

## CNS LAB 5 – LOCAL DNS

NAME: NAVYA PERAM

SRN: PES1UG21CS924

### Checks

```
Activities Terminal
Oct 15 05:07
seed@VM: ~/Labsetup5
[10/15/23]seed@VM:~/Labsetup5$ docksh 5b
root@5bb00e8d81ab:/# export PS1="User:PES1UG21CS924:Navya:\w\n$>"
User:PES1UG21CS924:Navya:/
$>dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 24370
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: c89648dab56f511001000000652bab60aa6bb194460d9ef6 (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: Sun Oct 15 09:05:36 UTC 2023
;; MSG SIZE rcvd: 90

User:PES1UG21CS924:Navya:/
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 30584
```

The ip address is obtained from the zone file on the attacker nameserver. Since the attacker nameserver has an ip address of 10.9.0.153, we observe that the server was setup in the correct manner.

```
Activities Terminal
Oct 15 05:07
seed@VM: ~/Labsetup5
;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:05:36 UTC 2023
;; MSG SIZE rcvd: 90

User:PES1UG21CS924:Navya:/
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 30584
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: d79abbaecfb79a3601000000652bab7bb8104eb1707c3845 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

;; Query time: 2460 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:06:03 UTC 2023
;; MSG SIZE rcvd: 88

User:PES1UG21CS924:Navya:/
$>dig @ns.attacker32.com www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns.attacker32.com www.example.com
```

Here, the query goes to the local DNS server and it returns the ip address of example.com, which we know is always constant and of the value 93.184.216.34

```
Activities Terminal Oct 15 05:07
seed@VM: ~/Labsetup5
;; Query time: 2460 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:06:03 UTC 2023
;; MSG SIZE rcvd: 88

User: PES1UG21CS924:Navya:/
$>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: 63794
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 9360cdadab01351501000000652bab8e4b6bc25491e23963 (good)
;; QUESTION SECTION:
;www.example.com. IN A

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

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Sun Oct 15 09:06:22 UTC 2023
;; MSG SIZE rcvd: 88

User: PES1UG21CS924:Navya:/
$>S
```

Here, the DNS query for example.com goes to the attacker's nameserver which then returns it's ip address as 1.2.3.5 . On contrasting with the above two methods, we can imply that this ip has been spoofed.

## Task 1

### Before

```
Activities Terminal Oct 15 05:34
seed@VM: ~/Labsetup5
;; MSG SIZE rcvd: 88

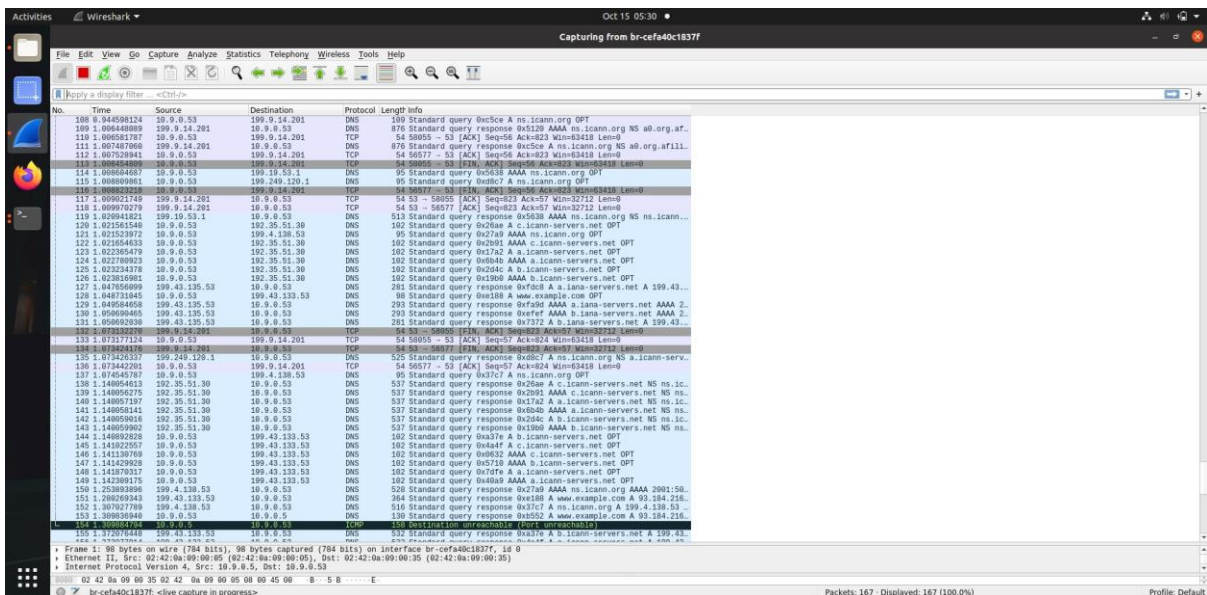
User: PES1UG21CS924:Navya:/
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
; global options: +cmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46418
; 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: 72 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:30:00 UTC 2023
;; MSG SIZE rcvd: 64
```



After

```
Activities Terminal Oct 15 05:34
seed@VM: ~/Labsetup5
www.example.com. IN A
;; ANSWER SECTION:
www.example.com. 259200 IN A 1.1.1.1
;; Query time: 72 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:30:00 UTC 2023
;; MSG SIZE rcvd: 64
User: PES1UG21CS924:Navya:/
$>dig www.example.com
<<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 58818
;; 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: 55 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:32:15 UTC 2023
;; MSG SIZE rcvd: 64
User: PES1UG21CS924:Navya:/
$>
```

