明逸認證測驗中心

資訊安全專業認證

資訊技術類

參考試題編號：ISP(T)-IT-A-01-20211103

補充事項：

一、 本參考試題約佔考題 40%~50%比例。

二、 正式考試將由此試題隨機抽 20 題，選項將可能會有不同組合或變化。

三、 試題採不定期新增。

認證科目：資訊安全專業認證-資訊技術

一、選擇題(multiple choice)

第 1 題

請問 SSH (Secure Shell) 服務預設是使用哪一個連線 Port？而實務上我們會將此 Port 設定成？(請選擇以下最佳答案)

(A). SSH 預設為 21 Port，實務上採用預設較為方便，並將 root 帳戶停用。
(B). SSH 預設為 80 Port，實務上採用預設較為方便，並將 root 帳戶停用。
(C). SSH 預設為 21 Port，實務上會將 Port 設為 25，並將 root 帳戶停用。
(D). SSH 預設為 22 Port，實務上會將 Port 設為 3921，並將 root 帳戶停用。

第 2 題

因更新過程失敗，導致不正確資料些入資料庫，請問此案例屬於哪種資安概念被破壞？

(A). 真實性。
(B). 機密性。
(C). 完整性。
(D). 可用性。

第 3 題

請問以下何者可以在網路邊緣設定 IP 位址、端口、協議、應用軟體等項目，並允許或拒絕通訊的指令，可有效管理網路通訊安全？

(A). 虛擬化技術。
(B). 網路安全閘道。
(C). 防火牆規則。
(D). 網際網路安全協定。

第 4 題

CentOS 系統下若需設定 iptables 防火牆規則，請問應編輯哪項檔案後，重開機即可生效？
(A). vi /etc/iptables.rules。
(B). vi /etc/sysconfig/iptables。
(C). vi /usr/iptables.rules。
(D). vi /usr/sysconfig/iptables。

第 5 題

請問以下關於 WEP / WEP2 加密機制最為安全？

(A). WEP-PSK (AES)。
(B). WEP-PSK (TKIP)。
(C). WEP2-PSK (AES)。
(D). WEP2-PSK (TKIP)。
(E). WPAWPA2-PSK (KIP / AES)。

第 6 題

調降無線網路 AP 射頻功率，可降低何種掃描攻擊？

(A). 戰爭駕駛攻擊 (War driving)。
(B). 邪惡雙胞胎攻擊 (Evil Twin)。
(C). 流氓接入點攻擊 (Rogue Access Point)。
(D). 藍牙漏洞攻擊 (Bluesnarfing)。

第 7 題

您的朋友為了重灌電腦從網路下載了 Windows 10 專業版 ISO 及破解啟用器，當破解器執行後系統性能開始變得頓頓卡卡的，並於防毒軟體出現病毒提示。請問此案例屬於以下哪種惡意軟件？

