TECNOLÓGIC NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

PRACTICA 2 Investigación

PRESENTA:

Rael Gabriel Bautista

Sandra Gabriela Velasco Guzmán

Amilkar Vladimir Reyes Reyes

Arnol Jesus Cruz Ortiz

ASESOR:

EDWARD OSORIO SALINAS

CARRERA:

INGENIERA EN SISTEMAS COMPUTACIONALES

SEMESTRE:7US

Tlaxiaco, Oax.10 de septiembre de 2024.

"Educación, ciencia y tecnología, progreso día con día" ®

INDICE

LDAP

permite a las organizaciones almacenar, administrar y proteger información sobre la organización, sus usuarios y activos.

¿Qué es LDAP?

LDAP es un protocolo abierto que facilita el acceso y la autenticación de información almacenada en servicios de directorio.

Se utiliza tanto en redes públicas como privadas, lo que lo hace versátil para obtener datos como nombres de usuario, contraseñas y otros recursos de red.

Active Directory (AD), desarrollado por Microsoft, utiliza LDAP para gestionar y autenticar usuarios y recursos en redes de Windows, pero LDAP también es compatible con otras plataformas (Linux, Unix, etc.).

SSO (Single Sign-On) es una de las funcionalidades que LDAP habilita, permitiendo que los usuarios accedan a múltiples sistemas con una única autenticación.

¿Cómo funciona?

Proceso de conexión en LDAP:

1. **Conexión inicial**: El cliente se conecta al **Directory System Agent (DSA)** a través del puerto TCP/IP 389 para iniciar una sesión LDAP.
2. **Establecimiento de conexión**: Se establece una conexión entre el cliente y el servidor.
3. **Intercambio de datos**: Los datos se intercambian entre el cliente y el servidor, dependiendo de la operación que se solicite.

Estructura del DSA:

- El **Directory System Agent** organiza la información en una estructura **jerárquica**, con objetos que pueden ser contenedores para otros objetos.

- Cada elemento en esta jerarquía tiene un **Nombre Distinguido (DN)**, que actúa como una ruta completa hacia el objeto en la estructura.
- El **Nombre Distinguido Relativo (RDN)** clasifica los elementos dentro de la jerarquía de forma más precisa.

Operaciones básicas en LDAP:

Agregar: Permite añadir nuevas entradas al servidor de directorio. Si una entrada con el mismo nombre ya existe, se rechaza con un mensaje de error.

Enlazar (Autenticación): Valida el estado de autenticación de una sesión. Se pueden usar métodos de autenticación **Simple** o **SASL**.

Desenlazar: Finaliza las conexiones y libera los recursos que se podrían haber asignado a operaciones abortadas.

Modificar: Permite modificar las entradas existentes. Las modificaciones permitidas incluyen:

- Agregar un nuevo valor.
- Reemplazar un valor existente.
- Eliminar un valor.

Buscar y comparar: Se puede buscar información según atributos específicos como nombre, tamaño o tipo, y comparar entradas.

Borrar: Elimina una entrada del directorio. La solicitud debe ser precisa y cumplir con los requisitos establecidos, como proporcionar el nombre correcto de la entrada a borrar y los controles de solicitud adjuntos.

¿Usos y riesgos de seguridad?

Debido a que LDAP facilita las conexiones a recursos privados, existen riesgos de ciberseguridad asociados con este protocolo, siendo los más críticos las inyecciones de LDAP.

Una inyección LDAP es un tipo de ciberataque en el que se inyecta código a través de una aplicación web para acceder a información confidencial en un directorio LDAP.

El código inyectado contiene metacaracteres LDAP que modifican las solicitudes legítimas de los clientes LDAP para lograr objetivos maliciosos.

Una inyección LDAP podría resultar en una violación de datos, escalada de privilegios de usuario o secuestro de cuenta.

Las inyecciones de LDAP son posibles cuando los servidores no validan la legitimidad de las solicitudes de los clientes LDAP, lo que permite a los ciberatacantes comunicarse libremente con los servidores LDAP.

Cómo prevenir las inyecciones de LDAP**.**

Las inyecciones de LDAP se pueden mitigar con los siguientes controles de seguridad. Aplicar la validación de entrada del lado del servidor: todas las entradas deben validarse con una lista de caracteres y cadenas permitidos.

Escape de cadenas de entrada controladas por el usuario: esto convertirá las entradas maliciosas en valores de cadena y no en predicados LDAP. Implementar el principio de privilegios mínimos: al proteger la cuenta LDAP necesaria para vincular un directorio, las consultas LDAP no se ejecutarán sin autorización.

RADIUS:

(Remote Authentication Dial-In User Service) protocolo de autenticación, autorización y auditoría que se diseñó a partir de una necesidad concreta: controlar y garantizar el acceso a recursos de computación heterogéneos.

Características de RADIUS.

Los actuales servicios destinados a AAA (Authentication, Authorization & Accounting) tienen mucho que ver con RADIUS porque persiguen objetivos similares.

Propiedades

- Protocolo no orientado a conexión, que usa UDP y no emplea conexiones directas.
- El modelo de seguridad es punto-a-punto.
- Es stateless (no es consciente del estado de la conexión).
- Soporta mecanismos de autenticación PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol) mediante PPP.
- Usa MD5 para ocultar las credenciales transferidas.
- Proporciona unos 50 atributos/valores diferentes, con la opción de definir otros específicos de cada proveedor.
- Implementa el modelo autenticación-autorización-auditoría.

Formatos de paquete y puertos

Se emplea una estructura predecible de paquetes, basada en dos partes principales:

- **Cabecera/header**
  - Código
  - Identificador
  - Longitud
  - Autenticador

- **Carga/datos**
  - Atributos
  - Valores

Códigos

ID MENSAJE	DESCRIPCIÓN
1	*Access-Request*
2	*Access-Accept*
3	*Access-Reject*
4	Accounting-Request
5	Accounting-Response
11	*Access-Challenge*
12	Status-Server
13	Status-Client
255	Reservado

Tabla 1 Tipos de códigos RADIUS, en cursiva los utilizados en autenticación y autorización

Lo que has descrito es una estructura clave en el protocolo RADIUS (Remote Authentication Dial-In User Service), un protocolo utilizado para la autenticación, autorización y contabilización de usuarios que acceden a redes.

Identificador:

Este campo de un octeto se utiliza para identificar y mantener el orden correcto de los mensajes en la conversación entre cliente y servidor RADIUS, como solicitudes, respuestas o procesos de desafío-respuesta (challenge-response).

Los servidores pueden usar el Identificador junto con otros elementos, como direcciones IP, puertos UDP de origen y marcas temporales, para detectar y descartar mensajes duplicados.

Longitud:

Este campo de dos octetos indica la longitud total del mensaje RADIUS, incluyendo todos sus campos: código, identificador, longitud, autenticador y atributos.

La longitud mínima de un mensaje RADIUS es de 20 bytes, y el tamaño máximo es de 4096 bytes, según lo definido en los estándares RFC.

Autenticador:

El campo Autenticador tiene un tamaño fijo de 16 octetos y sirve para asegurar la integridad del mensaje y verificar la autenticidad del remitente.

Existen dos tipos de autenticadores:

1. **Request authenticator:** Se utiliza en mensajes de tipo Access-Request y Accounting-Request. Este valor se genera aleatoriamente para prevenir ataques como el de repetición (replay attack).

2. **Response authenticator**: Se utiliza en respuestas de tipo Access-Accept, Access-Reject y Access-Challenge. Se genera usando un hash MD5, calculado sobre el código, el identificador, la longitud, el request-authenticator y el secreto compartido (shared secret) del cliente y servidor RADIUS.

Estos campos son fundamentales para garantizar la seguridad y el correcto enrutamiento de los mensajes en el proceso de autenticación en RADIUS.

Ejemplo:

```
ResponseAuth =
MD5(Code+ID+Length+RequestAuth+Attributes+Secret)
```

TACACS+

¿Qué es TACACS+?

