**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №13**

*дисциплина: Основы администрирования операционных систем*

Студент: Ко Антон Геннадьевич Студ. билет № 1132221551 Группа: НПИбд-02-23

**МОСКВА**

2024 г.

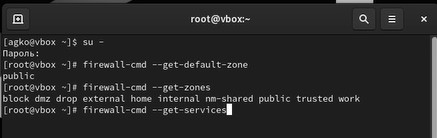
# Цель работы:

Целью данной работы является получение навыков настройки пакетного фильтра в Linux.

**Выполнение работы:**

# Управление брандмауэром с помощью firewall-cmd:

Получим полномочия администратора: **su -**. После чего определим текущую зону по умолчанию, введя: **firewall-cmd --get-default-zone** и доступные зоны, введя: **firewall-cmd --get-zones.** Посмотрим службы, доступные на нашем компьютере, используя **firewall-cmd --get-services** (Рис. 1.1):



**Рис. 1.1.** Запуск терминала и получение полномочий администратора,

определение текущей зоны по умолчанию и доступные зоны. Просмотр служб, доступных на компьютере.

Определим доступные службы в текущей зоне: **firewall-cmd --list-services**

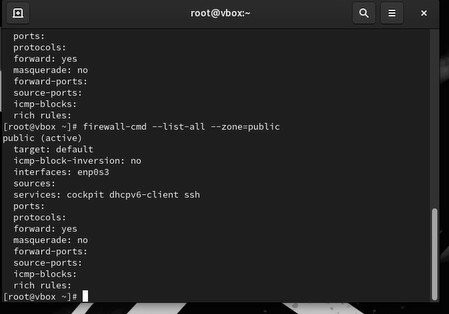
(Рис. 1.2):



**Рис. 1.2.** Определение доступных служб в текущей зоне.

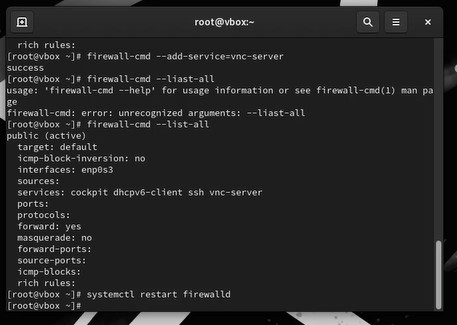
Сравним результаты вывода информации при использовании команды

**firewall-cmd --list-all** и команды **firewall-cmd --list-all --zone=public** (Рис. 1.3):



**Рис. 1.3.** Сравнение результатов вывода информации при использовании команд.

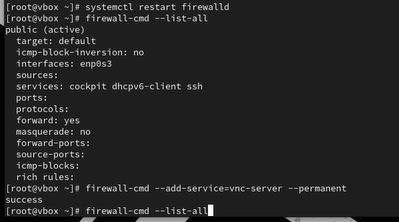
Добавим сервер VNC в конфигурацию брандмауэра: **firewall-cmd --add- service=vnc-server** и проверим, добавился ли vnc-server в конфигурацию: **firewall-cmd --list-all** (добавился). Перезапустим службу firewalld: **systemctl restart firewalld** (Рис. 1.4):



**Рис. 1.4.** Добавление сервера VNC в конфигурацию брандмауэра, проверка добавления в конфигурацию, перезапуск службы firewalld.

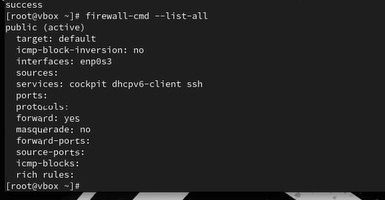
Проверим, есть ли vnc-server в конфигурации: **firewall-cmd --list-all.** Обратим внимание, что служба vnc-server больше не указана. Добавим службу vnc-server ещё раз, но на этот раз сделаем её постоянной, используя команду **firewall-cmd**

**--add-service=vnc-server --permanent** (Рис. 1.5):



**Рис. 1.5.** Проверка наличия vnc-server в конфигурации, добавление службы vnc- server, сделав её постоянной.

Теперь проверим наличие vnc-server в конфигурации: **firewall-cmd --list-all.** Мы видем, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения (Рис. 1.6):



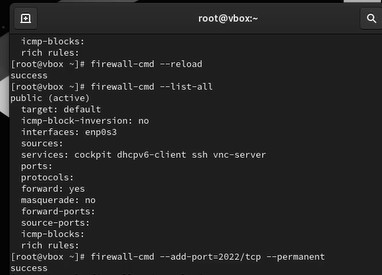
**Рис. 1.6.** Проверка наличия vnc-server в конфигурации.

