

Липецкий государственный технический университет

Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №6

по дисциплине «Операционная система Linux»

Авторизация по ключу ssh

Студент

Титов В. А.

Группа АС-20

Руководитель

Кургасов В. В.

к.п.н.

Липецк 2022 г.

Цель работы

Лабораторная работа предназначена для целей практического ознакомления с программным обеспечением удаленного доступа к распределённым системам обработки данных.

Ход работы

1. Запуск анализатора трафика tcpdump на 23 порту

1) Устанавливаем терминальный мультиплексор – tmux

```
root@debian:/home/vlad# apt install tmux
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Уже установлен пакет tmux самой новой версии (3.1c-1+deb11u1).
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не об
новлено.
root@debian:/home/vlad#
```

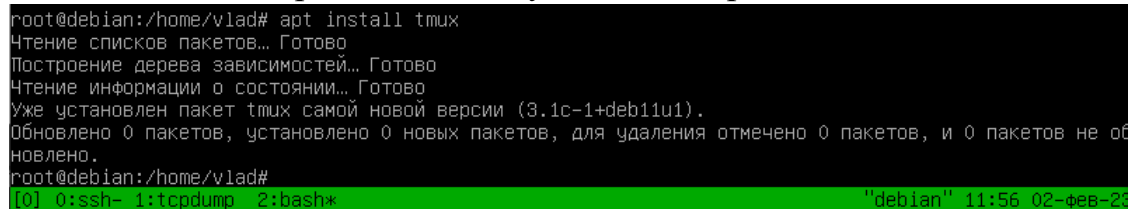


Рис.1. Установка tmux

2) Устанавливаем анализатор трафика – tcpdump

```
root@debian:/home/vlad# apt install tcpdump
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libpcap0.8
Следующие НОВЫЕ пакеты будут установлены:
  libpcap0.8 tcpdump
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не об
новлено.
Необходимо скачать 625 кВ архивов.
После данной операции объём занятого дискового пространства возрастёт на 1 744 кВ.
Хотите продолжить? [Д/н] д
Пол:1 http://deb.debian.org/debian bullseye/main amd64 libpcap0.8 amd64 1.10.0-2 [159 kB]
Пол:2 http://deb.debian.org/debian bullseye/main amd64 tcpdump amd64 4.99.0-2+deb11u1 [466 kB]
Получено 625 кВ за 7с (93,9 kB/s)
Выбор ранее не выбранного пакета libpcap0.8:amd64.
(Чтение базы данных ... на данный момент установлено 35244 файла и каталога.)
Подготовка к распаковке .../libpcap0.8_1.10.0-2_amd64.deb ...
Распаковывается libpcap0.8:amd64 (1.10.0-2) ...
Выбор ранее не выбранного пакета tcpdump.
Подготовка к распаковке .../tcpdump_4.99.0-2+deb11u1_amd64.deb ...
Распаковывается tcpdump (4.99.0-2+deb11u1) ...
Настраивается пакет libpcap0.8:amd64 (1.10.0-2) ...
Настраивается пакет tcpdump (4.99.0-2+deb11u1) ...
Обрабатываются триггеры для man-db (2.9.4-2) ...
Обрабатываются триггеры для libc-bin (2.31-13+deb11u5) ...
```

