# 🔐 Ethical Hacking Project

## Scanning and Enumerating a Local Network with Nmap

# Table of Contents

Project: Simulating Real-World Network Exploitation and Defense

**🎯 Project Objectives**

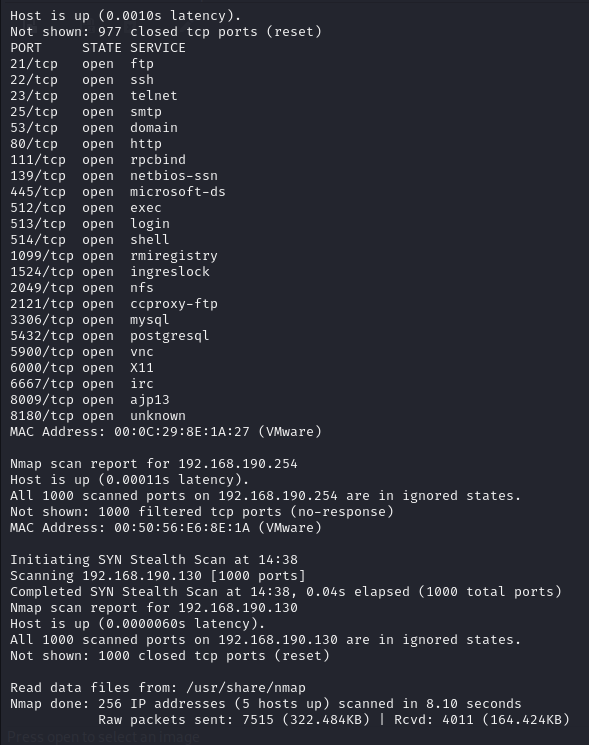
To understand and apply techniques in:

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

**🛠 Tools Used**

* Kali Linux (Attacker Machine)
* Metasploitable (Target Machine)
* Nmap
* **Nmap** (short for **Network Mapper**) is an open-source tool used for **network discovery** and **security auditing**.
* John the Ripper
* **John the Ripper** (often just called **John**) is a **fast, open-source password cracker**. It's primarily used for recovering weak or lost passwords by **brute-force** or **dictionary-based attacks**.
* Metasploit Framework
* The Metasploit Framework is one of the most powerful and widely used tools for penetration testing, vulnerability exploitation, and red teaming. It provides a modular platform to test and exploit known vulnerabilities in networks, systems, and applications.

**🔍 Task 1: Basic Network Scan**



Command:

nmap -v 192.168.190.0/24

Expected Output:

Nmap scan report for 192.168.190.129

Host is up (0.0010s latency).

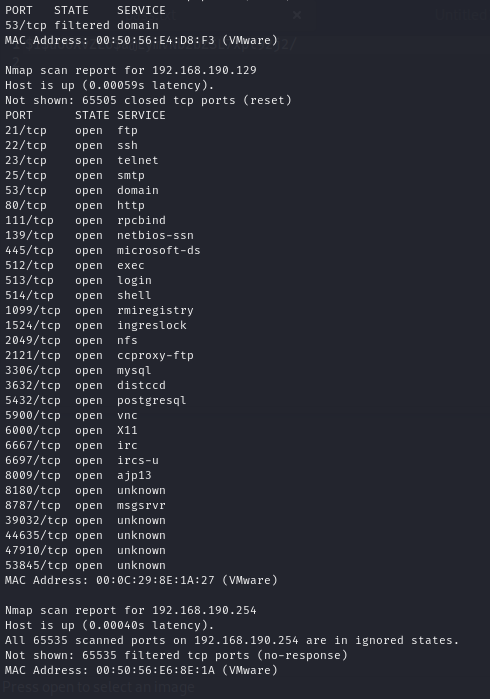
|  |  |  |
| --- | --- | --- |
| PORT | STATE | SERVICE |
| 21/tcp | open | ssh |
| 22/tcp | open | telnet |
| 25/tcp | open | smtp |
| 53/tcp | open | domain |
| 80/tcp | open | http |

Nmap scan report for 192.168.190.2

Host is up (0.0020s latency).

|  |  |  |
| --- | --- | --- |
| PORT | STATE | SERVICE |
| 53/tcp | filtered | domain |

