Network Traffic Analysis for Cybersecurity

Abayomi Awe

July 3, 2024

1 Proposal

In today's digital era, with the increasing reliance on technology and interconnected systems, cybersecurity has become a critical concern. The proliferation of cyber criminal activities, such as network attacks and Advanced Persistent Threats, poses significant risks to individuals, businesses, and even nations. This project aims to address the importance of network traffic analysis in cybersecurity and its relevance in detecting and preventing cyber threats.

Many researchers worked on network intrusion detection technology can be achieved in real-time under high-speed network intrusion detection using machine learning algorithm. N. S. Mangrulkar et al 2014 [7] reviews different type of possible network attacks and detection mechanism proposed by various researchers that have capabilities of detecting such attacks. Based on their research several well-known machine learnings like Decision tree, Ripple Rule, Random Forest, and Bayesian network was applied. Dong et al 2022 [8] investigate the huge impact and losses on business websites due to network attack in a complex internet environment.

Their analysis is based on network analysis, security countermeasures and how it is applicable to network security protection. In addition, it will further investigate how to determine the strategies and techniques needed for efficient detection and prevention of cybercrime [11]. By analysing network traffic patterns and identifying anomalies, this project aims to improve the detection and response capabilities of cybersecurity systems.

1.1 Research area

Cybersecurity is an increasingly important field, as the frequency and complexity of cyberattacks continue to rise. These attacks pose significant risks to individuals, organizations, and society as a whole[14]. In addition, there are several factors that contribute to the proliferation of criminal actions in cybersecurity. These factors include the profitability of cybercrime, the ease and low cost of tools used in attacks, and the ability for attackers to remain anonymous and operate from anywhere in the world.

Cybercrime has evolved into a sophisticated ecosystem, with various actors and elements working together to carry out illicit activities[16]. This ecosystem

includes the cybercrime underground, where cybercriminals trade tools, services, and stolen data. The research area of network traffic analysis for cybersecurity focuses on understanding the characteristics and patterns of cybercriminal activities in network traffic. By analyzing network traffic data, researchers aim to detect and prevent cyberattacks more effectively[15].

By understanding the common characteristics of cybercriminal activities in network traffic, researchers can develop techniques and methodologies for detecting and preventing these attacks (Broadhead, 2018). Network traffic analysis is a key component in cybersecurity as it allows for the identification and detection of cybercriminal activities[15].

Network traffic is a process of characterizing packet flows on the network. Typical Network traffic consists of packets being exchanged among hosts. Hence, network traffic analysis is related with extracting, analysing and recognizing significant and interesting´ patterns on the network. Moreover, network traffic allows obtaining useful information about activity that is going around network. Network traffic analysis has been increasingly used as a mechanism to improve performance and security of computer networks used for business, research institutes, ordinary users and other organizations.

1.2 Project Goals

The primary goal of this project is network traffic analysis in a real-time and how to evaluate network attack outside and within a enterprise network domain. Through research and practical experimentation, we aim to achieve the following goals:

- To explore and analyse network traffic analysis in real-time
- To develop graphical visual network traffic analysis.
- To develop rules in snort that will allow, block replace, whitelist, blacklist and ignore packet.
- To develop how generate alert message.

By analysing network traffic patterns and identifying anomalies, this project aims to improve the detection and response capabilities of cybersecurity systems.

1.3 Research Questions

Some of the key research questions that should be careful investigate:

- How is the Snort NIDS used in a network environment and how is it configured?
- How is it configured to effectively detect and prevent potential network threats?[12].

- What are the benefits and limitations of using Snort NIDS for network traffic analysis?
- What are the most common types of network attacks that can be detected through network traffic analysis?.
- How to integrate signature-based threat detection on the network traffic.

