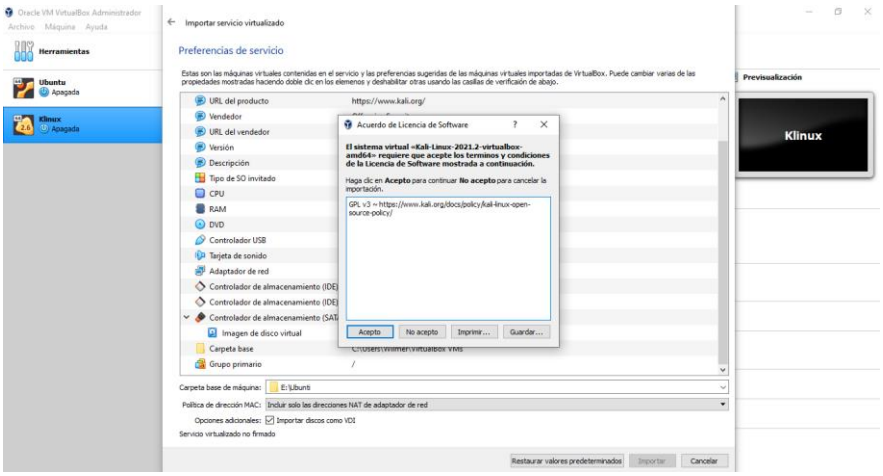
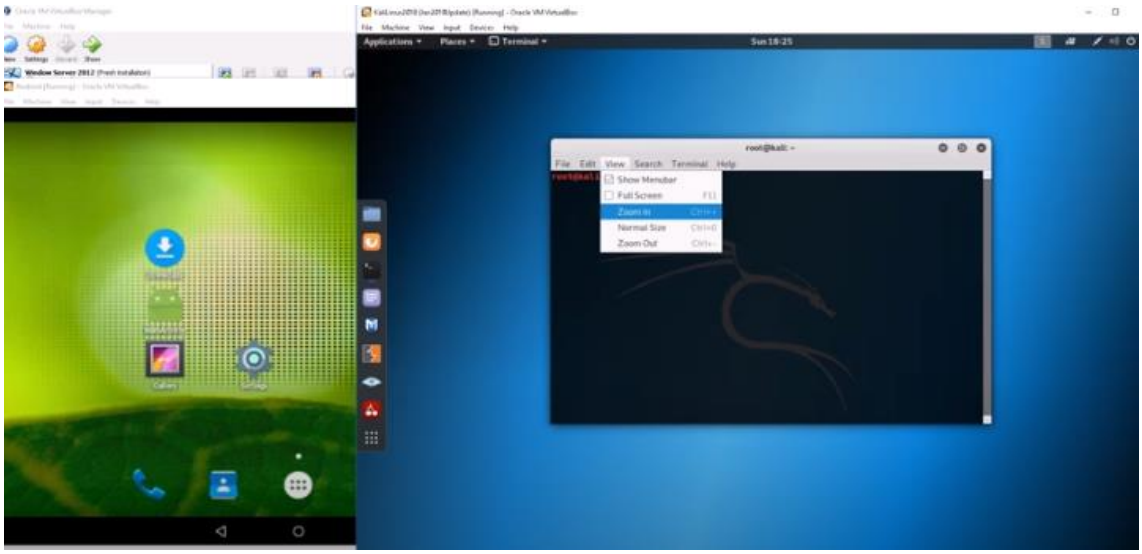
UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD DE FILOSOFIA, LETRAS Y CIENCIAS DE LA EDUACION
CARRERA DE PEDAGOGIA DE LA INFORMATICA
ADMINSTRACIÓN DE CENTROS INFORMÁTICOS
INFORME DE KALI-INUX
METAEXPLOID

