INTRUSIONES DE SEGURIDAD

AUTOR: WALTER MADRIGAL CHAVES

NOVIEMBRE: 2020

San Marcos

Contenido

INTRODUCCIÓN

El campo de la ciberseguridad en los últimos años ha tomado mucha fuerza en la comunidad tecnológica, al evidenciarse ataques cibernéticos por parte de hackers a organizaciones gubernamentales, corporaciones privadas o usuarios comunes. Todo esto ha puesto el foco de atención sobre este tipo de prácticas que hacen que nuestra actividad con sistemas informáticos pueda ser vulnerada por individuos en el campo tecnológico, quienes cuentan con habilidades y herramientas que permiten comprometer la información, la confidencialidad de contraseñas, fotografías del teléfono móvil y saldos bancarios, entre otros.

Es importante saber que lo que veremos a continuación es una identificación de dichas prácticas que recaen sobre lo no ético, ya que por donde se quiera ver son acciones, que pueden ir desde perjudicar a un usuario hasta la extorsión, el robo o el secuestro de información.

Ante ese fenómeno, los profesionales en informática cumplen una tarea importante en términos de combatir dichas prácticas ilegales de manera autorizada; sin embargo, dentro de los límites de la ética es posible que profesionales de este campo estén en la delgada línea de hacer buenas prácticas de hackeo o poco éticas al usar técnicas en cualquiera de los dos extremos del campo profesional.

HISTORIA DEL HACKEO

Los inicios de los hackers, como hoy en día los conocemos, se dan alrededor de la década de 1960, fecha en la que el Instituto Tecnológico de Massachusetts (MIT) obtuvo el PDP-1 (Programmed Data Processor-1) que cumple un importante papel como referente histórico en la historia de la computación por ser además el computador en el que se ejecutó el primer videojuego computacional de la historia.

La afición por la computación en el MIT coincide con varias fuentes en que determinaron y crearon el término hacker. Los hackers son un grupo de estudiantes y profesionales que conformaron el club: Tech Model Railroad, que se transformó en un grupo de gran importancia del MIT. Para quienes hacían estudios en el MIT durante dicha década, el término hack se usaba para aludir a soluciones sencillas, prácticas e innovadoras para atacar un problema y no se asociaba con un grupo de personas con ideas comunes frente a una complicación computacional.

Se sabe que los hackers toman los retos computacionales por diversión y ocio; con el transcurrir del tiempo dicho término empezó a asociarse a programadores informáticos con grandes habilidades y destrezas. Esta tendencia día a día tomaba más fuerza en institutos y universidades alrededor del mundo, lo cual identificaba a un hacker como un individuo con talentos e ingenio para las ciencias de la programación.

El desarrollo de estas prácticas era motivo de admiración y se volvieron el centro de atención de quienes les apasionaba la computación por los retos que conllevaba combinar programación con la creatividad, para solucionar problemas poco comunes y con la generación de un sinnúmero de variables y códigos que orientaban la comprensión a caminos alternativos.

Con lo anterior, se puede identificar en la historia de la computación los inicios de las actividades de hackeo que inicialmente no concebían intrusiones directas a los sistemas; no obstante, lo que se deja como referente es que en 1969 el MIT se convierte en la cuna de los primeros hackers, quienes con ingenio lograron modificar un software y un hardware para ampliar las funcionalidades de diseño para mejorar el rendimiento o cambiar su funcionamiento de fábrica.

Capitán Crunch 1972

John T. Draper fue una de las primeras personas en aplicar el término hackear un sistema o ingresar sin permiso al mismo. Fue un programador estadounidense, que pasó a la historia por la hazaña de hackear el sistema de líneas de telefonía de ese entonces de AT&T por medio de un teléfono y un silbato que venía en las cajas de un cereal infantil de aquel entonces, como se muestra en la figura 1.

Imagen 1 Silbato de Capitán Crunch

Fuente: https://bit.ly/2NwddOS

Descubrió que aquellos silbatos emitían un tono de 2600 hertz, frecuencia que servía para anular el sistema telefónico en el modo de operador. Una vez en el sistema vulnerado lograba hacer llamadas telefónicas a cualquier destino sin la

necesidad de pagar por el servicio de telefonía. La empresa logró hacer que arrestaran a Draper, quien fue a la cárcel por el cargo de fraude electrónico.

Legión de Doom - 1984

Este llamativo grupo de activistas cibernéticos se unió para transferir y compartir el conocimiento y las actividades de hackeo en el campo de la informática. Llegó a reclutar más de 20 hackers, quienes se hacían llamar con curiosos alias tomados de caricaturas o superhéroes del momento.

Esta organización fue seguida por el Servicio Secreto de los EE. UU. Doom se infiltró en varios sistemas informáticos de empresas durante la década de los 80, algunos de los integrantes de este grupo hacktivista fueron encarcelados; sin embargo, muchos lograron mantenerse en el anonimato.

El gusano Morris - 1988

El mes de noviembre de 1988 se define como un punto de gran importancia en la historia de los delitos cibernéticos. Un estudiante de nombre Robert Morris, graduado de la Universidad de Cornell y programador de software, hizo un desarrollo que eludía la fase de autenticación de ciertos sistemas informáticos que solicitaban contraseña, en un impulso por determinar la magnitud de lo que habría creado hasta entonces, liberó el desarrollo en internet y de esta manera por equivocación terminó dando las bases del primer virus informático conocido a la fecha.

Este se aprovechaba de un error de programación que se repetía muchas veces, esta era una instrucción que se traducía en la indisponibilidad de los sistemas donde se alojaba el programa, por lo que las autoridades de esta rama, en ese entonces, reaccionaron ante la emergencia y se creó el equipo de respuesta para combatir futuras amenazas de seguridad.

Robert Morris fue juzgado por este hecho, así mismo, fue uno de los primeros al que le aplicarían la Ley contra el fraude y el abuso informático en EE. UU. De

ahí se desprende el dato de Morris Worm, que afectó a más de 5000 sistemas informáticos y ocasionó daños financieros enormes.

Kevin Poulsen - Dark Dante (1990)

Kevin Poulsen, hacker informático conocido mundialmente como Dark Dante, logró eludir al FBI durante varios años. Su proeza más importante la hizo con una serie de hackeos en una red telefónica de estaciones de radio. Dicha emisora había organizado un concurso: regalaría un Porsche a la llamada número 102.

El hackeo de Poulsen consistió en manipular el concurso al bloquear todas las demás llamadas entrantes y asegurarse el premio. Pero como ningún hacker se detiene, siguió hackeando ilegalmente las estaciones con la misma mecánica de llamadas, obteniendo dinero y otro tipo de beneficios materiales.

Finalmente, el FBI lo puso en el radar, Poulsen fue arrestado, procesado y acusado de fraude electrónico. Al salir de la cárcel, Poulsen se volvió periodista para una respetada revista en la que escribió sobre ciberseguridad.

Es claramente visible que los inicios del hackeo fueron con un objetivo de innovación, creatividad y una iniciativa para mejorar comportamientos de un sistema. Sin embargo, con el transcurrir de los años la ética de los individuos mencionados tomó rumbos de criminalidad, por lo que queda preguntarse: ¿fueron adecuados los castigos a esos individuos que hackearon dichos sistemas? ¿Valió la pena para ellos ir a la cárcel? ¿Qué los impulsó a cambiar su propósito inicial? Al contestar estas preguntas los futuros profesionales del hackeo ético tendrán claridad sobre las actividades en este campo, que siempre deberán estar regidas por la legalidad.

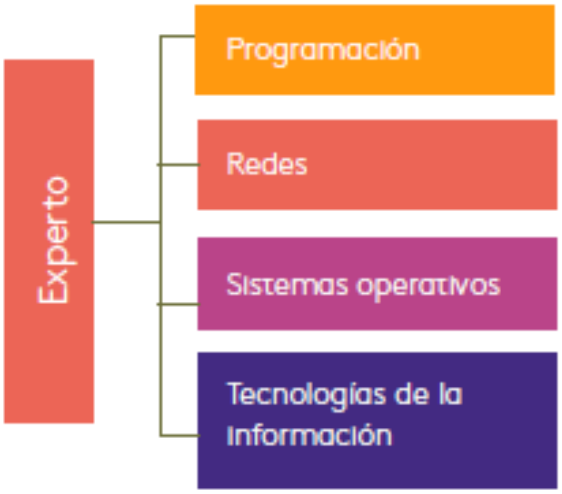
HACKER ÉTICO

Ya tuvimos un acercamiento a los inicios del hackeo, ahora podremos ver un enfoque de lo que es un hacker ético, quien se encarga de ayudar a prevenir y

proteger los sistemas de información que pueden ser vulnerables, y permite compararlos con los hackers que alteran, sabotean o destruyen sistemas.

Un hacker ético es un experto en una o muchas ramas de la informática las tecnologías de la información, el desarrollo de software (programación), las redes y los sistemas operativos (descritos en la siguiente figura), que al conocer todos estos campos y combinarlos con habilidades de exploración e investigación puede anticiparse a la búsqueda de vulnerabilidades en sistemas informáticos para organizaciones o empresas con el fin de encontrar planes de mejora que ayuden a resolver debilidades en la seguridad.

Imagen 2 Campos de conocimiento de un hacker



Fuente: Elaboración propia

TIPOS DE HACKERS

Los hackers a lo largo de los años fueron obteniendo una fama peyorativa sin importar el fin para el que usaran sus técnicas y actividades de hackeo, por lo que se tuvo que hacer una clasificación según los fines y categorización a partir de la actividad que desempeñen en el campo informático, fueron separados en tres categorías generales:

- Sombrero blanco
- Sombrero gris
- Sombrero negro

Sombrero blanco

Los hackers de sombrero blanco tienen una importante función en el campo de la informática, se dedican a buscar, detectar, descubrir e investigar debilidades de seguridad en sistemas informáticos. Así como en las películas de Starwars donde se ubican en dos bandos, los personajes buenos tenían el lado luminoso de la fuerza y el lado oscuro era para los malos.

En esta medida se consideran buenos ya que su propósito es hallar, detectar o ayudar a la solución de los agujeros o vulnerabilidades de seguridad en los sistemas informáticos. Además, las principales motivaciones de los hackers de sombrero blanco son el reconocimiento mundial y fortalecer y endurecer la seguridad de los sistemas por medio de sus hallazgos.

Con ello vienen grandes empleos por los gigantes informáticos, que siempre están en la búsqueda de nuevos talentos para robustecer los equipos de ciberseguridad en las organizaciones, sin olvidar que dichas actividades estarán siempre bajo la línea de lo legal, donde nunca se alteran las normas o leyes que los pueden judicializar

Sombrero negro

Este grupo de hackers, siguiendo con la analogía de la película de Starwars, son los del lado oscuro de la fuerza, que se denominarían los malos; los delincuentes que deben ser judicializados debido a que su falta de ética los ha llevado a utilizar los conocimientos y habilidades en beneficio propio y con fines delictivos. Este tipo de hackers buscan las fallas o agujeros de seguridad en los

sistemas informáticos y los aprovechan en función de un beneficio financiero, sabotaje, diversión o destrucción de los sistemas informáticos.

Su objetivo está limitado por los permisos restringidos en los sistemas, es allí donde escalan los privilegios: si una contraseña en un sistema obstaculiza el ingreso a la información, entonces la violan con técnicas de fuerza bruta o ingeniería social, ya sea para afectar la imagen de una organización, alterar el contenido, hacer sabotaje o afectar la operación de una empresa para que los sistemas no puedan prestar servicios.

Los anteriores son solo unos casos de lo mal que puede obrar un hacker de sombrero negro, sin olvidar que se venden al mejor postor. Si tienen una oportunidad de vulnerar ilegalmente un sistema informático no dudarán en hacerlo, algunos crean scripts que venden para que más hackers puedan seguir delinquiendo. Son criminales que roban y trafican información, contraseñas, correos, números de tarjetas bancarias, entre otras cosas.

Sombrero gris

Son el punto intermedio entre los buenos y los malos, lo que quiere decir, que no son los malos que vulneran información para venderla en el ciber-mercado negro, pero tampoco son buenos que se conforman con ayudar únicamente a endurecer y fortalecer la seguridad de los sistemas informáticos sin esperar algo a cambio.

Su forma de actuar logra estar en ambas categorías al usar sus habilidades y destrezas en la búsqueda y detección de vulnerabilidades de manera no autorizada, que luego informan a los directos afectados para que aseguren la brecha de seguridad esperando beneficios financieros; por lo general son trabajadores autónomos, que actúan de forma individual, ya que su actividad puede involucrar ciertas prácticas ilegales, aunque por lo general, se mantienen en el anonimato.

HACKTIVISMO

El hacktivismo es una combinación de dos términos: el hackeo y el activismo. Sabemos ya que el hacker es una persona con grandes conocimientos en informática o tecnologías de la información, que accede a cualquier sistema informático que logre ser vulnerado. El activismo en este contexto es cómo la realización de acciones directas y militantes abarcan objetivos políticos y sociales.

En resumen, el hacktivismo es un grupo u organización de individuos que, por medio de la utilización de técnicas y prácticas de hackeo, persiguen un fin político y social. Sin embargo, no son hackers del todo, sino que persiguen una causa con objetivos y fines éticos, bajo una ideología de ir en contra de organizaciones que atropellan los derechos o hacen daño a las comunidades.

¿Qué hacen los hacktivistas?

Estas organizaciones hacktivistas utilizan herramientas y técnicas con las que efectúan robos de información, ataques a VPN (Virtual Private Network), ataques de denegación de servicio, spoofing, ataques de injection SQL (Structured Query Language), suplantación y alteración de datos, entre otros, con el fin de hacer sentir su causa.

Muchas de las protestas van de la mano con alteraciones de páginas gubernamentales u organizaciones que han considerado vulnerar de alguna manera los derechos de la sociedad, haciendo burlas en sus portales web; a este tipo de ataque se le llama Defacement.

También la forma de operar conlleva ataques que inhabilitan el servicio de algún sistema informático a lo que se le llama denegación de servicio, sin olvidar otra serie de ataques elaborados con el fin de fortalecer su forma de protesta. Muchas veces logran penetrar en estos sitios web y vulnerar la seguridad, que

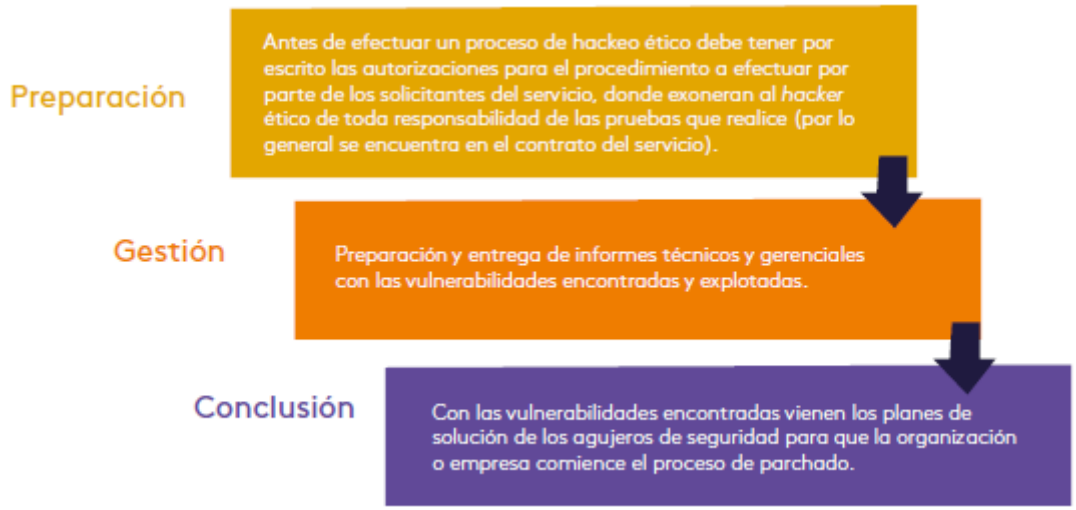
hace visible la información al resto de usuarios, con las implicaciones mediáticas que esto trae.

Aunque es una discusión mundial determinar si es bueno o malo lo que hacen las organizaciones hacktivistas, habrá quienes los criminalicen, así como los que los justifiquen en su causa. No obstante, se debe tener en cuenta que ingresar, modificar o destruir un sistema informático de manera no autorizada constituye un delito.

¿Qué debe hacer un hacker ético?

Un hacker ético debe estar en la capacidad de reconocer las fases de un proceso de evaluación de la seguridad de un sistema y proceder según se observa en la siguiente figura:

Imagen 3 Fases de un proceso de seguridad



Fuente: Elaboración propia

MODOS DE HACKEO ÉTICO

- **Redes remotas:** por lo general se ejecutan desde internet y se materializan en ataques de denegación de servicio que hacen colapsar

el servidor donde se aloja el sistema informático, en este caso la página web.

- **Redes locales:** este modo de hackeo ético se logra teniendo acceso a la red de la empresa u organización: acceso a la wifi interna de la compañía, a la computadora de la recepcionista de la empresa o simplemente al equipo portátil de un empleado.

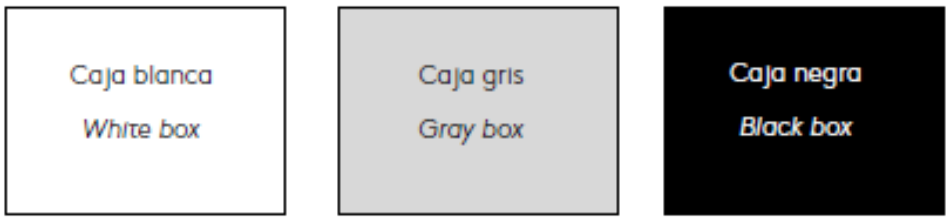
- **Ingeniería social:** probar la confianza de los empleados, hacerse pasar por alguien de la empresa, regalar a un empleado una memoria USB con malware o keylogger, suplantar una página oficial de la compañía aprovechándose de la ingenuidad de los empleados; siempre el eslabón más débil de la seguridad: el error humano.

- **Seguridad física:** burlar sistemas de seguridad perimetrales que permitan tener acceso a dispositivos de almacenamiento o terminales desatendidas.

Tipos de hackeo ético (test) de seguridad

Según la cantidad de información que se conozca de los objetivos a efectuar, el hackeo ético se categoriza entre:

Imagen 4 Categorías del hackeo ético



Fuente: Elaboración propia

Caja blanca: el interesado de estas pruebas provee el código fuente del sistema, documentación y direcciones IP de servidores o equipos de

empleados; este tipo de prueba simula el ataque y el daño que lograría hacer un empleado de la compañía u organización descontento, desleal o ingenuo.

En este tipo de prueba se relacionan las fallas lógicas, perfiles de usuario mal configurados frente a permisos, no validación en las entradas de datos, utilización de usuarios genéricos y agujeros de seguridad interna, que permiten probar dichos frentes de seguridad y funciones de manera individual.

Caja negra: en este tipo de prueba, el hacker ético no tiene acceso al código ni a la documentación y mucho menos a una dirección IP de servidores o equipos de usuarios. Lo único con lo que cuenta para las pruebas es lo que logre encontrar de manera pública en internet u otros medios. Se simula un ataque dirigido por un hacker de sombrero negro, por lo que aplicar técnicas para el reconocimiento del objetivo es más complejo.

Caja gris: es una combinación de las dos anteriores, por lo general se da el rango de direcciones IP definiéndolo como alcance de las pruebas de hackeo.

¿Por qué es necesario el hackeo ético?

La importancia y necesidad de tener un hacker ético en las organizaciones es que será capaz de ofrecer un panorama acerca de los agujeros de seguridad o vulnerabilidades detectadas en la infraestructura donde se efectuaron las pruebas, para dar a conocer las malas parametrizaciones de los dispositivos o sistemas, aplicaciones que se puedan materializar en auténticos ataques en la organización por hackers de sombrero negro.

También es importante porque logrará identificar sistemas o dispositivos que son vulnerables por falta de actualizaciones, lo que se traduce en disminuir tiempo, esfuerzos y dinero requeridos en caso de un verdadero ataque o desastre en la organización.

Código de conducta de un hacker ético

Es importante mencionar que los hackers éticos se deben basar en buenos principios que garanticen a las organizaciones la seguridad de tener unas pruebas que estén alineadas por la buena conducta del hacker de sombrero blanco. A continuación, se listan algunos de los lineamientos a seguir por un hacker ético:

- No omitir información de las pruebas, generando reportes completos de las actividades efectuadas.
- Mantener en estricta confidencialidad la información entregada por la organización, así como los resultados de las pruebas.
- No tener conflicto de intereses en la infraestructura donde ejecutará las pruebas.
- No aceptar dádivas en función de alterar el resultado de las pruebas para favorecer los informes.
- No alterar o modificar los resultados o análisis manteniendo las debidas medidas para garantizar la integridad y confidencialidad de las pruebas.
- Efectuar las pruebas sobre el alcance acordado de manera responsable sin ir más allá de lo solicitado.
- Ser responsable en su rol y función.

CONCLUSIONES Y RECOMENDACIONES

- Los inicios informáticos definieron un punto de partida crucial para las mentes curiosas y creativas de quienes en esa rama buscaban mejorar o modificar funcionamientos de dispositivos electrónicos y computacionales.
- Sin embargo, dichas iniciativas también fueron aprovechadas por personajes que no tuvieron ética para usar sus habilidades en favor de la innovación, pero sí a favor del beneficio propio por medio de robos, ingeniería social o vulnerabilidades en los sistemas.
- El hackeo con fines de lucro es una actividad ilícita, por lo general no terminan nada bien: siempre hay problemas legales y judiciales.
- Es muy buena práctica aplicar pruebas de penetración a los sistemas, esto ayudará a corregir errores y huecos por donde un verdadero delincuente informático puede realizar daños.

REFERENCIAS BIBLIOGRÁFICAS

Corera, G. (2015). Intercept: the secret history of computers and spies. Londres, Reino Unido: Hachette UK.

Porterfield, J. (2017). White and black hat hackers. Nueva York, EE. UU.: Rosen Publishing Group

Gregg, M. (2017). Certified ethical hacker (CEH) cert guide. Indianapolis, EE. UU.:

Pearson Education.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica