Cyber and IT Security Foundation

Sample Exam

Edition 201611

CYBER & IT SECURITY

Content

Introduction

This is a set sample questions for Cyber and IT Security Foundation (CISEF.EN).
The Rules and Regulations for EXIN's examinations apply to this exam.

This set consists of 20 multiple-choice questions. The real exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is the correct answer.

The maximum number of points that can be obtained for set of sample questions is 20. Each correct answer is worth one point. If you obtain13 points or more you will pass. For the real exam this is 26 points.

The time allowed for this set of sample questions is 30 minutes.

Good luck!

Sample exam

1 / 20

A hub represents the central component, with which a star topology-based network can be built.

What is the **main** reason that hubs are hardly ever used anymore?

A) A hub is only able to recognize the hardware address of a node, not the logical address (IP address). For this reason a hub is not suitable to be used in local network environments.

B) A hub is not able to recognize any address information. Therefore, a hub will send network traffic, which is destined for a particular host, to all other hosts in the network. For this reason the network will be overloaded when many hosts want to communicate.

C) A hub is able to recognize the hardware address of a node, but ignores this and will send network traffic, which is destined to a particular host, to all other hosts in the network. For this reason network traffic can be easily intercepted.

D) A hub is only able to recognize the logical address (IP address) of a node. For this reason a hub is not suitable to be used in local network environments.

2 / 20

ARP (Address Resolution Protocol) represents one of the most important network protocols in TCP/IP-based network environments.

What does ARP basically do?

A) ARP translates the hardware address of a node to its IP address.

B) ARP replies with the IP address of a particular node to any node that requests this.

C) ARP translates the IP address of a node to its hardware address.

D) ARP replies with the hardware address of a particular node to the default gateway.

3 / 20

An intrusion detection system (IDS) can be used to monitor and filter network traffic.

From the viewpoint of detection, which **main** IDS types can be distinguished?

A) Anomaly-based and heuristic-based
B) Anomaly-based and behavior-based
C) Signature-based and knowledge-based
D) Behavior-based and knowledge-based

4 / 20

A consultant is hired by a company that wants advice on how to organize and implement patch management. He recommends that:

1. patches should be tested first.
2. patches should be implemented as soon as possible after they are released.

What additional recommendation should he make?

A) Critical systems should be patched before the less critical ones.
B) Both critical systems and less critical systems should be patched at the same time.
C) Less critical systems should be patched before the critical ones.

5 / 20

A sandbox represents a well-known mechanism that is used for the execution of applets.

What is the **main** function of a sandbox?

A) It provides a protective area for code or applet execution.
B) It provides an execution environment for the Java Security Manager.
C) It guarantees that malware is not able to break out of the sandbox.
D) It enforces the execution of Java applets.

6 / 20

The Relational Database Management System is the dominant database management model.

What does a foreign key represent or provide?

A) It represents a column that uniquely identifies a row in a table.
B) It provides a method for referential integrity.
C) It provides a link or reference to a primary key in the same table.
D) It represents the relationship between columns.

7 / 20

Databases are very challenging from a security perspective. One of the more risky vulnerabilities is inference.

How can inference be explained?

A) As the corruption of data integrity by input data errors or erroneous processing.
B) As running processes at the same time, thus introducing the risk of inconsistency.
C) As bypassing security controls at the front end, in order to access information for which one is not authorized.
D) As deducing sensitive information from available information.

8 / 20

A digital signature is one of the most important methods to ensure the authenticity of digital information.

How is a digital signature created from the digital fingerprint (hash) of the information?

A) The hash is encrypted with the session key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with a corresponding session key.
B) The hash is encrypted with the public key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding private key.
C) The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding public key.
D) The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding public key.

9 / 20

Digital certificates represent an important component in any Public Key Infrastructure (PKI).

What should **never** be included in a digital certificate?

A) The digital signature of the certificate authority (CA) that has issued the digital certificate.
B) The private key of the party to whom the digital certificate is tied.
C) The identity of the party that owns the digital certificate.
D) The start and end date of the period, in which the digital certificate is valid.

10 / 20

The IPSec security specification provides several methods of implementation.

For what purpose and how is the IPSec tunnel mode used?

A) For end-to-end protection. Only the IP payload is protected.
B) For link protection. Only the IP payload is protected.
C) For end-to-end protection. Both the IP payload and IP header are protected.
D) For link protection. Both the IP payload and IP header are protected.

11 / 20

A governmental organization wants to ensure the integrity of information that is communicated between parties.

What is needed to achieve this?

