1° Luglio 2005

An introduction to the OSSTMM and ISECOM's Professional Certifications

ISECOM Institute for Security and Open Methodologies

Raoul Chiesa, C.T.O. @ Mediaservice.net (DSD)

ISECOM Director of Communications

OSSTMM Security Trainer (OPST, OPSA)

@ Mediaservice.net Srl – **D**ata **S**ecurity **D**epartment
ISECOM Italian Affiliate
Exclusively Authorized Regional Training Partner

The Speaker

Raoul Chiesa

✓ Founder & CTO, **@ Mediaservice.net**
Data Security Department/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

INDEX

I – *ISECOM*

- Who is who
- Our History
- The Projects
- Zoom: the OSSTMM

II – *PROFESSIONAL SECURITY CERTIFICATIONS*

- OPST
- OPSA
- Contacts
- Q&A

ISECOM

ISACA Roma

ISECOM: Who is Who

- Our Mission:
  - To provide global, practical, useable security knowledge and knowledge-tools to solve problems caused by insecurity, privacy violations, ethical violations, and poor safety measures.

- Our Audience:
  - Corporations and Organizations (Metrics)
  - Professionals and quasi-professionals (Rules of Engagement)
  - Universities and Colleges (Academic Alliance Program)
  - Teens and pre-teens (Hacker Highschool)

ISECOM: The History

- Established in January 2001 as the **Ideahamster Organization**.
- Dedicated to the development of standards and open methodologies.
- Uses an **open, peer-review** process.
- An **independent**, non-political, non-profit, third party.

ISECOM

ISACA Roma

ISECOM: The Founder

Pete Herzog

[pete@isecom.org]

- ✓ Managing Director of ISECOM
- ✓ Creator of the Open Source Security Testing Methodology Manual (OSSTMM)
- ✓ Creator of Hacker High School International
- ✓ Professor of Security Testing for the IT Security Masters Program at La Salle University
- ✓ Professor of Business Information Security for the MBA program at ESADE
- ✓ Security business advisor for GFT Iberia S.A.
- ✓ Security Testing Trainer for Intense School Inc.

Edit View Favorites Tools Help

Back Search Favorites Media

http://www.isecom.org/ Go Links

ISECOM

Institute for Security and Open Methodologies

PARTNERS: ACADEMIC | BUSINESS | TRAINING

www.osstmm.org / www.hackerhighschool.org

- NEWS & PRESS
- TRAINING SCHEDULE
- MAILING LISTS
- FORUM
- SPONSORS
- TEAM
- MEDIA KIT
- CONTACT
- LICENSE
- ABOUT US
- CERTIFICATION
- TRAINING PARTNERS
- GOLD/SILVER TEAM AREA
- THE INVISIBLE CATALOG

ISECOM GOLD TEAM

JOIN THE ISECOM GOLD TEAM!

Confirm the OSSTMM testing and report certification requirements

- PROJECTS
  - Security Testing
    - OSSTMM - Open Source Security Testing Methodology Manual
    - OSSTMM Shortcuts
    - Internal Security Testing
    - BSTA Workbook - Business Security Testing & Analysis Workbook
  - Application Security
    - SPSMM - Secure Programming Standards Methodology Manual
    - Theses
  - Security Tools
    - Operational
    - Development
  - Open Protocol Resource
  - Security Training
    - JACK - Jack of all Trades Security Testing Training Supplement
    - OPST - OSSTMM Professional Security Tester Certification
    - OPSA - OSSTMM Professional Security Analyst Certification
    - OPSS - OSSTMM Professional Security Series
    - Hacker High School
  - Incident Handling
    - SIPES - Security Incident Policy Enforcement System
  - Business Integrity Testing
  - Software Quality Testing
    - STICK - Software Testing Checklist

ISECOM SILVER TEAM ISECOM GOLD TEAM
UPDATES - PRE-RELEASES up to 6 months earlier
Join the ISECOM GOLD or SILVER TEAM
www.isecom.org/subscribe.htm

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

OSSTMM CERTIFICATIONS

"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.

"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

ISECOM: The Projects

- **OSSTMM** – Open Source Security Testing Methodology Manual
- **RAV**s – The Security Metrics
- **BIT** – Business Integrity Testing Methodology Manual
- **OPRP** – Open Protocol Resource Project
- **SIPES** – Security Incident Policy Enforcement System
- **SPSMM** – The Secure Programming Standards Methodology Manual
- **STICK** – Software Testing Checklist
- **ISM 3.0** – Information Security Maturity Model
- **HHS** – Hacker High School

ISECOM

ISECOM

ISACA Roma

ZOOM:
The OSSTMM Project

ISECOM

ISACA Roma

ISECOM: The OSSTMM

- Our chief project is the OSSTMM.
- The Open Source Security Testing Methodology Manual used by:
  - ✓ Worldwide Financial Institutions
  - ✓ the U.S. Department of Treasury for testing U.S. financial institutions
  - ✓ U.S. Navy and Air Force
  - ✓ MANY More companies than I can list here.
- The OSSTMM is a methodology for testing security systems for everything, from guards and locked doors to mobile communication towers and satellites.

