AT*SQA

Cybersecurity Testing Micro-Credential

Syllabus

Copyright Notice

AT*SQA

MICRO-CREDENTIAL

Cybersecurity Testing

Table of Contents

Cybersecurity Testing

References

General Information

STUDY TIME – 200 MINS.

KEYWORDS

cyberattack, cybersecurity, cybersecurity testing, fuzzing, cybersecurity controls, social engineering, system hardening, threat actors, threat intelligence, threat modeling, vulnerabilities

LEARNING OBJECTIVES FOR CYBERSECURITY TESTING

Introduction

(K1) Recall the definition of cybersecurity
(K1) Recall the cybersecurity attributes of assets
(K1) Recall the function of cybersecurity controls

The Purpose of Cybersecurity Testing

(K2) Explain the necessity to both verify requirements and validate the system during cybersecurity testing

Cybersecurity Differences

(K2) Explain the unique differences of cybersecurity testing

Cybersecurity Testing Approaches

(K1) Recall when cybersecurity test planning should take place within the SDLC
(K2) Explain how cybersecurity testing contributes to risk management
(K2) Explain how testing can enhance the stages of a cybersecurity effort

Conducting Cybersecurity Testing

(K1) Recall why cybersecurity testing must be pre-authorized
(K2) Explain how white-box testing is used in cybersecurity testing LO-6.5.c (K2) Explain how black-box testing is used in cybersecurity testing LO-6.5.d (K1) Recall the controls that can be targeted by cybersecurity tests

The Environment of Constant Change

(K1) Recall ways to keep up to date with cybersecurity and cybersecurity testing practices

Introduction

Cybersecurity was commonly called information security or information assurance - the latter emphasizing the need to be confident or assured that digital resources are in fact secured. Cybersecurity refers to protecting computer systems, including their electronic data, software and hardware, from theft or damage as well as from disruption or misdirection of the services they provide.

Valued data or computerized processes are referred to as assets. Their security attributes typically are described as confidentiality (and its corollary, privacy), integrity, and accessibility: the so-called “CIA” triad. Confidential material should only be entrusted to designated parties for specific purposes, respecting the owner’s privacy. The integrity of an asset is dependent on the assurance that it has not been tampered with via unauthorized access. When data or a service is needed, it needs to be accessible only to authorized users.

Cybersecurity addresses the need to protect the integrity and confidentiality of digital assets, as well as the accessibility of online processes. Computerized systems in the past suffered almost all of their failures due to defects in design or implementation. Today, however, so-called threat actors (malicious individuals or groups) conduct cyberattacks to compromise systems by deliberately misusing them. Critical infrastructures – including energy, communication, transportation, and finance – are now heavily computerized; defenses against online assaults are the essential responsibility of cybersecurity.

Protection of system resources and processes is the function of cybersecurity controls. These controls range from straightforward precautions such as account passwords to sophisticated automated detection and response mechanisms. Different cybersecurity controls may be designed to reduce the likelihood of successful attacks or to minimize the damage done if any attacks succeed. None of these protections are flawless, hence, anyone wishing to compromise computerized systems will be looking for weaknesses, known as vulnerabilities, in the controls.

Consider the situation in terms of the classic elements of criminality: motive, means, and opportunity. Vulnerabilities in cybersecurity controls are the opportunities - success depends on bypassing these controls. Malicious individuals and groups might be motivated by greed, revenge or ideology. But they will need knowledge, skills, and resources – the means of attacking – to take advantage of an opportunity and successfully compromise security. The strength of their motivation determines their persistence or willingness to risk detection.

The Purpose of Cybersecurity Testing

Cybersecurity testing probes systems to reveal potential failures in furnishing the desired level of security.

As with any other testing, cybersecurity testing reveals the presence of defects but cannot confirm their absence. It provides value both as verification (“Was it built right?”) and as validation (“Was the right thing built?”).

Where security requirements have been specified, testing can verify how adequately these requirements are satisfied. Threat modeling, based on threat intelligence, anticipates the nature of assaults that might be encountered in the operating environment of the system. System designers provide corresponding controls, and testing can verify the extent to which those controls provide the specified protection.

Specification of what a system should do is often less difficult than elaborating what the system should not do. Beyond defining and confirming controls, one must probe for unacceptable behaviors and validate proper functioning in an operational environment. To be realistic and meaningful, these tests need to model the projected capabilities of realistic adversaries, as identified through threat modeling.

Cybersecurity Differences

- **It must be responsive to a rapidly changing environment –** Vulnerabilities in complex interrelated systems are usually subtle and may lie dormant for years before suddenly being exposed. Systems also evolve by the modification or addition of features and by new interactions with other hardware and software, any of which can introduce new vulnerabilities.

- **The adequacy of established controls is under constant active probing –** Threat actors of widely varying motivations, capabilities, and resources fill the arena. When they can expose the weakness of a control they will promptly seek to exploit it and, in some cases, expose it to other threat actors. The ability and resources possessed by threat actors will only increase, especially as state- sponsored attacks increase.

- **Cybersecurity testing must address detection, response, and recovery after controls fail –** It needs to establish the resilience of the system when vulnerabilities are successfully exploited. It must evaluate how well risk mitigation supplements risk avoidance.

- **Human shortcomings are at least as prominent as technological challenges –** Exploits through various low-tech means (known as social engineering) are a leading cause of security failures. Countermeasures must address policies, procedures, and awareness campaigns.

Cybersecurity Testing Approaches

Of all the quality attributes, security might be the most difficult to "bolt on" or "patch in" after substantial software development has already been done. Cybersecurity test planning must contribute to the design and implementation of a system as early as possible. It should reinforce secure design and coding best practices, and include a risk analysis that is focused on cybersecurity.

Risk exists when a threat might take advantage of a vulnerability. Lowering the probability of that occurring is known as risk avoidance, and decreasing the consequences when it does occur is known as risk mitigation. To go one step further, risk mitigation must also be tested by probing the responses that occur when a control fails. By revealing otherwise undetected weaknesses, cybersecurity testing can direct efforts that support risk avoidance. The goal is to reduce overall risk exposure (and its uncertainty) to an acceptable level.

Potential security weaknesses in isolated system components may be investigated by static techniques. Manual or automated inspections, such as port scans and code scans, can provide early identification of insecure design patterns or coding practices. After a completed system is installed in its operational environment, additional dynamic security issues will arise (i.e., issues that can only be seen during execution) and must also be addressed.

Testing can enhance each stage of a cybersecurity effort as follows:

- **Identify –** Confirm identification, categorization and prioritization of the data and processes to be safeguarded (note that an adversary might value these assets differently and have different priorities)
- **Protect –** Analyze the protection of each asset category with corresponding controls that will stop or slow attempts to compromise the system
- **Detect –** Demonstrate the ability to detect intrusions and provide timely actionable analysis
- **Respond –** Exercise the responses and determine how well affected parties are notified, damage is minimized, and further access is shut off
- **Recover –** Demonstrate the speed and extent of recovering operational status and restoring data and confidence

Conducting Cybersecurity Testing

A testing project should establish terms of engagement that define the nature and scope of activities. If a live system is to be tested, it should specify how much notice will be given and to whom. All cybersecurity testing must be pre-authorized in writing by appropriate management to avoid testers being mistaken for malicious insiders (which can carry criminal penalties).

Cybersecurity testing covers the full software development lifecycle, so it will parallel and reinforce secure software engineering practices. It may be performed or be a part of reviews and audits at key specification, design, implementation, and integration stages. It will evaluate the performance of threat modeling and static code analysis.

Cybersecurity testing, like other types of testing, can and should be conducted in two different modes: “black-box” - which attends to external system behaviors; and “white- box” (or clear-box) – which utilizes structural knowledge of the as-built system. In black-box testing, an “outsider” will gather information via system reconnaissance. They will use that information to craft attacks that can be mimicked in penetrationtesting to see what they can attack. In white-box testing, the “insider” threat is modeled by treating the system’s internals as visible and thus uniquely exploitable.

A wide range of testing approaches are available. One automated black-box technique involves fuzzing - inserting random variations of expected input values to detect sensitivities that might be exploited. Another mode of testing is derived from the practice of military exercises. A designated “red team” of attackers (composed of internal or external experts) is pitted against a “blue team” of defenders (drawn from internal operations personnel). The exercise may be performed on a facsimile of the SUT, or may be a “tabletop” exercise without a real system.

Targeted tests should probe the adequacy of specific controls. These may include:

- Policy and procedure enforcement
- System hardening (reducing the attack surface by eliminating as many security risks as possible)
- Access control mechanisms for authentication (who you are), authorization (what you can do), and accountability (what did you do)
- Input validation
- Encryption
- Error and exception handling
- Intrusion detection
- Malware scanning
- Resistance to social engineering

The Environment of Constant Change

Best cybersecurity and cybersecurity testing practices may be found in various technical guidance documents and consensus standards, as well as through professional organizations and educational institutions. “Best practices” may be “required practices”, if mandated by government laws. Regulatory requirements may also apply to specific financial, medical, transportation, energy or other sectors. In such settings, the adequacy of testing would be judged by the extent to which it confirmed compliance with applicable mandatory requirements.

New technologies and new applications of existing technologies will continually introduce new security concerns. Seemingly stable, long-time tools and applications often reveal long-time vulnerabilities under the scrutiny of determined adversaries. External laws and regulations, as well as user expectations, change over time too. Keeping up-to-date with changes in these requirements and best practices, as well as technological advances, should be accomplished through ongoing professional development - reading, conversing and attending events with fellow practitioners.

References

ISO/IEC/IEEE Standards

- ISO/IEC/IEEE 12207:2017
- ISO/IEC/IEEE 15288

Trademarks

The following registered trademarks and service marks are used in this document:

- AT*SQA® is a registered trademark of the Association for Testing and Software Quality Assurance

Books

[Anderson00]: Anderson, L.W. and Krathwohl, D.R. (2000) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Allyn & Bacon: Boston MA, ISBN-10: 080131903X

[Firtman]: Maximiliano Firtman, "Programming the Mobile Web", O'Reilly Media;

Second Edition (April 8, 2013), ISBN-10: 1449334970

[PMBOK] Project Management Institute, "A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Sixth Edition, 2017, ISBN-10: 9781628251845

Other References

The following references point to information available on the Internet. Even though these references were checked at the time of publication of this syllabus, AT*SQA cannot be held responsible if the references are not available anymore. AT*SQA is not endorsing any of these sites or their products. The references are provided as a source of information only.

https://techcrunch.com/2013/03/25/ip-oh-my-gosh-all-that-money-just-disappeared/ https://www.reuters.com/article/us-facebook-settlement/facebook-settles-lawsuit-over-

2012-ipo-for-35-million-idUSKCN1GA2JR

[NASDAQ] https://www.sec.gov/news/press-release/2013-2013-95htm

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Revision 2. 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[WCAG] https://www.w3.org/WAI/policies/

AT*SQA

MICRO-CREDENTIAL

Cybersecurity Testing

www.atsqa.org