Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Операционные системы»

Лабораторная работа № 2  
«Базовые приемы работы в с пользователями в ОС Linux»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Коротяев А.Н.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[Задание 1. 4](#_Toc130993769)

[1. Создание нового пользователя 4](#_Toc130993770)

[2. Изменение пароля для созданного пользователя 5](#_Toc130993771)

[3. Изменение первичной группы и места расположения домашнего каталога пользователя 5](#_Toc130993772)

[4. Создание новой группы 6](#_Toc130993773)

[5. Добавление пользователей в созданную группу 6](#_Toc130993774)

[6. Переключение на созданного пользователя 6](#_Toc130993775)

[7. Выполнение команд от лица суперпользователя 6](#_Toc130993776)

[8. Добавление пользователя в группу с повышенными привилегиями 7](#_Toc130993777)

[9. Выполнение команды от лица суперпользователя (добавление в группу sudo) 7](#_Toc130993778)

[10. Добавление пользователя в группу audio вручную 8](#_Toc130993779)

[11. Редактирование файла /etc/sudoers 8](#_Toc130993780)

[12. Разрешение на перезагрузку компьютера 9](#_Toc130993781)

[13. Изменение домашней директории на /usr/bin/nologin 9](#_Toc130993782)

[14. Работа с файлом shadow 10](#_Toc130993783)

[15. Использование *usermod -L* 10](#_Toc130993784)

[16. Удаление созданных пользователя и группы 11](#_Toc130993785)

[Задание 2 12](#_Toc130993786)

[1. Краткий обзор на возможности John the Ripper 12](#_Toc130993787)

[2. Перенос файлов */etc/passwd* и */etc/shadow* 12](#_Toc130993788)

[3. Формирование исходного файла для анализа 12](#_Toc130993789)

[4. Изучение файла словаря /etc/share/john/password.lst 13](#_Toc130993790)

[5. Процедура анализа паролей с использованием словаря паролей и модификаций по умолчанию 13](#_Toc130993791)

[6. Редактирование файла конфигураций, настройка собственных правил модификаций словаря паролей 14](#_Toc130993792)

[7. Процедура анализа паролей с использованием собственных правил 14](#_Toc130993793)

[Вывод 17](#_Toc130993794)

**Цель работы:** знакомство управлением пользователями в ОС Linux. Практическое применение теоретических знаний при работе с пользователями. Знакомство с утилитой *John the Ripper*.

**Ход работы:**

Комментарий: Лабораторная работа выполнена в ОС Kali Linux, установленной на виртуальной машине VMware Workstation. Выбор этого дистрибутива обусловлен упрощением решения некоторых поставленных задач (работа с John The Ripper). Пользователем по умолчанию установлен пользователь с логином *iankie*, имеющий права суперпользователя.

# Задание 1.

## Создание нового пользователя

Для создания нового пользователя воспользуемся командой *adduser user01:*

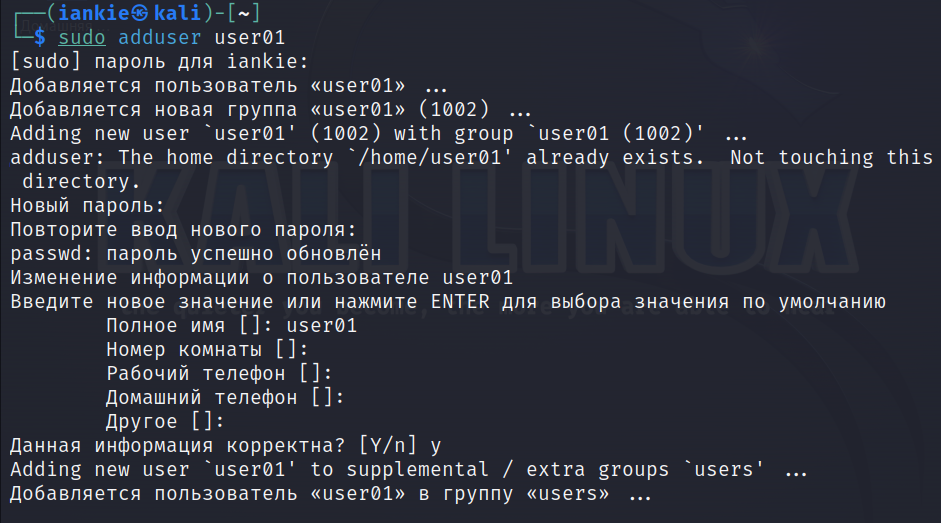
**

Рисунок 1. Создание нового пользователя

Команду следует вводить с приставкой *sudo* (если текущая сессия запущена не от лица суперпользователя), иначе можно получить следующее сообщение:

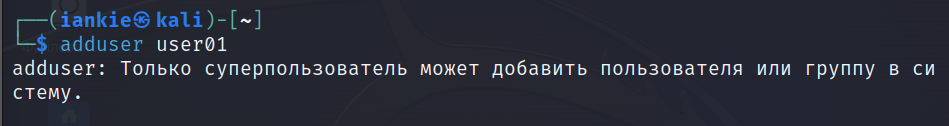


Рисунок 2. Возможная ошибка при создании нового пользователя

## Изменение пароля для созданного пользователя

Чтобы изменить пароль для существующего пользователя, нужно использовать команду *passwd user01* (вновь с приставкой *sudo*)*:*

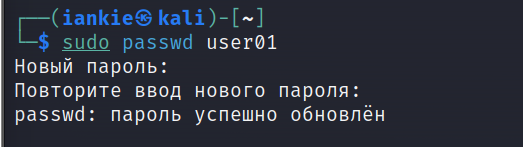
**

Рисунок 3. Изменение пароля пользователя

## Изменение первичной группы и места расположения домашнего каталога пользователя

Предварительно добавим директорию */home/user01home/*, которая будет использована при смене места расположения домашнего каталога.

Чтобы изменить первичную группу пользователя и место расположение его домашнего каталога нужно использовать следующую команду: *sudo usermod -g users -d /home/user01home/*:

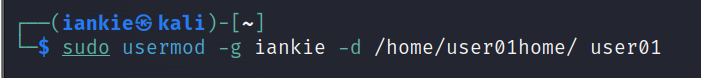


Рисунок 4. Изменение группы и домашнего каталога пользователя

Здесь:

*-g* – меняет первичную группу на указанную;

*-d* – меняет домашний каталог на указанный.

Проверим:

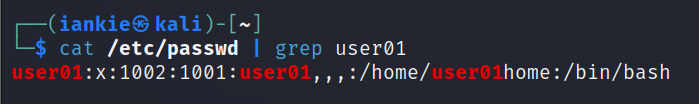


Рисунок 5. Результат изменений

## Создание новой группы

Чтобы создать новую группу, нужно использовать команду: *addgroup group01*

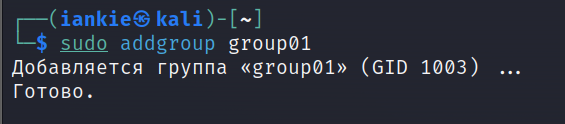


Рисунок 6. Создание новой группы

## Добавление пользователей в созданную группу

Чтобы добавить существующих пользователей в созданную группу (добавим пользователя *user01* в группу *group01*), нужно использовать команду: *usermod -a -G group01 user01*

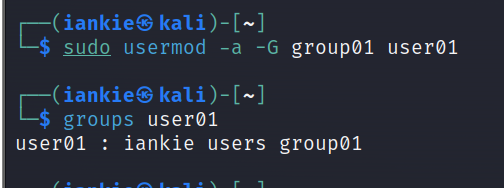


Рисунок 7. Добавление пользователя в группу

Здесь:

*-a* – добавляет пользователя в дополнительные группы, указанные в параметре -G, не удаляя пользователя из других групп;

*-G* – указание группы.

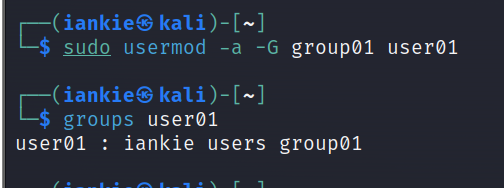


Рисунок 8. Результат

## Переключение на созданного пользователя

Используем команду su – user01, чтобы переключиться на созданного пользователя:

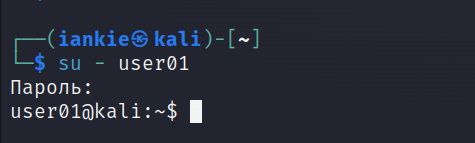


Рисунок 9. Переключение на пользователя user01

## Выполнение команд от лица суперпользователя

Попробуем выполнить любую команду от лица суперпользователя, например, *sudo ls:*

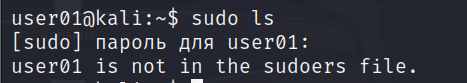


Рисунок 10. Выполнение команды от лица суперпользователя

Получаем ошибку: пользователя user01 нет в файле sudoers, что указывает на отсутствие у пользователя прав на исполнение команд от лица суперпользователя.

