DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.6**	**Actividad**	Investigación LDAP y Kerberos				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	30/04/2021
Compet. Genéricas	4.1, 4.5, 5.2,			Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

- Identificar los protocolos de autenticación, LDAP (Lightweight Directory Access Protocol) y KERBEROS.

2. Introducción

Los controles de acceso mediante los protocolos LDAP-KERBEROS, permiten verificar la autenticación de la comunicación de dos servidores en una red insegura y demostrar su identidad mutuamente de manera segura.

3. Instrucciones (Descripción) de la actividad

1. Investigar la definición de los protocolos LDAP y Kerberos, así como de la importancia de su utilización. (al menos una cuartilla por cada protocolo)
2. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.
3. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

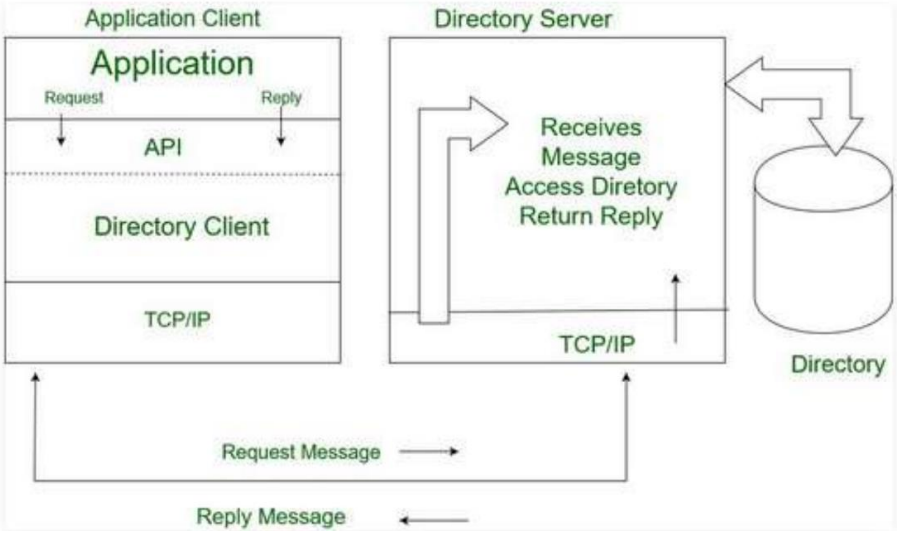
4. Desarrollo

LDAP

LDAP son las siglas de Lightweight Directory Access Protocol. Es un protocolo de aplicación estándar de la industria y neutral para el proveedor que se utiliza para acceder y administrar servicios de información de directorio y proporciona un medio para administrar la membresía de usuarios y grupos almacenados en Active Directory. Fue desarrollado por Tim Howes, Steve Kille y Wengyik Yeong en 1993. Originalmente, LDAP era solo un protocolo de red utilizado para obtener datos de un directorio X.500 (una serie de estándares de redes informáticas que cubren los servicios de directorio electrónico).

El Protocolo ligero de acceso a directorios (LDAP) es un protocolo de Internet que funciona en TCP / IP y se utiliza para acceder a la información de los directorios. El protocolo LDAP se utiliza básicamente para acceder a un directorio activo.

Directorios: Los directorios son un conjunto de objetos con atributos similares, organizados de forma lógica y jerárquica. Por ejemplo, directorios telefónicos. Es una aplicación de base de datos distribuida que se utiliza para administrar atributos en un directorio.



Algunas de sus **características** más importantes son:

- ❖ Código abierto: OpenLDAP es una implementación de código abierto del Protocolo ligero de acceso a directorios, lo que significa que se puede descargar libremente.
- ❖ Admite TLS: dado que LDAP es compatible con la seguridad de la capa de transporte, los datos confidenciales se pueden proteger.
- ❖ Flexibilidad: LDAP admite una amplia gama de bases de datos para almacenar directorios, lo que permite a sus usuarios elegir la base de datos de acuerdo con el tipo de información que el servidor necesita para circular.
- ❖ Popular: debido a la API de cliente bien definida, la cantidad de aplicaciones habilitadas para LDAP está aumentando.
- ❖ El modelo funcional de LDAP es más simple debido a que omite la característica duplicada, rara vez utilizada y esotérica.
- ❖ Es más fácil de entender e implementar.
- ❖ Utiliza cadenas para representar datos

Algunas de sus **ventajas** con respecto a otros protocolos de administración de directorios son:

- ✓ Tiene implementación en código abierto que lo hace gratuito y de fácil acceso.
- ✓ Es liviano considerando otros protocolos modernos.

- ✓ Incluye fuertes mecanismos de codificación y restricciones y varios tipos de autenticación a través de SASL (autenticación simple y capa de seguridad), lo que lo hace altamente seguro.
- ✓ Tiene un amplio apoyo de la industria.
- ✓ Es utilizado por muchos servicios como DNS.
- ✓ Los datos presentes en LDAP están disponibles para muchos clientes y bibliotecas.
- ✓ DAP admite muchos tipos de aplicaciones.
- ✓ LDAP es muy general y tiene seguridad básica.

Su **desventaja principal** es que tiene problemas con el manejo de bases de datos relacionados, por lo que es complicado realizar implementaciones con gestores de esta arquitectura de bases de datos.

Entre las **funciones principales** de este protocolo se rescatan:

- ❖ Limitan el tráfico de la red para aumentar su rendimiento. En una entidad, por ejemplo, si su política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que lo bloqueen, lo que reduce considerablemente la carga de la red y aumenta su rendimiento.
- ❖ Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro lo haga a esa misma área.
- ❖ Filtran el tráfico según su tipo. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de redes sociales.
- ❖ Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos.

Las **operaciones principales** que permite configurar las entradas de directorio son:

- ❖ Búsqueda de criterios especificados por el usuario
- ❖ Agregar una entrada
- ❖ Eliminar una entrada
- ❖ Modificar una entrada
- ❖ Modificar el nombre distinguido o el nombre distinguido relativo de una entrada
- ❖ Comparando una entrada

Es posible dar un avistamiento más meticuloso al funcionamiento de LDAP si nos enfocamos en los modelos en los que se encuentra basado:

1. **Modelo de información**

Este modelo describe la estructura de la información almacenada en un directorio LDAP. En este modelo, la información básica que se almacena en un directorio se denomina entidad. Las entradas aquí representan un objeto de interés en el mundo real, como personas, servidor, organización, etc. Las entradas contienen una colección de atributos que contienen información sobre el objeto. Cada atributo tiene un tipo y uno o más valores.

Aquí, los tipos de atributo están asociados con la sintaxis y la sintaxis especifica qué tipo de valores se pueden almacenar.

2. **Modelo de nomenclatura**

Este modelo describe cómo se organiza e identifica la información en un directorio LDAP. En este, las entradas están organizadas en una estructura en forma de árbol llamada Árbol de información de directorio (DIT). Las entradas se organizan dentro de DIT según su nombre distinguido DN. DN es un nombre único que identifica inequívocamente una sola entrada.

