WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Network Watch Dog using Raspberry Pi

Mr. K. Arun Kumar[1], Mr. S. Vignesh[2], Abinesh. M[3], Mohamed Althaf. S[4]

[1]Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, arunkumar.inurture@gmail.com
[2]Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, vignesh.s@inurture.co.in
[3,4]B. Sc Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu
abineshmurugan53@gmail.com[3], althafaluvi29@gmail.com[4]
DOI: https://doi.org/10.55248/gengpi.4.523.42043

ABSTRACT—

The security of network devices can be threatened by a range of threats, including hacking, malware, and unauthorized access, making it essential to have measures in place to prevent and detect such security breaches works and acts as an IDS. This review paper explores the latest security feature by implementing the IDS to analyze the network traffic to detect and prevent cyber attacks on network devices. Also, the paper ensures using Suricata to control incoming and outgoing network traffic based on security rules.

Keywords— Raspberry Pi, Suricata, IDS, AWS, EveBox.

I. Introduction

The need for network security is growing rapidly as the number of connected devices and systems increases. Network devices are often integrated into critical systems, such as healthcare devices, industrial control systems, and smart homes, making them a prime target for cyber attacks. Therefore, it is imperative to implement robust security measures to protect network devices, and data from potential cyber-attacks to ensure the safety and privacy of user's data.

However, as the number of network devices increases and more information is shared among such devices, they become more vulnerable to cyber-attacks. Attackers can exploit security vulnerabilities in network infrastructures to perform complex cyber attacks. These cyber-attacks include denial of service (DOS) attacks, man-in-the-middle (MITM), ping of death attacks, and privacy threats.

Network devices have low power and limited computing and storage capabilities, thus making them vulnerable to several attacks. This thesis aims to design, implement, and test a gateway called the raspberry house, a security gateway for detecting and preventing intrusions on network devices. Specifically, the gateway targets one of the major attacks on network devices. The proposed gateway has been implemented using raspberry pi 3b+, and experimental analysis has been carried out against several DOS attacks, such as SYN flood attack, ICMP flood attack, and the. In addition, the proposed Network gateway is based on shell scripts, and to enable it to run detection and prevention mechanisms autonomously, our research also considers the use of system services. The results show that the raspberry house can detect, and alert, these dos attacks in real-time, particularly applicable to small network devices with resource constraints.

The objective of this project is to design and implement an effective IDS to monitor and protect networks, data, and devices from cyber attacks.

The project involves the following steps:

1. Analysis of network architecture and network devices to identify potential security vulnerabilities and threats.
2. Designing the IDPS to effectively detect and prevent cyber attacks, such as DOS, ping of death, and brute force attacks, etc...
3. Implementation of the IDS on network devices to monitor and protect them in real-time.

The IDS is an essential component of network security and helps to ensure the CIA of data and systems. The project will provide a secure and reliable solution for protecting network devices from cyber attacks and ensuring the safety of users and their data.

Network security is still a challenging topic for protecting devices and networks from cyberattacks. To help users detect the possible attacks targeting their network devices, we designed and proposed an IDS system running on the low-cost raspberry pi board. Our system can detect some popular attacks, which are password attacks, DOS attacks, and ping of death attacks.

II. Abbreviations and Acronyms

OS - Operating System
IDS - Intrusion Detection System
ICMP - Internet Control Message Protocol
DOS - Denial of Service
DDOS - Distributed Denial of Service
IP - Internet Protocol
CIA - Confidentiality, Integrity, and Availability
AWS - Amazon Web Service
S3 - Simple Storage Service
CLI - Command Line Interface

III. Raspberry Pi

The Raspberry Pi is a series of single-board computers developed by the raspberry pi foundation in the united kingdom. It was created to promote basic computer science to young people in developing countries. Raspberry Pi boards are small, low-cost, and high-performance computers that can run a variety of operating systems, including Linux and Windows 10 IoT Core. They can be used for a wide range of projects, including media centers, game consoles, robotics, and Internet of Things (IoT) devices.

Overall, the raspberry pi's versatility and low cost make it an attractive option for a wide range of projects and applications.

The Raspberry Pi can be used in various networking projects, some of which include:

Network Monitoring: The Raspberry Pi can be used to monitor network traffic, bandwidth usage, and network performance using open-source software such as Nagios or Zabbix.

Network Security: The Raspberry Pi can be used to create a network security appliance, such as a firewall or intrusion detection system (IDS), using open-source software such as Snort or Suricata

Network File Server: The Raspberry Pi can be used to create a low-cost file server for small offices or homes using software such as Samba or OwnCloud.

VPN Server: The Raspberry Pi can be used to create a VPN (Virtual Private Network) server, allowing remote access to a private network over the internet.

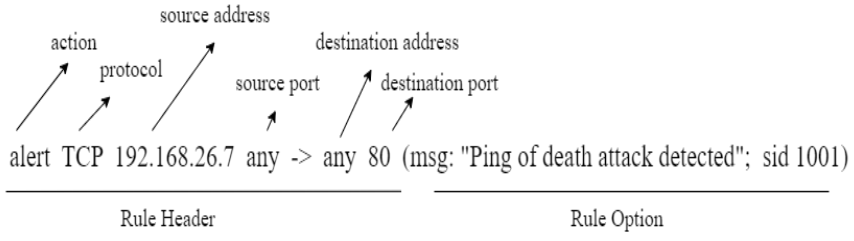
Overall, the raspberry pi's low cost and versatility make it an attractive option for networking projects, especially for small-scale or home-based projects.

And this research paper covers the network security appliance by using open source software Suricata.

IV. Suricata

Suricata is a free and open-source network intrusion detection and prevention system (IDS/IPS) that is designed to monitor network traffic for malicious activity. It uses a combination of signature-based and behavior-based detection techniques to identify potential threats, and can also be configured to block traffic that matches specific rules or

Signatures. Suricata can be configured to detect a wide range of network-based attacks, including malware, botnets, phishing, and DDoS attacks. It can also be used to monitor network traffic for compliance purposes, such as monitoring the transmission of sensitive data or monitoring network usage by employees. Overall, Suricata is a powerful and flexible IDS system that is widely used in the information security community for network monitoring and threat detection. Finally, Suricata can log information about network traffic and intrusion attempts, which can be used for analysis and forensic purposes to identify the root cause of a security incident and help prevent similar incidents from occurring in the future.



There are several advantages of using Suricata for network intrusion detection:

Open-Source: Suricata is free and open-source software, which means that it can be freely used, modified, and distributed without any licensing fees.

High Performance: Suricata is designed to handle high-speed network traffic, making it suitable for deployment in high-volume network environments.

Multi-Threaded: Suricata is designed to take advantage of multi-core processors, allowing it to efficiently process network traffic and improve performance.
Flexible Rule Engine: Suricata's rule engine is highly flexible and can be configured to detect a wide range of network-based attacks and malicious activities.
Protocol Support: Suricata supports a wide range of network protocols, including TCP, UDP, ICMP, and HTTP, making it suitable for monitoring traffic in a variety of network environments.

Overall, Suricata is a powerful and flexible network intrusion detection and prevention system that offers many advantages over proprietary alternatives. Its open-source nature, high performance, and flexibility make it an attractive option for organizations of all sizes looking to enhance their network security posture.

V. Amazon Web Service

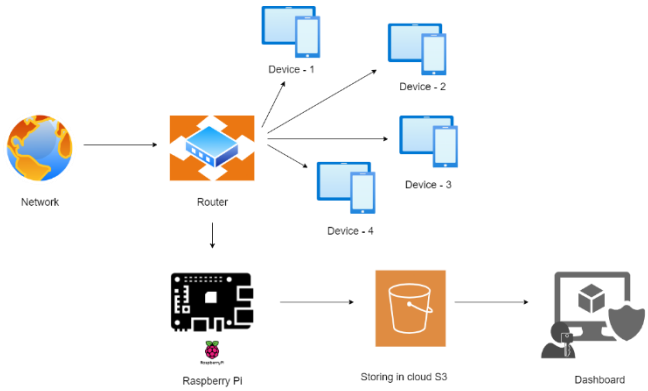
Amazon Web Services (AWS) is a cloud computing platform provided by amazon that offers a wide range of cloud-based services, including computing, storage, networking, database, and analytics services. The AWS CLI provides a unified interface for accessing and managing AWS services, making it easier for developers and system administrators to automate their workflows and manage their AWS resources. Amazon Simple Storage Service (S3) is a cloud-based storage service provided by Amazon Web Services (AWS). S3 is designed to provide scalable and durable storage for businesses of all sizes. S3 is also highly scalable, allowing businesses to easily scale their storage needs up or down as needed, without any upfront costs or commitments.

