Лабораторная работа №13

Фильтр пакетов

Юсупова Ксения Равилевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Задание

1. Используя firewall-cmd:

– определить текущую зону по умолчанию;
– определить доступные для настройки зоны;
– определить службы, включённые в текущую зону;
– добавить сервер VNC в конфигурацию брандмауэра.

2. Используя firewall-config:

– добавьте службы http и ssh в зону public;
– добавьте порт 2022 протокола UDP в зону public;
– добавьте службу ftp.

3. Выполните задание для самостоятельной работы (раздел 13.5).

3 Выполнение лабораторной работы

Получили полномочия администратора, определили текущую зону по умолчанию, доступные зоны и посмотрели службы, доступные на компьютере(рис. 3.1).

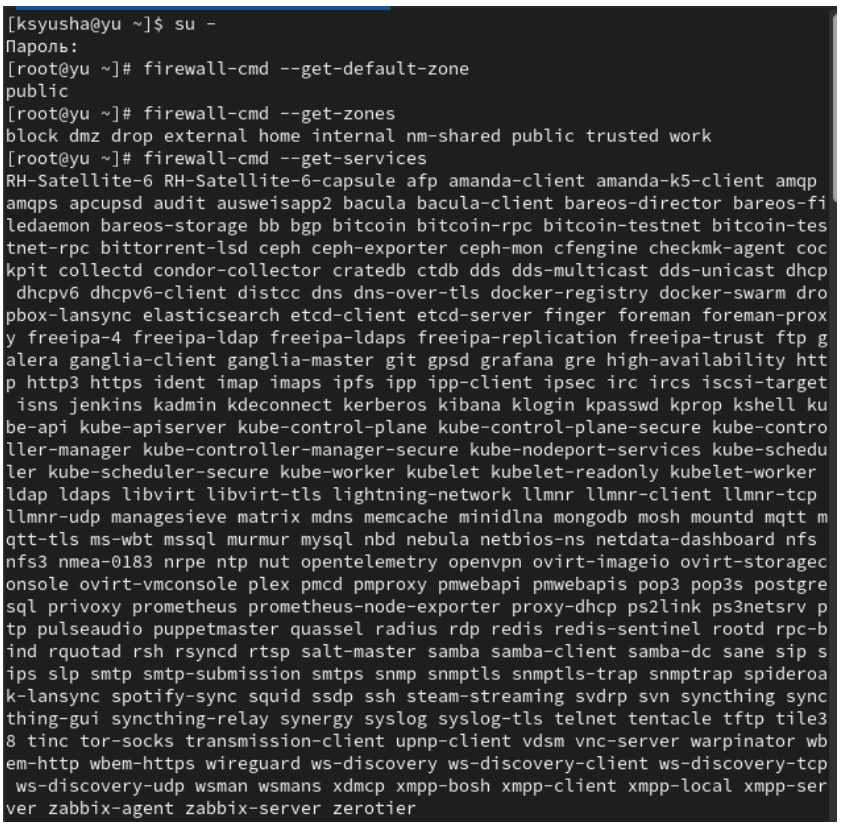

Рис. 3.1: Выполнили пункты 1-4 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Определили доступные службы в текущей зонеи сравнили результаты вывода информации при использовании команды firewall-cmd –list-all и команды firewall-

cmd –list-all –zone=public (рис. 3.2).

