International Journal of Emerging Science and Engineering (IJESE)
ISSN: 2319–6378 (Online), Volume-12 Issue-12, November 2024

Network Threat Detection and Modelling

Mahendra V, Manjunatha G S, Nagaraja G S, Shushrutha K S

Abstract: ***Network threat detection and modelling are critical aspects of network security in an organization since the many devices connecting to the internet can be vulnerable. Network attacks are unauthorized actions on the digital assets within an organizational network. Malicious parties usually execute network attacks to alter, destroy, or steal private data. Perpetrators in network attacks tend to target network perimeters to gain access to internal systems. In this project the incoming traffic and outgoing network traffic is analyzed and from the several devices in an organization and security determined and made easy to visualize by the security analyst to take necessary action. Firstly, the network traffic related information is collected assets or end points in an organization which are exposed to the external world. In fact, the assets will be having data related to external world in the form of IP addresses to which domain or traffic they are being connected or they being accepted. These IP addresses are processed to obtain the actual location and domain which is used to visualize the geographical location of incoming and outgoing traffic and some data like port number are also collected to know the protocol being used by assets are secure. And vulnerable port numbers are displayed in user Interface to take necessary action by the security analyst. In this project for threat detection. The some of the standard compliance like CIS (Center for Internet Security) benchmarks are used to determine the network vulnerabilities in the assets that can be easily attacked by the attackers and the firewall configurations and other network configurations are verified according to these standards. If any of the required check or compliance failing is indicated as a threat in the UI so that security analyst can take necessary action on that particular asset which have security breach or which is vulnerable.***

Keywords: Center for Internet Security, Internet Protocol

I. INTRODUCTION

In today's digital landscape, cyber-attacks have become a prevalent and concerning issue. These attacks encompass a wide range of malicious activities aimed at breaching the security of computer systems, networks, or digital devices. Cyber attackers, which can include individuals, criminal organizations, or even nation-state actors, employ various techniques such as malware infections, phishing scams, denial-of-service attacks, and ransomware attacks to gain unauthorized access, manipulate, or destroy data. To counteract the damaging effects of cyber-attacks, robust cybersecurity measures are essential. Cybersecurity involves safeguarding computer systems, networks, and digital devices from unauthorized access, theft, and harm. It encompasses a diverse array of security practices, including the use of firewalls, intrusion detection and prevention systems, antivirus software, and encryption. Additionally, cybersecurity involves educating users about safe online behavior and providing training on identifying and responding to potential cyber threats to combat advanced network threats effectively, organizations must implement advanced security measures such as compliance configurations based on the standards of CIS.

Manuscript received on 01 June 2024 | Revised Manuscript received on 21 October 2024 | Manuscript Accepted on 15 November 2024 | Manuscript published on 30 November 2024.
*****Correspondence Author(s)
Mahendra V*, BE Student, Department of Computer Science and Engineering, RV College of Engineering, Bengaluru (Karnataka), India. Email ID: mahivirakthmath@gmail.com
Manjunatha G S, BE Student, Department of Electronics and Communication Engineering, RV College of Engineering, Bengaluru (Karnataka), India. Email ID: manjunathags.ec19@rvce.edu.in
Dr. Nagaraja G S, Professor and Associate Dean, Department of Computer Science and Engineering, RV College of Engineering, Bengaluru (Karnataka), India. Email ID: nagarajags@rvce.edu.in
Dr. Shushrutha K S, Associate Professor, Department of Electronics and Communication and Engineering, RV College of Engineering, Bengaluru (Karnataka), India. Email ID: shushruthaks@rvce.edu.in

