# IT-SECURITY FOUNDATION

## Sample Exam

SECO INSTITUTE

# Sample Exam IT-Security Foundation

SECO-Institute issues the official IT-Security courseware to accredited training centres where students are trained by accredited instructors. Students can take their exams at an accredited exam centre or directly at the SECO-Institute. Attending an official certification course is not a prerequisite for taking an exam. Upon successful completion of a foundation exam (with a passing score of 60%), students can claim their digital badge at the SECO-Institute.


This document provides a sample exam for you to familiarise yourself with the structure and topic areas of the current IT-Security Foundation examination. We strongly recommend you to test your knowledge before taking the actual assessment. The results of this test do not count towards your certification assessment.

**Examination type**

- Computer-based
- 40 Multiple choice: 2,5 points per question

**Time allotted for examination**

- 60 minutes

**Examination details**

- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no
- The Rules and Regulations for SECO-Institute examinations apply to this exam

# Questions

**Question 1**

Which order for Computer Architecture Components is correct?

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

**Question 2**

What is the correct definition of 'Emanations'?

A. Electrical, mechanical, optical signals that contain information
B. TEMPEST: "hear" key strokes as typed on keyboards
C. Timing channels that modify the timing of events relative to each other
D. Storage channels that communicate via a stored object

**Question 3**

What components are NOT managed by the Operating System?

A. Hardware components and Memory
B. I/O operations to local File systems
C. User processes as a collection of instructions and assigned resources
D. Data blocks read and written disk

**Question 4**

What kind of system can run Multiple OSes simultaneously?

A. Grid computing
B. Mainframe
C. Multi-tier system
D. Grid computing Multi layered OS

**Question 5**

Which kind of software is used to connect different applications?

A. Middleware
B. Monolithic OS
C. Multithreading OS
D. Multi-tier architecture

**Question 6**

What is the best way to defend a stand-alone PC against malware?

A. Install Intrusion Prevention + AV, harden system, automatically install patches
B. Automatically install patches, install host-based intrusion detection + AV, awareness training
C. Install AV + firewall, harden system, automatically install patches, educate users
D. Automatically install patches + AV, block opening of unsigned messages or files, educate users

**Question 7**

How does a switch relay traffic to nodes?

A. Simple switches repeat the data to all nodes in the Content Addressable Memory (CAM) table
B. A Switch interconnects different networks based on the destination hardware addresses of the NIC
C. A Switch can only direct traffic based on private IP addresses of local network nodes
D. Switches know the port to which each node is attached and send data only to the destination node

**Question 8**

Which layer is identical in both the OSI and the TCP/IP model?

A. Application
B. Data Link
C. Network
D. Transport

**Question 9**

Which organisation maintains the TCP/IP standards?

A. Institute of Electrical and Electronics Engineers (IEEE)
B. Internet Engineering Task Force (IETF)
C. American National Standards Institute (ANSI)
D. International Telecommunication Union (ITU)

**Question 10**

On which TCP/IP layer(s) does the ARP operate?

A. Link layer + Internet layer
B. Link layer
C. Internet layer
D. Internet layer + Transport layer

**Question 11**

What is the best description of TCP/IP Protocol Encapsulation?

A. Data frames are moved up the TCP/IP stack and each layer adds the configuration data of that layer
B. Data frames are encapsulated in the 'data' part, the 'address' part of the packet cannot be encrypted
C. Data frames are passed down the TCP/IP stack and each layer adds an envelope with the data necessary for that layer
D. The sender (receiver) side moves data down (up) the TCP/IP stack, this allows different software to communicate

**Question 12**

Which Security Protocol operates on the Internet layer?

A. IPsec
B. SSH
C. S/MIME
D. WPA2

**Question 13**

What is the best description of a 'statefull firewall'?

A. The firewall examines the packet headers of all sessions
B. The firewall examines the packets for each session in combination
C. The firewall examines both the packet headers and data frames
D. The firewall examines the TCP/UDP packet headers (Transport layer)

**Question 14**

What description best fits 'Network Address Translation (NAT)'?

