《資通網路與安全》

一、請說明軟體定義網路（Software-Defined Networking, SDN）的三層基本架構與核心理念，並分析其對傳統網路管理與資安策略帶來的影響。（25分）

試題評析	為近年命題熱門的SDN考題。
考點命中	《高點・高上網路講義》第4章，張又中編撰，頁4-21。

答：

(一)軟體定義網路（Software-Defined Networking, SDN）是一種新的網路架構，其將路由器的控制平面 (Control Plane) 從資料平面 (Data Plane) 中分離出來，並以軟體方式實作。此架構可讓網管人員在不更動硬體裝置的前提下，以中控方式用程式重新規劃網路。目前的主流有ForCES與OpenFlow。Facebook、Google都在其資料中心使用OpenFlow協定，並成立開放網路基金會來推動此技術。

其三層基本架構如下：

應用層 Application Layer	包含企業應用程式，與控制層的溝通以API來達成。
控制層 Control Layer	SDN控制軟體所在，提供網路架構修改、變更網路協定等服務。
基礎架構層 Infrastructure Layer	網路裝置的硬體建置，與控制層透過控制平面與資料平面之介面進行溝通。

(二)對傳統網路管理與資安策略帶來的影響如下：

1.大幅簡化網路管理。

2.易於更新通訊協定。

3.直覺維護網路架構。

二、企業常透過網路位址轉譯（Network Address Translation, NAT）技術來節省公有IP位址，然而在進行內部服務外部化（例如公開Web、Mail、VPN等伺服器）時，NAT設計可能帶來一些限制或挑戰，請說明兩項限制或挑戰並提出對應的兩種解決方法。（25分）

試題評析	典型NAT考題。
考點命中	《高點・高上網路講義》第3章，張又中編撰，頁3-14。

答：

組織內部有多台主機，然只有少量公開IP位址，可於組織內部的多台主機使用內部IP，並透過NAT將內部IP與外部IP作對應轉換。

NAT設計可能的限制或挑戰及可對應的解決方法有：

1.增加交換路徑的延遲

採用Open NAT，惟可能造成資安風險。

2.並非所有應用程式都支援

透過啟用路由器之UPnP Universal Plug and Play)，來解決應用程式不支援NAT的問題。

三、請說明社交工程攻擊與技術性攻擊（如惡意程式、SQL Injection）在手法與防禦策略上的差異，並分析企業若僅依賴技術防禦可能面臨的風險。（25分）

試題評析	屬社交工程之分析比較題型。
考點命中	1.《高點・高上資訊安全實務講義》第2章，張又中編撰，頁2-20~21。 2.《高點・高上資訊安全實務講義》第3章，張又中編撰，頁3-13。

答：

(一)社交工程(Social Engineering)係指利用人性弱點、人際交往或者互動特性所發展出來的一種攻擊方法。早期社交工程是使用電話或者其他非網路的方式來詢問個人資料；而目前社交工程大多利用電子郵件、即時通訊軟體、社群網站、網頁或簡訊來進行攻擊。

技術性攻擊以SQL Injection為例，則是透過寫入特殊SQL程式碼來發動攻擊，由於此種方式是經由標準且既定的程序操作，輸入具破壞性的SQL程式碼，對現階段的防火牆或是防駭系統而言難以防範。

