WHITE HAT: HACKING ÉTICO

Castro, Cubillos, Sandra, Milena
sandra.cubillos21@gmail.com
Universidad Piloto de Colombia

***Resumen*—** Como parte de un buen proceso de seguridad en las organizaciones, el test de penetración o hackeo ético se ha convertido recientemente 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.

Así como en un automóvil se debe garantizar que las cerraduras sean seguras para evitar que un ladrón pueda entrar y llevárselo, en un proceso de una organización el test de penetración permitirá conocer las posibles fallas o huecos en la seguridad, que de no ser tratados a tiempo, puede llevar robo de información o dinero, con las consecuencias que esto implica para la empresa, sus empleados y su reputación.

***Índice de Términos*—** Hacking, ética, vulnerabilidad, prueba de penetración.

***Abstract* —** As part of a good process of security in organiza**tions,** the penetration test of ethical hacking has recently become a fundamental tool to validate the level of security in all types of companies, allowing to discovering failures in established protocols or in the characteristics of the products or the processes of the company.

Just as in an automobile it is necessary to ensure that the locks are safe to prevent a thief from entering and carrying, in an organization process the penetration test allows to know the possible failures of "gaps" in the security, that of no service treated on time, you can carry out the money information, with the implications that it implies for the company, its employees and its reputation.

***Keywords*—** Hacking, ethics, vulnerability, penetration test.

I. INTRODUCCIÓN

Este documento se encuentra basado en la comprensión del artículo: "About Penetration Testing", publicado por la sociedad IEEE.

El cual abarca un tema muy interesante en la rama de la seguridad informática, como lo son las pruebas de penetración y la implicación que abarcan.

La prueba de penetración es un análisis de un aspecto del sistema. Lo que significa que un archivo confidencial puede ser leído por un programa o una herramienta específica que pueda ser ejecutado y los datos en el sistema pueden ser cambiados, esto implica que el sistema pueda ser reconfigurado, es decir, que puedan ser alteradas las propiedades de seguridad informática.

Sin embargo, cuando se van a realizar estos análisis, es necesario dejar desde un principio cual es el alcance y definir el objetivo genérico. Porque no se trata de solo saber si es posible o no el ingreso al sistema, si no que tan difícil es hacerlo aprovechando las vulnerabilidades que este posea.

Por eso es importante que se deba partir por la identificación de estas 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.

Existe un código ético conocido popularmente como: ley del hacking, que obliga a que los estudiantes aprendan a apreciar las cuestiones implicadas, y piensen en las consecuencias de sus acciones.

En la actualidad se divaga sobre la respuesta a la pregunta: ¿Es delito el hacking ético? Según el artículo 197.3: "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho de excluirlo, será castigado con penas de prisión de seis meses a dos años".

Según la interpretación de esta ley, se encuentran dos puntos de vista, a favor y en contra. Los individuos que se encuentran a favor declaran que el hacking ético no cumple los requisitos para ser considerado un delito, porque ingresa con la única intención de obtener vulnerabilidades y poder avisarlas para que sean corregidas. Y las personas que se encuentran en contra, repercutan que el simple hecho de ingresar ya es delito.

II. HACKING ÉTICO

El hacking ético consiste en una auditoría, que es realizada por profesionales del área de seguridad de la información, estas personas utilizan sus habilidades y conocimientos, para identificar las brechas de seguridad en una entidad y son llamados como pentester. La actividad que ellos realizan se conoce con el nombre de hacking ético o pruebas de penetración.

Las pruebas de penetración nacieron de los primeros ataques informáticos que sucedieron en las organizaciones, atacando la confidencialidad de la información sensible de los clientes y empleados, de esta manera se vieron afectadas las entidades por grandes pérdidas de dinero y perjudica su reputación, hasta que los clientes por miedo a que su información fuese accedida por hackers, optaron por trasladarse a otras entidades, que les ayuden a garantizar la confidencialidad y transparencia en la información privada. Desde aquí es donde interviene el hacker ético, que su principal labor, 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.

A medida que ha avanzado la tecnología, se ha ido incrementando nuevas técnicas de intrusión que atentan contra la seguridad de la información que afectan los tres pilares fundamentales: confidencialidad, integridad y disponibilidad.

