Цель задания

Освоить работу логирования в Linux.

Научиться искать открытые файлы и процессы.

Познакомиться с утилитами мониторинга.

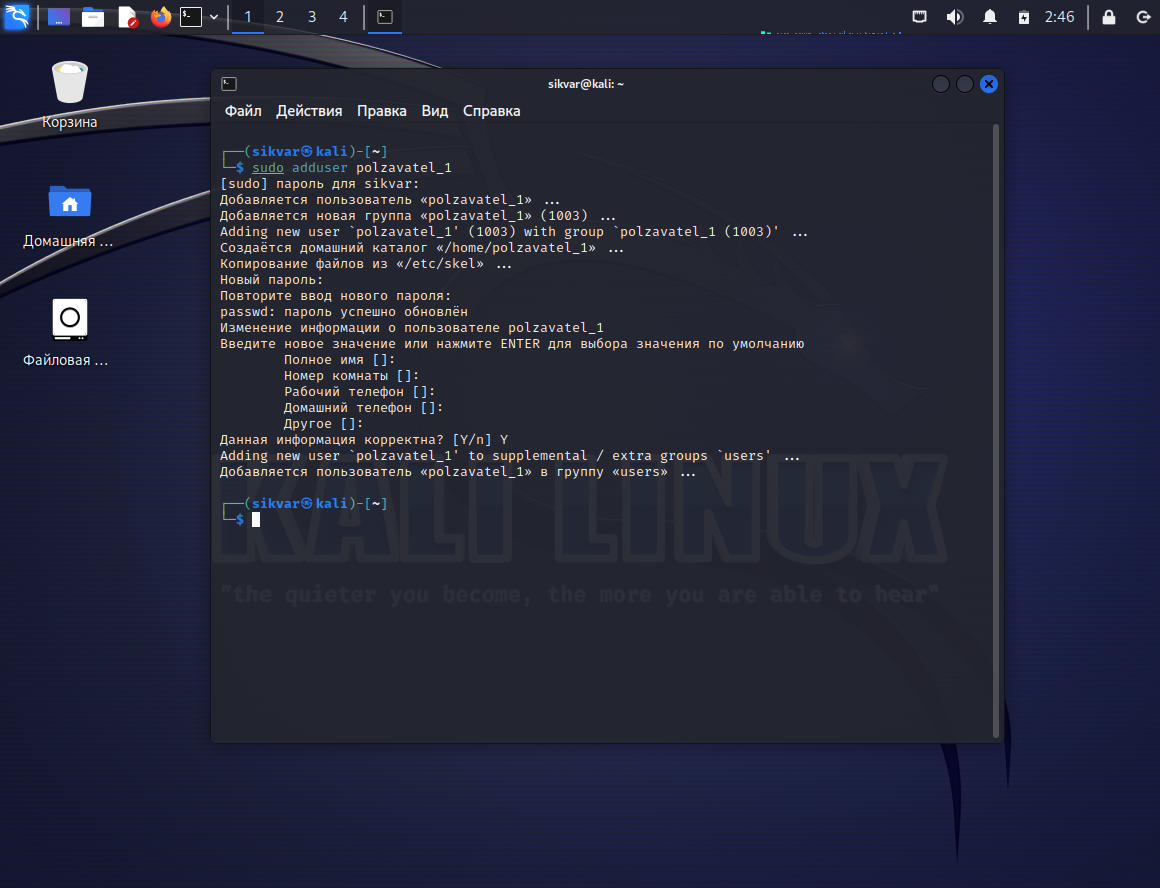
**Задание 1. Поиск открытых файлов**

Руководитель попросил вас провести небольшое расследование, для которого вам понадобятся утилиты по мониторингу. Вам нужно узнать, какие файлы пользователей открыты на ПК в корпоративной сети.

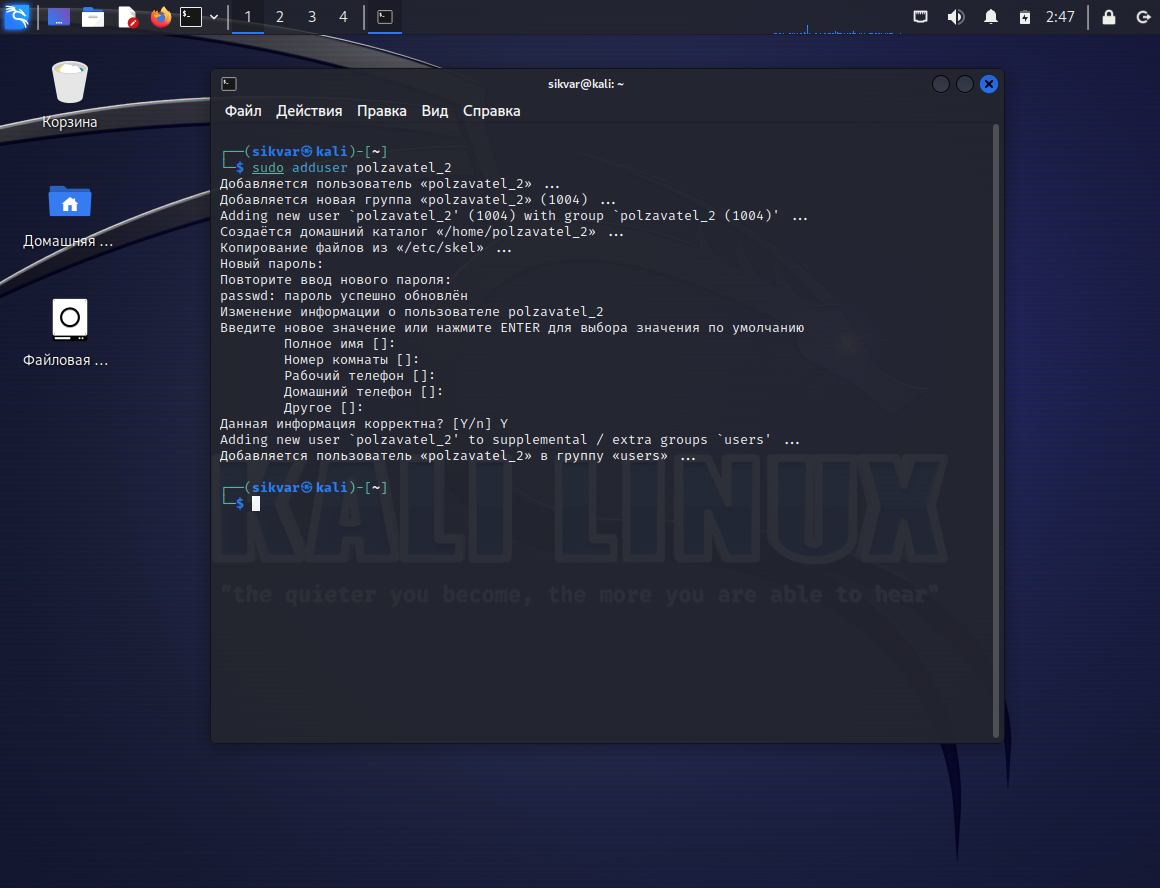
Предлагаем выполнить задание на своём ПК, чтобы потренироваться:

1 Создал трёх пользователей с помощью утилиты useradd.