(二)綜合以上，我們瞭解社交工程攻擊與技術性攻擊在手法與防禦策略上的差異，在於社交工程的攻擊方法，主要是

針對人性弱點，非僅為技術防禦，故企業若僅依賴技術防禦，仍然有可能發生資安事件，因而導致企業損失，故可進行如社交工程演練，提升員工對於社交工程的警覺。

社交工程的防禦方法如下：

1.不點選、開啟來路不明的郵件、網頁或簡訊。

2.不加入即時通訊軟體、社群網站不明身份的好友或回復不明訊息。

3.安裝防毒軟體並更新病毒碼。

4.取消郵件預覽功能。

5.以純文字模式開啟郵件。

6.設定垃圾郵件過濾機制。

7.關閉郵件自動下載圖片及其他內容。

四、企業在面對重大資安事件（如勒索病毒入侵或大規模資料外洩）時，若無有效的資安事件應變計畫，可能產生那些影響？請舉例說明，並提出具體改善建議。（25分）

試題評析	資安事件應變計畫，屬於策論題型，可整合理論與實務提出完整論述。
考點命中	《高點・高上資訊安全實務講義》第2章，張又中編撰，頁2-5。

答：

(一)勒索病毒(Ransomware)分為鎖定受害者電腦的非加密型，以及系統性加密受害者檔案的加密型。其要求受害者繳納贖金，以取回電腦的控制權或是加密金鑰。通常透過特洛伊木馬，將自身掩蓋為看似無害的檔案。

若企業在面臨重大資安事件時（如勒索病毒入侵或大規模資料外洩）缺乏有效的應變計畫，可能造成以下影響：

1.業務中斷。

2.財務損失。

3.法律責任。

4.品牌形象受損。

5.失去客戶信任。

(二)有效的資安事件應變計畫是企業不可或缺的防禦機制。勒索病毒發生或大規模資料外洩時的緊急應變措施如下：

1.中斷網路連線。

2.立即關閉主機。

3.緊急清查與宣導。

4.評估災情與救援。

5.重灌系統與相關軟體。

以台灣中油於2020年5月4日遭受的勒索病毒攻擊為例，該勒索病毒將營運資料加密，導致相關系統一度停擺，甚至緊急切斷網路影響全臺加油站的服務。具體改善建議為可透過事先規劃、演練和持續改進，企業方可將資安事件的負面影響降至最低，以確保業務的持續運作和長期發展。

高點・高上公職

考取學長姊大推的優秀師資

資料結構

王致強(蕭立人)

- 獨創「程式碼記憶法」，大幅縮短記憶　和答題的時間！
- 教學採考題導向，範圍由淺入深，即使是底子不好，也能茅塞頓開！

廖○成(高大資管畢)

應屆考取　113高考資訊處理

資料結構要掌握這門科目對我來說非常不容易，**不過王致強老師教得非常好**，教學中有時候連比國考難的研究所考題都會提點，也讓大家能夠掌握國考所需再更以上的資料結構實力，我覺得非常不錯！

資通安全

金乃傑(魏取向)

- 以「學習地圖」概念展現資訊管理多構面的知識，並引入自創圖示標記知識所在位置及相連概念；輔以口訣背誦關鍵名詞、要點。

蔡○諺(中興應數畢)

跨域考取

113高考資訊處理【狀元】

題庫班專注於實戰演練，通過不斷作題，能更快適應考試題型，並且針對薄弱環節進行強化。**金乃傑老師在今年考試中預測的範圍非常準確**，特別是在加密演算法與資料保護法規的部分，考題幾乎全中。

資訊管理

蕭維文

- 具有產業與學術經驗，從不同角度提供最客觀的科技觀點。
- 時事與理論精準結合科技產業，透過精闢分析讓同學理解資訊界。

李○翌(北市大資科畢)

應屆考取

113高考資訊處理、普考資訊處理

資訊管理這科廣到沒有範圍，如果有寫考古題就會發現講義是由各種考古題的解答堆疊出來的，因此**蕭維文老師的魚骨解答法就顯得非常重要**，只需把改卷教授想要的關鍵字搭配以上的方法就可以把答案湊出來。

更多命中實證

更多上榜經驗分享

考點命中實證

《資料結構》

一、某一公司有下圖所示的8個優先順序分別為高或低的待執行工作，且將依順序自A至H每間隔一天的時間放入對應的高優先執行佇列（Qucue）或低優先執行佇列（Qucue），例如A（低）表示A工作排於第一天放入低優先執行佇列，而C（高）表示C工作排於第三天放入高優先執行佇列。此外，執行每個工作所需完成的時間均於工行名稱下顯示，例如執行A工作需要2天時間完成，而執行B工作需要1天時間完成。最後，各個工作的執行規則為，當高優先執行佇列內有工作待完成時，須優先執行該佇列內的工作（由第一個開始執行），直到高優先執行佇列內沒有任何待完成工作時，才可執行低優先執行佇列內的工作（由第一個開始執行）。