Gracias a ello, nace el término de hacking ético que se define como el valor ético que tiene una persona o un grupo de personas que tienen un conocimiento en informática y seguridad, para realizar ataques de pruebas controlados, ya sea en redes, sistemas informáticos, de software o de hardware, para un fin beneficioso, donde se puedan encontrar las vulnerabilidades que sean reportadas por medio de un documento formal a una empresa, entidad, persona u organización para que estas tomen medidas de prevención referente a ataques posteriores o malware malintencionados.

La persona que realiza estos ataques es llamado hacker.

El hacker por medio de las pruebas de penetración, intenta de múltiples formas burlar la seguridad para reportar las vulnerabilidades a la empresa para que así puedan mejorar su seguridad.

Dadas las funcionalidades de un hacker ético, surge la pregunta: ¿Qué hace un hacker para hacer los ataques?

Esto es lo que puede hacer un hacker:

A. *Fase 1 – Reconocimiento:*
El hacker hace el reconocimiento pasivo previo a cualquier ataque, recopila información sobre el objetivo a atacar.

Reconocimiento activo donde se puede realizar el ataque ejemplo Probar la red para detectar:

- Hosts accesibles
- Puertos abiertos
- Localización de Reuters
- Detalles de sistemas operativos y servicios

B. *Fase 2 – Escaneo:*
Se escanean los diferente medios por donde se puede hacer el ataque, como por ejemplo la red, pero esta se realiza ya con información de la fase previa.

C. *Fase 3 – Ataque: obtener acceso:*
Obtención de acceso, se refiere al ataque propiamente dicho, por ejemplo, hacer uso de un exploit o bug, para obtener una contraseña.

D. *Fase 4 – Ataque: mantener acceso*
Mantenimiento del acceso, se trata de seguir tendiendo los privilegios obtenidos.

E. Fase 5 – Borrado de evidencia:
Borrar las evidencias con lo que pueda ser descubierto.

El hacker ético para evitar los ataques debe hacer lo siguiente: primero un hacker ético intenta responder a los siguientes interrogantes:

A. ¿Qué puede saber un intruso de su objetivo?

B. ¿Qué puede hacer un intruso con esa información?

C. ¿Se podría detectar un intento de ataque?

Fases de un proceso de evaluación de la seguridad:

A. Preparación – Se debe tener un contrato firmado por escrito, donde se exonere al hacker ético de toda responsabilidad como consecuencia de las pruebas que realice (siempre que sea dentro del marco acordado).

B. Gestión – Preparación de un informe, donde se detallen las pruebas y posibles vulnerabilidades detectadas.

C. Conclusión – Comunicación a la empresa del informe y de las posibles soluciones.

Están son las pruebas de los hacking ético:

A. Redes remotas – Simulación de un ataque desde Internet.

B. Redes locales – Simulación de un ataque desde dentro (empleados, hacker que ha obtenido privilegios en un sistema).

C. Ingeniería social – Probar la confianza de los empleados.

D. Seguridad física – Accesos físicos (equipos, cintas de backup).

Dada las pruebas esto es lo que debe entregar un hacker a la empresa:

A. Ethical Hacking Report.

B. Detalles de los resultados de las actividades y pruebas de hacking realizadas. Comparación con lo acordado previamente en el contrato.

C. Se detallarán las vulnerabilidades y se sugiere cómo evitar que hagan uso de ellas.

D. Deben quedar registrados en el contrato dichas cláusulas de confidencialidad.

Toda la información debe ser “confidencial” en el momento de la entrega.

De acuerdo a lo anterior, el pentester se debe poner en la tarea en identificar las vulnerabilidades encontradas de la organización y se deben de basar en los siguientes parámetros para lograrlo. Como son los siguientes:

A. Recopilación de la información – Consiste en hacer un análisis para identificar y llegar a la manera en que pudo suceder la fuga o hueco de información sensible que ocurrió en una organización, ya sea por: falla humana, error en la infraestructura interna, cliente o usuario externo, proveedor de Internet, la red que este desprotegida, un error de programación, por descuido del área de administración que pudo haber fallado en la manera de no haber definido desde un principio los roles y control de acceso acorde a los perfiles que tiene un empleado.

De igual manera, se puede obtener información a través de los logs, en el cual se detalle desde el momento que se pudo meter el atacante y si hubo alguna modificación en la información o alteración del mismo.

