



# Penetration Testing Practice

## 滲透測試實務應用

### 01 資訊安全滲透測簡介

孫士勝

Shi-Sheng Sun, Ph.D.

[sssun@nccu.edu.tw](mailto:sssun@nccu.edu.tw)

# 免責聲明

## Disclaimer

- 本課程所教授之滲透測試相關技術僅能於課堂中進行，若有任何超出範圍的動作，皆屬個人行為。  
The penetration testing techniques taught in this course are only to be used within this course. Any actions taken outside of this scope are the sole responsibility of the individual.
- 學員於課後使用任何網路攻擊技術對任何資訊設備進行攻擊，皆屬個人行為。  
Students are solely responsible for any network attacks carried out on any equipment after the course using any network attack techniques.

法規名稱：中華民國刑法 EN

法規類別：行政 > 法務部 > 檢察目

所有條文

編章節

條號查詢

條文檢索

沿革

立法歷程(附帶決議)

※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革

### 第 二 編 分 則

#### 第 三 十 六 章 妨 害 電 腦 使 用 罪

- 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。
- 第 359 條 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- 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。
- 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。
- 第 362 條 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- 第 363 條 第三百五十八條至第三百六十條之罪，須告訴乃論。

# ACM 道德與專業行為準則

## ACM Code of Ethics and Professional Conduct

- 1.1 增進人類社會福祉(Contribute to society and human well-being.)
- 1.2 避免傷害任何人(Avoid harm to others.)
- 1.3 誠實與值得信任(Be honest and trustworthy.)
- 1.4 公平且無犯罪意圖的行動(Be fair and take action not to discriminate.)
- 1.5 尊重智慧財產權(Honor property rights including copyrights and patent.)
- 1.6 維持智慧財產的完整性(Give proper credit for intellectual property.)
- 1.7 尊重他人隱私(Respect the privacy of others.)
- 1.8 遵守保密原則(Honor confidentiality.)



# 課前問券

- 資訊安全滲透測簡介課前問卷
- <https://forms.gle/YGqJDrjUk13YCgzRA>





# 滲透測試目的


- 滲透測試的目的
  - 瞭解可能被利用的途徑
  - 瞭解目前系統與網路的安全強度
  - 明白弱點、強化安全

# 瞭解可能被利用的途徑

- 訊息的不當揭露與竄改
- 網路架構設計不良
- 防火牆設定不良
- 系統及應用程式漏洞
- 系統及應用程式設計不良
- ...

# 瞭解目前系統與網路的安全強度

- 入侵者所需之時間花費之評估
  - ✓ 是否可以在有效時間內取得想要資訊
- 遭受入侵後可能的影響程度之評估
  - ✓ 是否會影響到系統的主控權
- 資通安全政策落實程度之評估



# 明白弱點、強化安全

- 系統與網路安全的強化
  - ✓ 發現系統的弱點及評估其威脅性
- 降低遭受攻擊後所造成的損失



# 滲透測試範疇

- 攻擊途徑**由小到大**可分為:

- ✓ **單一系統**：如提供特定服務的網站，此類多是屬於網站滲透測試。
- ✓ **伺服器**：針對一種或多種服務的特定設備或電腦進行滲透。
- ✓ **區段或主機群(Server farm)**：尋找可以做為跳板的主機，找出潛在漏洞。
- ✓ **全系統**：測試所有相關的資訊系統。
- ✓ **人員安全**：尋找資安意識較低的員工社交工程。
- ✓ **全組織機構**：開放所有資產進行測試，最能貼近與模擬駭客攻擊。

# 滲透測試(Penetration Testing, PT)

- 委託有資安知識與經驗之技術團隊，來**模擬入侵**以測試系統的安全性
- 利用**駭客思維**、工具與技術來測試與驗證受測系統的安全性
- **手動測試**可能比自動測試有較高的準確率，檢測深度也較深

# 滲透測試專案流程



# 確認專案需求與規範(1/2)

- 確認測試**範圍**、**期間**及**時段**。
- 確認測試**方法**或使用**工具**。
- 確認測試**判定條件**。
- 說明滲透期間造成資料損毀的可能性及對應的解決方法。
- 將上述協商做成**滲透測試同意書**與**執行計畫書**。
- 簽署合約取得**合法滲透**授權，避免觸犯法律。

# 確認專案需求與規範(2/2)

- 執行滲透測試作業的方式

- ✓ 黑箱(接近實際的駭客攻擊)

- ✓ 只告知檢測目標，測試者在不知道原始碼的情況下進行測試，可以依照操作手冊進行測試，也可以使用自動化工具進行網站弱點掃描，可由滲透測試者自行發揮，進一步可以模擬真實駭客攻擊。

- ✓ 白箱(考驗系統的安全防護能力)

- ✓ 提供檢測目標的弱點資訊，測試者可在了解程式碼、與功能邏輯的情況下進行測試，直接對原始碼進行掃描尋找漏洞；可以運用於開發時程式碼函示的單元測試，整合測試，也可以運作團隊Code Review機制。

- ✓ 灰箱(無法主動提供完整的受測目標資訊)

- ✓ 灰箱測試為上兩者的混合模式，介於白箱與黑箱測試之間，測試者了解部分程式碼，大概知道特定功能如何運作，不需要像白箱測試需要了解程式、模組的細節，但了解運作機制，能夠用於黑箱測試，以增加弱點發現和錯誤分析的效率。

- ✓ 雙黑箱(對內部人員保密下進行)

- ✓ 又稱雙盲測試。授權方可以在不告知系統維運人員及相關人員之前提下，授權測試方進行合法的攻防演練，測試方盡可能模擬真實駭客攻擊情境，並測試系統維運人員及相關人員的警覺性及應變能力。

- ✓ 雙白箱(協助並確認系統漏洞)

- ✓ 測試者和受測人員都知道對方的存在，目的為協助授權方找出並確認系統漏洞。

# 滲透測試專案流程



# 進行滲透測試

- 資訊蒐集
- 資訊洩密主因
- 網路與主機掃描
- 弱點利用
- 權限跳脫與提升

# 資訊蒐集方式

- 從聊天、報章雜誌等傳統管道蒐集資料
- 從網路上蒐集受測目標的相關訊息(如網域名稱及網址)
  - ✓ Google Hacking
  - ✓ Whois
  - ✓ 網站下可下載之文件
  - ✓ 各類人肉搜索方式





# Google Hacking

- **Google Hacking**是一種利用google搜尋引擎尋找安全漏洞的技術，透過進階的搜尋指令查找符合特定字串的結果。
- 關鍵字
  - ✓ 搜尋相關內容
  - ✓ 相關度

# 網頁基本架構



網址: url

www.sundaymore.com › tag › 髮型 ▼

2020人熱髮型推介！女生中長髮短髮造型特輯| SundayMore ...

選擇適合自己臉型的髮型是增加個人魅力的重要一環，無論你是曲髮直髮的女生，只要透過簡易編髮技巧、美髮產品、頭髮飾物就可以打造出令人眼前一亮的形象。

髮型 · 女生中長髮短髮造型特輯 · 3大秋冬短髮造型2020：耳下 ... · 髮色

標題: title

style-map.com › ranking

2020網友熱推！最新潮流時尚髮型| StyleMap 美配

煩惱髮型嗎？集結全港最多最優質的美髮設計師，萬張髮型作品任你挑！多種風格髮型實拍及精選髮型設計師、髮廊推薦。快來收藏髮型靈感、分享喜愛的髮型作品 ...

www.harpersbazaar.com › beauty › hair ▼

完美髮型| 哈潑時尚Harper's BAZAAR Taiwan

完美髮型. 精選5大不挑臉型韓系「鎖骨短髮、C字短髮」推薦！短髮、中短髮過渡期長度也不尷尬. 不挑臉型的短髮範本都幫你整理好了！By Zoey Lee. 2020秋冬 ...

內容: text

## 📰 焦點新聞

2020秋冬「鎖骨捲髮」髮型範本！《后翼棄兵》復古捲髮正夯，中短髮&微捲度撩人無敵！

BEAUTY美人圈 · 23 小時前



髮型 | 大熱韓系瀏海：低調觸角染輕鬆減齡、耳邊瀏海打造V臉

香港01 · 9 小時前



# Google Hacking 常用語法

- **inurl**:在url中是否存在該關鍵字
- **intext**:搜索網頁正文內容
- **intitle**:在網頁標題中搜索關鍵字
- **site**:test.com 搜索該網站及其host或url
- **filetype**:獲取目標的文件類型
  - filetype : doc|docx|pdf 將返回所有以doc、docx、pdf結尾的文件URL
- **link**:返回所有與目標url做鏈接的url。如搜索：link:www.test.com則可返回所有和www.test.com 有連結的url
- **cache**:搜索google關於某些內容的頁庫存檔
  - <https://webcache.googleusercontent.com/search?q=cache:test.com>
  - 「頁庫存檔」功能悄悄移除，Google 不再備份整個網路[1]
  - Bing表示...

[1] “「頁庫存檔」功能悄悄移除，Google 不再備份整個網路,” 科技新報, 2024.02.05,  
<https://technews.tw/2024/02/05/we-do-not-see-any-cache-links-in-google-search/>



# Google Hacking 語法之例子

- **inurl**:在url中是否存在該關鍵字
  - inurl:指甲美容 inurl:髮型
- **intext**:搜索網頁正文內容
  - intext:指甲美容 intext:髮型
- **intitle**:在網頁標題中搜索關鍵字
  - intitle:指甲美容 intext:髮型

