Лабораторная работа №11

Администрирование сетевых подсистем

Машков Илья Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

2 Задание

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root.
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя.
3. Настройте удалённый доступ к серверу по SSH через порт 2022.
4. Настройте удалённый доступ к серверу по SSH по ключу.
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080.
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере.
7. Используя удалённое SSH-соединение, запустите с клиента графическое приложение на сервере.
8. Напишите скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile.

3 Выполнение лабораторной работы

3.1 Запрет удалённого доступа по SSH для пользователя root

Запускаю лог системных событий на сервере, а затем перехожу на клиент и пытаюсь получить доступ к серверу посредством ssh, но данная попытка терпит не удачу, т.к. client и server между собой никак не связаны (рис. [3.1]).

Рис. 3.1: Попытка обращения к серверу с помощью ssh

В файле sshd_config запрещаю вход на сервер пользователю root (рис. [3.2]).

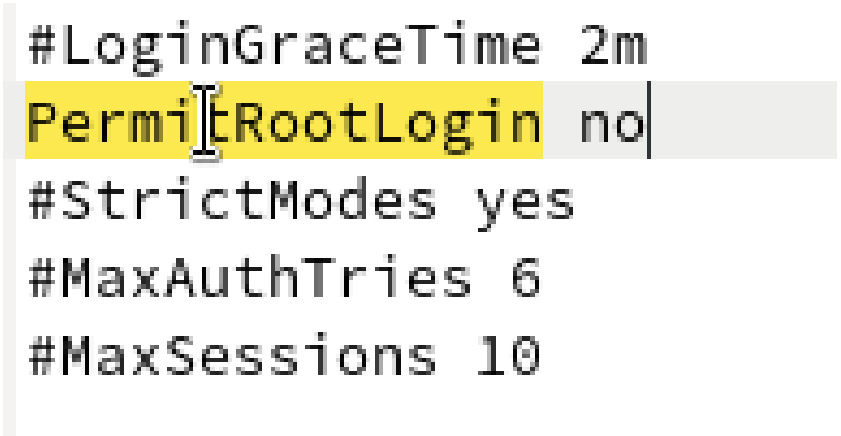

Рис. 3.2: Запрет доступа для пользователя root

Перезапускаю службу sshd (рис. [3.3]).

```
[root@server ~]# systemctl restart sshd
[root@server ~]#
```

Рис. 3.3: Перезапуск sshd

Снова пытаюсь получить доступ к серверу, но, увы, неудачно (рис. [3.4]).

```
[user@client ~]$ ssh root@server
ssh: Could not resolve hostname server: Name or service not known
[user@client ~]$
```

Рис. 3.4: Попытка обращения к серверу

3.2 Ограничение списка пользователей для удалённого доступа по SSH

Снова открываю файл sshd_config и добавляю строку, показанную на скрине, а потом перезагружаю sshd (рис. [3.5]). Ожидаемо, что повторная отправка тоже закончилась неудачей.

