UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Seguridad en la Red Informática Mundial

Metodología OSSTMM
Open Source Security Testing Methodology Manual

Semana 3 clases 5 y 6

Mtra. María Noemí Araiza Ramírez

Metodología OSSTMM

Manual de Metodología de Pruebas de Seguridad de Código Abierto o bien se conoce como Manual de la Metodología Abierta del Testeo de Seguridad.

Fue creado por Pete Herzog y desarrollado por ISECOM (Institute for Security and Open Methodologies) http://www.isecom.org

ISECOM es una organización sin fin de lucro, dedicada al desarrollo de metodologías para la verificación de la seguridad, programación segura, verificación de software y concientización en seguridad.

OSSTMM es el proyecto más destacado de ISECOM, sin embargo también tiene otros:

SCARE
The Source Code Analysis and Risk Evaluation.
Análisis de código fuente y evaluación de riesgos.

Child Safety and Security Methodology
Una metodología para enseñar seguridad a los niños a través de juegos e historias

Home Security Methodology
Metodología para mantener seguros los hogares y mantenerlos a salvo de posibles amenazas

National Security Methodology
Definición de políticas y metodologías para mejorar la seguridad nacional.

OSSTMM

Es uno de los estándares más usado en auditorías de seguridad para revisar la seguridad de los sistemas desde Internet.

Incluye un marco de trabajo que describe las fases que hay que realizar para la ejecución de la auditoría.

OSSTMM

Hay plantillas que brinda OSSTMM para aplicar técnicas de Hackeo ético, para identificar puntos débiles de la empresa o del sistema que se audita.

Toma en cuenta cada detalle en la seguridad de las organizaciones, que son susceptibles a vulnerabilidades.

OSSTMM

La plantilla de datos reflejará cuáles módulos y tareas han sido probados (test de penetración) hasta su conclusión, cuáles no y su justificación, así como las pruebas no aplicables, con su justificación.

OSSTMM

Se propone interiorizar la seguridad, por lo que se persigue cualquiera de estas tres situaciones:

Crear una barrera (lógica o física) entre el activo y las amenazas.

Trabajar con las amenazas para reducirlas a un estado donde su efecto produzca un daño mínimo

Destruir por completo las amenazas

OSSTMM

Análisis de seguridad

Analisis de Seguridad aqui se refiere a la habilidad de transformar la informacion en inteligencia de seguridad.

Esto requiere entender más que sólo la información, también de dónde vino, cómo y cuándo fue recolectada, y cualquier restricción del proceso de recolección.

La parte final del proceso de análisis es crear inteligencia accionable, información derivada de hechos que puede ser usada para la toma de decisiones.

Esta es la clara distinción entre el análisis de seguridad y riesgos.

OSSTMM

Análisis de seguridad

En el análisis de seguridad, se producen hechos incluso si dichos hechos proponen algo que no se puede conocer dada la información recolectada.

En el análisis de riesgo, se especulan y derivan opiniones basadas en la información.

El análisis de riesgo puede usar el análisis de seguridad para obtener respuestas más acertadas, sin embargo el análisis de seguridad no puede usar el análisis de riesgo para mejorar su certeza.

Por esta razón se recomienda un análisis confiable.

OSSTMM

Análisis de seguridad

La diferencia fundamental entre hacer un análisis de riesgo versus un análisis de seguridad es que en el análisis de seguridad nunca se analiza la amenaza.

Esto se debe a que se asume que se sabe qué amenazas existen, cuándo pueden atacar, cómo llegarán y a dónde irán, es algo reservado para el análisis de riesgo.

En el análisis de seguridad, se estudia y mide la superficie de ataque alrededor de un objetivo.

Esto entonces permitirá entender dónde hay amenazas, si hay alguna, si pueden o no atacar.

OSSTMM

Análisis de seguridad

Por ejemplo, considera una pared muy alta.

El análisis de riesgo considera que es lo que puede atravesar la pared, pero el análisis de seguridad se enfoca en dónde están las grietas, si la estructura es solida, y si la pared es lo suficientemente gruesa o alta como para prevenir el acceso y responder al ataque.

Un análisis de seguridad también le permitirá asegurar si los controles correctos existen, la forma en la que deben funcionar, y la forma correcta de cubrir los puntos interactivos de varios vectores accesibles y canales.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OSSTMM

Análisis de seguridad

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OSSTMM

Buscar vulnerabilidades

OSSTMM

Técnica de análisis de seis pasos

1

Crear los conocimientos del objetivo a estudiar, evitando información especulativa.

2

Determinar el nivel global de experiencia para el tipo de objetivo y la cantidad de información.

3

Determinar cualquier parcialidad en la fuente de información que pudieran desviarnos del objetivo final.

OSSTMM

Técnica de análisis de seis pasos

4

Traducir las palabras propias de la fuente de información, para diferencias cosas comunes de posibles trampas.

