Proactive Security: what I learned over the last 20 years

(a.k.a. «Pentesting field experiences: 1995-2015»)

Raoul «Nobody» Chiesa

ISECOM Board of Directors

Founding Partner, President, Security Brokers SCpA

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

NIC

ISACA
Gūstot vērtību no uzticamām informācijas sistēmām
Latvijas nodaļa

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Disclaimer

- The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the view of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers**, its **Associates** and **Associated Companies,** and **Technical Partners**.
- Contents of this presentation **cannot be quoted or reproduced**.

Abstract

- I performed my very **first penetration test back in 1995**, against a VAX/VMS target.
- Since that year 'till today, **tons of stuff** happened : DEC was acquired by Compaq (which was acquired by HP), Sun Solaris and IBM Aix kept on being sold worldwide, X.25 networks have been shut down all over (?), and IPv6 will enjoy our pentesting lives over the next decades, along with 5G and the IoT…
- Back in 2000 I joined **ISECOM**, those folks which gifted to the whole world the amazing **OSSTMM** (Open Source Security Testing Methodology Manual), adding real professionalism, and a worldwide shared methodology, to the proactive security field, along with **+10.000 supporters** and dozens of **Key Contributors**.
- Nevertheless, organizations still do **fall in plenty of mistakes** when dealing with the topic of penetration testing from strategic, business and operations perspectives.
- This talk will (try to) provide the audience with my **field experiences**, and should be useful both for the "op geeks" and the managers, highlighting those errors made by the Customers, which definitely ruined my Friday nights, week-ends and personal life over the last 20 years…. And I realy hope this won't happen anymore! ;)

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Agenda

- Introductions
- Key issues
- Security/Vulnerability Assessment: you don't know what you (really) want
- The ISECOM Proactive Security Square
- You can't always test what should really be tested
  - Time constrains, Budget limitations
  - Legal Authorizations
  - Those who just don't care ☹
- Common, shared security testing methodology
  - The OSSTMM
  - OSSTMM going ISO/IEC (along with NIST)
- You may not be delivered with ALL of your exposures and vulnerabilities
  - Field Experiences from the Red Team
  - Lack of experience on specific sectors (i.e. SCADA&ICS, Automotive, Aiports, etc…)
  - No Test-bed = no party
- Conclusions
- Links
- Contacts, Q&A

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Introductions

The speaker

- President, Founder, **The Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Indipendent Special Senior Advisor on Cybercrime @ **UNICRI** (United Nations Interregional Crime & Justice Research Institute)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various security communities**

The Security Brokers

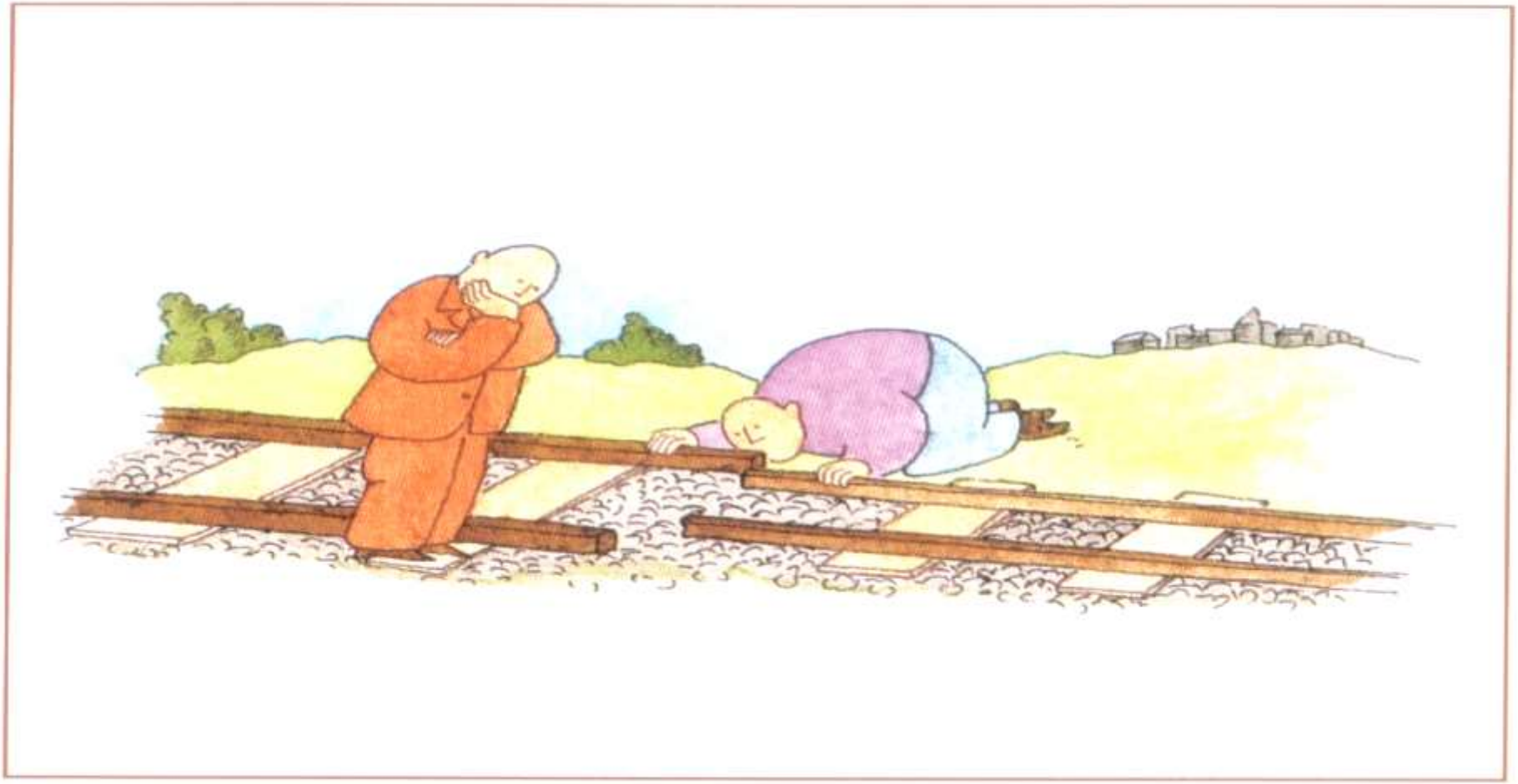
- We deal with **extremely interesting, niche topics**, giving our strong know-hows gained from **+20 years of field experience** and from our **+30 experts**, very well known all over the world in the'**Information Security** and **Cyber Intelligence** markets.
- Our **Key Areas** of services can be resumed as:
  - **Proactive Security**
    - With deep experiences on TLC & Mobile, SCADA & IA, ICN & Trasportation, Space & Air, Oil&Gas, e-health, […]
  - **Post-Incident**
    - Attacker's profiling, Digital Forensics (Host, Network, Mobile, GPS, etc..), Trainings
  - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
    - On-demand «Ninja Teams»
    - Security Incident PR Handling & Management
  - **Psychological, Social and Behavioural aspects (applied to cyber environments)**
  - **Cybercrime Intelligence**
    - Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, Technical & Operational support towards CERTs and LEAs/LEOs,[…]
  - **Information Warfare & Cyber War** (only for MoDs)
    - 0-day and Exploits – Digital Weapons
    - OSINT

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Issue # 1

THE MINDSET

Mindsets and Backgrounds



BREAK! Let's play a game: Jack the Electrician

- **Think about <u>10 ways</u> to turn off the light into this room.**

1. Turn the switch off.
2. Break the bulb.
3. Rip out the wiring.
4. Overload the electricity in the room.
5. Cut the electricity to the room.
6. Add a brighter light source to the room.
7. Wait until it dies on it's own and don't allow anyone to change it.
8. Ask someone to shut the light off.
9. Cover the bulb with a cloth.
10. Close your eyes.

- **Destruction** of any part of the **process chain effects the end result**.
- **Attacking the process** (side attacks) **is essential to security testing**.

Mindsets and backgrounds

- Depending on the **country**, your **referent** at the **client's side** will be:
  - xperienced IT guy (NOT InfoSec guy)
  - Unexperienced IT guy
  - Unexperienced InfoSec guy
  - Auditor's background
  - Risk Officer
  - Privacy Officer
  - Management background
  - Former Law Enforcement Officer
  - Experienced Infosec guy (rare as the **white truffles** and **black swans**!)

- Most of them (**80%**) will **NOT understand you** (different languages): lingo (slang), terminologies, acronyms, etc… ☹
- Most of them (**95%**) will **not know enough** about pentesting.

Shopping for Security

[Into the customer's mind]

- **Do I need** a security test?
- **How often** do I need a security test?
- **Who** should do the security test?
- Is it better to have a **consultant** do it or **train some people** to do it **internally**?
- **What do I need to know** about hiring a consultant?
- (and) I need to **spend as less as possible**!

Issue # 2

HUMAN BEINGS & SINS

When customer doesn't really need it

- I **rejected a very few customers** in my carrier.
- Those were the guys which **didn't really care** about a professional, quality-based pentest, a honest project, the right budget.
- They just had to «**get a pentest report**» to cover their own ass ☹
- Or, you feel that the report will **used to shit on someone of their colleagues (different departments).**
  - Or, it will be printed in order to fix an unstable desk.
  - Or, it will be hidden into a file cabinet.
  - Or, it will just disappear (happened with a GSM operator back in 1999).
    - (Then the report apperead again in 2001 ☺

Issue # 3

«TERMINOLOGIES» (a little bit more, actually!)

[aka: when terminologies impact on quality, security, budget]

«Security (Vulnerability) Assessment»

- It just **doesn't mean something really**
- It leads to **misunderstandings (i.e. Automated testings VS manual ones)**
- It may lead to **poor security testing (i.e. False Positives/Negatives)**
- It helps those market's players **without real experiences and skills**
- It helps those who **just takes care about the economical aspects** and to **speculate over Information Security** ☹
- If **YOU** (your organization, your ISP, your country) are insecure, **I** will be insure (my ISP, my organization, my country).
- That's why when it's **about security testing**, budget **should NOT limit** the **overall quality** of the project.

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

YESTERDAY

✓ …we had different “schools” (way of thinking)

- **Automated Testings (Vulnerability Scanning/Assessment)**

“our scanner uses A.I. over neural networks and everything it’s under HA“

- **Manual Testings (Ethical Hacking, Pentesting, Unconventional Security Testing)**

“the most advanced & up-to-date hacking techniques”
“we have the best hackers in the world (or whatever)”
“...Uh, yeah, you know, we use Latvia hackers!”

