**Московский государственный технический**

**университет им. Н.Э. Баумана**

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

Курс «Сетевая безопасность»

Отчет по лабораторной работе №3

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| студент группы ИУ5-73Б |  | преподаватель каф. ИУ5 |
| Терентьева Софья  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |  | Симонов Михаил Фёдорович  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |

Москва, 2024 г.

Цель работы:

Изучить инфраструктуру открытых ключей на примере создания сертификата удостоверяющего центра, подписи сертификата, и настройки веб-сервера для использования TLS (transport layer security, протокол защиты транспортного уровня).

Ход работы:

1. Запустить ВМ:

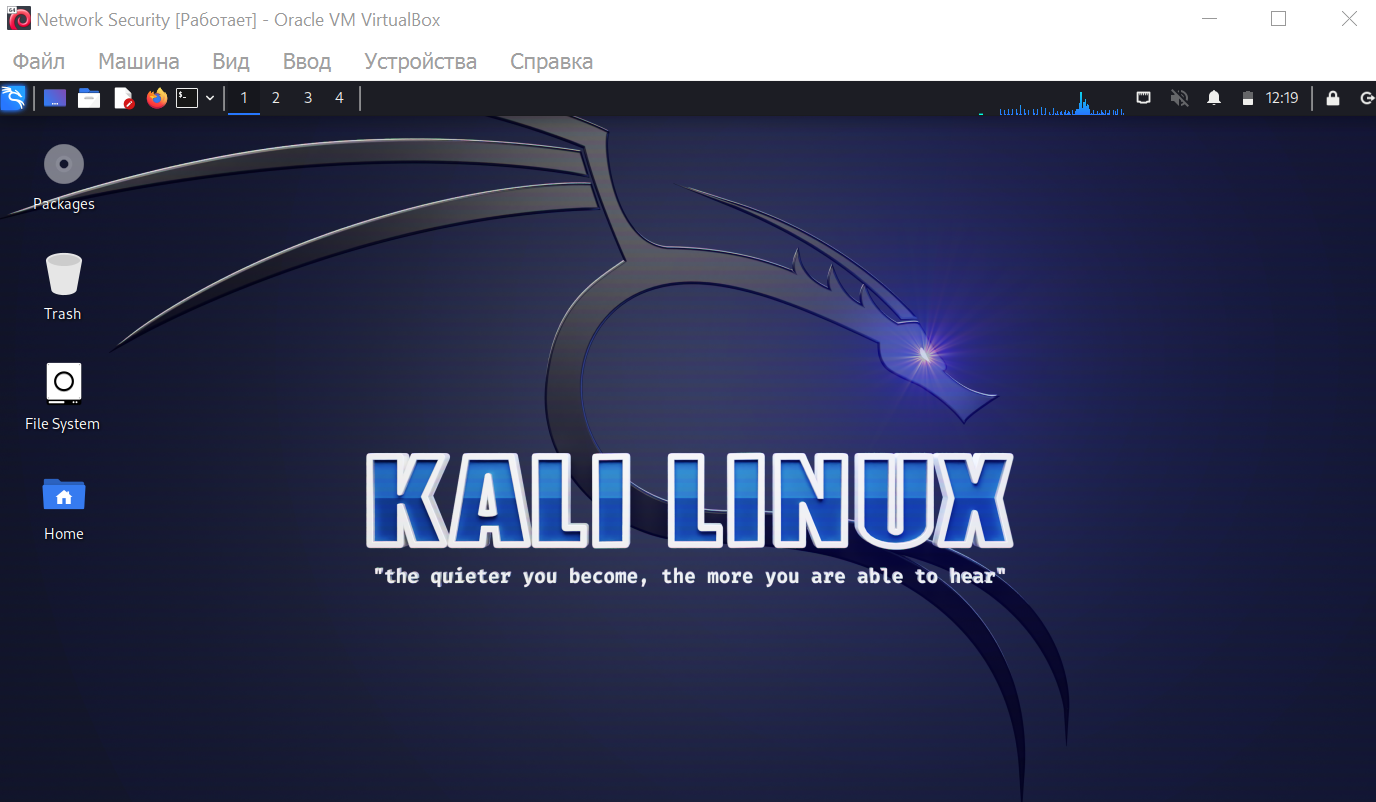
Для запуска ВМ сначала создадим ее на основе образа:

Тип: Linux, Debian (64-bit)

Оперативная память: 2560 МБ, процессор: 2+

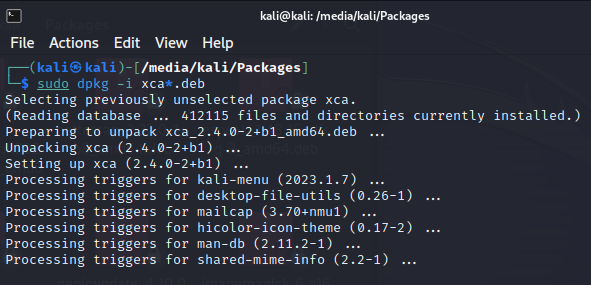
Жесткий диск: отсутствует

CD диски: kali-linux-2023.1-live-amd64.iso и kalipackages.iso

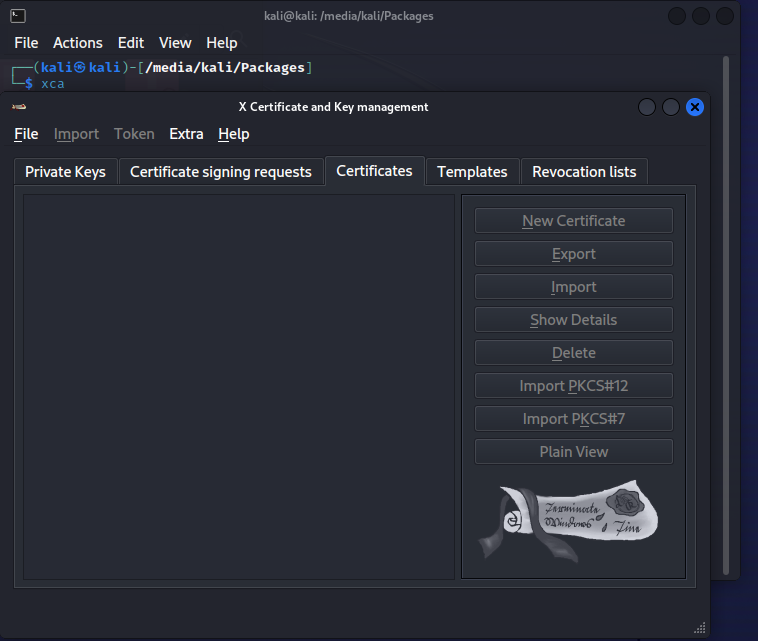


1. Запустить XCA, создать базу данных:

Установим программный пакет ХСА:



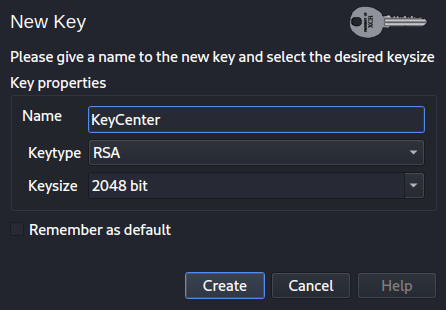
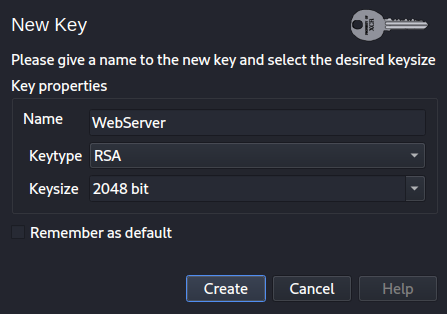
Запустим ХСА:



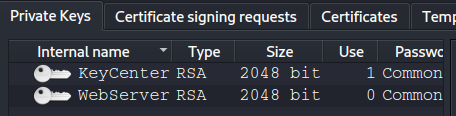
Для создания базы данных необходимо выбрать File > New DataBase, после чего ввести название XCA\_DB и нажать Save.

