CYBERARK®

傳遞雜湊(Pass-the-Hash)

解決方案概述

何謂傳遞雜湊(Pass-the-Hash)?

駭客用來滲透組織的工具和技術始終不斷地進化，而駭客竊取憑證一直是受到關切的問題點所在，因為受損的憑證會使駭客更容易存取組織最關鍵的資產，且不會被查覺到。

傳遞雜湊是一種利用竊取而來的憑證所施行的攻擊技術，常被用於進階的攻擊並對組織造成重大的風險。此一技術牽涉到攻擊者從某台電腦中竊取到帳號憑證，並利用它對網路中其它的存取點進行認證。傳遞雜湊的攻擊無需純文字密碼，而可讓攻擊者使用密碼散列作認證。此密碼散列值是在針對安全儲存體建立密碼散列時，原始密碼經過單向的數學函數演算後所產生的。

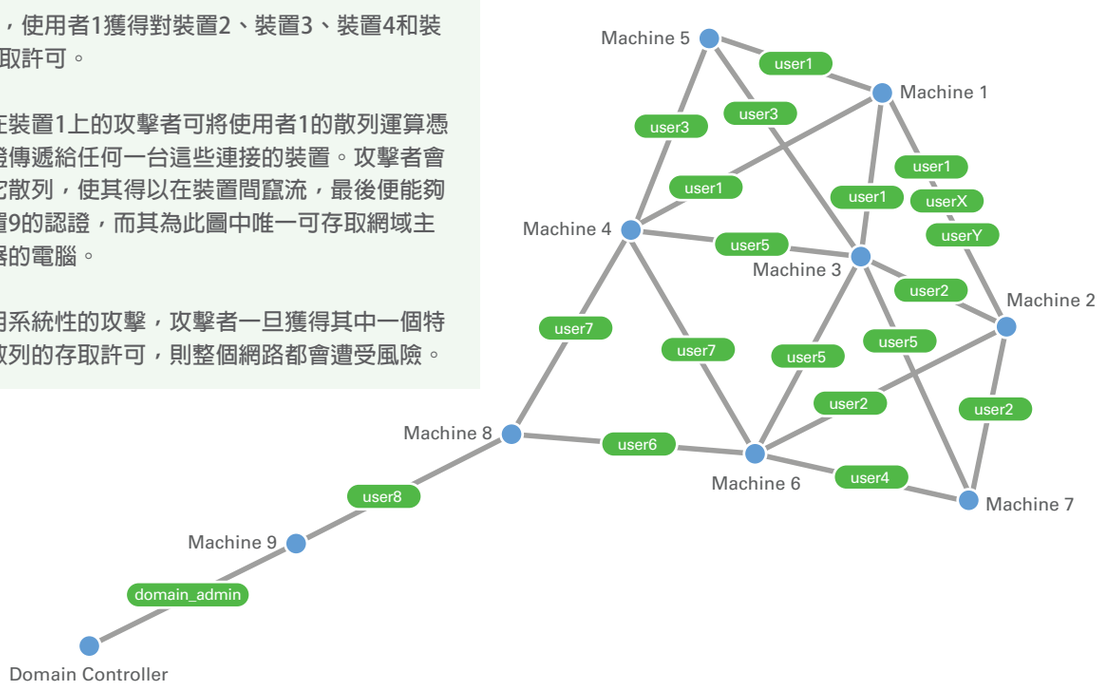
因為傳遞雜湊攻擊利用的是受保護之散列形態中的密碼，故它讓攻擊者可以在完全不知道純文字密碼的情形中能模仿經認證的使用者。攻擊者亦可在其它系統和服務中重複使用(傳遞)這些被竊取並經過散列演算的憑證，以獲取更多深入的存取許可。例如，若攻擊者獲得了一個網域管理者已登入過之裝置的存取權，就可經由這網域竊取網域帳號憑證，並透過該網域存取該帳號所有的相關資源、權限和特權。透過此一途徑，攻擊者便可一步步接近網域主控站。

因此，任何儲存散列的機器皆可能構成傳遞雜湊攻擊的第一步，使駭客得以獲得組織最關鍵和敏感的數據資料。被儲存下來的散列會使得整個網域中的複數個裝置都有安全上的漏洞。下圖顯示出了傳遞雜湊攻擊可在其中一台裝置上啟動，並可輕易地對網域主控站作存取動作。

從裝置1，使用者1獲得對裝置2、裝置3、裝置4和裝置5的存取許可。

因此，在裝置1上的攻擊者可將使用者1的散列運算憑證和認證傳遞給任何一台這些連接的裝置。攻擊者會尋找其它散列，使其得以在裝置間竄流，最後便能夠通過裝置9的認證，而其為此圖中唯一可存取網域主控伺服器的電腦。

藉由使用系統性的攻擊，攻擊者一旦獲得其中一個特權密碼散列的存取許可，則整個網路都會遭受風險。



傳遞雜湊會對組織產生重大威脅，因為若密碼和其散列未能被妥善管理時，此攻擊便可造成針對組織核心不當的存取。這些攻擊讓攻擊者得以操縱網路運作卻不會被查覺到，進而使得它們很難被偵測到。

找出傳遞雜湊的弱點

減緩傳遞雜湊攻擊風險的第一步是找出容易受到這些攻擊的帳號和裝置。CyberArk的Discovery & Audit (CyberArkDNA™)是一個獨立運作且容易使用的工具，可掃描整個網路並辨識出可能易受傳遞雜湊攻擊的裝置，以便獲得精確的整體圖像。此工具能處理下列的問題：

- 哪些裝置易遭受傳遞雜湊攻擊?
- 這樣的攻擊如何在組織內部執行?
- 那些帳號可以啟動傳遞雜湊攻擊並讓組織面臨風險?
- 哪些裝置最具風險且應該先被處理以減緩風險?
- 是甚麼讓機器易遭受攻擊，以及要如何降低風險?

