# Experiment Number: 7th

|  |  |
| --- | --- |
| **Student Name**: Lagan Verma | **UID:** 20BCS3515 |
| **Branch:** CSE (Information Security) | **Section & Group**: 20BIS-1/A |
| **Semester:** 5th | **Date**: 10/11/ 2022 |
| **Course Name**: NDE LAB | **Course Code**: 20CSB-331 |

1. **Aim/Overview of the Practical:**

To understand and implement the concept of DNS Server and Client.

# Task to be Done:

To understand and implement the concept of DNS Server and Client.

# Procedure:

**What is a DNS server?**

A DNS server is computer server that contains a database of public IP addresses and their associated hostname, and in most cases serves to resolve, or translate those names to IP addresses as requested. DNS servers run

special software and communicate with each other using special protocols. To set up the DNS server we need two virtual machines, here, we will implement with the help of 2 Ubuntu virtual machines running on my laptop and I named the server virtual machine as Ubuntu and the client virtual machine as Ubuntu client. To understand how DNS server works we use Wireshark packet capture to see how the request is handled by the DNS

server.

# Step-1: Installing Wireshark on Server virtual machine

In this, you can use the given below command to Install Wireshark with this command. After installing Wireshark we will start setting up the DNS server.

*sudo apt-get install wireshark*

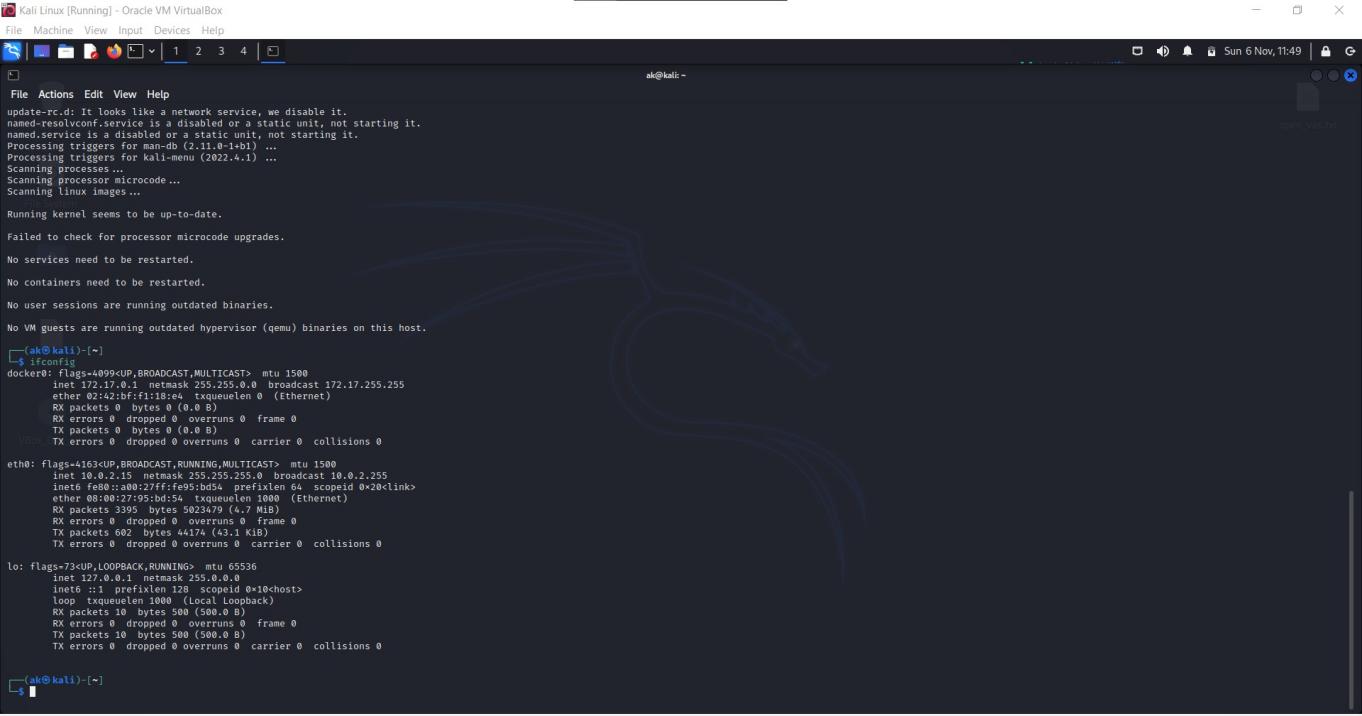


# Step-2: Configuring client virtual machine

We need to add the IP Address of the custom DNS server to the client machine.

