Auditoría, Evaluación, Test de seguridad → metodología abierta ¿OSSTMM....?

(Por: Alejandro Corletti Estrada)
Universidad Politécnica de Madrid
acorletti@hotmail.com

Madrid, noviembre de 2005.

ABSTRACT

La problemática actual de seguridad en la masa de las empresas tiene un trasfondo oculto que debe ser encarado por sus responsables, si se tuviera que resumir en pocas líneas se podría presentar como sigue:

- Creciente nivel de vulnerabilidades y mayor grado de exposición de recursos.
- Imposibilidad de contar con personal especializado y actualizado.
- Dificultad para cuantificar su nivel de riesgo.

Al solicitar apoyo de consultoría a empresas especializadas, es casi una norma general que le indiquen que el primer paso a seguir es la realización de una "auditoría de seguridad".....

A lo largo de este texto se tratará de establecer una relación entre:

- Lo que el cliente verdaderamente necesita.
- Cómo se puede clasificar lo que habitualmente se engloba bajo "Auditorías de seguridad".
- Si es posible respetar algún método que permita repetir esta tarea y obtener índices de evolución.

La propuesta final, es el ejemplo que propone esta metodología abierta denominada OSSTMM (Open-Source Security Methodology Manual), la cual no se desea remarcar como mejor o peor que cualquier otra, sino simplemente como una guía gratuita a tomar como referencia ante la necesidad que suele tener todo responsable de sistemas al pedir este tipo de asesoramientos y/o contratarlos.

Palabras clave: Auditoría y evaluación de seguridad, penetration test, OSSTMM.

DESARROLLO

I. Lo que el cliente verdaderamente necesita.

La hipótesis que se presenta trata de reflejar una problemática de seguridad que se encuentra en exponencial crecimiento y con una vorágine tal que no permite a los responsables de sistemas de las "pymes", mantener personal al tanto de lo que sucede día a día. Es más, este hecho se podría considerar casi como asumido por esta línea de empresas, es decir, los gerentes de sistemas ya son plenamente conscientes que un alto nivel de capacitación en seguridad es una cuestión cara y cuya relación coste/beneficio, tiene un cierto límite marcado por el conocimiento básico de seguridad de sus administradores y un claro umbral, superado el cual (por situaciones puntuales o por periodicidad), se debe solicitar el apoyo externo.

Este apoyo externo, cada vez más frecuente (por la simple relación coste/beneficio planteada), se podría englobar en dos grandes causas:

- Problemas puntuales de seguridad: Cuando ocurren hechos que superan el conocimiento básico de sus administradores.
- Periódicos: Cuando se ha llegado a una situación que hace necesaria una cierta evaluación de alguna plataforma, un nuevo servicio o una "Cuantificación del nivel de riesgo"

Al solicitar este apoyo de consultoría a empresas especializadas, es casi una norma general que le indiquen que el primer paso a seguir es la realización de una auditoría de seguridad. Este consejo puede considerarse válido, pues es muy difícil poder evaluar o tomar cualquier acción con escaso conocimiento de la infraestructura que se posee, pero aquí es donde hay que detenerse seriamente para plantear lo que el cliente verdaderamente necesita y cómo llevarlo a cabo.

El cliente necesita:

- Soluciones.
- Garantías.
- Índices (o parámetros).

.....y en ese orden.....

¡¡¡ Y NADA MÁS !!!, pues partimos de la hipótesis que no es un especialista en seguridad, y para eso confía en la empresa consultora.

- **Soluciones:** El cliente es consciente que tiene un problema, es muy frecuente que no tenga claro de qué se trata o de dónde proviene, pero está seguro que lo tiene. Independientemente de todo el trabajo de análisis, detección y evaluación que se realice, el resultado final del mismo debe proporcionar descripciones muy claras de cómo solucionarlo, pues caso contrario, no tendría sentido la totalidad del trabajo. Este punto es de vital interés, pues es difícil para el experto, bajar al nivel de alguien que no tiene por qué tener idea de seguridad y explicarle con todas las letras los pasos que debe seguir para solucionar el mismo.

- **Garantías:** Todo el trabajo que se realice debe culminar ofreciendo dos tipos de garantías:

  - Que se ha detectado la masa de los problemas de seguridad: Este aspecto no es trivial, pues acorde al tipo de trabajo que se realice y al tiempo dedicado, se podrá profundizar más o menos. Lo que no se puede dudar, es que durante el proceso de contratación, hay que hablar claro y dejar constancia de hasta dónde llegará el trabajo a realizar, pues no se puede aducir al finalizar esta actividad que determinadas actividades no se han realizado, o peor aún, dejar dudas sobre el nivel de seguridad de su infraestructura, pues esa parte no se había contratado, etc...

