COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

TEST

```
victim:10.9.0.5:PES1UG20CS280:
$>dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49058
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 11557d9843556484010000006341a268423d3b3cab7ceaa9 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

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

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:16:40 UTC 2022
;; MSG SIZE  rcvd: 90

victim:10.9.0.5:PES1UG20CS280:
```

When the dig command is executed, the DNS request packet is forwarded to the attacker machine (attacker's nameserver). The zone file on the attacker's machine redirects the IP address 10.9.0.153, that of the attacker. This answer appears in the answer section as seen above.

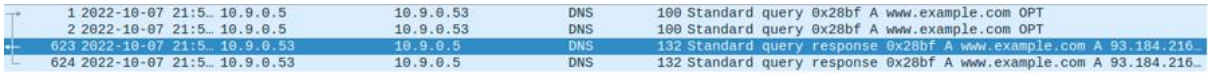
```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2801
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2c416170f64d9e78010000006341a348efdf2fd369d5ef9f (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        86400   IN      A       93.184.216.34

;; Query time: 2152 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:20:24 UTC 2022
;; MSG SIZE  rcvd: 88

victim:10.9.0.5:PES1UG20CS280:
$>
```

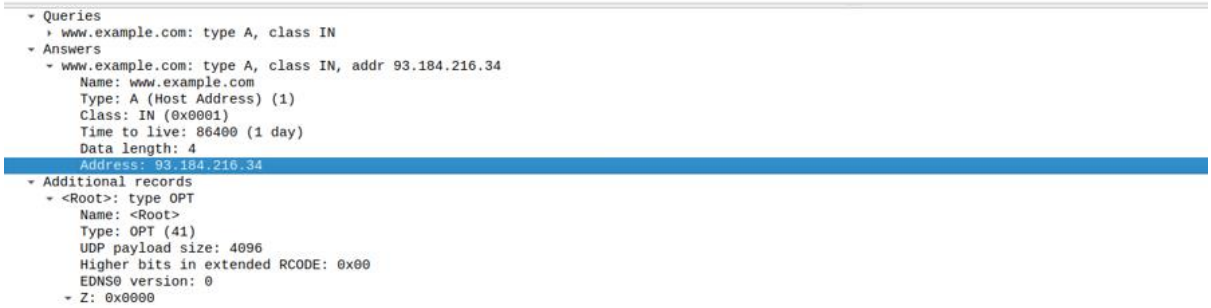
When dig is executed, the DNS query goes to the root server and the official nameserver of example.com and the corresponding IP address of the official nameserver is redirected back to the victim machine.

COMPUTER NETWORK SECURITY LAB -05

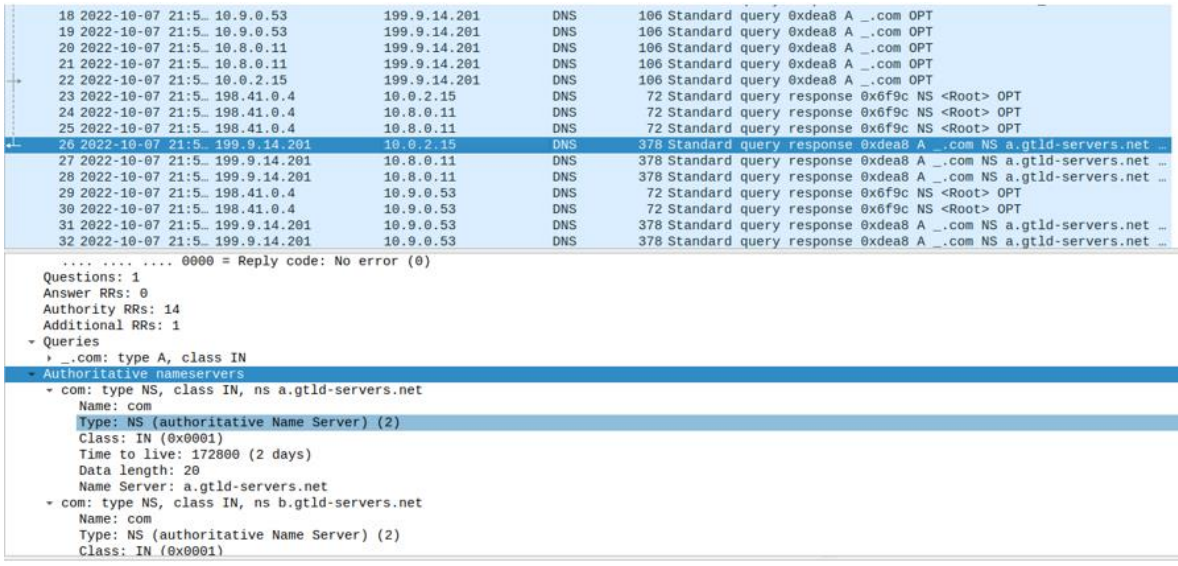
Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section





The corresponding outputs on Wireshark are as shown above.



COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

```
victim:10.9.0.5:PES1UG20CS280:
$>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: 48338
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 89426df8d6ad36a7010000006341a376a98859fe235c119d (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 4 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Sat Oct 08 16:21:10 UTC 2022
;; MSG SIZE  rcvd: 88

victim:10.9.0.5:PES1UG20CS280:
$>
```

When the dig command is redirected to the attacker's nameserver, the IP address stored in the zone file of the attacker redirects the wrong/fake IP address to the victim machine, Hence, the IP address received as an answer is 1.2.3.5 as opposed to what was received before.

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

TASK 1 – DIRECTLY SPOOFING THE RESPONSE TO THE USER

The screenshots for the dig www.example.com are attached above. The IP address sent to the victim machine as answer is the actual IP address of example.com obtained from the legitimate nameserver.

The Wireshark screenshots attached above show the DNS Query response packets being exchanged between the victim machine and the local DNS server.

After this task has been done, we ought to flush the local DNS cache.

```
local-dns:10.9.0.53:PES1UG20CS280:
$>rndc flush
local-dns:10.9.0.53:PES1UG20CS280:
```

The local DNS cache is flushed before starting the attack.

When the victim machine uses the dig command, the DNS query is redirected to the local DNS server. The local DNS server does not hold the answer and hence it redirects the query to the root server and appropriate name servers to obtain the mapping/answer.

The attacker sniffs this DNS query packet and spoofs a DNS reply/ answer with the wrong IP address and redirects it back to the victim as though the response is from the local DNS server. The corresponding output at the victim machine is as shown below-

```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14545
;; 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: 84 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:25:16 UTC 2022
;; MSG SIZE  rcvd: 64

victim:10.9.0.5:PES1UG20CS280:
```

The local DNS cache obtains the actual IP address from the legitimate name server (the spoofed packet has been directly sent by the attacker to the victim machine, not the local DNS server). It therefore caches it and when we see the contents of bind file w.r.t example , we get the below output-

COMPUTER NETWORK SECURITY LAB -05

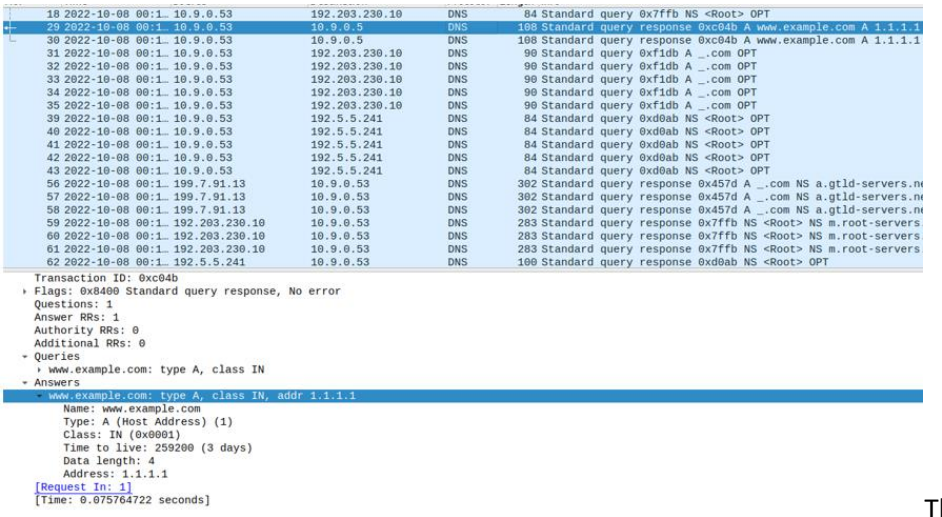
Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

```
$>cat /var/cache/bind/dump.db | grep example
example.com.            691196  NS      a.iana-servers.net.
                                        20221022214625 20221001223409 1686 example
.com.
www.example.com.        691196  A       93.184.216.34
                                        20221022040544 20220930163209 1686 example
.com.
local-dns:10.9.0.53:PES1UG20CS280:
$>
```

Details of the spoofed DNS packet is shown below

```
###[ DNS ]###
          id        = 14545
          qr        = 0
          opcode    = QUERY
          aa        = 0
          tc        = 0
          rd        = 1
          ra        = 0
          z         = 0
          ad        = 1
          cd        = 0
          rcode     = ok
          qdcount   = 1
          ancount   = 0
          nscount   = 0
          arcount   = 1
          \qd        \
           |###[ DNS Question Record ]###
           |  qname     = 'www.example.com.'
           |  qtype     = A
           |  qclass    = IN
          an        = None
          ns        = None
          \ar        \
           |###[ DNS OPT Resource Record ]###
           |  rrname    = '.'
           |  type      = OPT
           |  rclass    = 4096
           |  extrcode  = 0
           |  version   = 0
           |  z         = 0
           |  rdlen     = None
           |  \rdata     \
           |   |###[ DNS EDNS0 TLV ]###
           |   |  optcode   = 10
           |   |  optlen    = 8
           |   |  optdata   = '\x94\xd8\xe9\xb9\xb1\x81\x93\x1b'

.
Sent 1 packets.
^Cseed-attacker:PES1UG20CS280:
```

The spoofed DNS packet from the attacker is sent to the victim directly.



The IP addresses of the local DNS server and the victim machine are flipped in the spoofed packet to make the victim believe that the response was from the local DNS server(when in reality it was not).

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

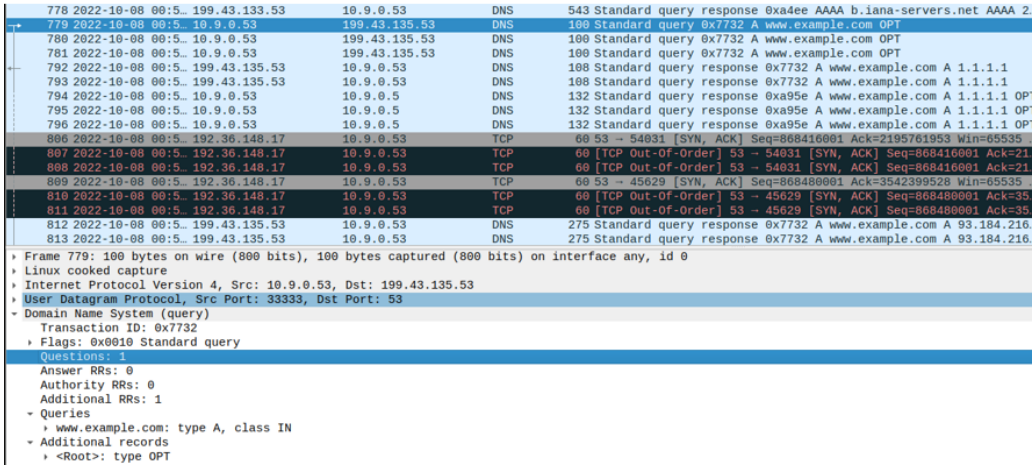
TASK 2 - DNS Cache Poisoning Attack – Spoofing Answers

In this task, the attacker spoofs a DNS reply packet to the local DNS server. The local DNS server stores the wrong mapping and in turn redirects the wrong IP address to the victim machine.