1. Создать два приватных ключа: один для удостоверяющего центра, другой для сертификата веб-сервера:

Для создания приватного ключа выбрать вкладку Private Keys, нажать New Key, ввести название ключа, выбрать тип и длину, нажать Create:

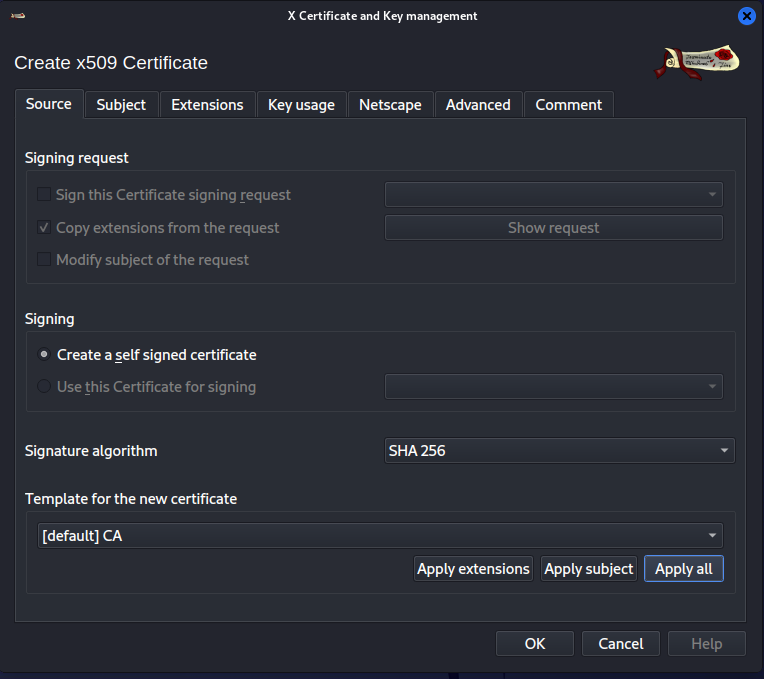
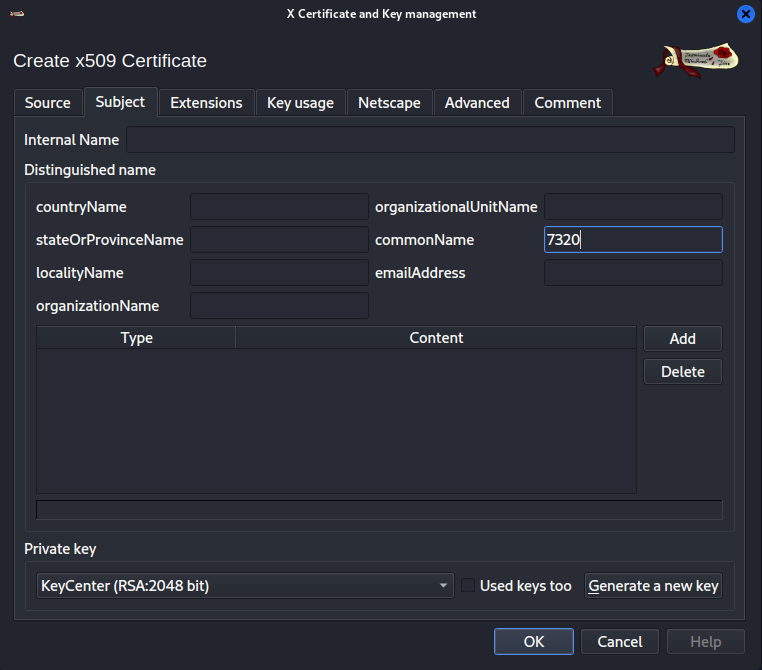
 

Проверим успешность создания ключей:



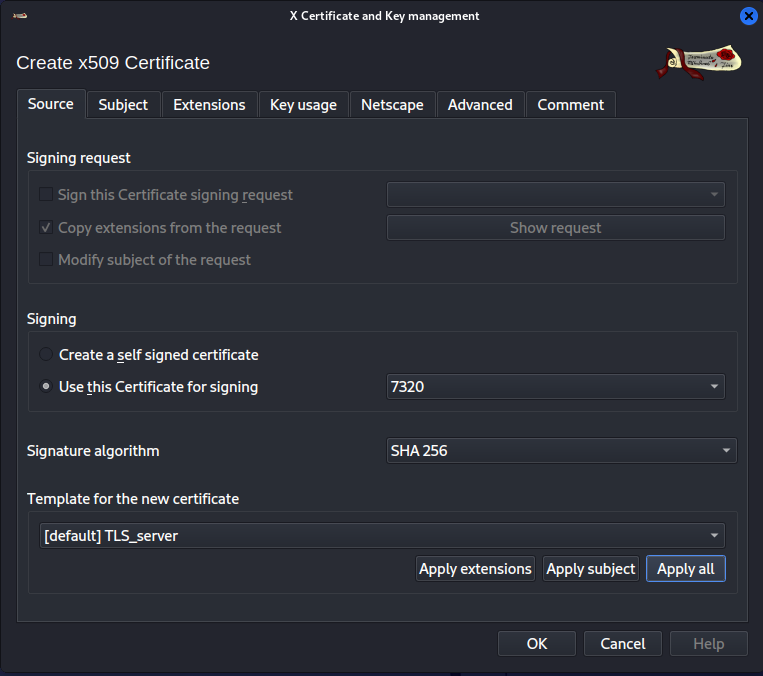
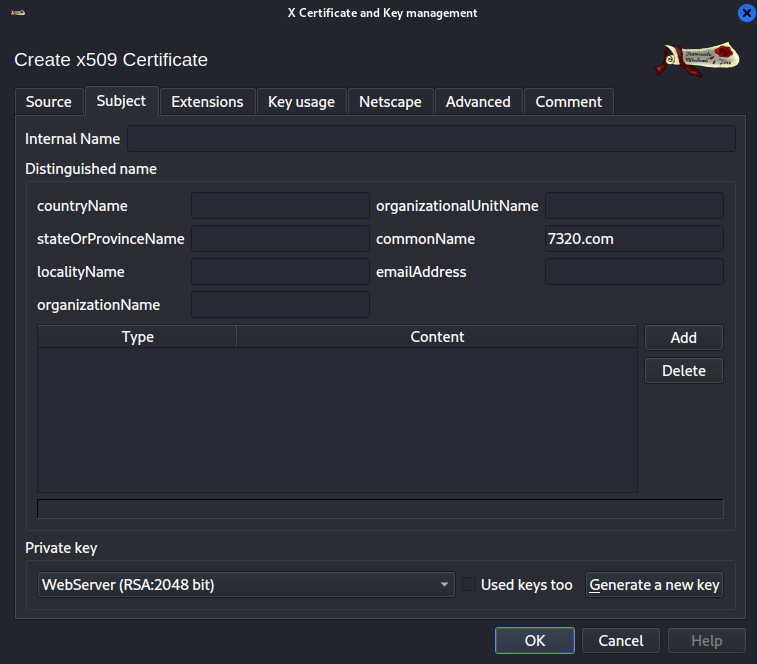
1. Создать самоподписанный сертификат УЦ. В commonName включить номер группы и порядковый номер студента в группе:

Для создания сертификата необходимо во вкладке Certificates нажать New Certificate. Выбрать издателя сертификата (Create a self signed certificate), выбрать шаблон ([default] CA) для удостоверяющего центра, нажать Apply all. Заполнить поля во вкладке Subject (поля commonName в контексте лабораторной работы будет достаточно). Выбрать правильный приватный ключ (Private key) и нажать OK.

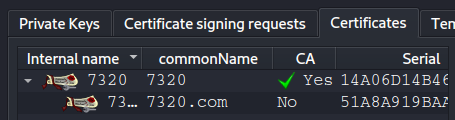
 

1. Создать сертификат для веб-сервера, изданный УЦ. Задать commonName «7320.com»:

Для создания сертификата необходимо во вкладке Certificates нажать New Certificate. Выбрать издателя сертификата (Use this Certificate for signing), выбрать шаблон ([default] TLS\_server) для удостоверяющего центра, нажать Apply all. Заполнить поля во вкладке Subject (поля commonName в контексте лабораторной работы будет достаточно). Выбрать правильный приватный ключ (Private key) и нажать OK.

