

# Липецкий государственный технический университет

Кафедра прикладной математики

Отчет по лабораторной работе № 7  
«Авторизация по ключу ssh»  
по курсу «Операционная система Linux»

Студент

\_\_\_\_\_  
подпись, дата

Киренский Д.К.

Группа

Руководитель

Доцент, к. пед. наук

\_\_\_\_\_  
подпись, дата

Кургасов В.В.

Липецк 2022 г.

# Содержание

<b>Цель работы</b>	<b>3</b>
<b>1. Ход работы</b>	<b>4</b>
1.1. Запуск анализатора трафика tcpdump (порт 23)	4
1.2. Попытка установки соединения (порт 23)	5
1.3. Запуск анализатора трафика tcpdump (порт 22)	6
1.4. Попытка установки соединения (порт 22)	7
1.5. Установление шифрованного соединения с удаленным сервером	8
1.6. Вывод информации об удаленной системе	9
1.7. Передача файла по шифрованному каналу	10
1.8. Формирование зашифрованных ключей	12
1.9. Передача публичного ключа	13
1.10. Подключение к удаленной системе	14
1.11. Передача файла по шифрованному каналу	15
1.12. Содержимое файла telnet.log	16
1.13. Содержимое файла ssh.log	17
<b>Выводы</b>	<b>18</b>
<b>Контрольные вопросы</b>	<b>19</b>

## Цель работы

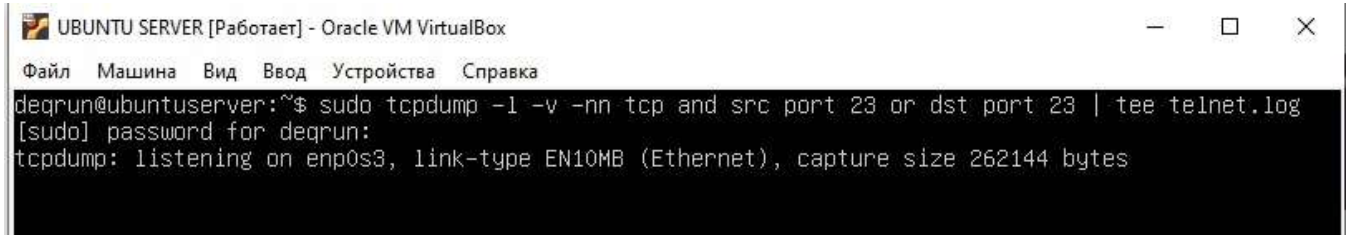
Организовать доступ к удаленному серверу по ssh (без ввода пароля (по ключу)) имея следующие исходные данные:

- IP: 178.234.29.197
- Порт: 22
- Логин: stud5
- Пароль: ZH6BuESF68

## 1. Ход работы

### 1.1. Запуск анализатора трафика tcpdump (порт 23)

Запустим tmux, откроем в нем новое окно и введем команду для анализа трафика 23 порта tcpdump.

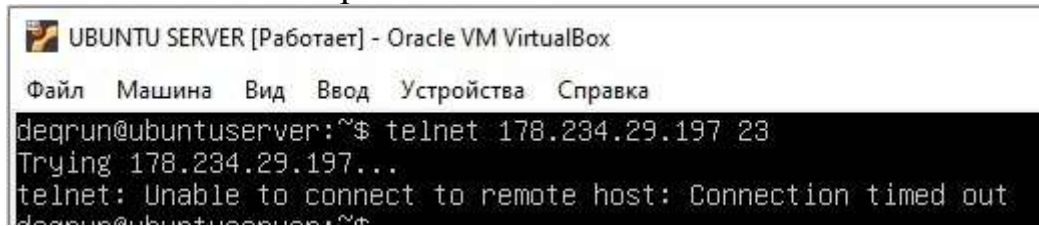
A screenshot of a terminal window titled "UBUNTU SERVER [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The terminal shows the user "degrun@ubuntuserver" at the prompt "~\$". They enter the command "sudo tcpdump -i -v -nn tcp and src port 23 or dst port 23 | tee telnet.log". The terminal prompts for a password "[sudo] password for degrun:". After the password is entered, the output is "tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes".

```
degrun@ubuntuserver:~$ sudo tcpdump -i -v -nn tcp and src port 23 or dst port 23 | tee telnet.log
[sudo] password for degrun:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Рисунок 1 – Запуск анализатора трафика tcpdump.

## 1.2. Попытка установки соединения (порт 23)

Перейдем к начальному окну и проверим соединение с 178.234.29.197 с 23 портом.



