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

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 инициирующие 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 соединени 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. Отметь 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

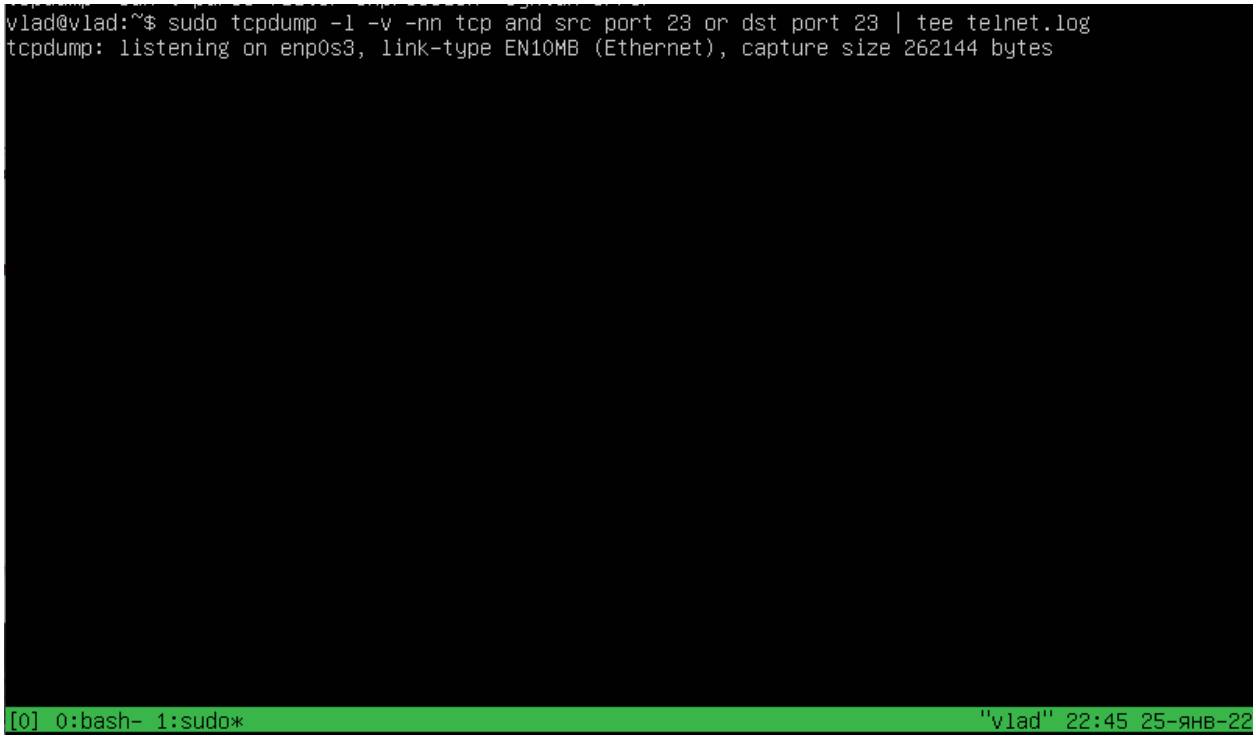


Рисунок 1 – Запуск анализатора трафика tcpdump

2) Попытка установки соединения (порт 23)

• Ctrl-b 0 (переход к 0 окну)

