TÉRMINOS DE SEGURIDAD DE DATOS:

ATTACK VECTORS:

Un "attack vector" (vector de ataque) es una vía o medio a través del cual un atacante puede explotar una vulnerabilidad en un sistema o red para llevar a cabo un ataque. Los vectores de ataque pueden incluir métodos como la explotación de software vulnerable, ingeniería social, malware, phishing, inyección de código, entre otros.

HACK VALUE:

El "hack value" se refiere al valor que un ataque o una acción de hacking tiene para el atacante o para la comunidad de hackers en general. Algunos ataques pueden tener un alto valor en términos de reconocimiento y notoriedad dentro de la comunidad de hacking, mientras que otros pueden tener un alto valor económico si se trata de robo de datos financieros u otra información valiosa.

TARGET:

El "target" es el objetivo de un ataque. Puede ser una entidad, sistema o recurso que un atacante intenta comprometer o dañar. Los objetivos pueden variar desde redes informáticas hasta dispositivos físicos o incluso individuos.

EXPLOIT:

Un "exploit" es un conjunto de instrucciones, código o técnica utilizada para aprovechar una vulnerabilidad en un sistema, aplicación o dispositivo con el fin de lograr algún tipo de acceso no autorizado, control o daño. Los exploits pueden ser utilizados para llevar a cabo diferentes tipos de ataques, como inyección de código, toma de control remoto, entre otros.

ZERO-DAY ATTACK:

Un "zero-day attack" es un tipo de ataque en el que un atacante aprovecha una vulnerabilidad de la que aún no se ha lanzado un parche o solución por parte del fabricante o desarrollador. El término "zero-day" se refiere al hecho de que el tiempo entre el descubrimiento de la vulnerabilidad y su explotación es cero días, lo que significa que el ataque se lanza tan pronto como se descubre la vulnerabilidad, antes de que haya una defensa disponible.

VULNERABILITY:

Una "vulnerability" (vulnerabilidad) es una debilidad o fallo en un sistema, software o hardware que podría ser explotado por un atacante para comprometer la seguridad del sistema o causar daños. Las vulnerabilidades pueden ser el resultado de errores de programación, configuraciones incorrectas o problemas de diseño.

DAISY CHAINING:

"Daisy chaining" es un término que se utiliza en el contexto de la ciberseguridad para referirse a la técnica de conectar varios dispositivos o componentes en cadena, de manera que la salida de uno se conecta a la entrada del siguiente. En el contexto de ataques, esto podría referirse a la explotación de múltiples vulnerabilidades en cadena para lograr un objetivo final, por ejemplo, explotar una serie de sistemas interconectados para acceder a un sistema objetivo.