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
AllowUsers vagrant
#GatewayPorts no
```

Рис. 3.5: Редактирование sshd_config

Снова редактирую sshd_config, добавляя к ранее внесённой строке имя пользователя (рис. [3.6]).

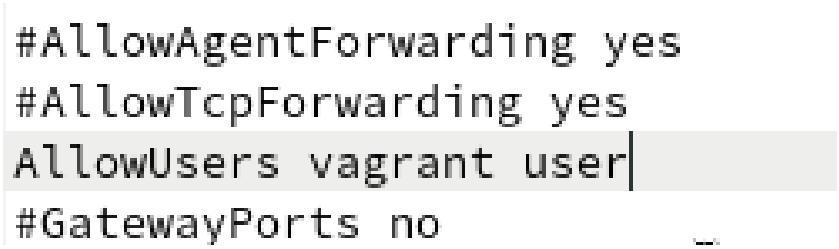

Рис. 3.6: Повторное редактирование sshd_config

3.3 Настройка дополнительных портов для удалённого доступа по SSH

В файл sshd_config добавляю строки, позволяющие организовать весь процесс через два порта (рис. [3.7]).

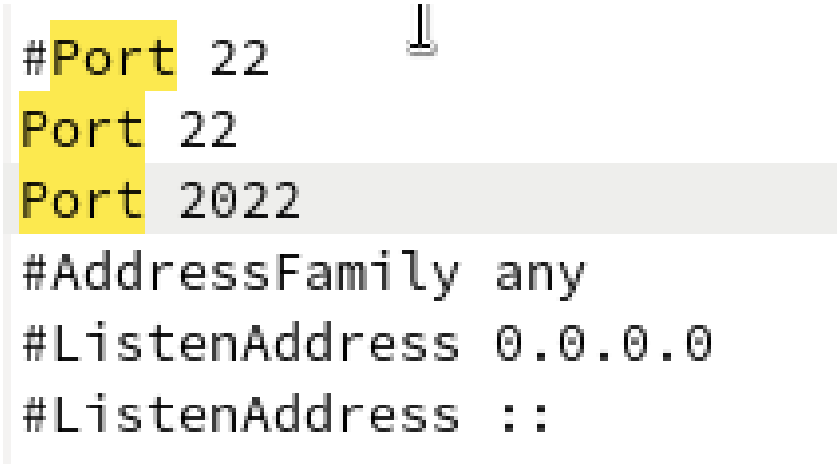

Рис. 3.7: Добавление организации через два порта

Перезапускаю службу sshd и просматриваю её статус. Вижу, что организацию через порт 2022 не получилось сделать (рис. [3.8]).

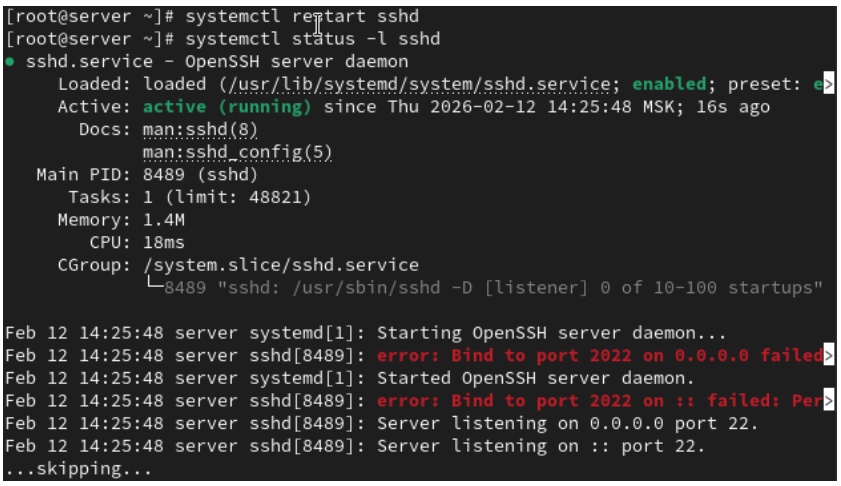

Рис. 3.8: Перезапуск sshd и и просмотр статуса

Смотрю логи и замечаю, что в доступе было отказано из-за службы SELinux (рис. [3.9]).

Рис. 3.9: Логи sshd

Исправляю метки SELinux относительно порта 2022, перенастраиваю межсетевой экран на работу с TCP-портом 2022, перезапускаю службу и просматриваю статус. В этот раз всё исправно (рис. [3.10]).