A. The translation from IP addresses to MAC addresses
B. The translation from MAC adresses to router ports
C. The translation from IP adresses to web site names
D. The translation from public (external) to private (internal) IP addresses in the packet and vice versa

**Question 15**

Which protocol provides the best security for sock-to-socket communication?

A. SSL 3
B. IPsec
C. TLSv1.2
D. logical VPN with encryption

**Question 16**

What is the best solution to guarantee security in Client / Server applications?

A. Validate user input e.g. to avoid buffer overflows
B. Encrypt (authentication) traffic between Client and Server
C. All security must be done on the server side
D. Use security components without known vulnerabilities

**Question 17**

Which is NOT one of the Open Web Application Security Project (OWASP) most critical security risk?

A. Broken Authentication and Session Management
B. Opened attachments from untrusted origin
C. Unvalidated Redirects and Forwards in Networks, Systems and Software
D. Missing Function Level Access Control

**Question 18**

Why is securing database such a challenge?

A. Multiple users and applications can access data in the database at the same time
B. Databases are the most widely used storage places for digital information
C. Databases software enable the definition, storage, modification, administration and retrieval of information
D. The database model cannot provide transaction persistence and fault tolerance

**Question 19**

Which is NOT one of the three SQL sublanguages?

A. Data Dictionary
B. Data Definition
C. Data Manipulation
D. Data Control

**Question 20**

What item is best described by: database software to centralise the management of data?

A. Directory Service
B. Data Dictionary
C. Data Manipulation language (DML)
D. Repository

**Question 21**

Which Database Vulnerability is best described by "Avoiding security controls at the front end to access information"?

A. Aggregation
B. Compromising database views
C. Interception of data
D. Bypass attack

**Question 22**

Which is an example of an Output Control as a countermeasure against Data contamination?

A. Transaction counts, hash totals
B. Error detection and correction
C. Validation of transactions through reconciliation
D. Self-checking digits

**Question 23**

Which of the countermeasures against Database vulnerabilities is a preventive control?

A. Audit trail
B. Data contamination controls
C. Monitor database access
D. Logging database mutations

**Question 24**

What is the ROT13 encryption of "information is not knowledge" (spaces are omitted!)

A. uzradymfuazuezafwzaixqpsq
B. umevlonomnibyfjecffwyumul
C. vnfwmpopnojczgkfdggxzvnvm
D. vasbezngvbavfabgxabjyrqtr

**Question 25**

Which statement is true about a text hashed or encrypted?

A. Hashing leads to a text with a fixed length, regardless of the input
B. With sufficient computer power, a hashed text can be reproduced
C. Hashing a text and encrypting the hash is never useful
D. Encrypting a text and hashing the cryptotext is never useful

**Question 26**

Ensuring confidential communication with 1000 users, how many keys are necessary using symmetric vs. asymmetric encryption?

A. For 1000 users, 124750 symmetric keys and 1000 asymmetric keys are needed
B. For 1000 users, 1000 symmetric keys and 124750 asymmetric keys are needed
C. For 1000 users, 499500 symmetric keys and 2000 asymmetric keys are needed
D. For 1000 users, 2000 symmetric keys and 499500 asymmetric keys are needed

**Question 27**

How are the disadvantages of asymmetric encryption solved for exchanging confidential information?

A. The message key is encrypted using the public key of the recipient
B. The message key is encrypted using the public key of the sender
C. The message key is exchanged using a confidential hash function
D. The message is encrypted using a previously shared key

**Question 28**

When is a hash function considered to be comprimised?

A. When a colission text can be crafted in a short time to fit any given hash
B. When a colision attack is (much) more succesful than theory predicts
C. When te integrity of the hash function no longer can be guaranteed
D. When a better hash function is available to replace its predecessor

**Question 29**

Using good and confidential encryption keys, which main factor determines the strenght of a crypto system according to Kerckhoff's principle?

A. The fact that the algorithms must remain secret for attackers (black box)
B. The (publicly assessed) strength of the algorithms, used to produce ciphertexts
C. The number of possible keys (keyspace) must be large enough to make brute force attacks unfeasible
D. To increase the difficulty of attacks, no information must be publicly available (security by obscurity)

**Question 30**

What is NOT a task of the Certifcate Authority (CA)?

