ADMINISTRACION CONTROL ACCESOS

Seguridad básica

- Cuentas de usuarios
- Cuentas de grupos
- LINUX
  - Chmod, chgrp, …
- WINDOWS
  - Panel Usuarios

Seguridad Windows

- Bloqueos de cuenta
- Bitlocker
- Certificados e infraestructura de clave pública (PKI)
- Confianzas de dominio y bosque
- Autenticación Kerberos
- Autenticación heredada (NTLM)
- Permisos, control de acceso y auditoría
- Problemas de canales seguros
- Plantillas de seguridad
- Inicio de sesión con tarjeta inteligente

Security Identifiers (SID)

- El Identificador Relativo (RID) es parte del Identificador de Seguridad (SID) en los dominios de Microsoft Windows. Es la parte del SID que identifica a un principal de seguridad (un usuario, grupo o equipo) en relación con la autoridad que expidió el SID.

GUIAS DE SEGURIDAD

- https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/500-guias-de-entornos-windows.html

Controlador de dominio /LDAP

- Para comprender mejor qué son los controladores de dominio echemos un vistazo a la primera palabra, “dominio”. Un dominio se relaciona con una red que aloja varias computadoras y dispositivos.
- Piense en el dominio como un concentrador maestro al que están conectados todos los dispositivos y ese concentrador puede controlar cualquier dispositivo que sea parte de la red. Esto incluye cosas como:
  - Ordenadores
  - Laptops
  - Impresoras
  - Cámaras de seguridad
  - Servidores
  - Y otros dispositivos
- Todos los componentes conectados están registrados en una base de datos central ubicada en el controlador de dominio.

Controlador de dominio / AD

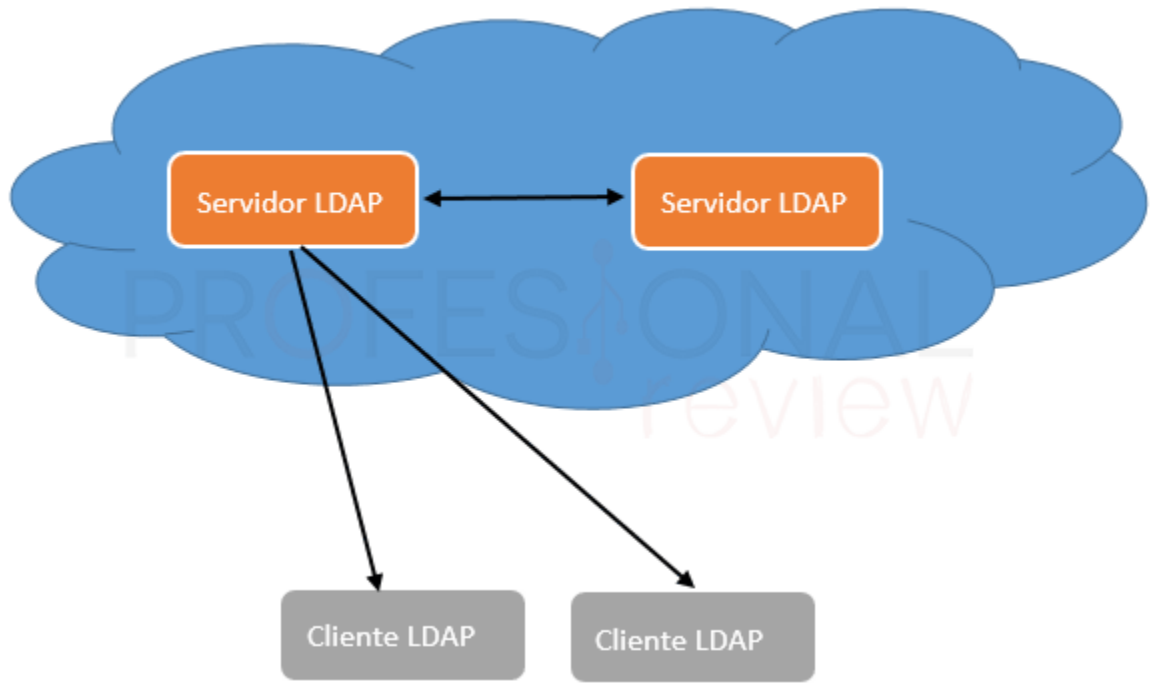
- Cuando vea el término “controlador de dominio”, también verá un término asociado, “Active Directory (AD)”, que es un servicio de directorio de Microsoft para sus redes de dominio de Windows.