1.4 Deliverables

The deliverables for this project will include these following:

- A enterprise network topology for network traffic analysis.
- EWK: EWK is a stack that comprise of three platform: Elasticsearch, Wazuh and Kibana. They are always refers as Elasticsearch, the EWK stack gives you the ability to aggregate logs from all your systems and applications, analyze these logs, perform end-point detection and response and create visualizations for application and infrastructure monitoring, faster troubleshooting, and security analytics.
- PFSENSE: pfSense software includes the same features as most expensive commercial firewall solutions. Pfsense firewall will be sitting between the public network and private network, and also configuration of snort rules will done on pfsense.
- DMZ: Webmail server and proxy server are common devices found DMZ which communicate the public.
- Domain Controller: It will serves as active directory domain for the network

2 Literature Review

In today's digital age, where connectivity and technology play a crucial role in our daily lives, cybersecurity has become one of the most pressing issues. The emergence of digital media, the Internet, and online social media have brought about new challenges and vulnerabilities in terms of cyber-attacks. These cyber-attacks pose a serious threat to individuals, companies, and government organizations, as they seek to steal sensitive information, disrupt systems, and cause financial and reputational damage. To address these challenges, researchers and experts in the field of cybersecurity have been actively analyzing current cyber-attacks and developing strategies to defend against them. In a literature review conducted by researchers from the University of the Management and Technology in Lahore, Pakistan, it was found that cyber security research has primarily focused on a few widespread security flaws such as malware, phishing, and denial-of-service attacks[2].

However, it is important to expand the scope of research and consider other factors such as network traffic analysis. Network traffic analysis plays a crucial role in enforcing cybersecurity. By monitoring and analyzing the flow of network traffic, potential attacks can be detected and mitigated.By examining patterns, anomalies, and suspicious activities in network traffic, cybersecurity professionals can identify potential threats and take appropriate action to prevent them. In addition to traffic flow monitoring, applied statistics using formulated mathematical models can also be applied for the purpose of cybersecurity. These statistical models can help in identifying patterns and trends that may indicate the presence of malicious activity in network traffic.

Another important aspect of network traffic analysis is the detection of keylogging and network eavesdropping attacks. Keylogging and network eavesdropping attacks are common methods used by cybercriminals to gain unauthorized access to sensitive information. In a study by Xie et al [6], the authors discuss the importance of understanding keylogging and network eavesdropping attacks in information security education. The study aims to provide academics with the necessary knowledge teach these security topics effectively and encourage their inclusion in information security modules.In their research, Xie et al [6] highlight the need for teaching keylogging and network eavesdropping attacks in information security education.They suggest that by incorporating these topics into the curriculum, students can develop a better understanding of these threats and learn valuable skills to prevent and mitigate them.

In addition, Network Traffic Analysis continues to be a fundamental tool for cybersecurity professionals. By examining data packets that travel across a network, NTA tools provide critical visibility into the type, origin, and destination of traffic. This level of scrutiny is essential in the rapid identification of unusual patterns that may signify a cyber threat, such as malware or data exfiltration attempts.

Daria S. Lavrova, Maria A. Poltavtseva, Anna A. Shtyrkina's discussion in "Security analysis of cyber-physical systems network infrastructure" proposes an innovative solution for analyzing high volumes of network traffic within

the context of cyber-physical systems. Their approach suggests that big data methodologies such as filtering and aggregation can help manage these volumes effectively, with the width of the multifractal spectrum of network traffic serving as a security metric[1]. This indicates the potential of merging network traffic analysis with big data methods for enhanced security measures.

In depth studies by these researcher's D. Zhao et al showcase the dynamic nature of network traffic analysis for cybersecurity and the diverse strategies being investigated to confront the complex obstacles presented by contemporary cyber threats. The integration of cutting-edge technologies such as deep learning and blockchain into network traffic analysis signifies a promising avenue for enhancing the effectiveness and flexibility of cyber defense mechanisms. A key advantage of network traffic analysis for cybersecurity lies in its capacity to detect and classify malware by analyzing time-series data[17].

