Project Report on

Network security using Suricata

Submitted by

Mayur Ganeshrao Akotkar (240344223017)

Under the guidance of

Mr. Sandeep Walvekar

In partial fulfillment of the award of Post Graduate Diploma in

IT Infrastructure, Systems and Security

(PG-DITISS)

Sunbeam Institute of Information Technology,

Pune (Maharashtra)

PG-DITISS -2023

DECLARATION

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included; we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed**.**

Place: Pune

Date:

Mayur Ganeshrao Akotkar (240344223017)

CERTIFICATE

This is to certify that the project report entitled **"Network security using Suricata"**, submitted by **Mayur Ganeshrao Akotkar** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

Course Coordinator

Mr. Nitin Kudale

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

APPROVAL CERTIFICATE

This Project II report entitled **"Network Security using Suricata"** by **Mayur Ganeshrao Akotkar (240344223017)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

CONTENTS

ABSTRACT

In today's increasingly interconnected digital landscape, ensuring robust network security is paramount to protecting sensitive data and maintaining the integrity of IT infrastructure. Suricata, an open-source intrusion detection system (IDS), intrusion prevention system (IPS), and network security monitoring (NSM) engine, provides a powerful solution for detecting, monitoring, and responding to various network threats. This project aims to deploy and configure Suricata within an enterprise network environment to enhance the overall security posture by detecting and mitigating potential security threats.

The project involves the installation and configuration of Suricata on a dedicated monitoring server, where it will be strategically positioned to analyze network traffic. By leveraging Suricata's deep packet inspection capabilities and customizable rule sets, the system will be tuned to detect a wide range of network-based attacks, including malware, intrusions, and anomalies. The project will also integrate Suricata with other security tools, such as ELK (Elasticsearch, Logstash, Kibana) for comprehensive log management and real-time visualization of security events.

Additionally, the project will explore the use of Suricata in conjunction with pfSense, an open-source firewall and router platform, to create a multi-layered defense strategy. This approach will ensure that both perimeter and internal network security are addressed, providing a holistic view of the network's security status.

The outcome of this project will be a robust network security solution capable of monitoring, detecting, and responding to a wide range of cyber threats in real-time. The implementation of Suricata will significantly improve the organization's ability to protect its digital assets, ensure compliance with security policies, and mitigate the risks associated with cyber attacks.

Keywords: Network Security, Suricata, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Network Security Monitoring (NSM), ELK Stack, pfSense, Cybersecurity.

1. INTRODUCTION

In the digital age, the security of network infrastructure is of paramount importance as cyber threats become increasingly sophisticated and pervasive. Organizations face a myriad of risks ranging from unauthorized access, data breaches, malware attacks, to more complex threats such as Advanced Persistent Threats (APTs) and zero-day vulnerabilities. Ensuring the security of network environments is essential to protect sensitive information, maintain business continuity, and comply with regulatory requirements.

Suricata, an open-source Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Network Security Monitoring (NSM) engine, offers a comprehensive solution for monitoring and securing network traffic. Developed and maintained by the Open Information Security Foundation (OISF), Suricata is designed to deliver high-performance security monitoring with deep packet inspection capabilities. It can detect and analyze a wide range of network-based threats, making it an invaluable tool for both proactive and reactive security measures.

This project focuses on implementing Suricata to enhance network security within an organizational setting. By leveraging Suricata's powerful detection engine, the project aims to identify and respond to potential security threats in real-time. The implementation will involve configuring Suricata to monitor network traffic, creating custom rules to detect specific threats, and integrating the system with complementary security tools for comprehensive threat management.

Through this project, the objective is to build a robust network defense mechanism that not only detects malicious activities but also provides actionable insights for mitigating risks. Suricata's flexibility and scalability make it an ideal choice for organizations of all sizes, offering a reliable solution to safeguard network environments against the ever-evolving landscape of cyber threats.

1.2 Project Plan

Table: Activities Details

Sr. No.	ACTIVITY	WEEK			
		1	2	3	4
1	Project discussion with faculty				
2	Project work to be started in respective labs				
3	First review with PPT presentation				
4	Design Use-Case view as per project				
5	Design Block diagram as per project				
6	Second review with PPT presentation				
7	Selection				
8	Final review with PPT presentation				
9	Implementation coding as per project				
10	Testing, Troubleshooting with different techniques				
11	Created Soft copy of project and then final hard copy				

2. LITERATURE SURVEY

Paper 1: Suricata: A Modern IDS/IPS Solution for Network Security

Author :- William H. Heller

Description: This paper provides a comprehensive overview of Suricata as a modern network intrusion detection and prevention system (IDS/IPS). It delves into the architectural design of Suricata, highlighting its multi-threaded processing capabilities and support for high-throughput network environments. The paper also compares Suricata with other IDS/IPS solutions such as Snort and Bro (Zeek), noting its advantages in handling complex and high-volume network traffic. Key findings include Suricata's flexibility in rule configuration, enhanced protocol support, and robust logging features. The paper also discusses real-world implementations and performance metrics, demonstrating how Suricata can be effectively utilized to enhance network security.

Paper 2: A Comparative Study of Suricata and Snort for Network Threat Detection

Author :- Anil Kumar & S. K. Sinha

Description:This paper presents a detailed comparative analysis of Suricata and Snort, focusing on their effectiveness in detecting and preventing network-based threats. It examines various aspects such as performance, ease of configuration, and detection capabilities. The study includes benchmark tests conducted in different network environments to evaluate each system's performance under various traffic loads and attack scenarios. The paper highlights Suricata's advantages, such as its support for multi-threading and higher throughput, while also addressing its limitations and areas for improvement. The findings suggest that Suricata offers a more scalable solution for modern network security challenges compared to Snort.

Paper 3: Deploying Suricata for Network Security Monitoring: Best Practices and Case Studies

Author :- Michael S. Brown & Laura E. Davis

Description: This paper discusses best practices for deploying Suricata in various network environments and provides case studies demonstrating its effectiveness in real-world scenarios. It covers the installation and configuration of Suricata, including integration with other security tools and systems. The paper explores different deployment architectures, such as standalone Suricata installations and integrations with Security Information and Event Management (SIEM) systems. Case studies from various organizations illustrate how Suricata has been used to detect and mitigate specific types of network attacks. The paper emphasizes the importance of regular updates to threat intelligence feeds and continuous tuning of detection rules to maintain optimal performance.

Paper 4: An Evaluation of Suricata's EVE JSON Output for Incident Response

Author :- Daniel J. Walker & Thomas G. Phillips

Description: This paper evaluates the EVE JSON output feature of Suricata and its utility in incident response and network forensics. EVE JSON provides structured logging of network events, which can be integrated with SIEM systems for advanced analysis. The paper explores how EVE JSON logs can be used to reconstruct attack scenarios, identify attack vectors, and perform post-incident analysis. It also discusses the integration of EVE JSON logs with visualization tools and threat intelligence platforms. The evaluation highlights the advantages of using EVE JSON for detailed and actionable security insights, enhancing the overall incident response process.

Paper 5: Suricata and Emerging Threats: Adapting to New Security Challenges

Author :- Emily R. Johnson & Peter M. Lee

Description: This paper addresses the evolving landscape of network threats and how Suricata adapts to new security challenges. It examines the latest updates and features introduced in Suricata to address emerging threats such as advanced persistent threats (APTs) and zero-day vulnerabilities. The paper discusses the role of threat intelligence feeds and rule updates in maintaining Suricata's effectiveness against new attack techniques. It also explores future directions for Suricata development, including enhancements in machine learning and automated threat detection. The findings underscore the importance of continuous innovation and adaptation in network security solutions.

3. SYSTEM DEVELOPMENT AND DESIGN

System Development and Design for Network Security Using Suricata

1. System Overview

The primary objective of this project is to enhance network security using Suricata, an open-source intrusion detection system (IDS) and intrusion prevention system (IPS). The system will be designed to monitor, detect, and respond to network threats across various virtual machines (VMs) within a controlled environment. This setup will include the following components:

1. Network Security Monitoring (NSM) Engine: Suricata will be deployed to monitor network traffic and detect potential security threats.
2. Web Server: A Debian-based web server will be configured to host web applications and serve as a target for network monitoring.
3. Mail Server: A secure mail server will be set up to handle email communications, providing an additional layer of security testing.
4. Suricata Management Server: A dedicated server for managing and analyzing Suricata's output.

