高點·高上 調查局特考

完整課程規劃，一路挺你到上榜

先修課程
- 奠定法學架構
- 銜接正課

正規課程
- 各家學說兼備
- 面授、VOD、雲端三軌並行，多元學習更彈性

經典題庫班 申論寫作正解班
- 經典題庫班：掌握破題、解題技巧
- 申論寫作正解班：老師親自批改知盲點

總複習
- 時事與命題重點整理

狂作題班
- 考前6週助教手把手指導，海量作題提分快

口試實戰班 體能實測班
- 指導書面報告，提供口試及體能測驗技巧

王牌師資坐鎮，正課、加強都超給力

立即試聽


韓律(康皓智)
行政法


劉律(劉睿揚)
刑事訴訟法


榮律(張鏡榮)
刑法


鄭泓(鄭凱文)
中級會計學


初錫(蘇世岳)
政治學


張海平(陳治平)
社會學


金乃傑(魏取向)
資通安全

五大課輔系統，應援系統最全面

洞悉時事修法議題，補足最新法律動態。

考情&修法講座

線上會考

擬真模考，針對科目做全體排名，實力一手掌握。

專業老師進行「口試模擬」提升考生論述能力。


口試實戰

歷屆考古題

蒐錄歷屆考古題，提供考生平時作答練習，培養預試高分。

名師親自示範高分寫法，培養申論答題架構。

申論題專欄

113/8/31前憲司律/司特/調特准考證**報名享優惠！**

面授/網院特價**33,000**元起、雲端特價**46,000**元起

《資訊安全實務》

一、請回答下列有關數位鑑識之問題：

(一)在數位鑑識（Digital Forensics）標準作業程序中，何謂資料採集（Data Acquisition）？（15 分）

(二)在某次數位鑑識調查中，資安事件調查員成功從犯罪現場獲取了數位證據，調查人員現在必須保存這些數位證據以便進一步分析。為了確保數位證據的完整性，調查人員應優先考慮採取那些行動？（10 分）

命題意旨	數位鑑識流程步驟目的。
答題關鍵	考生必須對於數位鑑識流程有所認識，每個步驟的目的為何，並搭配數位證據保全標準作業程序與資安事件實務案例答題。

【擬答】

(一)在數位鑑識中，根據 CEH 定義，資料採集是一項具有系統化和必須小心操作的流程，目標在於保存資料、資料收集和復原資料的步驟符合規範，使鑑識出來的結果具有完整性、認證性和合法性。

1.保存資料：現場保存資料有分兩種：

(1)揮發性資料：電腦系統中若電源關閉或是系統關機，資料內容會消逝。

(2)邏輯性資料：儲存於作業系統中的非揮發性儲存體，如：SSD、硬碟、光碟片。

現場查扣的數位證據蒐證時，必須對所蒐集到的資料做完整性驗證並記錄 Hash 值於相關表單中。

2.資料收集：收集資訊設備相關裝置。

(1)電腦、周邊設備及數位儲存媒體。

(2)網路連線設備與登入紀錄、印表機和隨手相關的筆記本或是帳號密碼。

(3)雲端使用相關紀錄與儲存資訊。

3.資料復原：將被刪除或是資訊隱藏的資料復原，例如：Encase、FTK 軟體。

(二)可採行動有：

1.現場全程照相與錄影。

2.標記所有證物，並記錄編號、順序與封緘。

3.搜扣相關軟硬體、文件、帳號密碼，若是系統已登入，過程中保持電力足夠。

4.紀錄螢幕畫面、時間、網路連線紀錄與登入帳號密碼。

5.保存記憶體資料。

6.備份原始硬碟資料的副本後，進行雜湊值驗證，再進行鑑識分析，使鑑識結果與原有數據資料具有一致性。

7.查扣相關物品經手人皆須記載與簽名。

二、請回答下列問題：

(一)資安調查人員正在對從受害系統取得的某惡意程式之可執行檔進行分析，該調查人員是否可以在無原始程式碼的情況下對可執行檔進行逆向工程？如果是，其步驟為何？（15 分）

(二)說明軟體逆向工程（Software Reverse Engineering）之目的為何？（10 分）

命題意旨	惡意程式逆向分析概念與步驟。
答題關鍵	逆向工程不僅可以為正規商業資訊系統分析的解碼，亦可以為資訊安全的目的，如何分析既有可執行的惡意程式，了解攻擊程式的手法與企圖，在攻防兩端無盡頭的資訊安全競賽，讓攻擊者的傷害降到最低，避免主要主機遭受侵害。拿高分關鍵不在於技術解釋，而是如何將步驟與應用案例加以說明。

【擬答】

(一)機器語言→組合語言→高階程式語言→EXE 檔案，現今的執行檔案通常是高階程式語言所撰寫出來的產物，逆向工程是對於既有執行檔案進行逆向的分析與研究，從電腦看得懂的 0 和 1 機器碼，回推執行檔案的原始碼結構，業界常用逆向工程工具如：IDA Pro、x64dbg。

