

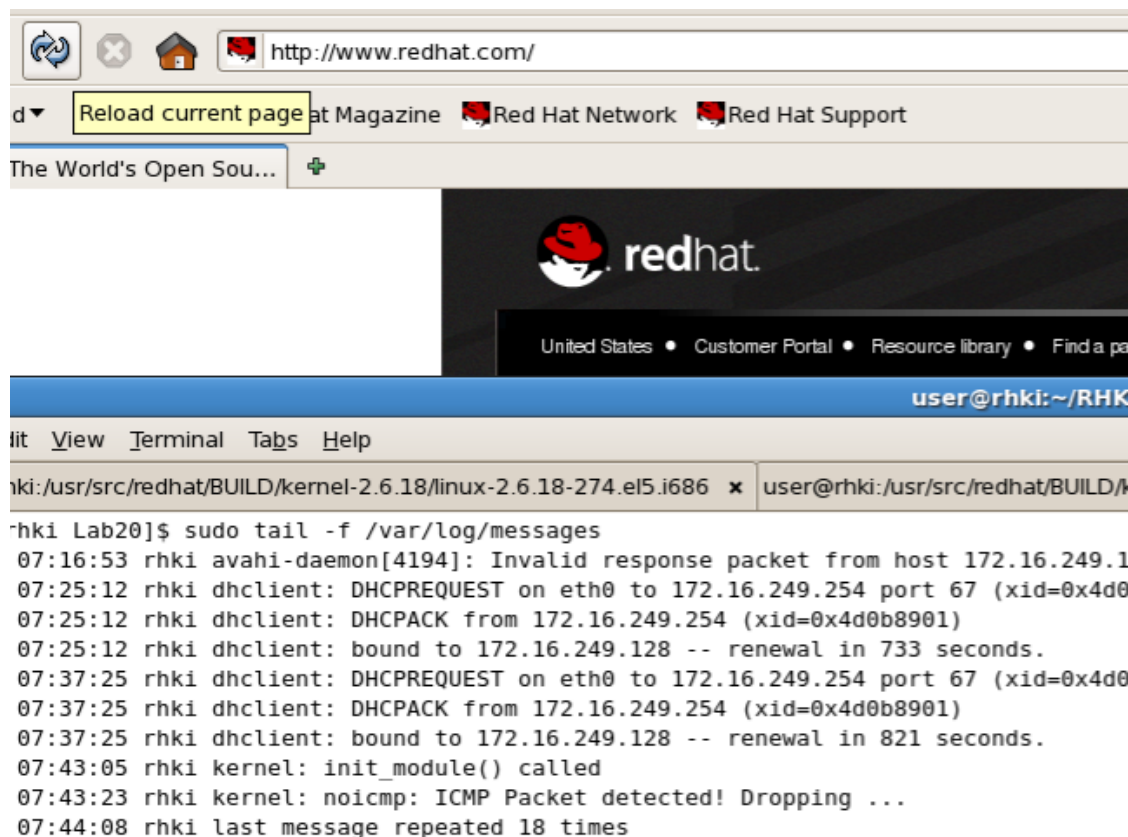


RedHat Linux Kernel Internals Laboratory Exercises

Lab 20: Networking – No ICMP

Objective: In this lab you will develop an LKM called “noicmp” that will kill all incoming and outgoing ICMP Packets in the kernel. This will expose you to the net/ip header and give you greater control over the entire packet contents

1. Complete the code below for “netdead” to kill network traffic on the host. Test your module by browsing to the internet while “pinging”. Unlink the previous lab, your TCP packets should get through! Log each time a packet is dropped.



The screenshot shows a web browser window at the top with the address bar displaying `http://www.redhat.com/`. Below the browser is a terminal window. The terminal prompt is `rhki Lab20]$`. The user has run the command `sudo tail -f /var/log/messages`, which displays the following log entries:

```
07:16:53 rhki avahi-daemon[4194]: Invalid response packet from host 172.16.249.1
07:25:12 rhki dhclient: DHCPREQUEST on eth0 to 172.16.249.254 port 67 (xid=0x4d0
07:25:12 rhki dhclient: DHCPACK from 172.16.249.254 (xid=0x4d0b8901)
07:25:12 rhki dhclient: bound to 172.16.249.128 -- renewal in 733 seconds.
07:37:25 rhki dhclient: DHCPREQUEST on eth0 to 172.16.249.254 port 67 (xid=0x4d0
07:37:25 rhki dhclient: DHCPACK from 172.16.249.254 (xid=0x4d0b8901)
07:37:25 rhki dhclient: bound to 172.16.249.128 -- renewal in 821 seconds.
07:43:05 rhki kernel: init_module() called
07:43:23 rhki kernel: noicmp: ICMP Packet detected! Dropping ...
07:44:08 rhki last message repeated 18 times
```

Hints:

- Examine the struct for `sk_buff`, `iphdr`, and `icmphdr` and filter out only ICMP
- Include the file `net/ip.h` for access to the ip header.
- The function `skb_network_header()` may be of help as well.