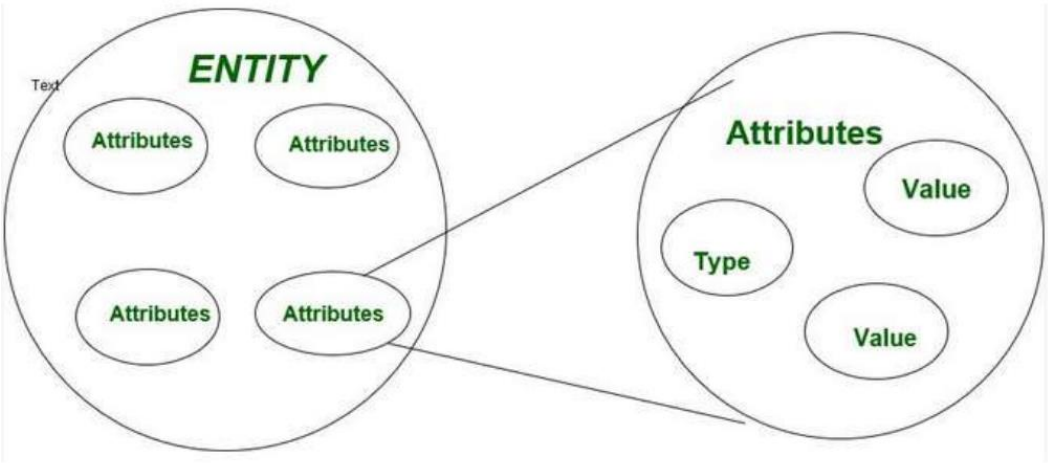
3. **Modelo funcional**

LDAP define operaciones para acceder y modificar entradas de directorio. En esto discutimos acerca de las operaciones LDAP de una manera independiente del lenguaje de programación Las operaciones LDAP se pueden dividir en las siguientes categorías: Consulta, Actualizar y Autenticación

4. **Modelo de seguridad**

Este modelo describe cómo se puede proteger la información en el directorio LDAP del acceso no autorizado. Se basa en la operación BIND. Se pueden realizar varias operaciones de vinculación.

La interacción entre el cliente y servidor LDAP implementa las funciones y operaciones principales de LDAP de acuerdo con lo mostrado en el siguiente esquema:



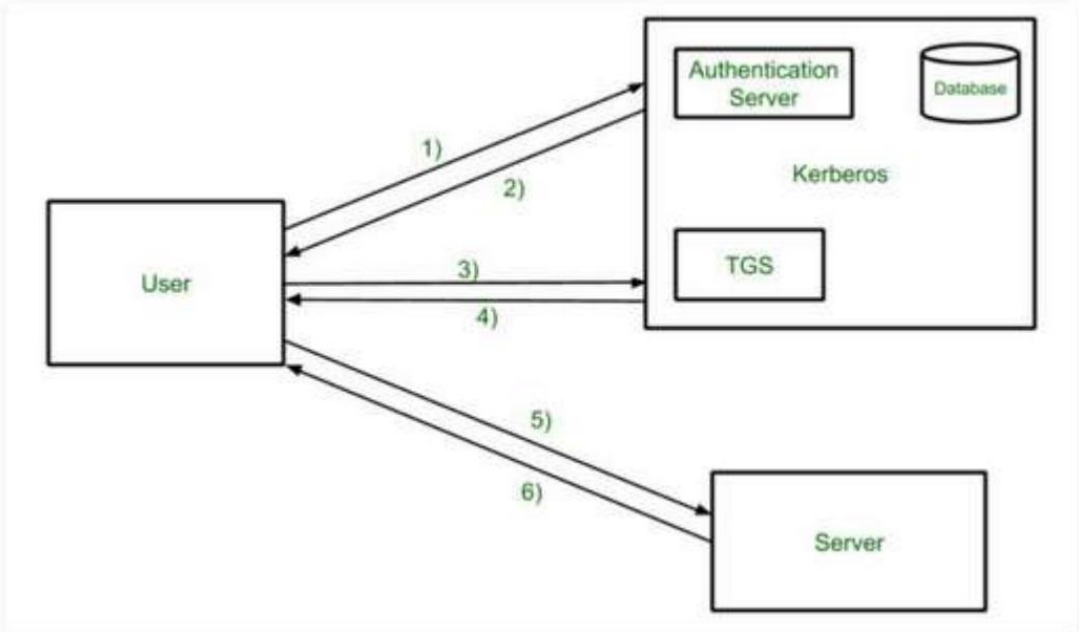
Kerberos

Kerberos proporciona un servidor de autenticación centralizado cuya función es autenticar a los usuarios en los servidores y los servidores a los usuarios. En la autenticación Kerberos, el servidor y la base de datos se utilizan para la autenticación del cliente. Kerberos se ejecuta como un servidor de confianza de terceros conocido como Centro de distribución de claves (KDC). Cada usuario y servicio de la red es un principal.

