OSSTMM V 2.1

Eduardo Jorge Feres Serrano Neves eth0

www.h2hc.com.br

ISECOM

- **What is it?**
  Institute for Security and Open Methodologies.
- **Which the proposal?**
  We are dedicated to providing practical security awareness, research, certification and business integrity.
- **Which the area of performance?**
  EUA, EUROPA

OSSTMM

- **A little of history:** The OSSTMM was created with intention of only citing norms and methodologies for the security community, but, as she got a great success, today it ja counts on two valid certficações: OSSTMP and OSSTMA, and its recognition through the world all.

OSSTMM

- **Where it consists?**

  - Professional standard for security tests
- **Which the objective?**

  - To create methodologies for security tests
- **Publish Target?**

  - Professionals of security area or people with knowledge in the area

OSSTMM

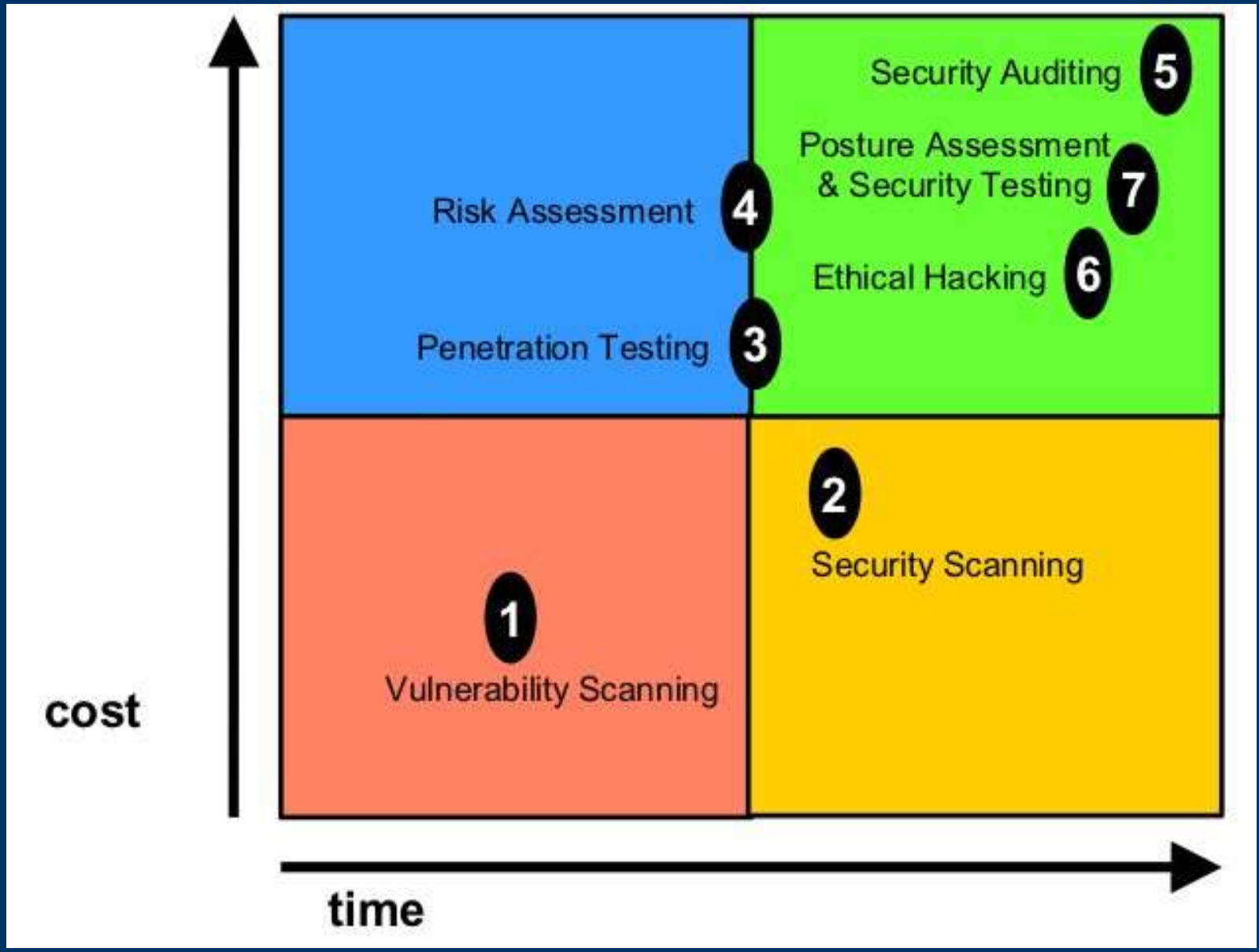
- **Validity of the test?**

  - It must follow some standards to be considered by the ISECOM

Standards of the ISECOM

- Quantifiable
- Based on the merit of the tester and analyst not on brand
- Consistent and repeatable
- Thorough
- Valid beyond the “now” time frame
- Compilant to individual and local laws and the human right to privacy

Cost X Time


Security Auditing
5
Posture Assessment
& Security Testing
7
Risk Assessment
4
Ethical Hacking
6
Penetration Testing
3
2
Security Scanning
1
Vulnerability Scanning
cost
time

Cost X Time

- Vulnerability Scanning
- Security Scanning
- Penetration Testing
- Risk Assessment
- Security Auditing
- Ethical Hacking
- Security Testing

Compliance

- It follows norms and laws created for the countries
- **Austria**

  - Austria Data Protection act 2000
- **USA**

  Federal Information Security Management act.

  USA Government Information Security Reform

  Children's Online Privacy Protection act (COPPA)

Compliance

- **Germany**

  Deutsche Bundesdatenschutzgezets (BDSG)
- **Spain**

  Spanish LOPD ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal Art. 15 LOPD – Art 5

  LSSICE

Compliance

- **Canada**

  Corporate Governance

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

  UK data Protection Act 1998

  Corporate Governance

Compliance

- **Australia**

  Privacy Act Amendments of Australia

  National Privacy Principle(NPP)

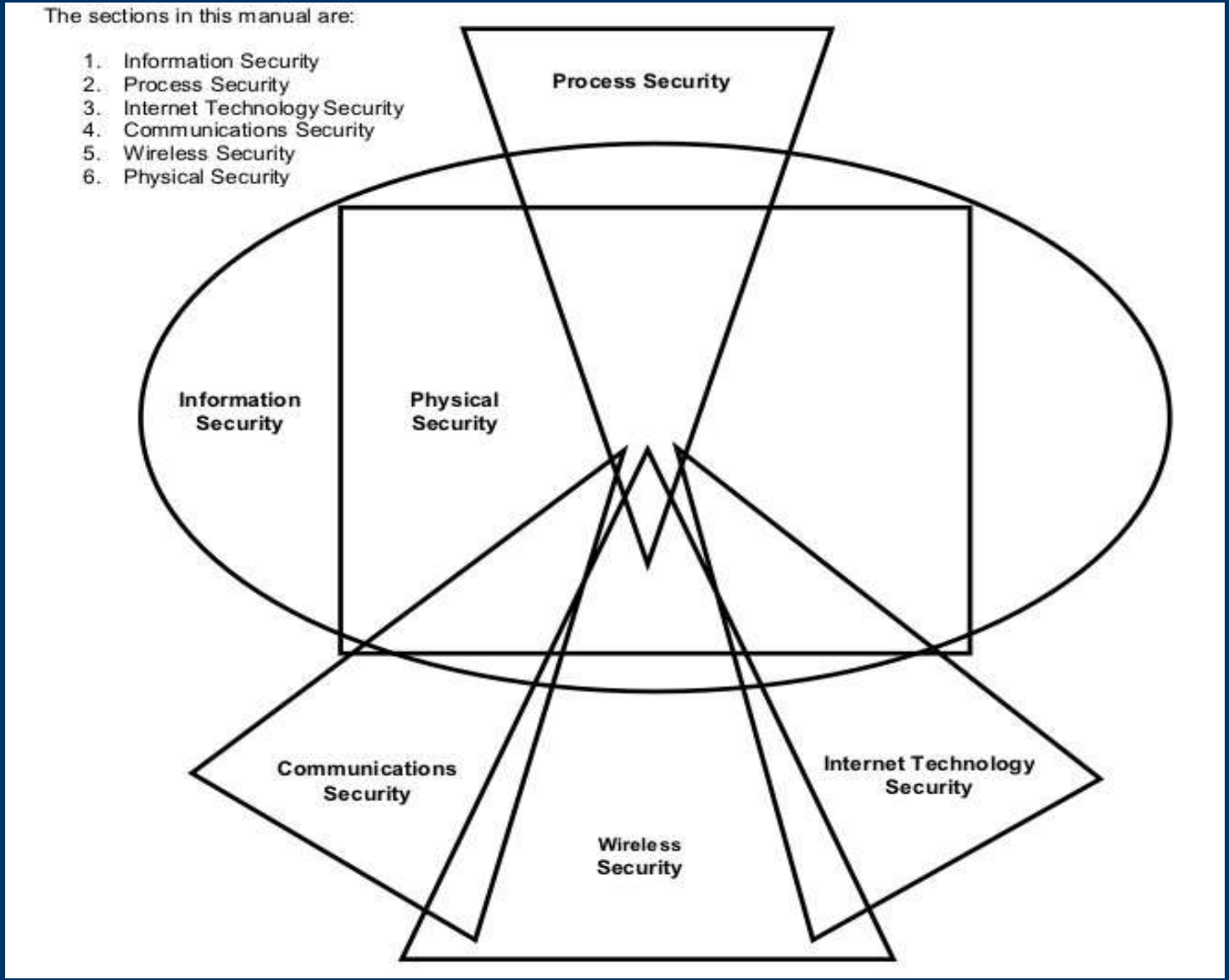
Best Pratices

- IT Information Libary
- Germany: IT Baseline Protection Manual
- German IT Systems
- ISO 17799-2000
- GAO/FISCAM
- SET
- NIST
- MTRE

Process

- Visibility
- Access
- Trust
- Authentication
- Non-Repudiation
- Confidentiality
- Privacy
- Authorization
- Integrity
- Safety
- Alarm

The Security Map



The Security Map

- **Information Security Testing**
  - Posture Assesssment
  - Information Integrity Review
  - Intelligence Survey
  - Competitive Intelligence Scouting
  - Human Resources Review
  - Privacy Control Review
  - Information Controls Review

The Security Map

- **Process Security Testing**
  - Posture Review
  - Request Testing
  - Reverse Request Testing
  - Trusted Persons Testing

The Security Map

- **Internet Technology Security Testing**
  - Logistic and Controls
  - Posture Review
  - Intrusion Detection Review
  - Network Surveying
  - System Service Identification
  - Competitive Intelligence Scouting
  - Privacy Review
  - Document Grinding

The Security Map

- **Internet Technology Security Testing(cont)**
  - Internet Application Testing
  - Exploit Research and Verification
  - Routing
  - Trusted System Testing
  - Access Control Testing
  - Password Cracking
  - Containment Measures
  - Denial of Service Testing

The Security Map

- **Internet Technology Security Testing(cont)**
  - Security Policy Review
  - Alarm and Logs Review

The Security Map

- **Communications Security Testing**
  - Posture Review
  - PBX Testing
  - Voice Mail Testing
  - FAX Testing
  - Modems Survey

The Security Map

- **Wireless Security Testing**
  - Posture Review
  - Electromagnetic Radiation Testing
  - 802.11 Wireless Network Testing
  - Bluetooth Network Testing
  - Wireless Input Device Testing
  - Wireless Handheld Testing
  - Cordless Communication Testing
  - Wireless Surveillance Testing

The Security Map

- **Wireless Security Testing(cont)**
  - Wireless Transaction Device Testing
  - RFID Testing
  - Infrared Testing
  - Privacy Review

The Security Map

- **Physical Security Testing**
  - Access Controls Testing
  - Perimeter Review
  - Monitoring Review
  - Alarm Response Review
  - Location Review
  - Environment Review

Risk Evaluation

- Security
- Privacy
- Practicality
- Usability

““Perfect Security””

- **Internet Gateway and Services**
  - No unencrypted remote access
  - No unauthenticated remote access
  - Restriction deny all allow specifically
  - Monitor it all and log it
  - Decentralize
  - Limit inter-system trust
  - Quarantine all inputs and validate them

““Perfect Security””

- **Internet Gateway and Services(cont)**
  - Install only the applications / daemons necessary
  - Layer the security
  - Invisible is best show only necessary
  - Simplicity prevents configuration errors
- **Mobile Computing**
  - Quarantine all inputs and validate them

““Perfect Security””

- **Mobile Computing (cont)**
  - No unencrypted remote access
  - No unauthenticated remote access
  - Encrypt accordingly
  - Install only the applications / daemons necessary
  - Invisible is best show only necessary
  - BIOS password required
  - Security Training

““Perfect Security””

- **Applications**

  - Usability of security features should be a strength
  - Assure bussiness justifications for all inputs and outputs
  - Validate all inputs
  - Limit trust (System and User)
  - Encrypt data

““Perfect Security””

- **Applications(cont)**
  - Hash the components
  - All acctions occur on the server side
  - Layer the security
  - Invisible is best show only necessary
  - Trigger it to alarm

““Perfect Security””

- **People**

  - Decentralized authority
  - Person responsability
  - Personal security and privacy controls
  - Trained in defined legalities and ethics from security policys
  - Limit access to information and infrastructure

Risk Assessment Values

- **RAVs**
- **Definition of RAVs**

  1 – Degree of degradation of each module is individual

  2 – Definition of a time cycle

  3 – It has you influence of others modules?

  4 – Establish weights

  5 – Type: identified, verified and not applied

Risk Types

- Vulnerability
- Weakness
- Concem
- Information Leak
- Unknown

	Verified	Identified	Not Applicable
Vulnerability	3.2	1.6	0.4
Weakness	1.6	0.8	0.3
Concern	0.8	0.4	0.2
Information Leak	0.4	0.2	0.1
Unknown	0.2	0.1	–

Section and Modules

- The divided methodology and in modules, sessions and tasks
- Sessions are the points of the map of the security
- Module is the flow of the methodology
- Tasks are inputs and outputs of data of the Modules

Modules and Tasks

- Example of Module

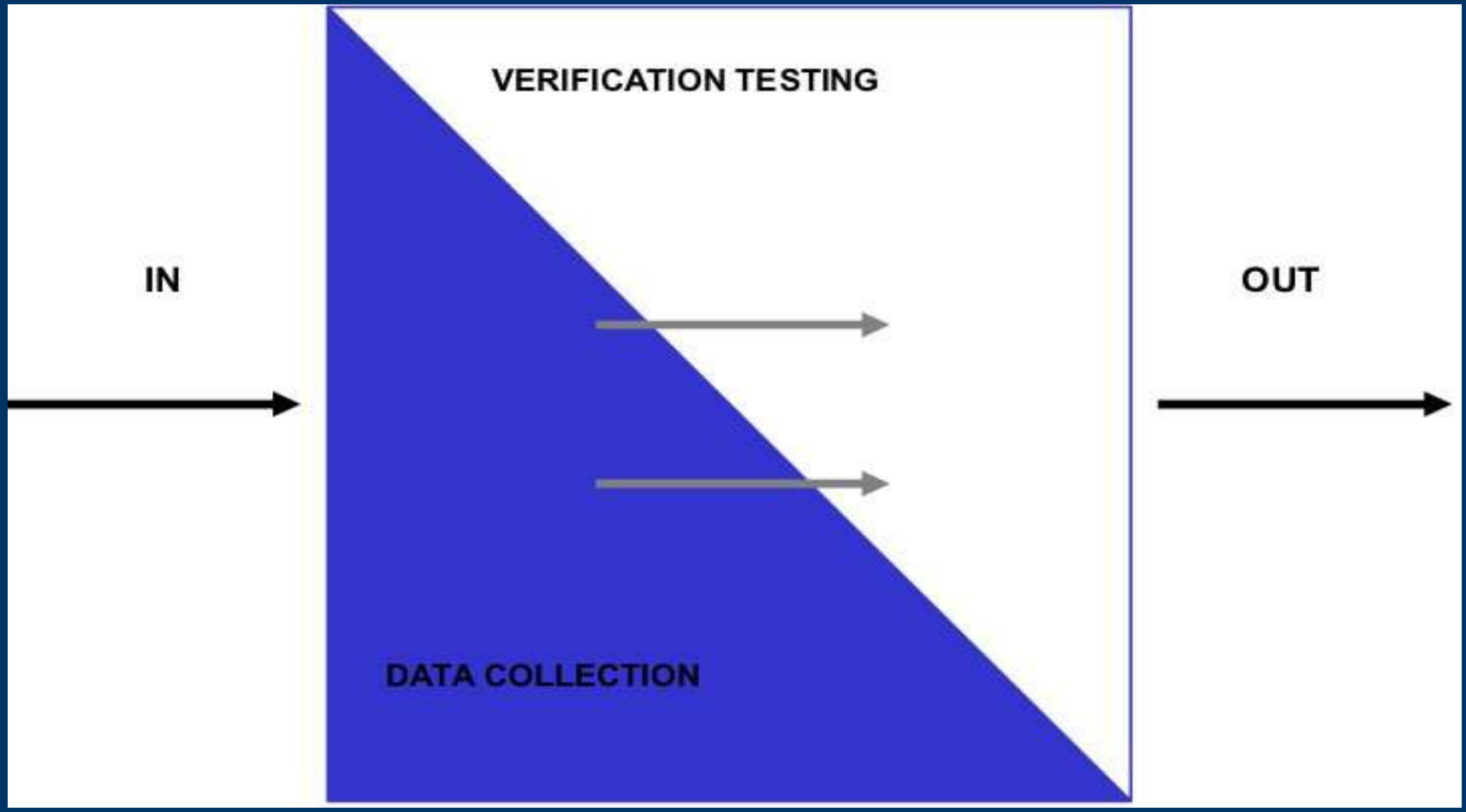
Module Name
Description of the module.

Expected Results:	Item Idea Concept Map

Group task description.
- Task 1
- Task 2

Methodology

- Diagram of the methodology



The end!!

Eduardo Jorge Feres Serrano Neves - eth0
eduardo@securityopensource.org.br
serrano.neve@gmail.com.br