```
UBUNTU SERVER [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
degrun@ubuntu-server:~$ telnet 178.234.29.197 23
Trying 178.234.29.197...
telnet: Unable to connect to remote host: Connection timed out
degrun@ubuntu-server:~$
```

Рисунок 2 – Попытка установки соединения.

23 порт недоступен, нет возможности подключиться к серверу удалённо.

### 1.3. Запуск анализатора трафика tcpdump (порт 22)

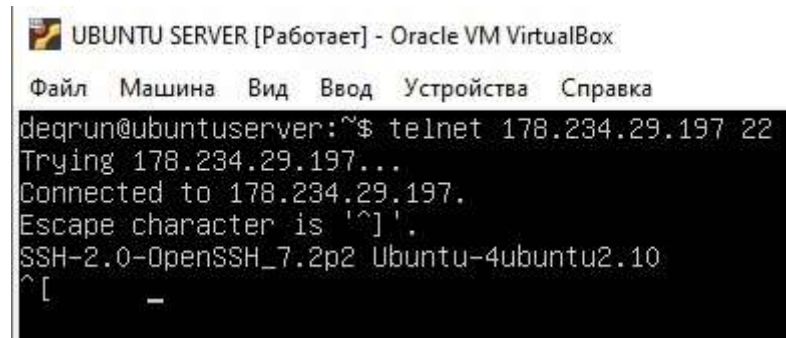
Запустим tmux, откроем в нем новое окно и введем команду для анализа трафика 22 порта tcpdump. Данные о трафике будем записывать в файл ssh.log

```
deqrun@ubuntu-server:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Рисунок 3 – Запуск анализатора трафика tcpdump.

#### 1.4. Попытка установки соединения (порт 22)

Перейдем к начальному окну и проверим соединение с 178.234.29.197 с 22 портом.



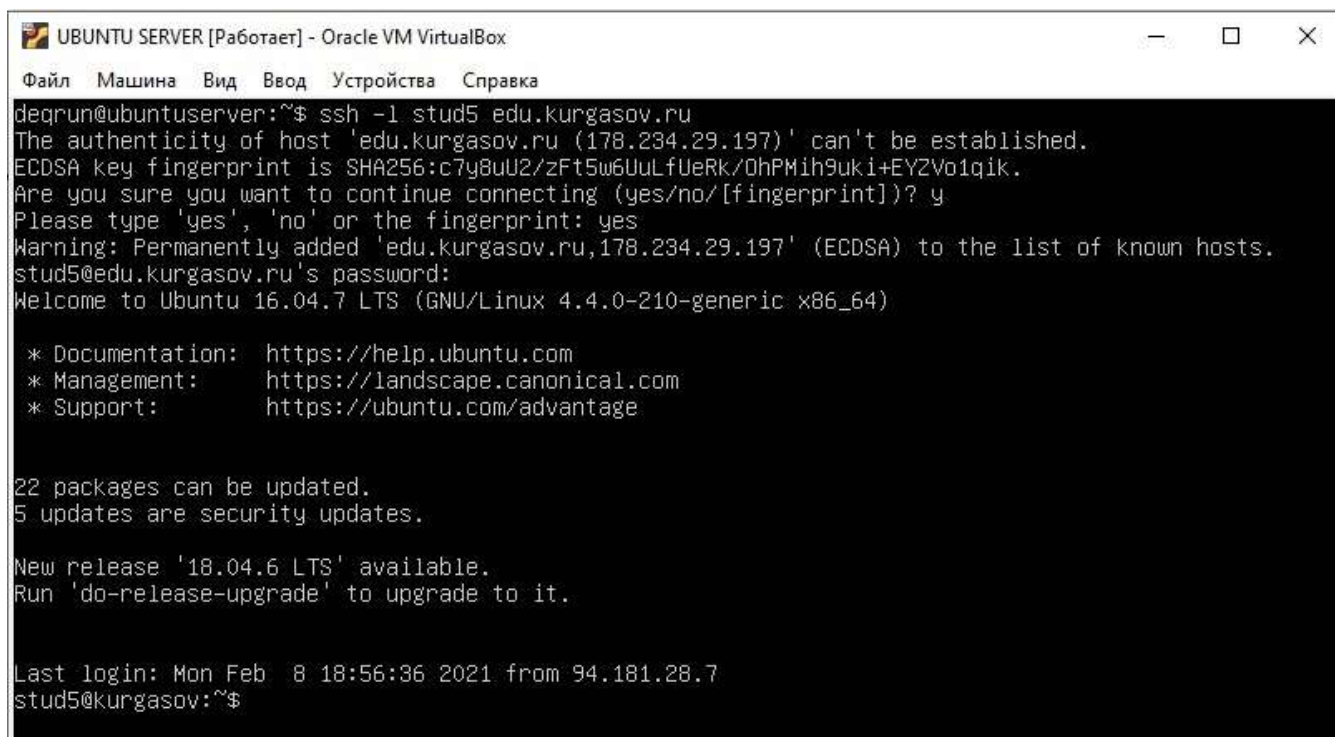
```
UBUNTU SERVER [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
degrun@ubuntuserver:~$ telnet 178.234.29.197 22
Trying 178.234.29.197...
Connected to 178.234.29.197.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
^[ _
```