ISECOM

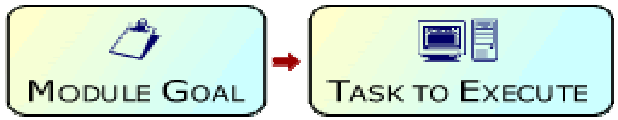
ISACA Roma

OSSTMM: OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

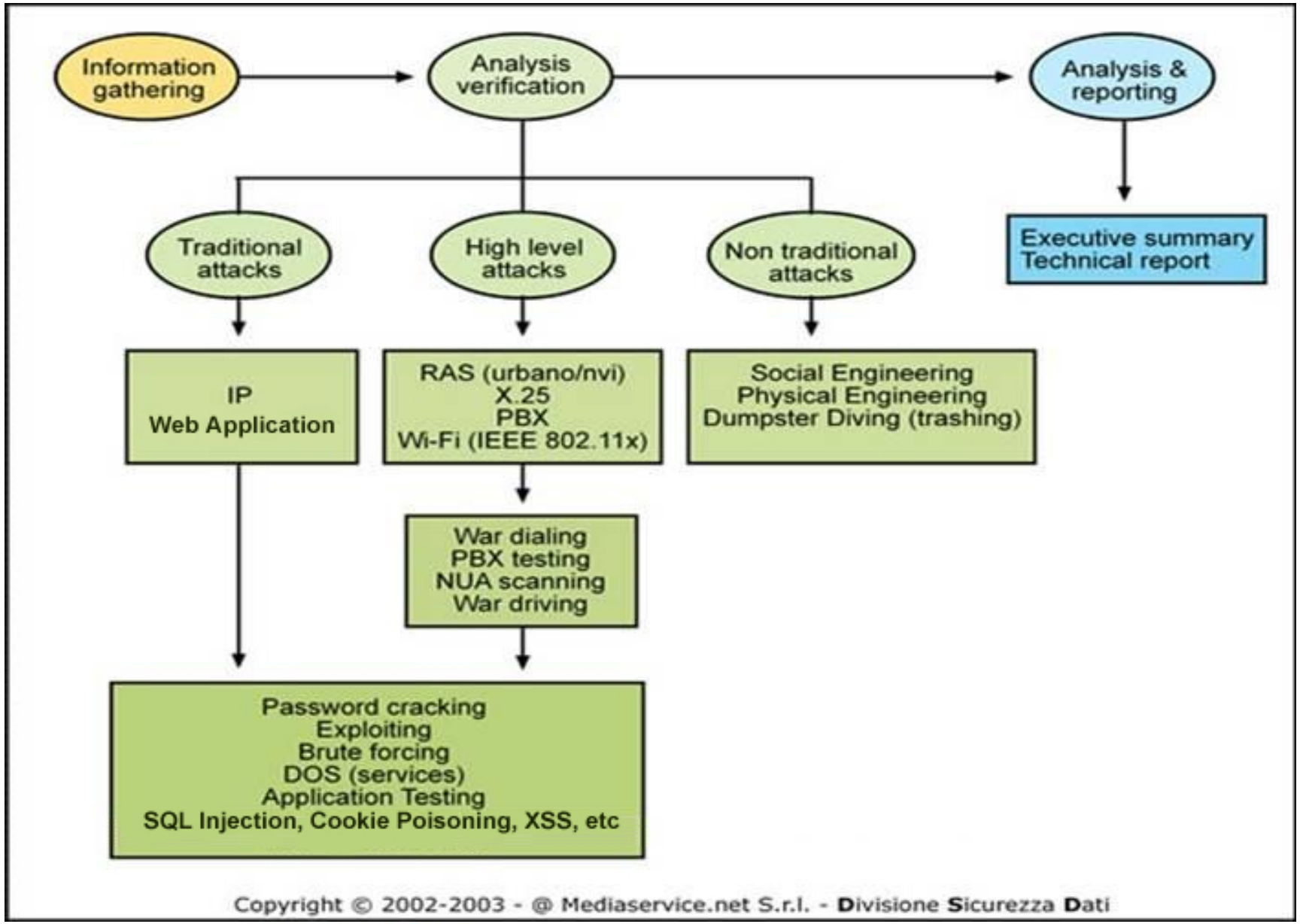
The OSSTMM is an international methodology focused on Proactive Security Testings, developed by ISECOM (**Institute for Security and Open Methodologies**, USA): the output can be repeated, compared and evaluated in a numerical manner (RAVs).

• the OSSTMM defines rules and guidelines, as well as the RAVs (technical risk level)
• the OSSTMM **doesn't substitute** the Risk Analysis field, but works on the process that creates its results:

• Open Source project, +150 contributors, free use of the methodology
• Works on apparals, infrastructures, single targets
• Cross-standard: IP, xSTN, X.25, mobile
• Adopted by governative and private organizations all around the world
• Modular logic: 6 operating areas (modules)