5

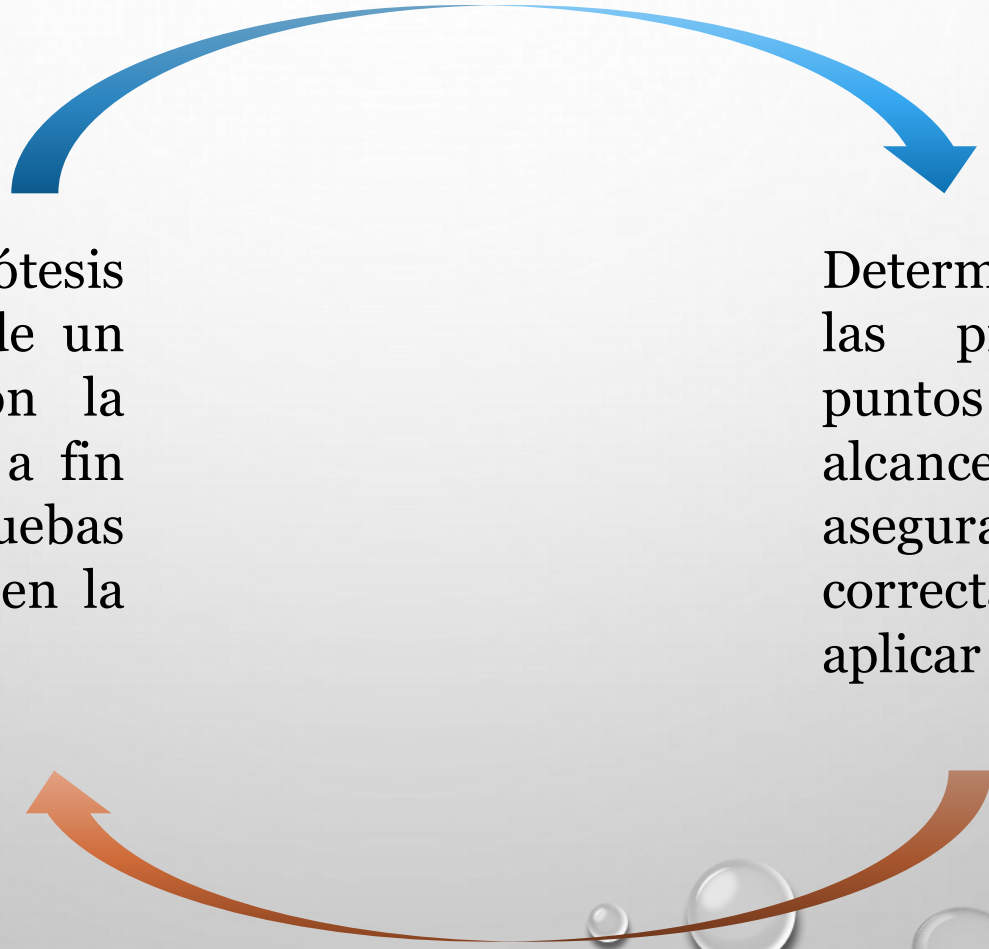
Asegurar que los equipos de prueba se han calibrado adecuadamente, así como los ambientes de prueba, para asegurar que los resultados no están contaminados.

6

Asegurar que los estados de transición han sido removidos, para asegurar que los resultados no provienen de fuentes indirectas.

OSSTMM

Caracterizar los resultados



Se debe hacer una hipótesis de la interactividad de un punto de acceso con la superficie de ataque, a fin de formular las pruebas correctas que verifiquen la hipótesis

Determinar con anterioridad las propiedades de los puntos de interacción y sus alcances, con la finalidad de asegurar las pruebas correctas, cuando se deban aplicar

OSSTMM

Informes transparentes

De forma clara y sencilla se deben transmitir los resultados obtenidos:

Limitaciones identificadas y verificadas
Determina si las pruebas son peligrosas o muy costosas.

Objetivos no probados
Si la prueba no pudo completarse por tiempo, dificultades, ambientes de prueba muy dinámicos.

Desconocidos
Este valor muestra el nivel de dificultad de la prueba, y son resultados que se dan por válidos.

OSSTMM

Análisis de los seis pasos

De forma clara y sencilla se deben transmitir los resultados obtenidos:

Fallas en procedimientos y procesos de seguridad
Qué puede ocurrir cuando no se cumple con los procesos.

Falsos positivos y el significado de generarlos
Para ciertos tiempos y situaciones, no aparece la exposición a ciertas vulnerabilidades.

OSSTMM

Análisis de los seis pasos

De forma clara y sencilla se deben transmitir los resultados obtenidos:

Conformidad
El analista necesita utilizar el resultado de las pruebas para determinar si se cumplió el objetivo con los resultados de las pruebas.

Buenas prácticas
Permite definir soluciones configurables para cada caso.

