

MOCA 2004
Metro Olografix Camp
20-22 Agosto 2004, Pescara



OSSTMM

METHODOLOGY & PROFESSIONAL CERTIFICATION PROGRAMS



OSSTMM	PROFESSIONAL SECURITY TESTER	(OPST)
OSSTMM	PROFESSIONAL SECURITY AUDITOR	(OPSA)
OSSTMM	PROFESSIONAL SECURITY EXPERT	(OPSE)



Raoul Chiesa, C.T.O. Divisione Sicurezza Dati

ISECOM Director of Communications

OSSTMM Professional Security Trainer

@ Mediaservice.net Srl - Divisione Sicurezza Dati
OSSTMM Authorized Regional Training Partner

COPYRIGHT

Questo insieme di slides è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste slides è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.



ISECOM

INDICE

I - LA METODOLOGIA

- Open Source Security Testing Methodology Manual
- Compliance
- Legislazioni
- Best Practices
- Best Practices & Intelligence Areas



ISECOM

II - TRAININGS E CERTIFICAZIONI PROFESSIONALI

- OSSTMM Professional Security Tester (OPST)
"the hacker mind and the professional methodology"
- OSSTMM Professional Security Analyst (OPSA)
"professional business security analysis and consultancy from the international security standard"
- OSSTMM Professional Security Expert (OPSE)
- Riferimenti

OSSTMM: A WorldWide Security Standard



ISECOM



“The quality of a security test can be externally validated by the customer as meeting or exceeding the OSSTMM, and thereby providing a defacto level of service guarantee the security professional can quote.

Also, the OSSTMM may be used for training, by identifying skills or methods that must be honed in preparation for security testing. And lastly, the OSSTMM may be used during a security test itself as a manual and guide for success.



The OSSTMM strives to be the security professional's "goto" tool with regard to security testing methodology, and the OSSTMM contributors have vowed they will succeed in this endeavor.”

**Don Bailey, senior security tester from the Mitre Corporation,
US Government supplier**

Il Relatore



Raoul Chiesa

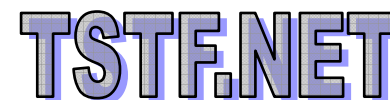
Founder & CTO, @ **Mediaservice.net**
Divisione Sicurezza Dati/DSD-LAB

Steering Committee, **CLUSIT**
Italian Association for the Computer Security

Board of Director's Member, **ISECOM**
Institute for Security and Open Methodologies, USA

Authorized International Trainer, **ISECOM**
OPST & OPSA Official Certification Programs

Southern Europe Reference Member, **T.S.T.F.**
Telecom Security Task Force, USA, EU, ASIA



L'azienda

- Un team indipendente di professionisti della sicurezza IT
- +10 anni di esperienza nel penetration testing e security consulting di alto livello
- Specializzati nelle telco e nel settore delle telecomunicazioni
- Ricercatori ed Auditor indipendenti
- Ci piacciono le “missioni impossibili” e le problematiche di sicurezza “hard-to-solve”



ISECOM

Clients Portfolio (estratto)



ISECOM

Arma dei Carabinieri (ROS Roma), Ospedale S. Giovanni Battista di Torino (Ospedale delle Molinette), Banca Mediocredito Friuli Venezia Giulia, Bo*frost SpA, Bulgari SpA, CNR di Milano (Security Task Force) Telecom Italia SpA (Italia ed Estero), Editorial Group “L’Espresso” (La Repubblica, Kataweb, Radio DJ, etc..), ITC/ILO - International Training Center of the ILO (ONU), Mirato SpA (marchi Malizia, Clinians, Intesa – settore farmaceutico/chimico), NoiCom SpA, Pirelli SpA – Corporate Security Department, TIM SpA, Vodafone Omnitel SpA, University of Udine, University of Milano (DSI), UNICRI – United Nations Interregional Crime and Justice Research Institute (ONU), Zyxel Telecommunications Inc. (TAIWAN), Watchguard Technologies Inc. (USA).



ISECOM

OSSTMM: LA METODOLOGIA

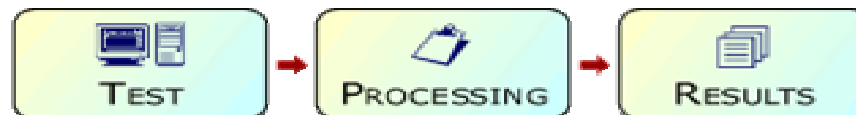
OSSTMM

OPEN SOURCE SECURITY TESTING

METHODOLOGY MANUAL

Metodologia internazionale per l'esecuzione di test di sicurezza sviluppata dall'ISECOM (**Institute for Security and Open Methodologies**, USA): ripetibile, confrontabile e quantificabile (RAVs)

- Definisce un insieme di regole e linee guide, oltre ai RAVs (valore tecnico del rischio)
- Non chiama in causa l'analisi dei risultati, ma il processo che li crea:



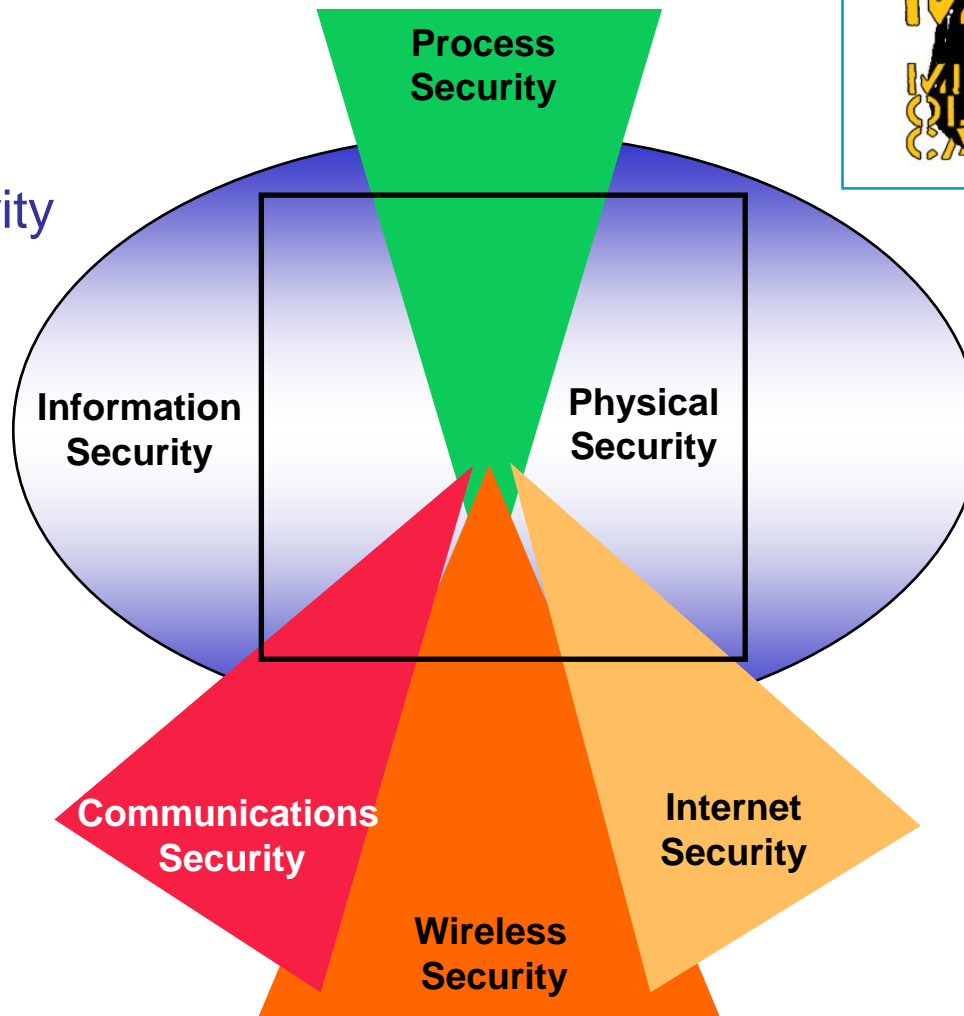
- Progetto open source, +150 contributors, libero utilizzo
- Applicabile ad apparati, infrastrutture, singoli target
- Cross-standard: IP, xSTN, X.25, mobile
- Adottato da organizzazioni governative e private in tutto il mondo
- Logicità Modulare: 6 aree operative (modules)



