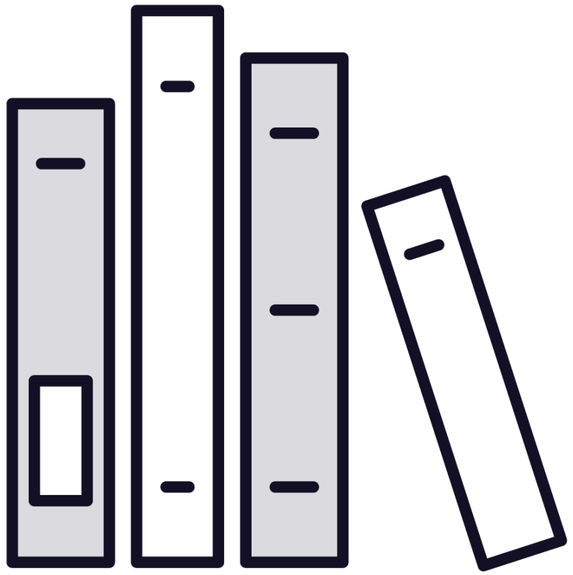
Assessment Frameworks

Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

What Are Assessment Frameworks?



Pre-defined methodologies for penetration testing

Defines what should be tested, not how to test

Ensures that you covered all the minimum test requirements

Should be a base for your test, but not all your test

Penetration Test Execution Standards (PTES)

A standard covering all the phases from penetration testing, from pre-engagement to reporting

Detailed Technical Guidelines:
http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

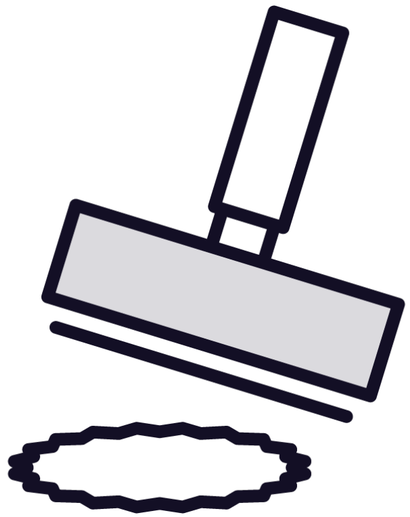
Open-source Security Testing Methodology Manual (OSSTMM)

In-depth description of each step of a penetration testing

From pre-engagement to reporting

Also includes physical security assessments, social engineering, and wireless security

Council of Registered Ethical Security Testers (CREST)



An organization that defines pentest standards and best practices

It has accreditations for companies and professionals

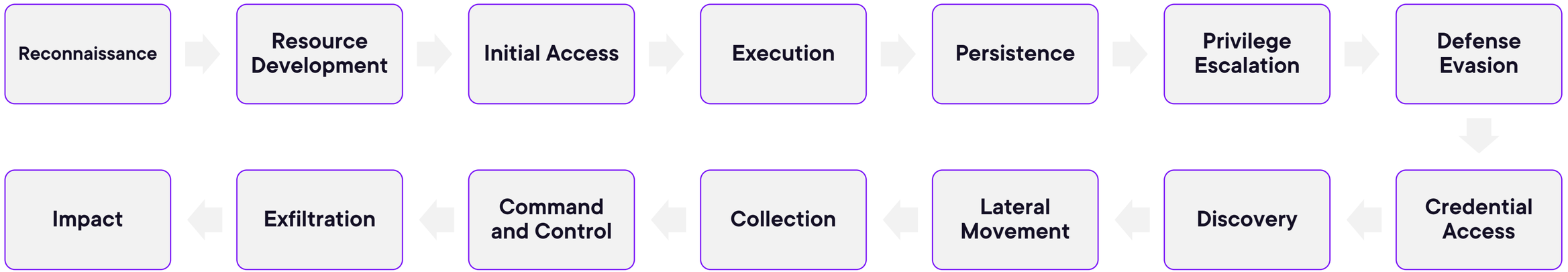
Some clients might require that all testers be CREST certified

MITRE ATT&CK

Framework for adversary emulation (Advanced Persistent Threats – APTs)

Contains the Tactics Techniques and Procedures (TTPs) used by well known threat actors

Usually adopted during red-team exercises



National Institute of Standards and Technology (NIST)

Non-regulatory agency of the United States Department of Commerce

A few publications regarding pentesting

Technical Guide to Information Security Testing (NIST 800-115)

- Techniques for the assessment
- Impact of the testing
- Root cause analysis
- Sensitive data handling
- etc.

