CSE 406

Computer Security

Project Final Report

**DoS attack to the DNS server (using spoofed IP address)**

Name : Abdur Rahman Fahad

Std ID : 1605069

Group : 02

Lab Group : B1

Department of Computer Science and Engineering

Bangladesh University of Engineering and Technology

**Steps of the attack**

DoS attack (Denial-of-Service attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Here we will attack the DNS (Domain Name Server) using spoofed IP address. We will perform the attack by sending lots of meaningless DNS query to the DNS server.

Here are the steps of the attack:

**Setting up the Environment**

For the simulation of this attack, we need 3 machines on the same network.

1. A Local DNS Server (which is to be attacked).  
2. The attacker machine.  
3. The victim User on the network to test the attack result.

So, at first I created 3 virtual machines (each Ubuntu 16.04 LTS) on Oracle  
VM Virtual Box using network type as Bridged Adapter so that, all the virtual  
machines were at the same network with host OS.

**Setting up Local DNS Server**

I wrote the following commands on terminal:

$ sudo apt-get install bind9

In this way I configured my DNS Server with Bind9 on a virtual machine.

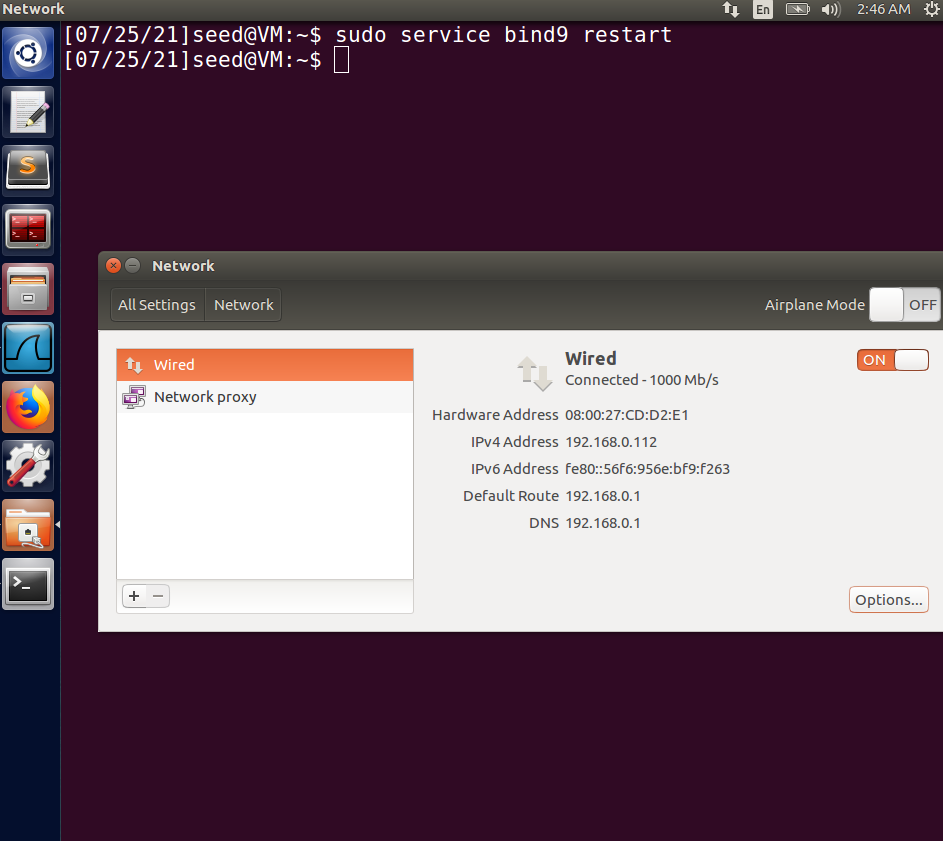
Then I wrote the commands in the terminal:

1. To flush the DNS cache,

$ sudo rndc flush

1. To start newly configured DNS Server:

$ sudo service bind9 restart



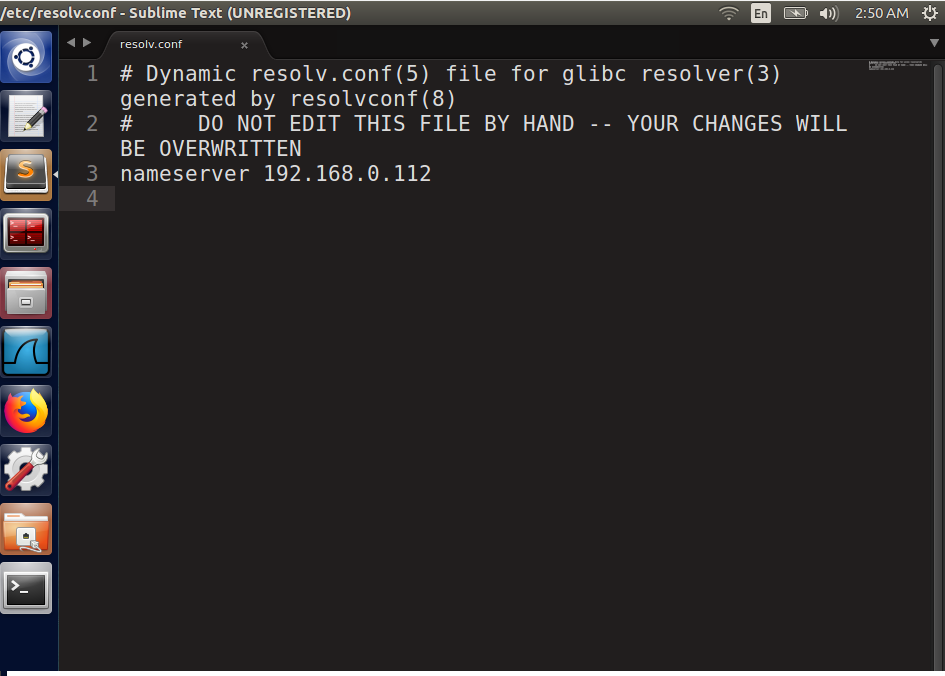
**Setting up victim’s DNS Server**

To change victim’s DNS server address, I opened /etc/resolv.conf file and changed the line

nameserver 127.0.1.1

to

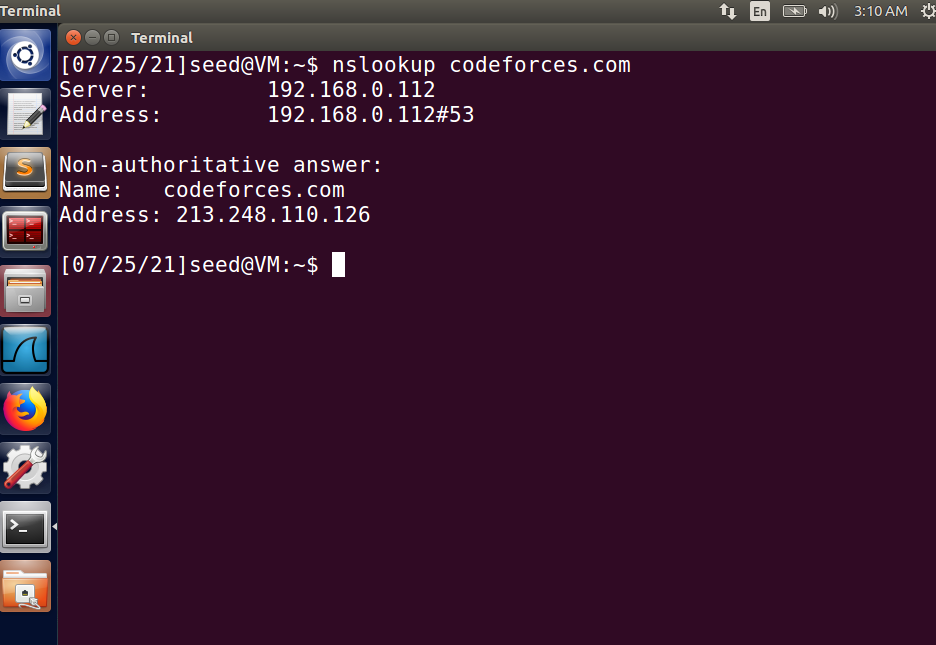
nameserver 192.168.0.112 (DNS Server’s IP)



