Tanmay Fadnavis

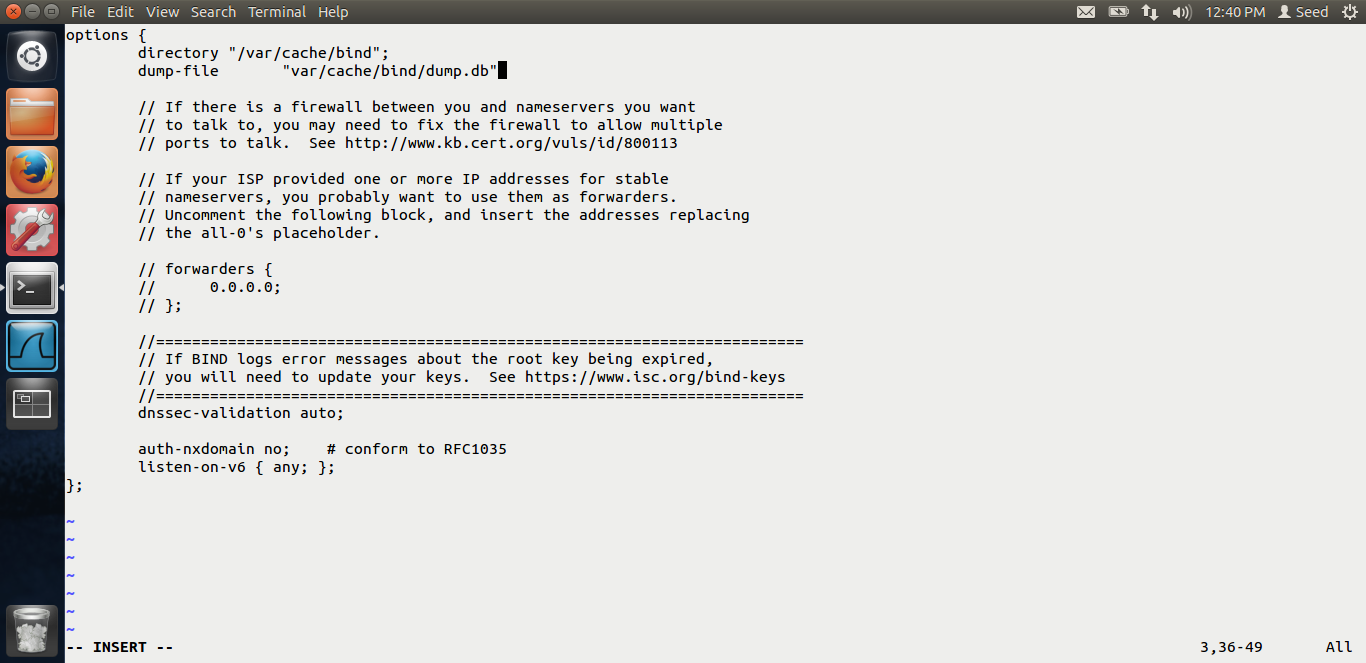
SUID: 971141760

INTERNET Security

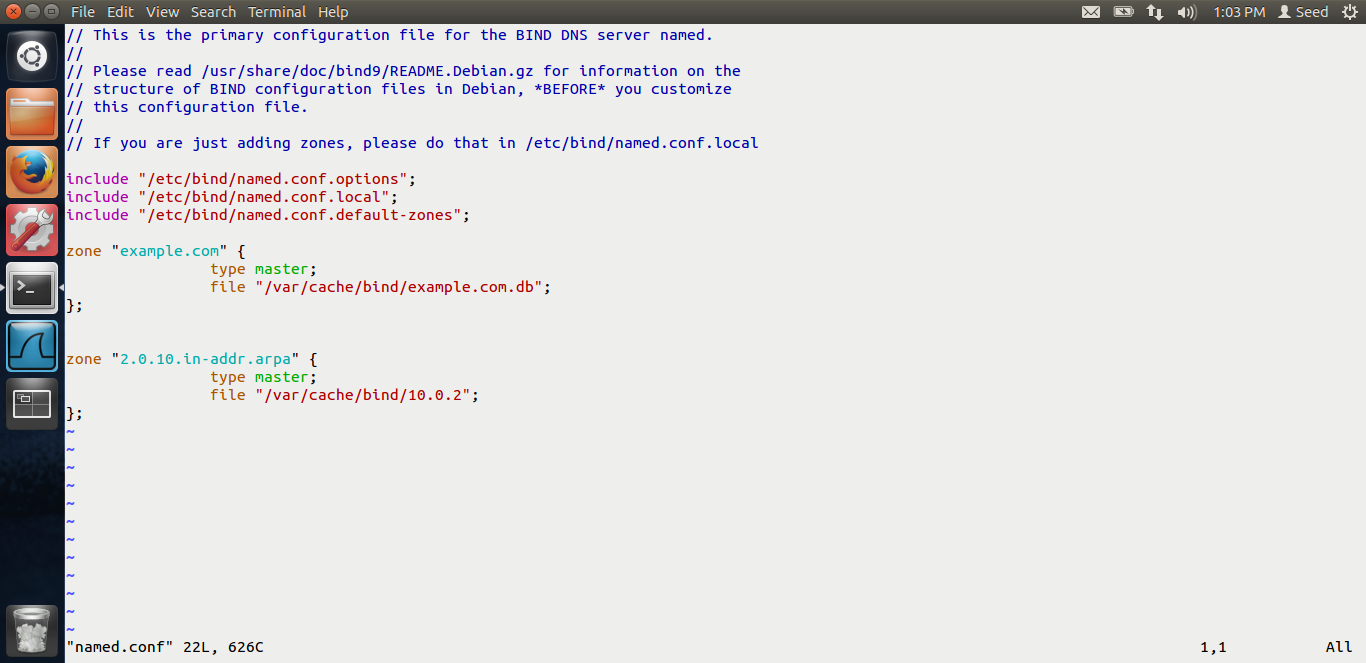
Lab - 5