Web, Mobile, and OT Frameworks

Open Web Application Security Project (OWASP)

A non-profit organization focused on improving the overall security of software

Mainly focused on web applications

Several open-source tools, training, and local chapters

OWASP TOP 10

1- Broken Access Control

2- Cryptographic Failures

3- Injection

4- Insecure Design

5- Security Misconfigurations

6- Vulnerable and Outdated Components

7- Identification and Authentication Failures

8- Software and Data Integrity Failures

9- Security Logging and Monitoring Failures

10- Server-Side Request Forgery

OWASP Mobile Application Security Verification Standard (MASVS)

Guidelines for testing mobile application

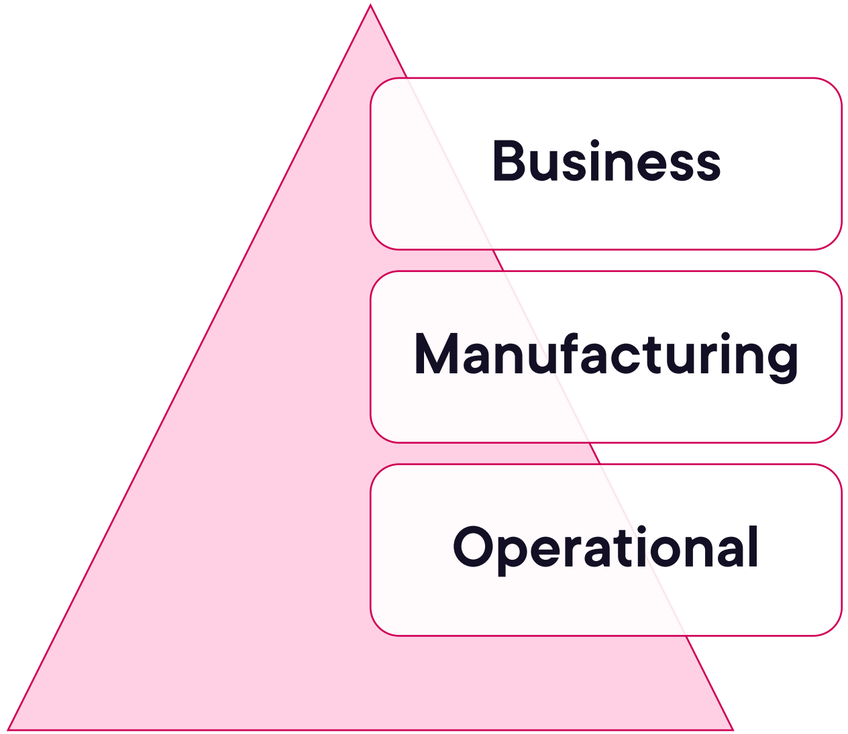
Divided into categories:

- Storage, crypto, authentication, network, platform, code, resilience, and privacy

Includes detailed checklists and what to check in each category

Purdue Model

Model for Industrial Control Systems (ICS) and Operational Technology (OT)



Simplified

Review the applicable models and frameworks.

Vary according to the type of OT

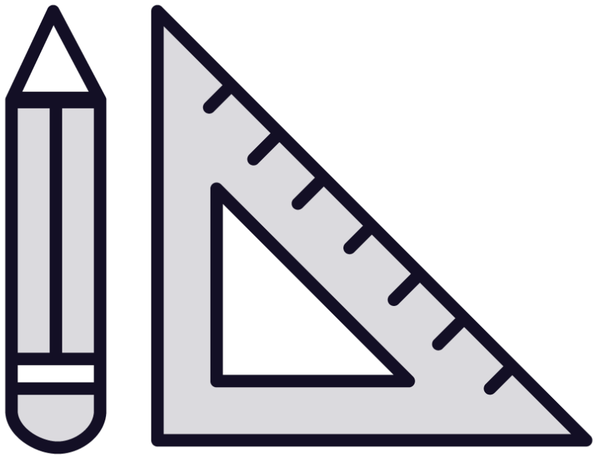
- Power plants
- Manufacturing
- Oil companies

Globomantics Scenario: Selected Methodologies

Client Name	Globomantics
Methodologies	> Penetration Test Execution Standards (PTES) > OWASP Top 10

Threat Modelling Frameworks

Why Use Modeling Threats



In some cases, the clients want to simulate a specific threat

Perform more meaningful tests based on actual potential threats

Several frameworks available for threat modelling

DREAD

Risk assessment model to quantify and prioritize threats

Give a score to each of the five categories:

- Damage potential
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Calculate the final score and prioritize the threats

STRIDE

Threat modeling methodology created by Microsoft

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation

Risk-based framework for managing cyber risks

Broader and incorporates organizational context

The process includes:

- Identifying critical assets and processes
- Assessing threats and vulnerabilities
- Determine risk based on impact and likelihood

Up Next:

Collaboration and Communication