МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет автоматизации и информатики

Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №6

по курсу “ОС Linux”

Студент ПИ-21-1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Красиков И. А.

(подпись, дата)

Руководитель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кургасов В.В.

(подпись, дата)

Липецк 2023

Оглавление

[Цель работы 3](#_Toc1)

[Ход работы 4](#_Toc2)

[1. Запуск анализатора трафика tcpdump на 23 порту 4](#_Toc3)

[2. Установка соединения с удаленной системой по порту 23 5](#_Toc4)

[3. Запуск tcpdump на порту 22 5](#_Toc5)

[4. Подключение по ssh к удаленной системе 5](#_Toc6)

[5. Вывод информации об удаленной системе 6](#_Toc7)

[6. Создание файла и передача его на удаленную систему по шифровальному каналу 6](#_Toc8)

[7. Формирование зашифрованного ключа 7](#_Toc9)

[8. Передача зашифрованного ключа на удаленную систему 7](#_Toc10)

[9. Попытка подключения по ssh к удаленной системе 8](#_Toc11)

[10. Повторная передача файла 8](#_Toc12)

[11. Содержимое файлов telnet.log и ssh.log 9](#_Toc13)

[Ответы на контрольные вопросы 10](#_Toc14)

# **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

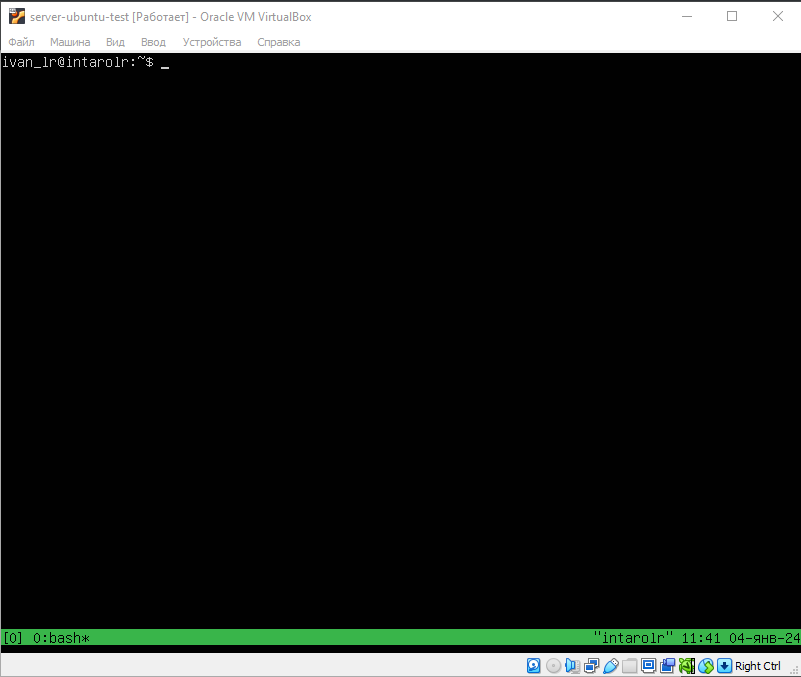


Рисунок 1 – Запуск tmux



Рисунок 2 – Запуск tcpdump по порту 23

## 2. Установка соединения с удаленной системой по порту 23

Для удаленной системы используется вторая ВМ соединенная с основной ВМ по сетевому мосту.

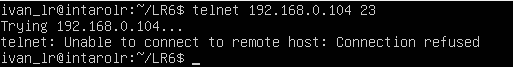


Рисунок 3 – Подключение к удаленной системе

Получаем ошибку подключения.

