SECO INSTITUTE

INFORMATION SECURITY

IT-SECURITY

DATA PROTECTION

ETHICAL HACKING

SECURE SOFTWARE

BUSINESS CONTINUITY

CRISIS MANAGEMENT

IT SECURITY FOUNDATION

UNDERSTANDING IT SECURITY ADMINISTRATION

Sample Exam Questions

Introduction

This document contains 5 questions (and answers) that help you familiarise yourself with the structure and topic areas of the SECO-Institute's IT-Security Foundation certification exam.

To download our Complete Sample Exam, create a free study account at https://members.seco-institute.org

We recommend you to take the Complete Sample Exam before registering for the certification exam.

The results of the Sample Exam do not count towards your examination score.

Certification exam

You can book your exam with an accredited training partner or directly with the SECO-Institute. To schedule an exam at the SECO-Institute's website, go to: https://www.seco-institute.org/how-to-book-your-exam-schedule-an-exam/

By passing the certification exam and earning an IT-Security Foundation certificate, you demonstrate that you have an overall understanding of fundamental IT security principles, security challenges and best-practice remedies. You are aware of the security threats that face your IT infrastructure, and you know how to secure each component to protect your organisation from security risks.

Exam format

- 40 multiple-choice questions
- Time allowed: 60 minutes
- Closed-book exam
- Pass mark: 60% of the total marks

Questions

Question 1

Which of the following gives a logical order for computer architecture components, where each following component is built upon the previous component?

A. Firmware, Hardware, Software, Applications
B. Hardware, Firmware, Operating System, Applications
C. Hardware components, Memory and I/O operations, File system
D. Hardware, Operating System, Software, User Data

Question 2

What is the correct definition of 'emanations'?

A. Electrical, mechanical, optical and/or audible signals generated by devices
B. Using signals for purposes they were initially not intended for
C. Timing channels that modify the timing of events relative to each other
D. Storage channels that communicate with each other via a stored object

Question 3

Which of the following statements is correct?

A. An OS is in control of all bits written to a storage medium
B. An OS manages all hardware connected to the system it is running on
C. An OS is in control of all I/O communications to and from the system
D. An OS manages the users of the peripherals connected to it

Question 4

What is the best way to defend an individual PC against malware?

A. Install anti-malware software, automatically install patches, and regularly review the system's log files
B. Install a host-based Intrusion Detection System, install antivirus software, and automatically install patches
C. Harden the system, automatically install patches, install anti-malware software, and install a host-based firewall
D. Automatically install patches, install antivirus software, and make opening of unsigned messages or files impossible

Question 5

What is the best solution to guarantee security in client-server applications?

A. Do all security verification on the server side
B. Validate user input before accepting it
C. Encrypt all traffic between client and server
D. Use security components without known vulnerabilities

Answers

Question	Answer	Explanation
1	B	A computing platform consists of internal hardware (e.g. CPU, memory chips, logic circuits) and external hardware (e.g. printer, keyboard, display). Hardware is controlled by firmware (drivers and other software directly associated with hardware) to make it function properly. The Operating System communicates with that firmware to make it do what it should do. In their turn applications (e.g. a web browser) can be used by users to tell the Operating system what specific tasks should be performed.
2	A	All devices are prone to generate and emit, or in other words emanate, signals. When it is possible for an unauthorised third party to receive these signals and infer information from them, it might be possible to use this information in an attack.
3	C	To be able to guarantee the integrity of the system an OS must be in control of all I/O. However, that does not mean it is in control of all data written to a storage medium. Once data becomes part of the slack space on that medium, the OS will not bother itself with that data anymore. Nor does it mean it has to be in control of all hardware connected to it. It will be in control of essential hardware, like memory, but for example peripherals will not be fully controlled by the OS (e.g. a printer will still need to manage its own firmware and possibly even its users).
4	C	Hardening and installing the latest patches will reduce the attack surface of the PC, as do using firewalls and antivirus/anti-malware software. Intrusion Detection Software will not prevent a system from being hacked (you can use Intrusion Prevention Systems for that). Blocking the opening of unsigned messages or files will seriously restrict the usability of the PC, and not block many types of attack. Reviewing log files is a good idea (if one has the knowledge to interpret them), but will always be after-the-fact.

5	A	Since the client side cannot be fully controlled, all security should be done on the server. That is the only way to be reasonably sure the data has not been manipulated. Encryption will help against eavesdropping and manipulation on the wire, but gives no guarantees on the host. Validating input is good, but as long as the client side is not trusted it will not provide sufficient assurance, not even when done exclusively on the server side. Using secure components is good as well, but what if the user is manipulated or has bad intentions? Or if the network is not trustworthy?

INFORMATION SECURITY

IT-SECURITY

DATA PROTECTION

ETHICAL HACKING

SECURE SOFTWARE

BUSINESS CONTINUITY

CRISIS MANAGEMENT