Another research based on network traffic analysis was carried out by L. Chen et al. that delve into the practical application of blockchain technology in network traffic analysis for cybersecurity. The scholars emphasize the potential of blockchain to serve as a decentralized and tamper-proof platform for storing network traffic data, thereby enhancing the integrity and authenticity of the analyzed information. They argue that the implementation of blockchain-based network traffic analysis systems can contribute to improved transparency and accountability in cybersecurity operations, ultimately strengthening the defense against cyber attacks[18].

The "Introduction to a network forensics system for cyber incidents analysis" highlights the importance of traffic analysis in the field of cyber incident analysis. It introduces Cyber Blackbox as a system that enables a dedicated approach to network traffic analysis. Although the details are not provided in the given information, it suggests that Cyber Blackbox may possess specialized forensic capabilities to effectively address and comprehend cyber incidents[5].

In conclusion, network traffic analysis plays a crucial role in cybersecurity by enabling the detection and resolution of cyber incidents, improving network efficiency, and fortifying the security of cyber-physical systems. Furthermore, network traffic analysis continuously adapts and improves to match the ever-changing realm of cyber threats. It is imperative for cybersecurity experts to remain abreast of the latest research and developments in network traffic analysis to safeguard networks and systems against emerging threats, thereby ensuring the overall security and dependability of the network infrastructure.

3 Project Plan

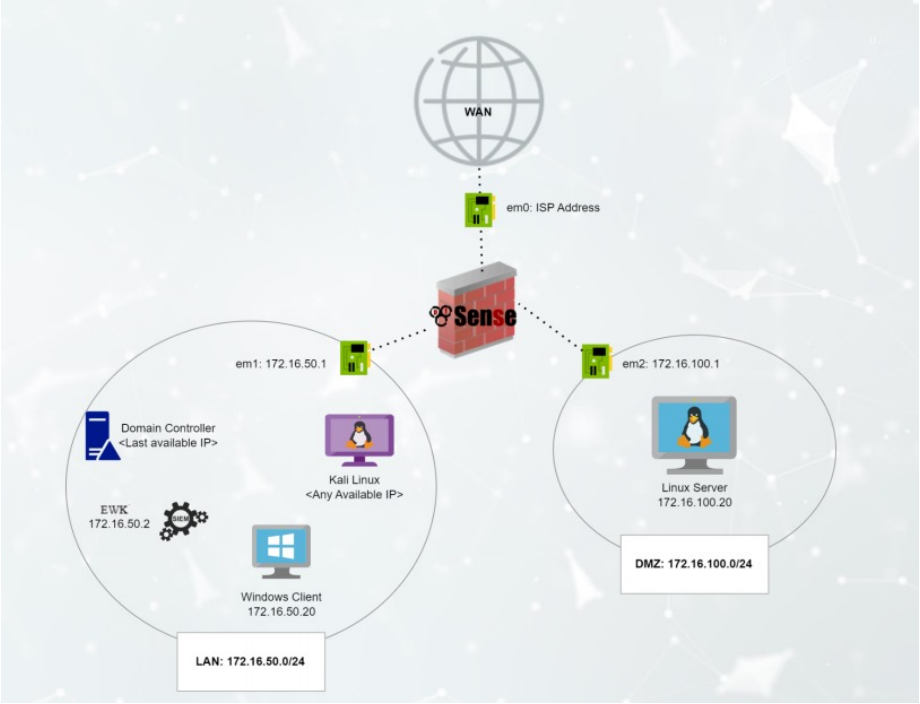

Figure 1: Enterprise Network Topology

The description of the network topology in Figure 1 as follows:

1. The firewall will be sitting between the internet and the private network.
2. The private network is comprising of the Local Area Network (LAN) and the Demilitarize zone (DMZ) where the web servers and the public facing services will be residing.
3. On the firewall, Network Intrusion Detection System (e.g. SNORT) will be installed, there will be SNORT rules and firewall rules for blocking and alerting based on specify rules and actions.
4. Access to the DMZ will be via port forward.
5. Then the Security Operation Center (SOC), is part of the organization security team that monitors all activities on the network, in this situation, the WAZUH will be employed, WAZUH is an End point Detection and Response (EDR) system with the help of Kibana and Elasticsearch for visualization and Log parsing, and Wazuh agent will be installed on all the end point which will be sending logs Wazuh Manager including the

servers in the DMZ which will be processed by the Elasticsearch and being displayed by Kibana.

