**Network Penetration Testing With Real-World Exploits And Security Remediation.**

**Name: Sejal Verma**

**Course: CSE(Cyber Security)**

# 1. Project Objectives

The objective of this project is to simulate a real-world network penetration test on a virtual network environment to identify vulnerabilities, exploit them ethically, including scanning, enumeration, exploitation, privilege escalation, and remediation.

# 2. Network Penetration Testing: Theory

Network penetration testing is a proactive security assessment technique used to evaluate the resilience of a network against potential Cyberattacks.

The process include multiple phases:

1. Reconnaissance – Collecting preliminary information about the target system or network.

2. Scanning & Enumeration – Identifying live systems, open ports, and services to discover potential vulnerabilities.

3. Exploitation – Attempting to gain unauthorized access by leveraging known security flaws.

4. Post-Exploitation – Performing actions such as privilege escalation, data extraction, or persistence to assess the potential impact of a breach.

5. Remediation – Recommending and implementing measures to fix identified vulnerabilities and improve overall security posture.

# 3. Project Requirements

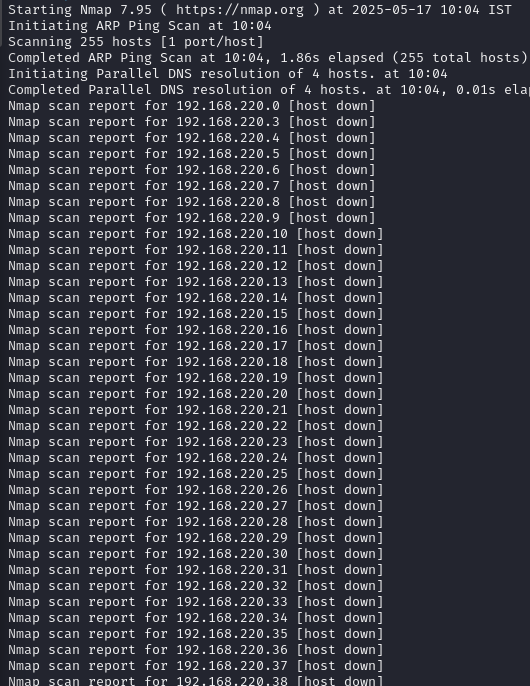
|  |  |
| --- | --- |
| Kali Linux | The Attackers machine |
| Metasploitable | A vulnerable machine to practice attacks on. |
| nmap | For network scanning, port discovery, OS detection |
| John the Ripper | For cracking hashed passwords obtained from /etc/shadow. |

# 4. Tools Used

- Nmap – Network scanning and port discovery  
- Nikto – Web server vulnerability scanner  
- Metasploit Framework – Exploitation framework  
- John the Ripper – Password hash cracking