TACACS+ es un protocolo de autenticación, autorización y contabilidad (AAA) compatible con cualquier proveedor que le permite centralizar y controlar el acceso del administrador a enrutadores, conmutadores, cortafuegos, equilibradores de carga y puntos de acceso WiFi.

1. Configuración del servidor TACACS+: Se define la dirección IP del servidor, la contraseña secreta compartida y otras configuraciones como el puerto y el tiempo de espera.

2. Autenticación de usuarios: Los usuarios autenticados a través de TACACS+ se asignan a cuentas locales o plantillas en el dispositivo. Si no hay cuentas locales, se asigna la plantilla `remote` de manera predeterminada.

3. Opciones adicionales: Se pueden configurar varias características opcionales, como el uso de una instancia de administración para enrutar los paquetes TACACS+ y la actualización periódica del perfil de autorización del usuario.

4. Configuración de múltiples servidores: Es posible configurar el mismo servicio de autenticación para varios servidores, proporcionando redundancia y asegurando que, si un servidor falla, otro pueda manejar la autenticación.

5. Autorización personalizada: Junos OS permite definir atributos específicos del proveedor para otorgar permisos específicos a usuarios autenticados por TACACS+.

6. Verificación: Después de la configuración, se debe verificar que el servidor TACACS+ autentique a los usuarios correctamente mediante comandos de verificación.

KERBEROS

¿Qué es Keberos?

Kerberos es un protocolo de autenticación de red utilizado en sistemas informáticos no seguros, diseñado para verificar la identidad de los usuarios y servicios en una red mediante el uso de criptografía y un tercero confiable (KDC, Centro de Distribución de Claves). Desarrollado originalmente por el MIT en la década de los 80 para su proyecto Athena, es ampliamente utilizado hoy en día, especialmente en los sistemas de Microsoft Windows, además de estar disponible para otros sistemas operativos como UNIX, Linux y macOS.

Funcionamiento de Kerberos:

1. Cliente: Inicia la solicitud de autenticación.

2. Servidor de Autenticación (AS): Verifica al cliente y emite un Ticket-Granting Ticket (TGT) si la autenticación es exitosa.

3. Ticket-Granting Server (TGS): Emite tickets de servicio para acceder a recursos específicos.

4. Servidor de Host: El recurso o servicio al que el usuario quiere acceder.

El proceso general implica que el cliente solicita un ticket al AS, recibe un TGT, lo presenta al TGS, que luego emite un ticket de servicio. Este ticket se utiliza para acceder al recurso del servidor, garantizando que la comunicación sea segura y autenticada.

Ventajas de Kerberos**:**

- No se envían contraseñas en texto claro.
- Alta seguridad mediante criptografía y verificación de terceros.
- Soporte para autenticación mutua, lo que asegura que tanto el cliente como el servidor se autentican mutuamente.

Desventajas:

- Si el KDC falla, la red entera puede quedar inoperativa.
- Requiere sincronización precisa de las fechas y horas entre los servidores y clientes.
- Los sistemas más antiguos pueden no ser compatibles, y está sujeto a ataques de fuerza bruta y phishing.

ACL

¿Qué es ACL (Lista de Control de Acceso)?

Una Lista de Control de Acceso (ACL) es un mecanismo utilizado en redes para controlar el tráfico de datos mediante una serie de reglas. Estas reglas permiten o deniegan el paso de paquetes a través de una interfaz de red en función de ciertos criterios especificados en el encabezado del paquete. Las ACL son características esenciales en los sistemas IOS de Cisco y se utilizan ampliamente para gestionar y asegurar el tráfico en redes.

Tareas de las ACL:

1. Limitación de Tráfico: Las ACL pueden limitar el tráfico en la red para mejorar el rendimiento, por ejemplo, bloqueando ciertos tipos de tráfico no deseado, como video.

2. Control del Flujo de Tráfico: Pueden restringir la entrega de actualizaciones de routing para asegurar que provengan de fuentes conocidas.

3. Seguridad Básica: Permiten controlar el acceso a distintas partes de la red y restringir el acceso a servicios específicos.

