

# Professional Security Tester - OPST



## OSSTMM PROFESSIONAL SECURITY TESTER CERTIFICATION (OPST)

**Orientado a:** Todos aquellos profesionales con conocimientos básicos de seguridad y que quieran aportar a su trabajo una completa metodología en la realización de pruebas de seguridad.

### **Requisitos:**

- Conocimiento de lenguajes de programación de preferencia Perl, C y Java.
- Conocimiento de Shell Scripting, PHP, ASP, Javascript, HTML y HTMLS.
- Conocimiento en sistemas operativos UNIX (LINUX), Windows.
- Conocimiento en protocolos de comunicaciones.
- Conocimiento de Equipos de Comunicaciones como ruteadores, firewalls y switches o hubs.
- Conocimiento de Bases de Datos My SQL, MS SQL Server y otras.
- Conocimiento en Técnicas de Cifrado.
- Conocimiento del Idioma Inglés (Técnico) y facilidad para el trabajo en equipo.

### **Beneficios:**

Realizar prácticas y laboratorios con herramientas clave en las pruebas de seguridad.  
Disponer de una metodología para realizar pruebas completas de seguridad.



# Professional Security Tester - OPST

## Estructura del Curso y Material

El curso se compone de:

40 horas de formación intensiva por profesionales de la seguridad

4 horas de examen para obtener el Certificado en OPST (último día) con posibilidad de extensión al día sábado.

Libros oficiales de OSSTMM

**Profesor:** Instructor certificado como “Trainer” y en OPST por ISECOM

(<http://www.isecom.org>),

**Contenido:** El curso se inicia con un repaso de los conceptos fundamentales de Linux, protocolos y los diferentes perfiles de seguridad. Se divide en tres partes: Seguridad de la Información Corporativa, Prueba Práctica de Seguridad, y Prueba Agresiva de Seguridad.

**La Seguridad de la Información Corporativa** es la parte donde se reciben los conocimientos necesarios de seguridad corporativa que prueban e incorporan el secreto del cliente, evaluación del riesgo, pruebas legales, fundamentos éticos, informes, los procesos de prueba y normas del contrato, todo comprendido en las llamadas “Reglas de Compromiso”.



# Professional Security Tester - OPST

**La Prueba Práctica de Seguridad** está conformada por los conceptos y conocimientos imprescindibles para la realización de pruebas de seguridad basándonos en OSSTMM, que nos permite proporcionar evaluaciones y conclusiones.

En el módulo de **Prueba Agresiva de Seguridad**, el alumno evalúa el trasfondo técnico de los términos y necesidades para proporcionar una prueba OSSTMM certificada.

El contenido del curso se divide en:

- Entender el trasfondo de la prueba de seguridad.
- Entender porqué una prueba de seguridad no es sólo hacer hacking.
- Entender qué es el OSSTMM y lo que se consigue.
- Desarrollar un servidor del ataque en Linux y Windows.
- Instalación de las herramientas de prueba en el servidor del ataque.
- Encontrar y usar los recursos que los evaluadores profesionales de seguridad utilizan para encontrar las nuevas herramientas de prueba y hacking.
- Visualizar y entender paquetes de Internet, protocolos y servicios.
- Entender la presencia de la seguridad.
- Partes implicadas en un asesoramiento.
- Saber realizar un asesoramiento.



# Professional Security Tester - OPST

- Entender cómo trabaja OSSTMM.
- Entender las tareas del área de la seguridad de la información según la OSSTMM.
- Saber cómo construir un equipo de seguridad.
- Entender las reglas del contrato de ventas y comercialización iniciales a través del workshop final.
- Saber completar una prueba de seguridad básica.
- Saber cómo completar una prueba de seguridad avanzado que incluya un firewall remoto, ruteador, y prueba de un IDS.
- Entender las tareas en el área de la seguridad de comunicaciones según OSSTMM.
- Entender las tareas en el área de la seguridad física según OSSTMM.
- Entender las tareas en el área de la seguridad Wireless según OSSTMM.
- Entender las tareas en el área de la seguridad de los procesos de según OSSTMM.
- Entender cómo concluir los servicios de las diferentes pruebas de seguridad como Denegación de Servicio (DoS), prueba de verificación, prueba de aplicación, ingeniería social, VPN, ruteadores, firewall, IDS y pruebas periódicas.

