### Задание 19.4.2 (HW-03)

**Персонализация:** Михайлов Юрий Никитич (uramihajlov481@gmail.com)

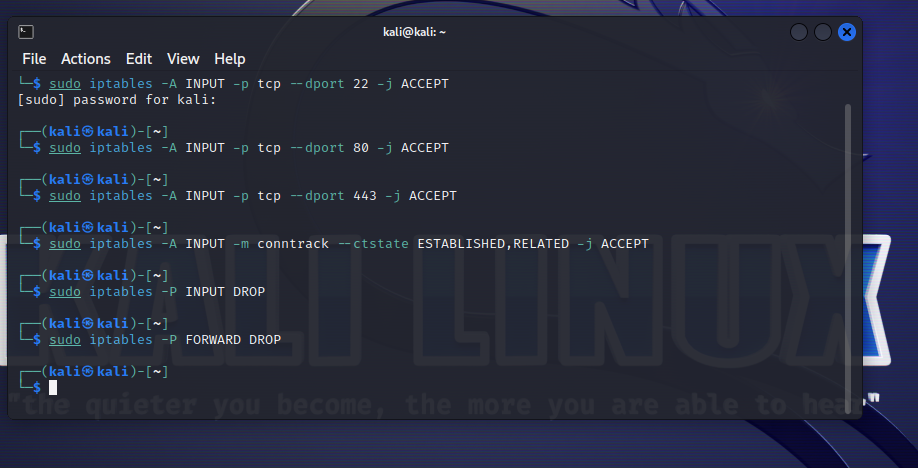
**Лабораторная работа:** Задание**№**19.4.2 (HW-03)**:**

Общая информация:

* Период тестирования: 27.03.2024
* Объект тестирования: firewall (iptables)
* Описание действий:

**Описание действий:  
  
1) Настройка правил для портов TCP:**

* **sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT**: Эта команда добавляет правило для разрешения входящих TCP-соединений на порт 22 (SSH).
* **sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT**: Эта команда добавляет правило для разрешения входящих TCP-соединений на порт 80 (HTTP).
* **sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT**: Эта команда добавляет правило для разрешения входящих TCP-соединений на порт 443 (HTTPS).
* **sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT**: Это правило разрешает входящие пакеты, связанные с уже установленными TCP-соединениями.



**2) Настройка правил для порта UDP:**

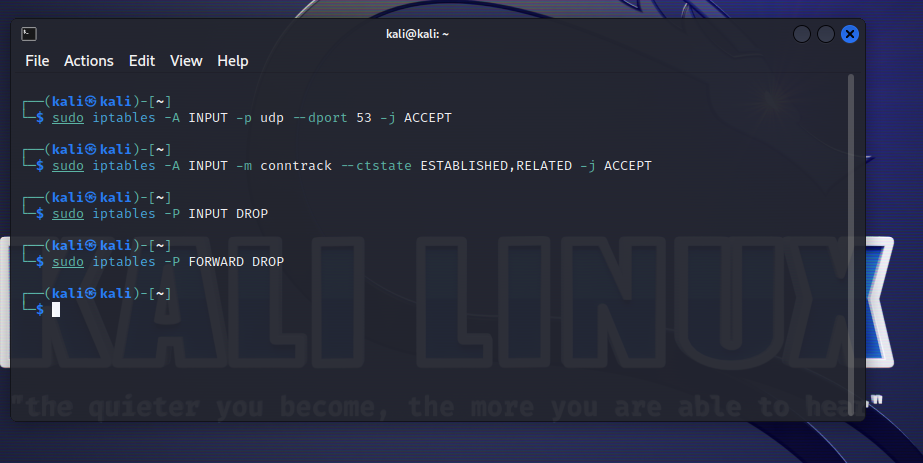
* **sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT: Эта команда добавляет правило для разрешения входящих UDP-соединений на порт 53 (DNS).**

**3) Запрещение входящего ICMP-трафика:**

* + **sudo iptables -A INPUT -p icmp --icmp-type 8 -j REJECT: Эта команда добавляет правило для отклонения входящего ICMP-трафика, который используется для отправки эхо-запросов (ping). Тип ICMP-пакета 8 обозначает эхо-запрос.**

**4) Установка политики по умолчанию:**

* + **sudo iptables -P INPUT DROP: Эта команда устанавливает политику по умолчанию для входящего трафика как DROP, что означает, что все входящие пакеты, не совпадающие с уже определенными правилами, будут отброшены.**
  + **sudo iptables -P FORWARD DROP: Эта команда устанавливает политику по умолчанию для трафика, проходящего через маршрутизатор, также как DROP.**

****

**5) Сохранение правил:**

* + **sudo iptables-save > /etc/iptables/rules.v4: Эта команда сохраняет текущие правила iptables в файл /etc/iptables/rules.v4, чтобы они применялись при перезагрузке системы.**

**6) Включение перенаправления IP-трафика:**

* + **sudo sysctl -w net.ipv4.ip\_forward=1: Эта команда включает перенаправление IP-трафика, если оно не было включено. Это может потребоваться, если ваша система выполняет функции маршрутизации или NAT.**

****

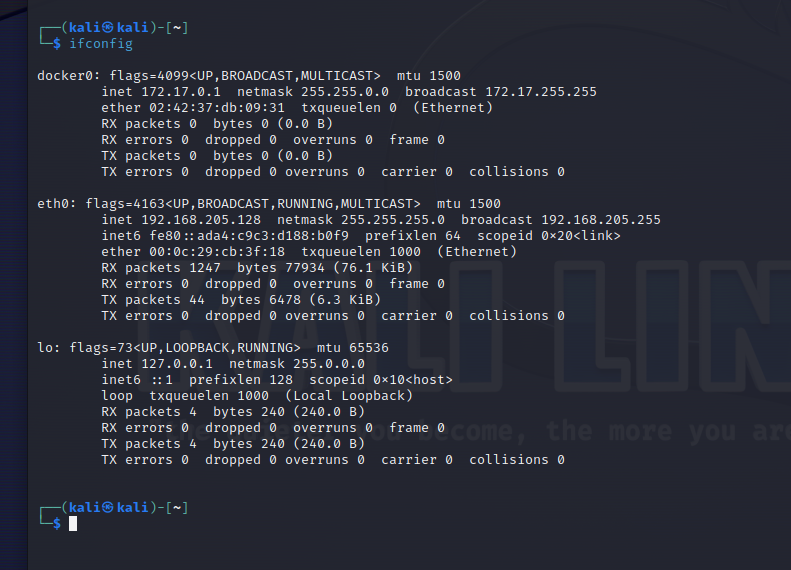
**7) Отображение текущих правил:**

* + **sudo iptables -L -n: Эта команда отображает текущие правила iptables, которые были установлены.**

****

**8) Отображение информации о сетевых интерфейсах:**

* **ifconfig: Эта команда отображает информацию о сетевых интерфейсах, включая их IP-адреса.**

****