



mediaservice.net
CORPORATE SECURITY & IMAGE

OPST

OSSTMM PROFESSIONAL SECURITY TESTER

TECHNICAL CERTIFICATION

*DOCUMENTO INFORMATIVO PER LA
CERTIFICAZIONE PROFESSIONALE
E LA VERIFICA DEI PREREQUISITI NECESSARI*

“The hacker mind and the professional methodology”



INDICE

DESCRIZIONE DEL PERCORSO FORMATIVO PER LA CERTIFICAZIONE ISECOM OPST	3
PROGRAMMA DEL CORSO DI CERTIFICAZIONE ISECOM OPST	5
PREREQUISITI PER LA CERTIFICAZIONE OPST	6
TARGET AUDIENCE	7
I VANTAGGI RISPETTO AD ALTRI CORSI DI FORMAZIONE E CERTIFICAZIONE IN SICUREZZA INFORMATICA	8
OBIETTIVI DELLA CERTIFICAZIONE OPST	9
PRICING	10
PER ULTERIORI INFORMAZIONI	11

DESCRIZIONE DEL PERCORSO FORMATIVO PER LA CERTIFICAZIONE ISECOM OPST

OSSTMM Professional Security Tester (OPST) è la certificazione professionale ufficiale per l'esecuzione di test di sicurezza conformi alla metodologia **OSSTMM** (Open Source Security Testing Methodology Manual) dell'**ISECOM** (Institute for Security and Open Methodologies, USA – <http://www.isecom.org/>).



L'OSSTMM fornisce una **metodologia completa** per l'esecuzione di Security Testing, diretti sia verso la parte esterna al perimetro aziendale, sia verso la parte interna: questa metodologia è nel contempo adatta anche all'esecuzione di test di sicurezza dalla rete interna all'area DMZ aziendale e viceversa, prendendo in considerazione le **sei** diverse aree della Corporate Security proprie dell'OSSTMM, denominate **Moduli Operativi**.

Lo scopo del corso di certificazione **OPST** (OSSTMM Professional Security Tester) è di promuovere l'acquisizione della conoscenza necessaria affinché il partecipante possa essere considerato un esperto nello svolgimento di test di sicurezza: capace, pieno di risorse ed autosufficiente.

Il corso di formazione è focalizzato all'acquisizione delle capacità tecniche necessarie per l'esecuzione di security testing e delle capacità di business **utili e necessarie** a fornire motivazioni, efficienza e comprensione verso le attuali richieste provenienti dal mercato IT.

Il corso permette, inoltre, di vivere e cercare di recepire l'esperienza maturata negli anni e la conoscenza diretta di un professionista della sicurezza, il quale si propone come guida nel processo intrapreso.

Secondo le direttive di ISECOM e nelle intenzioni della @ Mediaservice.net, la partecipazione al corso non deve avere come unico fine il superamento dell'esame e dunque il raggiungimento della certificazione OPST: questa, da sola, porterà un valore aggiunto minore al discente certificato ed alla comunità di sicurezza internazionale laddove non si sia riusciti - parallelamente al conseguimento della certificazione stessa - nell'obiettivo di formare una risorsa con una **forte etica**, indirizzata al miglior espletamento delle proprie competenze ed esperienze professionali.

La Certificazione OPST è rivolta ad utenti dotati di un **buon grado di conoscenza** in materia di reti e di sicurezza.

Il corso prevede la conoscenza degli elementi di amministrazione di base della piattaforma Linux, dei protocolli di rete e delle tecniche di security testing; si propone inoltre di portare il partecipante alla comprensione delle risposte utili al superamento del test d'esame relativo ai sei moduli operativi previsti dall'**OSSTMM (Physical Security, Communications Security, Wireless Security, Information Security, Internet Security e Process Security)**.

Gli studenti apprenderanno l'utilizzo di numerosi strumenti per l'esecuzione di test di sicurezza (**Security Testing ed Evaluation**): tali strumenti sono gratuitamente reperibili su Internet all'indirizzo http://osstmm.mediaservice.net/sec_tools.html.

Si tratta dunque di un corso di certificazione professionale che si prefigge di trasferire le capacità necessarie a diventare **esperti di test pratici di sicurezza** e ad essere pronti ad un ingresso nel mondo del lavoro – o all'apporto di know-how tecnico-operativo specifico nella propria attuale professione - immediatamente successivo al conseguimento della certificazione: fornendo alle aziende **valore aggiunto e professionalità** concreti.

Si tratta di un grande patrimonio di informazioni per tutte quelle persone che lavorano nell'ambito della sicurezza e nel settore delle reti, oltre che di un "hardening" delle capacità di coloro che desiderano confrontarsi con la realtà – pratica – della rete, delle rule of engagement, del calcolo dei RAV, della gestione del processo aziendale di sicurezza proattiva.

