

Tutorial BURP SUITE



Ivana Sánchez Pérez

14/07/2025

Índice

Índice	2
1. Introducción	4
1.1. ¿Qué problema resuelve y por qué es importante?	4
1.2. Requisitos e Instalación	4
2. Pasos previos	5
2.1. Instalación de una Máquina Virtual para el entorno de práctica	5
2.1.1. ¿Por qué usar una VM? Aislamiento y seguridad	5
2.1.2. Opciones de software de virtualización (VirtualBox / VMware)	6
2.2. Instalando un Sistema Operativo para Pruebas (ej. Kali Linux)	7
2.2.1. Descargando e instalando Kali Linux en tu VM	7
2.2.2. Actualizando el sistema y dependencias	9
2.3. Comprobación de la configuración de red de la VM	10
2.3.1. Verificando la dirección IP y conectividad a internet	10
3. Instalación de Burp Suite Community Edition	12
3.1. Descarga y Requisitos de Java	12
3.2. Descarga del instalador oficial de Burp Suite Community	13
3.3. Proceso de Instalación Paso a Paso	15
3.3.1. Ejecutando el instalador (Windows, Linux, macOS)	15
3.3.2. Aceptando términos y seleccionando directorio	16
3.3.3. Finalizando la instalación y primer inicio	18
3.4. Lanzamiento inicial de Burp Suite	19
3.4.1: Opciones de proyecto (proyecto temporal vs. proyectos persistentes)	19
3.4.2: Configuración por defecto y la interfaz principal	21
4. Configuración Inicial de Burp Suite	22
4.1. Configurando el Proxy Listener de Burp	22
4.1.1. Verificando el Listener por defecto (127.0.0.1:8080)	22
4.1.2. Ajustes avanzados del Listener (opcional)	23
4.2. Configurando tu Navegador para Burp Proxy	24
4.2.1. Usando el navegador integrado de Burp (opción más sencilla)	24
4.2.2. Configuración manual en Firefox (ejemplo detallado)	25
4.2.3. Instalación del Certificado CA de Burp Suite para HTTPS	27
4.2.4. Importar el certificado a nivel del sistema operativo (para Chrome y otras apps)	29
4.2.5. Configuración de Chrome	31
4.2.6. FUNCIONAMIENTO DE BURP SUITE	34
Sugerencias prácticas	35

4.2.7. Estructura de una solicitud HTTP/S en Burp	36
4. Guía de Uso Básico: Intercepción de Tráfico Web	36
5.1. Preparando un Entorno de Prueba Seguro	36
5.1.1. Introducción a laboratorios de práctica	36
5.1.2. Consideraciones de seguridad: ¡Nunca pruebes en sitios reales sin permiso!	38
5.2. Pasos del Caso Práctico: Modificando un Login Simple	38
5.2.1. Reenviando la solicitud modificada ("Forward")	42
5.3. Explorando el Historial HTTP	43
5.3.1. Revisando solicitudes y respuestas pasadas en "HTTP history"	43
5.3.2. Filtrando y buscando en el historial	44
5. Herramientas Fundamentales de Burp Suite	45
6.1. Burp Repeater: Modificando y Reenviando Solicitudes Manualmente	45
6.1.1. ¿Para qué sirve Repeater?	45
6.1.2. Cómo enviar una solicitud a Repeater	45
6.1.3. Usando Repeater: Modificar y Enviar	46
6.2. Burp Intruder: Automatizando Ataques Personalizados (con limitaciones en Community Edition)	47
6.2.1. ¿Para qué sirve Intruder?	47
6.2.2. Cómo enviar una solicitud a Intruder	47
6.2.3. Usando Intruder: Posiciones, Payloads y Tipos de Ataque	48
6.3. Otras Herramientas de Burp Suite (Mención)	51
7. Anexo 1: Solución de Problemas Comunes	52
7.1. El navegador no se conecta al proxy de Burp	52
7.2. Errores de certificado HTTPS	54
7.3. Burp Suite no inicia o da errores de Java	55
8. Consejos Adicionales para Tu Trayectoria con Burp Suite	56
Caido: Un Nuevo Contendiente	57
Tabla de ventajas y desventajas: Caído vs Burp Suite	58

1. Introducción

Burp Suite es un conjunto de herramientas integradas para realizar pruebas de seguridad en aplicaciones web (web penetration testing). Desarrollado por PortSwigger, se trata de una herramienta indispensable para pentesters, bug hunters y desarrolladores que buscan asegurar sus aplicaciones.

De una forma resumida, podemos decir que Burp Suite se trata de un proxy desarrollado con java que busca vulnerabilidades en aplicaciones web.

Existen dos versiones principales:

- **Community Edition:** Gratuita, ofrece funcionalidades básicas pero muy útiles. Es la versión en la que se centrará este tutorial.
- **Professional Edition:** De pago, con funciones avanzadas como escaneo automático de vulnerabilidades y más herramientas.

Un esquema resumen muy completo lo ha realizado Miguel Angel y está disponible aquí:

<https://www.mindomo.com/mindmap/6882c4ba1abf40679ac85877f3b83304>

1.1. ¿Qué problema resuelve y por qué es importante?

Las aplicaciones web son un objetivo común para los atacantes. Burp Suite ayuda a los profesionales de la seguridad a encontrar vulnerabilidades (como inyección SQL, XSS, autenticación rota, etc.) antes de que los atacantes lo hagan. Su importancia radica en que actúa como un intermediario (proxy), permitiendo interceptar, inspeccionar y modificar el tráfico HTTP/S entre el navegador y el servidor, lo que facilita el control y la manipulación de las solicitudes y respuestas de la web.

1.2. Requisitos e Instalación

Para asegurar un funcionamiento óptimo de Burp Suite, hay que tener en cuenta los siguientes requisitos y las recomendaciones para el entorno de práctica.

Requisitos de Hardware y Software

- **Sistema Operativo:**
 - Windows (7 o posterior, 64-bit recomendado)
 - macOS

- Linux (especialmente **Kali Linux**, a menudo preinstalado o de fácil instalación)
- **RAM:** Mínimo 4 GB (8 GB o más recomendado para un mejor rendimiento).
- **Espacio en disco:** Al menos 1 GB de espacio libre.
- **Java:** Burp Suite requiere Java Runtime Environment (JRE) versión 11 o superior. Asegúrate de tenerlo instalado y configurado correctamente.
- **Navegador Web:** Un navegador moderno (Firefox o Chrome son los más recomendados para configurar el proxy).

2. Pasos previos

Antes de sumergirnos en la instalación y configuración de Burp Suite, es fundamental preparar un entorno seguro y controlado. Trabajar con herramientas de ciberseguridad, incluso en un contexto de aprendizaje, requiere precauciones. Las Máquinas Virtuales son la solución ideal para este propósito, ya que nos permiten crear un laboratorio aislado sin afectar nuestro sistema operativo.

2.1. Instalación de una Máquina Virtual para el entorno de práctica

2.1.1. ¿Por qué usar una VM? Aislamiento y seguridad

Utilizar una máquina virtual para tus prácticas con Burp Suite ofrece ventajas significativas:

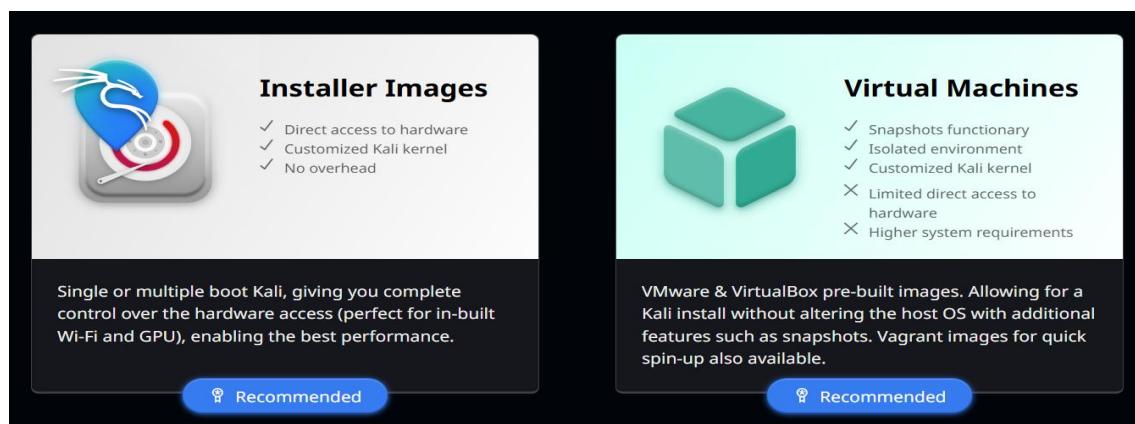
- **Aislamiento:** La VM funciona como un ordenador independiente dentro de tu sistema anfitrión (host). Esto significa que cualquier software malicioso o configuración errónea que puedas encontrar o aplicar durante tus pruebas se contendrá dentro de la VM, sin afectar tu sistema operativo principal.
- **Seguridad:** Al trabajar con herramientas de seguridad y, potencialmente, interactuar con aplicaciones web vulnerables, el riesgo de comprometer tu sistema es real. Las VMs mitigan este riesgo al proporcionar un entorno descartable que puedes restablecer fácilmente a un estado anterior si algo sale mal.
- **Flexibilidad:** Puedes crear múltiples VMs con diferentes sistemas operativos y configuraciones, adaptándote a las necesidades específicas de cada prueba o laboratorio.
- **Facilidad de recuperación:** Las VMs permiten tomar "snapshots" (instantáneas) de su estado. Si en algún momento estropeas la configuración o el sistema, puedes revertir a una instantánea anterior en cuestión de segundos.

2.1.2. Opciones de software de virtualización (VirtualBox / VMware)

Existen varias plataformas de virtualización populares que puedes utilizar para crear tus máquinas virtuales. Nos centraremos en dos de las más utilizadas en entornos de ciberseguridad:

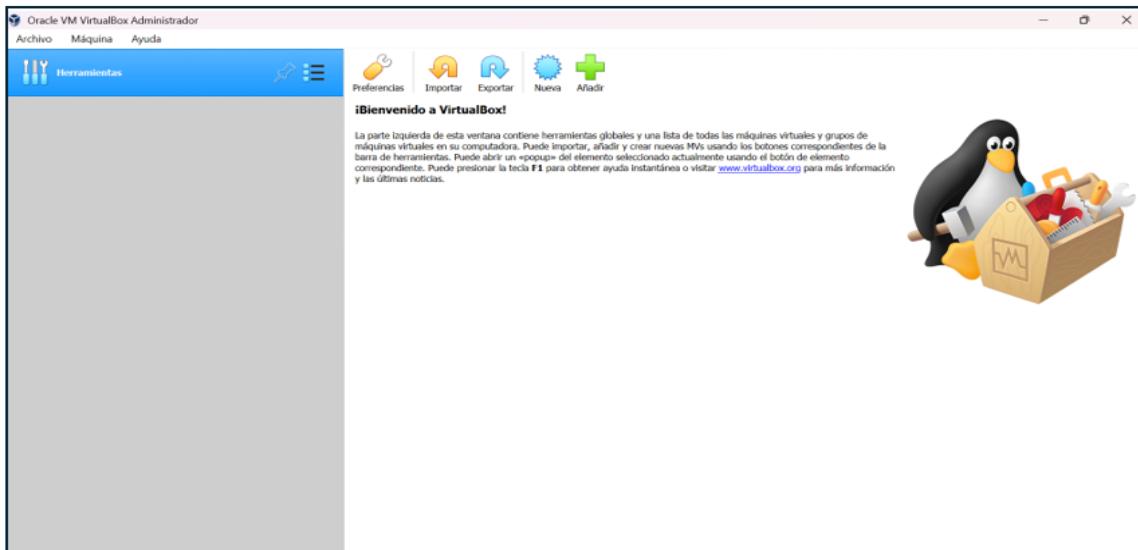
- **Oracle VM VirtualBox: La versión 6.1 o la 7.0**
 - **Ventajas:** Es completamente gratuito y de código abierto, lo que lo hace accesible para todos. Es multiplataforma, disponible para Windows, macOS y Linux. Es muy popular y cuenta con una gran comunidad, lo que facilita encontrar soporte y tutoriales.
 - **Descarga:** Puedes descargarlo desde la página oficial: <https://www.virtualbox.org/wiki/Downloads>
 - **Instalación:** El proceso de instalación es similar al de cualquier otro software en tu sistema operativo principal. Simplemente descarga el instalador y sigue los pasos del asistente.
- **VMware Workstation Player (Gratis para uso no comercial) / Workstation Pro (De pago):**
 - **Ventajas:** Ofrece un rendimiento generalmente superior y características más avanzadas que VirtualBox, especialmente para entornos más complejos o profesionales. VMware Player es gratuito para uso personal.
 - **Descarga:** Puedes descargar VMware Workstation Player desde la página oficial: <https://www.vmware.com/es/products/workstation-player/workstation-player-evaluation.html>
 - **Instalación:** Al igual que VirtualBox, descarga el instalador y sigue el asistente de instalación.

Algunas comparaciones que puedes tener en cuenta:



Live Boot	WSL
 <ul style="list-style-type: none"> ✓ Un-altered host system ✓ Direct access to hardware ✓ Customized Kali kernel ✗ Performance decrease when heavy I/O <p>Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.</p>	 <ul style="list-style-type: none"> ✓ Access to the Kali toolset through the WSL framework ✗ Userland actions only ✗ Not Kali customized kernel ✗ No direct access to hardware <p>Windows Subsystem for Linux (WSL) is included out of the box with modern Windows. Use Kali (and Win-KeX) without installing additional software.</p>

Recomendación: Para empezar, **VirtualBox** es una excelente opción debido a su coste (gratuito) y su curva de aprendizaje amigable.



2.2. Instalando un Sistema Operativo para Pruebas (ej. Kali Linux)

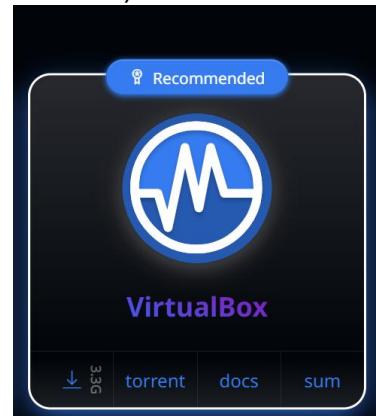
Para este tutorial, utilizaremos **Kali Linux** como nuestro sistema operativo de pruebas. Kali es una distribución de Linux basada en Debian, diseñada específicamente para pruebas de penetración y auditoría de seguridad, y viene con muchas herramientas preinstaladas, incluyendo Burp Suite.

2.2.1. Descargando e instalando Kali Linux en tu VM

1. Descargar la Imagen ISO o la Ova de Kali Linux:

- Ve a la página oficial de descargas de Kali Linux: <https://www.kali.org/get-kali/>

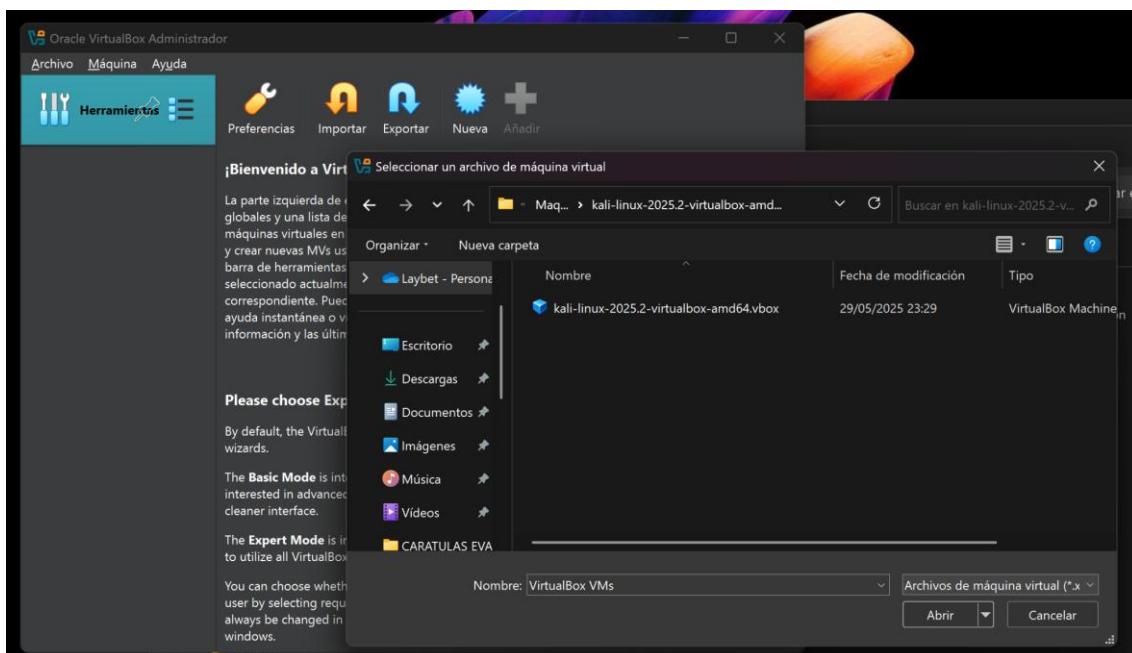
- Busca la sección "Virtual Machines" y descarga la imagen preconstruida para tu software de virtualización (VirtualBox o VMware). Esta opción es la más sencilla, ya que la VM ya viene preconfigurada. Si prefieres instalarlo desde cero, descarga la imagen "**Installer**".
- Recomendación: Para principiantes, la imagen preconstruida (VMware o VirtualBox image) es la opción más rápida y sencilla. Descárgala y, una vez descomprimida, simplemente impórtala en tu software de virtualización (en VirtualBox, **Archivo > Importar Servicio Virtualizado**).



La documentación ampliada la puedes conseguir en este enlace [doc](#)

2. Instalar/Importar Kali Linux en la VM:

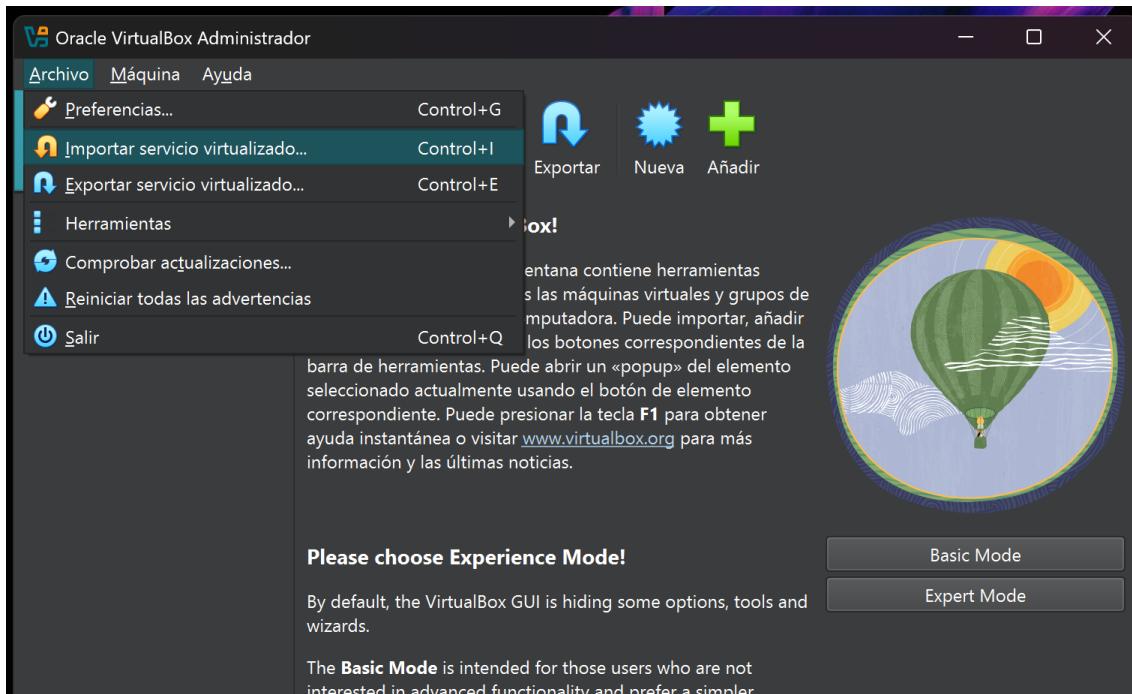
- Añadir



- Si descargaste una imagen preconstruida (OVF/OVA):

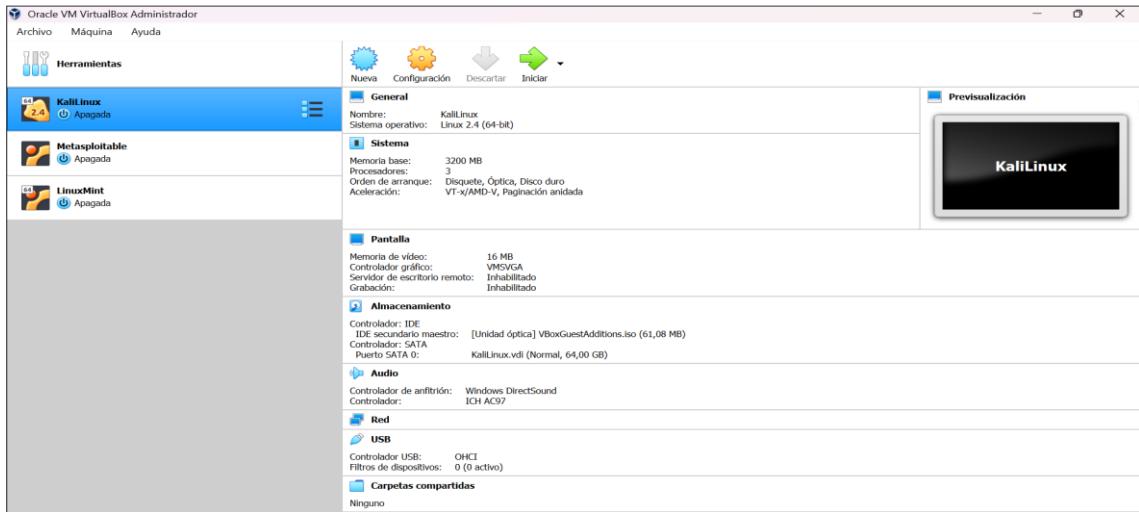
- Abre VirtualBox o VMware.
- Ve a **Archivo -> Importar Servicio Virtualizado...** (o similar).

- Navega hasta el archivo .ova o .ovf que descomprimimos y seleccionalo.
- Sigue al asistente, aceptando las configuraciones predeterminadas (puedes ajustar la RAM o CPUs si lo deseas) y haz clic en "**Importar**".



