Firewall

N7.1. What is `netfilter` and what are its benefits?

N7.2. What are the five `netfilter` hooks for IPv4? What are their purposes?

N7.3. Please answer the following questions about netfilter:

1. A packet from S to D arrives at D, which netfilter hooks on D will this packet pass through?
2. A packet from S to D arrives at a router R, which netfilter hooks on R will this packet pass through?
3. A packet is created on host S, and it will be sent to D. Which netfilter hooks on S will this packet pass through?

N7.4. Why do we need to build a kernel module in order to use the `netfilter` hooks?

N7.5. The following code tries to block the computer from accessing the web server (HTTP) running on host `10.0.2.5`. Please complete the code by replacing `@@@@@@@` with actual code.

```
static struct nf_hook_ops filterHook;
int setUpFilter(void){
  filterHook.hook = @@@@@@;                    ①
  filterHook.hooknum = NF_INET_POST_ROUTING;
  filterHook.pf = PF_INET;
  filterHook.priority = NF_IP_PRI_FIRST;
  nf_register_hook(&@@@@@@@);                  ②
  return 0;
}
void removeFilter(void){
  nf_unregister_hook(&@@@@@@@);                ③
}
module_init(@@@@@@@);                          ④
module_exit(@@@@@@@);                          ⑤


unsigned int block(void *priv, struct sk_buff *skb,
                 const struct nf_hook_state *state)
{
  if(!skb){
    printk(KERN_INFO,"packet receive not correct\n");
    return NF_DROP;
  }

  struct iphdr *iph;
  struct tcphdr *tcph;
```

```
  iph = ip_hdr(@@@@@@);                          ⑥
  tcph = (void *)iph+iph->ihl*4;

  __u32 sou_ip = iph->saddr;
  __u32 des_ip = iph->daddr;
  __u16 sou_port = tcph->source;
  __u16 des_port = tcph->dest;

  if(des_ip==in_aton("@@@@@@") &&                ⑦
     ntohs(des_port)== @@@@@@) {                 ⑧
    return @@@@@@;                               ⑨
  }
  return NF_ACCEPT;
}
```

N7.6. Based on the `netfilter` diagram (can be found in the book), please describe which filter is best for enforcing the following rules:

- Restricting what comes into a computer
- Restricting what goes out of a computer

N7.7. Other than being used to implement firewalls to block packets, can `netfilter` be used to modify packets? What are the other applications of `netfilter`?

N7.8. Three functions, F1, F2, and F3, are registered to the netfilter hooks. F1 is registered to `NF_INET_POST_ROUTING` with a priority `-110`. F2 is registered to `NF_INET_LOCAL_OUT` with a priority `-120`. F3 is registered to `NF_INET_LOCAL_OUT` with a priority `-100`. F4 is registered to `NF_INET_FORWARD` with a priority `-110`. When we send out an ICMP echo request packet from this machine, which functions will be invoked, and in what order?

N7.9. If a hook function returns `NF_ACCEPT` for a packet, this packet will be accepted. Is this true or false, why?

N7.10. Three functions are registered to a netfilter hook with the following order: F1 $\rightarrow$ F2 $\rightarrow$ F3. (1) If function F2 returns `NF_ACCEPT`, will function F3 be invoked or not? (2) If function F2 returns `NF_DROP`, will function F3 be invoked or not?

N7.11. Which netfilter hook do the following `iptables` chain correspond to, respectively: (1) the `filter` table's `INPUT` chain, (2) the `nat` table's `OUTPUT` chain, and the `mangle` table's `POSTROUTING` chain?

N7.12. ★
The `SYNPROXY` is a firewall to filter out SYN flooding attack packets. Please find articles from the Internet about `SYNPROXY`, and explain at high-level how it works.

N7.13. What are the benefits of stateful firewalls that support connection-based firewall rules? Please use examples to illustrate the benefit.

N7.14. In Ubuntu, a program is called `ufw`, which stands for Uncomplicated Firewall. Is this a real firewall?

N7.15. Add a rule in iptables to accept packets from a trusted network `192.168.10.0/24`

N7.16. A machine has an IP address `10.0.20.5`. On this machine, you need to block incoming connections to its ports 22, 23, 80, and 443. What will you do?

N7.17. Assuming that we have four identical UDP services running on four different machines (all listening to port 9000), and we want to distribute the load, so each machine takes one fourth of the incoming requests. How do we do this? Please provide the concrete `iptables` rules (you can use A, B, C, and D to represent the IP address of these four machines).

N7.18. ICMP and UDP do not have connections, but Linux's connection tracking does track ICMP and UDP. What do the "connections" mean for ICMP and UDP?

N7.19. When we run `conntrack -L`, we get the following results. How long will each of the connection last before it times out in the connection tracking?

```
tcp      6 431752 ESTABLISHED src=10.0.5.5 dst=52.89.15.44 ...
udp      17 1 src=10.0.5.5 dst=10.0.5.3 sport=68 dport=67 ...
icmp     1 29 src=10.0.5.5 dst=1.1.1.1 type=8 code=0 id=16 ..
```