CYBERARK®

Pass-the-Hash

解決方案簡介

什麼是 Pass-the-Hash？

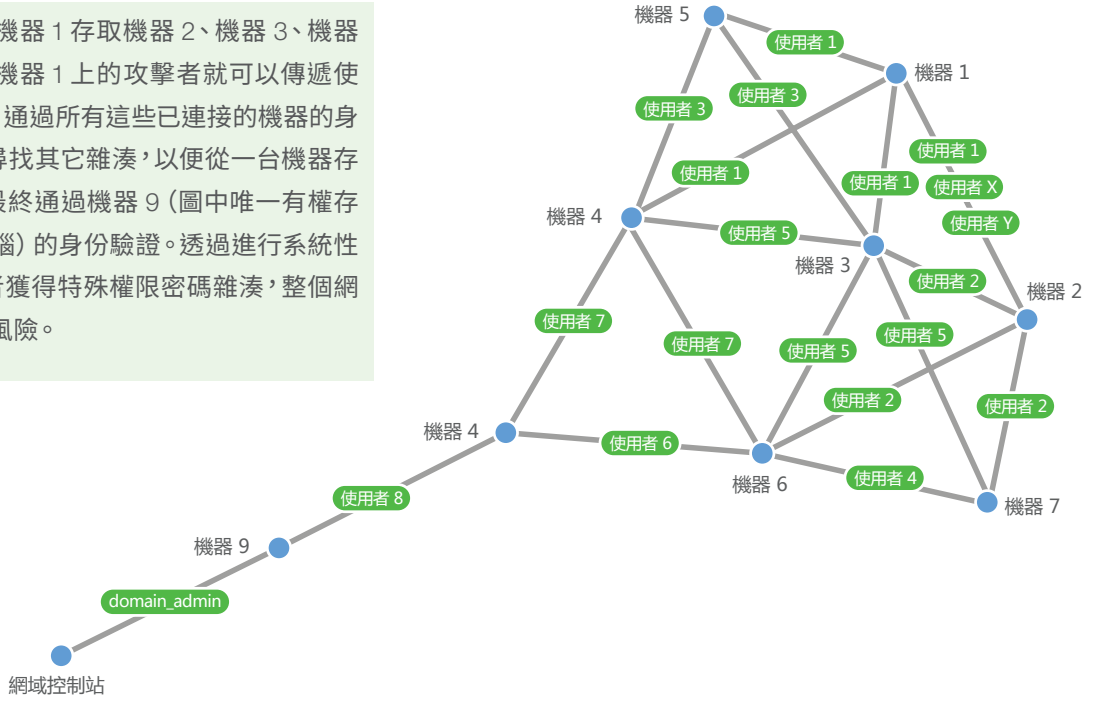
駭客潛入企業內部的工具及技術在不斷進化。但是，憑證竊取一直受到持續關注，因為利用洩露的憑證，攻擊者可以更輕鬆地存取企業最關鍵的資產，而不會被察覺。

Pass-the-Hash 是一種利用被盜憑證的攻擊技術，通常用在複雜攻擊中，並且造成企業重大風險。攻擊者可以利用這種技術從一台電腦中竊取帳號憑證，然後使用這些憑證通過網路中其它存取點的身份驗證。攻擊者可利用 Pass-the-Hash 攻擊，使用密碼雜湊而通過身份驗證，而無需純文字密碼。密碼雜湊是指原始密碼經過單向數學函數產生的值，而建立密碼雜湊是為了進行安全儲存。

由於 Pass-the-Hash 攻擊會利用受保護雜湊狀態的密碼，因此，攻擊者就可以偽裝成已通過身份驗證的使用者，而無需知道純文字密碼。此外，攻擊者還可以將竊取的雜湊憑證重複用於（傳遞給）其它系統及服務，以獲得更全面更深入的存取權限。例如，如果攻擊者獲得網域管理員已登入的電腦的存取權限，則攻擊者就可以竊取網域帳號憑證，並存取該帳號在整個網域中的所有資源、權限及特殊權限。這樣，攻擊者就可以逐步接近網域控制站。

