INFORME DE AUDITORÍA DE SEGURIDAD

Daniel Miranda Barcelona

Versión demostrativa para portfolio (sin datos sensibles reales)

Fecha: 24/09/2025
Proyecto: AD-001
Versión 1.0

Declaración de Confidencialidad 4
Descargo de Responsabilidad 4
Información de Contacto 4
Resumen de la Evaluación 5
Fases de la auditoría 5
Pruebas de penetración interna 6
Procesado, cracking parcial y reutilización de hashes 6
Pass-the-Hash y movimiento lateral 6
Enumeración de Active Directory y recopilación de información 7
Post-explotación: acceso al DC y volcado de NTDS 7
Artefactos y trazabilidad (referencia interna — evidencias incluidas en este documento) 7
Resumen de hallazgos técnicos críticos (síntesis) 8
Clasificación de Severidades y Factores de Riesgo 9
Niveles de Severidad 9
Factores de Riesgo 9
Probabilidad 9
Impacto 10
Alcance de la Evaluación 10
Detalles de la Evaluación 10
Exclusiones del Alcance 10
Permisos del Cliente 11
Resumen ejecutivo 12
Alcance y Limitaciones de Tiempo 12
Resumen de Pruebas 12
Notas y recomendaciones del auditor 13
Fortalezas y Debilidades Clave 14
Fortalezas 14
Debilidades 14

Copyright© **DMB SECURITY LABS**

Resumen de vulnerabilidades 15

Boletín de calificaciones 18

Resultados técnicos 21

IPT-001 – MS08-067: Ejecución Remota de Código en el Servicio de Servidor de Windows 21

IPT-002 – MS17-010: Ejecución Remota de Código en el Servicio de Servidor de Windows 23

IPT-003 – SMB-SIGNING-DISABLED: Firma SMB deshabilitada — Susceptible a NTLM Relay 26

IPT-004 – RDP-NLA-DISABLED: RDP sin Network Level Authentication 28

IPT-005 – LLMNR/NBT-NS Poisoning: Captura de Credenciales NTLMv1/v2 30

IPT-006 – PASSWORD-POLICY-WEAK: Política de contraseñas con longitud mínima insuficiente y bloqueo de cuentas deshabilitad 34

IPT-008 – SMB-SHARE-LISTING-ONLY: Share visible pero requiere autenticación. 36

IPT-009 – USER-ENUM: Enumeración de usuarios válida vía Kerberos/SMB 39

IPT-010 – ASREP-ROASTABLE: Cuenta susceptible a AS-REP Roasting detectada 41

IPT-011 – KERBEROAST: Contraseña de cuenta de servicio recuperada por Kerberoast 43

IPT-012 – NTDS-DUMP: Volcado de NTDS y extracción de hashes 45

IPT-013 – GOLDEN TICKET: Emisión forjada de TGT Kerberos usando el hash de KRBTGT 47

Copyright© **DMB SECURITY LABS**

Declaración de Confidencialidad

Este documento es propiedad exclusiva de **DMB Security Labs** y de la organización evaluada. Contiene información confidencial y de carácter reservado.

Queda estrictamente prohibida su reproducción, distribución o uso, total o parcial, en cualquier formato, sin el consentimiento previo por escrito de ambas partes.

La organización evaluada podrá compartir este documento con auditores o autoridades bajo acuerdos de confidencialidad, con el fin de acreditar el cumplimiento de requisitos relacionados con pruebas de seguridad o auditorías técnicas.

Descargo de Responsabilidad

Esta auditoría de seguridad representa una **fotografía en un momento determinado**. Los hallazgos y recomendaciones aquí descritos se basan en la información recopilada durante el período de evaluación, y no contemplan cambios o modificaciones posteriores a esa fecha.

Debido a las limitaciones de tiempo inherentes a este tipo de análisis, no se ha realizado una evaluación completa de todos los controles de seguridad.

El enfoque del trabajo se centró en identificar **los controles más débiles** y vectores de ataque más probables desde la perspectiva de un atacante real.

Se recomienda realizar auditorías de seguridad periódicas (al menos una vez al año), llevadas a cabo por personal interno o por terceros cualificados, con el fin de validar la eficacia continua de los controles implementados.

Información de Contacto

Nombre	Cargo	Contacto
Daniel Miranda	Auditor de seguridad	Dmirandab@dmbsec.com

Copyright© **DMB SECURITY LABS**

Resumen de la Evaluación

Entre el 2**0 de septiembre y el 26 de septiembre de 2025**, la organización solicitó a **DMB Security Labs** la realización de una **auditoría de seguridad interna**, con el objetivo de evaluar el estado de su infraestructura frente a buenas prácticas del sector y amenazas reales, mediante la ejecución de una prueba de penetración con enfoque ofensivo.

La evaluación se realizó siguiendo el marco metodológico **PTES (Penetration Testing Execution Standard)**.

Todas las vulnerabilidades identificadas han sido clasificadas utilizando la escala de puntuación **CVSS (Common Vulnerability Scoring System)**.

Fases de la auditoría

El proceso de auditoría se llevó a cabo siguiendo las siguientes fases:

- **Planificación:**
  Se definieron los objetivos del cliente y se establecieron las reglas de compromiso para la evaluación.
- **Descubrimiento:**
  Se realizó un reconocimiento activo y pasivo, incluyendo escaneo de red, enumeración de servicios y recopilación de información para detectar debilidades y vectores de ataque.
- **Explotación:**
  Se procedió a confirmar vulnerabilidades mediante técnicas de explotación controlada, con el objetivo de validar el impacto real y obtener acceso a los sistemas.
- **Post-explotación:**
  Se realizaron movimientos laterales, escaladas de privilegios, extracción de credenciales y análisis del entorno comprometido para evaluar el alcance de los vectores de ataque.
- **Reporte:**
  Se documentaron todas las vulnerabilidades confirmadas, técnicas utilizadas, intentos fallidos, así como los puntos fuertes y débiles de la organización en cuanto a seguridad.

Copyright© **DMB SECURITY LABS**

Pruebas de penetración interna

Durante esta fase, se llevaron a cabo diversas técnicas ofensivas con el objetivo de evaluar el impacto real de una intrusión interna. Las acciones realizadas incluyeron:

Envenenamiento LLMNR / NBT-NS (MITM) — Intercepción de credenciales

- **Descripción:** Fueron forzadas resoluciones de nombre en la red para provocar respuestas hacia un actor atacante y capturar respuestas de autenticación.
- **Herramienta / técnica empleada:** Responder (captura de peticiones y hashes NTLM).
- **Resultado:** Captura de múltiples hashes NTLMv1/v2 pertenecientes a usuarios estándar y a cuentas con privilegios administrativos.
- **Evidencia en el informe:** capturas y salidas de Responder incluidas en la bitácora.

Procesado, cracking parcial y reutilización de hashes

- **Descripción:** Los hashes capturados se formatearon y analizaron; donde fue relevante, se intentó cracking offline; otros hashes se reutilizaron en autenticaciones remotas (PtH).
- **Herramientas empleadas:** John / Hashcat (cracking); impacket-wmiexec, impacket-psexec, netexec para autenticación remota con hashes.
- **Resultado:** Algunos hashes fueron crackeados parcialmente; se realizaron autenticaciones exitosas empleando hashes; demostración práctica de acceso con credenciales extraídas.
- **Evidencia en el informe:** resultados de cracking y capturas de sesiones remotas documentadas en la bitácora.

Pass-the-Hash y movimiento lateral

- **Descripción:** Reutilización de hashes para autenticarse en hosts remotos y escalar/transferir accesos dentro del dominio.
- **Hosts impactados (ejemplos del laboratorio):** PC-ISIDRO, PC-DAVID, SERVIDOR-AD (Controlador de Dominio).
- **Herramientas empleadas:** impacket-wmiexec, impacket-psexec, smbexec / netexec.

Copyright© **DMB SECURITY LABS**

- **Resultado:** Accesos administrativos remotos confirmados en varias máquinas; ejecución de comandos remotos y obtención de shells.
- **Evidencia en el informe:** capturas de consola y registros de sesiones en el anexo.

Enumeración de Active Directory y recopilación de información

- **Descripción:** Enumeración profunda de usuarios, búsqueda de SPNs y detección de cuentas con Kerberos pre-auth deshabilitado (AS-REP), además de extracción de GPOs relevantes.
- **Herramientas empleadas:** kerbrute, impacket-GetNPUsers, impacket-GetUserSPNs, PowerView (Get-AD*), nmap (scripts: rdp-ntlm-info, smb2-security-mode, etc.).
- **Resultado:** Listados de usuarios válidos, SPNs identificados (ej.: sql_svc), cuentas AS-REP roasterables y GPOs con configuraciones inconsistentes (firmas LDAP/SMB no forzadas).
- **Evidencia en el informe:** salidas de comandos y capturas incluidas en la sección de bitácora y anexos.

Post-explotación: acceso al DC y volcado de NTDS

- **Descripción:** Tras obtener credenciales administrativas se procedió a obtener un volcado del Active Directory (NTDS) y a extraer hashes de cuentas críticas.
- **Herramientas empleadas:** netexec --ntds, impacket-secretsdump, mimikatz (lsadump::dcsync) y utilidades de volcado sobre snapshot cuando fue necesario.
- **Resultado:** Volcado del NTDS con extracción de múltiples hashes, incluido el hash de krbtgt; confirmación de RIDs y cuentas extraídas.
- **Evidencia en el informe:** fichero de volcado y salidas de mimikatz documentadas en la bitácora del presente informe.

Artefactos y trazabilidad (referencia interna — evidencias incluidas en este documento)

- Capturas y logs de Responder (hashes originales y timestamps).
- Resultados de cracking (John/Hashcat) y su porcentaje de éxito (archivos de salida/potfiles).
- Registros de sesiones remotas (wmiexec, psexec, netexec) con comandos ejecutados y capturas de pantalla.

Copyright© **DMB SECURITY LABS**

- Exportaciones de GetUserSPNs, GetNPUsers, Get-GPOReport -All (XML) y salidas de nmap.
- Volcado NTDS y salidas de mimikatz (lsadump::dcsync) con detalle de cuentas extraídas (incluido krbtgt).

Nota: todas las capturas, salidas y artefactos mencionados están integrados en la bitácora y los anexos de este informe; no se requieren ficheros externos adicionales.

Resumen de hallazgos técnicos críticos (síntesis)

- Envenenamiento LLMNR/NBT-NS → hashes NTLMv1/v2 capturados.
- Cracking y/o reutilización de hashes → autenticaciones remotas (PtH) y movimiento lateral.
- Compromiso de host(s) y del DC → volcado NTDS y extracción del hash krbtgt.
- SPNs explotables (Kerberoast) y cuentas AS-REP roasterables → credenciales de servicio recuperadas (ej.: sql_svc).
- GPOs y configuración de firma/cifrado inconsistentes → riesgo real de relay y suplantación.

