Ethical Hacking: Conciencia de Seguridad

Gustavo Callejas Espinoza
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
gustavo.bionicle@gmail.com

***Resumen*—Como parte de un buen proceso de seguridad en las organizaciones, el test de penetración o hackeo ético se ha convertido en una herramienta fundamental para validar el nivel de seguridad en todo tipo de empresas, permitiendo descubrir fallas en los protocolos establecidos o en las características de los productos o procesos de la compañía.**

Palabras clave— Hacking, ética, vulnerabilidad, empresa.

I. INTRODUCCIÓN

La era actual es la de la información. A diferencia de otras épocas, el valor que tiene la información hoy en día, es muy alto. Esto se debe a que países, compañías y hasta organizaciones sin fines de lucro manejan una gran cantidad de información ya sea financiera, contable, de personas, procesos, resultados en el mercado y otros muchos.

Debido a la que información se ha vuelto uno de los cimientos de una empresa, la pérdida de la misma puede comprometer el funcionamiento o su éxito. Esto hace que se vuelva sensible la adquisición de nuevas tecnologías a una empresa para tener un funcionamiento eficaz, ya que puede comprometer la integridad y la seguridad de su información [1].

Llámelos hackers, crackers, intrusos o atacantes, todos son intrusos que intentan entrar en sus redes y sistemas. Algunos lo hacen por diversión, algunos lo hacen con fines de lucro o algunos simplemente lo hacen para interrumpir sus operaciones y tal vez ganar algún reconocimiento. Aunque todos tienen una cosa en común; están tratando de descubrir una debilidad en su sistema para explotarla.

También existen los hackers éticos que emplean las mismas herramientas y técnicas que los intrusos, pero no dañan el sistema ni roban información. En cambio, evalúan la seguridad de los sistemas de destino e informan a los propietarios con las vulnerabilidades que encontraron e instrucciones sobre cómo remediarlas. El vasto crecimiento de Internet ha traído muchas cosas buenas como comercio electrónico, correo electrónico, fácil acceso a grandes almacenes de material de referencia, etc. Como, con la mayoría de los avances tecnológicos, también hay otro lado: piratas informáticos criminales que robarán secretamente la información de la organización. y transmitirlo por Internet. Estos tipos de hackers se denominan “Hackers de sombrero negro (*Black Hat Hacker*)”. Entonces, para superar estos problemas importantes, surgió otra categoría de hackers llamados “Hackers de sombrero blanco (*White Hat Hacker*)” [2].

Es importante que se deba partir por la identificación de las vulnerabilidades. Para esto es necesario tener un pensamiento fuera de lo común, porque los atacantes podrían no poseer el conocimiento, ni la información suficiente, pero si el tiempo para intentar hasta que el resultado sea exitoso.

II. MARCO TEÓRICO

A. Vulnerabilidades en los sistemas informáticos

Una vulnerabilidad es alguna característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente. Las vulnerabilidades pueden provenir de muchas fuentes, desde el diseño o implementación de los sistemas, los procedimientos de seguridad, los controles internos y otros; se trata en general de protecciones inadecuadas o insuficientes, tanto físicas como lógicas, procedimentales o legales de alguno de los recursos informáticos [3]. Las vulnerabilidades al ser explotadas resultan en fisuras en el esquema de la seguridad con potenciales impactos nocivos para la organización. Las vulnerabilidades pueden ser encontradas en:

- Fallas en el diseño o construcción de programas.
- Uso de computadoras, programas y equipos de red de tipo genérico en aplicaciones críticas.
- Confianza excesiva en algún único dispositivo u oficina de seguridad.
- Incumplimiento de las políticas y procedimientos de seguridad.
- Fallas de seguimiento en el monitoreo o indicadores de seguridad.
- Ausencia de gobernanza de los activos informáticos.
- Cambio frecuente de elementos de la plataforma informática.
- Falta de una adecuada segregación de funciones.
- Planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas.
- Ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas.
- Equipos, programas y redes "heredados" de generaciones tecnológicas anteriores.
- Errores inherentes al diseño de microprocesadores y microcódigos que se encuentran en rutinas básicas o "núcleo" de los sistemas, o en el encriptado o virtualización.
- Falta de concientización del personal.

