**Name:- Sharaf Nagatheja**

**Email:-** [**nasharaf@iu.edu**](mailto:nasharaf@iu.edu)

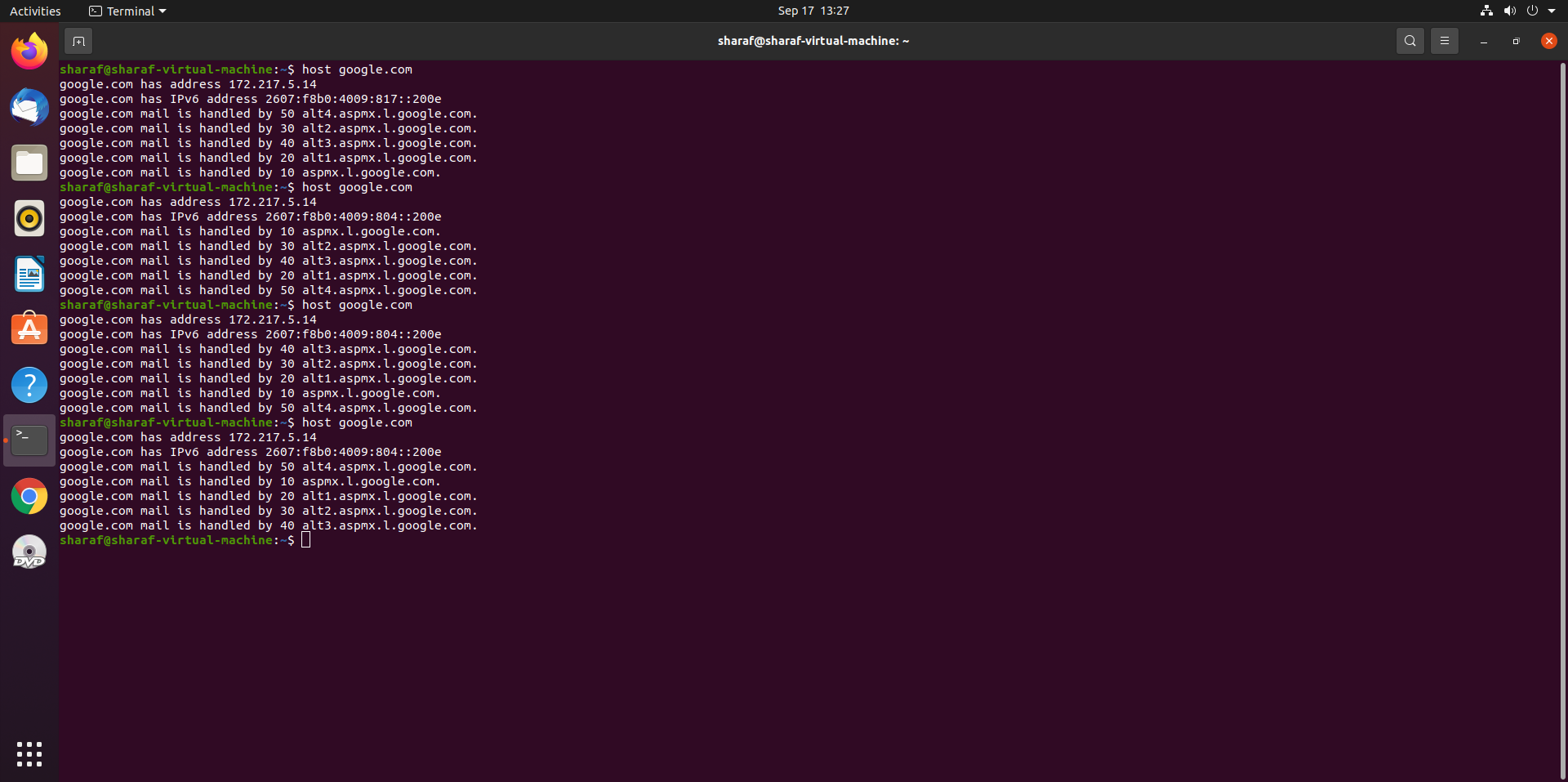
**Id:- 2000927206**

**Computer Networks Lab3**

**Task 1:**

1. **Load balancing refers to distributing incoming network traffic across multiple compute resources. How can DNS be used to load balance services? Give a concrete explanation for google.com**

