**Липецкий государственный технический университет**

Факультет автоматизации и информатики

Кафедра Автоматизированных систем управления

Отчет по лабораторной работе № 7

«Работа с SSH»

по курсу «ОС Linux»

Грунау Г. Ю.

Студент

Группа АИ-18

Кургасов В. В.

Руководитель

Липецк 2021 г.

# Цель работы

Лабораторная работа предназначена для целей практического ознакомления с программным обеспечением удаленного доступа к распределённым системам обработки данных.

# Выполнение работы

Запустим терминальный мультиплексор tmux и создадим новое окно, в котором запустим анализатор трафика tcpdump с фильтром пакетов получаемых и передаваемых от узла domen.name с TCP-портом источника и назначения 23. С помощью команды tee, вывести отфильтрованные IP-пакеты на терминал и сохранить данные в файл telnet.log, в домашнем каталоге пользователя. Для этого следует воспользоваться командой

**sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log**

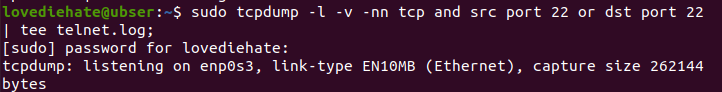


Рисунок – Анализатор трафика telnet

Установим соединение с удаленным сервером по протоколу TELNET.

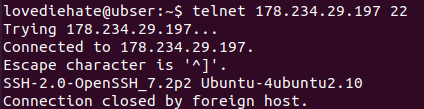


Рисунок – Попытка соединения

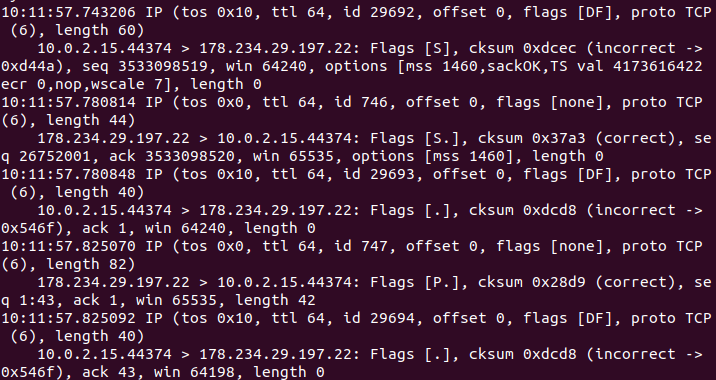


Рисунок – Логи подключения

Как мы видим на рисунке 2 соединение было установлено, однако сервер не предлагает нам пройти авторизацию. А также на рисунке 3 в окне с анализатором трафика можно понять по отфильтрованным ip-пакетам, что подключение было успешным.

Теперь запустим анализатор трафика по порту 22, но с файлом ssh.log

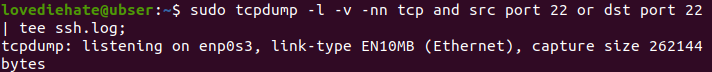


Рисунок – Анализатор трафика ssh

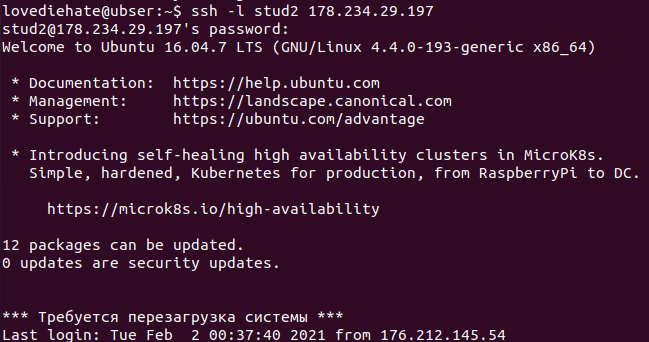


Рисунок – Подключение к удалённому узлу по SSH

В окне с анализатором трафика можно увидеть логи успешного подключения с отфильтрованными по 22 порту ip-пакетами.

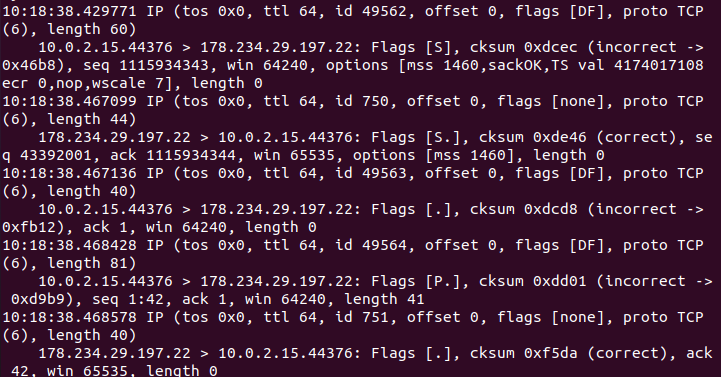


Рисунок – Логи из ssh.log

Выполнив команду uname –a в удаленном узле, можно получить информацию о нём:



Рисунок – Информация об удалённой системе

Теперь откроем новое окно для того, чтобы создать файл c содержанием требуемой информации в нашей локальной системе.



Рисунок – Текстовый файл

С помощью команды scp filename login@domenname:/home/stud2 передадим наш файл по шифрованному каналу.



Рисунок – Передача файла

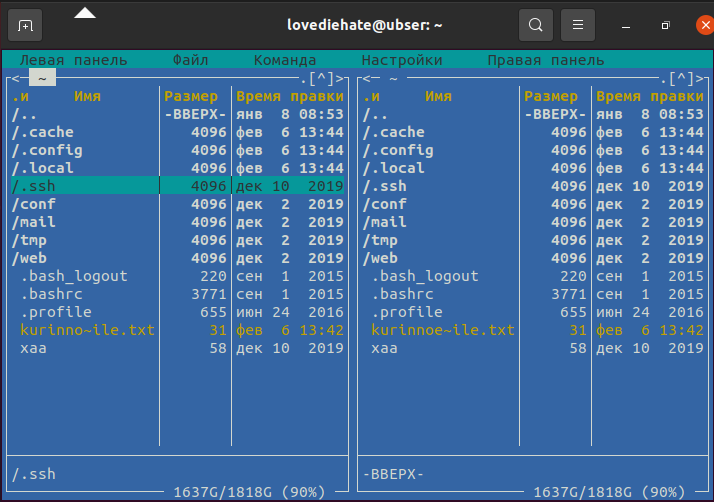
С помощью команды mc на удаленном узле можно проверить файл.

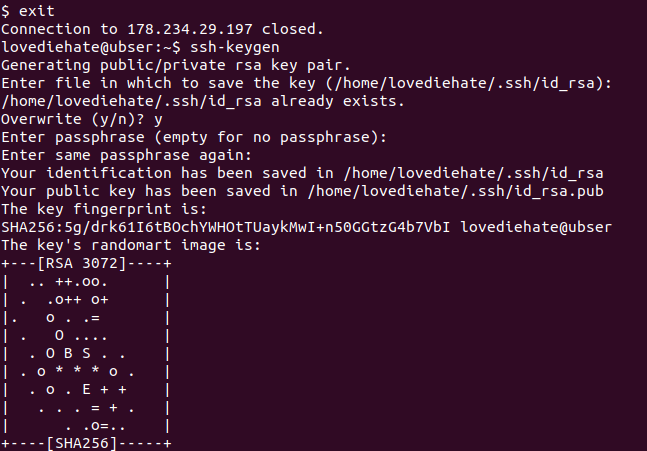
Рисунок – Переданный файл на удаленном узле

Рисунок – Генерация ключа

На рисунке 11 изображена генерация публичного и приватного ключей SSH.

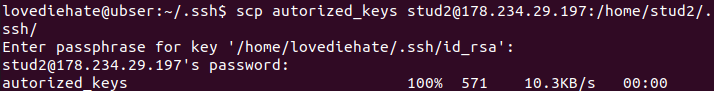
С помощью команды scp передадим сгенерированный публичный ключ на локальный узел, предварительно переименовав его в authorized\_keys

Рисунок – Передача ключей

Снова сделаем попытку подключения к удаленному узлу:

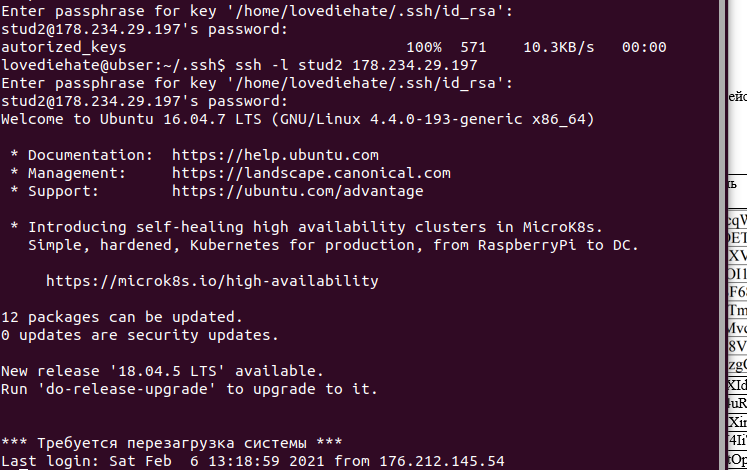


Рисунок – Подключение к удаленной системе

Теперь система помимо пароля запросила у меня кодовое слово для приватного ключа, которое я вводил при генерации шифров.

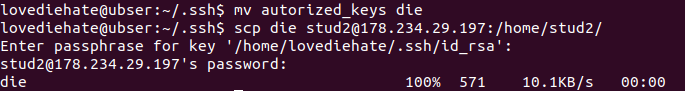
Попробуем ещё раз передать файл с локальной системы, переименовав его:

Рисунок – Передача файла

Система запросила у меня кодовое слово, которое я указал при генерации.

Проверим наличие файла, авторизовавшись в системе и выполнив команду **mc**.

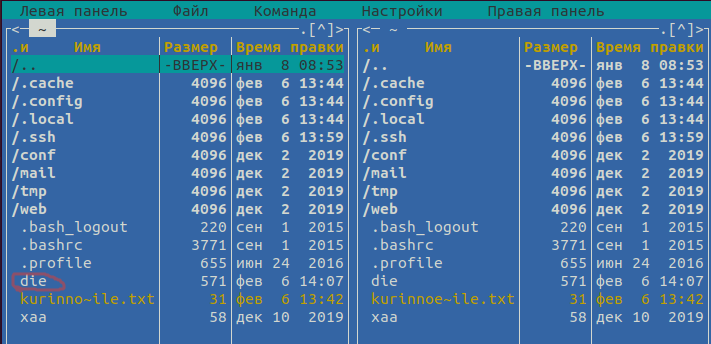


Рисунок – Наличие файла в удаленной системе

Теперь приостановим работу анализатора трафика с помощью комбинации ctrl+c:



Рисунок – Завершение процесса