Portfolio of Evidence (POE)

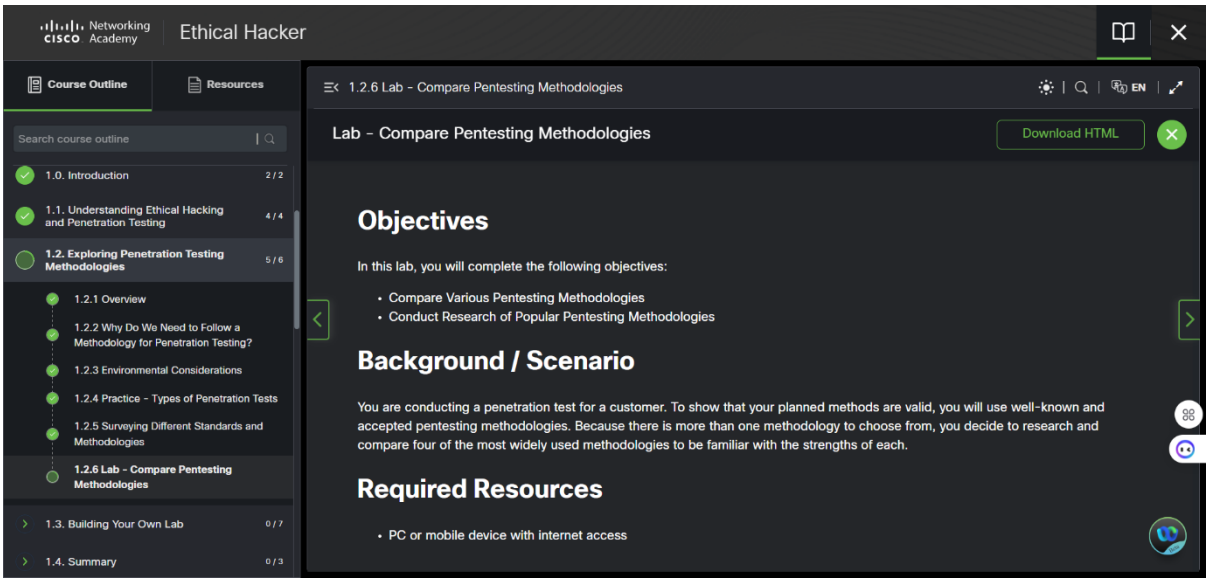
Lab Title: Compare Pentesting Methodologies
Learner Name: Motlalepula Jonathan Mojatau
Date: 16/09/2025
Course / Program: Ethical Hacking – Cisco Networking Academy

1. Lab Description & Objectives

In this lab, I researched and compared four widely used penetration testing methodologies: **OSSTMM, PTES, OWASP WSTG, and MITRE ATT&CK**.

The objectives were:

- Research four common pentesting methodologies.
- Document their key features, purposes, and use cases.
- Compare their strengths and weaknesses.
- Understand how to select and apply a methodology for a penetration test.

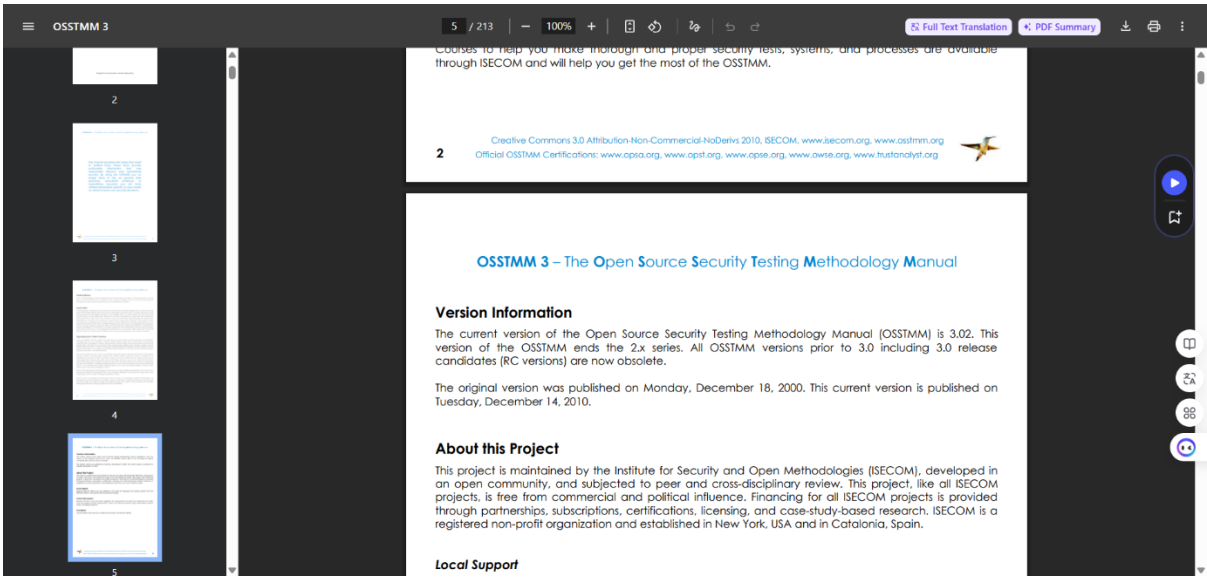


2. Research Findings

OSSTMM (Open Source Security Testing Methodology Manual)

