Informe de Tercer Laboratorio

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Septiembre 2025

Tabla de Contenido

Pag.

Tabla de Ilustraciones

Pag.

Introducción

Este tercer laboratorio de seguridad y auditoría de redes tiene como objetivo simular un entorno controlado que represente una red real, permitiendo poner en práctica técnicas de reconocimiento, análisis y explotación de servicios/puertos vulnerables.

Dentro de este entorno se configuraron diferentes máquinas virtuales, entre ellas Kali Linux como sistema atacante, y Windows Server junto con Fedora Linux como sistemas víctimas. A través del uso de herramientas como Metasploit Framework y msfvenom, se generaron archivos ejecutables maliciosos (.exe para Windows y .elf para Linux) que, al ser ejecutados en las máquinas objetivo, permitieron establecer sesiones remotas mediante Meterpreter.

De esta manera se busca comprender los mecanismos de explotación, los riesgos de ejecutar archivos no confiables y la importancia de aplicar medidas de seguridad en los sistemas operativos tanto Windows como Linux.

Objetivos

Objetivo General

Simular un entorno controlado que represente una red real mediante el uso de máquinas virtuales en red NAT, con el fin de poner en práctica técnicas de generación y ejecución de archivos maliciosos que permitan obtener acceso remoto a sistemas Windows y Linux a través de Metasploit Framework.

Objetivos Específicos

Crear una red NAT e integrar las máquinas virtuales para establecer un entorno seguro para llevar a cabo el laboratorio.

Escanear la red con Nmap con el fin de identificar dispositivos conectados.

Generar archivos ejecutables maliciosos con msfvenom (.exe y .elf) para Windows y Linux respectivamente.

Implementar un servidor Apache en Kali para distribuir los archivos maliciosos a las máquinas víctimas.

Obtener acceso remoto a las máquinas víctimas mediante sesiones Meterpreter.

Desarrollo

Ataque a Windows Server 2003

Desde la máquina atacante en este caso Kali Linux, se procede a crear un ejecutable malicioso para obtener acceso remoto a Windows Server 2003.

Ilustración 1 Creación de ejecutable .exe

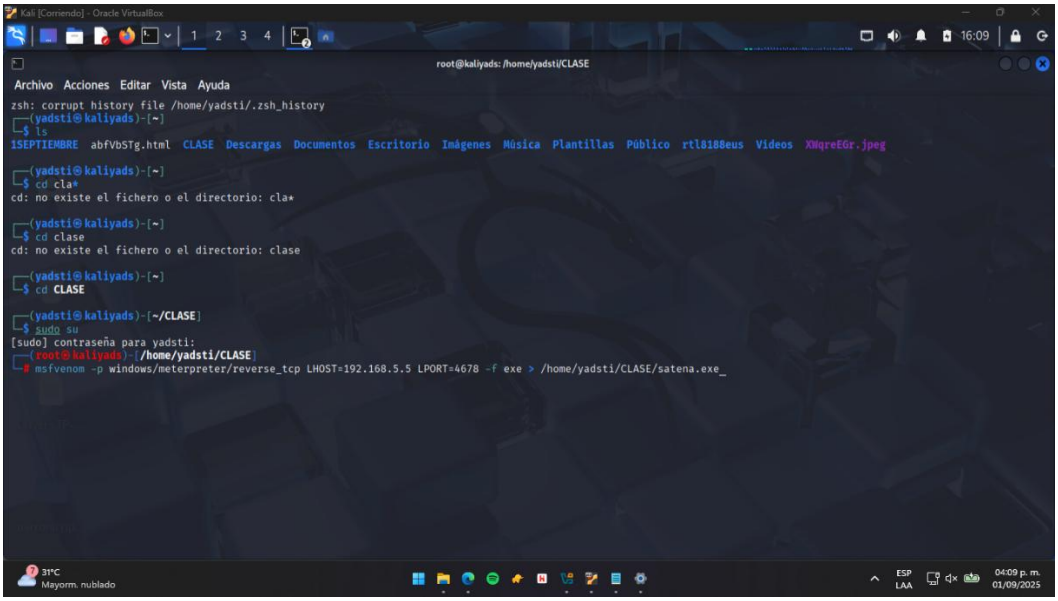
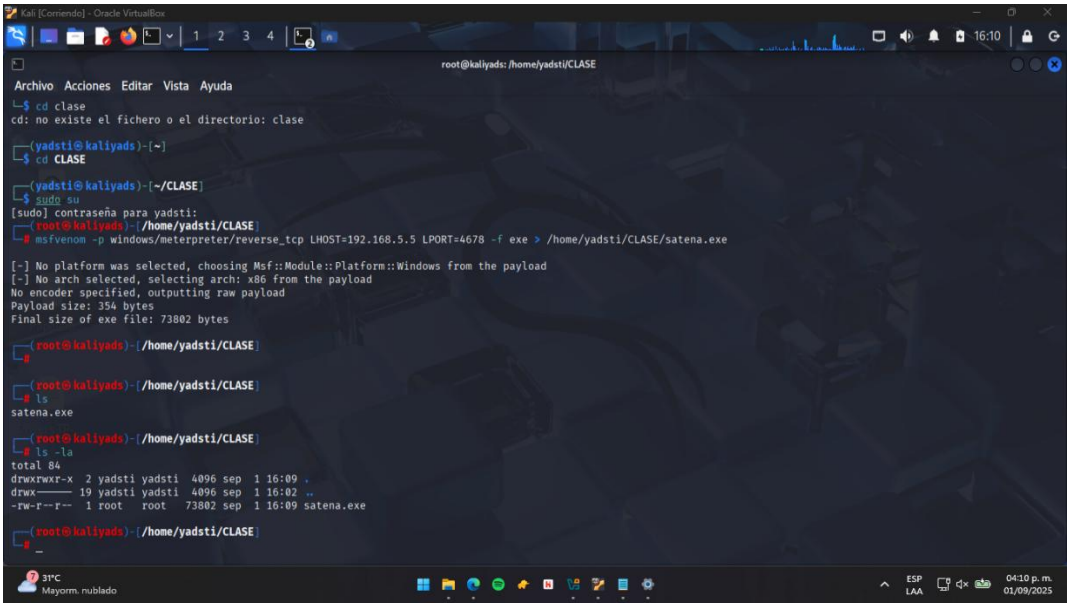
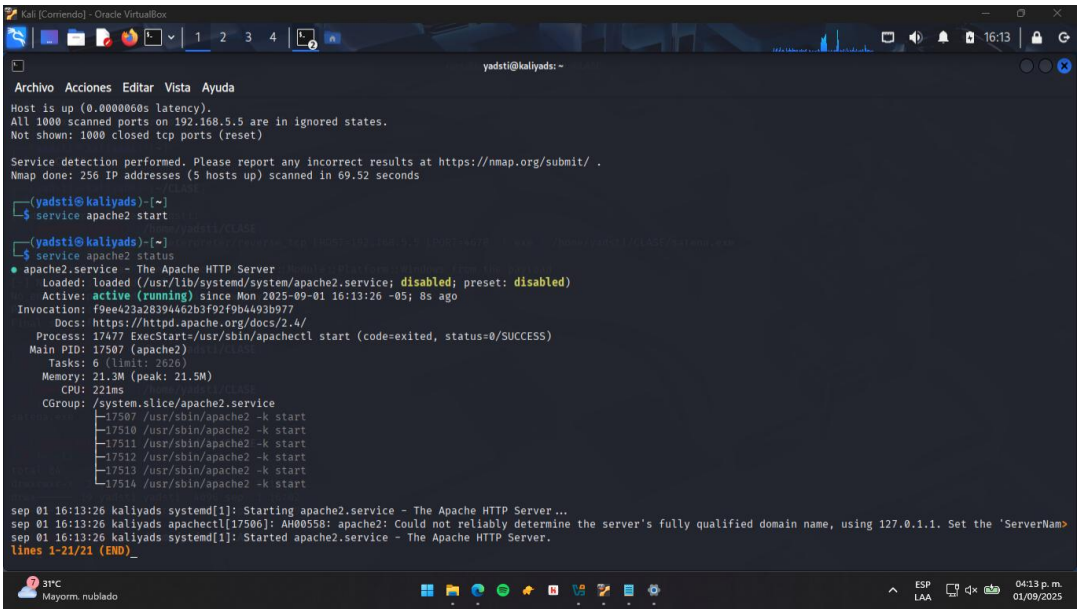


Ilustración 2 Verificación de ubicación del archivo



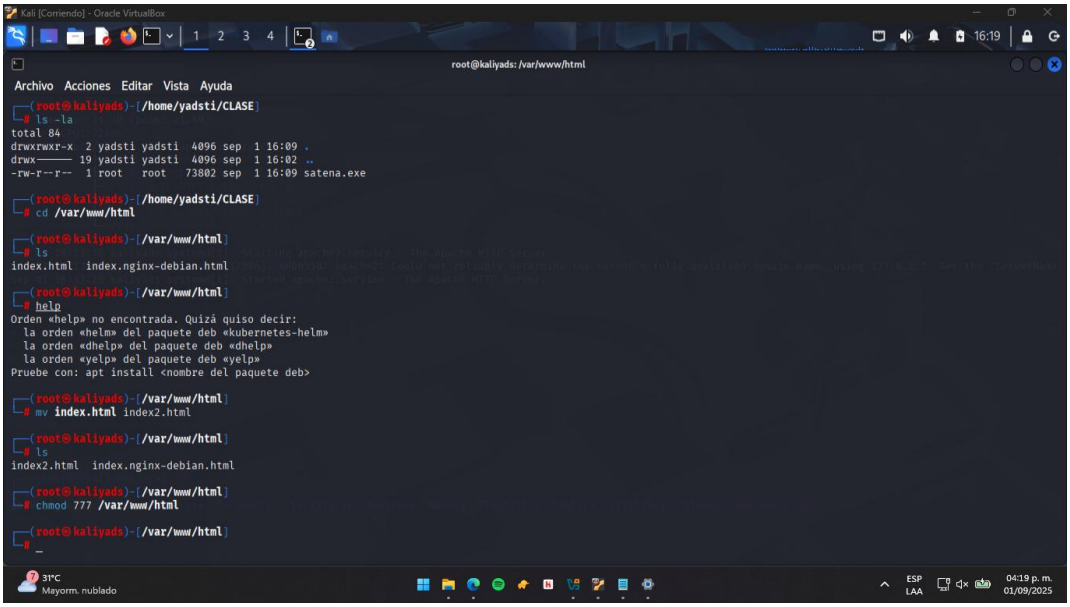
Luego se activa el servidor de Apache.

Ilustración 3 Activación de Apache



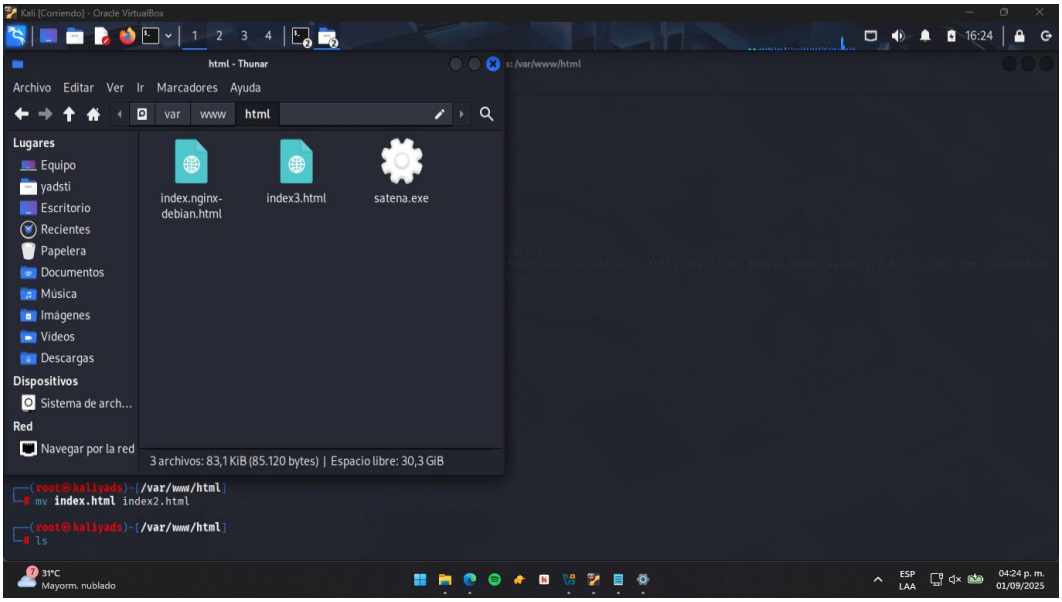
Luego se procede a cambiar el nombre de index.html a index2.html para que al ingresar la dirección IP del servidor en lugar de llevarnos a la pagina por defecto del servidor, muestre el directorio y de ahí poder descargar el ejecutable.

