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   
«Криптографические методы защиты информации»

Лабораторная работа №8  
«*Kerberos*. Настройка и организация связи.»

Студенты: Клоченко И.Е.

Преподаватель: Соколов И.П.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[Ход работы 3](#_Toc136525011)

[Вывод 15](#_Toc136525012)

[Контрольные вопросы 16](#_Toc136525013)

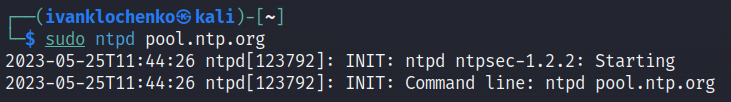
**Цель работы:**

Знакомство с Kerberos.

## Ход работы

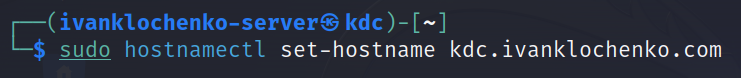
* 1. В лабораторной работе используется образ виртуальной машины *Kali* *Linux* с учетными записями *ivanklochenko* и *ivanklochenko*-*server* для машины клиента и машины сервера соответственно.
  2. Выполняем синхронизацию времени на обоих машинах.

Для этого на обоих машинах используем дефолтный сервер *pool*.*ntp*.*org* для синхронизации через *NTP*.



**Рисунок 1**. Синхронизация часов с сервером NTP на машине клиента

* 1. Задаем новое сетевое имя на серверной машине.

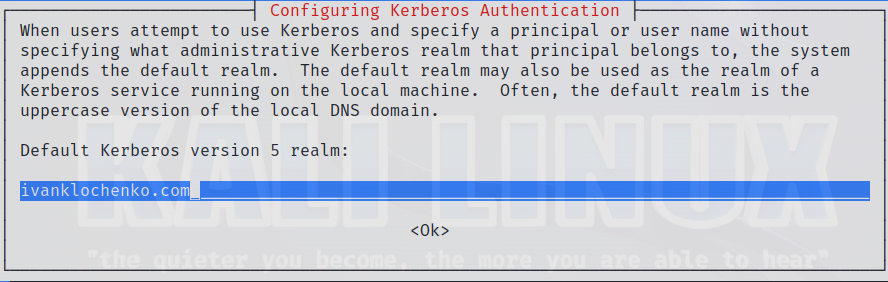


**Рисунок 2**. Задание нового сетевого имени на серверной машине

В качестве домена 2 уровня я использовал свои имя и фамилию.

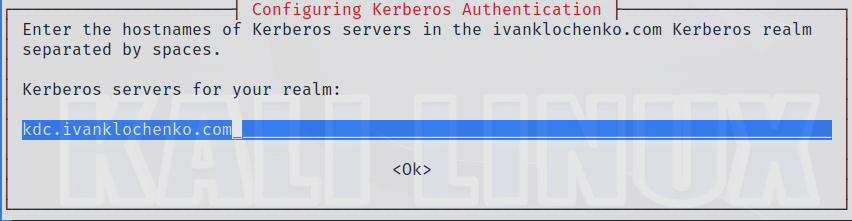
* 1. Устанавливаем пакеты *krb*5-*kdc* и *krb*5-*admin*-*server* на серверной машине.

Во время установки указываем область *Kerberos* по умолчанию.



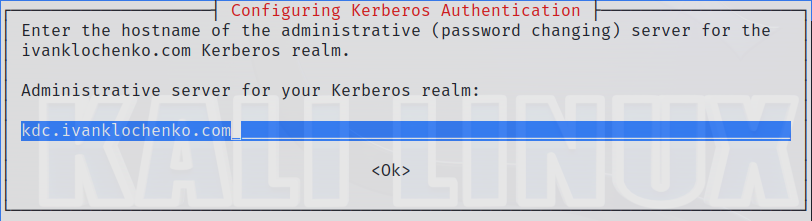
**Рисунок 3**. Область Kerberos по умолчанию

Далее в качестве сервера *Kerberos* для созданной на предыдущем этапе области указываем уже использовавшееся имя *kdc*.*ivanklochenko*.*com*.