# ENVIRONMENT SETUP

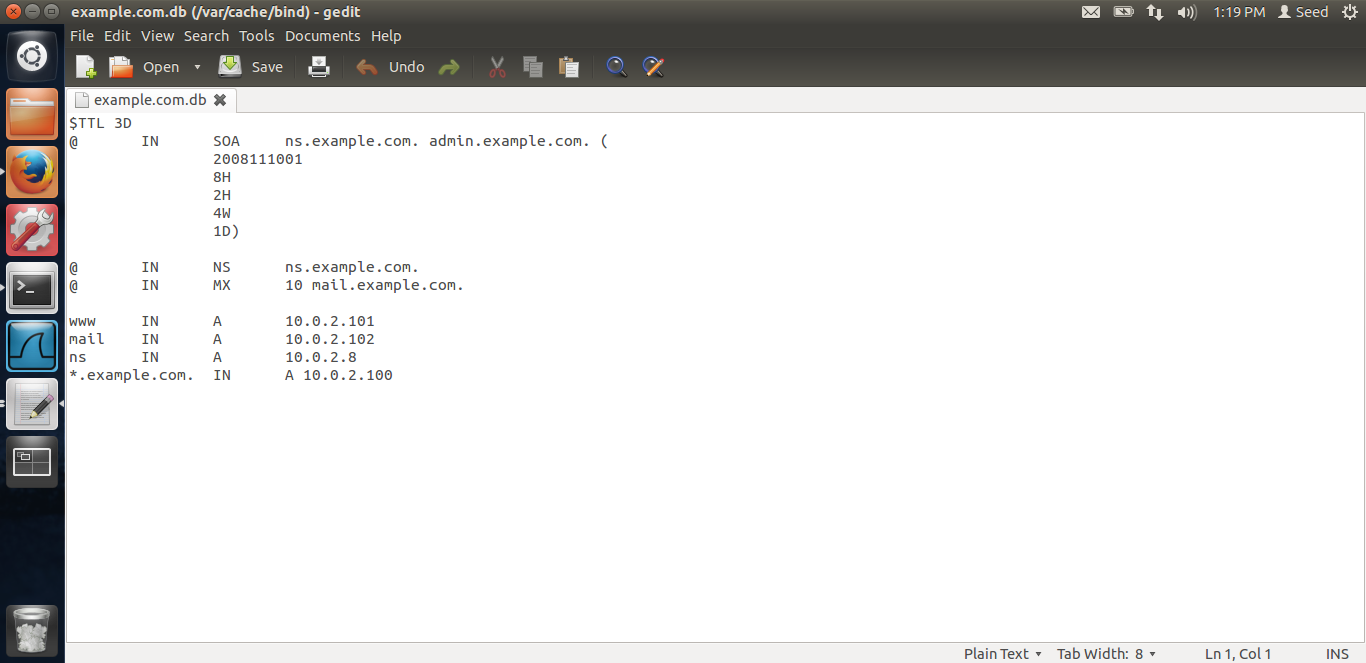
The screen shots for environment set-up are below.



I add the dump file location in the named.conf.options file.

