



# Implementación de Entornos Controlados para Pruebas de Seguridad

## Introducción

- La ciberseguridad moderna requiere prácticas proactivas.
- El **pentesting** permite identificar vulnerabilidades antes que los atacantes.
- Pero: ¿Dónde practicar sin dañar sistemas reales?  
✓ Solución: **Entornos controlados de seguridad ofensiva**



## ¿Qué es un Entorno Controlado?

- 💡 Infraestructura aislada y segura
- 🎯 Diseñada para simular plataformas vulnerables
- ✅ Permite pruebas reales sin riesgo para entornos productivos
- 🛡️ Ideal para entrenamiento, evaluación de herramientas y práctica profesional



## Herramientas Clave para Crear Entornos

### Vulnhub

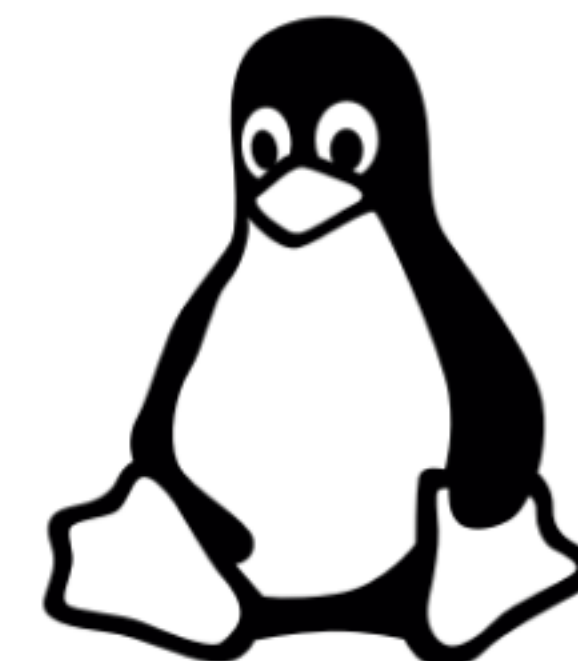
- **Función:**
  - Proveer máquinas virtuales vulnerables.
- **Beneficio:**
  - Permite practicar explotación en entornos realistas.
  - Escenarios diseñados para simular retos del mundo real.

### Docker

- **Función:**
  - Crear contenedores ligeros y rápidos.
- **Beneficio:**
  - Facilita la simulación instantánea de entornos.
  - Portabilidad total entre sistemas y plataformas.

### Kali Linux

- **Función:**
  - Distribución especializada en seguridad ofensiva.
- **Beneficio:**
  - Incluye una suite completa de herramientas para pentesting.
  - Ideal para pruebas de intrusión y análisis de seguridad.





## Kali Linux – La Base del Laboratorio

- 🧪 Distribución creada por Offensive Security
- 🔧 +600 herramientas preinstaladas para pruebas de seguridad
- 📀 Opciones de uso: Live USB, VM o instalación completa
- 📦 Gestor de paquetes APT
- 🔄 Actualizaciones constantes con últimas técnicas y CVEs



## Estructura Interna de Kali Linux

### Carpetas esenciales:

- **/bin, /usr/bin** → Comandos ejecutables
- **/etc** → Configuraciones
- **/opt** → Herramientas adicionales
- **/var/log** → Registros del sistema


