DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.3**	**Actividad**	Investigación Listas de Control de Accesos				
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:	16/04/2021
Compet. Genéricas		4.1, 4.5, 5.2,		Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

- Identificar los tipos de listas de control de acceso

2. Introducción

Los controles de acceso son soluciones de hardware y software que se utilizan para administrar el acceso a recursos y a los sistemas, las listas de control de acceso (ACL) definen el tipo de tráfico permitido en una red informática.

3. Instrucciones (Descripción) de la actividad

1. Elaborar un resumen con los tipos de Listas de Acceso.

2. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Práctica, 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

Definición

En seguridad informática, una lista de control de acceso (ACL) es una lista de permisos asociados con un recurso del sistema (objeto). Una ACL especifica qué usuarios o procesos del sistema tienen acceso a los objetos, así como qué operaciones están permitidas en determinados objetos. Cada entrada en una ACL típica especifica un asunto y una operación. Por ejemplo, si un objeto de archivo tiene una ACL que contiene (Alice: leer,

escribir; Bob: leer), esto le daría a Alice permiso para leer y escribir el archivo y solo le daría a Bob permiso para leerlo.

Ventajas

- La posibilidad de mejorar el rendimiento de la red limitando determinado tráfico, por ejemplo , se puede impedir que los empleados de una oficina descarguen o visualicen ficheros de video. Los ficheros de video ocupan mucho ancho de banda y pueden colapsar la red.
- Posibilidad de permitir o denegar el acceso de equipos a ciertas zonas de la red. Por ejemplo, los alumnos que utilizan el servidor que proporciona servicios a su aula no deberían tener acceso al servidor de la secretaría del centro o los empleados que trabajan en una zona de red no deberían acceder a la zona de red donde trabaja el personal de administración.
- Permiten que no se ejecuten determinados comandos por la red destinados a fines malintencionados, etc.

Funciones

- 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.

Filtrado de Paquetes (Workflow)

El filtrado de los paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes, y la transferencia o el bloqueo de estos según criterios determinados. Las ACL estándares filtran sólo en la Capa 3, mientras que las ACL extendidas filtran en las capas 3 y 4 del modelo OSI.

El criterio de filtrado establecido en cada entrada de una ACL es la dirección IP de origen. Un router configurado con una ACL estándar toma la dirección IP de origen del encabezado del paquete y comienza a compararla con cada entrada de la ACL de manera secuencial. Cuando encuentra una coincidencia, el router realiza la instrucción correspondiente, que puede ser: permitir o bloquear el paquete, y finaliza la comparación. Si la dirección IP del paquete no coincide con ninguna entrada en la ACL, se bloquea el paquete por definición.

La última instrucción de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La

denegación implícita bloquea todo el tráfico. Debido a esto, una ACL que no tiene al menos una instrucción permitida bloqueará todo el tráfico.

Para la configuración de las Listas de Control de Acceso de los routers, es importante conocer que estas se aplican para el intercambio de paquetes de datos tanto a las interfaces de red de entrada como de salida. En este sentido:

- Las ACL de entrada: procesan los paquetes entrantes al router antes de dirigirse a la interfaz de salida. Constituyen un elemento de eficacia, porque ahorran la sobrecarga de encaminar búsquedas si el paquete se descarta. Son ideales para filtrar paquetes de datos cuando la red conectada a una interfaz de entrada es el único origen de estos que se deben examinar.
- Las ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida del router, y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica un mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

Máscaras Wildcard

Cada entrada de una ACL incluye el uso de una máscara wildcard o “comodín”. Una máscara wildcard es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección del paquete debe examinar para obtener una coincidencia. Como ocurre con las máscaras de subred, los números 1 y 0 en la máscara wildcard identifican lo que hay que hacer con los bits de dirección IP correspondientes. Sin embargo, en una máscara wildcard, estos bits se utilizan para fines diferentes y siguen diferentes reglas:

- Bit 0 de la máscara wildcard: se establece la coincidencia con el valor del bit correspondiente en la dirección IP.
- Bit 1 de la máscara wildcard: se omite el valor del bit correspondiente en la dirección IP.

Mientras que las máscaras de subred utilizan 1 y 0 binarios para identificar la red, la subred y la porción del host de una dirección IP las máscaras wildcard los utilizan para filtrar direcciones IP individuales o grupos de ellas, permitiendo o denegando el acceso a los recursos. A las máscaras wildcard a menudo se las denomina “máscaras inversas”. La razón es que, a diferencia de una máscara de subred en la que el 1 binario equivale a una coincidencia y el 0 binario no, en las máscaras wildcard es al revés. Aunque el cálculo de la máscara wildcard puede ser difícil, un método abreviado para determinarla es restar a 255.255.255.255 la máscara de red de la dirección IP.

Para simplificar el trabajo con la máscara wildcard se emplean además las palabras clave host y any, que eliminan la necesidad de introducirlas para identificar un host específico o toda una red, además de facilitar la lectura de la lista de control de accesos, ya que proporcionan pistas visuales en cuanto al origen o el destino de los criterios:

- La palabra host reemplaza la máscara wildcard 0.0.0.0, la cual indica que todos los bits de la dirección IP deben coincidir para filtrar solo un host.
- La opción any sustituye la dirección IP y la máscara 255.255.255.255. Esto establece que se omita la dirección IP completa o que se acepte cualquier dirección.

