ESTUDIO DE TIPOS DE ATAQUES INFORMÁTICOS

Cómo actúan los piratas informáticos

¿Estamos seguros detrás de nuestros antivirus gratis? ¿Son nuestros datos, los de una persona “normal”, queridos por los piratas en la red? Desgraciadamente, estamos más en peligro de lo que parece, no solo nuestros datos suelen querer los atacantes. A continuación lo abordamos.

Autores:

Juan Diego Berraquero Romero

Miguel Jiménez Cazorla

Indice

1. Ataques informáticos
2. Tipos de ataques
3. Consecuencias y cómo prevenirlos
4. Ataques más relevantes y más conocidos
5. Falsos mitos sobre los ciberataques
6. Conclusión
7. Bibliografía

1. Ataque informático:

Un ataque informático se define como un intento organizado e intencionado causado por una o más personas para causar daños o problemas a un sistema en red.

Estos ataques consisten en aprovechar alguna debilidad o fallo en el software, hardware, en incluso, en las personas que forman parte del entorno de la red atacada, para obtener un beneficio, por lo general, económico, causando un efecto negativo en la seguridad del sistema.

Otras definiciones relevantes:

- *"Un ataque informático o ciberataque es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control , desestabilizar o dañar otro sistema informático" (Wikipedia)*
- "*Un ciberataque es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que atacan a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos que están albergadas en servidores remotos, por medio de actos maliciosos usualmente originados de fuentes anónimas que también roban, alteran o destruyen un blanco específico mediante el hackeo de un sistema vulnerable*" (Wikipedia)

2. Tipos de ataques informáticos

De entre una gran cantidad de tipos de ataques, hemos seleccionado a nuestro gusto, una serie de ellos:

- man-in.-the-middle
- ataques DoS
- ping de la muerte*
- ARP Spoofing
- Ing. Social
- Key loggers
- Ataques Aplic. Web
    - Inyeccion SQL
    - Envenenamiento de Cookies
    - Phishing
    - Web Defacement
- Virus
- Troyanos
- Gusanos
- Malware

1. Man-In-The-Middle

En criptografía un ataque ***man-in-the-middle*** (MITM) es un tipo de ataque informático en el que el atacante tiene conexiones independientes con las víctimas, y transmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante. El atacante debe ser

capaz de interceptar todos los mensajes que van entre las dos víctimas e inyectar nuevos, lo cual es sencillo en muchas circunstancias.

Un ataque man-in-the-middle puede tener éxito solo cuando el atacante puede hacerse pasar por cada punto final a satisfacción de la otra (esto es un ataque de autenticación mutua).

2. Ataque DoS

Los ataques **DoS**, "***Denial of Service***", son un tipo de ataques informáticos, generalmente llevados a cabo localmente, por el cual el atacante busca bloquear un servidor o servicio mediante la sobrecarga del mismo o simplemente aprovechando un fallo que cause el bloqueo, y posteriormente el cierre del proceso o servicio del software afectado. Otro tipo de ataque similar al DoS es el DDoS, o "Distributed Denial of Service". Este tipo de ataque se caracteriza por llevarse a cabo por varios piratas informáticos a la vez (o por una botnet) y debe realizarse a través de Internet.

Mediante los ataques DoS, los piratas informáticos pueden, por ejemplo, saltarse las medidas de seguridad de un equipo o servidor, leer los valores de la memoria más allá de los límites del proceso e incluso conseguir permisos de administrador en el equipo, con los peligros que eso supone. A diferencia de estos, en los ataques DDoS, los atacantes generan un tráfico muy elevado hasta que, finalmente, el servidor víctima del ataque no es capaz de procesar todo el tráfico y termina por bloquearse, en el mejor de los casos.

Estos tipos de ataque no tienen como finalidad infectar un sistema con malware, sino que los atacantes buscan simplemente sobrecargar del ancho de banda de una red o un servidor, congestionar de los recursos del sistema y explotar posibles vulnerabilidades en el software y en los fallos de seguridad.

3. Ping de la muerte

Como bien sabemos, ***ping*** es un comando encontrado en muchos sistemas operativos, utilizado principalmente para encontrar problemas en una red particular. Este comando envía solicitud de respuesta a través del cable que incluye un paquete de datos de tamaño modificable. Configurándose de cierta manera, este comando inunda el servidor objetivo con peticiones ping haciendo que se bloquee.

Los atacantes, modificando el tamaño del paquete a enviar hasta el máximo que permita la ruta hacen que el servidor objetivo no sepa manejar dicho tamaño y termine bloqueándose.