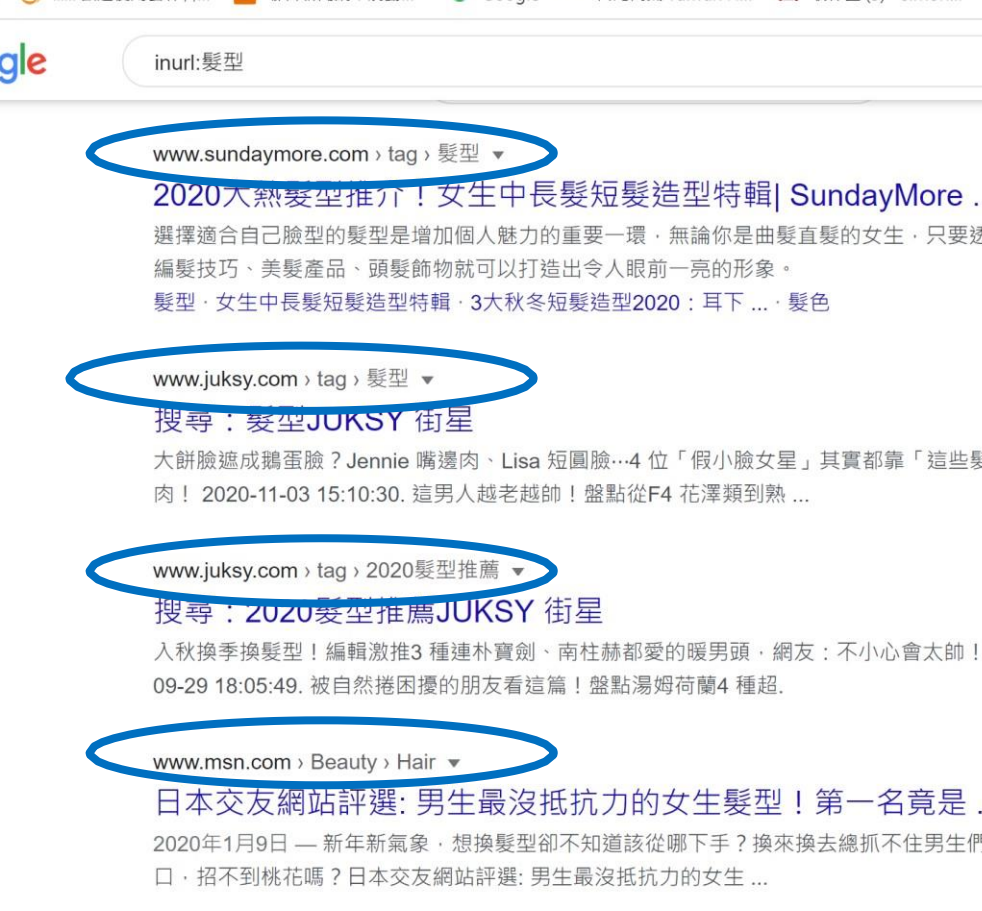


# Google Hacking 的語法(1/6)

- **inurl**:在url中是否存在該關鍵字
  - inurl:指甲美容    inurl:髮型



Department of Computer Science  
National Chengchi University



inurl:髮型 - Google 搜尋

google.com/search?q=inurl%3A髮型&oq=inurl%3A髮型&aqs=chrome..69i57j69i58.1065j0j7&sourceid=chrome&i

應用程式 歡迎使用雲林科... 聯合新聞網：觸動... Google 台灣高鐵 Taiwan H... 收件匣 (3) - simon... www.schprs.

Google inurl:髮型

www.sundaymore.com › tag › 髮型 ▼

2020大熱髮型推介！女生中長髮短髮造型特輯| SundayMore ...

選擇適合自己臉型的髮型是增加個人魅力的重要一環，無論你是曲髮直髮的女生，只要透過簡易編髮技巧、美髮產品、頭髮飾物就可以打造出令人眼前一亮的形象。

髮型 · 女生中長髮短髮造型特輯 · 3大秋冬短髮造型2020：耳下 ... · 髮色

www.juksy.com › tag › 髮型 ▼

搜尋：髮型JUKSY 街星

大餅臉遮成鵝蛋臉？Jennie 嘴邊肉、Lisa 短圓臉...4 位「假小臉女星」其實都靠「這些髮型」藏肉！ 2020-11-03 15:10:30. 這男人越老越帥！盤點從F4 花澤類到熟 ...

www.juksy.com › tag › 2020髮型推薦 ▼

搜尋：2020髮型推薦JUKSY 街星

入秋換季換髮型！編輯激推3 種連朴寶劍、南柱赫都愛的暖男頭，網友：不小心會太帥！ 2020-09-29 18:05:49. 被自然捲困擾的朋友看這篇！盤點湯姆荷蘭4 種超.

www.msn.com › Beauty › Hair ▼

日本交友網站評選: 男生最沒抵抗力的女生髮型！第一名竟是 ...

2020年1月9日 — 新年新氣象，想換髮型卻不知道該從哪下手？換來換去總抓不住男生們的胃口，招不到桃花嗎？日本交友網站評選: 男生最沒抵抗力的女生 ...

zh.100ke.info › wiki › 髮型 ▼

发型- 维基百科，自由的百科全书

髮型指頭髮的修剪、整形，或戴上裝飾品所整理的頭髮型式。通常为了审美、宗教、社交、职业



# Google Hacking 的語法(3/6)

- **inurl**:在url中是否存在該關鍵字
  - inurl:指甲美容    inurl:髮型
- **intext**:搜索網頁正文內容
  - intext:指甲美容    intext:髮型









# Google Hacking 的語法(5/6)

- **inurl**:在url中是否存在該關鍵字
  - inurl:指甲美容    inurl:髮型
- **intext**:搜索網頁正文內容
  - intext:指甲美容    intext:髮型
- **intitle**:在網頁標題中搜索關鍵字
  - intitle:指甲美容    intext:髮型

# Google Hacking 的intitle 語法(6/6)

intitle:指甲美容 - Google 搜尋

google.com/search?xsrf=AleKk01ZK7s7qkU\_mXTCYINCFNhHfTZDFw%3A1605444462662&ei=biOxX-H1J8uzn

intitle:指甲美容

trouble-care.com › 美甲, 指甲修護

**指甲美容師的美甲注意事項!! 牢記6點健康指甲守則| 妳的煩惱 ...**  
妳在剪指甲的時候是否有些特殊習慣? 從小就習慣剪短短的指甲, 沒剪反而不習慣? 剪太長之後還要很長修剪, 為了省 ...  
2017年12月27日 · 上傳者: 霸氣冠哥Kay

