**Министерство науки и высшего образования Российской Федерации** ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий Дисциплина:**

«Вычислительные сети и контроль безопасности в компьютерных сетях»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

«Безопасность DNS»

**Выполнил:**

Кукелко Владислав, студент группы N3349

(подпись)

Молитвин Илья, студент группы N33Изображение выглядит как текст, соединитель

Контент, сгенерированный ИИ, может содержать ошибки.45

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Коптяев Александр, студент группы N3345

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Бучаев Абдулхамид Яхьевич, преподаватель ФБИТ

(отметка о выполнении)

(подпись)

**Содержание**

[Введение 2](#_Toc197282544)

[Ход работы 3](#_Toc197282545)

[Заключение 8](#_Toc197282546)

# Введение

Цель работы: изучить основные принципы работы системы доменных имен DNS, получить представление об основных угрозах безопасности DNS, изучить основы настройки серверов DNS на примере BIND.

Для этого необходимо решить следующие задачи:

* настроить лабораторный стенд согласно сетевой схеме;
* на сервере SRV1 настроить зону lab.test. С помощью утилит dig/nslookup проверить работоспособность зоны;
* На сервере SRV1 настроить делегирование поддомена my.lab.test на сервер SRV2. На сервере SRV2 настроить зону my.lab.test, проверить ее работоспособность с клиентского устройства;
* Для дочерней зоны my.lab.test настроить механизм DNSSEC для обеспечения защиты от атак типа DNS-spoofing. Убедиться в корректности разрешения имен и проверки цифровой подписи DNS-запросов.

# Ход работы

Работа выполнялась на двух ВМ с ОС Linux Ubuntu, клиентом была хостовая машина с Win 11.

SRV1 – 192.168.56.101 SRV2 – 192.168.56.102 Client – 192.168.56.1

Для того чтобы настроить зону нам нужно последовательно прописать настройки в следующие файлы: named.conf.options, named.conf.local, db.lab.test