# 5. Task

Task 1: Basic Network Scan



Task 2: Reconnaissance

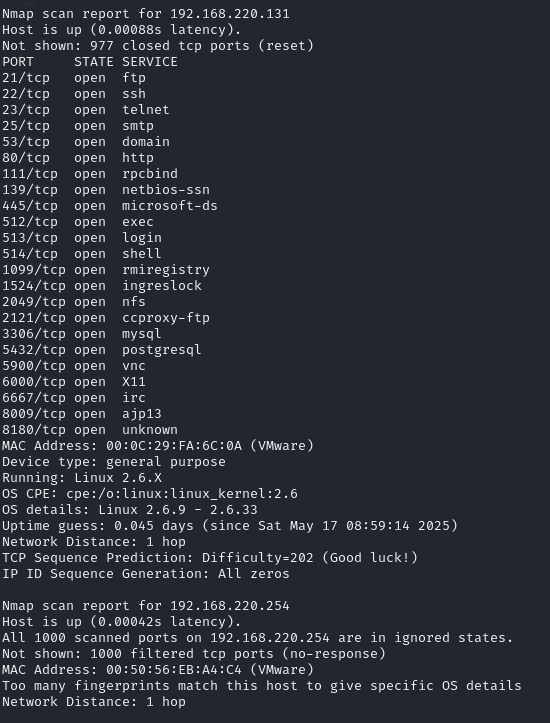
A. Scanning for Hidden Ports

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

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

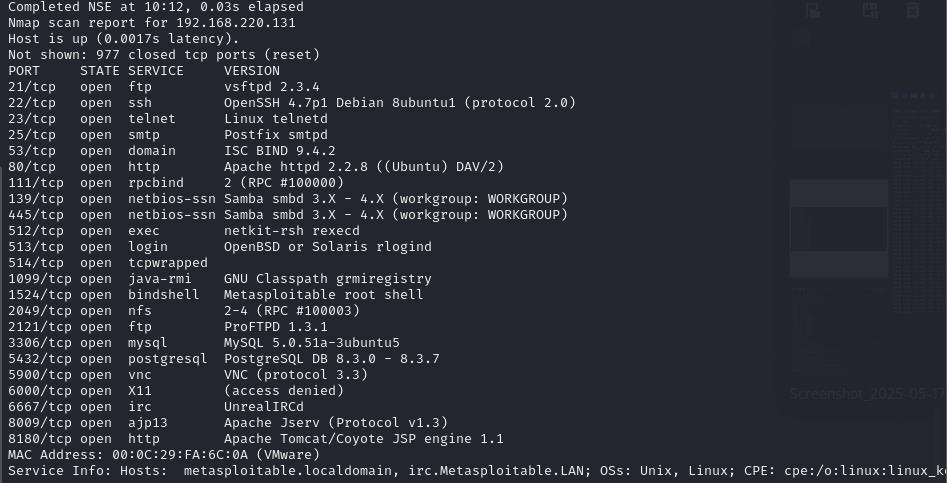
\*\*List of Hidden Ports:\*\*

* 8787
* 53204
* 53452
* 59437
* 3632



B. Service Version Detection

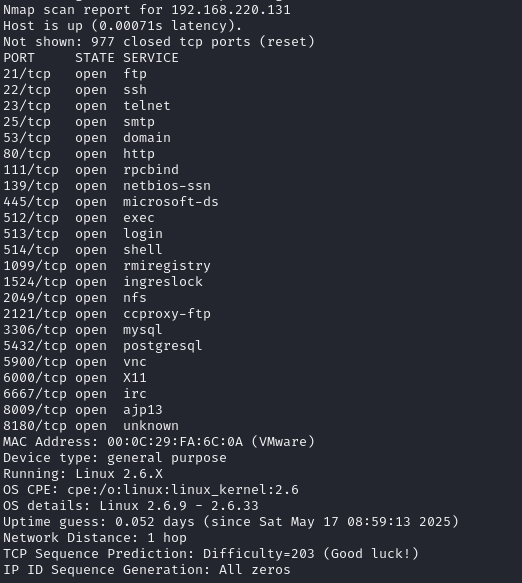
|  |
| --- |
| Bash |
| nmap -v -sV 192.168.220.131 |



Task 3: Operating System Detection

nmap -v -O 192.168.160.132

Output:



Task 3 - Enumeration

Target IP Address – 192.168.220.131

Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

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 |

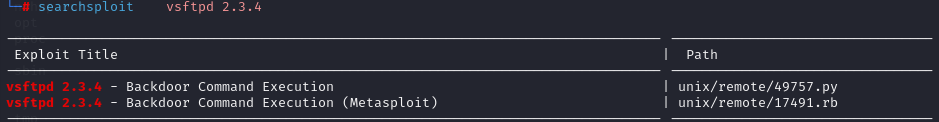
Task 4: Exploitation of Services

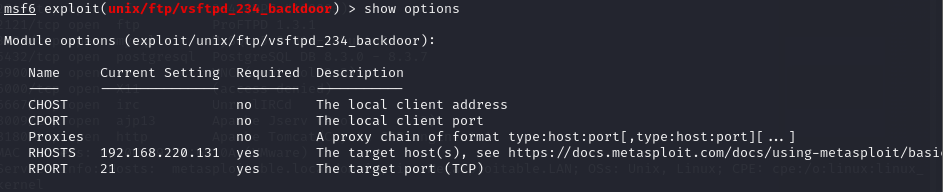
Performed exploits using Metasploit on:

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`:

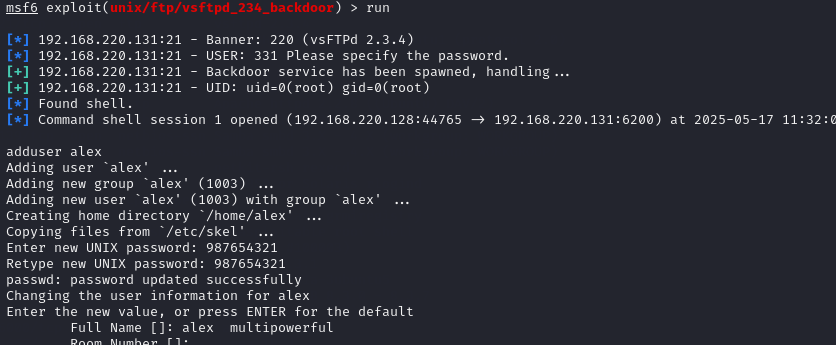
bash

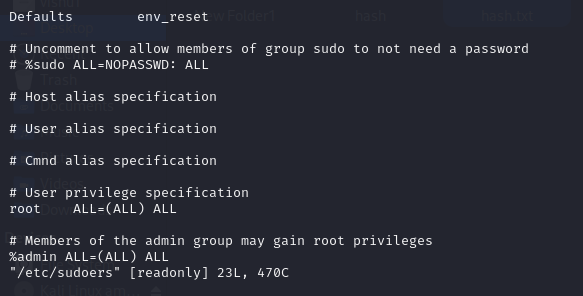
alex:x:1003:1003:alex multipowerful,,,:/home/alex:/bin/bash

Details from `/etc/shadow`:

bash

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



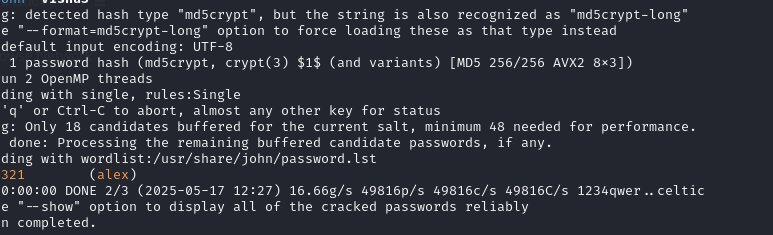


Task 6: Cracking Password Hashes

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

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

|  |
| --- |
| Bash |
| john sejal |
|  |



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

Major Learnings

Through this project, I learned to manage Linux users and understand how passwords are stored and cracked using tools like John the Ripper. I used Nmap commands to scan for open ports, detect running services, and identify operating systems. The project helped me identify system vulnerabilities and software updates and better configurations. Overall, it improved my practical understanding of system and network security.