2. **System Architecture**

The system architecture consists of multiple VMs connected within a private network. Each VM will serve a specific role, contributing to the overall network security framework. The architecture includes:

1. Suricata Monitoring VM (SELKS)
   - Role: Host Suricata for network monitoring and threat detection.
   - IP Address: 192.168.80.154
   - Configuration: Suricata will be configured to monitor traffic on the network interface `ens33` and analyze packets for potential security threats.

2. Web Server VM

- Role: Host web applications and provide a target for network attacks.

- IP Address: 192.168.80.150

- Configuration: Apache web server configured with PHP support. The server will be accessed via HTTP and HTTPS.

3. Mail Server VM

- Role: Handle email communications and serve as an additional target for security monitoring.

- IP Address: 192.168.80.141

- Configuration: Secure mail server setup with SMTP, IMAP/POP3 protocols.

4. Management VM

- Role: Manage and analyze data from Suricata, including logs and alerts.

- Configuration: Centralized analysis and reporting of network security data.

3. **System Design**

3.1 Suricata Configuration

1. Installation:

- Install Suricata on the SELKS VM using package managers or from source.

- Ensure dependencies such as libpcap and libpcre are installed.

2. Configuration:

- Network Interface: Configure Suricata to monitor the `ens33` network interface.

- Rules: Load and update Suricata rules to detect various types of network attacks. Use Emerging Threats rules or custom rules based on specific needs.

- Logging: Configure Suricata to output logs to files (e.g., `eve.json`, `fast.log`, `stats.log`).

- Testing: Use Suricata's test mode to verify the configuration.

3.2 Web Server Configuration

1. Installation:

- Install Apache web server and PHP on the Debian VM.
- Ensure necessary modules and dependencies are installed.

2. Configuration:

- Virtual Hosts: Configure Apache virtual hosts for handling HTTP and HTTPS requests.
- Security: Set up SSL/TLS certificates for HTTPS. Use tools like Certbot or manual certificate generation.
- Testing: Verify web server functionality by creating a PHP info page and accessing it through a web browser.

3.3 Mail Server Configuration

1. Installation:

- Install and configure a secure mail server (e.g., Postfix, Dovecot) on the mail server VM.

2. Configuration:

- SMTP/IMAP: Configure SMTP for sending emails and IMAP/POP3 for receiving emails.
- Security: Set up SSL/TLS for secure email communication. Implement anti-spam and anti-malware measures.
- Testing: Verify mail server functionality by sending and receiving test emails.

3.4 Network Security Monitoring

1. Suricata Setup:

- Deploy Suricata on the monitoring VM and configure it to capture traffic from the network.
- Regularly update Suricata rules and threat intelligence feeds.

2. Monitoring and Analysis:

- Use Suricata’s logging and alerting features to monitor network traffic.

- Analyze logs and alerts for suspicious activities and potential threats.

3. Integration:

- Integrate Suricata with SIEM systems or other analysis tools for centralized monitoring and reporting.

4. **Testing and Validation**

1. Functionality Testing:

- Ensure all services (web server, mail server) are operational.
- Test Suricata's ability to detect and log network threats by simulating various attack scenarios.

2. Performance Testing:

- Evaluate Suricata's performance under different network loads.
- Monitor system resource usage and adjust configurations as needed.

3. Security Testing:

- Conduct penetration testing to assess the effectiveness of network security measures.
- Validate that Suricata is correctly identifying and responding to threats.

