

Методические указания
для выполнения лабораторной работы №4
по курсу «Сети ЭВМ и телекоммуникации»

Тема работы: Изучение методов настройки сетевых экранов и технологии отображения портов.

Цель работы: Получить навыки настройки межсетевого экрана (netfilter) в ОС Linux. Выявить множество параметров, доступных для администрирования в межсетевом экране.

Порядок выполнения работы

В данной работе будет проведена установка и конфигурирование программного обеспечения фильтрации сетевого трафика. Рекомендуется придерживаться следующего плана выполнения:

1. Создать правило для использования межсетевого экрана в режиме запрета всех входящих передач с компьютера с адресом 10.44.0.66. При установленном пакете iptables это реализуется следующей командой:

```
iptables -A INPUT -s 10.44.0.66 -j DROP
```

В результате проделанных действий были заблокированы входящие пакеты приходящие от компьютера, имеющий IP адрес 10.44.0.66. Блокировка проверяется командой ping 10.44.0.30.

2. Удалить добавленное правило из цепочки правил командой:

```
iptables -D INPUT -s 10.44.0.66 -j DROP
```

Удаление правила соответствует разрешению прохождения пакетов на адрес 10.44.0.30.

Команда iptables -F очищает все правила в каждой цепочке.

3. Провести эксперимент с пробросом пакетов с сетевого порта одного компьютера на другой компьютер с заданным ip-адресом. Для этого запускаются две виртуальные машины под управление ОС Unix и ПО эмуляции виртуальной машины VirtualBox. В качестве типа внешней связи для сетевого адаптера выберем сетевой мост, что способствует прямому соединению с локальной сетью по схеме заезда.

4. На каждой из виртуальных машин необходимо узнать ip адреса, анализом вывода команды ifconfig. Необходимо выбрать среди виртуальных компьютеров сетевой шлюз волевым решением.

На шлюзе вводятся команды:

- 1) iptables -t nat -A PREROUTING -p tcp -d 10.44.0.31 --dport 22 -j DNAT --to-destination 10.44.0.30:22
- 2) iptables -A FORWARD -i eth0 -d 10.44.0.30 -p tcp -d 10.44.0.31 --dport 22 -j ACCEPT

Содержание отчета

1. Цель работы;
2. Ход выполнения работы с промежуточными выводами и графическими фрагментами копий экрана;
3. Выводы по работе и их возможные обобщения;