Informe de auditoría de las pruebas de seguridad

Certificación de verificación de seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM. ORG

ID del informe		**Fecha**	
Auditor principal		**Prueba Fecha Duración**	
Ámbito e índice		**Vectores**	
		Tipo de prueba	
Canales			

Soy responsable de la información contenida en este informe y he verificado personalmente que toda la información contenida en el mismo es factual y verdadera.

FIRMAEMPRESA SELLO/SELLO

Certificación OPST		**Certificación OPSA**	

VALORES DE SEGURIDAD OPERATIVA

Visibilidad	
Acceso	
Confianza	

LIMITACIONES

abilidad a **la continuidad**	
Debilidad	
Preocupación	
Exposición	
Anomalía	

VALORES DE CONTROL

Autenticación	
Indemnización	
Resiliencia	
Subyugación	
VALORESVulner	
No repudio	
Confidencialidad	
Privacidad	
Integridad	
Alarma	

OpSec		**Controles reales**	
Limitaciones		**Seguridad Δ**	

Protección real		**Seguridad real**	

VISIÓN GENERAL
Este Manual de Metodología de Pruebas de Seguridad de Código Abierto proporciona una metodología para realizar una prueba de seguridad exhaustiva. Una prueba de seguridad es una medición precisa de la seguridad a nivel operativo, sin suposiciones ni pruebas anecdóticas. Una metodología adecuada permite realizar mediciones de seguridad válidas, coherentes y repetibles.

ACERCA DE ISECOM
ISECOM, creador y encargado del mantenimiento del OSSTMM, es una organización independiente de investigación en seguridad sin ánimo de lucro y una autoridad de certificación definida por los principios de colaboración abierta y transparencia.

TÉRMINOS Y DEFINICIONES RELACIONADOS
Este informe puede hacer referencia a palabras y términos que pueden interpretarse con otras intenciones o significados. Esto es especialmente cierto en las traducciones internacionales. Este informe intenta utilizar términos y definiciones estándar como los que se encuentran en el vocabulario OSSTMM 3, que se ha basado en NCSC-TG-004 (Teal Green Book) del Departamento de Defensa de EE.UU. cuando procede.

PROPÓSITO
El propósito principal de este Informe de Auditoría es proporcionar un esquema de informe estándar basado en una metodología científica para la caracterización precisa de la seguridad a través del examen y la correlación de una manera coherente y fiable. El propósito secundario es proporcionar directrices que, una vez seguidas, permitan al auditor proporcionar una auditoría OSSTMM certificada.

PROCESO
Este Informe de Auditoría debe acompañar al documento completo del informe de la prueba de seguridad que proporciona pruebas de la prueba y de los resultados según lo definido en la declaración de trabajo entre la organización de pruebas y el cliente.

VALIDEZ
Para que este Informe de Auditoría OSSTMM sea válido, debe cumplimentarse de forma clara, correcta y completa. El Informe de Auditoría OSSTMM debe estar firmado por el probador o analista principal o responsable y acompañarse del sello de la empresa titular del contrato o subcontrato de la prueba. Este informe de auditoría debe mostrar en ESTADO DE REALIZACIÓN qué Canal y los Módulos y Tareas asociados han sido probados hasta su finalización, no probados hasta su finalización, y qué pruebas no eran aplicables y por qué. Un informe que documente que sólo se han completado partes específicas de la prueba del Canal debido a limitaciones de tiempo, problemas del proyecto o rechazo del cliente puede seguir siendo reconocido como una auditoría oficial de la OSSTMM si va acompañado de este informe que muestre claramente las deficiencias y las razones de las mismas.

CERTIFICACIÓN
La certificación OSSTMM es la garantía de la seguridad de una organización según las pruebas exhaustivas de la norma OSSTMM y está disponible por vector y canal para las organizaciones o partes de organizaciones que mantengan un nivel de rav de un mínimo del 90% validado anualmente por un auditor externo independiente. La validación de las pruebas de seguridad o de las métricas trimestrales está sujeta a los requisitos de validación de ISECOM para garantizar la coherencia y la integridad.

1. REVISIÓN DE LA POSTURA

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
1.1	Objetivos empresariales y mercados identificados.		
1.2	Identificación de la legislación y la normativa aplicables a los objetivos del ámbito de aplicación.		
1.3	Políticas empresariales identificadas.		
1.4	Políticas de ética empresarial e industrial identificadas.		
1.5	Identificación de las culturas y normas de funcionamiento.		
1.6	Tiempos y flujos de operación identificados aplicables a los objetivos del ámbito de aplicación.		
1.7	Identificados todos los canales necesarios para este ámbito.		
1.8	Identificados todos los vectores para este ámbito.		