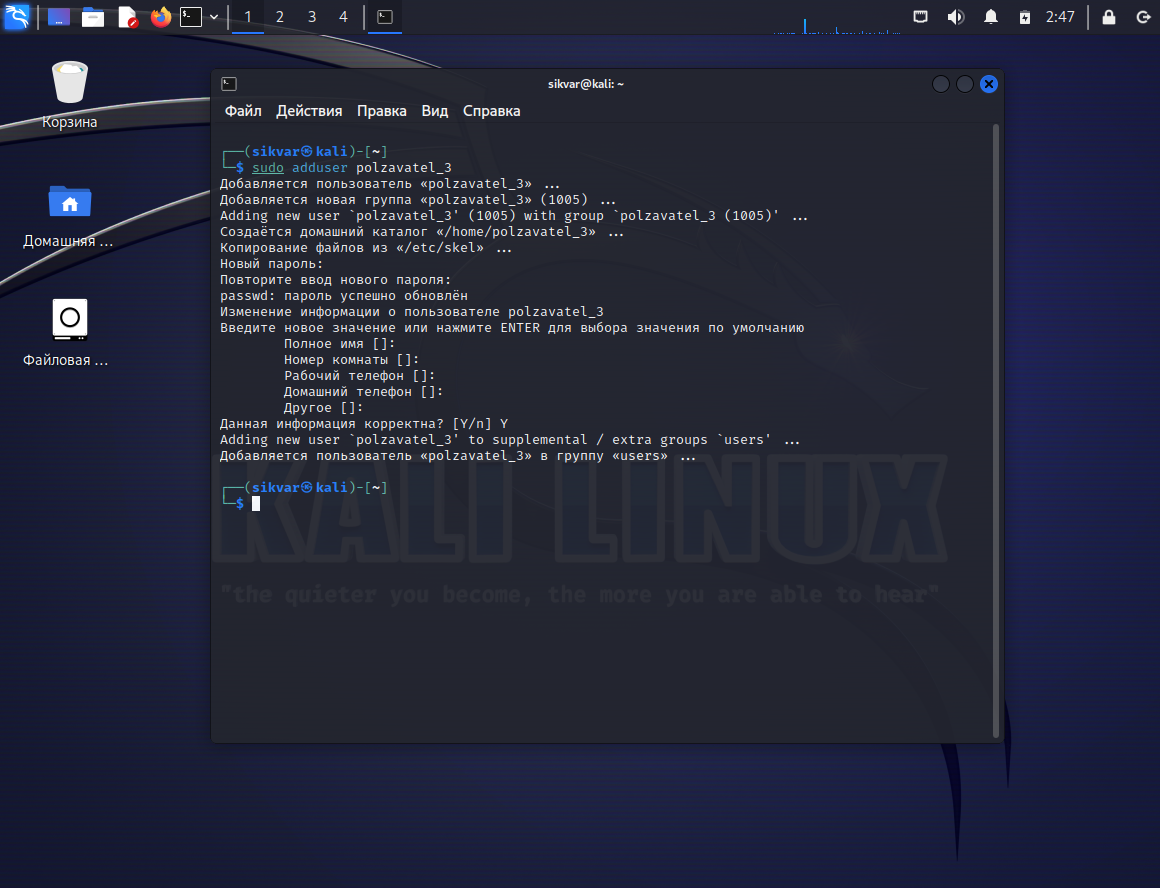
1.1 Пользователь 1



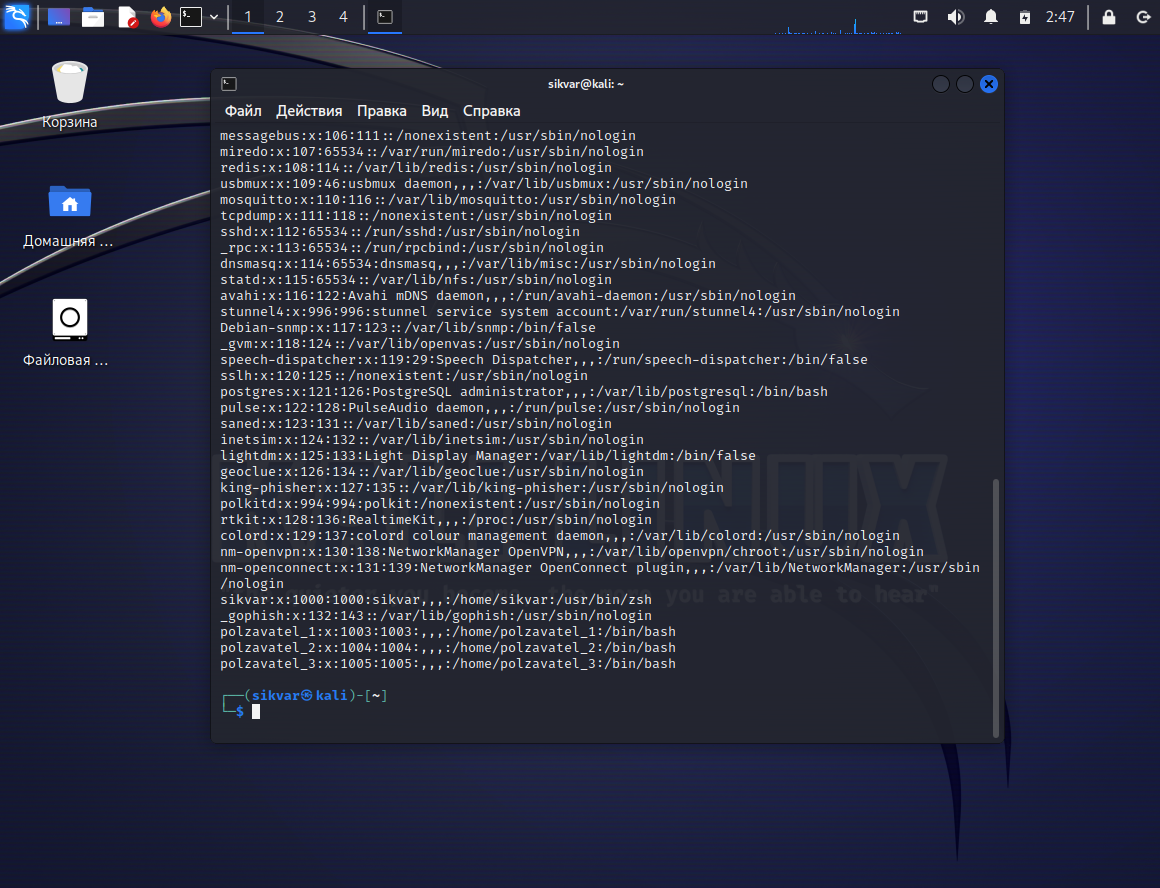
1.2 Пользователь 2



1.3 Пользователь 3