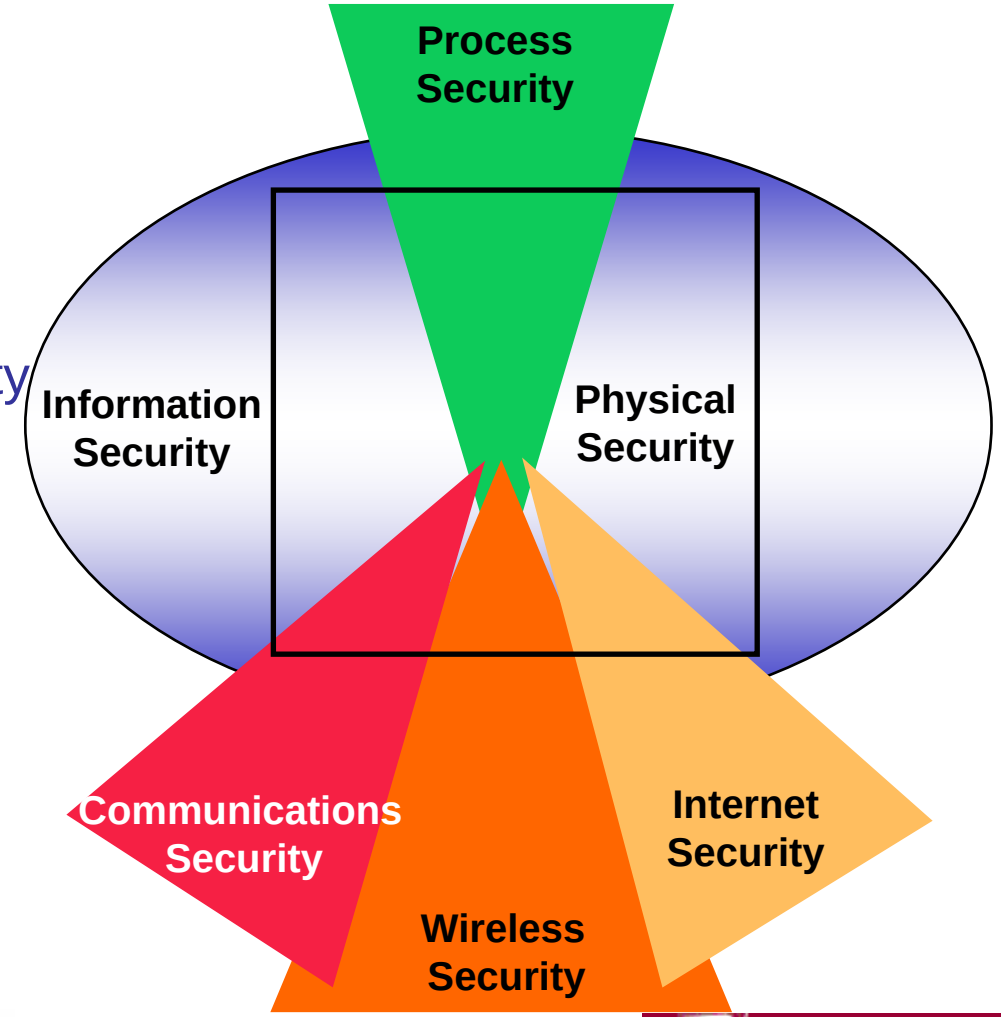


SECURITY TESTING: “THE STANDARD” APPROACH



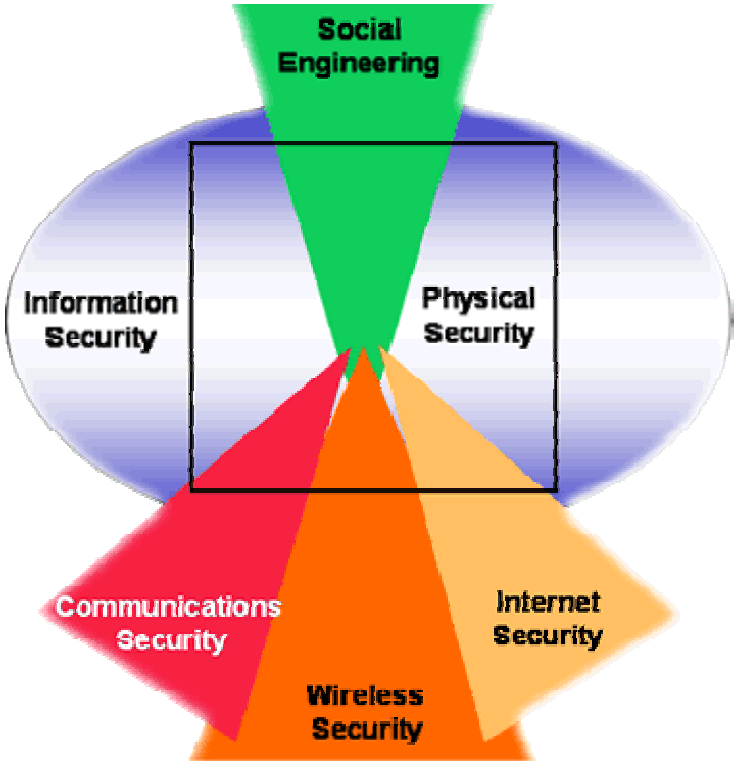
OSSTMM: THE MODULES

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



OSSTMM: OPERATING AREAS

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

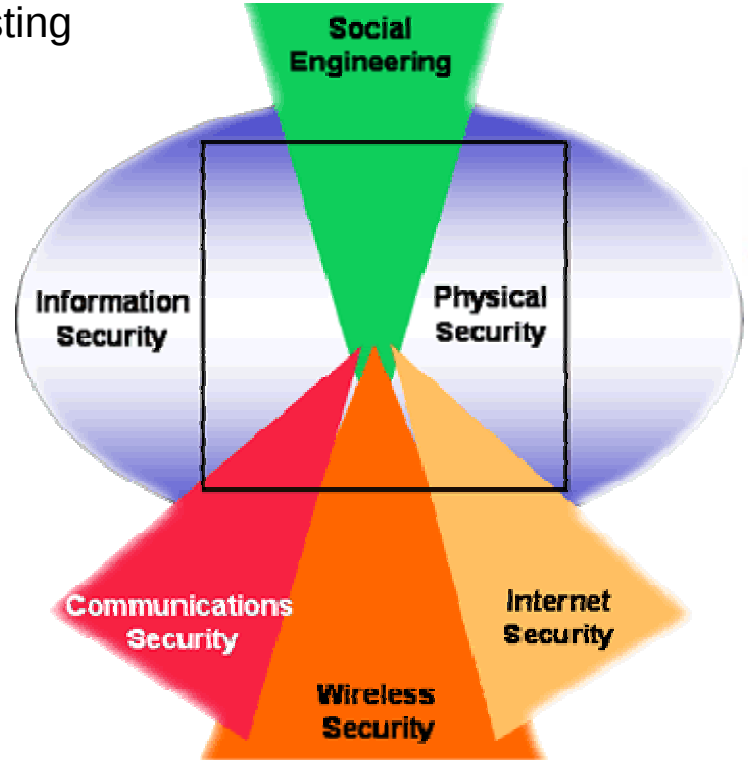
Social Engineering (Process Security)
- Request Testing
- Guided Suggestion Testing
- Trusted Persons Testing

OSSTMM: OPERATING AREAS (2)

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

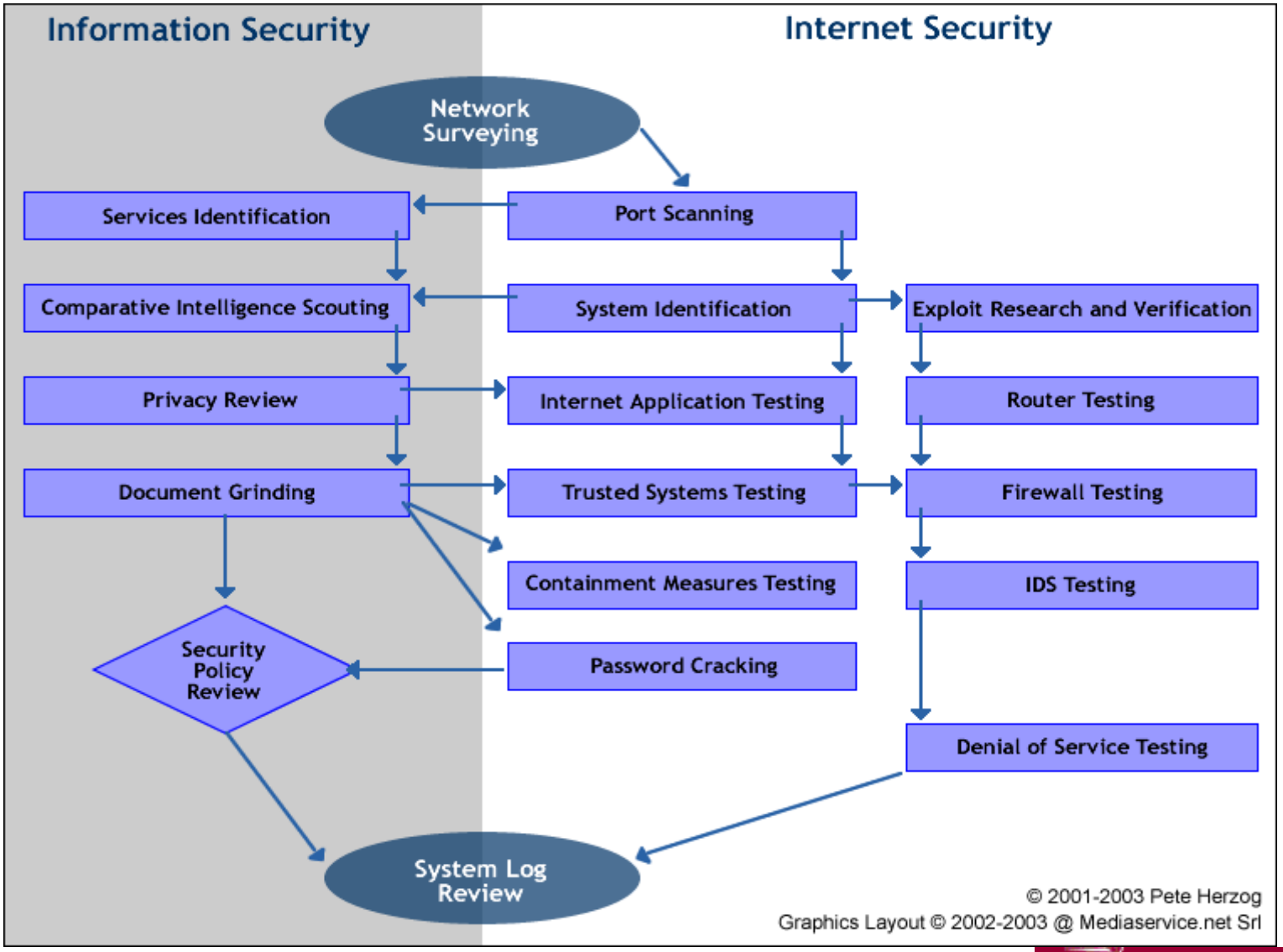
Communications Security
- PBX Testing
- Voicemail Testing
- FAX review
- Modem Testing