  - Que al aplicar las soluciones recomendadas, el nivel de riesgo se reduce a los índices deseados, o mejor aún, que lo que se propone es "la mejor solución" a sus problemas, pues es lo que recomiendan los especialistas del tema.

  En definitiva, con garantías se quiere expresar que luego de la actividad que se realice, el cliente puede encarar las soluciones recomendadas, confiado en que es su mejor opción y que al aplicar las mismas, su nivel de riesgo ha mejorado sensiblemente.

  NOTA: Una excusa "Omnipresente" y bastante desagradable para evadir garantías (aunque lamentablemente no deja de ser cierta), es que surgen nuevas vulnerabilidades día a día, por lo tanto una vez finalizada toda actividad, "No se puede garantizar la seguridad absoluta aplicando las soluciones propuestas", pues mañana habrá algo nuevo que afecte a la infraestructura.....Que pena.....(Confianza, seriedad, sinceridad.....etc, etc, etc)

- **Índices (o parámetros):** Desde mi enfoque personal, creo que uno de los problemas más grandes que tiene un gerente de sistemas es "Cuantificar la seguridad", pues como todos pueden apreciar es un "bien intangible". SE DEBE HACER TODO ESFUERZO POSIBLE PARA PONERLE NÚMEROS a la misma. Ya hay varias estrategias a seguir al respecto y en Internet se puede encontrar mucho de esto (ESPACIO PARA PUBLICIDAD: Recomiendo que miren un método que he propuesto hace tiempo que lo denominé "Matriz de Estado de Seguridad", está publicado en varias web. Su objetivo es aplicar todos los indicadores objetivos posibles, dejando de lado la subjetividad). El no contar con índices o parámetros, ocasiona dos grandes perjuicios:

  - Desconocimiento del grado de seguridad y de la evolución del mismo, no pudiendo plantear objetivos o umbrales a cumplir (¡¡muy negativo!!).

  - Imposibilidad de demostrar el ROI en temas de seguridad ante la dirección de la empresa (¡¡¡Catastrófico!!!).

  Un trabajo de auditoría externa es la mejor oportunidad para cuantificar el nivel de seguridad, pues todo especialista en el tema posee la "expertiz" necesaria para jugar con ellos, promediando valores. Los parámetros más importantes a considerar son:

  - **Criticidad:** Este parámetro refleja el daño que puede causar a ese sistema la explotación de esa vulnerabilidad por quien no debe.

  - **Impacto:** Independientemente de la criticidad de una vulnerabilidad encontrada, esta puede causar daño a sistemas que son el sustento de la empresa, que mantienen datos de alta

clasificación (LOPD), o una fuerte pérdida de imagen de empresa, etc. O por el contrario, puede ser Crítica para ese servicio, pero el mismo no cobra mayor interés para el buen funcionamiento de la empresa.

- **Visibilidad:** Este indicador puede servir como multiplicador de los anteriores, pues no posee el mismo riesgo un servidor de Internet "Front End", que uno interno de la empresa con accesos restringidos.

- **Popularidad:** Este parámetro, si bien puede ser muy discutido, permite indicar el grado de "visitas, conexiones o sesiones" que posee un sistema. El empleo o no de este indicador permite considerar, que si existiere una vulnerabilidad sobre el mismo, se puede suponer que tiene mayo grado de "exposición" que el resto. Se admite aquí que puede ser valorado o no.

- **Magnitud:** Cuántos sistemas afecta. Este parámetro es muy interesante tenerlo en cuenta por niveles, es decir una misma plataforma puede estar conformada por varios sistemas, pero también existen sistemas que forman parte de varias plataformas, que permiten el paso hacia ellas, que autentican, que filtran, que monitorizan, etc. Es decir, hay plataformas cuya magnitud "Directa" es muy clara y dependen únicamente de ellas, pero hay otras que para su funcionamiento necesitan la participación de otros elementos. En concreto, una cadena se corta por el eslabón más débil, por lo tanto, si no se considera la magnitud de una infraestructura, y se solucionan o evalúan únicamente los aspectos puntuales de cada host, el resultado no es el óptimo.

- **Facilidad de explotación:** Una determinada vulnerabilidad, puede presentar desde la ejecución de una simple herramienta pública en Internet y desde allí mismo, hasta una elaborada técnica de intrusión, que conlleva amplios conocimientos y pasos por parte del ejecutante. En este valor entra también en juego el grado de visibilidad del sistema, el grado de segmentación interna, la autenticación, el control de accesos, etc.

