INSTITUTO TECNOLÓGICO
JOSÉ MARIO MOLINA
PASQUEL Y HENRÍQUEZ
ZAPOPAN

TECNOLÓGICO MARIO MOLINA PASQUEL Y HENRÍQUEZ.

HACKING ÉTICO.

LUIS ALBERTO VARGAS GONZÁLEZ.

TALLER DE INVESTIGACIÓN 1.

IRMA TOSCANO BARAJAS.

GUADALAJARA,JALISCO A 9 DE MAYO DE 2022.

Contenido

.

1.

Primero que nada:¿Que es el hacking ético?

El hacking ético, también llamado de sombrero blanco, hace referencia al modo en que una persona, mejor conocida como hacker, utiliza todos sus conocimientos sobre informática y ciberseguridad para hallar vulnerabilidades o fallas de seguridad dentro de un sistema.

Los hackers éticos son expertos en seguridad de la información que irrumpen en los sistemas informáticos por petición de sus clientes. Se considera ética esta variable porque existe un consentimiento previo por parte de la “víctima”, es decir, el cliente, para detectar las fallas.

Objetivo de la investigación.

Conocer las ventajas y desventajas de la práctica del hacking ético a nivel sociedad, empresarial y gubernamental.

Planteamiento del problema.

¿Por qué genera controversia plantear el hacking ético como un medio de prevención de ataques a futuro?

El hacking ético nace como medida para combatir a los piratas informáticos con malas intenciones. Las empresas contratan a estos profesionales porque necesitan probar su seguridad. Al otorgar su permiso, efectivamente cubren sus ojos y oídos corporativos mientras se llevan a cabo estas pruebas.

Tipo de investigación.

Investigación de tipo explicativa; Se explicarán las relaciones de causa y efecto por las cuales se llevó a el fenómeno del hacking ético, el cual ha llevado a mucha controversia en su uso debido a sus métodos poco ortodoxos para la prevención de ataque.

Hipótesis.

El Hacking Ëtico es la única manera de combatir los peligros y amenazas que las empresas y la sociedad sufren año tras año.

Justificación.

Debido a las crecientes exposiciones de amenazas en la red , los empresarios y miembros de la sociedad se ven obligados a buscar distintas opciones de mitigación de las mismas, por lo que el Hacking Ëtico se vuelve una opción muy usada por toda clase de miembros de la sociedad y del mundo empresarial, es un tema altamente discutido, debido a esas crecientes exposiciones se predice que será la única manera de mitigar estos riesgos en la red, más precisamente con la llegada de nuevas tecnologías como el metaverso , lugar donde se podría interactuar con elementos hasta ahora físicos , haciéndolos virtuales.

Impactos;social,empresarial y gubernamental.

Al tener un crecimiento exponencial del uso de la red de internet para todo tipo de actividades , ya sean educativas , personales, sociales y empresariales , una correcta y bien implementada investigación acerca del hacking ético sería de gran ayuda para entender el impacto económico, social y sobre todo tecnológico en la creación de nuevos trabajos relacionados al hacking ético y prevención de amenazas, a la constante evolución de las plataformas de seguridad (TPM) de los computadores, a la adaptación de más y mejores protocolos de red e interconexiones, se puede argumentar que ; el impacto de esta investigación se podría dar en estos tres sectores del desarrollo humano a nivel global.

Glosario.

1. Hacker: Un hacker es una persona curiosa, que se interesa en todo tipo de tecnología principalmente, pero el término incluso se podría ampliar hacia otros campos del saber humano.
2. SO: Sistemas operativos dedicados a la realización de distintas tareas en un hardware determinado.
3. Hardware: Componentes físicos de un sistema informático.
4. Software: Componentes digitales de un sistema informático.
5. 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.
6. Hacking ético: Conjunto de actividades mediante las cuales se prueba la confiabilidad de un sistema informático y que son legales hasta cierto límite

Glosario

7. 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.

8. OWASP: OWASP Foundation. “Guía de pruebas OWASP versión 3.0”.

Introducción profundizada a investigación.

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 término 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

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

Desarrollo.

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 comienzan 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

16

Qué evalúa un hacker ético?

Principalmente pruebas de penetración a sistemas de archivos y documentos confidenciales.

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:

Respuesta a la pregunta de investigación.

¿Por qué genera controversia plantear el hacking ético como un medio de prevención de ataques a futuro?