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



ISECOM

OSSTMM: Operating Flow (example)

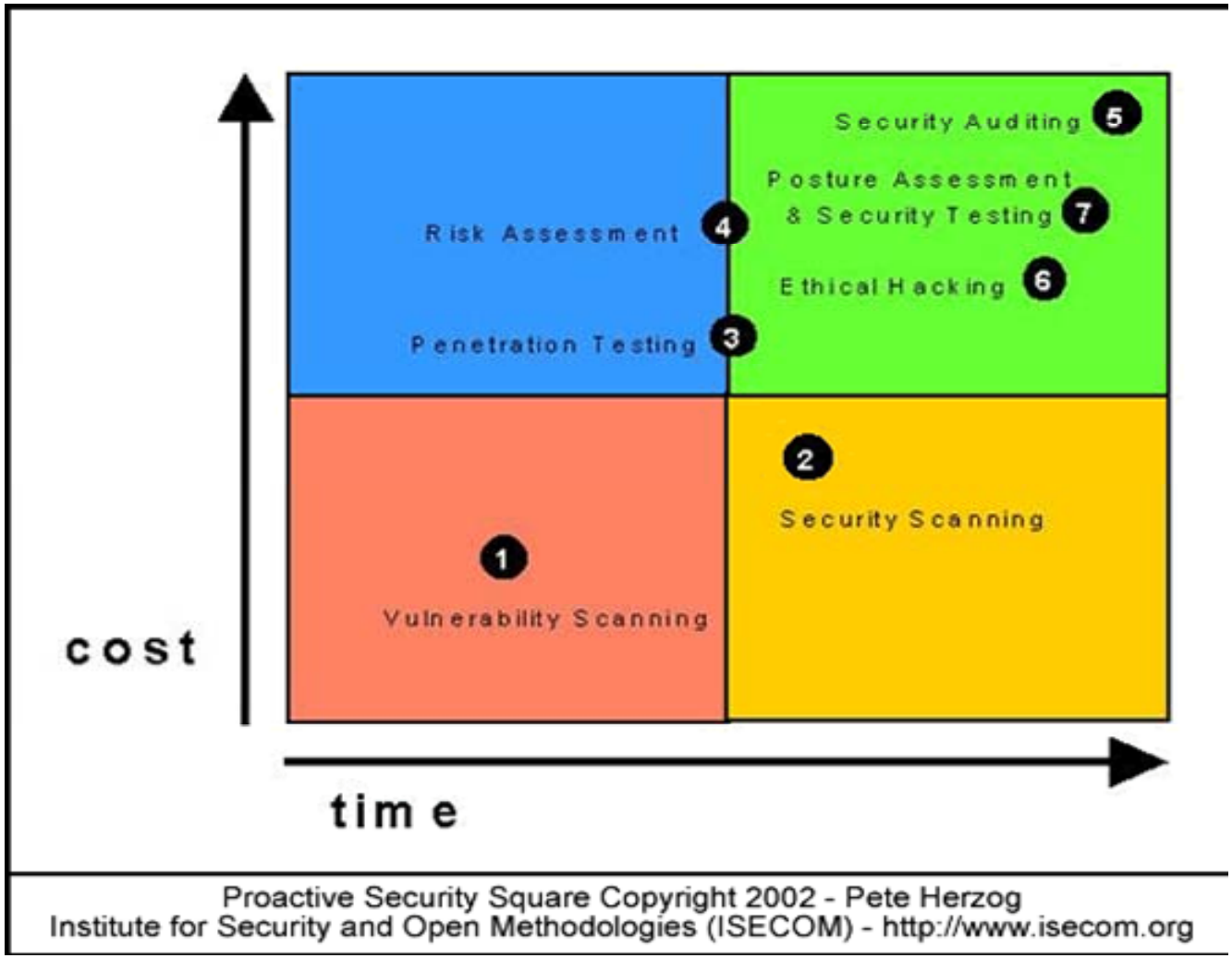


ISECOM

ISECOM

ISACA Roma

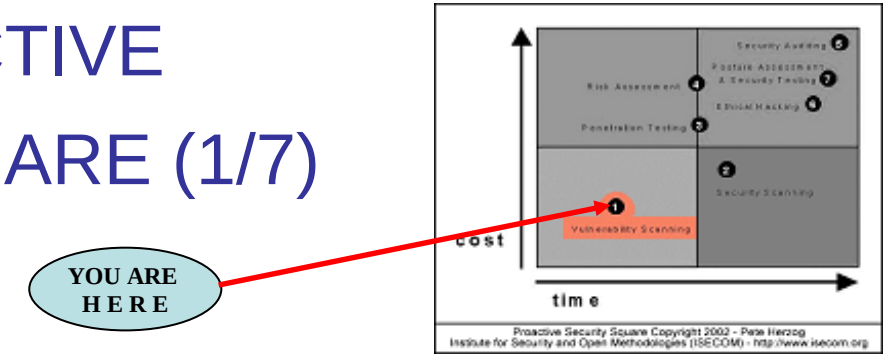
THE PROACTIVE SECURITY SQUARE



ISECOM

Deep Level: Basic

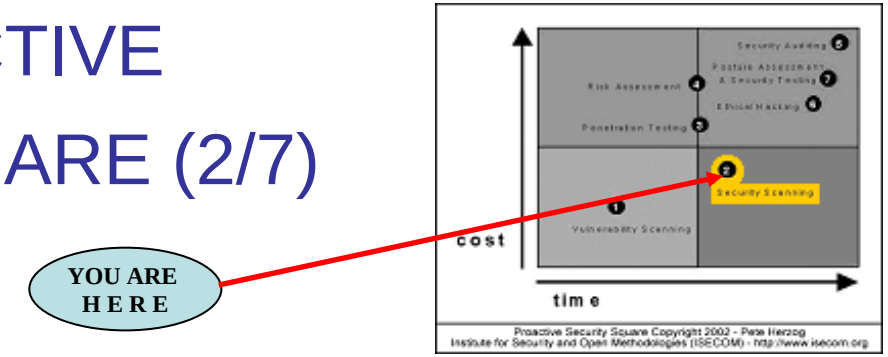
THE PROACTIVE SECURITY SQUARE (1/7)



(1) Vulnerability Assessment/Scanning :

- **Automatized** testings;
- English **language** reports “fits for everybody”;
- **Huge** number of false positive/negative (fake alerts, fake “security sense”);
- It **just cares** about the “IP” world.

THE PROACTIVE SECURITY SQUARE (2/7)

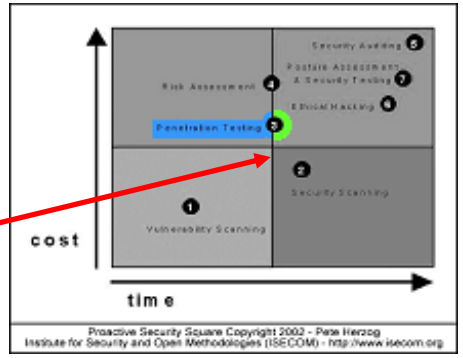


(2) Security Scanning:

- Automatized scannings + **hand-made verifications**;
- Final report is available in **various languages** (english, italian, etc);
- **Manual tuning** of the False Positives and Negatives;
- ..But we keep on to take care **only about the IP** world...

Deep Level: Medium

THE PROACTIVE SECURITY SQUARE (3/7)

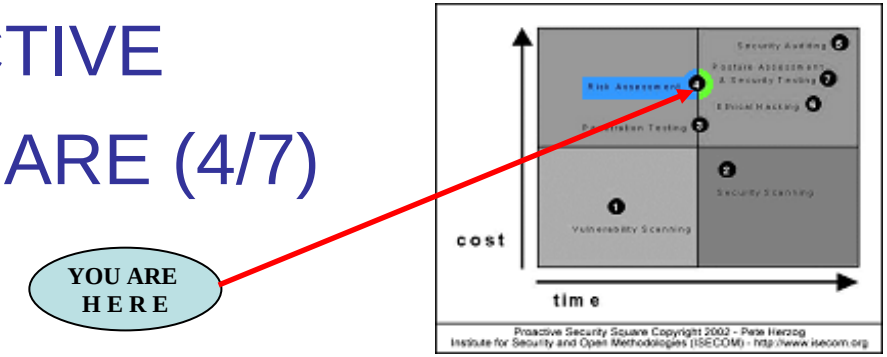


(3) Penetration Testing:

- Verification actions are **manually executed**, following **proprietary methodologies** (pentester's personal background or attack team specific know-hows);
- Final report is **directly written** by the executing Tiger Team and it's sent to the end-customer in his **home language**;
- You can bundle **special testing services** (optionally), such as Social Engineering,Trashing, Physical Intrusion, Web Applications Security Testing, Black-box Penetration Test, etc;