除了易受傳遞雜湊攻擊的安全弱點外，CyberArk DNA亦會顯示出特權帳號安全風險的程度，這些特權帳號經常是審查失敗和進階針對性攻擊的根本原因。

減緩傳遞雜湊攻擊

密碼散列在微軟Windows作業系統中並未被特別防護處理，因而一直是固定不變的直到密碼被手動更改為止。傳遞雜湊攻擊就是利用這個特性。微軟已承認此一弱點並發佈一份報告，其中強調了傳遞雜湊的危險性，並詳細說明"為何微軟無法藉由更新版本來處理此問題？"

為了要執行傳遞雜湊攻擊，攻擊者必須先衝破周邊防線然後才能獲取密碼散列。散列之獲取可經由許多不同的方法實現，包括由任何具有管理者層級特權的使用者從安全帳號管理員(SAM)伺服器轉儲散列/憑證、轉儲存放在lsass.exe程序記憶體中的憑證、以及搜尋終端和伺服器之間的LM和NTLM的挑戰-應答對話。

要減緩傳遞雜湊攻擊的風險，組織應實施深度防禦的策略。微軟的報告提出了兩項主要的建議以供減緩傳遞雜湊攻擊："限制並保護高特權網域帳號"和"限制並保護具有管理者特權的本機帳號"。CyberArk的解決方案符合這些建議，提供具整合性的特權帳號安全解決方案以防止遭受傳遞雜湊攻擊。

減緩傳遞雜湊攻擊的最佳做法

控制並管理「通往您企業的鑰匙」

CyberArk Enterprise Password Vault 可針對每一個特權使用者和服務帳號建立獨特的密碼，並限制只有經授權的使用者可以對其進行存取，以降低風險。這可降低未經授權的使用者或攻擊者獲得存取特權帳戶散列和使用者密碼的機會。即使攻擊者真的得以對某個散列進行存取，所造成的傷害也會比較小，因為每一個特權帳號都有自己獨一無二的散列。

經常變更密碼

特權密碼應該盡可能地經常輪動變更以降低散列被利用的機會。例如，使用CyberArk Enterprise Password Vault，其可依據企業政策自動定期變更密碼。CyberArk的特權帳號安全解決方案也可針對關鍵任務的特權帳號強制執行"一次性密碼"的做法。

1 "Mitigating Pass-the-Hash (PtH) and Other Credential Theft Techniques", http://www.microsoft.com/en-us/download/details.aspx?id=36036

移除本機管理者特權
CyberArk Viewfinity可讓組織移除本機帳號的管理者權限，並強制執行最少特權政策。當本機帳號的管理者權限被移除後，即使攻擊者侵入了這個本機帳號，組織仍可防止攻擊者獲得所需的特權以獲取散列，並防止其執行傳遞雜湊攻擊。

防護特權運作
CyberArk Privileged Session Manager 在管理者和目標裝置之間執行代理伺服器的動作，保護特權帳號憑證並確保這些憑證不會洩漏給易受攻擊的端點。CyberArk Privileged Session Manager防止特權憑證暴露於端點，因此可降低它們被竊取用來進行傳遞雜湊攻擊的風險。

快速偵測威脅
CyberArk Privileged Threat Analytics™會分析Kerberos授權協議的流量以偵測進行中的攻擊。當具備了針對特權帳戶活動和關鍵性攻擊向量的威脅偵測能力，組織會收到有可能被入侵的警訊，例如像是憑證竊取攻擊，並得以在重大損害發生之前採取快速的回應。

總結

傳遞雜湊是一種愈來愈普遍的網路攻擊技術，因此也是各組織愈來愈關切的問題。了解並辨識出威脅是減緩傳遞雜湊攻擊的第一步。CyberArk的系列解決方案能幫助組織找出易遭受傳遞雜湊攻擊的裝置，並以Privileged Account Security進一步減緩這些攻擊的風險。

個案研究：

使用CyberArk Viewfinity來減緩遭受傳遞雜湊攻擊的風險

使用之前

組織缺乏成熟的安全措施。所有的員工都可以在其工作站上對本機管理員帳號進行存取，而且為了方便使用，他們經常使用這些管理員帳號。
在這樣的情況下，攻擊者可以很容易經由網路釣魚獲得對其中一個工作站的存取，然後經由此一端點從SAM資料庫獲取網域管理者的散列，因為這些帳號有過多的使用者特權。

使用之後

組織運用CyberArk Viewfinity並成功排除了攻擊者從組織端點獲取散列的可能性，因為攻擊者無法獲得所需的特權。
經由移除本機管理者權限，組織減緩了遭受傳遞雜湊的風險，並大幅減少了整體的受攻擊面。