Отчет по лабораторной работе №11

Настройка безопасного удалённого доступа по протоколу SSH

Галацан Николай, НПИбд-01-22

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

## 2.1 Запрет удалённого доступа по SSH для пользователя root

Запускаю ВМ через рабочий каталог. На ВМ server вхожу под собственным пользователем и перехожу в режим суперпользователя. Задаю пароль для пользователя root. В дополнительном терминале запускаю мониторинг системных событий. С клиента пытаюсь получить доступ к серверу через SSH-соединение через пользователя root, однако в доступе отказано (рис. 1).

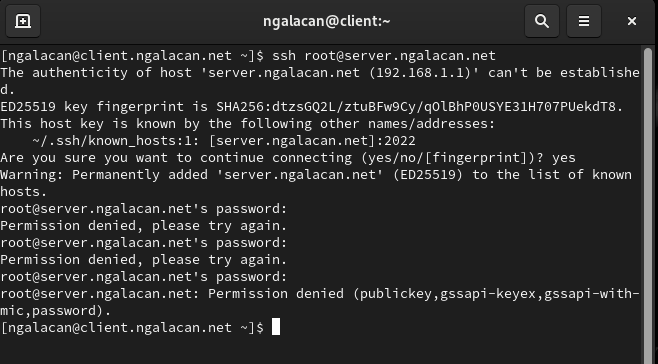


Рис. 1: Попытка получения доступа к серверу через root: отказ

В конфигурационном файле /etc/ssh/sshd\_config запрещаю вход на сервер пользователю root (рис. 2)

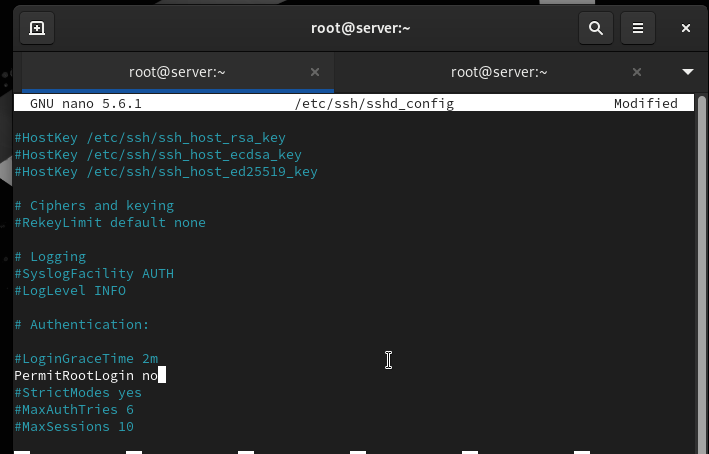


Рис. 2: Запрет входа на сервер пользователю root

Перезагружаю sshd. Повторяю попытку получения доступа через root, вновь получаю отказ в доступе.

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

клиента пытаюсь получить доступ к серверу через SSH-соединение через пользователя ngalacan, доступ получен (рис. 3)

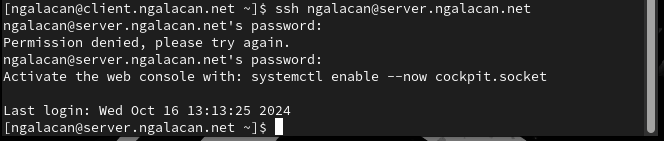


Рис. 3: Попытка получения доступа к серверу через ngalacan: доступ получен

В конфигурационном файле /etc/ssh/sshd\_config добавляю строку (рис. 4)

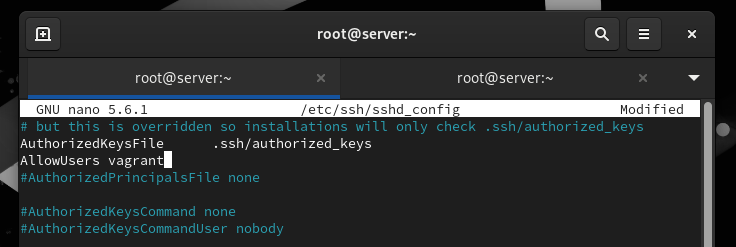


Рис. 4: Добавление строки в конфигурационный файл

Перезагрузив sshd, вновь пытаюсь с клиента получить доступ через пользователя ngalacan, но в доступе отказано (рис. 5).

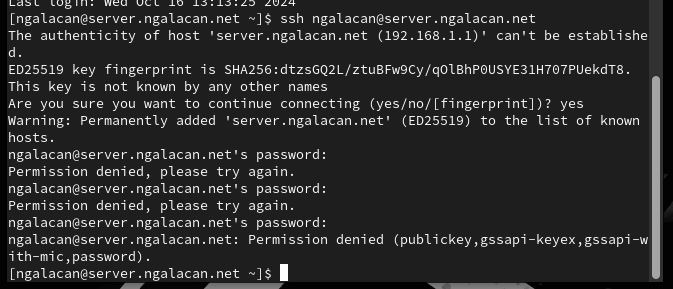


Рис. 5: Попытка получения доступа к серверу через ngalacan: отказ

В файле /etc/ssh/sshd\_config изменяю строку AllowUsers vagrant ngalacan. Пытаюсь с клиента получить доступ через пользователя ngalacan, доступ получен (рис. 6).

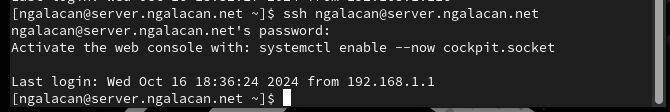


Рис. 6: Попытка получения доступа к серверу через ngalacan: доступ получен

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

В файле /etc/ssh/sshd\_config добавляю порты (рис. 7).

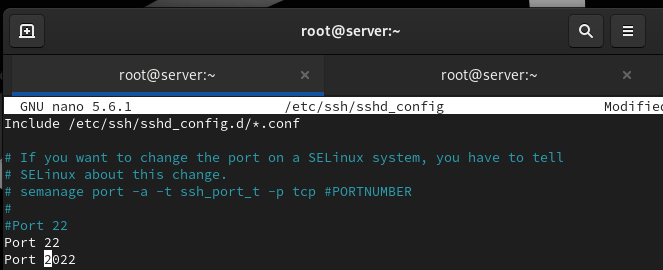


Рис. 7: Добавление портов

Перезапускаю sshd и просматриваю статус. Выводится отказ в работе через порт 2022 (рис. 8).

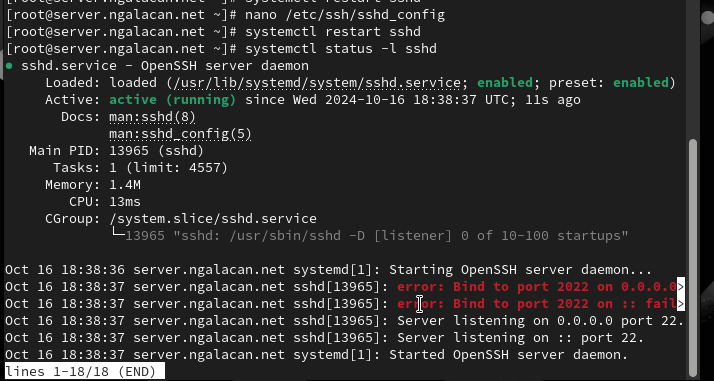


Рис. 8: Статус sshd: отказ в работе через порт 2022

Дополнительно просматриваю журнал системных событий и вижу сообщения об ошибках в SELinux (рис. 9).

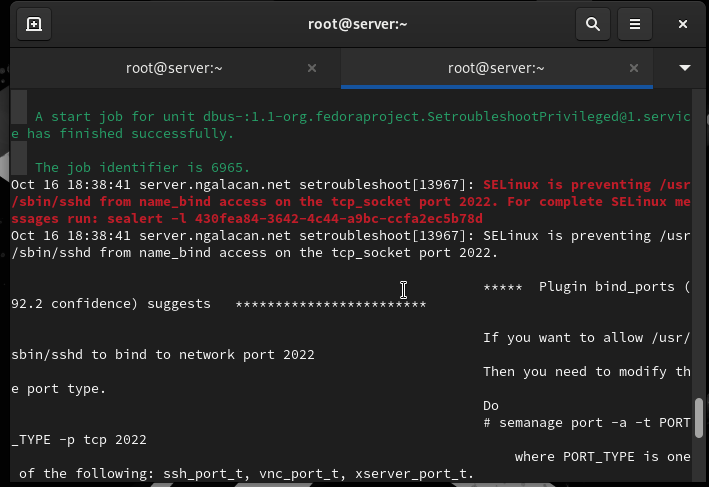


Рис. 9: Ошибки в журнале системных событий

Исправляю метки SELinux к порту 2022, настраиваю межсетевой экран, перезапускаю sshd и вновь просматриваю статус. Прослушиваются оба порта (рис. 10).

