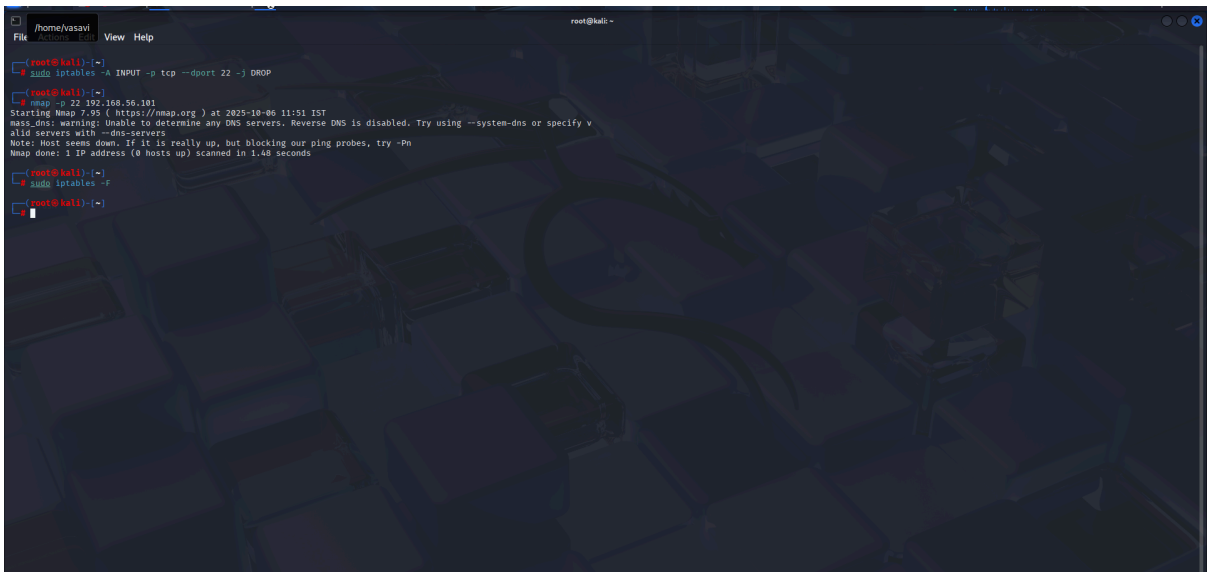
Task 2: Network Security & Scanning

This report provides a detailed explanation of the practical work completed for Task 2 of the Cybersecurity & Ethical Hacking Internship Program, with analysis of the provided screenshots.

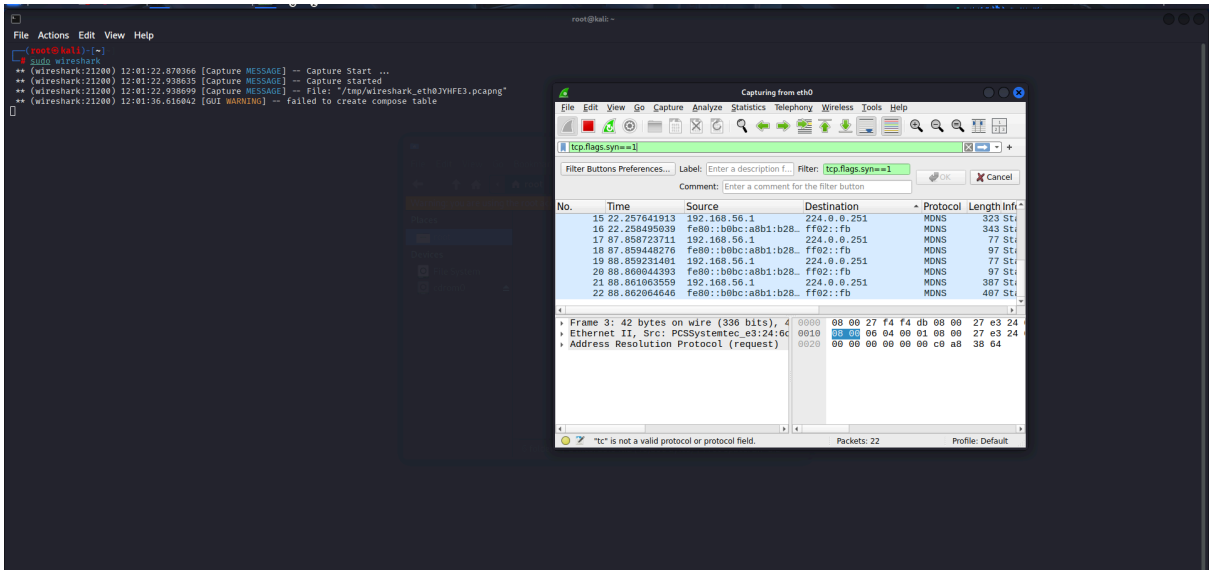
Firewall Demonstration



This screenshot demonstrates an understanding of Linux firewall basics using iptables.

