

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Прикладные информационные технологии» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ №8**

**В РАМКАХ ДИСЦИПЛИНЫ «ОПЕРАЦИОННЫЕ СИСТЕМЫ»**

Выполнил:

Студент 2-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

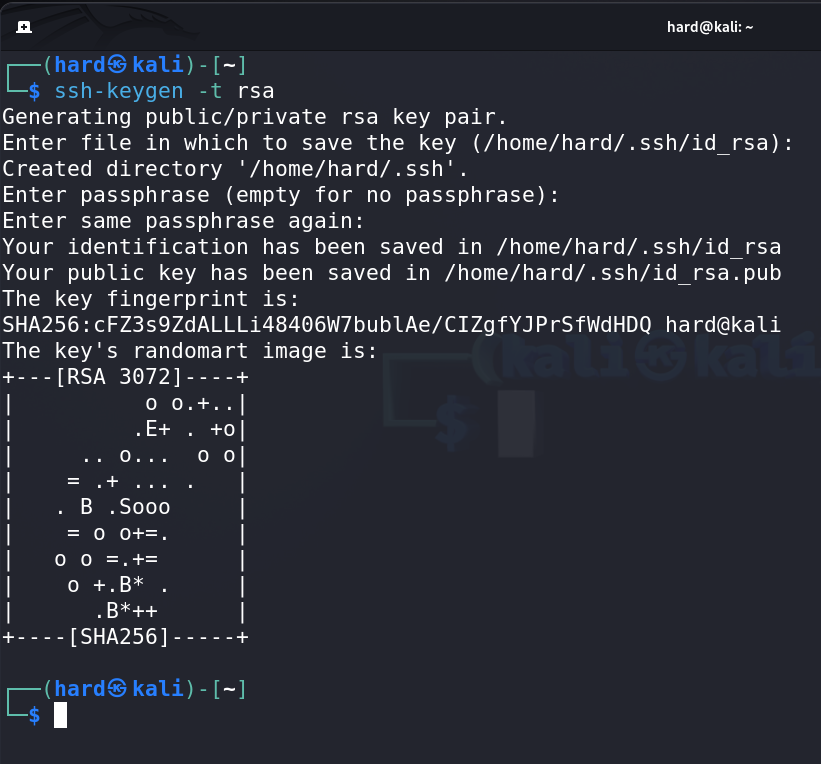
Оглавление

[Задание 3](#_Toc163922152)

[Листинг программы 5](#_Toc163922153)

