



¿Quieres ser un hacker ético? Un experto que hackea desde los 6 años te da unos tips

CIUDAD DE MÉXICO. 26 de enero de 2023.- Desde que Santiago Rosenblatt tenía 6 años de edad, despertó una peculiar curiosidad por ingresar a los sistemas de los videojuegos y plataformas que consumía diariamente, y encontró que tenían medidas de seguridad poco robustas y expuestas a vulnerabilidades.

Eso, sin lugar a dudas, fue un parteaguas para incrementar su pasión por construir soluciones innovadoras y útiles que le permitieran ayudar a resolver problemas, y que en el presente ha sido la base para ayudar a muchas empresas a que mejoren sus sistemas de ingeniería informática y ciberseguridad.

Lo anterior se vuelve muy importante sobre todo en un contexto como el actual, en el que se prevé que amenazas como el *ransomware* le costarán a las empresas a nivel global hasta USD \$265 mil millones anuales hacia 2030, de acuerdo con [KPMG](#).

De ese modo, la importancia de que las organizaciones se apoyen de los servicios de un *hacker* ético se incrementa, motivo por el cual es crucial que cada vez más personas se adentren en el mundo de *hacking*, pero no con fines maliciosos, sino con el objetivo de ayudar a las empresas a protegerse.

Y sí, aunque exista quienes creen que el robo de datos y el secuestro de información puede dejar mucho dinero, es importante destacar que el *hacking* ético también es una forma de obtener ingresos muy relevantes sin incurrir en la ilegalidad. Datos de [Glassdoor](#) indican que los *hackers* éticos obtienen un sueldo promedio de USD \$113,500 al año (poco más de 2.2 millones de pesos)

Así que si eres entusiasta del *hacking* ético, Santiago Rosenblatt comparte los siguientes consejos que serán importantes para lograrlo:

- Investiga y no dejes de investigar

Esto se debe a que el cibercrimen no deja de evolucionar. Por ese motivo, los conocimientos en protección de sistemas y *hacking* no son algo que se aprenda una sola vez y se pueda emplear para siempre. Por el contrario es importante estar siempre inmiscuido en cursos, lecturas y todo tipo de programas que ayuden a nutrir más y más los conocimientos sobre la forma en la que se puede intervenir un sistema, conocer más técnicas de detección de vulnerabilidades y saber qué amenazas son las más latentes.

- Ningún *background* es obsoleto.



Este consejo básicamente está orientado para quienes son entusiastas del *hacking* pero que no tienen *background* en sistemas y Tecnologías de la Información (TI). Si bien será importante que estudien algún curso y/o carrera enfocada en programación, informática o materias relacionadas a los sistemas, deben saber que los conocimientos que adquirieron en cualquier otro sector no son obsoletos y, por el contrario, forman parte de las herramientas que necesitarán al convertirse en *hackers*.

Esto se debe a que todas las empresas de todos los sectores están sumamente expuestas al cibercrimen en la actualidad. Por eso, contar con conocimientos en *hacking* y al mismo tiempo saber de qué forma se mueven las industrias que requieren de la protección de un *hacker* ético, puede representar una ventaja competitiva al momento de crear estrategias para salvaguardar los datos de una compañía.

- **Certifícate en alguna tecnología**

Las empresas dedicadas a la ciberseguridad requieren expertos que no solo tengan un amplio *background* en TI y sistemas, sino que tengan conocimientos sobre diversas especialidades para abarcar una mayor cantidad de conocimientos.

Por ejemplo, en el caso de Strike, colaboran *hackers* éticos especializados en materias como *crypto*, *e-commerce*, *healthtech* y *fintech* por mencionar un ejemplo. Entre mayor sea el nivel de especialización del *hacker* ético, más valioso y confiable será para la compañía que lo contrata al momento de optar por sus servicios.

- **Conoce más sobre los pentesting**

Es importante saber que el *pentesting* es uno de los métodos más demandados en la actualidad por parte de las empresas que acuden al *hacking* ético. Es por eso que es importante saber con exactitud qué se necesita para realizar este tipo de análisis manual en los sistemas de las empresas, mediante los cuales se encuentran vulnerabilidades como lo haría un *hacker* malicioso, pero con el objetivo de ayudar.

Los escaneos tradicionales para las compañías les entregan resultados hasta después de un mes y medio, lo cual puede ser demasiado tiempo para reparar una vulnerabilidad. Como *hacker* ético, utilizando el *pentesting*, se pueden entregar resultados a las empresas que contraten el servicio hasta en menos de 24 horas.

Es importante decir, para concluir, que el trabajo de los *hackers* éticos es fundamental actualmente y seguirá siéndolo, pero también implica una enorme responsabilidad. La confianza de las empresas está en las manos del especialista que se encargará de adentrarse al sistema y encontrar vulnerabilidades, por lo que es importante siempre trabajar bajo un



enfoque de ética que permita entregar resultados positivos y generar un ambiente de confiabilidad con el cliente.

“Desde la fundación de Strike, nos hemos enfocado en reunir a los mejores hackers éticos del mundo, los más preparados y certificados a nivel internacional, a través de rigurosos procesos de autenticación y confianza para tener un equipo muy robusto y sofisticado en cuanto a técnicas de hacking, con el objetivo de realmente ayudar a las empresas a protegerse de mejor manera. Esto se debe además a que cada día crece más la necesidad de tener este tipo de especialistas a la mano, por lo que es importante que cada vez más personas se interesen por capacitarse en el rubro y defender a las empresas de los cibercriminales”, concluye Santiago Rosenblatt.

Sobre Strike

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: <https://strike.sh/>

Síguenos en nuestras redes sociales:

Instagram - @strikesecurity

Twitter - @strike_secure

LinkedIn - Strike

Contacto para prensa México

another

Ahtziri Rangel | PR Expert

+ 52 1 55 1395 6970

ahtziri.rangel@another.co