

Hacking a Contrareloj.

Autor: Hugo Vázquez Caramés para la Comisión de Seguridad de la Asociación de Internautas

Artículo extraído de <http://www.internautas.org/html/3355.html>

La seguridad informática es una especialidad de la Telemática relativamente reciente. En 1988 Robert T. Morris liberó un gusano que paralizó casi completamente Internet. La mitificación por parte de la prensa de los autores de ésta y posteriores acciones ilegales, ha llevado a que miles de jóvenes en todo el mundo se hayan lanzado a una carrera obsesiva por emular a sus "ídolos"; léase Morris, Kevin Mitnick y otros más que surgieron tras su estela. Al mismo tiempo y como toda ciencia o tecnología reciente, la Telemática también ha visto surgir expertos y especialistas de nuevo cuño. Normal, es lo que siempre sucede hasta que la divulgación, conocimiento y aplicación real se extiende por los entresijos públicos y privados de la Sociedad.

21-12-2005 - Así y paralelamente a dicha evolución, el mito del **"hacker"** también ha ido sufriendo una constante transformación. Ese término que antes era sinónimo de **"gurú"**, se ha convertido en la etiqueta que define al individuo que accede ilegalmente a ordenadores y sistemas. Individuo que no obstante, para realizar dichas acciones (modificación de páginas web, programación de virus, ac-ceso no autorizado a sistemas, etc.) necesita de un cierto conocimiento técnico. Conocimiento generalmente superior al del ciudadano medio -de ahí su aura popular- pero que sin embargo no es indicativo ni fiable, al nivel que nos interesa, para la realización exitosa de un proceso tan complejo como es el **"Test de Intrusión"**.

Otro protagonista en el tema que nos ocupa, es el experto en seguridad. Persona técnica formada en el problema a base de cursos y cuya experiencia, contrastada en **"intrusiones reales"**, se ciñe a las auditorías de seguridad efectuadas en las empresas para las que ha trabajado en plantilla. Un profesional que a pesar de su desconocimiento de la realidad que acosa a las empresas en temas de seguridad, en muchas ocasiones garantiza el éxito en un **"Test de Intrusión"**. Y aún existe otro tipo de profesional en Seguridad Telemática. Su perfil es una combinación de los dos anteriores: experiencia profesional más posesión real de **"background"** en temas de hacking.

De todos esos profesionales, algunos investigan y publican los fallos de seguridad encontrados, y otros, jamás publican nada; algunos son excelentes programadores y otros no lo son en absoluto, como también encontramos al que literalmente "adora" la tecnología con la que trabaja y de tal modo, que ocupa todo su tiempo libre con "más tecnología".

Ahora bien, y a pesar de que todos tienen "algo" en común -su conocimiento y dedicación a la seguridad- ese "algo" no puede considerarse como determinante para poder realizar un **"Test de Intrusión"** con éxito. O lo que es lo mismo, ninguno de esos profesionales garantiza que sean buenos **"Pen-Tester"**. ¿Porqué? Por múltiples y variadas razones.

Se podría afirmar que el que es capaz de atacar con éxito un sistema informático, tal vez posea una visión de conjunto más amplia que el que no lo hizo nunca. Pero ello no garantiza que sea un buen **"Pen-Tester"**. Podría compararse a jugar un partido de fútbol en la playa con una final del Campeonato del Mundo. La presión no es la misma y la exigencia de conocimientos **"reales"** tampoco.

Vulnerar sistemas por cuenta propia de manera no remunerada y por el simple reto de superarse a uno mismo tiene varias "ventajas". La más importante es que nadie se entera cuando la incursión sale mal. ¿Alguien ha escuchado quejarse a algún hacker de la cantidad de sistemas que nunca ha logrado penetrar? En segundo lugar, no hay límite de tiempo y esto es muy importante. Cualquier individuo decidido y con unos mínimos conocimientos de seguridad, puede romper gran parte de los sistemas que se conectan a Internet.

También se podría argumentar que una buena "base" académica en informática es imprescindible para poder realizar un buen **"Test de Intrusión"**. Quienes se dedican a esta actividad saben que no es así. La formación académica, como cualquier otra es muy importante, y hay que valorarla aunque no nos garantice nada. Pero ojo, tampoco caigamos en el error contrario, en el de creer que con simple experiencia real en este tipo de pruebas ya es suficiente. Tampoco es eso aunque si es muy importante destacarla y ponerla en primer lugar: en el de los requerimientos profesionales a la hora de juzgar a un **Pen-Tester**.

¿Y la capacidad técnica? A pesar de parecer pesimista, creo que tampoco es suficiente. Muchos expertos en seguridad telemática confunden la capacidad técnica con la habilidad para realizar un "Test de Intrusión". Existen infinidad de empresas y expertos en seguridad telemática -o en alguna de sus áreas- que sin embargo no destacan por su efectividad en los "Tests de Intrusión".

