

Taller de Investigación 1

Segunda parte del protocolo de investigación.

Luis Alberto Vargas González.

Fecha: 22/03/2022.

Redactar su contenido, hilando párrafos y citando apropiadamente las

referencias.

Debe contener:

\*\* Introducción

\*\* Elaboración de glosario.

\*\* Redactar las respuestas a las preguntas de investigación o bien los objetivos.

específicos planteados.

\*\* Una conclusión acerca de lo que obtuvo en su investigación.

1. Introducción.

Para poder hablar sobre hacking ético se necesita aclarar el significado según la RAE de hacker:

Hacker: Pirata Informático.

Como se puede notar, es muy ambigua esta descripción y significado de la palabra, lo que conlleva a denotar interpretaciones igualmente ambiguas y en general equivocadas.

Un hacker es una persona curiosa, que se interesa en todo tipo de tecnología principalmente , pero el termino incluso se podría ampliar hacia otros campos del saber humano, por ejemplo: un biólogo que descubre la cura de un virus es un hacker biológico , pues descifra el “código” del virus y lo estudia a profundidad para llegar a la solución del problema que causa y como se puede constatar , esta es una actividad benéfica para la sociedad, pues contribuye al mejoramiento de la salud de la población.

Y para todo esto; ¿Qué hace un hacker ético?

Primero que nada hay que definir los tipos de hackers, los hay 3:

1. Hackers de sombrero blanco.
2. Hackers de sombre negro.
3. Hackers de sombrero gris.

Hackers de sombrero blanco; son los encargados de proteger todo tipo de información que este en peligro de ser capturada por un hacker de sombrero negro o gris, sin embargo, se encargan de “apagar” el incendio y/o ataque después de haber iniciado, no de prevenir que dicho ataque ocurra, como se diría coloquialmente.

Hackers de sombrero negro; son los encargados de provocar estos “incendios” o ataques hacia una persona u organización, para generalmente ganar una recompensa económica.

Hackers de sombrero gris; son aquellos dedicados a hacer las actividades tanto del sombrero blanco como del negro, sin importar el bando moral o ético que se vea implicado en el juego, este tipo de hacker es el menos “ético” debido a que su lealtad está solo en sus propios intereses y no en los de la organización que los contrate, pudiendo fácilmente redirigir el ataque hacia el mismo contratista si la compañía u objetivo les remunera de una forma más cuantiosa.

1. Un hacker ético hace exactamente las mismas actividades que un hacker de sombrero negro , solo con la diferencia de poder evitar que dichas amenazas lleguen a ocurrir, esto previamente informado hacia la alta gerencia de una organización o contratista en donde mediante un contrato de tipo legal el hacker ético se compromete a no divulgar a nadie más que a los implicados las vulnerabilidades encontradas, donde en este mismo se especifican los horarios de trabajo, accesos y niveles de autorización de dicho contrato, alcance de pruebas, etc.

(Gacharná G., F. I. (2009). Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. I, 4(6), 46–49. <https://doi.org/10.26620/uniminuto.inventum.4.6.2009.46-49>).

1. Glosario:
2. Hacker: Un hacker es una persona curiosa, que se interesa en todo tipo de tecnología principalmente, pero el termino incluso se podría ampliar hacia otros campos del saber humano.
3. SO: Sistemas operativos dedicados a la realización de distintas tareas en un hardware determinado.
4. Hardware: Componentes físicos de un sistema informático.
5. Software: Componentes digitales de un sistema informático.
6. Ataque informático: Evento en el cual, mediante distintas técnicas de infiltración, se prueba o se intenta corromper la seguridad al acceso de información de un sistema.
7. Hacking ético: Conjunto de actividades mediante las cuales se prueba la confiabilidad de un sistema informático y que son legales hasta cierto limite.
8. Sniffing: Se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en Internet.
9. OWASP: OWASP Foundation. “Guía de pruebas OWASP versión 3.0”.
10. Respuestas.
11. ¿Por qué genera controversia plantear el hacking ético como un medio de prevención de ataques a futuro?

Para atrapar a un intruso, se necesita pensar como uno, bajo esta premisa nace el concepto de hacking ético. (Rojas, M. E. F. (2018, 6 agosto). Hacking ético: una herramienta para la seguridad informática. Universidad Piloto de Colombia. <http://repository.unipiloto.edu.co/handle/20.500.12277/2932>).

Se puede decir que; con muchas seguridad, el hacking ético (6) es la única manera en gran medida por la cual se pueden prevenir y asegurar frente a los ataques los sistemas informáticos; si no se identifican las vulnerabilidades y comiencen los ataques informáticos(5), es solo cuestión de tiempo en que lleguen a ser explotadas. (Rojas, M. E. F. (2018, 6 agosto). Hacking ético: una herramienta para la seguridad informática. Universidad Piloto de Colombia. <http://repository.unipiloto.edu.co/handle/20.500.12277/2932>).

