

Липецкий государственный технический университет

Кафедра прикладной математики

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

Студент

подпись, дата

Богомолов Е.А.
фамилия, инициалы

Группа

Руководитель

Доцент, к. пед. наук
ученая степень, ученое звание

подпись, дата

Кургасов В.В.
фамилия, инициалы

Липецк 2021 г.

Содержание

Цель работы	3
1. Ход работы	4
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. Запуск анализатора трафика tcpdump (порт 22)	8
1.6. Установление шифрованного соединения с удаленным сервером	9
1.7. Вывод информации об удаленной системе	10
1.8. Передача файла по шифрованному каналу	11
1.9. Формирование зашифрованных ключей	12
1.10. Передача публичного ключа	13
1.11. Подключение к удаленной системе	14
1.12. Передача файла по шифрованному каналу	15
1.13. Содержимое файла telnet.log	16
1.14. Содержимое файла ssh.log	17
Выводы	18
Контрольные вопросы	19

Цель работы

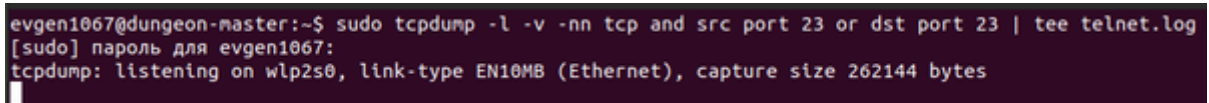
Организовать доступ к удаленному серверу по ssh (без ввода пароля (по ключу)) имея следующие исходные данные:

- IP: 178.234.29.197
- Порт: 22
- Логин: stud1
- Пароль: kfM4Uz7cqW

1. Ход работы

1.1. 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)

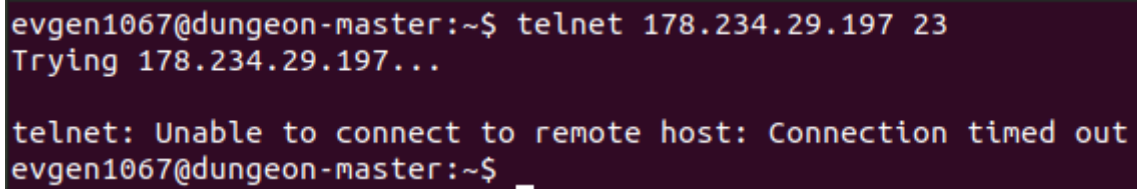


```
evgen1067@dungeon-master:~$ sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log
[sudo] пароль для evgen1067:
tcpdump: listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Рисунок 1 – Запуск анализатора трафика tcpdump.

1.2. Попытка установки соединения (порт 23)

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

A terminal window with a dark purple background. The text is in a monospaced font. The first line shows the user 'evgen1067' at the host 'dungeon-master' in the directory '~' typing 'telnet 178.234.29.197 23'. The second line shows the output 'Trying 178.234.29.197...'. The third line shows the error message 'telnet: Unable to connect to remote host: Connection timed out'. The fourth line shows the prompt 'evgen1067@dungeon-master:~\$' followed by a cursor.

```
evgen1067@dungeon-master:~$ telnet 178.234.29.197 23
Trying 178.234.29.197...

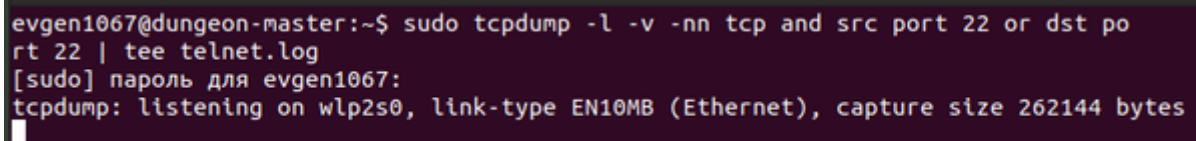
telnet: Unable to connect to remote host: Connection timed out
evgen1067@dungeon-master:~$
```

Рисунок 2 – Попытка установки соединения.

23 порт недоступен, нет возможности подключиться к серверу удалённо.

1.3. 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 telnet.log`
(запуск анализатора трафика и сохранение данных в файл)

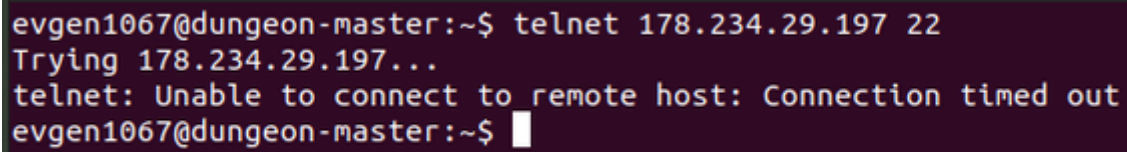


```
evgen1067@dungeon-master:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst po  
rt 22 | tee telnet.log  
[sudo] пароль для evgen1067:  
tcpdump: listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Рисунок 3 – Запуск анализатора трафика tcpdump.