We observe that the response to the DNS query sent by the user of example.com is spoofed by the attacker to be 1.1.1.1

```
Activities Terminal Oct 15 05:34
seed@VM: ~/Labsetup5
Sent 1 packets.
^Cattacker: PES1UG21CS924:Navya:/volumes
$>python3 task1.py
###[ Ethernet ]###
dst = 02:42:0a:09:00:35
src = 02:42:0a:09:00:05
type = IPv4
###[ IP ]###
version = 4
ihl = 5
tos = 0x0
len = 84
id = 11958
flags = 0
frag = 0
ttl = 64
proto = udp
chksum = 0x3798
src = 10.9.0.5
dst = 10.9.0.53
\options
###[ UDP ]###
sport = 36299
dport = domain
len = 64
chksum = 0x149d
###[ DNS ]###
id = 58818
qr = 0
opcode = QUERY
aa = 0
```

```
Activities Terminal Oct 15 05:34
seed@VM: ~/Labsetup5
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 ]###
| rrtype = ' '
| type = OPT
| rclass = 4096
| extrcode = 0
| version = 0
| z = 0
| rdlen = None
| \rdata
| ###[ DNS EDNS0 TLV ]###
| | opcode = 10
| | optlen = 8
| | optdata = '\x9ez\xc9\xe0,\xa1%\xd8'
Sent 1 packets.
```

We observe that the packet is sent by the attacker. The packet has the DNS reply for the user's query.



Wireshark interface showing a packet capture on interface br-efad40c1837f. The capture is filtered by 'br-efad40c1837f:live capture in progress'. The packet list shows various protocols including DNS, ARP, and TCP. The packet details pane shows the structure of a DNS query packet (Standard query query 65552 A www.example.com OPT). The packet bytes pane shows the raw data of the packet.

Wireshark interface showing a packet capture on interface br-efad40c1837f. The capture is filtered by 'br-efad40c1837f:live capture in progress'. The packet list shows various protocols including DNS, ARP, and TCP. The packet details pane shows the structure of a DNS query packet (Standard query query 65552 A ns.icann.org OPT). The packet bytes pane shows the raw data of the packet.

Wireshark interface showing a packet capture on interface br-efad40c1837f. The capture is filtered by 'br-efad40c1837f:live capture in progress'. The packet list shows various protocols including DNS, ARP, and TCP. The packet details pane shows the structure of a DNS query packet (Standard query query 65552 A ns.icann.org OPT). The packet bytes pane shows the raw data of the packet.

The image shows a terminal window with a dark theme. The title bar at the top indicates the system is 'Activities' and the window is titled 'Terminal'. The terminal prompt is 'root@c33ab4e54e97: /'. The user has executed several commands to manage DNS records:

```
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc dumpdb -cache
local dns:PES1UG21CS924:Navya:/
$>cat /var/cache/bind/dump.db | grep example
```

The output of the last command shows DNS records for 'example.com' and 'www.example.com'.

```
example.com.          691042   NS       a.iana-servers.net.
                     20231028140639 20231007162139 37939 example.com.
www.example.com.      691042   A        93.184.216.34
                     20231028192921 20231007122139 37939 example.com.

local dns:PES1UG21CS924:Navya:/
$>
```

Here, we can view the cache of the DNS server and find no change, as the spoofed packet was sent to the user by the attacker. There is no change in the ip address here.

Activities
Wireshark
Oct 15 05:54

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capturing on br-cfa40c1b37f

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.1	192.168.1.1	EP	60	Standard query 0x411f to www.example.com OPT
2	0.000370000	192.168.1.1	192.168.1.1	NS	22	Standard query (header) to 192.168.1.1
3	0.000201995	192.168.1.1	192.168.1.1	DNS	88	Standard query 0x042d A - com OPT
4	0.000133001	192.168.1.1	192.168.1.1	DNS	70	Standard query response 0x042d A - com NS - glbl-nservers.net
5	0.000148000	192.168.1.1	192.168.1.1	DNS	200	Standard query response 0x042d A - com NS - glbl-nservers.net
6	0.000420000	192.168.1.1	192.168.1.1	TCP	76	43768 -> NS [ACK] Seq=41 Win=64240 Len=0 MSS=1460 SACK_PERM=1
7	0.000154000	192.168.1.1	192.168.1.1	TCP	74	50135 -> NS [SYN] Seq=41 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	0.000179000	192.168.1.1	192.168.1.1	TCP	60	58 -> 43760 [SYN, ACK] Seq=41 Win=32768 Len=0 MSS=1460
9	0.000184000	192.168.1.1	192.168.1.1	TCP	68	58 -> 50135 [SYN, ACK] Seq=41 Win=32768 Len=0 MSS=1460
10	0.000200000	192.168.1.1	192.168.1.1	TCP	54	43769 -> NS [ACK] Seq=41 Win=64240 Len=0
11	0.000200000	192.168.1.1	192.168.1.1	DNS	94	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
12	0.000200000	192.168.1.1	192.168.1.1	DNS	102	Standard query 0x0407 A - com OPT
13	0.000351742	192.168.1.1	192.168.1.1	DNS	96	Standard query 0x0408 NS -<root> OPT
14	0.000379915	192.168.1.1	192.168.1.1	TCP	54	58 -> 50135 [ACK] Seq=41 Win=32768 Len=0
15	0.000420000	192.168.1.1	192.168.1.1	TCP	54	53 -> 43769 [ACK] Seq=41 Win=32768 Len=0
16	0.000418402	192.168.1.1	192.168.1.1	DNS	1153	Standard query response 0x0408 NS -<root> NS a root-servers.net
17	0.000418700	192.168.1.1	192.168.1.1	DNS	1221	Standard query response 0x0407 A - com NS a glbl-servers.net
18	0.000417736	192.168.1.1	192.168.1.1	DNS	94	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
19	0.000419624	192.168.1.1	192.168.1.1	DNS	94	43769 -> NS [ACK] Seq=41 Win=64240 Len=0
20	0.000437798	192.168.1.1	192.168.1.1	TCP	54	43769 -> NS [FIN, ACK] Seq=41 Win=64240 Len=0
21	0.000455424	192.168.1.1	192.168.1.1	TCP	54	53 -> 43769 [ACK] Seq=41 Win=32768 Len=0
22	0.000455464	192.168.1.1	192.168.1.1	TCP	54	50135 -> NS [FIN, ACK] Seq=41 Win=64240 Len=0
23	0.000454108	192.168.1.1	192.168.1.1	TCP	54	53 -> 50135 [ACK] Seq=41 Win=32768 Len=0
24	0.0004900225	192.168.1.1	192.168.1.1	DNS	96	Standard query 0x0406 A - example.com OPT
25	0.0004900225	192.168.1.1	192.168.1.1	DNS	375	Standard query response 0x0406 A - example.com NS a ns1.serve...
26	0.000515039	192.168.1.1	192.168.1.1	DNS	101	Standard query 0x0405 A - ns1.serve-net OPT
27	0.0005056174	192.168.1.1	192.168.1.1	DNS	101	Standard query 0x0404 AAAA - ns1.serve-net OPT
28	0.0007484412	192.168.1.1	192.168.1.1	DNS	101	Standard query 0x0320a A - ns1.serve-net OPT
29	0.000761917	192.168.1.1	192.168.1.1	DNS	101	Standard query 0x030b AAAA - ns1.serve-net OPT
30	0.000761917	192.168.1.1	192.168.1.1	TCP	60	43769 -> NS [ACK] Seq=41 Win=64240 Len=0
31	0.000761917	192.168.1.1	192.168.1.1	TCP	54	43769 -> NS [ACK] Seq=41 Win=64240 Len=0
32	0.000761917	192.168.1.1	192.168.1.1	TCP	54	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
33	0.000761917	192.168.1.1	192.168.1.1	TCP	54	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
34	0.000761917	192.168.1.1	192.168.1.1	TCP	54	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
35	0.000761917	192.168.1.1	192.168.1.1	TCP	54	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
36	0.000761917	192.168.1.1	192.168.1.1	TCP	54	50135 -> NS [ACK] Seq=41 Win=64240 Len=0
37	0.000761917	192.168.1.1	192.168.1.1	TCP	54	5013