shopee.tw › search › keyword=指甲美容組

**指甲美容組- 優惠推薦- 2019年12月|蝦皮購物台灣**  
你想要找的指甲美容組- 網路人氣推薦商品就來蝦皮購物, 買指甲美容組- 商品來蝦皮台灣享超低折扣優惠與運費補助, 提供賣家評價與100%蝦皮承諾保障!

www.hellotoby.com › 臺灣 › 美容

**2020台灣最佳指甲美容推薦! Toby - HelloToby**  
只需回答幾條問題讓Toby了解妳指甲美容的需求, 讓我們為您從台北指甲美容服務中尋找配對, 再由指甲美容專家向您免費報價。指甲美容包括: 美容師、指甲 ...  
★★★★★ 評分: 5 · 92 則評論

www.nails.com.tw

**Nails 指甲彩繪美容保養全球資訊網- 美甲美容美睫紋繡用品專賣店**  
Nails 指甲彩繪美容保養全球資訊網- 美甲美容美睫紋繡用品專賣店。

www.naillabotw.com › product

**SpaLuce 指甲美容液Plus10ml - Nail Labo**  
Future Nail 直接可見監製產品指甲想要健康, 周遭的皮膚狀態也很重要! 由日本指甲專門科醫生- 東禹彥所監製的 ...  
2019年12月10日 · 上傳者: Future Nail School & Sales フューチャーネイルスクール&サロン

intitle:髮型 - Google 搜尋

google.com/search?xsrf=AleKk03yJs4pzOiWtM4FSqBvAlxoRTbylg%3A1605444913870&ei=MSWxX\_LoNkaFr7wPgrC3

intitle:髮型

Google 搜尋

www.sundaymore.com › tag › 髮型

**2020大熱髮型推介! 女生中長髮短髮造型特輯| SundayMore ...**  
選擇適合自己臉型的髮型是增加個人魅力的重要一環, 無論你是曲髮直髮的女生, 只要透過簡易編髮技巧、美髮產品、頭髮飾物就可以打造出令人眼前一亮的形象。  
髮型 · 女生中長髮短髮造型特輯 · 3大秋冬短髮造型2020: 耳下 ... · 髮色

style-map.com › ranking

**2020網友熱推! 最新潮流時尚髮型| StyleMap 美配**  
煩惱髮型嗎? 集結全台最多最優質的美髮設計師, 萬張髮型作品任你挑! 多種風格髮型實拍及精選髮型設計師、髮廊推薦。快來收藏髮型靈感、分享喜愛的髮型作品 ...

焦點新聞

2020秋冬「鎖骨捲髮」髮型範本! 《后翼棄兵》復古捲髮正夯, 中短髮&微捲度撩人無敵!  
beauty美人圈 · 22 小時前

17歲加日混血正妹宛如洋娃娃 新髮型亮相網友心動: 一見鍾情!  
UDN 聯合新聞網 · 2 天前

全部顯示

www.harpersbazaar.com › beauty › hair

**完美髮型| 哈潑時尚| harper's BAZAAR Taiwan**

# Google Hacking 之site語法



Google

"政治大學" site:edu.tw filetype:xlsx OR filetype:docx

新聞 圖片 影片 地圖 購物 書籍 航班 財經

約有 4,930 項結果 (搜尋時間：0.26 秒)

 nccu.edu.tw  
https://acc.nccu.edu.tw › QP-A00-01-01(11107) DOC

[國立政治大學](#)

國立政治大學. 產學合作計畫經費結案通知單. 填表日期: 年 月 日. 計畫代碼. 計畫編號. 計畫名稱. 計畫主持人. 核定金額(元). 實支金額(元). 結餘金額(元). (核定金額-實支 ...

 nccu.edu.tw  
https://www.alumni.nccu.edu.tw › uploads › 國... DOC

[國立政治大學校友個資事項告知暨使用同意書](#)

... 政治大學(以下簡稱本校)執行校友服務相關業務. 本校將遵守中華民國「個人資料保護法」與相關法令之規範, 蒐集、處理及利用個人資料, 以維護您的權益。 國立政治大學 ...

 nccu.edu.tw  
https://acc.nccu.edu.tw › sites › default › files DOC

[國立政治大學校務基金管理委員會第屆第次會議提案單](#)

國立政治大學校務基金管理委員會第屆第次會議. 提案單. 提案單位(人): 主管: (簽章). 提案連署人: 承辦人員: (簽章). 分機: . 案由: . 說明: . 辦法: . 附件 ...

 nccu.edu.tw  
https://tiipm.nccu.edu.tw › 考生學經歷審核表 DOC

[國立政治大學資訊科學學系](#)

國立政治大學科管智財所蒐集個人資料同意書暨考生資料正確性聲明. 本人獲知並瞭解貴所因112學年度博士班甄試事由向本人索取以上所填資料, 並同意貴所於此目的之必要範圍 ...

- 利用google查詢網址中包含 edu.tw 裡的 xlsx, docx 檔案搜尋結果，並強制需有「政治大學」字串
- 根據輸入的指令不同可以查找出需多不同的結果



# More about Google Hacking

- 可參考 1000 Best Google Dorks List (Google Hacking Guide) – 2024
  - <https://gbhackers.com/latest-google-dorks-list/>
- 未來課程投影片將有延伸舉例

# whois

- WHOIS (whois)是用來查詢網際網路中域名的IP以及所有者等資訊的傳輸協定。
- 現在出現了一些基於網頁介面的簡化線上查詢工具，甚至可以一次向不同的資料庫查詢。
- 網頁介面的查詢工具仍然依賴WHOIS協定向伺服器傳送查詢請求，command line下的whois工具仍然被系統管理員廣泛使用。

# whois

- 透過**whois**查詢網域(Domain Name)名稱的基本訊息，在滲透測試中，網域名稱的註冊資訊、管理員與Email、內部的DNS伺服器清單是較需要的。