Рисунок 4 – Попытка установки соединения.

22 порт доступен, соединение выполнено успешно.

## 1.5. Установление шифрованного соединения с удаленным сервером

Выполним команду `ssh -l stud5 edu.kurgasov.ru`.



```
UBUNTU SERVER [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
degrun@ubuntuserver:~$ ssh -l stud5 edu.kurgasov.ru
The authenticity of host 'edu.kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/0hPMih9uki+EY2Vo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'edu.kurgasov.ru,178.234.29.197' (ECDSA) to the list of known hosts.
stud5@edu.kurgasov.ru's password:
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.

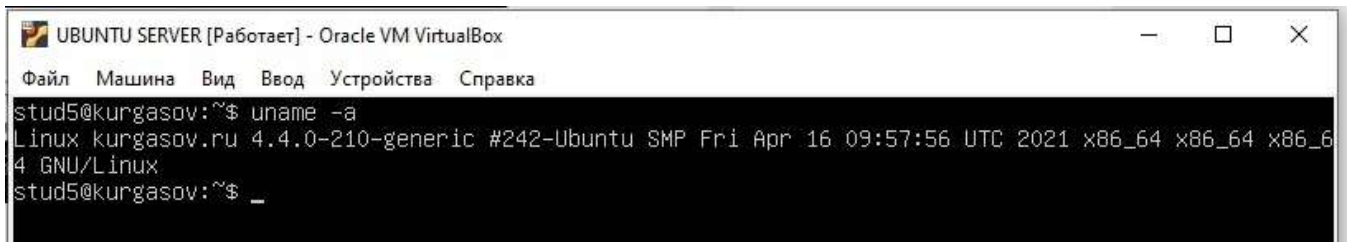
Last login: Mon Feb  8 18:56:36 2021 from 94.181.28.7
stud5@kurgasov:~$
```

Рисунок 5 – Установление шифрованного соединения.



## 1.6. Вывод информации об удаленной системе

Выведем информацию о системе с помощью команды `uname -a`.



```
UBUNTU SERVER [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
stud5@kurgasov:~$ uname -a
Linux kurgasov.ru 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
stud5@kurgasov:~$ _
```

Рисунок 6 – Вывод информации об удаленной системе.

## 1.7. Передача файла по зашифрованному каналу

Создадим на нашей виртуальной машине текстовый файл и перенесем его на сервер с помощью команды `scp`.

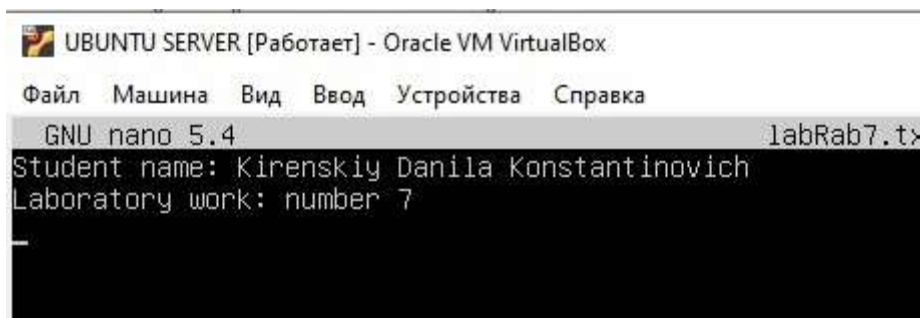


Рисунок 7 – Содержимое файла labRab7.txt.

```
deqrun@ubuntuserver:~$ nano labRab7.txt
deqrun@ubuntuserver:~$ ls
command_six.txt  directory_example  script      script13  script19  script24  snap
composer.json    installer          script10.1  script15  script20  script25  telnet.log
composer.lock    labRab7.txt        script10.2  script16  script20_new  script8  text.txt
demo             my.gz             script11    script17  script21  script_8  vendor
directory20      my.tar            script12    script18  script22  script_9
deqrun@ubuntuserver:~$ scp labRab7.txt stud5@edu.kurgasov.ru:/home/stud5
stud5@edu.kurgasov.ru's password:
labRab7.txt                                     100% 73  19.3KB/s  00:00
deqrun@ubuntuserver:~$ _
```

Рисунок 8 – Передача файла по зашифрованному каналу.

