淺談AD資訊安全防護

蘇柏鳴 / 金融聯合徵信中心 資安部

一、Active Directory（AD）簡介[1]

Active Directory（AD）認證是一種微軟目錄服務，用於儲存使用者、使用者群組和電腦的相關資訊以進行認證與網域存取管理。Windows環境使用AD來儲存、共用和管理網路資訊與資源，可簡化管理員和終端使用者的工作，同時增強組織的安全性。管理員可以享受集中化的用戶和許可權管理，以及通過AD群組原則功能對電腦和使用者配置進行集中控制。

1. 物件（Object）

Active Directory的最小儲存單元為物件（Object），每個物件均有自己的schema屬性，可以儲存不同的資料，基本物件有以下幾種：

（1）Domain Controllers，儲存網域所屬的網域控制站（簡稱DC、域控）。

（2）Computers，儲存加入網域的電腦物件。

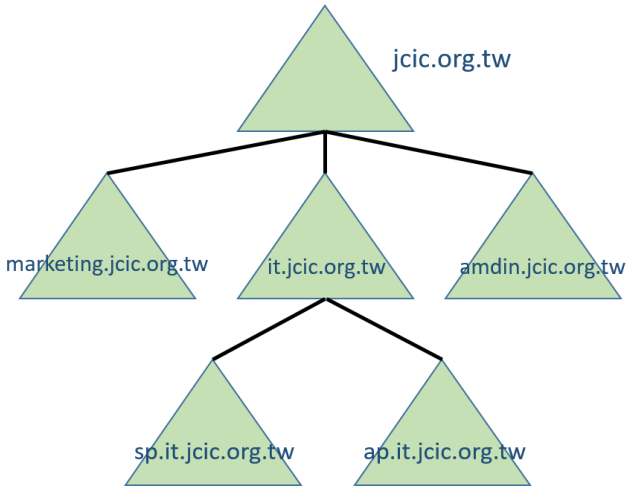
（3）Builtin，儲存內建的帳戶群組。

（4）Users，儲存AD中的使用者物件。

2. 樹系與多網域

網路環境相當龐大與複雜時，網域可能會有多個，在AD之中網域可以有一個或多個，而一個大型機構可能會利用組織架構來組織網域物件，在AD中會有數個網域情況下，若需要在網域中共享資料或是做委派管理與組態設定時，便需要建立彼此間的組織關係，微軟將AD中多網域相互的關係階層化，稱為網域樹（domain tree），網域樹結構以DNS識別方式來區分如圖1。

圖1 內含子網域的Active Directory網域樹的結構



[1] 維基百科 https://zh.m.wikipedia.org/zh-tw/Active_Directory。

3. 森林（Forest）

在多個網域的環境下，可能在不同的網域之間會需要交換與共享資料，像是組態設定、使用者帳戶與群組原則設定等，在這個時候需要有一個角色來做為不同網域間的資訊交換角色，同時又必須要符合AD樹狀結構的規範，因此微軟在多網域之間建立了一個中介用的角色，稱為森林（Forest），一個組織中最多只能有一個Forest，在Forest下則是各自的網域樹系，而在Forest下的網域或網域樹系間，可以共享資訊。

二、AD主要驗證方式

（一）NTLM

1. NTLM Hash

在說明NTLM Hash之前必須先提一下LM Hash（LAN Manager Hash），Windows最早用的加密算法，由IBM設計，但因LM Hash存在一些問題（ex.密碼長度最大只能為14個字元），目前已不再使用，為了解決LM Hash演算法和身份驗證方案中固有的安全弱點，Microsoft 於之後引入了NTLM Hash。