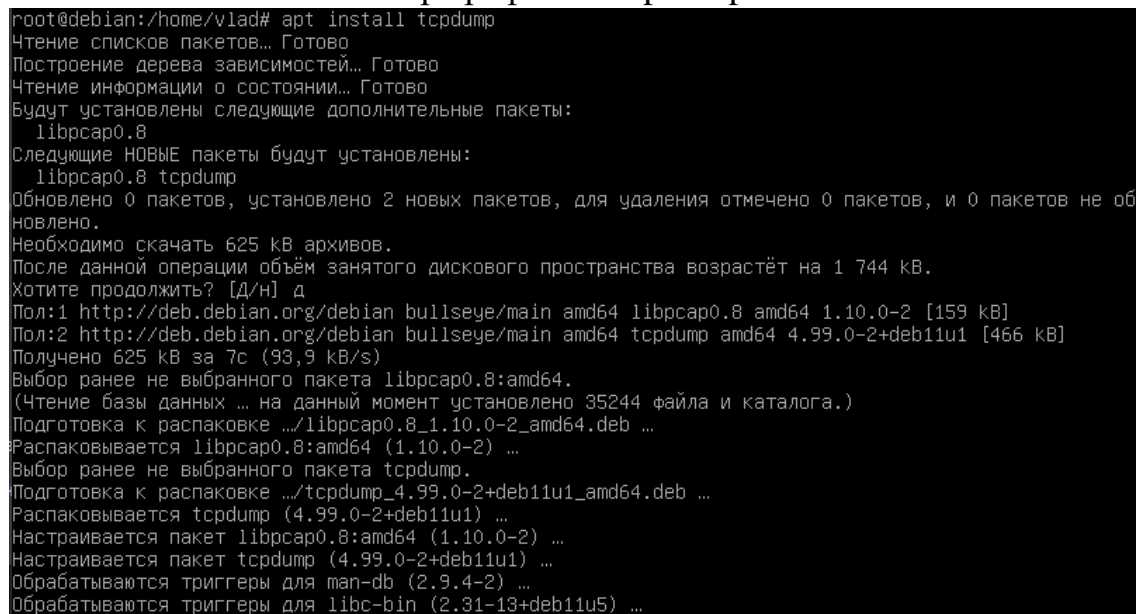


Рис.2. Установка tcpdump

3) Запустим анализатор трафика и сохраним данные в файл

```
root@debian:/home/vlad# tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telenet.log
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

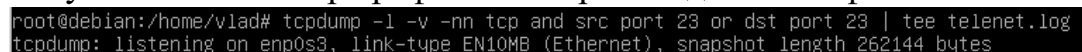


Рис.3. Запуск анализатора трафика tcpdump

2. Попытка установки соединения на 23 порту

- 1) Переходим к начальному окну с помощью Ctrl+b 0
- 2) Попробуем подключиться через telnet по ip – 178.234.29.197 на 23 порту

```
root@debian:/home/vlad# telnet 178.234.29.197 23
Trying 178.234.29.197...
telnet: Unable to connect to remote host: Connection timed out
root@debian:/home/vlad#
```

Рис.4. Попытка подключения по ip – 178.234.29.197

Ошибка, невозможно подключиться к серверу удаленно.

3. Запуск анализатора трафика tcpdump на 22 порту

- 1) Создаем новое окно комбинацией Ctrl+b с в tmux
- 2) Запускаем анализатор трафика

```
root@debian:/home/vlad# tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee telnet.log
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Рис.5. Запуск анализатора трафика tcpdump

4. Попытка установки соединения на 22 порту

- 1) Переходим к начальному окну с помощью Ctrl+b 0
- 2) Попробуем подключиться через telnet по ip – 178.234.29.197 на 22 порту

```
root@debian:/home/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_8.4p1 Debian-5+deb11u1
Connection closed by foreign host.
root@debian:/home/vlad#
```

Рис.6. Попытка подключения по ip – 178.234.29.197

Ошибка, невозможно подключиться к серверу удаленно.

5. Запуск анализатора трафика на 22 порту

- 1) Создадим новое окно с помощью комбинации Ctrl+b с
- 2) Запускаем анализатор трафика tcpdump с сохранением данных в файл

```
root@debian:/home/vlad# tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Рис.7. Запуск анализатора трафика tcpdump

6. Установление шифрованного соединения с удаленным сервером

```
root@debian:/home/vlad# ssh -l cn61763 vh314.timeweb.ru
cn61763@vh314.timeweb.ru's password:

-----
//  ( )  _ _ _ _ _ | | / / //  //  //
//  //  //  //  //  //  //  //  //  //
//  //  //  //  //  //  //  //  //  //

Last login: Thu Feb  2 10:36:18 2023 from 176.59.43.158
cn61763@vh314:~$ _
[0] 0:ssh* 1:tcpdump-
```

Рис.8. Установление шифрованного соединения с удаленным сервером

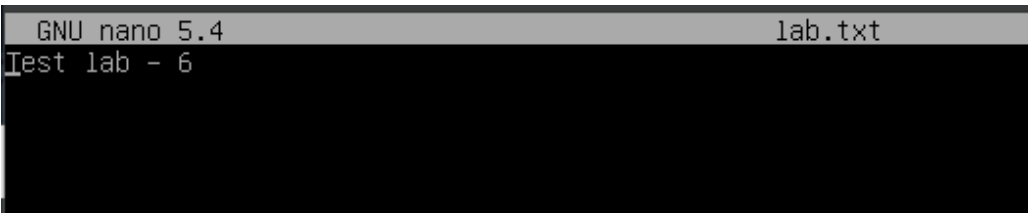
7. Получение информации об удаленной системе

