Tipos de ataques informáticos. Formas de actuación los piratas informáticos.

1) ¿Qué es un hacker?

Aproximadamente después de los inicios de la computación basada en máquinas automáticas apareció un nuevo término relacionado con esta rama, un término muy conocido hoy en día por básicamente todo el mundo. Desde su aparición este término adquirió una connotación negativa, hoy en día se sigue viendo afectado por esta connotación. Este término se puede definir como "todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo", como se puede apreciar en esta definición un hacker no tiene que ser perjudicial en sí, de hecho, vamos a tratar un poco sobre los dos tipos de hackers que existen hoy en día en el mundo para dejar un poco más claro este término.

- White hats: Más comúnmente conocido como hacker ético, se refiere a una ética hacker que se centra en asegurar y proteger los sistemas de tecnologías de la información y comunicación. Normalmente estas personas suelen trabajar en equipos de seguridad de empresas, estos equipos son llamados "zapatillas o equipos tigre".
- Black hat: Estos son los más famosos, los que la sociedad teme, ya que son los que se dedican a usar sus conocimientos para romper sistemas de seguridad de computadoras, colapsando servicios de servidores web o incluso apoderándose de una red en concreto. Todo esto con el objetivo de obtener algún bien que suele ser información privilegiada o dinero.

En los últimos años, estos términos han salido más a la luz ya que los ataques se han vuelto más famosos. Como ejemplo podemos poner el último ataque de un "ramsonware", concretamente llamado "wanna cry" que ha afectado a varias empresas en todo el mundo. Entre estas empresas podemos encontrar grandes de telecomunicaciones como "Telefonica" o grandes bancos como "BBVA" que se han visto sin sistemas informáticos ya que han sido codificados por este malware.

2) ¿Qué es un ataque informático?

En la historia del mundo siempre han existido ataques. Los primeros ataques se daban en tribus, era la lucha cuerpo a cuerpo. Más tarde las guerras, lucha con armas. Por último, en esta era los ataques que se dan son ataques informáticos, en busca de algún tipo de información o dinero. Ahora bien, para acuñar el término de ataque informático podemos decir que "Un ataque informático es un intento organizado e intencionado causado por más de una persona para infringir daños a la seguridad de un sistema informático o red". Estos ataques

suelen darse por un grupo de personas llamadas “piratas informáticos o hackers” y se suelen dar a grandes corporaciones, empresas importantes de la que se pueda obtener mucho dinero o información que pueda afectar al estado de la misma. Los ataques informáticos se aprovechan de alguna debilidad o fallo en el software, hardware o incluso en las personas que forman parte de una comunidad informática.

A modo de ejemplo y de forma resumida, vamos a exponer algunos de los ataques más importantes de la historia de la informática.

- En agosto de 2014, unos piratas rusos se apoderaron de 1200 millones de claves de seguridad de 420000 páginas de internet en el mundo. Entre ellas se vieron afectadas tanto páginas importantes como no tan importantes.
- En enero de 2015, un empleado de una empresa de solvencia que supuestamente trabajaba como consultor se dedicó a robar datos de tarjetas de créditos que iban a ser emitidas a los clientes. Esto conllevó la anulación de pagos online de más de dos millones de surcoreanos.
- En diciembre de 2013 la cadena de distribución estadounidense “Target” fue víctima de un ataque en el que se robaron datos personales a 110 millones de clientes. De todos estos clientes a 70 millones se les robaron los datos personales y el restante 40 se les robaron las cuentas bancarias y la información de las tarjetas de crédito.
- En agosto de 2015, el grupo de piratas informáticos “The Impact Team” publicó 30 gigas de datos de usuarios de la red social “Ashley Madison”. Las revelaciones provocaron el suicidio de un alto número de usuarios en Estados Unidos y Canadá ya que el fin de esta red social era ser infiel a tu pareja.
- En septiembre de 2015, un virus llamado “KeyRaider” logró piratear más de 225000 cuentas de apple.
- En agosto de 2014, la “nube” de apple fue hackeada y se robó una colección de casi quinientas fotografías privadas de varias celebridades.
- En septiembre de 2012, el grupo de hackers “Anonymous” hicieron caer la página de la presidencia de la nación y la administración federal de ingresos (AFIP).

Estos son los ataques más importantes o más “famosos” que se han dado hasta ahora, cada uno de estos ataques se ha dado de una forma diferente. Nosotros vamos a intentar abarcar las formas más comunes de ataque y explicar su funcionamiento.

3) Herramientas usadas para ataques informáticos.