6. In the LAN, the difference machines, the Domain controller, controls the activities in the domain which includes, resource allocation, user creation and deleting, security police aggregation.

7. Wazuh has agents for almost all the vendors which can be easily integrated which makes one of the best open sourced EDR.

The estimated duration for setting up the whole project:

- Setting up the topology: 2 weeks.
- Setting up the EWK stack: 2 weeks.
- Setting up the SNORT: 2 weeks
- Configure SNORT for setting up of attacks: 2 weeks.
- Run attacks: 2 weeks.

4 Evaluation Methodology

The methodology evaluation of this project will be based on how snort will be configured against set of attack compromising the network traffic. The snort rules will be implemented to ensure that the Intrusion Detection System is effectively detecting and protecting the network from potential threat.

Snort is a freely available network intrusion detection and prevention system (IDS/IPS) that observes network activity and recognizes suspicious behavior on Internet Protocol (IP) networks. Organizations have implement Snort by utilizing a rule-based language that integrates protocol, signature, and anomaly-based examination techniques to pinpoint harmful data packets in network traffic and prevent possible network attacks.

Here are the steps to evaluate snort configuration against a set of attacks:

Generate Test Traffic: Create a set of test scenarios that simulate different types of attacks, such as port scanning, malware detection, or network eavesdropping. Tools like metasploit, nmap or customize script will be use to attack scenarios to generate test traffic.

Configure Snort: Make sure that Snort is properly configured to monitor and analyze the network traffic. This includes setting up rules and filters to detect specific attack signatures.

Execute the Test Scenarios: Run the generated test traffic through the Snort system to see if it correctly identifies and alerts on the simulated attacks.

Analyze the Results: Review the output generated by Snort during the test scenarios.Look for any alerts or alarms that indicate successful detection of the simulated attacks.

Analyze False Positive and Negative: Detect and rectify any instances of legitimate traffic being mistakenly identified as an attack (false positives), as well as any missed attacks (false negatives). Modify rules and configurations to reduce the occurrence of false positives, while ensuring that the detection capabilities remain intact.

Documentation: Record the test scenarios, outcomes, and any modifications applied to the snort configuration. Ensure that all changes made to the Snort configuration are properly documented.

4.1 Understanding Snort Structure

A Snort rule comprises multiple components.

- Action: Determines what snort should do when the rule matches (alert, log or drop).
- Protocol: Identifies the network protocol being used(e.g TCP, UDP amd ICMP).
- Source/Destination IP addresses and ports: Establishes the source and destination of the traffic flow.
- Rule Options: Includes extra conditions for matching, like content, keywords, or specific flags.

4.2 Define the Rule Header

The primary layout of a snort rule is structured in the following manner:
`action protocol source_ip source_port -> destination_ip destination_port (options)`

- Action: Alert, Log, Pass, Activate, Dynamic.
- Protocol: tcp, udp, icmp, ip.
- IP addresses: Source and destination IP addresses.
- Ports: Source and destination ports.

4.3 Specify Rule Options

Rule options give specific criteria for matching. Here are a number of commonly used options:

- msg: Message explanation for the log.
- content: Search for specific content in the packet payload.
- sid: and rev: Unique snort ID and rule revision.
- classtype: Classification of the rule (e.g attempted-admin, successful-admin).

4.4 Rules Example

4.4.1 Port Scan Detection

```
alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS \
(msg:"Possible Port Scan"; flags:S; sid:1000002;)
```

An alert is generated by this rule upon detection of a TCP packet containing the SYN flag, which may indicate a port scan taking place.

