

110 年公務人員高等考試三級考試試題

類 科：資訊處理
科 目：資通網路

曹勝老師解題

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)

1. 《考題難易》：★★
2. 《解題關鍵》：VPN/IPsec 基本題，掌握 IPsec 協定概念，搭配 106 國安特考、108 高考類似題即可完美作答。
3. 《命中特區》：資通網路講義 P608、P688 頁完全命中

【擬答】：

(一)IPsec 被設計用來提供 1.入口對入口通信安全，由單個節點提供分組通信的安全性給多台機器（甚至可以是整個區域網路）；2.端到端分組通信安全，由作為端點的電腦完成安全操作。並經由此二模式以構建虛擬私人網路（VPN）。IPSec 應用情境如下：

1. 傳輸模式（Transport mode）：僅加密或認證上層協定的資料，例如在區域網路中的兩台電腦 A 與 B，可直接建立連線（不必經由路由器或防火牆），且 A 與 B 具有處理 IPSec 封包的能力時，則可使用 IPSec 的傳輸模式。
2. 通道模式（Tunnel mode）：IPSec 會加密或認證整個封包，並在最外面再加上一個新的 IP 表頭，當 IPSec 連線兩端的電腦有一端或兩端不具處理 IPSec 封包能力，而必須透過具有 IPSec 能力的路由器或防火牆來代為處理 IPSec 封包時，即必須使用通道模式。

(二)在 VPN 網路上，都希望將內部的網路位址隱藏起來，並透過 NAT（Network Address Translator）將內部位址轉換到外部位址，區域網路透過 Internet 網路做 VPN 連接，並且將 IPSec AH Tunnel 與 NAT 軟體安裝於雙方網路的『安全閘門』（Security Gateway, SG）上，當內部網路 A 的工作站欲傳送封包給內部網路 B 的工作站時，SG-A 將工作站 A 所發送的封包經由 IPSec AH Tunnel 包裝。區域網路 B 的 SG-B 收到封包後，再拆解外部標頭，並從事認證的工作，如果認證無誤的話，便捨棄外部標頭，恢復原來封包格式，並發送到內部網路；工作站 B 再由網路上收到該封包。如此，對雙方工作站而言，並不知道有 VPN 網路的存在，猶如在同一區域網路上運作一樣。

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)

1. 《考題難易》：★★★★
2. 《解題關鍵》：DNSSEC 應用題，需要掌握 DNS 運作方式，搭配 103 調查局特考資訊安全實務科目類似題可以完美作答。
3. 《命中特區》：資管與資通安全講義 P573 完全命中

【擬答】：

(一)域名系統安全擴充（Domain Name System Security Extensions，DNSSEC）是 IETF 對確保由域名系統（DNS）中提供的關於網際網路協定（IP）網路使用特定類型的資訊規格套件。它是對 DNS 提供給 DNS 客戶端（解析器）的 DNS 資料來源進行認證，並驗證不存在性和校驗資料完整性驗證，但不提供機密性和可用性。

(二)DNSSEC 旨在保護應用程式（以及服務這些應用程式的快取解析器）免受偽造或不當操縱的 DNS 數據所造成的影響（例如域名伺服器快取污染的數據）。來自 DNSSEC 保護區的所有答案都經過數位簽章。通過檢驗數位簽章，DNS 解析器可以核實資訊是否與區域所有者發布的資訊相同（未修改和完整），並確係實際負責的 DNS 伺服器所提供。雖然保護 IP 位址的正確性是許多使用者關注 DNSSEC 的直接課題，DNSSEC 還可以保護 DNS 中發

公職王歷屆試題 (110 高考三級)

布的其他任何數據：包括文字記錄 (TXT) 和郵件交換記錄 (MX)，並可用於引導發布參照儲存在 DNS 中的加密憑證的其他安全系統：例如憑證記錄 (CERT 記錄, RFC 4398)，SSH 指紋 (SSHFP, RFC 4255)，IPSec 公鑰 (IPSECKEY, RFC 4025) 和 TLS 信任錨 (TLSA, RFC 6698)。

(三)DNSSEC 可防禦之攻擊

1. 資料完整性 (data integrity)

DNSSEC 使用數位簽章的技術，將每筆 RR 做簽章產生 RRSIG (Resource Record Signature)，而收到資料方可使用 Public Key + RRSIG 來驗證是否為原本詢問之 RR 紀錄，以此來驗證中間是否有被竄改。

2. 來源可驗證性 (origin authentication of DNS data)

在 DNSSEC 中，所謂的公正的第三方就是上層的 Domain DNS Server，也就是 DNS Server 必須將自己的 Public Key (DNSKEY) 做一次數位簽章後放在 Parent Zone Server，這種新的 RR(Resource Record) types 稱為 DS(Delegation Signer)，因此由 Parent Zone 中的 DS 紀錄可驗證 Child Zone 之 DNSKEY 確實是正確且未經竄改。

3. 可驗證之不存在性 (authenticated denial of existence)

將所有 DNS 紀錄依照字母排序，而在每個網址間加上一筆 NSEC 紀錄並做電子簽章。當查詢到不存在的網址時，DNSSEC 會回應 NSEC 紀錄，查詢者可比對 NSEC 紀錄中前後對應的字母來確認是否真的不存在，這就是所謂的“可驗證之不存在性”。

(四)DNSSEC 無法防禦之攻擊：

1. 隱密性(Confidentiality)

DNSSEC 傳遞的 RR & 及 RRSIG 傳輸過程皆未加密，因此中間可能被 sniffer 之設備或程式讀取。但被讀取不代表能假造，因為駭客並無 DNS Server 之 Private Key，因此無法假造出 RRSIG 的資料而不被發覺。

2. 服務可用性(Availability)

DNSSEC 僅是一項服務，若有駭客發動 DDoS 攻擊，不斷的詢問成千上萬個網址，則 DNS Server 可能因負荷過重而無法正常運作。不過這項弱點應是所有 Internet 服務皆共有的現象，而不單是 DNSSEC 之弱點。

志光學儒保成

工科人專屬學習規劃

精心安排完整豐富的上榜課程

工科考試所需要的資源，我們通通幫你準備好了

法科
架構班

學校沒教的，我們教給你！
名師精解法科知識，
結合實務例子，助你建構
法科概念。

扎實
正規班

完整堂數規劃，循序漸進學
習，讓您深度修習工科各專
業學科知識。

作文
實戰班

作文再也不是理工人的痛！
透過專業老師的輔導，快速
強化您的寫作架構、邏輯概
念。

主題
題庫班

主題式教學，搭配各類試題
演練，進行考點分析及破題
要點訓練，讓您短時間各科
實力倍增。

精華
總複習

考前重點總複習，精準掌握
重要考點，讓您考前實力突
飛猛進。

考前提要
關懷講座

名師考前最終提點，穩定你
累積許久的實力，讓你的觀
念更加清晰。

全國全真
模擬考

檢視應考實力、訓練臨場反
應、掌握最新考題趨勢，全
程比照考試時程，模擬考場
實戰氛圍，讓您能以平常心
應考！

工科
全科班

公職十國營完善循環課程規
劃，All in One課程一次到
位，奠定穩固基礎、強化上
榜實力。

109普考 電子工程
曾○維
一年考取

我是工科人，我工頂啦！

由於考試的題目非常靈活，參加題庫班，除了勤做考古題外，大量實作解說，很快地強化我的考前記憶，每做一道題目馬上能判斷是在哪一章節，然後再進行解題。

■完整課程資訊詳洽全國志光·學儒·保成門市■



為你專屬設計的學習模式， 讓你靈活學習、輕鬆準備！

我們都在 **志光學儒保成** 成功找到工科人的工頂人生

多元學習模式

- 面授學習**
直接，有效
→ 實際面對面教學，現場解決您的疑惑。
→ 優質專業名師，幫您統整、分析考試重點資訊。
→ 定期的大小測驗，您可隨時檢視學習效果。
- 雲端函授**
自主，彈性
→ 不用煩惱通勤問題，課程教材直接送到家。
→ 反覆聽課，不怕觀念聽不懂。
→ 完全自由，可自主安排學習進度。
- 視訊學習**
便利，專注
→ 安靜舒適的上課環境，提高您的專注力。
→ 看課時間能自由預約，無須擔心時間衝突。
→ 可依需求暫停、倒轉或快轉，深度學習超簡單。



專業名師指導，提升解題順暢度！
本以為適合閱讀，但發現穩定的生活才是我想要的。老師的教材都有明確分析與統整，再加上會由老師出申論題讓考生做練習，增加寫題目的敏感及順暢度。考前還有總複習課程，精準預測範圍、統整考前重點。
全國探花 李○庭 109年鐵路員級機械工程



選對好老師，中年轉職好順利！
我遭過公司裁員，覺得公職夠穩定，決定踏上國考之路。隔了20幾年重拾書本，選擇好的補習班讓我事半功倍。熱力學老師跟流體力學老師，我非常推崇，只要照著老師講的記下來、寫下來，這樣就夠了。
1年考取 古○芳 109年高考機械工程



題庫班老師的講解，對我幫助很大！
畢業後工作，累的要死薪水卻不怎麼樣。剛好朋友推薦鐵路特考，就挑戰看看。我覺得機械原理的題庫班對我幫助很大，跟著老師一起解，不懂的地方聽老師講解，覺得聽完很多疑問就會解開並且對我幫助很大。
優秀考取 謝○軒 109年鐵路佐級機械工程

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)

- 1. 《考題難易》：★★★
- 2. 《解題關鍵》：DDoS 進階應用題，掌握 DDoS 概念，配合 110 關務特考類似題即可作答。
- 3. 《命中特區》：資通網路講義 P611-612 DDoS 攻擊與防禦方式完全命中

