

Липецкий государственный технический университет
Факультет автоматизации и информатики
Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №7
по Операционной системе Linux
Работа с SSH

Студент

Пехова А.А.

Группа ПИ-19

Руководитель

Кургасов В.В.

Доцент, к.п.н.

Липецк 2022 г.

Цель работы

Ознакомиться с программным обеспечением удалённого доступа к распределённым системам обработки данных.

Задание

1. Создать подключение удаленного доступа к системе обработки данных, сформировать шифрованные ключи и произвести их обмен с удаленной системой, передать файл по шифрованному туннелю, воспользовавшись беспарольным доступом с аутентификацией по публичным ключам.

2. Выполнить подключение с использованием полноэкранного консольного оконного менеджера screen.

1. Запустить терминал с командной оболочкой ОС и ввести команду `tmux` (терминальный мультиплексор). Комбинациями клавиш `Ctrl-b` с создать новое окно и запустить 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;
```

2. В первом окне терминального мультиплексора попытаться установить соединение с удаленным сервером `domen.name` по протоколу TELNET. Для авторизации следует использовать логин `student`; /при возможности организовать такой доступ инженерами кафедры АСУ ЛГТУ/

3. Воспользовавшись окном сетевого монитора, анализировать прохождение сетевых пакетов между узлами назначения. Отметить пакеты инициации соединения `telnet`;

4. Подключившись к удаленной системе ввести пароль `Password` и выполнить команду `uname -a`, выведя тем самым информацию об удаленной системе. Для разрыва соединения использовать команду `logout`;

5. В окне сетевого монитора отметить пакеты иницирующие разрыв сессии `telnet`. Прервать фильтрацию пакетов сетевым анализатором `tcpdump`, воспользовавшись комбинацией `Ctrl-c`. В файле `telnet.log` выделить записи установления и разрыва соединения с сервером `telnet`;

6. Снова запустить анализатор сетевого трафика с фильтром пакетов получаемых и передаваемых узлу `domen.name` с TCP-портом источника и назначения 22. С помощью команды `tee`, вывести отфильтрованные IP-пакеты на терминал и сохранить данные в файл `ssh.log`, в домашнем каталоге

пользователя. Для этого следует воспользоваться командой `sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log`;

7. Переключившись на первое окно терминального мультиплексора, с помощью команды `ssh -l student domen.name` попытаться установить шифрованное соединение с удаленным сервером `domen.name`. Проследить передачу и прием пакетов между узлами в окне сетевого анализатора. Отметить взаимодействующие TCP-порты;

8. Подключившись к удаленной системе ввести пароль `Password` и выполнить команду `uname -a`, выведя информацию об удаленной системе;

9. Создать текстовый файл с содержанием ФИО и номера лабораторной работы на локальном узле и с помощью команды `scp -v -o User=student/home/student/имя_файла domen.name:/home/student/` передать его по шифрованному каналу на удаленную систему. Проверить наличие копии переданного файла на удаленном узле, воспользовавшись файловым менеджером «Midnight Commander» (команда `mc` на удаленной системе);

10. Отключившись от удаленного узла (команда `exit`), на локальном хосте, сформировать зашифрованные ключи, воспользовавшись командой `ssh-keygen`;

11. Используя команду `scp` с указанием места расположения файла (публичного ключа) на локальной системе (`/home/student/.ssh/key.pub`), произвести его передачу по шифрованному туннелю на удаленный узел в заданный каталог `/home/student/.ssh/` под именем `authorized_keys`. Проследить процесс пересылки пакетов между удаленными узлами в окне анализатора пакетов;

12. Воспользовавшись командой `ssh -l student domen.name`, снова сделать попытку подключения к удаленной системе. Отметить отличия в процедурах подключения и регистрации пользователя на удаленной системе;

13. Аналогично, с помощью команды `scp`, произвести повторную передачу текстового файла на удаленный узел. Убедиться в наличии переданной копии файла на удаленном хосте. Отметить отличия в процедуре передачи файла;

14. Остановить анализатор сетевых пакетов, воспользовавшись комбинацией `Ctrl-c`. Просмотреть содержимое файла `ssh.log`, отметить пакеты инициации сетевого взаимодействия и разрыва соединений TCP.

Ход работы

Начальные данные:

Логин – stud7

Пароль – QaucbE5Mvc

Запуск анализатора трафика tcpdump (порт 23)

- tmux (терминальный мультиплексор)
- Ctrl-b c (создание нового окна)
- sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log

(запуск анализатора трафика и сохранение данных в файл)

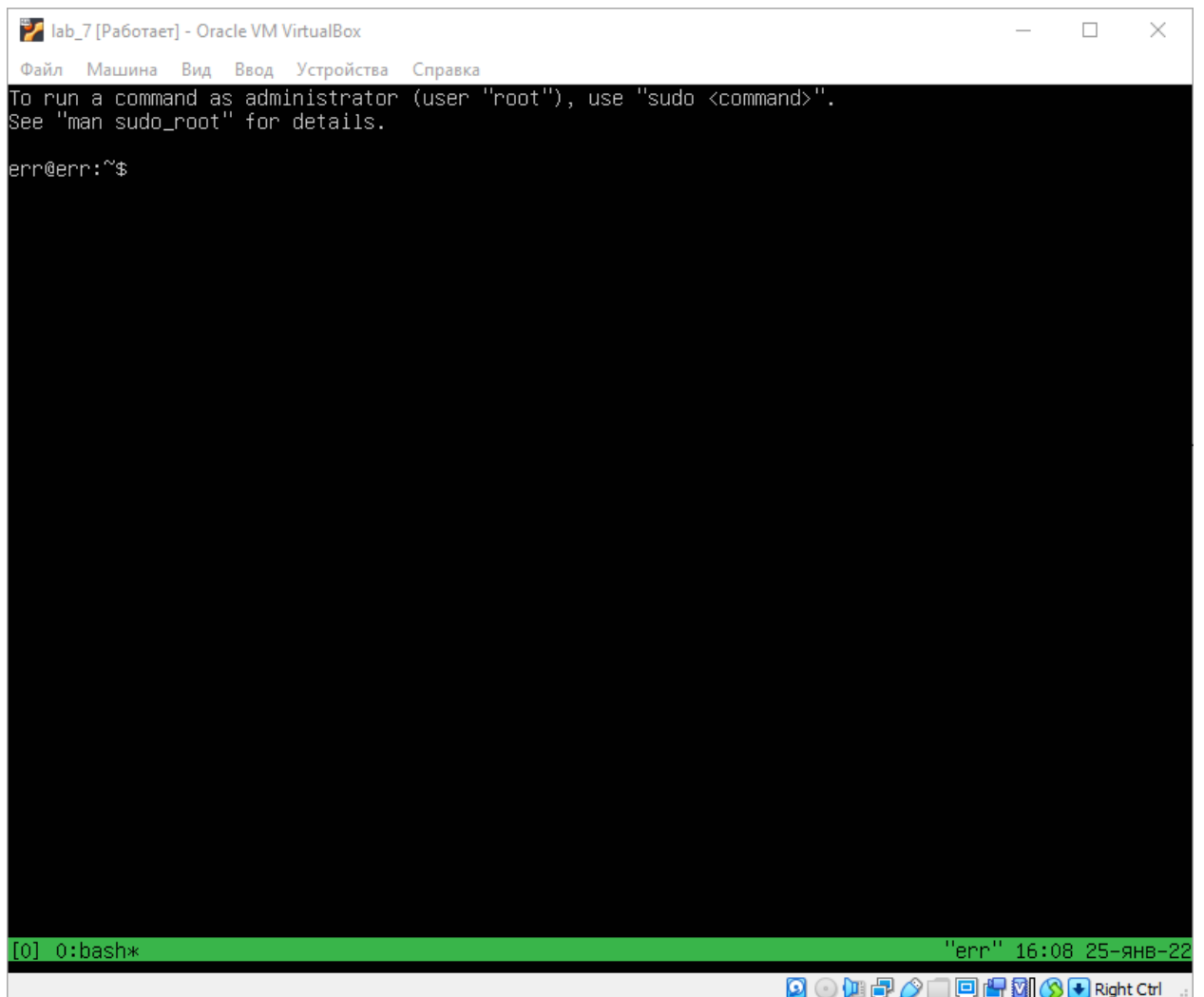
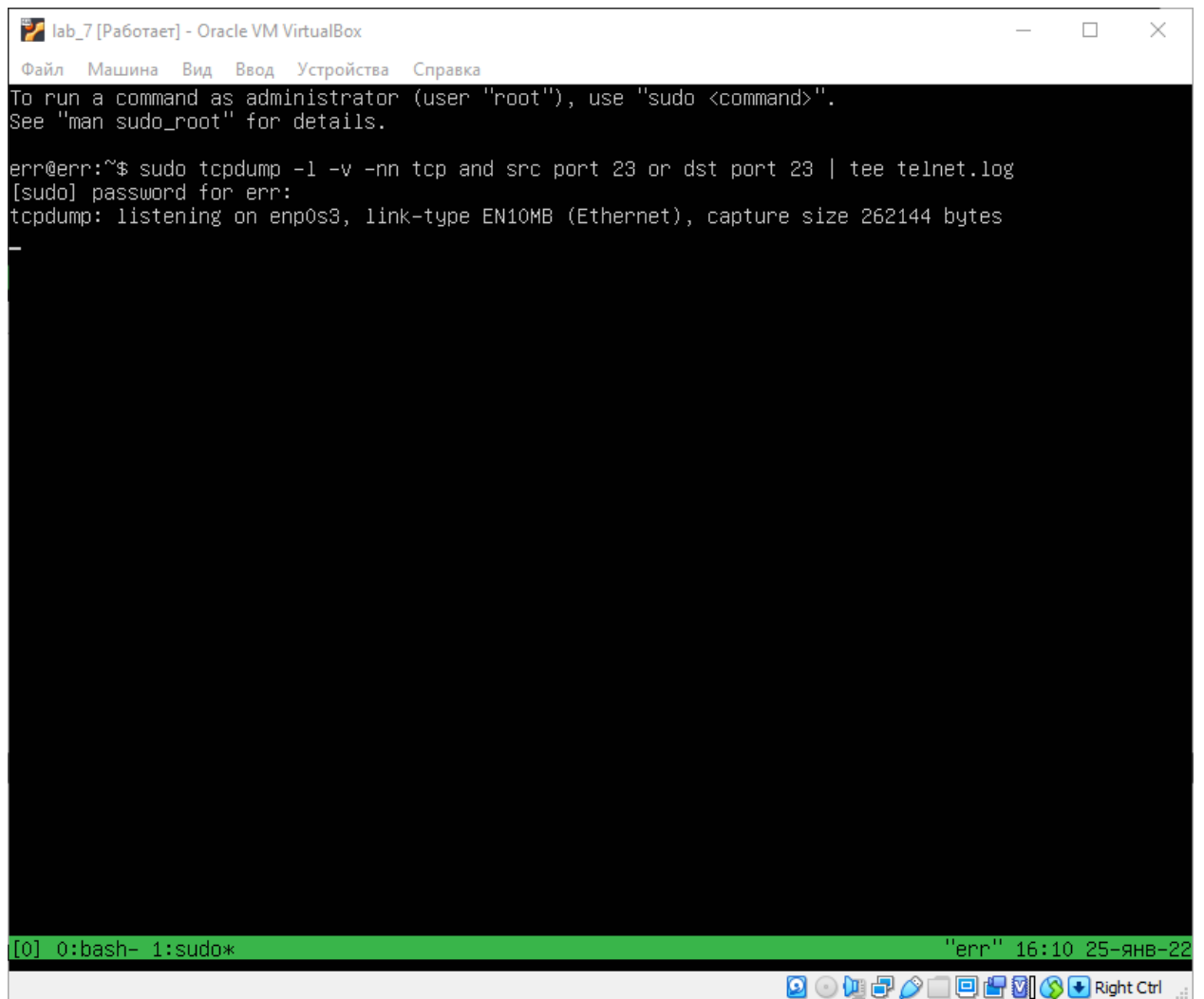


Рисунок 1 – tmux



The screenshot shows a terminal window titled "lab_7 [Работает] - Oracle VM VirtualBox". The menu bar includes "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The terminal text is as follows:

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

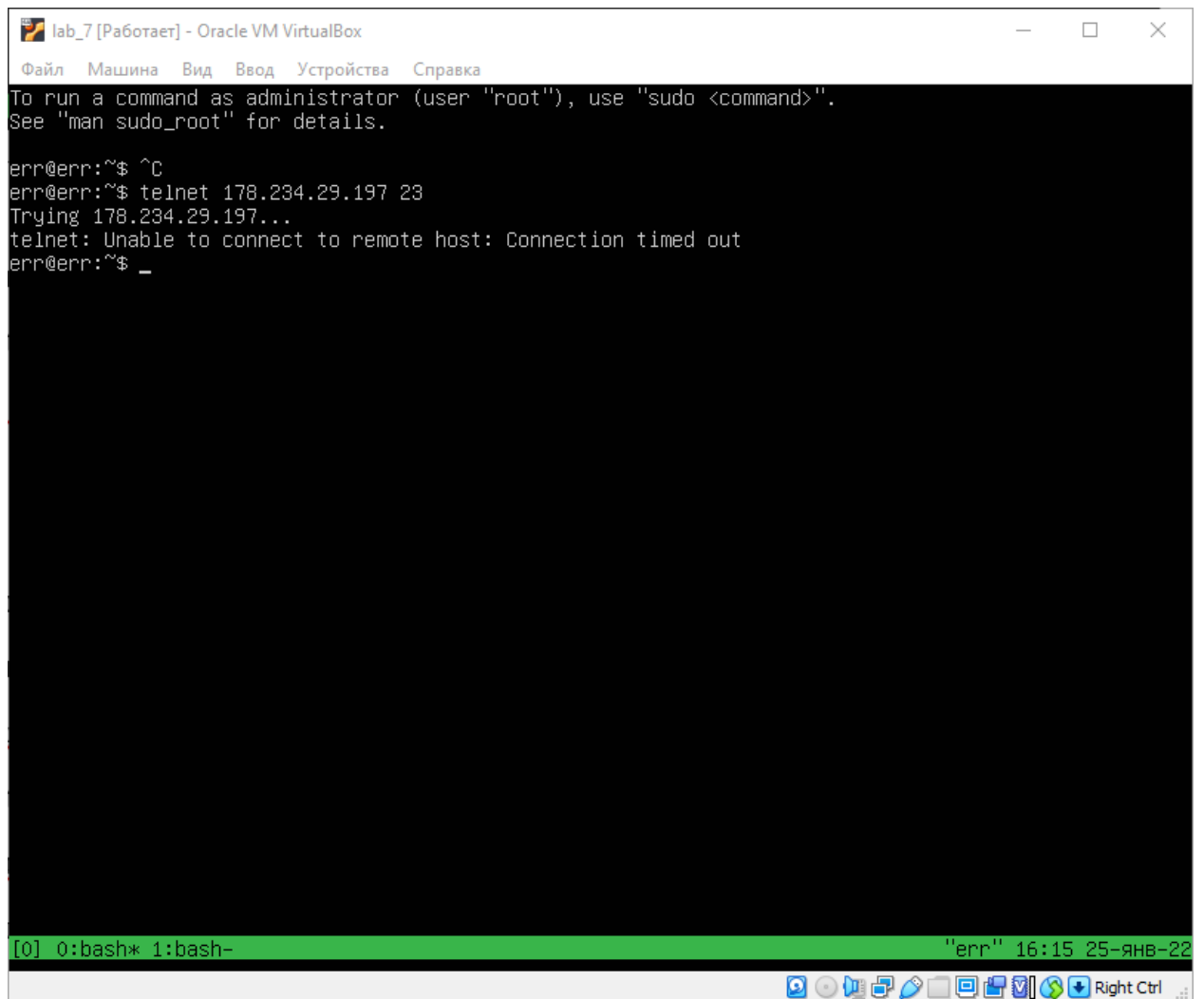
err@err:~$ sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log
[sudo] password for err:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
-
```

