

# Липецкий государственный технический университет

Кафедра прикладной математики

Отчет по лабораторной работе № 6  
«Авторизация по ключу ssh»  
по курсу «ОС Linux»

Студент

\_\_\_\_\_  
подпись, дата

Гришагин Е.Е.  
\_\_\_\_\_  
фамилия, инициалы

Группа

ПМ-19-2

Руководитель

\_\_\_\_\_  
ученая степень, ученое звание

\_\_\_\_\_  
подпись, дата

Кургасов В.В.  
\_\_\_\_\_  
фамилия, инициалы

Липецк 2022 г.

# Содержание

Задание кафедры	3
1. Ход работы	4
2. Контрольные вопросы	10

# Задание кафедры

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

- IP: 178.234.29.197
- Порт: 22
- Логин: stud2
- Пароль: w549QriOET

# 1. Ход работы

Запуск анализатора трафика tcpdump для telnet и его логирование.

```
excul@exculserver:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee telnet.log
[sudo] password for excul:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
14:31:37.800291 IP (tos 0x10, ttl 64, id 27320, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.39904 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0x042d), seq 10072529
20, win 64240, options [mss 1460,sackOK,TS val 550829463 ecr 0,nop,wscale 7], length 0
14:31:37.854667 IP (tos 0x0, ttl 64, id 35, offset 0, flags [none], proto TCP (6), length 44)
    178.234.29.197.22 > 10.0.2.15.39904: Flags [S.], cksum 0x2d7f (correct), seq 2048001, ack 100725
2921, win 65535, options [mss 1460], length 0
14:31:37.854709 IP (tos 0x10, ttl 64, id 27321, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.39904 > 178.234.29.197.22: Flags [.] , cksum 0xdc8 (incorrect -> 0x4a4b), ack 1, win 6
4240, length 0
14:31:37.915942 IP (tos 0x0, ttl 64, id 36, offset 0, flags [none], proto TCP (6), length 82)
    178.234.29.197.22 > 10.0.2.15.39904: Flags [P.], cksum 0x1eb5 (correct), seq 1:43, ack 1, win 65
535, length 42
14:31:37.915968 IP (tos 0x10, ttl 64, id 27322, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.39904 > 178.234.29.197.22: Flags [.] , cksum 0xdc8 (incorrect -> 0x4a4b), ack 43, win
64198, length 0
```

Рисунок 1 - Запуск анализатора трафика

Запуск telnet.

```
excul@exculserver:~$ 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 2 - Запуск telnet

Запуск анализатора трафика tcpdump для ssh и его логирование.

```
excul@exculserver:~$ 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

Соединение с сервером через ssh при помощи логина и пароля

```
excul@exculserver:~$ ssh -l stud2 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/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.
stud2@edu.kurgasov.ru's password:
Permission denied, please try again.
stud2@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: Fri Jan 28 17:34:26 2022 from 37.112.145.90
stud2@kurgasov:~$ _
```

Рисунок 4 - Соединение с сервером через ssh

Защищённая передача файла с помощью логина и пароля

```
excul@exculserver:~$ scp lr_6.txt stud2@edu.kurgasov.ru:/home/stud2
stud2@edu.kurgasov.ru's password:
lr_6.txt                                100% 33    0.9KB/s  00:00
excul@exculserver:~$
```

Рисунок 5 - Защищённая передача файла

Генерация ssh-ключа для безпарольной аутентификации.

```

excul@exculserver:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/excul/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/excul/.ssh/id_rsa
Your public key has been saved in /home/excul/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:zFAsU6xFdmzdUy317GuTpmxn+JxzCWIrhWUwcb9xk2g excul@exculserver
The key's randomart image is:
+---[RSA 3072]---+
|      ==000 . .|=|
|      00+++ 0 +.=|
|      .= .0  E *0|
|      .+  0. +..|
|      S +   . .|
|      . + .  0|
|      0 0 0*.|
|      . ..0==+|
|      . .0++0|
+-----[SHA256]-----+
excul@exculserver:~$

