Design an Intrusion Detection System Using Raspberry Pi

Deepesh Agrawal
(211000016)
International Institute of Information
Technology, Naya Raipur
deepesh21100@iiitnr.edu.in

Rahul Sidar
(211000043)
International Institute of Information
Technology, Naya Raipur
deepesh21100@iiitnr.edu.in

Shikhar Reyya
(211000052)
International Institute of Information
Technology, Naya Raipur
shikhar21100@iiitnr.edu.in

***ABSTRACT* : In today's digitally connected world, securing networks against unauthorized access and malicious activities is of paramount importance. Intrusion Detection Systems (IDS) play a crucial role in safeguarding networks by identifying and responding to suspicious behavior and potential security breaches. This project aims to design and implement an Intrusion Detection System using Raspberry Pi, a versatile and cost-effective single-board computer. The proposed system utilizes the Raspberry Pi's computational capabilities and GPIO (General Purpose Input/Output) pins to monitor network traffic and detect anomalies. Through the integration of open-source software packages Snort, the Raspberry Pi will analyze incoming and outgoing network packets in real-time. Suspicious patterns and deviations from normal network behavior will trigger alerts, notifying administrators of potential security threats.**

Keywords : IDS (Intrusion Detection System), Raspberry Pi, Snort.

INTRODUCTION

With the proliferation of interconnected devices and the exponential growth of data traffic, ensuring the security of computer networks has become increasingly challenging. Cyber threats, ranging from malware attacks, to data breaches, pose significant risks to the integrity and confidentiality of sensitive information. In this context, the implementation of robust security measures, including Intrusion Detection Systems (IDS), is indispensable for detecting and mitigating potential threats in real-time. Traditionally, IDS solutions have been implemented on dedicated hardware appliances or high-end servers, often requiring substantial financial investments. However, the emergence of low-cost, miniature computing platforms such as the Raspberry Pi has opened up new possibilities for developing affordable yet effective security solutions. The Raspberry Pi, with its compact size, low power consumption, and sufficient computational capabilities, presents an attractive option for building custom IDS systems tailored to specific requirements. This project seeks to leverage the capabilities of the Raspberry Pi to design and implement an Intrusion Detection System capable of monitoring and analyzing network intrusion in real-time.

LITERATURE SURVEY

[1] In a study conducted by J. Jeremiah, an Intrusion Detection System (IDS) was proposed to bolster network security utilizing Raspberry Pi honeypot technology within the Kali Linux environment. Presented at the 2019 International Conference on Cybersecurity (ICoCSec), the research aimed to enhance cybersecurity measures through innovative means. The study emphasized the significance of IDS in detecting and mitigating security threats, leveraging Raspberry Pi's capabilities as a cost-effective computing platform. By deploying

honeypots on Raspberry Pi devices and integrating them with Kali Linux IDS, the system aimed to provide real-time monitoring and analysis of network traffic. The keywords associated with the study include Communication, Security, Information, Honeypot, Raspberry Pi, Data Analysis, Network, and Internet of Things (IoT). While the research showcased promising results in enhancing network security, it also underscored the importance of continuous refinement and adaptation to address evolving cyber threats.

[2].F. R. Hariawan and S. U. Sunaringtyas presented a research study focusing on the design and implementation of an integrated security system utilizing Raspberry Pi 4 for home network protection. The study, presented at the 2021 17th International Conference on Quality in Research (QIR), emphasized the importance of robust cybersecurity measures for home networks. By combining an Intrusion Detection System (IDS), multiple honeypots, and a packet analyzer, the system aimed to provide comprehensive protection against security threats. Leveraging the capabilities of Raspberry Pi 4, a versatile and cost-effective computing platform, the research proposed a practical solution for home network security. The study highlighted the significance of real-time monitoring and analysis of network traffic to detect and mitigate intrusions effectively. While promising, the research also identified challenges such as resource constraints and scalability issues that need to be addressed for optimal system performance. Overall, the study provided valuable insights into enhancing cybersecurity for home networks using Raspberry Pi-based solutions.

[3]In a recent study by Sasikumar and Seethal, the authors explored the development of a network intrusion detection and deduce system. Published in the Turkish Journal of Computer and Mathematics Education (TURCOMAT), the research focused on addressing the growing challenges of network security. The study emphasized the importance of robust intrusion detection mechanisms in identifying and mitigating security threats effectively. Additionally, the authors proposed a deduce system, which analyzed network traffic patterns to infer potential security breaches. By combining intrusion detection with deduce capabilities, the system aimed to provide comprehensive protection against network intrusions. The research highlighted the significance of real-time monitoring and analysis of network traffic in detecting anomalous behavior and unauthorized access attempts. While promising, the study also identified challenges such as false positives and scalability issues that need to be addressed for optimal system performance. Overall, the research contributed valuable insights into enhancing network security through innovative intrusion detection and deduce systems.Muhammad, Resevoa Moral, Indrarini Dyah Irawati, and Muhammad Iqbal conducted a study on the implementation of an integrated security system for network intrusion. Published in the Journal of Hunan University Natural Sciences, their research focused on addressing the challenges posed by network intrusions and enhancing cybersecurity measures. The study emphasized the importance of adopting a holistic approach to network security, integrating multiple security components to mitigate threats effectively. By combining intrusion detection, firewalls, encryption, and other security measures, the integrated system aimed to provide comprehensive protection against unauthorized access and malicious activities. The research highlighted the significance of proactive monitoring and response strategies in detecting and thwarting network intrusions. While promising, the study also identified challenges such as system complexity and resource constraints that need to be addressed for optimal system performance. Overall, the research contributed valuable insights into enhancing network security through the implementation of integrated security systems