When the dig command is executed on the victim's machine, the victim sends a DNS query packet to the local DNS server. The local DNS server in turn sends out the query outside the local network (to the appropriate legitimate nameserver). However, the attacker spoofs a response packet to the local DNS server and the IP address of example.com is mapped to 1.1.1.1

```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32318
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dabf4a470f40ba79010000006341a5f6d6958c8f9cb8e084 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 1451 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:31:50 UTC 2022
;; MSG SIZE  rcvd: 88

victim:10.9.0.5:PES1UG20CS280:
```

As seen below, the local DNS server queries the root and the nameserver for the response initially. However the spoofed response from the attacker having the IP address 1.1.1.1 makes the local DNS server store 1.1.1.1 in its cache, thus redirecting the wrong IP address to the victim machine.



COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

```
###[ DNS ]###
           id        = 53945
           qr        = 0
           opcode    = QUERY
           aa        = 0
           tc        = 0
           rd        = 0
           ra        = 0
           z         = 0
           ad        = 0
           cd        = 1
           rcode     = ok
           qdcount   = 1
           ancount   = 0
           nscount   = 0
           arcount   = 1
           \qd        \
            |###[ DNS Question Record ]###
            |  qname     = 'www.example.com.'
            |  qtype     = A
            |  qclass    = IN
           an        = None
           ns        = None
           \ar        \
            |###[ DNS OPT Resource Record ]###
            |  rrname    = '.'
            |  type      = OPT
            |  rclass    = 512
            |  extrcode  = 0
            |  version   = 0
            |  z         = D0
            |  rdlen     = None
            |  \rdata     \
            |   |###[ DNS EDNS0 TLV ]###
            |   |  optcode   = 10
            |   |  optlen    = 8
            |   |  optdata   = '\x9f*\xf3?\x10\x869\x1f'

.
Sent 1 packets.
^Cseed-attacker:PES1UG20CS280:
```

The corresponding spoofed packet information is displayed above.

```
local-dns:10.9.0.53:PES1UG20CS280:
$>rndc dumpdb -cache
local-dns:10.9.0.53:PES1UG20CS280:
$>cat /var/cache/bind/dump.db | grep example
example.com.            777493  NS      a.iana-servers.net.
www.example.com.        863894  A       1.1.1.1
local-dns:10.9.0.53:PES1UG20CS280:
```

The wrong entry caused by response spoofing is stored in the cache of the local DNS server as can be seen above.

COMPUTER NETWORK SECURITY LAB -05

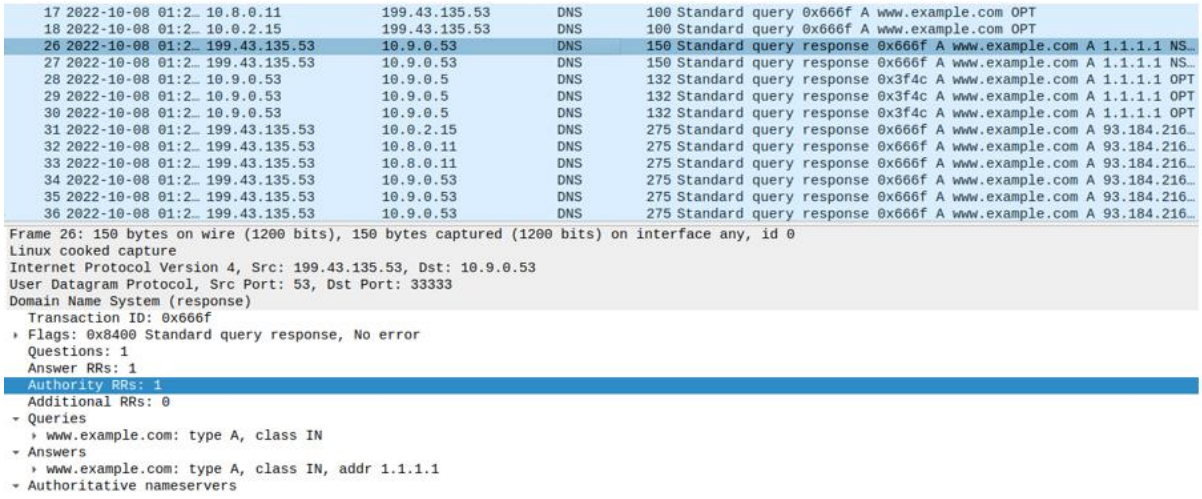
Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

TASK 3 - Spoofing NS Records

In this task, when the attacker sends the spoofed DNS response packet to the local DNS server, the attacker also sends the nameserver detail in the authority section of the DNS reply packet. The local DNS server caches that detail and redirects any other DNS queries that have the same domain to the attacker's machine.

```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37253
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a696edaefe2bfe49010000006341a707e129466a37970ed8 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 2027 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:36:23 UTC 2022
;; MSG SIZE  rcvd: 88

victim:10.9.0.5:PES1UG20CS280:
```

On the victim machine, the result is the same as the previous tasks.



We see that in the response packet, along with the answer, the attacker sends the detail about its nameserver to the local DNS server so it can be cached. The size of the Authority RR is 1, indicating one NS record detail held in it.

The next time when the client uses the dig command for ftp.example.com, the local DNS server redirects the query to the attacker machine.

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

The IP address of ftp.example.com in the attacker's zone file is 1.2.3.6. This is redirected back to the local DNS sever which in turn redirects it back to the victim machine.

```
victim:10.9.0.5:PES1UG20CS280:
$>dig ftp.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36181
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b2e93bab76e1827a010000006341a75fe858339ab19af345 (good)
;; QUESTION SECTION:
;ftp.example.com.               IN      A

;; ANSWER SECTION:
ftp.example.com.        259200  IN      A       1.2.3.6

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:37:51 UTC 2022
;; MSG SIZE  rcvd: 88

victim:10.9.0.5:PES1UG20CS280:
```

The corresponding spoofed DNS packet for www.example.com is as shown below

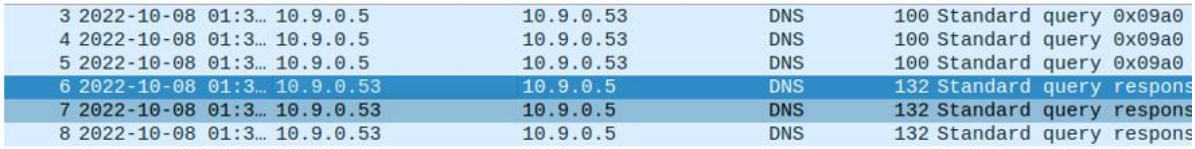
```
           id        = 18403
           qr        = 0
           opcode    = QUERY
           aa        = 0
           tc        = 0
           rd        = 0
           ra        = 0
           z         = 0
           ad        = 0
           cd        = 1
           rcode     = ok
           qdcount   = 1
           ancount   = 0
           nscount   = 0
           arcount   = 1
           \qd        \
            |###[ DNS Question Record ]###
            |  qname     = 'www.example.com.'
            |  qtype     = A
            |  qclass    = IN
           an        = None
           ns        = None
           \ar        \
            |###[ DNS OPT Resource Record ]###
            |  rrname    = '.'
            |  type      = OPT
            |  rclass    = 512
            |  extrcode  = 0
            |  version   = 0
            |  z         = D0
            |  rdlen     = None
            |  \rdata     \
            |   |###[ DNS EDNS0 TLV ]###
            |   |  optcode   = 10
            |   |  optlen    = 8
            |   |  optdata   = '\x9f*\xf3?\x10\x869\x1f'

.
Sent 1 packets.
^Cseed-attacker:PES1UG20CS280:
$>
```

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

```
local-dns:10.9.0.53:PES1UG20CS280:
$>cat /var/cache/bind/dump.db | grep example
example.com.            777490  NS      ns.attacker32.com.
ftp.example.com.        863979  A       1.2.3.6
www.example.com.        863891  A       1.1.1.1
local-dns:10.9.0.53:PES1UG20CS280:
```

The local cache of the DNS server after the attack is successful is as shown below. It holds the name server of the attacker's machine and fake IP addresses for www.example.com and ftp.example.com.



