企業資安職能地圖 - 資安人才規劃與培訓

張智凱、陳仲寬、卓政逸

Outline

- 駭客、學術及產業間的資安落差
- 資安職能地圖
- 亥客書院經驗分享及數據統計
- 攻防平台設計
- 資安技術能力評量

Outline

- 駭客、學術及產業間的資安落差
- 資安職能地圖
- 亥客書院經驗分享及數據統計
- 攻防平台設計
- 資安技術能力評量

駭客、學術及產業間的資安落差

- **各領域對資安發展之方向及目標不同**
  - 駭客文化 – 追求技術之卓越。
  - 學術慣例 – 化複雜技術為系統性的教材。
  - 產業通則 – 投資必須要有明確的目標，最好短期就有具體效益。
- **產業現況**
  - 由於產業發展脈絡使然，一般產業較缺乏專職資安人員。
  - 現有資訊人員缺乏資安相關技術基底。
  - 不易說服高層投入經費於資安工作。
  - 講求效益，偏好現有工具應用與資安自動化。
  - 相較於學術教材或技術文件，更需要有系統的實務培訓課程。

資安培訓角色規劃

- 透過學術圈的培訓經驗與基礎建設，引介駭客圈的頂尖技術，協助解決產業界資安培訓問題。

Outline

- 駭客、學術及產業間的資安落差
- 資安職能地圖
- 亥客書院經驗分享及數據統計
- 攻防平台設計
- 資安技術能力評量

資安職能規劃

- **企業資安三問：**
  - **一家企業必須具備怎樣的資安人才？**
    - 規劃企業專屬職能地圖 -> 依據職能地圖規劃人才需求
  - **如何培養這些資安人才？**
    - 資安課程設計 -> 針對不同職能，設計資安學程
    - 資安攻防平台 -> 教學重點，讓學員進行實作練習
  - **如何知道資安人才是否已具備足夠的技術？**
    - 資安能力評量 -> 以實作題為導向，測試學員資安實戰技能

資安職能地圖

- 資安技術演進快速包羅萬象，並無單一套技能適合所有的資安人員
- 資安技能可以從兩個不同的維度進行分類

工作內容	技術領域
• 政策管理設計職 • 系統設計及佈建職 • 系統維運職 • 系統檢測職	• 威脅情資 • 資料保護 • 認證與稽核 • 可靠性與可用性

職能地圖

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測 – 惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測 – 阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 系統權限提升 網路權限提升	阻斷式攻擊

針對不同規模的資安人力建議

- **大型公司**
  - 必須有CISO(資安長)辦公室，負責整體制度設計(橫軸)。
  - 核心縱軸成立工作團隊 (如：雲端儲存公司必須有資料保護team、可靠性及可用性team...)。
  - 特定縱軸或橫軸外包 (如：縱軸-威脅情資分析，或橫軸-滲透測試委外)。
- **中型公司**
  - 可成立CISO(資安長)辦公室。
  - 或由CIO(資訊長)辦公室兼任，下設一級資安部門。
  - 由資安部門主導制度設計，成立橫軸-營運維護team。
  - 橫軸-系統設計與實做、與橫軸-滲透測試可委外。
- **一人資安**
  - 延攬較具宏觀資安視野的人材負責規劃與營運兩橫軸，其餘技術項目委外。

針對不同規模的資安人力建議

- 一人資安
  - 延攬較具宏觀資安視野的人材負責規劃與營運兩橫軸，其餘技術項目委外。
  - 規劃佛學、禪修、冥想、祝禱等課程，以強化資安人員之心理素質及通靈能力。

圖片來源：Created by Freepik

職能地圖

			靠性及可用性
			基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
	全性資訊與事件管 日誌整合系統 情資交換系統	實作 統建置 統建置 護建置	統建置 置 設建置	可容錯 網路
運維護	情資分析 數位鑑識 事件應變 網路流量分析 程式、漏洞攻 惡意程式分析	維運 理 統維運 統維運 護維運	管理 入侵偵測監 使用者行為監控 權限稽核 公開金鑰基礎建設維	測 – 阻斷 防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	漏洞 碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 系統權限提升 網路權限提升	

圖片來源(右至左)： Created by Freepik 、Created by Yurlick - Freepik.com、Created by Dooder - Freepik.com

職能與課程規劃

- **專業資安職能分類**
  - 政策管理設計職
  - 系統設計及佈建職
  - 系統維運職
  - 系統檢測職
- **學程單位設計**
  - 以技術領域為單位 (表格縱軸)
  - 以資安工作內容為單位 (表格橫軸)
  - 以相近區塊為單位 (表格區塊)

職能地圖 - 培訓學程

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測－惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測－阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 帳號權限提升 網路權限提升	阻斷式攻擊

管理法律專業學程

事故回應與處理學程

網路與系統安控學程

可靠性系統學程

滲透測試學程

針對高階主管規劃課程

- **老闆的資安教育不能等！！！**
- **制度設計(橫軸)：管理法律專業學程**
  - **管理面**
    - 資安政策制定
    - 風險控管
  - **法律面**
    - 資通安全管理法
    - 個人資料保護法
    - 其他相關法律
- **資安概論及新知**
  - **因應攻擊之防禦策略與應變處理：**
    「公開資料的隱私-以發票資訊為例」、「加密工具的漏洞及誤用案例分析」、
    「勒索軟體預防與應變」、「防火牆與入侵偵測系統」、
    「進階持續性威脅(APT)案例分析與鑑識」、「網頁安全威脅與網頁滲透測試」

針對資安人員規劃課程

- **以一個學程搭配個別專業課程**
- **例如：威脅管理營運相關職位**
  - **事件回應與處理學程 (主要)**
    - 制度設計：事件回應與處理
    - 系統設計與實作：資安日誌與事件管理系統建置
    - 營運維護：情資分析、事件回應與處理
    - 滲透測試：弱點掃描、漏洞利用、網頁漏洞
  - **數位鑑識學程 (擷取單科)**
    - 營運維護：數位鑑識概念與實作、網路流量分析與檢測、惡意程式檢測實務

針對一般IT人員規劃課程

- **資安概論及新知課程**
  - **例如：因應攻擊之防禦策略與應變處理**
    「公開資料的隱私-以發票資訊為例」、「加密工具的漏洞及誤用案例分析」、
    「勒索軟體預防與應變」、「防火牆與入侵偵測系統」、
    「進階持續性威脅(APT)案例分析與鑑識」、「網頁安全威脅與網頁滲透測試」

- **職掌相關學程或單科**
  - **資料庫設計職務**：資料保護相關課程、容錯系統相關課程...
  - **軟體開發職務**：程式安全相關課程、系統滲透測試...
  - **網頁開發職務**：網頁安全相關課程、網頁滲透測試...
  - .....