- **Security through Obscurity Security Testing**

“…You should not be interested about how we get our job done…let us think about these kind of things…it’s our job, after all ! ”

TODAY

…we got "methodologies"

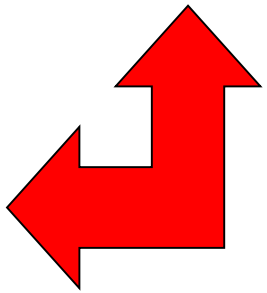
- Vulnerability Scanning/Assessment
- Security Scanning
- Penetration Testing
- Risk Assessment
- Security Auditing
- Ethical Hacking
- Posture Assessment & Security Testing

KEY DIFFERENCES:

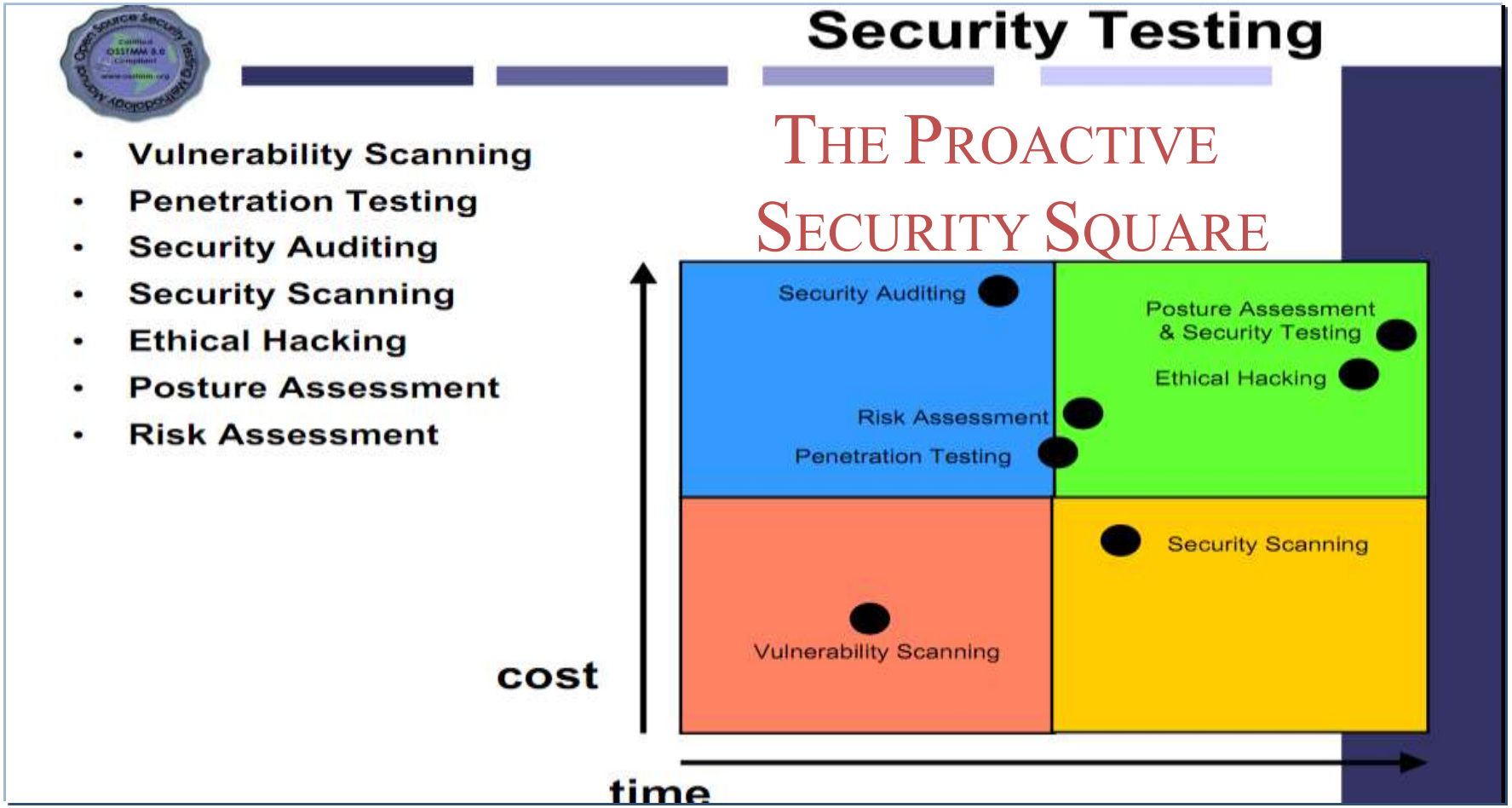
- Execution costs
- Execution times

LEVEL 2 DIFFERENCES:

- **Which methodology or "school"/expertise is applied ?**
- **Is it possibile to compare and repeat the results ?**
- **Do the results have numerical values to clarify the "Risk Value" ?**
- **Is the work compliant to standards and legislations ?**

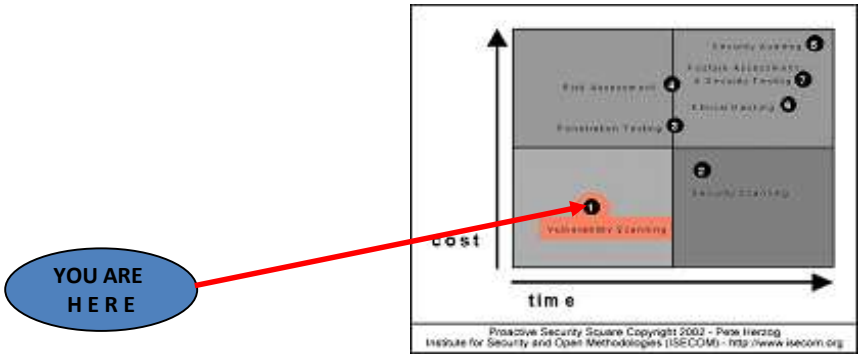


Standard SecTesting approaches



© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

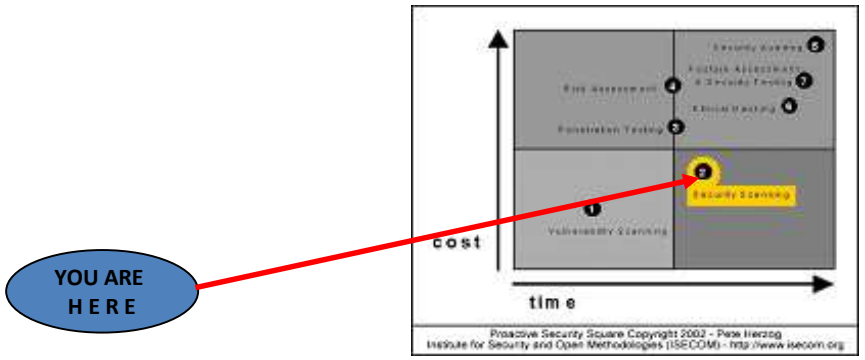
ISECOM Proactive Security Square (1/7)



(1) Vulnerability Scanning/Assessment:

- Automated verifications
- Final report "english-only"
- High percentage of false positives/negatives (false alarms, false "sense of security")
- It just works on the "IP" area

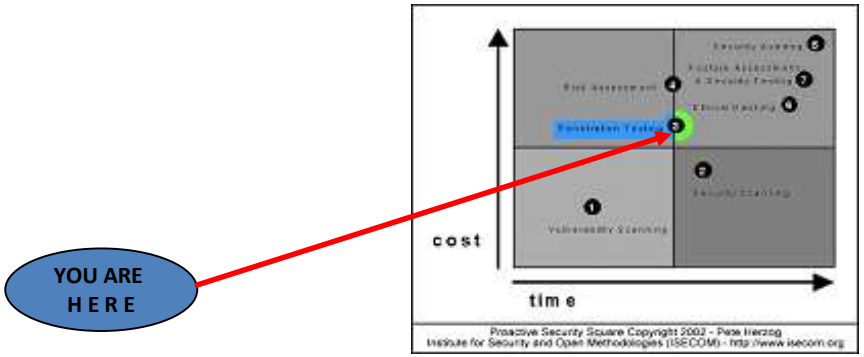
ISECOM Proactive Security Square (2/7)



(2) Security Scanning:

- Automated scannings; manual verifications
- Final Report can be in other languages than English
- Manual Tuning of False Positives/Negatives
- It just works on the "IP" area

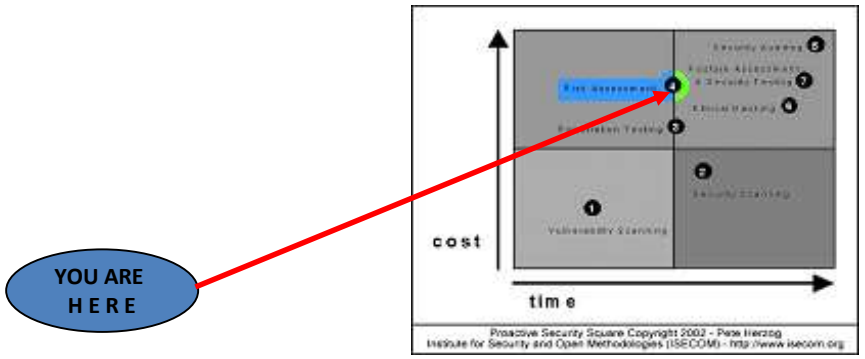
ISECOM Proactive Security Square (3/7)



(3) Penetration Testing:

- "Manually executed" verification actions, under proprietary roadmaps / approaches (the personal background of the pentester or of the Attack Team)
- Final Report is written in client's language by the Tiger Team
- The client can choose addictional options such as Social Engineering, Trashing, Physical Intrusion, Web Applications SecurityTesting, etc...
- It doesn't work on the "IP" area only
- Execution time grows considerally on each single asset

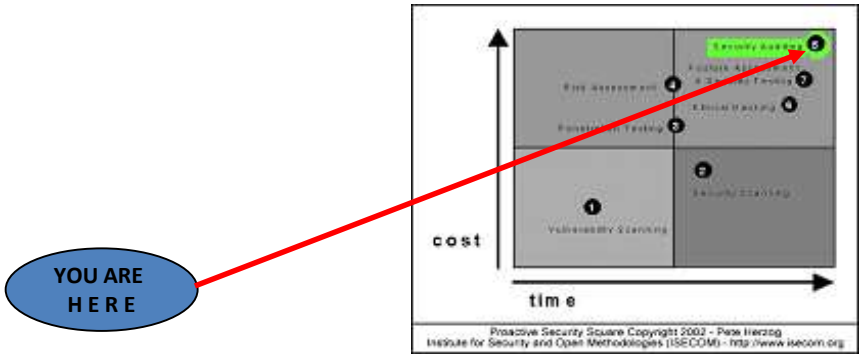
ISECOM Proactive Security Square (4/7)



(4) Risk Assessment:

- Evaluation-and-correlation actions between the datas obtained from the security testing operations and the company's risk value
- The results could have been generated from the previous 3 methodologies for the risk's technical analysis
- It needs a long execution-time
- If the technical testing's results failed, all the risk analysis will pay the consequences (and the investments too…)

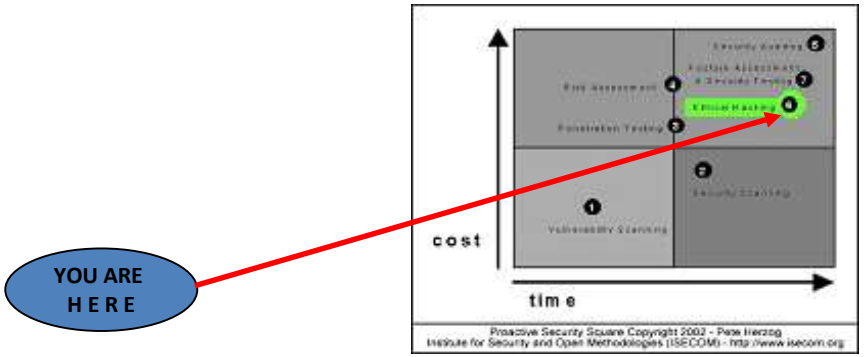
ISECOM Proactive Security Square (5/7)



(5) Security Auditing:

- Auditing actions - typically inside ones - on the whole IT infrastructure, executed from the project and implementation point of view (not ROI or Financial Auditings)
- Normally, it is manually executed and the Security Report output must meet the specific needs of the Client and/or must consider specific and pointed-out assets
- This can be generated as the result of different methodologies for the proactive security, matched with the standard's risk analysis methodologies

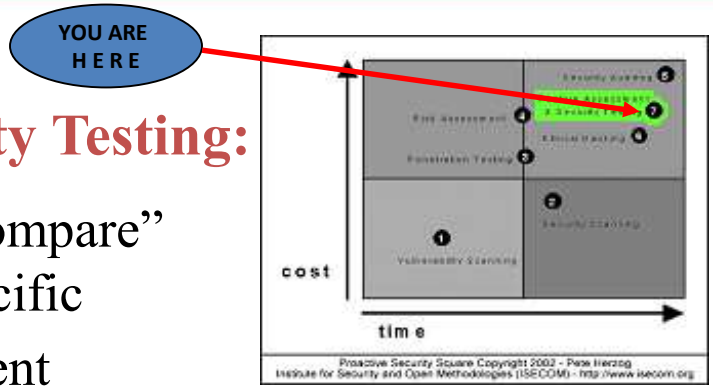
ISECOM Proactive Security Square (6/7)



(6) Ethical Hacking:

- 360° verification actions, targetted toward specific assets or infrastrucutures
- It requires FULL OPERATIN AUTHORIZAZION + "Free to Jail" (needed for the testings listed at point 3)
- Is is executed throught the following - conjucted - actions:
  1. **Penetration Testing (IP, xSDN, X.25/X.121, SAT, …)**
  2. **Phreaking**
  3. **Social Engineering, Physical Intrusion, Trashing**
  4. **Reverse Engineering**
  5. **Black Box Testing**

ISECOM Proactive Security Square (7/7)



(7) Posture Assessment & Security Testing:

- Repeated actions of "verify and compare" (follow-up) executed during a specific time-period agreeded with the Client
- The analysis are based on initial knowledge factors - that are expressed in the "Final Considerations & Practical Suggestions" generated from the previous security testing's actions - and are execlusively based on the OSSTMM methodology, that is repeteable and quantificable (RAVs)
- The Security Report is manually reported by the Tiger Team in the Client's native language and respects the international standard guidelines (legislations and best practices) such as ISO/IEC 27001, 27005, GAO, FISCAM, PCI-DSS, etc
- The Security Report is OSSTMM certified

Issue # 4

THE METHODOLOGY

Before the next slide

- How many of you here ever **hired a (Red, Tiger, whatever) Team** in order to **execute a Penetration** Test at your company or agency?
- How many of you **perform Penetration Tests** as **a job** ?
- In **both cases**, **which was** the Penetration Testing **methodology used** ?