Nombre: Wilmer Fernando Ponce Robles

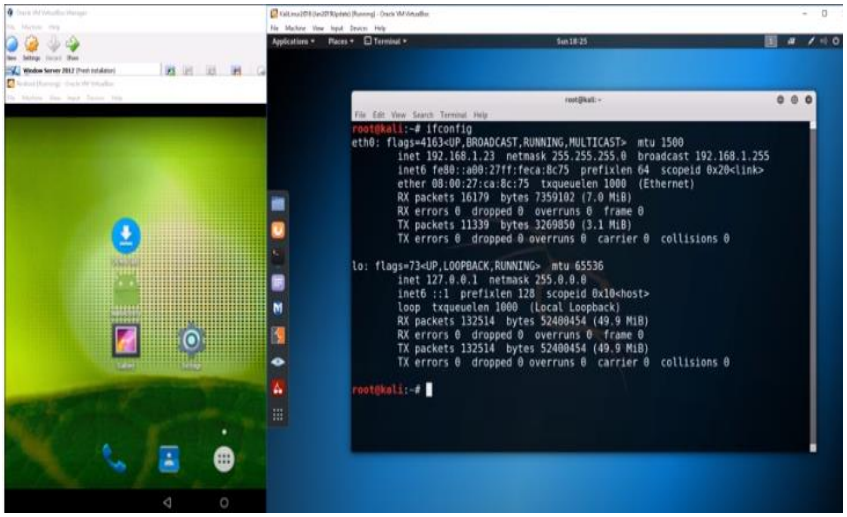
Instalación en máquina virtual



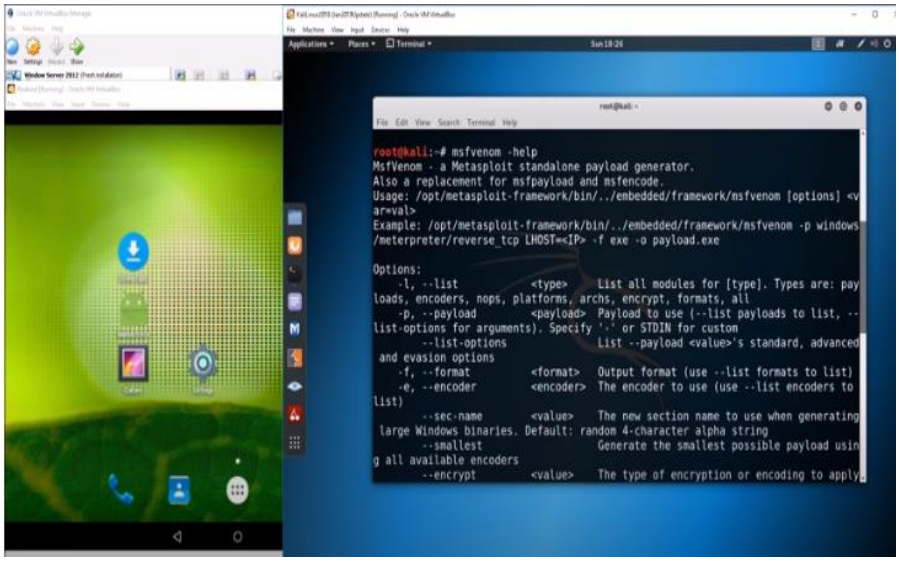
Inicio



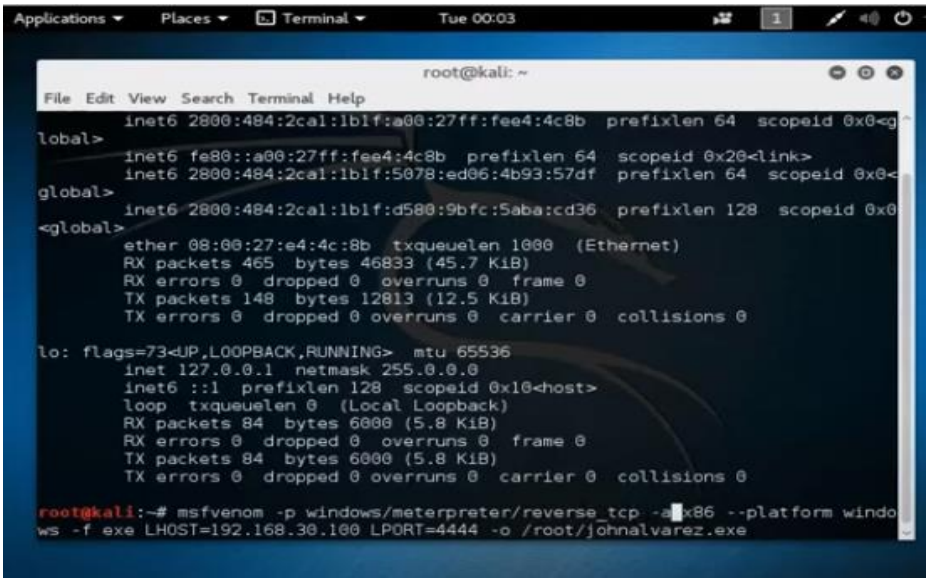
Prueba de comandos



Visualización de la lista de comandos a partir de msfvenom –help



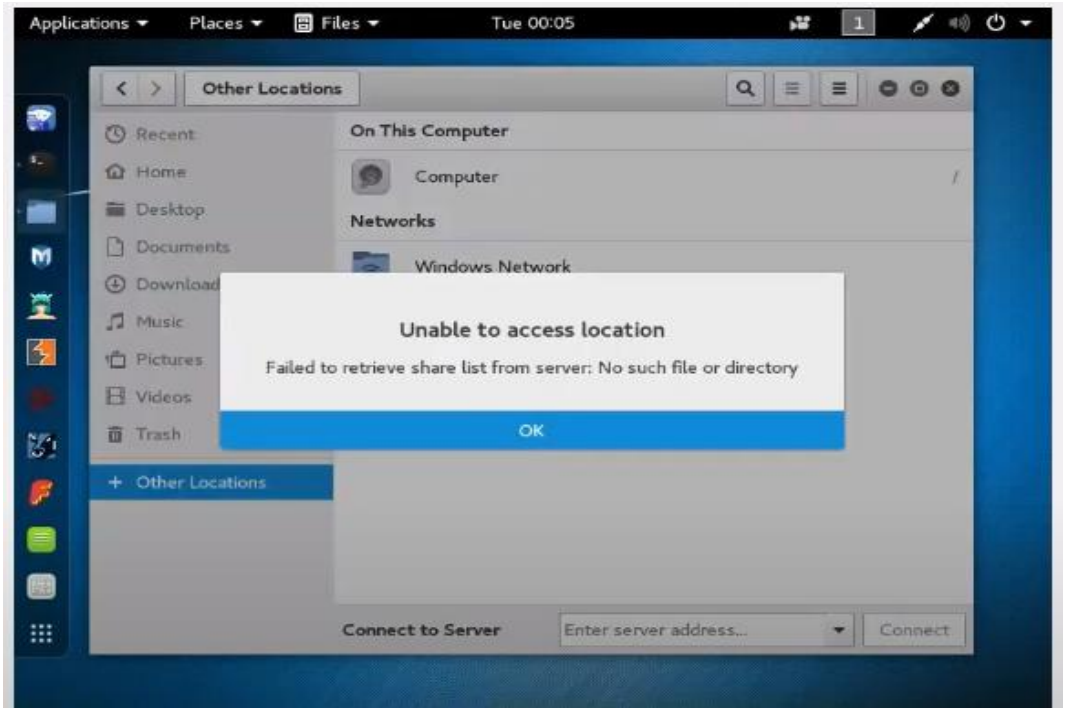
Comando para empezar se establece el comando msfvenom, nombre del sistema operativo, dirección de la red, puerta de enlace y el nombre del malware



Se genera un archivo, y este debemos llevarlo a Windows 10, hacer que el usuario de la máquina ejecute este archivo y poder empezar el ataque, a través de ingeniería social u otros medios