B. Bases de Datos – Permite realizar una recolección de datos y que se puedan disponer los recursos, para hacer pruebas de todas las contraseñas posibles, como por ejemplo: fecha de nacimiento, número de identificación, cuentas de correo que se encuentran dentro de la entidad y usar un servicio que requiera algún tipo de autenticación, ya sea por:
- ssh
- ftp
- rlogin

- telnet, etc.

C. *Internet* – Es la principal fuente para poder encontrar información adecuada para utilizar una herramienta que ayude a encontrar el procedimiento o el paso a paso a seguir, que se debe de realizar, que ayude a replicar la brecha de seguridad que pudo lograr de manera exitosa el atacante. Una de estas herramientas y que es la más usada, se llama: Google hacking, la cual permite visualizar los datos relevantes como lo son:

- Información sensible
- Bases de datos
- Vulnerabilidades encontrados por atacantes que han realizado a otras organizaciones.
- Usuarios
- Errores típicos de un sistema operativo, etc.

D. *Huellas dactilares* – Es una de las técnicas más usadas, que permite hacer una recopilación de la información por medio del escaneo de la red y lograr el objetivo por medio de rangos de direcciones IP y dominios, para tener un detalle de esa información.

E. *Peticiones de HTTP* –Consiste en generar errores que puedan ser ocultos por el objetivo, puede ser utilizado por los diferentes protocolos, ya sea por código malicioso, SQL Injection, FTP, repositorios de archivos confidenciales, código fuente de la página.

III. ¿CÓMO SE VE REFLEJADO EL ARTÍCULO EN LA REALIDAD COLOMBIANA?

Con la creciente ola de escándalos por robo de información o dinero en bancos y empresas, así como los ataques constantes a las plataformas del gobierno, en Colombia es urgente que se tomen en cuenta los procesos de " hackeo ético" para mejorar la seguridad en las empresas.

Un ejemplo práctico que se vio reflejado para el año 2013 la causa número uno fue el hacking, que ocasiono el 35% de los incidentes. Esto causo que el 76% de las identidades quedaran expuestas. pérdida o robo de un dispositivo fue la tercera causa que provoco el 27% de la fuga de datos. Como se puede observar en la Figura Nº1.

La cuota que pide un hacker para robar la información de una tarjeta crédito puede llegar alrededor de unos 100 dólares, dependiendo de la dificultad del ataque, según cifras de Symantec, entidad número uno en seguridad informática del mundo.

Para los hackers su época preferida es en temporada de vacaciones y navidad, porque aumentan las transacciones de manera considerable.

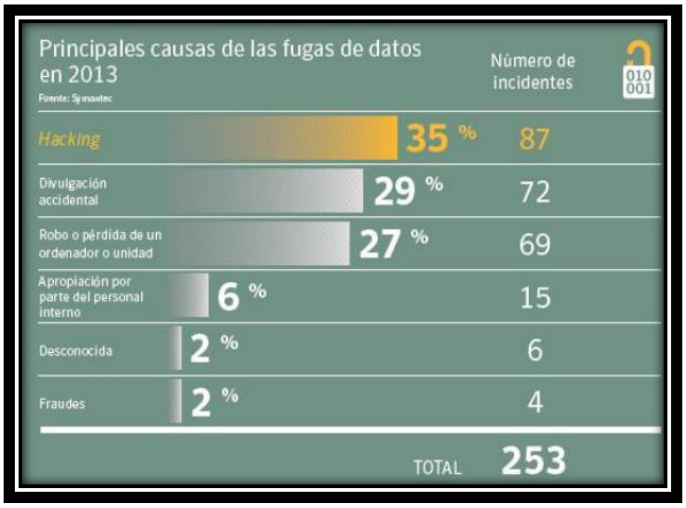

Fig. 1. Certicámara. Validez y seguridad jurídica y electrónica. El cual explica las principales causas de las fugas de datos que ocurrieron durante el año del 2013. [5]

Ya no es una situación que solamente ocurre en Estados Unidos o Europa, ya los escándalos de ataques de seguridad llegaron al país.

Otro caso práctico que se presentó en la entidad financiera BBVA, con un robo multimillonario, por parte de uno de sus ex- funcionarios, sucedido hace menos de 1 año en Bogotá.

La mayoría de los casos se presentan por el mal uso que se le da a la información, por falta de incentivos o motivaciones a los empleados, y de concientizarlos que la información es uno de los principales activos, que se deben de realizar campañas de sensibilización de la manera como se puede prevenir y reducir los riesgos.