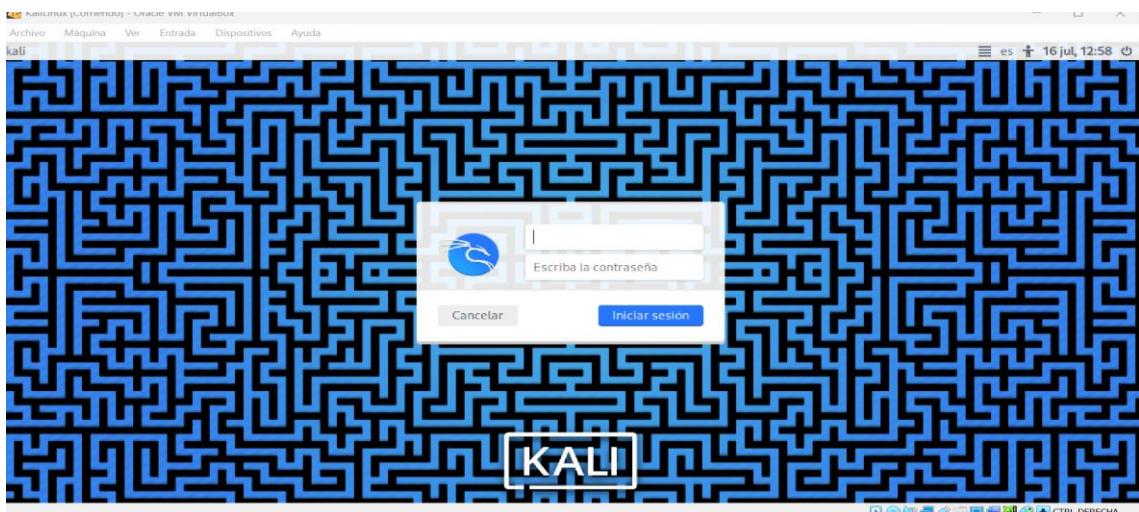
- **Si descargaste la imagen ISO (instalación desde cero):**

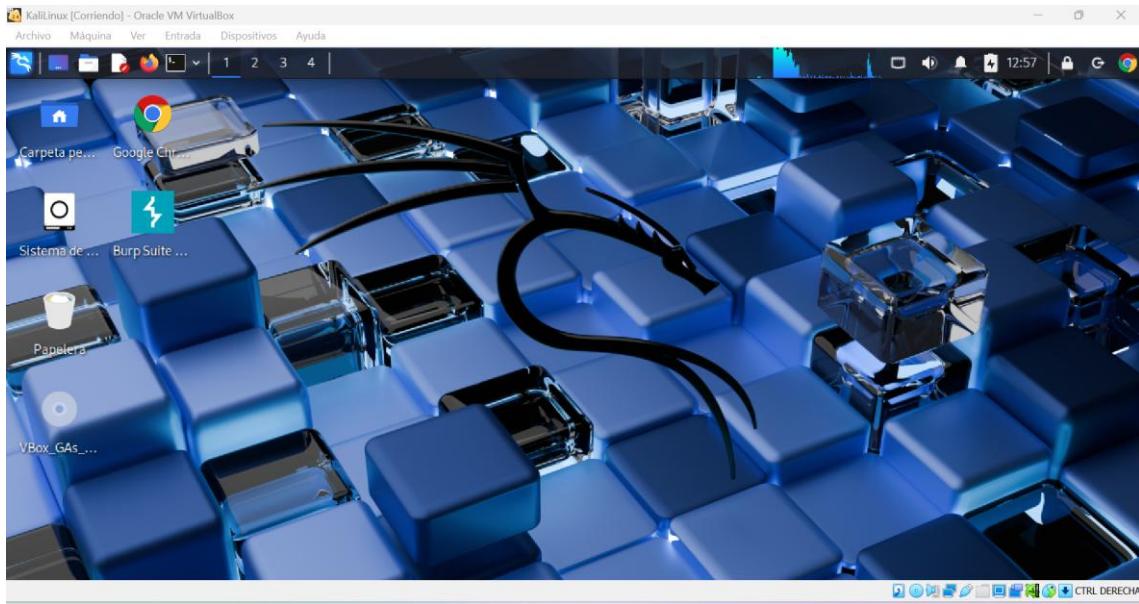
- Una vez creada la VM vacía (como se explica en 0.1.3), selecciona tu VM en el software de virtualización.
- Ve a la configuración de la VM (Configuración en VirtualBox, VM Settings en VMware).
- En la sección de Almacenamiento (VirtualBox) o CD/DVD (VMware), monta la imagen ISO de Kali Linux como si fuera un disco de instalación.
- Inicia la VM y sigue el proceso de instalación de Kali Linux, que es similar al de cualquier sistema operativo: selecciona idioma, ubicación, teclado, crea un usuario y contraseña, particiona el disco (puedes elegir "Guided - Use entire disk") e instala el software.
- En la configuración de red he seleccionado "Adaptador Puente", pues considero que es la mejor opción, al conectarse a mi red real como un dispositivo más.



3. Credenciales por defecto de Kali Linux (si usas la imagen preconstruida):

- **Usuario:** kali
- **Contraseña:** kali
- **Nota:** Se recomienda cambiar la contraseña por defecto después de la primera sesión para mejorar la seguridad.



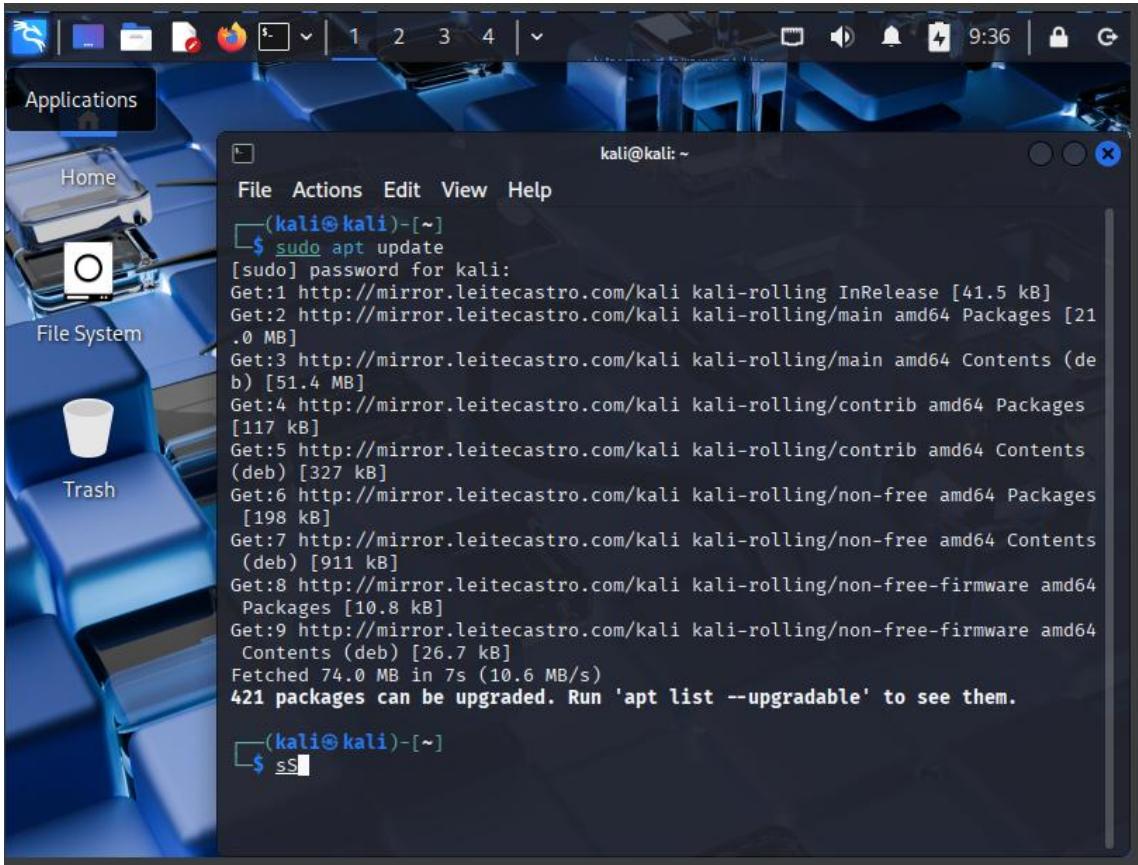


2.2.2. Actualizando el sistema y dependencias

Una vez que Kali Linux esté instalado y funcionando, es crucial actualizarlo para asegurarte de tener las últimas versiones de software y parches de seguridad.

- 1. Abrir una Terminal:** Inicia Kali Linux y abre una terminal (el icono de la pantalla negra).
- 2. Actualizar el Índice de Paquetes:** Ejecuta el siguiente comando para actualizar la lista de paquetes disponibles en los repositorios de Kali:

```
sudo apt update
```



A screenshot of a Kali Linux desktop environment. On the left, there's a dock with icons for Home, File System, and Trash. A terminal window is open in the center, showing the command `sudo apt update` being run. The output of the command is displayed, showing package downloads from a mirror. The terminal window title bar says "kali@kali: ~". The status bar at the top shows the date and time as 9:36.

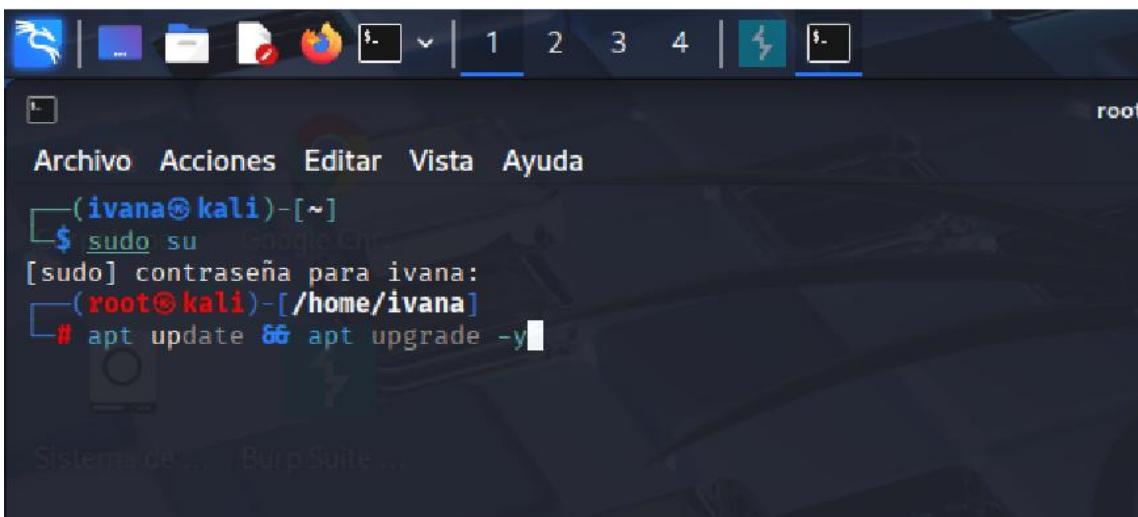
```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://mirror.leitecastro.com/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.leitecastro.com/kali kali-rolling/main amd64 Packages [21
.0 MB]
Get:3 http://mirror.leitecastro.com/kali kali-rolling/main amd64 Contents (de
b) [51.4 MB]
Get:4 http://mirror.leitecastro.com/kali kali-rolling/contrib amd64 Packages
[117 kB]
Get:5 http://mirror.leitecastro.com/kali kali-rolling/contrib amd64 Contents
(deb) [327 kB]
Get:6 http://mirror.leitecastro.com/kali kali-rolling/non-free amd64 Packages
[198 kB]
Get:7 http://mirror.leitecastro.com/kali kali-rolling/non-free amd64 Contents
(deb) [911 kB]
Get:8 http://mirror.leitecastro.com/kali kali-rolling/non-free-firmware amd64
Packages [10.8 kB]
Get:9 http://mirror.leitecastro.com/kali kali-rolling/non-free-firmware amd64
Contents (deb) [26.7 kB]
Fetched 74.0 MB in 7s (10.6 MB/s)
421 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ ss
```

sud

3. Actualizar los Paquetes Instalados: Despues de actualizar el índice, actualiza todos los paquetes instalados a sus últimas versiones:

`sudo apt upgrade -y` (El -y al final acepta automáticamente cualquier pregunta de confirmación).



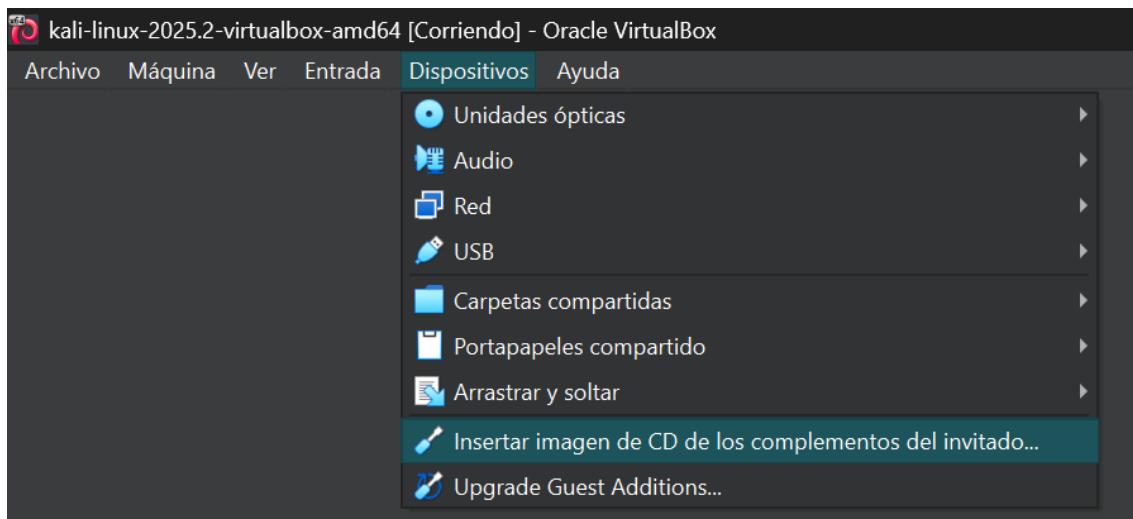
A screenshot of a Kali Linux desktop environment. A terminal window is open, showing the user switching to root using `sudo su`. The terminal title bar shows "root". The user then runs the command `apt update & apt upgrade -y`. The status bar at the top shows the date and time as 9:36.

```
Archivo Acciones Editar Vista Ayuda
(ivana㉿kali)-[~]
$ sudo su
[sudo] contraseña para ivana:
(root㉿kali)-[/home/ivana]
# apt update & apt upgrade -y
```

Reiniciar la VM (si es necesario): Después de una actualización importante, especialmente si se actualiza el kernel, es buena práctica reiniciar la VM:

```
sudo reboot
```

4. Guest Additions de Virtualbox



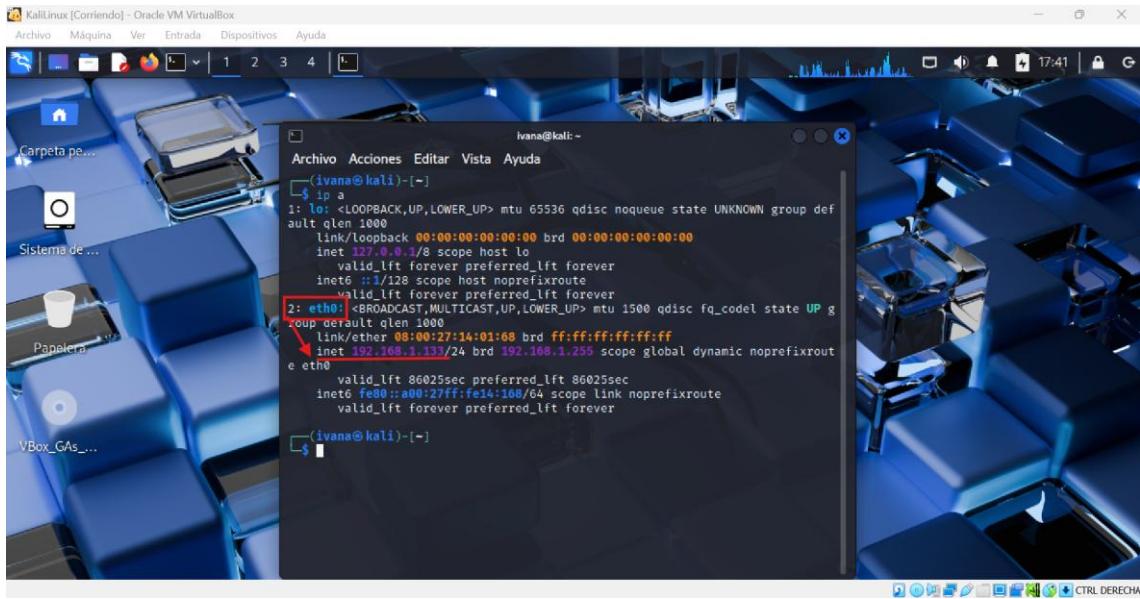
2.3. Comprobación de la configuración de red de la VM

La conectividad de red es fundamental para que Burp Suite pueda interactuar con aplicaciones web. Necesitas asegurarte de que tu VM tenga acceso a internet y, si vas a montar laboratorios internos, que pueda comunicarse con otras VMs o aplicaciones en tu red de prueba.

2.3.1. Verificando la dirección IP y conectividad a internet

1. Verificar la dirección IP de la VM:

- Abre una terminal en Kali Linux. Y ejecuta el comando: **ip a**
- Busca la interfaz de red (generalmente eth0 o enp0s3)



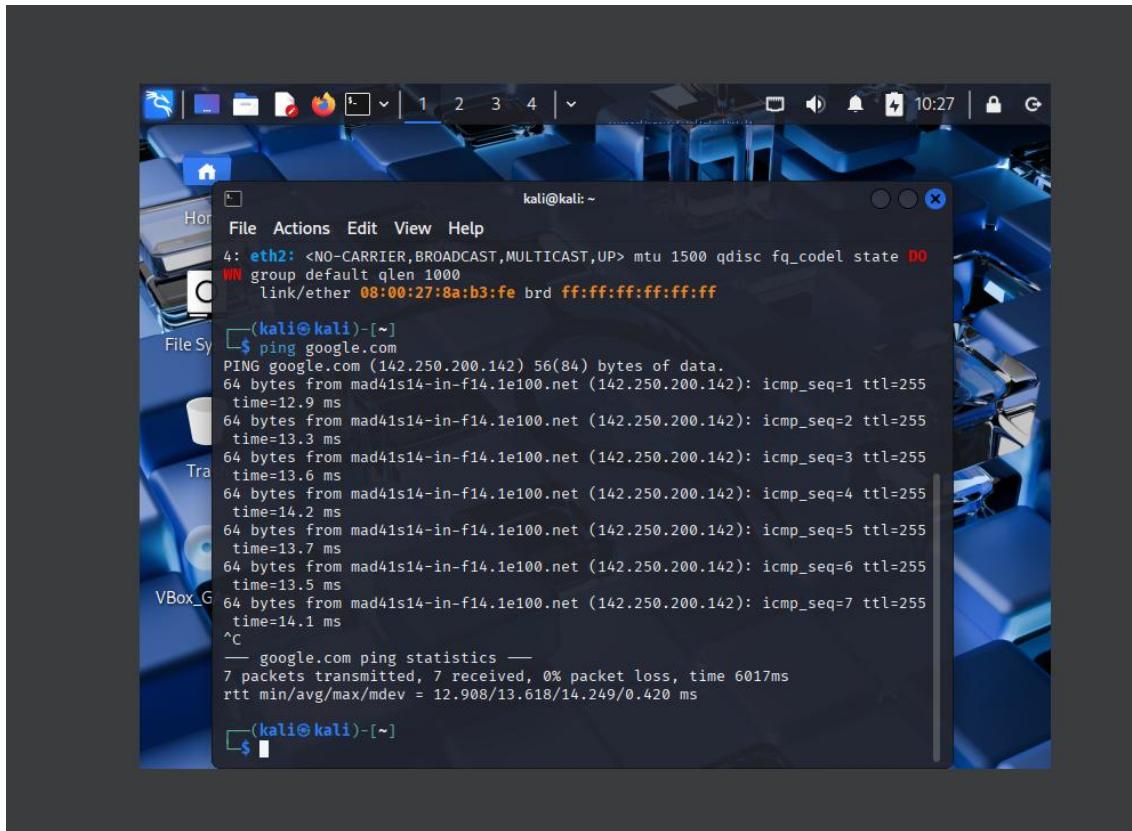
2. Comprobar la conectividad a internet:

- En la misma terminal, intenta hacer un ping a un sitio web conocido:

ping google.com

```
(ivana㉿kali)-[~]
$ ping google.com
PING google.com (142.250.200.78) 56(84) bytes of data.
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=1 ttl=118
time=17.3 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=2 ttl=118
time=16.8 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=3 ttl=118
time=17.9 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=4 ttl=118
time=18.7 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=5 ttl=118
time=21.5 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=6 ttl=118
time=18.1 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=7 ttl=118
time=16.1 ms
^C
— google.com ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6110ms
rtt min/avg/max/mdev = 16.061/18.050/21.467/1.609 ms

(ivana㉿kali)-[~]
```



3. Instalación de Burp Suite Community Edition

Ahora que tienes tu entorno de máquina virtual preparado y actualizado, es el momento de instalar la herramienta principal de este tutorial: **Burp Suite Community Edition**. Esta es la versión gratuita que te permitirá aprender y practicar las bases del pentesting web.

3.1. Descarga y Requisitos de Java

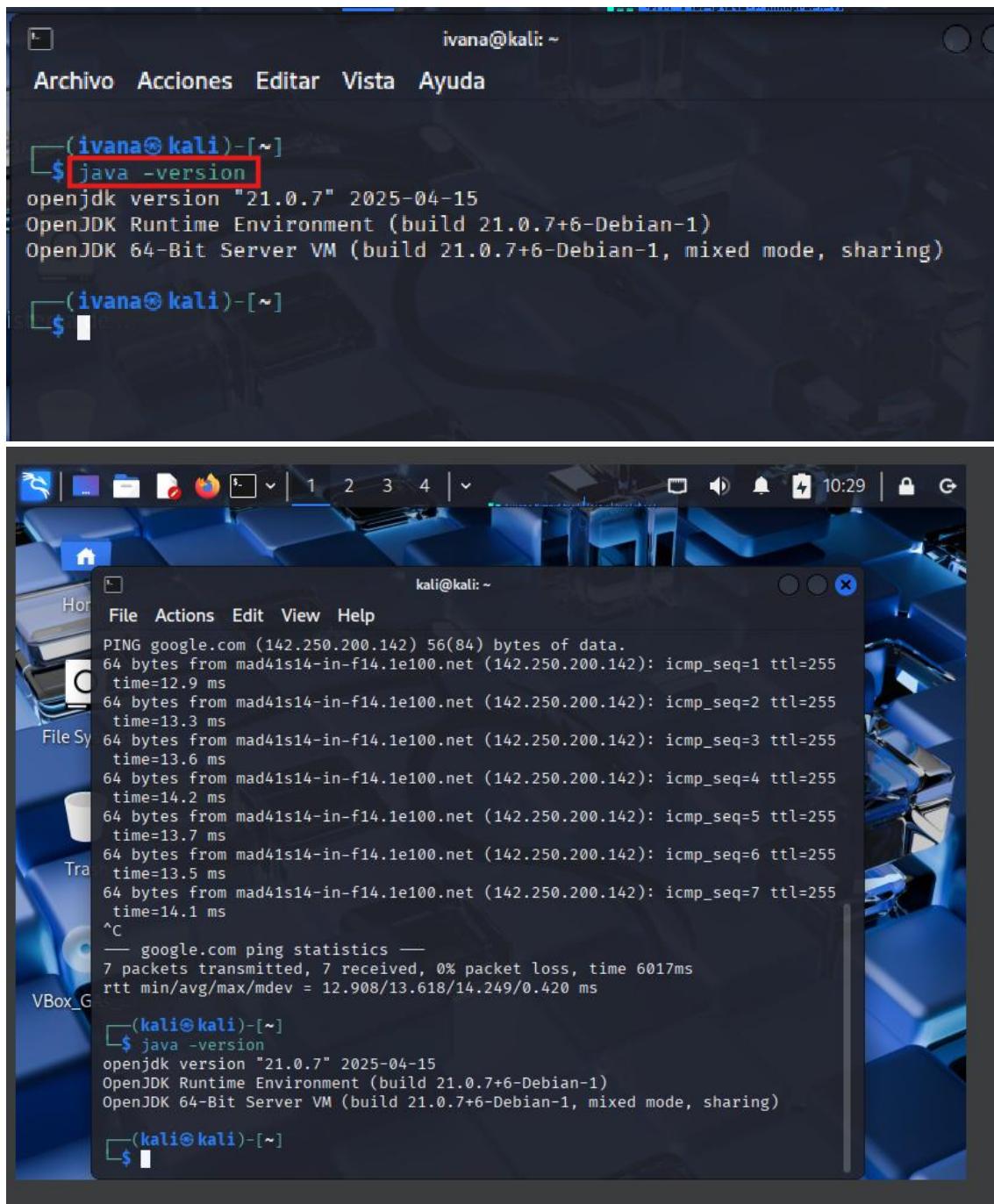
Burp Suite está escrito en Java, lo que lo hace compatible con diferentes sistemas operativos. Sin embargo, esto significa que necesitas tener **Java Runtime Environment (JRE)** instalado en tu sistema para que Burp funcione correctamente.

