【L21 資訊安全規劃實務樣題】

（D）	1. （單選題）關於 MS-SQL 資料庫的存取控制設計，下列敘述何者較符合安全設計？ (A) 資訊系統開發運作，使用 SA 做為資訊系統存取資料庫的帳號及密碼，符合資料庫安全存取設計 (B) MS-SQL 系統可以建立多個資料庫，滿足不同資訊系統需求，所以可以讓不同委外開發商之資訊系統，共用同一組帳號密碼來存取不同資料庫，符合資料庫安全存取設計 (C) 某資訊系統有其前台系統（讀取）與後台管理系統（讀寫刪除）對資料庫進行存取，前台管理系統與後台管理系統可以共用同一個 DBO 帳號與密碼 (D) 資訊系統所使用資料庫若採用 Microsoft Azure 上的 PaaS MS-SQL 資料庫服務 （非自建虛擬機再另行安裝的 MS-SQL 資料庫系統），該雲端 PaaS MS-SQL 是無法使用 SA 帳號密碼
*答案解析：Microsoft Azure 上的 PaaS MS-SQL 資料庫 SA 權限因安全考量，微軟不提供 SA 權限供使用者使用，可參考 Microsoft Azure PaaS MS-SQL 管理原則	

（D）	2. （單選題）在 OWASP 的最新 TOP10 IoT 資安威脅中，下列何者問題最為嚴重？ (A) 不安全的網路服務 (B) 缺乏安全的更新機制 (C) 不安全的元件 (D) 預設或容易猜測的通行碼
*答案解析：OWASP TOP10 裡 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project	

（A） （C） （D）	3. （複選題）某集團業務行政人員，收到外部訂單資料，未依據資安規範，確認信寄來源，便開啟郵件 pdf 附件，以及點開信中 URL 連結，以致該員工電腦感染蠕蟲，且被該員工電腦通訊錄名冊資料被竊取或竄改，造成公司郵件資料外洩，進而偽造該員工郵件信箱寄出相關惡意郵件給通訊錄成員，擴大資料外洩風險，請問下列敘述何者為風險處理的程序？ (A) 該員工通報資資安事件，並由 IT 接手後續處理，並通知全公司 (B) 該員工的電腦，由該員自行進行掃毒，不另行通知資安人員 (C) IT 需確認該員資料，有進行符合公司規定之備份 (D) 需進行全公司資安教育宣導以及進行政策性全公司掃毒
*答案解析：需通報資安人員，進行其他防護與攔阻處置	

【題組題】

《情境說明》 王先生使用是網路購物已長達 10 年以上，ABC 線上購物是王先生最常使用的平台，最近幾年，ABC 線上購物更把服務範圍擴展至全球，美國、加拿大和歐洲各國都成立分公司，且這些國家的會員數，也佔 ABC 線上購物的 20%以上，王先生常接到莫名其妙的推銷電話，也偶爾會接到一些詐騙電話，上網查詢後，才發現 ABC 線上購物的客戶資料庫個資外洩，共有 2 萬多名用戶，共計超過 10 萬筆的資料受到影響。	
（C）	(1) （單選題） 在這次個資外洩事件中，王先生對自己的損失？ (A) 不能求償，因為就現況來說，並未造成具體損害 (B) 不能求償，因為網購公司不屬於八大行業 (C) 可以求償，並可以透過團體訴訟的方式提起損害賠償訴訟 (D) 可以求償，但必須自己尋找律師提起損害賠償訴訟
（C）	(2) （單選題） ABC 線上購物查明資料外洩原因後，下列何項處置較不適當？ (A) 先需再確認當事人是否有實質金錢損失，才能決定如何處置 (B) 於當事人來詢問時，由專人回答 (C) 依法，一定要以電話或信件通知當事人 (D) 依法，以適當方式通知當事人即可
（B）	(3) （單選題）若 ABC 公司為了業務分析，會將統計資料完全去識別化之後，進行大數據分析，在接獲使用者以電話或信件通知，要求刪資料，請問下列敘述何者正確？ (A) 當事人資料必須刪除，統計數據也須刪除 (B) 當事人資料必須刪除，統計數據無需刪除 (C) 當事人資料無需刪除，統計數據須刪除 (D) 當事人資料無需刪除，統計數據也無需刪除
（A）（B） （C）（D）	(4) （複選題）ABC 線上購物，若為了增加業績，開始增加實體店面，請問，在實體店面，進行「告知」使用者個資法要求事項，下列何者為符合個資法要求的方式？ (A) 言詞並留下相關紀錄 (B) 電子郵件 (C) 簡訊 (D) 紙本書面