Los principales **componentes** de Kerberos son:

- **Servidor de autenticación** (AS): El servidor de autenticación realiza la autenticación inicial y el ticket para el servicio de concesión de tickets.
- **Base de datos**: El servidor de autenticación verifica los derechos de acceso de los usuarios en la base de datos.
- **Servidor de concesión de tickets** (TGS): El servidor de concesión de tickets emite el ticket para el servidor

Podemos resumir el funcionamiento de acuerdo con el siguiente esquema:



1. Inicio de sesión de usuario y servicios de solicitud en el host. Por lo tanto, el usuario solicita el servicio de concesión de tickets.
2. La autenticación del servidor verifica el derecho de acceso del usuario mediante la base de datos y luego proporciona la clave de sesión y de concesión de tickets. Los resultados se cifran con la contraseña del usuario.
3. El descifrado del mensaje se realiza con la contraseña y luego se envía el ticket al Ticket Granting Server. El Ticket contiene autenticadores como el nombre de usuario y la dirección de red.
4. El servidor de concesión de tickets descifra el ticket enviado por el usuario y el autenticador verifica la solicitud y luego crea el ticket para solicitar servicios del servidor.
5. El usuario envía el ticket y el autenticador al servidor.
6. El servidor verifica el Ticket y los autenticadores generan el acceso al servicio. Después de este Usuario puede acceder a los servicios.

LDAP vs Kerberos

Podemos establecer las diferencias entre LDAP y Kerberos mediante un estudio detallado de las características de cada uno de ellos. Por un lado, sabemos que LDAP ofrece un protocolo de código abierto con una arquitectura flexible, opera sobre TCP / IP y SSL directamente, es automático y proporciona un amplio soporte en todas las industrias; mientras que Kerberos previene varios ataques de intrusión, proporciona autenticación a través de Internet para aplicaciones web, ofrece una confianza única en la raíz y elimina los escenarios de malla completa, así como permitir la interoperabilidad con otros dominios de acceso.

Siendo más específicos, podemos establecer el siguiente cuadro comparativo entre ambos protocolos:

LDAP	Kerberos
Es la abreviatura de Protocolo ligero de acceso a directorios.	No significa algo en concreto
LDAP se utiliza para autorizar los detalles de las cuentas cuando se accede a ellas.	Kerberos se utiliza para administrar credenciales de forma segura.
No es un código abierto, pero tiene una implementación como Open LDAP que son de código abierto.	Es un software de código abierto que proporciona servicios gratuitos.
Es compatible con la autenticación de dos factores con el protocolo RADIUS.	Es compatible con la autenticación de dos factores.
LDAP agrega autenticación en dos opciones SASL o autenticación anónima.	Kerberos agrega alta seguridad y brinda autenticación mutua.
Proporciona autenticación en aplicaciones de varios niveles.	Proporciona autenticación en aplicaciones de varios niveles.

5. Conclusiones

Es interesante observar las diferentes características que nos proveen cada uno de estos protocolos de directorios dentro de una red. En particular, considero que LDAP ofrece una serie de herramientas más llamativas para empresas de gran volumen al tener una conectividad simple con los servicios de AD que proveen algunos sistemas y plataformas como Microsoft Azure; mientras que Kerberos sería la opción ganadora en implementaciones más pequeñas y experimentales ofreciendo un nivel de administración casi tan bueno como el de LDAP de manera gratuita.

6. Referencias

Ernesto. A. (31/10/2019). Lightweight Directory Access Protocol (LDAP) Recuperado el 27/04/2021 de: https://www.geeksforgeeks.org/lightweight-directory-access-protocolldap/

(17/09/2020). Kerberos. Recuperado el 27/04/2021 de: https://www.geeksforgeeks.org/kerberos/