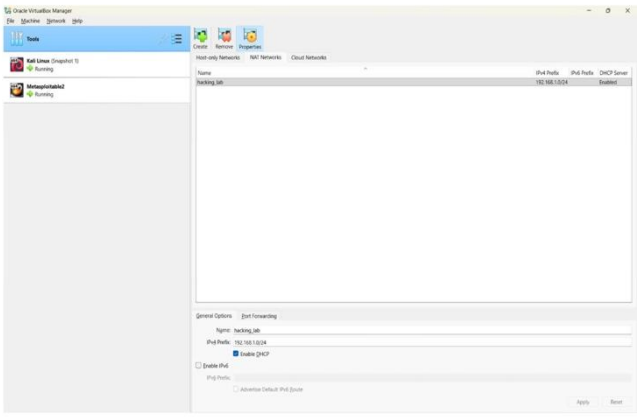
Penetration Testing Lab Using Nmap

Tool Used: Nmap
Environment: Kali Linux (Attacker) & Metasploitable2 (Target)
Host OS: Windows
Virtualization Tool: VirtualBox

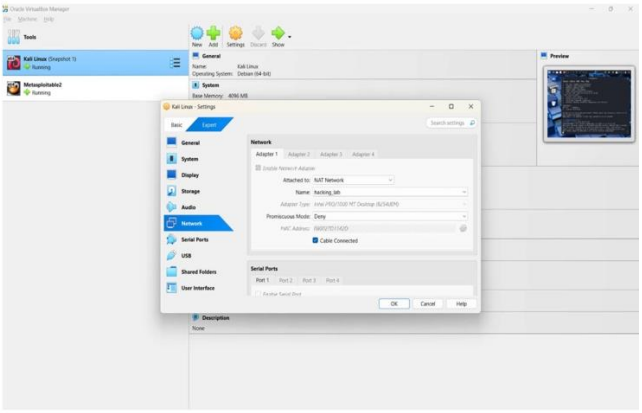
Step 1: Lab Environment Setup

VirtualBox showing Kali & Metasploitable2 running

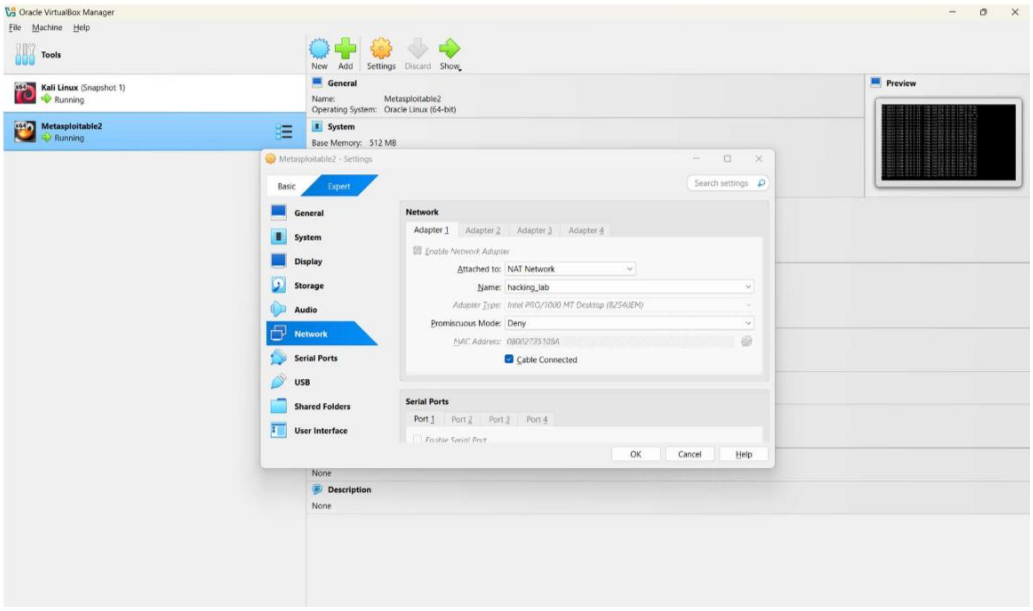
hacking_lab network



Kali connection to hacking_lab



Metasploitable2 connection to hacking_lab



Two virtual machines were created and configured on a Windows laptop using VirtualBox:

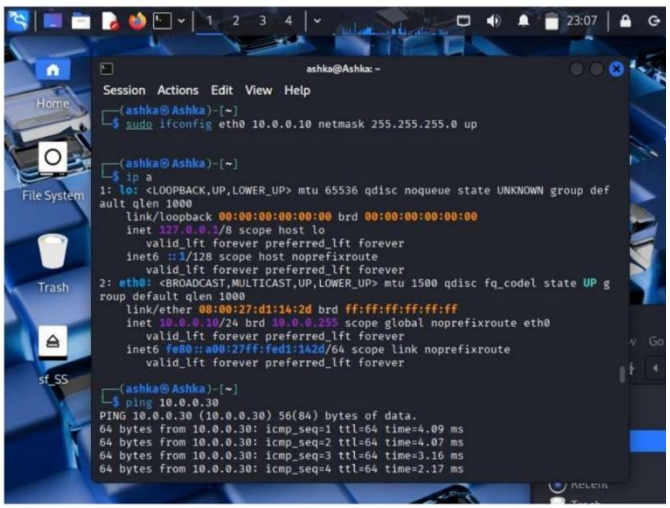
- Kali Linux – used as the attacker machine
- Metasploitable2 – used as the vulnerable target machine

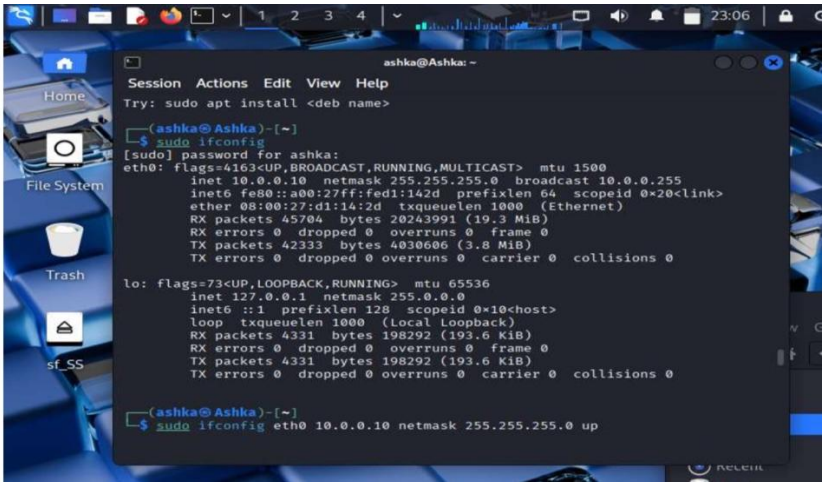
Both machines were connected to the same virtual network to allow communication.

Step 2: Verifying Network Connectivity

Kali terminal showing IP address
Metasploitable2 terminal showing IP address

Kali ping to 10.0.0.30





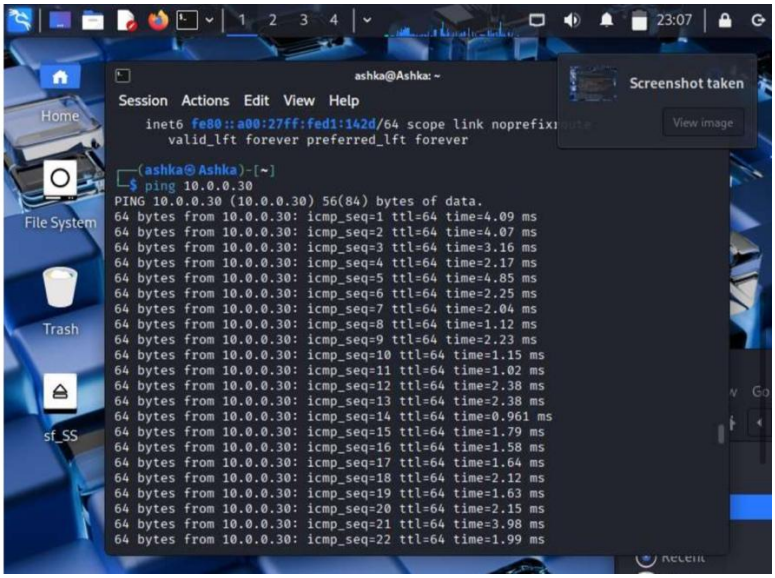
The IP addresses of both virtual machines were identified to confirm network connectivity. The following commands were used.

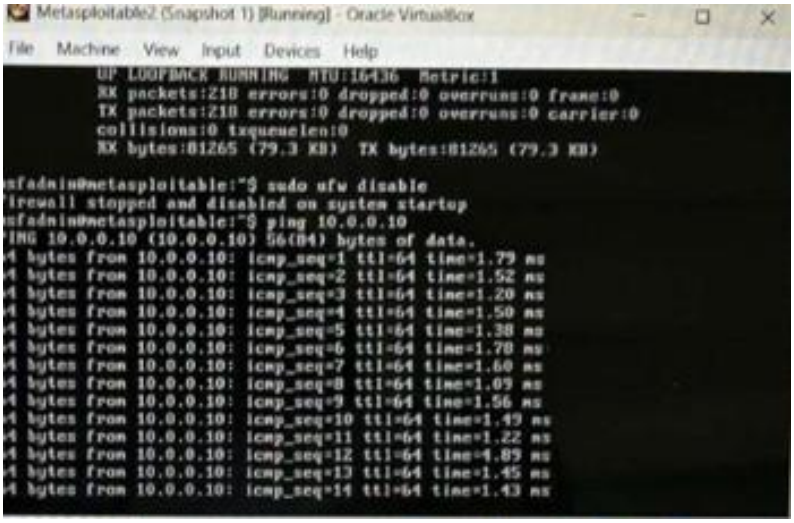
ip a (on Kali)
ifconfig (on Metasploitable2)

Each machine displays its IP address, confirming they are on the same network.

Step 3: Ping Test (Connectivity Check)

Kali ping command





A ping test was conducted from Kali Linux to Metasploitable2 to verify communication between the machines:

Command used:

ping <Metasploitable_IP>

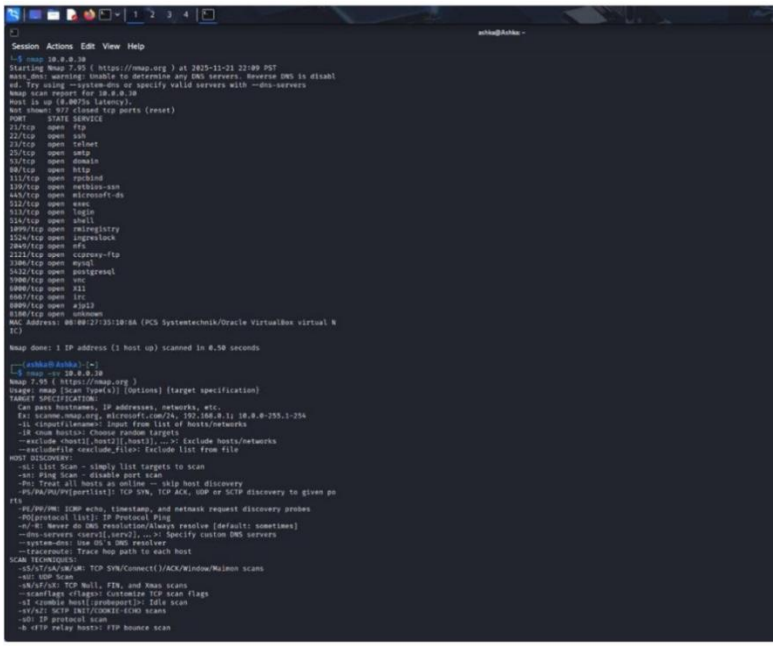
Successful ICMP responses confirmed stable connectivity between the attacker and target systems.

Step 4: Basic Nmap Scan (Host Discovery)

Nmap basic scan

INFORMATION GATHERING WITH NMAP

Basic Scan (Check if target is alive) command: nmap



A simple Nmap scan was performed to confirm the target is alive.

Command used:

nmap <Target_IP>

This revealed that the host was active and presented multiple open ports, indicating a broad attack surface.