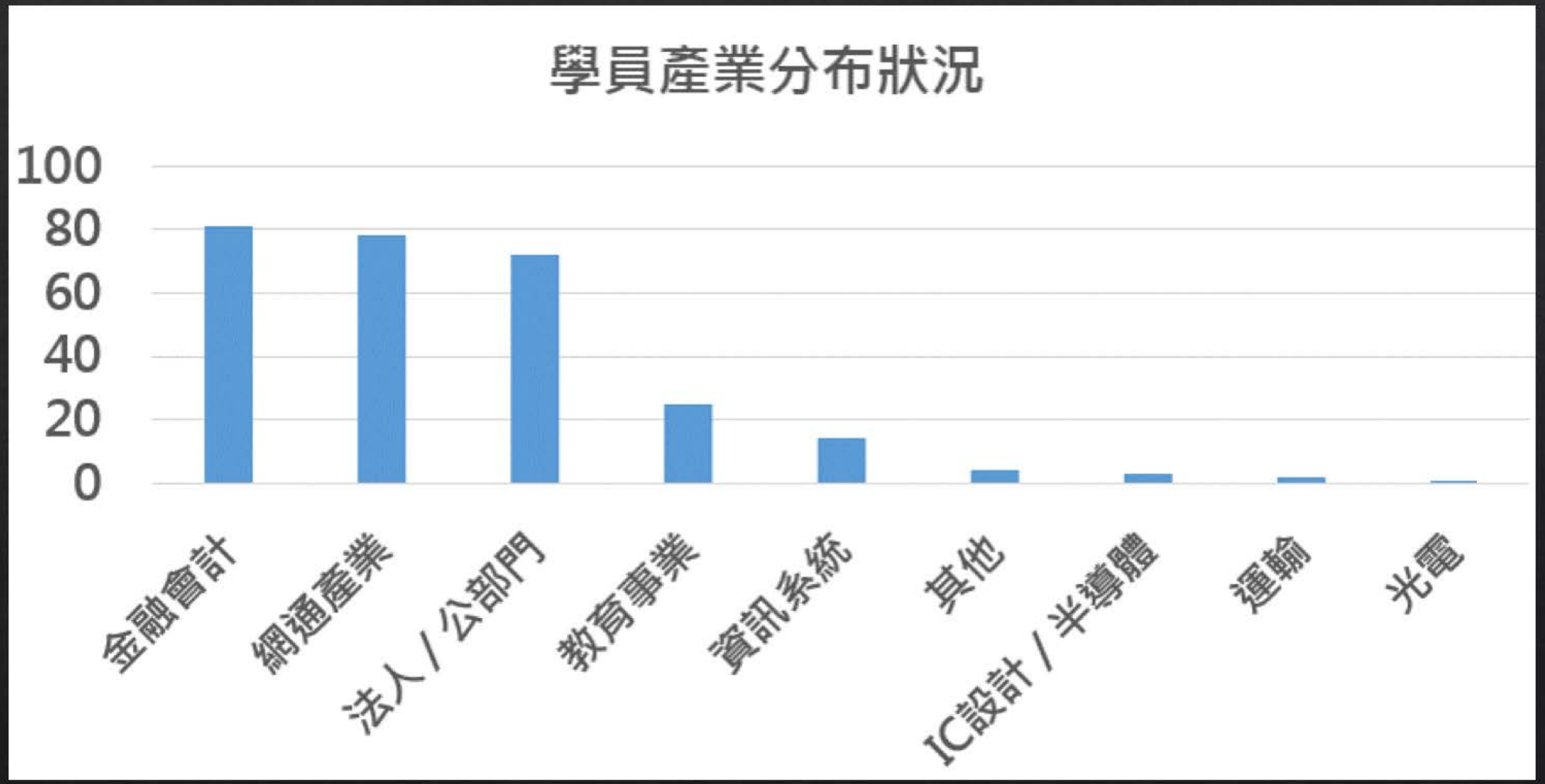
Outline

- 駭客、學術及產業間的資安落差
- 資安職能地圖
- 亥客書院經驗分享及數據統計
- 攻防平台設計
- 資安技術能力評量

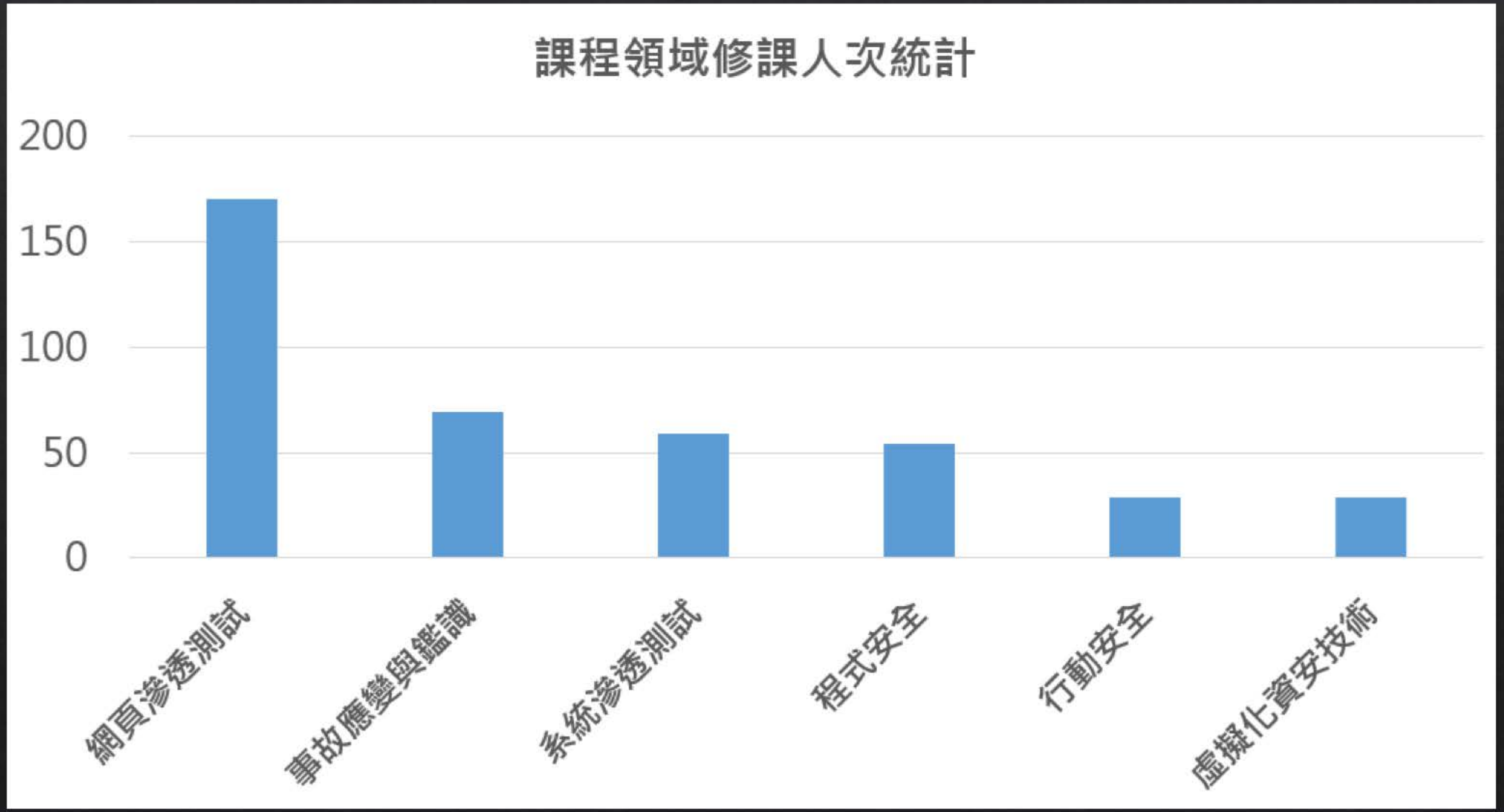
過去一年半的開課經驗

- **課程規劃與執行經驗**
  - 整理資料，觀察不同產業所專注的資安問題。
  - 業界程度平均普遍高 -> 要讓老闆明確了解課程能學到什麼，才會願意買單
    - 重視商業工具。
    - 業務分布廣，變動性高。
    - 學員背景知識較充足，整體上課成效落差較小。
  - 公務單位較兩極化 -> 課程設計要讓各種背景的學員都能有收穫
    - 重視Open Source工具。
    - 需求方向明確。
    - 學員背景知識落差較大，整體上課成效落差亦較大。