Tipos

Al crear una lista de control de acceso un administrador de red tiene varias opciones; en este sentido, la complejidad del diseño de dicha red determina el tipo de ACL necesaria. Por lo general, existen dos tipos clásicos de ACL:

- ACL estándar: que permiten el filtrado de paquetes de datos únicamente verificando la dirección IP de origen. De esta manera, si un dispositivo es denegado por una ACL estándar, se deniegan todos los servicios provenientes de él. Este tipo de ACL sirve para permitir el acceso de todos los servicios de un usuario específico, o LAN, a través de un router y a la vez, denegar el acceso de otras direcciones IP. Las ACL estándar están identificadas por el número que se les ha asignado. Para las listas de acceso que permiten o deniegan el tráfico IP, el número de identificación puede variar entre 1 y 99 o entre 1300 y 1999.

- ACL extendidas: filtran no sólo según la dirección IP de origen, sino también según la dirección IP de destino, el protocolo y los números de puertos. Con frecuencia son más empleadas que las ACL estándar, porque son más específicas y ofrecen un mayor control. El rango de números de las ACL extendidas va de 100 a 199 y de 2000 a 2699.

Adicionalmente, tanto a las ACL estándar como extendidas es posible hacerles referencia mediante un nombre descriptivo en lugar de un número, lo que se conoce como ACL nombradas. Existen además otros tipos de ACL, enfocados en propósitos específicos de configuración y manejo del filtrado de los paquetes de datos, como son las ACL dinámicas, reflexivas, basadas en tiempo, y basadas en el contexto, entre otras.

Una vez creada, una ACL debe asociarse a una interfaz de la siguiente manera:

- Modo de acceso entrante: Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento (evita la sobrecarga asociada a las búsquedas en las tablas de enrutamiento si el paquete ha de ser descartado por las pruebas de filtrado).
- Modo de acceso saliente: Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión. Las listas de acceso no actúan sobre paquetes originados en el propio router, como las actualizaciones de enrutamiento a las sesiones Telnet salientes.

La siguiente lista muestra los rangos de listas de acceso numeradas:

- IP estándar: 1-99 y 1300-1999
- IP extendida: 100-199 y 2000-2699
- DECnet: 300-399
- XNS estándar: 400-499
- XNS extendida: 500-599

- Apple Talk: 600-699
- IPX estándar: 800-899
- IPX extendida: 900-999
- Filtros Sap: 1000-1099

Consideraciones Adicionales de Configuración

La configuración de la ACL puede ser una tarea compleja. Para cada interfaz de red de un router, puede haber varias políticas necesarias para administrar el tipo de tráfico que se tiene permitido ingresar o salir de ella. Como buenas prácticas es recomendable configurar ACL independientes tanto para el tráfico entrante como para el saliente. Las siguientes son algunas pautas para el uso de las ACL:

- Utilizar la ACL en los routers de firewall ubicados entre la red interna y la externa (como Internet).
- Emplear la ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de la red interna o que sale de esta.
- Configurar la ACL en los routers de frontera, es decir, los ubicados en los límites de las redes, lo que proporciona una separación básica de la red externa, o entre un área menos controlada y otra más importante de la propia red.
- Configurar la ACL para cada interfaz de red (de entrada, o de salida), del router de frontera.

El uso de las ACL requiere prestar atención a los detalles y un extremo cuidado. Los errores pueden ser costosos en términos de tiempo de inactividad, esfuerzos de resolución de problemas y servicio de red deficiente. Antes de configurar una ACL, se requiere una planificación básica. La correcta conformación de la ACL puede contribuir a que la red funcione de forma eficiente. En este sentido, se deben configurar donde tengan mayor impacto. Las reglas básicas que se deben considerar son:

- Las ACL estándar se colocan cerca del destino del tráfico. Esto se debe a sus limitaciones, pues no se puede distinguir el destino.
- Las ACL extendidas se colocan cerca del origen del tráfico por eficiencia, para evitar tráfico innecesario en el resto de la red.

5. Reflexión

El uso de listas de control de acceso es de gran importancia para llevar un control y regular la seguridad dentro de la red, así como garantizar un correcto uso de la misma. Implementar listas de acceso en una red de trabajo puede ser de gran utilidad para garantizar un ambiente enfocado a las actividades laborales designados a los empleados, eliminando la presencia de algunos factores distractores; además, privar el acceso a determinados sitios y a realizar determinadas operaciones en la web puede ser de gran utilidad para establecer un estándar de seguridad y tener un margen mucho más acotado en caso de necesitar de una intervención técnica para el mantenimiento de la red, pues se sabe con certeza que sitios y operaciones estaban permitidas.

6. Referencias

- Ernesto. A. (31/10/2019). Tipos de lista de Acceso. Recuperado el 13/04/2021 de: https://aprenderedes.com/2019/10/tipos-de-listas-de-acceso/

- N/A (21/01/2019). ACL: Lista de Control de Accesos. Recuperado el 13/04/2021 de: https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html