《資訊管理與資通安全》

一、請回答下列有關網際網路與通訊網路問題：（25分）

(一)TCP/IP網路中，OSPF通訊協定是屬於那一層次架構？又其英文全名為何？

(二)TCP/IP網路中，HTTPS是屬於那一層次架構？又其英文全名為何？

(三)TCP/IP網路中，SSL是屬於那一層次架構？又其英文全名為何？

(四)網際網路上網址中.com與.org指的是什麼？

(五)請定義什麼是ADSL（含英文全名）？

試題評析	此題為基本的概念解釋題，同學只需要對基本概念有所掌握即可。

答：

(一)網路層（Internet Layer），開放式最短路徑優先（Open Shortest Path First）是一個基於IP協定的路由協定，用於在單一自治系統（autonomous system, AS）內利用Dijkstra最短路徑演算法來決策路由路徑。

(二)應用層（Application Layer），超文本傳輸安全協定（HyperText Transfer Protocol Secure）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。HTTPS開發的主要目的，是提供對網站伺服器的身分認證，保護交換資料的隱私與完整性。

(三)傳輸層（Transport Layer），安全通訊協定（Secure Sockets Layer）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。

(四)此為頂級網域（Top-level Domain, TLD）為域名的最後一個部份，即是域名最後一點之後的字母，其中「com」是commercial的縮寫，代表商業性的網站。「org」為organization的縮寫，在創立時主要供給非營利組織、國際組織...等使用，現在已經沒有任何限制，可以用於任何場合，包括盈利和非營利組織、機構、團體。

(五)非對稱數位使用者線路（Asymmetric Digital Subscriber Line），ADSL因為上行（從使用者到電信服務提供商方向，如上傳動作）和下行（從電信服務提供商到使用者的方向，如下載動作）頻寬不對稱（即上行和下行的速率不相同）因此稱為非對稱數位使用者線路。它採用分頻多路復用技術把普通的電話線分成了電話、上行和下行三個相對獨立的頻道，從而避免了相互之間的干擾。

二、請寫出下列防火牆（Firewall）之定義與其相關問題：

(一)請定義什麼是防火牆？並寫出防火牆之四項主要的功能？（17分）

(二)請說明系統或網路管理師管控防火牆時，為什麼必須先了解應用層（Application layer）中那一些通訊協定之應用埠（Port）可被使用？（8分）

試題評析	此題為防火牆的基本考題，針對第一小題只要掌握基本概念即可。第二小題是經過一點轉化，同學在答題上要與網路應用層的說明還有應用服務的提供融會貫通即可回答。
考點命中	《高點・高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁67-70。

答：

(一)

防火牆是一個架設在網際網路與內網之間的資安系統，根據持有者預定的策略來監控往來的傳輸。防火牆可能是一台專屬的網路裝置，也可執行於主機之上，以檢查各個網路介面的網路傳輸。它是目前最重要的一種網路防護裝置，從專業角度來說，防火牆是位於兩個或以上網路間，實行網路間存取或控制的一組元件集合之硬體或軟體。

主要四項功能為：

1.入侵檢測功能：主要有反埠掃描、檢測拒絕服務工具、檢測伺服器入侵、檢測木馬或網路蠕蟲攻擊、檢測緩衝區溢位攻擊等功能，可以極大程度上減少網路威脅因素的入侵，有效阻擋大多數網路安全攻擊。

2.網路地址轉換功能 / 代理伺服器（Proxy Server）：利用防火牆技術可以有效實現內部網路或者外部網路的IP地址轉換，可以分為源地址轉換和目的地址轉換。源地址轉換主要用於隱藏內部網路結構，避免受到

【版權所有，重製必究！】

來自外部網路的非法訪問和惡意攻擊，有效緩解地址空間的短缺問題，而目的地址轉換主要用於外網主機訪問內網主機，以此避免內部網路被攻擊。有些防火牆會用代理伺服器來做到類似之功能，在使用者與網路之間提供一個中間人服務或代理伺服器，例如組織內的使用者想要存取網路上的資源，就會透過此代理伺服器和網路上的資源溝通與交換資料。

3.網路操作的審計監控功能：通過此功能可以有效對系統管理的所有操作以及安全資訊進行記錄，提供有關網路使用情況的統計資料，方便計算機網路管理以進行資訊追蹤。

4.強化網路安全服務：防火牆技術管理可以實現集中化的安全管理，將安全系統裝配在防火牆上，在資訊訪問的途徑中就可以實現對網路資訊保安的監管。

(二)

目前有許多的攻擊手法是透過應用層（Application Layer），而Port（埠）在一個電腦操作系統中扮演通訊的端點（endpoint）。每個通訊埠都會與主機的IP地址及通訊連線使用的協定相關。一個通訊階段作業（communications session）的完成，除了需要資料來源及目標位址外，還需要指定通訊埠才能完成。