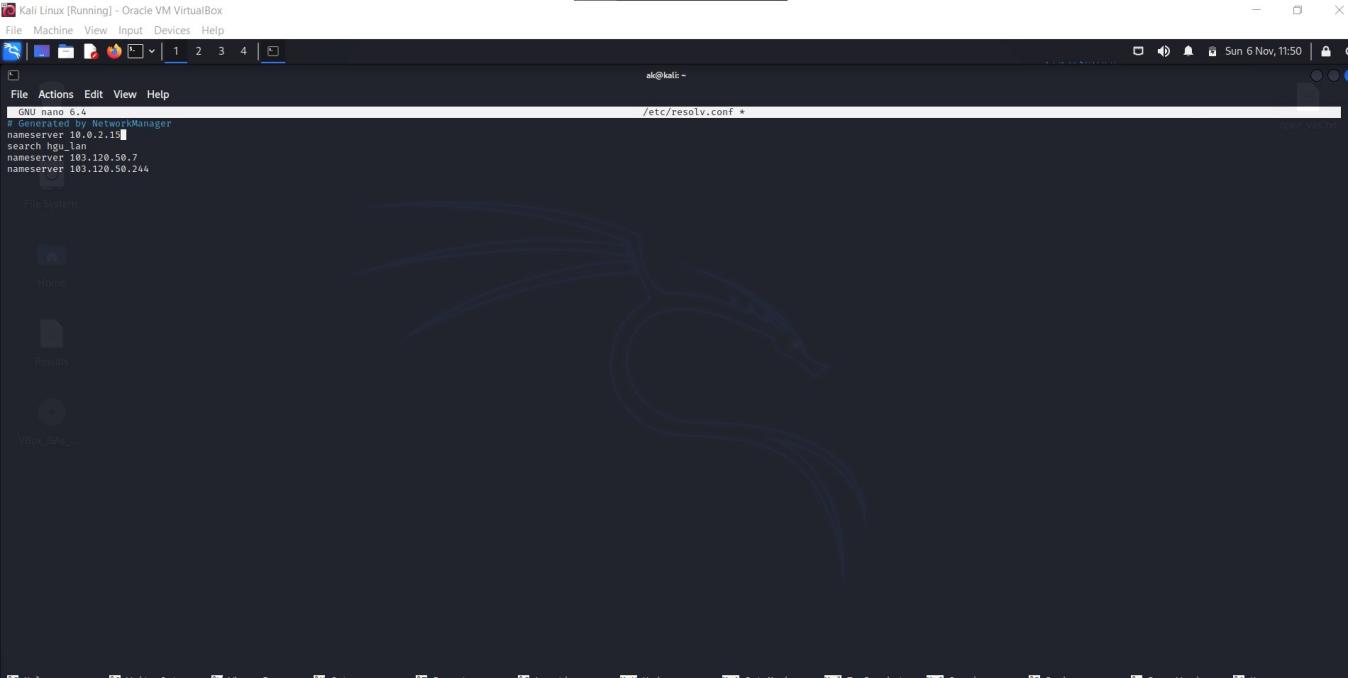
This is done by adding the IP address of the server to the file */etc/resolv.conf* which stores the order of DNS server resolution. This ensures that the custom DNS server will be used to resolve names. To find the IP Address of the server virtual machine first go to server virtual machine and this command in the terminal