Pentesting methodology

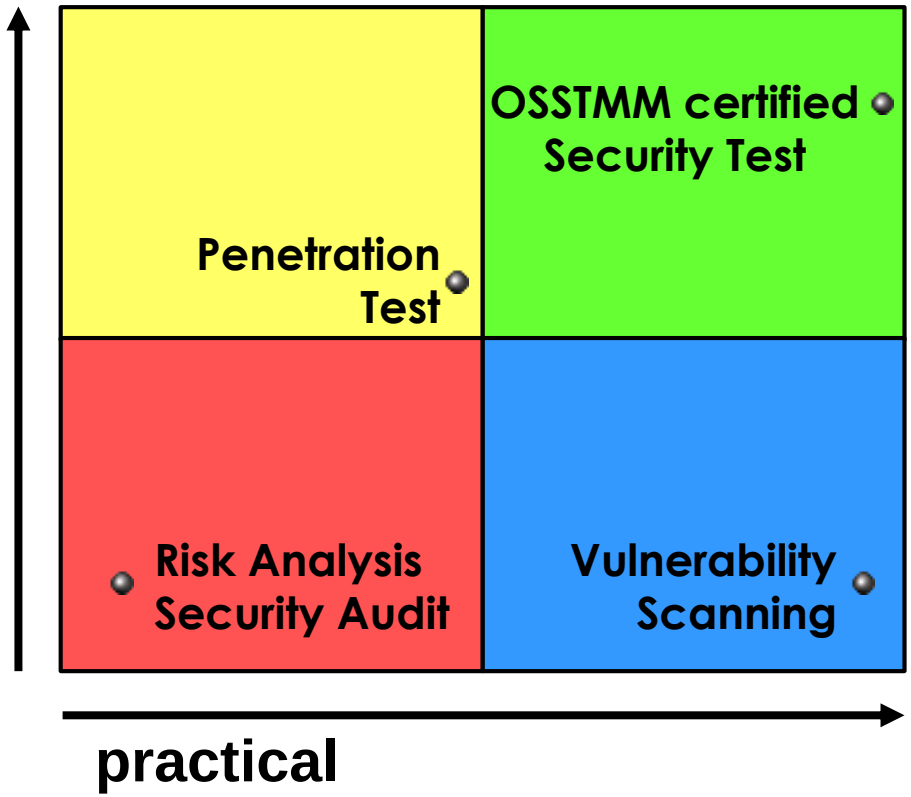
- This is the very first, **key issue** when it's about pentesting.
- Clients **get crazy** when trying to «compare» **different security reports** from **different pentesting companies**.
- Most pentesting companies claim to **use their «own, internal pentesting methodology»**.
  - And, «**we cannot disclose it with you** [customer], sorry!»
- **WTH**?!? ☹

Talking IT Security seriously (1)

- *What is a Security Test?*

  A security test should be a **measurement of configurations, legal compliancy, best practices and operational processes - in action (live).**

  - A **qualified** inspection.
    - Quantitative
    - Qualitative

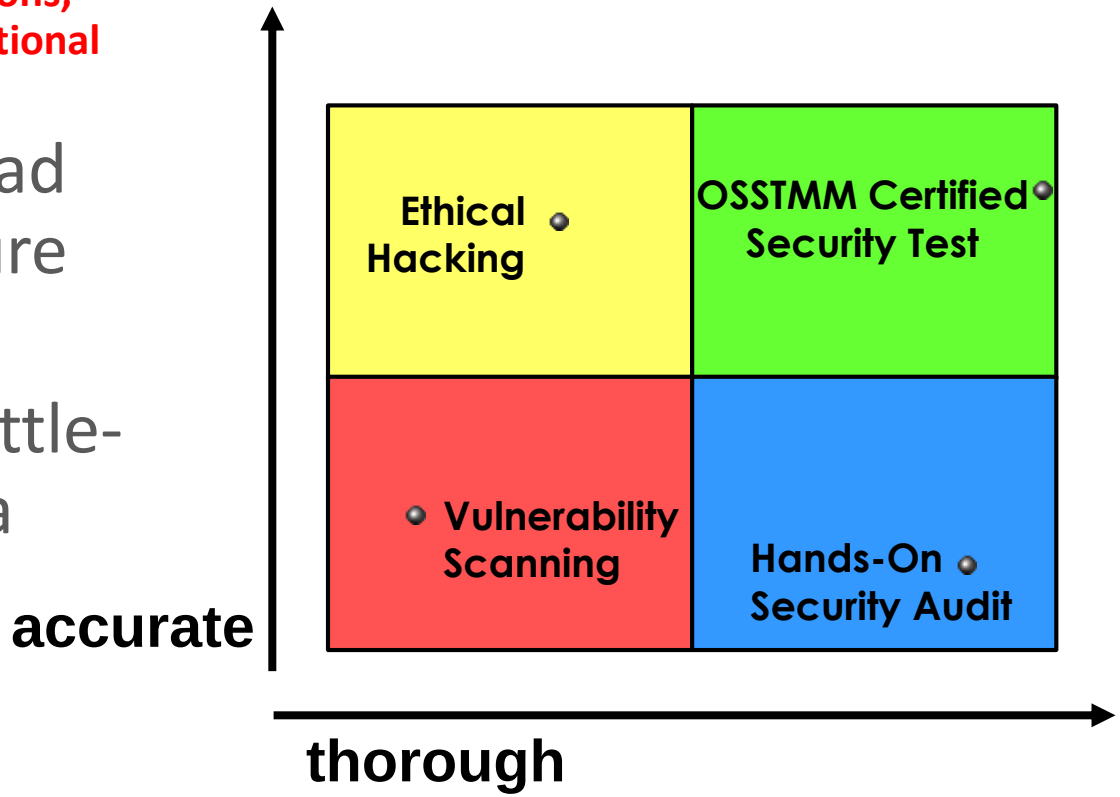


Talking IT Security seriously (2)

- *What is a Security Test?*

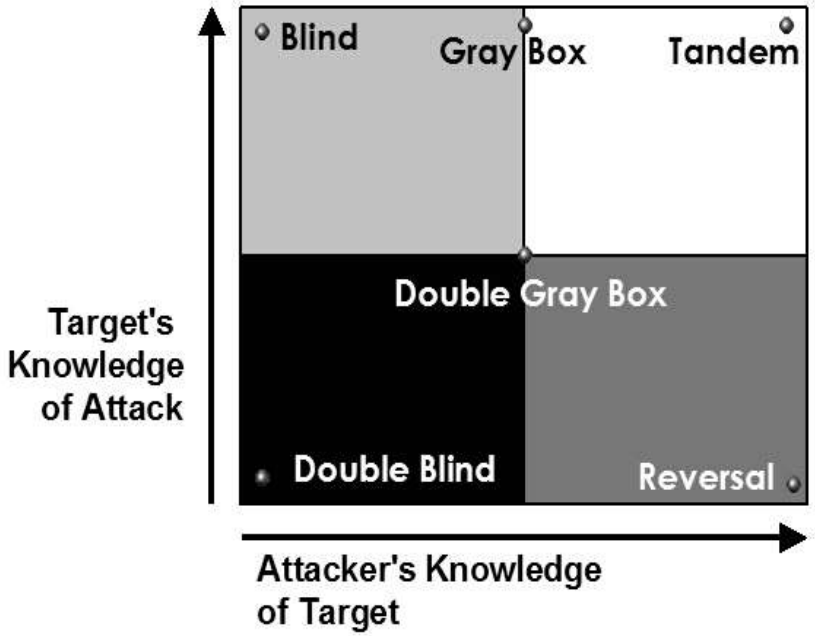
  A security test should be a **measurement of configurations, legal compliancy, and operational processes in action**.

  - **Qualitative**: a dead network is a secure network.
  - **Quantitative**: a little-used network is a more secure network.