Primero verificamos si ya tienes Java instalado y si la versión es la adecuada. Burp Suite requiere **Java 11 o superior**. Abrimos un terminal en Kali Linux y comprobamos la versión de Java con el comando **java -version**.

Si Java está instalado, verás una salida similar a esta:

```
openjdk version "11.0.23" 2024-04-16
OpenJDK Runtime Environment (build 11.0.23+9-Ubuntu-1ubuntu122.04.1)
```

OpenJDK 64-Bit Server VM (build 11.0.23+9-Ubuntu-1ubuntu122.04.1, mixed mode, sharing)



Si no tuvieras Java instalado o la versión es anterior a la 11, deberás instalar Java 11 o superior. Aunque Kali Linux lo suele tener preinstalado, si no fuera el caso, puedes instalarlo con:

sudo apt update

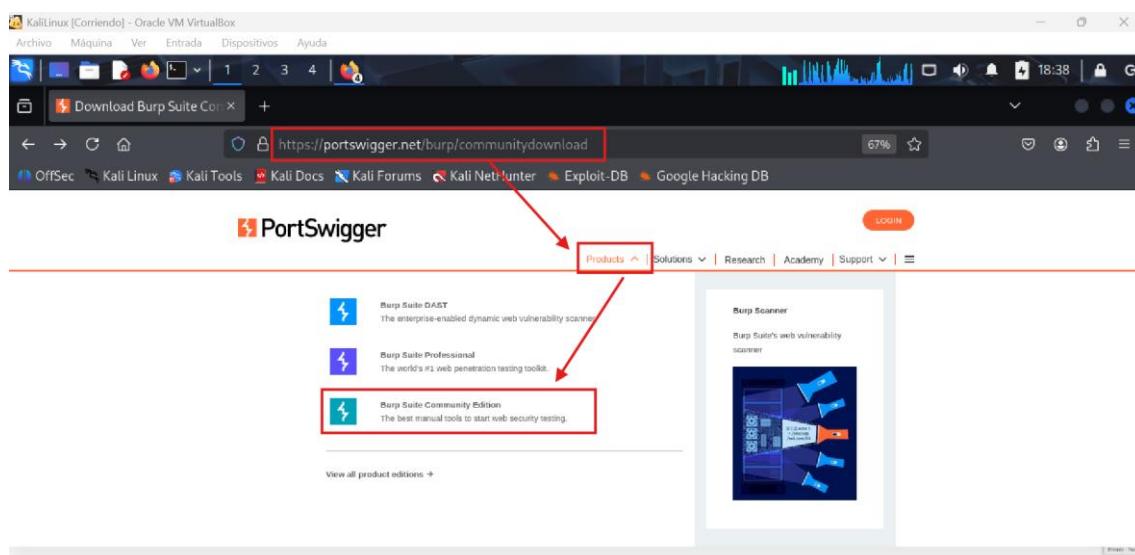
sudo apt install default-jre -y

Esto instalará la versión predeterminada de JRE, que en sistemas actuales suele ser Java 11 o posterior.

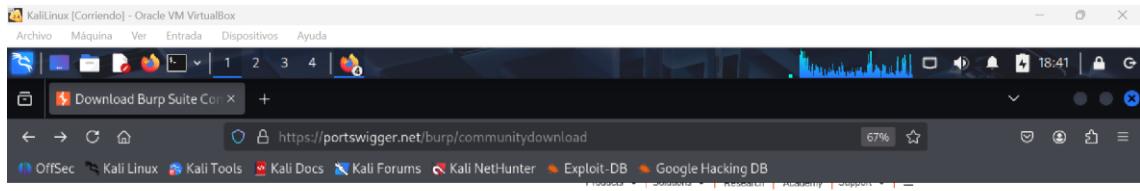
3.2. Descarga del instalador oficial de Burp Suite Community

Es crucial descargar Burp Suite desde la fuente oficial para evitar versiones modificadas o maliciosas.

1. **Abrir el Navegador Web:** En tu máquina virtual de Kali Linux, abre un navegador web (Firefox es el predeterminado en Kali).
2. **Ir a la Página de Descarga Oficial:** Navega a la siguiente URL:
<https://portswigger.net/burp/communitydownload>
3. **Seleccionar el Instalador:**
 - En la página, busca la sección de descarga para "**Burp Suite Community Edition**".



- Selecciona la versión adecuada para tu sistema operativo. Para Kali Linux, elegirás el instalador "**Linux (64-bit)**" o "**Linux (x64)**".



Burp Suite Community Edition

Start your web security testing journey for free - download our essential manual toolkit.

[Enter your email to download](#) [DOWNLOAD](#)



[Go straight to downloads →](#)

PortSwigger

Professional / Community 2025.5.6

30 June 2025 at 14:32 UTC

Burp Suite Community Edition [Linux \(x64\)](#)

[Download](#)

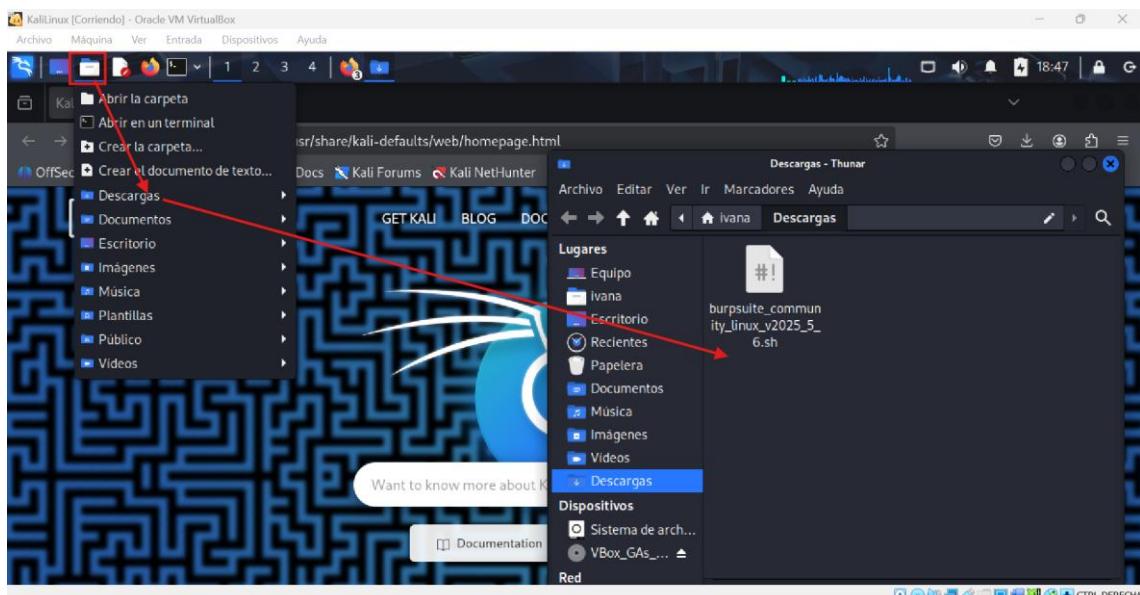
show checksums

We've upgraded Burp's browser to Chromium 138.0.7204.50 for Windows & Mac and 138.0.7204.49 for Linux. For more information, see the [Chromium release notes](#).

Usage of this software is subject to the [licence agreement](#).

[All releases →](#)

- Haz clic en el botón de "Download" (Descargar). Es posible que PortSwigger te pida un reCAPTCHA para verificar que no eres un robot.



3.3. Proceso de Instalación Paso a Paso

Con el instalador descargado y Java listo, el proceso de instalación de Burp Suite es bastante sencillo.

3.3.1. Ejecutando el instalador (Windows, Linux, macOS)

Aquí nos centraremos en el proceso para Linux, que es lo más común en un entorno de Kali.

1. **Abrir una Terminal:** Abre una nueva terminal en Kali Linux y entra en modo de superusuario:

Sudo su

- Te pedirá tu contraseña de usuario (la de Kali Linux). Ingresa y presiona Enter.

2. **Navegar al Directorio de Descarga:** Usa el comando cd para ir a la carpeta donde descargaste el instalador. Si lo guardaste en Descargas:

cd Descargas/

3. **Dar Permisos de Ejecución:** El archivo .sh que descargaste es un script de instalación. Para ejecutarlo, primero necesitas darle permisos de ejecución:

chmod +x burpsuite_community_linux_v2025_5_6.sh

4. **Ejecutar el Instalador:** Ahora, ejecuta el script de instalación con sudo (para permisos de administrador):

./burpsuite_community_linux_v2025_5_6.sh

KaliLinux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali: /home/ivana/Descargas

```
(ivan@kali)-[~]
$ sudo su
(root@kali)-[/home/ivana]
# cd Descargas

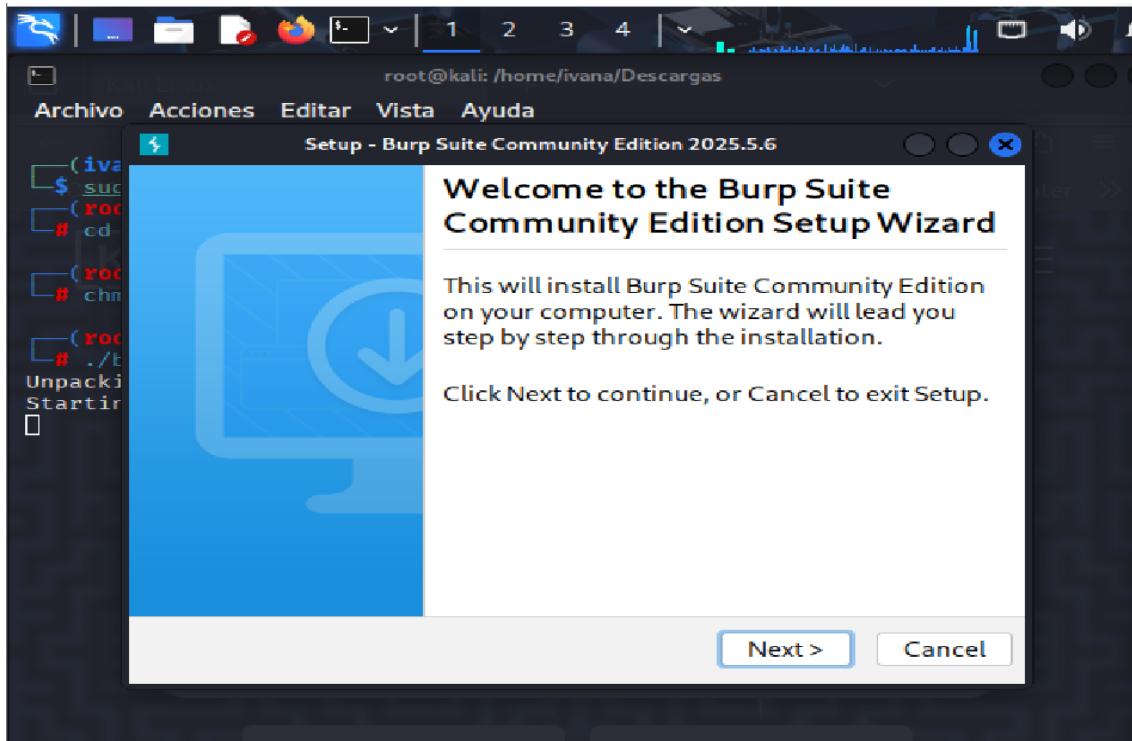
(root@kali)-[/home/ivana/Descargas]
# chmod +x burpsuite_community_linux_v2025_5_6.sh

[root@kali]-[/home/ivana/Descargas]
# ./burpsuite_community_linux_v2025_5_6.sh
Unpacking JRE ...
Starting Installer ...
```

3.3.2. Aceptando términos y seleccionando directorio

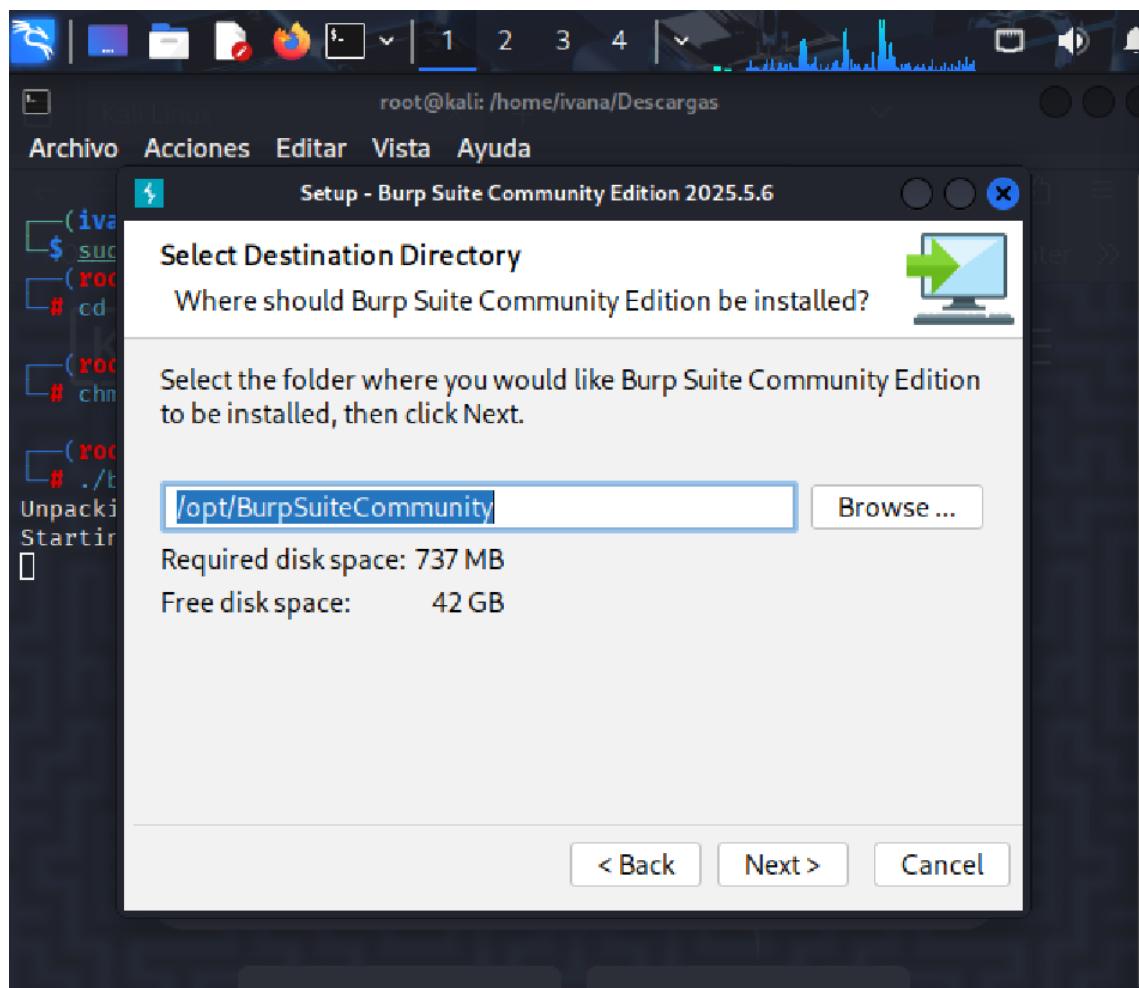
El instalador gráfico se iniciará y te guiará a través de los pasos.

1. **Pantalla de Bienvenida:** Haz clic en "Next".



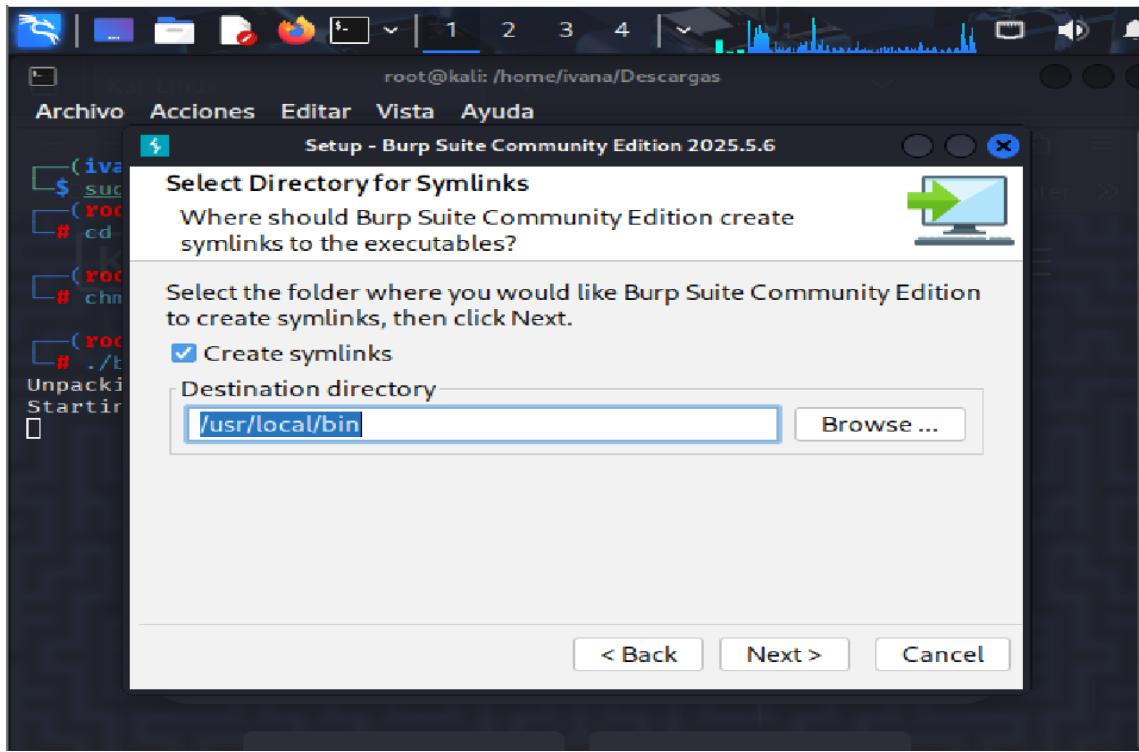
2. **Acuerdo de Licencia:** Lee el acuerdo de licencia (si lo deseas) y selecciona "I accept the agreement" (Acepto el acuerdo). Haz clic en "Next".
3. **Seleccionar Carpeta de Instalación:**

- La ubicación predeterminada suele ser /opt/BurpSuiteCommunity. Esta es una ubicación estándar y recomendada para programas opcionales en Linux.
- Puedes cambiarla si lo deseas, pero para la mayoría de los usuarios, la predeterminada es la mejor opción.
- Haz clic en "Next".



4. Seleccionar Creación de Enlaces Simbólicos:

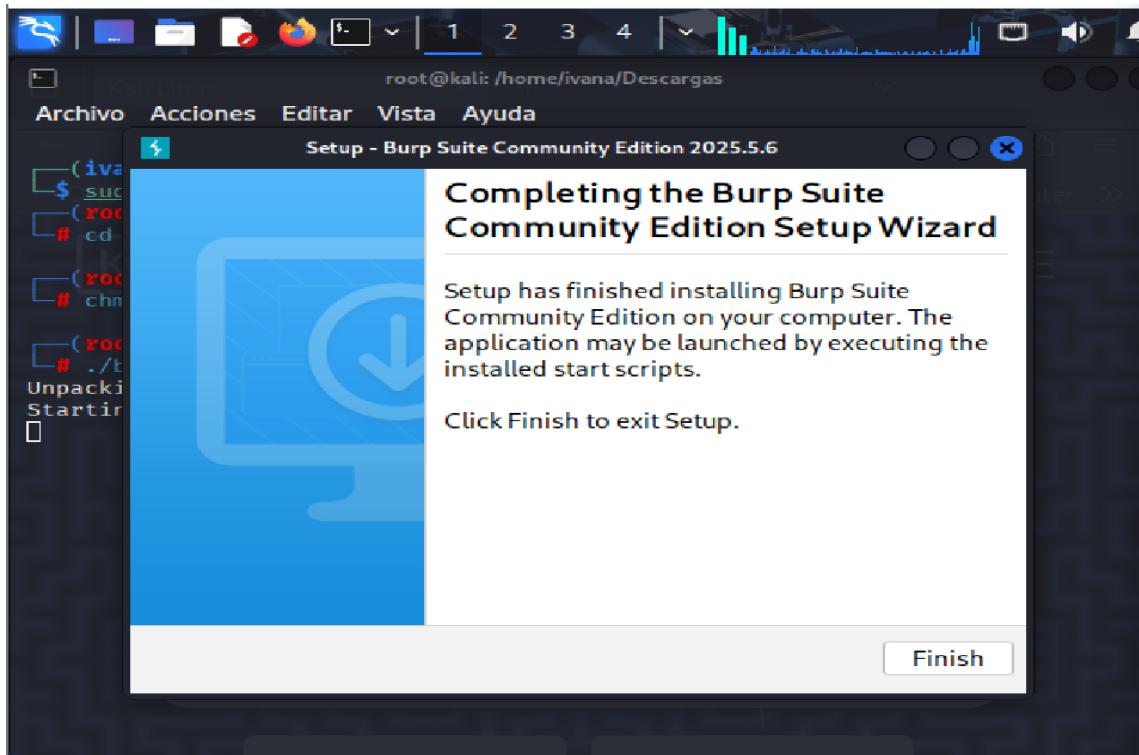
- Deja la opción marcada para "Create symlinks". Esto hará que Burp Suite sea más fácil de iniciar desde la terminal o desde el menú de aplicaciones.
- Haz clic en "Next".