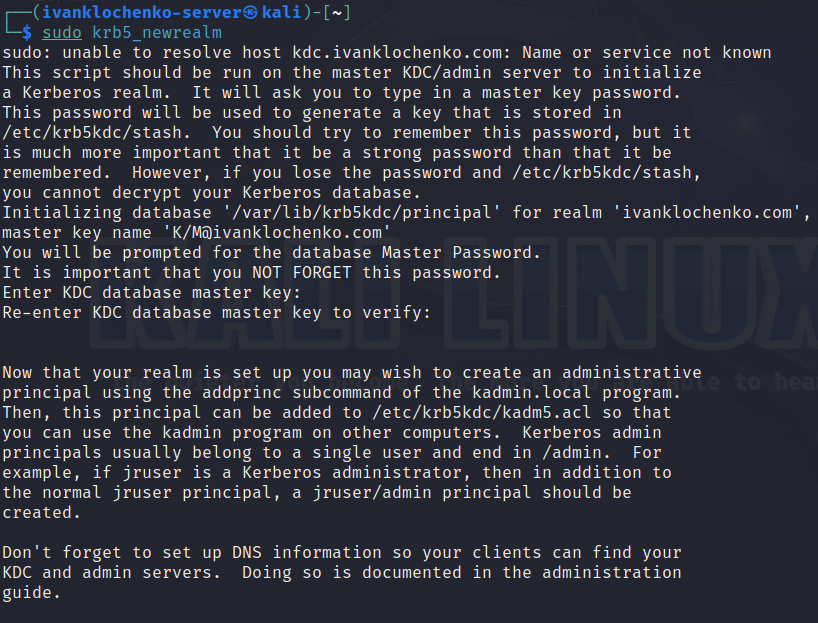
**Рисунок 4**. Установка сервера Kerberos для созданной области

Далее указываем управляющий сервер для области *Kerberos*.



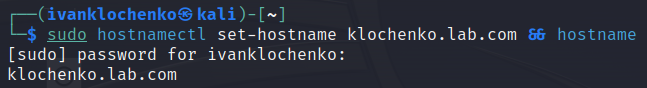
**Рисунок 5**. Указание управляющего сервера для созданной области Kerberos

* 1. Создаем новую область *Kerberos*.



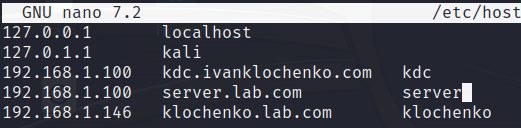
**Рисунок 6**. Создание новой области Kerberos

* 1. Переходим к настройке клиентской машины. Задаем новое сетевое имя. Использую имя и фамилию в названии.



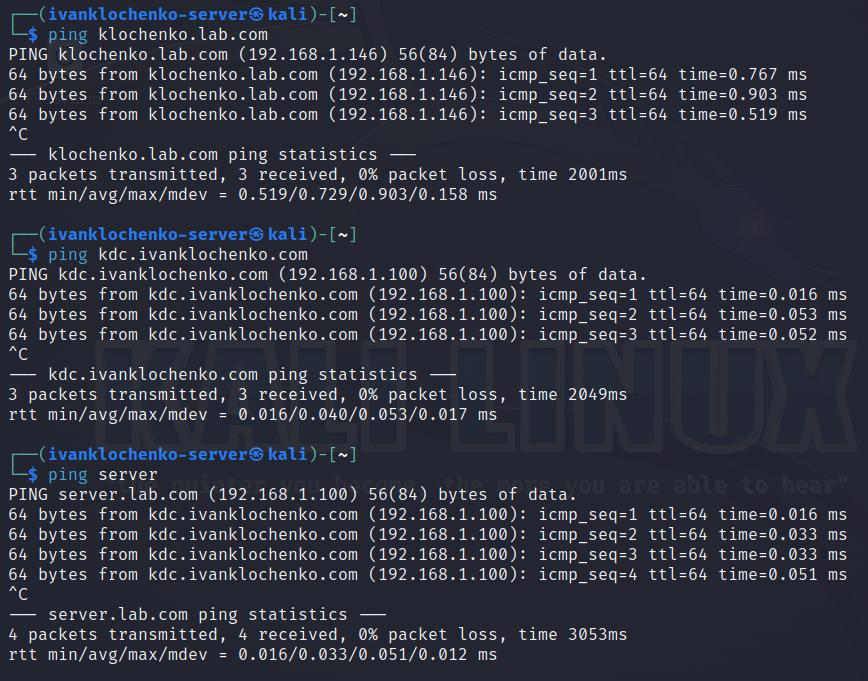
**Рисунок 7**. Задание сетевого имени на клиентской машине