Выйдем из сессии *user01*.

## Добавление пользователя в группу с повышенными привилегиями

Один из способов дать определенному пользователю привилегии – это добавить его в группу, которая имеет эти привилегии. В ОС Kali Linux нет группы *wheel*, но есть группа *sudo*, которая обладает повышенными привилегиями. Попробуем добавить пользователя *user01* в эту группу. В сессии *root* выполним следующую команду:

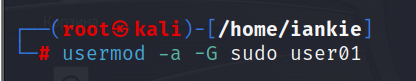


Рисунок 11. Добавление пользователя user01 в группу sudo

Результат:

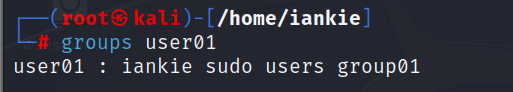


Рисунок 12. Результат выполнения команды

## Выполнение команды от лица суперпользователя (добавление в группу sudo)

Переключимся на пользователя *user01* и повторим попытку выполнить команду от лица суперпользователя:

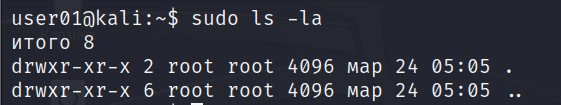


Рисунок 13. Выполнение команды от лица суперпользователя

Успешно.

## Добавление пользователя в группу audio вручную

В сессии суперпользователя выполним команду *nano /etc/group.* Открывается окно текстового редактора *nano* c содержимым файла */etc/group*. Находим строку с именем группы audio:

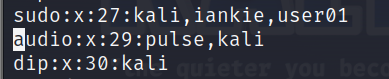


Рисунок 14. Группа audio

Добавляем через запятую пользователя user01, записываем изменения комбинацией клавиш Ctrl+O, подтверждая имя сохраняемого файла, и выходим из редактора комбинацией клавиш Ctrl+X. Проверяем результат:

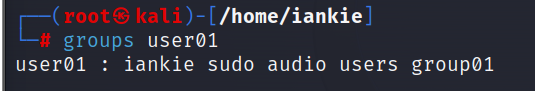


Рисунок 15. Группы пользователя user01

## Редактирование файла /etc/sudoers

Еще один способ повысить привилегии пользователя – это модифицировать файл */etc/sudoers*, прописав права в нем.

В сессии суперпользователя откроем для редактирования файл */etc/sudoers* в редакторе *nano.* Так как с повышением привилегий пользователя user01 все прошло успешно, для показательности произведенных действий создадим пользователя *user02*. Добавим строку *user02 ALL=(ALL) NOPASSWD: ALL:*

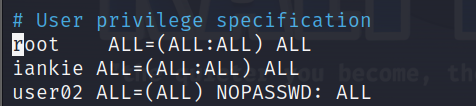


Рисунок 16. Редактирование файла /etc/sudoers

Сохраняем изменения в файле и выходим из редактора. Входим в сессию *user02* и пытаемся выполнить команду от лица суперпользователя:

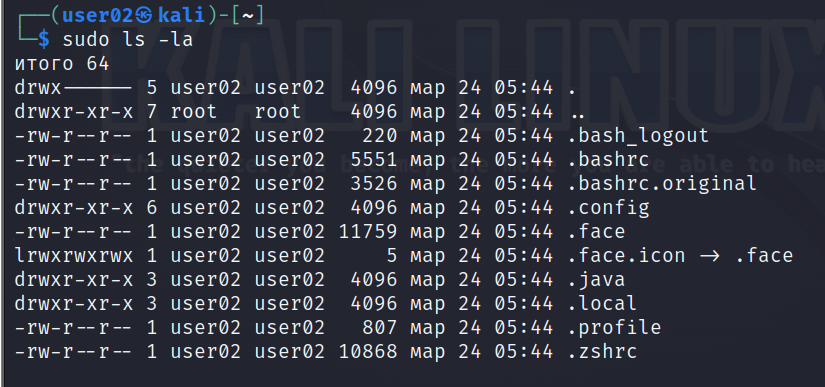


Рисунок 17. Выполнение команды от лица суперпользователя (user02)

## Разрешение на перезагрузку компьютера

В файле sudoers можно прописать права для управления командой *reboot*, которая позволяет перезагрузить компьютер.

