Ethical Hacking Basics Course

By : Mohammad Askar
@Mohammadaskar2

Module 2
Pentesting Methodologies.

Definition of Penetration Testing

Penetration Testing is the proccess 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.

Definition of Vulnerability Assessment

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

The Difference Between Vulnerability Assessment and Penetration Test

PTES Methodology

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

PTES Sections

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

Other PT Methodologies

- OWASP.
- NIST.
- OSSTMM.

OWASP

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

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.

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.

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 Applocation Penetration Testing.
- Physical Penetration Testing.

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.

Pre-Engagement

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

Contract Example