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 6 clases 11 y 12

Mtra. María Noemí Araiza Ramírez

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

"El cortafuegos controla el flujo del tráfico de la red corporativa, la DMZ, e Internet. Opera en una política de seguridad y usa ACL's (Listas de Control de Acceso).

Este módulo está diseñado para asegurar que sólo lo que debe estar expresamente permitido puede ser aceptado dentro de la red, todo lo demás debe ser denegado.

El auditor debe entender la configuración del cortafuegos provista entre los servidores y los servicios que hay detrás.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

Repasando los logs necesarios de los servidores para verificar los tests desempeñados en presencia de Internet, especialmente en casos donde los resultados de los tests no son inmediatamente evidentes para el auditor.

Resultados Esperados:	Información en el firewall como servicio y como sistema Información de las características implementadas en el firewall Perfil de la política de seguridad de la red a partir de la ACL Lista de los tipos de paquetes que deben entrar en la red Lista de tipos de protocolos con acceso dentro de la red Lista de los sistemas "vivos" encontrados Lista de paquetes, por número de puerto, que entran en la red Lista de protocolos que han entrado en la red Lista de rutas sin monitorizar dentro de la red

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

El Cortafuegos 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

Testeo de Control de Acceso

Verificación de la configuración de las ACL

4 Testear la ACL del cortafuego en contra de las políticas de seguridad y en contra de la regla "Denegar Todo".

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

6 Verificar que el cortafuegos esté haciendo detección de direcciones de origen falso

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

8 Testear las capacidades externas del cortafuegos desde el interior.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

9 Determinar el éxito de los métodos de identificación de cortafuegos a través de las distintos paquetes de respuesta.

10 Verificar la posibilidad de escanear usando técnicas ocultas SYN para enumeración a través del cortafuegos.

11 Verificar la posibilidad de escanear para enumeración usando puertos orígenes específicos.

12 Cuantificar la habilidad del cortafuegos para manejar fragmentos superpuestos como los usados en ataques del tipo TEARDROP.

13 Cuantificar la habilidad del cortafuegos para manejar fragmentos de paquetes diminutos.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

14 Testear la habilidad del cortafuegos para manejar series de paquetes SYN entrantes (inundación)

15 Testear la respuesta del cortafuegos a paquetes con la bandera RST activada.

16 Testear el mantenimiento del cortafuegos con paquetes UDP estándar.

17 Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando paquetes ACK (mensaje del destino al origen que confirma su recepción).

18 Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando paquetes FIN (último paquete de una conexión).

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

19 Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando paquetes NULL

20 Verificar la habilidad del cortafuegos para protegerse de varias técnicas midiendo el tamaño de ventana en el paquete (WIN).

21 Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando todas las banderas activadas (XMAS).

22 Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando IPIDs.

23 Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando protocolos encapsulados.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

24 Cuantificar la robustez del cortafuegos y su susceptibilidad a los ataques de denegación de servicios con conexiones TCP ininterrumpidas.

25 Cuantificar la robustez del cortafuegos y su susceptibilidad a los ataques de denegación de servicios con conexiones TCP temporales.

26 Cuantificar la robustez del cortafuegos y su susceptibilidad a los ataques de denegación de servicios con datagramas UDP.

27 Cuantificar la respuesta del cortafuegos a todos los tipos de paquetes ICMP.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Control de Acceso

Revisión de Registros del Cortafuegos

28 Testear el proceso de registro del cortafuegos

29 Verificar escaneos TCP y UDP en los registros del servidor

30 Verificar escaneos de vulnerabilidades automatizados

31 Verificar deficiencias de registros de servicios

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistema de Detección de Intrusos

IDS (Sistema de detección de intrusiones) se refiere a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y así, reducir el riesgo de intrusión.

Existen dos tipo importantes de IDS: el grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red, y el grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistema de Detección de Intrusos

Este test se enfoca al rendimiento y susceptibilidad de un IDS. Algunos de estos tests están relacionados con ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estos tests.