- It **does not stop at the "IP"** world (RAS, Backup_ISDN, X.25, DECnet, Wi-Fi, Web Applications, etc...);
- The execution time grows up **on each single tested asset**.

Deep Level: Medium

THE PROACTIVE SECURITY SQUARE (4/7)

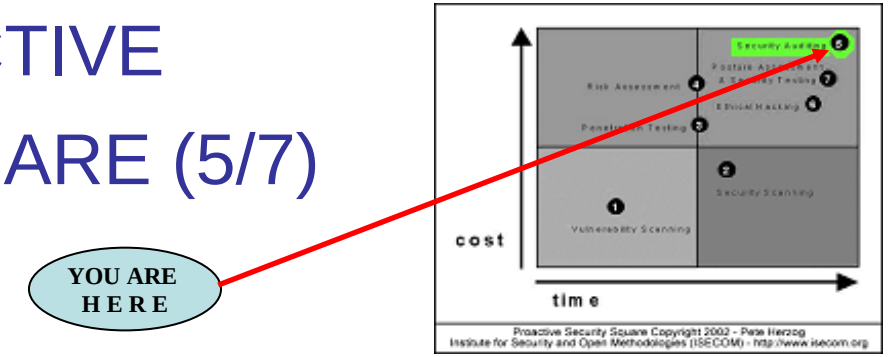


(4) Risk Assessment:

- **Evaluation** and **correlation** actions, toward the **datas mined** from testing operations and the company's risk values;
- Results can be generated **from the 3 previous** technical analysis' methodologies;
- It needs a **long execution time**;
- If the technical testings results are somehow "false", the whole risk analysis **will pay the consequences** (and the economic investments as well !).

Deep Level: High

THE PROACTIVE SECURITY SQUARE (5/7)

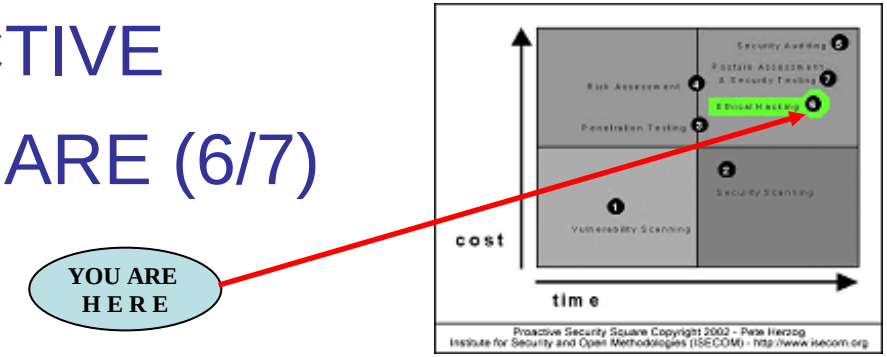


(5) Security Auditing:

- Auditing actions – tipically from the **internal environment** – of the whole IT information infrastructure: the analysis looks at the **projectual**, **procedural** and **implementation** points of view and security issues, exposures and flaws;
- It is manually executed, with a **strong customizing** final report, based on the effective client's needings, taking also under consideration specific assets or company's businesses;
- It can be the final result of proactive security methodologies, **married with** standard risk analysis methodologies (CRAMM, etc..).