Una delle caratteristiche principali è l'acquisizione di esperienza professionale sulla capacità di valutare, pianificare e realizzare un progetto di Security Testing: l'intenzione è di fare degli allievi dei veri professionisti della sicurezza, capaci di eseguire un progetto dalla sua **definizione iniziale** alla **stesura della reportistica conclusiva**, utilizzando per raggiungere questo risultato le necessarie ore di laboratorio previste dal corso OPST.

Questo è quanto necessario per superare l'esame di certificazione ed essere pronti ad acquisire **esperienza diretta sul campo**, elemento fondamentale – a nostro avviso – per la corretta crescita della figura di ogni professionista della sicurezza informatica.

Concludiamo questa descrizione del percorso formativo e di certificazione riportando alcuni "quote", ovverosia commenti pubblici rilasciati da partecipanti a sessioni di certificazione OPST.

"ISECOM's OPST training course is first rate and goes well beyond theory by providing extensive hands on practice. Based on the OSSTMM it ensures every candidate has a clear understanding of the professional, ethical, business and technical issues involved in carrying out a thorough security test. I would highly recommend this course for all security and network security professionals who want to understand and further develop your security and penetration testing skill set."

Tom O'Connor, an employee of a US Bank.

"The OPSA is probably the first certification test that I have taken that I thought had any value. I liked the fact that I had to do something that tested my applied knowledge during the test, instead of my ability to discern dirty testing tricks, memorize test questions, or simply waltz through with test-taking ability."

Colby Clark, Security Analyst.

"I enjoyed the instructors' elaborations and real-world correlations to class lectures and labs. Overall, this is a fantastic course!"

*R.M., US Marine Corps,
CND Company, Red Team.*

"Il corso di certificazione OPST consente ai partecipanti di misurare e confrontare la propria esperienza sul campo con un modello - quale la metodologia OSSTMM - che rappresenta una efficace formalizzazione di tutte le attività che devono essere condotte durante un processo di analisi di sicurezza su infrastrutture ICT.

Il risultato del corso che ho seguito è stato una stimolante sequenza di attività mentali, operative e di consuntivazione, che garantiscono ai partecipanti una esperienza formativa tale da diventare un vero professionista del "Professional Security Testing", effettivamente rivolto a fornire affidabilità e ripetibilità nei risultati, garantendo la percezione di fiducia e gli standard metodologici ai clienti fruitori della prestazione di analisi delle vulnerabilità."

*Liberio Marconi,
IT Consulting & Certification Authority Dept.
Trustitalia SpA, VERISIGN Italian Affiliate.*

PROGRAMMA DEL CORSO DI CERTIFICAZIONE ISECOM OPST

Il corso si svolge nell'arco di **cinque giornate** di tipo "intensive", comprensive dell'esame finale di certificazione il quale si terrà il pomeriggio del **quinto giorno** ed avrà una durata di **quattro ore**. L'esame consiste nell'applicazione, teorica e pratica, di quanto appreso durante il corso.

E' possibile riassumere le giornate formative in **tre componenti principali**, tutte basati sulla versione più recente di OSSTMM e sulla documentazione internazionale presente nel settore dell'esecuzione di test di sicurezza a livello professionale: **Business Information Security**, **Practical Security Testing** ed **Aggressive Security Testing**.

- ü **Business Information Security** è il modulo formativo che riguarda le necessità relative all'attività in materia di test di sicurezza ed ingloba argomenti quali la riservatezza delle informazioni, la valutazione dei rischi, le testing legalities, le etiche professionali, il reporting, il processo di test e le regole d'impiego;
- ü **Practical Security Testing** è il modulo di formazione tecnica per la definizione dei termini e delle necessità per i test di sicurezza, basato sull'ultima versione dell'OSSTMM per l'esecuzione di assessment e di stime;
- ü **Aggressive Security Testing** è la technical baseline avanzata per la definizione dei termini e delle necessità per l'esecuzione di un test di sicurezza, completo e **certificato** OSSTMM per quanto concerne le sezioni Information Security ed Internet Security.

PREREQUISITI PER LA CERTIFICAZIONE OPST

Data la natura **particolarmente strutturata** del corso ed il forte impegno necessario per il superamento dell'esame finale, il candidato alla Certificazione Professionale OPST deve **obbligatoriamente** rispettare i seguenti requisiti:

- ü buona conoscenza della suite **TCP/IP** e dei suoi **principali protocolli**;
- ü esperienza nell'amministrazione base dei sistemi ***NIX** e **Microsoft Windows**;
- ü dimestichezza nell'installazione e nella configurazione di **software di verifica ed analisi della sicurezza** (specificatamente su distribuzioni *NIX); dei sopraccitati software è richiesta, inoltre, un'esperienza di base nell'utilizzo;
- ü conoscenza e comprensione delle **architetture di rete**;
- ü conoscenza base dei **principali servizi TCP/IP** (HTTP, FTP, TELNET, SSH) **nell'ottica dello svolgimento di analisi di sicurezza**;
- ü conoscenza base dei **sistemi per la sicurezza in rete**: *router, firewall, intrusion detection system*;
- ü conoscenza delle **dinamiche di attacco a sistemi informativi**.