ISECOM

OSSTMM: AREE OPERATIVE

- Internet Security
- Information Security
- Physical Security
- Communications Security
- Wireless Security
- Process Security



ISECOM

OSSTMM: AREE OPERATIVE



ISECOM

INTERNET SECURITY

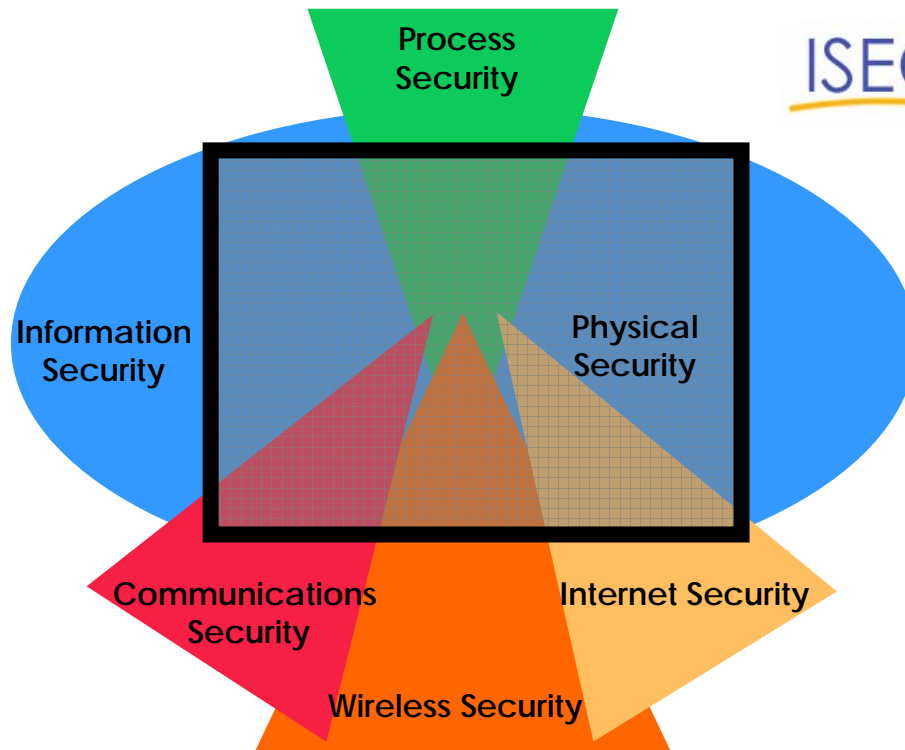
- Network Surveying
- Port Scanning
- Services Identification
- System Identification
- Vulnerability Research and Verification
- Internet Application Testing
- Router Testing
- Trusted Systems Testing
- Firewall Testing
- Intrusion Detection System Testing
- Containment Measures Testing
- Password Cracking
- Denial of Service Testing

INFORMATION SECURITY

- Competitive Intelligence Scouting
- Privacy Review
- Document Grinding

PROCESS SECURITY

- Request Testing
- Guided Suggestion Testing
- Trusted Persons Testing



OSSTMM: AREE OPERATIVE



ISECOM

WIRELESS SECURITY

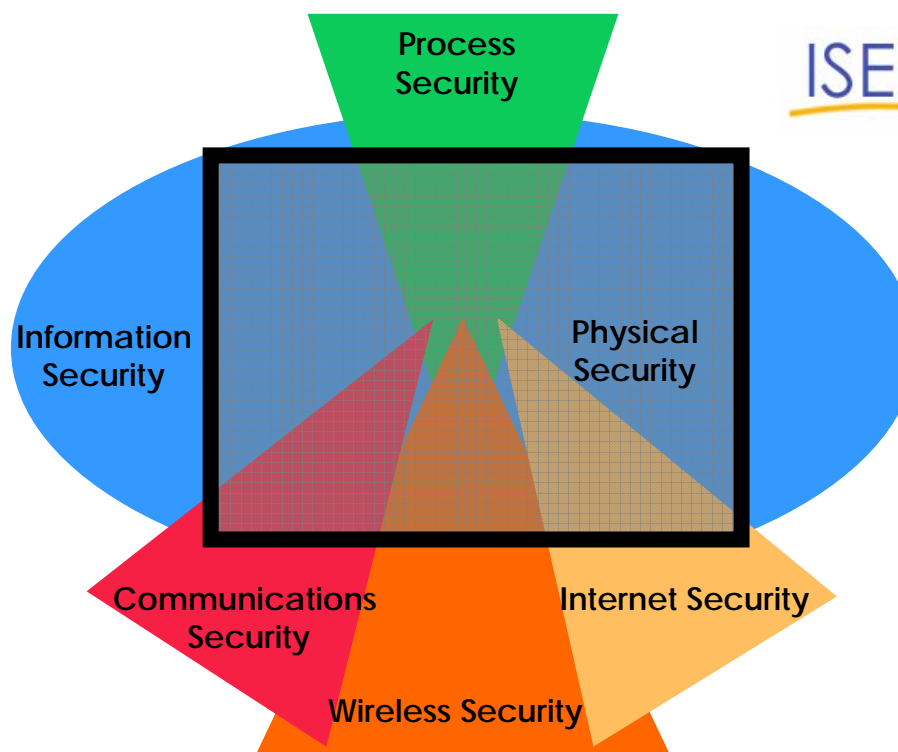
- Wireless Networks Testing
- Cordless Communications Testing
- Privacy Review
- Infrared Systems Testing