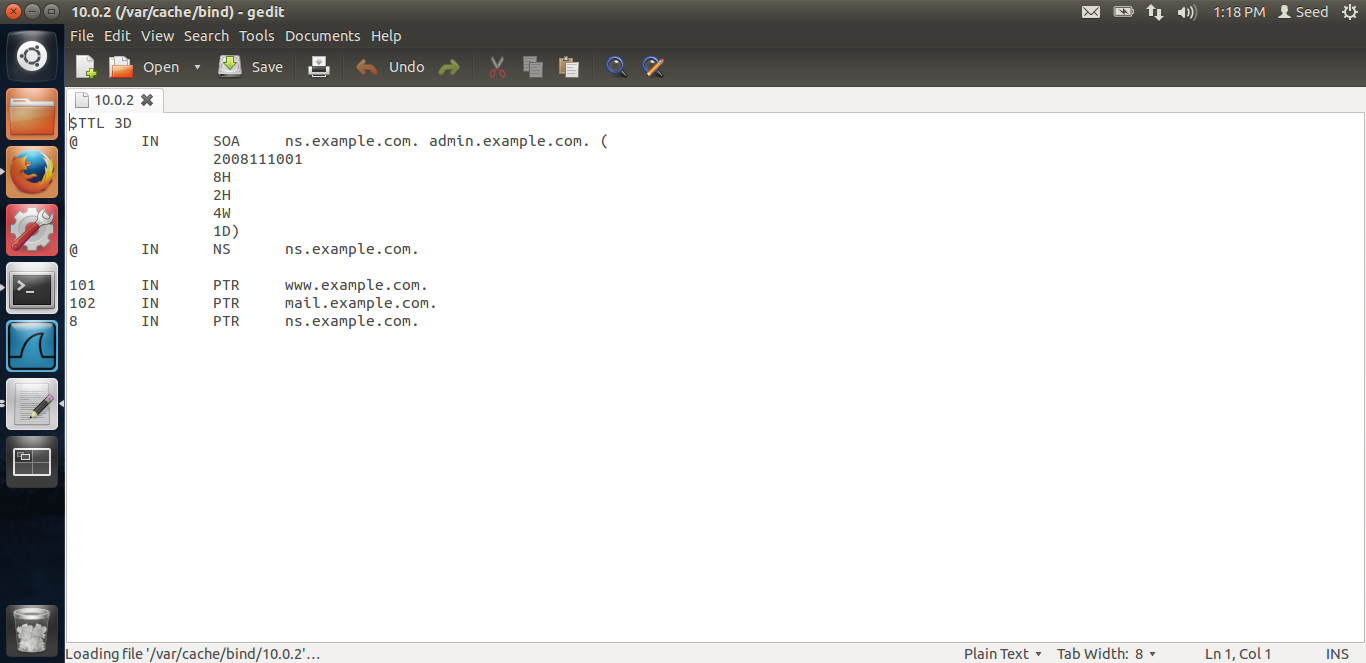


I add the zone values in the named.conf files. This means that our dns server manages the example.com zone.

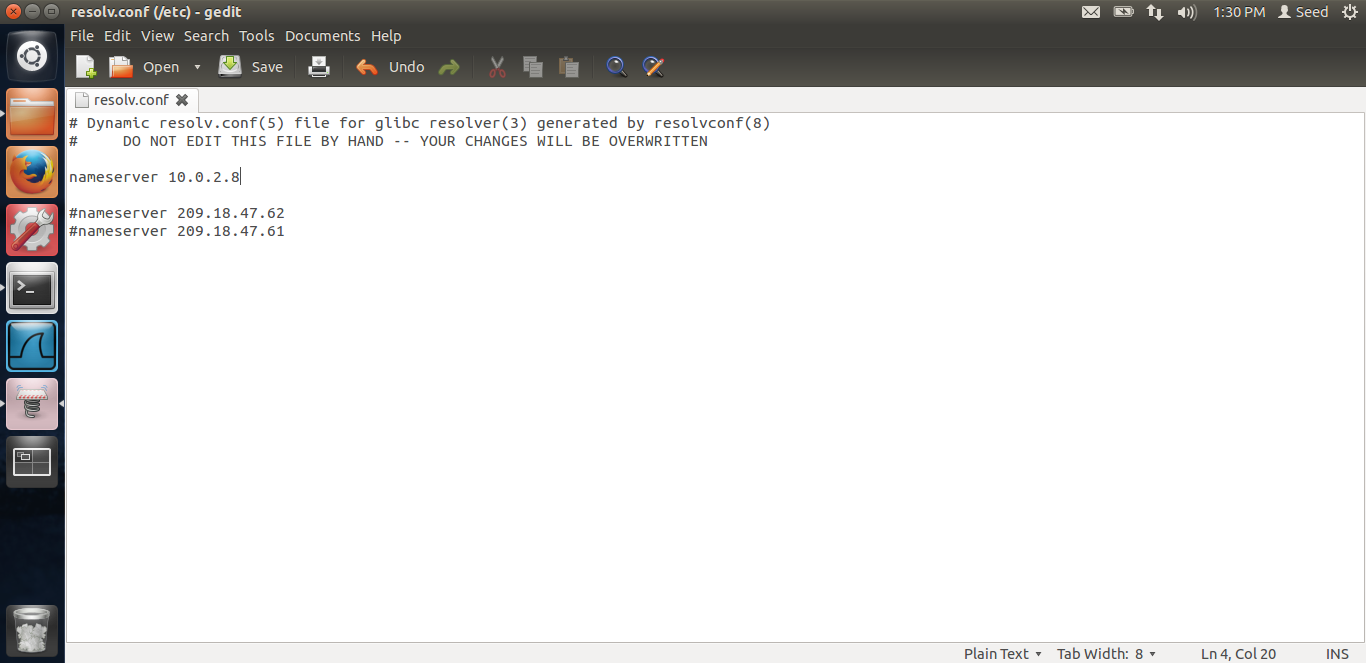


This is the example.com.db file provided by Dr Du.

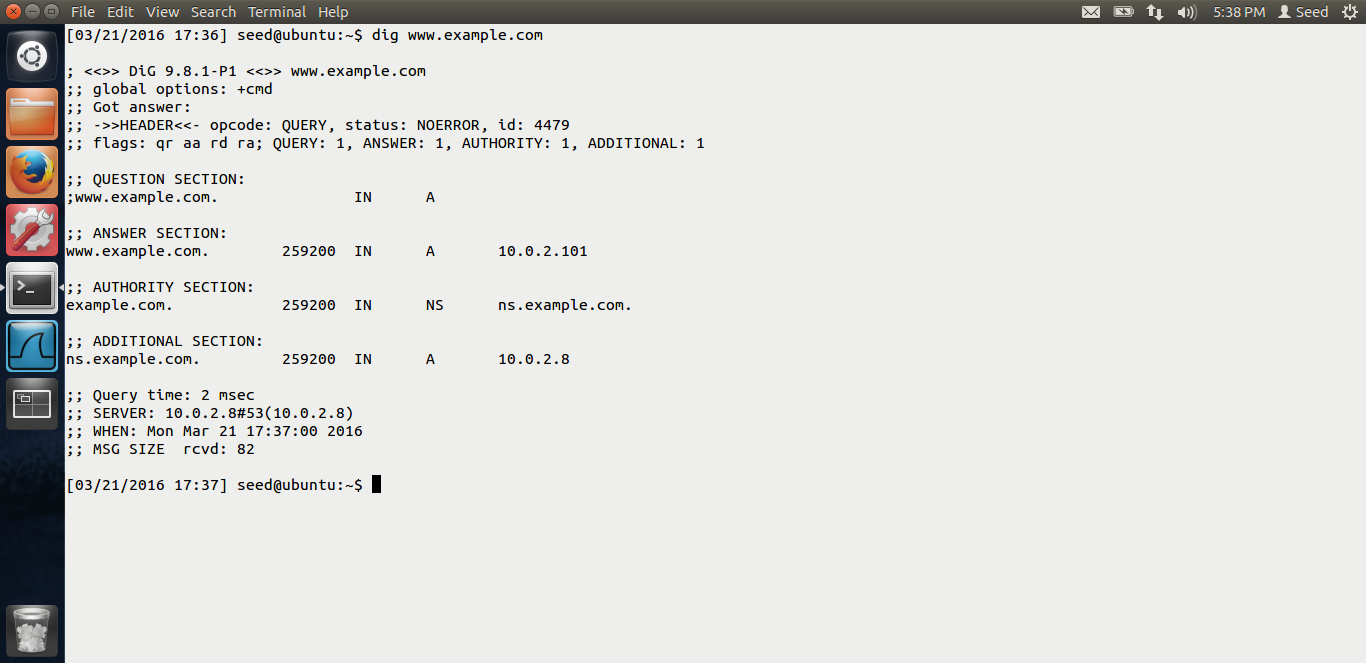
We are setting up the zone files. Actual DNS resolution is put in the zone file.