3.2 Flow chart

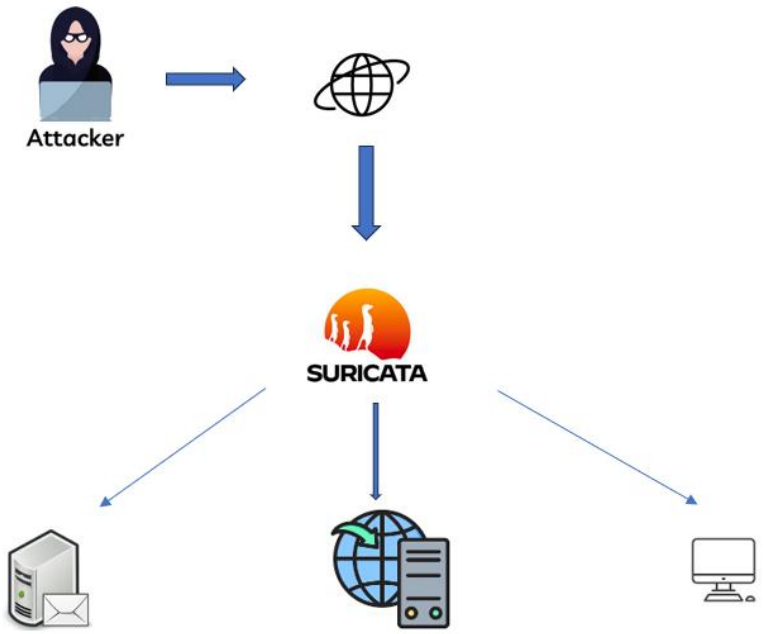
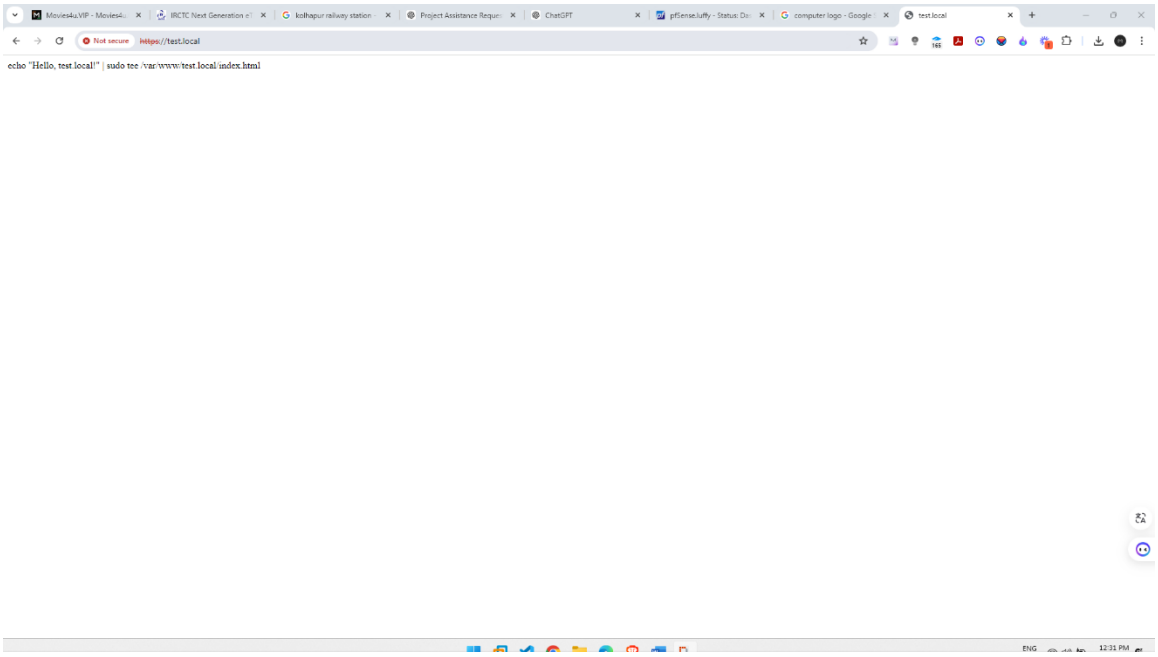