The terminal window has a green status bar at the bottom with the text "[0] 0: bash- 1: sudo*" and a timestamp "err" 16:10 25-январь-22". The bottom of the window shows a standard Linux desktop taskbar with various icons and a "Right Ctrl" button.

Рисунок 2 – Запуск анализатора трафика tcpdump

Попытка установки соединения (порт 23)

- Ctrl-b 0 (переход к 0 окну)
- telnet 178.234.29.197 23



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

err@err:~$ ^C
err@err:~$ telnet 178.234.29.197 23
Trying 178.234.29.197...
telnet: Unable to connect to remote host: Connection timed out
err@err:~$ _
```

[0] 0: bash* 1: bash- "err" 16:15 25-января-22

Рисунок 3 – Попытка установки соединения

23 порт недоступен, нет возможности подключиться к серверу удалённо.

Запуск анализатора трафика tcpdump (порт 22)

- tmux (терминальный мультиплексор)
- Ctrl-b с (создание нового окна)
- `sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee telnet.log`
(запуск анализатора трафика и сохранение данных в файл)

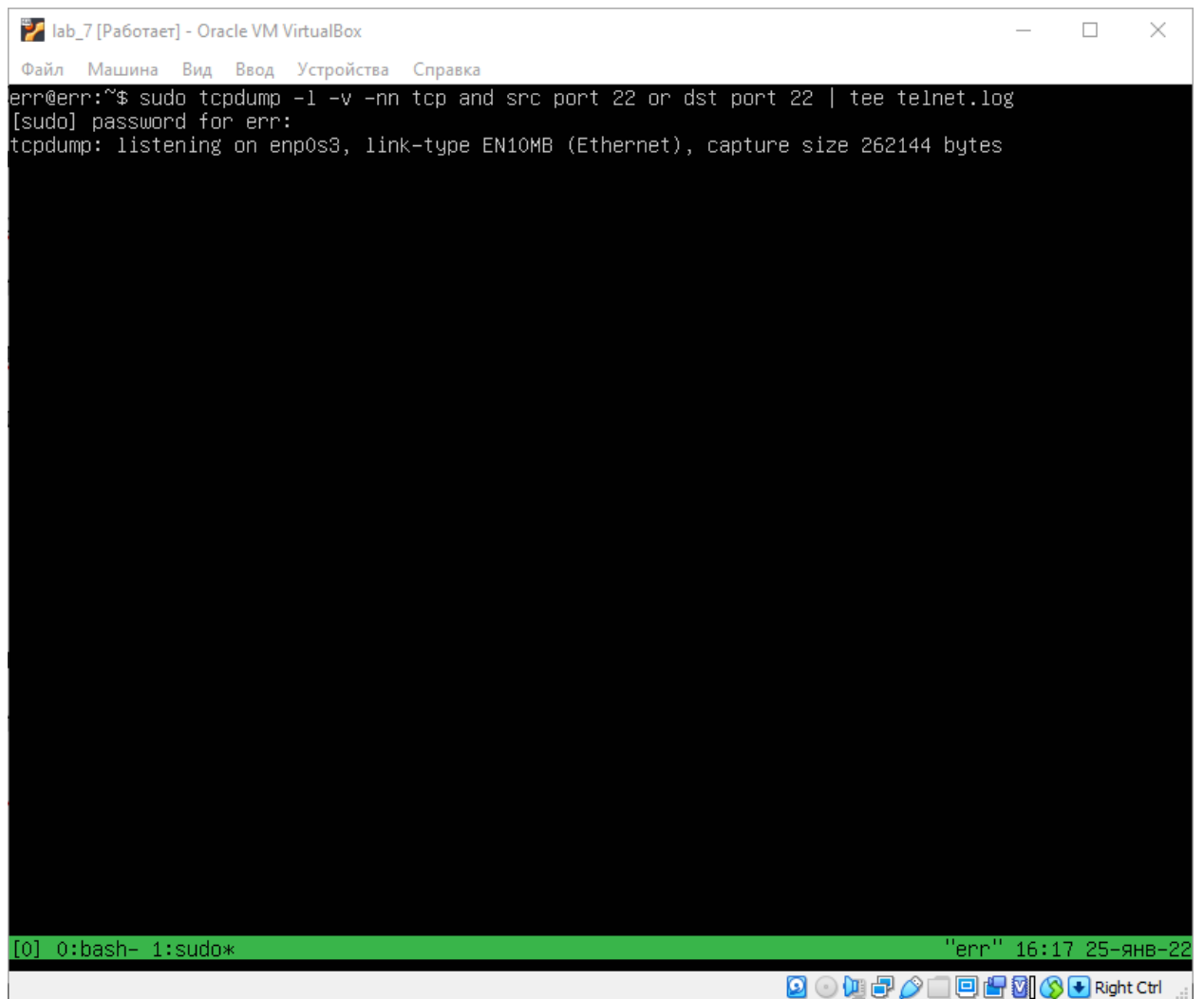


Рисунок 4 – Запуск анализатора трафика tcpdump

Попытка установки соединения (порт 22)

- Ctrl-b 0 (переход к 0 окну)
- telnet 178.234.29.197 22

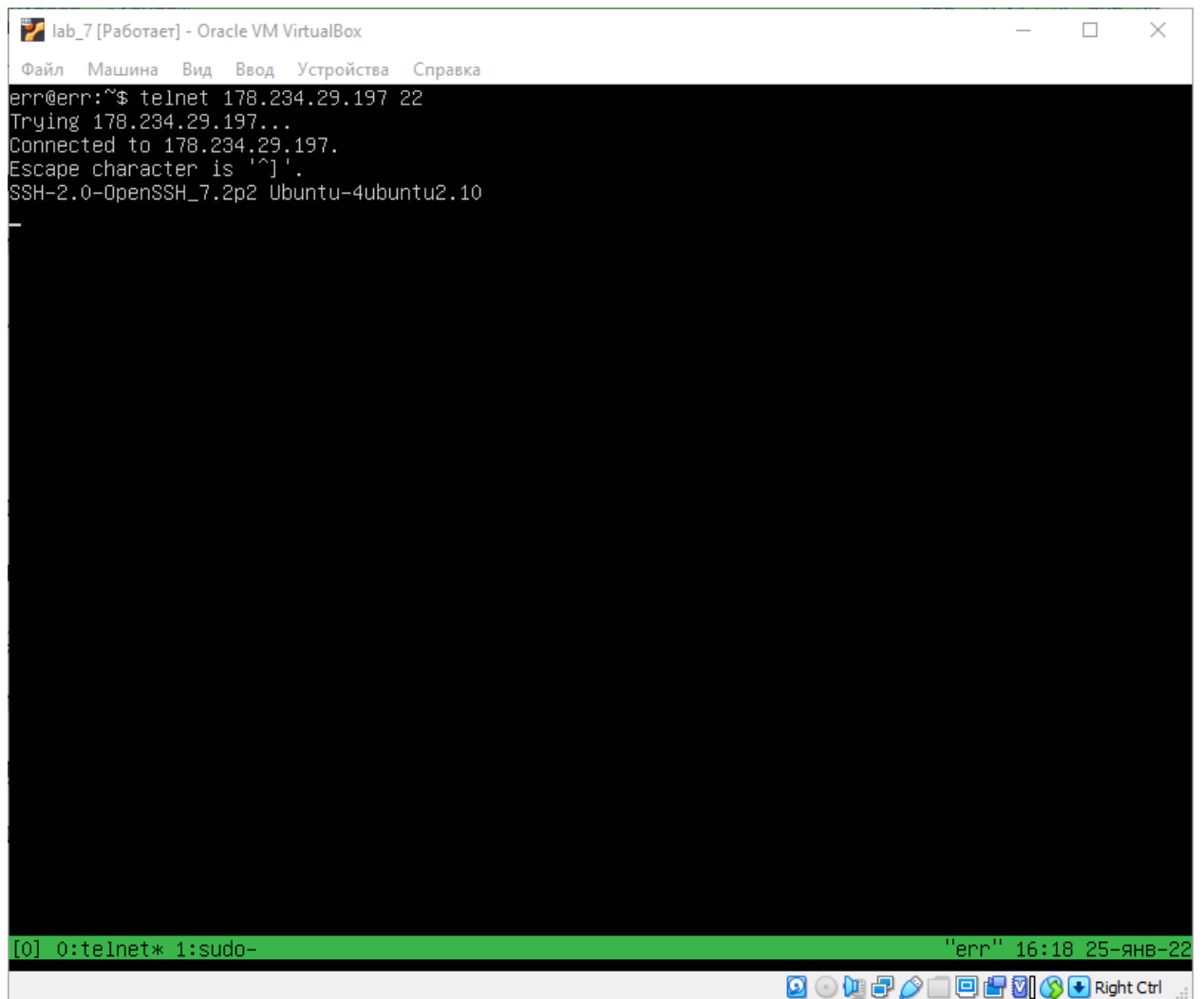


Рисунок 5 – Попытка установки соединения

Подключение удалось.