步驟：

1.資訊萃取：

(1)靜態分析：不執行檔案，直接透過工具進行逆向工程原始碼分析，分析範圍大且完整。

(2)動態分析：執行惡意程式檔案，觀察程式執行時的真實行為，還原真實運作情形。

2.塑模結構：透過反編譯器將收集到的指令，還原組合成抽像模型的流程，例如：原有系統模組架構圖、系統分析的流程圖。

3.審查重建：確認分析結果的效用，若將模型付諸實踐，是否可以和原有惡意攻擊程式達到一樣成效攻擊，確保模型的有效性。

(二)逆向工程目的：

1.分析惡意程式的目的行為與模組架構。

2.網路流量、網域目的與封包特徵。

3.感染的程式與檔案。

4.被修改的程式與檔案。

5.侵入的作業系統弱點與事後防範與更新。

三、 請回答下列問題：

(一)在網路安全攻擊中，何謂 Session Hijacking Attack？何謂 IP Spoofing？以上兩者之關係為何？（15 分）

(二)說明什麼是 sniffing？其目的為何？（10 分）

命題意旨	OWASP 常見攻擊。
答題關鍵	OWASP 公布的傳統前十大攻擊樣式必須要了解，有些時候，攻擊手法基於計算機原理很類似，然而手法雖然雷同，但是攻擊標的的差異的不同，防護手段也會隨之變化。

【擬答】

(一)Session Hijacking Attack 及 IP Spoofing 定義：

1.Session Hijacking Attack：session 指的是登入網站後，網站會創建一組一串數字和字母會話 ID ，稱為 session ID，用於身分驗證的有效狀態，會話劫持是攻擊者竊取被害者與主機間的會話通訊。常見攻擊手法有：

(1)跨腳本攻擊。

(2)網路竊聽。

(3)截取受害者與主機間的封包傳遞，若是於網址 get 方法傳遞變數，session 變數未加密的話，則直接暴露於公開網路中。

(4)中間人攻擊或是不安全的 wifi 連線。

2.IP Spoofing：IP spoofing 是建立帶有被修改過，假的來源位址封包標頭，屬於 OSI 第三層中的網際網路通訊協定定義，隱藏或偽裝傳送者的身分和模仿另一個網域系統，如：模仿 140.112.x.x IP，或實現 DDos、網路攻擊目標而事後躲避司法偵查。

IP spoofing 可以用來 TCP 建立連線時，竊取 session ID，與通訊過程中，使用 IP spoofing 進行中間人攻擊，達到會話劫持目的。

(二)sniffing：一種資料封包攔截技術，常見的會將網卡調整為「promiscuous mode」，不論目的是否為本身機器，將經過的封包皆予以收下，著名軟體為 wireshark。

1.正常用途：sniffering 技術並非全然為惡意，網管人員經常透過 sniffering 技術，了解整個網路的狀況、流量、異常與組織政策控管；此外，防火牆、常見的 IDS、IPS 技術便是搭配 sniffering 監聽網路，分析是否有潛在惡意攻擊。

2.攻擊用途：對特定轉往目的的封包進行攔截，加以分析封包中所攜帶的敏感資訊，如：密碼、信用卡帳密、醫療資訊等等。

四、 請回答下列關於資訊安全之問題：

(一)攻擊者不斷尋找利用傳送訊息進行破壞的新威脅。請說明 phishing、vishing 與 smishing 之差異。（15 分）

(二)簡述何謂 S/MIME（Secure/Multipurpose Internet Mail Extensions）？（10 分）

命題意旨	網路郵件攻擊名詞解釋與電子郵件安全方法。
答題關鍵	隨著猜猜我是誰、簡訊釣魚、或是攻擊者透過深偽技術模仿語音攻擊手法，滲透內部社交工程騙取敏感資料，因此電子郵件安全加密變得重要；第一小題為第二小題的前身，假如不知道S/MIME在做什麼，可以由第一小題的釣魚攻擊回推第二小題的防禦手段。

【擬答】

(一)phishing、vishing 與 smishing 之差異為：

1.phishing：網路釣魚，攻擊者企圖從電子郵件中夾帶惡意網址、新奇的新聞或是正式的文件通知，透過偽裝成信譽卓著的銀行機關、公部門或是親信友人，獲得被害者個資、帳密密碼和信用卡明細等個人敏感資訊的犯罪詐騙過程，用一個假以亂真的網站，網址的 0 改成英文的"O"，通常搭配輔助 XSS 攻擊和中間人攻擊。

2.vishing：語音釣魚攻擊，社交工程攻擊手段，駭客會假冒為受害者信任的友人或公司放鬆戒備。近一年來詐騙集團利用「生成式 AI」技術，生成相同的語調與聲頻語音通話，使用各種話術試圖從受害者取得各種機敏資訊，例如金融帳戶、社群個資、掌管的商業、公務系統權限。

3.SMiShing: 網路釣魚簡訊，原始是一種以手機簡訊的網路釣魚攻擊手法，例如：台電繳費通知、電信升級廣告。近年來，廣義的網路釣魚簡訊，趨勢為透過社交網站為平台，發出假美女網紅徵友、假帥哥機師徵友和投資詐騙廣告的釣魚簡訊。

(二) S/MIME：由第一小題可以得知電子郵件傳送需要完整性、機密性、來源鑑別性與不可否認性，因此 S/MIME 是一種進行數位簽章和加密的網際網路標準，與憑證相結合，概念上與 PKI 憑證認證流程相近，代表信件由信任的網域伺服器所發出，而非網路上的隨機釣魚。以使用 outlook 為例：

1.信任中心設定，匯入憑證。

2.憑證及演算法選擇雜湊與加密演算法。

3.設定郵件加入數位簽章。

4.郵件加密顯示，若沒有受信任的網域，則發出的信件將沒有認證符號。