```
cn61763@vh314:~$ uname -a
Linux vh314 5.4.0-120-generic #136~18.04.1-Ubuntu SMP Fri Jun 10 18:00:44 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
cn61763@vh314:~$ _
[0] 0:ssh* 1:tcpdump- "debian" 10:40 02-фев-23
```

Рис.9. Информация об удаленной системе

8. Передача файла по зашифрованному каналу

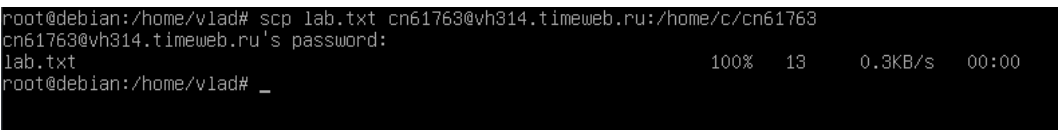
1) Создадим файл командой nano и запишем тестовую строку



```
GNU nano 5.4 lab.txt
Test lab - 6
```

Рис.10. Тестовая строка файла lab.txt

2) Передадим файл по зашифрованному каналу командой scp



```
root@debian:/home/vlad# scp lab.txt cn61763@vh314.timeweb.ru:/home/c/cn61763
cn61763@vh314.timeweb.ru's password:
lab.txt                                100% 13      0.9KB/s  00:00
root@debian:/home/vlad# _
```

Рис.11. Передача файла по зашифрованному каналу

3) Проверим копию файла lab.txt



Левая панель				Правая панель			
Файл		Команда		Файл		Команда	
Имя	Размер	Время правки		Имя	Размер	Время правки	
..	-ВВЕРХ-	янв 23 18:56		..	-ВВЕРХ-	янв 23 18:56	
.bash_history	42	янв 23 19:01		.bash_history	42	янв 23 19:01	
.bash_logout	220	янв 23 18:56		.bash_logout	220	янв 23 18:56	
.bashrc	3526	янв 23 18:56		.bashrc	3526	янв 23 18:56	
.profile	807	янв 23 18:56		.profile	807	янв 23 18:56	
dump.sql	2064	янв 23 21:32		dump.sql	2064	янв 23 21:32	
lab.txt	13	фев 2 10:43		lab.txt	13	фев 2 10:43	
ssh.log	172317	фев 2 10:48		ssh.log	172317	фев 2 10:48	

Совет: Вы сможете видеть скрытые файлы .*, установив опцию в меню Конфигурация.

root@debian:/home/vlad#

1Помощь 2Меню 3Просмотр 4Правка 5Копия 6Перенос 7Изменить 8Удалить 9МенюМС 10Выход

[0] 0:ssh- 1:tcpdump 2:мс*

Рис.12. Проверка копии файла

9. Создание зашифрованных ключей

- 1) Для начала выйдем из терминального мультиплексора tmux с помощью команды `exit`
- 2) Далее с помощью команды `ssh-keygen` создадим зашифрованные ключи

```
root@debian:/home/vlad# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:aLkwiXpoi2+2cbpGi2onVKgNTIDfsEF0NMD7fcJCHbk root@debian
The key's randomart image is:
+---[RSA 3072]-----+
|+++o+  .|
|..+. .o|
|o..* .o|
|..+.o Eo|
|o+o+o+ S|
|+.o+=+..|
|o+o*...o|
|= o.|
|.Bo.|
+---[SHA256]-----+
root@debian:/home/vlad#
```

[0] 0:ssh- 1:tcpdump 2:bash* "debian" 10:53 02-фев-23

Рис.13. Создание зашифрованных ключей

10. Передадим публичный ключ

```
root@debian:/home/vlad# ssh-copy-id -i ~/.ssh/id_rsa.pub cn61763@vh314.timeweb.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.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 all the new keys
cn61763@vh314.timeweb.ru's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'cn61763@vh314.timeweb.ru'"
and check to make sure that only the key(s) you wanted were added.

root@debian:/home/vlad#
```

[0] 0:ssh- 1:tcpdump 2:bash* "debian" 10:57 02-фев-23

Рис.14. Передача публичного ключа

11. Подключение к удаленной системе