PROBLEM STATEMENT

Developing a cost-effective, accessible, and adaptable intrusion detection system (IDS) remains a challenge for small businesses, educational institutions, and individuals due to the high cost, technical complexity, and limited customization options of existing solutions. Additionally, resource-constrained environments face difficulties in deploying and maintaining IDS systems. There is a need for a scalable and customizable IDS solution that leverages the Raspberry Pi platform to provide affordable, user-friendly, and effective network security monitoring capabilities.

MOTIVATION

The motivation behind this project is to address the pressing need for effective and affordable network security solutions in today's technology-driven world. Raspberry Pi is hosting critical services for a business or organization, downtime caused by a DDoS attack can lead to financial losses due to lost productivity, missed opportunities, or damage to reputation.

Raspberry Pi's networking capabilities, users can remotely monitor and manage their intrusion detection system and honeypot deployments from anywhere with internet access.

PROPOSED METHODOLOGY

Intrusion Detection System (IDS) uses honeypots as part of its strategy to detect and analyze suspicious activities or attempts by external systems to access a network or system.

A honeypot is a decoy system or network resource designed to attract and monitor unauthorized or malicious activities. If the IDS detects suspicious activities or signs of a potential intrusion, it generates alerts or notifications which can trigger further investigation, response actions, or mitigation measures to protect the network and systems.

Limitation :

- Limited detection capabilities of the Pentbox IDS system.
- Lack of advanced Rule-Based Analysis.
- Less comprehensive reporting and logging.

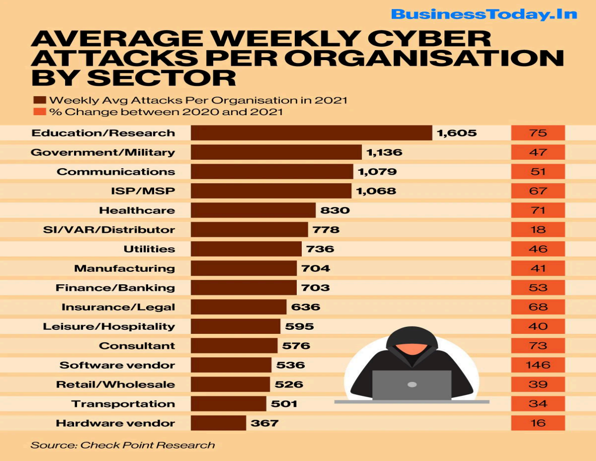

Fig 1 cyber attack stats

- Scaling challenge in a large environment.

Snort is a leading open-source network intrusion detection and prevention system (NIDS/NIPS) developed by Sourcefire, now owned by Cisco. It's widely used for real-time traffic analysis and packet logging on IP networks.It's highly customizable through the use of rules, which define conditions to trigger alerts or actions when specific network traffic patterns are detected. Snort can be deployed as a standalone sensor or integrated into existing security architectures, providing organizations with an effective means to monitor and protect their network infrastructure against cyber threats.

IMPLEMENTATION

fig2: snort

1. Installing Snort on Raspberry Pi:

Snort is a widely used open-source network intrusion detection system (NIDS) that can be installed on various platforms, including the Raspberry Pi. To install Snort on Raspberry Pi, you can use the following command in the terminal:

```
sudo apt install snort
```

2. Configuring the snort config file:

After installing Snort, you need to configure its main configuration file, snort.conf, to customize the IDS settings according to your network environment. One crucial configuration is setting the HOME_NET variable to specify the IP address range of your local network. You can edit the snort config file using a text editor like nano or vim:

```
sudo nano /etc/snort/snort.conf
```

3. Starting Snort Service:

After configuring snort.conf, you can start the Snort service using the following command:

```
sudo systemctl start snort
```

4.Checking Snort Service Status:

To verify that Snort is running correctly, you can check its status using the systemctl command:

```
sudo systemctl status snort
```

5. Viewing Traffic with Snort:

You can monitor network traffic in real-time using Snort's command-line interface. Run the following command to start Snort in verbose mode (-v):

```
sudo snort -v
```

This command will display detailed information about the network traffic being monitored by Snort.

