**ETHICAL HACKING PROJECT**

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

**INTRODUCTION:**

This project simulates a realistic penetration testing environment to explore how attackers compromise systems and how defenders secure them. It uses vulnerable virtual machines and professional tools to demonstrate each phase of an ethical hacking engagement, offering practical exposure to cybersecurity techniques and defense strategies. The goal is to help learners understand both the offensive and defensive aspects of network security through a guided, hands-on experience.

Two primary virtual machines are used:

Kali Linux – An advanced, Debian-based Linux distribution tailored for penetration testing, digital forensics, and ethical hacking. It comes pre-installed with a wide range of security tools, making it the preferred OS for security professionals.

Metasploitable – A deliberately insecure Ubuntu-based Linux virtual machine created for training and testing in vulnerability assessment and exploitation. It contains numerous outdated services and misconfigurations, serving as an ideal target for penetration testing.

The project is divided into key phases of a typical penetration testing lifecycle:

1. Network Scanning – Identifying active hosts and open ports using tools such as Nmap.

2. Reconnaissance – Gathering intelligence about network architecture, services, operating systems, and version information.

3. Enumeration – Pulling detailed data from target services, such as user lists, network shares, and service banners.

4. Exploitation – Using tools like Metasploit to exploit known vulnerabilities and gain access to the target system.

5. Privilege Escalation – Escalating privileges by exploiting system weaknesses or creating high-level users.

6. Password Cracking – Extracting and cracking password hashes using tools like John the Ripper to access user accounts.

7. Remediation – Suggesting practical solutions to address discovered vulnerabilities, such as applying patches, disabling unused services, and enforcing password policies.

By completing this project, we gain a deep understanding of how cyber attacks are conducted and how to defend against them effectively. It emphasizes critical cybersecurity principles such as secure configurations, software updates, and threat detection, preparing learners for real-world roles in ethical hacking and system protection.

**PROJECT REQUIREMENTS:**

Two Operating Ststems:

1. Kali linux (Attacking Machine)

2. Metasploitable machine (Target Machine)

**TOOLS USED:**

1. Nmap

2. Metasploit Framework

3. John the Ripper

4. Metasploitable2

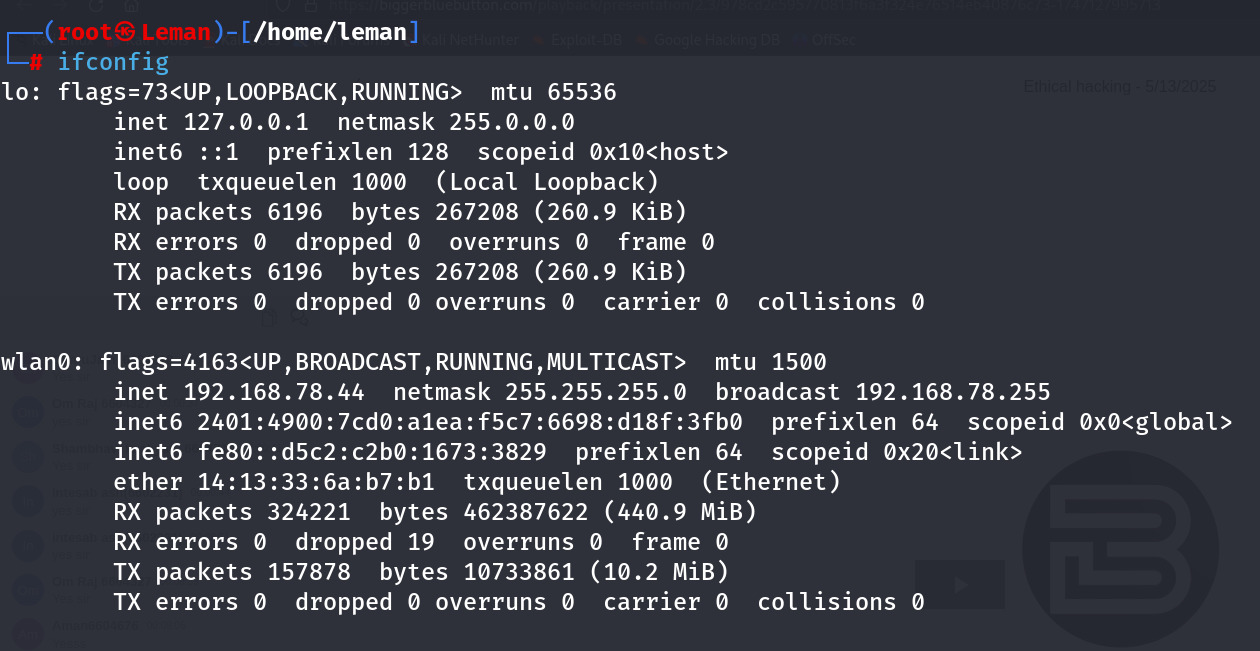
**TASKS:**

**Task 1 - NETWORKING SCANNING**

Task 1 : Basic Networking Scan

Step 1 : Open a terminal on your Kali Linux Machine.