Para referenciar este artículo (IEEE):

[N] G. Callejas, «Ethical Hacking: Conciencia de Seguridad» *Revista PGI. Investigación, Ciencia y Tecnología en Informática,* nº 7, pp. 43-46, 2020.

1) Vulnerabilidades en el mundo

Kaspersky Lab registro los ataques durante el mes de noviembre del año 2016, donde el mayor número de ataques fue el 14 de noviembre con 334407 ataques registrados [4].

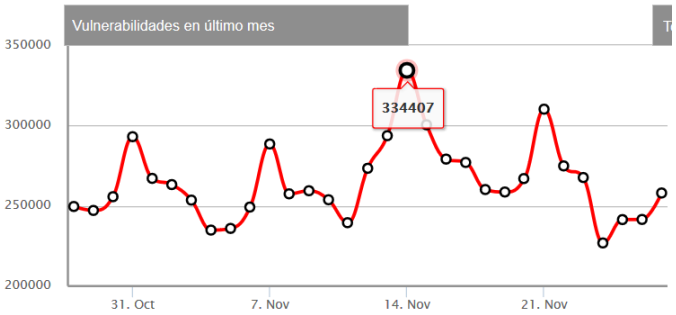

Fig. 1. Vulnerabilidades registradas en el mundo durante el mes de noviembre de 2016

2) Vulnerabilidades en Latinoamérica

Según la encuesta de ESET en Latinoamérica, la principal preocupación es "Vulnerabilidades de software y sistemas" con el 58% de las respuestas afirmativas, seguido por "Malware" (54%) y, en el tercer puesto, el "Acceso indebido la información" (46%) [5].

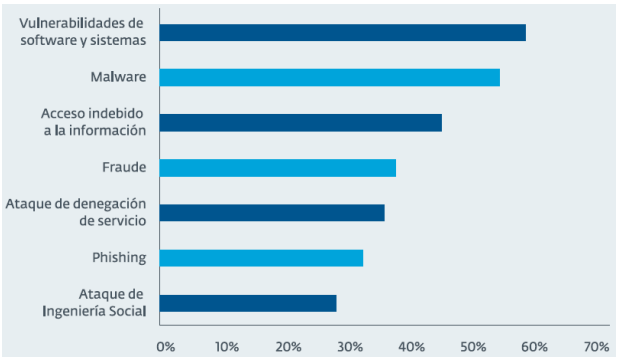

Fig. 2. Ataques informáticos en Latinoamérica

3) Vulnerabilidades en Bolivia

En Bolivia se registraron al menos 23 ataques a páginas web pertenecientes al estado, una de ellas fue la Armada, la mayoría de los ataques estaban relacionados con la demanda marítima de Bolivia contra Chile [6].

Casos similares ocurrieron el año 2016, fueron hackeadas las páginas web de la Defensoría del Pueblo, la Gobernación de Santa Cruz, la Dirección General de Migración, la Escuela de Idiomas del Ejército, la Escuela Militar de Ingeniería (EMI), y del Sistema de Contrataciones Estatales (SICOES) [7]. Los procedimientos de ataque fueron difundidos en YouTube [8].