## 3. Запуск tcpdump на порту 22



Рисунок 4 – Запуск tcpdump на порту 22

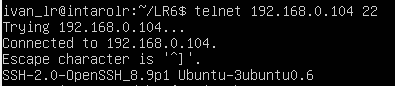


Рисунок 5 – подключение к удаленной системе по порту 22 через telnet

## 4. Подключение по ssh к удаленной системе

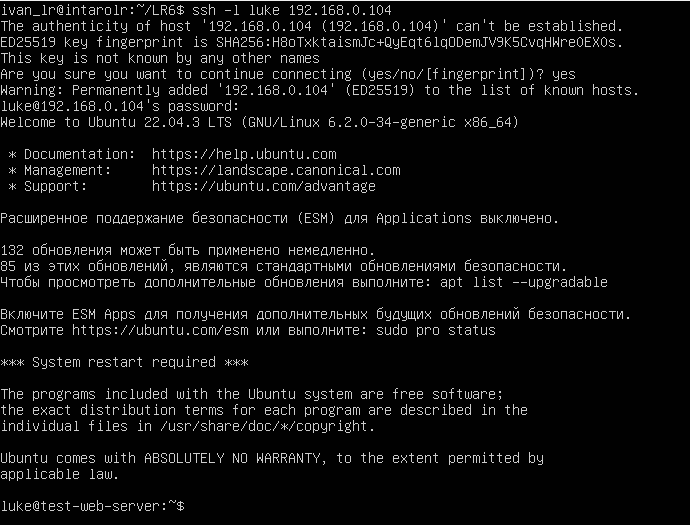


Рисунок 6 – Подключение по ssh

## 5. Вывод информации об удаленной системе

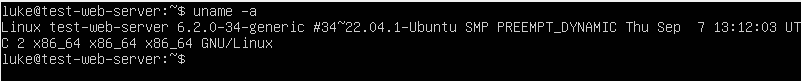


Рисунок 7 – uname -a

## 6. Создание файла и передача его на удаленную систему по шифровальному каналу

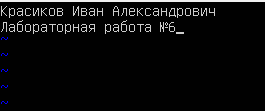


Рисунок 8 – Содержимое файла lr6

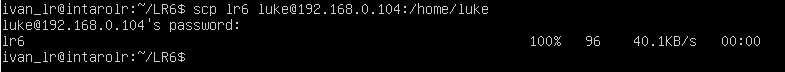


Рисунок 9 – Передача файла

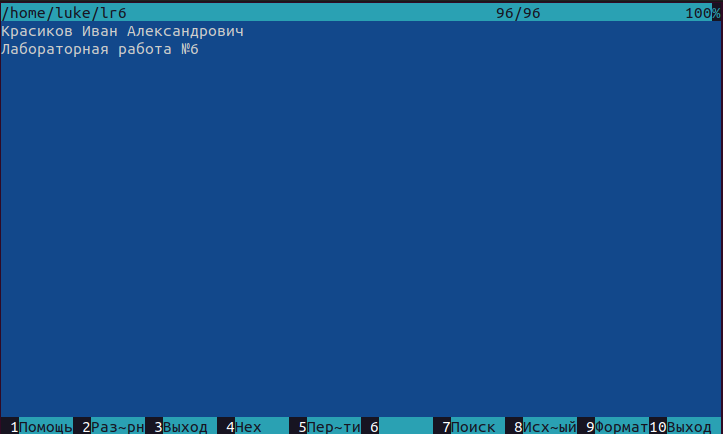


Рисунок 10 – Проверка наличия и содержимого файла на удаленной системе

## 7. Формирование зашифрованного ключа

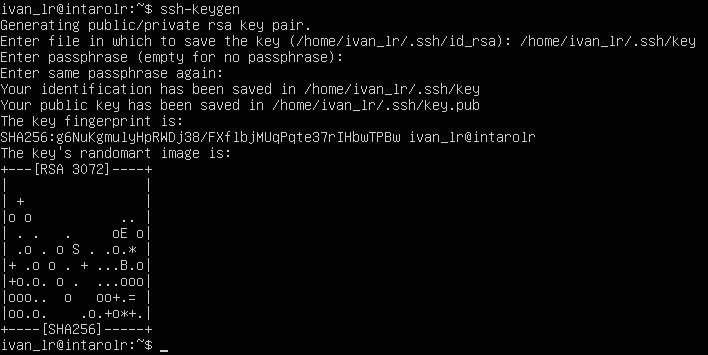


Рисунок 11 – формирование зашифрованного ключа

## 8. Передача зашифрованного ключа на удаленную систему

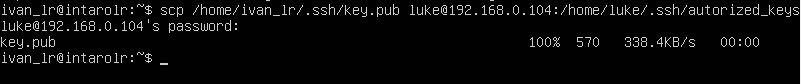


Рисунок 12 – Передача ключа на удаленную систему

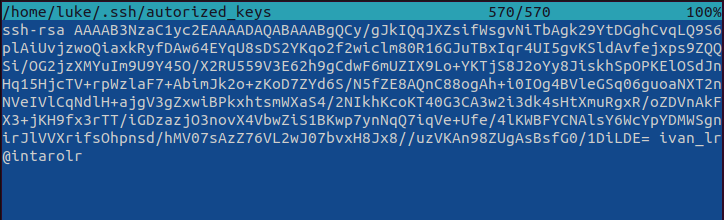


Рисунок 13 – Проверка передачи ключа

## 9. Попытка подключения по ssh к удаленной системе

При подключение указываем шифрованный ключ

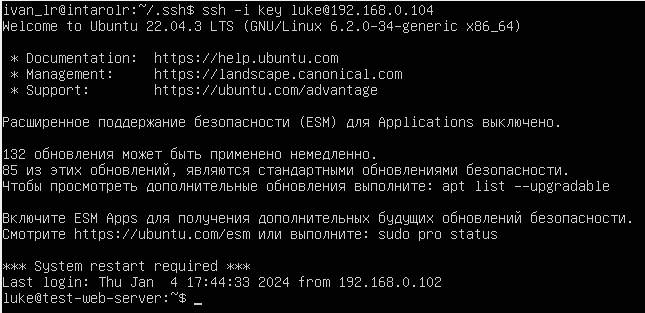


Рисунок 14 – Подключение по ssh

При подключение по ssh с указание ключа, пароль не требуется.

## 10. Повторная передача файла



Рисунок 15 – Передача файла с указание шифрованного ключа

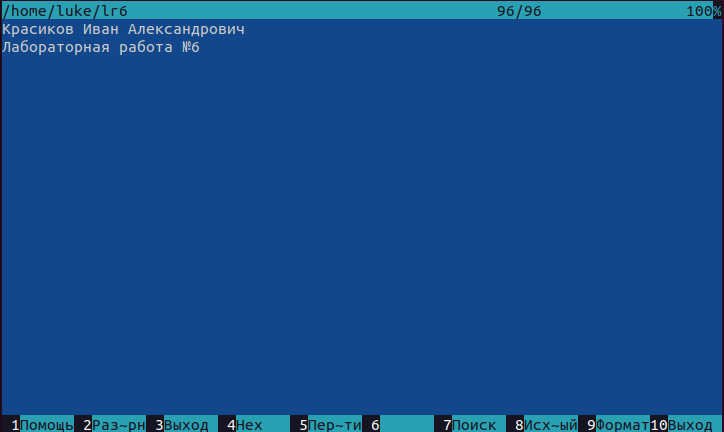


Рисунок 16 – Проверка передачи файла

При передачи файла с указанием ключа, не требуется пароль.