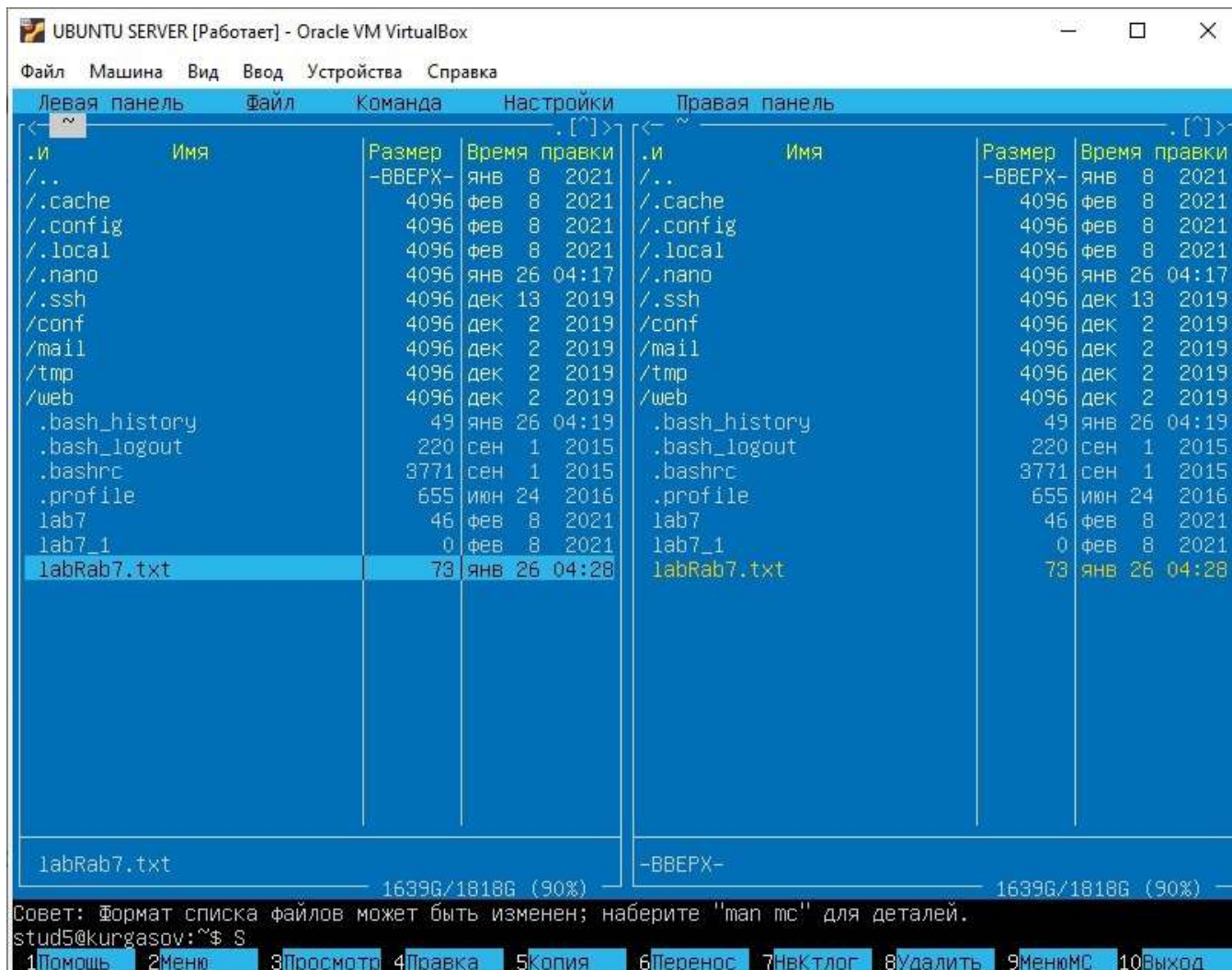