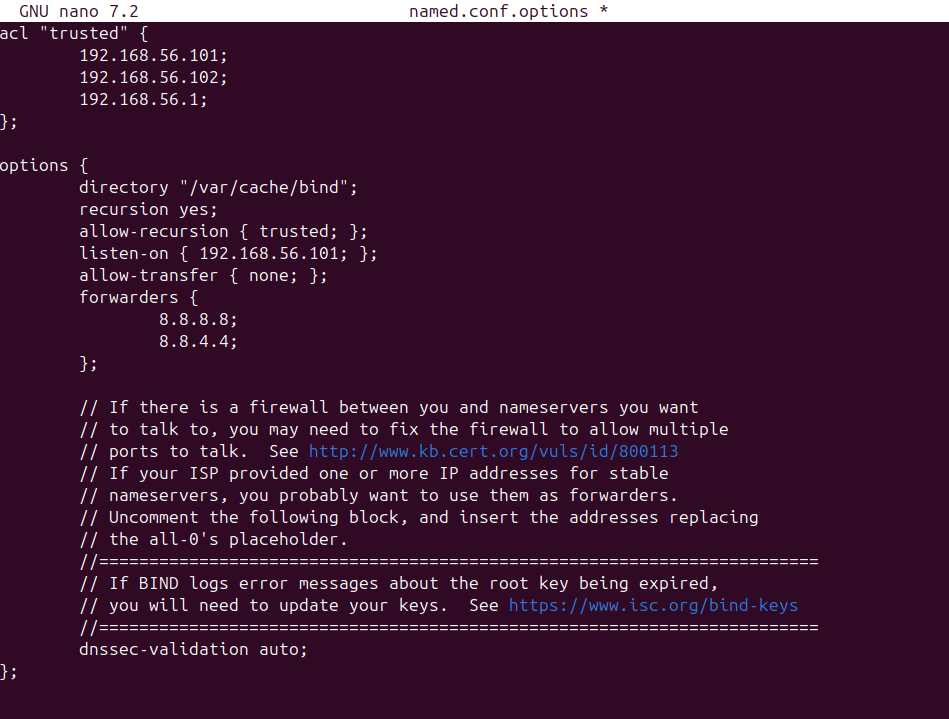


Рис. 1 – Содержимое named.conf.options

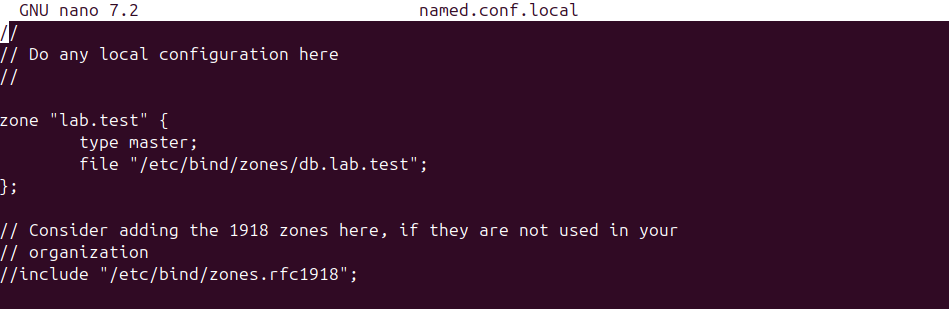


Рис. 2 – Содержимое named.conf.local

Далее создадим директорию zones и файл зоны.



Рис. 3- Директория zones

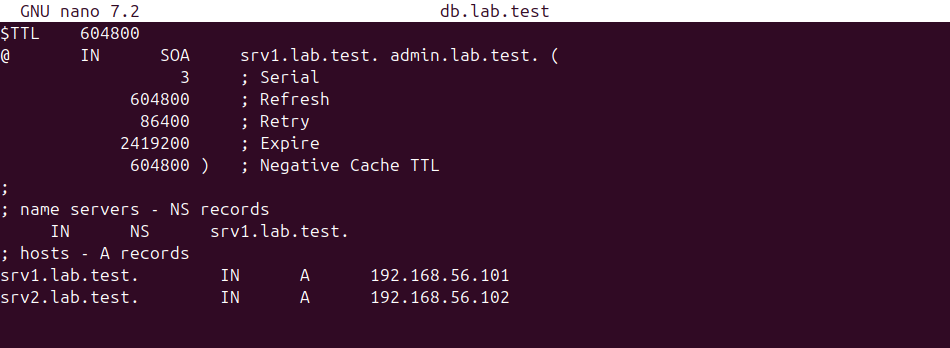


Рис. 4 – Файл зоны db.lab.test

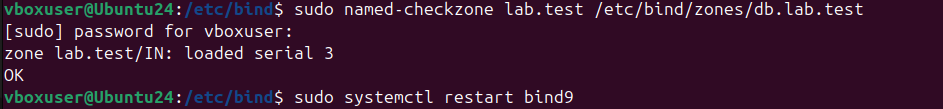


Рис. 5 – Проверка загрузки зоны

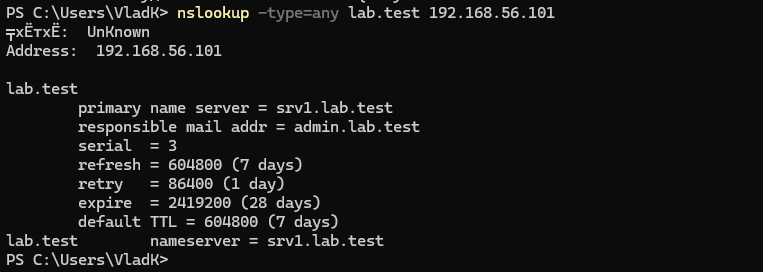


Рис. 6 – Результаты проверки зоны с клиента с помощью nslookup

Теперь настроим делегирование поддомена my.lab.test на сервер SRV2

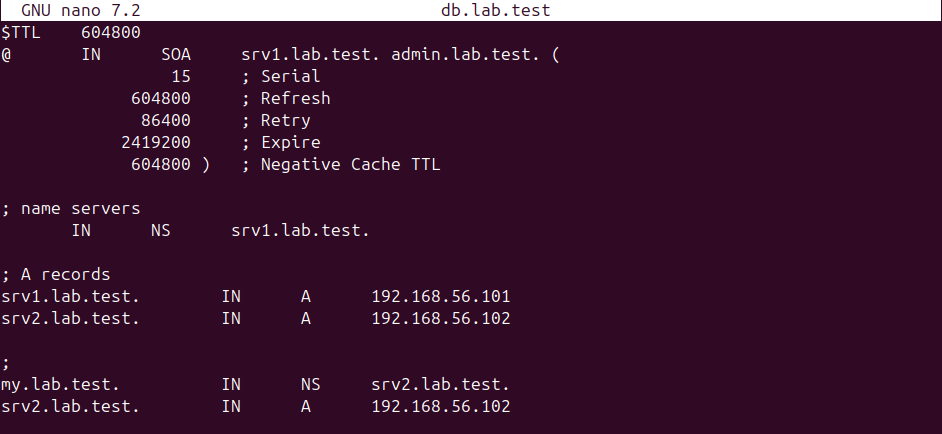


Рис. 7 – Добавление делегирования

Настройки SRV2

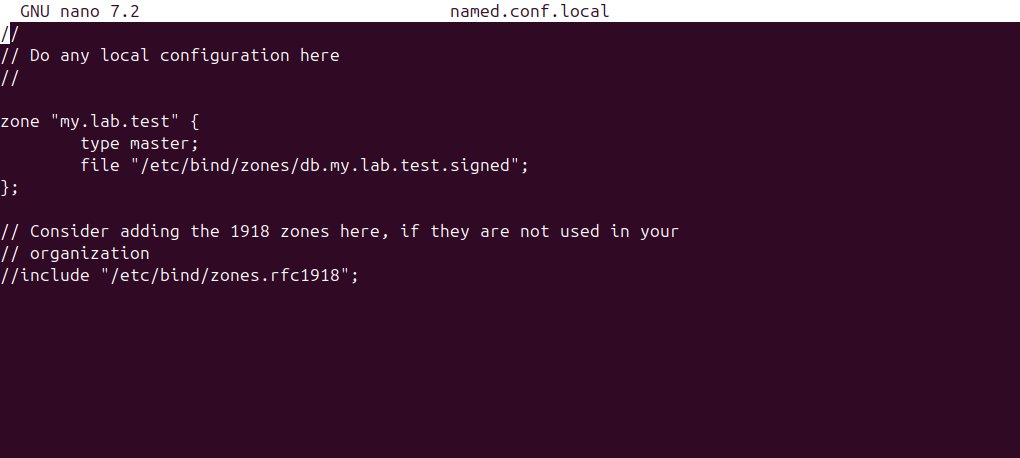


Рис. 8 – Содержимое named.conf.local ()