6. Sending Email with Python Script:

To send email notifications from Raspberry Pi, you can use Python along with SMTP (Simple Mail Transfer Protocol) libraries such as smtplib. First, you need to write a Python script that connects to an SMTP server and sends an email. Here's the python script

```
import smtplib
smtpUser = 'rahulsidar1700@gmail.com'
smtpPass = 'axij regg sgps pawc'
toAdd = 'rahulsidar2056@gmail.com'
fromAdd = smtpUser
subject = 'TEST EMAIL using PYTHON'
header = 'To:' + toAdd + '\n' + 'From: ' + fromAdd + '\n' + 'Subject:' + subject
body = 'INTRUSION DETECTED IN YOUR SYSTEM'
print (header + '\n' + body)
s = smtplib.SMTP('smtp.gmail.com',587)
s.ehlo()
s.starttls()
s.ehlo()
s.login(smtpUser, smtpPass)
print("Login Successful")
s.sendmail(fromAdd, toAdd, header + '\n\n' + body)
s.quit()
```

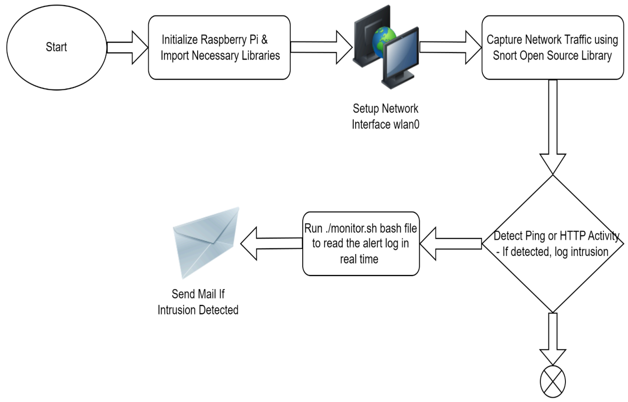
Start
Initialize Raspberry Pi & Import Necessary Libraries
Setup Network Interface wlan0
Capture Network Traffic using Snort Open Source Library
Detect Ping or HTTP Activity - If detected, log intrusion
Run ./monitor.sh bash file to read the alert log in real time
Send Mail If Intrusion Detected

fig3: flow chart

By following these steps, you can set up Snort on Raspberry Pi for intrusion detection and configure email notifications to alert you of potential security threats detected by the IDS**.**

RESULT

The result of this project is a functioning Intrusion Detection System (IDS) running on a Raspberry Pi, capable of monitoring network traffic, detecting anomalies, and alerting administrators to potential security threats.The project create a cost-effective and accessible solution for enhancing network security, particularly suitable for small-scale deployments, educational institutions, or individuals seeking to protect their networks against cyber threats. Additionally, the project demonstrates the versatility of the Raspberry Pi platform for implementing security solutions and showcases the integration of open-source software and custom scripts to achieve desired functionality.

CONCLUSIONS

The development and implementation of an Intrusion Detection System (IDS) using the Raspberry Pi platform represents a significant step towards addressing the challenges associated with network security in resource-constrained environments. Throughout this project, we have demonstrated the feasibility and effectiveness of leveraging the Raspberry Pi's computational capabilities to build a cost-effective, accessible, and customizable IDS solution. The findings of this research are the potential of the Raspberry Pi platform as a viable option for deploying intrusion detection solutions, particularly for small businesses, educational institutions, and individuals with limited resources or technical expertise. By democratizing access to network security technologies, we can empower organizations and individuals to safeguard their digital assets and mitigate the risks posed by cyber threats.

FUTURE SCOPE

Further enhancements and optimizations can be made to the IDS system, including the integration of additional detection mechanisms such as Integration with IoT Devices Extending the IDS to monitor and secure Internet of Things (IoT) devices connected to the network. This would involve developing lightweight agents or sensors compatible with various IoT platforms and protocols. Enhanced Machine Learning Algorithms, Further refining and optimizing the machine learning algorithms used for anomaly detection. This includes exploring deep learning techniques for more accurate and adaptive detection of network intrusions.

REFERENCES

[1] J. Jeremiah, "Intrusion Detection System to Enhance Network Security Using Raspberry PI Honeypot in Kali Linux," 2019 International Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, 2019, pp. 91-95, doi: 10.1109/ICoCSec47621.2019.8971117. keywords: {Communication;Security;Information;Honeypot;Raspberry Pi;Data Analysis;Network;Internet of Things (IoT)},

[2] F. R. Hariawan and S. U. Sunaringtyas, "Design an Intrusion Detection System, Multiple Honeypot and Packet Analyzer Using Raspberry Pi 4 for Home Network," 2021 17th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering, Depok, Indonesia, 2021, pp. 43-48, doi: 10.1109/QIR54354.2021.9716189.

[3] Sasikumar, Seethal. "Network intrusion detection and deduce system." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.9 (2021): 404-410.

[4]Muhammad, Reserva Moral, Indrarini Dyah Irawati, and Muhammad Iqbal. "Integrated Security System Implementation for Network Intrusion." Journal of Hunan University Natural Sciences 48.6 (2021).