TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1 – UNIDAD 2

Universidad Tecnológica de Pereira | faceIT

Lección 2: Ciberataques

Son esfuerzos intencionales para robar, exponer o alterar información. Incluyen los intentos de destrucción de datos, destrucción de aplicaciones y accesos no autorizados a sistemas o dispositivos.

Pueden ocurrir por varios actores como son:
Atacantes con intenciones delictivas que buscan robar información y venderla para su beneficio económico. Por ejemplo, el robo de credenciales bancarias para transferir fondos a sus propias cuentas, o estafas para que personas les envíen dinero manipuladas por los datos que el atacante muestra conocer.

Extorsionistas que buscan robar grandes cantidades de datos valiosos para cobrar un rescate a cambio de la información. Por ejemplo, cifrar datos de un hospital para que la entidad pague a cambio de liberar todas las imágenes diagnósticas con las que se han llevado casos de pacientes durante los últimos años. En este caso es información muy complicada de reconstruir y el atacante tiene altas probabilidades de recibir el dinero de la extorsión.

Atacantes activistas políticos: Son atacantes asociados a ciberterrorismo y conflictos entre naciones. Un caso conocido lo reportó BBC el 10 de mayo de 2021 (EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país - BBC News Mundo) en donde atacantes robaron más de 100 gb de datos de los oleoductos nacionales. Esta red distribuye el 45% del suministro del Diesel y gasolina necesaria para los aviones de muchas ciudades importantes.

El ataque implicó el apagón de redes en 18 estados y el alza en precios por el desabastecimiento.

Otros ataques se dan por espionaje corporativo, con la intención de robar bases de datos valiosas, o incluso con empleados que tienen acceso a una red corporativa y están descontentos por el trato que reciben.

También se tienen casos de amenazas internas, como empleados con accesos y privilegios en una red, los cuales deliberadamente o accidentalmente exponen información.

Algunas técnicas comunes de ciber ataque son:

Malware: La palabra malware significa software malicioso. Son programas diseñados para dañar datos, exponer accesos y, en general, tomar el control de redes o dispositivos. Al tener el control, es fácil para un atacante borrar datos, eliminar archivos críticos para el funcionamiento de un sistema, desconfigurar redes y equipos, e incluso, utilizar la capacidad de cómputo de un dispositivo para fines ilícitos. Dentro del malware se clasifican amenazas como:

Caballos de troya: Son programas que se disfrazan como utilidades (por ejemplo, programas para descargar videos de youtube, o para ver quien te sigue en redes sociales) y engañan a los usuarios para que los instalen. Una vez instalados pueden instalar más programas y crear brechas de seguridad.

Ransomware: Es sofware diseñado para cifrar la información de un computador. Este cifrado utiliza algoritmos avanzados de codificación. Al cifrar los datos, los delincuentes exigen pagos a cambio de la clave de cifrado y restaurar la funcionalidad de los equipos, promesa que muchas veces incumplen luego de recibir el pago, dejando a la víctima sin dinero y sin datos. Si se quisieran intentar claves, un computador moderno tardaría más de 1500 años en encontrar la clave correcta por la complejidad del cifrado, lo que significa que deja los datos inutilizables. Como ejemplos notorios está el caso de WannaCry en 2017 que afectó hospitales y gobiernos. NotPetya en 2017, y StuxNet en 2010, que intentó sabotear instalaciones nucleares en irán alterando el funcionamiento de centrifugadoras industriales para que explotasen.

Scareware: Software con mensajes falsos para que una víctima se asuste y descargue un programa malicioso (ransomware) También se usan para robar datos. Por ejemplo, páginas que, sin analizar un computador, lanzan alertas de que tiene un virus y llevan al usuario con engaños a descargar programas para librarse de ese virus.

Spyware: Son programas que permanecen ocultos en el computador y recopilan información confidencial sin que los usuarios se den cuenta. Por ejemplo, hay programas como los keyloggers que envían a internet todo lo que un usuario escribe en su teclado, facilitando el robo de usuarios, contraseñas e información sin codificar, fácil de leer por atacantes.

Rootkits: Son programas que permiten a atacantes hacerse pasar por el administrador de un sistema. Con esos permisos, les es fácil instalar otros programas, controlar computadores y realizar robos de información. Suelen venir incluidos en programas como por ejemplo, aquellos que evitan pagar licencias de Windows o de office y que personas o empresas emplean por desconocimiento de las fallas en la seguridad que implica.

Gusanos: Es software con la capacidad de replicarse en la memoria y en otros dispositivos en una red. Al copiarse a otros dispositivos puede tener robos extensos de información.

Sniffers: Son programas de interceptación. Estos programas pueden analizar una red produciendo un mensaje conocido como broadcast. Este mensaje llega a todos los equipos conectados a una misma red. Por ejemplo, un mensaje puede ser “enviame tu dirección IP”, así, fácilmente se pueden identificar todos los equipos conectados a una red y luego capturar todos los mensajes cuyo destino es el equipo al cual interesa atacar. No importa si el equipo está por red cableada o por WiFi, el mensaje llegará y se podría leer información sin cifrar. Los atacantes lo emplean para identificar contraseñas, números de tarjetas de crédito y en general, mensajes que tengan información valiosa para ser explotada.