Для этого создадим командный алиас файле *sudoers*:

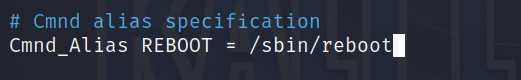


Рисунок 18. Создание командного алиаса

Теперь нужно прописать спецификацию привилегий для пользователя (*user01*):

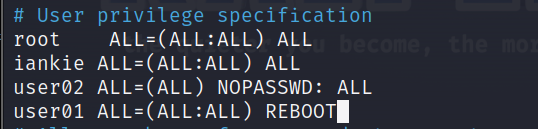


Рисунок 19. Спецификации привилегий пользователя user01.

Еще один вариант разрешить пользователю перезагружать компьютер, прописав в спецификациях привилегий слово ALL вместо алиаса REBOOT.

## Изменение домашней директории на /usr/bin/nologin

В ОС Kali Linux нет файла */usr/bin/nologin*, вместо него используется */sbin/nologin.* В файле */etc/passwd* изменить домашнюю директорию пользователя user01 на */sbin/nologin*:

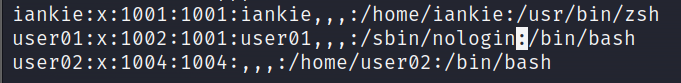


Рисунок 20. Изменение домашней директории на /sbin/nologin пользователя user01

Попытаемся войти от лица пользователя user01:

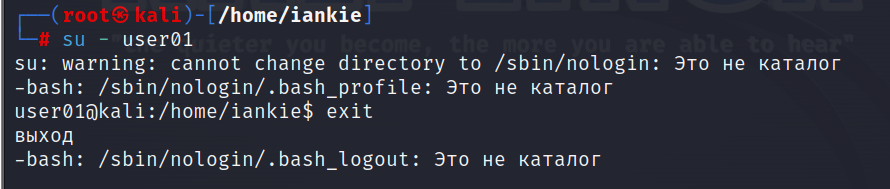


Рисунок 21. Вход от лица пользователя user01

Выведена очевидная ошибка открытия директории */sbin/nologin*, потому что это не директория, а программа.

## Работа с файлом shadow

Файл */etc/shadow* используется для хранения паролей всех существующих в системе пользователей.

Строку с пользователем *user01* можно получить следующей командой:

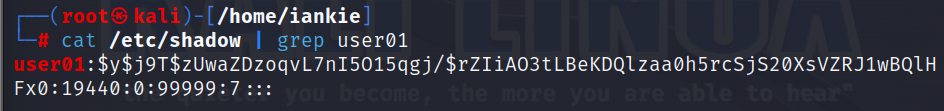


Рисунок 22. Файл /etc/shadow

Если обратить внимание на хэш пароля, то в начале можно обнаружить следующее: *$y$.* Это начало указывает на тип хэша, в данном случае это *yescript.*

## Использование *usermod -L*

Команда *usermod* с параметром *-L* блокирует указанную учетную запись.

После введения команды *usermod -L user01* в файле */etc/shadow* строка с именем *user01* изменилась:

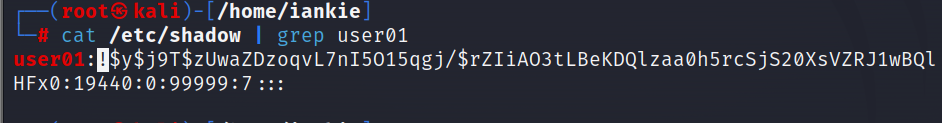


Рисунок 23. Изменение строки с пользователем user01

Появился спецсимвол «!», который свидетельствует о том, что учетная запись заблокирована. Попробуем войти в учетную запись:

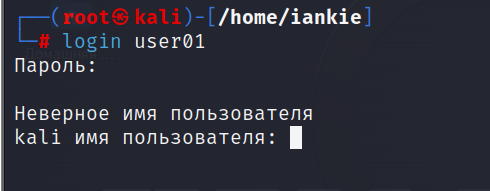


Рисунок 24. Попытка входа под пользователем user01

Войти не получится, потому что спецсимвол «!», который появился в результате команды *usermod -L*, запрещает нам использовать пароль для аутентификации под пользователем *user01* – это и есть блокировка учетной записи (невозможность войти под установленным паролем).

