DATOS DE LA ACTIVIDAD							
No. de Actividad:	**1.8**	**Investigación**	**Conceptos AAA**				
Unidad:	Unidad: 1: Riesgos de seguridad informática en infraestructura de red						
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:	05/03/2021
Compet. Genéricas	4.1, 4.5, 5.2, 5.5			Competencia Profesional		CP1-1	

1. Objetivo(s) de la actividad

Conocer los identificar los conceptos de autorización, autenticación y registro.

2. Instrucciones (Descripción) de la actividad

1. Investigar los conceptos: Autenticación , Autorización y Registro, como se aplican estos conceptos en un sistema informático.

2. Identificar las características de los servidores AAA : TACACS, RADIUS, características, ventajas y desventajas ,

3. 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.

4. 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.

3. Desarrollo de la actividad

Autenticación, autorización y registro (AAA)

Son un conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información. Se sigue

un protocolo para autenticar a un usuario basándose en la identidad verificable del usuario, autorizar a un usuario basándose en sus derechos de usuario y contabilizar el consumo de recursos de una red de un usuario.

Autenticación: Se refiere a la confirmación de que, el usuario que solicita los servicios sea un usuario valido de los servicios de red solicitados. Se define como un proceso entre dos entidades, una de ellas da a conocer su identidad y la otra lo verifica. En informática sirve como implementación de seguridad para que las personas que acceden al sistema/información sean identificables.

Autorización: Se refiere a otorgar tipos específicos de recursos y/o servicios a un usuario, basado en su autenticación, los servicios que solicitan, y el estado actual del sistema. La autorización puede basarse en restricciones, por ejemplo, restricciones de hora del día o restricciones de ubicación física, o restricciones contra múltiples inicios de sesión por parte del mismo usuario. La autorización determina la naturaleza del servicio que se otorga a un usuario.

Los ejemplos de tipos de servicio incluyen, entre otros:

- Filtrado de direcciones IP
- Asignación de direcciones
- Asignación de rutas
- QoS / servicios diferenciales
- Control de ancho de banda / gestión de tráfico
    - Tunelización obligatoria a un punto final específico y cifrado.

Las aplicaciones o permisos de autorización lo determinan el servidor del servicio y varía de acuerdo con políticas propias de las entidades.

Registro: La contabilidad se refiere al seguimiento del consumo de recursos de red por parte de los usuarios. Esta información se puede utilizar para fines de administración, planificación, facturación u otros. La contabilidad en tiempo real se refiere a la información contable que se entrega al mismo tiempo que el consumo de los recursos. La contabilidad por lotes se refiere a la información contable que se guarda hasta que se entrega en un momento posterior. La información típica que se recopila en la contabilidad es la identidad del usuario, la naturaleza del servicio prestado, cuándo comenzó el servicio y cuándo terminó. Dicha información del estudio dinámico los usa comúnmente para la planificación.

Servidores AAA

TACACS

Terminal Access Controller Access-Control System (TACACS) se refiere a una familia de protocolos relacionados que manejan la autenticación remota y los servicios relacionados para el control de acceso en red a través de un servidor

centralizado. El protocolo TACACS original, que se remonta a 1984, se utilizó para comunicarse con un servidor de autenticación, común en las redes UNIX más antiguas; generó protocolos relacionados:

Extended TACACS (XTACACS) es una extensión patentada de TACACS introducida por Cisco Systems en 1990 sin compatibilidad con versiones anteriores del protocolo original. TACACS y XTACACS permiten que un servidor de acceso remoto se comunique con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

Terminal Access Controller Access-Control System Plus (TACACS+) es un protocolo desarrollado por Cisco y lanzado como estándar abierto a partir de 1993. Aunque derivado de TACACS, TACACS + es un protocolo separado que maneja autenticación, autorización y contabilidad (AAA) servicios. TACACS+ ha reemplazado en gran medida a sus predecesores.

TACACS+ es un protocolo cliente/servidor que proporciona la Seguridad centralizada para los usuarios que intentan tener el Acceso de administración a un Router o a un servidor de acceso a la red. El TACACS+ proporciona estos servicios del Authentication, Authorization, and Accounting (AAA):

- Autenticación de los usuarios que intentan iniciar sesión al equipo de red
- Autorización de determinar qué nivel de usuarios del acceso debe tener
- El considerar para no perder de vista todos los cambios el usuario hace

Este protocolo utiliza una administración de red simplificada incrementando su seguridad al permitir centralizar la gestión de los usuarios en la red a través de políticas de acceso de usuarios, grupos, comandos, ubicación, subred o tipo de dispositivo.

Del mismo modo el protocolo TACACS+ proporciona un registro completo de todos los usuarios que se registraron y de los comandos que utilizaron, reflejando de forma clara que es un protocolo orientado a la administración donde se puede tener de forma detallada toda aquella información sobre los usuarios y dispositivos de red que interactuaron en determinado momento y, además, proporcionar un registro detallado de cada acción realizada

Una de las características más importantes de TACACS + es la separación entre autenticación, autorización y registro, sin embargo, es importante tener en cuenta que a pesar de que el protocolo cuente con las tres posibilidades (AAA) de configuración, su uso e implementación depende de la necesidades del usuario y no es de carácter impositivo su uso ya que cada uno es independiente del otro, aunque estas tres características juntas pueden ser muy efectivas en control y cuidado de la información.

Dentro las múltiples ventajas de separar autenticación, autorización y registro, es que permite adaptar el protocolo de forma más sencilla y eficiente a las necesidades

propias de cada cliente, puede integrarse con otros procesos de negociación tales como PPP, el proceso de autorización puede convertirse en un proceso dinámico, en lugar, de depender directamente de la autenticación

RADIUS

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Service) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wifi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuándo comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red(NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos. Se comprende tres elementos:

- Un protocolo con un formato de trama que utiliza el User Datagram Protocol (UDP) /IP.
- Un servidor.
- Un cliente.

El servidor se ejecuta en un equipo central típicamente en el sitio de cliente, mientras que los clientes residen en los servidores de acceso por marcado y pueden ser distribuidos en la red.

Modelo Cliente/Servidor
Un servidor de acceso a la red (NAS) actúa como cliente de RADIUS. El cliente es responsable de traspasar información del usuario a servidores RADIUS designados y de actuar según la repuesta recibida. Los servidores RADIUS son responsables de recibir las solicitudes de conexión del usuario, autenticar al usuario y devolver la información de configuración necesaria para que el cliente pueda brindarle el servicio al usuario. Los servidores RADIUS pueden actuar como clientes de servidor alterno respecto de otros servidores de autenticación.

Seguridad de redes
Las transacciones entre el cliente y el servidor RADIUS son autenticadas mediante el uso de un secreto compartido, que nunca se envía por la red. Además, cualquier contraseña de usuario se envía cifrada entre el cliente y el servidor RADIUS. Esto elimina la posibilidad de que una persona que hace snooping en una red no segura pueda determinar la contraseña de un usuario.

Mecanismo de Autenticación flexible
El servidor RADIUS soporta una variedad de métodos para autenticar un usuario. Cuando se proporciona con el nombre de usuario y la contraseña original otorgados por el usuario, puede soportar el PPP, el Password Authentication Protocol (PAP), o el Challenge Handshake Authentication Protocol (CHAP), UNIX login, y otros mecanismos de autenticación.

Comparación de TACACS+ y RADIUS

UDP y TCP
RADIUS usa UDP mientras que TACACS + usa TCP. TCP ofrece varias ventajas sobre UDP. TCP ofrece un transporte orientado a la conexión, mientras que UDP ofrece una entrega con el mejor esfuerzo. RADIUS requiere variables programables adicionales, como intentos de retransmisión y tiempos de espera para compensar el transporte de mejor esfuerzo, pero carece del nivel de soporte integrado que ofrece un transporte TCP:

- El uso de TCP proporciona un reconocimiento por separado de que se ha recibido una solicitud, dentro de (aproximadamente) un tiempo de ida y vuelta de la red (RTT), independientemente de lo cargado y lento que pueda estar el mecanismo de autenticación de backend (un reconocimiento de TCP).

- TCP proporciona una indicación inmediata de un servidor bloqueado o que no se está ejecutando mediante un reinicio (RST). Puede determinar cuándo un servidor falla y vuelve al servicio si usa conexiones TCP de larga duración. UDP no puede diferenciar entre un servidor que no funciona, un servidor lento y un servidor que no existe.

- Mediante el uso de keepalives de TCP, los bloqueos del servidor se pueden detectar fuera de banda con solicitudes reales. Las conexiones a varios servidores se pueden mantener simultáneamente, y solo necesita enviar mensajes a los que se sabe que están en funcionamiento.

- TCP es más escalable y se adapta a redes en crecimiento y congestionadas.

Cifrado de paquetes
RADIUS cifra solo la contraseña en el paquete de solicitud de acceso, del cliente al servidor. El resto del paquete no está encriptado. Otra información, como nombre de usuario, servicios autorizados y contabilidad, puede ser capturada por un tercero.

TACACS + cifra todo el cuerpo del paquete pero deja un encabezado TACACS + estándar. Dentro del encabezado hay un campo que indica si el cuerpo está encriptado o no. Para fines de depuración, es útil tener el cuerpo de los paquetes sin cifrar. Sin embargo, durante el funcionamiento normal, el cuerpo del paquete está completamente encriptado para comunicaciones más seguras.

Autenticación y autorización
RADIUS combina autenticación y autorización. Los paquetes de aceptación de acceso enviados por el servidor RADIUS al cliente contienen información de autorización. Esto dificulta la separación de la autenticación y la autorización.

TACACS + usa la arquitectura AAA, que separa AAA. Esto permite soluciones de autenticación independientes que aún pueden usar TACACS + para autorización y contabilidad. Por ejemplo, con TACACS +, es posible utilizar la autenticación Kerberos y la autorización y contabilidad TACACS +. Después de que un NAS se autentica en un servidor Kerberos, solicita información de autorización de un servidor TACACS + sin tener que volver a autenticarse. El NAS informa al servidor TACACS + que se ha autenticado correctamente en un servidor Kerberos y, a continuación, el servidor proporciona información de autorización.

Durante una sesión, si se necesita una verificación de autorización adicional, el servidor de acceso verifica con un servidor TACACS + para determinar si el usuario tiene permiso para usar un comando en particular. Esto proporciona un mayor control sobre los comandos que se pueden ejecutar en el servidor de acceso mientras se desacopla del mecanismo de autenticación.

Soporte multiprotocolo

RADIUS no admite estos protocolos:
- Protocolo de acceso remoto AppleTalk (ARA)
- Protocolo de control del protocolo de tramas NetBIOS
- Interfaz de servicios asíncronos de Novell (NASI)
- Conexión X.25 PAD

TACACS + ofrece soporte multiprotocolo.

Gestión de enrutadores
RADIUS no permite a los usuarios controlar qué comandos se pueden ejecutar en un enrutador y cuáles no. Por lo tanto, RADIUS no es tan útil para la administración de enrutadores ni tan flexible para los servicios de terminal.

TACACS + proporciona dos métodos para controlar la autorización de los comandos del enrutador por usuario o por grupo. El primer método es asignar niveles de privilegios a los comandos y hacer que el enrutador verifique con el servidor TACACS + si el usuario está autorizado en el nivel de privilegio especificado. El segundo método es especificar explícitamente en el servidor TACACS +, por usuario o por grupo, los comandos que están permitidos.

Interoperabilidad
Debido a varias interpretaciones de la Solicitud de comentarios (RFC) de RADIUS, el cumplimiento de las RFC de RADIUS no garantiza la interoperabilidad. Aunque varios proveedores implementan clientes RADIUS, esto no significa que sean interoperables. Cisco implementa la mayoría de los atributos de RADIUS y agrega más constantemente. Si los clientes usan solo los atributos RADIUS estándar en sus servidores, pueden interoperar entre varios proveedores siempre que estos proveedores implementen los mismos atributos. Sin embargo, muchos proveedores implementan extensiones que son atributos patentados. Si un cliente utiliza uno de estos atributos ampliados específicos del proveedor, la interoperabilidad no es posible

4. Reflexión

Conocer las características de los servidores de AAA más utilizados en la implementación de medidas de seguridad en las redes es de suma importancia para estar al tanto de como pueden ser llevadas a la práctica en un momento posterior, así como configurarlos de manera correcta cuando se establezcan redes en los diferentes entornos donde nos desarrollemos. Podemos ver como los servidores de AAA tienen características comunes y como sus diferencias son las que hacen que uno sea mejor opción que otra en una implementación de seguridad en particular.

Referencias:

- Cisco C. (14 January 2008). TACACS+ and RADIUS Comparison. Retrieved at 05/03/2021 from : https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

- L. Grant (19 February 2018). The TACACS+ Protocol. Retrieved at 05/03/2021 from: https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-08.html

- RADIUS SARL. (2014). THE FREERADIUS TECHNICAL GUIDE. Retrieved at 05/03/2021 from: https://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf

- Cisco Press. (22 February 2002). Examining Cisco AAA Security Technology. Retrieved at 05/03/2021 from: https://www.ciscopress.com/articles/article.asp?p=25471&seqNum=4