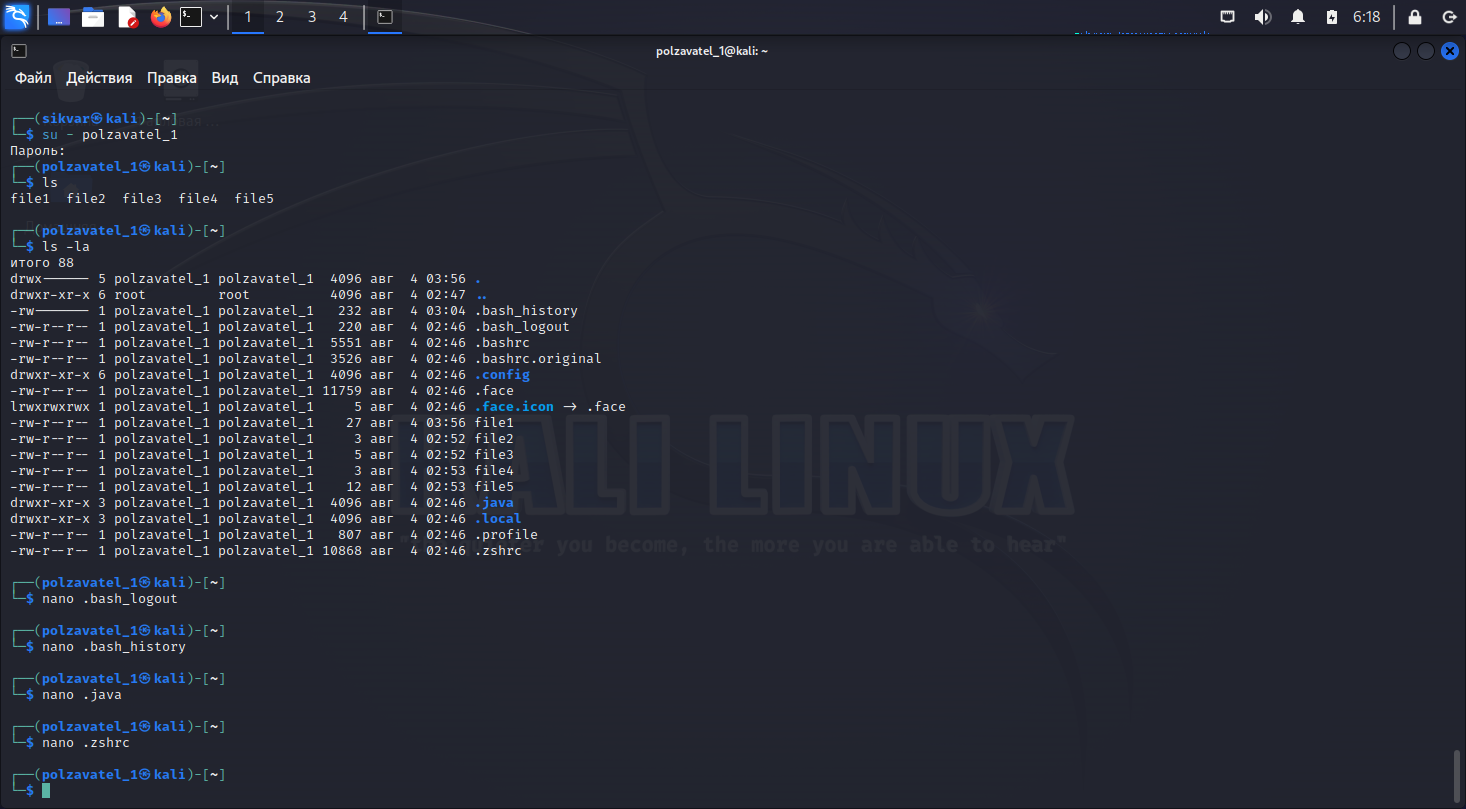


1.4 вывод cat /etc/sudoers

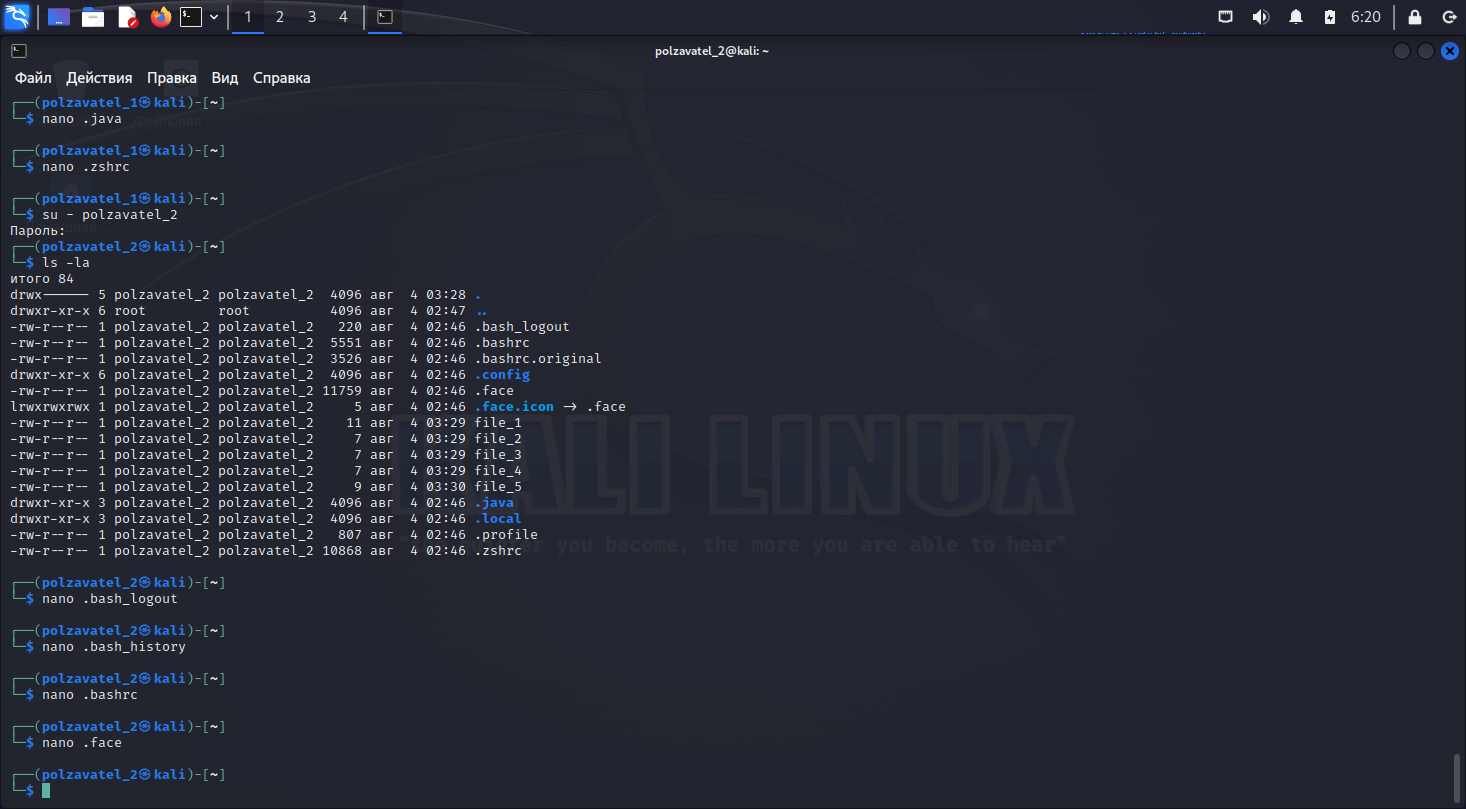


2 Открыл любые файлы от имени каждого пользователя.