【L22 資訊安全防護實務樣題】

（B）	1. （單選題） 關於 SQL Injection 攻擊的防護，下列何者較佳？ (A) Https 安全連線 (B) ModSecurity (C) 網路層防火牆 (D) 計算雜湊函數值
*答案解析：Modsecurity 為應用層防火牆	

（B）	2. （單選題） M 公司授權進行內部網路的安全活動，相關人員於過程中使用 Nmap 進行掃描，發現有內部主機使用 vsftpd2.3.4，經判斷後發現具備漏洞可利用，後續使用 Msfconsole 成功利用漏洞。請問上述情境說明為進行下列何者？ (A) 弱點掃描 (B) 滲透測試 (C) 社交工程 (D) 封包竊聽
*答案解析：掃描發現漏洞，並進一步確認與利用漏洞，故為滲透測試。	

（B）	3. （單選題） 為數位證據進行雜湊值（Hash）是為了下列哪些目的？ (A) 機密性 (B) 完整性 (C) 可用性 (D) 可歸責性

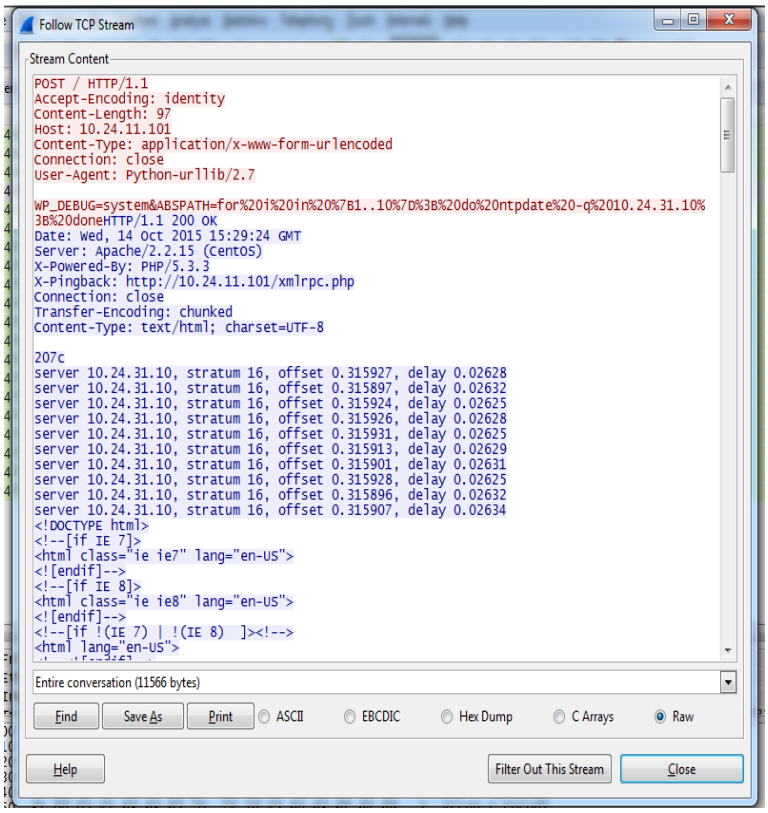
【題組題】

《情境說明》

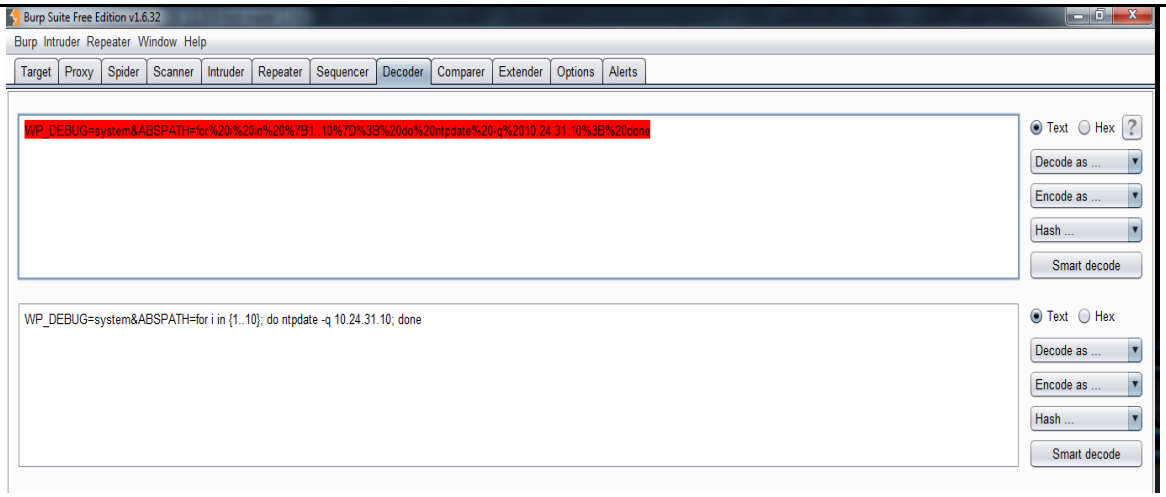
XYZ 企業接獲大量員工通報：許多主從式架構 （Client-Server Mode） 之應用服務無法正常使用。系統管理人員確認其應用程式伺服器皆正常，因此著手進行網路流量分析期望能發現問題。

No.	Time	Source	Destination	Protocol	Length	Info
1	2015-10-14 11:28:43.786109	10.24.11.101	10.2.2.2	SSH	194	Encrypted response packet len=128
2	2015-10-14 11:28:43.787049	10.2.2.2	10.24.11.101	TCP	66	52751 > ssh [ACK] Seq=1 Ack=129 Win=814 Len=0 TSval=2825
3	2015-10-14 11:28:45.169094	CtrixsIn_0a:00:00	PVST+	STP	64	RST. Root = 32768/3251/00:0d:ec:f1:38:fc Cost = 0 Port
4	2015-10-14 11:28:47.169820	CtrixsIn_0a:00:00	PVST+	STP	64	RST. Root = 32768/3251/00:0d:ec:f1:38:fc Cost = 0 Port
5	2015-10-14 11:28:48.179873	10.2.2.100	10.24.11.101	TCP	74	54843 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PI
6	2015-10-14 11:28:48.179987	10.24.11.101	10.2.2.100	TCP	74	http > 54843 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=
7	2015-10-14 11:28:48.181005	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=207
8	2015-10-14 11:28:48.181083	10.2.2.100	10.24.11.101	HTTP	142	GET / HTTP/1.1
9	2015-10-14 11:28:48.181190	10.24.11.101	10.2.2.100	TCP	66	http > 54843 [ACK] Seq=1 Ack=77 Win=14592 Len=0 TSval=48
10	2015-10-14 11:28:48.429040	10.24.11.101	10.2.2.100	TCP	2962	[TCP segment of a reassembled PDU]