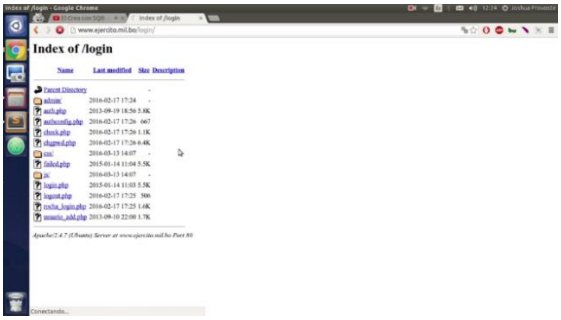

Fig. 3. Ataque a la página web del ejército de Bolivia

B. Ataques más peligrosos

- Gusano Morris, el gusano es un virus que se divulga por medio de los correos electrónicos, como es el caso del SIRCAM. El primer gusano lo realizo Robert Morris en 1988 cuando estaba en la universidad [9].
- Carbanak. Los ataques comenzaron en 2013 y fueron dirigidos contra más de 100 bancos, sistemas de pagos electrónicos y otras instituciones en más de 30 países. Los ataques aún se están llevando a cabo, de acuerdo con un comunicado de la firma de ciberseguridad Kaspersky, que fue la primera en reportar el hecho en una exclusiva de The New York Times. Los reportes preliminares decían que la suma extraída era de 300 millones de dólares (US), pero ahora Kaspersky dijo que los robos ascienden hasta 1,000 millones de dólares (US) [10].
- WannaCry. El ransomware que ataca a las redes usando SMBv1, un protocolo que ayuda a los equipos a comunicarse con las impresoras y otros dispositivos conectados a la red. Esta versión, diseñada en 2003, dejó a los equipos expuestos a los hackers y esta vulnerabilidad se denominó MS17-010. Microsoft creó un parche para corregirla a principios de marzo para las versiones de Windows a las que seguía ofreciendo soporte, pero cualquier persona que no lo instalara se convertía en blanco fácil para los hackers que habían diseñado WannaCry [11].

C. Hacking Ético

El hacking ético es una forma de hacer una evaluación de seguridad. Los resultados de un hackeo ético son un informe detallado de los hallazgos, así como un testimonio de que un pirata informático con una cierta cantidad de tiempo y habilidades puede o no puede atacar con éxito un sistema u obtener acceso a cierta información. El hacking ético se puede categorizar como una evaluación de seguridad, un tipo de capacitación, una prueba para la seguridad de un entorno de tecnología de la información. El hacking ético muestra los riesgos que enfrenta un entorno de tecnología de la información y se pueden tomar acciones para reducir ciertos riesgos o aceptarlos [2].

Consiste en buscar e identificar vulnerabilidades en los sistemas de la organización que fue atacada, para poder determinar de dónde se produjo la fuga o el hueco de seguridad que encontró el atacante, con ello poder mitigarlos, reducir los riesgos y evitar fugas de información que es sensible [12]. Por medio de pruebas de penetración, intenta de múltiples formas burlar la seguridad para reportar las vulnerabilidades a la empresa para que así puedan mejorar su seguridad, generalmente un hacker ataca de la siguiente forma:

- Fase 1 - Reconocimiento: El hacker hace un previo reconocimiento pasivo a cualquier ataque, recopila información sobre el objetivo a atacar. Como ser: Hosts accesibles, puertos abiertos, localización de Routers, detalles de sistemas operativos y servicios.
- Fase 2 - Escaneo: se escanean los diferentes medios por donde se puede hacer el ataque, como por ejemplo la red, pero esta se realiza ya con información de la fase previa.

- Fase 3 - Ataque (obtener acceso): se refiere al ataque propiamente dicho, por ejemplo, hacer uso de un exploit o bug, para obtener una contraseña.
- Fase 4 - Ataque (mantener acceso): mantenimiento del acceso, se trata de seguir teniendo los privilegios obtenidos.
- Fase 5 - Borrado de evidencia: Borrar las evidencias con lo que pueda ser descubierto.

III. Discusión

A. *Las empresas y la seguridad informática*

En las empresas, se debe adquirir una cultura en todos los empleados, en la cual se incluya que, para la organización, la información es uno de los aspectos más importantes de su quehacer diario y que la protección y la calidad de esa información debe mantenerse en todo momento. Por esto para un empleado de la empresa debe ser importante tener en cuenta la seguridad informática y que cualquier acto en contra de este aspecto de la información, puede causarle pérdidas irreparables a la organización [13].

El buen uso de las herramientas informáticas (e-mail, usuarios y contraseñas de sistemas de información, bases de datos, aplicativos, antivirus, entre otros) redundará en que existan menos inconvenientes más adelante. El mal uso de cualquiera de estos subsistemas de información puede generar una vulnerabilidad y provocar un riesgo de ataque.

Es muy importante en una empresa que todos los sistemas de cómputo y todos los componentes del sistema de información estén configurados correctamente, que todos los sistemas tengan las últimas actualizaciones, pues esto evitará posibles fallos de seguridad.