# whois

- 指令： `whois options IP`
- 語法說明
  - ✓ `-h host`：指定網域名稱解析伺服器，預設透過 `whois.networksolutions.com` 或是 `whois.arin.net` 來進行解析。
  - ✓ `-p POST`：預設為43，可以透過指令指定要連接的port。

# whois

- 範例：whois nccu.edu.tw

```
[ ][/home/sssun] whois nccu.edu.tw
Ministry of Education Computer Center
  12th Fl, 106, Heping E. Road, Sec 2.
  Taiwan Republic of China, R.O.C
  TW

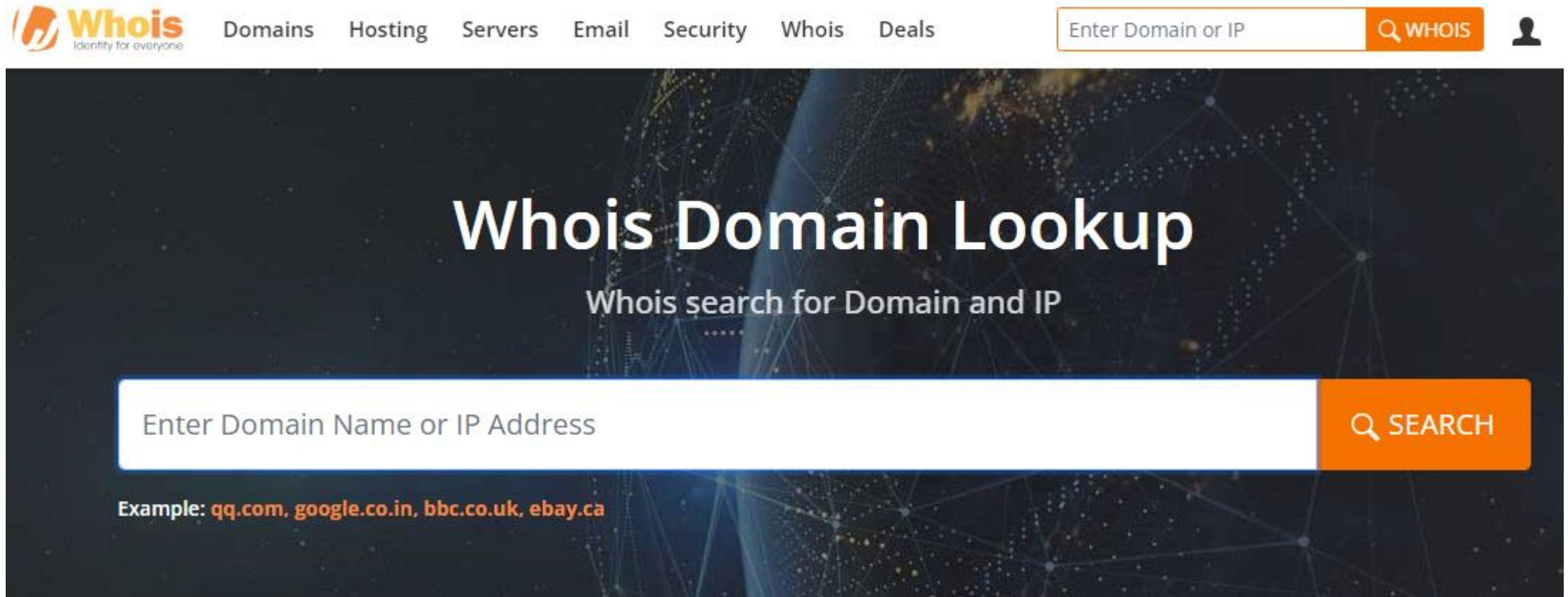
Domain Name: edu.tw

Contact:
  TANet, Administrator  tanetadm@moe.edu.tw
  886-2-77129008
```



# whois(WEB)

- 網址：<https://www.whois.com/whois/>



The screenshot shows the homepage of the Whois Domain Lookup service. At the top, there is a navigation bar with the Whois logo (tagline: 'Identity for everyone') and links for Domains, Hosting, Servers, Email, Security, Whois, and Deals. A search bar in the top right corner contains the text 'Enter Domain or IP' and a 'WHOIS' button. The main content area features a large, dark background with a network diagram. The title 'Whois Domain Lookup' is prominently displayed in white, followed by the subtitle 'Whois search for Domain and IP'. Below this, there is a large white search input field with the placeholder text 'Enter Domain Name or IP Address' and an orange 'SEARCH' button. At the bottom of the main area, an example is provided: 'Example: qq.com, google.co.in, bbc.co.uk, ebay.ca'.

# whois(WEB)



Domains Hosting Servers Email Security Whois Deals

Enter Dom

google.com

Updated 18 hours ago ↻



## Domain Information

Domain:	google.com
Registrar:	MarkMonitor Inc.
Registered On:	1997-09-15
Expires On:	2028-09-13
Updated On:	2019-09-09
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com



## Registrant Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/google.com">https://domains.markmonitor.com/whois/google.com</a>



## Administrative Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/google.com">https://domains.markmonitor.com/whois/google.com</a>



## Technical Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/google.com">https://domains.markmonitor.com/whois/google.com</a>

