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

\*\*1. Project Objectives\*\*

The objective of this project is to simulate a real-world network penetration test using a vulnerable machine (Metasploitable) and an attacker machine (Kali Linux). This involves network scanning, service enumeration, exploitation, user privilege escalation, password cracking, and providing proper remediation steps.

\*\*2. Introduction\*\*

This project aims to develop an understanding of practical cybersecurity techniques by simulating a penetration testing environment. Students use Kali Linux as the attacker system and Metasploitable as the target. Tools like Nmap, Metasploit, and John the Ripper are used to identify and exploit vulnerabilities.

\*\*3. Theoretical Background\*\*

Penetration testing involves simulating cyberattacks on systems to identify vulnerabilities before attackers do. Key phases include:

- Reconnaissance

- Scanning

- Enumeration

- Exploitation

- Post-exploitation

- Reporting and Remediation

\*\*4. Project Requirements\*\*

|  |  |
| --- | --- |
| Requirements | Tools |
| Attacker OS | Kali Linux |
| Target OS | Metasploitable(Linux 2.6) |
| Primary Toolset | Nmap, Metasploit ,John |

\*\*5. Tools Usage

\*\*Nmap\*\* for scanning and reconnaissance

\*\*Metasploit\*\* for exploitation

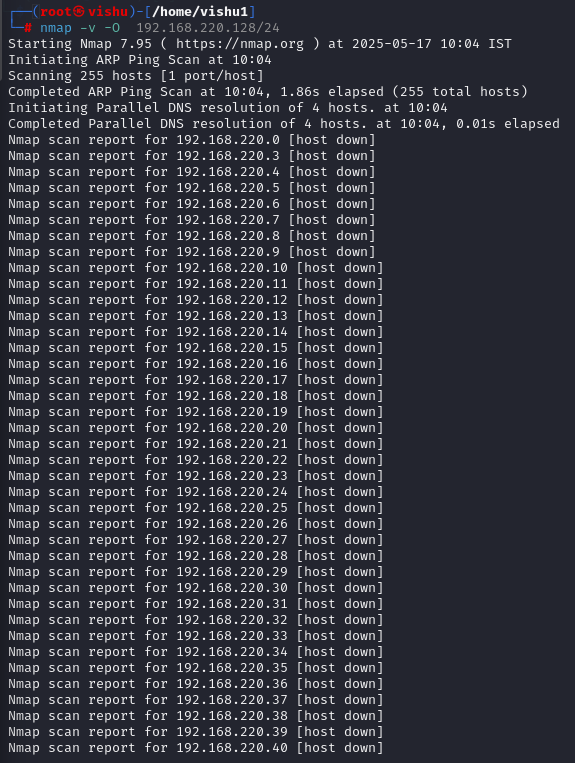
\*\*John the Ripper\*\* for password cracking