Перезагрузим конфигурацию firewalld и просмотрим конфигурацию времени выполнения:

# firewall-cmd --reload firewall-cmd --list-all

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP:

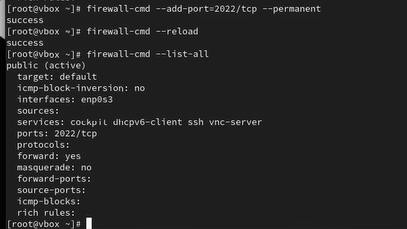
# firewall-cmd --add-port=2022/tcp --permanent (Рис. 1.7):



**Рис. 1.7.** Перезагрузка конфигурации firewalld и просмотр конфигурации времени выполнения, добавление в конфигурацию межсетевого экрана порт

2022 протокола TCP.

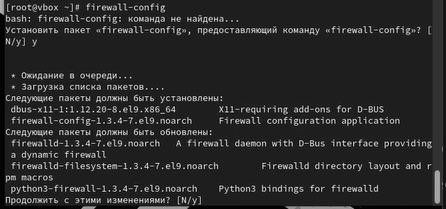
Затем перезагрузим конфигурацию firewalld: **firewall-cmd --reload** и проверим, что порт добавлен в конфигурацию: **firewall-cmd --list-all** (Рис. 1.8):



**Рис. 1.8.** Перезагрузка конфигурации firewalld и проверка добавления порта в конфигурацию.

# Управление брандмауэром с помощью firewall-config:

Откроем терминал и получим полномочия администратора, после чего установим интерфейс GUI firewall-config (Рис. 2.1):



**Рис. 2.1.** Получение полномочий администратора и установка интерфейса GUI firewall-config.

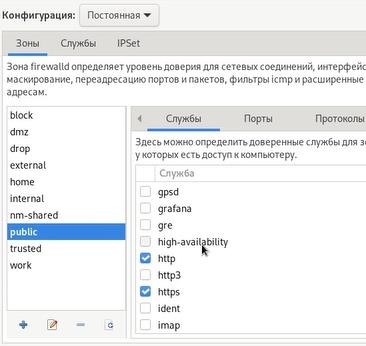
После успешной установки откроем терминал под учётной записью своего пользователя и запустим интерфейс GUI firewall-config: **firewall-config**.

Нажмём на выпадающее меню рядом с параметром **Configuration**. Откроем раскрывающийся список и выберем **Permanent**. Это позволит сделать постоянными все изменения, которые мы вносим при конфигурировании (Рис. 2.2):



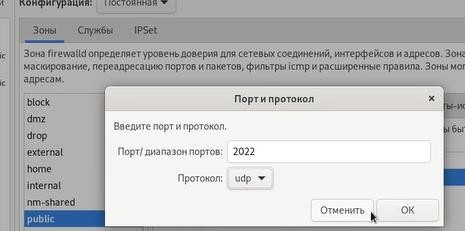
**Рис. 2.2.** Позволение делать постоянными все изменения при конфигурировании.

Далее выберем зону **public** и отметим службы **http**, **https** и **ftp**, чтобы включить их (Рис. 2.3):



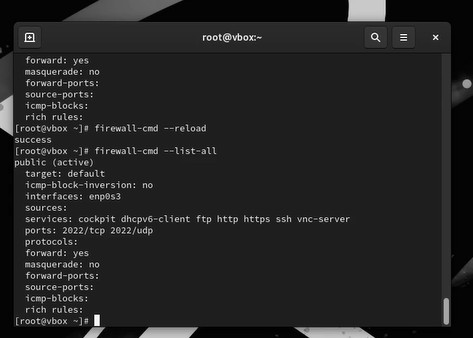
**Рис. 2.3.** Включение служб http, https и ftp.

На следующем шаге выберем вкладку Ports и на этой вкладке нажмём Add. Введём порт 2022 и протокол udp, нажмём ОК, чтобы добавить их в список. Затем закроем утилиту firewall-config (Рис. 2.4):



**Рис. 2.4.** Добавление порта 2022 и протокол udp, закрытие утилиты firewall- config.

В окне терминала введём **firewall-cmd --list-all**, обратим внимание, что изменения, которые мы только что внесли, ещё не вступили в силу. Это связано с тем, что мы настроили их как постоянные изменения, а не как изменения времени выполнения. Перегрузим конфигурацию firewall-cmd: **firewall-cmd -- reload** (Рис. 2.5).