**🧭 Task 2: Reconnaissance**



Command:

nmap -v 192.168.190.0/24

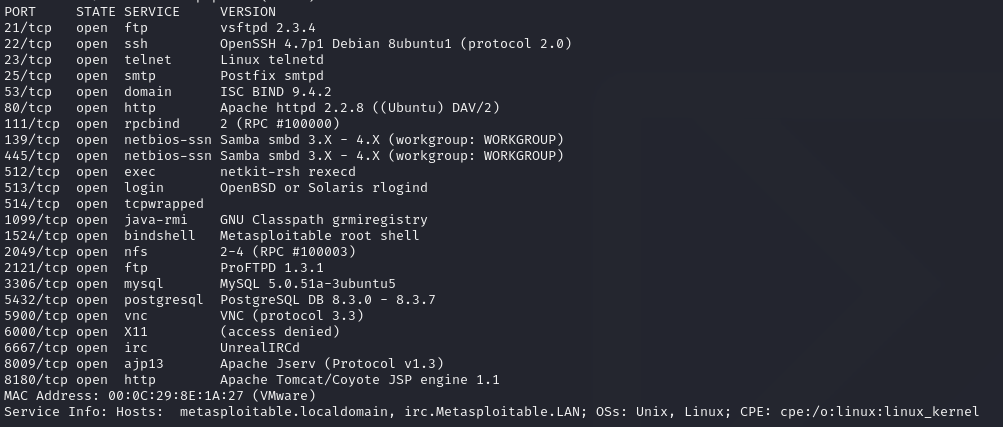
Expected Output:

Nmap scan report for 192.168.190.129

Host is up (0.0010s latency).

Total Hidden Ports: 7

|  |  |  |
| --- | --- | --- |
| 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 | exex |
| 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 |
| 3632/tcp | open | distccd |
| 5432/tcp | open | postgresql |
| 5900/tcp | open | vnc |
| 6000/tcp | open | X11 |
| 6667/tcp | open | irc |
| 6697/tcp | open | ircs-u |
| 8009/tcp | open | ajp13 |
| 8180/tcp | open | unknown |
| 8787/tcp | open | msgsrvr |
| 39032/tcp | open | unknown |
| 44635/tcp | open | unknown |
| 47910/tcp | open | unknown |
| 53845/tcp | open | unknown |

**2.1 Scanning for Hidden Ports**

**2.2 Service Version Detection**

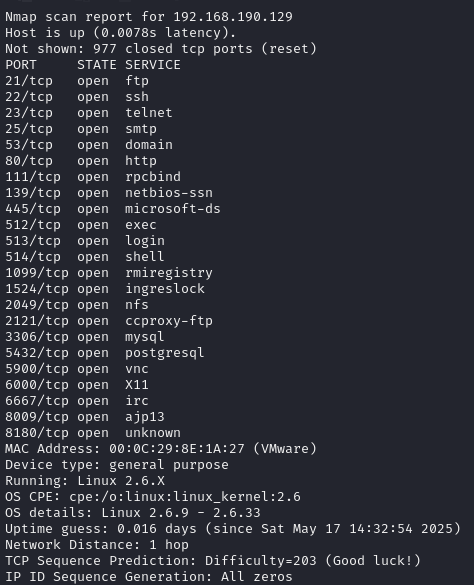
Command:

nmap -v -sV 192.168.129.0/24

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 | 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 192.168.190.0/24

Expected Output:

MAC Address: 00:0C:29:8E:1A:27 (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

**📋 Task 3: Enumeration Summary**

Target IP Address: 192.168.190.129

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: : 00:0C:29:8E:1A:27 (VMware)

Device Type: General-purpose

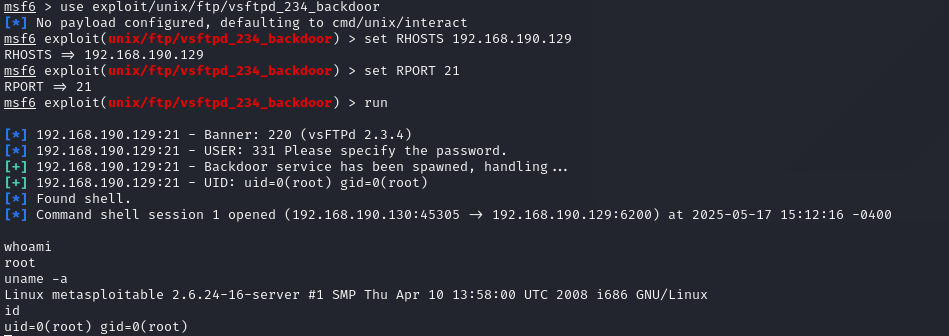
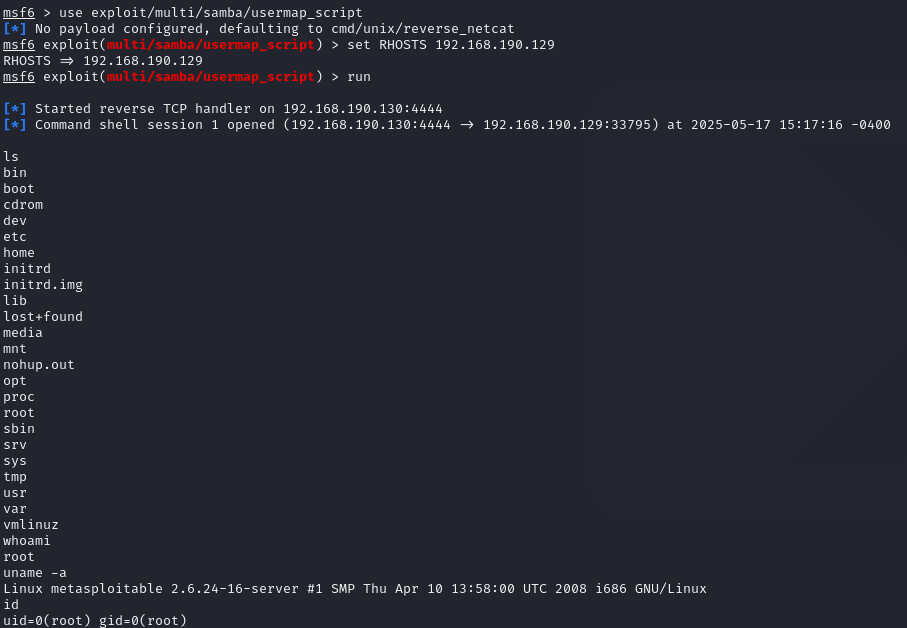
Open Services (Excluding Hidden Ports)

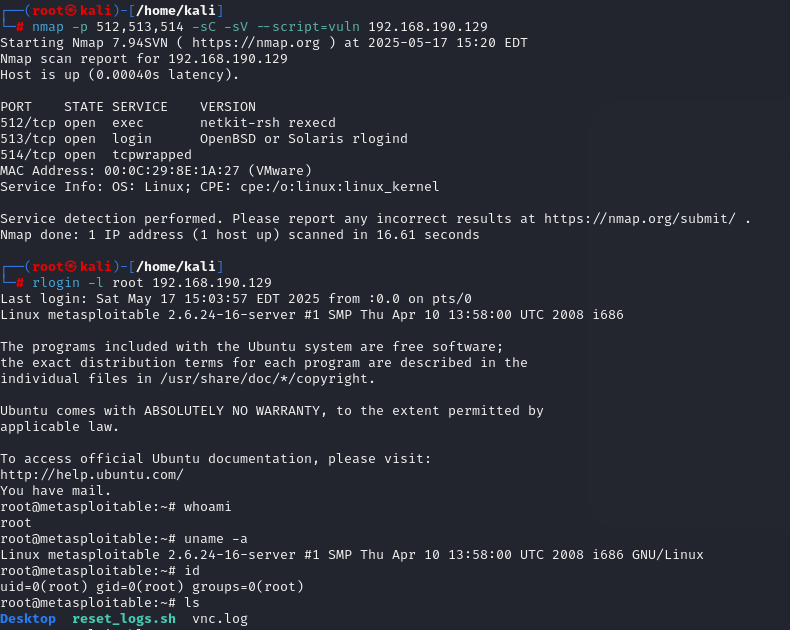
|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 21/tcp | open | ftp | vsftpd 2.3.4 |
| 22/tcp | open | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 |

Hidden Services

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 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**

 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 aman

Password: hello

/etc/passwd Entry:



/etc/shadow Hash:

 aman:$1$OmkgXvQT$dhA10N62JqZ7/wr2eprgn.

**🔓 Task 6: Cracking Password Hash**

Stored Hash in `aman.txt`:

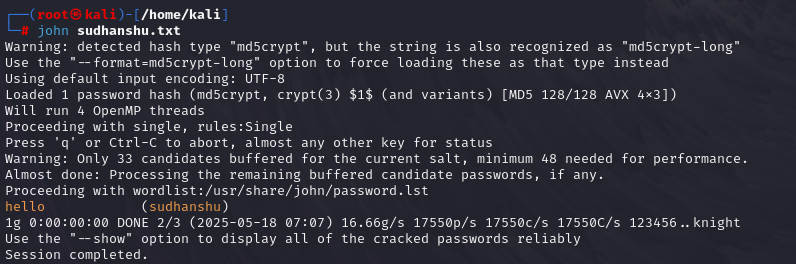
aman:$1$OmkgXvQT$dhA10N62JqZ7/wr2eprgn.

# Cracking Commands:

john aman.txt

john aman.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.