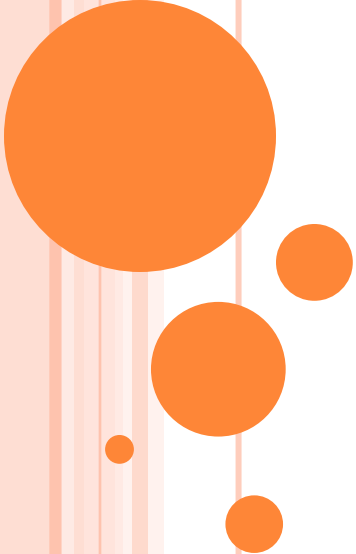




企業機房的資安維運與監測

面對資安的巨大挑戰，企業必須積極部署防護

關於本次課程內容與注意事項

- 一共分為三個SESSION
- 每個SESSION約50分鐘
- 每個SESSION中場會休息5-10分鐘
- 最後的SESSION會有Q & A時間，上課時也能發問
- 講課內容會視來賓的專業程度而做適度調整，希望大家來聽課都能有滿滿的收獲
- 資安議題不是紙上談兵就好，所以特別安排現場示範，讓大家看看實際的駭客攻擊狀況
- 上課時請勿錄音、錄影，以尊重講師智財權
- 上課前請將手機切換為靜音或關閉，謝謝合作



講師：李志文 KEN.LEE@TTS.BZ

「優福網資訊有限公司」的創辦人

- 從事IT產業已超過20年，AWS已使用12年以上
- 2008年就開始使用AWS雲端，2009年開始分享雲端
- 2010年開發出手機保姆App，獲得國內許多媒體報導
- 因此而受邀至許多知名企業和學校單位演講雲端
- 2012和2014年各花了幾個月進行幾大公有雲的實測
- 曾協助國內知名遊戲業者改善AWS雲端使用成本，迅速幫客戶省下每月**百萬**台幣的雲端費用
- 曾為知名電商平台(Lativ)提供雲端教育訓練課程
- 為了協助客戶，我還獨力開發了幾個雲端工具
- 2017年開發出清查雲端工具INSTAWATCHER
- 2018年正式授權獨家代理三年給AWS台灣代理商



全台最用心的雲端顧問

[HTTPS://WWW.TTS.BZ](https://www.tts.bz)

協助您在不同階段善用雲端服務

Step 1

了解雲端服務

AWS教學手冊

協助客戶學會操控AWS等雲端服務

Step 2

挑選雲端廠商

三大公有雲實測

協助客戶挑選合適的雲端廠商

Step 3

評估雲端成本

問雲

協助客戶快速試算雲端成本並找出最佳方案

Step 4

管理雲端資源

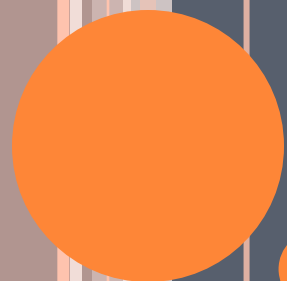
INSTAWATCHER

協助客戶管理雲端主機和掌握使用資源

AWS教學手冊、三大公有雲實測報告、問雲、INSTAWATCHER的開發者
曾為知名企業省下每月100萬的雲端費用、協助他們管理26個AWS帳號



全台最用心的雲端顧問
李志文 ken.lee@tts.bz



SESSION (一)

SESSION (一)

- 企業機房常見的硬體設備
- 企業機房的核心硬體設備
- 企業機房常見的網路架構
- 企業機房的其它連網設備
- 企業機房常見的各種對外服務
- 企業機房常見的遠端管理方法
- 企業機房常見的資安防護設備



企業機房常見的硬體設備

阿Ken講雲



機房中常見的硬體設備

企業機房的核心硬體設備

阿Ken講雲



機房中常見的硬體設備

企業機房常見的網路架構



企業機房的其它連網設備

- 遠端KVM (例如IP KVM)
- IoT設備 (例如智慧插座)
- DVR／IPCam設備
- 門禁設備



企業機房常見的各種對外服務

- Web服務 (http／https)，包括各種API服務
- Email服務 (smtp／pop3／imap...)
- 檔案傳輸服務 (ftp／smb／scp...)
- 影音即時串流服務 (RTSP)
- 其它自訂的socket連線服務 (例如proxy／chat...)
- 資料庫服務，安全的做法是透過API來提供
- 檔案儲存服務，安全的做法是透過API來提供
- 遠端管理服務，方便管理人員從遠端進行管理



