**Липецкий государственный технический университет**

Факультет автоматизации и информатики

Кафедра Автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №7

по курсу "Операционная система Linux"

авторизация по ключу ssh

Поленников А.А.

|  |  |  |
| --- | --- | --- |
| Студент |  |  |
| Группа АИ-17 | Кургасов В.В. |  |
| Руководитель  Доцент |  |  |

Липецк 2019г.

Ход работы

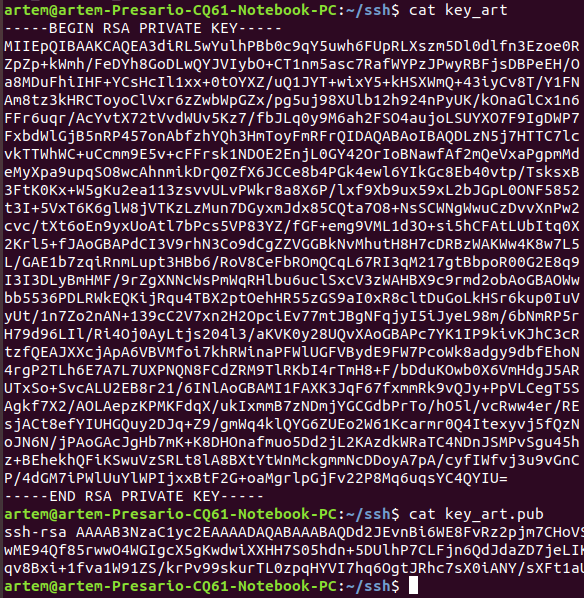


Рисунок 1 – сгенерированные ключи командой ssh -keygen

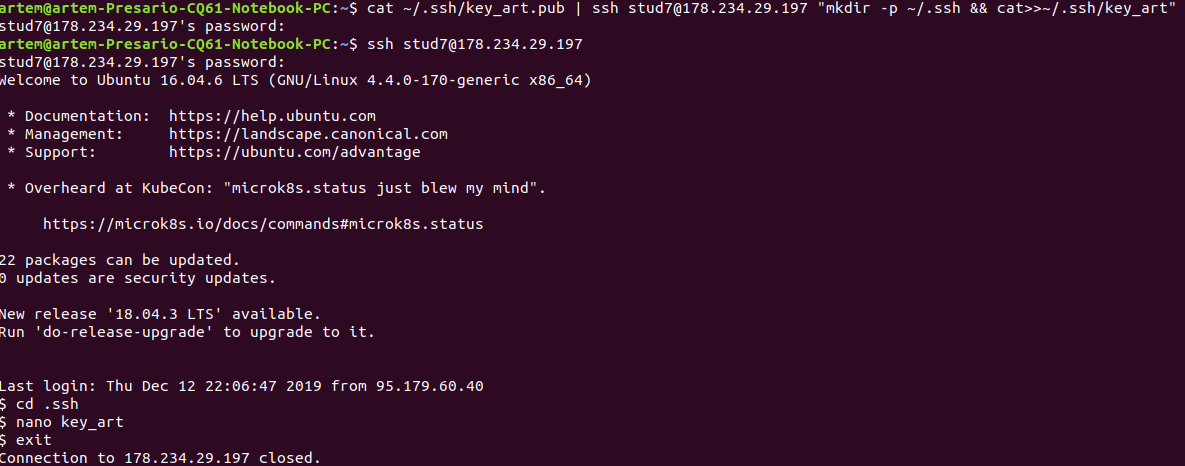


Рисунок 2 – копирование открытого ключа на сервер

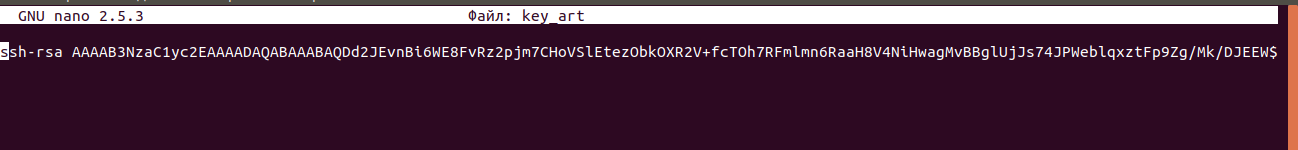


Рисунок 3 – просмотр файла открытого ключа на сервере

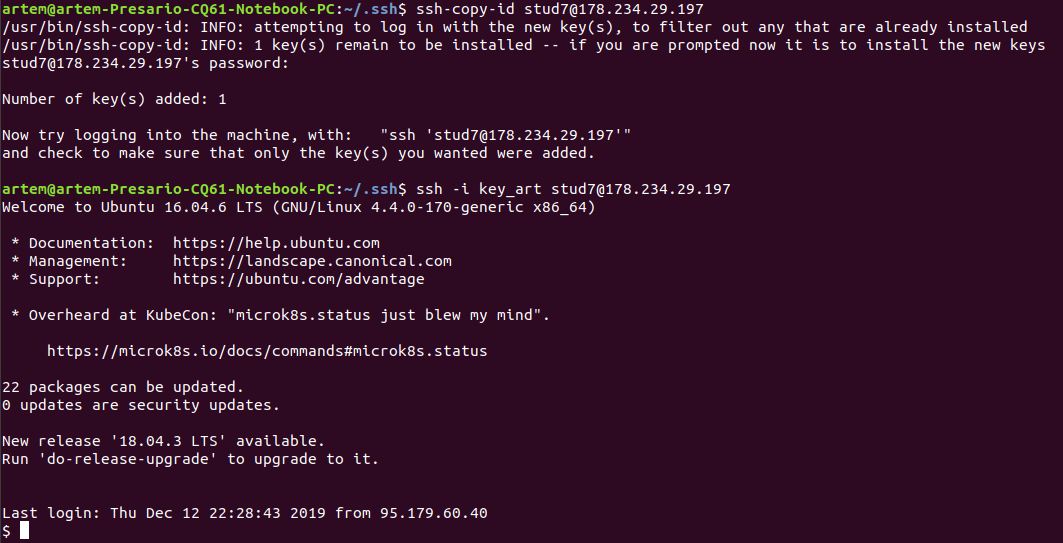


Рисунок 4 – копирование ключа на удаленный сервер с использованием утилиты ssh-copy-id

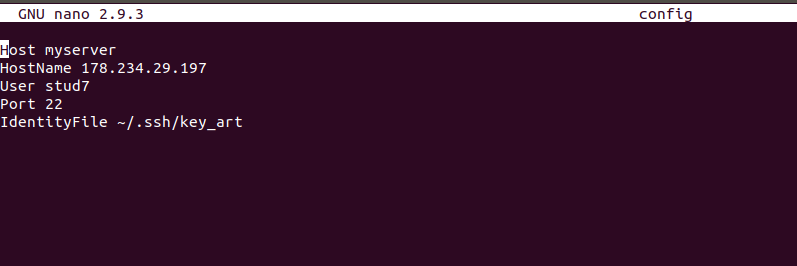


Рисунок 5 – создание файла конфигураций в случае удобного подключения к разным серверам

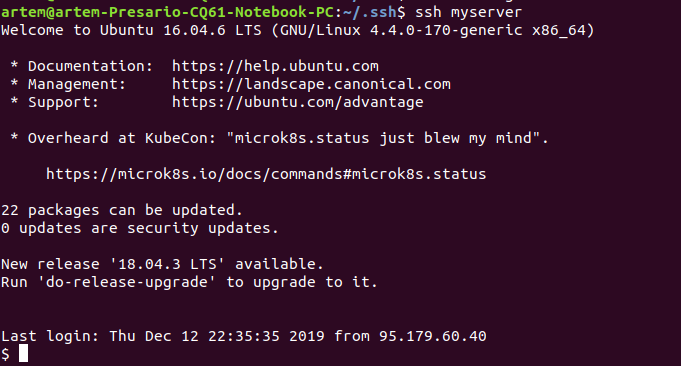


Рисунок 6 – доступ к серверу

Вывод

В данной работе был осуществлен доступ на сервер с помощью SSH - это зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами. Доступ был осуществлен при помощи помещенного на сервер ключа доступа, следовательно пароль не был использован.

Контрольные вопросы:

1. Что такое ключ ssh? В чем преимущество их использования?