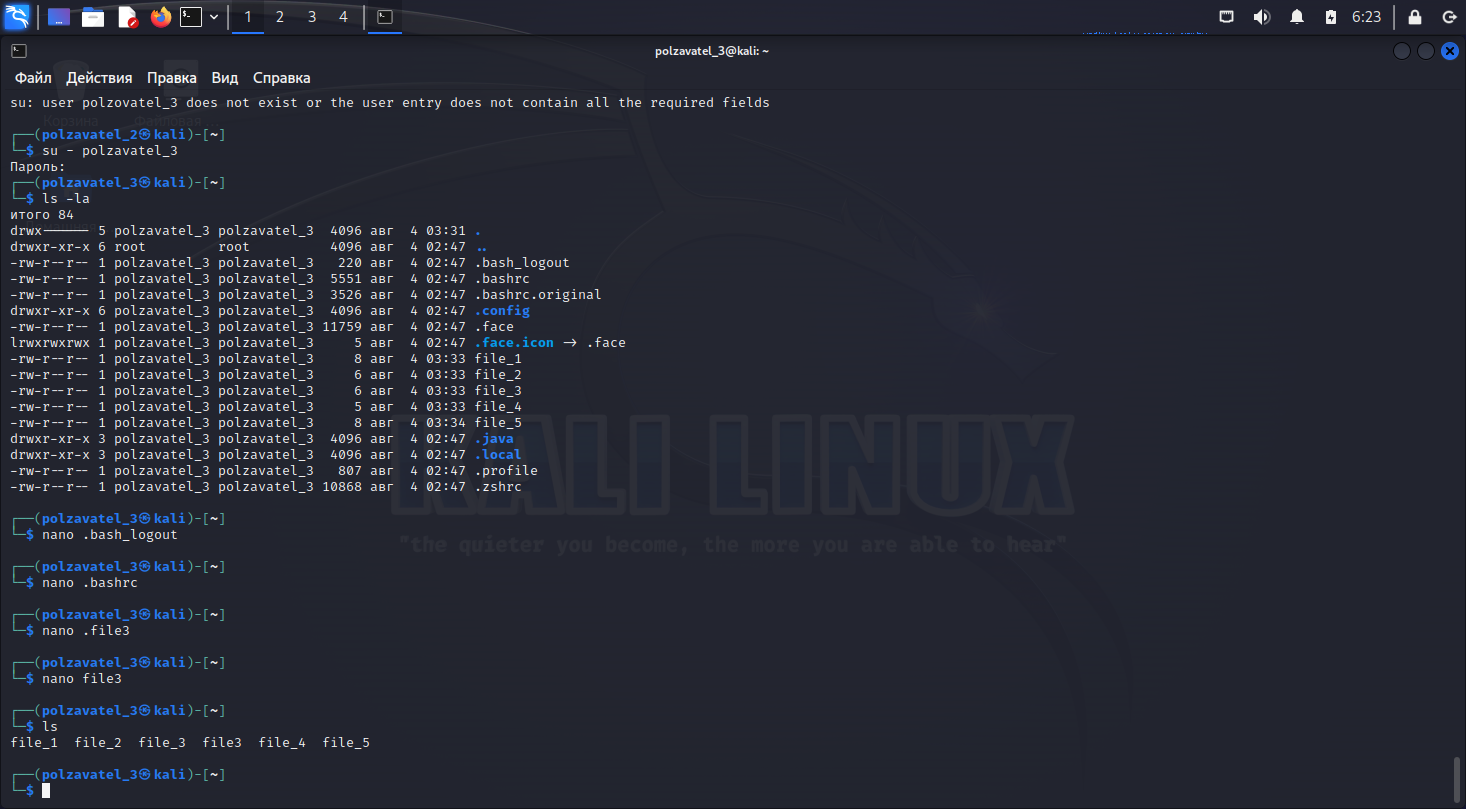
2.1 Открываем от пользователя 1



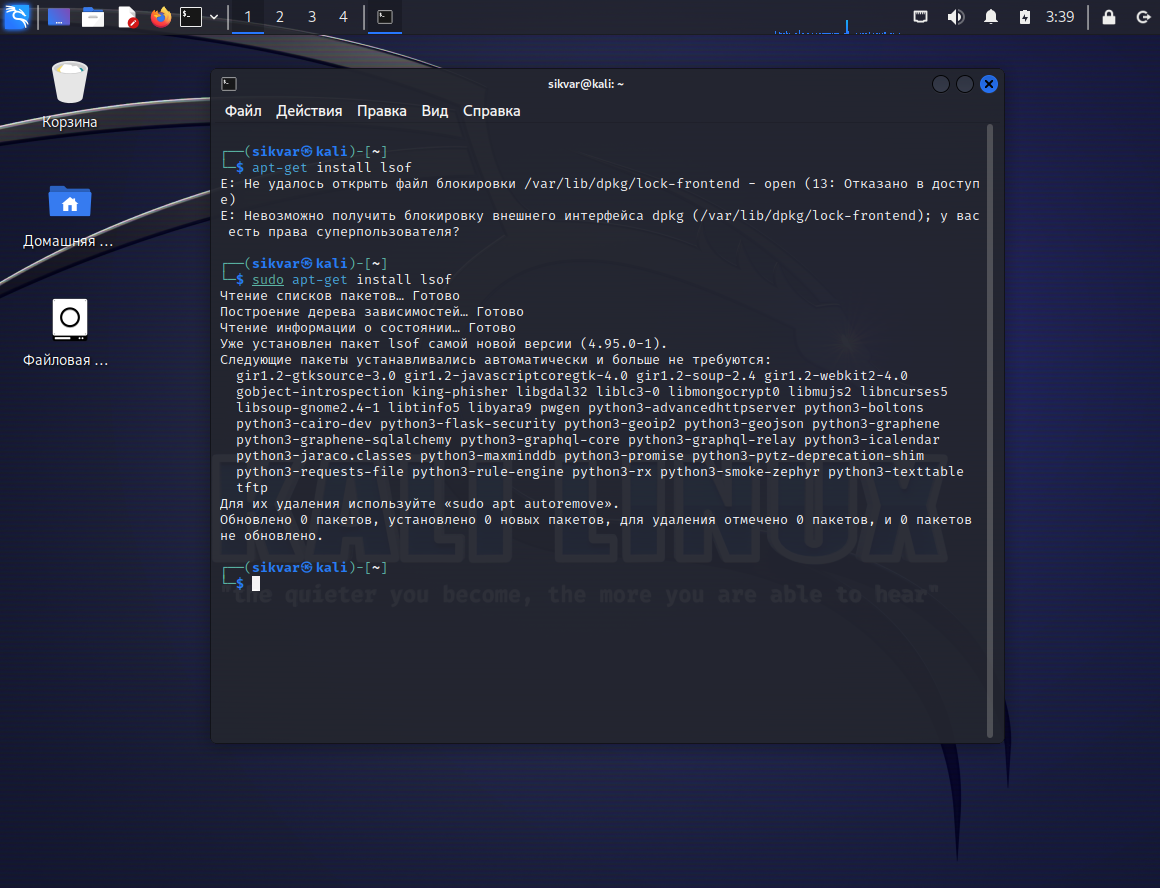
2.2 Открываем от пользователя 2



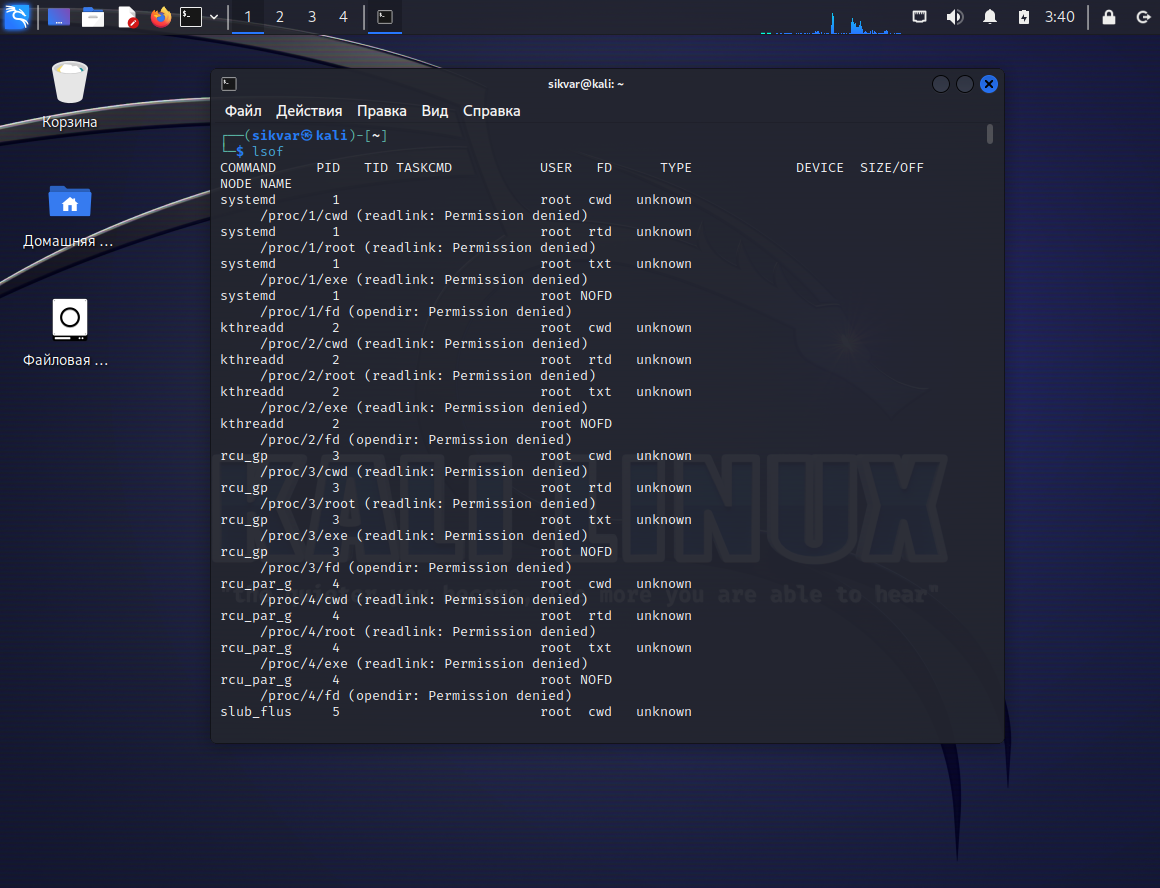