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 más 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.

Viabilidad.

Métodos de la investigación:

El presente proyecto se basa en una investigación de tipo explicativa y completa sobre todo lo referente al hacking ético, sus implicaciones en la sociedad civil, empresarial, y gubernamental. Por lo tanto, el tipo de alcance de la investigación es meramente descriptiva y explicativa referente a la pregunta de investigación

Viabilidad

Materiales de la investigación.

Para completar dicha investigación se necesita de: 1. Editor de textos para escribir todos los documentos de la investigación. 2. Bibliografías (mínimo 10 de ellas). 3. Encuesta a la sociedad civil sobre la investigación y sus aristas de valor y de ventajas y desventajas del hacking ético

Viabilidad

Recursos teóricos.

El tema de investigación cuenta con revistas científicas, tecnológicas, artículos de investigaciones previas, citados y fechados correctamente, videos e informes de investigación.

Viabilidad

Recursos humanos.

El estudio poblacional será realizado a integrantes de la sociedad en general, conformada por ingenieros, abogados, profesionistas de diversas ramas del saber, personas con educación mínima requerida y personas con educación sobresaliente por igual.

Recursos de tiempo (temporal).

El presente trabajo será realizado en un corto plazo de aproximadamente 6 meses de duración dentro del año 2022, los cuales conforman el semestre general completo en el que se está solicitando dicha investigación.

Recursos financieros.

Se requieren recursos monetarios propios del investigador, ya que son mínimos los requerimientos de uso monetario y no necesitan ser extraídos de ninguna entidad financiera pública o privada.

Validación

Al ser realizada la encuesta hacia la sociedad civil en general, se sacaron distintas conclusiones acerca de las respuestas de dicha encuesta.

1. La sociedad tiene poco conocimiento y poco tiempo de haberse involucrado en los temas de ciberseguridad, seguridad en redes sociales y sistemas, y en hacking ético.

2. Se tiene muy poco claro la diferencia entre hacking ético y el ilegal.

3. Las personas no han recibido en ningún medio de desarrollo de si mismas (escuela, trabajo, familia) la educación e información necesaria para poder llevar a cabo prácticas seguras de ciberseguridad y por consiguiente de hacking ético por parte de algún especialista.

Validación.

6. Pocos integrantes de la sociedad han estado inmersos en alguna práctica de ciberseguridad y/o de hacking ético.

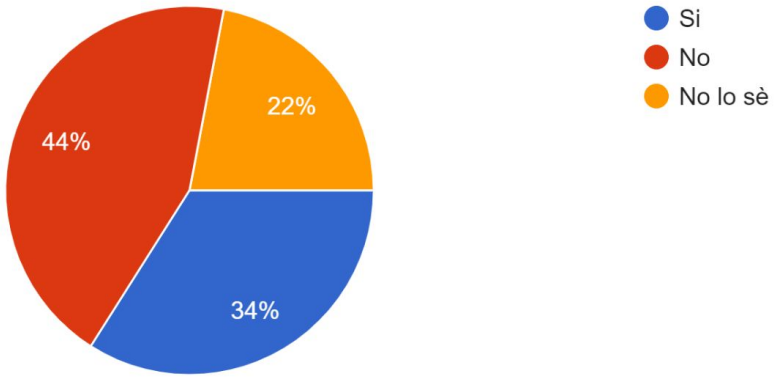
7. Existe un alto índice de personas que han sufrido un ataque o no se han dado cuenta de ello de software o de hacking informático.

8. El 70% de encuestados están de acuerdo con la conclusión de (Rojas M.E.F 2018(6 de agosto)) “Para atrapar a un intruso, se necesita pensar como uno, bajo esta premisa nace el concepto de hacking ético.”

Validación.

