

1. Run the kernel image with “qemu” (<https://www.qemu.org/>) & forward port 80 (guest) to port 3000 (host). The “nographic” flag is used because the QEMU GUI doesn’t display the BusyBox terminal.

Command: `qemu-system-mipsel -kernel BootMe_openwrt-malta-le-vmlinux-initramfs.elf -nographic -net nic,model=pcnet -net user,hostfwd=tcp::3000-:80`

```
(kali㉿kali)-[~/Desktop/bootme]
$ qemu-system-mipsel -kernel BootMe_openwrt-malta-le-vmlinux-initramfs.elf -nographic -net nic,
model=pcnet -net user,hostfwd=tcp::3000-:80
```

2. If we try to “curl” the forwarded site, we get a “Connection reset by peer error”. This can be fixed by flushing all **iptables** chains.

```
(kali㉿kali)-[~]
$ curl http://127.0.0.1:3000
curl: (56) Recv failure: Connection reset by peer
```

```
root@OpenWrt:/# iptables -F
root@OpenWrt:/#
```

3. Now the website is accessible & the website can be visited on localhost with port 3000, to get the flag.

OpenWrt - Overview - LuCI - Mozilla Firefox

OpenWrt - Overview - LuCI

127.0.0.1:3000/cgi-bin/luci/

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB

OpenWrt

No password set!
There is no password set on this router. Please configure a root password to protect the web interface.

Authorization Required
Please enter your username and password.

Username

Password

Login Reset

Powered by LuCI Master (git-21.032.71059-a567b3d) / OpenWrt SNAPSHOT r15668-d33cd383ed hi(YAY_I_WAS_BOOTED)