新北市學校資訊組長增能研習

公開來源情資偵查技術

Open Source Intelligence, OSINT

教資科資安組輔導員 余宗翰 2024.04.23

開始之前

刑法第 358 條

無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

刑法第 360 條

無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

刑法第 361 條

對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

目標：提升校園資訊安全

本日課程大綱

- 概論
- Shodan
- DNSDumpster
- Google Hacking
- 其他資安資源
- 總結

問題：**如何維護**校園資訊安全?

校園資訊安全縱深防禦策略

要求	內容
進階	**威脅獵捕**
中等	組態管理、流量監控
基礎	網路架構

威脅

天災

人禍

有心 / 無意

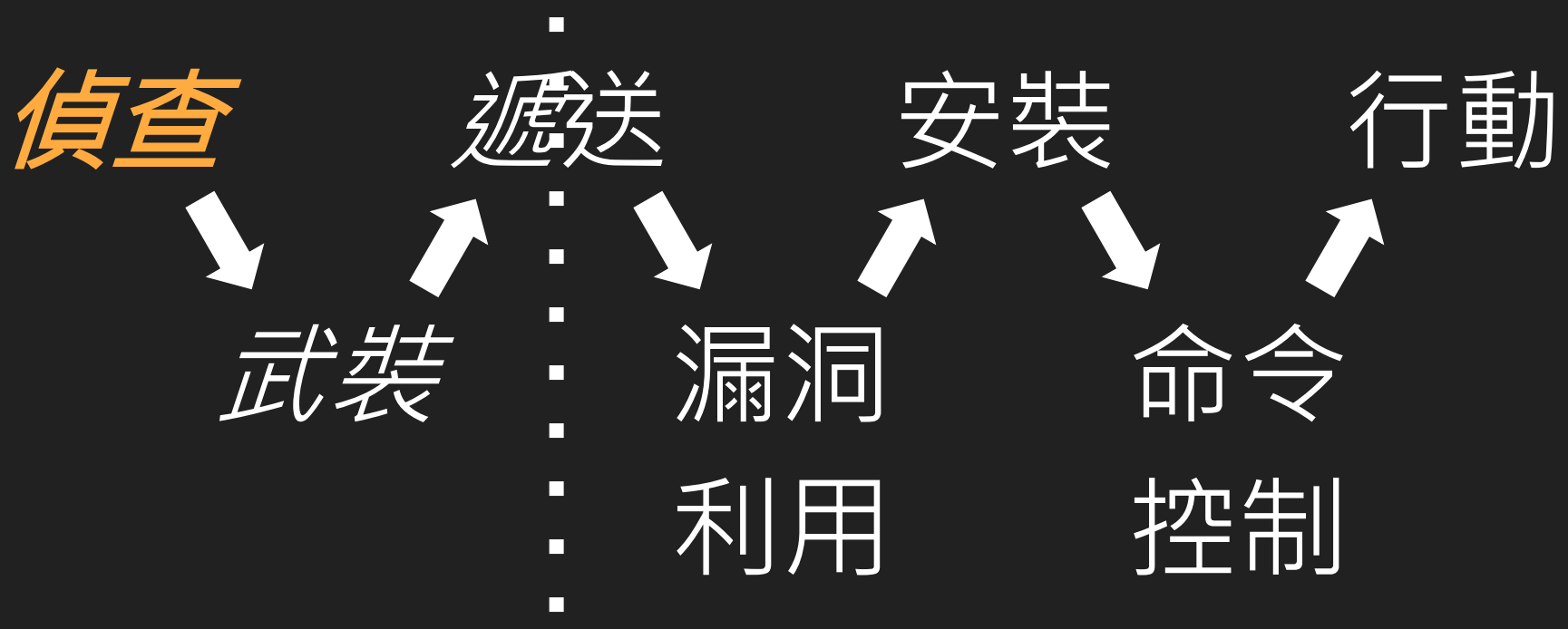
內部 / 外部

問題：駭客如何**挑選目標**並**進行攻擊**

駭客

黑帽	**腳本小子**
白帽	**駭客團隊**
灰帽	**國家資助**

網路攻擊鍊 Cyber Kill Chain



進階補充 MITRE ATT&CK：https://attack.mitre.org

偵查

主動

發起掃描

社交工程

被動

網路情報

明/暗

Lab1.1:
請對目標 **www.google.com**
確認其是否在線上

Lab1.2:
請對目標 ip **8.8.8.8**
確認其是否在線上

命令提示字元：**ping 8.8.8.8**

Lab1.3:
請對目標 ip **192.168.1.10**
確認其是否在線上

命令提示字元：**ping 192.168.1.10**

1.請求

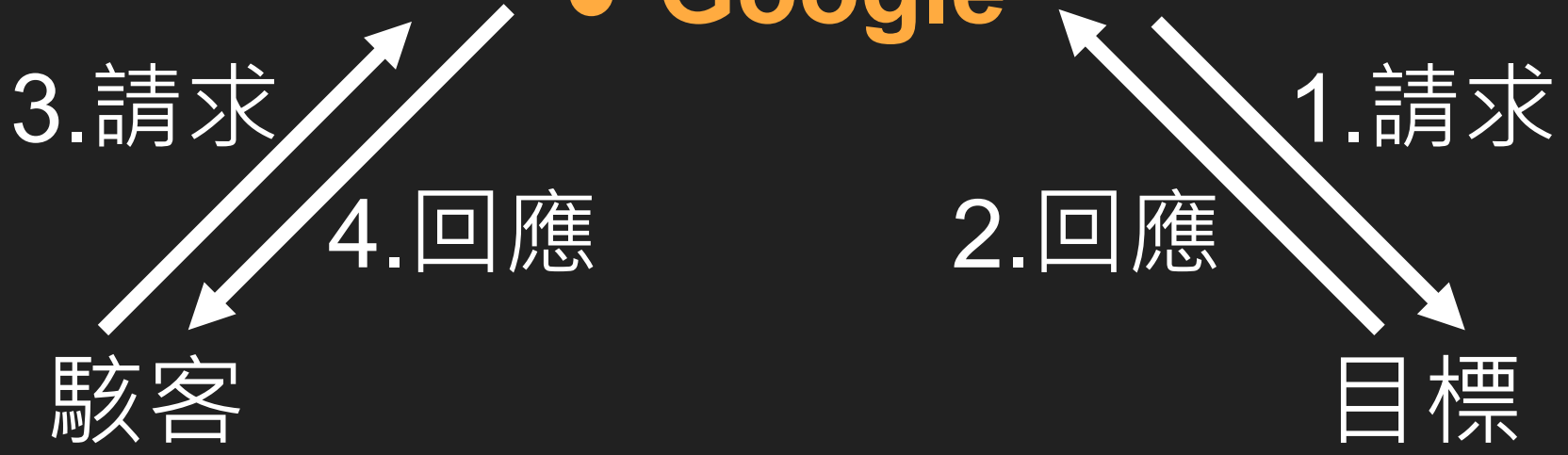
駭客  目標

2.回應

公開來源情資

Open **S**ource **Int**elligence, **OSINT**

- **Shodan**
- **DNSDumpster**
- **Google**



Shodan

Shodan

內容：暴露於**真實ip**之設備資訊

步驟：

1. 連上Shodan：https://www.shodan.io
2. 登入帳號(可用google帳號登入)
3. 單一位址 **真實ip**
4. 整個網段 **net:xxx.xxx.xxx.xxx/xx**
5. 分析
    a. 數量：掌握暴露之設備
    b. 弱點：CVE、port、訊息、時間
    c. 檢查是否屬實
    d. 紀錄後進行修正

Lab2.1:
請連上Shodan後
搜尋 **8.8.8.8**
1. 此服務最後被掃瞄到是**何時**
2. 觀察看看這個位址有無**弱點Vulnerability**
3. 開了哪些**Port**
4. 是否可透過**瀏覽器**存取服務

Lab2.2:

請找出學校官網被分配到的**ip**

找到後再以Shodan搜尋此ip

1. 此服務最後被掃瞄到是**何時**
2. 觀察看看這個位址有無**弱點Vulnerability**
3. 開了哪些**Port**
4. 是否可透過**瀏覽器**存取服務

命令提示字元：**nslookup www.OOO.ntpc.edu.tw**

Lab2.3:
請找出學校被分配到的**真實ip網段**
找到後以google帳號**登入Shodan**搜尋