- **Facilidad o coste de solución:** Este valor es muy subjetivo y debe ser evaluado con mucho cuidado pues es el punto de partida para planificar las soluciones. Se presentan aquí muchas combinaciones y a mi juicio es el parámetro que determina la "Expertiz" de una auditor, pues si realmente sabe, será capaz de interpretar con mayor claridad la problemática del cliente y proponerle un plan de acción "realista y eficiente" para los recursos del cliente. Se debe tener en cuenta aquí no solo la simple recomendación, sino como cada una de ellas puede o no ser aplicada (pues habrá aplicaciones o servicios que no lo permitan), puede involucrar a muchos dispositivos más, puede ocasionar actualizaciones de hardware y software, rediseños, caídas de sistemas, etc....

- **Tiempo de solución:** Es un parámetro muy relacionado con el anterior, y nuevamente dependerá de la "Expertiz" del auditor y de sus ganas de involucrarse con el cliente para tener en cuenta todos sus sistemas. Una de las mayores satisfacciones para el auditor (lo digo por experiencia propia) es poder entregarle al cliente un cronograma de cómo emprender las soluciones, con todo el nivel de detalle posible (Gant, hitos, valores a alcanzar mes a mes, recursos, prioridades, objetivos, etc), si se llega a esto es porque el auditor, se ha involucrado en tal medida con la empresa, que conoce hasta el último detalle a considerar para poder estimar este "Project". Esto para el cliente es lo máximo que puede desear, pues le permite organizar su

plan de acción, presentarlo a la dirección de la empresa y acorde a los recursos que obtenga, definirá su estrategia al corto/medio plazo, para cumplir las acciones aceptadas. Se debe considerar también que es la mejor forma que posee la dirección de realizar el seguimiento del dinero que invirtió, pues los hitos serán todo lo claros que hagan falta. Este aspecto sin lugar a dudas, si se hacen bien las cosas, incrementará la confianza y los fondos que la gerencia informática tendrá para el próximo ejercicio.

Por último, relacionado a las métricas de seguridad, es muy interesante la lectura del modelo que propone NIST a través del documento *"Security Metrics Guide for Information Technology Systems"*, el mismo desarrolla una métrica de seguridad basada en el alcance de objetivos y metas, lo que se plasma en resultados, de forma muy precisa. El mismo puede ser descargado en: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

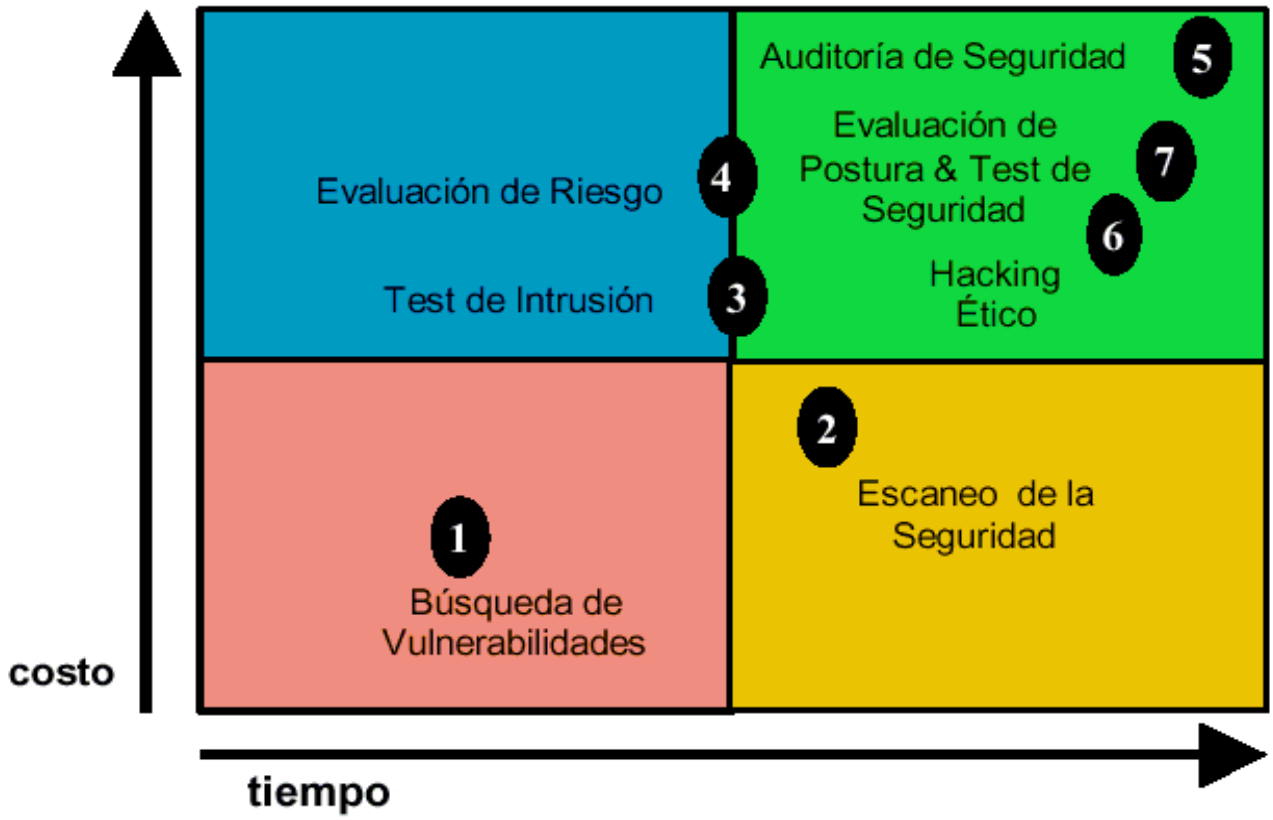
II. Cómo se puede clasificar lo que habitualmente se engloba bajo "Auditorías de seguridad".