1.4. Попытка установки соединения (порт 22)

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

A terminal window with a dark purple background. The text is as follows:

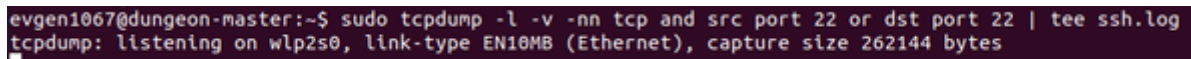
```
evgen1067@dungeon-master:~$ telnet 178.234.29.197 22
Trying 178.234.29.197...
telnet: Unable to connect to remote host: Connection timed out
evgen1067@dungeon-master:~$
```

Рисунок 4 – Попытка установки соединения.

22 порт недоступен, нет возможности подключиться к серверу удалённо.

1.5. 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)

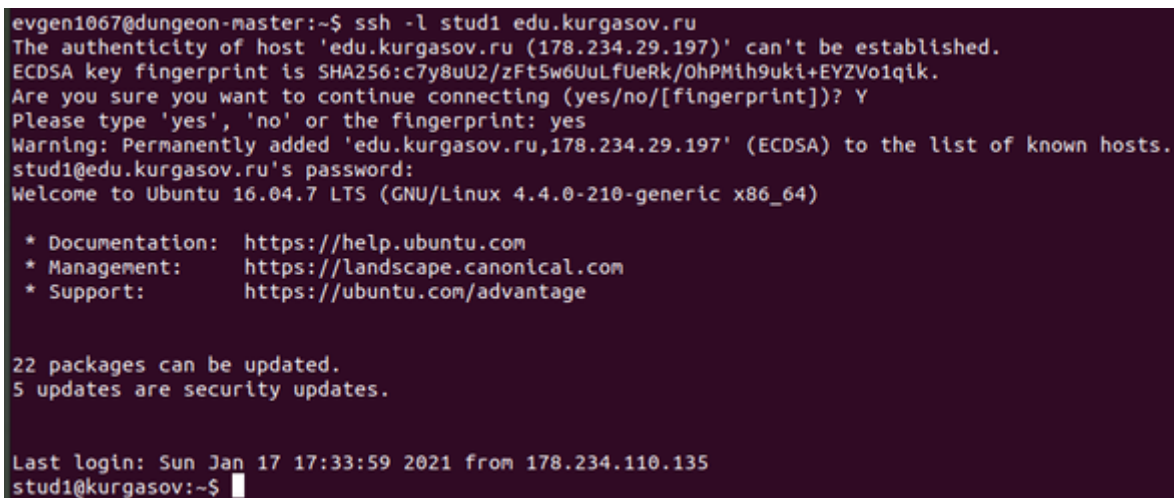


```
evgen1067@dungeon-master:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log
tcpdump: listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Рисунок 5 – Запуск анализатора трафика.

1.6. Установление шифрованного соединения с удаленным сервером

- `ssh -l stud1 edu.kurgasov.ru`



```
evgen1067@dungeon-master:~$ ssh -l stud1 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])? 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.
stud1@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

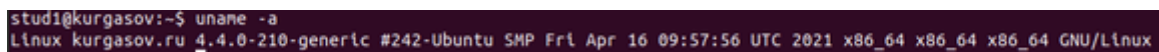
22 packages can be updated.
5 updates are security updates.

