

Capítulo 1

Instalación y despliegue del entorno de pruebas

En esta sección vamos a aprender a instalar y desplegar el entorno de pruebas.

1.1. Instalando VirtualBox

Vamos a instalar VirtualBox, aunque puede usarse cualquier plataforma de virtualización o incluso contenedores. Con Linux es muy sencilla la instalación.

Listing 1.1: Instalación de VirtualBox en Linux.

```
# sudo apt-get update  
# sudo apt-get install virtualbox
```

Si utilizamos Windows es simplemente una instalación con asistente, podemos descargar el instalador desde el enlace:
<https://www.virtualbox.org/wiki/Downloads>

1.2. Creación y configuración de red NAT en VirtualBox

Antes de levantar y configurar las máquinas vamos a crear una red NAT en VirtualBox, esto permite que comuniquemos las máquinas virtuales entre ellas de forma aislada y además tengamos salida a Internet desde las mismas. Vamos al menú de red (Archivo > Preferencias > Red)

Una vez que aquí agregamos una nueva red (usando el botón con el + de color verde) y la editamos (usando el botón con engranaje de color naranja). Podéis darle la dirección que queráis pero es recomendable habilitar el DHCP para evitar tener que configurar la red.

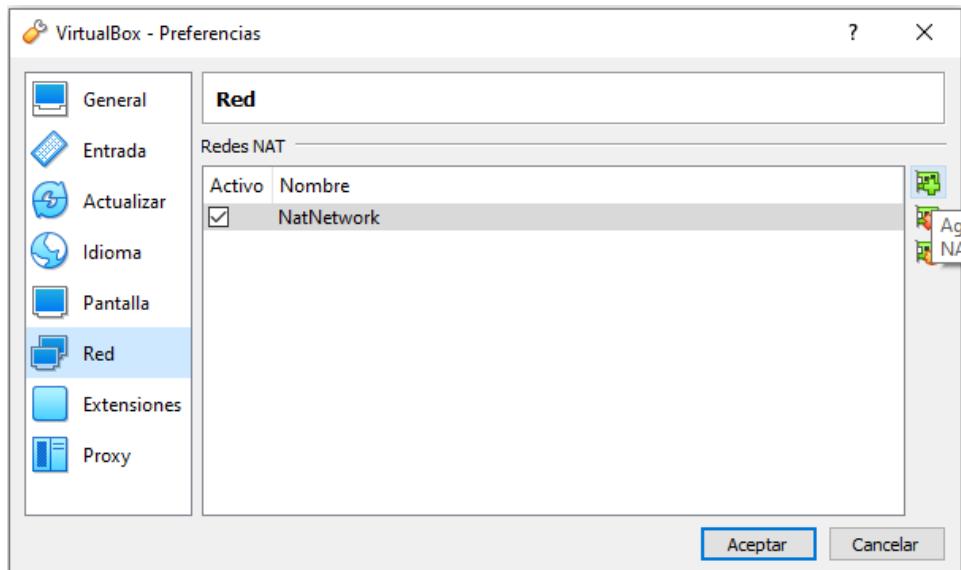


Figura 1.1: Menú de red de VirtualBox

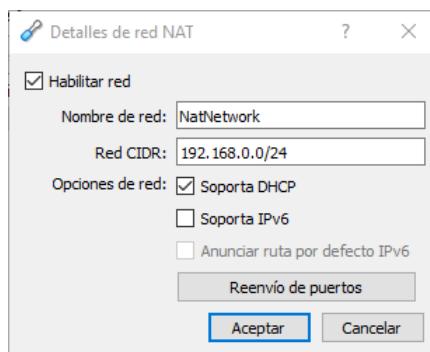


Figura 1.2: Menú de edición de red

1.3. Despliegue de Kali Linux y OWASP Broken Web Applications

Vamos a descargar, configurar y levantar las maquinas virtuales para realizar los ejercicios. Utilizaremos 2 máquinas virtuales, estas son Kali Linux y OWASP BWA.

1.3.1. Kali Linux

Aunque podríamos descargar el ISO e instalarlo, nosotros descargaremos directamente el OVA, este fichero nos va a permitir desplegar la máquina de forma directa.

Descargaremos el OVA en el siguiente enlace: <https://www.kali.org/get>

kali/#kali-virtual-machines

Aunque podemos emplear cualquiera de las 2 versiones, yo selecciono la de 64 bits. Podéis descargarla de forma directa o mediante torrent.

+ KALI LINUX VMWARE IMAGES				
– KALI LINUX VIRTUALBOX IMAGES				
Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2021.1	3.6G	b907b61ed584c8eef57dc81e45f8e8af608cc1e0f203711e6c57653b938ef69
Kali Linux VirtualBox 32-Bit (OVA)	Torrent	2021.1	3.2G	fb0ec2dff7d83ec042c2376f740f8c3e92d230caadadee0ffe483c1b809a1013

Figura 1.3: Página de descarga del OVA de Kali Linux

Una vez descargado el OVA simplemente hacemos doble click para que aparezca la ventana de importar. Otra opción es buscar el OVA desde la opción *Importar servicio virtualizado* que se encuentra en *Archivo*.