企業機房常見的遠端管理方法

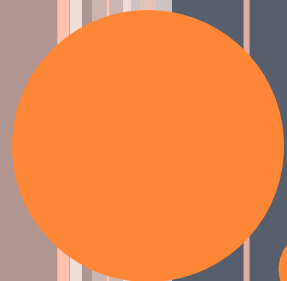
- VPN
- SSH
- RDP
- VNC
- 遠端KVM (例如IP KVM)



企業機房常見的資安防護設備

- 防火牆／次世代防火牆
- VPN
- IDS／IDP／IPS
- UTM
- WAF
- AntiSpam
- AntiVirus





SESSION (二)

SESSION (二)

- 企業機房與雲端服務的混合模式
- 淺談雲端服務的資安防護措施
- 了解雲端服務的潛在資安風險
- 資安的防護要從主機監測做起
- 現今常見的監測軟體介紹
- INSTAWATCHER的介紹
- INSTAWATCHER的比較
- INSTAWATCHER實機示範
在實體主機和雲端主機運作INSTAWATCHER



企業機房與雲端服務的混合模式

- 透過任務／服務的分割來進行混搭
- 利用Site to Site VPN串接至雲端
- 直接從機房串接至雲端 (Direct Connect)



淺談雲端服務的資安防護措施

- AWS的資安防護措施從機房實體開始做起，包括：
 - # Physical and Environmental Security
 - # Network Security
 - # AWS Account Security...

https://aws.amazon.com/tw/architecture/security-identity-compliance/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=*all&awsf.methodology=*all
- 使用AWS雲端服務時就能享有基本的網路資安防護
- 若需要進階的資安防護，也可付費租用，例如WAF



了解雲端服務的潛在資安風險

- 登入的帳號沒有啟用MFA (二次驗證機制)
- 沒有定期清查IAM帳號權限
- S3 Bucket權限設為公開
- 程式碼內嵌重要的Key
- 會造成的資安問題
 - # 存放在S3雲端儲存空間的資料外洩
 - # IAM權限不夠完善，造成資料外洩
 - # Key的外洩導致資料外洩、被盜開主機、損失大量金錢...
- 國外曾有案例就是因為雲端資安沒有做好，被駭客入侵後，導致公司關閉（Code Spaces，現在的網域名稱被其它公司註冊用來做廣告）



資安的防護要從主機監測做起

企業必須監看伺服器運作狀態的原因

掌握效能瓶頸

能清楚知道伺服器的運作狀態才能判斷效能瓶頸所在：

- △CPU用量
- △高CPU用量的程式
- △MEM用量 (記憶體)
- △高MEM用量的程式
- △即時網路流量 (In & Out)
- △每小時網路流量 (In & Out)
- △磁碟空間用量

預防勝於治療

避免資安風險

下列項目可協助判斷是否受到駭客攻擊或入侵：

- △TCP服務埠
- △CPU用量
- △高CPU用量的程式
- △網路流量 (In & Out)
- △磁碟空間用量

避免資料損毀

若有監測伺服器運作狀態，並結合主動通知機制時，就能提早發現異常、避免問題發生或擴大。當然，唯有落實完善的備援機制才能真正避免資料的損毀。

控管營運成本

確認效能瓶頸後才能有效控管成本：

- △不必亂花錢盲目升級伺服器等級
- △不必浪費時間胡亂猜測問題所在
- △知道問題才能找對解決方案
- △時間和人力都是重要成本

提早發現問題 避免問題擴大

避免服務中斷

伺服器服務會中斷的常見原因：

- △CPU用量持續偏高造成當機
- △MEM用量持續偏高造成當機
- △磁碟空間不足造成服務異常
- △網路頻寬不足(用雲端就不怕)
- △被駭客攻擊或入侵

INSTAWATCHER
Save your time, save your money.

現今常見的監測軟體介紹

- Open Source的監測軟體
 - # Nagios
 - # Cacti
 - # Zabbix
 - # LibreNMS
- 商業付費的監測軟體
 - # Nagios XI
 - # DataDog
 - # WhatsUp Gold
 - # Solarwinds
- 我們自行研發的AWS清查和主機監測軟體
 - # INSTAWATCHER



INSTAWATCHER的介紹

- 能快速清查N個AWS帳號在16個Region的使用資源
- 不必花錢購買監測專用伺服器
- 支援各家雲端平台的主機
- 超過自定警戒值會發送簡訊
- 能一次掌握單台主機的所有運作狀態
- 也能一次掌握所有主機的運作狀態
- 採用多重設計阻絕資安風險
- 採用交叉架構避免偵測服務中斷
- 可針對特定主機設定斷線通知
- 更多詳情可參考

