiyo University can utilize the benefit of Snort to safeguard their network with minimal cost.

Usmanu Danfodiyo University network is designed using fiber optic-based backbone comprising of three rings on the 3 campuses: Permanent Site, City Campus, and

College of Health Sciences (UDUTH) all the three campuses are connected. The network runs on Cisco and juniper Devices (Router, Firewall, CORE Switch, DMZ (demilitarize Zone) Switch, Split Switch, and Transparent Switch). The University Network is divided into two segments (LAN & DMZ network). All University client machines are connected to LAN network segment on CORE-Switch. However, all University Servers that hosted their services which are accessible in and outside their network are connected to DMZ (demilitarize Zone) Network segment.

Network security issues have been a major challenge on Usmanu Danfodiyo University networks for a long time. University networks are protected from malicious hackers using firewall. However, firewall does not have the ability to detect hostile intent or identify types of attack on allowed services. All the University Servers are on DMZ (demilitarize Zone) network and all their services are hosted on to these servers. These services are being public to everyone connected to the Internet. Therefore, these servers can anytime be compromise by hackers that may lead to the breach of their security.

In this Paper, Snort Intrusion Detection System (Snort-IDS) will be deployed on demilitarize Zone (DMZ) network segment of Usmanu Danfodiyo University to help in detecting any suspicious traffic thereby safeguarding their servers.

II. RELATED WORKS

Several researchers have proposed different approaches and models to address the various types of security breaches of computer network and computer systems. Some previous works reviewed are presented as follows:

Sasikumar in [2] proposed Network Intrusion Detection and Deduce System (NIDDS). It detects the attack using a a low-powered computer called Raspberry Pi It gives successive updating of the mark information to the data set in genuine world and gives notification if there is any interruption.

Niemiec et al. in [3] presented a new multivariable heuristic intrusion detection algorithm based on different types of flags and values of entropy. They proposed default values for parameters of a heuristic algorithm and values regarding detection thresholds. Their solution has been implemented in a well-known, open-source system and verified with a series of tests and investigated how updating the variables affects the intrusion detection process.

Xu et al. in [4] presented a modern service model for OpenStack clouds called Network Intrusion Detection System as a Service (NIDSaaS). They implemented a prototype of NIDSaaS and evaluated it on a multi-node OpenStack testbed. their evaluation results show that NIDSas outperforms existing VM-based NIDS service approach substantially in terms of service launch time and resource usage.

Hamsaveni in [5] identified the number of hopeful algorithms and provides an outline of recent developments in the single keyword pattern matching for IDS. The proposed Logo Pattern Matching algorithm is compared with the exiting algorithms and the result shows that the algorithm is faster and more reliable in network security applications. The results of algorithm show an improvement in average comparing, faster than the original algorithms, less character comparison and performs less number of attempts compared to the exiting algorithms.

Anthi et al in [6] proposed a three-layer Intrusion Detection System (IDS) that apply a supervised method to detect a range of popular network based cyber-attacks on IoT networks. The system is evaluated within a smart home testbed consisting of 8 popular commercially available devices. They demonstrates that the proposed architecture can automatically differentiate between IoT devices on the network, whether network activity is malicious or benign, and detect which attack was deployed on which device connected to the network successfully.

Li et al in [7] developed CBSigIDS. It is a generic framework of collaborative blockchained signature-based IDSs that incrementally build and update a trusted signature database in a collaborative IoT environment. Their results demonstrate that CBSigIDS can enhance the robustness and effectiveness of signature-based IDSs under adversarial scenarios.

Alsakran et al in [8] proposed an experimental evaluation between the widely used open-source NIDSs namely Snort, Suricata and Bro IDS to find the most suitable one for smart homes in term of detection accuracy and resources consumption including CP and memory utilization. They use dockers to show that each system had its strengths and weaknesses Their experiment results show that Suricata is the best performing NIDS for smart homes.

Garg in [10] proposed a hybrid intrusion detection system using SNORT in a Campus environment. In this system a new algorithm called pre-processor is added to the Snort detection engine to find the detection anomalies. This engine filters all the files and loads the attacked or infected files into its loader by .conf file command. The system is design using some tools (i.e. SNORT IDS, SNORT Rules, and Windows Operating System). The proposed System is called H-Snort (Hybrid Snort). The system is implemented by website that displays the system status (such as network traffic, detected anomalies, e.t.c) which allowed it to be configuring easily. the result of the system test indicates that several attacks on LAN network segment have been detected through detection engine which filters all the files and loads them into its loader by configuration (.conf) file.

The limitation of the work is that the system is implemented only on LAN network segment which can be improved by implementing on DMZ network segment.
Considering the reviewed of the Garg (2014) work which focuses only on LAN network segment, our work will be focusing on deploying Snort intrusion detection system on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University Network.