Ilustración 4 Modificación nombre index



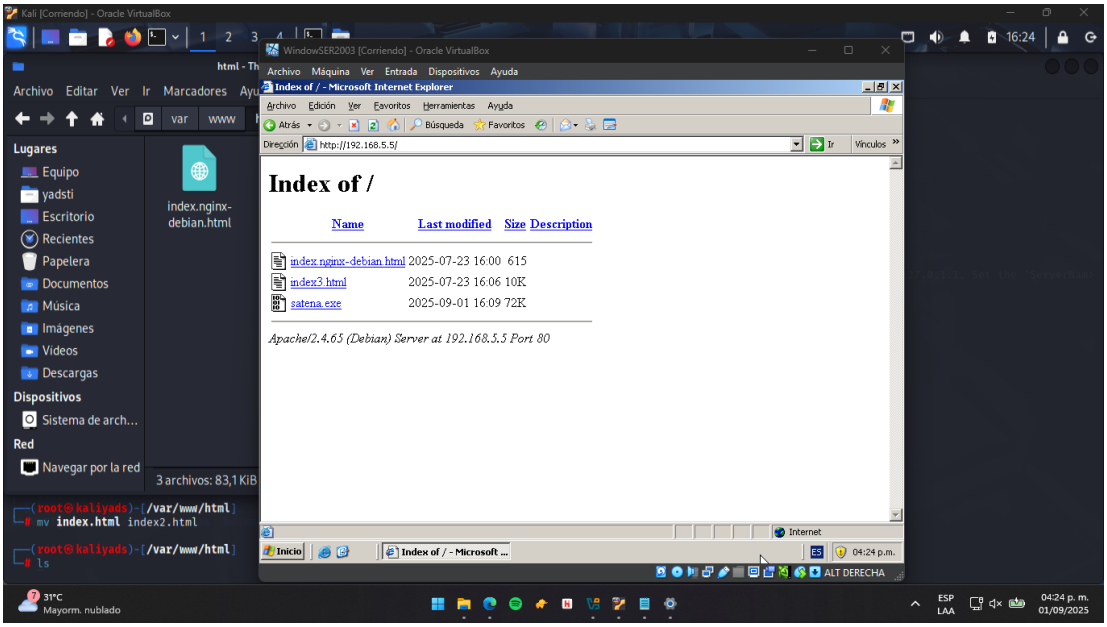
Luego el ejecutable creado se agrega a la carpeta html del servidor Apache.

Ilustración 5 Ejecutable Windows en Apache



Después desde la máquina de Windows Server 2003 (victima) se ingresa a la dirección IP del servidor y se descarga el ejecutable.

Ilustración 6 Descarga ejecutable Windows



Se procede a configurar el payload para capturar la información al momento de que la victima ejecute el archivo, para esto hay que abrir msfconsole, buscar multi/handler y configurarlo con el LHOST y RHOST, los mismos que se utilizaron al momento de crear el archivo.

Ilustración 7 Msfcsonle

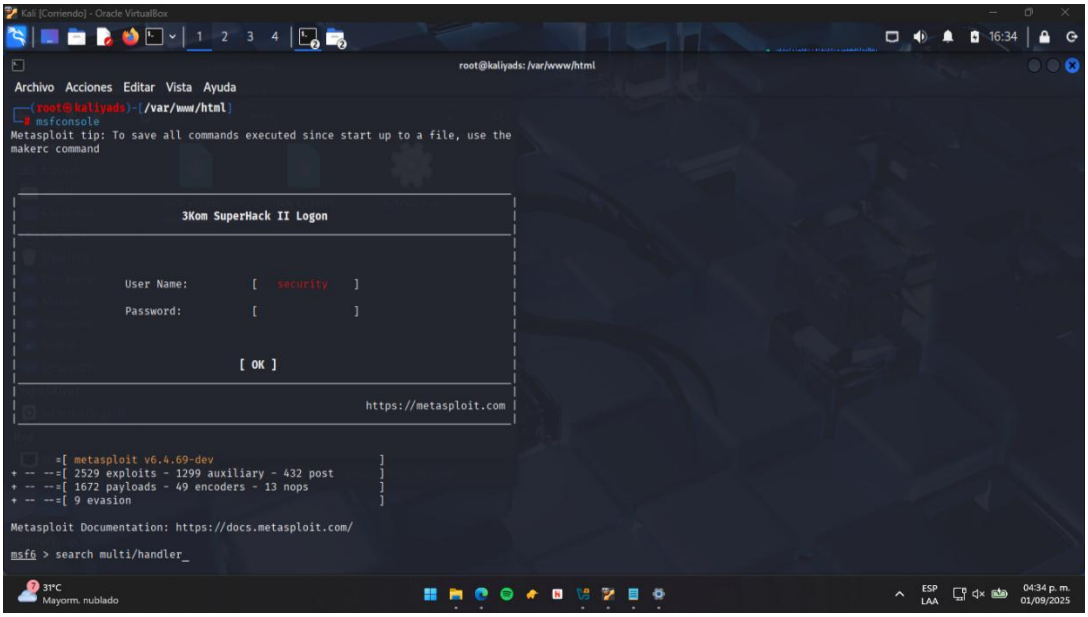
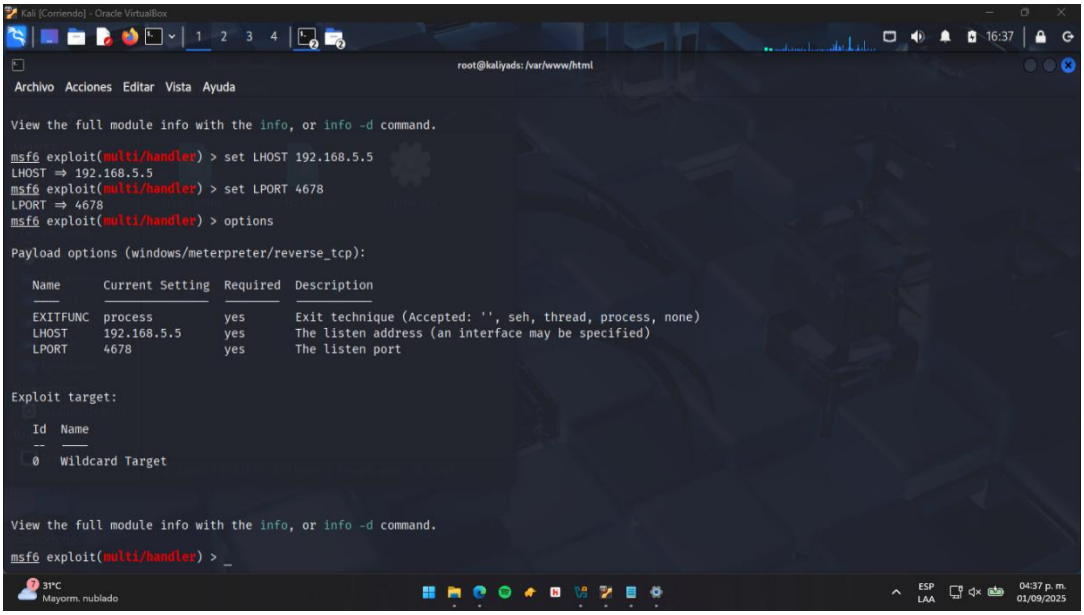
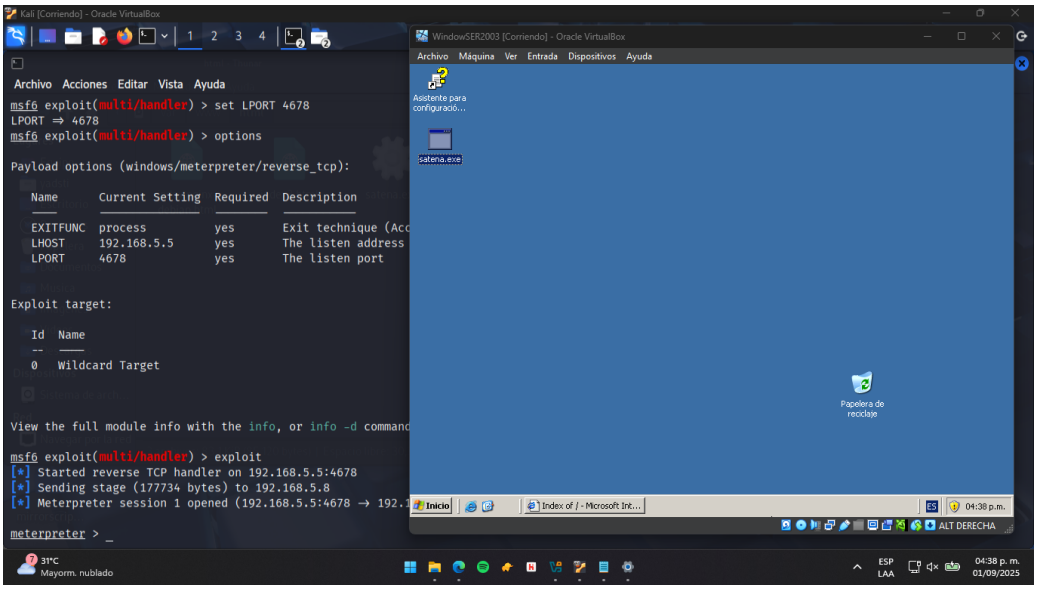


Ilustración 8 Configuración de Payload



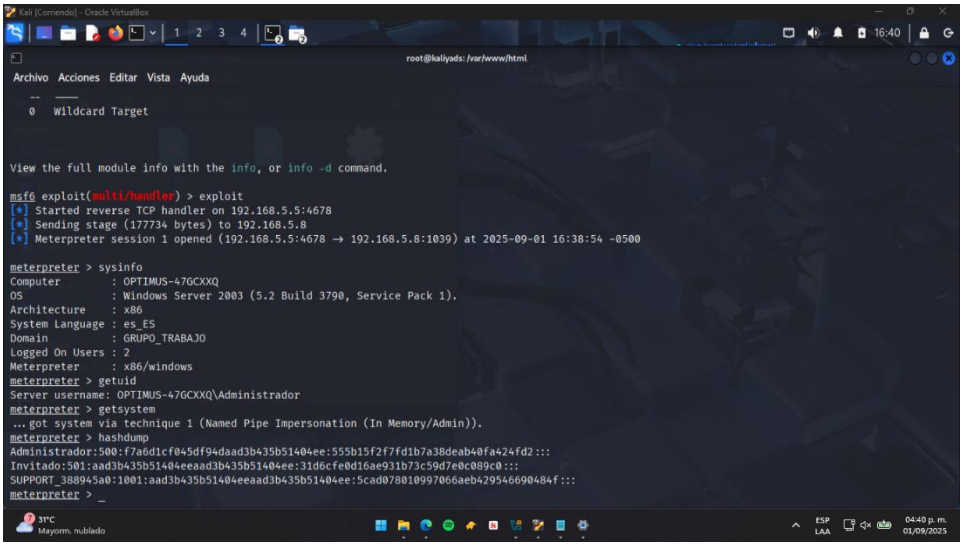
Luego de que se configura el payload se ejecuta el comando exploit y se abre el archivo satena.exe en Windows Server 2003 y como se evidencia en la siguiente ilustración se captura la información y se abre la sesión de meterpreter.

Ilustración 9 Exploit

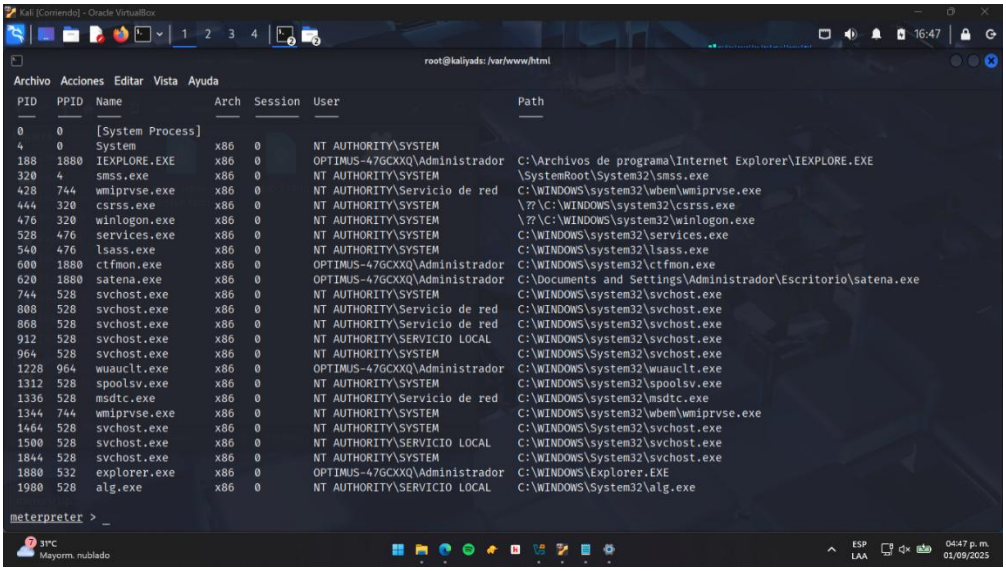


Una vez es exitoso se procede a obtener la información del sistema operativo utilizando el comando **sysinfo,** luego se obtiene el usuario con el comando **getuid,** después se escalan permisos con el comando getsystems.

