Standard Glossary of Terms used in Software Testing

Version 3.1

Terms Changed since 13-Sep-2015

International Software Testing Qualifications Board

fault attack

See Also: negative testing, security attack

Directed and focused attempt to evaluate a specific quality characteristic of a test object by attempting to force specific failures to occur. Usually focused on reliability or security.

Changes:

2016-03-18 - Updated definition to conform to security syllabus

---

abuse case

See Also: use case

A use case in which some actors with malcious intent are causing harm to the system or to other actors.

Changes:

2016-03-18 - New Term - Security Syllabus

---

account harvesting

The process of obtaining lists of email addresses for use in bulk email messages.

Changes:

2016-03-18 - New Term - Security Syllabus

---

anti-malware

Software that is used to detect and inhibit malware. See also malware.

Changes:

2016-03-18 - New Term - Security Syllabus

---

attack vector

A path or means by which an attacker can gain access to a system for malicious purposes.

Changes:

2016-03-18 - New Term - Security Syllabus

---

attacker

See Also: hacker

A person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.

Changes:

2016-03-18 - New Term - Security Syllabus

---

authentication

See Also: authorization

A procedure determining whether a person or a process is, in fact, who or what it is declared to be.

Changes:

2016-03-18 - New Term - Security Syllabus

---

authorization

See Also: authentication

Permission given to a user or process to access resources.

Changes:

2016-03-18 - New Term - Security Syllabus

---

botnet

A network of compromised computers, called bots or robots, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.

Changes:

2016-03-18 - New Term - Security Syllabus

---

cross-site scripting (XSS)

Ref: NIST.IR.7298

A vulnerability that allows attackers to inject malicious code into an otherwise benign website.

Changes:

2016-03-18 - New Term - Security Syllabus

---

data obfuscation

Data transformation that makes it difficult for a human to recognize the original data.

Changes:

2016-03-18 - New Term - Security Syllabus

---

data privacy

The protection of personally identifiable information or otherwise sensitive information from undesired disclosure

Changes:

2016-03-18 - New Term - Security Syllabus

---

demilitarized zone (DMZ)

See Also: network zone

A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, commonly the Internet.

Changes:

2016-03-18 - New Term - Security Syllabus

---

denial of service (DOS)

A security attack that is intended to overload the system with requests such that legitimate requests cannot be serviced.

Changes:

2016-03-18 - New Term - Security Syllabus

---

encryption

The process of encoding information so that only authorized parties can retrieve the original information, usually by means of a specific decryption key or process.

Changes:

2016-03-18 - New Term - Security Syllabus

---

ethical hacker

A security tester using hacker techniques.

Changes:

2016-03-18 - New Term - Security Syllabus

---

firewall

A component or set of components that controls incoming and outgoing network traffic based on predetermined security rules.

Changes:

2016-03-18 - New Term - Security Syllabus

---

computer forensics

The practice of determining how a security attack has succeeded and assessing the damage caused.

Changes:

2016-03-18 - New Term - Security Syllabus

---

fuzz testing

A software testing technique used to discover security vulnerabilities by inputting massive amounts of random data, called fuzz, to the component or system.

Changes:

2016-03-18 - New Term - Security Syllabus

---

hacker

See Also: attacker

A person or organization who is actively involved in security attacks, usually with malicious intent.

Changes:

2016-03-18 - New Term - Security Syllabus

---

hashing

Transformation of a variable length string of characters into a usually shorter fixed-length value or key. Hashed values, or hashes, are commonly used in table or database lookups. Cryptographic hash functions are used to secure data.

Changes:

2016-03-18 - New Term - Security Syllabus

---

information assurance

Ref: NIST.IR.7298

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Changes:

2016-03-18 - New Term - Security Syllabus

---

information security

Ref: NIST.IR.7298

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Changes:

2016-03-18 - New Term - Security Syllabus

---

insider threat

A security threat originating from within the organization, often by an authorized system user.

Changes:

2016-03-18 - New Term - Security Syllabus

---

intrusion detection system (IDS)

See Also: malware scanning

A system which monitors activities on the 7 layers of the OSI model from network to application level, to detect violations of the security policy.

Changes:

2016-03-18 - New Term - Security Syllabus

---

malware

Software that is intended to harm a system or its components.

Changes:

2016-03-18 - New Term - Security Syllabus

---

malware scanning

See Also: intrusion detection system

Static analysis aiming to detect and remove malicious code received at an interface.

Changes:

2016-03-18 - New Term - Security Syllabus

---

network zone

A sub-network with a defined level of trust. For example, the Internet or a public zone would be considered to be untrusted.

Changes:

2016-03-18 - New Term - Security Syllabus

---

password cracking

Ref: after NIST.IR.7298

A security attack recovering secret passwords stored in a computer system or transmitted over a network.

Changes:

2016-03-18 - New Term - Security Syllabus

---

penetration testing

A testing technique aiming to exploit security vulnerabilities (known or unknown) to gain unauthorized access.

Changes:

2016-03-18 - New Term - Security Syllabus

---

pharming

A security attack intended to redirect a web site's traffic to a fraudulent web site without the user's knowledge or consent.

Changes:

2016-03-18 - New Term - Security Syllabus

---

phishing

An attempt to acquire personal or sensitive information by masquerading as a trustworthy entity in an electronic communication.

Changes:

2016-03-18 - New Term - Security Syllabus

---

reconnaissance

The exploration of a target area aiming to gain information that can be useful for an attack.

Changes:

2016-03-18 - New Term - Security Syllabus

---

salting

See Also: hashing

A cryptographic technique that adds random data (salt) to the user data prior to hashing.

Changes:

2016-03-18 - New Term - Security Syllabus

---

script kiddie

See Also: hacker

A person who executes security attacks that have been created by other hackers rather than creating own ones.

Changes:

2016-03-18 - New Term - Security Syllabus

---

security attack

Ref: after NIST.IR.7298

An attempt to gain unauthorized access to a system or component, resources, information, or an attempt to compromise system integrity.

Changes:

2016-03-18 - New Term - Security Syllabus

---

security audit

An audit evaluating an organization's security processes and infrastructure.

Changes:

2016-03-18 - New Term - Security Syllabus

---

security policy

A high-level document describing the principles, approach and major objectives of the organization regarding security.

Changes:

2016-03-18 - New Term - Security Syllabus

---

security procedure

A set of steps required to implement the security policy and the steps to be taken in response to a security incident.

Changes:

2016-03-18 - New Term - Security Syllabus

---

security vulnerability

A weakness in the system that could allow for a successful security attack.

Changes:

2016-03-18 - New Term - Security Syllabus

---

social engineering

Ref: NIST.IR.7298

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Changes:

2016-03-18 - New Term - Security Syllabus

SQL injection

A security attack inserting malicious SQL statements into an entry field for execution.

Changes:

2016-03-18 - New Term - Security Syllabus

---

system hardening

The step-by-step process of reducing the security vulnerabilities of a system by applying a security policy and different layers of protection.

Changes:

2016-03-18 - New Term - Security Syllabus

---

vulnerability scanner

A static analyzer that is used to detect particular security vulnerabilities in the code.

Changes:

2016-03-18 - New Term - Security Syllabus