• telnet 178.234.29.197 23

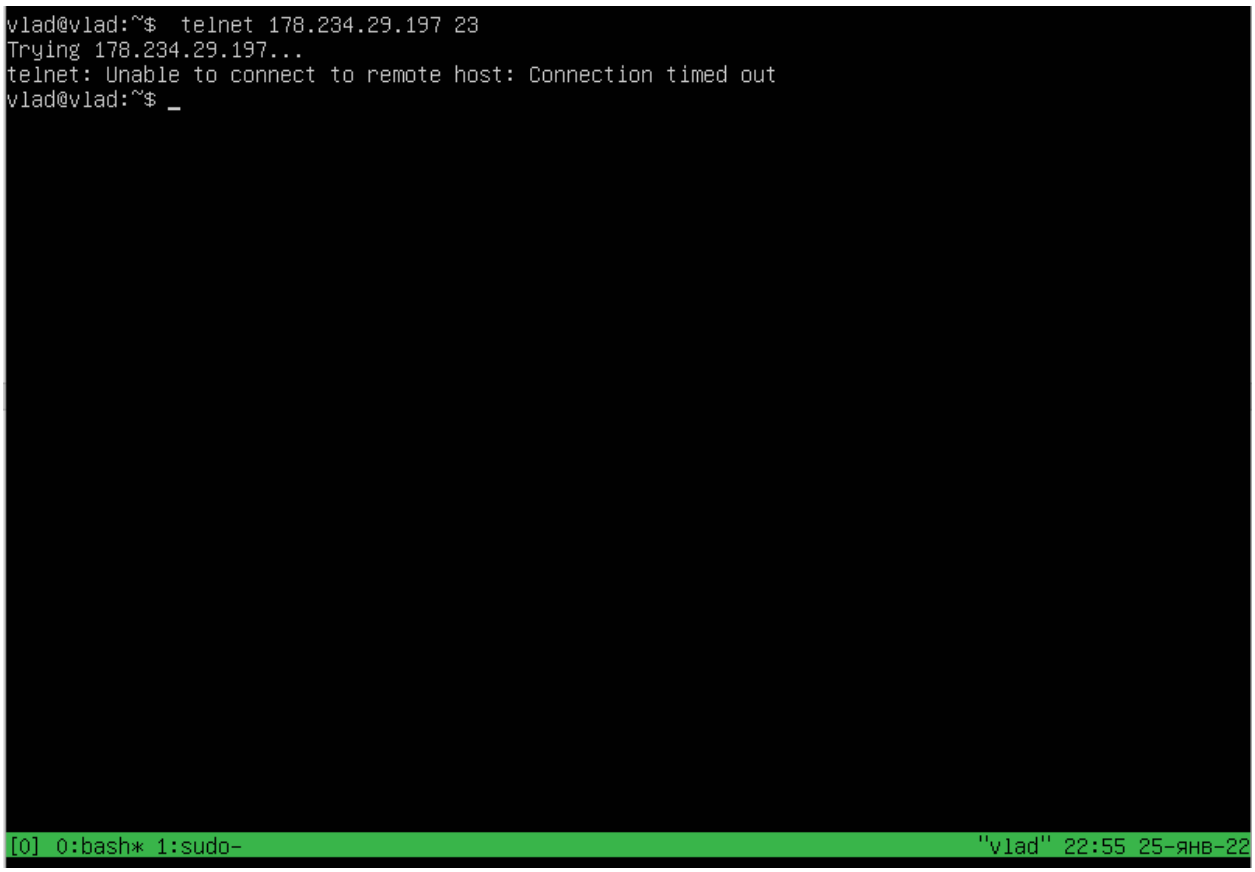


Рисунок 2 – Попытка установки соединения

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

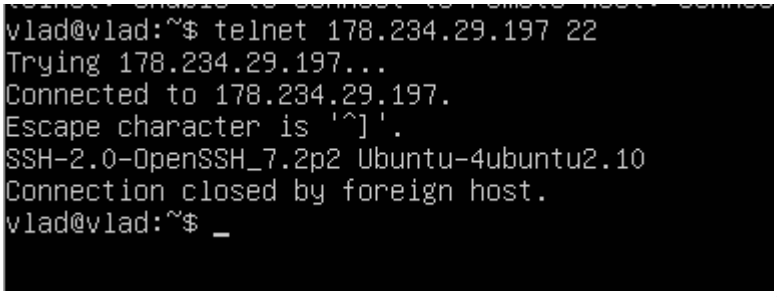
sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log

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



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

Рисунок 5 – Запуск анализатора трафика

6) Установление шифрованного соединения с удаленным сервером

• ssh –l stud11 edu.kurgasov.ru

Рисунок 6 – Установление шифрованного соединения

7) Вывод информации об удаленной системе

• uname -a

Рисунок 7 – Вывод информации об удаленной системе.

