Artículo del redactor jefe

Traducción de Textos

Curso 2007/2008

Versión	Cambio
1.4RC	Revisado el texto
1.3	Traducido el décimo tercer párrafo
1.2	Traducido el duodécimo párrafo

Autor:
Rubén Paje del Pino
i010328

Índice de contenido

1. Primer párrafo (corregido el 10-XII-07)

Es necesario tomar posiciones respecto a los hackers

¿Cómo debería ser nuestra relación con la comunidad "hacker". Es posible que recuerde la noticia de la revista "Security Views" del mes pasado que trataba del "hacking ético" y el "hacking bueno" en la que un joven de la India quien modificó una página web, luego se le dijo a su dueño como proteger su sitio de ataque y más tarde fue contratado por la agencia del gobierno de EE.UU. Más tarde el "Dynamic Duo" entró en la administración federal de la aviación (FAA) para demostrar que era vulnerable a ataques. No puedo sacar de mi cabeza estas historias y noticias, por tanto los estudiaré en el editorial de este mes. La principal cuestión a resaltar es el tipo y grado de relación con la comunidad hacker que nosotros como profesionales de la seguridad de la información debemos mantener.

2. Segundo párrafo (corregido parcialmente el 10-XII-07)

Para empezar, la llamada "comunidad hacker no se trata de una única entidad, es tan diversa como la comunidad de los "hackers blancos", curiosamente es tan antigua como la misma profesión de la seguridad de la información. La primera generación de hacker se ajustaba a su definición hacían público los programas que habían pirateado y como a menudo tenían recursos informáticos insuficientes, localizaban y luego utilizaban sistemas con suficientes recursos para compilar, ejecutar y validar sus programas, además su software servía de gran ayuda para la joven comunidad internauta. Sin embargo su problema era que muy a menudo no tenían autorización para utilizar los sistemas a los que accedían. Curiosamente, justificaban su comportamiento afirmando que los sistemas a los que accedían se infrautilizaban y en tanto en cuanto no se estropeaba nada estaba bien utilizar algunos ciclos sin carga útil. Nadie parecía conseguir superar el tope que ese tipo de acceso fue dando y no parecía haber ninguna ley que prohibiera dicho acceso en un primer momento.

3. Tercer párrafo (corregido el 10-XII-07)

Las cosas han cambiado drásticamente desde los tiempos de los primeros hackers. Internet hoy es enorme (posiblemente tiene unos 400 millones de usuarios ahora), está fuera de control y es francamente peligroso, principalmente debido a la actividad de una nueva raza de hackers. Lejos quedan los días en los que accedían a sistemas sin autorización rigiéndose por un código ético que abogaba por no dañar a las máquinas. El acceso no autorizado a Internet fue un común denominador en la mayoría de ataques que ocasionaron unos daños estimados en aproximadamente 445 millones de dólares según individuos de 223 organizaciones que completaron la encuesta FBI/CSI del 2002. Los ataques por denegación de servicio y las modificaciones de páginas web comprometen ahora las dos formas más frecuentes de incidentes a la seguridad en Internet. La legislación (a pesar se ser insuficiente en su mayoría) persigue ahora el acceso no autorizado en gran parte del mundo. De acuerdo con esto unos pocos de los profesionales de la seguridad de la información abogan por conocer lo que está haciendo la comunidad hacker – nosotros necesitamos conocer a nuestro enemigo, además de hablar. Otros van más lejos y contratan en la actualidad personas quienes realizaban accesos no autorizados en el pasado reiteradamente o quienes todavía se dedican a actividades ilegales. Su razonamiento es el siguiente: "nadie sabe mejor que ellos como romper la seguridad y como defender adecuadamente los sistemas y las redes".

4. Cuarto párrafo (corregido el 10-XII-07)

Una cuestión realizada durante el último año indicaba que más de un tercio de los directores de empresa desearían contratar a Kevin Mittnick, un condenado criminal informático, como consultor de seguridad. Algunos vendedores retan a los hacker con gran publicidad, invitando a cualquiera intentar romper la seguridad de su producto y si luego nadie puede marca su producto como "a prueba de hackers" o "probado por hackers". Y algunos miembros altamente respatados de la comunidad de la seguridad acuden y a veces dan charlas en las llamadas conferencias de hackers.

5. Quinto párrafo (corregido el 17-XII-07)

¿Hasta donde debe llegar nuestra relación con la comunidad hacker? Mi recomendación es que no muy lejos. Considere lo siguiente:

6. Sexto párrafo (corregido el 18-XII-07)

·¿Cuanto hemos aprendido de la comunidad hacker durante estos años? Me gustaría decir que hemos aprendido algo, pero no mucho para todo el tiempo, dinero y energía invertidos. Si ha asistido a alguna conferencia de hacker, es probable que este de acuerdo que, a menos que no supiera casi nada sobre las pruebas de intrusión antes que asistiera al evento, allí se aprende muy poco. Mi impresión sobre las conferencias de hackers a las que he ido es que la gente toma la palabra es la gente orgullosa de sí misma y dijeron cosas poco importantes, hablando sobre todo de ellos mismos y lo bueno que son. En la mayoría de los casos las conferencias de hackers se parecen en gran medida a una reunión de amigos.

7. Séptimo párrafo (corregido el 18-XII-07)

·Muchos profesionales del área parecen tener la impresión de que los miembros de la comunidad hacker son más listos que los propios profesionales de la seguridad de la información. Así que cuando se realiza la prueba de intrusión, por ejemplo, ninguno parece estar más cualificado que quien ataca sistemas. En cuanto este razonamiento. Por una parte, aún no he encontrado a nadie de la comunidad hacker que supiera todo sobre atacar sistemas, de hecho he encontrado algunas veces a los llamados genios del hacking que son muy buenos sólo cuando llevan a cabo un número limitado de ataques muy bien ensayados. Contratando a tales personas para llevar acabo un a prueba de intrusión, sin embargo, aseguramos que la prueba incluirá sólo los métodos conocidos por los llamados genios. Por el contrario, muchas personas de la comunidad blanca entienden las pruebas de intrusión como una ciencia. Puede ser que estos no sean la clase de persona que inventan los nuevos métodos de ataques, pero estudian como son y pudieran atacarse los sistemas y se lo plantean de una forma sistemática y minuciosa. Cuando están realizando la prueba de intrusión el cliente puede estar seguro que ha sido optimizada al máximo y con el mínimo riesgo de producir daños o problemas.

8. Octavo párrafo (corregido el 18-XII-07)

·El absoluto desdén que la comunidad de los hackers tiene por la ética me preocupa

enormemente. Por contra los individuos quienes obtienen la certificación CSSIP deben aceptar con un conjunto de principios éticos que rigen su conducta. Estos profesionales pueden y de hecho pierden su certificación por actuar de manera contraria a estos principios. Estoy más cómodo tratando con las personas que actúan en un plano ético definido.

9. Noveno párrafo (corregido el 18-XII-07)

Corren tiempos difíciles. Muchos profesionales altamente cualificados en nuestra área están actualmente en el paro, y sin embargo se han contratado miembros de la comunidad hacker en vez de a estos profesionales para desempeñar las tareas relacionadas con la seguridad, lo que es un golpe bajo a nuestros compañeros de la profesión.

10. Décimo párrafo (corregido el 18-XII-07)

·Al asociarnos con los miembros de la comunidad hacker daña nuestra reputación como profesionales de la seguridad y si los policias se reúnen con criminales solo cuando surgen necesidades profesionales, nosotros deberíamos hacer lo mismo. Para asegurar que mantenemos el nivel de respetabilidad que hemos ido ganando dentro de la profesión, necesitamos ser cautos con esos con los que nos asociamos.

11. Undécimo párrafo (corregido el 18-XII-07)

·Los llamados retos para hackers que se llevan a cabo en las “conferencias de hackers” y en otros lugares no son probablemente más que un truco publicitario. En unas cuantas pruebas el fabricante que la lleva acabo ha reducido de forma drástica la posibilidad de éxito de los atacantes poniendo por ejemplo un cortafuegos adicional entre los puntos de origen y destino del ataque

12. Duodécimo párrafo (corregido el 18-XII-07)

De otro lado, los fabricantes que organizan los retos para hackers lo que verdaderamente hacen es reforzar la falsa idea de que “los hackers lo hacen mejor”.

13. Décimo tercer párrafo (corregido el 18-XII-07)

En resumen:

·No hagamos propaganda a quienes infringen la ley.

·No legitimemos lo que hacen.

·Limitemos nuestro contacto con ellos.

·No les contratemos.

Dejemos claro que estamos en contra de ellos

Dr. E. Eugen Schultz, CISSP

Redactor Jefe