出國報告(出國類別：訓練)

參加 HITB 於荷蘭阿姆斯特丹舉辦之「2023 年 Hack In The Box Security Training for Abusing Active Directory」

服務機關：桃園國際機場股份有限公司

姓名職稱：彭俊智 (工程師)

派赴國家/地區：荷蘭/阿姆斯特丹

出國期間：112 年 4 月 14 日至 4 月 20 日

報告日期：112 年 5 月 5 日

目錄

摘要

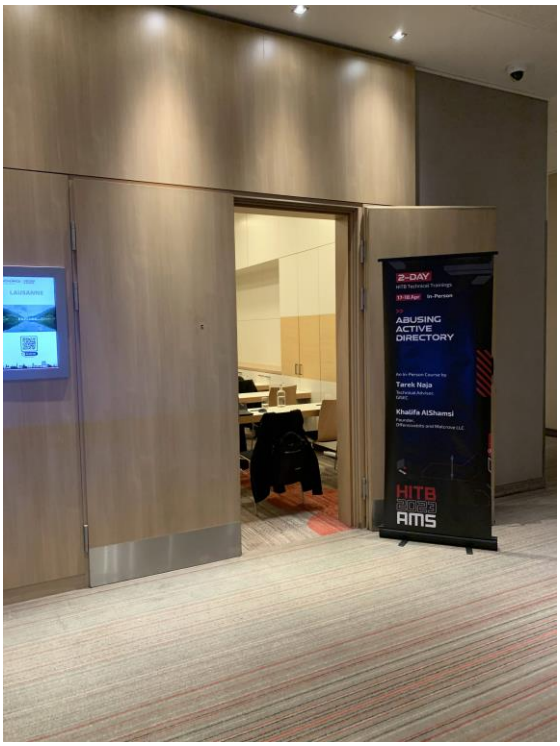
隨著各類新興科技迅速發展，總統曾經於公開場合不斷強調「資安即國安」，且近來資安攻擊事件頻傳，無論是系統及個人資料受到的威脅越來越多，攻擊態樣多元且頻繁。本公司為關鍵基礎設施，且為特定非公務機關之最高責任等級，除了強化自身資安防護能力，亦無時無刻培養專業人員之資訊與資安技術能力與素養。

政府近年來持續強化國家層級的資訊安全外，期待與大家共同努力提升資安防禦及應變能力，進一步強化整體韌性。面對接踵而來且沒有煙硝的資訊及網路戰，沒有人可以置身事外，亦隨時隨地皆可發生。隨著 2018 年通過，「資通安全管理法」，2022 年 8 月數位發展部成立；爰此，強化資安需要綜合考慮各個方面，包括技術、策略、人員等，並進行定期評估和測試，不斷更新和改進相關措施，從而提高資安水準，進而保護公司或組織之資訊資產。

2023 年 4 月 17 日至 21 日於荷蘭阿姆斯特丹舉行之「HITBSecConf2023 - Amsterdam」除了論壇亦包含本次資安訓練 Abusing Active Directory, Hacking BLE, Hacking RFID/NFC, IC Reverse Engineering & Code Extraction, Offensive Mobile Reversing and Exploitation, Introductory Automotive Cyber Security 等等。從 IT 安全 IoT 安全與 OT 安全皆有探討，以深入淺出講解並輔以實際操作，使更為深刻，恰能符合並精進資安相關職能之需要。

壹、目的

行程日期	地點	紀要
112/4/14	桃園-荷蘭 阿姆斯特丹	啟程(CI73)2240~0720L
112/4/17 至 112/4/18	荷蘭 阿姆斯特丹 Movenpick(莫凡比飯店)	本次主要參與「Abusing Active Directory」教育訓練，範圍主要以地端自建 AD 與導入 AZURE AD 為主軸，探討 AD 本身的安全性與利用 Power Shell 如何取得相關 AD 資訊與提權。了解 APT 如何在本地和公/私有雲中濫用 Active Directory。對於系統工程師、滲透測試人員與可能執行紅藍軍成員，更可了解 AD 之 PowerShell 操作功能，倘若無積極與良善監管，反之易使駭客為之所用。
112/4/19+1	荷蘭 阿姆斯特丹-桃園	返程(CI74)1100~0600L