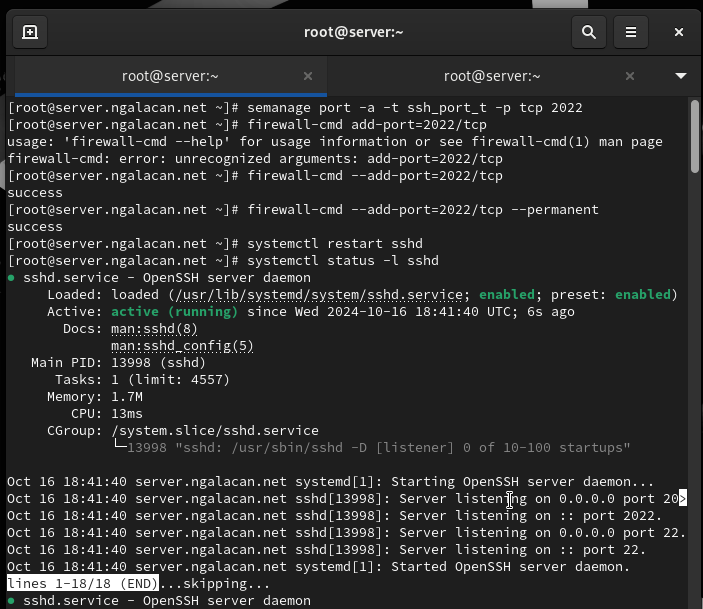


Рис. 10: Исправление меток SELinux, настройка межсетевого экрана, просмотр статуса sshd

C клиента пытаюсь получить доступ через пользователя. После открытия оболочки получаю доступ в root. Отлогиниваюсь от root и от пользователя на сервере. Повторяю попытку получения доступа через порт 2022, повторяю те же самые действия (рис. 11).

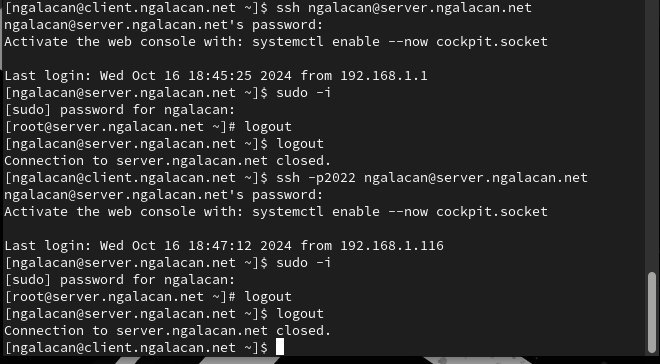


Рис. 11: Попытка получения доступа к серверу через ngalacan и через порт 2022: доступ получен

## 2.4 Настройка удалённого доступа по SSH по ключу

В файле /etc/ssh/sshd\_config разрешаю аутентификацию по ключу, перезапускаю сервис (рис. 12)

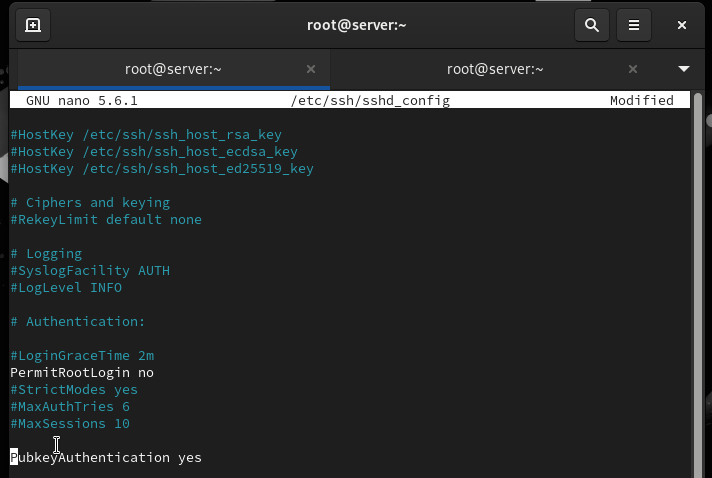


Рис. 12: Разрешение аутентификации по ключу

На клиенте генерирую SSH-ключ и копирую его на сервер. Пробую получить доступ к серверу через пользователя. Доступ получен, теперь не запрашивается пароль. Отлогиниваюсь с помощью ctrl+d (рис. 13).