Запуск анализатора трафика tcpdump (порт 22)

- tmux (терминальный мультиплексор)
 - Ctrl-b c (создание нового окна)
 - sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log
- (запуск анализатора трафика и сохранение данных в файл)

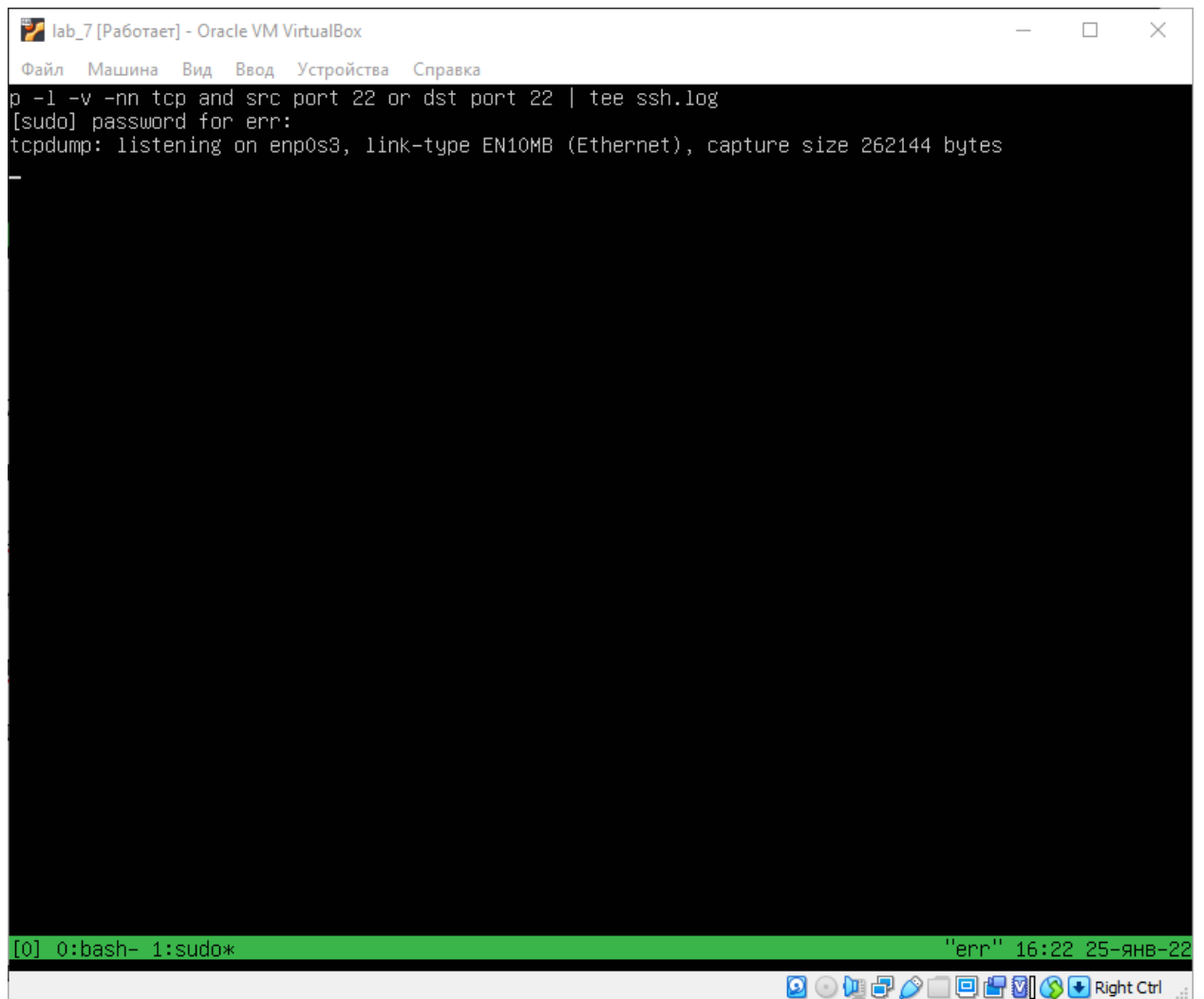
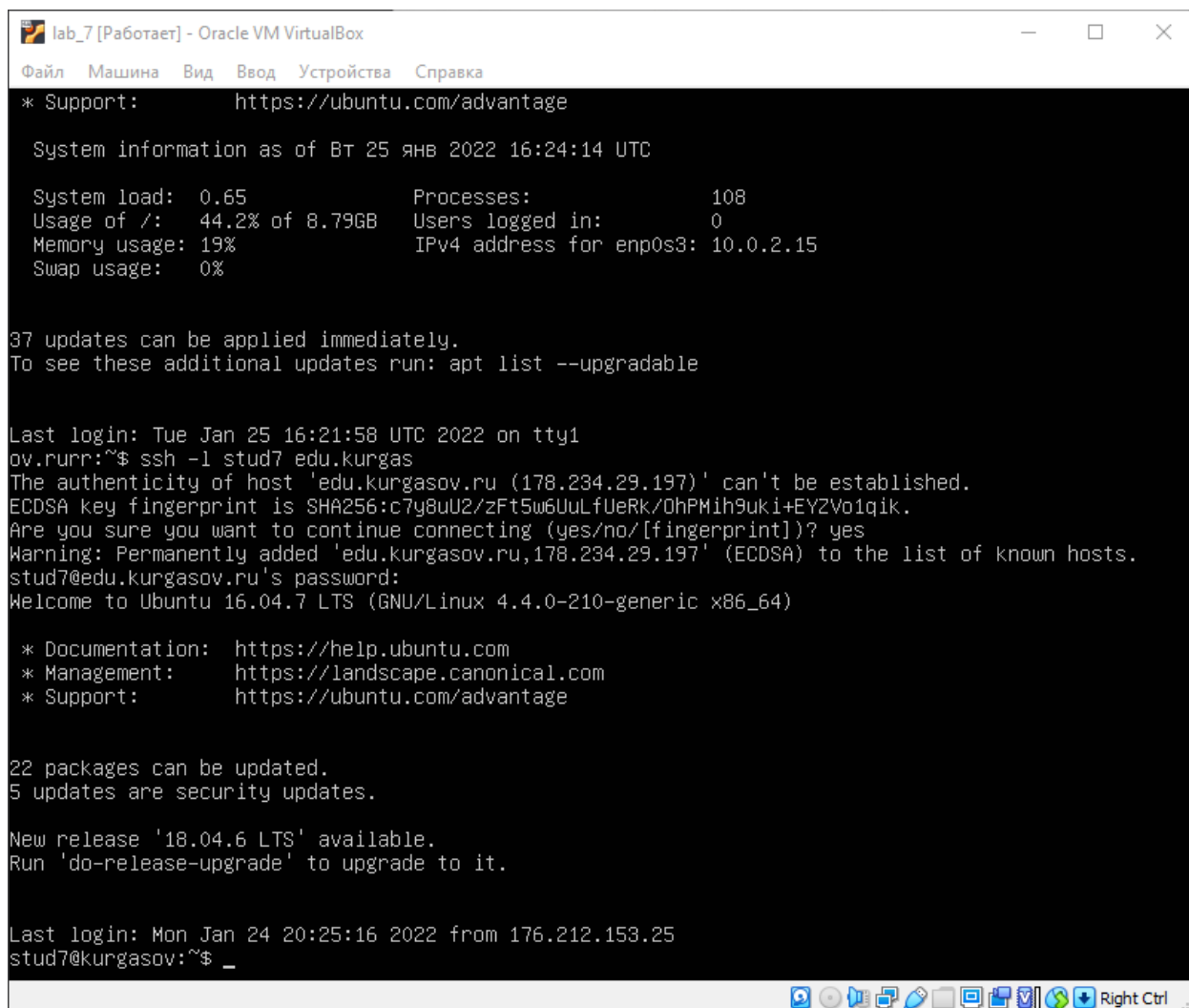


Рисунок 6 – Запуск анализатора трафика

Установление шифрованного соединения с удаленным сервером

- `ssh -l stud7 edu.kurgasov.ru`



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
* Support:      https://ubuntu.com/advantage

System information as of Вт 25 янв 2022 16:24:14 UTC

System load:  0.65          Processes:           108
Usage of /:   44.2% of 8.79GB Users logged in:     0
Memory usage: 19%          IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%

37 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Jan 25 16:21:58 UTC 2022 on tty1
ov.rurr:~$ ssh -l stud7 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])? yes
Warning: Permanently added 'edu.kurgasov.ru,178.234.29.197' (ECDSA) to the list of known hosts.
stud7@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.

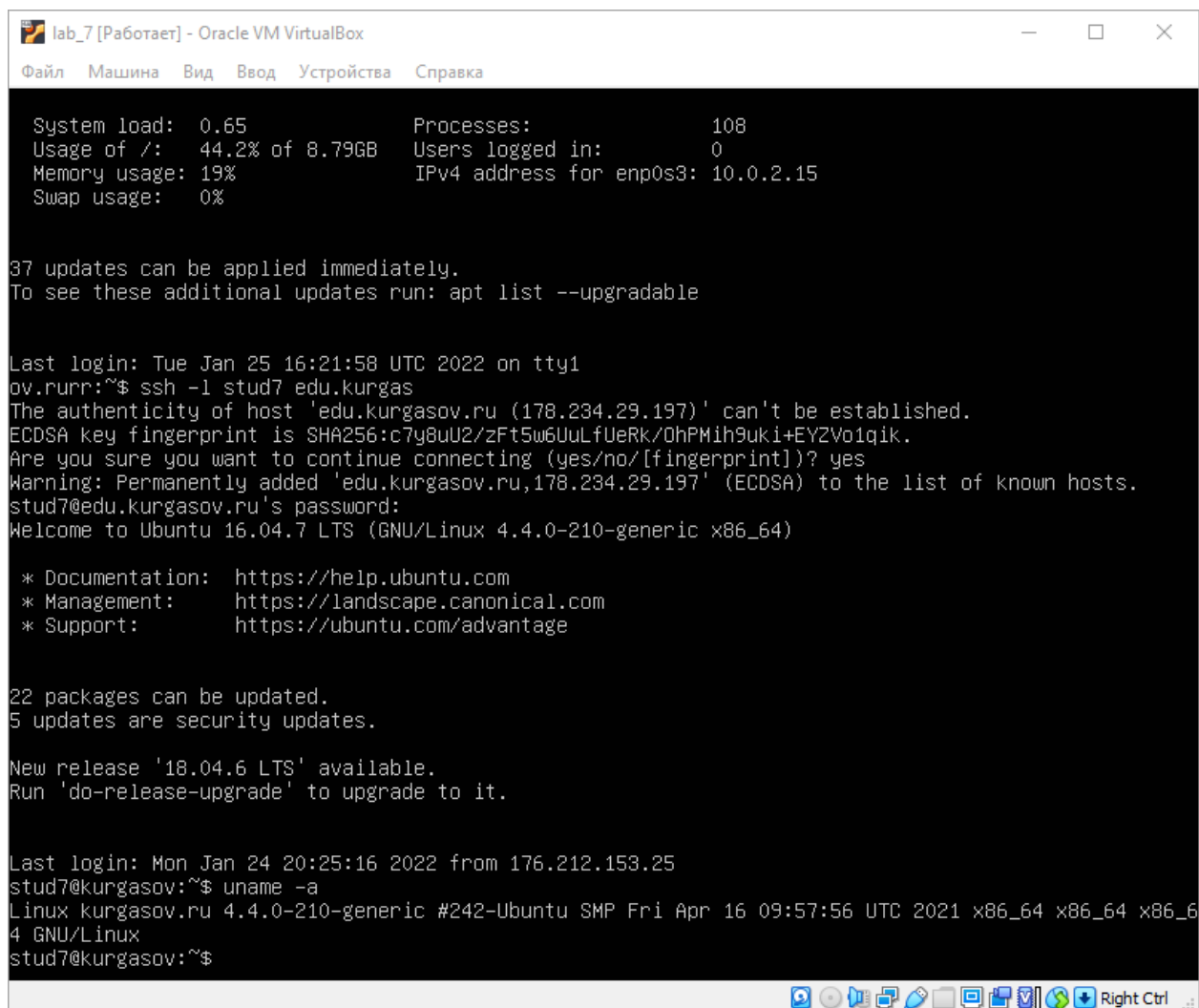
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Jan 24 20:25:16 2022 from 176.212.153.25
stud7@kurgasov:~$ _
```

