## Lab Setup

* Download the lab setup file

**wget https://seedsecuritylabs.org/Labs\_20.04/Files/Firewall/Labsetup.zip**

* Unzip the lab setup file

**unzip Labsetup.zip**

* Go to the unzipped folder

**cd Labsetup/**

* Build the container image

**dcbuild**

* Start the container

**dcup > ../output.log 2>&1 &**

* Shut down the container

**dcdown**

## LKM (Loadable Kernel Module)

* Prepare the module **<module\_name>.c**
* Prepare a **Makefile**

**obj-m += <module\_name>.o**

**all:**

**make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules**

**clean:**

**make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean**

* Run the **Makefile**

**make**

* Clear the message buffer

**sudo dmesg -C**

* Insert the module

**sudo insmod <module\_name>.ko**

* Check if the module is inserted

**lsmod | grep <module\_name>**

* The module should be working now
* Remove the module

**sudo rmmod <module\_name>**

## Useful Resources

* <https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture>
* <https://www.cloudsigma.com/the-architecture-of-iptables-and-netfilter/>
* <https://levelup.gitconnected.com/write-a-linux-firewall-from-scratch-based-on-netfilter-462013202686>
* <https://www3.cs.stonybrook.edu/~ezk/cse506-s19/handouts/kdk-Netfilter.pdf>
* <https://infosecwriteups.com/linux-kernel-communication-part-1-netfilter-hooks-15c07a5a5c4e>
* <https://www.opensourceforu.com/2022/08/building-a-stateless-firewall-using-netfilter-in-linux/>
* iptables manual
  + <https://man.cx/?page=iptables(8)>
  + <https://linux.die.net/man/8/iptables>
* header files
  + <https://github.com/torvalds/linux/blob/master/include/linux/netfilter.h>
  + <https://github.com/torvalds/linux/blob/master/include/linux/netfilter_ipv4.h>
  + <https://github.com/torvalds/linux/blob/master/include/linux/ip.h>
  + <https://github.com/torvalds/linux/blob/master/include/linux/tcp.h>
  + <https://github.com/torvalds/linux/blob/master/include/linux/udp.h>
  + <https://github.com/torvalds/linux/blob/master/include/linux/if_ether.h>
  + <https://github.com/torvalds/linux/blob/master/include/linux/inet.h>