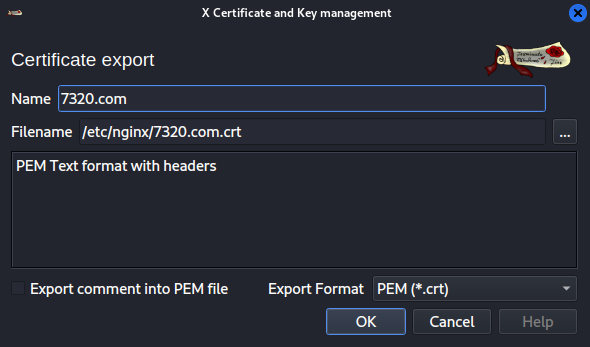
 

Проверим успешность создания сертификатов:

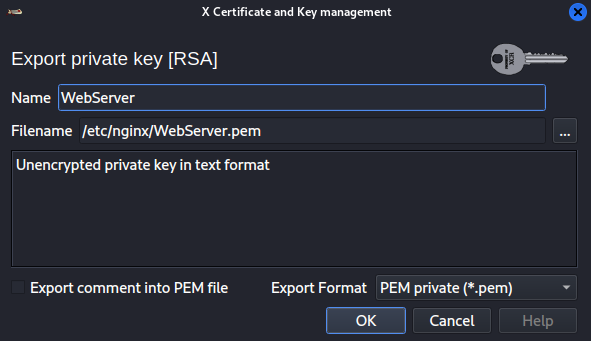


1. Экспортировать полную цепочку сертификата веб-сервера, приватный ключ сертификата веб-сервера, и сертификат УЦ:

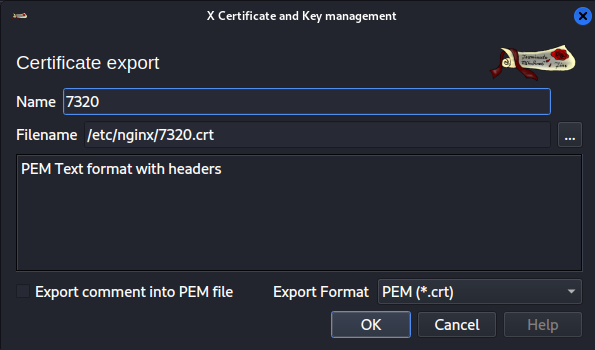
Для экспорта полной цепочки необходимо выбрать необходимый сертификат, нажать кнопку Export. Ввести название файла, выбрать формат PEM chain (\*.pem) и нажать OK.



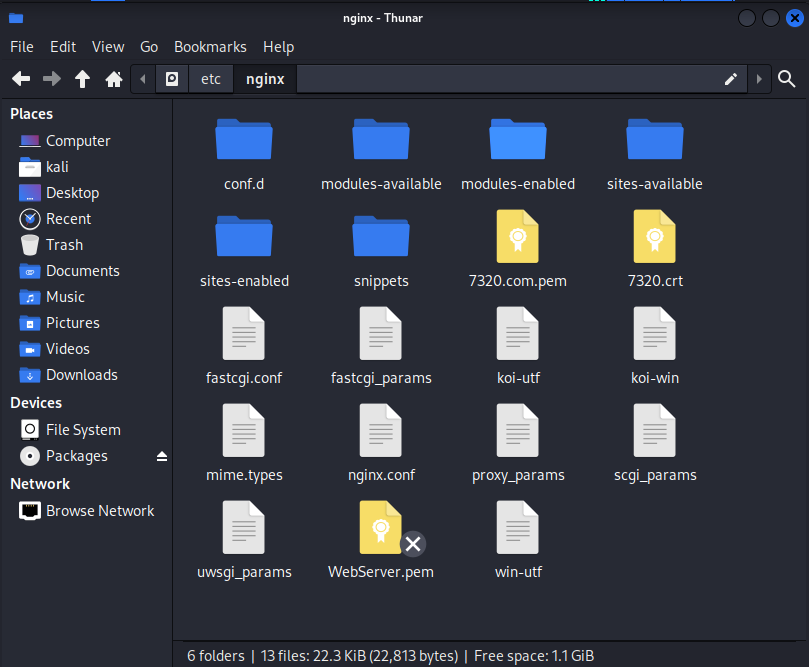
Для экспорта приватного ключа веб-сервера необходимо выбрать необходимый ключ, нажать кнопку Export. Ввести название файла, выбрать формат PEM private (\*.pem) и нажать OK.