Resultados Esperados:	Tipo de IDS Nota del rendimiento de los IDS bajo una sobrecarga Tipo de paquetes eliminados o no escaneados por el IDS Tipo de protocolos eliminados o no escaneados por el IDS Nota del tiempo de reacción y tipo del IDS Nota de la susceptibilidad del IDS Mapa de reglas del IDS Lista de falsos positivos del IDS Lista de alarmas perdidas del IDS Lista de rutas no monitorizadas en la red

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistema de Detección de Intrusos

El IDS y sus características

1 Verificar el tipo de IDS con información recogida de la Inteligencia de Información

2 Determinar la esfera de protección o influencia.

3 Testear los estados de alarma del IDS.

4 Testear los parámetros de sensibilidad de las firmas pasado 1 minuto, 5 minutos, 60 minutos, y 24 horas.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistema de Detección de Intrusos

Testeo de configuración IDS

5	Testear la configuración del IDS para reacciones múltiples, ataques variados (inundación).
6	Testear la configuración del IDS para reacciones como URLs manipuladas y rutinas de explotación.
7	Testear la configuración del IDS para reacciones ante cambios de velocidad al enviar paquetes.
8	Testear la configuración del IDS para reacciones ante cambios aleatorios de velocidad durante un ataque.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistema de Detección de Intrusos

9 Testear la configuración del IDS para reacciones ante cambios aleatorios de protocolos durante un ataque.

10 Testear la configuración del IDS para reacciones ante cambios aleatorios de origen durante un ataque.

11 Testear la configuración del IDS para reacciones ante cambios de puerto de origen.

12 Testear en el IDS, la habilidad de manejar paquetes fragmentados.

13 Testear en el IDS, la habilidad de manejar métodos de ataques de sistemas específicos.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Sistema de Detección de Intrusos

14	Testear los efectos y reacciones del IDS. Una dirección IP contra varias direcciones.
15	Encontrar alertas de IDS sobre escaneos de vulnerabilidades.
16	Encontrar alertas de IDS sobre descifrado de contraseñas
17	Encontrar alertas de IDS de testeos de sistemas confiados.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Medidas de Contingencia

Las medidas de contingencia dictan el manejo de lo penetrable, programas maliciosos y emergencias.

La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados.

Debe ser necesario responder primero a una nueva cuenta de correo electrónico de pruebas o al sistema de escritorio donde el administrador pueda monitorear.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Medidas de Contingencia

Resultados Esperados:	Definición de las capacidades Anti-Troyano Definición de las capacidades Anti-Virus Identificación de las Medidas de Contingencia de Escritorio Identificación de las Debilidades de Contingencia de Escritorio Lista de recursos de contingencia

1 Medir el mínimo de recursos necesarios que se necesitan en el subsistema para realizar las tareas.

2 Verificar los recursos disponibles a este subsistema que necesiten realizar estas tareas, y que recursos están protegidos desde este subsistema.

3 Verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Medidas de Contingencia

4 Verificar recursos innecesarios.

5 Verificar las propiedades del sistema de contingencia.

6 Verificar la detección de medidas presentes para la detección de accesos 'no comunes' a los recursos 'necesarios'.

7 Medidas de configuración del sistema.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Descifrado de Contraseñas

Es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizados, que dejan al descubierto la aplicación de algoritmos criptográficos débiles o contraseñas débiles debido a factores humanos.

Este módulo puede incluir técnicas para averiguar manualmente las contraseñas, que explote los usuarios y contraseñas por defecto en aplicaciones o sistemas operativos (p.ej. Usuario: System Contraseña: Test) o fácilmente predecible por parte del error de un usuario (p.ej. Usuario: joe Contraseña: joe).

Metodología OSSTMM

Seguridad de las tecnologías de internet

Descifrado de Contraseñas

Este puede ser un sistema para obtener acceso a un sistema inicialmente, quizá sea siempre con acceso de administrador o root, pero sólo con fines educativos.

Una vez entrado con privilegios de root o administrador en un sistema, el descifrado de contraseñas consiste en obtener acceso a sistemas o aplicaciones adicionales (gracias a los usuarios cuyas contraseñas sean coincidentes en múltiples sistemas) y es una técnica válida que puede ser usada por influencia del sistema a través de un test de seguridad.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Descifrado de Contraseñas

Descifrados de contraseñas minuciosos pueden ser realizados como un ejercicio de simple y debe ser subrayada la necesidad de algoritmos criptográficos fuertes para contraseñas de almacenamiento de sistemas de llave, también subrayar la necesidad del refuerzo de una política estricta de contraseñas de usuario, generación automática.

