第8章

弱點評估與管理(邵立翔)

1. 公開蒐集

多來自媒體，網路社群，公開社群，觀察報告，專業學術活動，深度網路。

1. 蒐集技巧

證書透明度(certificate Transparency，CT)；Censys ; 內容安全政策(Content Security Policy ，CSP); WHOIS服務; 自治系統(AS);

1. Google hacking

常用指令:intext,intitle,cache,define,filetype,info,related,inurl,site; 搜尋引擎 Bing & Shodan;

1. 公共漏洞與暴露

(CVE)Common Vulnerabilities and Exposures 有資安資料庫專門蒐集漏洞

1. 評鑑系統

(CVSS)Common Vulnerability Scoring System運用數學方程式判定某特定網路是否安全

惡意程式種類與防護(邵立翔)

1. 威脅弱點

威脅(threat)弱點(vulnerability):存在的弱點本身不會造成傷害，必須是攻擊才算威脅

1. 零時差攻擊

(Zero-day Attaack 0-day):無法被漏洞工具偵測掃描，並在發布的第一時間攻擊

1. 惡意程式種類

病毒，蠕蟲，木馬程式，釣魚網頁，間諜軟體

1. 電腦病毒種類/躲避監視種類

複合型病毒()巨集病毒()反防毒病毒()千面人病毒()隱藏型病毒()變體()通道()

加殼病毒

1. 早期電腦病毒
2. 惡意程式的種類
3. 混和攻擊
4. 攻擊工具(特權提升)
5. 網際攻擊狙殺鏈
6. 資訊安全防禦機制
7. 惡意程式事件處理程序

加密勒索軟體攻擊(黃建龍)

1. 加密勒索攻擊
2. 勒索軟體感染方式
3. 勒索軟體及服務
4. 感染勒索後的應變措施

駭客攻防 (黃建龍)

1. 分類
2. 階段過程
3. 隊伍介紹

資訊安全備份管理(湯芸姍)

1. 生命週期
2. 備援及層次應用
3. 備份策略
4. 備份計畫內容
5. 資料區分
6. 方式與媒體
7. 位置模式
8. 差異比較
9. 平率與保留週期
10. 工具
11. 備份回復測試

日誌管理

1. 資訊安全監控維運中心
2. 主要功能
3. 八大習慣
4. 事件管理
5. 異常行為