Oct 15 05:54 • Capturing from br-ef40c1837f

No.	Time	Source	Destination	Protocol	Length	Info
108	1.161214862	10.9.0.53	10.9.0.53	TCP	54	53 → 49193 [ACK] Seq=787 Ack=57 Win=32712 Len=0
109	1.161214869	10.9.0.53	10.9.0.53	DNS	95	Standard query 0x50f AAAA ns.icann.org OPT
110	1.161214876	10.9.0.53	10.9.0.53	TCP	54	53 → 49193 [ACK] Seq=787 Ack=57 Win=32712 Len=0
111	1.172208079	10.9.0.53	10.9.0.53	DNS	513	Standard query response 0x50f AAAA ns.icann.org NS ns.icann.org.
112	1.172208086	10.9.0.53	10.9.0.53	DNS	95	Standard query 0x50f AAAA ns.icann.org OPT
113	1.172208093	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA c.icann-servers.net OPT
114	1.172208100	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA b.icann-servers.net OPT
115	1.172208107	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA a.icann-servers.net OPT
116	1.172208114	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org NS ns.icann.org.
117	1.172208121	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
118	1.172208128	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
119	1.172208135	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
120	1.172208142	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
121	1.172208149	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
122	1.172208156	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
123	1.172208163	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
124	1.172208170	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
125	1.172208177	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
126	1.172208184	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
127	1.172208191	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
128	1.172208198	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
129	1.172208205	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
130	1.172208212	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
131	1.172208219	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
132	1.172208226	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
133	1.172208233	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
134	1.172208240	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
135	1.172208247	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
136	1.172208254	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
137	1.172208261	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
138	1.172208268	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
139	1.172208275	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
140	1.172208282	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
141	1.172208289	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
142	1.172208296	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
143	1.172208303	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
144	1.172208310	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
145	1.172208317	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
146	1.172208324	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
147	1.172208331	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
148	1.172208338	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
149	1.172208345	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
150	1.172208352	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
151	1.172208359	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
152	1.172208366	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT
153	1.172208373	10.9.0.53	10.9.0.53	DNS	102	Standard query 0x50f AAAA ns.icann.org OPT

Frame 1: 95 bytes on wire (764 bits), 95 bytes captured (764 bits) on interface br-ef40c1837f, 10.9.0.53  
 Ethernet II, Src: br-ef40c1837f, Dst: 10.9.0.53, Len: 95  
 Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.53  
 User Datagram Protocol, Src Port: 4096, Dst Port: 49193  
 Domain Name System (Standard query response) 0x50f AAAA ns.icann.org NS ns.icann.org. 1.1.1.1

We can observe that the spoofed packet has reached the user much before the actual response.

```

seed@VM: ~/Labsetup5
User: PES1UG21CS924:Navya:/
$dig www.example.com

;<<<> DiG 9.16.1-Ubuntu <<<> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36751
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d186ac81c2d94a4d01000000652bb6de7d5760cbeb80c7cc (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

;; Query time: 1244 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 09:54:38 UTC 2023
;; MSG SIZE rcvd: 88

User: PES1UG21CS924:Navya:/
$

```

We find out the response to the DNS query has been spoofed by the attacker to be 1.1.1.1



```
Oct 15 05:55
seed@VM: ~/Labsetup5
Sent 1 packets.
^Cattacker:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:0b
src      = 02:42:0a:09:00:35
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 39704
flags    =
frag     = 0
ttl      = 64
proto    = udp
chksum   = 0x86e2
src      = 10.9.0.53
dst      = 199.43.135.53
\options
###[ UDP ]###
sport    = 33333
dport    = domain
len      = 64
chksum   = 0x58f0
###[ DNS ]###
id       = 48538
qr       = 0
opcode   = QUERY
aa       = 0
```

```
Oct 15 05:55
seed@VM: ~/Labsetup5
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
\var
###[ DNS OPT Resource Record ]###
| rname   = '.'
| type    = OPT
| rclass  = 512
| extrcode = 0
| version = 0
| z       = 00
| rdlen   = None
| \rdata
| ###[ DNS EDNS0 TLV ]###
| | opcode = 10
| | optlen  = 8
| | optdata = '\xe4\x03ehD5wV'
```

