PASO 01

🖥️ Instalación de VirtualBox (El Hipervisor)

VirtualBox es un software de virtualización (hipervisor) que nos permite crear un "computador dentro de tu computador". Esto es fundamental en ciberseguridad: nos deja ejecutar sistemas operativos vulnerables y herramientas de hacking en un entorno controlado, sin arriesgar tu sistema operativo principal (Windows, macOS o Linux).

📥 Descarga e Instalación Base

Ve al sitio oficial `virtualbox.org` y descarga la versión para tu sistema operativo. Ejecuta el instalador y sigue los pasos por defecto. Cuando termine, te recomendamos descargar también el **VirtualBox Extension Pack** (desde la misma web), que añade soporte para USB 2.0/3.0 y otras funciones avanzadas.

💡 Requisitos de Hardware para un Laboratorio Estable

Para que todo funcione fluido, tu computadora física necesita **al menos 8 GB de RAM** (16 GB es lo ideal) y unos **60 GB de espacio libre en disco**. Además, debes tener la **virtualización activada en la BIOS/UEFI** de tu equipo (busca en el arranque opciones como "Intel VT-x", "AMD-V" o "SVM Mode" y actívalas).

🌐 Crear el Entorno Aislado (Red Host-Only)

En hacking ético, **jamás** debes conectar una máquina vulnerable a tu red doméstica real. Si un malware se escapa, podría infectar tu router o los dispositivos de tu casa. Para evitarlo, crearemos una red privada interna.

1. Abre VirtualBox y ve al menú superior **Archivo → Administrador de Red de Host**.
2. Haz clic en el botón **Crear** (o el ícono de "+").
3. Se creará una nueva interfaz de red (normalmente llamada `vboxnet0`) con una IP asignada, por ejemplo, `192.168.56.1`.
4. Haz clic en la pestaña **Servidor DHCP** y asegúrate de que la casilla **"Habilitar servidor"** esté marcada. Esto hará que las máquinas reciban IPs automáticas.

Esta red será el "cable" invisible que conectará a nuestro atacante (Kali) con nuestras víctimas (Metasploitable y DVWA).

PASO 02

🐉 Configurar Kali Linux (La Máquina Atacante)

Kali será nuestro equipo de trabajo. Lo configuraremos con dos tarjetas de red: una para que tenga internet y pueda descargar actualizaciones (NAT) y otra para que se conecte a nuestras víctimas en el laboratorio (Host-Only).

🛠️ Creación y Asignación de Recursos

1. En VirtualBox, haz clic en **Nueva**.
2. Nombre: `Kali-Linux`. Tipo: **Linux**. Versión: **Debian (64-bit)**.
3. Asigna **al menos 2048 MB de RAM** (si tienes 16 GB, puedes darle 4096 MB para mayor fluidez).
4. Selecciona **"Crear un disco duro virtual ahora"**. Tipo: VDI. Almacenamiento: **Dinámicamente asignado**. Tamaño: **80 GB**.

💿 Cargar la Imagen ISO e Instalar

Selecciona tu máquina Kali y ve a **Configuración → Almacenamiento**. Haz clic en el ícono de disco óptico vacío, selecciona "Elegir un archivo de disco óptico virtual" y busca la ISO de Kali descargada.

Inicia la máquina y elige **Graphical Install**. Sigue el asistente paso a paso:

- **Idioma:** Español (Colombia).
- **Teclado:** Español (Latinoamérica).
- **Red:** Nombre de host: `kali`.
- **Usuario:** Crea tu usuario y contraseña (anótalos bien).
- **Particionado:** "Guiado - utilizar todo el disco".

⚙️ Configuración de los Dos Adaptadores de Red

Una vez instalado, apaga la máquina virtual. Ve a **Configuración → Red**. Habilita dos adaptadores:

- **Adaptador 1:** `NAT`. Esto le da a Kali acceso a internet para que puedas ejecutar `sudo apt update` y descargar herramientas.
- **Adaptador 2:** `Adaptador solo-anfitrión` (Host-Only). Selecciona la red `vboxnet0` que creaste en el Paso 1. Esta es la red donde vivirá el ataque.

Al encender Kali, abre la terminal y ejecuta el comando `ip a`. Deberías ver dos interfaces: `eth0` (NAT) y `eth1` (Host-Only, con IP 192.168.56.x).

PASO 03

🎯 Desplegar Metasploitable 2 (Víctima Linux)

Metasploitable 2 es una máquina virtual de Ubuntu que ha sido intencionalmente diseñada con múltiples vulnerabilidades (puertos abiertos, contraseñas débiles, servicios desactualizados). Es el "conejillo de indias" perfecto para tus primeras pruebas de penetración.

📦 Importar el Disco Virtual

1. Descarga el archivo `.zip` de Metasploitable 2 desde la web de Rapid7 o SourceForge.
2. Descomprímelo en tu computadora. Verás una carpeta con un archivo de disco `.vmdk`.
3. En VirtualBox, haz clic en **Nueva**. Nombre: `Metasploitable2`. Tipo: Linux. Versión: **Ubuntu (64-bit)**. RAM: **1024 MB**.
4. En la pantalla del disco duro, selecciona **"Usar un archivo de disco duro virtual existente"** y busca el archivo `.vmdk` que descomprimiste.
5. Haz clic en Crear.

🔑 Configurar Red y Credenciales

Antes de iniciar, ve a **Configuración → Red**. Cambia el Adaptador 1 a **Adaptador solo-anfitrión (Host-Only)**. Es vital que esta máquina NO tenga NAT ni acceso a internet.