(A). 廣告軟體。
(B). 特洛伊木馬。
(C). 邏輯炸彈。
(D). 殭屍病毒。

第 8 題

小張是一位程式設計師，他寫了一個 8 位元的字串變數，但未強制設定限制 8 位元組，因此若超過 8 位元依然可以複製該變數。請問此程式可能會受何種攻擊？

(A). 跨平台攻擊。
(B). 目錄遍歷。
(C). 緩衝區溢位攻擊。
(D). 會話劫持。

第 9 題

在分析程式碼過程中，您發現某段 JavaScript 會導致定期發送數據置系統上其他服務，這可能是哪種攻擊？

(A). XML 注入。
(B). SQL 注入。
(C). Buffer Overflow。
(D). DDoS。

第 10 題

小張是一名網站開發公司員工，負責網站專案發開相關業務，近日發現有一個專案網站容易遭受 SQL 注入攻擊，請問應採取下列那一項措施為佳？

(A). 更新網站 SSL 憑證。
(B). 表單添加輸入資料時檢核與驗證。
(C). 安裝防火牆限制惡意 IP。
(D). 將主機系統進行安全更新。

第 11 題

以下哪一種攻擊會導致網路流量被中斷，且被加入惡意程式碼或竄改？

(A). 冒用攻擊。
(B). 駕駛攻擊。
(C). 中間人攻擊。
(D). 冒用攻擊。

第 12 題

您想為你的雲端 LINUX 伺服器提高安全性，限制 SSH、FTP、MYSQL 等服務登入驗證失敗 3 次後拒絕登入，您應該使用哪一工具達成這樣實作？

(A). fail2ban。
(B). iptables。
(C). Postfix。
(D). clamav。

第 13 題

請問以下哪一種攻擊可能透過某電腦及未知 IRC 服務器來掃描網路上其他主機？

(A). 特洛伊木馬。
(B). 殭屍網路。
(C). 隱藏程序。
(D). 蠕蟲病毒。

第 14 題

以下哪一種是滲透類型是只透過程式碼進行測試，進而找出程式碼對系統內部可能出現之錯誤或缺口，針對問題進行修正。(對於使用者介面或功能不進行測試)？

(A). 白盒測試。
(B). 灰盒測試。
(C). 黑盒測試。
(D). 原始碼測試。

第 15 題

公司進行滲透測試主要目的？

(A). 將公司資訊人員培訓成白帽駭客。
(B). 找出公司內部所有漏洞及弱點證明公司資安無虞。
(C). 增加資訊人員招聘需求，以提升公司資訊安全能力。
(D). 了解測試結果對公司可能產生的影響或威脅，進而評估進一步。

第 16 題

因應疫情居家辦公所需，公司為提升管理效率，正在評估添購一套雲端管理系統，在評估系統時，主管要求資訊人員針對該系統安全性進行各項漏洞掃描。經檢測後，資訊人員回報「該雲端管理系統不會產生系統性威脅問題，但該系統可能存在多項漏洞」。請問針對此案例，除上述所應用到之檢測評估外，資訊人員也應該列入以下哪項評估？

(A). 威脅評估。
(B). 風險評估。
(C). 程式碼評估。
(D). 弱點評估。

第 17 題

請問鑑定分析師可透過以下何處找到系統程序進入點位置(hook)？

(A). RAM。
(B). Rootkit。
(C). BIOS。
(D). SSD。

第 18 題

請問以下和者實作可為數據備份做最佳的安全控制及防護措施？

(A). RAID 5 本機備份。
(B). 本機虛擬化備份。
(C). 透過使用者端以 P2P 方式備份。
(D). 異地備份。

第 19 題

請問一下哪一種狀況可能導致數據遺失？

(A). 資訊工程部門透過 SSH 登入系統進行系統更新。
(B). 部門之間透過 SFTP 傳送資料。
(C). 將伺服器資料存定期備份於另外一台異地 VM。
(D). 資訊人員從伺服器透過 USB 將網站資料複製到開發環境進行網站編修。

第 20 題

定量分析可以運用於以下哪一項目中?

(A). 財務分析。
(B). 資產價值。
(C). 工作幸福感。
(D). 技術轉移。

第 21 題

Gmail 網路信箱服務屬於以下哪一種雲端技術?

(A). PssS。
(B). SaaS。
(C). IaaS。
(D). GaaS。

第 22 題

下列何者屬於偵測式安全控制措施?

(A). 架高地板。
(B). 消防設備。
(C). 監視器。
(D). 防火牆。

第 23 題

對於一個攻擊者可以透過以下哪種方式，從封閉源碼的應用軟體環境中找出安全漏洞?

(A). 反編譯。
(B). 漏洞掃描。
(C). 使用手冊。
(D). 模糊測試。

第 24 題

請問 Microsoft Baseline Security Analyzer 用途為何？

(A). 掃描系統安全性紀錄是否有異常。
(B). 掃描系統是否存在惡意程式。
(C). 掃描系統是否有未安裝之安全性更新。
(D). 掃描系統是否有新版本可更新。

第 25 題

以下關於 Cisco 研發之 L2F (Layer 2 Forwarding Protocol) 敘述何者正確?

(A). L2F 透過 TCP 使用 1611 連接埠。
(B). L2F 不支援撥接連線建立通道協定。
(C). L2F 不具備身分驗證功能，且可進行加密。
(D). L2F 具備身分驗證功能，但不可進行加密。

第 26 題

關於指紋掃描儀主要驗證敘述何者為真?

(A). 透過用戶的行為動作進行驗證。
(B). 透過用戶身上的指紋進行驗證。
(C). 透過用戶腦波進行驗證。
(D). 透過用戶所配戴進行裝置。

第 27 題

企業內部可以透過以下那種方式防止未授權的員工進入機房?