Step 2 : Check the IP using ifconfig command.

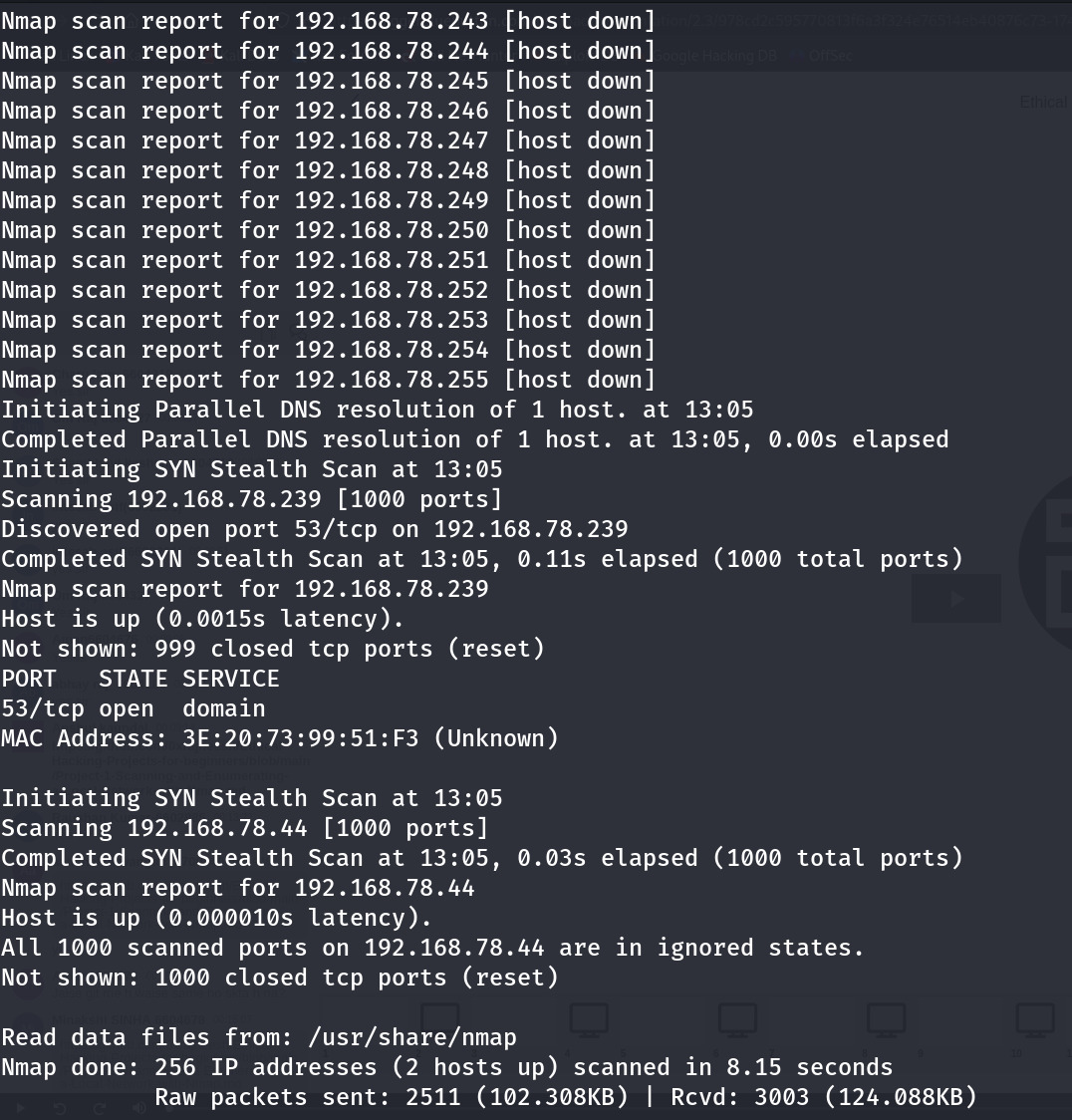


Step 3 : Run a basic scan on your local network.

nmap -v 192.168.78.44

Expected Output: A list of devices on the network, their IP addresses, and the open ports. This -v Option will show a detailed view of the running scan.

