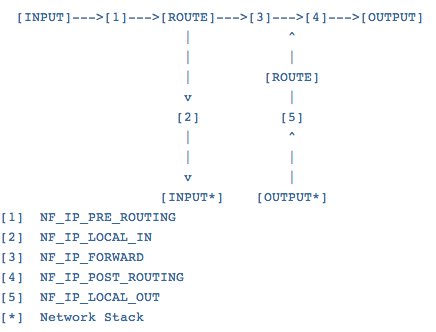


**Networking**

***Objective: In this lab you will develop a LKM called*** netdead ***that will kill all incoming and outgoing network traffic in the kernel.***

Netfilter is a packet filtering subsystem in the Linux kernel stack and has been there since kernel 2.4.x. Netfilter's core consists of five hook functions declared in linux/netfilter\_ipv4.h. Although these functions are for IPv4, they aren't much different from those used in the IPv6 counterpart. The hooks are used to analyze packets in various locations on the network stack. This situation is depicted below:



NF\_IP\_PRE\_ROUTING is called right after the packet has been received. This is the hook we are most interested in for our micro-firewall. NF\_IP\_LOCAL\_IN is used for packets that are destined for the network stack and thus has not been forwarded. NF\_IP\_FORWARD is for packets not addressed to us but that should be forwarded. NF\_IP\_POST\_ROUTING is for packets that have been routed and are ready to leave, and NF\_IP\_LOCAL\_OUT is for packets sent out from our own network stack. Each function has a chance to mangle or do what it wishes with the packets, but it eventually has to return a Netfilter code. Here are the codes that can be returned and what they mean:

NF\_ACCEPT: accept the packet (continue network stack trip)

NF\_DROP: drop the packet (don't continue trip)

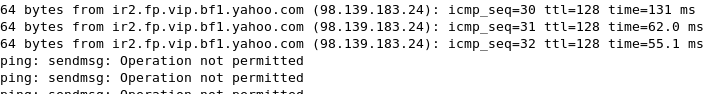
NF\_REPEAT: repeat the hook function

NF\_STOLEN: hook steals the packet (don't continue trip)

NF\_QUEUE: queue the packet to userspace

1. Complete the code below for netdead to kill network traffic on the host:





* Examine netfilter.h for info on the struct nf\_hook\_ops

