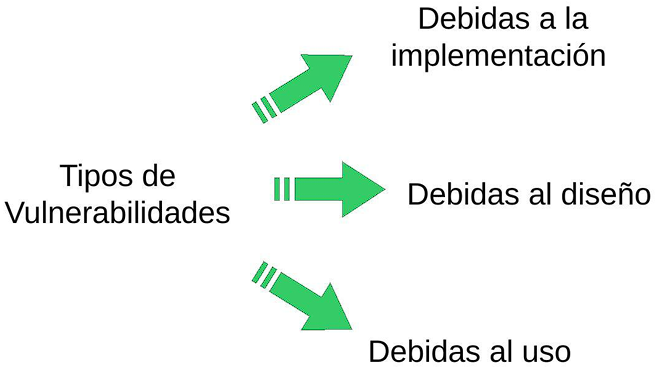
Unidad 2 – ULTRA RESUMEN

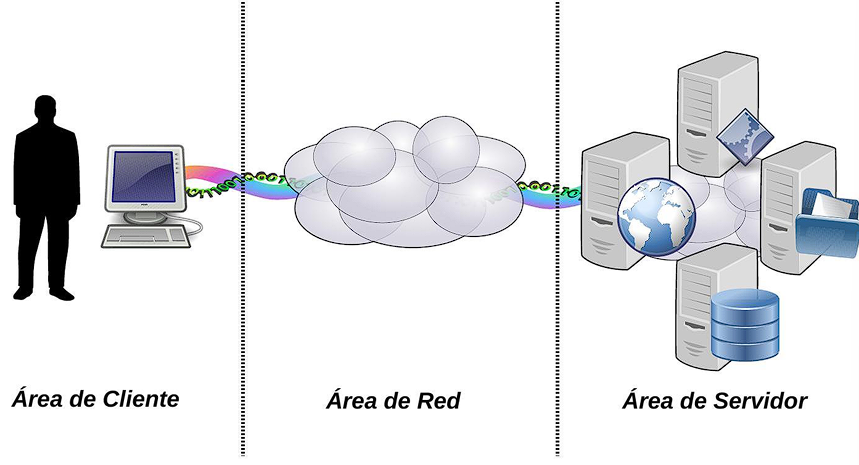
**DAÑO;** Prejuicio que se produce cuando un sistema informático falla. Dicho prejuicio debe ser cuantificable.

**RIESGO;** Producto entre la magnitud de un daño, y a la probabilidad de que este tenga lugar.

**AMENAZA;** Situación de daño cuyo riesgo de producirse es significativo

**VULNERABILIDAD**; Deficiencia en un sistema susceptible de producir un fallo en el mismo

**EXPLOIT;** Cualquier técnica que permita aprovechar una vulnerabilidad de un sistema para producir un daño en el mismo.



**LA NUBE**

*Ventajas*

* Facilidad de acceso a la información desde diferentes ubicaciones y dispositivos
* Infraestructura flexible y escalable basada en servicios
* Reducción de costos por infraestructura y servicios
* Centralización de administración y gestión de datos

*Desventajas*

* Dependencia en la infraestructura y servicios externos
* Dependencia en servicios de comunicación externos para acceder a los sistemas y datos propios
* Pérdida del control de la seguridad de la información.

Ataques a aplicación conocidas

* *Common Vulnerabilities and Exposures* o *CVE* es un código asignado a una vulnerabilidad que le permite ser identificada de forma univoca. <https://cve.mitre.org/>
* *Common Weakness Enumeration* o *CWE* es una lista de tipos de debilidades de software y hardware, las mismas se encuentran clasificadas y con identificadores del tipo CWE – numero.

<https://cwe.mitre.org/>

* *NVD, National Vulnerability Database*, del *NIST* es el repositorio del gobierno de EEUU para la gestión de datos de vulnerabilidades basados en los estándares.

<http://nvd.nist.gov/home.cfm>

* *CVSS, Common Vulnerability Scoring System*, es un conjunto de estándares abiertos para asignar un valor o puntaje de severidad a una vulnerabilidad. Este puntaje va desde 0.0 a 10.0, siendo este último el de mayor severidad.

Prevencion de vulnerabilidades

* Listas bugtraq
* Sistrmas automáticos de análisis
  + DATS; scanners de vulnerabilidades
  + SAST; auditoria automática de código
  + IAST; detectan vulnerabilidades en tiempo real durante la ejecución de una aplicación.
  + Redes trampa

**CERT; Computer Emergency Response Team**

**CSIRT; Centro de respuesta a incidentes de seguridad informática**

Son equipos reconocidos por la dirección de su organización como responsables de gestionar indicentes de seguridad informática que le competen según su alcance y comunidad.