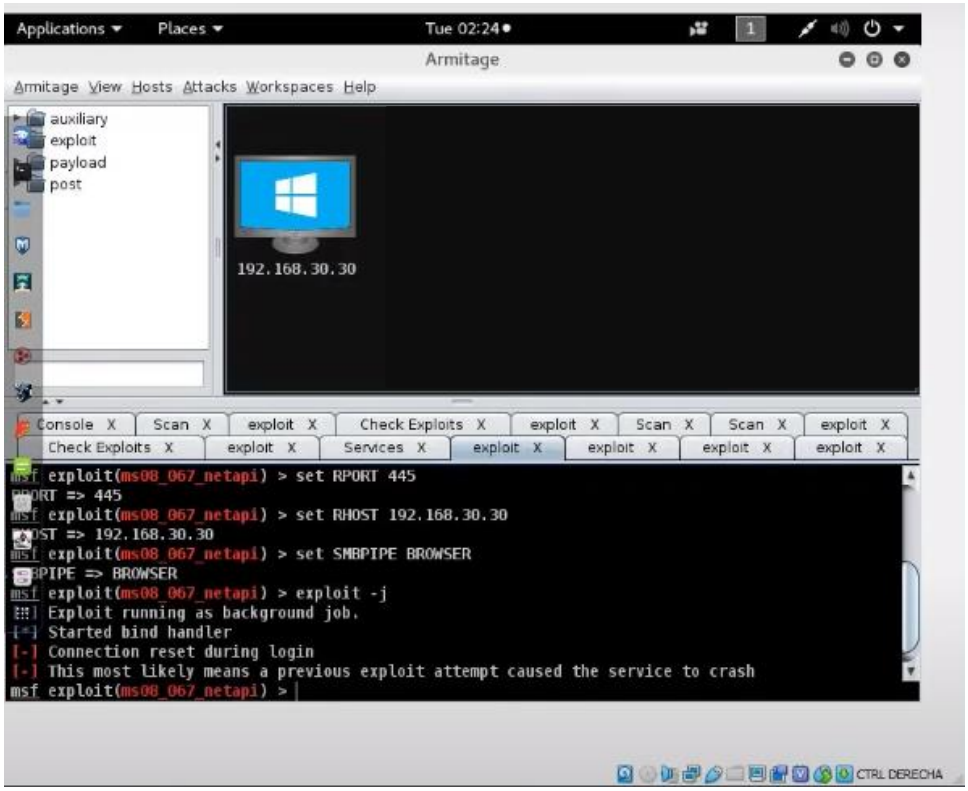
Este ataque se establecerá a través de la red, para ello es importante colocar de manera correcta la puerta de enlace y el host

Por ejemplo, en la siguiente imagen se visualiza un error en la conexión, esto se debe a que el usuario de Windows 10 todavía no ha ejecutado el archivo