* 1. Просматриваем *IP* адреса клиентской и серверных машин. Затем на серверной машине редактируем файл хостов /*etc*/*hosts*/ внеся данные о новых сетевых именах и *IP* адресах машин.



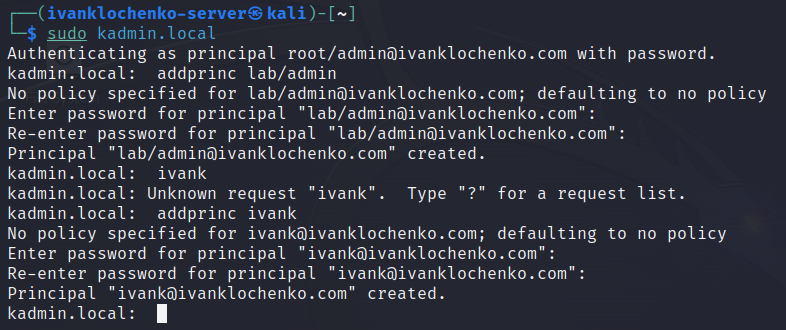
**Рисунок 8**. Редактирование файла с хостами на серверной машине

* 1. Проверяем связь доменных имен с *IP* адресами, выполнив команду *ping*.



**Рисунок 9**. Проверка между хостами

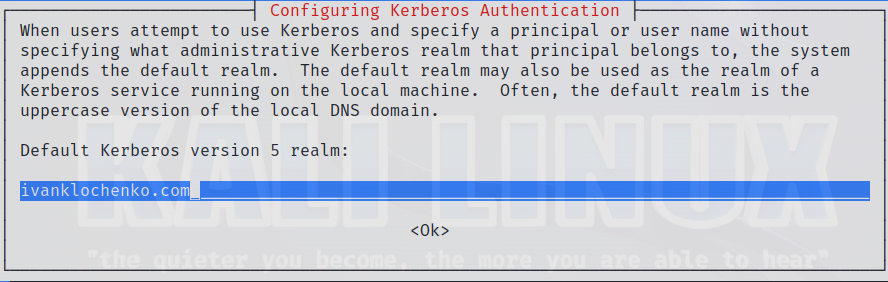
* 1. Создаем пользователей *lab*/*admin* и *ivanklo*.



**Рисунок 10**. Создание пользователей в области lab.ivanklochenko.com

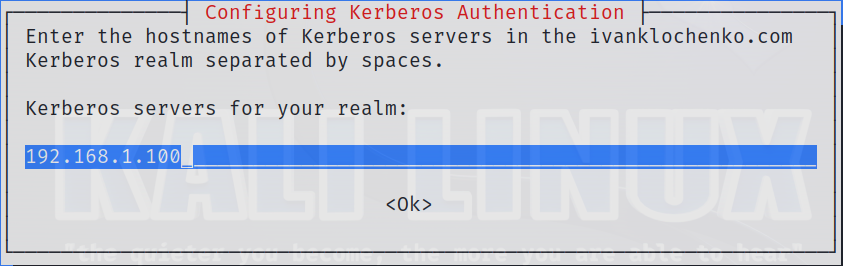
* 1. Переходим к настройке клиентской машины. Установим дополнительные компоненты *krb*5-*user*, *libpam*-*krb*5, *libpam*-*ccreds*, *auth*-*client*-*config* (нет такого пакета).

Указываем название области.



