

网络空间安全实训

57117225

宋宇星

Task1:配置客户端

设置静态首选域名服务器

```
nameserver 192.168.184.131
```

```
sudo resolvconf -u
```

利用 dig 命令得到 google 的 IP 地址

```
;; ANSWER SECTION:
www.google.com.      923      IN       A        216.58.200.4
Query time: 25 msec
```

从回应可以看出它来自我们刚刚设置的 DNS 服务器

```
;; Query time: 35 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 12:23:16 EDT 2020
;; MSG SIZE rcvd: 59
```

在我们的服务器中，Wireshark 捕获到了 DNS 请求。

51	2020-09-15 12:23:16.3204531...	192.168.184.132	192.168.184.131	DNS	87 Star
52	2020-09-15 12:23:16.3214448...	192.168.184.131	192.5.5.241	DNS	87 Star
53	2020-09-15 12:23:16.3221869...	192.168.184.131	192.5.5.241	DNS	72 Star

Authority RRs: 0

Additional RRs: 1

▼ Queries

▶ www.google.com: type A, class IN

▼ Additional records

▼ <Root>: tvme OPT

Task2:设置本地 DNS 服务器

配置本地存储内容，禁用 DNSSEC

```
options {
    directory "/var/cache/bind";
```

```
dnssec-enable no;
dump-file "/var/cache/bind/dump.db";
```

重启 BIND9

```
[09/15/20]seed@VM-132:~$ sudo service bind9 restart
```

Ping 请求引起了 DNS 应答，服务器返回了 IP 地址

```
[09/15/20]seed@VM-132:~$ ping www.seu.edu.cn
PING seu-ipv6.cache.saaswaf.com (121.194.14.142) 56(84) bytes of data:
64 bytes from 121.194.14.142: icmp_seq=1 ttl=128 time=59.7 ms
64 bytes from 121.194.14.142: icmp_seq=2 ttl=128 time=59.4 ms
64 bytes from 121.194.14.142: icmp_seq=3 ttl=128 time=60.7 ms
64 bytes from 121.194.14.142: icmp_seq=4 ttl=128 time=59.0 ms
64 bytes from 121.194.14.142: icmp_seq=5 ttl=128 time=58.9 ms
64 bytes from 121.194.14.142: icmp_seq=6 ttl=128 time=59.1 ms
64 bytes from 121.194.14.142: icmp_seq=7 ttl=128 time=59.8 ms
^C
--- seu-ipv6.cache.saaswaf.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 15100ms
rtt min/avg/max/mdev = 58.945/59.562/60.767/0.670 ms
```

178	2020-09-15	12:52:11.0002500...	192.168.184.132	192.168.184.131	ICMP	117
179	2020-09-15	12:52:11.8209942...	192.112.36.4	192.168.184.131	DNS	89
180	2020-09-15	12:52:13.1636320...	192.58.128.30	192.168.184.131	DNS	89
181	2020-09-15	12:52:15.4530310...	199.7.83.42	192.168.184.131	DNS	89
182	2020-09-15	12:52:17.9560595...	192.36.148.17	192.168.184.131	DNS	89
183	2020-09-15	12:52:21.6842448...	:::1	:::1	UDP	64
184	2020-09-15	12:52:41.7042334...	:::1	:::1	UDP	64
185	2020-09-15	12:53:01.7201755...	:::1	:::1	UDP	64
186	2020-09-15	12:53:21.7337062...	:::1	:::1	UDP	64

Length: 53
Checksum: 0x361b [unverified]
[Checksum Status: Unverified]
[Stream index: 3]

▼ Domain Name System (response)
[Request In: 83]
[Time: 9.340878895 seconds]
Transaction ID: 0xe6c0
Flags: 0x8182 Standard query response, Server failure
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries

```
GNU nano 2.5.3 File: /var/cache/bind/dump.db
;
; Start view _default
;
; Cache dump of view '_default' (cache _default)
$DATE 20200915170251
; answer
www.google.com.      2394      IN A      172.217.174.196
; answer
seu-ipv6.cache.saaswaf.com. 2628 A      121.194.14.142
```

