SEGURIDAD INFORMÁTICA

FASE 3: CONSTRUCCIÓN

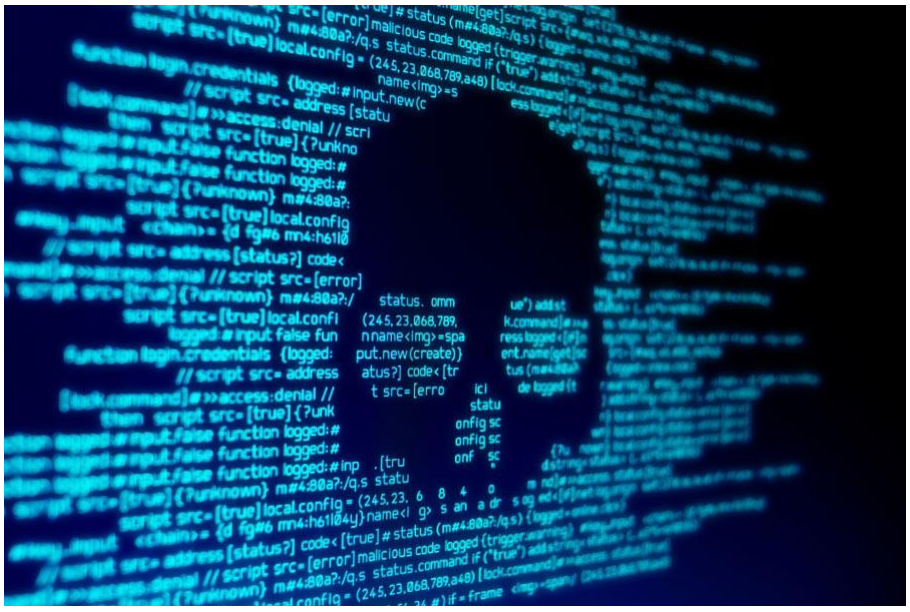
JORGE ALEXANDER ROMERO

CARLOS ALBERTO SOSA
TUTOR

GRUPO: 301122_29

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD DISEÑO DE SITIOS WEB
JUNIO 2019

¿QUÉ ES Y EN QUÉ CONSISTE UN ATAQUE INFORMÁTICO?



Un ataque informático se puede describir como una actividad hostil contra un sistema, un instrumento, una aplicación o un elemento que tenga un componente informático. Es una actividad que aspira a conseguir un beneficio para el atacante a costa del atacado. Existen diferentes tipologías de ataque informático que dependen de los objetivos que se quieren alcanzar, de los escenarios tecnológicos y de contexto.

Existen ataques que impiden el funcionamento de un sistema, ataques que apuntan a su compromisión, otros que aspiran a conquistar datos personales que están en un sistema o pertenecen a una empresa y los de ciberactivismo que sostienen causas o campañas de información y comunicación. Entre los ataques más difundidos, en los últimos tiempos, están los ataques con finalidad económica y los flujos de datos, llamados "Man-In-The-Middle" ("ataque de intermediario"): la finalidad de estos ataques es un sitio web popular o una base de datos para robar datos de tipo financiero.

Las personas que actúan un ataque informático, en solitario o en grupo, se llaman "Hackers".

¿Cómo prevenir los ataques si se es blanco de un hacker?

En esta primera fase el hacker hace una actividad de examen silencioso recurriendo a instrumentos online y recogiendo informaciones significativas usando sistemas no expuestos, pero accesibles. Se trata de una búsqueda pasiva

y por eso no se puede intervenir en ninguna manera. Después de esta primera fase, hay otra de examen activo donde el hacker busca vulnerabilidades y errores en el sistema que quiere atacar: el sujeto víctima, si dispone de adecuados instrumentos tecnológicos de defensa, puede lograr identificar el ataque.