## 11. Содержимое файлов telnet.log и ssh.log

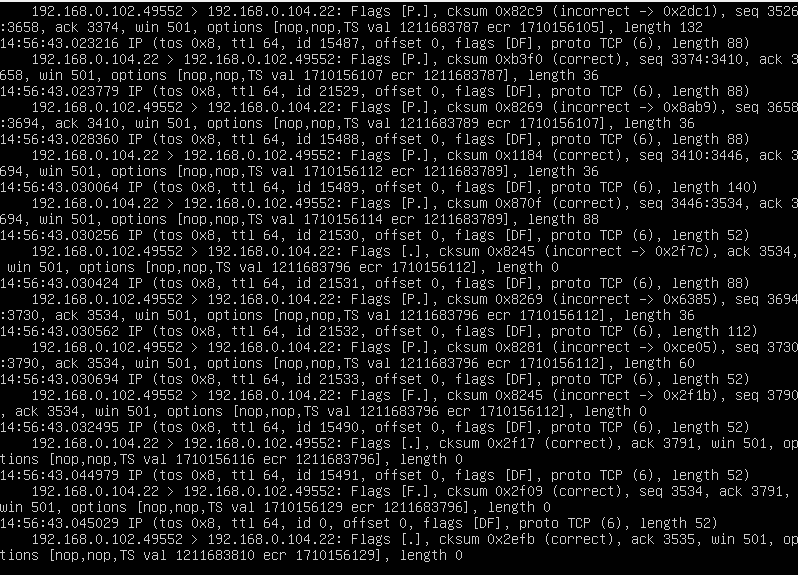


Рисунок 17 – ssh.log



Рисунок 18 – telnet.log

# Ответы на контрольные вопросы

**1)** Определите основные цели и задачи решаемые с помощью ПО удаленного доступа?

Программное обеспечение удаленного доступа предназначено для обеспечения возможности удаленного управления компьютерами и сетевыми ресурсами. Его основные цели включают удаленное администрирование, предоставление технической поддержки, доступ к файлам, обеспечение безопасности и мониторинг, а также поддержку дистанционной работы, что обеспечивает гибкость и эффективность в управлении информационными ресурсами из любой точки мира.

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

TELNET и SSH - это протоколы удаленного доступа, но SSH обладает рядом преимуществ и отличительных особенностей по сравнению с устаревшим TELNET:

**Безопасность:**

TELNET: Передает данные в открытом виде, что делает его небезопасным для передачи чувствительной информации.

SSH: Обеспечивает шифрование данных, обмен ключами и аутентификацию, обеспечивая высокий уровень безопасности при удаленном доступе.

**Шифрование:**

TELNET: Не предоставляет механизмы шифрования, что делает передаваемую информацию уязвимой для перехвата.

SSH: Использует криптографию для шифрования данных, предоставляя защиту от прослушивания и несанкционированного доступа.

**Аутентификация:**

TELNET: Обычно использует пароли для аутентификации, что менее безопасно и подвержено угрозам перехвата.

SSH: Предоставляет более сильные методы аутентификации, такие как использование ключей или двухфакторной аутентификации.

**Управление сеансами:**

TELNET: Просто передает текстовые команды, не предоставляя средства для эффективного управления сеансами и сетевыми ресурсами.

SSH: Позволяет более гибкое управление сеансами, поддерживает туннелирование, сжатие данных и перенаправление портов.

**Порт подключения:**

TELNET: Использует порт 23 для подключения, что может быть уязвимым к атакам и перехвату.

SSH: Обычно использует порт 22, но может быть настроен для использования другого порта, улучшая безопасность.

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

**Пароль:**

*Положительные аспекты:*

Прост в использовании и управлении.

Подходит для случаев, когда невозможно или неудобно использовать ключи.

*Отрицательные аспекты:*

Менее безопасен, так как подвержен атакам перебора паролей.

Возможны проблемы с безопасностью при передаче пароля по сети.

**Открытый ключ:**

*Положительные аспекты:*

Гораздо более безопасен, так как использует криптографию с открытым ключом.

Удобен для автоматизации процесса входа в систему.

*Отрицательные аспекты:*

Может потребовать дополнительных шагов для настройки, особенно для новых пользователей.

Возможны проблемы, если ключ утрачен или скомпрометирован.

**Аутентификация через агент:**

*Положительные аспекты:*

Повышает удобство использования открытых ключей, предотвращая необходимость ввода пароля каждый раз.

Улучшает безопасность, так как ключи не хранятся на удаленном сервере.

*Отрицательные аспекты:*

Требует запуска агента аутентификации на локальной машине, что может быть неудобно для некоторых пользователей.

Неправильная настройка может сделать систему менее безопасной.