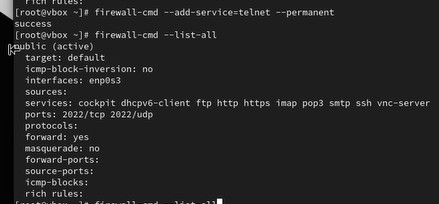
**Рис. 2.5.** Проверка изменений и перезагрузка конфигурации firewall-cmd.

# Самостоятельная работа:

Запустим терминал и получим полномочия администратора: **su -**. Создадим конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:

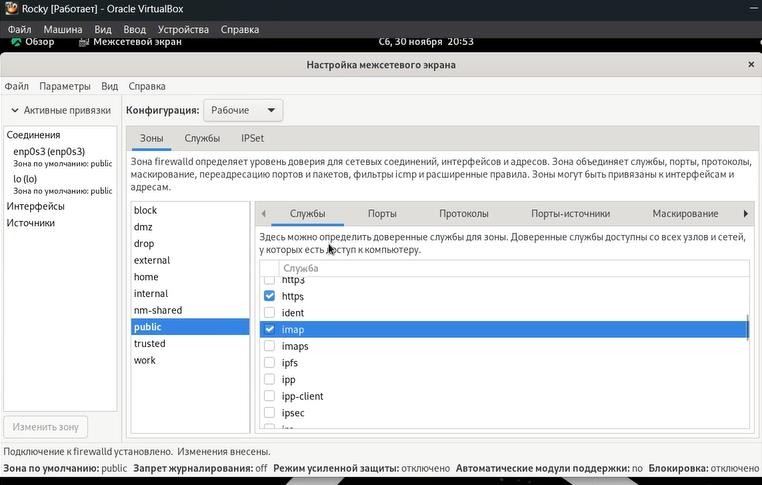
* **telnet;**
* **imap;**
* **pop3;**
* **smtp;**

Сделаем это как в командной строке (для службы telnet): **firewall-cmd—add- service=telnet --permanent**, так и в графическом интерфейсе (для служб imap, pop3, smtp): **firewall-config** (Рис. 3.1):



**Рис. 3.1.** Создание конфигурацию межсетевого экрана, позволяющая получить доступ к определённым службам.

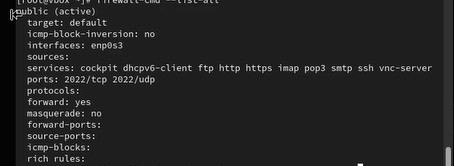
Нажмём на выпадающее меню рядом с параметром **Configuration**. Откроем раскрывающийся список и выберем **Permanent**. Далее выберем зону **public** и отметим службы **imap**, **pop3** и **smtp**, чтобы включить их. Затем закроем утилиту firewall-config (Рис. 3.2):



**Рис. 3.2.** Позволение делать постоянными все изменения при

конфигурировании, включение служб imap, pop3 и smtp, закрытие утилиты.

Убедимся, что конфигурация является постоянной и будет активирована после перезагрузки компьютера (Рис. 3.3):



**Рис. 3.3.** Перезагрузка конфигурации firewall-cmd и списка доступных

сервисов.

# Ответы на контрольные вопросы:

1. Какая служба должна быть запущена перед началом работы с

менеджером конфигурации брандмауэра firewall-config? **sudo systemctl start firewalld**

1. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию? **firewall-cmd -add-port/udp –permanent**
2. Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах? **firewall-cmd –list-all-zones**
3. Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра? **firewall-cmd –remove-service=vnc-server**
4. Какая команда firewall-cmd позволяет активировать новую

конфигурацию, добавленную опцией --permanent? **firewall-cmd –reload**

1. Какой параметр firewall-cmd позволяет проверить, что новая

конфигурация была добавлена в текущую зону и теперь активна? **firewall-cmd -**

# -list-all --zone=<zone-name>

1. Какая команда позволяет добавить интерфейс eno1 в зону public? **firewall- cmd –zone=public –change-interface=enol**
2. Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен**? В зону по умолчанию (firewall- cmd –get-default-zone)**

# Вывод:

В ходе выполнения лабораторной работы были получены навыки настройки пакетного фильтра в Linux.