UNIVERSIDAD ALFONSO X EL SABIO

BUSINESS & TECH

GRADO EN INFORMÁTICA

(GIF)

TRABAJO FIN DE GRADO

Análisis de la detectabilidad de técnicas ofensivas en entornos Active Directory mediante monitorización centralizada con ELK

DAVID JIMÉNEZ SALCEDO

JUNIO 2026

Índice

Índice de Ilustraciones

Índice de tablas

1. Introducción y objetivos

Mi Trabajo de Fin de Grado tiene como objetivo el análisis de la detectabilidad de técnicas ofensivas en entornos corporativos basados en Active Directory mediante el diseño, despliegue y monitorización de un laboratorio controlado. A diferencia de un enfoque centrado únicamente en la ejecución de ataques o en la explotación de vulnerabilidades, este trabajo se orienta a evaluar qué técnicas generan evidencias detectables en un sistema de monitorización y en qué condiciones dicha detección resulta efectiva.

Para ello, se ha construido una infraestructura que simula una red empresarial interna lo más realista posible compuesta por un controlador de dominio, workstations, un webserver, dos servidores de base de datos y un servidor de logs, los cuales permiten reproducir escenarios reales y generar eventos que puedan ser analizados posteriormente desde un punto de vista defensivo.

El laboratorio ha sido diseñado para simular de forma controlada distintas fases habituales dentro de una intrusión sobre una red basada en Active Directory incluyendo reconocimiento, enumeración, movimiento lateral, abuso de Kerberos, escalada de privilegios y persistencia. Además, se analiza el comportamiento de los sistemas de registro ante estas acciones y la capacidad de detección que ofrecen las distintas fuentes de datos disponibles. Para ello se han configurado usuarios, grupos, políticas de grupo y cuentas de servicio que permiten reproducir técnicas comúnmente utilizadas en entornos Active Directory reales. Estas técnicas se alinean con comportamientos descritos en el marco MITRE ATT&CK lo que permite contextualizar cada acción y facilitar el análisis posterior desde el punto de vista de la detectabilidad.

De forma paralela, todas las máquinas del dominio generan eventos que son centralizados en el servidor ELK01 el cual integra Elasticsearch, Kibana y Vector para la recolección, indexación y visualización de logs. Este enfoque permite no solo registrar la actividad del sistema, sino también analizar en detalle los eventos generados en cada fase, evaluar su detectabilidad y estudiar las limitaciones observadas en función de las fuentes de datos disponibles, la configuración de auditoría y el uso de herramientas adicionales como Sysmon.

El entorno ha sido desplegado en VMWare Workstation Pro componiéndose de 8 máquinas principales dentro del dominio “lab.local”, cada una con un rol específico que simula una infraestructura corporativa real. Una vez implementada la infraestructura se han ejecutado distintas técnicas sobre el entorno Active Directory comenzando desde un acceso inicial limitado y avanzando mediante técnicas de enumeración, abuso Kerberos, movimiento lateral mediante SMB, explotación de cuentas de servicio y abuso de servicios web y bases de datos. Todas estas acciones han sido monitorizadas en tiempo real mediante ELK permitiendo recopilar las evidencias necesarias para analizar el comportamiento del dominio ante cada técnica.

Por lo tanto, este proyecto tiene como principal objetivo analizar la capacidad real de detección de distintas técnicas ofensivas en Active Directory a partir de los eventos generados identificando qué acciones producen evidencias claras, cuáles requieren correlación avanzada y cuáles presentan una visibilidad limitada en los registros nativos de Windows sin el uso de telemetría adicional.

Finalmente, se destaca que se trata de un entorno de prueba controlado en el que determinados mecanismos de defensa han sido desactivados de forma deliberada con el objetivo de evitar interferencias y poder analizar de manera aislada los eventos generados y la detectabilidad asociada a cada técnica utilizada dentro del dominio.

2. Estado del arte

Active Directory en entornos corporativos

Active Directory es el servicio de directorio desarrollado por Microsoft que permite la gestión centralizada de identidades, autenticación y control de acceso en entornos corporativos. Se estructura de forma jerárquica en dominios, unidades organizativas (OUs) y objetos como usuarios, equipos o grupos lo que facilita la administración de forma ordenada y escalable. Esta organización permite aplicar políticas de seguridad mediante GPOs de forma centralizada garantizando consistencia en la configuración de todos los sistemas del dominio.

En el ámbito de la autenticación, el Active Directory usa principalmente el protocolo Kerberos que se basa en un sistema de tickets gestionado por el controlador de dominio y es el encargado de validar identidades dentro de la red. De forma complementaria también emplea NTLM para mantener compatibilidad con sistemas legacy. Con este modelo se evita el envío de contraseñas en texto claro aunque las configuraciones inseguras o el uso de cifrados débiles pueden ser explotados mediante técnicas como Kerberoasting o Pass-The-Hash.

Además de la autenticación, AD integra servicios esenciales como la resolución de nombre a través de DNS, la gestión de permisos a través de listas de control de acceso (ACLs) y la delegación de tareas administrativas a distintos perfiles dentro de la organización. Estas capacidades permiten una gestión más eficiente de grandes infraestructuras reduciendo la complejidad operativa y facilitando el control de accesos a recursos corporativos.

Debido a su papel central en la gestión de identidades y accesos Active Directory es un elemento crítico desde el punto de vista de la seguridad. El compromiso del dominio puede implicar el control total de la infraestructura permitiendo a un atacante acceder a sistemas, modificar configuraciones o mantener persistencia dentro del entorno.

Amenazas en entornos Active Directory

Debido al papel que tiene en la gestión de identidades y accesos, AD se ha convertido en uno de los principales objetivos en ataques dirigidos a entornos corporativos. Una vez que un atacante obtiene acceso inicial a la red el objetivo principal se convierte en la escalada de privilegios hasta alcanzar cuentas con altos niveles de autorización como administradores de dominio. Este proceso se suele dar en fases de postexplotación donde el atacante busca expandir su control dentro del entorno.

Existen múltiples técnicas ampliamente usadas que aprovechan tanto configuraciones inseguras como el propio funcionamiento de Active Directory, las cuales permiten recolectar información, moverse lateralmente y abusar de servicios internos del dominio. Algunas son:

- Enumeración de usuarios y recursos del dominio
- Abuso de Kerberos (Kerberoasting, PtT...)
- Movimiento lateral mediante protocolos como SMB (445/TCP) o RDP (3389/TCP)
- Explotación de cuentas de servicio mal configuradas
- Abuso de delegaciones y permisos excesivos

Una de las características más relevantes de estas técnicas es que muchas de ellas usan protocolos habituales del dominio, lo que hace que su actividad sea difícil de distinguir del actividad cotidiana generada por cuentas internas del dominio. Por ejemplo, cuando se hace uso de Kerberos o se accede a recursos compartidos son acciones habituales dentro de un dominio pero pueden ser explotadas con fines maliciosos.

Esta característica introduce un desafío directo desde el punto de vista de la detección ya que la presencia de eventos de autenticación o acceso no resulta suficiente por sí sola para determinar un comportamiento malicioso. La detección efectiva depende de relacionar eventos procedentes de distintas fuentes y analizarlos dentro de una misma secuencia temporal debido a que sin un análisis adecuado de los logs generados, muchas de estas actividades pueden pasar desapercibidas.

MITRE ATT&CK como marco de referencia

El framework MITRE ATT&CK es un modelo ampliamente usado en ciberseguridad el cual clasifica las tácticas y técnicas empleadas por atacantes en entornos reales. Se basa en conocimiento recopilado de incidentes reales y proporciona una estructura estandarizada que permite analizar el comportamiento de los adversarios de forma sistemática. Gracias a este enfoque es posible describir ataques complejos.

MITRE ATT&CK organiza las técnicas en distintas fases del ciclo de ataque, conocidas como tácticas, entre las que se incluyen reconocimiento, ejecución, persistencia, escalada de privilegios o movimiento lateral. Cada una de estas tácticas agrupa múltiples técnicas específicas que describen cómo un atacante puede alcanzar sus objetivos dentro de un sistema. Esta organización permite analizar un ataque no como acciones aisladas sino como una secuencia estructurada de comportamientos.

El uso de este framework es muy útil en tareas de detección y respuesta ya que permite mapear eventos y actividades observadas en los sistemas con técnicas concretas conocidas. De este modo se facilita la creación de reglas de detección, la correlación de eventos y la identificación de patrones de comportamiento malicioso dentro de la infraestructura.

En este trabajo las técnicas ejecutadas en el laboratorio se alinean con el marco MITRE ATT&CK lo que permite contextualizar cada fase del ataque y relacionarla con patrones de comportamiento conocidos. Este enfoque no solo aporta rigor al análisis sino que también permite evaluar la detectabilidad de cada técnica en función de los eventos generados y su visibilidad en el sistema de monitorización.

SIEM y detección de amenazas

Los sistemas SIEM o Security Information and Event Management permiten la recopilación, almacenamiento y análisis centralizado de eventos generados por distintos sistemas dentro de una infraestructura. Su principal objetivo es detectar actividades anómalas o potencialmente maliciosas mediante la correlación de eventos procedentes de múltiples fuentes.

En los entornos basados en Active Directory, los SIEM desempeñan un papel en el que permiten analizar los eventos críticos relacionados con autenticación, acceso a recursos, ejecución de procesos o actividad de la red. Con la centralización de los logs procedentes de controladores de dominio, workstations y servidores se facilita mucho la identificación de patrones de comportamiento y la reconstrucción de incidentes.

Sin embargo, la eficacia de estos sistemas depende mucho de la calidad y nivel de detalle de los datos que son recopilados, además de las reglas de detección implementadas. Sin esto y sin fuentes de datos enriquecidas como Sysmon, es posible que algunas actividades pasen desapercibidas.

Uno de los principales retos en la detección es diferenciar entre actividad legítima y maliciosa, especialmente cuando la actividad ofensiva se realiza mediante cuentas reales del dominio y protocolos habituales de administración. Es por eso por lo que además del uso de SIEM es necesario relacionar autenticaciones, accesos a recursos y actividad de procesos para identificar desviaciones respecto al comportamiento esperado para identificar desviaciones sutiles dentro del entorno.

Es importante destacar que la simple recopilación de logs no implica capacidad de detección. La detección efectiva requiere la definición de reglas, el análisis conjunto de registros y el conocimiento del comportamiento normal del sistema lo que introduce un componente analítico clave en los sistemas SIEM.

ELK como plataforma de monitorización

El stack ELK (Elasticsearch, Logstash, o Vector en nuestro caso, y Kibana) es una de las soluciones más usadas para la centralización y análisis de logs en entornos de seguridad.

Elasticsearch actúa como motor de almacenamiento e indexación permitiendo gestionar grandes volúmenes de datos de forma eficiente, mientras que Kibana proporciona capacidades de visualización y análisis mediante consultas de los datos recopilados.

Esto se combina con herramientas como Sysmon y Winlogbeat para obtener una visibilidad detallada de la actividad del sistema incluyendo eventos como la creación de procesos, conexiones de red, accesos a archivos o eventos de autenticación. Esta información amplia significativamente las capacidades de auditoría nativas que tiene Windows proporcionando un nivel mayor de detalle necesario para la detección de técnicas avanzadas.

ELK no solo actúa como repositorio de logs, sino como una plataforma clave para el análisis forense y la identificación de patrones asociados a actividades maliciosas.

En este trabajo ELK se usa como plataforma central para la recopilación y análisis de eventos generados durante las distintas fases del ataque permitiendo evaluar la detectabilidad de cada técnica en función de los registros disponibles. Esto convierte a ELK en un elemento fundamental para el análisis de comportamiento del atacante y la validación de mecanismos de detección dentro del laboratorio.

Retos en la detección de ataques AD

A pesar de la disponibilidad de herramientas avanzadas de monitorización, la detección de ataques en entornos AD sigue representando un desafío significativo. Muchas técnicas ofensivas generan eventos similares a los producidos durante tareas administrativas habituales, lo que dificulta identificar comportamientos anómalos únicamente a partir de eventos aislados. En estos casos la identificación del comportamiento malicioso requiere un análisis más profundo basado en contexto y relación entre eventos procedentes de distintas fuentes.

Además, la visibilidad del sistema depende en gran medida de la configuración de auditoría y de las fuentes de datos disponibles. La ausencia de configuraciones avanzadas o de herramientas como Sysmon limita la cantidad y calidad de la información registrada reduciendo la capacidad de detección. Esto puede provocar que determinadas acciones pasen desapercibidas o que no exista suficiente evidencia para identificar correctamente una técnica empleada por una atacante.

Otro aspecto relevante es la necesidad de correlacionar eventos procedentes de múltiples fuentes como logs de seguridad, eventos del sistema o registros de red. Muchas técnicas solo pueden ser detectadas cuando se analizan de forma conjunta con diferentes evidencias lo que incrementa la complejidad del análisis y requiere herramientas adecuadas.

En este sentido, uno de los principales retos no reside únicamente en la generación de eventos, sino en la identificación de aquellos que aportan valor real para la detección evitando tanto la falta de visibilidad como el exceso de ruido.

Fuentes de datos y autenticación en Active Directory

La detección de ataques en entornos AD depende, como ya se dijo, de las fuentes de datos disponibles y de la calidad de la información que estas proporcionan. Los sistemas Windows generan eventos de seguridad a través del registro de eventos, Security Logs, donde se almacenan actividades relacionadas con la autenticación, acceso a recursos, uso de privilegios o cambios en cuentas y grupos. Estos registros constituyen la base para el análisis de seguridad ya que reflejan el comportamiento del sistema y de los usuarios dentro del dominio.

Estos eventos también presentan limitaciones en cuanto al nivel de detalle y contexto disponibles, es por eso que las herramientas como Sysmon permiten ampliar la visibilidad del sistema registrando información más granular sobre la actividad del equipo como la creación de procesos, conexiones de red, carga de librerías o modificación en el sistema. Esta información adicional resulta especialmente útil para identificar técnicas avanzadas que no quedan claramente reflejadas en los logs.

Al correlacionar estos datos es posible obtener una visión más completa del comportamiento del sistema y detectar patrones que de forma aislada podrían pasar desapercibidos. Por otra parte, este aumento de visibilidad también se traduce en un aumento considerable del volumen de información generada.

En este contexto, se hace necesario aplicar técnicas de filtrado, correlación y análisis que permitan identificar los eventos realmente relevantes.

Evaluación de vulnerabilidades y métricas de severidad

La identificación de las vulnerabilidades tiene que ir acompañada de un proceso de evaluación que permita determinar su impacto real dentro de un sistema. Esta evaluación nos sirve para priorizar riesgos, comprender las posibles consecuencias de un ataque y establecer medidas de mitigaciones adecuadas.

Una vulnerabilidad no implica necesariamente un riesgo crítico por sí misma sino que su gravedad depende de más factores como la facilidad de explotación, el nivel de acceso requerido o el impacto que puede generar sobre los sistemas afectados. Por este motivo se usan metodologías estandarizadas que permiten clasificar y comparar vulnerabilidades de forma objetiva.

Uno de estos estándares es el Common Vulnerability Scoring System (CVSS) el cual proporciona un marco de referencia para evaluar la severidad de una vulnerabilidad en base a distintos parámetros relacionados tanto con su explotación como con su impacto. Este sistema tiene en cuenta aspectos como la complejidad del ataque, la necesidad de autenticación previa, nivel de interacción requerido y el impacto sobre la confidencialidad, integridad y disponibilidad de la información.

El uso de este tipo de métricas nos permite establecer una clasificación homogénea de las vulnerabilidades identificadas durante la fase de explotación del laboratorio. Para ello se tendrán en cuenta factores como el nivel de acceso inicial, posibilidad de escalada de privilegios, impacto sobre el dominio y la capacidad de propagación dentro de la red.

Con esto, además de permitir reproducir técnicas de ataque en el trabajo se puede analizar su impacto real dentro del entorno y contextualizar el impacto potencial de las técnicas empleadas dentro del entorno relacionando directamente las acciones del atacante con sus consecuencias en el sistema.

3. Diseño del laboratorio

Infraestructura del laboratorio y arquitectura de red

El proyecto simulará una red empresarial con nombre de dominio “lab.local”. El objetivo final del laboratorio es realizar y analizar ataques comunes a AD como enumeración, escalada de privilegios, movimiento lateral y persistencia además de evaluar su detección mediante el servidor de logs.

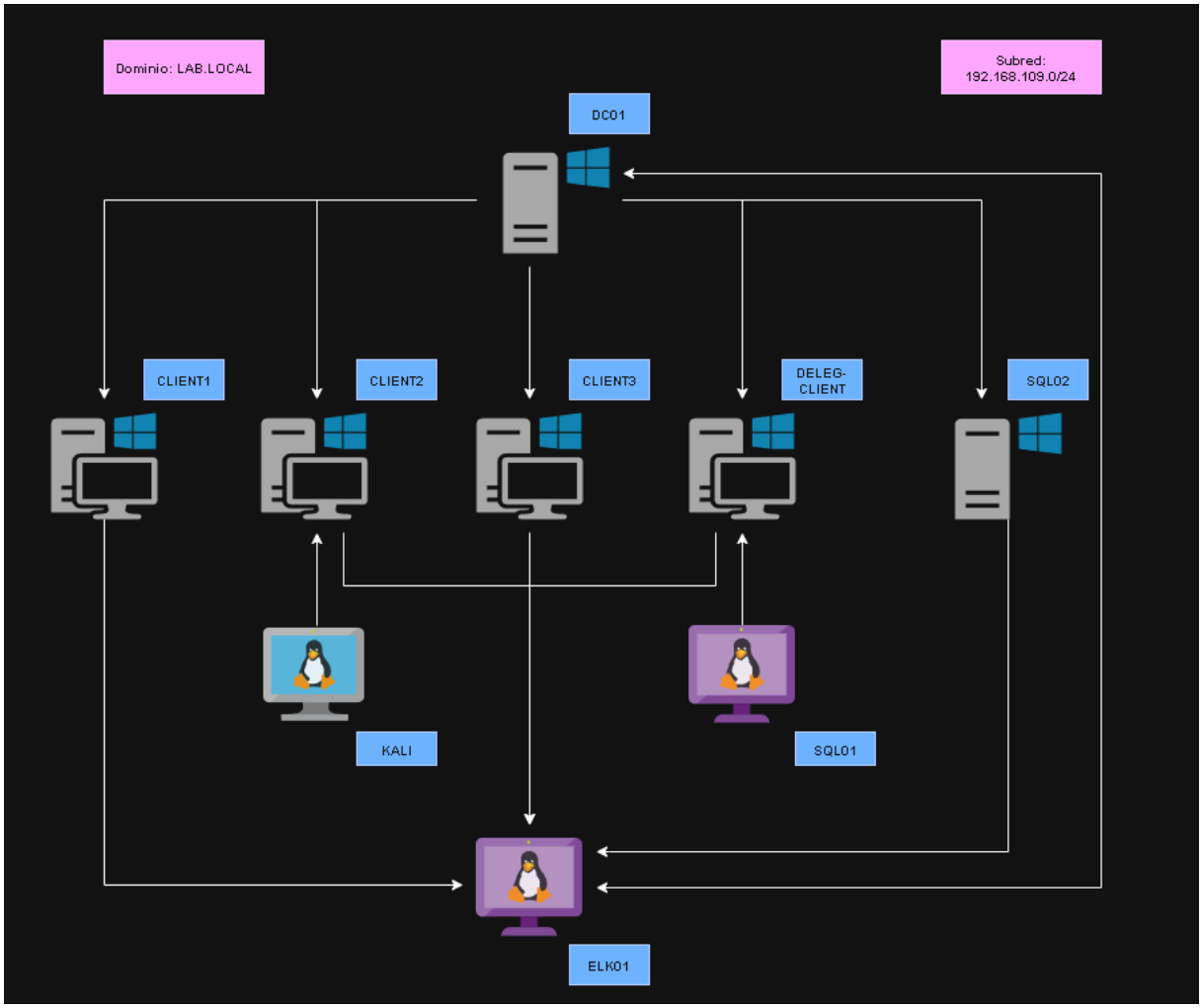

Ilustración 1. Arquitectura general del laboratorio Active Directory desplegado para el análisis ofensivo y defensivo

La imagen anterior muestra la arquitectura completa del laboratorio diseñado para el proyecto. Toda la infraestructura se encuentra dentro de la subred 192.168.109.0/24 y está compuesta por 8 máquinas principales además de un host de ataque basado en Kali Linux.

Todas las máquinas Windows tendrán Sysmon y Winlogbeat para poder enviar los logs a ELK01 mientas que SQL01 tendrá Vector para el mismo propósito.

En el diagrama se reflejan las relaciones de comunicación entre los distintos equipos y las dependencias al dominio. Todas las máquinas del dominio envían sus eventos a ELK01 a través de Vector y Winlogbeat. La máquina CLIENT2 actúa como punto inicial comprometido y permite el pivoting al resto de la infraestructura.

Todas las máquinas están unidas al dominio LAB.LOCAL y mediante comunicación directa con el controlador de dominio DC01 encargado de proporcionar los servicios de autenticación y gestión centralizada.

Sistemas Operativos Usados

El laboratorio ha sido diseñado usando distintos sistemas operativos con el objetivo de simular un entorno corporativo realista en el que coexisten varias tecnologías.

En primer lugar, se emplearon sistemas Windows tanto en estaciones de trabajo como servidores, usando versiones actuales como Windows 11 en los clientes y Windows Server 2022 en los servidores. Esta elección permite reproducir de forma fiel un entorno empresarial moderno en el que Active Directory constituye la base de la gestión de identidades y accesos. El uso de estos sistemas permite simular los mecanismos de autenticación, gestión de políticas y administración centralizada característicos de este tipo de infraestructuras.

Por otro lado, se incorporaron sistemas Linux en determinados servidores, basados en distribuciones como Ubuntu Server 24.04 con el fin de simular servicios corporativos en los que los sistemas Linux forman parte de la infraestructura usando mecanismos como Kerberos o LDAP para la gestión de identidades.

La inclusión de sistemas Linux dentro del dominio permite analizar escenarios más avanzados en los que servicios que no pertenecen al sistema Windows interactúan directamente con AD ampliando la superficie de ataque y permitiendo estudiar técnicas que afectan a entornos híbridos.

Finalmente se incluyó una máquina atacante basada en Kali, la cual integra una distribución muy usada en pruebas de pentesting. Esta me permite disponer de un conjunto completo de herramientas orientadas a la ejecución de técnicas de reconocimiento, enumeración, explotación y postexplotación dentro del entorno.

Roles de los sistemas

Clientes Windows

- **CLIENT1:** puesto de trabajo de un usuario estándar. Genera actividad típica de empleado (inicio de sesión interactivo, acceso a recursos del dominio) y permite representar un usuario. Se usa para simular un primer compromiso de credenciales
- **CLIENT2:** segundo puesto de trabajo estándar. Desde aquí se realizan las primeras acciones de enumeración desde un equipo de usuario. Tiene como objetivo el movimiento lateral y la validación de accesos a recursos compartidos y servicios internos
- **CLIENT3:** estación de trabajo asociada a un usuario de soporte con permisos delegados. Se usa para reflejar tareas reales de administración de escritorio y como posible salto intermedio en escenarios de escalada por permisos delegados.
- **DELEG-CLIENT:** equipo dedicado a escenarios de delegación Kerberos. Se emplea para pruebas de configuración de delegación y para reproducir técnicas que abusan de dicha delegación para acceder a servicios como otro usuario. Además, da servicio web a la red interna corporativa

Servidores Windows

- **DC01:** controlador de dominio. Proporciona Active Directory Domain Services y DNS, centraliza la autenticación (Kerberos/NTLM) y aplica GPOs. En él se definen OUs, grupos y cuentas de servicio o SPNs necesarios para reproducir configuraciones y errores frecuentes en entornos corporativos.
- **SQL02:** servidor miembro del dominio que expone un servicio de base de datos (SQL Server) para la red interna. Está pensado para generar superficie de ataque típica de MSSQL (enumeración de instancias, acceso por credenciales, ejecución de comandos si se habilita) y para trabajar con cuentas de servicio con SPN habituales en escenarios de Kerberoasting.

Sistemas Linux

- **ELK01:** servidor central de logs. Ejecuta el stack Elastic (Elasticsearch y Kibana, y el componente de ingesta Vector) para recibir, indexar y visualizar la telemetría del dominio. Su función es permitir evidencias en cada fase.
- **SQL01:** servidor Linux que integra una base de datos interconectada con el servidor web interno. Se utiliza para escenarios de explotación en bases de datos.

Máquina atacante

- **Kali:** máquina desde la que se realizan las fases de reconocimiento, enumeración y explotación dentro de la subred del laboratorio. Representa a un atacante con acceso a red interna por VPN o compromiso previo y agrupa las herramientas usadas como escáneres, utilidades para Kerberos, SMB, LDAP... y scripts de postexplotación.

Diseño Active Directory

La estructura de Active Directory ha sido diseñada para reproducir configuraciones habituales en entornos corporativos que permitan la ejecución de técnicas como enumeración, Kerberoasting, abuso de delegación y escalada de privilegios

Estructura organizativa (OUs)

Estas permiten agrupar usuarios, equipos y otros objetos de forma jerárquica para facilitar la aplicación de GPOs diferenciadas y una administración más ordenada. Se crearon las siguientes OUs en el entorno:

- **LAB-Users:** contiene cuentas de usuario estándar del dominio
- **Workstations:** agrupa las máquinas internas unidas al dominio
- **ServiceAccounts:** incluirá las cuentas de servicio usada por las aplicaciones y tareas automatizadas
- **LAB-Admins:** para cuentas de privilegios elevados como Helpdesk, lab_admin o los administradores de dominio delegados

Cuentas de usuario

Se han creado los siguientes usuarios:

- **User1:** usuario estándar del dominio asociado a la máquina CLIENT1.
    - OU: LAB-Users
    - Simula la actividad normal de un empleado

- **User2:** usuario con permisos limitados asociado a la máquina DELEG-CLIENT usado en pruebas de delegación
    - OU: LAB-Users
    - Sirve en escenarios de delegación
- **Attacker:** cuenta con permisos limitados asociada a la máquina CLIENT2 desde la cual se comenzará a realizar el ataque en la red interna
    - OU: LAB-Users
    - Sirve como usuario de entrada al dominio

- **Helpdesk:** miembro del grupo Helpdesk con privilegios delegados sobre equipos cliente, simularía el personal del soporte técnico, asociado a CLIENT3
    - OU: LAB_Admins
    - Simula personal de soporte técnico con permisos limitados de gestión de equipos (cambio de contraseñas, desbloqueo de cuentas…)

- **Lab_admin:** cuenta administrativa creada que tendrá privilegios administrativos en todo el dominio
    - OU: Lab-Admins
    - Sirve para administrar y realizar configuraciones que requieren altos privilegios dentro del dominio

Cuentas de servicio y SPNs

- **Svc-sql:** cuenta de servicio asociada a la base de datos utilizada por la aplicación web desplegada en SQL01
    - SPN: **MSSQLSvc/sql01.lab.local:3306**
    - OU: ServiceAccounts
    - Utilizada por el servicio web desplegado en DELEG-CLIENT para la conexión con la base de datos interna

- **Svc-sql02:** cuenta de servicio para el motor de base de datos SQL
    - SPN: **MSSQLSvc/sqlserver.lab.local:1433**
    - OU: ServiceAccounts
    - Simular acceso a base de datos con kerberos, pruebas de movimiento lateral hacia servidores de datos y kerberoasting sobre cuentas de servicio

- **Svc-web:** cuenta de servicio web IIS/HTTP
    - SPN: **HTTP/webserver.lab.local**
    - OU: ServiceAccounts
    - Application Pool de IIS y autenticación Kerberos web

Delegación de permisos

Se delega sobre la cuenta attacker el permiso Read all user information desde Active Directory Users and Computers. Esta delegación permite al usuario consultar información básica del resto de cuentas del dominio sin otorgarle capacidad de modificación. Este tipo de permisos se asigna habitualmente en entornos reales para facilitar tareas de soporte o auditoría, pero una delegación excesiva o mal controlada puede facilitar labores de reconocimiento por parte de un atacante constituyendo un punto de partida para la enumeración del dominio.

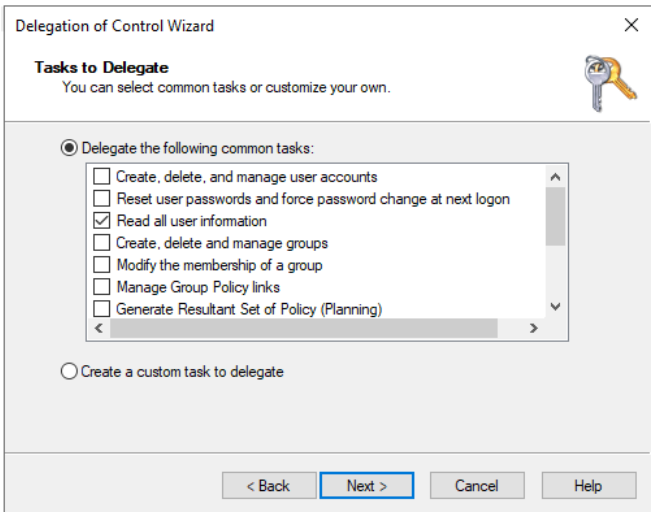

Ilustración 2. Configuración de delegación de permisos en Active Directory mediante Delegation of Control Wizard

La imagen anterior muestra el asistente de delegación de control de Active Directory utilizado para asignar permisos específicos sobre el objeto de dominio para concederle la capacidad de lectura sobre la información de usuarios.

Resumen de objetos del Active Directory

Se creó un script en .ps1 que nos diese por pantalla un resumen de lo creado hasta el momento:

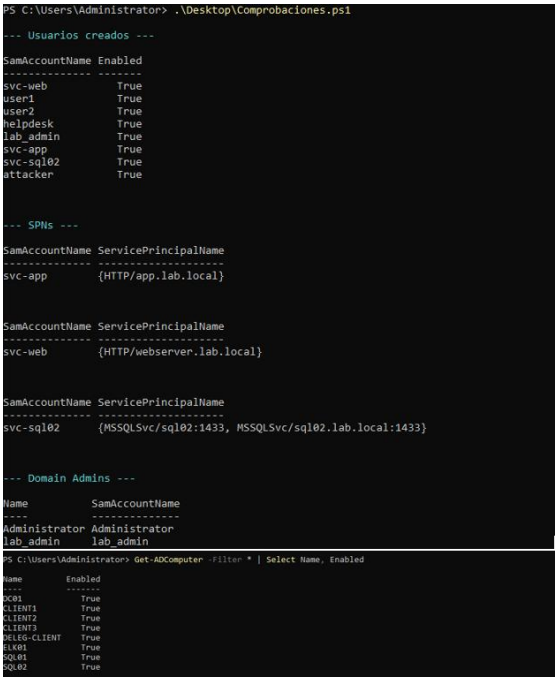

Ilustración 3. Verificación de usuarios, SPNs y equipos creados en el entorno Active Directory mediante script de PowerShell

Esta figura muestra todos los usuarios, máquinas y cuentas de servicio creadas en el entorno del laboratoria.

Sistemas de monitorización

Recolección de eventos

La recolección de eventos en el laboratorio se ha diseñado con el objetivo de obtener visibilidad sobre la actividad que se generará en los distintos sistemas creados durante la ejecución de los escenarios de ataque.

En los sistemas Windows se emplean mecanismos de registro avanzados, como Sysmon, que permiten ampliar la información recogida por el sistema operativo. Estos permiten capturar eventos relacionados con la ejecución de procesos, conexiones de red y actividad del sistema proporcionando un mayor nivel de detalles.

Además, se recopilan los eventos de seguridad nativos los cuales son enviados por agentes de recolección como Winlogbeat, incluyendo información sobre autenticaciones, uso de credenciales y actividad relacionada con los servicios de directorio. Esto será muy útil en el análisis de protocolos como Kerberos y en el seguimiento de los inicios de sesión dentro del dominio.

En los sistemas Linux se usan herramientas de recolección de logs, como Vector, que permiten capturar la actividad generada tanto por el sistema como por los servicios desplegados, como el servidor web y la base de datos, complementando así la visibilidad global del entorno.

Los eventos recopilados incluyen información sobre autenticación de usuarios, emisión de tickets Kerberos, ejecución de procesos, conexiones de red y acceso a recursos. Esto permitirá analizar el comportamiento del sistema y detectar actividades potencialmente maliciosas.

Sysmon y Winlogbeat en clientes Windows

Ambos componentes son esenciales para el registro y envío de eventos de seguridad hacia el servidor ELK01:

- Sysmon es una herramienta de Microsoft Systeminternals que amplía las capacidades de auditoría del sistema operativo registrando la información de forma detallada sobre la actividad del sistema
- Winlogbeat es un agente ligero desarrollado por Elastic que envía los registros de eventos de Windows a Elasticsearch para su análisis centralizado

Centralización de logs en ELK

La centralización de logs en el laboratorio se realizará mediante el servidor Linux ELK01 el cual actúa como punto central de recogida y análisis de los eventos generados por los distintos sistemas del dominio.

Para conseguirlo se ha empleado el stack ELK que está compuesto por Elasticsearch, Kibana y un Logstash (este último se cambió por Vector a conveniencia debido a que estaba dando fallos en el formato de los logs). Este será el encargado de recibir los eventos desde los distintos equipos del entorno.

Elasticsearch se encarga del almacenamiento e indexación de los registros permitiendo la consulta de estos de forma eficiente y facilitando el análisis de grandes volúmenes de datos generados durante la actividad del laboratorio.

El motor de búsqueda Kibana nos proporciona una interfaz de visualización que permite explorar los eventos recopilados, realizar búsquedas mediante queries y construir representaciones gráficas que faciliten la interpretación de la información.

Por la otra parte, Vector actuará como elemento que ingesta recibiendo y procesando los eventos enviados desde los sistemas Windows y Linux, asegurando su correcta integración dentro del sistema.

Esto nos permite disponer de una visión unificada del entorno facilitando la correlación de eventos entre diferentes máquinas y el análisis de la actividad generada durante las distintas fases del ataque.

Visibilidad y análisis

Una vez centralizados los eventos en ELK, fue posible analizar de forma conjunta la actividad generada en los distintos sistemas del dominio y relacionarla directamente con las técnicas ejecutadas durante las fases ofensivas del laboratorio.

A través de Kibana se pudieron explorar los registros de forma detallada mediante búsquedas KQL, filtros y visualizaciones dinámicas permitiendo analizar eventos concretos en función de distintos criterios como el usuario, la dirección IP, el Event ID, el host de origen o el servicio afectado. Esto permitió reconstruir gran parte de la actividad del atacante dentro del entorno y observar qué evidencias generaba cada técnica en tiempo real.

Este enfoque permitió transformar ELK en un sistema orientado no solo a almacenamiento de logs, sino también a detección y análisis de comportamiento dentro del laboratorio Active Directory, facilitando la evaluación práctica de la detectabilidad de las distintas técnicas utilizadas.

Servicios desplegados en el laboratorio

El laboratorio incluye distintos servicios desplegados que tienen como objetivo simular un entorno corporativo realista y proporcionar una superficie de ataque que nos deje probar la ejecución de diferentes técnicas durante la fase de compromiso.

Estos servicios han sido seleccionados y configurados de tal forma que permiten reproducirse en entornos empresariales incluyendo la interacción entre aplicaciones web, bases de datos y recursos compartidos en el entorno AD. Esta integración permite analizar no solo algunas vulnerabilidades individuales sino también el impacto de la relación entre distintos sistemas dentro de la infraestructura.

Servicio web (IIS)

Se ha desplegado un servicio web interno basado en IIS con el objetivo de simular una aplicación corporativa integrada en el dominio. Este servicio usa mecanismos de autenticación basados en AD permitiendo a los usuarios acceder mediante autenticación integrada, lo que reproduce escenarios reales en los que los servicios web forman parte de la infraestructura corporativa.

El servicio se ejecuta usando una cuenta de servicio dedicada (svc-web), lo que introduce un elemento clave desde el punto de vista de la seguridad. Este tipo de configuración es habitual en entornos reales y permite analizar el comportamiento de la autenticación Kerberos, así como posibles abusos relacionados con el uso de cuentas de servicio como la obtención de tickets o su reutilización.

Esta aplicación mantendrá comunicación con un sistema de base de datos interno generando un flujo de interacción entre servicios que resulta muy relevante desde el punto de vista ofensivo. Esta arquitectura me permite simular escenarios de explotación web, acceso a datos internos y posibles encadenamientos de vulnerabilidades entre distintos componentes del sistema.

Bases de datos (SQL y Maria DB)

Este entorno también cuenta con dos sistemas de base de datos que representan distintos escenarios habituales en infraestructuras corporativas permitiendo ampliar la superficie de ataque y simular diferentes vectores de compromiso.

Por un lado, tenemos un servidor de base de datos integrado en el dominio el cual usa una cuenta asociada y permite la autenticación mediante credenciales del dominio. Este tipo de configuración permite reproducir técnicas relacionadas con el abuso de cuentas de servicio, autenticación Kerberos y acceso a sistemas críticos dentro de la red.

Por otro lado, se ha desplegado un servidor de base de datos en un sistema Linux que da soporte directo al servidor web. Este componente permite simular escenarios de interacción entre aplicaciones y bases de datos, así como analizar posibles vulnerabilidades derivadas de configuraciones inseguras, accesos indebidos o exposición de servicios.

La coexistencia de ambos sistemas permite estudiar distintos tipos de ataques incluyendo acceso mediante credenciales comprometidas, ejecución de comandos a través de servicios de base de datos y movimiento lateral hacia sistemas con mayor privilegio.

Recursos compartidos (SMB)

Como parte del entorno se han configurado recursos compartidos accesibles del dominio con el objetivo de simular escenarios en los que la información interna puede estar expuesta debido a configuraciones inadecuadas o controles de acceso insuficientes al tener exceso de confianza por estar dentro de la red interna.

Estos recursos permiten a los usuarios del dominio acceder a información compartida donde puede haber datos sensibles, documentación interna o configuraciones incorrectas que facilitan el acceso no autorizado.

Desde el punto de vista de seguridad, los recursos SMB constituyen una superficie de ataque muy relevante ya que pueden facilitar tareas de reconocimiento, obtención de información sensible y apoyo en fases posteriores del ataque como el movimiento lateral o escalada de privilegios.

Este tipo de servicios permite analizar patrones de acceso y su visualización en los sistemas de monitorización del laboratorio.

Configuración de seguridad y vulnerabilidades

El laboratorio ha sido diseñado incorporando de forma intencionada diversas configuraciones que reflejan debilidades comunes en entornos corporativos basados en AD. Estas configuraciones permiten reproducir escenarios realistas de ataque y analizar tanto su impacto como su detectabilidad mediante el sistema de monitorización desplegado.

A diferencia de un entorno productivo donde las configuraciones están orientadas a minimizar riesgos, he introducido vulnerabilidades controladas que permiten estudiar el comportamiento de un atacante dentro de la red y su interacción con los distintos sistemas.

Cuentas de servicio y exposición de SPNs

En el entorno se han definido múltiples cuentas de servicio asociadas a distintos sistemas como aplicaciones web y bases de datos. Estas cuentas disponen de ServicePrincipalNames (SPNs) que permiten su identificación dentro del dominio y la autenticación mediante Kerberos.

Este tipo de configuración es habitual en entornos empresariales pero introducen una superficie de ataque relevante. La existencia de SPNs permite la ejecución de técnicas como Kerberoasting en las que el atacante puede solicitar tickets de servicio asociados a estas cuentas y tratarlos posteriormente fuera del sistema para intentar obtener sus credenciales.

Además, el uso de cuentas de servicio con privilegios elevados o configuraciones poco restrictivas incrementan el impacto potencial de un compromiso permitiendo su uso en fases posteriores como movimiento lateral o escalada de privilegios.

Delegación Kerberos

Se ha configurado un escenario de delegación en el equipo DELEG-CLIENT permitiendo que este pueda actuar en nombre de otros usuarios frente a distintos servicios del dominio.

Este tipo de configuración reproduce situaciones reales en las que determinados servicios requieren acceder a recursos en nombre de un usuario autenticado. Sin embargo, una delegación mal configurada puede ser explotada por el atacante para suplantar identidades y acceder a servicios con mayores privilegios.

La presencia de delegación permite analizar técnicas basadas en el abuso de tickets Kerberos y la impersonación de usuarios dentro del dominio.

Permisos delegados y control de acceso

Se han asignado permisos específicos a determinadas cuentas con el objetivo de simular escenarios reales de delegación de funciones dentro de la organización.

En particular la cuenta “attacker” dispone de permisos de lectura sobre los objetos del dominio lo que permite realizar tareas de enumeración avanzada sin necesidad de privilegios avanzados. Este tipo de configuraciones son habituales en entornos corporativos y pueden facilitar la obtención de información crítica por parte de un atacante.

Adicionalmente, la cuenta “Helpdesk” cuenta con privilegios delegados sobre equipos cliente reproduciendo el rol de personal de soporte técnico. Este tipo de cuentas, aunque no son administradores de dominio pueden ser usadas como punto intermedio en procesos de escalada de privilegios si sus permisos no están correctamente controlados.

Configuración insegura de servicios de base de datos

El entorno incluye configuraciones intencionalmente inseguras en los sistemas de base de datos.

En el caso del servidor SQL integrado en el dominio, se ha habilitado la autenticación mixta y se han asignado privilegios elevados a cuentas determinadas. Además, se han activado funcionalidades avanzadas que permiten la ejecución de comandos sobre el sistema.

Estas configuraciones permiten reproducir escenarios en los que un atacante puede abusar de credenciales comprometidas, ejecutar comandos de forma remota o escalar privilegios a través de servicios de base de datos.

Exposición de servicios web y uso de cuentas de servicio

El servicio web desplegado en el laboratorio usa autenticación integrada con AD mediante una cuenta de servicio dedicada.

Este tipo de configuración permite simular escenarios en los que la aplicación web interactúa con el dominio pero también introduce posibles vectores de ataque relacionados con abuso de autenticación Kerberos, reutilización de tickets o acceso a recursos internos a través del servicio.

La interacción entre el servicio web y otros sistemas como la base de datos permite además analizar escenarios de encadenamiento de vulnerabilidades entre distintos componentes del entorno.

Recursos compartidos y exposición de información

Como se ha explicado anteriormente, se han configurado recursos compartidos accesibles dentro del dominio con el objetivo de simular situaciones habituales en entornos corporativos donde la información no se encuentra correctamente protegida.

Estos recursos pueden contener datos sensibles o información interna que puede ser usada por un atacante durante la fase de reconocimiento. La exposición de este tipo de información facilita la identificación de usuarios, credenciales o configuraciones relevantes para fases posteriores del ataque.

Configuraciones inseguras de acceso anónimo (Null Sessions)

Este laboratorio también incluye configuraciones que permiten el acceso anónimo a determinados recursos del sistema, reproduciendo así una de las debilidades clásicas de entornos Windows mal configurados.

Este tipo de configuraciones permite a los usuarios no autenticados obtener información sobre el sistema como usuarios, grupos o recursos compartidos lo que facilita significativamente las tareas de reconocimiento inicial dentro de la red.

Permisos WMI, DCOM y administración remota

Se han otorgado permisos sobre tecnologías como WMI y DCOM a determinadas cuentas del dominio, lo que permite simular escenarios en los que los usuarios con privilegios limitados disponen de capacidades de administración remota.

Este tipo de configuraciones puede ser explotado por un atacante para ejecutar comandos de forma remota, generar actividad dentro del dominio o moverse lateralmente entre sistemas.

Adicionalmente, se ha habilitado el uso de mecanismos de administración remota como WinRM.

Configuraciones de seguridad relajadas

Con el objetivo de facilitar el análisis de las técnicas de ataque se han deshabilitado o relajado determinados mecanismos de seguridad como soluciones antivirus o restricciones adicionales sobre la ejecución de comandos.

Esta decisión permite observar de forma más clara el impacto de cada técnica y su reflejo en los registros del sistema, aunque se aleja de un entorno productivo real.

En conjunto las configuraciones que se han introducido permiten construir un entorno controlado que reproduce de forma realista múltiples vectores de ataque presentes en infraestructuras corporativas. La combinación de estas vulnerabilidades no solo facilita el estudio individual de cada técnica sino también el análisis de su encadenamiento permitiendo evaluar tanto el impacto del compromiso como su visibilidad dentro del sistema de monitorización.

4. Ejecución de ataques

En este apartado describiré la ejecución controlada de un conjunto de técnicas de ataque sobre el entorno AD con el objetivo de simular un escenario real de compromiso progresivo dentro de una red corporativa.

A diferencia de un enfoque simplemente descriptivo, el análisis no se centra únicamente en la ejecución de las técnicas sino en la evaluación de su impacto y un adelanto de la detectabilidad a priori dentro de un entorno monitorizado.

Para esto, el ataque se ha estructurado en fases que reflejan la evolución natural de una intrusión real desde el reconocimiento inicial hasta el compromiso total del dominio. Esta división permite analizar cada etapa de forma independiente identificando las técnicas utilizadas, las debilidades explotadas y los mecanismos de detección asociados.

Cada fase incluirá lo siguiente:

- Contextualización del escenario de ataque.
- Clasificación de las técnicas empleadas.
- Evaluación de las vulnerabilidades asociadas.
- Análisis de detectabilidad basado en las técnicas realizadas.

Este enfoque no solo permitirá comprender como se desarrolla el ataque sino también evaluar en qué medida cada técnica puede ser identificada mediante mecanismos de monitorización basados en logs.

Además, se mostrará que gran parte de las técnicas analizadas reutilizan protocolos y mecanismos nativos de Active Directory, lo que dificultará la diferenciación entre actividad maliciosa y comportamiento normal. Esto introduce la necesidad de adoptar modelos de detección basados en la correlación de eventos y análisis contextual en lugar de depender únicamente de indicadores aislados.

Finalmente, el análisis desarrollado en este apartado servirá como base para la construcción de un modelo estructurado de detectabilidad en el siguiente apartado donde se integran las distintas técnicas, eventos generados y fuentes de datos con el objetivo de evaluar su visibilidad real en un entorno SIEM.

Fase 1 – Reconocimiento de la red interna

Contexto del ataque

En esta fase se asume que el atacante ya dispone de acceso inicial a la red interna mediante la máquina CLIENT2, la cual se encuentra unida al dominio y opera utilizando una cuenta legítima del dominio. Este escenario es representativo de entornos corporativos reales en los que el compromiso inicial no se produce mediante explotación directa de vulnerabilidades externas, sino que se realizar a través de credenciales comprometidas o accesos previos.

A partir de aquí, el objetivo no es la explotación inmediata sino la obtención de información relevante del entorno que nos permita comprender la estructura del dominio, identificar activos críticos y planificar fases posteriores del ataque. Las técnicas empleadas en esta fase utilizan protocolos habituales del dominio, como LDAP, SMB o Kerberos, generando actividad similar a acciones habituales de gestión dentro del dominio.

Adicionalmente, el uso de técnicas como pivoting mediante herramientas como Chisel permite redirigir el tráfico a través de CLIENT2 provocando que todas las acciones ejecutadas desde la máquina atacante, Kali, aparenten originarse desde el equipo legítimo del dominio. Este comportamiento elimina indicadores clásicos de ataque como direcciones IP externas o patrones anómalos de red provocando que las conexiones aparenten originarse desde un equipo interno legítimo del dominio.

Desde el punto de vista de la detección, esta situación introduce un escenario especialmente complejo ya que las acciones de atacante quedan enmascaradas dentro del comportamiento normal de un usuario autenticado. Esto obliga a basar la detección en análisis de comportamiento y análisis contextual de la actividad en lugar de depender de indicadores tradicionales.

Clasificación de la técnica

Elemento	Descripción
Táctica	Reconnaissance/Discovery
Tipo de técnica	Enumeración y recolección de información
Superficie afectada	Active Directory y red interna
Naturaleza	Uso legítimo de servicios del sistema
Riesgo asociado	Exposición de información estructural del dominio

Tabla 1. Clasificación de la técnica de reconocimiento y enumeración en Active Directory

Evaluación de la vulnerabilidad general (Reconocimiento)

Campo	Valor
CWE	CWE-200 – Exposure of sensitive information
CVSS 3.1	5.3 (Medium)
Root Cause	Exceso de visibilidad del dominio y ausencia de restricciones en consultas internas
Impacto	Permite identificar usuario, servicios, equipos y relaciones dentro del dominio
Remediación	Aplicación de controles de acceso, segmentación de red y monitorización de consultas
Referencias	MITRE ATT&CK - Discovery

Tabla 2. Evaluación de la vulnerabilidad asociada a la exposición de información durante la fase de reconocimiento

El reconocimiento interno no constituye una vulnerabilidad critica de forma aislada. Sin embargo, su impacto radica en que permite al atacante reducir la incertidumbre del entorno y obtener información clave para fases posteriores del ataque.

Desde una perspectiva analítica, esta fase introduce un problema fundamental en la detección ya que la mayoría de las acciones realizadas generan señales válidas dentro del sistema, pero carecen de contexto suficiente para ser consideradas maliciosas de forma individual. Esto convierte el análisis de comportamiento en un elemento clave para su identificación.

Pivoting y ocultación del origen del ataque

El uso de túneles SOCKS mediante herramientas como Chisel introduce un mecanismo de evasión que altera la percepción del origen del tráfico. A través de esta técnica las herramientas

ejecutadas desde Kali usan CLIENT2 como punto intermedio de forma que todas las conexiones hacia el dominio parecen originarse desde un sistema legítimo.

Este comportamiento elimina uno de los principales indicadores de compromiso, la procedencia externa del tráfico provocando que las actividades maliciosas del atacante se integren dentro del patrón normal de uso del dominio.

Esto desplaza el problema de detección desde un enfoque basado en red hacia un enfoque basado en endpoint y comportamiento. La identificación del ataque pasa a depender de detectar anomalías en el uso del sistema como la ejecución de procesos, volumen de conexiones o patrones de acceso.

Desde el marco MITRE ATT&CK esta técnica está relacionada con:

- **T1090.001 – Internal Proxy**
- **T1572 – Protocol Tunneling**

En términos de detectabilidad, el pivoting representa una de las técnicas más complejas de identificar en esta fase ya que elimina los indicadores de red tradicionales y obliga a depender de correlación avanzada entre eventos de host y red situando su detectabilidad en un nivel bajo.

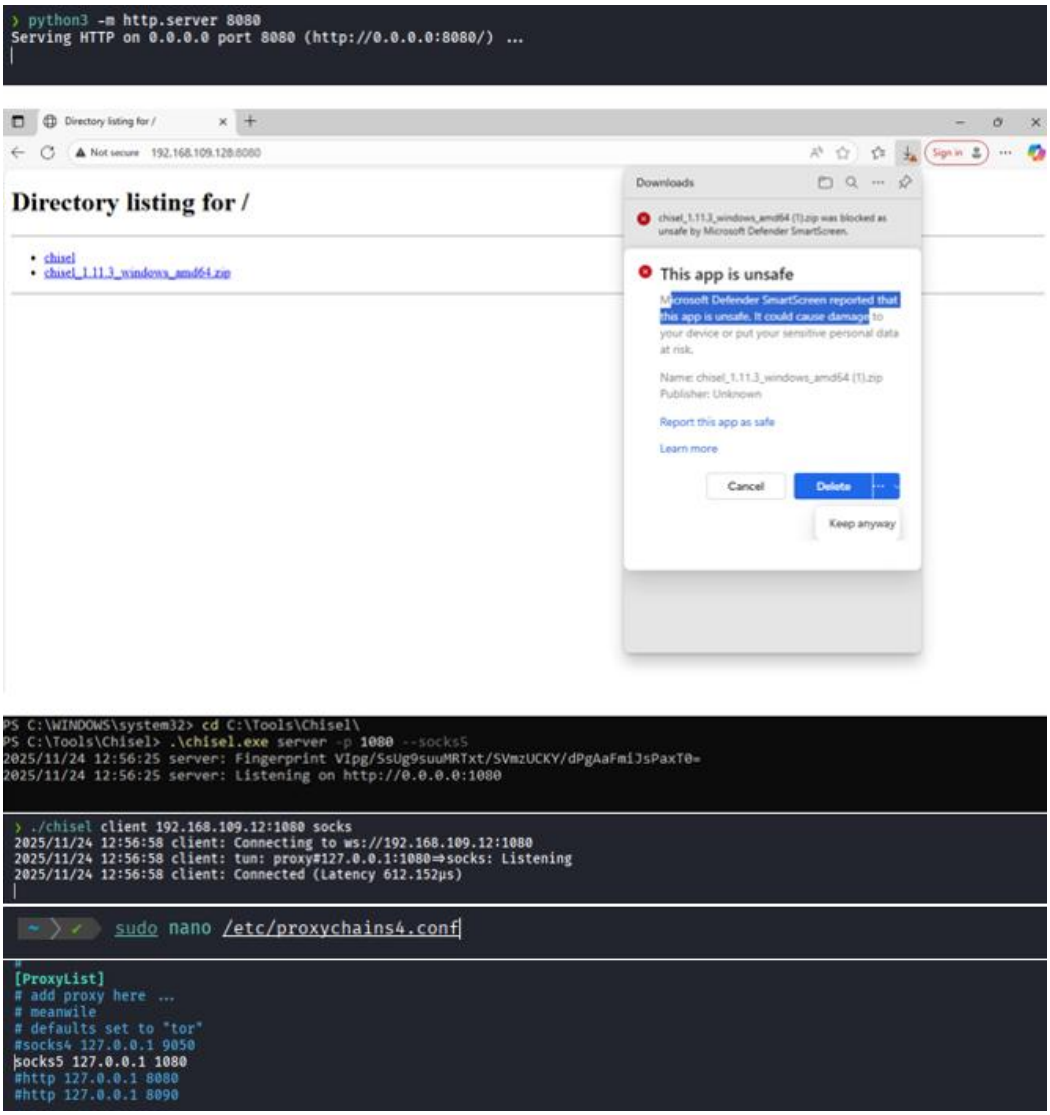

Ilustración 4. Establecimiento de túnel SOCKS mediante Chisel para la realización de pivoting a través de la máquina CLIENT2

La imagen muestra la transferencia de Chisel y creación de un túnel SOCKS usando esta herramienta que me permite redirigir el tráfico desde la máquina atacante hacia la red interna a través de CLIENT2.

Escaneo de red y descubrimiento de servicios

El escaneo de red permite identificar los hosts activos dentro de la red y los servicios expuestos en cada uno de ellos. Esta información resulta fundamental para determinar posibles vectores de ataque.

Desde el punto de vista de la seguridad, la posibilidad de realizar este tipo de escaneos sin restricciones evidencia la ausencia de segmentación de red y controles de acceso internos.