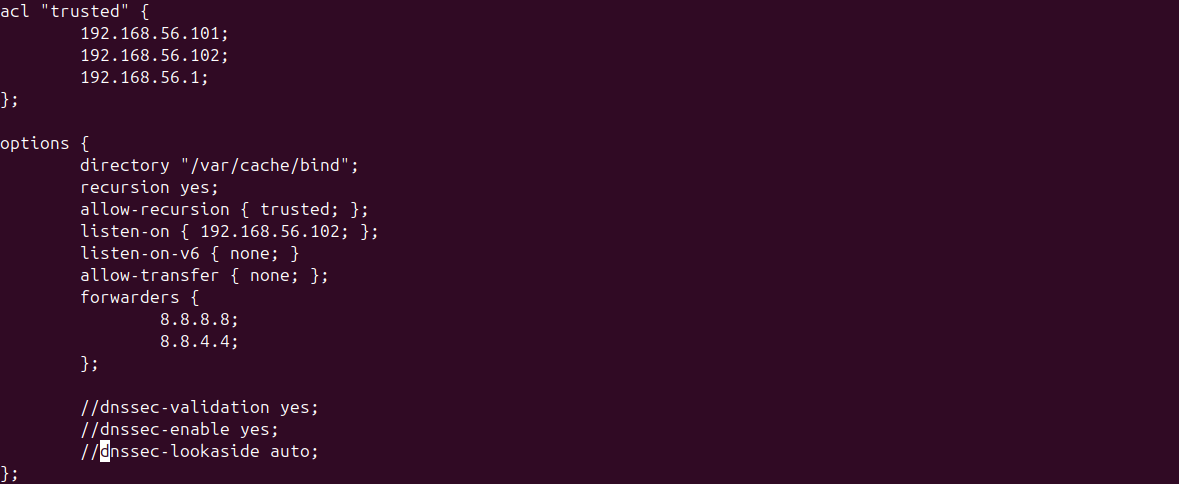


Рис. 9 – Содержимое named.conf.options

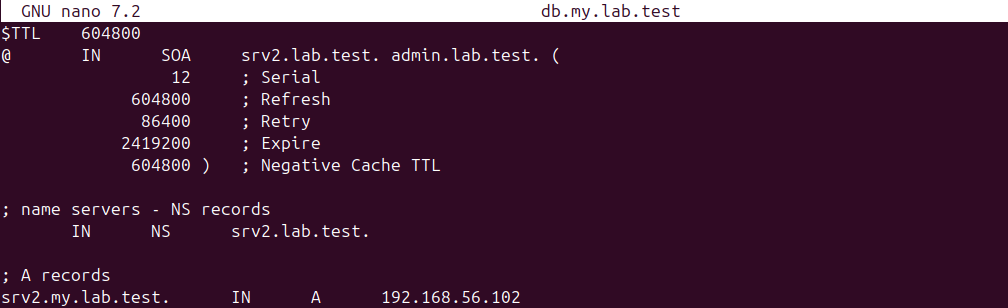


Рис. 10 - Файл зоны db.my.lab.test

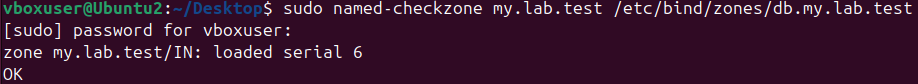


Рис. 11 – Проверка зоны

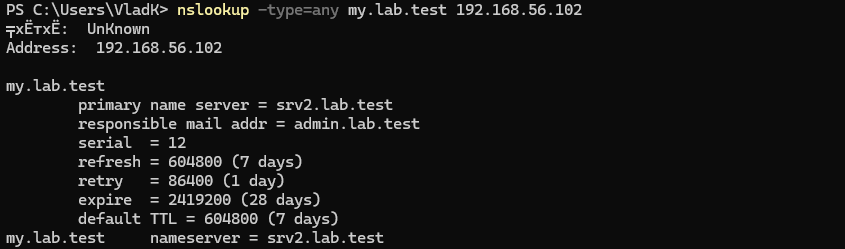


Рис. 12 – Результаты проверки зоны с клиента с помощью nslookup

Теперь настроим механизм DNSSEC

