

# OSSTMM Professional Security Tester Accredited Certification ( OPST )

Certificazione: OPST | Durata: 5 Giorni | Corso: in sede o dal cliente

## DESCRIZIONE DEL CORSO

OPST è un corso intensivo della durata di cinque giorni e permette ai partecipanti di sviluppare le competenze teoriche e pratiche necessarie per effettuare test di sicurezza seguendo le metodologie OSSTMM 3 ( Open Source Security Testing Methodology Manual ). Durante questo corso, i partecipanti acquisiranno le conoscenze e le competenze necessarie per pianificare ed effettuare professionalmente test di sicurezza interni ed esterni basandosi sulle metodologie OSSTMM3.

## SESSIONE D'ESAME

L'esame richiede complessivamente 140 risposte entro 4 ore e il punteggio minimo è del 60% ( con punteggi superiori al 90% è previsto il marchio di eccellenza ).Lo scopo è quello di dimostrare l'efficacia e l'accuratezza del testing e delle metodologie apprese durante il corso. Ogni domanda è formulata in risposta multipla.

L'esame è open book e non è possibile comunicare con gli altri studenti. L'esame combina domande e risposte su carta e online, da compilare una volta eseguiti i test basati sul laboratorio appositamente creato all'interno di una DMZ, e alla quale è possibile accedere da remoto attraverso Internet una volta registrati.

## A CHI SI RIVOLGE

Il corso si rivolge in particolare, ma non solo, a:

- Security Auditors
- Network Engineers
- Amministratori di sistema e di rete
- Sviluppatori, Network Architects, Security Analysts e ogni altra figura professionale in ambito IT

## PREREQUISITI

E' raccomandata la conoscenza e l'utilizzo di base dei sistemi operativi \*nix, delle operazioni da terminale, del funzionamento dei protocolli di rete e il funzionamento dei programmi e dei servizi di sistema.

Si raccomanda inoltre la conoscenza dell'OSSTMM3 Manual.

# OSSTMM Professional Security Tester Accredited Certification ( OPST )

Certificazione: OPST | Durata: 5 Giorni | Corso: in sede o dal cliente

## AGENDA

	GIORNO 1 Introduzione all'OSSTMM	GIORNO 2 4 Point Process	GIORNO 3 4 Point Process	GIORNO 4 Esecuzione del test	GIORNO 5 Esame	
09:00	Registrazione	Modulo 1: Induction	Modulo 3: Interaction	Preparazione e configurazione dei tools	Preparazione all'esame	
09:30	Introduzione ad ISECOM					
10:00	Introduzione all' OSSTMM Open source security testing methodology manual	Posture review, logistics	Process, verification, configuration verification, property validation	Port Scanning, system detection, services identification	Riepilogo, esecuzione di test e Q&A	
10:30	Terminologia e metodologia del manuale open source					
11:00	Break					
11:30	OSSTMM testing channels ( data networks, telecommunications, physical, human e spectrum )	Active Detection Verification	Segregation review, exposure verification, competitive intelligence scouting			
12:00					Registrazione all'esame	
12:30						
13:00	Pranzo					
14:00	Introduzione all'OPST	Modulo 2: Inquest	Modulo 4: Intervention		Esame	
14:30	Definizione di un test di sicurezza, legalità e codice di condotta	Visibility audit, access verification	Quarantine verification, privileges audit			
15:00	Break					
15:30	Metodologia di Testing					
16:00	Gestione degli errori					
16:30	Moduli di security testing, 4 Point Process	Trust verification, control verification	Survivability validation, alert and log review			
17:00						
17:30	Tools [Esercitazioni]	Tools [Esercitazioni]	Tools [Esercitazioni]	Tools [Esercitazioni]	Chiusura	

## MATERIALE DIDATTICO

Ad ogni partecipante al corso sarà fornito il seguente materiale didattico:

- Accesso ai laboratori di test da remoto
- Manuale di studio dello studente