4. Filtrado de Tráfico: Permiten o deniegan tipos de tráfico, como el correo electrónico o Telnet.

Filtrado de Paquetes

Las ACL utilizan listas secuenciales de instrucciones, conocidas como Entradas de Control de Acceso (ACE), que determinan si un paquete debe ser permitido o denegado. Estas instrucciones se aplican en el tráfico entrante o saliente a través de una interfaz de red.

ACL Estándar: Filtran el tráfico basado únicamente en la dirección IP de origen (Capa 3).

ACL Extendidas: Filtran el tráfico basándose en la dirección IP de origen y destino, así como en protocolos y puertos específicos (Capas 3 y 4).

Las ACL también incluyen una denegación implícita al final de la lista, que bloquea todo el tráfico que no coincide con ninguna de las ACE especificadas.

Funcionamiento de las ACL:

ACL de Entrada: Filtran paquetes antes de que se enruten a la interfaz de salida. Son útiles para reducir la carga de trabajo del enrutador al descartar paquetes no deseados antes del procesamiento de enrutamiento.

ACL de Salida: Filtran paquetes después de que se han enrulado a la interfaz de salida. Son ideales cuando se necesita aplicar el mismo filtro a múltiples interfaces de entrada antes de que los paquetes salgan.

RBAC

¿Qué es RBAC (El Control de Acceso Basado en Roles)?

El Control de Acceso Basado en Roles (RBAC) es un modelo de seguridad que gestiona los permisos de acceso a los sistemas informáticos en función de los roles que ocupan los usuarios dentro de una organización. En lugar de asignar permisos individuales a cada usuario, RBAC agrupa a los usuarios en roles y asigna permisos a estos roles, simplificando así la gestión y aumentando la seguridad.

Características del RBAC:

Asignación de Roles: Los permisos se asignan a roles específicos en lugar de a usuarios individuales. Cada usuario recibe uno o más roles basados en sus responsabilidades.

Roles y Permisos: Los roles definen un conjunto de permisos necesarios para realizar ciertas funciones. Los permisos pueden incluir acceso a archivos, aplicaciones, y recursos específicos.

Administración Centralizada: Los administradores asignan permisos a roles en lugar de a usuarios individuales, lo que reduce la complejidad y la posibilidad de errores.

Funcionamiento del RBAC:

Definición de Roles: Se definen roles que corresponden a las funciones dentro de la organización (e.g., Finanzas, Recursos Humanos).

Asignación de Permisos: Cada rol recibe un conjunto de permisos necesarios para las tareas que realiza.

Asignación de Roles a Usuarios: Los usuarios son asignados a roles basados en sus funciones dentro de la organización.

Gestión y Supervisión: Utilizando sistemas de gestión de acceso a la identidad (IAM), los administradores pueden supervisar y ajustar los permisos según sea necesario.

Ventajas del RBAC:

- **Flexibilidad:** Los cambios en roles o permisos se aplican automáticamente a todos los usuarios asignados a esos roles.
- **Menor Esfuerzo Administrativo:** Reduce la carga administrativa de gestionar permisos individuales.
- **Seguridad Mejorada:** Se asegura que los usuarios solo tienen los permisos necesarios para sus funciones, siguiendo el principio de menor privilegio.
- **Transparencia:** Los roles suelen tener nombres descriptivos, lo que facilita la comprensión de los permisos asignados.

Inconvenientes del RBAC:

- **Complejidad Inicial:** Definir roles y permisos puede ser laborioso, especialmente en organizaciones grandes.
- **Asignaciones Temporales:** Gestionar permisos temporales puede ser más complicado que hacerlo de forma individual.
- Escalabilidad: En organizaciones grandes, la creación de roles puede volverse compleja si no se gestiona adecuadamente.

Aplicación del RBAC:

RBAC es común en sistemas operativos como Microsoft Windows Server (a través del Directorio Activo), Linux (con SELinux), y Unix (Solaris). También es utilizado en sistemas empresariales para gestionar el acceso a aplicaciones y datos de forma eficiente y segura.

