**Términos de glosario de la semana 2**

**Términos y definiciones del curso 6, semana 2**

**Analizador de protocolos de red (rastreador de paquetes):** Herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red..

**Archivo pcap, captura de paquetes:** Archivo que contiene paquetes de datos interceptados desde una interfaz o red.

**Ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST):** Marco para la respuesta a incidentes que consta de cuatro fases: preparación, detección y análisis; contención; erradicación y recuperación; y actividad posterior a un incidente.

**Comando y control (C2):** Servidor o computadora que utilizan los agentes de amenaza para mantener comunicaciones con los sistemas comprometidos. De esta manera, controlan los dispositivos infectados, extraen datos, entre otras acciones.

**Datos de red:** Tipo de datos que se transmiten entre los dispositivos de una red.

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

**Exfiltración de datos:** Transmisión no autorizada de datos desde un sistema.

**Indicadores de compromiso (IoC):** Evidencia observable que sugiere indicios de un posible incidente de seguridad.

**Interfaz de línea de comandos (CLI):** Interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

**Manual de estrategias:** Guía que proporciona detalles sobre cualquier acción operativa.

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

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

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

**Sistema de detección de intrusiones (IDS, por sus siglas en inglés):** Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Sudo:** Comando que otorga temporalmente permisos elevados a usuarios específicos.

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

**tcpdump:** Analizador de protocolos de red de línea de comandos.

**Tráfico de red:** Cantidad de datos que circulan por una red.

**Usuario root (usuario raíz o superusuario)**:Usuario con amplios privilegios para modificar el sistema.

**Wireshark:** Analizador de protocolos de red de código abierto.