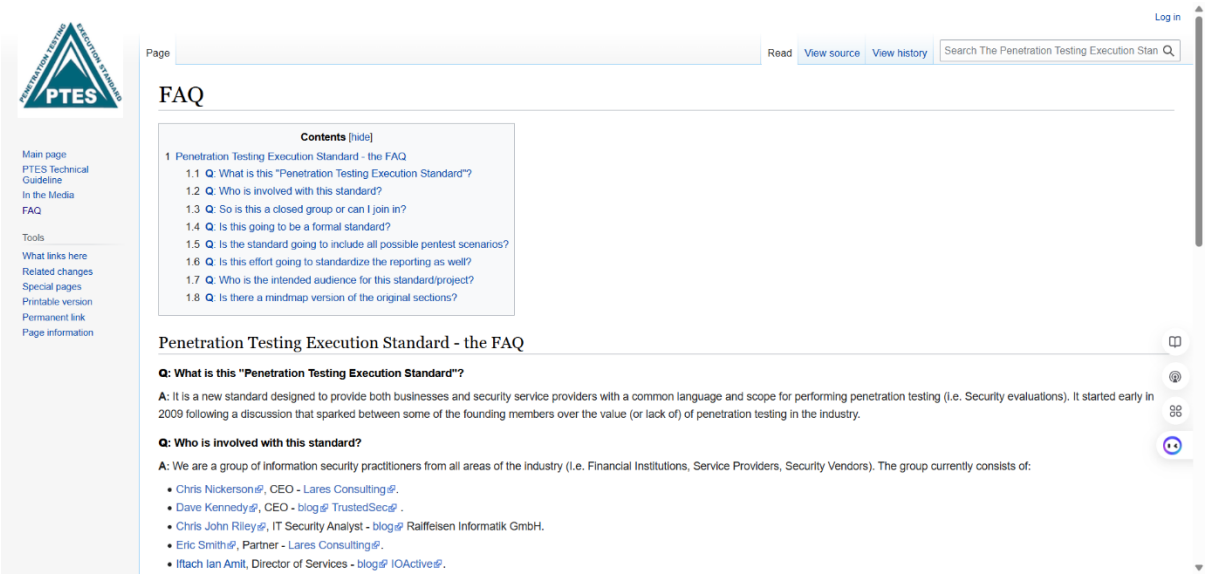
- **Version:** 3.02 (Dec 2010)
- **Developer:** ISECOM (Institute for Security and Open Methodologies)

- **Purpose:**
  - **Primary:** Provide a structured methodology for testing and analyzing the operational security of any environment.
  - **Secondary:** Offer guidelines for analysts to perform certified OSSTMM audits.
- **Assured Outcomes (if followed correctly):**
  1. Test is conducted thoroughly
  2. All necessary channels included
  3. Test complies with law
  4. Results are measurable and quantifiable
  5. Results are consistent and repeatable
  6. Results are fact-based, not assumptions



PTES (Penetration Testing Execution Standard)

- **Version:** v1.0
- **Seven Main Sections:**
  1. Pre-Engagement Interactions
  2. Intelligence Gathering
  3. Threat Modeling
  4. Vulnerability Analysis
  5. Exploitation
  6. Post-Exploitation
  7. Reporting
- **Purpose:** Provide businesses and security service providers with a common language and scope for performing penetration testing; set expectations and ensure consistent quality.
- **Supporting Document:** PTES Technical Guidelines (lists tools & techniques for each phase).



Log in

Page | Read | View source | View history | Search The Penetration Testing Execution Stan

PTES

Main page
PTES Technical Guideline
In the Media
FAQ

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

FAQ

Contents [hide]

1 Penetration Testing Execution Standard - the FAQ
1.1 Q: What is this "Penetration Testing Execution Standard"?
1.2 Q: Who is involved with this standard?
1.3 Q: So is this a closed group or can I join in?
1.4 Q: Is this going to be a formal standard?
1.5 Q: Is the standard going to include all possible pentest scenarios?
1.6 Q: Is this effort going to standardize the reporting as well?
1.7 Q: Who is the intended audience for this standard/project?
1.8 Q: Is there a mindmap version of the original sections?