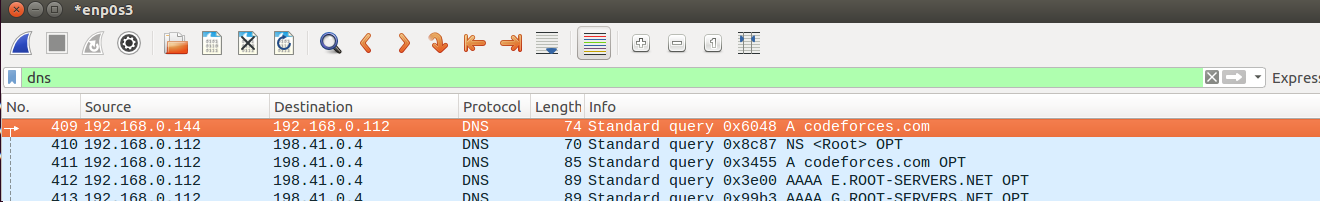
**Testing my new DNS Server**

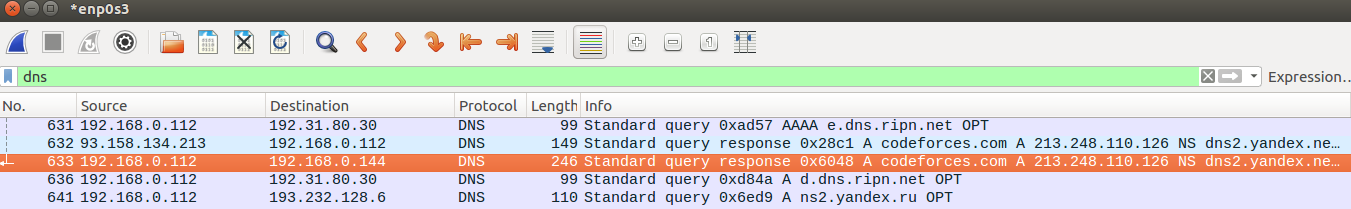
Now I’ll be checking if the DNS Server is working perfectly before the attack.

To do that I’ll run DNS queries from the user’s machine which will be resolved by the DNS server.



**Query Answer from DNS Server (192.168.0.112)**

****

****

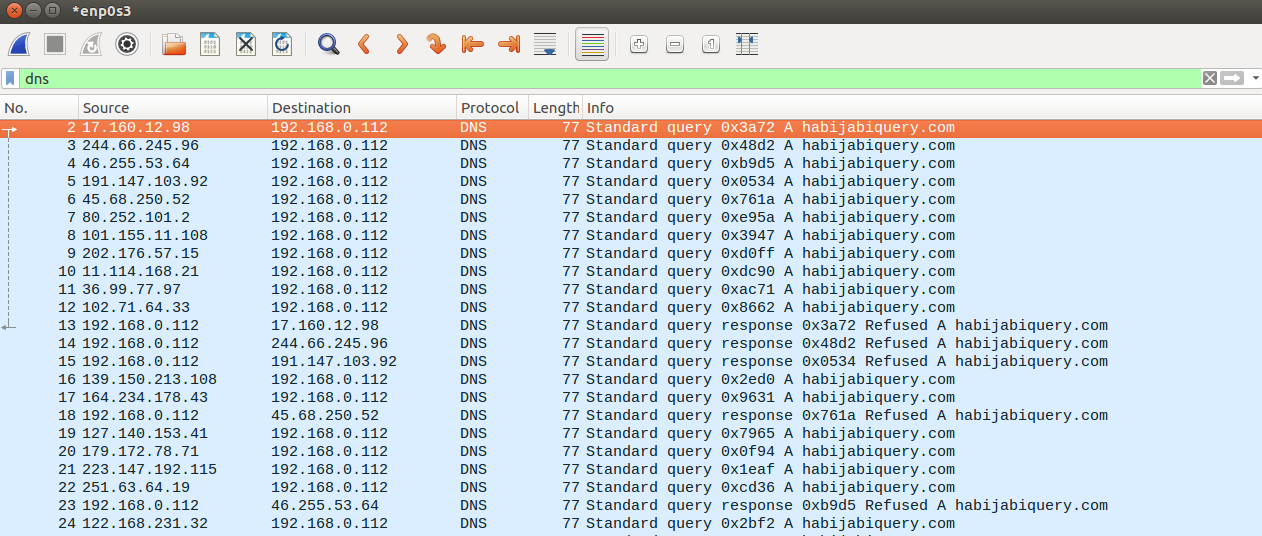
**Query observed from Server’s Wireshark**

**Initiating Attack and Observed Output**

With my attack code I sent thousands of random bogus query (habijabiquery.com) to the DNS Server (192.168.0.112)

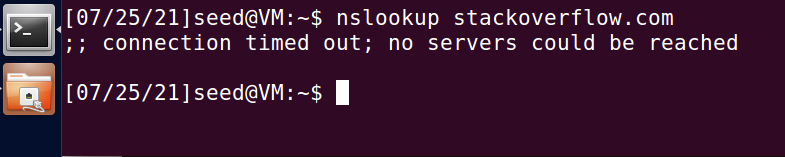


Then I observed those queries flooding the DNS Server

****

It can be seen that the source addresses of the queries are random and not actual IP address of the attacker, thus IP spoofing was done.

Now we can see that the victim’s query couldn’t be resolved as the server ran out of resources, it was unreachable.



So the attack was successful.

**Comment on Attack Success**

We sent bogus queries to DNS Server with a spoofed IP address in the source IP address field of IP Header. It failed to find a valid entry in cache and so, the DNS server sent the query to authoritative DNS Servers and waited for the result, which also eventually failed.

By doing this with many infinite loop and many more requests than usual, eventually the cache of DNS server was filled with bad requests. This way, it was possible to flood the targeted DNS and the server will denied any further service from any legit user and our attack was successful.