## Raw Whois Data

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns4.google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-02-18T07:27:26+0000 <<<
```

For more information on WHOIS status codes, please visit:  
<https://www.icann.org/resources/pages/epp-status-codes>

# 資訊洩密主因

- DEVCORE(戴夫寇爾)分析出從過往的滲透經驗中，有幾個是常見的資訊洩密的問題，分別為：
  - 管理介面洩漏
  - 目錄(Index of)洩漏
  - 錯誤訊息洩漏
  - 暫存、測試資訊
  - 版本控管
  - DNS資訊洩漏

# 網路與主機掃描

- 又稱為**弱點評估**
- 嘗試掃描受測目標，以取得以下資訊
  - 連接埠列表: port numbers
  - 使用什麼作業系統: 如Window, Linux, DOS
  - 網路應用程式名稱與版本: 如Bind 9.0
  - 是否存在已知的弱點: 如 SQL

# Scanning(掃描)

- 藉由掃描可以取得特定的IP、作業系統、網路和主機系統架構以及主機上所開啟的服務等等
- 掃描首先搜尋目標主機網路上可以連接到的主機，然後利用這些資訊來查出主機開啟哪些通訊埠(連接埠)，並且進一步偵測目標主機上所利用的作業系統類型和版本
- 掃描大概分為三類型
  - 通訊埠(連接埠)掃描
  - 網路架構掃描
  - 弱點掃描

# 網路掃描工具介紹

- 目前較為常見的網路掃描工具有Nmap、Saint、ISS、Cybercop Scanner、Advanced IP Scanner
- 目前被廣泛使用的網路掃描工具為Nmap，現有以圖形介面所開發的Zenmap，可在Windows系統下使用

# Nmap

- Nmap全名是Network Mapper，是由Gordon Lyon (aka his pseudonym: Fyodor Vaskovich)所開發的一套開放原始碼軟體。
- 可用於檢測本機或網路遠端主機的安全性弱點
- 主要功能是針對來源主機/網段作掃瞄
  - ✓ 目標主機所開放的TCP埠
  - ✓ 取得對應的網路服務類型
  - ✓ 應用軟體名稱與版本
- 可偵測出目標主機所使用的作業系統、封包過濾器及防火牆種類等資訊。
- 若要在windows下使用時，可利用圖形介面的Zenmap。

# Nmap操作簡介

- nmap -help 或 man nmap

```
[root@localhost ~]# nmap -help
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sl <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

```
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<nl=v1[,n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
    probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1[,url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
```



# Nmap操作簡介

```
[root@localhost ~]# nmap -sT localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-26 11:26 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000071s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
587/tcp   open  submission
726/tcp   open  unknown
783/tcp   open  spamassassin
993/tcp   open  imaps
995/tcp   open  pop3s
1723/tcp  open  pptp
2049/tcp  open  nfs
10024/tcp open  unknown
10025/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 19.32 seconds
```