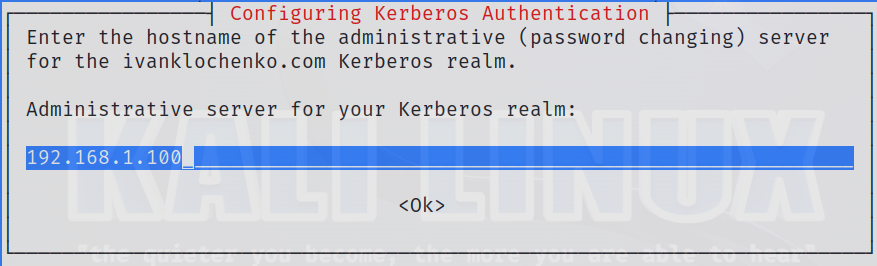
**Рисунок 11**. Задание названия области Kerberos

Указываем *IP* адрес сервера.



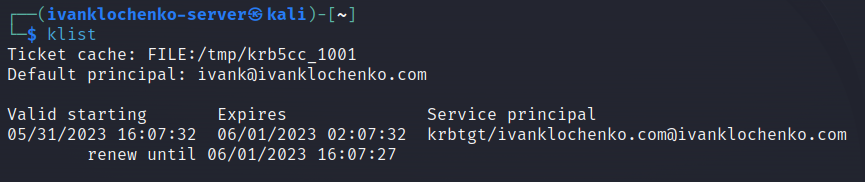
**Рисунок 12**. Указание IP сервера Kerberos

Указываем *IP* адрес управляющего сервера.



**Рисунок 13**. Указание IP управляющего сервера Kerberos

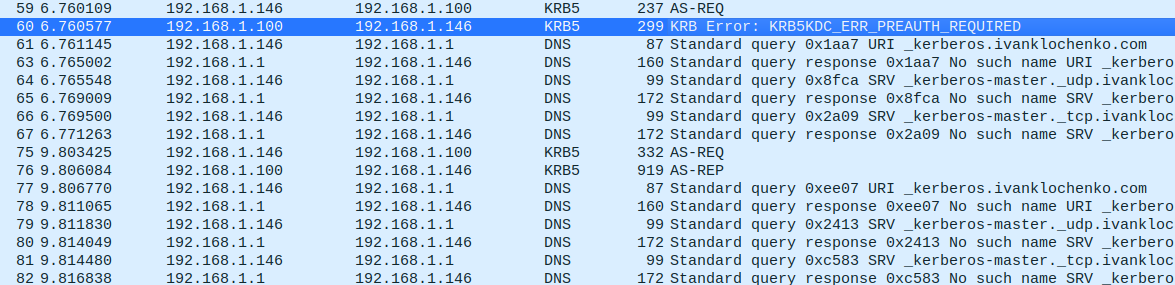
* 1. Аутентифицируемся на сервере и просматриваем выдаваемую информацию.



**Рисунок 14**. Аутентификация на сервера и просмотр выдаваемой информации

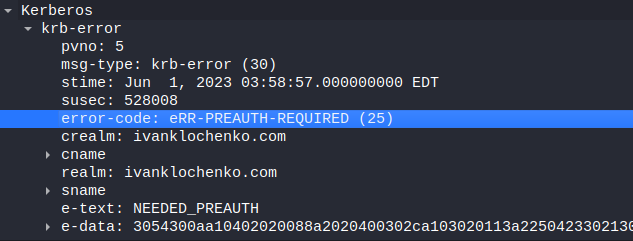
В выдаваемой информации указаны дата и время начала аутентификации, дата и время действия, название сервиса, на котором клиент прошел аутентификацию.

* 1. Проанализируем трафик с помощью *Wireshark*.



**Рисунок 15**. Захваченный трафик аутентификации пользователя ivank

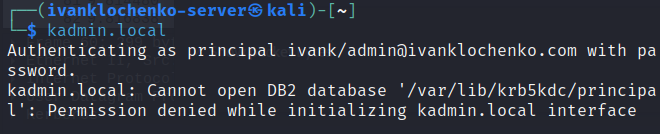
Первый ответ сервера на попытку авторизоваться сигнализирует об ошибке. Если просмотреть содержимое пакета, можно увидеть следующее.



**Рисунок 16**. Содержимое пакета ответа сервера

Если верить тексту поля *e*-*text*, то ошибка эта возникает из-за отсутствия пре-аутентификации.