Output of the Scan



**Task 2 - Reconnaissance**

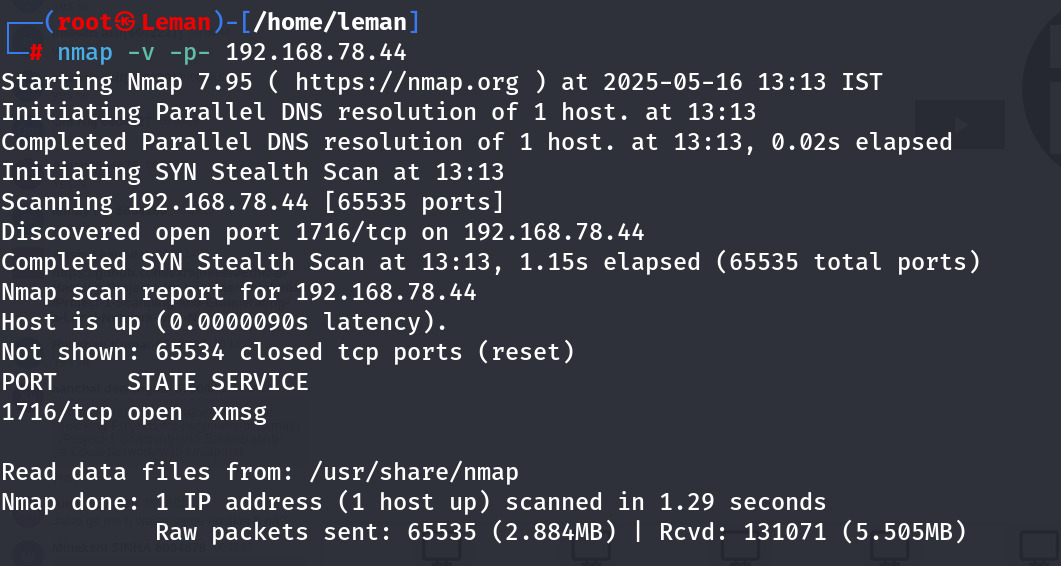
1. Scanning for the hidden ports -

Step 1: To scan for the hidden ports, we have to scan whole range of the ports on that specific targeted IP address.

nmap -v -p- 192.168.78.44

Expected Output: A list of hidden ports with services.