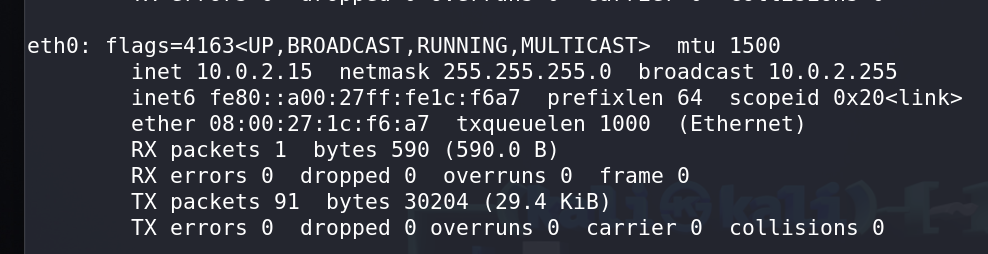
# Задание 1

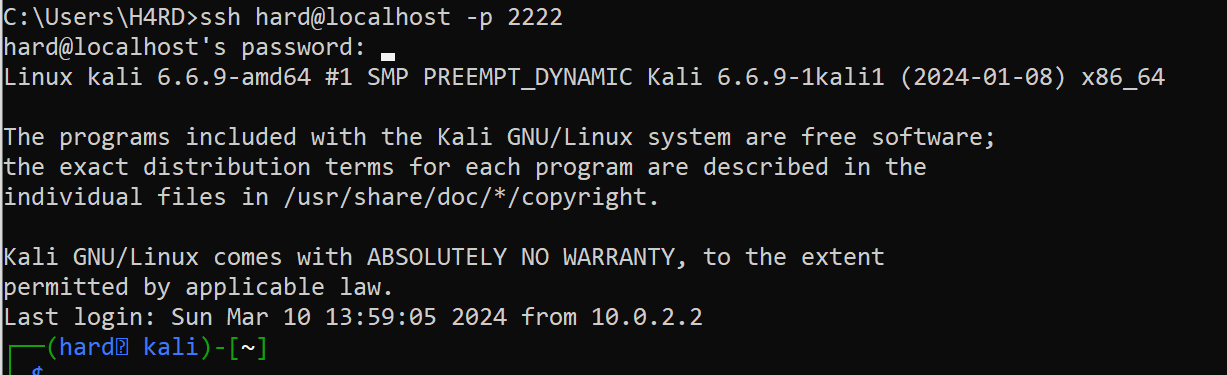
Сгенерируйте RSA ключ, скопируйте файл .ssh/identity.pub в файл .ssh/authorized\_keys (Поскольку у Вас один и тот же домашний каталог на всех машинах, то данная операция аналогична копированию файла на удаленную машину).



# Задание 2

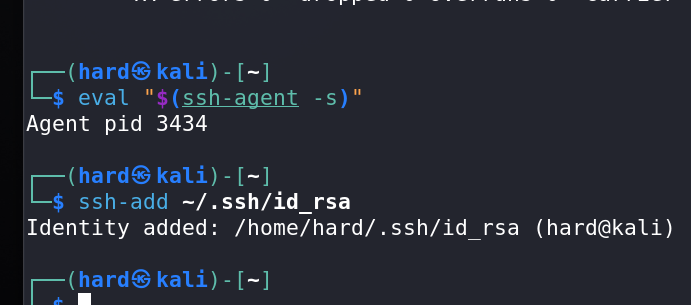
Зайдите на любую другую машину при помощи команды ssh.

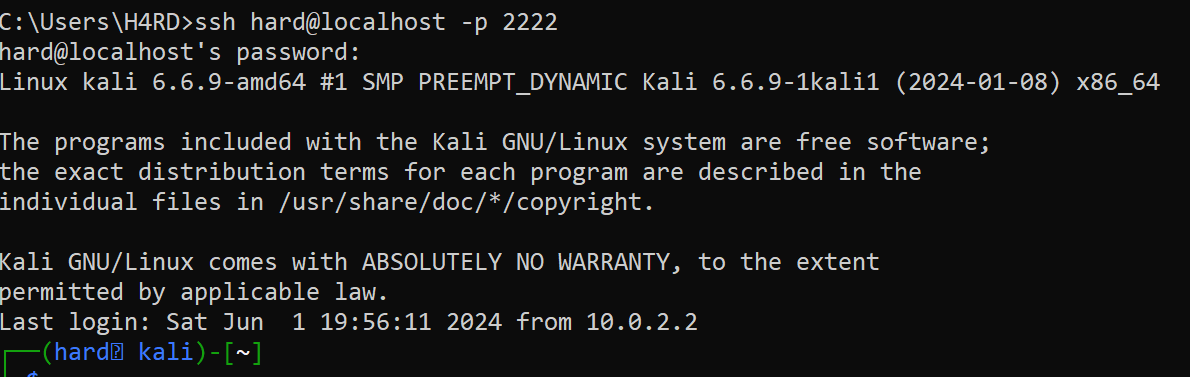




# Задание 3

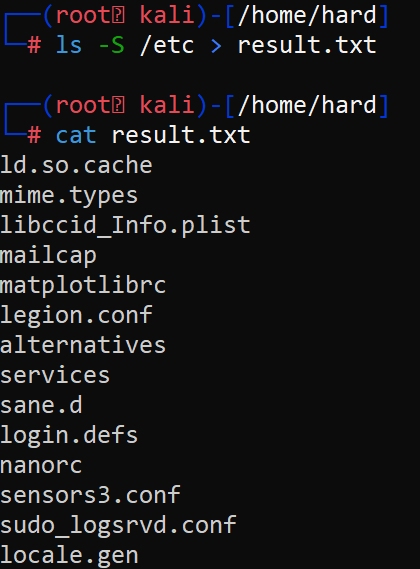
Запустите программу ssh-agent, добавьте в хранилище свой ключ. Зайдите при помощи программы ssh на другой компьютер.