II. NETWORK COMPLIANCE AND CIS

Network compliance refers to adhering to a set of rules, standards, and guidelines in the context of computer networks and information technology infrastructure. It involves ensuring that network systems, devices, and operations meet specific requirements established by regulatory bodies, industry standards, organizational policies, or security best practices. CIS (Center for Internet Security) Benchmarks are a set of best practices and guidelines developed by the Center for Internet Security, a nonprofit organization focused on promoting cybersecurity readiness and resilience. The CIS Benchmarks provide organizations with recommended security configurations and settings for various operating systems, software applications, and network devices. These benchmarks are created through a consensus driven process involving cybersecurity professionals, industry experts, and government entities. They are continuously updated and refined to reflect the latest. The CIS Benchmarks typically include configuration recommendations for security controls, system hardening, and vulnerability mitigation. They provide detailed step-by-step instructions for implementing security settings and configurations to reduce the attack surface and improve the overall security posture of the systems

III. SOCKET EVENTS

Socket events refer to the events or actions that occur during the life cycle of a socket connection in a network communication protocol, such as TCP/IP. Sockets allow programs to establish network connections and exchange data over the network. In event-driven programming, socket events trigger specific actions or call-backs in the application code, enabling developers to handle different stages of the socket connection. The specific events available may vary depending on the programming language or framework used, but some common socket events include: Connection Established occurs when a

client successfully establishes a connection with a server. It indicates that the initial handshake between the client and server has been completed, and they are now ready to exchange data. Data Received is triggered when data is received by a socket from the connected peer. It allows the application to read and process the received data. Data Sent occurs when data has been successfully sent from a socket to the connected peer. It indicates that the data transmission was completed without errors. Connection Closed signifies that the socket connection has been closed either by the client or the server. It could happen due to an intentional termination or an unexpected disconnection. Error Occurred is triggered when an error occurs during socket communication. It could be caused by issues such as network failures, timeouts, or protocol violations. Handling this event allows the application to handle and respond to errors appropriately. Connection Timeout is observed if a socket connection takes longer than a specified timeout period to establish, a connection timeout event may be triggered. This event allows the application to handle cases where connection establishment is delayed or unsuccessful. Connection Refused When a client attempts to establish a connection, but the server actively rejects the connection request, a connection refused event is triggered. This can happen if the server is not listening on the specified port or if it has reached its connection limit. These socket events provide developers with the means to control and respond to different stages of the network communication process. By handling these events, applications can implement specific logic to manage data transmission, error handling, and connection state changes effectively.

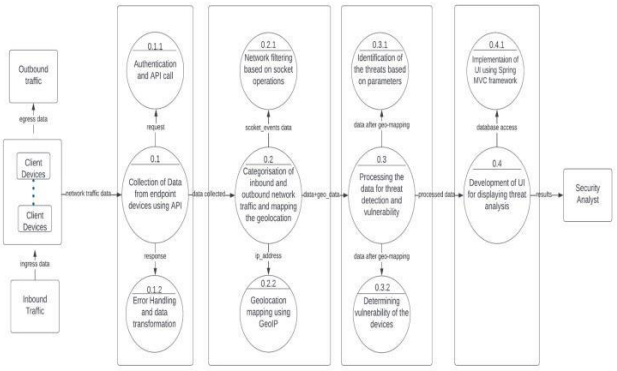
IV. RELATED WORK

In the first survey paper, we aim to present various methods and techniques that can be utilized to detect different stages of APT attacks, along with the application of learning methods. Furthermore, we explore how to enhance your threat detection framework intelligently to outsmart and decipher the strategies of adapting APT attackers [1]. The second paper recognizes APT as a threat that follows a comprehensive kill chain process. It provides an overview of intrusion detection and intrusion detection methods. Detecting APTs presents significant challenges, as well as the obstacles encountered in identifying APTs [2]. In this article [3], we explore and summarize the most popular and successful methods of protection utilized by organizations and individuals alike. Provides four distinct approaches for consideration as possible countermeasures to the advanced persistent threat These approaches have included well known signature-based methodology, manual analytical practices, statistical tactics and correlation concepts, as well as automatic leak prevention [4]. This paper [5] presents the outcomes of a comprehensive study on APTs, including their defining characteristics, attack models, and commonly observed techniques. The paper [6] also explores nonconventional countermeasures to mitigate APTs and highlights directions for future research. This paper [7] provides an overview of current research on APT attack detection, including previous findings, analysis of identified APTs, and detection methods for potential APT attacks. This paper [8] introduces a model for detecting APTs and presents a methodology for implementing it within a generic organization's network. To the best of our knowledge, this proposed method is the first to address APT modeling and provide a potential detection framework.

