01_外部專案 - 專案資訊 #1077

專案資訊 # 1064 (New-新增): 2025-PenTest

Krbtgt Password Unchanged for over 1 year

2025-11-10 13:31 - Joy Liao

狀態:	Resolved-解決	**開始日期:**	2025-08-01
優先權:	Normal	**完成日期:**	2025-12-31
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	0:00 小時
版本:		**耗用工時:**	0:00 小時

概述

N bookmark202505262315047796538150 04 "Krbtgt Password Unchanged for over 1 year

" A stale krbtgt password enables Golden Ticket attacks, letting attackers forge Kerberos tickets to impersonate any user, including admins, and maintain persistent, undetected domain access. The longer it goes unchanged, the greater the risk of widespread compromise. "To renew the Kerberos keys used to encrypt TGTs, it is necessary to manually change the krbtgt account password annually . It is recommended to perform this change using the script provided by Microsoft .

The password change must be performed twice to be effective.

It is noteworthy that any operation to change the password of the krbtgt account must be performed only in an Active Directory environment where replication between domain controllers is nominal. Therefore, it is essential to wait a period before the second password change.

It is also possible to manually reset the krbtgt account password , in the same way as for a regular account. If the provided script is not used, it is recommended to leave at least 24 hours between the two changes and to ensure effective replication between domain controllers. A strategy could be to perform a single password change every 6 months, in order to guarantee an effective annual change.

"

歷史

#1 - 2025-11-10 13:34 - Joy Liao

- 完成日期 設定為 2025-12-31

- 被分派者 設定為 益利 周

- 開始日期 從 2025-11-10 變更為 2025-08-01

#2 - 2025-11-27 17:55 - 益利 周

- 檔案 clipboard-202511271755-pgocl.png 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

Krbtgt 帳號 已進行多次密碼變更 最後一次變更是在 2025/11/24 下午 08:01:04

```
PS C:\Windows\system32> Get-ADUser -Identity "krbtgt" -Properties whenChanged | Select-Object Name, whenChanged

Name                                                  whenChanged
----                                                  -----------
krbtgt                                                2025/11/24 下午 08:01:04
```

檔案

clipboard-202511271755-pgocl.png	12 KB	2025-11-27	益利 周