

Introducción

¿Por dónde comienzo? Esa es, quizás, la pregunta más habitual que se hace todo aquel interesado en ingresar al universo heterogéneo que contempla la seguridad de los sistemas y sus activos. No es de extrañarse que esto sea así si tenemos en cuenta que hay demasiado material y que no hay una correcta plataforma o programa actual de educación formal sobre el tema.

Como si eso fuera poco, esto sucede en un momento de la historia en el que existe un auge de organizaciones altamente informatizadas en el que no hay dos iguales y en el que todas son bastante desorganizadas. Éstas utilizan Internet como recurso de comunicación para hacer movimientos constantes de información institucional pero apenas están tomando conciencia de la seguridad de la información y del alto valor que tiene ésta hoy en día.

En las páginas de este libro intentaré ser lo más claro posible en los conceptos y en el desarrollo, a través de palabras y definiciones sencillas. No sólo para que sea llevadera e interesante la lectura sino también para que desde un principiante estudiante de sistemas o ejecutivo interesado, hasta el técnico sin demasiada experiencia, descubran y aprendan acerca de este tema desde el principio y en forma ordenada. Por eso, cuando sea conveniente extender la explicación o el desarrollo de algún punto que no sea central, daré a conocer algún documento, recurso online o sitio web para su consulta.

La temática está basada en la descripción detallada de las técnicas básicas y usuales de ethical hacking, más precisamente de un Network Security Assessment externo (comprobación de seguridad en red cuyo contenido no está alineado a ninguna certificación, metodología o curso de ese estilo). También habrá introducciones teóricas sobre aspectos del ethical hacking, notas relacionadas a la formación ideal de un profesional de la seguridad, gestión de organizaciones formales y la utilización de herramientas y metodologías, entre otras cosas. Además, se verán conceptos propios acerca de los escenarios personales o la importancia de generar errores en un chequeo, como también recomendaciones de muchos otros recursos serios en cuanto a material de estudio.

En estas páginas que no se entrará en detalles sobre cómo explotar algunas vulnerabilidades que existen hoy en día porque éstas probablemente serán solucionadas muy pronto, y de ese modo el libro o gran parte de él, se tornaría obsoleto. Esto se debe a que un grupo de profesionales tarda mucho menos en programar la solución o en redactar un excelente whitepaper (documento) sobre ello que lo que tarda la imprenta en imprimir esta edición. Como esto haría que leer este libro diera la misma sensación que leer un periódico viejo, es preferible

concentrarse en dónde ir a buscar esa información para obtenerla a diario y así hacer que la teoría que aquí se expone sea útil en mayor porcentaje y por más tiempo. Esto será aplicable a la mayoría de los casos de ethical hacking o de seguridad informática (y de la información) con los que nos podamos encontrar y nos permitirá estar informados de modo correcto a través de canales eficientes. El fin de este libro es comunicar conocimiento significativo sobre la materia, apuntando a aquellos que desean iniciarse o descubrir nuevos puntos de vista. Espero que lo disfrute.

Carlos Tori.