3.3.3. Finalizando la instalación y primer inicio

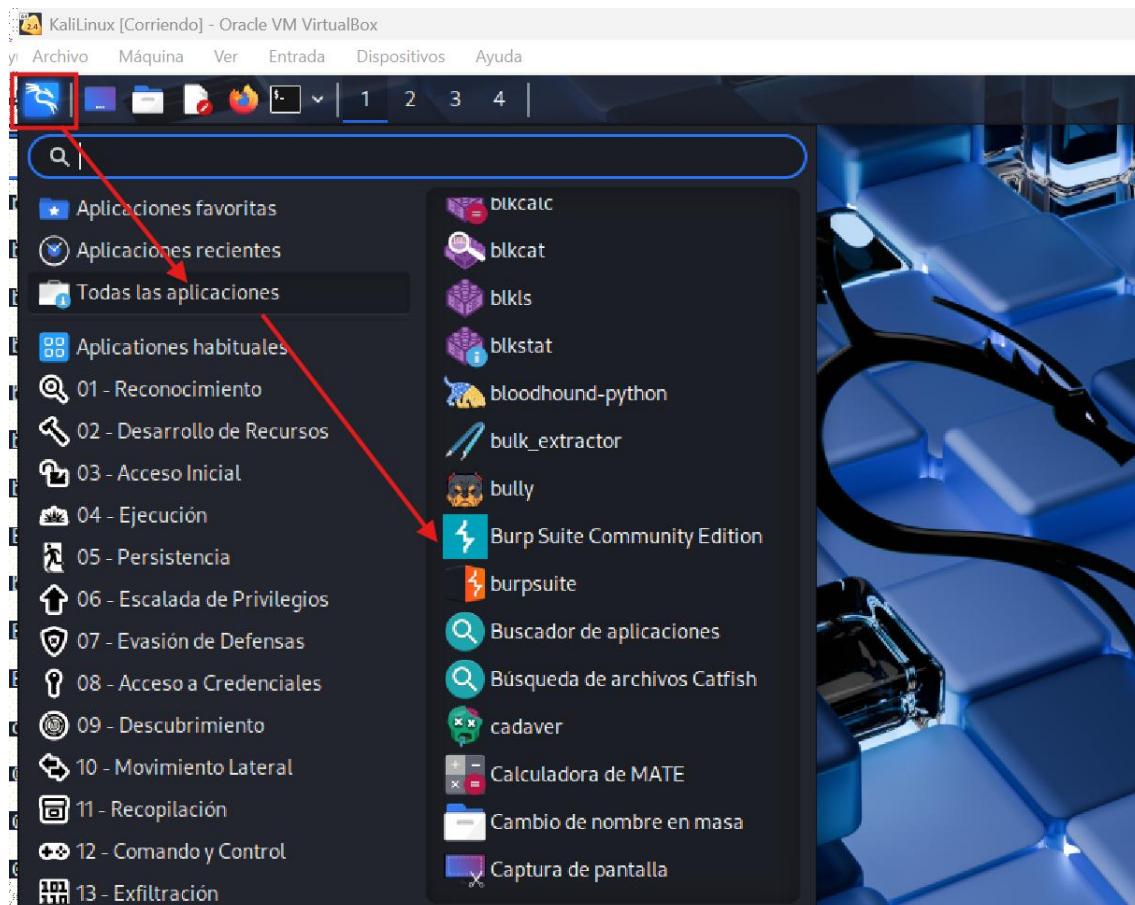
Una vez que la instalación haya terminado, recibirás una confirmación.

1. **Instalación Completada:** La barra de progreso llegará al 100%, y verás un mensaje de "Installation Complete". Haz clic en "Finish".



2. Lanzar Burp Suite por Primera Vez:

- Puedes iniciar Burp Suite de varias maneras:
 - Desde el **menú de aplicaciones** de Kali Linux (busca "Burp Suite Community Edition").



- Desde la **terminal**, simplemente escribiendo: **burpsuite** y presionando Enter.

3.4. Lanzamiento inicial de Burp Suite

La primera vez que inicies Burp Suite, te presentará algunas opciones relacionadas con la configuración de tu proyecto.

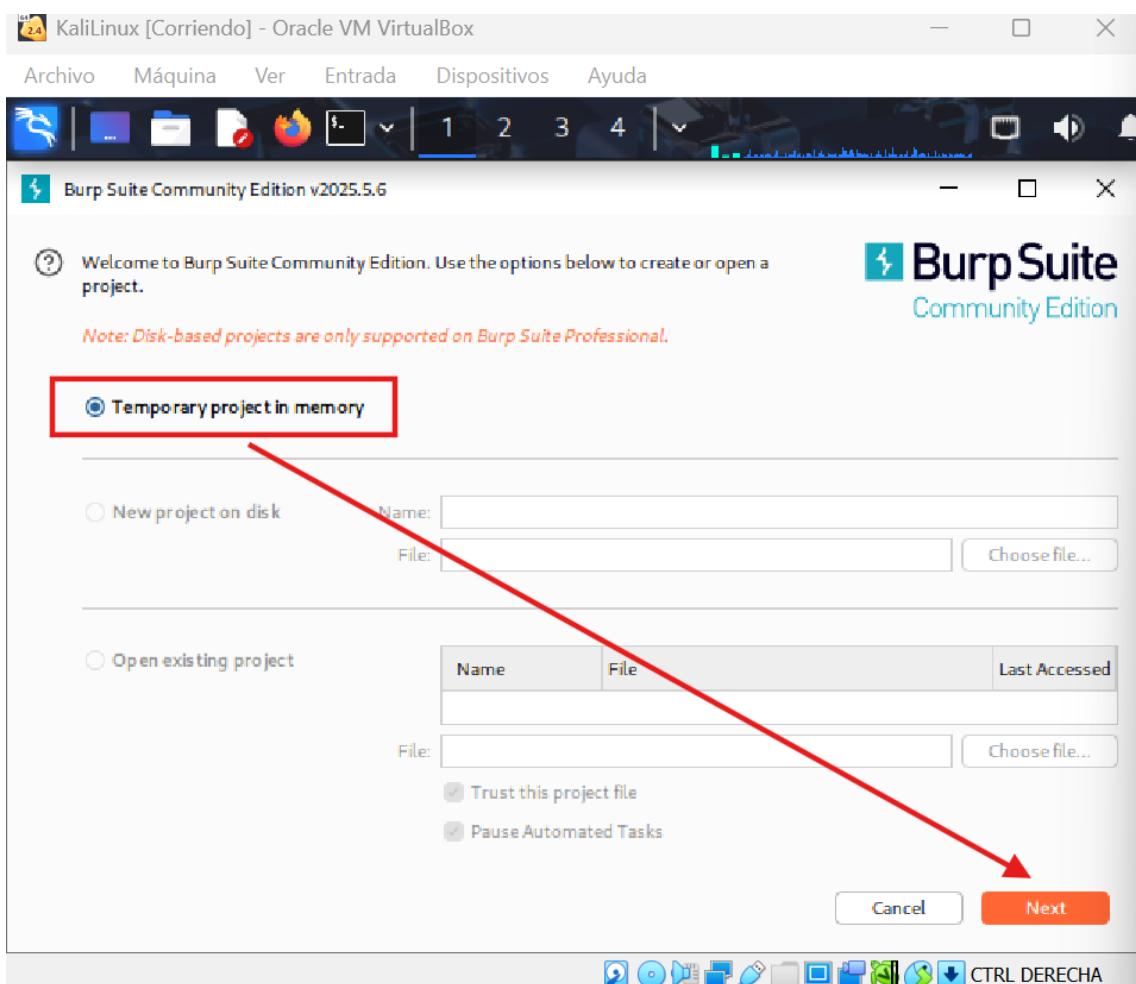
3.4.1: Opciones de proyecto (proyecto temporal vs. proyectos persistentes)

1. **Selección de Proyecto:** Cuando Burp Suite se inicie, verás una ventana de "Project options".
 - **Temporary project:** Esta es la opción **recomendada para empezar**. Crea un proyecto en memoria RAM que se borra al cerrar Burp Suite.

Es ideal para pruebas rápidas y para aprender, ya que no deja rastros de archivos en tu disco.

- **New project on disk:** Te permite guardar el estado de tu proyecto en un archivo en el disco. Útil para sesiones de prueba más largas o cuando necesitas guardar tu trabajo para reanudarlo más tarde.
- **Open existing project:** Para abrir un proyecto que hayas guardado previamente.

Para este tutorial, seleccionaremos "**Temporary project**", ya que es la única que nos permite la versión gratuita.

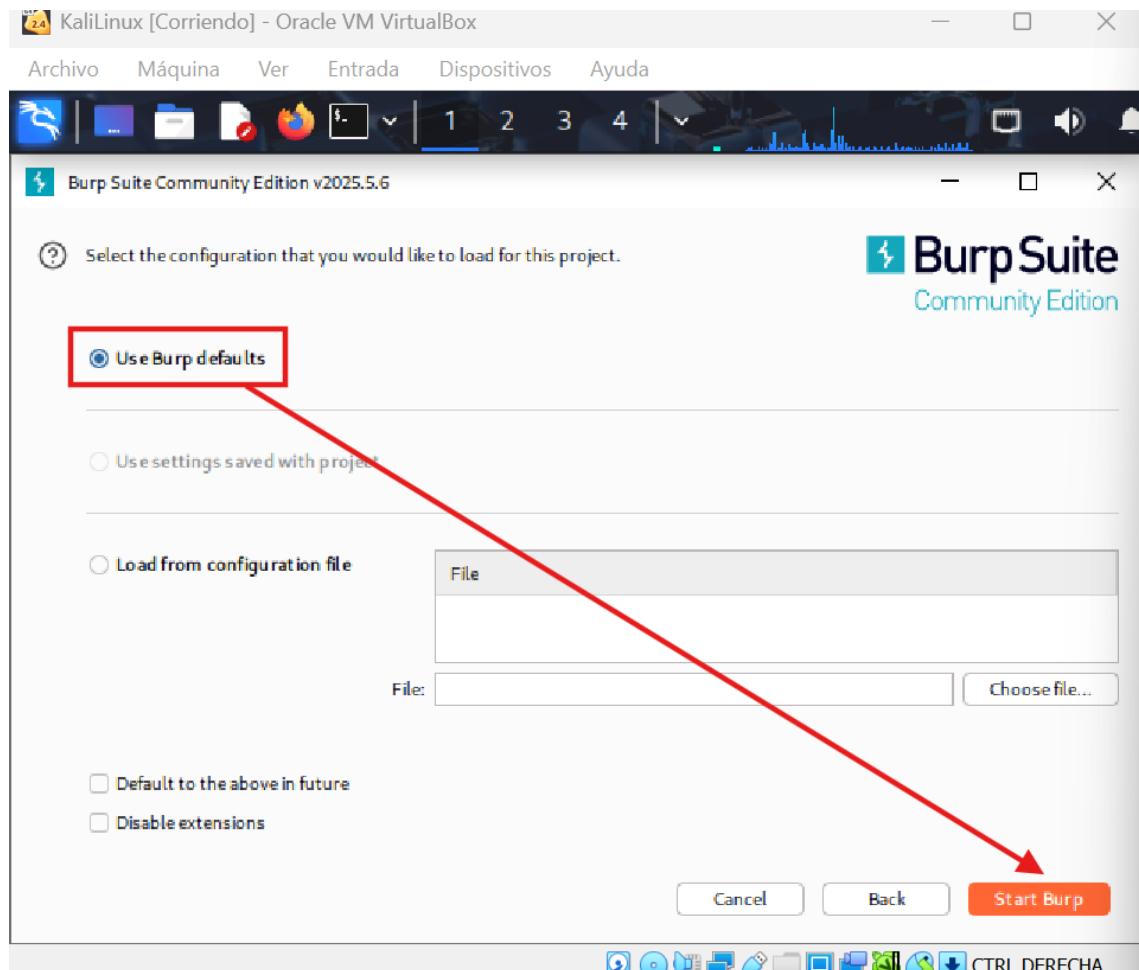


2. **Configuración de Burp:** La siguiente pantalla te preguntará si quieres usar la configuración por defecto o cargar una configuración de usuario.

- **Use Burp defaults:** Esta es la opción **recomendada para principiantes**. Carga la configuración predeterminada de Burp Suite, que es ideal para empezar.

- **Load from a configuration file:** Para cargar configuraciones guardadas previamente.

Selecciona "**Use Burp defaults**".



3. **Iniciar Burp:** Haz clic en el botón "Start Burp".

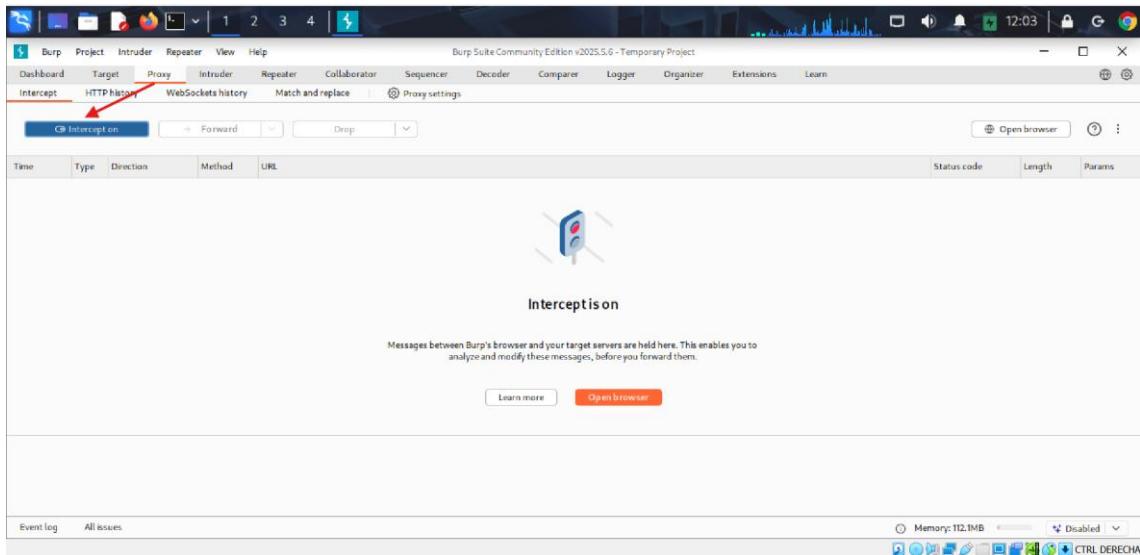
3.4.2: Configuración por defecto y la interfaz principal

Una vez que Burp Suite haya cargado, verás su interfaz principal.

1. Interfaz Principal:

- En la parte superior, verás una serie de pestañas (Dashboard, Target, Proxy, Intruder, Repeater, Decoder, Comparer, Extender, Options, Alerts). Cada una corresponde a una herramienta diferente dentro de Burp Suite.
- Por defecto, Burp Suite se ha abierto en la pestaña Learn. Me colocaré en la pestaña "**Proxy**" para comprobar que la subpestana

"**Intercept**" se encuentra activa, pues es aquí donde se interceptará el tráfico HTTP/S.



Felicidades! Ya tienes Burp Suite Community Edition instalado y funcionando en tu máquina virtual de Kali Linux. Ahora estás listo para el siguiente paso crucial: configurarlo para que tu navegador empiece a enviar el tráfico a través de él.

4. Configuración Inicial de Burp Suite

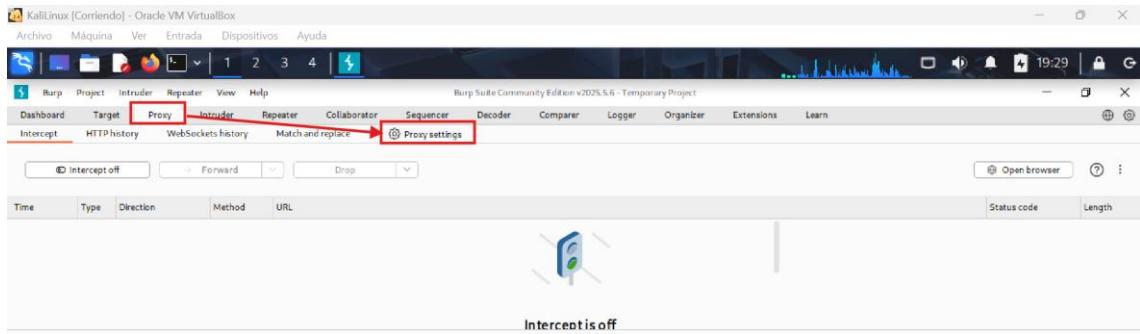
Una vez que Burp Suite está instalado y abierto, el siguiente paso crítico es configurarlo para que actúe como un intermediario (proxy) entre tu navegador y las aplicaciones web. Esto permite que Burp Suite intercepte, examine y modifique todo el tráfico HTTP/S que fluye entre ambos.

4.1. Configurando el Proxy Listener de Burp

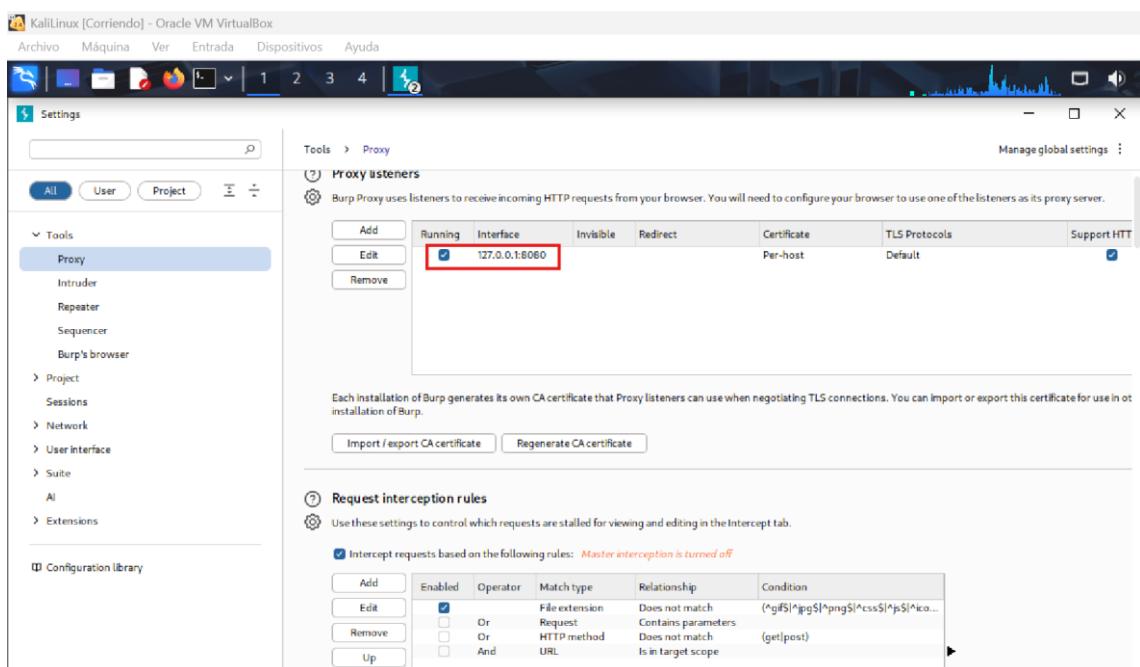
El "**Proxy Listener**" es el componente de Burp Suite que escucha las conexiones entrantes de tu navegador. Por defecto, Burp Suite ya tiene uno configurado, pero es importante saber dónde verificarlo y cómo ajustarlo si fuera necesario.

4.1.1. Verificando el Listener por defecto (127.0.0.1:8080)

- Abrir Burp Suite:** Asegúrate de que Burp Suite Community Edition esté en ejecución.
- Navegar a la pestaña Proxy:** En la interfaz principal de Burp Suite, haz clic en la pestaña "**Proxy**".
- Ir a la Subpestaña Options:** Dentro de la pestaña "Proxy", selecciona la subpestaña "**Options**".



- 4. Verificar el "Proxy Listeners":** En la sección "Proxy Listeners", deberías ver una entrada activa. Por defecto, esta entrada estará configurada para escuchar en la dirección IP 127.0.0.1 (localhost) y el puerto 8080.
- Asegúrate de que la casilla de verificación "**Running**" (Ejecutando) esté marcada para este listener. Si no lo está, márcala para activarlo.



4.1.2. Ajustes avanzados del Listener (opcional)

Aunque para empezar no necesitarás modificarlo, es bueno conocer algunas opciones:

- **Añadir/Eliminar Listeners:** Puedes añadir nuevos listeners si necesitas que Burp escuche en otra dirección IP o puerto, o eliminar los existentes. Haz clic en "**Add**" o "**Remove**".
 - Si añades uno, en "Bind to address" puedes seleccionar "All interfaces" si necesitas que otras máquinas en tu red puedan

proxyficar a través de tu Burp Suite (útil en algunos escenarios de laboratorio, pero no para empezar).

- **Request handling:** Esta sección define cómo Burp maneja las solicitudes que recibe. Por defecto, permite que todas las solicitudes pasen, pero podrías configurarlo para requerir un certificado de cliente, por ejemplo (avanzado).

Para este tutorial, nos mantenemos en **http://0.0.0.1:8080**.

4.2. Configurando tu Navegador para Burp Proxy

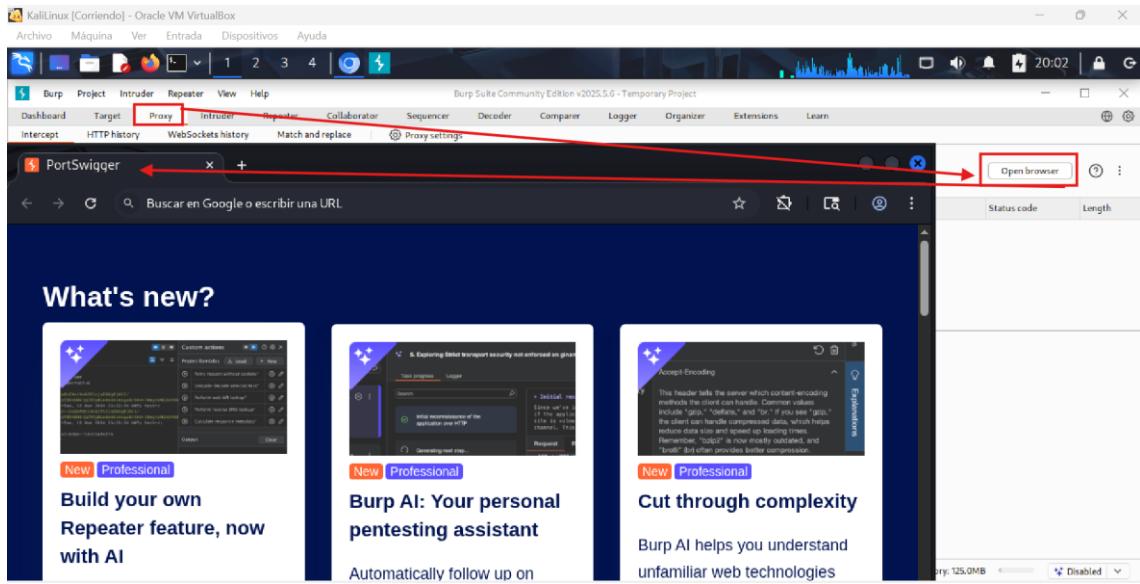
Ahora que Burp Suite está escuchando, debemos decirle a nuestro navegador que envíe todo su tráfico web a esa dirección y puerto. Tenemos dos opciones principales: usar el navegador integrado de Burp (el más fácil) o configurar un navegador externo como Firefox o Chrome.

4.2.1. Usando el navegador integrado de Burp (opción más sencilla)

Burp Suite incluye un navegador Chromium integrado que ya viene preconfigurado para usar el proxy de Burp. Esta es la forma **más rápida y sencilla** de empezar a interceptar tráfico, ya que no requiere configuración manual del navegador ni instalación de certificados (se maneja automáticamente para la sesión).