```

Рисунок 6 - Генерация ssh-ключа

Копирование публичной части сгенерированного ssh-ключа на сервер.

```

excul@exculserver:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud2@edu.kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/excul/.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 already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
stud2@edu.kurgasov.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'stud2@edu.kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.

excul@exculserver:~$ _

```

## Рисунок 7 - Передача ключа на сервер

Соединение с сервером через ssh при помощи логина и ключа.

```
excul@exculserver:~$ ssh -l stud2 kurgasov.ru
The authenticity of host '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 'kurgasov.ru' (ECDSA) to the list of known hosts.
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: Fri Jan 28 17:43:53 2022 from 37.112.145.90
stud2@kurgasov:~$
```

## Рисунок 8 - Соединение с сервером через ssh

Лог telnet.

```
GNU nano 4.8                                telnet.log
14:31:37.800291 IP (tos 0x10, ttl 64, id 27320, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.2.15.39904 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0x042d), seq 1007252
14:31:37.854667 IP (tos 0x0, ttl 64, id 35, offset 0, flags [none], proto TCP (6), length 44)
  178.234.29.197.22 > 10.0.2.15.39904: Flags [S.], cksum 0x2d7f (correct), seq 2048001, ack 10072
14:31:37.854709 IP (tos 0x10, ttl 64, id 27321, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39904 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x4a4b), ack 1, win
14:31:37.915942 IP (tos 0x0, ttl 64, id 36, offset 0, flags [none], proto TCP (6), length 82)
  178.234.29.197.22 > 10.0.2.15.39904: Flags [P.], cksum 0x1eb5 (correct), seq 1:43, ack 1, win 6
14:31:37.915968 IP (tos 0x10, ttl 64, id 27322, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39904 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x4a4b), ack 43, win
14:33:37.915979 IP (tos 0x0, ttl 64, id 38, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39904: Flags [F.], cksum 0x4511 (correct), seq 43, ack 1, win 655
14:33:37.916061 IP (tos 0x10, ttl 64, id 27323, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39904 > 178.234.29.197.22: Flags [F.], cksum 0xdcd8 (incorrect -> 0x4a4a), seq 1, ack
14:33:37.916305 IP (tos 0x0, ttl 64, id 39, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39904: Flags [.], cksum 0x4510 (correct), ack 2, win 65535, lengt
14:34:25.481194 IP (tos 0x0, ttl 64, id 43331, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.2.15.39906 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0x621f), seq 4537491
14:34:25.527274 IP (tos 0x0, ttl 64, id 48, offset 0, flags [none], proto TCP (6), length 44)
  178.234.29.197.22 > 10.0.2.15.39906: Flags [S.], cksum 0x2b78 (correct), seq 18624001, ack 4537
14:34:25.527318 IP (tos 0x0, ttl 64, id 43332, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39906 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x4844), ack 1, win
14:34:25.539597 IP (tos 0x0, ttl 64, id 43333, offset 0, flags [DF], proto TCP (6), length 81)
  10.0.2.15.39906 > 178.234.29.197.22: Flags [P.], cksum 0xdd01 (incorrect -> 0x23eb), seq 1:42,
14:34:25.539868 IP (tos 0x0, ttl 64, id 49, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39906: Flags [.], cksum 0x430c (correct), ack 42, win 65535, lengt
14:34:25.579828 IP (tos 0x0, ttl 64, id 50, offset 0, flags [none], proto TCP (6), length 82)
  178.234.29.197.22 > 10.0.2.15.39906: Flags [P.], cksum 0x1c85 (correct), seq 1:43, ack 42, win
14:34:25.579856 IP (tos 0x0, ttl 64, id 43334, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39906 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x481b), ack 43, win
14:34:25.580319 IP (tos 0x0, ttl 64, id 43335, offset 0, flags [DF], proto TCP (6), length 1552)
  10.0.2.15.39906 > 178.234.29.197.22: Flags [P.], cksum 0xe2c0 (incorrect -> 0x378c), seq 42:155
[ Read 1090 lines ]
```

Рисунок 9 - Лог telnet.

