HERRAMIENTA WEB PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE SEGURIDAD Y PRUEBAS DE PENETRACIÓN

José Bedón – Patricia Chávez
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral, ESPOL
Campus Gustavo Galindo Km 30.5 Vía Perimetral
Apartado 09-01-5863, Guayaquil, Ecuador
jbedonsanchez92@gmail.com – paxichav@espol.edu.ec

Resumen- Se implementó una herramienta, cuya función principal es de realizar pruebas de penetración en algún sistema en particular, en base a normas de seguridad informática como OSSTMM, uno de los estándares más usados; realizando el análisis de una de las capas de esta metodología para poder generar un informe detallado de las posibles vulnerabilidades del sistema analizado en ese aspecto específico. Previamente se realizó un análisis completo, de todas las herramientas externas que se necesitarían, para poder garantizar que esta herramienta sea suficientemente segura como para realizar un análisis de prueba de penetración de seguridad informática.

Abstract- A tool was implemented, whose main function is to perform penetration testing in a particular system, based on computer security standards like OSSTMM, one of the most used standards; performing analysis of the layers of this methodology to generate a detailed analysis of possible vulnerabilities discussed in that specific aspect system report. Previously a complete analysis of all the external tools that would be needed in order to ensure that this tool is safe enough for analysis penetration testing computer security was performed.

I. Introducción

Hoy en día en toda empresa grande o pequeña, algún negocio personal o mediano, o cualquier entidad que se maneje información, existe la necesidad de asegurar su información, ya sea para garantizar una buena imagen a la empresa, o debido a que se posea información valiosa. La información que se maneja constantemente puede originar que personas malintencionadas, aprovechen escenarios inseguros y procedan al robo de información. Por este motivo este trabajado está dirigido para instituciones que requieran realizar un análisis de seguridad informática en sus sistemas, de tal forma que sea accesible desde cualquier ordenador, sin necesidad de realizar instalaciones tediosas y garantizando la seguridad de la información proporcionada. Se puede generar un informe detallado del análisis requerido. Se explica los estándares para el correcto funcionamiento de la herramienta.

La herramienta está basada en el análisis que usa la metodología OSSTMM, para la detección de vulnerabilidades en las pruebas de seguridad, mediante el análisis por capas. Cada capa, consta de una serie de análisis, esta división ayuda a una mejor búsqueda del problema, siendo muy eficaz este método. Por lo que se cuantificará los diferentes niveles, es decir, se podrá obtener un grado de seguridad de lo que se esté evaluando. Debido a las limitaciones de tiempo, evalúa solo el nivel de capa de red de la metodología OSSTMM.

Con esta herramienta se busca que los usuarios, mejoren sus sistemas, y repitan el proceso las veces que sean necesarias, para poder corregir sus vulnerabilidades y así minimizar la existencia de problemas informáticos.

II. Diseño e Implementación de la Herramienta Web

Metodología OSSTMM

Esta metodología al igual que el resto son un conjunto de reglas y normas para controlar cuando, en qué momento y cómo son realizados los eventos de pruebas de penetración, sin embargo es una metodología que solo realiza un estudio desde un entorno externo, además de presentar diferentes análisis para las diferentes capas que se postulan en esta metodología como es la seguridad Física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la

información, seguridad de las tecnologías de internet y seguridad de procesos. Además un documento elaborado por la ISECOM menciona que para que una prueba de seguridad sea considerada dentro del estándar OSSTMM debe de considerarse algunos puntos como: "ser cuantificable, consistente y que se pueda repetir, válido más allá del tiempo actual, basado en méritos del consultor y analista pero no en marcas comerciales, exhaustivo, y concordante con leyes individuales y locales y derecho humano a la privacidad." [1]

Con el desarrollo de esta herramienta, lo que se logró es realizar un análisis basado en la metodología OSSTMM, sin embargo al ser cambiada en ciertos procesos para realizar pruebas de una manera más rápida, se pierde el valor como tal, pero lo que se logra es que la herramienta sea aún más intuitiva para los usuarios que requieren alguna revisión rápida de sus negocios.

La sección de Seguridad de Tecnologías de Internet comprende un gran número de módulos para realizar, con sus respectivas plantillas, y por motivo de que solo se tomará en cuenta a nivel de aplicaciones y redes, se omitirán ciertos módulos los cuales están indicados en la Tabla 3 donde se indica los procesos considerados en la herramienta.