OSSTMM


Seguridad de la **Información**
Seguridad **Física**
Seguridad de los **Procesos**
Se encuentra en constante evolución y se compone de las siguientes fases:
Seguridad **Inalámbrica**
Seguridad en las **Tecnologías de Internet**
Seguridad en las **Comunicaciones**

OSSTMM

Seguridad de la Información

Recolección de documentos

Revisión de privacidad

Revisión de la inteligencia competitiva

OSSTMM

Seguridad de los procesos

Testeo de solicitud

Testeo de sugerencia dirigida

Testeo de las personas confiables

OSSTMM

Seguridad de las tecnologías de internet

- Logística y controles
- Exploración de red
- Identificación de los servicios del sistema
- Búsqueda de información competitiva y revisión de privacidad
- Obtención de documentos

OSSTMM

Seguridad de las tecnologías de internet

- Búsqueda y verificación de vulnerabilidades
- Testeo de aplicaciones de internet
- Enrutamiento
- Testeo de sistemas confiados
- Testeo de control de acceso

OSSTMM

Seguridad de las tecnologías de internet

- Testeo de sistema de detección de intrusos
- Testeo de medidas de contingencia
- Descifrado de contraseñas
- Testeo de denegación de servicios
- Evaluación de políticas de seguridad

OSSTMM

Seguridad en las Comunicaciones

Testeo de PBX (Private Branch Exchange)

Testeo del correo de voz

Revisión del fax

Testeo del módem

OSSTMM

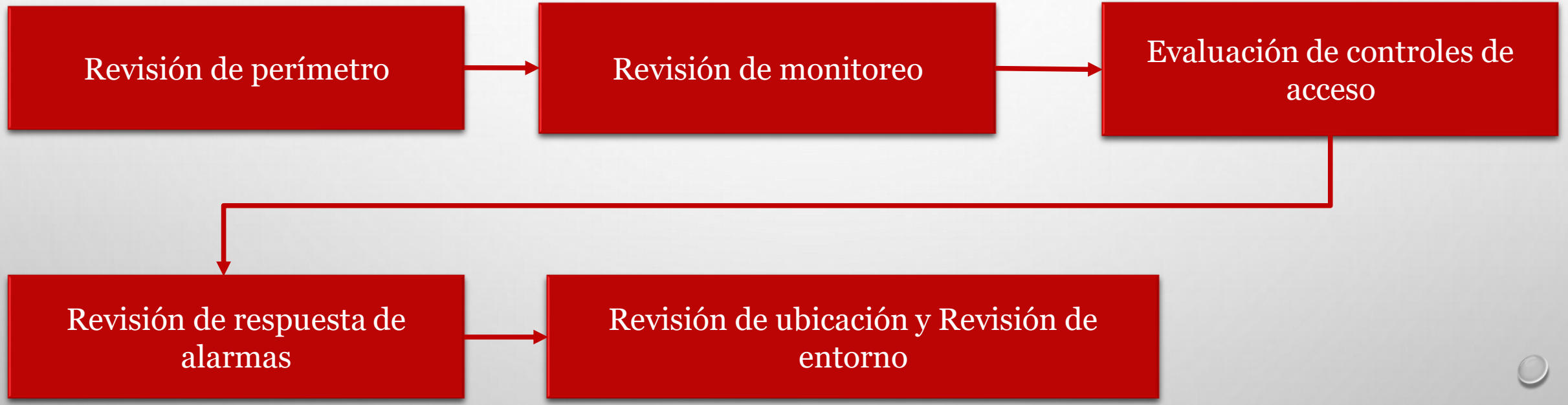
Seguridad Inalámbrica

OSSTMM

Seguridad Inalámbrica

OSSTMM

Seguridad Física



OSSTMM

Plantillas

Las siguientes plantillas son un ejemplo de los requisitos que deben cumplir los informes de cada una de las partes de la seguridad que se revisa.

Se indica la información que debe contenerse en el informe para que sea calificado dentro de la metodología OSSTMM

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OSSTMM

Plantilla de Perfil de Red

Rangos de IP que serán testeados y detalle de dichos rangos

Información de los dominios y su configuración

Información destacada de la transferencia de zonas

LISTA DE SERVIDORES

Dirección IP	Nombre(s) de dominio	Sistema operativo

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OSSTMM

Plantilla de Datos del Servidor

Dirección IP	Nombre de dominio

Puerto	Protocolo	Servicio	Detalles del servicio

MENSAJES DE BIENVENIDA:

Puerto	Protocolo	Mensaje de bienvenida

SECUENCIAS TCP:

Predicción de secuencia TCP:
Números de secuencia ISN TCP:
Generación de secuencias IPID:
Tiempo operacional

PREOCUPACIONES Y VULNERABILIDADES:

Preocupación o Vulnerabilidad
Ejemplo
Solución

Álvarez, Marañón, Gonzalo, and García, Pedro Pablo Pérez. Seguridad informática para empresas y particulares, McGraw-Hill España, 2004. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univunirsp/detail.action?docID=3195263.

Escrivá, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univunirsp/detail.action?docID=3217398.