IV. ATAQUES EN FACEBOOK

Esta es la red social más famosa del mundo, por ende se hace una de las más vulnerables en la parte de seguridad. A medida que pasan los días, se van encontrando más agujeros en la red y esto se debe por convertirse en uno de los canales favoritos para la distribución de phishing y malware.

Acorde a lo anterior en el año 2013 fue atacado Facebook y sucedió cuando los empleados de la entidad visitaron un sitio web de un desarrollador móvil, lo hicieron de manera inconsciente sin saber las consecuencias que podría arraigar esto, debido a que la información que millones de usuarios utilizan esta red social, podía estar afectada su información, los atacantes hubiesen hecho un mal uso de la misma. En este año el FBI investigo el ataque colaborando con la información desde donde fue posible que se originó, pero no informaron sobre lo sucedido.

Pero este no solo ha sido el único intento de ataque que le han realizado los hackers a Facebook, ellos se aprovechan de las vulnerabilidades que este presenta, debido al navegador ya que es muy inestable y es sensible ante cualquier tipo de ataque que se pueda hacer afectando la información de muchos usuarios que la usan y que publican información bastante comprometida en la red, y no se concientizan lo que estos personajes puedan hacer con ella.

Por eso Facebook ha hecho presencia sobre lo ocurrido y explican que este ataque de spam comenzó desde el 15 de noviembre de 2011, por una vulnerabilidad del navegador, que descubrieron los hackers. Este tipo de ataque infringe en la publicación de imágenes de pornografía de personajes famosos y de abuso a animales, accediendo a los muros de los usuarios sin tener su propio consentimiento. La manera como hacen que se llene de spam es en enviar código de javascript malicioso, por medio de rifas, premios o publicidad engañosa, de esta manera los atacantes logran que el usuario caiga, pero los usuarios no saben lo que hay detrás de estos mensajes e imágenes publicitarios y se ven tentados en copiar este código en la barra del navegador, con esto los hackers logran en acceder a todas las fotos que tienen los usuarios publicados en su muro y no solo esto sino acceden a su información.

Ante esta situación presentada, Facebook tomo medidas para validar que las demás cuentas de los usuarios no fueran atacadas y empezar a realizar una limpieza de los diferentes navegadores, para quitar ese código malicioso.

Acorde con lo anterior la mayoría los hackers debido a la disponibilidad de tiempo completo que tienen, se encargan de analizar y empezar a buscar vulnerabilidades que cuando las encuentran, publican en la página de la entidad y si esta no les presta mayor importancia, proceden en publicar esa vulnerabilidad encontrada en un sitio Web solo hecho para hackers, para que estos la puedan atacar y de esta manera ellos reciban una recompensa por ello, para este caso sucedió algo muy similar con Facebook, un hacker con el nombre: Anand Prakash encontró una vulnerabilidad para el 22 de Febrero de este año 2016 y este fue premiado por un valor de 15000 USD. Apenas Facebook se enteró, la corrigió en la fecha del 02 de Marzo de 2016.

La vulnerabilidad que encontró el hacker, consistió en lo siguiente: como la mayoría de los usuarios se les olvida la contraseña, existe una manera de poder recuperarla y era resetearla, se logra en ingresar un número de teléfono o de dirección de correo electrónico. En el momento en que se ingresan estos datos por la aplicación de Facebook, inmediatamente da una respuesta o notificación de enviar un código de seis dígitos, para que el usuario ingrese la nueva contraseña. Este consista en un ataque de fuerza bruta, en el cual se mencionaba que después de diez o doce intentos, el usuario será bloqueado. Ante este tipo de situación a Facebook se le olvido poner un umbral, para poder evitar este ataque, cosa que no sucedió.

V. VULNERABILIDAD DE WHATSAPP

Después de la aplicación de Facebook, existe whatsapp, que es la más usada por doscientos mil usuarios, esta es expuesta a toda la información que se comunican entre ellos mismos, ya sea número de cuentas bancarias, contraseñas de las mismas.

Desafortunadamente los usuarios no se imaginan lo que puede ocurrir, al ver que su información está siendo expuesta por atacantes que están interesados en acceder y al mismo tiempo en hacer un mal uso de la misma, podrían ocurrir robos y desfalcos.

La compañía de whatsapp puso en riesgo a los usuarios que utilizan la aplicación web, debido a que los hackers accedieron a la información personal.

Gracias a ello, la firma de seguridad Check Point, fue la que pudo detectar la intrusión que hicieron los hackers y detallar la manera como estos pudieron lograr el acceso, como por ejemplo, enviando tarjetas electrónicas de contacto que estas contenían: spam, malware, códigos maliciosos que estos permitían controlar los diferentes dispositivos y de esta manera poder manipularlos y poder disponer la información y datos de los usuarios.

Esta firma informo que esta vulnerabilidad encontrada por los hackers, fue muy fácil de ser explotada y se descubrió el 21 de Agosto y reparada el 27 de ese mismo mes en el año 2015.

Otra de las vulnerabilidades más importantes y con mayor concurrencia que estos intrusos aprovechan, es cuando los usuarios se conectan a la aplicación de whatsapp por wifi en: centros comerciales, cafés de Internet, hospitales, etc. Esta consiste cuando el usuario intenta enviar un mensaje, pero este no sale al receptor. Por ende, este se queda pegado en el móvil, lo cual esto es bastante provechoso por el atacante que copia ese mensaje y tiene presente que el usuario en vista que está conectado por la red inalámbrica, envía algún servicio por medio de un mensaje gratuito, ingresando el número del emisor. En el momento que el atacante utiliza esta forma para que el usuario acceda al mensaje, el servidor de whatsapp obtiene una respuesta y entrega el código de activación al número de remitente que selecciono el intruso. Esto provoca que la información ya está comprometida, lo cual logra que el atacante tenga acceso al teléfono y tener todos los datos de contactos e información sensible.

Esta vulnerabilidad se ha reportado en más de una ocasión, pero la empresa no le ha prestado mayor importancia, ya que fue comunicada por un usuario que se dio cuenta de esta problemática que aqueja y que es muy grave, porque se están violando los tres pilares fundamentales de la seguridad de la información, que son: confidencialidad, integridad y disponibilidad de la misma. Esto afecto a más de un 99% de los móviles que tienen el sistema operativo de android.

Acorde a lo anterior surge la necesidad de que se debería implementar un método de encriptación de mensajes que tengan contraseñas fuertes en el momento de la transmisión de un mensaje de un usuario a otro, cuando se utilice redes inalámbricas en lugares públicos, con esto poder evitar que exista un diablillo o hombre en el medio en el momento de esa comunicación, de esta manera le costara un poco de trabajo poder descifrar la información que viaja. Así se garantiza la seguridad en la información.

VI. VULNERABILIDAD DE TWITTER

Twitter se ha ido volviendo en una aplicación bastante fuerte en las redes sociales, ya que millones de sus usuarios publican información en sus cuentas, fotos, gustos, etc. Pero estos no son nada conscientes de la manera como viaja la información y no poder que se garantice con mayor confidencialidad de la misma y del medio en que esta viaja por medio de comunicación de una red, sin saber que en el momento en que pueda ocurrir esto, pueda existir un intruso en medio del canal que haga un mal uso de la misma. Es triste ver que los usuarios no hagan un buen uso de ella, traten en lo posible de no publicar en sus cuentas información que pueda ser fácil ante el atacante para manipularla.

De acuerdo a lo anterior sucedió un ataque masivo informático que hizo caer la plataforma de twitter, esto permitió que muchos usuarios que la usan no puedan enviar mensajes. Debido a esta situación, se empezó a generar la duda de que tan confiable pueda ser esta aplicación. En el momento en que se presentó lo ocurrido, apareció la entidad de Facebook, para notificar por medio de un blog de la BBC, que recibieron muchas peticiones que hicieron que se colapse el servicio y que no solo afecto a Twitter sino también Facebook.

Este ataque consistió en lo siguiente: se enviaron millones de peticiones masivas al servidor de twitter, esto ayudo a que se cayera el servicio. Hablo uno de

los creadores de la aplicación de Twitter, indicando que a pesar de la caída del servicio, no afecto ni fue comprometida la seguridad de la información de sus usuarios.