Interactúan entre si a fin de facilitar información oportuna para actuar frente a diferentes tipos de incidentes, determinar su impacto, alcance y naturaleza.

Funciones;

* Ayudar al publico objetivo a atenuar y prevenir incidentes graves de seguridad
* Ayudar a proteger informaciones valiosas
* Coordinar de forma centralizada la seguridad de la información
* Guardar evidencias, por si hubiera que recurrir a pleitos.
* Apoyar y prestar asistencia a usuarios para recuperarse de las consecuencias de los incidentes de seguridad
* Dirigir de forma centralizada la respuesta a los incidentes de seguridad.

**DOS – DENEGACION DE SERVICIO**

Ataque a un sistema que causa que un servicio sea inaccesible a los usuarios. Provoca la perdida de la conectividad de la red por el consumo del ancho de banda de la red de la victima o sobrecarga de los recursos computacionales del sistema de la víctima.

*Tipos:*

Volume-based DDoS attacks: El atacante inunda a la víctima con un gran volumen de paquetes o conexiones de red, sobrecargando el equipamiento de la red servidores o ancho de banda.

Application DDoS attacks: El atacante opera a nivel de aplicación usualmente por HTTP intentando saturar el servidor y/o un servicio que este presta.

Low-rate DOS (LDoS) attacks: El atacante utiliza una vulnerabilidad en el diseño o implementación de la aplicación.

**FLOODING**

La técnica de Flooding o Inundación busca generar solicitudes maliciosas a un servicio con la finalidad de hacer que el mismo se sature o entre en un modo de espera, de esta forma anula o limita su funcionamiento.

**BOTNET**

Conjunto de terminales que ejecutan software que permite su control total o parcial desde ubicaciones remotas

**SNIFFERS**

Programa de captura de las tramas de red, se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

Para redes Ethernet (LAN); Ethereal, WinPcap, Ettercap, RCPDump, WinDump, WinSniffer, Hunt, Darkstat, Traffic-vis.

Redes inalámbricas (wireless); Kismet, Network, Stumbler.

Atacando a navegadores;

*Tampering o Data Diddling:*

Se refiere a la modificación no autorizada de la información. Por ejemplo, múltiples sitios web han sido afectados al detectar cambios en el contenido de sus páginas.

*Ataques Mediante JavaScript:*

JavaScript es un lenguaje de programación usado por los diseñadores de sitios web. Este tipo de programas son utilizados para explotar fallas de seguridad de navegadores web y servidores de correo.

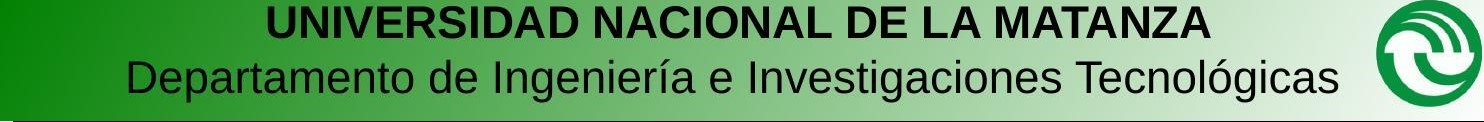
Ataques drive-by download

Infectan de forma masiva a los usuarios, simplemente ingresando a un sitio web determinado. Mediante esta técnica, los desarrolladores de malware

*Hijackers:*

Son programas que alteran el funcionamiento o configuración del cliente para que el atacante pueda "secuestrar" información de interés Ejemplo, Page hijacking, Session hijacking, Browser hijacking...

*Rootkits:*

Son programas que permiten que una aplicación maliciosa permanesca oculta en el sistema operativo o que la misma no pueda ser eliminada normalmente. Ejemplo, procesos fantasmas en paralelo.

*Backdoors:*

Son programas que habilitan un acceso alternativo al sistema permitiendo evitar el método de autenticación principal. Normalmente se instalan en los sistemas comprometidos para facilitar su posterior uso (local o remoto) por parte del atacante.

*Stealers:*

Son programas que acceden a la información almacenada en el equipo para facilitársela al atacante. Su principal objetivo son contraseñas almacenadas o recordadas en navegadores y clientes de email o mensajería

*Keyloggers:*

Son programas o dispositivos físicos que registran la actividad de los dispositivos de entrada, comúnmente el teclado.

*Ransomware:*

Son programas que retienen el control del equipo o cifran información almacenada en el mismo para que no pueda ser accedida, en muchos casos solicitan un pago para que sean desactivados. Algunos ejemplos son "Virus Ukash", "WannaCry", "Petya/NotPetya", "Cryptolocker" y "Cryptowall".