圖一 HITB Abusing Active Directory 訓練會場

圖二 HITB 訓練教室

貳、過程

課程主講為 Khalifa Alshamsi，他有 12 年的網路安全經驗，且為一家位於杜拜且專精於網路安全防禦公司的共同創辦人之一，講師照片如下圖所示。主要課程大綱如下：

1. PowerShell 功能與介紹

Khalifa (@kha1ifuzz) started his Penetration Testing career in 2014. He is a founder of a Offensivebits and Malcrove, companies specializing in Managed Cyber Defense and Offensive Security services. He led more than 60 projects in Penetration Testing and Red Teaming. He has worked as Strategic Technical Advisor to many organizations in UAE and worked on multiple projects such as developing Penetration Testing tools and discovering vulnerabilities.

Khalifa has also participated as an assistant trainer at the BlackHat course "Attacking and Securing APIs" and is regularly invited to deliver talks and workshops.

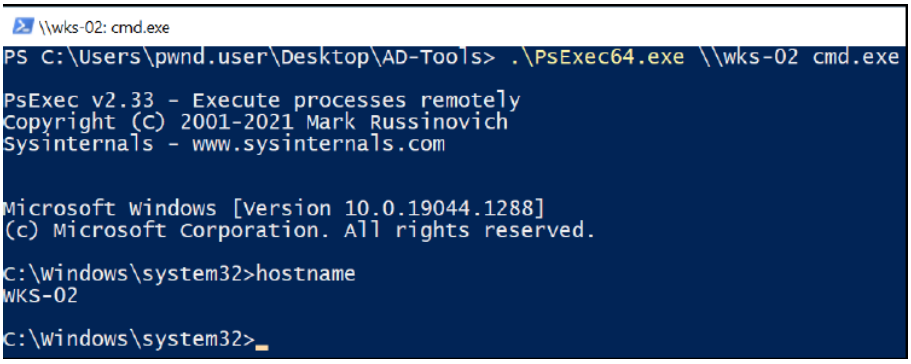
是一種由 Microsoft 開發的命令列介面和 script 語言。如同 LINUX 上有許多 SHELL，如 BASH、CSH、KSH 等等，而 Windows 系統預設的 shell，別於過去的批次檔(Batch file)，更是可用於自動化管理和配置 Windows 系統，與執行各種系統管理的功能或任務。主要特性在於跨平台的支援、具有物件導向與 pipeline 功能、整合微軟其他系統的能力如 AD、Exchange、AZURE 等。使用上有許多的基本功能，Get-XXX、Set-XXX 與整合 Pipe 與基本運算元-eq、-ne、-like、-Match 等。

BYPASS：它允許用戶繞過 PowerShell 的安全限制，執行未經信任的腳本和命令，使用 ExecutionPolicy 將其預設 Restricted 改為 Bypass，即可使用未經信任的腳本，便利駭客進行相關提權、系統核心操作等。

powerview.ps1：為開源 PowerShell 模組，用於快速和方便地執行 AD 列舉和攻擊。它是是攻擊者常用的工具之一，反之若愚受合法之的情況下使用 powerview.ps1，反而是非常高效能之管理工具。

2. Attack Plan(攻擊脈絡)：藉由找出目標使用者，透過 PS 語法並結合 SID 的判斷，找出 Domain Admin 管理員帳號，步驟有以下幾種。
   A. 找出 DC
   B. 找出網域管理員
   C. 找出網域管理員密碼雜湊
   D. 破解網域
   E. 破入目標伺服器
   F. 持續攻擊
3. Remote Access

   藉由遠端的方式竊取 AD 密碼的 HASH 值，常用的技術有 psexec, PS, WMI, WinRS, RDP, SMB Relay 等，上述幾種皆為 Windows 內建且合法使用的工具，可以簡化管理作業，但水能載舟亦能覆舟，反之不啻是駭客常用的工具之一。