References

[1] D. Lavrova, M. Poltavtseva, and A. Shtyrkina, "Security analysis of cyber-physical systems network infrastructure," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), May 2018. doi:10.1109/icphys.2018.8390812.

[2] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 3171–3189, Jan. 2020. doi:10.1007/s13369-019-04319-2.

[3] P. Kori and S. K. Singh, "Analysis Of Network Security Threats And Vulnerabilities By Development And Implementation Of a Security Network Monitoring Solution", Aug, 2016.

[4] S. A. Mohammed, S. M. Sani and D. D. Dajab. "Network Traffic Analysis: A Case Study of ABU Network". vol. 4. no. 4. pp. 33-39. Jan. 2013.

[5] Y. Choi, J.-Y. Lee, S. Choi, J.-H. Kim, and I. Kim, "Introduction to a network forensics system for Cyber Incidents Analysis," 2016 18th International Conference on Advanced Communication Technology (ICACT), Jan. 2016. doi:10.1109/icact.2016.7423270

[6] M. Xie, Y. Li, K. Yoshigoe, R. Seker, and J. Bian, "CAMAUTH: Securing web authentication with camera," 2015 IEEE 16th International Symposium on High Assurance Systems Engineering, Jan. 2015. doi:10.1109/hase.2015.41.

[7] N. S.Mangrulkar, A. R. Bhagat Patil, and A. S. Pande, "Network attacks and their detection mechanisms: A Review," International Journal of Computer Applications, vol. 90, no. 9, pp. 37–39, Mar. 2014. doi:10.5120/15606-3154.

[8] G. Dong, F. Liu, and G. Wu, "A website's network attack analysis and security countermeasures," Procedia Computer Science, vol. 208, pp. 577–582, 2022. doi:10.1016/j.procs.2022.10.080.

[9] A. S. Santisteban, L. Ocares, and L. Andrade-Arenas, "Analysis of National Cybersecurity Strategies," International Journal of Advanced Computer Science and Applications, vol. 11, no. 12, 2020. doi:10.14569/ijacsa.2020.0111288.

[10] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial Intelligence in cyber threats intelligence," 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Dec. 2018. doi:10.1109/iconic.2018.8601235.

[11] L. Tang, "Characteristic analysis and investigation strategy of Computer Network crime," Journal of Physics: Conference Series, vol. 1856, no. 1, p. 012002, Apr. 2021. doi:10.1088/1742-6596/1856/1/012002.

[12] Orebaugh, Biles, and Babbin, Snort Cookbook. O'Reilly Media, 2005.

[13] P. Hunton, "A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment," Digital Investigation, vol. 7, no. 3–4, pp. 105–113, Apr. 2011. doi:10.1016/j.diin.2011.01.002

[14] A. S. Santisteban, L. Ocares, and L. Andrade-Arenas, "Analysis of National Cybersecurity Strategies," International Journal of Advanced Computer Science and Applications, vol. 11, no. 12, 2020. doi:10.14569/ijacsa.2020.0111288.

[15] J. An and H.-W. Kim, "A data analytics approach to the cybercrime underground economy," IEEE Access, vol. 6, pp. 26636–26652, 2018. doi:10.1109/access.2018.2831667.

[16] S. Broadhead, "The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments," Computer Law And Amp; Security Review, vol. 34, no. 6, pp. 1180–1196, Dec. 2018. doi:10.1016/j.clsr.2018.08.005.

[17] D. Zhao, I. Traore, B. Sayed, W. Lu, S. Saad, A. Gharbani, D. Garant, "Botnet detection based on traffic behavior analysis and flow intervals," Computers and amp; Security, vol. 39, pp. 2–16, Nov. 2013. doi:10.1016/j.cose.2013.04.007.

[18] L. Chen, H. Lv, K. Fan, H. Yang, X. Kuang, A. Xu, and Y, Yang "A Survey: Machine Learning Based Security Analytics Approaches and Applications of Blockchain in Network Security," 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 2020, pp. 17-22, doi:10.1109/SmartBlock52591.2020.00011.