Inicia la máquina. Cuando pida login, usa las credenciales por defecto (tanto para usuario como para contraseña):

```
msfadmin login: msfadmin
Password: msfadmin
```

Una vez dentro, ejecuta el comando `ifconfig` en la terminal para ver la IP que te asignó la red Host-Only (ej. `192.168.56.102`). Anótala, la necesitarás para atacarla desde Kali.

PASO 04

🌐 Desplegar DVWA (Víctima Web)

Damn Vulnerable Web Application (DVWA) es una aplicación web llena de fallos de seguridad (Inyección SQL, XSS, inclusión de archivos, etc.). La usaremos para practicar hacking web. En lugar de instalar otra máquina virtual, la ejecutaremos con Docker directamente dentro de Kali para ahorrar recursos.

🐋 Instalar Docker en Kali

Docker es una plataforma de contenedores que permite ejecutar aplicaciones en entornos aislados. Abre la terminal en Kali y actualiza el sistema antes de instalar:

Terminal de Kali

```
kali@root:~$ sudo apt update && sudo apt upgrade -y
kali@root:~$ sudo apt install -y docker.io
kali@root:~$ sudo systemctl enable --now docker
```

🚀 Lanzar el Contenedor de DVWA

Ejecuta el siguiente comando. Docker descargará la imagen oficial y la pondrá a correr en el puerto 80 de tu máquina Kali:

Terminal de Kali

```
kali@root:~$
sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa
Unable to find image 'vulnerables/web-dvwa:latest' locally
latest: Pulling from vulnerables/web-dvwa
...
Status: Downloaded newer image for vulnerables/web-dvwa:latest
 * Running on http://0.0.0.0:80/
```

Ahora, abre el navegador Firefox dentro de Kali y ve a `http://localhost:80` (o `http://127.0.0.1`). Deberías ver la pantalla de login de DVWA. Las credenciales por defecto son:

```
Username: admin
Password: password
```

> 💡 **Entendiendo DVWA**
>
> DVWA corre dentro de tu propia máquina Kali. No necesitas una IP separada para ella; la atacarás desde la misma Kali usando `localhost` o `127.0.0.1`. Es ideal para practicar ataques web sin afectar a otros sistemas.

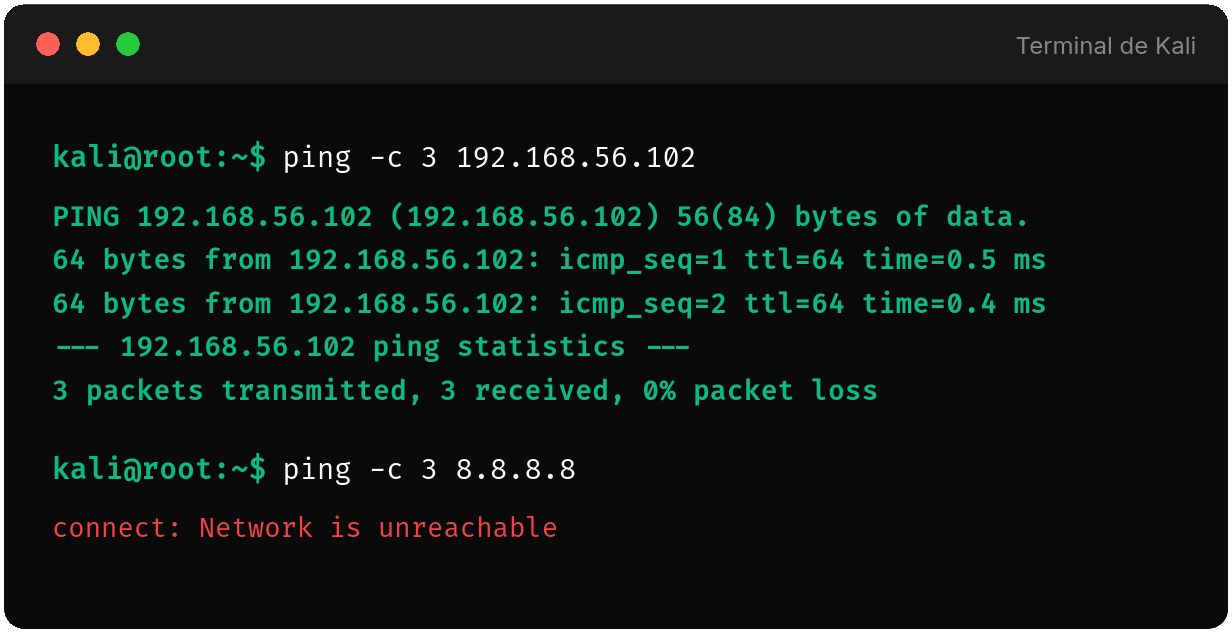
PASO 05

🔒 Verificación de Aislamiento (Prueba de Fuego)

El paso más importante para tu seguridad y la de tu red. Vamos a comprobar que Kali puede ver a las máquinas vulnerables, pero que el tráfico de ataque NO se escapa a tu red doméstica ni a internet.

🧪 Pruebas desde la Terminal de Kali

Ejecuta estos comandos y verifica los resultados. El primero comprueba la conectividad con la víctima, el segundo verifica que estás aislado de internet en esa interfaz:



Si el primer comando funciona (ves los paquetes de respuesta) y el segundo falla (*Network is unreachable*), **tu laboratorio está perfectamente aislado y listo para practicar**. Las máquinas vulnerables están en su propia "burbuja" sin acceso al mundo exterior.

🎓 ¡Laboratorio Listo!

Ya tienes tu entorno de pruebas con Kali (atacante), Metasploitable 2 (víctima de red) y DVWA (víctima web). En la próxima clase haremos el primer escaneo de puertos con Nmap y empezaremos a explotar Metasploitable 2.