Deep Level: High

THE PROACTIVE SECURITY SQUARE (6/7)



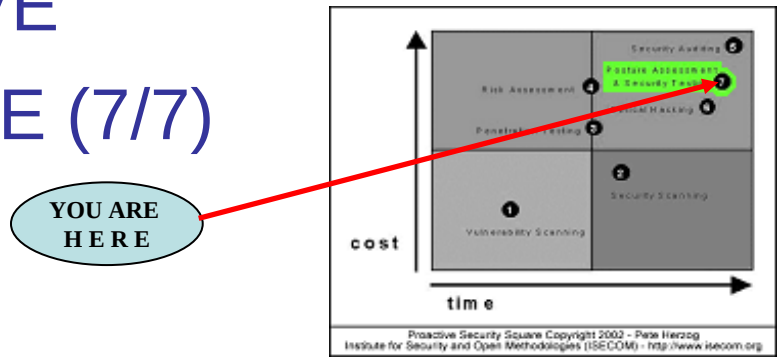
(6) Ethical Hacking:

- **360° degree** verification attacks, aimed towards **specific assets, services or infrastructures**;
- It requires "Full Operating Authorization" + "Free to Jail" when referred to particular testings (special options at point # 3);
- It is executed using unified actions of:

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 Penetration Testing**

Deep Level: High

THE PROACTIVE SECURITY SQUARE (7/7)



(7) Posture Assessment & Security Testing:

- **Repeated** verification and matching actions (follow-up), executed in a time-frame defined and agreed with the client (typically 1 y.);
- The analysis are based on **initial knowledge factors** (expressed in the vulnerabilities analysis, generated from the previous testing actions) and they are executed in **full respect of the OSSTMM** methodology (repeat and compare is possible, saving time & money !) and of its **RAVs** – Risk Assessment Values;
- The final report is manually generated from the Tiger Team, it's translated into the client's language and it is compliance to international guidelines and stadards, such as ISO/BSI, GAO, FISCAM, SARBANES-OXLEY;
- The Security Report is OSSTMM Certified (international).

“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

SECURITY TESTING, ACCORDING TO ISECOM

What makes testing worthwhile?

- According to ISECOM
  - A security test is only valid if it is:
    - Quantifiable
      - Can be numerically measured
    - Consistent and repeatable
      - Two testers would receive the same test results at the same time
    - Valid beyond the "now" time frame
      - Lasts and remains valid longer than the wet ink on the report
    - Based on the merit of the tester and analyst not on brands
      - It is based on smarts and not expensive tools
    - Thorough
      - A complete test where nothing is left untested from the scope
    - Compliant to individual and local laws and the human right to privacy
      - Puts the protection of personal privacy before corporate data

LEGAL COMPLIANCE

The OSSTMM can be used to test for various, international data privacy laws such as:

- **U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).**
- **Provincial Law of Quebec, Canada Act Regarding the Protection of Personal Information in the Private Sector (1993).**
- **The German Bundesdatenschutzgesetz (BDSG).**
- **The Spanish LOPD and LSSI privacy laws.**
- **UK Data Protection Act 1998.**
- **Australian Privacy Act and National Privacy Principle**

You should refer to the latest version of the OSSTMM for all the compliant laws.

COMPLIANCE: LEGISLATIONS (1/2)

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: LEGISLATIONS (2/2)

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

Under validation (OSSTMM 3.0)

BEST PRACTICES COMPLIANCE

The OSSTMM can be used to test for various, international best practices such as:

- **ISO 17799-2000 (BS 7799)**
  Compliance with all of the remote auditing and testing requirements
- **GAO and FISCAM**
  Remote Internet control activities found in the US General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM)
- **OWASP (Open Web Application Security Project)**
  Remote auditing of web applications
- **SCIP (Society of Competitive Intelligence Professionals)**
  Offensive and defensive market/business intelligence gathering techniques known as Competitive Intelligence
- **SET Secure Electronic Transaction(TM)**
  Testing the standard for electronic transactions from VISA
- **National Institute for Standards and Technology**
  Various NIST standards are tested:

✓ **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.

You should refer to the latest version of the OSSTMM for all the compliant best practices.

COMPLIANCE: BEST PRACTICE & IINTELLIGENCE AREAS

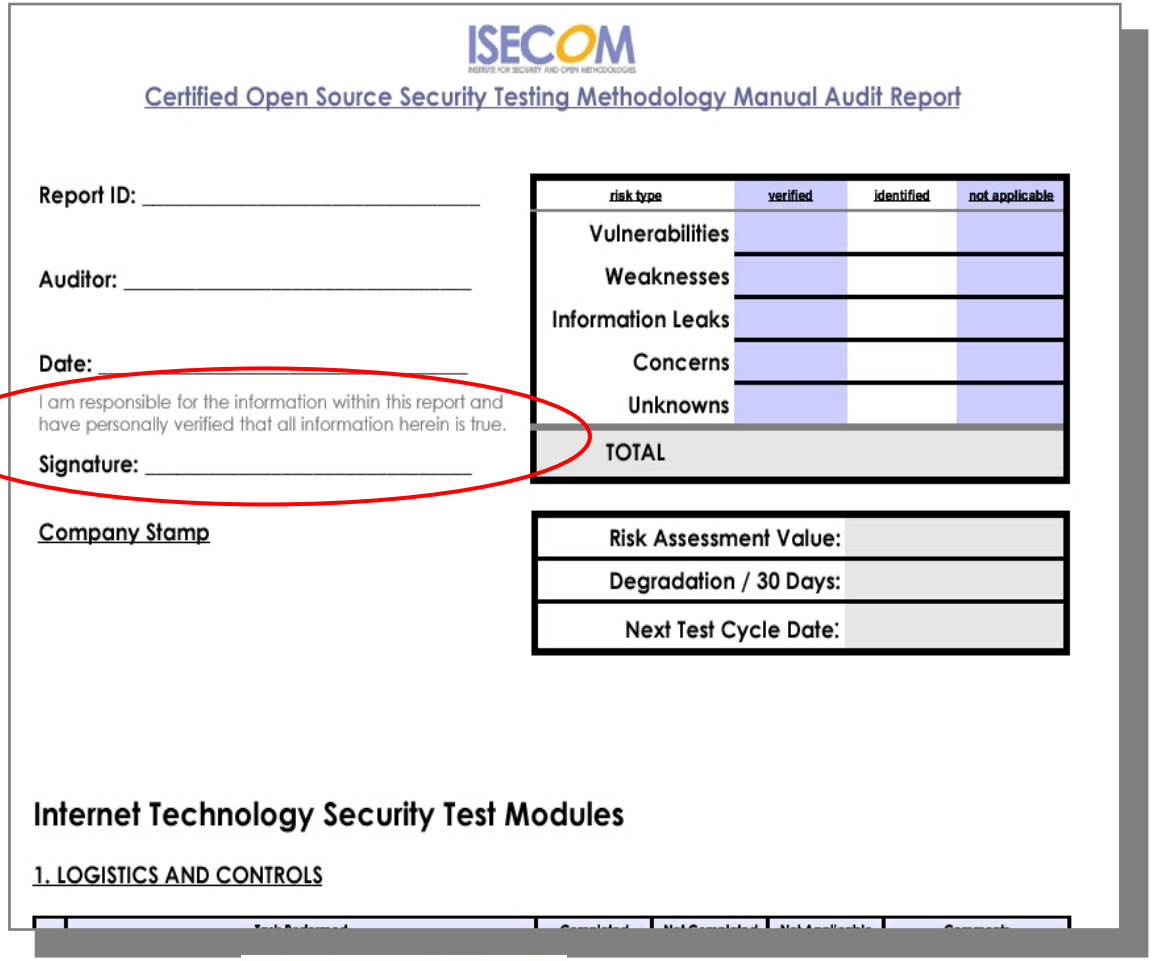
- **Breaking into computer networks from the Internet**, Roelof Temmingh, Sensepost (Pty) Ltd., South Africa
- **The MH DeskReference v1.2**, Rhino9 Team, USA
- **Security Reference Handbook 2001**, Symantec Corporation, USA
- **Auditing your Firewall Setup**, Lince Spitzner, Dec 2000, USA
- **Security 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

