1. **В чем различие между целями DROP и REJECT?**

   «выброс» пакета (DROP);

   отказ от получения пакета (REJECT);

   При выбросе пакета он просто теряется. Отказ от получения пакета вызывает отправление сообщения источнику пакета о том, что пакет не может быть принят.

2. **Какая очередность применения правил iptables?**

   При получении каждого пакета сетевая подсистема выбирает первое правило из таблицы. Если пакет соответствует данному правилу, то выполняется действие («цель»), указанное в правиле, если нет – проверяется следующее в цепочке правило. Если пакет не соответствует условиям ни одного из правил, выбирается «цель» по умолчанию, которая задается для каждой цепочки.

3. **Какие правила необходимо добавить в таблицу фильтрации для разрешения установления TCP-соединения?**

   iptables -t filter -A INPUT -s IP -p tcp--dport ПОРТ -j ACCEPT

4. **Дайте описание цепочек PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING. Какие из них есть в таблице фильтрации пакетов?**

   PREROUTING – для всех пакетов, приходящих извне;

   INPUT – для пакетов, пришедших извне и предназначенных для локальной системы;

   FORWARD – для маршрутизируемых пакетов, т.е. пакетов, пришедших извне и предназначенных для другой системы;

OUTPUT – для пакетов, созданных в данной системе;

POSTROUTING – для всех исходящих пакетов.

таблица filter – цепочки INPUT, FORWARD, и OUTPUT

5. **Что делает маскарадинг? Что такое NAT? Каковы отличия между ними?**

   Маскарадинг – это тип трансляции сетевых пакетов с подменой IP-адреса на IP-адрес узла, через который данный пакет проходит. Позволяет машинам, не имеющим реальных (внешних) IP-адресов, работать в сети Интернет.

   SNAT (source NAT) – это тип трансляции сетевых пакетов с подменой IP-адреса на указанный в правиле адрес.

6. **Есть ли способ выполнить п. 5 без использования правил по умолчанию? Если есть, то какой?**

   Сначала разрешаем icmp. Затем запрещаем все.