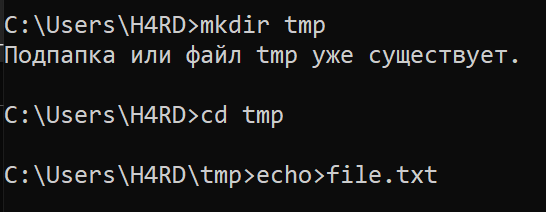
# Задание 4

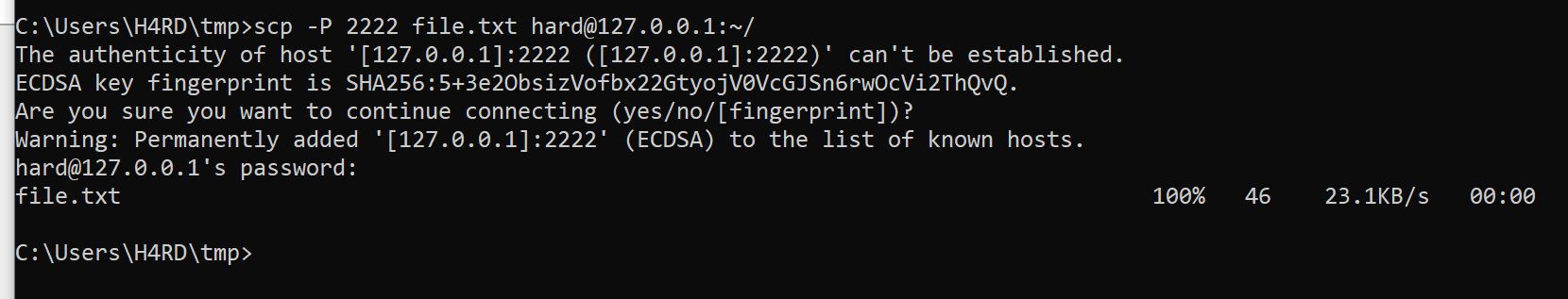
Выполните команду ls /etc на компьютере nix, отсортируйте результат на любом другом компьютере и сохраните результат в файле отчета.

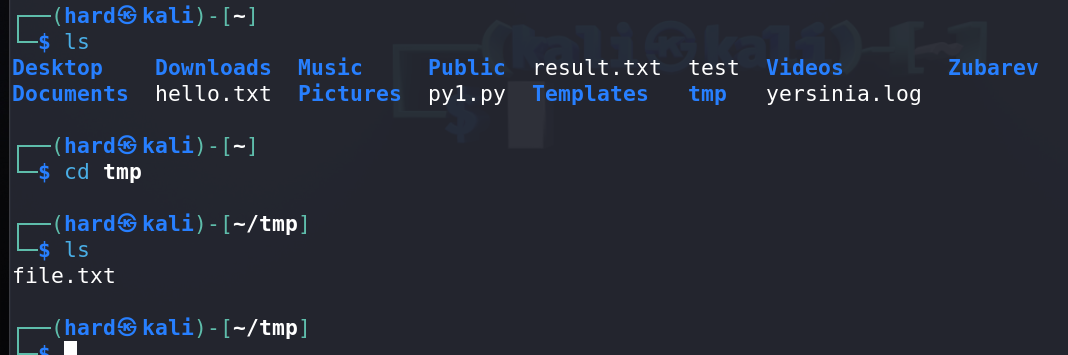


# Задание 5

Создайте в каталоге /tmp файл и скопируйте его на другую машину, также в каталог /tmp.