駭客利用這個特性將有害的流量偽裝成合法流量進而竊取有利的資訊，而透過了解每個port所代表的是哪個應用層協定，可以有效地將沒有用到的port或是有害的流量直接阻擋在外面，讓系統免於被駭客攻擊。

三、任何組織的應用資訊系統於網路安全控制上，資安或系統工程師必須定期或即時執行風險評估，來了解其資訊安全機制是否需改善以減輕其風險，請說明資訊系統之風險會因那三項主要的情境改變而有所變化？（25分）

試題評析	資訊風險評估是近幾年來常出現的題目，這類型的題目考試範圍非常廣泛，從辨識、評估到這題所考的再評估，都是需要針對風險評估有全面的理解才可以較好回答。在考場中，此題回答的重點為掌握資安風險因素即可。

答：

風險值的計算為評估事件發生機率及影響程度後，根據此計算出相對應的數值。其算法為「風險值=資訊資產價值 x 威脅等級 x 弱點等級」，故針對三者變動時需要再評估。

1.資訊資產價值

資訊資產在識別的時候，可以根據資產CIA的特性下去考量：

(1)機密性（Confidentiality）：資訊不得被未經授權之個人、實體或程序所取得或揭露的性質。

(2)完整性（Integrity）：對資訊之精確與完整安全保證的性質。

(3)可用性（Availability）：已授權實體在需要時可存取與使用資訊之性質。

通常會依照此三特性再去區分不同等級用以判斷。

2.威脅

威脅可能對系統、組織或資產造成一個有害的事件，例如：

(1)天然災害：颱風、地震、水災及停電等，可能威脅到資訊資產的可用性及完整性。

(2)為因素：非法存取資料、偷竊及竄改資料等，可能威脅到資訊資產的可用性及機密性

3.弱點

弱點存在於資產本身，並不會造成傷害。但如果沒有妥善管理，將促使威脅形成。例如：

(1)人員教育訓練不足。

(2)系統漏洞

四、請定義大數據（Big Data）中5V的意義；以及進行大數據分析（Big Data Analytics）時處理的程序（Process），請依順序說明應含那些步驟以期獲得較佳的分析結果？（25分）

試題評析	此題也是大數據的基本題型，掌握大數據的基本概念與處理流程即可迎刃而解。
考點命中	《高點・高上資訊管理與資通安全》第二回，蕭老師編撰，頁76-78。

答：

(一)

【版權所有，重製必究！】

大數據中的5V為：

1. 大量化（Volume）：非結構數據的超大規模和增長，總數據的80~90%，比結構化數據增長快10倍到50倍，是傳統數據倉庫的10倍到50倍。
2. 價值化（Value）：大量的不相關信息，對未來趨勢與模式的可預測分析，深度複雜分析。
3. 多樣化（Variety）：大數據的異構和多樣化，很多不同的形式（文字、圖像、影片、機器數據），無模式或者模式不明顯，不連貫的語法或句義。
4. 快速化（Velocity）：實時分析而非批量式分析，數據輸入，處理與丟棄，立竿見影而非事後見效。
5. 真實性（Veracity）：大數據中的內容是與真實世界中的發生息息相關的，研究大數據就是從龐大的網絡數據中提取出能夠解釋和預測現實事件的過程。

(二)

一般而言，大數據處理流程，可分為以下四步驟：

1. 數據採集：在大數據的數據的收集強調數據全體性、完整性，而不是抽樣調查。在大數據的採集過程中，其主要特點和挑戰是併發數高，比如每年的雙十一，淘寶都會有上百萬的用戶同時訪問，如何保證訪問順利，這就需要大量的資料庫支撐，依靠合理的分流、公有雲等架構方法，保證每一個數據的準確有用。
2. 數據導入和清洗處理：採集好數據，肯定不少是重複或是無用的數據，此時需要通過數據對數據進行處理，將這些來自前端的數據導入到集中的大型分散式資料庫，或者分散式儲存集群，並進行簡單的清洗和預處理工作。而這個過程當中最大的挑戰就是導入的數據量大，經常會達到百兆，甚至千兆級別。
3. 數據統計和分析：統計與分析很多是需要用到工具來處理，比如可視化工具、演算法模型和分類匯總來滿足企業的數據分析需求。這個過程最大的特點就是目的清晰，按照一定規則去分類匯總，才能得到有效分析，這部分處理起來也很占用系統資源。
4. 數據挖掘應用：數據最終目的無疑就是透過數據挖掘背後的聯繫，分析原因找出規律然後應用到實際業務中，前面幾個步驟的數據經過各種算法，計算分析然後提取出預測的結果，大膽假設，數據支持，然後驗證得出結論。該過程的挑戰主要是挖掘的演算法很複雜，並且計算涉及的數據量和計算量都很大。

大數據實現過程基本至少是需要這四個流程，不過其中的細節、工具的使用、數據的完整性等更需要結合業務、行業特點和整個時代變化而不斷變化更新，才能符合大數據時代的特點。

【版權所有，重製必究！】