Bloque 2.- Amenzas, vulnerabilidades y ataques.

Amenazas

Tabla de contenidos

- **Amenazas**
- **Vulnerabilidades**
- **Ciberataques**

Tabla de contenidos

Amenazas

- **Amenaza**
  - Una amenaza es una potencial violación de la seguridad que existe cuando hay una circunstancia, capacidad, acción o evento que podría ser una brecha de seguridad y causar daño.
  - *Fuente de amenaza:*
    - Adversaria: individuos, grupos, organizaciones o entidades que buscan explotar alguna debilidad del sistema.
    - No adversarias se refieren a desastres naturales o acciones erróneas realizadas por individuos en el curso de la ejecución de sus responsabilidades diarias.

Amenazas

- **Ejemplos de amenazas “adversarias”**
  - Fraude o robo de información (insiders o outsiders). Técnicas:
    - Medios sociales (facebook, Twitter, …): fake, cuentas no verificadas, … para enviar links maliciosos que conducen a ataques de ingeniería social.
    - Ingeniería Social: tfno, phishing, smishing,
    - APT (Advanced Persistent Threat – Amenzas avanzadas persistentes): intrusiones a largo plazo para obtener acceso a datos e información. Persistentes en el tiempo y monitorizados para no ser detectados y extraer información durante un largo periodo de tiempo.

Amenazas

- **Ejemplos de amenazas “adversarias”**
  - Insiders (amenazas internas): normalmente empleados. Puede ser sabotaje, soborno, ... Puede causar más daño por “la confianza”.
  - Hacker malicioso (visto anteriormente)
  - Código malicioso – malware (visto anteriormente)

Amenazas

- **Ejemplos de amenazas “no adversarias”**
  - Errores u omisiones: causadas de forma inadvertida por operadores del sistema que procesan cientos de transacciones o usuarios que crean y editan cientos de datos. Pueden degradar la integridad de los datos y del sistema. Pueden causar amenazas (si el error “rompe” el sistema”) o vulnerabilidades (si el error permite crear una amenaza al ser descubierto).
  - Pérdida de apoyo físico de de infraestructura: pérdida de energía, perdida de comunicaciones, cortes o fugas de agua, averías, inundaciones, … también disturbios o huelgas. Dan lugar a tiempo de inactividad del sistema o no funcionamiento normal del sistema.

Amenazas

- **Ejemplos de amenazas “no adversarias”**
  - Impacto de privacidad personal e intercambio de información: acumulación de grandes cantidades de **información identificable** por organizaciones gubernamentales y privadas y las posibles **brechas de seguridad**. **Intercambio de información privada de forma voluntaria** a través de medios sociales.

Tabla de contenidos

- **Amenazas**
- **Vulnerabilidades**
- **Ciberataques**

Vulnerabilidades

- **Vulnerabilidad**
  - Una vulnerabilidad es una **debilidad** en un sistema, procedimiento de seguridad del sistema, controles internos o implementación que podría ser **explotada por una fuente de amenaza**.
    - Las vulnerabilidades dejan a los sistemas **susceptibles** a una multitud de actividades que pueden resultar en **pérdidas significativas y a veces irreversibles** para un individuo, grupo u organización. Estas pérdidas pueden ir desde un único archivo dañado en un ordenador portátil o en un dispositivo móvil hasta bases de datos enteras en un centro de operaciones comprometidas.
    - Con las herramientas y los conocimientos adecuados, un adversario puede **explotar las vulnerabilidades** del sistema y obtener acceso a la información almacenada en ellos.
    - Los **daños** infligidos a los sistemas comprometidos pueden variar en **función de la fuente de la amenaza.**

Vulnerabilidades

- **Vulnerabilidad**
  - Años 70 y 80: encontrar fallos de seguridad (bugs): “penetrate-and-patch”
  - A partir de 2000: mejora gestión del ciclo de parches. Un enfoque moderno de leyes de divulgación de violaciones de seguridad, CERTs y divulgación responsable.
  - El ciclo para descubrir vulnerabilidades consiste en que alguien (investigador) descubre una vulnerabilidad en un sistema mantenido por un proveedor.
    - El investigador puede ser un cliente, un académico, un trabajador para una agencia de inteligencia o un delincuente.
    - La vulnerabilidad puede ser vendida para su explotación en el mercado delincuente, o anunciada al proveedor para que sea solucionada. (posible recompensa con “bug bounty program” - ver facebook o similares)

Vulnerabilidades

- **Vulnerabilidad**
  - Tipos:

    Zero-day

    - Hardware:
      - RAM
      - Firmware
      - USB
      - BIOS
      - ...