- Un servidor que ejecuta los Servicios de dominio de Active Directory se conoce como controlador de dominio.

Controlador de dominio /LDAP

- El protocolo LDAP es muy utilizado actualmente por empresa que apuestan por el software libre al utilizar distribuciones de Linux para ejercer las funciones propias de un directorio activo en el que se gestionarán las credenciales y permisos de los trabajadores y estaciones de trabajo en redes LAN corporativas en conexiones cliente/servidor.

- LDAP son las siglas de Protocolo Ligero de Acceso a Directorio, o en inglés Lightweight Directory Access Protocol). Se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.
- Un directorio remoto es un conjunto de objetos que están organizados de forma jerárquica, tales como nombre claves direcciones, etc. Estos objetos estarán disponibles por una serie de cliente conectados mediante una red, normalmente interna o LAN, y proporcionarán las identidades y permisos para esos usuarios que los utilicen.
- LDAP está basado en el protocolo X.500 para compartir directorios, y contiene esta información de forma jerarquizada y mediante categorías para proporcionarnos una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores. Es, por así decirlo, una guía telefónica, pero con más atributos y credenciales.


Servidor LDAP
Servidor LDAP
Cliente LDAP
Cliente LDAP

Como se almacena la información

- Entradas, llamadas objetos en Active Directory. Estas entradas son colecciones de atributos con un Nombre Distinguido (DN) Este nombre se utiliza para dar un identificador único e irrepetible a una entrada del directorio. Una entrada puede ser el nombre de una organización y de ella colgarán unos atributos. También una persona puede ser una entrada.

- Atributos: los cuales poseen un tipo identificador y los correspondientes valores. Los tipos se utilizan para identificar los nombres de atributos, por ejemplo “mail”, “name”, “jpegPhoto”, etc. Algunos de los atributos que pertenecen a una entrada debe ser obligatorios y otros opcionales.

- LDIF: el Formato de Intercambio de Datos de LDAP es la representación en texto ASCII de las entradas LDAP. Este debe ser el formato de los archivos que se utilicen para importar información a un directorio LDAP. Cuando se escriba una línea en blanco, significará el final de una entrada.

- dn: cn=Jose Castillo,dc=profesionalreview,dc=com
- cn: Jose Castillo
- givenName: Jose
- sn: Castillo
- telephoneNumber: +34 666 666 666
- mail: usuario@profesionalreview.com
- objectClass: inetOrgPerson
- objectClass: organizationalPerson
- objectClass: person
- objectClass: top

Estructura de una URL de acceso en LDAP

- Al efectuar conexiones remotas a un servidor LDAP, necesitaremos del uso de direcciones URL para obtener información de éste. La estructura básica
- **ldap://servidor:puerto/DN?atributos?ambito?filtros?extensiones**
- servidor o host: es la dirección IP o nombre de dominio del servidor LDAP
- puerto: el puerto de conexión del servidor, por defecto será el 389
- DN: nombre distinguido para usar en la búsqueda
- Atributos: es una lista de campos a devolver separados por comas
- Ámbito o scope: es el ámbito de la búsqueda
- Filtros: para filtra la búsqueda según el identificador del objeto, por ejemplo.
- Extensiones: serán las cadenas de caracteres extensiones de la URL en LDAP.

