IT-SECURITY PRACTITIONER

Sample Exam Questions

SECO INSTITUTE

Introduction

This document contains 4 questions (and answers) that help you familiarise yourself with the structure and topic areas of the SECO-Institute's IT-Security Practitioner 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/

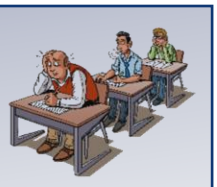
By passing the certification exam and earning an IT-Security Practitioner certificate, you demonstrate that you possess the skills of a competent IT Security professional. You have an in-depth understanding of attack trends and industry-approved mitigation techniques, you can perform a basic penetration test, and you can accomplish traditional security management tasks, such as developing policies and procedures.

Exam format

- Computer-based with remote proctoring
- Multiple-choice questions and essay-type questions
  - 10 multiple-choice questions
  - 5 open-ended questions
  - 1 essay question based on a case study

- Time allowed : 120 minutes
- Closed-book exam
- Pass mark : 60% of the total marks

Questions

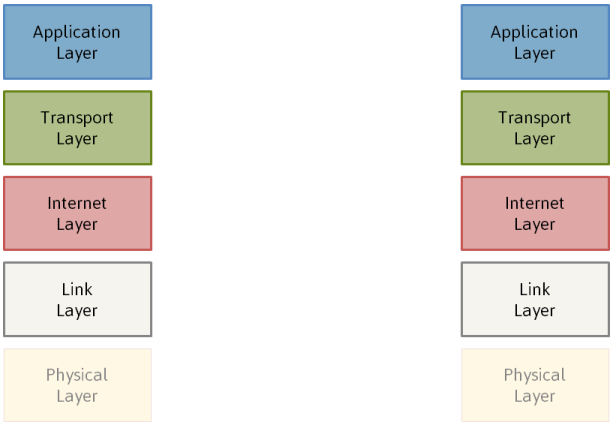


Question 1

Imagine that passwords are kept in a file on an arbitrary system.
What measures should be taken to preserve the confidentiality and the integrity of the passwords?

Question 2

a) On how many layers does a stateless firewall operate when it filters network traffic between two applications on separate systems? (See figure to the right.) Name those layers.
b) On which layers does filtering based on IP addresses and port numbers take place?
c) If Application-layer content has been encrypted, would it still be possible to filter out packets with particular IP addresses?
d) Does it make any sense for a stateless firewall to filter traffic on the Physical Layer? Why or why not?



Question 3

Booking.com asks you to test their site on the presence of vulnerabilities. Before the test, Booking asks you to sign a responsible disclosure contract. What does that mean for you? And what possible agreements could be made in that type of contract?

Question 4

Your company's Security Operations Center gets an alert. The message states that a core server of the enterprise resource planning process has been compromised and certain important files have been encrypted. The message states that a ransom must be paid in order to decrypt the files again. What possible actions should you consider if you mark this event as an incident?

Hint: the ENISA model should be taken as reference when you answer this question.

Answers

Question 1 – Answer

Confidentiality must be preserved by assigning privileges to the files where passwords – or hashed passwords – are stored. Security labels may also be attached to those files to prevent unauthorised disclosure. The same counts for databases or registries, where passwords are stored in tables.

Integrity is preserved by hashing the password files or columns in the mentioned tables. Individual passwords are often stored as hashes instead of the original string values.

Optional: Salting is done to make it harder to crack passwords out of the hash values. Each individual password is concatenated with a random value, belonging to that particular password, before the hash is calculated and stored into the password file or database. The salt values must also be stored along with the password hashes. Advantage: Identical passwords will have different hash values.

Question 2 – Answer

a) A stateless firewall consists of four layers, from bottom up: Physical, Link, Internet, and Transport.
b) The filtering takes place on the Internet and the Transport layer. It compares IP addresses, protocol numbers, and TCP or UDP port numbers with a set of predefined rules to filter them.
c) Because a stateless firewall does not examine the contents of application messages, this content may be encrypted. The headers of IP packets and TCP or UDP segments are not affected by this encryption.
d) Filtering the physical layer makes no sense because this layer only transmits bits. Content is not relevant.

Question 3 – Answer

From the lesson: Responsible disclosure is a tool for organisations and incident reporters to facilitate responsible reporting and handling of vulnerabilities in information systems, software and other ICT products. Incident reporters must hold off on publication until the organisation has been able to remedy the problem. The public prosecutor has its own responsibility to press charges on incident reporters.

A responsible disclosure contract might contain the following:

– Declaring to hold proprietary or private information in strict confidence
– Never to make use of proprietary information for your own purposes
– Not to copy proprietary information nor reverse-engineer it from innocent information
– Immediately inform the disclosing party of any important information or vulnerability found
– The agreement shall be governed by the laws of the jurisdiction in the country where the (headquarters of the) disclosing party is located

Example of a standard agreement: http://www.ipwatchdog.com/tradesecret/standard-confidentiality-agreement/

Question 4 – Answer

The relevance of the incident has already been determined, otherwise it would not have been declared an incident. Then the identification and classification process will be started, followed by a triage, in which impact and development over time will be determined. Thereafter, the person to resolve the incident will be assigned. An incident “ticket” will be opened, and the resolver will be given the task to analyse, solve, report, and finally archive the incident.

© SECO Institute

All rights reserved. No part of this document or its contents may be adapted, translated, stored, reproduced and/or made public in any form or by any means, either electronically through print, (photo)copy, recording, in digital form or in any other way, without the prior written permission of the SECO Institute. Making this document public also explicitly includes its use within courses, lessons, trainings, seminars and other forms of instruction or demonstration.

This document is granted to those who are participating or have participated in a training, course, seminar, or similar event developed or authorised by the SECO Institute. The contents of this document, or parts thereof, may not be submitted or made available to third parties under whatever title without the prior explicit permission of the SECO Institute.

Although the SECO Institute has done everything to prevent irregularities in this document, errors may still occur. Therefore, any person who acts on the basis of the content of this document does so at his/her own risk and is aware of the fact that the SECO Institute cannot be held accountable for any possible damage ensuing from his/her actions.

The authors of this document have done their utmost to identify all possible rightful parties other than the SECO Institute. Should you be a rightful party, or represent one, or know one, and be of the opinion that this document unjustly contains copyrighted material, please do not hesitate to contact the SECO Institute.