2.3 Открываем от пользователя 3



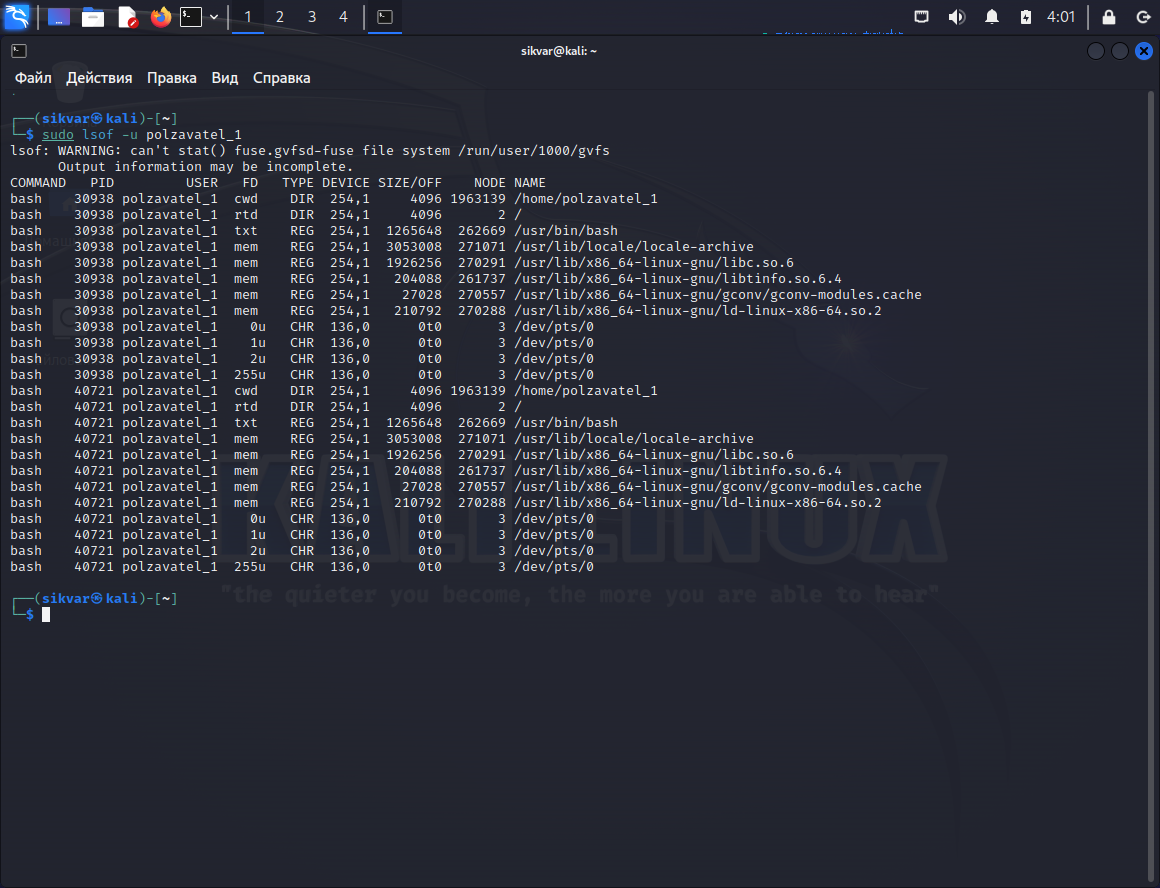
3. Утилита lsof была установлена.



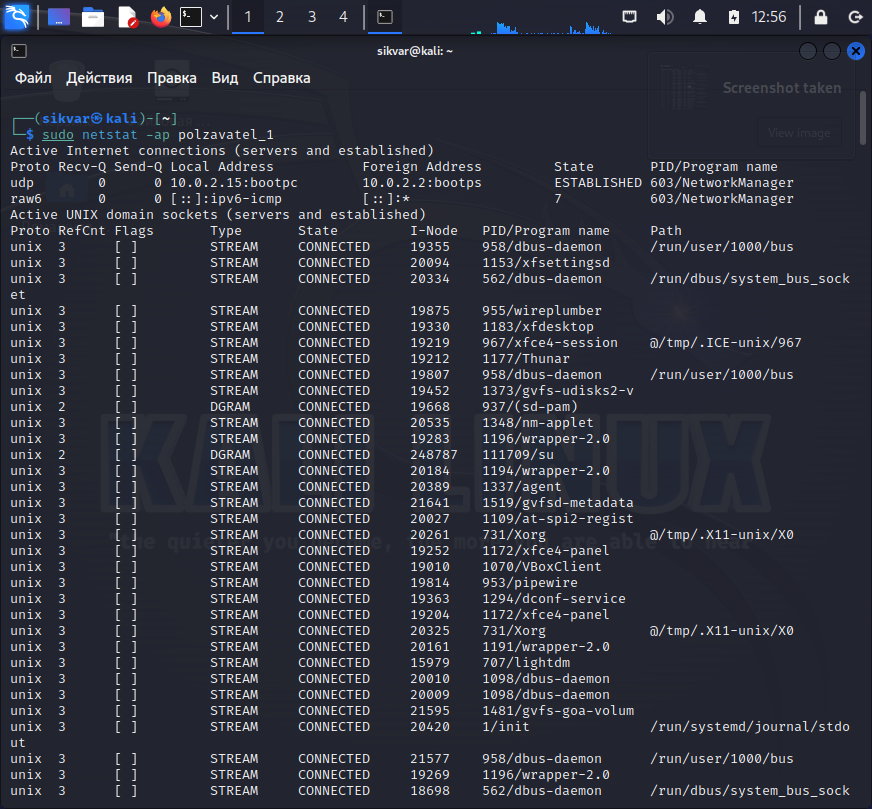
4. Открытые файлы в виде списка на экране.