Suman & Vikram in [10] proposed a security tool for intrusion detection in campus network environment using Snort. The system was configured in four modes; packet sniffer mode, packet logger mode, detection mode, and prevention mode. In this system, raw packets are captured using libcap and then decode forwarded to the detection engine. The detection engine then check the header of this packets as well as payloads against multiple thousand of rules stored in the database of pre-defined attack signatures. The system is able to detect several attacks in system rule file such attacks are denial of service attack, ping attempt, and identity spoofing attack. Every type of attack contains multiple alerts related to a particular signature. It detects the number of source that generate the attacks and the number of destination that received the attacks. Every signature of attack has a unique Id and from that Id full detail about signature is known. However, analysis indicates that the system has detected 12 signatures among which ICMP ping attack signature has the maximum number of alerts. The weakness of the work is that, the system performance becomes down during heavy network traffic which can be improved by adding new algorithm called pre-processor to the snort detection engine to avoid packet dropping.

Xiong & Peng in [11]proposed a distributed Snort Intrusion detection system model applying protocol analysis and pattern matching detecting method in order to improve the speed and accuracy of Snort intrusion detection system. It consists of three-layer structure: the sensor, data management centre and the management decision centre. Sensor collects data from the network, while the data management centre collects the alarm information for storage and classification of the alarm. The data management centre collects and analyze alarm information. The result of the system test shows clearly that the applications of campus network security have been improved effectively through the implementation of distributed Snort Intrusion detection system model, and also speed and accuracy of detecting attacks have been improved through the use of protocol analysis and pattern matching intrusion detecting methods. Protocol analysis use the network communication protocol of specific rules and analyzed the protocol information. Pattern machine compared protocol information with known network intrusion and system misused mode to find the violated behavior of the security policy. The weakness of the work is that the system collects and reacts to only intrusive packets with protocols on the network, any other intrusion that is not protocol wise will not be detected by the system.

Yi &Zhangin [12] proposed an implementation of a campus network security system based on distributed network intrusion detection technology. The system is designed using Protocol Analysis and Pattern Matching detection methods to improve the accuracy of intrusion detection and efficiency. It integrated a variety of attack detection technologies (such as data capture module, the data server module, secure communications module and the response module) which effectively detect different type of attacks. The system is able to detect and analyzed malicious behavior through data capture module from the packet capture, protocol analysis, and pattern matching. The weakness of this work is that it only detects remote attacks. The work can be improved to detect both remote attacks and local attacks within the network. Many local hackers hide their identity and compromise the security of the organizational network resources.

III. RESEARCH METHODOLOGY

Quantitative research method was adopted to evaluate the performance of the Snort Intrusion Detection System (IDS) on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University. Two Network traffics will be captured, one from the system that initiated the attack, and another traffic from snort-ids system on DMZ network segment. Traffic to be capture on Snort-ids system will be comparing against suspicious traffic detected by Snort-Ids System. Detection rate metric will be used to evaluate the performance of Snort-Ids system to know the rate at which it is able to suspicious traffic.

A. *Experimental Setup*

To evaluate the performance of the Snort Intrusion Detection System (IDS) on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University, A Snort Server will configure and deploy on DMZ network segment. This Server will be connected to the DMZ Switch on interface (ether1), and a Console Monitoring port. The Console monitoring port will be used by network administrator for monitoring Intrusion activities detected by Snort through web browser. A comprehensive working Snort System utilizes these tools to provide a web-based user interface with a backend database.

i. MySQL is used with Snort to log alert data.
ii. Apache acts as a web server.
iii. PHP is used as an interface between the web server and MySQL database.
iv. BASE (Basic Analysis and Security Engine) is a PHP package that is used to view and analyze Snort data using a web browser.
v. Barnyard2-2-1.13 is a dedicated spooler that generates alerts from snort and send to MYSQL database that reduce load on the snort.
vi. Pulledpork-0.7.0 this will automatically download the latest rule sets from snort website.
vii. Image Graph is used by BASE to create graph.

ADODB is used by BASE to connect to MySQL database

B. Performance Metrics

Detection Rate metric is chosen to evaluate the performance of Snort Intrusion Detection System (IDS) on demilitarized zone (DMZ) network segment of Usmanu Danfodiyo University. **Detection rate (DR):**The performance of Snort-ids can be measured in terms of number of correctly detected attack by the total number of traffics captured. The Snort-ids detection rate denoted by *DR*is defined by:

$$DR=\frac{correctlydetectedattacks}{totalnumberoftraffics}*100$$

IV. SYSTEM EVALUATION

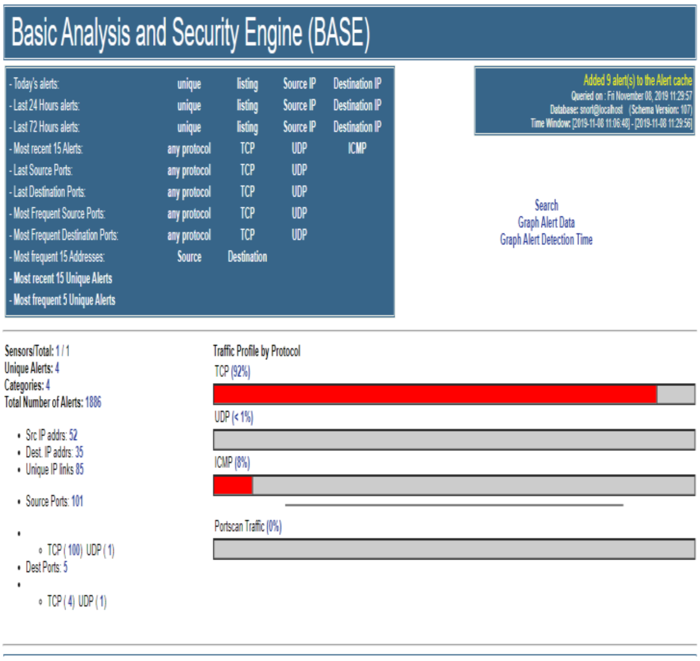
We initiated an attack from System with 82.101.148.57 IP address to the Server with 41.78.224.44 IP address on DMZ network segment. These traffics were compared against the traffics captured on Snort-ids system using wireshark. However, Traffic captured from Snort-ids System is compared against suspicious traffics detected by Snort-ids. These traffics are shown in Table 1 and Fig 1.

Table 1: Summary of Traffic captured on initiating system and traffic captured onSnort-ids system.

Application	*Initiating System*	*SNORT-IDS*	*% of Total Traffic*
TCP	1785	1785	100%
UDP	1	1	100%
ICMP (Ping)	150	150	100%
Total no. of Traffic	**1936**	**1936**	**100%**

From Table1, 1785 TCP, 1 UDP, and 150 ICMP traffic on Snort-ids system which total to 1936 were from the initiating system for a period of 28minutes. However, 1785 TCP, 1 UDP, and 150 ICMP traffic were also captured from Snort-ids system which total to 1936which is 100% of total number of traffic captured from the system that initiate the attack.

TCP, UDP, and ICMP traffic captured onSnort-Ids system initiated by System with 82.101.148.57 IP address to the Server with 41.78.224.44 IP address on DMZ network segment are compared against the number of TCP, UDP, and ICMP suspicious traffic detected by Snort-Ids system. This enable us to know how many traffic out of the total number of TCP, UDP, and ICMP traffic captured on Snort-Ids system were detected by itself. Figure1shows TCP, UDP, and ICMP suspicious traffic detected by Snort-Ids System.



Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Added 9 alert(s) to the Alert cache
Queried on : Fri November 08, 2019 11:29:57
Database: snort@localhost (Schema Version: 107)
Time Window: [2019-11-08 11:06:48] - [2019-11-08 11:29:56]

Search
Graph Alert Data
Graph Alert Detection Time

Sensors/Total: 1 / 1
Unique Alerts: 4
Categories: 4
Total Number of Alerts: 1886

- Src IP addrs: 52
- Dest. IP addrs: 35
- Unique IP links 85
- Source Ports: 101
-
  - TCP (100) UDP (1)
- Dest Ports: 5
-
  - TCP (4) UDP (1)

Traffic Profile by Protocol
TCP (92%)
UDP (< 1%)
ICMP (8%)
Portscan Traffic (0%)

Fig. 1: Suspicious Traffic Detected by Snort-ids

From Fig. 1 above, shows 1886TCP, UDP, and ICMP suspicious traffic were detected by Snort-ids system within the period of 28 minutes.

Table 2: Comparison of Snort-ids suspicious traffics detected against the total no. of Traffic captured that passed through it.

Application	*TrafficCaptured from Snort-ids System*	*Suspicious Traffic Detected by Snort-ids System*
TCP	1785	1745
UDP	1	1
ICMP (Ping)	150	140
Total no. of Traffic	**1936**	**1886**

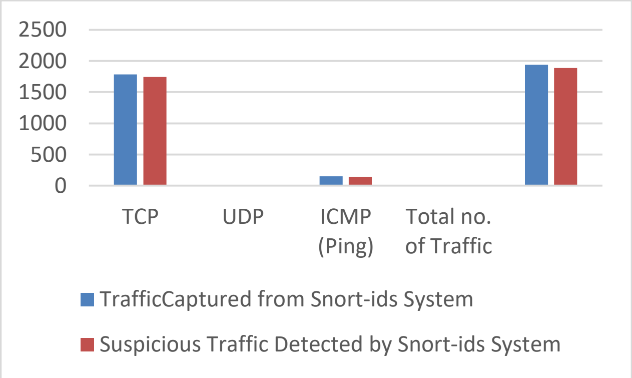


Fig. 2: **Comparison of Snort-ids suspicious traffics against the total no. of traffic captured from it.**