Herramientas

- OpenLDAP: es la implementación libre del protocolo LDAP. Tiene su propia licencia y es compatible con otros servidores que utilicen el mismo protocolo. Es utilizado por distintas distribuciones Linux y BSD.
- Active Directory: es un almacén de datos de directorio con licencia Microsoft e implementado en sus sistemas operativos server desde Windows 2000. Realmente bajo la estructura de Active Directory se encuentra un esquema LDAPv3, por lo que también es compatible con otros sistemas que implemente este protocolo en sus directorios.
- Red Hat Directory Server: es un servidor que también se basa en LDAP similar a Active Directory, pero mediante una herramienta de código abierto. Dentro de este directorio podremos almacenar objetos como usuarios claves, grupos, políticas de permisos, etc.
- Apache Directory Server: otra de las grandes implementaciones que utilizan LDAP es el directorio con licencia de Apache Software. Además, implementa otros protocolos como Kerberos y NTP y cuenta con una interfaz de vistas propias de las bases de datos relacionales.
- Novell Directory Services: este es el servidor de directorio propio de Novell para gestionar el acceso a un almacén de recursos en uno o varios servidores conectados en red. Se compone de una estructura de base de datos jerárquica orientada a objetos en la que se almacenan todos los objetivos típicos de los directorios.
- Open DS: terminamos esta lista con el directorio basado en java de SUN Microsystems, que posteriormente se liberaría para todos los usuarios. Por supuesto, está desarrollado en JAVA el necesitaremos el paquete Java Runtime Environmet para que éste funcione.

Beneficios

- Dar acceso solo a aquellos que lo necesitan
- Evite las infracciones de datos de “error del operador”
- La gestión centralizada reduce los costos
- Recursos informáticos compartidos
- Administre fácilmente las impresoras de red
- Cerrar el acceso no autorizado

controles de seguridad a los que tiene acceso mediante el uso de un controlador de dominio:

- Bloquee las cuentas de usuario con demasiados intentos fallidos de inicio de sesión.
- Inhabilite las cuentas de usuario inmediatamente cuando un empleado abandone su empresa.
- Configure automáticamente todas las computadoras para bloquear la pantalla después de un período de inactividad establecido.
- Requerir contraseñas de inicio de sesión para pantallas bloqueadas.
- Restrinja el acceso USB (unidad flash) por permisos de usuario.

Instalar LDAP o Domain COntrollr

Single Sign On

- Es un servicio de autenticación de usuario y sesión que permite a un individuo tener acceso a una o varias aplicaciones. El nombre y la contraseña es el tipo de SSO más común y facilita la administración de varios nombres de usuario y contraseñas

- El SSO funciona sobre una la relación de confianza establecida entre una aplicación, conocida como proveedor de servicios, y un proveedor de identidad. A menudo, la confianza se basa en un certificado que se intercambia entre ambos proveedores y puede usarse para firmar información de identidad y confirmar que las fuentes son de fiar.

- Bajo este método, los datos de identidad toman la forma de tokens que contienen bits de información de identificación sobre el usuario, por ejemplo: correo electrónico o nombre de usuario.

- El SSO hace posible que las funciones transfieran la responsabilidad de autenticar a los usuarios a alguna otra aplicación o servicio. Este tipo de autenticación seguro la has visto en algunas aplicaciones de bancarias al momento de confirmar una transacción.

- Una aplicación, sitio web o un cliente con correo electrónico es un proveedor de servicios. La mayoría de plataformas de esta índole incluyen su propia funcionalidad para autenticar usuarios; con SSO esa responsabilidad se entrega a un proveedor de identidad. Así cuando el usuario intenta acceder al proveedor de servicios, este consulta con el proveedor de identidad para asegurarse de que el usuario ha demostrado ser quien afirma ser. Algunos parámetros para asegurar la identidad de un usuario pueden ser la autenticación de dos factores (2FA) o biometría.

