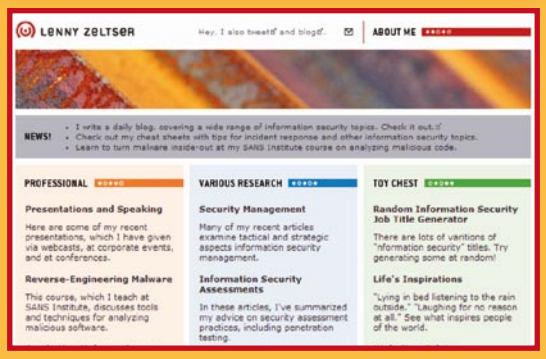
VISITA RECOMENDADA

http://zeltser.com
http://blog.zeltser.com



En esta ocasión recomiendo la visita de un sitio web creado y elaborado por **Lenny Zeltser**. Lenny no sólo es uno de los pocos profesionales de la seguridad que posee la certificación, altamente técnica, GSE de SANS, sino que también es MBA por la Universidad MIT Sloan. Ambos ingredientes son la clave de una valiosa mezcla de conocimientos de seguridad y de gestión en su sitio web **zeltser.com** y, especialmente, en su *blog* (localizado en **blog.zeltser.com**).

Navegar por zeltser.com es fácil: En la parte superior de la página principal Zeltser enlaza con su presencia en Twitter, su *blog* y con sus conocidas guías rápidas ("cheatsheets"): Twitter se ha convertido en la fuente más inmediata de noticias, también en el mundo de la seguridad. El quid está en seguir a aquellos proveedores de información real y relevante, Lenny es uno de ellos. Su *blog* es una fuente de conocimiento práctico. Sus guías rápidas son valiosas unidades comprimidas de contenido de seguridad, muy útiles para no reinventar la rueda cuando es necesario elaborar procedimientos básicos de seguridad, por ejemplo, en gestión de incidentes o análisis forense.

La portada de zeltser.com contiene tres columnas

• La primera columna se dedica a su aventura profesional, con enlaces a las presentaciones que realiza y a los cursos de SANS de los que es uno de los autores, como son el de ingeniería inversa y el de análisis de software maligno ("malware"). Ambos cursos son de una calidad técnica elevada, muy recomendables para analizar los ataques dirigidos a empresas basados en enlaces o ficheros adjuntos.

Lenny Zeltser utiliza en sus presentaciones el formato tradicional de diapositivas con notas en un fichero pdf, así como ficheros de audio e incluso "webcasts". Dos presentaciones a destacar son las relacionadas con la presencia de "malware" en las redes sociales y la de gestión de incidentes de seguridad "inesperados". Su contenido es preciso y facilita claridad de ideas en estos temas. También incluye el enlace a sus libros de análisis forense y seguridad en redes, del que es coautor junto a, entre otros, **Stephen Northcutt**.

• La segunda columna integra sus contenidos de investigación en seguridad, con temas tan fundamentales como la gestión eficiente de eventos históricos ("logs") o cómo presentar auditorías de seguridad que proporcionen valor al negocio. En esta sección también están presentes contenidos más genéricos sobre la historia de la tecnología (con episodios que tratan sobre radio o educación en Internet, entre otros).

• La tercera columna es más alternativa. Podemos divertirnos haciendo uso de un generador de títulos para posiciones de seguridad o leyendo frases que contribuyen a la inspiración diaria del lector. Demostrando que los profesionales de la seguridad suelen tener aficiones muy distintas a su quehacer laboral diario, encontramos un enlace a un rincón de poesía, con poemas suyos de 2005.

El *blog* de Lenny Zeltser requiere una mención especial. Ya ha cumplido un año. Con el compromiso de escribir un artículo cada día, aborda temas de seguridad muy actuales, con un destacado componente de reflexión y análisis y con limitados tecnicismos. Cada sábado publica una colección de enlaces a sus lecturas de seguridad favoritas de esa semana (artículos, *blogs*, papeles disponibles en Internet).

Finalizo con una sentencia del orador **Denis Waitley** que cita Lenny Zeltser en su sitio web, "Espera lo mejor, planea para resistir lo peor y prepárate para la sorpresa". Este *blog* nos ayuda precisamente a eso.

Alberto Partida Rodríguez
Especialista en Seguridad TI
http://securityandrisk.blogspot.com
http://twitter.com/itsecuriteer
Sugerencias y comentarios:
itsecuriteer@gmail.com