Técnicas de Auditoria: OSSTMM, ISSAF, OWASP

OSSTMM

OSSTMM (Manual de código abierto para la realización de pruebas de seguridad) establece un "estándar" para realizar auditorias de seguridad.

Se compone de los siguientes 15 Capítulos:

Capítulo 1: Que necesitas saber
Capítulo 2: Que necesitas hacer
Capítulo 3: Análisis de seguridad
Capítulo 4: Métricas operativas de seguridad
Capítulo 5: Análisis de confiabilidad
Capítulo 6: Flujo de trabajo
Capítulo 7: Pruebas de seguridad sobre personas
Capítulo 8: Pruebas de seguridad sobre entornos físicos
Capítulo 9: Pruebas de seguridad Wireless
Capítulo 10: Pruebas de seguridad sobre telecomunicaciones
Capítulo 11: Pruebas de seguridad para datos en red
Capítulo 12: Compliance o cumplimiento normativo
Capítulo 13: Creación de reportes con STAR (Security Test Auditing Report)
Capítulo 14: Qué obtienes
Capítulo 15: Descripción de la licencia.

Como podemos observar en la lista, detalla cada parte del "manual" explicándonos así los pasos que deberíamos seguir, con solo observar la lista podemos comprobar que esta metodología es muy completa. Desde mi punto de vista tiene apartados realmente necesarios y útiles como son los capítulos 7, 8, 9,11.

Uno de los puntos fuertes de OSSTMM es que a diferencia de otras metodologías es aplicable a todos los sectores, es decir no esta dirigido a por ejemplo: una aplicación Web o una base de datos, OSSTMM trabaja en casi todos los ámbitos de la seguridad, desde las pruebas de seguridad sobre personas hasta el cumplimiento de las normativas de protección de datos (así lo veo yo, por ejemplo el cumplimiento de la LOPD)

ISSAF

ISSAF (Information Systems Security Assessment Framework), es un estándar de calidad usado para cumplir con los requisitos de evaluación de las organizaciones. El Marco de Evaluación de Sistemas de Información de Seguridad (ISSAF) trata de integrar las siguientes herramientas de gestión y las listas de control interno, está compuesto por las siguientes fases:

Fase I - Planeación

Fase II - Evaluación

Fase III - Tratamiento

Fase IV - Acreditación

Fase V – Mantenimiento

El ISSAF utiliza fases como recopilación de información. Explotación, escalada de privilegios, manteniendo el acceso y ocultando huellas propias de un "atacante real" por lo que ISSAF puede ser de las metodologías mas completas a la hora de realizar una auditoria, al igual que OSSTMM está dirigido a cualquier tipo de sistema, aunque parece que esta está enfocada a grandes organizaciones.

OWASP

Al igual que OSSTMM e ISSAF es una metodología que se encarga de desarrollar y adquirir aplicaciones para securizar mayoritariamente plataformas Web.

OWASP es la organización encargada de realizar el famoso top 10 de las vulnerabilidades más explotadas del año. (Las siguientes son las del año 2013)

A1 Injection

A2 Broken Authentication and Session Management (was formerly 2010-A3)

A3 Cross-Site Scripting (XSS) (was formerly 2010-A2)

A4 Insecure Direct Object References

A5 Security Misconfiguration (was formerly 2010-A6)

A6 Sensitive Data Exposure (2010-A7 Insecure Cryptographic Storage and 2010-A9 Insufficient Transport Layer Protection were merged to form 2013-A6)

A7 Missing Function Level Access Control (renamed/broadened from 2010-A8 Failure to Restrict URL Access)

A8 Cross-Site Request Forgery (CSRF) (was formerly 2010-A5)

A9 Using Components with Known Vulnerabilities (new but was part of 2010-A6 – Security Misconfiguration)

A10 Unvalidated Redirects and Forwards

A diferencia de OSSTMM e ISSAF, OWASP como ya mencioné antes está enfocada directamente a aplicaciones Web, lo que, desde mi punto de vista saca directamente de la comparación con las otras dos metodologías anteriores.

Conclusión.

Comencemos con la primera, tiene una gran área de acción, ni tan limitada como OWASP ni tan grande como la de ISSAF, desde mi punto de vista ISSAF esta dirigida a grandes empresas a diferencia de OSSTMM que da a entender que maneja un entorno menor que ISSAF, OWASP también tiene un perfil importante, ya que creo que es usada por todos, grande, mediana y gran empresa. Ya que las aplicaciones WEB no distinguen de tamaño, obviamente las hay de mayor o menor importancia pero en todas es necesario estar bien protegidos, en lo que respecta a la facilidad de uso, las tres están igualadas ya que es necesario tener conocimientos para llevar a cabo cualquiera de las tres, en el apartado de utilización por parte de los auditores, supongo que ISSAF será la mas utilizada, al ser la mas completa en las auditorias convencionales (excluyendo las auditorias especificas para aplicaciones WEB) aun así pienso que deberán ser utilizadas según las necesidades del cliente .

La conclusión final es la siguiente, por lógica aplastante debería ser PETS pero ISSAF me parece un esquema de penetración muy completo y flexible, desde mi punto de vista es la más completa. (Sobre PETS no profundicé, ya que como anotaban los apuntes es una simplificación de OSSTMM e ISSAF, un nuevo estándar, que facilitará y obtendrá mejores resultados que las mencionadas anteriormente, en la información que he encontrado PETS es el estándar mas utilizado por pentesters.

Pre-engagement Interactions

Intelligence Gathering

Threat Modeling

Vulnerability Análisis

Exploitation

Post Exploitation

Reporting

Estas secciones definen bien lo que puede ser el esquema actual de un Test de penetración.