亞洲大學　資訊工程學系

資訊安全與管理 (Spring 2009) 期中考

Date: Apr. 17, 2009

一、填充題 (每題 2 分共 40 分)

1. 攻擊者送出的封包如山洪暴發般的瞬間擁至稱之為_洪泛攻擊_
2. _社會工程_是以非技術性的方式取得資訊，如利用欺騙員工來破壞系統安全性
3. 僅將封包傳遞給目的電腦的網路設備是 (1) 交換器(Switch) (2) 集線器(HUB) (3) 路由器(Router) (4) RJ45
4. 媒體存取控制（Media Access Control，MAC）位址是以 16 進制表示且以由_6_個 bytes 組成
5. 實體位址在網路網際上是可 Routing 的且必須向_ISP_取得
6. 部分網站程式將使用者輸入的資料直接交給資料庫處理，而未事先過濾可能有害的字元。讓駭客有機會在輸入的資料中夾帶 SQL 語言，進行_資料隱碼(SQL injection) 攻擊
7. 微軟作業系統下查詢自己電腦的網路資訊可用 _ipconfig_ 指令
8. __防火牆 Fire wall__可以過濾進入網路的封包及拒絕不能接受的封包的設備或軟體。
9. 負責轉換 IP 與網域名稱的是 _DNS_ 伺服器
10. 利用惡意且大多是違法的方式來躲避為通訊帳單、訂單、轉帳、或其它服務付費，此行為稱之為_飛客入侵_
11. 定義了最基礎的網路硬體標準是屬於網路七層架構(Open Systems Interconnect，OSI)中的__實體層_
12. 未通知當事人並取得其同意之前，資料持有者不得將當事人為特定目的所提供的資料運用在另一個目的上，法律上此屬於 _隱私權_
13. 無線網路比有線網路更難保障傳輸安全，有鑑於此，一種加密傳輸方法 Wired Equivalent Privacy (WEP) 被設計並廣為應用，然而此法已被完全被攻破，哪一種加密傳輸是為了修補 WEP 的問題? (a) EWP (B) WAP (C) WEP II (D) WPA
14. 由分散在世界各地的中毒電腦對目標電腦進行攻擊，使其無法提供服務稱之為 (a) DDoS (b) DoS (c) SoS (d) DNS
15. 下列何者為網路控制管理協定? (a) TCP (b) UDP (c) POP (d) ICMP
16. 駭客處在 A, B 兩方通訊的中間收 A 訊息並予以修改再傳給 B，收 B 訊息再修改再傳給 A，此種攻擊稱之為 _中間人攻擊 (Man in the Middle Attack)__
17. 一種看起來友善，實際上卻有惡意的程式是為 (a) 病毒 (b) 特洛伊木馬 (c) 駭客 (d) 鍵盤側錄程式
18. 下列何者非病毒躲避監視的方法 (a) 千面人(Polymorphism) (b) 升級 (Upgrade) (c) 隱藏 (Stealth) (d) 加殼 (armoring)
19. 攻擊者會送出一個具有相同來源與目標位址的偽造封包，形成自己傳給自己，導致試圖

送出訊息的系統當機，此種攻擊稱之為 (a) Land 攻擊 (b) Teardrop (淚痕)攻擊 (c) DoS(阻斷服務攻擊) (d) war-dialing (撥號攻擊)

20. 攻擊者會對目標系統的任意通訊埠發送非法的 UDP 封包系統會因為忙於回傳封包而負載過重，此種稱之為 (a) war-driving (駕駛攻擊) (b) Smurf 攻擊 (c) UDP 洪泛攻擊 (d) 阻斷服務攻擊

二、簡答題(每題 10 分)

1. 試說明何謂“入侵”，並列舉兩種入侵方式

   未經授權進行系統資料存取

   社會工程

   撥號攻擊(war-dialing)

   駕駛攻擊(war-driving)

2. 試說明何謂“駭客”，並列舉兩種“駭客”類型

   對電腦系統學有專精的人。

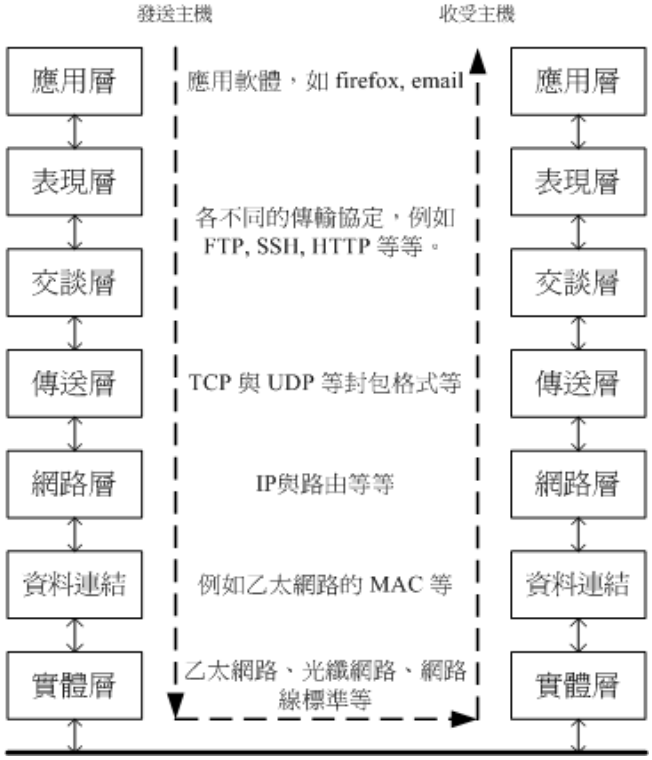
   白帽駭客

   黑帽駭客(怪客)

   灰帽駭客

   有道德的駭客

3. 試列示國際標準組織 (International Standards Organization, ISO)所制訂的開放系統互連模型（Open Systems Interconnect，OSI)七層架構。



4. 試比較有線網路與無線網路的差別，並列示兩種無線網路的傳輸方式。

有線：經有實體線路傳遞資料；相較於無線網路，傳輸速度較快;需基礎建設

無線：經由無線電波傳送資料；傳輸速度較慢；無需基礎建設

- ☐ 藍芽
- ☐ IEEE 802.11
- ☐ WiFi

5. 試說明網站架構的基本元件

- 瀏覽器 (browsers)：例如 Internet Explorer 或 FireFox 等
- 通訊協定 (transport protocols)：Hypertext Transfer Protocol (HTTP) 或有加密功能之 Secure Socket Layer (SSL)
- 網站伺服器 (web servers)：最常見的為以微軟為主的 Internet Information Server (IIS) 和開放原始碼的 Apache
- 網站應用 (applications)：有 Hypertext Preprocessor (PHP) 與 Active Server Page (ASP) 較常見。

6. 試說明何謂“阻斷服務攻擊”，並列示兩種電腦的實體限制。

利用各種方式使電腦超出電腦具有的實體限制以讓電腦停止所有的回應，讓合法使用者無法存取系統。

- 使用者個數
- 檔案大小
- 傳輸速度
- 儲存的資料量