**TEORÍA SOBRE CIBERSEGURIDAD**

**------------------------------------------- CONCEPTOS BÁSICOS ----------------------------------------------**

Seguridad Informática: Se encarga de proteger los activos relacionados con la tecnología. Información, Infraestructura y Usuarios. Preserva la confidencialidad, integridad y disponibilidad de la información.

Incidente: compromete los pilares de Confidencialidad, Integridad y Disponibilidad. Brecha: Se da cuando la empresa asume que hubo un incidente.

Seguridad de la Información: Preservación de la confidencialidad, Integridad y Disponibilidad de la Información.

• Confidencialidad: La información no puede estar disponible a personas no autorizadas a ella. • Integridad: La información debe ser precisa y debe estar completa sin haber sido modificada. • Disponibilidad: La información debe ser accesible a los usuarios que tengan autorización.

**---------------------------------------------- VULNERABILIDADES ----------------------------------------------**

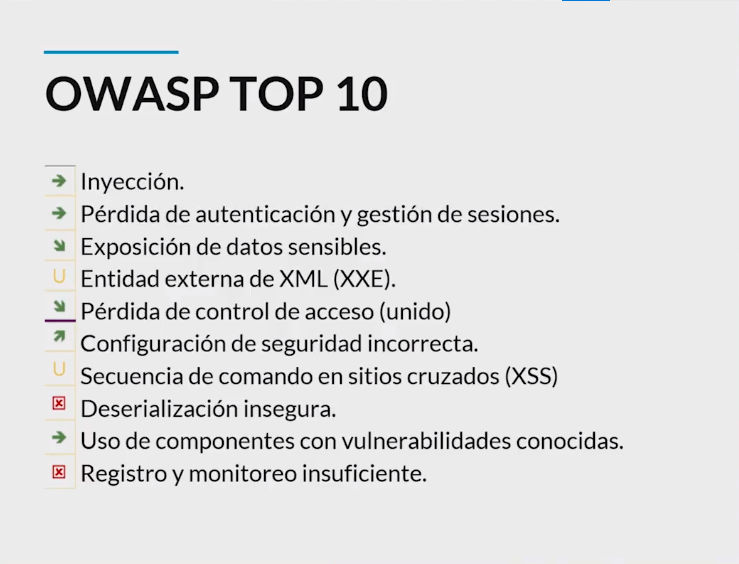
Una vulnerabilidad es un defecto o un fallo ocurrido por programación, diseño o configuración. Dicho fallo puede alterar el flujo normal del sistema y una persona mal intencionada puede realizar algo malicioso.

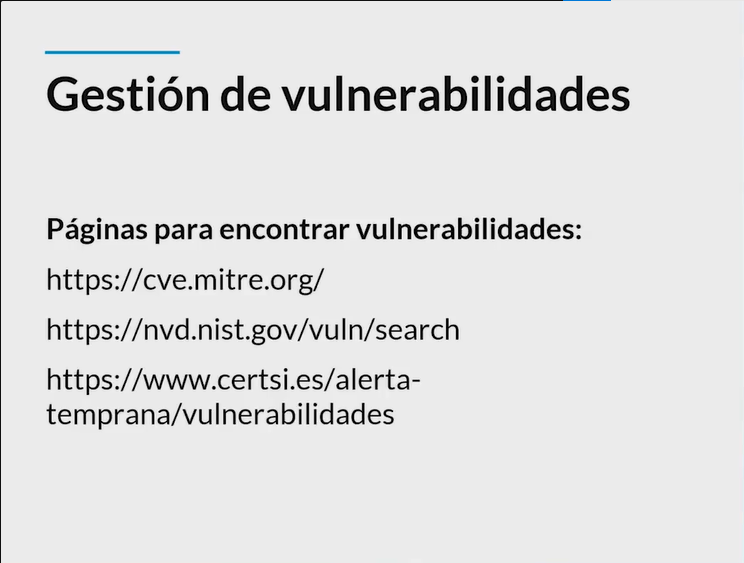
Clasificación:

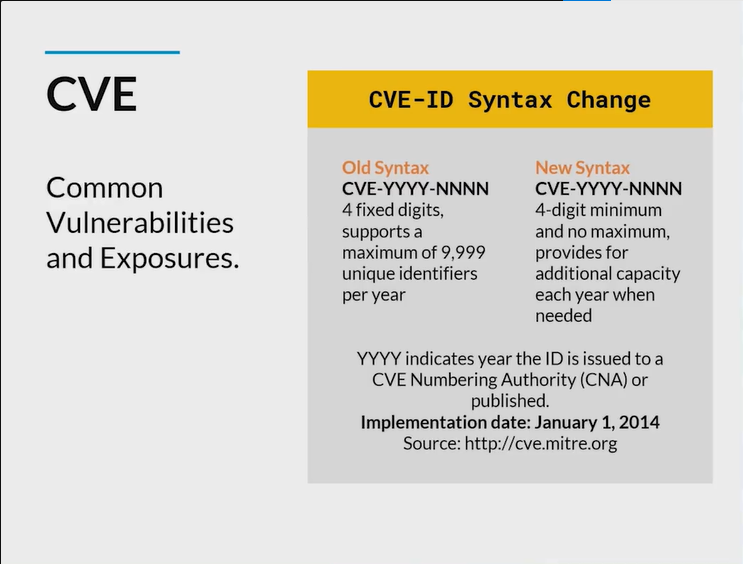
MITRE Top 25: Contiene los mayores errores de programación

