防火墙

N7.1. 什么是 `netfilter` ？它有什么好处？

N7.2. IPv4 的五个 `netfilter` hook 分别是什么？各自位于数据包路径的哪个阶段？

N7.3. 回答下列有关 `netfilter` 数据包路径的问题：

1. S 发往 D 的数据包到达目的主机 D 时，会经过 D 上的哪些 hook？
2. S 发往 D 的数据包经过路由器 R 时，会经过 R 上的哪些 hook？
3. 在主机 S 上创建了一个数据包，并将其发送到 D。该数据包将通过 S 上的哪个 netfilter 挂钩？

N7.4. 为什么使用 `netfilter` hook 的代码通常要构建为内核模块？

N7.5. 以下代码尝试阻止计算机访问主机 `10.0.2.5` 上运行的 Web 服务器（HTTP）。请通过以下方式完成代码将 `@@@@@@@` 替换为实际代码。

```
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. 根据书中的 netfilter 数据包路径图，哪些 hook 最适合实现下列规则？

- 限制进入计算机的内容
- 限制计算机的输出内容

N7.7. 除了实现防火墙丢弃数据包，netfilter 能否修改数据包？它还有哪些用途？

N7.8. 三个函数 F1、F2 和 F3 注册到 netfilter 挂钩。F1 注册到 NF_INET_POST_ROUTING，优先级为 -110。F2 注册到 NF_INET_LOCAL_OUT，优先级为 -120。F3 注册到 NF_INET_LOCAL_OUT，优先级为 -100。F4 注册到 NF_INET_FORWARD，优先级为 -110。当我们从本机发出 ICMP echo 请求数据包时，将调用哪些函数以及以什么顺序？

N7.9. 某 hook 回调对数据包返回 NF_ACCEPT，是否意味着该数据包最终一定会被系统接受？为什么？

N7.10. 三个函数注册到 netfilter 钩子，如下订单：F1 → F2 → F3。(1) 如果函数 F2 返回 NF_ACCEPT，函数 F3 是否会被调用？(2) 如果函数 F2 返回 NF_DROP，函数 F3 是否会被调用？

N7.11. 下列 `iptables` 链分别对应哪个 `netfilter` hook：（1）`filter` 表的 `INPUT`；（2）`nat` 表的 `OUTPUT`；（3）`mangle` 表的 `POSTROUTING`？

N7.12. ★
`SYNPROXY` 可帮助防火墙抵御 SYN flood。请查阅资料，并从高层说明其工作原理。

N7.13. 有状态防火墙支持基于连接状态的规则，这有什么好处？请举例说明。

N7.14. Ubuntu 中的 `ufw`（Uncomplicated Firewall）本身是真正执行包过滤的防火墙吗？

N7.15. 添加一条 iptables 规则，接受来自受信任网络 `192.168.10.0/24` 的入站包。

N7.16. 某机器的 IP 地址为 `10.0.20.5`。需要阻止发往该机 TCP 端口 22、23、80 和 443 的入站连接，应如何配置？

N7.17. 四台机器 A、B、C、D 都在 UDP 9000 端口运行相同服务。希望把到达路由器 UDP 8080 端口的请求大致均分给四台机器，请给出具体 iptables 规则。

N7.18. ICMP 和 UDP 本身不建立连接，但 Linux conntrack 仍会跟踪它们。此处的“连接”对 ICMP 和 UDP 分别表示什么？

N7.19. 下列 `conntrack -L` 输出中，各条目还要多久超时？

```
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 ..
```