Tipos de SSO

- SAML 2.0
- OAuth2
- CAS
- Shibboleth
- Tarjeta inteligente
- SSO personalizado

herramientas de SSO

- Duo + Cisco
- Keeper
- LastPass
- Rippling
- Okta

Herramientas de Autentiación SSO: Kerberos

- Kerberos es un protocolo de autenticación que permite a los sistemas y usuarios probar su identidad a través de un tercero de confianza.
- No es de autorización. Esto quiere decir que el protocolo se encarga de identificar a cada usuario, a través de una contraseña solo conocida por este, pero no determina a qué recursos o servicios puede acceder o no dicho usuario.
- El protocolo se desarrolló inicialmente en el Instituto de Tecnología de Massachusetts (MIT) como parte de un proyecto más grande llamado Proyecto Athena. El Proyecto Athena fue una iniciativa conjunta del MIT, Digital Equipment Corporation e IBM para construir un entorno informático distribuido para uso educativo.

- https://ciberseguridad.com/guias/prevencion-proteccion/kerberos/

- 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.

- El protocolo se centra en las entradas. Los tickets son emitidos por un tercero de confianza y utilizan cifrado simétrico (la clave que solo conoce el tercero de confianza) para establecer su confianza. Como explicaremos más adelante, ciertas contraseñas de usuario también se utilizan para cifrar y firmar tickets específicos. Sin embargo, la raíz de la seguridad del protocolo es la clave utilizada por el tercero de confianza.

- La implementación de Kerberos que se encuentra en Microsoft Active Directory se basa en el Servicio de autenticación de red Kerberos (V5), que se detalla en RFC 4120. Microsoft amplió la especificación del protocolo base agregando una serie de extensiones al protocolo (MS-KILE) para implementar comportamientos y características específicas de Active Directory y el sistema operativo Windows.

¿cómo funciona?

- Kerberos utiliza criptografía de clave simétrica y un centro de distribución de claves (KDC) para autenticar y verificar las identidades de los usuarios. Un KDC involucra tres aspectos:
- Un servidor de concesión de tickets (TGS) que conecta al usuario con el servidor de servicios (SS).
- Una base de datos Kerberos que almacena la contraseña y la identificación de todos los usuarios verificados.
- Un servidor de autenticación (AS) que realiza la autenticación inicial.
- Durante la autenticación, Kerberos almacena el ticket específico para cada sesión en el dispositivo del usuario final. En lugar de una contraseña, un servicio compatible con Kerberos busca este ticket. La autenticación Kerberos tiene lugar en un ámbito Kerberos, un entorno en el que un KDC está autorizado para autenticar un servicio, host o usuario.

Elementos que forman parte de Kerberos

- **Capa de transporte**
- Kerberos utiliza UDP o TCP como protocolos de transporte, que transmiten la información en claro, por lo cual es necesario que se encargue él mismo de proporcionar la capa de cifrado.
- El protocolo Kerberos utiliza los puertos UDP/88 y TCP/88, que se deben encontrar a la escucha en el KDC

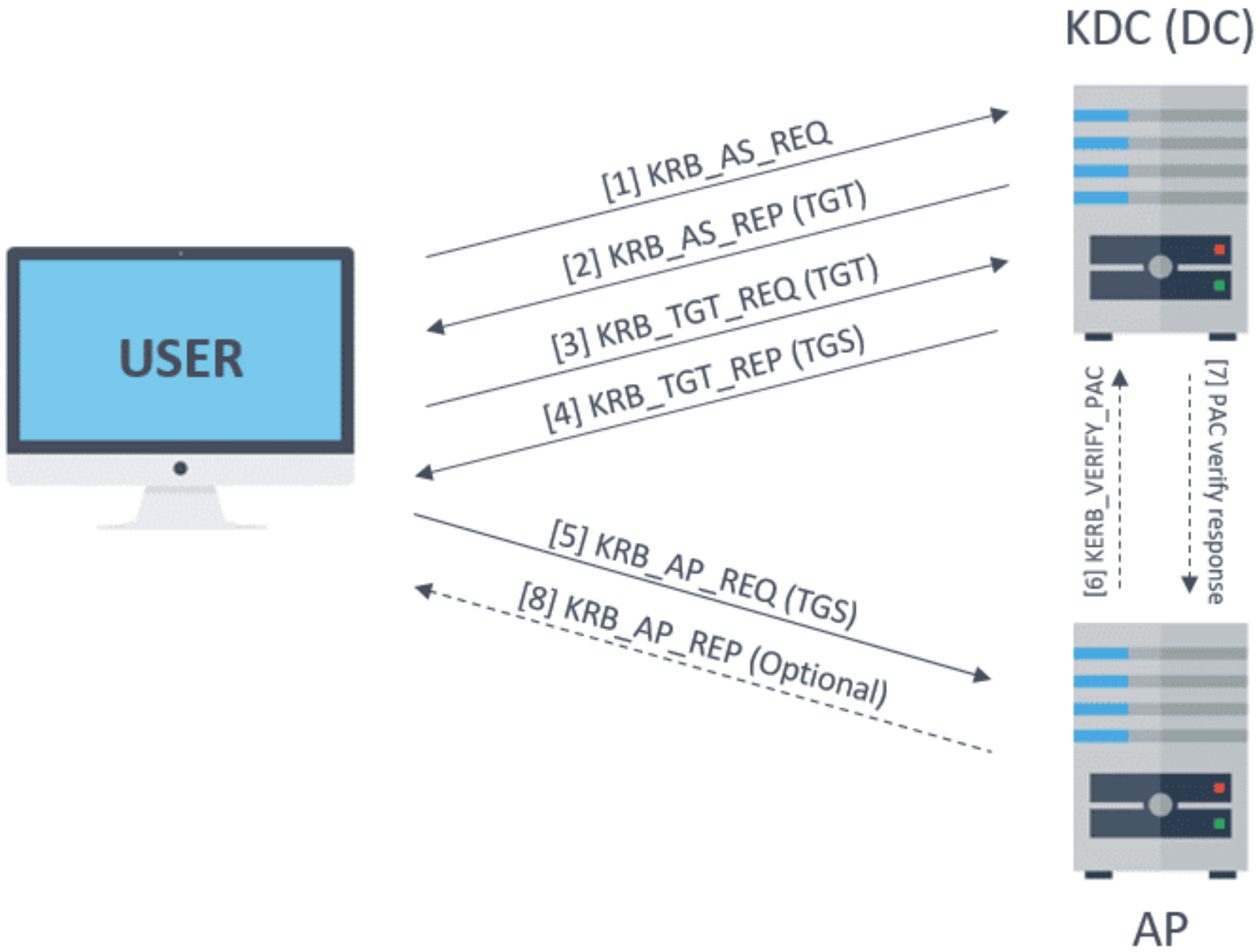
- **Agentes**
- En Kerberos intervienen varios servicios encargados de realizar la autenticación del usuario. Entre estos se encuentran los siguientes:
- El **cliente o usuario** que quiere acceder al servicio.
- El **AP** (Application Server) donde se expone el servicio al que el usuario quiere acceder.
- El **KDC** (Key Distribution Center), el servicio de Kerberos encargado de distribuir los tickets a los clientes, instalado en el DC (Controlador de dominio). Cuenta con el **AS** (Authentication Service), que se encarga de expedir los TGTs.

- **Claves de cifrado**
- Varias estructuras manejadas por Kerberos, como los tickets, se transmiten cifradas o firmadas. Esto evita que sean manipuladas por terceros. Las claves de cifrado utilizados por Kerberos, en Active Directory, son las siguientes:
- **Clave del KDC o krbtgt**: clave derivada del hash NTLM de la cuenta krbtgt.
- **Clave de usuario**: clave derivada del hash NTLM del propio usuario.
- **Clave de servicio**: clave derivada del hash NTLM del propietario del servicio, que puede ser una cuenta de usuario o del servidor.
- **Clave de sesión**: clave negociada por el cliente y el KDC.
- **Clave de sesión de servicio**: clave negociada para utilizar entre el cliente y el AP.

