代號：20250
頁次：4－1

108年公務人員特種考試外交領事人員及外交行政人員、民航人員、稅務人員及原住民族考試試題

考 試 別：外交人員考試
等　　別：四等考試
類 科 組：外交行政人員資訊組
科　　目：資訊安全與網路管理概要
考試時間：1 小時 30 分　　座號：_____

※注意：禁止使用電子計算器。

甲、申論題部分：（50 分）
㈠不必抄題，作答時請將試題題號及答案依照順序寫在申論試卷上，於本試題上作答者，不予計分。
㈡請以黑色鋼筆或原子筆在申論試卷上作答。
㈢本科目得以本國文字或英文作答。

一、下列有關網路攻擊方式，請詳細說明：（每小題 5 分，共 10 分）
㈠SSL Flood
㈡DNS Reflection 攻擊

二、對抗假新聞是社群網路安全的重要議題，請回答：
㈠misinformation 與 disinformation 的差異是什麼？（5 分）
㈡構成 disinformation 的基本要件是什麼？（10 分）

三、請試述下列名詞之意涵：（每小題 5 分，共 25 分）
㈠searchable encryption
㈡privacy by design
㈢unified threat management
㈣granular access control
㈤biometric authentication

乙、測驗題部分：（50 分）　　代號：5202
㈠本測驗試題為單一選擇題，請選出一個正確或最適當的答案，複選作答者，該題不予計分。
㈡共 25 題，每題 2 分，須用 2B 鉛筆在試卡上依題號清楚劃記，於本試題或申論試卷上作答者，不予計分。

1　有關密碼方法與協定的敘述，下列何者正確？
Ⓐ以 SHA-1 計算雜湊，必須使用安全金鑰（secret key）
Ⓑ為了避免相同的訊息，經由同一加密管道之後產生相同結果，我們通常會附加一組初始輸入值（Initialization Vector）
Ⓒ TLS 可抵擋 TCP RST 攻擊
Ⓓ MD5 是一種加密演算法

2　SMTP 是一種收發電子郵件的網路協定，下列訊息何者正確？
Ⓐ不可認證發信者　　Ⓑ傳送過程可保證訊息不被修改
Ⓒ訊息有加密　　Ⓓ具有不可否認性

3 一條通訊連線的發送端傳送一個訊息 Q 給接收端時，若先以雜湊方式產生 Q 之訊息摘要（Message Digest），再和 Q 一起傳送給接收端，接收端可以此訊息摘要做什麼？
㈠從事 Q 的完整性驗證（Integrity Checking）㈡了解 Q 的訊息內容
㈢知悉 Q 中是否攜帶解密金鑰 ㈣檢視 Q 是否是駭客（Hacker）重送的訊息

4 下列那一選項不是 Advanced Encryption Standard（AES）之加密過程中用到的函式？
㈠回合金鑰加密（AddRound Key）函式 ㈡位元組取代轉換（SubBytes）函式
㈢反移列轉換（InvShiftRows）函式 ㈣混行轉換（MixColumn）函式

5 空間域（Spatial Domain）藏入法的數位浮水印技術（Digital Watermarking），通常是將浮水印（Watermark）隱藏在創作品之數位資料的何處？
㈠MSB（Most Significant Bits）位置 ㈡LSB（Least Significant Bits）位置
㈢隨機挑選位元的位置 ㈣依安全設定範圍內所隨機挑選的位置

6 以金鑰加/解密，下列選項何者錯誤？
㈠非對稱式加/解密以公鑰加密，以私鑰解密
㈡數位簽章以私鑰加密，以公鑰解密
㈢ElGamal 密碼系統所產生的加/解密金鑰為非對稱式
㈣橢圓曲線加/解密所用金鑰為對稱式

7 在 UNIX 或 UNIX-like（例如，Linux）作業系統中，一個檔案的存取權限為 765，請問下列對應的顯示何者正確？
㈠rwxrw-r-x ㈡rw-rw-rw- ㈢rwx-w-rw- ㈣r-xrw-rwx

8 入侵偵測系統（Intrusion Detection System, IDS）的偵測方式，可以分成異常行為入侵偵測（Anomaly Intrusion Detection）和錯誤行為入侵偵測（Misuse Intrusion Detection）兩種，下列何者錯誤？
㈠以記錄檔（Profile）記錄正常行為可用以偵測網路異常行為
㈡錯誤行為入侵偵測須建立一個知識庫存放攻擊模式
㈢錯誤行為入侵偵測不會將合法網路行為誤判為異常行為
㈣門檻偵測是一種錯誤行為入侵偵測