<https://instawatcher.pro/introduction/>



INSTAWATCHER的比較

INSTAWATCHER

- ☀ 服務安全可靠
- ☀ 使用價格合理
- ☀ 資訊完整透明
- ☀ 部署迅速容易
- ☀ 操作簡單易懂
- ☀ 不必自行維運

- 👍 不必聘請專業的IT員工
- 👍 不必自行購買伺服器設備
- 👍 不必自行建置與維運伺服器
- 👍 安裝簡單不需要設定防火牆
- 👍 操作介面簡單且超級友善
- 👍 功能足夠且都是實際需要
- 👍 不能反向控制可確保資安
- 👍 不需要花錢和時間上課

年度成本概估：新台幣3.6萬元 (以監看10台為例)

- △ 伺服器硬體：0元 (由我們提供)
- △ 伺服器軟體：0元 (由我們提供)
- △ IT人員薪資：0元 (不必再請一個專人來顧)
- △ 可監看數量：沒有限制 (可視數量隨時擴展)
- △ 網路頻寬、電費、簡訊費用均由我們提供

為何需要掌握伺服器運作狀況?

掌握效能瓶頸
控管營運成本
避免服務中斷
避免資安風險
避免資料損毀

好工具把事情簡單化而非複雜化

歡迎來信洽詢

service@instawatcher.pro

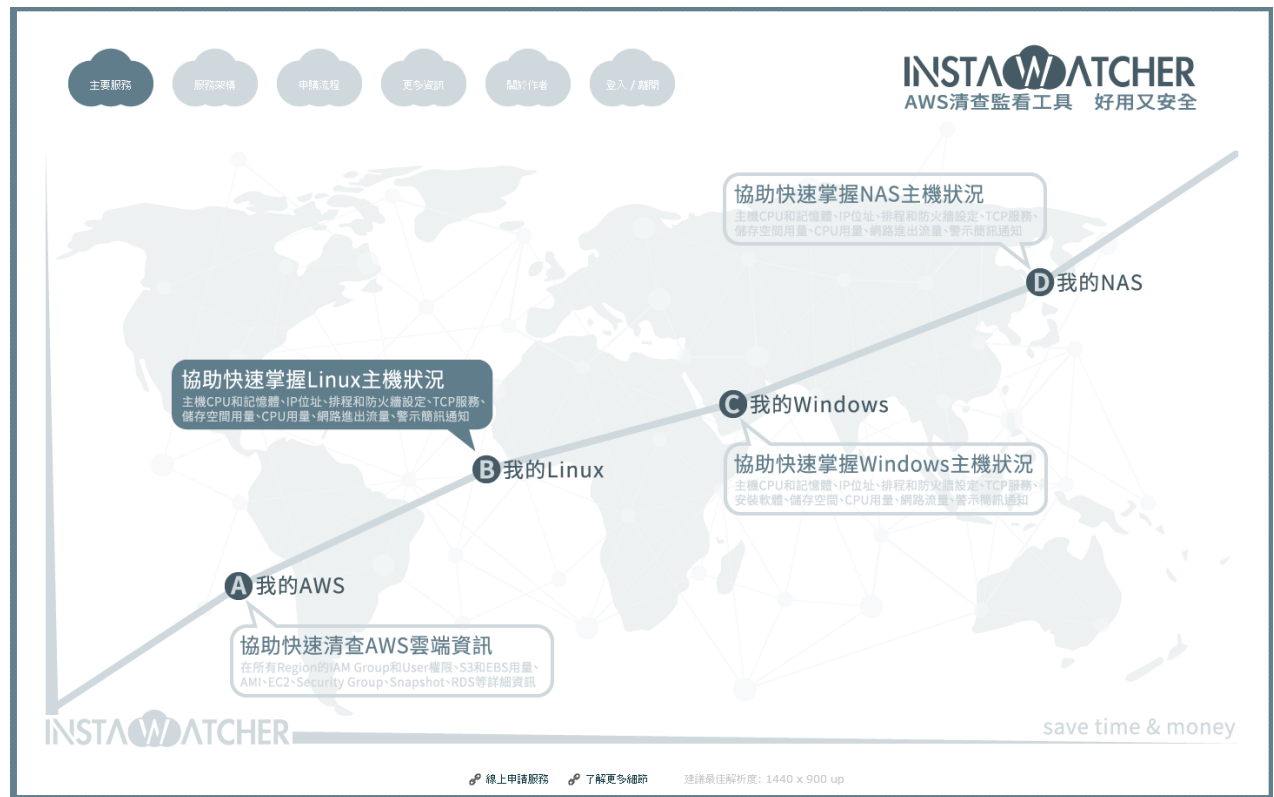
一般常見監控軟體



- △ 需要聘請專業的IT員工
- △ 需要自行購買伺服器設備
- △ 需要自行建置與維運伺服器
- △ 安裝麻煩並需要設定防火牆
- △ 操作介面難懂且不夠友善
- △ 功能超級多實際卻不需要
- △ 可反向控制須要注意資安
- △ 可能需要花錢和時間上課