## Удаление созданных пользователя и группы

Чтобы удалить созданных ранее пользователей, воспользуемся командой *deluser* *user01* и *deluser user02*:

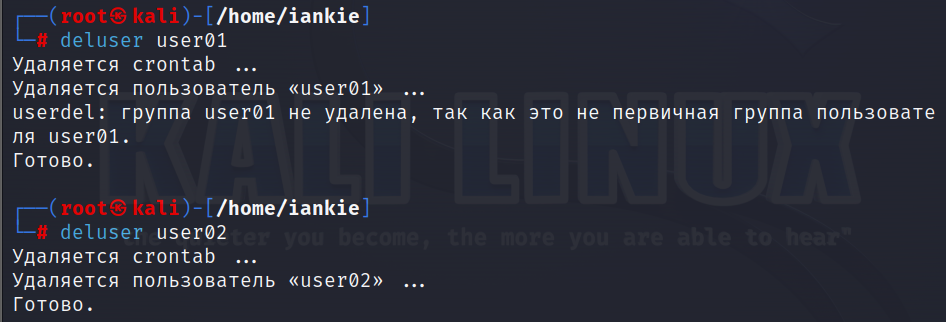


Рисунок 25. Удаление пользователей

Чтобы удалить созданную ранее группу, воспользуемся командой *delgroup group01:*

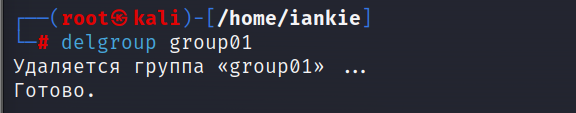
**

Рисунок 26. Удаление группы

# Задание 2

## Краткий обзор на возможности John the Ripper

John the Ripper – сложный и мощный инструмент, в первую очередь используемый для взлома паролей (тестирования безопасности паролей), а также для восстановления утерянных паролей. Может использовать в своей работе несколько методов, например, атаки по словарю (метод грубой силы – «brute force»), атаки на базы паролей (база MD5, SHA-1, SHA-256 хэшей) и другие. Есть возможность анализировать словари и списки паролей на наиболее часто используемые пароли и создавать соответствующие сценарии атак.

## Перенос файлов */etc/passwd* и */etc/shadow*

Скопируем (именно скопируем, а не перенесем) файлы */etc/passwd* и */etc/shadow* в отдельную папку /home/iankie/analys

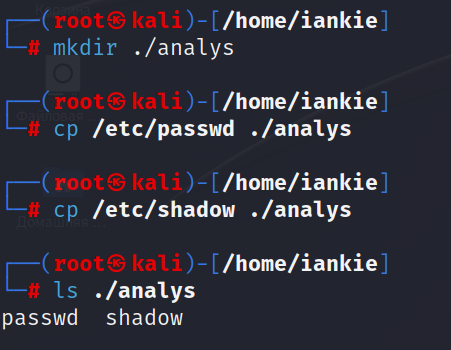
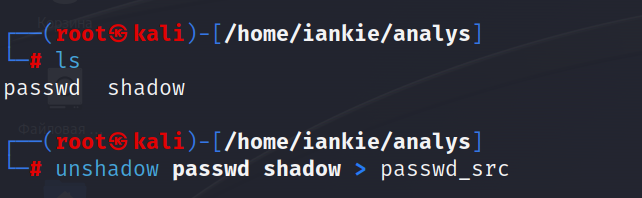


Рисунок 27. Перенос файлов /etc/passwd и /etc/shadow

## Формирование исходного файла для анализа

Сформируем исходный файл для анализа, используя команду *unshadow*



Команда unshadow объединяет файлы passwd и shadow в один файл с зашифрованными паролями пользователей.

