**CSE 421 ID: 17301121**

**Application Layer Protocols (HTTP.SMTP/POP)**

**Examination Lab**

**Objectives:**

Capture traffic and observe the PDUS for HTTP, SMTP, POP.

**Task 1: Observe HTTP traffic exchange between a client and server.**

**Step 1 – Run the simulation and capture the traffic.**

* Enter **Simulation** mode.
* Click on the PC1. Open the **Web Browser** from the **Desktop**.
* Enter **www.bracu.ac.bd** into the browser. Clicking on **Go** will initiate a web server request. Minimize the Web Client configuration window.
* Two packets appear in the **Event List**, a DNS request needed to resolve the URL to the IP address of the web server and an ARP request needed to resolve the IP address of the server to its hardware MAC address.
* Click the **Auto Capture / Play** button to run the simulation and capture events.
* Sit tight and observe the packets flowing through the network.

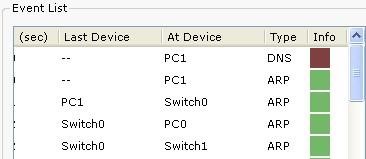


* When the above message appears Click “View Previous Events".
* Click on PC1. The web browser displays a web page appears.

**Step 2 – Examine the following captured traffic.**  Our objective in this lab is only to observe HTTP traffic.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Last Device** | **At Device** | **Type** |
| 1. | PC1 | Switch 0 | HTTP |
| 2.. | Local Web Server | Switch 1 | HTTP |

* Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.



When you click on the Info square for a packet in the event list the **PDU**  **Information** window opens. If you click on these layers, the algorithm used by the device (in this case, the PC) is displayed. View what is going on at each layer.

* Examine the PDU information for the remaining events in the exchange.

***For packet 1::***

What kind of HTTP packet is packet no. 1?

* No.1 packet is HTTP request packet.

Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see?

* I see basically information of HTTP request packet. Like, accepted language, connection type, host website.

***For packet 2:***

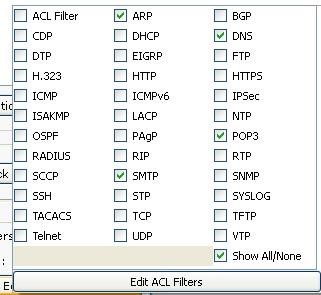
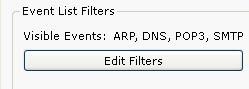
Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see? What kind of HTTP packet is this?

* I see HTTP response packet. Connection length in byte, server name & connection type of the hosted website are the type of Information given.

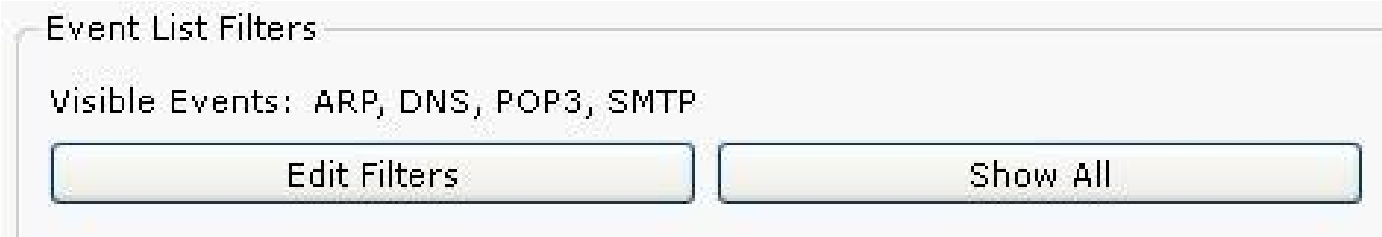
**Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.**

**Step 1 – Run the simulation and capture the traffic.**

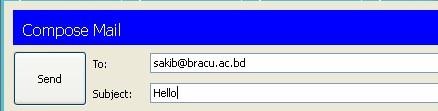
* On the Event List window click “Reset Simulation” button. All previous packets will disappear.
* At the bottom of the Event List window, there is a filter which filters the protocols that we want to see. Click Edit filters. Another window appears showing different protocols, unclick HTTP and click SMTP and POP3.



* Click a space anywhere outside the popup window, then it will disappear.
* Your Event List Filter should be as shown below:



Now click on the PC1. Close the web browser window. Open the **Email** from the **Desktop**. A mail browser window will open. Click “compose”, another window appears.



* Fill the window as shown and press send.
* Minimize the client window .
* Click the **Auto Capture / Play** button to run the simulation and capture events.
* Sit tight and observe the packets flowing through the network.
* This interaction is between the sender client and its email server.

**Step 2 – Examine the following captured traffic.**

Our objective in this lab is only to observe SMTP traffic.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Last Device** | **At Device** | **Type** |
| 3. | PC1 | Switch 0 | DNS |
| 4. | PC1 | Switch 0 | SMTP |
| 5. | Bracu Email Server | Switch 1 | SMTP |

* Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.
* Examine the PDU information.

***For packet 4::***

What is the purpose of this DNS packet?

* The purpose of this DNS packet is to get the email server’s IP addresses.

***For packet 5& 6::***

Explain why SMTP packet was sent to the email server and the server replied with an SMTP packet?

* SMTP basically takes the mail to the requested server as a confirmation that the server has received the mail. Also, it carries the MAC address of the server and the server responds with a SMTP packet. Moreover, it is verifying that server just got the mail.

**Step 3 – Run the simulation and capture the traffic for POP.**

* On the Event List window click “Reset Simulation” button. All previous packets will disappear.
* Now click on the PC0. Open the **Email** from the **Desktop**. A mail browser window will open. Click “**receive**”, minimize the window.
* Click the **Auto Capture / Play** button to run the simulation and capture events.

Sit tight and observe the packets flowing through the network.

* This interaction is between the sender client and its email server.

**Step 2 – Examine the following captured traffic.**

Our objective in this lab is only to observe POP traffic.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Last Device** | **At Device** | **Type** |
| 6. | PC1 | Switch 0 | DNS |
| 7. | PC1 | Switch 0 | POP3 |
| 8. | Bracu Email Server | Switch 1 | POP3 |

* Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.
* Examine the PDU information.

***For packet 6::***

What is the purpose of this DNS packet?

* The purpose of this DNS packet is to get the IP address of the email server.

***For packet 7&8::***

Explain why POP packet was sent to the email server and the server replied with a POP packet?

* The server replied with a POP packet which is carrying the expected e-mail for the client. Also, POP packet was sent to the email server, because it is required to store the email for that email address which was sending the POP packet.

•