A. Assure explicit trust by all parties
B. Issue, revoke and manage digital certifcates
C. Certify that a digital certifcate represents the certifcate owner
D. Initialise the certification process

**Question 31**

Which field is NOT included in a PKI certificate?

A. X.500 name of the RA
B. Validity of the certificate
C. Public key of the owner
D. The PKI algorithm used

**Question 32**

What is NOT a valid statement on Transport Layer Security / Secure Sockets Layer (TLS/SSL)?

A. Only TLS implementations above version 1.1 are secure
B. Operates at the OSI Transport, Session, Presentation and Application layer
C. It is based on asymmetric key cryptography, only for encryption
D. Capable of securing any transmission over TCP

**Question 33**

What term is best described by: trying to crack the implementation of an algorithm by observing power or time consumption

A. Cryptanalysis
B. Analytical attack
C. Side channel attack
D. Plaintext attack

**Question 34**

What is the function of a 'salt' value when storing a user password?

A. Varying the salt value per user ensures that not all users with the same password have the same hash
B. The salt value is a standard offset for the Random Number Generator, to mitigate against a rainbow table attack
C. Varying the salt value per user ensures that brute force attacks become unfeasible
D. Adding 'salt' to the password make the hash produced less predictable

**Question 35**

Which of the following statements about the Kerberos protocol is NOT true?

A. Kerberos is a network authentication protocol developed by MIT for Unix systems
B. Guards the network with Authentication, Authorisation and Asymmetric Cryptography
C. Kerberos provides strong authentication for client/server applications
D. Kerberos provides end-to-end security without sending passwords over the network

**Question 36**

Which of the following functions does NOT support accountability?

A. Strong authorisation
B. Audit logs (intelligence)
C. User training and awareness
D. Organisational behaviour

**Question 37**

What is NOT one of the principles governing the Authorisation process?

A. Need-to-know
B. Least privilege
C. Segregation of duties (SoD)
D. Account ownership

**Question 38**

Which of the following items is NOT an Authorisation Pitfall?

A. Segregation of duties (SoD) insufficiently applied
B. Too complex role models
C. No account lockout after a number of logon attempts
D. Authorisation creep

**Question 39**

Which of the following statements about Mobile Identity is FALSE?

A. Mobile devices are used for accessing social media, financial services, governmental services, education, healthcare, payment and many other services
B. The most important security measures include awareness, authentication (e.g. fingerprint scanner) and encryption of communication
C. Mobile devices introduce many risks, since they can be lost or stolen (beside from being hacked)
D. Most of the identity information is stored on the mobile device

**Question 40**

Which of the following items is NOT a characteristic of Security as a Service (SECaaS)?

A. Central handling of software upgrades
B. Deployment of security expertise, including governance of Identity management
C. Vulnerability management: malware definition updates, Email & Web content filtering
D. Logging, reporting and handling of events