過去一年半的開課經驗


學員產業分布狀況
100
80
60
40
20
0
金融會計
網通產業
法人/公部門
教育事業
資訊系統
其他
IC設計/半導體
運輸
光電

過去一年半的開課經驗


課程領域修課人次統計
200
150
100
50
0
網頁滲透測試
事故應變與鑑識
系統滲透測試
程式安全
行動安全
虛擬化資安技術

課間與學員閒聊的心得

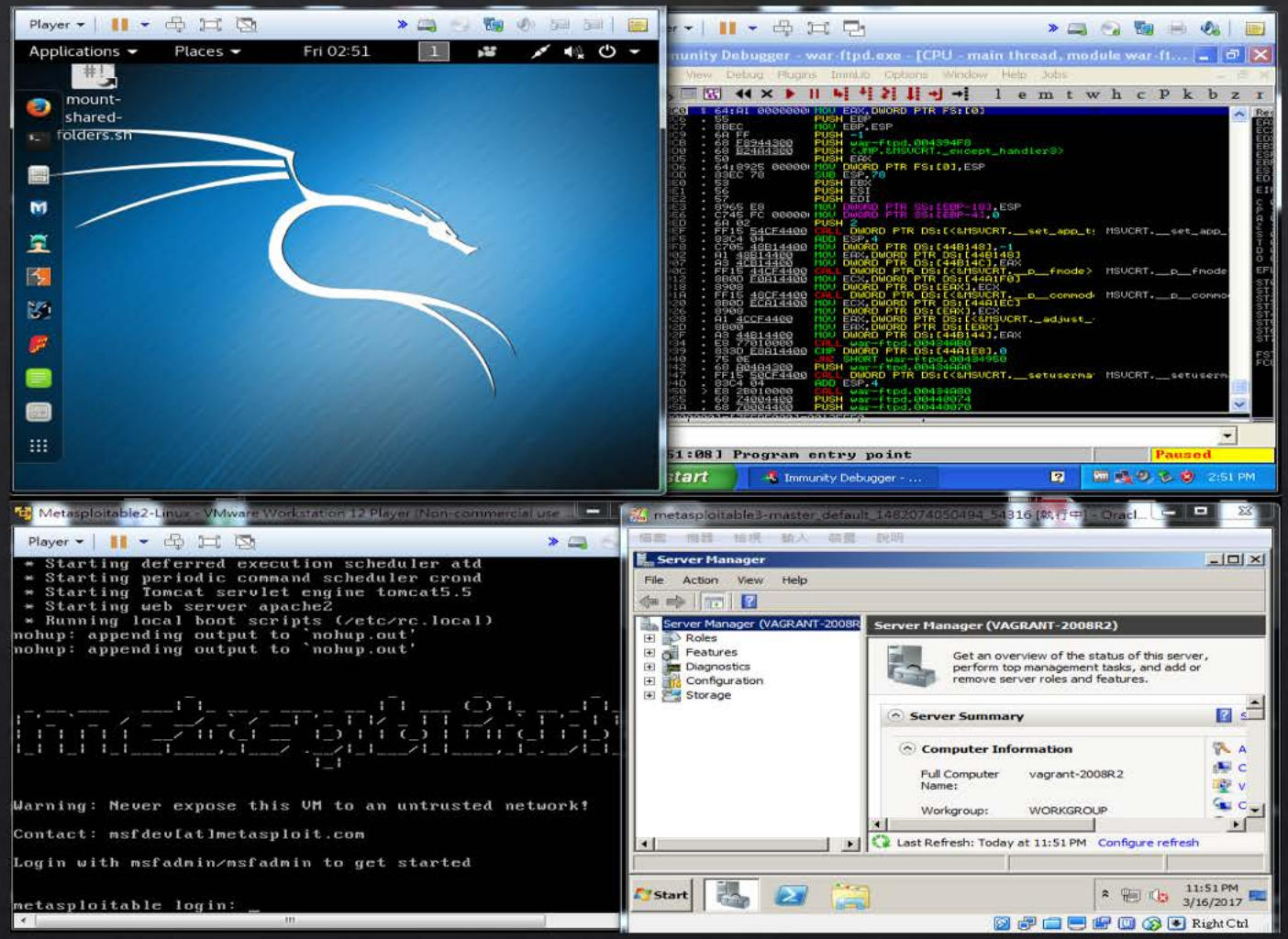
- 學員學習動機來自於可解決工作中實際遇到的問題。
- 近來關於滲透測試、事件處理、情資分析的研究相當熱門，但若沒有基礎的資安觀念與適當的系統安控，這些機制幫助有限。
- 例如：
  - 基礎的系統安控沒做好，如沒有正確備份Log、記錄Log，IR進場依舊難為無米之炊。
  - 開發人員沒有足夠程式/網頁安全的概念，每次PT都找到一堆漏洞，不是未經正確修補、就是下次又出現同樣的漏洞。

Outline

- 駭客、學術及產業間的資安落差
- 資安職能地圖
- 亥客書院經驗分享及數據統計
- 攻防平台設計
- 資安技術能力評量

資安工具箱

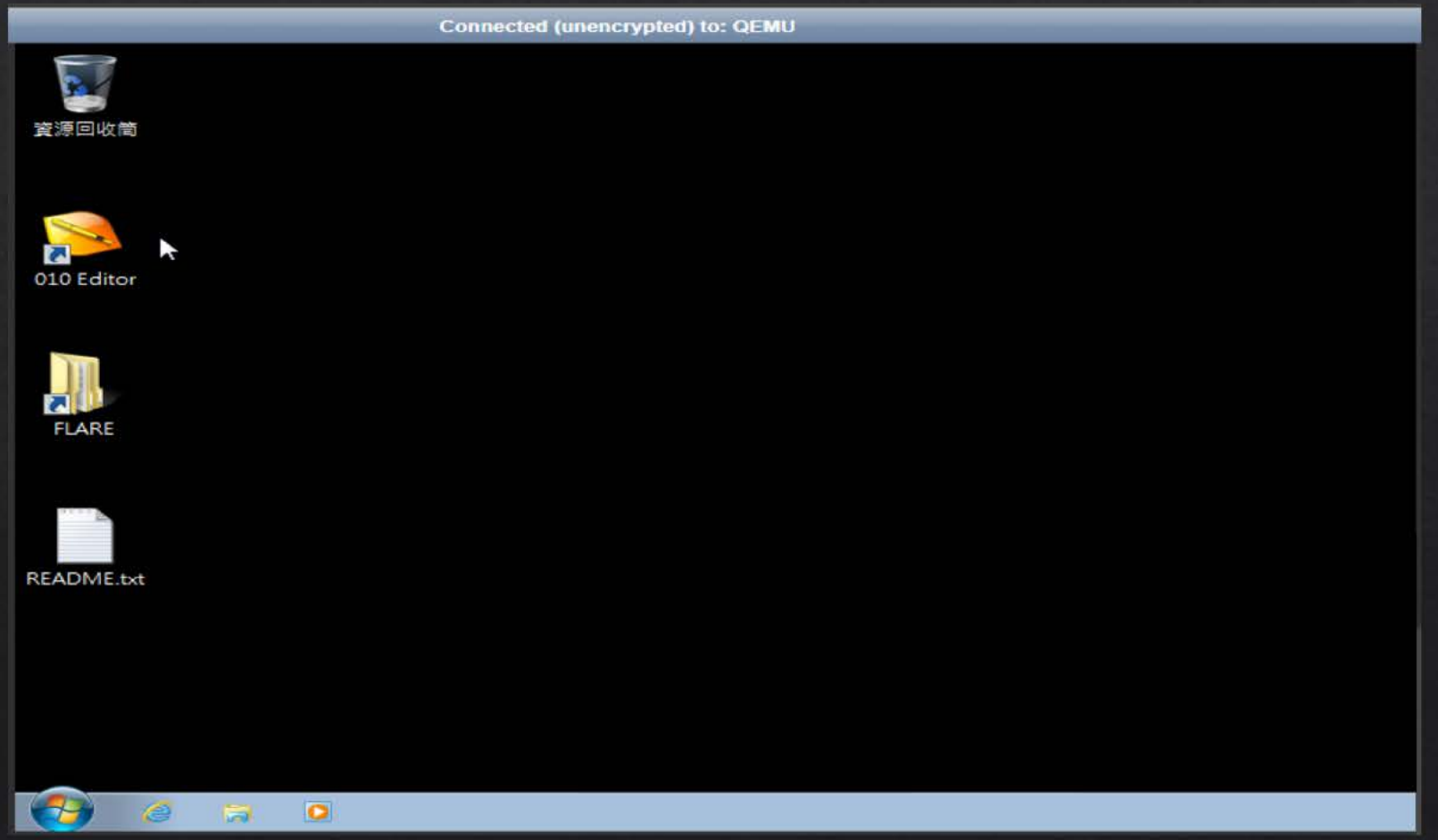
- 亥客書院課程以實作為主，課程中會協助學員建置各種資安攻防環境，以使學員可用此環境進行各項資安處理。
- 課程進行時，亦會提供建置完成之虛擬系統，以利學生於課程練習時間進行操作。
- 資安工具箱中包含各式資安相關工具
  - 滲透測試
  - 逆向工程
  - 數位鑑識
  - 資安稽核
  - 網路防禦
  - ...



