Липецкий государственный технический университет

Факультет автоматизации и информатики

Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №6

по Операционной системе Linux

Работа с SSH

Студент Жидков И.А.

Группа АС-19

Руководитель Кургасов В.В.

Доцент, к.п.н.

Липецк 2022 г.

Оглавление

Цель работы

Ознакомиться с программным обеспечением удаленного доступа к распределенным системам обработки данных.

Ход работы

Для начала запустим анализатор трафика.

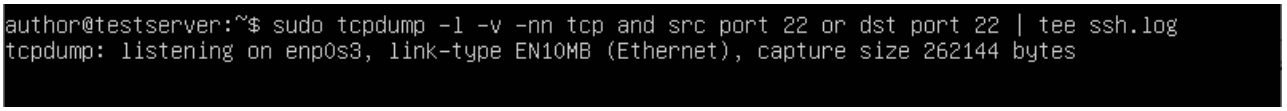

Рисунок 1 - Запуск анализатора трафика

Далее установим зашифрованное соединение.

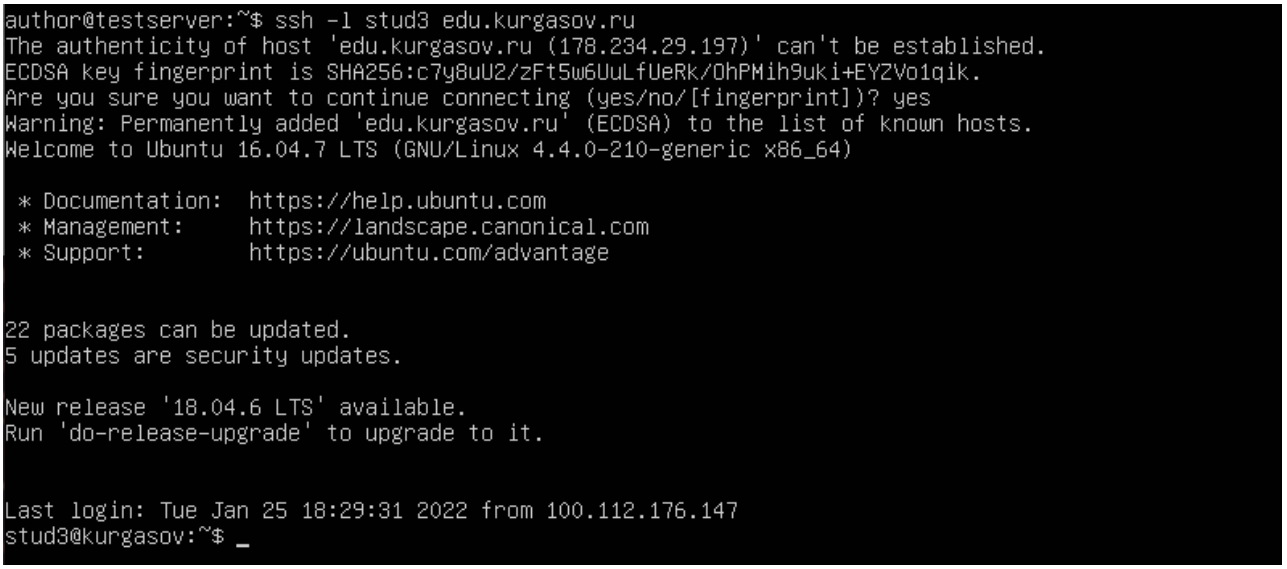

Рисунок 2 - установка соединения

Выведем информацию о системе.

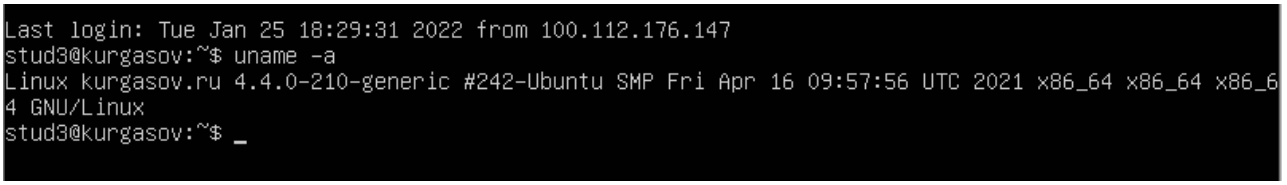

Рисунок 3 - информация о системе

Далее создадим файл lr7.txt и заполним данными.

