認識駭客的攻擊手法

組員:
08 歐陽筠
38 甘雨潔

「駭客」（hacker）

一詞一般有以下意義：

- 一個對（某領域內的）程式語言有足夠了解，可以不經長時間思考就能創造出有用的軟體的人。
- 喜愛編程(Coding)並享受在其中變得更擅長於編程的人。
- 喜愛自由(Freedom)，不易受約束，但覺得假如是為了喜愛的事物，可以被受適當的約束。

「黑客、怪客、垮客和劊客」（cracker）

一詞一般有以下意義：

- 一個惡意（一般是非法地）試圖破解或破壞某個程式、系統及網路安全的人。
- 「hacker」們建設，而「cracker」們破壞。

-來自維基百科wiki

一、白帽駭客(White Hat Hacker):

- 白帽駭客有能力入侵電腦系統、破壞系統。不過他利用他的技能來協助組織加強安全。
- 例如在資安公司進行滲透、弱掃的執行者，或負責資安網管人員。

二、黑帽駭客(Black Hat Hacker):

- 黑帽駭客也被叫做Cracker，他們利用自己的技能來進行非道德行為。如攻擊、竊取資料...。

三、灰帽駭客(Gray Hat Hacker):

- 灰帽駭客可以看成是偶而會做出非道德事情的白帽駭客。
- 例如在資安公司進行滲透測試的執行者，於工作其間取得的資訊，做為已用，即為灰帽駭客。

四、通訊駭客(Phreaker):

- 可以拆成Phone and freaker或是看成freeker，從字面就可猜出，有辦法打免費電話的駭客，利用其通訊專業技術，而可打免費的電話。

五、毛頭駭客(Script Kiddy):

- 是駭客中最少技術技能的駭客，對於系統、網路、程式知識都很匱乏，只能下載一些駭客程式進行攻擊行為，沒有撰寫自已程式的能力，對於運作原理也不了解。

六、信念駭客(Hacktivist):

- 心中總抱持一股信念而進行駭客行為，可能是政治、宗教，也常於攻擊成功後留下如國家的資訊、宗教的資訊...，為了信念而戰。

七、電腦安全駭客(Computer Security Hacker):

- 擁有電腦與網路知識的駭客，這樣駭客懂得網路運作原理與其資安風險，比如在一個有IPS的網路環境，他知道如何避開IPS的偵測與阻擋進行攻擊。

八、學術駭客(Academic Hacker):

- 這類駭客往往有較高的教育水平，通常任職於學術環境或是學生，懂得自己撰寫程式、研究攻擊運作原理...，常利用學術資源撰寫出很"聰明"的程式。
- 大部份在網路上會留下真名，著重在開放源始碼的系統。

九、興趣駭客(Hobby Hacker):

- 興趣駭客通常著重在家用電腦，比如破解在電腦上的軟體程式、讓iphone解鎖、超頻自己的電腦、把PC改成水冷、讓第四台解碼...

程式攻擊

- 程式漏洞攻擊，就是利用網站現有的漏洞，輸入有害的文字或程式碼，直接偷取各種網站資訊。

SQL Injection

- SQL Injection 中文又可以稱為， SQL 注入攻擊，駭客針對有此漏洞網站，透過網站的輸入欄位，上傳惡意的 SQL 代碼，使得 SQL 執行時發生管理員未預見的結果，而將資料庫的內容擷取出來。
- 2012 年，網路安全公司 Imperva 研究發現，一家公司平均每個月會遭到四次 SQL Injection 攻擊，而且零售業會比其它行業多遭受兩倍以上的攻擊。

XSS 攻擊

- XSS 全名是 Cross Site Scripting ，中文又可以稱為「跨站腳本攻擊」，這種攻擊方式也是利用惡意的程式代碼，將這些代碼輸入至網頁內容，常用的程式語言是 Javascript ，過去常發生在留言版，討論區等等功能，當 End-user 點擊帶有惡意代碼的進結， Browser 將被導到駭客指定的網頁，並且在 Browser 中執行有害的程式，藉此竊取用戶密碼或個人隱私。
- 研究發現，每 10 個網站裡面至少有 7 個網站有 XSS 漏洞。

DDoS 攻擊

- DDoS 全名是 Distributed Denial of Service Attack ，當網站遭到 DDoS 攻擊，這個網站就會停止他的服務，所以的用戶將無法接收到網站的任何訊息，也就是 End-user 被網站給拒絕了(Denial)，最簡單的 DDoS 攻擊，就是駭客短時間內傳送大量的網路封包，堵塞網站的流量，當封包超過網站的負載量，這個網站將無法再工作而停止服務，這個攻擊方式常常被「Anonymous」駭客組織使用。

Fraud 欺騙

- Fraud 就是指駭客透過各種手段欺騙用戶，使用戶執行錯誤的網頁操作，而不小心將個人資料傳送給駭客。

Phishing 釣魚

- 現代的人，大多已經知道不可以把個人隱私告訴不認識的人，但是你確定是誰正在跟你用通訊網體聊天嗎? 若是駭客取得你朋友的帳號，就能直接詢問你的個人隱私資料，另外像是傳送 Email，facebook message， 等等，也能傳送偽造的連結與表單給你填寫，一旦分不清真真假假，就很容易受騙上當。
-

Clickjacking

- Clickjacking 是 Click hijacking 這兩個字的合併，中文就是「點擊劫持」，駭客在一般的網站註冊表單中，寫入一些特殊 UI 顯示的 CSS 語法，只要在註冊頁中的確認註冊按鈕點擊區塊，多新增一顆透明的按鈕，因為按鈕是看不到的，User 會很自然而然的點擊「確認鈕」，殊不知點到的是駭客製造的假按鈕，不知不覺的就將自已的個人資料傳送給駭客。

CSRF

- CSRF 全名是 Cross Site Request Forgery Attack ，這也是跨站攻擊的一種，你是否常常聽到，網路安全人員都會叫別人離開電腦的時候，要記得登出網頁，或是銀行網站常常限制十分鐘內沒有操作，就會自動登出這種討人厭的功能。
- 假設你已經登入 Yahoo 帳號，而這時你又不小心點擊了駭客的連結，進入駭客製作好的網頁 A，這頁面會要求 Browser 去 Yahoo 取得你的會員資料，因為 Browser 認定你已經登入 Yahoo ，所以不會再被導到登入頁面，網頁 A 就能輕易的取得你的個人資料。