Сетевое экранирование. Работа с iptables.

- Войдите в систему и определите IP-адрес вашего компьютера. Используйте утилиты ifconfig или ip. Просмотрите текущие правила, установленные в iptables: `sudo iptables -L` (Сбрасываются правила `sudo iptables -F`)
  Никогда не сохраняйте вводимые правила командами типа *save* . Результаты выполнения ваших команд и вводимых правил, проверяйте и фиксируйте в отчете по лабораторной работе.

- Для целей безопасности и сокрытия внутренней сетевой инфраструктуры ICMP ping запросы извне можно запретить :

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

- Чтобы открыть хост для входящих ICMP запросов и исходящих ICMP ответов выполняются правила:

```
sudo iptables -I INPUT -i eth0 -p icmp --icmp-type 8 -s 0/0 -d
$SERVER_IP -m state --state NEW, ESTABLISHED, RELATED -j ACCEPT

sudo iptables -I OUTPUT -i eth0 -p icmp --icmp-type 0 -s
$SERVER_IP --d 0/0 -m state –state ESTABLISHED, RELATED -j
ACCEPT
```

где: `$SERVER_IP` - IP-адрес хоста,
`icmp-type 8` - эхо-запрос,
`icmp-type 0` - эхо-ответ,
`0/0` - любой адрес.

- Ограничить ping запросы определенным количеством в единицу времени можно:

```
sudo iptables -A INPUT -p icmp -m icmp -m limit -limit 1/second
-j ACCEPT
```

- Заблокировать все входящие запросы с определенного адреса (например, 192.168.0.6) можно:

```
sudo iptables -A INPUT -s 192.168.0.6 -j DROP
```

- Чтобы не пропускать все входящие запросы порта 80, надо выполнить:

```
sudo iptables -A INPUT -p tcp --dport 80 -j DROP
```

- Если необходимо заблокировать входящий запрос порта 80 с определенного адреса (например, 192.168.0.6), тогда:

```
sudo iptables -A INPUT -p tcp -s 192.168.0.6 --dport 80 -j DROP
```

- Сбросить трафик с определенного (00:0F:EA:91:04:08) MAC адреса:

```
sudo iptables -A INPUT -m mac –mac-source 00:0F:EA:91:04:08 -j
DROP
```

или разрешить только для протокола TCP:

```
sudo iptables -A INPUT -p tcp --destination-port 22 -m mac –mac-
source 00:0F:EA:91:04:08 -j ACCEPT
```

Для углубленного изучения iptables подойдет первоисточник, с наиболее подробным описанием:

https://www.opennet.ru/docs/RUS/iptables/#ACCEPTTARGET

https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

ТРЕБОВАНИЯ К ОТЧЕТАМ

По результатам выполнения лабораторных работ необходимо составлять отчет. Рекомендуется составлять отчет параллельно с выполнением заданий лабораторных работ, не оставляя этот процесс на потом. Отчет должен быть оформлен с титульным листом с названием университета, института и высшей школы. На титульном листе указывается ф.и.о. студента исполнителя работы, номер студенческой группы и ф.и.о. преподавателя.
В отчете приводится информация, удостоверяющая выполнение студентом заданий лабораторных работ: скриншоты с результатами исполнения сценариев, команд и программ, командных файлов, дампы памяти и пакетов, составленные вами скрипты (*BASH* или др.), ответы на поставленные в заданиях вопросы и т.д.
Результаты выполнения каждого из заданий должны предваряться в отчете фрагментом текста, формулирующим само задание (фрагменты копируются прямо из текста заданий).
Защита лабораторных работ происходит по предъявлению оформленного отчета и сопровождается демонстрацией исполнения программ и командных файлов, а также ответами на вопросы преподавателя.
Отчет можно создавать под *ОС Linux*, например, с помощью приложения *LibreOffice Writer* , сохраняя в *Home* каталоге вашего рабочего компьютера. Либо можете использовать офисные средства от MS Windows или MacOS.