Centro de
Investigación en
Computación

OSSTM

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Metodología
3. Resumen

Introducción

Generalidades

Resumen

Introducción

Generalidades

OSSTMM (*Open Source Security Testing Methodology Manual*)

- Desarrollado por el ISECOM

  ***I**nstitutte for **Se**curity and **O**pen **M**ethodologies*

- Versiones:
  - 2.0, 2.1, Años 2000-2002
  - 3.0, This current version is published on Tuesday, December 14, 2010.
- **Fuentes**
  - https://www.isecom.org/
  - https://www.isecom.org/OSSTMM.3.pdf (213 páginas)
  - Muchos videos:

    https://www.youtube.com/user/OWASPGLOBAL/videos

Introducción

Generalidades

OSSTMM

The Open Source Security Testing Methodology Manual is a complete methodology for penetration and security testing, security analysis and the measurement of operational security towards building the best possible security defenses for your organization.

RAV Calculator

A calculation sheet to simplify making ravs, the standard security metrics for measuring the Attack Surface of anything. It's necessary for completing the STAR.

STAR Sheet

The Security Test Audit Report (STAR) is a standardized summary of the results of a security or penetration test providing precise calculations of the Attack Surface, details of what was tested and how, and indemnification for testing organization. The STAR is required when OSSTMM certifying the security of an organization.

Introducción

Generalidades

Certificaciones

OPST

The OSSTMM Professional Security Tester proves a candidate has the skill and knowledge to perform accurate & efficient security tests on data networks.

http://www.opst.org

OPSA

The OSSTMM Professional Security Analyst proves a candidate can apply the principles of security analysis and attack surface metrics accurately & efficiently.

http://www.opsa.org

OPSE

The OSSTMM Professional Security Expert proves a candidate has learned all the security concepts within the most current, publicly available OSSTMM and the background to the research.

http://www.opse.org

OWSE

The OSSTMM Wireless Security Expert proves a candidate has the skill and knowledge to analyze and test the operational security of wireless technologies across the electromagnetic spectrum accurately & efficiently.

http://www.owse.org

CTA

The Certified Trust Analyst proves a candidate has the skills and knowledge to efficiently evaluate the trust properties of any person, place, thing, system, or process and make accurate and efficient trust decisions.

http://www.trustanalyst.org

Descripción de la Metodología

Definiciones

Resumen

OSSTM

Intro

- The primary purpose of this manual is to provide a scientific methodology for the accurate characterization of operational security (OpSec) through examination and correlation of test results in a consistent and reliable way.
- This manual is adaptable to almost any **audit type**, including:
    1. Penetration tests
    2. Ethical hacking
    3. Security assessments
    4. Vulnerability assessments
    5. Red-teaming
    6. Blue-teaming, and so forth.
- It is written as a security research document and is designed for factual security verification and presentation of metrics on a professional level.
- A secondary purpose is to provide guidelines which, when followed correctly, will allow the analyst to perform a **certified** OSSTMM audit.

OSSTM

Intro

Definiciones

Term	Definition
Attack Surface	The lack of vector.
Attack Vector	A sub-scope of a comple conquer alg down a pro type, until th
Controls	Impact and information various typ example, in prevent the equivalent v controls are relevant to information
Limitations	This is the operations, classified by level. Theref perform, an rusted lock imposed se necessary t and weak th Determining successful c One of its li operational
Operations	Operations public, oper or services t going in and
Perfect Security	The exact b
Porosity	All interacti Access, or Tr

Term	Definition
Safety	A form of p to be safe, effects of owner or m means to m
Security	A form of p the threat. asset or th threat or th from an operating c
Rav	The rav is uncontrolle quantitativ scale, 100 anything le More than be a probl complexity
Target	That within asset and c
Vector	The directio
Vulnerability	One classi deny acce and examp

1.2 Controls

When the threat is all around then it is controls which will provide safety in operations. Controls are a means to influence the impact of threats and their effects when interaction is required.

Just because you can't directly control it doesn't mean it can't be controlled. Control the environment and you control everything in it.