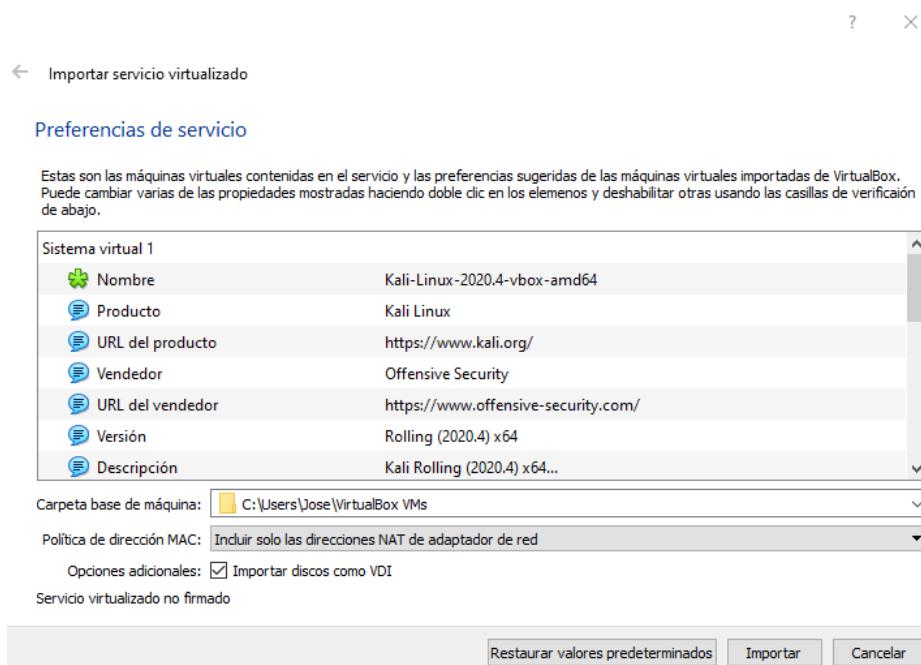


Figura 1.4: Ventana de importación de servicio virtualizado

Con las opciones por defecto seleccionaremos importar, esto provoca que aparezca la máquina en el menú de VirtualBox (puede tardar unos segundos).

Antes de arrancar la máquina la configuraremos para introducirla a la red NAT que creamos previamente. Con el botón derecho abrimos el menú de la máquina, aquí pulsaremos configuración (engranaje naranja).

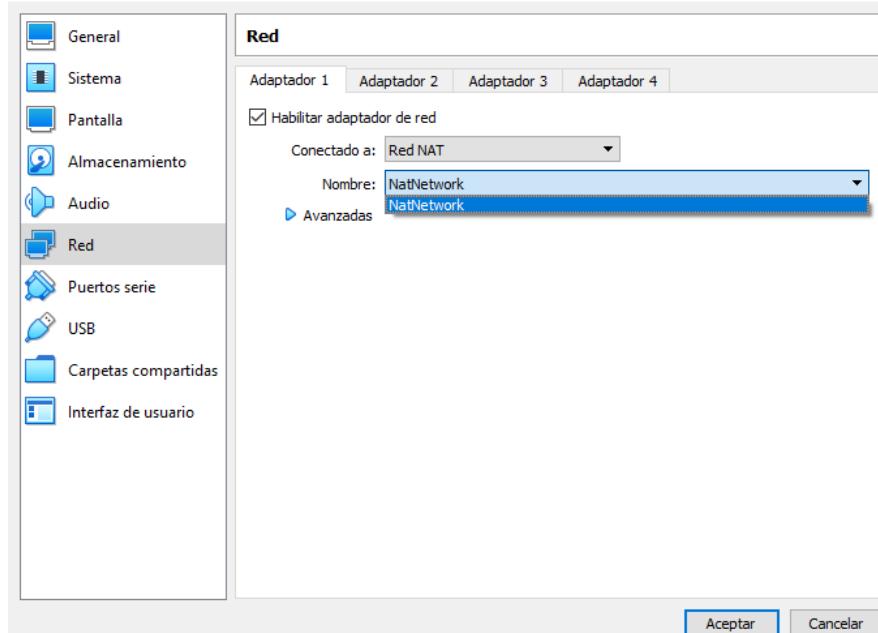


Figura 1.5: Configuración de red en máquina virtual.

Una vez aquí simplemente vamos a las opciones de red, seleccionamos *Red NAT* y elegimos nuestra red. Aquí podemos arrancar la máquina (simplemente pinchando 2 veces).

1.3.2. OWASP BWA

Los pasos a seguir son idénticos con esta máquina. Podéis descargarla en el siguiente enlace: <https://sourceforge.net/projects/owaspbwa/>.

Una vez descargada repetimos los pasos y nos aseguramos de meter esta máquina en la misma red. Con esto ya tenemos un laboratorio para realizar los ejercicios de web.

1.4. Conectando Kali Linux y OWASP BWA

Con las maquinas levantadas solo queda conocer la dirección de la máquina de OWASP y conectar con Kali Linux.

Una vez arrancada la máquina de OWASP BWA podemos ver en su terminal la IP con la que conectar. Desde Kali simplemente queda abrir Firefox y conectar.

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.1.131/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.131, via Samba at \\192.168.1.131\, or via phpmyadmin at
http://192.168.1.131/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: _
```

Figura 1.6: Banner de arranque de la máquina de OWASP.

The screenshot shows a web browser window with the URL 192.168.1.131. At the top, there's a navigation bar with links like 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', and 'MSFU'. Below the navigation bar, a yellow warning box contains the text: '!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!' with an exclamation mark icon. The main content area is titled 'TRAINING APPLICATIONS' and lists several links:

+ OWASP WebGoat	+ OWASP WebGoat.NET
+ OWASP ESAPI Java SwingSet Interactive	+ OWASP Mutillidae II
+ OWASP RailsGoat	+ OWASP Bricks
+ OWASP Security Shepherd	+ Ghost
+ Magical Code Injection Rainbow	+ bWAPP
+ Damn Vulnerable Web Application	

Figura 1.7: Página principal de OWASP BWA