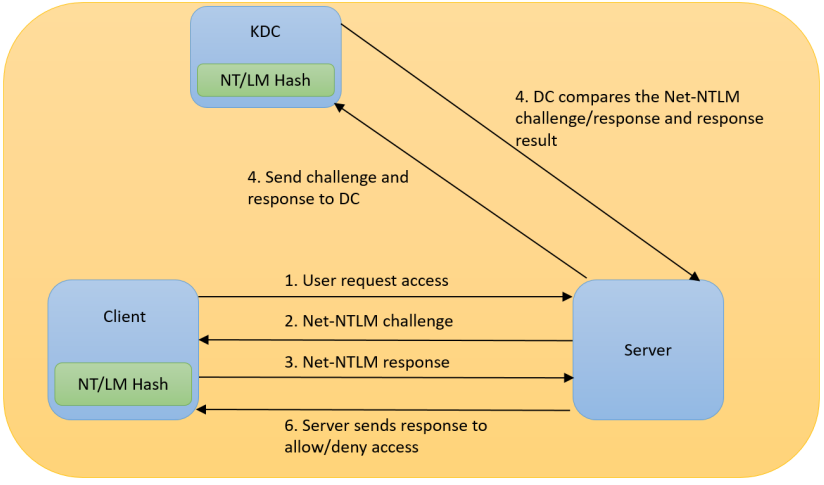
2. Net-NTLM 身分驗證

NTLM驗證是一種Challenge/Response驗證機制，驗證機制如下：

- 伺服器（Server）接受到Client發送的用戶名，判斷本地帳戶列表中是否有用戶名user_name，如果沒有就回應認證失敗，如果有此帳號，就生成Challenge，並從本地查找user_name對應之NTLM Hash，使用NTLM Hash 加密Challenge，生成一個Net-NTLM Hash 存於內存裡，並將Challenge發送給Client。
- Client接受到Challenge後，將自己提供的user_name的NTLM Hash 加密Challenge，這個結果叫Response，表現形式是Net-NTLM Hash，最後將Response發送給Server。
- Server收到Client發送的Response，將Response與之前的Net-NTLM Hash進行比較，如果相同就通過驗證。

但是Server 存放NTLM Hash 並不現實，所以就有圖2之架構。

圖2 Net-NTLM Authentication in AD



（二）Kerberos[2]

麻省理工學院研發Kerberos協定來保護雅典娜工程（Project Athena）提供的網路伺服器。這個協定以希臘神話中的人物Kerberos（或者Cerberus）命名，他在希臘神話中是Hades的一條兇猛的三頭保衛神犬，是一種電腦網路授權協定，用來在非安全網路中，對個人通信以安全的手段進行身分認證，軟體設計上採用Client/Server結構，並且能夠進行相互認證，即客戶端和伺服器端均可對對方進行身分認證。可以用於防止竊聽、防止重放攻擊、保護資料完整性等場合，是一種應用對稱金鑰體制進行金鑰管理的系統，驗證流程如圖3，相關縮寫說明如下：

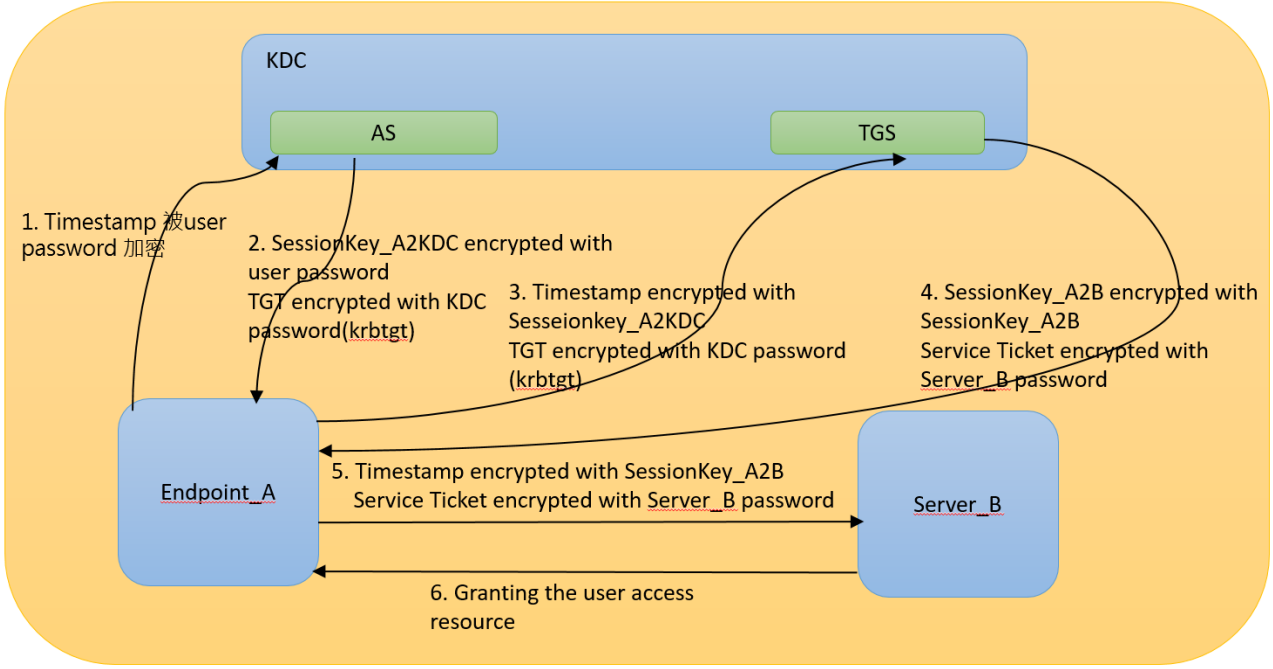
（1）AS（Authentication Server）：認證伺服器

（2）KDC（Key Distribution Center）：金鑰分發中心

（3）TGT（Ticket Granting Ticket）：票據授權票據，票據的票據

（4）TGS（Ticket Granting Server）：票據授權伺服器：

圖3 Kerberos驗證流程



2 維基百科 https://zh.wikipedia.org/zh-tw/Kerberos。

三、攻擊方式簡介

1. Pass the Hash （PtH）攻擊

攻擊者在獲得遠端主機的root權限後，為了進行橫向移動，通常會先提取各用戶的NTLM Hash，並利用 Pass the Hash 攻擊，模擬用戶登入其他主機，攻擊步驟：

（1）Admin account is Compromised，擁有一台價值較低主機的Administrator權限。

（2）Dump內存獲得該主機所有帳戶的hash（包含Administrator）。

（3）通過Pass the Hash嘗試登錄其他主機運用獲取的local administrator hash，然後重複進行PtH，在這個過程中，會得到一個local和domain user的hash列表。

（4）直到獲得域管理員帳戶hash，最終成功控制整個域。

2. Pass the Ticket

（1）Golden Ticket：必須竊取krbtgt的hash，偽造TGT去訪問任意資源。

（2）Silver Ticket：必須獲得目標服務的hash，偽造TGT去訪問任意資源。

（3）偽造Ticket的工具：Impacket、Mimikatz、Rubeus。

四、結論

AD Server 在現今資訊架構中帳號統一管控的普遍的做法，所以AD Server就成為資安攻擊的重點，近年最有名的Windows Netlogon遠端協定的漏洞「Zerologon」（編號 CVE-2020-1472），相當罕見地被通用漏洞評分系統（Common Vulnerability Scoring System，CVSS） 評為風險最高的 10 分，另外國內知名資安廠商宣稱「紅隊在時限內成功控制AD網域的比例為72%，換言之，國內每4家企業組織演練，就有約3家可被紅隊拿下AD」[3]，由此可見AD Server防護對於資安之重要性，但是經統計「竟有77%企業可從DMZ區直接存取AD」且AD 帳號權限相關設定也無法直觀判定是否會導致間接提權，所以好好檢視及驗證AD Server 權限設定是非常重要的資安課題。

3 IThome，臺資安業者揭露國內AD防護現況，盤點AD攻擊路徑與管理者帳號是當務之急，https://www.ithome.com.tw/news/151458。