2. LOGÍSTICA

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
2.1	Medidas de seguridad aplicadas a las pruebas.		
2.2	Determinación y contabilización de las inestabilidades de las pruebas.		
2.3	Determinación y contabilización de los tiempos de inactividad en el ámbito de aplicación.		
2.4	Determinación y contabilización del ritmo de las pruebas en función del entorno de pruebas y de la presencia de seguridad.		

3. VERIFICACIÓN DE DETECCIÓN ACTIVA

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
3.1	Determinación y contabilización de las interferencias.		
3.2	Probado con interferencias activas e inactivas.		
3.3	Determinación de las restricciones impuestas a las pruebas.		
3.4	Reglas de detección verificadas y previsibilidad.		

4. AUDITORÍA DE VISIBILIDAD

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
4.1	Objetivos determinados a través de todas las tareas de enumeración.		
4.2	Determinación de nuevos objetivos mediante la investigación de objetivos conocidos.		

5. VERIFICACIÓN DE ACCESO

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
5.1	Interacciones verificadas con puntos de acceso a todos los objetivos del ámbito.		
5.2	Tipo de interacción determinado para todos los puntos de acceso.		
5.3	Fuente determinada de interacción definida como servicio o proceso.		
5.4	Profundidad de acceso verificada.		
5.5	Verificadas las limitaciones de seguridad conocidas de los puntos de acceso descubiertos.		
5.6	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de los puntos de acceso descubiertos.		

6. VERIFICACIÓN DE CONFIANZA

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
6.1	Interacciones determinadas que dependen de otras interacciones para completar la interacción de prueba según las tareas.		
6.2	Objetivos determinados con relaciones de confianza con otros objetivos del ámbito para completar las interacciones.		
6.3	Objetivos determinados con relaciones de confianza con otros objetivos fuera del ámbito para completar las interacciones.		
6.4	Verificadas las limitaciones de seguridad conocidas de los fideicomisos descubiertos entre los fideicomisos.		
6.5	Verificadas las limitaciones de seguridad conocidas de las confianzas descubiertas entre los objetivos del ámbito y las interacciones de confianza.		
6.6	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de las confianzas descubiertas.		

7. VERIFICACIÓN DE CONTROLES

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
7.1	Verificación del funcionamiento de los controles de no repudio de acuerdo con todas las tareas.		
7.2	Verificación del funcionamiento de los controles de confidencialidad en todas las tareas.		
7.3	Verificado los controles para el funcionamiento de Privacidad de acuerdo con todas las tareas.		
7.4	Verificación de los controles para el funcionamiento de la Integridad de acuerdo con todas las tareas.		
7.5	Verificación de los controles para el funcionamiento de la alarma de acuerdo con todas las tareas.		
7.6	Verificadas las limitaciones de seguridad conocidas de todos los controles de las categorías de clase B.		
7.7	Búsqueda de técnicas novedosas de elusión y limitaciones de seguridad de todos los controles de las categorías de clase B.		

8. VERIFICACIÓN DEL PROCESO

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
8.1	Determinados todos los procesos que controlan la acción de interactividad con cada acceso.		
8.2	Verificada la interacción opera dentro de los confines del proceso determinado.		
8.3	Verificado que la interacción funciona dentro de los límites de la política de seguridad para tales interacciones.		
8.4	Determinado el desfase entre las operaciones de las interacciones y los requisitos de la postura a partir de la Revisión de la postura.		
8.5	Verificadas las limitaciones de seguridad conocidas de los procesos descubiertos.		
8.6	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de los procesos descubiertos.		

9. VERIFICACIÓN DE LA CONFIGURACIÓN Y LA FORMACIÓN

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
9.1	Requisitos de configuración/formación verificados según la postura en la Revisión de la postura.		
9.2	Verificación de la aplicación de los mecanismos de seguridad adecuados definidos en la Revisión de Postura.		

9.3	Verificado la funcionalidad y las limitaciones de seguridad dentro de las configuraciones/formación para los objetivos en el ámbito de aplicación.		
9.4	Búsqueda de técnicas novedosas de elusión y limitaciones de seguridad en las configuraciones/formación.		

10. VALIDACIÓN DE LA PROPIEDAD

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
10.1	Determinación de la cantidad y el tipo de propiedad intelectual sin licencia distribuida dentro del ámbito de aplicación.		
10.2	Verificar la cantidad y el tipo de propiedad intelectual sin licencia disponible para la venta/comercio con el vendedor originada dentro del ámbito.		

11. REVISIÓN DE LA SEGREGACIÓN

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
11.1	Determinación de la cantidad y ubicación de la información privada definida en la Revisión de Postura disponible a través de los objetivos.		
11.2	Determinado el tipo de información privada según la definición de la Revisión de Postura disponible dentro del ámbito.		
11.3	Verificado la relación entre la información de acceso público fuera del objetivo que detalla la información privada o confidencial definida en la Revisión de Postura y el alcance.		
11.4	Verificación de la accesibilidad de los accesos públicos dentro del objetivo para las personas con discapacidad.		