Для экспорта сертификата УЦ необходимо выбрать необходимый сертификат, нажать кнопку Export. Ввести название файла, выбрать формат PEM (\*.crt) и нажать OK.

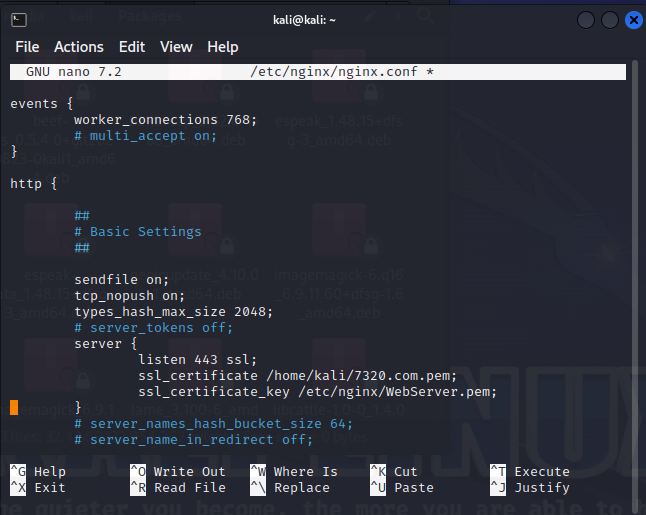


Проверим результаты экспорта:

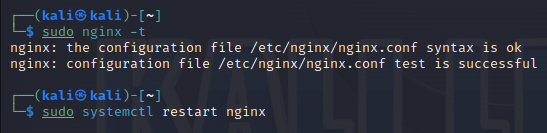


1. Настроить TLS в веб-сервере nginx:

Открыть в терминале /etc/nginx/nginx.conf в текстовом редакторе nano с правами root (sudo nano /etc/nginx/nginx.conf) и добавить строки следующим образом:

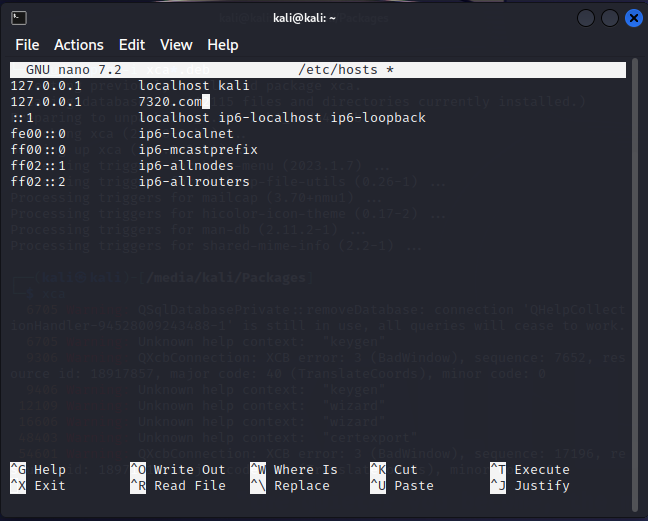


Сохранить, выйти из редактора, проверить файл командой sudo nginx –t, выполнить sudo systemctl restart nginx.



1. Добавить запись для распознавания доменного имени «7320.com» в файл hosts:

Открыть в терминале /etc/hosts в текстовом редакторе nano с правами root (sudo nano /etc/hosts) и добавить строку следующим образом:

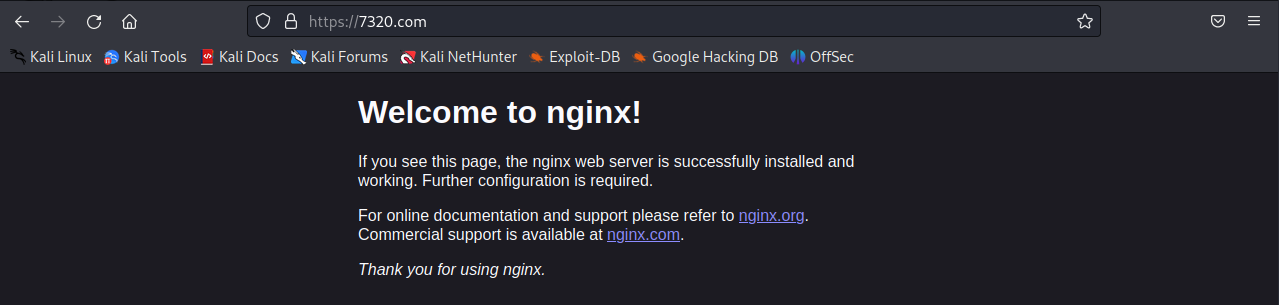


Сохранить, выйти из редактора.