各種資安工具箱截圖(離線)

線上工具箱

- 學生亦可透過網頁連線至線上工具箱
- 直接在網頁上操作，避免繁複的安裝過程



資安攻防演練平台

Running	hacker-college-Server-1	10.42.232.141	hackercollege	hacker-college:latest	None	
Running	healthcheck-healthcheck-1	10.42.84.15	hackercollege	rancher/healthcheck:v0.1.0	None	
Running	ipsec-ipsec-1	10.42.7.122	hackercollege	rancher/net:v0.7.5	None	
Running	ipsec-ipsec-cni-driver-1	None	hackercollege	rancher/net:v0.7.5	sh,-c,touch /var/log/rancher-ipam.log && e...	
Running	network-services-metadata-1	172.17.0.4	hackercollege	rancher/metadata:v0.6.8	start.sh,rancher-metadata,-subscribe	
Running	network-services-metadata-dns-1	None	hackercollege	rancher/dns:v0.11.0	rancher-dns,--metadata-server=localhost,-...	
Running	network-services-network-manager-1	None	hackercollege	rancher/network-manager:v0.2.19	plugin-manager,--metadata-url,http://ranch...	
Running	rancher-agent	None	hackercollege	rancher/agent:v1.1.2	run	
Running	rancher-server	172.17.0.2	hackercollege	rancher/server:v1.2.2	/usr/bin/s6-svscan,/service	
Running	rancher-server-proxy	172.17.0.3	hackercollege	nginx:1.11.8-alpine	nginx,-g,daemon off;	
Running	scheduler-scheduler-1	10.42.73.7	hackercollege	rancher/scheduler:v0.4.0	scheduler	
Running	test-crypto-threesix-1	10.42.2.186	hackercollege	bamboofox/cryptothreesix	None	
Running	test-magic-1	10.42.52.1	hackercollege	bamboofox/pwn_magic_type	None	
Running	test-pwn-pwnpickle-1	10.42.206.98	hackercollege	bamboofox/pwnpickle	None	
Running	test-web-banana-store-2-1	10.42.126.32	hackercollege	bamboofox/web_banana_store_2	None	
Running	test-web-base-1	10.42.183.45	hackercollege	bamboofox/webbase	None	

虛擬伺服器管理平台截圖

- 演練平台提供學生練習攻防技術的環境，以培養實務之能力操作。
- 協助課程講師設計上課練習，並提供平台放置管理練習伺服器群。
- 演練平台包含各種不同的伺服器群，給予學生在不同情境下練習的機會，以適應不同的實務場合。

支援不同模式的題目

- 涵蓋不同模式的資安練習
  - Jeopardy CTF – 大多專注於
  - Attack-Defense CTF – 多涵蓋了一些防禦面向
- 資安情境
  - 一台遭受攻擊機器，如何找出潛藏的後門程式？
  - 一台有漏洞的機器，如何修復？
- 針對不同職能，設計題目架構，以符合其工作實務

職能地圖-滲透測試題型設計

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測 – 惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測 – 阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 系統權限提升 網路權限提升	阻斷式攻擊

滲透測試題型模式與平台

- 滲透測試的工作項目以攻擊為主
- 題型模式
  - 提供一物件，如: 伺服器、檔案、加密訊息等
  - 學員嘗試攻擊物件上的資安弱點
  - 取得目標標誌
- 傳統CTF題型很多落在這種模式
- 測試攻擊、破解能力
- 題目範例一
  - 一伺服器上運行一具有Use-After-Free漏洞之服務
  - 學員必須寫出exploit並取得shell
- 題目範例二
  - 一已知加密演算法之密文，具有可預測亂數弱點
  - 學員需破解密文，取得原始明文

職能地圖-系統設計與實做題型設計

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測 – 惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測 – 阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 系統權限提升 網路權限提升	阻斷式攻擊

系統設計與實做題型模式與平台

- 此層之工作項目已實作或建置為主
- 題型模式
  - 提供一基礎環境(ex: VM) 給學員，學員可架設此系統
  - 提供一實作敘述，如: 實做一加密演算法
  - 提交完成之設定檔或程式碼
  - 審題伺服器於沙箱中編譯、執行此程式，並利用預寫之測試資料檢測正確性
  - 若實做正確，回傳一Flag代表實做正確(相容於傳統CTF平台)
- 較類似程式競賽的模式
- 測試學員開發與建置能力
- 題目範例一
  - 題目領域: 程式測試
  - 請依據附件程式法，利用GoogleTest設計測試資料，以達到100%測試涵蓋率。
  - 學員可透過網頁提交測試資料，若達成100%測試含蓋率，則會顯示出flag。
- 題目範例二
  - 題目領域: 密碼實作
  - 提供一自定義的protocol，及加密方式
    - getpub取得server public key
    - getSessionKey取得用public key加密後的 session key
    - getFlag 取得加密的flag

職能地圖-營運維護題型設計

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測 – 惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測 – 阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 系統權限提升 網路權限提升	阻斷式攻擊

營運維護題型模式與平台

- 此部分注重學員之修補問題的能力
- 題型模式
  - 提供一系統供學員遠端連線
  - 機器內部存在一些資安問題，需要學員進行修正
  - 審題方會以自動化之程式測試攻擊修補後的系統，若是修補成功，則提供學員Flag
- 類似攻防形式的防禦部分
- 題目範例一
  - 一服務具有SQL Injection漏洞，學員會給予此台機器之權限，以修正此問題
  - 學員完成修復後，平台會發出攻擊流量測試服務是否有修正，若有成功抵擋，則將flag傳給使用者
- 題目範例二
  - 一服務遭受特定ip機器DOS攻擊，學員需設定防火強過濾流量

職能地圖-制度設計題型設計

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測 – 惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測 – 阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 系統權限提升 網路權限提升	阻斷式攻擊