8) Передача файла по шифрованному каналу

• Ctrl-b c

• nano labrab7.txt

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

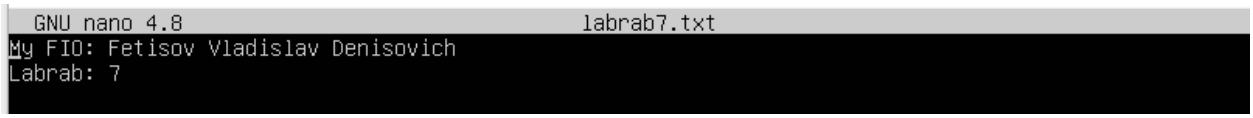


Рисунок 8 – Содержимое файла labrab7.txt

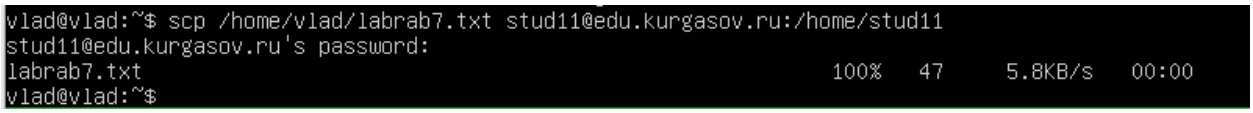


Рисунок 9 – Передача файла по шифрованному каналу

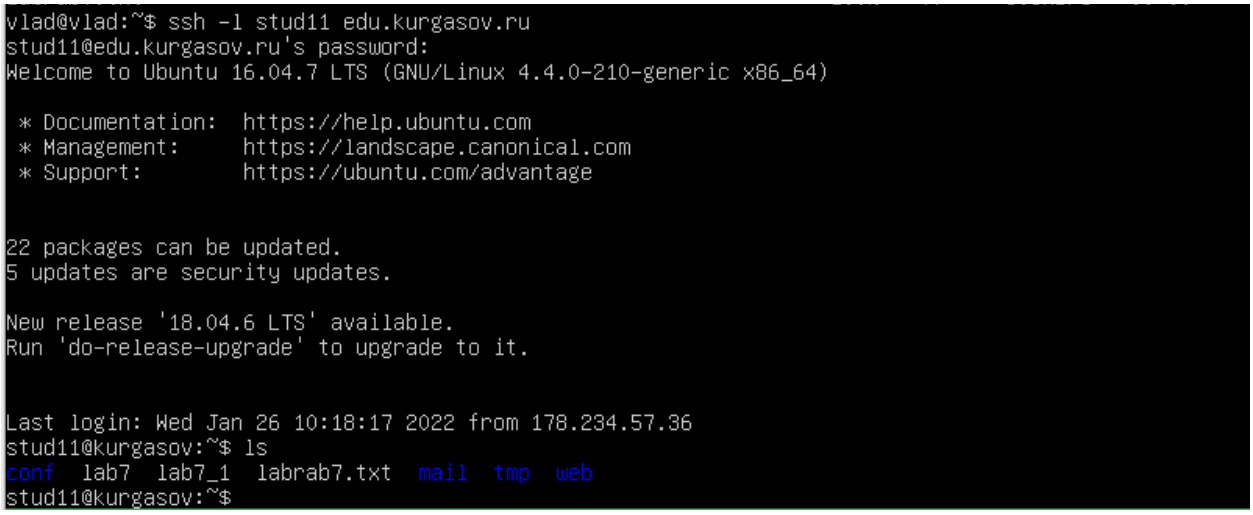


Рисунок 10 – Проверка наличия копии файла

9) Формирование зашифрованных ключей

• exit (выход)

• ssh-keygen (формирование зашифрованных ключей)