Copyright© **DMB SECURITY LABS**

Clasificación de Severidades y Factores de Riesgo

Niveles de Severidad

La siguiente tabla define los niveles de severidad utilizados a lo largo del informe, basados en el sistema de puntuación **CVSS v3.1**, con el fin de evaluar el impacto y el riesgo asociado a cada vulnerabilidad identificada:

Severidad	Rango CVSS	Descripción
Crítica	9.0 - 10.0	La explotación es directa y generalmente permite el compromiso total del sistema. Se recomienda aplicar medidas inmediatas.
Alta	7.0 – 8.9	La explotación es más compleja, pero puede derivar en elevación de privilegios, pérdida de datos o interrupciones. Se recomienda aplicar correcciones lo antes posible.
Media	4.0 - 6.9	Vulnerabilidades que requieren múltiples pasos, ingeniería social o condiciones específicas. Deben corregirse tras resolver las vulnerabilidades más graves.
Baja	0.1 – 3.9	No son explotables directamente, pero reducen la superficie de ataque. Pueden corregirse en ventanas de mantenimiento programadas.
Informativa	N/A	No se considera una vulnerabilidad. Se proporciona información útil, controles bien implementados o detalles adicionales detectados durante la evaluación.

Factores de Riesgo

El **riesgo** de una vulnerabilidad se evalúa en función de dos dimensiones:

Probabilidad

Evalúa la posibilidad de que una vulnerabilidad sea explotada en el entorno analizado. Depende de:

- Complejidad del ataque
- Existencia de herramientas públicas

Copyright© **DMB SECURITY LABS**

- Nivel técnico requerido por el atacante
- Configuración y exposición real del sistema objetivo

Impacto

Mide las consecuencias que tendría la explotación sobre la organización, incluyendo:

- Compromiso de la **confidencialidad, integridad o disponibilidad**
- **Pérdida de datos**
- **Impacto reputacional**
- **Consecuencias legales o financiera**

Alcance de la Evaluación

Detalles de la Evaluación

Se realizó una **prueba de penetración interna** sobre el rango de red **192.168.152.XXX/24**, con el objetivo de identificar vulnerabilidades y debilidades explotables dentro del entorno corporativo.

La evaluación se llevó a cabo desde una ubicación interna simulada, con acceso directo a la red local mediante una máquina de auditoría autorizada conectada al entorno y configuraciones específicas de red habilitadas.

Exclusiones del Alcance

A solicitud expresa del cliente, **DMB Security Labs** no ejecutó los siguientes tipos de ataques durante la auditoría:

- Ataques de **Denegación de Servicio (DoS)**
- Técnicas de **Ingeniería Social o Phishing**

Todos los demás vectores ofensivos no especificados en esta lista fueron permitidos y considerados dentro del alcance aprobado.

Copyright© **DMB SECURITY LABS**

Permisos del Cliente

El cliente proporcionó las siguientes condiciones para la realización de la prueba:

- Acceso interno a la red a través de una máquina conectada
- Acceso a puertos necesarios para el escaneo, enumeración y explotación controlada.

Copyright© **DMB SECURITY LABS**

Resumen ejecutivo

Durante la evaluación de seguridad del dominio **tssciber.local** se identificaron múltiples debilidades críticas que facilitan la obtención y reutilización de credenciales, la escalada de privilegios y el compromiso del Active Directory. Las pruebas permitieron: enumerar usuarios válidos, capturar hashes NTLM vía LLMNR/NBT-NS, explotar cuentas susceptibles a AS-REP y Kerberoast, y obtener un volcado del NTDS que contenía hashes de cuentas privilegiadas (incluido krbtgt). Estas condiciones posibilitan la emisión de tickets Kerberos forjados y el control persistente del dominio si no se remedia. Se recomiendan intervenciones urgentes (aislamiento, rotación de krbtgt, restauración/recuperación del DC, rotación de credenciales privilegiadas y detección continua).

Alcance y Limitaciones de Tiempo

Prueba de penetración interna realizada sobre la red asociada al dominio tssciber.local. La evaluación se centró en vectores AD críticos: Kerberos, LDAP/LDAPS, SMB, GPO y comparticiones. Hosts relevantes y hallazgos están documentados en la bitácora y el cuerpo del informe.

El trabajo se realizó dentro del periodo planificado y con tiempo limitado para cobertura exhaustiva de todas las máquinas del rango. Algunas acciones destructivas o que implican cambio permanente en el entorno productivo (por ejemplo, rotación real de krbtgt, ejecución de Golden Tickets en entornos vivos o inyección DCShadow en producción) no se llevaron a cabo; cuando fue necesario, las pruebas sensibles se ejecutaron únicamente en snapshots o entornos controlados.

Resumen de Pruebas

- **Reconocimiento y mapeo:** Escaneo de puertos y servicios (SMB, LDAP, RDP, WinRM) para identificar exposición y superficies de ataque.
- **Enumeración de usuarios:** Pruebas de enumeración Kerberos/SMB (ej.: Kerbrute) que devolvieron cuentas válidas del dominio.
- **Captura de credenciales:** Envenenamiento LLMNR/NBT-NS con Responder que permitió recoger respuestas NTLMv1/v2; se reutilizó un hash obtenido para PoC de Pass-the-Hash.

Copyright© **DMB SECURITY LABS**

- **Pruebas Kerberos:** Detección de cuentas AS-REP roasterables y ejecución de Kerberoast; extracción de TGS y cracking offline de contraseñas de cuentas de servicio (ej.: sql_svc).
- **Acceso y post-explotación:** Obtención de acceso autenticado a recursos SMB, uso de herramientas remotas (wmiexec/psexec) y volcado de NTDS desde el DC en laboratorio.
- **Revisión de configuración AD:** Exportación de GPOs y análisis de políticas (contraseñas, bloqueo de cuenta, firmas SMB/LDAP) y revisión de ACLs para identificar permisos inseguros.
-

Notas y recomendaciones del auditor

- Priorizar medidas de contención inmediatas: aislar el controlador comprometido, revocar sesiones/tickets y documentar la evidencia.
- Si se confirma extracción del hash krbtgt, ejecutar rotación doble de krbtgt y plan de recuperación controlado, no devolver a producción sin validación.
- Rotar y endurecer credenciales privilegiadas y de servicio (migración a gMSA/LAPS donde proceda) y activar MFA para cuentas administrativas.
- Desactivar LLMNR/NBT-NS en endpoints, forzar SMB signing y desplegar LDAPS, establecer LockoutThreshold y elevar MinPasswordLength.
- Implementar monitorización y detección específica en SIEM/EDR para: actividad Kerberos anómala (AS-REQ/AS-REP/TGS), intentos de Kerberoast, dumps NTDS, uso de Mimikatz/Responder y patrones de Pass-the-Hash.
- Restaurar controladores desde snapshots/backups verificados o reconstruir DC si existe duda sobre su integridad antes de reintegrarlos a la red.

Copyright© **DMB SECURITY LABS**

Fortalezas y Debilidades Clave

Fortalezas

- Existencia de GPOs y políticas de dominio aplicadas: hay una base de controles centralizada que puede aprovecharse para mitigaciones rápidas.
- Parte de la infraestructura presenta configuración de seguridad (por ejemplo, en algunos equipos SMB signing aparece habilitado), lo que reduce la superficie en esos nodos.
- La complejidad de contraseñas está activada en el dominio, proporcionando un punto de partida para mejorar la longitud y la política de rotación.

Debilidades

- Respuestas LLMNR/NBT-NS activas en la red que permitieron captura de hashes NTLM y facilitación de ataques de spoofing.
- Política de bloqueo inadecuada (LockoutThreshold = 0) y longitud mínima de contraseña baja (MinPasswordLength = 7), que facilitan fuerza bruta y cracking offline.
- Presencia de cuentas susceptibles a AS-REP y cuentas de servicio con SPN susceptibles a Kerberoast. Contraseñas reutilizadas o débiles.
- Exposición de servicios SMB/LDAP sin firma o cifrado obligatorio (SMB signing/LDAPS no forzados en todos los equipos), aumentando el riesgo de relay y sniffing.
- Volcado del NTDS y extracción de hashes, incluido el hash de krbtgt, que permite técnicas de dominio avanzadas (Golden Ticket, DCSync) si no se corrigen.

Copyright© **DMB SECURITY LABS**

Resumen de vulnerabilidades

- **IPT-012 – NTDS-DUMP: Volcado de NTDS y extracción de hashes**
  - **Severidad:** Crítica · **CVSS:** 10.0 · **CWE:** CWE-200 / CWE-522
  - **Descripción:** Volcado del NTDS obtenido; extraídos múltiples hashes (incl. krbtgt).
  - **Evidencia:** Dump NTDS, salidas de herramientas (netexec/secretsdump/mimikatz).
  - **Recomendación:** Aislar DC, rotar krbtgt ×2 y restaurar desde backup/snapshot verificado.
- **IPT-013 – GOLDEN TICKET: Emisión forjada de TGT (posible)**
  - **Severidad:** Crítica · **CVSS:** 10.0 · **CWE:** CWE-200 / CWE-287
  - **Descripción:** Hash de krbtgt presente en el volcado; posibilita forjado de TGT en entorno controlado.
  - **Evidencia:** Hash krbtgt en NTDS / salida mimikatz.
  - **Recomendación:** Rotar krbtgt doble, documentar y validar replicación.
- **IPT-009 – USER-ENUM: Enumeración de usuarios válida (Kerberos/SMB)**
  - **Severidad:** Crítica · **CVSS:** 10.0 · **CWE:** CWE-200
  - **Descripción:** Enumeración de cuentas válidas vía Kerberos/SMB confirmada; facilita ataques subsecuentes.
  - **Evidencia:** Resultados Kerbrute / correlación con NTDS.
  - **Recomendación:** Desactivar LLMNR/NBT-NS en endpoints y aplicar throttling/limites de respuesta.
- **IPT-005 – LLMNR / NBT-NS poisoning (Responder)**
  - **Severidad:** Crítica · **CVSS:** 9.3 · **CWE:** CWE-200
  - **Descripción:** Envenenamiento LLMNR/NBT-NS permitió captura de hashes NTLM; PoC reutilización (PtH).
  - **Evidencia:** Capturas Responder / hashes capturados.
  - **Recomendación:** Desactivar LLMNR/NBT-NS, forzar resolución DNS legítima y bloquear tráfico de spoofing.
- **IPT-011 – KERBEROAST: Contraseña de cuenta de servicio (sql_svc) recuperada**