4. ARP Spoofing

ARP Spoofing es uno de los ataques a las redes más utilizados, consiste en enviar mensajes ARP falsificados para hacer creer a la víctima que el usuario malintencionado es el router de la red local, y que debe enviar toda la información a él. De esta forma, podrá realizar diferentes tipos de ataques a la víctima.

El ataque viene a modificar el flujo de los datos enviados desde un PC Víctima que pasa a través de un Gateway para hacer un ataque de tipo MITM (*Man in the Middle*) consiguiendo que el tráfico de la víctima pase por una máquina Atacante de forma inocua para la víctima.

5. Ing. Social

La Ingeniería social tiene varias definiciones:

“Mentir a la gente para obtener información”

“El acto de manipular a la gente para llevar a cabo acciones o divulgar información confidencial” - Wikipedia

Uniendo éstas y varias más, llegamos a la conclusión de que la Ingeniería Social es el arte o, mejor aún, la ciencia, de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas.

Los atacantes utilizan métodos psicológicos para llegar a la víctima, hacer que la propia víctima confíe en él y luego sacarle toda la información que quiera (Datos bancarios, datos de empresa, contraseñas,...). De ahí, la importancia de ver a los empleados como otra puerta vulnerable hacia nuestro servidor.

6. Key Loggers

Tal y como su nombre indica (“Key” -*tecla*, y “logger” -*registrador*), este software o dispositivo hardware se encarga de registrar cada una de las pulsaciones que se hacen en el teclado y lo envía a un fichero.

Todos podemos ver claramente para qué querrían usar los piratas informáticos una herramienta así. Si además ese fichero lo puedes mandar a través de internet, el atacante solo le basta con infectar el ordenador que va a atacar y esperar que el KeyLogger le envíe todo lo que ha pulsado el usuario (contraseñas, correos, cuentas,... todo lo que haya hecho)

¿Cómo podemos darnos cuenta de que nos están “grabando” todas nuestras pulsaciones?

Pues mirando por ejemplo el uso de CPU, obviamente a simple vista no se va a poder ver, pero si aumentamos la carga del programa sí. Esto último lo podemos hacer simplemente con pulsar muchas teclas a la vez durante un buen tiempo, veremos aparecer una carga significante de la CPU y podremos saber así que estamos infectados.

7. Ataque Aplicaciones Web

- Los **ataques de inyección**, más específicamente ***sqli*** (*Structured Query Language Injection*) son una técnica para modificar una cadena de consulta de base de datos mediante la inyección de código en la consulta. El SQLI explota una posible vulnerabilidad donde las consultas se pueden ejecutar con los datos validados.

SQLI siguen siendo una de las técnicas de sitios web más usadas y se pueden utilizar para obtener acceso a las tablas de bases de datos, incluyendo información del usuario y la contraseña. Este tipo de ataques son particularmente comunes en los sitios de empresas y de comercio electrónico donde los hackers esperan grandes bases de datos para luego extraer la información sensible.

Los ataques sqli también se encuentran entre los ataques más fáciles de ejecutar, que no requiere más que un solo PC y una pequeña cantidad de conocimientos de base de datos.

- Los **ataques de envenenamiento** de cookies implican la modificación de los contenidos de una cookie (información personal almacenada en la computadora de un usuario web) para eludir los mecanismos de seguridad. Al usar ataques de envenenamiento de cookies, los atacantes pueden obtener información no autorizada sobre otro usuario y robar su identidad, ya que las cookies se transmiten por la red en texto plano.

- El ***phishing*** es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

  Los mensajes de phishing parecen provenir de organizaciones legítimas como PayPal, UPS, una agencia gubernamental o su banco. Sin embargo, en realidad se trata de imitaciones. Los correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa y se le embaucada para que facilite información sobre su cuenta, lo que puede provocar el robo de su identidad.

- La **desfiguración del sitio web** (Web Defacement) es un ataque a un sitio web que cambia la apariencia visual del sitio. Estos son típicamente el trabajo de los crackers del sistema, que entran en un servidor web y reemplazan el sitio web alojado con uno propio. Lo más probable es que este tipo de ataques se hagan intencionalmente para arruinar la reputación de la compañía que ha alojado este sitio web.

8. Virus

Un virus informático es un software malicioso que se adhiere a un programa o archivo para poder propagarse de un equipo a otro e infectarlos a medida que se desplaza. Al igual que los virus naturales, la gravedad de los virus puede variar, desde daños leves hasta daños que pueden afectar al funcionamiento del sistema.