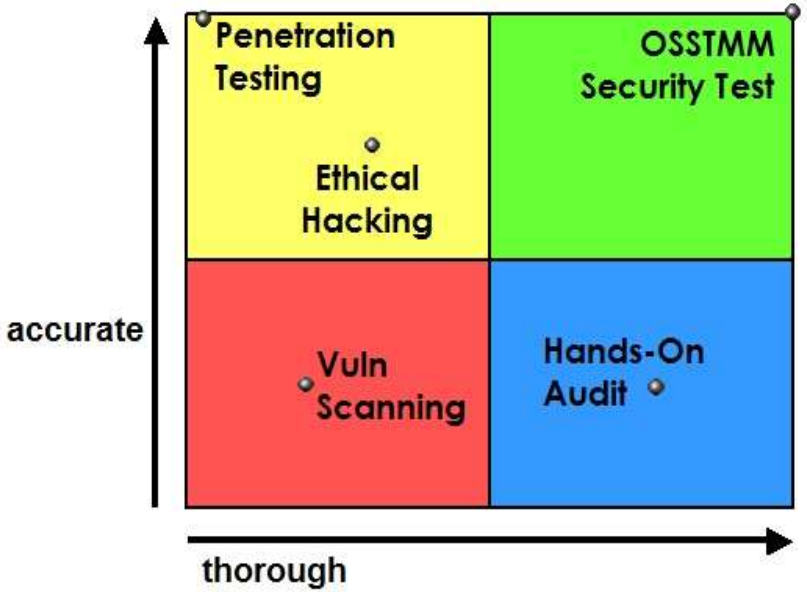


Security Tests

Common Test Methods



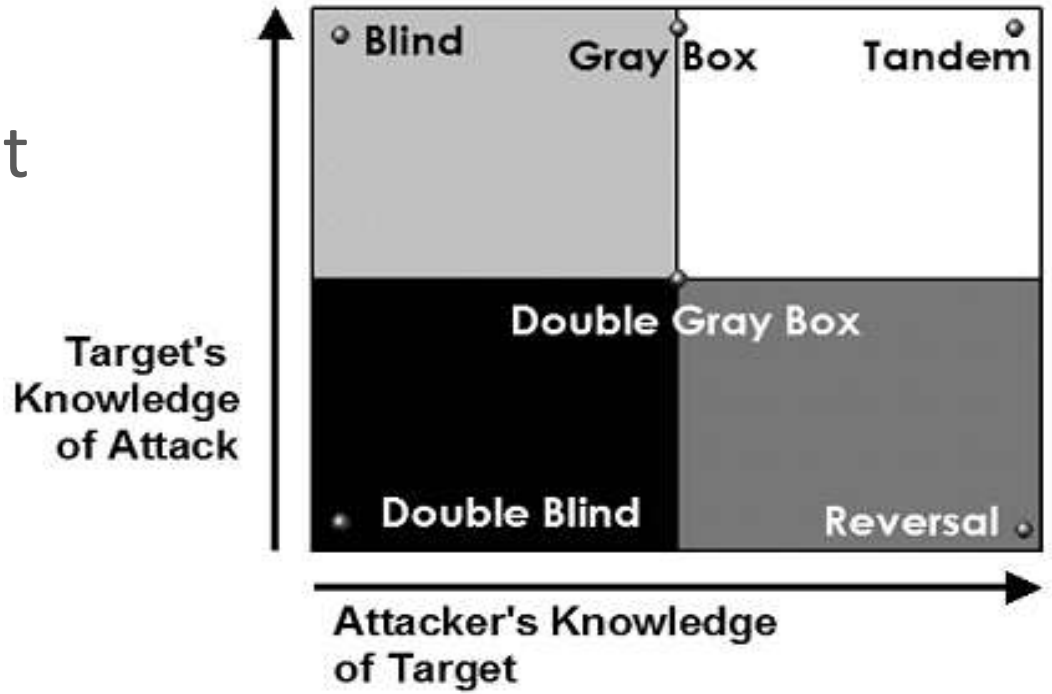
Common Test Types



© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

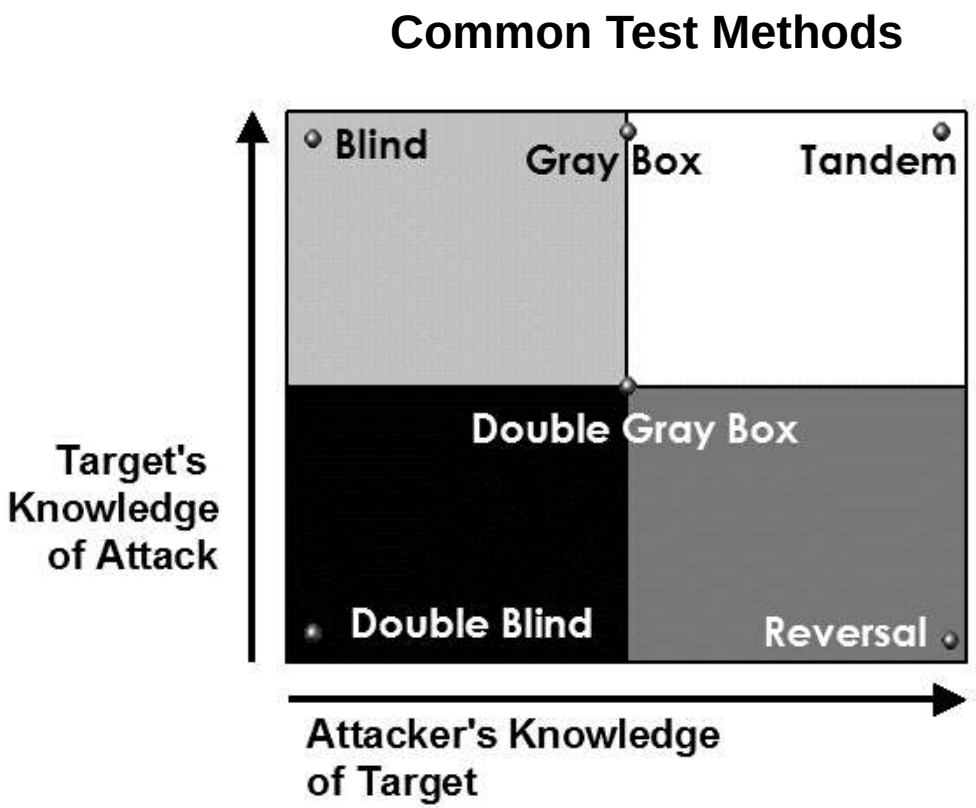
OSSTMM: test typologies

The OSSTMM is an **high-level** methodology. It **does not supply** a difference between a Vulnerability Assessment and a Penetration Test, while it supplies values and roadmaps about «how to» **run complete Security Verifications**.



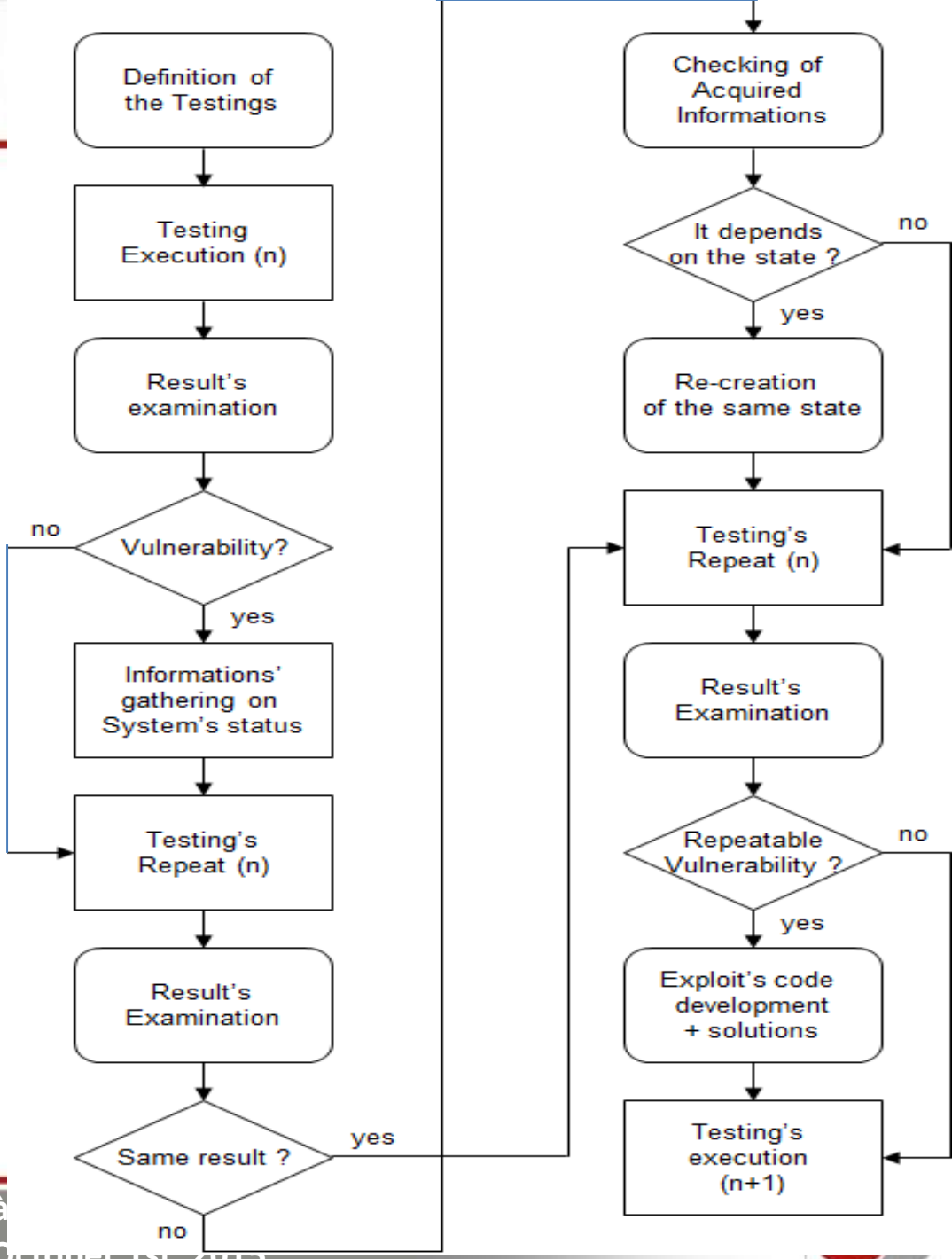
OSSTMM 3 Test Types

- **Blind**
  - War Gaming, Role Play
- **Double Blind**
  - Penetration Testing
- **Gray Box**
  - Often a Self Assessment
- **Double Gray Box**
  - Also a White Box Audit
- **Tandem**
  - Also a Crystal Box Audit
- **Reversal**
  - Red Team Exercise



Security Testing Defined

- A test is a **measurement of the operations**.
- **Knowing how something works** helps you **identify what doesn't work**.
- We measure to assure a good fit. **If we cannot measure security we cannot assure it's appropriateness** in a uniform manner.
- It is the foundation for **risk analysis**.



© 2015 Raoul Chiesa / Security Brokers Società

ISECOM

- **I**nstitute for **SEC**urity and **O**pen **M**ethodologies
- Originally a «security Think-Tank» (IdeaHamster, Est. 2000)
- Established on **January 2001**, founded by **Pete Herzog**
- Non-Profit Organization (C503) registered in the **USA** and **EU** with headquarters in **New York City** and **Barcellona** (Spain)
- **Open Source Community** registered OSI
- Developping **many Open Source projects** (i.e. HPP, HHS, BPB – ***see later***)
- **Coordinates** the **Certification** of the **Security Personnel**

HACKERS HPP PROFILING PROJECT

ISECOM INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Hacker Highschool hackerhighschool.org

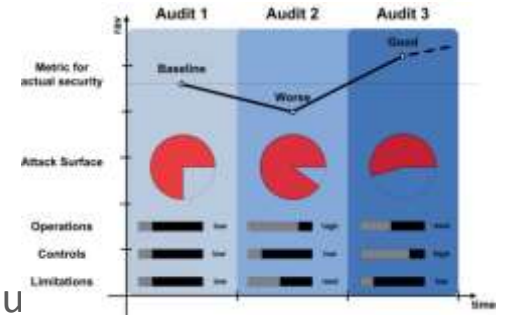
The ISECOM Mission

- 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 (OSSTMM, Security Metrics, HPP)**
  - **Professionals and quasi-professionals (Rules of Engagement, HPP)**
  - **College students (Academic Alliance Program)**
  - **Teens and pre-teens (Hacker High School, Bad People Project)**

The ISECOM Projects

- **OSSTMM** – The 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 Manu
- **STICK** – Software Testing Checklist
- **ISM 3.0** – Information Security Maturity Model
- **HHS** – Hacker High School
- **HPP** – Hacker's Profiling Project
- **BPB** – The Bad People Project

Hacker Highschool
SECURITY AWARENESS FOR TEENS

HACKERS HPP
PROFILING PROJECT

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

OSSTMM: introduction

- Our chief project is the **OSSTMM**.
- The **Open Source Security Testing Methodology Manual**
- **+ 3.000.000 downloads worldwide**
- Originally **designed by Pete Herzog** for **IBM ISS Force** (1998)
- It become an **Open Source project** in 2000 (December 18th)
  - **IT'S FREE! (http://www.osstmm.org for download)**
- The OSSTMM is **a methodology for testing security systems for everything**, from guards and locked doors to mobile communication towers and satellites.
  - **It just WORKS!** ☺

OSSTMM: details

- An **International Standard** for **Security Testing** and **Security Analysis**
- A **methodology** based on **a scientific approach**
- A **resource** in order to be **really measure** the **Operational Security**
- A way to **totally reduce** false positives and false negatives (forget «**Vulnerability Assessments**!!)
- A **concrete process** to be functional and **really secure**
- An **Ethics code** with clearly-defined **Rules of Engagement**
- **Released on December 14°, 2010, as its third release (OSSTMM 3.0)**

The Open Source Security Testing Methodology Manual (OSSTMM) is an open standard methodology for performing security tests. Since it's inception in January 2001, the OSSTMM has become the most widely used, peer-reviewed, comprehensive security testing methodology in existence. While other methodologies and best practices attack security testing from a 50,000 foot view, the OSSTMM focuses on the technical details of exactly which items need to be tested, what to do during a security test, and when different types of security tests should be performed. The OSSTMM provides testing methodologies for the following six security areas: Information Security, Process Security, Internet Technology Security, Communications Security, Wireless Security, and Physical Security.