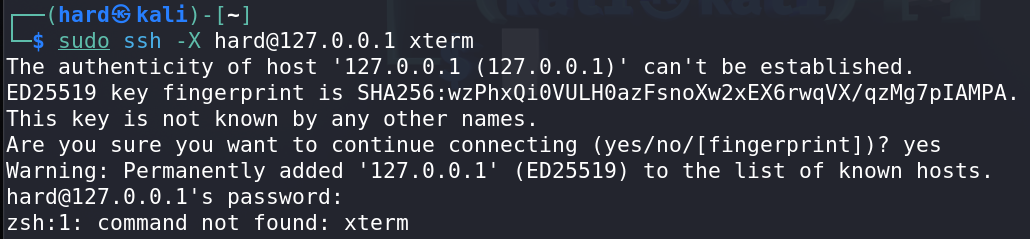






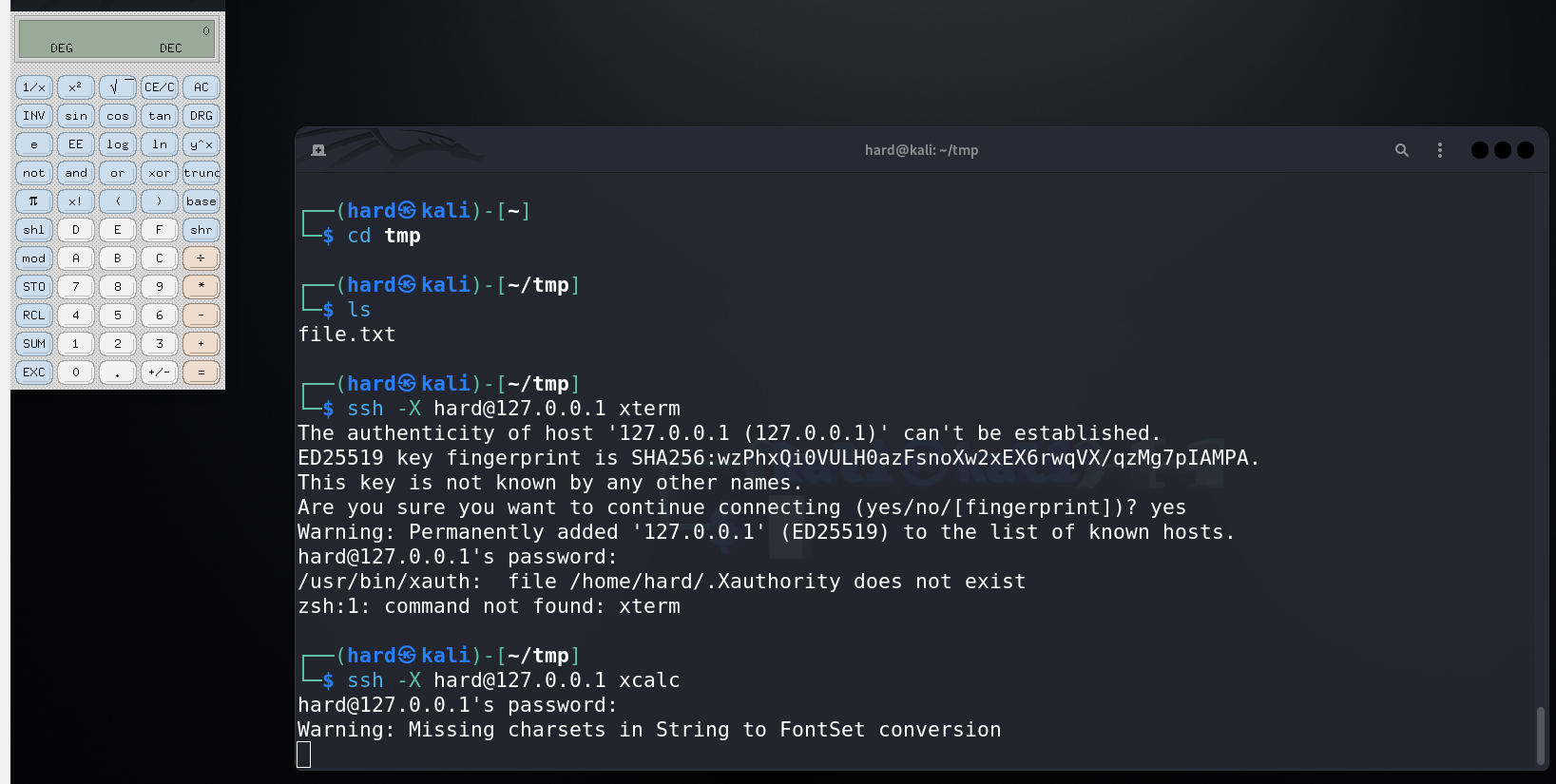
