Лабораторная работа № 5

# Безопасность DNS

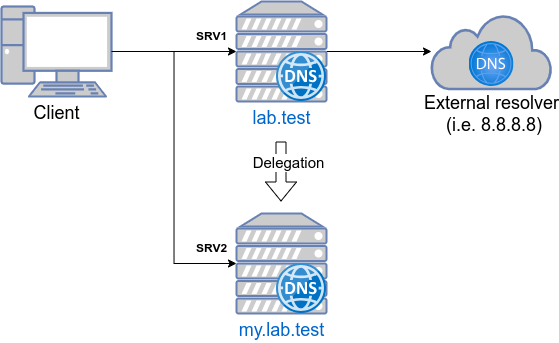
### Цель работы

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

### Задачи

* Настроить лабораторный стенд согласно сетевой схеме. Для настройки лабораторного стенда можно использовать среду GNS3 либо ПО для работы с виртуальными машинами.
* 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.

### Сетевая схема



### Содержание работы

* Настроить лабораторный стенд. В качестве серверов SRV1 и SRV2 могут быть использованы виртуальные машины под управлением ОС Linux с установленной на них службой BIND. VM SRV1 имеет 2 интерфейса: Host-only network и NAT/Bridge (для перенаправления на внешний резолвер всех запросов, не относящихся к домену *lab.test*)
  + ***Установка BIND***

*sudo apt-get install bind9 bind9utils bind9-doc*

Для включения в BIND режима IPv4 необходимо в файле */etc/default/bind9* добавить опцию -4

*OPTIONS="-u bind -4"*

и перезапустить сервис.

* + ***Настройка BIND***

Основные настройки сервиса прописываются в файле */etc/bind/named.conf.options*

Здесь добавляем список клиентов, для которых разрешены рекурсивные запросы:

*acl "trusted" {*

*192.168.56.101; # srv1 - можно также прописать localhost*

*192.168.56.102; # srv2*

*192.168.56.1; # client*

*};*

Редактируем блок настроек:

*options {*

*directory "/var/cache/bind";*

*recursion yes; # разрешаем рекурсивные запросы*

*allow-recursion { trusted; }; # разрешаем рекурсивные запросы только от доверенных клиентов*

*listen-on { 192.168.56.101; }; # приватный адрес SRV1, на котором будет работать сервис DNS*

*allow-transfer { none; }; # запрет переноса зоны*

*forwarders {*

*8.8.8.8;*

*8.8.4.4;*

*}; # перенаправление запросов, неизвестных серверу на Google DNS*

*. . .*

*};*

* В качестве клиента можно использовать машину хоста либо виртуальную машину в той же сети Host-only. Для тестирования на клиентской машине должны быть установлены утилиты dig либо nslookup.
* Настраиваем зону *lab.test* на SRV1.

В файле */etc/bind/named.conf.local* прописываем:

*zone "lab.test" {*

*type master;*

*file "/etc/bind/zones/db.lab.test"; # путь к файлу зоны*

*};*

Пример файла зоны */etc/bind/zones/db.lab.test* (не забываем увеличивать на 1 значение Serial при внесении любого изменения в файл зоны до перезапуска сервиса named!):

*$TTL 604800*

*@ IN SOA srv1.lab.test. admin.lab.test. (*

*3 ; Serial*

*604800 ; Refresh*

*86400 ; Retry*

*2419200 ; Expire*

*604800 ) ; Negative Cache TTL*

*;*

*; name servers - NS records*

*IN NS srv1.lab.test.*

*; hosts - A records*

*srv1.lab.test. IN A 192.168.56.101*

*srv2.lab.test. IN A 192.168.56.102*

* Аналогично зоне *lab.test* создаем зону *my.lab.test,* при этом в качестве сервера имен, ответственного за данную зону указываем сервер SRV2

*; name servers - NS records*

*IN NS srv2.lab.test.*

* Настраиваем DNSSEC для зоны *my.lab.test*

В каталоге /etc/bind/keys генерируем мастер-ключ (Key-Signing Key, KSK):

*dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE my.lab.test*

где RSASHA1 - используемые алгоритмы шифрования/хэширования,

2048 - длина ключа.

Генерируем ключ зоны (Zone-Signing Key, ZSK)

*dnssec-keygen -a RSASHA1 -b 2048 -n ZONE my.lab.test*

Копируем содержимое ключей в файл зоны:

*cat Kmy.lab.test.\*key >> /etc/bind/zones/db.my.lab.test*

Подписываем зону:

*dnssec-signzone -o my.lab.test -e +3mo -N INCREMENT -K /etc/bind/keys db.my.lab.test*

В данном примере время действия RRSIG ограничено 3 месяцами.

После успешного подписания зоны в каталоге хранения зон появляется новый файл *db*.*my.lab.test.signed*

Включаем DNSSEC в */etc/bind/named.conf.local*

*options {*

*...*

*dnssec-enable yes;*

*dnssec-validation yes;*

*dnssec-lookaside auto;*

*}*

В настройке зоны my.lab.test меняем путь к файлу и перезапускаем BIND:

*zone "my.lab.test" {*

*type master;*

*file "/etc/bind/zones/db.my.lab.test.signed"; # путь к файлу зоны*

*};*

Проверяем корректность отдачи RRSIG:

*dig my.lab.test +dnssec*

Помимо файла *db*.*my.lab.test.signed*, который содержит подписанную зону, команда *dnssec-signzone* генерирует еще один файл *dsset-my.test.lab.* Этот файл содержит набор DS записей, которые должны быть прописаны в настройках родительской зоны *lab.test* на сервере SRV1

### Требования к отчету

В отчете необходимо привести:

* Схему лабораторного стенда с указанием IP-адресов
* Конфигурацию файлов зоны lab.test и my.lab.test
* Результаты тестирования настроек зоны (вывод команды dig)
* Выводы