12. VERIFICACIÓN DE LA EXPOSICIÓN

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
12.1	Búsqueda de objetivos disponibles a través de fuentes públicas ajenas al ámbito de aplicación.		
12.2	Búsqueda de activos organizativos disponibles, tal y como se definen en la Revisión de Postura, a través de fuentes disponibles públicamente fuera del ámbito.		
12.3	Determina el acceso, la visibilidad, la confianza y controla la información disponible públicamente dentro de los objetivos.		
12.4	Determinado un perfil de la infraestructura de canales de la organización para todos los canales probados a través de la información disponible públicamente dentro de los objetivos.		
12.5	Determinado un perfil de la infraestructura de canales de la organización para todos los canales probados a través de la información disponible públicamente fuera del alcance.		

13. INTELIGENCIA COMPETITIVA SCOUTING

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
13.1	Determinado el entorno empresarial de socios, proveedores, trabajadores y mercado a través de la información pública disponible sobre los objetivos dentro del ámbito de aplicación.		
13.2	Determinado el entorno empresarial de socios, vendedores, distribuidores, proveedores, trabajadores y mercado a través de información pública disponible fuera del ámbito.		
13.3	Determinado el entorno de la organización a través de la información pública disponible sobre los objetivos dentro del ámbito.		
13.4	Determinado el entorno organizativo a través de información pública disponible fuera del ámbito.		

14. VERIFICACIÓN DE LA CUARENTENA

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
14.1	Métodos de cuarentena verificados para las interacciones con los objetivos del ámbito.		
14.2	Métodos de cuarentena verificados para las interacciones de los objetivos con otros objetivos fuera del ámbito.		
14.3	Duración verificada de la cuarentena.		
14.4	Proceso de cuarentena verificado desde la recepción hasta la liberación.		
14.5	Verificadas las limitaciones de seguridad conocidas de las cuarentenas descubiertas.		
14.6	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de las cuarentenas descubiertas.		

15. AUDITORÍA DE PRIVILEGIOS

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
15.1	Verificado el medio de obtener legítimamente privilegios para todas las interacciones autenticadas.		
15.2	Verificado el uso de identificación fraudulenta para obtener privilegios.		
15.3	Verificado el medio de eludir los requisitos de autenticación.		
15.4	Verificado el medio de tomar privilegios de autenticación no pública.		
15.5	Verificado el medio secuestrando otros privilegios de autenticación.		
15.6	Verificadas las limitaciones de seguridad conocidas de los mecanismos de autenticación descubiertos para escalar privilegios.		
15.7	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de los mecanismos de autenticación descubiertos para escalar privilegios.		
15.8	Profundidad determinada de todos los privilegios de autenticación descubiertos.		
15.9	Determinada la reutilización de todos los privilegios de autenticación descubiertos en los mecanismos de autenticación de todos los objetivos.		
15.10	Requisitos verificados para obtener privilegios de autenticación de prácticas discriminatorias según la Revisión de Postura.		
15.11	Medios verificados para obtener privilegios de autentificación de prácticas discriminatorias para las personas con discapacidad.		

16. VALIDACIÓN DE LA CAPACIDAD DE SUPERVIVENCIA Y CONTINUIDAD DEL SERVICIO

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
16.1	Determinación de las medidas aplicables para interrumpir o detener la continuidad del servicio hacia y desde los objetivos.		
16.2	Procesos de continuidad verificados y mecanismos de seguridad activos para los objetivos.		
16.3	Verificación de las limitaciones de seguridad conocidas de los procesos y mecanismos de seguridad y continuidad del servicio descubiertos.		
16.4	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de los procesos y mecanismos de seguridad y continuidad del servicio descubiertos.		

17. ENCUESTA FINAL, ALERTA Y REVISIÓN DE REGISTROS

	TAREA	COMENTARIOS	ESTADO DE FINALIZACIÓN
17.1	Métodos verificados para registrar y alertar de las interacciones con los objetivos del ámbito.		
17.2	Métodos verificados para registrar y alertar de las interacciones de los objetivos con otros objetivos fuera del ámbito.		
17.3	Verificada la velocidad de grabación y alerta.		
17.4	Verificada la persistencia del registro y la alerta.		
17.5	Verificación de la integridad del registro y de las alertas.		
17.6	Verificado el proceso de distribución de registros y alertas.		
17.7	Verificadas las limitaciones de seguridad conocidas de los métodos de grabación y alerta descubiertos.		
17.8	Búsqueda de nuevas técnicas de elusión y limitaciones de seguridad de los métodos de grabación y alerta descubiertos.		