Práctica 3: Seguridad en entornos Web

En anteriores prácticas hemos visto cuáles son algunos de los protocolos para asegurar las comunicaciones en redes. Sin embargo, además de la comunicación, es necesario que los extremos de la misma sean seguros. Por ejemplo, no sirve de nada una conexión DTLS entre un cliente y un servidor si éste está comprometido. En este entorno, la labor de los administradores de seguridad es cada vez más necesaria y compleja. En esta práctica se propone dar a conocer al alumno algunas de las vulnerabilidades presentes en servidores web, y cómo deben enfrentarse a ellas para solucionarlas pero sin perder la funcionalidad.

Un análisis de seguridad debe analizar todas las capas del servicio ofrecido, puesto que si una es comprometida, todas ellas lo serán. En el caso de la práctica será necesario atender a los siguientes aspectos para analizar la seguridad del servicio ofrecido.

- Configuración del servidor Web : módulos, políticas, etc.
- Configuración de la base de datos : accesibilidad, etc.
- Configuración del Sistema Operativo : firewall, usuarios, permisos, etc.

El Wiki alojado en el servidor web a analizar incluye una introducción a los principales aspectos de seguridad a analizar durante la práctica.

Objetivo

El objetivo de la práctica consiste en analizar la seguridad de un servidor web (dado en forma de máquina virtual) y tomar las medidas apropiadas para la securización del mismo.

Para la realización de la práctica se han instalado en el laboratorio (aula 1.0.A01) 3 máquinas virtuales por equipo, llamadas alfa, beta y auditora. Las máquinas alfa y beta contienen un servidor web, sobre las que se realizarán los análisis de seguridad. La máquina auditora servirá de ayuda en la realización de estos análisis. Todas las máquinas virtuales instaladas en los equipos del aula se encuentran en la misma red virtual (192.168.1.X), y por lo tanto son visibles entre ellas (aunque no con la máquina Host). Cada grupo de prácticas deberá buscar otro grupo con el que realizarán una parte de la práctica. A cada uno de los grupos se le asignará una máquina distinta (alfa o beta), con la que se trabajará durante todo el desarrollo de la práctica. Es fundamental mantener el mismo equipo durante la realización de la práctica en las distintas sesiones. De esta manera los cambios hechos en las máquinas se guardarán de una sesión a otra.

Servicios ofrecidos

Como se ha comentado, uno de los retos principales que se le presenta a un administrador de seguridad es la de proporcionar seguridad a los servidores sin perder la funcionalidad de los servicios que éstos ofrecen. A continuación se explican cuáles son los servicios que deberán proporcionar las máquinas alfa o beta, según corresponda:

1. Servicios web. Se dispone de un “Apache2”, Versión Apache/2.2.4 (Ubuntu). Es un servidor web con una configuración vulnerable a diversos ataques. El servidor dispone de 3 aplicaciones:
   - ”Mediawiki”: versión 1.9.3. Aplicación php que gestiona y visualiza contenidos web con formato wiki. Se trata de una wiki de seguridad que ofrece cierta información que puede ser usada para la realización de la práctica, y que podrá ser modificada si se desea. Esta modificación sólo podrá ser realizada por el administrador de la wiki, para lo cuál se dispone de un usario, admin, con la clave admin. La wiki está alojada en el directorio /var/www/mediakili-1.9.3, y se puede acceder a ella a través del navegador bien escribiendo la ip del equipo (local o remoto) o bien escribiendo localhost (local)

- Una aplicación cuya funcionalidad es añadir y buscar artículos en la base de datos del portal. Se accede mediante la url : http://localhost(o ip)/mediawiki-1.9.3/insertar/. Consta de tres ficheros php: index.php, buscar.php e insert.php. Esta aplicación se encuentra en el directorio /var/www/mediawiki-1.9.3/insertar.
- "PhpMyAdmin": versión 2.11.5.1. Se trata de un gestor de bases de datos MySql a través de un portal web. La url de acceso es http://localhost(o ip)/phpmyadmin. Esta aplicación permite de una forma gráfica administrar la base de datos y realizar consultas, inserciones, borrados, etc de los registros que en ella se encuentra. Para motivar la securización de esta aplicación, existe en el sistema una base de datos ficticia que almacena datos de cuentas y clientes de un banco inexistente.

2. Login por ssh pero solo con permiso para administrar la web.
3. Administración de la máquina (usuario root) solo a través de la máquina local

Actividades a Realizar

La realización de la práctica se ha dividido en actividades que deben ser realizadas en orden. La descripción de cada actividad viene dada a continuación.

Actividad 1

Analizar el estado actual del firewall iptables de la máquina y configurarlo para que acepte conexiones únicamente en los servicios que deben estar activos. La configuración actual del firewall se encuentra en el fichero:

`/etc/init.d/firewall.sh`

Para esta actividad será necesario consultar manuales en Internet desde la máquina host (las virtuales no tienen salida a Internet) puesto que no será posible acceder a la documentación de la wiki hasta que no se cambie la configuración del firewall.

Actividad 2

Realizar un análisis de seguridad de la máquina (alfa o beta) sin acceder localmente a la misma. Para ello se recomienda utilizar la máquina auditora, ala Memoriaunque no hay restricciones en cuanto al software o mecanismos de análisis a utilizar. En cualquier caso, la memoria deberá incluir una descripción de los análisis realizados. La máquina auditora dispone de un Nessus, que es un programa de escaneo para detección de vulnerabilidades con un entorno gráfico sencillo. Se puede encontrar información acerca de Nessus en http://www.nessus.org.

Actividad 3

Acceder a la máquina analizada y arreglar los fallos de seguridad encontrados en la actividad anterior. El acceso de forma local a la máquina puede mostrar problemas de seguridad no detectados en la actividad anterior. Por ello, también será necesario analizar la máquina localmente y solucionar todos los problemas encontrados en este segundo análisis. En la sección 2 de la wiki de las máquinas se puede encontrar información útil para esta actividad.

Actividad 4

Realizar un análisis de seguridad sobre la máquina de la pareja. Cada pareja deberá analizar una máquina del tipo contrario a la analizada por ellos en un primer lugar. Los fallos encontrados por los compañeros deberán ser corregidos y documentados. Esta actividad servirá a los alumnos como ensayo para la prueba final en la cuál la securización de las máquinas serán verificadas por los profesores. Es por ello que se recomienda a los alumnos la asistencia a clase el día que se realice esta actividad, fecha que se comunicará por email al menos con una semana de antelación.

Contenido del informe

Por cada una de las actividades realizadas durante la práctica se incluirá en la memoria lo siguiente:

- Vulnerabilidades de seguridad o problemas encontrados durante el análisis realizado en la actividad.
- Importancia de las mismas y por qué son un riesgo para la seguridad o para la disponibilidad del servidor.
- Breve descripción de posibles procedimientos para la explotación de las vulnerabilidades encontradas.
- Explicación de las acciones llevadas a cabo para solucionar el problema y justificación de las mismas.

URL Máquinas Virtuales (VMWare)

- http://www.seg.inf.uc3m.es/ocw/ssd/alfa.tar.gz
- http://www.seg.inf.uc3m.es/ocw/ssd/beta.tar.gz
- http://www.seg.inf.uc3m.es/ocw/ssd/auditora.tar.gz