9 Linux 作業系統安全機制由 Linux-PAM（Linux-Pluggable Authentication Modules）負責，使用者可事先依安全政策為應用程式 A 設定驗證（Authentication，或稱認證）條件與程序。在必要時，Linux-PAM 會取出 A 之設定檔案，對 A 進行驗證。請問下列選項何者不是 Linux-PAM 的四種驗證類別（Type）之一？
㈠鑑別（Authentication）
㈡帳戶（Account）
㈢通行密碼（Password）
㈣兩個處理（Processes）之間的隔絕（Isolation）方式

10 有關防火牆 DMZ 網路的規劃，下列何者正確？
㈠DMZ 是內部網路，重要伺服器所在的網段
㈡DMZ 是外部公開的網路
㈢DMZ 可存取內部網路
㈣DMZ 位於內部與外部網路之間

11 資訊隱碼攻擊（SQL Injection Attack）通常是利用 SQL 語言的什麼機制，來引發對資料庫系統的攻擊？
㈠以註解（Comments）規避安全驗證
㈡在 HAVING 子句（Having clause）中設定資料過濾條件
㈢以省略 WHERE 子句的卡氏乘積（Cartesian product）擴展資料組合
㈣以 SELECT 子句中之 DISTINCT 功能整併資料

12 假亂數產生器（Pseudo Random Number Generator, PRNG）可用在資料加/解密，下列選項何者錯誤？
㈠加密和解密雙方需採用相同的種子（Seed）
㈡採用 PRNG 進行加/解密，是一種對稱式加/解密方式
㈢加密和解密雙方皆須準備一個 PRNG
㈣相同的種子可能產生不同的加/解密金鑰

13 在比特幣（Bitcoin）的交易和挖礦程序中，下列選項何者錯誤？
㈠比特幣電子錢的樣式是一個區塊鍊（Chain of Blocks）
㈡所有經確認的交易紀錄都會依序放在區塊上
㈢新區塊產生後，則挖礦成功
㈣比特幣挖礦就是為 SHA-256 雜湊函數找出一個讓雜湊值開頭是連續幾個 0 的 Nonce

14 下列何者與 SQL Injection 防禦方法無關？
㈠預置敘述（Prepared Statement）　㈡參數化查詢（Parameterized Query）
㈢輸入驗證（Input Validation）　㈣禁用 JavaScript

15 有關網頁應用防火牆（Web Application Firewall, WAF）的使用，下列何者正確？
㈠老舊應用程式易有相容性問題，不適合使用
㈡使用網路層的過濾機制
㈢若要過濾 SSL 連線，必須擁有保護伺服器的私密金鑰
㈣無法排除 SQL Injection 攻擊

16 網路服務狀況，若使用傳輸層的掃描方式，下列何者正確？
㈠TCP connection scan 掃描負擔重，必須完成三向交握程序
㈡SYN-scan 可掃描 UDP 的服務
㈢可使用 ICMP 進行傳輸層掃描
㈣PING 是一種傳輸層網路偵錯工具

17 社交攻擊採用的技術中，有關 Phishing 的說明，何者錯誤？
㈠Phishing 可透過 email 發送
㈡XSS 攻擊通常需要經由 Phishing，引誘用戶點擊連結
㈢可透過 Phishing 取得用戶的 http cookie 內容，攔截重要的交易過程
㈣SQL Injection 攻擊必須配合 Phishing 才能進行

18 有關 DDoS（Distributed Denial of Service）的敘述何者正確？
㈠頻寬放大攻擊可透過 TCP 達成
㈡攻擊者可偽造 TCP 來源 IP
㈢NTP 是網路時鐘對時的協定，常被不當利用進行頻寬放大攻擊
㈣DNS 伺服器常被當作 SYN Flood 的攻擊目標

19 Microsoft Office CVE-2019-1111 發布的訊息摘要如下：An attacker can leverage this issue to execute arbitrary code in the context of the current user. 請問此訊息有何安全上的威脅？
㈠上述訊息說明為一種病毒程式，可感染 Office 軟體
㈡這是一種專門勒索 Office 的程式
㈢只要有上述 CVE 涵蓋的 Office 版本，打開 Office 文件，可能被安裝後門
㈣只要不上網，就不用擔心上述安全風險