制度設計題型設計

- 經典的Cyber Rage模式
- 提供一預先設計之劇本，測試設計之制度/SOP是否能正確執行
- 測試制度設計，以及營運維護的人是否能正確執行

攻防平台小結

- 為輔助課程實作練習，我們開發一攻防平台輔助課程
- 從課程、技術練習到CTF等支援不同的應用
- 透過課程、CTF及自行出題，持續豐富平台上的練習深廣度
- 提供工具箱，加速學員練習的效率
- 方便管理、架設新的題目

Outline

- 駭客、學術及產業間的資安落差
- 資安職能地圖
- 亥客書院經驗分享及數據統計
- 攻防平台設計
- 資安技術能力評量

資安技術能力評量 – 重視實作

- 對企業而言，評量員工技術能力是一項困難的問題
  - 對已有基礎的學員，如何評估其技術能力是否符合？
  - 補助學員修課，是否有成效？
- 許多單位接洽亥客書院，協助認証評量其資安人員之技能程度
- 此部分說明我們如何規劃/設計整體評量方式

評量設計理念

- 以評量學員技能(Ability)為目標，以彌補其他偏重知識(Knowledge)及技術(Skill)為重的評量方式
  - 解決一件問題，需要知識與技術的搭配
  - 知道但不會用、會單一技術但無法應用於解決問題
- 實作、實作、實作
- 一次評量領域不宜太大，需夠細緻，以準確評估技術能力是否能負擔工作項目
  - 不需測試學員是否為全才，而是測試其是否能處理工作事項
- 將新的技術及概念納入測試範圍內

設計評量範圍

1. 職能地圖
2. 修課需求

依照職能地圖設計評量分類

	威脅情資	資料保護	認證及稽核	可靠性及可用性
制度設計	資安事件協調處理 資安事件審核與管理 事件應變政策制定	密碼機制設計 檔案管理機制設計 資料保護機制設計	帳號權限設計 稽核制度設計 使用者行為政策設計 存取政策設計	基礎架構設計 系統容錯制度與SOP設計 阻斷式攻擊應變SOP
系統設計與實做	安全性資訊與事件管理建置 日誌整合系統 情資交換系統 事件應變SOP	密碼機制實作 資料儲存系統建置 通訊加密系統建置 資料外洩防護建置	防火牆系統建置 網域使用者管理系統建置 使用者行為監控建置 公開金鑰基礎建設建置	可容錯系統建置 網路基礎建設防禦建置
營運維護	情資分析 數位鑑識 事件應變 網路流量分析與檢測－惡意程式、漏洞攻擊 惡意程式分析檢測	密碼機制維運 機密檔案管理 資料儲存系統維運 通訊加密系統維運 資料外洩防護維運	帳號管理 網域權限系統管理 防火牆與入侵偵測監控維運 使用者行為監控 權限稽核 公開金鑰基礎建設維運	系統備份 網路基礎建設維運 資訊基 網路流量分析與檢測－阻斷式攻擊檢測 阻斷式攻擊檢測防護應變
滲透測試	弱點掃描 軟體漏洞 網頁漏洞	密碼學漏洞 密碼學機制誤用 資料外洩掃描	帳號密碼強度檢測 帳號權限提升 網路權限提升	阻斷式攻擊

管理法律專業學程

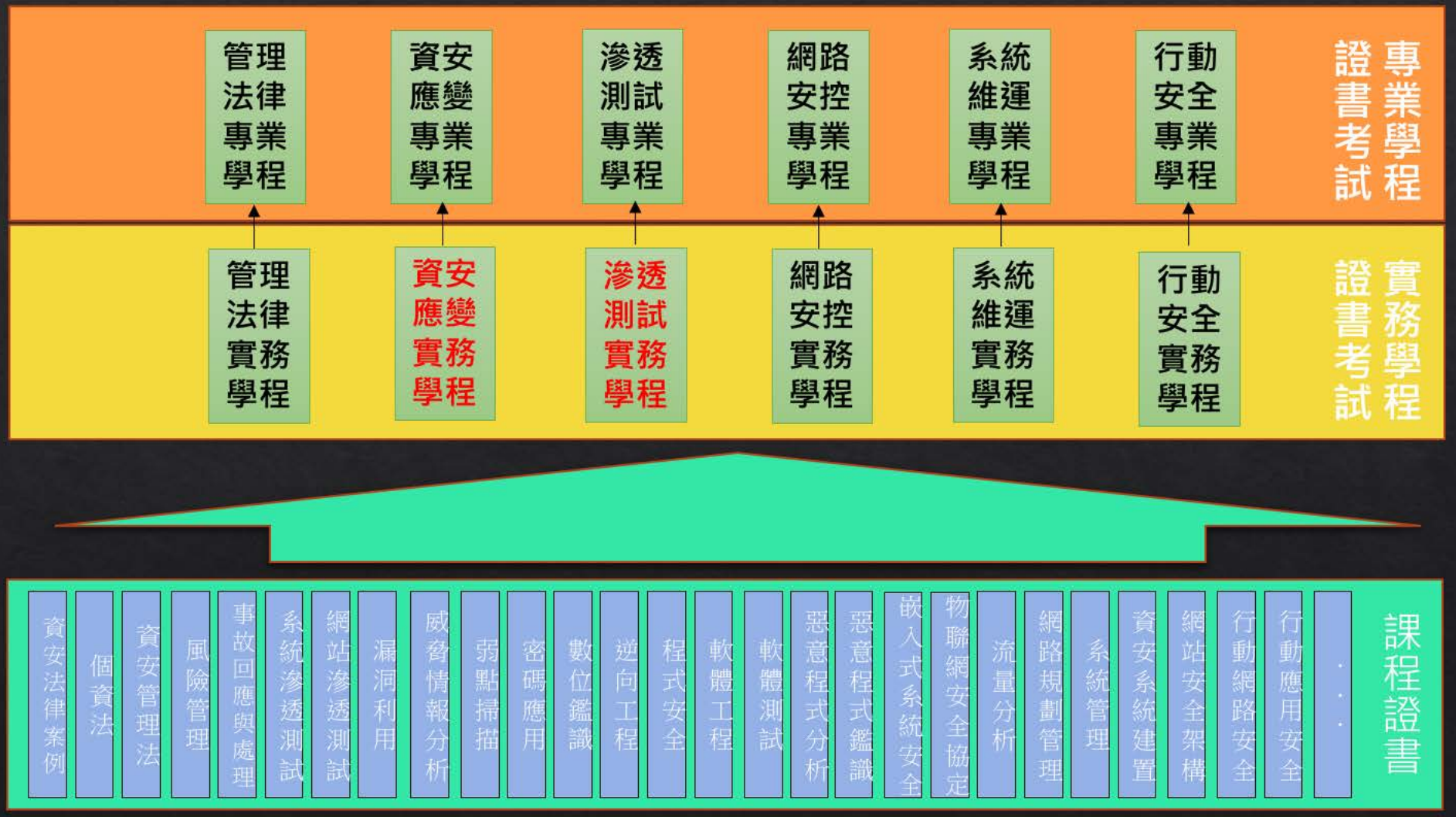
事故回應與處理學程

網路與系統安控學程

可靠性系統學程

滲透測試學程

亥客學程及證書


專業學程證書考試
管理法律專業學程
資安應變專業學程
滲透測試專業學程
網路安控專業學程
系統維運專業學程
行動安全專業學程
實務學程證書考試
管理法律實務學程
資安應變實務學程
滲透測試實務學程
網路安控實務學程
系統維運實務學程
行動安全實務學程
課程證書
資安法律案例
個資法
資安管理法
風險管理
事故回應與處理
系統滲透測試
網站滲透測試
漏洞利用
威脅情報分析
弱點掃描
密碼應用
數位鑑識
逆向工程
程式安全
軟體工程
軟體測試
惡意程式分析
惡意程式鑑識
嵌入式系統安全
物聯網安全協定
流量分析
網路規劃管理
系統管理
資安系統建置
網站安全架構
行動網路安全
行動應用安全
. . .