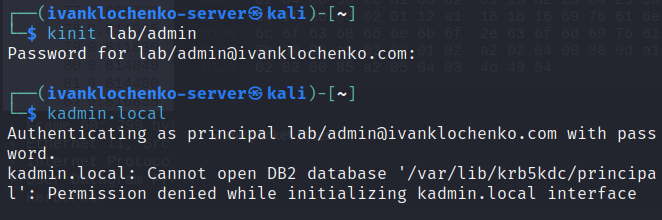
* 1. Запустим *kadmin*.*local* на серверной машине.



**Рисунок 17**. Вывод сообщения после команды kadmin.local

Это сообщение говорит нам о том, что произведена аутентификация пользователя *ivank* и что у него недостаточно прав для того, чтобы обратиться к БД *DB*2 для добавления принципалов.

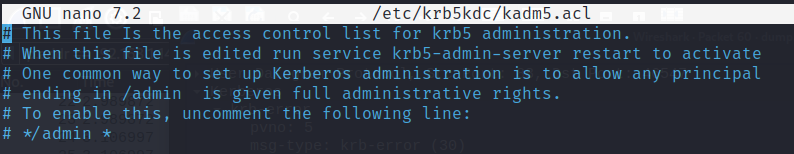
* 1. Заходим под *lab*/*admin* и пробуем снова.



**Рисунок 18**. Попытка выполнения команды от lab/admin

Поведение предсказуемое, потому что *lab*/*admin* точно такой же принципал, что и *ivank*, и права у него ровно такие же.

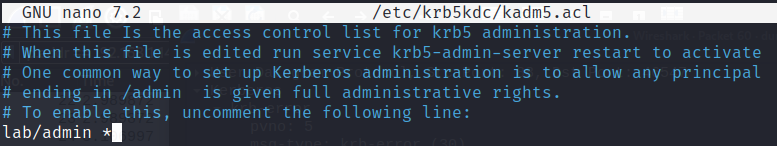
* 1. Откроем для редактирования *Access* *List* *Kerberos*.



**Рисунок 19**. Файл kadm5.acl

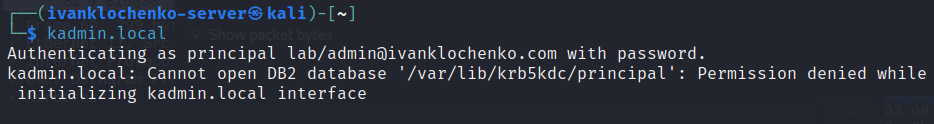
Для того, чтобы дать права пользователю *lab*/*admin*, нужно просто раскомментировать посдеднюю строку этого файла. Это будет означать, что все пользователи с суффиксом /*admin* будут иметь права редактирования *kadmin*.*local*.

* 1. Расскоментируем эту строку и изменим ее так, чтобы дать разрешение только *lab*/*admin*.



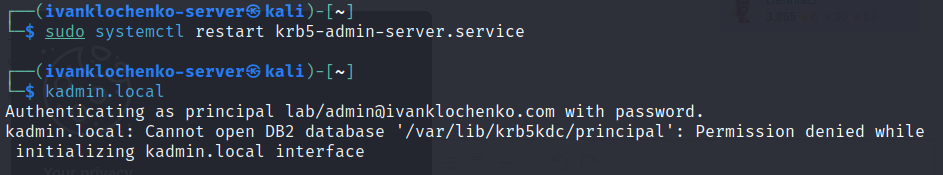
**Рисунок 20**. Выдача прав lab/admin

* 1. Повторим команду *kadmin*.*local*.



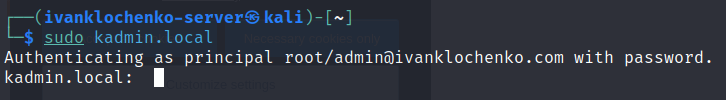
**Рисунок 21**. Снова Permission denied

* 1. Перезапускаем сервис *Kerberos* и пробуем снова.