```
root@debian:/home/vlad# ssh -l cn61763 vh314.timeweb.ru
Enter passphrase for key '/root/.ssh/id_rsa':

_____
//__(_)-_--|_|//___//____
///_/_-_-) |//_/_-_) \
///_/_/_/_\_/|_|/_/_/_/_\

Last login: Thu Feb  2 10:40:02 2023 from 176.59.43.158
cn61763@vh314:~$ _
[0] 0:ssh- 1:tcpdump 2:ssh*
```

Рис.15. Подключение к удаленной системе

12. Передача файла по зашифрованному каналу

```
root@debian:/home/vlad# scp lab.txt cn61763@vh314.timeweb.ru:/home/c/cn61763
Enter passphrase for key '/root/.ssh/id_rsa':
lab.txt                                                                    100% 13      0.2KB/s  00:00
root@debian:/home/vlad#
```

Рис.16. Передача файла по зашифрованному каналу

13. Просмотр содержимого файла telnet.log

```

GNU nano 5.4                                telnet.log
22:53:01.734518 IP (tos 0x10, ttl 64, id 35338, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.38696 > 178.234.29.197.22: Flags [S], cksum 0xdce4 (incorrect -> 0xf407), seq 144879
22:53:01.778092 IP (tos 0x0, ttl 64, id 845, offset 0, flags [none], proto TCP (6), length 44)
    178.234.29.197.22 > 10.0.2.15.38696: Flags [S.], cksum 0xdea4 (correct), seq 31104001, ack 144
22:53:01.778157 IP (tos 0x10, ttl 64, id 35339, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.38696 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0xfb70), ack 1, win
22:53:01.826757 IP (tos 0x0, ttl 64, id 846, offset 0, flags [none], proto TCP (6), length 80)
    178.234.29.197.22 > 10.0.2.15.38696: Flags [P.], cksum 0x9060 (correct), seq 1:41, ack 1, win
22:53:01.826840 IP (tos 0x10, ttl 64, id 35340, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.38696 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0xfb70), ack 41, wi
22:55:01.918608 IP (tos 0x0, ttl 64, id 851, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.38696: Flags [F.], cksum 0xf638 (correct), seq 41, ack 1, win 65
22:55:01.918830 IP (tos 0x10, ttl 64, id 35341, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.38696 > 178.234.29.197.22: Flags [F.], cksum 0xdcd8 (incorrect -> 0xfb6f), seq 1, ac
22:55:01.919139 IP (tos 0x0, ttl 64, id 852, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.38696: Flags [.], cksum 0xf637 (correct), ack 2, win 65535, leng
23:05:03.068738 IP (tos 0x0, ttl 64, id 39914, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.33426 > 178.234.29.197.22: Flags [S], cksum 0xdce4 (incorrect -> 0xf993), seq 106129
23:05:03.123088 IP (tos 0x0, ttl 64, id 874, offset 0, flags [none], proto TCP (6), length 44)
    178.234.29.197.22 > 10.0.2.15.33426: Flags [S.], cksum 0xf0f6 (correct), seq 47616001, ack 106
23:05:03.123154 IP (tos 0x0, ttl 64, id 39915, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.33426 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x0dc3), ack 1, win
23:05:03.123904 IP (tos 0x0, ttl 64, id 39916, offset 0, flags [DF], proto TCP (6), length 80)
    10.0.2.15.33426 > 178.234.29.197.22: Flags [P.], cksum 0xdd00 (incorrect -> 0xa7c1), seq 1:41,
23:05:03.124615 IP (tos 0x0, ttl 64, id 875, offset 0, flags [none], proto TCP (6), length 40)
    178.234.29.197.22 > 10.0.2.15.33426: Flags [.], cksum 0x088c (correct), ack 41, win 65535, ler
23:05:03.188671 IP (tos 0x0, ttl 64, id 876, offset 0, flags [none], proto TCP (6), length 80)
    178.234.29.197.22 > 10.0.2.15.33426: Flags [P.], cksum 0xa28a (correct), seq 1:41, ack 41, win
23:05:03.188722 IP (tos 0x0, ttl 64, id 39917, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.33426 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x0d9b), ack 41, wi
23:05:03.190054 IP (tos 0x0, ttl 64, id 39918, offset 0, flags [DF], proto TCP (6), length 1552)
    10.0.2.15.33426 > 178.234.29.197.22: Flags [F.], cksum 0x9a2a (incorrect -> 0x72ac), seq 144879

```

Рис.17. Просмотр содержимого файла telnet.log

14. Просмотр содержимого файла ssh.log