Copyright© **DMB SECURITY LABS**

  - **Severidad:** Alta · **CVSS:** 8.8 · **CWE:** CWE-521 (weak passwords)
  - **Descripción:** TGS de SPN crackeado; credencial de servicio recuperada (contraseña repetida/débil).
  - **Evidencia:** Exportación GetUserSPNs y logs de cracking.
  - **Recomendación:** Rotar contraseña de sql_svc, considerar gMSA/LAPS y reducir privilegios.
- **IPT-010 – AS-REP roasterable account**
  - **Severidad:** Alta · **CVSS:** ~8.x · **CWE:** CWE-287 / CWE-200
  - **Descripción:** Cuenta con Kerberos pre-auth deshabilitado; AS-REP obtenido y crackeable offline.
  - **Evidencia:** Output GetNPUsers / AS-REP hashes.
  - **Recomendación:** Habilitar Kerberos pre-authentication y rotar credenciales afectadas.
- **IPT-003 – SMB signing deshabilitado / posibilidad NTLM relay**
  - **Severidad:** Alta · **CVSS:** 9.x (contextual) · **CWE:** CWE-287
  - **Descripción:** SMB signing no forzado en varios hosts; riesgo de NTLM relay y manipulación.
  - **Evidencia:** Escaneos SMB / configuración GPO parcial.
  - **Recomendación:** Forzar SMB signing en servidores y clientes; deshabilitar SMBv1.
- **IPT-004 – RDP sin NLA (host detectado)**
  - **Severidad:** Media-Alta · **CVSS:** ~7.x · **CWE:** CWE-287
  - **Descripción:** RDP muestra prompt de login sin Network Level Authentication en al menos un host.
  - **Evidencia:** nmap rdp-ntlm-info / comprobación RDP.
  - **Recomendación:** Habilitar NLA en RDP y restringir accesos RDP por firewall/segmentación.
- **IPT-008 – SMB-SHARE-ACCESIBLE (autenticado, ADMIN$/C$)**
  - **Severidad:** Alta/Crítica (según alcance) · **CVSS:** 9.8 (si RW/ADMIN$) · **CWE:** CWE-200
  - **Descripción:** Shares accesibles con credenciales administrativas; acceso a ADMIN$/C$ presente.
  - **Evidencia:** smbmap / smbclient / Get-SmbShare / Get-SmbShareAccess.
  - **Recomendación:** Restringir shares, auditar accesos y eliminar uso innecesario de ADMIN$.
- **IPT-006 – PASSWORD-POLICY-WEAK**

Copyright© **DMB SECURITY LABS**

- **Severidad:** Alta · **CVSS:** ~7.x · **CWE:** CWE-521
- **Descripción:** Política con MinPasswordLength=7 y LockoutThreshold=0; facilita brute-force y cracking offline.
- **Evidencia:** Salida Get-ADDefaultDomainPasswordPolicy.
- **Recomendación:** Aumentar MinPasswordLength (≥12), configurar LockoutThreshold (≈5) y habilitar MFA para cuentas críticas.

Copyright© **DMB SECURITY LABS**

Boletín de calificaciones

Explotación inicial (Recon & enumeración)

Calificación: Aprobado *(alto riesgo detectado)*

Comentario: Durante la fase de reconocimiento y enumeración se identificaron múltiples vectores que permiten obtener información explotable del dominio: técnicas Kerberos (enumeración y respuesta del KDC), resolución insegura (LLMNR/NBT-NS) y servicios legados (SMBv1). Estas debilidades se materializaron en resultados prácticos como captura de hashes NTLM y listado de cuentas válidas que aumentan considerablemente la probabilidad de compromisos posteriores.

Evidencia: Resultados de Kerbrute, capturas de Responder, salidas de escaneo (nmap/smb) y correlación con el volcado NTDS.

Recomendación inmediata: Desactivar LLMNR/NBT-NS en endpoints, deshabilitar SMBv1, forzar SMB signing y aplicar límites/throttling en servicios de autenticación.

Explotación y post-explotación

Calificación: Crítico

Comentario: Se logró acceso autenticado y volcado de la base de cuentas (NTDS) en el controlador de dominio. La extracción de hashes, incluyendo el hash de krbtgt, y la reutilización de credenciales (pass-the-hash) demuestran control a nivel dominio y capacidad de persistencia.

Evidencia: Volcado NTDS almacenado en entorno de pruebas, salidas de netexec/secretsdump, y registros de uso de herramientas (mimikatz/netexec/wmiexec).

Recomendación inmediata: Aislar el DC afectados, revocar sesiones/tickets, preparar restauración desde snapshot/backup verificado y planificar rotación doble de krbtgt.

Copyright© **DMB SECURITY LABS**

Escalada de privilegios y movimiento lateral

Calificación: Crítico / Alto
Comentario: Existen rutas prácticas de escalada (Kerberoast, AS-REP, DCSync, PtH) y cuentas de servicio con SPN explotables; la combinación de estos vectores facilita escalada a privilegios de dominio y movimiento lateral sostenido.
Evidencia: Resultados de GetUserSPNs/GetNPUsers, TGS/AS-REP capturados y crackeados, y pruebas de wmiexec/psexec exitosas.
Recomendación inmediata: Rotar contraseñas de cuentas de servicio críticas (ej. sql_svc), aplicar gMSA/LAPS donde proceda, habilitar Kerberos pre-auth y revisar ACLs con prioridad.

Detección y respuesta (SIEM / EDR / logs)

Calificación: Insuficiente
Comentario: No se detectó evidencia de alertas o bloqueos tempranos ante las técnicas empleadas (kerberos anómalo, dumps NTDS, uso de herramientas ofensivas). La ausencia de reglas específicas limita la capacidad de respuesta frente a ataques de identidad.
Evidencia: Falta de registros/alertas relevantes observadas durante la prueba. Dependencias registradas en bitácora.
Recomendación inmediata: Desplegar reglas SIEM/EDR para AS-REQ/AS-REP/TGS anómalos, actividad Mimikatz/Responder y volcado NTDS, configurar alertas críticas y runbooks de respuesta.

Política y gobernanza (contraseñas y bloqueo)

Calificación: Mejorable
Comentario: La política de dominio muestra debilidades relevantes: MinPasswordLength bajo (7) y LockoutThreshold desactivado (0). Estas configuraciones facilitan ataques de fuerza bruta y cracking offline. Además, se detectaron cuentas con preautenticación deshabilitada y reutilización de contraseñas.
Evidencia: Salida de Get-ADDefaultDomainPasswordPolicy, GPO exportadas y ejemplos de contraseñas recuperadas por Kerberoast/NTDS.
Recomendación inmediata: Incrementar longitud mínima de contraseña (≥12), habilitar LockoutThreshold razonable (3 intentos), aplicar password history y activar MFA en cuentas privilegiadas.

Copyright© **DMB SECURITY LABS**

Postura general y hardening (GPO / servicios de red)

Calificación: Mejorable

Comentario: Existen GPOs definidos pero la aplicación es heterogénea, opciones críticas (SMB signing, LDAP integrity/LDAPS) no se forzan de manera uniforme. La presencia de servicios sin cifrado o con configuraciones legacy incrementa la superficie.

Evidencia: Exportación de GPOs (Default Domain / Default Domain Controllers), resultados de nmap y comprobaciones de firma LDAP/SMB.

Recomendación inmediata: Forzar RequireSecuritySignature en servidores y clientes, desplegar LDAPS operativo con certificados válidos, y realizar un hardening centralizado mediante GPOs verificables.

Observación final:

Los hallazgos más críticos apuntan a un compromiso de identidad y control del dominio más que a vulnerabilidades aisladas de hosts. La prioridad operacional debe centrarse en contener y remediar la exposición del AD (aislamiento, rotación de krbtgt, restauración de DCs y rotación de credenciales) y, de forma paralela, en reducir la superficie de enumeración y mejorar la detección. Las evidencias completas y las capturas están documentadas en el informe técnico y la bitácora asociada.

Copyright© **DMB SECURITY LABS**

Resultados técnicos

IPT-001 – MS08-067: Ejecución Remota de Código en el Servicio de Servidor de Windows

Severidad: Crítica
CVSS v3.1 Base Score: 10.0
Vector CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVE: CVE-2008-4250 (MS08-067).
CWE: CWE-119 (Buffer Overflow).

Equipos afectados:

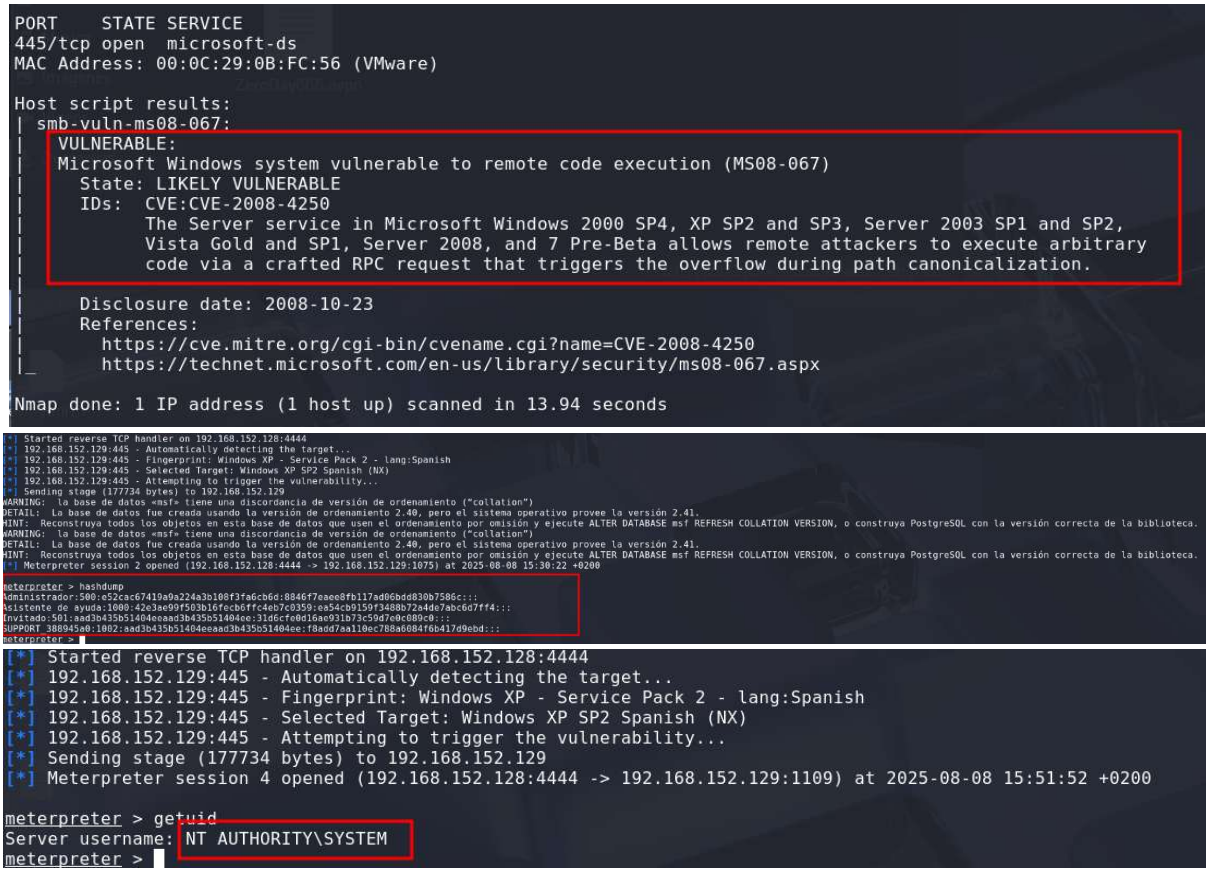
- **192.168.152.129 – PC-DAVID**

Descripción:
Se identificó que el host es vulnerable a **MS08-067**, una vulnerabilidad crítica en el servicio RPC de Windows que permite la ejecución remota de código sin autenticación. El fallo se debe a una validación incorrecta de las solicitudes RPC, lo que posibilita la ejecución de código arbitrario con privilegios **SYSTEM**.