Tabla 1 Procesos considerados en la Sección de Seguridad [2]

Módulos	Considerado
Logística y Controles	Si
Sondeo de Red	Si
Identificación de Servicios de Sistemas	Si
Búsqueda de Información Competitiva	No
Revisión de Privacidad	No
Obtención de Documentos	No
Búsqueda y Verificación de Vulnerabilidades	Si
Testeo de Aplicaciones de Internet	No
Enrutamiento	Si
Testeo de Sistemas Confiados	No
Testeo de Control de Acceso	No
Testeo de Sistema de Detección de Intrusos	No
Testeo de Medidas de Contingencia	No
Descifrado de Contraseñas	Si
Testeo de Denegación de Servicios	Si
Evaluación de Políticas de Seguridad	No

Diseño Modular

La metodología de OSSTMM como ya se ha mencionado anteriormente se encuentra dividida en sectores, y cada sector tiene una serie de procesos a elaborar, por este motivo es que la elaboración de un diseño de datos y como se va a manejar la información dentro de la herramienta, resulta ser más adecuada para implementar, es por este motivo, que se ha decidido crear módulos para la elaboración de secciones, y módulos para los procesos. La ventaja de hacer esta consideración, es que en futuros cambios sobre la metodología, estos cambios puedan ser realizados de una manera muy intuitiva, ya sea por aumentar un proceso, o aumentar alguna sección o modificarla, lo que evitará algún conflicto con el resto de procesos o plantillas establecidas. En la Figura 1 se especifica un esquema de cómo se realizarán los módulos, los cuales representan una respectiva tabla por parte de la base de datos.

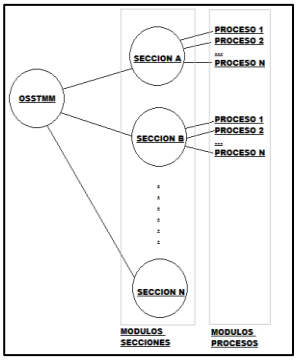

Figura 1. Esquema Modularizado de la Metodologías OSSTMM

Por lo tanto se procedió a realizar el Diagrama de Entidad Relación, por lo que se estableció la elaboración de unas tablas núcleo, que será la de psi_seccion y psi_proceso, los cuales tendrán todos las secciones y procesos respectivamente relacionados, por lo tanto cada sección y proceso se tendrá una tabla, que se relacionará con la principal. Es decir, si se requiere acoplar más procesos o secciones para completar la metodología OSSTMM, la implementación sea eficaz. Además, esta estructura nos permite tener en la herramienta un creador de perfiles, los cuales configuraremos a nuestras necesidades, es decir

dar la posibilidad al usuario de elegir que análisis puede realizar, y generar reportes solo de los configurado.

La arquitectura de la Herramienta Web, está basada en el modelo que ofrece Symfony que ayuda al desarrollo de las aplicaciones que estas esté debidamente ordenadas y seccionadas, por lo que se aprovecha esta ventaja para separar las distintas metodologías a implementar en la herramienta en paquetes distintos, así como de tener un paquete principal para el control de la herramienta en general, así como se muestra en la Figura 2

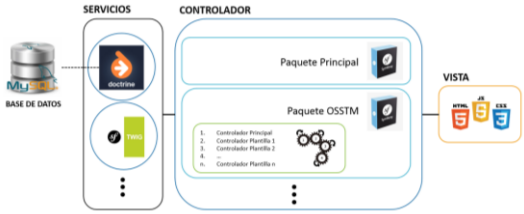

Figura 2. Arquitectura de la Herramienta Web P.S.I.

Consideraciones Operacionales

Hay dos entornos de trabajo que hay que considerar al momento de elaborar la herramienta web, estos entornos son el de producción y el de desarrollo. Por este motivo hay que tener una serie de precauciones antes de poner en funcionamiento la herramienta como son las versiones tanto del sistema operativo, como la del framework y las versiones de PHP y apache. El proyecto de la herramienta está desarrollado en el framework de Symfony, sin embargo existe 2 versiones del mismo, la versión 1.x es la antigua, y usa una jerarquía distinta en la distribución de carpetas y funcionamiento del mismo, por lo que lo esencial es que sea sobre la versión 2.x ya que bajo esas normas se realizó la herramienta web, además hay que considerar la versión de WAMP, en caso de estar en entorno de desarrollo, ya que es un conjunto de servicios como apache y php, dependiendo de la versión de WAMP, dependerá las versiones de PHP y Apache, por lo que se recomienda revisar la documentación respectiva [3].

La herramienta web está diseñada usando MySQL como gestor de base de datos, el mismo que viene integrado en WAMP, sin embargo para poder realizar modificaciones en el mismo es necesario, importar todas las tablas que se estén usando en el proyecto. Aunque los comandos de Symfony nos permiten crear automáticamente las tablas en la base de datos, esto genera el problema de que las configuraciones iniciales como la de los módulos de secciones y procesos no se encuentren disponibles. Además se debe realizar las configuraciones necesarias como la conexión a la base de datos que se vaya a usar, Symfony trae un servicio de manejo de base de datos el cual es Doctrine ORM, este paquete maneja ciertas bases de datos relacionales como MySQL, PostgreSQL, Microsoft SQL, además de otro paquete que es Doctrine ODM, que maneja base de datos no relacionadas como MongoDB, por lo que se debe de indicar las configuraciones que base de datos se usará; además de proveer las credenciales respectivas para la conexión.