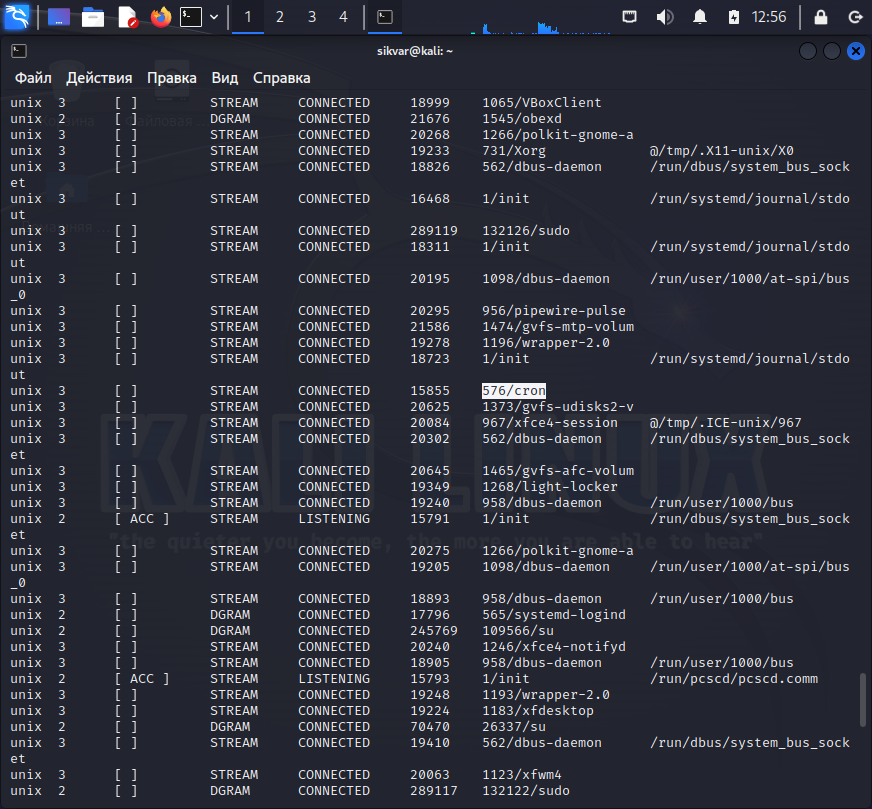


5. Так как под подозрение попал один сотрудник, вывел список всех открытых файлов пользователя.



6.

Вывожу список открытых сетевых сокетов, чтобы понять, через какое приложение с открытым портом мог пробраться злоумышленник.Команда sudo netstat -ap отображает информацию о всех активных сетевых соединениях на компьютере с помощью утилиты netstat. Она также отображает информацию об открытых портах и приложениях, которые используют эти порты.Команда -a показывает информацию обо всех открытых портах, включая те, которые не используются приложениями. Эта опция может быть полезна, если мы хотим проверить, какие порты открыты в нашей системе, но не хотите использовать -n для отображения только номеров портов.Опция -p показывает информацию только о тех портах, которые используются приложениями. Это может быть полезно, если мы хотим узнать, какие приложения используют определенные порты и как они работают.

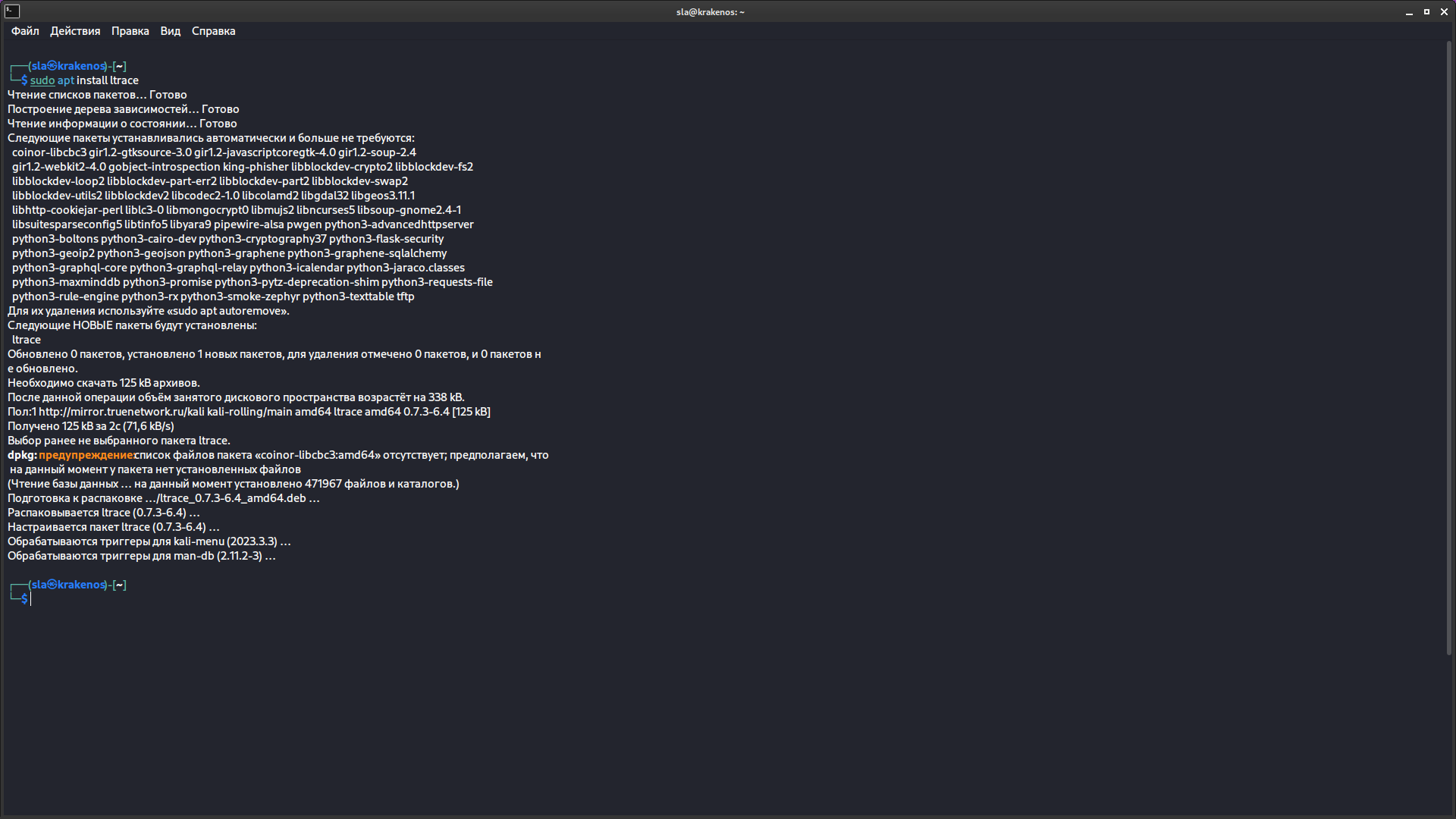


Мои предположения и аргументы:

Я считаю что это планировщик задач Cron. Т.к злоумышленник может использовать утилиту cron для первоначального или повторного выполнения вредоносного кода при закреплении в инфраструктуре, горизонтального распространения или для повышения привилегий.После получения доступа к операционной системе злоумышленник может закрепиться в ней и продолжить получать доступ к системе вне зависимости от прерываний доступа.

**Задание 2. Отображение вызовов приложений**

1.Установка утилиты ltrace



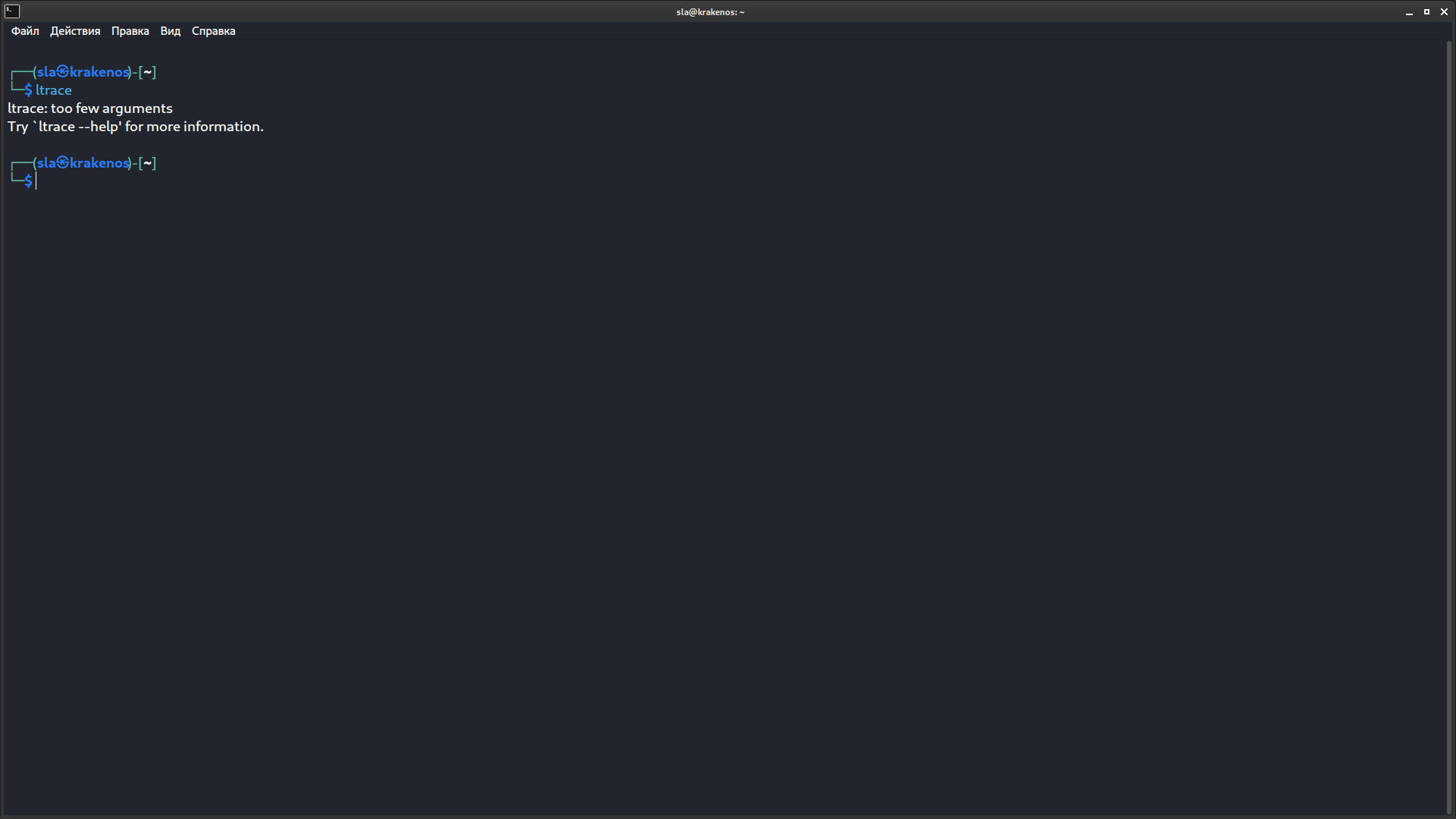
2.

Описание:

ltrace — это программа, которая просто выполняет указанную команду до завершения. Она перехватывает и записывает вызовы динамических библиотек, вызываемые исполняемым процессом, и сигналы, полученные этим процессом. Она также может перехватывать и печатать системные вызовы, выполняемые программой.

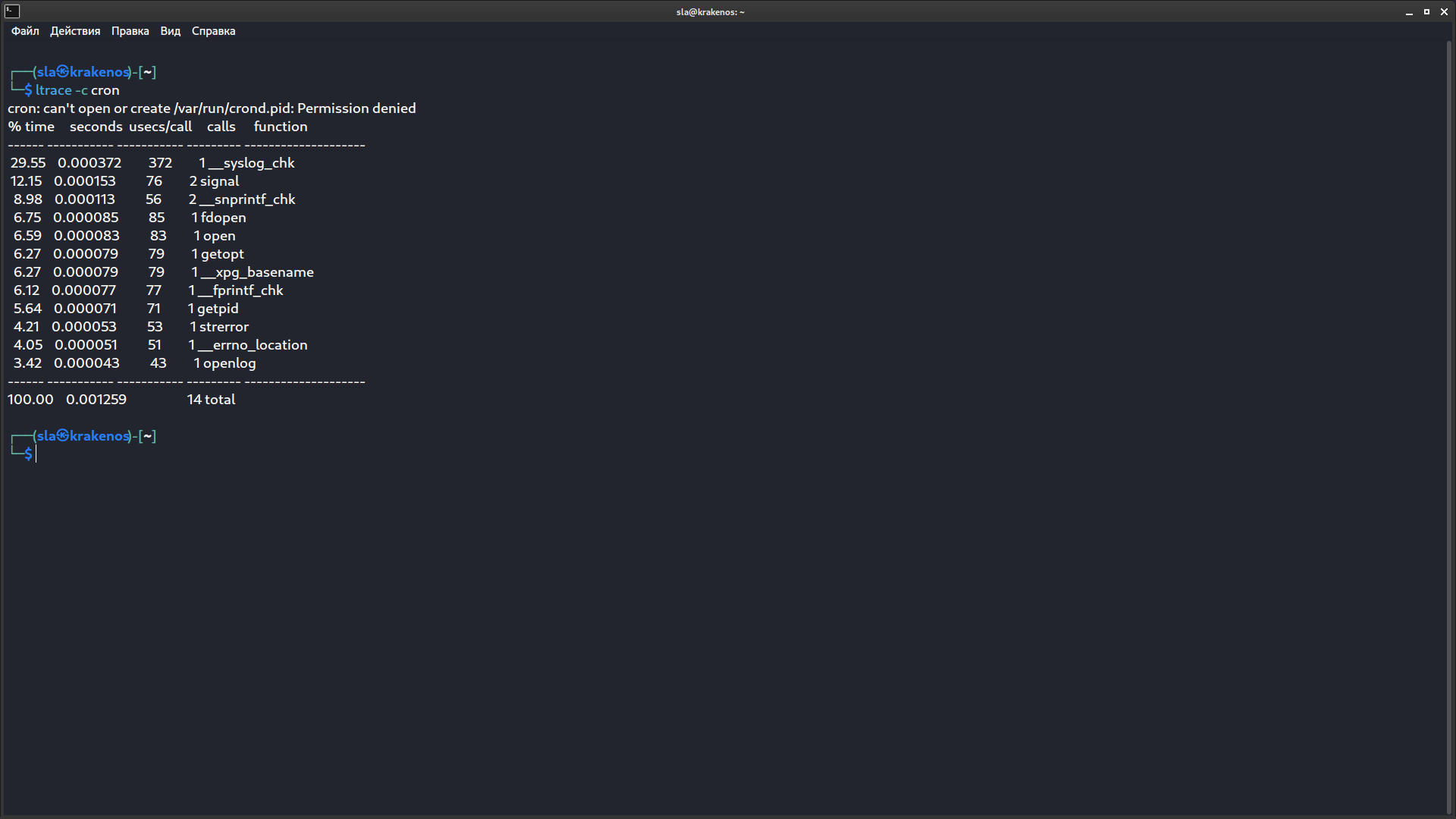
3.

При запуске утилиты был такой вывод:



3.1

Изучая трассируемый процесс более подробно,я получил полную таблицу всех системных вызовов, используемых процессом, включая ошибки. Это может быть очень полезно при сравнении нормально работающей системы с неисправной, позволяя быстро находить отличия в их поведении.Опция -с позволяет подсчитать время и вызовы для каждого обращения к библиотеке и сообщите сводку при выходе из программы.



##### 

##### 

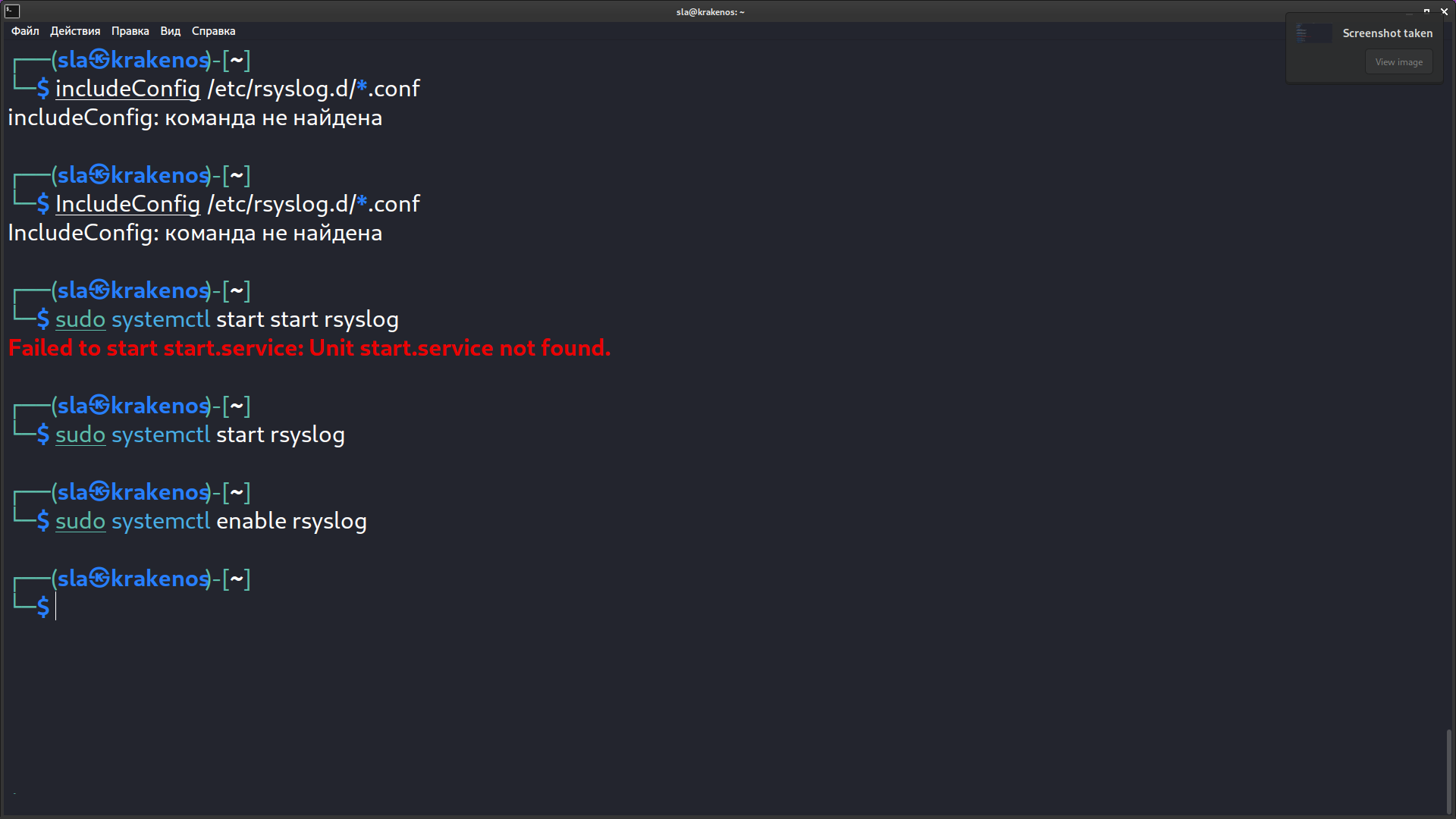
##### 

**Задание 3. Работа с логами**

1.Установил сервис rsyslog.

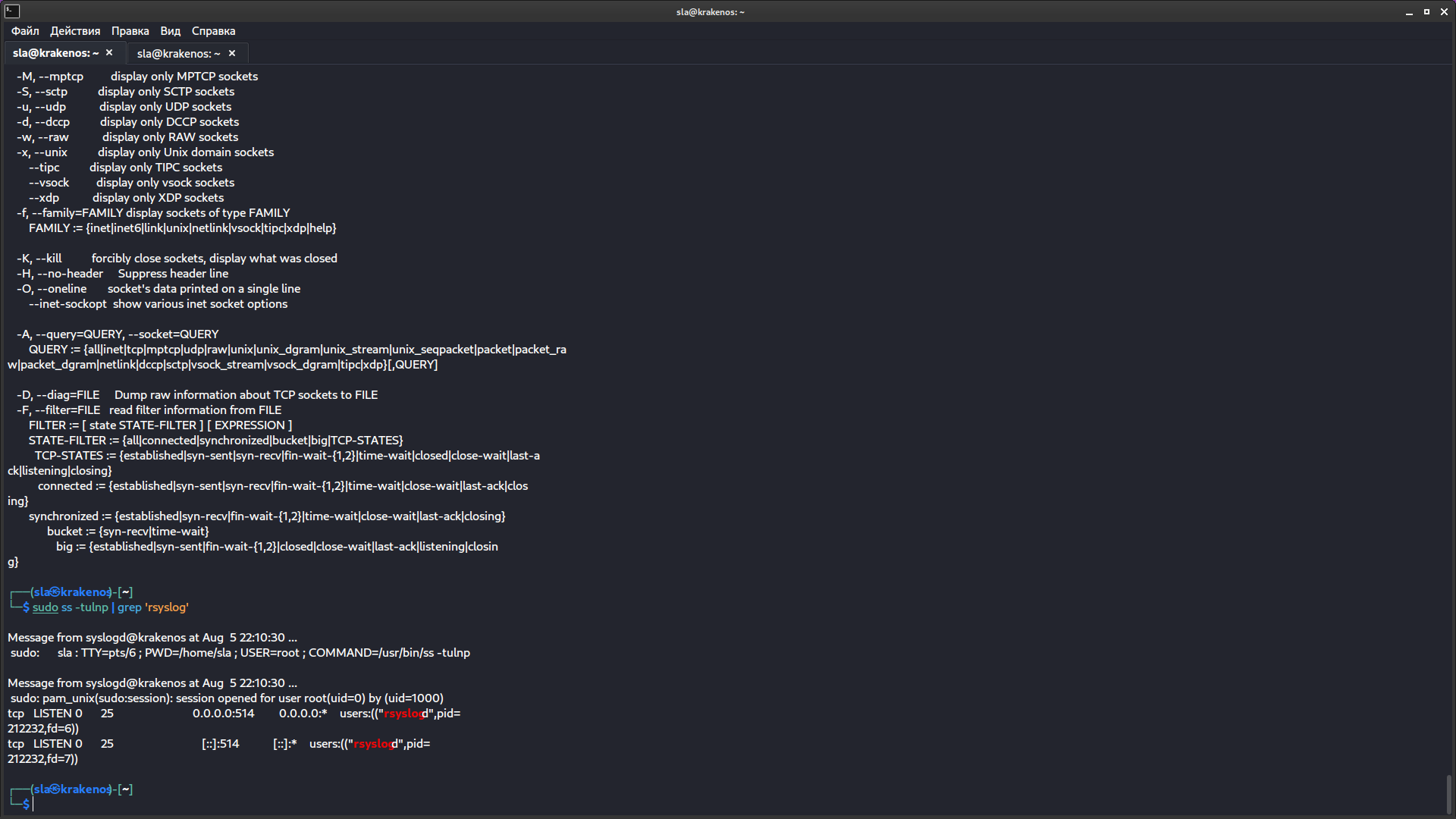


2.Запустил сервис. Убедился, что всё прошло успешно.





3.Настроил rsyslog и запустил его в работу.



4.Краткое пояснение о результатах запуска и о том, что выводится на экран.

После того как я добавил правило в /etc/rsyslog.conf

Правило→ \*. \* @@192.168.100.10:514

После этого произвел рестарт службы $sudo systemctl restart rsyslog

Далее требуется проверить сетевые сокеты rsyslog.

для этого я использовал $ sudo ss -tulpn | grep ‘rsyslog’

## 