Above is the file for DNS reverse look up. The ip address are that of the NAT Network which we are using in the lab. After the set up is done, we are restarting the DNS server.



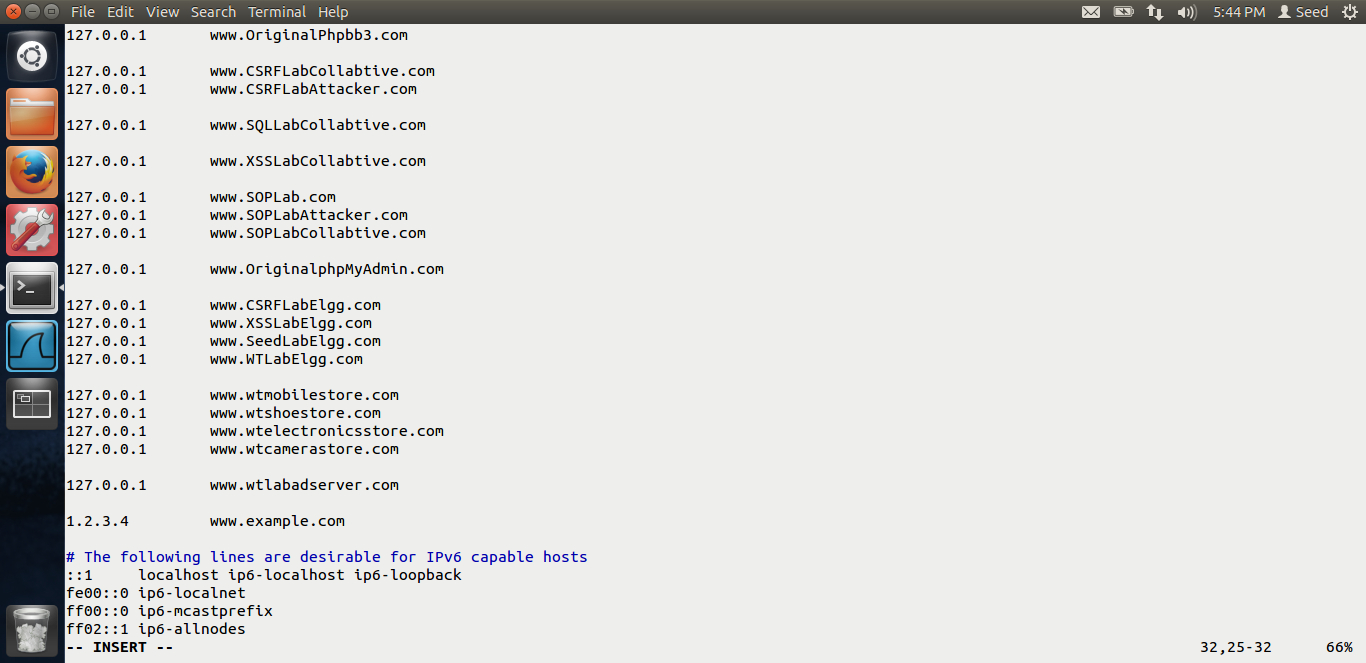
Above is the screen shot for the user machine. We are configuring the nameserver ip to our virtual machine’s ip where we have set-up the DNS server.



After all the set-up has been done, if we dig [www.example.com](http://www.example.com), we see that the in the answer section, the ip is that provided by our local DNS. Along with the authority section. Thus, our set-up is successful. Let us try the attacks.