En términos de detectabilidad esta actividad genera múltiples conexiones hacia distintos sistemas lo que produce señales observables. Sin embargo, dichas señales no son intrínsecamente maliciosas ya que pueden corresponder a herramientas de administración o monitorización legítimas.

Por ello su detección efectiva requiere identificar patrones anómalos como:

- Un volumen elevado de conexiones en un intervalo reducido de tiempo.
- Acceso a múltiples sistemas sin justificación operativa.

Desde el marco MITRE ATT&CK:

- **T1046 – Network Service Discovery**

Esto implica que su detectabilidad es media en ausencia de mecanismos de correlación avanzada ya que depende de la interpretación contextual de los eventos generados.

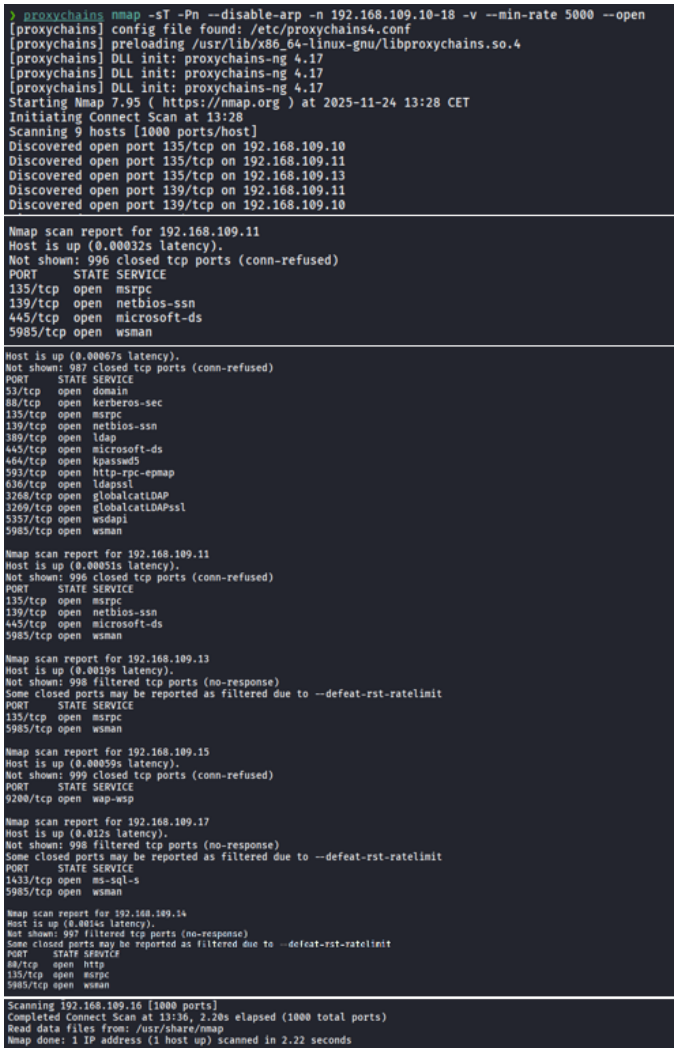

Ilustración 5. Escaneo de red interno mediante Nmap a través de túnel SOCKS

En esta imagen se muestra la ejecución de un escaneo de red usando la herramienta Nmap a través del proxychain creado el cual permite redirigir el tráfico mediante el túnel SOCKS previamente establecido, con lo que se consigue hacer descubrimiento de host y servicios a través de un equipo comprometido dentro del dominio

Como resultado se identifican múltiples servicios expuestos en las diferentes máquinas activas de la red como son SMB (445), RPC (135) o WinRM (5985).

Enumeración de usuarios mediante Kerberos (Kerbrute)

La enumeración de usuarios se realiza mediante el uso de Kerbrute una herramienta que aprovecha el comportamiento del protocolo de Kerberos para distinguir entre cuentas válidas e inválidas.

A diferencia de un ataque de fuerza bruta tradicional, esta técnica no busca obtener credenciales sino validar la existencia de cuentas dentro del dominio lo que la convierte en una fase previa clave para ataques posteriores.

Campo	Valor
CWE	CWE-203 – Observable Discrepancy
CVSS 3.1	6.5 (Medium - High)
Root Cause	Respuestas diferenciadas del servicio Kerberos

Impacto	Enumeración masiva de cuentas válidas
Remediación	Monitorización y detección de patrones anómalos
Referencias	MITRE ATT&CK – T1087.002 (Domain Account Discovery)

Tabla 3. Evaluación de la vulnerabilidad asociada a la enumeración de usuarios mediante Kerberos

Desde el punto de vista de la detección, esta técnica presenta una visibilidad limitada cuando se analiza de forma aislada ya que las solicitudes Kerberos forman parte del comportamiento normal del dominio. Pero, su identificación es posible mediante el análisis del comportamiento, sobre todo a través de:

- Volumen anómalo de solicitudes en corto periodo de tiempo.
- Enumeración secuencial de nombres de usuario.
- Actividad no asociada a procesos interactivos legítimos.

Esto evidencia que la detección no depende de un evento concreto sino de la correlación temporal y contextual de múltiples acciones situando su detectabilidad en un nivel medio cuando se analiza de forma aislada.

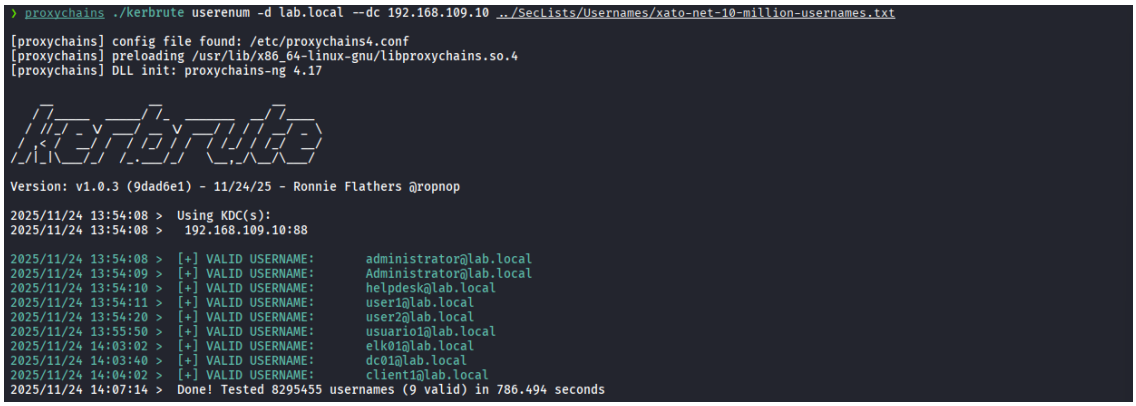

Ilustración 6. Enumeración de usuarios del dominio mediante Kerberos utilizando Kerbrute

La imagen muestra la ejecución de la herramienta Kerbrute a través de proxychains que me permite realizar la enumeración de usuarios validos en el dominio mediante el protocolo Kerberos. Como resultado se ha obtenido un conjunto de usuarios válidos incluyendo cuentas administrativas que pueden ser útiles en fases posteriores del ataque.

Recolección de información estructural BloodHound

El uso de BloodHound junto con SharpHound permite realizar una recolección avanzada de información sobre la estructura del dominio construyendo un modelo completo de relaciones entre usuarios, grupos y permisos.

Campo	**Valor**
CWE	CWE-269 – Improper Privilege Management
CVSS 3.1	7.5 (High)
Root Cause	Exceso de privilegios y complejidad de permisos
Impacto	Identificación de rutas completas de compromiso
Remediación	Revisión de permisos y delegaciones
Referencias	MITRE ATT&CK – Discovery / Privilege Escalation

Tabla 4. Evaluación de la vulnerabilidad asociada al exceso de privilegios y enumeración avanzada de Active Directory

Desde el punto de vista analítico, esta técnica presenta una detectabilidad superior a las otras actividades de reconocimiento debido a la generación de múltiples interacciones con el dominio.

Por otro lado, estas interacciones se realizan mediante protocolos legítimos como LDAP, SMB y Kerberos lo que implica que los eventos generados pueden confundirse con actividad administrativa.

Desde el marco MITRE ATT&CK:

- **T1087.002 - Domain Account Discovery**
- **T1069.002 - Domain Groups Discovery**
- **T1482 - Domain Trust Discovery**

La identificación de la actividad requiere identificar patrones agregados como:

- Alta frecuencia de consultas LDAP.
- Enumeración masiva de objetos del dominio.
- Correlación entre ejecución de procesos y actividad de red.

Por estas razones, la detectabilidad de esta actividad puede considerarse como media/alta especialmente cuando se analizan patrones agregados de actividad.

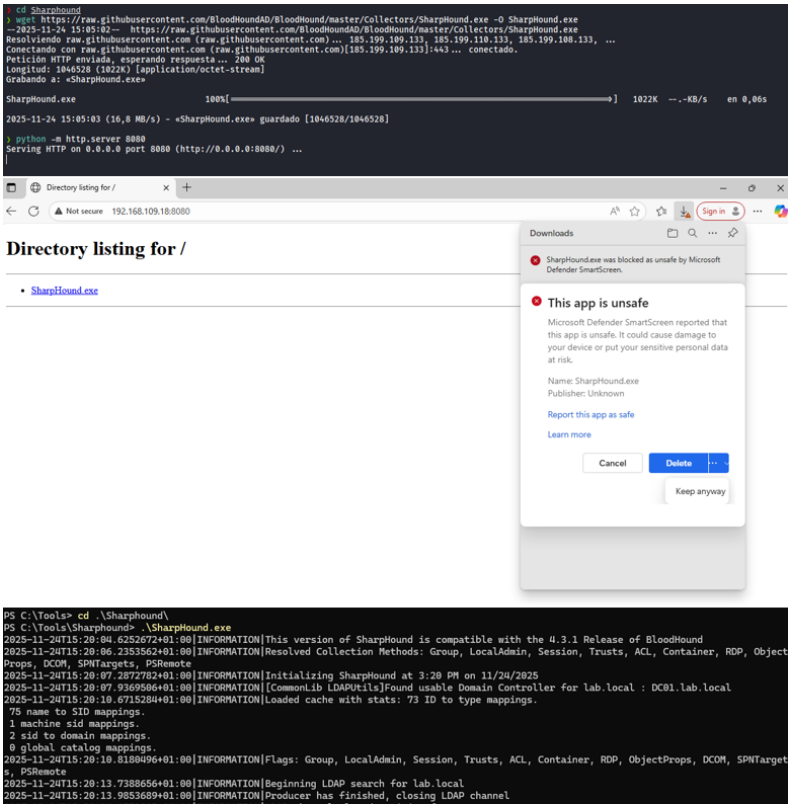

Ilustración 7. Recolección de información del dominio mediante SharpHound

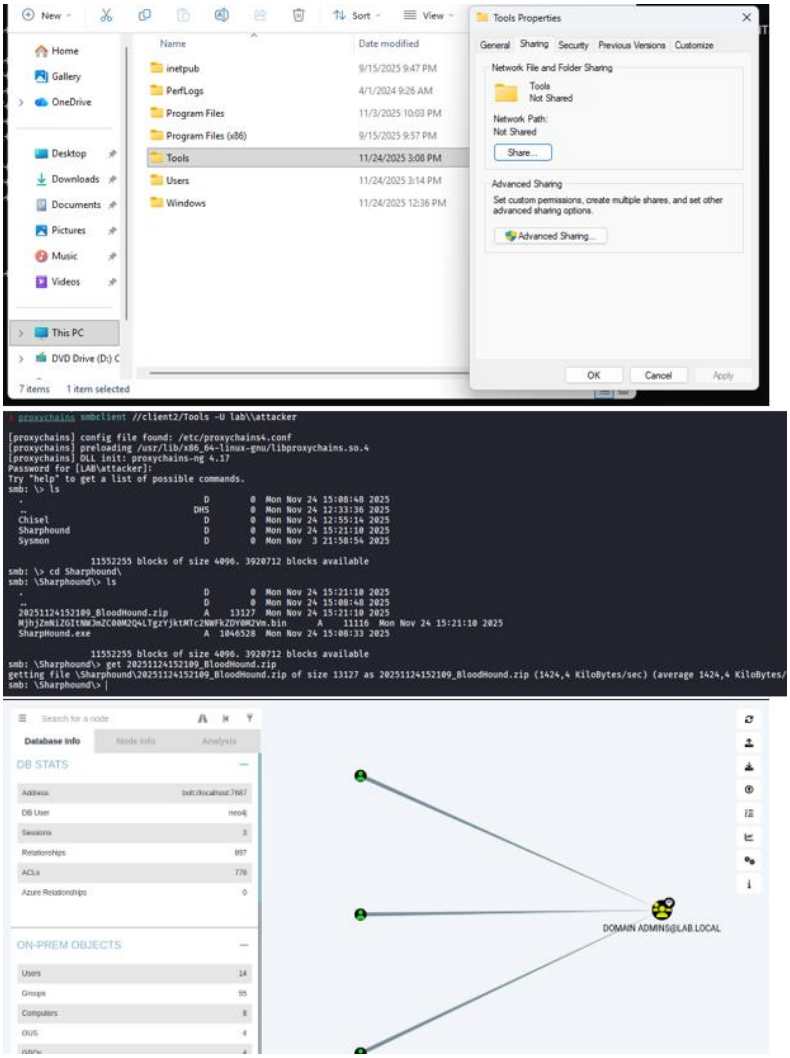

Ilustración 8. Visualización de hallazgos en BloodHound

La imagen muestra el proceso de transferencia de la herramienta SharpHound a la máquina víctima y tras esto la recolección de información del dominio mediante esta, así como la creación de una carpeta compartida que nos permitirá descargar esta información para posteriormente cargarla en BloodHound y visualizar las relaciones entre usuarios, grupos y sistemas dentro del entorno AD.

Conclusión de la fase

La fase de reconocimiento pone de manifiesto que la exposición de información dentro del entrono Active Directory constituye un factor crítico de riesgo.

A través de herramientas legítimas y sin necesidad de privilegios elevados, he sido capaz de obtener una visión detallada del dominio y preparar el terreno para fases posteriores.

Desde el punto de vista de la detección observamos lo siguiente:

- La mayoría de las técnicas generan señales válidas dentro del sistema.
- Los eventos individuales carecen de contexto suficiente para ser considerados maliciosos.
- La detección dependerá de la correlación y análisis de comportamiento.

De forma comparativa el pivoting representa la técnica con menor detectabilidad, mientras que herramientas como BloodHound generan un mayor volumen de eventos, aunque igualmente dependientes de análisis contextual.

Esto evidencia que las técnicas más críticas no son aquellas que generan menos eventos, sino las que sus eventos son indistinguibles de actividad legítima.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Escaneo de red	Conexiones a múltiples hosts	Media	Requiere análisis de volumen y patrón
Kerbrute	Solicitudes Kerberos	Media	Actividad legítima sin correlación
BloodHound	Consultas LDAP/SMB	Media/Alta	Genera patrones sostenidos
Pivoting	Tráfico interno	Baja	Elimina indicador de origen externo

Tabla 5. Evaluación de detectabilidad de técnicas de reconocimiento y enumeración en Active Directory

Esta evaluación refleja que la detectabilidad en esta fase no depende de la existencia de eventos sino de la capacidad de interpretarlos dentro de un contexto. También se observa que ninguna de las técnicas presenta detectabilidad alta de forma aislada, lo que refuerza la necesidad de modelos de detección basados en interpretación conjunta de logs.

Fase 2 – Acceso a recursos compartidos y obtención de credenciales

Contexto del ataque

Tras completar la fase inicial de reconocimiento, el siguiente paso consiste en identificar posibles vectores de acceso derivado de las configuraciones inseguras dentro del entorno. En este caso el objetivo es verificar si existen recursos compartidos accesibles que puedan contener información sensible.

A partir de la información obtenida en la fase anterior, se identificó que la máquina CLIENT1 tiene expuesto un servicio SMB por el puerto 445/TCP, lo que sugiere la posibilidad de existencia de recursos compartidos accesibles dentro del dominio.

Este escenario es representativo de entornos corporativos en los que los recursos compartidos se usan para facilitar el intercambio de información entre usuarios pero que debido a una mala gestión de permisos, puede convertirse en un vector de exposición de información crítica.

Desde el punto de vista ofensivo, esta fase supone un cambio respecto al reconocimiento ya que no solo se busca información estructural del dominio sino datos que permitan avanzar hacia el compromiso de nuevas cuentas.

Clasificación de la técnica

Elemento	Descripción
Táctica	Discovery/Credential Access

Tipo de técnica	Acceso a recursos compartidos y recolección de credenciales
Superficie afectada	Recursos SMB y sistemas del dominio
Naturaleza	Uso legítimo de servicios del sistema
Riesgo asociado	Exposición de credenciales y datos sensibles

Tabla 6. Clasificación de la técnica de acceso a recursos compartidos y obtención de credenciales

Evaluación de la vulnerabilidad (Acceso a recursos compartidos)

Campo	Valor
CWE	CWE-522 –Insufficently Protected Credentials
CVSS 3.1	7.1 (High)
Root Cause	Configuración incorrecta de permisos en recursos compartidos
Impacto	Exposición de información sensible y credenciales en texto plano
Remediación	Restricción de accesos, control de permisos y auditoria de recursos
Referencias	MITRE ATT&CK – Discovery / Credential access

Tabla 7. Evaluación de la vulnerabilidad asociada a la exposición de credenciales en recursos compartidos SMB

El acceso a recursos compartidos mal configurados constituye una de las debilidades más comunes en entornos corporativos. Aunque el uso de SMB es legítimo, una gestión inadecuada de permisos puede provocar la exposición de información crítica.

Desde una perspectiva más analítica, esta fase introduce un cambio relevante respecto la fase anterior ya que las acciones realizadas siguen siendo legítimas pero el impacto potencial es significativamente mayor. Esto puede derivar directamente en el compromiso de credenciales.

Acceso a recursos SMB

Desde la sesión comprometida en CLIENT2 se procedió a enumerar los recursos compartidos disponibles en CLIENT1. Como resultado se identificó un recurso compartido llamado “PublicShare” el cual permitía acceso a usuarios autenticados del dominio e incluso acceso anónimo.

Una vez verificado el acceso, se procedió a la exploración del contenido del recurso identificando múltiples archivos que simulaban documentación interna.

Este tipo de configuración refleja una práctica que es habitual en entornos con baja madurez en seguridad donde los recursos compartidos se usan sin aplicar controles adecuados de acceso ni clasificación de la información.

Desde el punto de vista de la detectabilidad, esta actividad presenta una complejidad similar a la de la fase 1 ya que el acceso a recursos SMB es una acción habitual dentro del dominio. Es por esto por lo que los eventos generados no son intrínsecamente sospechosos requiriendo un análisis contextual para su identificación.

Desde el marco MITRE ATT&CK:

- **T1135 – Network Share Discovery**
- **T1021.002 – SMB/Windows Admin Shares**

Esto implica que su detectabilidad es baja cuando se analiza de forma aislada ya que depende de identificar accesos no habituales o fuera del comportamiento esperado del usuario.

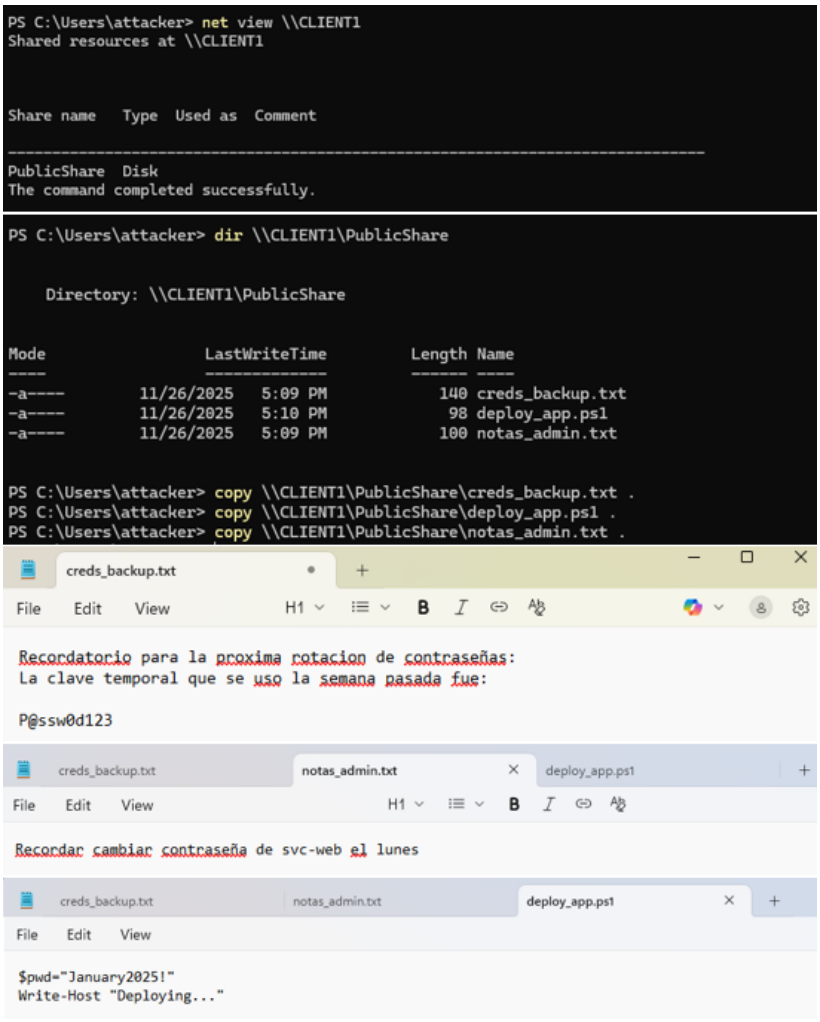

Ilustración 9. Acceso a recurso compartido SMB y obtención de credenciales en texto plano

La imagen muestra el acceso al recurso compartido SMB en la máquina CLIENT1 y la exploración del contenido junto con la obtención de archivos que contienen información sensible como contraseñas reutilizadas y credenciales almacenadas en texto plano que posiblemente pertenezcan a una cuenta del dominio.

Exposición de credenciales en texto plano

Campo	Valor
CWE	CWE-522 –Insufficently Protected Credentials
CVSS 3.1	7.5 (High)
Root Cause	Almacenamiento de credenciales en texto plano
Impacto	Compromiso directo de cuentas
Remediación	Eliminación de credenciales en texto plano y control de accesos
Referencias	MITRE ATT&CK – 1522.001

Tabla 8. Evaluación de la vulnerabilidad asociada al almacenamiento de credenciales en texto plano

Durante la exploración del recurso compartido se identificaron archivos que contenían credenciales almacenadas en texto plano. Este tipo de hallazgo representa una de las

debilidades más críticas dentro de entornos corporativos ya que elimina la necesidad de realizar ataques de fuerza bruta o exploración avanzada.

La presencia de credenciales en texto plano suele estar asociada a malas prácticas operativas como almacenamiento de contraseñas en documentos compartidos, reutilización de credenciales o falta de controles de acceso adecuados.

Desde el punto de vista analítico, esta situación introduce un salto cualitativo en el ataque ya que transforma una fase de descubrimiento en una oportunidad de compromiso directa.

En cuanto a la detectabilidad, este tipo de exposición presenta una visibilidad muy limitada:

- No genera eventos específicos asociados a actividades maliciosas.
- El acceso a los archivos se realiza mediante protocolos legítimos.
- No existe diferencia observable entre acceso legítimo y malicioso.

Por esto, la detectabilidad se considera baja ya que depende completamente del análisis contextual del acceso a la información:

- **T1552.001 – Credentials in files**

Ataque de password spraying

Campo	Valor
CWE	CWE-307 – Improper restriction of excessive authentication attemps
CVSS 3.1	6.8 (Medium/High)
Root Cause	Falta de controles efectivos contra intentos distribuidos
Impacto	Compromiso de cuentas mediante credenciales válidas
Remediación	Detección de patrones de autenticación anómalos
Referencias	MITRE ATT&CK – T1110.003

Tabla 9. Evaluación de la vulnerabilidad asociada a ataques de Password Spraying sobre cuentas del dominio

A partir de las credenciales obtenidas se prepara un ataque de Password Spraying con el objetivo de validar su uso en múltiples cuentas del dominio.

Esta técnica consiste en probar una o pocas contraseñas sobre un conjunto amplio de usuarios, evitando generar bloqueos de cuenta y reduciendo la probabilidad de detección.

Para ello, se usó la información recopilada en la fase de reconocimiento para construir una lista de usuarios válidos del dominio.

Desde el punto de vista analítico esta técnica representa una evolución respecto a ataques de fuerza bruta tradicionales ya que prioriza el sigilo frente al volumen de los intentos.

En términos de detectabilidad, el Password Spraying presenta una complejidad elevada debido a:

- Genera un número reducido de intentos por usuario.
- Imita errores de autenticación legítimos.
- Evita mecanismos de bloqueo de cuenta.

La detección necesita identificar patrones distribuidos para ser efectiva, como:

- Intentos fallidos en múltiples cuentas con una misma contraseña.
- Actividad de autenticación anómala en un corto periodo de tiempo.

Desde el marco MITRE ATT&CK:

- **T1110.003 – Password Spraying**

Esto sitúa su detectabilidad en un nivel medio-alta cuando se analiza de forma aislada dependiendo en gran medida de los mecanismos de correlación de eventos.

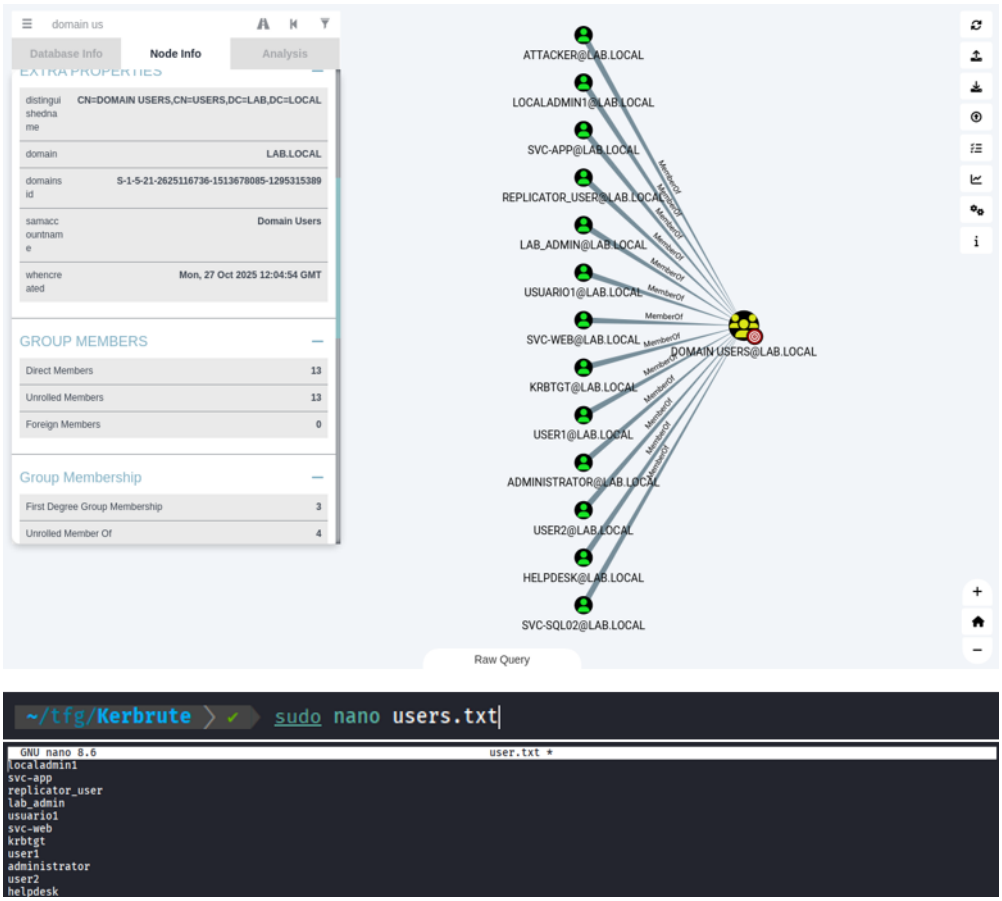

Ilustración 10. Identificación de usuarios del dominio y preparación del conjunto de objetivos

La imagen muestra la identificación de usuarios validos del dominio mediante herramientas de enumeración y la construcción de una lista de cuentas objetivo válidas que será usadas para el password spraying.

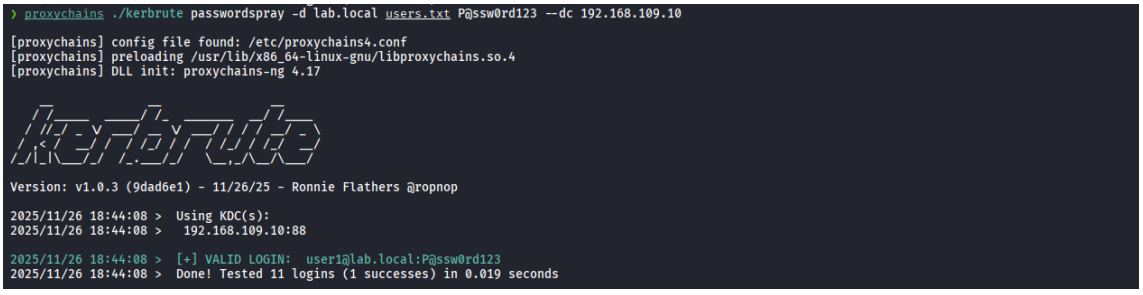

Ilustración 11. Ejecución de ataque de Password Spraying y obtención de credenciales válidas

Esta imagen muestra la ejecución de un ataque de password spraying mediante Kerbrute aplicando la contraseña común encontrada previamente sobre la lista de usuarios válidos creada. Como resultado tenemos una coincidencia en el usuario “user1” que confirma la existencia de credenciales débiles o reutilizadas en el entorno.

Compromiso de cuenta de usuario

Como resultado del ataque de Password Spraying se logró identificar que una de las credenciales obtenidas correspondía a la cuenta "user1" permitiendo su compromiso.

Este hecho marcará el inicio de la siguiente fase en el que se pasa de una posición de acceso limitado a disponer de credenciales válidas de otro usuario del dominio.

Desde el punto de vista analítico, representa un cambio crítico en el ataque ya que:

- Se produce una expansión del acceso dentro del dominio.
- Se incrementa la superficie de ataque disponible.
- Se habilitan nuevas posibilidades de movimiento lateral.

En términos de detectabilidad este tipo de compromiso puede pasar desapercibido si no se analizan anomalías en el comportamiento de inicio de sesión ya que el uso de credenciales válidas no genera alertas por sí mismo.

Conclusión de la fase

La fase de acceso a recursos compartidos y obtención de credenciales pone en manifiesto que la exposición de información sensible constituye uno de los vectores de ataque más críticos en entornos AD.

A través de configuraciones inseguras y malas prácticas operativas se ha podido obtener credenciales sin necesidad de realizar técnicas complejas.

Desde el punto de vista de la detección hemos observado que:

- Las acciones realizadas usan servicios legítimos del sistema.
- No existen claramente diferenciadores de actividad maliciosa.
- La detección esta sujeta a un análisis contextual y correlación.

Esto evidencia que las fases más críticas del ataque no siempre implican técnicas avanzadas sino el aprovechamiento de debilidades básicas en la gestión de la información.

Se observa que el uso de credenciales válidas reduce significativamente la detectabilidad del ataque ya que elimina la necesidad de comportamientos anómalos evidentes dificultando su identificación sin mecanismos avanzados de correlación.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Acceso SMB	Acceso a recursos compartidos	Media	Actividad legítima sin contexto
Exposición de credenciales	Acceso a archivos	Baja	No genera eventos específicos
Password Spraying	Intentos de autenticación	Media/Baja	Distribuido y difícil de correlacionar
Uso de credenciales válidas	Inicio de sesión	Baja	Comportamiento indistinguible del legítimo

Tabla 10. Evaluación de detectabilidad de técnicas de acceso a recursos compartidos y abuso de credenciales

Esta evaluación refleja que la detectabilidad en esta fase se ve reducida tanto por el uso de credenciales válidas como de servicios legítimos, lo que dificulta la diferenciación entre actividad maliciosa y del comportamiento legítimo dentro del entorno.

Fase 3 – Abuso de Kerberos y delegación

Contexto del ataque

Tras el compromiso inicial de la cuenta "user1" en la fase 2 ahora disponemos de acceso legítimo a la Workstation CLIENT1. En este punto, el objetivo ha evolucionado desde la obtención de credenciales hacia la explotación mediante técnicas específicas del protocolo Kerberos.

Esta fase se centra en el abuso de funcionalidades legítimas de autenticación en AD especialmente aquellas relacionadas con la gestión de tickets Kerberos y cuentas de servicio. A diferencia de fases anteriores donde se ha explotado configuraciones inseguras, ahora se aprovecha del propio diseño del sistema.

Desde el punto de vista operativo, nos encontramos en un contexto autenticado lo que nos permite interactuar directamente con el KDC y solicitar tickets Kerberos asociados a distintos servicios del dominio.

Este escenario es especialmente crítico ya que muchas de estas operaciones forman parte del funcionamiento normal del sistema, dificultando su detección sin mecanismos avanzados de análisis.

Clasificación de la técnica

Elemento	Descripción
Táctica	Credential Access/Privilege Escalation/Lateral Movement
Tipo de técnica	Abuso de Kerberos y delegación
Superficie afectada	AD y cuentas de servicio
Naturaleza	Uso legítimo del protocolo Kerberos
Riesgo asociado	Compromiso de cuentas de servicio y suplantación de identidades

Tabla 11. Clasificación de la técnica de abuso de Kerberos y delegación en Active Directory

Evaluación de vulnerabilidades (Kerberoasting)

Campo	Valor
CWE	CWE-522 – Insufficiently protected credentials
CVSS 3.1	7.5 (High)
Root Cause	Uso de cifrados débiles (RC4) en tickets Kerberos
Impacto	Obtención de credenciales de cuentas de servicio
Remediación	Uso de AES, rotación de credenciales y cuentas gestionadas
Referencias	MITRE ATT&CK – T1558.003 (Kerberoasting)

Tabla 12. Evaluación de la vulnerabilidad asociada al abuso de Kerberos mediante técnicas de Kerberoasting

El kerberoasting es una técnica que permite solicitar tickets de servicio TGS asociados a cuentas con SPN y posteriormente intentar descifrarlos offline. Este comportamiento es posible debido a que los tickets están cifrados con la clave de la cuenta de servicio.

Desde la perspectiva analítica, esta técnica no explota una vulnerabilidad tradicional sino una debilidad inherente del diseño de Kerberos cuando se usan configuraciones inseguras.

Enumeración de SPNs en el dominio

El primer paso consiste en identificar los servicios del dominio que disponen de SPNs o Service Principal Names, ya que estos representan objetivos potenciales para Kerberoasting.

Para ello se emplean herramientas como Rubeus que permiten interactuar directamente con Kerberos desde un entorno Windows autenticado.

Esta enumeración me permite identificar:

- Servicios disponibles en el dominio.
- Cuentas de servicio asociadas.
- Posibles objetivos para extracción de tickets.

Desde el marco MITRE ATT&CK:

- **T1558.003 – Kerberoasting**

En términos de detectabilidad es media/alta cuando se analiza de forma aislada dependiendo del volumen de solicitudes, frecuencia anómala y patrones no habituales de acceso.

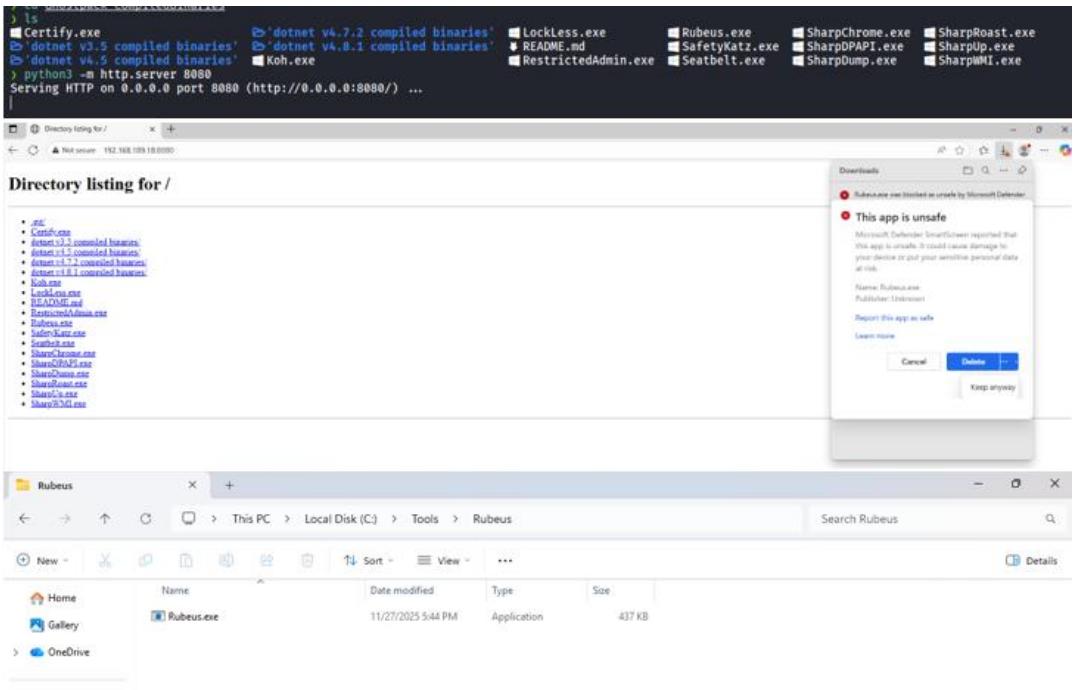

Ilustración 12. Transferencia de herramientas al sistema comprometido mediante servidor HTTP

Esta imagen muestra la transferencia de la herramienta Rubeus desde la máquina atacante hacia el sistema comprometido mediante un servidor HTTP temporal montado en Python. Esta herramienta me permite interactuar con Kerberos. Desde la máquina objetivo se descarga mediante el navegador visitando el HTTP montado por lo que no hace falta el uso de herramientas complejas desde la parte de la víctima.

Ilustración 13. Ejecución de Kerberoasting mediante Rubeus y obtención de hashes de cuentas de servicio

En esta imagen se muestra la ejecución de la herramienta Rubeus para realizar un ataque de Kerberoasting permitiendo la obtención de tickets de servicio TGS asociado a cuentas con SPN en el dominio

Como resultado, identificamos múltiples cuentas y se obtienen los respectivos hashes de las credenciales de estas cuentas los cuales descifraremos offline.

Obtención y crackeo de credenciales (svc-web)

Tras obtener los hashes cifrados vimos que se trataba de un cifrado RC4-HMAC (etype23), el cual es vulnerable a ataques de fuerza bruta offline. Mediante herramientas como John the Ripper se logró recuperar la contraseña en texto claro de la primera cuenta, “svc-web”.

Desde el punto de vista analítico esta técnica presenta una característica clave:

- El proceso de descifrado ocurre fuera del entorno monitorizado.

Esto implica lo siguiente:

- No se generan eventos adicionales en el dominio.
- La actividad es prácticamente invisible tras la obtención del ticket.

En términos de detectabilidad se traduce a:

- La solicitud del ticket puede ser observable.
- El crackeo es completamente invisible.

Por esto, la detectabilidad global puede considerarse media/baja.

Ilustración 14. Descifrado offline de credenciales de cuenta de servicio

La imagen muestra como tras la obtención del TGS asociado a “svc-web” mediante Kerberoasting, se almacenó de forma offline y se usó herramientas de cracking de contraseñas como John the Ripper. Tras esto se consiguió recuperar la contraseña de la cuenta de servicio en texto plano usando una wordlist de la seclist.

Acceso a recursos mediante cuenta comprometida

Una vez comprometida la cuenta “svc-web”, se usó para autenticarse en la máquina DELEG-CLIENT mediante SMB. Durante esta fase se identificó un recurso compartido llamado “WebRoot” el cual contenía archivos de configuración asociados al servidor web.

Este tipo de archivos suele incluir contenido como:

- Credenciales de conexión a bases de datos.
- Cadenas de conexión.
- Información sensible de la aplicación.

Desde un punto de vista analítico, este paso refleja un patrón común en entornos reales (compromiso de una cuenta > acceso a recursos > obtención de más credenciales).

En términos de detectabilidad:

- El acceso a SMB es legítimo.
- Se realiza con credenciales válidas.
- No genera eventos claramente diferenciadores.

Por esto su detectabilidad es baja

Ilustración 15. Validación de credenciales mediante acceso SMB con cuenta comprometida

En la imagen se muestra la validación de las credenciales obtenidas previamente mediante la herramienta de crackmapexec confirmando su validez frente al servicio SMB del Workstation DELEG-CLIENT.

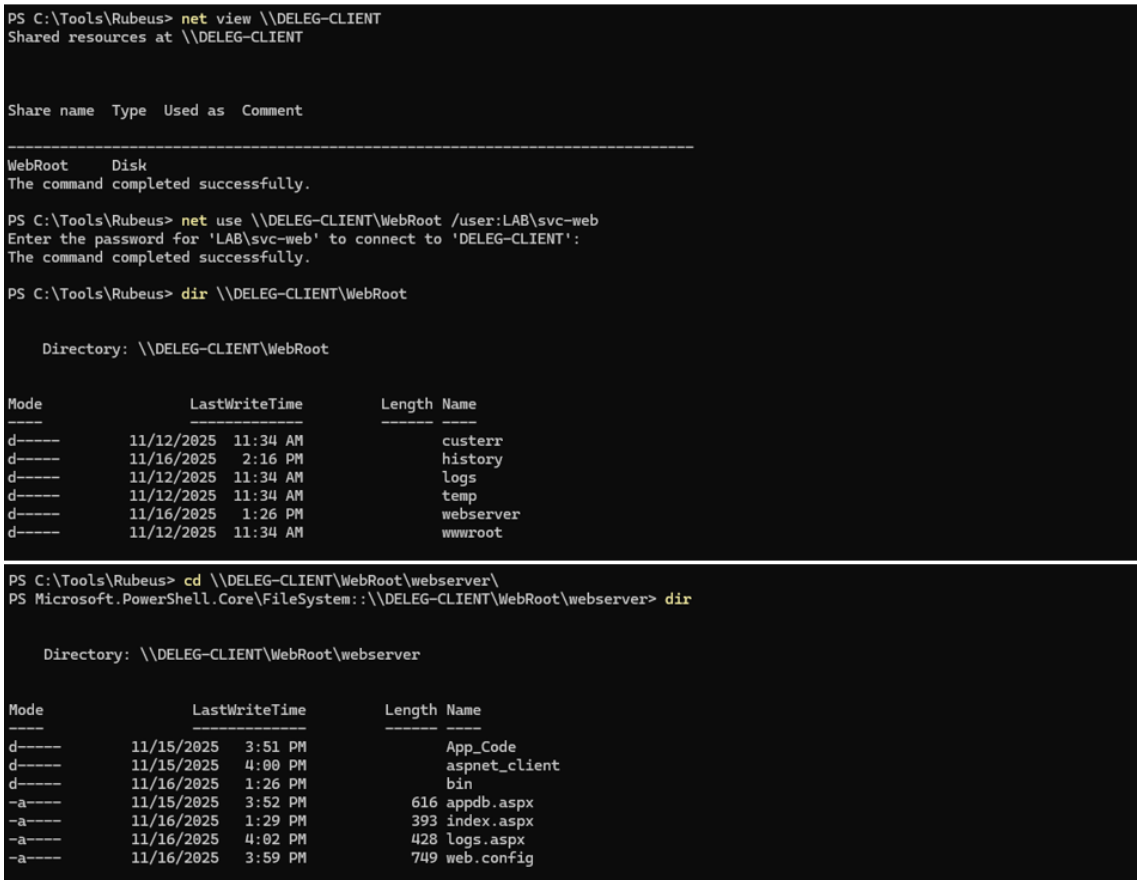

Ilustración 16. Acceso a recurso compartido SMB mediante credenciales válidas

Aquí se muestra el acceso al recurso compartido “WebRoot” en el sistema DELEG-CLIENT usando la cuenta comprometida “svc-web” y la exploración de su contenido

Una vez autenticado podemos navegar por la estructura de directorios del sistema accediendo a componentes de la aplicación web y archivos asociados.

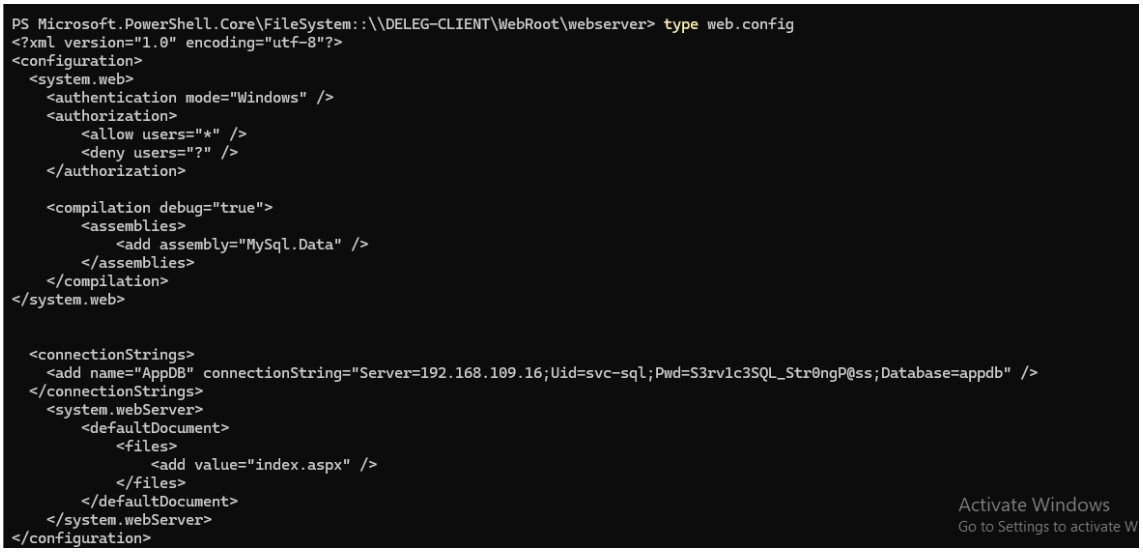

Ilustración 17. Identificación de credenciales en archivo de configuración de aplicación web

Por último, se muestra la visualización del archivo web.config en el cual se identifican credenciales de acceso a base de datos almacenadas en texto claro. Este tipo de configuración representa una debilidad critica ya que permite al atacante obtener nuevas credenciales sin necesidad de realizar ataques adicionales.

Abuso de delegación Kerberos (S4U)

Campo	Valor
CWE	CWE-269 – Improper privilege management
CVSS 3.1	8.2 (High)
Root Cause	Configuración insegura de delegación Kerberos
Impacto	Suplantación de identidades sin conocer credenciales
Remediación	Restricción de delegación y uso de Kerberos constrained delegation
Referencias	MITRE ATT&CK – T1550.003 (Pass-The-Ticket)

Tabla 13. Evaluación de la vulnerabilidad asociada al abuso de delegación Kerberos y suplantación de identidades

Tras comprometer la cuenta svc-web se identificó que esta cuenta disponía de permisos de delegación, lo que permitió abusar del mecanismo S4U2Self. Esto permite solicitar un ticket en nombre de otro usuario sin necesidad de conocer la contraseña.

Posteriormente, este ticket fue usado para autenticarse contra DELEG-CLIENT como “user2” y poder movernos lateralmente.

Desde el punto de vista analítico, esta técnica representa un punto crítico del ataque ya que permite:

- Escalada de privilegios.
- Movimiento lateral.
- No requiere interacción del usuario suplantado.

Desde el marco MITRE ATT&CK:

- **T1550 – Use Alternate Authentication Material**
- **T1134 – Access Token Manipulation**

En términos de detectabilidad:

- Las solicitudes de tickets son legítimas.
- No hay uso de credenciales robadas directamente.
- La actividad puede parecer administrativa.

Por esto, su detectabilidad puede considerarse baja en ausencia de correlación avanzada.

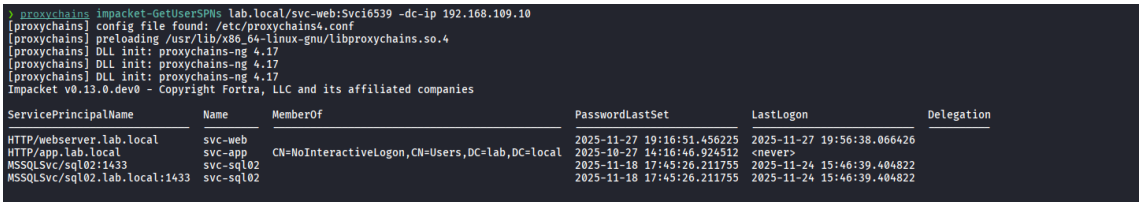

Ilustración 18. Identificación de cuentas con delegación Kerberos habilitada

La imagen muestra la enumeración de cuentas del dominio con delegación Kerberos configurada identificando servicios que puedan ser usados para suplantar identidades dentro del entorno. Podemos observar que la cuenta “svc-web” dispone de permisos de delegación sobre determinados servicios lo que la convierte en un objetivo crítico para el atacante.

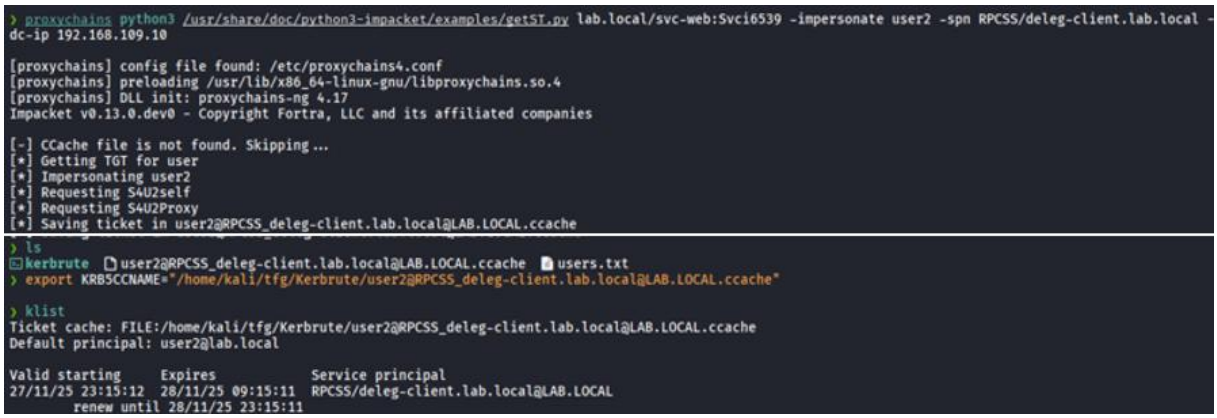

Ilustración 19. Abuso de delegación Kerberos mediante generación de ticket impersonado

En esta imagen se muestra el uso de la herramienta getST para abusar de la delegación Kerberos permitiendo la suplantación de la identidad de otro usuario del dominio. Mediante esta técnica solicitó un ticket de servicio en nombre de otro usuario, en este caso “user2”, usando las credenciales de la cuenta comprometida “svc-web”.

Ilustración 20. Acceso remoto a sistema mediante ticket Kerberos impersonado

Por último, se muestra el uso del ticket Kerberos previamente generado para acceder al sistema DELEG-CLIENT mediante autenticación sin contraseña. Este acceso confirma que la suplantación de identidad ha sido exitosa permitiéndome operar con privilegios del usuario impersonado.

Conclusión de la fase

La fase de abuso de Kerberos pone de manifiesto que el propio diseño del sistema puede ser usado como vector de ataque cuando se combina con configuraciones inseguras.

A diferencia de fases anteriores en las que se explotaban errores operativos en esta fase se aprovechan funcionalidades legítimas del sistema para escalar privilegios y suplantar identidades

Desde el punto de vista de detección se observa que:

- Las acciones realizadas son completamente legítimas.
- Muchas de las actividades generan eventos válidos.
- Parte del ataque ocurre fuera del entorno monitorizado.

Esto evidencia que las técnicas más avanzadas no necesariamente generan más ruido, sino que se integran mejor dentro del comportamiento normal del sistema.

Se observa que el uso de mecanismos como Kerberos reduce significativamente la detectabilidad del ataque al permitir operaciones complejas sin necesidad de generar comportamientos anómalos evidentes.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Enumeración SPNs	Solicitudes kerberos	Media	Actividad legítima dependiente del volumen
Kerberoasting	Solicitudes TGS	Media/Baja	Crackeo offline no detectable
Uso de svc-web	Autenticación SMB	Baja	Uso de credenciales válidas
Abuso de delegación	Solicitud de tickets	Baja	Operaciones legítimas del sistema

Tabla 14. Evaluación de detectabilidad de técnicas de abuso de Kerberos y delegación en Active Directory

Esta evaluación refleja que la detectabilidad en esta fase se ve reducida por el uso de mecanismos internos de autenticación lo que dificulta la identificación de actividad maliciosa sin correlación avanzada.

Se observa que ninguna de las técnicas analizadas presenta detectabilidad alta de forma aislada reforzando la necesidad de modelos de detección basados en comportamiento y trazabilidad de acciones dentro del dominio.

Fase 4 – Acceso y explotación de servicios de base de datos

Contexto del ataque

Tras el abuso de mecanismos Kerberos y la obtención de múltiples credenciales en la fase anterior, ahora dispongo de acceso privilegiado a distintos recursos del dominio. En este punto el objetivo será la explotación de servicios críticos concretamente los relacionados con bases de datos corporativas.

En entornos reales los sistemas de base de datos representan activos de alto valor ya que almacenan información sensible y suelen operar mediante cuentas de servicio con privilegios elevados. Esto los convierte en un objetivo prioritario dentro de fases avanzadas del ataque.

En la red interna se encontraron dos sistemas de bases de datos relevantes:

- SQL01 con MariaDB asociado a la aplicación web.
- SQL02 un servidor SQL integrado en el dominio.

El objetivo de esta fase será validar el acceso a estos servicios, comprometer cuentas asociadas y en última instancia obtener capacidad de ejecución remota de código.

Clasificación de la técnica

Elemento	Descripción
Táctica	Credential Access/Lateral Movement/Execution
Tipo de técnica	Abuso de cuentas de servicio y explotación
Superficie afectada	Servidores SQL y servicios de base de datos
Naturaleza	Uso legítimo de credenciales y funcionalidades del sistema
Riesgo asociado	Acceso a información crítica y ejecución remota de comandos

Tabla 15. Clasificación de la técnica de abuso de cuentas de servicio y explotación de servicios SQL

Acceso a la base de datos SQL01

Una vez obtenida las credenciales de la cuenta “user2”, el siguiente paso consistió en intentar establecer conexión con la base de datos SQL01 asociada al servidor web corporativo y basada en MariaDB con el objetivo de comprobar su accesibilidad y analizar el contenido almacenado.

La conexión se realizó usando credenciales válidas del dominio permitiendo acceso directo al motor de base de datos sin necesidad de explotación adicional. Desde el punto de vista operativo este escenario es muy relevante ya que se ha podido reutilizar credenciales para acceder a uno de los activos más sensibles de la infraestructura.

Una vez autenticado, se procedió a enumerar las bases de datos disponibles mediante comandos SQL identificando la base de datos “appdb” asociada a la aplicación web desplegada en el entorno. Posterior a esto, se analizaron las tablas presentes observando las estructuras relacionadas con usuarios (users) y registros de actividad de la aplicación (applogs).

Desde el punto de vista analítico, este paso representa una transición relevante en el ataque:

- Pasamos a comprometer directamente la capa de aplicación y datos.
- Usamos credenciales válidas para acceder a información sensible sin generar actividad claramente anómala.

En términos de detectabilidad, esta actividad presenta una complejidad elevada debido a que:

- El acceso se realiza mediante credenciales válidas.
- Las consultas SQL ejecutadas son legítimas.
- No existen indicadores claramente diferenciadores de actividad maliciosa.

Esto implica que la detección requiere principalmente del análisis contextual. Desde el marco MITRE ATT&CK:

- **T1078 – Valid Accounts**
- **T1213 – Data from Information Repositories**

Ilustración 21. Acceso al servidor SQL01 y enumeración de bases de datos mediante credenciales válidas

La imagen muestra la exploración de la base de datos “appdb” en el servidor SQL01 mediante credenciales válidas previamente comprometidas. Durante la enumeración de las tablas identificamos dos, “users” la cual almacena credenciales de usuarios y “app_logs” que registra la actividad del servidor web.

Se accedió vía Shell mediante el uso de proxychains junto con la herramienta de imapcket wmiexec que nos permitió loggearnos usando el ticket Kerberos anteriormente obtenido y tras esto nos conectamos mediante el uso de mariadb con las credenciales obtenidas de la otra base de datos del usuario svc-sql que encontramos en el archivo de configuración web.config en la fase anterior.

Exposición de credenciales en la base de datos SQL01

Durante la exploración de la base de datos “appdb”, se identificó la tabla “users” la cual almacenaba credenciales de usuarios en texto plano. Entre los datos recuperados se encontraban nombres de usuario, contraseñas y otra información asociada a cuentas de la aplicación.

La presencia de credenciales sin mecanismos de protección adecuados representa una debilidad muy crítica dentro de entornos corporativos ya que elimina la necesidad de realizar ataques complejos de fuerza bruta o explotación avanzada.

Campo	Valor
CWE	CWE-522 – Insufficiently Protected Credentials
CVSS 3.1	7.5 (High)
Root Cause	Almacenamiento inseguro de credenciales
Impacto	Compromiso adicional de cuentas
Remediación	Uso de cifrados fuertes y gestión segura de cuentas
Referencias	MITRE ATT&CK – T1552 (Unsecured Credentials)

Tabla 16. Evaluación de la vulnerabilidad asociada al almacenamiento inseguro de credenciales en servicios y bases de datos

Desde el punto de vista analítico, esta refleja una debilidad habitual en aplicaciones corporativas desarrolladas sin criterios adecuados de seguridad donde las credenciales son almacenadas directamente en bases de datos sin aplicar técnicas de protección como hashing o cifrado.

Adicionalmente, este tipo de exposición incrementa el impacto del ataque ya que no solo se compromete el sistema actual, sino que se obtiene información potencialmente reutilizable en otros servicios debido a prácticas comunes de reutilización de contraseñas.

En términos de detectabilidad esta actividad presenta una debilidad muy limitada:

- El acceso a las bases de datos se realiza mediante credenciales válidas.
- Las consultas SQL ejecutadas son legítimas.
- La lectura de información no genera eventos claramente maliciosos.
- No existe diferenciación observable entre acceso administrativo y acceso malicioso.

Es por esto por lo que su detectabilidad puede considerarse baja ya que la identificación dependerá completamente del análisis contextual de las consultas realizadas y del comportamiento del usuario autenticado.

Desde el marco MITRE ATT&CK:

- **T1552 – Unsecured Credentials**

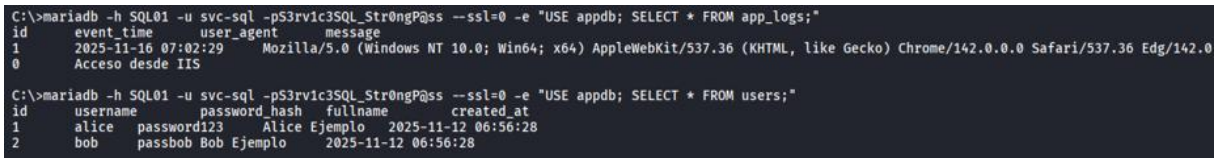

Ilustración 22. Exposición de credenciales en texto plano dentro de la base de datos SQL01

Esta imagen muestra la exposición de información sensible almacenada en las tablas de la aplicación web corporativa. Durante el análisis de la tabla “users” se localizaron varias credenciales de la aplicación. Adicionalmente, se identificaron registros de actividad en la tabla “app_logs” permitiendo observar información relacionada con el uso de la aplicación y actividad de los usuarios.

Evaluación de la vulnerabilidad (Kerberoasting sobre svc-sql02)

Campo	Valor
CWE	CWE-522 – Insufficiently Protected Credentials
CVSS 3.1	7.5 (High)
Root Cause	Uso de cifrado débil en tickets Kerberos
Impacto	Compromiso de cuentas de servicio criticas
Remediación	Uso de cifrados fuertes y gestión segura de cuentas
Referencias	MITRE ATT&CK – T1558.003 (Kerberoasting)

Tabla 17. Evaluación de la vulnerabilidad asociada al abuso de Kerberos sobre cuentas de servicio críticas mediante Kerberoasting

En la fase anterior obtuvimos los tickets Kerberos con el objetivo de obtener el TGS asociado a cuentas de servicio con SPNs, en este caso usaremos el hash obtenido previamente de la cuenta svc-sql02.

Esta técnica mantiene las mismas características que el Kerberoasting de la fase previa, pero con la diferencia de que el impacto es mayor ya que se compromete una cuenta de servicio asociada a un servicio crítico, como es la base de datos.

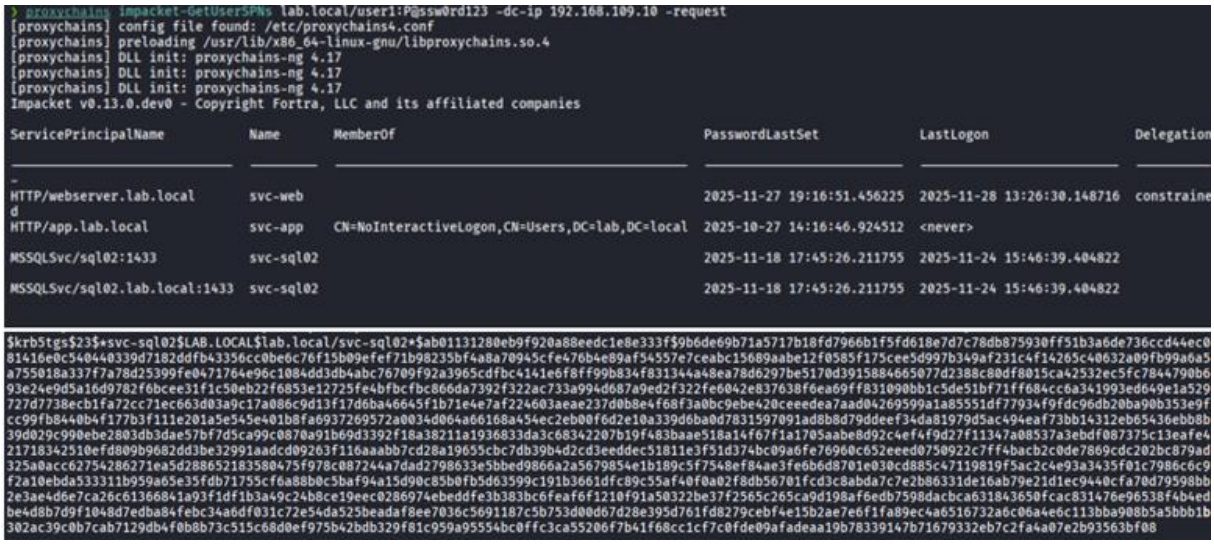

Ilustración 23. Obtención y descifrado offline del ticket Kerberos asociado a la cuenta svc-sql02

En esta imagen se muestra la ejecución del ataque Kerberoasting al igual que en la fase anterior pero ahora centrándonos en la cuenta svc-sql02 que tiene un SPN asociado al servidor SQL.

Obtención de credenciales de svc-sql02

Una vez obtenido el ticket Kerberos se procede al descifrado offline recuperando la contraseña en texto plano de la cuenta svc-sql02.

Este proceso se realiza fuera del entorno monitorizado, lo que implica que:

- No se generan eventos adicionales en el dominio.
- No puede ser detectado directamente.

Desde el punto de vista de la detectabilidad como se vio en la fase previa:

- La solicitud del ticket puede ser observable.
- El proceso de crackeo es completamente invisible.

Por esto, su detectabilidad global se mantiene en medio/bajo.

Ilustración 24. Descifrado offline del ticket Kerberos asociado a la cuenta svc-sql02

Aquí se muestra como tras la obtención del ticket TGS se procede al descifrado offline del hash obtenido usando herramientas de cracking como John the Ripper. Como resultado se obtiene la contraseña en texto plano asociada a la cuenta svc-sql02.

Acceso al servidor SQL02

Con las credenciales obtenidas se estableció conexión con el servidor SQL02 desde CLIENT1 usando una aplicación cliente de base de datos que venía preinstalada en el sistema. Esta autenticación fue exitosa y permitió:

- Acceso al motor de base de datos.
- Visualización del contenido almacenado.
- Validación de permisos asociados a la cuenta.

Desde el punto de vista analítico, este paso representa un patrón crítico en ataques reales en el que la reutilización de credenciales de servicio permite acceso a sistemas internos.

En términos de detectabilidad:

- El acceso se realiza con credenciales válidas.
- No requiere explotación de vulnerabilidades.
- Puede confundirse con actividad legítima

Por ello su detectabilidad es baja. Desde el marco MITRE ATT&CK:

- **T1078.002 – Domain Accounts**

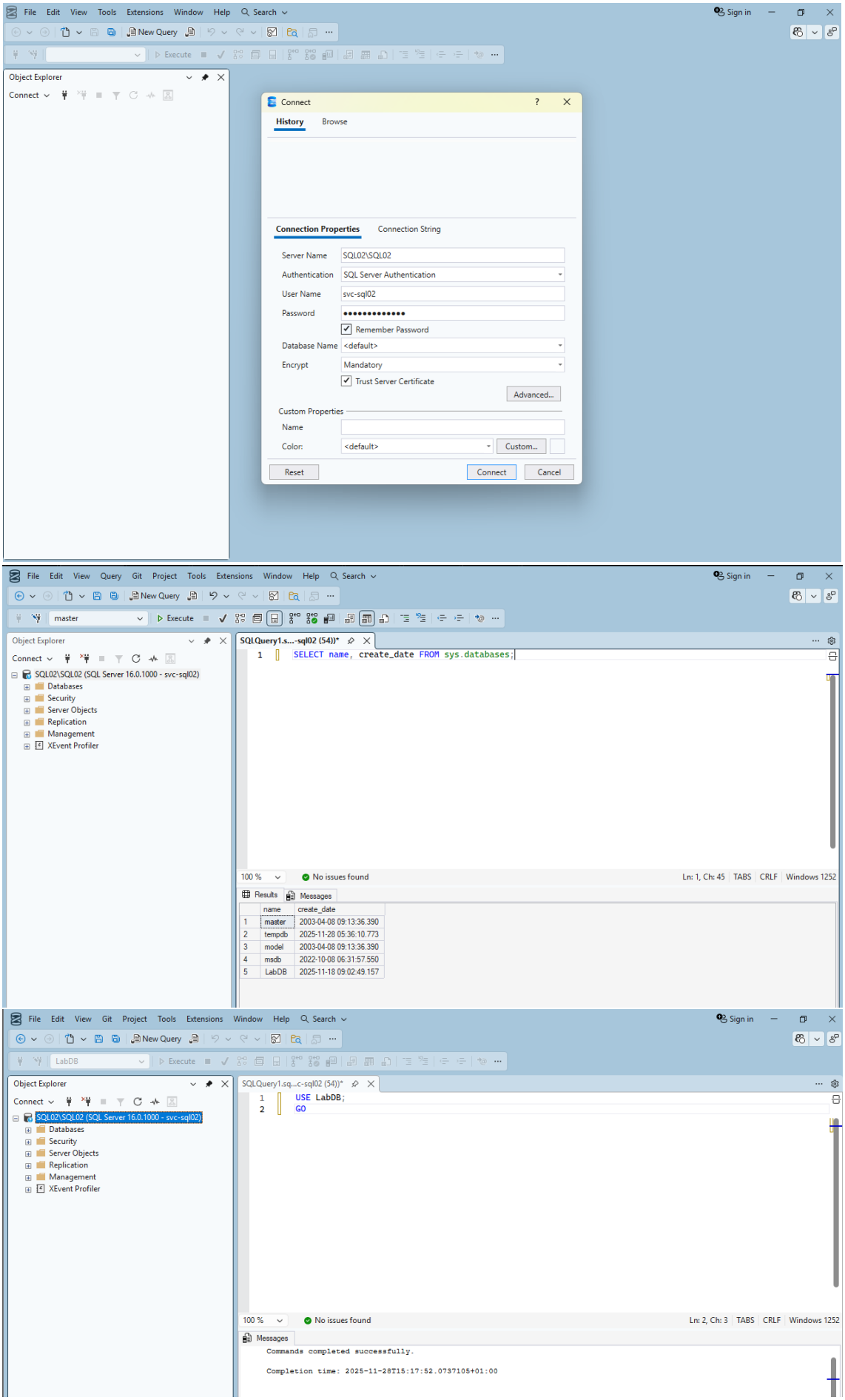

Ilustración 25. Acceso y validación de permisos sobre el servidor SQL02 mediante credenciales comprometidas

Esta imagen muestra el acceso al servidor SQL02 usando las credenciales comprometidas de la cuenta svc-sql02, así como la validación de los permisos disponibles sobre el sistema de la base de datos.

Una vez establecida conexión mediante autenticación SQL Server se procedió a enumerar bases de datos disponibles y verificar el nivel de acceso asociado a la cuenta comprometida. Como resultado se confirmó la capacidad de interacción con la base de datos "LabDB" validando el compromiso efectivo del servicio SQL.

Exposición de credenciales en la base de datos SQL02

Durante la exploración del contenido de la base de datos, se identificaron nuevas credenciales que pueden ser usadas en fases posteriores. Este comportamiento refleja una debilidad habitual en entornos corporativos donde:

- Las aplicaciones almacenan credenciales en bases de datos.
- No existen mecanismos de protección adecuados.
- Se reutilizan contraseñas entre servicios.

Campo	Valor
CWE	CWE-522 – Insufficiently Protected Credentials
CVSS 3.1	7.5 (High)
Root Cause	Almacenamiento inseguro de credenciales
Impacto	Compromiso adicional de cuentas
Remediación	Uso de cifrados fuertes y gestión segura de cuentas
Referencias	MITRE ATT&CK – T1552 (Unsecured Credentials)

Tabla 18. Evaluación de la vulnerabilidad asociada al almacenamiento inseguro de credenciales en sistemas y servicios corporativos

Desde el punto de vista de detectabilidad:

- El acceso a la base de datos ha sido legítimo.
- La lectura de datos no genera eventos sospechosos.
- No existe diferenciación entre acceso normal y malicioso.

Por esto su detectabilidad es baja.

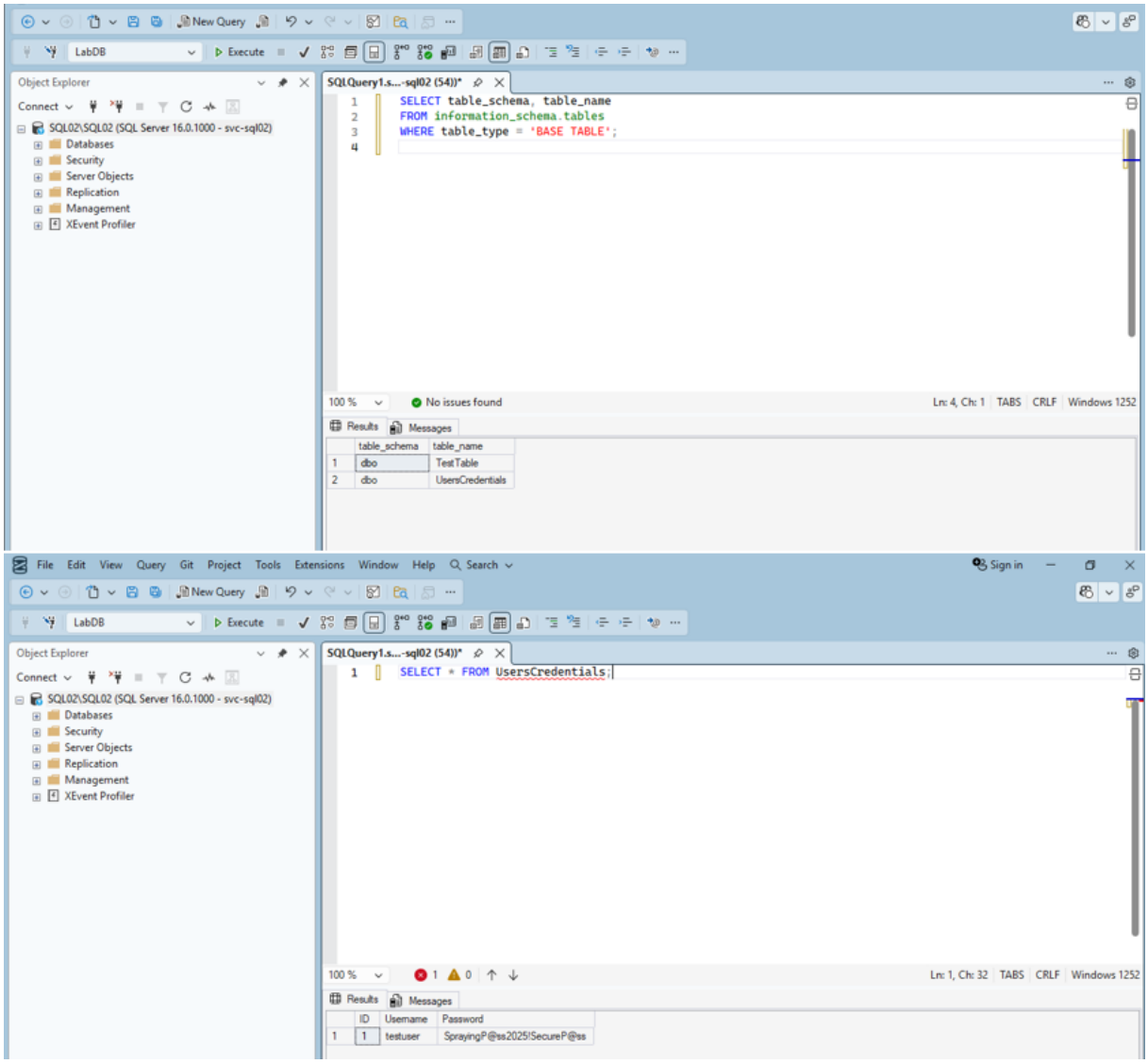

Ilustración 26. Enumeración de tablas y obtención de credenciales almacenadas en la base de datos LabDB

Esta imagen muestra la exploración de la base de datos “LabDB” tras el acceso exitoso al servidor SQL02 mediante la cuenta comprometida svc-sql02.

Primero se realiza una enumeración de tablas disponibles dentro de la base de datos identificando la tabla “UsersCredentials”, la cual contiene información sensible relacionada con usuarios del sistema.

Tras esto se ejecuta una consulta en la tabla obteniendo credenciales almacenadas en texto plano. Este tipo de información me permite ampliar el alcance del compromiso reutilizando nuevas credenciales en fases posteriores.

Ejecución remota de comandos en SQL02 (xp_cmdshell)

Campo	Valor
CWE	CWE-288 – Improper access control
CVSS 3.1	8.8 (High)
Root Cause	Habilitación de funcionalidades peligrosas en SQL Server
Impacto	Ejecución remota de comandos en el sistema
Remediación	Deshabilitar xp_cmdshell y restringir privilegios
Referencias	MITRE ATT&CK – T1059 (Command and Scripting Interpreter), T1505.001 (SQL Stored Procedures)

Tabla 19. Evaluación de la vulnerabilidad asociada a la ejecución remota de comandos mediante xp_cmdshell en SQL Server

Una vez obtenido el acceso al servidor SQL02, se habilitó la funcionalidad xp_cmdshell permitiéndome la ejecución de comandos en el sistema operativo desde el motor de base de datos.

Desde un punto de vista analítico, este paso representa una transición critica de acceso a datos hacia control del sistema.

Esto implica lo siguiente:

- Ejecución remota de comandos.
- Posibilidad de movimiento lateral.
- Persistencia en el sistema.

En términos de detectabilidad:

- Puede generar eventos si esta monitorizado pero el uso puede confundirse con tareas administrativas.

Por esto, su detectabilidad puede considerarse media en ausencia de reglas específicas.

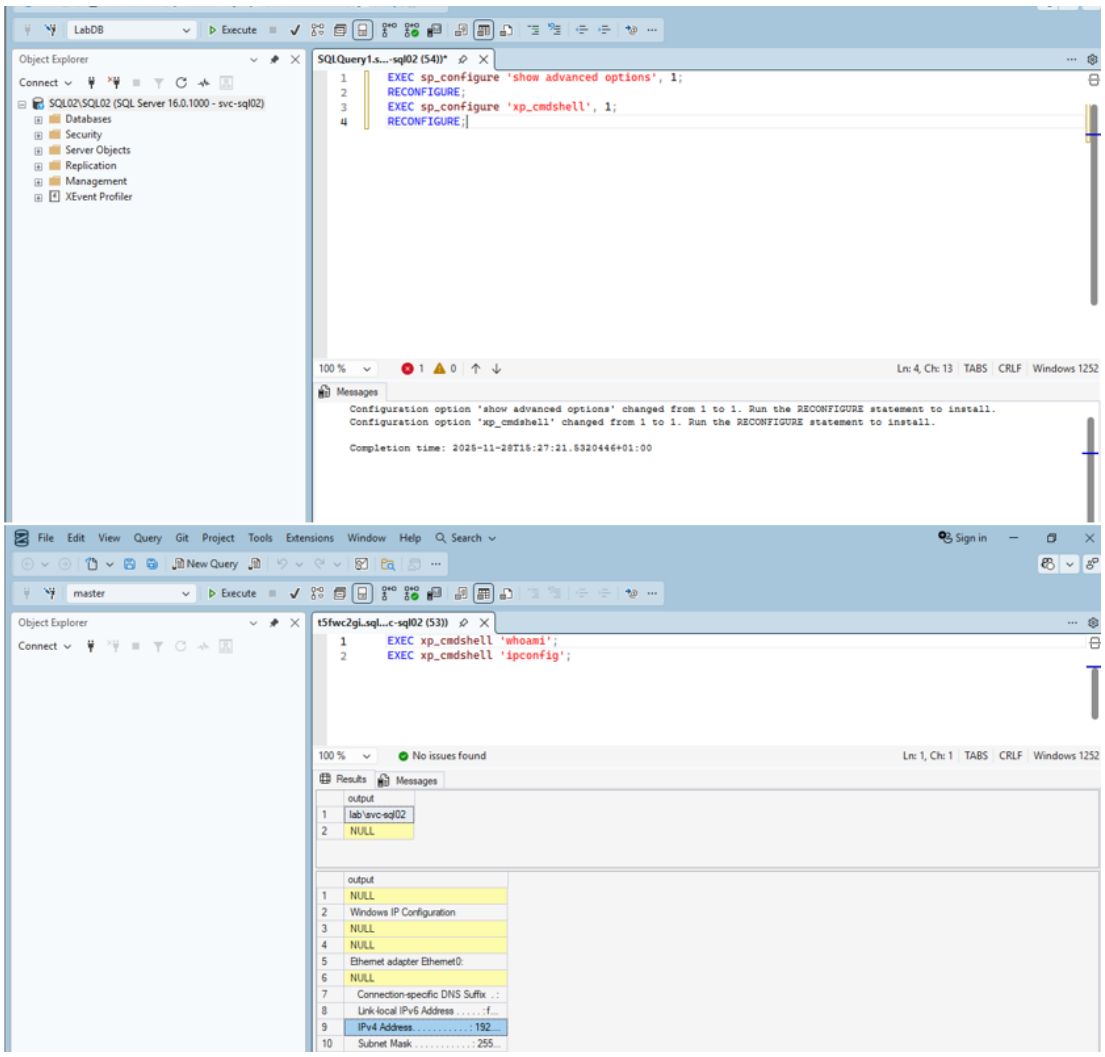

Ilustración 27. Habilitación y ejecución remota de comandos mediante xp_cmdshell en SQL02

Se muestra la habilitación de la funcionalidad xp_cmdshell en el servidor SQL02, así como la ejecución de comandos del sistema operativo directamente desde el motor de base de datos.

Una vez activada esta funcionalidad, se ejecutan comandos como whoami o ipconfig confirmando la capacidad de interacción con el sistema operativo y validando la ejecución remota de comandos sobre el servidor.

Conclusión de la fase

La fase de explotación de servicios de base de datos pone de manifiesto que las bases de datos corporativas y las cuentas de servicio asociadas constituyen uno de los vectores más críticos dentro de entornos AD.

A través de la combinación de Kerberoasting, reutilización de credenciales, acceso a bases de datos, exposición de credenciales almacenadas y ejecución remota de comandos pude ampliar progresivamente el nivel de acceso y obtener control sobre sistemas críticos en el entorno.

Durante esta fase se observa una transición clara desde el compromiso de mecanismos de autenticación hacia el acceso directo a información sensible de aplicación y ejecución sobre sistemas interno. El acceso a SQL01 permitió identificar credenciales almacenadas de forma

insegura dentro de la base de datos “appdb”, mientras que el compromiso de SQL02 habilitó la capacidad de ejecución remota mediante funcionalidades propias del motor SQL.

Desde el punto de vista analítico esta fase evidencia que el uso de credenciales válidas y funcionalidades legítimas reduce significativamente la visibilidad del ataque ya que muchas de las acciones realizadas son compatibles con el comportamiento esperado de administradores, aplicaciones o cuentas de servicio.

Desde el punto de vista de la detección, se observa lo siguiente:

- Muchas acciones se realizan mediante autenticaciones legítimas.
- Parte del ataque ocurre fuera del entorno monitorizado.
- Las consultas SQL y accesos a bases de datos pueden confundirse con actividad normal.
- La detección depende principalmente de correlación, contexto y análisis de comportamiento.

Adicionalmente, se observa que las fases relacionadas con acceso a datos presentan una detectabilidad especialmente baja debido a que la lectura de información sensible no genera indicadores claramente maliciosos cuando se realiza mediante credenciales válidas.

Esto evidencia que las técnicas más críticas no siempre implican explotación avanzada sino el abuso de configuraciones inseguras y credenciales reutilizadas para operar de forma legítima dentro del entorno comprometido.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Kerberoasting svc-sql02	Solicitudes kerberos	Media/Baja	Crackeo offline no detectable
Acceso a SQL01 mediante user2	Autenticación MariaDB	Baja	Uso de credenciales válidas
Exposición de credenciales en appdb	Consultas SQL/lectura de datos	Baja	Actividad indistinguible de acceso legítimo
Uso de credenciales svc-sql02	Autenticación SQL	Baja	Reutilización de credenciales válidas
Acceso de base de datos SQL02	Consultas SQL	Baja	Actividad compatible con administración
xp_cmdshell	Ejecución de comandos	Media	Puede generar eventos si esta monitorizado

Tabla 20. Evaluación de detectabilidad de técnicas de abuso de cuentas de servicio y explotación de servicios SQL

Esta evaluación refleja que la detectabilidad en esta fase se ve reducida principalmente por el uso de credenciales válidas y funcionalidades legítimas de los sistemas de base de datos.

Se observa que las actividades relacionadas con acceso y lectura de información presentan una visibilidad especialmente limitada ya que las consultas SQL y autenticaciones pueden confundirse fácilmente con operaciones administrativas o comportamientos normales de la aplicación.

Asimismo, las técnicas que implican ejecución directa sobre el sistema como xp_cmdshell incrementan parcialmente la visibilidad aunque continúan dependiendo de reglas específicas de monitorización y correlación avanzada para ser identificadas correctamente.

De forma general, ninguna de las técnicas analizadas presenta una detectabilidad alta de forma aislada reforzando la necesidad de modelos basados en comportamiento, correlación temporal y análisis contextual de eventos.

Fase 5 – Escalada de privilegios, persistencia y compromiso del dominio

Contexto del ataque

Tras comprometer el servidor SQL02 y obtener acceso mediante credenciales válidas, nos encontramos en una posición privilegiada dentro del entorno. En esta fase el objetivo principal es escalar privilegios hasta alcanzar control total del sistema y del dominio, así como establecer mecanismos de persistencia.

A diferencia de fases anteriores en las que hemos dependido de configuraciones inseguras o credenciales expuestas, ahora ya disponemos de acceso directo a sistemas críticos. Esto me permite el uso de técnicas avanzadas orientadas a:

- Escalada de privilegios locales.
- Ejecución remota de comandos.
- Extracción de credenciales del dominio.
- Persistencia a largo plazo.

Esta fase representa el punto culminante del ataque donde se materializa todo el impacto total sobre la infraestructura completa.

Clasificación de la técnica

Elemento	Descripción
Táctica	Privilege Escalation/Credential Access/Persistence
Tipo de técnica	Escalada de privilegios y abuso de Kerberos
Superficie afectada	Servidor SQL02 y AD
Naturaleza	Uso de herramientas legítimas y abuso de privilegios
Riesgo asociado	Compromiso total del sistema del dominio

Tabla 21. Clasificación de la técnica de escalada de privilegios y abuso avanzado de Kerberos en Active Directory

Evaluación de la vulnerabilidad (Ejecución remota y LOLBins)

Campo	Valor
CWE	CWE-284 – Improper Access Control
CVSS 3.1	8.5 (High)
Root Cause	Uso de herramientas del sistema sin restricciones
Impacto	Ejecución remota de código en el sistema
Remediación	Restricción de binarios y control de ejecución
Referencias	MITRE ATT&CK – T1218 (Signed Binary Proxy Execution), T1105 (Ingress Tool Transfer)

Tabla 22. Evaluación de la vulnerabilidad asociada al abuso de herramientas legítimas y ejecución remota de código

En esta fase se usan herramientas como “Certutil” para transferir binarios al sistema comprometido. Este tipo de técnicas es conocido como LOLBins o Living Of The Land Binaries, los cuales permiten ejecutar acciones maliciosas sin necesidad de introducir software externo detectable.

Desde un punto de vista analítico, este enfoque reduce significativamente la superficie de detección ya que se usan herramientas legítimas del sistema operativo.

Transferencia de herramientas y ejecución remota

Para continuar con la explotación se transfirió herramientas como Mimikatz, PrintSpoofer y Netcat al servidor SQL02 mediante un servidor HTTP controlado por nosotros como atacantes.

Estas herramientas me permiten:

- Extraer credenciales (Mimikatz).
- Escalada de privilegios (PrintSpoofer).
- Establecer shells remotas (Netcat).

Desde el punto de vista de la detectabilidad:

- El uso de Certutil puede generar eventos pero es una herramienta legítima.
- Puede confundirse con actividad administrativa.

Por esto la detectabilidad es media en ausencia de reglas específicas.

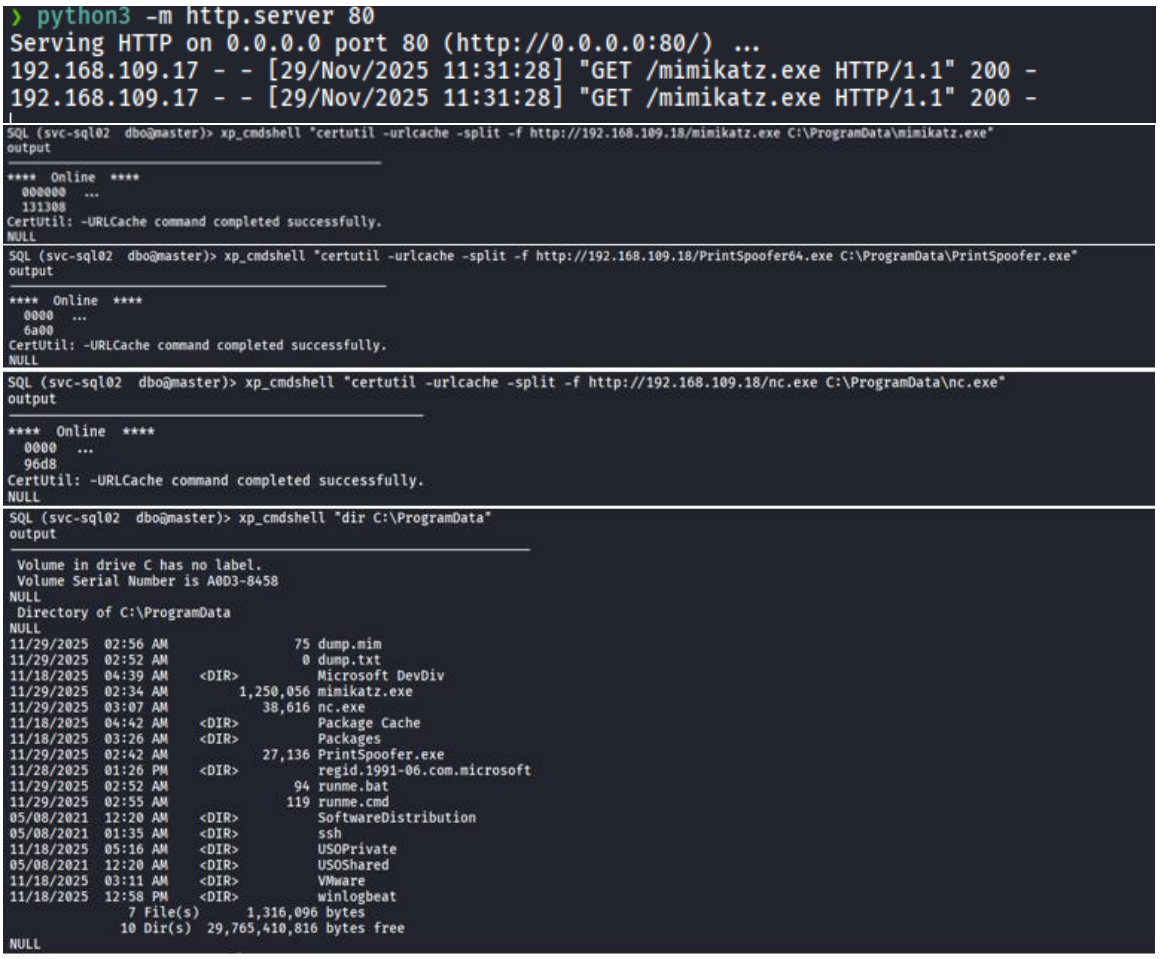

Ilustración 28. Transferencia de herramientas al servidor SQL02 mediante HTTP y certutil

La imagen muestra la transferencia de herramientas desde la máquina atacante hacia el servidor SQL02 usando un servidor temporal HTTP montado en Python y usando Certutil para descargar estos archivos desde la terminal de xp_cmdshell antes conseguida.

Con esto conseguimos descargar los diferentes binarios en el sistema las cuales están orientadas a la postexplotación y elevación de privilegios como es Mimikatz y PrintSpoofer.

Escalada de privilegios locales (PrintSpoofer)

Campo	Valor
CWE	CWE-269 – Improper Privilege Management
CVSS 3.1	8.8 (High)
Root Cause	Configuración insegura de servicios privilegiados
Impacto	Obtención de privilegios SYSTEM
Remediación	Restricción de privilegios y actualización de parches
Referencias	MITRE ATT&CK – T1068 (Explotation for Privilege Escalation)

Tabla 23. Evaluación de la vulnerabilidad asociada a la escalada de privilegios mediante abuso de servicios privilegiados

Mediante el uso de PrintSpoofer se logra escalar privilegios hasta obtener ejecución como NT AUTHORITY\SYSTEM en el servidor SQL02. Esto lo conseguimos creando un archivo .bat, el cual lanza un cmd hacia nuestro listener usando netcat, que se ejecutará mediante PrintSpoofer. Esta herramienta nos permite abusar de privilegios de servicios para obtener la ejecución con privilegios.

Este paso representa un punto muy crítico por las siguientes razones:

- Se obtiene control total del sistema.
- Se habilita el acceso a credenciales almacenadas.
- Se permite la ejecución de cualquier acción.

En términos de detectabilidad:

- Puede generar eventos en el sistema pero depende de monitorización especifica.

Por esto su detectabilidad es media.

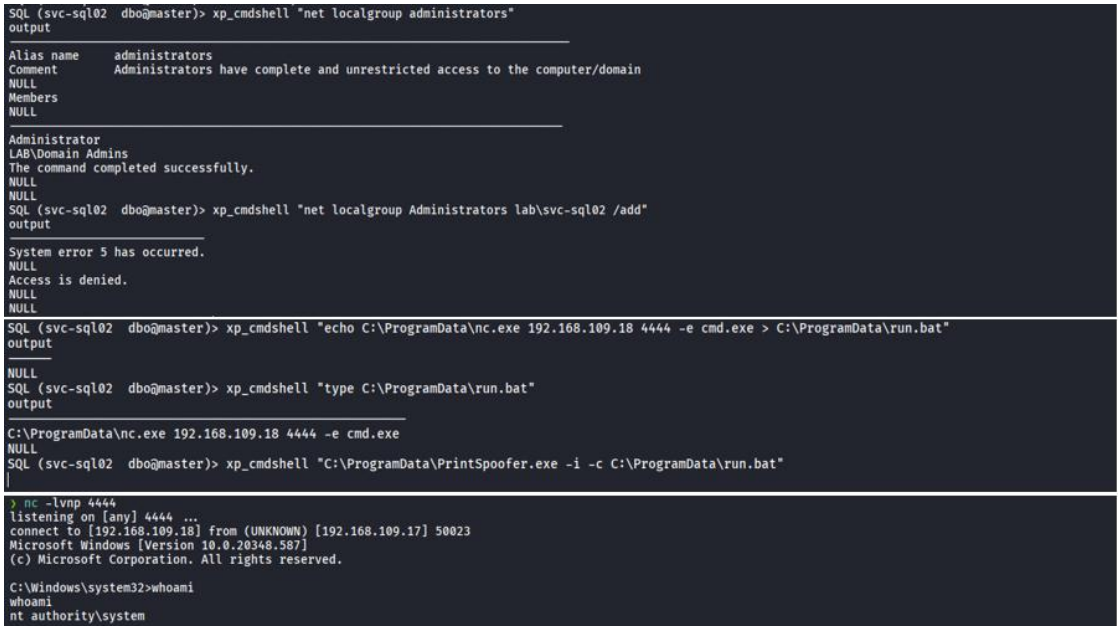

Ilustración 29. Escalada de privilegios locales mediante abuso de PrintSpoofer

Esta imagen muestra la explotación de la herramienta PrintSpoofer para realizar una escalada de privilegios local en el servidor SQL02 obteniendo la ejecución de comandos con privilegios NT AUTHORITY\SYSTEM.

Primero verifiqué que la cuenta comprometida no disponía de privilegios administrativos suficientes para modificar grupos locales en el sistema, y posteriormente se preparó una reverse Shell usando Netcat que se ejecutó con PrintSpoofer mediante xp_cmdshell permitiendo elevar privilegios y obtener una sesión remota con control total sobre el servidor.

Ataque DCSync

Campo	Valor
CWE	CWE-269 – Improper Privilege Management
CVSS 3.1	9.1 (High)
Root Cause	Permisos excesivos de replicación en AD
Impacto	Extracción de credenciales críticas del dominio
Remediación	Restricción de permisos de replicación y monitorización de privilegios
Referencias	MITRE ATT&CK – T1003.006 (DCSync)

Tabla 24. Evaluación de la vulnerabilidad asociada al abuso de permisos de replicación en Active Directory mediante DCSync

Tras obtener privilegios elevados dentro del dominio se ejecutó un ataque DCSync usando Mimikatz con el objetivo de simular el comportamiento de un controlador de dominio y solicitar información de replicación directamente desde AD.

A través de esta técnica pude extraer los hashes y credenciales asociadas a cuentas críticas del dominio, incluyendo KRBTGT, usada por Kerberos para la generación y validación de tickets de autenticación.

Desde el punto de vista técnico, el ataque DCSync no requiere de acceso físico al controlador de dominio ni extracción directa de la base de datos NTDS.dit, sino que abusa del mecanismo legítimo de replicación de AD permitiendo obtener información sensible mediante peticiones válidas dentro del protocolo.

Desde un punto de vista más analítico esta técnica representa uno de los escenarios más críticos dentro de un entorno AD debido a:

- Permite comprometer completamente el sistema de autenticación Kerberos.
- Facilita ataques posteriores como Golden Ticket.
- Usa funcionalidades legítimas del dominio.
- Reduce significativamente los indicadores clásicos de compromiso.

Desde el marco MITRE ATT&CK esta actividad se relaciona con:

- **T1003.006 – DCSync**

En términos de detectabilidad:

- Las solicitudes de replicación pueden generar eventos específicos, pero estas forman parte del funcionamiento normal del dominio.
- La actividad puede confundirse con replicaciones legítimas entre controladores de dominio.

Por esto su detectabilidad puede considerarse media especialmente en entornos sin monitorización especifica de privilegios de replicación.

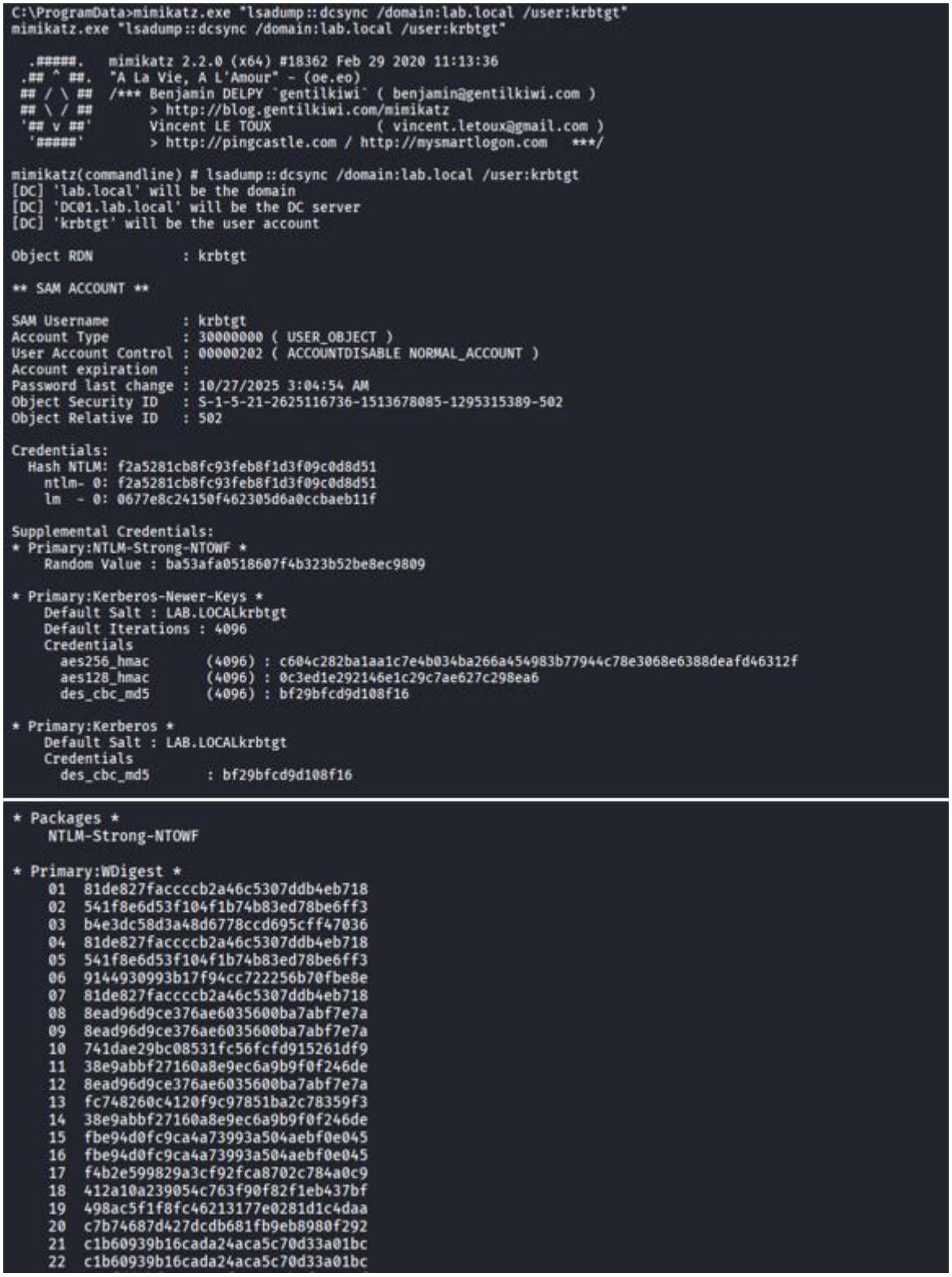

Ilustración 30. Ejecución de ataque DCSync y extracción de credenciales del controlador de dominio

Esta imagen muestra la ejecución del ataque DCSync mediante la herramienta Mimikatz que permite solicitar al controlador de dominio información de replicación asociada a la cuenta KRBTGT del dominio. Con esta técnica simulamos el comportamiento de un controlador de dominio legítimo obteniendo hashes y credenciales almacenadas en AD sin necesidad de acceder físicamente al DC ni interactuar con el proceso LSASS.

Como resultado obtenemos credenciales criticas asociadas a la cuenta que es usada por Kerberos para la firma y generación de tickets dentro del dominio.

Generación de Golden Ticket

Campo	Valor
CWE	CWE-287 – Improper Authentication
CVSS 3.1	9.5 (High)
Root Cause	Compromiso de la cuenta KRBTGT
Impacto	Control persistente y total del dominio
Remediación	Rotación de KRBTGT y control estricto de privilegios
Referencias	MITRE ATT&CK – T1558.001 (Golden Ticket)

Tabla 25. Evaluación de la vulnerabilidad asociada al abuso de autenticación Kerberos mediante Golden Ticket

Una vez obtenido el hash de la cuenta KRBTGT mediante el ataque DCSync, procedí a la generación de un Golden Ticket usando Mimikatz. Para esto primero se tuvo que identificar el SID asociado al dominio y al usuario administrativo usado durante el ataque.

El ticket generado permitió crear autenticaciones Kerberos válidas sin necesidad de interactuar continuamente con el controlador de dominio proporcionando persistencia y privilegios elevados dentro del entorno comprometido.

Posteriormente, ser verificó la correcta carga del ticket comprobando su presencia en la cache Kerberos del sistema y validando el acceso privilegiado sobre recursos del dominio. Adicionalmente, se creó un nuevo usuario con privilegios administrativos demostrando la capacidad de mantener persistencia incluso tras cambios parciales en las credenciales comprometidas.

Desde el punto de vista analítico, esta técnica representa uno de los ataques más críticos dentro de AD debido a que compromete directamente el mecanismo central de autenticación Kerberos. Esto implica lo siguiente:

- Persistencia indefinida dentro del dominio.
- Suplantación de identidades privilegiadas.
- Capacidad de autenticación sin credenciales legítimas.
- Recuperación de acceso incluso tras mitigaciones parciales.

Desde el marco MITRE ATT&CK:

- **T1558.001 – Golden Ticket**

En términos de detectabilidad:

- Parte del proceso ocurre offline.
- El ticket generado es válido desde la perspectiva del dominio.
- No requiere autenticación constante contra el controlador de dominio.
- La actividad puede confundirse con autenticación Kerberos legítima.

Por esto, su detectabilidad puede considerarse baja en ausencia de monitorización avanzada de tickets Kerberos y correlación temporal de eventos.

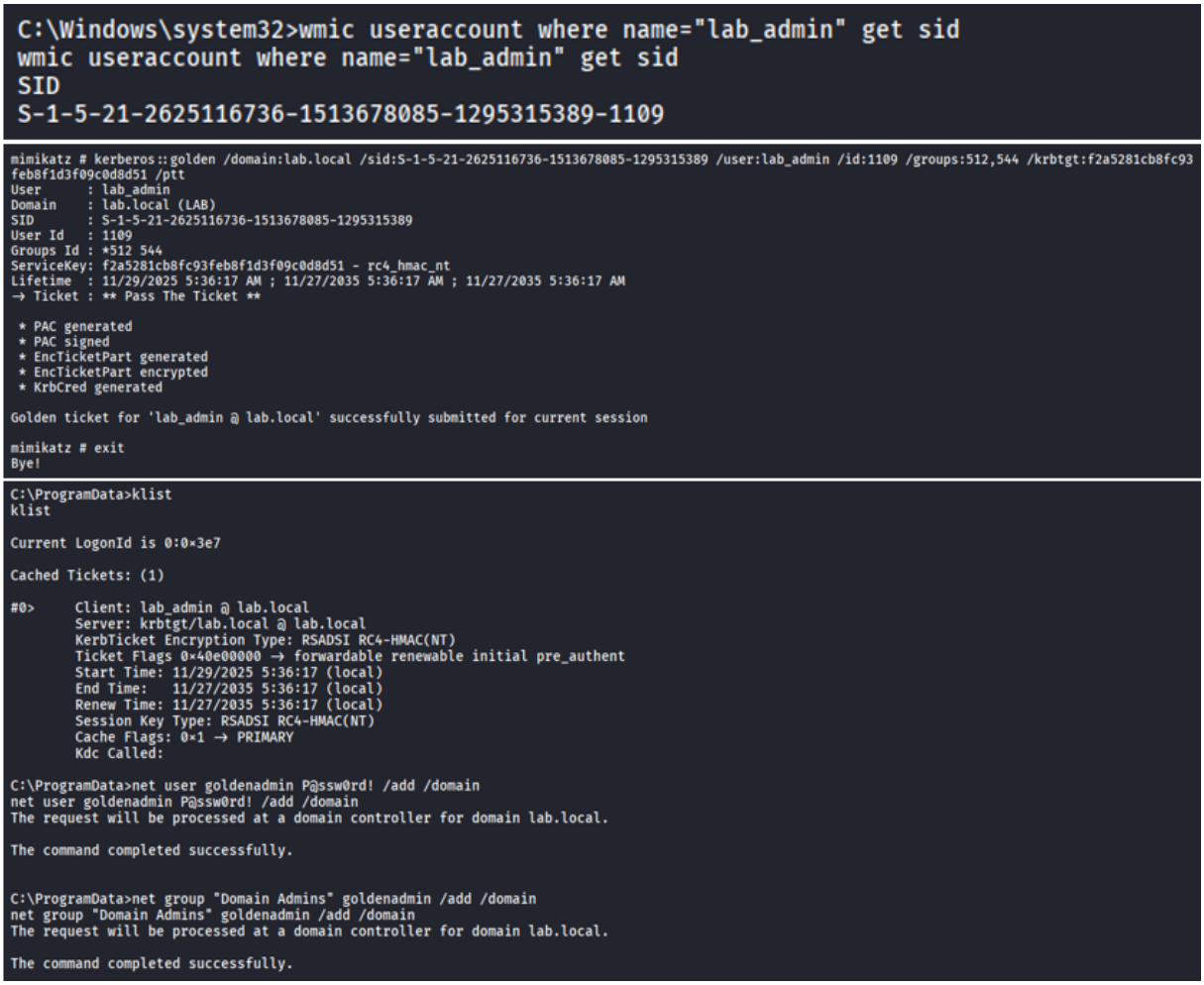

Ilustración 31. Generación de Golden Ticket y establecimiento de persistencia en Active Directory

Esta imagen muestra la generación de un Golden Ticket mediante la herramienta Mimikatz usando el hash de la cuenta KRBTGT obtenido previamente a través de DCSync. Para esto se necesita el SID del dominio y se generó un ticket Kerberos falsificado asociado a la cuenta "lab_admin".

Posteriormente, el ticket fue inyectado en la sesión activa permitiendo la autenticación persistente frente a los servicios de AD. Como resultado logré crear una nueva cuenta privilegiada llamada "goldenadmin" y añadirla al grupo de "Domain Admins" consolidando el control total sobre el dominio.

Generación y uso de Silver Ticket

Campo	Valor
CWE	CWE-287 – Improper Authentication
CVSS 3.1	8.8 (High)
Root Cause	Compromiso de hashes NTLM asociados a servicios
Impacto	Acceso no autorizado a servicios concretos
Remediación	Protección de cuentas de servicio y rotación de credenciales
Referencias	MITRE ATT&CK – T1558.002 (Silver Ticket)

Tabla 26. Evaluación de la vulnerabilidad asociada al abuso de autenticación Kerberos mediante Silver Ticket

Tras comprometer la cuenta de servicio “svc-sql02” en fases anteriores he querido demostrar cómo se genera un Silver Ticket con el objetivo de poder autenticarme directamente contra el servicio SQL asociado a SQL02.

Para ello, se usó el hash en formato MD4 de la cuenta comprometida junto con información del dominio y del servicio objetivo generando así un ticket Kerberos falsificado válido únicamente para este servicio. Posteriormente, el ticket fue convertido a formatos compatibles (. ccache) para poder usarlo con herramienta Impacket.

Una vez cargado el ticket en memoria, se validó el acceso al servicio SQL sin necesidad de interactuar directamente con el controlador de dominio demostrando así la capacidad de autenticación local sobre el servicio comprometido.

Desde el punto de vista analítico, el ataque Silver Ticket es una característica especialmente relevante. A diferencia de Golden Ticket la autenticación se realiza directamente contra el servicio objetivo evitando gran parte de la monitorización asociada al controlador de dominio. Esto implica:

- Reducción significativa de visibilidad en el DC.
- Persistencia limitada pero altamente sigilosa.
- Acceso directo a servicios específicos.
- Uso de autenticación Kerberos aparentemente valida.

