臺灣土地銀行107年度一般金融人員及專業人員甄試試題

甄試類組【代碼】：八職等-資訊安全人員（二）【N5626】

科目二：綜合科目【含作業系統管理、資料庫系統管理、網路管理、資訊安全管理(含 Firewall、IPS、WAF、AD、SIEM、防毒)】

＊入場通知書編號：＿＿＿＿＿＿＿＿＿＿

注意：①作答前先檢查答案卷，測驗入場通知書編號、座位標籤、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卷作答者，不予計分。
②本試卷為一張雙面，非選擇題共5大題，每題各20分，共100分。
③非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採**橫式**作答，並請**依標題指示之題號於各題指定作答區內作答**。
④**請勿於答案卷書寫應考人姓名、入場通知書編號或與答案無關之任何文字或符號。**
⑤本項測驗僅得使用簡易型電子計算器（不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝（錄）影音、資料傳輸、通訊或類似功能），且不得發出聲響。應考人如有下列情事扣該節成績10分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑥**答案卷務必繳回，未繳回者該節以零分計算。**

第一題：

在LINUX作業系統中，哪些指令可以改變「檔案屬性」？哪些指令可以改變「權限」？請舉例說明之。【20分】

第二題：

資料庫管理系統(DBMS)於執行資料交易(Transaction)時，所具備的四大特性為何？請簡略說明之。【20分】

第三題：

我國資通安全管理法在2018年5月立法院三讀通過，而訂有對於資通安全事件進行通報的責任。例如：

資通安全管理法第十四條要求：
公務機關為因應資通安全事件，應訂定通報及應變機制 .....。

資通安全管理法第十八條要求：
特定非公務機關為因應資通安全事件，應訂定通報及應變機制。
特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。.....

請問，在進行資通安全事件通報時，應該要包含哪些項目？並舉例說明。【20分】

第四題：

在Windows網域當中，我們常會使用AD伺服器，設定該網域當中的Windows作業系統之電腦所應遵守的規則。例如我國政府組態基準就有對於AD之帳戶原則進行要求，其中包括六項密碼原則與三項帳號鎖定原則。請說明這九項原則各自在規範哪些項目？【20分】

【請接續背面】

第五題：

請回答下列問題：

（一）MRTG (Multi Router Traffic Grapher)是普遍採用的網路流量監控統計之開源軟體(open source)。請問其運作主要是依據何種網路協定？並請簡述其運作原理。【6 分】

（二）在 Windows 作業系統中，啟動「命令提示字元(command prompt)」，執行「netstat -a」或「netstat -a | more」dk3 可得到如下圖所示的訊息。今欲統計分析該主機連結到不同網站的數量，請簡述您的作法。【4 分】

```
C:\Users>netstat -a

使用中連線
  協定    本機位址              外部位址              狀態
  TCP    113.23.80.155:7680     w118-249:9135         TIME_WAIT
  TCP    113.23.80.155:7680     w118-249:9136         TIME_WAIT
  TCP    113.23.80.155:55286    tl-in-f125:5222       ESTABLISHED
  TCP    113.23.80.155:57020    a23-219-32-120:https  CLOSE_WAIT
  TCP    113.23.80.155:57021    a23-219-32-120:https  CLOSE_WAIT
  TCP    113.23.80.155:62039    tsa01s08-in-f14:https ESTABLISHED
  TCP    113.23.80.155:62050    tsa01s08-in-f14:https ESTABLISHED
  TCP    113.23.80.155:62105    tsa03s01-in-f5:https  ESTABLISHED
  TCP    113.23.80.155:62212    203.104.153.1:https   ESTABLISHED
  TCP    113.23.80.155:62328    e1:https              ESTABLISHED
  TCP    113.23.80.155:62330    e2:https              ESTABLISHED
  TCP    113.23.80.155:62367    162.125.82.3:https    CLOSE_WAIT
  TCP    113.23.80.155:62368    162.125.82.3:https    CLOSE_WAIT
  TCP    113.23.80.155:62369    tm-in-f94:https       ESTABLISHED
  TCP    113.23.80.155:62373    162.125.34.129:https  ESTABLISHED
  TCP    113.23.80.155:62836    e2a:https             ESTABLISHED
  TCP    113.23.80.155:62851    ec2-52-72-159-235:https TIME_WAIT
  TCP    113.23.80.155:62865    161.69.45.200:https   TIME_WAIT
  TCP    113.23.80.155:62867    tsa01s08-in-f10:https TIME_WAIT
  TCP    113.23.80.155:62876    162.125.34.6:https    CLOSE_WAIT
  TCP    113.23.80.155:62907    tsa01s08-in-f8:https  ESTABLISHED
  TCP    113.23.80.155:62908    stg:https             ESTABLISHED
  TCP    113.23.80.155:62909    server-13-35-37-117:https ESTABLISHED
```

（三）請依據以下之 SNMP object 定義，繪製其所定義的表格，同時標註各欄位名稱及資料型別(data type)。【4 分】

routeTable OBJECT-TYPE
SYNTAX SEQUENCE OF RouteEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “This entity’s routing table”
::={NEW-MIB 3}
routeEntry OBJECT-TYPE
SYNTAX RouteEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “A route to a particular destination”
INDEX {dest}
::={routeTable 1}

RouteEntry ::=
SEQUENCE{
dest IpAddress,
next IpAddress
}
dest OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION “The address of a particular destination”
::={RouteEntry 1}
next OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
DESCRIPTION “The internet address of the next hop”
::={RouteEntry 2}

（四）國際標準組織(ISO)所提出網路管理模型(network management model)，包括 5 個概念性的領域，在實務上還需要遵循特定的程序。請就「安全管理(security management)」，扼要描述其所涵蓋之內容。【6 分】