El "Test de Intrusión" es un arte y como todo arte, necesita de una técnica especial y de un conocimiento particular para sublimar los deseos que se pretenden: alcanzar la Verdad, el objetivo del "Test de Intrusión", es decir, llegar a la Verdad de si el sistema es invulnerable, inexpugnable.

En mi modesta opinión, la capacidad de romper la seguridad de un sistema en un tiempo determinado, requiere de una combinación de cualidades que van mas allá de la típica definición de un experto de seguridad. Cualidades que como todos sabemos, no son otras que experiencia, conocimientos, curiosidad, ambición, tesón, paciencia, criterio, sacrificio, método, improvisación, reflejos, abstracción, creatividad, astuta modestia.. Y fe. Fe en uno mismo, fe en poseer esas cualidades que solo unos pocos poseen, o sea: Fe en poder demostrar en todo momento y en cualquier situación, que se es un "Pen-Tester" solo eso, un "Pen-Tester".pero un buen Pen-Tester.

Básicamente un "Test de Intrusión" consiste en ver si se puede "romper" la seguridad de los sistemas del cliente en un tiempo determinado. Para ello es muy importante entender que el hecho NADA tiene que ver con la simple enumeración de "posibles" vulnerabilidades de los sistemas del cliente y por tanto, sin llegar a aprovecharlas. Hay que hacerlo y llegar al final. Existe un abismo entre estas dos formas de actuar o de tratar el mismo problema. Es a la segunda solución a la que con toda lógica se la suele llamar "**Auditoría de Seguridad**" ahora bien, no entremos a discutir que actuación profesional es más conveniente y aceptable pues considero que ambas lo son aunque con objetivos diferentes.

Los "Tests de Intrusión" son una especie de "**match**" informático con dos participantes -la empresa contra el "Tiger Team"- y un solo premio. Al final y por mucho que maquillemos la realidad o queramos darle un aire más "sofisticado", como en todo "match" se trata de eso, de un premio para el vencedor. El que el cliente concede cuando contrata un "Test de Intrusión" porque entre otras cosas, desea, "necesita" comprobar lo segura que es su red. Pero, ¿Es posible verificar el estado de un sistema en el breve lapso de tiempo que dura un "Test de Intrusión"? No, no es posible pero sí que se puede demostrar que NO es seguro. Sí, y de tal modo que cuando finaliza el "Test de Intrusión" siempre nos encontramos con la siguiente situación: Si el "Tiger Team" consiguió "entrar" en los sistemas del cliente, éste se mostrará preocupado por el estado de su seguridad pero satisfecho con los resultados del Test y con el servicio contratado. Pero si el "Tiger Team" no consiguió acceder a los sistemas del cliente, el cliente habrá quedado satisfecho con la seguridad de su empresa pero inconscientemente insatisfecho con la empresa contratada para hacer el test.

Teniendo en cuenta esto, es importante entender por qué no todo el mundo sirve para este trabajo. Un trabajo donde para desarrollarlo correctamente, se requiere de una constante improvisación. Donde no se permiten "peros" ni "objeciones" y mucho menos "perdedores". Y en el que es más importante el resultado que el "como" o las "florituras" llevadas a cabo. Un trabajo donde se tiene el aliento del cliente en el "cogote" y la música del "tic-tac" del reloj cual espada de Damocles. Un trabajo donde el éxito es una obligación y el fracaso un estigma para tu imagen y la de tu Empresa. Y mientras se siente todo eso, has de seguir adelante con el compromiso adquirido porque al final, y siempre es así, al cliente lo único que le importa y quiere del "mago" que le está hurgando en el sistema, es que haga magia. Pero claro, no es lo mismo la magia del hacker desde la tranquilidad de su casa, entre discos y programas favoritos y con "niña" al lado, que el hacking a contrareloj del "Pen-Tester".

Hugo Vázquez Caramés
(Director Técnico de PENTEST, Consultores de Seguridad Telemática)
<http://www.pentest.org>

Nota: "La empresa española "PENTEST" tal vez sea una de las mejores del entorno europeo en la realización de Tests de Intrusión. Empresa que basa su éxito en la recluta para cada tipo de proyecto de los mejores "Pen-Testers" existentes en la problemática a auditar. Una vez seleccionados, forma un equipo de auditores o "Tiger Team" que pone al servicio del cliente. Normalmente los "Tiger Team" de "PENTEST" no solo son los mejores, sino también los más motivados pues trabajan a partir de la propia libertad de sus conocimientos y experiencia y de la que concede Pentest para el desarrollo de su función profesional.