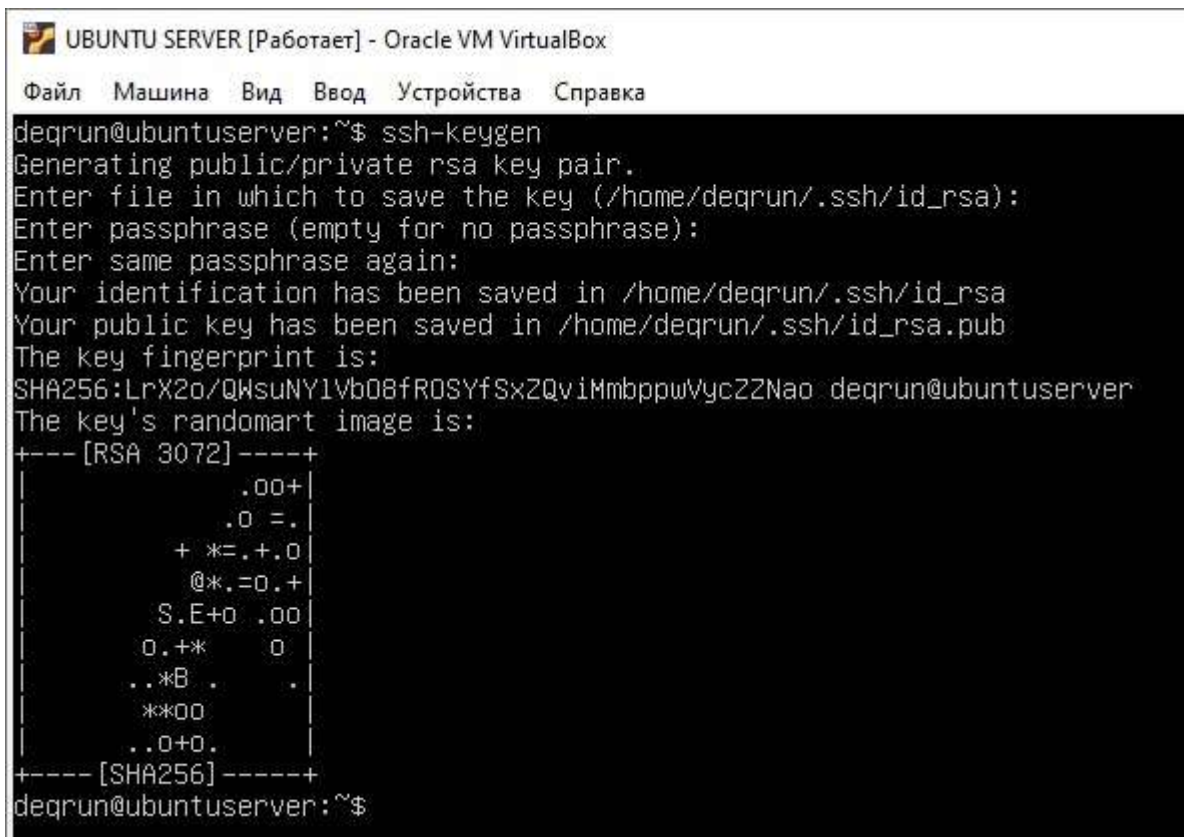


