UNIVERSIDAD INTERNACIONAL DE LA RIOJA

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

Seguridad en la Red Informática Mundial

Metodología OSSTMM
Open Source Security Testing Methodology Manual

Semana 5 clases 9 y 10

Mtra. María Noemí Araiza Ramírez

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

"En este módulo se deben enumerar los servicios de Internet activos o accesibles así como traspasar el cortafuegos con el objetivo de encontrar más máquinas activas.

El testeo de diferentes protocolos dependerá del tipo de sistema y servicios que ofrecen los sistemas.

Cada servidor activo en Internet dispone de 65.536 puertos TCP y UDP posibles (incluido el Puerto 0). No es necesario comprobar todos estos puertos en cada sistema, se deja a la libre elección del equipo que realiza los tests."

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

"Una vez los puertos abiertos han sido identificados, es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio.

En algunos casos, más de una aplicación puede encontrarse detrás de un servicio donde una aplicación es la que realmente escucha en dicho puerto y las otras se consideran componentes de la aplicación que escucha.

Un buen ejemplo de esto es PERL que se instalo para ser usado por las aplicaciones web. En este caso, el servicio que escucha es el demonio HTTP y el componente es PERL.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Resultados Esperados:	Puertos abiertos, cerrados y filtrados Direcciones IP de los sistemas activos Direccionamiento de los sistemas de la red interna Lista de los protocolos descubiertos de tunelizado y encapsulado Lista de los protocolos descubiertos de enrutado soportados Servicios activos Tipos de Servicios Tipo y nivel de parcheado de las Aplicaciones de los Servicios Tipo de Sistema Operativo Nivel de parcheado Tipo de Sistema Lista de sistemas activos Mapa de la red

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Enumeración de sistemas

1 Recoger respuestas de broadcast desde la red

2 Intentar traspasar el cortafuegos con valores estratégicos de TTLs (Firewalking) para todas las direcciones IP.

3 Emplear ICMP y resolución inversa de nombres con el objetivo de determinar la existencia de todos los sistemas en la red.

4 Emplear paquetes TCP con puerto origen 80 y el bit ACK activo en los puertos de destino 3100-3150, 1001-10050, 33500-33550 y 50 puertos aleatorios por encima del 35000 para todos los sistemas de la red.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Enumeración de sistemas

5 Emplear paquetes TCP fragmentados en orden inverso mediante escaneos FIN, NULL y XMAS en los puertos destino 21, 22, 25, 80 y 443 para todos los servidores de la red.

6 Usar escaneos TCP SYN sobre los puertos 21, 22, 25, 80 y 443 para todos los servidores de la red.

7 Emplear intentos de conexión a DNS para todos los servidores de la red.

8 Emplear FTP y Proxies para relanzar los escaneos al interior de la DMZ para los puertos 22, 81, 111, 132, 137 y 161 para todos los servidores de la red.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Enumeración de Puertos

9 Usar escaneos SYN TCP (Half-Open) para enumerar puertos abiertos, cerrados o filtrados para aquellos puertos TCP utilizados por defecto en el test, en todos los servidores de la red.

10 Usar scaneos TCP full connect para escanear todos los puertos por encima del 1024 en todos los servidores de la red.

11 Usar escaneos TCP fragmentados en orden inverso para enumerar puertos y servicios para el conjunto de puertos definidos en el Apéndice B por defecto para todos los servidores de la red.

12 Usar escaneos UDP para enumerar puertos abiertos o cerrados para los puertos UDP por defecto si UDP no está siendo filtrado. [Recomendación: primero comprobar el sistema de filtrado para un subconjunto de puertos UDP.]

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Verificación de Respuestas para Varios Protocolos

13 Verificar y examinar el uso de tráfico y protocolos de enrutamiento.

14 Verificar y examinar el uso de protocolos no estándar.

15 Verificar y examinar el uso de protocolos cifrados.

16 Verificar y examinar el uso de TCP e ICMP sobre IPV6.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Verificación de Respuestas a Nivel de Paquete

17 Identificar la predictibilidad de las secuencias TCP.

18 Identificar la predictibilidad de los números de secuencia TCP ISN.

19 Identificar la predictibilidad de la Generación de Secuencia IPID.

20 Identificar el up-time del sistema.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Identificación de Servicios

21 Relacionar cada puerto abierto con un servicio y protocolo.

22 Identificar el nivel de parcheado del sistema a partir de su up-time.

23 Identificar la aplicación tras el servicio y su nivel de parcheado empleando los banners o la identificación de huellas.