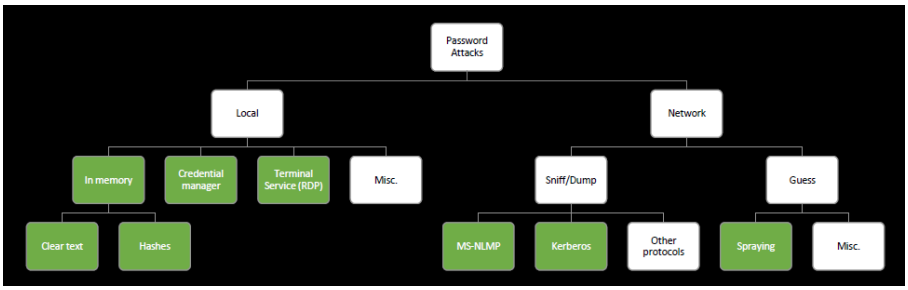


4. Password 攻擊

密碼攻擊的方式有許多類型，舉凡如暴力破解、字典攻擊、彩虹表、側錄、弱密碼儲存、封包分析等；如下圖所示，基本上可區分本地端與網路層，然而暴力破解最為容易相對也最為耗時。

其中密碼噴灑屬上述攻擊手法中的字典、彩虹表且與特定用戶的融合技術，它針對大量的帳戶嘗試使用少量的常見密碼，相較於使用大量的密碼，如彩虹表來進行暴力破解攻擊，這種攻擊方式比較有效且速度快。因為很多人在設置密碼時會使用簡單、容易被猜測的密碼，如「password、123456」等等。

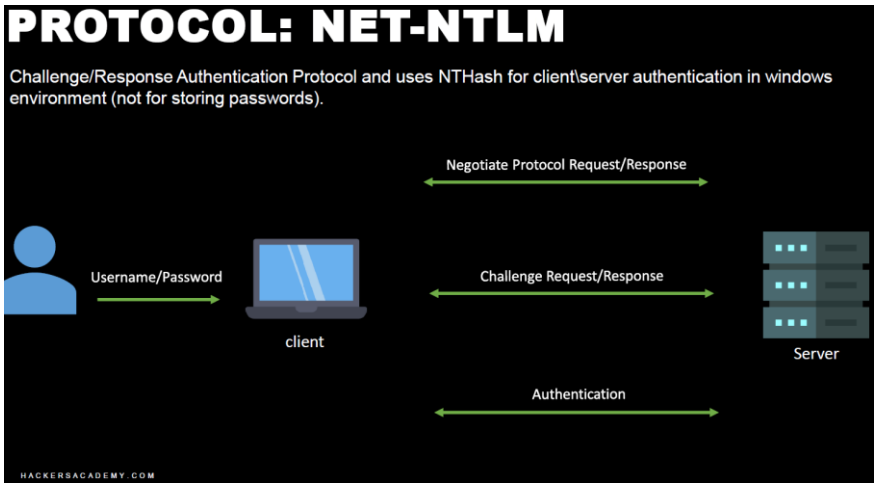
密碼策略：設定於 Group Policy 中，透過 PS 之 Get-ADDefaultDomainPasswordPolicy 即可取得，倘若藉由上述遠端存取的方式亦然。



5. Domain Password 噴灑

透過 Github 取得特定的 PS 語法，創建一個 userlist，並使用一個或多個常見密碼進行嘗試。攻擊者通常會在某個時間段內嘗試登錄大量的帳戶，但又可以最大限度地避免帳戶被鎖定，且無須最高權限即可執行。

Attacking NTLM



傳統之 NTLM 存在於如 LSASS、SAM 與 NTDS 等區域，且通常採 MD4 進行編碼並以 UTF-16 的方式儲存；常見之破解方式有離線取得明文之密鑰匙或雜湊值比對。