B. *Cultura de seguridad informática*

Las empresas pierden miles de millones de dólares al año como resultado del hackeo y otras infracciones informáticas. Muchas veces, el costo real no puede evaluarse porque los efectos de una violación de seguridad pueden persistir durante años después del ataque real. Las empresas pueden perder la confianza del consumidor y, en muchos casos, son legalmente responsables de cualquier pérdida para sus clientes. El costo de recuperarse de un ataque puede extenderse rápidamente: honorarios legales, honorarios de investigación, desempeño de acciones, gestión de reputación, atención al cliente, etc. Las empresas y, más recientemente, los consumidores, están invirtiendo cada vez más dinero para prevenir un ataque antes de que realmente suceda. Las empresas que almacenan datos personales y financieros de los consumidores están tomando medidas adicionales para garantizar la seguridad de los datos [2].

En la cultura de la seguridad informática no se trata de saber, como ocurría en la escuela, colegio o universidad para simplemente aprobar; lo que sugiere la cultura de la seguridad informática es el saber para poder razonar, valorar y, en consecuencia, actuar freten a las tecnologías de información (TI). Para un empleado de la empresa debe ser importante tener en cuenta la seguridad informática y que cualquier acto en contra de este aspecto de la información [14].

El desarrollo de la cultura debe llegar a toda la estructura de la organización, empezando por la alta gerencia, que es la que tiene que apoyar sin vacilaciones las políticas a seguir en materia de seguridad informática. Sus políticas deben ser flexibles, para ir adaptándola a los cambios de la propia organización, a la evolución de las tecnologías que el mercado cada día pone a nuestra disposición, y a las nuevas vulnerabilidades que puedan surgir en un mundo cambiante y evolutivo como el que hoy vivimos. Una vez establecidas las políticas, la cultura de seguridad exige que se den a conocer a la organización; es aquí donde se debe tener el conocimiento y la diligencia de saber explicar y hacer comprender el por qué se ha marcado esa política concreta y no otra.

C. *Limitaciones del Hacking ético*

El hacking se basa en el principio simple de encontrar las vulnerabilidades de seguridad en los sistemas y redes antes que los hackers, desafortunadamente, las definiciones comunes de tales pruebas generalmente se detienen en los sistemas operativos, la configuración de seguridad y el nivel de "errores". Al limitar el ejercicio al nivel técnico mediante la realización de una serie de pruebas puramente técnicas, una prueba de hacking ético no es mejor que un "diagnóstico" limitado de la seguridad de un sistema.

El tiempo también es un factor crítico en este tipo de pruebas. Los hackers tienen una gran cantidad de tiempo y paciencia para encontrar vulnerabilidades en el sistema. Lo más probable es que contrate a un "tercero de confianza" para que realice estas pruebas por usted, por lo que para usted el tiempo es dinero. Otra consideración en esto es que al utilizar un "tercero" para realizar sus pruebas, estará proporcionando "información privilegiada" para acelerar el proceso y ahorrar tiempo. La oportunidad de descubrimiento puede verse limitada ya que las pruebas solo pueden trabajar aplicando la información que se les ha proporcionado.

Una limitación adicional de este tipo de prueba es que generalmente se enfoca en áreas externas en lugar de internas, por lo tanto, es posible que solo pueda ver la mitad de la ecuación. Si no es posible examinar un sistema internamente, ¿cómo se puede establecer que un sistema está "a salvo de ataques", basándose únicamente en pruebas externas? Básicamente, este tipo de prueba por sí solo nunca puede proporcionar garantías absolutas de seguridad. En consecuencia, estas técnicas de evaluación pueden parecer, al principio, ser fundamentalmente defectuosas y tener un valor limitado, porque es posible que no se descubran todas las vulnerabilidades [2].

IV. Conclusiones

Para poder contrarrestar estos malos inconvenientes existen muchas soluciones en nuestra actualidad, con una gran cantidad de herramientas desarrolladas especialmente para cumplir con la función de proteger nuestra información, existe herramientas de con licencia propietario y otras que son software libre, cada una de ellas con sus diferentes características y valor económico.

Se debe tomar en cuenta que no se puede proteger en su totalidad la información, ya que existen muchos riesgos dentro o fuera de la organización, sin embargo, se debe estar preparado y dispuesto a reaccionar con rapidez contra los ataques las amenazas y vulnerabilidades que invaden las redes de internet.