SSH - это зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами.

Аутентификация по ключу SSH более надежна чем по паролю.

Каждая пара ключей состоит из открытого и закрытого ключа. Ключ сохраняется на стороне клиента и не должен быть доступен кому-либо еще. Утечка ключа позволит злоумышленнику войти на сервер, если не была настроена дополнительная аутентификация по паролю.

Открытый ключ используется для шифрования сообщений, которые можно расшифровать только закрытым ключом. Это свойство и используется для аутентификации с помощью пары ключей.

1. Как сгенерировать ключи ssh в разных ОС?

С помощью утилиты ssh-keygen в зависимости от ОС

1. Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Нет не возможно

1. Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями (наличие/отсутствие пароля на «секретный» ключ и т.п.)

Да созданные пары ключей будут различаться

1. Перечислите доступные ключи для ssh-keygen.exe

   RSA, DSA, EDSA, ED25519

1. Можно ли использовать один «секретный» ключ доступа с разных ОС, установленных на одном ПК/на разных ПК?

Да возможно в обоих случаях

7. Возможно ли организовать подключение «по ключу» ssh к системе c ОС Windows, в которой запущен OpenSSH сервер?

Да возможно

8. Какие известные Вам сервисы сети Интернет позволяют организовать доступ к ресурсам посредством SSH ключей?

[Www.kurgasov.ru](http://Www.kurgasov.ru/), github.com