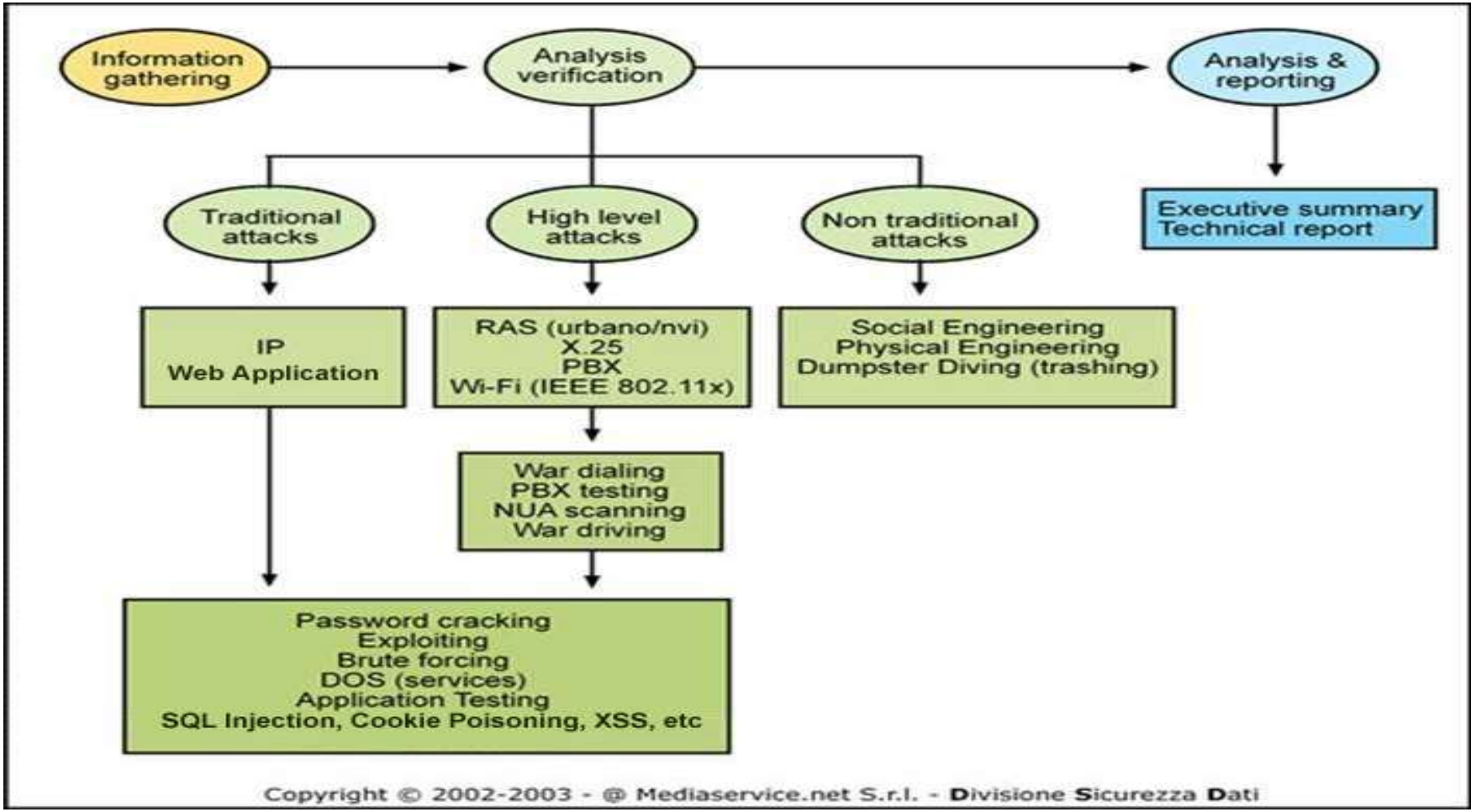
The Open Source Security Testing Methodology Manual

OSSTMM: how it works

- 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** (**RAV**s).
- 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:

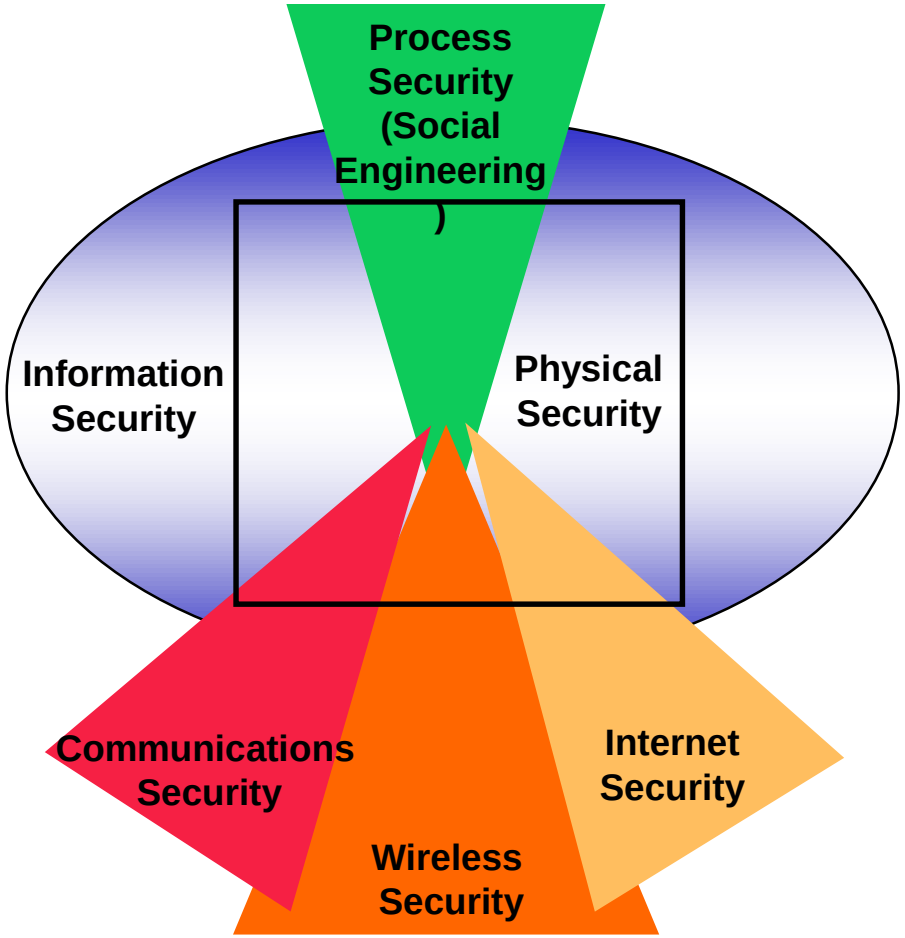
- Open Source project, +200 contributors worldwide, **free use of the methodology**
- Works on apparals, **infrastructures, single targets**
- Cross-standard: **IP(v4/V6), xSTN (PSTN, ISDN), X.25, mobile, Wireless (IEEE 802.11*, Bluetooth, Zigbee, ….)**
- Adopted by governative and private organizations **all around the world**
- Modular logic: **6 operating areas** (modules)

Security Testing: the "standard" approach



(since OSSTMM 2.0): the modules

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

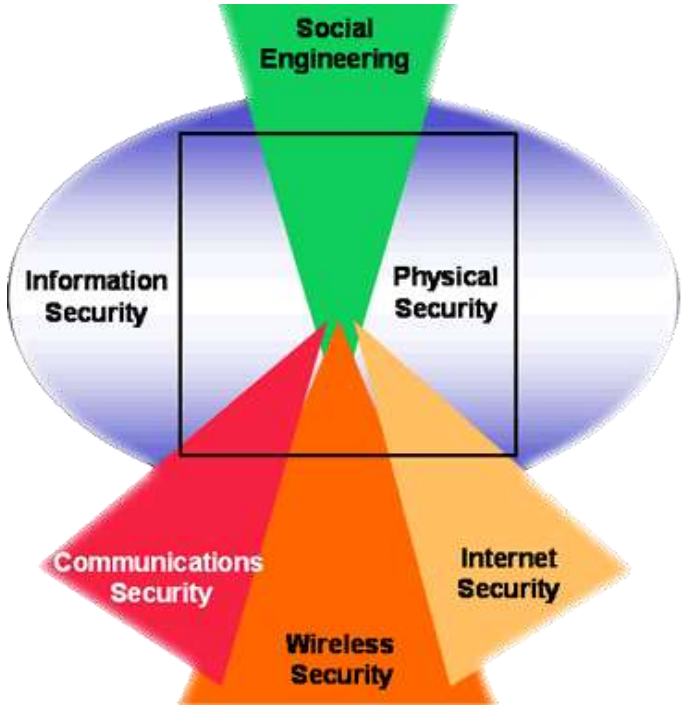


(since OSSTMM 2.0): operating areas

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

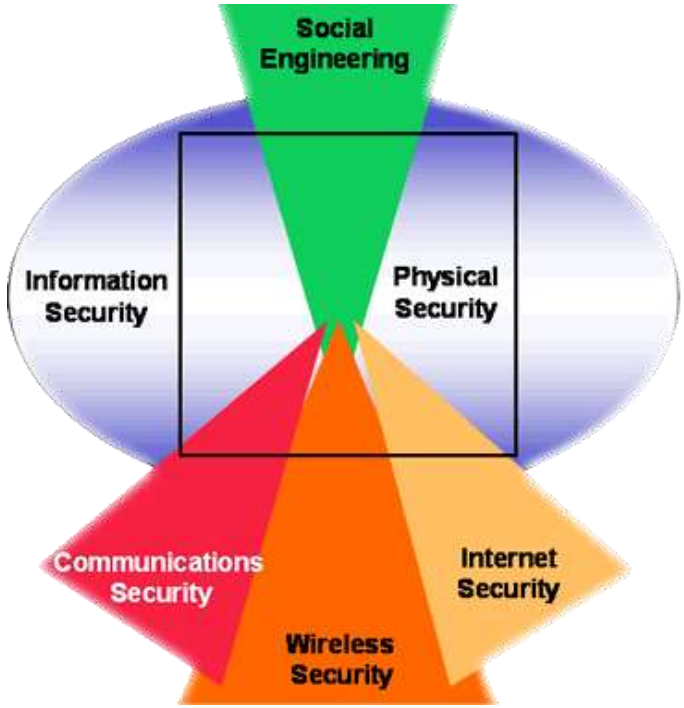


(since OSSTMM 2.0): operating areas (2)

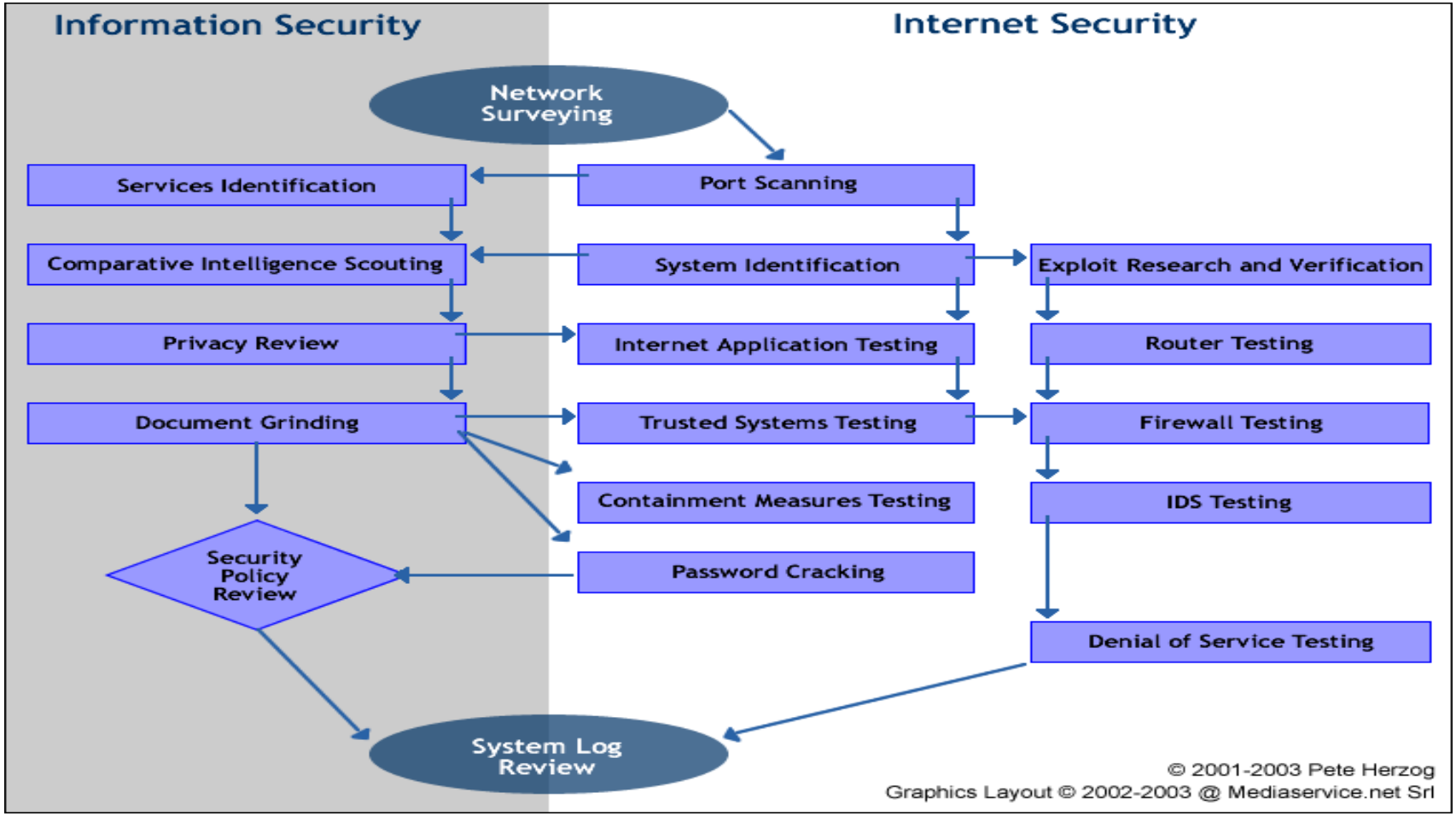
Wireless Security
- Wireless Networks Testing
- Cordless Communications Testing
- Privacy Review
- Infrared Systems Testing

