




Ethical Hacking Basics Course

By : Mohammad Askar
@Mohammadaskar2



Module 2

Pentesting Methodologies.



Definition of Penetration Testing

Penetration Testing is the process to simulate attacks on computer systems to figure out security weakness and exploit it to gain access to the system features and data.

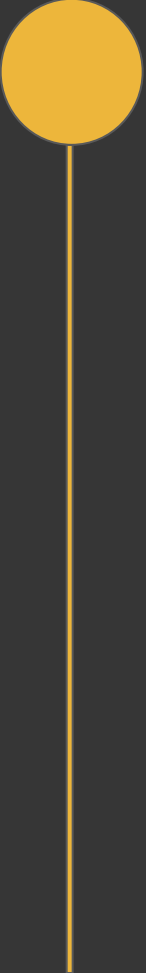
Also called :

- PT.
- Pentesting.
- Ethical Hacking.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Definition of Vulnerability Assessment

Vulnerability assessment (Vulnerability Analysis) mainly is the process of identifying , Ranking and sorting vulnerabilities in a computer system and report it to the system admin.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running parallel to the left edge of the text area.

The Difference Between Vulnerability Assessment and Penetration Test

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

PTES Methodology

- Penetration Testing Execution Standard.
- The Most Common Penetration Testing methodology.
- We will use it in this course.
- <http://www.pentest-standard.org/>.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running parallel to the left edge of the slide.

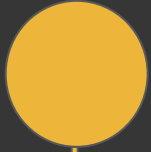
PTES Sections

1. Pre-engagement.
2. Intelligence Gathering.
3. Threat Modeling.
4. Vulnerability Analysis.
5. Exploitation.
6. Post Exploitation.
7. Reporting.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Other PT Methodologies

- OWASP.
- NIST.
- OSSTMM.



OWASP

- Open Web Application Security Project.
- Free online community includes experts and companies from all around the world .
- OWASP TOP 10.
- OWASP Testing Guide.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

OSSTMM

- Open Source Security Testing Methodology Manual.
- The OSSTMM is about operational security , It is about knowing and measuring how well security works. This methodology will tell you if what you have does what you want it to do and not just what you were told it does.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running parallel to the left edge of the text area.

Penetration Testing Types

- White Box Penetration Testing.
- Black Box Penetration Testing.
- Gray Box Penetration Testing.



White Box Penetration Testing

- The Client Should share information about targets.
- Everything is clear for the attacker and the client.
- Great test to simulate the internal threats.



Black Box Penetration Testing

- Full Real World Simulated Attack.
- No information should be shared with the attacker.
- Test the Real world Threats.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Gray Box Penetration Testing

- The Client Share Some information about the targets.
- The attacker perform a PT depends on the shared information.



Penetration Testing Categories

- Network Penetration Testing.
- Wireless Network Penetration Testing.
- Web Application Penetration Testing.
- Mobile Application Penetration Testing.
- Physical Penetration Testing.

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Terminologies

- Vulnerability : Vulnerability is a weak spot in your computer system that might be exploited by a security threat.
- Exploit : the method that we use to make benefit from the vulnerability.
- Threat : possible danger that could effects computer systems.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left side of the slide.

Pre-Engagement

- Work Scope.
- who is responsible about this PT and who to contact ?
- legal issues.
- The fees \$\$\$
- Rules of Engagement.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running parallel to the left edge of the text.

Contract Example