Рисунок 9 – Проверка наличия копии файла.

## 1.8. Формирование зашифрованных ключей

Сформируем зашифрованный ключ с помощью команды `ssh-keygen`.



```
UBUNTU SERVER [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
degrun@ubuntuserver:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/degrun/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/degrun/.ssh/id_rsa
Your public key has been saved in /home/degrun/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:LrX2o/QWsuNY1Vb08fR0SYfSxZQviMmbppwVycZZNao degrun@ubuntuserver
The key's randomart image is:
+---[RSA 3072]-----+
|          .00+      |
|         .0 =.     |
|        + * = . + . |
|       @ * . = 0 . + |
|      S.E+0 .00    |
|     0.+*      0   |
|    ..*B .       . |
|   **00         |
|  ..0+0.        |
+-----[SHA256]-----+
degrun@ubuntuserver:~$
```

Рисунок 10 – Формирование зашифрованных ключей

## 1.9. Передача публичного ключа

Передадим сгенерированный ключ на сервер с помощью команды `ssh-copy-id`.

```
/usr/bin/ssh-copy-id: ERROR: failed to open ID file '-/.ssh/id_rsa.pub': No such file
degrun@ubuntuserver:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud5@edu.kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/degrun/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
stud5@edu.kurgasov.ru's password:

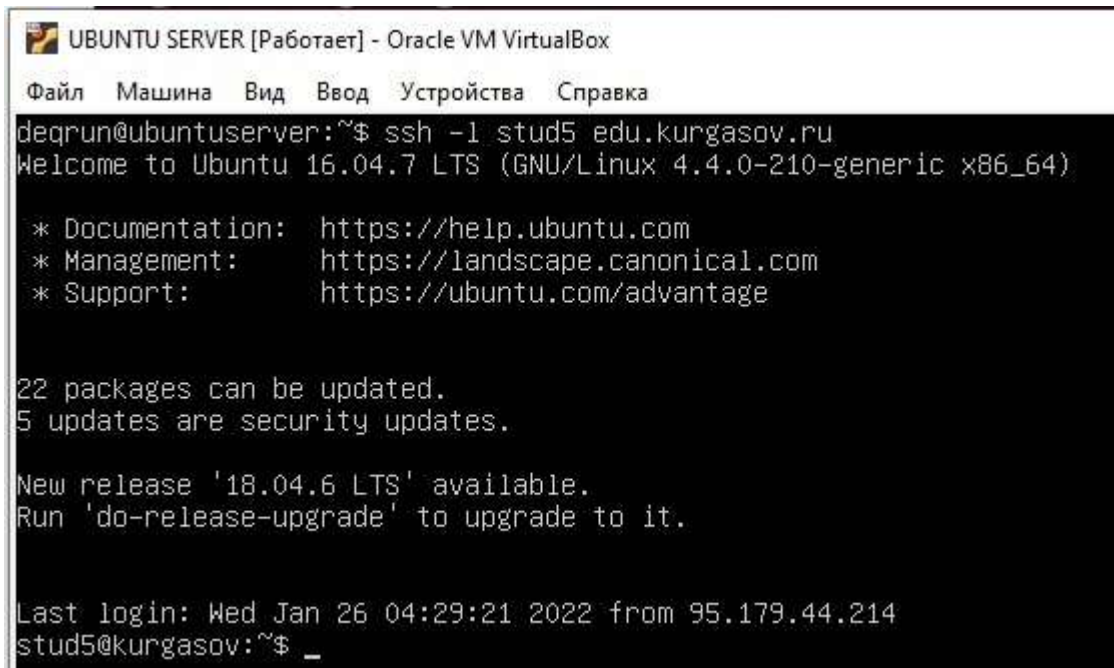
Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud5@edu.kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.
degrun@ubuntuserver:~$
```

Рисунок 11 – Передача публичного ключа

## 1.10. Подключение к удаленной системе

Подключимся к удаленной системе, благодаря ssh пароль при входе не потребовался.



```
UBUNTU SERVER [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
deqrun@ubuntuserver:~$ ssh -l stud5 edu.kurgasov.ru
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.

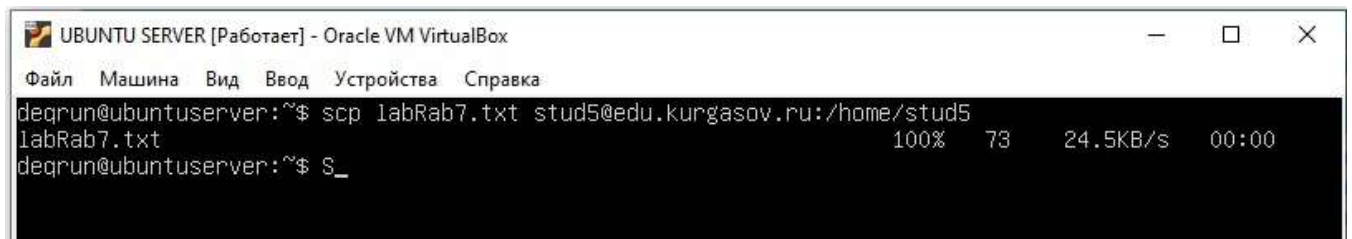
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Jan 26 04:29:21 2022 from 95.179.44.214
stud5@kurgasov:~$ _
```

Рисунок 12 – Подключение к удаленной системе.

### 1.11. Передача файла по зашифрованному каналу

Передадим файл удаленной системе, пароль снова не понадобился благодаря ssh.