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



Security Testing: the OSSTMM approach

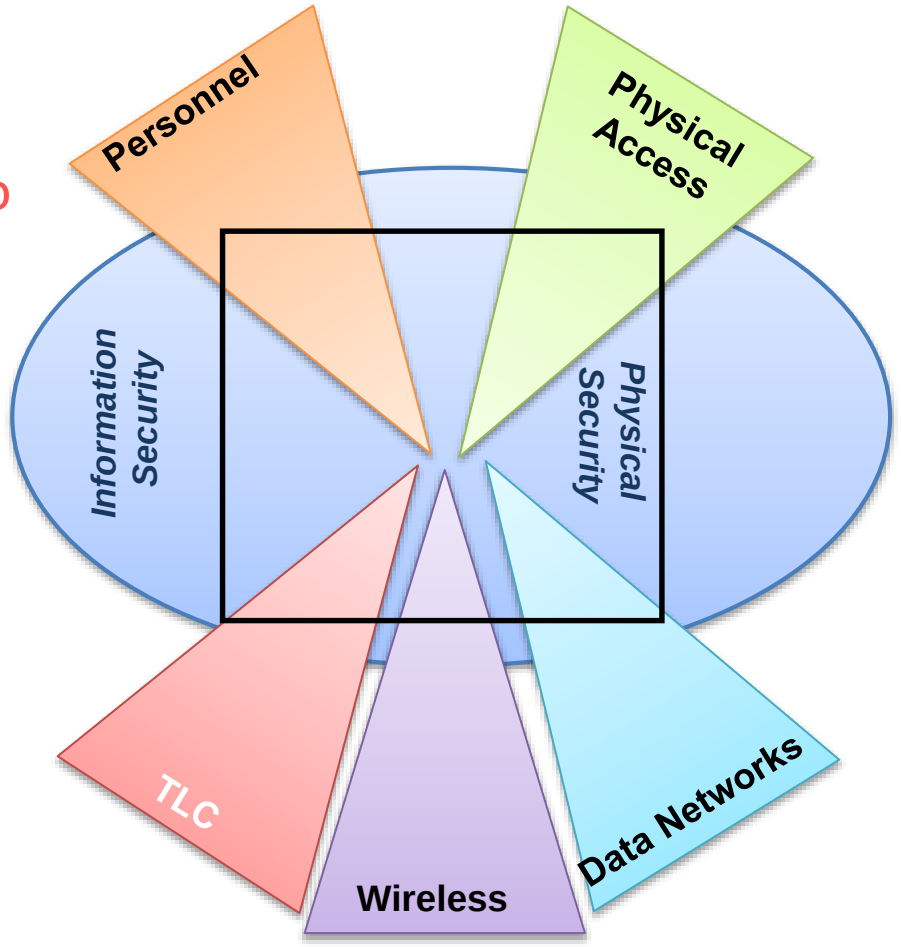


OSSTMM 3.0: Attack Channels (paths)

Each channel foreseen **a set of verifications**, which allows you to verify ALL of the relevant aspects to your security goals, such as:

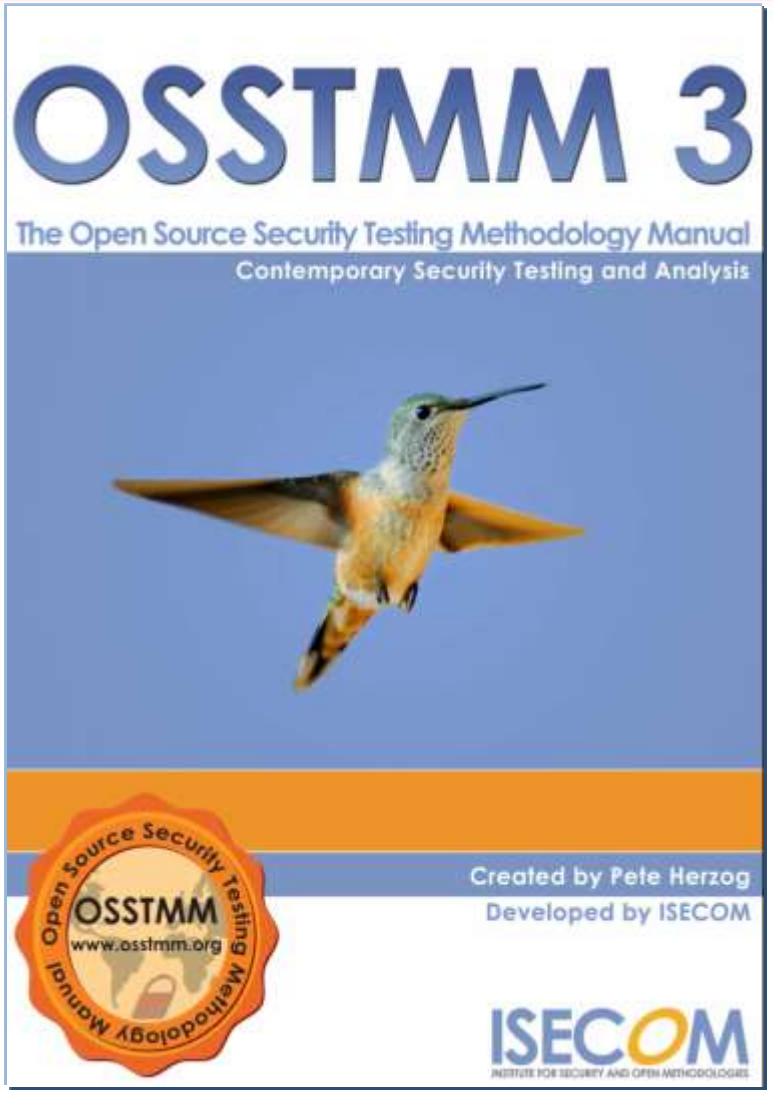
Data Networks:

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



The OSSTMM 3.0

- **Download it** from www.osstmm.org
- Designed for **e-book readers** and **double-sided printing** (we love the earth)
- 211 pages
- **Open Source**: Creative Commons 3.0 Attribution Non-commercial derives 2010



The core team

Primary Contributors

The following people are listed alphabetically by company. Each has been a substantial influence to the development of this OSSTMM.

ISECOM
- **Pete Herzog, Managing Director**
- **Marta Barceló, Director of Operations**
- **Richard Feist, ISECOM Board Member**
- **Robert E. Lee, ISECOM Board Member**
- **Cor Rosielle**
- **Raoul Chiesa, ISECOM Board Member**
- **Marco Ivaldi**
- **Fabrizio Sensibile**

adMERITia GmbH, Germany
- **Heiko Rudolph, ISECOM Board Member**
- **Aaron Brown**

Bell Canada, Canada
- **Rick Mitchell**

Dreamlab Technologies Ltd., Switzerland
- **Nick Mayencourt, ISECOM Board Member**
- **Adrian Gschwend**

GCP Global, Mexico
- **Francisco Puente**

KCT Data, Inc., USA
- **Kim Truett, ISECOM Board Member**

La Salle URL, Spain
- **Jaume Abella, ISECOM Board Member**

OneConsult GmbH, Switzerland
- **Christoph Baumgartner, ISECOM Board Member**

Lots of people helping the ISECOM community!

Contributions

Alberto Perrone
Martin Dion, Above Security, Canada
Lars Heidelberg, adMERITia GmbH, Germany
Martin Pajonk, adMERITia GmbH, Germany
Dru Lavigne, Carleton University, Canada
Todd A. Jacobs, Codegnome, USA
Phil Robinson, Digital Assurance, UK
Philipp Egli, Dreamlab Technologies Ltd., Switzerland
Daniel Hulliger, Dreamlab Technologies Ltd., Switzerland
Simon Nussbaum, Dreamlab Technologies Ltd., Switzerland
Sven Vetsch, Dreamlab Technologies Ltd., Switzerland
Colby Clark, Guidance Software, USA
Andy Moore, Hereford InfoSec, UK
Peter Klee, IBM, Germany
Daniel Fernandez Bleda, Internet Security Auditors, Spain
Jay Abbott, Outpost24 / Lab106, Netherlands
Steve Armstrong, Logically Secure, UK
Simon Wepfer, OneConsult GmbH, Switzerland
Manuel Krucker, OneConsult GmbH, Switzerland
Jan Alsenz, OneConsult GmbH, Switzerland
Tobias Ellenberger, OneConsult GmbH, Switzerland
Shaun Copplestone, The Watchers Inc., Canada
Ian Latter, Pure Hacking, Australia
Ty Miller, Pure Hacking, Australia
Jordi André i Vallverdú, La Caixa, Spain
Jim Brown, Thrupoint, USA
Chris Griffin, ISECOM, USA
Charles Le Grand, USA
Dave Lauer, USA
John Hoffoss, Minnesota State Colleges and Universities, USA
Mike Mooney, USA
Pablo Endres, Venezuela / Germany
Jeremy Wilde, compliancetutorial.com, UK / France
Rob J. Meijer, Netherlands
Mike Simpson, USA / Germany

Review and Assistance

Gunnar Peterson, Arctec Group, USA
Dieter Sarrazyn, Ascure nv., Belgium
Bob Davies, Bell Canada, Canada
Josep Ruano, Capside, Spain
Adrien de Beaupre, Canada
Clement Dupuis, CCCure, Canada
Armand Puccetti, CEA, France
Mike Vasquez, City of Mesa, USA
Jose Luis Martin Mas, davinci Consulting, Spain
Sylvie Reinhard, Dreamlab Technologies Ltd., Switzerland
Raphaël Haberer-Proust, Dreamlab Technologies Ltd., Switzerland
Josh Zelonis, Dyad Security, USA
Bora Turan, Ernst and Young, Turkey
Luis Ramon Garcia Solano, GCP Global, Mexico
John Thomas Regney, Gedas, Spain
Mike Aiello, Goldman Sachs, USA
Dirk Kuhlmann, HP, UK
John Rittinghouse, Hypersecurity LLC, USA
Massimiliano Graziani, IISFA, Italy
Jose Navarro, Indiseg, Spain
Timothy Phillips, Information Assurance Solutions, USA
Joan Ruiz, La Salle URL, Spain
Drexx Laggui, L&A Inc, Philippines
Víktu Pons i Colomer, La Salle URL, Spain
Roman Drahtmueller, Novell, Germany
Hernán Marcelo Racciatti, SICLABS, Argentina
Tom Brown, RWE Shared Services IS, UK
Marcel Gerardino, Sentinel, Dominican Republic
Manuel Atug, SRC Security Research & Consulting GmbH, Germany
Torsten Duwe, SUSE, Germany
Michael S. Menefee, WireHead Security, USA
Alexander J. Herzog, USA
Ruud van der Meulen, Netherlands
Chris Gatford, HackLabs, Australia
Wim Remes, Belgium

The OSSTMM 4.0

- **Under peer-review since June 12, 2013**
- **Join the peer review team (help us!)**
- **Become a ISECOM supporter (Gold, Silver, Bronze) and get it**
- **Wait 'till it'll get public**
- 255 pages
- **Open Source**: Creative Commons 3.1 Attribution Non-commercial derives 2013

OSSTMM 4

Contemporary Security Testing and Analysis

4.01 Draft Version for Team Members Only

Creative Commons 3.01 Attribution-NoDerivs 2013, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