This shows the spoofed packet sent by the attacker. One packet is sent here.

```
Oct 15 05:56
root@c33ab4e54e97: /
seed@VM: ~... x seed@VM: ~... x seed@VM: ~... x seed@VM: ~... x root@c33ab... x root@26ab... x seed@VM: ~... x
local dns:PES1UG21CS924:Navya:/
$>rncd flush
local dns:PES1UG21CS924:Navya:/
$>rncd flush
local dns:PES1UG21CS924:Navya:/
$>rncd flush
local dns:PES1UG21CS924:Navya:/
$>rncd dumpdb -cache
local dns:PES1UG21CS924:Navya:/
$>cat /var/cache/bind/dump.db | grep example
example.com.          777499 NS      a.iana-servers.net.
www.example.com.      863899 A        1.1.1.1
local dns:PES1UG21CS924:Navya:/
$>
```

We observe that the cache of the local DNS server is updated to the ip address of the spoofed reply, from which we can infer that the attack was successful.



## Task 3

```
Oct 15 06:15
seed@VM: ~/Labsetu5

Sent 1 packets.
^Cattacker: PES1UG21CS924: Navya: /volumes
$>python3 task3.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:0b
src      = 02:42:0a:09:00:35
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 56283
flags    =
frag     = 0
ttl      = 64
proto    = udp
chksum   = 0x481f
src      = 10.9.0.53
dst      = 199.43.133.53
\options
###[ UDP ]###
sport    = 33333
dport    = domain
len      = 64
chksum   = 0x56f0
###[ DNS ]###
id       = 9211
qr       = 0
opcode   = QUERY
aa       = 0
tc       = 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       = 0
| rdlen   = None
| \rdata
| |###[ DNS EDNS0 TLV ]###
| | optcode = 10
| | optlen  = 8
| | optdata = '\x8e\xe5\x17\xdeq\xafZ\x0c'

Sent 1 packets.
^Cattacker: PES1UG21CS924: Navya: /volumes
$>
```

We observe that the spoofed reply is sent by the attacker.

```
Oct 15 06:14 • seed@VM: ~/Labsetup5
www.example.com. 259200 IN A 1.1.1.1

;; Query time: 60 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:13:32 UTC 2023
;; MSG SIZE rcvd: 88

User: PES1UG21CS924:Navya:/
$>dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 17315
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 06947098abf325e901000000652bbb87cf9aab5a1a0b2a30 (good)
;; QUESTION SECTION:
;www.example.com. IN A

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

;; Query time: 864 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:14:31 UTC 2023
;; MSG SIZE rcvd: 88

User: PES1UG21CS924:Navya:/
$>
```

We observe that the response is spoofed by the attacker to be 1.1.1.1. This response is then sent to the DNS query.

Oct 15 06:14 • Capturing from br-afa40c1837f

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.9.0.53	10.9.83.42	DNS	80	Standard query 0x1353 A www.example.com OPT
2	0.004240647	10.9.0.53	10.9.83.42	DNS	80	Standard query 0x239a A ...com OPT
3	0.006511506	10.9.0.53	10.9.83.42	DNS	80	Standard query 0x339f NS <root> OPT
4	0.024249817	10.9.7.83.42	10.9.0.53	DNS	380	Standard query response 0x239a A ...com NS a.gtld-servers.net ...
5	0.024551654	10.9.7.83.42	10.9.0.53	DNS	70	Standard query response 0x339f NS <root> OPT
6	0.025179869	10.9.0.53	10.9.7.83.42	TCP	74	41293 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
7	0.027243322	10.9.0.53	10.9.7.83.42	TCP	74	52673 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
8	0.044332863	10.9.7.83.42	10.9.0.53	TCP	58	53 -> 41293 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
9	0.044398494	10.9.0.53	10.9.7.83.42	TCP	54	41293 -> 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.044719061	10.9.0.53	10.9.7.83.42	DNS	90	Standard query 0x1353 NS <root> OPT
11	0.045072487	10.9.7.83.42	10.9.0.53	TCP	58	53 -> 52673 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12	0.045765113	10.9.0.53	10.9.7.83.42	TCP	54	52673 -> 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	0.045954887	10.9.0.53	10.9.7.83.42	DNS	102	Standard query 0x4c7b A ...com OPT