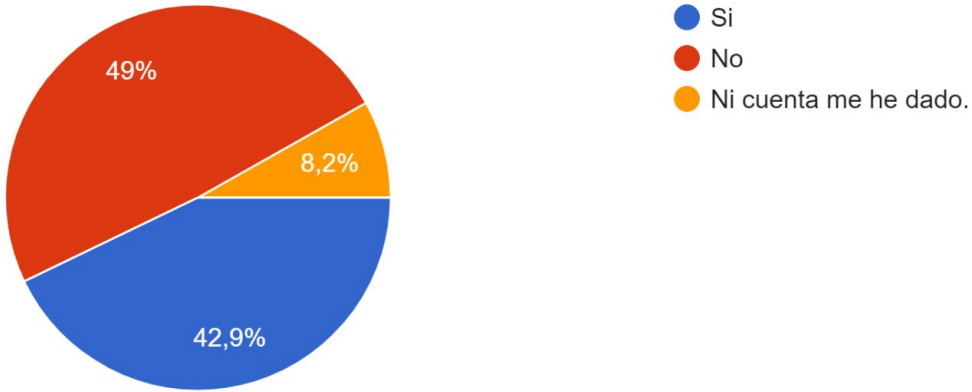
¿Sabes la diferencia entre hacking ético, y hacking ilegal ??

50 respuestas



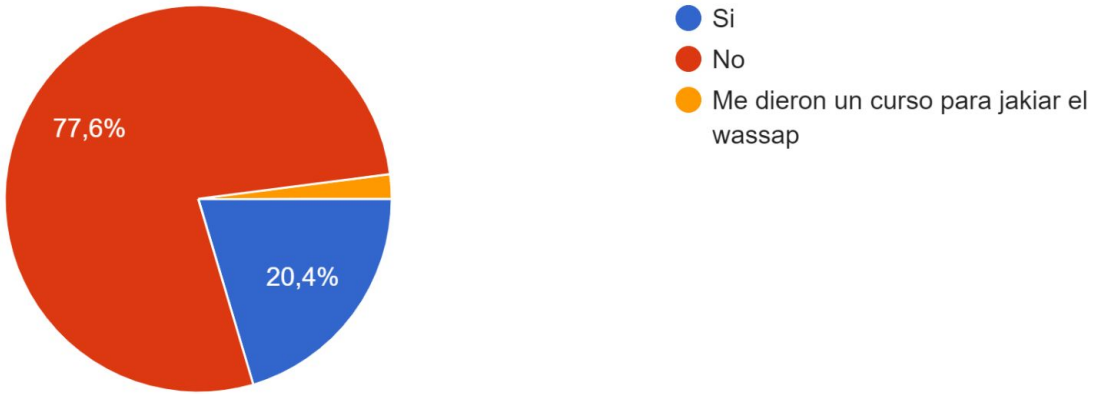
¿Alguna vez has tenido problemas de hackeo en las tecnologìas que usas ? Ejemplo: filtración de tus datos como fotos, contactos , chats , cuentas d...es sociales, suplantación de identidad, phishing ?

49 respuestas



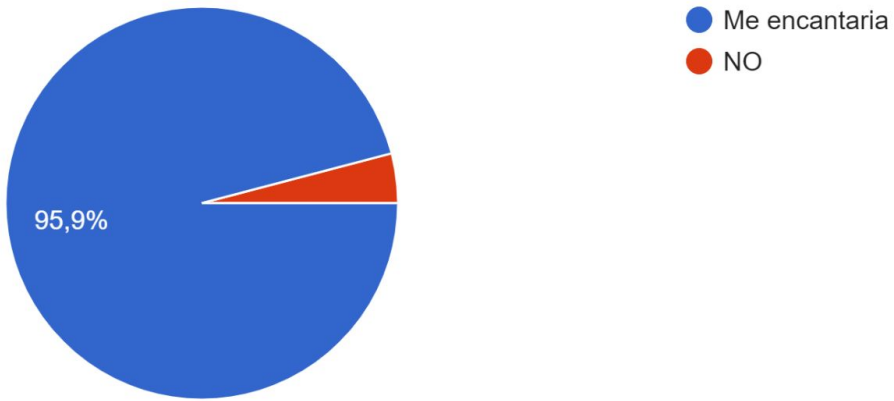
Alguna vez has recibido educación para la prevención de algún problema informàtico o de hackeo por parte de un especialista ?

