Отчёт по лабораторной работе №11

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

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

Выполнен вход на сервер под пользователем с административными привилегиями и задан пароль для пользователя root с помощью команд sudo -i и passwd root. В процессе изменения пароля система выдала предупреждение о недостаточной длине пароля, после чего пароль был успешно обновлён ([рис. 1](#fig-1)).

|  |
| --- |
| Рисунок 1: Изменение пароля пользователя root с помощью passwd |

С клиента выполнена попытка подключения к серверу по SSH от имени пользователя root с помощью команды ssh root@server.alkamal.net. Аутентификация завершилась ошибкой Permission denied, что свидетельствует об отклонении доступа сервером ([рис. 2](#fig-2)).

|  |
| --- |
| Рисунок 2: Отказ в аутентификации при SSH-подключении пользователя root |

В конфигурационном файле /etc/ssh/sshd\_config на сервере установлен параметр PermitRootLogin no, запрещающий удалённый вход пользователя root по SSH ([рис. 3](#fig-3)).

|  |
| --- |
| Рисунок 3: Параметр PermitRootLogin no в файле sshd\_config |

После перезапуска службы sshd повторная попытка подключения с клиента под пользователем root завершилась сообщением Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password), что подтверждает успешный запрет удалённого доступа для root ([рис. 4](#fig-4)).

|  |
| --- |
| Рисунок 4: Повторная ошибка SSH-аутентификации после запрета входа root |

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

С клиента выполнено SSH-подключение к серверу под пользователем alkamal с помощью команды ssh alkamal@server.alkamal.net. Аутентификация прошла успешно, о чём свидетельствует вывод приглашения командной строки удалённой системы и информация о предыдущих входах ([рис. 5](#fig-5)).

|  |
| --- |
| Рисунок 5: Успешное SSH-подключение пользователя alkamal к серверу |

В конфигурационном файле /etc/ssh/sshd\_config добавлена строка AllowUsers vagrant, ограничивающая список пользователей, которым разрешён удалённый доступ по SSH ([рис. 6](#fig-6)).

|  |
| --- |
| Рисунок 6: Добавление директивы AllowUsers vagrant в sshd\_config |

После внесения изменений выполнен перезапуск службы sshd командой systemctl restart sshd для применения новой конфигурации ([рис. 7](#fig-7)).

|  |
| --- |
| Рисунок 7: Перезапуск службы sshd после изменения конфигурации |

Повторная попытка подключения с клиента под пользователем alkamal завершилась ошибкой Permission denied, что связано с отсутствием данного пользователя в списке, указанном в директиве AllowUsers ([рис. 8](#fig-8)).

|  |
| --- |
| Рисунок 8: Отказ в SSH-доступе пользователю alkamal после ограничения AllowUsers |

В файл /etc/ssh/sshd\_config внесено изменение: строка AllowUsers vagrant заменена на AllowUsers vagrant alkamal, что добавляет пользователя alkamal в разрешённый список ([рис. 9](#fig-9)).

|  |
| --- |
| Рисунок 9: Расширение списка AllowUsers: vagrant alkamal |

После повторного перезапуска службы sshd выполнена новая попытка подключения с клиента под пользователем alkamal, которая завершилась успешно, что подтверждается появлением приглашения командной строки сервера ([рис. 10](#fig-10)).

|  |
| --- |
| Рисунок 10: Успешное SSH-подключение после добавления пользователя в AllowUsers |

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

В конфигурационном файле /etc/ssh/sshd\_config добавлена дополнительная строка Port 2022 ниже существующей строки Port 22, что задаёт прослушивание двух TCP-портов процессом sshd ([рис. 11](#fig-11)).

|  |
| --- |
| Рисунок 11: Добавление порта 2022 в конфигурацию sshd |

После перезапуска службы выполнена проверка расширенного статуса systemctl status -l sshd. В журнале зафиксированы сообщения error: Bind to port 2022 ... failed: Permission denied, что указывает на запрет использования данного порта механизмом SELinux. При этом служба продолжила работу на порту 22 ([рис. 12](#fig-12)).

