# 資安導論——Linux 學習 + Wireshark 封包分析

## 壹、Linux 介紹

### 一、Linux 的誕生

Linux 最初由 Linus Torvalds 在 1991 年開發，他當時是一名芬蘭赫爾辛基大學的學生，因為對當時的 MINIX 作業系統不滿意，便決定自行開發一套新的內核（Kernel）。他將這個專案開放給全球的開發者共同改進，並最終形成了今天的 Linux 作業系統。

### 二、發展與演進

（一）**1991** 年

Linus Torvalds 發布第一個 Linux 內核版本（0.01）。

（二）**1992** 年後

Linux 內核採用了 GNU 通用公共授權（GPL），這讓它成為自由軟體，促進了社群的發展。

（三）**1993-1994** 年

出現了多個 Linux 發行版（如 Slackware、Debian），這些發行版為 Linux 的普及奠定基礎。

（四）**2000** 年代

Linux 在伺服器領域崛起，許多企業開始使用 Linux 作為伺服器系統，例如 Red Hat、CentOS 等。

（五）近年

Linux 被廣泛應用於雲端運算、行動裝置（如 Android）、嵌入式系統（如路由器、物聯網設備）以及超級電腦領域。

### 三、核心特性

（一）開放原始碼

任何人都可以自由使用、修改和發佈。

（二）多使用者、多工作業系統

允許多個使用者同時操作，並支援多工處理。

（三）高度客製化

可以根據需求調整系統，適用於伺服器、桌面、嵌入式設備等多種環境。

### 四、劣勢

| 缺點 | 描述 |
| --- | --- |
| 學習門檻較高 | Linux 主要依賴指令操作，對於習慣圖形介面的使用者來說，需要花費時間學習。 |
| 軟體相容性問題 | 部分商業軟體（如 Adobe Photoshop、Microsoft Office）沒有 Linux 版本，需要透過模擬器（如 Wine）或虛擬機運行。 |
| 硬體驅動支援有限 | 部分廠商不提供 Linux 版本的驅動程式，可能導致某些硬體無法正常運作。 |
| 遊戲支援較少 | 雖然近年來透過 Steam 等平台 Linux 遊戲數量增加，但仍不如 Windows 豐富。 |

| | |
|---|---|
| 企業環境相容性 | 某些企業環境仍以 Windows 為主，Linux 可能需要額外設定才能與 Windows 網域或其他專屬軟體整合。 |
| 技術支援較少 | 雖然 Linux 有強大的社群支援，但不像 Windows 或 macOS 有官方專屬客服，問題解決可能需要自行搜尋資料或詢問論壇。 |

這些缺點使得 Linux 在桌面應用、多媒體及遊戲使用的普及率相對較低，但它仍然在伺服器、嵌入式系統、開發環境等領域有廣泛應用，其重要性依舊不容小覷。

# 貳、熟悉 Linux 的基本概念與常用指令

## 一、基本系統概念

### (一)目錄架構

| 目錄 | 功能描述 |
|---|---|
| **/** | 根目錄，所有檔案與目錄的起點 |
| **/bin** | 存放基本系統指令，如 **ls**、**cp** |
| **/etc** | 存放系統設定檔 |
| **/home** | 存放使用者的家目錄 |
| **/var** | 存放變動資料(如日誌 **log** 檔案) |
| **/usr** | 存放應用程式與程式庫 |
| **/tmp** | 存放臨時檔案 |
| **/dev** | 存放裝置檔案(如 **/dev/sda**) |

### (二)權限管理

| 權限 | 符號 | 作用 |
|---|---|---|
| 讀取 | **r** | 允許讀取檔案內容 |
| 寫入 | **w** | 允許修改檔案內容 |
| 執行 | **x** | 允許執行檔案(如腳本) |

