Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное
учреждение высшего образования
“Национальный исследовательский университет ИТМО”

Факультет инфокоммуникационных технологий

Лабораторная Работа №7

по дисциплине “Компьютерные сети”

Выполнил студенты:
Алексеев Павел Алексеевич
Смирнов Тимур Олегович
Группа №K33421
Проверил:
Харитонов Антон

Санкт-Петербург
2022

Цель работы: закрепить понимание принципов работы DNS, получить практические навыки использования утилит работы с серверами системы DNS и конфигурирования DNS сервера на платформе Linux;

Часть 2. Получение информации из DNS с помощью утилиты dig

1. На хосте c7-1 с выполните команду dig www.itmo.ru. В консольном выводе изучите состав секций HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER: 192.168.0.1, WHEN и MSG SIZE. Соотнесите значения полей секции HEADER со значениями остальных полей. **(!)**

```
vboxuser@UBUNTU:~$ dig www.itmo.ru

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54414
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.itmo.ru.                   IN      A

;; ANSWER SECTION:
www.itmo.ru.            7200    IN      A       51.250.54.78

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 05 21:08:33 MSK 2022
;; MSG SIZE  rcvd: 56
```

2. На хосте c7-1 с помощью утилиты dig решите следующие задачи **(!)**:
    a. Выведите только результат разрешения имени www.itmo.ru (только IP адрес),

```
vboxuser@UBUNTU:~$ dig www.itmo.ru +short
51.250.54.78
```

    b. Выведите на экран подробную информацию о разрешении имени, с выводом всех промежуточных серверов, определите какой именно DNS сервер вернул IP адрес хоста.

    dig +trace www.itmo.ru

```
vboxuser@UBUNTU:~$ dig +trace www.itmo.ru

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> +trace www.itmo.ru
;; global options: +cmd
.                       14400   IN      NS      m.root-servers.net.
.                       14400   IN      NS      a.root-servers.net.
.                       14400   IN      NS      b.root-servers.net.
.                       14400   IN      NS      c.root-servers.net.
.                       14400   IN      NS      d.root-servers.net.
.                       14400   IN      NS      e.root-servers.net.
.                       14400   IN      NS      f.root-servers.net.
.                       14400   IN      NS      g.root-servers.net.
.                       14400   IN      NS      h.root-servers.net.
.                       14400   IN      NS      i.root-servers.net.
.                       14400   IN      NS      j.root-servers.net.
.                       14400   IN      NS      k.root-servers.net.
.                       14400   IN      NS      l.root-servers.net.
;; Received 519 bytes from 127.0.0.53#53(127.0.0.53) in 16 ms
```

c. Выведите конфигурационную запись (SOA) домена itmo.ru, определите, значения каждого из числовых параметров записи, что они означают?

dig SOA +multiline www.itmo.ru

```
vboxuser@UBUNTU:~$ dig SOA +multiline www.itmo.ru

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> SOA +multiline www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24906
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.itmo.ru.                   IN SOA

;; AUTHORITY SECTION:
itmo.ru.                3600 IN SOA ns.itmo.ru. hostmaster.itmo.ru. (
                                    2021011510 ; serial
                                    3600       ; refresh (1 hour)
                                    1800       ; retry (30 minutes)
                                    86400      ; expire (1 day)
                                    3600       ; minimum (1 hour)
                                    )

;; Query time: 36 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 05 21:22:51 MSK 2022
;; MSG SIZE  rcvd: 90
```

HEADER: код операции, статус ответа, идентификатор запроса, флаги:

qr - запрос или ответ (query/response)

ra - recursion desired

ra - recursion available

QUESTION SECTION: текущий запрос

ANSWER SECTION: ответ, полученный от DNS: имя домена, время жизни в секундах, класс (IN - Internet), тип (A - IPv4) IP адрес домена.

AUTHORITY SECTION: показывает имена DNS-серверов, которые обработали запрос

WHEN: время создания запроса

MSG SIZE: размер сообщения

d. Определите, какие сервера обрабатывают почту домена itmo.ru.

MX - mail exchange

dig MX itmo.ru

```
vboxuser@UBUNTU:~$ dig MX itmo.ru

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> MX itmo.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31955
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;itmo.ru.                       IN      MX

;; ANSWER SECTION:
itmo.ru.                7200    IN      MX      10 emx.mail.ru.

;; ADDITIONAL SECTION:
emx.mail.ru.            25      IN      A       217.69.139.180
emx.mail.ru.            25      IN      A       94.100.180.180

;; Query time: 36 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 05 21:24:04 MSK 2022
;; MSG SIZE  rcvd: 93
```

e. Определите какие DNS сервера обслуживают зону itmo.ru и какие у них ip адреса.

dig itmo.ru NS

```
vboxuser@UBUNTU:~$ dig itmo.ru NS

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> itmo.ru NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27309
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;itmo.ru.                       IN      NS

;; ANSWER SECTION:
itmo.ru.                7200    IN      NS      ns.itmo.ru.
itmo.ru.                7200    IN      NS      ns3.itmo.ru.
itmo.ru.                7200    IN      NS      ns5.itmo.ru.
itmo.ru.                7200    IN      NS      ns2.itmo.ru.

;; ADDITIONAL SECTION:
ns.itmo.ru.             4089    IN      A       77.234.194.2

;; Query time: 44 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 05 21:30:20 MSK 2022
;; MSG SIZE  rcvd: 123
```

f. Значение записи в зоне обратного просмотра для 87.250.250.242.

dig -x 87.250.250.242

```
vboxuser@UBUNTU:~$ dig -x 87.250.250.242

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> -x 87.250.250.242
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 917
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;242.250.250.87.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
242.250.250.87.in-addr.arpa. 201 IN     PTR     ya.ru.

;; Query time: 24 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 05 21:28:00 MSK 2022
;; MSG SIZE  rcvd: 75
```

g. Определите количество серверов, поддерживающих корневую зону.

dig . NS +noall + answer

```
vboxuser@UBUNTU:~$ dig NS +noall +answer
.                       6685    IN      NS      a.root-servers.net.
.                       6685    IN      NS      m.root-servers.net.
.                       6685    IN      NS      h.root-servers.net.
.                       6685    IN      NS      d.root-servers.net.
.                       6685    IN      NS      j.root-servers.net.
.                       6685    IN      NS      b.root-servers.net.
.                       6685    IN      NS      l.root-servers.net.
.                       6685    IN      NS      f.root-servers.net.
.                       6685    IN      NS      i.root-servers.net.
.                       6685    IN      NS      g.root-servers.net.
.                       6685    IN      NS      c.root-servers.net.
.                       6685    IN      NS      k.root-servers.net.
.                       6685    IN      NS      e.root-servers.net.
```

Часть 3. Настройка кэширующего DNS сервера

Цель этой части – настроить хост c7-1 как кэширующий DNS сервер для хоста c7-2.

1. С помощью утилиты firewall-cmd разрешите службе dns получать доступ к сети.
2. С помощью systemctl включите и запустите службу bind (она называется named)
3. Отредактируйте /etc/named.conf так, чтобы:
    a. Сервер отвечал на IPv4 адресе из вашей локальной сети,
    b. Не работал поверх IPv6
    c. Позволял обычные и рекурсивные запросы только с ip адресов вашей локальной сети (между c7-1 и c7-2) и с самого хоста c7-1.
    d. Делал рекурсивные запросы.
    e. Вместо версии сервера выводил при запросе «My Own DNS Server»

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html
acl trusted {
        10.0.0.1;
        10.0.0.2;
};

options {
        listen-on port 53 { 127.0.0.1; 10.0.0.0/24; };
        listen-on-v6 port 53 { none; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { trusted; };
        allow-recursion { trusted; };
        version "My Own DNS Server";

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
```

```
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

4. Проверьте разрешение имен на хосте c7-2.

```
[root@c7-2 ~]# ping www.ya.ru
PING ya.ru (87.250.250.242) 56(84) bytes of data.
```

Часть 4. Создание собственной доменной зоны

1. Отредактируйте /etc/named.conf так, чтобы добавить зону на сервер зону домена name_file.local, не допускать трансфер зоны, разрешать все обновления и хранить зону в файле /var/named/name_file.local.db
2. Для проверки файла конфигурации используйте утилиту named-checkconf

```
zone "lan.local" IN {
        type master;
        allow-transfer { none; };
        allow-update { any; };
        file "/var/named/lan.local.db";
};

include "/etc/named.rfc1912.zones";
"/etc/named.conf" 74L, 2043C written
[root@c7-1 ~]# sudo named-checkconf /etc/named.conf
[root@c7-1 ~]# _
```

3. Создайте файл name_file.local.db, содержащий следующие параметры для домена name_file.local:
    a. Имя основного DNS сервера ns1
    b. E-mail администратора hostmaster@name_file.local
    c. Серийный номер зоны по шаблону YYYYMMDDhhmm
    d. Время обновления реплики 43200
    e. Время до повторной попытки 3600
    f. Время работы реплики без обновления 3600000
    g. Минимальный TTL 300
    h. Ip адрес ns1 равный внутреннему IP хоста c7-1
    i. Имя gate c IP равным внутреннему IP хоста c7-1
    j. Псевдоним www, направляющий клиента на хост gate.name_file.local.

```
[root@c7-1 ~]# cat /var/named/lan.local.db
$TTL 300
@       IN      SOA     ns1.lan.local.  root@lan.local (
                        202211121813    ; Serial
                        43200           ; Refresh
                        3600            ; Retry
                        3600000         ; Expire
                        300 )           ; Negative Cache TTL

;

@       IN      NS      ns1.template.lan.

ns1     IN      A       10.0.0.1
gate    IN      A       10.0.0.1
www     IN      CNAME   gate.lan.local.
```

4. Для проверки файла зоны используйте утилиту named-checkzone

```
[root@c7-1 ~]# sudo named-checkzone lan.local /var/named/lan.local.db
zone lan.local/IN: loaded serial 2022111218
OK
```

5. На хосте c7-2 проверьте, что все записи в вашем домене работают

```
[root@c7-2 ~]# ping www.ya.ru
PING ya.ru (87.250.250.242) 56(84) bytes of data.
```