# Задание 6

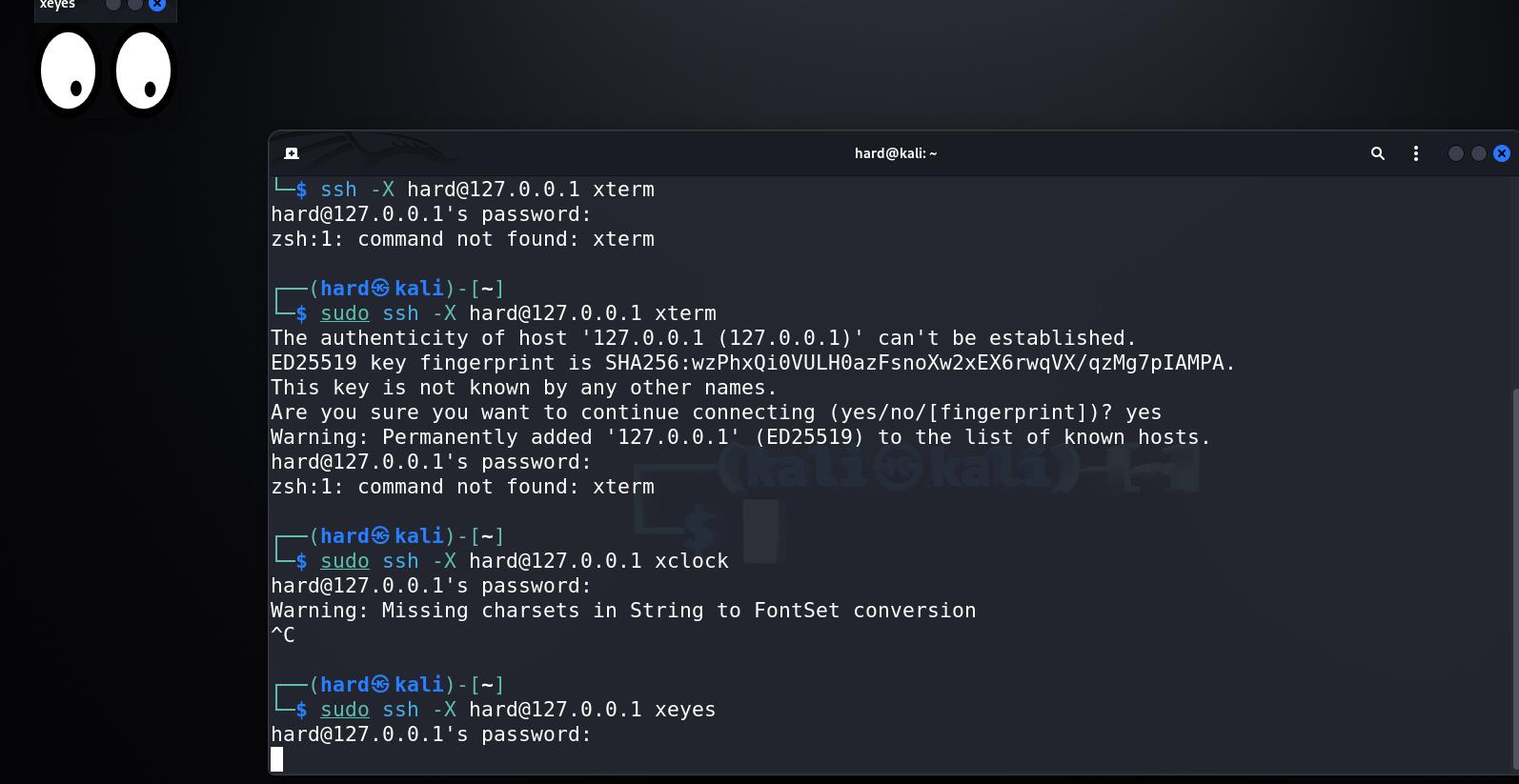
Запустите на другом компьютере программу xterm.