14	0.062805979	10.9.7.83.42	10.9.0.53	DNS	1153	Standard query response 0x4c7b NS <root> NS a.root-servers.net...
15	0.062944384	10.9.0.53	10.9.7.83.42	TCP	54	41293 -> 53 [ACK] Seq=43 Ack=1180 Win=63742 Len=0
16	0.064040061	10.9.0.53	10.9.7.83.42	TCP	54	41293 -> 53 [ACK] Seq=43 Ack=1180 Win=63742 Len=0
17	0.065048603	10.9.7.83.42	10.9.0.53	DNS	1221	Standard query response 0x4c7b A ...com NS a.gtld-servers.net ...
18	0.066139760	10.9.0.53	10.9.7.83.42	TCP	54	52673 -> 53 [ACK] Seq=0 Ack=1160 Win=63073 Len=0
19	0.066633064	10.9.0.53	10.9.7.83.42	TCP	54	52673 -> 53 [FIN, ACK] Seq=0 Ack=1160 Win=63073 Len=0
20	0.067969887	10.9.7.83.42	10.9.0.53	TCP	54	53 -> 41293 [ACK] Seq=1180 Ack=44 Win=32725 Len=0
21	0.068007751	10.9.7.83.42	10.9.0.53	TCP	54	53 -> 52673 [ACK] Seq=1180 Ack=50 Win=32719 Len=0
22	0.070404187	10.9.0.53	102.33.14.30	DNS	90	Standard query 0xa873 A ...example.com OPT
23	0.080088796	10.9.7.83.42	10.9.0.53	TCP	64	53 -> 41293 [FIN, ACK] Seq=1180 Ack=50 Win=32725 Len=0
24	0.085180332	10.9.7.83.42	10.9.0.53	TCP	54	53 -> 52673 [FIN, ACK] Seq=1180 Ack=50 Win=32719 Len=0
25	0.085184332	10.9.0.53	10.9.7.83.42	TCP	54	41293 -> 53 [ACK] Seq=44 Ack=1161 Win=63742 Len=0
26	0.085201433	10.9.0.53	10.9.7.83.42	TCP	54	52673 -> 53 [ACK] Seq=50 Ack=1180 Win=63073 Len=0
27	0.120254730	102.33.14.30	10.9.0.53	DNS	975	Standard query response 0xa873 A ...example.com NS a.lana-serv...
28	0.122589785	10.9.0.53	10.9.14.201	DNS	101	Standard query 0x8b8d A a.lana-servers.net OPT
29	0.122618556	10.9.0.53	10.9.14.201	DNS	101	Standard query 0x91d4 AAAA a.lana-servers.net OPT
30	0.127084888	10.9.0.53	10.9.14.201	DNS	101	Standard query 0xccc2 A b.lana-servers.net OPT
31	0.127172519	10.9.0.53	10.9.14.201	DNS	101	Standard query 0x64af AAAA b.lana-servers.net OPT
32	0.187650001	10.9.14.201	10.9.0.53	DNS	350	Standard query response 0x8b8d A a.lana-servers.net NS a.gtld...
33	0.187659846	10.9.14.201	10.9.0.53	DNS	350	Standard query response 0x91d4 AAAA a.lana-servers.net NS a.g...
34	0.187661446	10.9.14.201	10.9.0.53	DNS	350	Standard query response 0xccc2 A b.lana-servers.net NS a.g...
35	0.187663051	10.9.14.201	10.9.0.53	DNS	350	Standard query response 0x64af AAAA b.lana-servers.net NS a.g...
36	0.190484297	10.9.0.53	10.9.14.201	TCP	74	50843 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
37	0.191384533	10.9.0.53	10.9.14.201	TCP	74	50843 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
38	0.192223366	10.9.0.53	10.9.14.201	TCP	74	50843 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
39	0.193084832	10.9.0.53	10.9.14.201	TCP	74	50843 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
40	0.257964180	10.9.14.201	10.9.0.53	TCP	58	53 -> 50843 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
41	0.257967053	10.9.14.201	10.9.0.53	TCP	58	53 -> 50843 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
42	0.257970506	10.9.14.201	10.9.0.53	TCP	58	53 -> 50843 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
43	0.257972731	10.9.14.201	10.9.0.53	TCP	58	53 -> 50843 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
44	0.258051210	10.9.0.53	10.9.14.201	TCP	54	50789 -> 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
45	0.257146099	10.9.0.53	10.9.14.201	TCP	54	50921 -> 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
46	0.258768758	10.9.0.53	10.9.14.201	TCP	54	50843 -> 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
47	0.258781497	10.9.0.53	10.9.14.201	TCP	54	50843 -> 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
48	0.258921056	10.9.0.53	10.9.14.201	DNS	115	Standard query 0x8d50 AAAA a.lana-servers.net OPT