Man in the middle: Este ataque consiste en que un atacante manipula una red (conectándose sin autorización) para instalar programas de interceptación de datos. Esto le permite al atacante conseguir y redirigir todos los paquetes salientes de un computador y luego falsificar las respuestas haciéndose pasar por el servidor. De esta forma roban usuarios, claves, e información confidencial. A menudo sucede aprovechándose de errores de escritura. Por ejemplo, un atacante puede comprar el dominio gmal.com (sin una i, mal escrito, en vez de gmail) y allí colocar un sitio web exactamente igual al legítimo. Un usuario desprevenido puede no notar el error en la escritura de la dirección y exponer fácilmente tanto su usuario como sus contraseñas para acceder a sus servicios.

Ataques en redes públicas: En ocasiones requerimos conectarnos a internet desde un aeropuerto, un hotel, un centro comercial, entre otros, que tienen redes públicas de WiFi. En general, estas redes no tienen buena seguridad de la información, con lo que atacantes pueden fácilmente entrar y aplicar ataques de sniffers y del tipo man in the middle. Incluso, se han registrado casos en donde los atacantes crean redes gratuitas con nombres similares a redes legítimas y así interceptan datos.

Denegación de servicio: estos ataques se realizan sobrecargando un sistema. Es decir, se intenta pasar tráfico fraudulento por un servidor, que intenta determinar si debe contestar o no a las solicitudes de información. Cuando los ataques son desde muchos dispositivos constantemente, los servidores suelen emplear toda su CPU abrumando el sistema y evitando que este responda a solicitudes legítimas. De esta forma se reduce la capacidad de un sistema en hacer sus funciones. Estos ataques suelen distribuirse, es decir, utilizar muchos computadores o celulares infectados que hagan solicitudes constantemente a u mismo servidor.

Compromiso de cuentas

Ocurre cuando un atacante toma el control de la cuenta de un usuario legítimo. Los hackers pueden lograr esto mediante:

- **Phishing:** Envían correos o mensajes engañosos para robar contraseñas.
- **Bases de datos robadas:** Compran contraseñas filtradas en la web oscura.
- **Ataques de fuerza bruta:** Usan herramientas como Hashcat para probar combinaciones de contraseñas automáticamente hasta encontrar la correcta.

Ataques de intermediario (MiTM)

En este tipo de ataque, un hacker se infiltra entre dos partes que están comunicándose, como un usuario y un servidor, sin que se den cuenta. Esto suele ocurrir en redes Wi-Fi públicas no seguras. Los atacantes pueden:

- Leer o modificar correos electrónicos.
- Secuestrar sesiones de usuarios al hacerse pasar por ellos.
- Acceder a datos confidenciales o sistemas sensibles.

Ataques a la cadena de suministro

Aquí, los hackers no atacan directamente a la víctima, sino a sus proveedores, ya que estos suelen tener acceso a las redes de la empresa.

- Ejemplo real: En 2020, hackers rusos atacaron SolarWinds y distribuyeron malware disfrazado de actualización. Esto permitió el acceso a datos confidenciales de agencias del gobierno de EE. UU., como el Departamento del Tesoro y Justicia.

1. **Script entre sitios (XSS)**
   - Insertan código malicioso en páginas web legítimas.
   - Este código puede robar datos del usuario o redirigirlo a sitios falsos.
   - Suele usarse JavaScript para este tipo de ataque.
2. **Inyección SQL**
   - Los hackers envían comandos maliciosos a bases de datos a través de campos como formularios de búsqueda o login.
   - Pueden extraer información como números de tarjetas de crédito o datos personales.
3. **Túnel DNS**
   - Esconden tráfico malicioso en las solicitudes DNS.
   - Esto permite eludir firewalls y robar datos o comunicar malware con sus controladores.
4. **Exploits de día cero**
   - Se aprovechan de fallos desconocidos o no reparados en software.
   - Los atacantes usan estas vulnerabilidades antes de que las empresas puedan solucionarlas.

5.Ataques sin archivos

- Inyectan código malicioso directamente en la memoria del equipo, sin usar archivos que puedan ser detectados.
- A menudo usan herramientas como PowerShell para robar datos o alterar configuraciones.

6.Suplantación de DNS

- Alteran registros DNS para redirigir a los usuarios a sitios falsos.
- Las víctimas creen estar en un sitio legítimo, pero terminan entregando datos sensibles o descargando malware.

Ingeniería social: Son técnicas utilizadas sobre sistemas seguros para convencer o engañar a personas que tienen un acceso legítimo de que creen accesos inseguros. Se basan en el engaño a personas y en la manipulación para que crean que deben actuar en contra de los protocolos de seguridad por motivos importantes, por ejemplo, un atacante se puede hacer pasar por el jefe de una compañía y pedir claves de acceso o dar órdenes a empleados de hacer cosas que comprometan la seguridad de una empresa.