Puesta en Marcha

Considerando los estudios realizados, para la elaboración de la herramienta de pruebas de seguridad informática, se decidió realizarla en lenguaje de programación PHP, usando el framework Symfony, además de usar MySQL como gestor de la base de datos. Para poder realizar el desarrollo de esta aplicación, se la realizo sobre un equipo con sistema operativo Windows 8, con procesador Intel® Core™ i7-4702MQ CPU @ 2.20 GHz, con memoria RAM de 8Gb, y para el entorno de desarrollo en un entorno de infraestructura de internet WAMP Server 2.4, que usa las herramientas de Apache 2.2.4, PHP 5.4.12 y MySQL 5.6.12, El framework de Symfony 2.6. Todos estos elementos son con los que se realizó el entorno de desarrollo. Sin embargo puede haber variantes sobre las versiones que se usen al momento de poner la aplicación en producción, ya que en un servidor web, se puede realizar instalaciones de cada servicio de manera independiente sin usar WAMP, por este motivo se especifica los requerimientos mínimos para que la herramienta web pueda ser puesta en producción, para obtener estos datos se procedió a revisar los requerimientos mínimos para desarrollar en Symfony, es decir según el sitio oficial de Symfony requiere como mínimo PHP 5.3.3. [4]

III. Comparativa de Resultados

Para los resultados obtenidos se recopiló información en base a los criterios y escenarios anteriormente mencionado es decir, con dos escenarios, uno el dominio de prueba scanme.nmap.org y pequeña red de laboratorios. Por este motivo se procedió a realizar el estudio

de los tres primeros pasos en un hacking ético los cuales son: reconocimiento, escaneo y enumeración.

En base a los resultados obtenidos se procedió a usar las herramientas para poder documentar los resultados obtenidos, en la Tabla 2 se muestran las diferentes características tomadas en cuenta para la evaluación de las herramientas, donde las características que se deben recalcar es que la herramienta P.S.I. no cuenta con utilidades de terceros integradas, es decir que vienen incorporados en la aplicación, sin embargo es necesario tomar en consideración que la herramienta P.S.I. maneja la generación de reportes basados en plantillas de la metodologías OSSTMM, por lo que resulta una gran ventaja para la documentación final de las auditorías.

Tabla 2 Comparativa de las Diferentes Herramientas Usadas

Características	P.S.I.	MagicTree	Dradis
Plataforma	Multiplataforma: PHP	Multiplataforma: Java	Multiplataforma: Ruby
Código Abierto	Si	No	Si
Arquitectura	Aplicación Web	Aplicación de Escritorio	Aplicación Web
Nmap	No	Si	Si
OpenVas	No	Si	Si
Agregar documentos	Si	Si	Si
Buscar información en los documentos	Si	si	Si
Manejo de Metodologías	Si	No	No
Reportes usando la Metodología OSSTMM	Si	No	No

IV. Conclusiones

Los reportes en una consultoría para evaluar la seguridad de la información en una empresa son esenciales, ya que es el resultado del trabajo realizado en documentos, por lo que al hacer uso de herramientas que nos faciliten estas tareas, como de generar reportes en base a una metodología como la OSSTMM, resulta muy ventajoso ya que nos reduce el tiempo para la etapa de la entrega del informe en una auditoría.

El diseño en módulos de cualquier herramienta o aplicación es muy importante ya que nos permite entender de una mejor forma la arquitectura de cómo está diseñada, por lo que al hacer uso de esto, se pudo proponer un proyecto en el cual pueda ser entendible para el desarrollador y con un reducido problemas de conflicto en los diferentes módulos.
Para poder modificar la metodología que se usa, es adecuado que se agregue un nuevo espacio de trabajo sobre el proyecto desarrollado en Symfony pues así se evita, tener inconsistencias en cuanto a la funcionalidad y arquitectura que está siguiendo la herramientas PSI.

V. Recomendaciones

A pesar de que la herramienta de PSI no cuenta con utilitarios para la búsqueda de vulnerabilidades como Magic Tree y Dradis, sería adecuado trabajar con módulos para estas utilidades, y así poder implementarlas, sin embargo el agregar utilitarios se ve la necesidad de cambiar el entorno de trabajo donde se lo realiza actualmente ya que necesitaría utilitarios propios de distribuciones como Kali.

La herramienta web PSI, es adecuada para usuarios que son inexpertos en el asunto de seguridad informática, ya que le facilita crear perfiles sobre l metodología OSSTMM y así realizar pequeñas evaluaciones o las que crea convenientes.

VI. Referencias

[1] L. Fridman, Una comparación del rendimiento de los frameworks de Ruby: Sinatra, Padrino, Goliat y Ruby on Rails, http://altoros.com.ar/blog/una-comparacion-del-rendimiento-de-los-frameworks-de-ruby-sinatra-padrino-goliat-y-ruby-on-rails/, fecha de consulta 08 Febrero 2015.

[2] ISECOM, OSSTMM 2.1, 23 Agosto 2003. http://isecom.securenetltd.com/osstmm.en.2.1.pdf, fecha de consulta 20 Abril 2015.

[3] WAMPSERVER, WampServer, http://www.wampserver.com/en/, fecha de consulta 29 Abril 2015.

[4] SensioLabs, Symfony, http://symfony.com/doc/current/reference/requirements.html, fecha de consulta 20 Abril 2015].