Cuando en 1997, la cultura de la seguridad informática comenzó a tomar fuerza, se pensó que los hackers éticos podían ofrecer sus servicios a las empresas para ayudarlas a ser menos vulnerables, y en 2001 arrancaron en forma este tipo de asesorías.

Convencer a las compañías de contratar un hacker, por mucho que se llame ético, y conseguir el permiso para que ingrese y juegue con sus sistemas no ha sido fácil. “No puedes llegar y simplemente decir te ofrezco un hackeo ético, debes explicar muy bien qué es esto y cuáles son los objetivos”, comenta Luis Alberto Cortés, consultor en seguridad y hackeo ético

Así, el término poco a poco se ha ido aceptando, ahora los hackers éticos empiezan a ser conocidos y buscan sus servicios. Por otra parte, grandes empresas de seguridad, como Ernest & Young o Price Waterhouse, han empezado a ofrecer servicios de hackeo ético, lo cual ayuda a generar mayor confianza en este tipo de asesorías.

(Soriano, G. A. (2017, 3 agosto). Hacking ético: mitos y realidades. Rutic. <https://www.ru.tic.unam.mx/handle/123456789/1761>)

¿Qué evalúa un hacker ético?

Los servicios que con mayor frecuencia ofrecen los hackers blancos (hackers éticos) a las empresas son las pruebas de penetración, con la intención de analizar si la compañía está preparada para soportar un ataque sofisticado perpetrado desde fuera, es decir por un hacker externo o por un atacante interno con conexión a la red.

Durante las pruebas de penetración, según enumera Víctor Chapela, se analizan tanto la red interna, como Internet, aplicaciones expuestas, servidores, puertos y avenidas de acceso, además se hacen pruebas de contraseñas. Al mismo tiempo, se analiza la red inalámbrica, de ésta se revisa la configuración, se hace sniffing [7] de tráfico y contraseñas, intentando penetrar y romper el cifrado.

Parte de la auditoría incluye también revisar módems y hardware (3), VPN, páginas webs así como demás sistemas de software(4), incluso se hace ingeniería social, es decir se trabaja con el personal o con los asociados de la empresa para ver si se dejarían engañar para proporcionar contraseñas o acceso a la red.

De igual forma, se mide el nivel de respuesta a incidentes internos, también se busca emular si un empleado de bajos privilegios podría tener acceso a los estados financieros o a la nómina de la compañía. Se consideran además los valores de los activos, la criticidad de la vulnerabilidad y la probabilidad del ataque, su impacto, la forma de corregirlo y el esfuerzo requerido para esto.

Para evitar cualquier contratiempo o daño a la infraestructura, o continuidad de negocio del cliente, las pruebas siguen una metodología y manejan estándares, como el Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, por sus siglas en inglés) o el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP).

Según el Mapa de Seguridad propuesto por el OSSTMM (8), las secciones a las cuales se aplican el hacking ético son las siguientes:



(Soriano, G. A. (2017, 3 agosto). Hacking ético: mitos y realidades. Rutic. <https://www.ru.tic.unam.mx/handle/123456789/1761>)

Bajo esta argumentación anteriormente expuesta, se puede afirmar con seguridad que las razones por las cuales el hacking ético es un tema polémico al plantearse como una solución de prevención mas que de solución de ataques informáticos es debido principalmente a la mala fama con la cual se han etiquetado a los diversos tipos de hackers que existen como bien lo argumentó (Soriano G.A, 2017), y por igual, debido al desconocimiento de las distintas técnicas y referencias de estándares autorizados incluso por organizaciones de calidad como ISO, para el uso y desarrollo del hacking ético; al desconocerse dichas regulaciones, se tiende a etiquetar en extremo, dicha actividad y a dichos profesionales como criminales dedicados a la simple cotización y destrucción de sistemas informáticos construidos.

1. Conclusión:

El hacking ético es una técnica aplicada a distintos escenarios, por lo que es importante hacerlo del conocimiento de la gente en beneficio de las organizaciones; así la relación entre detección y explotación de vulnerabilidades existentes podrá controlarse de la mejor manera posible.

Como se pudo constatar, el hacking ético no es una actividad generada y desarrollada por organizaciones y/o actores en calidad de criminales, que se dediquen simplemente a arruinar los sistemas informáticos de las empresas por mero disfrute o diversión, sino mas bien enfocados en un objetivo en común; prevenir futuros ataques de organizaciones y actores en el papel de verdaderos criminales que efectivamente puedan ocasionar daños irreparables a dichos sistemas informáticos.