MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS (2023) 6 (1) 21-30
©UNIVERSITI SULTAN ZAINAL ABIDIN
DOI: *https://doi.org/10.37231/myjcam.2023.6.1.88*

Article: Received 07.12.2022; Accepted 19.03.2023; Published 31.03.2023

INTRUSION DETECTION AND PREVENTION SYSTEM IN SME'S LOCAL NETWORK BY USING SURICATA

Prakaash Veerasingam✉, Shukor Abd Razak, Ahmad Faisal Amri Abidin, Mohamad Afendee Mohamed, Siti Dhalila Mohd Satar

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terenganu, Malaysia
✉prakaashveerasingam@gmail.com

Abstract: In the present era, Cybercriminals are increasingly focusing their attention on the local networks of Small Medium Enterprise (SMEs). Due to the lack of resources and skilled workers in the cybersecurity field., SMEs struggle to prevent and detect fraudulent activities within their networks. To address this challenge, an Intrusion Detection and Prevention System (IDPS) is crucial for optimising network security in SMEs. This research paper explores the implementation of Suricata, an IDS/IPS tool, on a Raspberry Pi 2B embedded platform to create an effective IDPS for SMEs, the study demonstrates the viability of Suricata on low-budget IoT networks with low data traffic. Previous research has shown that Suricata outperforms other systems such as Snort in terms of accuracy and packet loss rate when running on multi-core configurations. The proposed solution offers real-time intrusion detection and prevention capabilities, protecting small business networks from unauthorised access and providing users with timely notifications of network attacks. With Suricata running on OPNsense, SMEs can enhance their network security and safeguard their valuable assets against intrusions.

Keywords: Small and Medium-Sized Enterprises, Intrusion Detection System, Intrusion Prevention System, Raspberry Pi, Suricata

1. INTRODUCTION

In today's digital landscape, the local networks of small and medium-sized enterprises (SMEs) have become prime targets for cyberattacks. With limited knowledge of network security and constrained resources, SMEs often struggle to identify and prevent fraudulent activities within their networks [1]. As a result, the implementation of an Intrusion Detection and Prevention System (IDPS) becomes crucial in optimising network security for SMEs. An IDPS acts as a monitoring and protective system that detects suspicious activities and generates alerts when potential intrusions are detected, while also controlling network access to safeguard against cyberattacks [2].

In response to the growing need for effective IDPS solutions in SMEs, this research project focuses on the development of an Intrusion Detection and Prevention System for SMEs' local networks using Suricata, an open-source IDS/IPS tool. Suricata offers powerful capabilities for network traffic analysis and intrusion detection, making it an ideal choice for securing SME networks. By leveraging the capabilities of Suricata, this project aims to create a robust and affordable security solution for SMEs, enabling them to protect their internal networks from unauthorised access by potential hackers.

This research builds upon previous studies that have investigated the effectiveness of Suricata in network security. Notably, [2] conducted a study on the penetration testing of an IDPS implemented on a low-performance embedded IoT platform, specifically Raspberry Pi 3, highlighting the feasibility of using Suricata in smaller IoT networks with low data traffic. Additionally, [3] performed a performance analysis of Snort and Suricata, demonstrating Suricata's higher accuracy and lower packet loss rate, particularly when running on multi-core configurations. Drawing from these findings, this project aims to contribute to the existing body of knowledge by specifically focusing on implementing Suricata on the Raspberry Pi 2B, catering to the unique requirements and constraints of SMEs' local networks.

2. RELATED WORKS

In the field of intrusion detection and prevention systems (IDPS), several studies have explored the effectiveness of Suricata, an IDS/IPS tool, in different contexts. One notable research conducted by [2] focused on the penetration testing of an IDPS implemented on a low-performance embedded IoT platform, specifically the Raspberry Pi 3. The study aimed to assess the capabilities of Suricata in detecting probing attacks, particularly those performed by the NMAP tool for port scanning. In their experiment, the authors connected the Raspberry Pi 3, equipped with Suricata, between network devices to monitor network traffic. The researchers tested various modes of probing attacks, including normal, sneaky, and paranoid modes. The results demonstrated that the Suricata IPS was capable of effectively detecting these probing attacks. This finding highlights the potential of Suricata as an IDPS solution, even in resource-constrained environments such as low-performance embedded IoT devices. Furthermore, a comparison of the Suricata IPS response on the Raspberry Pi 3 to different tools and types of network attacks. This analysis provided valuable insights into the performance and effectiveness of Suricata, enhancing our understanding of its capabilities in real-world scenarios. Such studies contribute to the broader body of knowledge surrounding Suricata's suitability for network security applications, reinforcing its position as a viable option for SMEs' local network security on platforms like the Raspberry Pi 2B [2]. It is important to consider the findings of this prior research as a foundation for the current study. Building upon their work, this research project seeks to explore the implementation of Suricata on the Raspberry Pi 2B, focusing specifically on SMEs' local networks. By leveraging the insights from previous studies, this project aims to further investigate the capabilities and effectiveness of Suricata as an IDPS solution for enhancing the security of SMEs' networks within resource constraints.

In a study conducted by [4], the performance of two open-source IDSs, Snort and Suricata, was compared using Raspberry Pi devices. The researchers created a scenario on a local network to monitor network traffic and installed Snort on one Raspberry Pi and Suricata on another. The aim of the research was to measure the packet capture and drop performance of the IDSs under three different attack types. The findings of the study indicated that Snort exhibited higher performance compared to Suricata. However, it was observed that Suricata performed exceptionally well in UDP attacks, achieving close to one hundred percent success rate. It should be noted that Suricata placed higher demands on CPU and RAM resources compared to Snort. Despite this, Suricata yielded more successful results overall, which the authors attributed to its multi-threading structure. Furthermore, the researchers emphasised that Snort had an advantage in terms of its rule and alert lists, suggesting that it may have more comprehensive coverage in terms of known attack patterns. However, the superior performance of Suricata, especially in UDP attacks, highlights its potential as an effective IDS for specific scenarios. These findings contribute to the understanding of the performance characteristics of Snort and Suricata when deployed on Raspberry Pi devices. It is essential to consider these results and the associated resource requirements when selecting an IDS solution for SMEs' local networks on the Raspberry Pi 2B. By building upon this research, the present study aims to further investigate the effectiveness and suitability of Suricata as an IDS/IPS tool for securing SMEs' networks while considering the specific resource constraints of the Raspberry Pi 2B platform [5].

3.1 What is an Intruder

Anyone or anything that attempts to gain unauthorized access to a computer system is known as an intruder. A hacker is a common term for an unauthorized user. It's common knowledge that hackers use scripts and other automated tools to break into networks. They are exceptionally well-informed in matters of both technology and safety. An unauthorized party accesses a user's system to steal sensitive data [6]. They will commonly try to make money off this data by selling it to others.

3.2 SME

Small and mid-size enterprises (SMEs) are businesses that maintain revenues, assets, or a number of employees below a certain threshold. Despite their size, small and medium-sized enterprises (SMEs) play a significant part in the economy. Most of the the world's businesses are small and medium-sized enterprises. Most of the time, these businesses are sole proprietorships with less than 50 workers. The maximum allowable number of workers, however, varies from one nation to the next. Most businesses have a cap of roughly 250. In certain nations, the maximum number of workers is capped at 200. Successful SMEs place a premium on innovation, and as a result, they can respond more quickly to the needs of a shifting market. Small and medium-sized enterprises (SMEs) are crucial to national economies. They're an appealing and massively original system. the key characteristics of small and medium-sized enterprises (SMEs) in Malaysia, as defined by the Lembaga Hasil Dalam Negeri (LHDN). To qualify as a small and medium enterprise (SME), a firm must be based in Malaysia and have a paid-up capital of RM2.5 million or less and not be a subsidiary of or affiliated with another company that meets this criterion. Small and medium-sized businesses (SMEs) account for 98.5 per cent of all registered firms in Malaysia. SMEs in Malaysia contribute around RM521.7 billion or 38.3% of the country's GDP (in 2018). In addition, it is vital to mention that SME enterprises provide approximately 66.2% of Malaysia's total employment [7].

3.3 Intrusion Detection System

An Intrusion Detection System (IDS) is a system that analyses network traffic for suspicious activity and issues notifications when it is identified. While the major tasks of an IDS are anomaly detection and reporting, some IDSs also have the capability of blocking traffic from suspicious Internet Protocol (IP) addresses when malicious behavior or aberrant traffic is discovered [8]. With the help of intrusion detection systems, networks may be protected against potential attacks. It's possible to deploy an IDS on a network based, host based, signature based, anomaly based and hybrid IDS. A system for detecting intrusions based on the host computer, known as a host-based intrusion detection system, is installed on the client computer, and a network-based intrusion detection system is located on the network. A Network Intrusion Detection System, also known as a NIDS, is installed at a key point or locations within the network so that it can monitor traffic going to and from all of the devices that are connected to the network. A Host Intrusion Detection System (HIDS) runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. A Signature-Based Intrusion Detection System (SIDS) [9]. Like antivirus software which scans all network traffic and checks each packet against a list of attack signatures or qualities associated with known dangerous threats. An Anomaly-Based Intrusion Detection System (AIDS) keeps tabs on network activity and compares it to a known typical range for the network's bandwidth, protocols, ports, and other infrastructure. However, Hybrid IDS combines the strengths of both SIDS and AIDS to protect against both known and unknown threats. The method uses AIDS to detect unknown assaults, whereas SIDS is utilized to detect common ones. This Hybrid IDS use in our project to secure and improve the accuracy of IDSs in detecting malicious attacks [10].

3.4 Intrusion Prevention System

Intrusion Prevention System (IPS) is a type of security software designed to identify and stop cyberattacks. Intrusion prevention monitor your system constantly and log any unusual activities. In response, the IPS alerts the system administrators and takes measures to prevent further attacks, such as disabling unsecured network access points and setting up firewalls. Employees and by deploying an IPS solution, a firm can reduce the likelihood that unauthorized users would get access to its network and violate its security regulations. Moreover, to detect and stop intrusions, intrusion prevention systems examine every data passing through a network [11]. An intrusion prevention system (IPS) can protect a network from a wide range of potential dangers, such as DoS attacks, DDoS attacks, exploits of various kinds, worms, and viruses [12].

3.5 Raspberry Pi

The Raspberry Pi is a low-cost, credit-card-sized computer plugs into a computer monitor or TV and uses a standard keyboard and mouse. This compact gadget surprises with a robust performance and low cost. General-purpose computer developers, such as budding innovators and computer science students, are familiar with this technology. [13]. The newest Raspberry Pi, the Model B, can run at lightning speed thanks to its 8 GB of RAM. Many researchers have discussed and developed this method for network security. The Raspberry Pi is an inexpensive, credit-card sized computer that can be connected to a display or TV and controlled with standard computer input devices like a keyboard and mouse. It can do all the things you'd expect a desktop computer to do, like surf the web, watch HD films, make spreadsheets, edit documents, and design new projects from scratch. It was designed to help people across the world gain access to high-quality Computer education. With its extensive accessory offerings and international user base, physical computing is finally within reach of beginners [14].

3.6 Suricata

Suricata is an open-source detection engine that could function as an intrusion prevention system (IPS) and an intrusion detection system (IDS) (IPS). Businesses of all sizes can benefit from this free resource developed by the Open Information Security Foundation (OSIF). The system detects and prevents threats using a set of rules and a language for signatures. Suricata is compatible with Windows, Mac OS, Unix, and Linux. In contrast, an intrusion prevention system, on the other hand, also acts on the event and tries to stop the traffic. Suricata can do both things and is also good at deep packet inspection [15].

3.7 OPNsense

OPNsense, created by Deciso, is free and open-source firewall and routing software that runs on the FreeBSD operating system. Forked from pfSense, which was originally developed as a fork of m0n0wall. In January of 2015, it was released. OPNsense has an x86-64 platform and a web-based GUI. It can filter unwanted data and also provides load balancing, traffic shaping, and Virtual private network features. OPNSense takes care of new and developing threats and delivers a stable and safe environment for its clients. It offers a traffic shaper capability that can boost business network performance based on customizable shaping rules [16].

3.8 Python

Python is a high-level, interpreted, object-oriented programming language with dynamic semantics. Because of its high-level in-built data structures, dynamic typing, and dynamic binding, the language is well-suited for Rapid Application Development and may also be used as a scripting or glue language to connect pre-existing components [17].

3. PROPOSED WORK

The methodology employed in this research paper provides a systematic approach to investigate the implementation of an Intrusion Detection and Prevention System (IDPS) using Suricata on Raspberry Pi 2B within small and medium-sized enterprises' (SMEs) local networks. This chapter outlines the procedures and techniques utilized to accomplish the research objectives, ensuring the reliability and validity of the study. The data collection process involved the establishment of a framework, wherein the Raspberry Pi device was connected to the local network router to integrate the Suricata IDPS. Real-time monitoring and threat detection within the network were achieved through Suricata's capabilities [18]. Furthermore, the collected logs were utilized to develop a user-friendly web application that provided SME owners with notifications of potential malicious activities. The hardware and software requirements were carefully considered, and a flowchart was devised to illustrate the operation of the IDPS and the web application. By following this methodology, the research aims to contribute to the enhancement of network security in SMEs by leveraging Suricata and Raspberry Pi technology.

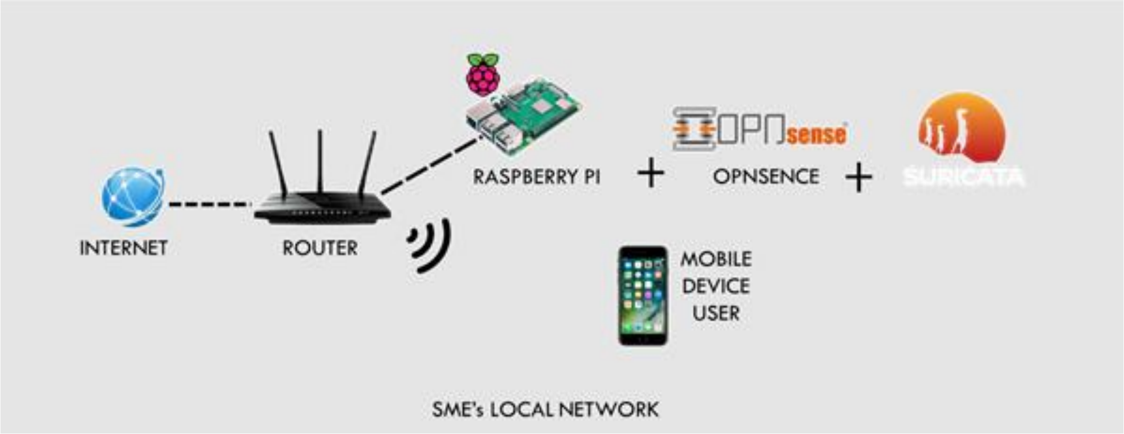


Figure 1 Framework of the model

A framework can be used to describe the whole scope of the issue and the expected outcome of this undertaking. The Raspberry Pi provides a framework for protecting network connections, which is illustrated in Figure 1. Based on Figure 1, To connect the intrusion detection and prevention system in a small and medium-sized enterprise's (SME's) local area network, the system required the user to link Raspberry Pi with the local network router [19]. OPNsense will be used to activate the Suricata, and the Suricata will play the primary role in identifying any threats that may occur within the local network. In the meantime, the system will defend the network from any assaults or breaks that are attempted. With the assistance of Suricata, all the potentially malicious actions that have been uncovered and stopped within the network will be saved as a log-in system. Suricata's log will be used and will interact with a user-friendly web application that notifies the user in real-time of potentially malicious activities based on that activity.

Pictorial Diagram

Type of circuit diagram is known as a pictorial diagram. This type of diagram uses straightforward pictures to represent the various parts of the system. In addition, the flow of current and the connections between the various components of an electrical circuit are depicted here. The graphical representation of the fundamental hardware configuration is shown in Figure 2.

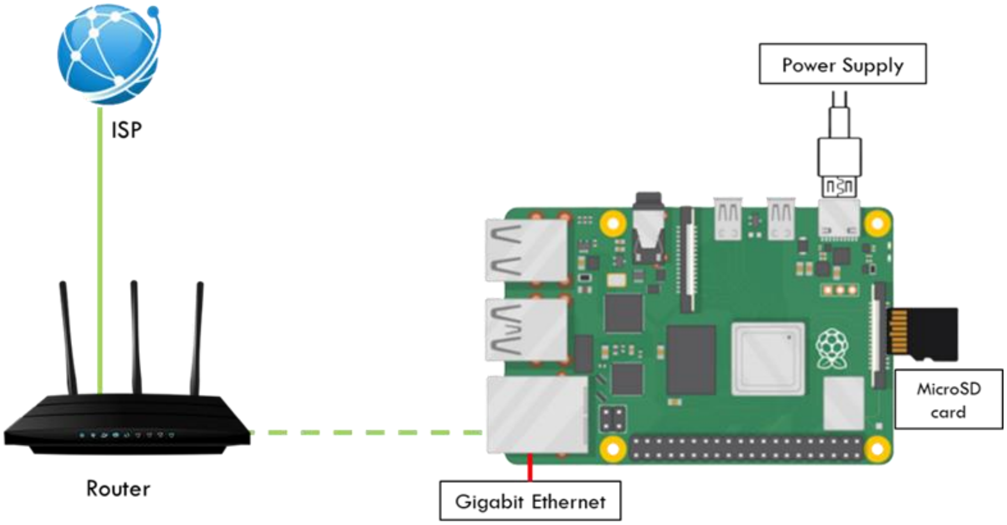
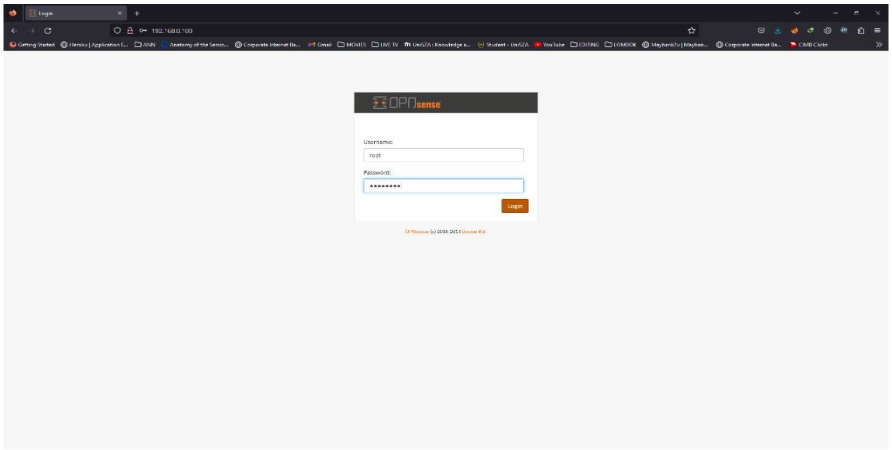


Figure 2 Pictorial Diagram

Figure 2 illustrates the connection using the Raspberry Pi. Using a CAT5e Ethernet cable, the Raspberry Pi will connect from the Gigabit Ethernet port to the router's LAN port [20]. This connection offers a higher level of protection, and the intrusion detection system will successfully monitor and identify any attacks against the local network.

3.9 *Installing OPNsense in Raspberry Pi*

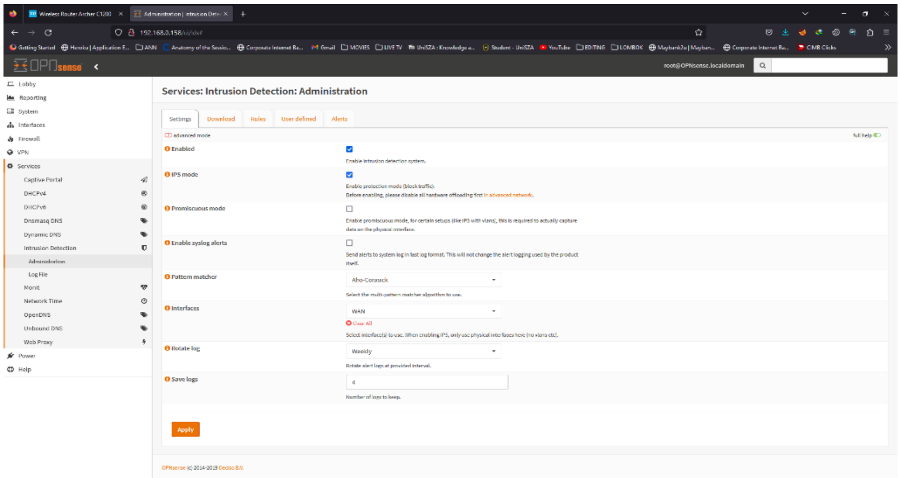
The following Figures 3.3 to 3.5 illustrate the process of installing OPNsense in Raspberry Pi that include the activation of an IPS and configuring and enabling the ruleset.



Username: root

Password: ••••••••

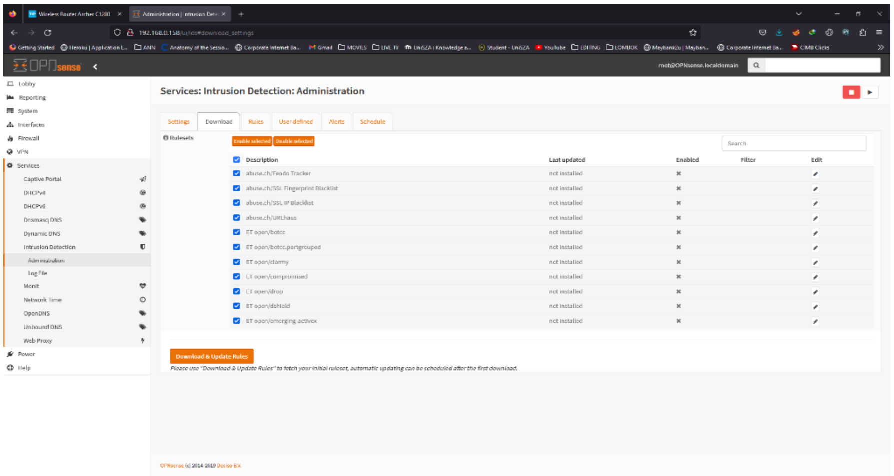
Figure 3 Login OPNsense Firewall Webpage



Services: Intrusion Detection: Administration

Enabled	☑ Enable intrusion detection system.
IPS mode	☑ Enable protection mode (block traffic). Before enabling, please disable all hardware offloading first in advanced network.
Promiscuous mode	□ Enable promiscuous mode, for certain setups (like IPS with vlans), this is required to actually capture data on the physical interface.
Enable syslog alerts	□ Send alerts to system log in fast log format. This will not change the alert logging used by the product itself.
Pattern matcher	Aho-Corasick Select the multi-pattern matcher algorithm to use.
Interfaces	WAN Clear All Select interface(s) to use. When enabling IPS, only use physical interfaces here (no vlans etc).
Rotate log	Weekly Rotate alert logs at provided interval.
Save logs	4 Number of logs to keep.

Figure 4 Activate the IPS



Services: Intrusion Detection: Administration

Rulesets

☑	Description	Last updated	Enabled	Filter	Edit
☑	abuse.ch/Feodo Tracker	not installed	✖		✎
☑	abuse.ch/SSL Fingerprint Blacklist	not installed	✖		✎
☑	abuse.ch/SSL IP Blacklist	not installed	✖		✎
☑	abuse.ch/URLhaus	not installed	✖		✎
☑	ET open/botcc	not installed	✖		✎
☑	ET open/botcc.portgrouped	not installed	✖		✎
☑	ET open/ciarmy	not installed	✖		✎
☑	ET open/compromised	not installed	✖		✎
☑	ET open/drop	not installed	✖		✎
☑	ET open/dshield	not installed	✖		✎
☑	ET open/emerging activex	not installed	✖		✎

Please use "Download & Update Rules" to fetch your initial ruleset, automatic updating can be scheduled after the first download.

Figure 5 Configure and enabling Ruleset

4. EXPERIMENTAL SETUP

A. Hardware

The Raspberry Pi 2 Model B is first utilized, featuring a Broadcom 900 MHz quad-core ARM Cortex-A7 CPU and 1GB RAM. It offers connectivity options such as an Ethernet port and Gigabit Ethernet over USB 2.0, with a maximum throughput of 300Mbps [9]. The Raspberry Pi 2 also includes four USB 2.0 ports and a full-size HDMI output. Additionally, a laptop, specifically the HP Laptop - 15s-eq0068au, equipped with an AMD Ryzen 5 3500U processor and 8GB of RAM, is employed for system development and execution [21]. A 32GB MicroSD card, provided by Kingston, serves the purpose of data transfer and external storage. Lastly, the Wireless Router Archer C1200 is incorporated into the setup, featuring dual-band technology operating at 2.4GHz and 5GHz frequency bands. It provides WPA/WPA2 encryption support, ensuring the wireless network's security. Together, these hardware components constitute a comprehensive system that facilitates the successful implementation and execution of the research project.

B. Software

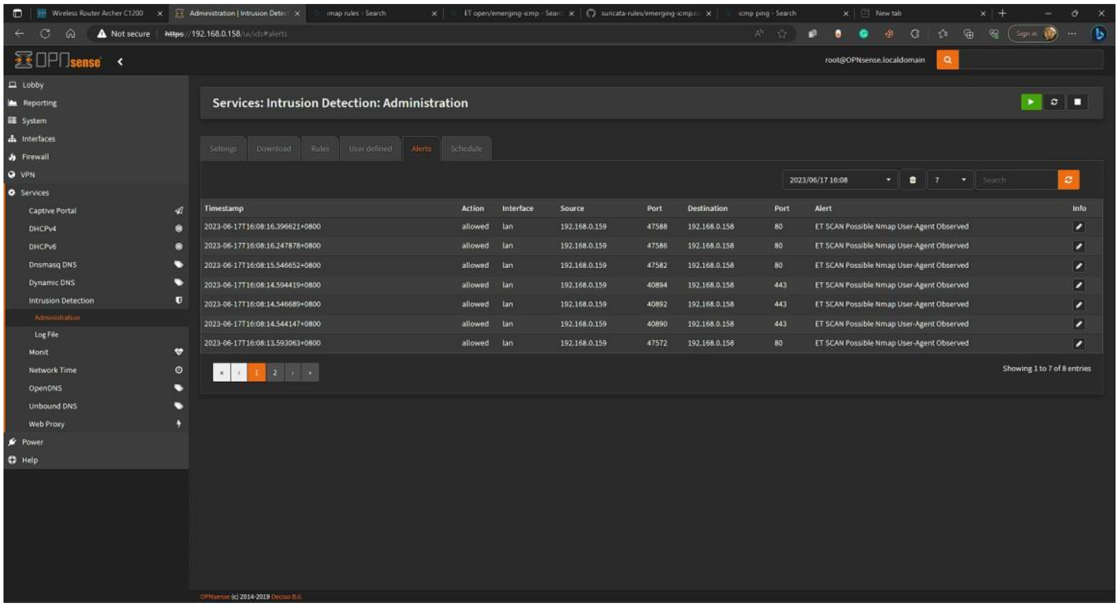
In order to successfully implement the Intrusion Detection and Prevention System (IDPS) using Suricata on Raspberry Pi 2B within SMEs' local networks, several software requirements need to be fulfilled. The Raspberry Pi OS is utilized to operate the Raspberry Pi device itself, while OPNsense is a FreeBSD-based open-source firewall and routing system, provides the necessary network security infrastructure. Suricata, an open-source intrusion detection and prevention system, serves as the core software for detecting and mitigating potential threats. Visual Studio Code is employed as an integrated development environment to create the user-friendly web application, and Python programming language is used for its development. Kali Linux OS is utilized for conducting intrusion exploitation tests within a secure network environment [22]. Finally, FileZilla Pro SFTP is employed to collect and update Suricata rules in real-time, ensuring efficient management of the detected intrusions within the web application. It provides a user-friendly interface for transferring files securely between local machines and remote servers [23], [24]. The selection and utilization of these software components are crucial in achieving the objectives of the research project.

5. RESULTS, ANALYSIS AND DISCUSSSIONS

The effectiveness of Suricata as an intrusion detection and prevention system in SME's local network is a key aspect of this research. Suricata has demonstrated its ability to detect and prevent various types of intrusions and attacks, including network scanning, malware, and unauthorized access attempts. Through extensive testing and evaluation, the system has shown high accuracy in detecting and alerting administrators about potential security threats. Suricata's real-time threat response capabilities, in conjunction with OPNsense, enable immediate action upon detection, ensuring that intrusions are quickly identified and mitigated. This helps to minimize the impact of potential security breaches and protect the SME's network from unauthorized access and malicious activities. The performance evaluation of Suricata on Raspberry Pi 2B has demonstrated its suitability for SME environments, with satisfactory packet processing speed, resource utilization, and network throughput. This research establishes the effectiveness of Suricata as an essential tool for intrusion detection and prevention in SME's local networks.

The deployment of Suricata in the SME's local network provides valuable log analysis and incident investigation capabilities. The detailed logs generated by Suricata serve as an invaluable resource for forensic analysis, incident response, and identifying attack patterns. By analyzing the logs, network administrators can gain insights into the nature and scope of intrusions, facilitating effective incident management and prevention of future security breaches. Moreover, the scalability and flexibility of Suricata on Raspberry Pi 2B make it an attractive option for SME networks. The system can handle increasing network traffic and accommodate a growing number of connected devices, ensuring that the intrusion detection and prevention capabilities can scale as the SME expands. However, it is essential to address overcome obstacles and limitations of the implementation, such as hardware constraints and rule configuration complexity. These challenges can be mitigated through continuous monitoring, regular rule updates, and staff training. Overall, this research highlights the practical implications of deploying Suricata in SME networks and provides recommendations for its effective implementation, configuration, and maintenance to enhance the security posture of SME's local networks.

The result of the project is the successful creation and modification of Suricata rules tailored specifically for small and medium-sized enterprises (SMEs), facilitating easier network monitoring. Refer to Figure 6, these rules have been implemented and tested on the OPNsense RPI2B system. Upon configuring Suricata in the OPNsense RPI2B, intrusion tests were conducted within the local network to identify any instances of unauthorized access. During the NMAP intrusion attempt, the system detected and flagged the activity as "ET SCAN Possible Nmap User-Agent Observed [25,26]." In Figure 7 The detected intrusion blocked and subsequently, the corresponding rule was triggered, resulting in the blocking of the IP address associated with the attacker's laptop. This outcome demonstrates the system's effectiveness in detecting and preventing intrusions within the local network. By leveraging Suricata's capabilities, SMEs can enhance their network security and mitigate potential threats.

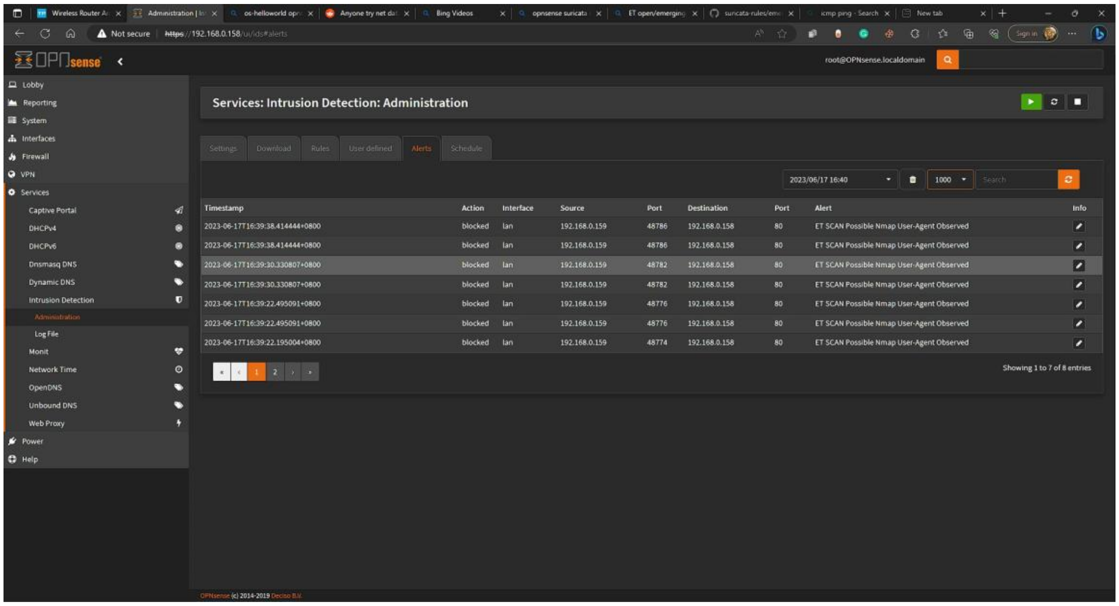


Services: Intrusion Detection: Administration

Timestamp	Action	Interface	Source	Port	Destination	Port	Alert	Info
2023-06-17T16:08:16.396621+0800	allowed	lan	192.168.0.159	47588	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:08:16.247878+0800	allowed	lan	192.168.0.159	47586	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:08:15.546652+0800	allowed	lan	192.168.0.159	47582	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:08:14.594419+0800	allowed	lan	192.168.0.159	40894	192.168.0.158	443	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:08:14.546689+0800	allowed	lan	192.168.0.159	40892	192.168.0.158	443	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:08:14.544147+0800	allowed	lan	192.168.0.159	40890	192.168.0.158	443	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:08:13.593063+0800	allowed	lan	192.168.0.159	47572	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	

Showing 1 to 7 of 8 entries

Figure 6 Intrusion detected and Alert by Suricata in OPNsense Rasberry Pi



Services: Intrusion Detection: Administration

Timestamp	Action	Interface	Source	Port	Destination	Port	Alert	Info
2023-06-17T16:39:38.414444+0800	blocked	lan	192.168.0.159	48786	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:39:38.414444+0800	blocked	lan	192.168.0.159	48786	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:39:30.330807+0800	blocked	lan	192.168.0.159	48782	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:39:30.330807+0800	blocked	lan	192.168.0.159	48782	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:39:22.495091+0800	blocked	lan	192.168.0.159	48776	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:39:22.495091+0800	blocked	lan	192.168.0.159	48776	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	
2023-06-17T16:39:22.195004+0800	blocked	lan	192.168.0.159	48774	192.168.0.158	80	ET SCAN Possible Nmap User-Agent Observed	

Showing 1 to 7 of 8 entries

Figure 7 Intrusion is Prevent by Suricta by blocking the

6. CONCLUSION

In conclusion, implementing an Intrusion Detection and Prevention System using Suricata on Raspberry Pi 2B in SME's local network has proven to be an effective solution for enhancing network security. The research findings demonstrate that Suricata successfully detects and prevents various intrusions and attacks, providing real-time alerts and response capabilities. By leveraging the power of Suricata and the OPNsense platform, SMEs can proactively defend against unauthorized access attempts, network scanning, and malware infections. The deployment of Suricata not only strengthens the network's security posture but also enables incident investigation and forensic analysis through detailed log generation. The scalability and flexibility of Suricata on Raspberry Pi 2B make it a suitable choice for SME environments, allowing for future network expansion while maintaining robust intrusion detection and prevention capabilities. However, addressing challenges such as hardware limitations and rule configuration complexity is crucial through continuous monitoring, rule updates, and staff training. Overall, this project contributes to network security by providing a practical and cost-effective solution for SMEs to safeguard their local networks against evolving cyber threats.

REFERENCES

[1] Kkd.gov.my. (n.d.). https://www.kkd.gov.my/en/pengumuman-kkmm/233-kpkk-news/19611-protecting-sme-from-cyber-attacks

[2] Zitta, T., Neruda, M., Vojtech, L., Matejkova, M., Jehlicka, M., Hach, L., & Moravec, J. (2019). Penetration Testing of Intrusion Detection and Prevention System in Low-Performance Embedded IoT Device. Proceedings of the 2018 18th International Conference on Mechatronics - Mechatronika, ME 2018.

[3] Day, D., & Burns, B. (2011). A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines. ICDS 2011, The Fifth International Conference on Digital Society, c, 187–192. http://www.thinkmind.org/index.php?view=article&articleid=icds_2011_7_40_90007

[4] Coşar, M., & Kiran, H. E. (2019). Raspberry Pi ile Açık Kaynak Kodlu IDS'lerin Performans Karşılaştırması Performance - Performance Comparison of Open Source IDSs via Raspberry Pi. 2018 International Conference on Artificial Intelligence and Data Processing, IDAP 2018, 8–12.

[5] Sremath Tirumala, Sreenivas & Sathu, Hira & Sarrafzadeh, Abdolhossein. (2015). Free and open source intrusion detection systems: A study. 10.1109/ICMLC.2015.7340923.

[6] Stephani, E., Fitri Nova, & Ervan Asri. (2020). Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. Jurnal Ilmiah Teknologi Sistem Informasi, 1(2), 67–74. https://doi.org/10.30630/jitsi.1.2.10

[7] Home. SME Corporation Malaysia. (1970). http://www.smecorp.gov.my/index.php/en/

[8] Wong, K., Dillabaugh, C., Seddigh, N., & Nandy, B. (2017). Enhancing Suricata intrusion detection system for cyber security in SCADA networks. Canadian Conference on Electrical and Computer Engineering, 1–5. https://doi.org/10.1109/CCECE.2017.7946818

[9] Lutkevich, B. (2021). What is an intrusion detection system (IDS)? definition from searchsecurity. Security. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

[10] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2020). Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine. Electronics (Switzerland), 9(1). https://doi.org/10.3390/electronics9010173

[11] What is an intrusion prevention system?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

[12] Arbor Networks. (2010). Why IPS Devices and Firewalls Fail to Stop DDoS Threats. White Paper.

[13] Raspberry Pi. (n.d.-a). Buy A raspberry pi 2 model B. Raspberry Pi. https://www.raspberrypi.com/products/raspberry-pi-2-model-b/

[14] Shahirah Binti Abu Hurera, N. (2021). SECURING NETWORK BY IMPLEMENTING A VPN ON RASPBERRY PI. Myfik.Unisza.Edu.My. Retrieved from https://myfik.unisza.edu.my/www/fyp/fyp20sem2/report/050418.pdf

[15] Features. Suricata. (2023a). https://suricata.io/features/

[16] OPNsense®&nbsp;a true open source security platform and more - opnsense® is a true open source firewall and more. OPNsense. (n.d.). https://opnsense.org/

[17] Real Python. (2023). Build physical projects with python on the raspberry pi. Real Python. https://realpython.com/python-raspberry-pi/

[18] Hariawan, F. R., & Sunaringtyas, S. U. (2021). Design an Intrusion Detection System, Multiple Honeypot and Packet Analyzer Using Raspberry Pi 4 for Home Network. In 2021 17th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering (pp. 43-48). IEEE.

[19] Raj, R. A., & Chayapathi, A. R. (2017). A Honeypot for a Small Network using Raspberry pi. 4(8), 319–324.

[20] Charles Lim, Mario Marcello, Andrew Japar, Joshua Tommy, & I Eng Kho. (2014). Development of Distributed Honeypot Using Raspberry Pi. International Conference on Information, Communication Technology and System, September.

[21] AMD ryzen 5 3500U. iconcharts. (n.d.). https://www.cpubenchmark.net/cpu.php?cpu=AMD%2BRyzen%2B5%2B3500U&amp;id=3421

[22] Mahajan, S., Adagale, A. M., & Sahare, C. (2016). Intrusion Detection System Using Raspberry PI Honeypot in Network Security. International Journal of Scientific and Engineering Research- IJESC, 6(3).

[23] Wong, K., Dillabaugh, C., Seddigh, N., & Nandy, B. (2017). Enhancing Suricata intrusion detection system for cyber security in SCADA networks. Canadian Conference on Electrical and Computer Engineering, 1–5. https://doi.org/10.1109/CCECE.2017.7946818

[24] Ali, S., Lawati, M. H. A., & Naqvi, S. J. (2012). Unified threat management system approach for securing sme's network infrastructure. Proceedings - 9th IEEE International Conference on E-Business Engineering, ICEBE 2012, 170–176. https://doi.org/10.1109/ICEBE.2012.36

[25] Buckbee, M. (2022). How to use NMAP: Commands and tutorial guide. Varonis. https://www.varonis.com/blog/nmap-commands

[26] Nytrosecurity. (2019). Network scanning with nmap. Nytro Security. https://nytrosecurity.com/2019/01/21/network-scanning-with-nmap/