A) Asymmetric encryption
B) Symmetric encryption
C) Both hashing and symmetric encryption
D) Both hashing and asymmetric encryption

12 / 20

Biometrics become ever more important as a means to verify the identity of users.

Which feature of biometrics represents a **major** consideration for organizations that want to implement it?

A) The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are equal.
B) The way users swipe their tablet or smartphone can be used as a behavioral mechanism for biometrics.
C) The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are within acceptable levels.
D) Face recognition cannot be used as a biometric mechanism, because it is very inaccurate.

13 / 20

Many organizations strive for Single Sign-on (SSO) for their users.

What is **most** important to consider when implementing SSO?

A) By introducing one set of credentials for all applications a cybercriminal could, by obtaining the credentials, get access to all the applications at once.
B) Enterprise wide single sign-on (ESSO) is not possible due to the diversity of applications within most organizations.
C) Enterprise single sign-on (ESSO) systems are very expensive for web applications. Because most applications are web-based, there is no business case for ESSO.
D) Single sign-on uses one set of credentials that give access to all applications at once. Hence, these credentials must be thoroughly secured.

14 / 20

What does Security Assertion Markup Language (SAML) provide?

A) Authenticate users in enterprise environments.
B) Authenticate both users and applications in enterprise environments.
C) Use social networks for authentication ('Use your Facebook account to login').
D) Secure exchange authentication information in a federated environment.

15 / 20

In the context of authorization the principle of 'need-to-know' is one of the most important ones to consider.

What does the principle of 'need-to-know' mean?

A) Critical tasks can only be completed by at least two individuals, so that collusion is needed to be able to commit fraud.
B) Users should be assigned with a minimum level of access rights to perform their tasks.
C) Users should have access to only the information that is needed to perform their tasks.
D) Users should be assigned only temporary access rights to perform their tasks.

16 / 20

An organization is **not** willing to share any resources.

Which deployment model in Cloud Computing represents the most secure one?

A) Community cloud
B) Hybrid cloud
C) Private cloud
D) Public cloud

17 / 20

Identity as a Service (IDaaS) is one of the emerging service models in Cloud Computing.

What does IDaaS provide?

A) identity governance and authentication for internal users
B) identity governance and authentication for customers, business partners and other external users
C) identity governance and authentication for internal and external users
D) Single sign-on (SSO) for external users

18 / 20

Hackers and cyber criminals usually perform their activities according to a well-structured plan.

What is the **best** order in which these activities are performed within a well-structured plan?

A) Enumeration, footprinting, getting access, privilege escalation, erasing tracks
B) Reconnaissance, enumeration, getting access, privilege escalation, erasing tracks
C) Reconnaissance, scanning, getting access, privilege escalation, maintaining access
D) Scanning, enumeration, getting access, privilege escalation, maintaining access

19 / 20

Social engineering is one of the **most** successful attack methods of cybercriminals.

What is regarded as a form of social engineering?

A) Cryptoware

B) Denial of Service (DOS) attack

C) Phishing

D) Spam

20 / 20

What tool represents a scanning tool?

A) Nessus

B) John the Ripper

C) Metasploit

D) Ophcrack

Answer key

1 / 20

A hub represents the central component, with which a star topology-based network can be built.

What is the **main** reason that hubs are hardly ever used anymore?

A) A hub is only able to recognize the hardware address of a node, not the logical address (IP address). For this reason a hub is not suitable to be used in local network environments.

B) A hub is not able to recognize any address information. Therefore, a hub will send network traffic, which is destined for a particular host, to all other hosts in the network. For this reason the network will be overloaded when many hosts want to communicate.

C) A hub is able to recognize the hardware address of a node, but ignores this and will send network traffic, which is destined to a particular host, to all other hosts in the network. For this reason network traffic can be easily intercepted.

D) A hub is only able to recognize the logical address (IP address) of a node. For this reason a hub is not suitable to be used in local network environments.

A) Incorrect. A hub is not able to handle any (logical/hardware) address information.

B) Correct. A hub is only able to forward data packets, without recognizing any address information in it. See Workbook, Chapter Node, connections and Addressing.

C) Incorrect. A hub is not able to handle any (logical / hardware) address information.

D) Incorrect. A hub is not able to handle any (logical / hardware) address information.

2 / 20

ARP (Address Resolution Protocol) represents one of the most important network protocols in TCP/IP-based network environments.

What does ARP basically do?

A) ARP translates the hardware address of a node to its IP address.

B) ARP replies with the IP address of a particular node to any node that requests this.

C) ARP translates the IP address of a node to its hardware address.

D) ARP replies with the hardware address of a particular node to the default gateway.

A) Incorrect. ARP is used to broadcast the question 'who has <IP address>?'. The host with the correct IP address will answer with its hardware (MAC) address.