【擬答】：

(一)分散式阻斷服務(Distributed Denial of Service, 簡稱 DDOS)攻擊是各種類型的攻擊，可以集中在一個特定的層。第 7 層攻擊專注於第 7 層功能，如 HTTP，SNMP，FTP 等。第 7 層攻擊需要比網絡層攻擊更少的帶寬和數據包來中斷服務。例如，像 SYN Flood 這樣的網絡層攻擊需要大量數據包來執行有效的 DDoS 攻擊。相反，數量有限的數據包可以大規模地進行 DDoS 攻擊。Layer7 DDoS 攻擊方式如：

1. HTTP Flood

是應用層 DDoS 攻擊中最突出的。當 HTTP 請求發送到服務器時，它會使用相當多的資源。因此，有限數量的這些數據包能夠利用所有的服務器資源。是以大量消耗系統資源為目的，通過向 IIS 這樣的網路服務程式提出無節制的資源申請來破壞正常的網路服務。旨在透過使 HTTP 伺服器無法處理請求來摧毀 HTTP 伺服器。如果伺服器受到數量超出其處理能力的請求轟炸，該伺服器會丟棄合法的請求，甚至會崩潰。

2. CC(Challenge Collapsar)攻擊

是指攻擊者借助代理伺服器類比真實使用者，不斷向目標網站發送大量請求，如頻繁請求某個動態 URL 或某個不存在的 URL，致使源站大量回源，耗盡網站伺服器性能，進而致使目標網站拒絕服務。

3. POST Flood 攻擊

攻擊者利用攻擊工具或者操縱僵屍主機，向目標伺服器發起大量的 HTTP POST 報文，消耗伺服器資源，使伺服器無法回應正常請求。

(二)防禦方式：

公職王歷屆試題 (110 高考三級)

1. 威脅情報庫

通過大資料分析平臺，即時匯總分析攻擊事件的日誌，提取攻擊特徵（如 IP、URL、User-Agent、Refer 等），並對這些特徵進行威脅等級評估，形成威脅情報庫，對於高風險性的 IP、UA、URL、Refer 等會自動下發到全網防護節點中，一旦後續請求命中威脅情報庫中的高風險性特徵，則直接攔截，最大限度地提高防禦效率，避免 CC 攻擊對網站的影響。

2. 個性化策略配置：

如請求沒有命中威脅情報庫中的高風險特徵，則通過個性化策略配置（如 IP 黑白名單、IP 訪問頻率控制）防禦攻擊；

3. 日誌自學習：

即時動態學習客戶網站的訪問特徵（如客戶每個資源的訪問量、行為特徵等），建立網站的正常訪問基線，一旦超過基線即進行阻擋。

志光學儒保成

公職工科+國營事業

1+1 更有力 準備公職的同時，可報考國營事業考試，善用重疊考科，一次準備就能多次上榜！

上榜路徑大公開！一年內超過8次上榜機會！

初等考	關務特考	鐵路特考	高普考	調查局特考
1月	4月	6月	7月	8月
●最易上手的公職考試	●考科少於同職等考試	●佐級錄取率最高 (110年因疫情延至9月)	●主流考試，缺額眾多 (110年因疫情延至10月)	●三等月薪76,000起 (110年因疫情延至10月)

地方特考	自來水評價人員	台電考試	中油僱員	國營事業職員級
12月	不定期舉辦	不定期舉辦	不定期舉辦	不定期舉辦
●考科同高普考	●只考選擇題	●考科少、好準備	●只考2科，多為選擇題	●國營退休潮，缺額多，工科類科競爭者少

錄取率高 109年 工科錄取率 最高達**19.42%**

電力工程	電子工程	機械工程	資訊工程
高考 19.42% 普考 17.33%	高考 9.04% 普考 9.39%	高考 18.27% 普考 13.70%	高考 12.92% 普考 10.47%

四、HTTP 乃應用層通訊協定，但未提供資料安全性。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)

1. 《考題難易》：★★
2. 《解題關鍵》：本題為 HTTPS/TLS 基本題，掌握 SSL/TLS 協定概念，參考 104 身障特考、110 國安特考類似題即可得解。
3. 《命中特區》：資通網路講義 P576-577、P676 完全命中

【擬答】：

- (一)超文本傳輸安全協定 (HyperText Transfer Protocol Secure, HTTPS) 是一種透過計算機網路進行安全通訊的傳輸協定。HTTPS 經由 HTTP 進行通訊，但利用 SSL/TLS 來加密封包。傳輸層安全性協定 (Transport Layer Security, TLS) 及其前身安全通訊協定 (Secure Sockets Layer, SSL) 是一種安全協定，目的是為網際網路通訊提供安全及資料完整性保障。
- (二)HTTPS 中的 TLS 使用 X.509 認證，之後利用非對稱加密演算來對通訊方做身分認證，之後交換對稱金鑰作為會談金鑰 (Session key)。這個會談金鑰是用來將通訊兩方交換的資料做加密，保證兩個應用間通訊的保密性和可靠性，使客戶與伺服器應用之間的通訊不被攻擊者竊聽。