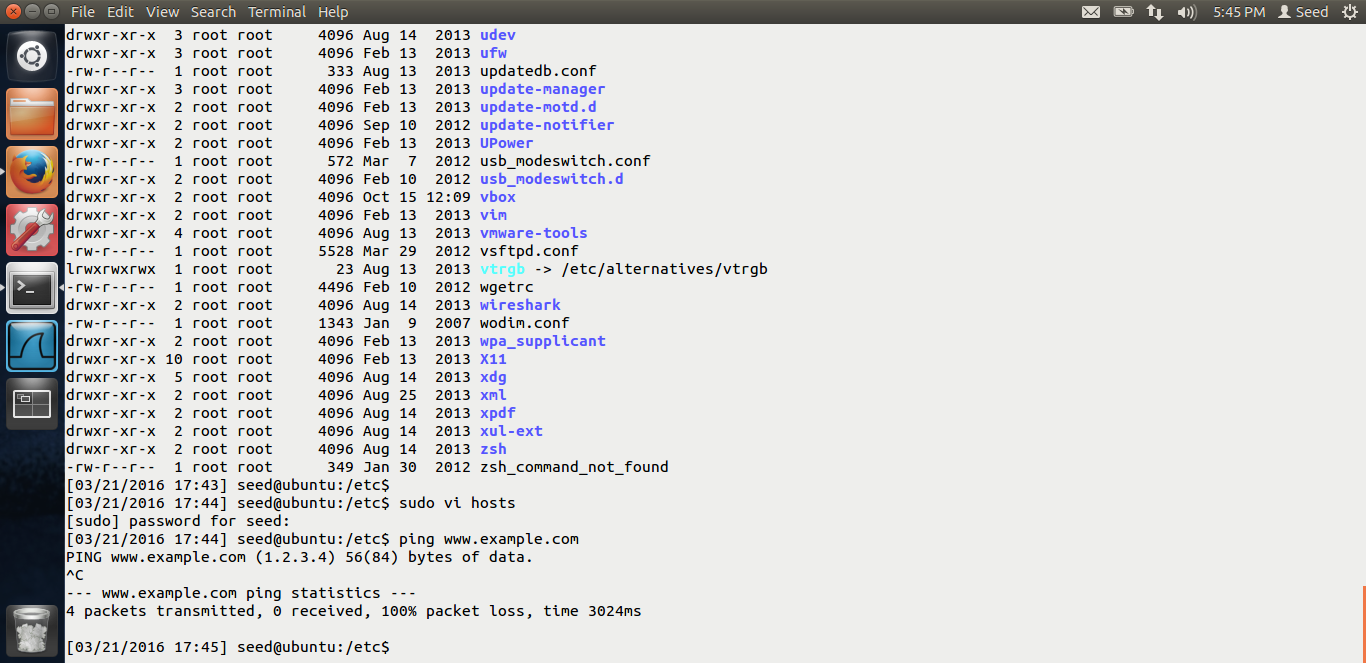
# TASK 1: MODIFYING HOSTS FILE

In this, the attacker have already compromised the user machine. He modifies the host file and changes the ip of example.com



In the above screen shot, we see that, in the /etc/hosts file, the example.com ip is 1.2.3.4 This is the malicious ip. Now this ip will he hit when the user tries to go to [www.example.com](http://www.example.com)

We can see the output via ping.

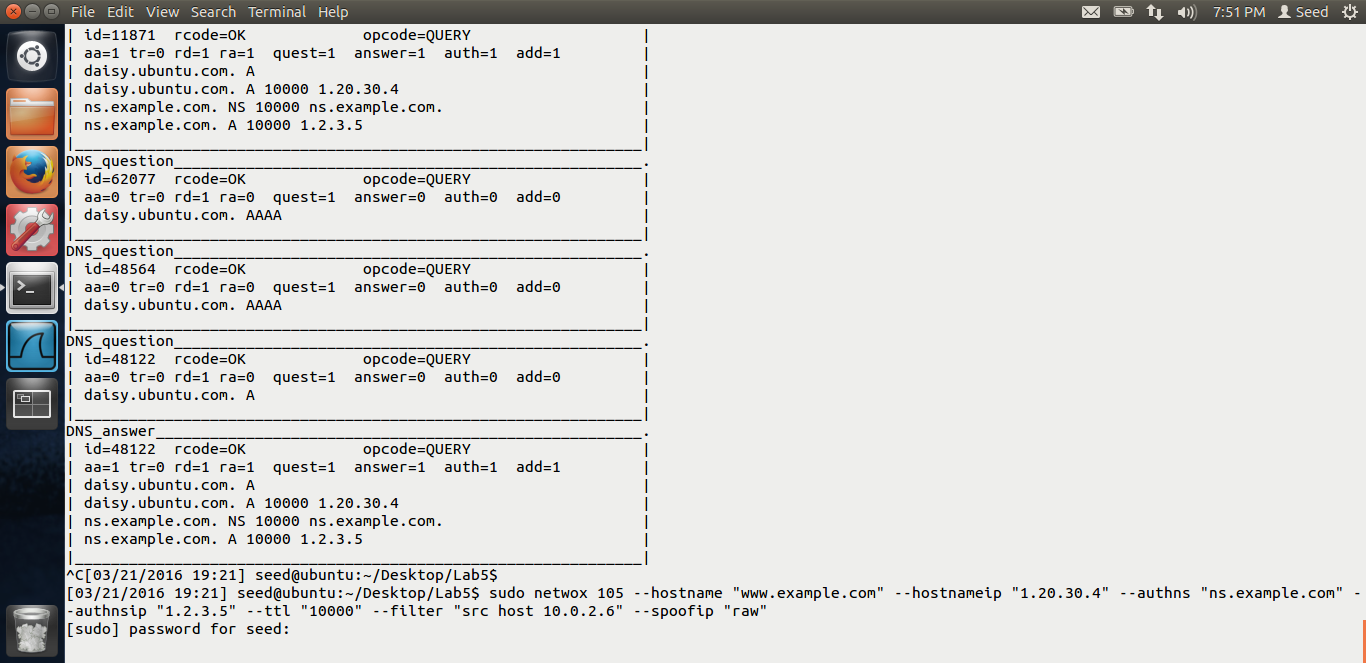


If we ping [www.example.com](http://www.example.com), in the screen shot, we can see that the ip is 1.2.3.4 Thus our attack is successful.