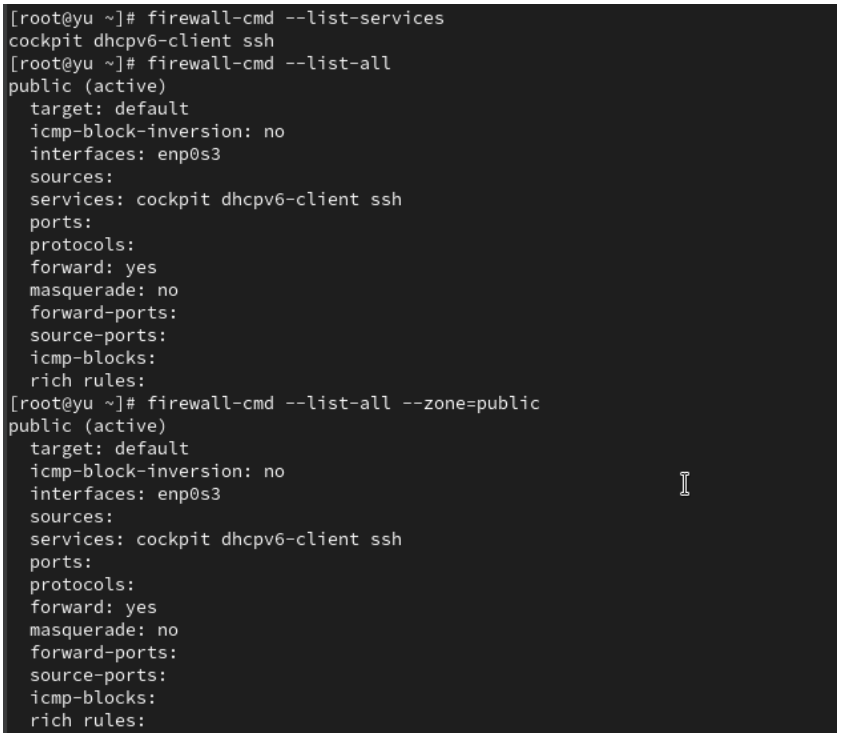

Рис. 3.2: Выполнили пункты 5-6 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Добавили сервер VNC в конфигурацию брандмауэра, проверили, что добавился vnc-server в конфигурацию. Перезапустили службу firewalld и проверили, что vnc-server нет в конфигурации, так как при использовании команды firewall-cmd –add-service=vnc-server без параметра –permanent правило добавляется только в текущую (runtime) конфигурацию брандмауэра, но не сохраняется в постоянную конфигурацию.(рис. 3.3).

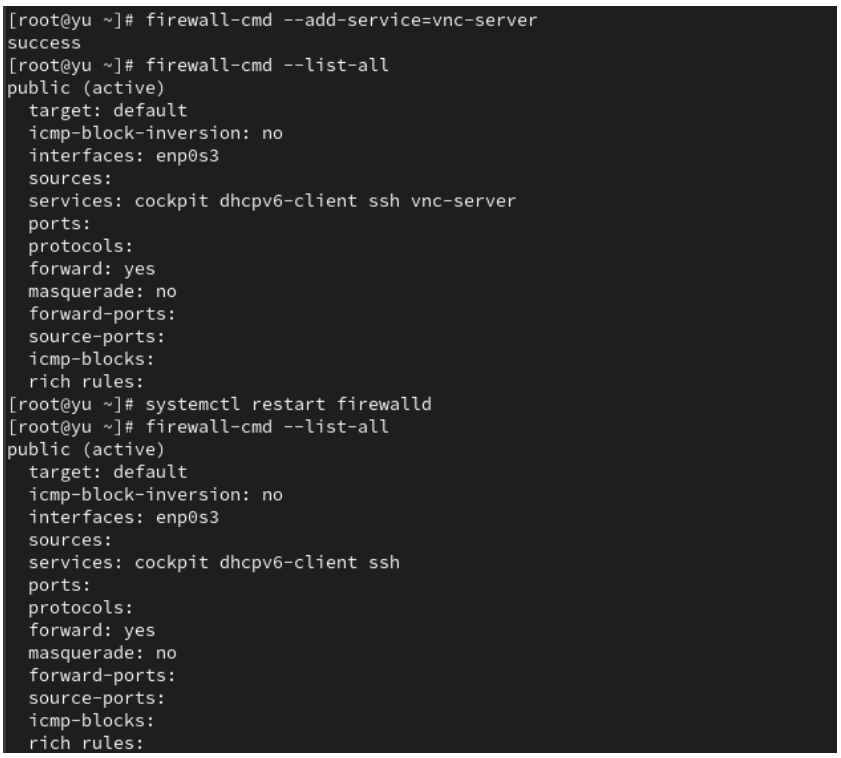

Рис. 3.3: Выполнили пункты 7-10 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Добавили службу vnc-server ещё раз, но на этот раз сделали её постоянной и проверили наличие vnc-server в конфигурации. Увидели, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения. Перезагрузилите конфигурацию firewalld и просмотрели конфигурацию времени выполнения(рис. 3.4).

```
[root@yu ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@yu ~]# firewall-cmd --reload
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.4: Выполнили пункты 11-13 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Добавили в конфигурацию межсетевого экрана порт 2022 протокола TCP и перезагрузили конфигурацию firewalld. Проверили, что порт добавлен в конфигурацию(рис. 3.5).

```
[root@yu ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@yu ~]# firewall-cmd --reload
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.5: Выполнили пункты 14 и 15 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Открыли терминал и под учётной записью своего пользователя запустили интерфейс GUI firewall-config. Нажали выпадающее меню рядом с параметром Configuration . Открыли раскрывающийся список и выбрали Permanent . Это позволило сделать постоянными все изменения, которые вносим при конфигурировании. Выберали зону public и отметили службы http, https и ftp, чтобы включить их. (рис. 3.6).