1. **Navegar a la Pestaña Proxy -> Intercept:** Asegúrate de estar en la pestaña "**Proxy**" y en la subpestaña "**Intercept**".
2. **Abrir el Navegador Integrado:** Haz clic en el botón "**Open browser**" (Abrir navegador) en la parte superior.

Observación: Se abrirá una nueva ventana de navegador. Cualquier sitio web que visites en esta ventana pasará automáticamente a través de Burp Suite. Este navegador es ideal para pruebas manuales rápidas.



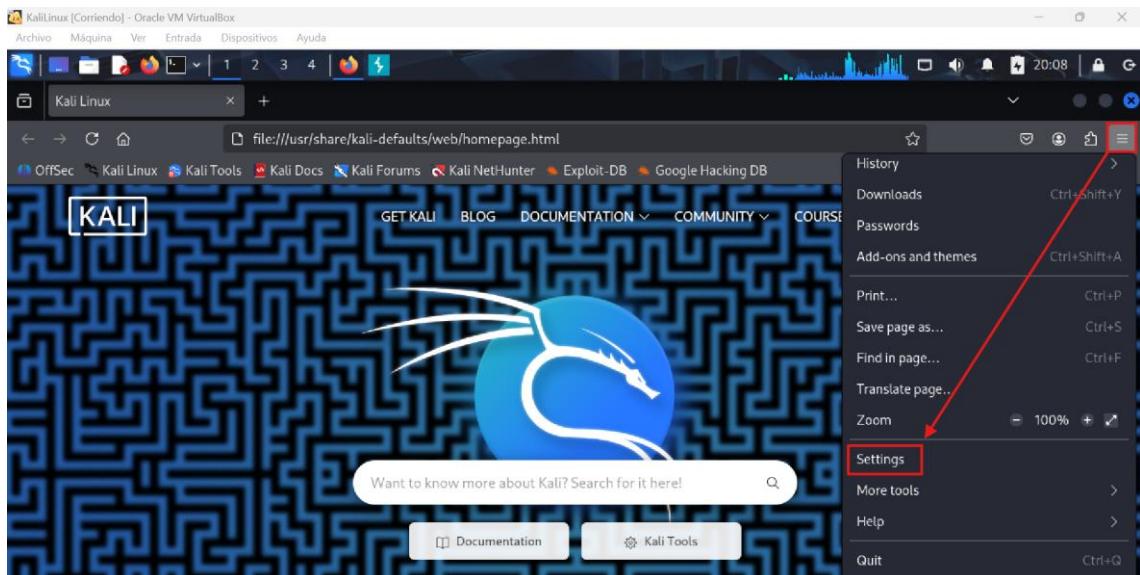
4.2.2. Configuración manual en Firefox (ejemplo detallado)

Mozilla Firefox es un navegador popular para trabajar con Burp Suite debido a su sencilla configuración de proxy integrada y a cómo maneja los certificados.

1. **Abrir Firefox:** Inicia el navegador Firefox en tu máquina virtual de Kali Linux.

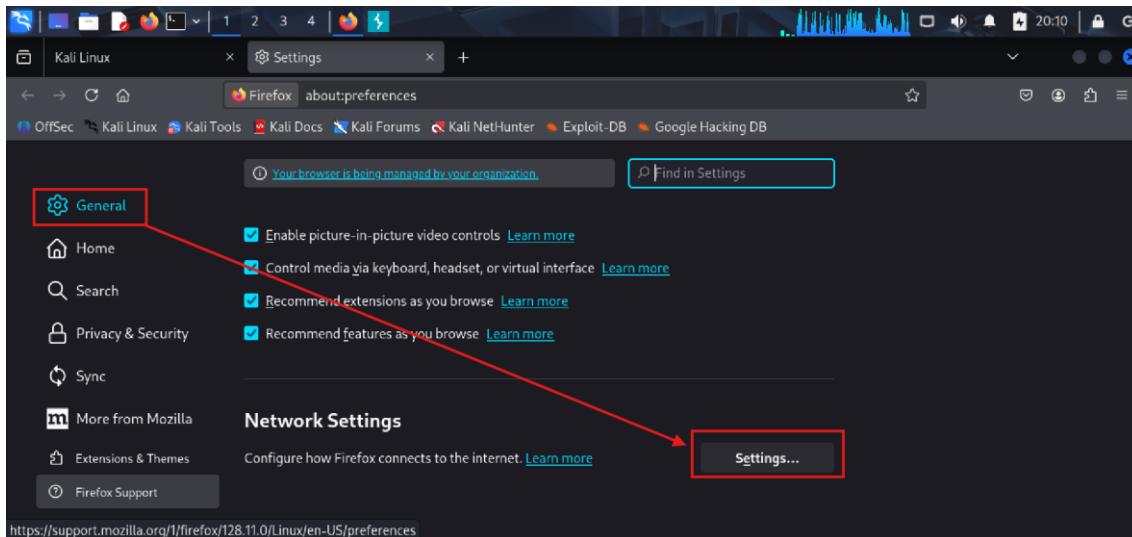
2. **Acceder a la Configuración:**

- Haz clic en el **botón de menú (tres líneas horizontales)** en la esquina superior derecha del navegador.
- Selecciona **"Settings"** (Preferencias/Opciones, dependiendo de tu sistema y versión).



3. Navegar a la Configuración de Red:

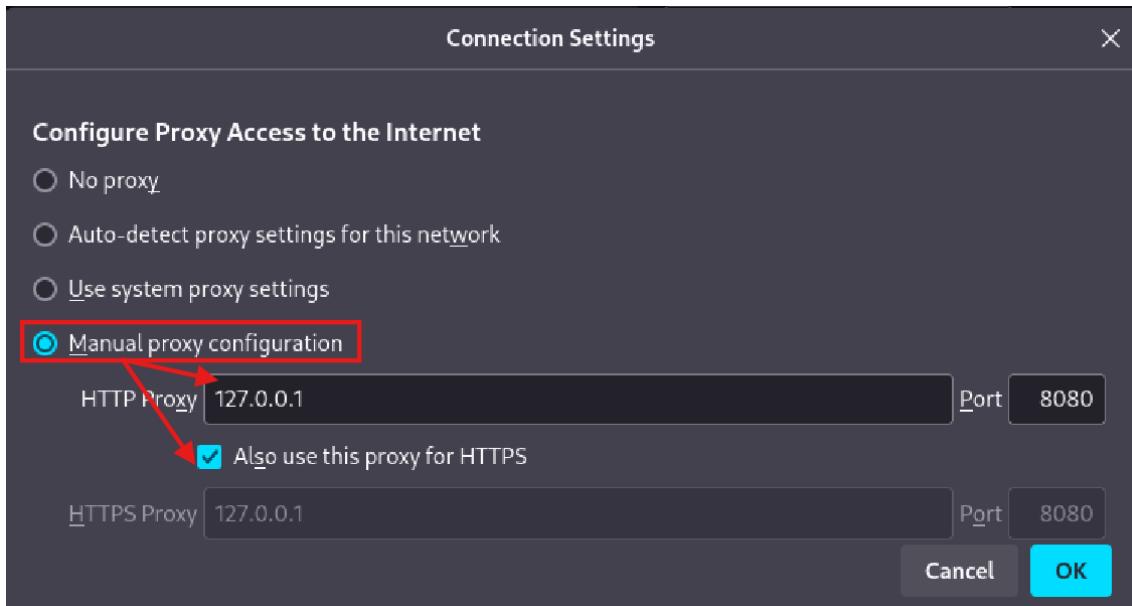
- En el menú lateral izquierdo, haz clic en "**General**".
- Desplázate hacia abajo hasta la sección "**Network Settings**" (Configuración de red).
- Haz clic en el botón "**Settings...**" (Configuración...).



4. Configurar el Proxy Manualmente:

- En la ventana "Connection Settings" (Configuración de conexión), selecciona la opción "**Manual proxy configuration**" (Configuración manual del proxy).
- En el campo:
 - "**HTTP Proxy**" escribe 127.0.0.1 y puerto 8080
 - "**HTTPS Proxy**" haz clic en la casilla “Usar el mismo proxy para todos los protocolos”
- **Importante:** Asegúrate de que el campo "No proxy for" (Sin proxy para) esté vacío o no contenga 127.0.0.1 ni localhost.

- Haz clic en "OK" para guardar los cambios y cerrar la ventana de configuración de conexión.



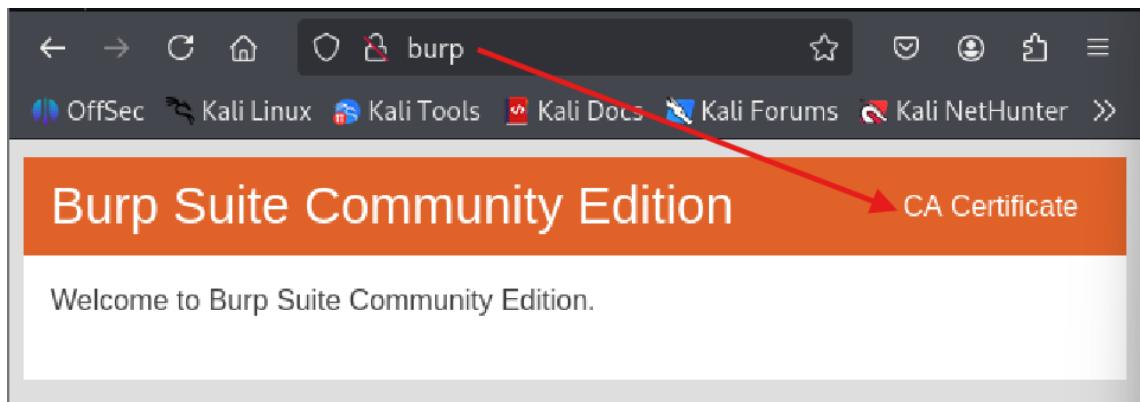
4.2.3. Instalación del Certificado CA de Burp Suite para HTTPS

Cuando Burp Suite intercepta tráfico HTTPS, actúa como un "man-in-the-middle". Para hacer esto sin que tu navegador muestre advertencias de seguridad (ya que Burp está "descifrando" y "recifrando" el tráfico), necesitas instalar el **Certificado de Autoridad (CA) raíz de Burp Suite** en tu navegador como una autoridad de confianza.

Sin este certificado, cada vez que visites un sitio HTTPS a través de Burp, verás errores como "Su conexión no es privada" o "Advertencia de riesgo potencial de seguridad".

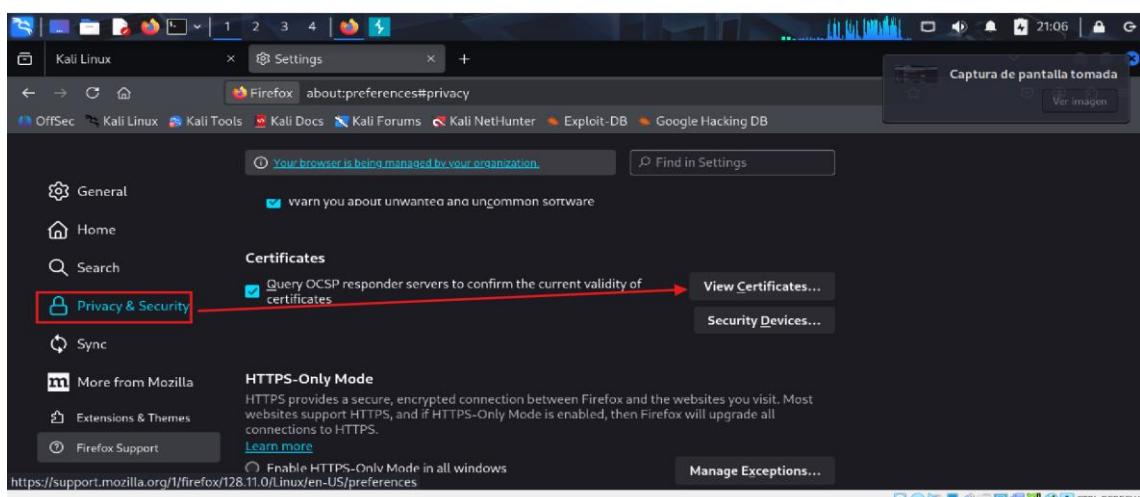
Abre **Burp Suite**.

1. Ve a la pestaña **Proxy** → **Intercept** y asegúrate de que el botón diga "**Intercept is off**" (desactívalo si está encendido).
2. Luego ve a <http://burp> desde Firefox.
3. Haz clic en "**CA Certificate**" para descargar el certificado de Burp.

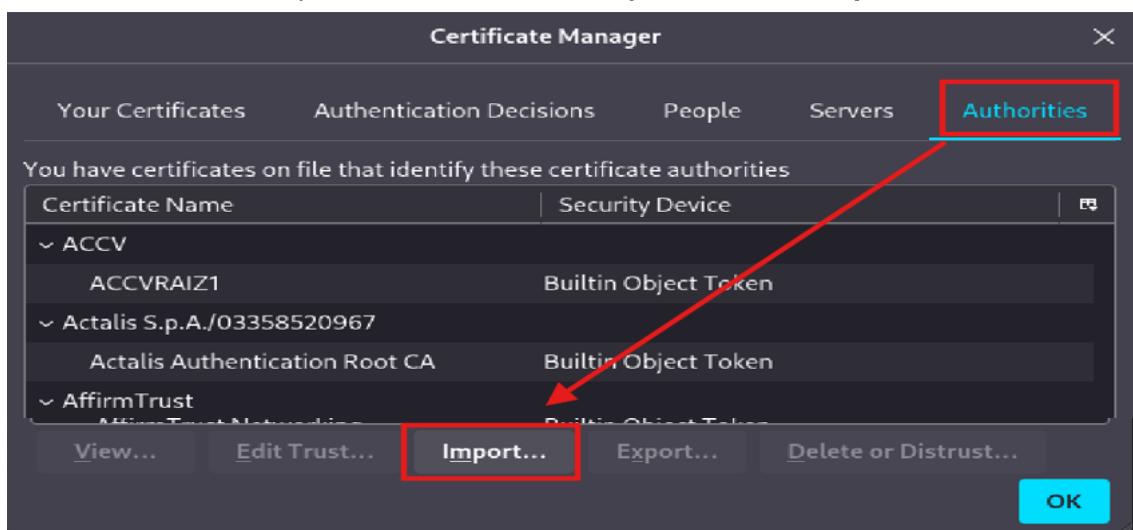


4. En Firefox, ve al:

- **Botón de menú (tres líneas horizontales)** en la esquina superior derecha del navegador.
- Baja a **Settings → Privacidad y seguridad → Certificados** → Clic en "Ver certificados".

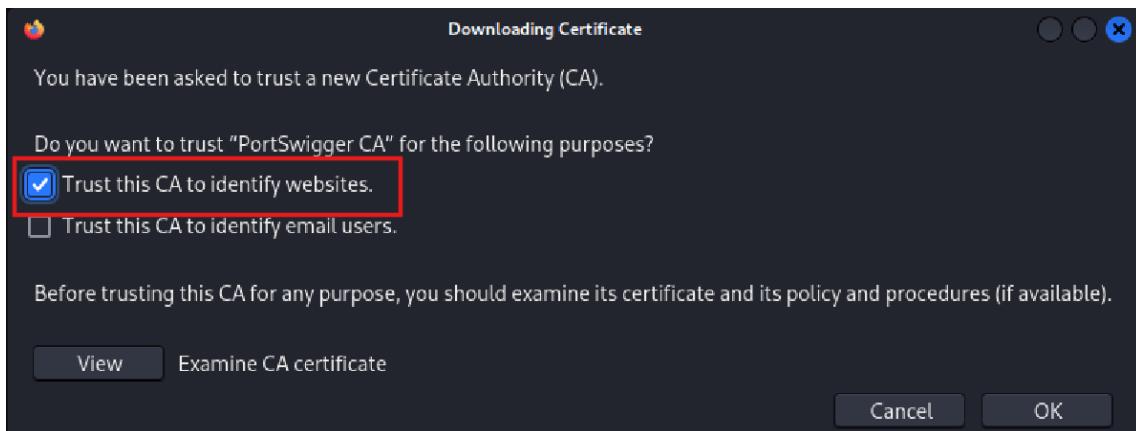


- Ve a la pestaña "**Autoridades**" y haz clic en "**Importar**".



- Importa el archivo .cer que descargaste.

- Marca la opción "**Confiar en esta CA para identificar sitios web**" y acepta.



Ahora, cuando navegues a sitios HTTPS a través de Burp Suite en Firefox, no deberías ver advertencias de seguridad.

4.2.4. Importar el certificado a nivel del sistema operativo (para Chrome y otras apps)

A diferencia de Firefox, Chrome (y otras aplicaciones) suelen depender del almacén de certificados del sistema operativo. El proceso puede variar ligeramente entre distribuciones de Linux, pero aquí te daré la forma general para Kali Linux.

1. Mover el Certificado a una Ubicación de Confianza:

- Abre una terminal en Kali Linux.
- Crea un directorio para certificados confiables si no existe:
sudo mkdir -p /usr/local/share/ca-certificates/extra
- Mueve el certificado cacert.der descargado a esta carpeta:

```
sudo mv Descargas/cacert.der /usr/local/share/ca-
certificates/extra/burpsuite_ca.crt
```

Nota: Renombramos el archivo a .crt porque es un formato común para certificados de confianza en Linux.

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/ivana
Archivo Acciones Editar Vista Ayuda
[(ivana㉿kali)-[~]
$ sudo su - Google Chrome...
[sudo] contraseña para ivana:
[root㉿kali)-[/home/ivana]
# mkdir -p /usr/local/share/ca-certificates/extra
[root㉿kali)-[/home/ivana]
# mv Descargas/cacert.der /usr/local/share/ca-certificates/extra/burpsuite_ca.crt
[root㉿kali)-[/home/ivana]
#
```

2. Actualizar el Almacén de Certificados del Sistema:

- Ejecuta el comando para actualizar la lista de certificados de confianza del sistema:
sudo update-ca-certificates
- Deberías ver un mensaje indicando que se ha añadido un nuevo certificado (ej. "1 added, 0 removed").

```
Archivo Acciones Editar Vista Ayuda
[(root㉿kali)-[/home/ivana]
# sudo update-ca-certificates
Updating certificates in /etc/ssl/certs ...
rehash: warning: skipping burpsuite_ca.pem, it does not contain exactly one
certificate or CRL
rehash: warning: skipping ca-certificates.crt, it does not contain exactly one
certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d ...
Procesando disparadores para ca-certificates-jdk (20240118) ...
Adding debian:burpsuite_ca.pem
done.
done.

