
🧪 Guía Paso a Paso: Laboratorio de Pentesting con Kali Linux + DVWA

🛠️ Requisitos Previos

- PC o portátil con mínimo 8GB de RAM y 60GB de disco.
- VirtualBox o VMware instalado.
- ISO de **Kali Linux**.
- Imagen de **DVWA** (puede ser instalada sobre Ubuntu Server o usar una máquina ya configurada).
- Red en modo **“Red Interna”** o **NAT Network** para simular entorno real.

---

1. 📥 Descargar e instalar las máquinas virtuales

✅ Kali Linux

1. Descarga la imagen oficial desde: https://www.kali.org/get-kali/
2. Crea una VM en VirtualBox:
    - RAM: mínimo 2 GB.
    - Disco: mínimo 20 GB.
    - Tarjeta de red: “Red Interna” (con el mismo nombre que la otra VM).

✅ DVWA (opción 1: instalar sobre Ubuntu)

1. Instala Ubuntu Server o Desktop (puedes usar también Debian).

Instala LAMP:

```
sudo apt update && sudo apt install apache2 mariadb-server php php-mysqli git
```

2.

Clona DVWA:

```
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git
sudo chown -R www-data:www-data DVWA
```

3.

Configura la base de datos:

```
sudo mysql -u root
CREATE DATABASE dvwa;
CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'dvwapass';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwauser'@'localhost';
FLUSH PRIVILEGES;
exit
```

4.

Configura el archivo de DVWA:

```
cd /var/www/html/DVWA/config
cp config.inc.php.dist config.inc.php
sudo nano config.inc.php
```

Modifica:

```
$_DVWA[ 'db_user' ] = 'dvwauser';
$_DVWA[ 'db_password' ] = 'dvwapass';
```

5.

Reinicia servicios y accede en navegador:

```
sudo systemctl restart apache2 mariadb
```

6. En Kali, accede a: `http://<IP-DVWA>/DVWA/setup.php`

Nota: Puedes ver la IP de la máquina DVWA con `ip a` o `hostname -I`.

---

2. 🔧 Configuración de Red

- Ambas máquinas deben estar en **la misma red interna** para simular un entorno realista.

- Verifica conectividad con `ping` desde Kali hacia la IP de DVWA.

---

3. 🔐 Preparar DVWA para pruebas

- Accede a DVWA desde Kali: `http://<IP-DVWA>/DVWA`
- Usuario por defecto: `admin` / `password`
- En la sección de configuración de seguridad, baja el nivel a “Low” para empezar.
- Ejecuta la configuración de la BBDD en “Create / Reset Database”.

---

4. 🧪 Empezar pruebas de penetración

Desde Kali, puedes practicar con herramientas como:
Nikto

```
nikto -h http://<IP-DVWA>
```

- **OWASP ZAP** o **Burp Suite** (interceptar peticiones)

sqlmap

```
sqlmap -u
"http://<IP-DVWA>/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="PHPSESSID=..."
```

-

nmap

```
nmap -sV -Pn <IP-DVWA>
```

-

---

5. 🔁 Repite con otras configuraciones

Cuando domines DVWA, puedes cambiar el nivel de seguridad de la aplicación o montar otras máquinas vulnerables como:

- **Metasploitable2**
- **OWASP Broken Web Applications**
- **bWAPP**
- **VulnHub VMs**

✅ Buenas prácticas

- Nunca conectes estas máquinas vulnerables a Internet.
- Usa snapshots para restaurar el entorno si rompes algo.
- Documenta cada prueba: objetivo, herramienta usada, resultado y lección aprendida.
- Usa herramientas como **CherryTree** o **Obsidian** para llevar tus notas técnicas.