Рисунок 11 – Формирование зашифрованных ключей

10) Передача публичного ключа

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

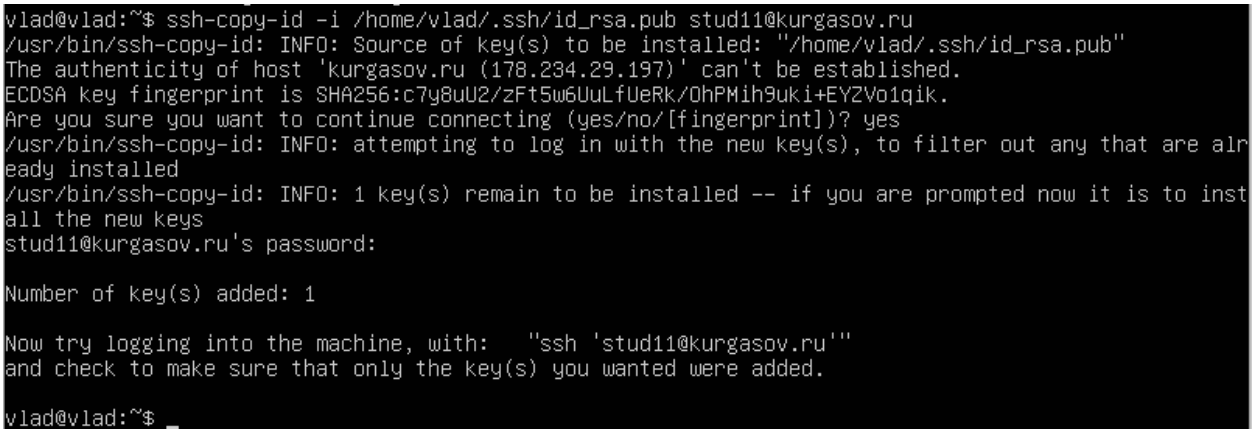


Рисунок 12 – Передача публичного ключа

11) Подключение к удаленной системе

• ssh –l stud11 edu.kurgasov.ru

Благодаря ssh пароль при входе не потребовался.

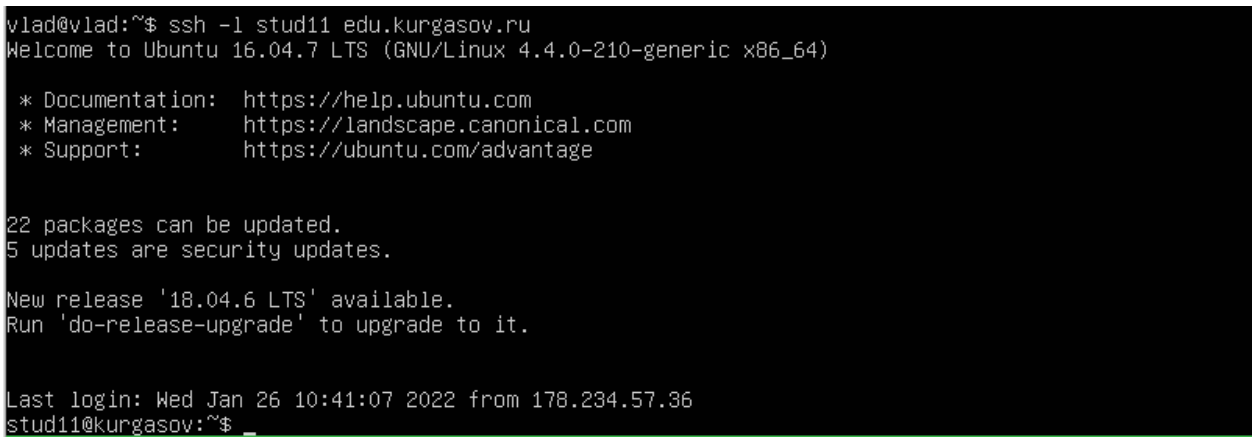


Рисунок 13 – Подключение к удаленной системе.

12) Передача файла по шифрованному каналу

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

Благодаря ssh пароль не понадобился.