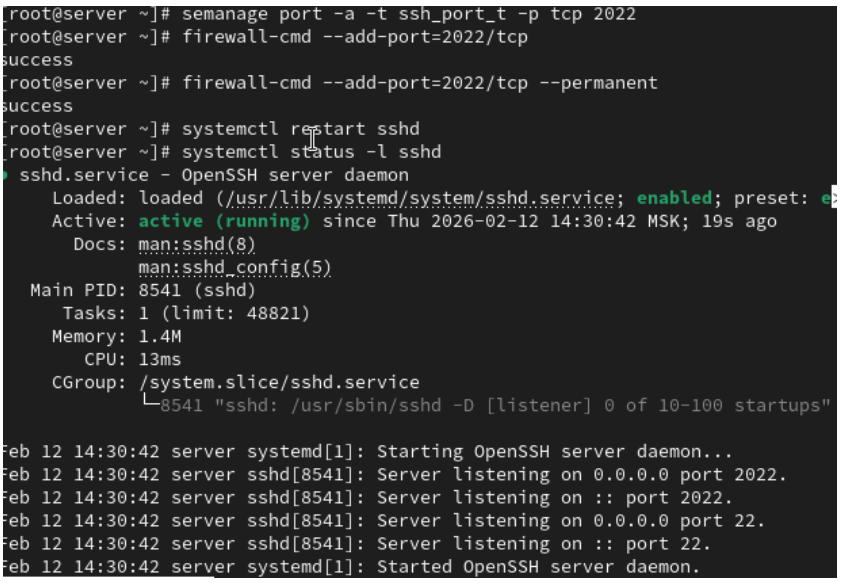

Рис. 3.10: Работа с метками безопасности, межсетевым экраном и перезапуск службы

3.4 Настройка удалённого доступа по SSH по ключу

В файле sshd_config добавляю строку, показанную на скрине (рис. [3.11]).

Рис. 3.11: Повторное редактирование sshd_config

Генерирую ssh-ключ (рис. [3.12]).

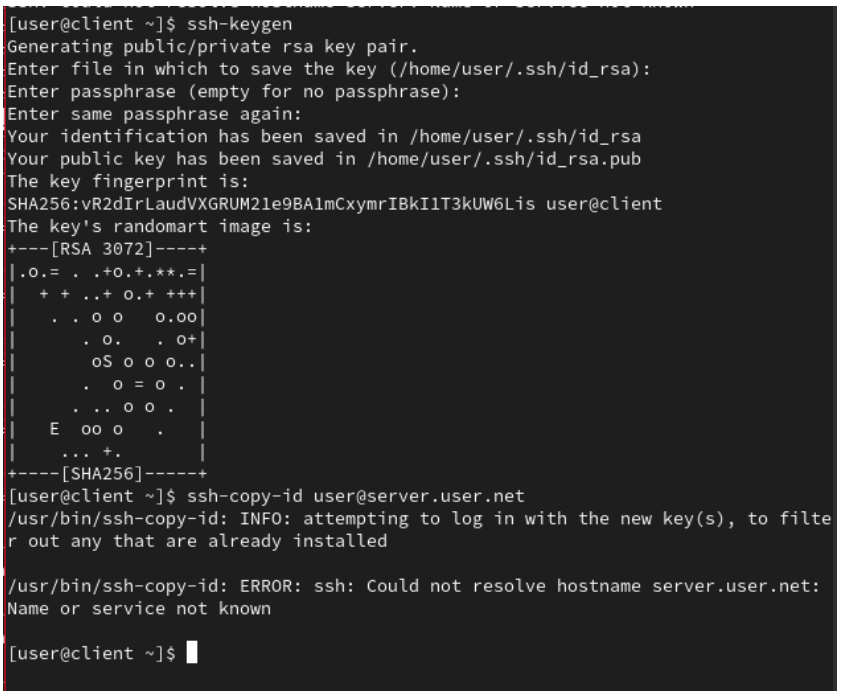

Рис. 3.12: Генерация ssh-ключа

Отправка ключа и обращение к серверу окончились ничем (рис. [3.13]).

Рис. 3.13: Обращение к серверу (и снова неудачное)

3.5 Организация туннелей SSH, перенаправление TCP-портов

На клиенте просматриваю активные службы с протоколом TCP (рис. [3.14]).

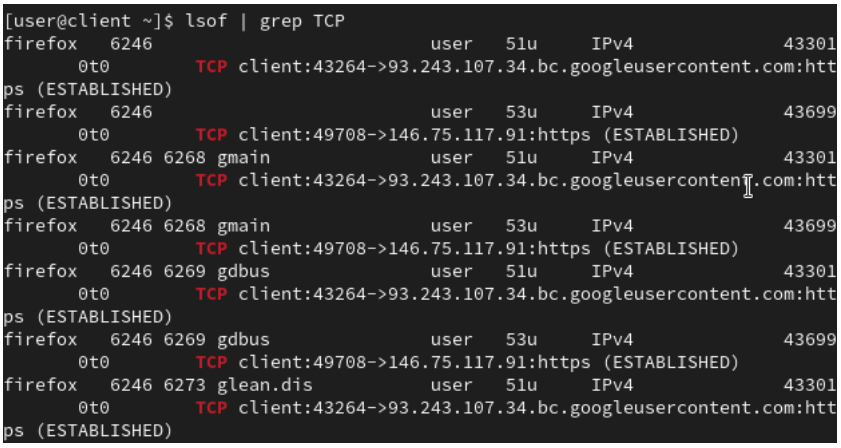

Рис. 3.14: Просмотр процессов с поротоколом TCP

Перенаправляю 80-ый порт на сервер server.user.net на порт 8080 на локальной машине (рис. [3.15]).

Рис. 3.15: Перенаправление портов

Затем просматриваю список служб с тем же протоколом, но, т.к. нет связи клиента с сервером, ничего не поменялось. Потом перехожу на адрес localhost:8080 и вижу, что к такому адресу я обратиться не могу по вышеобозначенной причине (рис. [3.16]).

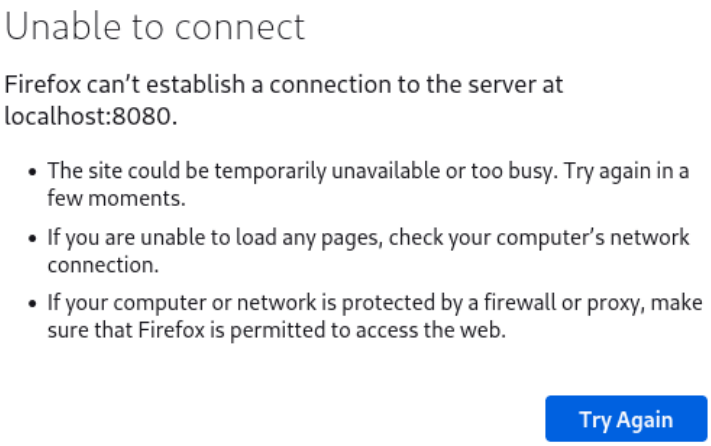

Рис. 3.16: localhost:8080

3.6 Запуск графических приложений через SSH (X11Forwarding)

В файле sshd_config разрешаю отображать на локальном клиентском компьютере графические интерфейсы X11 (рис. [3.17]).

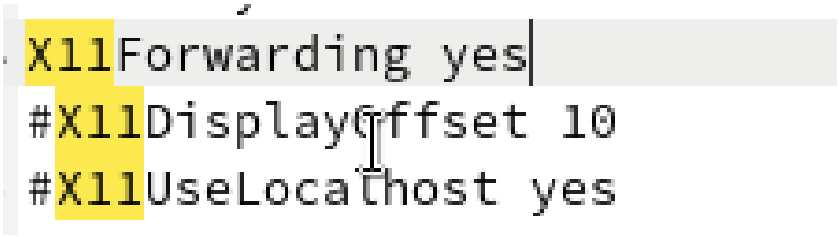

Рис. 3.17: Разрешение отображения граф. интерфейсов

3.7 Внесение изменений в настройки внутреннего окружения виртуальной машины

Копирую все задействованые в этой лабе конфигурационные файлы в файлы внутреннего окружения машины server. Создаю файл sshd.sh, который будет повторять все ключевые моменты из этой лабы при запуске системы (рис. [3.18]).

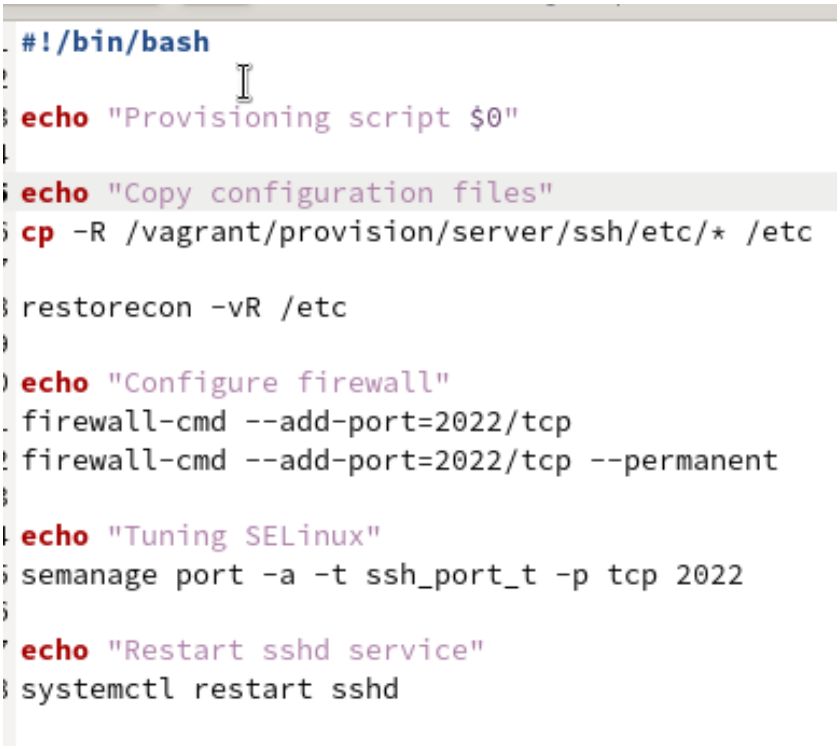

Рис. 3.18: sshd.sh

Для отработки скрипта добавляю соответствующую запись в Vagrantfile (рис. [3.19]).

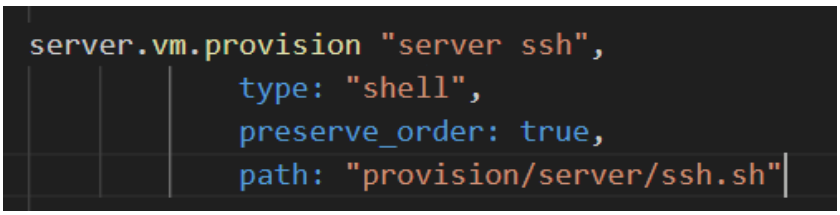

Рис. 3.19: Редактирование Vagrantfile

4 Выводы

В процессе выполнения данной лабораторной работы я приобрёл практические навыки по настройке удалённого доступа к серверу с помощью SSH.

Список литературы

Администрирование сетевых подсисем