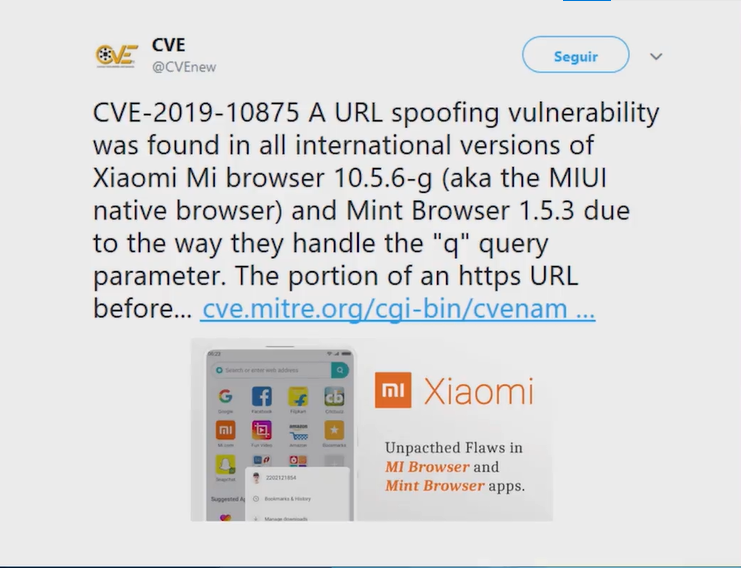
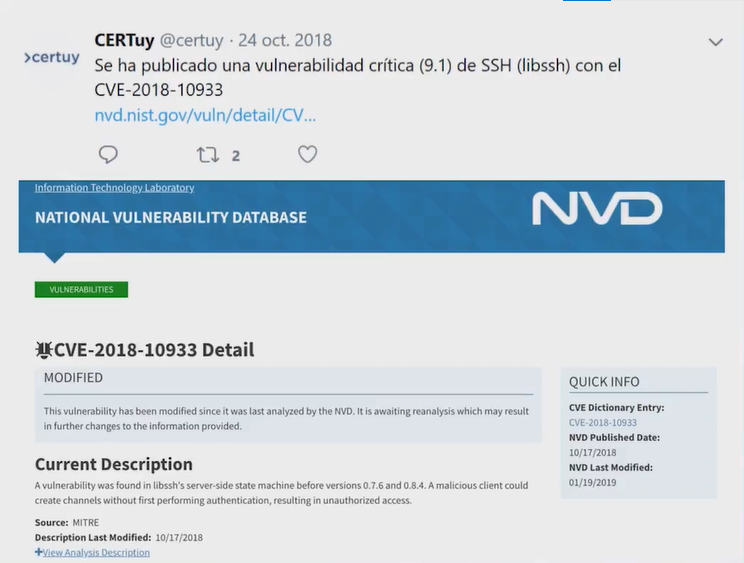
OWASP Top 10: Vulnerabilidades de seguridad más críticas en aplicaciones web.

SANS Top 20: Lista de vulnerabilidades que requiere solución inmediata.







**Ejemplos de la vida real sobre vulnerabilidades**

**--------------------------------------------- ¿QUÉ ES UNA AMENAZA? ------------------------------------------**

**Definición1:**  
Una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que pudiera explotar una vulnerabilidad. (RFC 282).

**Definición2:**  
Posible causa de un incidente no deseado, que puede resultar en daños a un sistema u organización. (ISO 27000:2009. Overviewand Vocabulary).

Existen diferentes categorías de amenazas que son:

* Red: Una red es conjuntos de dispositivos conectados por un canal de comunicación con el propósito de compartir información. Mediante este, la información viaja de un lado a otro, por lo cual un agente malicioso puede irrumpir en el mismo y robar datos sensibles.
* Host: Se dirige a un sistema particular en el que reside información valiosa en el cual los atacantes intentan violar la seguridad.
* Aplicación: Una aplicación puede ser vulnerable si no se toman las medidas de seguridad adecuadas durante el desarrollo, implementación y mantenimiento.

**Algunos conceptos clave**

* Denegación de servicio: se inhabilita un sistema sobrecargándole con peticiones y llevarlo al punto del colapso para que el servicio que presta se detenga o se reinicie.
* Inyección SQL: basados en las peticiones que puedes hacer a una base de datos SQL, un hacker se puede aprovechar para ingresar sus propios valores y usurpar credenciales de acceso, con ello podrá tener acceso a las operaciones CRUD sobre la base de datos afectada.
* Directorio transversal: Consiste en explotar una vulnerabilidad en la cual los directorios que deberían tener configurados privilegios a ciertos usuarios no los tienen y cualquier usuario puede acceder a dicha información comprometiendo el principio de confidencialidad.
* Cross-site scripting (XSS): Consiste en ejecutar códigos maliciosos en el navegador de un usuario cuando acceda a una página web o a una aplicación web. Las páginas como foros, servicios de mensajería o las que permiten insertar comentarios son más propensas a sufrir de esta vulnerabilidad.
* RAT (Remote Administration Tool): Controlar un sistema a través de conexión remota. Generalmente para esto se usa un troyano.
* Bankers o trojan-bankers: Es un troyano diseñado para robar datos bancarios.
* Botnet-Downloader: una botnet es un malware capaz de tomar control de uno o más dispositivos para ejecutar rutinas maliciosas.
* Backdoors: literalmente significa puertas traseras y son malwares diseñados para crear una entrada y permitir el acceso de un atacante al sistema.
* Proxy: Es un troyano cuya tarea es usar el dispositivo para enviar spam a través de internet.
* Keyloggers: Permite registrar los inputs de un usuario a través del teclado de un dispositivo con el fin de apoderarse de información sensible.

**¿Qué es un Ataque?**

Definición1:  
Un asalto a la seguridad del sistema, derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema (RFC 2828).

Definición2:  
Cualquier acción que comprometa la seguridad de la información de una organización (Stallings).

Motivaciones detrás de un ataque:

* Robo y manipulación de información.
* Interrumpir la continuidad del negocio.
* Daño a la reputación.
* Tomar venganza.
* Propagación de creencias religiosas o políticas.

**Tipos de ataques**

Ataques al sistema operativo: La búsqueda de fallas se realizará en lo concerniente al propio sistema base de todo el resto del software, de tal modo que, muchas veces, independientemente de lo que se encuentre por encima, se podrá explotar y tomar control del sistema en caso de que sea vulnerable.

* En los cuales se incluyen:
* Buffer Overflow.
* Bugs en el sistema operativo.
* Ataques al sistema de autenticación incorporado.
* Cracking de passwords y mecanismos de encriptación.

Ataques a las aplicaciones: En este caso, la variedad es mayor. Existen miles y miles de piezas de software y programas de todo tipo y tamaño, disponibles en el mundo. Por supuesto, entre tantos millones de líneas de código, necesariamente se producen errores.

Las aplicaciones amplían la superficie de ataque de un sistema, por lo que se recomienda siempre evitar la instalación de aquellas que no se requieran, siguiendo el principio de seguridad que sugiere el minimalismo.

Como pueden ser:

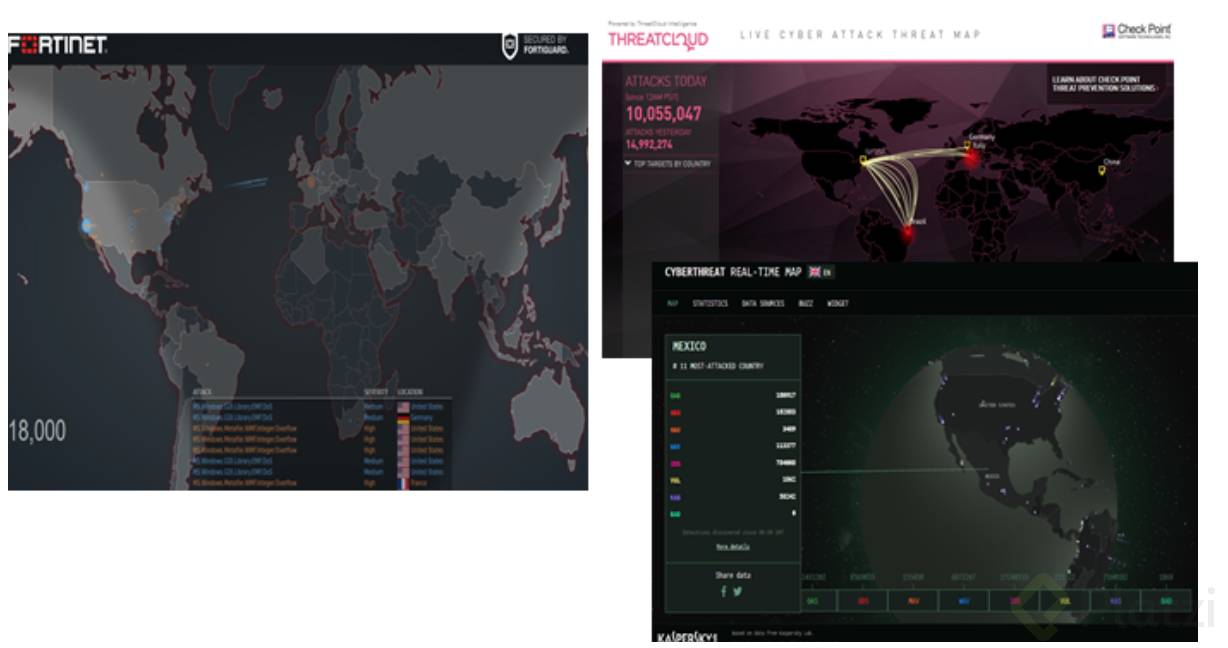
* Denegación de servicio.
* Inyección SQL.
* Directorio transversal.
* Cross-site scripting.

