Fases de un ataque a un Sistema Informático

José Luis Calle Condori
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
jlc_inf@yahoo.es

***Resumen*—El internet a través de los años ha evolucionado, siendo esta la red más grande del mundo donde se encuentra la mayor cantidad de información, al mismo tiempo los ataques a sistemas informáticos también van evolucionado, los cuales ponen en riesgo la información de instituciones públicas y privadas, atentando contra la confidencialidad, integridad y disponibilidad de la información. Razón por la cual en el presente trabajo de investigación se describe las fases de un ataque a un sistema informático. La investigación tiene un enfoque cualitativo. Las fuentes consultadas corresponden a: revistas digitales, repositorios académicos, bibliotecas digitales y sitios web. Los resultados hallados muestran que existen 5 fases por las cuales suele pasar un ataque a un sistema informático al momento de ser ejecutado. En conclusión, conocer las fases de un ataque a un sistema informático nos ayuda a actuar de manera proactiva frente a los posibles ataques a sistemas informáticos.**

Palabras clave—amenaza informática, ataques informáticos, información, vulnerabilidad

I. INTRODUCCIÓN

La presente investigación se refiere al tema de fases de un ataque a un sistema informático, que consiste en el estudio de la estructura de un ataque informático a un sistema, sabiendo que métodos utilizaron para ingresar a un sistema informático sin autorización.

Un ataque a un sistema informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización [1].

En la revisión de trabajos previos, Mamani [2], en su artículo "Fases de un Ataque Hacker", explica que un ataque hacker se basa en 5 fases importantes, para poder llevarlo a cabo de manera exitosa y las fases de un ataque son muy importantes para el hacker como también lo son para la victima que no conoce de la estrategia del ataque. Asimismo, Plaza [3], en su informe de trabajo práctico de suficiencia "Métodos de ataque informáticos", explica que en la actualidad la detección de ataques informáticos juega un papel muy importante en la seguridad del procesamiento de datos en los sistemas informáticos y muestra la importancia de la seguridad información, permitiendo tomar conciencia de la importancia de la información como un activo más de una organización, permitiendo prevenir ataques utilizando mecanismos de defensa. Izquierdo y Tafur [4], en su tesis "Mecanismos de Seguridad para Contrarrestar Ataques Informáticos en Servidores Web y Base de Datos", realizaron la comparación de mecanismos de seguridad que fueron capaces de contrarrestar ataques informáticos, con el propósito de capturar información de los intrusos y aumentar la seguridad en los servidores web y base de datos.

En la actualidad el internet es la red más grande del mundo donde se encuentra la mayor cantidad de información de instituciones públicas y privadas, debido a que muchas de las actividades que se realizan de forma cotidiana en las instituciones dependen en mayor o menor medida de sistemas informáticos.

El crecimiento de Internet y de los servicios telemáticos ha contribuido a que hoy en día cualquier computadora conectada a internet este expuesta a diversas amenazas que invaden las redes.

Actualmente se realizan ataques con mayor frecuencia a sistemas informáticos, una consecuencia es el aumento en el número de ataques informáticos que ponen en riesgo la seguridad de la información comprometiendo la confidencialidad, integridad y disponibilidad de la información de las instituciones.

Debido a la frecuencia de los ataques a sistemas informáticos en la actualidad cada vez es más normal escuchar que instituciones públicas y privadas fueron víctimas de ataques informáticos, a continuación, se exponen algunos casos publicados en periódicos digitales:

- Según el periódico digital La Razón informa que: Sitios de medios estatales sufren ataque informático [5].
- Los sitios en internet de los medios estatales Patria Nueva, el periódico Cambio y la Agencia Boliviana de Información (ABI) sufrieron un ataque informático que redireccionó sus páginas web a una página de contenido pornográfico.
- Según el periódico digital El Diario informa que: Un ciberataque se registra en Bolivia cada día [6].
- Un ataque cibernético por día se registra en Bolivia, según el reporte del representante del colectivo ciudadano "Más y mejor internet para Bolivia", Mario Durán, fundamentado en mapas de ciberataques diseminados por la red.
- Según el periódico digital El Deber informa que: Ciberataque golpea a gran escala en todo el mundo [7].