Task3:在本地 DNS 服务器中 host a zone

创建 zones

```
*named.conf
/etc/bind

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

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";
};
```

创建正向查找 zone 文件

```

$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

```

编辑逆向检索 zone 文件

Open  *192.168.0.db
/etc/bind

```

$TTL 3D
@      IN      SOA      ns.example.com. admin.example.com. (
      1          ; Serial
      8H         ; Refresh
      2H         ; Retry
      4W         ; Expire
      1D )       ; Minimum

@      IN      NS       ns.example.com.
101    IN      PTR      www.example.com.
102    IN      PTR      mail.example.com.
10     IN      PTR      ns.example.com.

```

重新用 dig 寻找 www.example.com 的 IP 地址

```

[09/15/20]seed@VM-131:~$ sudo service bind9 restart
[09/15/20]seed@VM-131:~$ dig @127.0.0.1 www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @127.0.0.1 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51655
;; 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: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 15 14:13:48 EDT 2020
;; MSG SIZE rcvd: 93

[09/15/20]seed@VM-131:~$

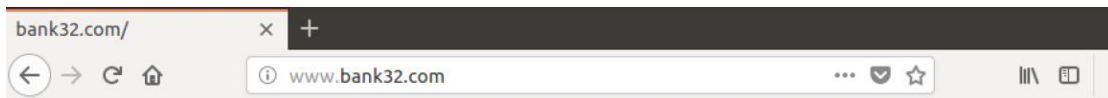
```


Task4:修改 Host File

修改前 ping

```
[09/15/20]seed@VM-131:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=1 ttl=128 time=59.2 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=2 ttl=128 time=68.7 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=3 ttl=128 time=48.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=4 ttl=128 time=48.4 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=5 ttl=128 time=48.9 ms
^C
--- bank32.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 48.424/54.799/68.750/8.089 ms
[09/15/20]seed@VM-131:~$
```

修改前网页



编辑 Host File

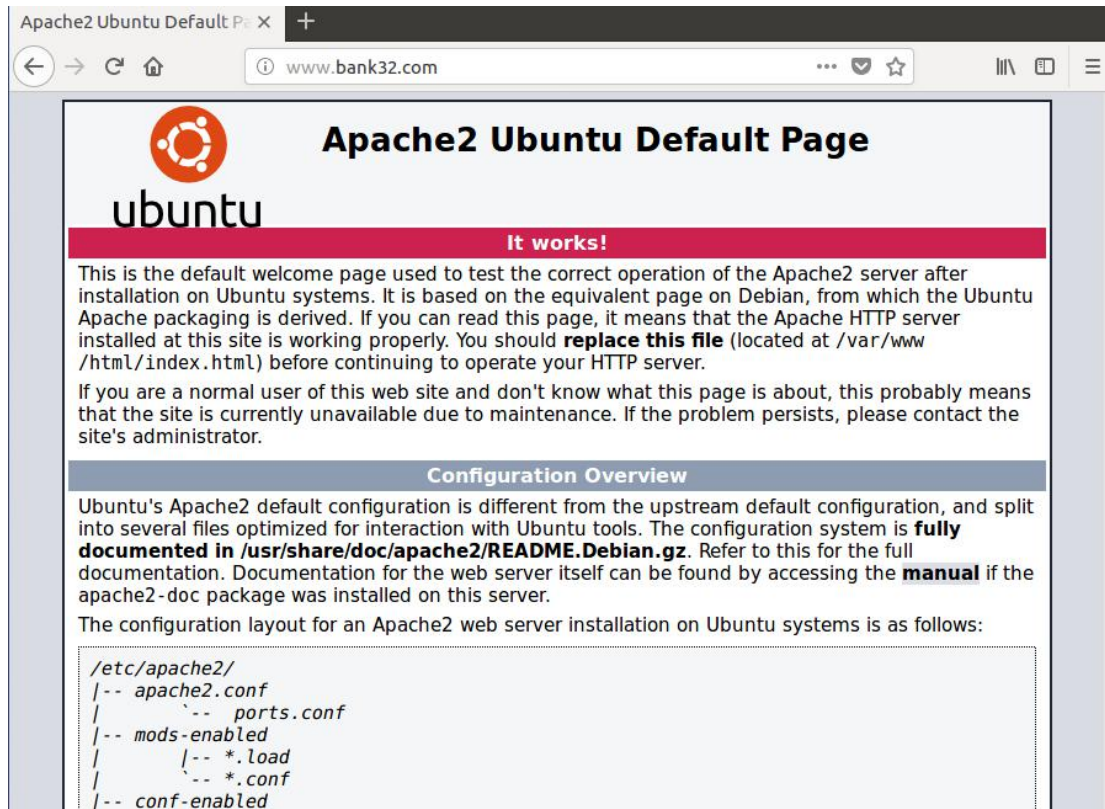
```
Open ▾ hosts
/etc/

127.0.0.1 localhost
127.0.1.1 VM

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1 User
127.0.0.1 Attacker
127.0.0.1 Server
127.0.0.1 www.SeedLabSQLInjection.com
127.0.0.1 www.xsslabelgg.com
127.0.0.1 www.csrflabelgg.com
127.0.0.1 www.csrfattacklab.com
127.0.0.1 www.repackagingattacklab.com
127.0.0.1 www.seedlabclickjacking.com
192.168.184.131 www.bank32.com
```