Sono inoltre richieste:

- ü buona conoscenza della lingua inglese e delle terminologie tecniche;
- ü conoscenza del Manuale OSSTMM 2.0;
- ü esperienza lavorativa o di ricerca pari ad almeno un anno nel settore della ICT Security.

Per ogni allievo e per tutta la durata del corso è infine necessaria la **disponibilità di un notebook** (dotato di scheda di rete *Ethernet 10/100 Mbit/s*), sul quale siano già stati installati due Sistemi Operativi a "dual boot":

- ü **Microsoft** (*OS Microsoft 2000/XP*)
- ü **Linux** (*Slackware, Red Hat, Mandrake, Suse*) o ***BSD** (*OpenBSD, FreeBSD, NetBSD*) a scelta del discente.

N.B. E' importante che sul computer portatile di ogni partecipante siano presenti ambedue le due tipologie di sistemi operativi, gestibili anche con **emulatori O.S.** (*wmware, wine, etc.*)

TARGET AUDIENCE

I seguenti profili professionali sono stati individuati in qualità di "Suggested Target Audience" da ISECOM ed @ Mediaservice.net:

- ü Amministratori di Sistema
- ü Amministratori di Rete
- ü Responsabili Sicurezza Informatica
- ü Security Staff di NOC e SOC
- ü Security Tester
- ü Security Auditor
- ü ISO/BSI Lead Auditor
- ü Security Consultant
- ü Tutti coloro che lavorano professionalmente nel campo della System & Network Security

I VANTAGGI RISPETTO AD ALTRI CORSI DI FORMAZIONE E CERTIFICAZIONE IN SICUREZZA INFORMATICA

1. **Comprovata e diretta esperienza**

I corsi tradizionali sono spesso basati sull'esperienza di singole persone o aziende. Questo corso di certificazione professionale è invece basato sulla metodologia OSSTMM, la quale incorpora il know-how di più di 150 esperti internazionali.

2. **Riconoscimento internazionale**

La metodologia OSSTMM si è imposta come riferimento internazionale tra i *security expert* di autorità, università ed aziende del settore: è oggi utilizzata dai security-tester più rinomati come guideline efficace e standard per le verifiche di sicurezza proattiva.

3. **Metodologia comprensiva**

Il corso non è focalizzato verso l'insegnamento di **come** utilizzare i singoli strumenti software, ma fornisce invece una metodologia generale per l'esecuzione di Security Testing "from the outside to the inside".

4. **Informazioni aggiuntive**

Il corso di formazione non insegna solo gli aspetti tecnici toccati in un Security Testing, ma affronta anche gli aspetti legali, etici e le ottiche di business della *proactive security*.

5. **Esame internazionalmente riconosciuto**

Al termine del corso i partecipanti dovranno sostenere l'esame finale, il quale è indipendente dall'insegnante ed è certificato dall'ISECOM e dall'Università La Salle di Barcellona.



OBIETTIVI DELLA CERTIFICAZIONE OPST

- q Durante il Security Training i partecipanti verranno affrontati i seguenti argomenti:
 - ü Comprendere in che cosa consiste la professione di *Security Tester*
 - ü Comprendere perché i test di sicurezza non sono solo "*hacking*"
 - ü Comprendere che cosa è l'**OSSTMM** e che cosa si propone di trasmettere
 - ü Sviluppare server di attacco su piattaforme **Linux** e **Windows**
 - ü Installare e configurare **software di verifica ed analisi della sicurezza sulle attack box**
 - ü Individuare e sfruttare le risorse di cui si servono i professionisti dei test di sicurezza per aggiornarsi sui nuovi strumenti disponibili
 - ü Visualizzare e comprendere la struttura dei pacchetti TCP/IP, dei principali protocolli e dei servizi
 - ü Comprendere il concetto di "*security presence*"
 - ü Comprendere e saper valutare i fattori critici e le implicazioni di un **security testing**
 - ü Essere **in grado di eseguire** un security testing
 - ü Sapere come eseguire in maniera completa un test di sicurezza di base
 - ü Sapere come eseguire in maniera completa un'analisi di sicurezza avanzata che comprenda i test di firewall, di router e di sistemi xIDS