Evidencia:

- Sistema operativo: Windows XP SP2 sin parches de seguridad aplicados.
- Confirmación de vulnerabilidad: explotación exitosa con obtención de shell remota con privilegios SYSTEM.

Copyright© **DMB SECURITY LABS**



Impacto:

Permite el compromiso completo del sistema afectado sin credenciales previas, instalación de software malicioso, exfiltración de datos y uso como punto de pivote.

Recomendaciones:

1. Migrar de forma inmediata a un sistema operativo soportado.
2. Aplicar el parche de seguridad MS08-067 si la migración no es inmediata.
3. Restringir el acceso al servicio RPC mediante cortafuegos.

IPT-002 – MS17-010: Ejecución Remota de Código en el Servicio de Servidor de Windows

Severidad: Crítica

CVSS v3.1 Base Score: 8.8

Vector CVSS: /AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE: CVE-2017-0144
CWE:

- **CWE-20 (Improper Input Validation)**
- **CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer — buffer overflow).**

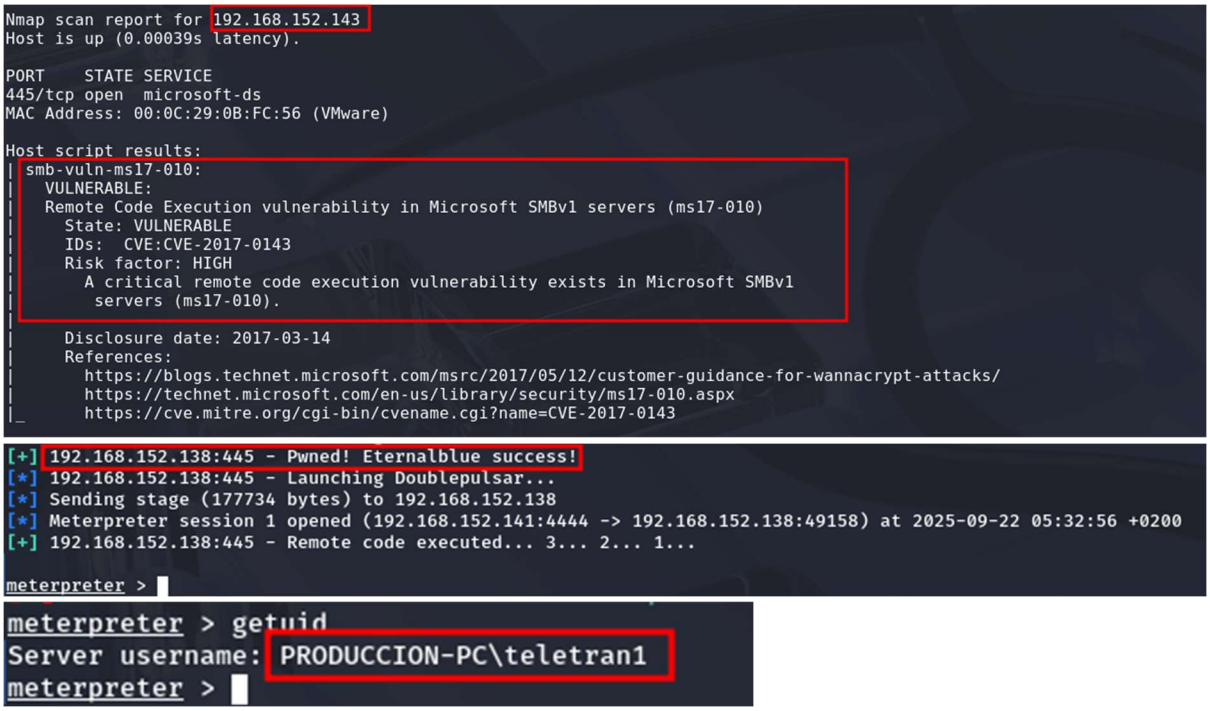
Equipos afectados:

- **192.168.152.129 – PC-DAVID**

Descripción:
Se identificó que el host **192.168.152.129 (PC-DAVID)** es vulnerable a **MS17-010 / CVE-2017-0144** en la implementación del servicio SMBv1 de Windows.
Esta vulnerabilidad permite que un atacante remoto, sin autenticación, envíe paquetes SMB especialmente construidos que provocan corrupción de memoria y posibilitan la **ejecución remota de código** en contexto SYSTEM. Puede usarse para comprometer el equipo, desplegar malware y moverse lateralmente dentro de la red.

Copyright© **DMB SECURITY LABS**

Evidencia:



Impacto:

Ejecución remota de código con privilegios **SYSTEM** en el host afectado, lo que conlleva compromiso total del equipo, posible movimiento lateral, despliegue de ransomware/otros malware y exfiltración o destrucción de datos.

Recomendaciones:

- **Aplicar inmediatamente el parche MS17-010** en todos los sistemas afectados y verificar con un nuevo escaneo que no quedan equipos sin parchear.
- **Aislar y bloquear SMB**: desconectar/aislar el host comprometido y bloquear tráfico SMB (TCP 445/139) entre segmentos y desde/hacia redes no confiables mediante firewall/ACLs hasta aplicar parches.
- **Deshabilitar SMBv1** donde sea posible y activar mecanismos de endurecimiento de SMB (p. ej. SMB signing) tras verificar compatibilidades con aplicaciones.
- **Ejecutar contención y análisis forense**: preservar logs, volcado de memoria e imágenes; realizar análisis para identificar alcance (persistencias, pivoteo) y, si procede, restaurar desde imágenes limpias.

Copyright© **DMB SECURITY LABS**

- **Desplegar monitorización y control**: activar/afinar reglas IDS/IPS para detectar patrones de EternalBlue/DoublePulsar, y habilitar Sysmon/EDR para detectar creación de servicios inusuales, accesos a lsass.exe y ejecución remota de procesos.

Copyright© **DMB SECURITY LABS**

IPT-003 – SMB-SIGNING-DISABLED: Firma SMB deshabilitada — Susceptible a NTLM Relay

Severidad: Media
CVSS v3.1 Base Score: 5.3 (Medium)
Vector CVSS: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CWE:

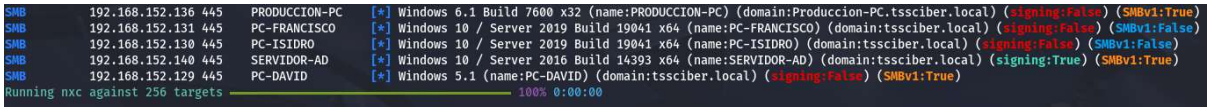
- **CWE-347 — Improper Verification of Cryptographic Signature.** (Falta/omisión de verificación/uso de firmas en el protocolo SMB.)
- **CWE-306 — Missing Authentication for Critical Function.** (La falta de firma permite autenticaciones/relay sin garantías de integridad del emisor.)

Equipos afectados:

- **192.168.152.129 – PC-DAVID**
- **192.168.152.136 - PRODUCCION-PC**

Descripción:
Se identificó que los hosts listados tienen **SMB signing deshabilitado**. Esta configuración implica que las comunicaciones SMB no requieren ni verifican firmas criptográficas en los mensajes, lo que permite a un atacante en la red realizar ataques tipo **MITM/NTLM relay** o manipular paquetes SMB para forzar autenticaciones relayadas. En práctica, esto facilita el abuso de autenticaciones NTLM contra servicios que aceptan el reenvío, posibilitando movimiento lateral o escalada de privilegios en la red.

Evidencia:



Impacto:

Posible suplantación o manipulación de comunicaciones SMB y **facilitación de ataques NTLM relay**, con riesgo de movimiento lateral y compromiso de servicios que acepten credenciales relayadas. Impacto principalmente en **integridad** y **autenticación**, con potencial escalada operacional si se combina con otros vectores.

Copyright© **DMB SECURITY LABS**

Recomendaciones:

- **Habilitar SMB signing** (GPO) en servidores y clientes.
- **Deshabilitar NTLM** o restringirlo vía políticas (migrar a Kerberos).
- **Bloquear SMB** (TCP 445/139) entre segmentos no necesarios con firewall/ACL.
- **Identificar y hardenear** servicios que aceptan NTLM (IIS, shares, RPC).
- **Activar detección** (IDS/EDR/SIEM) para ntlm-relay/Responer y monitorizar logs SMB.