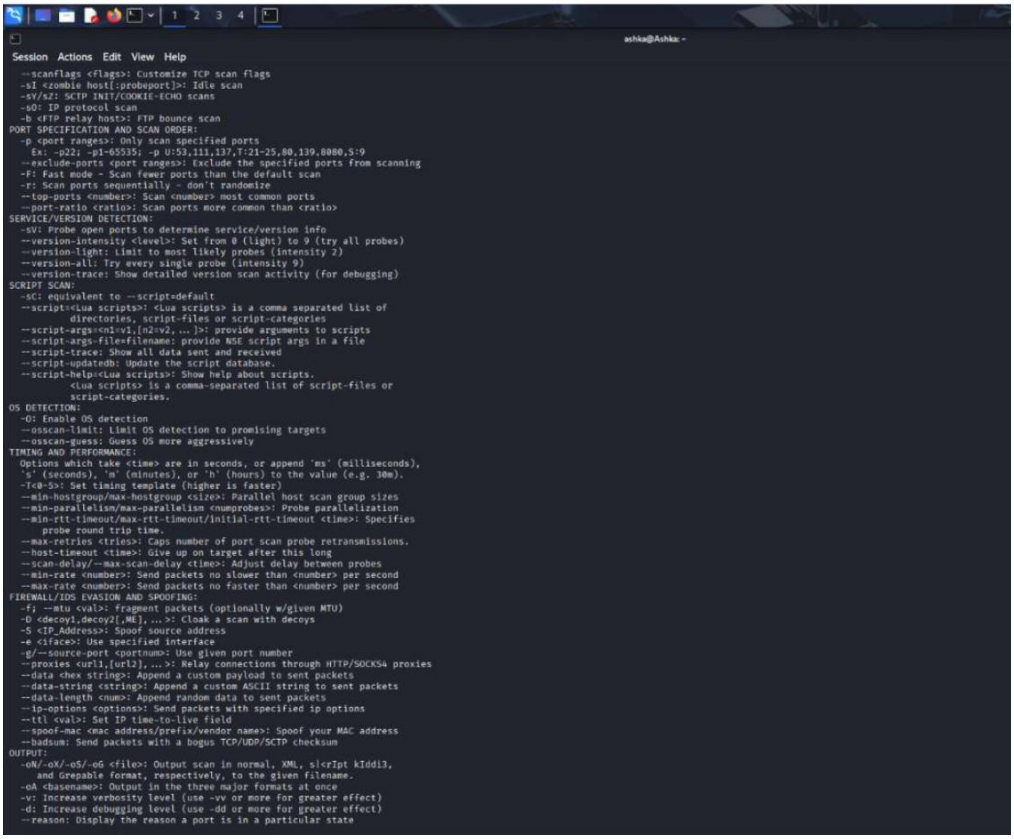
Nmap displays:

- Host is up
- List of open ports such as 21, 22, 80, 139, etc.

Step 5: Full Port Scan

Full Nmap port scan

Detailed Scan Command: nmap -sv



A comprehensive port scan was conducted to detect all open ports:

Command used:

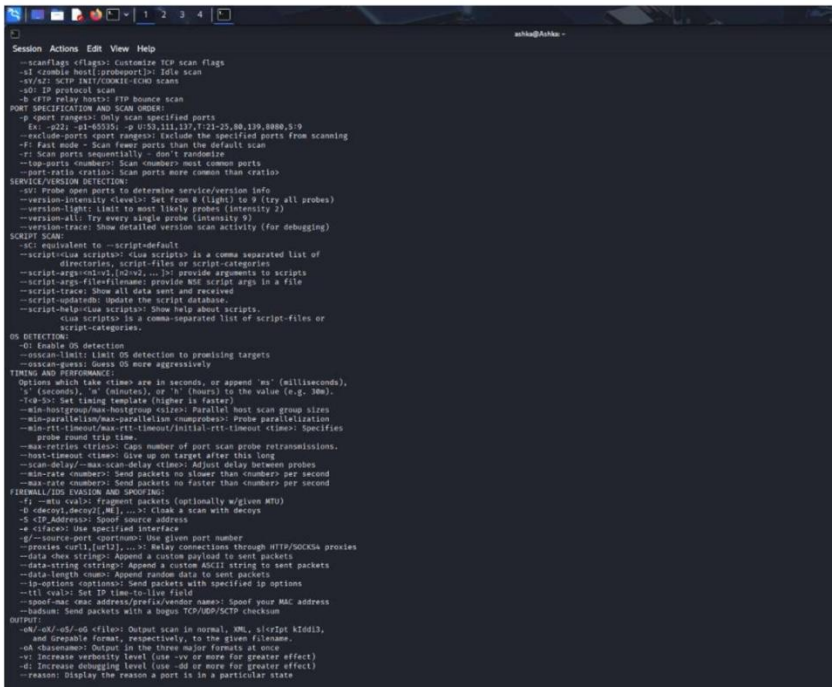
nmap -p- <Target_IP>

All open ports on the system are displayed, revealing potential attack points.

Step 6: Service and Version Detection

Nmap -sV output

Detailed Scan Command: nmap -sv



The following command was used to identify specific services and their versions:

Command used:

nmap -sV <Target_IP>

Detailed information such as:

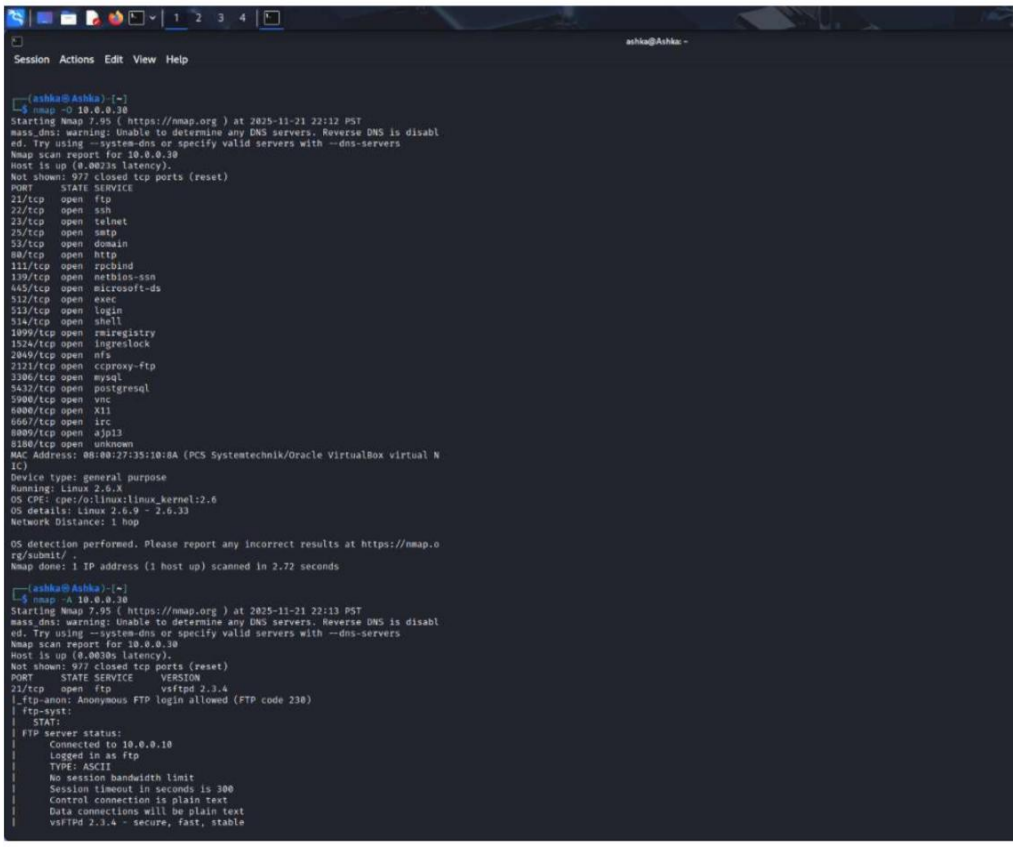
- FTP version
- Apache web server version
- SSH version

This revealed outdated or vulnerable software.

Step 7: Operating System Detection

OS detection scan

OS Detection command: nmap -O



Nmap was used to guess the operating system of the target:

Command used:

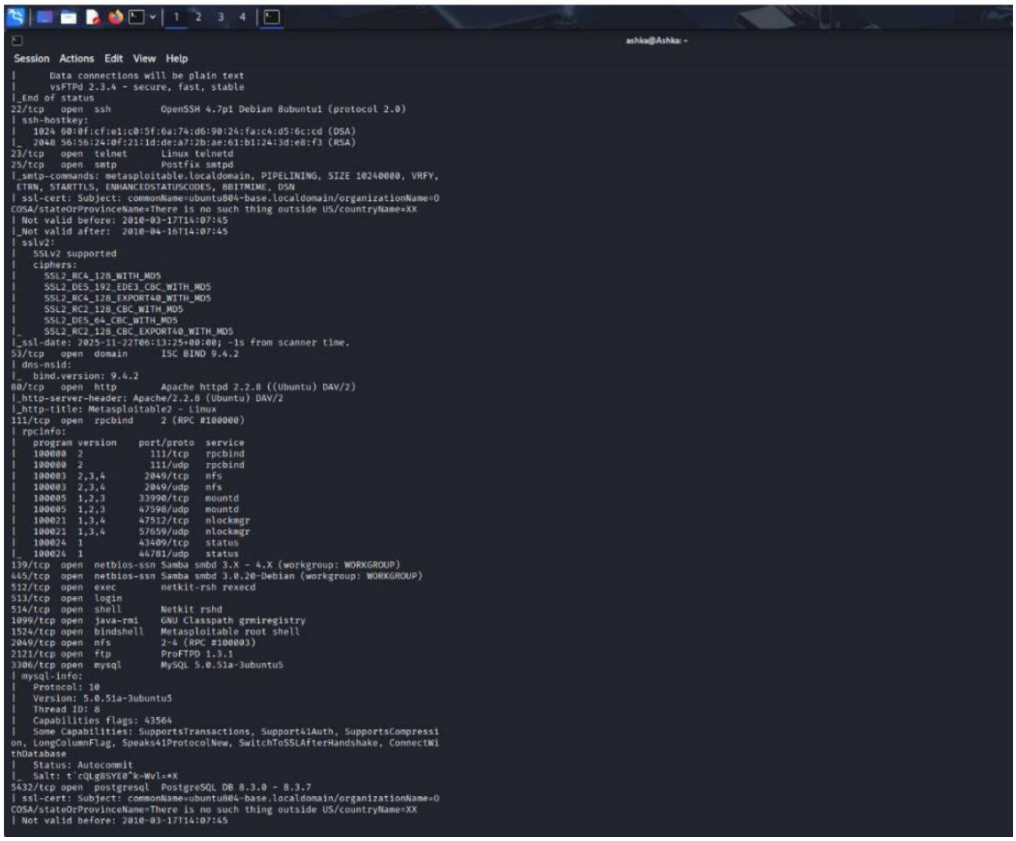
nmap -O <Target_IP>

Results indicated that the target system was Linux-based.

Step 8: Aggressive Scan

Aggressive scan results

Aggressive Full Scan (Main Evidence) command: nmap -A



An aggressive scan was conducted to gather detailed system information:

Command used:

nmap -A <Target_IP>

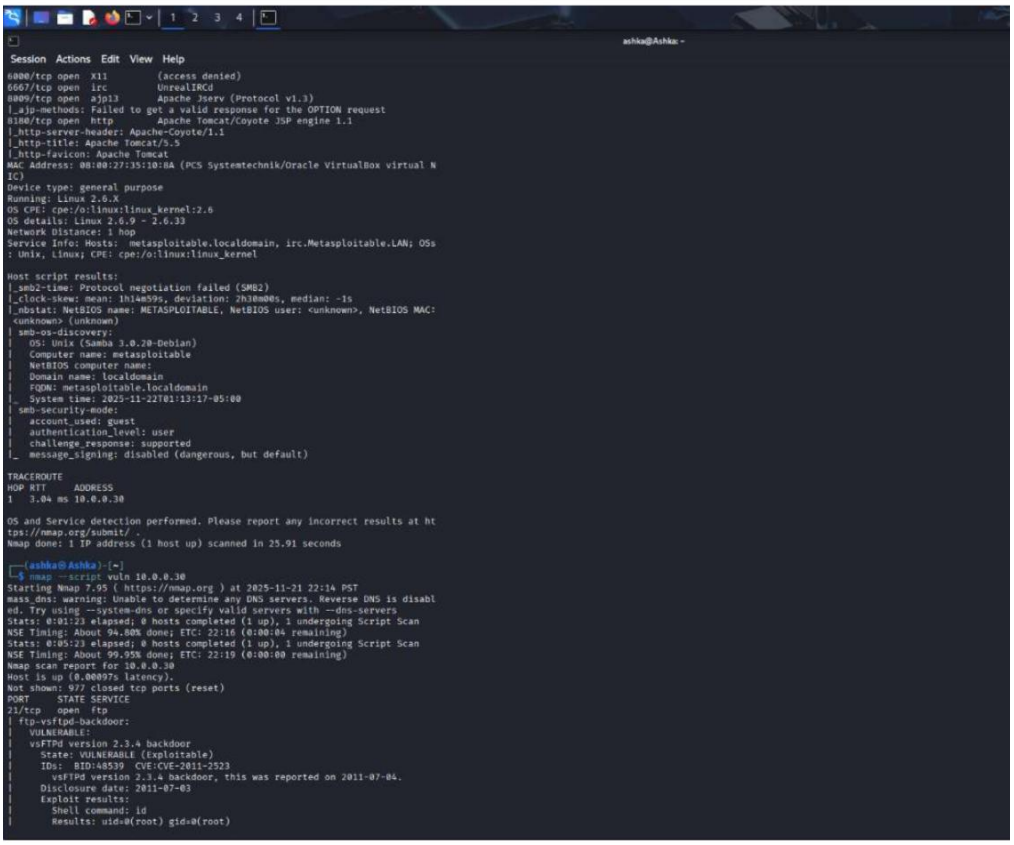
Shows:

- Open ports
- Services
- OS details
- Script results
- Comprehensive system profile is created.

Step 9: Vulnerability Script Scan

Nmap Scripting Engine (NSE) vulnerability scan

VULNERABILITY CHECK USING NMAP SCRIPTS command: nmap --



A vulnerability script scan was performed using Nmap's NSE engine:

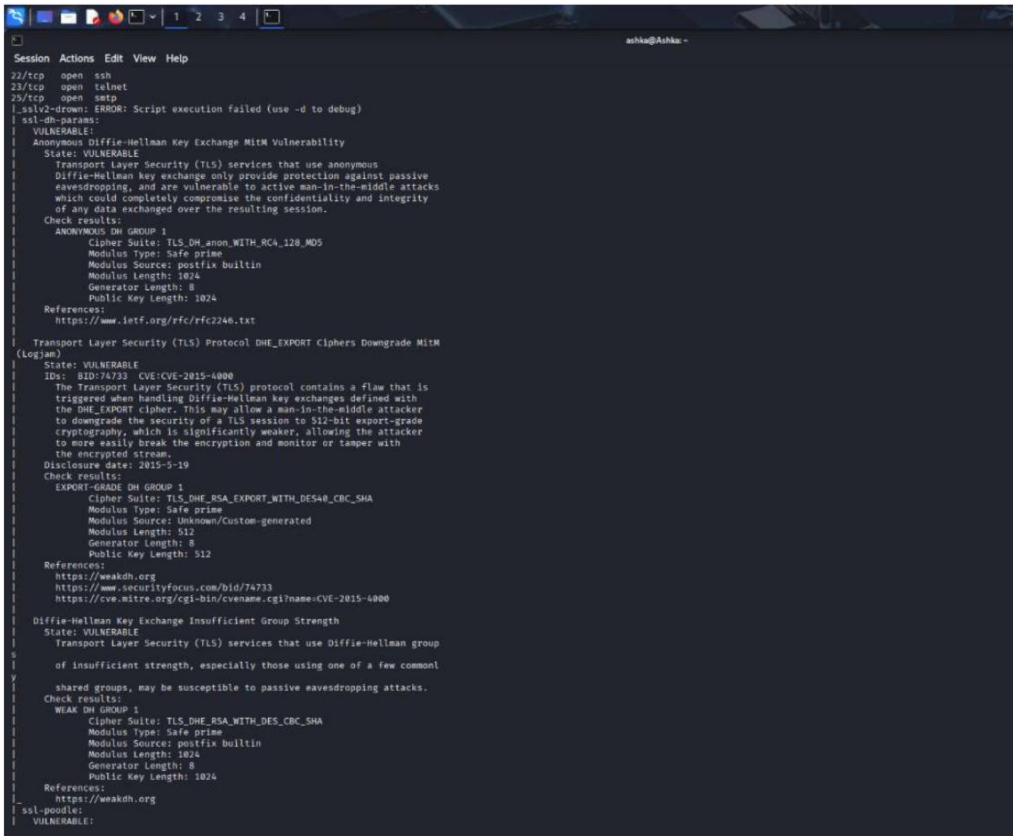
Command used:

nmap --script vuln <Target_IP>

This scan identified several vulnerabilities associated with insecure service configurations and outdated software packages.

Step 10: Results Analysis

Summary of scan findings



The penetration test revealed the following key vulnerabilities:

- Weak services
- Open ports
- Possible entry points

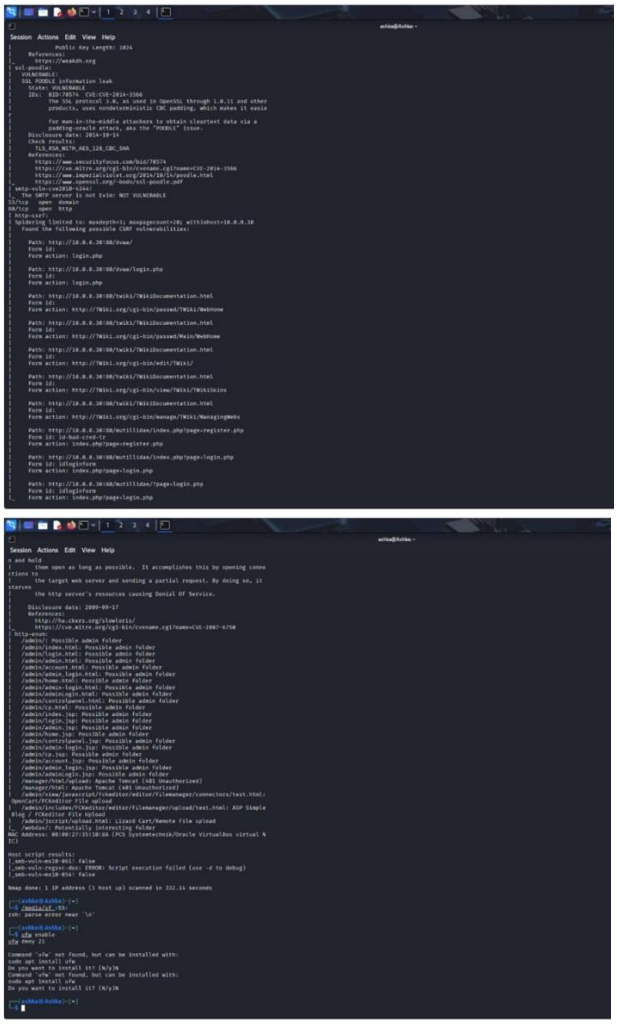
A clear list of high-risk services like:

- Open FTP with anonymous access
- Outdated Apache server
- Exposed SMB services

These conditions significantly increase the likelihood of unauthorized access and system compromise if deployed in a real-world environment.

Step 11: Simulated Exploitation Preparation

Identified vulnerable port focus



Vulnerable ports were selected as possible exploitation targets based on risk.

Identification of critical weaknesses to demonstrate attack potential.

Step 12: Risk Classification

Vulnerabilities were ranked by severity:

- High Risk – Open FTP, SMB shares
- Medium Risk – Outdated services
- Low Risk – Informational ports

Expected Result

Clear prioritization for remediation.

Practical Summary

This penetration test simulated a real attacker lifecycle within a controlled lab environment. Kali Linux was used as the attacking machine, while Metasploitable2 was configured as the vulnerable target. Using Nmap, several scans were conducted to identify open ports, running services, operating system details, and security weaknesses.

The tests revealed multiple vulnerabilities including exposed services, outdated software versions, and insecure configurations. These findings demonstrated how attackers can exploit weak system setups and reinforced the importance of proactive security controls.

Key Findings

- Multiple open ports increasing attack surface
- Weak service configurations
- Outdated applications vulnerable to exploitation
- Potential for unauthorized system access