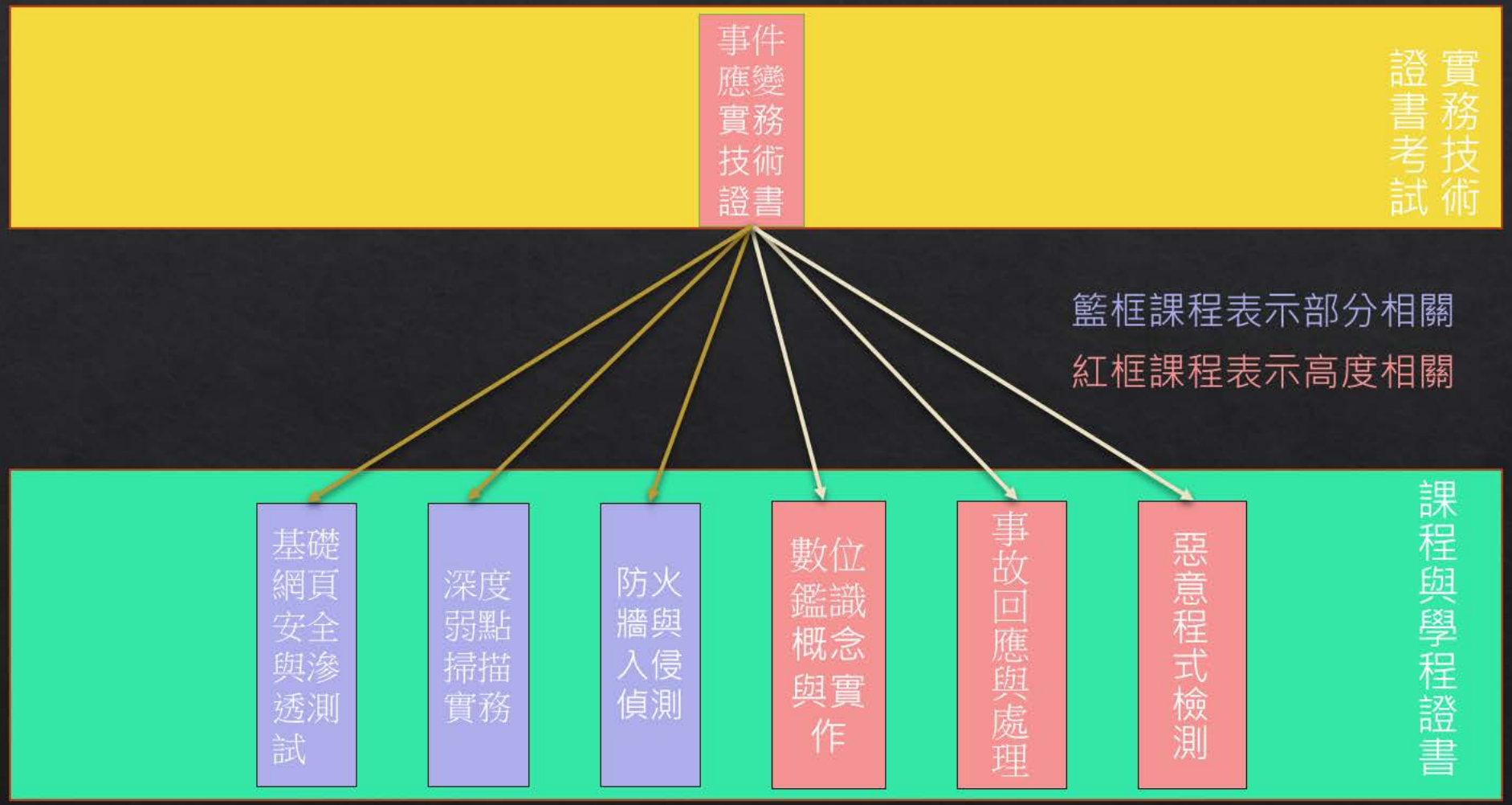
評量種類選擇

- 目前人力資源無法一次完成所有評量，因此選取少數幾個做為實驗
- 依開課報名人數經驗、需求評估，以下面兩個為初期推動目標
  - 滲透測試實務技術證書考試
    - 通過考試者將具備滲透測試實務技術，能夠針對一般系統進行弱點掃描以及滲透測試，以評估目標系統的安全強度並發現安全漏洞。
  - 事件應變實務技術證書考試
    - 通過考試者將具備資安事件的實務應變能力，能妥善應對資安事件、減低傷害、初步找出事件原因並嘗試修正系統。