Last login: Sun Jan 17 17:33:59 2021 from 178.234.110.135
stud1@kurgasov:~$
```

Рисунок 6 – Установление шифрованного соединения.

1.7. Вывод информации об удаленной системе

- `uname -a`

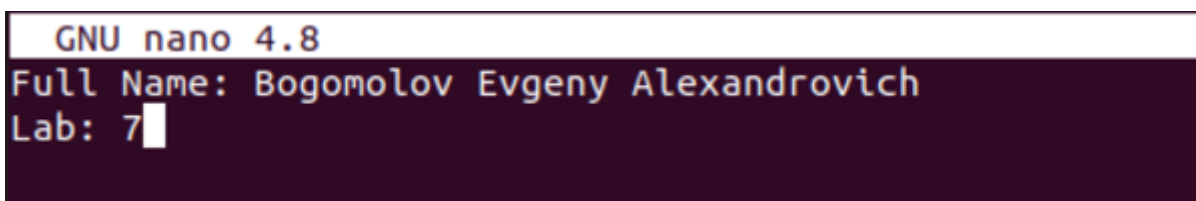
A terminal window with a dark background. The prompt is 'stud1@kurgasov:~\$'. The command 'uname -a' has been entered and executed. The output is displayed on the next line: 'Linux kurgasov.ru 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux'.

```
stud1@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
```

Рисунок 7 – Вывод информации об удаленной системе.

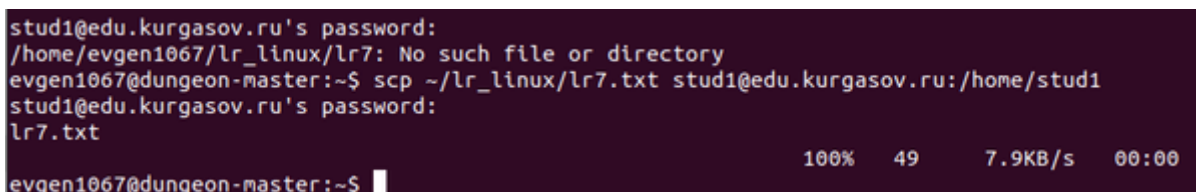
1.8. Передача файла по зашифрованному каналу

- Ctrl-b c
- nano lr7.txt
- scp -v -o /lr_linux/lr7.txt stud1@edu.kurgasov.ru:/home/stud1



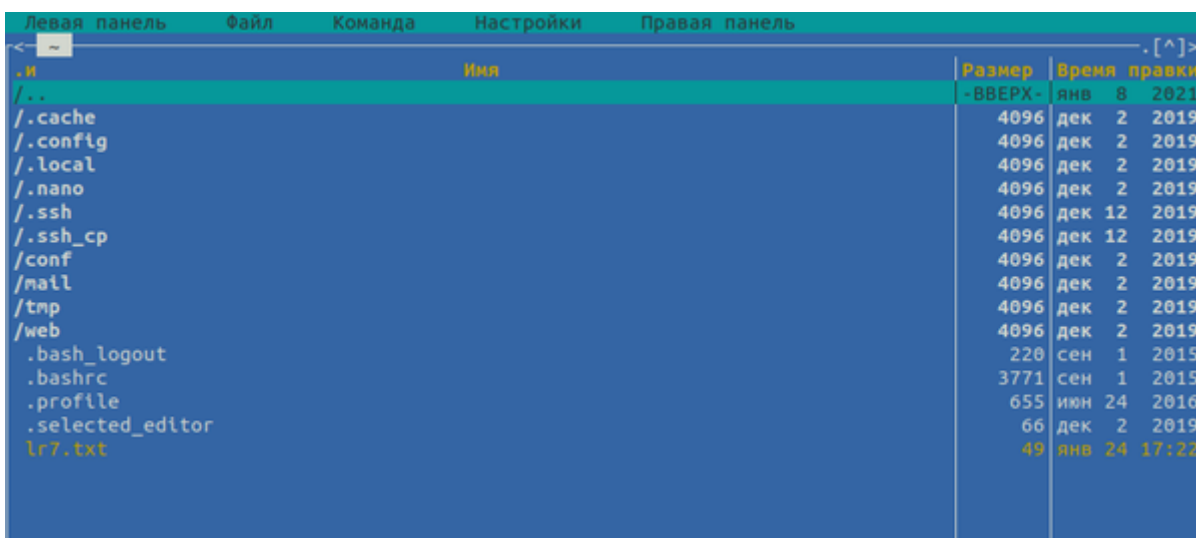
```
GNU nano 4.8
Full Name: Bogomolov Evgeny Alexandrovich
Lab: 7
```

Рисунок 8 – Содержимое файла lr7.txt.