範例權限格式：

**-rwxr-xr-- 1 user group 1234 Mar 24 12:34 example.sh**

| 欄位 | 說明 |
|---|---|
| **-** | 檔案類型(**d** 代表目錄，**-** 代表檔案) |
| **rwx** | 擁有者權限 |
| **r-x** | 群組權限 |

| | |
|---|---|
| **r--** | 其他人權限 |

(三)使用者與群組

| 類型 | 描述 |
|---|---|
| **root** | 系統管理員，擁有最高權限 |
| 一般使用者 | 只能操作自己的檔案 |
| **sudo** 指令 | 讓一般使用者執行管理員權限的指令 |

(四)軟體管理

| **Linux** 發行版 | 套件管理工具 | 指令範例 |
|---|---|---|
| CentOS / RHEL | **dnf** 或 **yum** | **dnf install package** |
| Debian / Ubuntu | **apt** | **apt install package** |

## 二、常用操作指令

(一)檔案與目錄操作

| 指令 | 功能 |
|---|---|
| **ls** | 列出目前目錄中的檔案與資料夾 |
| **cd** | 切換目錄，如 **cd /home/user** |
| **pwd** | 顯示當前所在的目錄位置 |
| **mkdir** | 建立新資料夾，例如 **mkdir test** |
| **rmdir** | 刪除 空 資料夾 |
| **rm** | 刪除檔案或目錄，如 **rm -r mydir** |
| **cp** | 複製檔案或目錄，例如 **cp file1 file2** |
| **mv** | 移動或重新命名檔案，例如 **mv oldname newname** |

(二)檔案內容操作

| 指令 | 功能 |
|---|---|
| **cat** | 顯示檔案內容，如 **cat file.txt** |
| **tac** | 反向顯示檔案內容 |
| **less / more** | 分頁顯示檔案內容，如 **less file.txt** |

| | |
|---|---|
| **head** | 顯示檔案的前幾行，如 **head -n 10 file.txt** |
| **tail** | 顯示檔案的最後幾行，如 **tail -n 10 file.txt** |
| **grep** | 在檔案中搜尋字串，例如 **grep "error" logfile.txt** |

（三）權限與擁有者管理

| 指令 | 功能 |
|---|---|
| **chmod** | 更改檔案權限，如 **chmod 755 script.sh** |
| **chown** | 更改檔案擁有者，如 **chown user:group file.txt** |
| **chgrp** | 更改檔案群組，如 **chgrp users file.txt** |

（四）系統管理

| 指令 | 功能 |
|---|---|
| **ps** | 查看目前運行的程序 |
| **top / htop** | 監控系統運行狀況 |
| **df** | 查看磁碟空間使用情況 |
| **du** | 計算檔案或目錄大小，如 **du -sh /home** |
| **free** | 檢查記憶體使用情況 |
| **uptime** | 查看系統運行時間 |
| **who** | 顯示當前登入的使用者 |
| **uname** | 顯示系統資訊，如 **uname -a** |