自A至H每間隔一天的時間放入對應的高優先佇列或低優先佇列

H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
1	2	1	1	2	2	1	2

（一）試計算執行此8個工作需要多少天方可完成。（10分）

（二）試計算此8個工作自放入佇列至開始執行的平均等待時間。（15分）

試題評析　佇列相關的基本應用問題，題目本身十分平易。在題意確實掌握的狀況下，正常操作佇列，計算正確時間，取分不難。

考點命中　《資料結構》，高點文化出版，王致強編著，頁4-16～4-17。

答：

（一）總共需要12天可以完成8個工作，如下圖：（灰底為執行中工作，括號為工作剩餘天數）

天數	12	11	10	9	8	7	6	5	4	3	2	1
到達工作					H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
所需天數					1	2	1	1	2	2	1	2
高優先佇列				G(1)	G(2)	G(2)E(1)	F(1)D(1)	D(2)	D(2)C(1)	C(2)		-
低優先佇列	H(1)	H(1)E(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	E(1)B(1)	E(1)B(1)	E(1)B(1)	B(1)	B(1)	B(1)A(1)	A(2)

（二）各項工作等待時間如下表：

工作	H	G	F	E	D	C	B	A
等待時間	4天	1天	1天	6天	1天	0天	8天	0天

《資通網路與安全》

五、防火牆（Firewall）是當今企業常見的安全防護設備，請問：

（一）企業常用防火牆隔離出一個網段，稱為DMZ（Demilitarized Zone），請詳細說明其用意為何。（5分）

（二）WAF（Web Applicatiou Firewall）和傳統的封包過濾式防火牆（Packet filtered Firewall）有何不同？請詳細說明。（10分）

（三）防火牆常根據從外部收到的IOC（Indicator of Compromise）來做規則調整，請問IOC的意義為何？（5分）

試題評析　本題為資訊安全之防火牆種類及安全網路架構之題型。

考點命中　《高點・高上資通安全講義》第二回，金乃傑編撰，頁14～28，第三章防護架構，二、防火牆（Firewall）與相關技術。

答：

（一）DMZ（Demilitarized zone）是介於內外路由器間的區域，用於放置組織對外重要的伺服器。DMZ 照字面直翻是指非軍事區域，而電腦網路中 DMZ 可以解析為一個既不屬於內部網域同時也不屬於外部網域的一個特殊區域，其目的就是了為防止外來人侵者直接存取內部機密資料，針對不同資源而提供不同安全級別的保護區域。一般企業將網路伺服器放在 DMZ 供網際網路使用者查詢使用，這些伺服器無法連接到內部資料，因此如果不幸被外來人侵者侵入，重要的資料仍不至於外洩。

（二）WAF（Web Application Firewall）提供應用層的訊息過濾與轉送處理，主要依據應用層的資訊來決定是否放行封包流量，與傳統的封包過濾式防火牆相較，WAF 可過濾傳送的資料內容與命令，確保應用層協定的安全；亦可過濾封包內容與命令，阻斷針對應用協定的攻擊。

（三）IOC 為電腦鑑識中的工具器物(Artifact)，其可從網路或作業系統中觀察，與電腦入侵高度相關。傳統的 IOC 包含病毒特徵、IP 位址、惡意檔案的 MD5 雜湊值，或是殭屍網路(Botnet)命令與控制伺服器的網址或網域名稱。通過事件回應與電腦鑑識的處理過程識別 IOC 後，其可用於入侵檢測系統(Intrusion Detection System, IDS)與防病毒軟體，對未來的攻擊嘗試進行早期檢測。