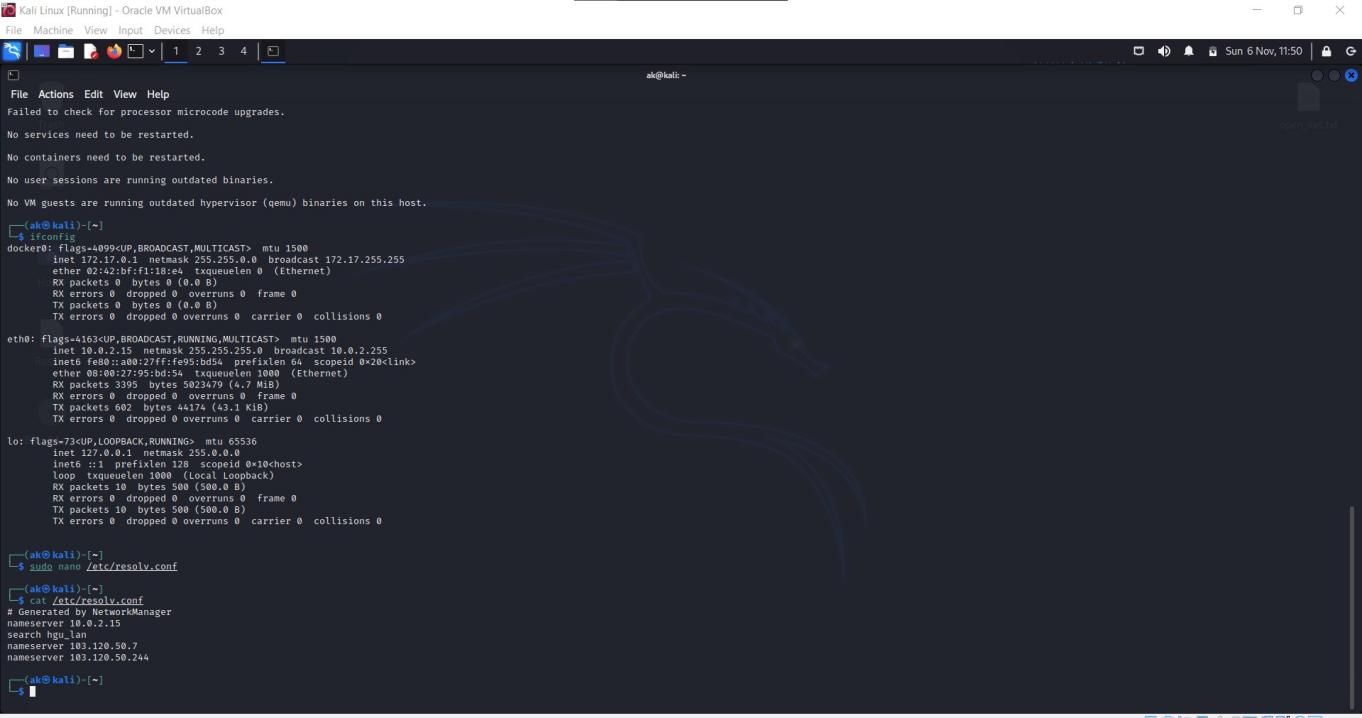
*ifconfig*



The value after the **inet** is IP Address in my case my IP address of the server machine is **10.0.2.15**. Now, go to the client virtual machine and in the terminal run this command and enter the user password to open that file.

*sudo nano /etc/resolv.conf*





You will find the screen similar to this. Now add this line in the first line of the file and save it. **nameserver 10.0.2.15**.