```
stud1@edu.kurgasov.ru's password:
/home/evgen1067/lr_linux/lr7: No such file or directory
evgen1067@dungeon-master:~$ scp ~/lr_linux/lr7.txt stud1@edu.kurgasov.ru:/home/stud1
stud1@edu.kurgasov.ru's password:
lr7.txt
100% 49 7.9KB/s 00:00
evgen1067@dungeon-master:~$
```

Рисунок 9 – Передача файла по зашифрованному каналу.



Имя	Размер	Время	Правки
..	-	ВВЕРХ	-
./cache	4096	дек 2 2019	
./config	4096	дек 2 2019	
./local	4096	дек 2 2019	
./nano	4096	дек 2 2019	
./ssh	4096	дек 12 2019	
./ssh_cp	4096	дек 12 2019	
./conf	4096	дек 2 2019	
./mail	4096	дек 2 2019	
./tmp	4096	дек 2 2019	
./web	4096	дек 2 2019	
./bash_logout	220	сен 1 2015	
./bashrc	3771	сен 1 2015	
./profile	655	июн 24 2016	
./selected_editor	66	дек 2 2019	
lr7.txt	49	янв 24 17:22	

Рисунок 10 – Проверка наличия копии файла.

1.9. Формирование зашифрованных ключей

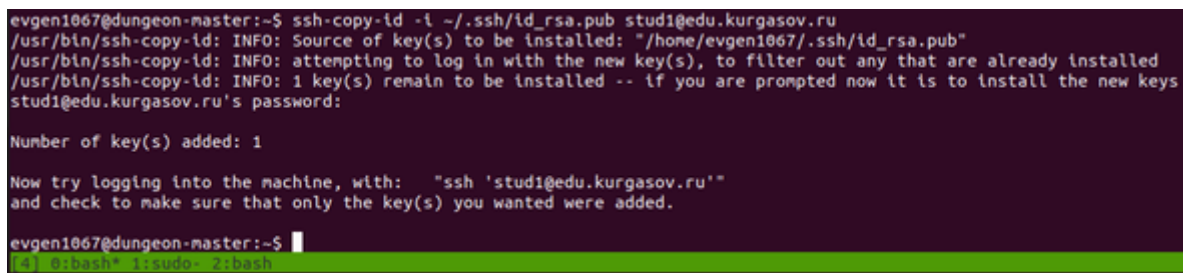
- exit (выход)
- ssh-keygen (формирование зашифрованных ключей)

```
evgen1067@dungeon-master:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/evgen1067/.ssh/id_rsa):
/home/evgen1067/.ssh/id_rsa already exists.
Overwrite (y/n)? Y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/evgen1067/.ssh/id_rsa
Your public key has been saved in /home/evgen1067/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:XsMTKdppoZwImDSjE9pR5TAuAIVMHKHz3BrDn8+LNDw evgen1067@dungeon-master
The key's randomart image is:
+---[RSA 3072]-----+
|OX=+.+.|
|*Ooo +. |
|O + . . o o|
| * + o = = .|
| * o = S =|
| * . o . o|
|. E .|
|. *|
|. +.|
+-----[SHA256]-----+
evgen1067@dungeon-master:~$
```

Рисунок 11 – Формирование зашифрованных ключей

1.10. Передача публичного ключа

- `ssh-copy-id -i ~/.ssh/id_rsa.pub stud1@kurgasov.ru`



```
evgen1067@dungeon-master:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud1@edu.kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/evgen1067/.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
stud1@edu.kurgasov.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud1@edu.kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.