Desafortunadamente las redes sociales son un punto blanco para los intrusos, estas siempre estarán expuestas a las diferentes vulnerabilidades que estos atacantes puedan encontrar y de igual manera, se aprovechen de la debilidad de sus sistemas, para atacarlas y ver la manera tan fácil de poder acceder a ellas. Por el momento para prevenir, se aconseja usar menos esta aplicación de Twitter, ante las posibles vulnerabilidades que este presenta.

VII. VULNERABILIDAD DE ANDROID Y SKYPE

Las aplicaciones para el sistema operativo android siguen siendo vulnerables. Se detectan 58 aplicaciones maliciosas en android marketplace, que Google aún está quitando de su tienda y de las 260.000 unidades que se calculan infectadas.

Ahora es el turno de skype para androide, ya que se ha comprobado que es vulnerable a maliciosos usuarios o aplicaciones que podrían acceder a su información almacenada.

Gracias a la entidad de Inteco CERT, reporto un incidente de vulnerabilidad que descubrió de la aplicación de skype, que corresponde a un ataque xss (cross site scripting). Esta amenaza permite que un intruso pueda tomar el control de la cuenta de un usuario y así mismo poder acceder a la información privada. Las versiones que comúnmente se presenta, son las siguientes: skype 5.3.0.120 y versiones anteriores para la plataforma de windows xp, vista, 7.

Por eso, es muy necesario que los usuarios tengan actualizado las aplicaciones, para evitar y reducir los riesgos que pueda estar afectada la información.

VIII. ¿CÓMO SE PODRÍA APLICAR ESTE ARTÍCULO A LA FORMACIÓN PROFESIONAL?

El artículo crea conciencia acerca de la responsabilidad profesional que se debe tener para preservar las propiedades de la seguridad informática y bajo ninguna circunstancia acceder a cometer adversidades. Porque el conocer las vulnerabilidades que presenta un sistema, no implica que debe aprovecharse de estas para obtener beneficios propios.

Sirve para aplicar el concepto de hacking ético en la vida profesional, con la finalidad, de utilizar los conocimientos de seguridad informática para realizar pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, con el fin de reportarlas para tomar medidas sin poner en riesgo el sistema.

IX. ¿QUÉ SE DEBERÍA PROFUNDIZAR PARA AFIANZAR EL TEMA DE HACKING ÉTICO?

Una de las cuestiones que surgen a partir de la lectura del artículo es la razón por la cual a partir de la existencia de una ley para el hacking ético, porque en la actualidad se divaga en su interpretación, se debe tener en cuenta el objetivo final de los hackers de sombrero blanco y los hackers de sombrero negro. Existe una brecha tan insignificante entre los dos objetivos finales, ya que los dos pueden ir exactamente por el mismo camino, pero con la gran diferencia es que el hacker ético sabe exactamente en qué momento decir: hasta este punto puedo llegar, en cambio la intención del otro no termina en este punto, así conozca la delimitación, sigue adelante para poder cumplir su objetivo.

Otra cuestión formada es la exploración de las herramientas existentes para realizar pruebas de penetración, nmap (identifica equipos activos, sistemas operativos, existencia de filtros), nessus (identifica vulnerabilidades), metasploit framework (explotación de las vulnerabilidades), kali linux o bracktrack (distribución de linux diseñada principalmente para pruebas de penetración), el cerebro, etc. El hecho es saber explotar estas herramientas para mitigar las vulnerabilidades, pero en fin la herramienta más útil que se tiene es pensar en ir un paso adelante del atacante, no perder de vista el objetivo final que siempre será la protección de la información. Estar en un ciclo constante de búsqueda de vulnerabilidades, porque la amenaza va a estar constante y nunca va a descansar.

La manera como se debe entregar la información a una empresa es otro interrogante, que es generado porque se sabe que existen muchos métodos de realizar el estudio de las vulnerabilidades como lo son: cramm, isamm, iso 27001, iso 27005, migra, octave, etc. Pero no es una información fácil de obtener.

X. CONCLUSIONES

Los pensamientos de las personas siempre serán diferentes, por este motivo existen los ataques beneficiosos y malignos.

Toda acción de un ser humano, toma diferentes perspectivas de ética como pueden ser malas o buenas; el hacking ético tiene como principal objetivo, dar un diferente punto de vista a las personas que dedican su tiempo a encontrar vulneraciones en las empresas u organización, que puedan ayudar a convertir estas ideas en metodologías para la protección informática de ellas.

