¿Qué es Metasploitable 2?

Metasploitable 2 es una máquina virtual creada por la empresa de *software* de seguridad informática Rapid7, que también es la desarrolladora del famoso *framework* de explotación Metasploit. Ahora bien, **Metasploitable 2 está diseñada especialmente para ser hackeada y, por lo tanto, cuenta con *softwares* y aplicaciones web vulnerables de forma deliberada**. En conclusión, es un entorno ideal para aprender hacking ético de manera segura.

A continuación, te explicaremos **cómo instalar Metasploitable 2 en VMware**, un *software* de virtualización ideal para manejar varias máquinas virtuales a la vez. No obstante, también puedes instalarla en otro programa si deseas, como **VirtualBox** o **KVM**.

¿Cómo instalar Metasploitable 2?

Para instalar Metasploitable 2, dirígete a uno de los dos links que se encuentran en la página oficial de Rapid7. Por medio de cualquiera de estos enlaces, podrás descargar una carpeta comprimida con varios archivos en ella. La carpeta pesa aproximadamente 825 MB y contiene 13 elementos. Uno de ellos es un fichero con extensión .vmx llamado Metasploitable.vmx, que es un archivo de VMware. Al hacer doble clic en este, se abrirá VMware automáticamente con la maquina virtual metasploitable instalada.

Haz clic en el botón «**Start this virtual machine**» y la máquina arrancará todos sus *softwares* y servidores de manera automática. Para conocer su dirección ip metasploitable , ejecuta el comando «**ifconfig**» en la terminal, como puedes ver en la siguiente imagen:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.175.130  Bcast:192.168.175.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3703 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1932 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:415573 (405.8 KB)  TX bytes:898033 (876.9 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2073 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2073 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1011153 (987.4 KB)  TX bytes:1011153 (987.4 KB)

msfadmin@metasploitable:~$
```

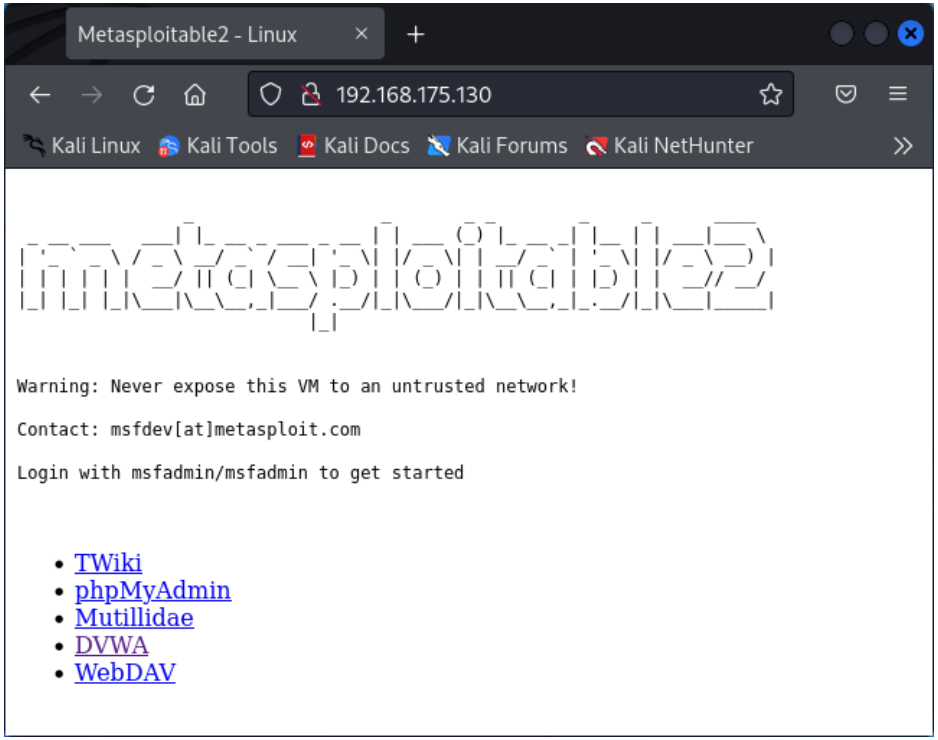
¿Cómo explotar Metasploitable 2?

Ya hemos visto cómo instalar Metasploitable 2 en VMware. Ahora, hablaremos brevemente sobre su explotación. Existen dos tipos de hacking que se pueden practicar con esta máquina virtual: **hacking de sistemas** y **hacking web**.

Dado que Metasploitable 2 de metasploit fue desarrollada por Rapid7, es de esperar que se pueda explotar, principalmente, a partir del *framework* de Metasploit. **Este *framework* reúne miles de *exploits*, escáneres de vulnerabilidades y *payloads* que funcionan en Metasploitable 2**. Por eso, es la herramienta ideal para practicar *pentesting* de sistemas de forma segura.

Hacking web

Los servidores de Metasploitable 2 alojan aplicaciones web deliberadamente vulnerables, como DVWA, TWiki, phpMyAdmin, Multillidae y WebDAV. Para acceder a estas aplicaciones y practicar pentesting web con ellas, accede a la dirección IP de la máquina virtual Metasploitable 2 desde un navegador en otra máquina.



Las cinco aplicaciones web alojadas en los servidores de Metasploitable 2 **cuentan con cientos de vulnerabilidades** para poner a prueba tus habilidades como hacker web.

Se pide:

1. Una vez finalizado, sube a la plataforma un documento con capturas de pantalla, que muestren los pasos realizados.