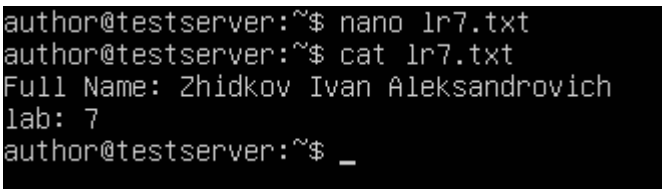

Рисунок 4 - содержание файла

При помощи команды scp ~/lr7.txt stud3edu.kurgasov.ru:/home/stud3 передадим файл на сервер.

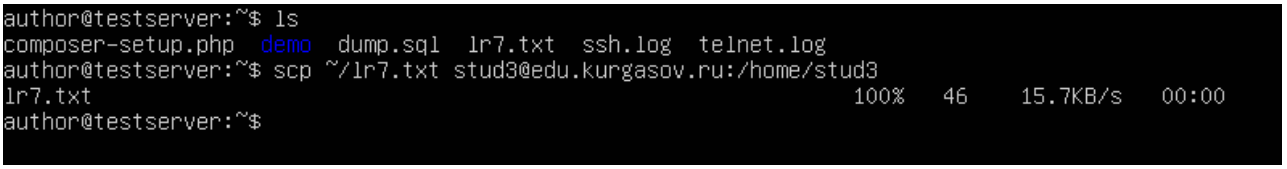

Рисунок 5 - передача файла

Теперь генерируем ssh-ключ

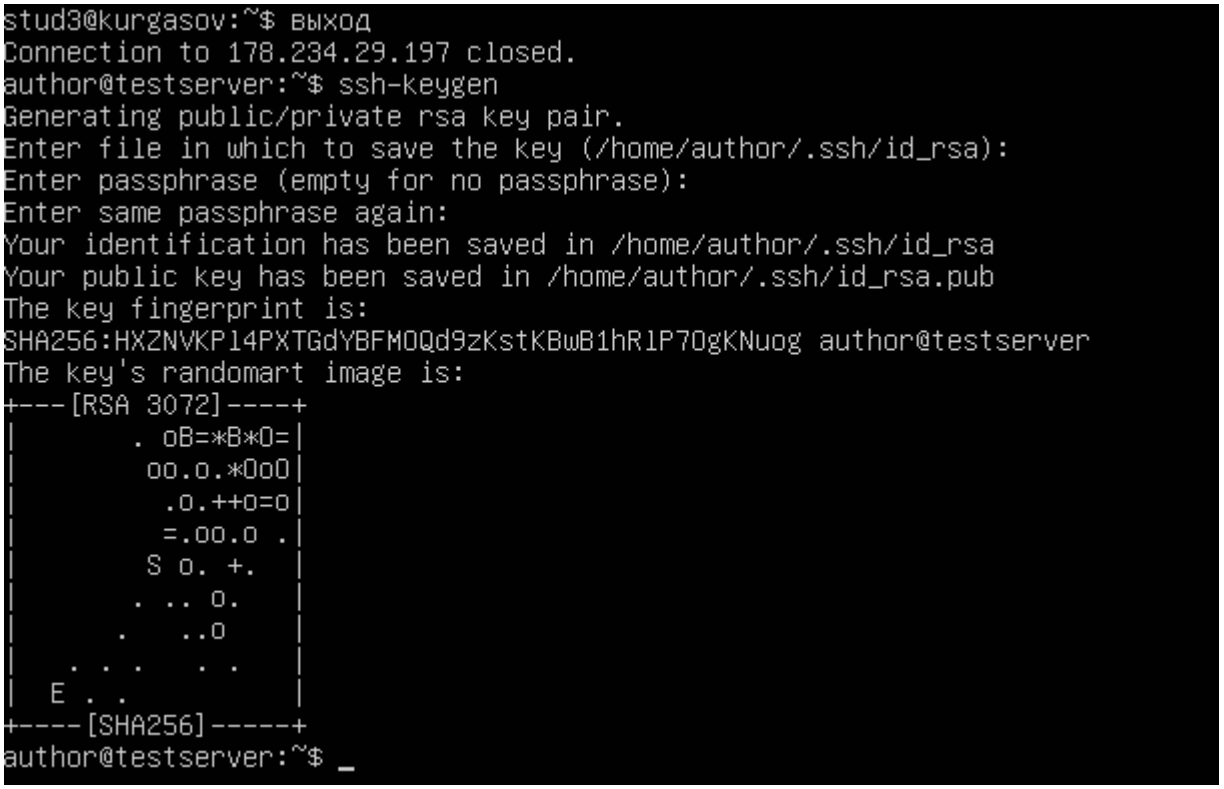

Рисунок 6 - генерация ключа

После этого мы должны передать публичный ключ на сервер с помощью команды ssh-copy-id с использованием опции –i, которая позволяет передать в качестве операнда расположение файла, хранящего публичный ключ:

Рисунок 7 - передача ключа

И теперь пробуем подключиться к серверу без использования пароля:

```
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'stud3@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

author@testserver:~$ ssh stud3@178.234.29.197
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Jan 25 18:11:44 2022 from 100.112.176.147
stud3@kurgasov:~$
```

Рисунок 8 - подключение без пароля

Проверим логи tcpdump

```
n 63440, length 0
17:04:34.577959 IP (tos 0x0, ttl 64, id 196, offset 0, flags [none], proto TCP (6), length 216)
    178.234.29.197.22 > 10.0.2.15.36556: Flags [P.], cksum 0x0ee5 (correct), seq 4335:4511, ack 4206
, win 65535, length 176
17:04:34.577966 IP (tos 0x10, ttl 64, id 60484, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.36556 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x5d15), ack 4511, wi
n 63440, length 0
17:04:34.578028 IP (tos 0x10, ttl 64, id 60485, offset 0, flags [DF], proto TCP (6), length 76)
    10.0.2.15.36556 > 178.234.29.197.22: Flags [P.], cksum 0xdcfc (incorrect -> 0x781e), seq 4206:42
42, ack 4511, win 63440, length 36
17:04:34.578066 IP (tos 0x10, ttl 64, id 60486, offset 0, flags [DF], proto TCP (6), length 100)
    10.0.2.15.36556 > 178.234.29.197.22: Flags [P.], cksum 0xdd14 (incorrect -> 0xad77), seq 4242:43
02, ack 4511, win 63440, length 60
17:04:34.578109 IP (tos 0x0, ttl 64, id 197, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.36556: Flags [.], cksum 0x54c2 (correct), ack 4242, win 65535, len
gth 0
17:04:34.578129 IP (tos 0x10, ttl 64, id 60487, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.36556 > 178.234.29.197.22: Flags [F.], cksum 0xdcd8 (incorrect -> 0x5cb4), seq 4302, a
ck 4511, win 63440, length 0
17:04:34.578167 IP (tos 0x0, ttl 64, id 198, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.36556: Flags [.], cksum 0x5486 (correct), ack 4302, win 65535, len
gth 0
17:04:34.578197 IP (tos 0x0, ttl 64, id 199, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.36556: Flags [.], cksum 0x5485 (correct), ack 4303, win 65535, len
gth 0
17:04:34.583951 IP (tos 0x0, ttl 64, id 200, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.36556: Flags [F.], cksum 0x5484 (correct), seq 4511, ack 4303, win
 65535, length 0
17:04:34.583966 IP (tos 0x10, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.36556 > 178.234.29.197.22: Flags [.], cksum 0x5cb3 (correct), ack 4512, win 63440, len
gth 0
^C282 packets captured
282 packets received by filter
0 packets dropped by kernel

author@testserver:~$
[0] 0:bash- 1:bash*                                          "testserver" 17:05 25-Jan-22
```

Рисунок 9 - логи

Вывод

В результате выполнения лабораторной работы я получил знания по программному обеспечению удаленного доступа к распределенным системам обработки данных. Научился устанавливать шифрованное соединение с удаленным сервером, передавать файлы по шифрованному каналу на удаленную систему. Также понял, как передавать публичный ключ по шифрованному туннелю на удаленный узел и подключаться к удаленной системе без использования пароля.