NTLM Hash Example: fc525c9683e8fe067095ba2ddc971889

NET NTLM-V1/V2

V1 則是炳棄傳統 NTLM 的雜湊演算法，進而改以 DES 的方式加密處理，並加上 16bytes 的亂數混合，增進破解之難度。

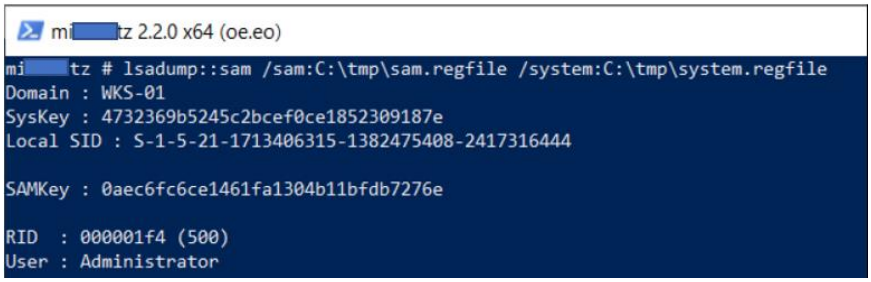
V2 則是較為近代使用之方式，Challenge 值除了亂數再加上時間戳記，並使用 HMAC_MD5 的方式加密處理。

NET-NTLMv2 capture Example:
Administrator::ALTO:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

由上述可見，改良後 V2 比傳統 NTLM 在祕文長度與複雜度上都精進許多，增加被破解的複雜度。

6. Dumping SAM 及 LSA 密文

密碼儲存於上述兩個資料庫中，可藉由常見的 M 開頭之駭客工具進行破解。



故防禦上，應該藉由 SOC 或是端點防護、防毒軟體等，加強監控並拒絕該軟體之執行，避免帳號與密碼遭受破解；另一方面，Windows 之 Sysinternal 的工具亦應該封鎖，避免遭受濫用。

7. Kerberos

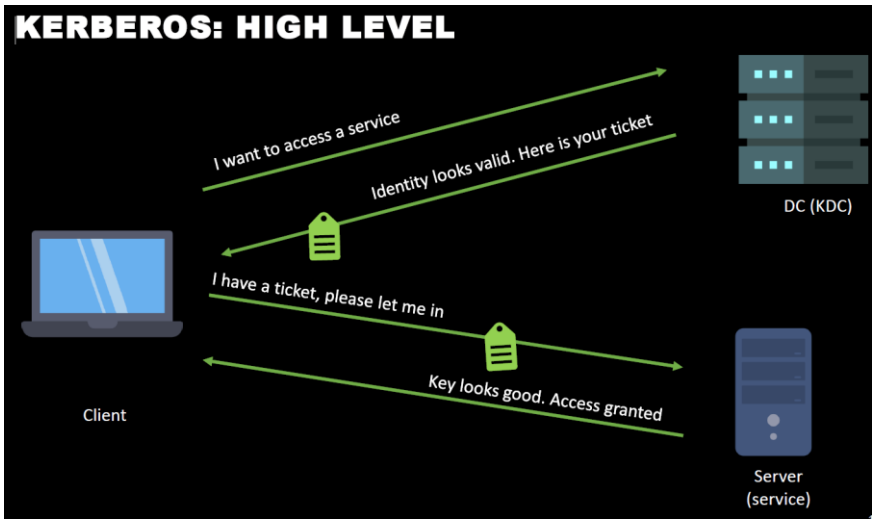
取代現行 MS-NTLM 認證，新版之 Windows 皆使用該身分認證技術，並使用 TCP/UDP 88 當作溝通埠口，倘若失效則回復 NTLM。

功能上主要為使用者欲存取系統服務時進行身份確認，有以下幾種角色構成該服務之運行：

A. KDC：通常運行於 DC，並針對 Kerberos 認證服務之伺服器。
B. AS：接收認證請求。
C. TGT：用於加密 krbtgt 金鑰，用於使用者於 KDC 中請求核發票證。
D. TGS：用於加密 service 金鑰，用於使用者存取服務之認證。