V. METHODOLOGY

A. Overview

The idea of detecting network threats follows four phases which are network traffic data collection, mapping the collected data to its geolocation, processing the data to detect threats and vulnerabilities and visualisation of the obtained results to analyse and detect threats [11]. The below figure 2 depicts the data flow diagram of the network threat detection process [12].



[Fig.1: Data Flow Diagram of the Network Threat Detection]

B. Approach

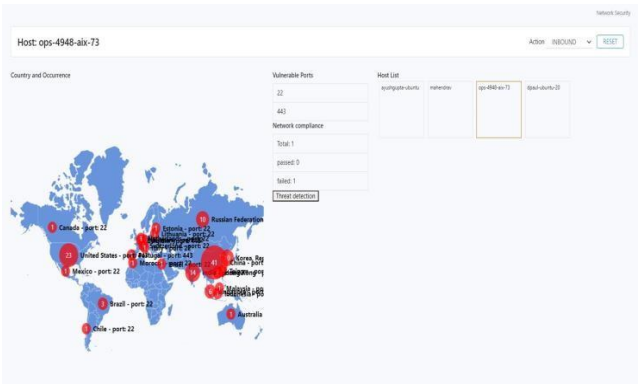
The first step involves network traffic data collection of the socket events using API to fetch from the osquery [26]. After collection of socket events data from assets irrespective of the operating, the collected data is processed by categorizing the data into Inbound data and outbound data which is used by other API to upload it to data base [9]. The collected data contains several attributes that provide valuable information about socket events, including remote address, local address, action, remote port, local port, executable name, and process ID (PID) [10]. These attributes help to characterize and analyse network communication patterns [13]. The categorized data is then used get required information such as vulnerable ports and remote addresses which is used get the geolocation of respective IP and also used get domain information [14]. In the data processing the local IP adresses are ignored since the main aim of the project is to detect the network threats outside the local network, that is the data coming from external word and data going to external world is important and the geographical location of respective data is then determined using pygeoip library and maxmind data base [15]. In the last two modules, the data is processes based on the parameters of compliance configurations and the vulnerabilities of the devices are determined [16].

Network compliance with established security standards, such as CIS benchmarks, is checked [17][18]. By comparing the inbound and outbound data against these

standards, security analysts can identify any deviations or violations that may indicate potential security risks [19]. Non-compliant systems are flagged as they pose a threat to the overall security posture of the network [20]. Additionally, the results of the network compliance evaluation for outbound connections [21]. By presenting the compliance status alongside the outbound data, security analysts can assess the overall adherence to security standards and identify any potential vulnerabilities or non-compliant systems within the network [22][23]. The result is displayed in a user interface along with traffic movement [24] [25].

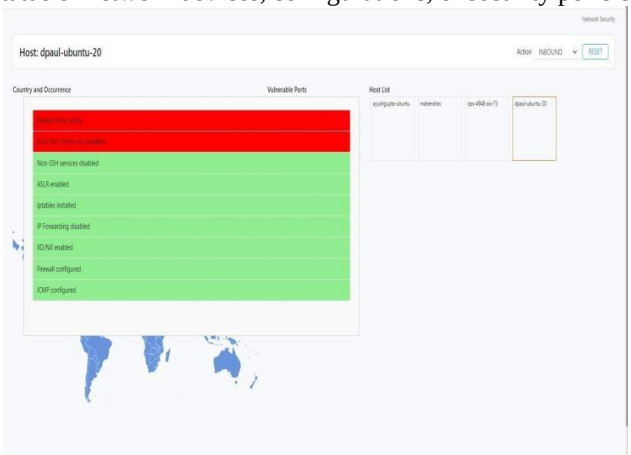
VI. RESULT AND DISCUSSION

The Results of the Threat Detection are displayed in a user interface along with a map to exhibit the network traffic movement across the world as shown in Fig 2.