ABAC

¿Qué es ABAC (Control de Acceso Basado en Atributos)?

El Control de Acceso Basado en Atributos (ABAC) es un modelo de seguridad que otorga privilegios de acceso en función de los atributos asociados a los usuarios, recursos y el entorno. A diferencia del Control de Acceso Basado en Roles (RBAC), que asigna permisos según roles predefinidos, ABAC ofrece un control de acceso más granular y flexible.

Características de ABAC

Atributos Utilizados:

- **Atributos de Usuario:** Información sobre el usuario, como puesto de trabajo, nivel de antigüedad, y departamento.
- **Atributos de Recurso:** Información sobre el recurso, como el tipo de archivo, propietario, y nivel de sensibilidad.
- **Atributos del Entorno**: Condiciones externas como red, geolocalización, y hora del día.

Políticas de Acceso: Los administradores definen políticas que especifican qué combinación de atributos es necesaria para permitir o denegar el acceso a un recurso.

Evaluación Dinámica: Cuando un usuario solicita acceso a un recurso, el sistema verifica los atributos del usuario y del recurso en el contexto del entorno actual para decidir si se concede el acceso.

Ejemplos de Políticas ABAC:

Acceso a Información de Nómina: Solo los miembros del departamento de Recursos Humanos pueden acceder a esta información, y solo durante el horario comercial habitual. Además, el usuario puede acceder únicamente a los datos de su propia sucursal.

Acceso a Datos de Ventas: Un representante de ventas en la región de Estados Unidos puede acceder a oportunidades de ventas y datos confidenciales relacionados.

Beneficios de ABAC:

Control Granular: Permite una definición más detallada y específica de los permisos de acceso basados en múltiples atributos.

Flexibilidad: Puede adaptarse a una variedad de escenarios y necesidades de acceso, mejorando la seguridad y la eficiencia.

Adaptabilidad: Permite ajustes dinámicos basados en el contexto actual (como la ubicación o el horario).

ABAC en Microsoft Entra

Microsoft Entra combina RBAC y ABAC permitiendo a los administradores definir roles y agregar condiciones adicionales basadas en atributos. Por ejemplo, una política puede requerir que un usuario tenga un rol específico y que el objeto al que se accede tenga una etiqueta de metadatos particular para permitir la lectura.

Desventajas de ABAC:

- Complejidad: La configuración y el mantenimiento de políticas basadas en atributos pueden ser más complicados que en RBAC.
- Gestión de Políticas: Requiere una planificación cuidadosa y una gestión continua para mantener la eficacia y evitar la sobrecarga administrativa.

PBAC

¿Qué es Control de Acceso Basado en Políticas (PBAC)?

En los entornos tecnológicos modernos, conectar identidades con activos digitales es un desafío crucial. Con el auge de la computación en la nube, microservicios, y aplicaciones SaaS, las estrategias tradicionales de control de acceso, como RBAC (Control de Acceso Basado en Roles) y ABAC (Control de Acceso Basado en Atributos), enfrentan dificultades de escalabilidad y flexibilidad. Estas limitaciones se deben a la falta de un enfoque centralizado y dinámico, lo que es necesario para manejar entornos tecnológicos distribuidos y cambiantes.

Autorización:

La autorización es el proceso de determinar quién tiene acceso a qué, cuándo y cómo, basado en políticas alineadas con las necesidades empresariales y los requisitos de seguridad. Dada la complejidad de los entornos actuales, las estrategias de autorización necesitan ser más flexibles y adaptables.

Características:

Centralización de Políticas: PBAC proporciona un marco de gestión de autorización centralizado, coordinando RBAC, ABAC y decisiones en tiempo real.

Flexibilidad: Permite a los propietarios de aplicaciones crear políticas claras y adaptables que se ajusten a las necesidades específicas de la organización.

Interfaz de Usuario: Ofrece una interfaz de usuario gráfica que permite a los gestores de negocios y propietarios de aplicaciones definir y aplicar políticas sin necesidad de conocimientos técnicos profundos.

