

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

ЛАБОРАТОРНАЯ РАБОТА №7
по Операционной системе Linux
Работа с SSH

Студент

Фетисов В. Д.

Группа ПИ-19

Руководитель

Кургасов В.В.

Доцент, к.п.н.

Липецк 2022 г.

Оглавление

Цель работы	3
Задание.....	3
Ход работы	5
Вывод.....	12
Контрольные вопросы.....	13

Цель работы

Лабораторная работа предназначена для целей практического ознакомления с программным обеспечением удаленного 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.

Необходимые для выполнения практического задания

IP 178.234.29.197 порт 22 Логин: stud11 Пароль: F0Cp4uRfSo

Ход работы

1) Запуск анализатора трафика tcpdump (порт 23)

- tmux (терминальный мультиплексор)
- Ctrl-b c (создание нового окна, автоматически переключается на него)
- 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
```



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

Рисунок 1 – Запуск анализатора трафика tcpdump

2) Попытка установки соединения (порт 23)

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

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

[0] 0: bash* 1: sudo-

"vlad" 22:55 25-января-22

Рисунок 2 – Попытка установки соединения

23 порт недоступен, нет возможности подключиться к серверу удалённо.

3) Запуск анализатора трафика tcpdump (порт 22)

- tmux (терминальный мультиплексор)
- Ctrl-b c (создание нового окна, и переключение на него)
- 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
```

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

```
[0] 0: bash- 1: sudo 2: sudo*
```

```
"vlad" 23:00 25-янв-20
```

Рисунок 3 – Запуск анализатора трафика tcpdump

4) Попытка установки соединения (порт 22)

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

```
vlad@vlad:~$ 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
Connection closed by foreign host.
vlad@vlad:~$ _
```

g

Рисунок 4 – Попытка установки соединения

Подключение удалось.

5) Запуск анализатора трафика tcpdump (порт 22)

- tmux (терминальный мультиплексор)
- Ctrl-b c (создание нового окна, и переключение на него)
- sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log

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

[0] 0: bash- 1: sudo 2: sudo 3: sudo* "vlad" 07:14 26-января-22
```

Рисунок 5 – Запуск анализатора трафика

6) Установление шифрованного соединения с удаленным сервером

- `ssh -l stud11 edu.kurgasov.ru`

```
vlad@vlad:~$ ssh -l stud11 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/DhPMih9uki+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.
stud11@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 19:05:46 2022 from 176.59.172.220
stud11@kurgasov:~$
```

Рисунок 6 – Установление шифрованного соединения

7) Вывод информации об удаленной системе

- `uname -a`


```
stud11@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
stud11@kurgasov:~$
```

Рисунок 7 – Вывод информации об удаленной системе.

8) Передача файла по зашифрованному каналу

- Ctrl-b c
- nano labrab7.txt
- scp home/vlad/labrab7.txt stud11@edu.kurgasov.ru:/home/stud11

```
GNU nano 4.8 labrab7.txt
My FIO: Fetisov Vladislav Denisovich
Labrab: 7
```

Рисунок 8 – Содержимое файла labrab7.txt

```
vlad@vlad:~$ scp /home/vlad/labrab7.txt stud11@edu.kurgasov.ru:/home/stud11
stud11@edu.kurgasov.ru's password:
labrab7.txt                                100% 47    5.8KB/s  00:00
vlad@vlad:~$
```

Рисунок 9 – Передача файла по зашифрованному каналу

```
vlad@vlad:~$ ssh -l stud11 edu.kurgasov.ru
stud11@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: Wed Jan 26 10:18:17 2022 from 178.234.57.36
stud11@kurgasov:~$ ls
conf  lab7  lab7_1  labrab7.txt  mail  tmp  web
stud11@kurgasov:~$
```

Рисунок 10 – Проверка наличия копии файла

9) Формирование зашифрованных ключей

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

```

stud11@kurgasov:~$ exit
ВЫХОД
Connection to edu.kurgasov.ru closed.
vlad@vlad:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vlad/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/vlad/.ssh/id_rsa
Your public key has been saved in /home/vlad/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:UfDCf6/d9K0+UrsDRj/J94Sptg4FMw6dQ90uckKues vlad@vlad
The key's randomart image is:
+---[RSA 3072]-----+
|
|  . . .
|  . o o .
|  . + 0 . o
|    o o = . .
|    S + B oo
|      * @0..
|     = o.*.o
|    =o* +o|
|    .E+B**+|
+-----[SHA256]-----+
vlad@vlad:~$

```

Рисунок 11 – Формирование зашифрованных ключей

10) Передача публичного ключа

- `ssh-copy-id -i /home/vlad/.ssh/id_rsa.pub stud11@kurgasov.ru`

```

vlad@vlad:~$ ssh-copy-id -i /home/vlad/.ssh/id_rsa.pub stud11@kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/vlad/.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/OhPMih9uki+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
stud11@kurgasov.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud11@kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.
vlad@vlad:~$

```

Рисунок 12 – Передача публичного ключа

11) Подключение к удаленной системе

- `ssh -l stud11 edu.kurgasov.ru`

Благодаря ssh пароль при входе не потребовался.