Para tratar de diferenciar bien las opciones que se puede tener en cuenta a la hora de solicitar este tipo de actividades, se deben considerar al menos tres grandes grupos:

- Penetration Test: Se trata de una actividad con objetivo específico y acotado empleando técnicas de hacking y en general aplicando metodologías de "Caja Negra" (Sin ningún tipo de información, mas allá de la que puede contar cualquier individuo ajeno a la empresa)
  Según la definición de OSSTMM: *Test de seguridad con un objetivo definido que finaliza cuando el objetivo es alcanzado o el tiempo ha terminado.*
- Diagnóstico o evaluación de Seguridad: Comprende una actividad más amplia, en general tanto desde fuera como desde dentro de la empresa, siempre relacionado a actividades eminentemente técnicas, y puede realizar por medio de "Caja Negra o Blanca" (con total conocimiento de la información de la empresa)
  Según la definición de OSSTMM: *Una visión general de la presencia de seguridad para una estimación de tiempo y horas hombre.*

- Auditoría de seguridad: Comprende a lo anterior y también una visión más amplia en cuanto a planes y políticas de seguridad, revisión de normativas, aplicación de LOPD, procedimientos, planos, inventarios, audiencias, etc. Es decir involucra la visión más amplia a considerar, sin dejar ningún aspecto librado al azar.
  Según la definición de OSSTMM: *Inspección manual con privilegios de acceso del sistema operativo y de los programas de aplicación de un sistema. En los Estados Unidos y Canadá, "Auditor" representa un vocablo y una profesión oficiales, solamente utilizado por profesionales autorizados. Sin embargo, en otros países, una "auditoría de seguridad" es un término de uso corriente que hace referencia a Test de Intrusión o test de seguridad.*

Para completar un poco el enfoque que ISECOM (Institute for Security and Open Methodologies), entidad responsable del proyecto OSSTMM, ofrece sobre estas clasificaciones se presenta a continuación una gráfica que simboliza con mayor detalle las actividades que pueden ser llevadas a cabo (La misma se presenta textualmente figura en sus manuales):
ISECOM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet:



1. **Búsqueda de Vulnerabilidades:** se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

2. **Escaneo de la Seguridad:** se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.

3. **Test de Intrusión:** se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.

4. **Evaluación de Riesgo:** se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. **Auditoría de Seguridad:** hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

6. **Hacking Étic**o: se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

7. **Test de Seguridad y su equivalente militar, Evaluación de Postur**a, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

III. ¿Es posible respetar algún método que permita repetir esta tarea y obtener índices de evolución?

En este punto es donde se plantea a título de guía lo que propone OSSTMM. Se reitera, no porque sea mejor o peor que cualquier otra que pueda emplear una empresa consultora, sino simplemente por ser una referencia gratuita y sobre todo porque tiene su punto de partida en respetar la mayoría de los estándares, tal cual lo expresa en sus primeras páginas, estando en plena conformidad con los mismos (ISO-17799 o BS-7799, GAO y FISCAM, NIST,CVE de Mitre, etc.).

Resumidamente, esta metodología propone un proceso de evaluación de una serie de áreas que reflejan los niveles de seguridad que posee la infraestructura a auditar, a estos los denominará “Dimensiones de seguridad”, y consisten en el análisis de lo siguiente:

- Visibilidad.
- Acceso.
- Confianza.
- Autenticación.
- No repudio.
- Confidencialidad.
- Privacidad.
- Autorización.
- Integridad.
- Seguridad.
- Alarma.