Beneficios de PBAC:

Gestión Centralizada y Aplicación Distribuida: Permite gestionar las políticas de manera centralizada mientras se aplica la autorización en diferentes puntos de la infraestructura.

Visibilidad de Políticas: Los gestores pueden investigar, probar y aprobar políticas sin conocimientos técnicos, mejorando la gestión y auditoría de accesos.

Adaptación en Tiempo Real: Implementa decisiones de autorización en tiempo real, crucial para entornos basados en el modelo de confianza cero.

Evolución de la Autorización

1. Listas de Control de Acceso (ACL): Primer método para implementar autorización, basado en listas locales de usuarios y sus niveles de acceso. Su escalabilidad es limitada.

2. Control de Acceso Basado en Roles (RBAC): Asigna permisos a roles y luego a los usuarios. Aunque más gestionable que ACL, enfrenta problemas de escalabilidad y flexibilidad, como la "explosión de roles".

3. Control de Acceso Basado en Atributos (ABAC): Utiliza múltiples atributos (de usuario, recurso y entorno) para tomar decisiones de acceso más detalladas. Sin embargo, puede ser complejo de gestionar y no siempre considera las necesidades no técnicas.

Aspectos Clave de PBAC:

Adaptación a Tecnologías Modernas: Ideal para entornos con arquitecturas basadas en microservicios y múltiples plataformas.

Cumplimiento Normativo: Facilita la conformidad con regulaciones como GDPR al controlar el acceso de manera más estricta y evitar el acceso no autorizado a datos sensibles.

Autorización Dinámica:

PBAC se combina con autorización dinámica para tomar decisiones de acceso en tiempo real, basado en la identidad del usuario, el recurso al que intenta acceder y factores externos como señales de riesgo.

Principios del Modelo de Confianza Cero (Zero Trust):

Acceso por Sesión: Se evalúa la confianza en el solicitante antes de conceder acceso.

Políticas Dinámicas: Las decisiones de acceso se basan en políticas dinámicas que consideran atributos observables del cliente y el recurso.

CONCLUSIÓN

Los servicios de autenticación como LDAP, RADIUS, TACACS+ y Kerberos son fundamentales para garantizar la seguridad y el control de acceso en redes y sistemas informáticos. Cada uno de estos protocolos tiene características específicas que los hacen adecuados para diferentes entornos y necesidades de seguridad:

En general, estos protocolos mejoran la seguridad al centralizar y estandarizar el proceso de autenticación, garantizando que solo los usuarios autorizados accedan a los recursos de la red, y asegurando la integridad y confidencialidad de las comunicaciones. La elección de uno u otro depende de los requisitos específicos de la red, como el nivel de seguridad necesario, la complejidad de la infraestructura y las necesidades de administración de usuarios.

El control de acceso es fundamental para la seguridad de la información y la gestión de recursos en entornos tecnológicos modernos. A medida que las organizaciones evolucionan y adoptan tecnologías más complejas, como la computación en la nube y los microservicios, los métodos tradicionales de control de acceso enfrentan desafíos significativos en términos de escalabilidad y flexibilidad.

BIBLIOGRAFIA.

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

https://protegermipc.net/2020/05/06/que-es-el-protocolo-radius-caracteristicas-y-fases-de-autenticacion/

tacacs.net/lp-sp/

Autenticación TACACS+ | Junos OS | Juniper Networks

Autenticación Kerberos: cómo el servicio garantiza la ciberseguridad - IONOS MX

https://ccnadesdecero.es/listas-control-acceso-acl-router-cisco/

ACL servicios de autenticación - Búsqueda (bing.com)

https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-role-based-access-control-rbac/RBAC: ¿Qué es Role based access control? - IONOS España

https://www.ingecom.net/es/blog/320/rbac-vs-abac-cual-elegir/ RBAC vs ABAC: ¿Cuál elegir? (ingecom.net)

https://www.plainid.com/identity-security-posture-management-learning-hub/pbac-authorization-guide-for-the-enterprise/ PBAC - An Authorization Guide for the Enterprise | PlainID