修改后再 ping

```
[09/15/20]seed@VM-131:~$ ping www.bank32.com
PING www.bank32.com (192.168.184.131) 56(84) bytes of data.
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=2 ttl=64 time=0.073 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=3 ttl=64 time=0.070 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=4 ttl=64 time=0.326 ms
64 bytes from www.bank32.com (192.168.184.131): icmp_seq=5 ttl=64 time=0.126 ms
^C
--- www.bank32.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.031/0.125/0.326/0.105 ms
[09/15/20]seed@VM-131:~$
```



Task5:

加载攻击前:

```
[09/15/20]seed@VM-131:~$ dig www.example.net  
  
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49441  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096  
;; QUESTION SECTION:  
;www.example.net.                IN      A  
  
;; ANSWER SECTION:  
www.example.net.                5       IN      A      93.184.216.34  
  
;; Query time: 2 msec  
;; SERVER: 127.0.1.1#53(127.0.1.1)  
;; WHEN: Tue Sep 15 14:37:07 EDT 2020  
;; MSG SIZE rcvd: 60  
  
[09/15/20]seed@VM-131:~$
```



```
[09/15/20]seed@VM-132:~$ dig www.example.net
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 20276
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.                IN      A
;; ANSWER SECTION:
www.example.net.                600     IN      A      1.2.3.1
;; AUTHORITY SECTION:
.                               600     IN      NS      ns.example.net.
;; ADDITIONAL SECTION:
ns.example.net.                600     IN      A      1.2.3.2

;; Query time: 6 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:18:02 EDT 2020
;; MSG SIZE rcvd: 92

[09/15/20]seed@VM-132:~$
```

```
DNS answer
id=20276 rcode=OK          opcode=QUERY
aa=0 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=2
www.example.net. A
www.example.net. A 600 1.2.3.1
. NS 600 ns.example.net.
ns.example.net. A 600 1.2.3.2
. OPT UDPpl=4096 errcode=0 v=0 ...

^C
[09/15/20]seed@VM-128:~$
```

No.	Time	Source IP	Destination IP	Protocol	Length	Info
83	2020-09-15 15:18:02.4447445...	192.168.184.132	192.168.184.131	DNS	88	Standard query
84	2020-09-15 15:18:02.4500339...	192.168.184.131	192.168.184.132	DNS	136	Standard query response

User Datagram Protocol, Src Port: 46293, Dst Port: 53

Domain Name System (query)

[Response In: 84]