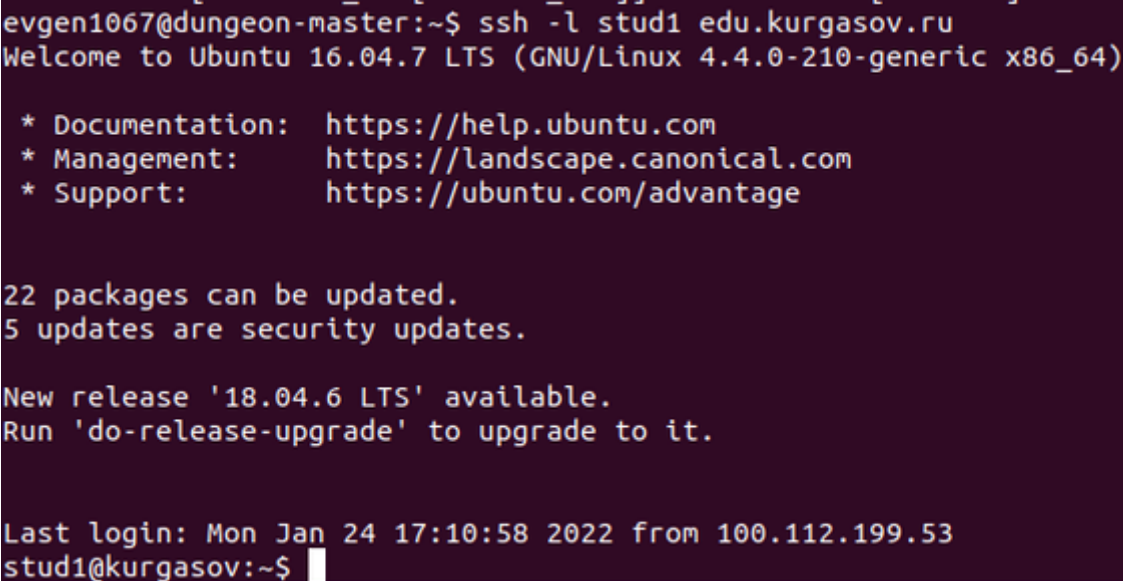
evgen1067@dungeon-master:~$
```

Рисунок 12 – Передача публичного ключа

1.11. Подключение к удаленной системе

- `ssh -l stud1 kurgasov.ru`

Благодаря ssh пароль при входе не потребовался.



```
evgen1067@dungeon-master:~$ ssh -l stud1 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.

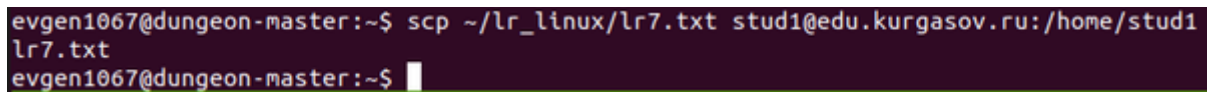
Last login: Mon Jan 24 17:10:58 2022 from 100.112.199.53
stud1@kurgasov:~$
```

Рисунок 13 – Подключение к удаленной системе.

1.12. Передача файла по зашифрованному каналу

- `scp -v -o /lr_linux/lr7.txt stud1@edu.kurgasov.ru:/home/stud1`

Благодаря ssh пароль не понадобился.



```
evgen1067@dungeon-master:~$ scp -v -o /lr_linux/lr7.txt stud1@edu.kurgasov.ru:/home/stud1
lr7.txt
evgen1067@dungeon-master:~$
```

Рисунок 14 – Передача файла по зашифрованному каналу.

1.13. Содержимое файла telnet.log

- nano telnet.log

Рисунок 15 – Содержимое файла telnet.log.

1.14. Содержимое файла ssh.log

- nano ssh.log

```
Ctrl nano 4.8 ssh.log
17:09:59.064554 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [S], cksum 0xc6e0d (correct), seq 3728998832, win 64240, options [max 1400,sackOK,TS val 837682427 ecr 0,nop,wscale 7], length 0
17:09:59.069982 IP (tos 0x0, ttl 59, id 3677, offset 0, flags [DF], proto TCP (6), length 60)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [S-], cksum 0xc5c6d (correct), seq 2372632793, ack 3728998833, win 28960, options [max 1400,sackOK,TS val 34376493 ecr 837682427,nop,wscale 7], length 0
17:09:59.070058 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [S-], cksum 0xc7782 (correct), ack 1, win 582, options [nop,nop,TS val 837682433 ecr 34376493], length 0
17:09:59.087324 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 93)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0x4338 (correct), seq 1:42, ack 1, win 582, options [nop,nop,TS val 837682450 ecr 34376493], length 41
17:09:59.095032 IP (tos 0x0, ttl 59, id 3676, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [S-], cksum 0xc855 (correct), ack 42, win 227, options [nop,nop,TS val 34376499 ecr 837682450], length 0
17:09:59.093802 IP (tos 0x0, ttl 59, id 3677, offset 0, flags [DF], proto TCP (6), length 94)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [P-], cksum 0xc4b5 (correct), seq 1:43, ack 42, win 227, options [nop,nop,TS val 34376524 ecr 837682450], length 42
17:09:59.093839 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [S-], cksum 0xc095 (correct), ack 43, win 582, options [nop,nop,TS val 837682556 ecr 34376524], length 0
17:09:59.094072 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 1448)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [S-], cksum 0xc1ab6 (correct), seq 42:1430, ack 43, win 582, options [nop,nop,TS val 837682557 ecr 34376524], length 1388
17:09:59.094286 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 176)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc0f5 (correct), seq 2430:1554, ack 43, win 582, options [nop,nop,TS val 837682557 ecr 34376524], length 124
17:10:00.000347 IP (tos 0x0, ttl 59, id 3676, offset 0, flags [DF], proto TCP (6), length 1828)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [P-], cksum 0xc4eef (correct), seq 43:1019, ack 42, win 227, options [nop,nop,TS val 34376526 ecr 837682556], length 976
17:10:00.000383 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [S-], cksum 0xc1cd0 (correct), ack 1019, win 581, options [nop,nop,TS val 837682563 ecr 34376526], length 0
17:10:00.002265 IP (tos 0x0, ttl 59, id 3679, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [S-], cksum 0xc1d06 (correct), ack 5554, win 250, options [nop,nop,TS val 34376526 ecr 837682557], length 0
17:10:00.006062 IP (tos 0x0, ttl 64, id 43877, offset 0, flags [DF], proto TCP (6), length 108)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc3d81 (correct), seq 1554:1602, ack 1019, win 581, options [nop,nop,TS val 837682569 ecr 34376526], length 48
17:10:00.011737 IP (tos 0x0, ttl 59, id 3680, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [S-], cksum 0xc5d98 (correct), ack 1602, win 250, options [nop,nop,TS val 34376528 ecr 837682569], length 0
17:10:00.022304 IP (tos 0x0, ttl 59, id 3682, offset 0, flags [DF], proto TCP (6), length 433)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [P-], cksum 0xc02a6 (correct), seq 1019:1383, ack 1602, win 250, options [nop,nop,TS val 34376531 ecr 837682569], length 364
17:10:00.022327 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [S-], cksum 0xc1b1e (correct), ack 1383, win 581, options [nop,nop,TS val 837682585 ecr 34376531], length 0
17:10:00.028032 IP (tos 0x0, ttl 64, id 43878, offset 0, flags [DF], proto TCP (6), length 68)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc2af6 (correct), seq 1602:1618, ack 1383, win 581, options [nop,nop,TS val 837692291 ecr 34376531], length 16
17:10:00.0771349 IP (tos 0x0, ttl 59, id 3682, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [S-], cksum 0xc2c99 (correct), ack 1618, win 250, options [nop,nop,TS val 34378969 ecr 837692291], length 0
17:10:00.0771399 IP (tos 0x0, ttl 64, id 43880, offset 0, flags [DF], proto TCP (6), length 90)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc4af9 (correct), seq 1018:1602, ack 1383, win 581, options [nop,nop,TS val 837692334 ecr 34378969], length 44
17:10:00.0777164 IP (tos 0x0, ttl 59, id 3683, offset 0, flags [DF], proto TCP (6), length 52)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [S-], cksum 0xc15ed (correct), seq 1383:1427, ack 1602, win 250, options [nop,nop,TS val 34378970 ecr 837692334], length 0
17:10:00.0777191 IP (tos 0x0, ttl 59, id 3684, offset 0, flags [DF], proto TCP (6), length 90)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc1d14 (correct), ack 1427, win 250, options [nop,nop,TS val 34378970 ecr 837692334], length 0
17:10:00.0777356 IP (tos 0x0, ttl 64, id 43882, offset 0, flags [DF], proto TCP (6), length 128)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc1c75 (correct), seq 1602:1730, ack 1427, win 581, options [nop,nop,TS val 837692340 ecr 34378970], length 68
17:10:00.0783698 IP (tos 0x0, ttl 59, id 3685, offset 0, flags [DF], proto TCP (6), length 104)
    178.234.29.197.22 > 192.168.0.13.55752: Flags [P-], cksum 0xc7f8b (correct), seq 1427:1479, ack 1730, win 250, options [nop,nop,TS val 34378972 ecr 837692340], length 52
17:10:00.0783915 IP (tos 0x0, ttl 64, id 43883, offset 0, flags [DF], proto TCP (6), length 552)
    192.168.0.13.55752 > 178.234.29.197.22: Flags [P-], cksum 0xc31f4 (correct), seq 1730:2230, ack 1479, win 581, options [nop,nop,TS val 837692346 ecr 34378972], length 500
    [Report:map.1378.ctp:0]
```

Рисунок 16 – 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?

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.