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-afa40c1837f, id 0

Ethernet II, Src: 02:42:0a:00:00:05 (02:42:0a:00:00:05), Dst: 02:42:0a:00:00:35 (02:42:0a:00:00:35)

Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.53

0000 02 42 0a 00 00 35 02 42 0a 00 00 05 00 45 00 08 5 b .....E

br-afa40c1837f: alive capture in progress

Packets: 153 / Displayed: 153 (100.0%) Profile: Default

Oct 15 06:14 • Capturing from br-caffe40c1837f

No.	Time	Source	Destination	Protocol	Length	Info
106	0.000000000	10.9.0.53	10.9.0.53	DNS	840	Standard query response 840 AAAA ns.icann.org NS a0.org.af.
107	0.000000000	10.9.0.53	10.9.0.53	TCP	54	37078 - 53 [ACK] Seq=56 Ack=787 Win=6366 Len=0
108	0.000000000	10.9.0.53	10.9.0.53	DNS	840	Standard query response 840 AAAA ns.icann.org NS b2.org.af.111.
109	0.000000000	10.9.0.53	10.9.0.53	TCP	54	60319 - 53 [ACK] Seq=56 Ack=787 Win=6366 Len=0
110	0.000000000	10.9.0.53	10.9.0.53	DNS	95	Standard query 840 AAAA ns.icann.org OPT
111	0.000000000	10.9.0.53	10.9.0.53	DNS	95	Standard query 840 AAAA ns.icann.org OPT
112	0.000000000	10.9.0.53	10.9.0.53	TCP	54	37078 - 53 [FIN, ACK] Seq=56 Ack=787 Win=6366 Len=0
113	0.000000000	10.9.0.53	10.9.0.53	TCP	54	60319 - 53 [FIN, ACK] Seq=56 Ack=787 Win=6366 Len=0
114	0.000000000	10.9.0.53	10.9.0.53	TCP	54	53 - 60319 [ACK] Seq=787 Ack=57 Win=52712 Len=0
115	0.000000000	10.9.0.53	10.9.0.53	TCP	54	53 - 60319 [ACK] Seq=787 Ack=57 Win=52712 Len=0
116	0.000000000	10.9.0.53	10.9.0.53	DNS	513	Standard query response 840 AAAA ns.icann.org NS a.icann-s.
117	0.000000000	10.9.0.53	10.9.0.53	DNS	513	Standard query response 840 AAAA ns.icann.org NS b.icann-s.
118	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
119	0.000000000	10.9.0.53	10.9.0.53	DNS	95	Standard query 840 AAAA ns.icann.org OPT
120	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
121	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
122	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
123	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
124	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
125	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
126	0.000000000	10.9.0.53	10.9.0.53	DNS	102	Standard query 840 AAAA ns.icann.org OPT
127	0.000000000	10.9.0.53	10.9.0.53	TCP	54	53 - 60319 [FIN, ACK] Seq=787 Ack=57 Win=52712 Len=0
128	0.000000000	10.9.0.53	10.9.0.53	TCP	54	53 - 60319 [FIN, ACK] Seq=787 Ack=57 Win=52712 Len=0
129	0.000000000	10.9.0.53	10.9.0.53	TCP	54	60319 - 53 [ACK] Seq=56 Ack=787 Win=6366 Len=0
130	0.000000000	10.9.0.53	10.9.0.53	DNS	98	Standard query 840 AAAA ns.icann.org OPT
131	0.000000000	10.9.0.53	10.9.0.53	DNS	293	Standard query response 840 AAAA ns.icann.org OPT
132	0.000000000	10.9.0.53	10.9.0.53	DNS	281	Standard query response 840 AAAA ns.icann.org OPT
133	0.000000000	10.9.0.53	10.9.0.53	DNS	281	Standard query response 840 AAAA ns.icann.org OPT
134	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
135	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
136	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
137	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
138	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
139	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
140	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
141	0.000000000	10.9.0.53	10.9.0.53	DNS	537	Standard query response 840 AAAA ns.icann.org OPT
142	0.000000000	10.9.0.53	10.9.0.53	ARP	42	Who has 10.9.0.53? Tell 10.9.0.1
143	0.000000000	10.9.0.53	10.9.0.53	ARP	42	10.9.0.53 is at 02:42:0a:09:00:35
144	0.000000000	10.9.0.53	10.9.0.53	DNS	148	Standard query response 840 AAAA ns.icann.org OPT
145	0.000000000	10.9.0.53	10.9.0.53	DNS	528	Standard query response 840 AAAA ns.icann.org OPT
146	0.000000000	10.9.0.53	10.9.0.53	DNS	516	Standard query response 840 AAAA ns.icann.org OPT
147	0.000000000	10.9.0.53	10.9.0.53	DNS	130	Standard query response 840 AAAA ns.icann.org OPT
148	0.000000000	10.9.0.53	10.9.0.53	DNS	364	Standard query response 840 AAAA ns.icann.org OPT
149	0.000000000	10.9.0.53	10.9.0.53	ARP	42	Who has 10.9.0.53? Tell 10.9.0.1
150	0.000000000	10.9.0.53	10.9.0.53	ARP	42	10.9.0.53 is at 02:42:0a:09:00:35
151	0.000000000	10.9.0.53	10.9.0.53	ARP	42	Who has 10.9.0.53? Tell 10.9.0.1
152	0.000000000	10.9.0.53	10.9.0.53	ARP	42	10.9.0.53 is at 02:42:0a:09:00:35
153	0.000000000	10.9.0.53	10.9.0.53	ARP	42	Who has 10.9.0.53? Tell 10.9.0.1

Frame 1: 88 bytes on wire (784 bits) captured (784 bits) on interface br-caffe40c1837f, id 0  
Ethernet II, Src: 02:42:0a:09:00:35, Dst: 02:42:0a:09:00:35 (02:42:0a:09:00:35)  
Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.53  
Hypertext Transfer Protocol, Src: 10.9.0.53, Dst: 10.9.0.53  
Packets: 153 | Displayed: 153 (100.0%) | Profile: Default

```

Oct 15 06:15 • seed@VM: ~/Labsetup5
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:14:31 UTC 2023
;; MSG SIZE rcvd: 88

User: PESIUG21CS924:Navya:/
$dig www.example.com

;<<< DiG 9.16.1-Ubuntu <<< www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 34280
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 29b330b72d8fef7101000000652bbbc3f990599dc350136 (good)
;; QUESTION SECTION:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 259147 IN A 1.1.1.1

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:24 UTC 2023
;; MSG SIZE rcvd: 88

User: PESIUG21CS924:Navya:/
$dig ftp.example.com

;<<< DiG 9.16.1-Ubuntu <<< ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 63951
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2ea1b2c0cbf746a201000000652bbbc4d6a4661964b287b (good)
;; QUESTION SECTION:
;ftp.example.com. IN A

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

;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:32 UTC 2023
;; MSG SIZE rcvd: 88

User: PESIUG21CS924:Navya:/
$

```

```

Oct 15 06:15 • seed@VM: ~/Labsetup5
www.example.com. 259147 IN A 1.1.1.1

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:24 UTC 2023
;; MSG SIZE rcvd: 88

User: PESIUG21CS924:Navya:/
$dig ftp.example.com

;<<< DiG 9.16.1-Ubuntu <<< ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 63951
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2ea1b2c0cbf746a201000000652bbbc4d6a4661964b287b (good)
;; QUESTION SECTION:
;ftp.example.com. IN A

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

;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:32 UTC 2023
;; MSG SIZE rcvd: 88

User: PESIUG21CS924:Navya:/
$

```

We observe that various fake ip addresses are given to the example domains, from which we can infer that the ns record has been spoofed.

```
Oct 15 06:17
root@c33ab4e54e97: /

seed@V... seed@V... seed@V... seed@V... root@c3... root@26... seed@V... seed@V...

www.example.com.      863899  A      1.1.1.1
local dns:PES1UG21CS924:Navya:/
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc dumpdb -cache
local dns:PES1UG21CS924:Navya:/
$>cat /var/cache/bind/dump.db | grep example
example.com.          777420  NS      ns.attacker32.com.
ftp.example.com.      863882  A      1.2.3.6
www.example.com.      863821  A      1.1.1.1
local dns:PES1UG21CS924:Navya:/
$>
```

We can observe the updated fake ip addresses of example.com in the cache of the local dns server. Proving that it has been spoofed.