As shown in Fig. 2 and Table 2, based on the Rule specified in snort-ids system Rules File to detect remote TCP (ssh), UDP (udp flood), and ICMP (ping)attack from initiating host with 82.101.148.57 IP address to server with 41.78.224.44 IP address on DMZ network segment as follows:

i. We initiated ssh attack from the attacking system to a server with 41.78.224.44 IP address for a period of 38 minutes and snort-ids system was able to detected 1745 TCP (ssh) suspicious traffic.
ii. We initiated udp flood attack from the attacking system to a server with 41.78.224.44 IP address for a period of 38 minutes and snort-ids system was able to detected 1UDP (udp flood) suspicious traffic.
iii. We initiated ping attack from the attacking system to a server with 41.78.224.44 IP address for a period of 38 minutes and snort-ids system was able to detected 140ICMP (ping)suspicious traffic.

Furthermore, to ensure the rate at which Snort-ids detected this suspicious traffic, we used Detection Rate Metric as follows:

$$DR=\frac{\text{correctlydetectedattacks}}{\text{totalnumberoftraffics}}*100$$
$$=\frac{1886}{1936}*100=97\%$$

From the detection rate (DR) computation, the rate at which Snort-ids system correctly detect suspicious traffic is 97% out of the 100% traffic initiated by the attacking system. this shows clearly that snort-ids system is capable of detecting suspicious traffic by 97%.

V. CONCLUSION

Usmanu Danfodiyo University DMZ network without Snort-IDS provide room formal icious traffics to pass through without been detected. Based on the traffics we captured using Wireshark from DMZ network, it has clearly indicates that the security of Usmanu Danfodiyo University DMZ network can easily be compromise without Snort-ids system.

SNORT IDS was implemented together with various tools such as Snort Application, Pulledpork, Barnyard, Apache, MySQL, PHP, BASE, and ADODB to achieve web base intrusion detection system for analyzing suspicious traffic. The result obtained from the system evaluation indicates that Snort-ids system is able to detect suspicious traffic at the rate of 97%. However, with Snort-ids on DMZ network segment of Usmanu Danfodiyo University, Suspicious traffic can easily be detected. Snort-ids serve as security mechanisms for Usmanu Danfodiyo University to safeguard their DMZ network segment to detect suspicious traffics with minimal cost.

REFERENCES

[1] Bace, R. and P. Mell (2001). Intrusion detection systems. NIST Special Publication on Intrusion Detection Systems, Special Publication 800-31, pp 151-156

[2] Sasikumar, S. (2021). Network Intrusion Detection and Deduce System. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(9), 404-410.

[3] Niemiec, M., Kościej, R., & Gdowski, B. (2021). Multivariable Heuristic Approach to Intrusion Detection in Network Environments. *Entropy*, *23*(6), 776

[4] Xu, C., Zhang, R., Xie, M., & Yang, L. (2020, February). Network intrusion detection system as a service in openstack cloud. In *2020 International Conference on Computing, Networking and Communications (ICNC)* (pp. 450-455). IEEE.

[5] Hamsaveni, R. (2020). AN IMPLEMENTAION OF SNORT BASED INTRUSION DETECTION SYSTEM USING WIRELESS SENSOR NETWORK. *International Research Journal of Modernization in Engineering Technology and Science*, *2*(12), 12-22.

[6] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal*, *6*(5), 9042-9053.

[7] Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Future Generation Computer Systems*, *96*, 481-489.

[8] Alsakran, F., Bendiab, G., Shiaeles, S., & Kolokotronis, N. (2019, December). Intrusion detection systems for smart home IoT devices: experimental comparison study. In *International Symposium on Security in Computing and Communication* (pp. 87-98). Springer, Singapore.

[9] Garg, M. (2014). Intrusion Detection System in Campus Network: SNORT- The most powerful Open Source Network Security Tool, proceedings of International Journal of Advancement in Engineering Technology, Managemnt& Applied Science, Volume 1, pp 913-918.

[10] Sumani, R. and Vikram, S. (2013). Snort: An Open Source Network Security Tool for Intrusion Detection System in Campus Network Environment, proceedings of IJCTEE, Volume 2, pp 212-214.

[11] Xiong, C.H. & Peng, Z. (2012). Applied Research on Snort Intrusion Detection Model in Campus Network. Proceedings of IEEE 2012 Symposium on Robotics and Application, pp 596-599.

[12] Yi, H. & Zhang, Y. (2010). Research of campus network security system based on Intrusion Detection, proceedings of International Conference on Computer Design and Applications (ICCDA), pp 618-621.