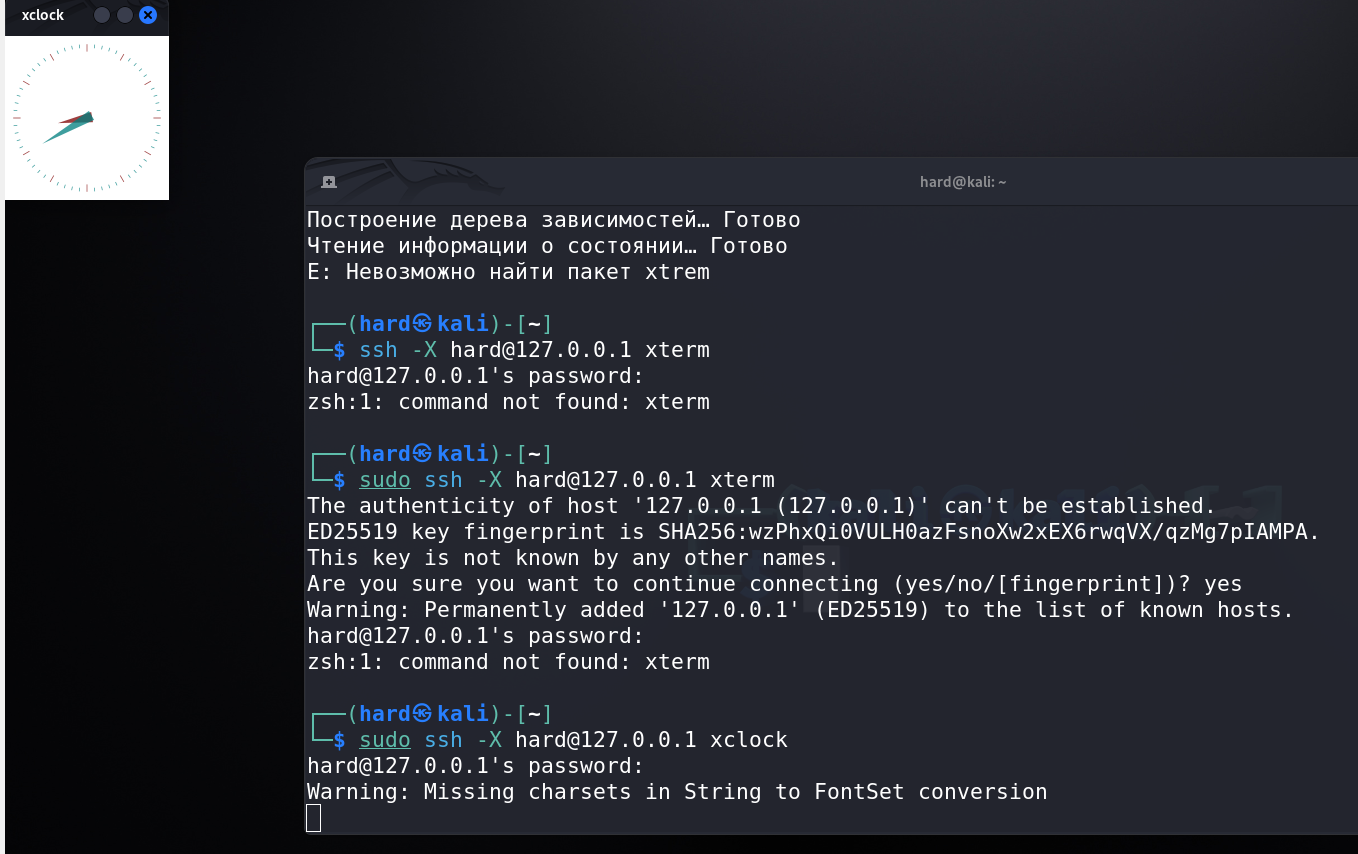


# Задание 7

Запустите на разных компьютерах программы xcalc, xclock, xeyes, xload



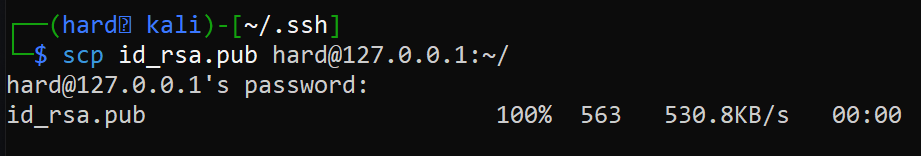


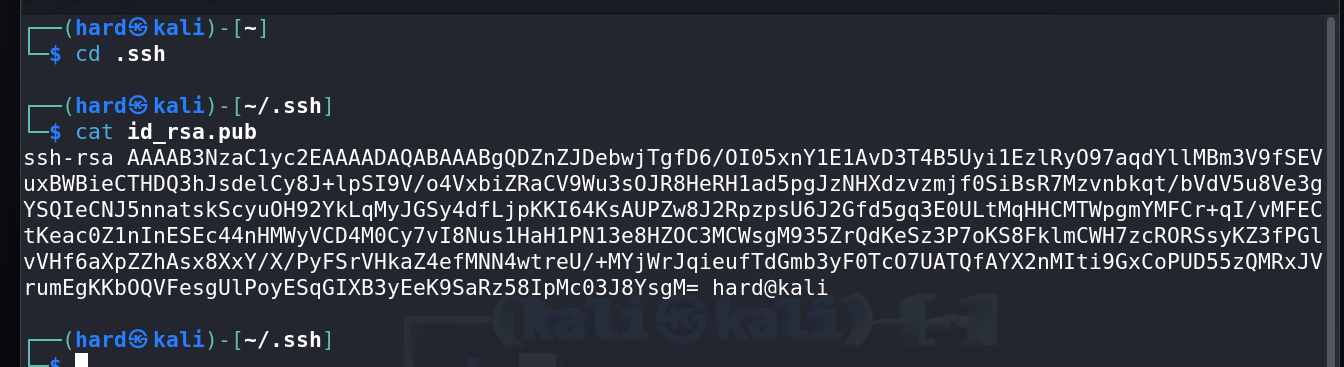




# Задание 8

Пробросить ключи на удаленную машину



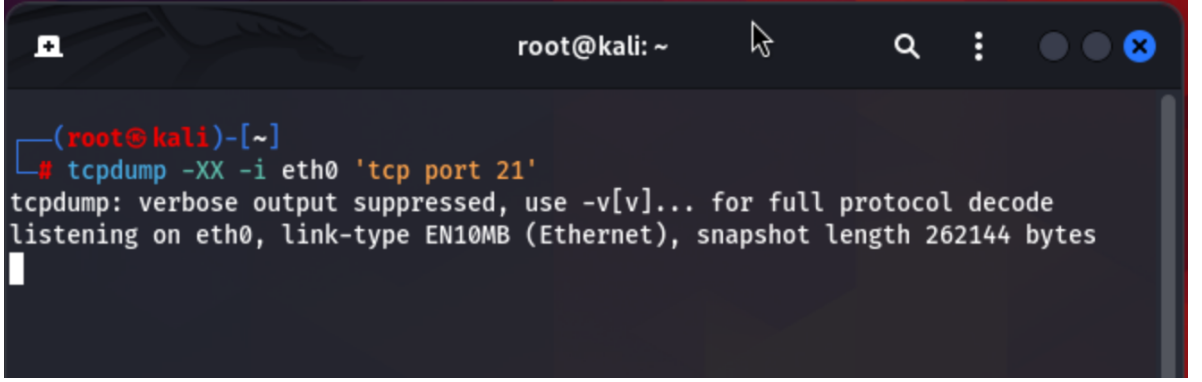