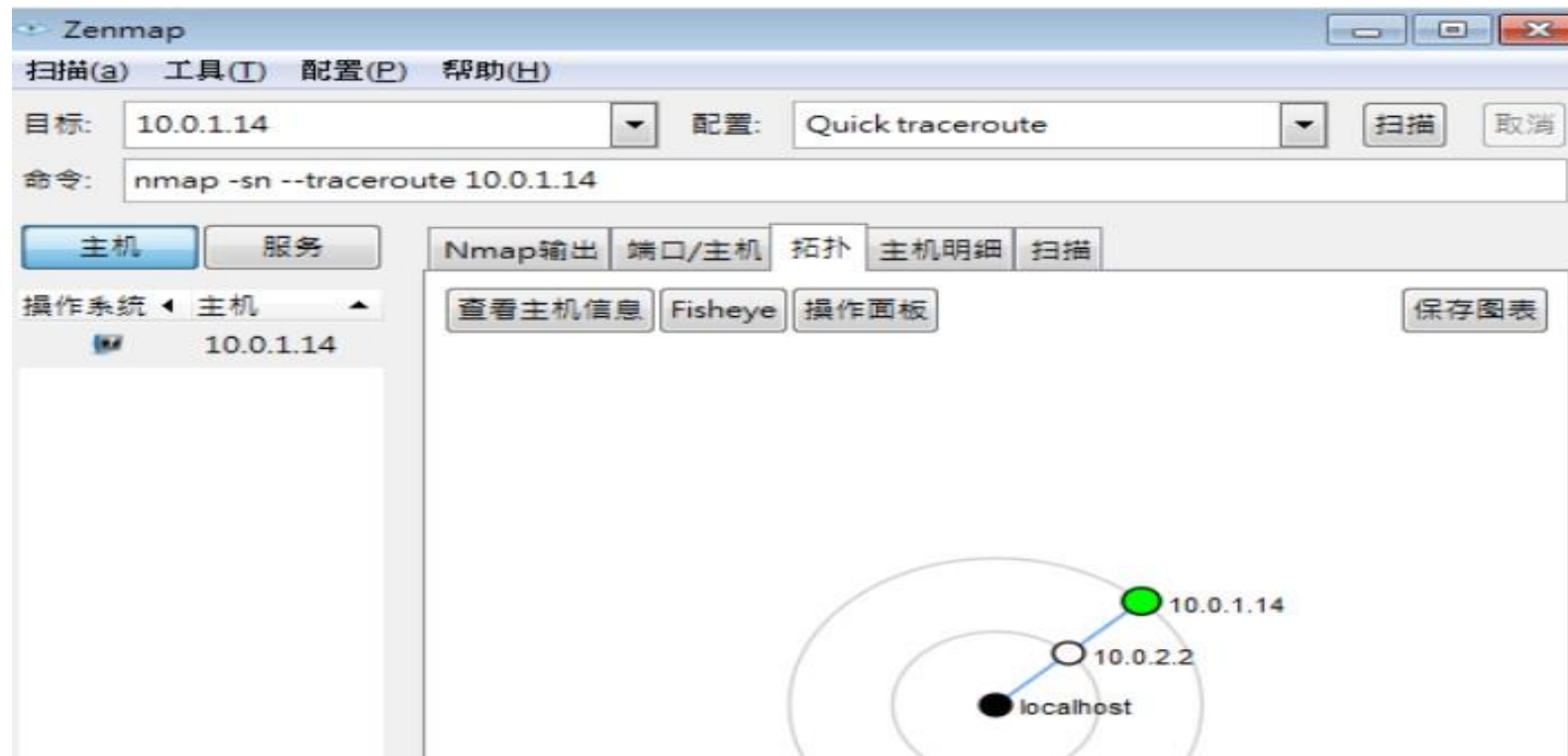
# Nmap操作簡介

- 內建有Ping Scan 可以用來確認目標主機是否為開啟狀態
- 且也可以設定特殊網路: ex:192.168.1.0/24



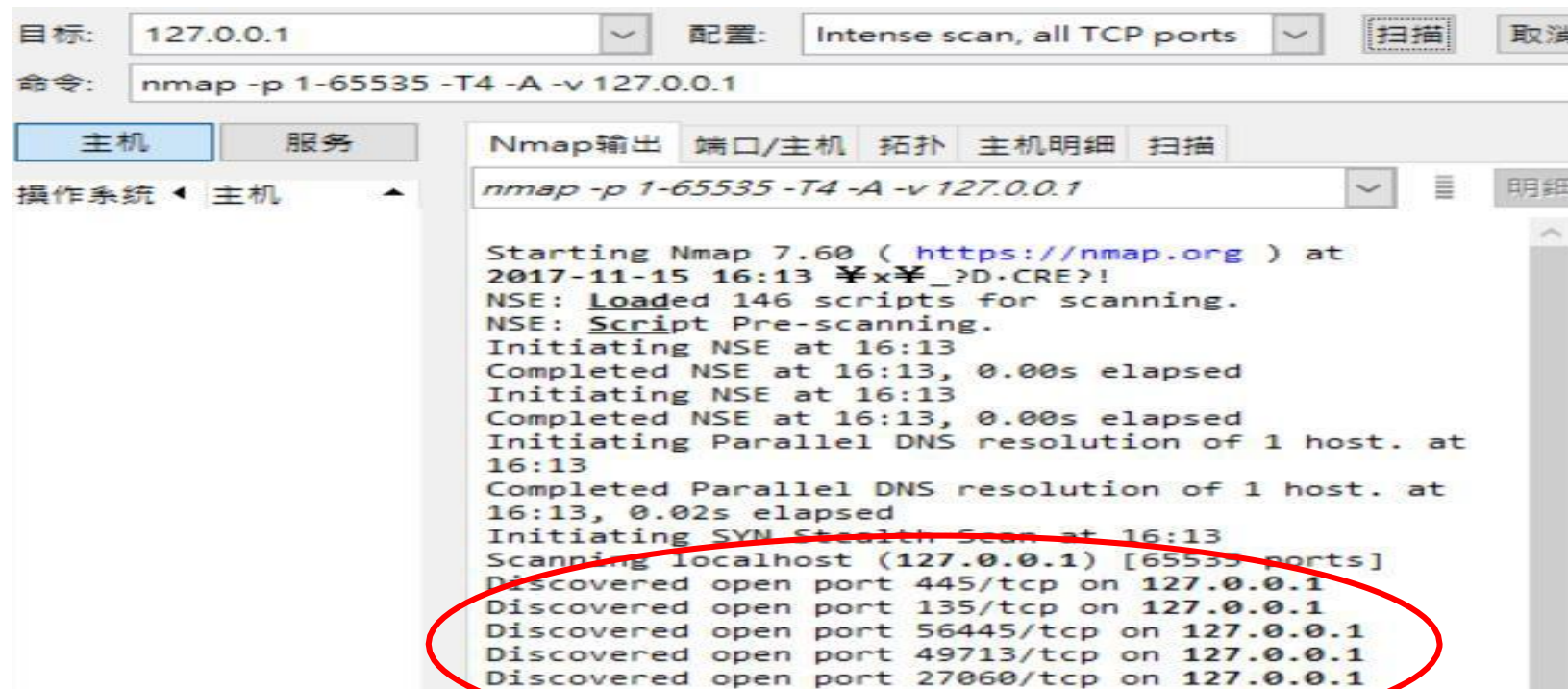
# Nmap操作簡介

- Traceroute 掃描可以看到目標主機經過哪些網路設備，且可產生簡易圖形拓樸給使用者觀看。



# Nmap操作簡介

- Port Scan 可以針對主機做port掃描，得到目標主機所開放的port資訊，並列出所該port所對應的網路服務類型和軟體版本之類的資訊



The screenshot shows the Nmap GUI interface. The target is set to 127.0.0.1 and the configuration is 'Intense scan, all TCP ports'. The command entered is 'nmap -p 1-65535 -T4 -A -v 127.0.0.1'. The output window shows the scan results, with the discovered open ports circled in red:

```
nmap -p 1-65535 -T4 -A -v 127.0.0.1

Starting Nmap 7.60 ( https://nmap.org ) at
2017-11-15 16:13 𐀀x𐀀_?D.CRE?!
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at
16:13
Completed Parallel DNS resolution of 1 host. at
16:13, 0.02s elapsed
Initiating SYN Stealth Scan at 16:13
Scanning localhost (127.0.0.1) [65535 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 56445/tcp on 127.0.0.1
Discovered open port 49713/tcp on 127.0.0.1
Discovered open port 27060/tcp on 127.0.0.1
```