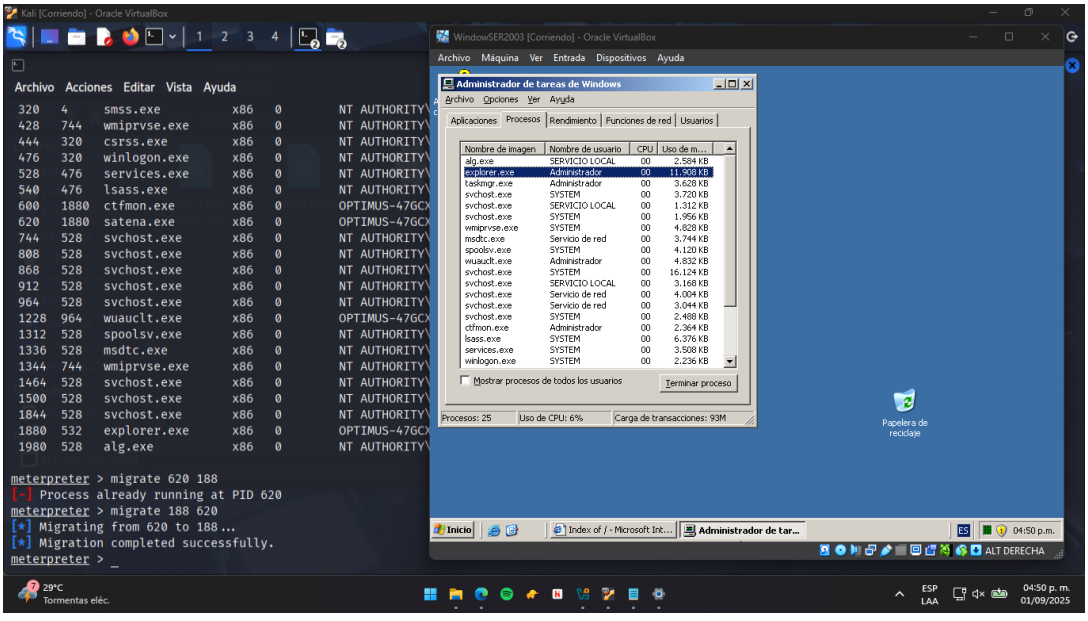
Ilustración 10 Información de la victima



Luego se listan los procesos utilizando el comando **ps,** esto para saber que procesos se están ejecutando en la víctima, esto con el fin de identificar el archivo que está capturando toda la información y tiene el acceso remoto.



Una vez identificado el archivo en función se procede a migrarlo a un proceso normal y rutinario del sistema operativo como es explorer.exe.

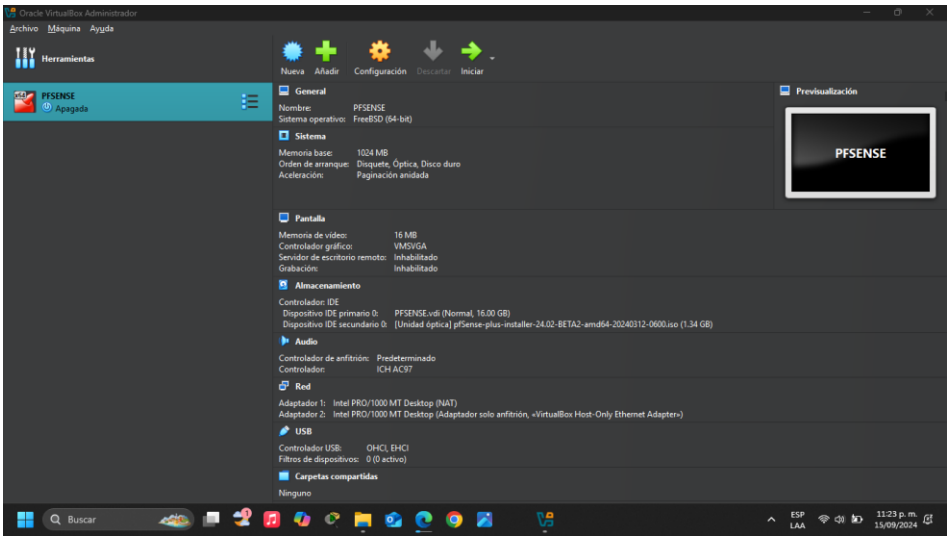


En la ilustración anterior se evidencia que se pudo migrar el proceso y por consiguiente ocultarlo

Configuración de Máquina Virtual de Fedora

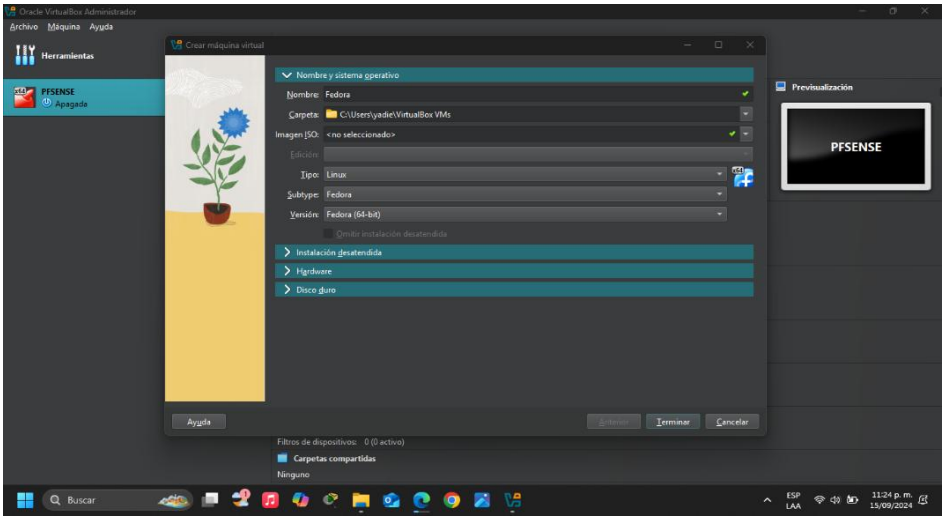
Como primer paso se inicia virtual box.

Ilustración 11 Inicio de Virtualbox



Luego se hace clic en la opción de **nueva** que tiene el símbolo de + de color verde, cuando se da clic en dicha opción se despliega una ventana emergente donde se nombra la máquina virtual como se evidencia en la **ilustración 12**.

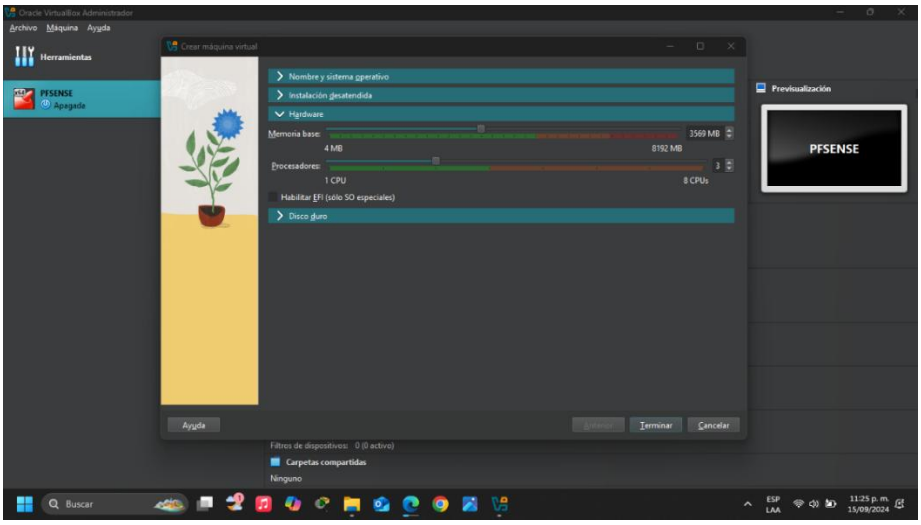
Ilustración 12 Asignación nombre máquina virtual



Luego de configurar el nombre de la máquina virtual, se hace clic sobre el apartado de Hardware para proceder a configurar la cantidad de memoria RAM y la cantidad de núcleos del

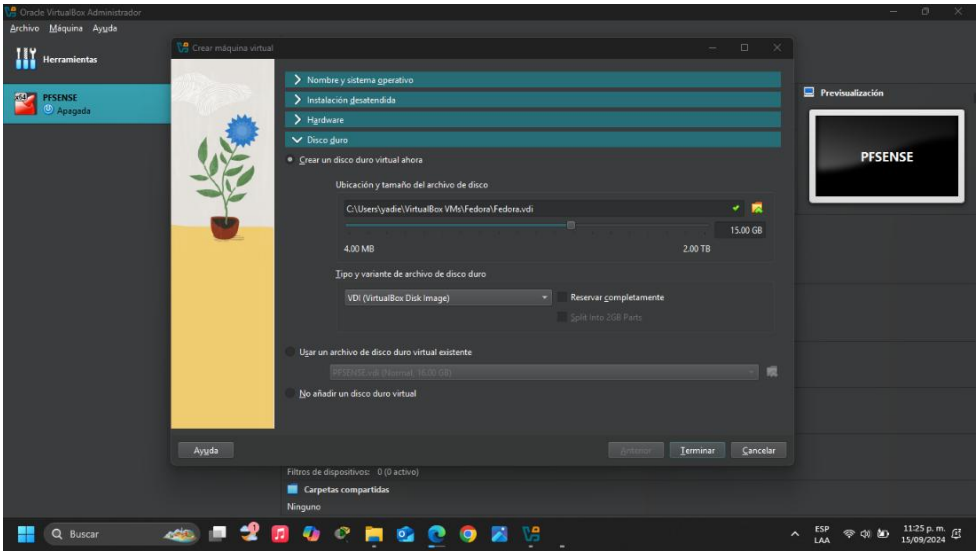
procesador que se le va a destinar a la máquina virtual para su funcionamiento. Lo recomendable es asignar recursos dentro del rango verde para que el sistema funcione de forma idónea.

Ilustración 13 Destinación de Hardware



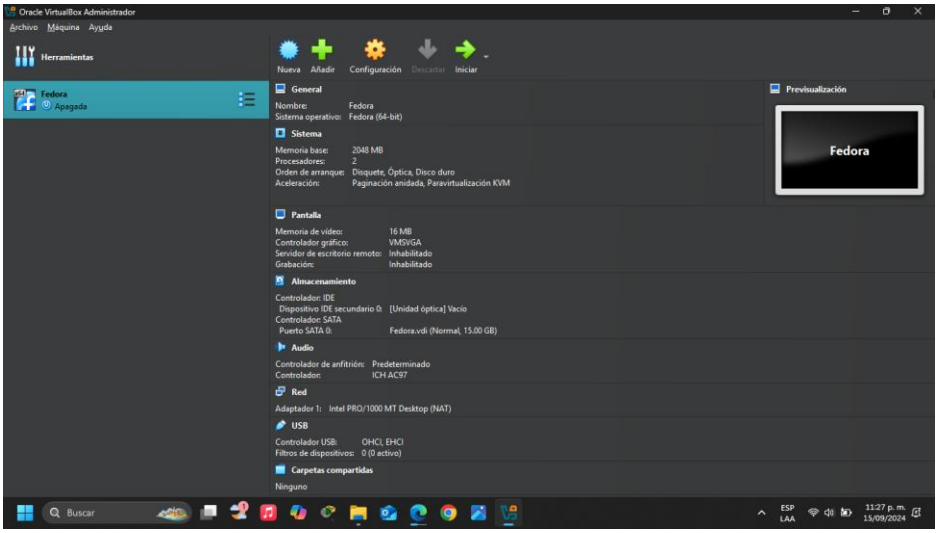
Después se hace clic en el apartado de disco duro, para asignar un espacio en el disco duro de la computadora, en este caso se asignan 15 GB.

Ilustración 14 Asignación de espacio disco duro



Luego de eso se hace clic en terminar y se observa la máquina virtual ya creada como se evidencia en la siguiente ilustración.