B) Incorrect. ARP is used to broadcast the question 'who has <IP address>?'. The host with the correct IP address will answer with its hardware (MAC) address.

C) Correct. A host that wants to know the hardware address of another host will send an ARP broadcast in the broadcast domain of the network saying 'who has <IP address>? Tell <IP address>'. The host with the correct IP address will answer with its hardware address. See Workbook, Chapter Node connections and addressing.

D) Incorrect. ARP is used to broadcast the question 'who has <IP address>?'. The host with the correct IP address will answer with its hardware (MAC) address.

3 / 20

An intrusion detection system (IDS) can be used to monitor and filter network traffic.

From the viewpoint of detection, which **main** IDS types can be distinguished?

A) Anomaly-based and heuristic-based
B) Anomaly-based and behavior-based
C) Signature-based and knowledge-based
D) Behavior-based and knowledge-based

A) Incorrect. Heuristic-based is not a characteristic of an IDs
B) Incorrect. Anomaly-based and behavior-based are synonyms
C) Incorrect. Signature-based and knowledge-based are synonyms
D) Correct. A behavior-based (also called anomaly-based) IDS is able to detect deviations in the amount and direction of traffic and non-conformity to protocols and conventions. The other type is the knowledge-based (also called signature-based) IDS that compares network traffic to the information in its database with signatures of malicious network traffic. See ITSF Workbook, chapter Advanced network filters.

4 / 20

A consultant is hired by a company that wants advice on how to organize and implement patch management. He recommends that:

1. patches should be tested first.
2. patches should be implemented as soon as possible after they are released.

What additional recommendation should he make?

A) Critical systems should be patched before the less critical ones.
B) Both critical systems and less critical systems should be patched at the same time.
C) Less critical systems should be patched before the critical ones.

A) Incorrect. Since patches could affect a system in a negative way, less critical systems should be patched first to see whether the patch causes harm.
B) Incorrect. Since patches could affect a system in a negative way, less critical systems should be patched first to see whether the patch causes harm.
C) Correct. Since patches could affect a system in a negative way, less critical systems should be patched first to see whether the patch causes harm. See Workbook, chapter .

5 / 20

A sandbox represents a well-known mechanism that is used for the execution of applets.

What is the **main** function of a sandbox?

A) It provides a protective area for code or applet execution.
B) It provides an execution environment for the Java Security Manager.
C) It guarantees that malware is not able to break out of the sandbox.
D) It enforces the execution of Java applets.

A) Correct. A sandbox is a virtualized environment for the execution of code or applets. See Workbook ITSF, chapter Sandbox.
B) Incorrect. The Java Security Manager is an example of a sandbox.
C) Incorrect. A sandbox provides a protective area for applet execution.
D) Incorrect. A sandbox enforces limited amounts of memory and processor resources.

6 / 20

The Relational Database Management System is the dominant database management model.

What does a foreign key represent or provide?

A) It represents a column that uniquely identifies a row in a table.
B) It provides a method for referential integrity.
C) It provides a link or reference to a primary key in the same table.
D) It represents the relationship between columns.

A) Incorrect. This is the definition of a primary key.
B) Correct. A foreign key provides a link to a primary key in another table, thus providing for referential integrity. See Workbook ITSF, chapter Relational database management model.
C) Incorrect. A foreign key can also link to a primary key in other tables.
D) Incorrect. A record represents a relationship between columns.

7 / 20

Databases are very challenging from a security perspective. One of the more risky vulnerabilities is inference.

How can inference be explained?

A) As the corruption of data integrity by input data errors or erroneous processing.
B) As running processes at the same time, thus introducing the risk of inconsistency.
C) As bypassing security controls at the front end, in order to access information for which one is not authorized.
D) As deducing sensitive information from available information.

A) Incorrect. Inference is defined as deducing sensitive information from available information
B) Incorrect. Inference is defined as deducing sensitive information from available information
C) Incorrect. Inference is defined as deducing sensitive information from available information
D) Correct. Inference can be explained as deducing sensitive information from information that is aggregated from public sources. See Workbook ITSF, chapter Database vulnerabilities.

8 / 20

A digital signature is one of the most important methods to ensure the authenticity of digital information.

How is a digital signature created from the digital fingerprint (hash) of the information?

A) The hash is encrypted with the session key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with a corresponding session key.
B) The hash is encrypted with the public key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding private key.
C) The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding public key.
D) The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding public key.