Penetration Testing Execution Standard - the FAQ

Q: What is this "Penetration Testing Execution Standard"?

A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations). It started early in 2009 following a discussion that sparked between some of the founding members over the value (or lack of) of penetration testing in the industry.

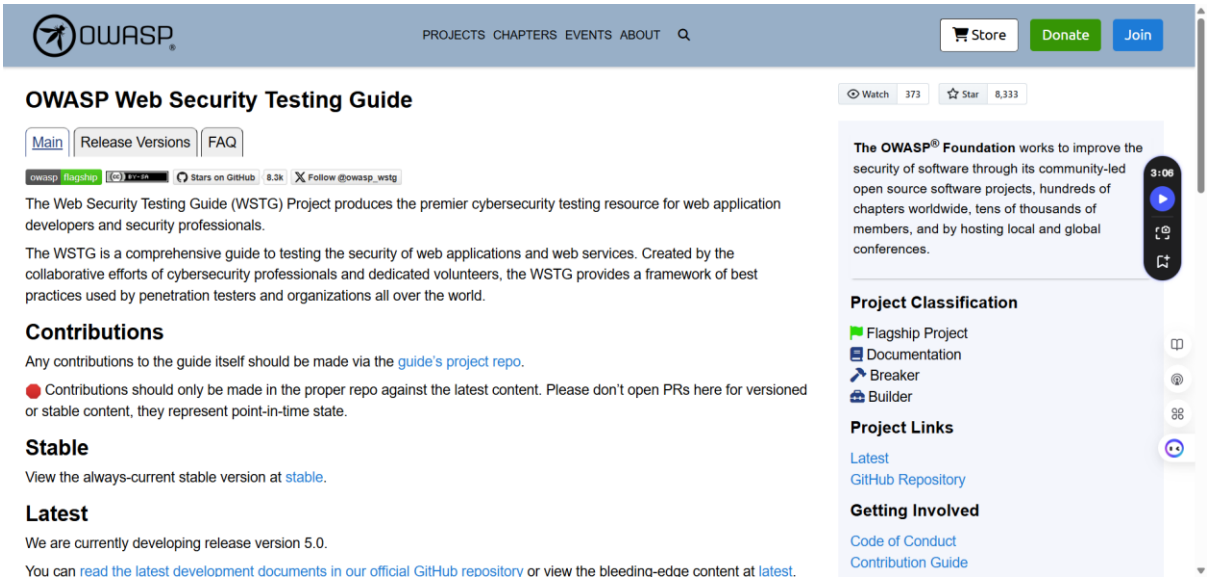
Q: Who is involved with this standard?

A: We are a group of information security practitioners from all areas of the industry (i.e. Financial Institutions, Service Providers, Security Vendors). The group currently consists of:

- Chris Nickerson, CEO - Lares Consulting.
- Dave Kennedy, CEO - blog TrustedSec .
- Chris John Riley, IT Security Analyst - blog Raiffeisen Informatik GmbH.
- Eric Smith, Partner - Lares Consulting.
- Iftach Ian Amit, Director of Services - blog IOActive.

OWASP WSTG (Web Security Testing Guide)

- **Version:** v4.1
- **Five Phases of Testing Framework:**
  1. Before Development Begins
  2. During Definition and Design
  3. During Development
  4. During Deployment
  5. During Maintenance and Operations
- **Purpose:** Provide a comprehensive guide for testing the security of web applications and web services throughout their lifecycle.
- **Twelve Active Test Categories:** Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Error Handling, Configuration Management, Cryptography Testing, Business Logic Testing, Client-Side Testing, and more.



OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Store | Donate | Join

OWASP Web Security Testing Guide

Main | Release Versions | FAQ

owasp flagship | Stars on GitHub 8.3k | Follow @owasp_wstg

The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing resource for web application developers and security professionals.

The WSTG is a comprehensive guide to testing the security of web applications and web services. Created by the collaborative efforts of cybersecurity professionals and dedicated volunteers, the WSTG provides a framework of best practices used by penetration testers and organizations all over the world.

Contributions

Any contributions to the guide itself should be made via the guide's project repo.

Contributions should only be made in the proper repo against the latest content. Please don't open PRs here for versioned or stable content, they represent point-in-time state.

Stable

View the always-current stable version at stable.

Latest

We are currently developing release version 5.0.

You can read the latest development documents in our official GitHub repository or view the bleeding-edge content at latest.