49 respuestas



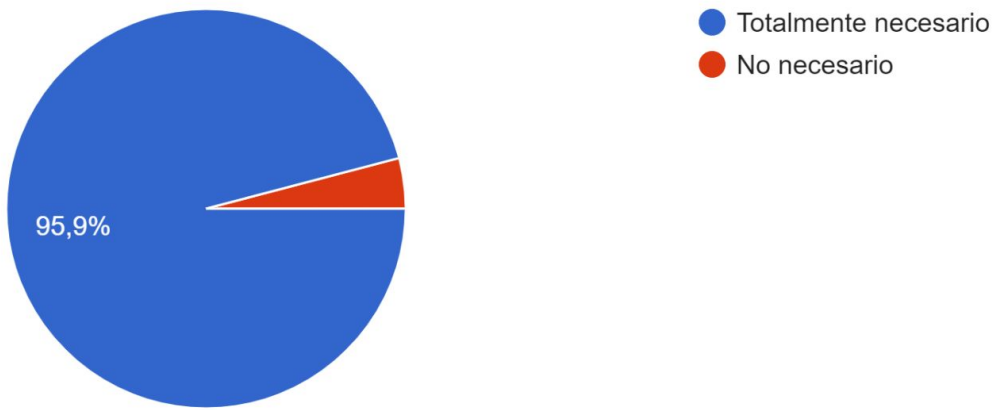
Te gustaría que en tu trabajo , escuela o medio de desarrollo, te enseñaran más tècnicas para la prevención del hacking ilegal?

49 respuestas



Después de haber contestado todas estas preguntas , analiza un poco tus respuestas y reflexiona: ¿Es importante el hacking ético para la prevención de cientos de errores y amenazas de la tecnologìa?

49 respuestas



Para finalizar¿Consideras que el hacking ético es la única opción viable para poder combatir las amenazas de hacking ilegal ??

49 respuestas

Análisis alternativa de solución.

Para poder llegar a la solución determinada de los objetivos de la investigación se requiere de un proceso bastante complejo y quizás por igual lento en cuanto a velocidad se refiere, el cual se describen algunas aristas de valor y de cobertura del mismo.

Objetivo: Conocer las ventajas y desventajas de la práctica del hacking ético a nivel sociedad, empresarial y gubernamental.

1. Difundir con cursos, talleres, informes, medios didácticos de aprendizaje, videos, conferencias, reuniones de carácter tanto civil, empresarial y gubernamental de manera continua y masiva la práctica del hacking ético a las 3 entidades anteriormente descritas.

2. Investigar en medios fiables de información los avances y problemas del hacking ético y del ilegal en los medios anteriormente descritos.

3. Involucrar a las empresas desarrolladoras de las tecnologías de uso masivo para que ellos cumplan con una función de auditoría y de enseñanza a la sociedad tanto de su medio empresarial, civil y gubernamental de cómo estructuran, realizan y corrigen pruebas de seguridad, además de su intervención en la práctica y mejoramiento de dichas arquitecturas de red, de computación, y de los procesos de hacking ético.

4. Involucrar a las instituciones de educación básica y superior para la enseñanza y adecuación de planes de estudio estructurados

Bibliografía

1. M.A, A. R. (2008, 17 septiembre). Ethical Hacking - CapÃtulo I - Por quÃ© â €œEthical Hackingâ€•? Digital Books.

http://reader.digitalbooks.pro/book/preview/42132/x630-fanjul-v2- 8?1646353528618

2. N.L, M. A. & Universidad Internacional SEK-Ecuador. (2014, 9 octubre). UANL. Universidad Internacional SEK-Ecuador.

https://core.ac.uk/download/pdf/236645046.pdf

3. Soriano, G. A. (2017, 3 agosto). Hacking ético: mitos y realidades. Rutic.

https://www.ru.tic.unam.mx/handle/123456789/1761

4. 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

5. 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

6. Giannone, A. O. (2019, 21 octubre). UTN - RIA - Método de inclusión de hacking ético en el proceso de testing de software. UTN. https://ria.utn.edu.ar/handle/20.500.12272/4068

7. O.S, J., & O.R:, A. (2015). Seguridad Informática; Conocer el ataque para una mejor defensa (3.a ed., Vol. 1) [Libro electrónico]. Ediciones ENI.

8. Rodriguez, L. A. E. (2020). Herramientas fundamentales del hacking ético. Medigraphic. https://www.medigraphic.com/cgibin/new/resumen.cgi?IDARTICULO=94154

9. Sandoval, H. M. E. (2016, 15 noviembre). Repositorio Digital - EPN: Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado. Bibdigital. https://bibdigital.epn.edu.ec/handle/15000/16836

10. Harris;Harper;Allen;Ness;Lester, S. A. E. C. J. M. (2005). Alianza SIDALC. SIDALC. http://www.sidalc.net/cgibin/wxis.exe/?IsisScript=SIDINA.xis&method=post&formato=2&cantidad=1&expresion=mfn=003628