**Términos del glosario de la semana 2**

**Términos y definiciones del curso 3, semana 2**

**Acceso Wi-Fi protegido (WPA):** Protocolo de seguridad para proteger las redes inalámbricas cuando un dispositivo busca conectarse a Internet.

**Archivo de libre escritura (World-writable file):** Archivo que puede ser alterado por cualquier persona.

**Cortafuegos (Firewall):** Sistema de seguridad de red que monitorea el tráfico desde o hacia una red con objetivo de filtrar el malicioso.

**Cortafuegos basado en la nube:** Tipo de cortafuegos alojado en la nube.

**Cortafuegos Stateful (gestión con estado):** Tipo de cortafuego que realiza un seguimiento de la información que pasa a través de él y filtra proactivamente las amenazas.

**Cortafuegos Stateless (gestión sin estado):** Tipo de cortafuegos que funciona según reglas predefinidas y no realiza un seguimiento de la información de los paquetes de datos.

**Encapsulación:** Proceso ejecutado por un servicio VPN que protege datos confidenciales al encapsularlos en otros paquetes de datos.

**Filtrado de puertos:** Función de cortafuegos que bloquea o habilita determinados números de puertos, con el fin de limitar la comunicación no deseada.

**Firewall:** (consultar Cortafuegos).

**IEEE 802.11 (Wi-Fi):** Conjunto de estándares que definen la comunicación para redes locales inalámbricas.

**Protocolo de control de transmisión (TCP):** Protocolo de Internet que permite a dos dispositivos establecer una conexión y transmitir datos.

**Protocolo de resolución de direcciones (ARP):** Protocolo utilizado  para determinar la dirección MAC del siguiente router o dispositivo a atravesar.

**Protocolo de transferencia de hipertexto (HTTP):** Protocolo de red que se utiliza para la comunicación entre clientes y servidores de sitios web.

**Protocolo seguro de transferencia de archivos (SFTP):** Protocolo seguro utilizado para transferir archivos de un dispositivo a otro a través de una red.

**Protocolo seguro de transferencia de hipertexto (HTTPS):** Protocolo de red que proporciona un método seguro de comunicación entre clientes y servidores de sitios web.

**Protocolo Secure Shell (SSH):** Protocolo de seguridad utilizado para crear un intérprete de comandos con un sistema remoto.

**Protocolo simple de administración de red (SNMP):** Protocolo de red utilizado para monitorear y administrar los dispositivos en una red.

**Protocolos de red:** Conjunto de reglas utilizadas por dos o más dispositivos de una red para describir el orden de entrega y la estructura de los datos.

**Red privada virtual (VPN):** Tecnología de seguridad de red que cambia la dirección IP de una persona para enmascarar su ubicación y establecer una conexión segura en Internet.

**Segmentación de red:** Técnica de seguridad que divide la red en segmentos.

**Servidor proxy:** Servidor que recibe las solicitudes de clientes y las reenvía a otros servidores.

**Servidor proxy de reenvío:** Servidor que regula y restringe el acceso a Internet para permitir la conexión sin comprometer la seguridad de la red interna.

**Servidor proxy inverso:** Servidor que regula y restringe el acceso de Internet a un servidor interno.

**Sistema de nombres de dominio (DNS):** Protocolo de red que traduce los nombres de dominio de Internet como direcciones IP.

**Tarjeta de interfaz de red (NIC):** Dispositivo que se instala en el interior de una computadora para que esta pueda conectarse a Internet.

**Zona controlada:** Subred que protege la red interna de la externa.

**Zona de seguridad:** Segmento de la red de una empresa que protege la red interna de Internet.

**Zona no controlada:** Parte de la red que está fuera de la organización.

Marcar como completo

Me gusta

No me gusta

Informar de un problema