Interactive Controls

The Class A Interactive Controls mak
influence visibility, access, or trust inte
Subjugation, Continuity, and Resilienc

1. **Authentication** is a control tl
authorization.
2. **Indemnification** is a control t
party. This contract may be in
rules are not followed, spec
provider in case of damages l
3. **Resilience** is a control over c
corruption or failure.
4. **Subjugation** is a control assuri
asset owner defines how the i
liability of loss from the interac
5. **Continuity** is a control over c
corruption or failure.

Process Controls

The other half of operation controls a
These controls do not directly influe
present. These are also known as Pro
Integrity, and Alarm.

6. **Non-repudiation** is a control
interactivity.
7. **Confidentiality** is a control fo
parties cannot be known outsi
8. **Privacy** is a control for assurin
between parties cannot be kr
9. **Integrity** is a control to assur
changed.
10. **Alarm** is a control to notify tha

OSSTM

Intro

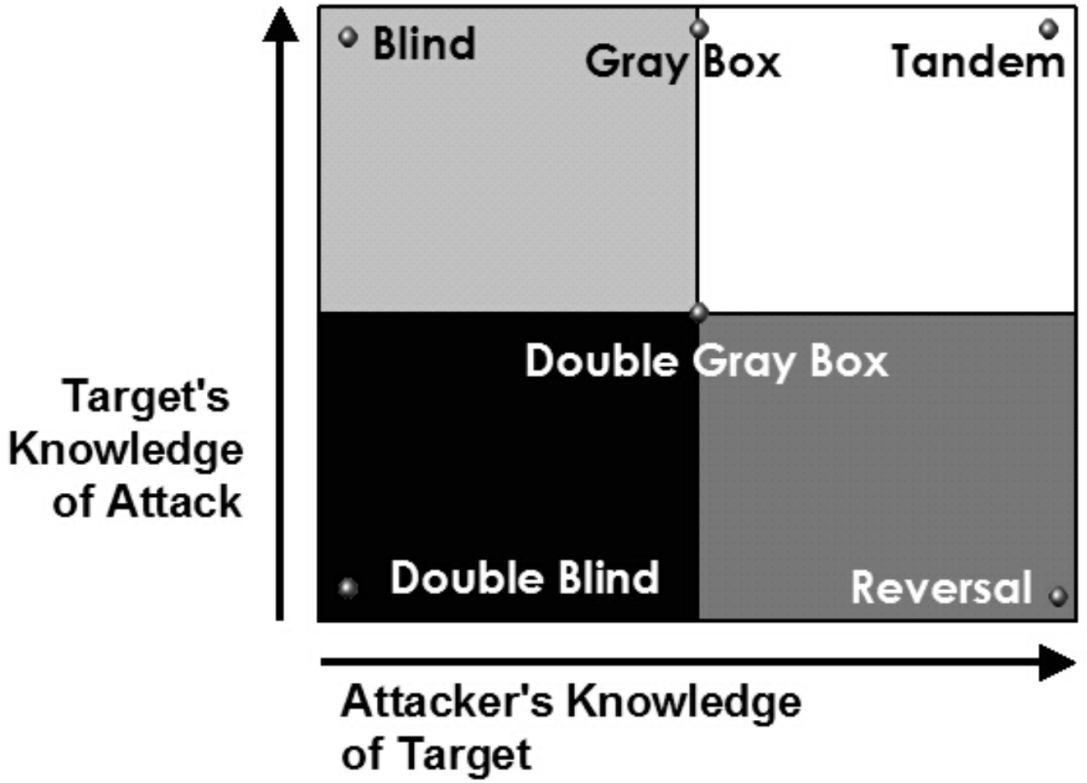
Channels

Class	Channel	Description
Physical Security (PHYSSEC)	Human	Comprises the human element of communication where interaction is either physical or psychological.
	Physical	Physical security testing where the channel is both physical and non-electronic in nature. Comprises the tangible element of security where interaction requires physical effort or an energy transmitter to manipulate.
Spectrum Security (SPECSEC)	Wireless	Comprises all electronic communications, signals, and emanations which take place over the known EM spectrum. This includes ELSEC as electronic communications, SIGSEC as signals, and EMSEC which are emanations untethered by cables.
Communications Security (COMSEC)	Telecommunications	Comprises all telecommunication networks, digital or analog, where interaction takes place over established telephone or telephone-like network lines.
	Data Networks	Comprises all electronic systems and data networks where interaction takes place over established cable and wired network lines. Data Networks

OSSTM

Intro

Common Test Types



OSSTM

Intro

PDF

Capítulos

7. Human Security Testing, pags. 105 – 119, 14 pp.
8. Physical ST, pags. 120 – 137, 17 pp.
9. Wireless ST, pags. 138 – 150, 12 pp.
10. Telecommunications ST, pags. 151 – 166, 15 pp.
11. Data Networks ST, pags. 167 – 184, 17 pp.

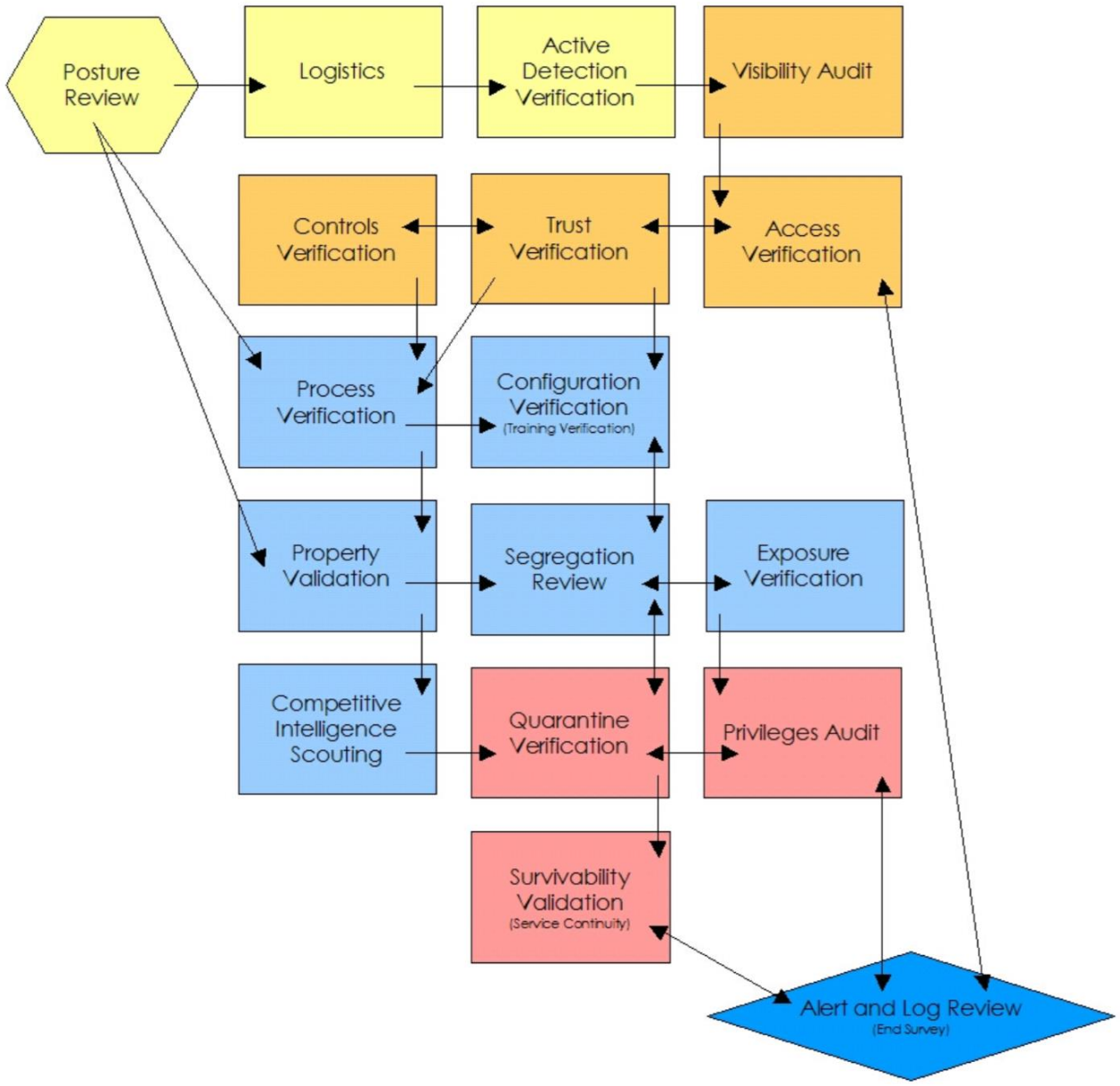
Total 75 páginas

OSSTM

Intro

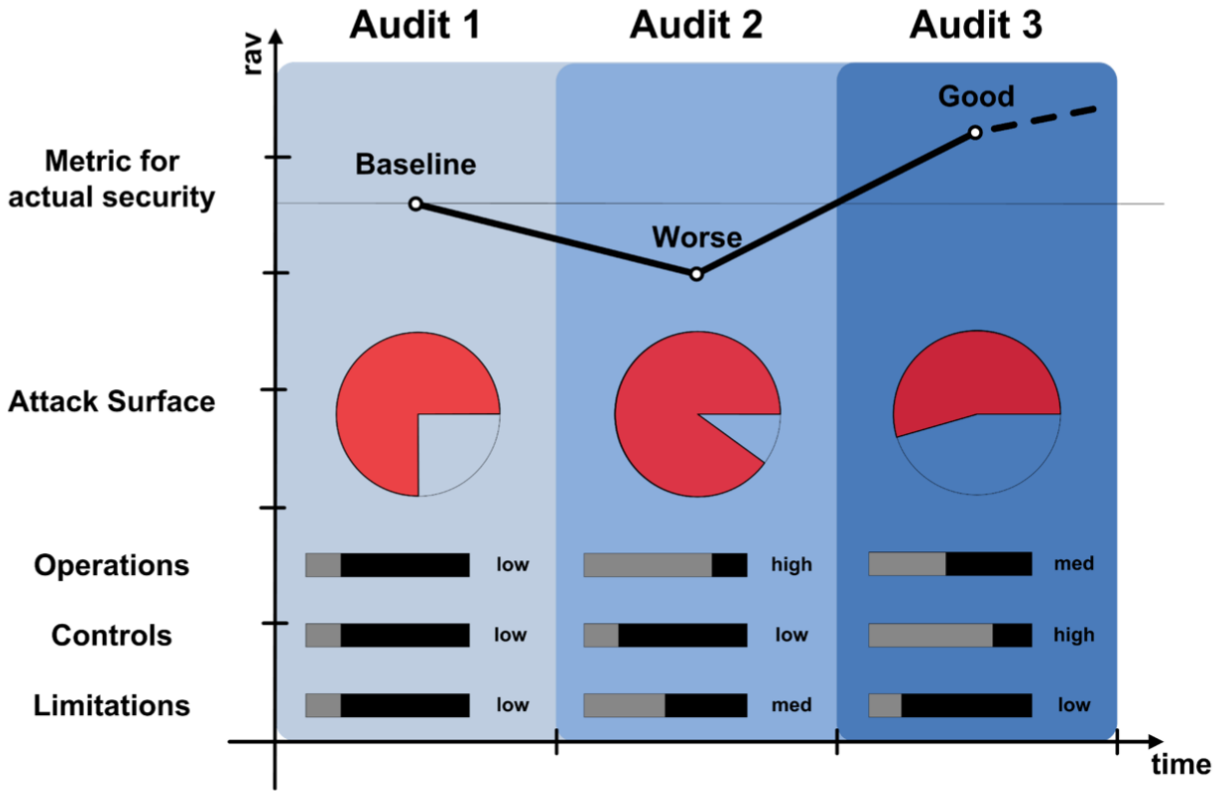
Metodología

Flujo de actividades
Pag 103 del PDF



OSSTM

Intro



Using ravs to measure and track the security of anything over time.

