

hACKING éTICO

Unidad 3. Actividad 3



01 de abril de 2024

Carlos DÍAZ MONTES

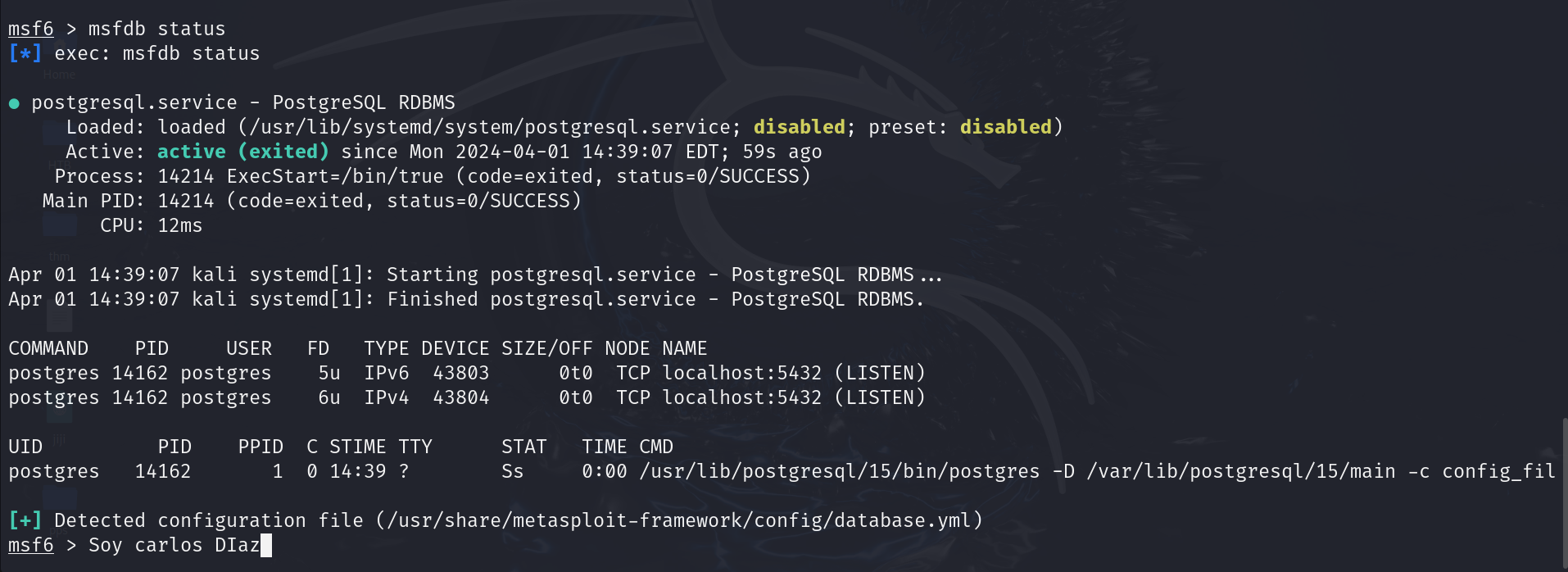
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Primeros pasos en metasploit 2](#_Toc162970237)

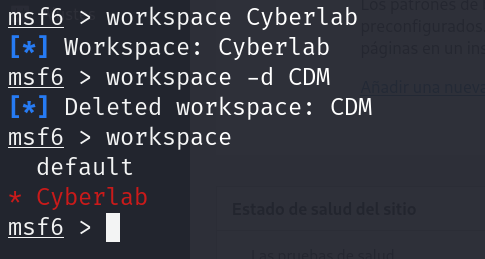
# Primeros pasos en metasploit

**Ejercicio 1: Conectado a la base de datos**



**Ejercicio 2: Gestión básica de workspaces**

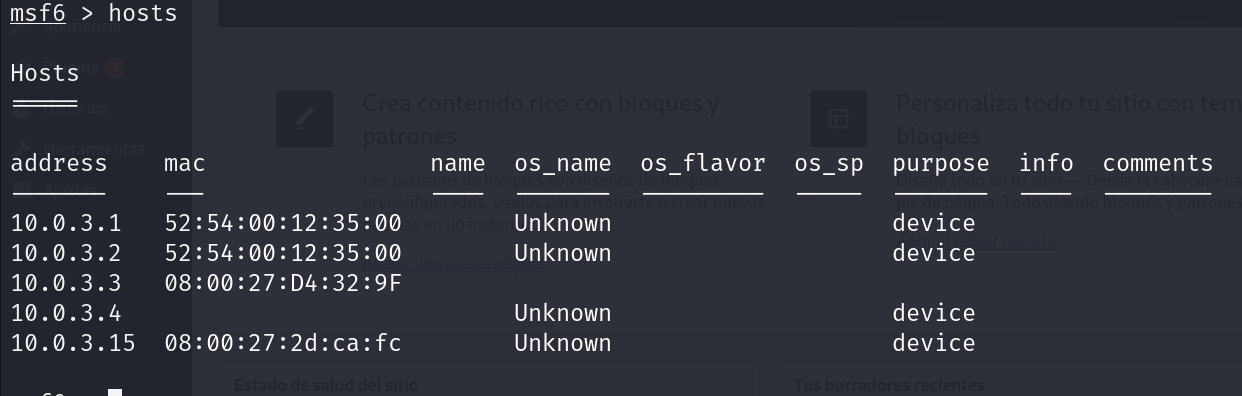




**Ejercicio 3: nmap desde metasploit**

Comando ejecutado:  


Resultado de los hosts:

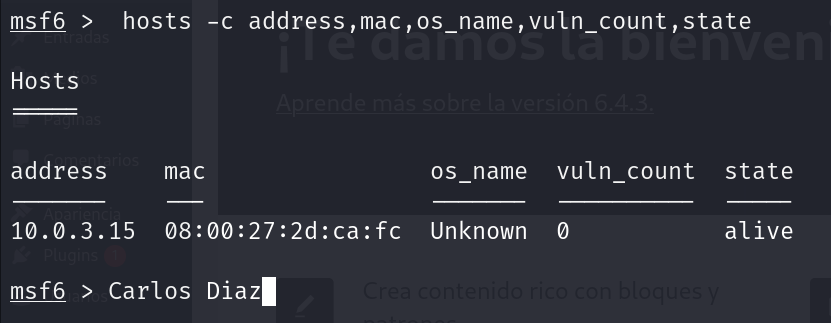


**Ejercicio 4: Borrar hosts**

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:

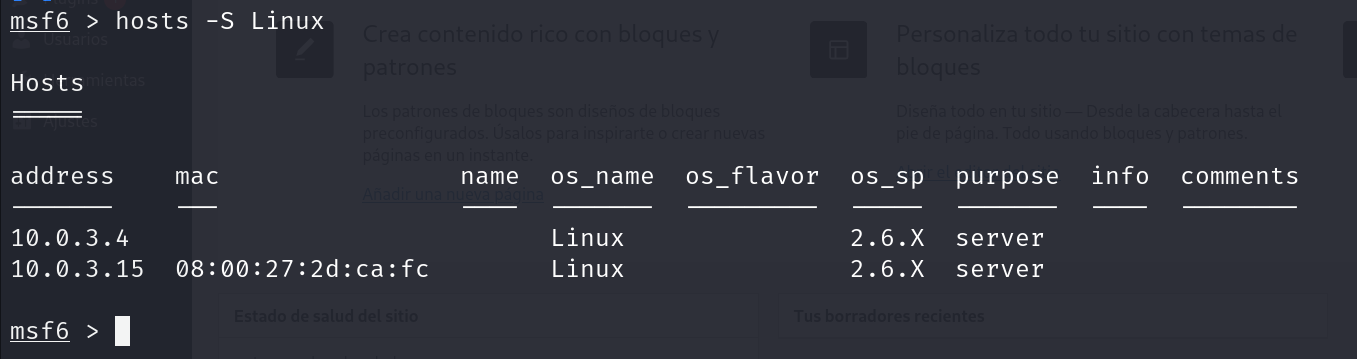


**Ejercicio 5: Cambiar columnas de hosts**



**Ejercicio 6: Consultar máquinas Linux**

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

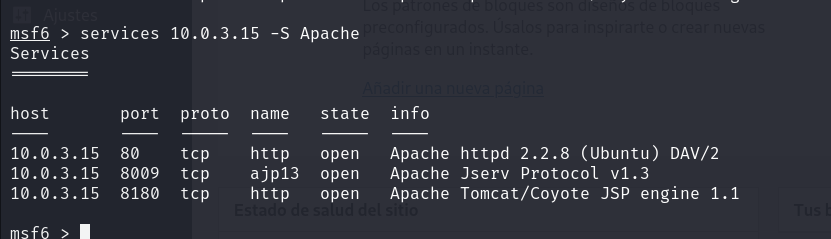


**Ejercicio 7: Poblar RHOSTS**

Lo he probado con el filtro Windows y Linux:



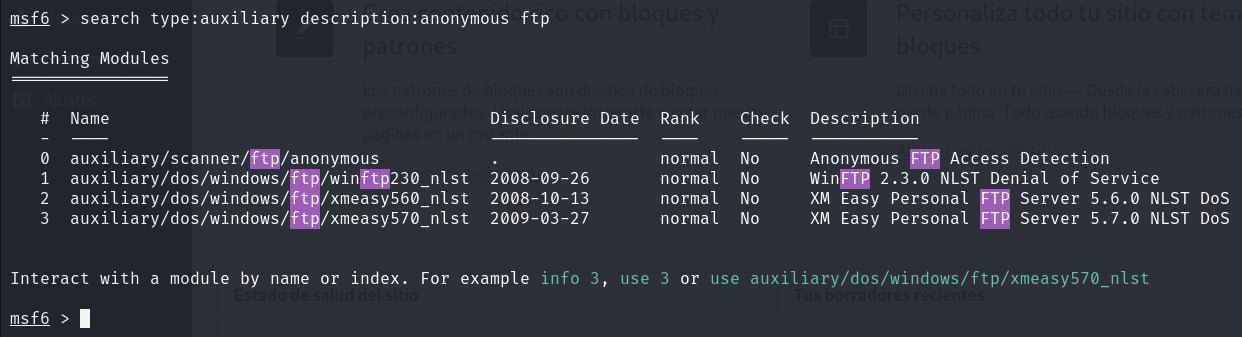
**Ejercicio 8: Filtrado de servicios de metasploitable 2**



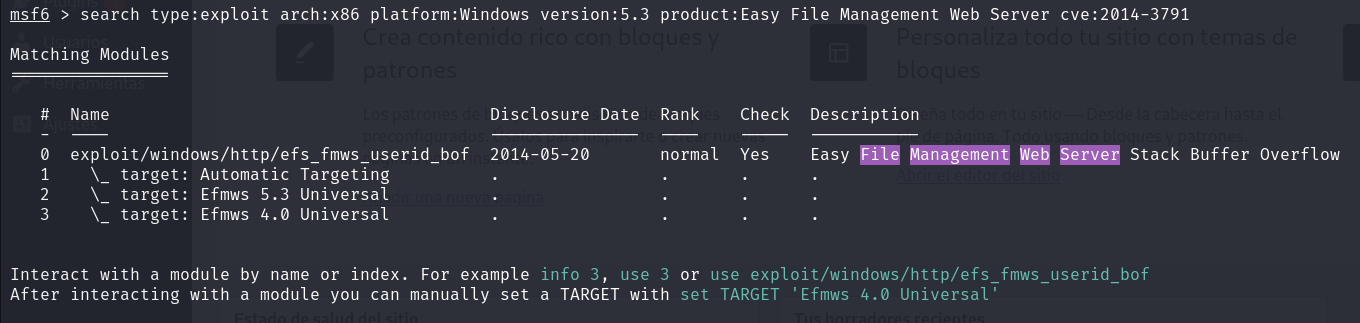
**Ejercicio 9: Filtrado de servicios según puerto**



**Ejercicio 10: Módulos auxiliares de ftp**



**Ejercicio 11: Busca el exploit!**



**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?

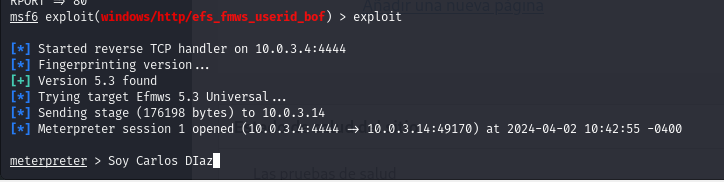
el exploit está diseñado para la plataforma Windows y específicamente para sistemas con arquitectura x86.

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.

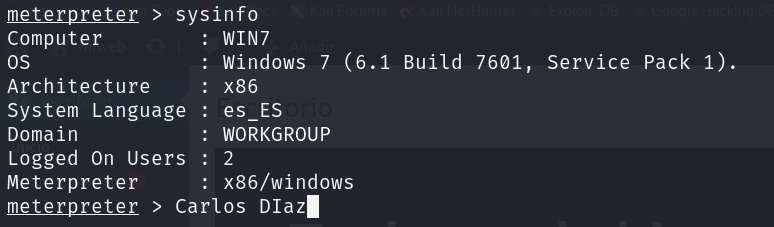
De aquí es donde he sacado la información:  


**Ejercicio 13: Ejecuta el exploit!**

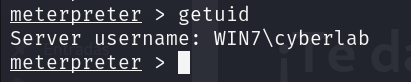


**Ejercicio 14: Información del objetivo con meterpreter**

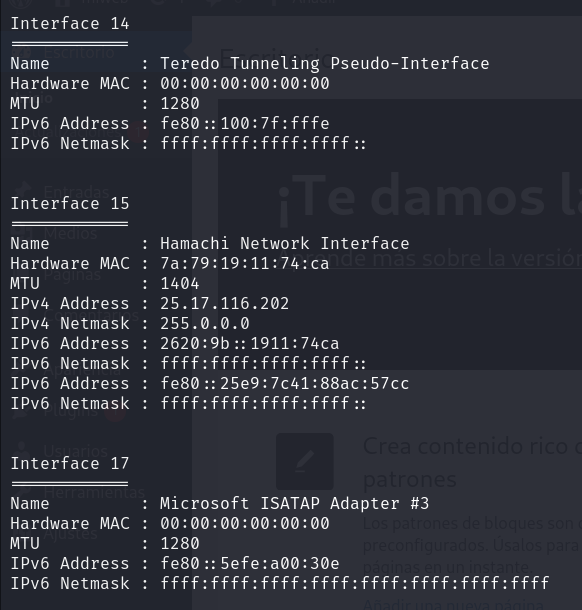
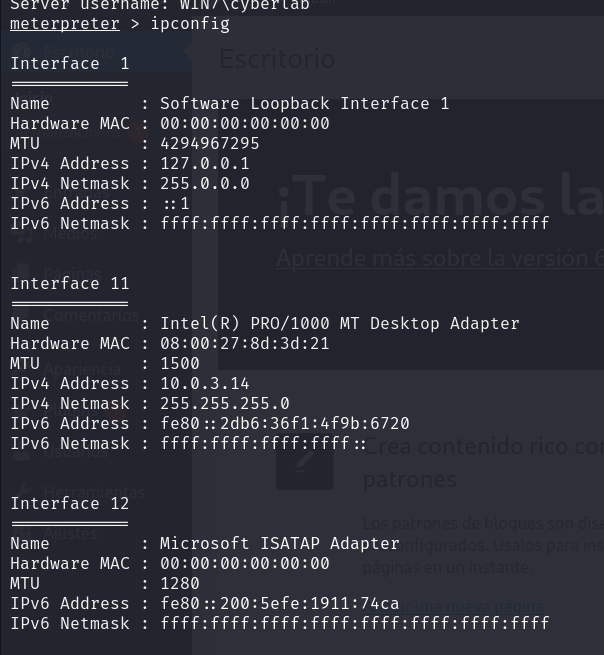
Sysinfo:



Getuid:

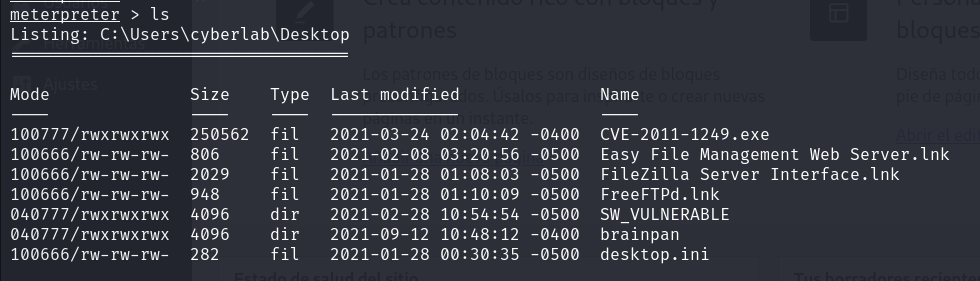


IPs de la máquina:

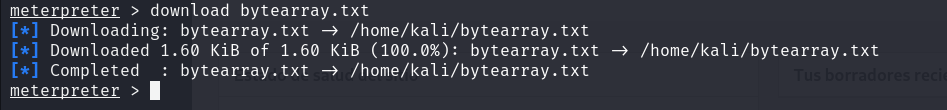


**Ejercicio 15: Descarga de ficheros**

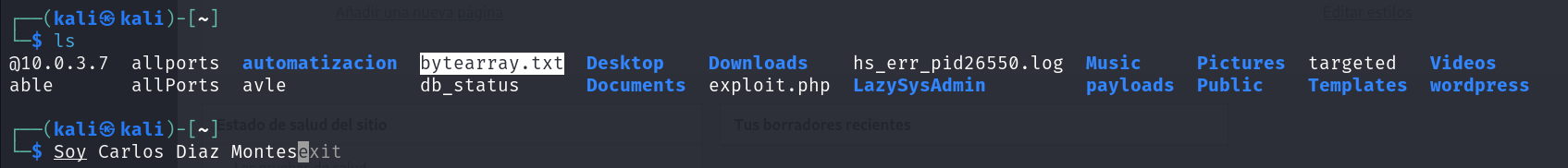
No encuentro el archivo que nos pide:



De todas maneras me voy a descargar otro archivo:

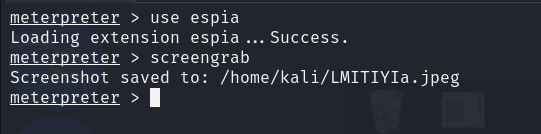


Aquí muestro que tengo el archivo en mi carpeta personal:

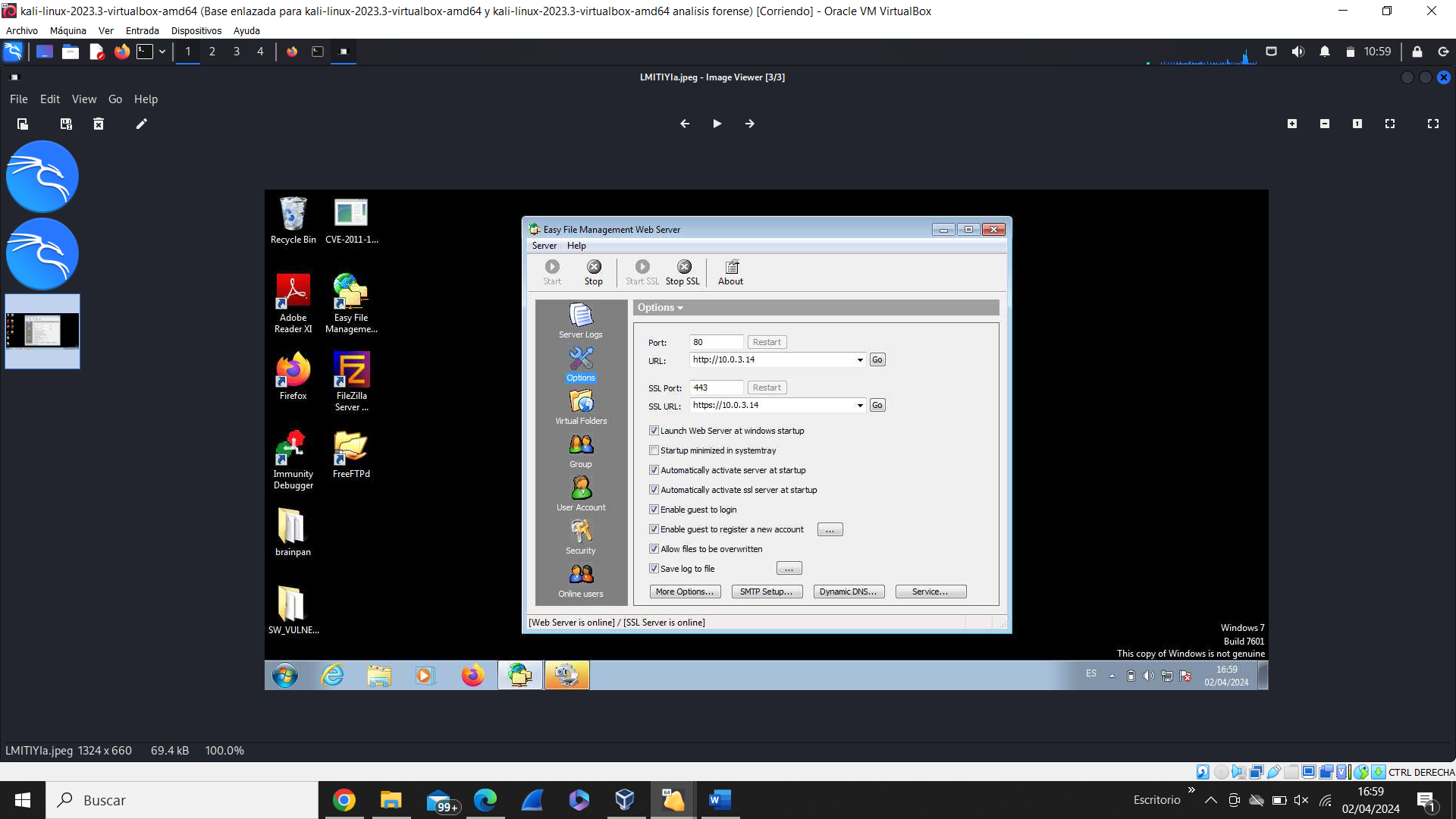


**Ejercicio 16: Captura de pantalla**

El comando usado para la captura de pantalla:



Resultado:



Comando usado para el streaming:

Este comando no lo he encontrado.

**Ejercicio 17: Keylogger**

