Security testing

Security testing is a process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended.[1] Due to the logical limitations of security testing, passing the security testing process is not an indication that no flaws exist or that the system adequately satisfies the security requirements.

Typical security requirements may include specific elements of confidentiality, integrity, authentication, availability, authorization and non-repudiation.[2] Actual security requirements tested depend on the security requirements implemented by the system. Security testing as a term has a number of different meanings and can be completed in a number of different ways. As such, a Security Taxonomy helps us to understand these different approaches and meanings by providing a base level to work from.

Confidentiality

- A security measure which protects against the disclosure of information to parties other than the intended recipient is by no means the only way of ensuring the security.

Integrity

Integrity of information refers to protecting information from being modified by unauthorized parties

- A measure intended to allow the receiver to determine that the information provided by a system is correct.

- Integrity schemes often use some of the same underlying technologies as confidentiality schemes, but they usually involve adding information to a communication, to form the basis of an algorithmic check, rather than the encoding all of the communication.
- To check if the correct information is transferred from one application to other.

Authentication

This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what its packaging and labelling claims to be, or assuring that a computer program is a trusted one.

Authorization

- The process of determining that a requester is allowed to receive a service or perform an operation.
- Access control is an example of authorization.

Availability

- Assuring information and communications services will be ready for use when expected.
- Information must be kept available to authorized persons when they need it.

Non-repudiation

- In reference to digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- A sender-id is usually a header transmitted along with message which recognises the message source.

Taxonomy

Common terms used for the delivery of security testing:

- **Discovery** - The purpose of this stage is to identify systems within scope and the services in use. It is not intended to discover vulnerabilities, but version detection may highlight deprecated versions of software / firmware and thus indicate potential vulnerabilities.
- **Vulnerability Scan** - Following the discovery stage this looks for known security issues by using automated tools to match conditions with known vulnerabilities. The reported risk level is set automatically by the tool with no manual verification or interpretation by the test vendor. This can be supplemented with credential based scanning that looks to remove some common false positives by using supplied credentials to authenticate with a service (such as local windows accounts).
- **Vulnerability Assessment** - This uses discovery and vulnerability scanning to identify security vulnerabilities and places the findings into the context of the environment under test. An example would be removing common false positives from the report and deciding risk levels that should be applied to each report finding to improve business understanding and context.
- **Security Assessment** - Builds upon Vulnerability Assessment by adding manual verification to confirm exposure, but does not include the exploitation of vulnerabilities to gain further access. Verification could be in the form of authorized access to a system to confirm system settings and involve examining logs, system responses, error messages, codes, etc. A Security Assessment is looking to gain a broad coverage of the systems under test but not the depth of exposure that a specific vulnerability could lead to.
- **Penetration Test** - Penetration test simulates an attack by a malicious party. Building on the previous stages and involves exploitation of found vulnerabilities to gain further access. Using this approach will result in an understanding of the ability of an attacker to gain access to confidential information, affect data integrity or availability of a service and the respective impact. Each test is approached using a consistent and complete methodology in a way that allows the tester to use their problem solving abilities, the output from a range of tools and their own knowledge of networking and systems to find vulnerabilities that would/ could not be identified by automated tools. This approach looks at the depth of attack as compared to the Security Assessment approach that looks at the broader coverage.
- **Security Audit** - Driven by an Audit / Risk function to look at a specific control or compliance issue. Characterized by a narrow scope, this type of engagement could make use of any of the earlier approaches discussed (vulnerability assessment, security assessment, penetration test).

- **Security Review** - Verification that industry or internal security standards have been applied to system components or product. This is typically completed through gap analysis and utilizes build / code reviews or by reviewing design documents and architecture diagrams. This activity does not utilize any of the earlier approaches (Vulnerability Assessment, Security Assessment, Penetration Test, Security Audit)

Tools

- Container and Infrastructure Security Analysis[3][4]
- SAST - Static Application Security Testing
- DAST - Dynamic Application Security Testing
- IAST - Interactive Application Security Testing[5]
- DLP - Data Loss Prevention
- IDS, IPS - Intrusion Detection System, Intrusion Prevention System
- OSS Scanning - Open Source Software Scanning (see Open-source software security)
- RASP - Runtime Application Self-Protection
- SCA - Software Composition Analysis[6]
- WAF - Web Application Firewall

See also

- National Information Assurance Glossary

References

1. *M Martellini, & Malizia, A. (2017). Cyber and chemical, biological, radiological, nuclear, explosives challenges : threats and counter efforts. Springer.*
2. *"Introduction to Information Security" US-CERT https://www.us-cert.gov/security-publications/introduction-information-security*
3. *"Container Security Verification Standard" (https://github.com/OWASP/Container-Security-Verification-Standard) . GitHub. 20 July 2022.*
4. *"Infrastructure as Code Security - OWASP Cheat Sheet Series" (https://cheatsheetseries.owasp.org/cheatsheets/Infrastructure_as_Code_Security_Cheat_Sheet.html) .*

5. *"OWASP DevSecOps Guideline - v-0.2 | OWASP Foundation" (https://owasp.org/www-project-devsecops-guideline/latest/02c-Interactive-Application-Security-Testing)* .
6. *"Component Analysis | OWASP Foundation" (https://owasp.org/www-community/Component_Analysis)* .

Last edited 10 days ago by BrownHairedGirl