[root㉿kali)-[/home/ivana]
#
```

3. Reiniciar Chrome: Cierra y vuelve a abrir Chrome para que cargue los nuevos certificados del sistema.

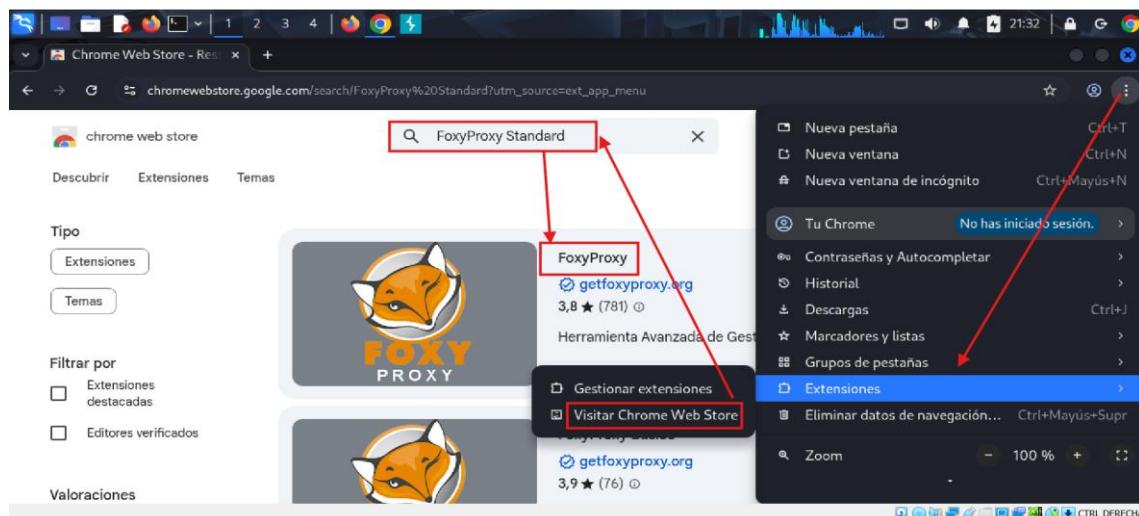
Con estos pasos, tu navegador (sea el integrado de Burp, Firefox o Chrome con FoxyProxy) y Burp Suite están listos para trabajar juntos. ¡Ahora puedes interceptar y examinar el tráfico web!

4.2.5. Configuración de Chrome

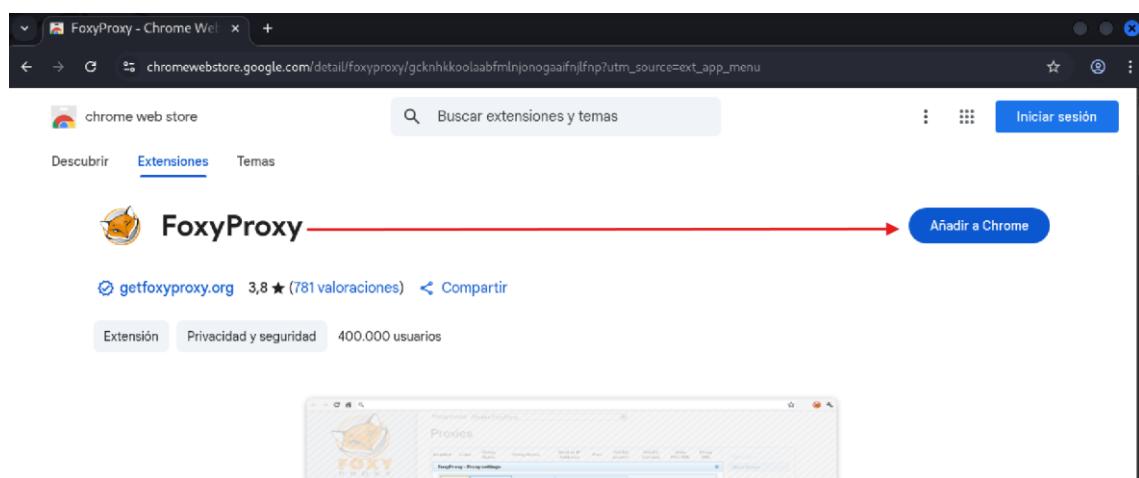
Google Chrome no tiene una opción de configuración de proxy manual tan sencilla para este propósito como Firefox. Por lo tanto, para usar Chrome con Burp Suite, la forma más recomendada es a través de una **extensión de navegador como FoxyProxy Standard**.

1. Instalar FoxyProxy Standard:

- Abre Chrome en tu VM de Kali Linux.
- Ve a la Chrome Web Store y busca "**FoxyProxy Standard**" o accede directamente a su página.

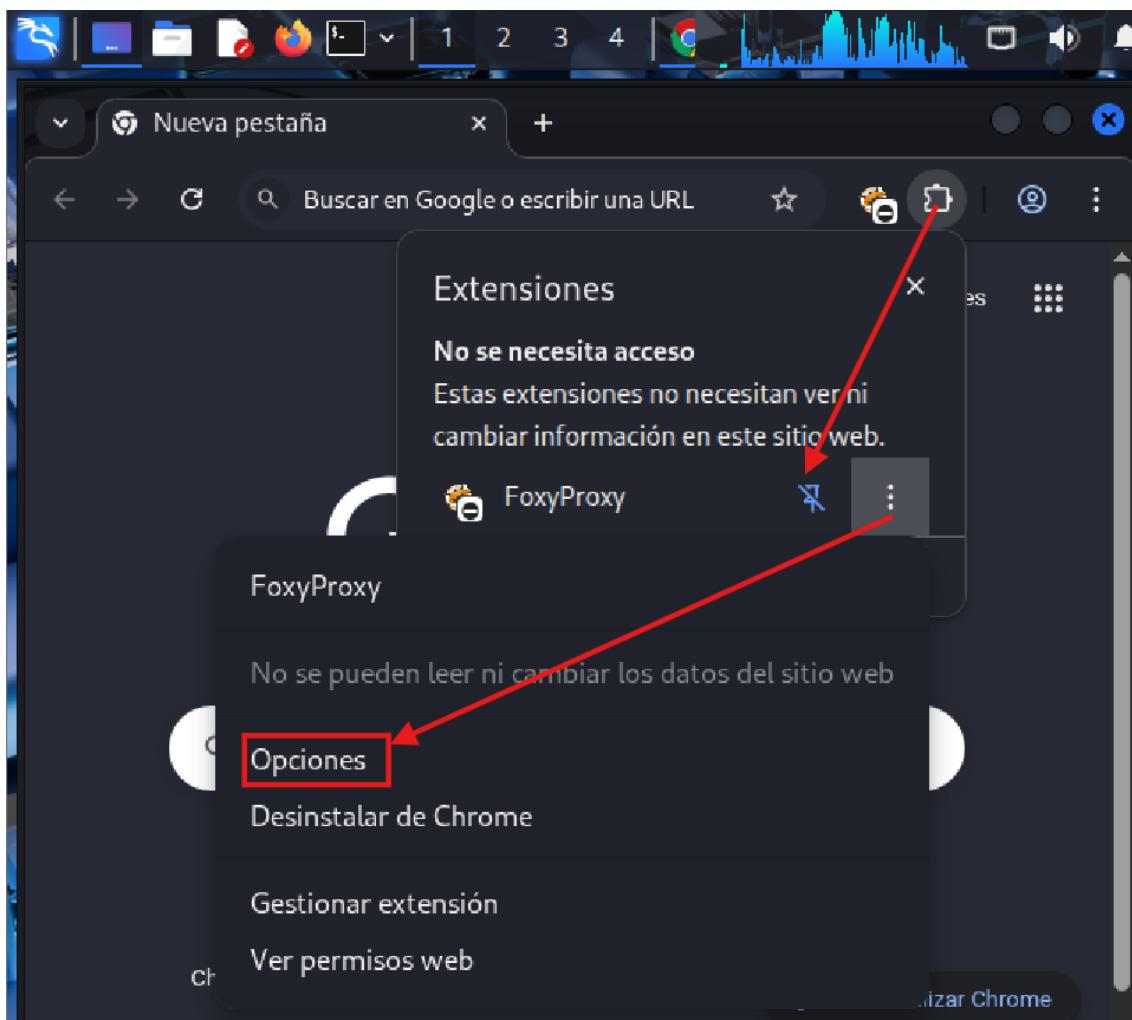


- Haz clic en "**Add to Chrome**" (Añadir a Chrome) y luego en "**Add extension**" (Añadir extensión) para instalarla.

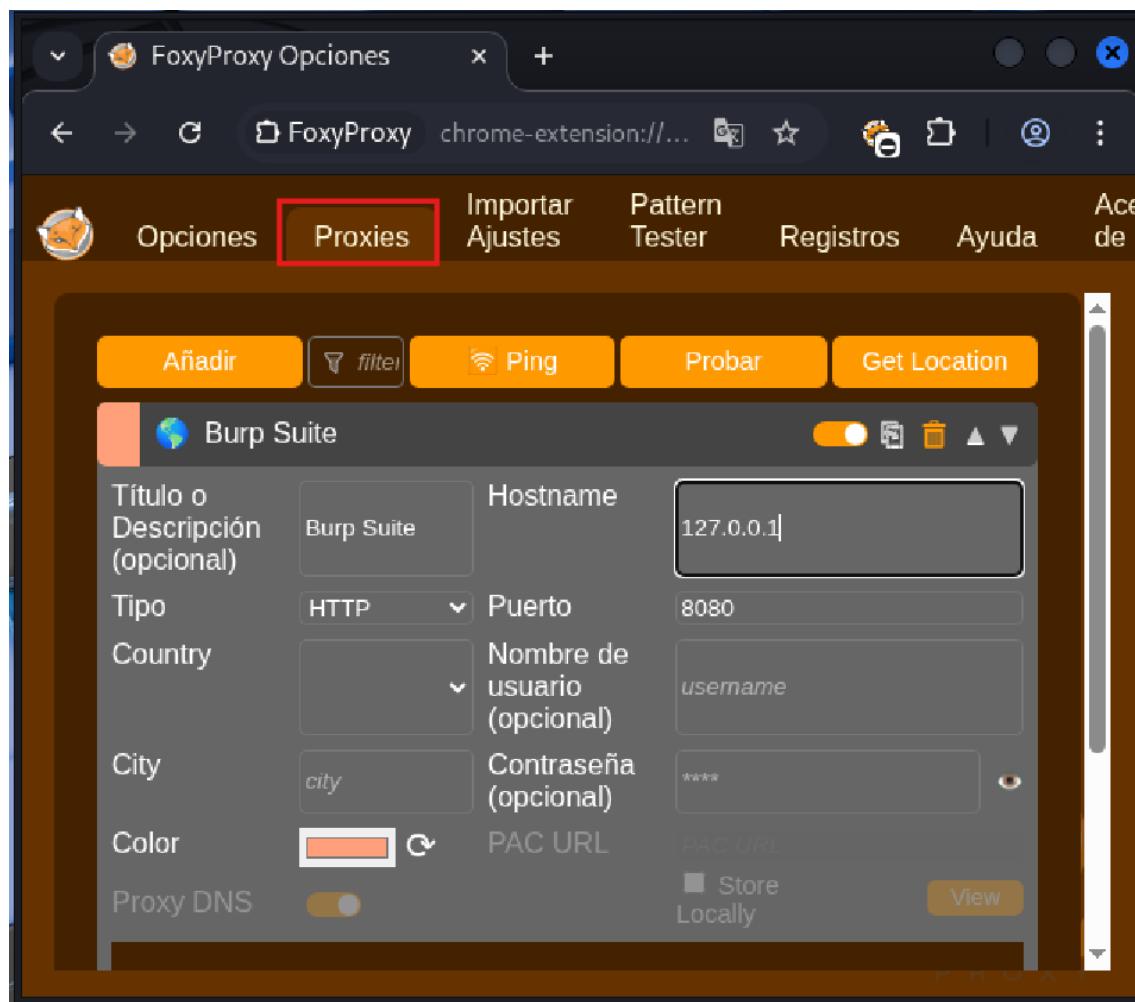


2. Configurar un Nuevo Proxy en FoxyProxy:

- Una vez instalada, el icono de FoxyProxy aparecerá en la barra de herramientas de Chrome (puede que necesites hacer clic en el icono del "puzzle" para verlo y "fijarlo").
- Haz clic en el icono de FoxyProxy y selecciona "**Options**" (Opciones).



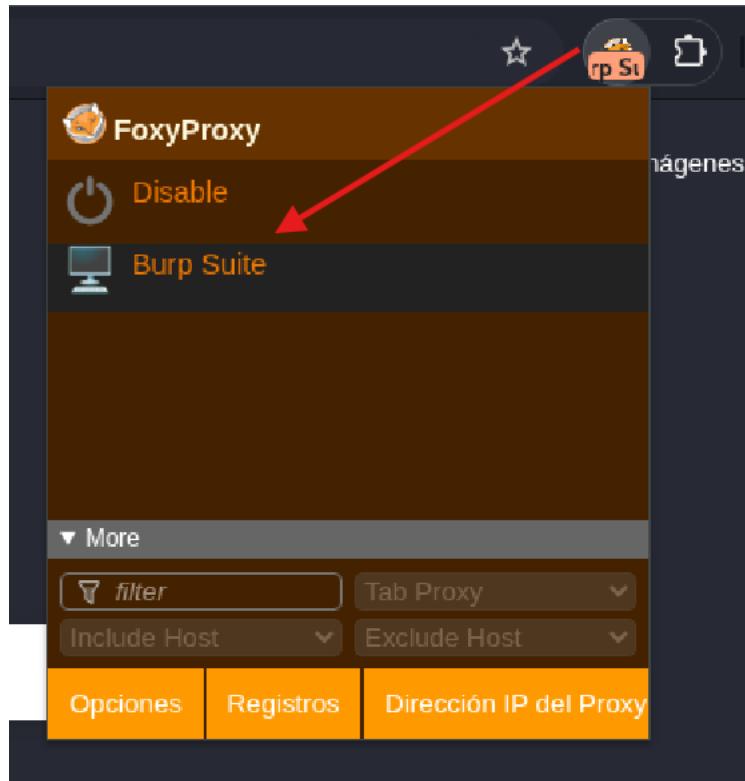
- Haz clic en el botón "**Proxy**" (Añadir nuevo proxy).
 - Dale un "Title" (Título) descriptivo, por ejemplo, "**Burp Suite**".
 - Puedes añadir una "Description" si quieres.
 - En "Hostname" ingresa 127.0.0.1.
 - En "Port" (Puerto), ingresa 8080.
 - Deja el tipo de proxy como "HTTP" (funciona para HTTP y HTTPS).



- Haz clic en "**Save**" (Guardar).

3. Activar el Perfil de Proxy:

- Para usar Burp Suite, haz clic en el ícono de FoxyProxy en la barra de herramientas.
- Selecciona el perfil "**Burp Suite**" que acabas de crear. El ícono de FoxyProxy cambiará de color para indicar que está activo.
- Cuando quieras dejar de usar Burp, simplemente selecciona "Turn Off" o "Use Chrome's Proxy Settings".



4.2.6. FUNCIONAMIENTO DE BURP SUITE

Cuando el botón "**Intercept is ON**" está activado, Burp Suite detiene cada petición que tu navegador hace antes de enviarla al servidor, dejándola en espera hasta que tú decidas qué hacer (puedes modificarla, reenviarla o descartarla). Mientras no pulses "**Forward**" o desactives la interceptación, el navegador seguirá "pensando" porque está esperando respuesta y, por tanto, la página no carga.

Al poner "**Intercept is OFF**", Burp Suite deja de detener (interceptar) cada petición y simplemente las deja pasar de inmediato. Por eso, tu navegador puede navegar y abrir páginas normalmente, y todas las peticiones/respuestas siguen quedando guardadas en el historial de Burp Suite para que puedas analizarlas después.

<https://rinku.tech/curso-kali-linux/utilizar-burpsuite/>

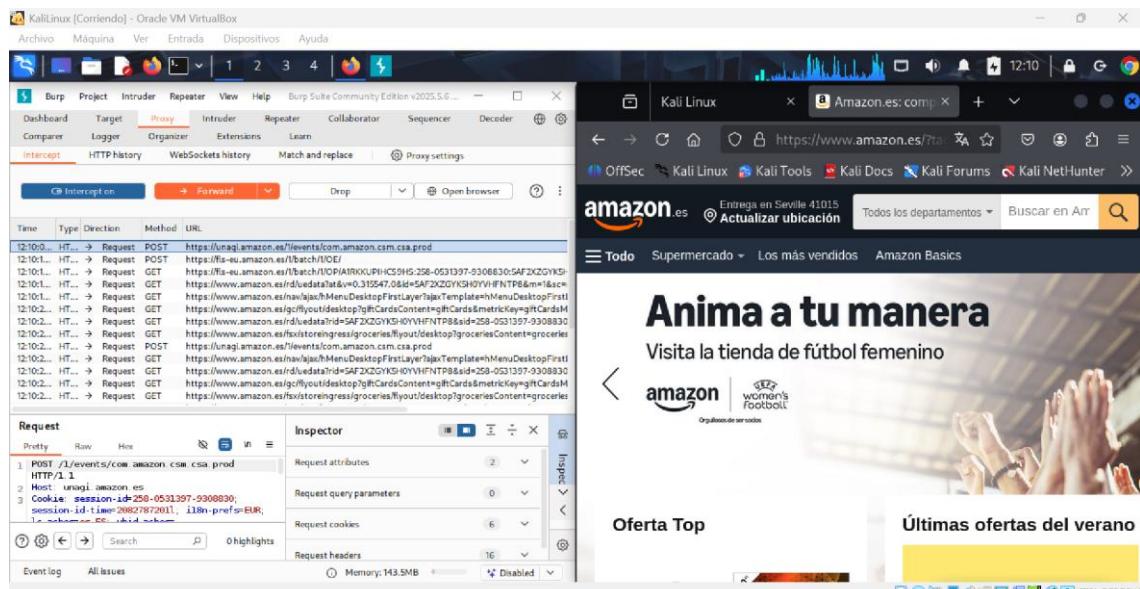
Estado de Intercept	¿Qué pasa?
Intercept is ON	El navegador se queda esperando. Debes reenviar (Forward) o desactivar Intercept para seguir.
Intercept is OFF	La navegación es normal. Las páginas cargan como siempre.

Sugerencias prácticas

- Activa Intercept solo cuando quieras modificar manualmente una petición específica.
- Déjalo en OFF para una navegación fluida y cuando solo quieras analizar el tráfico en el historial después.
- Puedes revisar el historial de todo el tráfico en Proxy > HTTP History incluso cuando Intercept está en OFF.

Esto es el flujo estándar de trabajo con Burp Suite: interceptas solo cuando lo necesitas y, el resto del tiempo, permites que la navegación fluya normalmente a través del proxy.

Si necesitas hacer pruebas modificando peticiones, actívalo solo puntualmente y recuerda volverlo a OFF para no bloquear toda la navegación.



4.2.7. Estructura de una solicitud HTTP/S en Burp

Cuando una solicitud es interceptada en la pestaña **Proxy -> Intercept**, verás diferentes secciones:

- **Raw (Crudo):** Muestra la solicitud HTTP completa tal como se envía (encabezados, cuerpo, etc.). Es la vista más fundamental.
- **Params (Parámetros):** Muestra una lista de los parámetros de la solicitud (parámetros GET/URL, parámetros POST/cuerpo, cookies), lo que facilita su identificación y edición.
- **Headers (Encabezados):** Muestra solo los encabezados HTTP de la solicitud.
- **Hex (Hexadecimal):** Muestra los datos de la solicitud en formato hexadecimal, útil para ver caracteres no imprimibles o binarios.
- **Browser (Navegador):** (Solo en la versión Professional) Intenta renderizar la solicitud para ver cómo la vería un navegador.

4. Guía de Uso Básico: Intercepción de Tráfico Web

El corazón de Burp Suite, especialmente en la Community Edition, reside en su capacidad para interceptar el tráfico HTTP/S entre tu navegador y un servidor web. Esto te permite inspeccionar cada solicitud y respuesta, e incluso modificarlas sobre la marcha.

5.1. Preparando un Entorno de Prueba Seguro

Antes de comenzar a interceptar, es vital recordar la importancia de dónde realizas tus pruebas. La ciberseguridad, incluso para aprender, debe practicarse de forma ética y legal.

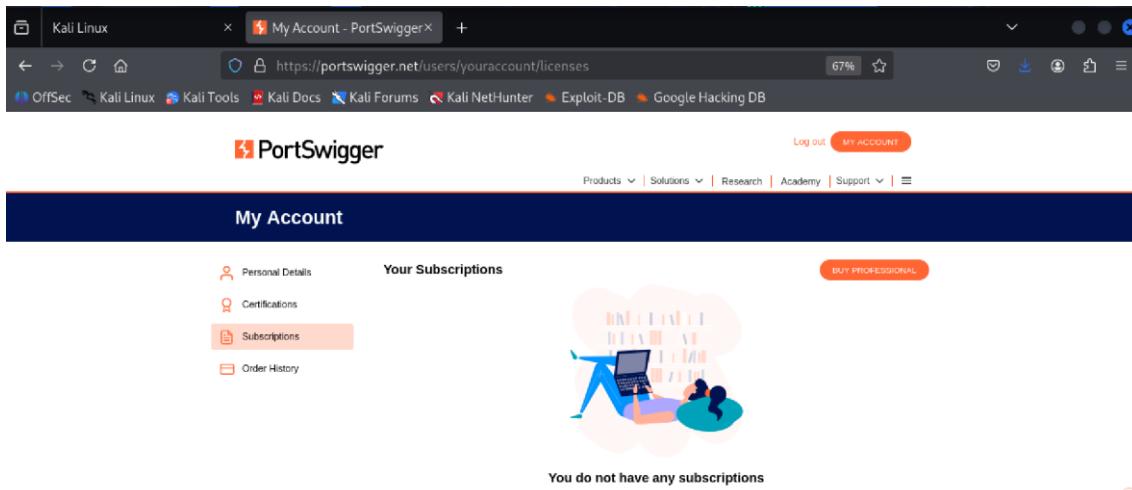
5.1.1. Introducción a laboratorios de práctica

Para garantizar un aprendizaje seguro, legal y ético, siempre debes practicar en entornos diseñados específicamente para pruebas de seguridad. Nunca utilices Burp Suite para probar sitios web de los que no tengas permiso explícito del propietario.

Aquí te presento algunas excelentes opciones para tus laboratorios:

- **PortSwigger Web Security Academy:**

- **Descripción:** Esta es la plataforma oficial de PortSwigger (los creadores de Burp Suite) y es **altamente recomendada** para principiantes. Ofrece una amplia gama de laboratorios interactivos y deliberadamente vulnerables, que cubren diversas vulnerabilidades web (SQL Injection, XSS, Autenticación, etc.).
- **Ventajas:** Es totalmente **gratuita**, está diseñada para integrarse perfectamente con Burp Suite, y sus laboratorios se restablecen automáticamente después de cada sesión, garantizando un entorno limpio y consistente. Incluye guías paso a paso para muchas vulnerabilidades.
- **Acceso:** Visita <https://portswigger.net/web-security/all-labs>. Necesitarás crear una cuenta gratuita para acceder a los laboratorios.



- **DVWA (Damn Vulnerable Web Application):**

- **Descripción:** DVWA es una aplicación web PHP/MySQL diseñada para ser vulnerable. Es un excelente recurso para aprender a realizar pruebas de penetración web.
- **Ventajas:** Puedes instalarla localmente en tu VM de Kali Linux o en otra VM separada, lo que te da control total sobre el entorno. Es muy versátil para simular diferentes niveles de seguridad y configuraciones.
- **Instalación (brevemente):** Requiere un servidor web (Apache), PHP y una base de datos MySQL/MariaDB. En Kali Linux, puedes instalar los componentes necesarios (`sudo apt install apache2 php libapache2-mod-php php-mysql mysql-server -y`) y luego descargar DVWA y configurarlo. Esto puede ser un poco más complejo para un principiante, pero hay muchos tutoriales online.

- **bWAPP (Buggy Web Application):**
 - **Descripción:** Similar a DVWA, bWAPP es otra aplicación web de propósito vulnerable que cubre más de 100 tipos de vulnerabilidades. A menudo se distribuye como una máquina virtual preconstruida (llamada "Bee-Box").
 - **Ventajas:** Cubre una gama muy amplia de vulnerabilidades. La versión "Bee-Box" simplifica la configuración al ser una VM lista para usar.
 - **Instalación:** Si usas Bee-Box, simplemente impórtala en VirtualBox o VMware como cualquier otra VM preconstruida (similar a cómo importaste Kali si usaste la imagen de VM).

Recomendación para este tutorial: Empezaremos con **PortSwigger Web Security Academy**, pues es la opción más sencilla y directa para practicar con Burp Suite sin complicaciones de configuración adicional de servidores web.

5.1.2. Consideraciones de seguridad: ¡Nunca pruebes en sitios reales sin permiso!

Es fundamental que tengas en cuenta las siguientes consideraciones de seguridad en todo momento:

- **Legalidad y Ética:** Realizar pruebas de seguridad en sistemas o aplicaciones de terceros sin su consentimiento explícito es ilegal y poco ético. Puede acarrear graves consecuencias legales.
- **Permiso Documentado:** Si alguna vez trabajas para una empresa o cliente, asegúrate de tener un contrato o acuerdo por escrito que autorice las pruebas de penetración.
- **Alcance (Scope):** Comprende claramente el "alcance" de la prueba: qué sistemas, IPs o URLs están permitidos para ser probados y cuáles no.

5.2. Pasos del Caso Práctico: Modificando un Login Simple

Δ LAB

APPRENTICE

SQL injection vulnerability allowing login bypass →

Not solved

Web Security Academy > SQL injection > Lab

Lab: SQL injection vulnerability allowing login bypass

Δ LAB

APPRENTICE

Not solved



This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user.



ACCESS THE LAB

⌚ Solution



⌚ Community solutions



La verdadera potencia de Burp Suite reside en su capacidad para interactuar con las solicitudes interceptadas.

Cuando una solicitud es interceptada en la pestaña **Proxy -> Intercept**, verás diferentes secciones:

- **Raw (Crudo):** Muestra la solicitud HTTP completa tal como se envía (encabezados, cuerpo, etc.). Es la vista más fundamental.
- **Params (Parámetros):** Muestra una lista de los parámetros de la solicitud (parámetros GET/URL, parámetros POST/cuerpo, cookies), lo que facilita su identificación y edición.
- **Headers (Encabezados):** Muestra solo los encabezados HTTP de la solicitud.

- **Hex (Hexadecimal):** Muestra los datos de la solicitud en formato hexadecimal, útil para ver caracteres no imprimibles o binarios.
- **Browser (Navegador):** (Solo en la versión Professional) Intenta renderizar la solicitud para ver cómo la vería un navegador.

Dedica un momento a explorar estas pestañas para entender la información que Burp te presenta sobre cada solicitud.

Ahora vamos a realizar un ejemplo práctico donde modificaremos una solicitud de login para intentar algo diferente a lo que el navegador pretendía enviar.. Usaremos un laboratorio de login de la Web Security Academy de PortSwigger o un formulario de login simple en un sitio de pruebas.

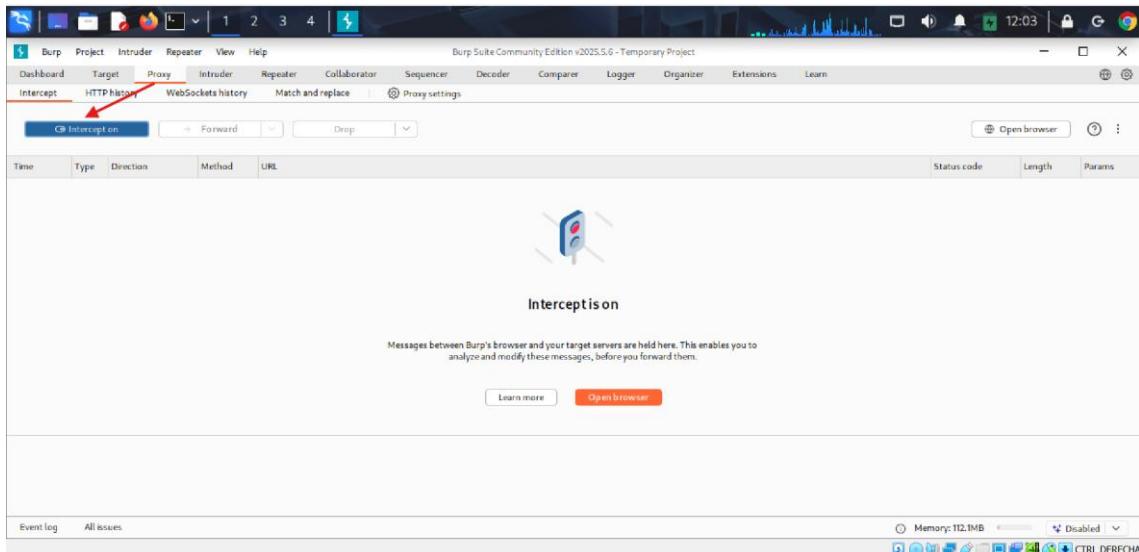
Pero ¿para qué sirve esto?

Pues entre otras cosas, porque nos va a permitir simplificar o automatizar las pruebas que requieran una rápida modificación de peticiones ya que podemos ver las respuestas y modificar las peticiones directamente en el proxy en tiempo real sin tener que pasar de nuevo por el cliente.

Escenario: Tienes un formulario de login con campos de usuario y contraseña. Intentaremos cambiar el nombre de usuario guest (invitado) a admin para ver si obtenemos una respuesta diferente.

Paso 1: Preparar Burp Suite

1. **Inicia Burp Suite** y asegúrate de que esté escuchando como proxy en 127.0.0.1:8080
2. **Configura tu navegador** (Firefox recomendado) para que todo el tráfico pase por ese proxy.
3. **Verifica que has instalado el certificado** de Burp Suite en el navegador para interceptar HTTPS.
4. Nos aseguramos que el proxy de Burp esté corriendo: en la pestaña **Proxy** de Burp Suite, vamos a la subpestaña **Intercept** y verificamos que está en **ON**



Paso 2: Navegar al sitio web de prueba

- Navega al formulario de login de PortSwigger en tu navegador Mozilla.**
<https://portswigger.net/users?returnurl=%2fusers%2fyouraccount%2fpersonaldetails>
- Introduce Credenciales de Prueba:** En el formulario de login, introduce credenciales falsas o de prueba, por ejemplo:
 - Username:** guest
 - Password:** 123

- Haz clic en "Login" (Iniciar sesión).** El navegador se "colgará" y la solicitud aparecerá en Burp Suite.
- Examina la Solicitud Interceptada:**
 - Vuelve a Burp Suite, pestaña Proxy -> Intercept.

- Observa la solicitud. Probablemente sea una solicitud POST a una URL como /login o /auth.

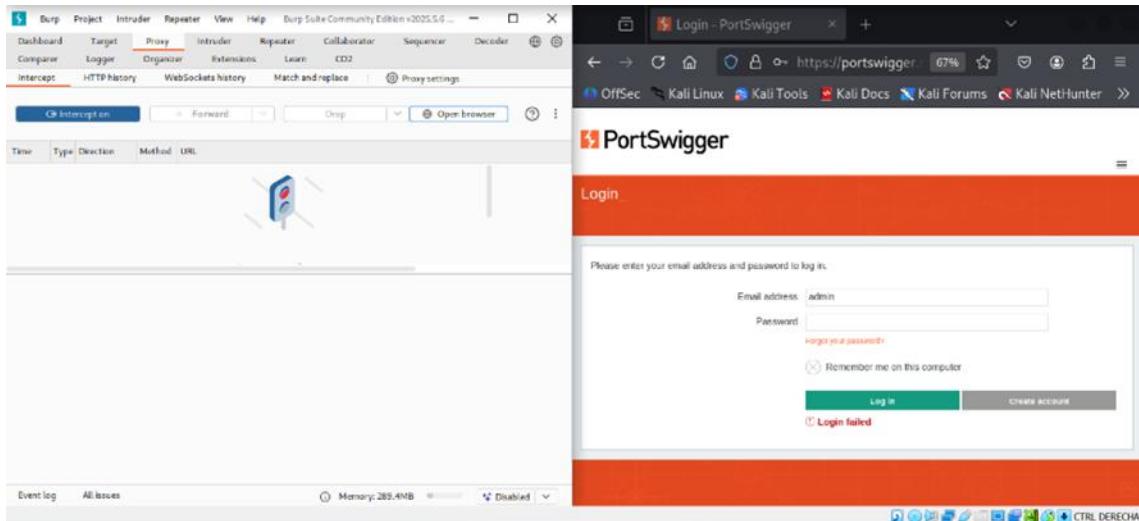
The screenshot shows two windows side-by-side. On the left is the Burp Suite interface, specifically the 'Proxy' tab. It displays a list of network requests and captures. One capture is selected, showing a POST request to 'https://ps.pwjk.pro/pwjk.php'. The request details pane shows the method as POST, URL as 'https://ps.pwjk.pro/pwjk.php', and various headers including 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' and 'Content-Length: 685'. The body parameters pane shows a single parameter named 'username' with the value 'guest'. On the right is a web browser window titled 'Login - PortSwigger' showing a login form for 'PortSwigger'. The form has fields for 'Email address' (containing 'guest') and 'Password' (containing '***'). Below the form are links for 'Remember me on this computer', 'Log In...', and 'Create account'.

5. Modifica el Parámetro username:

- Haz doble clic en el valor del parámetro username (que es guest).
- Cámbialo a **admin**.

6. Reenvía la Solicitud Modificada:

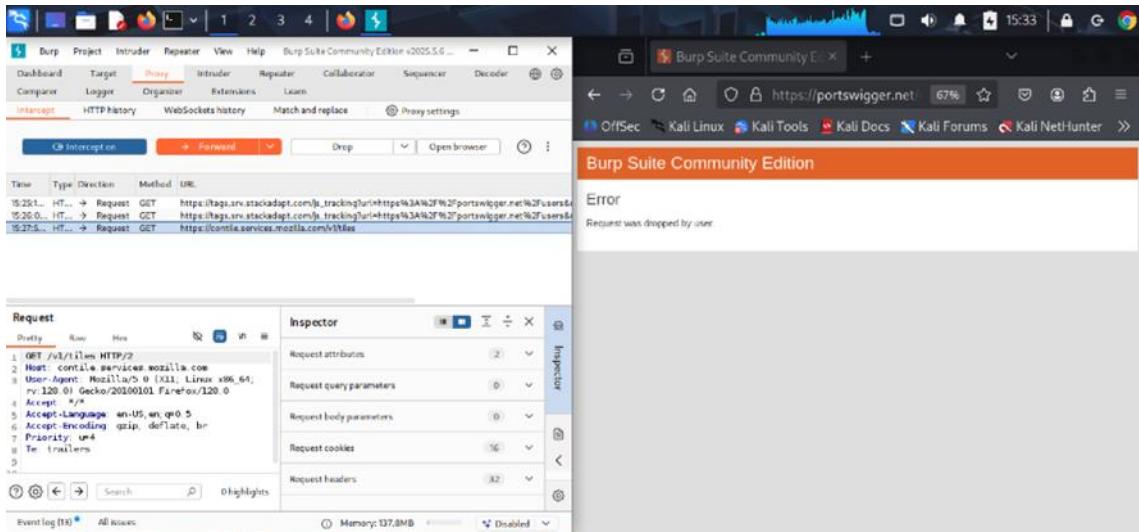
- Una vez que hayas realizado la modificación, haz clic en el botón **"Forward"** en Burp Suite. Esto enviará la solicitud modificada (con username=admin) al servidor web.
- Haz clic en "Forward" para cualquier otra solicitud que se intercepte hasta que la página se cargue en el navegador.



5.2.1. Reenviando la solicitud modificada (“Forward”)

El botón "Forward" es tu puerta de salida de la intercepción. Cada vez que Burp detiene una solicitud (o una respuesta), tú debes decidir si la envías tal cual, la modificas y la envías, o la "sueltas" (drop), lo que significa que no se envía al destino y el navegador recibirá un error de conexión.

- **Forward:** Envía la solicitud/respuesta al destino.
- **Drop:** Descarta la solicitud/respuesta. El navegador recibirá un error.



- **Action:** Despliega un menú con más opciones, como enviar la solicitud a otras herramientas de Burp (Repeater, Intruder, etc.), lo cual veremos más adelante.

5.3. Explorando el Historial HTTP

Aunque el "**Intercept**" te permite ver el tráfico en tiempo real, Burp Suite también mantiene un registro exhaustivo de todo el tráfico que pasa por el proxy, incluso cuando la intercepción está desactivada. Este registro se encuentra en la pestaña "**HTTP history**".

5.3.1. Revisando solicitudes y respuestas pasadas en "HTTP history"

- Desactiva la Intercepción:** Para permitir que tu navegador funcione normalmente y evitar detener cada solicitud, ve a la pestaña **Proxy -> Intercept** y haz clic en el botón "**Intercept is on**" para que cambie a "**Intercept is off**".
- Navega libremente:** Ahora puedes navegar por el sitio web de prueba.
- Explora "HTTP history":** Vuelve a Burp Suite y haz clic en la pestaña "**Proxy**", luego en la subpestana "**HTTP history**".
 - Verás una tabla con todas las solicitudes HTTP/S que han pasado por Burp, ordenadas cronológicamente.

The screenshot shows the Burp Suite interface with the "HTTP history" tab selected. The main window displays a table of network interactions, each row representing a single request or response. The columns include: ID, Host, Method, URL, Params, Edited, Status code, Length, HTTP type, References, File, Notes, TS, IP, Cookies, Time, and Listener port. Below the table, there's a status bar showing "Event log [0]" and "All issues". At the bottom, there are various tool icons and a memory usage indicator.

ID	Host	Method	URL	Params	Edited	Status code	Length	HTTP type	References	File	Notes	TS	IP	Cookies	Time	Listener port
1	https://portswigger.net	GET	/asusturum/%2fusers%2fyo... ✓			200	24307	HTML		Logon - PortSwigge...	✓	18.67.240.104	SessionID=0016...	15:11:34 20...	\$000	