|  |
| --- |
| Рисунок 12: Ошибка привязки к порту 2022 в статусе sshd |

Для разрешения использования порта 2022 выполнено добавление соответствующей метки SELinux командой semanage port -a -t ssh\_port\_t -p tcp 2022, а также открыт порт в межсетевом экране с помощью firewall-cmd. После этого служба sshd перезапущена ([рис. 13](#fig-13)).

|  |
| --- |
| Рисунок 13: Настройка SELinux и firewall для порта 2022 |

Повторная проверка статуса службы показала, что sshd прослушивает порты 22 и 2022 на адресах 0.0.0.0 и ::, что подтверждает корректную настройку ([рис. 14](#fig-14)).

|  |
| --- |
| Рисунок 14: sshd прослушивает порты 22 и 2022 |

С клиента выполнено подключение к серверу с указанием альтернативного порта ssh -p2022 alkamal@server.alkamal.net. Аутентификация прошла успешно, после чего выполнен переход в режим суперпользователя sudo -i и корректный выход из сеанса ([рис. 15](#fig-15)).

|  |
| --- |
| Рисунок 15: Успешное SSH-подключение через порт 2022 |

## 2.4 Настройка удалённого доступа по SSH по ключу

В конфигурационном файле /etc/ssh/sshd\_config на сервере установлен параметр PubkeyAuthentication yes, разрешающий аутентификацию по открытому ключу ([рис. 16](#fig-16)).

|  |
| --- |
| Рисунок 16: Параметр PubkeyAuthentication yes в sshd\_config |

На клиенте под пользователем **alkamal** выполнена генерация пары RSA-ключей с помощью команды ssh-keygen. Закрытый ключ сохранён в файл ~/.ssh/id\_rsa, открытый — в ~/.ssh/id\_rsa.pub, что подтверждается выводом утилиты ([рис. 17](#fig-17)).

|  |
| --- |
| Рисунок 17: Генерация пары SSH-ключей командой ssh-keygen |

Открытый ключ скопирован на сервер командой ssh-copy-id alkamal@server.alkamal.net. После ввода пароля пользователя ключ добавлен в файл ~/.ssh/authorized\_keys на сервере ([рис. 18](#fig-18)).

|  |
| --- |
| Рисунок 18: Копирование открытого ключа на сервер с помощью ssh-copy-id |

Повторное подключение к серверу выполнено командой ssh alkamal@server.alkamal.net. Аутентификация прошла без запроса пароля, что подтверждается непосредственным входом в оболочку удалённой системы ([рис. 19](#fig-19)).

|  |
| --- |
| Рисунок 19: Успешная SSH-аутентификация по ключу без ввода пароля |

## 2.5 Организация туннелей SSH, перенаправление TCP-портов

На клиенте выполнена проверка активных TCP-соединений командой lsof | grep TCP. До организации туннеля отсутствовали локальные прослушивающие сокеты на порту 8080 ([рис. 21](#fig-20)).

|  |
| --- |
| Рисунок 20: Проверка активных TCP-соединений до создания SSH-туннеля |

Выполнена команда ssh -fNL 8080:localhost:80 alkamal@server.alkamal.net, создающая локальный SSH-туннель. Параметр -L 8080:localhost:80 организует перенаправление: локальный порт 8080 клиента связывается с портом 80 сервера через защищённое SSH-соединение. Повторный вывод lsof | grep TCP показывает процесс ssh, прослушивающий порт localhost:8080 (webcache), а также установленное SSH-соединение в состоянии ESTABLISHED, что подтверждает успешное создание туннеля ([рис. 21](#fig-20)).

|  |
| --- |
| Рисунок 21: Прослушивание локального порта 8080 процессом ssh |

На клиенте в браузере открыт адрес http://localhost:8080. Отображается страница приветствия «Welcome to the server.alkamal.net server», что подтверждает корректное перенаправление HTTP-трафика через SSH-туннель на веб-сервер, работающий на сервере ([рис. 22](#fig-21)).

|  |
| --- |
| Рисунок 22: Доступ к веб-серверу через SSH-туннель на localhost:8080 |

## 2.6 Запуск консольных приложений через SSH

С клиента под пользователем **alkamal** выполнена команда ssh alkamal@server.alkamal.net hostname, которая запускает на удалённом сервере консольную утилиту hostname. В ответ получено имя узла server.alkamal.net, что подтверждает удалённое выполнение команды через SSH ([рис. 23](#fig-22)).