The screenshot shows a terminal window titled "UBUNTU SERVER [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

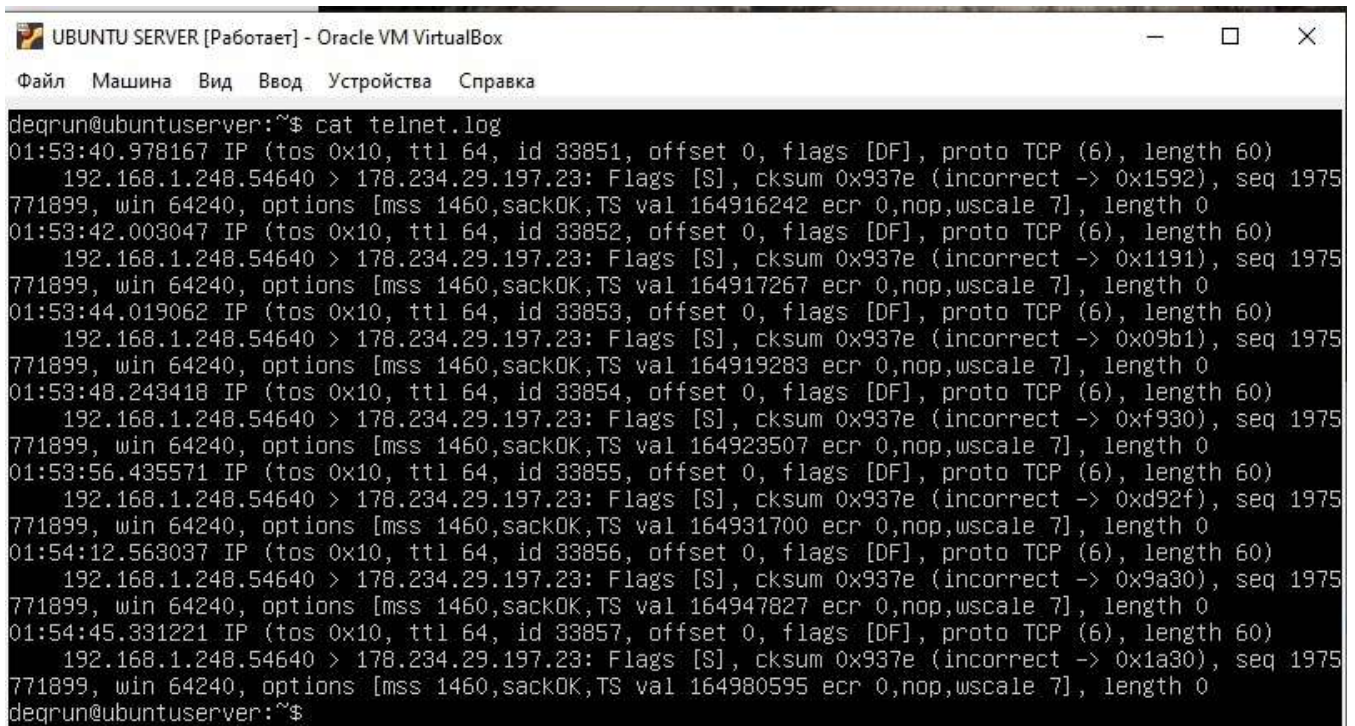
```
degrun@ubuntuserver:~$ scp labRab7.txt stud5@edu.kurgasov.ru:/home/stud5
labRab7.txt                                100% 73    24.5KB/s   00:00
degrun@ubuntuserver:~$ S_
```

Рисунок 13 – Передача файла по зашифрованному каналу.



## 1.12. Содержимое файла telnet.log

Просмотрим содержимое файла telnet.log.



```
degrun@ubuntuserver:~$ cat telnet.log
01:53:40.978167 IP (tos 0x10, ttl 64, id 33851, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0x1592), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164916242 ecr 0,nop,wscale 7], length 0
01:53:42.003047 IP (tos 0x10, ttl 64, id 33852, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0x1191), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164917267 ecr 0,nop,wscale 7], length 0
01:53:44.019062 IP (tos 0x10, ttl 64, id 33853, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0x09b1), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164919283 ecr 0,nop,wscale 7], length 0
01:53:48.243418 IP (tos 0x10, ttl 64, id 33854, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0xf930), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164923507 ecr 0,nop,wscale 7], length 0
01:53:56.435571 IP (tos 0x10, ttl 64, id 33855, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0xd92f), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164931700 ecr 0,nop,wscale 7], length 0
01:54:12.563037 IP (tos 0x10, ttl 64, id 33856, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0x9a30), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164947827 ecr 0,nop,wscale 7], length 0
01:54:45.331221 IP (tos 0x10, ttl 64, id 33857, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.248.54640 > 178.234.29.197.23: Flags [S], cksum 0x937e (incorrect -> 0x1a30), seq 1975
771899, win 64240, options [mss 1460,sackOK,TS val 164980595 ecr 0,nop,wscale 7], length 0
degrun@ubuntuserver:~$
```

Рисунок 14 – Содержимое файла telnet.log.