\*\*Linux Terminal\*\* for post-exploitation tasks

\*\*6. Tasks\*\*

\*\*Task 1: Basic Network Scan\*\*

|  |
| --- |
| Bash |
| nmap -v 192.168.220.128/24 |
|  |



\*\*Task 2: Reconnaissance\*\*

\*\*A. Scanning for Hidden Ports\*\*

|  |
| --- |
| Bash |
| nmap -v -p- 192.168.220.131 |

\*\*Total Hidden Ports Found: 7\*\*

\*\*List of Hidden Ports:\*\*

1. 8787

2. 47436

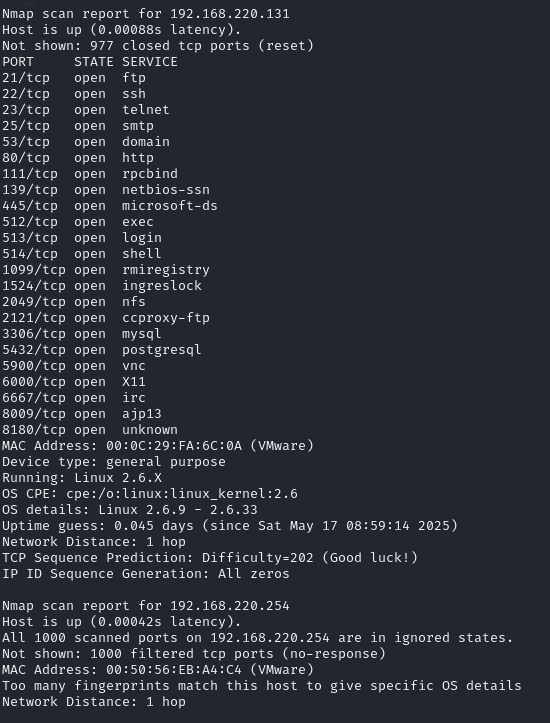
3. 50918

4. 59995

5. 60004

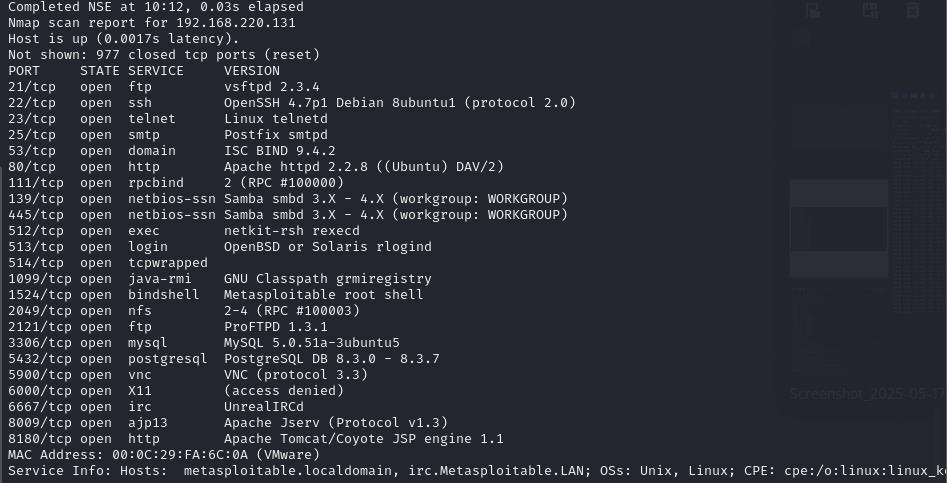
6. 55555

7. 31333



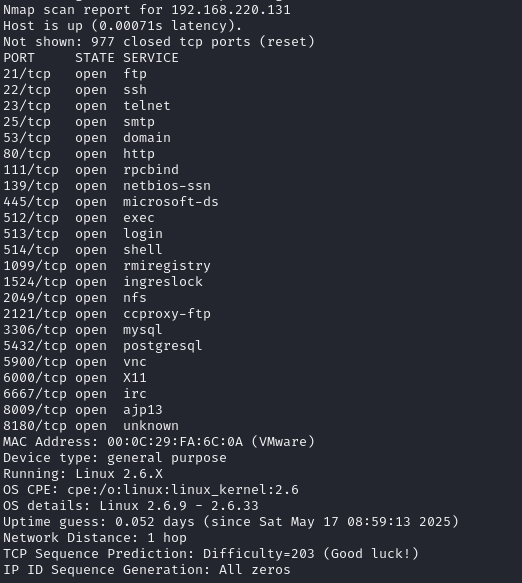
\*\*B. Service Version Detection\*\*

|  |
| --- |
| Bash |
| nmap -v -sV 192.168.220.131 |



\*\*C. Operating System Detection\*\*

|  |
| --- |
| Bash |
| nmap -v -O 192.168.120.131 |



\*\*Task 3: Enumeration\*\*

|  |
| --- |
| | Info | Value |
|  |
| | Target IP Address | 192.168.120.131 |
| | OS Details | Linux 2.6.9 - 2.6.33 |
| | MAC Address | 00:0C:29:FA:6C:0A |
| | Device Type | General Purpose |
| | OS CPE | cpe:/o:linux:linux\_kernel:2.6 |

\*\*Services on Open Ports:\*\*

|  |
| --- |
| | PORT | STATE | SERVICE | VERSION |
|  |
| | 21/tcp | open | ftp | vsftpd 2.3.4 |
| | 22/tcp | open | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 |
|  |

\*\*Hidden Ports:\*\*

|  |
| --- |
| | PORT | SERVICE | VERSION |
|  |
| | 8787/tcp | drb | Ruby DRb RMI |
| | 47436/tcp | mountd | RPC #100005 |
| | 50918/tcp | java-rmi | GNU Classpath grmiregistry |
| | 59995/tcp | nlockmgr | RPC #100021 |
| | 60004/tcp | status | RPC #100024 |

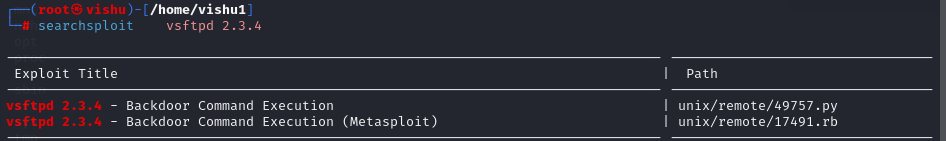
\*\*Task 4: Exploitation of Services\*\*