```

vlad@vlad:~$ ssh -l stud11 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 10:41:07 2022 from 178.234.57.36
stud11@kurgasov:~$

```

Рисунок 13 – Подключение к удаленной системе.

12) Передача файла по зашифрованному каналу

- `scp /home/vlad/labrab7.txt stud11@edu.kurgasov.ru:/home/stud11`

Благодаря ssh пароль не понадобился.

```

vlad@vlad:~$ scp /home/vlad/labrab7.txt stud11@edu.kurgasov.ru:/home/stud11
labrab7.txt                                100% 47      6.4KB/s   00:00
vlad@vlad:~$

```

Рисунок 14 – Передача файла по зашифрованному каналу

13) Содержимое файла telnet.log

- `nano telnet.log`

```

178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x69c8 (correct), seq 4051:4087, ack 316>
07:22:48.991639 IP (tos 0x10, ttl 64, id 52696, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcd8 (incorrect -> 0x2a28), ack 4087, w>
07:22:48.993230 IP (tos 0x0, ttl 64, id 5511, offset 0, flags [none], proto TCP (6), length 164)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0xf51e (correct), seq 4087:4211, ack 316>
07:22:48.993243 IP (tos 0x10, ttl 64, id 52697, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcd8 (incorrect -> 0x29ac), ack 4211, w>
07:22:48.993437 IP (tos 0x0, ttl 64, id 5512, offset 0, flags [none], proto TCP (6), length 100)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x19dd (correct), seq 4211:4271, ack 316>
07:22:48.993442 IP (tos 0x10, ttl 64, id 52698, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcd8 (incorrect -> 0x2970), ack 4271, w>
07:24:15.411306 IP (tos 0x10, ttl 64, id 52699, offset 0, flags [DF], proto TCP (6), length 76)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcdc (incorrect -> 0xf61a), seq 3162:3>
07:24:15.411669 IP (tos 0x0, ttl 64, id 5513, offset 0, flags [none], proto TCP (6), length 40)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x211d (correct), ack 3198, win 65535, le>
07:24:15.418697 IP (tos 0x0, ttl 64, id 5514, offset 0, flags [none], proto TCP (6), length 76)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x1027 (correct), seq 4271:4307, ack 319>
07:24:15.418715 IP (tos 0x10, ttl 64, id 52700, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcd8 (incorrect -> 0x2928), ack 4307, w>
07:24:15.603197 IP (tos 0x10, ttl 64, id 52701, offset 0, flags [DF], proto TCP (6), length 76)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcdc (incorrect -> 0xf429), seq 3198:3>
07:24:15.603531 IP (tos 0x0, ttl 64, id 5515, offset 0, flags [none], proto TCP (6), length 40)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x20d5 (correct), ack 3234, win 65535, le>
07:24:15.610936 IP (tos 0x0, ttl 64, id 5516, offset 0, flags [none], proto TCP (6), length 76)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0xc741 (correct), seq 4307:4343, ack 323>
07:24:15.610951 IP (tos 0x10, ttl 64, id 52702, offset 0, flags [DF], proto TCP (6), length 40)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcd8 (incorrect -> 0x28e0), ack 4343, w>
07:24:16.313175 IP (tos 0x10, ttl 64, id 52703, offset 0, flags [DF], proto TCP (6), length 76)
10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdcdc (incorrect -> 0x09ff), seq 3234:3>
07:24:16.313444 IP (tos 0x0, ttl 64, id 5517, offset 0, flags [none], proto TCP (6), length 40)
178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x208d (correct), ack 3270, win 65535, le>
07:24:16.322630 IP (tos 0x0, ttl 64, id 5518, offset 0, flags [none], proto TCP (6), length 76)

```

Рисунок 15 – Содержимое файла telnet.log

14) Содержимое файла ssh.log

- nano ssh.log