A) Incorrect. Encryption of the hash must be done with the private key of the sender, and verified with the public key of the sender. See Workbook ITSF, chapter Digital signatures.
B) Incorrect. Encryption of the hash must be done with the private key of the sender, and verified with the public key of the sender. See Workbook ITSF, chapter Digital signatures.
C) Incorrect. Encryption of the hash must be done with the private key of the sender, and verified with the public key of the sender. See Workbook ITSF, chapter Digital signatures.
D) Correct. Encryption of the hash must be done with the private key of the sender, and verified with the public key of the sender. See Workbook ITSF, chapter Digital signatures.

9 / 20

Digital certificates represent an important component in any Public Key Infrastructure (PKI).

What should **never** be included in a digital certificate?

A) The digital signature of the certificate authority (CA) that has issued the digital certificate.

B) The private key of the party to whom the digital certificate is tied.

C) The identity of the party that owns the digital certificate.

D) The start and end date of the period, in which the digital certificate is valid.

A) Incorrect. The digital signature of the certificate authority (CA) is vital to trust the certificate.

B) Correct. The private key should be kept secret at all times and should therefore not be published in a digital certificate. Instead, the public key is published with the digital certificate. See Worbook ITSF, chapter Public Key Infrastructure.

C) Incorrect. The identity of the party that owns the digital certificate is necessary to trust the certificate.

D) Incorrect. The period in which the digital certificate is valid is vital to trust the certificate.

10 / 20

The IPSec security specification provides several methods of implementation.

For what purpose and how is the IPSec tunnel mode used?

A) For end-to-end protection. Only the IP payload is protected.

B) For link protection. Only the IP payload is protected.

C) For end-to-end protection. Both the IP payload and IP header are protected.

D) For link protection. Both the IP payload and IP header are protected.

A) Incorrect. IPSec tunnel mode is used to protect links and provides both IP header and IP load encryption.

B) Incorrect. IPSec tunnel mode is used to protect links and provides both IP header and IP load encryption.

C) Incorrect. IPSec tunnel mode is used to protect links and provides both IP header and IP load encryption.

D) Correct. With IPSec tunnel mode the IP payload is protected (as with all modes). In addition, the original IP header information is protected as well. An alternative IP header with the IP address information of the endpoint of the tunnel is placed before the encrypted packed. See Workbook ITSF, chapter Virtual Private Network.

11 / 20

A governmental organization wants to ensure the integrity of information that is communicated between parties.

What is needed to achieve this?

A) Asymmetric encryption
B) Symmetric encryption
C) Both hashing and symmetric encryption
D) Both hashing and asymmetric encryption

A) Incorrect. In addition to Asymmetric encryption, also hashing is necessary to ensure integrity of information.
B) Incorrect. Only asymmetric encryption can be used to create a digital signature. Encryption of the hash must be done with the private key of the sender, and verified with the public key of the sender.
C) Incorrect. Only asymmetric encryption can be used to create a digital signature. Encryption of the hash must be done with the private key of the sender, and verified with the public key of the sender.
D) Correct. The sender should create a hash of the information, encrypt the hash with his or her private key and send the hash along with the information to the receiver. The receiver can verify the authenticity of the information by decrypting the hash with the public key of the sender. Subsequently, the integrity can be verified by creating a second hash. If the two hashes match, the integrity of the information has been preserved. See Workbook ITSF, chapter Asymmetric encryption.

12 / 20

Biometrics become ever more important as a means to verify the identity of users.

Which feature of biometrics represents a **major** consideration for organizations that want to implement it?

A) The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are equal.
B) The way users swipe their tablet or smartphone can be used as a behavioral mechanism for biometrics.
C) The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are within acceptable levels.
D) Face recognition cannot be used as a biometric mechanism, because it is very inaccurate.

A) Correct. With biometrics, there should be a balance between the acceptance and rejection errors. See Workbook ITSF, chapter Biometrics.
B) Incorrect. That a biometric method like swype dynamics can be used is not a security consideration.
C) Incorrect. Crossover error rate is the rate at which both acceptance and rejection errors are equal
D) Incorrect. Face recognition is not the most accurate biometric method, but it can still be used if false-acceptance errors are less important than false rejection errors.

13 / 20

Many organizations strive for Single Sign-on (SSO) for their users.

What is **most** important to consider when implementing SSO?

A) By introducing one set of credentials for all applications a cybercriminal could, by obtaining the credentials, get access to all the applications at once.
B) Enterprise wide single sign-on (ESSO) is not possible due to the diversity of applications within most organizations.
C) Enterprise single sign-on (ESSO) systems are very expensive for web applications. Because most applications are web-based, there is no business case for ESSO.
D) Single sign-on uses one set of credentials that give access to all applications at once. Hence, these credentials must be thoroughly secured.

