**CS 39006: Networks Lab**

**Assignment 2:**

**Understanding the Protocols of Application Layer**

SUBMITTED BY -

**15CS10031 - PANKAJ DHURVE**

**15CS30025 - SACHIN KUMAR**

**STEPS:**

1.Start Wireshark

2.In the menu bar, go to Capture -> Options

3.In the Input tab, select the interface ​ em1

4.Enter the following ​ capture filter

a. host 10.5.20.222 and host <your IP>

b. This will force wireshark to capture only the packets between the hosts

5.For HTTP, To access the server open a browser and enter the following url (uniform resource locator): http://10.5.20.222:8111 (or 8110 or 8100)

and then observe the packet traces using Wireshark.

6. Enter the ftp commands and watch the packet trace

7. After the capture completes, right click on any packet and click Follow -> TCP stream

a. You should see the data that was sent in the current TCP stream

8. In the capture filter you should see something like ​ tcp.stream eq 1 which

indicates stream number 1

a. By changing the stream number, we can see the various data that was sent in each stream

**1. Observing the packet traces obtained by accessing the HTTP server answer the**

**following:**

**a. Classify the different ports of the HTTP (i.e., 8100, 8110 and 8111) into**

**these classes namely, (i) HTTP 1.1 - with persistent connections, (ii) HTTP**

**1.1 - without persistent connections and (iii) HTTP 1.0. Justify your answer**

**from the observations.**

8111 - HTTP 1.1 PERSISTENT

8110 - HTTP 1.1 NON PERSISTENT

8100 - HTTP 1.0

**b. How many GET requests were issued to access each of the three HTTP**

**server instances?**

HTTP 1.1 PERSISTENT = 19 GET REQUEST

HTTP 1.1 NON PERSISTENT = 19 GET REQUEST

HTTP 1.0 : 19 GET REQUEST

**c. Obtain the amount of time elapsed between the HTTP GET requests and**

**their corresponding responses, while accessing each of these three HTTP**

**server instances?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Packets** | **HTTP 1.1 PERSISTENT**  **(ms)** | **HTTP 1.1**  **NON PERSISTENT**  **(ms)** | **HTTP 1.0 (ms)** |
| **Root** | **9** | **6** | **14** |
| **style.css** | **5** | **27** | **10** |
| **mobile.css** | **10** | **26** | **15** |
| **mobile.js** | **9** | **27** | **15** |
| **logo.png** | **14** | **57** | **14** |
| **satelite.png** | **149** | **273** | **195** |
| **project-image1.jpg** | **44** | **79** | **40** |
| **project-image2.jpg** | **47** | **79** | **28** |
| **project-image3.jpg** | **76** | **118** | **41** |
| **project-image4.jpg** | **76** | **139** | **57** |
| **mars-rover.jpg** | **115** | **269** | **223** |
| **finding-planet.jpg** | **82** | **224** | **199** |
| **new-satellitedish.jpg** | **83** | **274** | **223** |
| **bg-home.jpg** | **234** | **352** | **414** |
| **bg-transparent1.png** | **6** | **12** | **231** |
| **icons.png** | **28** | **14** | **251** |

|  |  |  |  |
| --- | --- | --- | --- |
| **audiowide-regular-webfront.woff** | **80** | **95** | **286** |
| **style.css** | **32** | **29** | **13** |
| **mobile.css** | **12** | **5** | **9** |

**d. What is the total page download time from each of these three HTTP server**

**instances? (total page download time = time of last response message**

**received - time of first GET request message sent)**

Port 8111: HTTP 1.1 PERSISTENT : 14.082147776 - 8.889499737 = 5.192648039 seconds

Port 8110: HTTP 1.1 NON PERSISTENT : 10.155456187 - 9.956863757 = 0.19859243 seconds

Port 8100: HTTP 1.0 : 3.179101714 - 3.017154363 = 0.161947351

**e. Check the user-agent field in the HTTP headers. What information**

**regarding the OS and Browser can you infer from the user-agent field?**

HTTP 1.1 PERSISTENT:

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n

HTTP 1.1 NON PERSISTENT :

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n

HTTP 1.0

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n

**2. Observe the packet traces by accessing the FTP server and answer the following:**

**a. What are the sequences of FTP messages exchanged between the server and**

**the client for (i) active mode connection, (ii) passive mode connection? Note**

**down the message type, FTP header fields, source IP, destination IP, source**

**port and destination port corresponding to those messages.**

ANS:

I)Active mode

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Message type** | **FTP Header Field** | **Source IP** | **Destination IP** | **Source port** | **Destination port** |
| **Response arg:** ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]  **Response code**: Service ready for new user (220) | Sequence number: 1  Next sequence no: 58  Acknowledgment number: 1  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Request command**: USER  **Request arg:** anonymous | Sequence number: 1  Next sequence no: 17  Acknowledgment no.:58  Header Length: 32 bytes | 10.147.79.90 | 10.5.20.222 | 58162 | 21 |
| 331 Anonymous login ok, send your complete email address as your password\r\n  **Response code:** User name okay, need password (331)  **Response arg**: Anonymous login ok, send your complete email address as your password | Sequence number: 58  Next sequence no: 133  Acknowledgment no.: 17  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Request command**: PASS | Sequence number: 17  Next sequence no: 24  Acknowledgment no.: 133  Header Length: 32 bytes | 10.147.79.90 | 10.5.20.222 | 58162 | 21 |
| 230-Welcome, archive user anonymous@10.147.79.90 !\r\n  **Response code:** User logged in, proceed (230)  **Response arg:** Welcome, archive user anonymous@10.147.79.90 ! | Sequence number: 133  Next sequence no: 185  Acknowledgment no.:24  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Response code:** User logged in, proceed (230)  **230**-The local time is: Thu Jan 25 01:47:51 2018\r\n  **230**-\r\n  **230**-This is an experimental FTP server. If you have any unusual problems,\r\n  **230**-please report them via e-mail to <root@localhost>.\r\n  **230**-\r\n  **230** Anonymous access granted, restrictions apply\r\n | Sequence number: 185  Next sequence no: 434  Acknowledgment no.:24  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Request command:** SYST | Sequence number: 24  Next sequence no: 30  Acknowledgment no.: 434  Header Length: 32 bytes | 10.147.79.90 | 10.5.20.222 | 58162 | 21 |
| **Response code:** NAME system type (215)  **Response arg**: UNIX Type: L8 | Sequence number: 434  Next sequence no: 453  Acknowledgment no: 30  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| 421 No transfer timeout (600 seconds): closing control connection\r\n  **Response code:** Service not available, closing control connection (421)  **Response arg:** No transfer timeout (600 seconds): closing control connection | Sequence number: 453  Next sequence no: 520  Acknowledgment no: 30  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |

II)Passive mode

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Message type** | **FTP Header Field** | **Source IP** | **Destination IP** | **Source port** | **Destination port** |
| **Response arg:** ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]  **Response code**: Service ready for new user (220) | Sequence number: 1  Next sequence no: 58  Acknowledgment number: 1  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Request command**: USER  **Request arg:** anonymous | Sequence number: 1  Next sequence no: 17  Acknowledgment no.:58  Header Length: 32 bytes | 10.147.79.90 | 10.5.20.222 | 58162 | 21 |
| 331 Anonymous login ok, send your complete email address as your password\r\n  **Response code:** User name okay, need password (331)  **Response arg**: Anonymous login ok, send your complete email address as your password | Sequence number: 58  Next sequence no: 133  Acknowledgment no.: 17  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Request command**: PASS | Sequence number: 17  Next sequence no: 24  Acknowledgment no.: 133  Header Length: 32 bytes | 10.147.79.90 | 10.5.20.222 | 58162 | 21 |
| 230-Welcome, archive user anonymous@10.147.79.90 !\r\n  **Response code:** User logged in, proceed (230)  **Response arg:** Welcome, archive user anonymous@10.147.79.90 ! | Sequence number: 133  Next sequence no: 185  Acknowledgment no.:24  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Response code:** User logged in, proceed (230)  **230**-The local time is: Thu Jan 25 01:47:51 2018\r\n  **230**-\r\n  **230**-This is an experimental FTP server. If you have any unusual problems,\r\n  **230**-please report them via e-mail to <root@localhost>.\r\n  **230**-\r\n  **230** Anonymous access granted, restrictions apply\r\n | Sequence number: 185  Next sequence no: 434  Acknowledgment no.:24  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |
| **Request command:** SYST | Sequence number: 24  Next sequence no: 30  Acknowledgment no.: 434  Header Length: 32 bytes | 10.147.79.90 | 10.5.20.222 | 58162 | 21 |
| **Response code:** NAME system type (215)  **Response arg**: UNIX Type: L8 | Sequence number: 434  Next sequence no: 453  Acknowledgment no: 30  Header Length: 32 bytes | 10.5.20.222 | 10.147.79.90 | 21 | 58162 |

**b. Distinguish between the command channel and data channel of the**

**communication for active and passive mode TCP. Who initiates the data**

**channel connection for (i) active mode, (ii) passive mode of FTP?**

Command Channel : Command channel carries the commands that are needed for proper functioning of the network

Data channel : Data Channel carries data

In active mode, it is the server that initiates the connection.

In passive mode, client initiates the connection.

**c. What is the port used for data communication (for both the active mode and**

**passive mode FTP connections)? What is the difference when the passive**

**mode is enabled by the client?**

Active mode:

Server Port: 21 (command port)

Client Port: 40212

Active port: 42850

Active IP address: 10.147.79.90

Passive Mode:

Server Port :21 (command port)

Client Port:40058

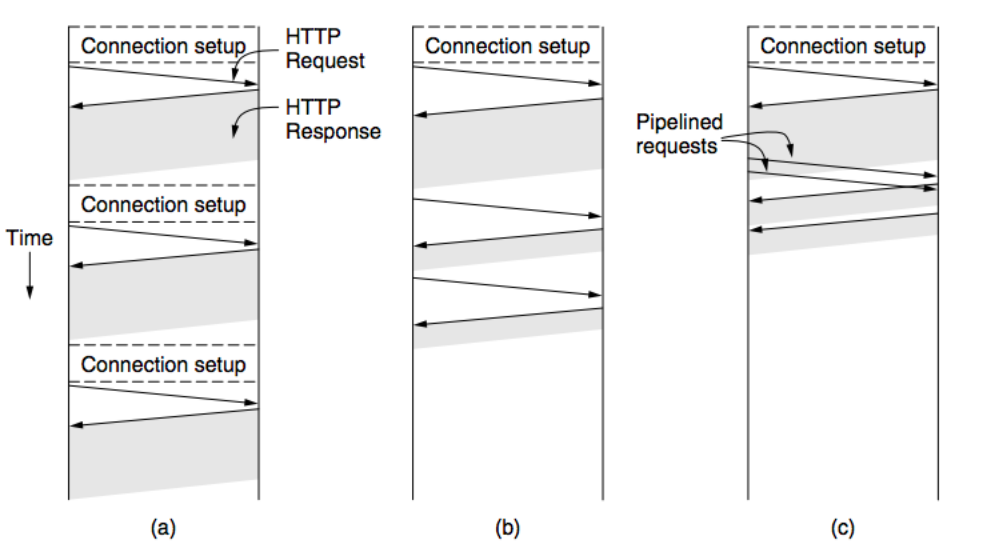
Passive port: 41516

Passive IP address: 10.5.20.222

In passive mode, client initiates the connection, hence the connection is secure. However, in active mode the server initiates the connection and the client’s firewall may block it.

**JUSTIFICATION:**

**HTTP :**

****

**HTTP 1.0 HTTP 1.1 PERSISTENT HTTP 1.1 NON PERSISTENT**

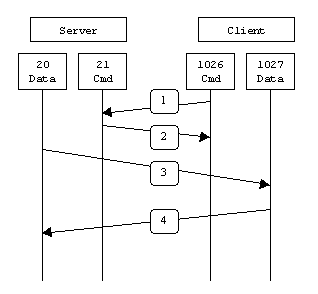
**HTTP 1.0 – After the connections were established, a single request was sent over and a single response was sent back. Then the TCP connections are released.**

**Create separate connections for every content in the web-page. Overhead is high.**

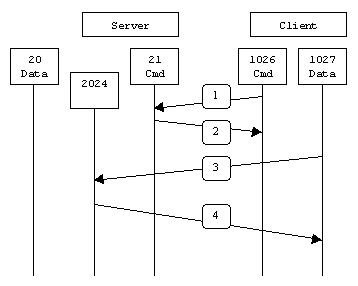
**Persistent Connection (HTTP 1.1) – send additional requests and additional responses in a single TCP connection (connection reuse).**

**It is also possible to pipeline requests.**

**Active FTP:**

****

**Passive FTP:**

****