01_外部專案 - 專案資訊 #1066

專案資訊 # 1064 (New-新增): 2025-PenTest

Domain Admin Vulnerable to Kerberoasting Attack

2025-11-10 13:28 - 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

NN "4.3.2

MITRE-T1558

" "Domain Admin Vulnerable to Kerberoasting Attack

It is possible to obtain the encrypted Kerberos service ticket of a domain admin for offline password cracking.

" "The exposure of encrypted service ticket empowers adversary to reveal the exact password to perform user impersonation or privilege escalation in this case.

It is noteworthy that the affected domain admin has never expiring password and has its password remain unchanged more than 2 years. This allows adversary ample time to perform offline cracking of its password.

" "Avoid assigning SPNs to Domain Admin accounts unless absolutely necessary.

Set long and complex passwords for service accounts and limit privileges of service accounts. If possible, use AES encryption instead of RC4 encryption."

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 13:49 - 益利 周

- 檔案 clipboard-202511271337-vwsq1.png 已新增

- 檔案 clipboard-202511271343-ve3dx.png 已新增

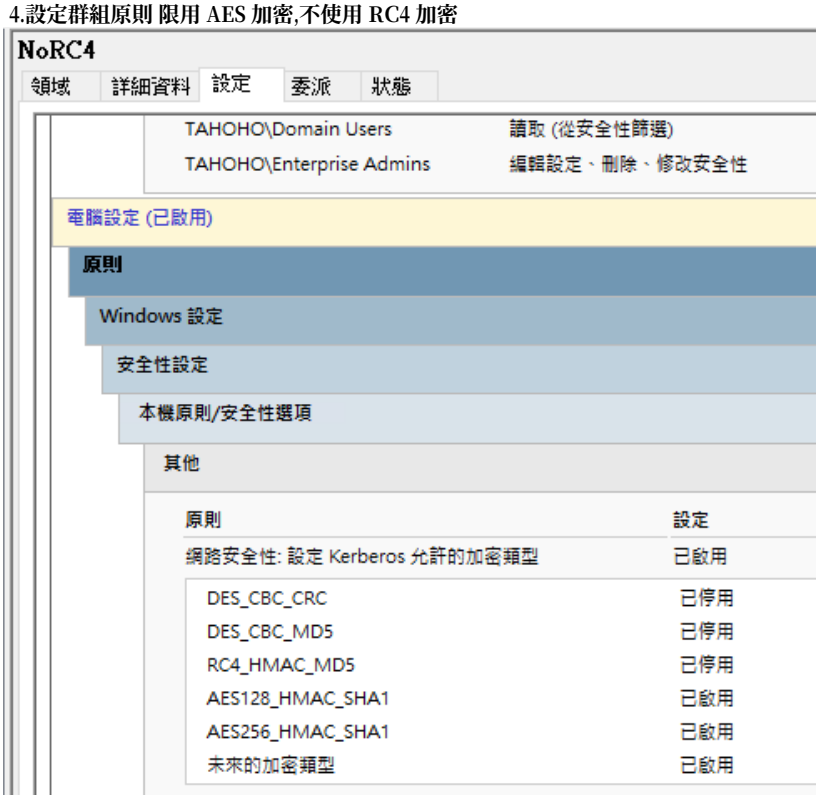
- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

1.新增 一般使用者 Domain User 授予 SPN
2.移除 Domain Admin 網域管理員帳戶的 SPN

```
PS C:\Windows\system32> Get-ADUser -Identity "OnyxSPN" -Properties ServicePrincipalNames


DistinguishedName     : CN=OnyxSPN,OU=Service,DC=tahoho,DC=com,DC=tw
Enabled               : True
GivenName             : SPN
Name                  : OnyxSPN
ObjectClass           : user
ObjectGUID            : 10e9616c-71ce-49c3-93f4-0abe9d1af9d8
SamAccountName        : OnyxSPN
ServicePrincipalNames : {HOST/OnyxSPN, HOST/OnyxSPN.tahoho.com.tw}
SID                   : S-1-5-21-845223939-707100287-312552118-20373
Surname               : Onyx
UserPrincipalName     : OnyxSPN@tahoho.com.tw



PS C:\Windows\system32>
PS C:\Windows\system32> Get-ADUser -Identity 'tahotbhq.admin' -Properties ServicePrincipalNames
>> Import-Module ActiveDirectory


DistinguishedName     : CN=admin TahoAD,CN=Users,DC=tahoho,DC=com,DC=tw
Enabled               : True
GivenName             :
Name                  : admin TahoAD
ObjectClass           : user
ObjectGUID            : 3e80a000-55bd-4a9d-afb3-a90036d47359
SamAccountName        : tahotbhq.admin
ServicePrincipalNames : {MSSQLSvc/TAHOERP.tahoho.com.tw, MSSQLSvc/TAHOERP.tahoho.com.tw:1433, MSSQLSvc/TAHOERP, MSSQLSv
                        c/TAHOERP:1433}
SID                   : S-1-5-21-845223939-707100287-312552118-500
Surname               :
UserPrincipalName     : tahotbhq.admin@tahoho.com.tw
```

3.變更 網域管理員帳戶 密碼
4.設定群組原則 限用 AES 加密,不使用 RC4 加密



檔案

clipboard-202511271337-vwsq1.png	29.1 KB	2025-11-27	益利 周
clipboard-202511271343-ve3dx.png	27.2 KB	2025-11-27	益利 周