1. Определите основные цели и задачи решаемые с помощью ПО удаленного доступа?

ПО удаленного доступа дает пользователю возможность подключаться к компьютеру с помощью другого устройства через интернет. Для создания удаленного подключения используют специальные программы. Обязательное условие — наличие постоянного доступа в интернет, компьютеров, обладающих определенными характеристиками и сервера. Такое ПО делает возможным подключение к другому компьютеру из любой точки мира. Программы позволяют видеть рабочий стол и выполнять все действия на удаленном устройстве, изменять настройки ПО, обмениваться файлами, шифровать передаваемые данные, проводить конференции, подключать веб-камеры, удаленные проекторы и прочие сетевые устройства.

2. Выделите отличительные особенности между режимами работы удаленного доступа по протоколам TELNET и SSH?

• Доступ к командной строке удаленного хоста одинаков для обоих протоколов, но основное различие этих протоколов зависит от меры безопасности каждого из них. SSH более защищен, чем TELNET.

• По умолчанию SSH использует порт 22, а TELNET использует порт 23 для связи, и оба используют стандарт TCP.

• SSH отправляет все данные в зашифрованном формате, а TELNET отправляет данные в виде обычного текста. Поэтому SSH использует безопасный канал для передачи данных по сети, а TELNET использует обычный способ подключения к сети и связи.

• SSH использует шифрование с открытым ключом для аутентификации удаленных пользователей, а TELNET не использует механизмов аутентификации. 19

• SSH больше подходит для использования в общедоступных сетях, а TELNET больше подходит для частных сетей.

3. Опишите способы установления соединения при использовании протокола SSH? Охарактеризуйте положительные и отрицательные аспекты приведенных методов.

22 порт, авторизация по паролю, без защиты
Вероятность взлома: **высокая**
Потери от флуда: **высокие**

22 порт, авторизация по ключам, без защиты
Вероятность взлома: **средняя**
Потери от флуда: **высокие**

22 порт, авторизация по ключам, защита на основе ограничения неудачных попыток авторизации
Вероятность взлома: **низкая**
Потери от флуда: **средние**

Нестандартный порт, авторизация по паролю, без защиты
Вероятность взлома: **высокая**
Потери от флуда: **низкие**

Нестандартный порт, авторизация по ключам, без защиты
Вероятность взлома: **средняя**
Потери от флуда: **низкие**

Нестандартный порт, авторизация по ключам, защита на основе ограничения неудачных попыток авторизации
Вероятность взлома: **низкая**
Потери от флуда: **низкие**

4. Основываясь на заданиях лабораторной работы, приведите практический пример использования систем удаленного доступа?

Системы удаленного доступа нужны тем компаниям, где большинство сотрудников находится за пределами офиса, на частичном фрилансе, аутсорсинге или в командировках, но при этом они нуждаются в обновлении рабочей информации, просмотре корпоративной почты и др. Им не нужно будет скачивать все необходимые для работы данные на внешний носитель или отправлять их по почте – достаточно связаться с офисным компьютером. Удаленный доступ используют системные администраторы для управления системой и устранения сбоев в ее работе, и руководители, желающие проконтролировать процесс выполнения задачи своими подчиненными.

5. Перечислите распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH? Приведите пример использования службы передачи файлов по безопасному туннелю?

Распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH: OpenSSH, PuTTY/KiTTY, SecureCRT, Xshell. Службы передачи файлов по безопасному туннелю можно использовать для передачи паролей.