20 在 4G/5G 網路中，使用者拿著手機 M 到國外（例如，A 國）的網路 N 漫遊，N 會請 M 的家網路（Home Network）驗證（Authenticate，又稱認證）M 所提供的資料，才允許 M 使用 N 的設備與服務，請問 M 向 N 提出服務連線時，至少需提供什麼資料，以進行驗證？
㈠International Mobile Subscriber Identity（IMSI）
㈡International Mobile Equipment Identity（IMEI）
㈢含行動裝置國家代碼（Mobile Country Code）之手機號碼
㈣以上三選項的陳述項目都需要

21 線上信用卡付款若採用安全電子交易 SET（Secure Electronic Transaction），其安全需求大致上有五項，下列何者不是這五項安全需求之一？
㈠交易資料的機密性（Confidentiality）　㈡交易資料的完整性（Integrity）
㈢身分鑑別（Authentication）　㈣交易資料的合法性（Validity）

22 頻域（Frequency Domain）藏入法的數位浮水印技術（Digital Watermarking），通常是先將被保護之創作品的影像，利用離散餘弦轉換（Discrete Cosine Transformation）或小波轉換（Wavelet Transformation）轉至頻域中，其次，再以頻域係數將浮水印（Watermark）隱藏在何處？
㈠低頻部分
㈡高頻部分
㈢任意挑選的頻率，但須記載，以便後續驗證
㈣間隔式地挑選的頻率

23 當使用者分別給予一個 ElGamal 加密演算法兩個明文，P1 和 P2，而 P1=P2；在使用相同 ElGamal 演算法細節與相同金鑰條件下，分別產生密文 E1 和 E2。其次，使用者又將 P1 和 P2 分別輸入到 RSA 加密演算法，在 RSA 相同演算法細節與金鑰條件下，分別產生密文 R1 和 R2，請問下列選項何者正確？
㈠E1=E2 且 R1≠R2　㈡E1≠E2 且 R1=R2　㈢E1=E2 且 R1=R2　㈣E1≠E2 且 R1≠R2

24 Alice 和 Bob 欲進行安全通訊，首先雙方各自選擇一個亂數當私鑰（Private Key），再各自依其私鑰產生一公鑰（Public Key），然後傳送該公鑰給對方，由接收方配合自己的私鑰產生一個加密金鑰，請問在此之後，Alice 和 Bob 各自傳送訊息給對方的加/解密方式是：
㈠非對稱式　㈡對稱式　㈢雜湊方式　㈣半對稱式

25 手機 M 和基地台 B 之間所建立的存取層（Access Stratum）無線連線會產生二金鑰，一金鑰從事 M 和 B 之間所傳遞訊息 P 之加/解密，另一金鑰的任務為：
㈠P 的完整性驗證（Integrity Checking）
㈡偵測駭客（Hacker）重送 P 所引發之重送攻擊（Replay Attack）
㈢建立 M 和 B 之間的 IPSec 通道
㈣建立 M 和 B 之間的虛擬私有網路（Virtual Private Network, VPN）

測驗式試題標準答案

考試名稱：108年公務人員特種考試外交領事人員及外交行政人員、民航人員、稅務人員及原住民族考試

類科名稱：外交行政人員資訊組

科目名稱：資訊安全與網路管理概要（試題代號：5202）

單選題數：25題　　單選每題配分：2.00分

複選題數：　　複選每題配分：

標準答案：

題號	第1題	第2題	第3題	第4題	第5題	第6題	第7題	第8題	第9題	第10題
答案	B	A	A	C	B	D	A	D	D	D

題號	第11題	第12題	第13題	第14題	第15題	第16題	第17題	第18題	第19題	第20題
答案	A	D	C	D	C	A	D	C	C	A

題號	第21題	第22題	第23題	第24題	第25題	第26題	第27題	第28題	第29題	第30題
答案	D	B	B	B	A					

題號	第31題	第32題	第33題	第34題	第35題	第36題	第37題	第38題	第39題	第40題
答案										

題號	第41題	第42題	第43題	第44題	第45題	第46題	第47題	第48題	第49題	第50題
答案										

題號	第51題	第52題	第53題	第54題	第55題	第56題	第57題	第58題	第59題	第60題
答案										

題號	第61題	第62題	第63題	第64題	第65題	第66題	第67題	第68題	第69題	第70題
答案										

題號	第71題	第72題	第73題	第74題	第75題	第76題	第77題	第78題	第79題	第80題
答案										

題號	第81題	第82題	第83題	第84題	第85題	第86題	第87題	第88題	第89題	第90題
答案										

題號	第91題	第92題	第93題	第94題	第95題	第96題	第97題	第98題	第99題	第100題
答案										

備　　註：