1. Добавить УЦ в Firefox:

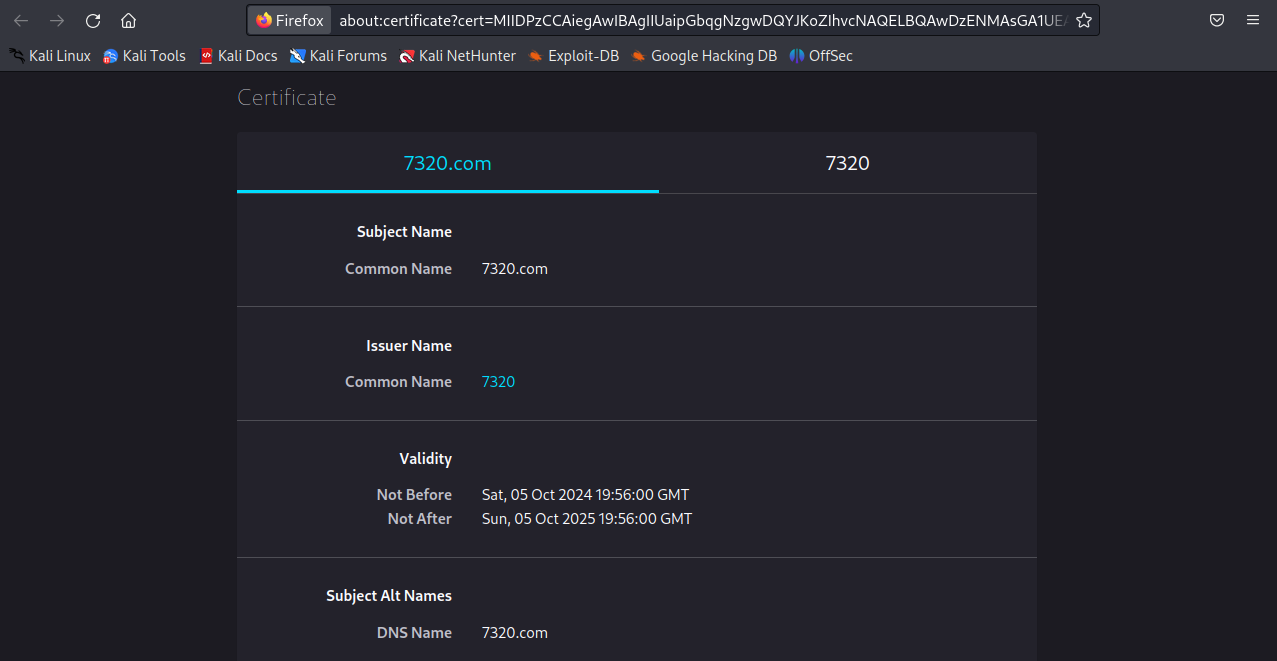
Нажать Alt на клавиатуре > Edit > Settings > Privacy & Security > View Certificates > Authorities > Import > 7320.crt (название файла сертификата УЦ), поставить галочку “Trust this CA to identify websites”, нажать OK.

