

Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No:05
	Section: B	Date: 10/10/2022

Verification of the DNS setup	
Screenshots	<p>Get the IP address of ns.attacker32.com</p> <pre> root@be6b413d2a40:/# export PS1='user:PES2UG20CS016:AdarshKumar/&gt;\$' user:PES2UG20CS016:AdarshKumar/&gt;\$ns.attacker32.com bash: ns.attacker32.com: command not found user:PES2UG20CS016:AdarshKumar/&gt;\$dig ns.attacker32.com  ; &lt;&lt;&gt;&gt; DiG 9.16.1-Ubuntu &lt;&lt;&gt;&gt; ns.attacker32.com ;; global options: +cmd ;; Got answer: ;; -&gt;&gt;HEADER&lt;&lt;- opcode: QUERY, status: NOERROR, id: 2535 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ; COOKIE: fa05d3fd89f602b2010000006345a122d06f87e688304ab5 (good) ;; QUESTION SECTION: ;ns.attacker32.com.                IN      A  ;; ANSWER SECTION: ns.attacker32.com.                259200  IN      A      10.9.0.153  ;; Query time: 8 msec ;; SERVER: 10.9.0.53#53(10.9.0.53) ;; WHEN: Tue Oct 11 17:00:18 UTC 2022 ;; MSG SIZE rcvd: 90 </pre> <p>From the zone file we get IP of the attacker 10.9.0.153</p>
	<p>Get the IP address of <a href="http://www.example.com">www.example.com</a></p> <pre> user:PES2UG20CS016:AdarshKumar/&gt;\$www.example.com bash: www.example.com: command not found user:PES2UG20CS016:AdarshKumar/&gt;\$dig www.example.com  ; &lt;&lt;&gt;&gt; DiG 9.16.1-Ubuntu &lt;&lt;&gt;&gt; www.example.com ;; global options: +cmd ;; Got answer: ;; -&gt;&gt;HEADER&lt;&lt;- opcode: QUERY, status: NOERROR, id: 39743 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ; COOKIE: 4502856cfdac3511010000006345a15f1f9a7ead338ee0d7 (good) ;; QUESTION SECTION: ;www.example.com.                IN      A  ;; ANSWER SECTION: www.example.com.                86400  IN      A      93.184.216.34  ;; Query time: 1820 msec ;; SERVER: 10.9.0.53#53(10.9.0.53) ;; WHEN: Tue Oct 11 17:01:19 UTC 2022 ;; MSG SIZE rcvd: 88 </pre>

There are two entries in the answer section one is the official name server and other one is the attacker's name-server.

```
user:PES2UG20CS016:AdarshKumar/>$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: 34928
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0b14a3f6f14e7ecb010000006345a19b14f82dc8b6927189 (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: Tue Oct 11 17:02:19 UTC 2022
;; MSG SIZE rcvd: 88
```

user:PES2UG20CS016:AdarshKumar/>\$

We requested the attacker's name-server we got IP as 1.2.3.5

### Task1:

### Directly Spoofing Response to User

Clearing the cache on the local DNS Server

```
[10/11/22]seed@VM:~/.../Labsetup$ docksh 4ac
root@4aca5a52c8d9:/# export PS1='local-server:PES2UG20CS016:AdarshKumar/>$'
local-server:PES2UG20CS016:AdarshKumar/>$rndc dumpdb -cache && grep example /var/cache/bind/dump.db
example.com.        690488  NS      a.iana-servers.net.
                    20221022214625 20221001223409 1686 example.com.
www.example.com.    690488  A       93.184.216.34
                    20221022040544 20220930163209 1686 example.com.
local-server:PES2UG20CS016:AdarshKumar/>$rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.  863181  A       10.9.0.153
local-server:PES2UG20CS016:AdarshKumar/>$
local-server:PES2UG20CS016:AdarshKumar/>$rndc flush
local-server:PES2UG20CS016:AdarshKumar/>$
```