Ilustración 15 Máquina fedora creada

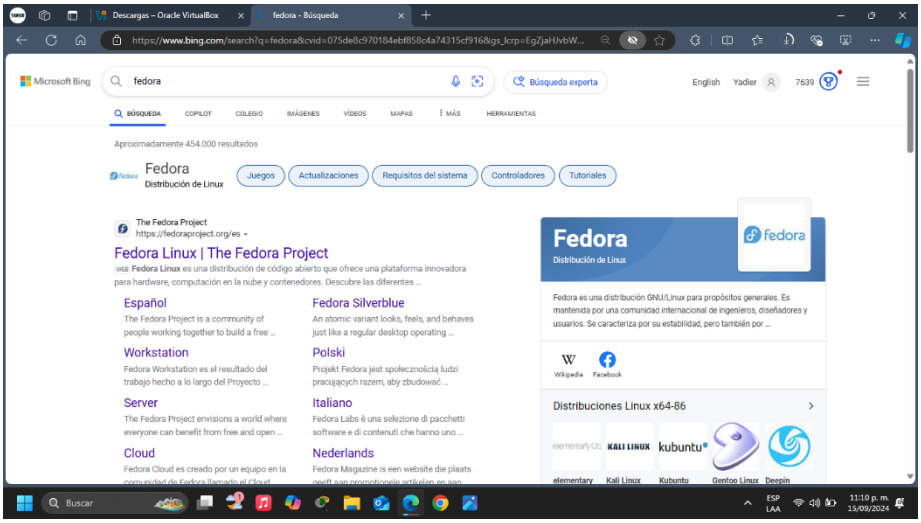


Luego de configurar la máquina virtual se procede a descargar el archivo de la imagen ISO de Fedora.

Descarga de imagen ISO de Fedora

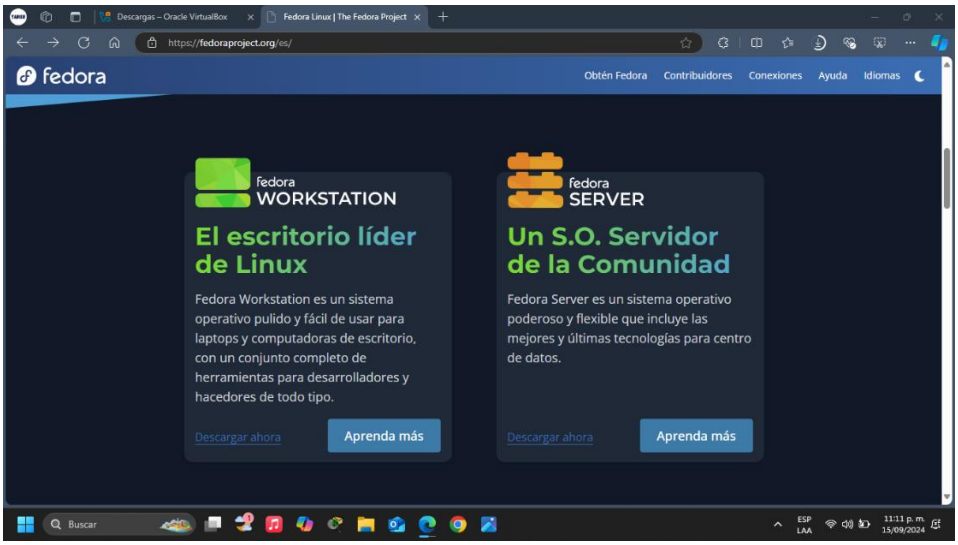
Se abre el navegador de preferencia, se busca y se ingresa al sitio de Fedora.

Ilustración 16 Proceso descarga Fedora



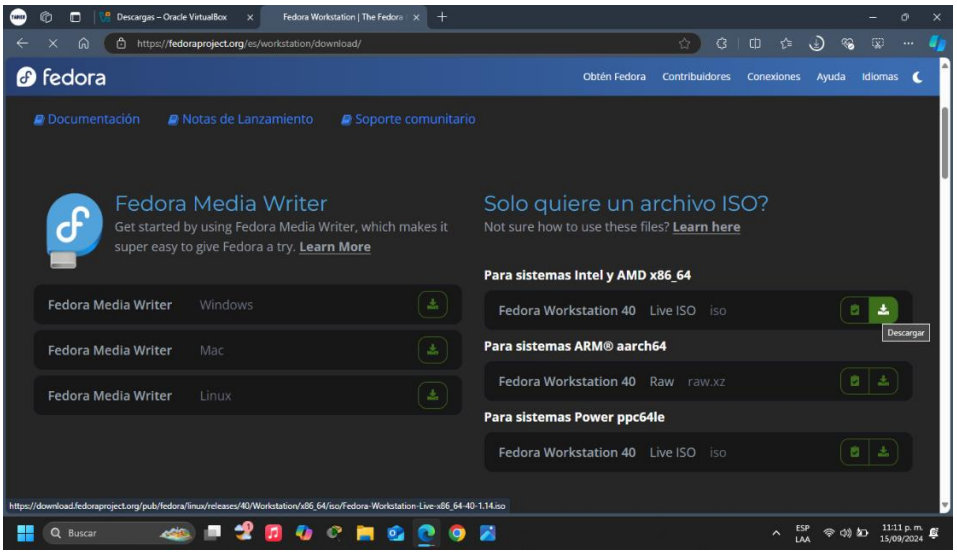
En el sitio de Fedora se hace clic en la parte que dice **Fedora Workstation**, específicamente en la opción de **descargar ahora**.

Ilustración 17 Sitio oficial Fedora



Estando allí se selecciona el archivo ISO para sistemas Intel y AMD x86_64 y se hace clic en descargar y la descarga iniciará automáticamente.

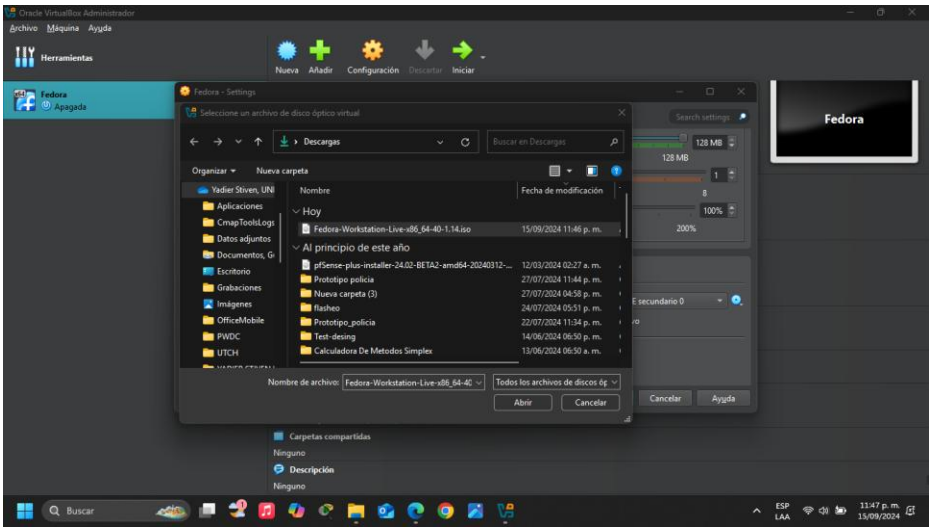
Ilustración 18 Descarga de archivo ISO



Después de que finalice la descarga, se abre nuevamente virtual box y la configuración de la máquina virtual con el nombre fedora, estando en la configuración se posiciona en el apartado de pantalla, en la parte de pantalla se posiciona en almacenamiento. En esa parte se da en el disco que está en la parte superior derecha y se le da en la opción de seleccionar de disco local, una vez

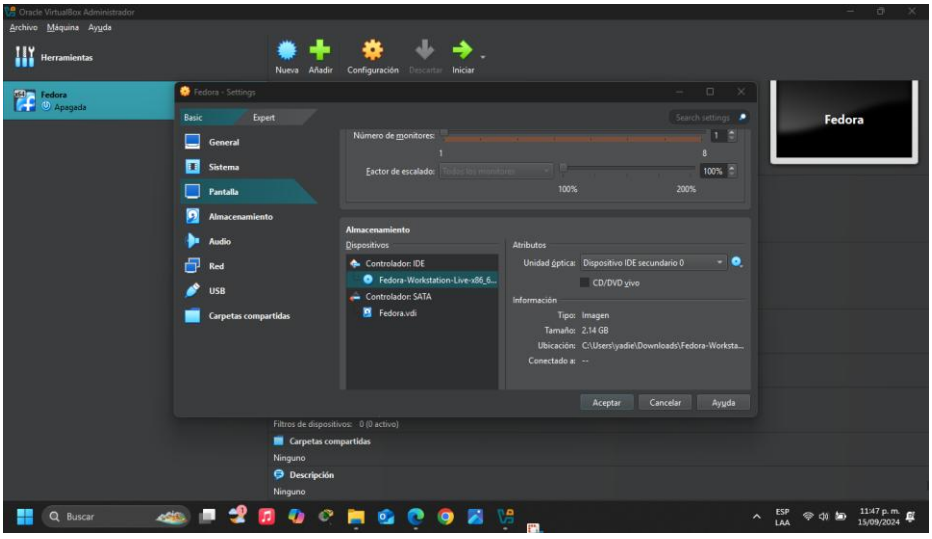
ahí se abre el explorador de archivo y se selecciona el archivo ISO, luego de eso se da en abrir y finalizar.

Ilustración 19 Inserción de archivo ISO en máquina virtual



Luego de eso, el apartado de pantalla en la parte de almacenamiento debería verse de la siguiente manera.

Ilustración 20 Máquina Configurada

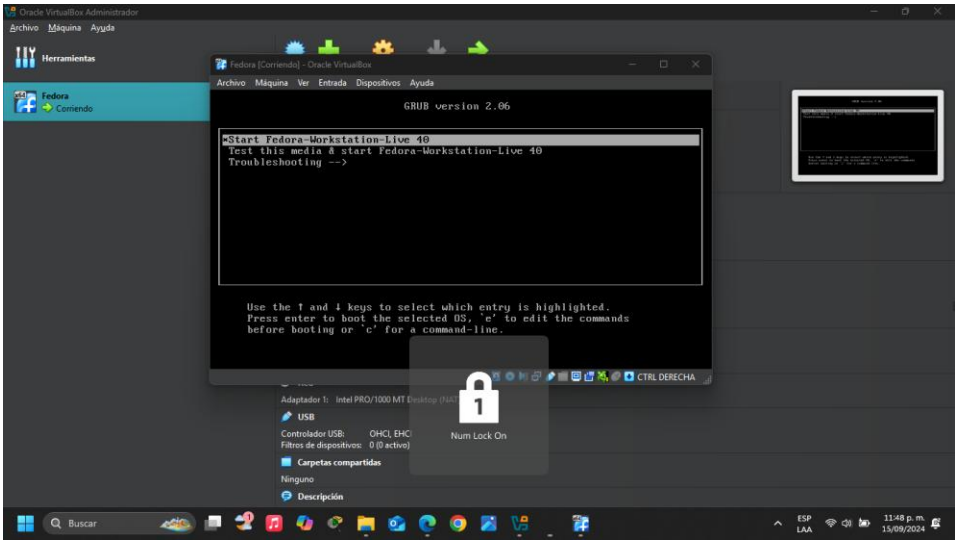


Instalación y configuración de Fedora

Luego de haber llevado a cabo los pasos anteriores, se procede con la instalación de Fedora, para ello se inicia la máquina virtual.

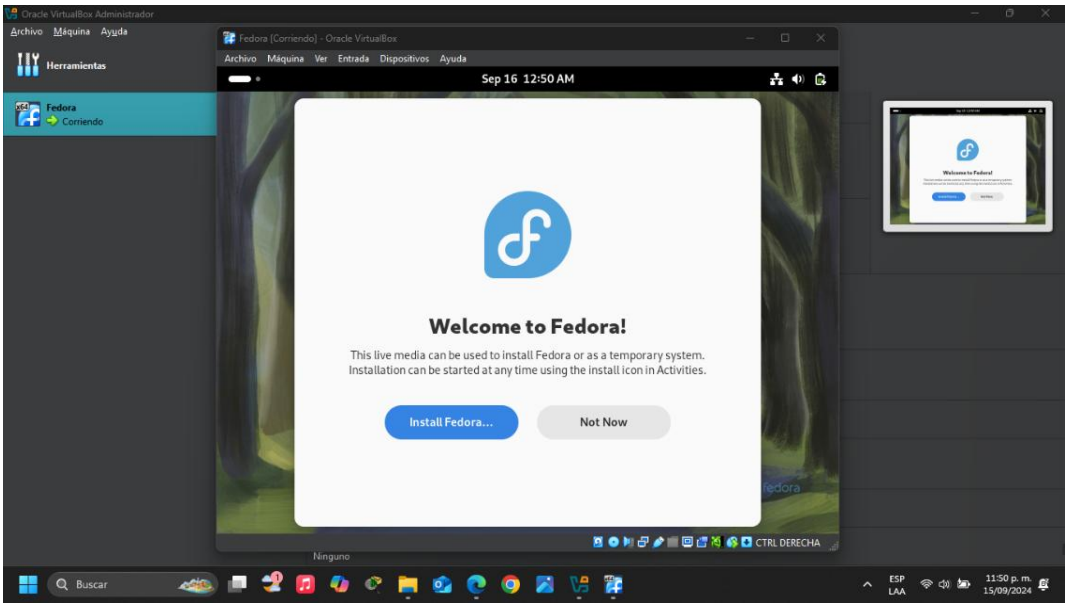
Cuando se inicia la máquina virtual de Fedora aparece un cuadro de dialogo como el que se observa en la ilustración 21, en dicho cuadro de dialogo seleccionar la primera opción y dar enter.

Ilustración 21 Grub



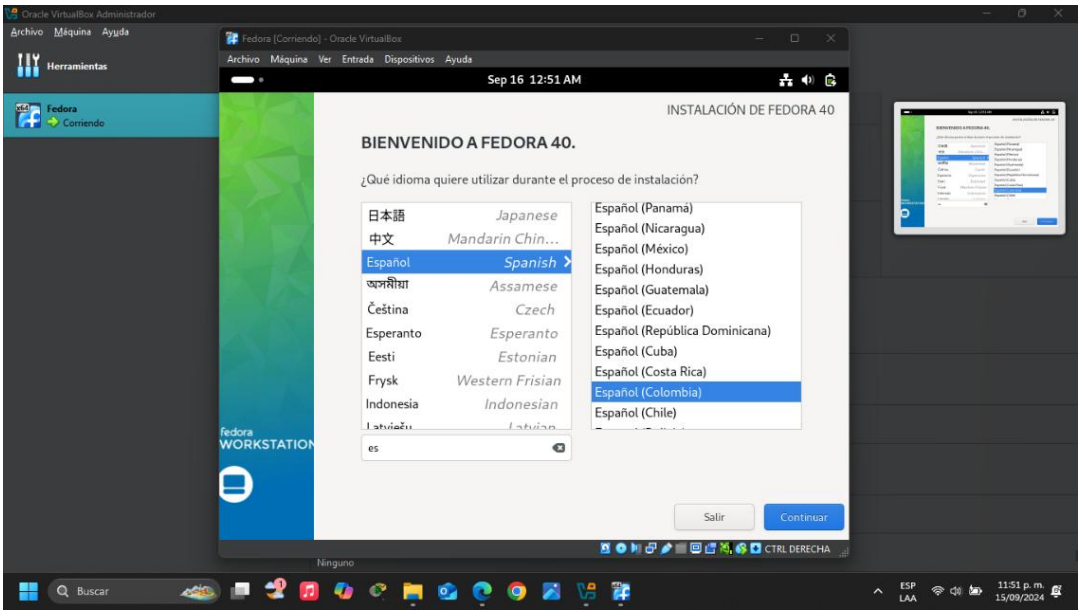
Luego de que eso cargue aparecerá una ventana emergente que da la bienvenida al sistema operativo Fedora, ahí mismo hacer clic en la opción de instalar fedora.

Ilustración 22 Instalación de fedora



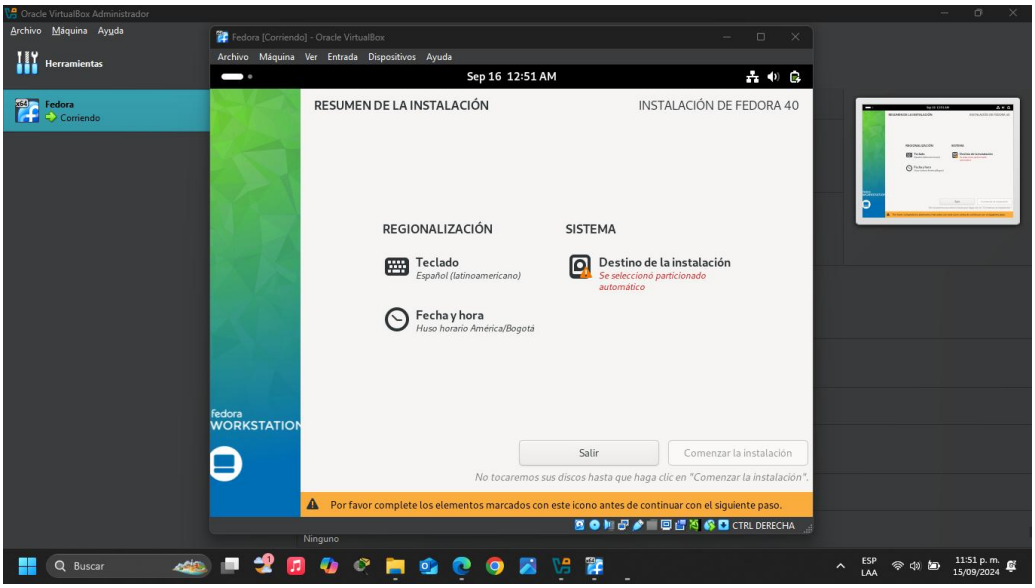
Después de hacer clic en el botón de instalar, el proceso de instalación permite seleccionar el lenguaje que se quiera utilizar durante la instalación.

Ilustración 23 Selección de idioma



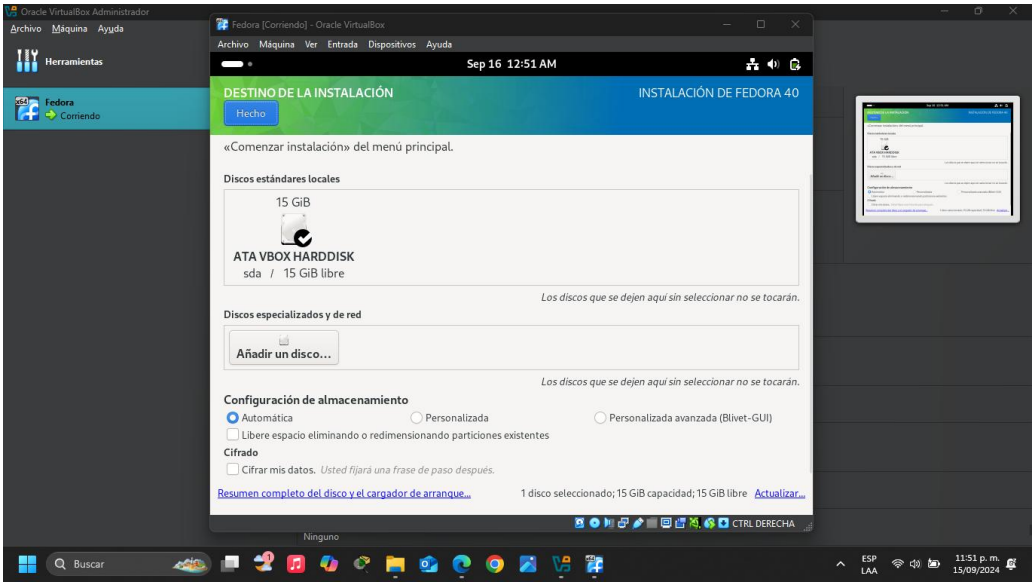
Una vez seleccionado el idioma con el que se desea realizar la instalación aparece un resumen de la instalación, además aparece una advertencia que pide verificar el destino de la instalación.

Ilustración 24 Resumen de instalación



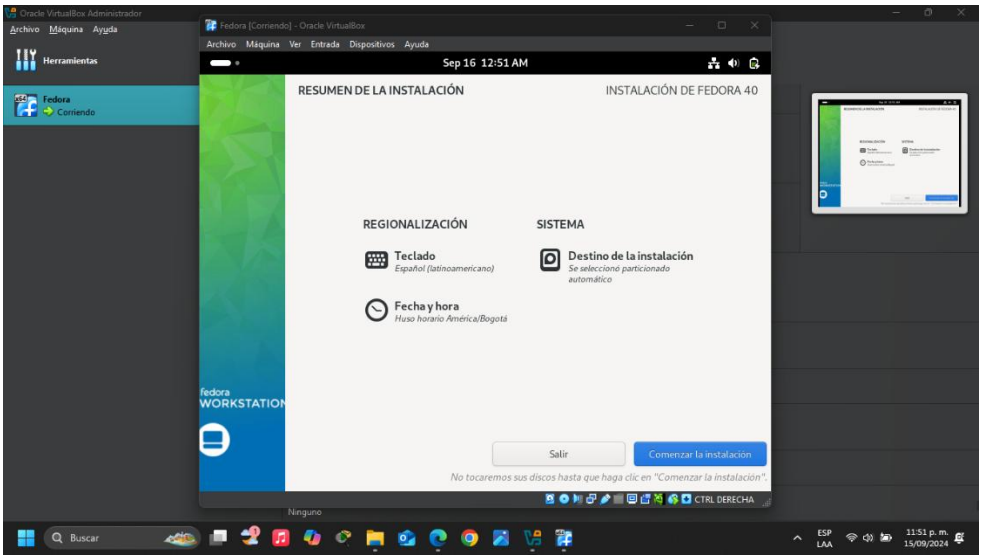
Para verificar el destino de la instalación se hace clic sobre la opción que dice **destino de la instalación**, una vez allí se revisa la información y se hace clic en hecho.

Ilustración 25 Destino de instalación



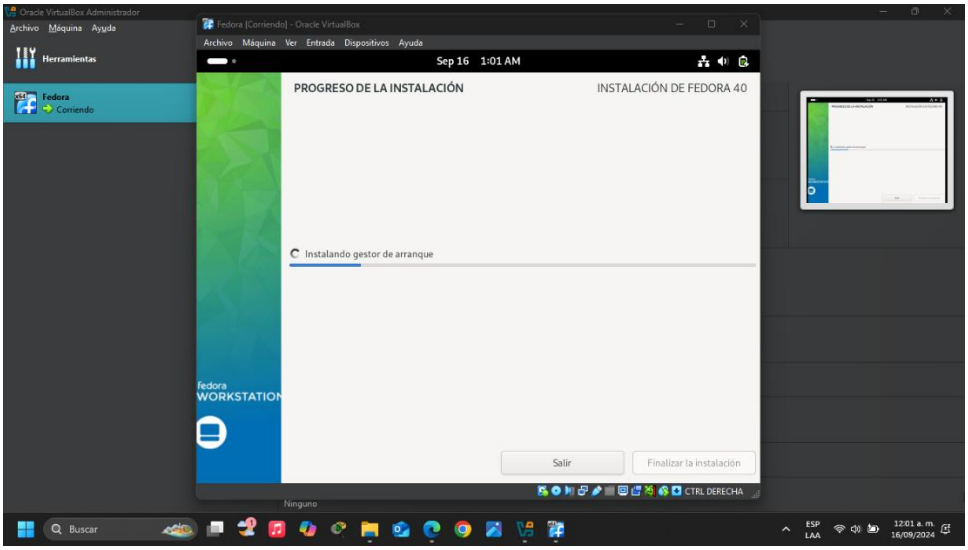
Luego de verificar el destino de la instalación se observa nuevamente la ventana de resumen de instalación y ya no se evidencia la advertencia, por lo que se hace clic en continuar instalación.

Ilustración 26 Resumen de instalación



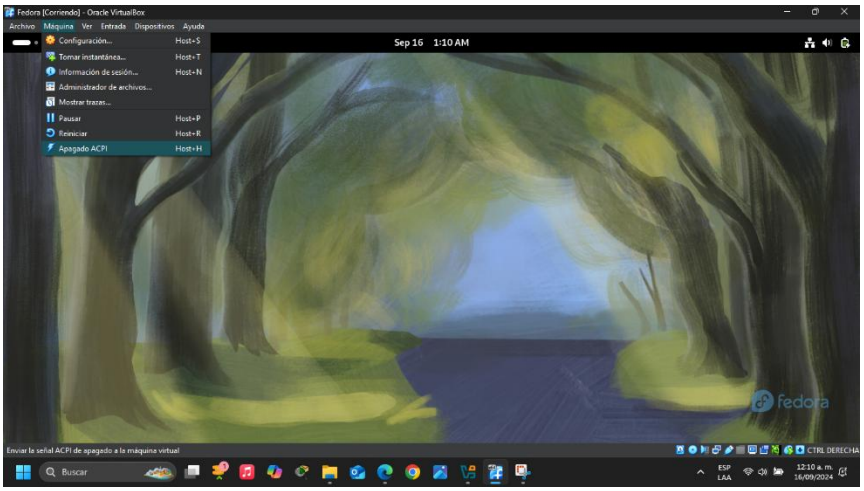
Después de eso el proceso de instalación inicia y solo queda esperar que el proceso finalice.

Ilustración 27 Progreso de instalación



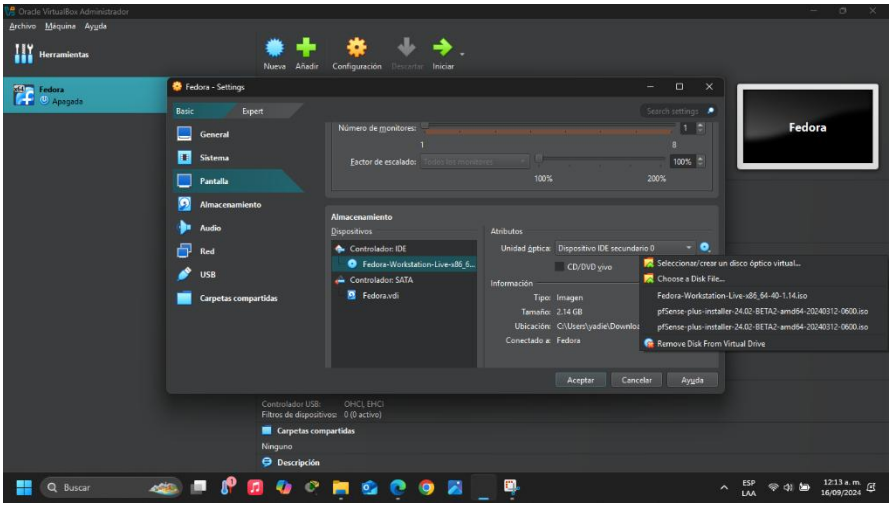
Una vez el proceso finaliza se aparece una interfaz como la que se ve en la siguiente ilustración, eso quiere decir que el sistema está instalado satisfactoriamente. Luego de esto se procede a apagar la máquina virtual debido a que falta un paso.

Ilustración 28 Apagar la máquina virtual



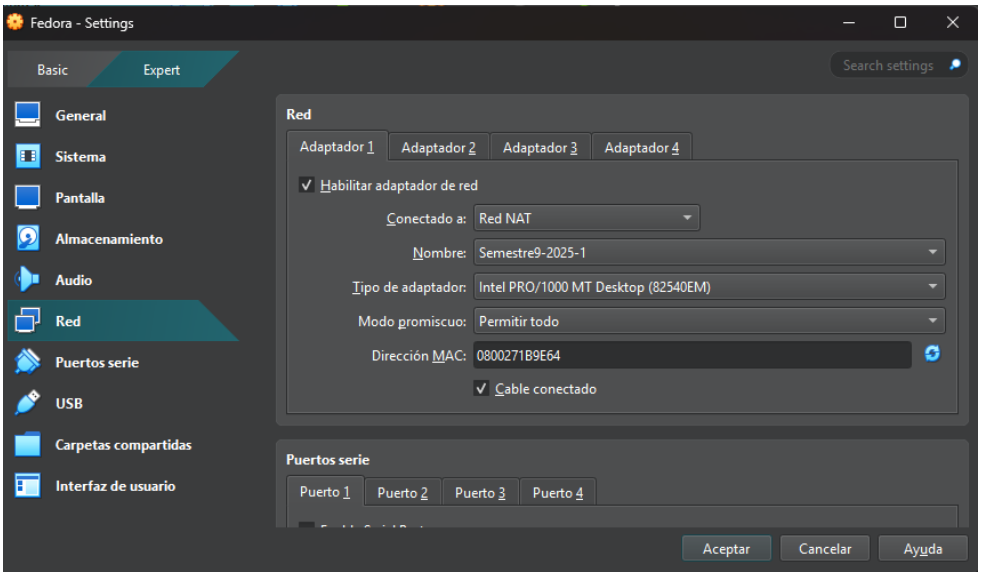
Una vez apagada la máquina virtual, se procede a abrir la configuración de la máquina virtual, exactamente en el apartado de pantalla, se le da en el disco y en la opción de quitar disco virtual, esto lo que hace es remover el Archivo ISO de fedora, esto se hace porque ya el sistema se instaló en nuestro disco local, si el archivo ISO no se retira, cada vez que se inicie la máquina virtual habría que instalar nuevamente el sistema operativo.

Ilustración 29 Remover archivo ISO



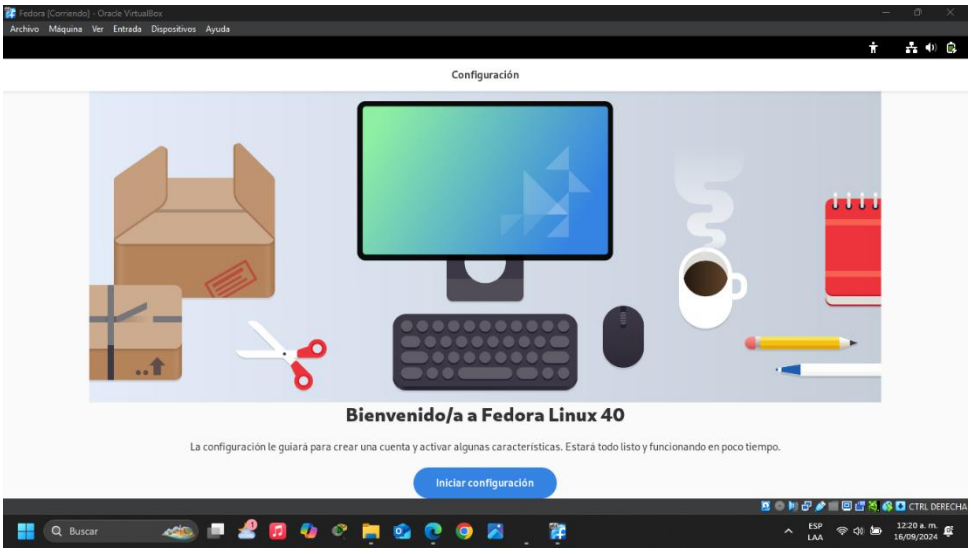
Luego en los ajustes de red se cambia a Red NAT para que quede en la red del ambiente controlado y pueda tener comunicación con las otras máquinas.

Ilustración 30 Cambio a Red NAT



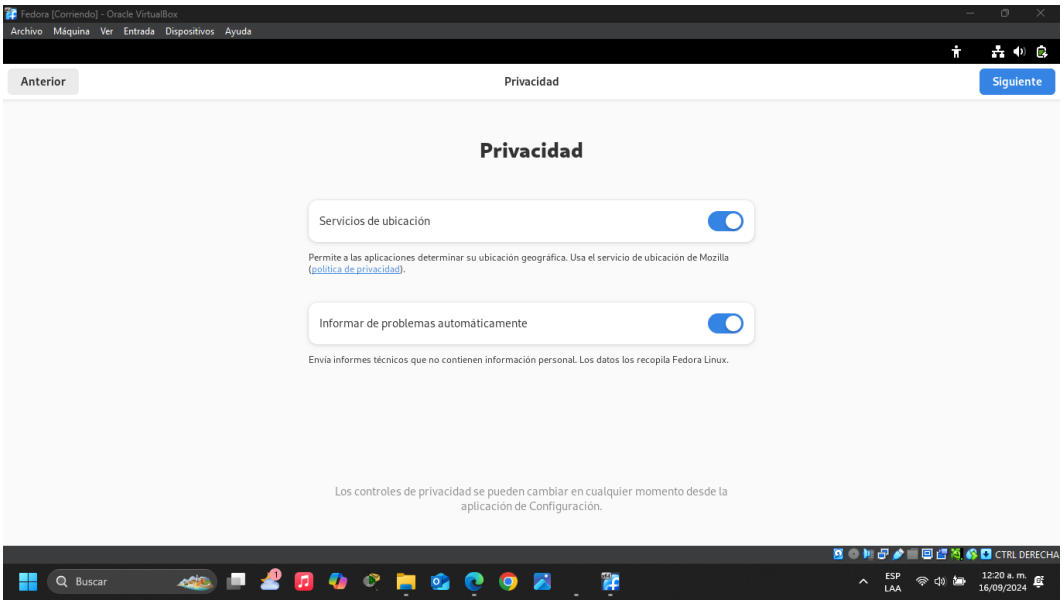
Una vez se remueve el archivo ISO, se inicia nuevamente la máquina virtual y debe aparecer un mensaje de bienvenida al sistema operativo Fedora y una invitación a hacer la configuración inicial como se evidencia en la siguiente ilustración.

Ilustración 31 Configuración inicial



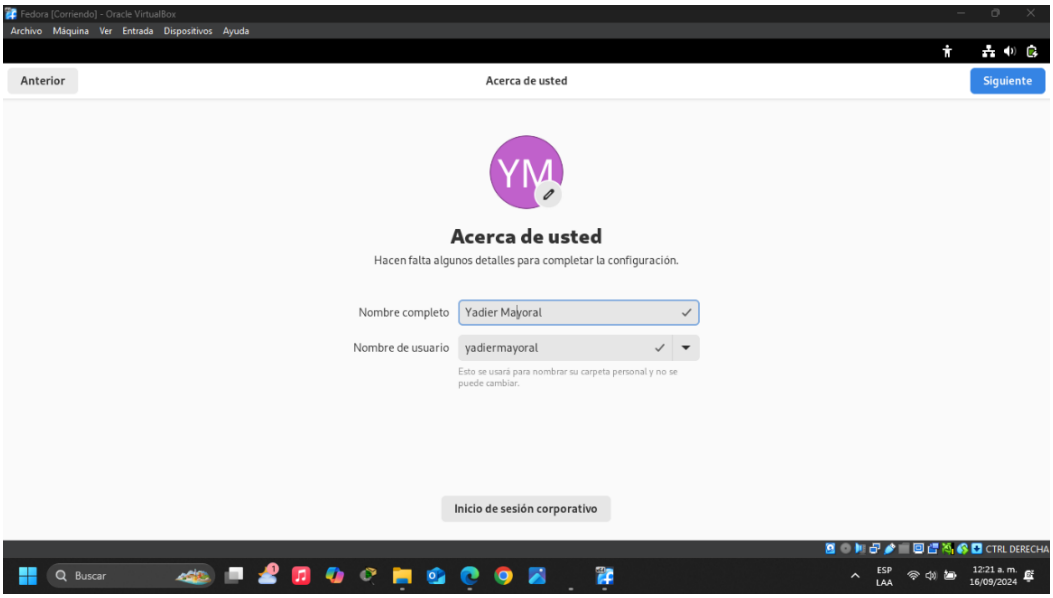
Se aceptan los términos de privacidad.

Ilustración 32 Términos de privacidad



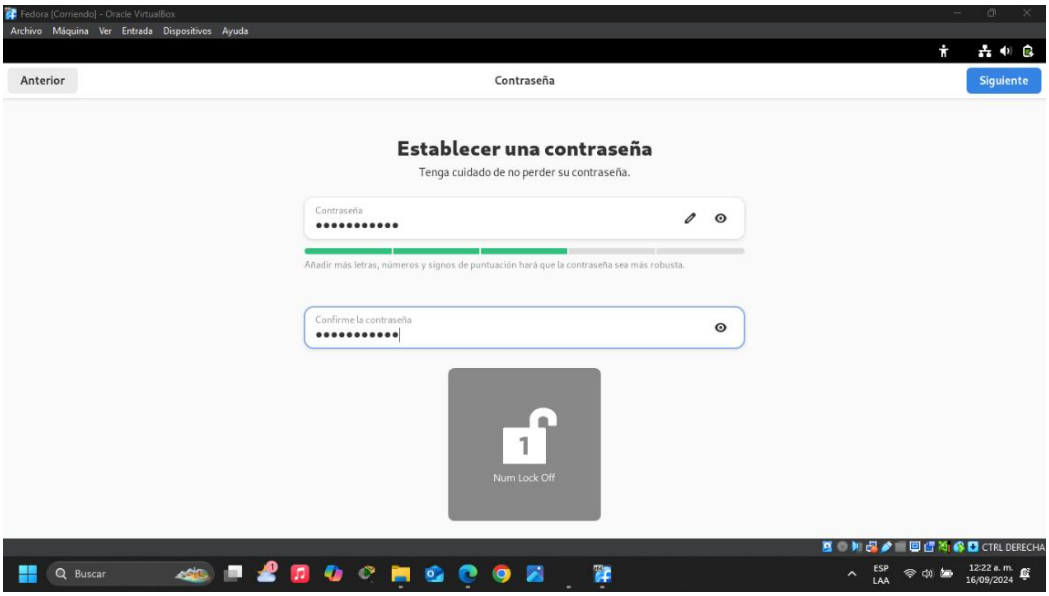
Luego pide información personal, como nombre, apellido y usuario.

