FIREWALLS

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

- A continuación, abordaremos a detalle el tema de como es que trabajan los firewalls a nivel de capas del modelo OSI, en que nos ayudan y cuales son los distintos tipos que existen, adicionalmente conocer las ventajas, desventajas y limitaciones que nos presentan cada uno de los tipos ya sean lógicos o físicos, adicionalente donde se deben de colocar los mismos para que nos protejas de los ataques externos.

Firewalls como herramientas de seguridad

Tipos de ataques informaticos

Existen varios tipos de ataques como son:

- Spoofing: significa copiar una película o un texto, aunque en el caso específico de las redes de computación, incluyendo Internet, hace referencia a un paquete del IP o protocolo de Internet (protocolo básico para enviar datos por Internet o cualquier otro tipo de red), del que un intruso hace una copia falsa de la dirección IP para esconder la identidad de quien envía el mensaje y así poder entrar a otras computadoras o redes.
- Ataque de negación del servicio: es mediante el cual el atacante impide al usuario legítimo tener acceso a la información y a los servicios de su computadora, lo que provoca que el usuario no tenga la posibilidad de accesar a su correo electrónico, sitios web, servicios en línea como bancos, líneas aéreas, etcétera.
- Rootkit y botnet: rootkit es una pieza de software instalada y escondida en la computadora de un usuario sin que éste sepa de su existencia y el botnet es un programa que se ejecuta de modo automático en la computadora, el cual tiene su origen en la palabra bot, que proviene de robot. Los botnets se refieren a computadoras que se controlan por una o más fuentes externas. Durante el ataque con los botnet, el atacante toma el control de una computadora infectándola con un virus u otro intruso maligno, lo que le permite tener acceso a la computadora.
- Phishing: Significa pesca, y es cuando los atacantes por medio de un correo o sitio web malicioso solicitan información personal haciendose pasar por una organización.

El modelo OSI

Sus siglas provienen del inglés Open System Interconnection y fue un modelo usado para estandarizar los intercambios de información entre equipos, para ello el conjunto completo se divide en 7 capas jerárquicas, donde cada una cuenta con funciones asociadas a ella y que presta servicio a las capas vecinas, donde cada capa para ´hacer una petición o envío de información al nivel equivalente, debe reconstruír la información y hacerla pasar por sus capas inferiores dónde cada una de ellas debe añadirle un encabezamiento específico, convirtiendse el mismo en un tren y una vez transferida, se descodificara la información y se liberan la petición o los datos que originaron el proceso.

Las 7 capas son Física, Conexión, Red, Transporte, Sesión, presentación y Aplicación. (***Para ampliar mas sobre el tema refiérase a el siguiente*** link)

¿Qué es un firewalls y como funciona?

Su traducción al español es cortafuego y éste protégé a los computadores de ataques externos a computadoras personales o redes de computadoras, puede ser de tipo físico o lógico, éste se puede configurar para bloquear datos provenientes de ciertos sitios o determinadas aplicaciones, a la vez que permite el paso de la información importante para la organización. Suele localizarse en el punto de unión entre dos redes y contiene una serie de reglas que debe cumplir, tambien rechaza los paquetes que no las cumplen, tambine puede estar configurado para registrar todos los intentos de entrada y salida de una red, así como para guardar esos registros. Asimismo, también es capaz de filtrar paquetes en función de su origen, su destino y el número de puerto de acceso, además Evita el congetionamiento de tránsito y controla el tipo de aplicaciones que acceden a internet, éste dispositivo tambien es vulnerable a otros tipos de daños

o ataques, como el daño o robo de información proveniente de los propios empleados de la organización.

Firewall de software y hardware

Entre estos dos tipos es importante destacar que el primero de ellos es mas barato, por lo cual las empresas pequeñas o personales suelen instalar de éste tipo, el mismo debe ser instalado directamente en cada una de las computadoras, en el caso del Segundo tenemos que es una caja que se coloca entre el router y una computadora o una red y lo que hace es que oculta la computadora de un usuario ante la red de internet. La mejor protección con firewall es instalar ambos tipos: el firewall de software y el firewall de hardware.

Los firewall de software de última generación

Estos realizan trabajo de filtrado en otras capas del modelo OSI, trabaja en la capa 7 que es la de aplicación de forma que el filtrado de información se adapta a las características propias de los protocolos de este nivel.

Limitaciones de los firewall

Algunas de ellas son:

- El filtrado de la información no es muy estricto lo que hace que las amenazas se mantengan vigentes.
- No protege de ataques internos a la organización o de las amenazas que provocan los usuarios descuidados o negligentes.
- Sólo brinda seguridad parcial, por lo que se aconseja tener otro elemento de seguridad.

CONCLUSIONES Y RECOMENDACIONES

En cuanto al tema de seguridad física y lógica de las redes, hemos logrado comprender el Soporte que nos brindan los firewalls y como es que los mismos se rigen bajo el modelo de estandar implentado por las capas del modelo OSI y con ello se ven los tipos de cortafuegos que existen y las recomendaciones que se nos hacen para aplicarlas a nivel físico como es la seguridad de las redes, edificios, datos entre otros, se recomienda incursionar en la investigación de temas que se han visto muy superficialmente como son las normas ISO.

REFERENCIAS BIBLIOGRÁFICAS

- Baca, G. (2016). *Introducción a la Seguridad informática* (1a. ed.). Grupo editorial Patria.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica