網路攻防戰

梁明章
國家高速網路與計算中心
副技術師

大綱

- 緒論
  - 資訊戰爭
  - 網路攻防戰
- 網路攻擊
- 網路防禦

緒論

資訊戰爭

- 資訊戰爭 Information War
  - 將作戰中各個環節都轉化成資訊，再以完善的資訊指揮控制系統進行作戰優化，以取得最優之作戰效能。
- 資訊戰 Information Warfare
  - 為保護己方資訊系統的完整性，免遭敵人利用、擾亂和毀壞，同時又要利用、擾亂和摧毀敵方的資訊系統及處理過程，以便獲得兵力或資源運用上的資訊優勢而採取的一系列行動。
- 資訊作戰 Information Operations
  - 在軍事資訊環境中為發揮、增強和保護己方軍隊收集、處理資訊並按照資訊行動的能力，以獲得在各種軍事行動中的優勢而採取的連續性軍事行動；一方面使敵方的資訊系統拒絕為其提供服務；另一方面又要阻止敵方利用己方的資訊和資訊服務能力。

資訊戰的樣式

- 指揮控制戰
  - 保護己方指揮控制能力的同時，削弱或破壞敵方的指揮控制能力，以便最終奪取制資訊權。
- 情報戰
  - 使己方指揮者能及時得到所需情報，並使敵方指揮者無法得到所需情報。
- 電磁戰
  - 電磁攻擊
    - 利用電子干擾、欺騙、定向能武器來破壞、摧毀或利用敵方使用電磁波段的能力。
  - 電磁防護
    - 防護己方使用電磁波段的能力。
  - 電磁戰支援
    - 搜尋敵方發射源，並查明敵方可能之行動。

資訊戰的樣式 (2)

- 心理戰
  - 穿透敵方的媒體防護，以向敵方軍民傳達經過挑選的的資訊，瓦解敵方軍民士氣、分化敵方陣營、削弱敵方戰力，達到不戰而屈人之兵或最小代價之勝利。
- 網路戰
  - 情報刺探
    - 能取得千軍萬馬也不見得可得到的情報。
  - 網路攻擊
    - 能做到千軍萬馬也不見得能達成的有效破壞。

陸海空星電一體化網路作戰

- 陸海空星電
  - 現代戰場已經從傳統的陸海空戰域，擴展到大氣層外的星空，以及無形的光電磁空間領域，誰能奪取制星權，就能居高臨下掌握戰場，誰能掌握光電磁網路空間，就能掌握廣大空間優勢。
- 陸海空星四大實體空域的各種作戰軍隊與設備，都需倚靠光電磁網路之資訊傳導，故制網路權已經成為各先進國家極為重視的戰法。