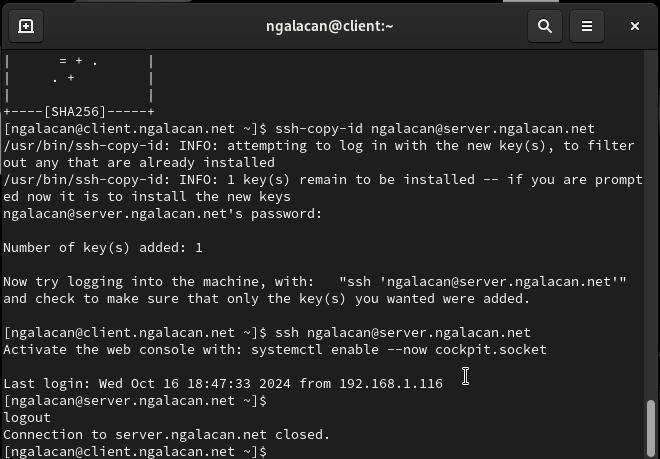


Рис. 13: Генерация SSH-ключа, копирование на сервер, попытка получения доступа: успешно

## 2.5 Организация туннелей SSH, перенаправление TCP-портов

На клиенте просматриваю, запущены ли какие-то службы с протоколом TCP (не запущены). Перенаправляю порт 80 на server.ngalacan.net на порт 8080. Вновь просматриваю службы с TCP (службы запущены) (рис. 14).

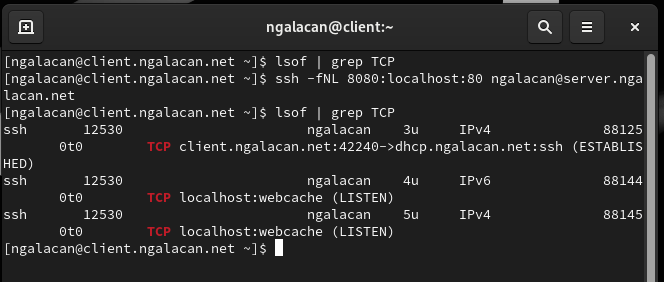


Рис. 14: Перенаправление порта 80 на server.ngalacan.net на порт 8080

Запускаю браузер и ввожу localhost:8080. Вижу приветственное сообщение сервера (рис. 15).

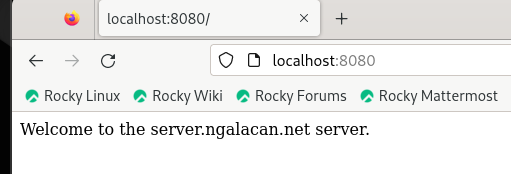


Рис. 15: localhost:8080 в браузере

## 2.6 Запуск консольных приложений через SSH

С клиента просматриваю имя узла, список файлов на сервере, почту (рис. 16).

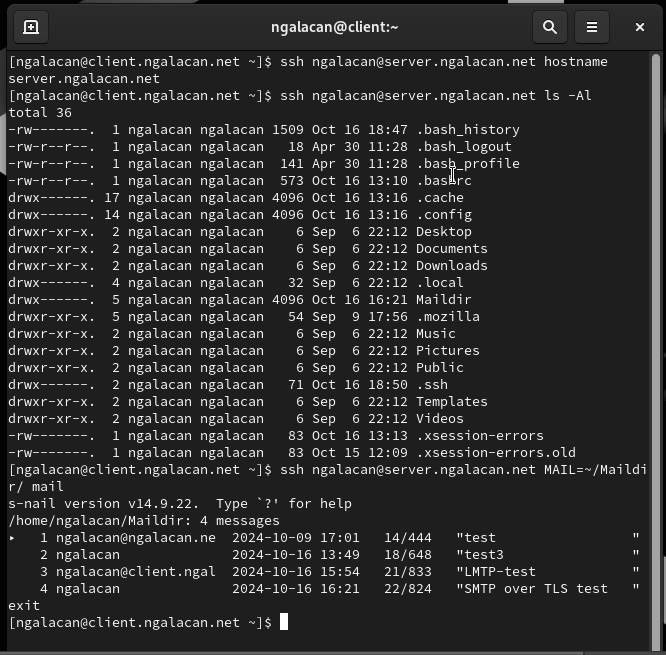


Рис. 16: Просмотр с клиента имени узла, файлов и почты на сервере

## 2.7 Запуск графических приложений через SSH

В файле /etc/ssh/sshd\_config разрешаю отображать на локальном клиентском компьютере графические интерфейсы X11 и перезапускаю сервис (рис. 17).

