**Ataques informáticos**

Un ataque informático consiste en aprovechar una vulnerabilidad de un software, hardware o de las personas empleando la ingeniería social.

Un ataque informático debe seguir unas pautas:

* Reconocimiento: Obtiene información de la víctima.
* Escaneo: Escaneo de puertos, nombres de host, ips, contraseñas, etc.
* Obtener acceso: Explotas las vulnerabilidades detectadas para entrar al sistema.
* Mantener acceso: Se coloca una puerta trasera para poder entrar en cualquier momento.
* Borrar huellas: Una vez entrado hay que borrar huellas, tales como el log o alarme de intrusos.

Un sistema de seguridad consta de tres elementos que son confidencialidad, integridad y disponibilidad, un atacante intentará explotar uno de estos tres elementos para entrar.

Las vulnerabilidades que se explotan normalmente son:

* Ingeniería social: Consiste en obtener la información de un usuario cercano al sistema. Dicha persona ya sea por negligencia o ignorancia puede permitir el acceso a un atacante. Para evitar esto la única contramedida es la educación, de este modo se evitar que sean engañados.
* Factor Insiders: La mayor parte de los ataques a empresas vienen desde el interior, ya sea por un empleado descontento o por un atacante que consiguió un empleo en la empresa y obtuvo permisos. Las contramedidas consisten en monitores de los ordenadores, deshabilitar USB, poner antivirus, proxy y políticas de Active Directory.
* Códigos maliociosos: El 80% de los ataques por código es mediante troyanos. Los troyanos entran al sistema a través de correo, usb, descargas, etc. Cuando entran activan su código y pueden funcionar como keylogger o para destruir datos. Las contramedidas consisten en implementar antivirus que analicen de forma heurística y analizar los nodos de la red.
* Contraseñas: Las contraseñas son uno de los blancos más buscado, su protección radica en la fortaleza de la contraseña pero, los empleados no pueden recordar contraseñas de diez dígitos y las terminan escribiendo. Se puede implementar un sistema de seguridad de doble factor, para que además de necesitar una cable se necesite una llave USB que almacena un certificado para entrar.
* Configuraciones predeterminadas: Muchas veces no cambiamos las configuraciones por defecto de los dispositivos, está es una vulnerabilidad muy explotada. Simplemente cambiado la configuración, ya sea contraseña u otros aspectos, podemos aumentar la seguridad significativamente.

Los atacantes aprenden constantemente nuevas formas de ataque a través de investigación. Las principales técnicas son con reconnaissance, discovery, footprinting o Google Hacking. Generalmente los atacantes hacen inteligencia de sus objetivos varios meses antes de las primeras pruebas.

En cuanto a las medidas preventivas estamos restringidos debido a la información que se encuentra ya en internet y la que se publicará en un futuro. Con respecto a la información que se publicará, se puede controlar gracias a rigurosas políticas de seguridad.

**Ataques que hallamos sufrido:**

DDoS, lo típico cuando estás aprendiendo en clase y los paquetes vuelan por la red, en grado medio bloquearon el router unas cuantas veces.

Phissing, el correo que te suelen mandar que acaba en spam diciéndote que has ganado mucho dinero que des el número de cuenta o móvil.