There is no packet spoofing when ftp.example.com is pinged, therefore the Authority RR's are 0.

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

TASK 4 - Spoofing NS Records for Another Domain

The result on victim's machine remains the same for www.example.com

```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54903
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3fe97bfb3d9f4756010000006341a7bfcea5b26104021d8d (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 1971 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:39:27 UTC 2022
;; MSG SIZE  rcvd: 88
```

In this attack, we intend to redirect www.google.com to the attacker's nameserver so that we can successfully redirect to the victim the wrong IP address to a website of a different domain.

When spoofing the DNS response packet (like in Task 3), we additionally add the nameserver of the attacker to the google domain and send this packet to the local DNS server.

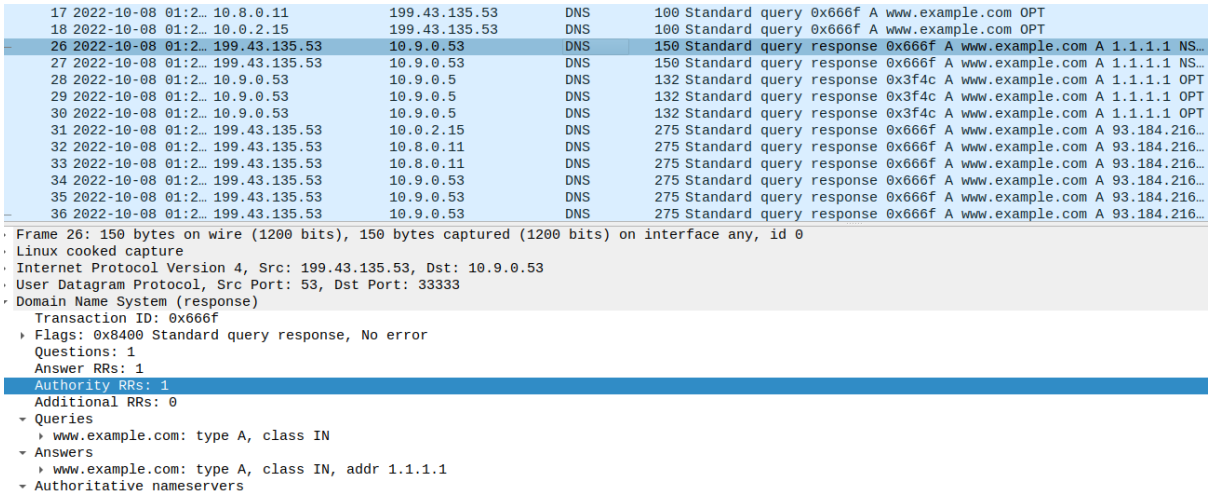
```
local-dns:10.9.0.53:PES1UG20CS280:
$>rndc dumpdb -cache
local-dns:10.9.0.53:PES1UG20CS280:
$>cat /var/cache/bind/dump.db | grep example
example.com.            777563  NS      ns.attacker32.com.
www.example.com.        863964  A       1.1.1.1
local-dns:10.9.0.53:PES1UG20CS280:
```

However, when we observe the local DNS cache, we see that the mapping of the nameserver to google.com is not established at the local DNS cache. Only the mapping of the attacker's nameserver to example.com is mapped.

This is also reflected when we execute the dig command for google.com. We see that the IP address obtained for google is from a legitimate nameserver and not the attacker's machine.

```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24945
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7c83e3817be7eaef010000006341aa13302e4d3ee6cd3d5c (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         300     IN      A       142.250.182.68

;; Query time: 1304 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:49:23 UTC 2022
;; MSG SIZE  rcvd: 87

victim:10.9.0.5:PES1UG20CS280:
```

On Wireshark we see that that only one Authority RR is recorded, not two. This indicates that the NS RR for google.com is dropped/ not included. This must indicate that the Authority section holds only those nameserver RRs that belong to the same domain (drops those that are out of zone) as the one in the DNS query. Responding with nameservers apart from what is queried can cause chaos in the network and hence is not allowed.



COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

The corresponding spoofed DNS packet for www.example.com

```
ra        = 0
z         = 0
ad        = 0
cd        = 1
rcode     = ok
qdcount   = 1
ancount   = 0
nscount   = 0
arcount   = 1
\qd        \
 |###[ DNS Question Record ]###
 |  qname     = 'www.example.com.'
 |  qtype     = A
 |  qclass    = IN
an        = None
ns        = None
\ar        \
 |###[ DNS OPT Resource Record ]###
 |  rrname    = '.'
 |  type      = OPT
 |  rclass    = 512
 |  extrcode  = 0
 |  version   = 0
 |  z         = D0
 |  rdlen     = None
 |  \rdata     \
 |   |###[ DNS EDNS0 TLV ]###
 |   |  optcode   = 10
 |   |  optlen    = 8
 |   |  optdata   = '\x9f*\xf3?\x10\x869\x1f'

.
Sent 1 packets.
^Cseed-attacker:PES1UG20CS280:
$>
```

Therefore, this indicates that we cannot use the NS RR of a different domain to cause cache poisoning of another domain via the Authority section.

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

TASK 5 - Spoofing Records in the Additional Section

The result of dig remains the same at the victim machine except for the additional resource records that are added to the Authority section and the Additional section.

```
victim:10.9.0.5:PES1UG20CS280:
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21482
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

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

;; ADDITIONAL SECTION:
ns.attacker32.com.      259200  IN      A       1.2.3.4
ns.example.net.         259200  IN      A       5.6.7.8
www.facebook.com.       259200  IN      A       3.4.5.6

;; Query time: 88 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sat Oct 08 16:46:07 UTC 2022
;; MSG SIZE  rcvd: 240
```

On the attacker machine, on executing the attack this is what is observed.

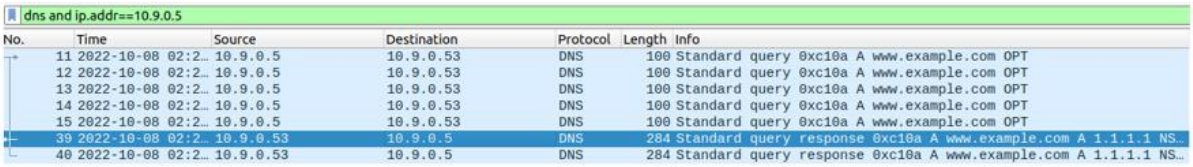
```
^Cseed-attacker:PES1UG20CS280:
$>python3 task5.py
.
Sent 1 packets.
.
Sent 1 packets.
^Cseed-attacker:PES1UG20CS280:
```

The detail of www.facebook.com is dropped by the DNS cache as it does not belong to the zone and hence that detail is dropped. The corresponding mappings that belong to the zone file are noted in the cache and the cache is updated suitably.

```
local-dns:10.9.0.53:PES1UG20CS280:
$>rndc dumpdb -cache
local-dns:10.9.0.53:PES1UG20CS280:
$>cat /var/cache/bind/dump.db | grep example
example.com.            777521  NS      ns.example.com.
www.example.com.        863922  A       1.1.1.1
local-dns:10.9.0.53:PES1UG20CS280:
$>
```

COMPUTER NETWORK SECURITY LAB -05

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section



The DNS packet has two Authority RRs and three Additional RRs, the details of which are shown in the screenshot above.