11	2015-10-14 11:28:48.429281	10.24.11.101	10.2.2.100	TCP	2962	[TCP segment of a reassembled PDU]
12	2015-10-14 11:28:48.429513	10.24.11.101	10.2.2.100	TCP	2962	[TCP segment of a reassembled PDU]
13	2015-10-14 11:28:48.429656	10.24.11.101	10.2.2.100	TCP	571	[TCP segment of a reassembled PDU]
14	2015-10-14 11:28:48.430184	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=2897 Win=35072 Len=0 TSval=
15	2015-10-14 11:28:48.430305	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=4345 Win=37888 Len=0 TSval=
16	2015-10-14 11:28:48.430461	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=5793 Win=40832 Len=0 TSval=
17	2015-10-14 11:28:48.430516	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=7241 Win=43776 Len=0 TSval=
18	2015-10-14 11:28:48.430582	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=8689 Win=46592 Len=0 TSval=
19	2015-10-14 11:28:48.430644	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=9194 Win=49536 Len=0 TSval=
20	2015-10-14 11:28:48.445966	10.24.11.101	10.2.2.100	TCP	1514	[TCP segment of a reassembled PDU]
21	2015-10-14 11:28:48.446018	10.24.11.101	10.2.2.100	HTTP	79	HTTP/1.1 200 OK (text/html)
22	2015-10-14 11:28:48.446277	10.24.11.101	10.2.2.100	TCP	66	http > 54843 [FIN, ACK] Seq=10655 Ack=77 Win=14592 Len=0
23	2015-10-14 11:28:48.447068	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=10642 Win=52480 Len=0 TSva
24	2015-10-14 11:28:48.447109	10.2.2.100	10.24.11.101	TCP	66	54843 > http [ACK] Seq=77 Ack=10655 Win=52480 Len=0 TSva
25	2015-10-14 11:28:48.447794	10.2.2.100	10.24.11.101	TCP	66	54843 > http [FIN, ACK] Seq=77 Ack=10656 Win=52480 Len=0
26	2015-10-14 11:28:48.447822	10.24.11.101	10.2.2.100	TCP	66	http > 54843 [ACK] Seq=10656 Ack=78 Win=14592 Len=0 TSva

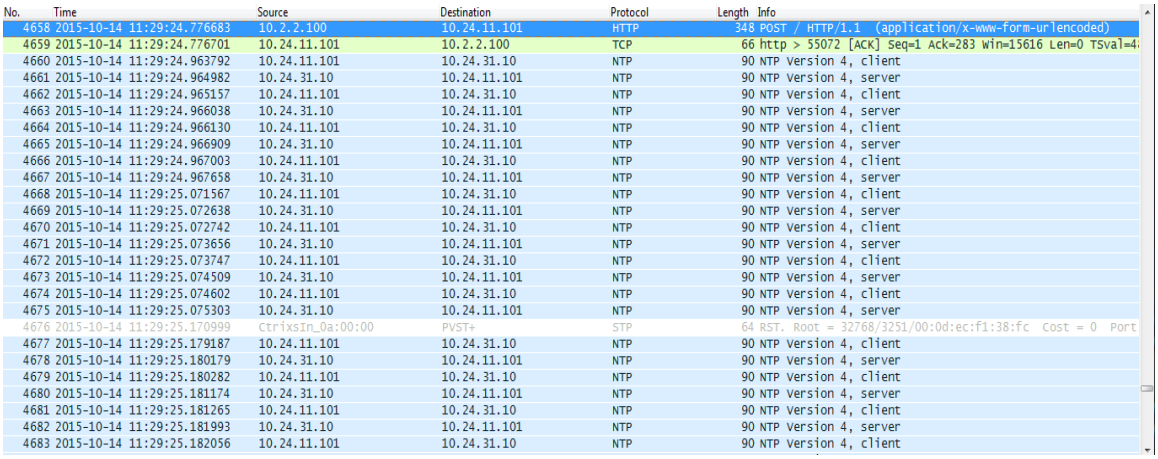
（圖一）



（圖二）



（圖三）



No.	Time	Source	Destination	Protocol	Length	Info
4658	2015-10-14 11:29:24.776683	10.2.2.100	10.24.11.101	HTTP	348	POST / HTTP/1.1 (application/x-www-form-urlencoded)
4659	2015-10-14 11:29:24.776701	10.24.11.101	10.2.2.100	TCP	66	http > 55072 [ACK] Seq=1 Ack=283 Win=15616 Len=0 TSval=4
4660	2015-10-14 11:29:24.963792	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4661	2015-10-14 11:29:24.964982	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4662	2015-10-14 11:29:24.965157	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4663	2015-10-14 11:29:24.966038	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4664	2015-10-14 11:29:24.966130	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4665	2015-10-14 11:29:24.966909	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4666	2015-10-14 11:29:24.967003	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4667	2015-10-14 11:29:24.967658	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4668	2015-10-14 11:29:25.071567	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4669	2015-10-14 11:29:25.072638	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4670	2015-10-14 11:29:25.072742	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4671	2015-10-14 11:29:25.073656	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4672	2015-10-14 11:29:25.073747	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4673	2015-10-14 11:29:25.074509	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4674	2015-10-14 11:29:25.074602	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4675	2015-10-14 11:29:25.075303	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4676	2015-10-14 11:29:25.170999	CtrixsIn_0a:00:00	PVST+	STP	64	RST. Root = 32768/3251/00:0d:ec:f1:38:fc Cost = 0 Port
4677	2015-10-14 11:29:25.179187	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4678	2015-10-14 11:29:25.180179	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4679	2015-10-14 11:29:25.180282	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4680	2015-10-14 11:29:25.181174	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4681	2015-10-14 11:29:25.181265	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client
4682	2015-10-14 11:29:25.181993	10.24.31.10	10.24.11.101	NTP	90	NTP Version 4, server
4683	2015-10-14 11:29:25.182056	10.24.11.101	10.24.31.10	NTP	90	NTP Version 4, client

（圖四）

（A）	(1) （單選題）本情境中，於下列何種資訊、網路設備進行流量分析能有效發現問題？ (A) 網路設備，例如： 核心交換機 （Core Switch） (B) 資訊設備，例如： 應用程式伺服器 （Application Server） (C) 資訊設備，例如： 終端電腦 (D) 終端設備，例如：手機
（C）	(2) （單選題）本情境中，系統人員進行網路封包擷取後，使用分析軟體打開其內容 （圖一）， 下列敘述何者正確？ (A) 10.24.11.10 對 10.2.2.2 發起 SSH 連線 (B) SSH 封包無需進行解密即可查詢其傳輸資料 (C) 10.2.2.100 試圖對 10.24.11.101 發起 HTTP GET Request (D) 10.2.2.100 為 HTTP 伺服器
（B）	(3) （單選題）本情境中，系統人員轉交相關資訊給資安人員分析， 發現其中有可疑 HTTP Request （圖二）。下列敘述何者不正確？

	(A) 此 HTTP Requst 使用 POST Method (B) 來源用戶端所使用為常見網頁瀏覽器 （Web Browser） (C) 目的應用程式為 PHP 所開發 (D) 目的網頁伺服器 （Web Server） 為 Apache
（C）	(4) （單選題）本情境中，資安人員觀察到該 HTTP Request 中可疑參數 （Parameter） （圖三） ，並綜合其他封包分析 （圖四） 可進行推論。下列敘述何者正確？ (A) 校時伺服器 （NTP Server） 被攻陷 （Comprise） 並成為 C&C 伺服器，嘗試控制用戶端 (B) 校時伺服器 （NTP Server） 被攻陷 （Comprise） 成為 C2 伺服器，開始攻擊用戶端 (C) 攻擊者對校時伺服器 （NTP Server） 伺服器發起阻斷服務 （DoS） 攻擊 (D) 應用程式伺服器 （Application Server） 對校時伺服器 （NTP Server） 發起阻斷服務 （DoS） 攻擊
答案解析： （1）於交換機上能收集各網段 （Subnet） 之流量，能有效分析問題 （3）從 User-Agent 中可觀察此 HTTP Request 為使用 Python 之 urllib 模組所產生，非正常 Web browser （4）從圖 2, 3 中可觀察傳入參數 ABSPATH 的值 Decode 後，其為 Shell script 使用迴圈方式執行 NTP 查詢指令；綜合圖 4 確實有大量連線記錄。	