# Answers

| Question | Answer | Explanation |
|---|---|---|
| 1 | A | A Computer Platform consists of Hardware (e.g. CPU, memory chips, logic circuits), Firmware (software etched into a hardware) and an Operating System. On such a platform Applications (e.g. Web Browser) can run |
| 2 | A | Emanations include electrical, mechanical, optical signals that contain information |
| 3 | D | Read / write of data Blocks to Disks are managed by the Disk Controller |
| 4 | B | A mainframe is a powerful computer that can host multiple virtual machines, which can each run a different OS |
| 5 | A | Applications can communicate with each other through middleware |
| 6 | C | Hardening and installing the latest patches reduces the attack profile, as do firewalls and AV. Host-based solutions like IDS and IPS cannot be applied on a stand-alone PC. Block unsigned files will seriously restrict the usability of the PC. |
| 7 | D | A switch links the MAC hardware address of the NIC to the switch port using the CAM table and sends data only to the destination node |
| 8 | D | Transport layer is present in both models; in the OSI model the Application layer is part of the Application layer in the TCP/IP model; the TCP/IP model refers to the Link layer |
| 9 | B | The IETF maintains the TCP/IP standards, the other organisations play an important role in the development of open standards |
| 10 | A | The ARP operates on the Link + Internet layers |
| 11 | C | Each lower TCP/IP layer adds an envelope with the data necessary for that layer |
| 12 | A | Only IPsec operates on the Internet layer; SSH, S/MIME = Application layer; WPA2 = Link layer |
| 13 | B | Stateful firewalls are 'sessions aware' and examine series of packets belonging to a session |
| 14 | D | A router translates public (external) to private (internal) IP addresses in packets and vice versa |
| 15 | C | Secure Socket Layer provides SSL/TLS to encrypt data, but SSL and earlier versions than TLSv1.2 are insecure |
| 16 | C | Since the User interface is not high-secure and the Client side is not controlled, all security must be done on the server side |
| 17 | B | To avoid opening attachments from untrusted origin is an awareness issue, not a security risk of web applications |
| 18 | A | Databases are very challenging from a security perspective, since multiple users and applications access them at the same time |
| 19 | A | A Data Dictionary is not a language, but provides underlying structure of the database |

| | | |
|---|---|---|
| 20 | A | A directory service is specialised database software to centralise the management of data |
| 21 | D | Bypass Attack: bypassing security controls at the front end to access information |
| 22 | C | Only "Validation of transactions through reconciliation" is an Output control, the rest are Input controls |
| 23 | B | Data contamination input and output controls signal errors before |
| 24 | D | vasbezngvbavfabgxabjyrqtr is the correct answer |
| 25 | A | Hashing leads to a text with a fixed length, regardless of the input. So texts longer than the hash cannot be reproduced from the hash |
| 26 | C | For (n) users, (n*(n-1)/2) symmetric keys and (2*n) asymmetric keys are needed. |
| 27 | A | When the message key is encrypted using the public key of the recipient, there is only a small text that needs to be asymmetrically encrypted |
| 28 | B | When a collision attack is (much) more successful than theory predicts, then attacks might become economically viable |
| 29 | B | According to Kerckhoff's principle, the strength of a crypto system may not depend on secrecy, only on the secrecy of the key. This means that encryption algorithms and implementations can be freely published, for public review. |
| 30 | D | Initialising the certification process is a RA task |
| 31 | A | The X.500 name of the RA is not part of a PKI certificate (X.500 name of the CA is) |
| 32 | C | TLS/SSL provides both encryption and authentication services based on asymmetric key cryptography |
| 33 | C | Side channel attack = trying to crack the implementation of an algorithm by observing power or time consumption |
| 34 | A | Varying the salt value per user ensures that not all users with the same password have the same hash |
| 35 | B | Kerberos guards the network with Authentication, Authorisation and Auditing, NOT Asymmetric Cryptography |
| 36 | A | "Strong authorisation" is not a function of Accountability like "strong Authentication" |
| 37 | D | Account ownership is a supporting technique for Accountability, not a principle for the Authorisation process |
| 38 | C | "No account lockout after a number of logon attempts" is an Authentication Pitfall, not an Authorisation Pitfall |
| 39 | B | The most important security measures for Mobile Identity include awareness, authentication and encryption *in general* (i.e. communication + data storage) |
| 40 | A | Central handling of software upgrades is a characteristic of Software as a Service (SaaS), not SECaaS |

## How to book your exam?

All our exams are delivered through an online examination system called ProctorU. To enrol for an exam, go to: https://www.seco-institute.org/certification-exams/how-to-book-exam/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

Review the examination rules at
https://www.seco-institute.org/html/filesystem/storeFolder/10/Rules-and-Regulations-for-SECO-Institute-Examinations-2017-11.pdf

## Digital badges


SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

SECO-Institute doesn't issue certification titles for Foundation courses. However, upon successful completion of your Foundation exam, you can claim your digital badge free of charge at the SECO-Institute.

https://www.seco-institute.org/claim-your-foundation-badge

**ITSF-Sample Exam-EN-v1.0**