Wargame 攻防研究

指導老師：林柏青副教授

組員：吳宗翰、劉興隆、張育恩

摘要

在這個資訊爆炸的時代，人們越來越仰賴網際網路、電腦系統，無論何時何地都身處其中，但在其帶來便利的同時，也漸漸衍生出資訊安全的問題，導致電腦中毒、隱私資料被竊取等問題，因此關於資安的知識越趨重要。

專題內容主要是透過解題與比賽（各大 wargame網站、CTF）的方式來學習，藉由解決在解題目的過程中所遇到的各種困難與認識、學習各式各樣的資訊安問題全知識。

資安領域介紹

Crypto & Steganography

透過某些特別的數學公式、演算法來加密，進而將明文轉換成密文。主要的技巧為了解各題目的加密演算法後，一步步將演算法逆推，最終得到明文。

Software Crack

主要將資訊藏在某個執行檔內，通常需要透過工具來協助解題，如以16進制的方式執行該檔、將該執行檔案的每個動作分解成組合語言等方式。

Web

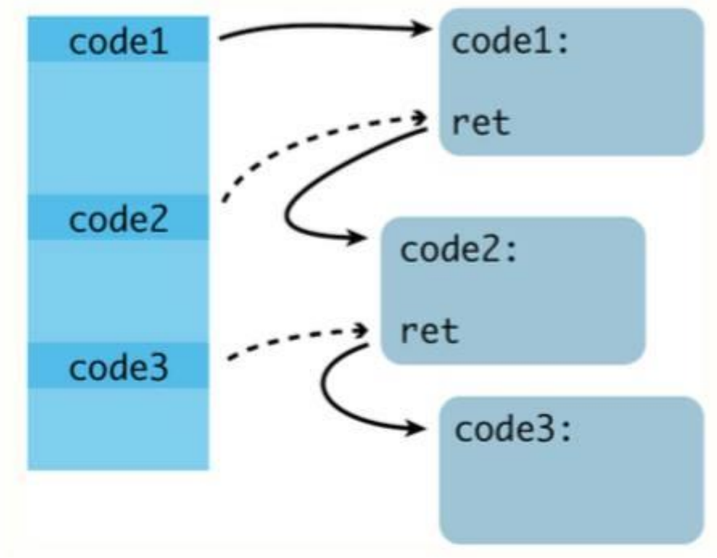
主要是將資訊隱藏在某個頁面，方式為觀察該網頁原始碼、注意各個可以和網站溝通的地方，透過觀察server特定資訊、 SQL injection 、XSS 等方式拿到帳號密碼、權限。

Forensics

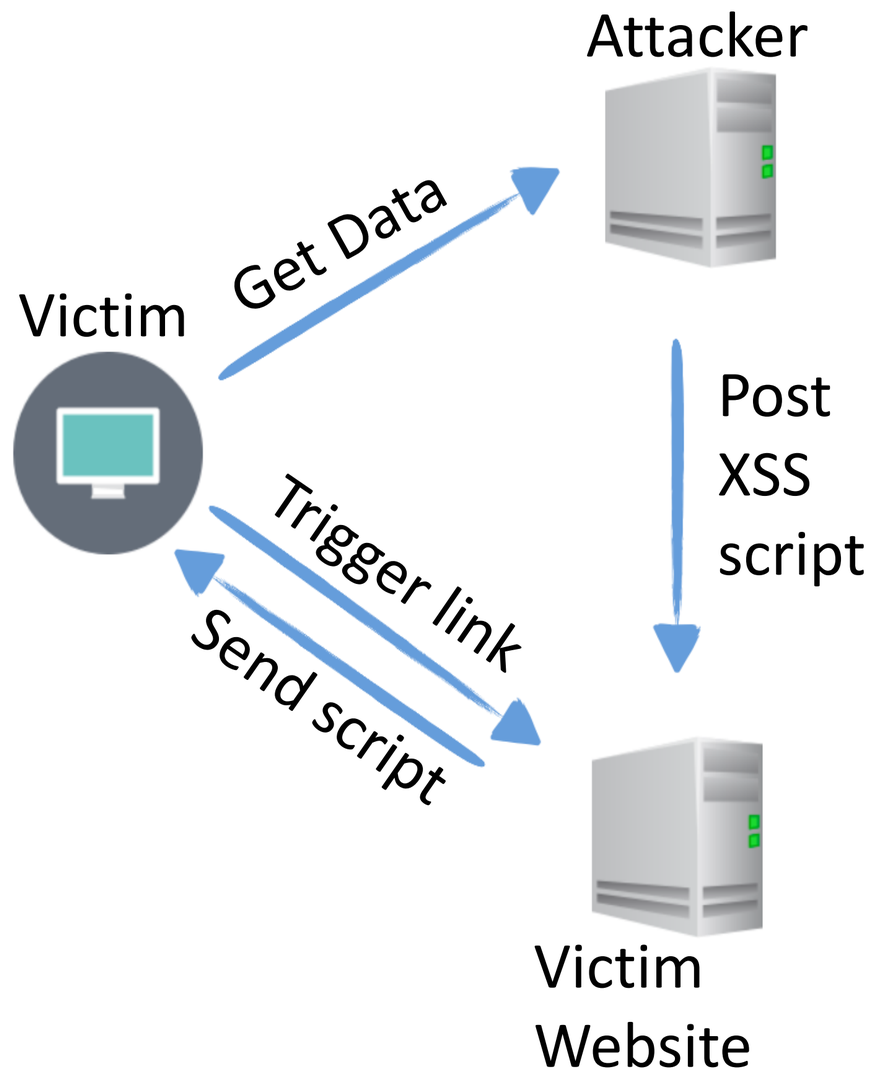
透過工具，分析網路上的封包或是Server 服務的版本或Patch，找到所需要的資訊， 以利之後的攻擊。

主要成果

Return Oriented Programming



XSS & CSRF



RSA Attack

$$n = p * q\ (p, q\ are\ prime)$$
$$\varphi(n) = (p-1) * (q-1)$$
$$Choose\ e\ that\ \gcd(e, \varphi(n)) = 1$$
$$d \equiv e - 1\ (mod\ \varphi(n))$$
$$\therefore\ e * d\ mod\ \varphi(n) = 1$$
$$Pub\_key(e, n), Priv\_key(d, n)$$
$$\therefore M^e\ mod\ n = Cypher$$
$$Cypher^d\ mod\ n = M$$