Just checking the cache before lab-start

Before performing the attack.

```
user:PES2UG20CS016:AdarshKumar/>$dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12705
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
; COOKIE: 3850e78ee8d63410010000006345ab94b2d424793e72b2a6 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

;; Query time: 1180 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Oct 11 17:44:52 UTC 2022
;; MSG SIZE rcvd: 88

user:PES2UG20CS016:AdarshKumar/>$
```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
794	2022-10-11 13:4...	10.8.0.11	199.43.134.53	DNS	164	Standard query 0xf8bd AAAA c.icann-servers.net OPT
795	2022-10-11 13:4...	10.8.0.11	199.43.134.53	DNS	164	Standard query 0xf8bd AAAA c.icann-servers.net OPT
796	2022-10-11 13:4...	10.0.2.4	199.43.134.53	DNS	164	Standard query 0xf8bd AAAA c.icann-servers.net OPT
797	2022-10-11 13:4...	10.9.0.53	199.43.134.53	DNS	164	Standard query 0x6f18 AAAA a.icann-servers.net OPT
798	2022-10-11 13:4...	10.9.0.53	199.43.134.53	DNS	164	Standard query 0x6f18 AAAA a.icann-servers.net OPT
799	2022-10-11 13:4...	10.8.0.11	199.43.134.53	DNS	164	Standard query 0x6f18 AAAA a.icann-servers.net OPT
800	2022-10-11 13:4...	10.8.0.11	199.43.134.53	DNS	164	Standard query 0x6f18 AAAA a.icann-servers.net OPT
801	2022-10-11 13:4...	10.0.2.4	199.43.134.53	DNS	164	Standard query 0x6f18 AAAA a.icann-servers.net OPT
802	2022-10-11 13:4...	199.43.135.53	10.0.2.4	DNS	530	Standard query response 0x669f AAAA ns.icann.org AAAA 2001:50...
803	2022-10-11 13:4...	199.43.135.53	10.8.0.11	DNS	530	Standard query response 0x669f AAAA ns.icann.org AAAA 2001:50...
804	2022-10-11 13:4...	199.43.135.53	10.8.0.11	DNS	530	Standard query response 0x669f AAAA ns.icann.org AAAA 2001:50...
805	2022-10-11 13:4...	199.43.135.53	10.9.0.53	DNS	530	Standard query response 0x669f AAAA ns.icann.org AAAA 2001:50...
806	2022-10-11 13:4...	199.43.135.53	10.9.0.53	DNS	530	Standard query response 0x669f AAAA ns.icann.org AAAA 2001:50...
807	2022-10-11 13:4...	199.43.135.53	10.0.2.4	DNS	518	Standard query response 0xaa4c A ns.icann.org A 199.4.138.53 ...
808	2022-10-11 13:4...	199.43.135.53	10.8.0.11	DNS	518	Standard query response 0xaa4c A ns.icann.org A 199.4.138.53 ...
809	2022-10-11 13:4...	199.43.135.53	10.8.0.11	DNS	518	Standard query response 0xaa4c A ns.icann.org A 199.4.138.53 ...
810	2022-10-11 13:4...	199.43.135.53	10.9.0.53	DNS	518	Standard query response 0xaa4c A ns.icann.org A 199.4.138.53 ...
811	2022-10-11 13:4...	199.43.135.53	10.9.0.53	DNS	518	Standard query response 0xaa4c A ns.icann.org A 199.4.138.53 ...
812	2022-10-11 13:4...	199.43.135.53	10.0.2.4	DNS	275	Standard query response 0xc29 A www.example.com A 93.184.216...
813	2022-10-11 13:4...	199.43.135.53	10.8.0.11	DNS	275	Standard query response 0xc29 A www.example.com A 93.184.216...
814	2022-10-11 13:4...	199.43.135.53	10.8.0.11	DNS	275	Standard query response 0xc29 A www.example.com A 93.184.216...
815	2022-10-11 13:4...	199.43.135.53	10.9.0.53	DNS	275	Standard query response 0xc29 A www.example.com A 93.184.216...
816	2022-10-11 13:4...	199.43.135.53	10.9.0.53	DNS	275	Standard query response 0xc29 A www.example.com A 93.184.216...
817	2022-10-11 13:4...	10.0.2.4	10.0.2.4	DNS	122	Standard query response 0x31ad A www.example.com A 93.184.216...

Internet Protocol Version 4, Src: 199.43.135.53, Dst: 10.0.2.4  
 User Datagram Protocol, Src Port: 53, Dst Port: 33333  
 Domain Name System (response)  
 Transaction ID: 0xc29  
 Flags: 0x8400 Standard query response, No error  
 Questions: 1  
 Answer RRs: 2  
 Authority RRs: 0  
 Additional RRs: 1  
 Queries  
 Answers  
 www.example.com: type A, class IN, addr 93.184.216.34  
 www.example.com: type RRSIG, class IN  
 Additional records  
 [Request In: 726]  
 [Time: 0.216201093 seconds]

Text item (text), 16 bytes

Packets: 864

```
local-server:PES2UG20CS016:AdarshKumar/>$rndc flush
local-server:PES2UG20CS016:AdarshKumar/>$rndc dumpdb -cache
local-server:PES2UG20CS016:AdarshKumar/>$cat /var/cache/bind/dump.db | grep example
example.com.                776876   NS      a.iana-servers.net.
www.example.com.            690477   A      93.184.216.34
                             20221022040544 20220930163209 1686 example.com.
local-server:PES2UG20CS016:AdarshKumar/>$
```

Here you can observe that we are getting legitimate output.

On attacker terminal after successful attack, we got one packet

```
^Cseed-attacker:PES2UG20CS016:AdarshKumar/>$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       = 58205
  flags    =
  frag     = 0
  ttl      = 64
  proto    = udp
  chksum   = 0x82f0
  src      = 10.9.0.5
  dst      = 10.9.0.53
  \options \
###[ UDP ]###
  sport    = 34732
  dport    = domain
  len      = 64
  chksum   = 0x149d
###[ DNS ]###
  id       = 40086
  qr       = 0
  opcode   = QUERY
  aa       = 0
  tc       = 0
  rd       = 1
```

On User terminal after attack we can observe that in answer section we are getting IP as 1.1.1.1

```
user:PES2UG20CS016:AdarshKumar/>$dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 11742
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ed2277bbed88bccd010000006345cac470b75888ff5e3c05 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                258516  IN      A      1.1.1.1

;; Query time: 112 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Oct 11 19:57:56 UTC 2022
;; MSG SIZE rcvd: 88

user:PES2UG20CS016:AdarshKumar/>$
```

Apply a display filter ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
22	2022-10-11 14:11	35.232.111.17	10.0.2.4	TCP	62	80 → 54274 [ACK] Seq=587751 Ack=1125764605 Win=32681 Len=0
20	2022-10-11 14:11	10.0.2.4	35.232.111.17	TCP	56	54274 → 80 [ACK] Seq=1125764518 Ack=587751 Win=64240 Len=0
19	2022-10-11 14:11	35.232.111.17	10.0.2.4	TCP	62	80 → 54274 [SYN, ACK] Seq=587750 Ack=1125764518 Win=32768 Len=0
18	2022-10-11 14:11	10.0.2.4	35.232.111.17	TCP	76	54274 → 80 [SYN] Seq=1125764517 Win=0 MSS=1460 SACK...
11	2022-10-11 14:11	10.9.0.53	10.9.0.53	ICMP	136	Destination unreachable (Port unreachable)
10	2022-10-11 14:11	10.9.0.53	10.9.0.53	ICMP	136	Destination unreachable (Port unreachable)
9	2022-10-11 14:11	10.9.0.53	10.9.0.53	ICMP	136	Destination unreachable (Port unreachable)
23	2022-10-11 14:11	35.232.111.17	10.0.2.4	HTTP	204	HTTP/1.1 204 No Content
21	2022-10-11 14:11	10.0.2.4	35.232.111.17	HTTP	143	GET / HTTP/1.1
17	2022-10-11 14:11	8.8.8.8	10.0.2.4	DNS	150	Standard query response 0x0ea3 A connectivity-check.ubuntu.co...
16	2022-10-11 14:11	10.0.2.4	8.8.8.8	DNS	102	Standard query 0x0ea3 A connectivity-check.ubuntu.com OPT
8	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	108	Standard query response 0x461e A www.example.com A 1.1.1.1
7	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	108	Standard query response 0x461e A www.example.com A 1.1.1.1
6	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	132	Standard query response 0x461e A www.example.com A 93.184.216...
5	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	132	Standard query response 0x461e A www.example.com A 93.184.216...
4	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	132	Standard query response 0x461e A www.example.com A 93.184.216...
3	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	100	Standard query 0x461e A www.example.com OPT
2	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	100	Standard query 0x461e A www.example.com OPT
1	2022-10-11 14:11	10.9.0.53	10.9.0.53	DNS	100	Standard query 0x461e A www.example.com OPT
13	2022-10-11 14:11	10.0.2.3	10.0.2.4	DHCP	592	DHCP ACK - Transaction ID 0x52d69ded
12	2022-10-11 14:11	10.0.2.4	10.0.2.3	DHCP	324	DHCP Request - Transaction ID 0x52d69ded
15	2022-10-11 14:11	PcsCompu_23:4f:e8		ARP	62	10.0.2.3 is at 08:00:27:23:4f:e8
14	2022-10-11 14:11	PcsCompu_2a:a3:b5		ARP	44	Who has 10.0.2.3? Tell 10.0.2.4

Frame 6: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface any, id 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.5
- User Datagram Protocol, Src Port: 53, Dst Port: 49468
- Domain Name System (response)
  - Transaction ID: 0x461e
  - Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 1
  - Authority RRs: 0
  - Additional RRs: 1
  - Queries
    - www.example.com: type A, class IN
  - Answers
    - www.example.com: type A, class IN, addr 93.184.216.34
  - Additional records

Text item (text), 16 bytes

```
local-server:PES2UG20CS016:AdarshKumar/>$rndc dumpdb -cache
local-server:PES2UG20CS016:AdarshKumar/>$cat /var/cache/bind/dump.db | grep example
example.com.          690680  NS      a.iana-servers.net.
                      20221022214625 20221001223409 1686 example.com.
www.example.com.      690680  A       93.184.216.34
                      20221022040544 20220930163209 1686 example.com.
local-server:PES2UG20CS016:AdarshKumar/>$
```

This still has legal entry it is because we targeted the user not the local host

In case the attack fails which is not my case:

```
// Delay the network traffic by 100ms
# tc qdisc add dev eth0 root netem delay 100ms
// Delete the tc entry
# tc qdisc del dev eth0 root netem
// Show all the tc entries
# tc qdisc show dev eth
```

seed@VM: ~/.../Labsetup

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x root@07e3002b65ea: /
user:PES2UG20CS016:AdarshKumar/>$tc qdisc add dev eth0 root netem delay 100ms
user:PES2UG20CS016:AdarshKumar/>$tc qdisc del dev eth0 root netem
user:PES2UG20CS016:AdarshKumar/>$tc qdisc show dev eth0
qdisc noqueue 0: root refcnt 2
user:PES2UG20CS016:AdarshKumar/>$tc qdisc add dev eth0 root netem delay 100ms
user:PES2UG20CS016:AdarshKumar/>$tc qdisc show dev eth0
qdisc netem 8002: root refcnt 2 limit 1000 delay 100.0ms
user:PES2UG20CS016:AdarshKumar/>$
```



### Task 2:

### DNS Cache Poisoning Attack – Spoofing Answers

Attacker  
Terminal