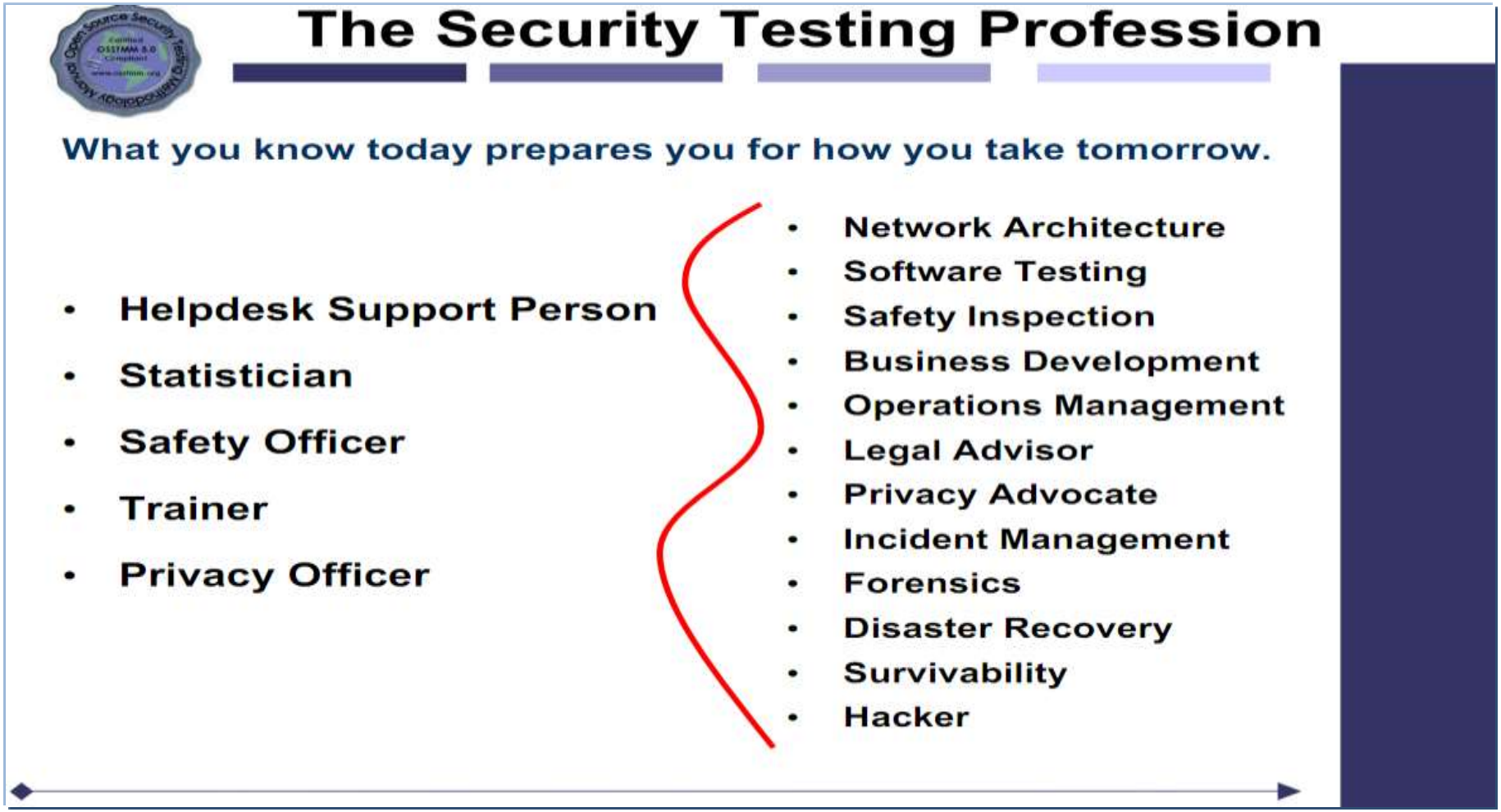
© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Issue #5: You can't always get it…

- You can't always test what should really be tested
  - Time constrains, Budget limitations
  - Legal Authorizations (your ISP? The Carrier? Cloud?)
  - Out of Scope
  - Entry points (i.e. RAS via PSTN/ISDN, X.25, VoIP, etc..)

- You may not be delivered with ALL of your exposures and vulnerabilities
  - Field Experiences from the Red Team
  - Lack of experience on specific sectors (i.e. SCADA&ICS, Automotive, Aiports, etc…)
  - No Test-bed = no party

Also, something you should know



Conclusions

End of story

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.

Links

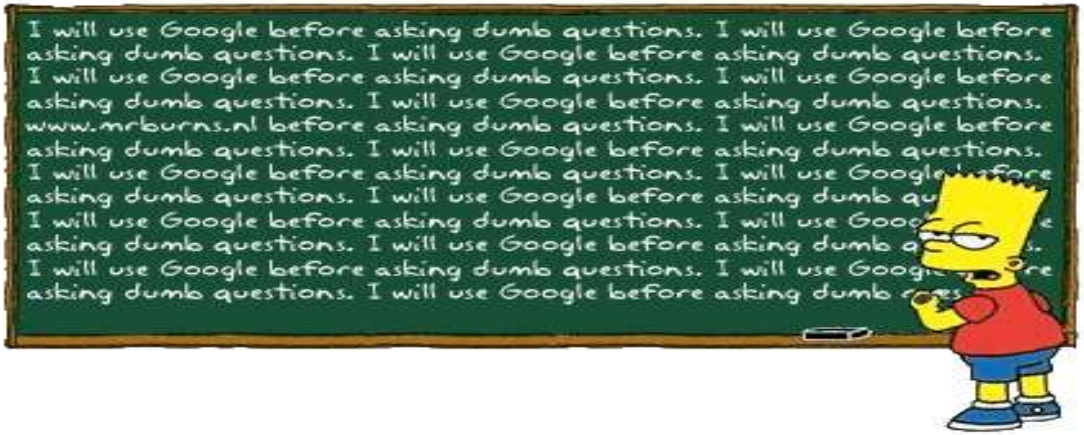
- www.isecom.org
- www.osstmm.org
- www.opsa.org
- www.opst.org
- www.opse.org
- www.owse.org
- www.hackerhighschool.org
- www.iso.org
- www.pcisecuritystandards.org
- attrition.org/dataloss

Contacts, Q&A

- **Need** anything, got **doubts**, wanna **ask me something**?
  - **raoul@ISECOM.org**
  - Public key: https://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?

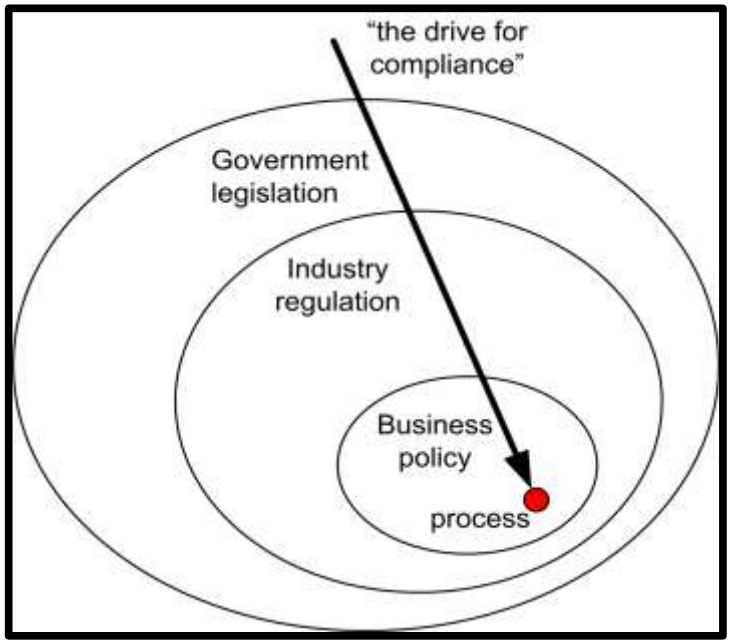


© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

EXTRA MATERIAL

OSSTMM Compliance

- **Legislation**. Compliance with legislation is **in accordance to region where the legislation can be enforced**. The strength and commitment to the legislation comes from its popularity and previously successful legal arguments and appropriately set and just enforcement measures. **Failure to comply to legislation may lead to criminal charges**.
- **Regulation**. Compliance to regulation is **in accordance to the industry or within the group where the regulation can be enforced**. Failure to comply with regulations most often leads to **dismissal from the group, a loss of privileges, a monetary fine, civil charges**, and in some cases where legislation exists to support the regulatory body, **criminal charges** can be made.
- **Policy**. Compliance to policy is **in accordance to the business or organization where the regulation can be enforced**. Failure to comply with policy most often leads to **dismissal from the organization, a loss of privileges, a monetary fine, civil charges**, and in some cases where legislation exists to support the policy makers, **criminal charges** can be made.



© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

OSSTMM for Audits

- Provides **Quantitative** and **Realistic Security Metrics**
- **Improves any** Risk Assessment or Risk Management Methodology
  - ISO 17799 / BS 7799 -> ISO/IEC 27001
  - Marion / Méhari (Risk Analysis methodology)
- Provides **calendaring of security tests** based on **natural degradation of security**
- **Quantifies** operational and actual risk types
- **Manages spending effectiveness**

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

OSSTMM going ISO….
(The new ISO "Hacking Standard")

- On May 2010, **ISO International Committee** requested ISECOM to supply deep details in order to start a process that will incorporate the OSSTMM into a new ISO standard for Security Testing.
- Here's extracts from the official ISECOM disclosure:

*"Some national standards organizations like **ANSI** in the USA and **UNINFO** in Italy have had their eye on the OSSTMM for years. Others, like **DIN** in Germany, were only recently shown the benefits of the OSSTMM but then supported it immediately.*

*Released for free in January 2001 by Pete Herzog as the underdog to the security industry's product-focused security advice, the manual achieved an instant cult following. The fact that OSSTMM is open to anyone for peer review and further research led to it growing from its **initial 12 page** release to its **current size of 200**.*

*The international support community also grew to over **7000 members** with dozens of research contributors dedicating their time to enhancing it. **For testing security operations and devising tactics it has no equal**. Its popularity and growth happened so fast that the non-profit organization ISECOM created the Open Methodology License (OML) asserting the OSSTMM as an open Trade Secret to assure it remained free, as in **no price, as well as free from commercial and political influence**. The OSSTMM seemed to have all the features of being the answer for securing the world except that it had never been formally recognized…until now."*

Mixing all together: different views and approaches, from ISO/IEC to OSSTMM and NIST

- The next section will highlight how ISECOM is closely working with ISO/IEC Committee and NIST Board of Directors in order to build a new, shared methodology for Security Testing and Product's Security Evaluation.
- You will recognize many of the aspects we've spoken about today, into a "big picture".
- All of the following process should be completed by 2015: this means we are already showing you what will came next.
- All the following slides belong to ISECOM and ISO/IEC JTC1/SC27 Working Group (see next slide)

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

ISO/IEC JTC1 SC27 numbers

- 20+ years of activity
- 59 national bodies represented
- 2 meetings per year
- 250 experts participating to the meetings (more to works)
- 97 published standards (27001 and 15408 as flagships)
- 5 vertical working groups
- 5 stages for standards approval (average 3 years path)
- 2/3 majority votes

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

SC27 WGs

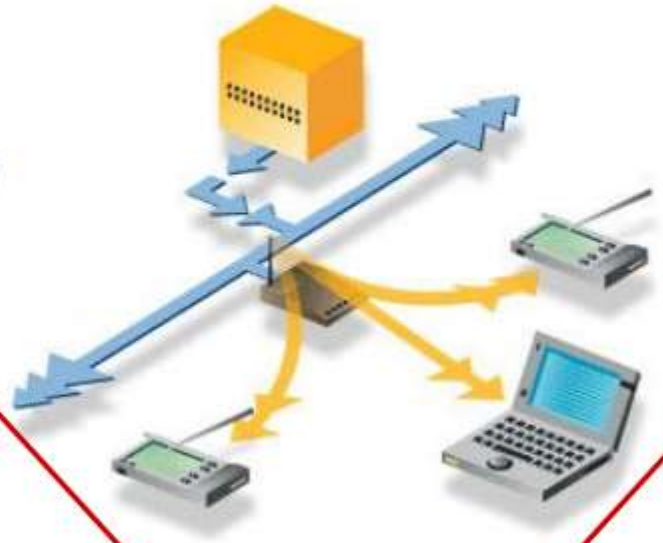

ISO
JTC1/SC27
IEC
WG1 - Information security management systems
WG2 - Cryptography and security mechanisms
WG3 - Security evaluation criteria
WG4 - Security controls and services
WG5 - Identity management and privacy technologies

Information Security Approach

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

ORGANIZATIONAL Approach

ISO/IEC 27001, COBIT , ITIL (ISO L.A., CISA)



MIXED Approach

PCI (ASV, QSA)

TECH Approach

OSSTMM, OWASP (OPSX, OWSE)

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

ISO/IEC 27001:2005

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Information Security Management System (ISMS)

An ISMS is designed to ensure the selection of security controls to protect information assets and give confidence to interested parties.