COMMUNICATIONS SECURITY

- PBX Testing
- Voicemail Testing
- FAX review
- Modem Testing

PHYSICAL SECURITY

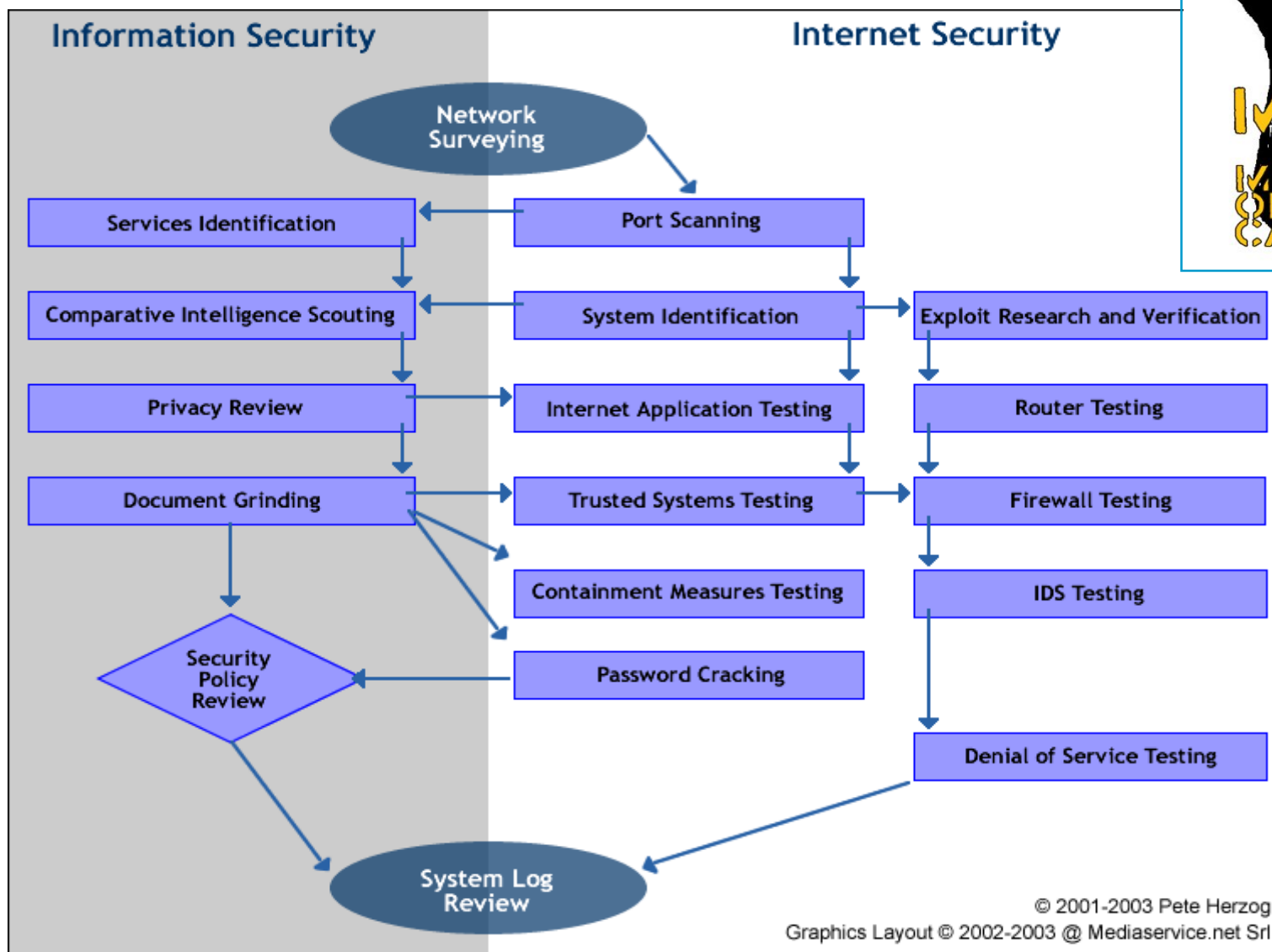
- Access Control Testings
- Perimeter Review
- Monitoring Review
- Alarm Response Review
- Location Review
- Environment Review



OSSTMM: AREE OPERATIVE



ISECOM



IMCOCIA

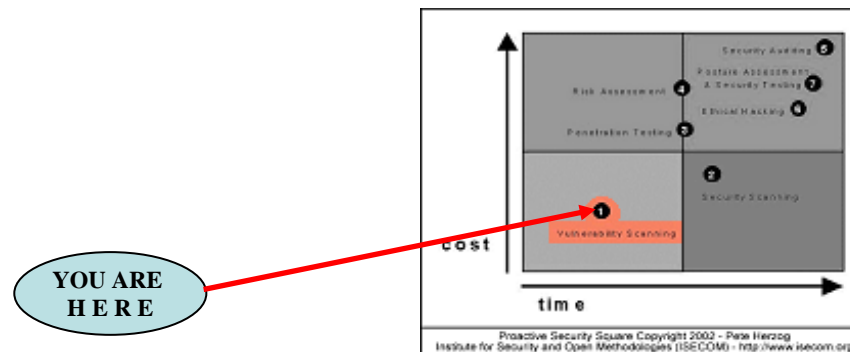
METRO

OLOGIA/AFIX

C/ALIP 2004

-
- The diagram illustrates the progression of security activities over time, organized into a 2x2 matrix. The vertical axis represents time, and the horizontal axis represents time. The activities are numbered 1 through 7, indicating a sequence of operations.
- | Activity | Color | Number |
|---------------------------------------|--------|--------|
| Vulnerability Scanning | Red | 1 |
| Security Scanning | Yellow | 2 |
| Penetration Testing | Blue | 3 |
| Risk Assessment | Blue | 4 |
| Ethical Hacking | Green | 6 |
| Security Auditing | Green | 5 |
| Posture Assessment & Security Testing | Green | 7 |

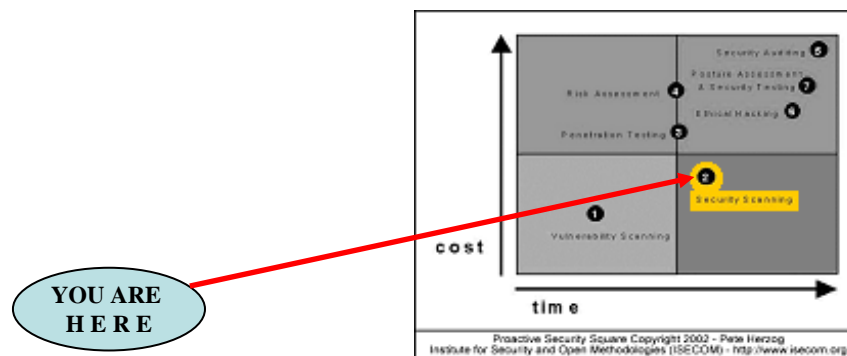
THE PROACTIVE SECURITY SQUARE (1/7)