# 弱點利用(1/2)

- 測試應用軟體漏洞、網站邏輯漏洞、作業系統漏洞、密碼破解等項目
- 為什麼要對弱點進行驗證？
  - 排除誤判的可能性
  - 證明該弱點是會造成威脅
  - 檢測是否可以利用該弱點提升權限
  - 檢測橫向攻擊可能性

# 弱點利用(2/2)

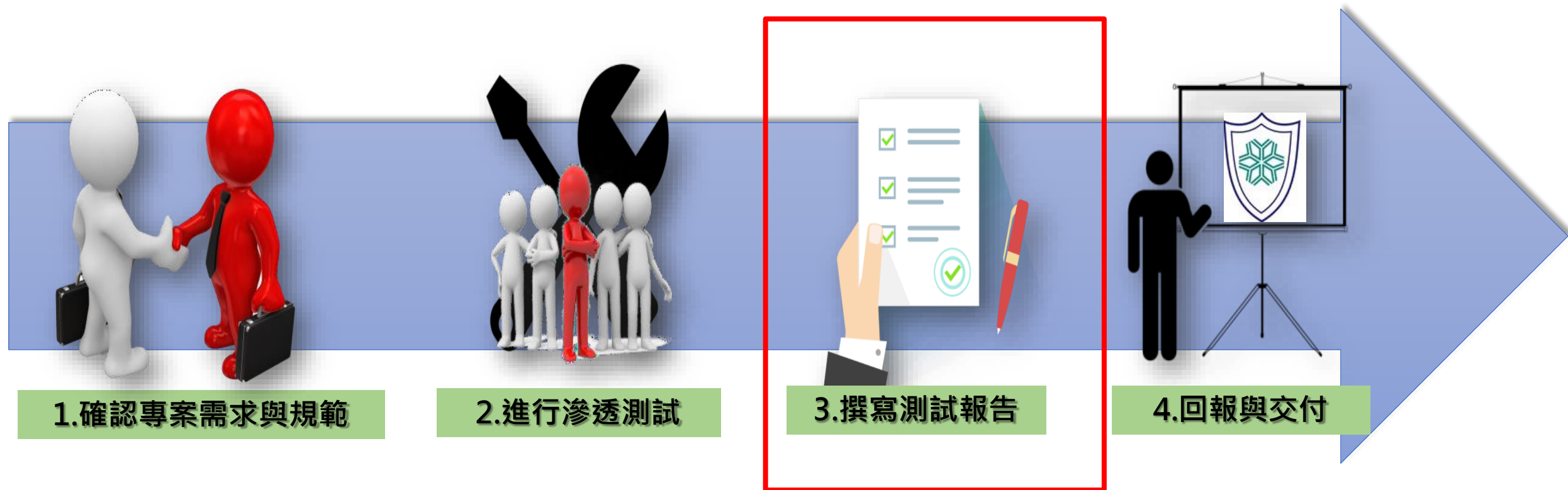
- 滲透測試的手法或工具與駭客攻擊沒有太大差異，因此在進行測試時必須預先擬定好對系統造成影響的對策。
  - 造成應用程式無法回應或嚴重延遲
  - 造成系統上當機
  - 資料或資料庫內容遭受損毀
  - 第三方順著測試時開啟的通道進入



# 權限跳脫與提升

- 取得了伺服器權限後，嘗試獲取伺服器最高root/admin權限，或是滲透內網其他伺服器。

# 滲透測試專案流程





# 撰寫測試報告

- 測試結束後須撰寫一份報告書，內容須詳列：
  - 摘要(整體風險與弱點整理)
  - 測試過程紀錄(測試範圍、測試工具、風險定義)
  - 所有弱點與其會造成的影響(需有截圖證明)
  - 弱點之進入點
  - 若為誤判也應詳細說明無法達成滲透的測試步驟
  - 風險等級及修補方式

# 滲透測試專案流程





# 回報與交付

- 針對測試結果進行過程與結果的報告，並提出修復與保護的建議，最後將文件交付，結束專案。



# 滲透測試報告撰寫(Reporting)

- 報告格式內容順序為：
- 摘要
- 簡介
- 執行過程
- 執行結果
  - 高/中/低風險
- 結論

# 滲透測試報告撰寫(Reporting)

- 透過報告可以讓對方知道你做了什麼測試
- 不能只是弱點掃描報告
  - 檢視所有弱點與其造成的影響
  - 排定修補順序
  - 視情況調整弱點的風險等級

# 撰寫測試報告(範例)

測試名稱

...

影響範圍

...

測試工具

...

測試結果(畫面)

...

發生概率

...

嚴重性評估

...

防護建議

...

參考資料

...

說明影響那些產品與範圍

該項是由那些工具進行測試的

附上測試截圖以證明結果

低/中/高來評估，並簡單描述

低/中/高來評估，並簡單描述

針對危險提供防護的建議

提供參考資料



# 相關網路安全訊息來源

- CVE, Common Vulnerabilities and Exposures
- 趨勢科技全球技術支援與研發中心-資安趨勢部落格
- TANet CERT台灣學術網路危機處理中心
- iThome資安日報
- HITCON ZeroDay漏洞通報平台



# 課後問券

- 資訊安全滲透測簡介課後問卷
- <https://forms.gle/Sxwhw9TtKxrkc8XZ8>





# Reference Materials

- Thanks to 「教育部資訊安全人才培育計畫」 & 「國網中心雲端資安攻防平臺（Cyber Defense eXercise，CDX）」



Q & A