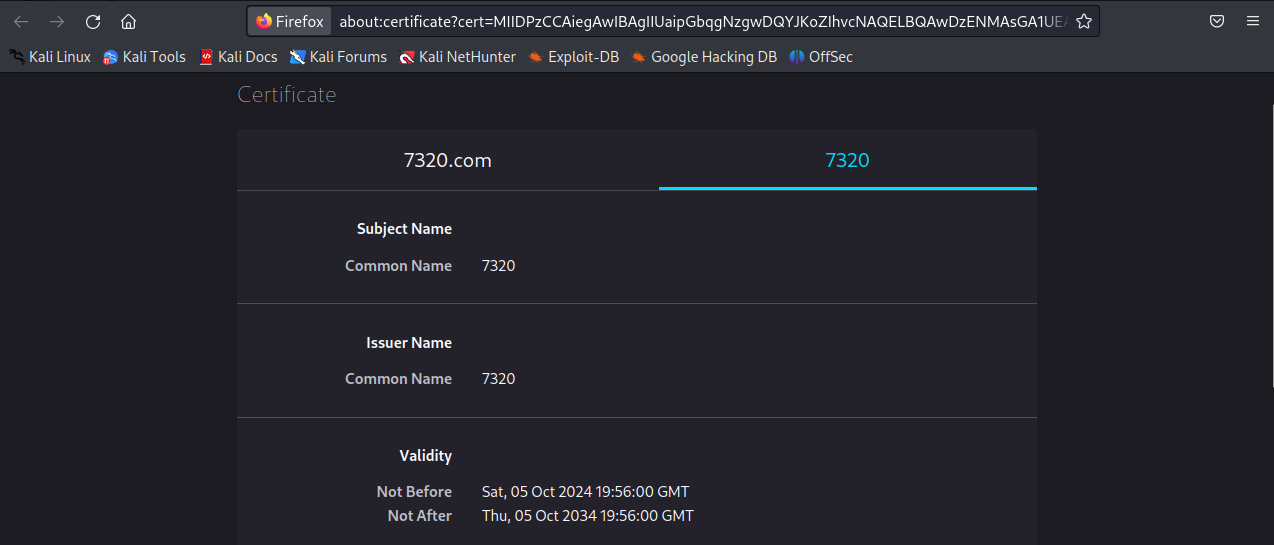
1. Открыть https://7320.com/ в Firefox (значок слева от значка терминала), продемонстрировать демо-страницу, информацию о сертификате веб-сервера и УЦ:



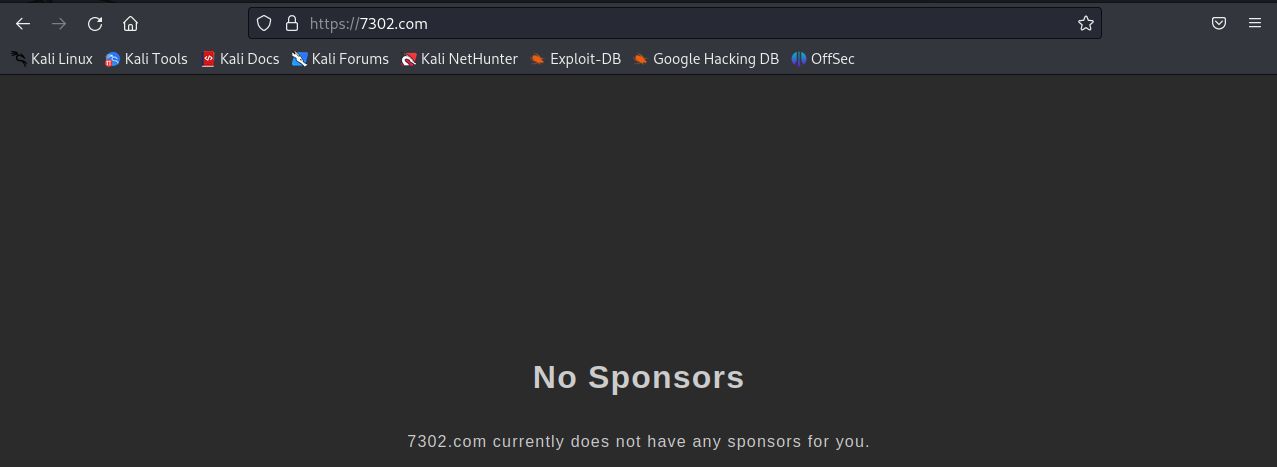
Информация о сертификате веб-сервера:

Для получения информации о сертификате нажать на значок с изображением замка, Connection secure > More information > View Certificate.





Попробуем «случайно» опечататься в адресе:



Веб-сервер настроен корректно.

Результаты выполнения работы:

В процессе выполнения лабораторной работы я познакомилась с инфраструктурой открытых ключей, протоколом TLS, научилась созданию удостоверяющих сертификатов и их применению.