ETHICS CODE OF CONDUCT

- Since security consulting & testing **is not a game** or “an hack”, certified testers must announce to the clients that they do **strictly respect** ISECOM’s **Rules of Engagement** during the **whole** security consulting process, from the pre-sales until the final reporting; **all** of the OPST/A certified security personell must follow these areas of ethics:

1. Sales and Marketing
2. Assessment/Estimate Delivery
3. Contracts and Negotiations
4. Scope
5. Providing Test Plant
6. Providing the Rules of Engament to the client
7. Testing
8. Reporting
9. Report Delivery

OSSTMM Certified Audit Report



ISECOM

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

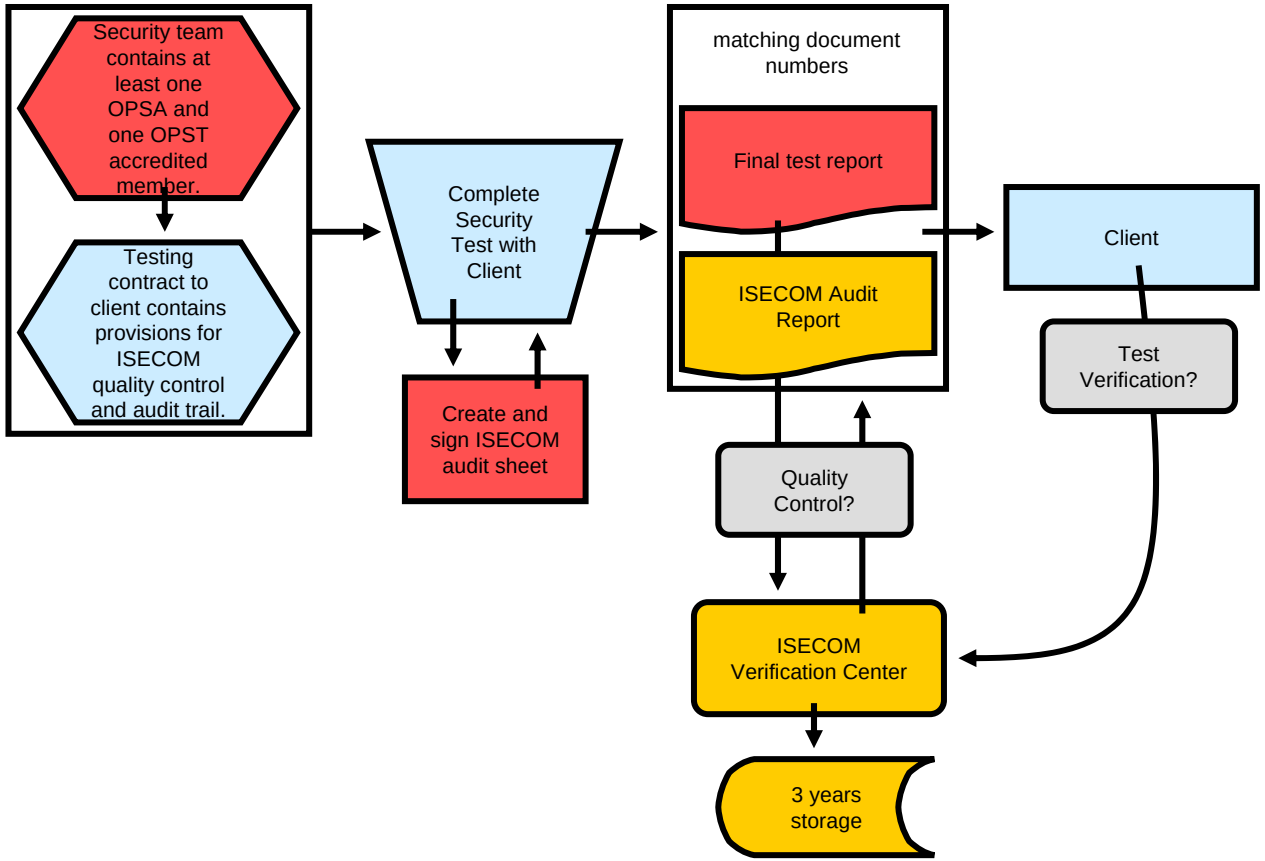
ISECOM

ISECOM

- Readable
- Accountable
- Countable
- Measurable
- Schedulable

ISACA Roma

OSSTMM Audit Report Process



- Credible
- Responsible
- Disclosable
- Storable
- Verifiable

Putting RAVs to Work

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

Work sheet for RAVs calculation

			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

Professional Security Certifications:

OPST, OPSA, OPSE

OSSTMM OPST Professional Security Tester

OSSTMM OPSA Professional Security Analyst

OSSTMM OPSE Professional Security Expert

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.
- ✓ Manages the Tiger Team.