Desde el marco MITRE ATT&CK:

- **T1558.002 – Silver Ticket**

En términos de detectabilidad puede considerarse muy baja en entornos sin monitorización avanzada de servicios Kerberos.

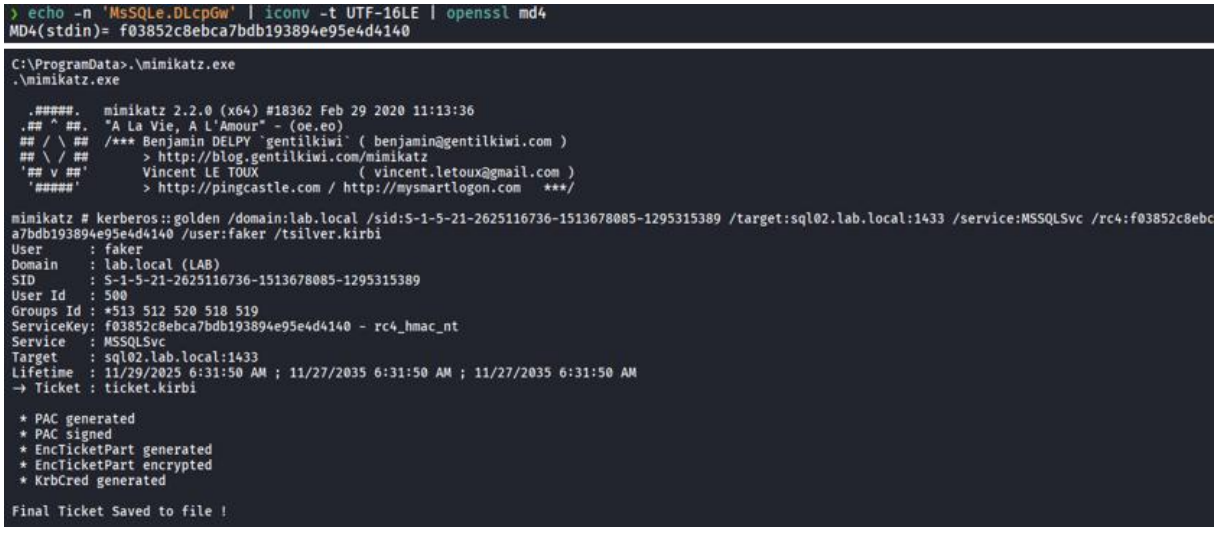

Ilustración 32. Generación de Silver Ticket para el servicio MSSQLSvc

Esta imagen muestra la generacion de un Silver Ticket asociado al servicio MSSQLSvc del servidor SQL02 usando Mimikatz. Para ello se uso el hash NTLM de la cuenta de servicio comprometida previamente generando un ticket Kerberos falsificado valido unicamente para el servicio SQL del sistema objetivo.

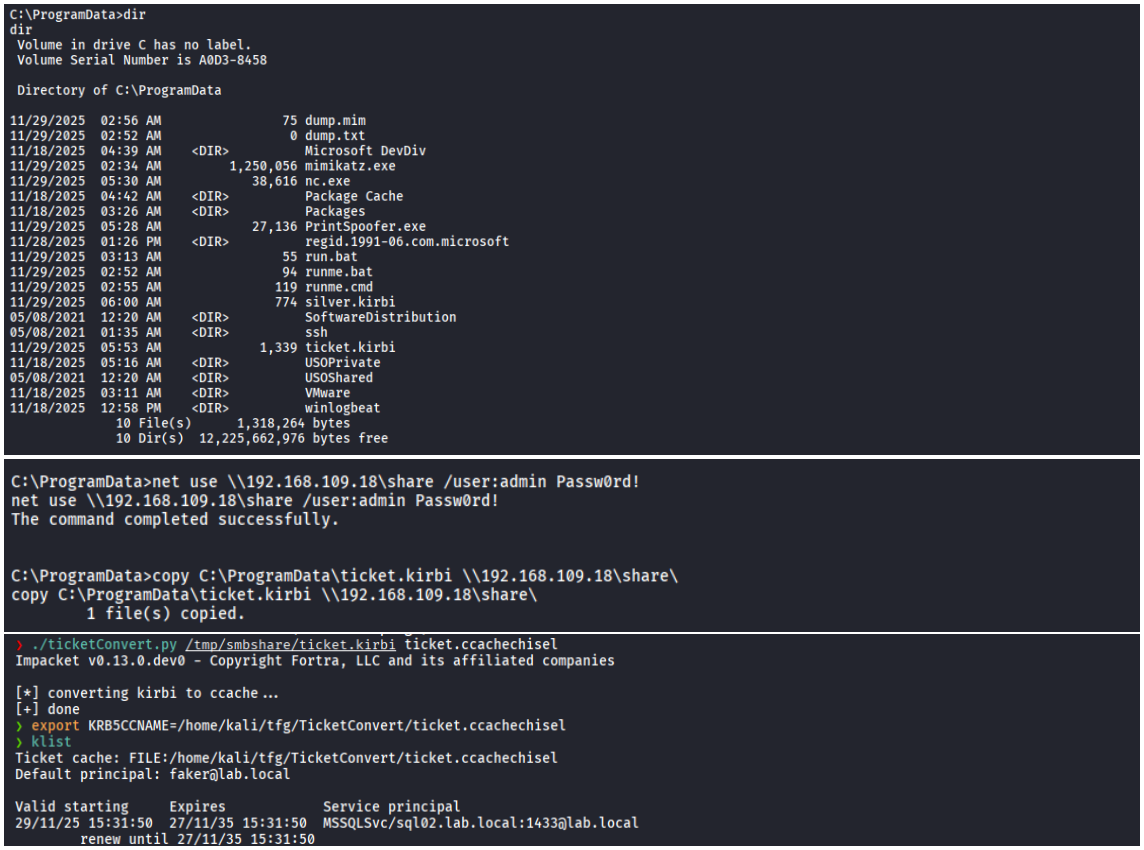

Ilustración 33. Transferencia y preparación del Silver Ticket para autenticación Kerberos

La imagen muestra el proceso de transferencia y conversion del Silver Ticket generado previamente para su reutilizacion desde la máquina Kali. Inicialmente, el ticket Kerberos se almacena en .kirbi dentro del sistema comprometido y posteriormente se transfiere mediante un recursos SMB hacia nuestra máquina atacante. Por último, se convierte a formato .ccache para su uso mediante herramientas Impacket compatibles con Kerberos en Linux.

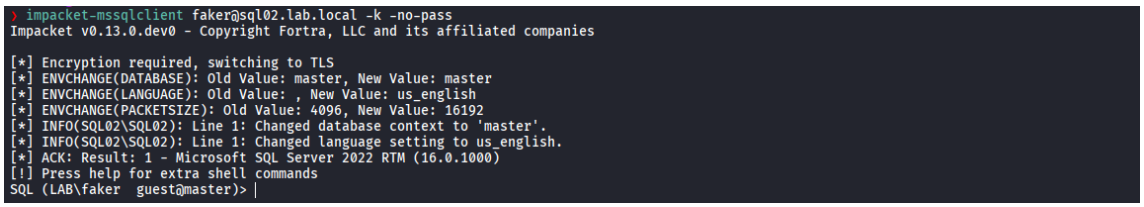

Ilustración 34. Acceso al servicio MSSQL mediante autenticación Kerberos falsificada

Esta imagen muestra el acceso al servicio MSSQL del servidor SQL02 usando el Silver Ticket previamente generado que nos permite autenticacion via Kerberos sin necesidad de credenciales válidas.

Mediante el uso del ticket falsificado, pude establecer conexión autenticada contra el servicio SQL usando una identidad arbitraria “faker” y obtener acceso directo al sistema comprometido.

Persistencia mediante privilegios SQL

Campo	Valor
CWE	CWE-284 – Improper Access Control
CVSS 3.1	8.6 (High)
Root Cause	Asignación excesiva de privilegios sobre SQL Server
Impacto	Persistencia y ejecución privilegiada sobre sistemas críticos
Remediación	Restricción de privilegios administrativos y revisión de cuentas de servicio
Referencias	MITRE ATT&CK – T1098 (Account Manipulation), T1505.001 (SQL Stored Procedures)

Tabla 27. Evaluación de la vulnerabilidad asociada a la persistencia y abuso de privilegios sobre SQL Server

Una vez validado el acceso al servicio SQL mediante Silver Ticket se comprobó que la cuenta comprometida disponía de privilegios elevados sobre el servidor SQL02 incluyendo permisos administrativos (sysadmin).

Con estos privilegios, procedí a establecer un mecanismo de persistencia mediante la creación y modificación de cuentas con acceso privilegiado al motor SQL permitiéndome recuperar acceso al sistema incluso en caso de pérdida de credenciales previamente comprometidas.

Desde un punto de vista operativo, esto representa una técnica especialmente relevante en ataques reales ya que permite mantener control persistente sobre servicios críticos usando funcionalidades administrativas legítimas del sistema.

Desde el punto de vista analítico, esta técnica evidencia como el abuso de privilegios sobre servicios de base de datos puede usarse no solo para acceso a información sino también para garantizar persistencia dentro del entorno comprometido. Esto implica:

- Persistencia a largo plazo.
- Recuperación de acceso tras mitigaciones parciales.
- Capacidad de ejecución privilegiada.
- Uso de mecanismos administrativos legítimos.

Desde el marco MITRE ATT&CK:

- **T1098 – Account Manipulation**
- **T1505.001 – SQL Stored Procedures**

En términos de detectabilidad:

- Las modificaciones administrativas pueden generar eventos, pero estas acciones pueden confundirse con tareas legítimas de administración SQL.
- La actividad depende principalmente de monitorización específica del motor de base de datos.

Por esto, su detectabilidad puede considerarse media especialmente en entornos donde no existe auditoria avanzada sobre acciones administrativas en SQL Server.

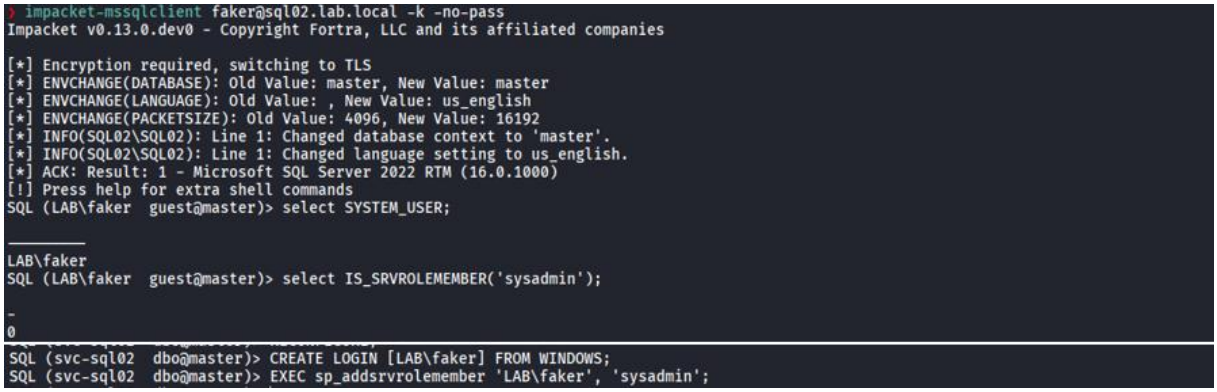

Ilustración 35. Validación de privilegios administrativos mediante autenticación Kerberos falsificada

La imagen muestra como tras el acceso con Silver Ticket a SQL02 se válida primero los privilegios obtenidos sobre SQL Server. Una vez verificado que no tenemos permisos de sysadmin, procedemos a asignárnoslos.

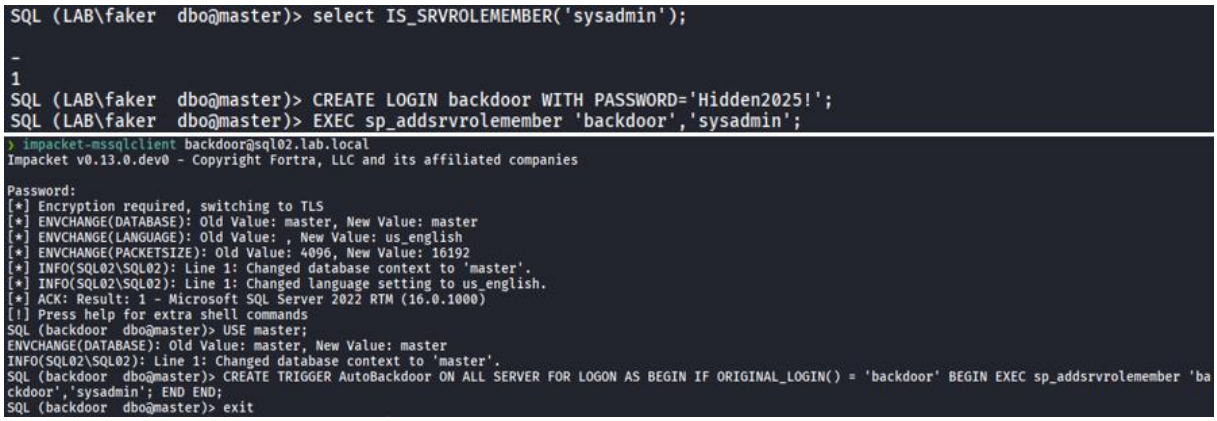

Ilustración 36. Establecimiento de persistencia mediante creación de cuentas y triggers en SQL Server

Esta imagen muestra la creación de un mecanismo de persistencia dentro del servidor SQL02 mediante la generación de una cuenta administrativa llamada “backdoor” y la implantación de un trigger automático asociado a la sesión. El trigger llamado AutoBackdoor diseñado para restaurar automáticamente privilegios elevados sobre la cuenta en futuras autenticaciones.

Ilustración 37. Verificación de persistencia mediante acceso con cuenta backdoor

Por último, se muestra la autenticación al servicio SQL02 usando la cuenta creada “backdoor” así como la validación de privilegios administrativos asociados a esta cuenta.

Conclusión de la fase

La fase de escalada de privilegios y compromiso del dominio representa el punto de mayor impacto del ataque ya que permite evolucionar desde acceso a un sistema hasta el control persistente de toda la infraestructura AD.

A través del abuso combinado con Kerberos, privilegios excesivos y herramientas legítimas del sistema se demuestra que muchas de las técnicas más críticas no requieren explotación tradicional sino el uso encadenado de configuraciones inseguras y credenciales comprometidas.

Desde el punto de vista analítico, esta fase evidencia varios aspectos relevantes:

- El uso de LOLBins y funcionalidades administrativas reduce significativamente la visibilidad del ataque.
- Técnicas como DCSync, Golden Ticket o Silver Ticket abusan directamente de mecanismos legítimos de AD y Kerberos.
- Parte del ataque ocurre offline limitando la capacidad de detección mediante logs tradicionales.
- La autenticación mediante tickets válidos dificulta diferenciar actividad maliciosa de comportamiento legítimo.

Asimismo, se observa que las técnicas con mayor impacto no son necesariamente las más ruidosas sino aquellas capaces de integrarse dentro del funcionamiento normal del entorno reduciendo la necesidad de explotación continua y facilitando persistencia a largo plazo.

De forma comparativa, acciones como PrintSpoofer o xp_cmdshell presentan una mayor detectabilidad al generar actividad observable sobre el sistema mientras que técnicas basadas en Kerberos presentan una detectabilidad considerablemente menor debido al uso de autenticaciones aparentemente válidas.

En conjunto esta fase ha demostrado que el compromiso completo de un entorno AD depende más de la acumulación progresiva de privilegios y relaciones de confianza que de una única vulnerabilidad critica aislada.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Uso de LOLBins	Ejecución de binarios	Media	Herramientas legítimas
Escalada con PrintSpoofer	Eventos de privilegio	Media	Depende de monitorización
DCSync	Solicitudes de replicación	Baja	Difícil de detectar
Golden Ticket	Autenticación Kerberos	Baja	No requiere validación constante
Silver Ticket	Acceso a servicios	Baja	No interactúa con DC
Backdoor SQL	Creación de usuario	Media/Baja	Puede pasar desapercibido

Tabla 28. Evaluación de detectabilidad de técnicas de escalada de privilegios, persistencia y abuso avanzado de Kerberos

Esta evaluación refleja que, a medida que se avanza en el ataque, la detectabilidad disminuye debido al uso de credenciales válidas y mecanismos internos del sistema.

Se observa que ninguna de las técnicas analizadas presenta una detectabilidad alta de forma aislada reforzando la necesidad de modelos de detección basados en la correlación de eventos.

Fase 6 – Reutilización de técnicas Kerberos y compromiso de servicios adicionales

Contexto del ataque

En esta fase se demostrará la aplicación de las técnicas que se han usado en las fases previas respecto a Kerberos, pero ahora usadas sobre el recurso del dominio DELEG-CLIENT el cual contiene el servidor web corporativo.

A diferencia de las otras fases en las que se introducían nuevas técnicas el objetivo de esta es demostrar la reutilización de ataques basados en Kerberos sobre distintos servicios y culminar con el compromiso de todas las máquinas y servicios creados en el laboratorio evidenciando que una misma debilidad puede afectar a múltiples activos.

DELEG-CLIENT ejecuta servicios bajo la cuenta de servicio “svc-web” la cual dispone de un SPN asociado. Esto lo convierte en un objetivo susceptible a ser explotado mediante técnicas como Kerberoasting y generación de tickets falsificados.

Desde el punto de vista del ofensivo esta fase demuestra la capacidad de escalar el ataque horizontalmente dentro del dominio comprometiendo múltiples sistemas mediante el mismo vector.

Debido a que se trata de una reutilización de técnicas, esta fase se explicará más por encima ya que en mayor medida se estarán repitiendo los pasos y técnicas pero con distinto objetivo.

Clasificación de la técnica

Elemento	Descripción
Táctica	Lateral Movement/Persistence
Tipo de técnica	Reutilización de tickets Kerberos (Silver Ticket)
Superficie afectada	DELEG-CLIENT
Naturaleza	Abuso de protocolos Kerberos
Riesgo asociado	Acceso no autorizado a servicios sin validación del DC

Tabla 29. Clasificación de la técnica de reutilización de tickets Kerberos mediante Silver Ticket

Evaluación de la vulnerabilidad (Silver Ticket)

Campo	Valor
CWE	CWE-287 – Improper Access Control
CVSS 3.1	8.8 (High)
Root Cause	Uso de claves de cuentas de servicio comprometidas
Impacto	Acceso directo a servicios sin autenticación centralizada
Remediación	Protección de cuentas de servicio y rotación de credenciales
Referencias	MITRE ATT&CK – T1558.002 (Silver Ticket)

Tabla 30. Evaluación de la vulnerabilidad asociada al abuso de tickets Kerberos mediante Silver Ticket

El uso de Silver Ticket permite al atacante generar tickets Kerberos válidos sin necesidad de interactuar con el controlador de dominio siempre que disponga de la clave de la cuenta del servicio asociada.

Desde el punto de vista analítico, esta técnica representa una de las más avanzadas de abuso de Kerberos ya que elimina completamente la dependencia del DC.

Preparación del ticket Kerberos

Para la generación del ticket, partimos del hash de la cuenta svc-web previamente obtenido el cual fue convertido a formato MD4 para su uso en Mimikatz. Este proceso permite construir manualmente el ticket Kerberos falsificado, incluyendo:

- SID del dominio.
- Identidad del usuario suplantado.
- SPN del servicio objetivo.

Desde el punto de vista de la detectabilidad:

- Esta fase se realiza offline.
- No genera eventos en el dominio salvo los generados al obtener los hashes mediante Kerberoasting en fases previas.

Por ello su detectabilidad es nula.

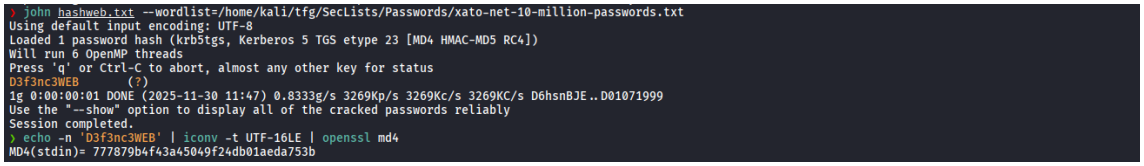

Ilustración 38. Preparación de clave Kerberos para la generación de Silver Ticket

La imagen muestra el proceso de preparación de la clave criptográfica que necesitamos para la generación del Silver Ticket como se vio en las fases previas.

Inicialmente realizamos el descifrado offline de la contraseña correspondiente a la cuenta de servicio comprometida mediante técnicas de cracking sobre el ticket Kerberos previamente obtenido. Posteriormente a esto, la contraseña se transforma en NTLM usando el algoritmo MD4 obteniendo la clave necesaria para la falsificación del ticket Kerberos.

Generación y conversión del ticket

Mediante Mimikatz, se generó el ticket con formato. kirbi el cual posteriormente fue convertido a formato. ccache para su uso en entorno Linux. Este paso permite integrar el ticket en herramientas como Impacket facilitando su uso en ataques posteriores.

Desde un punto de vista analítico, esta técnica evidencia que los ataques basados en Kerberos no dependen únicamente de herramientas específicas de Windows sino que pueden adaptarse a distintos entornos y plataformas aumentando significativamente la flexibilidad operativa del atacante.

Adicionalmente, el hecho de poder generar y reutilizar tickets válidos fuera del flujo normal de autenticación del dominio reduce la dependencia del controlador de dominio y dificulta la visibilidad centralizada del ataque.

Desde el marco MITRE ATT&CK:

- **T1558.002 – Silver Ticket**

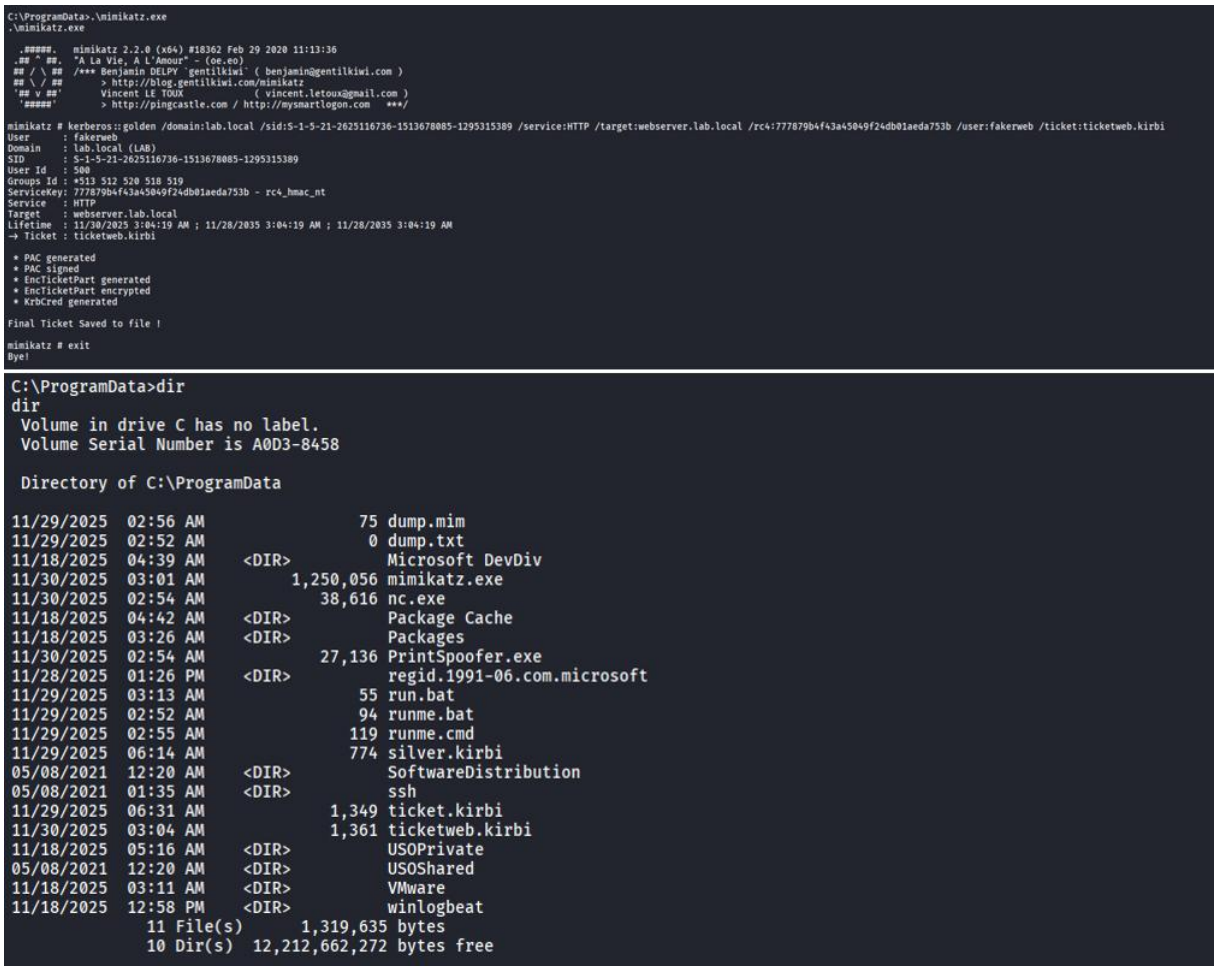

Ilustración 39. Generación y almacenamiento de Silver Ticket para el servicio web

Esta imagen muestra la generación de un Silver Ticket asociado al servicio HTTP del servidor "webserver.lab. local" mediante el uso de Mimikatz de la misma forma que se hizo con la cuenta del servidor SQL. Esta se almacena en formato. kirbi y posteriormente se pasará a un formato. ccache para su uso con herramientas Impacket.

Acceso al servicio web mediante Silver Ticket

Una vez cargado el ticket se accedió al servicio web alojado en DELEG-CLIENT comprobando que la autenticación Kerberos se realizaba correctamente sin necesidad de interacción con el controlador de dominio.

Este comportamiento confirma que:

- El servicio válida el ticket usando la clave local.
- No requiere validación adicional del DC.
- El acceso es completamente funcional.

Desde el punto de vista analítico, este paso demuestra una característica critica, el sistema objetivo confía en el ticket sin verificar su origen.

En términos de detectabilidad:

- No genera eventos en el controlador de dominio.

- La autenticación parece legítima.
- Solo podría detectarse en el propio servidor.

Por esto, su detectabilidad es baja.

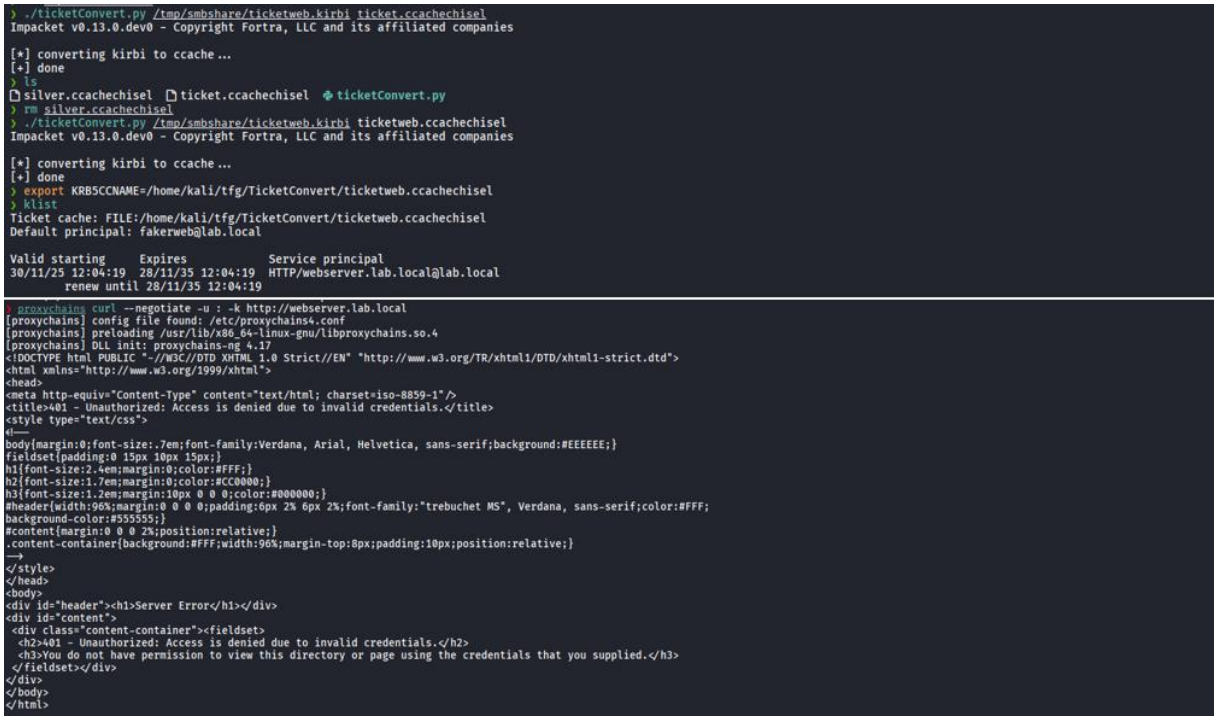

Ilustración 40. Acceso al servicio web mediante autenticación Kerberos falsificada (Silver Ticket)

Por último, se muestra la conversión a. ccache y tras esto su implementación en el sistema. Anteriormente no podíamos acceder a la web debido al error 401 Unauthorized indicando que el servidor rechazaba nuestra autenticación Kerberos debido al IIS/Active Directory, esto se debe a que no teníamos un ticket válido asociado al servicio HTTP.

Finalmente, se realiza una petición HTTP autenticada usando Kerberos a través de curl y proxychains que nos permite acceder al servidor web al mediante el ticket previamente generado.

Conclusión de la fase

La fase de reutilización de técnicas Kerberos pone de manifiesto que el compromiso de una única cuenta de servicio puede extenderse a múltiples sistemas dentro del dominio.

A través del uso de Silver Ticket fuimos capaces de:

- Acceder a servicios sin autenticación centralizada.
- Evitar mecanismos de detección basados en el DC.
- Reutilizar credenciales comprometidas en distintos sistemas.

Desde el punto de vista de la detección, se observa:

- Parte del ataque se realiza completamente offline.
- No se generan eventos en el controlador de dominio.
- La actividad puede parecer legítima en el sistema objetivo.

Esto evidencia que las técnicas basadas en Kerberos no solo permiten escalada vertical sino también expansión horizontal del ataque. Además, se observa que la reutilización de

credenciales y tickets reduce aún más la detectabilidad consolidando el control del atacante sobre el entorno.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Preparación del ticket	Procesos locales	Nula	Actividad oflfine
Generación del Silver Ticket	Uso de herramientas	Baja	No interactúa con el dominio, pero puede generar eventos locales en los endpoints
Uso del Ticket	Autenticación Kerberos	Baja	No pasa por el DC
Acceso al servicio web	Peticiones HTTP	Baja	Tráfico legítimo

Tabla 31. Evaluación de detectabilidad de técnicas de reutilización de tickets Kerberos mediante Silver Ticket

Esta evaluación refleja que esta fase presenta uno de los niveles de detectabilidad más bajos en todo el ataque debido a la ausencia de interacción con sistemas centralizados de autenticación.

Se observa que ninguna de las técnicas analizadas genera indicadores claros de compromiso de forma aislada reforzando la necesidad de monitorización en endpoints y correlación avanzada.

Fase 7 – Validación del compromiso total del dominio

Contexto del ataque

En esta fase final del punto de vista ofensivo, se válida el impacto del ataque en el entorno Active Directory demostrando que se ha alcanzado un nivel de control equivalente al de un administrador de dominio.

A diferencia de las otras fases donde el objetivo consistía en obtener acceso progresivamente a sistemas y credenciales, en este punto ya disponemos de privilegios suficientes para interactuar directamente con los componentes críticos del dominio y operar dentro del contexto legítimo de la infraestructura.

Este escenario representa la fase de consolidación del compromiso donde dejamos de depender de vulnerabilidades concretas y pasamos a aprovechar la propia confianza inherente del sistema. Como resultado, las acciones realizadas se ejecutan usando mecanismos legítimos de administración y autenticación, reduciendo la generación de indicadores claramente maliciosos.

El acceso que se ha alcanzado es consecuencia de la combinación progresiva de múltiples técnicas ejecutadas en fases anteriores:

- Compromiso de cuentas de servicio.
- Abuso de delegación Kerberos.
- Movimiento lateral mediante credenciales válidas.
- Escalada progresiva de privilegios.
- Persistencia mediante cuentas administrativas.

Desde un punto de vista analítico, esta fase es especialmente relevante porque pondrá de manifiesto una de las principales limitaciones en la detección de ataques avanzados en AD, que es que cuanto mayor es el nivel de privilegios alcanzado, más difícil resulta distinguir su actividad del comportamiento legítimo de administración.

Clasificación de la técnica

Elemento	Descripción
Táctica	Persistence/Privilege Escalation/Impact
Tipo de técnica	Validación de compromiso y control del dominio
Superficie afectada	Controlador de dominio y servicios críticos
Naturaleza	Uso de credenciales válidas y privilegios elevados
Riesgo asociado	Compromiso total del entorno AD

Tabla 32. Clasificación de la técnica de validación de compromiso y control total del dominio Active Directory

Evaluación de la vulnerabilidad (Compromiso del dominio)

Campo	Valor
CWE	CWE-284 – Improper Access Control
CVSS 3.1	10.0 (Critical)
Root Cause	Encadenamiento de múltiples debilidades y escalada progresiva de privilegios
Impacto	Control total del dominio y perdida completa de confianza
Remediación	Segmentación administrativa, hardening y monitorización avanzada
Referencias	MITRE ATT&CK – Persistence/Privilege Escalation

Tabla 33. Evaluación de la vulnerabilidad asociada al compromiso total y control completo del dominio Active Directory

El compromiso completo de un dominio AD representa el escenario de mayor impacto posible dentro de una infraestructura corporativa basada en identidades centralizadas.

Una vez alcanzado este nivel de acceso, disponemos de las siguientes capacidades:

- Controlar la autenticación del dominio.
- Acceder a cualquier sistema o recurso corporativo.
- Crear mecanismos de persistencia difíciles de eliminar.
- Modificar configuraciones críticas de seguridad.
- Alterar políticas del dominio y privilegios de usuarios.

Desde la perspectiva analítico, este escenario no debe interpretarse como el resultado de una única vulnerabilidad critica explotada, sino como la consecuencia acumulativa de múltiples configuraciones inseguras y debilidades operativas explotadas a lo largo del ataque.

Este refuerza la idea de que los ataques avanzados en AD no dependen normalmente de una explotación aislada, sino del abuso progresivo de relaciones de confianza dentro del entorno.

Dumping de credenciales del dominio

Una vez obtenidos los privilegios elevados dentro el entorno, se procede a realizar la extracción de credenciales directamente desde el controlador de dominio mediante herramientas orientadas a replicación y acceso a secretos almacenados en AD.

Esta técnica permite obtener:

- Hashes NTLM de cuentas.
- Credenciales de cuentas privilegiadas.
- Hashes asociados a KRBTGT.
- Cuentas máquina.
- Material criptográfico relacionado con Kerberos.

Desde el punto de vista ofensivo este paso representa una validación definitiva del compromiso del dominio ya que hemos obtenido acceso directo a los elementos usados por AD para la autenticación y generación de tickets Kerberos.

Además, el acceso al hash KRBTGT introduce la posibilidad de generar Golden Tickets como vimos en fases previas, permitiendo mantener persistencia prácticamente indefinida dentro del dominio incluso tras cambios de contraseñas en cuentas administrativas.

Desde el arco MITRE ATT&CK:

- **T1003 – OS Credential Dumping**

En cuanto a la detectabilidad:

- Parte de la actividad usa privilegios legítimos.
- La replicación de AD puede confundirse con comportamiento administrativo.
- No siempre existen eventos claramente diferenciadores.

Por esto, su detectabilidad puede considerarse media en ausencia de mecanismos específicos de auditoría y correlación avanzada.

Ilustración 41. Dumping de credenciales del dominio mediante extracción de hashes NTLM y secretos Kerberos

Esta imagen muestra la extraccion de credenciales del dominio AD usando herramientas de volcado de credenciales sobre el controlador de dominio DC01 como es SercretsDump.

Durante el proceso se recuperon hashes NTLM, credenciales Kerberos y secretos asociados a multiples cuentas del dominio incluyendo usuarios estándar, cuentas de servicio y cuentas privilegiadas como Administrator y krbtgt.

Acceso remoto al controlador de dominio

Tras obtener privilegios administrativos se validó el acceso remoto interactivo al controlador de dominio mediante RDP usando credenciales legítimas durante fases anteriores.

Desde el punto de vista operativo, este acceso confirma que tenemos control efectivo sobre el sistema más crítico de la infraestructura pudiendo interactuar directamente con:

- Active Directory.
- Servicios de autenticación.
- Configuración de políticas.
- Usuarios y grupos privilegiados.

Desde la perspectiva analítica, este compromiso introduce una situación especialmente compleja para la detección ya que el acceso se realiza usando mecanismos completamente legítimos del sistema y credenciales válidas.

Aunque el acceso RDP a un controlador de dominio representa una actividad de alto riego, la existencia del evento no implica necesariamente actividad maliciosa, especialmente en entornos donde existen tareas administrativas remotas habituales.

Desde el marco MITRE ATT&CK:

- **T1021.001 – Remote Desktop Protocol**

En términos de detectabilidad:

- Genera eventos de autenticación observables.
- Puede correlacionarse con accesos privilegiados inusuales.
- Requiere análisis contextual del origen y comportamiento de la sesión.

Por esto su detectabilidad puede considerarse media.

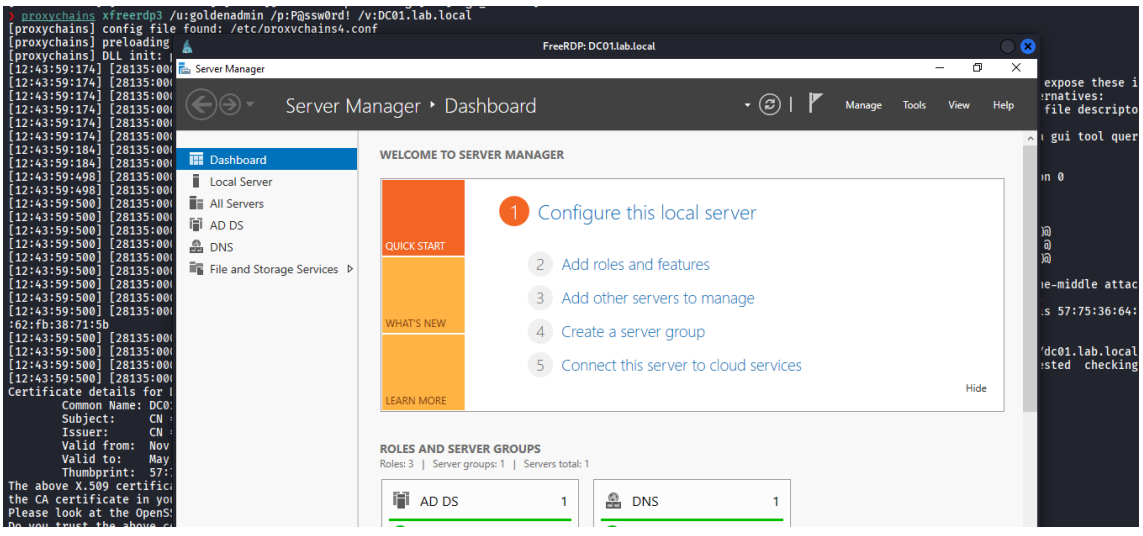

Ilustración 42. Acceso remoto al controlador de dominio mediante credenciales privilegiadas

La imagen muestra el acceso remoto al controlador de dominio DC01 usando el protocolo RDP mediante la cuenta privilegiada “goldenadmin” previamente creada durante las fases de persistencia y compromiso del dominio.

Como resultado se obtiene una sesión interactiva completa sobre el controlador de dominio accediendo directamente al entorno administrativo de Windows Server y disponiendo de control total sobre los servicios críticos de AD.

Validación de privilegios y pertenencia de grupos

Una vez establecido el acceso al controlador de dominio, se verificó la pertenencia de la cuenta creada con Golden Ticket a grupos críticos como Domain Admins y Enterprise Admins, confirmando el nivel máximo de privilegios dentro del entorno.

Asimismo, se analizaron los privilegios asociados a la sesión identificando capacidades típicas de cuentas administrativas:

- Gestión de usuarios y grupos.
- Modificación de políticas de seguridad.
- Acceso completo a recursos del dominio.
- Ejecución de operaciones sensibles del sistema.

Desde el punto de vista analítico, esta fase resulta especialmente relevante porque pone de manifiesto como se dejan de usar técnicas ofensivas complejas y pasamos a operar usando privilegios ya existentes.

Esto provoca que muchas de las acciones posteriores pierdan indicadores claramente anómalos y se integren dentro del comportamiento administrativo esperado.

En términos de detectabilidad:

- Las consultas sobre grupos y privilegios generan poca visibilidad.
- La actividad puede confundirse con administración legítima.
- La detección necesita principalmente del contexto de uso.

Por esto, la detectabilidad puede considerarse baja.

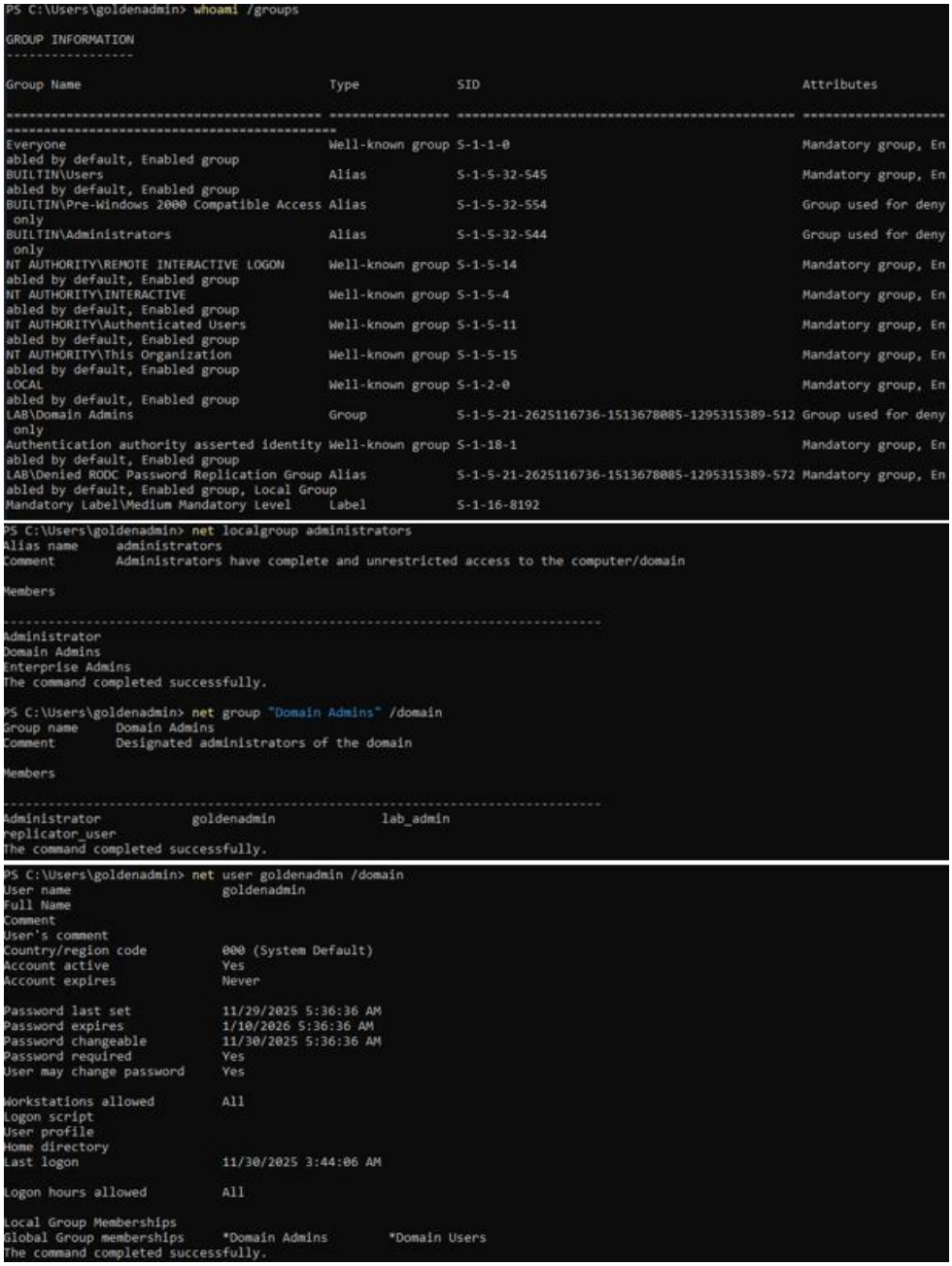

Ilustración 43. Validación de privilegios y pertenencia a grupos privilegiados en Active Directory

Esta imagen muestra la validación de privilegios asociados a la cuenta “goldenadmin”. Mediante comandos administrativos se verifico:

- La pertenencia de la cuenta a grupos privilegiados del dominio.
- Los privilegios administrativos efectivos sobre el sistema.
- El estado y configuración de la cuenta creada.

Como resultado se confirma que la cuenta dispone de privilegios elevados equivalentes a administración completa del dominio permitiendo control total sobre AD y los sistemas asociados.

Enumeración de infraestructura del dominio

Con privilegios ya consolidados se realizaron acciones de enumeración orientadas a validar la estructura crítica del dominio y los componentes responsables de su funcionamiento.

Entre los elementos identificadores se incluyen:

- Controladores de dominio.
- Roles FSMO.

Desde el punto de vista ofensivo, esta información permite comprender mejor la arquitectura de autenticación y administración del entorno facilitando tanto la persistencia como posibles movimientos posteriores si hubiese otros bosques.

Analíticamente esta actividad representa que cuantos más privilegios se poseen, más normales parecen las acciones del sistema. Esto implica que tareas potencialmente criticas pueden resultar prácticamente indistinguibles de actividad administrativa legítima.

Desde el marco MITRE ATT&CK:

- **T1482 – Domain Trust Discovery**
- **T1018 – Remote System Discovery**

En términos de detectabilidad:

- Las consultas LDAP forman parte del funcionamiento habitual.
- No existen indicadores inequívocos de compromiso.
- La actividad requiere correlación contextual avanzada.

Por ello, su detectabilidad se considera baja.

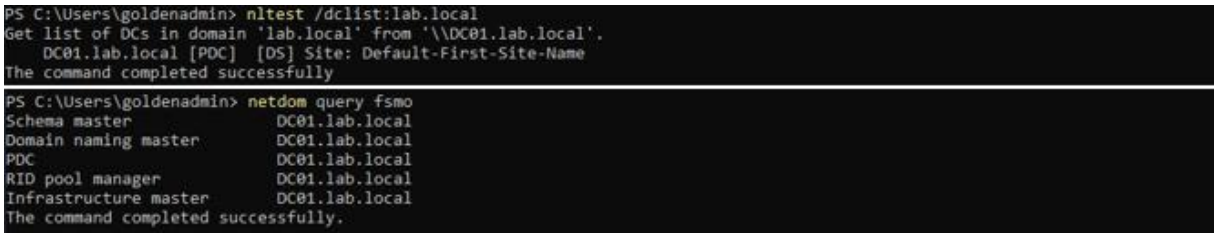

Ilustración 44. Enumeración de infraestructura crítica del dominio Active Directory

La imagen muestra la enumeración de componentes críticos de la infraestructura AD usando comandos administrativos identificando:

- Controladores de dominio asociados a Lab.local.
- Roles FSMO (Flexible Single Master Operations) del dominio.
- Servicios críticos asociados a la administración AD.

Como resultado se confirmó que el servidor DC01de lab.local concentra múltiples roles críticos del dominio como:

- Schema Master.
- Domain Naming Master.
- RID Master.
- PDC Emulator.
- Infrastructure Master.

Conclusiones de la fase

Esta fase final demuestra que hemos alcanzado un compromiso completo del entorno AD mediante el encadenamiento progresivo de múltiples técnicas ejecutadas a lo largo de las fases anteriores.

A diferencia de ataques basados exclusivamente en explotación técnica, el escenario desarrollado pone de manifiesto que el compromiso total del dominio puede alcanzarse principalmente mediante el abuso de relaciones de confianza, configuraciones inseguras y el uso de credenciales válidas.

Desde el punto de vista de la detección se observa un comportamiento especialmente relevante:

- Muchas de las acciones realizadas usan mecanismos legítimos del sistema.
- El uso de privilegios válidos reduce significativamente la visibilidad del ataque.
- Los eventos individuales carecen de capacidad suficiente para identificar el compromiso.
- La detección requiere de la correlación avanzada y análisis de comportamiento.

De forma comparativa, las fases del ataque presentan una menor detectabilidad que determinadas fases iniciales pese a representar un impacto significativamente superior. Esto evidencia una limitación critica de los modelos tradicionales de detección basados exclusivamente en eventos aislados o indicadores estáticos.

Evaluación de detectabilidad de la fase

Técnica	Tipo de señal	Detectabilidad	Justificación
Dumping de credenciales	Replicación y acceso a secretos	Media/Baja	Requiere auditoria específica
Acceso RDP al DC	Inicio de sesión remoto	Media	Actividad observable, pero legítima
Validación de privilegios	Consultas AD	Baja	Comportamiento administrativo
Enumeración de dominio	Consultas LDAP	Baja	Difícil de distinguir del uso normal

Tabla 34. Evaluación de detectabilidad de técnicas de validación de compromiso y control del dominio Active Directory

Esta evaluación refleja que la detectabilidad disminuye progresivamente conforme se va adquiriendo mayores privilegios del dominio.

Se observa que las técnicas con mayor impacto operativo no son las más visibles sino aquellas capaces de integrarse dentro del comportamiento legítimo usando credenciales válidas y funcionalidades administrativas nativas.

Conclusiones generales de la fase ofensiva

A lo largo de las fases se ha demostrado como un entorno AD puede ser comprometido de forma progresiva mediante el encadenamiento de múltiples técnicas reales usadas en ataques avanzados contra infraestructuras corporativas.

El ataque se inicia con actividades de reconocimiento y enumeración que pese a presentar un impacto limitado de forma aislada permiten identificar sistemas críticos, cuentas válidas y relaciones de confianza dentro del dominio. A partir de este punto, el compromiso evoluciona mediante el abuso de configuraciones inseguras, exposición de credenciales y uso de funcionalidades legítimas del sistema hasta alcanzar finalmente el control total del dominio.

Uno de los aspectos más relevantes durante el desarrollo del ataque es que el compromiso no depende de la explotación de una vulnerabilidad critica concreta sino de la acumulación de múltiples debilidades presentes en el entorno. Configuraciones inseguras en recursos SMB,

almacenamiento de credenciales en texto plano, uso de cifrados Kerberos débiles, delegaciones inseguras o privilegios excesivos que han permitido construir una cadena de ataque capaz de evolucionar desde un acceso limitado hasta privilegios equivalentes a Domain Admin.

Desde el punto de vista ofensivo, se observa que las fases iniciales generan una mayor cantidad de actividad visible dentro del entorno. Técnicas como el escaneo de red, Kerbrute o BloodHound producen múltiples consultas, conexiones y solicitudes de autenticación que pueden resultar observables mediante sistemas de monitorización. Sin embargo, aunque estas actividades generan mayor volumen de eventos su identificación depende del análisis contextual debido a que usan protocolos y funcionalidades nativas de Active Directory.

Por el contrario, en fases más avanzadas y con mayores privilegios la detectabilidad disminuye mucho pese a que el impacto operativo aumenta de forma considerable. El uso de credenciales válidas, acceso mediante SMB, abuso de delegaciones Kerberos o autenticación remota sobre sistemas críticos generan eventos válidos dentro del funcionamiento normal del dominio dificultando la diferenciación entre actividad administrativa legítima y comportamiento malicioso.

Este comportamiento pone de manifiesto una de las principales conclusiones obtenidas, las técnicas más peligrosas no son las más ruidosas sino las que se integran dentro del comportamiento legítimo del entorno usando funcionalidades nativas del sistema.

Adicionalmente, se observó que muchas de las acciones realizadas tenían una detectabilidad limitada cuando se analizaban de forma aislada. En la mayoría de las fases, los eventos adquieren más valor real para la detección cuando son interpretados mediante correlación temporal, contextual y multifuente.

En este sentido, el análisis realizado demuestra que la detección efectiva de ataques avanzados en entornos Active Directory no puede depender exclusivamente de firmas o eventos aislados, sino que requiere modelos basados en comportamiento, correlación avanzada y comprensión contextual de la actividad.

Finalmente, las fases que se han desarrollado en este apartado se han permitido validar como técnicas reales alineadas con MITRE ATT&CK pueden ejecutarse usando procedimientos utilizados que se aprovechan capacidades estándar del sistema y generar niveles de visibilidad diferentes en función de la fuente de datos disponible y así reforzando la idea de la importancia de la monitorización centralizada y el análisis contextual en entornos corporativos AD.

5. Análisis de detectabilidad de técnicas en Active Directory

El objetivo de este apartado es analizar la capacidad de detección de las técnicas que se ejecutaron durante las distintas fases que se ejecutaron en el apartado anterior evaluando que evidencias se generan, que fuentes de datos permiten observarlas y hasta qué punto estas actividades pueden diferenciarse del comportamiento legítimo dentro de un entorno corporativo.

A diferencia del anterior apartado que se centraba en la ejecución de los ataques y explotación del dominio junto con un adelanto de la detectabilidad, en esta parte el enfoque se pasa a la visibilidad defensiva del entorno. El propósito principal no es únicamente demostrar que una técnica puede ejecutarse con éxito sino estudiar la huella que deja en los sistemas de monitorización y que nivel de detectabilidad deja realmente.

Para ello todas las acciones realizadas durante el ataque fueron monitorizadas y correlacionadas mediante el stack ELK desplegado en el laboratorio. Este sistema actúa como núcleo del análisis permitiéndome centralizar, indexar y visualizar los eventos generados por las distintas máquinas del dominio. Gracias a esto es posible reconstruir la actividad que hemos generado como atacantes, identificar patrones de comportamiento y analizar las limitaciones observadas durante el proceso de detección.

El análisis se apoya principalmente en varias fuentes de datos:

- Security Logs de Windows, los cuales están encargados de registrar autenticaciones, uso de privilegios, acceso a recursos y eventos relacionados con AD y Kerberos.
- Sysmon, usado para ampliar la visibilidad del sistema mediante eventos detallados sobre la creación de procesos, conexiones de red, ejecución de binarios y actividad interna del host.
- Winlogbeat, empleado para el envío centralizado de eventos Windows hacia Elasticsearch.
- Vector, usado en sistemas Linux para recopilación y envío de logs relacionados con servidores web, bases de datos y actividad del sistema.
- Kibana, se usa como interfaz principal para la correlación y análisis de eventos mediante búsquedas KQL, filtros y dashboards.

El objetivo no consiste únicamente en comprobar si la técnica genera eventos sino en determinar si estos aportan valor real desde el punto de vista defensivo. En muchos casos, determinadas acciones generan registros que resultan ambiguos o difíciles de distinguir de la actividad del dominio, sobre todo cuando el atacante usa mecanismos legítimos como Kerberos, SMB o cuentas válidas.

Por esto, el análisis de detectabilidad se centra especialmente en aspectos como:

- Claridad de los eventos generados.
- Necesidad de correlación entre múltiples fuentes.
- Dependencia de Sysmon para aumentar la visibilidad.
- Diferencia entre actividad legítima y comportamientos maliciosos.
- Limitaciones observadas en los mecanismos de logging nativos de Windows.

Finalmente, este capítulo lo que busca es transformar el laboratorio desplegado en un modelo de análisis de detectabilidad que nos permita extraer conclusiones prácticas sobre que ataques son claramente visibles, cuales necesitan correlación avanzada y cuales pueden pasar prácticamente desapercibidos incluso en entornos monitorizados.

Metodología de evaluación

Con el objetivo de aportar una evaluación consistente y reproducible de la capacidad de detección del entorno, se definió una metodología basada en el análisis de eventos generados durante la ejecución de las técnicas ofensivas sobre el dominio AD.

Esta metodología no se centra únicamente en verificar si una acción genera logs, sino en evaluar si estos eventos proporcionan información útil desde el punto de vista defensivo y permite identificar actividad potencialmente maliciosa dentro de un entorno corporativo.

Para esto, mientras se ejecutaban las técnicas alineadas con el framework de MITRE ATT&CK, estas se monitorizan los eventos producidos tanto en el controlador de dominio como en workstations y servidores. Tras esto, los eventos se centralizaron los eventos y correlacionaron en ELK con el objetivo de analizar la visibilidad obtenida en cada fase del ataque.

El proceso de evaluación se realiza considerando los siguientes factores:

- Eventos generados por cada técnica.
- Fuente desde la que se obtiene la evidencia.
- Nivel de detalle disponible en los logs.
- Capacidad de detalle disponible en los logs.
- Capacidad de correlación entre eventos.
- Dificultad para diferenciar actividad legítima de actividad maliciosa.
- Dependencia de herramientas adicionales como Sysmon.

De esta forma el análisis no se limitará solo a documentar las evidencias sino que busca determinar que técnicas resultan claramente detectables, cuales solo resultan claramente identificables cuando se relacionan eventos procedentes de distintas fuentes de datos y cuales presentan una visibilidad reducida incluso en entornos monitorizados.

Fuentes de datos analizadas

La capacidad de detección del laboratorio depende directamente de las fuentes de datos disponibles y del nivel de visibilidad proporcionado por cada una de estas. Durante el análisis se usaron distintas fuentes de eventos procedentes tanto de sistemas Windows como Linux, todas ellas centralizadas en ELK para facilitar su correlación y análisis conjunto.

Security Logs

Registros de seguridad nativos de Windows que constituyen una de las principales fuentes de información dentro del laboratorio. Estos eventos fueron recopilados principalmente desde el controlador de dominio DC01 y desde las estaciones de trabajo unidas al dominio.

Los Security Logs proporcionan información de:

- Autenticaciones Kerberos y NTLM.
- Inicios y cierres de sesión.
- Acceso a recursos compartidos.
- Uso de privilegios.
- Cambios sobre cuentas, grupos y objetos del dominio.
- Solicitudes de tickets Kerberos.

Eventos como identificadores 4624, 4625, 4768, 4769, 4672 o 4662 son muy relevantes durante el análisis de técnicas como password spraying, Kerberoasting, movimiento lateral o DCSync.

Sin embargo, aunque estos registros permiten obtener visibilidad sobre gran parte de la actividad del dominio presentan limitaciones importantes en cuanto al detalle contextual disponible, especialmente en técnicas que usan mecanismos propios del entorno Windows.

Sysmon

Con el objetivo de ampliar la capacidad de monitorización se desplegó Sysmon en todas las máquinas del dominio. Este proporciona eventos mucho más detallados que los registros nativos de Windows dándonos visibilidad sobre:

- Creación de procesos.
- Relaciones parent-child entre procesos.
- Ejecución de herramientas ofensivas.

- Conexiones de red.
- Carga de DLLs y binarios.
- Persistencia y modificaciones del sistema.

Durante el análisis, Sysmon resultó especialmente útil para detectar actividad que apenas generaba evidencias dentro de Security Logs como la ejecución de herramientas postexplotación, uso de LOLBins o transferencia de binarios.

Además, permitió correlacionar procesos concretos con conexiones de red o autenticaciones observadas en otros registros aumentado la trazabilidad de determinadas técnicas ofensivas.

Por otro lado, Sysmon aumentó considerablemente el volumen de eventos generados haciendo necesario aplicar filtros y correlaciones para reducir el ruido y centrarse en los eventos relevantes.

Logs Linux

Los sistemas Linux presentes en el laboratorio también generaron registros relevantes durante el desarrollo de las fases ofensivas sobre todo en SQL01.

Estos logs fueron recopilados por Vector e incluían información relacionada con:

- Accesos al servidor web.
- Actividad sobre base de datos.
- Errores de autenticación.
- Ejecución de servicios
- Conexiones de red y actividad del sistema.

Aunque la visibilidad obtenida en sistemas Linux es menor que en los sistemas Windows monitorizados por Sysmon, estos registros también son útiles para correlacionar accesos a servicios web y bases de datos con eventos observados posteriormente en AD.

Esto permitió analizar ataques que involucraban múltiples sistemas y observar cómo determinadas técnicas generaron evidencias distribuidas entre diferentes fuentes de datos.

Elasticsearch y Kibana

Todos los eventos recopilados fueron centralizados en Elasticsearch y posteriormente analizados mediante Kibana, convirtiendo ELK en el núcleo principal del análisis de detectabilidad.

El uso de Kibana permitió:

- Realizar búsquedas mediante consultas KQL.
- Correlacionar eventos entre distintos sistemas.
- Filtrar eventos por usuario, host y EventID.
- Construir dashboards orientados a detección.
- Analizar secuencias temporales de actividad ofensiva.

Gracias a esta centralización fue posible reconstruir el comportamiento que hicimos como atacantes a lo largo de las distintas fases del compromiso del dominio y evaluar que técnicas generaban evidencias claras y cuales requerían correlación avanzada entre múltiples eventos para ser identificadas correctamente.

Además, ELK permitió también observar una de las principales conclusiones del laboratorio, que es que la existencia de logs no implica necesariamente capacidad de detección ya que muchas técnicas únicamente resultan identificables cuando varios eventos eran correctamente correlacionados dentro del SIEM.

Criterios de detectabilidad

Con el objetivo de poder realizar una evaluación homogénea de las distintas técnicas ofensivas ejecutadas, se definió varios niveles de detectabilidad en función de la calidad, claridad y capacidad de correlación de los eventos generados.

Estos criterios permiten clasificar cada técnica no solo por la existencia de logs asociados sino por la capacidad real que tendría un analista de seguridad para identificar comportamiento malicioso a partir de las evidencias del SIEM.

Uno de los aspectos más importantes durante el análisis fue comprobar que la generación de eventos no implica necesariamente una detección efectiva. En numerosos casos, las acciones ejecutadas producen registros válidos dentro del sistema pero estos pueden resultar ambiguos, insuficientes o difíciles de diferenciar de actividad legítima del dominio.

Por esto la detectabilidad de cada técnica se evaluó teniendo en cuenta factores como:

- La claridad de los eventos generados.
- Facilidad de correlación de eventos.
- Dependencia de Sysmon u otras fuentes.
- Nivel de ruido generado en el entorno.
- Diferenciación respecto a actividad legítima.
- Necesidad de contexto adicional para interpretar la evidencia.

A partir de estos se definieron 4 niveles principales de detectabilidad:

Alta	La técnica genera eventos claros, identificables y fácilmente correlacionables. La actividad puede detectarse de forma relativamente fiable mediante consultas o reglas básicas en ELK
Media	La técnica genera evidencias útiles pero requiere de correlación adicional, análisis temporal o contexto específico para diferenciarla correctamente de actividad legítima
Baja	Los eventos que se generan son ambiguos o similares a comportamiento normal del entorno. La detección resulta compleja y depende en gran medida del conocimiento previo o de fuentes adicionales como Sysmon
Nula	La técnica no genera apenas logs relevantes o la visibilidad disponible es insuficiente para identificarla de forma fiable mediante los mecanismos de logging desplegados

Tabla 35. Criterios de clasificación de detectabilidad utilizados en el análisis de técnicas ofensivas sobre Active Directory

Esta clasificación permite establecer una comparativa directa entre las técnicas del laboratorio y evaluar que mecanismos nos ofrecen una mayor capacidad de detección dentro del entorno AD monitorizado.

Además, estos niveles nos muestran que las técnicas que usan funcionalidades legítimas de Active Directory como Kerberos, SMB o reutilización de tickets suelen presentar una detectabilidad significativamente menor que aquellas que generan eventos administrativos anómalos o accesos privilegiados claramente identificables.

Por otro lado, también se observó que la detectabilidad no depende solo de la técnica empleada sino de factores adicionales como la configuración de auditoría, la presencia de Sysmon, el nivel de correlación implementado en ELK y el volumen de actividad legítima existente en el entorno. Esto implica que una misma técnica puede presentar distintos niveles de visibilidad dependiendo de la madurez del sistema de monitorización desplegado lo que convierte la correlación y el análisis contextual en elementos fundamentales dentro del proceso de detección.

Limitaciones del análisis

Aunque el laboratorio ha permitido reproducir múltiples técnicas reales contra el entorno AD y analizar su visibilidad a través de ELK es importante destacar que el análisis presenta una serie de limitaciones que deben tenerse en cuenta a la hora de interpretar los resultados obtenidos. Esto resulta fundamental para contextualizar correctamente las conclusiones extraídas y evitar asumir que los resultados observados pueden extrapolarse directamente a cualquier entorno corporativo real.

Además, muchos factores que afectan a la detectabilidad dependen directamente de la configuración del entorno, volumen de actividad y herramientas defensivas desplegadas.

Entorno controlado y reducido

El laboratorio se ha desarrollado en un entorno completamente controlado compuesto por un número reducido de máquinas y usuarios. Aunque esto facilita el análisis y análisis contextual de la actividad, también reduce el ruido presente en entornos reales.

En infraestructuras empresariales con cientos de equipos los eventos relacionados con autenticaciones, accesos SMB, ejecución de procesos o solicitudes Kerberos son mucho más frecuentes lo que dificulta la identificación de actividad anómala.

Por esto determinadas técnicas que en el laboratorio resultan claramente visibles, podrían pasar más desapercibidas en entornos reales que tengan mayor volumen de eventos legítimos.

Defensas desactivadas deliberadamente

Para poder ejecutar todas las técnicas ofensivas sin interferencias los mecanismos de defensa del entorno fueron desactivados de forma intencionada. Esto incluye los antivirus, restricciones avanzadas de ejecución y determinados controles de seguridad Windows.

Esta decisión permite estudiar de forma aislada las evidencias generadas por cada técnica pero también implica que el comportamiento observado no representa completamente un entorno real donde muchas herramientas ofensivas podrían haber sido bloqueadas antes incluso de generar determinados eventos.

Además, la ausencia de mecanismos preventivos favorece que algunas técnicas generen una trazabilidad mucho más limpia y observable de lo habitual.

Ausencia de soluciones EDR

El laboratorio no incorpora soluciones EDR usando únicamente logs nativos Windows, Sysmon y centralización en ELK. Esto supone una limitación importante ya que muchas plataformas EDR modernas incorporan capacidades avanzadas:

- Correlación automática.
- Análisis de comportamiento.
- Detección basada en anomalías.
- Trazabilidad de procesos.
- Detección de técnicas MITRE ATT&CK.
- Análisis de memoria y telemetría avanzada.

Como consecuencia, algunas técnicas que en este laboratorio presentan baja detectabilidad podrían resultar más visibles en entornos EDR correctamente configurados.

Por otro lado, esta ausencia también permite analizar con mayor claridad las limitaciones reales de los mecanismos de logging tradicionales en AD sin depender de herramientas avanzadas de terceros.

Dependencia de la configuración de auditoria

La visibilidad obtenida durante el análisis depende directamente de la configuración de auditoria aplicada sobre el dominio y los sistemas Windows.

Muchos de los eventos observados durante el laboratorio únicamente están disponibles cuando determinadas políticas de auditoria avanzada se encuentran habilitadas. En caso contrario, técnicas relevantes como DCSync, abuso de Kerberos o determinados accesos privilegiados pueden generar una visibilidad significativamente menor.

Esto implica que la detectabilidad observada no depende solo de la técnica usada, sino también del nivel de auditoria previamente desplegado en el entorno.

Correlación limitada y análisis manual

Aunque ELK permite centralizar y consultar eventos de múltiples fuentes, gran parte de la correlación realizada se realizó manualmente mediante búsquedas KQL y análisis temporal.

No se implementó un sistema avanzado de reglas automatizadas ni motores complejos de correlación entre eventos por lo que algunas técnicas requieren interpretación manual para poder ser identificadas.

Esto refleja una situación habitual en muchos entornos reales donde la existencia de logs no garantiza necesariamente una capacidad de detección efectiva sin reglas adecuadas o personal especializado que interprete las evidencias generadas.

Limitaciones propias de los logs de Windows

Los mecanismos de loggins nativos de Windows presentan limitaciones importantes desde el punto de vista ofensivo. Muchas acciones que se han realizado generaron eventos genéricos o ambiguos que resultan difíciles de distinguir de actividad administrativa legítima.

Técnicas como el movimiento lateral mediante SMB, reutilización de credenciales o uso de tickets Kerberos válidos pueden integrarse dentro del comportamiento normal del dominio dificultando enormemente su identificación sin un mayor contexto. Esto provoca que la detectabilidad no dependa únicamente de la existencia de eventos sino de la capacidad de contextualizar correctamente el comportamiento.

En consecuencia, uno de los principales hallazgos del laboratorio es que la monitorización basada únicamente en eventos aislados resulta insuficiente frente a técnicas avanzadas que usan funcionalidades legítimas del sistema.

Limitaciones temporales y de persistencia

El laboratorio se centró principalmente en la ejecución controlada de técnicas ofensivas y en el análisis de los eventos generados durante cada fase. Sin embargo, no se evaluaron escenarios prolongados de persistencia a largo plazo ni ataques distribuidos a lo largo de periodos extensos de tiempo.

En entornos reales, muchos atacantes operan de forma gradual y silenciosa durante semanas o meses reduciendo la generación de eventos sospechosos y dificultando aún más la detección basada en correlación temporal. Por lo tanto, los resultados obtenidos representan principalmente visibilidad de técnicas ejecutadas en ventanas temporales cortas y controladas.

En conjunto todas estas limitaciones reflejan que la detectabilidad observada durante el laboratorio debe interpretarse como una aproximación práctica al comportamiento real de los sistemas de monitorización pero no como una representación absoluta de todos los escenarios posibles. La capacidad de detección, por tanto, depende en gran medida del contexto operativo, del nivel de auditoria desplegado y la madurez de las herramientas defensivas usadas.

Tabla global de detectabilidad

Se elaboró una tabla global de detectabilidad en la que se relacionan las fases ofensivas, las técnicas empleadas, identificadores MITRE asociados y las principales evidencias observadas durante el análisis.

Esta tabla es el núcleo principal del análisis defensivo del trabajo ya que permite estudiar de forma estructurada que técnicas generan eventos claramente identificables, cuales requieren correlación avanzada y cuales presentan una visibilidad reducida incluso en un entorno de monitorización mediante ELK.

Además de los eventos generados, también se incluyen las principales fuentes de datos implicadas y observaciones relacionadas con la calidad de la detección, el ruido generado o las limitaciones observadas durante el análisis.

Uno de los aspectos más relevantes observados durante la elaboración de esta tabla es que la detectabilidad no depende únicamente de la técnica usada sino también del contexto en el que se ejecuta, del nivel de auditoria configurado y de la capacidad de correlación disponible en el SIEM. Hay técnicas que generan eventos muy claros en el controlador de dominio y pueden

resultar difíciles de interpretar sin contexto adicional, mientras que otras que apenas dejan evidencias visibles pese a comprometer completamente el dominio.

Fase	Técnica	MITRE ATT&CK	Eventos clave	Fuente principal	Detectabilidad	Observaciones
1	Pivoting mediante Chisel SOCKS	T1090.001	Sysmon ID 5	Sysmon Endpoint	Baja	Difícil de detectar sin reglas específicas orientadas a túneles y tráfico anómalo
1	Escaneo de red y descubrimiento de servicios	T1046	Event ID 5156	Endpoint Security Logs	Media	El tráfico generado puede confundirse fácilmente con inventariado o administración legítima
1	Reconocimiento mediante Kerbrute	T1087.002	Event ID 4771	DC01 Security Logs	Alta	Genera ruido en el controlador de dominio, pero requiere umbrales y correlación temporal
1	Enumeración Active Directory (BloodHound / SharpHound)	T1087.002 / T1069.002 / T1482	Sysmon ID 5	Sysmon	Media	Muy dependiente de Sysmon; LDAP resulta difícil de distinguir de actividad administrativa
2	Acceso SMB y shares expuestos	T1021.002 / T1135	Event ID 5140	Endpoint Security Logs	Baja	Actividad muy similar al uso normal de recursos compartidos
2	Obtención de credenciales en shares	T1552.001	Event ID 5145	Endpoint Security Logs	Baja	Solo destaca si existe monitorización específica sobre archivos sensibles
2	Password Spraying	T1110.003	Event ID 4625	DC01 Security Logs	Alta	Patrón claramente identificable mediante correlación temporal y volumen de fallos
3	Kerberoasting	T1558.003	Event ID 4769 (RC4)	DC01 Security Logs	Alta	Muy detectable cuando se analizan solicitudes TGS con cifrado RC4
3	Obtención y crackeo de credenciales svc-web	-	No genera eventos relevantes tras la extracción	Host atacante	Nula	El crackeo offline reduce considerablemente la visibilidad defensiva

3	Acceso a recursos mediante cuenta comprometida	T1078.002	Event ID 4624	DC01 Security Logs	Baja	El uso de credenciales válidas resulta muy difícil de distinguir de actividad legítima
3	Abuso de delegación Kerberos (S4U)	T1550 / T1134	EventID 4769	DC01 Security Logs	Baja	Muy difícil de distinguir sin contexto sobre delegación legítima
4	Acceso a SQL01	T1078 / T1213	EventID 4624	DC01 Security Logs	Baja	Desde el punto de vista del sistema se comporta como acceso legítimo
4	Exposición de credenciales en base de datos	T1552	Logs SQL, acceso a tablas sensibles	SQL02 Server Logs	Nula	Depende completamente del nivel de auditoría SQL habilitado
4	Acceso a SQL02	T1078.002	Event ID 4624	DC01 Security Logs	Baja	Desde el punto de vista del sistema se comporta como acceso legítimo
4	Activación de xp_cmdshell	T1059 / T1505.001	EventID 15457	SQL02 Security Logs	Alta	Muy visible cuando sqlservr.exe ejecuta cmd.exe o powershell.exe
5	PrintSpoofer (Privilege Escalation)	T1068	Sysmon ID 5	Sysmon Endpoint	Media	Requiere monitorización detallada de procesos y elevaciones
5	Ejecución de Mimikatz	T1003.001	Sysmon ID 5, EventID 4688	Sysmon y Security Logs del Endpoint	Alta	Muy detectable si Sysmon está correctamente configurado
5	DCSync	T1003.006	EventID 4662	DC01 Security Logs	Alta	Uno de los indicadores más claros de compromiso del dominio
5	Golden Ticket	T1558.001	EventID 4672	DC01 Security Logs	Baja	Difícil de detectar sin correlación avanzada y análisis de comportamiento
5	Creación de usuario privilegiado (goldenadmin)	T1136.002	EventID 4662	DC01 Security Logs	Alta	La creación de cuentas y su inclusión en grupos privilegiados genera eventos

						administrativos muy visibles
5	Silver Ticket	T1558.002	EventID 4624	MSSQL / Servicio objetivo	Baja	No requiere interacción con el DC, reduciendo enormemente la visibilidad
5	Persistencia mediante creación de usuario	T1098 / T1505.001	Logs SQL	SQL02 Server Logs	Nula	Evento en base de datos no registrado
6	Silver Ticket sobre servicio web	T1558.002	EventID 4624	IIS / Servicio objetivo	Baja	No genera solicitudes visibles al controlador de dominio
6	Abuso Kerberos sobre servicios web	T1550	EventID 4624	IIS / Endpoint	Baja	El acceso aparece como autenticación legítima al servicio
7	Dump de credenciales del dominio	T1003	EventID 4662	DC01 Security Logs	Alta	Muy visible cuando existe acceso a LSASS o replicación AD
7	Acceso RDP al controlador de dominio	T1021.001	EventID 4624 (LogonType 10)	DC01 Security Logs	Alta	Acceso remoto privilegiado fácilmente identificable
7	Uso de privilegios elevados	T1018 / T1482	EventID 4672	DC01 Security Logs	Alta	Indicador claro de sesión privilegiada dentro del dominio

Tabla 36. Tabla global de detectabilidad de técnicas ofensivas utilizadas en el entorno Active Directory monitorizado

A partir de esta tabla pueden extraerse varias conclusiones relevantes. En primer lugar, las técnicas relacionadas con abuso Kerberos como Kerberoasting o DCSync generan eventos muy útiles desde el punto de vista defensivo debido a la existencia de indicadores concretos y fácilmente correlacionables en los Security Logs del DC.

Por el contrario, técnicas basadas en reutilización de credenciales válidas, acceso SMB o uso de tickets falsificados presentan una detectabilidad considerablemente menor ya que gran parte de su actividad se integra dentro del comportamiento legítimo habitual del dominio.

También se observa una fuerte dependencia de Sysmon para detectar técnicas relacionadas con ejecución de procesos, LOLBins, transferencia de archivos o explotación local. Sin Sysmon muchas de estas acciones apenas dejarían trazabilidad suficiente para ser analizadas.

Finalmente, la tabla pone de manifiesto una de las principales ideas del trabajo. La existencia de logs no garantiza la capacidad de detección, en numerosos casos, la identificación real de actividad maliciosa depende de la correlación entre múltiples eventos del contexto operativo y del conocimiento previo del comportamiento habitual del entorno.

Análisis de detectabilidad por fases

Una vez definida la metodología de evaluación y establecida la tabla global de detectabilidad, en este apartado se realiza un análisis detallado de cada una de las fases ofensivas ejecutadas durante el laboratorio.

El objetivo es estudiar que evidencias generó cada técnica, que capacidad real de detección ofrecieron los mecanismos de monitorización desplegados y cuáles fueron las principales limitaciones observadas durante el análisis.

A diferencia del capítulo ofensivo centrado en la ejecución de ataques, esta sección se enfoca desde una perspectiva defensiva analizando la calidad de los eventos generados, la dificultad de interpretación y el nivel de correlación necesario para identificar comportamientos maliciosos dentro de AD.

Uno de los aspectos más relevantes observados durante el laboratorio es que muchas técnicas generan eventos válidos dentro del sistema pero estos no siempre resultan fácilmente distinguibles de actividad legítima. En consecuencia, la detectabilidad no depende de la existencia de logs sino de la capacidad de contextualización de la información disponible y correlacionar múltiples evidencias entre distintos sistemas.

Fase 1 – Reconocimiento de la red interna

La primera fase del ataque estuvo orientada al reconocimiento interno del dominio AD y a la obtención de la información sobre infraestructura desplegada. Durante esta etapa se realizaron técnicas de pivoting, escaneo de red, enumeración Kerberos y recolección de información estructural del dominio mediante herramientas como Chisel, Nmap, Kerbrute y BloodHound.

Desde el punto de vista defensivo, esta fase es de especial relevancia debido a que gran parte de las acciones ejecutadas usan protocolos legítimos del entorno corporativo como LDAP, SMB o Kerberos dificultando actividad maliciosa de comportamiento administrativo normal.

Pivoting mediante Chisel SOCKS

Esta primera técnica usada consistió en la creación de un túnel SOCKS mediante Chisel para redirigir tráfico hacia la red interna comprometida desde el host atacante. Esta actividad se corresponde con la técnica MITRE T1090.001 – Internal Proxy, una técnica frecuentemente usada para realizar pivoting y ocultar el origen real de las conexiones durante fases de postexplotación.

Desde el punto de vista defensivo, la visibilidad obtenida sobre esta actividad fue reducida. Los mecanismos nativos de auditoría de Windows apenas generaron evidencias relevantes sobre el túnel establecido por lo que la principal fuente de telemetría fue Sysmon.

Durante el análisis realizado en Kibana se identificaron varios eventos asociados al binario chisel.exe:

- Sysmon EventID 5: Terminación de proceso (Process terminated)

Se adjunta un log de muestra:

> {"message":"Process terminated: RuleName: - UtcTime: 2025-11-24 14:10:41.622 ProcessGuid: {28CFCBDB-47E9-6924-5803-000000000C00} ProcessId: 11540 Image: C:\\Tools\\Chisel\\chisel.exe User: CLIENT2\\david","winlog.event_data.Image":"C:\\Tools\\Chisel\\chisel.exe","@metadata.beat":"wi

nlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T15:10:41.622Z","agent.ephemeral_id":"2c4476db-c773-4ed3-b074-a3e0b74e1a64","agent.id":"cf1afe44-e1e1-47c1-a7b6-e8c57fda5efb","agent.name":"CLIENT2","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Process terminated (rule: ProcessTerminate)","event.code":"5","event.created":"2025-11-24T15:10:43.008Z","event.kind":"event","event.provider":"Microsoft-Windows-Sysmon","log.level":"information","source_type":"logstash","timestamp":"2025-11-24T15:10:41.622Z","winlog.channel":"Microsoft-Windows-Sysmon/Operational","winlog.computer_name":"CLIENT2.lab.local","winlog.event_data.ProcessGuid":"{28CFCBDB-47E9-6924-5803-000000000C00}","winlog.event_data.ProcessId":"11540","winlog.event_data.RuleName":"-","winlog.event_data.User":"CLIENT2\\david","winlog.event_data.UtcTime":"2025-11-24 14:10:41.622","winlog.event_id":"5","winlog.opcode":"Info","winlog.process.pid":"3488","winlog.process.thread.id":"4508","winlog.provider_guid":"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}","winlog.provider_name":"Microsoft-Windows-Sysmon","winlog.record_id":"1979","winlog.task":"Process terminated (rule: ProcessTerminate)","winlog.user.domain":"NT AUTHORITY","winlog.user.identifier":"S-1-5-18","winlog.user.name":"SYSTEM","winlog.user.type":"User","winlog.version":"3","_id":"j_o0tpoB11Fbndj0Bj5F","_ignored":"-","_index":"vector-2025.11.24","_score":17.178}

El registro generado permitió obtener una trazabilidad parcial sobre la ejecución de la herramienta ofensiva identificando:

- El binario usado en el pivoting.
- La ruta completa desde la que fue ejecutado.
- El usuario asociado a la cuenta comprometida.
- El endpoint afectado dentro del dominio.

La consulta KQL usada para localizar esta actividad relacionada con Chisel fue:

event.code:5 AND winlog.event_data.Image: *chisel*

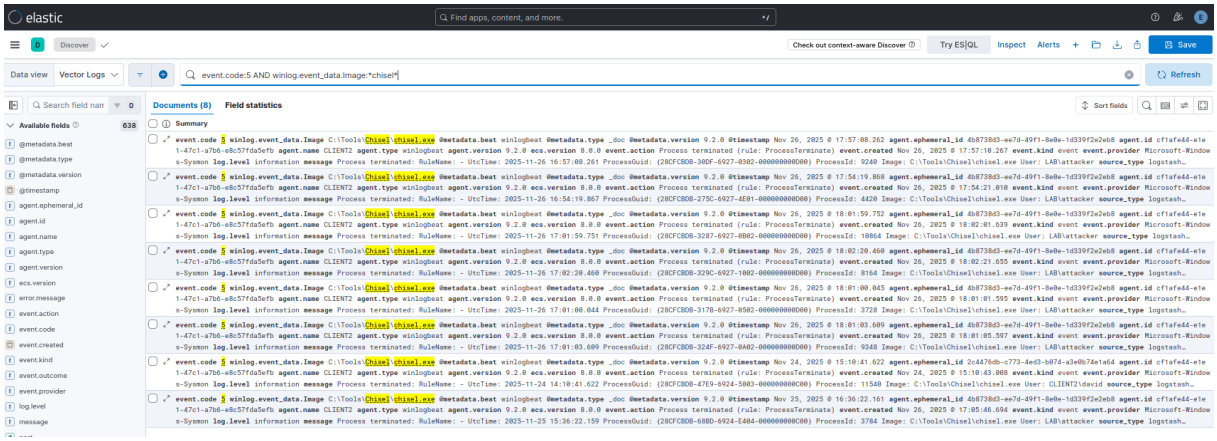

Ilustración 45. Eventos generados por la ejecución de Chisel en CLIENT2 mediante la cuenta LAB\attacker

En esta imagen podemos ver una volumetría de 8 eventos de chisel.exe generados desde CLIENT2 y por el usuario LAB\attacker.

La capacidad de detección depende en gran medida de:

- La monitorización avanzada proporcionada por Sysmon.
- Reglas especificar orientadas a herramientas de tunneling o pivoting.
- Correlación adicional con conexiones anómalas.
- Contextualización temporal respecto a otras actividades ofensivas del entorno.

Adicionalmente pudimos ver que herramientas como Chisel pueden ser fácilmente renombradas o ejecutadas desde rutas menos sospechosas reduciendo significativamente la efectividad de reglas basadas exclusivamente en nombres de binarios.

Desde la perspectiva defensiva, esta limitación resulta especialmente relevante ya que el comportamiento registrado comparte similitudes con herramientas legítimas de administración remota y software corporativo que usan conexiones persistentes o mecanismos de proxy internos. Como consecuencia de esto, diferenciar actividad ofensiva de comportamiento administrativo legítimo únicamente a partir de los eventos es complejo sin añadir correlación, hashes y contextualización.

Por ello, la detectabilidad de esta técnica se considera baja siendo actividad altamente dependiente de telemetría avanzada y de capacidades de correlación dentro del SIEM para poder ser identificada correctamente dentro del AD.

Escaneo de red y descubrimiento de servicios

Una vez establecido el pivoting hacia la red interna se realizaron tareas de descubrimiento de hosts y enumeración de servicios accesibles dentro del dominio. Esta actividad corresponde con la técnica MITRE T1046 – Network Service Discovery.

Durante esta fase se ejecutaron conexiones hacia distintos servicios internos del entorno Active Directory con el objetivo de identificar recursos accesibles, puertos expuestos y posibles vectores posteriores de enumeración y movimiento lateral. A diferencia de técnicas más avanzadas ejecutadas en fases posteriores, el reconocimiento inicial genero evidencias que eran poco concluyentes y altamente dependientes de contexto.

La principal fuente de evidencias identificada fue eventos de seguridad:

- EventID 5156: The Windows Filtering Plataform has permitted a connection.

Se adjunta log de muestra:

{"message":"The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 776 Application Name: \\device\\harddiskvolume3\\windows\\system32\\lsass.exe Network Information: Direction: Inbound Source Address: 192.168.109.12 Source Port: 55444 Destination Address: 192.168.109.10 Destination Port: 389 Protocol: 6 Interface Index: 6 Filter Information: Filter Origin: Unknown Filter Run-Time ID: 0 Layer Name: Receive/Accept Layer Run-Time ID: 44 Remote User ID: S-1-0-0 Remote Machine ID: S-1-0-0","winlog.event_data.DestPort.keyword":"389","winlog.event_data.SourceAddress":"192.168.109.12","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T16:21:02.535Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Filtering Platform Connection","event.code":"5156","event.created":"2025-11-24T16:21:03.909Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-11-24T16:21:02.535Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.Application":"\\device\\harddiskvolume3\\windows\\system32\\lsass.exe","winlog.event_data.DestAddress":"192.168.109.10","winlog.event_data.DestPort":"389","winlog.event_data.Direction":"Inbound","winlog.event_data.FilterOrigin":"Unknown","winlog.event_data.FilterRTID":"0","winlog.event_data.InterfaceIndex":"6","winlog.event_data.LayerName":"Receive/Accept","winlog.event_data.LayerRTID":"44","winlog.event_data.ProcessID":"776","winlog.event_data.Protocol":"6","winlog.event_data.RemoteMachineID":"S-1-0-0","winlog.event_data.RemoteUserID":"S-1-0-0","winlog.event_data.SourcePort":"55444","winlog.event_id":"5156","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"4","winlog.process.thread.id":"5720","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1509951","winlog.task":"Filtering Platform Connection","winlog.version":"1","_id":"J5d0tpoBScXz9zJbZqil","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":9.688}

Estos registros permitieron identificar conexiones entrantes hacia servicios internos expuestos en DC01, CLIENT1, CLIENT3... relacionados con servicios como SMB, LDAP, Kerberos, WinRM o RDP.

La KQL usada para localizar conexiones asociadas a puertos comúnmente usados durante la fase de reconocimiento fue:

```
winlog.event_data.DestPort.keyword :(20 OR 21 OR 22 OR 23 OR 25 OR 53 OR 67 OR 68 OR 69 OR 80 OR 88 OR 110 OR 123 OR 135 OR 137 OR 138 OR
```

139 OR 143 OR 161 OR 162 OR 389 OR 443 OR 445 OR 3389 OR 5985 OR 5986) and "192.168.109.12"

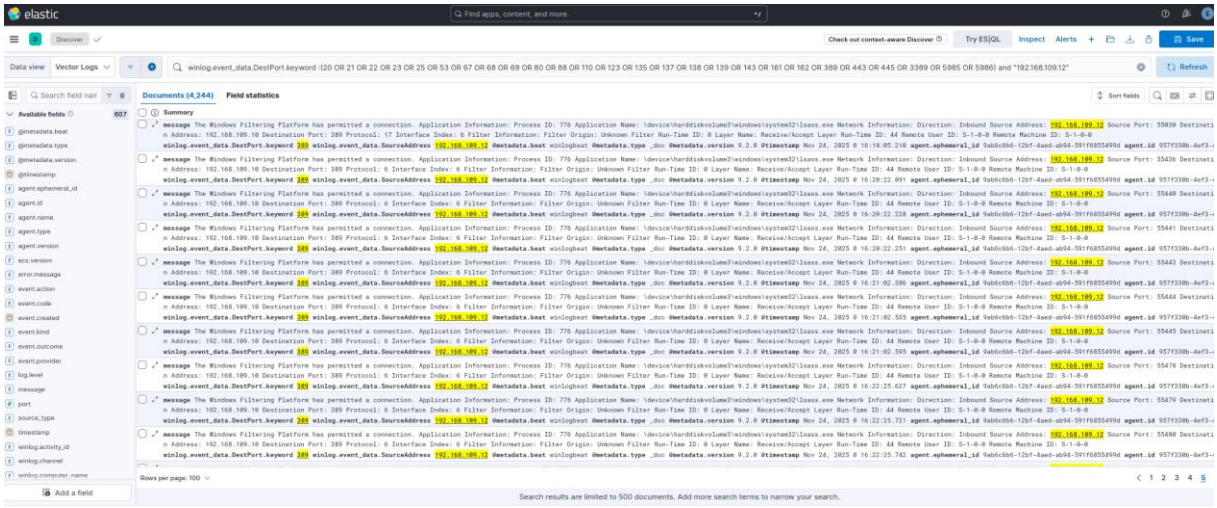

Ilustración 46. Eventos de tráfico permitido (Event ID 5156) generados durante el escaneo de red desde la IP 192.168.109.12 hacia servicios internos del dominio

En esta imagen, se muestra una volumetría total de 4.244 eventos de tráfico permitido hacia los hosts generando eventos desde la IP "192.168.109.12" con EventID 5156 a través de los puertos más comunes, en este caso los 389, y sensibles en escaneos de red.

El análisis temporal de los eventos permitió observar múltiples conexiones hacia servicios críticos del dominio desde sistemas internos, pero uno de los principales problemas detectados durante esta fase es que los eventos 5156 únicamente reflejan conexiones permitidas por el SO sin aportar contexto suficiente sobre la intención real de la actividad.

Desde la perspectiva defensiva, esta limitación resulta relevante en entornos AD debido a que gran parte del tráfico observado comparte características similares. Como consecuencia, diferenciar un escaneo ofensivo de comportamiento legítimo únicamente a partir de estos eventos resulta complejo sin mecanismos de correlación, análisis de frecuencia o telemetría avanzada de red.
Además, los registros obtenidos no permiten identificar directamente herramientas concretas de reconocimiento ni determinar de forma precisa si las conexiones observadas forman parte de actividad maliciosa o de procesos normales del entorno.

Por esto, la detectabilidad de esta técnica se considera media/baja ya que, aunque existen evidencias parciales relacionadas con conexiones internas hacia servicios crítico, la visibilidad resulta insuficiente para atribuir de manera fiable la actividad a un proceso claro de reconocimiento ofensivo.

Enumeración de usuarios mediante Kerbrute

Tras la fase inicial de reconocimiento de servicios internos se realizó enumeración de usuarios validos del dominio mediante Kerbrute usando solicitudes Kerberos contra el controlador de dominio. Esta actividad se corresponde con la técnica MITRE t1087.002 – Domain Account Discovery, y constituye una de las técnicas más habituales para válidas cuentas existentes dentro de entornos AD sin necesidad de autenticarse.

A diferencia de otras técnicas de reconocimiento ejecutadas previamente, la enumeración mediante Kerberos genero evidencias mucho más visibles sobre el controlador de dominio DC01, principalmente a través de eventos relacionados con el servicio de autenticación Kerberos.

Los principales eventos fueron los siguientes y se adjunta un log para cada uno:

- EventID 4771: Kerberos pre-authentication failed.

Se adjunta log de muestra:

{"event.code":"4771","winlog.event_data.IpAddress":"::ffff:192.168.109.12","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T17:05:53.586Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Kerberos Authentication Service","event.created":"2025-11-24T17:05:53.867Z","event.kind":"event","event.outcome":"failure","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"Kerberos pre-authentication failed. Account Information: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1125 Account Name: attacker Service Information: Service Name: krbtgt/LAB Network Information: Client Address: ::ffff:192.168.109.12 Client Port: 54299 Additional Information: Ticket Options: 0x40810010 Failure Code: 0x18 Pre-Authentication Type: 2 Certificate Information: Certificate Issuer Name: Certificate Serial Number: Certificate Thumbprint: Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options and failure codes are defined in RFC 4120. If the ticket was malformed or damaged during transit and could not be decrypted, then many fields in this event might not be present.","source_type":"logstash","timestamp":"2025-11-24T17:05:53.586Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.IpPort":"54299","winlog.event_data.PreAuthType":"2","winlog.event_data.ServiceName":"krbtgt/LAB","winlog.event_data.Status":"0x18","winlog.event_data.TargetSid":"S-1-5-21-2625116736-1513678085-1295315389-1125","winlog.event_data.TargetUserName":"attacker","winlog.event_data.TicketOptions":"0x40810010","winlog.event_id":"4771","winlog.keywords":"Audit Failure","winlog.opcode":"Info","winlog.process.pid":"776","winlog.process.thread.id":"3380","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1513685","winlog.task":"Kerberos Authentication Service","_id":"AZedtpoBScXz9zJbV-BF","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":13.437}

El evento anterior muestra un fallo de pre-authentication Kerberos procedente del sistema 192.168.109.12 contra la cuenta attacker. El código de error 0x18 indica que las credenciales son incorrectas, lo cual es característico durante procesos de enumeración o password spraying en AD.

- EventID 4768: A Kerberos authentication ticket TGT was requested.

Se adjunta log de muestra:

{"event.code":"4768","winlog.event_data.IpAddress":"::ffff:192.168.109.12","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-03T13:48:16.039Z","agent.ephemeral_id":"396ae2e7-a2f9-4936-b902-

b65aede37afe","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Kerberos Authentication Service","event.created":"2025-11-03T23:03:43.869Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"A Kerberos authentication ticket (TGT) was requested. Account Information: Account Name: CLIENT2$ Supplied Realm Name: LAB.LOCAL User ID: S-1-5-21-2625116736-1513678085-1295315389-1115 Service Information: Service Name: krbtgt Service ID: S-1-5-21-2625116736-1513678085-1295315389-502 Network Information: Client Address: ::ffff:192.168.109.12 Client Port: 49677 Additional Information: Ticket Options: 0x40810010 Result Code: 0x0 Ticket Encryption Type: 0x12 Pre-Authentication Type: 2 Certificate Information: Certificate Issuer Name: Certificate Serial Number: Certificate Thumbprint: Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.","source_type":"logstash","timestamp":"2025-11-03T13:48:16.039Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.IpPort":"49677","winlog.event_data.PreAuthType":"2","winlog.event_data.ServiceName":"krbtgt","winlog.event_data.ServiceSid":"S-1-5-21-2625116736-1513678085-1295315389-502","winlog.event_data.Status":"0x0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetSid":"S-1-5-21-2625116736-1513678085-1295315389-1115","winlog.event_data.TargetUserName":"CLIENT2$","winlog.event_data.TicketEncryptionType":"0x12","winlog.event_data.TicketOptions":"0x40810010","winlog.event_id":"4768","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"792","winlog.process.thread.id":"5692","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"304669","winlog.task":"Kerberos Authentication Service","_id":"vsO_S5oByvXe4XVqXqf0","_ignored":"message.keyword","_index":"vector-2025.11.03","_score":10.852}

Este registro evidencia solicitudes Kerberos dirigidas al servicio KRBTGT del dominio lab. local desde el mismo sistema origen involucrado en la actividad de enumeración.

La consulta KQL usada para localizar eventos relacionados con Kerberos fue:

```
event.code:(4768 OR 4771) AND
winlog.event_data.IpAddress:"192.168.109.12"
```

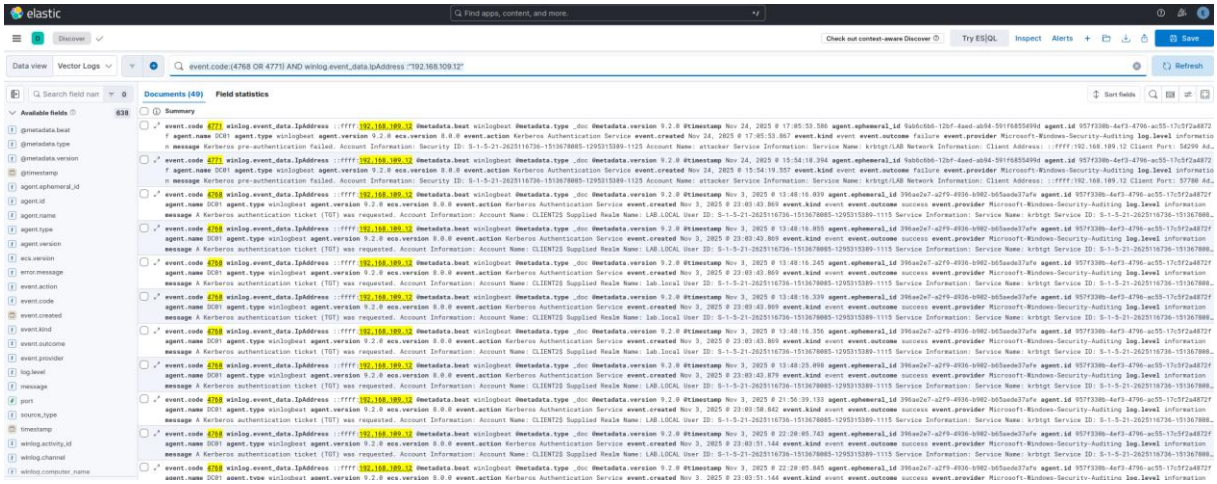

Ilustración 47. Eventos Kerberos (Event ID 4768 y 4771) generados durante la enumeración de usuarios mediante Kerbrute desde la IP 192.168.109.12

En esta imagen se muestra un total de 49 eventos generados desde la IP 192.168.109.12 con los EventID 4760 y 4771 que coinciden con actividad de enumeración Kerberos y el uso de Kerbrute.

Uno de los aspectos más relevantes observados durante esta fase, es que Kerberos proporciona una trazabilidad significativamente mayor a otras técnicas de reconocimiento interno. La generación repetitiva de solicitudes de autenticación y fallos de preautenticación producen patrones fácilmente observables sobre el controlador de dominio, especialmente cuando múltiples cuentas son consultadas desde una misma dirección IP en intervalos de tiempo reducidos.

Sin embargo, el análisis mostro ciertas limitaciones desde el punto de vista defensivo. Los eventos 4768 y 4771 forman parte del funcionamiento normal de AD y pueden generar de forma legítima debido a:

- Errores de autenticación de usuarios.
- Contraseñas caducadas.
- Sincronización incorrecta de credenciales.
- Servicios automatizados.
- Problemas normales de conectividad Kerberos.

Como consecuencia de esto, la detección efectiva de Kerbrute no depende únicamente de los eventos registrados, sino de la capacidad de correlacionar la frecuencia de solicitudes, volumen de errores, direcciones IP origen, cuentas objetivo y comportamiento temporal asociado.

Determinadas técnicas ofensivas generan eventos claramente visibles dentro del dominio, pero continúan requiriendo análisis contextual y correlación avanzada para poder diferenciar actividad maliciosa de comportamiento legítimo.

Por ello, la detectabilidad de esta técnica se considera alta ya que los eventos generados sobre el DC proporcionan evidencias consistentes y relativamente fáciles de identificar.

Enumeración Active Directory Mediate BloodHound y SharpHound

Tras la validación de usuarios y reconocimiento inicial del dominio, se realizó una recolección estructurada de información AD mediante SharpHound y BloodHound con el objetivo de identificar relaciones entre usuarios, grupos, permisos delegados, SPNs y posibles rutas de escalada de privilegios dentro del entorno.

Esta actividad corresponde a las técnicas MITRE:

- **T1087.002 – Domain Account Discovery**
- **T1069.002 – Domain Groups Discovery**
- **T1482 – Domain Trust Discovery**

A diferencia de otras fases de reconocimiento basadas únicamente en tráfico red, la ejecución de SharpHound genero evidencias mucho más identificables sobre el endpoint comprometido gracias a la telemetría proporcionada por Sysmon.

El principal evento observado fue:

- Sysmon EventID 5: Process terminated

Se adjunta log de muestra:

> {"message":"Process terminated: RuleName: - UtcTime: 2025-11-24 15:18:05.785 ProcessGuid: {28CFCBDB-76FD-6924-3E06-000000000C00} ProcessId: 600 Image: C:\\Tools\\Sharphound\\SharpHound.exe User: LAB\\attacker","winlog.event_data.Image":"C:\\Tools\\Sharphound\\SharpHound.exe","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T16:18:05.786Z","agent.ephemeral_id":"2c4476db-c773-4ed3-b074-a3e0b74e1a64","agent.id":"cf1afe44-e1e1-47c1-a7b6-e8c57fda5efb","agent.name":"CLIENT2","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Process terminated (rule: ProcessTerminate)","event.code":"5","event.created":"2025-11-24T16:18:07.231Z","event.kind":"event","event.provider":"Microsoft-Windows-Sysmon","log.level":"information","source_type":"logstash","timestamp":"2025-11-24T16:18:05.786Z","winlog.channel":"Microsoft-Windows-Sysmon/Operational","winlog.computer_name":"CLIENT2.lab.local","winlog.event_data.ProcessGuid":"{28CFCBDB-76FD-6924-3E06-000000000C00}","winlog.event_data.ProcessId":"600","winlog.event_data.RuleName":"-","winlog.event_data.User":"LAB\\attacker","winlog.event_data.UtcTime":"2025-11-24 15:18:05.785","winlog.event_id":"5","winlog.opcode":"Info","winlog.process.pid":"3488","winlog.process.thread.id":"4508","winlog.provider_guid":"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}","winlog.provider_name":"Microsoft-Windows-Sysmon","winlog.record_id":"2498","winlog.task":"Process terminated (rule: ProcessTerminate)","winlog.user.domain":"NT AUTHORITY","winlog.user.identifier":"S-1-5-18","winlog.user.name":"SYSTEM","winlog.user.type":"User","winlog.version":"3","_id":"BJdxtpoBScXz9zJbmKY_","_ignored":"-","_index":"vector-2025.11.24","_score":12.248}

El evento anterior evidencia la ejecución de SharpHound.exe sobre el sistema CLIENT2 usando la cuenta LAB\attacker. La información registrada permitió identificar:

- El binario usado durante la enumeración.
- Ruta exacta desde la que fue ejecutado.
- Usuarios asociados a la actividad.
- Endpoint comprometido.

La consulta KQL usada para localizar esta actividad relacionada fue:

```
event.code:5 AND winlog.event_data.Image: *SharpHound*
```

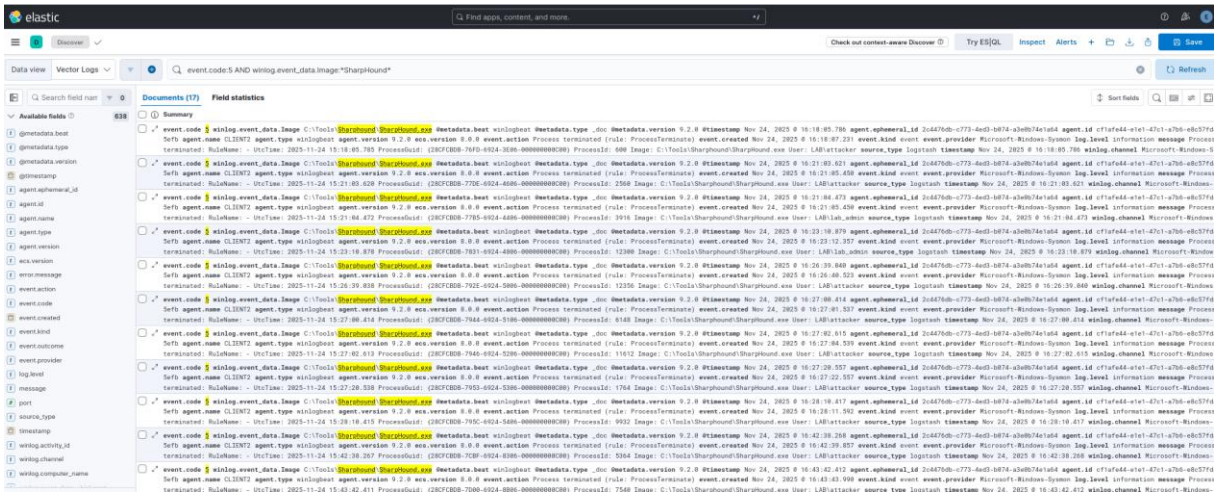

Ilustración 48. Eventos generados por la ejecución de SharpHound en CLIENT2 para la recolección de información del dominio Active Directory

Esta imagen muestra un total de 17 eventos en los que se terminó el proceso SharpHouns.exe ejecutado desde la ruta de C:\Tools en el host CLIENT2.

Desde el punto de vista defensivo, uno de los aspectos más relevantes observados es que la visibilidad obtenida no proviene directamente de la actividad LDAP generada por BloodHound sino de la ejecución del binario sobre el endpoint.

Esto resulta muy útil ya que las consultas LDAP realizadas por SharpHound usan mecanismos totalmente legítimos de AD compartiendo características idénticas con herramientas administrativas y procesos normales difíciles de considerar como maliciosos de forma aislada.

En este escenario, Sysmon proporciono la principal capacidad de trazabilidad al permitir identificar la ejecución de herramientas defensivas sobre el host comprometido. Sin embargo, incluso en presencia de este tipo de eventos, la detección continúa presentando las siguientes limitaciones:

- El binario puede ser renombrado fácilmente.
- La ejecución puede realizarse en rutas menos sospechosas.
- Herramientas similares pueden usar nombres legítimos.
- La actividad LDAP asociada continúa siendo altamente ambigua.

Este comportamiento manifiesta que unas muchas técnicas orientadas al reconocimiento AD se apoyan en funcionalidades legítimas del dominio y únicamente resultan identificables cuando existe correlación entre ejecución de procesos, contexto temporal y actividad posterior observada sobre otros sistemas.

Por ello, la detectabilidad de esta técnica se considera media ya que, aunque Sysmon proporciona evidencias relativamente claras sobre la ejecución SharpHound, la actividad LDAP subyacente continúa siendo difícil de diferenciar de comportamiento administrativo legítimo.

Conclusiones de detectabilidad de la fase

La fase de reconocimiento evidencio que muchas de las técnicas iniciales usadas contra entornos AD generan una visibilidad limitada y altamente contextual dentro de los mecanismos tradicionales de monitorización. Actividades como el descubrimiento de servicios internos o las

consultas LDAP produjeron eventos ambiguos y difíciles de diferencias de funcionamiento legítimo del dominio, sobre todo al usar protocolos legítimos como SMB, LDAP o Kerberos.

Sin embargo, determinadas técnicas como la enumeración Kerbrute si generaron patrones más visibles sobre el controlador de dominio a través de eventos Kerberos 4768 y 4771 permitiendo identificar comportamientos anómalos relacionados con autenticaciones repetitivas y fallos de preautenticación.

Además, el análisis mostro la importancia de Sysmon dentro de la capacidad de detección del entorno ya que herramientas como Chisel o SharpHound apenas habrían generado eventos usando únicamente los logs nativos de Windows.

En conjunto esta fase demuestra que las etapas iniciales de reconocimiento pueden pasar parcialmente desapercibidas incluso en entornos monitorizados con ELK, especialmente cuando el atacante usa funcionalidades legítimas del propio dominio y evita generar actividad claramente anómala desde el punto de vista del SO.

Fase 2 – Acceso a recursos y abuso de credenciales

Tras completar la fase inicial de reconocimiento y enumeración del dominio, el siguiente objetivo consistió en acceder a recursos compartidos internos con el propósito de localizar información sensible y obtener credenciales reutilizables dentro del entorno AD.

Durante esta fase se realizaron accesos SMB contra distintos sistemas del dominio, identificación de shares accesibles, búsqueda de ficheros con información sensible y ataques de password spraying orientados a comprometer cuentas válidas dentro de la infraestructura.