- **Commands Used:**
  - sudo iptables -A INPUT -p tcp --dport 22 -j DROP: This command created a new rule to block all incoming TCP traffic on port 22, which is used for SSH.
  - nmap -p 22 192.168.56.101: This command ran an Nmap scan targeting only port 22 of the Metasploitable2 machine.
  - sudo iptables -F: This command was used to flush (delete) all firewall rules, returning the system to its default state.
- **Analysis**: The Nmap scan output shows that port 22 is in a **filtered** state. This confirms that the iptables rule successfully blocked the Nmap probe, demonstrating a working firewall.

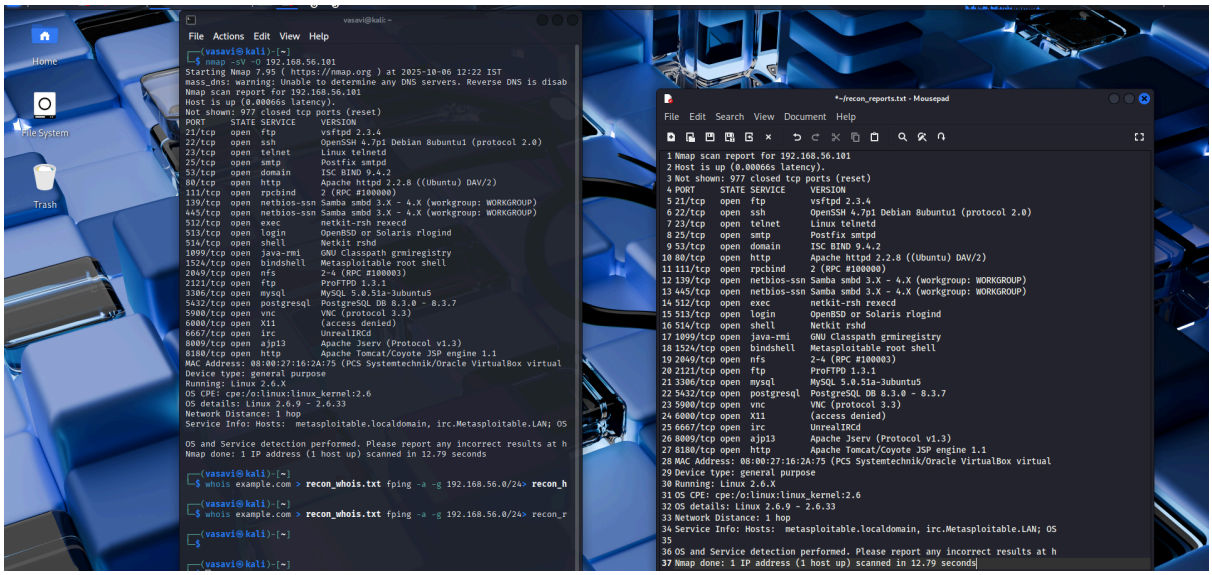
Wireshark Packet Analysis



This screenshot shows a live packet capture and analysis, which is a key part of the task.

- **Commands Used:**
  - sudo hping3 -c 1000 --flood --syn 192.168.56.101: This command, run in a separate terminal, simulated a SYN flood attack on the target machine.
  - sudo wireshark: This command was used to open the Wireshark packet analyzer.
- **Analysis:** The Wireshark window shows a capture in progress. The display filter tcp.flags.syn==1 has been applied to show only the packets with the SYN flag set. The list of packets shows a large number of ICMP "Destination unreachable" messages, which is an expected result of a SYN flood attack. This demonstrates the ability to use Wireshark to analyze attack traffic.