Transaction ID: 0x4f34

Flags: 0x0120 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 1

Queries

- www.example.net: type A, class IN

Additional records

- <Root>: type OPT

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 2

Queries

- www.example.net: type A, class IN

Answers

- www.example.net: type A, class IN, addr 1.2.3.1

Authoritative nameservers

- <Root>: type NS, class IN, ns ns.example.net

Additional records

- ns.example.net: type A, class IN, addr 1.2.3.2
- <Root>: type OPT

我们查看 dump file,

```
[09/15/20]seed@VM-131:~$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200915192326
; authanswer
;
;      276      IN NS      ns.example.net.
; authauthority
ns.example.net.      276      NS      ns.example.net.
; additional
;
;      276      A      1.2.3.2
; authanswer
www.example.net.      276      A      1.2.3.1
;
```

Task7:

由于 Scapy Python 脚本的性能，有时欺骗包比合法的 DNS 响应延迟到达，因此可能需要多次尝试才能成功攻击。攻击者注入一个恶意的命名服务器域

```
[09/15/20]seed@VM-132:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54447
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.      259200  IN      A      1.2.3.1

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

;; ADDITIONAL SECTION:
ns.attacker32.com.    259200  IN      A      1.2.3.4

;; Query time: 45 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:49:18 EDT 2020
;; MSG SIZE rcvd: 139

[09/15/20]seed@VM-132:~$
```

尝试挖掘 example.net 区域中的一个子域。从 Wireshark 我们发现一些由客户端发出的 DNS 请求被发送到 ns.attacker32.com，尽管这不是一个有效的权威域名服务器


```
[09/15/20]seed@VM-132:~$ dig seed.example.net

; <<> DiG 9.10.3-P4-Ubuntu <<> seed.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 64554
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
example.net.                3600    IN      SOA     ns.icann.org. noc.dns.icann.org. 2020091
002 7200 3600 1209600 3600

;; Query time: 45 msec
;; SERVER: 192.168.184.131#53(192.168.184.131)
;; WHEN: Tue Sep 15 15:54:31 EDT 2020
;; MSG SIZE rcvd: 101
```

192.228.79.201	192.168.184.131	DNS	147 Standard query response 0xdcf1 No such name A ns.attacker32.com SOA ns13.domaincontrol.com
192.168.184.131	192.168.184.132	DNS	147 Standard query response 0xiaba No such name A ns.attacker32.com SOA ns13.domaincontrol.com
192.168.184.132	192.168.184.131	DNS	91 Standard query 0x7f42 A ns.attacker32.com.localdomain
192.168.184.131	202.12.27.33	DNS	102 Standard query 0x634a A ns.attacker32.com.localdomain OPT
193.0.14.129	192.168.184.131	DNS	283 Standard query response 0x755b NS <Root> NS i.root-servers.net NS j.root-servers.net NS l.
192.168.184.131	192.58.128.30	DNS	72 Standard query 0x0d8e NS <Root> OPT
192.58.128.30	192.168.184.131	DNS	283 Standard query response 0x0d8e NS <Root> NS g.root-servers.net NS m.root-servers.net NS d.
192.168.184.131	192.36.148.17	DNS	72 Standard query 0x7f16 NS <Root> OPT
192.36.148.17	192.168.184.131	DNS	283 Standard query response 0x7f16 NS <Root> NS k.root-servers.net NS a.root-servers.net NS c.

Authority RRs: 1
Additional RRs: 0

▼ Queries

▼ ns.attacker32.com: type A, class IN

Name: ns.attacker32.com
[Name Length: 17]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

▼ Authoritative nameservers

▼ attacker32.com: type SOA, class IN, mname ns13.domaincontrol.com

Name: attacker32.com
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 3600
Data length: 56
Primary name server: ns13.domaincontrol.com
Responsible authority's mailbox: dns.jomax.net
Serial Number: 2020062300
Refresh Interval: 28800 (8 hours)
Retry Interval: 7200 (2 hours)
Expire limit: 604800 (7 days)
Minimum TTL: 600 (10 minutes)

Query Name (dns.qry.name), 19 bytes Packets: 1071 · Displayed: 1071 (100.0%) Profile: Default