Desde un punto de vista defensivo, esta fase resulta muy importante debida a que gran parte de las acciones ejecutadas usan mecanismos completamente legítimos del entorno Windows, especialmente SMB y autenticaciones NTLM/Kerberos. Como consecuencia, gran parte de la actividad observada comparte similitudes con accesos normales a recursos dificultando la diferencia de comportamiento ofensivo de actividad administrativa legítima.

Acceso SMB y enumeración de recursos compartidos

La primera técnica ejecutada durante esta fase consistió en el acceso y enumeración de recursos compartidos SMB dentro del dominio con tal de identificar shares accesibles y localizar información sensible reutilizable durante fases posteriores del ataque. Esta actividad se corresponde con la técnica MITRE T1021.002 – SMB/Windows Admin Shares y T1135 – Network Share Discovery.

Durante el análisis realizado en ELK se identificaron eventos relacionados tanto con autenticaciones de red como con acceso a recursos compartidos internos mediante SMB. El evento principal que se observa es:

- EventID 5140: acceso a recurso compartido SMB

Se adjunta log de muestra:

> {"event. code":"5140","message":"A network share object was accessed. Subject: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1115 Account Name: CLIENT2$ Account Domain: LAB Logon ID: 0x9e62fb Network Information: Object Type: File Source Address: 192.168.109.12 Source Port: 58622 Share Information: Share Name: *\\IPC$ Share Path: Access Request Information: Access Mask: 0x1 Accesses: ReadData (or ListDirectory) ","winlog.event_data.IpAddress":"192.168.109.12","@metadata.beat":"winlogbeat","@metadata.ty

pe":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-03T23:11:41.228Z","agent.ephemeral_id":"396ae2e7-a2f9-4936-b902-b65aede37afe","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"File Share","event.created":"2025-11-03T23:11:42.204Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-11-03T23:11:41.228Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AccessList":"ReadData (or ListDirectory)\n","winlog.event_data.AccessMask":"0x1","winlog.event_data.IpPort":"58622","winlog.event_data.ObjectType":"File","winlog.event_data.ShareName":"*\\IPC$","winlog.event_data.SubjectDomainName":"LAB","winlog.event_data.SubjectLogonId":"0x9e62fb","winlog.event_data.SubjectUserName":"CLIENT2$","winlog.event_data.SubjectUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1115","winlog.event_id":"5140","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"4","winlog.process.thread.id":"6856","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"389887","winlog.task":"File Share","winlog.version":"1","_id":"o8XGS5oByvXe4XVq0bJR","_ignored":"message.keyword","_index":"vector-2025.11.03","_score":13.088}

El evento anterior refleja acceso remoto desde el sistema 192.168.109.12 hacia un recurso compartido usado en Windows para comunicaciones SMB, autenticaciones remotas y enumeración de recursos dentro del dominio.

La consulta KQL usada durante el análisis fue:

```
event.code:5140 AND "192.168.109.12"
```

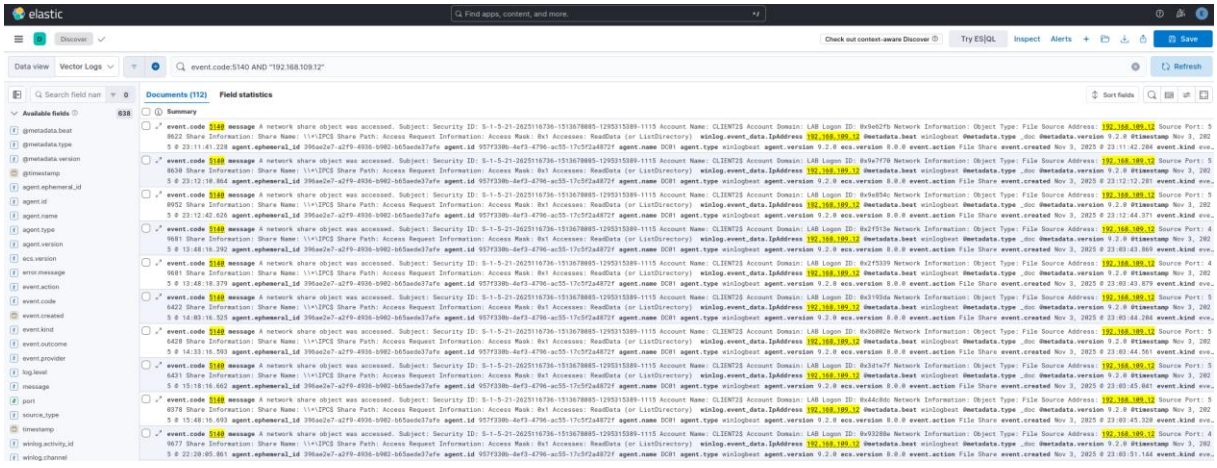

Ilustración 49. Eventos SMB (Event ID 5140) generados desde CLIENT2 durante el acceso a recursos compartidos del dominio

En la anterior imagen se ve una volumetría de un total de 112 eventos relacionados con Event Code 5140 generados desde la IP mencionada en la KQL y perteneciente a CLIENT2.

Esto nos permite identificar actividad SMB procedente del mismo sistema comprometido evidenciando accesos remotos hacia recursos compartidos del dominio.

Por otra parte, uno de los principales problemas observados durante esta fase, es que estos eventos forman parte del comportamiento normal de cualquier entorno Windows corporativo. El acceso a recursos SMB mediante autenticaciones Kerberos ocurre constantemente entre estaciones de trabajo, servidores y servicios internos del dominio.

Como consecuencia, los eventos registrados no permiten determinar por sí mismos si la actividad corresponde a enumeración ofensiva, acceso administrativo legítimo, funcionamiento normal del sistema o comunicaciones habituales entre equipos del dominio.

Este compartamiento muestra una de las mayores dificultades defensivas en entornos AD, y es que muchas técnicas de movimiento lateral y enumeración SMB usan mecanismos completamente legítimos del sistema, reduciendo significativamente la capacidad de detección basada únicamente en eventos individuales.

Por ello, la detectabilidad de esta técnica se considera baja ya que, aunque existen evidencias claras de autenticación y acceso SMB, la actividad observada continúa siendo altamente ambigua dentro del contexto normal de funcionamiento del dominio.

Obtención de credenciales en recurso compartidos

Tras identificar recursos SMB accesibles dentro del dominio, se realizaron tareas de búsqueda de información sensible y posibles credenciales almacenadas en shares corporativos. Esta actividad se corresponde con MITRE T1552.001 – Credentials in files.

Durante la fase se identificaron eventos relacionados con acceso detallado a recursos compartidos SMB, especialmente sobre shares críticos de AD. El principal evento observado fue:

- EventID 5145: Detailed File Share

Se adjunta log de muestra:

> {"event. code":"5145","message":"A network share object was checked to see whether client can be granted desired access. Subject: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1125 Account Name: attacker Account Domain: LAB Logon ID: 0xc0e0af Network Information: Object Type: File Source Address: 192.168.109.12 Source Port: 61356 Share Information: Share Name: *\\NETLOGON Share Path: \\??\\C:\\Windows\\SYSVOL\\sysvol\\lab.local\\SCRIPTS Relative Target Name: Default User.V6 Access Request Information: Access Mask: 0x80 Accesses: ReadAttributes Access Check Results: ReadAttributes: Granted by D:(A;;0x1200a9;;;WD)
> ","winlog.event_data.IpAddress":"192.168.109.12","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T15:14:57.754Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Detailed File Share","event.created":"2025-11-24T15:14:58.673Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-11-24T15:14:57.754Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AccessList":"ReadAttributes
> ","winlog.event_data.AccessMask":"0x80","winlog.event_data.AccessReason":"ReadAttributes: Granted by D:(A;;0x1200a9;;;WD)
> ","winlog.event_data.IpPort":"61356","winlog.event_data.ObjectType":"File","winlog.event_data.RelativeTargetName":"Default User.V6","winlog.event_data.ShareLocalPath":"\\??\\C:\\Windows\\SYSVOL\\sysvol\\lab.local\\SCRIPTS","winlog.event_data.ShareName":"*\\NETLOGON","winlog.event_data.SubjectDomainN

ame":"LAB","winlog.event_data.SubjectLogonId":"0xc0e0af","winlog.event_data.SubjectUserName":"attacker","winlog.event_data.SubjectUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1125","winlog.event_id":"5145","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"4","winlog.process.thread.id":"1564","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1490167","winlog.task":"Detailed File Share","_id":"7_o3tpoB11Fbndj00T9H","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":11.206}

Este evento refleja una solicitud de acceso desde le sistema 192.168.109.12 hacia un recurso compartido de la infraestructura interna.

La consulta KQL usada para localizar accesos detallados sobre recursos compartidos fue:

event.code:5145 AND "192.168.109.12"

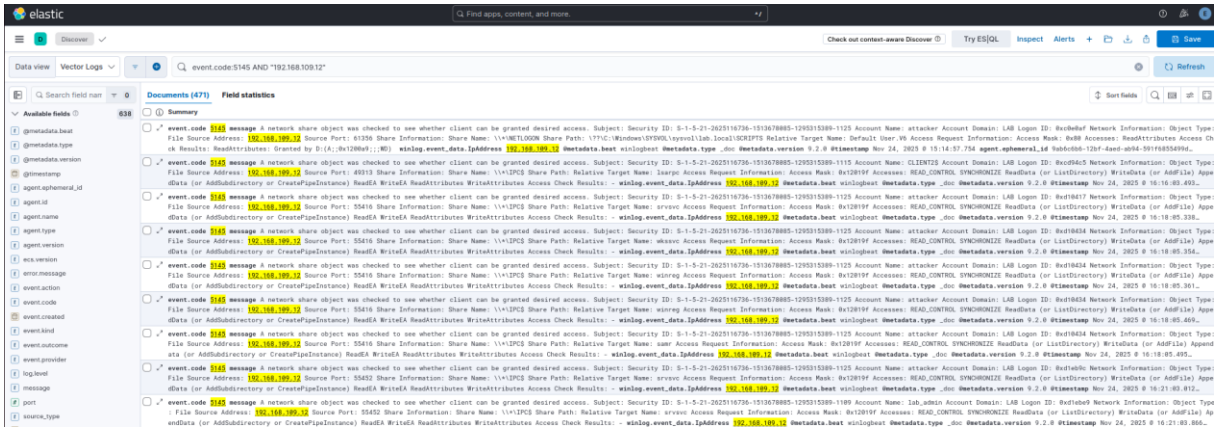

Ilustración 50. Eventos SMB (Event ID 5145) asociados a solicitudes de acceso a recursos compartidos realizadas desde CLIENT2

En esta imagen se muestran eventos 5145 de solicitudes de acceso a recursos SMB por parte de la máquina CLIENT2.

Uno de los aspectos más relevantes observados durante esta fase es que el evento 5145 proporciona una granularidad muy superior a eventos SMB más genéricos como el 5140, permitiéndonos identificar:

- Recurso compartido accedido.
- Fichero objetivo.
- Tipo de acceso solicitado.
- Permisos evaluados.

Sin embargo, desde una perspectiva defensiva continúa existiendo la limitación de que el acceso a recursos compartidos de este tipo, forman parte del comportamiento normal dentro de los entornos AD. Usuarios, workstations y servicios internos consultan constantemente estos recursos durante procesos legítimos relacionados con políticas de grupos, scripts de inicio de sesión y sincronización de configuraciones.

Como consecuencia, incluso con eventos detallados como son los 5145, diferenciar actividad ofensiva orientada a búsqueda de credenciales de comportamiento administrativo normal continúa siendo muy complejo sin mecanismo adicionales de correlación o contextualización.

Además, la visibilidad obtenida depende directamente del nivel de auditoria configurado sobre los recursos compartidos. En ausencia de auditoria avanzada sobre estos, gran parte de este tipo de accesos apenas generarían trazabilidad en el SIEM.

Por ello, la detectabilidad de esta técnica se considera baja ya que, aunque los eventos 5145 proporcionan información detallada sobre accesos SMB, la actividad observada continúa siendo muy ambigua dentro del funcionamiento normal de AD.

Password Spraying

Tras la enumeración inicial de usuarios y recursos compartidos, se realizó un ataque de password spraying con el objetivo de comprometer cuentas válidas del dominio mediante autenticaciones repetitivas contra múltiples usuarios. Esta actividad corresponde con la técnica MITRE T1110.003 – Password Spraying.

A diferencia de otras técnicas de reconocimiento observadas durante las fases anteriores, el password spraying genero evidencias mucho más visibles dentro de los Security Logs de Windows debido al elevado número de autenticaciones fallidas registradas sobre los sistemas objetivo.

Los principales eventos identificados fueron los:

- EventID 4625: An account failed to log on.

Se adjunta log de muestra:

{"event. code":"4625","message":"An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account for Which Logon Failed: Security ID: S-1-0-0 Account Name: davidcardela@gmail.com Account Domain: MicrosoftAccount Failure Information: Failure Reason: Unknown username or bad password. Status: 0xc000006d Sub Status: 0xc0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: CLIENT2 Source Network Address: 192.168.109.12 Source Port: 58630 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access is attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation names are not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.","winlog.event_data.IpAddress":"192.168.109.12","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-03T23:12:10.932Z","agent.ephemeral_id":"396ae2e7-a2f9-4936-b902-b65aede37afe","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-11-

03T23:12:12.281Z","event.kind":"event","event.outcome":"failure","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-11-03T23:12:10.932Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AuthenticationPackageName":"NTLM","winlog.event_data.FailureReason":"Unknown user name or bad password.","winlog.event_data.IpPort":"58630","winlog.event_data.KeyLength":"0","winlog.event_data.LmPackageName":"-","winlog.event_data.LogonProcessName":"NtLmSsp ","winlog.event_data.LogonType":"3","winlog.event_data.ProcessId":"0x0","winlog.event_data.ProcessName":"-","winlog.event_data.Status":"0xc000006d","winlog.event_data.SubjectDomainName":"-","winlog.event_data.SubjectLogonId":"0x0","winlog.event_data.SubjectUserName":"-","winlog.event_data.SubjectUserSid":"S-1-0-0","winlog.event_data.SubStatus":"0xc0000064","winlog.event_data.TargetDomainName":"MicrosoftAccount","winlog.event_data.TargetUserName":"davidcardela@gmail.com","winlog.event_data.TargetUserSid":"S-1-0-0","winlog.event_data.TransmittedServices":"-","winlog.event_data.WorkstationName":"CLIENT2","winlog.event_id":"4625","winlog.keywords":"Audit Failure","winlog.opcode":"Info","winlog.process.pid":"792","winlog.process.thread.id":"6012","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"389944","winlog.task":"Logon","_id":"YMXHS5oByvXe4XVqSrTS","_ignored":"message.keyword","_index":"vector-2025.11.03","_score":12.768}

En este evento se refleja un intento fallido de autenticación remota mediante NTLM desde el sistema 192.168.109.12 contra el host CLIENT1 usando un inicio de sesión Logon Type 3, asociado normalmente a accesos de red SMB.

El código de error:

- 0xc000006d → credenciales inválidas.

Este permitió identificar intentos de validación de credenciales no legítimas dentro del dominio, comportamiento característico durante las fases de password spraying.

La consulta KQL usada para localizar las autenticaciones fallidas fue:

event.code:4625 AND "192.168.109.12"

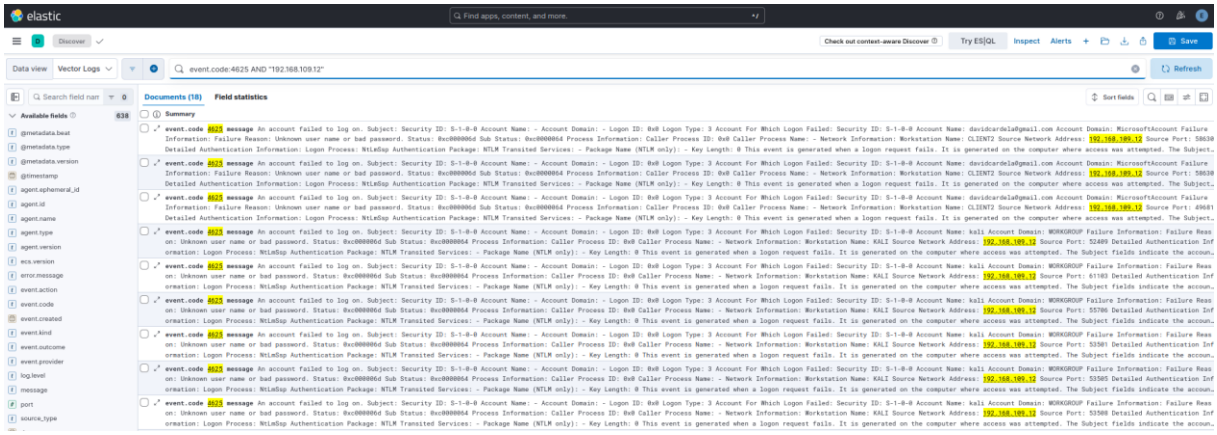

Ilustración 51. Eventos de autenticación fallida (Event ID 4625) generados desde la IP 192.168.109.12 mediante intentos de inicio de sesión remoto tipo 3

En esta imagen se muestran un total de 18 eventos donde se trató de iniciar sesión con credenciales inválidas desde la IP 192.168.109.12 a través de Logon Type 3.

El análisis temporal de los eventos permitió identificar múltiples intentos consecutivos de autenticación desde el mismo origen contra distintas cuentas del entorno generando un patrón claramente distinguible.

Sin embargo, desde una perspectiva defensiva, los eventos 4625 continúan presentando cierta ambigüedad de forma aislada. Fallos de autenticación similares pueden generarse también de forma legítima debido a errores de los usuarios, credenciales desactualizadas, servicios automatizados...

Como consecuencia, la detección efectiva de password spraying no depende solo de los logs individuales sino de la correlación temporal, numero de errores, numero de cuentas objetivo, repetición desde una misma IP, entre más cosas.

Por esto, la detectabilidad de esta técnica se considera alta ya que los eventos generados permiten identificar patrones anómalos relativamente claros cuando existen mecanismos adecuados de correlación y monitorización.

Compromiso de cuenta de usuario

Como resultado de la fase de password spraying se consigue comprometer una cuenta válida del dominio y reutilizar credenciales legítimas para continuar avanzando dentro de la infraestructura. Esta actividad se corresponde con la técnica de MITRE T1078 – Valid Accounts.

A diferencia de fases anteriores basadas en autenticaciones fallidas o actividad anómala fácilmente identificable, el uso de credenciales válidas redujo considerablemente la visibilidad defensiva ya que las acciones realizadas comenzaron a registrarse como accesos legítimos dentro del entorno AD.

El principal evento observado fue:

- EvetnID 4624 – An account was successfully logged on.

Se adjunta log de muestra:

{"event. code":"4624","message":"An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1106 Account Name: user1 Account Domain: LAB.LOCAL Logon ID: 0x6f95aa Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {BCAAD1F9-A877-9FA3-6CE7-E50DCA0F8534} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 192.168.109.11 Source Port: 57746 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation names are not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was
requested.","winlog.event_data.LogonType":"3","winlog.event_data.TargetUserName":"user1","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-12-31T10:59:58.343Z","agent.ephemeral_id":"1d7da995-514c-45f4-bd8a-8d6741bee1f8","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-12-31T10:59:59.711Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-
Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-12-31T10:59:58.343Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AuthenticationPackageName":"Kerberos","winlog.event_data.ElevatedToken":"Yes","winlog.event_data.ImpersonationLevel":"Impersonation","winlog.event_data.IpAddress":"192.168.109.11","winlog.event_data.IpPort":"57746","winlog.event_data.KeyLength":"0","winlog.event_data.LmPackageName":"-","winlog.event_data.LogonGuid":"{BCAAD1F9-A877-9FA3-6CE7-E50DCA0F8534}","winlog.event_data.LogonProcessName":"Kerberos","winlog.event_data.ProcessId":"0x0","winlog.event_data.ProcessName":"-","winlog.event_data.RestrictedAdminMode":"-","winlog.event_data.SubjectDomainName":"-","winlog.event_data.SubjectLogonId":"0x0","winlog.event_data.SubjectUserName":"-","winlog.event_data.SubjectUserSid":"S-1-0-0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetLinkedLogonId":"0x0","winlog.event_data.TargetLogonId":"0x6f95aa","winlog.event_data.TargetOutboundDomainName":"-","winlog.event_data.TargetOutboundUserName":"-","winlog.event_data.TargetUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1106","winlog.event_data.TransmittedServices":"-","winlog.event_data.VirtualAccount":"No","winlog.event_data.WorkstationName":"-","winlog.event_id":"4624","winlog.keywords":"Audit
Success","winlog.opcode":"Info","winlog.process.pid":"788","winlog.process.thread.id":"1876","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"2403310","winlog.task":"Logon","winlog.version":"2","_id":"kkK9cZsBkdi8L3731ZPR","_ignored":"message.keyword","_index":"vector-2025.12.31","_score":9.69}

El evento refleja una autenticación correcta mediante Kerberos usando la cuenta user1 contra el controlador de dominio DC01. El Logon Type 3 evidencia un acceso de red remoto comportamiento habitual durante conexiones SMB, acceso a recursos o autenticaciones internas dentro del dominio.

La consulta KQL usada para localizar autenticaciones exitosas relacionadas la cuenta comprometida fue:

```
event.code:4624 AND winlog.event_data.LogonType:"3" and "user1"
```

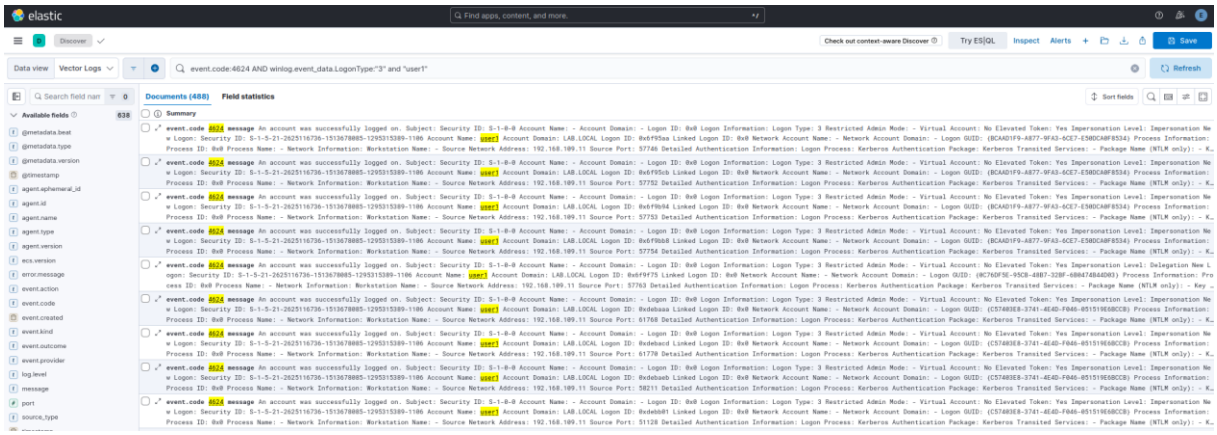

Ilustración 52. Eventos de inicio de sesión satisfactorio por red (Event ID 4624) asociados a la cuenta user1 mediante autenticación remota tipo 3

En esta imagen se muestran un total de 488 eventos de login satisfactorio por red con EventID 4624 que tuvieron como usuario destino la cuenta user1.

Uno de los aspectos más relevantes es que una vez comprometida una cuenta valida, la actividad ofensiva comienza a mezclarse casi completamente con el comportamiento normal del dominio. Desde la perspectiva del controlador de dominio, la autenticación registrada resulta indistinguible de un acceso legítimo realizado por el usuario real.

Además, el uso de Kerberos y credenciales válidas elimina gran parte de los indicadores anómalos presentes durante fases anteriores como errores de autenticación repetitivos o fallos de preautenticación reduciendo considerablemente la capacidad de detección basada únicamente en eventos individuales.

Desde una perspectiva defensiva, esta situación representa una de las principales dificultades en entornos AD modernos. Como consecuencia, la detección efectiva de este tipo de compromiso depende de:

- Correlación contextual.
- Análisis de comportamiento.
- Detección de acceso anómalos.
- Horarios inusuales.
- Movimientos laterales posteriores.
- Desviaciones respecto al comportamiento normal de la cuenta comprometida.

Por ello la detectabilidad de esta técnica se considera baja ya que el uso de cuentas válidas reduce significativamente la generación de eventos claramente sospechosos dentro del SIEM y dificulta atribuir la actividad a un compromiso real.

Conclusiones de detectabilidad de la fase

La segunda fase del ataque nos dio evidencias de como el uso de protocolos y mecanismos legítimos del entorno Windows reduce considerablemente la capacidad de detección dentro del Active Directory. Técnicas como el acceso a recursos SMB, la enumeración de shares o la reutilización de credenciales válidas generaron eventos ampliamente compatibles con actividad administrativa normal dificultando diferenciar el comportamiento ofensivo del legítimo.

Durante esta fase los eventos 4624, 5140 y 5145 proporcionaron trazabilidad útil sobre autenticaciones de red y acceso a recursos compartidos. Sin embargo, el análisis mostro que estos registros carecen de contexto suficiente para atribuir por sí mismo la actividad a un proceso claramente malicioso.

Por el contrario, las técnicas de password spraying si generaron patrones mucho más visibles mediante eventos 4625 asociados a autenticaciones NTLM fallidas repetitivas desde un mismo origen.

Finalmente, una vez comprometida una cuenta valida, la visibilidad defensiva disminuyo considerablemente. El uso de autenticaciones Kerberos legítimas provoco que gran parte de la actividad posterior comenzase a registrarse como comportamiento normal del dominio evidenciando una de las principales dificultades de los entornos AD, el abuso de credenciales válidas reduce significativamente la generación de indicadores claramente maliciosos.

Fase 3 – Kerberoasting y abuso de delegaciones Kerberos

Tras comprometer las credenciales válidas del usuario en la fase anterior, la siguiente fase del ataque estuvo orientada a la obtención de credenciales de servicios y abuso de funcionalidades legítimas de Kerberos para facilitar el movimiento lateral y escalada de privilegios dentro del entorno AD.

Durante esta etapa se realizaron técnicas de Kerberoasting, crackeo offline de credenciales y abuso de delegación Kerberos mediante mecanismos S4U apoyándose principalmente en el uso legítimo del protocolo Kerberos y cuentas de servicio del dominio.

Desde el punto de vista defensivo, esta fase resulto especialmente relevante debido a que gran parte de la actividad observada se ejecutó usando funcionalidades completamente legítimas del controlador de dominio. Como consecuencia, muchas de las acciones realizadas generaron eventos validos difíciles de distinguir del comportamiento administrativo normal sin mecanismos avanzados de correlación y análisis contextual.

Kerberoasting sobre cuentas de servicio

Una vez comprometida la cuenta user1, se realizaron solicitudes de tickets TGS asociados a cuentas de servicio del dominio con el objetivo de extraer material Kerberos susceptible de crackeo offline. Esta actividad se corresponde con la técnica MITRE T1558.003 – Kerberoasting.

El objetivo principal de la técnica consiste en solicitar tickets de servicio Kerberos vinculados a cuentas con SPN registrados dentro del AD para posteriormente intentar recuperar sus credenciales mediante ataques offline.

Durante el análisis en ELK se identificó principalmente eventos de:

- EventID 4769: A Kerberos Service ticket was requested.

Se adjunta log de muestra:

{"event. code":"4769","message":"A Kerberos service ticket was requested. Account Information: Account Name: user1@LAB.LOCAL Account Domain: LAB.LOCAL Logon GUID: {9F65724B-5B91-51EB-B6C5-3145A4203348} Service Information: Service Name: svc-sql02 Service ID: S-1-5-21-2625116736-1513678085-1295315389-1124 Network Information: Client Address: ::ffff:192.168.109.11 Client Port: 52896 Additional Information: Ticket Options: 0x40810000 Ticket Encryption Type: 0x17 Failure Code: 0x0 Transited Services: - This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.","winlog.event_data.IpAddress":"::ffff:192.168.109.11","winlog.event_data.TicketEncryptionType":"0x17","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-18T18:02:39.009Z","agent.ephemeral_id":"c93b5ea5-73e4-4ec9-8b0d-8d4ab4059986","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Kerberos Service Ticket Operations","event.created":"2025-11-18T21:52:27.914Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-11-18T18:02:39.009Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.IpPort":"52896","winlog.event_data.LogonGuid":"{9F65724B-5B91-51EB-B6C5-3145A4203348}","winlog.event_data.ServiceName":"svc-sql02","winlog.event_data.ServiceSid":"S-1-5-21-2625116736-1513678085-1295315389-1124","winlog.event_data.Status":"0x0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetUserName":"user1@LAB.LOCAL","winlog.event_data.TicketOptions":"0x40810000","winlog.event_data.TransmittedServices":"-","winlog.event_id":"4769","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"772","winlog.process.thread.id":"2792","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"798028","winlog.task":"Kerberos Service Ticket Operations","_id":"IBu9mJoBCTnK5MJAhEoM","_ignored":"message.keyword","_index":"vector-2025.11.18","_score":14.956}

El evento anterior muestra una solicitud legítima de ticket TGS realizada desde el sistema 192.168.109.11 usando la cuenta comprometida user1 contra la cuenta de servicio svc-sql02.

Uno de los aspectos más relevantes observados durante el análisis es el uso del tipo de cifrado (0x17) que corresponde con RC4-HMAC, un algoritmo frecuentemente asociado a escenarios de Kerberoasting debido a que permite realizar crackeo offline de los tickets usando herramientas como Hashcat o John The Ripper.

La consulta usada para localizar las solicitudes TGS potencialmente relacionadas con Kerberoasting fue:

event.code:4769 AND winlog.event_data.TicketEncryptionType:"0x17" and "*192.168.109.11*"

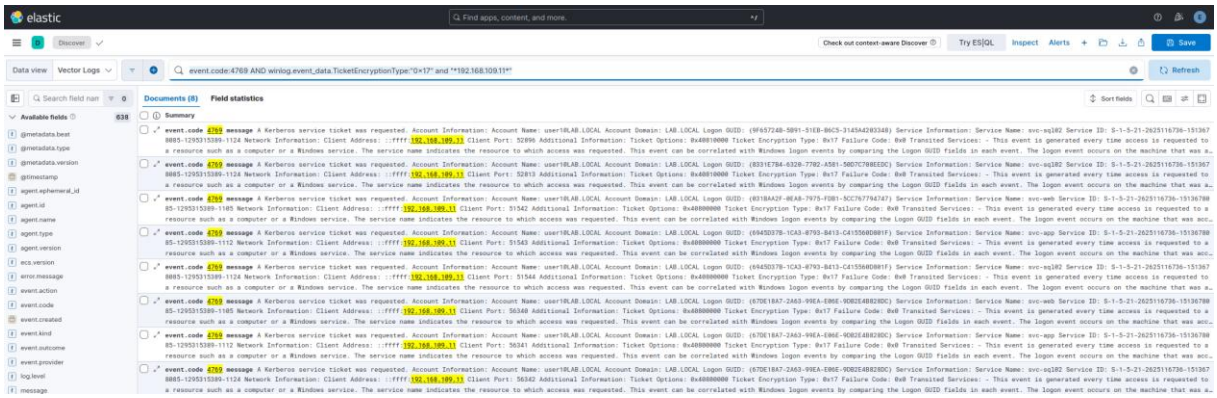

Ilustración 53. Eventos Kerberos TGS (Event ID 4769) generados por la cuenta user1 desde la IP 192.168.109.11 durante solicitudes de tickets de servicio

Esta imagen muestra un total de 8 eventos con EventID 4769 generados desde la IP 192.168.109.11 por el usuario user1.

Uno de los principales hallazgos observados durante esta fase, es que el evento 4769 forma parte del funcionamiento completamente normal del AD. La solicitud de tickets TGS ocurre constantemente durante el acceso legítimo a servicios corporativos, aplicaciones internas y cuentas de servicio del dominio.

Como consecuencia, la existencia aislada de un evento 4769 no constituye por sí solo una evidencia clara de actividad maliciosa. La capacidad de detección depende principalmente de correlacionar el volumen de solicitudes TGS, cuentas de servicio objetivo, cifrados RC4, frecuencia temporal y comportamiento habitual de la cuenta origen.

Además, el uso de una cuenta válida como user1 reduce considerablemente la generación de indicadores claramente anómalos ya que las solicitudes realizadas aparecen registradas como autenticaciones legítimas dentro del dominio.

Desde una perspectiva defensiva, uno de los principales indicadores más útiles observados durante esta fase fue precisamente de tickets RC4 ya que muchos entornos modernos priorizan AES y reducen progresivamente el uso de cifrados heredados. Como consecuencia, solicitudes TGS RC4 dirigidas a cuentas de servicio pueden constituir un indicador relevante de actividad potencialmente asociada a Kerberoasting.

Por ello, la detectabilidad de esta técnica se considera media/alta ya que, aunque los eventos 4769 proporcionan evidencias útiles sobre solicitudes TGS potencialmente sospechosas, la actividad continúa siendo altamente contextual y dependiente de correlaciona avanzada.

Obtención y crackeo offline de credenciales

Una vez obtenidos los tickets TGS asociados a cuentas de servicio, se realizó crackeo offline de las credenciales desde el sistema atacante con el objetivo de recuperar contraseñas reutilizables dentro del dominio.

A diferencia de otras técnicas observadas durante el laboratorio, esta fase presento una visibilidad nula en el entorno monitorizado. El principal motivo de esto es que el proceso de

crackeo se ejecutó completamente fuera de la infraestructura AD usando los tickets obtenidos previamente sin necesidad de interactuar nuevamente con el controlador de dominio.

Como consecuencia no se generaron eventos en DC01, no se observaron autenticaciones adicionales y no existió actividad directamente monitorizable desde ELK durante el crackeo.

Desde una perspectiva defensiva, esta característica resulta especialmente relevante ya que una vez extraído el material Kerberos necesario, la actividad ofensiva generada en esta actividad abandona completamente la visibilidad del SIEM.

Además, el éxito o fracaso del crackeo depende de:

- La complejidad de la contraseña.
- Políticas de longitud.
- Reutilización de credenciales.
- Capacidad computacional del atacante.

Este comportamiento pone de manifiesto una de las principales limitaciones de ataques Kerberoasting, la detección debe producirse necesariamente durante la fase inicial de solicitud de tickets ya que posterior a esto, el atacante podrá continuar el proceso completamente offline sin generar nuevas evidencias.

Por ello, la detectabilidad de esta técnica se considera nula, debido a la ausencia de telemetría observable.

Acceso mediante cuenta de servicio comprometida

Tras recuperar las credenciales asociadas a la cuenta de servicio mediante Kerberoasting, se realizaron autenticaciones legítimas dentro del dominio usando la cuenta svc-web. Esta actividad se relaciona con la técnica del MITRE T1078.002 – Domain Accounts.

A diferencia de fases anteriores basadas en errores de autenticación o solicitudes anómalas de los tickets Kerberos, el uso de una cuenta de servicio válida reduce considerablemente la visibilidad defensiva ya que la actividad observada comenzó a registrarse como comportamiento legítimo dentro del entorno AD.

El evento principal identificado durante esta fase fue:

- EventID 4624 – An account was successfully logged on.

Se adjunta log de muestra:

> {"event.code":"4624","winlog.event_data.TargetUserName":"svc-web","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-12T11:56:08.521Z","agent.ephemeral_id":"5de3ce98-5708-4f59-a3c2-83102462a148","agent.id":"204a2e51-7043-498b-98be-2483ea387784","agent.name":"DELEG-CLIENT","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-11-24T13:01:23.589Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"An account was successfully logged on. Subject: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1109 Account Name: lab_admin Account Domain: LAB Logon ID: 0x4ddee1 Logon Information: Logon Type: 3 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: No Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1105 Account Name: svc-web Account Domain: LAB Logon ID: 0x9b4863 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {1EF9F263-137C-10AC-7ACD-8A70893C4B73} Process Information: Process ID: 0x1490 Process Name:

C:\\Windows\\System32\\inetsrv\\InetMgr.exe Network Information: Workstation Name: DELEG-CLIENT Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation names are not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.","source_type":"logstash","timestamp":"2025-11-12T11:56:08.521Z","winlog.activity_id":"{12F58CD8-53C0-0000-7E8D-F512C053DC01}","winlog.channel":"Security","winlog.computer_name":"DELEG-CLIENT.lab.local","winlog.event_data.AuthenticationPackageName":"Negotiate","winlog.event_data.ElevatedToken":"No","winlog.event_data.ImpersonationLevel":"Impersonation","winlog.event_data.IpAddress":"-","winlog.event_data.IpPort":"-","winlog.event_data.KeyLength":"0","winlog.event_data.LmPackageName":"-","winlog.event_data.LogonGuid":"{1EF9F263-137C-10AC-7ACD-8A70893C4B73}","winlog.event_data.LogonProcessName":"Advapi","winlog.event_data.LogonType":"3","winlog.event_data.ProcessId":"0x1490","winlog.event_data.ProcessName":"C:\\Windows\\System32\\inetsrv\\InetMgr.exe","winlog.event_data.RemoteCredentialGuard":"-","winlog.event_data.RestrictedAdminMode":"-","winlog.event_data.SubjectDomainName":"LAB","winlog.event_data.SubjectLogonId":"0x4ddee1","winlog.event_data.SubjectUserName":"lab_admin","winlog.event_data.SubjectUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1109","winlog.event_data.TargetDomainName":"LAB","winlog.event_data.TargetLinkedLogonId":"0x0","winlog.event_data.TargetLogonId":"0x9b4863","winlog.event_data.TargetOutboundDomainName":"-","winlog.event_data.TargetOutboundUserName":"-","winlog.event_data.TargetUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1105","winlog.event_data.TransmittedServices":"-","winlog.event_data.VirtualAccount":"No","winlog.event_data.WorkstationName":"DELEG-CLIENT","winlog.event_id":"4624","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"876","winlog.process.thread.id":"7976","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"29391","winlog.task":"Logon","winlog.version":"3","_id":"GtO9tZoBLJY0ORQTeHQl","_ignored":"message.keyword","_index":"vector-2025.11.12","_score":12.18}

El evento refleja una autenticación correcta usando la cuenta de servicio svc-web sobre el sistema DELEG-CLIENT. Uno de los aspectos más relevantes observados es que la autenticación aparece asociada al proceso .

La consulta KQL usada para localizar las autenticaciones relacionadas con la cuenta de servicio fue:

```
event.code:4624 AND winlog.event_data.TargetUserName:"svc-web"
```

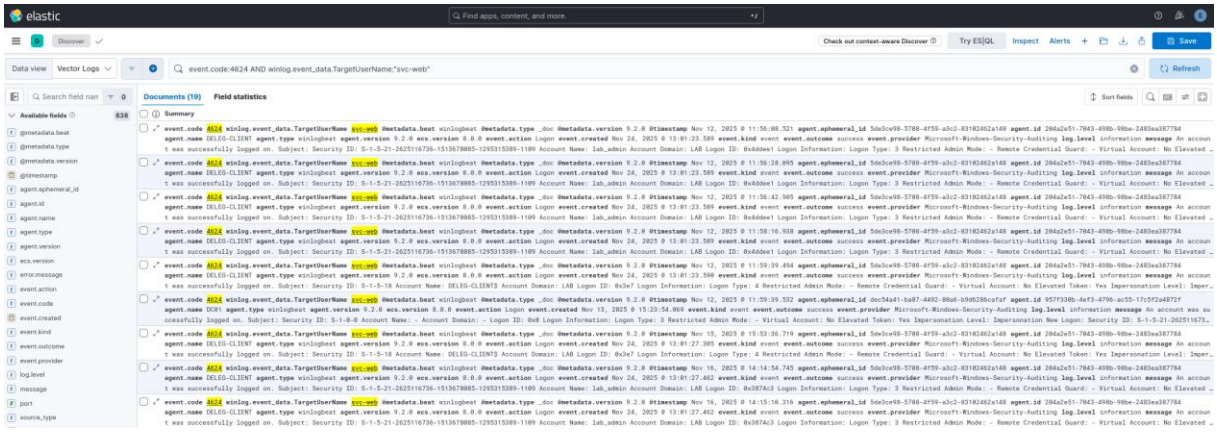

Ilustración 54. Eventos de inicio de sesión satisfactorio (Event ID 4624) realizados por la cuenta de servicio svc-web en el sistema DELEG-CLIENT

En esta imagen se muestran 19 eventos de login satisfactorio ejecutados por la cuenta de servicio svc-web en DELEG-CLIENT.

Uno de los principales hallazgos observados durante esta fase es que las cuentas de servicio generan actividad frecuente y completamente legítima dentro del dominio, especialmente en entornos con aplicaciones web, IIS, servicios automatizados y autenticaciones internas constantes.

Como consecuencia, el evento 4624 registrado resulta difícil de diferenciar de actividad legítima ya que la autenticación fue valida, se usó una cuenta legítima, el proceso asociado pertenece a Windows/IIS y no existen indicadores explícitos de actividad maliciosa dentro del propio evento.

Además, el uso del paquete de autenticación Negotiate y niveles normales de impersonación refuerza aún más la apariencia legítimade la actividad observada en los eventos.

Desde la perspectiva defensiva, este comportamiento pone de manifiesto que una vez que se ha comprometido la cuenta, los atacantes pueden usar mecanismos totalmente validos del dominio minimizando la generación de indicadores sospechosos.

Para una detección efectiva de esta actividad se requiere de:

- Correlación contextual.
- Comportamiento histórico de la cuenta.
- Análisis de accesos inusuales.
- Movimientos laterales posteriores.
- Desviaciones respecto al uso habitual de la cuenta de servicio comprometida.

Por ello, la detectabilidad de esta técnica se considera baja ya que el uso de autenticaciones legítimas mediante cuentas de servicio dificulta enormemente diferenciar actividad ofensiva de funcionamiento normal dentro del entorno AD.

Abuso de delegación Kerberos S4U

Por último, durante esta fase se realizaron técnicas de delegación Kerberos mediante mecanismos S4U (Service for User) con el objetivo de utilizar tickets legítimos del dominio para acceder a servicios internos usando cuentas de servicio comprometidas. Esta actividad se relaciona con la técnica del marco MITRE T1550 – Use Alternate Authentication Material y T1134 – Access Token Manipulation, y técnicas asociadas al abuso de delegación Kerberos.

Durante el análisis en ELK se identificaron principalmente:

- EventID 4769: A Kerberos Service ticket was requested.

Se adjunta log de muestra:

{"event.code":"4769","winlog.event_data.ServiceName":"svc-sql02","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-18T18:02:39.009Z","agent.ephemeral_id":"c93b5ea5-73e4-4ec9-8b0d-8d4ab4059986","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Kerberos Service Ticket Operations","event.created":"2025-11-18T21:52:27.914Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"A Kerberos service ticket was requested. Account Information: Account Name: user1@LAB.LOCAL Account Domain: LAB.LOCAL Logon GUID: {9F65724B-5B91-51EB-B6C5-3145A4203348} Service Information: Service Name: svc-sql02 Service ID: S-1-5-21-2625116736-1513678085-1295315389-1124 Network Information: Client Address: ::ffff:192.168.109.11 Client Port: 52896 Additional Information: Ticket Options: 0x40810000 Ticket Encryption Type: 0x17 Failure Code: 0x0 Transited Services: - This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.","source_type":"logstash","timestamp":"2025-11-18T18:02:39.009Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.IpAddress":"::ffff:192.168.109.11","winlog.event_data.IpPort":"52896","winlog.event_data.LogonGuid":"{9F65724B-5B91-51EB-B6C5-3145A4203348}","winlog.event_data.ServiceSid":"S-1-5-21-2625116736-1513678085-1295315389-1124","winlog.event_data.Status":"0x0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetUserName":"user1@LAB.LOCAL","winlog.event_data.TicketEncryptionType":"0x17","winlog.event_data.TicketOptions":"0x40810000","winlog.event_data.TransmittedServices":"-","winlog.event_id":"4769","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"772","winlog.process.thread.id":"2792","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"798028","winlog.task":"Kerberos Service Ticket Operations","_id":"IBu9mJoBCTnK5MJAhEoM","_ignored":"message.keyword","_index":"vector-2025.11.18","_score":7.984}

En este evento se muestra una solicitud TGS dirigida al servicio svc-sql02 desde el sistema 192.168.109.11 usando la cuenta user1@LAB.LOCAL.

Desde una perspectiva defensiva uno de los aspectos más relevantes observados durante esta fase es que los eventos generados durante el abuso de delegación Kerberos presentan características prácticamente idénticas a las observadas durante autenticaciones legítimas del dominio.

La consulta KQL usada para localizar solicitudes TGS relacionadas con cuentas de servicio fue:

```
event.code:4769 AND winlog.event_data.ServiceName: *svc*
```

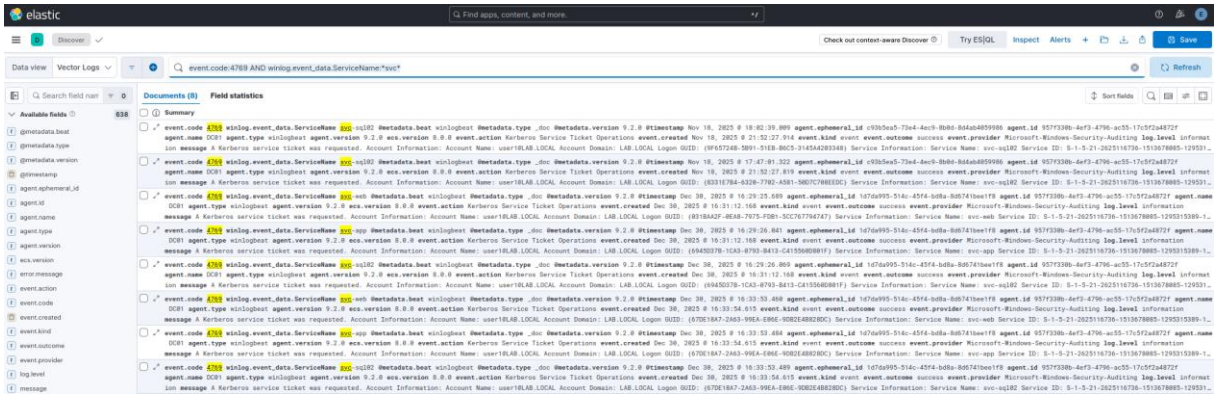

Ilustración 55. Eventos Kerberos TGS (Event ID 4769) asociados a solicitudes de tickets de servicio sobre cuentas con SPN realizadas por el usuario user1 desde CLIENT1

Esta imagen muestra un total de 8 eventos 4769 dirigidos hacia cuentas de servicio con SPN y generadas por el usuario user1 desde CLIENT1.

Uno de los principales problemas observados durante el análisis es que funcionalidades como S4U forman parte del comportamiento normal de Kerberos dentro del AD. Aplicaciones corporativas, IIS, SQL y otros servicios internos usan mecanismos de delegación de forma legítima para autenticar usuarios contra distintos recursos del dominio.

Como consecuencia, los eventos 4769 generados de esta actividad no contienen indicadores explícitos que permitan diferenciar fácilmente autenticaciones legítimas, solicitudes normales de servicios, delegación válida o abuso ofensivo de tickets Kerberos.

Además, como se dijo en apartados anteriores, el uso de cuentas válidas junto con solicitudes TGS correctamente autenticadas reduce la generación de actividad claramente sospechosa dentro del controlador de dominio.

Por esto la detectabilidad se considera baja, ya que, aunque existen evidencias relacionadas con solicitudes TGS sobre cuentas de servicio, la actividad observada continúa siendo altamente ambigua y difícil de diferenciar del funcionamiento normal del AD sin capacidad avanzadas de correlación y análisis contextual.

Conclusiones de detectabilidad de la fase

La tercera fase del ataque evidencio como muchas técnicas avanzadas contra AD se apoyan directamente en funcionalidades legítimas del protocolo Kerberos reduciendo la capacidad de detección basada únicamente en eventos individuales.

Durante esta etapa, los eventos 4769 proporcionaron la principal fuente de visibilidad sobre solicitudes TGS dirigidas a cuentas de servicio del dominio. El análisis permitió identificar peticiones asociadas a servicios concretos como svc-sql02, así como uso de cifrados RC4-HMAC frecuentemente relacionados con escenarios de Kerberoasting.

Sin embargo, el análisis también mostro que las solicitudes de tickets Kerberos forma parte del funcionamiento completamente legítimo de AD. Como consecuencia, la existencia aislada de eventos 4769 no constituye una evidencia concluyente de actividad ofensiva especialmente en entornos donde múltiples aplicaciones corporativas usan autenticaciones Kerberos y cuentas de servicio de forma continua.

Además, una vez obtenidas las credenciales de las cuentas de servicio, gran parte de la actividad posterior se registró como autenticaciones aparentemente legítimas mediante

eventos 4624 usando cuentas válidas y procesos completamente normales del entorno reduciendo la generación de indicadores maliciosos.

Otro aspecto relevante observado durante esta fase es la escasa visibilidad disponible frente al crackeo offline de ticket Kerberos. Una vez extraído el material TGS necesario, el atacante puede continuar el proceso fuera del dominio sin generar nuevas evidencias monitorizables sobre el controlador de dominio.

Finalmente, el abuso de delegación Kerberos mediante S4U puso de manifiesto una de las principales dificultades defensivas en AD, los atacantes pueden operar usando funcionalidades completamente legítimas del protocolo Kerberos mientras minimizan la generación de actividad anómala.

En conjunto esta fase demostró que el abuso de Kerberos constituye uno de los escenarios más complejos desde el punto de vista defensivo dentro de AD ya que gran parte de la actividad ofensiva observada resulta prácticamente indistinguible del funcionamiento legítimo del dominio sin mecanismos de correlación y análisis contextual.

Fase 4 – Compromiso de servicios SQL y web

Tras obtener acceso mediante cuentas válidas y credenciales de servicios comprometidas, la siguiente fase del ataque estuvo orientada al abuso de servicios internos expuestos dentro del dominio, especialmente servidores SQL Server e infraestructura IIS.

Durante esta etapa se realizaron autenticaciones contra servicios MSSQL, ejecución remota de consultas y abuso de la aplicación web interna usando cuentas comprometidas previamente obtenidas mediante Kerberoasting y enumeración de AD.

Desde el punto de vista ofensivo, esta fase resulto especialmente compleja debido a que gran parte de la actividad observada uso protocolos, procesos y autenticaciones totalmente legítimas dentro del entorno corporativo. Como consecuencia, muchas de las acciones realizadas generaron eventos validos difíciles de diferencias de administración normal o actividad legítima de las aplicaciones.

Acceso a SQL01 mediante credenciales comprometidas

Tras comprometer credenciales válidas asociadas a servicios SQL se realizaron autenticaciones remotas contra el servidor SQL01 con el objetivo de acceder a bases de datos internas del entorno corporativo. Esta actividad corresponde con la técnica MITRE T1078 – Valid Accounts y T1213 – Data from Information Repositories.

Durante esta fase se usó la cuenta comprometida svc-sql para establecer una conexión legítima contra un servicio SQL y ejecutar consultas directamente sobre la base de datos corporativa.

Desde una perspectiva defensiva, el acceso realizado genero eventos de autenticación validos dentro del controlador de dominio:

- EventID 4624: An account was successfully logged on.

Se adjunta log de muestra:

> {"event.code":"4624","winlog.event_data.TargetUserName":"SQL02$","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T16:57:58.610Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-

17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-11-24T16:57:59.110Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1122 Account Name: SQL02$ Account Domain: LAB.LOCAL Logon ID: 0xdadb35 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {12DB5BF1-C3A3-6990-AAFF-154AEB3587EA} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 192.168.109.17 Source Port: 49793 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation names are not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.","source_type":"logstash","timestamp":"2025-11-24T16:57:58.610Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AuthenticationPackageName":"Kerberos","winlog.event_data.ElevatedToken":"Yes","winlog.event_data.ImpersonationLevel":"Impersonation","winlog.event_data.IpAddress":"192.168.109.17","winlog.event_data.IpPort":"49793","winlog.event_data.KeyLength":"0","winlog.event_data.LmPackageName":"-","winlog.event_data.LogonGuid":"{12DB5BF1-C3A3-6990-AAFF-154AEB3587EA}","winlog.event_data.LogonProcessName":"Kerberos","winlog.event_data.ProcessId":"0x0","winlog.event_data.ProcessName":"-","winlog.event_data.RestrictedAdminMode":"-","winlog.event_data.SubjectDomainName":"-","winlog.event_data.SubjectLogonId":"0x0","winlog.event_data.SubjectUserName":"-","winlog.event_data.SubjectUserSid":"S-1-0-0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetLinkedLogonId":"0x0","winlog.event_data.TargetLogonId":"0xdadb35","winlog.event_data.TargetOutboundDomainName":"-","winlog.event_data.TargetOutboundUserName":"-","winlog.event_data.TargetUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1122","winlog.event_data.TransmittedServices":"-","winlog.event_data.VirtualAccount":"No","winlog.event_data.WorkstationName":"-","winlog.event_id":"4624","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"776","winlog.process.thread.id":"6444","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1513306","winlog.task":"Logon","winlog.version":"2","_id":"S5eWtpoBScXz9zJbIt7m","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":5.623}

Este evento refleja una autenticación correcta mediante Kerberos usando la cuenta SQL01$ contra el controlador de dominio DC01. El Logon Type 3 indica que es un acceso remoto de red asociado a comunicaciones internas y autenticaciones relacionadas con servicios SQL dentro del dominio.

La consulta realizada para localizar autenticaciones relacionadas con los servicios SQL fue:

event.code:4624 AND winlog.event_data.TargetUserName: *SQL01$*

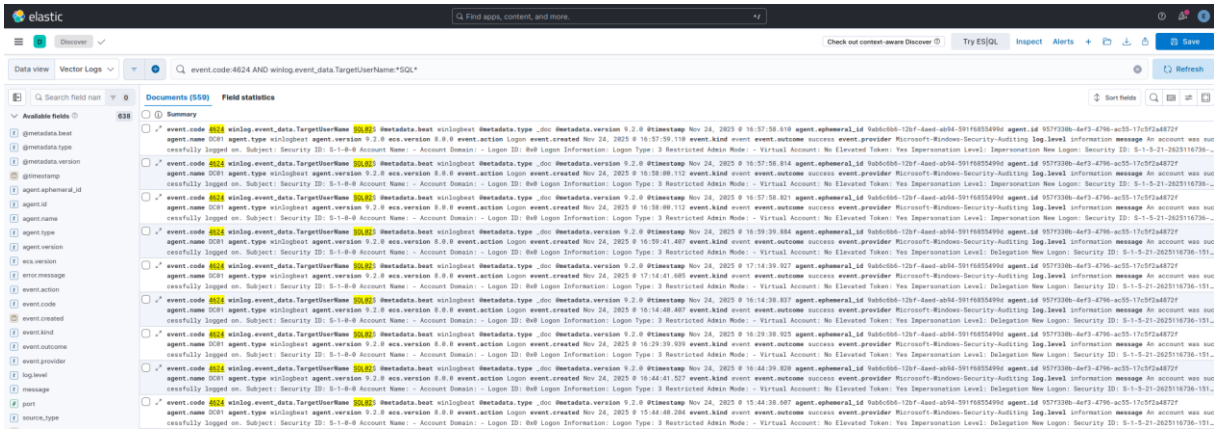

Ilustración 56. Eventos de inicio de sesión satisfactorio (Event ID 4624) sobre cuentas de servicio SQL mediante autenticación remota tipo 3 registrados en DC01

Esta imagen muestra eventos de inicio de sesión satisfactorios registrados en el DC01 que contienen cuentas de servicios SQL. Además, se encuentra en estos eventos que son Logon Type 3, es decir, inicios de sesión a través de red.