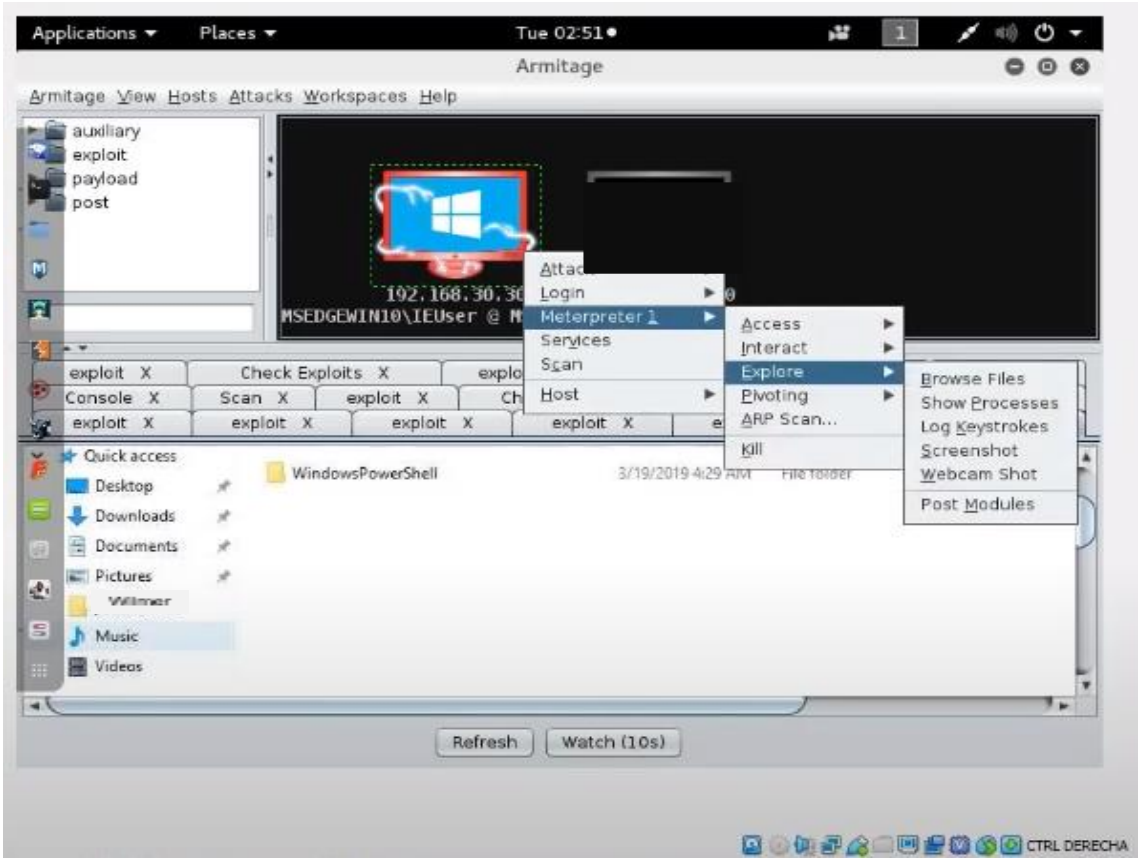


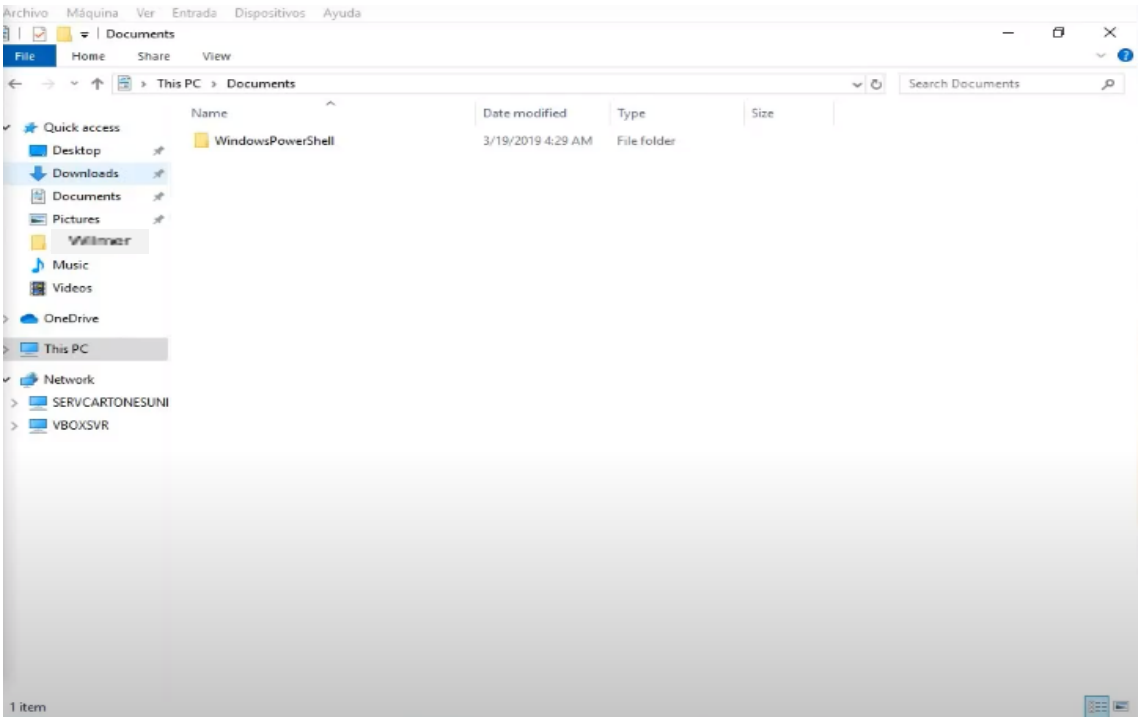
En el caso del software que se está utilizando en este momento, se habilita la siguiente ventana, esto se deja todo por defecto y presionar en connect.

Una vez que todo se haya realizado toda la configuración de manera correcta, en kali-linux aparecerá la siguiente ventana, la cual me da una imagen de un equipo con el logo de Windows 10, la cual puedo ejecutar e iniciar el ataque.



Luego de que haya empezado el ataque, en la parte inferior se puede ver una seria de opciones que sirven para ver las diversas tareas que está realizando el usuario de Windows 10. Por ejemplo se puede observar que está mostrando la carpeta en la cual el usuario atacado se encuentra, en tiempo real.


Applications
Places
Tue 02:51
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Login
Meterpreter 1
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Browse Files
Show Processes
Log Keystrokes
Screenshot
Webcam Shot
Post Modules
exploit X
Check Exploits X
Console X
Scan X
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
WindowsPowerShell
Refresh
Watch (10s)
CTRL DERECHA


Archivo Máquina Ver Entrada Dispositivos Ayuda
Documents
File Home Share View
This PC › Documents
Search Documents
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
SERVCARTONESUNI
VBOXSVR
WindowsPowerShell
3/19/2019 4:29 AM
File folder
1 item