|  |
| --- |
| Рисунок 23: Удалённое выполнение команды hostname через SSH |

Командой ssh alkamal@server.alkamal.net ls -Al получен подробный список файлов домашнего каталога пользователя на сервере. Вывод содержит права доступа, владельца, размер и дату изменения файлов, что подтверждает корректное удалённое выполнение команды ls ([рис. 24](#fig-23)).

|  |
| --- |
| Рисунок 24: Удалённый вывод списка файлов командой ls -Al |

Командой ssh alkamal@server.alkamal.net MAIL=~/Maildir/ mail выполнен запуск почтового клиента mail на сервере с указанием каталога Maildir. В выводе отображены 4 почтовых сообщения с указанием отправителя, даты и темы, что подтверждает успешный запуск консольного приложения на удалённой системе ([рис. 25](#fig-24)).

|  |
| --- |
| Рисунок 25: Удалённый просмотр почты через консольное приложение mail |

## 2.7 Запуск графических приложений через SSH (X11Forwarding)

В конфигурационном файле /etc/ssh/sshd\_config на сервере установлен параметр X11Forwarding yes, разрешающий пересылку графического трафика X11 через SSH-соединение ([рис. 26](#fig-25)).

|  |
| --- |
| Рисунок 26: Параметр X11Forwarding yes в sshd\_config |

С клиента выполнено подключение с поддержкой X11-перенаправления командой ssh -YC alkamal@server.alkamal.net firefox. Параметр -Y включает доверенное X11-перенаправление, -C активирует сжатие трафика. В результате графическое приложение Firefox, запущенное на сервере, отобразилось на клиентской машине, что подтверждает корректную работу X11Forwarding ([рис. 27](#fig-26)).

|  |
| --- |
| Рисунок 27: Запуск Firefox на сервере с отображением на клиенте через SSH X11Forwarding |

## 2.8 Внесение изменений в настройки внутреннего

На виртуальной машине **server** выполнен переход в каталог /vagrant/provision/server, создан каталог ssh/etc/ssh и в него скопирован конфигурационный файл sshd\_config, что обеспечивает сохранение настроек SSH во внутреннем окружении Vagrant ([рис. 28](#fig-27)).

|  |
| --- |
| Рисунок 28: Копирование файла sshd\_config в каталог provision/server/ssh |

В каталоге /vagrant/provision/server создан исполняемый файл ssh.sh, в котором реализован сценарий автоматической настройки: копирование конфигурационных файлов в /etc, восстановление контекстов SELinux (restorecon), открытие порта 2022 в firewalld, добавление порта 2022 в тип ssh\_port\_t с помощью semanage, а также перезапуск службы sshd ([рис. 29](#fig-28)).

|  |
| --- |
| Рисунок 29: Содержимое скрипта ssh.sh для автоматической настройки SSH |

В файле Vagrantfile в разделе конфигурации виртуальной машины **server** добавлен provision-блок типа shell с указанием пути provision/server/ssh.sh и параметром preserve\_order: true, что обеспечивает автоматическое выполнение созданного скрипта при загрузке виртуальной машины ([рис. 30](#fig-29)).

|  |
| --- |
| Рисунок 30: Добавление provision-блока для ssh.sh в Vagrantfile |

# 3. Выводы

В ходе работы выполнена комплексная настройка службы OpenSSH на виртуальной машине server. Реализованы меры повышения безопасности: запрещён удалённый вход пользователя root, ограничен список пользователей с помощью директивы AllowUsers, настроена аутентификация по ключу вместо пароля, а также организован доступ через альтернативный порт 2022 с корректной настройкой SELinux и межсетевого экрана.

Дополнительно реализованы механизмы SSH-туннелирования и X11-перенаправления, что позволило безопасно передавать TCP-трафик и запускать графические приложения удалённо. Проверена возможность выполнения консольных команд на сервере без интерактивного входа в систему.

Изменения интегрированы во внутреннее окружение виртуальной машины посредством provisioning-скрипта Vagrant, что обеспечивает автоматическое применение конфигурации и воспроизводимость настроенной среды.

# 4. 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