VI. EveBox

EveBox is an open-source web-based dashboard used for visualizing and analyzing events generated by the Suricata intrusion detection systems. It allows security teams to easily monitor their network traffic for potential security threats. EveBox provides a graphical user interface that displays alerts and other security events in real time. It offers various features such as event filtering, keyword search, IP reputation lookup, and geo-location mapping. It also supports multiple data sources, including Syslog, EVE JSON, and PCAP files. EveBox is highly customizable, allowing users to tailor the dashboard to their specific needs.

VII. Proposed Model

The proposed model involves several steps to successfully set up and configure Suricata for network security monitoring. The first step is to choose a Linux distribution that is compatible with Suricata and install it on a machine or virtual machine. Once the Linux distribution is set up, Suricata can be installed using the package manager of the chosen distribution or by compiling it from the source. The next step in the proposed model is to remove all the default rules and configure custom rules that will be used to detect and block suspicious traffic. In this case, the customs rules are designed to block suspicious ICMP packets and DOS attacks, etc... Once the rules have been set up, the network traffic can be monitored, and any suspicious activity that triggers the rules should be logged so that it can be investigated later. To store a log of blocked traffic, you can set up a cron job to upload the log to an AWS S3 bucket. This allows easy access to logs for detailed analysis and reporting. Finally, an evebox dashboard can be created to view Suricata's performance, including the logs, blocks, and other important metrics.



In summary, the proposed model involves installing and configuring Suricata, setting up custom rules, monitoring and logging suspicious activity, uploading logs to AWS S3, and creating a dashboard to view Suricata's performance. This model can be used to enhance network security by detecting and blocking potential security threats in real time.

VIII. Result & Discussions

Monitoring and analysis: A system capable of capturing and analyzing network traffic, identifying potential threats, and raising alerts when necessary.

Detection: A system that can alert malicious traffic, detect data exfiltration, and enforce access control policies.

Management and reporting: A system that provides a centralized management console, allows for monitoring and administration, and generates reports on the security status of the networks and devices.

☆ 1	2023-03-30 00:28:14 18 days ago	S: 52.219.158.195 D: 192.168.245.252	Possible Brute Force Attack Detected
☆ 1	2023-03-30 00:28:14 18 days ago	S: 192.168.245.252 D: 52.219.158.195	Possible Brute Force Attack Detected
☆ 3	2023-03-30 00:27:55 18 days ago	S: 192.168.245.116 D: 192.168.245.252	Possible Ping of Death attack detected
☆ 9534	2023-03-30 00:24:05 18 days ago	S: 192.168.245.252 D: 192.168.245.116	Possible Brute Force Attack Detected
☆ 9590	2023-03-30 00:23:46 18 days ago	S: 192.168.245.116 D: 192.168.245.252	Possible Brute Force Attack Detected
☆ 2	2023-03-30 00:13:10 18 days ago	S: fe80::030b:6f70:63fa:0b3f D: ff02::0016	Possible Ping of Death attack detected
☆ 2	2023-03-30 00:13:10 18 days ago	S: fe80::0c5d:d9ff:fefe:6eaf D: ff02::0001	Possible Ping of Death attack detected
☆ 1	2023-03-30 00:12:31 18 days ago	S: fe80::030b:6f70:63fa:0b3f D: ff02::0001	Possible Ping of Death attack detected
☆ 1	2023-03-30 00:12:21 18 days ago	S: :0000 D: ff02::0001:ffd2:4fa7	Possible Ping of Death attack detected
☆ 1	2023-03-30 00:09:25 18 days ago	S: 52.219.160.206 D: 192.168.245.252	Possible Brute Force Attack Detected
☆ 1	2023-03-30 00:09:25 18 days ago	S: 192.168.245.252 D: 52.219.160.206	Possible Brute Force Attack Detected

IX. Conclusion

Network security is still a challenging topic for protecting smart devices and networks from cyberattacks. To help users detect the possible attacks targeting their smart home devices, we designed and proposed an IDS system running on the low-cost raspberry pi board. Our system can detect some popular attacks, which are password attacks, DOS/DDOS attacks, and ping of death attacks. IDS provides three detection modes: mode by using Suricata IDS, anomaly-based mode by comparing with the auto-generated behavior profiles of each device, The detection results are shown as the graphics on the raspberry pi's user dashboard and as the alert however, we still get some false negative resulting in low detection accuracy.

X. Future Works

The future works of network security IDS involve leveraging advanced technologies to enhance the detection and prevention of sophisticated cyber attacks. Some potential areas of development include

1. Artificial Intelligence and Machine Learning: AI and ML can be used to enhance the accuracy of IDS by analyzing large amounts of network traffic and identifying patterns that may indicate an attack.

2. Cloud-based IDS: Cloud-based IDS can provide real-time monitoring and threat intelligence to help organizations detect and respond to threats quickly and efficiently.

3. Integration with other security tools: Integrating IDS with other security tools such as firewalls, antivirus software, and intrusion prevention systems can provide a comprehensive security solution that can detect and prevent a wide range of threats.

4. Automation: Automating the IDS processes can help reduce response times and increase the efficiency of security teams, enabling them to quickly respond to threats and mitigate their impact.

5. Threat Intelligence: Incorporating threat intelligence data into the IDS can help enhance its ability to detect and respond to new and emerging threats.

By leveraging these technologies and strategies, network security IDS can continue to evolve and provide organizations with robust security solutions to protect against the constantly evolving threat landscape.

REFERENCES

1. H. Harshita, "Detection and prevention of ICMP food DDOS attack," International Journal of New Technology and Research 2017.

2. P. Wanda and H. Jie, “A Survey of Intrusion Detection System,” International Journal of Informatics and Computation, Nov - 2018.

3. C. V. and S. P, “Icmp food attacks: A vulnerability analysis,” in Cyber Security. Advances in Intelligent Systems and Computing, vol. 729. Springer, Singapore, 2018.

4. Akash Garg and Prachi Maheshwari, “Performance Analysis of Snort-based Intrusion Detection System” International Conference on Advanced Computing and Communication Systems - 2018

5. Khalaf, B. A., Mostafa, S. A., Mustapha, A., Ismaila, A., Mahmoud, M. A., Jubaira, M. A., Hassan, M. H. A simulation study of syn flood attack in a cloud computing environment. 2019.

6. Radhika Chapaneri and Seema Shah, “A Comprehensive Survey of Machine Learning-Based Network Intrusion Detection” Springer Nature Singapore Pte Ltd - 2019.

7. Y. Jia, M. Wang, and Y. Wang, “Network intrusion detection algorithm based on deep neural network,” IET Information Security - 2019.

8. Z. Chiba et al, “Newest Collaborative and Hybrid Network Intrusion Detection Framework Based on Suricata and Isolation Forest Algorithm” Casablanca, Morocco - 2019.

9. A. J. Cui, C. Li, and X. M. Wang, “Real-time early warning of network security threats based on improved ant colony algorithm,” in Proceedings 12th International Conference on Intelligent Computation Technology and Automation - 2019.

10. N. Gao, L. Gao, Q. Gao, and H. Wang, “An Intrusion Detection Model Based on Deep Belief Networks,” - 2020.

11. Yusur Falah, Adnan Mohsin Abdulazeez "Intrusion Detection Systems Based on Machine Learning Algorithms" - 2021.

12. Bulletin of Electrical Engineering and Informatics Vol. 10, Rasefiberry: Secure and efficient Raspberry-Pi based gateway for smart home IoT architecture April - 2021.