```
07:17:36.982428 IP (tos 0x0, ttl 64, id 52633, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0x67c2), seq 8288269>
07:17:36.989750 IP (tos 0x0, ttl 64, id 5447, offset 0, flags [none], proto TCP (6), length 44)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [S.], cksum 0x268b (correct), seq 33088001, ack 8288>
07:17:36.989783 IP (tos 0x0, ttl 64, id 52634, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [L], cksum 0xdcd8 (incorrect -> 0x4357), ack 1, win >
07:17:36.990245 IP (tos 0x0, ttl 64, id 52635, offset 0, flags [DF], proto TCP (6), length 81)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdd01 (incorrect -> 0x1efe), seq 1:42, >
07:17:36.990482 IP (tos 0x0, ttl 64, id 5448, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [L], cksum 0x3e1f (correct), ack 42, win 65535, leng>
07:17:37.003755 IP (tos 0x0, ttl 64, id 5449, offset 0, flags [none], proto TCP (6), length 82)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x1798 (correct), seq 1:43, ack 42, win >
07:17:37.003766 IP (tos 0x0, ttl 64, id 52636, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [L], cksum 0xdcd8 (incorrect -> 0x432e), ack 43, win>
07:17:37.003904 IP (tos 0x0, ttl 64, id 52637, offset 0, flags [DF], proto TCP (6), length 1552)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xe2c0 (incorrect -> 0xc3c7), seq 42:155>
07:17:37.004979 IP (tos 0x0, ttl 64, id 5450, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [L], cksum 0x3841 (correct), ack 1502, win 65535, le>
07:17:37.004979 IP (tos 0x0, ttl 64, id 5451, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [L], cksum 0x380d (correct), ack 1554, win 65535, le>
07:17:37.011370 IP (tos 0x0, ttl 64, id 5452, offset 0, flags [none], proto TCP (6), length 1016)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x0810 (correct), seq 43:1019, ack 1554,>
07:17:37.011381 IP (tos 0x0, ttl 64, id 52639, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [L], cksum 0xdcd8 (incorrect -> 0x3c6c), ack 1019, w>
07:17:37.013484 IP (tos 0x0, ttl 64, id 52640, offset 0, flags [DF], proto TCP (6), length 88)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [P.], cksum 0xdd08 (incorrect -> 0x2f11), seq 1554:1>
07:17:37.013704 IP (tos 0x0, ttl 64, id 5453, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [L], cksum 0x340d (correct), ack 1602, win 65535, le>
07:17:37.029145 IP (tos 0x0, ttl 64, id 5454, offset 0, flags [none], proto TCP (6), length 404)
  178.234.29.197.22 > 10.0.2.15.39440: Flags [P.], cksum 0x8bc6 (correct), seq 1019:1383, ack 160>
07:17:37.029163 IP (tos 0x0, ttl 64, id 52641, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.39440 > 178.234.29.197.22: Flags [L], cksum 0xdcd8 (incorrect -> 0x3ad0), ack 1383, w>
[ Read 1716 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
```

Рисунок 16 – Содержимое файла ssh.log.

Вывод

Ознакомился на практике с программным обеспечением удаленного доступа к распределённым системам обработки данных.

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. Особенно пригодится эта функция 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 пр. 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. Применяется он и для дистанционного обучения в образовательных учреждениях.

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

Серверный процесс службы telnet по-умолчанию ожидает соединений на TCP-порту 23. Следует отметить, что протокол TELNET не имеет встроенной поддержки шифрования и является критически уязвимым к проведению любых видов сетевых атак.

В отличие от службы telnet, протокол SSH предоставляет шифрованное транспортное соединение к удаленной системе обработки данных. Передаваемая информация подвергается симметричному блочному шифрованию, с использованием одного из стойких алгоритмов шифрования — Blowfish или Triple DES (3DES). Особенностью работы протокола SSH является создание частного и публичного зашифрованных ключей. В процессе установления соединения и проверки подключения, удаленные узлы обмениваются публичными ключами, подтверждая т. о. свою подлинность. Серверный процесс ожидает подключений на TCP-порту 22.

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

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

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

** — имеется ввиду расход ресурсов сервера (процессор, диск, сетевой канал и т.п.) на обработку лавины запросов, обычно идущих на 22-й порт.

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

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

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

Повсюду где нужно получить доступ к компьютеру удаленно. Командировки, работа/учеба дистанционно, фриланс.

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.

Использовать службы передачи файлов по безопасному туннелю можно использовать для передачи паролей, зарплат и любой другой информации, которую хотите безопасно передать.