- Management System
- Scope flexibility
- Part of a complete framework of standards
  - 27002 Code of practice
  - 27003 Implementation guidelines
  - 27004 Measurements
  - 27005 Information Security Risk Management
  - 2701X Sector Specific, 2703X Technical Guides
- Universally recognized
- Indicates **what** to do, not **how** to do
- It is certifiable

MSS Approach

NIST SP800-115

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Technical Guide to Information Security Testing and Assessment

1. Introduction
- 1.1 Authority
- 1.2 Purpose and Scope
- 1.3 Audience
- 1.4 Document Structure

2. Security Testing and Examination Overview
- 2.1 Information Security Assessment Methodology
- 2.2 Technical Assessment Techniques
- 2.3 Comparing Tests and Examinations
- 2.4 Testing Viewpoints

3. Review Techniques
- 3.1 Documentation Review
- 3.2 Log Review
- 3.3 Ruleset Review
- 3.4 System Configuration Review
- 3.5 Network Sniffing
- 3.6 File Integrity Checking
- 3.7 Summary

4. Target Identification and Analysis Techniques
- 4.1 Network Discovery
- 4.2 Network Port and Service Identification
- 4.3 Vulnerability Scanning
- 4.4 Wireless Scanning
- 4.5 Summary

5. Target Vulnerability Validation Techniques
- 5.1 Password Cracking
- 5.2 Penetration Testing
- 5.3 Social Engineering
- 5.4 Summary

6. Security Assessment Planning
- 6.1 Developing a Security Assessment Policy
- 6.2 Prioritizing and Scheduling Assessments
- 6.3 Selecting and Customizing Techniques
- 6.4 Assessment Logistics
- 6.5 Assessment Plan Development
- 6.6 Legal Considerations
- 6.7 Summary

7. Security Assessment Execution
- 7.1 Coordination
- 7.2 Assessing
- 7.3 Analysis
- 7.4 Data Handling

8. Post-Testing Activities
- 8.1 Mitigation Recommendations
- 8.2 Reporting
- 8.3 Remediation/Mitigation

Annexes

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Other Standards

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Evolution Timeline

- **Early 2009**
  - Maturation of the idea to have **OSSTMM transposed as an ISO/IEC standard**, contacts with Pete and with SC27 secretariat
- **Beijing 2009**
  - Presentation to WG1 and preliminary discussion within 27008
- **Redmond 2009**
  - Submission of a proposal for integration in 27008 either as:
    - Text and Annex
    - 27008-2
    - New linkedstandard
  - Block by WG1, contacts with WG4

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Evolution Timeline

- **Malaka 2010**
  - Presentation to WG3 and WG4
  - Approval of a 1-year study period on Security Testing Methodology by WG3
- **Berlin 2010**
  - Submission of a proposal for using OSSTMM as a base for the Security Testing NWIP
  - Observations from other NB (AU, UK, NZ) to include other standards
- **Singapore 2011**
  - **Submission of a proposal for NWIP based on OSSTMM and NIST SP800-115**

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

Work path to the NWIP

1: OSSTMM Selection

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

1. What You Need to Know
- 1.1 Security
- 1.2 Controls
- 1.3 Information Assurance Objectives
- 1.4 Limitations
- 1.5 Actual Security
- 1.6 Compliance

2. What You Need to Do
- 2.1 Defining a Security Test
- 2.2 Scope
- 2.3 Common Test Types
- 2.4 Rules Of Engagement
- 2.5 The Operational Security Testing Process
- 2.6 Four Point Process
- 2.7 The Trifecta
- 2.8 Error Handling
- 2.9 Disclosure

3. Security Analysis
- 3.1 Critical Security Thinking
- 3.2 Recognize the OpSec Model
- 3.3 Look for Pattern Matching as a Sign of Errors
- 3.4 Characterize the Results
- 3.5 Look for Signs of Intuition
- 3.6 Transparent Reporting

4. Operational Security Metrics
- 4.1 Getting to Know the Rav
- 4.2 How to Make a Rav
- 4.3 Turning Test Results into an Attack Surface Measurement
- 4.4 The Operational Security Formula
- 4.5 The Controls Formula
- 4.6 The Limitations Formula
- 4.7 The Actual Security Formula

5. Trust Analysis
- 5.1 Understanding Trust
- 5.2 Fallacies in Trust
- 5.3 The Ten Trust Properties
- 5.4 The Trust Rules
- 5.5 Applying Trust Rules to Security Testing

6. Work Flow
- 6.1 Methodology Flow
- 6.2 The Test Modules
- 6.3 One Methodology

7. Human Security Testing

8. Physical Security Testing

9. Wireless Security Testing

10. Telecommunications Security Testing

11. Data Network Security Testing

12. Compliance

13. Reporting with the STAR

14. What do you get
- 14.1 The Möbius Defense
- 14.2 Get What We Need

15. Open methodology license

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

1: NIST Selection

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

1. Introduction
- 1.1 Authority
- 1.2 Purpose and Scope
- 1.3 Audience
- 1.4 Document Structure

2. Security Testing and Examination Overview
- 2.1 Information Security Assessment Methodology
- 2.2 Technical Assessment Techniques
- 2.3 Comparing Tests and Examinations
- 2.4 Testing Viewpoints

3. Review Techniques
- 3.1 Documentation Review
- 3.2 Log Review
- 3.3 Ruleset Review
- 3.4 System Configuration Review
- 3.5 Network Sniffing
- 3.6 File Integrity Checking
- 3.7 Summary

4. Target Identification and Analysis Techniques
- 4.1 Network Discovery
- 4.2 Network Port and Service Identification
- 4.3 Vulnerability Scanning
- 4.4 Wireless Scanning
- 4.5 Summary

5. Target Vulnerability Validation Techniques
- 5.1 Password Cracking
- 5.2 Penetration Testing
- 5.3 Social Engineering
- 5.4 Summary

6. Security Assessment Planning
- 6.1 Developing a Security Assessment Policy
- 6.2 Prioritizing and Scheduling Assessments
- 6.3 Selecting and Customizing Techniques
- 6.4 Assessment Logistics
- 6.5 Assessment Plan Development
- 6.6 Legal Considerations
- 6.7 Summary

7. Security Assessment Execution
- 7.1 Coordination
- 7.2 Assessing
- 7.3 Analysis
- 7.4 Data Handling

8. Post-Testing Activities
- 8.1 Mitigation Recommendations
- 8.2 Reporting
- 8.3 Remediation/Mitigation

Annexes

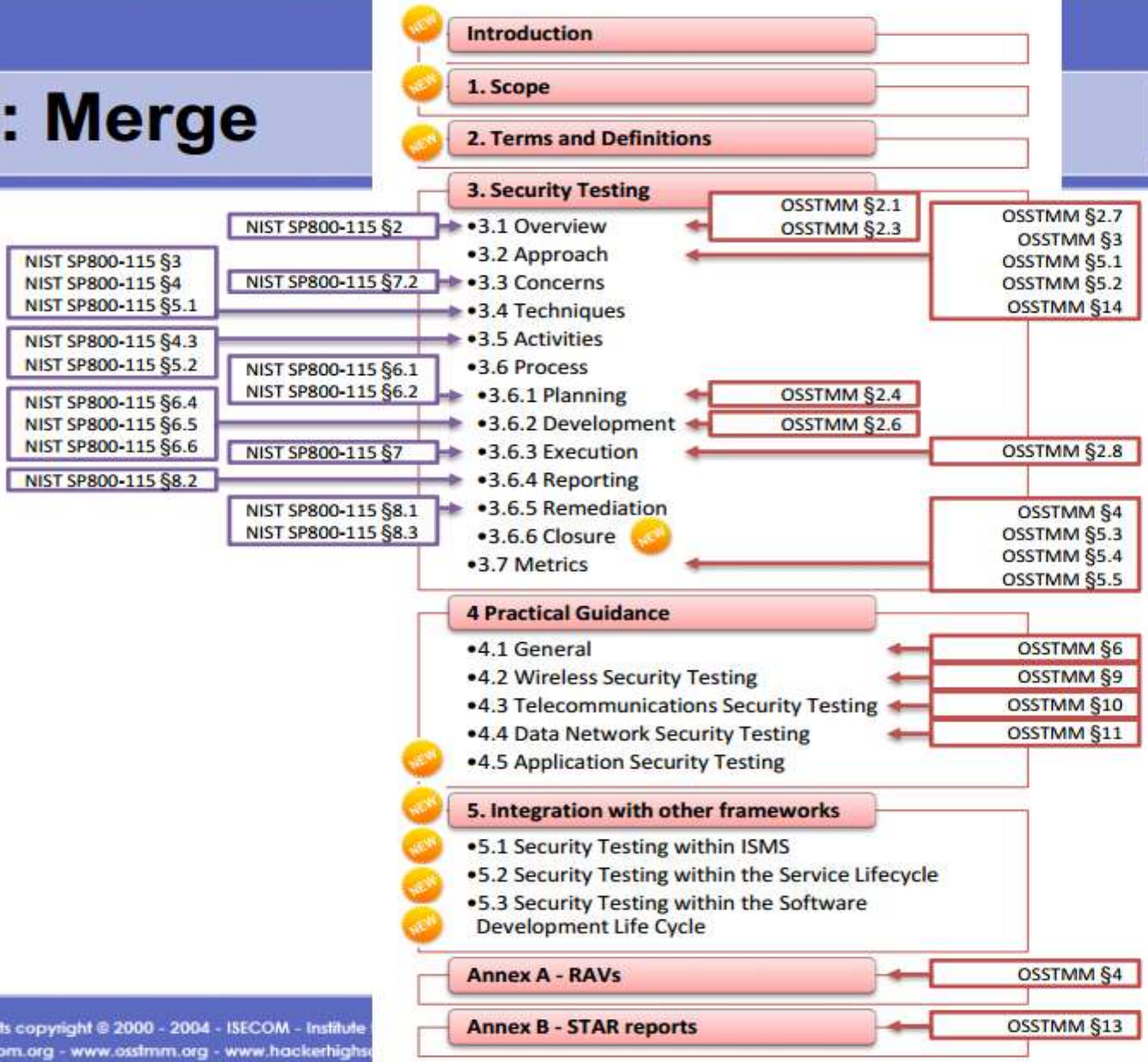
2: Modification

OSSTMM had many terms with different definitions than ISO, NIST didn't

Kept Terms	Changed Terms
• Anomaly	• Actual security
• Attack Surface	• Attack vector
• Continuity	• Channel
• Concern	• Limitations
• Exposure	• Loss control
• Indemnification	• Non-repudiation
• Porosity	• Operational security
• Resilience	• Operations
• Subjugation	• Privacy
• Target	• Safety
• Weakness	• Security
	• Trust
	• Vector
	• Vulnerability

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

3: Merge



All contents copyright © 2000 - 2004 - ISECOM - Institute
www.isecom.org - www.osstmm.org - www.hackerhighs

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni
NIC, ISACA & CERT LATVIA Conference - Riga, October 1st, 2015

4: New contents

A small amount of new contents has already been introduced, like

- **Testing phases**
- **Testing deliverables**

There are placeholders for new sections, which are:

1. **Integration with other frameworks**
2. **Testing techniques**
3. **Software security**
4. **Testing process and continuous improvement**

© 2015 Raoul Chiesa / Security Brokers Società Cooperativa per Azioni

What in the future?

Such a proposal, if becomes standard, could represent:

- **The reference for the market**
- **An increase of the attention on the subject**
- **A crossed strengthener among security standards and best practices**

2015 could be a possible approval date

A parallel path with OSSTMM should be held, allowing cross feedbacks but with mostly separate teams