設計考試項目設計

1. 選擇相關課程
2. 分析課程內容，建立課程技能樹
3. 擷取評量題目走向
4. 題目設計

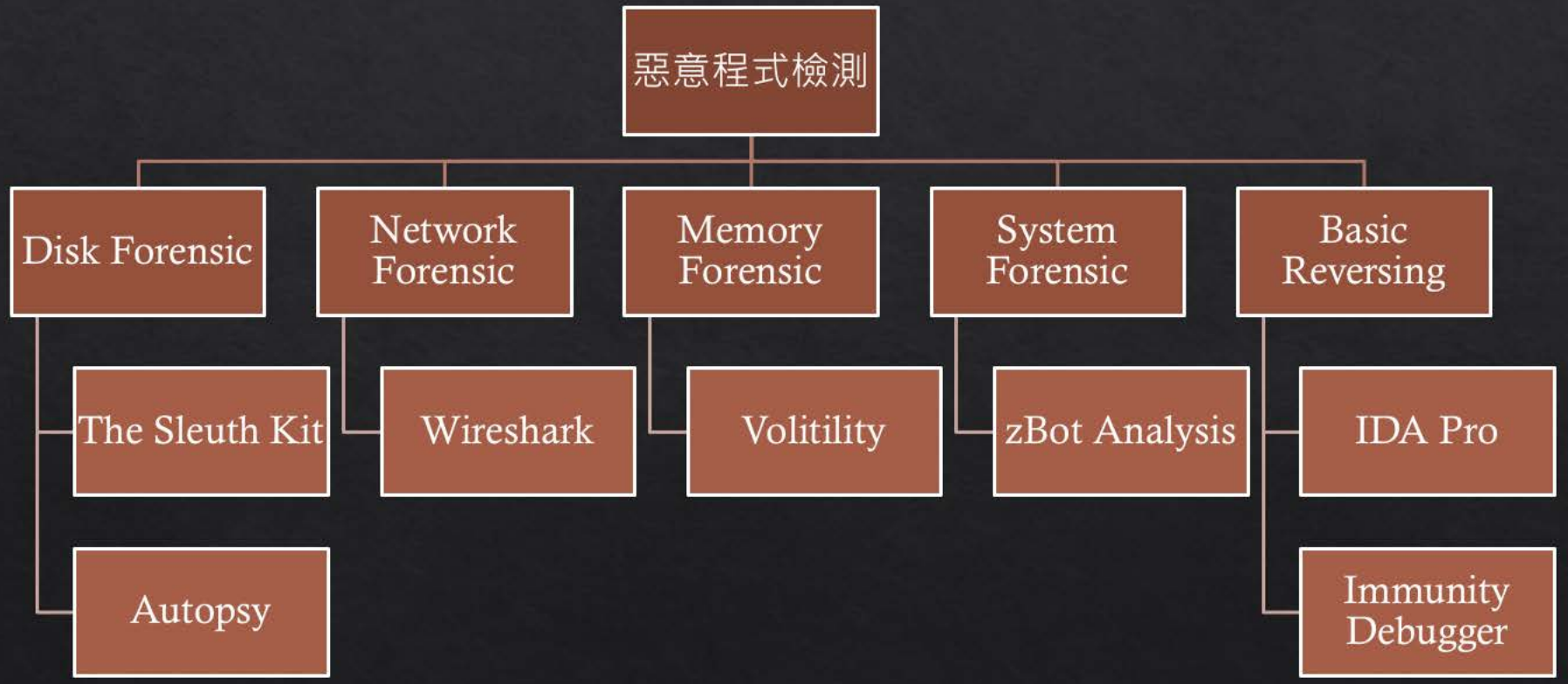
「事件應變實務技術證書」相關課程



事件應變實務技術證書

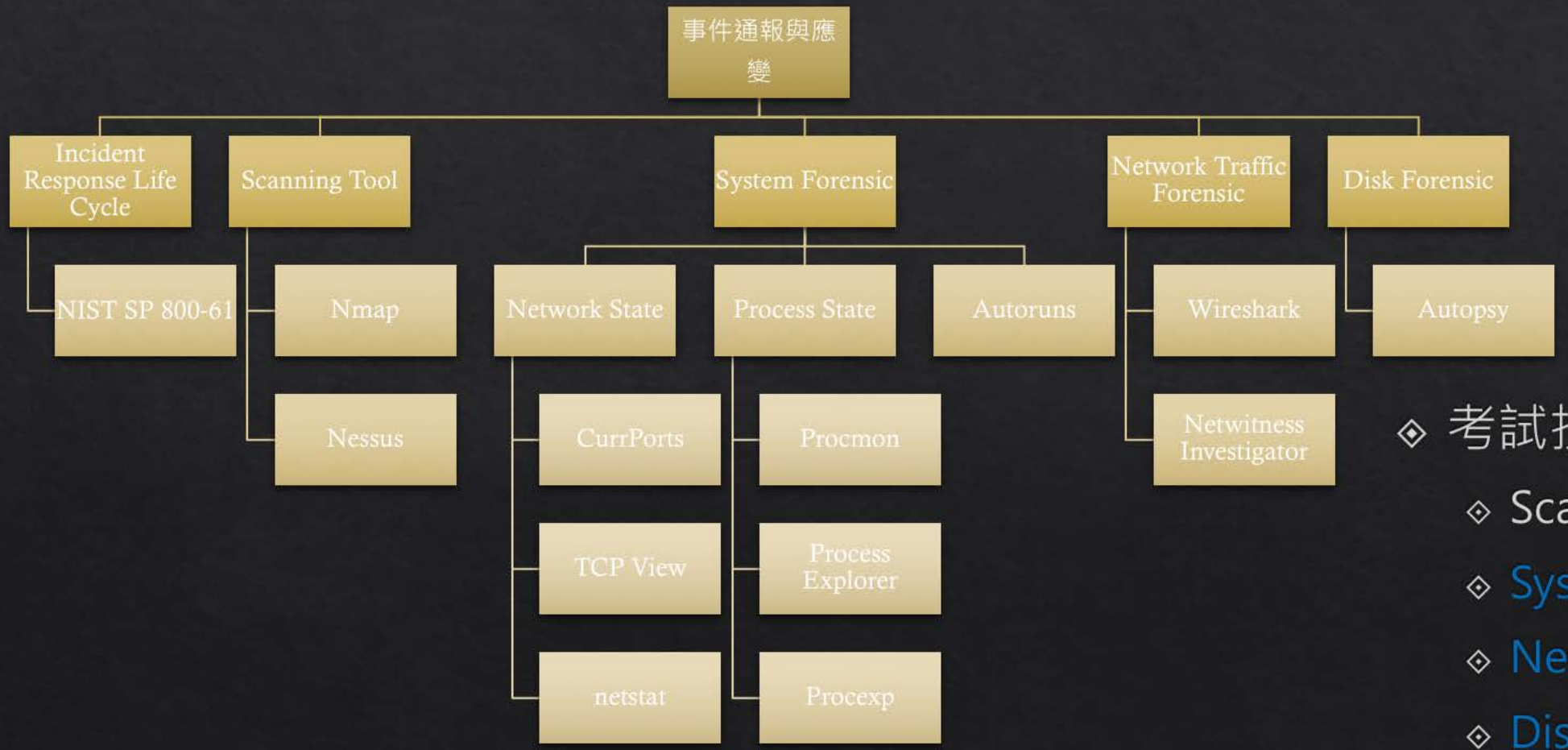
- 考試內容
  - 必考科目
    - 惡意程式檢測、事故回應與處理、數位見識概念與實作
  - 抽考科目
    - 基礎網頁安全與滲透測試、深度弱點掃描實務、防火牆與入侵偵測

惡意程式檢測



- 考試項目
  - Disk Forensic
  - Network Forensic
  - Memory Forensic
  - System Forensic
  - Basic Reversing

事件通報與處理



- 考試技能
  - Scanning Tools
  - System Forensic
  - Network Traffic Forensic
  - Disk Forensic