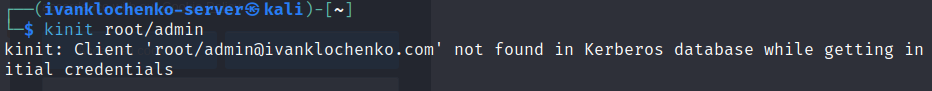
**Рисунок 22**. Снова ошибка после перезапуска службы

* 1. Добавим к команде приставку *sudo*.



**Рисунок 23**. Аутентификация под root/admin и успешное выполнение команды kadmin.local

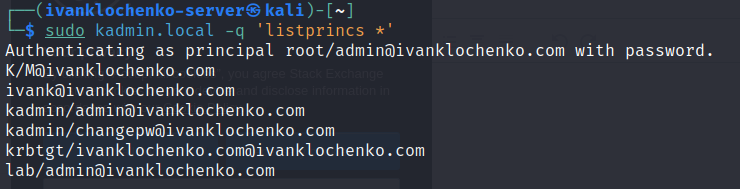
* 1. Попробуем авторизоваться под этим пользователем.



**Рисунок 24**. Попытка авторизации под пользователем root/admin

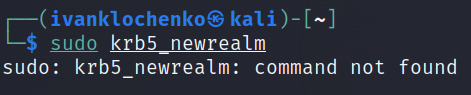
Ответ от *Kerberos* предсказуемый, потому что пользователя *root*/*admin* мы не создавали (это локальный администратор), а значит, его нет в БД принципалов.

* 1. Просмотрим список пользователей.



**Рисунок 25**. Список принципалов Kerberos

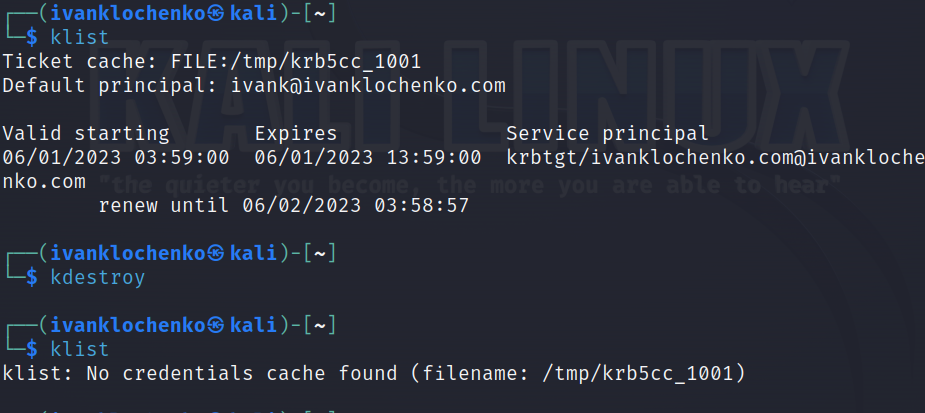
* 1. Запускаем захват трафика и пробуем авторизоваться под, например, *kadmin*/*admin*, сначала на сервере, потом на клиенте. Так как пароли для авторизации под автоматически созданными пользователями мне не известны, и на сервере, и на клиенте я не смог авторизоваться. Трафик отличается в *src* и *dst* *IP* адресах, в присутствии *AS*-*REQ* и *AS*-*REP* в трафике авторизации с клиента.
  2. Ранее на первоначальный запрос *AS\_REQ* мы получали ответ *KRB\_ERROR*, а сейчас *AS\_REP* как при успешной авторизации. Это происходит потому, что у созданных «от руки» пользователей, как было сказано ранее, не было *pre*-*authentication*, а у предустановленных пользователей (в пашем случае *kadmin*/*admin*) она есть. Ошибок не возникает, поэтому есть два флага *AS*-*REQ* и *AS*-*REP*.
  3. Сравниваем два *AS*-*REP*. Структура идентична, различаются поля с содержимым.
  4. То, что мы можем зайти под одним пользователем и не можем под другим, может свидетельствовать о возможных ограничениях, установленных на уровне службы или системы, которые могут запрещать доступ конкретным пользователям.
  5. Попробуем создать с клиентской машины новую область.