Watch 373 | Star 8,333

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

3:06

Project Classification

Flagship Project
Documentation
Breaker
Builder

Project Links

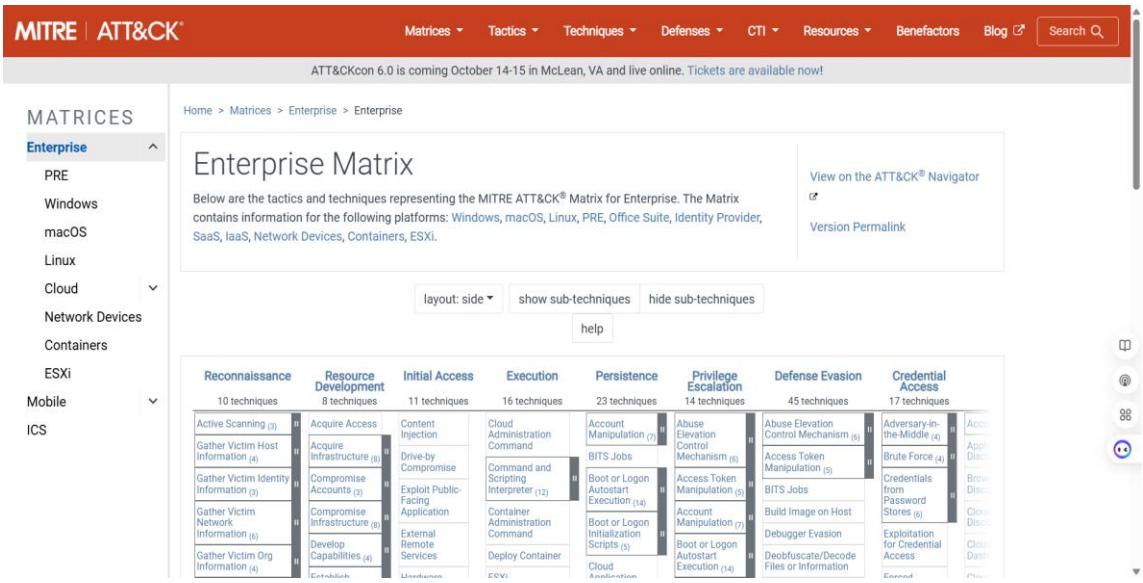
Latest
GitHub Repository

Getting Involved

Code of Conduct
Contribution Guide

MITRE ATT&CK

- **Version:** v17 (April 2025)
- **Purpose:** Provide a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world attack data.
- **Six Common Use Cases:**
    1. Adversary Emulation
    2. Red Teaming
    3. Behavioral Analytics Development
    4. Defensive Gap Assessment
    5. SOC Maturity Assessment
    6. Cyber Threat Intelligence Enrichment
- **Technology Domains:** Enterprise, Mobile, ICS
- **Reconnaissance Example:** *Gather Victim Identity Information*
    - **Sub-Techniques:** Email Addresses, Personal Data, Usernames
    - **Threat Actor Example:** *Lazarus Group* – gathered email addresses via phishing/OSINT to conduct later targeted attacks.



3. Comparative Analysis

Criteria	OSSTMM	PTES	OWASP WSTG	MITRE ATT&CK
Focus Area	General security testing	End-to-end pentest lifecycle	Web app testing	Adversary behavior knowledge base
Version Age	Older (2010)	Still current	Maintained, v4.1	Frequently updated

Criteria	OSSTMM	PTES	OWASP WSTG	MITRE ATT&CK
Coverage	Broad (network, physical, wireless)	Broad, detailed process	Web-specific	TTPs, tactics & techniques
Use Case	Baseline audits & measurable results	Full professional pentest	Web security checks	Threat modeling, red teaming
Strengths	Measurable results, compliance focus	Widely adopted industry standard	Developer-friendly & practical	Up-to-date with real attacker behavior
Limitations	A bit outdated, should be combined with newer standards	Requires skilled practitioners to apply properly	Limited to web & services	Not a methodology — just knowledge base

---

4. Practical Application / Use-Case

If I were conducting a penetration test for a client:

- I would use **PTES** as the main methodology for end-to-end coverage.
- Supplement with **OWASP WSTG** for the web applications.
- Reference **MITRE ATT&CK** for adversary emulation and to align findings with real-world TTPs.
- OSSTMM could help provide measurable, repeatable metrics in the final report.

---

5. Reflection & Lessons Learned

This lab helped me understand that no single methodology covers everything.

- **PTES** provides an excellent structured workflow.
- **OWASP WSTG** ensures I don't miss web-specific vulnerabilities.
- **MITRE ATT&CK** keeps my approach current with attacker techniques.
- Following a recognized methodology is critical for consistency, legal compliance, and producing professional, repeatable results.

---

7. References

- ISECOM – OSSTMM v3.02
- PTES – www.pentest-standard.org
- OWASP – Web Security Testing Guide v4.1
- MITRE ATT&CK – https://attack.mitre.org