Copyright© **DMB SECURITY LABS**

IPT-004 – RDP-NLA-DISABLED: RDP sin Network Level Authentication

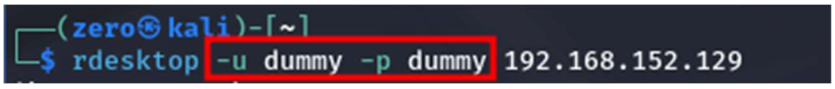
Severidad: Crítica (SO no soportado — Windows XP)
CWE: CWE-306 (Missing Authentication for Critical Function) / CWE-284 (Improper Access Control)

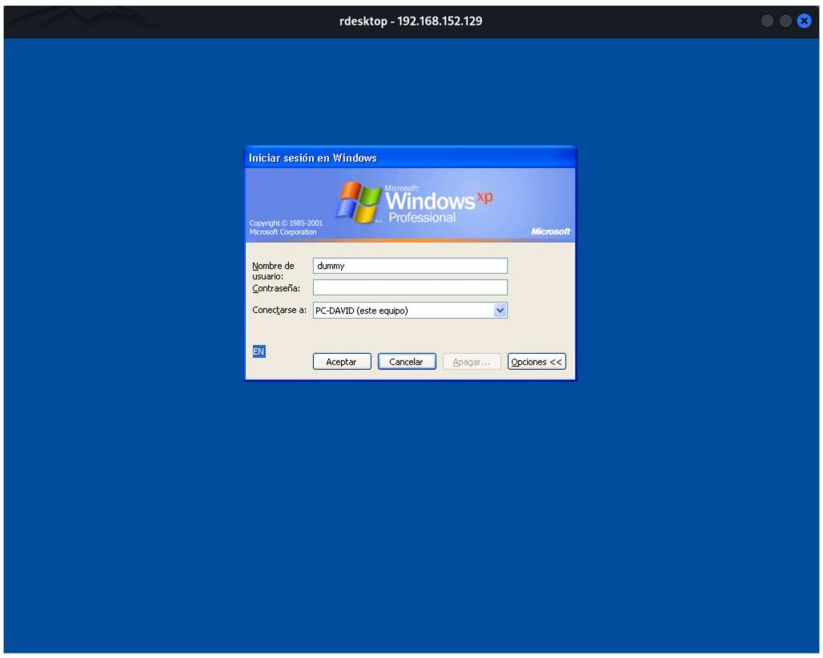
Equipos afectados:

- **192.168.152.129 – PC-DAVID**

Descripción:
Se identificó que el host **192.168.152.129 (PC-DAVID)** ejecuta **Remote Desktop sin Network Level Authentication (NLA)** y además corre **Windows XP**, un sistema operativo sin soporte y sin muchas de las mitigaciones modernas de RDP. La falta de NLA permite establecer sesiones RDP previas a la autenticación y facilita ataques de fuerza bruta, relay o explotación de vulnerabilidades RDP que no requieren autenticación previa. En un sistema EOL (XP) el riesgo práctico es muy elevado.

Evidencia:





Impacto:

Acceso remoto facilitado a un host sin soporte, con alto riesgo de compromiso total del equipo, movimiento lateral y explotación de vulnerabilidades RDP conocidas; incremento significativo de la probabilidad de intrusión y persistencia.

Recomendaciones:

- **Desconectar o aislar inmediatamente** el host (quitar acceso RDP y/o colocar en VLAN aislada) hasta que se remedie.
- **Actualizar o reprovisionar el host**: reemplazar Windows XP por un sistema soportado y actualizado (no es recomendable parchear XP; reimagen/reposición es la opción segura).
- **Bloquear RDP en el perímetro y restringir accesos**: permitir RDP únicamente desde VPN/Jump-Host gestionado y por ACLs de administración.
- **Habilitar NLA y autenticación multifactor** en hosts que lo soporten; para sistemas nuevos, usar RD Gateway o VPN + MFA.
- **Monitorizar y registrar** intentos RDP (SIEM), configurar bloqueo por intentos fallidos y revisar logs por accesos inusuales al equipo aislado.

Copyright© **DMB SECURITY LABS**

IPT-005 – LLMNR/NBT-NS Poisoning: Captura de Credenciales NTLMv1/v2

Severidad: Crítica
CVSS v3.1 Base Score: 9.3
Vector CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE:

- **CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor**.
- **CWE-287 — Improper Authentication (secundario)**.
- **CWE-319 / CWE-522 (relacionado)**

Equipos afectados:

- **192.168.152.140 – SERVIDOR-AD** → `Administrador` – *Reutilizado con éxito para compromiso total del dominio*.
- **192.168.152.129 – PC-DAVID** → `Administrador` – *Hash capturado pero no reutilizable por restricciones de inicio de sesión*.
- **192.168.152.131 – PRODUCCION-PC** → `teletran1` – *Hash capturado, no reutilizable*.
- **192.168.152.130 – PC-ISIDRO** → `icuartero` – *Hash capturado, no reutilizable*.
- **192.168.152.128 – PC-FRANCISCO** → `fsanz` – *Hash capturado, no reutilizable*.

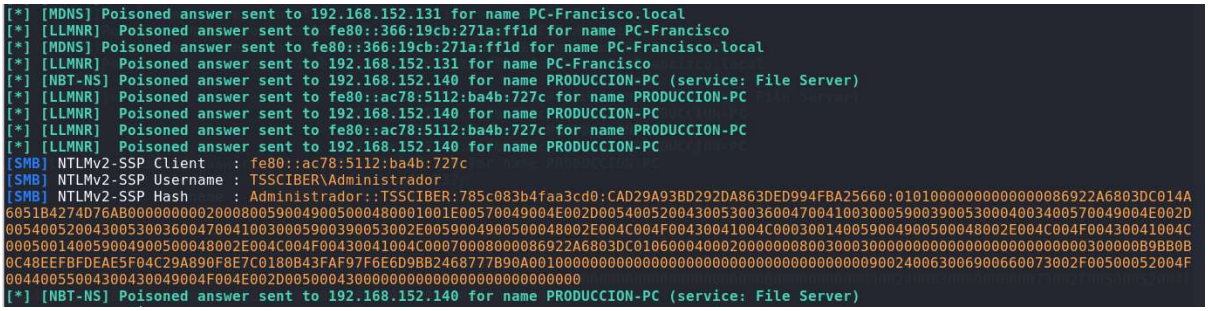
Descripción:
Varios hosts en la red responden a solicitudes LLMNR y NBT-NS, lo que permitió interceptar intentos de autenticación mediante ataques de *spoofing*.
Con la herramienta `Responder`, se capturaron múltiples hashes NTLMv1/v2 pertenecientes tanto a cuentas de usuario estándar como a cuentas privilegiadas de dominio.

El hash del usuario `Administrador` del **Controlador de Dominio** fue reutilizado exitosamente mediante *Pass-the-Hash* para obtener control total del dominio. Los demás hashes, aunque no reutilizables durante la prueba debido a restricciones de inicio de sesión o privilegios, siguen representando un riesgo de seguridad, ya que pueden ser utilizados para ataques de fuerza bruta offline o en otros entornos donde dichas credenciales sean válidas.

Copyright© **DMB SECURITY LABS**

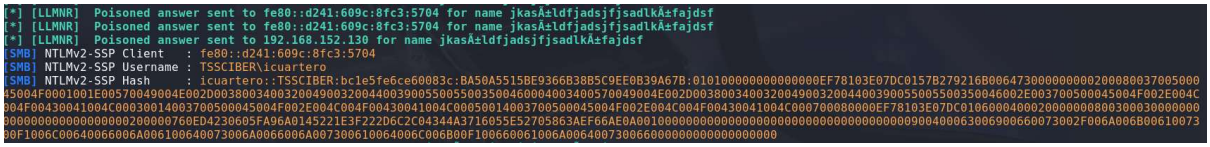
Evidencia:

- Hash NTLMv2 de `Administrador` (**SERVIDOR-AD**) → reutilizado para acceso al dominio.
- Hashes NTLMv2 de `Administrador` (**PC-DAVID**), `teletran1` (**PRODUCCION-PC**), `icuartero` (**PC-ISIDRO**), `fsanz` (**PC-FRANCISCO**).
- Herramientas: `Responder`, `netexec`, `psexec`.

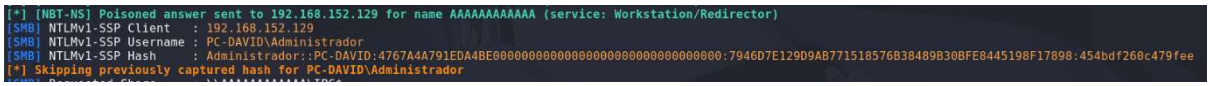



```
┌──(zeroday㉿zero)-[~/Documentos]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt --force
Created directory: /home/zeroday/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1!       (Administrador)
1g 0:00:00:00 DONE (2025-08-02 05:13) 5.882g/s 1036Kp/s 1036Kc/s 1036KC/s ROSES..311331
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(zeroday㉿zero)-[~/Documentos]
└─$
```