Output



Total hidden ports = 1

List of the hidden ports –

1. 1716/tcp open xmsg

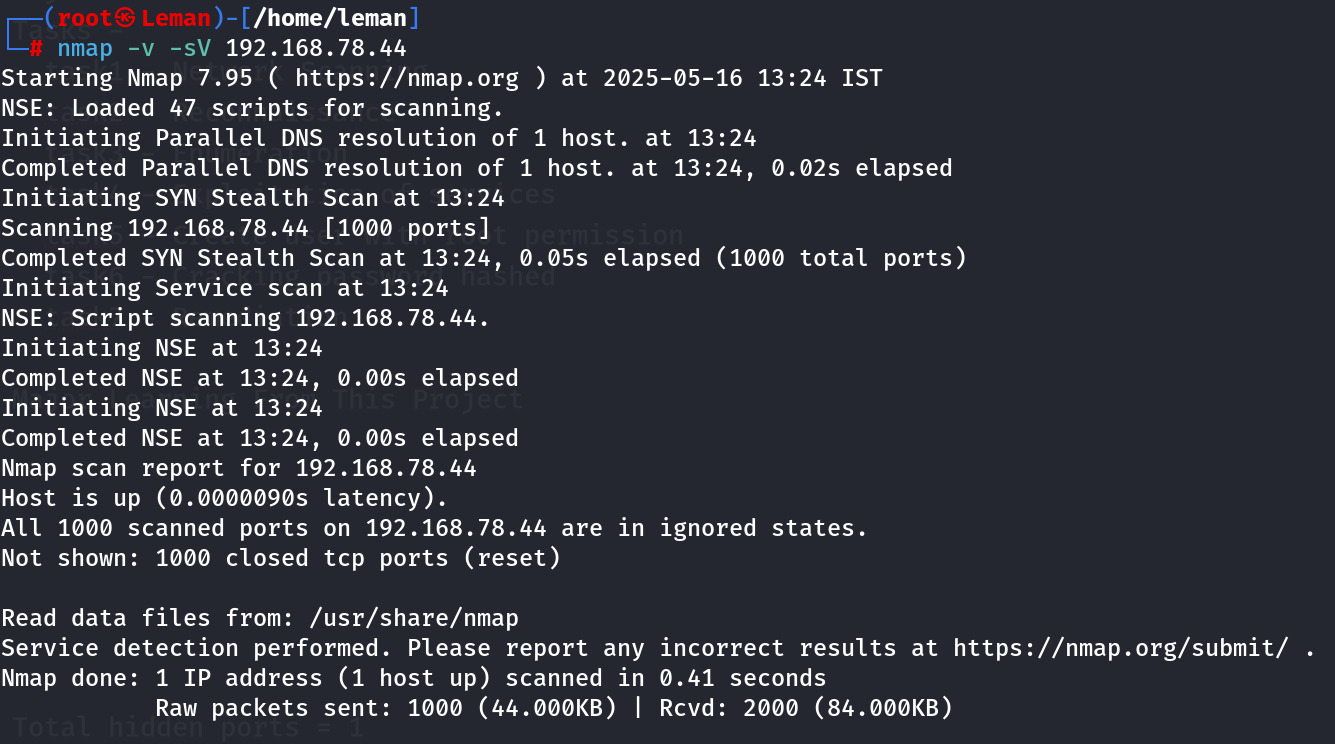
2. Service Version Detection

Step 1: Use the -sV option to detect the version of the services running on open ports:

nmap -v -sV 192.168.78.44

Expected Output: A detailed list os the open ports and the services running on them, including version information.

Output



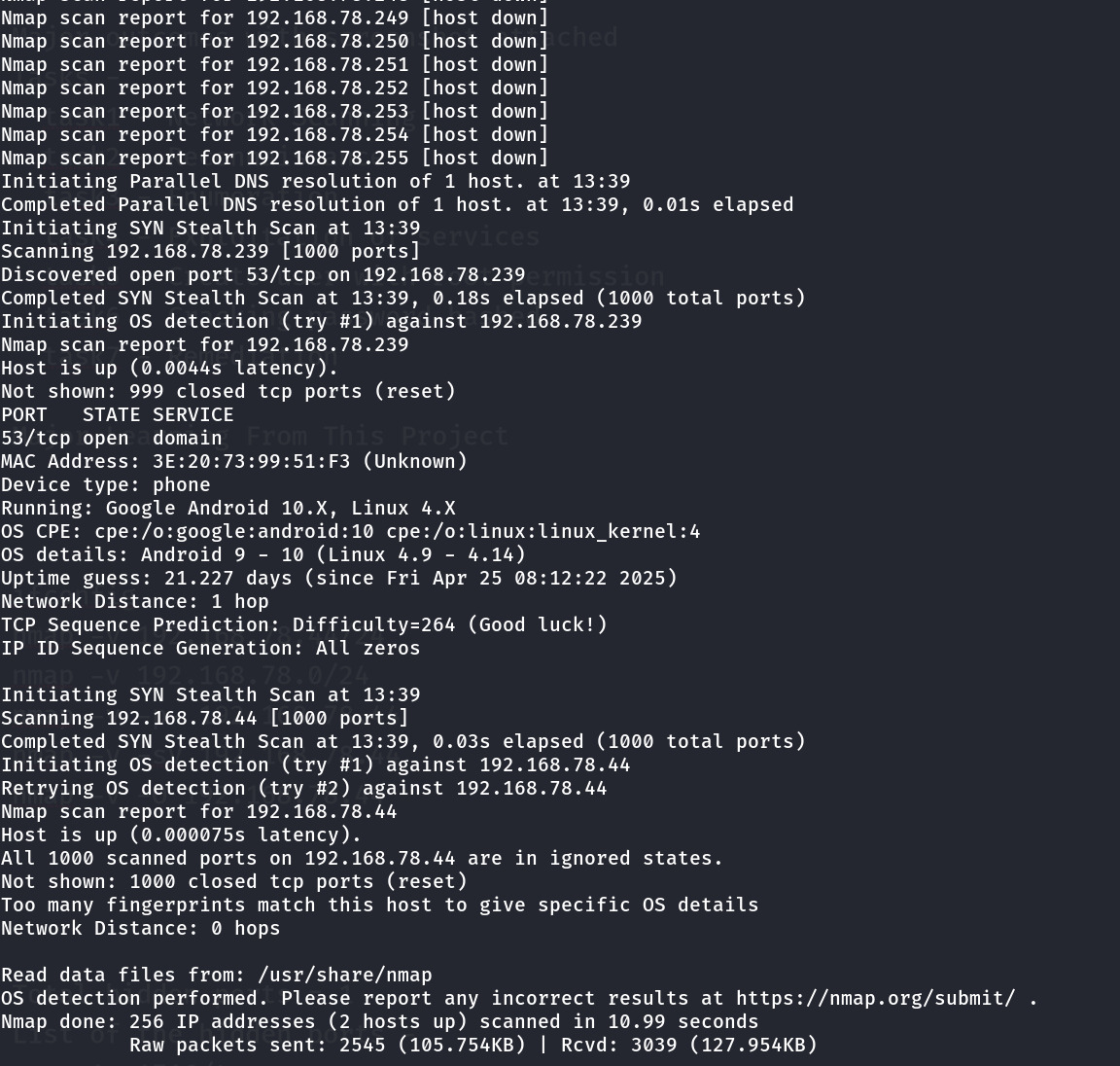
3. Operating System Detection

Step 1: Use the -O option to detect the operating system of the devices on the network:

nmap -v -O 192.168.78.44

Expected Output: The operating system details of the devices on the network.

Output



**Task 3: Enumeration**

Target IP address - 192.168.78.44

Operating System Detail: Google Android 10.X, Linux 4.X

Mac Address: 3E:20:73:99:51:F3 (Unknown)

Device type: phone

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

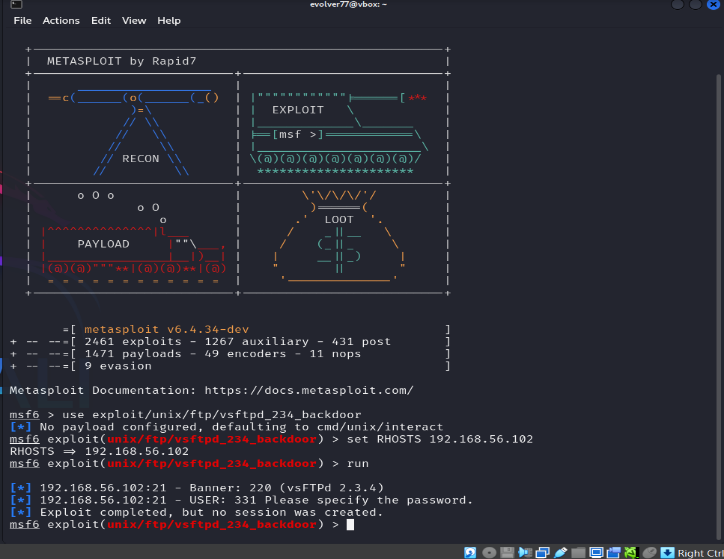
Hidden Ports with Service Version(ONLY HIDDEN PORTS):

1716/tcp open xmsg(RPC #131071)

**Task 4: Exploitation of services**

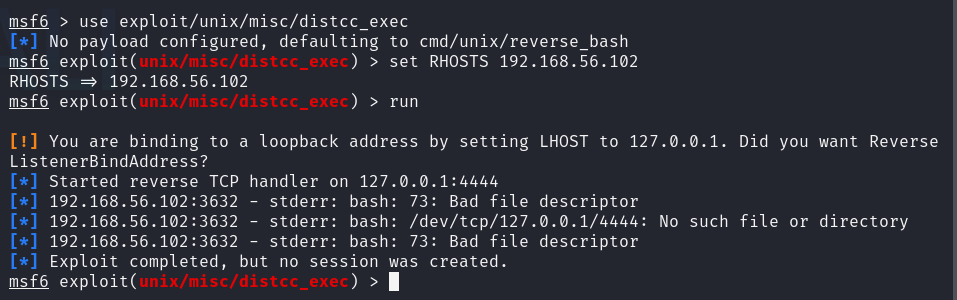
1. Exploit vsftpd 2.3.4 – Backdoor Command Execution

* Vulnerability : Backdoor Command execution vulnerability (CVE-2011-2523)
* Exploit Module : exploit/unix/ftp/vsftpd\_234\_backdoor



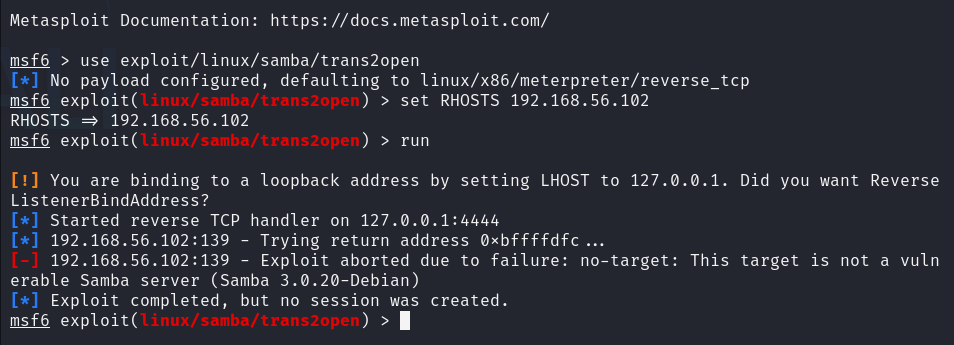
1. Exploit distccd – Remote Command Execution

* Vulnerability: distcc service allows remote command execution (CVE-2004-2687)
* Exploit Module: exploit/unix/misc/distcc\_exec



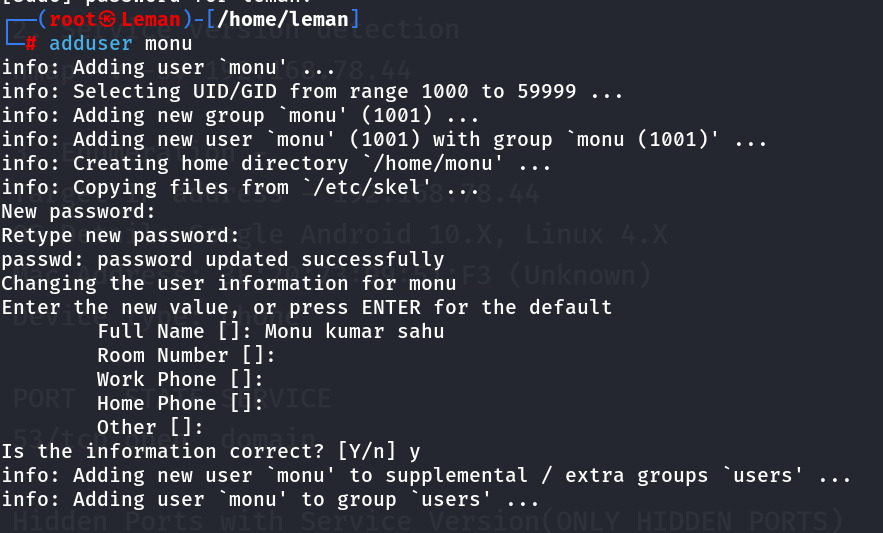
1. Exploit Samba smbd – Remote Command Execution

* Vulnerability: Samba trans2open overflow (CVE-2003-0201)
* Exploit Module: exploit/linux/samba/trans2open



Task 5: Create user with root permission

adduser monu



Set a simple password example 12345 or hello or 987654321

**NOTE** **-** **Every student have to use different password.**

Get the details of password hash in /etc/passwd



Get the details of hash in /etc/shadow



**Hash -** monu:$y$j9T$N4WQ3BgSMNRd Kd641Y4H0/p1$5FG1XwxT4GS+SH/nqxR5oGdyntymo2s 2sbdt+ZLdj2uJ.:20224:0:99999:7:::

Task 6: Cracking password hashes

Cracking password with prebuilt wordlist of john in default mode.

John passwd.txt

John passwd.txt --show

Cracked password – 12345

Task 7: Remediation and Recommendation

Identified Issues and Recommendations:

1. Outdated FTP Server (vsftpd 2.3.4):

Vulnerable to backdoor attack.

Remediation: Upgrade to latest secure version (e.g. vsftpd 3.0.5).

2. Outdated SSH server(OpenSSH 4.7p1):

Susceptible to brute force and potential RCE.

Remediation: Update to latest version (e.g. OpenSSH 9.6).

3. Insecure Java RMI Service:

Allows remote code execution.

Remediation: Disable or restrict RMI access with firewall rules.

MAJOR LEARNING

* Acquired hands-on knowledge of Nmap for network scanning and system enumeration.
* Built practical skills in exploiting services and escalating user privileges.
* Gained familiarity with password cracking methods using John the Ripper tool.
* Enhanced understanding of security measures and approaches for effective remediation