(1) Vulnerability Assessment (Scanning) :

- Verifiche automatizzate
- Report in lingua inglese
- Alto numero di falsi positivi e negativi (falsi allarmi, falso “senso di sicurezza”)
- Si limita alla parte “IP”

THE PROACTIVE SECURITY SQUARE (2/7)

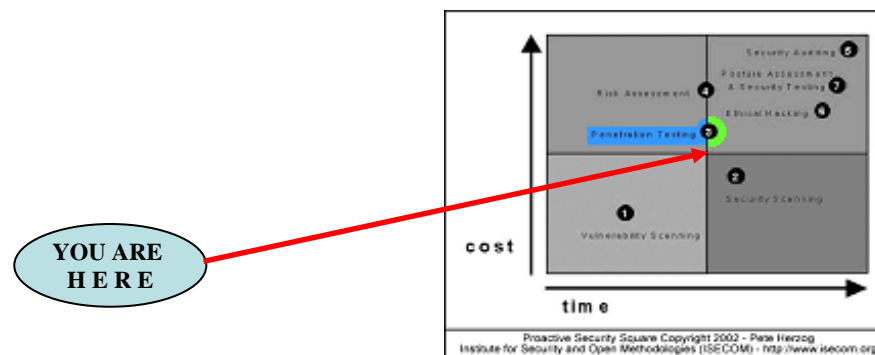


ISECOM

(2) Security Scanning:

- Scanning automatizzati; Verifiche manuali
- Report in lingua italiana o inglese
- Tuning manuale dei Falsi positivi e Negativi
- Si limita alla parte "IP"

THE PROACTIVE SECURITY SQUARE (3/7)



ISECOM

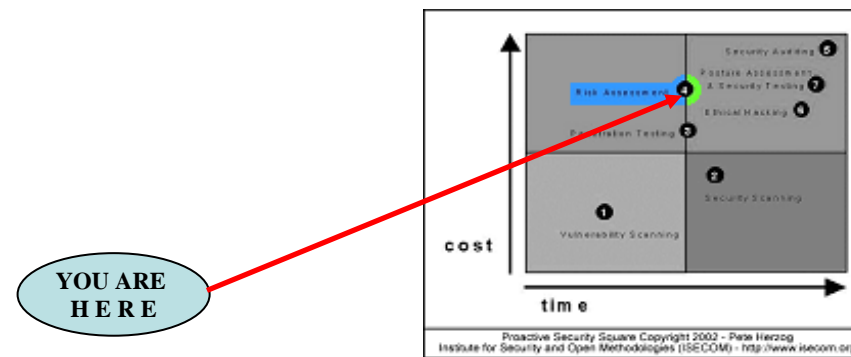
(3) Penetration Testing:

- Azioni di verifica eseguite manualmente secondo metodologie proprietarie (background personale del pentester o del team di attacco)
- Report redatto in lingua italiana dal Tiger Team
- Possibilità di abbinare opzioni quali Social Engineering, Trashing, Physical Intrusion, Web Applications Security Testing,
- Non si limita alla parte “IP” (RAS,X.25,DECnet,Wi-Fi,Web...)
- Aumenta il tempo di esecuzione su ogni singolo asset

THE PROACTIVE SECURITY SQUARE (4/7)



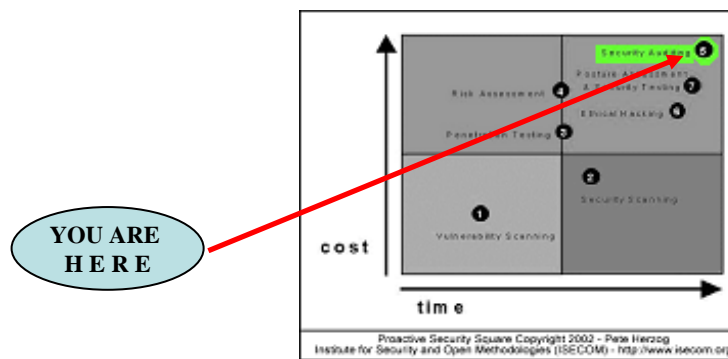
ISECOM



(4) Risk Assessment:

- Azioni di valutazione e correlazione tra i dati raccolti nelle operazioni di testing ed il valore aziendale del rischio
- I risultati possono essere generati dalle 3 precedenti metodologie di analisi tecnica del rischio
- Necessita di un lungo tempo di esecuzione
- Se i risultati dei test tecnici sono sfalsati, tutta l'analisi del rischio ne pagherà le conseguenze (e gli investimenti)

THE PROACTIVE SECURITY SQUARE (5/7)

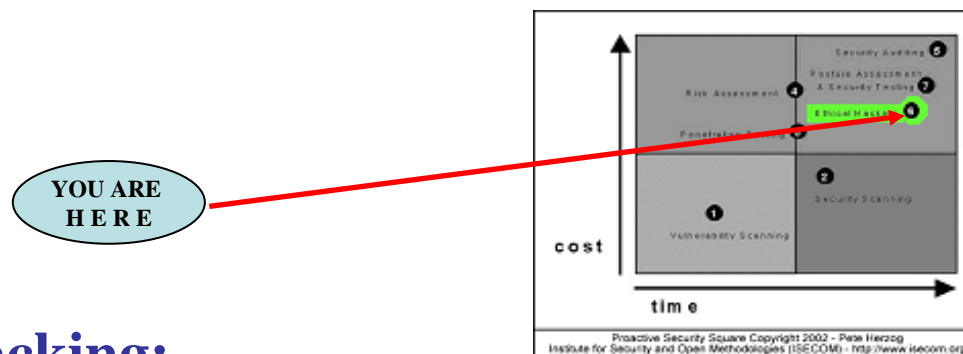


ISECOM

(5) Security Auditing:

- Azioni di Auditing - tipicamente interne – dell'intera infrastruttura informativa, analizzata dal punto di vista progettuale, procedurale ed implementativo
- Viene eseguito manualmente con personalizzazione del Report in base alle esigenze del Cliente e/o in considerazione di specifici asset e business aziendali
- Può essere il risultato di metodologie di sicurezza proattive, sposate con le metodologie standard di analisi del rischio

THE PROACTIVE SECURITY SQUARE (6/7)



ISECOM

(6) Ethical Hacking:

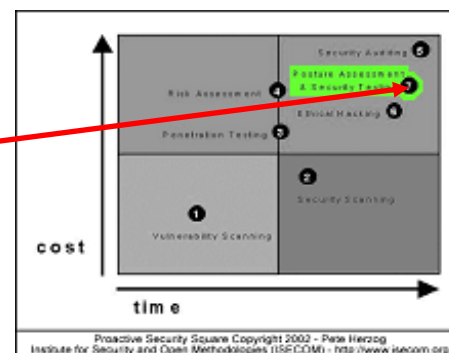
- Azioni di verifica a 360°, mirate verso asset, servizi o infrastrutture specifiche
- Richiede FULL OPERATING AUTHORIZATION + “Free to Jail” (per le verifiche al punto 3)
- Viene eseguito mediante azioni congiunte di
 1. Penetration Testing (IP, xSDN, X.25/X.121, SAT, Wi-Fi, Web Applications, ...)
 2. Phreaking
 3. **Social Engineering, Physical Intrusion, Trashing**
 4. Reverse Engineering
 5. Black Box Testing

THE PROACTIVE SECURITY SQUARE (7/7)



ISECOM

YOU ARE
HERE



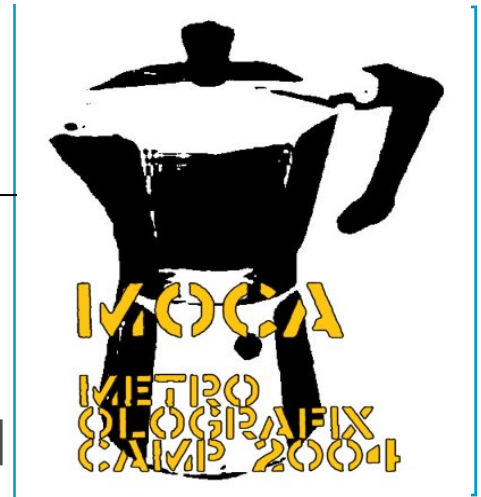
(7) Posture Assessment & Security Testing:

- Azioni ripetute di verifica e confronto (follow-up) eseguite in un arco temporale predefinito con il Cliente
- Le analisi si basano su fattori conoscitivi iniziali (espressi nei Piani di Rientro scaturiti da precedenti azioni di testing) e sono eseguite secondo la metodologia OSSTMM, ripetibile e quantificabile (RAVs)
- Il Report è redatto manualmente in lingua italiana dal Tiger Team e rispetta le guidelines standard (legislative e best practice) internazionali quali ISO/BSI, GAO, FISCAM
- Il Security Report finale è certificato OSSTMM



COMPLIANCE

- La metodologia OSSTMM è stata sviluppata nel pieno rispetto di diverse normative e standard internazionali riguardanti la protezione dei dati personali e l'information security in operazioni di security testing e risk assessment.



ISECOM

- I test che vengono eseguiti con la metodologia OSSTMM forniscono le informazioni necessarie ad analizzare le problematiche di data privacy nel rispetto delle attuali legislazioni e delle best practices - governative ed aziendali - maggiormente riconosciute.

COMPLIANCE: LEGISLAZIONI (1/2)



ISECOM

UNITED STATES OF AMERICA (USA)

- **USA Government Information Security Reform Act of 2000**
Section 3534(a)(1)(A)
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA).**
- **OCR HIPAA Privacy TA 164.502E.001, Business Associates**
[45 CFR §§ 160.103, 164.502(e), 164.514(e)]
- **OCR HIPAA Privacy TA 164.514E.001, Health-Related Communications and Marketing**
[45 CFR §§ 164.501, 164.514(e)]
- **OCR HIPAA Privacy TA 164.502B.001, Minimum Necessary**
[45 CFR §§ 164.502(b), 164.514(d)]
- **OCR HIPAA Privacy TA 164.501.002, Payment** [45 CFR 164.501]

GERMANY

- **Deutsche Bundesdatenschutzgesetz (BDSG)**
Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes
from 20. December 1990, BGBl. I S. 2954, 2955, zuletzt geändert durch das Gesetz zur
Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994,
BGBl. I S. 2325.

SPAIN

- **Spanish LOPD - Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal**
Art.15 LOPD -. Art. 5.

COMPLIANCE: LEGISLAZIONI (2/2)



ISECOM

CANADA

- Provincial Law of Quebec, Canada Act Respecting the Protection of Personal Information in the Private Sector (1993).

UNITED KINGDOM (UK)

- UK Data Protection Act 1998

AUSTRALIA

- Privacy Act Amendments of Australia

Act No. 119 of 1988 as amended, prepared on 2 August 2001 incorporating amendments up to Act No. 55 of 2001. The Privacy Act 1988 (Cth) (the Privacy Act) seeks to balance individual privacy with the public interest in law enforcement and regulatory objectives of government.

- National Privacy Principle (NPP) 6

provides that an individual with a right of access to information held about them by an organisation.

- National Privacy Principle (NPP) 4.1

provides that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

ITALY

In corso di validazione.

COMPLIANCE: BEST PRACTICES (1/2)



ISECOM

- **ISO 17799/2000 (BSI 7799)**

Full Compliance con tutti i requisiti di remote auditing e testing del BS7799 (ed il suo equivalente internazionale ISO 17799) per gli information security testing.

- **GAO and FISCAM**

Compliance con le attività di controllo del **US General Accounting Office's** () e del **Federal Information System Control Audit Manual** () laddove inerenti la sicurezza di rete (network security).

- **CASPR**

Full Compliance con le best practices e guidelines definite dai membri del **Commonly Accepted Security Practices and Recommendations** () e riguardanti il controllo dei documenti ed il peer review (Security Testing in Internet Security).

- **OWASP**

Full Compliance con le direttive dell'**Open Web Application Security Project** (), sezioni Remote Security Testing e Web Applications Auditing.

COMPLIANCE: BEST PRACTICES (2/2)



• SCIP

OSSTMM include tecniche di “intelligence gathering” verso il mercato/business di tipo offensivo e difensivo, definite come Competitive Intelligence e riconosciute dal **Society of Competitive Intelligence Professionals** (); viene inoltre introdotta la tecnica conosciuta come “Scouting”, al fine di confrontare il posizionamento market/business dell’organizzazione target dal punto di vista di altri intelligence professionals sulla rete Internet.



• SET

Compliance con i remote auditing test previsti del **Secure Electronic Transaction™** ()
Compliance Testing Policies and Procedures v4.1, 22 Febbraio 2000.

• NIST

OSSTMM è risultato “compliance through methodology” nei remote security testing ed auditing previsti dalle seguenti pubblicazioni del **National Institute of Standards and Technology** () :

- ♦ **An Introduction to Computer Security: the NIST Handbook**, 800-12;
- ♦ **Guidelines on Firewalls and Firewall Policy**, 800-41;
- ♦ **Information Technology Security Training Requirements a Role-and-Performance-Based Model**, 800-16;
- ♦ **DRAFT Guideline on Network Security Testing**, 800-42;
- ♦ **PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does**, 800-24;
- ♦ **Risk Management Guide for Information Technology Systems**, 800-30;
- ♦ **Intrusion Detection Systems**, 800-31.

COMPLIANCE: BEST PRACTICE & INTELLIGENCE AREAS



ISECOM

- **Breaking into computer networks from the Internet**, Roelof Temmingh, Sensepost (Pty) Ltd., South Africa
- **The MH DeskReference v1.2**, Rhino9 Team, USA
- **Security Reference Handbook 2001**, Symantec Corporation, USA
- **Auditing your Firewall Setup**, Lince Spitzner, Dec 2000, USA
- **Security of Information Technology**, NPG 2810.1, NASA Procedures and Guidelines, USA
- **The 10 Commandments of Counterintelligence**, James M. Olson, 2001, CIA's Center for the Study of Intelligence, USA
- **Studies of Intelligence**, Unclassified Edition, 2001, CIA's Center for the Study of Intelligence, USA
- **Security and Company Culture**, Michel G. McCourt, Workplace Violence Prevention Reporter, Dec 2001, USA

CARATTERISTICHE ESSENZIALI DEI TEST OSSTMM



- ☐ **Quantificabile:** definizione di una metrica di sicurezza (*RAV*)
- ☐ **Consistente e ripetibile:** stesse tipologie di risultati per diversi tester
- ☐ **Valido nel tempo:** non e' solo una "fotografia" della situazione scattata al tempo del test
- ☐ **Basato sull'abilita' del tester e non sui tool utilizzati:**
nessun legame a "brand" specifici
- ☐ **Completo**
- ☐ **Conforme alle leggi vigenti e al diritto di privacy**

ISECOM

OSSTMM “RULES OF ENGAGEMENT”

❑ Le Rules of Engagement sono una serie di **norme per la protezione** del Cliente e degli autori dei test


❑ **Coprono 9 aree operative:**

- ✓ Vendita e Marketing
- ✓ Attività di Assessment
- ✓ Negoziazioni e Contratti
- ✓ Obiettivi del test
- ✓ Pianificazione del test
- ✓ Notifica degli estremi del test al Cliente
- ✓ Fase di Testing
- ✓ Sviluppo e consegna Reportistica



ISECOM

OSSTMM Audit Report



Certified Open Source Security Testing Methodology Manual Audit Report

Report ID: _____

Auditor: _____

Date: _____

I am responsible for the information within this report and have personally verified that all information herein is true.

Signature: _____

Company Stamp

risk type	verified	identified	not applicable
Vulnerabilities			
Weaknesses			
Information Leaks			
Concerns			
Unknowns			
TOTAL			

Risk Assessment Value: _____

Degradation / 30 Days: _____

Next Test Cycle Date: _____

Internet Technology Security Test Modules

1. LOGISTICS AND CONTROLS

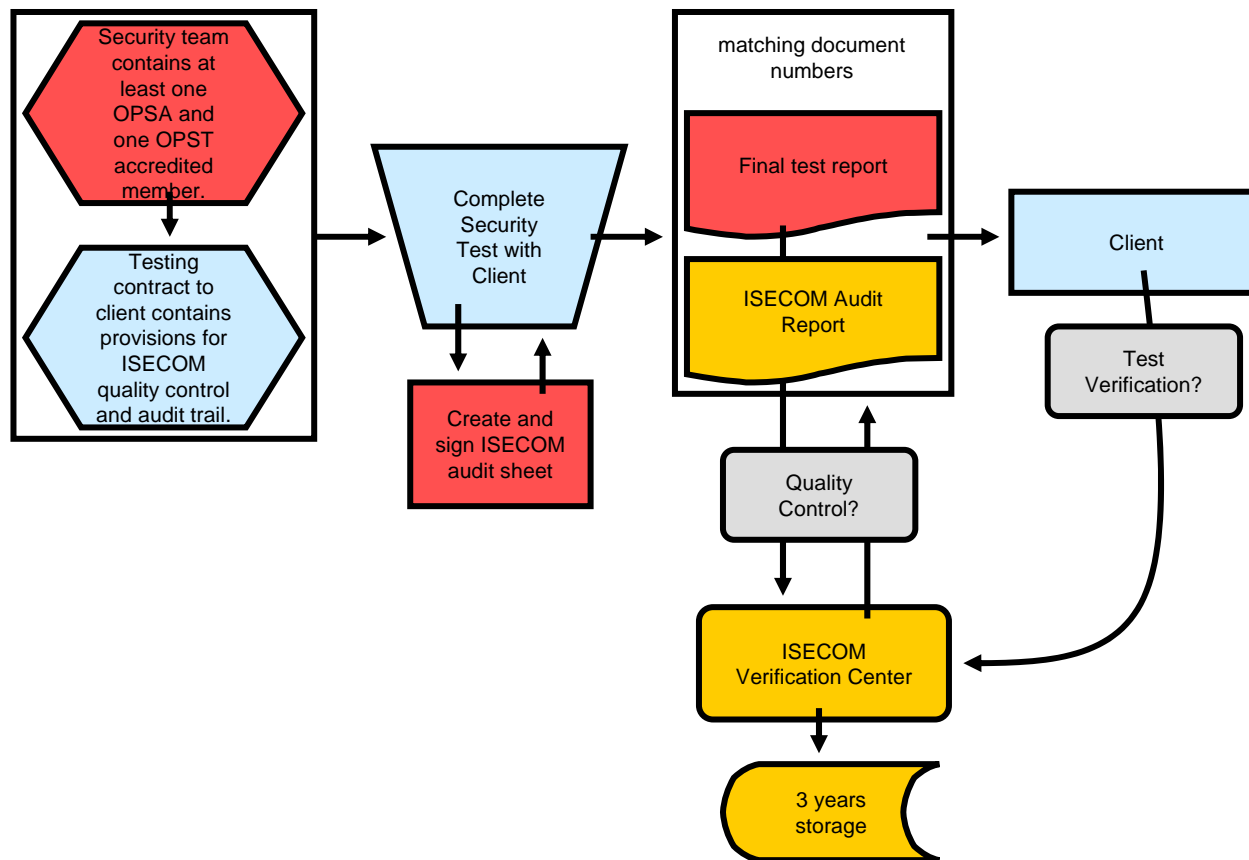
Test Module	Completed	Not Completed	Not Applicable	Comments



ISECOM

- Readable
- Accountable
- Countable
- Measurable
- Schedulable

OSSTMM Audit Report Process



- Credible
- Responsible
- Disclosable
- Storable
- Verifiable



ISECOM

Putting RAVs to Work

- Calculate Operational Risk
- Calculate Actual Risk
- Determine Acceptable Degradation Level
- Narrow in on one process or view the BIG PICTURE.



ISECOM



Foglio di Lavoro per il calcolo dei RAVs



			Verified	Identified			
		Vulnerability	0.0320	0.0160			
		Weakness	0.0160	0.0080			
		Concern	0.0080	0.0040			
		Exposure	0.0040	0.0020			
		Anomaly	0.0020	0.0010			
Visibility		3					
No Authorization		7					
Trusts		3					
Accesses		3					
Justified Risks %		0.00016000					
Base		99.99984000					
	verified	identified					
Vulns	6	8	0.32				
Weaknesses	1	1	0.02				
Concerns	0	0	0				
Exposures	3	4	0.02				
Anomalies	1	2	0				
			0.36800000				
Actual Risk	% attacks will be successful		0.36816000	0.00016000			
	cycles	1	99.63168059	99.99968000	0.36800000	0.00016000	0.36799941
		2	99.63152118	99.99952000	0.36800000	0.00016000	0.36799882
		3	99.63136177	99.99936000	0.36800000	0.00016000	0.36799823

ISECOM's PROFESSIONAL SECURITY CERTIFICATIONS: OPST, OPSA and OPSE Certification Programs



ISECOM



OSSTMM ABLE



OSSTMM Professional Security Analysts

- ☐ Can analyze test reports and sum up security weaknesses.
- ☐ Are walk-the-walk security personnel who are practical and resourceful.

OSSTMM Professional Security Tester

- ☐ Can perform OSSTMM tests and verify both positives and negatives.
- ☐ Are go-to security personnel who learn at a packet level where even expensive scanning tools can't go.



OSSTMM PROFESSIONAL SECURITY TESTER (OPST)

“the hacker mind and the professional methodology”

La Certificazione OPST e' la certificazione ufficiale per i test di sicurezza basati sull'Open Source Security Testing Methodology Manual.

L'obiettivo del percorso formativo - basato su tre moduli - è di fornire il trasferimento di know-how necessario per poter considerare la persona un abile security tester, capace di lavorare autonomamente.

I moduli si focalizzano sulle specifiche competenze tecniche necessarie al security testing professionale e sui business skills necessari per fornire motivazioni, efficienza e comprensione delle odierne necessità aziendali.

Il conseguimento della Certificazione OPST prevede il superamento di un esame di tipo “hands-on”, nel quale viene richiesto l'impiego delle competenze acquisite, individuando le vulnerabilità esistenti in un vero network remoto e fornendo i necessari piani di rientro alle problematiche riscontrate.

Il percorso di certificazione professionale è composto dai seguenti corsi di Security Training:

- **Practical Security Testing** è la *basic technical class* dove vengono definiti i punti e le problematiche nei security testing based, basandosi sull'ultima versione disponibile dell'OSSTMM, al fine di individuare i necessari assessments e fornire stime.
- **Aggressive Security Testing** è l'*advanced technical class* nella quale vengono affrontati i punti e definite le problematiche necessarie all'esecuzione di un security test completo ed OSSTMM-certified, ivi inclusi i testing verso assets quali firewall, IDS e router.
- **Business Information Security** è la *baseline information security class* per le problematiche di business in un security testing ed include argomenti quali la confidenzialità verso il cliente, il risk assessment, le autorizzazioni alle operazioni di verifica, l'etica, il reporting ed il processo di testing.

La durata totale del corso è di 60 ore, dopo le quali avviene l'esame per la certificazione della durata di 4 ore. Per l'ammissione all'esame finale è obbligatorio il completamento dei tre moduli, la cui frequenza è obbligatoria.



ISECOM

OPST's Feedbacks

"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."

Libero Marconi, Italy
IT Consulting & Certification Authority Dept.
Trustitalia SpA, VERISIGN Italian Affiliate

"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.



ISECOM

"This is the course that those of you who manage a professional services group wish that your consultants had. "

Erik Ohlson

OSSTMM PROFESSIONAL SECURITY ANALYST (OPSA)

“Professional business security analysis and consultancy from the international security standard”

La Certificazione OPSA e' la certificazione ufficiale per la security analysis basata sull'Open Source Security Testing Methodology Manual.

L'obiettivo del percorso formativo - basato su tre moduli - è di fornire il trasferimento di know-how necessario per poter considerare la persona un abile e capace Security Analyst e Test Manager.

I moduli si focalizzano sulle specifiche competenze analitiche e sulle capacità gestionali necessarie alla supervisione di security test OSSTMM-certified ed al loro completamento e posizionamento nel business aziendale.

Il conseguimento della Certificazione OPSA prevede il superamento di un unico esame, composto da una sessione teorica ed una sessione pratica, nel quale viene richiesto l'impiego delle competenze acquisite.

Il percorso di certificazione professionale è composto dai seguenti corsi di Security Training:

- **Security Analysis** è un modulo di tipo *knowledge transfer*, necessario per la comprensione di dati provenienti da diversi moduli OSSTMM e le loro modalità di applicazione verso le necessità aziendali.
- **Red Team Strategies** è il modulo che si focalizza sul Risk Assessment ed è progettato per portare il professionista a gestire un team di security tester dalle prime fasi di prevendita o preparazione sino al final reporting. Il corso analizza diverse strategie di redteam e blueteam per il raggiungimento dei risultati migliori, incluse strutture e modalità di attacco ed intrusione, sia dall'interno che dall'esterno.
- **Security Project Management** è l'ultimo corso per il conseguimento della certificazione OPSA, di tipo *knowledge transfer*, nel quale vengono trasferite ed illustrate esperienze dirette di progetti OSSTMM testing ed il loro environment. Il focus del modulo è il project management: time reporting, valutazioni e stime, team management, contratti, iterazione con il cliente, controllo sull'efficienza e controlli sui costi (inclusa la gestione del ROI attraverso le Risk Assessment Values di OSSTMM).

La durata totale del corso è di 60 ore, dopo le quali avviene l'esame per la certificazione della durata di 4 ore.

Per l'ammissione all'esame finale è obbligatorio il completamento dei tre moduli,



la cui frequenza è obbligatoria.



ISECOM

OPSA's Feedbacks

[...]

“Interessante e peculiare, poi, è la parte di programma che affronta gli aspetti legali ed etici e le ottiche di business della *proactive security*, completando il quadro di riferimento e fornendo la necessaria visione d'insieme ad un qualsiasi professionista della materia.

Il raggiungimento della certificazione passa dalla giusta combinazione di conoscenze tecniche e gestionali in materia di ICT security (pur non specifiche), ed un'esperienza lavorativa o di ricerca pari ad almeno tre anni nel settore (requisito, quest'ultimo, richiesto per l'accesso all'esame).

[...]