Muchas de la empresa implementan políticas de seguridad, esto a su vez provoca un gran reto a la misma, por lo contrario, se sabe que es impredecible sobre todo si se tiene en cuenta que cada vez los ataques de hackers son más constantes hacia las más grades instituciones públicas o privadas [15].

El hacking tiene tanto sus beneficios como sus riesgos. Los hackers son muy diversos. Pueden declarar en quiebra a una empresa o proteger los datos, aumentando los ingresos de la empresa. Mientras que los *White Hat Hackers* éticos ayudan a comprender las necesidades de seguridad de las empresas, los *Black Hat Hackers* se inmiscuyen ilegalmente y dañan la red para sus beneficios personales. lo que puede permitir que se viole su sistema de seguridad. Los hackers éticos ayudan a las organizaciones a comprender los problemas ocultos actuales en sus servidores y red corporativa.

El hacking ético es una herramienta que, si se utiliza correctamente, puede resultar útil para comprender las debilidades de una red y cómo podrían explotarse. Esto también concluye que el hacking es un aspecto importante del mundo informático. Se trata de ambos lados de ser bueno y malo. El hacking ético juega un papel vital en el mantenimiento y el almacenamiento de mucha información secreta, mientras que la piratería maliciosa puede destruirlo todo. Todo lo que depende es la intención del hacker. Es casi imposible llenar la brecha entre la piratería ética y maliciosa, ya que la mente humana no se puede conquistar, pero las medidas de seguridad pueden reforzarse.

REFERENCIAS

[1] E. Carabaguíaz, «Importancia del Aprendizaje de Ciberseguridad ante los Riesgos de las Tecnologías de Información,» *Revista de la Facultad de Tecnología de Información y Comunicación.*, vol. 1, nº 1, pp. 3-13, 2017.

[2] S. Bhawana, N. Ankit y K. Shashikala, «Study Of Ethical Hacking,» *International Journal of Computer Science Trendsand Technology (IJCST)*, vol. 2, nº 4, pp. 6-10, 2014.

[3] J. Voutssas, «Preservación documental digital y seguridad informática,» *Investigación bibliotecológica*, vol. 24, nº 50, pp. 127-155, 2010.

[4] Kaspersky Lab., «Secure List: Estadísticas,» 2016. [En línea].

[5] ESET, «Security Report Latinoamérica,» 2016. [En línea].

[6] A. Cuevas, «En 6 meses, al menos 23 páginas web del Estado fueron hackeadas,» *La Razón*, 2015.

[7] G. Tapia, «Siete páginas de instituciones públicas de Bolivia son hackeadas y difunden datos,» *La Razón*, 2016.

[8] J. Provoste, «Ejército de Bolivia Ejercito.mil.bo Gobierno de Bolivia,» 2016. [En línea]. Available: https://www.youtube.com/watch?v=YF28jWkOvYc.

[9] F. Ficarra, «Virus Informáticos: Entre el negocio y el temor,» *Centro Internacional de Estudios Superiores de comunicación para América Latina*, pp. 62-69, 2002.

[10] Ó. Gutiérrez, *La banda Carbanak está detrás del robo digital más grande de la historia*, 2015.

[11] Avast, «WannaCry,» s.f. [En línea]. Available: https://www.avast.com/es-es/c-wannacry.

[12] S. Castro, «White Hat: Hacking Ético,» 2017.

[13] C. Useche, «Hacking ético, detección de vulnerabilidades en sistemas informáticos,» 2015.

[14] D. Parra, «Gestión del riesgo en la seguridad informática: "Cultura de la auto seguridad informática",» *Ensayo de fin de especialización, Universidad Militar Nueva Granada, Bogotá, Colombia*, 2012.

[15] C. Albarracín, *Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas (Tesis de pregrado)*, Instituto Tecnológica Israel, Cuenca, 2011.

Breve CV del autor

Gustavo Callejas Espinoza es Licenciado en Informática, mención: Ingeniería de sistemas informáticos por la Universidad Mayor de San Andrés, La Paz (2015). Diplomado en educación superior, mención: organización y administración pedagógica del aula, UMSA-CEPIES (2017). Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría Informática en el Postgrado en Informática UMSA. Email: gustavo.bionicle@gmail.com.