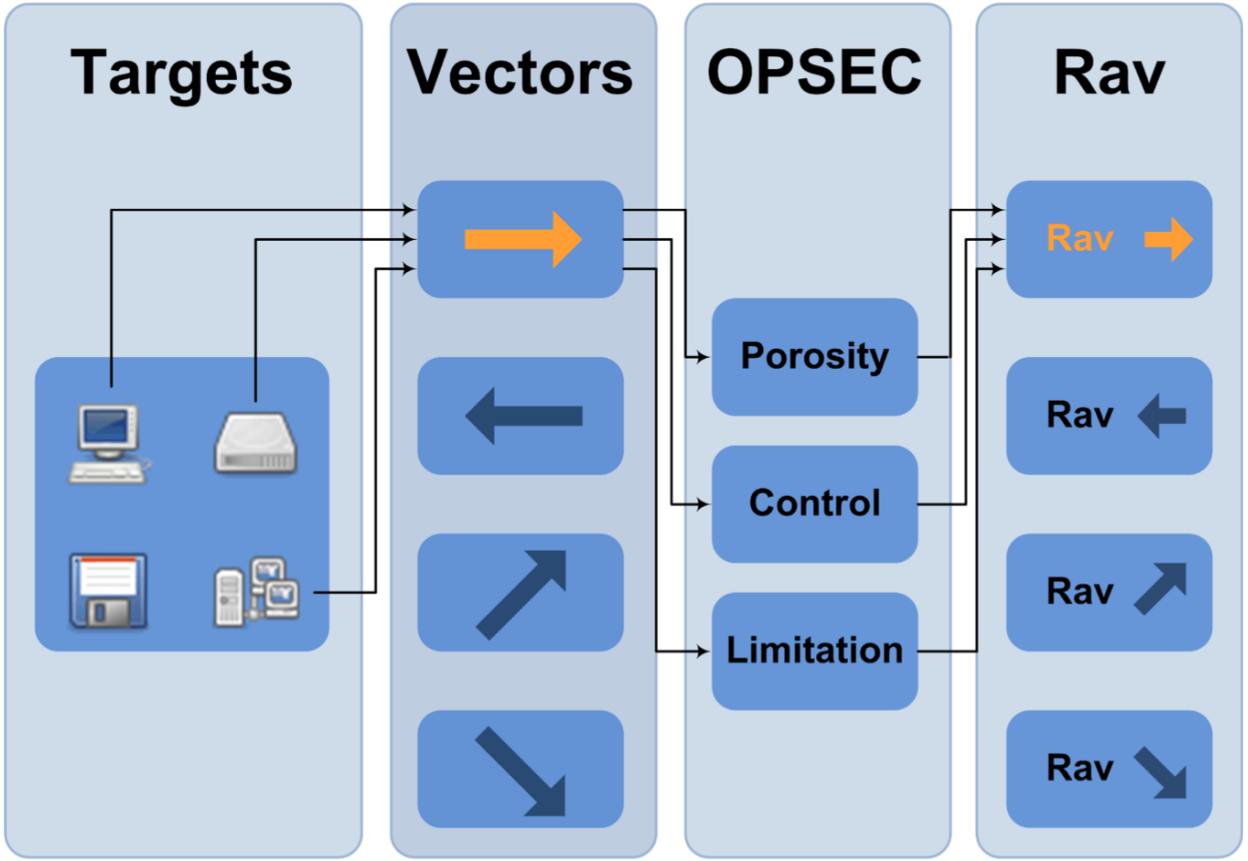
OSSTM

Intro

RAV

Risk Assessment Value

A set of attack surface metrics



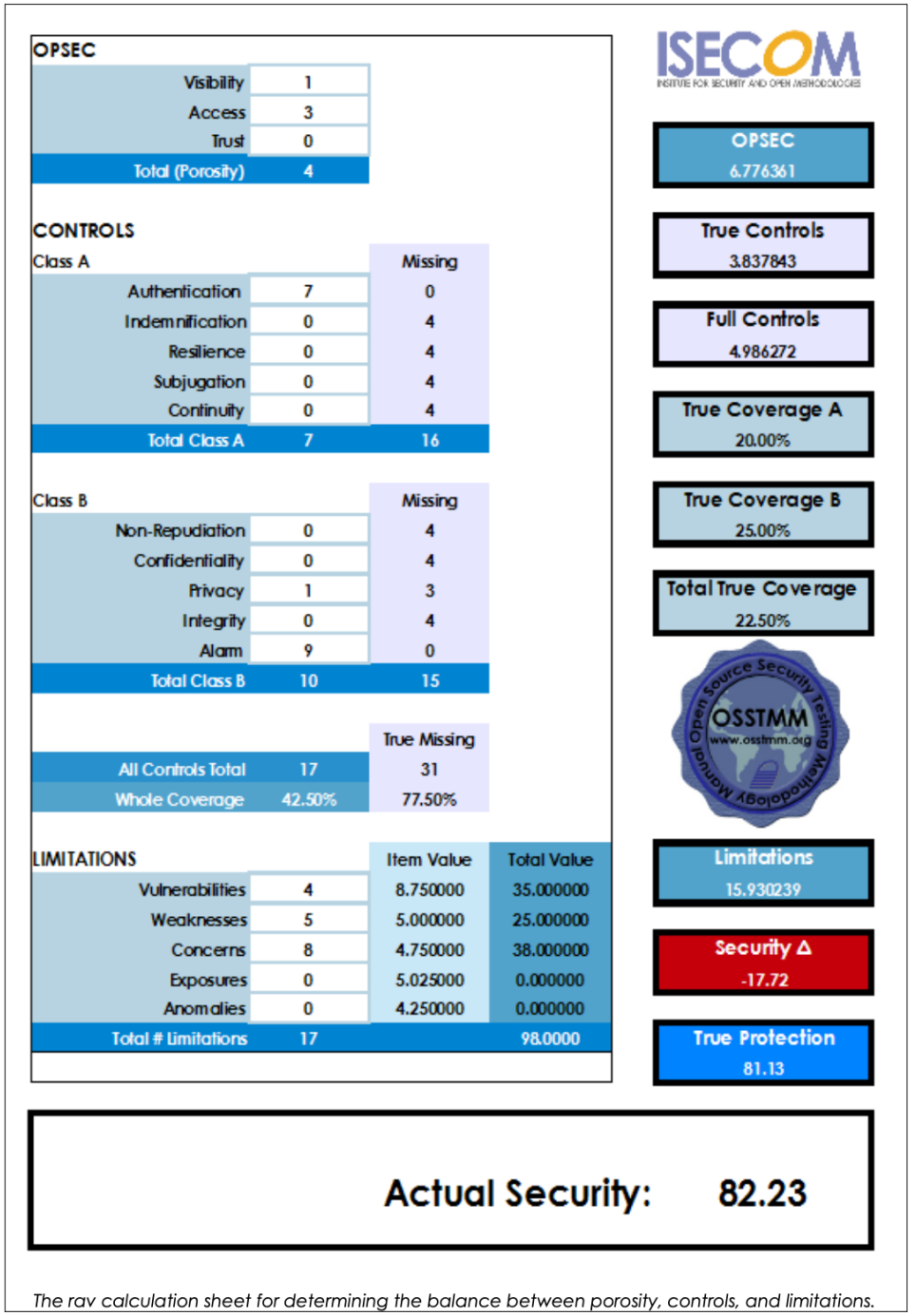
The simplicity of making a rav from a security test.

OSSTM

Intro

STAR

Security Test Audit Report



OPSEC	
Visibility	1
Access	3
Trust	0
Total (Porosity)	4

CONTROLS		
Class A		Missing
Authentication	7	0
Indemnification	0	4
Resilience	0	4
Subjugation	0	4
Continuity	0	4
Total Class A	7	16
Class B		Missing
Non-Repudiation	0	4
Confidentiality	0	4
Privacy	1	3
Integrity	0	4
Alarm	9	0
Total Class B	10	15
		True Missing
All Controls Total	17	31
Whole Coverage	42.50%	77.50%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	4	8.750000	35.000000
Weaknesses	5	5.000000	25.000000
Concerns	8	4.750000	38.000000
Exposures	0	5.025000	0.000000
Anomalies	0	4.250000	0.000000
Total # Limitations	17		98.0000

ISECOM

INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC 6.776361
True Controls 3.837843
Full Controls 4.986272
True Coverage A 20.00%
True Coverage B 25.00%
Total True Coverage 22.50%
Limitations 15.930239
Security Δ -17.72
True Protection 81.13

OSSTMM — Open Source Security Testing Methodology Manual — www.osstmm.org

Actual Security: 82.23

The rav calculation sheet for determining the balance between porosity, controls, and limitations.

Resumen

Ideas principales

Sesión

Resumen

Ideas principales

Es una metodología para realizar

Pruebas de Seguridad

Quien hace el resumen de este tema?

¿Características principales?
¿Para que se usa?
¿Cómo se diferencia de otros estándares?

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652