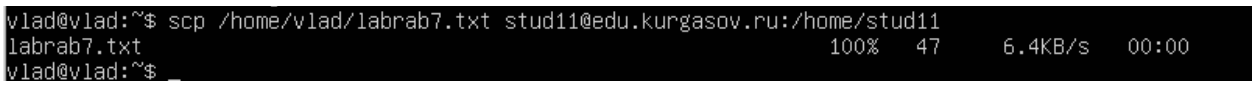


Рисунок 14 – Передача файла по шифрованному каналу

13) Содержимое файла telnet.log

• nano telnet.log

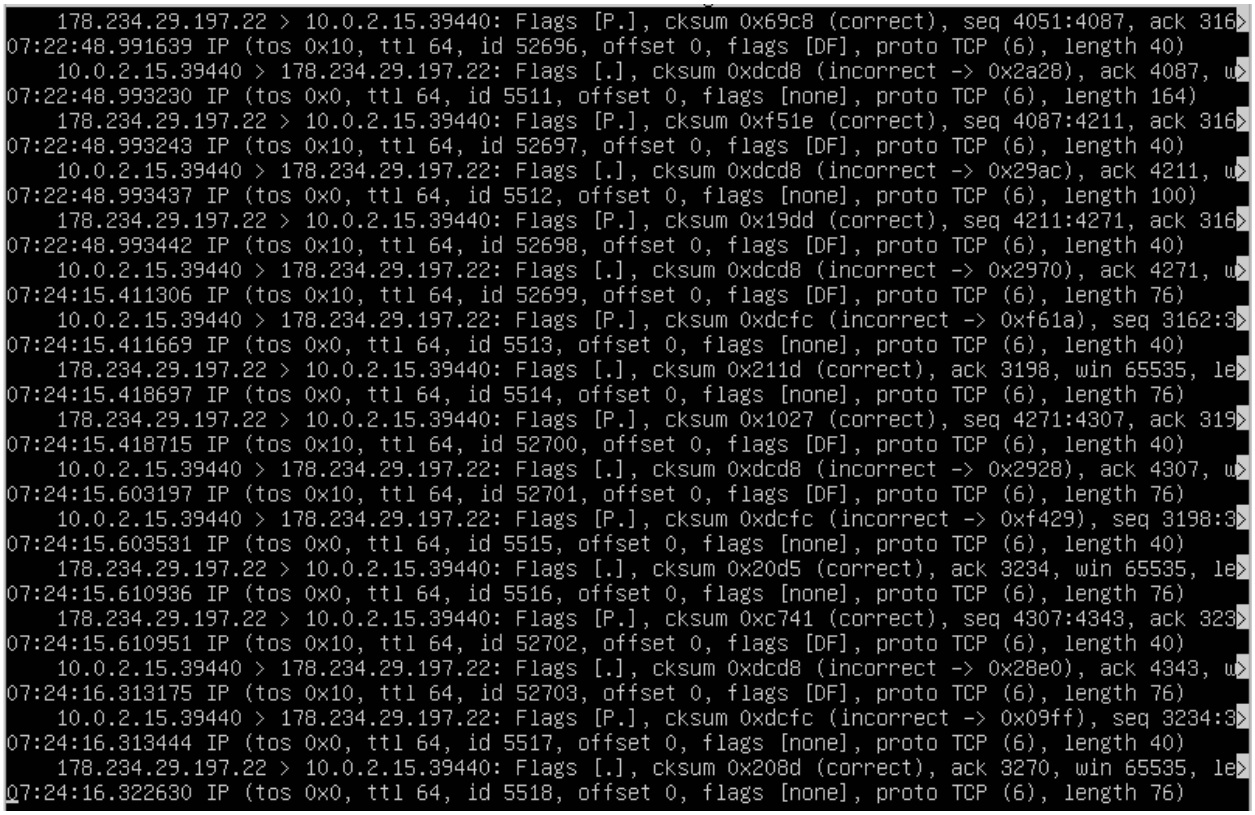


Рисунок 15 – Содержимое файла telnet.log

14) Содержимое файла ssh.log

• nano ssh.log

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 отличии 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.