Assignment - 2 , Report

Hemanth , Likhith , Akhil
15CS10051 , 15CS10019 , 13CS10018

HTTP Analysis :

Steps :

1. While accessing the server 10.5.20.222 , for each of the ports 8100,8110,8111 we set the following filter in the wireshark.

```
ip.addr == 10.5.20.222 && ip.addr = <our PC's IP>
```

2.We also disabled the cache in the network panel of the tab we used for testing and used that panel to verify the no of GET requests and download time.

Observation and Explanation :

In the user agent field of HTTP requests sent to server we can notice the clients Browser and its version no and OS type , which was common in either of the three ports used to access the server.

No of GET Requests were same for the three ports as they hosted same web pages .

1. Port - 8100

Most of the GET request response body contains 1.0 version number and every time before a GET request it was initiating a TCP Handshake (tcp syn req,syn ack,ack packets) . So it was the 1.0 non persistent server.

GET requests = 16 , Total download time = 90ms
Each GET request time = 10 to 20ms (on average)

2. Port - 8110

Most of the GET requests and responses body consisted of 1.1 version no , yet before each GET Request , a TCP Handshake was initiated , so it was 1.1 , non - persistent version.

GET Requests = 16 , Total Download time = 150ms
Each GET Request time = 10 - 20 ms (on average)

3. Port - 8111

Most of the GET requests and responses body consisted of 1.1 version no and TCP Handshake was initiated only once during the loading of the page . So it was 1.1 , persistent version.

GET Requests = 16 , Total Download time = 80ms

Each GET Request time = 10 - 20 ms (on average)

1. We can see that time to load decrease somewhat in persistent versions due to less repeated TCP initiations.
2. In the 1.1 , non - persistent version download time increased may be due to traffic at that time.

FTP Analysis :

Steps :

1. We have set a filter ip.addr == 10.5.20.222 in the wireshark before accessing the ftp server.
2. We first used the command ftp -d 10.5.20.222 to access the ftp server in the default active mode and then changed to the passive mode using passive command.

Observations and Justifications :

Host IP = 10.109.28.35
Server IP = 10.5.20.222

1. Active Mode :

At first the host starts an http connection with the 21 port of ftp server ,this is the command channel as the all the requests for user name , password based login were sent through this .

> host Port = 40850 , server - Port = 21
> FTP Headers mainly consisted of the requests,
> and the server info such as its type and version ,etc followed
> TCP ACK packets .

By typing ls or help command , the server initiates a http connection with host for the data channel, then the server sends data to host

> host Port = 20 , server - Port = 52439
> FTP-DATA were observed
> with data as headers .

2.Passive Mode :

We typed passive command to enter the passive mode , were the command channel ports didn't change .

host Port = 40850 , server - Port = 21
FTP Headers mainly consisted of the requests,
and the server info such as its type and version ,etc followed
TCP ACK packets .

When typed the ls command , a new http connection is established by the host to server for the data channel , then followed the FTP-DATA packets in the data channel followed by the TCP ACK packets in the command channel.

host Port = 44556, server - Port = 40402
FTP-DATA were observed
with data as headers .

*The server's Data channel port during passive mode was changed for different requests, where as in active mode it remained 20 always.
Explanation - In passive mode the process requesting/sending data in server gets port assigned independently by its OS , but in active mode it tries to send in the port 20 always to maintain standard.