```
seed-attacker: PES2UG20CS016: AdarshKumar /> $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       = 59236
  flags    =
  frag     = 0
  ttl      = 64
  proto    = udp
  chksum   = 0x3a96
  src      = 10.9.0.53
  dst      = 199.43.135.53
  \options \
###[ UDP ]###
  sport    = 33333
  dport    = domain
  len      = 64
  chksum   = 0x58f0
###[ DNS ]###
  id       = 16632
  qr       = 0
  opcode   = QUERY
  aa       = 0
  tc       = 0
  rd       = 0
  ra       = 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 = '\xf4Z\xa3\x99\xfc\xec\xa8h'
.
Sent 1 packets.
```

As we can see that in attacker terminal 1 packet is sent in IPv4 type.

User  
Terminal

```
user:PES2UG20CS016:AdarshKumar/>$dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3105
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d89cb77e0913c3a3010000006345b85a60e5cd63199559fd (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

;; Query time: 1464 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Oct 11 18:39:22 UTC 2022
;; MSG SIZE rcvd: 88

user:PES2UG20CS016:AdarshKumar/>$
```

Example.com has IP of 1.1.1.1

Wireshark  
Observation

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
Apply a display filter ... <Ctrl-/>									
No.	Time	Source	Destination	Protocol	Length	Info			
708	2022-10-11 14:3...	199.43.133.53	10.8.0.11	DNS	543	Standard query response	0xa5d0	AAAA b.iana-servers.net	AAAA 2...
709	2022-10-11 14:3...	199.43.133.53	10.8.0.11	DNS	543	Standard query response	0xa5d0	AAAA b.iana-servers.net	AAAA 2...
710	2022-10-11 14:3...	199.43.133.53	10.8.0.11	DNS	543	Standard query response	0xf44d	AAAA a.iana-servers.net	AAAA 2...
711	2022-10-11 14:3...	199.43.133.53	10.8.0.11	DNS	543	Standard query response	0xf44d	AAAA a.iana-servers.net	AAAA 2...
712	2022-10-11 14:3...	199.43.133.53	10.9.0.53	DNS	543	Standard query response	0xa5d0	AAAA b.iana-servers.net	AAAA 2...
713	2022-10-11 14:3...	199.43.133.53	10.9.0.53	DNS	543	Standard query response	0xa5d0	AAAA b.iana-servers.net	AAAA 2...
714	2022-10-11 14:3...	199.43.133.53	10.9.0.53	DNS	543	Standard query response	0xa5d0	AAAA b.iana-servers.net	AAAA 2...
715	2022-10-11 14:3...	199.43.133.53	10.9.0.53	DNS	543	Standard query response	0xf44d	AAAA a.iana-servers.net	AAAA 2...
716	2022-10-11 14:3...	199.43.133.53	10.9.0.53	DNS	543	Standard query response	0xf44d	AAAA a.iana-servers.net	AAAA 2...
717	2022-10-11 14:3...	199.43.133.53	10.9.0.53	DNS	543	Standard query response	0xf44d	AAAA a.iana-servers.net	AAAA 2...
725	2022-10-11 14:3...	199.43.135.53	10.9.0.53	DNS	108	Standard query response	0x40f8	A www.example.com	A 1.1.1.1
726	2022-10-11 14:3...	199.43.135.53	10.9.0.53	DNS	108	Standard query response	0x40f8	A www.example.com	A 1.1.1.1
739	2022-10-11 14:3...	10.9.0.53	10.9.0.5	DNS	132	Standard query response	0xc21	A www.example.com	A 1.1.1.1 OPT
740	2022-10-11 14:3...	10.9.0.53	10.9.0.5	DNS	132	Standard query response	0xc21	A www.example.com	A 1.1.1.1 OPT
741	2022-10-11 14:3...	10.9.0.53	10.9.0.5	DNS	132	Standard query response	0xc21	A www.example.com	A 1.1.1.1 OPT
742	2022-10-11 14:3...	10.9.0.53	192.36.148.17	DNS	127	Standard query	0x4fc3	AAAA ns.icann.org	OPT
745	2022-10-11 14:3...	10.8.0.11	192.36.148.17	DNS	127	Standard query	0x4fc3	AAAA ns.icann.org	OPT