24 Verificar la aplicación y su versión en el sistema.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

Identificación de Servicios

25 Localizar e identificar el remapeo de servicios o la redirección de sistemas.

26 Identificar los componentes de los servicios en escucha.

27 Usar peticiones propias de Troyanos y servicios UDP en todos los sistemas de la red.

Identificación de Sistemas

28 Examinar las respuestas de los sistemas para determinar el tipo de sistema operativo y su nivel de parcheado.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Identificación de los Servicios del Sistema

29 Examinar las respuestas de las aplicaciones para determinar su sistema operativo y su nivel de parcheado.

30 Verificar la predicción de secuencia TCP para todos los servidores de la red.

31 Busque ofertas de trabajo donde obtener información sobre los servidores y aplicaciones del objetivo.

32 Buscar en boletines técnicos y grupos de noticias información sobre los servidores y las aplicaciones del objetivo.

33 Relacionar la información recopilada con las respuestas de los sistemas para ajustar los resultados.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Búsqueda y Verificación de Vulnerabilidades

"La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red.

La investigación concerniente a la búsqueda de vulnerabilidades es necesaria hasta prácticamente el momento de la entrega del informe.

La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Búsqueda y Verificación de Vulnerabilidades

Es importante para los auditores identificar e incorporar en las pruebas que realizan los scripts y exploits que existen actualmente en el mundo.

Resultados Esperados:	Tipo de aplicación o servicio por vulnerabilidad Niveles de parches de los sistemas y aplicaciones Listado de posibles vulnerabilidades de denegación de servicio Listado de áreas aseguradas a través de ocultación o acceso visible Listado de vulnerabilidades actuales eliminando falsos positivos Listado de sistemas internos o en la DMZ Listado de convenciones para direcciones de e-mail, nombres de servidores, etc.. Mapa de red

Metodología OSSTMM

Seguridad de las tecnologías de internet

Búsqueda y Verificación de Vulnerabilidades

1 Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.

2 Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.

3 Intentar determinar vulnerabilidades por tipo de aplicación y sistema.

4 Intentar ajustar vulnerabilidades a servicios.

5 Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.

6 Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Búsqueda y Verificación de Vulnerabilidades

7 Identificar todas las vulnerabilidades relativas a las aplicaciones.

8 Identificar todas las vulnerabilidades relativas a los sistemas operativos.

9 Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los sistemas objetivo.

10 Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.

11 Verificar todos los positivos (Se debe tener en cuenta el contrato firmado con la organización objetivo en el caso de estar intentando penetrar o si se puede llegar a provocar una denegación de servicio).

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

"Un test de Aplicaciones de Internet emplea diferentes Técnicas de testeo de Software para encontrar "fallos de seguridad" en aplicaciones cliente/servidor de un sistema desde Internet.

Se refiere a aplicaciones cliente/servidor que sean desarrolladas por los administradores de sistema con propósitos de la empresa y programadas con cualquier tecnología y lenguaje de programación.

Como ejemplo: Aplicaciones web para transacciones entre empresas.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

Resultados Esperados:	Lista de Aplicaciones Lista de los Componentes de las Aplicaciones Lista de las Vulnerabilidades de las Aplicaciones Lista de los Sistemas Confiados por las Aplicaciones

Re-Ingeniería

1 Descomponer o Deconstruir los códigos binarios, si es posible.

2 Determinar las Especificaciones de Protocolo de la Aplicación Cliente/Servidor.

3 Adivinar la lógica del programa de los mensajes de error/debug en las salidas del programa y en el rendimiento y comportamiento del programa.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

Autenticación

4 Buscar las posibles combinaciones de contraseñas por fuerza bruta en las aplicaciones

5 A ser posible, buscar credenciales de cuentas válidas por fuerza bruta.

6 Saltarse el sistema de autenticación con una validación cambiada.

7 Saltarse el sistema de autenticación reproduciendo información de la autenticación.

8 Determinar la lógica de la aplicación para mantener las sesiones de autenticación – número (consecutivo) de intentos fallidos, intentos fuera de tiempo, etc.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

9 Determinar las limitaciones de control de acceso en las aplicaciones - permisos de acceso, duración de las sesiones, tiempo inactivo.

Administración de Sesiones

10 Determinar la Información de Administración de Sesiones – numero de sesiones concurrentes, Autenticaciones basadas en IP, Autenticación basada en roles, Autenticación basada en Identidad, uso de Cookies, ID de sesión dentro de las secuencias de codificación de la URL, ID de sesión en campos HTML ocultos, etc.

11 Adivinar la secuencia y formato de la ID de sesión

12 Determinar si la ID de sesión esta formada con información de direcciones IP; mirar si la misma información de sesión puede ser recuperada y reutilizada en otra máquina.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

13 Determinar las limitaciones de mantenimiento de sesión - uso del ancho de banda, limitaciones de bajadas/subidas de archivos, limitaciones en transacciones, etc.

14 Reunir bastante información con URL's exactas, instrucciones exactas, secuencias de acción / saltos de secuencia y/o omisiones de las páginas.

15 Reunir información sensible a partir de ataques Hombre-en-el-Medio.

16 Inyectar falsa información con técnicas de Hijacking (secuestro).

17 Reproducir la información reunida para engañar a las aplicaciones

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

Manipulación de la información de entrada

18 Encontrar las limitaciones de las variables definidas y de los protocolos - longitud de datos, tipo de datos, formato de la estructura etc.

19 Usar cadenas largas de caracteres para encontrar vulnerabilidades de desbordamientos de memoria en las aplicaciones.

20 Concatenar comandos en las cadenas de entrada de las aplicaciones.

21 Inyectar comandos SQL en las entradas de cadenas de caracteres de aplicaciones web basadas en bases de datos

22 Examinar vulnerabilidades "Cross-Site Scripting" en las aplicaciones web del sistema

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

23 Examinar accesos a directorios/ficheros no autorizados con directorios/rutas transversales en las entradas de cadenas de caracteres de las aplicaciones.

24 Usar cadenas específicas de codificación URL y/o codificación Unicode para saltarse los mecanismos de validación de las aplicaciones.

25 Ejecutar comandos remotos a través de "Server Side Include".

26 Manipular el estado de las cookies (session/persistent) para tirar o modificar la lógica dentro de las aplicaciones web "server-side".

27 Manipular los campos variables (ocultos) en los formularios HTML para tirar o modificar la lógica en las aplicaciones web "server inside"

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

28 Manipular las variables "Referrer", "Host", etc. del protocolo HTTP para tirar o modificar la lógica en las aplicaciones web "server inside"..

29 Usar información de entrada ilógica/ilegal para testear las rutinas de error de la aplicación y encontrar mensajes de error/depuración que sean útiles.

Manipulación de la Información de salida

30 Recuperar información importante/comprometedora guardadas en las cookies

31 Recuperar información importante/comprometedora en la caché de la aplicación cliente

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Aplicaciones de Internet

32 Recuperar información importante/comprometedora guardada en los objetos con número de serie

33 Recuperar información importante/comprometedora guardada en los archivos temporales y objetos

Filtración de información

34 Buscar información utilizable en campos ocultos de variables en formularios HTML y comentarios en los documentos HTML

35 Examinar la información contenida en los banners de la aplicación, instrucciones de uso, mensajes de bienvenida, mensajes de despedida, mensajes de ayuda, mensajes de error/depuración, etc.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Enrutamiento

"Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet.

Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o deniega paquetes.

Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Enrutamiento

"La protección también debe estar diseñada para restringir el flujo de salida de ciertos tipos de tráfico.

Los Router están siendo cada vez más complejos y algunos tienen propiedades desconocidas para el auditor y a veces para la organización auditada.

El papel del auditor es en parte determinar la función del router dentro de la DMZ.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Enrutamiento

Resultados Esperados:	Tipo de Router y Propiedades implementadas Información del router como servicio y como sistema Perfil de la política de seguridad de una red a partir de la ACL Lista de los tipos de paquetes que deben entrar en la red Mapa de las respuestas del router a varios tipos de tráfico Lista de los sistemas vivos encontrados

El Router y sus características

1 Verificar el tipo de router con información reunida de la obtención de Inteligencia.

2 Verificar si el router está dando servicio de traducción de direcciones de red (NAT).

3 Verificar las intrusiones con opciones TTL estratégicas en los paquetes ,(Firewalking) hecho en el módulo de escaneo de puertos

Metodología OSSTMM

Seguridad de las tecnologías de internet

Enrutamiento

Verificar la configuración de las ACL's del router

4 Testear la ACL del router en contra de las políticas de seguridad y en contra de la regla "Deny All".

5 Verificar si el router está filtrando el tráfico de la red local hacia afuera.

6 Verificar que el router esté haciendo detección de direcciones falsas.

7 Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.

8 Testear las capacidades externas del router desde el interior.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Enrutamiento

9 Cuantificar la habilidad que tiene el router para manejar fragmentos de paquetes muy pequeños.

10 Cuantificar la habilidad del router para manejar paquetes grandes.

11 Cuantificar la habilidad del router para manejar fragmentos coincidentes como los usados en ataques del tipo TEARDROP.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistemas Confiados

"El propósito de los testeos de sistemas confiados es afectar la presencia en Internet planteándose como una entidad confiada en la red.

El escenario de testeo es a veces más teoría que práctica, y en realidad mas que oscurecer la frontera entre un Test de Vulnerabilidad y un Testeo de Cortafuegos / ACLS, es dicha frontera.

Resultados Esperados:	Mapa de los sistemas dependientes de otros sistemas Mapa de las aplicaciones con dependencias a otros sistemas Tipos de vulnerabilidades que afectan a los sistemas de confianzas y aplicaciones

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistemas Confiados

1 Verificar las relaciones determinadas en la obtención de Inteligencia, Testo de Aplicaciones y Testeo de Servicios.

2 Testear las relaciones entre varios sistemas a través de provocación de eventos "event triggering" o engaño de origen.

3 Verificar que los sistemas puedan ser engañados.

4 Verificar qué aplicaciones pueden ser engañados.