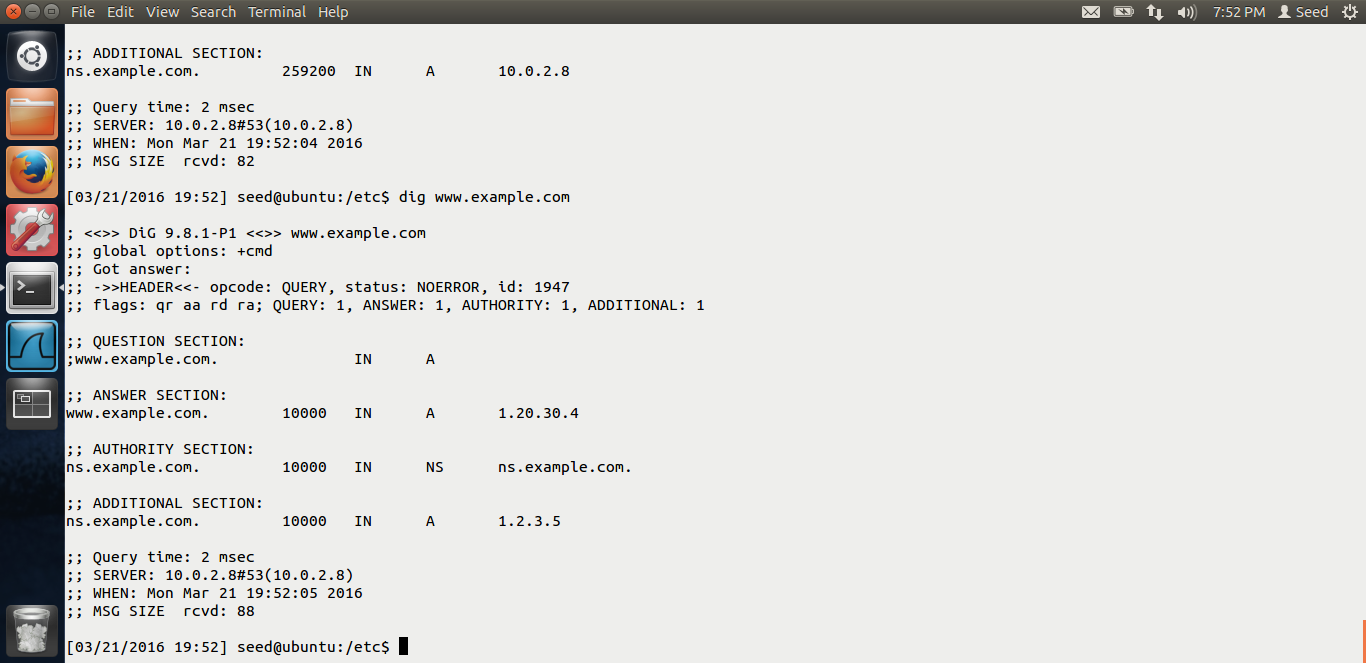
# TASK 2: DIRECTLY SPOOF RESPONSE TO USER.

The screen shots for task-2 are below.

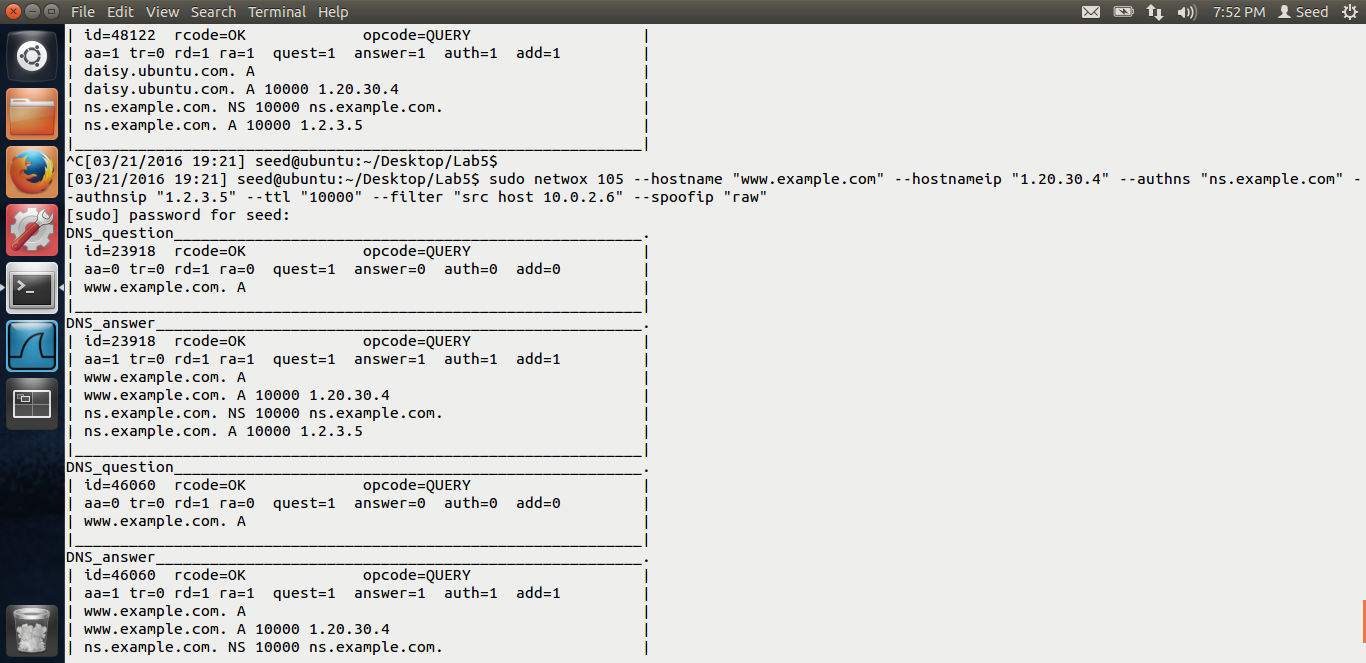
Here in this task, we are using the netwox 105 tool to sniff and spoof response to the user. So whenever user does dig [www.example.com](http://www.example.com), the attacker will launch the attack and try to spoof the response, i.e. spoofed ip of [www.example.com](http://www.example.com) to the user.