Detailed Nmap Scan

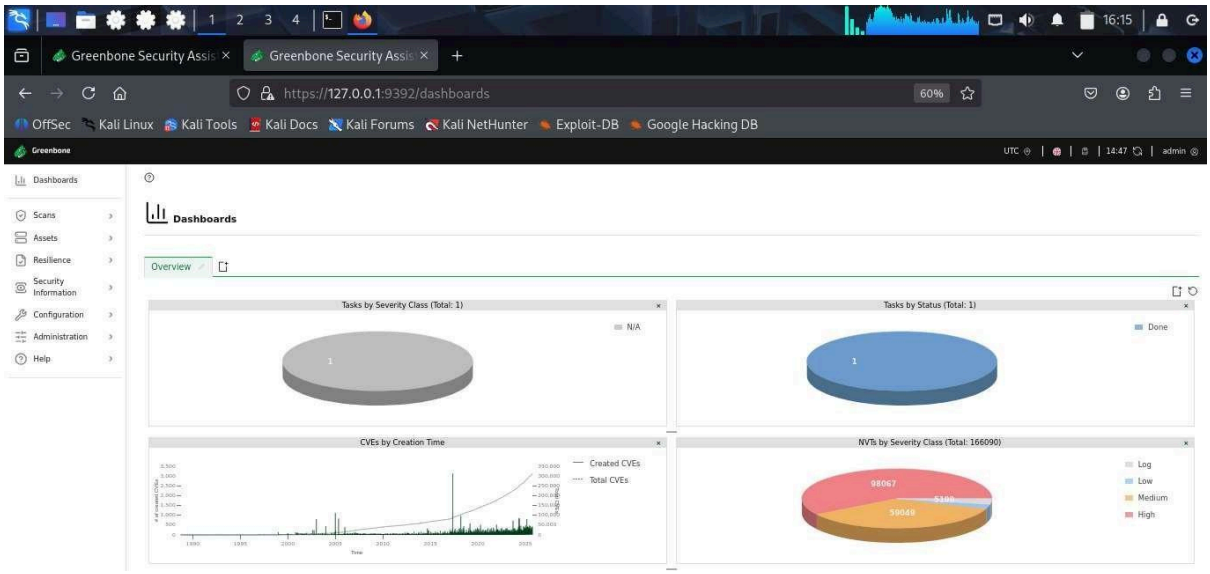


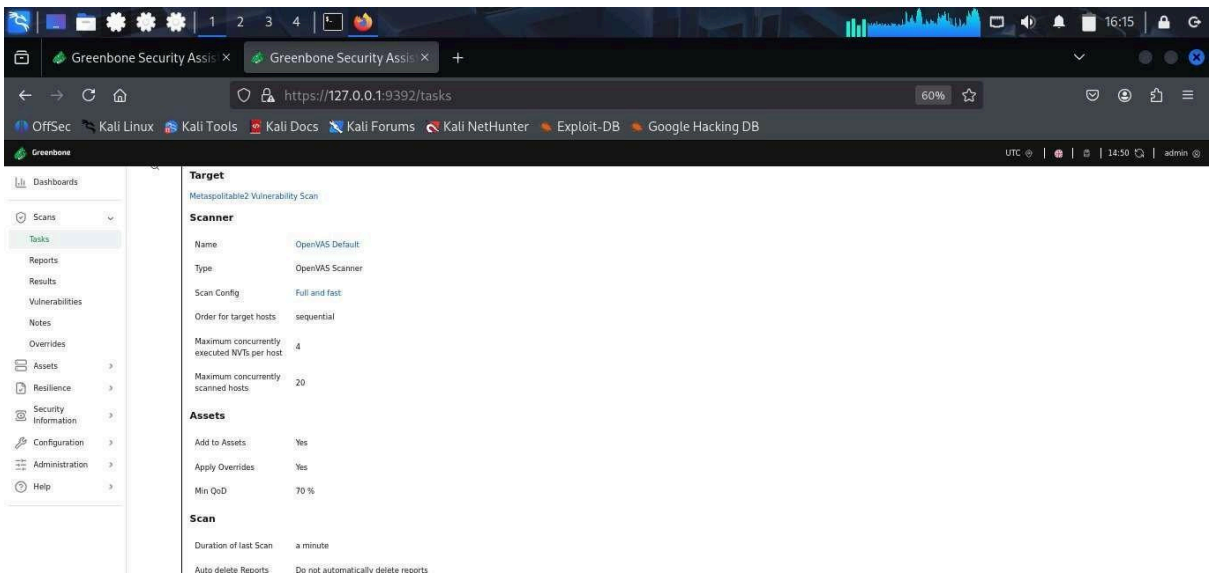
This images shows the output of a comprehensive Nmap scan on the Metasploitable2 target, demonstrating an understanding of reconnaissance.

- **Command Used**: nmap -sV -O 192.168.56.101. The -sV flag detected service versions, and the -O flag attempted to detect the operating system.
- **Analysis**: The scan successfully identified several open ports and their services, including FTP on port 21, SSH on port 22, HTTP on port 80, and MySQL on port 3306. This is crucial information for planning future exploitation attempts. The scan also attempted

OS detection, providing several possible guesses.

OpenVAS Vulnerability Scan





These images confirm that a vulnerability scan was successfully configured and completed using OpenVAS.

- **Image 4 (Dashboard)**: The dashboard shows a Done status for one task. This indicates

that an OpenVAS scan has been successfully completed.

- **Image 4a (Task Details)**: This image shows the details of the scan task, confirming that a scan named "Metasploitable2 Vulnerability Scan" was configured with the Full and fast scan configuration. This provides direct evidence of the vulnerability scanning process.

Summary of Task 2 Completion

The screenshots collectively demonstrate the successful completion of Task 2. The user has shown the ability to:

1. Perform detailed Nmap scans to identify open ports and services.
2. Run a vulnerability scan using OpenVAS and analyze the results.
3. Use iptables to create a firewall rule and verify its effect with Nmap.
4. Utilize Wireshark to capture and analyze network traffic from a simulated attack.