  Un ataque informático a gran escala sacudió al mundo ayer, al parecer aprovechando una falla expuesta en

Para referenciar este artículo (IEEE):
[N] J. Calle, «Fases de un ataque a un Sistema Informático» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 52-55, 2020.

documentos filtrados de la Agencia de Seguridad Nacional (NSA) de EEUU. El ataque se produjo mediante un virus "*ransomware*", una técnica utilizada por los hackers que bloquea archivos de los usuarios a menos que paguen a los atacantes una suma designada en la moneda virtual *Bitcoin*. El Departamento de Seguridad Nacional de Estados Unidos. dijo ser consciente de que las infecciones por el *ransomware* alcanzaron a "varios países". "Hasta ahora hemos detectado más de 75.000 ataques en 99 países", dijo Jakub Kroustek, de la empresa de seguridad Avast.

La investigación de esta problemática se realizó por el interés de conocer las fases de un ataque a un sistema informático. Considerando que en la actualidad los ataques a sistemas se realizan con mayor frecuencia generando un gran problema para las instituciones públicas y privadas, debido a que tienen una infraestructura tecnológica en crecimiento, de la cual dependen muchos de los procesos y el funcionamiento. La mayor parte de la información de las instituciones, se encuentra en los diferentes sistemas informáticos, equipos de computación y también existe información en formato físico.

Por lo antes mencionado, el objetivo de esta investigación es describir las fases de ataque a un sistema informático.

Dentro de los principales conceptos están:

A. Vulnerabilidad

De acuerdo a la seguridad informática, el término de vulnerabilidad hace referencia a "un estado viciado en un sistema informático que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas" [8].

Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario.
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
- Permitir a un atacante hacerse pasar por otra entidad.
- Permitir a un atacante realizar una negación de servicio.

B. Amenaza informática

Una amenaza informática es toda circunstancia, evento o persona que tiene el "potencial de causar daño a un sistema" [8]. En forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

C. Información

La información es "conjunto de datos organizados en poder de una entidad que poseen valor para la misma" [9]. Y en consecuencia necesita ser debidamente protegido.

Al hablar de información, se refiere sin importar la forma que esta adopte, a la documentación impresa o escrita, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Este activo se debería proteger de forma correcta mediante los controles de seguridad independientemente de la forma que este tome o los medios por los que se comparta o almacene.

D. Seguridad de la información

La seguridad de la información se refiere a la protección de una gama de amenazas para salvaguardar la continuidad de las operaciones del negocio sean estas ocasionadas dentro o fuera de la organización, disminuyendo los daños que estas amenazas causarían a la organización y aumentar las oportunidades de negocios. "Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización" [9].

Los pilares de la seguridad de la información son:

- Confidencialidad: Hace referencia a la cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización.
- Integridad: Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.
- Disponibilidad: Es aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.

Estos 3 pilares fundamentales de la seguridad de la información son parte de los objetivos que intentan comprometer los atacantes.

II. MÉTODOS

El presente trabajo de investigación tiene un enfoque cualitativo, porque está orientada a describir las fases de un ataque a un sistema informático. El diseño de investigación es no experimental porque se basa en la observación y de corte transversal porque se realizó una sola vez la recopilación de la información. El tipo de investigación es exploratorio, porque se realizó la búsqueda de información referente a la investigación. El método de investigación es inductivo, porque a partir de la información recopilada se realizó un análisis de esta información para realizar una conclusión general.

El tamaño de la muestra incluye un total de 17 documentos digitales recopilados de revistas digitales, repositorios académicos, bibliotecas digitales y sitios web.

Primero se realizó la investigación bibliográfica, se buscó documentos afines a la investigación, recopilando la información de diferentes fuentes consultadas que corresponden a: revistas digitales, repositorios académicos, bibliotecas digitales y sitios web. Segundo se realizó el análisis de la información recopilada, que comprende las relaciones establecidas entre criterios de diversos autores sobre la problemática. Tercero se realizó la evaluación de toda la información analizada para elaborar la descripción de las fases de un ataque a un sistema informático.

III. RESULTADOS

Del análisis de la información recopilada se puedo evidenciar que existen 5 fases por las cuales suele pasar un ataque a un sistema informático que son: reconocimiento, exploración, obtener acceso, mantener el acceso, borrar huellas.

Los principales documentos que se utilizaron para realizar la descripción de las fases de un ataque a un sistema informático se presentan en la Tabla I, donde se puede observar que cada autor tiene su forma de explicar cada fase.

TABLA I. RESULTADO DE ANÁLISIS DE DOCUMENTOS PRINCIPALES CONSULTADO

Documento recopilado	Resultado del análisis
Documento de Vallejos, Marcillo y Uvidia [10].	En reconocimiento indica que se recurre a diferentes recursos de internet como Google, entre tantos otros, para recolectar datos del objetivo. En exploración indica que se tiene que obtener la información de la víctima utilizando algunas herramientas como *network mappers, port* entre otros. En obtener acceso indica que se bebe realizar la explotación de vulnerabilidades utilizando técnicas como ataques de *buffer overflows, denial of service* entre otros. En mantener el acceso indica que se beben implantar herramientas que le permitan volver a acceder. En borrar de huellas indica que debe borrar todas las huellas que fue dejando durante la intrusión.
Documento de Guillinta y Merino [11].	En reconocimiento indica que es donde se llevara a cabo la recolección de la mayor cantidad de información referente a la empresa u objetivo. En escaneo indica que se logra obtener una visión de la situación actual de la empresa u objetivo. En obtener acceso indica que es la intrusión propiamente dicha ya que es en esta fase donde se procede a realizar los ataques para ingresar al sistema informático. En mantenimiento de acceso indica que se debe realizar de manera que según sea requerido por el atacante se pueda volver a ingresar al sistema. En eliminación de huellas indica que es importante para el atacante, asegurar que no se tenga conocimiento de las acciones que hayan sido realizadas dentro del sistema informático vulnerado.
Documento de Méndez [12].	En reconocimiento indica que se obtiene la información de la potencial víctima. En exploración indica que se tratar de obtener información sobre el sistema víctima. En obtener acceso indica que se comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema. En mantener el acceso indica que se debe implantan herramientas que le permitan volver a acceder. En borrar huellas indica que se eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

Nota. Fuente: elaboración propia

Se presenta el resultado final del análisis de toda la información recopilada en la Tabla II, que describe las fases de ataque a un sistema informático.

TABLA II. RESULTADO DEL ANÁLISIS DE LA INFORMACIÓN RECOPILADA

Fases de un ataque a un sistema informático	Descripción de la fase
Fase 1: reconocimiento	En esta fase se obtiene toda la información necesaria del objetivo y/o victima que puede ser una persona u organización, antes de lanzar un ataque. Consta de 2 tipos de reconocimiento pasivo y activo. El reconocimiento pasivo es cuando se obtiene información sin tener interacción directa con el objetivo. Se puede utilizar Google hacking, ingeniería social, monitorización de redes de datos. p.ej., *sniffing*, etc. El reconocimiento activo es cuando se tiene una interacción directa con el objetivo es decir que el atacante envía algún tipo de acción y tiene una respuesta. Se prueba la red para detectar hosts accesibles, puertos abiertos, localización de *routers*, detalles de sistemas operativos y servicios. Esta fase puede tomar bastante tiempo, ya que se analiza toda la información obtenida y se crea una estrategia para lanzar el ataque con mayor precisión.
Fase 2: exploración	En esta fase se utiliza toda la información que se obtuvo en la fase del reconocimiento, para identificar vulnerabilidades específicas. Por ejemplo, si en la fase 1 el atacante descubre que su objetivo o su víctima utiliza como sistema operativo, en la computadora atacada, Windows 7, entonces buscará vulnerabilidades específicas que tenga ese sistema operativo para saber por dónde atacarlo. Entre las herramientas que se utilizan durante la exploración se encuentra el *network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.* Con estas herramientas se puede explorar la red y los hosts en busca de más vulnerabilidades que le permitan el acceso al sistema.
Fase 3: obtener acceso	Esta fase es la más importante porque comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración. La explotación de vulnerabilidades puede ocurrir localmente, sin estar conectado, sobre la red de área local, o sobre el internet. Para ello, se suelen utilizar herramientas específicamente construidas para tal fin, conocidas como *exploit.* Las técnicas que generalmente utiliza el atacante, son ataques de *buffer overflows* (desbordamiento de *buffer*), *denial of service* (denegación de servicio), sesión *hijacking* (secuestro de sesión), y *password cracking* (romper o adivinar claves usando varios métodos como: *dictionary attack y brute force attack*).
Fase 4: mantener el acceso	En esta fase el atácate ya ha conseguido acceder al sistema y su prioridad es mantener ese acceso, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a internet. Para ello, suelen usar técnicas de *backdoor* (puertas traseras), *rootkits* (encubridor) y *trojans* (troyanos) para ganar acceso a cuentas de usuario con privilegios de administrador que faciliten el posterior acceso del atacante al sistema afectado. Con el fin de hacer más daño a la víctima, controlando el sistema que ya logró acceder. Al tener el control del sistema atacado, se puede usar el sistema como plataforma de lanzamiento de nuevos ataques informáticos, robar información personal como números de tarjetas de crédito u otra información clave, alterar el funcionamiento de aplicaciones de software y los datos del sistema atacado.
Fase 5: borrar huellas	En esta fase el atacante intentará borrar toda evidencia de cualquier posible rastro de sus actividades realizadas durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red, para así poder seguir accediendo al sistema atacado cuando se quiera. Además, es importante el borrando de huellas para anula la posibilidad de ser atrapado. Por lo general el atacante buscar eliminar o modificar los archivos de registro (*log*) o alarmas del sistema de detección de intrusos (IDS).

Nota. Fuente: elaboración propia

IV. Discusión

En esta investigación al determinar las fases de un ataque un sistema informático, se pude encontrar que existen 5 fases por las cuales suele pasar un ataque a un sistema informático estas fases son: Reconocimiento, Exploración, Obtener Acceso, Mantener el Acceso, Borrar Huellas. Estos resultados son corroborados por Guamán [13], en su tesis "Anatomía de un ataque informático", quien en su investigación llega a concluir que existen 5 fases que son: Reconocimiento, Exploración, Obtener Acceso, Mantener Acceso y Borrar Huellas en ese orden. Al comparar las descripciones de cada fase se puede observar que tiene el mismo objetivo.

En tal sentido, bajo lo referido anteriormente y al analizar estos resultados, confirmamos que para realizar un ataque a un sistema informático se tiene que seguir las 5 fases, porque contribuye de manera favorable para ingresar a un sistema sin autorización y tener el control del mismo.

V. Conclusiones

En conclusión, todo usuario que dispone de internet esta automáticamente expuesto a las intrusiones que invaden las redes, por lo que conociendo al enemigo y sus tácticas es como uno puede tomar las medidas de seguridad, necesarias o indispensables para evitar cualquier posible tipo de ataque.

Conocer las 5 fases de un ataque a un sistema informático nos ayuda a actuar de manera proactiva frente a los posibles ataques informáticos.

Se puede indicar que la seguridad es un campo muy amplio y en crecimiento, que se debe brindar la mayor atención posible, ya que existen cada vez más personas malintencionadas que intentan obtener datos o acceso a sistemas vinculados o propios de instituciones para indisponer los servicios u obtener información confidencial.

Se recomienda realizar capacitación sobre temas de seguridad de la información y prevención de ataques informáticos a todo el personal de la organización.

Referencias

[1] J. Mieres, «Ataques informáticos,» enero 2009. [En línea]. Available: https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnx3ZWJzaXRlZGF2aWR0aWNvbmF8Z3g6MmNhYzY3ZTg2YmYzOTMyMg. [Último acceso: 20 dic 2019].

[2] D. J. Mamani, «http://www.revistasbolivianas.org.bo/,» 12 junio 2013. [En línea]. Available: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a29.pdf. [Último acceso: 28 ene 2020].

[3] P. J. Plaza, «UNAP Repositorio Institucional Digital,» 2014. [En línea]. Available: http://repositorio.unapiquitos.edu.pe/bitstream/handle/UNAP/4485/Percy_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y. [Último acceso: 28 ene 2020].

[4] J. Izquierdo y T. E. Tafur, «Universidad Señor de Sipan,» 04 dic 2017. [En línea]. Available: http://repositorio.uss.edu.pe/bitstream/handle/uss/4062/TESIS_IzquierdoCabrera_TafurCallirgos.pdf?sequence=1&isAllowed=y. [Último acceso: 28 ene 2020].

[5] M. Basualdo, «La Razón» 19 julio 2015. [En línea]. Available: http://204.11.233.100/nacional/Sitios-medios-estatales-ataque-informatico_0_2309769115.html. [Último acceso: 20 dic 2019].

[6] «El Diario» 07 julio 2015. [En línea]. Available: https://m.eldiario.net/?n=66&a=2015&m=07&d=07. [Último acceso: 21 diciembre 2019].

[7] «El Deber» 13 mayo 2017. [En línea]. Available: https://eldeber.com.bo/87022_ciberataque-golpea-a-gran-escala-en-todo-el-mundo. [Último acceso: 21 dic 2019].

[8] J. Guerrero, «Seguridad Informática» 04 agosto 2015. [En línea]. Available: https://www.mindmeister.com/es/526521671/seguridad-informatica. [Último acceso: 21 dic 2019].

[9] M. A. Paredes, «EMA entidad mexicana de acreditación a.c.» 24 agosto 2017. [En línea]. Available: http://www.ema.org.mx/sectorsalud/descargas/dia2/Aplicaciones_informaticas_para_la_consulta.pdf. [Último acceso: 22 dic 2019].

[10] C. Vallejos, P. Marcillo y M. Uvidia Vélez, «CIDE Centro de Investigación y Desarrollo Profesional,» 2018. [En línea]. Available: http://www.cidepro.org/images/pdfs/ids.pdf. [Último acceso: 23 ene 2020].

[11] O. Guillinta y J. L. Merino, «Repositorio Académico UPC,» agosto 2016. [En línea]. Available: https://repositorioacademico.upc.edu.pe/handle/10757/620848. [Último acceso: 23 ene 2020].

[12] D. L. Méndez Ávila, «Universidad Israel,» noviembre 2011. [En línea]. Available: http://157.100.241.244/bitstream/47000/164/1/UISRAEL-EC-SIS-378.242-397.pdf. [Último acceso: 24 enero 2020].

[13] B. V. Guamán, «Universidad del Azuay 50 Años,» 2015. [En línea]. Available: http://dspace.uazuay.edu.ec/bitstream/datos/5046/1/11485.pdf [Último acceso: 27 enero 2020].

Breve CV del autor

José Luís Calle Condori es Licenciado en Informática con mención en Ingeniería en Sistemas Informáticos de la Universidad Mayor de San Andrés, La Paz. Diplomado Docencia Universitaria en educación superior UMSA, Centro Psicológico y de Investigación en Educación Superior (CEPIES). Email: jlc_inf@yahoo.es