- **Tickets**
- Kerberos maneja unas estructuras llamadas “Tickets”, que son entregados a los usuarios autenticados para que estos puedan realizar ciertas acciones dentro del dominio de Kerberos. Se distinguen 2 tipos:
- El **TGS** (Ticket Granting Service) es el ticket que se presenta ante un servicio para poder acceder a sus recursos. Se cifra con la clave del servicio correspondiente.
- El **TGT** (Ticket Granting Ticket) es el ticket que se presenta ante el KDC para obtener los TGS. Se cifra con la clave del KDC.

- **PAC**
- El **PAC** (Privilege Attribute Certificate) es una estructura incluida en la mayoría los tickets. Esta estructura contiene los privilegios del usuario y está firmada con la clave del KDC.
- Es posible para los servicios verificar el PAC comunicándose con el KDC, aunque esto no es común. No obstante, la verificación del PAC solo consiste en comprobar su firma, sin comprobar si los privilegios son correctos.
- Por otra parte, un cliente puede evitar que se incluya el PAC especificándolo en el campo KERB-PA-PAC-REQUEST de la petición del ticket.

- **Mensajes**
- El protocolo Kerberos permite la comunicación de los diferentes agentes a través de diferentes tipos de mensajes. los más interesantes son :
- **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**: Utilizado por el usuario para solicitar el TGS al KDC, utilizando el TGT.
- **KRB_TGS_REP**: Respuesta del KDC para enviar el TGS solicitado al usuario.
- **KRB_AP_REQ**: Utilizado por el usuario para identificarse contra el servicio deseado, utilizando el TGS del propio servicio.
- **KRB_AP_REP**: (Opcional) Utilizado por el servicio para autenticarse frente al usuario.
- **KRB_ERROR**: Utilizado por los diferentes agentes para notificar situaciones de error.


KDC (DC)
USER
[1] KRB_AS_REQ
[2] KRB_AS_REP (TGT)
[3] KRB_TGT_REQ (TGT)
[4] KRB_TGT_REP (TGS)
[5] KRB_AP_REQ (TGS)
[8] KRB_AP_REP (Optional)
[6] KERB_VERIFY_PAC
[7] PAC verify response
AP

- La autenticación Kerberos es un proceso de varios pasos que consta de los siguientes componentes:
- El cliente que inicia la necesidad de una solicitud de servicio en nombre del usuario.
- El servidor, que aloja el servicio al que el usuario necesita acceder.
- El AS, que realiza la autenticación del cliente. Si la autenticación es exitosa, se emite al cliente un vale de otorgamiento de boletos (TGT) o un token de autenticación de usuario, que es prueba de que el cliente ha sido autenticado.
- El KDC y sus tres componentes: el AS, el TGS y la base de datos Kerberos.
- La aplicación TGS que emite tickets de servicio.

Ataques de Kerberos

- **Overpass The Hash/Pass The Key (PTK)**
- La definición general del ataque Pass The Hash (PTH) es la de ataque que utiliza el hash del usuario para conseguir suplantar al mismo. Llevado al campo de los tickets Kerberos se denomina Overpass The Hash o Pass The Key.
- Si un atacante consigue obtener el hash de un usuario podría suplantar a este frente al KDC, y acceder a los servicios del dominio disponibles para dicho usuario.
- Los hashes de usuario se pueden extraer de los ficheros SAM de las estaciones de trabajo, del fichero NTDS.DIT de los DC, o de la memoria del proceso lsass (utilizando la herramienta Mimikatz) donde también es posible obtener las contraseñas en texto claro.