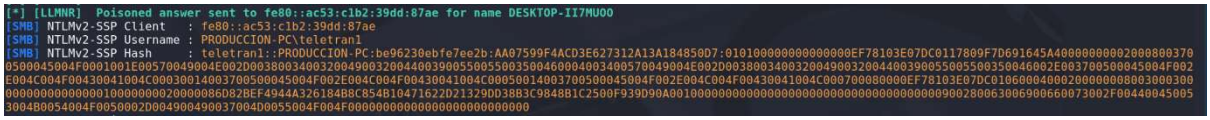
```
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.152.140.....
[*] Found writable share ADMIN$
[*] Uploading file jUOWvvnG.exe
[*] Opening SVCManager on 192.168.152.140.....
[*] Creating service fCoY on 192.168.152.140.....
[*] Starting service fCoY.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi▯n 10.0.14393]

(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```


[*] [LLMNR] Poisoned answer sent to fe80::d241:609c:8fc3:5704 for name jkasÃ±ldfjadsjfjsadlkÃ±fajdsf
[*] [LLMNR] Poisoned answer sent to fe80::d241:609c:8fc3:5704 for name jkasÃ±ldfjadsjfjsadlkÃ±fajdsf
[*] [LLMNR] Poisoned answer sent to 192.168.152.130 for name jkasÃ±ldfjadsjfjsadlkÃ±fajdsf
[SMB] NTLMv2-SSP Client : fe80::d241:609c:8fc3:5704
[SMB] NTLMv2-SSP Username : TSSCIBER\icuartero
[SMB] NTLMv2-SSP Hash : icuartero::TSSCIBER:bc1e5fe6ce60083c:BA50A5515BE9366B38B5C9EE0B39A67B:0101000000000000EF78103E07DC0157B279216B0064730000000002000800370050004500
45004F0001001E00570049004E002D0038003400320049003200440039005500550035004600040034005700490004E002D0038003400320049003200440039005500550035004602E0037005000450004F002E004C
004F0043004100 4C0003001400370050004500 4F002E004C004F0043004100 4C0005001400370050004500 4F002E004C004F0043004100 4C0007000800 0EF78103E07DC0106000400020000000800300030000000
0000000000000000020000760ED4230605FA96A0145221E3F222D6C2C04344A3716055E52705863AEF66AE0A0010000000000000000000000000000000000000000900400063006900660073002F006A006B00610073
00F1006C00640066006A0061006400730006A0066006A0073006100640006C006B00F100660061006A00640073006600000000000000000

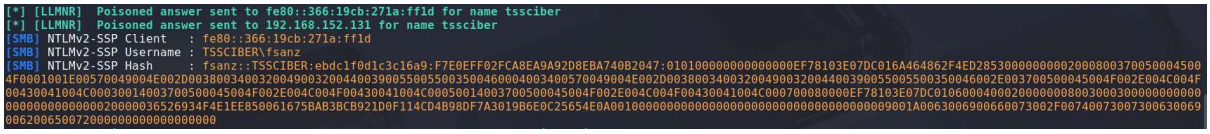
┌──(root㉿zero)-[/home/zeroday/Escritorio]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt icuartero --force
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Batman123$$ (icuartero)
1g 0:00:00:00 DONE (2025-08-07 02:14) 2.500g/s 2560p/s 2560c/s 2560C/s Password1!..gerardo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.


[*] [NBT-NS] Poisoned answer sent to 192.168.152.129 for name AAAAAAAAAAAA (service: Workstation/Redirector)
[SMB] NTLMv1-SSP Client : 192.168.152.129
[SMB] NTLMv1-SSP Username : PC-DAVID\Administrador
[SMB] NTLMv1-SSP Hash : Administrador::PC-DAVID:4767A4A791EDA4BE000000000000000000000000000000:7946D7E129D9AB771518576B38489B30BFE8445198F17898:454bdf260c479fee
[*] Skipping previously captured hash for PC-DAVID\Administrador

┌──(root㉿zero)-[/home/zeroday/Escritorio]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt pc-david --force
Warning: detected hash type "netntlm", but the string is also recognized as "netntlm-naive"
Use the "--format=netntlm-naive" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (Administrador)
1g 0:00:00:00 DONE (2025-08-07 02:15) 100.0g/s 100800p/s 100800c/s 100800C/s Password1!..mommy
Use the "--show --format=netntlm" options to display all of the cracked passwords reliably
Session completed.


[*] [LLMNR] Poisoned answer sent to fe80::ac53:c1b2:39dd:87ae for name DESKTOP-II7MUOO
[SMB] NTLMv2-SSP Client : fe80::ac53:c1b2:39dd:87ae
[SMB] NTLMv2-SSP Username : PRODUCCION-PC\teletran1
[SMB] NTLMv2-SSP Hash : teletran1::PRODUCCION-PC:be96230ebfe7ee2b:AA07599F4ACD3E627312A13A184850D7:0101000000000000EF78103E07DC0117809F7D691645A4000000000200080037
0050004500 4F0001001E00570049004E002D0038003400320049003200440039005500550035004600040034005700490004E002D0038003400320049003200440039005500550035004602E0037005000450004F002
E004C004F0043004100 4C0003001400370050004500 4F002E004C004F0043004100 4C0005001400370050004500 4F002E004C004F0043004100 4C0007000800 0EF78103E07DC0106000400020000000800300300
0000000000000001000000002000008 6D82BEF4944A326184B8C854B10471622D21329DD38B3C9848B1C2500F939D90A001000000000000000000000000000000000000900280063006900660073002F00440045005
3004B0054004F0050002D0049004900370040055004F004F0000000000000000000000000

┌──(root㉿zero)-[/home/zeroday/Escritorio]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt teletran1 --force
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (teletran1)
1g 0:00:00:00 DONE (2025-08-07 02:15) 100.0g/s 102400p/s 102400c/s 102400C/s Password1!..gerardo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.


[*] [LLMNR] Poisoned answer sent to fe80::366:19cb:271a:ff1d for name tssciber
[*] [LLMNR] Poisoned answer sent to 192.168.152.131 for name tssciber
[SMB] NTLMv2-SSP Client : fe80::366:19cb:271a:ff1d
[SMB] NTLMv2-SSP Username : TSSCIBER\fsanz
[SMB] NTLMv2-SSP Hash : fsanz::TSSCIBER:ebdc1f0d1c3c16a9:F7E0EFF02FCA8EA9A92D8EBA740B2047:0101000000000000EF78103E07DC016A464862F4ED2853000000002000800370050004500
4F0001001E00570049004F002D0038003400320049003200440039005500550035004600040034005700490004E002D0038003400320049003200440039005500550035004602FE0037005000450004F002E004C004F