Para un trabajo metódico y secuencial, describe seis secciones que abarcan el conjunto de los elementos que componen todo sistema actual, ellas son:

1 Seguridad de la Información

2 Seguridad de los Procesos

3 Seguridad en las tecnologías de Internet

4 Seguridad en las Comunicaciones

5 Seguridad Inalámbrica

6 Seguridad Física

En cada sección se especifican una serie de módulos a ser evaluados, teniendo en cuenta si aplica o no cada uno de ellos a la infraestructura en cuestión, el resultado de la observación de todos ellos es lo que permitirá "pintar" el mapa de seguridad.

Otro aspecto que trata con bastante detalle es la **Evaluación de riesgo**, teniendo en cuenta que dentro de cada módulo se encuentran los valores adecuados (RAVs) para obtener las métricas finales, lo cual como se recalcó en este texto es uno de los principios que debe tener en cuenta todo auditor si es consciente de las necesidades del cliente.

Al final de este manual, se ofrece el formato de todas las plantillas que pueden ser necesarias durante la auditoría, muchas de las cuales pueden no ser cumplimentadas en virtud de que no apliquen al sistema en cuestión, pero lo verdaderamente importante es que las que SI apliquen, proporcionan un verdadero estándar abierto, para que cuando sea necesario repetir cualquier aspecto de este trabajo se posea una Referencia clara, para que cualquier otra persona pueda evaluar y tomar como punto de partida de un nuevo análisis, el cual si respeta estos formatos será un claro índice de evolución en ese aspecto. Este tipo de acciones y sobre todo cuando son abiertas, es una de las cosas que más valoro en todo sistema informático, pues le dejan total libertad de acción a su verdadero dueño (el cliente), para tomar la decisión que más le guste a futuro, sin ningún tipo de compromiso u obligatoriedad de caer nuevamente en manos de la empresa anterior, la cual si fue de su agrado podrá hacerlo y sino no. (Bendito software libre!!!!).

Por último presenta la Licencia de Metodología Abierta (OML), cuyas líneas introductorias deseo expresarlas textualmente:

PREÁMBULO

"Una metodología es una herramienta que detalla QUIÉN, QUÉ, CUÁL Y CUÁNDO. Una metodología es capital intelectual y está a menudo enérgicamente protegido por instituciones comerciales. Las metodologías abiertas son actividades comunitarias que transforman todas las ideas en un solo documento de propiedad intelectual que está disponible sin cargo para cualquier individuo.

Con respecto a la GNU General Public License (GPL), esta licencia es similar con la excepción del derecho de los desarrolladores de software a incluir las metodologías abiertas que están bajo esta licencia en los programas comerciales. Esto hace que esta licencia sea incompatible con la licencia GLP.

La principal preocupación de los desarrolladores de metodologías abiertas que esta licencia tiene en cuenta, es que ellos recibirán el debido reconocimiento por su contribución y desarrollo, así como también el reservarse el derecho de permitir las publicaciones y distribuciones gratuitas cuando las metodologías abiertas no sean utilizadas en material comercial impreso del cual las ganancias se deriven ya sea de su publicación o distribución.

Como se pudo apreciar, esta última parte del trabajo no trata de ser un desarrollo de la metodología OSSTMM ni mucho menos, por eso justamente es que no la compara tampoco con otras, simplemente trata de remarcar que es posible aplicar técnicas o metodologías estándar, que permitan con total transparencia, mostrar resultados y dejar libertad de acción al cliente. Y este aspecto, remarco una vez más, se debe tener en cuenta como uno de los más importantes en TI para los tiempos que se avienen, pues ya no existe ninguna excusa sincera u honesta que de pie a dejar aferrado en algo a nadie cuando se trate de seguridad informática. La mejor y más sana solución que se debe ofrecer hoy en día a todo cliente, es justamente proporcionar un servicio y aferrar al mismo por el nivel de excelencia y no por otros nebulosos métodos, dejándole con absoluta sinceridad todas las herramientas que necesite para que pueda optar por quien lo desee, pero en virtud de la calidad con que se han hecho las cosas y el grado de satisfacción, no le quepan dudas si tiene que volver a levantar el teléfono pidiendo apoyo.

Independientemente de este nivel de excelencia, este tipo de metodologías estándar, lo que permiten es repetir la experiencia con la magnitud y la cantidad de veces que se desee, pudiendo en cada una de ellas evaluar el desvío que el sistema esta sufriendo, de forma totalmente numérica y objetiva.