## 1.13. Содержимое файла ssh.log

Просмотрим содержимое файла ssh.log.

```
degrun@ubuntuserver:~$ cat ssh.log
02:02:24.297955 IP (tos 0x10, ttl 64, id 23315, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.248.41272 > 178.234.29.197.22: Flags [S], cksum 0x937e (incorrect -> 0xb51b), seq 1032
500132, win 64240, options [mss 1460,sackOK,TS val 165439562 ecr 0,nop,wscale 7], length 0
02:02:24.301944 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    178.234.29.197.22 > 192.168.1.248.41272: Flags [S.], cksum 0x979d (correct), seq 1925578790, ack
1032500133, win 28960, options [mss 1400,sackOK,TS val 66662548 ecr 165439562,nop,wscale 7], length
0
02:02:24.301979 IP (tos 0x10, ttl 64, id 23316, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.248.41272 > 178.234.29.197.22: Flags [.], cksum 0x9376 (incorrect -> 0x3554), ack 1, w
in 502, options [nop,nop,TS val 165439566 ecr 66662548], length 0
02:02:24.312964 IP (tos 0x0, ttl 59, id 52206, offset 0, flags [DF], proto TCP (6), length 94)
    178.234.29.197.22 > 192.168.1.248.41272: Flags [P.], cksum 0x0fdd (correct), seq 1:43, ack 1, wi
n 227, options [nop,nop,TS val 66662551 ecr 165439566], length 42
02:02:24.312979 IP (tos 0x10, ttl 64, id 23317, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.248.41272 > 178.234.29.197.22: Flags [.], cksum 0x9376 (incorrect -> 0x351c), ack 43,
win 502, options [nop,nop,TS val 165439577 ecr 66662551], length 0
02:04:21.248292 IP (tos 0x0, ttl 59, id 52207, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.1.248.41272: Flags [F.], cksum 0xc0fd (correct), seq 43, ack 1, win
227, options [nop,nop,TS val 66692551 ecr 165439577], length 0
02:04:21.248576 IP (tos 0x10, ttl 64, id 23318, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.248.41272 > 178.234.29.197.22: Flags [F.], cksum 0x9376 (incorrect -> 0xf71f), seq 1,
ack 44, win 502, options [nop,nop,TS val 165556513 ecr 66692551], length 0
02:04:21.252138 IP (tos 0x0, ttl 59, id 52208, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.1.248.41272: Flags [.], cksum 0xf831 (correct), ack 2, win 227, opti
ons [nop,nop,TS val 66692552 ecr 165556513], length 0
degrun@ubuntuserver:~$ _
```

Рисунок 15 – Содержимое файла ssh.log.

## **Выводы**

В результате выполнения лабораторной работы я получил знания по программному обеспечению удаленного доступа к распределённым 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.

## **Контрольные вопросы**

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

Удаленный доступ — функция, дающая пользователю возможность подключаться к компьютеру с помощью другого устройства через интернет практически отовсюду. Пользователь работает с файлами и программами точно так же, как если бы он находился возле этого компьютера. Ему не нужно будет скачивать все необходимые для работы данные на внешний носитель или отправлять их по почте — достаточно связаться с этим компьютером.

### **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.

- 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.**

Secure Shell - это зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами. Если необходимо что-либо сделать на удаленном сервере, скорее всего, придется воспользоваться SSH и работать через терминал.

В SSH существует несколько способов авторизации. Вы можете каждый раз вводить пароль пользователя или использовать более безопасный и надежный способ - ключи SSH. Второе – предпочтительнее, так как более удобно для применения, не требует ввода пароля.

**Принцип работы.** SSH сервер может выполнять аутентификацию пользователей с помощью различных алгоритмов. Самый популярный - это аутентификация по паролю. Он достаточно прост, но не очень безопасный. Пароли передаются по безопасному каналу, но они недостаточно сложны для противостояния попыткам перебора, а вычислительная мощность современных систем в сочетании со специальными скриптами делают перебор паролей очень простым. Существуют способы дополнительной безопасности, например, fail2ban<sup>1</sup>, но аутентификация по ключу SSH более надежна.

Каждая пара ключей состоит из открытого и закрытого ключа. Секретный 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. Открытый ключ загружается на удаленный сервер, к которому необходимо получить доступ. Его нужно добавить в специальный файл ~/.ssh/authorized\_keys.

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

Тысячи компаний по всему миру пользуются системами удаленного доступа и полагаются на них как на ключевую функцию их отделов ИТ. Удаленный доступ применим в бесчисленных отраслях, начиная с транснациональных коммерческих корпораций и заканчивая образовательными учреждениями, обеспечивающими удаленное обучение студентов.

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.