因此，任何儲存有雜湊的機器都可能成為 Pass-the-Hash 攻擊的首要目標，以此存取企業最關鍵的敏感性資料。儲存的雜湊在整個網路的多台機器上將造成漏洞。下圖顯示如何在一台機器上實作 Pass-the-Hash 攻擊，進而輕鬆存取網域控制站。

使用者 1 可以透過機器 1 存取機器 2、機器 3、機器 4 及機器 5。因此，機器 1 上的攻擊者就可以傳遞使用者 1 的雜湊憑證，通過所有這些已連接的機器的身份驗證。攻擊者將尋找其它雜湊，以便從一台機器存取另一台機器，並最終通過機器 9（圖中唯一有權存取網域控制站的電腦）的身份驗證。透過進行系統性的攻擊，一旦攻擊者獲得特殊權限密碼雜湊，整個網路都可能因此面臨風險。



Pass-the-Hash 會使企業面臨嚴重威脅，因為如果未有效保護企業核心設備的密碼及其雜湊，攻擊者就可能透過上述攻擊存取這些設備。攻擊者可以利用這些攻擊在網路中暢行無阻且隱秘而極難被偵測。

確定 Pass-the-Hash 漏洞

要降低 Pass-the-Hash 攻擊的風險，第一步應確定易於受到這類攻擊的帳號及機器。CyberArk Discovery & Audit（CyberArk DNA ™）是容易使用的免安裝工具，可用於掃描整個網路並確定可能易於遭受 Pass-the-Hash 攻擊的機器，幫助您準確瞭解風險狀況。該工具解決以下問題：

- 哪些機器易於受到 Pass-the-Hash 攻擊？
- 如何在企業內部進行攻擊？
- 哪些帳號可能用於發起 Pass-the-Hash 攻擊，使企業面臨風險？
- 哪些機器面臨最大風險，應首先對其採取保護措施？
- 是什麼原因導致這些機器易於受到攻擊，如何降低風險？

除了 Pass-the-Hash 漏洞以外，CyberArk DNA 還可幫助瞭解特殊權限帳號安全風險的嚴重程度 - 通常是稽核失敗及遭受鎖定進階攻擊的根本原因。

阻止 Pass-the-Hash 攻擊

Pass-the-Hash 攻擊利用以下事實：Microsoft Windows 環境中的密碼雜湊未加 SALT 亂數值，因此在手動更改設定之前仍為靜態。Microsoft 已意識到這種漏洞，並發佈報告強調 Pass-the-Hash 的危險程度，同時詳細說明「Microsoft 為什麼不發佈更新以解決此問題？」

攻擊者必須突破邊界，然後取得密碼雜湊，才能進行 Pass-the-Hash 攻擊。 可以採用各種不同方法取得雜湊，包括由任何具有管理者級別特殊權限的人員從安全帳號管理器 (SAM) 轉存雜湊 / 憑證，轉存儲存在 lsass.exe 處理程序之記憶體中的憑證，以及偵聽用戶端與伺服器之間的 LM 及 NTLM 質詢 - 回應對話。

為了降低 Pass-the-Hash 攻擊的風險，企業應實施深度防禦策略。Microsoft 在報告中就如何防範 Pass-the-Hash 攻擊提出兩條主要建議：「限制並保護具有較高特殊權限的網域帳號」以及「限制並保護具有管理特殊權限的本機帳號」。根據這些建議，CyberArk 提供一整套特權帳號安全解決方案來防範 Pass-the-Hash 攻擊。

降低 Pass-the-Hash 風險的最佳實踐

控制並管理核心設備的密碼：CyberArk Enterprise Password Vault® 可為每個特權使用者及服務帳號建立唯一的密碼，並僅允許授權使用者進行存取，幫助降低攻擊風險。這降低未授權使用者或攻擊者存取特權帳號雜湊及使用者密碼的機率。即使攻擊者確實能夠存取雜湊，也不會造成太大風險，因為每個特權帳號雜湊都是唯一的。

經常更改密碼：應儘可能頻繁地更換特權帳號密碼，縮短攻擊者利用雜湊進行攻擊的可用時間。例如，使用 CyberArk 企業密碼金庫可以根據企業政策定期自動更改密碼。CyberArk 特權帳號安全解決方案還可以強制針對執行關鍵任務的特權帳號設定「一次性密碼」規則。

1 《防範 Pass-the-Hash (PtH) 及其它憑證盜竊攻擊》：http://www.Microsoft.com/en-us/download/details.aspx?id=36036

取消本機管理員特殊權限：CyberArk 終端特權管理器可協助企業取消本機帳號的管理權限，並執行最小權限原則。透過取消本機帳號的管理權限，即使攻擊者攻破本機帳號，企業也可以提供幫助，防止攻擊者獲得所需特殊權限來取得雜湊並進行 Pass-the-Hash 攻擊。

確保特權連線安全：CyberArk Privileged Session Manager® 將作為管理者與目標機器之間的代理器 (proxy)，可用於保護特權帳號憑證，確保不會將特權帳號憑證洩露給可能易於受到攻擊的中端。CyberArk 特權限連線管理器會防止在終端上披露特權憑證，進而降低在憑證竊取攻擊中使用憑證進行 Pass-the-Hash 的風險。

快速偵測威脅：CyberArk Privileged Threat Analytics ™會分析 Kerberos 流量以偵測進行中的攻擊。透過對特權帳號活動及關鍵性的攻擊向量進行針對性的威脅偵測，企業就可以警惕潛在的攻擊 (如憑證竊取攻擊)，並在威脅造成嚴重破壞之前迅速做出回應。

確定並阻止嘗試竊取憑證的可疑行為：CyberArk 終端特權管理器會控制終端上的特殊權限並遏制攻擊。此解決方案會判定未知應用程式，並在受限模式下運行這些程式，限制潛在的損害。此外，該解決方案還會透過行為分析來阻止嘗試竊取憑證的行為 (如 Pass-the-Hash)。這些至關重要的保護技術可協助企業強化現有終端的安全性。

總結

Pass-the-Hash 是日漸常見的網路攻擊技術，因此日益受到企業關注。瞭解並確定威脅是降低 Pass-the-Hash 攻擊風險的第一步。CyberArk 的系列解決方案可協助企業確定易於受到 Pass-the-Hash 攻擊的機器，並運用特權帳號安全解決方案降低這些攻擊的風險。

案例分析：

利用 CyberArk 終端特權管理器偵測 Pass-the-Hash 並降低風險

實作 CyberArk 終端特權管理器之前

企業缺乏成熟的安全實踐。所有員工均可以存取他們工作站上的本機管理者帳號，為了方便，員工會頻繁使用這些帳號。在這種情況下，攻擊者可以透過網路釣魚輕鬆獲得工作站的存取權限，然後透過被攻破的端點從 SAM 資料庫中取得網域管理者密碼雜湊，因為網域管理者雜湊具有大量特殊權限。

實作 CyberArk 終端特權管理器之後

企業實施 CyberArk 終端特權管理器，攻擊者幾乎不可能從企業中端中成功取得雜湊，因為攻擊者無法獲得必要的特殊權限。透過取消本機管理者權限，企業可減少整體受攻擊面，並降低 Pass-the-Hash 攻擊風險。除主動防範攻擊以外，中墩特權管理器還會偵測並阻止嘗試竊取憑證的行為，幫助企業阻止攻擊者進行 Pass-the-Hash 攻擊並防止其獲得未授權存取權限。