Лог ssh.



```
linux [Работаer] - Oracle VM VirtualBox
GNU nano 4.8 ssh.log
14:33:37.915979 IP (tos 0x0, ttl 64, id 38, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.39904: Flags [F.], cksum 0x4511 (correct), seq 2048044, ack 10072
14:33:37.916061 IP (tos 0x10, ttl 64, id 27323, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.39904 > 178.234.29.197.22: Flags [F.], cksum 0xdcd8 (incorrect -> 0x4a4a), seq 1, ack
14:33:37.916305 IP (tos 0x0, ttl 64, id 39, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.39904: Flags [..], cksum 0x4510 (correct), ack 2, win 65535, lengt
14:34:25.481194 IP (tos 0x0, ttl 64, id 43331, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0x621f), seq 4537491
14:34:25.527274 IP (tos 0x0, ttl 64, id 48, offset 0, flags [none], proto TCP (6), length 44)
    178.234.29.197.22 > 10.0.2.15.39906: Flags [S.], cksum 0x2b78 (correct), seq 18624001, ack 4537
14:34:25.527318 IP (tos 0x0, ttl 64, id 43332, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [..], cksum 0xdcd8 (incorrect -> 0x4844), ack 1, win
14:34:25.539597 IP (tos 0x0, ttl 64, id 43333, offset 0, flags [DF], proto TCP (6), length 81)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [P.], cksum 0xdd01 (incorrect -> 0x23eb), seq 1:42,
14:34:25.539868 IP (tos 0x0, ttl 64, id 49, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.39906: Flags [..], cksum 0x430c (correct), ack 42, win 65535, leng
14:34:25.579828 IP (tos 0x0, ttl 64, id 50, offset 0, flags [none], proto TCP (6), length 82)
    178.234.29.197.22 > 10.0.2.15.39906: Flags [P.], cksum 0x1c85 (correct), seq 1:43, ack 42, win
14:34:25.579856 IP (tos 0x0, ttl 64, id 43334, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [..], cksum 0xdcd8 (incorrect -> 0x481b), ack 43, win
14:34:25.580319 IP (tos 0x0, ttl 64, id 43335, offset 0, flags [DF], proto TCP (6), length 1552)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [P.], cksum 0xe2c0 (incorrect -> 0x378c), seq 42:155
14:34:25.580594 IP (tos 0x0, ttl 64, id 51, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.39906: Flags [..], cksum 0x3d2e (correct), ack 1502, win 65535, le
14:34:25.580594 IP (tos 0x0, ttl 64, id 52, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.39906: Flags [..], cksum 0x3cfa (correct), ack 1554, win 65535, le
14:34:25.626896 IP (tos 0x0, ttl 64, id 53, offset 0, flags [none], proto TCP (6), length 1016)
    178.234.29.197.22 > 10.0.2.15.39906: Flags [P.], cksum 0x6733 (correct), seq 43:1019, ack 1554,
14:34:25.626924 IP (tos 0x0, ttl 64, id 43337, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [..], cksum 0xdcd8 (incorrect -> 0x4159), ack 1019, w
14:34:25.630294 IP (tos 0x0, ttl 64, id 43338, offset 0, flags [DF], proto TCP (6), length 88)
    10.0.2.15.39906 > 178.234.29.197.22: Flags [P.], cksum 0xdd08 (incorrect -> 0x0ec9), seq 1554:1
14:34:25.630633 IP (tos 0x0, ttl 64, id 54, offset 0, flags [none], proto TCP (6), length 40)
```

Рисунок 10 - Лог ssh.

## 2. Контрольные вопросы

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

Ответ: 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. Вопрос: Выделите отличительные особенности между режимами работы удаленного доступа по протоколам TELNET и SSH?

Ответ:

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

Ответ:

- 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.

•

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

Ответ: 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. Вопрос: Перечислите распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH? Приведите пример использования службы передачи файлов по безопас-

ному туннелю?

Ответ: 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.