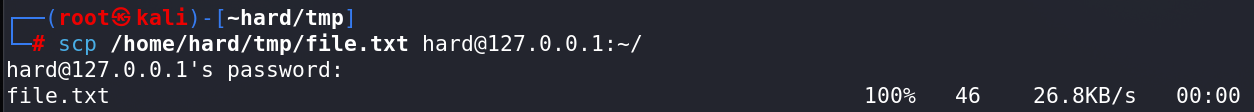
# Задание 9

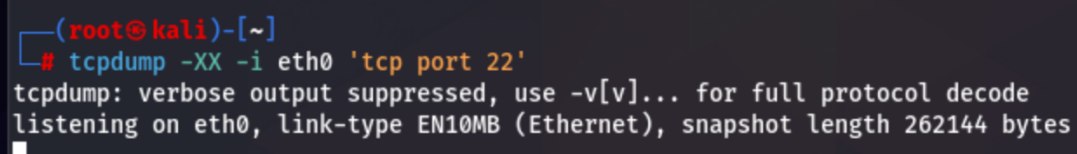
Проанализировать сравнительную скорость ssh-соединения, выполнив следующие замеры:

Выполнить передачу файла через FTP с помощью утилиты wget. Проанализировать проходящие пакеты с помощью утилиты tcpdump(-ХХ). Запомнить скорость передачи.

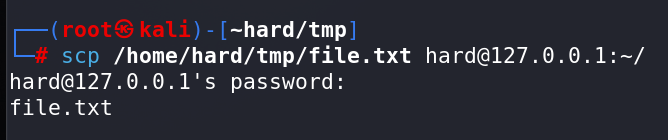


Выполнить передачу через ssh. Проанализировать проходящие пакеты с помощью утилиты tcpdump(-ХХ). Запомнить скорость передачи. Сравнить передаваемые пакеты и скорости передачи данных.





Включить сжатие ssh и повторить замер скорости. В каждом тесте анализировать результаты для файла состоящего из нулей и для файла состоящего из случайных последовательностей (dd if= /dev/urandom of=file ds=1M count=10), для текстового конфигурационного файла или бинарного файла.



# Ответы на вопросы

1. Для чего нужен протокол SSH?
   1. Безопасный доступ к удаленным серверам и машинам.
   2. Выполнение команд на удаленном сервере.
   3. Передача файлов через SCP (Secure Copy Protocol) и SFTP (Secure File Transfer Protocol).
   4. Туннелирование и перенаправление портов.
2. Почему этот протокол называют защищенным?

SSH называют защищенным, потому что он использует методы шифрования для обеспечения конфиденциальности и целостности данных, передаваемых по сети. Основные меры безопасности включают:

* 1. Аутентификация пользователей с использованием паролей или пар ключей (асимметричное шифрование).
  2. Шифрование трафика между клиентом и сервером, предотвращающее перехват и анализ данных.
  3. Целостность данных, обеспечивающая, что данные не были изменены в пути.

1. Какая информация нужна для того, чтобы подключиться к удаленной машине?

Для подключения к удаленной машине по SSH требуется следующая информация:

* 1. IP-адрес или доменное имя удаленной машины.
  2. Имя пользователя на удаленной машине.
  3. Метод аутентификации (пароль или пара ключей).
  4. Порт, на котором слушает SSH-сервер (по умолчанию это порт 22).

1. Из чего состоит пара ключей?

Пара ключей состоит из двух частей:

* 1. Открытый ключ (public key): Этот ключ можно свободно распространять. Он используется для шифрования данных.
  2. Закрытый ключ (private key): Этот ключ должен храниться в тайне. Он используется для расшифровки данных, зашифрованных соответствующим открытым ключом.

1. Каковы рекомендуемые действия по безопасному использованию SSH?

Для безопасного использования SSH рекомендуется:

* 1. Использовать пару ключей для аутентификации вместо паролей.
  2. Ограничить доступ по IP-адресам, чтобы только определенные устройства могли подключаться.
  3. Использовать сильные пароли и защищенные хранилища для закрытых ключей.
  4. Отключить root-доступ через SSH.
  5. Обновлять программное обеспечение SSH для защиты от уязвимостей.
  6. Настроить брандмауэр и инструменты мониторинга для отслеживания несанкционированных попыток доступа.

6. Как установить и настроить пакет OpenSSH в Linux и Windows?

В Linux:

sh

sudo apt update

sudo apt install openssh-server

sudo systemctl start ssh

sudo systemctl enable ssh

sudo systemctl status ssh

Настройка OpenSSH:

Файл конфигурации находится по адресу `/etc/ssh/sshd\_config`. В нем можно настроить различные параметры, такие как порт, методы аутентификации и т.д.

Перезапуск службы после изменений:

sudo systemctl restart ssh

В Windows:

1. Установка OpenSSH через PowerShell:

powershell

Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH\*'

Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

2. Запуск и настройка службы:

Start-Service sshd

Set-Service -Name sshd -StartupType 'Automatic'

3. Открытие порта в брандмауэре:

New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 2

4. Настройка OpenSSH:

Файл конфигурации находится по адресу `C:\ProgramData\ssh\sshd\_config`. В нем можно изменить параметры по аналогии с конфигурацией в Linux.

5. Перезапуск службы после изменений:

Restart-Service ssh