Glosario  
Ciberseguridad

## Términos y definiciones del Curso 3

A

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

**Actualización de parches:** Modificación de un programa o sistema operativo que soluciona vulnerabilidades de seguridad.

**Análisis de registros de red:** Proceso de examinar los registros de red para identificar eventos de interés.

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

**Ataque de denegación de servicio (DoS):** Un ataque dirigido a una red o servidor que los inunda con tráfico no deseado para inhabilitar los sistemas y servicios informáticos de forma temporal.

**Ataque de denegación de servicio distribuido (DDoS):** Tipo de ataque de denegación o servicio que utiliza múltiples dispositivos o servidores situados en diferentes ubicaciones, para inundar la red de destino con tráfico no deseado.

**Ataque de inundación del protocolo de mensajes de control de Internet (inundación ICMP):** Tipo de ataque DoS que consiste en enviar repetidamente paquetes ICMP a un servidor de red.

**Ataque de inundación sincronizada (SYN):** Tipo de ataque DoS que simula una conexión TCP/IP e inunda un servidor con paquetes SYN.

**Ataque de repetición:** Ataque a la red que consiste en interceptar un paquete de datos en tránsito para retrasarlo o repetirlo en otro momento.

**Ataque de suplantación de IP:** Ataque de red que consiste en cambiar la IP de origen de un paquete de datos para hacerse pasar por un sistema autorizado y obtener acceso a una red.

**Ataque en ruta:** Ataque en el que un agente de amenaza se coloca en medio de una conexión autorizada e intercepta o altera los datos en tránsito.

**Ataque ping de la muerte:** Tipo de ataque DoS causado cuando un/a hacker hace ping a un sistema enviándole un paquete ICMP que supera los 64 KB.

**Ataque pitufo (Smurf):** Tipo de ataque de denegación de servicio en el que un/a atacante detecta la dirección IP de un usuario autorizado y la inunda con paquetes ICMP.

**Autenticación de múltiples factores (MFA):** Medida de seguridad que exige que un/a usuario/a verifique su identidad de dos o más formas para acceder a un sistema o red.

B

**Bluetooth:** Función de comunicación inalámbrica que puede ser usada para transmisión de datos de corto alcance de un dispositivo digital a otro, creada por Bluetooth Special Interest Group.

**Botnet:** Un conjunto de computadoras infectadas por software malicioso (malware) que están bajo el control de un solo agente de amenazas, conocido como “bot herder”.

C

**Computación en la nube:** Práctica de usar servidores remotos, aplicaciones y servicios de red alojados en Internet en lugar de en dispositivos físicos locales.

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

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

**Cortafuegos Stateful (gestión con estado):** Tipo de cortafuegos 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.

D

**Dirección de control de acceso al medio (MAC):** Identificador alfanumérico único que se asigna a cada dispositivo físico de una red.

**Dirección de protocolo de Internet (IP):** Cadena única de caracteres que identifica la ubicación de un dispositivo conectado a Internet.

E

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

**Enrutador (Router):** Dispositivo que conecta varias redes entre sí.

F

**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**).

**Firewall basado en la nube:** (Consultar **Cortafuegos basado en la nube**).

G

**Gestión de eventos e información de seguridad (SIEM):** Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

**Gestión de identidad y acceso (IAM):**Conjunto de procesos y tecnologías que ayuda a las organizaciones a administrar las identidades digitales en su entorno.

H

**Hardware:** Componentes físicos de una computadora.

**Host**: Toda computadora o máquina conectada a una red a través de un nombre y número de IP determinados. Proporciona recursos, información y servicios a los usuarios.

**Hub (concentrador):** Dispositivo que transmite información a todos los dispositivos de una red.

I

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

L

**Línea base de configuración:** Conjunto documentado de especificaciones dentro de un sistema que se utiliza como base para futuras compilaciones, versiones y actualizaciones.

M

**Modelo de interconexión de sistemas abiertos (OSI):** Modelo de referencia para los protocolos de la red que describe las siete capas que las computadoras utilizan para comunicarse y enviar datos a través de la misma.

**Modelo TCP/IP:** Marco que se usa para visualizar cómo se organizan y transmiten los datos a través de una red.

**Módem:** Dispositivo que conecta el enrutador (router) a Internet y proporciona acceso a Internet a la red de área local (LAN).

P

**Paquete de datos:** Unidad básica de información que se desplaza desde un dispositivo a otro dentro de una red.

**Ping:** Herramienta de la línea de comandos de prácticamente cualquier sistema operativo (por ejemplo, Windows y Linux) que posea conectividad a red. Se utiliza para probar la posibilidad de acceder a un dispositivo a través de la red. El comando Ping envía una solicitud a un dispositivo específico mediante el uso del protocolo ICMP.

**Protocolo de mensajes de control de Internet (ICMP):** Protocolo de Internet que utilizan los dispositivos para informarse mutuamente sobre los errores de transmisión de datos a través de la red.

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

**Protocolo de control de transmisión (TCP) 3-way handshake:** Proceso de tres pasos utilizado para establecer una conexión autenticada entre dos dispositivos en una red.

**Protocolo de datagramas de usuario (UDP):** Protocolo de transmisión que no establece una conexión entre dispositivos..

**Protocolo de Internet (IP):** Conjunto de estándares utilizados para enrutar y direccionar paquetes de datos a medida que viajan entre dispositivos en una red.

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

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

**Protocolo de transferencia de hipertexto (HTTP):** Protocolo de red que se utiliza para la 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 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.

**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.

**Prueba de penetración (pen test):** Ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos.

**Puerto:** Interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

R

**Rastreo activo de paquetes:** Tipo de ataque en el que los paquetes de datos se manipulan durante su tránsito.

**Rastreo de paquetes (packet sniffing):** Práctica de capturar e inspeccionar paquetes de datos a través de una red.

**Rastreo pasivo de paquetes:** Tipo de ataque en el que un agente de amenaza se conecta a un hub de red y observa todo el tráfico.

**Red:** Grupo de dispositivos conectados.

**Red de área amplia (WAN):** Red que abarca un área geográfica de gran tamaño, como una ciudad, un estado o un país.

**Red de área local (LAN):** Red que abarca un área pequeña, como un edificio de oficinas, una escuela o una vivienda.

**Red en la nube:** Conjunto de servidores o computadoras que almacenan recursos y datos en centros de datos remotos a los que se puede acceder a través de Internet.

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

**Reforzamiento de la seguridad:** Proceso de fortalecer un sistema para reducir sus vulnerabilidades y su superficie de ataque.

**Router:** (consultar **Enrutador**).

S

**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 directo (o 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.

**Sistema operativo (SO):** Interfaz entre la computadora y el/la usuario/a.

**Subnetting:** Subdivisión de una red en grupos lógicos llamados subredes.

**Switch (conmutador):** Dispositivo que establece conexiones entre dispositivos específicos en una red, enviando y recibiendo datos entre ellos.

T

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

V

**Velocidad de conexión:** Rapidez con la que un dispositivo envía y recibe datos, que se mide en bits por segundo.

Z

**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.