Matthew Quander
12/7/2021
COSC647

Lab 7

Set Up:

1. Build kernel object file for hello.c:

```
Terminal
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$ make args="hello"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/lab7/LAB07_FIR
EWALL_STD modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

2. Install the compiled .ko file

```
seed@VM:~/.../LAB07_FIREWALL_STD$ sudo insmod hello.ko
seed@VM:~/.../LAB07_FIREWALL_STD$
```

3. Remove installed .ko file

```
seed@VM:~/.../LAB07_FIREWALL_STD$ sudo rmmod hello.ko
seed@VM:~/.../LAB07_FIREWALL_STD$
```

4. View result:

```
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$ tail /var/log/syslog
Dec 10 16:48:18 VM kernel: [  310.761092] hello: module license 'unspecified' ta
ints kernel.
Dec 10 16:48:18 VM kernel: [  310.761094] Disabling lock debugging due to kernel
 taint
Dec 10 16:48:18 VM kernel: [  310.761826] hello.c -- init_module() called
Dec 10 16:48:19 VM anacron[841]: Job `cron.daily' terminated
Dec 10 16:49:33 VM kernel: [  386.362105] hello.c -- cleanup_module() called
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

Compile dropAllPackets

```
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$ make args="dropAllPackets"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/lab7/LAB07_FIR
EWALL_STD modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

Install dropAllPackets.ko

```
seed@VM:~/.../LAB07_FIREWALL_STD$ sudo insmod dropAllPackets.ko
seed@VM:~/.../LAB07_FIREWALL_STD$
```

Ping TU website (1st attempt)

```
12/07/21]seed@VM:~/.../LAB07_FIREWALL_STD$ ping www.towson.edu
PING www.towson.edu (52.224.91.77) 56(84) bytes of data.
C
-- www.towson.edu ping statistics ---
91 packets transmitted, 0 received, 100% packet loss, time 194552ms

12/07/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

Matthew Quander
12/7/2021
COSC647

Task 01:

Line 22 gets the iphdr from the sk_buff as a pointer. Line 28 checks that the protocol of the iph struct is 17 (the UDP protocol number) and drops the packet if so (line 29), otherwise accepts it (line 32).

```
 8
 9 static struct nf_hook_ops nfho;
10
11 unsigned int hook_func(
12   void *priv,
13   struct sk_buff *skb,
14   const struct nf_hook_state *state
15 ) {
16   struct iphdr    * iph;
17   struct tcphdr   * tcph;
18   struct udphdr   * udph;
19
20   if (skb) {
21     // Get IP header from the socket buffer
22     iph = ip_hdr(skb);
23     ////////////////////////////////////////////////////////////
24     // TODO: Drop packet if the protocol is UDP
25     ////////////////////////////////////////////////////////////
26     //               Your code goes here                      //
27     ////////////////////////////////////////////////////////////
28     if (iph && iph->protocol == 17) {
29       return NF_DROP;
30     }
31   }
32   return NF_ACCEPT;
33 }
34
35 int init module() {
```

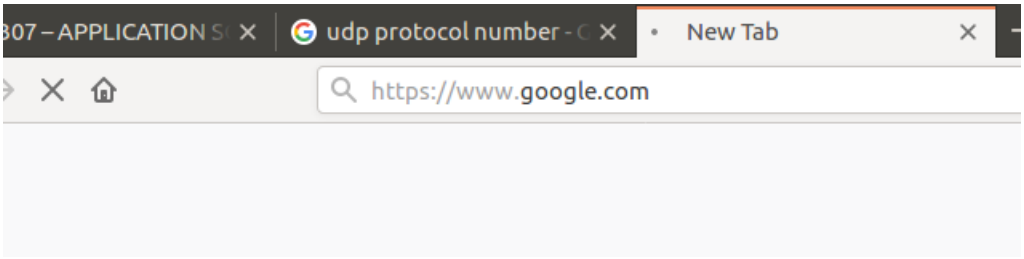
Install the dropUdpPackets.ko file

```
seed@VM:~/.../LAB07_FIREWALL_STD$ sudo insmod dropUdpPackets.ko
seed@VM:~/.../LAB07_FIREWALL_STD$
```