(A). 設置 RFID 讀卡機。
(B). 設置安全防撞裝置。
(C). 設置監視器。
(D). 設置防盜保全系統。

第 28 題

以下何者可被視為多重要素驗證?

(A). 通用門禁卡。
(B). 存取控制清單及密碼。
(C). 透過使用者帳號、密碼登入網站。
(D). 登入網站後須再透過自然人憑證進行授權。

第 29 題

有一位行政人員將常用帳號密碼儲存於 Excel 試算表內，並儲存於辦公室內桌上型電腦的桌面，請問以下哪種防護類型之安全機制，可避免檔案遺失或被盜時資料被揭露?

(A). 放置移動裝置。
(B). 放在目前電腦內資料夾。
(C). 將帳號密碼存在資料庫。
(D). 放在可移動儲存媒體。

第 30 題

下列何者適合儲存 SSL 會話使用之密鑰或憑證?

(A). 硬碟 (Hard drive)。
(B). 資料庫 (Database)。
(C). 硬體安全模組 (Hardware Security Module)。
(D). 記憶體模組 (Memory Module)。

第 31 題

若憑證已被破壞應將憑證發布於何處?

(A). 憑證託管機構。
(B). 網路註冊中心。
(C). 憑證撤銷清單。
(D). 雲端租賃商。

第 32 題

接收 PGP 加密文件時，必須先提供?

(A). 公開金鑰 (Public-key)。
(B). 私有金鑰 (Private Key)。
(C). 申請 DNS 託管時註冊之用戶名稱。
(D). 申請憑證時註冊之用戶名稱。

第 33 題

關於 RADIUS 伺服器目的以下何者為正確？

(A). 增強使用者密碼強度。
(B). 提供集中化驗證服務。
(C). 網路加密服務。
(D). 外部驗證服務。

第 34 題

透過 DNS 紀錄 TXT 來反垃圾郵件技術(防郵件詐欺)應啟用哪項技術？

(A). 郵件安全清單。
(B). 網路原則伺服器 (NPS)。
(C). 寄件者原則架構 (SPF)。
(D). SmartScreen 篩選工具。

第 35 題

當用戶重複執行下列哪行為後，系統會進行鎖定帳戶之程序？

(A). 防毒軟體之病毒碼嘗試更新多次失敗後。
(B). 嘗試安裝應用程式失敗後。
(C). 輸入多此密碼驗證失敗後。
(D). 使用多款未經授權之非法軟體後。

第 36 題

公司目前正在導入 Azure 雲端服務，您剛已部署一台 Linux VM 完成，請問您應該透過以下何種方式取得 ROOT 密碼？

(A). 透過 Azure 平台虛擬主機內選單：支援與疑難排解->重設密碼。
(B). 進入 SSH 透過以下指令進行密碼變更「sudo passwd root」。
(C). 在部屬 VM 前所設定之 ROOT 密碼，那時候自己設密碼的時候，就要記得了。
(D). 撥打微軟客服專線請客服幫忙重設密碼，待新密碼寄發至管理員信箱即可。

第 37 題

你是一間中小企業網路管理員人，你必須限制辦公室電腦只允許執行特定清單上的應用程式，請問您可以透過以下哪項實作?

(A). 用戶安全性管理員。
(B). 用戶端使用者權限。
(C). 系統設定共用程式。
(D). Applocker 群組原則。

第 38 題

公司在今年起，已強制所有連線必須限制特定 IP，因疫情關係近日工程師因在家工作，向您提出申請表希望可以在家透過 FTP 進行網站維護更新，該名工程師電腦固定 IP 為 219.85.100.168，請問您應新增哪項規則進行此項開放
(A). -A INPUT -s 219.85.168.125/32 -p tcp -m tcp --dport 21-j ACCEPT。
(B). -A INPUT -s 219.85.168.125/32 -p tcp -m tcp --dport 22 -j ACCEPT。
(C). -A INPUT -s 219.85.168.125/32 -p tcp -m tcp --dport 21 -j DROP。
(D). -A INPUT -s 219.85.168.125/32 -p tcp -m tcp --dport 22 -j DROP。

二、多選題(multiple choices)

第 1 題

您在一間企業資訊部門上班，公司近期為了提升工作彈性度，擬允許公司部分員工可透過遠端訪問公司內部資料。請問以下哪些資訊技術需要應用到？(請選擇 2 個答案)

(A). 防火牆。
(B). 網路存取控制。
(C). 子網路切割。
(D). 虛擬私人網路。
(E). 網路位址轉換。
(F). 代理伺服器。

第 2 題

WEP2 (Wired Equivalent Privacy 2) 加入了以下何種演算法以強化安全性？(請選擇 2 個答案)

(A). RC4。
(B). TKIP。
(C). AES。
(D). RC6。

第 3 題

無線網路常見哪兩種攻擊可未經當事人同意竊聽對話或收集數據？(請選擇 2 個答案)

(A). 邪惡雙胞胎攻擊 (Evil Twin)。
(B). 戰爭駕駛攻擊 (War driving)。
(C). 藍牙漏洞攻擊(BrakTooth) 。
(D). 流氓接入點攻擊 (Rogue Access Point)。

第 4 題

針對 KRACK 攻擊應如何因應為佳？(請選擇 3 個答案)

(A). 立即更新 KRACK 修補程式。
(B). 立即變更 Wi-Fi 密碼。
(C). 只透過 HTTPS 協定上網，避免透過 HTTP 進行資料交易。
(D). 盡量避免使用公用開放式無線網路，若使用公用網路應搭配信賴的 VPN 服務。
(E). 變更路由器。

第 5 題

郵件伺服器不應該允許使用以下哪寫副檔名？(請選擇 2 個答案)

(A). exe。
(B). zip。
(C). bat。
(D). txt。

第 6 題

Linux 系統下不同 OS 常見之「更新作業系統」指令以下何者正確？(請選擇 2 個答案)

(A). yum update。
(B). system update。
(C). debian update。
(D). cosys -y update。
(D). apt-get update。

第 7 題

以下那些事件屬於災難復原 (Disaster Recovery) 範疇?(請選擇 3 個答案)

(A). 資訊人員休假。
(B). 地震。
(C). 示威抗議。
(D). 新進人員基礎教育訓練。
(E). 駭客入侵。

第 8 題

請問使用數位簽章主要目的為何?(請選擇 2 個答案)

(A). 可用性。
(B). 不可否認性。
(C). 加密。
(D). 完整性。
(E). 複雜性。

第 9 題

關於以下硬體加密之敘述哪些是正確的? (請選擇 2 個答案)

(A). 必須搭配智慧卡進行運算加密。
(B). 相較於軟體加密，硬體加密較有效率。
(C). 硬體加密必須透過橢圓曲線加密演算法進行。
(D). 必須使用 HSM 檔案系統。
(E). 可搭配 TPM 進行運算加密。

第 10 題

啟用寄件者原則架構 (SPF) 同時，建議同時設定以下哪項，以保護網域並確保寄出之郵件能正常發送？(請選擇 2 個答案)

(A). SIP。
(B). DKIM。
(C). ASPMX。
(D). DMARC。

第 11 題

網際網路安全協定 (IPSec) 如何保護通訊會話? (請選擇 2 個答案)

(A). 拒絕未授權的傳輸內容。
(B). 資料承載加密。
(C). IP 標頭驗證。
(D). 將網路私密金鑰儲存於用戶端電腦並再加密保護。

第 12 題

針對 Cookie 之特性，請問下列何者易使用戶電腦安全性受影響?(請選擇 2 個答案)

(A). 自動記錄網站密碼。
(B). 自動加密使用者資料並傳送至政府單位。
(C). 屬於低安全性之檔案傳輸服務。
(D). 紀錄使用者於網路瀏覽之行為。

答案卷

參考答案

題號	答案
1	D
2	C
3	C
4	B
5	C
6	A
7	B
8	C
9	C
10	B
11	C
12	A
13	C
14	A
15	D
16	B
17	C
18	D
19	D
20	B
21	B
22	C
23	D
24	C
25	D
26	B
27	A
28	D
29	A
30	C

題號	答案
31	C
32	A
33	B
34	C
35	C
36	B
37	D
38	A
多選題	
1	AD
2	BC
3	AD
4	ACD
5	AC
6	AE
7	BCE
8	BD
9	BE
10	BD
11	BC
12	AD