747	2022-10-11 14:3...	10.8.0.2.4	192.36.148.17	DNS	127	Standard query	0x4fc3	AAAA ns.icann.org	OPT
760	2022-10-11 14:3...	10.9.0.53	192.36.148.17	DNS	127	Standard query	0x2e10	A ns.icann.org	OPT
763	2022-10-11 14:3...	10.8.0.11	192.36.148.17	DNS	127	Standard query	0x2e10	A ns.icann.org	OPT
765	2022-10-11 14:3...	10.8.0.2.4	192.36.148.17	DNS	127	Standard query	0x2e10	A ns.icann.org	OPT
778	2022-10-11 14:3...	199.43.135.53	10.0.2.4	DNS	275	Standard query response	0x40f8	A www.example.com	A 93.184.216...
779	2022-10-11 14:3...	199.43.135.53	10.8.0.11	DNS	275	Standard query response	0x40f8	A www.example.com	A 93.184.216...
780	2022-10-11 14:3...	199.43.135.53	10.8.0.11	DNS	275	Standard query response	0x40f8	A www.example.com	A 93.184.216...
▶ User Datagram Protocol, Src Port: 53, Dst Port: 36037 ▶ Domain Name System (response) Transaction ID: 0xc21 ▶ Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 1 ▶ Queries ▶ www.example.com: type A, class IN ▶ Answers ▶ www.example.com: type A, class IN, addr 1.1.1.1 ▶ Additional records ▶ <Root>: type OPT [Request In: 19] [Time: 1.362180337 seconds]									

In answer section we can observe the address as 1.1.1.1

Local – DNS cache	<pre> local-server:PES2UG20CS016:AdarshKumar/&gt;\$rndc flush local-server:PES2UG20CS016:AdarshKumar/&gt;\$rndc dumpdb -cache local-server:PES2UG20CS016:AdarshKumar/&gt;\$cat /var/cache/bind/dump.db   grep example example.com.          776875 NS      a.iana-servers.net. www.example.com.      863276 A       1.1.1.1 local-server:PES2UG20CS016:AdarshKumar/&gt;\$ </pre> <p>As we can see that here cache entry is also found with attacker IP unlike previous one.</p>
<b>Task 3:</b>	<b>Spoofing NS Records</b>
Attacker Terminal	<pre> seed-attacker:PES2UG20CS016:AdarshKumar/&gt;\$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       = 60771   flags    =   frag     = 0   ttl      = 64   proto    = udp   chksum   = 0x3697   src      = 10.9.0.53   dst      = 199.43.133.53   \options \ ###[ UDP ]###   sport    = 33333   dport    = domain   len      = 64   chksum   = 0x56f0 ###[ DNS ]###   id       = 57704   qr       = 0   opcode   = QUERY   aa       = 0   tc       = 0   rd       = 0 </pre> <p>On attacker terminal one packet sent</p>
User Terminal	<pre> user:PES2UG20CS016:AdarshKumar/&gt;\$dig www.example.com  ; &lt;&lt;&gt;&gt; DiG 9.16.1-Ubuntu &lt;&lt;&gt;&gt; www.example.com ;; global options: +cmd ;; Got answer: ;; -&gt;HEADER&lt;- opcode: QUERY, status: NOERROR, id: 5637 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ; COOKIE: 7dd704348bd1d093010000006345c0c5d990ded1622274a2 (good) ;; QUESTION SECTION: ;www.example.com.                IN      A  ;; ANSWER SECTION: www.example.com.                 259200  IN      A      1.1.1.1  ;; Query time: 1407 msec ;; SERVER: 10.9.0.53#53(10.9.0.53) ;; WHEN: Tue Oct 11 19:15:17 UTC 2022 ;; MSG SIZE rcvd: 88  user:PES2UG20CS016:AdarshKumar/&gt;\$ </pre>



```
root@user: /# dig ftp.example.com

;<>> DiG 9.16.1-Ubuntu <>> ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 62543
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 0c0499971b0ab0ae010000006329d93a8c989fa9f00df1fe (good)
;; QUESTION SECTION:
;ftp.example.com.                IN      A

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

;; Query time: 423 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Sep 20 15:16:10 UTC 2022
;; MSG SIZE rcvd: 88
```

### Wireshark output

No.	Time	Source	Destination	Protocol	Length	Info
621	2022-10-11 15:15:17.385281445	199.43.135.53	10.9.0.53	DNS	295	Standard query response 0x9018 AAAA b.iana-servers.net AAAA 2...
628	2022-10-11 15:15:17.385982936	10.9.0.53	199.43.133.53	DNS	100	Standard query 0xe168 A www.example.com OPT
629	2022-10-11 15:15:17.385993094	10.9.0.53	199.43.133.53	DNS	100	Standard query 0xe168 A www.example.com OPT
630	2022-10-11 15:15:17.385982936	10.9.0.53	199.43.133.53	DNS	100	Standard query 0xe168 A www.example.com OPT
631	2022-10-11 15:15:17.386007356	10.8.0.11	199.43.133.53	DNS	100	Standard query 0xe168 A www.example.com OPT
632	2022-10-11 15:15:17.386007356	10.8.0.11	199.43.133.53	DNS	100	Standard query 0xe168 A www.example.com OPT
633	2022-10-11 15:15:17.386008047	10.8.0.2.4	199.43.133.53	DNS	100	Standard query 0xe168 A www.example.com OPT
647	2022-10-11 15:15:17.447963449	199.43.133.53	10.9.0.53	DNS	150	Standard query response 0xe168 A www.example.com A 1.1.1.1 NS...
648	2022-10-11 15:15:17.447970682	199.43.133.53	10.9.0.53	DNS	150	Standard query response 0xe168 A www.example.com A 1.1.1.1 NS...
649	2022-10-11 15:15:17.461363512	10.9.0.53	10.9.0.5	DNS	132	Standard query response 0x1605 A www.example.com A 1.1.1.1 OPT
650	2022-10-11 15:15:17.461389571	10.9.0.53	10.9.0.5	DNS	132	Standard query response 0x1605 A www.example.com A 1.1.1.1 OPT
651	2022-10-11 15:15:17.461363512	10.9.0.53	10.9.0.5	DNS	132	Standard query response 0x1605 A www.example.com A 1.1.1.1 OPT
664	2022-10-11 15:15:17.555137162	10.9.0.53	192.36.148.17	DNS	127	Standard query 0x6109 A ns.icann.org OPT
667	2022-10-11 15:15:17.555322461	10.8.0.11	192.36.148.17	DNS	127	Standard query 0x6109 A ns.icann.org OPT
669	2022-10-11 15:15:17.555330835	10.8.0.2.4	192.36.148.17	DNS	127	Standard query 0x6109 A ns.icann.org OPT
682	2022-10-11 15:15:17.558529406	10.9.0.53	192.36.148.17	DNS	127	Standard query 0x6037 AAAA ns.icann.org OPT
685	2022-10-11 15:15:17.558720973	10.8.0.11	192.36.148.17	DNS	127	Standard query 0x6037 AAAA ns.icann.org OPT
687	2022-10-11 15:15:17.558728824	10.8.0.2.4	192.36.148.17	DNS	127	Standard query 0x6037 AAAA ns.icann.org OPT
688	2022-10-11 15:15:17.605975490	199.43.133.53	10.8.0.2.4	DNS	494	Standard query response 0xe168 A www.example.com A 93.184.216...
689	2022-10-11 15:15:17.606024502	199.43.133.53	10.8.0.11	DNS	494	Standard query response 0xe168 A www.example.com A 93.184.216...
690	2022-10-11 15:15:17.606035727	199.43.133.53	10.8.0.11	DNS	494	Standard query response 0xe168 A www.example.com A 93.184.216...
691	2022-10-11 15:15:17.606212091	199.43.133.53	10.9.0.53	DNS	494	Standard query response 0xe168 A www.example.com A 93.184.216...
692	2022-10-11 15:15:17.606226466	199.43.133.53	10.9.0.53	DNS	494	Standard query response 0xe168 A www.example.com A 93.184.216...
Answer RRs: 1 Authority RRs: 1 Additional RRs: 0 Queries www.example.com: type A, class IN Answers Authoritative nameservers example.com: type NS, class IN, ns.ns.attacker32.com Name: example.com Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 259200 (3 days) Data length: 19 Name Server: ns.attacker32.com [Retransmitted response. Original response in: 647] [Retransmission: True]						

We can see that in Authoritative nameserver an entry as ns.attacher32.com

```
local-server:PES2UG20CS016:AdarshKumar/>$rndc dumpdb -cache
local-server:PES2UG20CS016:AdarshKumar/>$cat /var/cache/bind/dump.db | grep example
example.com.                777202 NS      ns.attacker32.com.
www.example.com.            863603 A      1.1.1.1
local-server:PES2UG20CS016:AdarshKumar/>$
```

```
root@local-server: /# rndc dumpdb -cache

root@local-server: /# cat /var/cache/bind/dump.db | grep example
example.com.                777386 NS      ns.attacker32.com.
ftp.example.com.            863805 A      1.2.3.6
mail.example.com.            863788 A      5.6.7.8
```

We can see that the cache entries that contains example.com linked to attacker's name server this time and check the corresponding forge attacker's IP in [www.example.com](http://www.example.com) and its subdomain [ftp.example.com](http://ftp.example.com) as well.

This cache poising attack takes control of major domain including the sub-domain of example.com

<b>Task 4:</b>	<b>Spoofing NS Records for Another Domain</b>
Attacker Terminal	<pre> seed-attacker:PES2UG20CS016:AdarshKumar/&gt;\$python3 task4.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       = 39024   flags    =   frag     = 0   ttl      = 64   proto    = udp   chksum   = 0x898a   src      = 10.9.0.53   dst      = 199.43.135.53   \options \ ###[ UDP ]###   sport    = 33333   dport    = domain   len      = 64   chksum   = 0x58f0 ###[ DNS ]###   id        = 222   qr        = 0   opcode    = QUERY   aa        = 0   tc        = 0   rd        = 0   ra        = 0 </pre>
User Terminal	<pre> user:PES2UG20CS016:AdarshKumar/&gt;\$dig www.example.com  ; &lt;&lt;&gt;&gt; DiG 9.16.1-Ubuntu &lt;&lt;&gt;&gt; www.example.com ;; global options: +cmd ;; Got answer: ;; -&gt;&gt;HEADER&lt;&lt;- opcode: QUERY, status: NOERROR, id: 8162 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ; COOKIE: a828787835e44e29010000006345c3c8850dd25ca13ed55e (good) ;; QUESTION SECTION: ;www.example.com.                IN      A  ;; ANSWER SECTION: www.example.com.                259200  IN      A      1.1.1.1  ;; Query time: 1432 msec ;; SERVER: 10.9.0.53#53(10.9.0.53) ;; WHEN: Tue Oct 11 19:28:08 UTC 2022 ;; MSG SIZE rcvd: 88  user:PES2UG20CS016:AdarshKumar/&gt;\$ </pre>

No.	Time	Source	Destination	Protocol	Length	Info
870	2022-10-11 15:28:08.251637717	10.9.0.53	199.4.138.53	DNS	97	Standard query 0xc1c AAAA ns.icann.org OPT
871	2022-10-11 15:28:08.251659390	10.8.0.11	199.4.138.53	DNS	97	Standard query 0xc1c AAAA ns.icann.org OPT
872	2022-10-11 15:28:08.251659390	10.8.0.11	199.4.138.53	DNS	97	Standard query 0xc1c AAAA ns.icann.org OPT
873	2022-10-11 15:28:08.251668498	10.0.2.4	199.4.138.53	DNS	97	Standard query 0xc1c AAAA ns.icann.org OPT
874	2022-10-11 15:28:08.260178676	199.4.138.53	10.0.2.4	DNS	518	Standard query response 0x9737 A ns.icann.org A 199.4.138.53 ...
875	2022-10-11 15:28:08.260215246	199.4.138.53	10.8.0.11	DNS	518	Standard query response 0x9737 A ns.icann.org A 199.4.138.53 ...
876	2022-10-11 15:28:08.260221939	199.4.138.53	10.8.0.11	DNS	518	Standard query response 0x9737 A ns.icann.org A 199.4.138.53 ...
877	2022-10-11 15:28:08.260301278	199.4.138.53	10.9.0.53	DNS	518	Standard query response 0x9737 A ns.icann.org A 199.4.138.53 ...
878	2022-10-11 15:28:08.260310142	199.4.138.53	10.9.0.53	DNS	518	Standard query response 0x9737 A ns.icann.org A 199.4.138.53 ...
879	2022-10-11 15:28:08.260301278	199.4.138.53	10.9.0.53	DNS	518	Standard query response 0x9737 A ns.icann.org A 199.4.138.53 ...
887	2022-10-11 15:28:08.298210391	199.43.135.53	10.9.0.53	DNS	191	Standard query response 0x00de A www.example.com A 1.1.1.1 NS...
888	2022-10-11 15:28:08.298227731	199.43.135.53	10.9.0.53	DNS	191	Standard query response 0x00de A www.example.com A 1.1.1.1 NS...
889	2022-10-11 15:28:08.303235079	199.4.138.53	10.0.2.4	DNS	531	Standard query response 0x236d A b.iana-servers.net A 199.43...
890	2022-10-11 15:28:08.303264236	199.4.138.53	10.8.0.11	DNS	531	Standard query response 0x236d A b.iana-servers.net A 199.43...
891	2022-10-11 15:28:08.303269711	199.4.138.53	10.8.0.11	DNS	531	Standard query response 0x236d A b.iana-servers.net A 199.43...
892	2022-10-11 15:28:08.303358895	199.4.138.53	10.9.0.53	DNS	531	Standard query response 0x236d A b.iana-servers.net A 199.43...
893	2022-10-11 15:28:08.303387394	199.4.138.53	10.9.0.53	DNS	531	Standard query response 0x236d A b.iana-servers.net A 199.43...
894	2022-10-11 15:28:08.303358895	199.4.138.53	10.9.0.53	DNS	531	Standard query response 0x236d A b.iana-servers.net A 199.43...
895	2022-10-11 15:28:08.315087180	10.9.0.53	10.9.0.53	DNS	132	Standard query response 0x1fe2 A www.example.com A 1.1.1.1 OPT
896	2022-10-11 15:28:08.315087082	10.9.0.53	10.9.0.53	DNS	132	Standard query response 0x1fe2 A www.example.com A 1.1.1.1 OPT

Answer RRs: 1  
Authority RRs: 2  
Additional RRs: 0  
Queries  
  www.example.com: type A, class IN  
Answers  
  Authoritative nameservers  
    example.com: type NS, class IN, ns ns.attacker32.com  
      Name: example.com  
      Type: NS (authoritative Name Server) (2)  
      Class: IN (0x0001)  
      Time to live: 259200 (3 days)  
      Data length: 19  
      Name Server: ns.attacker32.com  
    google.com: type NS, class IN, ns ns.attacker32.com  
      Name: google.com  
      Type: NS (authoritative Name Server) (2)  
      Class: IN (0x0001)  
      Time to live: 259200 (3 days)  
      Data length: 19

Number of authoritative records in packet (dns.count.auth\_rr), 2 bytes

Packets: 977 - Displayed: 977 (1)

As we can see that Authoritative nameserver has two entries now

```
local-server:PES2UG20CS016:AdarshKumar/>>$rndc dumpdb -cache
local-server:PES2UG20CS016:AdarshKumar/>>$cat /var/cache/bind/dump.db | grep example
example.com.          777348 NS      ns.attacker32.com.
www.example.com.      863749 A       1.1.1.1
local-server:PES2UG20CS016:AdarshKumar/>>$
```

Cache entry's after digging [www.google.com](http://www.google.com) is still legal

```
root@4aca5a52c8d9: /
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x root@07e3002b65ee
local-server:PES2UG20CS016:AdarshKumar/>>$cat /var/cache/bind/dump.db | grep google
google.com.          777594 NS      ns1.google.com.
                    777594 NS      ns2.google.com.
                    777594 NS      ns3.google.com.
                    777594 NS      ns4.google.com.
ns1.google.com.      777594 A       216.239.32.10
ns2.google.com.      777594 A       216.239.34.10
ns3.google.com.      777594 A       216.239.36.10
ns4.google.com.      777594 A       216.239.38.10
www.google.com.      605094 A       142.250.195.100
; ns3.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]
; ns4.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]
; ns2.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]
; ns1.google.com [v4 TTL 4] [v6 TTL 4] [v4 success] [v6 success]
local-server:PES2UG20CS016:AdarshKumar/>>$
```

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

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup
seed-attacker:PES2UG20CS016:AdarshKumar/>>$python3 task5.py
.
Sent 1 packets.
```

User  
Terminal

```
user:PES2UG20CS016:AdarshKumar/>$dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
; COOKIE: a0aacd268d50f087010000006345c818e092bbee79f37657 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

;; Query time: 824 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Oct 11 19:46:32 UTC 2022
;; MSG SIZE rcvd: 88

user:PES2UG20CS016:AdarshKumar/>$
```

No.	Time	Source	Destination	Protocol	Length	Info
488	2022-10-11 15:46:32.819603442	199.43.134.53	10.9.0.53	DNS	295	Standard query response 0xddd1 AAAA a.iana-servers.net AAAA 2.
489	2022-10-11 15:46:32.819595414	199.43.134.53	10.9.0.53	DNS	295	Standard query response 0xddd1 AAAA a.iana-servers.net AAAA 2.
497	2022-10-11 15:46:32.866113741	199.43.133.53	10.9.0.53	DNS	284	Standard query response 0x6a78 A www.example.com A 1.1.1.1 NS.
498	2022-10-11 15:46:32.866132885	199.43.133.53	10.9.0.53	DNS	284	Standard query response 0x6a78 A www.example.com A 1.1.1.1 NS.
499	2022-10-11 15:46:32.927193722	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
500	2022-10-11 15:46:32.927223947	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
501	2022-10-11 15:46:32.927229222	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
502	2022-10-11 15:46:32.927873189	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
503	2022-10-11 15:46:32.927886270	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
504	2022-10-11 15:46:32.927873189	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
505	2022-10-11 15:46:32.928001477	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
506	2022-10-11 15:46:32.928001550	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
507	2022-10-11 15:46:32.928011370	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
508	2022-10-11 15:46:32.928013420	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
509	2022-10-11 15:46:32.928015072	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
510	2022-10-11 15:46:32.928015641	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
511	2022-10-11 15:46:32.929636421	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
512	2022-10-11 15:46:32.929646973	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
513	2022-10-11 15:46:32.929636421	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.
514	2022-10-11 15:46:32.929638671	192.41.162.30	10.0.2.4	DNS	539	Standard query response 0x4ddf A b.icann-servers.net NS ns.ic.

Authority RRs: 2  
Additional RRs: 3

- Queries
- Answers
- Authoritative nameservers
  - example.com: type NS, class IN, ns ns.attacker32.com
    - Name: example.com
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 259200 (3 days)
    - Data length: 19
    - Name Server: ns.attacker32.com
  - example.com: type NS, class IN, ns ns.example.com
    - Name: example.com
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 259200 (3 days)
    - Data length: 16
    - Name Server: ns.example.com
- Additional records

Text item (text), 42 bytes

Packets: 823 - Displayed: 823 (100.0%)

Here in Authoritative nameserver multiple entry are also created

```
local-server:PES2UG20CS016:AdarshKumar/>$rndc flush
local-server:PES2UG20CS016:AdarshKumar/>$rndc dumpdb -cache
local-server:PES2UG20CS016:AdarshKumar/>$cat /var/cache/bind/dump.db | grep example
example.com.                777363  NS      ns.example.com.
www.example.com.            863763  A      1.1.1.1
local-server:PES2UG20CS016:AdarshKumar/>$
```

Only one entry is visible because we used grep command for example only.