- **Pass The Ticket (PTT)**
- El Pass The Ticket se trata de obtener un ticket de usuario y utilizarlo para ganar acceso a los recursos para los que el usuario tenga permisos. Sin embargo, además del ticket, es necesario conseguir también la clave de sesión respectiva, para poder usar este en las comunicaciones con el servicio.
- Se pueden obtener los tickets mediante un ataque de Man-In-The-Middle, ya que estos viajan sobre UDP o TCP. No obstante, mediante este técnica no se consigue acceso a la clave de sesión.
- El otro método, ampliamente utilizado, es extraer dichos tickets de la memoria del proceso lsass, donde también se pueden encontrar las claves de sesión. Este procedimiento se puede realizar con la herramienta Mimikatz.
- Es preferible obtener un TGT, debido a que el TGS cuenta con la limitación de que solamente se puede utilizar contra un servicio, pero ambos pueden ser utilizados para este tipo de ataque.
- Se debe tener en cuenta que el tiempo por defecto de vida de los tickets es de 10 horas, tras lo cual no podrán ser utilizados.

- **Golden Ticket y Silver Ticket**
- El objetivo del ataque del Golden Ticket es construir un TGT, para lo cual se necesita la clave del krbtgt. Por tanto si se obtiene el hash NTLM de la cuenta krbtgt, es posible construir un TGT. Dicho TGT puede contar con la caducidad y permisos que se desee, consiguiendo incluso privilegios de administrador de dominio.
- El ticket continuará siendo válido aunque el usuario incluido cambie su contraseña. El TGT solo podrá ser invalidado si expira o cambia la contraseña de la cuenta krbtgt.
- El Silver Ticket es similar, pero esta vez se construye un TGS y lo que se requiere es la clave del servicio al que se quiere acceder. Esta clave se deriva del hash NTLM de la cuenta propietaria del servicio. Esta técnica no funcionará si el servicio verifica el PAC, ya que al no conocer la clave de krbtgt, no es posible firmarlo correctamente.

- **Kerberoasting**
- El Kerberoasting trata de usar los TGS para realizar cracking de las contraseñas de los usuarios offline.
- Como se ha visto anteriormente, los TGS vienen cifrados con la clave del servicio, que se deriva del hash NTLM de la cuenta propietaria del servicio. Normalmente los servicios son propiedad de las cuentas de ordenador en que se ejecutan. No obstante, estas contraseñas son demasiado complejas como para ser crackeadas. Esto también aplica a la cuenta krbtgt, haciendo que tampoco se pueda crackear el TGT.
- Pese a todo, en algunas ocasiones los propietarios de los servicios son cuentas de usuario normal. En estos casos es más factible crackear las contraseñas. Además, este tipo de cuentas suelen ser privilegiadas. Se debe tener en cuenta que con cualquier usuario de dominio es posible obtener un TGS para cualquier servicio, debido a que Kerberos no se encarga de la autorización.

- **ASREPRoast**
- El ASREPRoast es una técnica similar al Kerberoasting, que también busca el crackeo offline de las credenciales.
- Cuando un usuario está configurado con el atributo *DONT_REQ_PREAUTH*, no necesita preautenticación, con lo que es posible construir un mensaje *KRB_AS_REQ* sin conocer las credenciales del mismo.
- Una vez construido y enviado, el KDC responderá con un mensaje *KRB_AS_REP* que contiene datos cifrados con el hash de este usuario, pudiendo ser utilizados para el crackeo offline.

TECNICAS MITIGAR

- Vigilar eventos:
- 4624: Inicio de sesión de cuenta
- 4672: Inicio de sesión de administrador
- alertar sobre los 4769 para usuarios sensibles como la cuenta de administrador de dominio predeterminada
- Desde Powershell
- Get-WinEvent -FilterHashtable @{Logname='Security';ID=4672} -MaxEvents 1 | Format-List –Property

- ALGUNA REFERENCIA DE ATAQUES:

- https://pentestlab.blog/2018/04/09/golden-ticket/

- https://book.hacktricks.xyz/v/es/windows-hardening/active-directory-methodology/golden-ticket