Mohammad Ali Zahir

ID: 4007719

COMP 445: Data Communication & Network Protocols

February 16, 2022

Presented to: Mme Sandra Cespedes

COMP 445 Theory Assignment 2

1. Due to the concept of data encapsulation, the way of passing data to the network core from the network applications is independent. This would mean if the STP (standardized transport protocol) is followed, only the host would need to be running to exchange data.

2. For persistent mode, we could refer it as the keep-alive server. Which means that if the client requires to access the server multiple times, such as a bank website, the connection with the server will stay open until the client is done making his transactions. This usually stays for a definite amount of time. This mode would also work if the client kept on making requests to open the server. For non-persistent mode, if the client needs to access different servers at the same time, this would be the best mode. The client can easily close the server once the transaction is finished but would need to send the request every time.

3.

a) The RTT would be 250 000 km/s / 1000km = 250 s

b) We already have the RTT being 250 s, based on the overhead we would have to add them. We have 125000 bytes per seconds in total. Hence, we calculate the total bytes now, 8192 + 125 + 250 + 500 = 1.38 seconds + 250 seconds = 251.38 seconds

4. It is possible for the client to make a request to the server. To do this, a web attachment would be needed. With the web attachment, we would be able to send reaction without demand from the client. This would make it so once you are logged to a website, you would be able to send packets to a specific server, which will allow us to make a request to a server.

5.

a) To calculate link utilization, we would have to do

If 2 MB takes 50 requests per second, 1 GB will take 50 x 500 = 25 000 requests per seconds.

b) The utilization would be reduced by around ½ or 1/3.

c) Due to the proxy server, we would have to do stop between the client and the server, instead of the client going to the server. This would mean that it will take more time, and hence would not actually be advantageous.

6.

a) It is possible. The main advantage of this way is that we will have multiple intermediate servers. Which would mean if one failed, another one would more than likely still be there.

b) This is not possible since SMTP follows the mail format and HTTP does not.

7. There are a couple of ways of how this practice is possible. One way would be to use a different encoding scheme. Let's take for example the Base64 encoding scheme, this will encode data which was previously binary and turns it to a readable ASCII character. An example of this way of how we read from a binary file in Java and make it readable through File I/O. This way would not work with legacy systems, however, due to the some older systems incapability of reading through binary files.

8.

We can have DNS attacks in different kind of DNS servers.

For root servers, they can be hit with the denial-of-service attack but cannot be attacked since the DNS request cannot really reach the root server.

TLD are more vulnerable to DNS attacks, however, due to caching, the latency in the server is reduced which allows the TLD to not always be attacked by a DNS.

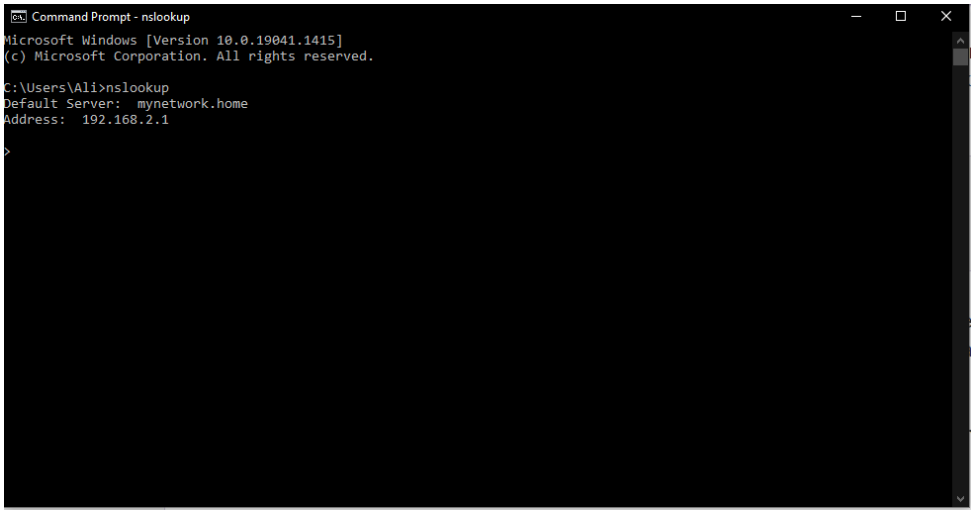
9.

a) It is a database containing contact and registration information for domain names. This database is usually public.

b) By searching whois on Google, I was able to find

1. http://whois.icann.org
2. http://whois.domaintools.com/

c)



d)

```
C:\Users\Ali>nslookup google.ca
Server:  mynetwork.home
Address:  192.168.2.1

Non-authoritative answer:
Name:    google.ca
Addresses:  2607:f8b0:400b:802::2003
          142.251.41.35


C:\Users\Ali>
```

e)

Point of Contact	
Name	Babin , Mike
Handle	BABIN22-ARIN
Company	Concordia University
Street	1455 de Maisonneuve Blvd. W. IITS, LB 800
City	Montreal
State/Province	QC
Postal Code	H3G 1M8
Country	CA
Registration Date	2015-01-08
Last Updated	2022-01-06
Comments	
Phone	+1-514-848-7622 (Fax) +1-514-848-2424 (Office)
Email	mike.babin@concordia.ca
RESTful Link	https://whois.arin.net/rest/poc/BABIN22-ARIN
See Also	Related organizations.

f)

The attacker targets all the databases and attacks them one-by-one.

g)

It should be publicly available. It allows to identify everyone which will increase communication. You could easily find info about a particular company. If it wasn't publicly available, there would be so many hurdles finding out the data from a company.

10.

By using client-server architecture, we would need to upload multiple files sequentially. With P2P, however, the server would only need to upload the file once, and whoever needs to download the file could how many ever times they would want. If the number of users is large, P2P is clearly the way to go because imagining 1000 users uploading multiple files at once would break a server.

11.

The tit-for-tat scheme, or as in specific torrent terms seeding/leeching has a major problem of security. While a person can get another file, it will get the file vulnerabilities, such as the virus attached to it, and the nature of the file (the name could be something, but the actual file could be something else). Since torrent are shared files, this would make it that the virus would spread very fast due to sometimes millions of people downloading the same file at once. If someone stops seeding, the tit-for-tat system just dies down and there lies its biggest vulnerability.

12.

Congestion can cause to poor connection. Once this happens, some platforms like YouTube for example, auto adjust the quality to the lowest one (usually 144 p) until the connection becomes more stable again. In video games, the connection loss is manifested by lag.