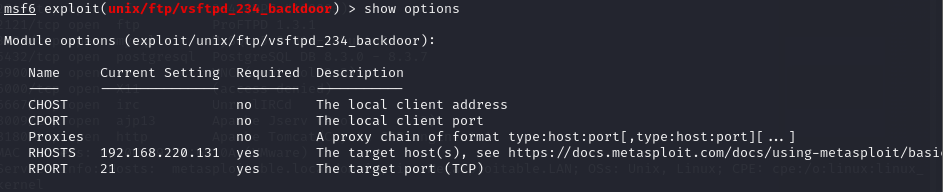
Performed exploits using Metasploit on:

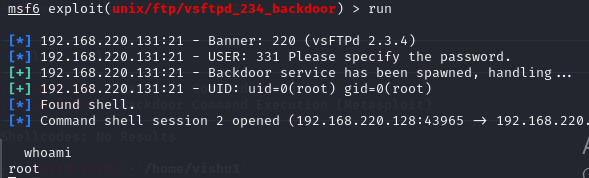
1. \*\*vsftpd 2.3.4\*\* – Backdoor vulnerability

2. \*\*Java-RMI\*\* – Remote code execution

3. \*\*SSH\*\* – Brute-force attack







\*\*Task 5: Create User with Root Permission\*\*

|  |
| --- |
| Bash |
| adduser alex |

Password: `987654321`

Details from `/etc/passwd`:

bash

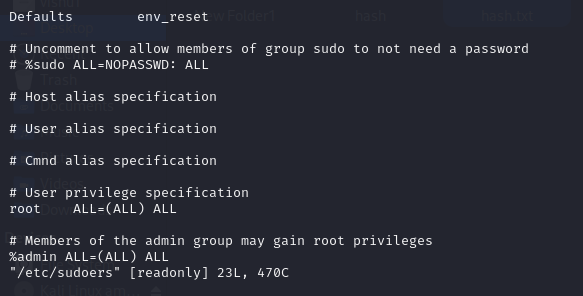
alex:x:1003:1003:alex multipowerful,,,:/home/alex:/bin/bash

Details from `/etc/shadow`:

bash

alex:$1$sl/n8aEt$.IVE3KrI4pq3v//zbruLG0:20225:0:99999:7:



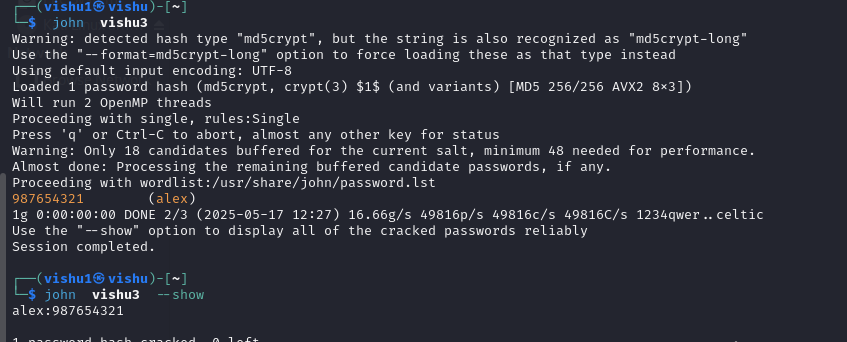


\*\*Task 6: Cracking Password Hashes\*\*

1. \*\*Stored hash in file:\*\* `vishu3`

2. \*\*Command to crack:\*\*

|  |
| --- |
| Bash |
| john vishu3 |
| john vishu3 –show |



\*\*Task 7: Remediation\*\*

\*\*Vulnerability: vsftpd 2.3.4\*\*

\*\*Current Version on System:\*\* vsftpd 2.3.4

\*\*Known Vulnerability:\*\* Backdoor command shell

\*\*Latest Version:\*\* vsftpd 3.0.5

\*\*Remediation:\*\*

Upgrade to the latest version using:

bash

sudo apt update && sudo apt install vsftpd

- Disable anonymous login

- Use SFTP or SCP instead of FTP

\*\*References:\*\*

- [https://nvd.nist.gov](https://nvd.nist.gov)

- [https://www.vsftpd.org](https://www.vsftpd.org)

\*\*Major Learnings\*\*

Through this project, I learned how to scan and enumerate network systems using Nmap, exploit vulnerable services using Metasploit, create privileged users, and crack password hashes. I gained practical skills in identifying and remediating real-world vulnerabilities and understanding the importance of system updates and secure configurations.