El hacking ético es importante que sea conocido por varias empresas u organizaciones, para que así puedan llevar una prevención o una seguridad informática anticipada antes de sufrir algún ataque malicioso, por esto es sugerido a las empresas que contraten los servicios de hacking ético.

Tener claro la metodología para realizar un buen test de penetración para así poder verificar y sacar unas buenas conclusiones de acuerdo a la vulnerabilidad que está sufriendo la empresa u organización.

También gracias a las nuevas tendencias que están surgiendo debido al auge de dispositivos móviles, como tablets y smartphones y las famosas aplicaciones, hacen aumentar considerablemente el fenómeno de la inseguridad informática.

Acorde a lo anterior, las empresas deben de realizar campañas de sensibilización a sus empleados, esto ayuda a identificar en el momento en que puedan ser atacados y en caso dado que se llegue a presentar, enseñarles cómo deben corregirlo y de igual manera informar, para poder solucionar y mitigar el riesgo de que pueda existir alguna fuga en la información. No solo como mitigarlos, sino que refuercen sus contraseñas, que las cambien cada mes, y que esta no sea la misma, de que protejan su correo electrónico con el envío de mensajes que lleguen a ir cifrados tanto el de emisor como receptor, con esto se previene que si existe un diablillo o un hombre en el canal de comunicación, le cueste al intruso tratar de poder descifrar la información que está viajando. Es necesario que cifren sus archivos y que en el momento que la compañía utilice el personal para realizar hacking ético, eliminen las evidencias que se encontraron y tratar en lo posible que no se dejen en ningún equipo, pues el intruso puede estar alerta sobre las vulnerabilidades que se encontraron y que estas puedan ser expuestas, esto sería una falla para la información de la compañía, quedaría mal y su reputación estaría por el piso, esto implicaría que los clientes abandonen la compañía.

REFERENCIAS

[1] Harris, S. et. al. “Hacking ético. Traducción de: Gray hat hacking” (2005). Madrid: Anaya Multimedia.

[2] USA: University of California, About Penetration Testing, Matt Bishop, bishop@cs.ucdavis.edu, Deborah A. Frincke, deborah.frincke@pnl.gov

[3] http://es.slideshare.net/nilsoncas/electricidad-ieee?related=1

[4] https://kn0wledge.files.wordpress.com/2009/06/etica-hacker1.pdf

[5] https://web.certicamara.com/media/70550/panorama-actual-de-amenzas-y-retos-en-seguridad.pdf

[6] http://www.portafolio.co/portafolio-plus/los-ataques-informaticos-mas-peligrosos-el-bolsillo

[7] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[8] http://itsecurity.telelink.com/brute-force-attack

[9] Picouto, F. et. al. “Hacking práctico” (2004). España: Anaya Multimedia.

[10] Daltabuit, E. et. al. “Seguridad de la información” (2007). Noriega, México: Limusa

[11] Aceituno, V. “Seguridad de la información: Expectativas, riesgos y técnicas de protección “(2006). México: Limusa.

[12] Rodríguez, L. A. “Seguridad de la información en sistemas de cómputo” (1995). México D.F: Ventura.

[13] E-WORLD: Arm yourself against black hats, Anonymous. Businessline. Chennai: Jul 12, 2010.

[14] DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure, Ronald I Raether Jr. Business Law Today. Chicago: Sep/Oct 2008. Tomo 18, No. 1; Pág. 55

[15] Ethical hacking on rise, Bill Goodwin. Computer Weekly. Sutton: Jan 31, 2006. Pág. 8 (1 página)

[16] Ethical Hackers: Testing the Security Waters, Phillip Britt. Information Today. Medford: Sep 2005. Tomo 22, No. 8; Pág. 1 (2 páginas)

[17] IT takes a thief: Ethical hackers test your defenses Bill Coffin. Risk Management. New York: Jul 2003. Tomo 50, No. 7; Pág. 10).

[18] MITNICK, Kevin, "Controlling the Human Element of Security. The Art Of Deception", Ed. John Wiley&Sons Australia, USA, 2002, 577 pp.
http://www.ey.com/Publication/vwLUAssets/EY-Conociendo-hackeo-etico/$FILE/EY-Hacking-Etico.pdf

Castro Cubillos, Sandra Milena. Ingeniera de Sistemas de la Universidad Libre de Colombia. De igual forma tiene conocimientos en el área de calidad de software.