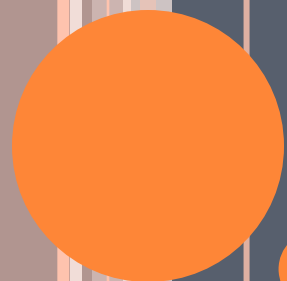
年度成本概估：新台幣45萬元 (以監看10台為例)

- △ 伺服器硬體：3萬元 (DIY型的電腦主機)
- △ 伺服器軟體：0元 (這裡使用免費軟體)
- △ IT人員薪資：42萬 (以最低年薪來算)
- △ 可監看數量：10~30台 (視伺服器可承載能力)
- △ 尚未納入計算的成本：網路頻寬、電費、簡訊費用



實機示範

在實體主機和雲端主機運作INSTAWATCHER



SESSION (≡)

SESSION (三)

- 駭客入侵的執行階段與常見攻擊手法
- 駭客進行入侵攻擊的兩大重要主軸
- CDN服務對於駭客攻擊的防護能力
- 駭客和資安公司都愛用的專業工具
- Kali Linux攻擊示範
弱點掃描攻擊和INSTAWATCHER監測



駭客入侵的執行階段與常見攻擊手法

- 駭客入侵執行階段可概分為：
 - # 情報的搜集（可分為被動掃描、主動掃描）
 - # 威脅建模
 - # 漏洞分析
 - # 漏洞利用
 - # 後滲透攻擊
 - # 完成攻擊並建置後門
- 駭客的人侵可能會從委外廠商、企業員工迂迴而來
- 駭客除了使用滲透攻擊工具直接攻擊以及透過各種破解軟體、電子郵件、手機簡訊和網站來誘騙，也會使用社交工程手法與AI語音詐騙方式，還能透過USB Rubber Ducky、Aroduino或OMG連接線入侵



駭客進行入侵攻擊的兩大重要主軸

- 作業系統（Operating System）
 - # Windows
 - # Linux
- 軟體程式（Application）
 - # 有提供對外服務的Application，例如Web、Email
 - # 能穿透防火牆與外部連線的Application，例如p2p