Vulnerabilidades

- **Vulnerabilidad**
  - Tipos:
    - Software:
      - Desbordamiento de buffer
      - Condición de carrera
      - Formatos de cadena
      - XSS (Cross Site Scripting – VBScript – JavaScript
      - Inyección SQL
      - Denegación de servicio
      - Ventanas engañosas

Vulnerabilidades

- **Vulnerabilidad**
  - **CERT** (Computer Emergency Response Team – Equipo de Respuesta ante Emergencias Informáticas - EEUU) / **CSIRT** (Computer Security Incident Response Team – Equipo de Respuesta ante Incidencias de Seguridad Informática - Europa): estudia el **estado de seguridad global de redes y ordenadores** y proporciona servicios de **respuesta ante incidentes a víctimas de ataques** en la red, **publica alertas** relativas a **amenazas y vulnerabilidades** y ofrece información que mejora la seguridad de estos sistemas.

    (https://www.incibe-cert.es)

Vulnerabilidades

- **Vulnerabilidad**
  - **CERT** (Computer Emergency Response Team – Equipo de Respuesta ante Emergencias Informáticas - EEUU) / **CSIRT** (Computer Security Incident Response Team – Equipo de Respuesta ante Incidencias de Seguridad Informática - Europa): estudia el **estado de seguridad global de redes y ordenadores** y proporciona servicios de **respuesta ante incidentes a víctimas de ataques** en la red, **publica alertas** relativas a **amenazas y vulnerabilidades** y ofrece información que mejora la seguridad de estos sistemas.

    (https://www.incibe-cert.es)
  - SOC (Security Operations Center - Centro de Operaciones de Seguridad): es una empresa/organismo de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

Vulnerabilidades

- **Vulnerabilidad**
  - **NVD** (National Vulnerability Database): depósito del gobierno de los EEUU de datos de gestión de vulnerabilidades basados en estándares. Estos datos permiten la automatización de la gestión de vulnerabilidades, la medición de la seguridad y el cumplimiento de las normas. El NVD incluye bases de datos de referencias de listas de comprobación de seguridad, fallos de software relacionados con la seguridad, desconfiguraciones, nombres de productos y métricas de impacto.

    (https://nvd.nist.gov/ - https://www.incibe-cert.es/alerta-temprana/vulnerabilidades)
  - **CVE** (Common Vulnerabitlities and Exposures): proporciona un método de referencia para las vulnerabilidades y exposiciones de seguridad de la información conocidas públicamente. Es operado por MITRE (https://cve.mitre.org/) la cual es es una organización estadounidense sin ánimo de lucro con doble sede en Bedford (Massachusetts), y McLean (Virginia).

Tabla de contenidos

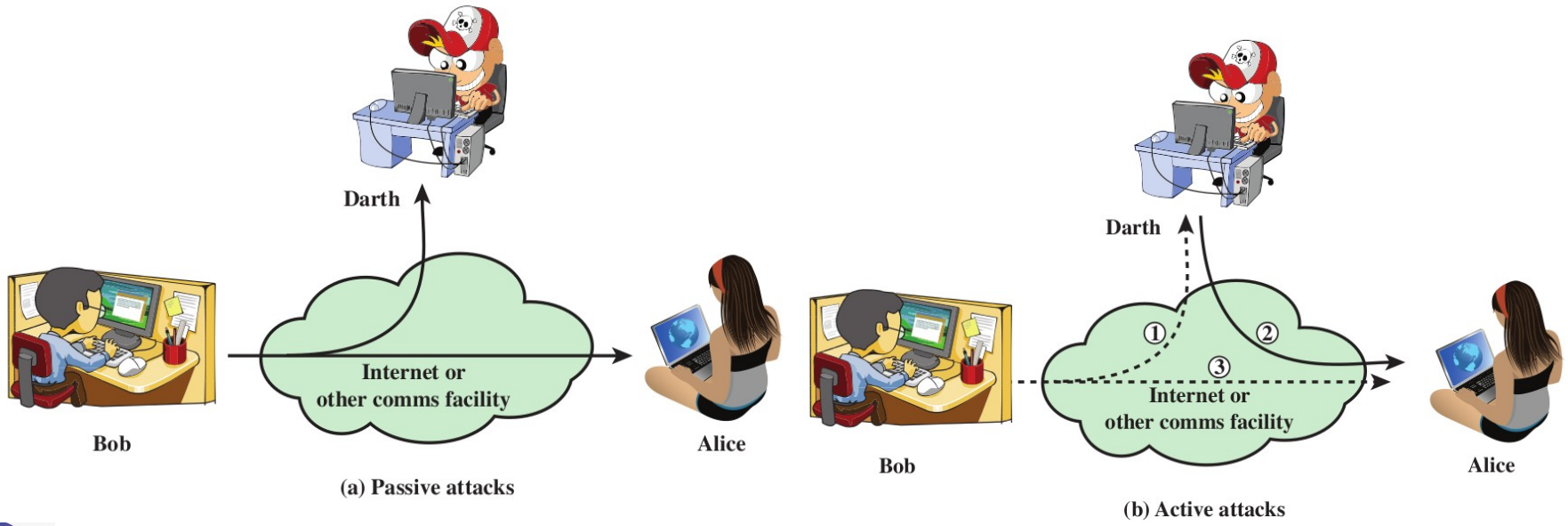
- **Amenazas**
- **Vulnerabilidades**
- **Ciberataques**

Ciberataques

- **Ataque informático - ciberataque:**
  - Intento deliberado para evadir los servicios de seguridad y violar la política de seguridad de un sistema.
  - Intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo.
  - Cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo de tomar el control, desestabilizar o dañar un sistema informático (ordenador, red privada, etcétera).

Ciberataques

- **Tipos :**
  - **Pasivo:** Intenta aprender o hacer uso de la información de un sistema pero sin afectar a los recursos
  - **Activo**: Intenta alterar los recursos del sistema o afectar a sus operaciones.



Ciberataques

- **Tipos:**
  - **Ataque de intercepción pasiva (eavesdropping)**

    Esto sucede cuando un hacker captura y "escucha" el tráfico de red. Este ataque también se conoce como sniffing o snooping.
  - **Ataque de Modificación de Datos**

    Si los hackers han obtenido tráfico de la empresa, pueden alterar los datos en el paquete sin el conocimiento del remitente o del receptor.
  - **Ataque de suplantación de dirección IP**

    Un atacante crea un paquete IP que parece provenir de una dirección válida dentro de la intranet corporativa.
  - **Ataques basados en contraseñas**

    Si los harckers descubren una cuenta válida de usuario, los hackers tienen los mismos derechos que el usuario real. Los hackers pueden usar una cuenta válida para obtener listas de otros usuarios, información de red, cambios de servidor y configuraciones de red, y modificar, redirigir o borrar datos.
  - **Ataques de Ingeniería Social**

    Usuario es el eslabón más débil (pretexting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, dumpster diving)

Ciberataques

- **Tipos:**
  - **Ataque de Denegación de Servicio (DoS)**

    Un ataque de DoS impide el uso normal de una computadora o red por parte de usuarios válidos. Un ataque de DoS también puede saturar una computadora o toda la red con tráfico hasta que se apaguen por sobrecarga. Un ataque de DoS también puede bloquear tráfico; eso deriva en la pérdida de acceso a recursos de red por parte de usuarios autorizados.
  - **Ataque man-in-the-middle**

    Este ataque se produce cuando los hackers se colocan entre un origen y un destino. Entonces ahora pueden monitorear, capturar y controlar la comunicación en forma activa y transparente.
  - **Ataque de Claves Comprometidas**

    Si un atacante obtiene una clave secreta, esa clave se conoce como una clave de riesgo. Una clave comprometida puede utilizarse para obtener acceso a una comunicación asegurada sin que el emisor ni el receptor se enteren del ataque. (Ej. Wifi)
  - **Ataque de analizador de protocolos**

    Un analizador de protocolos es una aplicación o un dispositivo que puede leer, monitorear y capturar intercambios de datos en la red y leer paquetes de red. Si los paquetes no están cifrados, un analizador de protocolos permite ver por completo los datos que los componen. (Ej: CDP)

Ataques de Ingeniería Social

- La ingeniería social es un ataque de acceso que intenta manipular a las personas para que realicen acciones o divulguen información confidencial. Tipos:
  - **Pretexto:** Un atacante finge necesitar datos personales o financieros para confirmar la identidad del destinatario.
  - **Suplantación de identidad (phishing)**: El atacante envía un mensaje fraudulento que parece ser de una fuente legítima y confiable, para hacer que el destinatario instale malware en su dispositivo o revele información personal o financiera.
  - **Suplantación de identidad focalizada (spear phishing)**: El atacante crea un ataque de suplantación de identidad (phishing) dirigido específicamente a una persona u organización.
  - **Correo electrónico no deseado (spam)**: También conocido como correo basura, es correo electrónico no solicitado que suele contener enlaces nocivos, malware o información engañosa.
  - **Algo por algo (something for something)**: A veces se denomina "quid pro quo" y es cuando el atacante solicita información personal a cambio de algo como un obsequio.
  - **Carnada (Baiting)**: Un atacante deja deliveradamente una unidad flash infectada con malware en un sitio público. Una víctima encuentra la unidad, la coloca en su equipo portátil y sin darse cuenta instala malware.
  - **Simulación de identidad (Impersonation)**: Este tipo de ataque es donde un atacante finge ser alguien más para ganarse la confianza de la víctima.
  - **Infiltración (tailgating)**: Es un tipo de ataque presencial en el cual el atacante sigue muy de cerca a una persona autorizada para poder acceder a un área protegida.
  - **Espiar por encima del hombro (shoulder surfing)**: Es un tipo de ataque presencial en el cual el atacante mira con disimulo sobre el hombro de una persona para robar sus contraseñas u otra información.
  - **Inspección de basura (Dumpster diving)**: Tipo de ataque presencial en el cual el atacante hurga en la basura en busca de documentos confidenciales

Ataques de Ingeniería Social

- Prácticas recomendadas

Amenzas, vulnerabilidades y ataques