## Task 4

```
Oct 15 06:30
seed@VM: ~/Labsetu5

seed@VM: ~/Labsetu... seed@VM: ~/Labsetu... seed@VM: ~/Labsetu... seed@VM: ~/Labsetu... root@c33ab4e54e97: / seed@VM: ~/Labsetu... root@26abff54c30: / seed@VM: ~/Labsetu...

www.example.com.      259200  IN      A      1.1.1.1

;; Query time: 95 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:28:03 UTC 2023
;; MSG SIZE rcvd: 88

User:PES1UG21CS924:Navya:/
$>dig www.example.com

; <<> DiG 9.16.1-Ubuntu <<> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 4334
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: fab40e7b95c6849701000000652bbf1e146b9a3e77723c75 (good)
;; QUESTION SECTION:
;www.example.com.          IN      A
;; ANSWER SECTION:
www.example.com.          259200  IN      A      1.1.1.1

;; Query time: 1411 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:29:50 UTC 2023
;; MSG SIZE rcvd: 88

User:PES1UG21CS924:Navya:/
$>
```





Activities Wireshark Oct 15 06:30 Capturing from br-efef40c1837f

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
97	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=1, ttl=64
98	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=1, ttl=64
99	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=2, ttl=64
100	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=2, ttl=64
101	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=3, ttl=64
102	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=3, ttl=64
103	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=4, ttl=64
104	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=4, ttl=64
105	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=5, ttl=64
106	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=5, ttl=64
107	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=6, ttl=64
108	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=6, ttl=64
109	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=7, ttl=64
110	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=7, ttl=64
111	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=8, ttl=64
112	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=8, ttl=64
113	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=9, ttl=64
114	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=9, ttl=64
115	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=10, ttl=64
116	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=10, ttl=64
117	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=11, ttl=64
118	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=11, ttl=64
119	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=12, ttl=64
120	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=12, ttl=64
121	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=13, ttl=64
122	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=13, ttl=64
123	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=14, ttl=64
124	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=14, ttl=64
125	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=15, ttl=64
126	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=15, ttl=64
127	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=16, ttl=64
128	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=16, ttl=64
129	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=17, ttl=64
130	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=17, ttl=64
131	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=18, ttl=64
132	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=18, ttl=64
133	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=19, ttl=64
134	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=19, ttl=64
135	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=20, ttl=64
136	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=20, ttl=64
137	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=21, ttl=64
138	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=21, ttl=64
139	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=22, ttl=64
140	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=22, ttl=64
141	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=23, ttl=64
142	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=23, ttl=64
143	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) 64 bytes to 192.168.1.1: seq=24, ttl=64
144	0.000000	192.168.1.1	192.168.1.1	ICMP	60	Echo reply (ping) 64 bytes from 192.168.1.1: seq=24, ttl=64

Frame 1: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface br-efef40c1837f, id 0  
 Ethernet II, Src: 02:42:0a:00:00:05 (02:42:0a:00:00:05), Dst: 02:42:0a:00:00:05 (02:42:0a:00:00:05)  
 Internet Protocol Version 4, Src: 10.9.9.5, Dst: 10.9.9.5  
 0000 02 42 0a 00 00 05 02 42 0a 00 00 05 08 00 45 0e 8 5 8 .....E

br-efef40c1837f: alive capture in progress

Packets: 143 | Displayed: 143 (100.0%)

Profile: Default

The packets which modify the authority section are captured and can be viewed in the above wireshark screenshot.

Activities Terminal Oct 15 06:31

root@c33ab4e54e97: /

```

seed@V... seed@V... seed@V... seed@V... root@c3... seed@V... root@26... seed@V...
$>rndc flush
local dns:PES1UG21CS924:Navya:/
$>rndc dumpdb -cache
local dns:PES1UG21CS924:Navya:/
$>cat /var/cache/bind/dump.db | grep example
example.com. 777514 NS ns.attacker32.com.
www.example.com. 863915 A 1.1.1.1
local dns:PES1UG21CS924:Navya:/
$>

```

We observe that the spoofed ip for example.com gets stored in the cache. However, the spoofed ip for google.com isn't stored which may occur due to dnssec validation. This usually occurs when dnssec is enabled for a website but the spoofed response doesn't have the correct dnssec signature leading the packet to be rejected by the server.

## Task 5

```
Activities Terminal Oct 15 06:41
seed@VM: ~/Labsetu... seed@VM: ~/Labsetu... seed@VM: ~/Labsetu... seed@VM: ~/Labsetu... root@c33ab4e54e97: / seed@VM: ~/Labsetu... root@26abff544c30: / seed@VM: ~/Labsetu...

User: PES1UG21CS924:Navya:/
$>dig www.example.com

; <<> DiG 9.16.1-Ubuntu <<> www.example.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38491
; 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: 71 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:40:49 UTC 2023
;; MSG SIZE rcvd: 240

User: PES1UG21CS924:Navya:/
$>
```