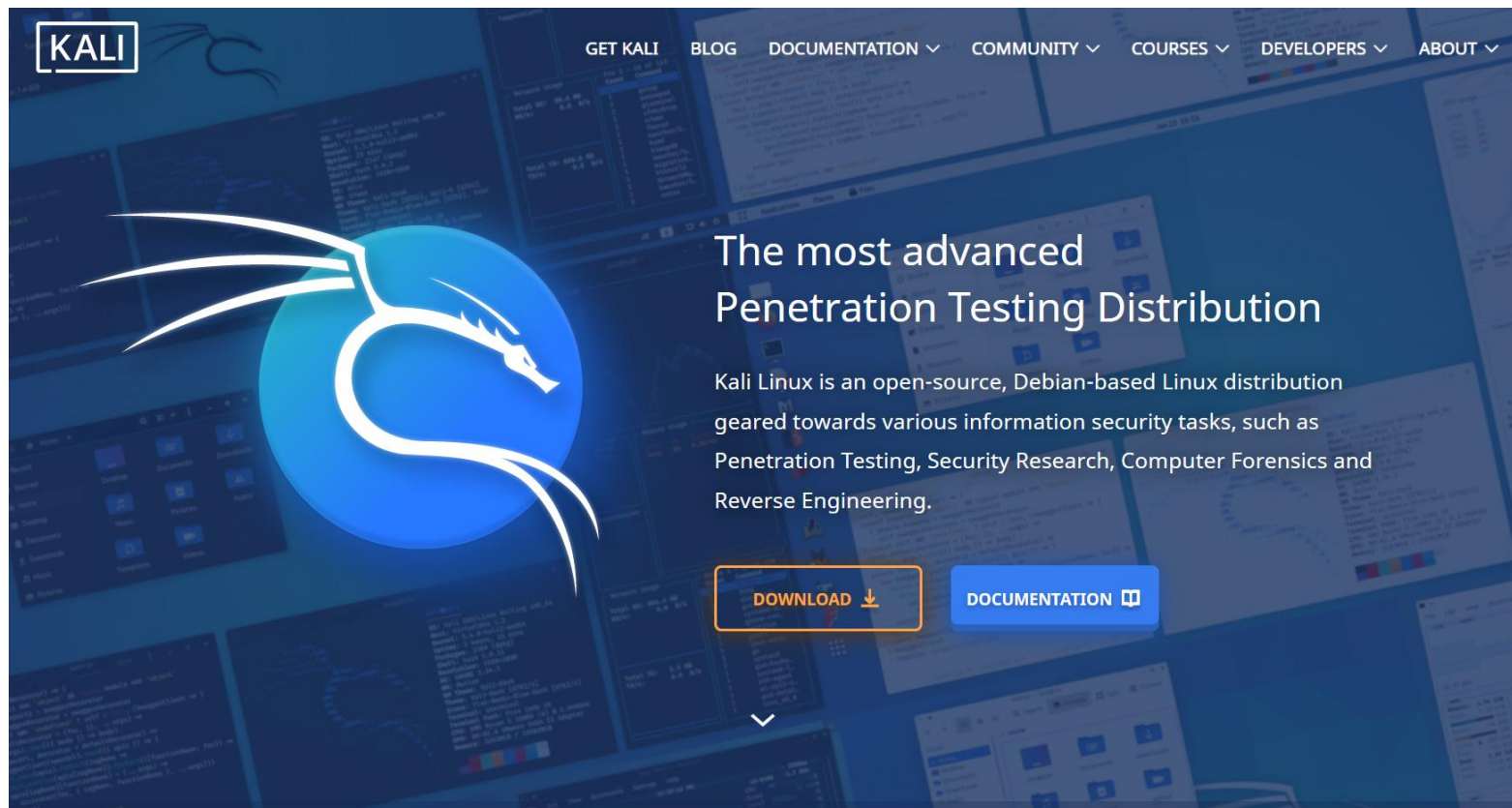


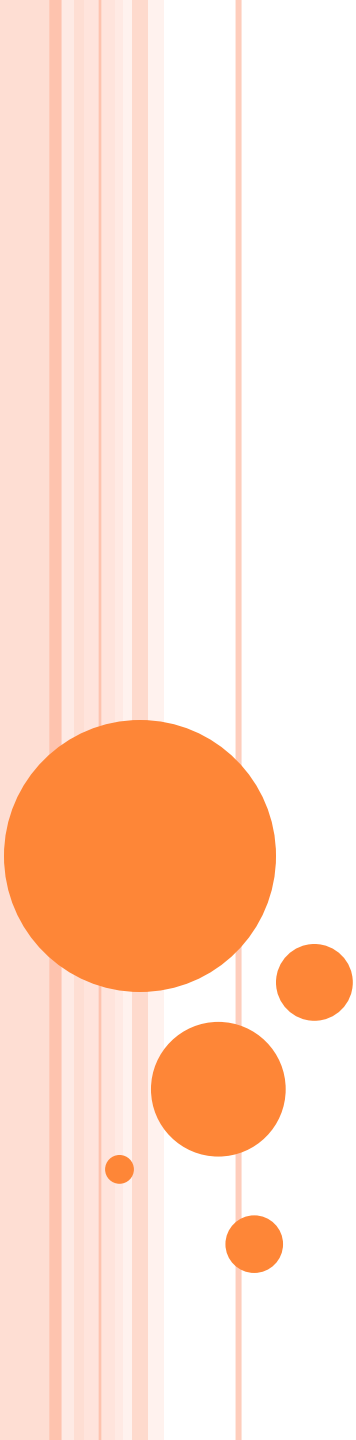
CDN服務對於駭客攻擊的防護能力

- CDN主要是將圖片、影片等內容cache至全球節點
- 最重要的能力是可以緩解DDoS等大量連線的攻擊
- 想要針對Web Application的攻擊就必須啟用更進階的防護服務，例如WAF (Web Application Firewall)
- CloudFlare還能代管DNS，能有效隱藏主機IP
- 實際上企業對外服務的主機還是會有Public IP
- 一旦駭客透過OSINT找出企業主機的真實Public IP，就能繞開CDN，直接針對該主機進行各種滲透攻擊



駭客和資安公司都愛用的專業工具





KALI LINUX攻擊示範

弱點掃描攻擊和INSTAWATCHER監測



Q & A

謝謝大家參加今天的課程，希望都能有滿滿的收獲

Q & A時間



優福網資訊有限公司

[HTTPS://WWW.TTS.BZ](https://www.tts.bz)