2	https://burpselfservice.mos...	GET	/-1.html			200	65054	HTML			✓	34.26.137.309		15:11:34 20...	\$000	
3	https://openqa.gentoo.org	POST	/apiclient			200	3940	JSON			✓	34.26.137.309		15:11:34 20...	\$000	
4	https://content-signature-2...	GET	/yjchalmz0204023remote-setti...			200	3831	text	chart		✓	34.26.137.309		15:11:34 20...	\$000	
5	https://adobea.mozilla.org	GET	/			301	1474	HTML			✓	151.101.3.31		15:11:35 20...	\$000	
6	https://adobea.mozilla.org	GET	/AdobeaMozilla/5.0(Linux; U; ...			200	341	HTML			✓	34.26.137.309		15:11:35 20...	\$000	
7	https://adobea.mozilla.org	GET	/AdobeaMozilla/5.0(Linux; U; ...			200	216	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
8	http://172.17.0.1:8080/	GET	/avicecess%2f3p04			200	216	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
9	http://172.17.0.1:8080/	GET	/avicecess%2f3p04			200	216	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
10	http://172.17.0.1:8080/	GET	/avicecess%2f3p04			200	240	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
11	https://adobe-img.mozilla.org	GET	/AdobeaMozilla/5.0(Linux; U; ...			200	255	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
12	https://adobe-img.mozilla.org	GET	/AdobeaMozilla/5.0(Linux; U; ...			204	253	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
13	https://adobe-img.mozilla.org	GET	/AdobeaMozilla/5.0(Linux; U; ...			204	205	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
14	https://adobe-img.mozilla.org	GET	/AdobeaMozilla/5.0(Linux; U; ...			204	205	text	text		✓	34.26.137.309		15:11:35 20...	\$000	
15	https://portswigger.net	GET	/bananamap/bananamap/comme...			200	2740	XML	xml		✓	18.67.240.104	AVISAL3APP-0...	15:12:04 20...	\$000	
16	https://portswigger.net	GET	/bananamap/bananamap/comme...			200	5424	XML	xml		✓	18.67.240.104	AVISAL3APP-0...	15:12:04 20...	\$000	
17	https://portswigger.net	GET	/bananamap/bananamap/comme...			200	36259	HTML	xml	banner-map-orange.c...	✓	18.67.240.104	AVISAL3APP-0...	15:12:05 20...	\$000	
18	https://portswigger.net	GET	/bananamap/bananamap/comme...			200	3670	XML	xml		✓	18.67.240.104	AVISAL3APP-0...	15:12:05 20...	\$000	
19	https://portswigger.net	GET	/			101	240	text	text		✓	34.26.137.309		15:12:05 20...	\$000	
20	https://portswigger.net	GET	/bananamap/bananamap/comme...			200	240	text	text		✓	34.26.137.309		15:12:05 20...	\$000	
21	https://portswigger.net	GET	/bananamap/bananamap/comme...			200	240	text	text		✓	34.26.137.309		15:12:05 20...	\$000	
22	https://portswigger.net	GET	/			101	240	text	text		✓	34.26.137.309		15:12:05 20...	\$000	
23	https://sys.pwktk.pro	GET	/sys.php			200	439	HTML	php		✓	34.26.137.309		15:12:05 20...	\$000	
24	https://sys.pwktk.pro	GET	/sys.php?uri=http%3A%2F%2F...			204	225	text	text		✓	34.26.137.309		15:12:05 20...	\$000	
25	https://sys.pwktk.pro	POST	/sys?uri=http%3A%2F%2Fuser%3f%			200	5231	JSON			✓	18.67.240.104	AVISAL3APP-0...	15:12:35 20...	\$000	
26	https://sys.pwktk.pro	POST	/sys?uri=http%3A%2F%2Fuser%3f%			200	5231	JSON			✓	18.67.240.104	AVISAL3APP-0...	15:12:35 20...	\$000	
27	https://sys.pwktk.pro	POST	/sys?uri=http%3A%2F%2Fuser%3f%			204	1307	text	text		✓	34.26.137.309		15:12:35 20...	\$000	
28	https://sys.pwktk.pro	GET	/sys.php			204	127	text	text		✓	34.26.137.309		15:12:35 20...	\$000	
29	https://portswigger.net	POST	/bananamap/bananamap/comme...			200	5231	JSON			✓	18.67.240.104	AVISAL3APP-0...	15:13:48 20...	\$000	
30	https://portswigger.net	POST	/bananamap/bananamap/comme...			200	5231	JSON			✓	18.67.240.104	AVISAL3APP-0...	15:13:48 20...	\$000	
31	https://portswigger.net	POST	/bananamap/bananamap/comme...			200	5231	JSON			✓	18.67.240.104	AVISAL3APP-0...	15:13:48 20...	\$000	
32	https://portswigger.net	POST	/bananamap/bananamap/comme...			200	5231	JSON			✓	18.67.240.104	AVISAL3APP-0...	15:13:48 20...	\$000	

- Haz clic en cualquier fila de la tabla para ver los detalles completos de esa solicitud y su respuesta asociada en el panel inferior. Esto incluye las vistas "Raw", "Headers", "Params", etc., tanto para la solicitud (Request) como para la respuesta (Response).

The screenshot shows the Burp Suite interface with the "HTTP history" tab selected. The main area displays a table of captured requests with columns for Host, Method, URL, Params, Edited, Status code, Length, MIMI type, Extension, Title, Notes, TLS, IP, Cookies, Time, and Listener port. Below the table, there are "Request" and "Response" tabs with their respective content panes. To the right, there is an "Inspector" pane with sections for Request attributes, Request query parameters, Request headers, and Response headers. At the bottom, there's an event log and a status bar indicating memory usage.

5.3.2. Filtrando y buscando en el historial

El historial puede volverse muy largo en sitios complejos. Burp Suite ofrece opciones de filtrado para ayudarte a encontrar lo que buscas.

- 1. Barra de Filtro:** En la parte superior de la tabla "HTTP history", verás una barra de filtro. Puedes hacer clic en ella para desplegar opciones.
- 2. Opciones de Filtrado Comunes:**

- Display Filter:** Permite filtrar por tipo de contenido (HTML, CSS, imágenes), códigos de estado (200 OK, 404 Not Found), tipo de solicitud (GET, POST), y si están en el alcance del "Target scope" (veremos esto más adelante).
- Search:** Puedes buscar texto específico dentro de las solicitudes y respuestas del historial. Muy útil para encontrar cadenas como "password", "token", o nombres de funciones específicas.

This screenshot shows the "HTTP history" table with a filter dialog box overlaid. The dialog has several sections: "Settings mode" (selected), "Bambella mode", "Filter by request type" (checkboxes for Show only in-scope items, Hide items without responses, Show only parameterized requests), "Filter by MIME type" (checkboxes for HTML, Script, XML, CSS, Other text, Images, Flash, and Other binary), "Filter by status" (checkboxes for 2xx [Success], 3xx [Redir], 4xx [Request], and 5xx [Server]), and "Filter by search term" (text input for "RegEx" and "Case sensitive", checkboxes for "Show only" and "Hide" specific file extensions like .asp, .mprx, .php, .js, .sql, .jpg, .png, .css). At the bottom of the dialog are "Show all", "Helpful", "Revert changes", "Cancel", "Apply", and "Apply & Close" buttons. The main table below shows a list of captured requests with columns for Type, Extension, Title, Notes, TLS, IP, Cookies, Time, and Listener port.

Con esto, has completado la guía de uso básico de Burp Suite. Ahora sabes cómo interceptar tráfico, modificar solicitudes y revisar el historial. ¡Esta es la base para casi todas las pruebas de seguridad web que realizarás con Burp!

5. Herramientas Fundamentales de Burp Suite

Además del Proxy, Burp Suite ofrece una suite de herramientas integradas, cada una diseñada para una tarea específica en el proceso de prueba de penetración web. Nos centraremos en **Repeater** e **Intruder**, que son cruciales para el análisis manual y la automatización de ataques.

6.1. Burp Repeater: Modificando y Reenviando Solicitudes Manualmente

Repeater es una herramienta fundamental para la manipulación manual de solicitudes HTTP/S. Te permite tomar una solicitud que has interceptado (o de tu historial), modificarla a tu gusto y reenviarla al servidor repetidamente, observando las respuestas en tiempo real. Es ideal para probar diferentes entradas, parámetros o encabezados para descubrir cómo reacciona la aplicación.

6.1.1. ¿Para qué sirve Repeater?

- **Prueba de vulnerabilidades de inyección:** Modificar valores de parámetros para probar inyecciones SQL, XSS, Command Injection, etc.
- **Enumeración:** Cambiar IDs de usuarios, productos o recursos para ver si puedes acceder a información no autorizada.
- **Análisis de lógica de negocio:** Experimentar con diferentes flujos de datos para entender cómo la aplicación procesa la información.
- **Depuración:** Enviar solicitudes específicas para depurar el comportamiento de la aplicación.

6.1.2. Cómo enviar una solicitud a Repeater

La forma más común de usar Repeater es enviándole una solicitud que ya has capturado.

1. Intercepta una solicitud (o usa el historial):

- Asegúrate de que tu navegador esté configurado para Burp Proxy y navega a un sitio web de prueba (ej. un laboratorio de PortSwigger Web Security Academy).

- Puedes interceptar una solicitud en la pestaña **Proxy -> Intercept** o seleccionar una solicitud de la pestaña **Proxy -> HTTP history**.

2. Envía la solicitud a Repeater:

- Una vez que tengas la solicitud visible (ya sea interceptada o seleccionada del historial), haz **clic derecho** sobre ella.
- En el menú contextual, selecciona "**Send to Repeater**" (Enviar a Repeater).

3. Accede a la pestaña Repeater:

- Ahora, haz clic en la pestaña "**Repeater**" en la interfaz principal de Burp Suite. Verás la solicitud que enviaste en una nueva pestaña numerada dentro de Repeater.

6.1.3. Usando Repeater: Modificar y Enviar

Dentro de la pestaña Repeater, la interfaz se divide en dos paneles principales:

- **Panel de Solicitud (Request):** Aquí verás la solicitud HTTP/S que enviaste. Puedes editar cualquier parte de ella: URL, encabezados, cuerpo (POST data), parámetros GET, etc.
- **Panel de Respuesta (Response):** Despues de enviar la solicitud, la respuesta del servidor aparecerá aquí. Puedes verla en formato "Raw", "Pretty" (formateada), "Headers", "Hex", o incluso "Render" (para ver cómo se vería en un navegador, útil para XSS).

Pasos para usar Repeater:

1. **Modifica la solicitud:** En el panel "Request", realiza los cambios que deseas. Por ejemplo, si la solicitud es un GET a /product?id=123, puedes cambiar id=123 a id=124 o id=admin. Si es un POST con datos de formulario, puedes modificar los valores de los campos.
2. **Envía la solicitud:** Haz clic en el botón "**Send**" (Enviar) en la parte superior del panel "Request".
3. **Analiza la respuesta:** La respuesta del servidor aparecerá en el panel "Response". Examina si tus cambios tuvieron algún efecto. ¿Obtuviste un error? ¿Accediste a nueva información? ¿La página se comportó de manera diferente?
4. **Repite el proceso:** Puedes seguir modificando la solicitud y haciendo clic en "Send" cuantas veces quieras, lo que hace a Repeater increíblemente útil para el "fuzzing" manual y la prueba iterativa.

6.2. Burp Intruder: Automatizando Ataques Personalizados (con limitaciones en Community Edition)

Intruder es una herramienta potente para automatizar ataques personalizados contra aplicaciones web. Permite enviar un gran número de solicitudes modificadas de forma sistemática, lo que es ideal para tareas como el "brute-forcing" de contraseñas, la enumeración de usuarios, el "fuzzing" de parámetros o la detección de vulnerabilidades basadas en respuestas.

¡Importante para la Community Edition! La versión gratuita de Burp Suite (Community Edition) tiene **limitaciones significativas** en Intruder:

- **Velocidad limitada:** Los ataques son intencionadamente lentos.
- **Funcionalidad reducida:** Algunas opciones avanzadas y tipos de ataque no están disponibles.
- **Sin guardado de sesión:** No puedes guardar tus proyectos de Intruder.

A pesar de estas limitaciones, Intruder en la Community Edition sigue siendo útil para entender su funcionamiento y realizar pruebas a pequeña escala.

6.2.1. ¿Para qué sirve Intruder?

- **Brute-forcing de credenciales:** Probar combinaciones de usuario/contraseña.
- **Enumeración de usuarios/recursos:** Descubrir usuarios válidos o recursos ocultos.
- **Fuzzing:** Enviar entradas inesperadas o malformadas para encontrar errores o vulnerabilidades.
- **Ataques de diccionario:** Usar listas de palabras para probar parámetros o encabezados.

6.2.2. Cómo enviar una solicitud a Intruder

Al igual que con Repeater, el primer paso es enviar una solicitud a Intruder.

1. **Intercepta una solicitud (o usa el historial):**
 - Captura una solicitud relevante (ej. una solicitud POST de login) en **Proxy -> Intercept** o selecciónala de **Proxy -> HTTP history**.
2. **Envía la solicitud a Intruder:**
 - Haz **clic derecho** sobre la solicitud.
 - Selecciona "**Send to Intruder**" (Enviar a Intruder).

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the center pane, a list of captured HTTP requests is displayed. A specific request is selected, and a context menu is open over it. The 'Send to Intruder' option is highlighted with a red box. Other options in the menu include 'Send to Repeater', 'Send to Sequence', 'Send to Organizer', 'Send to Computer (request)', 'Send to Computer (response)', 'Show response in browser', 'Request in browser', 'Pretty / Raw', 'Engagement tools (Pro version only)', 'Show new history window', 'Add notes', 'Highlight', 'Delete item', 'Clear history', 'Copy URL', 'Copy as curl command (bash)', 'Copy links', 'Save item', and 'Event log (IT)'. To the right of the list, there is an 'Inspector' panel showing detailed information about the selected request.

3. Accede a la pestaña Intruder:

- Haz clic en la pestaña "Intruder" en la interfaz principal de Burp Suite. Verás la solicitud en la subpestana "Positions".

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. Within the 'Intruder' tab, the 'Positions' subtab is active. It displays a list of parameters from a selected request, each with its current value and a 'Replace' field where payloads can be entered. To the right of this list, there is a 'Payloads' section containing a large blue rocket icon. Below the rocket, text reads 'To get started, highlight the part of the request or target you want to replace, then click Add \$ to set a payload position.' At the bottom of the 'Payloads' section, there is a note: 'Event log (IT) All issues' and 'Memory: 140.2MB Disabled CTRL DERECHA'.

6.2.3. Usando Intruder: Posiciones, Payloads y Tipos de Ataque

La configuración de un ataque en Intruder implica varios pasos clave:

1. Pestaña "Positions" (Posiciones):

- Aquí defines dónde Intruder insertará tus "payloads" (las cadenas de texto que quieras probar).
- Burp Suite intentará adivinar automáticamente las posiciones de los parámetros y las marcará con símbolos **\$**.

- **"Clear \$"**: Haz clic en este botón para eliminar todas las marcas de posición automáticas.
- **"Add \$"**: Selecciona el texto en la solicitud que quieras que sea una posición de payload y haz clic en "Add \$".
- **"Auto \$"**: Vuelve a intentar el marcado automático de posiciones.
- **Ejemplo:** Para un ataque de fuerza bruta de contraseña, solo querías que la posición del payload fuera el valor del parámetro password.

2. Pestaña "Attack type" (Tipo de ataque):

- Define cómo se combinan los payloads si tienes múltiples posiciones.
- **Sniper (Francotirador)**: El más común. Utiliza un único conjunto de payloads y los inserta, uno por uno, en cada posición de payload definida. Ideal para probar una lista de payloads contra múltiples puntos de inyección.
- **Battering Ram (Ariete)**: Utiliza un único conjunto de payloads y los inserta *simultáneamente* en *todas* las posiciones de payload definidas.
- **Pitchfork (Horca)**: Utiliza múltiples conjuntos de payloads (uno por cada posición) y los inserta simultáneamente, tomando el primer payload de cada conjunto, luego el segundo, y así sucesivamente.
- **Cluster Bomb (Bomba de racimo)**: Utiliza múltiples conjuntos de payloads y los inserta en *todas las combinaciones posibles*. Muy potente, pero también muy lento (especialmente en Community Edition) y genera mucho tráfico.

3. Pestaña "Payloads":

- Aquí defines las listas de payloads que Intruder utilizará.
- **Payload options**: Puedes cargar payloads desde un archivo (ej. una lista de contraseñas o nombres de usuario), o añadir payloads manualmente.