Yes, DNS can also be used for load balance services mostly web content distribution. It is used to perform load distribution among replicated servers. There are so many busy sites which are replicated over multiple servers. For example, google.com, yahoo.com etc. And for each server running there will be different Ip addresses associated with alias host name. When client makes a request DNS usually considers client request came from first Ip address set in the list of Ip addresses stored in the DNS database. Then for another set of requests made by client the DNS rotates the addresses and gives response from different replicated servers. This process is usually used for load balancing when there are huge number of clients accessing a specific website. While we consider google.com there are millions of people who access to google.com every day but never faces any issue as there is DNS load balancing taking place. Here is the example for google.com of how DNS is rotating addresses and giving responses from different replicated web servers. DNS also uses round robin algorithm to rotate Ip addresses.



1. **DNS has been around since 1985 and the core protocol is still being used today. What is the inherent weakness of DNS (as of**[**RFC1035**](https://www.ietf.org/rfc/rfc1035.txt)**; excluding**[**DNSSEC**](https://datatracker.ietf.org/doc/html/rfc4033)**)? Give an example of how an attacker might utilize it.**

As we can see there are so many services offered by DNS like web and email which makes it to be a critical componenet of internet infrastructure, with many great services offered by DNS there comes so many vulnerabilites. The primary attack which can occur is DDoS bandwidth-flooding attack against DNS servers which means an attacker can send to each dns root server a deluge of packets so that the majority DNS queries are never getting answered. The attackers can send truck load of ICMP ping messages to each of 13 DNS root Ip addresses. Although this type of attack can be minimised by protecting DNS servers with packet fileters which blocks ICMP ping messages directed at the root servers. Another type of DDoS attack is to send a deluge of DNS queries to top-level domain servers. It is harder to filter DNS queries directed to DNS servers and top-level domain servers. DNS can be attacked in other ways which can be man-in-the-middle attack. The attacker intercepts queries from hosts and returns bogus replies. In DNS poisoning attack the attacker tries to make server accept these bogus records into cache. To avoid these type of attacks DNSSEC has been deployed which is secured version of DNS.

1. **Perform a manual iterative DNS query for mail-relay.iu.edu with dig starting from the root servers. List all commands and their outputs and explain why you issued every command. Do not use tracing features (dig +trace) for your final write-down.**

Based on Internet protocol version 4 DNS will be having 13 root servers a,b,c,d,e,f,g,h,I,j,k,l,m.

dig @b.root-servers.net edu q-A

So, this command is used to connect to all Edu servers using root server

dig @a.edu-servers.net iu.edu q-A

From ANS section digging one more root server for iterative process

dig @dns1.iu.edu mail-relay.iu.edu

From ANS section using DNS server connect to mail relay server and checking for Ip addresses

dig @<ip address> mail-relay.iu.edu

Using DNS Ip address access mail relay in the last step where it will provide recursion is not available

Using dig we can see the original Ip address of the domain name system.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

Text

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **You are sitting in a coffee shop and are connected to a public WLAN. You fire up wireshark and start sniffing the traffic of other customers. You notice that all of their traffic is over https so you cannot simply read it. You also notice something striking about the DNS traffic, what is it and what are the implications?**

It is showing that normally packets wont be having src and destination Ip address but DNS is showing the src and destination Ip address which will help attackers make a DDoS attack or Man in the middle attack can perform any type of attacks.

Graphical user interface, text, application, email

Description automatically generated

Here to see the response of host we need to select a transaction id and click apply as a filter then it will show us in how many responses DNS have been returned.

Graphical user interface, text, application

Description automatically generated

So here if we want to get response of that specific host then we can simply double click on it and apply time filter as a column

Graphical user interface, text, application

Description automatically generated

1. **Suppose that IU has an internal DNS cache. You are an ordinary user (no network admin). Can you determine (and if yes, how) if a given external website was recently accessed?**

Yes, we can determine if a given external website was recently accessed as if it is recently accessed the query time will be 0ms as it is stored in DNS cache or else it may take 4ms or more than that to retrieve.

Text

Description automatically generatedText

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**All the above content is referred from text book and wrote in my own words to understand things easily.**