# Step-3: Configuring Server virtual machine

To set up the DNS server we need a software called bind9, bind9

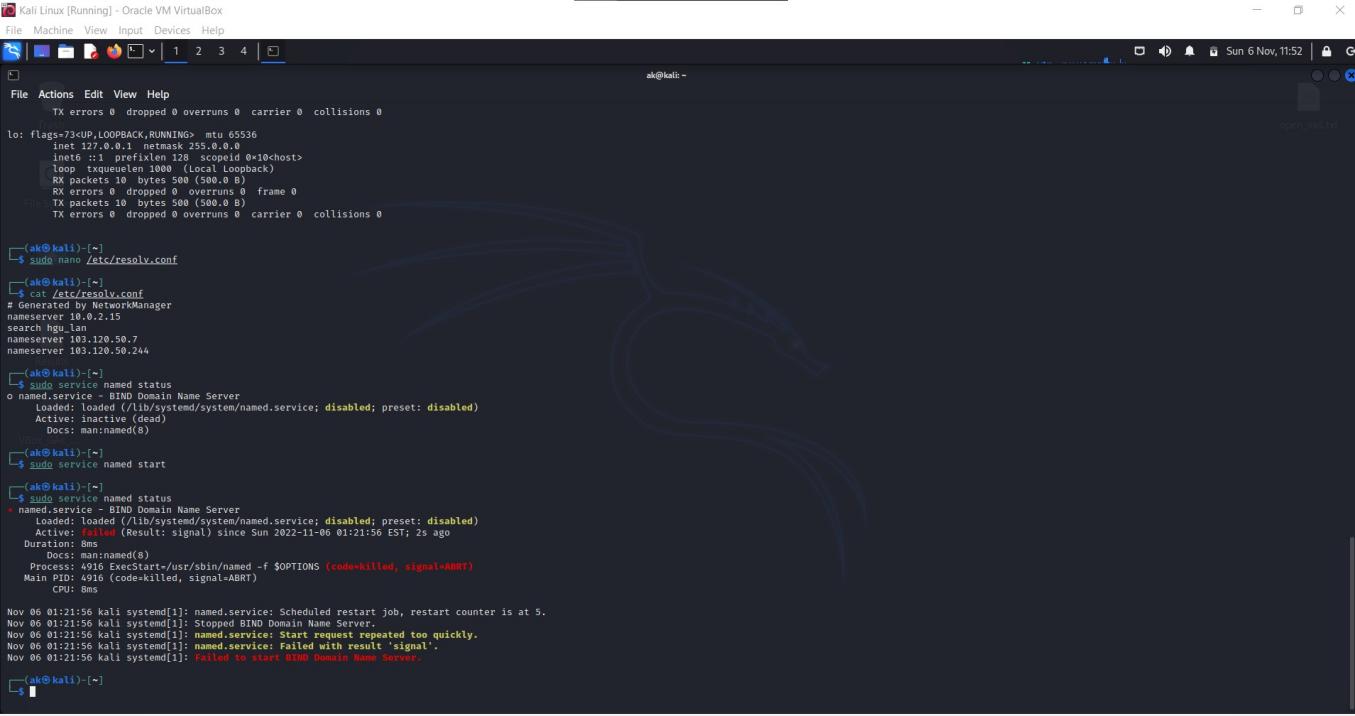
server is used as the DNS server on the server virtual machine. It can be installed using the below command.

*sudo apt-get install bind9*



After installing bind9. Let’s check the status of the bind9 server whether it’s running or not with this command.

*sudo service named status*



If you see active (running) then we are good to go, If you see

something else like failure or stopped or inactive type this command and restart your server virtual machine this will fix the issue.