Uno de los aspectos más relevantes observados durante esta fase es que las autenticaciones relacionadas con SQL forman parte del funcionamiento completamente normal de aplicaciones corporativas, automatizaciones backend y comunicaciones internas entre sistemas. Además, las cuentas de máquina y servicios SQL generan autenticaciones constantes en el entorno AD dificultando enormemente diferenciar la actividad ofensiva del comportamiento legítimo.

Como consecuencia, y aunque el atacante consiguió acceso real sobre el servicio SQL usando credenciales comprometidas, los eventos generados continúan presentando características prácticamente idénticas a las actividades normales.

Este comportamiento muestra que una de las dificultadas defensivas frente al abuso de servicios SQL en entornos AD es que el atacante opera usando autenticaciones completamente válidas para minimizar la generación de actividad claramente sospechosa.

Por ello, la detectabilidad de esta técnica se considera baja ya que, desde la perspectiva del sistema, la actividad observada se comporta como un acceso legítimo a SQL Server usando credenciales válidas del dominio.

Exposición de credenciales en base de datos

Una vez obtenido acceso sobre el servidor MSSQL comprometido, se realizaron consultas dirigidas para localizar información sensible y posibles credenciales almacenadas dentro de bases de datos corporativas. Esta actividad se corresponde principalmente con la técnica MITRE T1552 – Unsecured Credentials.

Durante esta fase se identificaron tablas potencialmente sensibles dentro de la base de datos appdb, incluyendo estructuras relacionadas con usuarios y registros internos de la aplicación. A diferencia de otras técnicas observadas, esta fase presento una visibilidad prácticamente nula

dentro del entorno de monitorización. El principal motivo de esto es que gran parte de la actividad ofensiva se ejecutó sobre el motor SQL usando consultas completamente legítimas sin necesidad de generar autenticaciones adicionales o eventos anómalos sobre el controlador de dominio.

Como consecuencia, la visibilidad depende de:

- Loggins internos de SQL Server (como el analizado previamente).
- Nivel de auditoría SQL habilitado.
- Monitorización de consultas sobre tablas sensibles.
- Capacidad de correlacionar eventos de acceso y actividad SQL.

En muchos entornos las operaciones como “SHOW DATABASES, SHOW TABLES, SELECT…” no generan telemetría dentro del SIEM o únicamente quedan registradas en logs internos del propio servidor SQL, como es en nuestro caso.

Desde la perspectiva defensiva, esta característica resulta especialmente relevante ya que una vez comprometido el servicio MSSQL, el atacante puede continuar realizando enumeración y extracción de información sensible usando funcionalidades completamente normales del motor de base de datos.

El éxito de esta técnica depende de:

- La existencia de credenciales almacenadas.
- Permisos asociados a una cuenta comprometida.
- Nivel de segregación entre servicios y usuarios.
- Auditoria habilitada para consultas SQL.
- Capacidad de monitorizar tablas sensibles.

Este comportamiento nos enseña que gran parte de la actividad puede ejecutarse usando consultas completamente legítimas y compatibles con operaciones administrativas normales sin generar indicadores sospechosos.

Por ello, la detectabilidad de esta técnica se considera nula ya que la visibilidad depende casi completamente del nivel de auditoria SQL habilitado y de la capacidad del entorno para monitorizar accesos sobre información sensible dentro de las bases de datos.

Acceso a SQL02 mediante credenciales comprometidas

Una vez obtenidas las credenciales válidas asociadas a servicios, en este caso SQL, dentro del dominio, se realizaron autenticaciones remotas contra el servidor SQL02 usando mecanismos legítimos de Kerberos. Esta actividad se corresponde con MITRE T1078.002 – Domain Accounts.

Durante el análisis realizado en ELK se identificaron principalmente:

- EventID 4624: An account was successfully logged on.

Se adjunta log de muestra:

{"event.code":"4624","winlog.event_data.TargetUserName":"SQL02$","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.1","@timestamp":"2025-12-10T12:18:33.083Z","agent.ephemeral_id":"9daed569-0d23-4c7e-a395-5adc1d9f0ac4","agent.id":"eb9bdf9e-a979-4c11-bc2f-a65491abdc4a","agent.name":"SQL02","agent.type":"winlogbeat","agent.version":"9.2.1","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-12-31T11:02:17.902Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-

Windows-Security-Auditing","log.level":"information","message":"An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SQL02$ Account Domain: LAB.LOCAL Logon ID: 0xb840c Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {9A1B5B8E-4F08-591B-C535-767A5B36DA54} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation names are not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.","source_type":"logstash","timestamp":"2025-12-10T12:18:33.083Z","winlog.activity_id":"{04ED7E70-5D31-0001-2D7F-ED04315DDC01}","winlog.channel":"Security","winlog.computer_name":"SQL02.lab.local","winlog.event_data.AuthenticationPackageName":"Kerberos","winlog.event_data.ElevatedToken":"Yes","winlog.event_data.ImpersonationLevel":"Impersonation","winlog.event_data.IpAddress":"-","winlog.event_data.IpPort":"-","winlog.event_data.KeyLength":"0","winlog.event_data.LmPackageName":"-","winlog.event_data.LogonGuid":"{9A1B5B8E-4F08-591B-C535-767A5B36DA54}","winlog.event_data.LogonProcessName":"Kerberos","winlog.event_data.LogonType":"3","winlog.event_data.ProcessId":"0x0","winlog.event_data.ProcessName":"-","winlog.event_data.RestrictedAdminMode":"-","winlog.event_data.SubjectDomainName":"-","winlog.event_data.SubjectLogonId":"0x0","winlog.event_data.SubjectUserName":"-","winlog.event_data.SubjectUserSid":"S-1-0-0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetLinkedLogonId":"0x0","winlog.event_data.TargetLogonId":"0xb840c","winlog.event_data.TargetOutboundDomainName":"-","winlog.event_data.TargetOutboundUserName":"-","winlog.event_data.TargetUserSid":"S-1-5-18","winlog.event_data.TransmittedServices":"-","winlog.event_data.VirtualAccount":"No","winlog.event_data.WorkstationName":"-","winlog.event_id":"4624","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"740","winlog.process.thread.id":"788","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"2693","winlog.task":"Logon","winlog.version":"2","_id":"bkK_cZsBkdi8L3732Zq_","_ignored":"message.keyword","_index":"vector-2025.12.10","_score":8.266}

Este evento refleja, al igual que con SQL01, una autenticación correcta mediante Kerberos usando en este caso la cuenta SQL02$ directamente sobre el servidor SQL02. El Logon Type 3 evidencia un acceso remoto de red asociado a autenticaciones internas y comunicaciones relacionadas con servicios MSSQL dentro del dominio

La consulta KLQ usada para localizar autenticaciones relacionadas con el SQL Server fue:

event.code:4624 AND winlog.event_data.TargetUserName:"SQL02$"

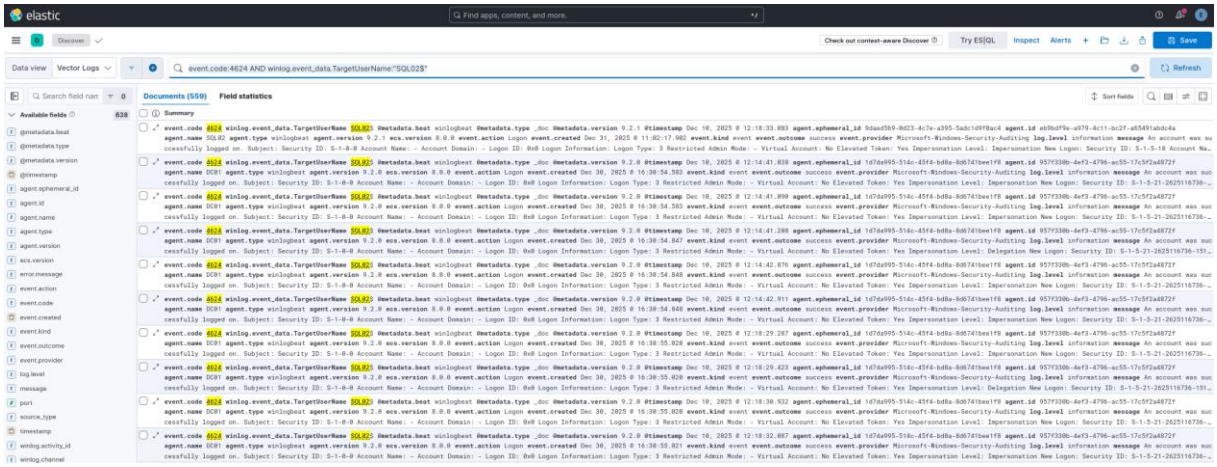

Ilustración 57. Eventos de inicio de sesión satisfactorio (Event ID 4624) sobre el sistema SQL02 mediante autenticación remota tipo 3 usando la cuenta de máquina SQL02$

En esta imagen se muestran eventos de inicio de sesión exitosos contra el SQL02 usando la cuenta máquina SQL02 y con Logon Type 3, a través de red.

Se obtuvo las mismas observaciones y análisis que en el apartado “Acceso a SQL01 mediante credenciales comprometidas” debido a que se trata prácticamente de la misma actividad, pero con distinto objetivo, en nuestro caso actual SQL02.

Por ello la detectabilidad también se considera baja ya que, desde la perspectiva del sistema, la actividad observada se comporta como una autenticación legítima SQL Server usando credenciales válidas del dominio.

Activación de xp_cmdshell y ejecución de comandos

Finalmente, durante esta fase se realizó el abuso de las funcionalidades internas de SQL Server mediante la activación de xp_cmdshell, permitiendo ejecutar comandos directamente sobre el sistema operativo desde el propio motor MSSQL. Esta actividad corresponde con MITRE T1059 – Command and Scripting Interpreter y T1505 – SQL Stored Procedures.

A diferencia de otras técnicas observadas en fases anteriores, la activación de xp_cmdshell genero una visibilidad considerablemente más clara y superior dentro del entorno de monitorización debido a que implica una modificación explicita de configuración sobre el servidor SQL.

Durante el análisis realizado en ELK se identificó principalmente el evento:

- EventID 15457: cambio de configuración SQL Server.

Se adjunta log de muestra:

> {"message":"Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.","winlog.event_data.param0":"xp_cmdshell","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.1","@timestamp":"2025-11-18T18:05:08.692Z","agent.ephemeral_id":"95acf7a4-bfd3-4f89-9a26-9fb125efa66c","agent.id":"eb9bdf9e-a979-4c11-bc2f-a65491abdc4a","agent.name":"SQL02","agent.type":"winlogbeat","agent.version":"9.2.1","ecs.versi

on":"8.0.0","event.action":"Server","event.code":"15457","event.created":"2025-11-18T21:58:50.389Z","event.kind":"event","event.provider":"MSSQL$SQL02","log.level":"information","source_type":"logstash","timestamp":"2025-11-18T18:05:08.692Z","winlog.channel":"Application","winlog.computer_name":"SQL02.lab.local","winlog.event_data.param1":"0","winlog.event_data.param2":"1","winlog.event_data.param3":"613C00000A0000000C000000530051004C00300032005C00530051004C00300032000000060000004C00610062004400420000000FE7F0000","winlog.event_id":"15457","winlog.keywords":"Classic","winlog.opcode":"Info","winlog.provider_name":"MSSQL$SQL02","winlog.record_id":"1488","winlog.task":"Server","winlog.user.domain":"LAB","winlog.user.identifier":"S-1-5-21-2625116736-1513678085-1295315389-1106","winlog.user.name":"user1","winlog.user.type":"User","_id":"hRzDmJoBCTnK5MJAg3HD","_ignored":"-","_index":"vector-2025.11.18","_score":17.305}

El evento anterior muestra la activación de xp_cmdshell sobre el servidor SQL02 usando la cuenta user1. Uno de los aspectos más relevantes observados es que SQL Server registra explícitamente la modificación de esta configuración dentro de los logs de aplicación MSSQL.

La consulta KQL usada para localizar la activación xp_cmdshell fue:

event.code:15457 AND message: *xp_cmdshell*

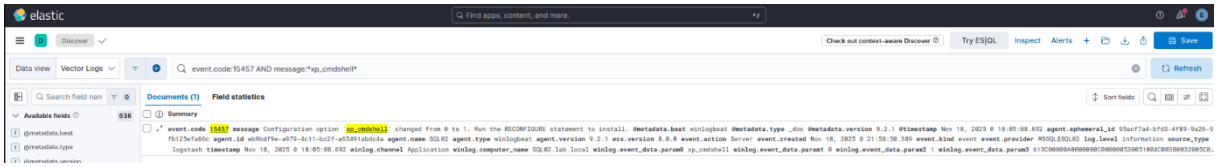

Ilustración 58. Evento asociado a la activación de la funcionalidad xp_cmdshell en el servidor SQL02

Esta imagen muestra un evento de activación xp_cmdshell dentro del host SQL02.

Desde una perspectiva defensiva, uno de los principales hallazgos observados es que la activación de xp_cmdshell constituye un comportamiento altamente sospechoso dentro de la mayoría de los entornos modernos.

Aunque esta funcionalidad puede usarse legítimamente para tareas administrativas concretas, en la práctica suele permanecer desactivada, su uso está fuertemente restringido y constituye uno de los mecanismos más habituales para el abuso ofensivo de SQL Server.

Además, una vez habilitado, el atacante puede ejecutar cmd[.]exe poweshell[.]exe, scripts, herramientas de postexplotación, comandos en el sistema operativos... directamente desde el contexto del servicio MSSQL.

Otro aspecto especialmente relevante es que esta actividad puede correlacionarse fácilmente con:

- Procesos hijos como sqlservr[.]exe.
- Eventos Sysmon.
- Ejecución PowerShell.
- Conexiones de red posteriores.

Como consecuencia esta técnica proporciona una visibilidad significativamente superior al resto. Esta técnica nos enseña que las funcionalidades peligrosas de SQL Server pueden

convertirse en mecanismos de ejecución remota altamente detectables cuando existe monitorización adecuada.

Es por esto que la detectabilidad de esta técnica se considera alta ya que la activación de xp_cmdshell constituye un comportamiento claramente anómalo y fácilmente identificable dentro de entornos SQL monitorizados.

Conclusiones de detectabilidad de la fase

La cuarta fase del ataque, evidencio como el comportamiento de servicios corporativos como MSSQL y aplicaciones web permiten al atacante operar usando protocolos, autenticaciones y funcionalidades completamente legítimas dentro del entorno AD.

Durante esta etapa, gran parte de la actividad ofensiva se apoyó en cuentas válidas y autenticaciones Kerberos correctamente registradas mediante eventos 4624, reduciendo la generación de indicadores maliciosos dentro del SIEM. Tanto el acceso a SQL01 como las autenticaciones sobre SQL02 presentaron características prácticamente idénticas a las observadas durante el funcionamiento normal de servicios corporativos y comunicaciones internas entre sistemas.

El análisis mostro que la visibilidad sobre accesos a bases de datos y consultas SQL dependen casi completamente del nivel de auditorio habilitado sobre el propio servidor MSSQL. Actividades como enumeración de bases de datos, consultas sobre tablas sensibles o acceso a información potencialmente critica no generaron volumetría útil.

Por el contrario, determinadas acciones asociadas al abuso avanzado de MSSQL si generaron indicadores mucho más visibles dentro del entorno monitorizado. La activación de xp_cmdshell mediante el evento 15457 proporciono una evidencia especialmente relevante desde el punto de vista defensivo ya que este comportamiento resulta altamente anómalo en la mayoría de los entornos corporativos y suele asociarse directamente a escenarios de ejecución remota y postexplotación sobre SQL Server.

En conjunto, esta fase muestra que mientras que una gran parte de la actividad ofensiva puede integrarse completamente dentro del funcionamiento normal de aplicaciones y servicios empresariales, determinadas técnicas avanzadas como xp_cmdshell continúan generando indicadores altamente detectables cuando existe una monitorización adecuada sobre AD, SQL Server y Sysmon.

Fase 5 – Escalada de privilegios y compromiso del dominio

Esta fase estuvo orientada a la obtención de privilegios elevados dentro del dominio y al establecimiento de mecanismos de persistencia capaces de garantizar acceso continuado sobre la infraestructura AD.

Durante esta etapa se realizaron técnicas de escalada local de privilegios, robo de credenciales en memoria, replicación maliciosa del dominio mediante DCSync, abuso avanzado de Kerberos mediante Golden y Silver Ticket y se crearon nuevas cuentas privilegiadas dentro del entorno corporativo.

Desde el punto de vista defensivo, esta fase presento alguno de los indicadores más visibles observados durante todo el laboratorio, especialmente en técnicas relacionadas con LSASS, replicación de AD y modificaciones administrativas y grupos privilegiados.

Sin embargo, determinadas técnicas basadas en tickets Kerberos falsificados continuaron presentando una visibilidad significativamente menor debido a que permiten al atacante operar usando autenticaciones aparentemente legítimas sin necesidad de interactuar constantemente con el controlador de dominio.

Escalada de privilegios con PrintSpoofer

Tras obtener acceso inicial sobre el sistema comprometido SQL02, se realizó escalada local de privilegios usando PrintSpoofer para obtener privilegios elevados sobre el endpoint comprometido. Esta actividad corresponde con la técnica MITRE T1068 – Explotation for Privilege Escalation.

Durante el análisis realizado en ELK se identificaron principalmente eventos de Sysmon asociados con la ejecución de herramientas ofensivas:

- Sysmon EventID 5: Process terminated

Se adjunta log de muestra:

> {"message":"Process terminated: RuleName: - UtcTime: 2025-12-31 10:12:20.895 ProcessGuid: {621ECB58-F704-6954-3101-000000000B00} ProcessId: 3352 Image: C:\\Tools\\PrintSpoofer64.exe User: SQL02\\Administrator","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.1","@timestamp":"2025-12-31T11:12:20.907Z","agent.ephemeral_id":"9daed569-0d23-4c7e-a395-5adc1d9f0ac4","agent.id":"eb9bdf9e-a979-4c11-bc2f-a65491abdc4a","agent.name":"SQL02","agent.type":"winlogbeat","agent.version":"9.2.1","ecs.version":"8.0.0","event.action":"Process terminated (rule: ProcessTerminate)","event.code":"5","event.created":"2025-12-31T11:12:22.301Z","event.kind":"event","event.provider":"Microsoft-Windows-Sysmon","log.level":"information","source_type":"logstash","timestamp":"2025-12-31T11:12:20.907Z","winlog.channel":"Microsoft-Windows-Sysmon/Operational","winlog.computer_name":"SQL02.lab.local","winlog.event_data.Image":"C:\\Tools\\PrintSpoofer64.exe","winlog.event_data.ProcessGuid":"{621ECB58-F704-6954-3101-000000000B00}","winlog.event_data.ProcessId":"3352","winlog.event_data.RuleName":"-","winlog.event_data.User":"SQL02\\Administrator","winlog.event_data.UtcTime":"2025-12-31 10:12:20.895","winlog.event_id":"5","winlog.opcode":"Info","winlog.process.pid":"2788","winlog.process.thread.id":"2772","winlog.provider_guid":"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}","winlog.provider_name":"Microsoft-Windows-Sysmon","winlog.record_id":"791","winlog.task":"Process terminated (rule: ProcessTerminate)","winlog.user.domain":"NT AUTHORITY","winlog.user.identifier":"S-1-5-18","winlog.user.name":"SYSTEM","winlog.user.type":"User","winlog.version":"3","_id":"K0LJcZsBkdi8L373N6g5","_ignored":"-","_index":"vector-2025.12.31","_score":1}

En este evento se evidencia la ejecución de PrintSpoofer sobre el servidor SQL02. Aunque el evento registrado corresponde con el proceso de finalización, Sysmon permite identificar información especialmente relevante desde la perspectiva defensiva como:

- Nombre de la herramienta.
- Ruta del binario ejecutado.
- Usuario asociado al proceso.
- Sistema afectado.

La consulta KQL usada para localizar actividad relacionada con PrintSpoofer fue:

event.code:5 AND message: *PrintSpoofer*

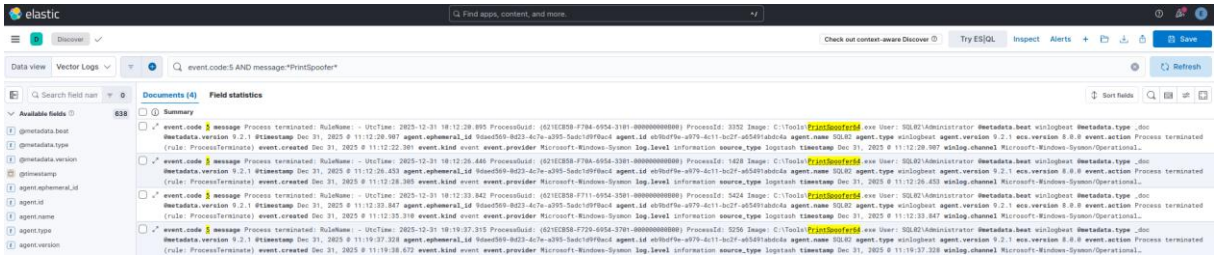

Ilustración 59. Eventos de finalización de ejecución de la herramienta PrintSpoofer en SQL02 desde la ruta C:\Tools

En esta imagen se muestran 4 eventos de finalización de ejecución de la herramienta PrintSpoofer en el sistema SQL02. El ejecutable se encontraba alojado en la ruta C:\Tools.

Uno de los aspectos más relevantes observados durante esta fase es que herramientas como PrintSpoofer generan visibilidad relativamente elevada cuando Sysmon se encuentra correctamente configurado sobre le endpoint comprometido.

Además, la aparición de binarios ofensivos ejecutados fuera de rutas habituales del sistema constituyen un comportamiento claramente anómalo dentro de la mayoría de los entornos corporativos monitorizados.

Por otra parte, la capacidad real de detección depende significativamente de la configuración de Sysmon, reglas de monitorización de proyectos, correlación de herramientas ofensivas conocidas y supervisión de escalada local de privilegios.

Este comportamiento muestra que las técnicas de escalada local de privilegios continúan dependiendo en gran medida de la capacidad defensiva desplegada directamente sobre los sistemas comprometidos y no únicamente del controlador del dominio.

Por ello, la detectabilidad de esta técnica se considera media/alta ya que Sysmon proporciona evidencias útiles sobre la ejecución de la herramienta de escalada de privilegios, aunque la detección efectiva precisa de monitorización avanzada y reglas específicas sobre procesos sospechosos.

Ejecución de Mimikatz

Una vez obtenidos privilegios elevados sobre el servidor comprometido, se ejecutaron técnicas orientadas a la extracción de credenciales en memoria mediante acceso al proceso lsass. Esta actividad corresponde con la técnica MITRE T1003.001 – OS Credential Dumping: LSASS Memory.

Durante esta fase se identificaron eventos asociados a creación de procesos críticos del sistema y actividad relacionada con LSASS, junto con la terminación del proceso de ejecución de Mimikatz:

- EventID 4688: Process creation.
- Sysmon EventID 5: Process terminated.

Se adjunta log de muestra:

{"agent.name":"SQL02","message":"A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x2e4 New Process Name: C:\\Windows\\System32\\lsass.exe Token Elevation Type: TokenElevationTypeDefault (1) Mandatory Label: S-1-16-16384 Creator Process ID: 0x278 Creator Process Name: C:\\Windows\\System32\\wininit.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled, and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.","winlog.computer_name":"SQL02.lab.local","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.1","@timestamp":"2025-11-24T15:44:26.078Z","agent.ephemeral_id":"9e0da3b2-6810-43da-926b-fc39492f6f18","agent.id":"eb9bdf9e-a979-4c11-bc2f-a65491abdc4a","agent.type":"winlogbeat","agent.version":"9.2.1","ecs.version":"8.0.0","event.action":"Process Creation","event.code":"4688","event.created":"2025-11-24T15:46:47.920Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-11-24T15:44:26.078Z","winlog.channel":"Security","winlog.event_data.MandatoryLabel":"S-1-16-16384","winlog.event_data.NewProcessId":"0x2e4","winlog.event_data.NewProcessName":"C:\\Windows\\System32\\lsass.exe","winlog.event_data.ParentProcessName":"C:\\Windows\\System32\\wininit.exe","winlog.event_data.ProcessId":"0x278","winlog.event_data.SubjectDomainName":"-","winlog.event_data.SubjectLogonId":"0x3e7","winlog.event_data.SubjectUserName":"-","winlog.event_data.SubjectUserSid":"S-1-5-18","winlog.event_data.TargetDomainName":"-","winlog.event_data.TargetLogonId":"0x0","winlog.event_data.TargetUserName":"-","winlog.event_data.TargetUserSid":"S-1-0-0","winlog.event_data.TokenElevationType":"TokenElevationTypeDefault (1)","winlog.event_id":"4688","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"4","winlog.process.thread.id":"496","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"3283","winlog.task":"Process Creation","winlog.version":"2","_id":"q5dVtpoBScXz9zJbDj8l","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":6.178}

Este evento refleja actividad relacionada con el proceso lsass[.]exe, componente crítico de Windows encargado de gestionar autenticaciones, credenciales y tokens de seguridad dentro del sistema operativo.

Durante escenarios de credential dumping mediante herramientas como Mimikatz, el proceso LSASS constituye uno de los principales objetivos debido a que almacena:

- Hashes NTLM.
- Tickets Kerberos.
- Credenciales en memoria.
- Tockens de autenticación reutilizables.

Se adjunta log de muestra:

{"message":"Process terminated: RuleName: - UtcTime: 2025-12-31 10:31:49.793 ProcessGuid: {621ECB58-FA9B-6954-9701-000000000B00} ProcessId: 1168 Image: C:\\Program Files\\mimikatz.exe User: SQL02\\Administrator","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.1","@timestamp":"2025-12-31T11:31:49.797Z","agent.ephemeral_id":"9daed569-0d23-4c7e-a395-5adc1d9f0ac4","agent.id":"eb9bdf9e-a979-4c11-bc2f-a65491abdc4a","agent.name":"SQL02","agent.type":"winlogbeat","agent.version":"9.2.1","ecs.version":"8.0.0","event.action":"Process terminated (rule: ProcessTerminate)","event.code":"5","event.created":"2025-12-31T11:31:51.228Z","event.kind":"event","event.provider":"Microsoft-Windows-Sysmon","log.level":"information","source_type":"logstash","timestamp":"2025-12-31T11:31:49.797Z","winlog.channel":"Microsoft-Windows-Sysmon/Operational","winlog.computer_name":"SQL02.lab.local","winlog.event_data.Image":"C:\\Program Files\\mimikatz.exe","winlog.event_data.ProcessGuid":"{621ECB58-FA9B-6954-9701-000000000B00}","winlog.event_data.ProcessId":"1168","winlog.event_data.RuleName":"-","winlog.event_data.User":"SQL02\\Administrator","winlog.event_data.UtcTime":"2025-12-31 10:31:49.793","winlog.event_id":"5","winlog.opcode":"Info","winlog.process.pid":"2788","winlog.process.thread.id":"2772","winlog.provider_guid":"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}","winlog.provider_name":"Microsoft-Windows-Sysmon","winlog.record_id":"907","winlog.task":"Process terminated (rule: ProcessTerminate)","winlog.user.domain":"NT AUTHORITY","winlog.user.identifier":"S-1-5-18","winlog.user.name":"SYSTEM","winlog.user.type":"User","winlog.version":"3","_id":"H0LbcZsBkdi8L373DbNC","_ignored":"-","_index":"vector-2025.12.31","_score":1}

Este otro evento muestra la terminación de ejecución de Mimikatz desde la ruta C:\Tools en el sistema SQL02 ejecutada por el Administrator. Este evento tiene Sysmon EventID 5.

La consulta KQL usada para localizar actividad relacionada con LSASS fue:

event.code:4688 AND message: *lsass.exe* and "SQL02"

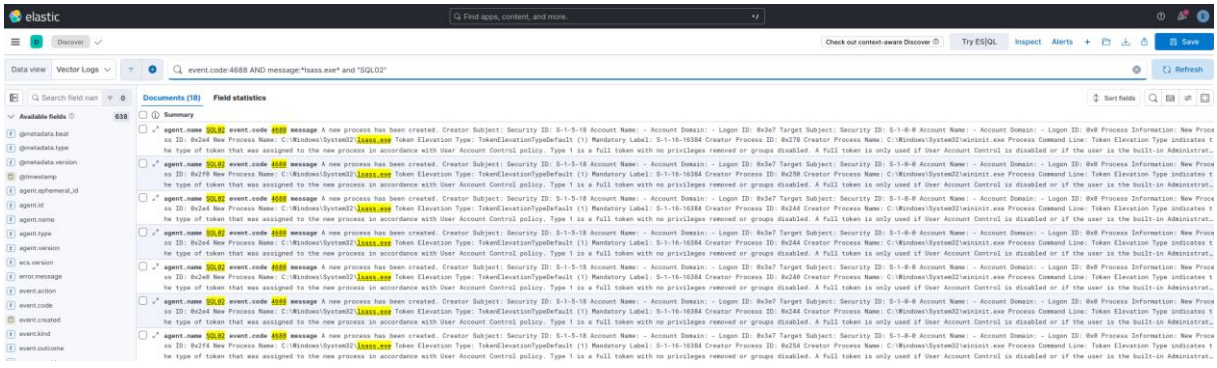

Ilustración 60. Eventos de creación de procesos relacionados con lsass.exe registrados en el sistema SQL02

En esta imagen se muestra 18 eventos de creación de procesos lsass[.]exe desde el sistema SQL02.

event.code:5 AND message: *mimikatz*

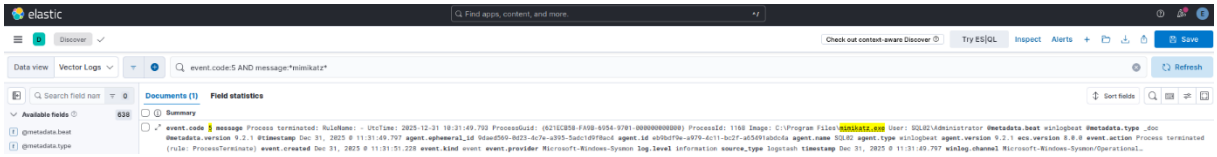

Ilustración 61. Proceso de terminación de la ejecución de Mimikatz.

Desde una perspectiva defensiva, uno de los aspectos más relevantes observados durante esta parte de la fase es que los accesos a LSASS constituyen uno de los comportamientos más monitorizados dentro de entornos Windows modernos.

Además, soluciones EDR, Sysmon y mecanismos avanzados de protección suelen detectar accesos no autorizados a LSASS, lectura de memoria, apertura de handles privilegiados, ejecución de herramientas de dumping y procesos asociados a extracción de credenciales.

Aunque el evento corresponde a la creación de proceso y no muestra el volcado directamente de memoria, la correlación con actividad de Mimikatz sobre LSASS constituye un indicador especialmente claro dentro del contexto del laboratorio.

Otro aspecto importante es que muchos ataques modernos contra AD dependen directamente de la capacidad del atacante para acceder a credenciales almacenadas en memoria mediante herramientas como Mimikatz.

Por ello, la detectabilidad de esta técnica se considera alta ya que la actividad relacionada con acceso LSASS y credential dumping suele generar indicadores claramente sospechosos cuando existen mecanismos adecuados de monitorización sobre endpoints y procesos críticos del sistema.

DCSync

Tras obtener privilegios elevados dentro del dominio, se ejecutó la técnica DCSync con el objetivo de abusar de los mecanismos de replicación de AD y obtener información sensible del dominio. Esta actividad corresponde con la técnica MITRE T1003.006 – DCSync.

Durante el análisis en ELK se identificaron eventos relacionados con acceso a objetos de servicio de directorio:

- EventID 4662: Directory Service Access
- Se adjunta log de muestra:

{"event.code":"4662","winlog.event_data.Properties":"Control Access {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T20:26:50.369Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Directory Service Access","event.created":"2025-11-24T20:26:51.784Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"An operation was performed on an object. Subject : Security ID: S-1-5-18 Account Name: DC01$ Account Domain: LAB Logon ID: 0x148c65 Object: Object Server: DS Object Type: %{19195a5b-6da0-11d0-afd3-00c04fd930c9}

Object Name: %{63ea1f70-4a1a-42b1-95b3-81341d362585} Handle ID: 0x0 Operation: Operation Type: Object Access Accesses: Control Access Access Mask: 0x100 Properties: Control Access {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9} Additional Information: Parameter 1: - Parameter 2: ","source_type":"logstash","timestamp":"2025-11-24T20:26:50.369Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AccessList":"Control Access
","winlog.event_data.AccessMask":"0x100","winlog.event_data.AdditionalInfo":"-","winlog.event_data.HandleId":"0x0","winlog.event_data.ObjectName":"%{63ea1f70-4a1a-42b1-95b3-81341d362585}","winlog.event_data.ObjectServer":"DS","winlog.event_data.ObjectType":"%{19195a5b-6da0-11d0-afd3-00c04fd930c9}","winlog.event_data.OperationType":"Object Access","winlog.event_data.SubjectDomainName":"LAB","winlog.event_data.SubjectLogonId":"0x148c65","winlog.event_data.SubjectUserName":"DC01$","winlog.event_data.SubjectUserSid":"S-1-5-18","winlog.event_id":"4662","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"776","winlog.process.thread.id":"904","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1521407","winlog.task":"Directory Service Access","_id":"MZhVt5oBScXz9zJbdgG2","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":11.023}

El elemento más relevante aquí es el GUID “{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}”. Este identificador está asociada al permiso de DS-Replication-Get-Changes usado en operaciones de replicación de AD. Este tipo de permisos resulta especialmente relevante en ataques DCSync ya que permite solicitar información del directorio simulando comportamientos propios de un controlador de dominio.

La consulta KQL usada para localizar esta actividad fue:

event.code:4662 AND (winlog.event_data.Properties: *1131f6aa* OR winlog.event_data.Properties: *1131f6ad*)

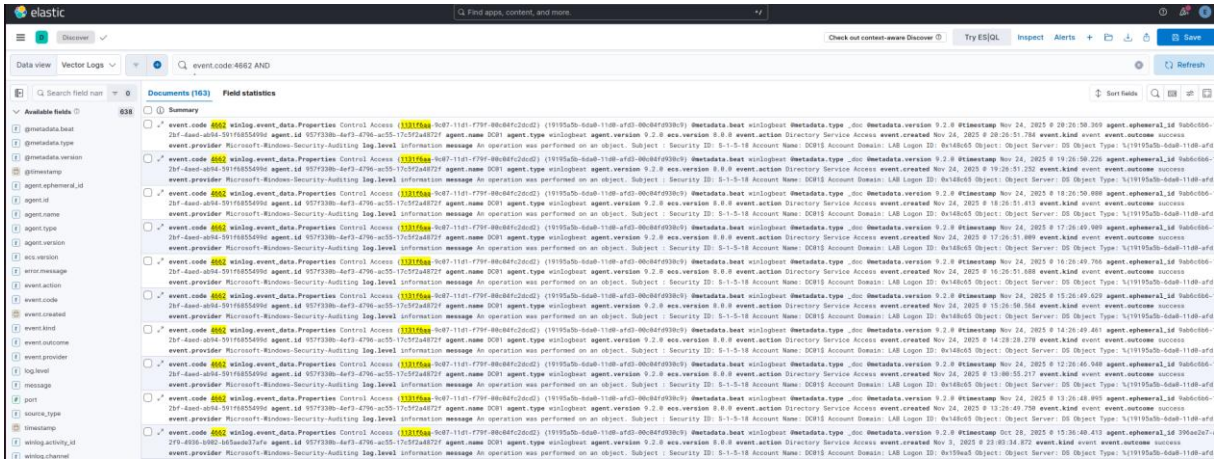

Ilustración 62. Eventos de acceso a replicación de Active Directory asociados al GUID 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2, característicos de actividad DCSync

En esta imagen se muestran eventos con los GUID {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} usados en replicación de Active Directory, muy relevante en ataques DCSync.

Uno de los aspectos más importantes observados durante la fase es que el evento 4662 puede generar una cantidad considerable de ruido dentro de AD ya que determinadas operaciones de replicación son legítimas cuando las realizan controladores de dominio. En este caso concreto, la cuenta observada es DC01$ por lo que el evento aislado no debe interpretarse automáticamente como malicioso.

Aun así, la presencia de permisos de replicación como DC-Replication-Get-Changes constituye una evidencia especialmente sensible que debe ser monitorizada de forma específica. En un entorno real, la aparición de estos eventos asociados a cuentas que no sean controladores de dominio o cuentas autorizadas de replicación sería un indicador muy sólido de posible DCSync.

Por esto la detectabilidad de esta técnica se considera alta siempre que exista auditoria avanzada sobre objetos de AD y reglas específicas orientadas a permisos de replicación.

Golden Ticket

Tras obtener acceso al hash KRBTGT mediante técnicas de replicación del dominio, se realizaron ataques Golden Ticket con el objetivo de generar tickets Kerberos falsificados capaces de otorgar privilegios elevados dentro del entorno AD. Esta actividad se corresponde con la técnica MITRE T1558.001 – Golden Ticket.

Durante el análisis en ELK se identificó principalmente:

- EventID 4672: Special privilege assigned to new logon.

Se adjunta log de muestra:

{"agent.name":"SQL02","event.code":"4672","winlog.event_data.SubjectDomainName":"LAB","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.1","@timestamp":"2025-11-24T11:56:56.368Z","agent.ephemeral_id":"9daed569-0d23-4c7e-a395-5adc1d9f0ac4","agent.id":"eb9bdf9e-a979-4c11-bc2f-a65491abdc4a","agent.type":"winlogbeat","agent.version":"9.2.1","ecs.version":"8.0.0","event.action":"Special Logon","event.created":"2025-12-31T11:02:17.898Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SQL02$ Account Domain: LAB Logon ID: 0x34355 Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege","source_type":"logstash","timestamp":"2025-11-24T11:56:56.368Z","winlog.activity_id":"{04ED7E70-5D31-0001-2D7F-ED04315DDC01}","winlog.channel":"Security","winlog.computer_name":"SQL02.lab.local","winlog.event_data.PrivilegeList":"SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege","winlog.event_data.SubjectLogonId":"0x34355","winlog.event_data.SubjectUserName":"SQL02$","winlog.event_data.SubjectUserSid":"S-1-5-18","winlog.event_id":"4672","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"740","winlog.process.thread.id":"788","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"2600","winlog.task":"Special Logon","_id":"EUK_cZsBkdi8L3732Zq_","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":10.121}

Este evento refleja una autenticación con privilegios elevados sobre el sistema comprometido. Entre los privilegios observados destacan capacidades especialmente sensibles como:

- SeDebugPrivilege.
- SeBackupPrivilege.
- SeRestorePrivilege.
- SeImpersonatePrivilege.

Este tipo de privilegios suele encontrarse asociado a cuentas administrativas, cuentas de sistema o sesiones altamente privilegiadas del dominio.

La query KQL usada para localizar este tipo de autenticaciones privilegiadas es:

event.code:4672 AND winlog.event_data.SubjectDomainName:"LAB" AND NOT winlog.event_data.SubjectUserName: *$ AND NOT winlog.event_data.SubjectUserName:"SYSTEM" AND agent.name:("SQL02")

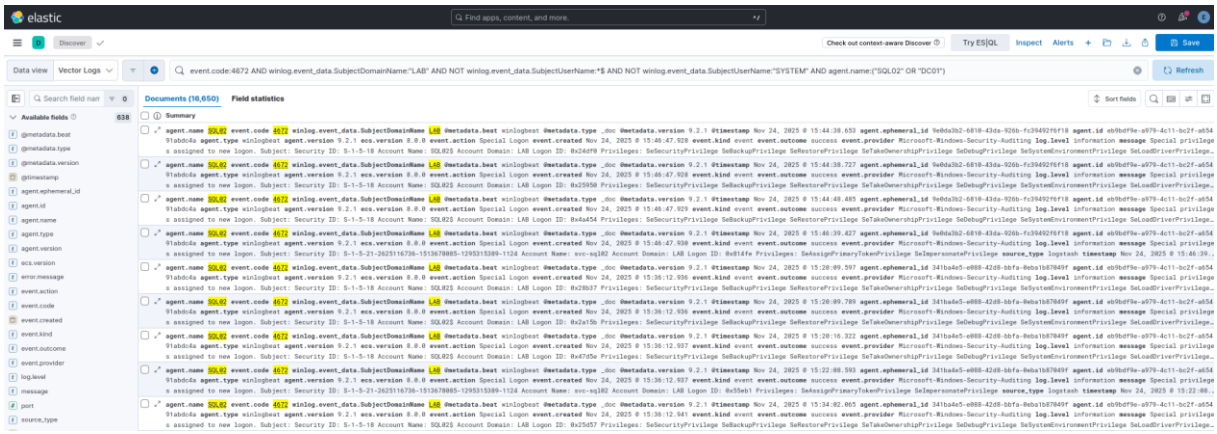

Ilustración 63. Eventos de inicio de sesión con privilegios especiales (Event ID 4672) registrados en el sistema SQL02

Esta imagen muestra evento de inicio de sesión con privilegios elevados sobre SQL02.

Durante el análisis fue necesario aplicar filtros específicos sobre los eventos 4672 debido a la elevada cantidad de ruido generada por cuentas del sistema y cuentas máquina dentro del entorno AD. Como consecuencia, se excluyeron autenticaciones SYSTEM y cuentas terminadas en $ con el objetivo de reducir falsos positivos y centrar el análisis sobre autenticaciones potencialmente sospechosas.

Uno de los aspectos más relevantes observados durante esta fase es que Golden Ticket permite generar autenticaciones aparentemente legítimas usando tickets Kerberos validos desde la perspectiva del sistema y del controlador del dominio.

Como consecuencia de esto, las autenticaciones suelen registrarse correctamente, los eventos generados son similares a accesos administrativos legítimos y gran parte de la actividad puede confundirse con comportamiento normal del dominio.

Además, eventos como 4672 no permiten confirmas directamente el uso de Golden Ticket de forma aislada ya que también aparecen habitualmente durante autenticaciones administrativas legítimas. Por ello la detección efectiva necesita de:

- Correlación avanzada de eventos.

- Análisis de comportamiento Kerberos.
- Revisión de privilegios asignados.
- Monitorización contextual de autenticaciones privilegiadas.

Este comportamiento pone de manifiesto que el atacante puede operar usando tickets aparentemente validos mientras mantiene privilegios elevados dentro del dominio sin generar indicadores claramente anómalos.

Por esto, la detectabilidad de esta técnica se considera baja ya que diferenciar autenticaciones legítimas de posibles tickets falsificados requiere capacidades avanzadas de correlación y análisis sobre actividad Kerberos dentro del entorno AD.

Creación de usuario privilegiado (goldenadmin)

Con el objetivo de establecer persistencia y disponer de una cuenta privilegiada dentro del dominio, se creó el usuario goldenadmin y se usaron permisos elevados sobre AD. Esta actividad se corresponde con la técnica MITRE T1136.002 – Create Account: Domain Account.

Durante el análisis realizado en ELK se identificó eventos asociados a actividad administrativa sensible sobre el controlador de dominio, destacando:

- EventID 4662 – Directory Service Access

Se adjunta log de muestra:

> {"message":"An operation was performed on an object. Subject : Security ID: S-1-5-21-2625116736-1513678085-1295315389-2101 Account Name: goldenadmin Account Domain: LAB Logon ID: 0x8999e5 Object: Object Server: DS Object Type: %{19195a5b-6da0-11d0-afd3-00c04fd930c9} Object Name: %{63ea1f70-4a1a-42b1-95b3-81341d362585} Handle ID: 0x0 Operation: Operation Type: Object Access Accesses: Control Access Access Mask: 0x100 Properties: Control Access {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9} Additional Information: Parameter 1: - Parameter 2: ","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-12-31T12:52:51.734Z","agent.ephemeral_id":"1d7da995-514c-45f4-bd8a-8d6741bee1f8","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Directory Service Access","event.code":"4662","event.created":"2025-12-31T12:52:53.488Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","source_type":"logstash","timestamp":"2025-12-31T12:52:51.734Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AccessList":"Control Access ","winlog.event_data.AccessMask":"0x100","winlog.event_data.AdditionalInfo":"-","winlog.event_data.HandleId":"0x0","winlog.event_data.ObjectName":"%{63ea1f70-4a1a-42b1-95b3-81341d362585}","winlog.event_data.ObjectServer":"DS","winlog.event_data.ObjectType":"%{19195a5b-6da0-11d0-afd3-00c04fd930c9}","winlog.event_data.OperationType":"Object Access","winlog.event_data.Properties":"Control Access {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}","winlog.event_data.SubjectDomainName":"LAB","winlog.event_data.SubjectLogonId":"0x8999e5","winlog.event_data.SubjectUserName":"goldenadmin","winlog.event_data.SubjectUserSid":"S-1-5-21-2625116736-1513678085-1295315389-2101","winlog.event_id":"4662","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"788","winlog.process.thread.id":"916","winl

og.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"2415038","winlog.task":"Directory Service Access","_id":"BEIlcpsBkdi8L373PM7r","_ignored":"message.keyword","_index":"vector-2025.12.31","_score":1}

El evento anterior muestra actividad realizada por la cuenta goldenadmin sobre objetos de servicio de directorio. El GUID “{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}”, corresponde, como se dijo en un apartado anterior de esta misma fase, al permiso DS-Replication-Get-Changes-All, asociado a operaciones de replicación de AD y considerado altamente sensible dentro del dominio.

La consulta KQL para localizar actividad relacionada con goldenadmin fue:

event.code:4662 AND
winlog.event_data.SubjectUserName:"goldenadmin"

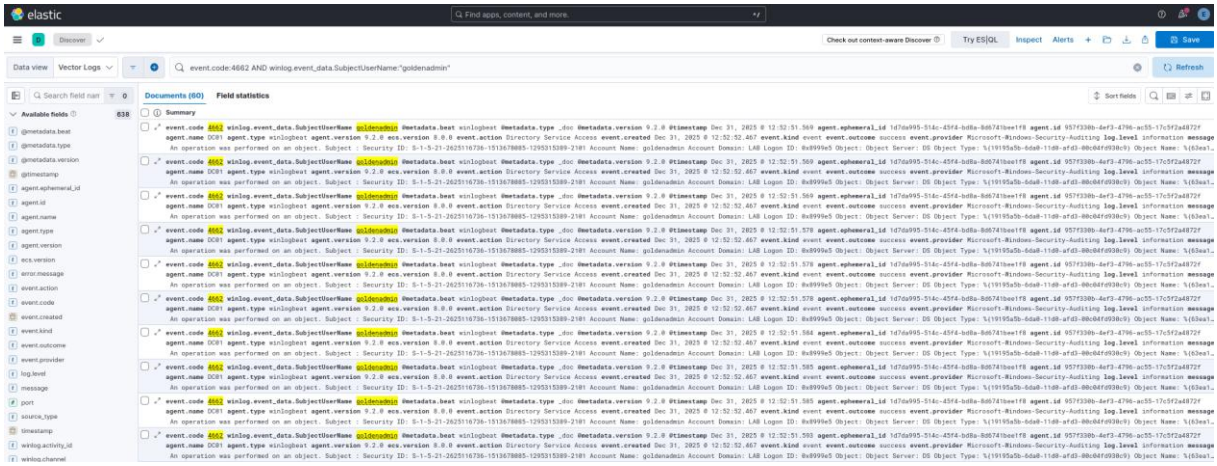

Ilustración 64. Eventos de acceso y operaciones sensibles sobre Active Directory ejecutadas por la cuenta goldenadmin

Esta imagen muestra actividad sobre directorios y actividad sensible de directorio de AD ejecutada por goldenadmin.

Este evento resulta muy relevante porque evidencia que la cuenta goldenadmin no solo existe dentro del dominio, sino que además aparece asociada a operaciones sensibles de AD. En un entorno real, una cuenta recientemente creada realizando acciones de control sobre objetos de directorio o permisos de replicación constituiría un indicador crítico de compromiso.

A diferencia de técnicas más sigilosas como Golden Ticket o Silver Ticket, la creación y uso de cuantas privilegiadas deja una trazabilidad administrativa mucho más clara dentro del dominio. Es por esto que la detectabilidad de esta técnica se considera alta, ya que genera eventos visibles y altamente sensibles en los Security Logs del DC.

Silver Ticket

Durante esta fase se usaron tickets Kerberos asociados al servicio objetivo con el propósito de acceder a recursos internos sin requerir una validación completa y continua contra el

controlador de dominio. Esta actividad se corresponde con la técnica MITRE T1558.002 – Silver Ticket.

Esta técnica presenta una característica especialmente relevante desde el punto de e vista defensiva y es que el atacante puede autenticarse directamente contra el servicio objetivo usando un ticket manipulado localmente, reduciendo considerablemente la generación de evidencias en DC01. Esto provoca que gran parte de la actividad pase desapercibida para el SIEM y no existe una correlación avanzada entre múltiples fuentes.

Durante el análisis realizado en ELK se identificaron principalmente:

- EventID 4624 - An account was successfully logged on.

Se adjunta log de muestra:

{"event.code":"4624","winlog.event_data.AuthenticationPackageName":"Kerberos","winlog.event_data.LogonType":"3","winlog.event_data.TargetUserName":"SQL02$","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T16:57:58.610Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-11-24T16:57:59.110Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2625116736-1513678085-1295315389-1122 Account Name: SQL02$ Account Domain: LAB.LOCAL Logon ID: 0xdadb35 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {12DB5BF1-C3A3-6990-AAFF-154AEB3587EA} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 192.168.109.17 Source Port: 49793 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation names are not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.","source_type":"logstash","timestamp":"2025-11-24T16:57:58.610Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.ElevatedToken":"Yes","winlog.event_data.ImpersonationLevel":"Impersonation","winlog.event_data.IpAddress":"192.168.109.17","winlog.event_data.IpPort":"49793","winlog.event_data.KeyLength":"0","winlog.event_data.LmPackageName":"-","winlog.event_data.LogonGuid":"{12DB5BF1-C3A3-6990-AAFF-154AEB3587EA}","winlog.event_data.LogonProcessName":"Kerberos","winlog.event_data.ProcessId":"0x0","winlog.event_data.ProcessName":"-","winlog.event_data.RestrictedAdminMode":"-","winlog.event_data.SubjectDomainName":"-","winlog.event_data.SubjectLogonId":"0x0","winlog.event_data.SubjectUserName":"-","winlog.event_data.SubjectUserSid":"S-1-0-

0","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetLinkedLogonId":"0x0","winlog.event_data.TargetLogonId":"0xdadb35","winlog.event_data.TargetOutboundDomainName":"-","winlog.event_data.TargetOutboundUserName":"-","winlog.event_data.TargetUserSid":"S-1-5-21-2625116736-1513678085-1295315389-1122","winlog.event_data.TransmittedServices":"-","winlog.event_data.VirtualAccount":"No","winlog.event_data.WorkstationName":"-","winlog.event_id":"4624","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"776","winlog.process.thread.id":"6444","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1513306","winlog.task":"Logon","winlog.version":"2","_id":"S5eWtpoBScXz9zJbIt7m","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":8.825}

Este evento evidencia una autenticación de red sobre la cuenta de servicio SQL02$, asociada al acceso hacia el entorno SQL comprometido. Sin embargo, el principal problema desde la perspectiva defensiva es que el sistema interpreta esta autenticación como completamente legítima ya que el ticket presentado es válido criptográficamente para el servicio objetivo

La consulta KQL usada para localizar este tipo de acceso fue:

```
event.code:4624 AND
winlog.event_data.AuthenticationPackageName:"Kerberos" AND
winlog.event_data.LogonType:"3" AND
winlog.event_data.TargetUserName:"SQL02$"
```

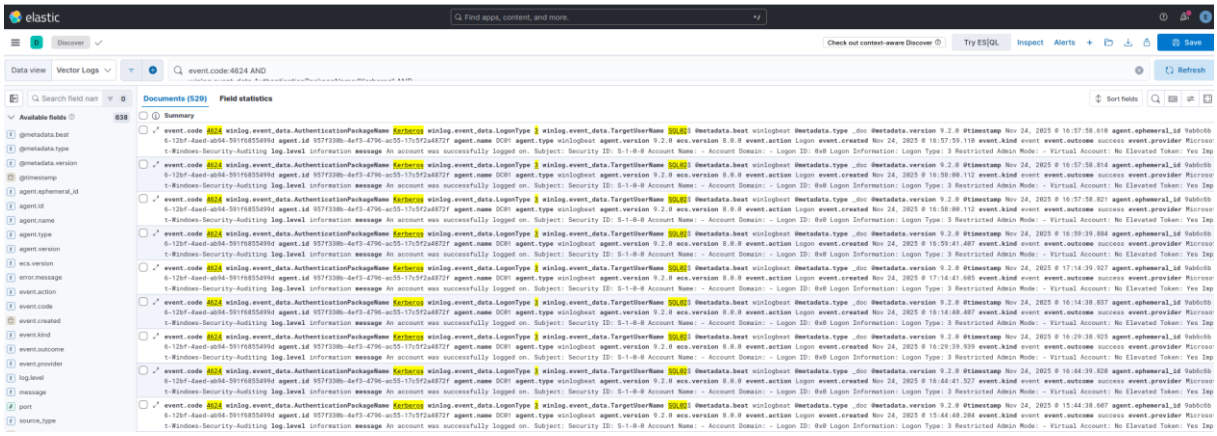

Ilustración 65. Eventos de autenticación Kerberos (Event ID 4624) asociados a la cuenta de servicio SQL02$

Esta imagen muestra eventos de autenticación sobre la cuenta de servicio de SQL02 mediante el protocolo Kerberos.

Además, durante el laboratorio no se observaron eventos adicionales especialmente anómalos asociados a la validación de ticket, precisamente porque Silver Ticket evita gran parte de la interacción habitual con el KDC. Esto supone una diferencia importante respecto a otras técnicas donde el controlador de dominio participa de manera más evidente durante el proceso de autenticación.

La detectabilidad depende en gran medida de elementos indirectos como la correlación entre autenticaciones y ausencia de solicitudes TGS previas, uso anómalo de cuentas de servicio, acceso desde equipos no habituales, patrones laterales inconsistentes...

En entornos sin correlación avanzada estos eventos suelen confundirse fácilmente con autenticaciones Kerberos legítimas generados por servicios internos, cuentas máquina o procesos automatizados.

Por ello, la detectabilidad de Silver Ticket se considera baja ya que los registros generados presentan un comportamiento elevado muy similar al tráfico normal de autenticación Kerberos y no existe una evidencia directa que permita identificar la falsificación del ticket.

Persistencia mediante creación de usuario

Tras obtener acceso administrativo sobre SQL02 se crea una cuenta de usuario dentro de la instancia SQL con el objetivo de mantener persistencia sobre la base de datos comprometida. Esta actividad se corresponde con la técnica MITRE T1098 – Account Manipulation, y T1505.001 - SQL Stored Procedures.

A diferencia de la creación de cuentas AD, esta acción no genero eventos claros en los Security Logs ni del controlador ni en el endpoint. La persistencia se produjo dentro del propio motor SQL por lo que su visibilidad dependía directamente del nivel de auditorio habilitado en MSSQL.

Durante el análisis se realizaron búsquedas sobre eventos del proveedor MSSQL$SQL02 incluyendo sentencia como CREATE LOGIN, CREATE USER, ALTER ROLE o sp_addsrvrolmember, pero no se localizaron registros específicos asociados a la creación del usuario.

La consulta usada fue:

```
agent.name:"SQL02" AND event.provider:"MSSQL$SQL02" AND
(message: *CREATE LOGIN* OR message: *CREATE USER* OR message:
*ALTER ROLE* OR message: *sp_addsrvrolemember*)
```

No se obtuvieron resultados evidenciando una limitación importante, si SQL Server no tiene habilitada auditoria avanzada sobre cambios de seguridad y creación, la creación de usuarios dentro de la base de datos puede pasar desapercibida.

Por ello, la detectabilidad de esta técnica se considera nula ya que no se observaron evidencias de esta actividad. Su detección depende de la configuración especifica de auditoria dentro de SQL.

Conclusiones de detectabilidad de la fase

La fase 5 concentró algunas de las actividades más críticas del laboratorio ya que incluyó escalada de privilegios, ejecución de herramientas ofensivas, acceso a credenciales en memoria, abuso de replicación de Active Directory, falsificación de tickets Kerberos y mecanismos de persistencia tanto en el dominio como en SQL Server.

En primer lugar, las técnicas ejecutadas sobre el endpoint SQL02, como PrintSpoofer y Mimikatz, generaron una visibilidad elevada gracias a Sysmon y a los eventos de finalización de procesos. La aparición de binarios como PrintSpoofer64.exe o mimikatz.exe, junto con actividad relacionada con lsass.exe, constituye un indicador especialmente relevante dentro de un entorno.

Por otro lado, DCSync generó evidencias muy sensibles en DC01 mediante eventos 4662 asociados a permisos de replicación como DS-Replication-Get-Changes y DS-Replication-Get-Changes-All. Aunque estos eventos pueden generar ruido cuando proceden de controladores de dominio legítimos, su aparición asociada a cuentas no esperadas representa un indicador sólido de compromiso.

Las técnicas basadas en tickets Kerberos falsificados presentaron una detectabilidad menor. En el caso de Golden Ticket los eventos 4672 reflejaron autenticaciones con privilegios elevados, pero no permiten confirmar por sí mismos el uso de tickets falsificados. De forma similar, Silver Ticket generó eventos 4624 aparentemente legítimos sobre el servicio objetivo reduciendo la visibilidad en el controlador de dominio y dificultando su identificación sin correlación avanzada.

La creación y uso de la cuenta goldenadmin aportó una evidencia especialmente clara de actividad sensible sobre Active Directory, ya que se observaron eventos 4662 asociados a operaciones de control sobre el directorio y permisos de replicación. Esto refuerza que las acciones administrativas sobre AD suelen ser más detectables que las técnicas basadas únicamente en abuso de autenticaciones válidas.

Finalmente, la persistencia mediante creación de usuario dentro de SQL Server presentó la menor visibilidad de la fase. Aunque se analizaron eventos del proveedor MSSQL$SQL02, no se localizaron registros específicos asociados a CREATE LOGIN, CREATE USER o modificaciones de roles, evidenciando una limitación clara de auditoría en MSSQL.

En conjunto, esta fase mostró una detectabilidad muy variable, desde alta para ejecución de herramientas ofensivas, DCSync y actividad administrativa sensible, pasando por baja para Golden Ticket y Silver Ticket y terminando en nula para la persistencia interna en SQL Server sin auditoría avanzada.

Fase 6 – Reutilización de técnicas Kerberos y compromiso de servicios adicionales

La fase 6 se centró principalmente en el abuso de autenticaciones Kerberos sobre servicios web internos usando técnicas previamente analizadas durante la fase 5, más concretamente ataques relacionados con Silver Ticket y uso indebido de tickets Kerberos validos sobre IIS y otros servicios HTTP internos.

Las técnicas MITRE empleadas fueron:

- T1558.002 – Silver Ticket.
- T550 – User Alternate Authentication Material.

Desde el punto de vista de monitorización, ambas actividades generaron eventos prácticamente idénticos a los ya documentados en fases anteriores.

Las principales características observadas durante esta fase es que el acceso al servicio web comprometido apareció en los registros como una autenticación Kerberos completamente legítima. Debido a esto, no se identificaron indicadores claramente diferenciables que permitan distinguir de forma sencilla entre actividad normal y actividad ofensiva únicamente mediante eventos individuales.

En el caso de Silver Ticket, la dificultad de detección continúa siendo especialmente elevada debido a que el ticket es validado directamente por el servicio comprometido sin necesidad de generar solicitudes visibles adicionales hacia el controlador de dominio. Como consecuencia, gran parte de la telemetría asociada al proceso de autenticación queda limitada exclusivamente al servidor IIS o al endpoint objetivo.

De forma similar, el abuso Kerberos sobre servicios web mediante credenciales o tickets validos genero únicamente eventos estándar de autenticación 4624 interpretados por el sistema como accesos legítimos al servicio.

No obstante, debido a que tanto los eventos generados como las consultas KQL usadas, patrones de autenticación y limitaciones defensivas coinciden prácticamente en su totalidad con los ya desarrollados anteriormente para Silver Ticket y abuso Kerberos en la fase 5, no se profundizara nuevamente en el análisis individual de estas técnicas.

Finalmente, la detectabilidad de esta fase debe interpretarse siguiendo las mismas consideraciones previamente descritas en fases anteriores manteniéndose una visibilidad reducida y una elevada dificultad para diferencia actividad ofensiva de autenticaciones legítimas dentro del dominio.

Fase 7 – Validación del compromiso total del dominio

La fase 7 tuvo como objetivo validar el nivel de compromiso alcanzado sobre el dominio tras las haber ejecutado todas las fases previas. En esta etapa se realizaron acciones orientadas a comprobar y mostrar el control efectivo sobre el Active Directory mediante acceso privilegiado, extracción de credenciales del dominio y uso de sesiones administrativas sobre el controlador de dominio.

A diferencia de fases anteriores donde muchas técnicas presentan una visibilidad reducida por apoyarse en protocolos legítimos o autenticaciones aparentemente normales, esta fase genero indicadores más claros de compromiso avanzado dentro del entorno ELK.

Las técnicas principales fueron:

- Dump de credenciales del dominio.
- Acceso RDP al controlador de dominio.
- Uso de privilegios elevados dentro del dominio.

Dump de credenciales del dominio

Una vez alcanzado un nivel elevado de privilegios dentro del entorno AD, se realizó la extracción de credenciales del dominio usando secretsdump desde el sistema Kali. Esta actividad se corresponde con la técnica MITRE T1003 – OS Credential Dumping.

A diferencia de técnicas clásicas de credential dumping basadas en acceso directo a lsass.exe, este caso de extracción de credenciales se realizó mediante el abuso de mecanismos de replicación AD usando DCSync. Como consecuencia, la principal telemetría observada en el análisis estuvo relacionada con ventos de acceso al servicio de directorio:

- EventID 4662 – Directory Service Access.

Se adjunta log de muestra:

{"event.code":"4662","winlog.event_data.Properties":"Control Access {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T20:26:50.369Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.name":"DC01","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Directory Service Access","event.created":"2025-11-24T20:26:51.784Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-

Windows-Security-Auditing","log.level":"information","message":"An operation was performed on an object. Subject : Security ID: S-1-5-18 Account Name: DC01$ Account Domain: LAB Logon ID: 0x148c65 Object: Object Server: DS Object Type: %{19195a5b-6da0-11d0-afd3-00c04fd930c9} Object Name: %{63ea1f70-4a1a-42b1-95b3-81341d362585} Handle ID: 0x0 Operation: Operation Type: Object Access Accesses: Control Access Access Mask: 0x100 Properties: Control Access {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9} Additional Information: Parameter 1: - Parameter 2: ","source_type":"logstash","timestamp":"2025-11-24T20:26:50.369Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AccessList":"Control Access
","winlog.event_data.AccessMask":"0x100","winlog.event_data.AdditionalInfo":"-","winlog.event_data.HandleId":"0x0","winlog.event_data.ObjectName":"%{63ea1f70-4a1a-42b1-95b3-
81341d362585}","winlog.event_data.ObjectServer":"DS","winlog.event_data.ObjectType":"%{19195a5b-6da0-11d0-afd3-00c04fd930c9}","winlog.event_data.OperationType":"Object Access","winlog.event_data.SubjectDomainName":"LAB","winlog.event_data.SubjectLogonId":"0x148c65","winlog.event_data.SubjectUserName":"DC01$","winlog.event_data.SubjectUserSid":"S-1-5-18","winlog.event_id":"4662","winlog.keywords":"Audit Success","winlog.opcode":"Info","winlog.process.pid":"776","winlog.process.thread.id":"904","winlog.provider_guid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1521407","winlog.task":"Directory Service Access","_id":"MZhVt5oBScXz9zJbdgG2","_ignored":"message.keyword","_index":"vector-2025.11.24","_score":11.023}

El elemento GUID “{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}” es el identificador del permiso DS-Replication-Get-Changes visto en fases anteriores. Este está asociado a operaciones de replicación de AD y es especialmente relevante en ataques DCSync realizados mediante herramientas como secretsdump

La consulta KQL usada para localizar la actividad fue:

```
event.code:4662 AND (winlog.event_data.Properties: *1131f6aa*) AND
NOT winlog.event_data.SubjectUserName: *$
```

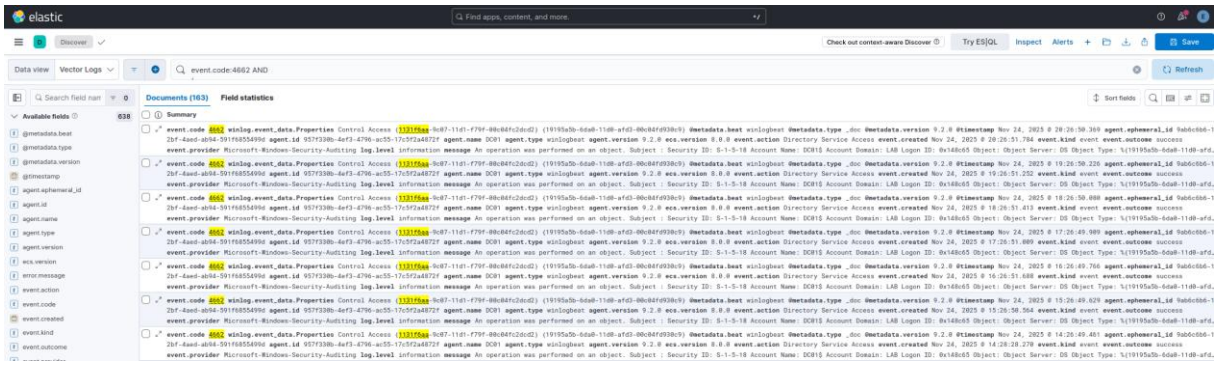

Ilustración 66. Eventos de acceso a objetos de Active Directory (Event ID 4662) asociados a permisos de replicación utilizados en actividades DCSync

Esta imagen muestra eventos 4662 asociados a permisos de replicación de AD que son importantes en eventos relacionados con DCSync.

Uno de los aspectos más importantes observados durante esta fase es que los eventos generados aparecen asociados a la cuenta máquina DC01$. Este comportamiento es habitual

debido a que las operaciones de replicación son procesadas internamente por el propio KDC y usan mecanismos legítimos de AD.

Como consecuencia la atribución directa del evento al atacante no resulta sencilla mediante análisis aislado del log. Precisamente esta característica es una de las principales dificultadas de DCSync ya que gran parte de la actividad puede confundirse con replicación legítima del dominio si no existe relación contextual adicional.

Aun así, la presencia del GUID de DS-Replication-Get-Changes o DS-Replication-Get-Changes-All sigue siendo un indicador muy sensible dentro de AD y debe monitorizarse de forma específica, especialmente cuando aparece asociado a cuentas no habituales o patrones anómalos de replicación.

Por ello, la detectabilidad de esta técnica se considera alta ya que las operaciones de replicación generan eventos relevantes desde la perspectiva defensiva, aunque su correcta interpretación requiera de contexto y correlación avanzada.

Acceso RDP al controlador de dominio

Tras obtener privilegios elevados dentro del entorno AD se realizó acceso remoto al controlador de dominio DC01 mediante RDP. Esta actividad corresponde con la técnica MITRE T1021.001 – Remote Services: Remote Desktop Protocol.

Durante el análisis realizado en ELK se identificaron principalmente eventos de autenticación remota sobre el controlador de dominio:

- EventID 4624 – An account was successfully logged on.

Se adjunta log de muestra:

> {"agent.name":"DC01","event.code":"4624","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T21:43:37.756Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Logon","event.created":"2025-11-24T21:43:39.085Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 10 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: LAB.LOCAL Logon ID: 0x10a3cff Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {59C59C82-E00B-5B43-016F-2FF83C1B4B1A} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: ::1 Source Port: 54955 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0","source_type":"logstash","timestamp":"2025-11-24T21:43:37.756Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.AuthenticationPackageName":"Kerberos","winlog.event_data.ElevatedToken":"Yes","winlog.event_data.ImpersonationLevel":"Impersonation","winlog.event_data.IpAddress":"::1","winlog.event_data.IpPort":"54955","winlog.event_data.KeyLength":"0","winlog.event_data.LogonProcessName":"Kerberos","winlog.event_data.LogonType":"10","winlog.event_data.TargetDomainName":"LAB.LOCAL","winlog.event_data.TargetUserName":"DC01$","winlog.event_id":"4624","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1569670"}

El elemento más relevante de este evento es el valor de Logon Type 10 que es el identificador que corresponde con autenticaciones realizadas mediante RDP. Desde la perspectiva defensiva este tipo de eventos resulta especialmente útil para identificar accesos interactivos remotos hacia sistemas críticos del entorno corporativo especialmente controladores de dominio.

La consulta KQL usada para localizar acceso RDP sobre DC01 fue:

event.code:4624 AND agent.name:"DC01" AND winlog.event_data.LogonType:"10"

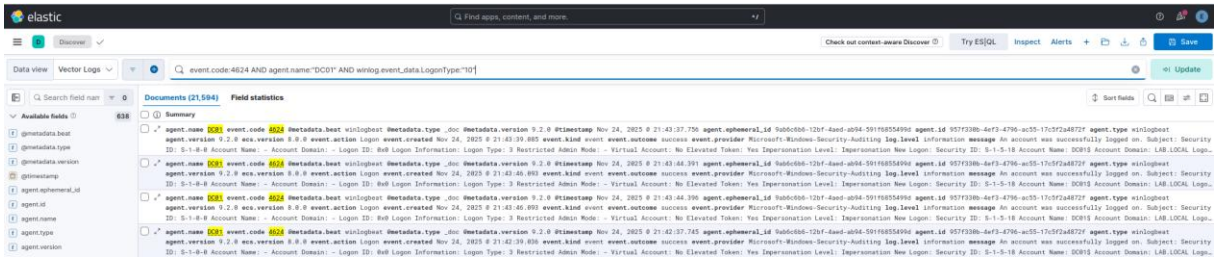

Ilustración 67. Eventos de inicio de sesión remoto mediante RDP (Logon Type 10) registrados en el controlador de dominio DC01

Esta imagen muestra eventos de inicio de sesión mediante RDP en el controlador de dominio.

Uno de los aspectos más importantes observados es que los accesos RDP generan una trazabilidad mucho más visible que otras técnicas usadas anteriormente durante el laboratorio. A diferencia de Golden Ticket o Silver Ticket donde gran parte de la actividad puede confundirse con tráfico Kerberos legítimo, las conexiones RDP producen eventos de autenticación interactiva claramente identificables dentro de los Security Logs.

La combinación de Logon Type 10, autenticaciones Kerberos, Acceso sobre DC01 y sesiones privilegiadas constituyen un indicador especialmente sensible desde el punto de vista defensivo.

Por ello, la detectabilidad de esta técnica se considera alta ya que los accesos RDP generan eventos claramente identificables y fácilmente correlacionables dentro de los Security Logs del controlador de dominio.

Uso de privilegios elevados

Una vez establecido el acceso sobre el controlador de dominio DC01, se identificaron sesiones con privilegios elevados asociadas a autenticaciones privilegiadas dentro del entorno AD. Esta actividad se corresponde con la técnica MITRE T1018 – Remote System Discovery, y T1482 – Domain Trust Discovery.

Durante el análisis realizado en ELK se identificaron principalmente:

- EventID 4672: Special privileges assigned to a new logon.

Se adjunta log de muestra:

{"agent.name":"DC01","event.code":"4672","winlog.event_data.SubjectDomainName":"LAB","@metadata.beat":"winlogbeat","@metadata.type":"_doc","@metadata.version":"9.2.0","@timestamp":"2025-11-24T21:43:37.756Z","agent.ephemeral_id":"9ab6c6b6-12bf-4aed-ab94-591f6855499d","agent.id":"957f330b-4ef3-4796-ac55-17c5f2a4872f","agent.type":"winlogbeat","agent.version":"9.2.0","ecs.version":"8.0.0","event.action":"Special Logon","event.created":"2025-11-

24T21:43:39.085Z","event.kind":"event","event.outcome":"success","event.provider":"Microsoft-Windows-Security-Auditing","log.level":"information","message":"Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: LAB Logon ID: 0x10a3cff Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege","source_type":"logstash","timestamp":"2025-11-24T21:43:37.756Z","winlog.channel":"Security","winlog.computer_name":"DC01.lab.local","winlog.event_data.PrivilegeList":"SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege","winlog.event_data.SubjectLogonId":"0x10a3cff","winlog.event_data.SubjectUserName":"DC01$","winlog.event_id":"4672","winlog.provider_name":"Microsoft-Windows-Security-Auditing","winlog.record_id":"1569669"}

Este evento evidencia la asignación de privilegios elevados sobre una nueva sesión autenticada dentro del controlador de dominio. Entre los privilegios más sensibles destacan:

- SeDebugPrivilege.
- SeBackupPrivilege.
- SeRestorePrivilege.
- SeImpersonatePrivilege.
- SeEnableDelegationPrivilege.

Este tipo de privilegios se encuentra asociado a cuentas altamente privilegiadas dentro del dominio y permiten realizar operaciones críticas sobre el sistema operativo, credenciales, servicios y mecanismos de autenticación.

La consulta KQL usada para localizar sesiones privilegiadas sobre DC01 fue:

```
event.code:4672 AND agent.name:"DC01" AND
winlog.event_data.SubjectDomainName:"LAB" AND NOT
winlog.event_data.SubjectUserName:"SYSTEM" AND NOT
winlog.event_data.SubjectUserName: *$
```

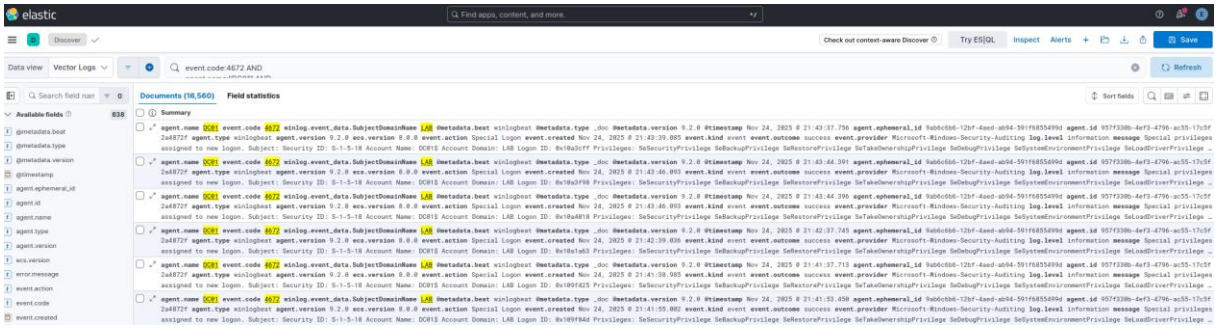

Ilustración 68. Eventos de asignación de privilegios especiales (Event ID 4672) registrados en el controlador de dominio DC01

En esta imagen se muestran eventos de asignación de privilegios especiales sobre el controlador de dominio DC01.

Desde una perspectiva defensiva, el EventID 4672 constituye uno de los indicadores más relevantes para identificar sesiones administrativas o autenticaciones con privilegios elevados dentro de AD.

La presencia de los privilegios sensibles es especialmente relevante desde el punto de vista defensivo ya que suelen estar relacionados con operaciones críticas de administración y control del dominio.

Por ello, la detectabilidad de esta técnica se considera alta ya que las sesiones privilegiadas generan eventos administrativos claramente identificables dentro de los Security Logs del controlador de dominio.

Conclusiones de detectabilidad de la fase

La fase 7 represento el punto de mayor impacto operativo dentro del laboratorio ya que el atacante consiguió acceso directo sobre el controlador de dominio y capacidad para operar con privilegios elevados dentro del AD. Desde la perspectiva defensiva, esta etapa presento un nivel de visibilidad considerablemente superior al observado en fases anteriores debido a que muchas de las acciones realizadas afectaron directamente a servicios críticos del dominio y generaron eventos altamente sensibles dentro de los Security Logs.

Uno de los aspectos más relevantes de esta fase es que las técnicas relacionadas con replicación AD, acceso remoto privilegiado y uso de privilegios administrativos generan una trazabilidad mucho más clara dentro de entornos monitorizados. Eventos como EventID 4662, 4624 y 4672, permiten identificar operaciones especialmente sensibles dentro del dominio, autenticaciones remotas y sesiones privilegiadas dentro del DC01.

En el caso concreto del dump de credenciales mediante técnicas equivalentes a DCSync, la presencia del GUID asociado a permisos de replicación constituye uno de los indicadores más útiles desde la perspectiva defensiva. Aun así, también se observó una limitación importante ya que gran parte de estos eventos aparecen asociados a cuentas máquina DC01$, lo que introduce ruido y dificulta diferenciar automáticamente la actividad legítima de replicación frente al abuso ofensivo.

Por otra parte, el acceso RDP al controlador de dominio genero eventos claramente identificables gracias al uso de Logon Type 10 proporcionando una visibilidad mucho más elevada que otras técnicas basadas exclusivamente en Kerberos. Este comportamiento demuestra que los accesos interactivos remotos continúan siendo uno de los mecanismos más sencillos de monitorizar dentro de entornos Windows corporativos.

Asimismo, los eventos 4672 asociados a privilegios especiales permitieron identificar sesiones altamente privilegiadas dentro del dominio. La correlación entre autenticaciones, sesiones remotas y privilegios elevados proporcionan evidencias especialmente relevantes desde el punto de vista defensivo.

De forma general esta fase pone de manifiesto que el comportamiento directo del controlador de dominio incrementa notablemente la superficie de detección para el SIEM. A diferencia de fases anteriores donde muchas técnicas podían operar de manera relativamente sigilosa usando tickets Kerberos validos o autenticaciones aparentemente legítimas, las acciones realizadas sobre DC01 generaron registros administrativos mucho más visibles y fácilmente correlacionables.

Por ello, la detectabilidad global de esta fase se considera alta ya que las operaciones realizadas afectaron directamente a mecanismos críticos de autenticación, replicación y

administración del dominio generando múltiples evidencias observables dentro del entorno monitorizado.

Comparativa de detectabilidad entre técnicas

Una vez analizadas individualmente las distintas fases del laboratorio, ahora es posible realizar una comparación transversal entre técnicas ejecutadas con el objetivo de identificar cuales presentan mayor capacidad de detección, cuales generan más ruido dentro del entorno y cuales pueden pasar prácticamente desapercibido incluso en sistemas monitorizados.

Este análisis comparativo permite evaluar no solo la capacidad ofensiva de cada técnica sino también el comportamiento real de los mecanismos de logging desplegados en el dominio y las limitaciones observadas durante el proceso de monitorización. Durante las fases del laboratorio, se comprobó que la detectabilidad de una técnica no depende necesariamente de su impacto sobre el entorno o del nivel de privilegios obtenido, sino principalmente de varios factores relacionados con la visibilidad disponible:

- Eventos generados por la técnica.
- Contexto en el que se ejecuta.
- Nivel de auditoria habilitado.
- Capacidad de correlación del SIEM.
- Similitud respecto al comportamiento legítimo del dominio.

Como consecuencia, algunas técnicas extremadamente críticas desde el punto de vista ofensivo generan evidencias muy claras dentro del sistema mientras que otras capaces de comprometer servicios sensibles apenas dejan trazabilidad. Esto fue muy visible en ataques basados en reutilización de credenciales válidas o abuso de Kerberos donde gran parte de la actividad observada resulta prácticamente indistinguible del comportamiento normal del entorno.

Comparativa global de técnicas

A partir de las fases analizadas anteriormente, pude establecer una comparativa global entre las siguientes técnicas ejecutadas en el laboratorio:

Técnica	Detectabilidad	Dependencia de Sysmon	Necesidad de correlación	Observaciones
Escaneo de red	Baja	Alta	Alta	El tráfico generado puede confundirse fácilmente con tareas legítimas de administración o inventariado

Kerbrute	Media	Baja	Alta	Genera eventos Kerberos visibles, aunque requiere análisis temporal y umbrales adecuados
BloodHound / SharpHound	Baja	Media	Alta	SharpHound realiza múltiples consultas LDAP sobre usuarios, grupos y relaciones de privilegios en intervalos reducidos de tiempo
Password Spraying	Alta	Baja	Alta	Las secuencias masivas de autenticaciones fallidas producen patrones claramente identificables
Acceso SMB lateral	Baja	Baja	Alta	Los eventos SMB 5140 y 5145 aparecen con frecuencia en accesos internos a recursos compartidos del dominio

Kerberoasting	Alta	Baja	Media	Las solicitudes TGS asociadas a cifrado RC4 pueden indicar intentos de obtención de tickets Kerberos para cuentas de servicio vulnerables
Delegación Kerberos (S4U)	Media	Baja	Alta	Requiere contexto adicional sobre delegaciones legítimas configuradas en el entorno
Acceso SQL con credenciales válidas	Baja	Baja	Alta	Desde el punto de vista del sistema se comporta como actividad corporativa legítima
xp_cmdshell	Alta	Alta	Media	La ejecución de cmd.exe o powershell.exe desde sqlservr.exe resulta altamente anómala
Explotación web	Baja	Media	Alta	El elevado volumen de tráfico HTTP dificulta enormemente la detección

Transferencia de herramientas	Media	Alta	Alta	Detectable principalmente mediante creación de archivos y ejecución de binarios observados con Sysmon
PrintSpoofer	Media	Alta	Alta	La elevación es observable, aunque compleja de clasificar sin contexto adicional
DCSync	Alta	Baja	Media	Los accesos de replicación Active Directory generan eventos extremadamente específicos
Golden Ticket	Baja	Media	Alta	Presenta muy poca visibilidad directa dentro de los Security Logs

Silver Ticket	Nula/Baja	Media	Alta	La ausencia de interacción con el controlador de dominio reduce enormemente la detección
Reutilización de tickets Kerberos	Baja	Baja	Alta	El uso de tickets válidos se comporta como autenticación legítima
Dumping de credenciales	Alta	Alta	Media	El acceso a LSASS constituye uno de los comportamientos más anómalos observados

Tabla 37. Resumen comparativo de detectabilidad de técnicas ofensivas en entornos Active Directory monitorizados mediante ELK y Sysmon

Esta comparativa muestra que la existencia de logs no implica necesariamente una detección efectiva. En numerosos casos las técnicas generan eventos validos dentro del sistema, pero dichos eventos carecen de suficiente contexto para ser considerados sospechosos de forma aislada.

Técnicas con mayor detectabilidad

Las técnicas que presentaron una detectabilidad más alta durante el laboratorio fueron principalmente aquellas que generan eventos muy específicos dentro del controlador de dominio o producen actividad claramente anómala a nivel de sistema operativo. Entre las más visibles tenemos:

- Password Spraying.
- Kerberoasting.
- DCSync.
- Dumping de credenciales.
- Ejecución de comandos mediante xp_cmdshell.

En estos casos la detección resulto relativamente sencilla debido a la existencia de indicadores muy concretos dentro de los logs como, por ejemplo:

- Grandes volúmenes de eventos 4625 en ataques de fuerza bruta dirigida.

- Eventos 4769 asociados al uso de cifrado RC4 en Kerberoasting.
- Eventos 4662 relacionados con replicación AD en DCSync.
- Acceso a LSASS detectado mediante Sysmon EventID 10.
- Procesos hijos anómalos ejecutados desde sqlservr.exe.

Además, muchas de estas técnicas producen patrones poco habituales dentro del funcionamiento normal del dominio facilitando la creación de reglas de detección eficaces dentro del SIEM.

Otro aspecto relevante es que estas técnicas no solo generan eventos claros, sino que además presentan una baja ambigüedad respecto al comportamiento legítimo. Esto también reduce la necesidad de contexto adicional para interpretar correctamente la evidencia obtenida.

Técnicas con mayor dificultad ofensiva

En contraste, las técnicas más complejas de detectar fueron aquellas que usan mecanismos completamente legítimos del sistema y generan actividad prácticamente idéntica a la observada diariamente dentro del entorno corporativo.

Las más problemáticas desde este punto de vista fueron las siguientes:

- Enumeración LDAP mediante BloodHound.
- Movimiento lateral mediante SMB.
- Acceso SQL con credenciales válidas.
- Explotación de servicios web.
- Reutilización de tickets Kerberos.

Estas técnicas no destacan por ausencia de eventos sino por el elevado nivel de ruido asociado a los protocolos usados. Por ejemplo, dentro de un dominio de AD es completamente normal ver consultas LDAP constantes, accesos SMB entre workstations y servidores, autenticaciones Kerberos legítimas, conexiones frecuentes a bases de datos SQL y gran volumen de tráfico HTTP hacia servidores internos.

Como consecuencia de esto, la actividad ofensiva queda diluida entre miles de eventos legítimos generados continuamente por el entorno.

Durante el laboratorio se comprobó que este tipo de técnicas requieren una fuerte dependencia de los siguientes elementos:

- Correlación temporal.
- Análisis de comportamiento.
- Contexto del usuario y del host.
- Baselines de actividad normal.
- Reglas avanzadas orientadas a anomalías.

Esto evidencia que la dificultad principal no reside en generar eventos sino en diferenciar correctamente actividad maliciosa de comportamiento corporativo habitual.

Técnicas de menor visibilidad

Las técnicas con menor visibilidad fueron principalmente las basadas en abuso avanzado de Kerberos y reutilización de credenciales válidas:

- Silver Ticket.

- Golden Ticket.
- Pass-The-Hash.
- Movimiento lateral mediante credenciales comprometidas.

Estas técnicas presentan una característica especialmente problemática, y es que desde el punto de vista del sistema gran parte de la actividad parece completamente legítima.

En el caso concreto de Silver Ticket, el controlador de dominio ni siquiera participa directamente en determinadas autenticaciones, reduciendo la capacidad de detección centralizada. Esto limita la generación de eventos relevantes en DC01 y desplaza la visibilidad únicamente al servicio comprometido.

Golden Ticket también presento una detectabilidad reducida debido a que los tickets generados continúan usando mecanismos validos de Kerberos. Aunque pueden observarse ciertos comportamientos anómalos, la identificación efectiva requiere de correlaciones avanzada y análisis contextual profundo.

Este comportamiento convierte las técnicas basadas en abuso de tickets Kerberos en algunos de los escenarios más complejos de detectar dentro de entornos AD monitorizados.

Impacto de Sysmon en la visibilidad del entorno

Uno de los hallazgos más importantes observados durante el laboratorio fue el enorme impacto que tiene Sysmon sobre la capacidad de detección del entorno.

Las técnicas relacionadas con:

- Ejecución de herramientas ofensivas.
- LOLBins.
- Transferencia de binarios.
- Dumping de credenciales.
- Elevación local de privilegios.
- Ejecución remota de comandos.

Estas dependen casi completamente de la telemetría adicional proporcionada por Sysmon. Si esta herramienta, muchas actividades habrían quedado reducidas únicamente a autenticaciones genéricas o conexiones de red sin contexto suficiente para interpretar correctamente el comportamiento del atacante.

La capacidad de Sysmon fue especialmente útil par a registrar:

- Terminación de procesos.
- Acceso a procesos sensibles.
- Creación y modificación de archivos.

Gracias a esta información fue posible reconstruir gran parte de la actividad ofensiva de los Security Logs nativos de Windows no reflejan adecuadamente.

Por lo tanto, una de las principales conclusiones obtenidas es que una monitorización basada únicamente en logs nativos de Windows resulta insuficiente frente a técnicas modernas de postexplotación y movimiento lateral.

Dependencia de correlación y análisis contextual

Otro aspecto importante observado es que muchas técnicas únicamente resultaron detectables cuando varios eventos eran correlacionados correctamente dentro del SIEM.

En estos casos, los eventos individuales carecían de suficiente contexto para considerarse sospechosos por si solos. El valor defensivo aparecía únicamente al reconstruir secuencias completas de actividad ofensiva.

Algunos ejemplos son:

- Múltiples eventos 4625 seguidos de un 4624 exitoso.
- Solicitudes TGS anómalas combinadas con uso posterior de cuentas de servicio.
- Accesos SMB precedidos por enumeración LDAP.
- Autenticaciones privilegiadas seguidas de acceso a LSASS.
- Ejecución de herramientas ofensivas tras conexiones remotas previas.

Esto demuestra que la simple existencia de logs no implica capacidad real de detección. La efectividad defensiva depende principalmente de:

- La calidad de las reglas implementadas.
- Conocimiento del comportamiento normal del entorno.
- Granularidad de las fuentes de datos disponibles.
- Capacidad de correlación en el SIEM.
- Capacidad de análisis contextual de nuestra parte.

Conclusiones comparativas

A partir de este análisis transversal realizado, puede extraerse varias conclusiones relevantes sobre la detectabilidad de ataque en entornos AD monitorizados:

- Las técnicas más peligrosas no siempre son las más visibles.
- Kerberoasting y DCSync generan evidencias especialmente útiles defensivamente.
- SMB, LDAP y la reutilización de credenciales presentan una detectabilidad considerablemente menor.
- Sysmon mejora la trazabilidad en el entorno.
- Muchas técnicas solo pueden identificarse mediante correlación avanzada.
- El uso de credenciales válidas continúa siendo uno de los mayores retos desde el punto de vista defensivo.
- La monitorización basada únicamente en Security Logs resulta insuficiente frente a técnicas modernas de postexplotación.
- La capacidad real de detección depende más de la correlación y del contexto que de la cantidad de eventos generados.

Finalmente, el análisis realizado demuestra que la detectabilidad en AD no depende exclusivamente de la existencia de mecanismos de logging sino de la capacidad del entorno para interpretar correctamente el comportamiento observado. En consecuencia, la detección efectiva requiere combinar múltiples fuentes de datos, correlación avanzada y conocimiento contextual del funcionamiento normal del dominio.

Conclusiones del análisis de detectabilidad

El análisis realizado a lo largo de este apartado de las distintas fases ofensivas del laboratorio ha permitido evaluar de forma práctica la capacidad real de detección de múltiples técnicas usadas habitualmente en ataques contra entornos AD. A diferencia de un enfoque centrado únicamente en la explotación ofensiva, esta parte del trabajo ha permitido estudiar qué evidencias generan estas técnicas ofensivas, cómo se comportan los sistemas de monitorización ante ellas y cuáles son las principales limitaciones observadas desde el punto de vista defensivo.

Uno de los principales hallazgos obtenidos durante el análisis es que la existencia de logs no implica necesariamente capacidad real de detección. En numerosos casos, las técnicas ejecutadas sí generaban eventos dentro del sistema, pero estos eran ambiguos, insuficientes o demasiado similares a la actividad habitual del dominio. Esto fue especialmente visible en técnicas basadas en reutilización de credenciales válidas, acceso SMB, abuso de delegaciones Kerberos (S4U), Golden Ticket o Silver Ticket.

En estos escenarios, la dificultad principal no fue la ausencia de eventos sino la complejidad de diferenciar actividad maliciosa de comportamiento corporativo normal. Precisamente, algunas de las técnicas con mayor impacto ofensivo fueron también las que presentaron una detectabilidad más reducida durante el laboratorio. Esto permitió observar que severidad e identificabilidad no mantienen una relación directa dentro de entornos Active Directory.

Por el contrario, las técnicas que generaron una detectabilidad más alta fueron aquellas que produjeron eventos muy específicos o comportamientos claramente anómalos dentro del entorno. Entre las más visibles destacaron Password Spraying, Kerberoasting, DCSync y determinadas acciones de persistencia mediante creación de cuentas privilegiadas. En términos generales, las técnicas asociadas a autenticaciones anómalas, replicación de Active Directory o asignación de privilegios elevados resultaron significativamente más visibles que aquellas basadas en reutilización de tickets Kerberos o uso de credenciales válidas.

Estas técnicas generaron indicadores particularmente útiles desde el punto de vista defensivo como eventos 4769 asociados a RC4, secuencias masivas de autenticaciones fallidas, eventos 4662 relacionados con replicación de Active Directory o asignaciones de privilegios especiales. En consecuencia, resultó mucho más sencillo construir reglas de detección y correlaciones eficaces dentro de ELK.

En un punto intermedio se situaron técnicas como BloodHound, SharpHound, xp_cmdshell o PrintSpoofer. Estas actividades sí generaron evidencias relevantes dentro del entorno, aunque en muchos casos requerían análisis adicional para interpretarse correctamente. Por ejemplo, las consultas LDAP realizadas por BloodHound podían confundirse con tareas administrativas reales, mientras que técnicas como xp_cmdshell o PrintSpoofer únicamente resultaron claramente visibles cuando se disponía de telemetría avanzada basada en Sysmon.

Otro de los aspectos más relevantes observados durante el análisis fue el enorme impacto que tuvo Sysmon sobre la visibilidad del entorno. Gran parte de las técnicas de postexplotación apenas dejaron evidencias relevantes dentro de los Security Logs nativos de Windows y únicamente se pudieron reconstruir gracias a la telemetría adicional proporcionada por Sysmon.

Gracias a esta información fue posible identificar la ejecución de herramientas ofensivas, LOLBins, elevaciones de privilegios locales, transferencia de binarios, creación de procesos sospechosos y dumping de credenciales. Esto demostró una dependencia clara de Sysmon para detectar técnicas relacionadas con ejecución de procesos, herramientas ofensivas y abuso de binarios legítimos del sistema. Sin esta telemetría adicional, gran parte de estas

actividades habrían presentado una visibilidad extremadamente reducida utilizando únicamente los mecanismos de logging nativos del sistema operativo.

Esto permitió extraer una de las principales conclusiones del trabajo: una monitorización basada exclusivamente en Security Logs resulta claramente insuficiente frente a técnicas modernas de postexplotación y movimiento lateral.

Además, el análisis demostró que la correlación constituye uno de los elementos más importantes dentro del entorno de detección. En numerosos casos, los eventos individuales no resultaban suficientemente representativos por sí solos y únicamente adquirían valor defensivo cuando eran analizados conjuntamente dentro del SIEM.

Esto demostró que la capacidad real de detección depende principalmente de la calidad de las reglas empleadas, capacidad de correlación del SIEM, nivel de auditoría desplegado, fuentes de datos disponibles y conocimiento contextual del comportamiento normal del entorno.

Otro aspecto especialmente relevante observado fue la diferencia existente entre detectabilidad e impacto ofensivo. Algunas de las técnicas más críticas desde el punto de vista del compromiso del dominio fueron precisamente aquellas que presentaron una visibilidad más reducida dentro del entorno monitorizado.

Estas técnicas usan mecanismos legítimos del sistema y reducen considerablemente la generación de eventos sospechosos, dificultando enormemente su identificación incluso en entornos monitorizados.

En el caso concreto de Silver Ticket, el hecho de que determinadas autenticaciones no requieran interacción directa con el controlador de dominio reduce drásticamente la capacidad de detección centralizada. Esto limita considerablemente la visibilidad disponible en los logs del DC y provoca que gran parte de la actividad quede registrada exclusivamente en el host que ofrece el servicio comprometido, sin generar trazabilidad completa en el controlador de dominio, convirtiéndolo en uno de los escenarios más complejos observados durante el análisis.

Por otro lado, también se comprobó que la detectabilidad depende enormemente del contexto del entorno monitorizado. El laboratorio fue desplegado en una infraestructura controlada y con un volumen relativamente reducido de actividad legítima, lo que facilitó considerablemente la identificación de determinados comportamientos anómalos.

En un entorno corporativo real con cientos o miles de equipos, gran parte de los eventos observados durante el laboratorio quedarían mezclados entre enormes volúmenes de autenticaciones, accesos SMB, tráfico LDAP y actividad administrativa legítima, aumentando significativamente la dificultad del proceso de detección.

En consecuencia, una de las conclusiones más importantes del trabajo es que la detección efectiva en AD no depende únicamente de recopilar logs, sino de la capacidad del entorno para interpretar correctamente el comportamiento observado a partir de la correlación, análisis contextual y fuentes de telemetría adecuadas.

Finalmente, el laboratorio ha permitido demostrar que Active Directory continúa siendo un entorno especialmente complejo desde el punto de vista defensivo debido a que muchas de las técnicas usadas por atacantes se apoyan en funcionalidades completamente legítimas del sistema. Esto provoca que la línea entre actividad normal y comportamiento malicioso sea extremadamente difusa en numerosos escenarios.

Como conclusión, la capacidad real de detección frente a ataques avanzados requiere combinar:

- Múltiples fuentes de datos.
- Monitorización avanzada mediante herramientas como Sysmon.
- Correlación entre eventos.
- Análisis temporal y contextual.
- Conocimiento profundo del funcionamiento normal del dominio.

A partir de todo el análisis realizado, puede concluirse que la detectabilidad en Active Directory depende menos de la existencia de eventos aislados y más de la capacidad del entorno para correlacionar múltiples fuentes de datos, interpretar comportamientos anómalos y mantener visibilidad avanzada sobre sistemas, procesos y autenticaciones.

6. Conclusiones Finales

Con la realización de este Trabajo de Fin de Grado se ha permitido desarrollar una visión global y práctica sobre uno de los mayores retos actuales en ciberseguridad corporativa, que es la protección y detección de amenazas en entornos Active Directory. Más allá de la ejecución técnica de ataques o de la implementación de herramientas de monitorización, el proyecto ha servido para demostrar cómo la seguridad de una infraestructura moderna depende en gran medida de la capacidad de comprender el comportamiento real del atacante dentro del sistema y no únicamente de la existencia de mecanismos preventivos tradicionales.

Uno de los aspectos más relevantes observados durante el desarrollo del laboratorio es que Active Directory continúa representando el núcleo operativo de la mayoría de las infraestructuras empresariales modernas concentrando autenticación, autorización, gestión de identidades y control de acceso. Precisamente por esa centralización cualquier debilidad dentro del dominio tiene un impacto potencialmente crítico sobre toda la organización. Sin embargo, el trabajo demuestra que el riesgo no suele estar asociado exclusivamente a vulnerabilidades técnicas complejas, sino a configuraciones inseguras, exceso de confianza interna y malas prácticas administrativas acumuladas con el tiempo.

A lo largo del proyecto se ha comprobado que un atacante no necesita explotar fallos sofisticados para comprometer un entorno corporativo completo. En muchos casos basta con combinar pequeñas debilidades aparentemente aisladas como credenciales expuestas en recursos compartidos, cuentas de servicio mal configuradas, permisos excesivos, delegaciones inseguras o reutilización de contraseñas. Individualmente muchas de estas configuraciones podrían considerarse riesgos menores o incluso habituales dentro de entornos reales. Sin embargo, cuando se analizan desde una perspectiva ofensiva encadenada se convierten en elementos que facilitan enormemente la progresión del ataque.

Este punto resulta especialmente importante porque pone de manifiesto que la seguridad no falla necesariamente por una única vulnerabilidad crítica, sino por la acumulación progresiva de pequeñas decisiones inseguras que combinadas generan rutas completas de compromiso. Precisamente, una de las principales aportaciones de este trabajo ha sido demostrar de forma práctica cómo un atacante puede evolucionar desde un acceso limitado hasta el control total del dominio utilizando exclusivamente funcionalidades legítimas del sistema y configuraciones habituales en organizaciones reales.

En este contexto, el proyecto evidencia que las técnicas modernas de postexplotación han evolucionado hacia modelos mucho más silenciosos y difíciles de identificar. Herramientas y técnicas como Kerberoasting, abuso de tickets Kerberos, movimiento lateral mediante SMB, uso de WinRM, enumeración LDAP o abuso de delegaciones no generan necesariamente

comportamientos claramente maliciosos desde el punto de vista del sistema operativo. Por el contrario, utilizan exactamente los mismos protocolos y servicios empleados diariamente por administradores, usuarios y aplicaciones corporativas.

Este hecho introduce uno de los mayores desafíos actuales para los equipos defensivos, diferenciar actividad legítima de actividad maliciosa cuando ambas comparten los mismos mecanismos técnicos. Durante el desarrollo del laboratorio quedó demostrado que muchas acciones ofensivas generan eventos válidos y esperables dentro del dominio reduciendo enormemente la eficacia de modelos tradicionales basados únicamente en alertas estáticas o eventos individuales.

En consecuencia a esto, el trabajo permite concluir que la detección moderna en Active Directory ya no puede depender exclusivamente de indicadores simples o reglas aisladas. La realidad observada durante el proyecto demuestra que la detección efectiva depende de contextualización, correlación temporal y análisis de comportamiento. No basta con registrar eventos sino que es necesario interpretar cómo se relacionan entre sí, qué secuencia siguen y si representan desviaciones respecto al comportamiento normal del entorno.

Precisamente aquí cobra especial importancia el uso de plataformas SIEM y sistemas de observabilidad avanzada como ELK. La centralización de logs permitió comprobar que disponer de grandes volúmenes de información no garantiza automáticamente capacidad de detección. De hecho, uno de los problemas más relevantes identificados fue el enorme nivel de ruido generado por sistemas corporativos modernos. La dificultad no radica en obtener datos sino en identificar cuáles aportan realmente valor analítico.

Durante el análisis realizado, muchas técnicas ofensivas únicamente pudieron identificarse cuando se correlacionaron múltiples evidencias procedentes de distintas fuentes. Por ejemplo, determinadas solicitudes Kerberos podían parecer completamente normales de forma aislada pero adquirían relevancia al relacionarse con ejecución de procesos sospechosos, patrones anómalos de autenticación o accesos inusuales entre sistemas. Esto evidencia que la detección efectiva depende cada vez más de modelos de comportamiento y no de eventos independientes.

Otro aspecto significativo es la importancia que adquieren las fuentes de telemetría enriquecidas. La incorporación de Sysmon permitió aumentar considerablemente la visibilidad sobre el comportamiento interno de los sistemas proporcionando información crítica sobre creación de procesos, conexiones de red, acceso a memoria o relaciones parent-child entre aplicaciones. Sin este tipo de telemetría avanzada gran parte de las técnicas utilizadas habrían pasado prácticamente desapercibidas o habrían carecido de suficiente contexto para su análisis.

Del mismo modo, el proyecto demuestra que muchas organizaciones continúan centrando sus esfuerzos defensivos principalmente en amenazas externas, dejando en segundo plano la monitorización interna del dominio. Sin embargo, una vez obtenido acceso legítimo mediante credenciales válidas, el atacante puede operar dentro de la infraestructura con un nivel de visibilidad extremadamente reducido. Este comportamiento quedó claramente reflejado en múltiples fases del laboratorio, especialmente en aquellas basadas en reutilización de credenciales y abuso de autenticación Kerberos.

Otro de los elementos más importantes observados es la relación directa entre privilegios delegados y superficie de ataque. Active Directory está diseñado para facilitar la administración distribuida de entornos complejos pero precisamente esa flexibilidad puede convertirse en un problema cuando los permisos no se controlan adecuadamente. El análisis realizado mediante BloodHound permitió visualizar cómo pequeñas delegaciones administrativas o relaciones

indirectas entre objetos pueden generar rutas completas de escalada de privilegios difíciles de detectar a simple vista.

Desde una perspectiva estratégica, el trabajo también pone de manifiesto la necesidad de adoptar modelos de seguridad basados en “Zero Trust” y segmentación lógica dentro del dominio. La excesiva confianza implícita entre sistemas internos continúa siendo uno de los principales facilitadores del movimiento lateral. Una vez comprometido un equipo, el atacante puede aprovechar relaciones legítimas entre servicios para expandirse progresivamente por la infraestructura.

Igualmente, el proyecto demuestra la importancia crítica de la higiene de credenciales dentro de las organizaciones. La reutilización de contraseñas, el almacenamiento inseguro de credenciales o el uso de cuentas de servicio con configuraciones débiles continúan siendo uno de los principales vectores de compromiso en entornos corporativos. En muchos casos, las técnicas más efectivas no fueron las más sofisticadas sino aquellas que aprovecharon errores operativos básicos acumulados dentro del dominio.

A nivel metodológico, el uso del marco MITRE ATT&CK aportó una estructura muy valiosa para contextualizar cada técnica dentro de tácticas reales observadas en incidentes de ciberseguridad. Esto permitió no solo clasificar técnicamente las acciones realizadas sino también entender cómo se relacionan entre sí dentro de una intrusión completa. El resultado es un análisis mucho más cercano a escenarios reales de ataque y defensa, alejándose de enfoques puramente académicos o aislados.

Asimismo, la utilización de métricas CVSS permitió complementar el estudio desde una perspectiva orientada al riesgo, ayudando a comprender que la severidad de una vulnerabilidad no depende únicamente de su complejidad técnica sino también de su capacidad para formar parte de cadenas de ataque más amplias.

Desde un punto de vista académico y profesional, el desarrollo de este proyecto ha supuesto una experiencia especialmente enriquecedora al integrar conocimientos de redes, sistemas, seguridad ofensiva, monitorización y análisis defensivo dentro de un único entorno práctico. La construcción completa del laboratorio, la resolución de problemas reales de configuración y la validación experimental de las técnicas me permitieron obtener una comprensión mucho más profunda de cómo funcionan realmente las infraestructuras corporativas modernas.

Finalmente, este trabajo permite extraer una conclusión especialmente relevante, en ciberseguridad, la dificultad ya no reside únicamente en evitar que un atacante entre en la infraestructura sino en ser capaces de detectar cómo se comporta una vez dentro. Los entornos Active Directory modernos presentan una complejidad tan elevada y una integración tan profunda entre servicios que muchas actividades maliciosas se confunden fácilmente con operaciones legítimas del sistema.

Por tanto, la principal reflexión que deja este proyecto es que la seguridad efectiva en entornos corporativos debe evolucionar desde modelos centrados exclusivamente en prevención hacia enfoques orientados a visibilidad, correlación y análisis continuo del comportamiento. La capacidad de comprender el contexto de los eventos, identificar desviaciones y relacionar evidencias dispersas se convierte así en uno de los pilares fundamentales de la defensa moderna frente a amenazas avanzadas.

7. Bibliografía

[1] MITRE Corporation, *MITRE ATT&CK Framework*, MITRE ATT&CK, s. f.

[2] Microsoft, *Active Directory Domain Services Overview*, Microsoft Learn, s. f.

[3] Microsoft, *Kerberos Authentication Overview*, Microsoft Learn, s. f.

[4] Elastic NV, *Elastic Stack Documentation*, Elastic Documentation, s. f.

[5] Microsoft, *Sysmon Documentation*, Sysinternals, s. f.

[6] Elastic NV, *Winlogbeat Documentation*, Elastic Documentation, s. f.

[7] Elastic NV, *Kibana Guide*, Elastic Documentation, s. f.

[8] FIRST, *Common Vulnerability Scoring System v3.1 Specification Document*, FIRST, s. f.

[9] Hack The Box, *Hack The Box Academy – Pentester Role Path*, Hack The Box Academy, s. f.

[10] PortSwigger, *Web Security Academy*, PortSwigger, s. f.

[11] Fortra, *Impacket Documentation*, GitHub, s. f.

[12] OpenWall, *John the Ripper Documentation*, OpenWall, s. f.

[13] Nmap Project, *Nmap Reference Guide*, Nmap.org, s. f.

[14] Offensive Security, *Kali Linux Tools Documentation*, Kali Linux Documentation, s. f.

[15] VMware, *VMware Workstation Pro Documentation*, VMware Documentation, s. f.

[16] INE Security, *eJPTv2 – eLearnSecurity Junior Penetration Tester Certification*, INE Security, s. f.

[17] INE Security, *INE Penetration Testing Student Training Path*, INE Security, s. f.

[18] Linux Professional Institute, *LPIC-1: Linux Administrator Certification*, Linux Professional Institute, s. f.

[19] C. Bresnahan y R. Blum, *LPIC-1 Linux Professional Institute Certification Study Guide*, Sybex, 2019.

[20] G. D. Singh, *The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire*, 2nd ed., Packt Publishing, 2022.

[21] Universidad Alfonso X el Sabio, *Apuntes y material docente de la asignatura Administración de Sistemas del Grado en Ingeniería Informática*, s. f.

[22] Universidad Alfonso X el Sabio, *Documentación técnica y material docente relacionado con redes y administración de infraestructuras corporativas del Grado en Ingeniería Informática*, s. f.

[23] OpenAI, ChatGPT (GPT-5.5), OpenAI, 2025. Utilizado como herramienta de apoyo para la revisión lingüística, mejora de la redacción y corrección de estilo del documento; no empleado como fuente de contenido técnico.