Introducción

Justificación y objetivo

Actualmente, la información tiene una relevancia crítica en el mundo empresarial. El avance en la tecnología ha permitido que un gran número de personas tengan acceso a ésta y a los servicios de las organizaciones, tanto gubernamentales como educativas. Dicha información se genera, procesa, transforma y almacena a través de diversas infraestructuras de red y, debido a que dichas tecnologías no se encuentran exentas a los errores o a los descuidos, los activos más valiosos de las empresas se exponen de manera constante a la utilización no autorizada por terceras personas. Considerando lo anterior, es evidente la importancia que adquiere el hecho de identificar las vulnerabilidades y mitigar las fallas de seguridad existentes en los sistemas.

Una de las maneras de prevenir y disminuir los riesgos antes mencionados es la realización de pruebas de penetración o Hacking Ético, con la finalidad de intentar comprometer la red de la organización y así evaluar su seguridad previamente.

El desarrollo de este proyecto se llevó a cabo dentro de la red de un laboratorio que forma parte de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. Éste cuenta con 11 equipos, un *switch* (siguiendo la topología estrella), un *router* inalámbrico y un *servidor*, entre otros dispositivos. Sus servicios de red, que en el pasado han sufrido ataques y bloqueos, proporcionan información a los estudiantes de la carrera de Ingeniería en Computación para su formación educativa.

Es por ello que el objetivo de este proyecto de tesis es llevar a cabo las pruebas pertinentes, a través del uso de herramientas para encontrar las vulnerabilidades y evaluar la seguridad de la red del laboratorio antes mencionado pretendiendo con ello hacer las recomendaciones necesarias para mitigar o solucionar tales vulnerabilidades.

Aplicación

El campo de aplicación de este proyecto es muy amplio, ya que puede ser implementado en sistemas computacionales pertenecientes tanto a organizaciones públicas como privadas, en donde la manipulación de información crítica no sólo es frecuente, sino indispensable para el buen desarrollo de las actividades diarias.

Método

Las actividades realizadas se basan en el concepto de *pentesting*, que consiste en simular un ataque real a los sistemas que se fijan como objetivo, con la finalidad de evaluar las vulnerabilidades existentes en ellos y, finalmente, mejorar la seguridad de la información de una entidad.

Para tales fines, desarrollamos las pruebas siguiendo las siguientes fases:

- Investigación previa.
- Pruebas de penetración a la red interna.
- Análisis de resultados.
- Recomendaciones y conclusiones.

Herramientas

Para realizar una prueba de penetración es necesario contar con una serie de aplicaciones que permitan realizar ataques a dispositivos específicos además de la evaluación de los resultados. Las herramientas seleccionadas para tal fin serán enumeradas y descritas más adelante cuando se defina el plan de pruebas habiéndose seleccionado de un amplio catálogo las que pensamos, cumplirán de un mejor modo nuestras expectativas.

Perspectivas y contribuciones

Con la correcta preparación y puesta en práctica del proyecto se pretende, en primera instancia, identificar posibles fallas de seguridad que comprometan en mayor o menor medida la integridad de la servicios de red e información del laboratorio de computación de la Facultad de Ingeniería de la UNAM.

Justo es decir que además se obtendrá una valiosa experiencia en el manejo práctico de algunas de las herramientas utilizadas en el mundo de la seguridad informática aunque, si bien es cierto que no se habrán de manejar todas las herramientas disponibles, se realizó un gran esfuerzo por seleccionar de una larga lista las más usadas y populares con el fin de realizar una adecuada valoración de la seguridad.

Por otro lado, se pretende también que la información obtenida en las fases de análisis de resultados y recomendaciones, sea lo bastante trascendente como para ser tomada en cuenta por el administrador del laboratorio logrando así, contribuir a solucionar las vulnerabilidades críticas que posiblemente sean encontradas y así mitigar el impacto de un ataque.