Resultados Esperados:	Ficheros de Contraseñas descifrados o no descifrados Lista de cuentas, con usuario o contraseña de sistema Lista de sistemas vulnerables a ataques de descifrado de contraseñas Lista de archivos o documentos vulnerables a ataques de descifrado de contraseñas Lista de sistemas con usuario o cuenta de sistema que usan las mismas contraseñas

Metodología OSSTMM

Seguridad de las tecnologías de internet

Descifrado de Contraseñas

1 Obtener el fichero de contraseñas desde el sistema que guarda nombres de usuario y contraseña.

- Para sistemas Unix, ha de estar en /etc/passwd o/y /etc/shadow.
- Para sistemas Unix que tienen que realizar autenticaciones SMB, puede encontrar las contraseñas de NT en /etc/smbpasswd.
- Para sistemas NT, ha de estar en /winnt/repair/Sam._ (u otra, más dificil de obtener variantes)

2 Arranque un ataque automatizado de diccionario al fichero de contraseñas.

3 Arranque un ataque de fuerza burta al fichero de contraseñas.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Descifrado de Contraseñas

4 Usar contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.

5 Arranque Programas automatizados de descifrado en ficheros cifrados que haya encontrado (como documentos PDF o Word) como intento de recopilar más datos y subrayar la necesidad de un cifrado del sistema o de documentos más fuerte.

6 Verificar la edad de las contraseñas.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Denegación de Servicios

La Denegación de Servicios (DoS) es una situación donde una circunstancia, sea intencionada o accidental, previene el sistema de tal funcionalidad como sea destinada. En ciertos casos, el sistema debe funcionar exactamente como se diseñó, nunca fue destinado para manejar la carga, alcance, o parámetros que abusen de ellos.

Es muy importante que los tests de DoS reciban ayuda adicional de la organización y sea monitorizada a nivel privado. Inundación y ataques DoS Distribuidos (DDoS) están específicamente no comprobados y prohibidos por este manual.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Denegación de Servicios

Los ataques de inundación y los ataques DDoS SIEMPRE causarán ciertos problemas y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo.

Resultados Esperados:	Lista de puntos débiles en presencia de Internet incluidos los puntos individuales por averías Establecer un punto de referencia para un uso normal Lista de comportamientos de sistema por un uso excesivo Lista de sistemas vulnerables a DoS

Metodología OSSTMM

Seguridad de las tecnologías de internet

Testeo de Denegación de Servicios

1 Verificar que las cuentas administrativas y los archivos y recursos del sistemas están asegurados apropiadamente y todos los accesos están concedidos con "Mínimo Privilegio".

2 Comprobar las restricciones de sistemas expuestas a redes sin confianza.

3 Verificar que los puntos de referencian están establecidos a partir de un actividad normal del sistema.

4 Verificar que los procedimientos están en un lugar que responde a una actividad irregular.

5 Verificar la respuesta a una información negativa SIMULADA (ataques propaganda)

6 Testear cargas de red y de servidor excesivas.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Evaluación de Políticas de Seguridad

Es un documento escrito legible que contiene las políticas que delinean la reducción de riesgos en una organización con la utilización de tipos específicos de tecnologías.

Existen dos funciones a llevar a cabo:
La primera, es el testeo de lo escrito contra el estado actual de las conexiones de la presencia en Internet y de otras conexiones no relacionadas a Internet.

La segunda, asegurar que la política este incluida dentro de las justificaciones de negocio de la organización, y de los estatutos legales locales, federales e internacionales, en especial en referencia a los derechos y responsabilidades tanto del empleador como de los empleados y la ética de privacidad personal.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Evaluación de Políticas de Seguridad

Algunos puntos a tomar en cuenta son:

- Comparar la política de seguridad contra el estado actual de la presencia en Internet.
- Aprobación de la Gerencia – Busque cualquier signo que revele que la política está aprobada por la gerencia.
- Cerciórese de que la documentación está adecuadamente almacenada, ya sea electrónicamente o en otros medios, y que la política ha sido leída y aceptada por el personal incluso antes de que ellos obtengan acceso a los sistemas informáticos.