Рисунок 7 – Установление шифрованного соединения

Вывод информации об удаленной системе

- `uname -a`



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

System load: 0.65          Processes:             108
Usage of /: 44.2% of 8.79GB Users logged in:      0
Memory usage: 19%         IPv4 address for enp0s3: 10.0.2.15
Swap usage: 0%

37 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Jan 25 16:21:58 UTC 2022 on tty1
ov.rurr:~$ ssh -l stud7 edu.kurgas
The authenticity of host 'edu.kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/OhPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'edu.kurgasov.ru,178.234.29.197' (ECDSA) to the list of known hosts.
stud7@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 Jan 24 20:25:16 2022 from 176.212.153.25
stud7@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
stud7@kurgasov:~$
```

Рисунок 7 – Вывод информации об удаленной системе.

Передача файла по зашифрованному каналу

- Ctrl-b c
- nano lr7.txt
- scp ~/lab7.txt stud7@edu.kurgasov.ru:/home/stud7

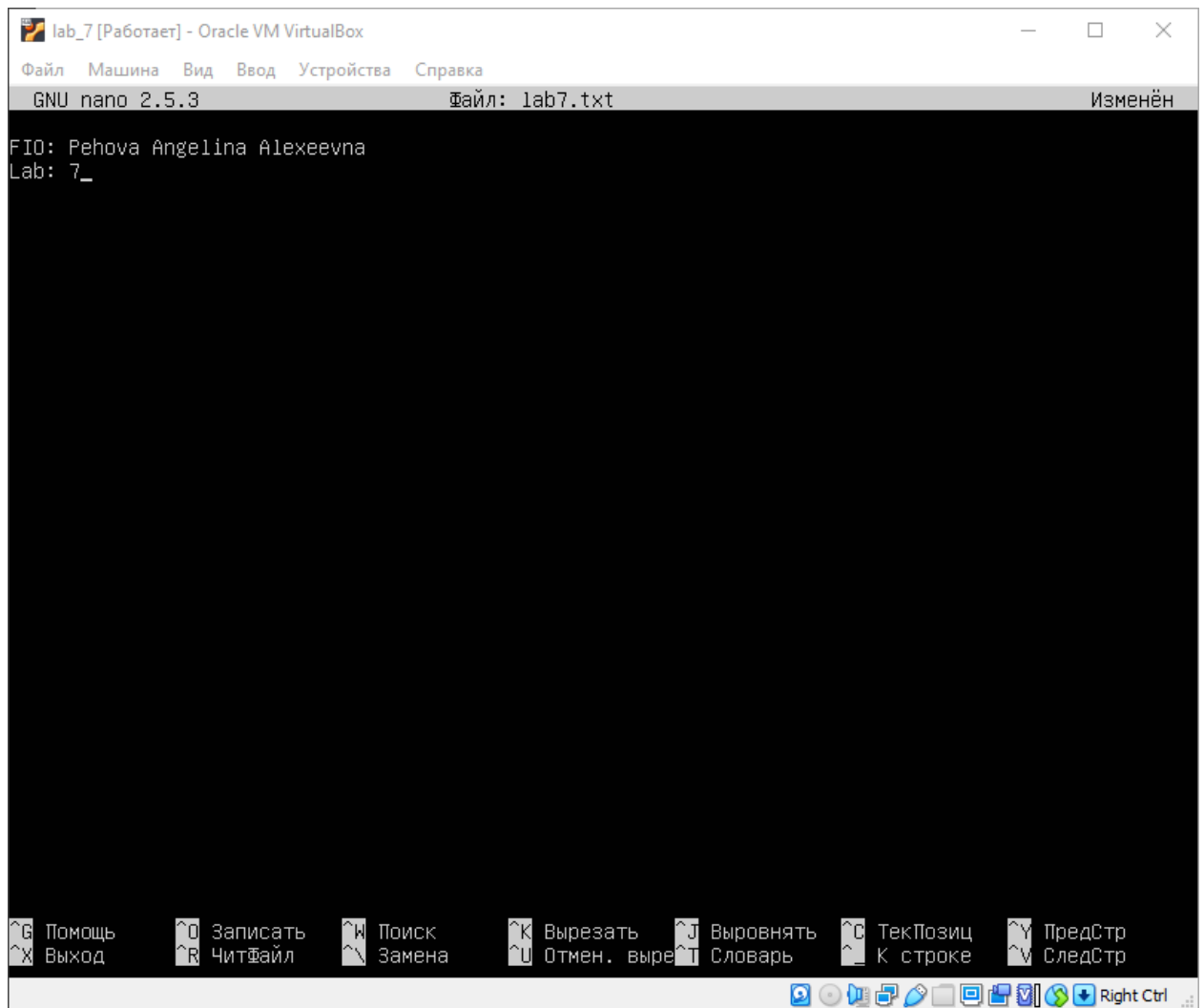


Рисунок 8 – Содержимое файла lab7.txt

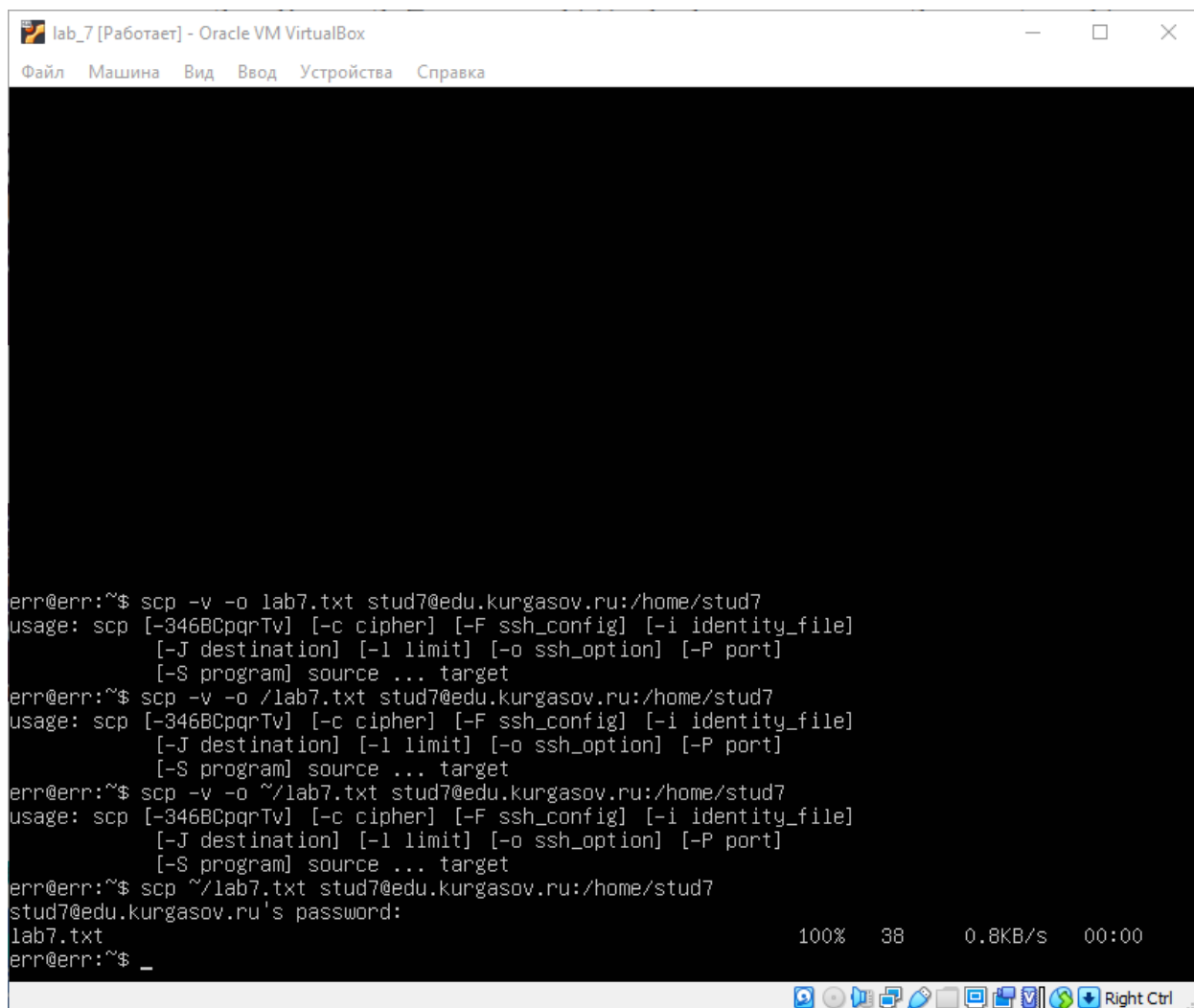
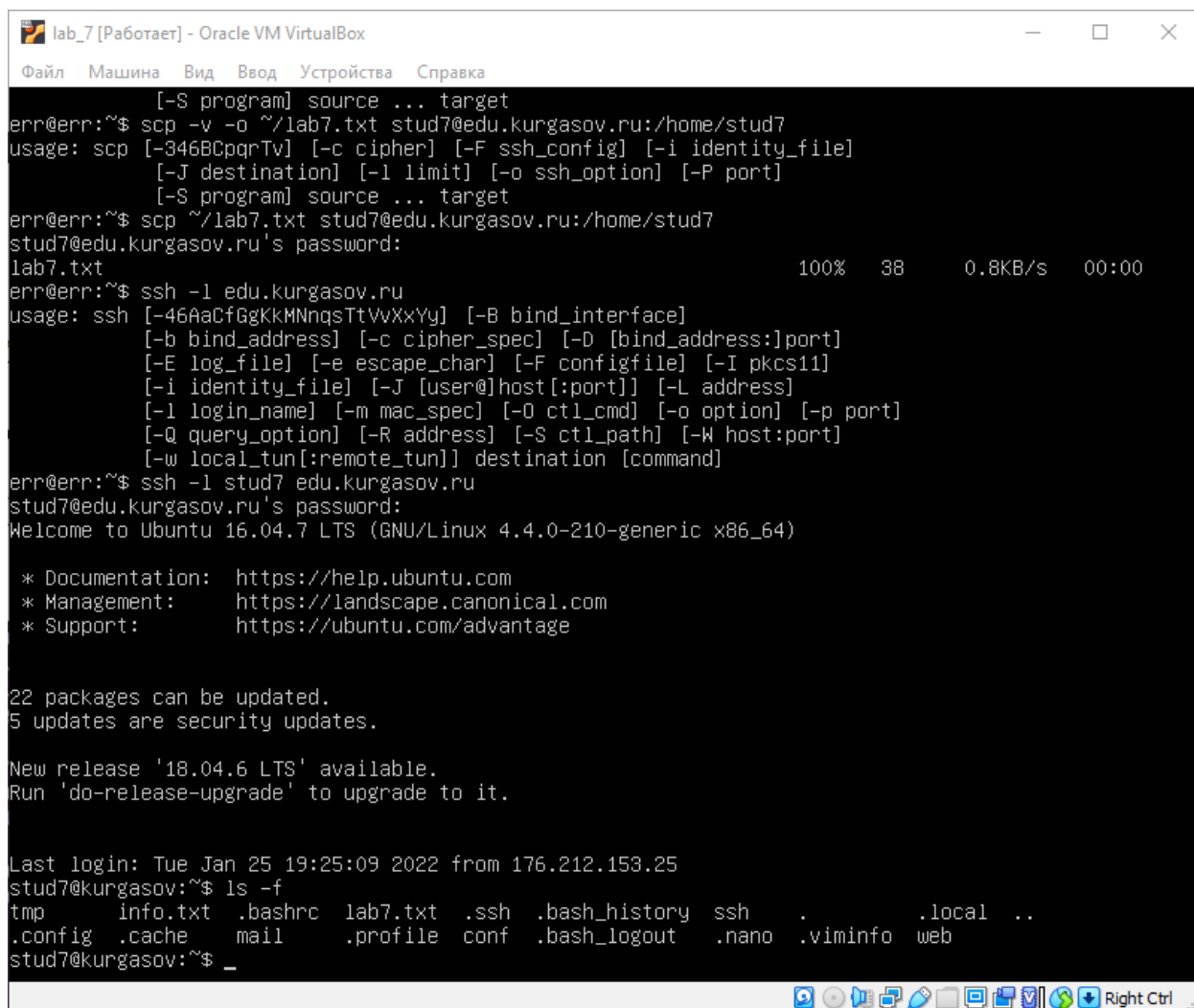


Рисунок 9 – Передача файла по зашифрованному каналу



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

[-S program] source ... target
err@err:~$ scp -v -o ~/lab7.txt stud7@edu.kurgasov.ru:/home/stud7
usage: scp [-346BCpqrTv] [-c cipher] [-F ssh_config] [-i identity_file]
          [-J destination] [-l limit] [-o ssh_option] [-P port]
          [-S program] source ... target
err@err:~$ scp ~/lab7.txt stud7@edu.kurgasov.ru:/home/stud7
stud7@edu.kurgasov.ru's password:
lab7.txt                                100%  38    0.8KB/s   00:00
err@err:~$ ssh -l edu.kurgasov.ru
usage: ssh [-46AaCfGgKkMnNqsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
          [-w local_tun[:remote_tun]] destination [command]
err@err:~$ ssh -l stud7 edu.kurgasov.ru
stud7@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.

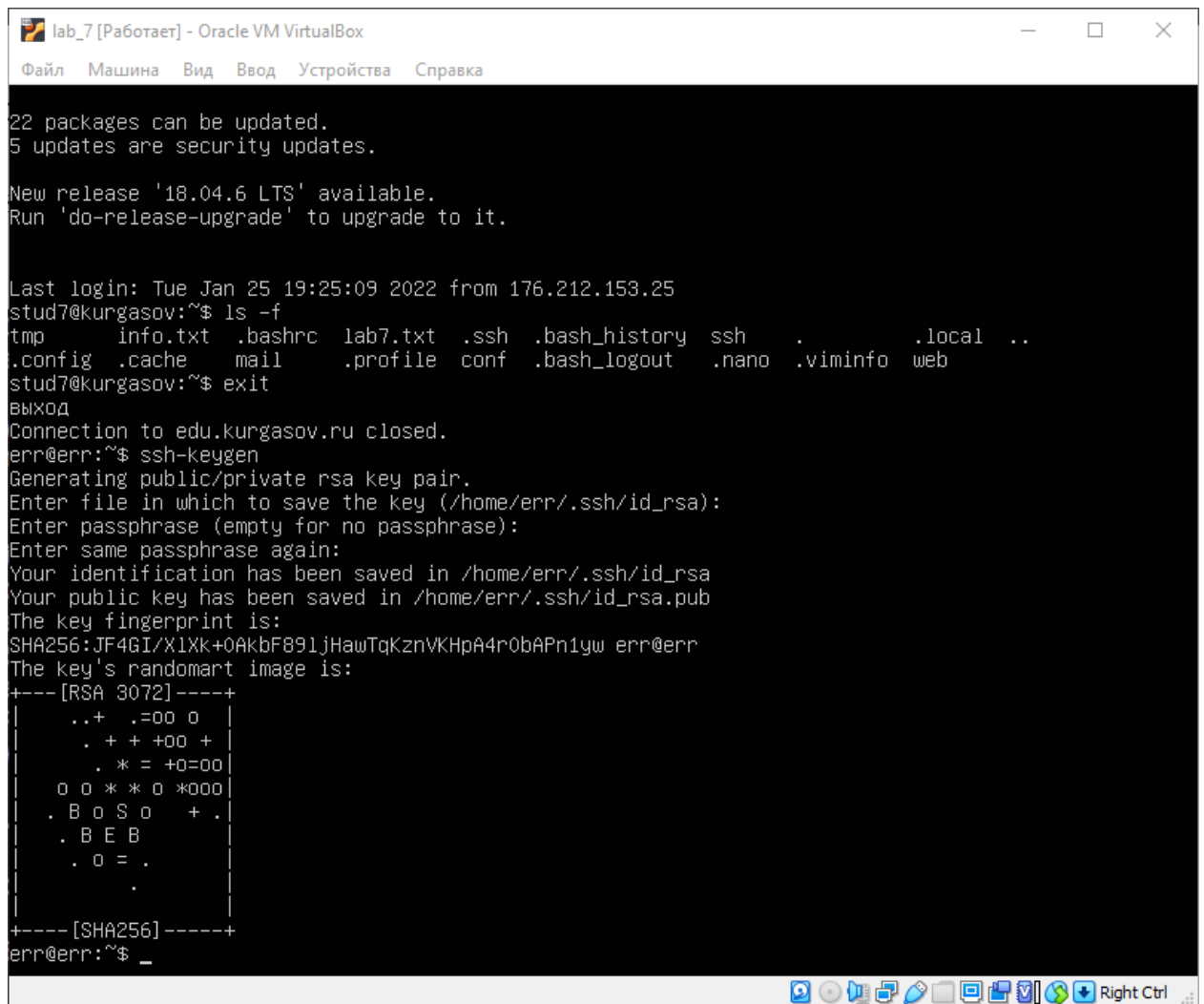
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 25 19:25:09 2022 from 176.212.153.25
stud7@kurgasov:~$ ls -f
tmp      info.txt  .bashrc  lab7.txt  .ssh     .bash_history  ssh      .      .local  ..
.config  .cache   mail     .profile  conf     .bash_logout  .nano   .viminfo  web
stud7@kurgasov:~$ _
```

