Introduction to Computer Network Project 2

HTTP Packet

一、 實驗目的

在 Project1，我們已經學會如何使用 Wireshark 擷取封包，並且透過觀察各個封包的 格式，可得知各個封包的行為，也大致瞭解了 HTTP protocol 是如何運作。 本次實驗主要是讓同學更瞭解 HTTP Protocol，透過檢索不同網頁時，觀察不同網頁 行為將會有不同的 TCP message formats，試著瞭解並且分析他們。

本次實驗分為下列三個部分：

1. Retrieving large HTML files
2. Retrieving HTML files with embedded objects
3. HTTP authentication and security

我們將在下面一一詳細敘述之。

二、 實驗介紹

在 Project2，要請同學先清空 browser 的 cache 後，再次觀察 HTTP GET messages 是否會有不一樣的行為發生。

也請同學**盡可能關閉會使用網路的應用程式、網頁**，避免蒐集到與實驗無關的封包，造成分析困難。

清除 browser 的 cache 的方法

- 若是在 Internet Explorer：工具->網際網路選項->一般->瀏覽歷程記錄->刪除->勾選” Temporary Internet Files”->刪除。
- 若是在 Google Chrome、Firefox：檔案->新增無痕式視窗，利用此視窗就不會有之前的 cache。若須清除無痕的暫存，只需要關閉所有無痕視窗再重開即可。
- 在不同的瀏覽器下，清除 cache 的步驟、路徑各不相同。

1. Retrieving large HTML files Project2 的第一部分，要請同學觀察當連上內容長短不同的網頁時，觀察 multiple TCP packets 的行為。

   步驟 1：開啟你的 web browser，並且確定 browser 的 cache 已經清空。

   步驟 2：開啟 Wireshark 擷取封包

   步驟 3：連上內容較短的網頁

   http://nctucs_icn.nctu.me/Project2/pro2_1.html

   步驟 4：再連上內容較長的網頁

http://nctucs_icn.nctu.me/Project2/pro2_2.html

試著觀察封包回答下列問題：
(1) 當連上短內容的網頁時，browser 共發出了幾個 HTTP GET request messages？ 當連上長內容的網頁時，browser 共發出了幾個 HTTP GET request messages？
(2) 一個 HTTP response 需要多少 data-containing TCP segments？
(3) 當收到 HTTP GET request 的回應，其回應的 status code and phrase 為何？

2. Retrieving HTML files with embedded objects
現在我們所瀏覽的網頁，幾乎都含有 embedded objects，像是 image files，通常我 們 image files 會存放在另外一部主機。在這一部份，請同學連上助教所提供的網頁， 觀察其封包行為，並且試著回答下列問題。
步驟 1：開啟你的 web browser，並且確定 browser 的 cache 已經清空。
步驟 2：開啟 Wireshark 擷取封包
步驟 3：連上助教所提供的網頁:
http://nctucs_icn.nctu.me/Project2/pro2_3.html

試著觀察封包回答下列問題：
(1) browser 共送出幾個 HTTP GET request messages？而這些 GET request 是送往哪個 Internet addresses？
(2) 當網頁內容含有兩張的影像，你的 browser 是一張圖片下載完再載另外一張，或 是兩張影像平行下載？請解釋。

3. HTTP authentication and security
現今網路安全越來越受到重視，卻似乎依舊不安全。所以 Project2 的第三部分，我們要更進一步瞭解 HTTP 的認證與安全。 在這一部份請同學連上助教所提供需要帳號、密碼的網頁，輸入並且登入後，試著觀察封包行為並回答下列問題。
步驟 1：開啟你的 web browser，並且確定 browser 的 cache 已經清空。
步驟 2：開啟 Wireshark 擷取封包
步驟 3：連上 password-protected 的網頁
http://nctucs_icn.nctu.me/Project2/HTTP-wireshark-file5.html
username：icn
password：rocks

試著觀察封包回答下列問題：

(1) 觀察一開始 browser 所發出的 HTTP GET message，server 對其的回應 (status code and phrase)。

(2) 當 browser 送出第二次 HTTP GET message 時，此時的 HTTP GET message 有什麼新的 field？

4. BONUS： 利用上面助教所給的網址登入後，會在 HTTP GET message 的 header 看到加密過的帳號(icn)和密碼(rocks)。現在我們知道是利用 Base64 所加密，可透過下列網址進行解密：
   http://www.motobit.com/util/base64-decoder-encoder.asp
   請同學試著在封包裡找出**加密過後的帳號、密碼**，貼出其截圖並且回答出**解密過後的帳號、密碼**內容。

三、 Requirements

1. 各小題請適當地搭配圖檔作解釋。
2. 請依題號回答
3. 實驗相關心得，自己學到了什麼?

四、 Rules

1. 請於報告上註明自己實驗之環境（如 OS, 網卡型號, …等）
2. 請勿抄襲，抄襲者本實驗以 0 分計算
3. Due day : 11/16，23:59
4. 請將報告輸出為 pdf
5. 報告繳交方式：請上傳到 e3，檔名格式為 project2_學號.pdf
6. 如有任何問題，可以至工三 638 詢問助教，以下是助教聯絡方式
   icnta@win.cs.nctu.edu.tw

五、 Reference:

[1] Wireshark Homepage, http://www.wireshark.org/

[2] Wireshark user's guide, http://www.wireshark.org/docs/wsug_html/