- q Al termine del corso il partecipante sarà inoltre in grado di eseguire e portare a termine con accuratezza le varie tipologie di test di sicurezza illustrate dal manuale **OSSTMM**, quali:
 - ü test di DoS (*Denial of Service testing*)
 - ü test di verifica delle vulnerabilità (*Verification testing*)
 - ü test di verifica della sicurezza delle applicazioni (*Application testing*)
 - ü test di ingegneria sociale (*Social Engineering*)
 - ü test di verifica delle connessioni VPN (*VPN testing*), dei Router, dei Firewall e degli IDS (*Router, Firewall, IDS testing*)
 - ü test di sicurezza periodici (*Periodic testing*)

- q Infine, lo studente avrà compreso le logiche e le basi operative e procedurali dell'**OSSTMM** (ultima release disponibile) e sarà quindi in grado di:
 - ü Comprendere come utilizzare nello svolgimento delle attività di analisi della sicurezza la metodologia **OSSTMM**
 - ü Comprendere le finalità della sezione "**IT Security**" del manuale **OSSTMM**
 - ü Comprendere le finalità della sezione "**Communications Security**" del manuale **OSSTMM**
 - ü Comprendere le finalità della sezione "**Physical Security**" del manuale **OSSTMM**
 - ü Comprendere le finalità della sezione "**Wireless Security**" del manuale **OSSTMM**
 - ü Comprendere le finalità della sezione "**Information Security**" del manuale **OSSTMM**
 - ü Comprendere le finalità della sezione "**Process Security**" del manuale **OSSTMM**
 - ü Essere in grado di gestire le "**Rules of Engagement**" così come descritte nel manuale **OSSTMM**

PRICING

Certification	Class	Description
OPST	Module #1	Practical Security Testing Course
OPST	Module #2	Aggressive Security Testing Course
OPST	Module #3	Business Information Security Course

Standard Price, final certification exam excluded	€ 3.000,00 + VAT
Standard Price, final certification exam included	€ 3.450,00 + VAT
Sconto Forze Armate e Forze dell'Ordine**	sconto 15%
Sconto Soci CLUSIT**	sconto 10%
Sconto Soci ISACA**	sconto 10%
Early Bird Registration*	sconto 5%

OPST Certification Exam Only, without class (private students) € 450,00

* Lo sconto Early Bird è cumulativo con le altre voci di sconto.

** Gli sconti per associazioni e L.E.A. (Law Enforcement Agency) non sono cumulabili.

Note

- q I costi indicati sono espressi in Euro, si intendono IVA esclusa e per singolo studente.
- q Il pagamento è da intendersi anticipato all'atto di conferma iscrizione al corso.
- q Tutti i corsi sono condotti nella massima qualità ed eseguiti **esclusivamente** da trainer autorizzati e direttamente formati presso la sede europea di ISECOM (Barcellona).
- q La frequentazione del corso è obbligatoria per tutta la durata dello stesso.
- q E' possibile sostenere il solo esame di certificazione (privatista); consigliamo tale scelta a quei partecipanti con un **forte know-how** di sicurezza informatica, penetration testing e dell'OSSTMM stesso.
- q Il corso include:
 - ü Aula corsi attrezzata;
 - ü Connettività dedicata per tutta la durata del corso;;
 - ü Workbook OPST;
 - ü Dispense utili allo svolgimento del corso;
 - ü Accesso all'ISECOM Test Network (ITN Online Sessions) per tutta la durata del corso e per la sessione di esame di certificazione;
 - ü Rilascio dell'Attestato di Certificazione in caso di superamento dell'esame finale;
 - ü Tutti gli Attestati di Certificazione sono rilasciati da ISECOM e dall'Università La Salle di Barcellona;
 - ü La certificazione riporterà un livello finale di punteggio, in funzione del numero di risposte esatte rispetto alle 140 domande dell'esame finale e basato sulle seguenti classificazioni:

Ø	A+	=	0 risposte errate
Ø	A	=	da 1 a 14 risposte errate
Ø	B	=	da 15 a 28 risposte errate
Ø	C	=	da 29 a 42 risposte errate
Ø	D	=	da 43 a 56 risposte errate
 - ü Qualora in numero di risposte errate sia pari o superiore a **57**, il candidato non avrà superato l'esame di certificazione OPST: in questo caso potrà risostenere l'esame di certificazione usufruendo di una forte scontistica sulla tassa d'esame.

PER ULTERIORI INFORMAZIONI:



Web: <http://www.mediaservice.net>
<http://osstmm.mediaservice.net>
Mail: info@mediaservice.net
Uffici: Via San Bernardino, 17
10141 - Torino (Italia)



Web: <http://www.isecom.org>
<http://www.osstmm.org>
Mail: training@osstmm.org
Tel: +39 011 3272100
Fax: +39 011 3246497

You can **play** with **hacker** tools
and techniques...
or you can do your job.
STOP talking security and **START** doing it.

www.isecom.org