Un alto número de ataques se puede hacer aprovechando de una debilidad tecnológica, como un error de programación, o una humana, como una contraseña estandar no cambiada. Una buena estrategia para prevenir un ataque siguiente o detectar los responsables puede ser la de memorizar los datos de acceso no solo en local, sino también en un sistema de almacenamiento de datos que permita archivarlos al exterior. El hacker trata de borrar sus rastros, pero tener los datos duplicados permite sea restablecerlos, sea tener un rastro de quien ha accedido a estos.

En la mayoria de los casos de ataques informáticos, la estrategia es silenciosa y las víctimas no se dan cuenta del ataque hasta que esto no haya pasado y no haya comprometido el sistema. Existen otros ataques que tienen como objectivo un daño a la imagen: el ataque será visible porque aparecerán pantallas de error o de denuncia, bloques de páginas u otras cosas decididas por el hacker que ha querido que el ataque fuese evidente.

Tipos de ataques informáticos

Existen numerosos tipos de ciberataques, cada uno con unas características o unos objetivos diferentes. Debido a la complejidad de sus nombres, la mayoría de ellos en inglés, es complicado saber de qué se tratan. Por ello, vamos a describir los principales ataques informáticos:

- **Malware**

También llamado software malicioso, por su traducción del inglés (malicious software). Su función principal es introducirse en un equipo y dañarlo de diversas formas.

Las más comunes son las siguientes:

- **Virus.** El virus permanece inactivo hasta que un usuario lo ejecuta. En este momento el virus comienza a infectar los archivos extendiéndose por todo el equipo.

- **Worms (gusanos).** El objetivo de los gusanos informáticos es infectar los archivos del equipo para difundirlos. Tienen la capacidad de extenderse a otros equipos sin necesidad de que un usuario los ejecute.

- **Troyanos.** Los troyanos muestran la apariencia de un programa fiable, pero esconden otro tipo de malware que es instalado automáticamente con el objetivo de tomar el control del equipo.

- **Keyloggers.** Son capaces de registrar todas las pulsaciones del teclado. Esta información es utilizada para conseguir contraseñas y datos de la víctima.

- **Spyware.** El objetivo principal de este malware es el robo de información.

- **Adware.** El adware se encarga de mostrar publicidad al usuario a través de banners, pop-ups, nuevas ventanas en el explorador… En muchos casos, el objetivo secundario también es obtener información sobre la actividad del usuario en la red.

- **Ransomware.** Es el tipo de ataque más común en la actualidad. Se basa en el cifrado de los datos, restringiendo el acceso a los archivos del equipo para pedir un pago por el rescate de los mismos. En la mayoría de los casos en bitcoins.

- **Denegación de servicio distribuido (DDoS)**

Este tipo de ataque informático consiste en generar una enorme cantidad de tráfico desde numerosos dispositivos a un sitio web. Debido a este drástico aumento del tráfico, el rendimiento de la red disminuye hasta el punto de que dicha red se satura y se interrumpe su funcionamiento normal.

Los ataques DDoS son de los más difíciles de evitar debido a la complejidad que han adquirido durante estos últimos años y a la importancia que han adquirido las transacciones a través de Internet.

- **Ingeniería social**

En la mayoría de los casos, los problemas informáticos son provocados por errores de los propios empleados, por ello es importante capacitar a los usuarios.

Muchos de estos ataques informáticos son a través del llamado phishing. Este tipo de ataques se basa en una suplantación de identidad.

El caso más común es el envío de un correo electrónico aparentemente de una entidad conocida (bancos, netflix, facebook…) en el que de algún modo conduce al usuario a un enlace malicioso donde introduce su usuario y contraseña.

- ✓ Como podemos ver, existe una enorme variedad de ataques informáticos, cada uno con una función o un objetivo concreto

Bibliografía

SOCROMTEAM. (2019). Los tipos de ataques informáticos más comunes. Recuperado de https://sicrom.com/blog/tipos-ataques-informaticos/

D' Adamo, L. (2017). Qué es y en qué consiste un ataque informático. Recuperado de https://www.consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/