net:xxx.xxx.xxx.xxx/xx
查出對應網段暴露之結果

Shodan掃描結果(弱點、過度揭露)對應處理方式

建議採行策略**依序**如下

1. **服務關閉下架**
2. 修補弱點或調整組態設定 + 移入內網 + 其他緩解措施
3. 修補弱點或調整組態設定 + 其他緩解措施 + 規劃下架 / 移入內網時程
4. 緩解措施 + 規劃下架 / 移入內網時程(可洽教網諮詢)

※以月為單位持續追蹤

※防火牆代答之處理

Shodan掃描結果(弱點、過度揭露)對應處理方式

- **根治**優先
- 其次**緩解**

DNSDumpster

DNSDumpster

內容：公開之**DNS**(網址與ip對應)資訊

步驟：

1. 連上DNSDumpster：https://dnsdumpster.com
2. 搜尋學校網域
3. 分析
    a. DNS Servers
    b. MX Records
    c. TXT Records
    d. **Host Records (A)** <--- 看這就好

Lab3:
請連上DNSDumpster後
搜尋**學校網域**
如學校官網網址為 www.OOO.ntpc.edu.tw
就輸入 **OOO.ntpc.edu.tw**
1. 檢查**Host Records (A)**有多少不認得的紀錄
2. 觀察網址與ip對應關係

DNSDumpster掃描結果(無提供服務之網站)對應處理方式

建議採行策略**依序**如下

1. **服務關閉下架 + DNS移除對應紀錄**
2. **服務關閉下架**
3. 以月為單位持續追蹤

Google Hacking

Google Hacking

內容：網頁、圖片、影片和其他內容

步驟：

1. 連上google：https://www.google.com
2. 結合**符號和標準運算子**與
   Cloud Search 運算子以及欲搜尋之**關鍵字**
3. 檢視結果

Lab4.1:
請連上google後
搜尋**學校官網**中
是否含有帶關鍵字「**身分證**」之「**excel檔**」

Lab4參考資料(引用 + 修改自 Cloud Search 說明)

Cloud Search 運算子	說明
filetype:	找出網路論壇的內容，或是含有特定副檔名的附件，例如 .doc、.html、.jpeg、.pdf 和 .xlsx。如要尋找 Google 協作平台的內容，請將類型指定為 .html。這個運算子可用於尋找 Google Workspace 的內容。 查詢範例：**關鍵字 filetype:(doc OR pdf)**
site:	找出 Google 協作平台的內容。這個運算子可用於尋找 Google Workspace 的內容。 查詢範例：**關鍵字 site:drive.google.com**

Lab4.2:
請連上google後
參考Lab4.1的模式
搜尋**學校官網**中
是否含有帶關鍵字「**OOO**」之「**OOO檔**」
關鍵字與檔案格式自訂

Google Hacking 搜尋結果(過度揭露)對應處理方式

頁面類：**更新 / 刪除頁面**

檔案類：**刪除檔案**

其他資安資源

結束之前

刑法第 358 條

無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

刑法第 360 條

無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

刑法第 361 條

對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

獵捕威脅

保障安全