Above in the screen shot, we can see that command to run the netwox 105 tool. We are spoofing [www.example.com](http://www.example.com) with ip 1.20.30.4, along with the authns name server, etc.



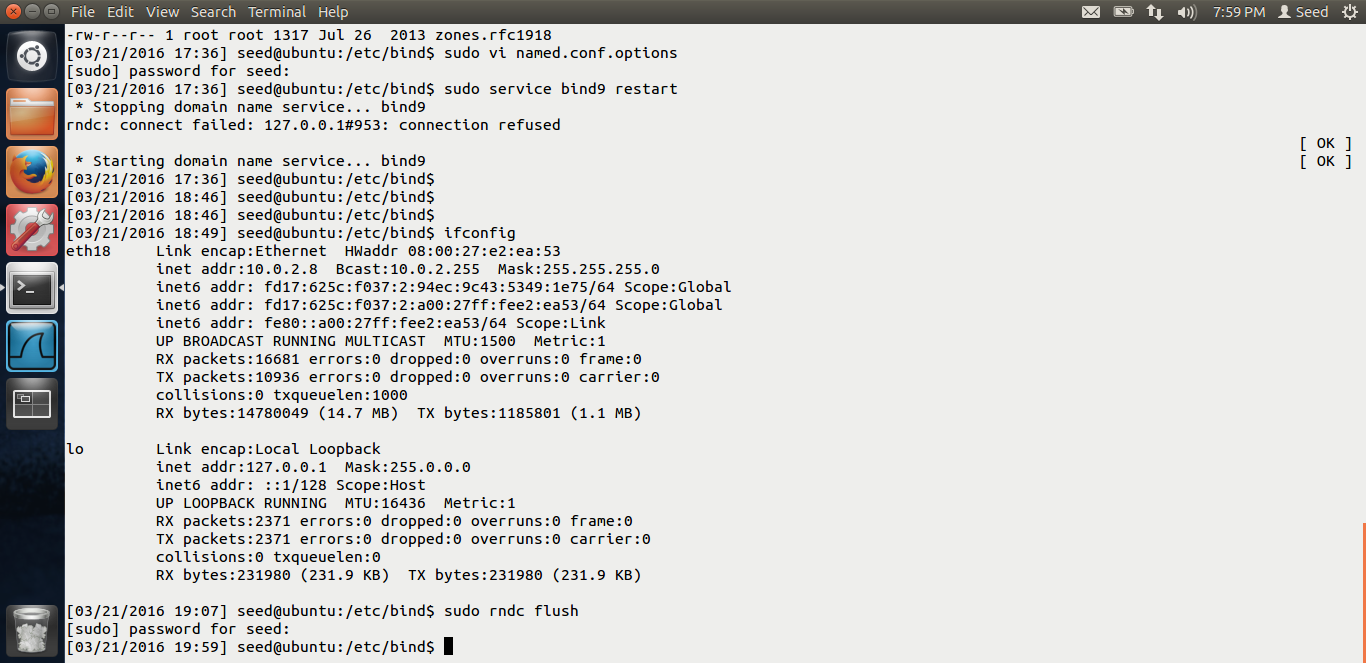
In the above screen shot, we can see that, when the user digs [www.example.com](http://www.example.com), in the answer section, he is getting the spoofed ip and the spoofed ip of the nameserver. Thus the attack is successful. However, not everytime the attacker wins Because sometimes, the DNS server’s reply goes earlier than the attacker. In our case, the DNS server has the answer to the domain [www.example.com](http://www.example.com) already. Thus, not always the attack is successful.



