102年公務人員特種考試警察人員考試、
102年公務人員特種考試一般警察人員考試及　代號：20160　全一頁
102年特種考試交通事業鐵路人員考試試題

等　　別：二等一般警察人員考試
類　　科：刑事警察人員數位鑑識組
科　　目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）
考試時間：2小時　座號：＿＿＿＿＿＿＿＿

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、請詳細解釋下列專有名詞：（每小題5分，共20分）
㈠旁通道攻擊（side-channel attacks）
㈡弱點掃瞄（vulnerability scan）
㈢共同準則（common criteria）
㈣強制型存取控制（mandatory access control）

二、位址解析協定（Address Resolution Protocol, ARP）愚弄（spoofing）（通稱 ARP spoofing）是進行中間人攻擊（man-in-the-middle attack）的常用手法，請問：
㈠何謂中間人攻擊？請舉例說明。（5分）
㈡ARP spoofing的工作原理為何？請詳細說明之。（10分）
㈢DNS（domain name service）spoofing和ARP spoofing有何不同？請簡述其工作原理。（5分）

三、開發資訊系統時，如果遵循一些安全設計原則（security principles），這樣即使系統遭受攻擊，也可以降低損害。請針對下列四個安全設計原則，分別說明其意義，並舉例說明若遵照該原則，可以減少那方面的損害？（每小題5分，共20分）
㈠最小權限（least privilege）
㈡完全仲裁（complete mediation）
㈢分散權限（separation of duties）
㈣預設失效安全（fail-safe default）

四、有關防火牆（firewall）：
㈠封包過濾式防火牆（packet filtering firewall）和代理人為基底式防火牆（proxy-based firewall）的工作原理有何不同？請分別說明之。（10分）
㈡防火牆和入侵預防系統（intrusion prevention system, IPS）有何區別？請詳細說明之。（10分）

五、有關數位鑑識（digital forensics）：
㈠數位鑑識的目的為何？請詳細說明之。（10分）
㈡請列出進行數位鑑識必須經歷的幾個步驟（請依先後次序列出），並簡單說明各步驟的意義。（10分）