```
GNU nano 5.4 ssh.log
10:35:46.776508 IP (tos 0x0, ttl 64, id 39004, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [S], cksum 0x8f07 (incorrect -> 0x5398), seq 8920593
10:35:46.854075 IP (tos 0x0, ttl 64, id 866, offset 0, flags [none], proto TCP (6), length 44)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [S.], cksum 0xbf02 (correct), seq 704001, ack 892059
10:35:46.854160 IP (tos 0x0, ttl 64, id 39005, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [.], cksum 0x8ef3 (incorrect -> 0xdbce), ack 1, win
  176.57.210.144.22 > 10.0.2.15.38890: Flags [DF], proto TCP (6), length 80)
10:35:46.855196 IP (tos 0x0, ttl 64, id 39006, offset 0, flags [DF], proto TCP (6), length 80)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [P.], cksum 0x8f1b (incorrect -> 0x75cd), seq 1:41,
10:35:46.855921 IP (tos 0x0, ttl 64, id 867, offset 0, flags [none], proto TCP (6), length 40)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [P.], cksum 0xd697 (correct), ack 41, win 65535, leng
10:35:46.943237 IP (tos 0x0, ttl 64, id 868, offset 0, flags [none], proto TCP (6), length 81)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [P.], cksum 0xac3e (correct), seq 1:42, ack 41, win
10:35:46.943283 IP (tos 0x0, ttl 64, id 39007, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [.], cksum 0x8ef3 (incorrect -> 0xdba6), ack 42, win
10:35:46.944133 IP (tos 0x0, ttl 64, id 39008, offset 0, flags [DF], proto TCP (6), length 1552)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [P.], cksum 0x94db (incorrect -> 0xf37f), seq 41:155
10:35:46.980881 IP (tos 0x0, ttl 64, id 869, offset 0, flags [none], proto TCP (6), length 40)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [.], cksum 0xd0ba (correct), ack 1501, win 65535, le
10:35:46.980887 IP (tos 0x0, ttl 64, id 870, offset 0, flags [none], proto TCP (6), length 40)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [.], cksum 0xd086 (correct), ack 1553, win 65535, le
10:35:47.136145 IP (tos 0x0, ttl 64, id 871, offset 0, flags [none], proto TCP (6), length 1120)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [P.], cksum 0xe2a0 (correct), seq 42:1122, ack 1553,
10:35:47.149574 IP (tos 0x0, ttl 64, id 39010, offset 0, flags [DF], proto TCP (6), length 88)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [P.], cksum 0x8f23 (incorrect -> 0x771c), seq 1553:1
10:35:47.150388 IP (tos 0x0, ttl 64, id 872, offset 0, flags [none], proto TCP (6), length 40)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [.], cksum 0xcc1e (correct), ack 1601, win 65535, le
10:35:47.270826 IP (tos 0x0, ttl 64, id 873, offset 0, flags [none], proto TCP (6), length 492)
  176.57.210.144.22 > 10.0.2.15.38890: Flags [P.], cksum 0x8f1f (correct), seq 1122:1574, ack 160
10:35:47.312045 IP (tos 0x0, ttl 64, id 39011, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [.], cksum 0x8ef3 (incorrect -> 0xd171), ack 1574, u
10:35:50.282877 IP (tos 0x0, ttl 64, id 39012, offset 0, flags [DF], proto TCP (6), length 56)
  10.0.2.15.38890 > 176.57.210.144.22: Flags [P.], cksum 0x8f03 (incorrect -> 0xc738), seq 1601:1
[ Read 3216 lines ]
^G Help      ^O Записать  ^W Поиск     ^K Cut       ^T Execute   ^C Location  M-U Отмена
^X Выход     ^R Чит.файл ^N Замена   ^U Paste     ^J Выводить  ^_ К строке  M-E Повтор
[0] 0:~$ bash- 1:tcpdump 2:~$ "debian" 16:57 02-фев-23
```

Рис.18. Просмотр содержимого файла ssh.log

Вывод

В ходе данной лабораторной работы мною были получены навыки по программному обеспечению удаленного доступа к распределенным 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.