0043004100 4C0003001400370050004500 4F002E004C004F0043004100 4C0005001400370050004500 4F002E004C004F0043004100 4C0007000800 0EF78103E07DC0106000400020000000800300300000000
0000000000000002000003652934F4E1EE850061675BAB3BCB921D0F114CD4B98DF7A3019B6E0C25654E0A001000000000000000000000000000000000000900 1A0063006900660073002F00740073007300630069
006200650072000000000000000000

┌──(root㉿zero)-[/home/zeroday/Escritorio]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt fsanz --force
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Melon123$$ (fsanz)
1g 0:00:00:00 DONE (2025-08-07 02:14) 100.0g/s 102400p/s 102400c/s 102400C/s Password1!..gerardo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

Impacto:

- Compromiso total del dominio a través de credenciales privilegiadas.
- Riesgo de escalada de privilegios mediante reutilización de hashes.
- Potencial de ataques de fuerza bruta offline para obtener contraseñas en texto plano.

Recomendaciones:

1. Deshabilitar LLMNR y NBT-NS mediante GPO en todos los sistemas.
2. Forzar Kerberos y deshabilitar NTLM siempre que sea posible.
3. Configurar **SMB Signing** obligatorio.
4. Cambiar de forma inmediata las contraseñas de todas las cuentas afectadas.
5. Implementar segmentación de red para limitar el movimiento lateral de atacantes.

Copyright© **DMB SECURITY LABS**

IPT-006 – PASSWORD-POLICY-WEAK: Política de contraseñas con longitud mínima insuficiente y bloqueo de cuentas deshabilitad

Severidad: Alta
CWE:

- **CWE-521 (Weak Password Requirements)**
- **CWE-307 (Improper Restriction of Excessive Authentication Attempts)**

Equipos afectados:

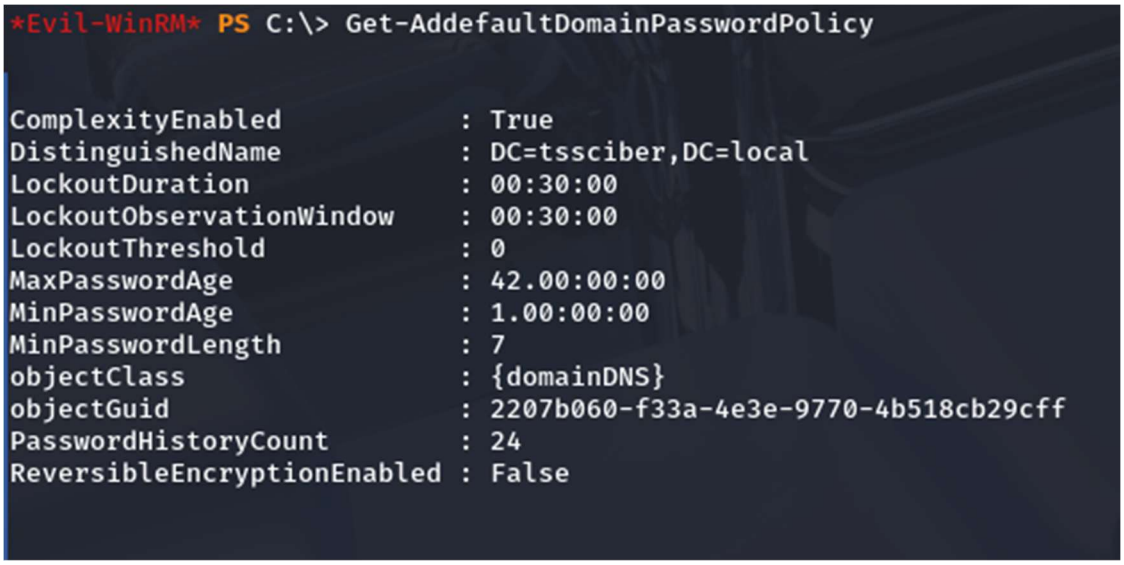
- **192.168.152.140 – SERVIDOR-AD**
- **192.168.152.129 – PC-DAVID**
- **192.168.152.131 – PRODUCCION-PC**
- **192.168.152.130 – PC-ISIDRO**
- **192.168.152.128 – PC-FRANCISCO**

Descripción: Se identificó que la política de dominio permite contraseñas con longitud mínima de **7** caracteres y que el umbral de bloqueo de cuentas (LockoutThreshold) está en **0**, lo que significa que las cuentas **no se bloquean** tras intentos fallidos. Esta combinación facilita ataques de *credential stuffing*, *password spraying* y reduce el coste de cracking offline de hashes NTLM.

Evidencia:

- MinPasswordLength = **7**
- ComplexityEnabled = **True**
- PasswordHistoryCount = **24**
- LockoutThreshold = **0** (bloqueo deshabilitado)
- LockoutDuration = 00:30:00
- MaxPasswordAge = 42 días
  (Captura: salida de Get-ADDefaultDomainPasswordPolicy).

Copyright© **DMB SECURITY LABS**



Impacto:

Longitudes mínimas bajas y ausencia de bloqueo incrementan significativamente la probabilidad de acceso no autorizado por fuerza bruta / spraying y facilitan el compromiso de cuentas; en combinación con enumeración de usuarios, puede llevar a acceso inicial y movimiento lateral.

Recomendaciones:

- **Aumentar longitud mínima y usar passphrases:** establecer MinPasswordLength ≥ 12 (ideal 12–14) y promover passphrases; además implementar una **lista de contraseñas prohibidas** (banned-passwords).
- **Habilitar bloqueo de cuentas:** configurar LockoutThreshold (ej. 5 intentos) y LockoutDuration/ObservationWindow (ej. 15–30 min), valorando el riesgo DoS en servicios críticos.
- **Implementar MFA:** desplegar autenticación multifactor para cuentas privilegiadas (y, si es posible, para usuarios generales) para reducir riesgo ante credenciales robadas.
- **Mantener controles complementarios:** conservar PasswordHistoryCount >= 24 y ComplexityEnabled = true; usar Fine-Grained Password Policies (FGPP) para excepciones de cuentas críticas.
- **Detectar y monitorizar ataques de credenciales:** activar alertas SIEM/IDS para patrones de password spraying/credential stuffing, contabilizar fallos de

Copyright© **DMB SECURITY LABS**

autenticación por cuenta/origen y revisar MaxPasswordAge (42 días aceptable si se aplica MFA y banned-passwords; considerar ajustar a la política corporativa).

IPT-008 – SMB-SHARE-LISTING-ONLY: Share visible pero requiere autenticación

Severidad: Crítica
CVSS v3.1 Base Score: 10.0
Vector CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

Afectados:

- **192.168.152.129 – PC-DAVID**

Descripción: Se detectaron shares SMB que requieren autenticación y, usando credenciales válidas obtenidas en la **IPT005,** se obtuvo acceso con permisos de lectura/escritura a recursos incluidos **ADMIN$** y **C$**. Un share identificado como **"Mis documentos / Contraseñas de la Empresa"** sugiere presencia de datos sensibles. El acceso permite extracción de información, subida/ejecución de binarios y potencial movimiento lateral.

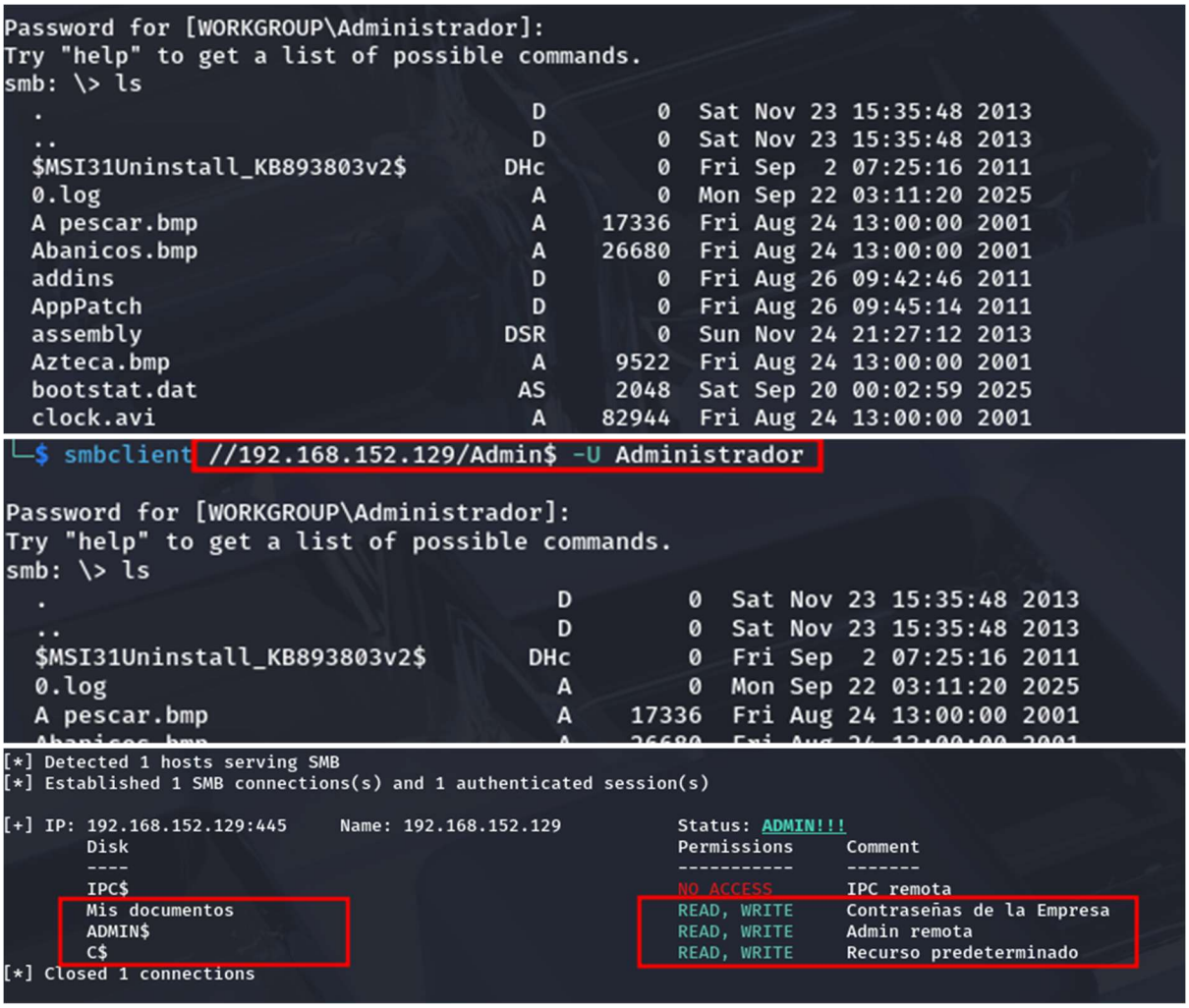
Copyright© **DMB SECURITY LABS**

Evidencia:

```
┌──(zero㉿kali)-[~]
└─$ smbclient -L //192.168.152.129
Password for [WORKGROUP\zero]:

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC remota
        Mis documentos  Disk      Contraseñas de la Empresa
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

```
┌──(zero㉿kali)-[~/.nxc/logs/ntds]
└─$ smbclient -L "//192.168.152.129" -N


        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC remota
        Mis documentos  Disk      Contraseñas de la Empres
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```


Copyright© **DMB SECURITY LABS**



Impacto: Un atacante con estas credenciales puede extraer contenido sensible, desplegar malware o ejecutar código remoto (vía ADMIN$ / servicios), facilitando escalada y compromiso adicional en la red. El riesgo es crítico si las credenciales usadas pertenecen a usuarios con privilegios elevados.

Recomendaciones:

- **Eliminar o restringir shares innecesarios** (aplicar principio de mínimo privilegio).
- **Restringir acceso SMB por ACLs y firewall** — permitir sólo hosts/segmentos imprescindibles.
- **Deshabilitar SMBv1 y forzar SMB signing** en servidores y clientes.
- **Mover datos sensibles fuera de shares públicos** a repositorios cifrados/controlados y aplicar DLP.

Copyright© **DMB SECURITY LABS**

IPT-009 – USER-ENUM: Enumeración de usuarios válida vía Kerberos/SMB

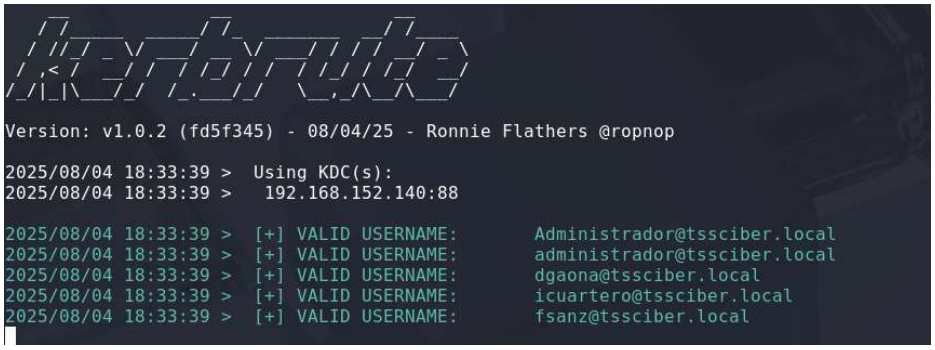
Severidad: Crítica
CVSS v3.1 Base Score: 10.0
Vector CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

Equipos afectados:

- **192.168.152.140 – ServidorAD**

Descripción:
La prueba de enumeración contra el KDC/SMB devolvió respuestas que permiten identificar cuentas de dominio válidas (ej.: Administrador, administrador, dgaona, icuartero, fsanz). Las mismas identidades se corroboraron en el volcado NTDS obtenido, confirmando la veracidad de la enumeración. Además, se detectó la presencia del hash relacionado con la cuenta krbtgt en el volcado lo que aumenta el riesgo.

Evidencia:



Impacto:
La capacidad de enumerar cuentas válidas facilita ataques posteriores de fuerza bruta y técnicas Kerberos (AS-REP roasting, Kerberoast). Si a esto se suma un volcado del NTDS (y la extracción de hashes como krbtgt), un atacante podría escalar privilegios a nivel de dominio, emitir tickets forjados o realizar movimiento lateral masivo. En este contexto el impacto potencial es muy alto para confidencialidad, integridad y disponibilidad del dominio.

Recomendaciones:

- **Forzar SMB signing y LDAPS.** (RequireSecuritySignature=1, usar LDAPS).
- **Bloqueo de cuentas.** (LockoutThreshold ≈ 5 + duración/ventana).
- **MFA en cuentas privilegiadas.** (administradores y acceso remoto).
- **Contraseñas más fuertes + rotar krbtgt si aplica.** (mínimo ≥12; rotación ×2).
- **Monitorizar Kerberos/LDAP.** (reglas SIEM para AS-REQ/AS-REP/TGS y fallos múltiples).

Copyright© **DMB SECURITY LABS**

IPT-010 – ASREP-ROASTABLE: Cuenta susceptible a AS-REP Roasting detectada

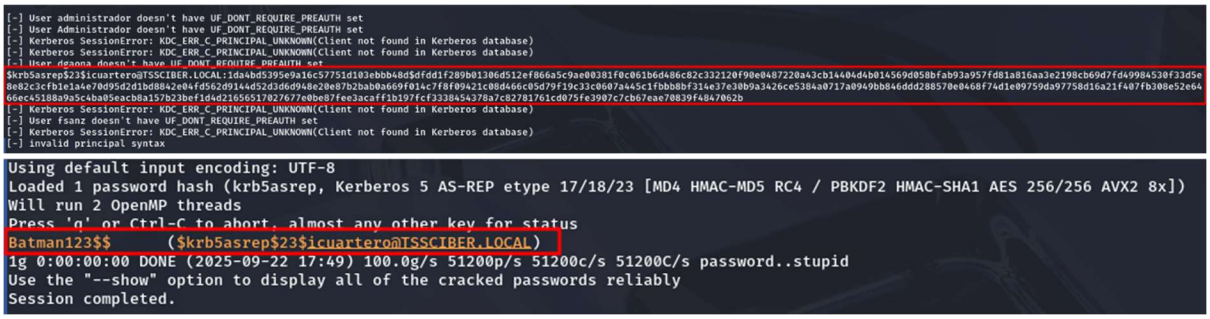
Severidad: Alta
CVSS v3.1 Base Score: 7.5
Vector CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: CWE-200 (Exposure of Sensitive Information) / CWE-255 (Credentials Management)

Equipos afectados:

- **192.168.152.140 – SERVIDORAD**

Descripción: Se ha detectado una cuenta de dominio configurada sin preautenticación Kerberos (AS-REP roasterable). Esto permitió obtener el AS-REP hash y se pudo crackear offline. La existencia de cuentas con Do not require Kerberos preauthentication habilitado facilita ataques offline contra la contraseña del usuario.

Evidencia:



Impacto: Un atacante que capture el AS-REP hash puede realizar cracking offline y, si obtiene la contraseña, autenticarse como el usuario objetivo. Dependiendo del nivel de privilegios de la cuenta, esto puede permitir acceso a recursos internos, movimiento lateral y posible escalada. Por ello el riesgo es alto mientras haya cuentas con preautenticación deshabilitada y contraseñas débiles.

Recomendaciones:

- **Habilitar preautenticación Kerberos** — desactivar “Do not require Kerberos preauthentication” en las cuentas.

Copyright© **DMB SECURITY LABS**

- **Forzar contraseñas fuertes y rotación** — longitud ≥12, complejidad y expiración.
- **Implementar MFA** — especialmente en cuentas con privilegios o accesos remotos.
- **Monitorizar AS-REP/AS-REQ** — reglas SIEM para detectar hashes AS-REP y actividad de cracking.
- **Forzar cambio de credenciales comprometidas** — reset inmediato de la cuenta afectada y revisar sesiones activas.

Copyright© **DMB SECURITY LABS**

IPT-011 – KERBEROAST: Contraseña de cuenta de servicio recuperada por Kerberoast

Severidad: Alta
CVSS v3.1 Base Score (recomendado): 8.8 (Alta)
Vector CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
CWE:

- **CWE-521 — *Weak Password Requirements* (contraseñas de servicio demasiado débiles).**
- **CWE-200 (Exposure of Sensitive Information).**
- **CWE-287 (Improper Authentication).**

Equipos afectados:

- **192.168.152.140 – SERVIDORAD**

Descripción: Cuenta de servicio sql_svc con SPN fue objetivo de Kerberoast: se obtuvieron TGS cifrados y se pudo crackear la contraseña. **Nota:** si sql_svc tiene permisos sobre otros recursos (bases de datos, backups, permisos en AD o capacidad para escribir en servicios), el impacto operativo puede escalar significativamente y requerir clasificación de riesgo mayor.

Evidencia:

Impacto:

- Exposición de credenciales de servicio: posibilita acceso directo a recursos internos (bases de datos, archivos, servicios).
- Movimiento lateral y escalada: si la cuenta tiene accesos privilegiados, puede permitir compromisos adicionales en la red.

Copyright© **DMB SECURITY LABS**

- Persistencia/ejecución: un atacante puede usar la cuenta para ejecutar servicios, automatizaciones o mantener acceso persistente.

Recomendaciones:

- **Forzar contraseñas fuertes para cuentas de servicio** (longitud ≥16, sin reuse).
- **Migrar a Managed Service Accounts / gMSA** para evitar contraseñas estáticas.
- **Reducir privilegios de cuentas con SPN** (principio de mínimo privilegio).
- **Rotar contraseñas de la cuenta sql_svc inmediatamente** y revisar usos recientes.
- **Monitorizar/alertar peticiones TGS y spikes de cracking** (SIEM: detección de Kerberoast / solicitudes TGS masivas).

Copyright© **DMB SECURITY LABS**

IPT-012 – NTDS-DUMP: Volcado de NTDS y extracción de hashes

Severidad: Crítica
CVSS v3.1 Base Score: 10.0
Vector CVSS: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CWE:

- **CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor.**
- **CWE-522 — Insufficiently Protected Credentials.**
- **CWE-287 — Improper Authentication.**

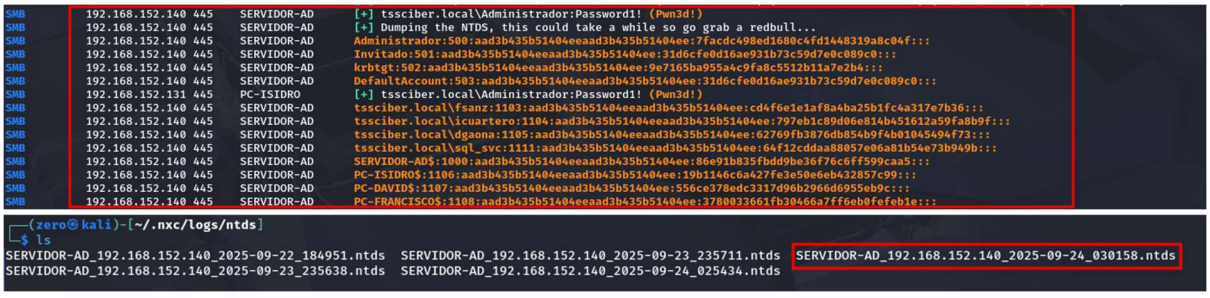
Equipos afectados:

- **192.168.152.140 – SERVIDORAD**

Descripción:

Se ha obtenido un volcado del fichero NTDS del controlador de dominio y se han extraído múltiples hashes de cuentas de dominio (incluyendo cuentas de servicio y krbtgt). **Nota:** la presencia del hash de krbtgt permite, en un entorno controlado, la emisión forjada de TGTs (Golden Ticket) si se combina con los datos adecuados — rotación inmediata requerida si se confirma extracción.

Evidencia:



Impacto:

- Compromiso total de credenciales del dominio (hashes de usuarios y cuentas de servicio).
- Posibilidad de emitir Golden Tickets (persistencia y acceso ilimitado).

Copyright© **DMB SECURITY LABS**

- Movimiento lateral, escalada de privilegios y extracción masiva de datos.
- Pérdida de integridad de AD (inserción de cuentas/privilegios) y riesgo de indisponibilidad de servicios críticos.
- Riesgo regulatorio y pérdida reputacional por exposición de datos.

Recomendaciones:

- Aislar el controlador de dominio comprometido y revocar todas las sesiones administrativas.
- Rotar la cuenta **krbtgt** dos veces y documentar el proceso.
- Restaurar o reconstruir el/los DC desde snapshots/backups verificados y validar replicación.
- Rotar y endurecer credenciales privilegiadas y de servicio; migrar a gMSA/LAPS y activar MFA para cuentas administrativas.
- Cifrar y restringir accesos a backups críticos; desplegar reglas SIEM/EDR para detección de dumps NTDS y uso de herramientas ofensivas.

Copyright© **DMB SECURITY LABS**

IPT-013 – GOLDEN TICKET: Emisión forjada de TGT Kerberos usando el hash de KRBTGT

Severidad: Crítica
CVSS v3.1 Base Score: 10.0
Vector CVSS: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Equipos afectados:

- **192.168.152.140 – SERVIDORAD**

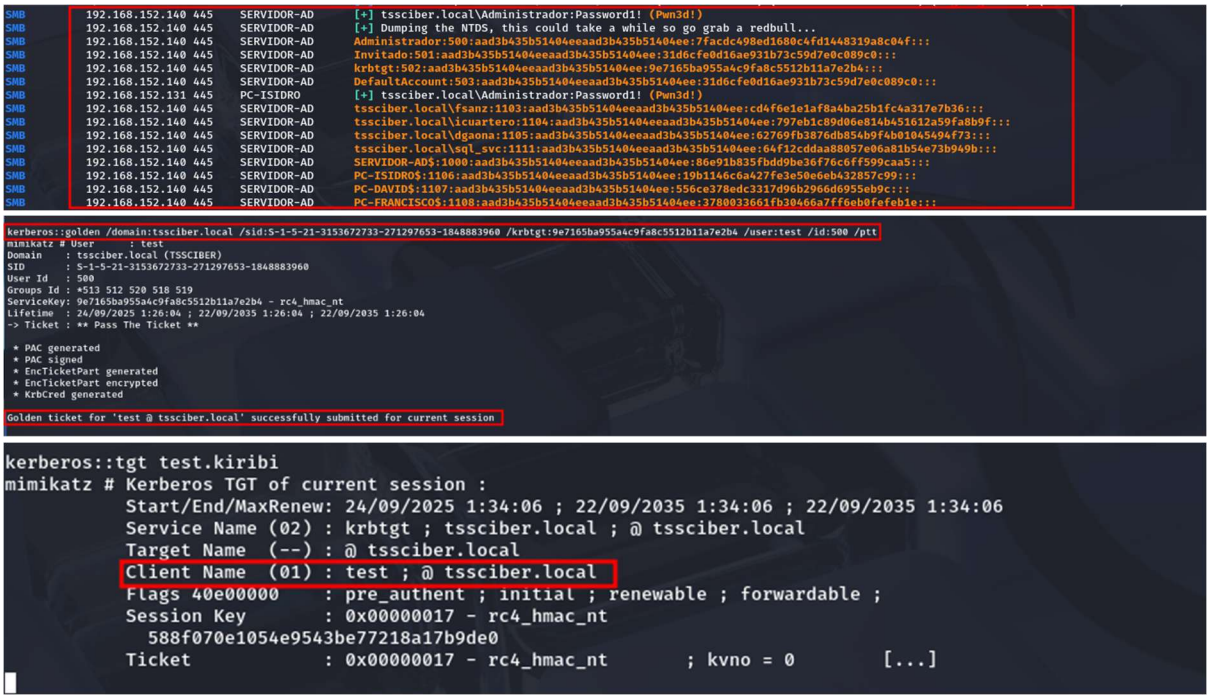
Descripción:

El acceso inicial en el laboratorio se obtuvo tras capturar credenciales NTLM durante ataques de tipo LLMNR/NBT-NS poisoning. Posteriormente, los hashes NTLM capturados fueron descifrados/validados y reutilizados para autenticación (Pass-the-Hash / uso directo de credenciales), lo que permitió obtener privilegios administrativos en hosts clave. Con credenciales administrativas se realizó acceso al controlador de dominio y se volcaron las credenciales de AD (NTDS), incluida la cuenta krbtgt. A partir de esa extracción se demostró la posibilidad de forjar TGT Kerberos válidos (Golden Ticket), confirmada mediante inyección de ticket y verificación de TGT activo en la sesión.

Se ha identificado y extraído el hash de la cuenta krbtgt del dominio (TSSCIBER.LOCAL). La cuenta krbtgt es la clave maestra utilizada por el KDC para firmar/validar Ticket Granting Tickets (TGT). La disponibilidad del hash de krbtgt permite la generación forzada de TGT válidos (Golden Tickets), lo que posibilita el acceso persistente y furtivo con privilegios de dominio, saltándose controles de autenticación y auditoría convencionales. **Las capturas incluidas muestran tanto la extracción del hash de krbtgt como la creación/inyección de tickets Kerberos en la sesión.**

Copyright© **DMB SECURITY LABS**

Evidencia:



Impacto: La extracción del hash de krbtgt y la capacidad de forjar TGT permiten el compromiso completo y persistente del dominio, evasión de controles de acceso y de detección, y la capacidad de actuar como cualquier usuario del dominio, incluyendo administradores. Esto representa control total sobre la infraestructura de Active Directory.

Recomendaciones:

- Rotar la cuenta krbtgt **dos veces consecutivas** siguiendo el procedimiento oficial y planificado (rotación controlada en ventanas de mantenimiento).
- Restringir y auditar el acceso a los privilegios Replicating Directory Changes / SeEnableDelegation y al servicio LDAP; revisar y minimizar cuentas con permisos DCSync.
- Implementar modelo de administración por niveles (tiered administration) y proteger cuentas de alto privilegio con MFA y credenciales no reutilizadas.
- Habilitar y afinar detección de anomalías Kerberos (alertas para emisión inusual de TGT, uso de tickets con duración anómala o tickets firmados con claves no rotadas).

Copyright© **DMB SECURITY LABS**