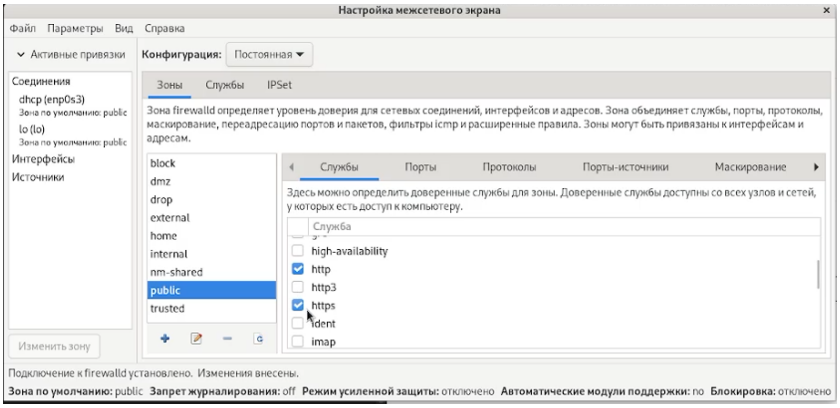

Рис. 3.6: Выполнили пункт 1-3 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

Выбрали вкладку Ports и на этой вкладке нажали Add . Ввели порт 2022 и протокол udp, закрыли утилиту firewall-config.(рис. 3.7).

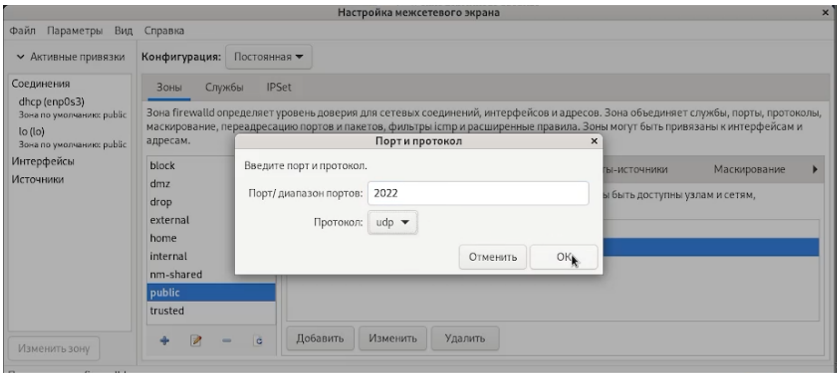

Рис. 3.7: Выполнили пункт 4 и 5 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

В окне терминала ввели firewall-cmd –list-all. Обратили внимание, что изменения, которые только что внесли, ещё не вступили в силу. Это связано с тем, что

настроили их как постоянные изменения, а не как изменения времени выполнения. Перегрузили конфигурацию firewall-cmd и список доступных сервисове, увидели, что изменения были применены.(рис. 3.8).

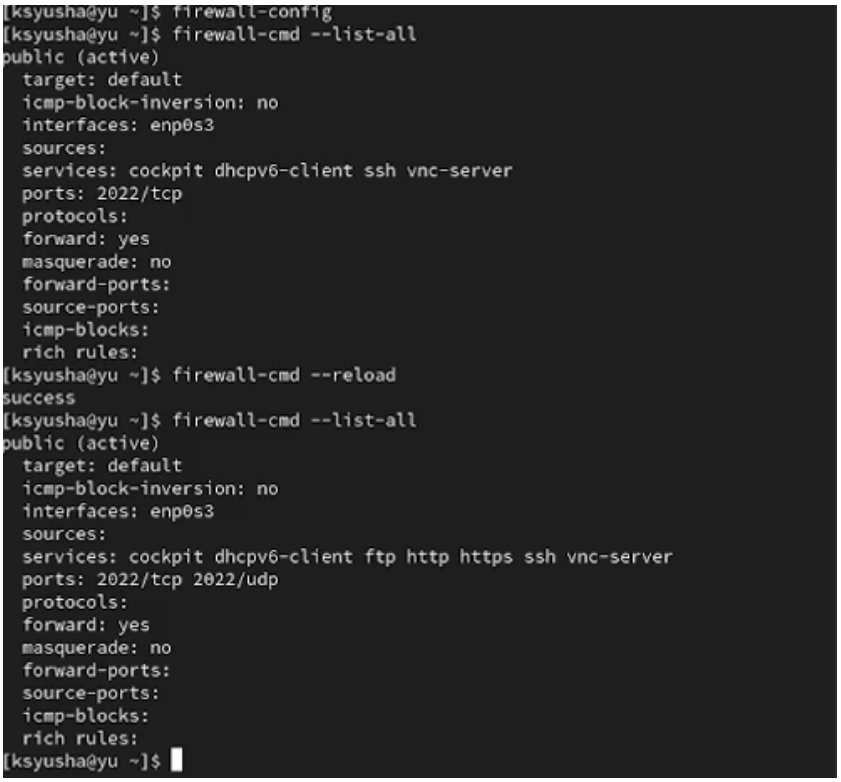

Рис. 3.8: Выполнили пункты 6 и 7 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

4 Выполнение самостоятельной работы

Создали в командной строке конфигурацию межсетевого экрана, которая позволяет получить доступ к службе telnet(рис. 4.1).

Рис. 4.1: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

Создали в графическом интерфейсе конфигурацию межсетевого экрана, которая позволяет получить доступ для служб imap, pop3, smtp (рис. 4.2).

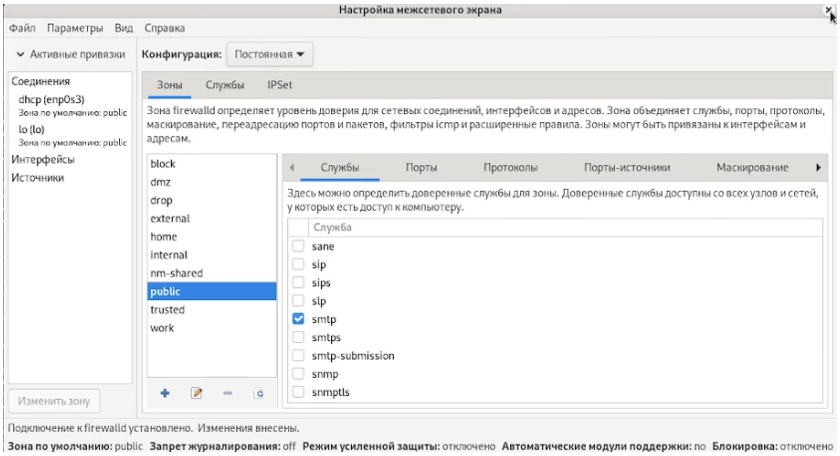

Рис. 4.2: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

Убедились, что конфигурация является постоянной и будет активирована после перезагрузки компьютера.(рис. 4.3).

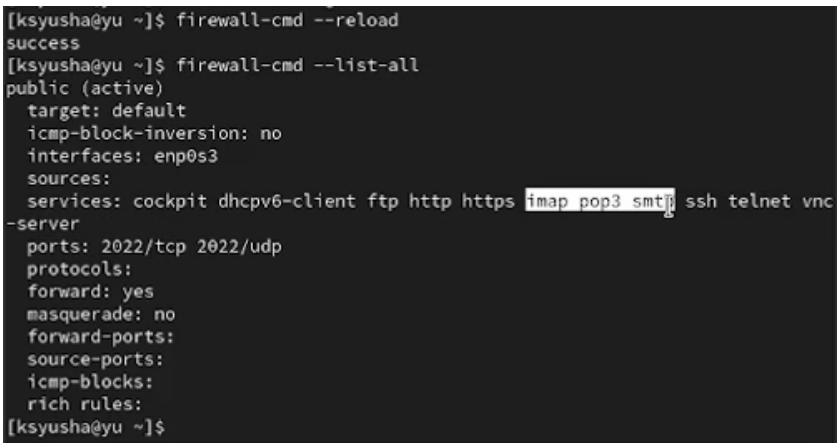

Рис. 4.3: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

5 Ответы на контрольные вопросы

1. Служба firewalld.service должна быть запущена перед работой с firewall-config, так как этот графический инструмент является фронтендом для управления демоном firewalld.

2. Команда firewall-cmd –add-port=2355/udp добавляет UDP-порт 2355 в текущую зону. Без параметра –permanent изменение будет временным и сбросится после перезагрузки службы.

3. Команда firewall-cmd –list-all-zones показывает полную конфигурацию всех зон, включая службы, порты, протоколы и настройки каждой зоны.

4. Команда firewall-cmd –remove-service=vnc-server удаляет службу vnc-server из текущей конфигурации. Для постоянного удаления нужно добавить параметр –permanent.

5. Команда firewall-cmd –reload активирует постоянную конфигурацию, загружая правила, добавленные с параметром –permanent, без полной перезагрузки службы.

6. Параметр –list-all показывает текущую активную конфигурацию выбранной зоны, позволяя убедиться, что изменения применились и теперь активны.

7. Команда firewall-cmd –zone=public –add-interface=eno1 назначает интерфейс eno1 конкретной зоне public. Для постоянного назначения требуется параметр –permanent.

8. Новый интерфейс автоматически добавляется в зону по умолчанию (обычно public), если не указана конкретная зона. Зону по умолчанию можно проверить командой firewall-cmd –get-default-zone.

6 Выводы

В ходе лабораторной работы мы получили навыки настройки пакетного фильтра в Linux.