Ilustración 33 Información personal



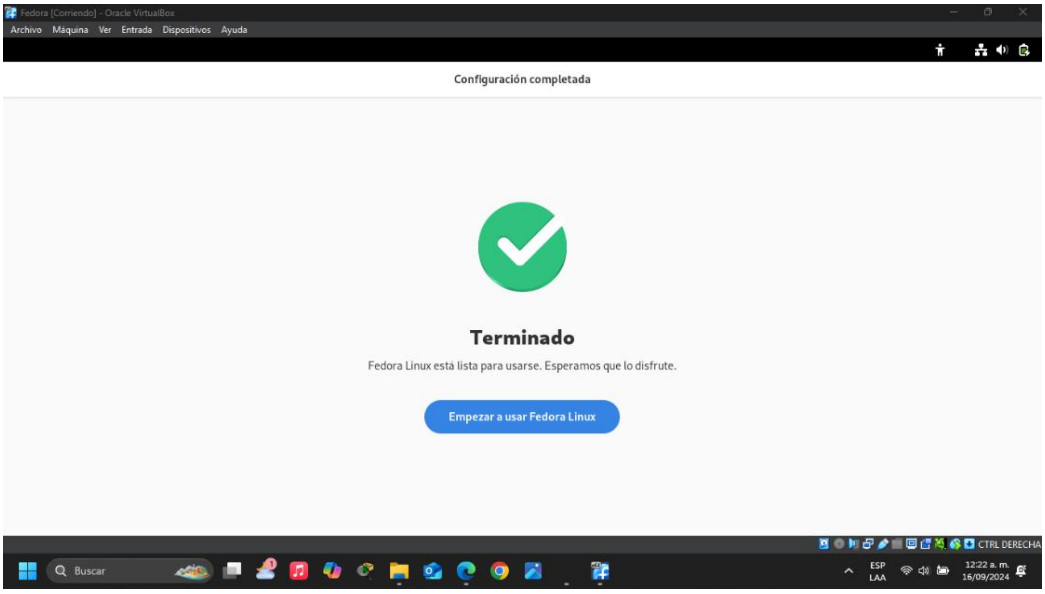
Luego se procede a crear una contraseña.

Ilustración 34 Establecer una contraseña



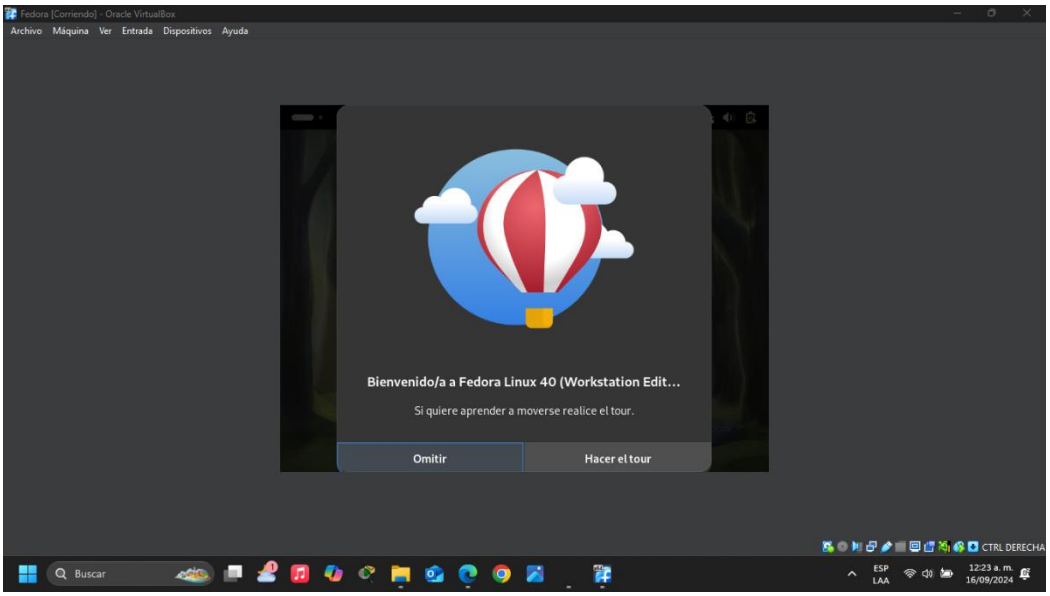
Luego de establecer la contraseña se hace clic en siguiente y aparece una ventana de configuración completada.

Ilustración 35 Configuración terminada



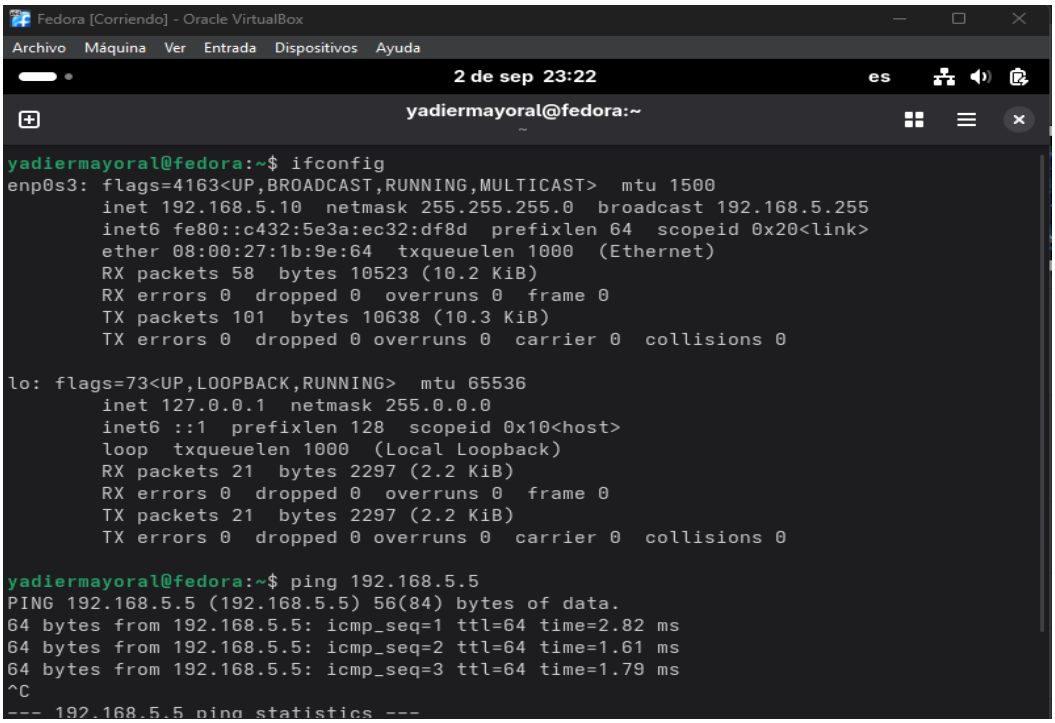
Luego de hacer los tres pasos anteriores la configuración estará terminada y se podrá utilizar Fedora.

Ilustración 36 Primera vez en fedora



Luego de que el Fedora está instalado se verifica que si haya tomado una dirección ip de la red NAT.

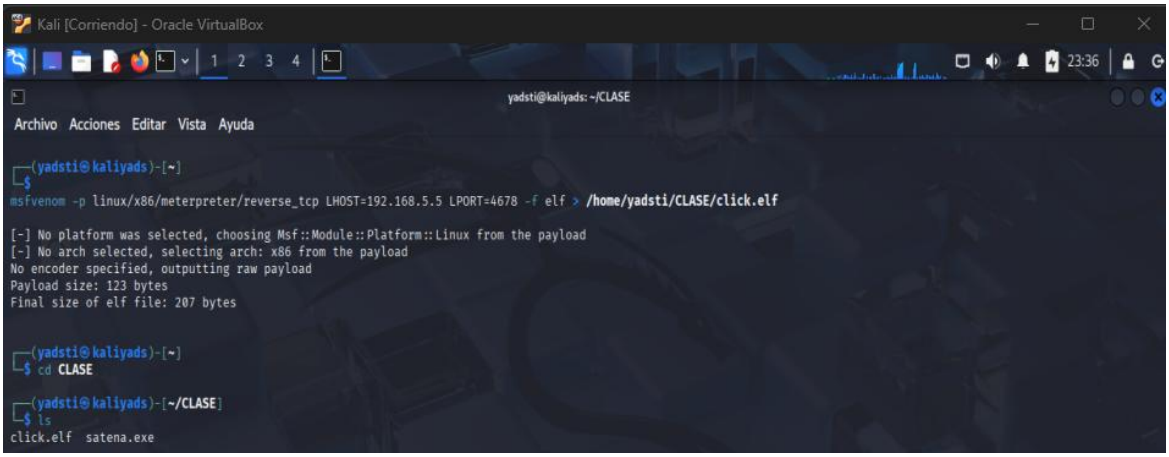
Ilustración 37 Verificación de asignación IP



Ataque a Fedora

Luego de que se crea la máquina virtual de Fedora, desde la máquina de Kali se procede a crear el archivo ejecutable malicioso tipo ejecutable Linux (.elf). En la siguiente ilustración se pueden evidenciar los dos archivos ejecutables maliciosos, uno de Windows y otro de Linux creados.

Ilustración 38 Creación de archivo malicioso Linux



Luego de eso se activa el servicio de Apache1 y se modifica el directorio html del servidor agregando el ejecutable de Linux para que pueda ser descargado.

Ilustración 39 Activación de Apache2

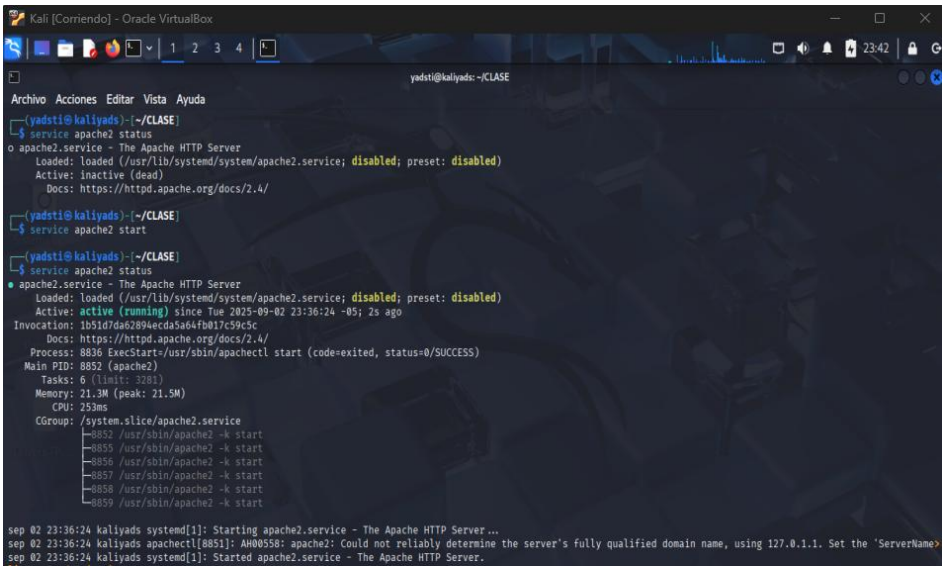
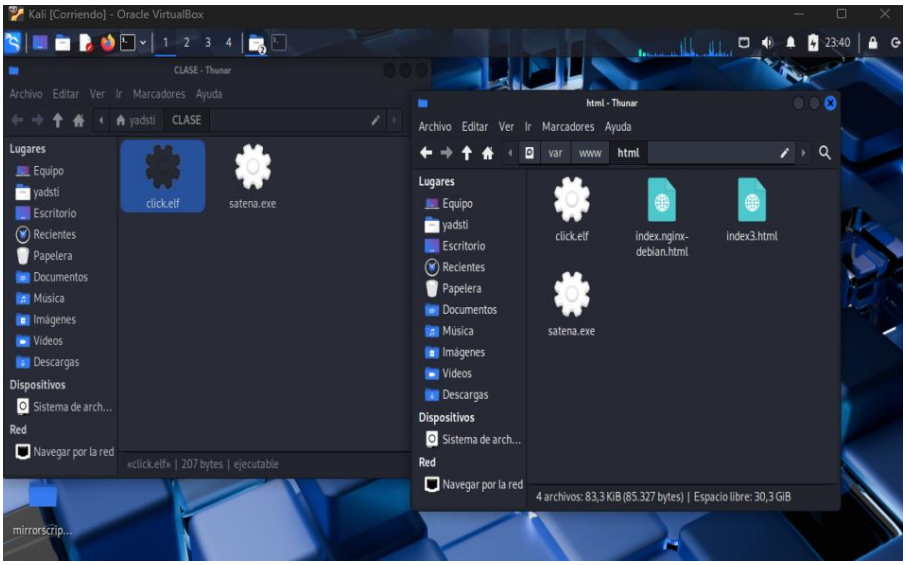
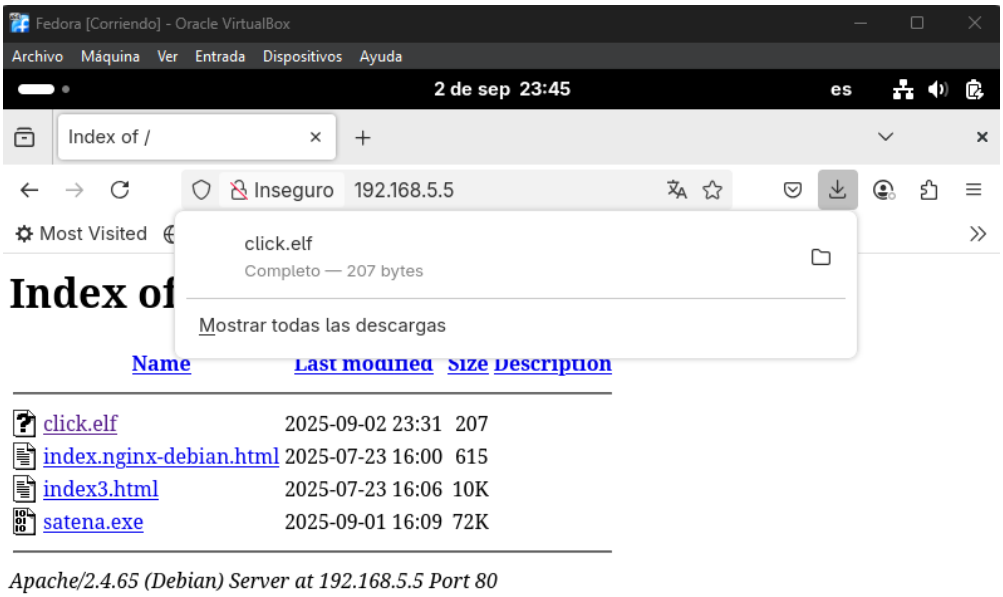