Como para cualquier situación, en el mundo de la informática también existen herramientas para diferentes procedimientos. Tratando el tema del que estamos hablando vamos a ver algunas de las herramientas más usadas para proceder con ataques informáticos:

- Nmap: Una de las herramientas más usadas a nivel mundial para el escaneo de redes es esta. Nmap no solo realiza escáneres de puertos si no que realiza varias tareas como el horario de usos de servicios de red, control de host y la actividad en la red del mismo, identificar la configuración de seguridad de un ordenador, etc. Esta herramienta es usada por los dos bandos de hackers, el ético y el destructivo.
- Metasploit: Los exploits son pequeñas piezas software que se dedican a buscar y aprovechar debilidades en la seguridad de redes o computadoras. Esta aplicación es un kit de exploits de los más completos, dentro vamos a encontrar software que sirve para analizar la seguridad de cualquier sistema o máquina.
- Angry IP scanner: Esta aplicación, también conocida como IPScan, destaca por la sencillez de su uso y su velocidad. Su aplicación principal se resume en escanear puertos y direcciones IP de una red.
- Cain and Abel: Esta es una de las herramientas más potentes si se trata el tema de recuperación de contraseñas. Desde ella vamos a poder llevar a cabo una serie de ataques para intentar buscar debilidades en las contraseñas o si es posible adivinarlas a través de técnicas de explotación, por fuerza bruta, por diccionario y por criptoanálisis. Un punto fuerte de esta aplicación es la compatibilidad que tiene con hashes de contraseñas, entre ellos encontramos NTLM, MD2, MD5, SHA-1 y SHA-2.
- John The Ripper: Siguiendo con los descifradores de contraseñas, esta aplicación es una de las más potentes en cuanto a ataques de diccionario y, sobre todo, ataques de fuerza bruta. Otros aspectos interesantes de John The Ripper es que puede llevar a cabo tareas como buscar posibles grietas analizando hashes o comparando datos de salida al generar contraseñas.
- THC Hydra: Aplicación usada para comprobar la robustez de una contraseña mediante ataques de diccionario o de fuerza bruta, especialmente en páginas web. Esta herramienta es más usada en el hacking ético.
- Burp Suite: Herramienta que cuenta con dos funcionalidades, burp suite spider que enumera los parámetros potencialmente más vulnerables de una red e intruducer que se encarga de automatizar y planificar los ataques.

- Ettercap: Es una herramienta que se usa para llevar a cabo ataques como ARP posioning para identificar sistemas dentro de una red y tras esto poder llevar a cabo ataques más avanzados con herramientas específicas.
- Wapiti: Es una herramienta poco conocida pero su número de usuarios va creciendo cada vez más. Es una herramienta capaz de escanear una red o un sistema e identificar todas las vulnerabilidades que tiene. Tiene muchos apartados de pago más específicos entre los que podemos encontrar análisis de código en diferentes idiomas de programación para evitar la inyección de código por ejemplo.

Entre todas las herramientas expuestas anteriormente nos encontramos que algunas de ellas son más usadas por profesionales de seguridad para evitar que los ataques entren dentro del sistema y otras son más usadas para atacar. Estas preferencias dependen de varios factores, entre ellos el grado de dificultad de uso de la herramienta, la velocidad que tarda cada herramienta para actuar o la carga que ejerce cada herramienta al sistema. Por supuesto no solo existen las herramientas anteriormente citadas, existen muchísimas más que no son tan conocidas como las anteriores.

4) <u>Tipos de ataques informáticos</u>

Esta es la parte más importante del trabajo ya que es en lo que desemboca el uso de las herramientas que hemos estado tratando hasta ahora. A continuación, se va a exponer diferentes tipos de ataques cuya técnica para llevarse a cabo a cambiado a lo largo de los años. Al principio los ataques se llevaban a cabo simplemente averiguando una contraseña que tenía suficientes permisos como para poder modificar archivos importantes pero cada vez se han ido perpetuando más formas y métodos para llevar a cabo ataques, tanto es esto que hoy en día una persona con muy pocos conocimientos de seguridad o de informática sería capaz de dejar fuera de serie un sistema de seguridad con un herramienta suficientemente potente y un simple tutorial de uso o unas instrucciones que seguir. Actualmente se distinguen siete tipos de ataques diferentes:

- Ingeniería social.
- Ingeniería social inversa.
- Trashing o cartoneo.
- Ataques de monitorización.
- Ataques de autenticación.
- Denial of Service (DoS)
- Ataques de modificación/Daño.

- **Ingeniería social:** Manipulación de las personas para que realicen actos que normalmente no están acostumbrados a realizar para que revelen información importante sobre el sistema. Normalmente esto ocurre a causa de la experiencia o conocimientos del atacante y de la falta de conocimientos del atacado. Este tipo de ataques son algunos de los más usados a la hora de averiguar claves de usuario y contraseñas. Algunas medidas de seguridad que se pueden tomar contra este tipo de ataques son: Tener servicio técnico propio y de confianza y dar instrucción a los usuarios para que no respondan ninguna pregunta que pueda poner en peligro el sistema.

- **Ingeniería social inversa:** Consiste en generar una situación inversa a la que se genera en los ataques de ingeniería social. Lo más usual es que el atacante publicite de alguna manera que puede ayudar a los usuarios y aprovechar la llamada de estos para pedirles información del sistema. Este tipo de ataque es más difícil de generar que el anterior y se suele utilizar cuando los usuarios están alertados o conocen la existencia de los ataques de ingeniería social. Algunas de las situaciones más frecuentes en las que se da el problema son:
    - Generación de un fallo en el funcionamiento normal del sistema. Esto requiere que el intruso tenga un cierto contacto con el sistema para ocasionar el fallo.
    - Comunicación a los usuarios de que la solución la puede dar el intruso.
    - El intruso se camufla como servicio técnico del sistema.

- **Trashing o cartoneo:** Es uno de los ataques más simples, el ejemplo más común que se pone es que todos los usuarios usan un papel en el que apuntan su usuario o su contraseña hasta que lo recuerdan y entonces se deshacen de este papel. Estas son grandes oportunidades para que los atacantes se hagan con contraseñas o llaves de acceso al sistema. Hay dos tipos de trashing, el físico que ya hemos explicado y el lógico que se basa en hacer escáneres de bufferes de datos entre redes o impresoras buscando palabras clave de cada usuario.

- **Ataques de monitorización:** Este tipo de ataques consisten en observar a la víctima y a su sistema con el fin de establecer formas de entrar y atacar en el futuro. Dentro de este ataque hay varias formas de observación, entre ellas:

    - Shoulder Surfing: Consiste en observar físicamente el usuario y la contraseña de los usuarios. Esto puede ocurrir si la tienen apuntada cerca del ordenador o si se observa por encima del hombro.

- Decoy o señuelos: Son programas diseñados con la misma interfaz que otro original. Normalmente en ellos se imita la situación de logueo en algún sistema, una vez escrito el usuario y la contraseña el programa los guarda y deja que el sistema actue con normalidad. Esto permitirá al atacante recopilar información sobre el usuario para usarla en el futuro.
- Scanning o búsqueda: Este tipo de ataque lleva en uso mucho tiempo. La idea de su uso es recorrer tantos puertos abiertos como sea posible en una red y guardar información de aquellos que sean receptivos o de uso relevante para el atacante. Escanear puertos implica técnicas de fuerza bruta que consisten en enviar paquetes de diferentes protocolos y se deduce que servicios están escuchando por las respuestas recibidas o no recibidas. Dentro de este subataque existen diferentes variantes del mismo:
    - TCP connect scanning: Forma básica de escaneo de puertos TCP en la que si el puerto está escuchando devolverá una respuesta. La ventaja que tiene este subataque es su simplicidad pero tiene una gran desventaja y es que es fácilmente detectable por el administrador.
    - TCP SYN scanning: Este tipo de ataque utiliza el protocolo Three-way-Handshake para hacer el scanning de puertos. Principalmente lo que hace es abrir “media” conexión TCP entre el servidor y el cliente para comprobar que el puerto está abierto o cerrado. Para ello el cliente envía un paquete SYN y espera la respuesta, si obtiene respuesta se envía de forma inmediata un RST para terminar la conexión. La ventaja de este ataque es que pocos sitios están preparados para registrarlos y la desventaja es que en sistemas Linux se necesitan privilegios de administrador para realizar estos procedimientos.
    - TCP FIN Scanning– Stealth Port Scanning: A veces el método de escaneo anterior es poco “limpio” ya que hay firewalls que escanean constantemente los puertos en busca de estas conexiones incompletas. Para ello nace esta variación de ese tipo de escaneo que basa su funcionamiento en el paquete FIN. A este tipo de paquete solo responden los puertos que están cerrados pero los que están abiertos los suelen ignorar y son indetectables. Esta es una forma de detectar el estado de los puertos.
    - Fragmentation scanning: Este ataque es una variación de los anteriores. En lugar de enviar un paquete completo envía fragmentos de ip que son indetectables por los firewalls. La desventaja y la razón por la que se hacen detectables estas

técnicas de escaneo es porque el manejo de estos pequeños paquetes ralentiza todas las maquinas implicadas.

- Eavesdropping-Packet Sniffing: Este tipo de ataque se basa en la vulnerabilidad de las redes a la pasiva intercepción del tráfico de red. Esta interacción se realiza con los Packet Sniffers, son programas que monitorean los paquetes que circulan por la red. Este tipo de programas pueden ser colocados en cualquier máquina con acceso a internet o en el mismo router. Los sniffers actúan sobre las tarjetas de red y las ponen en modo promiscuo lo que hace que recojan todos los paquetes aunque no coincidan con su dirección mac. Esto hace que todos los paquetes pasen por una misma máquina lo que permite al Sniffer analizar los paquetes en busca de información como contraseñas o cosas del estilo. La mayoría de los sniffers no se pueden detectar por lo que lo difícil de estos procedimientos es colocar el software en el lugar debido.
- Snooping-Downloading: El objetivo de estos ataques es obtener información sin modificarla. Pero no se limita a recoger los paquetes y a analizarlos como la técnica anterior sino que también hace una copia de ellos y los descarga en otra máquina para que el atacante pueda analizarlos con detenimiento.

- **Ataques de autenticación:** Este sistema tiene como objetivo engañar al sistema de la víctima para identificarse dentro del mismo, generalmente lo hace tomando las sesiones ya establecidas. Dentro de este tipo de ataque informático se pueden disinguir subataques que se basan en este:
  - Spoofing-Looping: El objetivo de este ataque es hacerse pasar por otros usuarios usualmente para realizar ataques de Snooping o tampering. Esta técnica lo que hace es usar un sistema al que se accede robando el ususario y contraseña de otra persona y a partir de ahí enlazar con otros sistemas haciendo que su rastreo sea prácticamente imposible.
  - Spoofing: Son tipos de ataques que se llevan a cabo sobre protocolos y que requieren que se domine completamente el conocimiento sobre el protocolo. Hay varios tipos de Spoofing, entre ellos los más importantes:
    - IP Spoofing: Se generan paquetes con el campo from de la dirección IP cambiada, normalmente usando el nombre de un tercero para camuflar la verdadera identidad del atacante.
    - DNS Spoofing: Este ataque se lleva acabo mediante la manipulación de paquetes UDP pudiéndose ver afectado el servidor DNS en el peor de los casos. Principalmente cambiando direcciones IP por direcciones de páginas falsas.

        - Web Spoofing: Se crea un sitio web completamente falso pero similar estéticamente al que la víctima desea entrar. Con esto el atacante consigue recopilar todos los datos de la víctima que desee.
        - IP Splicing-Hijacking: En este caso el atacante espera a que la víctima este identificada en el sistema para después suplantar la identidad de la víctima en el sistema. Para ello el atacante necesita un Sniffer que esté analizando todos los paquetes de la comunicación entre el usuario y servidor.
        - Uso de Backdoors: Las puertas traseras son trozos de código que se suelen usar en los test de funcionamiento del programa y que para la versión final se suelen eliminar. Esto no siempre es así, ya que a veces por intención o sin intención de los programadores esto se queda ahí y si alguien la descubre podrá saltarse fácilmente los métodos de seguridad y acceder al sistema.
        - Uso de Exploits: Utilizando la herramienta que se ha explicado en el apartado anterior se aprovechan los defectos de los algoritmos que generan las claves para entrar en el sistema.
        - Obtención de passwords: Este método comprende la obtención mediante algoritmos de fuerza bruta las contraseñas de los usuarios. Normalmente los usuarios escogen palabras con mucha relación con su vida diaria y que raramente se cambian por lo que no siempre es necesario usar la fuerza para sacar la contraseña, en cambio cuando si es necesario se suelen usar varias máquinas a la vez actuando sobre el mismo servidor con diccionarios de claves probando miles de claves hasta encontrar la correcta.
- **Denial of Service (DoS):** Los protocolos que existen hoy día fueron diseñados para usarse en una comunidad abierta y en la que mucha gente participaría, por lo que la mayoría de las veces es más fácil tirar abajo unos servicios que acceder a su interior, es por esto, que se crearon este tipo de ataques. De este tipo de ataques encontramos varias formas diferentes de actuar y procedimientos como:
    - Jamming o flooding: La finalidad principal de este ataque es desactivar o saturar completamente los recursos de un sistema. Para ello lo que se hace es enviar solicitudes que requieren establecer conexión de forma masiva, el sistema responde al mensaje pero como no vuelve a obtener respuesta al final se acaba saturando la memoria.
    - Syn Flood: Este ataque es el más famoso de los ataques de este tipo. Consiste en que el cliente envía una petición de conexión con el servidor pero no responde al ACK que envía el servidor por lo que el

servidor reserva una pila por una cantidad de tiempo por cada conexión. Al enviar múltiples conexiones cada vez se debilita más la capacidad para prestar los demás servicios y se acaba tirando el servidor.

- Connection Flood: Consiste en monopolizar todas las conexiones simultaneas que admite un servidor por un solo usuario para que no se puedan atender las peticiones de los demás.
- Net Flood: Consiste en enviar simultáneamente tantos paquetes de conexión a un servidor que se satura la línea de forma que las conexiones reales no tienen forma de entrar en ella.
- Land attack: Este ataque aprovecha un error en la implementación de la pila del protocolo TCP de las plataformas Windows. El ataque consiste en enviar a un puerto abierto un paquete construido con la dirección y el puerto origen igual que la dirección y el puerto destino. Esto hace que tras varios paquetes enviados y recibidos por la misma máquina, esta se termine colgando.
- Smurf o Broadcast Storm: Consiste en mandar un paquete broadcast a muchos equipos con la dirección destino cambiada para que todos la acepten, entonces cuando todos a la vez envíen un paquete ICMP a la máquina cliente este será devastador.
- OOB, Supernuke o Winnuke: Un ataque muy común en equipos con Windows que tengan abierto el puerto de NetBIOS. Se envían paquetes Out of Band que la máquina detecta como inválidos, cuando tienen que manejar un gran número de estos paquetes la máquina se vuelve inestable.
- Teardrop I y II-Newtear-Bonk-Boink: Al igual que el ataque anterior, este tipo de ataques afectan a fragmentos de paquetes. Algunas implementaciones de las pilas IP no son capaces de volver a montar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue.

- **Ataques de modificación-Daño:** Estos ataques son un tipo de técnicas que tienen como objetivo la modificación no autorizada y ficheros de un sistema. También pueden modificarse programas que se ejecutan en el sistema. Entre ellos se pueden clasificar diferentes ataques dentro de este ámbito:
    - Tampering o Data Diddling: Modificación no autorizada de los datos o el software instalado en el sistema de la víctima. En estos casos es especialmente preocupante cuando el intruso ha obtenido permisos de administrador en el sistema.
    - Borrado de huellas: Es una tarea importante que tiene que cumplir un intruso en el sistema después de haber accedido para que el administrado no descubra por donde ha entrado. Consideramos

huellas como todas las tareas que realizó el intruso en el sistema y que por lo general se guardan el logs.

- Ataques mediante java Applets: Aunque Java es uno de los lenguajes más conocidos por su seguridad, en los navegadores de interenet de hoy día se incluyen máquinas virtuales de Java para que se ejecute su contenido. Estas máquinas virtuales pueden ser modificadas por atacantes para que extraigan información y la envíen por internet.
- Ataques mediante JavaScript y VBSscript: Estos dos lenguajes son usados por diseñadores web por lo que son ejecutados por navegadores web. Hoy en día estos idiomas se utilizan para ver los fallos de navegadores e intentar mejorarlos.
- Ataques mediante ActiveX: ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft y es un lenguaje que hace competencia con Java, pero con una variación y es que ActiveX comprueba la seguridad con certificados y firmas digitales. Cuando un usuario accede a una página web, en numerosas ocasiones se le pide que acepte el certificado, es aquí donde reside el peligro. Normalmente ningún usuario lee lo que el certificado trata y cuando se acepta pasa a ejecutar el programa sin ninguna restricción, pudiendo estar entonces haciendo algo dañino en nuestra máquina.
- Vulnerabilidades en los navegadores: Aquí voy a tratar los fallos intrínsecos de los navegadores, entre ellos uno de los más importantes, “Buffer Overlow”. Buffer Overlow consiste en explotar una debilidad de los buffer que la aplicación usa para almacenar las entradas del usuario. Este fallo acompañado de protocolos como “.lnk” o “.url” se amplifica y lo hace más difícil de detectar.

Hasta aquí los principales tipos de ataques que se llevan a cabo día a día, entre ellos hemos tocado los temas más repetidos y más famosos. Pero claramente estos no son todos los tipos de ataques. Cada día se investigan más formas de proteger la seguridad de un sistema, pero al igual que con el malware o los virus informáticos los ataques de piratas informáticos siempre irán un paso por delante de las defensas.