## Изучение файла словаря /etc/share/john/password.lst

Изучим файл словаря /etc/share/john/password.lst

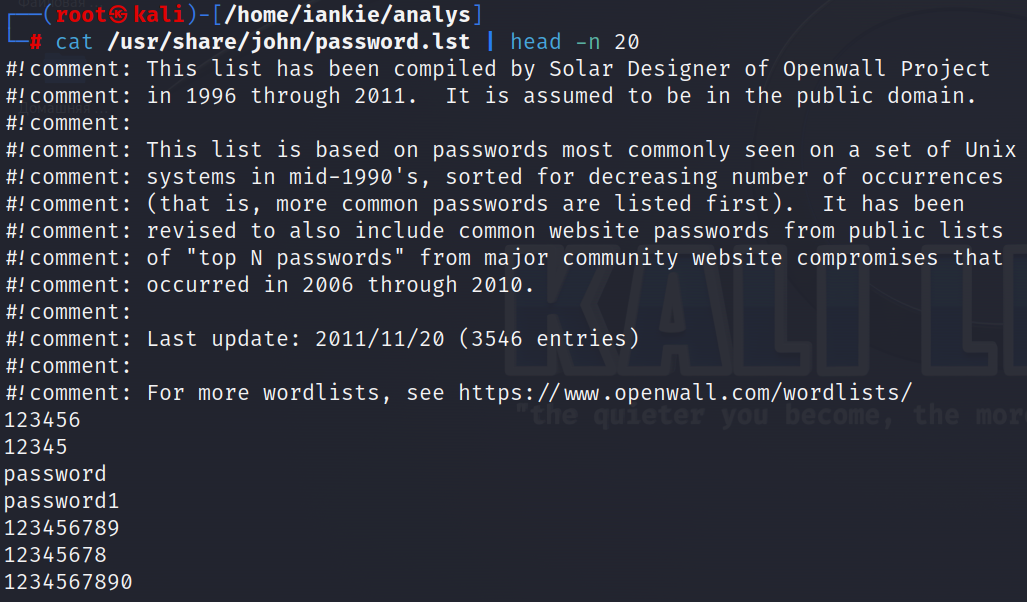


Рисунок 28. Содержимое файла словаря /etc/share/john/password.lst

Файл содержит 3559 строк наиболее распространенных паролей. Первые строки содержат информацию о создателе и том, где можно получить еще словари.

## Процедура анализа паролей с использованием словаря паролей и модификаций по умолчанию

Выполняем следующую команду для анализа паролей:

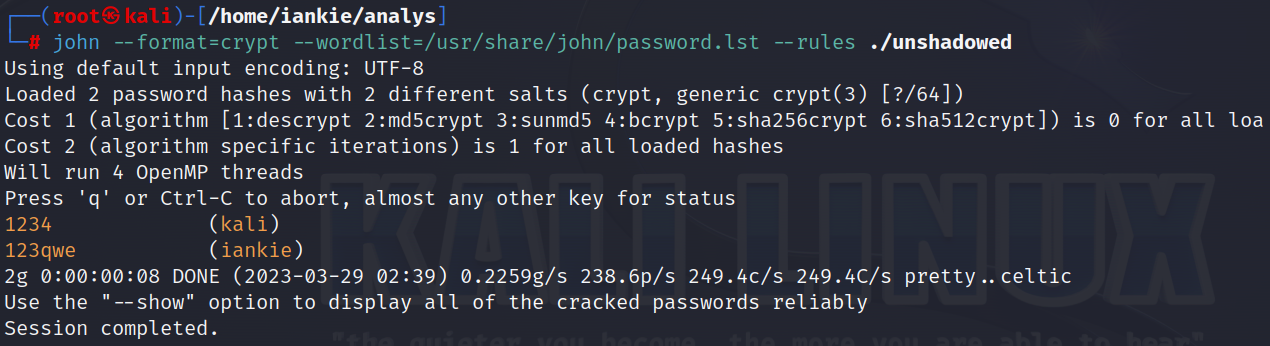


Рисунок 29. Анализ паролей с использованием словаря и их модификаций по умолчанию

Важно отметить, что указание параметра *--format=crypt* – обязательно, в противном случае программа не будет работать.

Этим параметром мы отправляем формат хэша (yescrypt) программе.

Примерная продолжительность работы программы – 8 секунд.