- **Payload processing**: Puedes aplicar reglas a tus payloads (ej. codificar URL, añadir prefijos/sufijos).
- **Payload settings**: (Más avanzado) Configura cómo se generan los payloads (ej. números secuenciales, caracteres aleatorios).

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the main pane, there is a list of captured requests. A red arrow points from the top of the list to the 'Payloads' panel on the right. The 'Payloads' panel has 'Payload type: Simplelist' selected. It contains three entries: '1234', 'holo', and 'admin'. Another red arrow points from the bottom of the payload list back to the main request list.

4. Pestaña "Options" (Opciones):

- Configuraciones generales del ataque, como el número de hilos (threads), el manejo de errores, las reglas de "grep" (para buscar cadenas específicas en las respuestas) y la configuración de redirecciones.

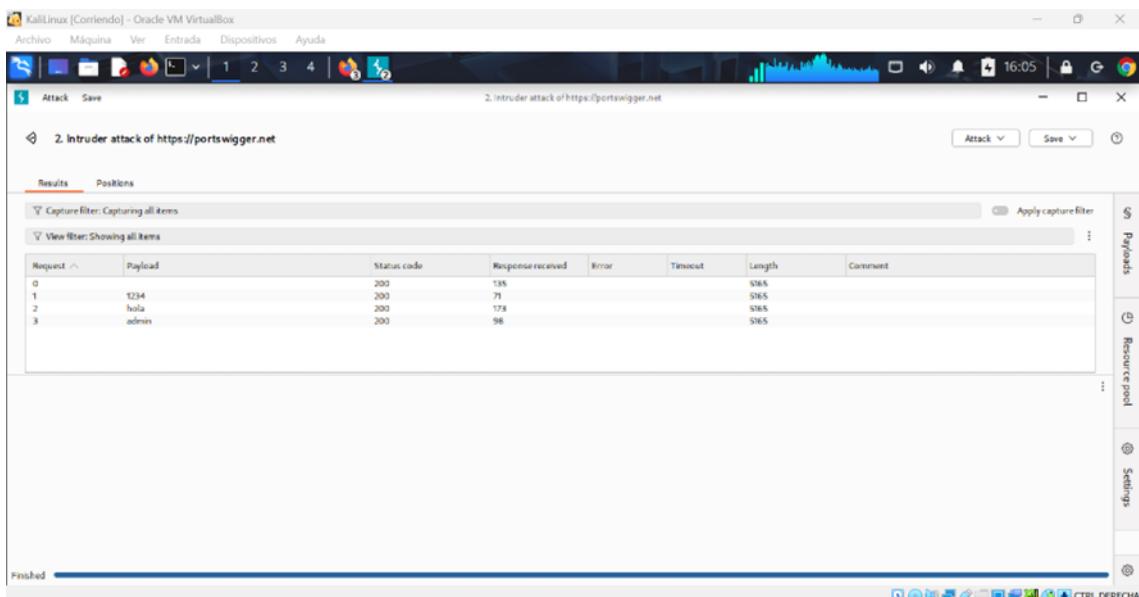
5. Iniciar el Ataque:

- Una vez configurado, haz clic en el botón "**Start attack**" (Iniciar ataque) en la esquina superior derecha de la pestaña Intruder.
- Advertencia:** En la Community Edition, te recordará las limitaciones de velocidad.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A large red arrow points directly at the 'Start attack' button located in the top right corner of the main workspace.

6. Analizar los Resultados:

- Se abrirá una nueva ventana con los resultados del ataque. Verás una tabla con cada solicitud enviada, su payload, el código de estado de la respuesta, el tamaño de la respuesta, y otros detalles.
- Puedes ordenar las columnas (por ejemplo, por tamaño de respuesta o código de estado) para identificar respuestas interesantes que puedan indicar una vulnerabilidad (ej. un tamaño de respuesta diferente para un usuario válido vs. inválido).
- Al hacer clic en una fila, puedes ver la solicitud y la respuesta completas para esa entrada específica.

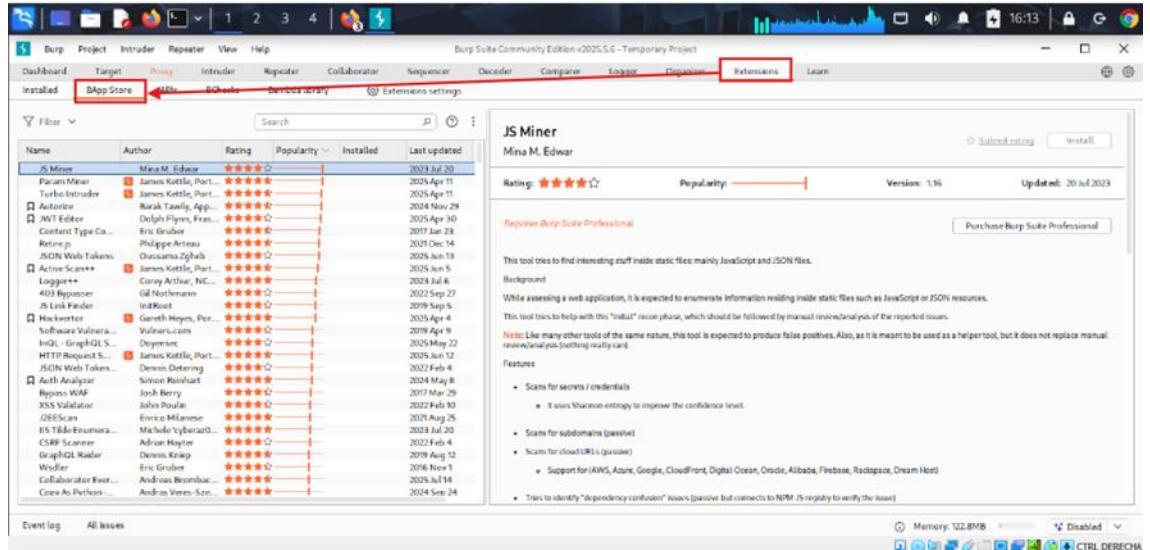


6.3. Otras Herramientas de Burp Suite (Mención)

Aunque Proxy, Repeater e Intruder son las más usadas para empezar, Burp Suite Professional incluye muchas otras herramientas potentes:

- **Dashboard:** Muestra un mapa del sitio web que estamos probando, con todas las URLs descubiertas y sus detalles.
- **Target:** Punto de partida para cualquier prueba de seguridad web. Nos da una visión general y detallada de la aplicación web que probamos.
- **Scanner (Solo Pro):** Un escáner de vulnerabilidades automatizado que busca fallos comunes en aplicaciones web.
- **Sequencer (Solo Pro):** Analiza la aleatoriedad de tokens de sesión y otros valores importantes.
- **Decoder:** Permite codificar y decodificar datos en varios formatos (URL, HTML, Base64, etc.).

- **Comparer:** Compara dos solicitudes o respuestas byte a byte para identificar diferencias sutiles.
- **Extender:** Permite cargar extensiones (BApps) para añadir funcionalidades personalizadas a Burp Suite o crear nuestros propios plugins.



Con **Repeater** e **Intruder**, tienes las herramientas para llevar tus pruebas de seguridad web al siguiente nivel, permitiéndote manipular y automatizar interacciones con las aplicaciones.

7. Anexo 1: Solución de Problemas Comunes

Es habitual encontrarse con pequeños obstáculos al principio al configurar herramientas como Burp Suite. No te preocupes, la mayoría de los problemas tienen soluciones sencillas. Aquí te presentamos los inconvenientes más frecuentes y cómo abordarlos.

7.1. El navegador no se conecta al proxy de Burp

Este es, con diferencia, el problema más común al configurar Burp Suite por primera vez. Si tu navegador muestra errores de conexión o simplemente no carga ninguna página, es probable que haya un problema con la configuración del proxy.

Posibles causas y soluciones:

1. Burp Suite no está escuchando (Proxy Listener inactivo):

- **Verificación:** En Burp Suite, ve a la pestaña **Proxy** y luego a la subpestana **Options**. En la sección "Proxy Listeners", asegúrate de que el listener en 127.0.0.1:8080 esté marcado como "**Running**" (Ejecutando). Si no lo está, marca la casilla.

- **Solución:** Activa el listener. Si no aparece, créalo usando el botón "Add".

2. El navegador no está configurado para usar el proxy de Burp:

- **Verificación:** Vuelve a revisar la configuración del proxy en tu navegador.
 - **Navegador integrado de Burp:** Si usas el navegador integrado, este problema es raro, ya que viene preconfigurado. Asegúrate de que lo abres desde el botón "Open browser" en la pestaña "Intercept".
 - **Firefox:** Ve a Settings > General > Network Settings > Settings... y confirma que "Manual proxy configuration" esté activado con 127.0.0.1 y puerto 8080 para HTTP y SSL.
 - **Chrome (con FoxyProxy):** Haz clic en el ícono de FoxyProxy y asegúrate de que el perfil "Burp Suite" (o como lo hayas nombrado) esté seleccionado y activo.
- **Solución:** Corrige cualquier error en la dirección IP o el puerto del proxy en tu navegador. Asegúrate de que no haya otros proxies o VPNs activas que puedan interferir.

3. El "Intercept" de Burp Suite está "On":

- **Verificación:** Cuando el botón "Intercept is on" en la pestaña **Proxy** > **Intercept** está activo, Burp detiene *todas* las solicitudes hasta que las reenvías manualmente. Si no estás esperando interceptar algo específico, el navegador parecerá que no carga nada.
- **Solución:** Si solo quieres que el tráfico fluya, asegúrate de que el botón diga "**Intercept is off**". Siempre puedes activarlo cuando quieras capturar una solicitud específica.

4. Firewall bloqueando la conexión:

- **Verificación:** Tu sistema operativo o un software de firewall (incluido el de Kali Linux, si lo has configurado) podría estar bloqueando las conexiones al puerto 8080 o las comunicaciones entre el navegador y Burp.
- **Solución:** Desactiva temporalmente el firewall para probar. Si funciona, deberás añadir una regla para permitir la conexión en el puerto 8080 para Burp Suite. En Kali Linux, si usas ufw: sudo ufw allow 8080/tcp.

7.2. Errores de certificado HTTPS

Cuando intentas acceder a un sitio HTTPS a través de Burp Suite y ves advertencias de seguridad como "Su conexión no es privada", "Riesgo potencial de seguridad" o "NET::ERR_CERT_AUTHORITY_INVALID", significa que tu navegador no confía en el certificado SSL que Burp Suite le está presentando. Esto ocurre porque Burp está actuando como intermediario y generando sus propios certificados para el tráfico cifrado.

Posibles causas y soluciones:

1. El Certificado CA de Burp no está instalado o no es de confianza:

- **Verificación:** Vuelve a los pasos de la Sección 2.3.1 (para Firefox) o 2.3.2 (para Chrome/Sistema). Asegúrate de haber descargado el certificado cacert.der de <http://burpsuite/> y lo hayas importado como una "**Autoridad de Certificación de confianza**".
- **Solución:** Reinstala el certificado CA de Burp Suite siguiendo los pasos exactos. Asegúrate de marcar la opción de "Confiar en esta CA" para identificar sitios web" al importarlo.

2. Usando el navegador integrado de Burp y aún así hay problemas:

- **Verificación:** Si estás usando el navegador integrado y aún así ves advertencias, puede que la versión de Burp Suite no esté manejando correctamente los certificados para ese sitio en particular, o que haya un problema en tu entorno.
- **Solución:** Reinicia Burp Suite y/o el navegador integrado. A veces, un simple reinicio resuelve problemas temporales.

3. Certificado de navegador obsoleto o corrupto:

- **Verificación:** En casos muy raros, tu almacén de certificados del navegador podría estar corrupto.
- **Solución:** Intenta usar un navegador diferente que no esté configurado para Burp para ver si el problema persiste. Si no, considera reiniciar el perfil de tu navegador o reinstalarlo como último recurso.

7.3. Burp Suite no inicia o da errores de Java

Si Burp Suite no se lanza en absoluto, se cierra inesperadamente o muestra mensajes de error relacionados con Java, es probable que tengas un problema con tu instalación de Java o con la forma en que Burp Suite intenta usarlo.

Posibles causas y soluciones:

1. Versión de Java incorrecta o no instalada:

- **Verificación:** Burp Suite requiere **Java Runtime Environment (JRE) versión 11 o superior**. Abre una terminal y ejecuta `java -version`.
- **Solución:** Si Java no está instalado o es una versión anterior a la 11, instala la versión correcta. En Kali Linux, puedes usar `sudo apt install default-jre -y` para instalar la versión predeterminada (que suele ser 11+).

2. Problemas con la ruta de Java (PATH):

- **Verificación:** Aunque es menos común con los instaladores modernos, la variable de entorno PATH podría no estar apuntando a la instalación correcta de Java.
- **Solución:** Si has instalado Java manualmente o tienes varias versiones, asegúrate de que la versión 11 o superior sea la predeterminada o especifica la ruta completa al ejecutable de Java al lanzar Burp. Por ejemplo, si tienes Java en `/usr/lib/jvm/java-11-openjdk-amd64/bin/java`, podrías intentar `sudo /usr/lib/jvm/java-11-openjdk-amd64/bin/java -jar /path/to/burpsuite.jar` (si usaste el archivo JAR en lugar del instalador).

3. Archivos de Burp Suite dañados:

- **Verificación:** Si el instalador se descargó de forma incompleta o fue corrompido.
- **Solución:** Descarga el instalador de Burp Suite Community Edition nuevamente desde la página oficial de PortSwigger y vuelve a intentar la instalación.

4. Permisos insuficientes para el instalador/ejecutable:

- **Verificación:** En Linux, si no le diste permisos de ejecución al script `.sh` o no lo ejecutaste con `sudo`.
- **Solución:** Asegúrate de ejecutar `chmod +x burpsuite_community_linux_v*.sh` antes de `sudo ./burpsuite_community_linux_v*.sh` al instalar. Para ejecutar Burp después, el acceso directo debería funcionar, o puedes usar `burpsuite` desde la terminal.

8. Consejos Adicionales para Tu Trayectoria con Burp Suite

Dominar Burp Suite es un proceso continuo. Aquí tienes algunos consejos para seguir mejorando tus habilidades:

1. **Practica Constantemente:** La clave para dominar Burp Suite es la práctica. Sigue utilizando los **laboratorios de PortSwigger Web Security Academy** y explora otros entornos vulnerables como **DVWA** o **bWAPP**. Cada laboratorio te presentará un desafío nuevo y te obligará a usar Burp Suite de diferentes maneras.
2. **Entiende HTTP/S a Fondo:** Burp Suite es una herramienta HTTP/S. Cuanto mejor entiendas los **conceptos de HTTP/S** (métodos, encabezados, códigos de estado, cookies, sesiones, etc.), más eficaz serás usando Burp Suite para identificar y explotar vulnerabilidades. Dedica tiempo a aprender cómo funciona la web "por debajo".
3. **Explora el "Scope" (Alcance) en la Pestaña "Target":** Aunque no lo cubrimos en detalle, la pestaña "**Target**" y su subpestaña "**Scope**" son muy importantes. Configurar un alcance adecuado te ayuda a **filtrar el tráfico relevante** y a evitar la intercepción de sitios o recursos innecesarios, lo que mantiene tu historial más limpio y tu enfoque claro. Es una de las mejores prácticas para un trabajo eficiente.
4. **Aprende de las Respuestas:** No te centres solo en las solicitudes que envías. La **respuesta del servidor** es igual de importante. Busca cambios en el código de estado, el tamaño de la respuesta, los mensajes de error o la presencia de información sensible para identificar posibles vulnerabilidades.
5. **Utiliza las "Actions" (Acciones):** Cuando haces clic derecho en una solicitud (ya sea en Intercept o en HTTP History), verás un menú de "**Action**". Este menú es tu puerta de entrada para enviar esa solicitud a otras herramientas de Burp (Repeater, Intruder, Decoder, Comparer). Familiarízate con él.
6. **Mantente al Día:** La seguridad web evoluciona constantemente. Asegúrate de **actualizar Burp Suite regularmente** para obtener las últimas características y parches. Sigue los blogs de seguridad y los canales de PortSwigger para mantenerte informado sobre las nuevas técnicas y vulnerabilidades.

7. **Explora la Documentación Oficial:** PortSwigger ofrece una **documentación muy completa** para Burp Suite. Si tienes dudas sobre una función o quieres profundizar, la documentación oficial es tu mejor amiga: <https://portswigger.net/burp/documentation>.
8. **Considera Burp Suite Professional (a futuro):** Si te dedicas profesionalmente al pentesting, la versión **Professional** ofrece un valor inmenso con su **escáner de vulnerabilidades automatizado** (Scanner), funciones avanzadas de Intruder, Sequencer, y muchas otras características que acelerarán y mejorarán tus pruebas.

Recursos Adicionales:

- **Documentación Oficial de PortSwigger:** portswigger.net/burp/documentation
- **PortSwigger Web Security Academy:** portswigger.net/web-security (laboratorios interactivos para practicar vulnerabilidades).
- **Tutoriales en Video:**
<https://www.youtube.com/watch?v=7qMJAkxZI0I>
<https://www.youtube.com/watch?v=nVTEYdZo28U>

Caido: Un Nuevo Contendiente

Caido es una herramienta moderna para pentesters y auditores de seguridad web que ha surgido como un serio competidor para el clásico Burp Suite. Desarrollada en Rust, destaca por su alto rendimiento, estabilidad y una interfaz gráfica intuitiva que facilita el análisis de aplicaciones web, APIs REST y entornos GraphQL. Sus principales características son la facilidad de uso, la automatización avanzada de pruebas, la gestión eficiente de proyectos y funciones exclusivas orientadas a mejorar la productividad y la experiencia del pentester.

Funciones más llamativas:

- **Interfaz de Usuario (UI) Moderna**, muy intuitiva para usuarios de todos los niveles

- **Rendimiento:** muy eficiente y rápida, capaz de manejar grandes volúmenes de tráfico sin ralentizarse.
- **Enfoque en la Simplicidad y Eficiencia:** Busca agilizar el proceso de pentesting con flujos de trabajo eficientes.
- **Automatización integrada:** Ofrece capacidades de automatización avanzadas para pruebas de penetración.
- **Soporte avanzado para APIs:** Tiene un buen soporte para el análisis de APIs RESTful y GraphQL, algo cada vez más importante.
- **Versión Gratuita (Community):** automatización de pruebas similar al “Intruder”de Burp Suite, pero sin limitaciones en su versión gratuita.

Tabla de ventajas y desventajas: Caído vs Burp Suite

Característica	Caído	Burp Suite
Interfaz	Moderna, minimalista e intuitiva. Fácil para principiantes.	Completa, pero más densa y tradicional.
Automatización	Sin restricciones en la versión gratuita (“Automate”).	Limitada en la versión gratuita (Intruder limitado).
Gestión de proyectos	Puede manejar varios proyectos simultáneamente.	Requiere reinicios en la versión gratuita.

Proxy invisible	Sí, permite interceptar tráfico de clientes no configurables.	No disponible nativamente.
Sobrescritura de DNS	Sí, mayor control en resolución de dominios.	Limitado o más complejo.
Integración navegador	Sencilla y nativa, instalación rápida.	A través de extensiones y plugins.
Desempeño y Ligereza	Muy ligero y rápido, sin problemas de memoria.	Puede saturar recursos en grandes flujos.
Desarrollo de plugins	Plugins usando tecnologías web estándar (JS, HTML, CSS).	Plugins generalmente en Java.
Precio	Versión gratuita con funciones avanzadas, versión pro más económica.	Gratis limitado, versión Pro cara.
Madurez y comunidad	Creciente, en pleno desarrollo.	Amplia, madurez técnica y amplia documentación.
Compatibilidad	Multi-plataforma (Windows, Linux, Mac), despliegue sencillo.	Multi-plataforma, instalación conocida.

Soporte corporativo	Limitado, comunidad en expansión.	Soporte profesional por Portswigger.
---------------------	-----------------------------------	--------------------------------------