網路攻防戰的難題

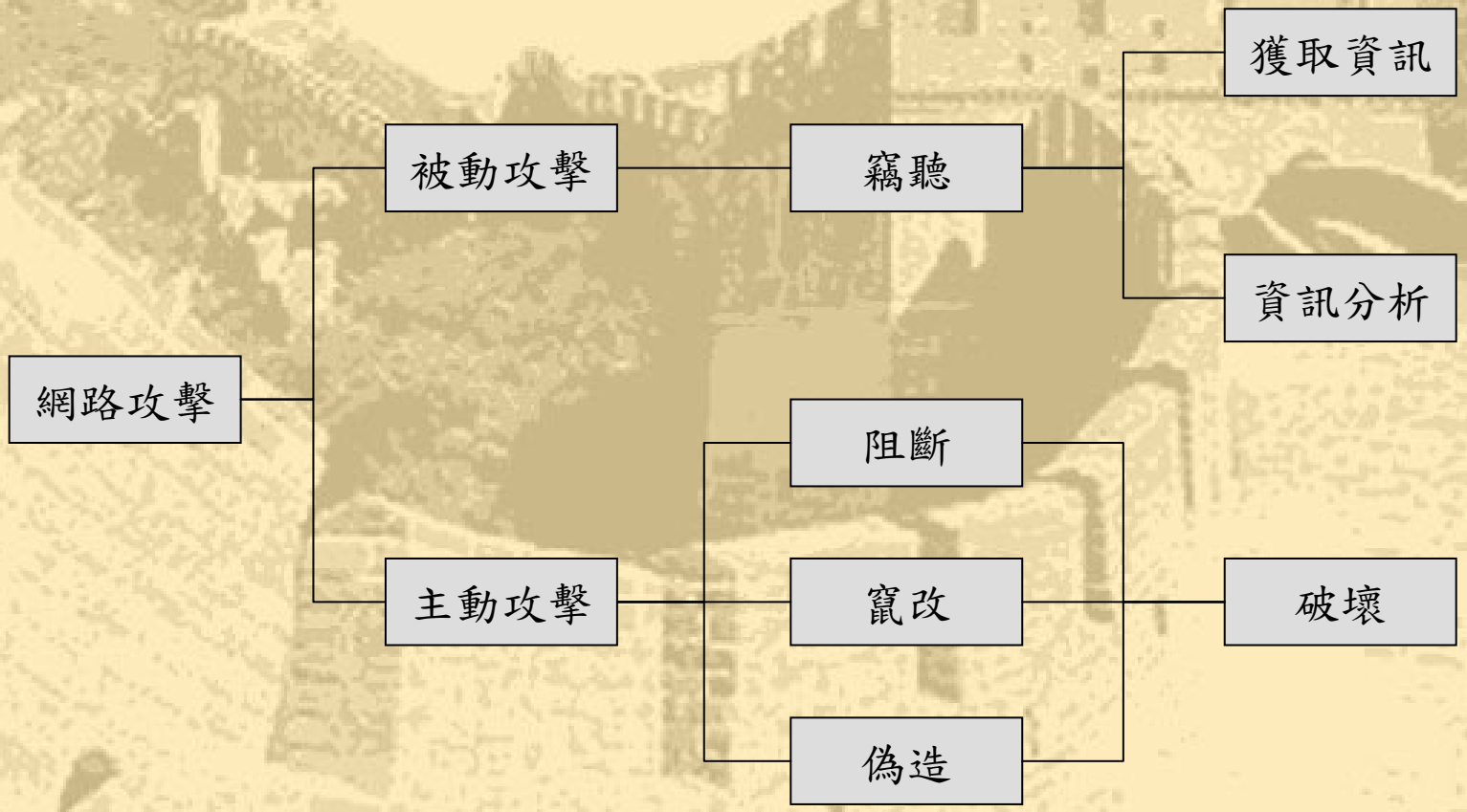
- 攻擊
  - 難以克服物理上隔絕的敵方網路。
  - 難以隱蔽地自敵方網路中傳出竊得的資訊而不被察覺。
  - 難以保護自身不被暴露及反追蹤來源。
- 防禦
  - 技術已基本成熟，實際產品也較多，但新技術總會比攻擊慢一步。

安全的性質

- **CIA**
  - **C：機密性(Confidentiality)**：資訊不得被未經授權之個人、實體或程序所取得或揭露的性質。
  - **I：完整性(Integrity)**：對資訊之精確與完整安全保證的性質。
  - **A：可用性(Availability)**：已授權實體在需要時可存取與使用資訊之性質。
- **AAA**
  - **Authentication 認證：確認身份**
  - **Authorization 授權：授予應得之權限**
  - **Accounting 稽查：記錄其行為**
- **其他性質**
  - **可鑑別性(Authenticity)**：可證明一主體或資源之識別就是其所聲明者的特性。鑑別性適用於如使用者、程序、系統與資訊等實體。
  - **可歸責性(Accountability)**：確保實體之行為可唯一追溯到該實體的性質。
  - **不可否認性(Non-repudiation)**：對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。
  - **可靠性(Reliability)**：始終如一預期之行為與結果的性質。


網路攻擊

網路攻擊方式



網路攻擊的步驟

- 調查目標網域
  - 網路拓樸結構、主機、OS、服務、應用程式資訊
- 擬定攻擊目標與策略
- 掃瞄目標系統
- 攻擊目標系統
  - 獲得超級權限
  - 銷毀或弭平入侵痕跡
  - 確保再控制能力
  - 獲取所要資訊、破壞目標資訊
  - 植入邏輯炸彈或代理人程式
- 發掘目標系統與其他系統的信任關係，並藉此攻擊其他系統

常見網路攻擊手段

- 服務阻斷型攻擊
- 侵入控制型攻擊
- 資訊收集型攻擊
- 假資訊攻擊
- 破壞型攻擊
- 解密攻擊
- 鑑別偽造攻擊

常見網路攻擊手段(1)

- 服務阻斷型攻擊
  - Ping of Death：ICMP size crash
  - Teardrop：IP segment number overlay
  - UDP Flooding：UDP echo loop
  - SYN Flooding：Fake Three Hand Shaking
  - Land：SYN-ACK loop
  - Smurf：Ping echo to broadcast address
  - Fraggle：smurf using UDP echo
  - 郵件洪水攻擊
  - 畸形封包攻擊
  - 大封包洪水攻擊

常見網路攻擊手段(2)

- 侵入控制型攻擊
  - 通行碼猜測
  - 特洛伊木馬
  - 緩衝區溢出

常見網路攻擊手段(3)

- 資訊收集型攻擊
  - 掃瞄攻擊
    - Ping scan、Port scan、Reset、SYN-ACK、DNS-Reply
  - OS探測
    - 壞封包回應檢測
  - 利用服務
    - DNS Zone Data Transfer
    - Finger
    - LDAP
  - Sniffer