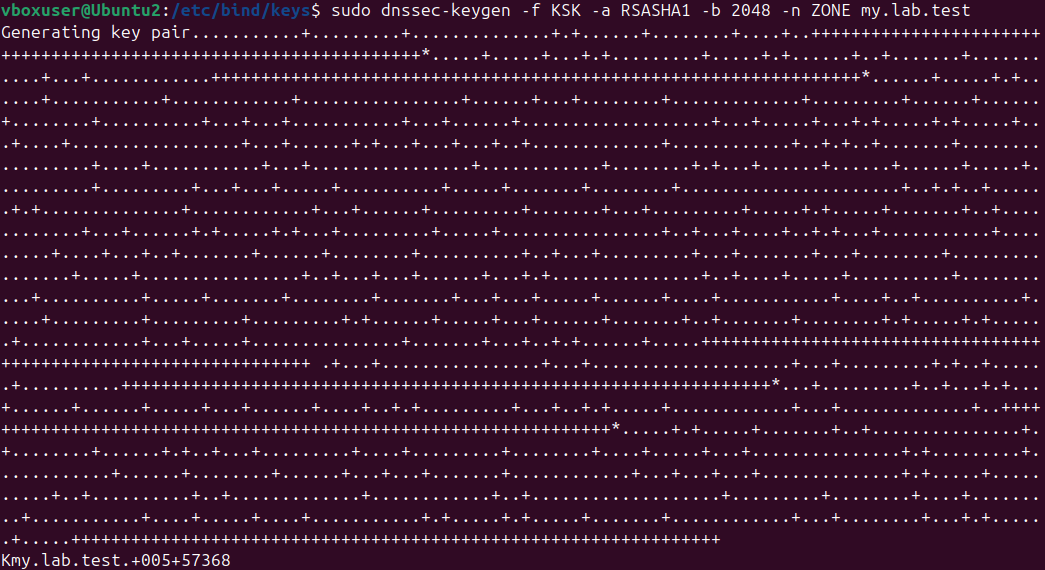


Рис. 13 – Генерация мастер-ключа

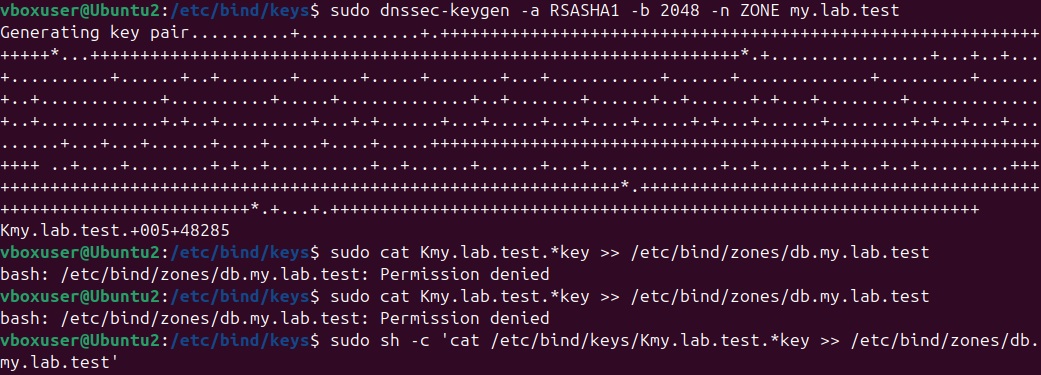


Рис. 14 – Генерация ключа зоны

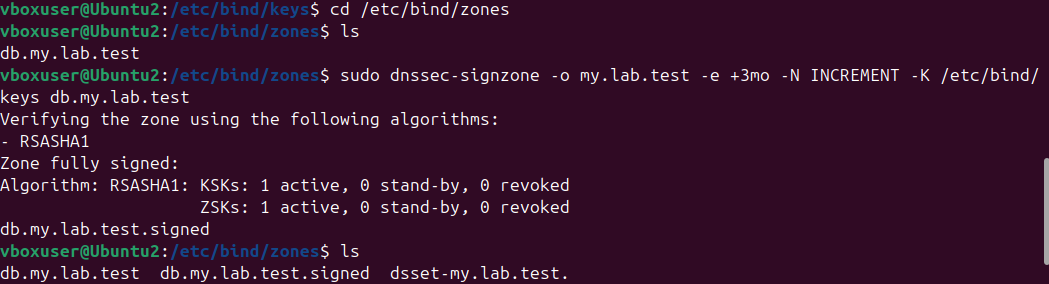


Рис. 15 – Подпись зоны

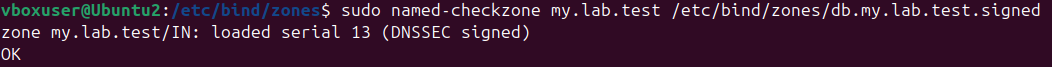


Рис. 16 – Проверка подписи

# Заключение

В ходе выполнения лабораторной работы были изучены основы настройки серверов DNS на примере BIND.