Honeypot y Obscurity

Catholic.net TI

Hay dos teorías o formas de defensa que son realmente casos de estudios, los cuales proponen métodos para hacer menos la forma en sistemas tecnológicos de cualquier tipo son atacados, los Honeypot y la Obscurity.

El termino honeypot o tarro de miel, es precisamente un programa, un sitio, un servidor o un conjunto de ellos que es montado y calibrado con la intención de atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los honeypots pueden distraer a los atacantes de las partes más importantes de los sistemas, y advertir rápidamente de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque.

Estos métodos son complicados de implementar cuando se cuentan con pocos recursos humanos y de infraestructura, ya que deben de ser construidos para su simulación de una manera profesional y ordenada, solo asi podrán cumplir con su objetivo. Es importante conocer a quienes nos atacan, saber como lo hacen, como lo intentan y de conseguirlo, como lo lograron, de ahí que sea una herramienta muy valiosa.

La seguridad basada en la oscuridad, no es otra cosa mas que esconder lo más posible como funciona un sistema dentro del mismo sistema, ocasionando que los que ataquen se frustren y desistan, propiamente no es un método de defensa y en ocasiones podría parecer hasta demasiado simple, pero no deja de ser un recursos, la intención es precisamente esa, hacer que sea muy difícil de hallar lo que puede ser vulnerable.

Por la forma de presentar esto este método se debería complementar con otro más, la ofuscación como paso final, esto es, tomar un programa bien escrito y desarrollar un rango de transformaciones sintácticas para hacer la ingeniería en reversa algo tan difícil que de hecho, sea desechable como opción para decodificar código. Esta nueva teoría es parte de una nueva investigación, que sugiere como la seguridad en un juego de información incompleta, buscando siempre aprender (y mucho) examinando los comportamientos de los atacantes, así como los algoritmos que usan para sus agresiones. El “oscurecer” el panorama de los que atacan, de acuerdo con esta investigación, da alguna ventaja y mejora las posibilidades de salir mejor librado. En breve: la oscuridad complementado con la ofuscación es un buen principio general, pues dificulta al atacante saber cómo atacarlo a uno.