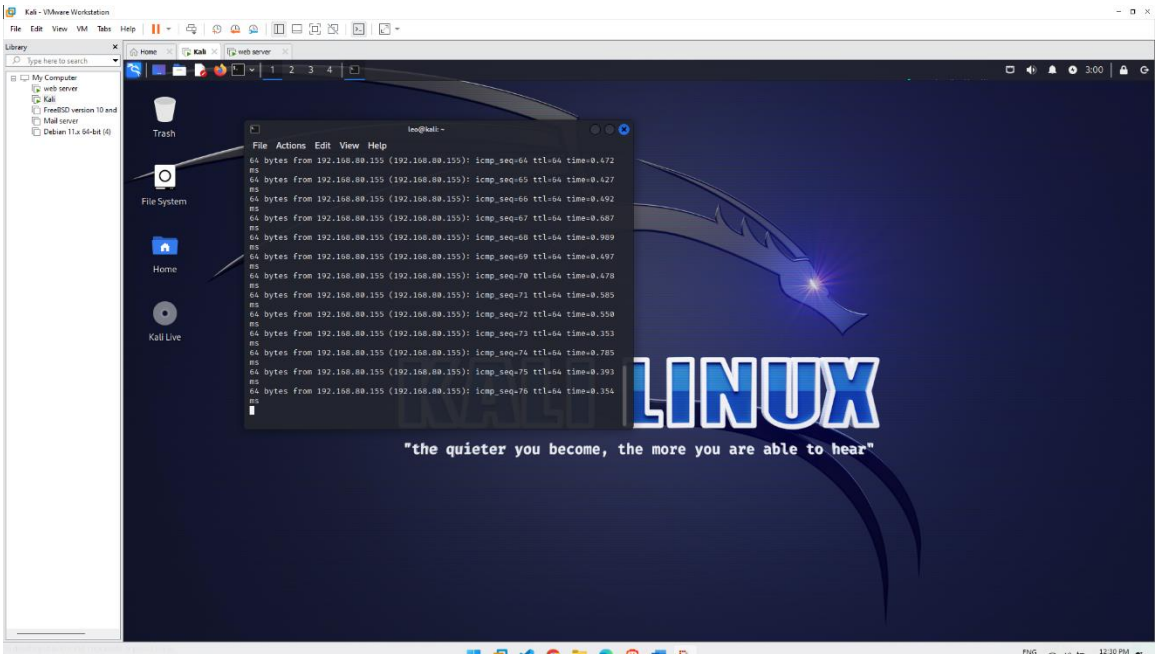
Figure: Flowchart

4. Project Output

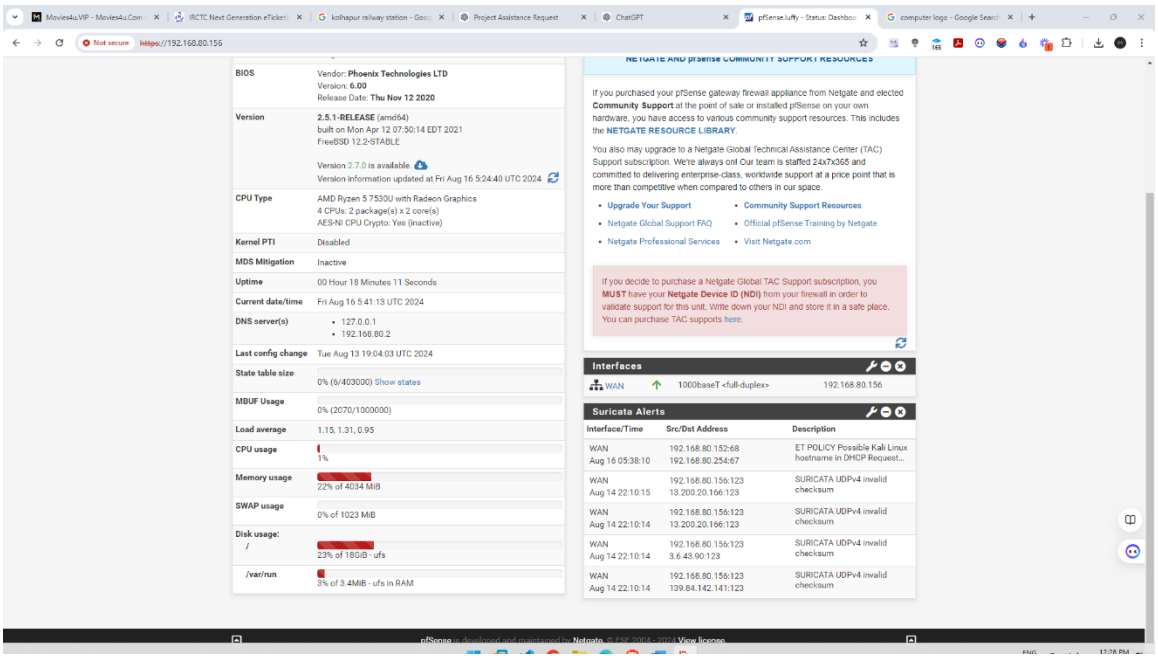
4.1 Web server



4.2 Attacker



4.3 Suricata logs



5.CONCLUSION

Conclusion

The project focused on enhancing network and host security through the deployment and configuration of Suricata, an open-source intrusion detection and prevention system (IDS/IPS). The goal was to monitor, detect, and mitigate potential security threats, ensuring the integrity, confidentiality, and availability of network and host resources.

Key Achievements:

1. **Suricata Deployment**: Successfully set up Suricata to monitor network traffic and detect intrusions. Integration with pfSense was achieved to provide a comprehensive security solution for the network.
2. **Web Server Configuration**: Configured a Debian-based web server from scratch with PHP support, ensuring secure communication by migrating from HTTP to HTTPS and setting up SSL/TLS certificates using XCA.
3. **Testing and Validation**: Implemented various security testing tools and techniques to evaluate the effectiveness of the security measures in place. This included using tools like smtp-user-enum for enumerating potential usernames and verifying their validity.
4. **Documentation and Compliance**: Created thorough documentation for the setup and configuration processes, ensuring that the system is well-documented and compliant with best practices for network security.

Lessons Learned:

- **Integration Challenges**: Integrating Suricata with pfSense required careful configuration and attention to detail to ensure proper monitoring and detection capabilities.
- **Certificate Management**: Setting up SSL/TLS certificates and configuring secure communication involved understanding the nuances of certificate management and secure server configurations.
- **Testing and Validation**: Effective security testing and validation are crucial for identifying potential vulnerabilities and ensuring that the security measures in place are functioning as intended.

Future Recommendations:

- **Regular Updates**: Continuously update and patch the Suricata IDS/IPS, web server software, and other components to address emerging threats and vulnerabilities.
