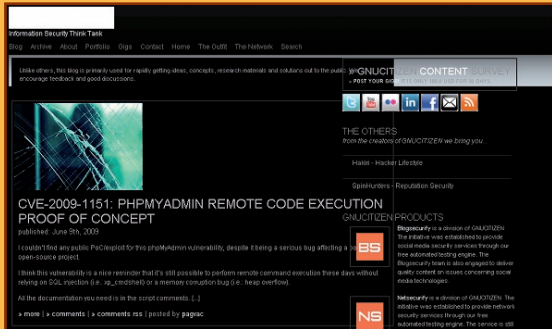




VISITA RECOMENDADA

gncitizen.org



metedores para pruebas de penetración.

- Una reflexión sobre cómo podría usarse una aplicación para el iPhone como sencilla herramienta para obtener información útil a la hora de robar en viviendas en Estados Unidos.

En 2008, el blog de gncitizen.org saltó a la prensa por la descripción publicada sobre cómo comprometer el “router” ADSL más popular y extendido en los hogares del Reino Unido.

En las páginas de este sitio, a la derecha, se presentan una serie de productos de seguridad, algunos

Según el diccionario Espasa, la palabra “hacking” se traduce al castellano como “piratería informática”. Dicho término tiene como segunda acepción “el delito contra la propiedad física e intelectual”. El sitio que recomiendo visitar en este número de septiembre de 2009 de nuestra revista SIC, **gncitizen.org**, propone una definición alternativa de “hacking”: *ser más “listo” que los demás*. De este modo, el concepto de “hacking” aparece en cualquier escenario, sea técnico o no.

Gncitizen.org se crea, o mejor dicho, se rediseña, en 2006 de la mano de **Adrian Pastor** (conocido como “pagvac”) y **Petko D. Petkov** (conocido como “pdp”). Son dos expertos en seguridad localizados actualmente en el Reino Unido que se conocieron estudiando informática en Londres. Compartían el interés por la seguridad e idearon un blog en inglés que pronto se dio a conocer entre los profesionales del sector por su carácter práctico e innovador y también por preferir calidad a cantidad, punto que se agradece cuando la mayoría de nosotros frecuentamos regularmente ya un número considerable de sitios web.

Cada mes Petko o Adrian publican tres o cuatro artículos relacionados con pruebas de seguridad perimetral (“penetration testing”), seguridad en aplicaciones web, así como seguridad en sistemas embebidos<sup>1</sup>: una problemática muy actual, poco estudiada hasta ahora, pero imprescindible en un futuro ya presente dada la “ubicuidad” de dichos dispositivos.

Se accede al blog de gncitizen.org directamente desde la página principal del sitio web. Como ejemplo, estos son los contenidos tratados en tres de sus últimas entregas:

- Una prueba de concepto, código fuente incluido, que explota la vulnerabilidad descubierta en phpadmin (CVE-2009-1151).
- Cómo comprometer la seguridad de una cámara IP marca Linksys utilizando para ello la vulnerabilidad CVE-2008-4390.
- Un nuevo repositorio de código en Jeriko. Jeriko es una colección de “scripts” muy pro-

de ellos pendientes de lanzamiento. Describiré brevemente tres de ellos:

- “Securls” es una colección de las últimas noticias relacionadas con la seguridad aparecidas en lugares reputados de Internet, muy similar a lo que uno mismo puede construirse manualmente con un lector RSS o servicios como “google reader”. Sin duda, éste es el servicio que más interés inicial puede despertar entre los lectores.

- “Blogsecurify” ofrece una sencilla auditoría gratuita de seguridad para cualquier blog publicado en wordpress del que se sea autor. Está basado en el uso de un motor automático de pruebas. Eso sí, para ello se necesita mencionar en el blog el nombre de su herramienta. Los resultados obtenidos no son excepcionales pero sí dan una pista sobre si el blog es vulnerable a ataques de “cross site scripting”.

- “Secapps”, por último, ofrece una consola del lenguaje de programación “python” basada en Java y da acceso a un proyecto de pruebas de seguridad en aplicaciones web con el nombre de “WebAcid”.

Para finalizar, me gustaría citar dos sitios alternativos creados también por los mismos autores cuyos enlaces se encuentran en gncitizen.org bajo el epígrafe “los otros” (“the others”): **hakiri.org** y **spinhunter.org**. Hakiri.org versa sobre el estilo de vida “hacker” mientras que spinhunter.org, actualizado con menos frecuencia, lo hace sobre relaciones públicas y reputación. En la primera, como ejemplo de las reflexiones que proponen los autores, cabe destacar el enlace a una breve intervención del autor **Seth Godin** en el marco de las charlas TED sobre por qué las tribus humanas cambiarán el mundo. En la segunda, se enlaza con un discurso del filósofo **Noam Chomsky** sobre propaganda corporativa y gubernamental. Cuando menos, abrirá ciertos interrogantes en la mente del lector/oyente.



**Alberto Partida Rodríguez**

Especialista en Seguridad TI

**Securityandrisk.blogspot.com**

Sugerencias y comentarios:

**apartidar@gmail.com**

<sup>1</sup> Con frecuencia, así se traduce la expresión “embedded systems”. Sin embargo, los filólogos recomiendan “sistemas inmersos” como traducción más apropiada al castellano.