Metodología OSSTMM

Seguridad de las tecnologías de internet

Evaluación de Políticas de Seguridad

- Identifique los procedimientos de manejo de incidentes, para asegurarse de que las brechas de seguridad son manejadas por las personas adecuadas
- Conexiones entrantes – Verifique los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet (Internet -> DMZ, Internet -> red interna.)
- Conexiones salientes – Las conexiones salientes pueden producirse entre la red interna y DMZ, así como también entre la red interna e Internet.
- Verifique que la política de seguridad establezca las medidas de contención y los tests de ingeniería social basados en el uso indebido de Internet por parte de los empleados, de acuerdo con la justificación de negocios y las mejores prácticas de seguridad.

Metodología OSSTMM

Seguridad en las Comunicaciones

Testeo de PBX (Private Branch Exchange)

Testeo del correo de voz

Revisión del fax

Testeo del módem

Metodología OSSTMM

Seguridad en las Comunicaciones

Testeo de PBX (Private Branch Exchange)

Este es un método para lograr acceso privilegiado a la central telefónica de la organización objetivo.

Resultados Esperados:	Lista de sistemas PBX que permitan ser administrados remotamente Lista de los sistemas que permitan acceso desde cualquier lugar del mundo a la terminal de mantenimiento. Lista de todos los sistemas telefónicos que estén en modo de escucha y de manera interactiva.

1. Revisar los detalles de llamadas en busca de indicios de abuso.
2. Asegurarse que las cuentas administrativas no tengan contraseñas por defecto, ni que las mismas puedan ser fácilmente adivinadas.
3. Verificar que el sistema operativo se encuentre actualizado y con los últimos parches aplicados.
4. Verificar el acceso remoto para el mantenimiento del sistema.
5. Testear la autenticación de las llamadas entrantes.
6. Verificar la autenticación remota de las llamadas entrantes.

Metodología OSSTMM

Seguridad en las Comunicaciones

Testeo del Correo de Voz

Este es un método para lograr acceso privilegiado a los sistemas de correo de voz de la organización y de su personal interno..

Resultados Esperados:	Lista de las casillas de correo de voz que son accesibles desde cualquier ubicación en el mundo. Lista de los códigos de llamadas entrantes a las casillas de correo de voz y sus correspondientes *Números* de Identificación Personal (PINs).

1. Verificar el tamaño del PIN y su frecuencia de cambio.
2. Identificar información de usuarios y de la organización.
3. Verificar el acceso remoto para el mantenimiento del sistema.
4. Testear la autenticación de las llamadas entrantes.
5. Verificar la autenticación remota de las llamadas entrantes.

Metodología OSSTMM

Seguridad en las Comunicaciones

Revisión del FAX

Este es un método para enumerar maquinas de FAX y lograr acceso privilegiado a los sistemas en los que estos quizás se encuentren.

Resultados Esperados:	Lista de los sistemas de FAX. Lista de los tipos de sistemas de FAX y sus posibles programas operativos. Recopilación de información alojada en la memoria de los sistemas de FAX. Mapa del manejo de protocolos de FAX dentro de la organización.

1. Asegurarse que las cuentas administrativas no tengan las contraseñas por defecto, ni que las mismas sean fácilmente adivinables.
2. Testear FAX poling.
3. Verificar el acceso remoto para el mantenimiento del sistema.
4. Testear la autenticación de las llamadas entrantes.
5. Verificar la autenticación remota de las llamadas entrantes.

Metodología OSSTMM

Seguridad en las Comunicaciones

Testeo del Modem

Este es un método para enumerar módems y lograr acceso privilegiado a los sistemas de modems habilitados en los sistemas de la organización objetivo.

Resultados Esperados:	Lista de los sistemas con módems que se encuentren a la escucha. Lista de los tipos modem y sus programas operativos. Lista de los esquemas de autenticación de los módems. Lista de usuarios y contraseñas de acceso vía modem Mapa del manejo de protocolos de modem dentro de la organización.

1. Escanear la central para módems.
2. Asegurarse que las cuentas no tengan las contraseñas por defecto, ni que las mismas sean fácilmente adivinables.
3. Asegurarse que el sistema operativo y las aplicaciones del modem estén actualizados y con los últimos parches aplicados.
4. Verificar el acceso remoto para el mantenimiento del sistema.
5. Testear la autenticación de las llamadas entrantes.
6. Verificar la autenticación remota de las llamadas entrantes.