Ilustración 40 Archivo malicioso en apache



Una vez organizado todo, se dirige a la maquina victima al navegador y se pone la dirección ip del servidor apache para proceder con la descarga del ejecutable.

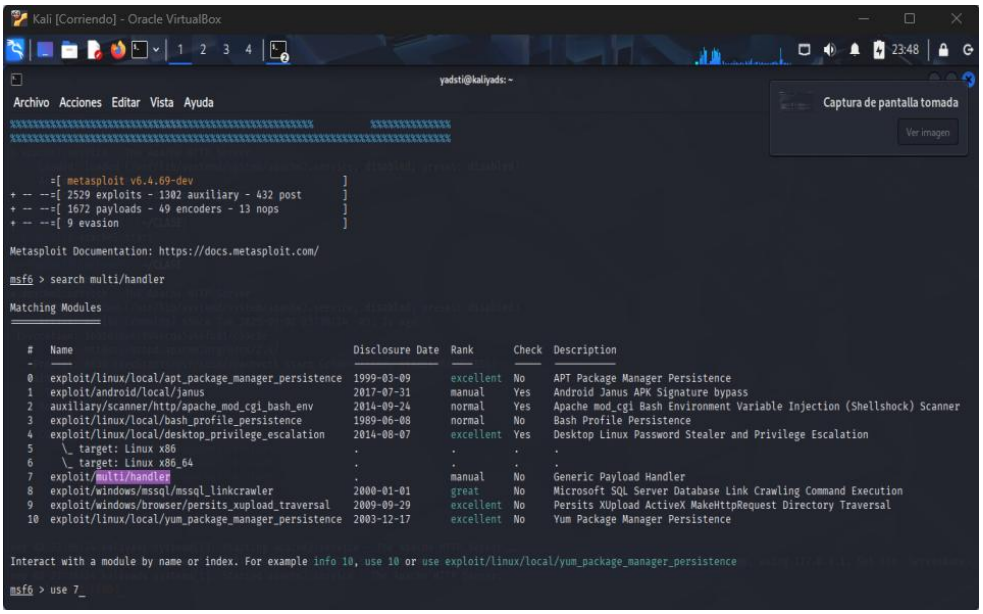
Ilustración 41 Acceso a Apache y descarga ejecutable Linux



Una vez descargado el archivo ejecutable no se ejecuta de una vez, primero hay que ingresar a msfconsole para preparar todo y que se pueda capturar la información y crear la sesión

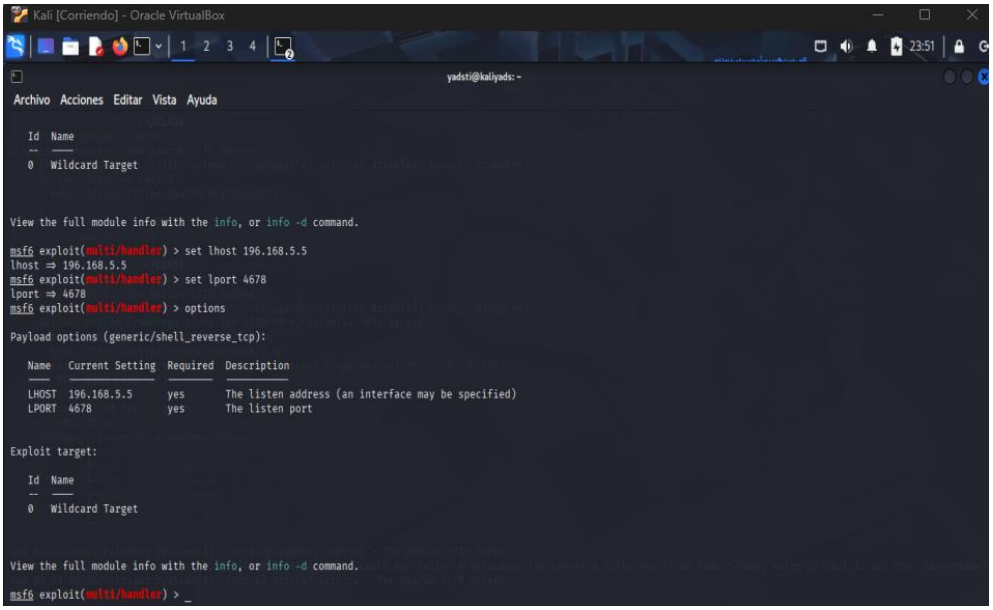
en meterpreter. Una vez se inicie msfconsole se busca multi/handler que es el payload que se va a utilizar para el ataque.

Ilustración 42 Msfconsole - multi/handler



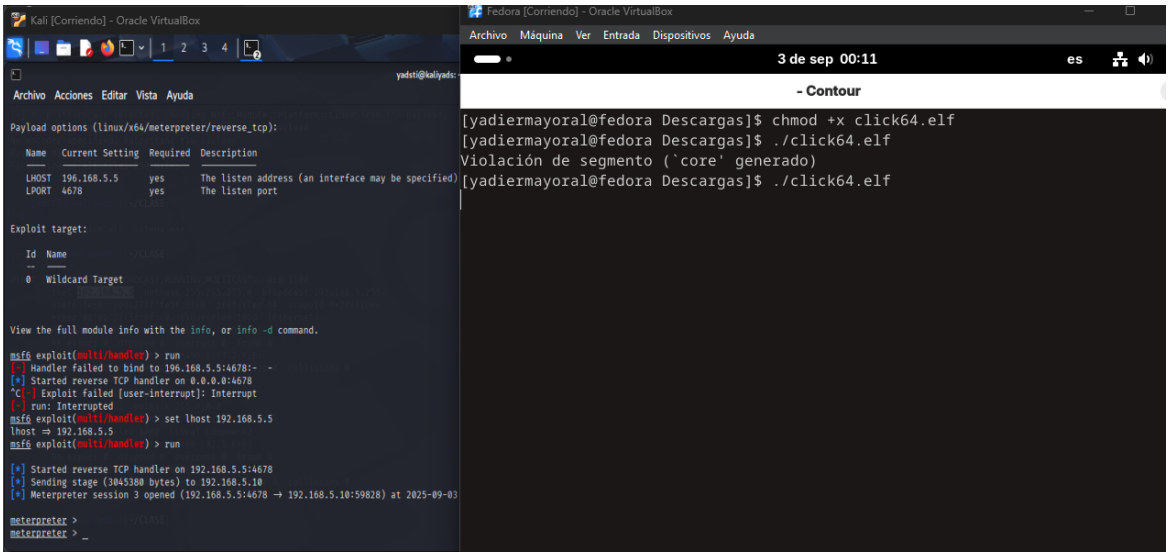
Luego se selecciona el payload se revisa la configuración y se pone el LHOST y LPORT, tal cual como se puso al momento de la creación del ejecutable.

Ilustración 43 Configuración Payload



Una vez se configura el payload se ejecuta el mismo y este queda a espera que en la maquina victima se abra el ejecutable.

Ilustración 44 Exploit fedora



Cómo se puede evidenciar en la ilustración anterior al ejecutar el ejecutable, se obtiene el acceso a meterpreter.

Ilustración 45 Acceso a Fedora

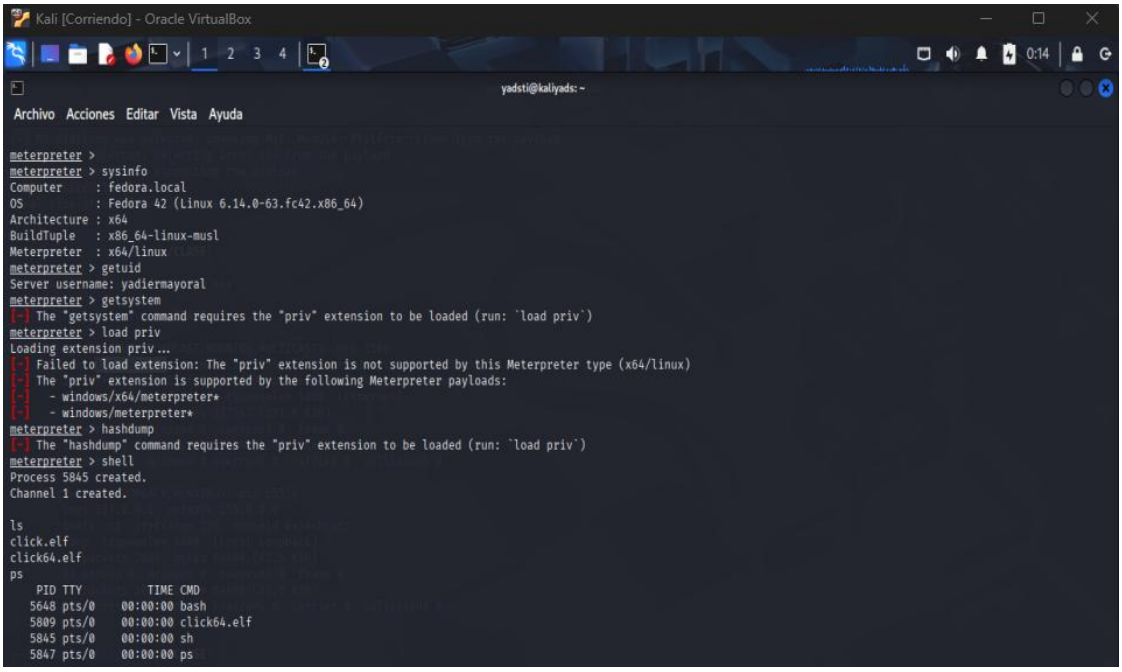


Ilustración 46 Migración fallida

En las ilustraciones se ven algunos errores y es porque no siempre los comandos que funcionan en Windows meterpreter, funcionan en Linux meterpreter, a pesar de que los dos se explotan de formas similares hay comandos diferentes para acceder a la información de cada uno, por ejemplo, en este caso no fue posible migrar el proceso como se hizo con Windows server.

Conclusión

El desarrollo de este laboratorio de seguridad y auditoría de redes permitió simular un entorno real en el que fue posible aplicar técnicas de generación y ejecución de archivos maliciosos, orientados a obtener acceso remoto mediante **Meterpreter**. A través de la implementación de una red NAT y el uso de **Kali Linux** como máquina atacante, se logró comprometer tanto un sistema **Windows** como una distribución de **Linux Fedora**, evidenciando las diferencias en las funcionalidades disponibles para cada plataforma.

En Windows fue posible ejecutar un archivo (.exe) que permitió abrir sesión en Meterpreter con funciones avanzadas, mientras que, en Linux, aunque se consiguió ejecutar un ejecutable (.elf) y establecer la sesión remota, se evidenció la limitación de ciertas funciones como migrate o hashdump, que son propias de entornos Windows.

Con este ejercicio se reafirma la importancia de contar con configuraciones seguras y mantener un control constante sobre las aplicaciones y servicios en los equipos, ya que incluso la simple ejecución de un archivo descargado puede otorgar control al atacante.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes. Quibdó*