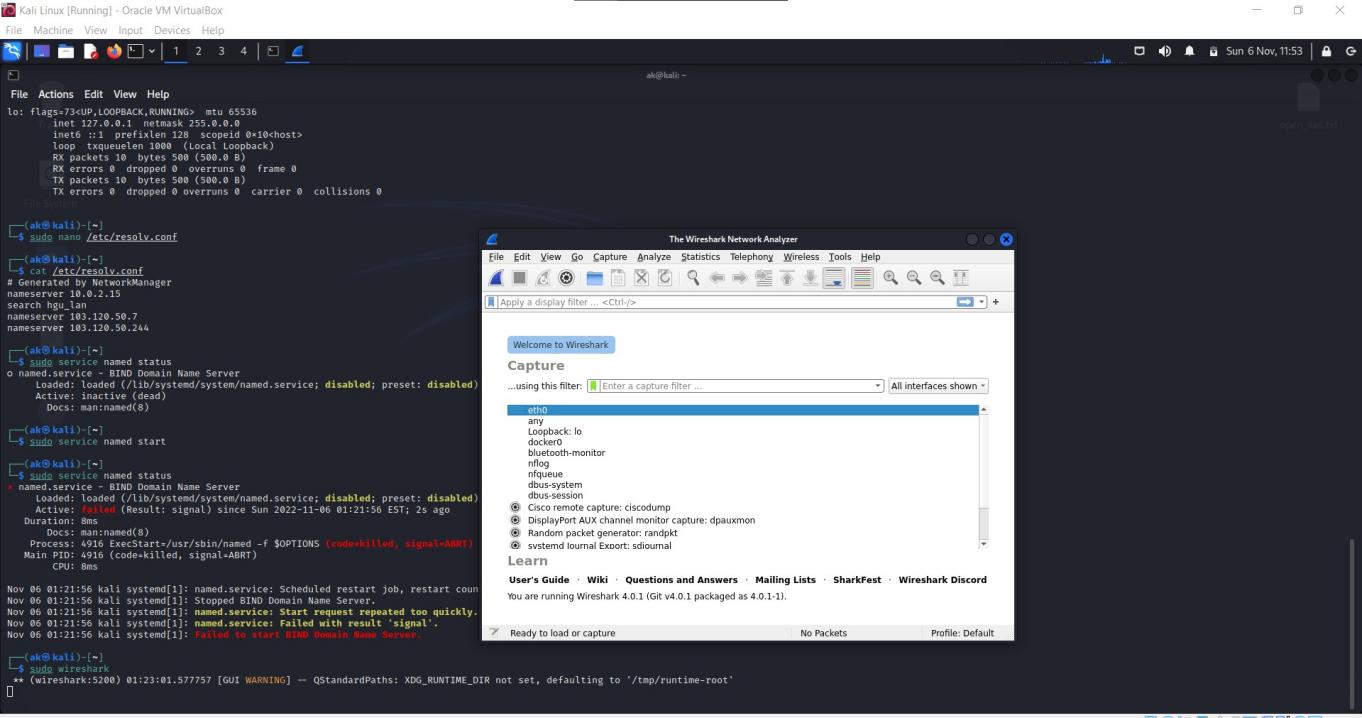
*sudo service named restart*

Now, we just finished setting up the local DNS server now we are going to see how it works.

# Step-4: Performing the packet capture with Wireshark

Go to the server virtual machine and open the terminal and type this command to open the Wireshark.