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.
- ✓ Operates in the Tiger Team.

ISECOM

ISECOM

Accredited by La Salle University

OSSTMM OPSA Professional Security Analyst

OSSTMM OPST Professional Security Tester

ISACA Roma

OSSTMM PROFESSIONAL SECURITY TESTER (OPST)

"the hacker mind and the professional methodology"

OSSTMM Professional Security Tester (OPST) is the official professional certification for carrying out security tests complying with the **ISECOM** (Institute for Security and Open Methodologies, USA – http://www.isecom.org/) **OSSTMM** methodology (Open Source Security Testing Methodology Manual).

The OSSTMM provides a **complete methodology** for Security Testing, both involving attacks from outside and within the company. This methodology can also be applied for security tests involving the internal network of the company's DMZ area. It takes into consideration **six** different Corporate Security areas defined by the OSSTMM, called **Operating modules**.

The aim of the ISECOM **OPST** certification course is to provide participants with the necessary knowledge to perform security tests in a professional and autonomous way.

The training course focuses on the acquisition of the technical skills necessary to perform security tests, as well as the business skills **useful and necessary** to acquire the motivations, efficiency and understanding of the current IT market demands. The course requires a basic knowledge of the administrative elements of the Linux platform, network protocols and security testing techniques.

It aims to make participants able to find useful responses to pass the test concerning the six operating modules included in the **OSSTMM** (**Physical Security**, **Communications Security**, **Wireless Security**, **Information Security**, **Internet Security** and **Process Security**).

OSSTMM PROFESSIONAL SECURITY TESTER (OPST)

"the hacker mind and the professional methodology"

The course spans **five intensive days**, including the **five hours** for the final certification exam, which takes place in the afternoon of the fifth day and requires participants to put into practice what they have learnt during the lessons.

The five training days can be summarized into **three main components**, all based on the latest version of the OSSTMM and the international documentation present in the professional test performance sector: **Business Information Security**, **Practical Security Testing** and **Aggressive Security Testing**.

❑ **Business Information Security** is the training module concerning safety testing requirements and deals with topics like confidentiality of information, risk assessment, testing legalities, professional ethics, reporting, test procedures and implementation rules;

❑ **Practical Security Testing** is the technical training module aiming to define the terms and requirements for security tests, on the basis of the latest version of the OSSTMM for assessments and evaluations;

❑ **Aggressive Security Testing** is the advanced technical baseline for defining the terms and requirements for performing a complete and OSSTMM **certified** security test, as regards the sections Information Security and Internet Security.

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 al 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"

OSSTMM Professional Security Analyst (OPSA) is the official professional certification for Security Analysis, complying with the **ISECOM** (Institute for Security and Open Methodologies, USA – http://www.isecom.org/) **OSSTMM** methodology; it is based on the OSSTMM (Open Source Security Testing Methodology Manual), the Business Security Testing and Analysis Workbook (BSTA) and the OSSTMM Internal.

The objective of the OPSA certification is to provide the *security professional* who works in the field of ICT security with theoretical and practical **multilevel certification**.

The training course focuses on the analytical knowledge and *security knowledge* needed to analyze security and risks. It defines the business and *project management* skills necessary in security projects and in the management of a company's internal *security teams*.

The ISECOM OPSA certification is a great source of information for all those who work in the field of security and networks; moreover, it enhances the skills of those who want to grasp what a network really is, the *rules of engagement* an calculation of RAV, by analyzing the results achieved and managing a company's proactive security process.

OSSTMM PROFESSIONAL SECURITY ANALYST (OPSA)

"professional business security analysis and consultancy from the international security standard"

The course spans intensive **four** days, on the basis of the type of participants to each session, plus the morning of the fifth day, during which participants will dedicate one hour to a *program review* with their teacher and **five hours** to the final certification exam. Attendance is **compulsory.**

The training days can be summarized as **three main components**, all based on the latest version of the OSSTMM and the international documentation present in the professional test performance sector: **Security Analysis**, **Red Team Strategies** and **Security Project Management**.

❑ The module **Security Analysis** is a guideline to understand security test results like log files, security tool outputs and protocol dumps, as well as the implementation of OSSTMM modules depending on the expected results and practical solutions, from the point of view of *business motivation*. Strategies for the assessment of technical risks, system and network contingency tests and solutions for the network security architecture are also taken into consideration.

❑ The module **Red Team Strategies** provides a thorough insight into the rules for resorting to security consulting, from the pre-sale phase to the preparation phase and the issuing of a final Security Report, including the laboratory and the use of groups of *professional security testers*.

❑ Finally, the module **Security Project Management** provides an overview of projects of *OSSTMM compliance* tests and their applications. It focuses on the management of projects: reporting on the timing, assessment, team management, technical requirements and specifications in contract, interaction with customers, test efficiency an cost control, including the management of investment profitability (ROI) by means of OSSTMM *Risk Assessment Values*.

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 (OSSTMM).

❑ 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.

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: OPSE will be available in 2006.

ISECOM Certification's Example

Certificate of Completion

awarded to

Raoul Chiesa

Certification Number: AIZV553

ISECOM

LA SALLE
Enginyeria
Arquitectura

OSSTMM PROFESSIONAL SECURITY TRAINER

Trainer training for the accredited
OSSTMM 2.5. Professional Security Tester certification

by

ISECOM

Institute for Security and Open Methodologies
December 2002

Peter V. Herzog
Managing Director

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

OPSE - OSSTMM Professional Security Expert

- Junior Project Managers
- Junior Security Testers
- Chief Information Officers; Chief Technical Officers

SUBSCRIPTION REQUIREMENTS

OSSTMM Professional Security Tester (OPST)

- English language
- Advanced knowledge of TCP/IP
- Advanced knowledge of network topologies and technologies
- Advanced Experience with Unix and Windows NT based networks
- >1 year of experience in the security-testing field

OSSTMM Professional Security Analyst (OPSA)

- English language
- Base knowledge of TCP/IP
- Base knowledge of network topologies and technologies
- Base Experience with Unix and Windows NT based networks
- >2 years of experience in the security field

OPSE - OSSTMM Professional Security Expert (OPSE)

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

..Lesson Learned..

Now that we have all this useful information, it would be nice to do something with it. (Actually, it can be emotionally fulfilling just to get the information. This is usually only true, however, if you have the social life of a glass of water.)

Unix Programmer's Manual.

Edited for clarity.

MORE INFO?

www.isecom.org
www.osstmm.org
osstmm.mediaservice.net

ISECOM's Certification Programs:

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

Mail Contacts	raoul@isecom.org
Web Contacts	http://www.isecom.org http://osstmm.mediaservice.net/