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

Выполняя почти все лабораторные работы, я использовал ssh для удаленного доступа из командной строки Windows к ВМ ubuntu-server

**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

**6)** Что такое ключ ssh? В чем преимущество их использования?

Ключ SSH (Secure Shell) - это пара криптографических ключей, состоящая из открытого и закрытого ключа, используемая для аутентификации при подключении к удаленному серверу через протокол SSH. Преимущество использования ключей SSH заключается в усилении безопасности, поскольку они предоставляют более сильные механизмы аутентификации по сравнению с паролями. Кроме того, они обеспечивают удобство автоматизации процесса входа в систему и поддерживают безопасные методы передачи файлов и проксирования трафика.

**7)** Как сгенерировать ключи ssh в разных ОС?

Для работы с SSH-ключами используются утилиты, входящие в оболочку OpenSSH. Они работают под Linux, Windows и MacOS. Для Linux и Windows для генерации ключа отработает команда ssh-keygen. Еще ей можно указать параметр –t и после указать тип создаваемого ключа (алгоритм шифрования определяет тип).

8) Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Нет, из секретного ключа нельзя восстановить публичный ключ, и наоборот. Секретный ключ используется для расшифровки данных или подписи, в то время как публичный ключ используется для проверки этих подписей или зашифрованных данных. Важным свойством криптографических алгоритмов, используемых в SSH, является то, что они являются односторонними функциями, и восстановление закрытого ключа из открытого или наоборот математически невозможно при текущем уровне знаний.

9) Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями (наличие/отсутствие пароля на «секретный» ключ и т.п.)

Пары ключей, сгенерированные на одном ПК при одинаковых исходных условиях (даже с одинаковыми параметрами, такими как отсутствие пароля на секретном ключе), обычно будут отличаться. Это связано с использованием случайных чисел при генерации ключей, что приводит к уникальным значениям даже при повторных попытках на том же компьютере. Тем не менее, степень уникальности зависит от качества генератора случайных чисел и может быть повлияна конкретными настройками генерации ключей.

10) Перечислите доступные ключи для ssh-keygen.exe

o - Заставляет ssh-keygen сохранять закрытые ключи, используя новый формат OpenSSH, а не более совместимый формат PEM.

t - Указывает тип ключа для создания. Возможными значениями являются `rsa1" для версии протокола 1 и `dsa", `ecdsa", `ed25519" или `rsa" для версии протокола 2.

v - Подробный режим. Заставляет ssh-keygen печатать сообщения об отладке о ее ходе. Это полезно для генерации модулей отладки.

y - Эта опция считывает закрытый файл формата OpenSSH и печатает открытый ключ OpenSSH в стандартный вывод.

p - Запрашивает изменение ключевой фразы файла закрытого ключа вместо создания нового закрытого ключа. 16

e - Эта опция будет считывать закрытый или общедоступный файл ключа OpenSSH и распечатывать для стандартного вывода ключ в одном из форматов, указанных параметром -m.

i - Этот параметр будет считывать незашифрованный файл закрытого (или открытого) ключа в формате, указанном -m выберите и распечатайте совместимый с OpenSSH закрытый (или открытый) ключ в стандартный вывод

11) Можно ли использовать один «секретный» ключ доступа с разных ОС, установленных на одном ПК/на разных ПК?

Можно. Считается, что ssh-ключи не изнашиваются, поэтому их можно не менять и использовать для доступа на разные удаленные системы. Но лучше так не делать, потому что это снижает безопасность – получив один раз закрытый ключ, мы сможем получить доступ ко всем удаленным системам, которые используют пару публичного ключа этого ssh-ключа.

12) Возможно ли организовать подключение «по ключу» ssh к системе c ОС Windows, в которой запущен OpenSSH сервер?

Конечно, ведь поддержку OpenSSH для этого и ввели. Подключаться к винде и без ssh и OpenSSH можно было, но это было трудным занятием, а соединение не всегда стабильным.

13) Какие известные Вам сервисы сети Интернет позволяют организовать доступ к ресурсам посредством SSH ключей?

GitHub поддерживает авторизацию по ssh, для этого нужно создать секрет в аккаунте github и сохранить в секрете публичный ключ, а потом с машины постучаться на github – выполнить клон репозитория, пулл в него или что-то похожее.