Software Systems Verification and Validation

Assoc. Prof. Andreea Vescan

Babeș-Bolyai University
Cluj-Napoca
2020-2021

Lecture 11:
Security Testing

SSVV - Exams

- Teams
- General channel
  - Files
  - 2021_SSVV_Exams_Schedule.xlsx

SSVV_Quiz3_Lectures

- 100 XP
- 10 minutes

Outline

- Security testing
  - Definition
  - Terms
- Security testing types
- Security testing - More information
- Penetration testing
  - Definition
  - Demo
- Security testing
  - Video presentations by students

Security testing

- **Video presentations**
  - **Created by a team**
  - **Each video ~ 5 minutes**
    - **Audio + written + visual**

- Team 1:
  - Security Testing (by students in 2019)

Security testing

- **SECURITY TESTING** is a type of software testing that intends to uncover vulnerabilities of the system and determine that its data and resources are protected from possible intruders.

http://softwaretestingfundamentals.com/security-testing/

- **Security terms (**https://www.qualitestgroup.com/white-papers/what-is-security-testing/)
  - **Asset** – Anything that has value to an organization, subject to many kinds of threats. [ISO/IEC 13335-1:2004]
  - **Threat** – A potential cause of an unwanted incident, which may result in harm to a system or organization. [ISO/IEC 27001:2005]
  - **Vulnerability** – Defined as a weakness of an asset or group of assets that can be exploited by one or more threats. [After ISO/IEC 27001:2005]. Vulnerabilities can be found in software, information systems, network protocols and devices, etc. If vulnerability is not managed, it will allow a threat to materialize. Examples of vulnerability include unpatched software, weak passwords, lack of access control, no firewall installed, etc.
  - **Risk** – The potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of information assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and the severity of its consequences.
  - **Information security**– the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. [ISO27002:2005] Industrial espionage is unauthorized collection of confidential, classified or proprietary documents.

Security testing types

http://blog.qatestlab.com/2017/02/07/security-testing-types/

Security testing - More information

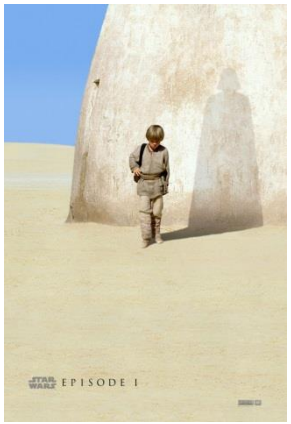
- **Open Web Application Security Project**
  - **OWASP Top 10 Web Application Security Risks**
  - https://www.veracode.com/directory/owasp-top-10
  - dedicated to providing unbiased, practical information about application security
  - updated in 2017 to provide guidance to developers and security professionals on the most critical vulnerabilities that are commonly found in web applications, which are also easy to exploit.
  - These 10 application risks are dangerous because they may allow attackers to plant malware, steal data, or completely take over your computers or web servers.

- **STRIDE Threat Models**
  - https://dev.to/petermbenjamin/demystifying-stride-threat-models-230m
  - Application Security advocates encourage developers and engineers to adopt security practices as early in the Software Development Life Cycle (SDLC) as possible.
  - One such security practice is **Threat Modeling**.
    - *Threat Models are a systematic and structured way to identify and mitigate security risks in our software*.

Learning to hack

To decide – use power for

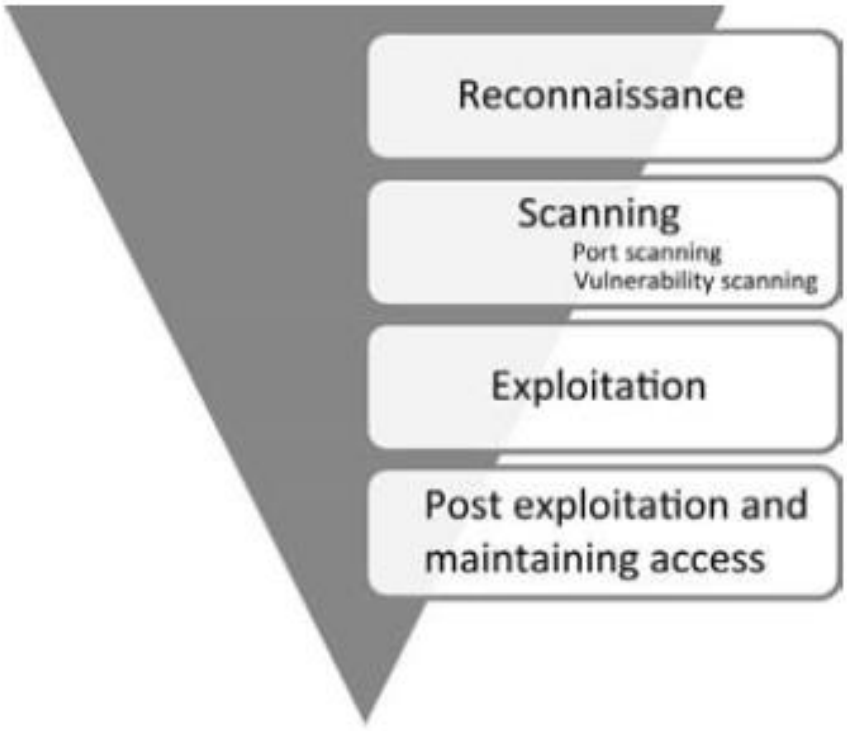
GOOD ? BAD

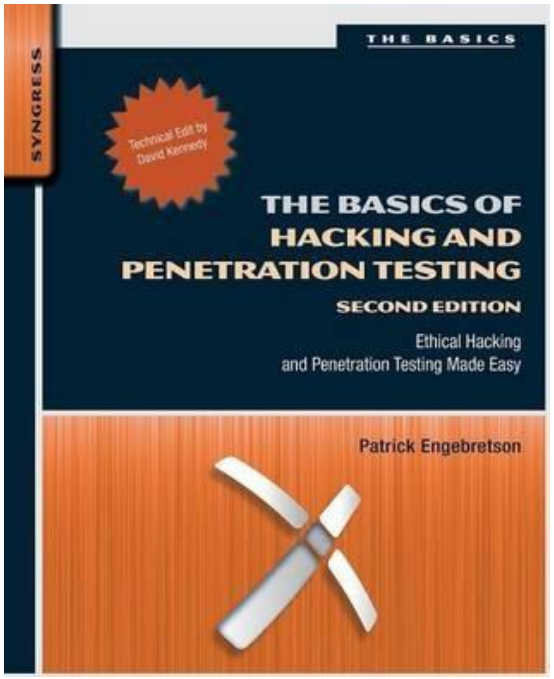


https://www.starwars.com/news/star-wars-in-mythology-the-shadow

Penetration testing

- A penetration test - attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.
  - https://www.veracode.com/security/penetration-testing





Penetration testing

Demo

- Kali Linux
  - https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
- Metasploitable2 (Linux)
  - https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Metasploit Framework (MSF)
  - https://www.metasploit.com/

  - https://www.youtube.com/watch?v=CktYFft7K8Q
  - Last 25 minutes

Security testing

- **Video presentations**
  - **Created by a team**
  - **Each video ~ 5 minutes**
    - **Audio + written + visual**

- Team 2:
  - SQL injection (by students in 2019)

Security testing

Questions

- Thank You For Your Attention!