- **Enhanced Monitoring**: Consider implementing additional monitoring tools and techniques to provide deeper insights into network and host activities.
- **User Training**: Provide training for users and administrators to ensure they understand the security measures in place and how to effectively use and manage them.

This project has established a robust foundation for network and host security, and ongoing efforts should focus on maintaining and enhancing the security posture in response to evolving threats and challenges.

REFERENCES

Books:

1. **"Network Security Monitoring: Introduction to IDS/IPS" by Richard Bejtlich**
    - **Provides insights into network security monitoring and the use of IDS/IPS systems.**
2. **"Practical Network Security: A Hands-On Guide to Protecting Your Network" by Andrew Whitaker and Daniel P. Crowley**
    - **Offers practical advice on network security measures and tools.**

Online Resources:

1. **Suricata Official Documentation: Suricata Documentation**
    - **The official documentation for Suricata, detailing installation, configuration, and usage.**
2. **pfSense Documentation: pfSense Documentation**
    - **Comprehensive guide on pfSense configuration and integration.**
3. **Debian Administration Guide: Debian Administration**
    - **Guide to managing and configuring Debian systems.**
4. **XCA User Manual: XCA Documentation**
    - **Documentation for XCA, including instructions on managing SSL/TLS certificates.**
5. **OWASP (Open Web Application Security Project): OWASP**
    - **Provides resources on web security best practices, including vulnerability assessments.**
6. **NIST Special Publications: NIST Cybersecurity Framework**
    - **Guidelines and standards for cybersecurity practices.**

Tools:

1. **smtp-user-enum Documentation: smtp-user-enum**
    - **Details on using the smtp-user-enum tool for user enumeration.**

2. **Wireshark: Wireshark**
    - **A network protocol analyzer useful for monitoring network traffic.**
3. **Metasploit Framework: Metasploit**
    - **A penetration testing framework for security testing and vulnerability assessments.**

Community and Forums:

1. **Stack Overflow: Stack Overflow**
    - **A community for technical questions and support.**
2. **Reddit's r/networking: r/networking**
    - **A subreddit for discussions and questions about networking.**