Administración de seguridad de red

Administración de servicios en red

Integrantes:

Rojas Alvarado Luis Enrique

Miranda Sandoval Mario A.

Hernández Escobedo Fernando

Objetivo

- Controlar el acceso a los recursos de la red, protegerla de modo que no pueda ser dañada (intencional o involuntariamente) y que la información que es vulnerable sea utilizada con autorización apropiada

Funciones

- Identificación y autentificación del usuario (id y clave de acceso).
- Dar permisos específicos a los usuarios de la red.
- Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.
- Define las medidas de prevención y las acciones a llevar a cabo frente a ataques de virus o intrusos al sistema.

Características de un Sistema Seguro.

- Confidencialidad: Los objetos de un sistema han de ser accedidos únicamente por elementos autorizados y que estos no van a convertir esa información en disponible para otras entidades.

- Integridad: Los elementos solo pueden ser modificados por elementos autorizados de manera controlada.

- Disponibilidad: Los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

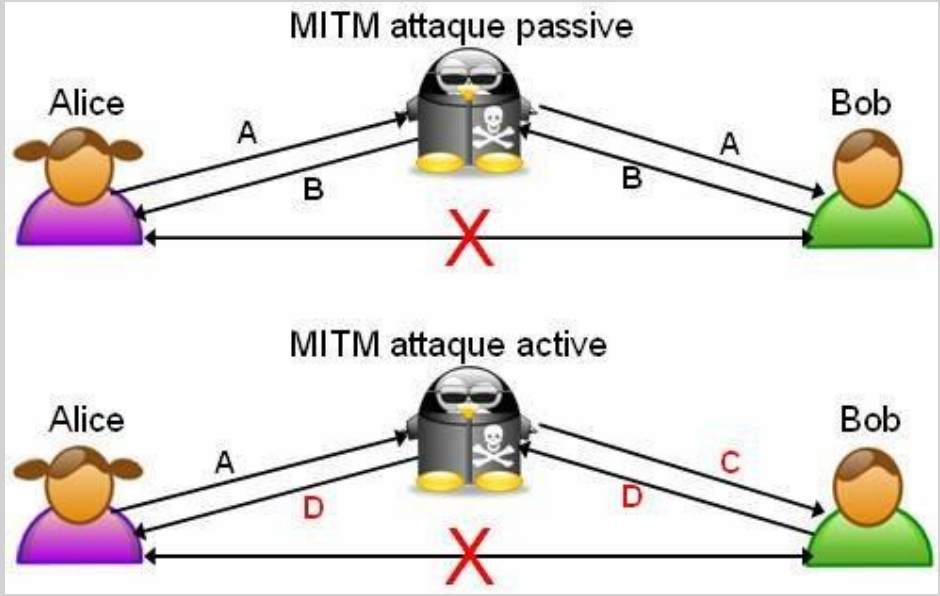
Tipos de amenazas.

- Interrupción de servicio: Que nunca se deje de ofrecer un servicio.
- Interceptación de datos: Los datos en un sistema solo podrán tener acceso los usuarios autorizados.
- Modificación de nuestros datos: Los datos solo serán modificados por usuarios válidos.
- Suplantanción de indentidad: Que no se creen usuarios no autorizados.

Tipos de ataques

ATAQUES ACTIVOS

ATAQUES PASIVOS



Ataques activos

En este tipo de ataques existe evidencia del hecho por mal funcionamiento de componentes o servicios, o por sustitución de usuarios en ejecución de tareas orientados a tratar de conseguir información privilegiada o interrumpir un servicio crítico para la organización, puede ser desde el interior o del exterior.

Ejemplo de ataques activos

- Modificación del contenido de los datos que circulan por la red
- Alteración del orden de llegada de los datos
- Supresión de mensajes con un destino particular
- Saturación de la red con datos inútiles para degradar la calidad de servicio
- Engaño de la identidad de un host o usuario para acceder a datos confidenciales
- Desconfiguraciones para sabotaje de servicios.

Ataques pasivos

Ataques difíciles de detectar, ya que no se produce evidencia física del ataque pues no hay alteración de datos ni mal funcionamiento o comportamiento fuera de lo habitual de la red, escucha o "intercepción del tráfico de la red y los servicios involucrados", estudio de parámetros de configuración de manera ilegal por parte del intruso, robo de información sensible para las organizaciones.

Ejemplo de ataques pasivos

Un ataque pasivo involucra a alguien que escucha en las bolsas de telecomunicaciones o grabar de forma pasiva la actividad del ordenador. Un ejemplo del primer caso es un tráfico de red atacante oler usando un analizador de protocolos o algún otro software de paquetes de captura. El atacante encuentra una manera de conectar a la red y empieza a capturar el tráfico para su posterior análisis.

Ejemplo de ataques pasivos

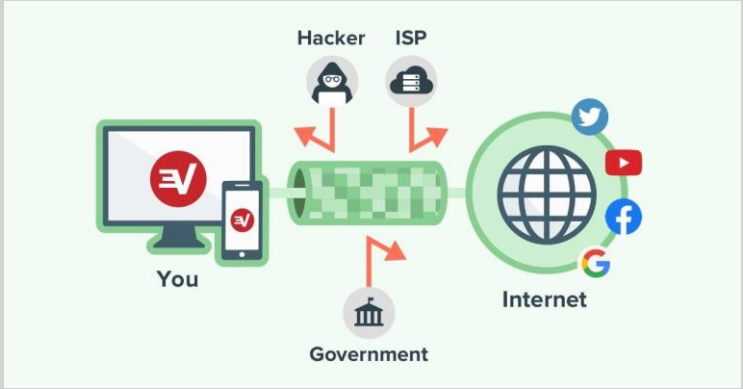
Otros atacantes se basan en capturadores de teclado, por lo general como un caballo de Troya en una "descarga gratuita", para registrar pulsaciones de teclas, como nombres de usuario y contraseñas. El objetivo, sin importar el método, es sólo para escuchar y grabar los datos de paso. El ataque pasivo en sí no es perjudicial, per se, pero la información recopilada durante la sesión puede ser extremadamente perjudicial.

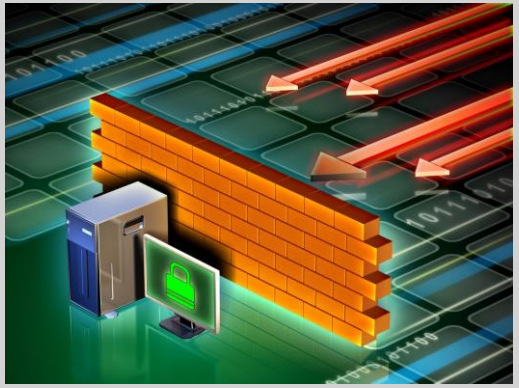
Estrategia de defensa

- Protección: debe configurar sus redes y redes lo más correctamente posible
- Detección: debe ser capaz de identificar cuándo ha cambiado la configuración o si algún tráfico de red indica un problema
- Reacción: después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro. (Única forma posible con las copias de seguridad).

Defensas generales

- Control de acceso
- Prevención de perdida de datos
- Seguridad del correo electrónico
- Firewalls
- Antimalware
- VPN
- Movíl y seguridad inalámbrica





Métodos de autenticación.

- Algo que el usuario sabe.
- Algo que éste posee.
- Una característica física del usuario. (Autentificación biométrica).

Problemas.

El principal problema no viene de los ataques externos sino del factor humano, como lo son:

- Descuido.
- Usuarios malintencionados.
- Uso de servicios inseguros. (ftp, telnet, www)
- Falta de organización.
- Contraseñas.

Bibliografía

•[1] Interpolados, “Administración de la seguridad de red”, 26/julio/2018. https://interpolados.wordpress.com/2018/07/26/administracion-de-la-seguridad-de-red/. Recuperado el 06/10/2020.

•[2] Silvia Eugenia Mesa Correa, “Seguridad en redes”, 2010, http://redesysegu.blogspot.com/p/administracion-de-redes.html. Recuperado el 06/10/2020.

•[3] Viridiana Navarro, “Ataques activos y pasivos.”, 19/feb/2019, https://prezi.com/p/z9txp6dwpqkm/ataques-activos-y-pasivos/. Recuperado el 06/10/2020.

•[4] Josh Fruhlinger, “¿Qué es la seguridad de la red?”, 2018, https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red . Recuperado el 06/10/2020.

•[5] José Gpe. Vargas Hernández, “Administración de redes y seguridad informática”, 2002, https://www.gestiopolis.com/administracion-de-redes-y-seguridad-informatica/ . Recuperado el 06/10/2020.