**Рисунок 26**. Попытка создания новой области на машине клиента

Безуспешно, так как инструмент *krb*5*\_newrealm* входит в состав администраторских утилит *krb*5-*admin*-*server*, *krb*5-*kdc*.

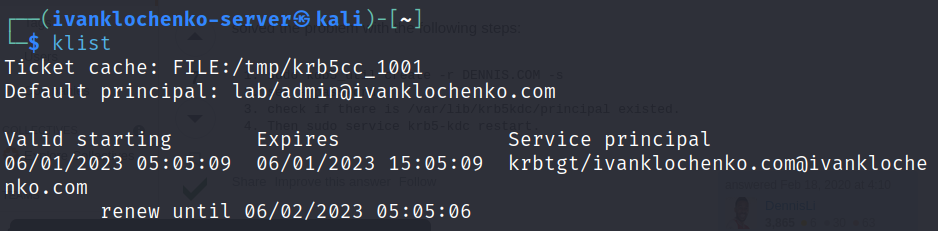
* 1. Выполним на клиентской машине команду *kdestroy*.



**Рисунок 27**. Команда kdestroy

Команда уничтожает активные билеты авторизации пользователя *Kerberos*.

* 1. Посмотрим *klist* на серверной машине.



**Рисунок 28**. Список билетов авторизации пользователей на серверной машине

Как видно из скриншота, список билетов на сервере остался неизменным, что может свидетельствовать о применимости *kdestroy* только для текущей машины (в моем случае клиентской).

## Вывод

В ходе выполнения лабораторной работы были освоены основные техники работы с *Kerberos*.

Была проведена конфигурационная настройка с указанием области по умолчанию, названий серверов.

Созданы принципалы. Проведена процедура аутентификации с получение *TGT*.

Изучен трафик аутентификации *Kerberos* и структура пакетов *AS*-*REQ* и *AS*-*REP*. Выяснены причины возможных ошибок, а также разницы пакетов-ответов от сервера.

Изучена возможность редактирования *Access* *List* для *kadmin*.*local*.

Изучена возможность очистки активных билетов авторизации пользователей *Kerberos*.

## Контрольные вопросы

**В:**

Для чего служат автоматически созданные пользователи в системе kerberos?

**О:**

Автоматически созданные пользователи в системе Kerberos служат для обеспечения аутентификации и авторизации клиентов в рамках Kerberos-аутентификации. Они представляют собой стандартные учетные записи, которые можно использовать для проверки и тестирования функциональности Kerberos.

**В:**

Если не выполнять аутентификацию под принципала под каким принципалом будут выполнятся команды без приставки *sudo*?

**О:**

Если не выполнять аутентификацию под принципалом, то команды без приставки *sudo* будут выполняться от имени текущего пользователя системы (локального пользователя на клиентской машине), а не от имени принципала *Kerberos*. Такие команды будут работать в пределах прав доступа и разрешений, присвоенных локальному пользователю.

**В:**

Можно ли с клиентской машины редактировать серверные файлы?

**О:**

Нет, с клиентской машины нельзя редактировать серверные файлы напрямую. Серверные файлы, такие как файлы базы данных KDC или конфигурационные файлы Kerberos, находятся на сервере Kerberos и могут быть изменены только с административной станции или с сервера самого Kerberos.

**В:**

Почему нельзя создать новую область с клиентской машины?

**О:**

Создание новой области (realm) в Kerberos требует административных привилегий и доступа к серверу Kerberos. Это действие должно выполняться с серверной стороны, а не с клиентской машины. Администратор Kerberos должен иметь доступ и разрешения для создания и настройки новой области.

**В:**

Если установить на клиентскую машину пакеты как для серверной получится ли изменять серверные файлы? Если да то где они меняются?

**О:**

Установка пакетов, предназначенных для серверной части Kerberos, на клиентскую машину позволит использовать клиентские инструменты и утилиты для работы с сервером Kerberos. Однако это не дает возможности непосредственно изменять серверные файлы, так как они находятся на самом сервере Kerberos. Они изменятся, но на клиентской машине, потому что клиентская машина при установке пакетов администрирования kdc сервера, сама станет сервером и конфигурационные файлы будут относиться к ней.