[Fig.2: Network Traffic and Vulnerability Data]

In Fig. 2, we can also see the details about vulnerable ports and the configuration tests count of passed and failed. As mentioned above, it helps security analysts and administrators or users to quickly assess the compliance status of network devices, configurations, or security policies



[Fig.3: Network Compliance Evaluation for Threat Detection]

The network compliance and the threats determined are displayed for each asset and can be accessed in the UI by clicking on the required asset under the Host List. The configurations are then displayed on a popup window with colors green and red where red represents the vulnerability and green represents that that configuration is enabled as shown in Fig. 3. The system or assets which are failed these CIS benchmark checks are indicated as in red in colour as a network threat since it has failed network configurations the assets are vulnerable to the attack from outside the network and can cause security breach. So, these are marked in red in colour and the if the assets have matched or passed the CIS benchmark are marked in green in colour.

VII. CONCLUSION

In summary, this project emphasized the importance of network threat detection and modeling in safeguarding organizational networks. By leveraging analysis of the traffic movement, geographic visualization, compliance benchmarks, and user-friendly interfaces, the project aimed to provide security analysts with valuable insights into potential threats and vulnerabilities within the network, enabling them to take timely and appropriate actions to mitigate risks and protect the organization's digital assets. In the future, our objective is to enhance the threat detection model by incorporating newer techniques that will enable the identification of complex and sophisticated cyber-attacks and also be scalable and performance efficient to deal with large amounts of data.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Khalid, Adam, Anazida Zainal, Mohd Aizaini Maarof, and Fuad A. Ghaleb. "Advanced persistent threat detection: A survey." 3rd International Cyber Resilience Conference (CRC), 2021, pp. 1-6. IEEE Doi: https://doi.org/10.1109/CRC50527.2021.9392626
2. X. Lu, J. Han, Q. Ren, H. Dai, J. Li, and J. Ou, "Network threat detection based on correlation analysis of multi-platform multi-source alert data," Multimedia tools and applications, vol. 79, pp. 33 349–33 363, 2020. Doi: https://doi.org/10.1007/s11042-018-6689-7
3. M. Wo´zniak, J. Si lka, M. Wieczorek, and M. Alrashoud, "Recurrent neural network model for iot and networking malware threat detection," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5583–5594, 2020. Doi: https://doi.org/10.1109/TII.2020.3021689
4. Alshamrani, Adel, et al. "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities." IEEE Communications Surveys & Tutorials, 2019. Doi: https://doi.org/10.1109/COMST.2019.2891891
5. R. Ranjan 'Detecting Advanced Persistent Threats: A Comparative Analysis of Machine Learning Approaches', 2017
6. M. Zahidul Islam, 'A Survey of Advanced Persistent Threats: Techniques, Tools and Challenges', 2017
7. M. Joshi and T. H. Hadi, "A review of network traffic analysis and prediction techniques," arXiv preprint arXiv:1507.05722, 2015. Doi:

https://doi.org/10.48550/arXiv.1507.05722
8. Amin Kharraz, 'A Survey of Advanced Persistent Threats: Detection, Analysis, and Mitigation', 2015, Journal of Network and Computer Applications.
9. Advanced Persistent Threats - detection and defense - IEEE, MIPR, 2015. Doi: https://doi.org/10.1109/MIPRO.2015.7160480
10. A study on advanced persistent threats in Proc. IFIP Int. Conf. Commun. Multimedia Security, P. Chen, L. Desmet, and C. Huygens, 2014. Doi: https://doi.org/10.1007/978-3-662-44885-4_5
11. N. Virvilis and D. Gritzalis, "The big four-what we did wrong in advanced persistent threat detection?" In 2013 international conference on availability, reliability and security, IEEE, 2013, pp. 248–254. Doi: https://doi.org/10.1109/ARES.2013.32
12. Giura, Paul, and Wei Wang. "A context-based detection framework for advanced persistent threats." 2012 International Conference on Cyber Security. IEEE. Doi: https://doi.org/10.1109/CyberSecurity.2012.16
13. S. Khanna, H. Chaudhry, and G. S. Bindra, "Inbound & outbound email traffic analysis and its spam impact," in Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE, 2012, pp. 181– 186. Doi: https://doi.org/10.1109/CICSyN.2012.42
14. C. Rossow, C. J. Dietrich, H. Bos, et al., "Sandnet: Network traffic analysis of malicious software," in Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, 2011, pp. 78–88. Doi: https://doi.org/10.1145/1978672.1978682
15. M. A. Qadeer, A. Iqbal, M. Zahid, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in 2010 Second International Conference on Communication Software and Networks, IEEE, 2010, pp. 313–317. Doi: https://doi.org/10.1109/ICCSN.2010.104
16. M. Kihl, P. Odling, C. Lagerstedt, and A. Aurelius, "Traffic analysis and charac- ¨ terization of internet user behavior," in International Congress on Ultra-Modern Telecommunications and Control Systems, IEEE, 2010, pp. 224–231. Doi: https://doi.org/10.1109/ICUMT.2010.5676633
17. M. Aswal, P. Rawat, and T. Kumar, "Threats and vulnerabilities in wireless mesh networks," International Journal of Recent Trends in Engineering, vol. 2, no. 4, p. 155, 2009.
18. C. So-In, "A survey of network traffic monitoring and analysis tools," Cse 576m computer system analysis project, Washington University in St. Louis, 2009.
19. M.-k. Choi, R. J. Robles, C.-h. Hong, and T.-h. Kim, "Wireless network security: Vulnerabilities, threats and countermeasures," International Journal of Multimedia and Ubiquitous Engineering, vol. 3, no. 3, pp. 77–86, 2008
20. W Pechhold, O Grassl, and W v Soden, "Dynamic shear compliance of polymer melts and networks," Crosslinking and scission in polymers, pp. 199–222, 1990. Doi: https://doi.org/10.1007/BF01410674
21. Sharma, P., & Site, S. (2022). A Comprehensive Study on Different Machine Learning Techniques to Predict Heart Disease. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 2, Issue 3, pp. 1–7). https://doi.org/10.54105/ijainn.c1046.042322
22. Priyatharshini, Dr. R., Ram. A.S, A., Sundar, R. S., & Nirmal, G. N. (2019). Real-Time Object Recognition using Region based Convolution Neural Network and Recursive Neural Network. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 4, pp. 2813–2818). https://doi.org/10.35940/ijrte.d8326.118419
23. Japneet Kaur, Harmeet Singh, Intrusion Detection Techniques for Secure Communication in Different Wireless Networks. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 9S2, pp. 668–671). https://doi.org/10.35940/ijitee.i1137.0789s219
24. Maniraj, S. P., G, S., Sravani, P., & Reddy, Y. (2019). Object Boundary Detection using Neural Network in Deep Learning. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 1, pp. 4453–4457). https://doi.org/10.35940/ijeat.a1608.109119
25. Pagare, S., & Kumar, Dr. R. (2024). Human Action Recognition using Long Short-Term Memory and Convolutional Neural Network Model. In International Journal of Soft Computing and Engineering (Vol. 14, Issue 2, pp. 20–26). https://doi.org/10.35940/ijsce.i9697.14020524
26. Saroj, S. K., Yadav, M., Jain, S., & Mishra, R. (2020). Performance Analysis of Q-Leach Algorithm in WSN. In International Journal of Inventive Engineering and Sciences (Vol. 5, Issue 10, pp. 1–4). https://doi.org/10.35940/ijies.i0977.0651020