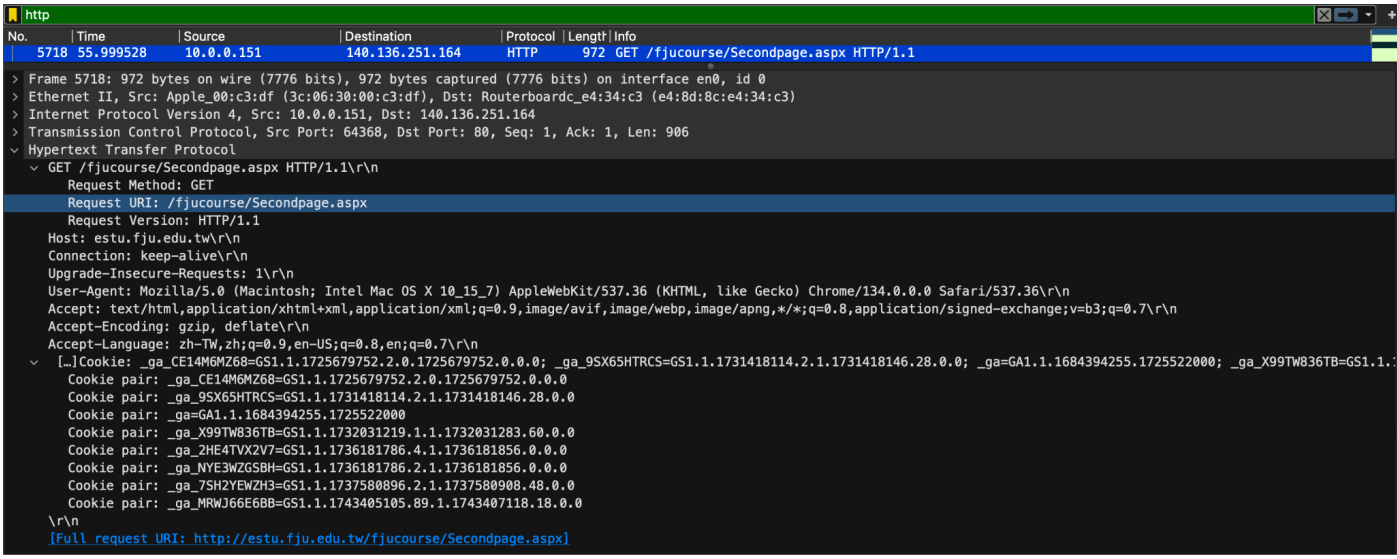
（五）檔案壓縮與解壓縮

| 指令 | 功能 |
|---|---|
| **tar** | 打包與解壓，如 **tar -cvf archive.tar dir/** |
| **gzip / gunzip** | 壓縮與解壓 **.gz** 檔案 |
| **zip / unzip** | 壓縮與解壓 **.zip** 檔案 |

# 參、Wireshark 封包分析

## 一、整體內容

以[輔仁大學113學年度第二學期開課資料查詢系統]為例




# 二、分析

## (一)HTTP GET 請求

| 欄位 | 內容 | 作用 |
|---|---|---|
| **Request Line** | **GET /fjucourse/Secondpage.aspx HTTP/1.1** | GET 方法請求伺服器上的 /fjucourse/Secondpage.aspx 頁面。 |
| **Host** | **estu.fju.edu.tw** | 指定請求的目標伺服器。 |
| **Connection** | **keep-alive** | 讓伺服器保持 **TCP** 連線開啟，以便後續請求可重用。 |
| **Upgrade-Insecure-Requests** | **1** | 告知伺服器，若可用 HTTPS，則應該升級為 HTTPS。 |
| **User-Agent** | **Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36** | 提供用戶端的瀏覽器資訊，讓伺服器可依照裝置類型提供適合的內容。 |
| **Accept** | **text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7** | 告訴伺服器客戶端可以接受哪些 MIME 類型的回應，如 HTML、XML、圖片等。 |

| | | |
|---|---|---|
| **Accept-Encoding** | **gzip, deflate** | 告知伺服器客戶端支援哪些壓縮方式（gzip、deflate），減少傳輸數據量。 |
| **Accept-Language** | **zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7** | 指定客戶端的語言偏好，讓伺服器可以回應適當語言的內容（繁體中文優先）。 |

（二）**Set-Cookie**（伺服器回應時設定的 **Cookie**）

當使用者第一次訪問網站時，伺服器透過 Set-Cookie 指示瀏覽器儲存特定 Cookie，用來存儲使用者資訊或會話識別碼。

| **Cookie** 名稱 | 值（部分） | 屬性 | 作用 |
|---|---|---|---|
| **_ga_CE14M6MZ68** | **GS1.1.1725679752.2.0.1725679752.0.0.0** | **HttpOnly; Secure; SameSite=Lax** | 追蹤使用者行為，並確保該 Cookie 只能透過 HTTPS 傳輸，不可透過 JavaScript 存取。 |
| **_ga_9SX65HTRCS** | **GS1.1.1731418114.2.1.1731418146.28.0.0** | **HttpOnly; Secure; SameSite=Lax** | Google Analytics 相關 Cookie，用於區分不同的用戶。 |
| **_ga** | **GA1.1.1684394255.1725522000** | **Secure; SameSite=None** | 主要的 Google Analytics 追蹤識別碼。 |
| **_ga_X99TW836TB** | **GS1.1.1732031219.1.1.1732031283.60.0.0** | **Secure** | 可能與特定區段的使用者識別或行為分析有關。 |
| **_ga_2HE4TVX2V7** | **GS1.1.1736181786.4.1.1736181856.0.0.0** | **HttpOnly; Secure** | 進一步追蹤使用者的瀏覽行為，增強分析數據準確性。 |

