Сетевое экранирование. Применение правил iptables

- Войдите в систему и определите IP-адрес вашего компьютера. Используйте утилиты ifconfig или ip. Кроме того, в дальнейшем понадобятся IP-адреса еще одного-двух компьютеров сети.

- Просмотрите текущие правила, установленные в iptables:
`sudo iptables -L` (Сбрасываются правила `sudo iptables -F`)

  Результаты выполнения ваших команд, а также последствия применения вводимых вами правил протоколируйте в отчете о лабораторной работе.
  Никогда не сохраняйте вводимые правила командами типа *save* .

- Введите правило, блокирующее весь входящий трафик на ваш компьютер. Блокировать весь приходящий трафик нужно в таблице filter (выбирается по умолчанию) цепочки INPUT:
```
sudo iptables -A INPUT -j DROP
```
  Проверьте наличие введенного правила в системе.
  Текущие правила в iptables в заданной таблице можно посмотреть командой `sudo iptables -t <table-name> -L`
  Убедитесь, что весь трафик блокирован, например, по бездействию браузера, ping и др.

- Добавьте правила для фильтрации входящего трафика (с использованием целей DROP и ACCEPT) так, чтобы веб-трафик проходил, а остальной был блокирован.
  Вначале запретим весь трафик:
```
sudo iptables -P INPUT DROP
```
  Разрешим трафик для loopback, чтобы внутренние сервисы нормально работали:
```
sudo iptables -A INPUT -i lo -j ACCEPT
```
  Теперь разрешим те TCP и UDP соединения, которые сами создаем:
```
sudo iptables -A INPUT -p tcp -m state --state
               ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p udp -m state --state
               ESTABLISHED,RELATED -j ACCEPT
```
  Разрешим работу DNS-сервиса:
```
sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p tcp --sport 53 -j ACCEPT
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p udp --sport 53 -j ACCEPT
```
  Разрешим http и https:
```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```
  Убедитесь в том, что теперь веб-трафик стабилен.

Посмотреть видеоматериалы по данной тематике можно, например, на ресурсах:

Introduction:
https://www.youtube.com/watch?v=iP8YWcvKDr0

Tables and Chains:
https://www.youtube.com/watch?v=jgH976ymdoQ

Rules and Targets:
https://www.youtube.com/watch?v=0QAiEtsKEpc

Packet Processing:
https://www.youtube.com/watch?v=yE82upHCxfU

Working with iptables:
https://www.youtube.com/watch?v=9rLVI2UUdoo

Для углубленного изучения iptables подойдет первоисточник, с наиболее полным 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.