## Редактирование файла конфигураций, настройка собственных правил модификаций словаря паролей

Откроем для редактирования файл */etc/john/john.conf* и найдем строку «*# Single crack mode rules*»:

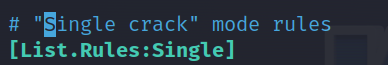


Рисунок 30. Строка с правилами модификации по умолчанию

Над этими строками создаем аналогичную секцию (*Study*) для собственных правил и регистрируем два правила:

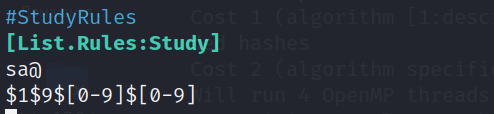


Рисунок 31. Создание собственной секции регистрация правил

## Процедура анализа паролей с использованием собственных правил

Важно отметить, что если проводить процедуру на том же файле (то есть анализировать те же хэши), программа выдаст следующее сообщение:

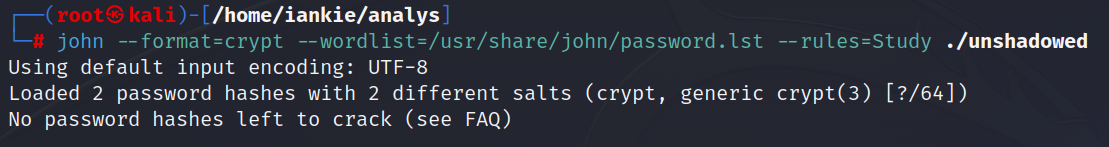


Рисунок 32. Вариант ответа программы

Это значит, что пароли по этим хэшам вычислены, и John the Ripper отказывается делать это снова. Поэтому для показательности действенности второго метода, меняем пароли у двух учетных записей *kali* и *iankie* на новые, вновь производим процедуру unshadow, а затем уже переходим к анализу:

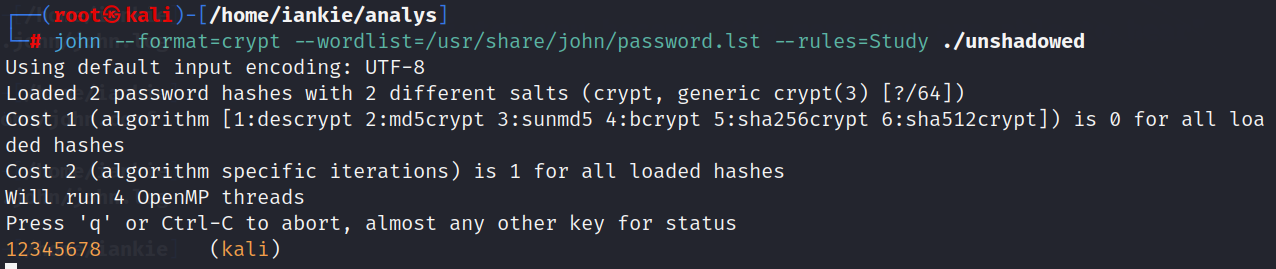


Рисунок 33. Анализ паролей

Анализ производится сильно дольше, чем в предыдущем способе. На момент принудительного завершения программы время работы составляло почти 25 минут. Был вычислен пароль для пользователя *kali.*

Изменим правило:

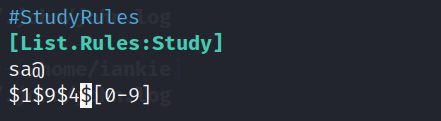


Рисунок 34. Изменение правила в файле конфигураций

Заново запустим программу:

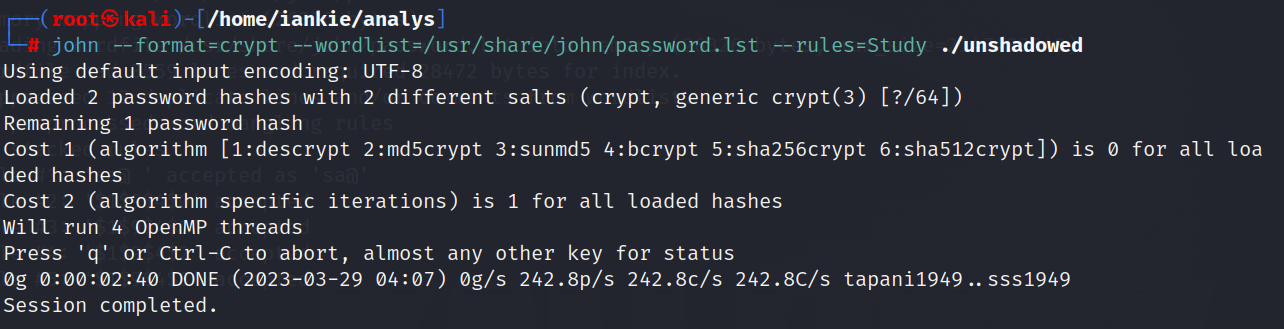


Рисунок 35. Повторный анализ паролей с измененным правилом

Так как пароль для пользователя kali программа уже вычислила, она выдает предупреждение: «Remaining 1 password hash» - остался один хэш пароля, который еще не вычислен.

Программа не смогла вычислить пароль для пользователя *iankie* («123qwerty»).

Изменим словарь на знаменитый «*rockyou*» и повторим попытку:

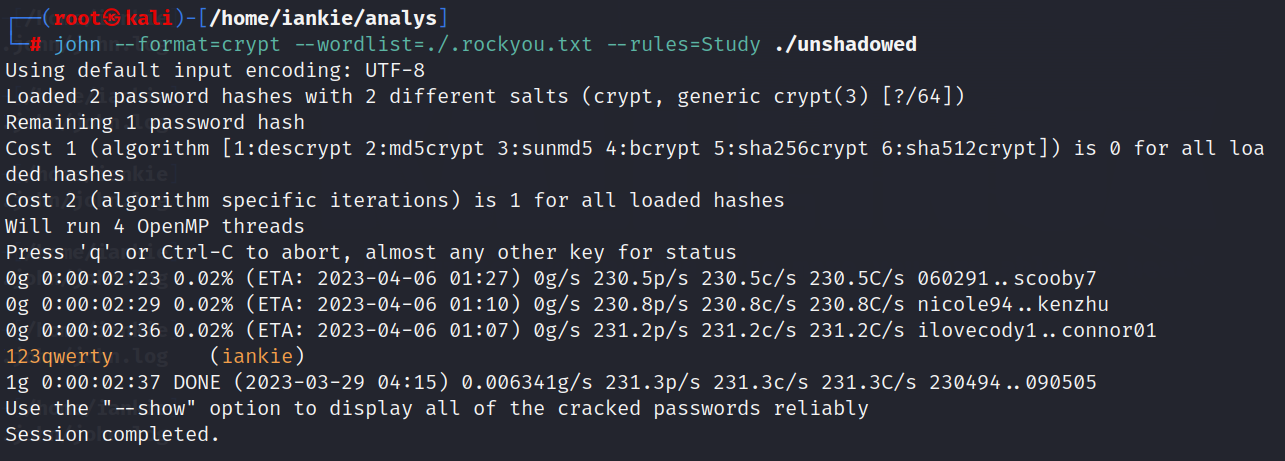


Рисунок 36. Повторный анализ паролей с другим словарем

В этом случае программе понадобилось почти 3 минуты, чтобы с указанным правилом и словарем «*rockyou*» вычислить пароль для пользователя *iankie.*

Вывод:

Если использовать популярный пароль, то время, потраченное на его вычисление, измеряется в секундах. Если использовать менее популярный пароль, то без настроенных правил пароль вычислить будет сложнее – увеличится время, уменьшится шанс успешного вычисления. Настроенные правила (в том числе маска) увеличивает шансы на успешное вычисление пароля за меньшее время.

# Вывод

В ходе выполнения первой части лабораторной работы были освоены базовые навыки управления пользователями и группами в ОС Linux на примере дистрибутива Kali Linux. Практически закреплены умения: добавлять, удалять, модифицировать учетные записи, к примеру, менять пароль пользователя, перемещать пользователей между группами, присваивать права на такие действия в системе, как завершение работы или перезагрузка системы, выполнение действий от лица суперпользователя. Было изучено, где находятся данные пользователя, в том числе хэши паролей пользователей.

В ходе выполнения второй части лабораторной работы были освоены навыки работы с утилитой *John the Ripper*. Было произведено несколько анализов паролей, хэши которых находятся в файле *shadow*:

* со словарем по умолчанию и правилами по умолчанию
* со словарем по умолчанию и настроенными правилами
* со словарем *rockyou* и настроенными правилами

Сделан вывод по итогам проведения разных анализов.