運行概念如下圖所示：

A. Client：對 DC 發送一個服務請求。
B. DC：確認該使用者的票證 Ticket 是否合法。
C. Clent：取得一個有效之票證。
D. DC：確認該票證為有效，允許存取。



8. Kerberos 缺失與破解方式

A. AS-Rep Roasting

使用者帳號可能被設定為「Do not require Kerberos pre authentication」。藉由離線的方式破解該加密的使用者密碼。主要是利用該用戶被設定為無需使用 Kerberos 的 pre authentication，導致該用戶密碼僅以較弱的加密演算法加密，僅利用 ReXXus 工具即可輕易取得用戶密碼。

防禦上可由以下幾種方式：

- 強化密碼的長度、複雜度等。
- 找出有被設定為無須 Kerberos pre authentication 的用戶

```
Get-ADUser -Filter 'useraccountcontrol -band 4194304' -Properties
useraccountcontrol | Format-Table name
```

- 找出有權限設定的用戶

(Get-ACL "AD:$((Get-ADUser -Filter 'useraccountcontrol -band 4194304').distinguishedname)").access

B. Kerberoasting

Kerberoasting 攻擊是 Tim Medin 在 DerbyCon 2014 上發佈的一種攻擊方法，同時亦發佈攻擊工具 kerberoast。此後，才意識到該微軟之服務的相關弱點，相關研究人員也對該攻擊手法進行改進；目前在 GitHub 上揭露了許多針對該弱點之工具，促使 Kerberoasting 進而發展成為 AD 攻擊的方法之一。

攻擊條件：

- 取得 AD 一般使用者帳號。
- Service Principle Name(SPN)

SPN 是使用 Kerberos 驗證之網路服務之 unique 識別碼，組成的元件包含服務類別、主機名稱，亦包含連接埠。通常 Windows AD 內建帳號會自動註冊 SPN，然而一般使用者 AD 的帳號在執行時，需手動的方式註冊 SPN，相關與法如下列所示。

```
Setspn -s http/<computer-name>.<domain-name> <domain-user-account>
```

網域內主要有主機帳號、使用者帳號、服務帳號等 3 種類型：

- 主機帳號：由系統隨機設置，且每 30 天自動變更一次。
- 使用者帳號：通常密碼之複雜度由電腦 Policy 制定，如 GCB 之帳號及密碼原則；而於複雜度要求較高的網域，增加破密之複雜度。
- 服務帳號：通常應用軟體安裝時自動設定，且 SPN 幾乎不會異動，由於大部分應用軟體沒有提供修改服務帳號的功能和介面，例如 MS SQL Server 服務的 sqlsvc 帳號。

參、心得及建議

本次課程雖然只有短短 2 天，重點主要探討 Windows AD 的濫用與攻擊手法，技術上約莫 90%皆以 Power Shell 工具進行操作、10%則採開源之破密工具程式。

課程要求每位學員自備 NB，且得具備一定的硬體規格，以利架設 VM 環境(包含攻擊端及防禦端)，俾利符合該課程之「實作為主、理論為輔」之原則。

除了第一天介紹課程所需之基本知識外，相當著重於相關工具的實作，尤其是 Gitlab 上可以找到工具程式，透過講師授與破解概念後，甫以簡短的練習與實地操作，使參訓人員熟悉工具的操作，以提升學習成效；爰此，因為工具容易取得，故對於參訓人員而言，於回到公司後，遂能輕易完成工作上之

任務，達到「為用而訓」之目標。

反之，水能載舟、亦能覆舟。內建之微軟工具與開源程式的運用與取得之便利，亦為駭客常利用之工具之一；這門課演示許多攻擊手法，但亦可為系統管理員更為便利且縮短工作時效上的技術。另一方面，於防堵上，可由 SOC 加強監控一般使用者電腦及非正常上班時間，於組織或公司是否有使用 PowerShell 命令工具與相關破解或提權的開源工具，並由以下警訊窺知其風險：

1. 以 base64 編碼後之 powershell 語法。
2. 從外網下載 powershell 語法。
3. 將 powershell 語法加入系統排程。
4. Invoke 語法嵌入。
5. 使用非限制原則。
6. 於 Windows 下隱藏 powershell 服務之執行。

惟相關系統管理員視需求進行伺服器或 AD 之 DC 進行維運操作前，應採事先申請核准與通報，降低受駭客利用與攻擊之風險。