常見網路攻擊手段(4)

- 假資訊攻擊
  - 偽造回應
    - DNS
    - Web
  - 偽造 Email
  - 綁架連線

常見網路攻擊手段(5)

- 破壞型攻擊
  - 邏輯炸彈
  - 病毒
  - 硬體元件攻擊
    - 改寫EEPROM密碼
    - 改寫BIOS密碼
    - 以微生物侵蝕元件

常見網路攻擊手段(6)

- 解密攻擊：以找出加密法與金鑰為最終目標
  - 唯密文解密（最難）
  - 同內容之密文明文參照解密（最易）
  - 來源密文與回應明文選擇參照解密

常見網路攻擊手段(7)

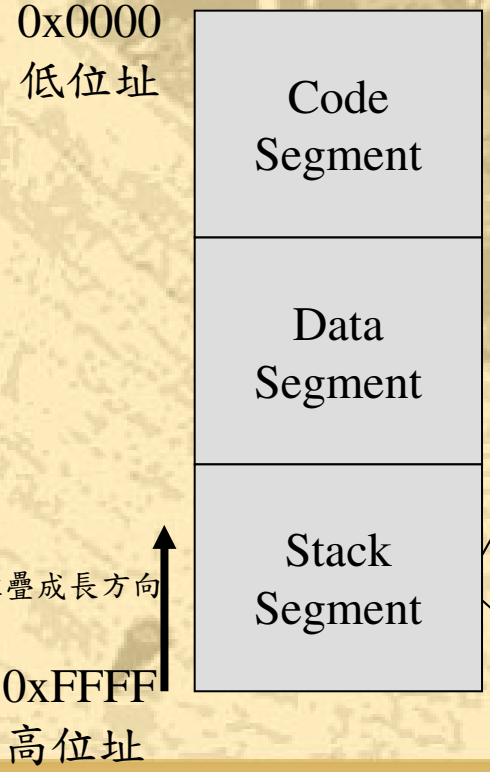
- 身份鑑別冒充攻擊：冒充合法身份入侵系統或劫取金鑰。
  - 反射攻擊
  - 中間人攻擊
  - 重放攻擊

主要攻擊技術分析

- 緩衝區溢出攻擊技術
- 欺騙攻擊技術
- 病毒技術
- 特洛伊木馬技術

主要攻擊技術分析(1)

- 緩衝區溢出攻擊技術
  - Runtime Process 結構分區與堆疊溢出原理



大部分CPU與OS實作堆疊的方式多半是從記憶體高位址往低位址使用，作為執行期動態配置的區域變數記憶體空間。
常數與全域變數則置放於資料節區。

0xF000 char buf2[5]
0xF008 char buf1[10]
0xF014 EBP（前一個堆疊返回位址）
0xF018 RET（函式結束返回位址）
0xF01C 參數1
0xF020 參數2
0xF024 參數3

gets(buf1);
沒檢查輸入長度
可輸入遠超過10bytes的入侵程式碼

最重要的覆蓋目標，導致返回至入侵程式碼位址繼續執行

主要攻擊技術分析(1)

- 緩衝區溢出攻擊技術
  - 植入法
  - 利用Process現有的Function Code
  - 修改Function Point
  - 修改longjmp指標

主要攻擊技術分析(2)

- 欺騙攻擊技術
  - IP欺騙
    - 推測B連A的Three-Hand-Shake序列號
    - 癱瘓主機B
    - 假冒B繼續跟A完成Three-Hand-Shake
  - DNS欺騙
    - B發出DNS request 給 DNS server A
    - 搶在A之前假冒A reply 假的回答給B
  - Web欺騙
    - 建立與假冒對象相似的網頁
    - 把假的URL植入熱門網頁或Email，誘使USER至假網頁
    - 將USER的動作轉達至真網頁，並將回應轉達給USER

主要攻擊技術分析(3)

- 病毒技術
  - 抗分析病毒技術
    - 自我加密技術
    - 反跟蹤技術
  - 隱形病毒技術
  - 自我變化型病毒技術
  - 嵌入性病毒技術
  - 超級病毒技術
  - 破壞性感染病毒技術
  - 自我進化型病毒技術
  - 誘騙型病毒技術

主要攻擊技術分析(4)

- 特洛伊木馬技術
  - 隱藏Port
    - 寄生：寄生在正常服務的Port
    - 潛伏：平時不開Port，受到特殊條件觸發（例如ICMP）才開Port
    - 嵌入網路驅動程式、系統動態函式庫、Kernel
  - 隱藏通信
  - 隱藏Process
  - 反向Port

硬體式網路攻擊

- 飛彈、炸彈
  - 直接毀壞網路設備、機房等等
- 微波武器
- 電磁脈衝武器
- 微生物兵器