We observe that the spoofed packet is received in the additional section of the DNS reply along with the spoofed records.

```
Activities Terminal Oct 15 06:41
seed@VM: ~/Labsetup5
seed@V... seed@V... seed@V... seed@V... root@c3... seed@V... root@26... seed@V...

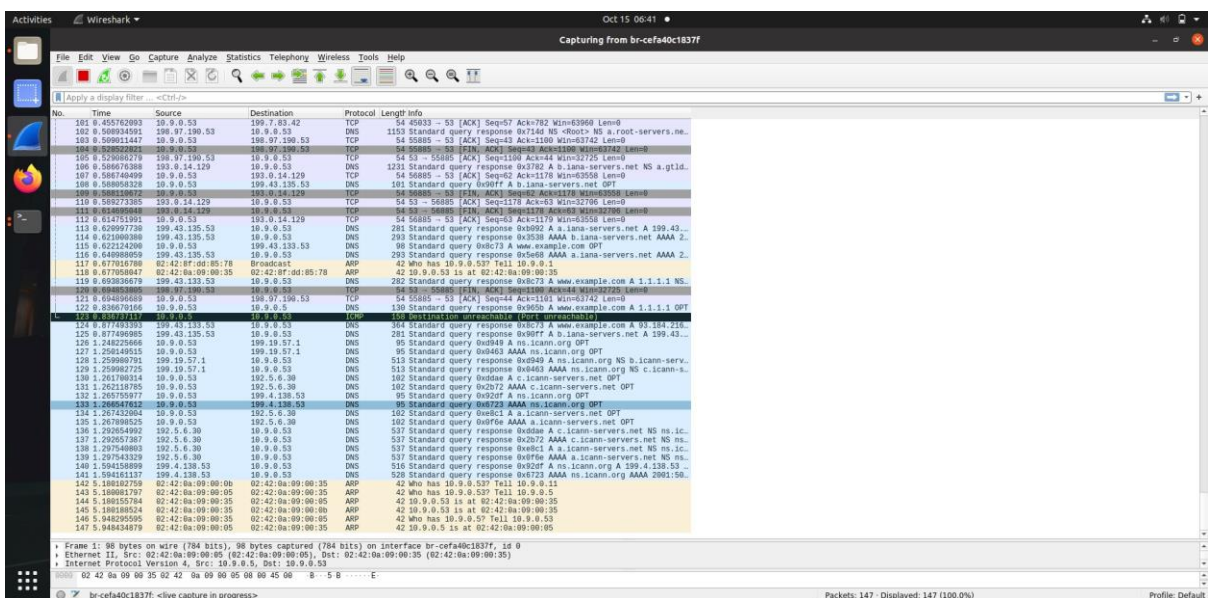
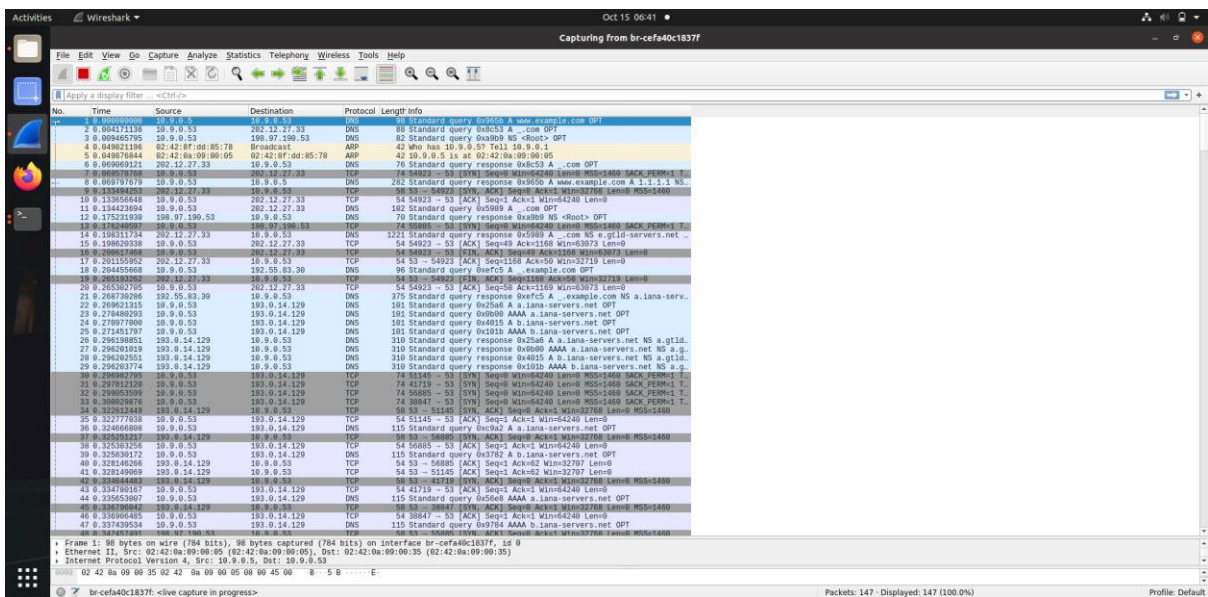
\rddata \
|###[ DNS EDNS0 TLV ]###
|  opcode  = 10
|  optlen   = 8
|  optdata  = '\xe4\x03ehD5wV'

.
Sent 1 packets.
^Cattacker: PES1UG21CS924:Navya:/volumes
$>^C
attacker: PES1UG21CS924:Navya:/volumes
$>^C
attacker: PES1UG21CS924:Navya:/volumes
$>python3 task5.py

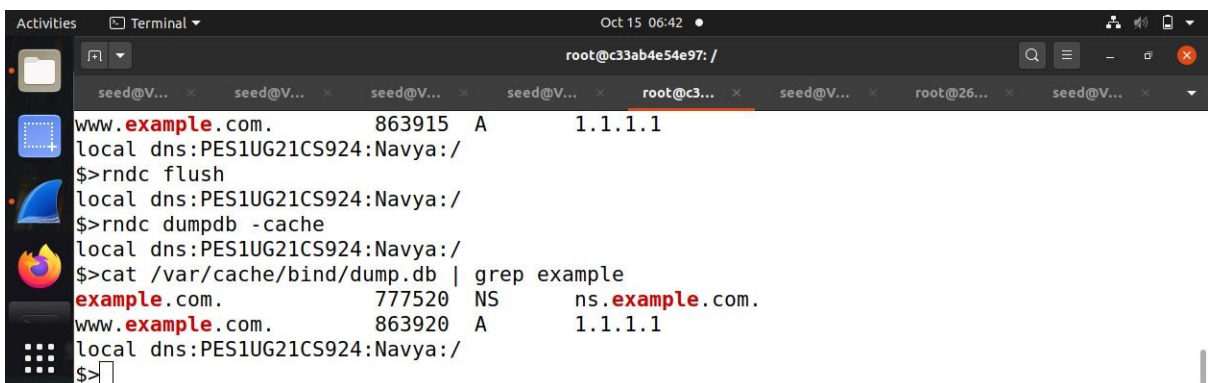
.
Sent 1 packets.

.
Sent 1 packets.
```

We observe that two packets have been sent by the attacker since there are two ns fields in the written code.



From these screenshots we can observe both the first and second spoofed packet.



We observe that the DNS records of the additional section are not cached. This occurs as they are not given a high priority compared to that of the authoritative section. This might be due to increasing the security and making only specific sections high priority.