Si tratta, in sostanza, di una metodologia che si è imposta come riferimento internazionale tra i gli esperti di sicurezza in autorità, università ed aziende del settore e che è in corso di adozione da parte dei security-tester come linea guida per le verifiche di sicurezza proattiva (*security testing “from the outside to the inside”*), una metodologia che promette di divenire davvero uno dei “*need-to-know*” per i professionisti della sicurezza.

Sonia Valerio, Italy, GCFW, CISSP, OPSA

I also attended the OPSA course at Black Hat and found it a good use of my time and budget. After speaking with other Black Hat Training attendees during lunches, many of whom seemed unhappy with the other course offerings, I felt that I made a good choice at least with regards to that particular conference.

In general I felt it was more geared towards consultants than internal testers, and wish it would have been available a few years ago when I was consulting. This is the course that those of you who manage a professional services group wish that your consultants had. Very business oriented and complementary to technical skills, although technical enough for anyone inexperienced with pen-testing.

**From SecurityFocus.com,
Pentest archives, 06/08/2003**



ISECOM

"I am an OPSA now. Which I think is very cool. I really enjoyed the test. It 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, California, OPSA,
CISSP, CCSA, CCNP, CCNA,
MCSE, MCP+I, A+.**

OSSTMM PROFESSIONAL SECURITY Expert (OPSE)



- ☐ The OPSE certification is the official ISECOM's OSSTMM certification based on the Open Source Security Testing Methodology Manual.
- ☐ The OSSTMM provides a complete methodology on performing security testing from the outside to the inside.
- ☐ This certification determines your ability to comprehend the OSSTMM.

☐ To become accredited you need:

- Understand the testing concepts for all sections and modules in the newest version of the OSSTMM.
- Understand how to calculate project plans and man hours.
- Be able to calculate project time scheduling and man hours according to the OSSTMM Rules of Thumb.
- Be able to calculate Risk Assessment Values.
- Understand the Rules of Engagement.

ISECOM

OSSTMM PROFESSIONAL SECURITY Expert (OPSE)

- ❑ Unlike the OPST and OPSA, the OPSE is not an open book exam.
- ❑ The exam is 4 hours of 100 knowledge questions in 10 categories:

1. Professional
2. Project Planning
3. Process
4. Risk Assessment
5. Information Security Testing
6. Process Security Testing
7. Internet Technology Security Testing
8. Communications Security Testing
9. Wireless Security Testing
10. Physical Security Testing

- ❑ In a nutshell, the OPSE is for professionals with little networking and security experience. It is a fast track certification to prove one has a thorough knowledge of the OSSTMM, how it works, what it means, and why it is applied.

NB: The OPSE will be available in 2005 (1st Q).



ISECOM

ESAME E RILASCIO DEI CERTIFICATI (1/3)



ISECOM

ESAME

- ☐ Le sessioni di esame hanno una durata massima di 4 ore (5) per OPST, OPSA ed OPSE.
- ☐ Il Training Network dell'ISECOM (ITN) è configurato per essere operativo ed utilizzabile dagli studenti durante i corsi e nelle sessioni pratiche degli esami per la certificazione.

RILASCIO DEI CERTIFICATI

- ☐ I certificati possono essere di due tipi:
 - **Class Certificates** per la frequentazione di singoli corsi (Security Trainings) e
 - **Certificazioni Professionali** OPST, OPSA ed OPSE.
- ☐ I Class Certificates vengono rilasciati agli studenti che scelgono singoli e specifici percorsi formativi, ma ricordiamo come sia necessario seguire tutti i corsi che compogono un Percorso Formativo Professionale per poter sostenere l'esame di certificazione.
- ☐ Tutti gli attestati riportano l'intestazione e sono approvati dall'Università La Salle, istituzione riconosciuta a livello mondiale (cfr. <http://www.lasalle.org/Spanish/Apost/Links/linksalp.html>).
- ☐ Tutti i corsi sono condotti nella massima qualità ed esclusivamente da trainer autorizzati e direttamente formati dall'ISECOM e da Ideahmster Organization.

ESAME E RILASCIO DEI CERTIFICATI (2/3)



REGOLE DI COMPORTAMENTO

- ❑ L'obiettivo delle Certificazioni Professionali OSSTMM è di produrre professionisti e non solamente tecnici preparati.

E' compito dei Professional Security Trainer valutare e giudicare ogni studente sulla base della professionalità così come delle capacità tecniche.



- ❑ Durante lo svolgimento delle lezioni, i Trainer hanno l'obbligo di espellere dalla classe - senza alcun rimborso economico - i partecipanti che non mantengano un comportamento etico o che non utilizzino le proprie conoscenze tecniche in maniera professionale, ivi inclusi:

- testing, hacking o tentativi di hacking al di fuori dello scopo della formazione e del contesto delle sessioni pratiche di laboratorio, sia verso sistemi esterni che sistemi interni della @ Mediaservice.net (IT), ISECOM (USA) ed Università La Salle (ES);
- disturbo durante l'esame di certificazione;
- qualunque dimostrazione di maleducazione e mancanza di professionalità.

ESAME E RILASCIO DEI CERTIFICATI (3/3)



ISECOM



TARGET AUDIENCE

OSSTMM Professional Security Tester (OPST)

- System administrators; Network administrators; Security Managers
- NOC or SOC Security Staff; security personnel
- Penetration Testers
- People involved in network/system security as a professional

OSSTMM Professional Security Analyst (OPSA)

- Security Consultants
- Penetration Testers; Security Auditors; ISO/BSI Auditors
- Security Project Managers; Security R&D Managers; Chief Technical Officers
- Anyone involved in a company's security process

OSSTMM Professional Security Expert (OPSE)

- Project Managers
- R&D Managers
- Chief Information Officers; Chief Technical Officers
- Junior Security Consultants
- Privacy Reviewers



ISECOM

PREREQUISITI

OSSTMM Professional Security Tester (OPST)

- English language
- Base knowledge of TCP/IP
- Base knowledge of network topologies and technologies
- Base Experience with Unix and Windows NT based networks

OSSTMM Professional Security Analyst (OPSA)

- English language
- Advanced knowledge of TCP/IP
- Advanced knowledge of network topologies and technologies
- Advanced Experience with Unix and Windows NT based networks

OSSTMM Professional Security Expert (OPSE)

- English language
- Base knowledge of TCP/IP
- Base knowledge of network topologies and technologies



ISECOM

RIFERIMENTI



D.S.D.
DIVISIONE SICUREZZA DATI



OSSTMM Certification Programs:

- **OPST** Professional Security Tester
- **OPSA** Professional Security Analyst
- **OPSE** Professional Security Expert



Raoul Chiesa, Director of Communications, ISECOM

Mail Contacts

info@mediaservice.net
dsd@mediaservice.net

(General Enquiries)

(Security Enquiries)

Web Contacts

<http://osstmm.mediaservice.net/>
<http://www.isecom.org/>
<http://www.osstmm.org/>