**Set-Cookie** 屬性說明：

1. **Secure**：僅在 HTTPS 連線時傳輸，避免在未加密的 HTTP 傳輸時被攔截。
2. **HttpOnly**：瀏覽器的 JavaScript 無法存取該 Cookie，減少 XSS（跨站腳本攻擊）風險。
3. **SameSite**：防止 CSRF（跨站請求偽造）攻擊。Lax 允許同站請求攜帶 Cookie，而 None 則允許跨站請求傳遞 Cookie。

（三）**Cookie Header**（瀏覽器發送的 **Cookie**）

在後續的 HTTP 請求中，瀏覽器會自動將儲存的 Cookie 附加到 Cookie Header 中發送給伺服器。用於追蹤使用者的網頁瀏覽歷史、分析用戶行為並顯示個性化內容、提供身份驗證（若有 session 相關的 Cookie）。

| **Cookie** 名稱 | 值（部分） | 用途 |
|---|---|---|
| **_ga_CE14M6MZ68** | **GS1.1.1725679752.2.0.1725679752.0.0.0** | Google Analytics 追蹤 ID，記錄使用者訪問行為。 |
| **_ga_9SX65HTRCS** | **GS1.1.1731418114.2.1.1731418146.28.0.0** | Google Analytics Cookie，用於區分不同的瀏覽者。 |
| **_ga** | **GA1.1.1684394255.1725522000** | 主要識別碼，用於統計訪問次數與時間。 |
| **_ga_X99TW836TB** | **GS1.1.1732031219.1.1.1732031283.60.0.0** | 可能與網站特定區域的流量分析有關。 |
| **_ga_2HE4TVX2V7** | **GS1.1.1736181786.4.1.1736181856.0.0.0** | 進一步分析使用者的互動行為。 |
| **_ga_NYE3WZGSBH** | **GS1.1.1736181786.2.1.1736181856.0.0.0** | 另一組 Google Analytics Cookie，可能是區分不同設備的變數。 |
| **_ga_7SH2YEWZH3** | **GS1.1.1737580896.2.1.1737580908.48.0.0** | 記錄使用者的會話狀態。 |
| **_ga_MRWJ66E6BB** | **GS1.1.1743405105.89.1.1743407118.18.0.0** | 追蹤使用者在網站上的行為，可能與持續時間有關。 |

# 肆、心得

## 一、Linux

在學習 Linux 的過程中，我認識到 Linux 的目錄架構、常用指令、權限管理、使用者與群組概念等基礎知識，並熟悉了如 ls、cd、chmod、ps 等 Linux 的操作指令。此外，我也發現 Linux 具有高穩定性、開放原始碼的優勢，同時被廣泛應用於雲端運算、行動裝置、嵌入式系統以及超級電腦領域，但也存在學習門檻較高、軟體相容性問題等缺點。在這次學習中，我對 Linux 的系統管理與應用有了更深入的認識，未來希望能更熟悉 Shell 腳本及伺服器管理，以提升實務應用能力。

## 二、Wireshark

透過對 Wireshark 的學習與實作，我深入了解了 HTTP GET 請求與 Cookie 的運作機制，特別是 Set-Cookie 和 Cookie Header 之間的關係。透過 Wireshark 捕捉封包，我觀察到 GET 請求會攜帶 Host、User-Agent、Accept 等標頭，以及 Cookie Header 來傳遞用戶資訊。同時，伺服器回應時會使用 Set-Cookie 來設定新的 Cookie，影響後續請

求的狀態管理。我也學習到 Secure、HttpOnly、SameSite 等 Cookie 屬性如何影響安全性。這次學習強化了我對網路協議分析、網站身份驗證及安全機制的理解，對於未來的應用與開發有很大幫助。