Errores en configuraciones: El caso de las configuraciones, ya sean del sistema operativo o de las aplicaciones, también constituye un punto sensible, dado que por más seguro que sea un software, una mala configuración puede derrumbar toda nuestra arquitectura de seguridad.

No perdamos de vista que en Internet existe una gran cantidad de sitios que presentan contraseñas por defecto de aplicaciones y dispositivos, por ejemplo, <http://cirt.net/passwords> . En este sitio podremos encontrar, clasificados por fabricante, una gran variedad de dispositivos con sus claves predefinidas.

La solución más efectiva a estos problemas, sin dudas, es el hardening. Este proceso consiste en utilizar las propias características de dispositivos, plataformas y aplicaciones para aumentar sus niveles de seguridad.

Visualizar ataques en tiempo real:  
<https://cybermap.kaspersky.com/>  
<https://www.fireeye.com/cyber-map/threat-map.html>  
<https://threatmap.fortiguard.com/>  
<https://www.akamai.com/es/es/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp>  
<http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17887&view=map>

<https://threatmap.checkpoint.com/ThreatPortal/livemap.html> ****

**¿Qué es un Malware?**

Término que describe a un archivo que pretende hacer algo dentro de una computadora, celular, Tablet… sin el consentimiento del usuario legítimo.

Existen familias de malware como son: Gusanos, Virus, Ransomware, Spam, Hoax, Scam entre otros.

Se les denomina “Familias” porque se generan a partir de un virus mutado, esto hace referencia a que es el mismo virus que se usó anteriormente pero con algunas modificaciones para complicar la detección por los antivirus.

Virus: El principal funcionamiento de los virus, es crear un daño a la computadora infectada.

La diferencia de estos a otras amenazas, es que la mayor parte de su código se origina en un archivo llamado huésped, de este modo, cada vez que el archivo es ejecutado, primero se ejecuta el archivo y en segunda parte se ejecuta el virus.

Worms: Los gusanos a diferencia de los virus, no necesitan un huésped para permanecer infectado la computadora, su método de ataque es por medio de la red, medios extraíbles, redes sociales, redes p2p, etc. Su objetivo es ir infectando computadoras a su paso, destruir, copiar, mover, o hasta filtrar información de las computadoras por donde pasa.

Troyanos: Son programas maliciosos que proporcionan una conexión directa con la víctima, su principal objetivo es la sustracción de información.

Existen varios tipos de este malware, nombrados por su forma de operar:

* RAT (Remote Administration Tool)
* Banker
* Botnet-Downloader
* Backdoors
* Proxy
* Keyloggers

Ransomware: El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados.

Para tener en cuenta: Cyber Kill Chain  
Los siete pasos de Cyber ​​Kill Chain® mejoran la visibilidad de un ataque y enriquecen la comprensión de un analista de las tácticas, técnicas y procedimientos de un adversario**.**

**Las siete fases de la Kill Chain son:  
**

* Reconocimiento: Conocer y aprender del objetivo utilizando diversas técnicas.
* Creación del arma: Desarrollo o adecuación del código al medio sobre el que se buscará la infección.
* Entrega: La transmisión del código malicioso a través de algún medio como email, web, usb, etc.
* Explotación: Aprovechamiento de alguna vulnerabilidad en el software o hardware o error humano para ejecutar el software malicioso.
* Instalación: El software malicioso se asegura de poder ejecutarse de forma permanente en el equipo infectado.
* Comandos & Control (C2): El código malicioso se comunica a una sede central, proporcionando a los atacantes acceso remoto.
* Exfiltración: En este punto se lleva a cabo el robo de información o el verdadero objetivo del ataque.

Más información: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>