Ping google.com to test:

```
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$ ping www.google.com
ping: unknown host www.google.com
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

Test google.com through the browser



Task 02:

Matthew Quander
12/7/2021
COSC647

Line 23 gets the iphdr from the sk_buff as a pointer. Line 25 checks if the iph protocol is 6, which is for TCP. Lines 27 and 43 typecast iphdr to either tcphdr or udphdr depending on iphdr's "protocol" property. Lines 37 and 54 compare the value of source_port to 80 and 443 which are the numbers for HTTP and HTTPS. If it is HTTP/HTTPS (i.e., a web packet) then it is dropped, otherwise it's accepted.

dropWebPackets.c (~/Desktop/lab7/LAB07_FIREWALL_STD) - gedit

Open

LAB07_FIREWALL_INSTRUCTIONS.txt | dropWebPackets.c

```
15 ) {
16   struct iphdr    * iph;
17   struct tcphdr   * tcph;
18   struct udphdr   * udph;
19   u16    source_port = 0;
20
21   if (skb) {
22     // Get IP header from the socket buffer
23     iph = ip_hdr(skb);
24
25     if (iph && iph->protocol == 6 ) { //6 for TCP
26       // Typecast to either tcphdr or udphdr pointer
27       tcph = (struct tcphdr *)((__u32 *)iph + iph->ihl);
28       ////////////////////////////////////////////////////////////
29       // TODO: Check the source port to port 80 or 443 of web datagrams
30       ////////////////////////////////////////////////////////////
31       //                Your code goes here                     //
32       ////////////////////////////////////////////////////////////
33       if (tcph) {
34         // Convert the source port to integer 16bits
35         source_port = ntohs(tcph->source);
36       }
37       if ( source_port == 80 || source_port == 443) { // for http and https
38         return NF_DROP;
39       }
40     }
41     else if (iph && iph->protocol == 17) { // for UDP
42       // Typecast to either tcphdr or udphdr pointer
43             udph = (struct udphdr *)((__u32 *)iph + iph->ihl);
44
45       ////////////////////////////////////////////////////////////
46       // TODO: Check the source port to port 80 of web datagrams
47       ////////////////////////////////////////////////////////////
48       //                Your code goes here                     //
49       ////////////////////////////////////////////////////////////
50       if (udph) {
51         // Convert the source port to integer 16bits
52         source_port = ntohs(udph->source);
53       }
54       if ( source_port == 80 || source_port == 443) {// for http and https
55         return NF_DROP;
56       }
57     }
58   }
59   return NF_ACCEPT;
60 }
```

C ▾ Tab Width: 8 ▾ Ln 54, Col 47 ▾

Run command to make kernel object file (can ignore warning):

Matthew Quander
12/7/2021
COSC647

```
Terminal
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$ make args="dropWebPackets"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/lab7/LAB07_FIR
EWALL_STD modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/Desktop/lab7/LAB07_FIREWALL_STD/dropWebPackets.o
/home/seed/Desktop/lab7/LAB07_FIREWALL_STD/dropWebPackets.c: In function 'init_m
odule':
/home/seed/Desktop/lab7/LAB07_FIREWALL_STD/dropWebPackets.c:69:3: warning: ISO C
90 forbids mixed declarations and code [-Wdeclaration-after-statement]
   int result = nf_register_hook(&nfho);
   ^
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Desktop/lab7/LAB07_FIREWALL_STD/dropWebPackets.mod.o
  LD [M]  /home/seed/Desktop/lab7/LAB07_FIREWALL_STD/dropWebPackets.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

Run command to install kernel object file:

```
/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$ sudo insmod dropWebPackets.ko
/10/21]seed@VM:~/.../LAB07_FIREWALL_STD$
```

Test google.com in the browser and through the ping command. Web packets are blocked (browser) but data packets still come through the terminal: