Project 4

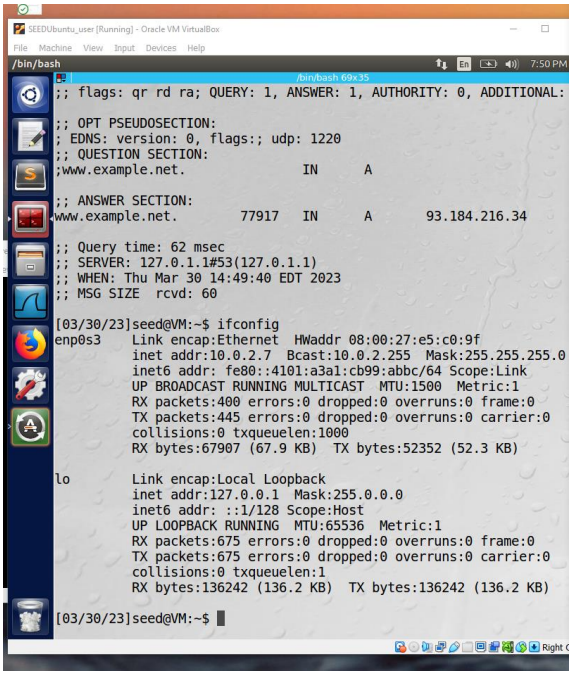
Local DNS Attack Lab

Margi Amin M19219371

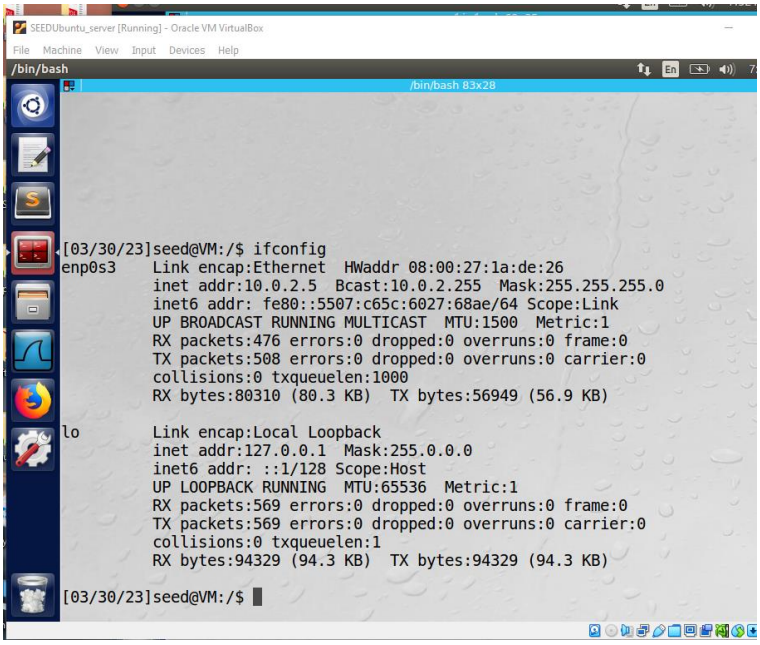
Lab Environment: (Used Virtual machine of project 3)

I successfully set up three virtual machines according to the instructions provided in the paper.

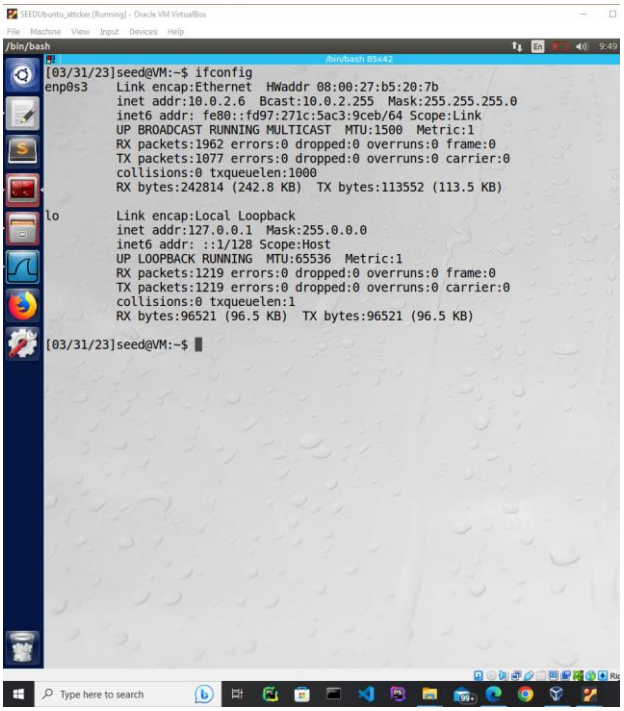
This is my user machine with IP address of 10.0.2.7.



This is my server machine with IP address of 10.0.2.5.



This is my attacker's machine with 10.0.2.6.

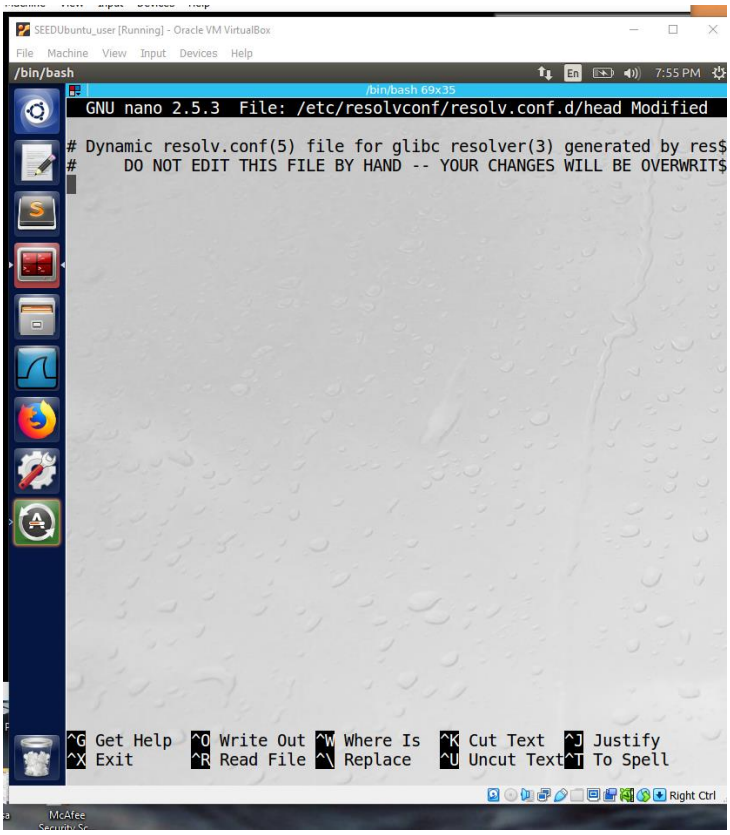


Task 1: Configure the User Machine

Step 1:In user machine:

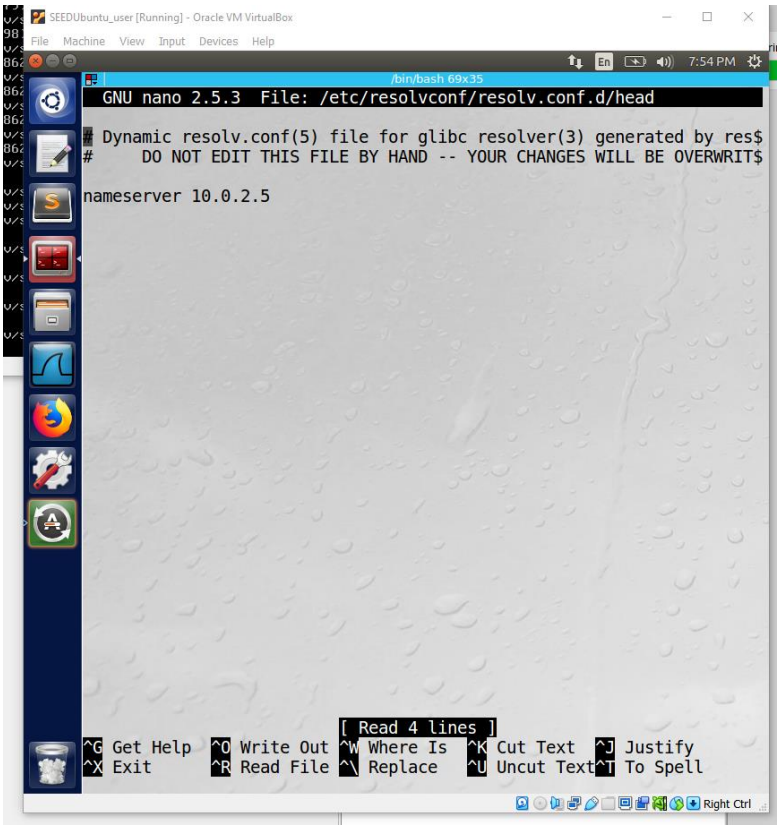
Sudo nano /etc/resolvconf/resolv.conf.d/head or cat /etc/resolv.conf

This command will pop up the following screen:



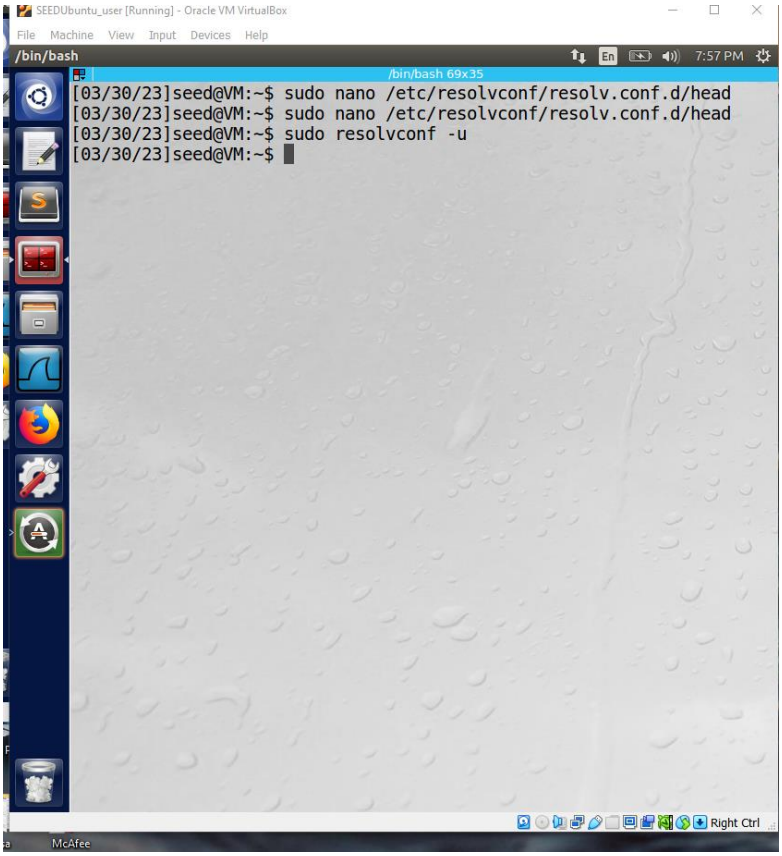
Step 2: In this I edited following command:

Nameserver 10.0.2.7

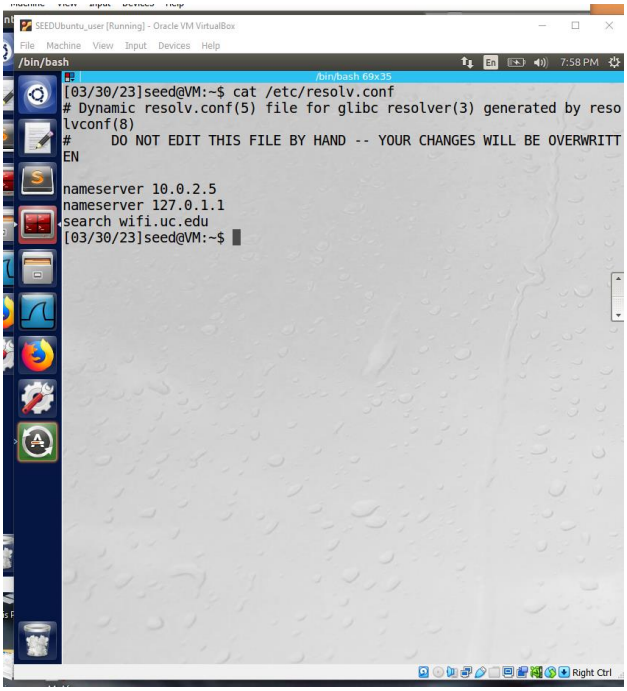


Step 3: run following command in user:

Sudo resolvconf –u



Step 4: cat to confirm updates in /etc/resolv.conf



Here we can see that name server(10.0.2.5) is added in the output of our DNS server

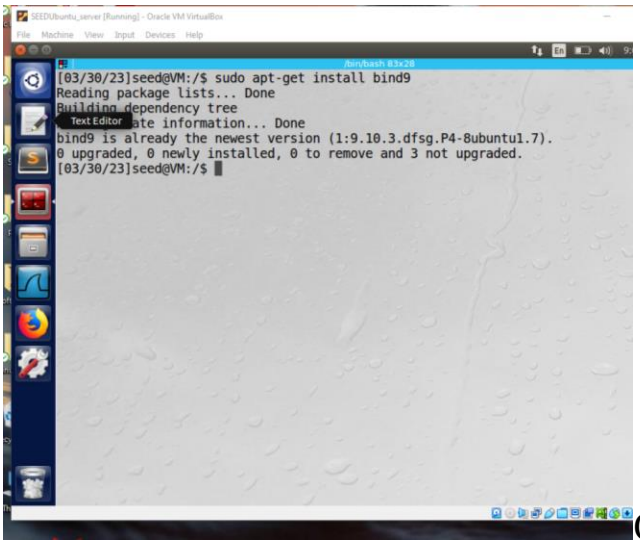
so our user machine is configured.

Task 2: Set up a Local DNS Server

Step 1: configure the bind 9 server

In server install bind9 by following command

Sudo apt-get install bind9



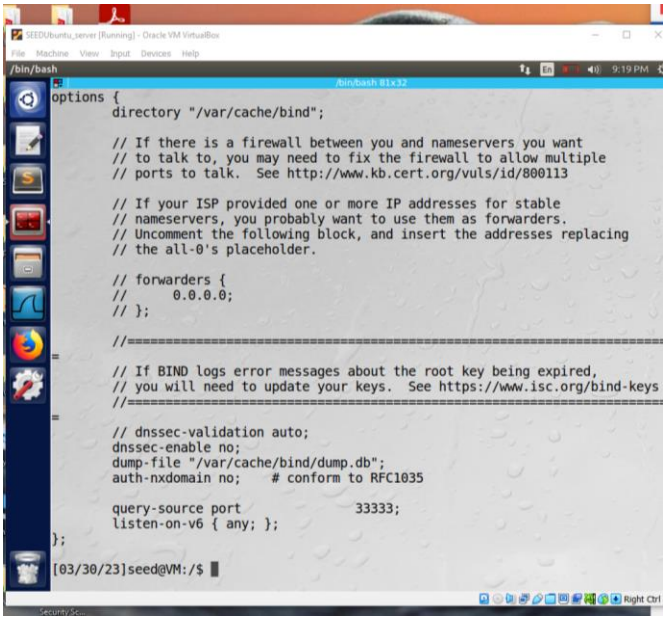
Cat

In server run following command

Cat /etc/bind/named.conf.options

And add dump file

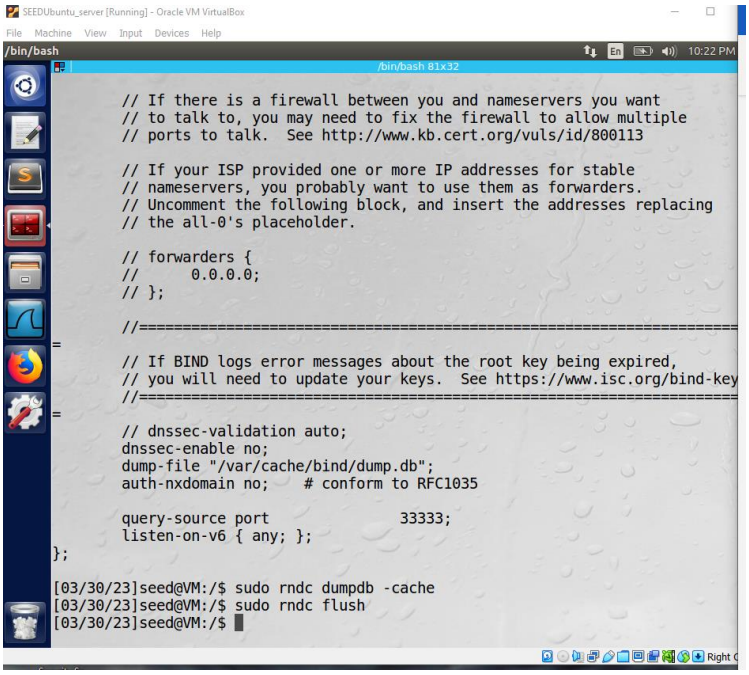
“dump-file “/var/cache/bind/dump.db”



In server do following command :

Sudo rndc dumpdb –cache //dump cache to file

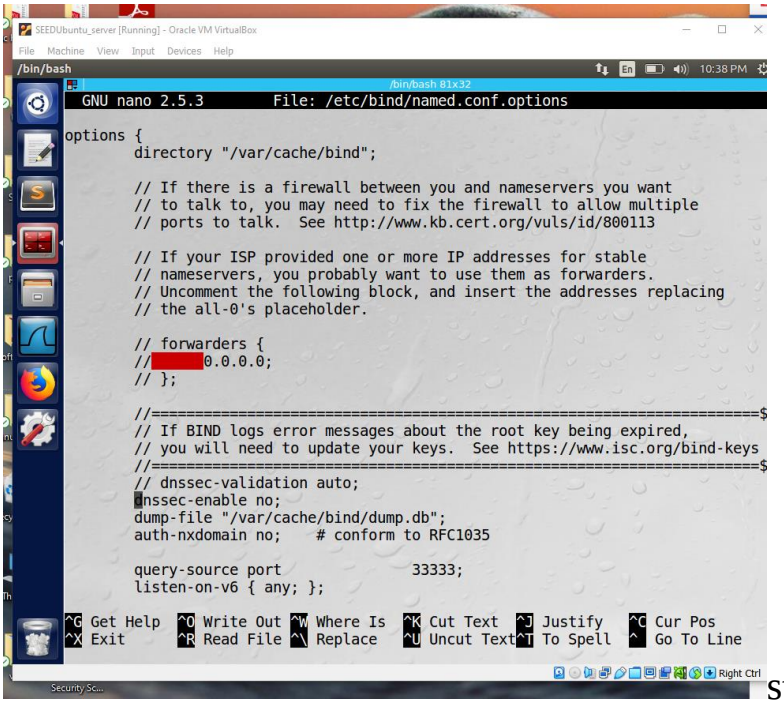
Sudo rndc flush //flush DNS cache



Step 2: turn off DNSSEC

In server do following command:

Sudo nano /etc/bind/named.conf.options

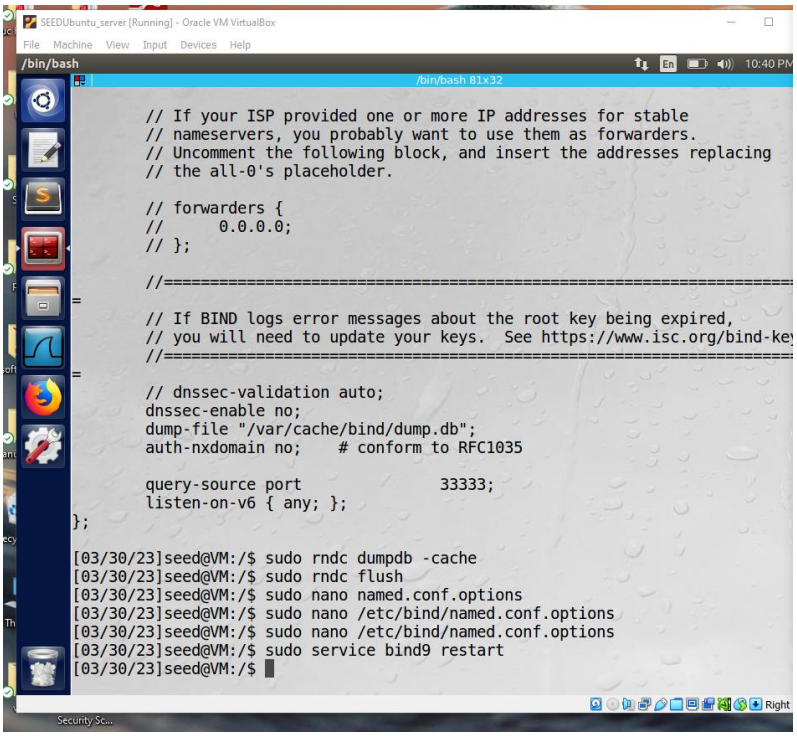


ste

Step 3: Start DNS server

Then in server do following command:

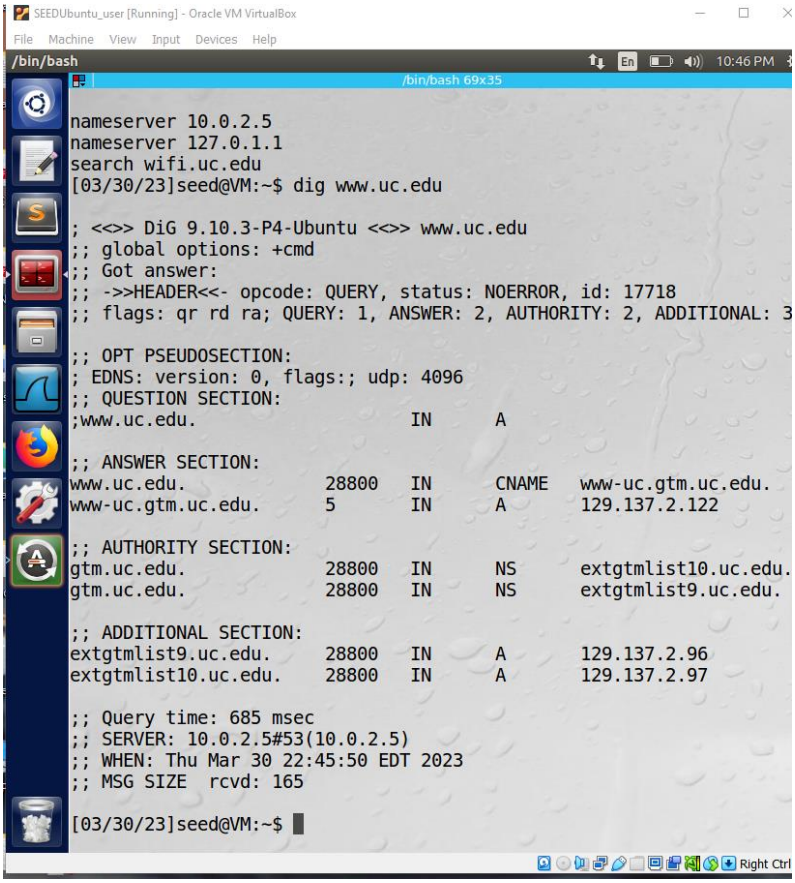
Sudo service bind9 restart



Step 4: Use the DNS server:

In user run following command:

Dig www.uc.edu

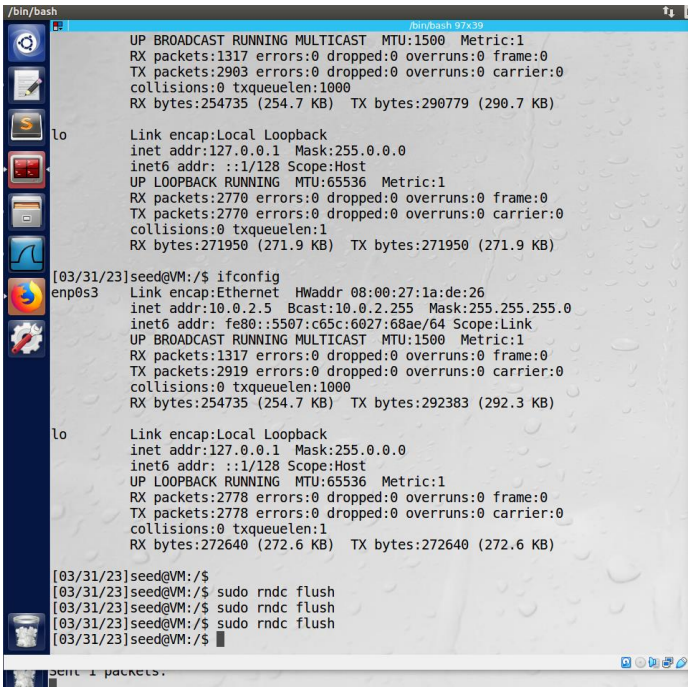


Here we can say that local DNS server is 10.0.2.5.

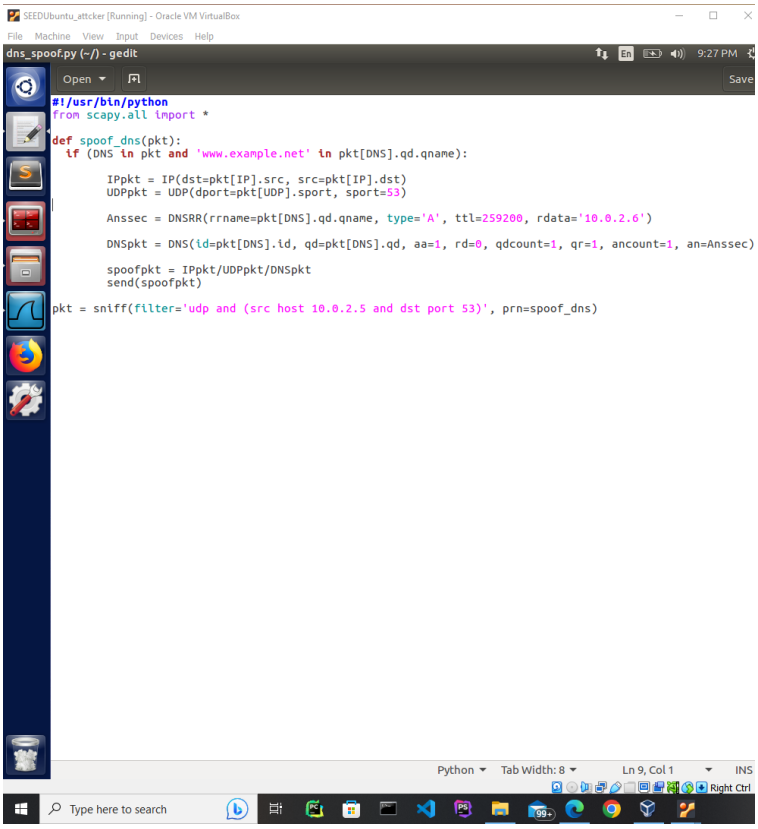
Task 6: DNS cache Poisoning Attack

In serve do following command:

Sudo rndc flush

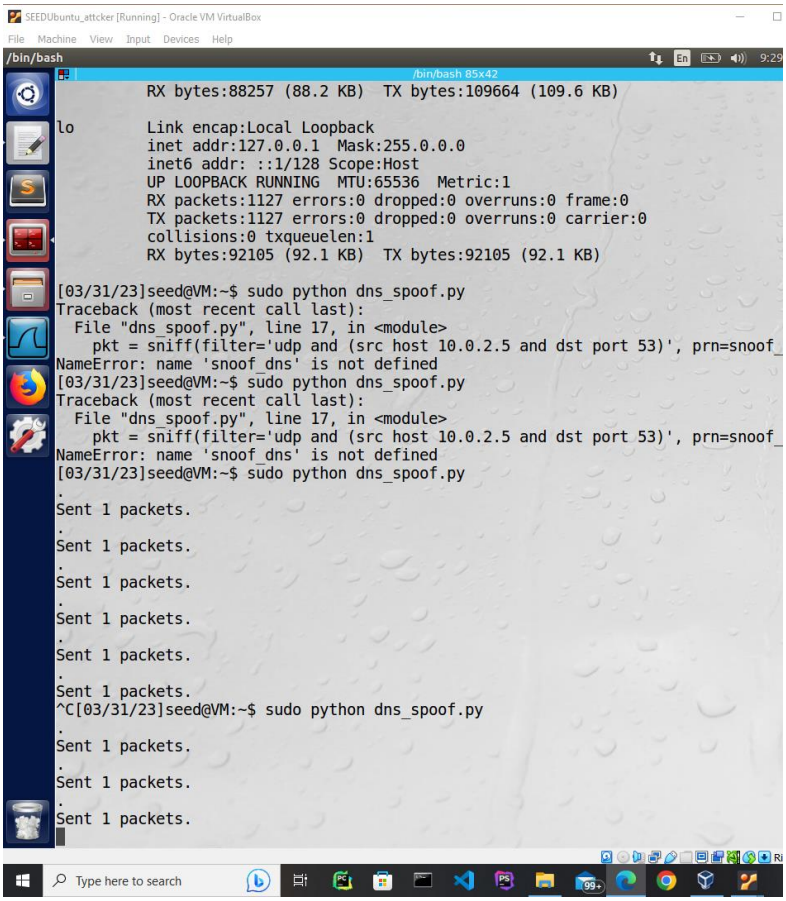


In attacker create python file dns_spoof.py with following content:



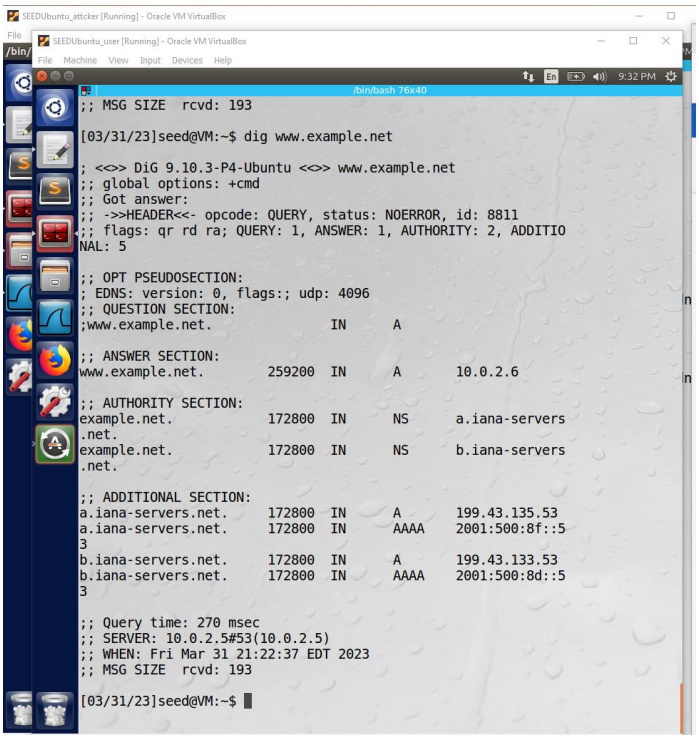
Run the file using following command

Sudo python dns_spoof.py



In user machine try following command to Test the local DNS poising attack:

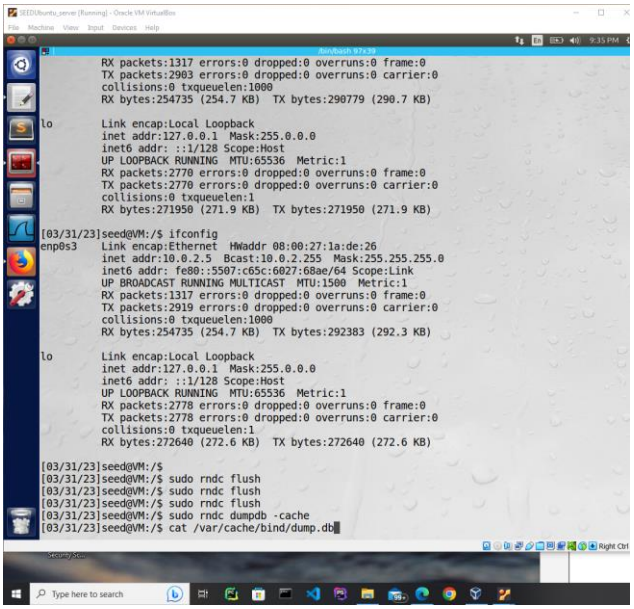
Dig www.example.net



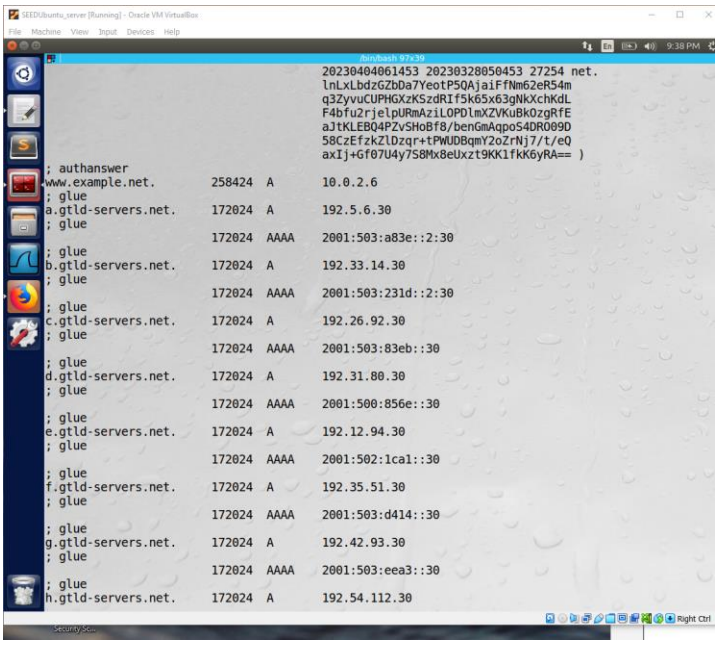
Here we can see that DNS info at user is manipulated by attacker. In answer section we can see 10.0.2.6.

To test the Local DNS poisoning attack to following command in server:

sudo rndc dumpdb -cache
cat /var/cache/bind/dump.db



Output of following command:



Here we can see that :

Authanswer gives www.example.net . And with IP of 10.0.2.6

By this we can say that cache is been poisoned.

And In attacker machine we can see packet sent.

```
          RX bytes:88257 (88.2 KB)  TX bytes:109664 (109.6 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:1127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:92105 (92.1 KB)  TX bytes:92105 (92.1 KB)

[03/31/23]seed@VM:~$ sudo python dns_spoof.py
Traceback (most recent call last):
  File "dns_spoof.py", line 17, in <module>
    pkt = sniff(filter='udp and (src host 10.0.2.5 and dst port 53)', prn=snoof_dns)
NameError: name 'snoof_dns' is not defined
[03/31/23]seed@VM:~$ sudo python dns_spoof.py
Traceback (most recent call last):
  File "dns_spoof.py", line 17, in <module>
    pkt = sniff(filter='udp and (src host 10.0.2.5 and dst port 53)', prn=snoof_dns)
NameError: name 'snoof_dns' is not defined
[03/31/23]seed@VM:~$ sudo python dns_spoof.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
^C[03/31/23]seed@VM:~$ sudo python dns_spoof.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```