《資訊安全實務》

一、請說明系統稽核紀錄應包含那些項目？稽核紀錄分析的目的為何？以及系統稽核紀錄的保護方式有那些。（30 分）

【擬答】

(一)系統稽核記錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性。

(二)稽核記錄分析的目的，在於提出改善報告之執行情形：

1.缺失或待改善之項目及內容。

2.發生原因。

3.為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施。

4.前款措施之預定完成時程及執行進度之追蹤方式。

(三)系統稽核記錄的保護方式有：

1.運用雜湊(Hash)或其他適當機制，確保系統稽核記錄的完整性(Integrity)。

2.定期備份系統稽核紀錄至與原稽核系統不同之系統。

3.安裝備援系統，提高系統稽核記錄之可用性(Availability)。

二、Bind Shell 與 Reverse Shell 是惡意攻擊者為了取得目標的作業系統權限寫出的惡意程式碼，會以多種方式植入目標的作業系統並執行。攻擊者會利用社交工程或是伺服器可提供檔案上傳的漏洞，將 Shell 上傳並執行。請說明何謂 Bind Shell 與 Reverse Shell，並說明如何防止 Bind Shell 與 Reverse Shell 的攻擊。（30 分）

【擬答】

Bind Shell 為惡意攻擊者將 Shell 繫結至一通訊埠(Port)上，並據此通訊埠與遠端主機的 IP 位址，主動直接存取、發送命令給遠端主機。適用於惡意攻擊者與遠端主機位於同一網路，或是可透過 Internet 直接連通，而不用透過防火牆(Firewall)或是網路位址轉譯(Network Address Translation, NAT)之情境。

由於防火牆或是 NAT 可能阻隔惡意攻擊者與遠端主機的通訊，且防火牆通常會阻擋異常的外部對內部之連線。故 Reverse Shell 則是遠端主機透過 Shell，由內部向外部的惡意攻擊者進行通訊。例如，惡意攻擊者利用通訊埠 8080，被動等待遠端主機的連線，為駭客控制殭屍電腦的手法之一。

防止 Bind Shell 與 Reverse Shell 的攻擊之方法：

1.檢視防火牆連線政策

除了檢視防火牆外部連線到內部的連線政策外，也要檢視防火牆內部連線到外部的連線政策，關閉不必要的通訊埠，並建立連線 IP 位址黑名單與白名單。

2.安裝入侵偵測系統/入侵預防系統

(Intrusion Detection System, IDS/Intrusion Prevention System, IPS)

例如：可於重要伺服器上安裝主機型入侵偵測系統(Host-based IDS, HIDS)，並針對系統上的重要檔案、日誌檔(Log File)、甚至是系統呼叫(System Call)進行監控，所有流入本機的封包皆會被接收並分析，一旦符合入侵規則便發出警告。

3.定期/不定期檢測 Rootkit、Process 與執行程式

如發現有異常現象，如特別高的網路流量、CPU 使用率、占用的記憶體空間等，即要提高警覺，進行後續處理。

三、何謂錯誤行為入侵偵測（Misuse Intrusion Detection）？其運作方式為何？（25 分）

【擬答】

錯誤行為入侵偵測是將各種已知的入侵模式或攻擊行為的特徵建成資料庫，用來分析比對來源資料是否符合特徵。若符合，則判斷其為入侵；若不符合，則判斷為正常。

此種入侵偵測方法採負面表列，需要不斷更新特徵資料庫，適用於偵測超級管理者(root)權限被入侵、系統

日誌檔被異動或病毒碼程式植入等攻擊，誤判率低。然而，由於入侵行為需符合特徵資料庫，故新型態的入侵行為可能偵測不到，漏判率高。

四、假設您曾經註冊過一個網站的會員，但是忘了密碼，點選忘記密碼的功能後，該網站將您本來的密碼以明文方式寄出。請說明該網站可能存在那些安全問題？並提出可行的改善措施。（15 分）

【擬答】

(一)網站以明文儲存密碼

網站以明文儲存會員密碼，如網站被入侵，可能導致會員密碼被竊取。改善措施為會員密碼以雜湊值(Hash Value)儲存，藉由比對雜湊值判斷輸入會員密碼的正確性。

(二)網站以明文傳送密碼

網站將會員密碼以明文的方式在網路上傳送，若被攻擊者中途劫取，其將可獲得會員密碼。改善措施為網站以加密方式如 PGP 來寄出加密後的郵件，提升機密性(Confidentiality)。

(三)會員以明文儲存密碼

會員收到密碼後，以明文儲存，故如被攻擊，可能外洩會員密碼。改善措施為網站傳送重設密碼連結，並請會員回答預設問題並得到正確答案後，才可重設密碼。