### Gestión de paquetes con APT:

```
sudo apt update  
sudo apt upgrade  
sudo apt autoremove
```




The Quieter you become, the more you are able to hear


## Vulnhub – Máquinas Virtuales Vulnerables

 Plataforma comunitaria con VMs diseñadas para ser vulnerables

 Rango de dificultad: desde básico hasta avanzado

 Uso en VirtualBox o VMware

 Configuración típica: NAT o red solo-anfitrión

 Recomendación: probar máquinas como DVWA, Mr. Robot, Kioptrix



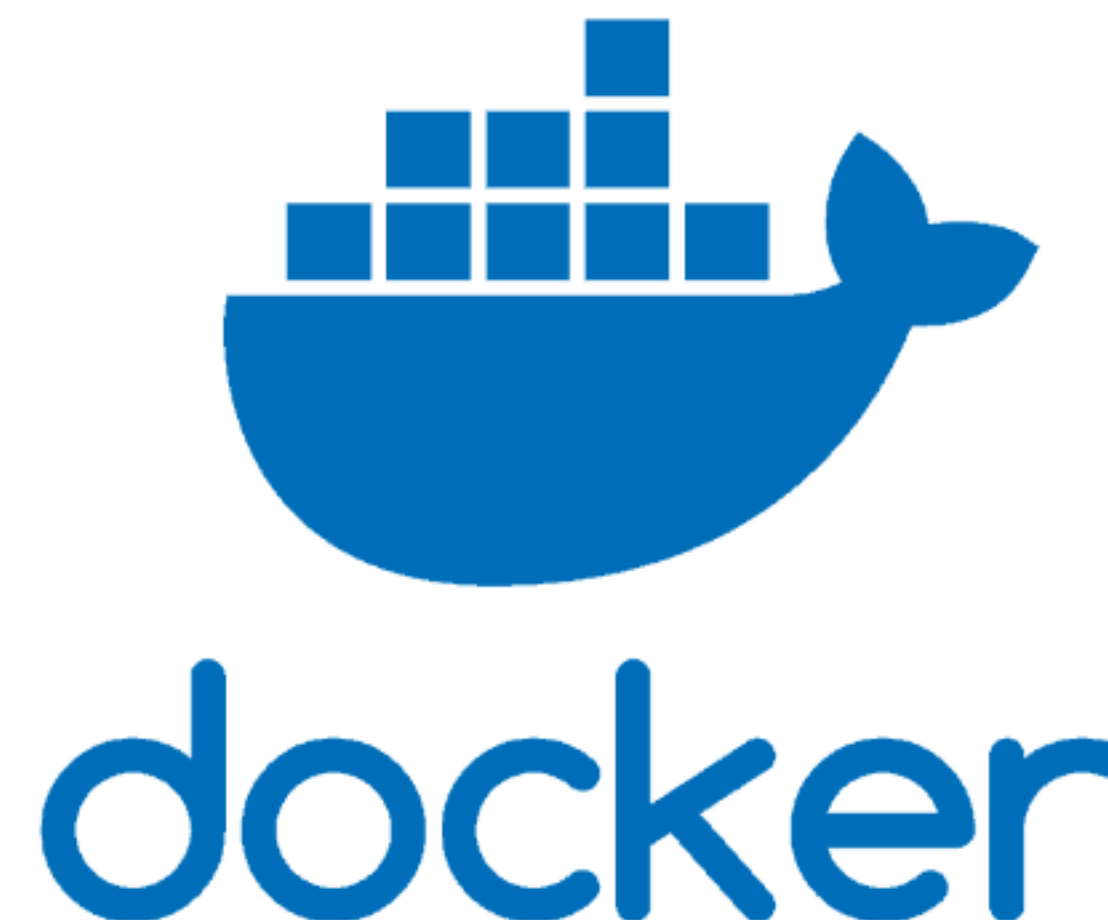
## Docker – Vulnerabilidades en Minutos

- ⚙️ Contenedores reproducibles, ligeros y aislados
- 🎯 Ideal para lanzar retos sin sobrecargar recursos
- 📦 Instalación:

```
sudo apt install docker.io  
sudo systemctl start docker
```

### 🔥 Levantar DVWA:

```
sudo docker run -d -p 80:80 vulnerables/web-dvwa
```





## Herramientas Prácticas con Kali

### Nmap

- Escaneo de puertos y servicios

### Ejemplo:

- `nmap -sV -sC -O <IP>`

### Metasploit

- Explotación estructurada
  - `msfconsole → use exploit/... → set RHOSTS → exploit`

### SQLMap

- Detección de inyecciones SQL
  - `sqlmap -u "http://IP/dvwa/..." --cookie="..."`



## Aplicaciones Web – Proxies y Pruebas

- ✦ Burp Suite y OWASP ZAP
  - Proxies de interceptación
  - Auditoría de aplicaciones web
  - Pruebas de fuzzing, inyección, autenticación, etc.



## Ética Profesional en el Pentesting

- ⚠ Nunca realizar pruebas sin autorización
- 📜 Obtener permisos explícitos
- 🛡 Respetar normativas locales e internacionales
- ✓ Buenas prácticas = confianza + legalidad



## Conclusión

- ✓ Kali Linux + Vulnhub + Docker = Laboratorio de ciberseguridad ofensiva
- ✓ Permite desarrollar habilidades sin poner en riesgo infraestructuras reales
- ✓ Base para entrenar, investigar y simular amenazas modernas
- 🎯 La ética y el conocimiento técnico van siempre de la mano en seguridad informática.





