

Taller de Investigación 1.

Primera parte del protocolo de investigación.

Luis Alberto Vargas González.

Fecha:16/02/2022.

Maestra: Irma Toscano Barajas.

Escribir los primeros tres elementos del protocolo de

investigación utilizando el tema de su elección.

1.- Tema

2.- Objetivo

3.- Planteamiento del problema

4.- Tipo de investigación

1. Hacking Ético.
2. Conocer las ventajas y desventajas de la practica del hacking ético a nivel sociedad, empresarial y gubernamental.
3. ¿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.

1. 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 ataques.

Escribir la segunda parte del protocolo de investigación

utilizando el tema de su elección.

5.- Hipótesis

6.- Justificación

7.- Impactos

\* Social

\* Tecnológico

\* Económico

\* ambiental

1. El Hacking Ëtico es la única manera de combatir los peligros y amenazas que las empresas y la sociedad sufren año tras año.
2. 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, mas precisamente con la llegada de nuevas tecnologías como el metaverso , lugar donde se podría interactuar con elementos hasta ahora físicos , haciéndolos virtuales.
3. 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 seria 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.

Desarrollo:

\*\*Introducción al tema de investigación

\*\* Elaborar un mapa mental o un índice de las fuentes bibliográficas que utilizaras

para dar solución a las hipótesis planteadas.

Introducción al Hacking ético.

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 esta 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 mas cuantiosa.

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.

**Índice de referencias.**

1. M.A, A. R. (2008, 17 septiembre). *Ethical Hacking - CapÃ­tulo I - Por quÃ© âEthical 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/cgi-bin/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/cgi-bin/wxis.exe/?IsisScript=SIDINA.xis&method=post&formato=2&cantidad=1&expresion=mfn=003628>