Como punto importante, es de destacar que los virus no se pueden propagar sin intervención humana. Los usuarios propagan el virus de manera involuntaria, compartiendo archivos, enviando mensajes de correo, etc.

9. Troyanos

Un troyano no se puede confundir con un virus puesto que no tienen nada que ver. Es un programa diseñado para destruir un sistema haciéndose pasar por un programa real y auténtico. Estos, a diferencia de los virus, no se replican.

Además, los troyanos abren una puerta trasera en el equipo que facilita a los atacantes el acceso al sistema para robar información personal y confidencial.

10. Gusanos

Los gusanos tienen un diseño similar a los virus y se consideran una clase secundaria de virus. Los gusanos se propagan de ordenador en ordenador pero, a diferencia de los virus, tienen la capacidad de desplazarse sin intervención humana. Un gusano se aprovecha de las funciones de transferencia de archivos o de información del sistema, que le permiten viajar por sus propios medios. El mayor peligro de un gusano es su capacidad de replicarse en su sistema. Es decir, en lugar de enviar un solo gusano, su equipo puede enviar centenares o miles de copias de sí mismo, lo que puede tener consecuencias devastadoras.

11. Malware

Se usa para denominar a cualquier software que tenga intenciones dañinas para un sistema. Su objetivo principal es infiltrarse y dañar un PC. Los 3 anteriores, troyanos, gusanos y virus son distintos tipos de malware.

3. Consecuencias de los ataques y cómo prevenirlos

Al ser víctimas de un ciberataque, corremos por una gran lista de consecuencias y posibles sucesos que nos podrían perjudicar a raíz de este, algunos de ellos podrían ser:

- Perder información valiosa, de carácter confidencial o personal, lo cual puede traer pérdidas económicas o invasión a la privacidad, entre otras cosas.
- Se podría filtrar información de una compañía y de sus clientes, cuya secuela podría ser el quiebre de esta y la pérdida de trabajo de todos sus empleados.
- Existiría la posibilidad de que salieran a la luz fotos o datos privados, que fueron guardados en discos duros virtuales.
- Algunas personas, como es el caso de las celebridades, estarían expuestas al acoso, tanto de medios de comunicación, como de fanáticos y reporteros.
- Mediante cualquier tipo de hackeo, estamos expuestos al entorpecimiento en el funcionamiento de los equipos, lo que podría suponer para una compañía, un gasto extra para la reposición o reparación de estos dispositivos.

A continuación damos una lista de “consejos” que se deberían seguir para intentar tener una seguridad lo más fiable posible en nuestros sistemas:

Utilizar un antivirus que analice todas las descargas. Asegúrate de tener un antivirus instalado, actualizado al día para que reconozca el mayor número de virus, y realiza análisis regularmente de todo el sistema.

Mantener el sistema operativo y el navegador actualizados. Los virus aprovechan los agujeros del SO y navegador para infectar los dispositivos. Como contramedida los fabricantes corrigen los programas a través de actualizaciones. La mejor forma para estar protegido es activar las actualizaciones automáticas de tu SO, navegador, plugins del navegador y resto de aplicaciones.

Cuidar las contraseñas. Al introducirlas se debe estar seguro de que es la página correcta, ya que puede parecer idéntica a la legítima y tratarse de una suplantación (phishing). No se debe utilizar la misma contraseña en diferentes servicios porque si acceden a una cuenta fácilmente podrán acceder al resto. Tampoco se ha de compartir las contraseñas con nadie, aunque digan que son del servicio técnico, los servicios respetables nunca solicitarán las contraseñas por propia iniciativa.

Confiar en la web, pero sin ser ingenuo. Hay que permanecer alerta, no todo lo que se dice en Internet tiene por qué ser cierto. Ante la duda, contrastar la información en otras fuentes de confianza.

No hacer clic en enlaces que resulten sospechosos. Se debe ser precavido antes de seguir un enlace al navegar, en el correo, en la mensajería instantánea o en una red social. Los mensajes falsos que los acompañan pueden ser muy convincentes con el fin de captar la atención del usuario y redirigirle a páginas maliciosas.

Tener cuidado con lo que se descarga. No hay que precipitarse y descargarse cualquier cosa, ya que nuevas amenazas surgen cada día y los antivirus no pueden combatirlas todas. Hay que descargar los ficheros solo de fuentes confiables y los programas desde sus páginas oficiales.

Desconfiar de los correos de remitentes desconocidos. Ante la duda, es recomendable no responder a los mismos y eliminarlos directamente.

No abrir ficheros adjuntos sospechosos. Si es de un conocido hay que asegurarse de que realmente lo quiso enviar. Los virus utilizan esta técnica para propagarse entre los contactos del correo, así como los contactos de la mensajería instantánea y de las redes sociales.

Pensar antes de publicar. Los servicios actuales de Internet facilitan las relaciones sociales, lo que conlleva a su vez se publiquen mucha información sobre las personas (datos personales, imágenes, gustos, preferencias, etc.). Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado por parte de otras personas, es necesario que se gestionen adecuadamente.

Conoce los riesgos asociados al uso de Internet. ¡Hay que mantenerse al día! Es aconsejable estar suscrito a los boletines de correo de la OSI, que incluyen los últimos avances de actualidad.

Y añadir un par de casos más para las empresas, y es que la red empresarial debe ser segura. Se debe **saber quiénes se conectan a ella**. Quienes la administran deben contar con una visión completa del funcionamiento de la misma en todo momento. También es imperativo diseñarla de modo que, en caso de ataque, existan opciones para **segmentar la red y aislar las infecciones**, y también se debe invertir en la capacitación de los empleados. Según la consultora EY, los ataques responden, en un 83 por ciento, a empleados descuidados.

4. Ataques más relevantes y más conocidos

En este apartado, os contamos una serie de casos muy conocidos a nivel mundial de ataques que dejaron un buen daño en los sistemas.

- **Hack EEUU:160 millones de usuarios (ataque bursátil):**

  El gran ciberataque de Estados Unidos afectó a 160 millones de usuarios y repercutió en el índice bursátil NASDAQ, así como en el Dow Jones y en empresas como JC Penney, 7-Eleven. Este famoso crackeo sí afectó a datos de tarjetas bancarias, en concreto a las de 160 millones de clientes. El asalto duró desde 2005 hasta 2012 y fueron involucradas cinco personas de origen ruso. Este asunto fue quizá el mayor ciberataque de la historia del país, ya que afectó al mercado de valores tecnológico de Wall Street y consiguió sacar a la luz secretos de numerosas empresas. Los cibercriminales se apropiaron también de información sobre comunicaciones privadas de reputados directores de empresas del NASDAQ y también sobre datos financieros.

- **Sony PlayStation**

  El 16 de abril, los hackers violaron la seguridad del servicio Sony Online Entertainment, robando la información personal de 25 millones de usuarios y alrededor de 23,400 datos bancarios de la región europea corrieron peligro. Este fue el preludio de la tragedia.

  Al día siguiente, el 17 de abril de 2011, los hackers destruyeron la seguridad de la PlayStation Network, robando la información personal de 77 millones de usuarios.

  Fue hasta el 20 de abril que Sony no tuvo más opción que desconectar su servicio en línea a nivel mundial. Este evento aún es conocido como la violación de seguridad digital más grande de la historia. Tras la intervención del FBI y el gobierno de Estados Unidos, al final, Sony reforzó su seguridad y restableció su servicio el 14 de mayo de 2011. Y el 23 de mayo, Sony anunció que este ataque le había costado 171 millones de dólares.

- **Stuxnet, casi accidente nuclear en 2010, en Natanz**

  En enero de 2010, los inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Natanz, Irán, notaron con desconcierto que las centrifugadoras usadas para enriquecer uranio estaban fallando. Curiosamente, los técnicos iraníes que reemplazaban las máquinas también parecían asombrados.

  El "gusano" - ahora conocido como Stuxnet - tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.

- **Ucraniano viviendo en España roba 10.000 MILL en cajeros a distancia (más reciente)** Se trata del capo de Carbanak (y también de la organización Cobalt), un ciudadano ucraniano de 34 años que traía de cabeza desde hace al menos cuatro años a varios países por su capacidad para desvalijar bancos a distancia infiltrándose en sus sistemas informáticos.

  Una estimación del botín total logrado con los distintos 'softwares' de la organización (Anunak, Cobalt y Carbanak) llegaría hasta los 10.000 millones, según fuentes del sector de la ciberseguridad.

  Los ladrones primero penetraban en la red informática del banco en cuestión con correos maliciosos a trabajadores, que pinchaban de alguna manera en archivos adjuntos y permitían la entrada del virus. Después, iban ascendiendo poco a poco en los diferentes anillos del sistema, hasta reconocer los resortes de control de cajeros y transferencias, y por último los obligaban a soltar el dinero, bien forzando transferencias o bien haciendo a los cajeros escupir billetes.

- **Un ciberataque afectó a Twitter, Netflix y Spotify**

  Un poderoso ataque informático contra los servidores de Dyn, un proveedor de direcciones DNS, hizo caer un número importante de conexiones a Internet en la costa este de Estados Unidos y afectó durante horas a sitios y servicios como Twitter, Netflix, Spotify, Reddit y The New York Times, entre otros.

  La empresa Dyn informó a través de un comunicado que se trató de un ataque de denegación distribuida de servicio (DDoS) y señaló que si bien logró restaurar sus servicios, pero algunos clientes aún podrían seguir con inconvenientes.

5. Falsos mitos

Como curiosidad, hemos añadido este apartado donde comentamos cuán es la ignorancia sobre la importancia de un ataque y cómo existe una falsa seguridad en el día a día de todo el mundo:

- "**La base de virus, ha sido actualizada**". Creo que no cabe duda que la amplia mayoría conocemos esta frase del antivirus. Está claro, que mantener el antivirus actualizado es una de las condiones fundamentales para tener seguridad en el PC, no obstante, no es suficiente. Siempre existirá la posibilidad de que un nuevo ataque pueda surgir antes de que el antivirus sepa reconocerlo.
- **Creer que el firewall lo frena todo**. Aunque los cortafuegos son esenciales, no son perfectos. Basta con que por cualquier razón (y como programa software que es) tenga un error, lo que haría al sistema vulnerable de determinados ataques.
- **Creer que no somos un blanco interesante**. Algo muy común es preguntarnos, ¿por qué me van a hackear a mi?, ¿qué sacan conmigo si no soy ni tengo nada valioso? Simplemente el hecho de que puedan controlar nuestro ordenador, y el de mucha gente más, facilita al atacante a realizar un ataque DDos contra un servicio Web.
- "**No abro ningún adjunto, los virus no pueden entrar.**" Falso. Hay virus, como el Blaster, que ingresan a la PC sólo por estar conectadas con Internet, si Windows no está debidamente actualizado.

6. Conclusión

Como conclusión, hemos confirmado nuestra suposición al comenzar el trabajo. No estamos concienciados de la importancia que tiene la seguridad informática en nuestras vidas. No solo a nivel privado y personal, sino también a nivel empresarial.

Si bien es cierto, se conciencia a la sociedad sobre la seguridad que te aporta tener un antivirus en el sistema, pero no se conciencia de los métodos de ataques a los que un antivirus, por bueno que sea, es vulnerable.

Es importante que se dé a conocer a todos la importancia de salvaguardar nuestros datos, y los de nuestra empresa. Aunque a veces la intención de los piratas es simplemente fastidiar dejando los sistemas inservibles, otras, buscan quedarse con nuestros datos y venderlos al mejor postor. Como sabemos, estamos en la era del Big Data y la moneda de cambio es la información. Es por esto que cada vez tenemos que invertir más en nuestras empresas en el departamento de seguridad informática, donde un equipo especializado tiene que controlar tanto la seguridad del sistema como la seguridad a nivel empleado.

Con la seguridad a nivel empleado, nos referimos a que, como hemos visto en el trabajo, un empleado puede ser una puerta de acceso para un atacante a nuestra red, por lo que es de gran importancia tener controlado estas vías mediante formación, denegación de acceso a información sensible, etc.

Resumiendo, la seguridad en nuestros sistemas es cada vez un tema más importante a tratar. Si queremos evitar un desastre a nuestra empresa, debemos tener un gran sistema de seguridad que consiga evitar o paliar cualquier ataque, tanto interno, como externo.

7. Bibliografía

- https://www.lanacion.com.ar/793784-los-diez-mitos-de-la-seguridad-informatica
- https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/
- https://seguridadpcs.wordpress.com/terminologias-2/ataque-man-in-the-middle/
- https://www.softzone.es/2016/07/14/ataques-dos-ddos-podemos-protegernos
- https://www.bebee.com/producer/@fran-brizzolis/ataque-de-arp-spoofing-que-es-y-como-podemos-defendernos
- https://www.avast.com/es-es/c-phishing
- https://sites.google.com/a/correo.unimet.edu.ve/ciberataques/anuncios/consecuencias-de-los-ciberataques
- https://www.heraldo.es/noticias/comunicacion/2015/03/31/diez_consejos_para_prevenir_ataque_informatico_348654_311.html
- http://www.eltiempo.com/tecnosfera/novedades-tecnologia/consejos-para-prevenir-y-enfrentar-ataques-informaticos-92972

- https://blogthinkbig.com/los-crackeos-mas-sonados-de-la-historia
- http://www.elmundo.es/espana/2018/03/26/5ab8bdeb268e3ed01d8b4636.html
- https://www.redbull.com/mx-es/robo-de-cuentas-de-la-playstation-network