Рисунок 10 – Проверка наличия копии файла

Формирование зашифрованных ключей

- exit (выход)
- ssh-keygen (формирование зашифрованных ключей)



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

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

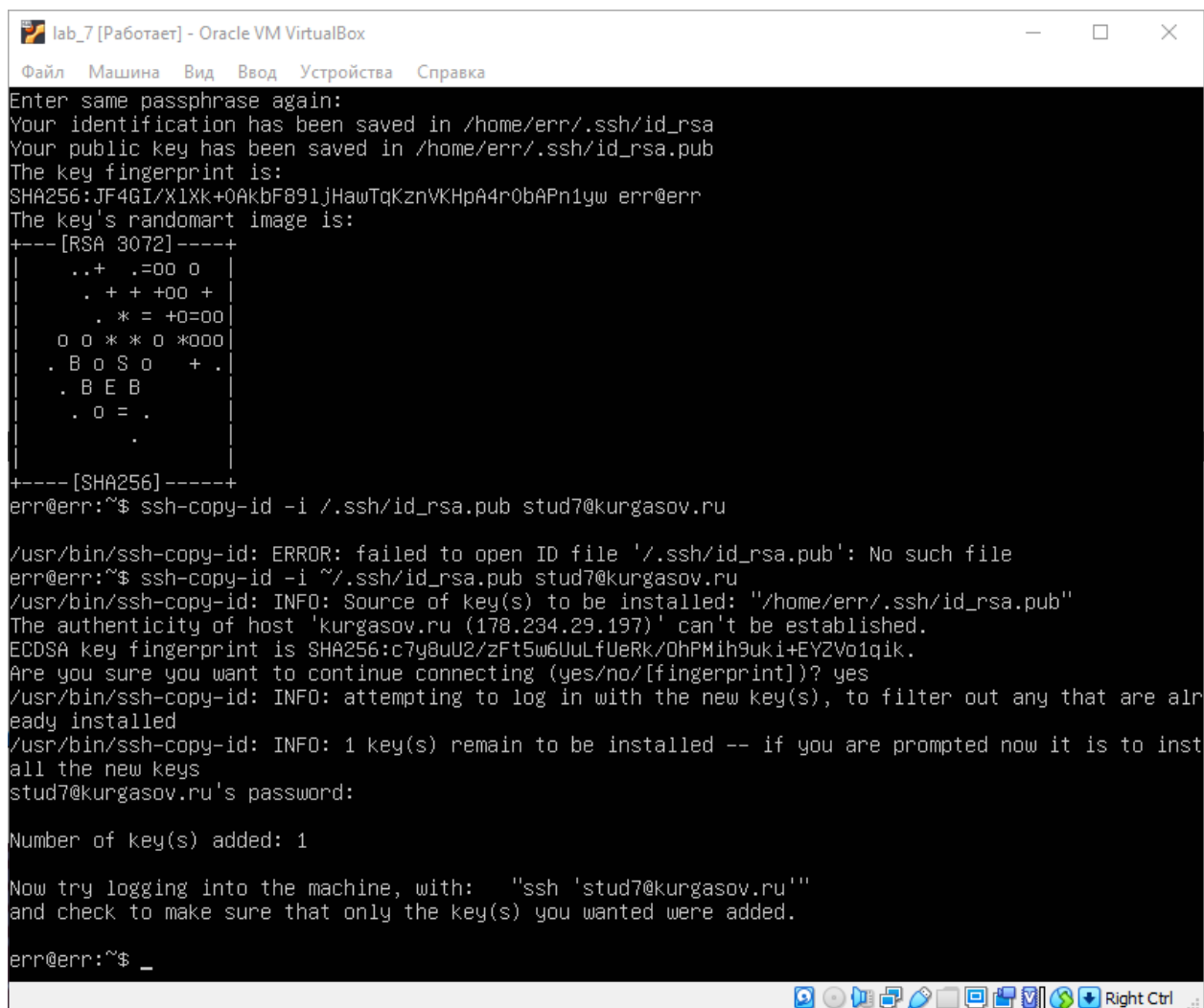
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 25 19:25:09 2022 from 176.212.153.25
stud7@kurgasov:~$ ls -f
tmp      info.txt  .bashrc  lab7.txt  .ssh     .bash_history  ssh      .      .local  ..
.config  .cache   mail     .profile  conf     .bash_logout  .nano    .viminfo  web
stud7@kurgasov:~$ exit
ВЫХОД
Connection to edu.kurgasov.ru closed.
err@err:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/err/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/err/.ssh/id_rsa
Your public key has been saved in /home/err/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:JF4GI/XlXk+0Akbf891jHawTqKznVKHpA4r0bAPn1yw err@err
The key's randomart image is:
+---[RSA 3072]-----+
|  ..+  ..=00 0 |
|  . + + +00 + |
|  . * = +0=00 |
|  0 0 * * 0 *000 |
|  . B 0 S 0  + . |
|  . B E B |
|  . 0 = . |
|  . |
+-----[SHA256]-----+
err@err:~$ _
```

Рисунок 11 – Формирование зашифрованных ключей

Передача публичного ключа

- `ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@kurgasov.ru`



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Enter same passphrase again:
Your identification has been saved in /home/err/.ssh/id_rsa
Your public key has been saved in /home/err/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:JF4GI/X1XK+0Akbf891jHawTqKznvKHpA4r0bAPn1yw err@err
The key's randomart image is:
+---[RSA 3072]-----+
|  ..+  .==00 0 |
|  . + + +00 + |
|  . * = +0=00 |
|  0 0 * * 0 *000 |
|  . B 0 S 0   + . |
|  . B E B      |
|  . 0 = .      |
|                |
+---[SHA256]-----+
err@err:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@kurgasov.ru

/usr/bin/ssh-copy-id: ERROR: failed to open ID file '/.ssh/id_rsa.pub': No such file
err@err:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/err/.ssh/id_rsa.pub"
The authenticity of host 'kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/DhPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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
stud7@kurgasov.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud7@kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.

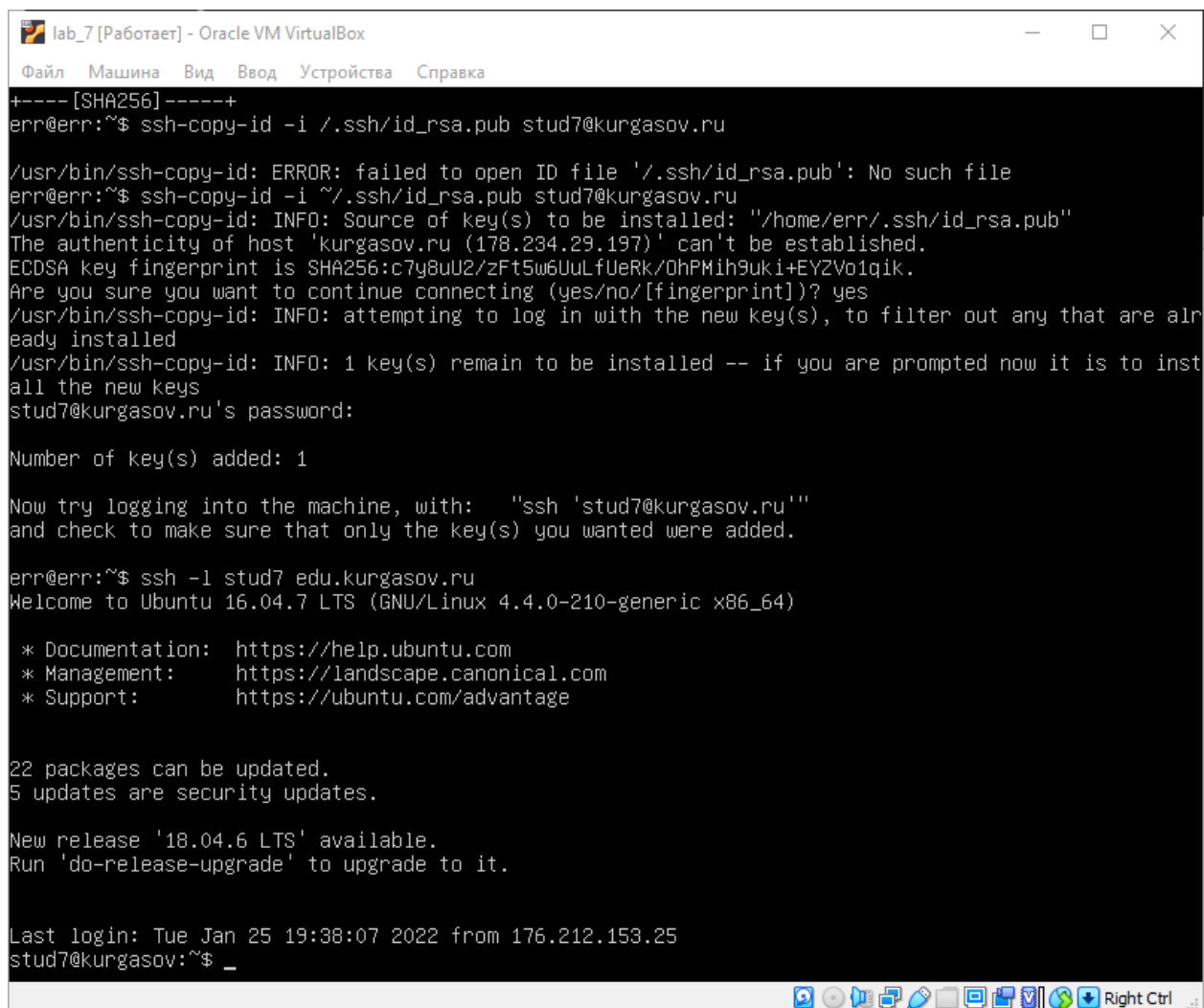
err@err:~$ _
```

Рисунок 12 – Передача публичного ключа

Подключение к удаленной системе

- `ssh -l stud7 edu.kurgasov.ru`

Благодаря ssh пароль при входе не потребовался.



```
+----[SHA256]-----+
err@err:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@kurgasov.ru

/usr/bin/ssh-copy-id: ERROR: failed to open ID file '/.ssh/id_rsa.pub': No such file
err@err:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/err/.ssh/id_rsa.pub"
The authenticity of host 'kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/0hPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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
stud7@kurgasov.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud7@kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.

err@err:~$ ssh -l stud7 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.

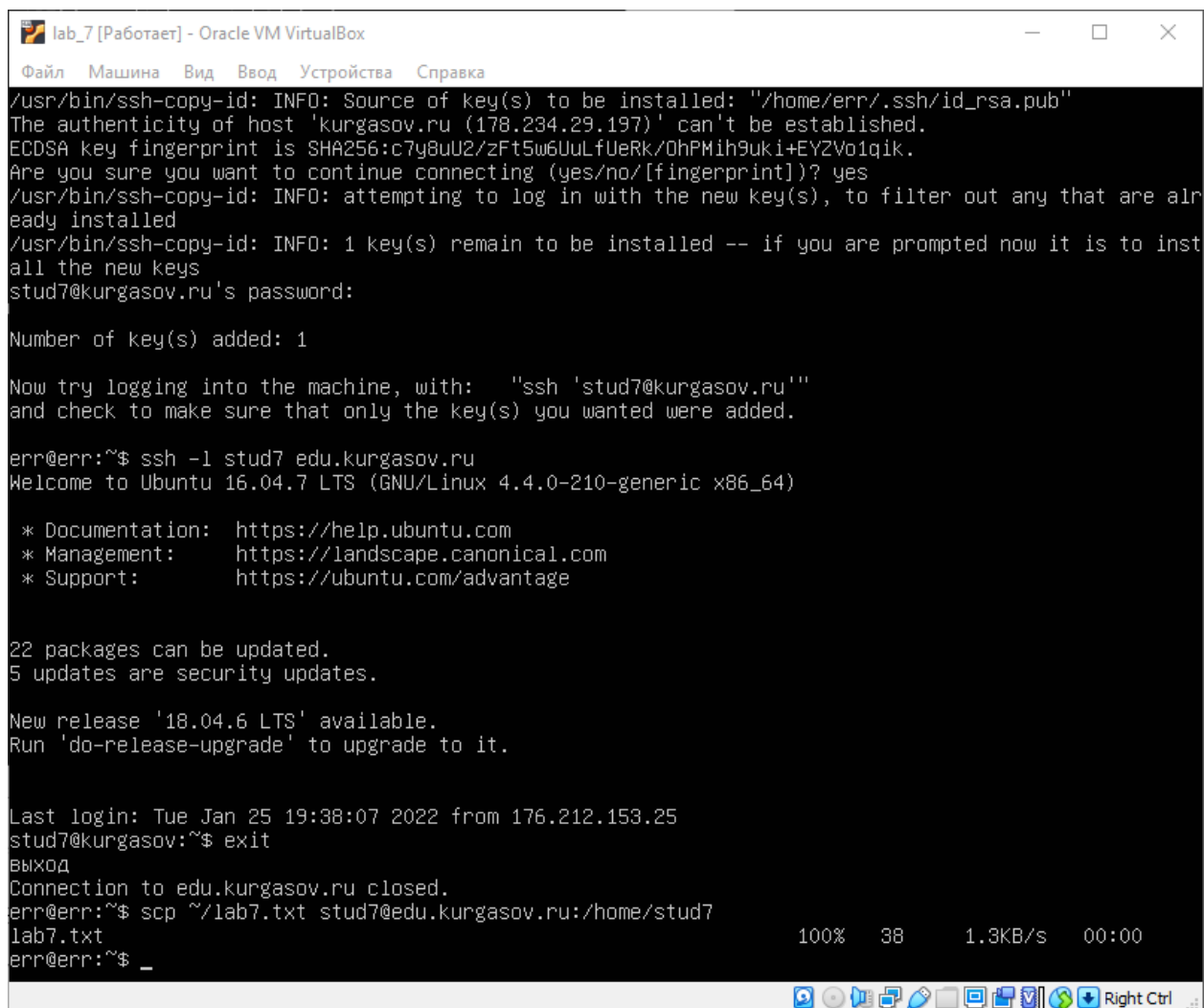
Last login: Tue Jan 25 19:38:07 2022 from 176.212.153.25
stud7@kurgasov:~$ _
```

Рисунок 13 – Подключение к удаленной системе.

Передача файла по зашифрованному каналу

- `scp ~/lab7.txt stud7@edu.kurgasov.ru:/home/stud7`

Благодаря ssh пароль не понадобился.



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/err/.ssh/id_rsa.pub"
The authenticity of host 'kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/0hPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install all the new keys
stud7@kurgasov.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud7@kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.

err@err:~$ ssh -l stud7 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.

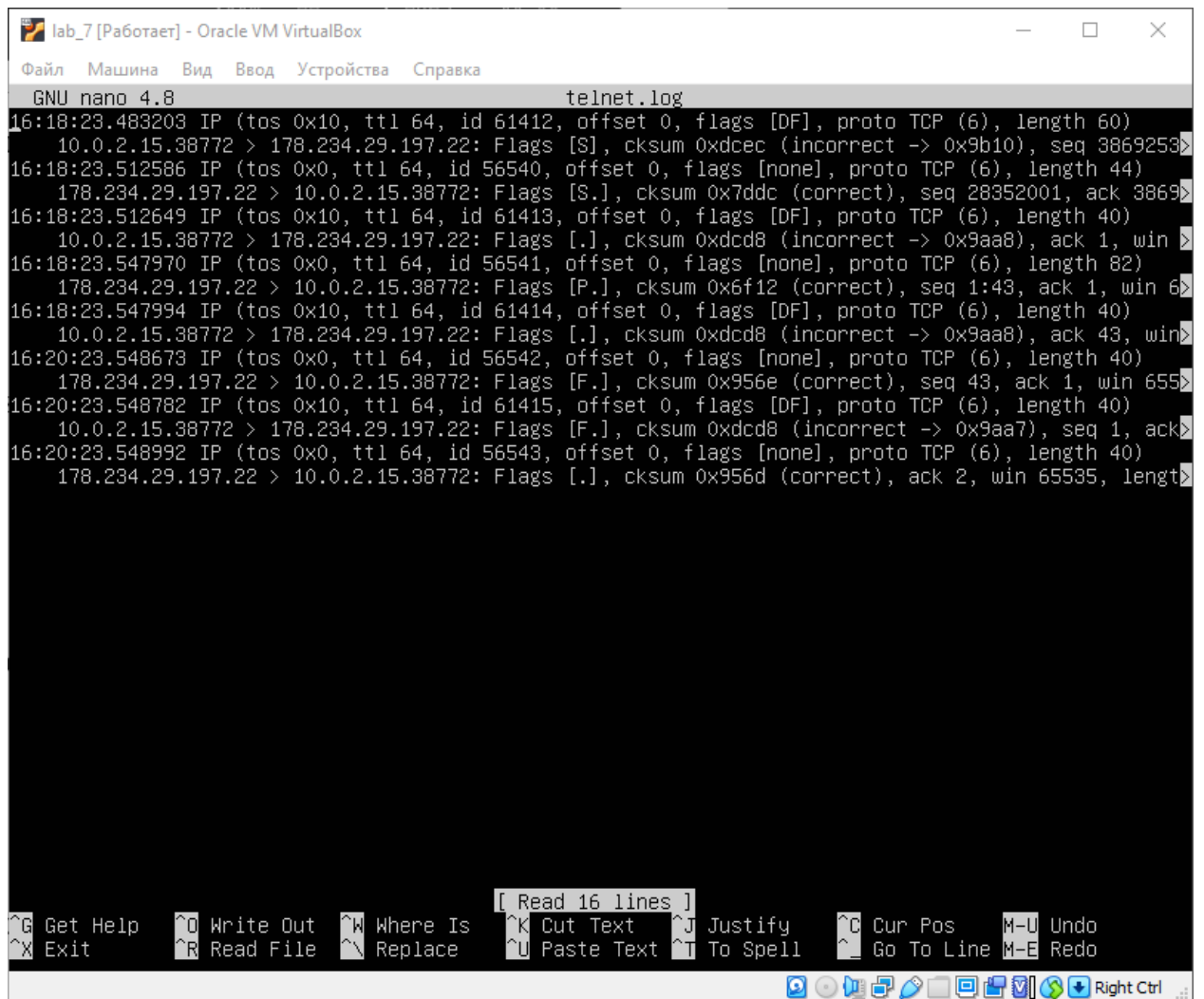
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 25 19:38:07 2022 from 176.212.153.25
stud7@kurgasov:~$ exit
выход
Connection to edu.kurgasov.ru closed.
err@err:~$ scp ~/lab7.txt stud7@edu.kurgasov.ru:/home/stud7
lab7.txt                                100%  38    1.3KB/s   00:00
err@err:~$ _
```

Рисунок 14 – Передача файла по зашифрованному каналу

Содержимое файла telnet.log

- nano telnet.log



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 4.8                               telnet.log
16:18:23.483203 IP (tos 0x10, ttl 64, id 61412, offset 0, flags [DF], proto TCP (6), length 60)
10.0.2.15.38772 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0x9b10), seq 3869253>
16:18:23.512586 IP (tos 0x0, ttl 64, id 56540, offset 0, flags [none], proto TCP (6), length 44)
178.234.29.197.22 > 10.0.2.15.38772: Flags [S.], cksum 0x7ddc (correct), seq 28352001, ack 3869>
16:18:23.512649 IP (tos 0x10, ttl 64, id 61413, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.38772 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x9aa8), ack 1, win >
16:18:23.547970 IP (tos 0x0, ttl 64, id 56541, offset 0, flags [none], proto TCP (6), length 82)
178.234.29.197.22 > 10.0.2.15.38772: Flags [P.], cksum 0x6f12 (correct), seq 1:43, ack 1, win 6>
16:18:23.547994 IP (tos 0x10, ttl 64, id 61414, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.38772 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x9aa8), ack 43, win>
16:20:23.548673 IP (tos 0x0, ttl 64, id 56542, offset 0, flags [none], proto TCP (6), length 40)
178.234.29.197.22 > 10.0.2.15.38772: Flags [F.], cksum 0x956e (correct), seq 43, ack 1, win 655>
16:20:23.548782 IP (tos 0x10, ttl 64, id 61415, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.38772 > 178.234.29.197.22: Flags [F.], cksum 0xdcd8 (incorrect -> 0x9aa7), seq 1, ack>
16:20:23.548992 IP (tos 0x0, ttl 64, id 56543, offset 0, flags [none], proto TCP (6), length 40)
178.234.29.197.22 > 10.0.2.15.38772: Flags [.], cksum 0x956d (correct), ack 2, win 65535, lengt>

[ Read 16 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^_ Replace   ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
Right Ctrl
```

Рисунок 15 – Содержимое файла telnet.log

Содержимое файла ssh.log

- nano ssh.log

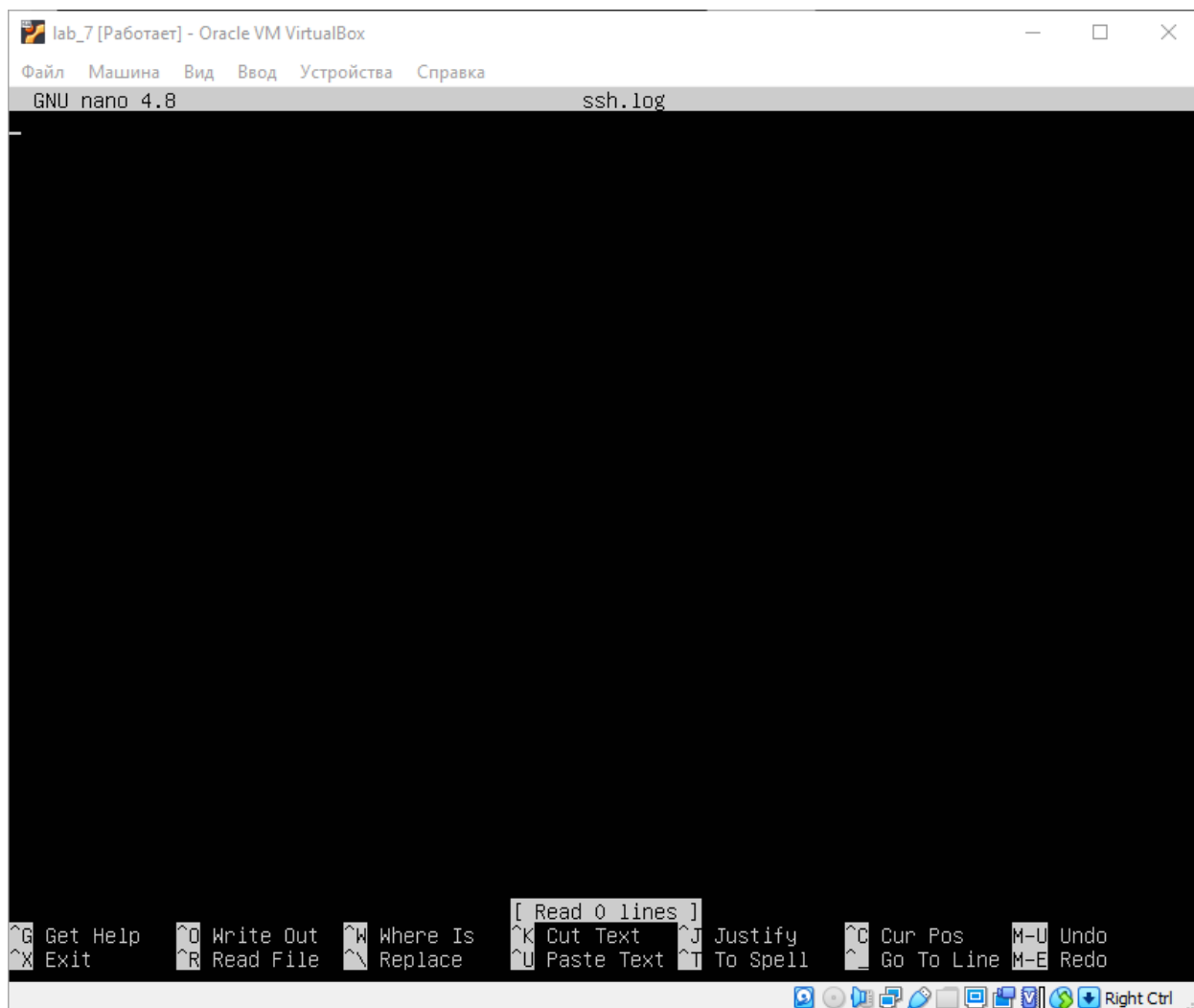


Рисунок 16 – Содержимое файла ssh.log.

Вывод

В ходе выполнения лабораторной работы были изучены основы работы с программным обеспечением удалённого доступа к распределённым системам обработки данных.

Ответы на контрольные вопросы

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.
- 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.

* — значения параметров (высокий, средний, низкий) носят относительный характер и служат только для сравнения показателей.

** — расход ресурсов сервера (процессор, диск, сетевой канал) на обработку запросов, обычно идущих на 22-й порт.

*** – произвести взлом, если для авторизации используются RSA ключи, сложно, однако неограниченное количество попыток авторизации делает это возможным.

**** – количество попыток авторизации ограничено, но серверу приходится обрабатывать их от большого количества злоумышленников.

Конфигурация	Вероятность взлома	Потери от флуда**
22 порт, авторизация по паролю, без защиты	Высокая	Высокие
22 порт, авторизация по ключам, без защиты	Средняя***	Высокие
22 порт, авторизация по ключам, защита на основе ограничения неудачных попыток авторизации	Низкая	Средние****
Нестандартный порт, авторизация по паролю, без защиты	Высокая	Низкие
Нестандартный порт, авторизация по ключам, без защиты	Средняя***	Низкие
Нестандартный порт, авторизация по ключам, защита на основе ограничения неудачных попыток авторизации	Низкая	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.