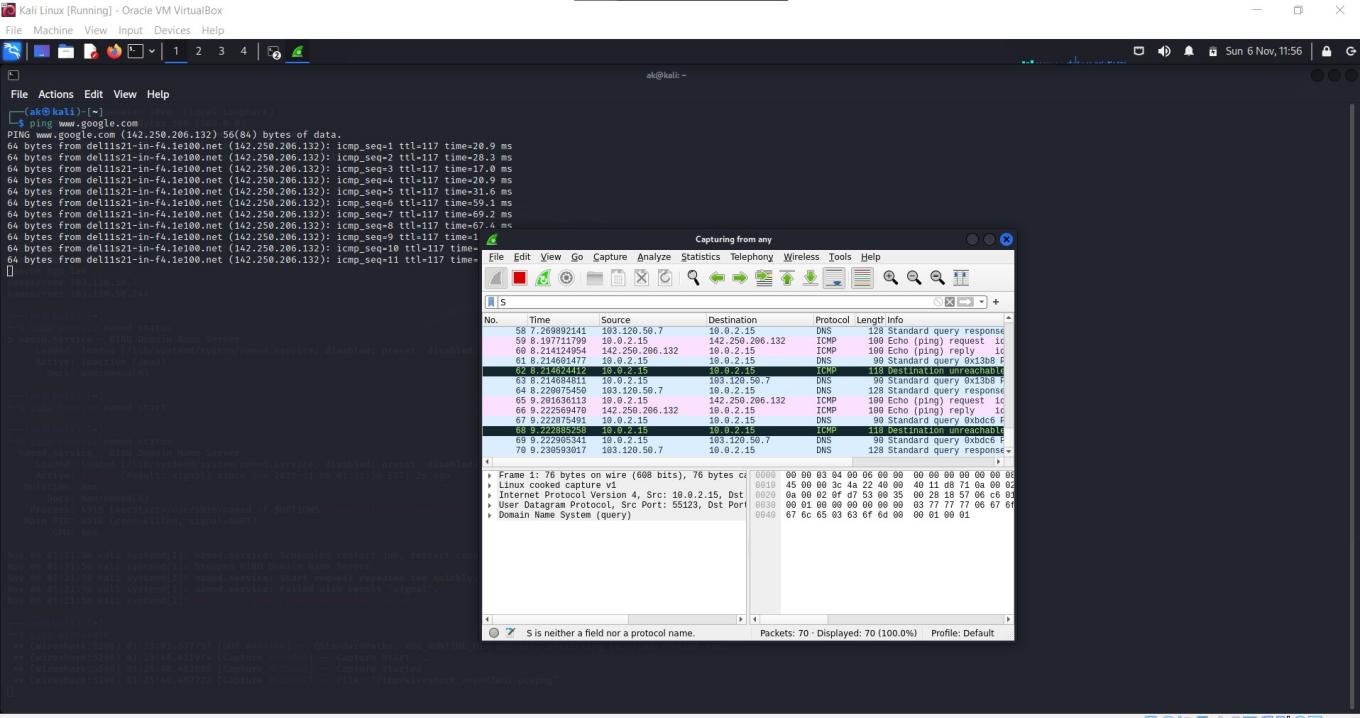
*sudo wireshark*



After Wireshark gets opened double click on any or click on any and

right click and click on start capture. Now quickly go to Client virtual machine and open terminal and ping any website for example, ping [www.google.com](http://www.google.com/)

*ping* [*www.google.com*](http://www.google.com/)

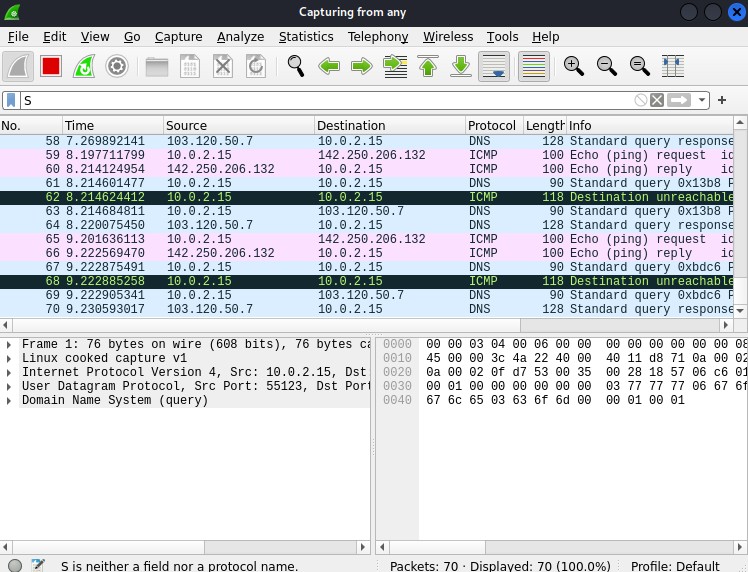


After 15 or 20 seconds press <CTRL> + C to stop the pinging the

[www.google.com](http://www.google.com/).

Now go to the server virtual machine and stop the capturing of the Wireshark by pressing the red button on the top left side of the panel this will stop the capturing of the Wireshark.

Now, type DNS on the display filter and press enter. Now, Observe the first frame of the packet capture in screenshot, source is IP address of the client virtual machine and the destination is the IP address of the server which implies that the client is sending request to the server virtual machine to get the results for the webpage [www.google.com](http://www.flipkart.com/)



# Learning Outcomes (What I have learnt):

1. Learned about packet capturing with wireshark.
2. Learned about bind9.
3. Learned about DNS.
4. Editing nameservers in kali.

**Evaluation Grid (Created as per the Assessment Model):**

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
| 1. | Worksheet completion |  | 8 |
| 2. | Conduct of Experiment |  | 12 |
| 3. | Quiz/Viva Voce |  | 10 |
|  | Total |  | 30 |