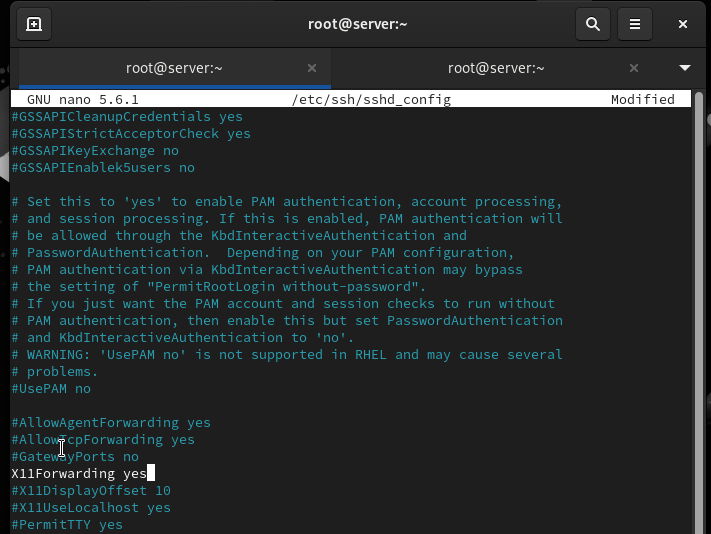


Рис. 17: Разрешение отображения графических интерфейсов X11

С клиента удаленно подключаюсь к серверу и запускаю firefox (рис. 18).

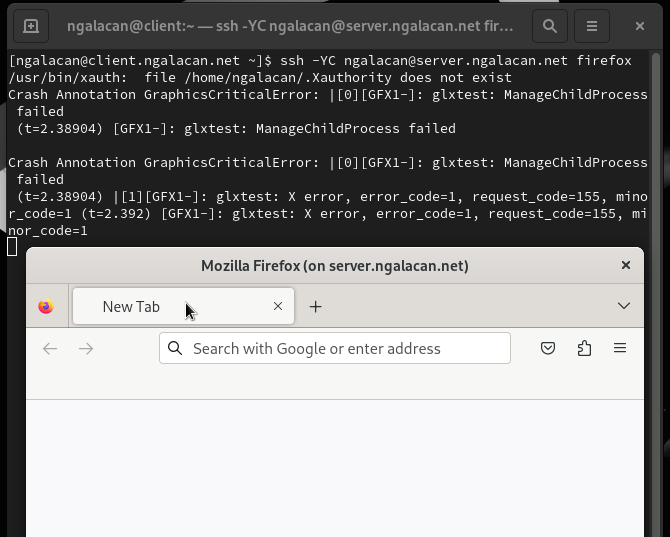


Рис. 18: Запуск firefox на сервере через клиент

## 2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую в соответствующие каталоги конфигурационные файлы:

cd /vagrant/provision/server  
mkdir -p /vagrant/provision/server/ssh/etc/ssh  
cp -R /etc/ssh/sshd\_config /vagrant/provision/server/ssh/etc/ssh/

Создаю файл /vagrant/provision/server/ssh.sh (рис. 19).

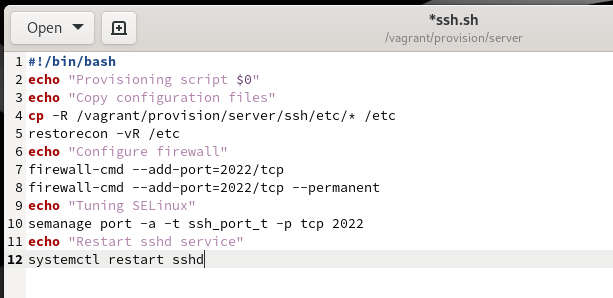


Рис. 19: Редактирование ssh.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавляю следующую запись:

server.vm.provision "server ssh",  
 type: "shell",  
 preserve\_order: true,  
 path: "provision/server/ssh.sh"

# 3 Выводы

В результате выполнения работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.

# 4 Ответы на контрольные вопросы

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

В файле /etc/ssh/sshd\_config конфигурации прописать PermitRootLogin no и AllowUsers alice.

1. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

Для настройки удалённого доступа по SSH через несколько портов нужно отредактировать файл конфигурации SSH и добавить строку Port <порт>.

1. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?

Для установки фонового соединения без команды используется параметр -N при использовании команды ssh: ssh -N <hostname>

1. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?

ssh -fNL 80:localhost:55555 server2.example.com

1. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?

semanage port -a -t ssh\_port\_t -p tcp 2022

1. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?

firewall-cmd --add-port=2022/tcp --permanent