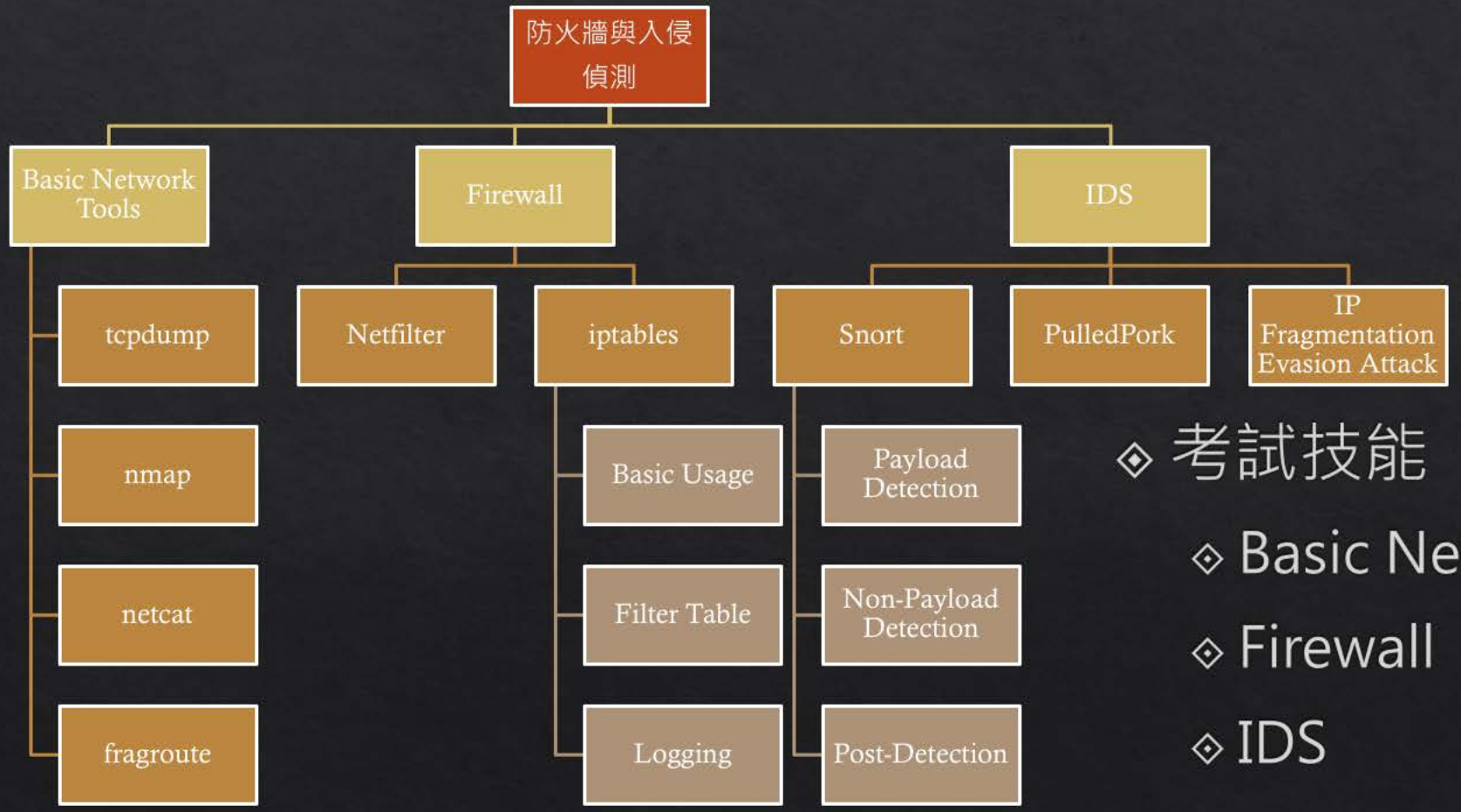
數位鑑識概念與實作

- 考試技能
  - 硬碟鑑識

必修實作考試項目

惡意程式檢測	事件回應與處理	數位鑑識概念與實作
System Forensics	System Forensics	
Memory Forensics		
Disk Forensics	Disk Forensics	Disk Forensics
Network Forensics	Network Forensics	
Software Reversing - Elementary		
	Vulnerability Scanning	

防火牆與入侵偵測

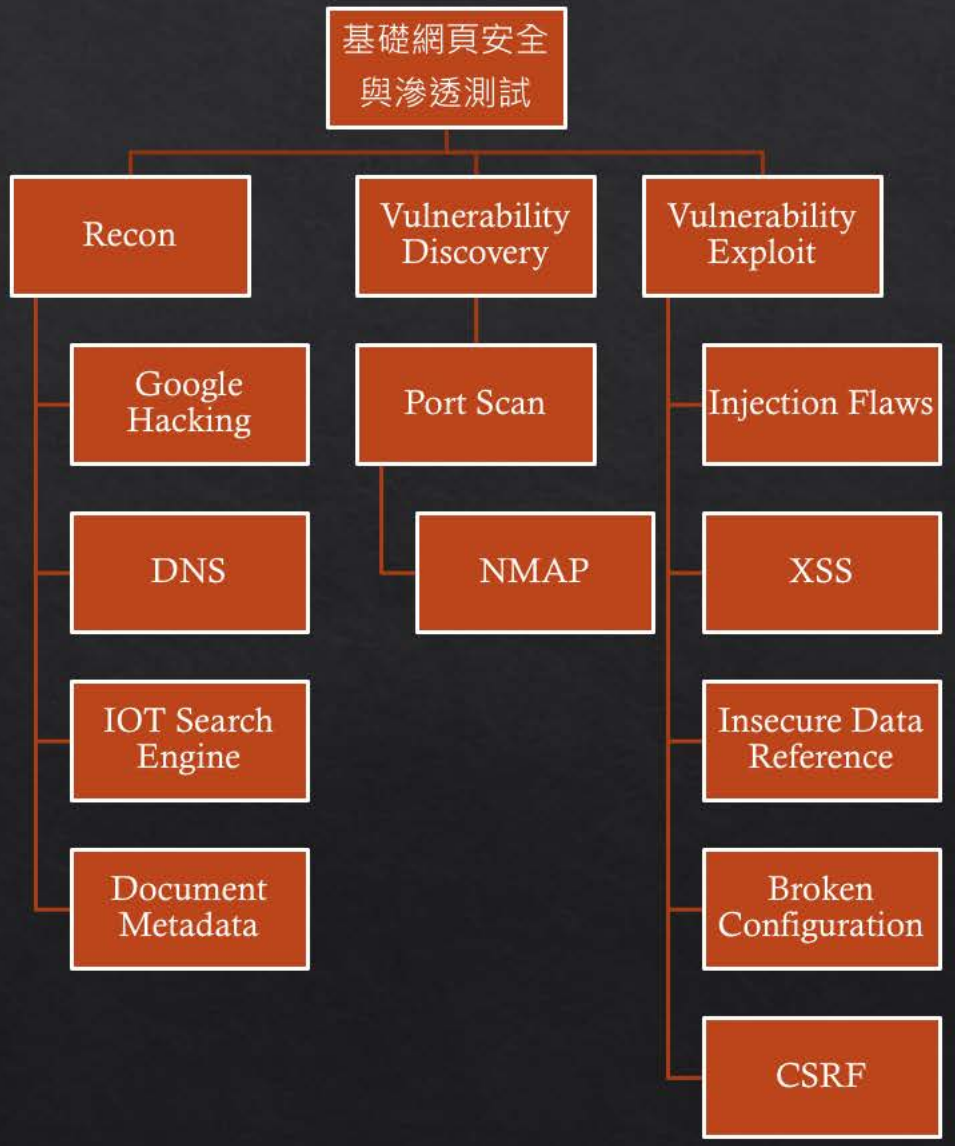


- 考試技能
  - Basic Network Tools
  - Firewall
  - IDS

深度弱點掃描實務

- 考試技能
  - Crawler
  - Vulnerability Scan
  - Vulnerability Scan Report Analysis

基礎網頁安全與滲透測試



- 考試項目
  - Recon
  - Port Scanning
  - Injection
  - XSS
  - Insecure Data Reference
  - CSRF

選修實作考試項目

防火牆與入侵偵測	深度弱點掃描實務	基礎網頁安全與滲透測試
Network Monitoring		
Firewall		
IDS		
	Crawler	
	Vulnerability Scanning	
	Scan Report Analysis	
		Recon
		Port Scanning
		Injection
		XSS
		CSRF
		Insecure Data Reference

題目設計(進行中)

- 題目設計
  - 以半小時到一小時能完成為主
  - 並非專注於某項工具如何使用，而是專注於解決問題
  - 開放性解決問題方法
  - 不通靈 – 題目設計需有依據

頒授證書

- **課程證書**
  - 完成每門課程且通過課後測驗，頒授課程結業證書。
- **實務學程證書**
  - 目前規劃包含六大類實務學程。
  - 達成各學程之修課條件，通過學程考試後，頒授實務學程證書。
- **專業學程證書**
  - 各類實務學程皆有進階專業學程。
  - 達成各學程之修課條件，通過專業學程考試後，頒授專業學程證書。

事件應變實務技術證書

- 考試辦法(暫定)
  - 1小時筆試及5小時上機實作，共6小時測驗時間
  - 筆試為約20題選擇題，佔總成績30%
  - 上機實作為約10題實作題，佔總成績70%
  - 總成績超過70分為通過標準
- 時間地點(暫定)
  - 2018年9月~10月
  - 交大台北校區
  - 提供25–30人

結　論

- 駭客、學術及產業間存在資安落差，應建立互利合作機制。
- 人材規劃可先建構專屬職能地圖，再依公司規模與核心業務決定自建或委外項目。
- 培訓課程可考量人員職掌與層級，以學程搭配單科的方式規劃。
- 現階段以筆試為主之證書與評量已相當成熟，未來應積極開發實做測驗，以收互補之效。
- 「實務資安」的培訓正處於萌芽期，需求眾多但專業開課單位較少，課程內容良莠不齊，亟需來自駭客圈的火力支援。

Thanks.