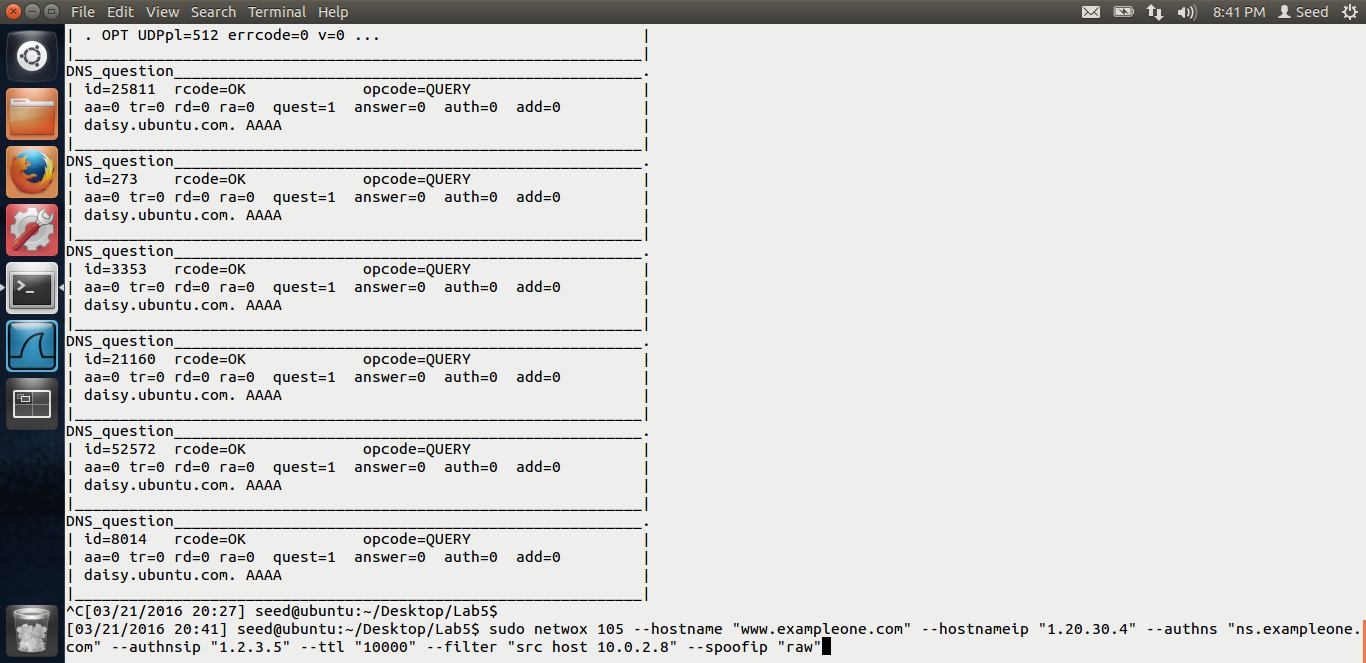
This is the output on the attacker’s machine.

# TASK 3: DNS SERVER CACHE POISONING

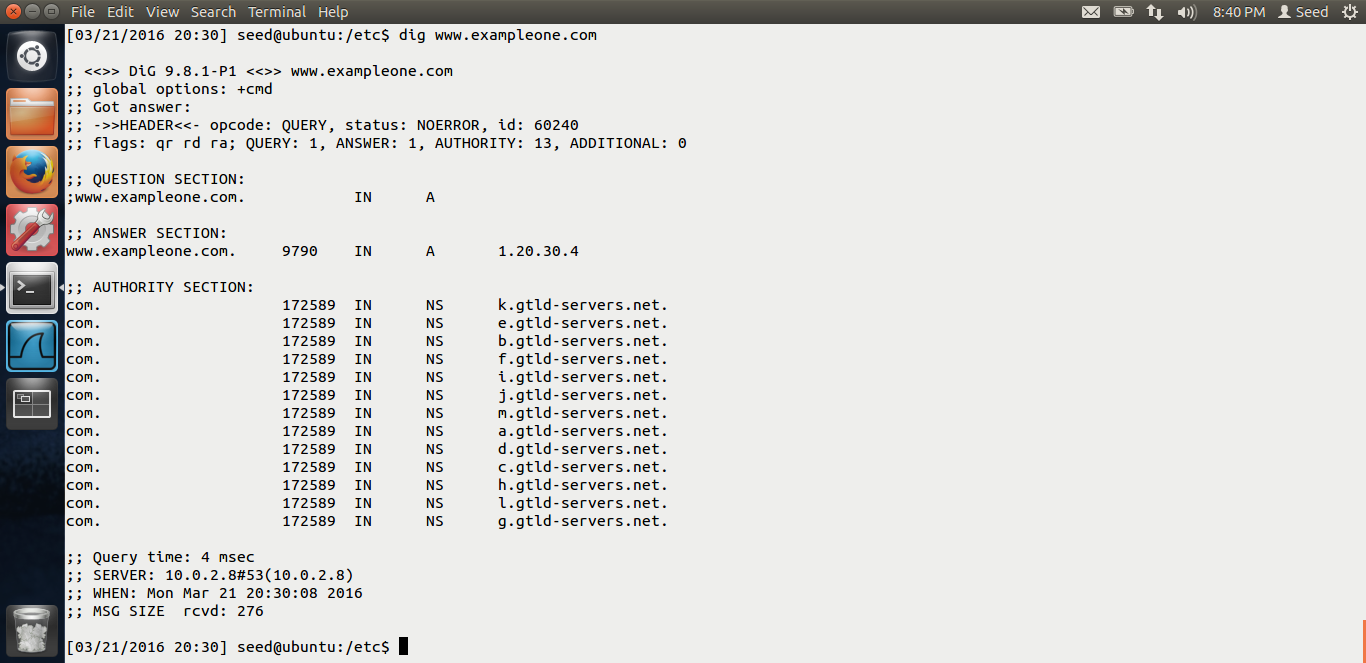
The screen shots for task-3 are below.



First, we clear the cache of the DNS server.



Then, we run the same netwox tool 105 but in the filter, instead of the victim’s ip, we give the ip address of the DNS server.



Thus, after the cache is poisoned, we can see that if the user digs [www.exampleone.com](http://www.exampleone.com), this domain is not in the DNS server’s machine, it gets the spoofed ip in the answer section, 1.20.30.4

But in the authoritative section, it gets the global top level domain name servers. Also, if we stop the attack at this point, the data will remain in the DNS cache as long as the field value in TTL. Thus, this attack will be there for a long time.

End of Lab-5.