大吉 總複習班 ➔ 提升統整力

求勝科目 共同科目+專業科目

好試解籤 重點歸納、時事修法以及命題趨勢提醒。

達人推薦 張逸仙 普考地政

高點總複習課程不僅可以快速複習重點，命中率也很高！我特別推薦許文昌跟于俊明老師，教學認真、教材豐富，非本科系的考生也能快速上手，讀書更有效率！

考場保庇價 三等5,000元 四等4,000元起 定價8,000元起

大吉 題庫班 ➔ 打造高分力

求勝科目 經濟學/財政學/稅法/會計/審計/政會

好試解籤 名師嚴選經典考題，傳授看題能力以及教導高分答題技巧！

達人推薦 柯辰穎 高普考財稅行政雙榜

隨著考期越來越近，我開始感到心慌，所以跑去報名會計＆經濟＆財政的題庫班，老師解題讓我釐清觀念，增加解題能力。

考場保庇價 1,800元起/科 4堂/科 定價5,000元

高點 高上 高普考 衝刺 考運亨通 商資・地政 必勝錦囊

大吉 申論寫作班 ➔ 論正寫題力

求勝科目 審計/民法

好試解籤 課前練題，高質量批改服務，建立答題架構，提高寫作高分力！

達人推薦 李濤亦 高普考會計雙榜

高點老師猜申論題命中率非常高！審計公報後期時間不太⊠，只抓老師重點來背，申論竟拿到32分！

考場保庇價 2,500元/科 6堂起/科 定價5,000元

大吉 公經進階班 ➔ 鞏固強試力

好試解籤 透析考題趨勢，加強進階內容，使考生能進一步掌握艱深考題。

達人推薦 陳樂庭 高考經建行政【狀元】

推薦張政(張家瑋)老師的公經進階課程，他用數理詳細說明觀念，讓我實力大增！

考場保庇價 2,500元

以上考場優惠110/10/20前有效，限面授/VOD，當期最新優惠洽各分班櫃檯或高上生活圈！

另有行動版課程隨時可上 試聽＆購課，請至

1 知識達購課館 ec.ibrain.com.tw

2 高點網路書店 publish.get.com.tw

# 《資通網路》

| | |
|---|---|
| 試題評析 | 本次網路考題滿滿的資訊安全，故學員在準備上如課程所提，需以資訊處理綜合專業科目之高度準備。《孫子兵法・九變》有云：無恃其不來，恃吾有以待之。 |
| 考點命中 | 第二題：《高點・高上資訊安全實務講義》第3章，張又中編撰，頁3-6～7。<br>第三題：《高點・高上資訊安全實務講義》第3章，張又中編撰，頁3-9～10。 |

一、近年來員工在家工作的需求量日益增加，因此企業建置VPN，提供員工遠端登錄企業網路。請說明VPN所採用的IPSEC運作原理，以及如何管理VPN避免企業遭受攻擊。（25分）

**答：**

虛擬私有網路(Virtual Private Network, VPN)是一種常用於連接中、大型企業或組織間的私人網路通訊方法。其透過公用的網路架構如Internet來傳送如Intranet的網路訊息，而不用架構價格昂貴的專線。

對於在家工作的員工而言，其可利用已加密的通道協議(Tunneling Protocol)來達到保密、傳送端認證、訊息完整性等私人訊息安全效果，可用不安全的公眾網路如Internet來傳送可靠、安全的訊息，並可存取Intranet資源如檔案伺服器、郵件伺服器等，如同身在Intranet一樣。值得注意的是，加密訊息與否是可以控制的，沒有加密的VPN訊息依然有被竊取的危險。

IPSEC作用於網路層(Network Layer)，為多服務、多演算法，及多單元規模的架構。提供機密性、完整性，並避免重傳攻擊，描述於RFC2401、2402、2406及2410。

二、DNS通訊協定並不安全，因此IETF提出DNSSEC期望改善其安全問題。請說明DNSSEC運作原理、所提供之安全服務、可防禦之攻擊以及無法防禦之攻擊。（25分）

**答：**

由於DNS的查詢與回應封包並未加密，因此駭客可於其中偽造，將使用者導向錯誤的主機，或是進行DNS放大攻擊。因此，DNSSEC利用公開加密演算法與雜湊函數來提供：

1.資料完整性(Data Integrity)
2.來源可驗證性(Origin Authentication of DNS Data)
3.可驗證之不存在性(Authenticated Denial of Existence)

DNS弱點：

1.機密性(Confidentiality)
DNSSEC 的 RR 與 RRSIG 於傳輸過程皆未加密，資訊可能被攻擊者攔截。
2.可用性(Availability)
如攻擊者發動針對 DNS 伺服器的 DoS、DDoS 攻擊，則其仍可能因負荷過重而無法正常運作。

三、分散式阻斷服務（Distributed Denial of Service，簡稱DDoS）攻擊可能造成網路無法使用，因此網管人員需採取一些防範措施，避免網路運作異常。DDoS 攻擊可分為三大類：流量為基礎之攻擊、通訊協定攻擊以及Layer 7 DDoS攻擊。若某網站伺服器被Layer 7 DDoS攻擊，請舉例說明Layer 7 DDoS攻擊，以及防禦方式。（25分）

**答：**

Layer 7 DDoS係指專注於第7層功能的DDoS攻擊，與流量為基礎之攻擊相較，其可利用數量較少的封包來大規模地進行DDoS攻擊，且可能被誤認為正常的封包流量。例如：HTTP Flooding，主要利用耗費資源的Post Request來讓攻擊標的崩潰。

Layer 7 DDoS攻擊防禦方式：

1.使用應用程式前端硬體(Application Front End Hardware)。
2.使用入侵防禦系統(Intrusion Prevention System, IPS)。

3.阻斷服務防禦系統(DoS Defense System, DDS)。
4.利用黑洞與水坑(Blackholing and Sinkholing)。
5.清洗管線(Clean Pipes)。

四、HTTP乃應用層通訊協定，但未提供資料安全性。目前網站多採用HTTPS以保護資料安全性。請說明HTTPS之運作原理，以及可提供之安全服務。（25分）

**答**：

超文字安全傳輸協定(HyperText Transfer Protocol Secure, HTTPS)運作原理：
1.雙方交換 Hello 訊息並協議安全參數，檢視是否有可重複使用的 Session ID。
2.交換金鑰材料，並製作前置主秘密金鑰(Pre-master Secret)。
3.交換身份憑證。
4.利用前置主秘密金鑰製作秘密金鑰(Master Secret)。
5.登錄安全參數於會議連結(Session Connection)。
6.依照安全機制傳輸應用層資料。

HTTPS提供之安全服務：
1.提供完整性。
2.雙方秘密通訊，達成機密性。
3.用戶端和伺服器端的參數協商。
4.用戶端和伺服器端的相互認證。

【版權所有，重製必究！】