A) Correct. By its nature, single sign-on introduces the so-called key to the kingdom. Therefore, additional security measures should always be considered with SSO. See ITSF_IT-Security_Foundation-Day_2-20160107 slide 67
B) Incorrect. It is possible to implement ESSO for all sorts of applications, e.g. by using SAML.
C) Incorrect. It is not very expensive to implement ESSO even for web applications, e.g. by using SAML.
D) Incorrect. Because credentials need to be thoroughly secured at all times, this is not specific for single sign-on.

14 / 20

What does Security Assertion Markup Language (SAML) provide?

A) Authenticate users in enterprise environments.

B) Authenticate both users and applications in enterprise environments.

C) Use social networks for authentication ('Use your Facebook account to login').

D) Secure exchange authentication information in a federated environment.

A) Incorrect. SAML is an XML-based standard used to exchange authentication and authorization information.

B) Incorrect. SAML is an XML-based standard used to exchange authentication and authorization information.

C) Incorrect. SAML is an XML-based standard used to exchange authentication and authorization information.

D) Correct. SAML is used to exchange authentication information (called assertions) in a federated environment. See ITSF_IT-Security_Foundation-Day_2-20160107 slide 70

15 / 20

In the context of authorization the principle of ‘need-to-know’ is one of the most important ones to consider.

What does the principle of ‘need-to-know’ mean?

A) Critical tasks can only be completed by at least two individuals, so that collusion is needed to be able to commit fraud.
B) Users should be assigned with a minimum level of access rights to perform their tasks.
C) Users should have access to only the information that is needed to perform their tasks.
D) Users should be assigned only temporary access rights to perform their tasks.

A) Incorrect. 'Need to know' means that users should have access to only the information that is needed to perform their tasks.
B) Incorrect. 'Need to know' means that users should have access to only the information that is needed to perform their tasks.
C) Correct. The principle of need-to-know means that users have access to only the necessary information. See ITSF_IT-Security_Foundation-Day_2-20160107 slide 78.
D) Incorrect. 'Need to know' means that users should have access to only the information that is needed to perform their tasks.

16 / 20

An organization is **not** willing to share any resources.

Which deployment model in Cloud Computing represents the most secure one?

A) Community cloud
B) Hybrid cloud
C) Private cloud
D) Public cloud

A) Incorrect. A community cloud is deployed by a community of organizations with shared concerns.
B) Incorrect. In a hybrid cloud resources are shared with other parties.
C) Correct. A private cloud is the exclusive domain of the organization itself. See Workbook ITSF, chapter Cloud Computing characteristics.
D) Incorrect. In a public cloud resources are shared with other parties.

17 / 20

Identity as a Service (IDaaS) is one of the emerging service models in Cloud Computing.

What does IDaaS provide?

A) identity governance and authentication for internal users
B) identity governance and authentication for customers, business partners and other external users
C) identity governance and authentication for internal and external users
D) Single sign-on (SSO) for external users

A) Incorrect. IDaaS provides identity governance and authentication for both internal and external users.
B) Incorrect. IDaaS provides identity governance and authentication for both internal and external users.
C) Correct. IDaaS provides for both identity governance and authentication for all user groups, the organization has a relationship with. See Workbook ITSF, chapter Identity as a Service (IDaaS).
D) Incorrect. IDaaS provides services for both internal and external users.

18 / 20

Hackers and cyber criminals usually perform their activities according to a well-structured plan.

What is the **best** order in which these activities are performed within a well-structured plan?

A) Enumeration, footprinting, getting access, privilege escalation, erasing tracks
B) Reconnaissance, enumeration, getting access, privilege escalation, erasing tracks
C) Reconnaissance, scanning, getting access, privilege escalation, maintaining access
D) Scanning, enumeration, getting access, privilege escalation, maintaining access

A) Incorrect. 'Footprinting' is not a term linked to hacking systems, 'fingerprinting' is.
B) Correct. Reconnaissance and enumeration can be defined as the activities to gather information that must be completed first in order to be able to get access. See Workbook ITSF, chapter Steps for penetration.
C) Incorrect. Erasing tracks is essential to hide system breaches.
D) Incorrect. Erasing tracks is essential to hide system breaches.

19 / 20

Social engineering is one of the **most** successful attack methods of cybercriminals.

What is regarded as a form of social engineering?

A) Cryptoware
B) Denial of Service (DOS) attack
C) Phishing
D) Spam

A) Incorrect. Cryptoware operates without the oversight of the system user.
B) Incorrect. A DOS attack is an attack to restrict access to services, independent of user actions.
C) Correct. Phishing can be regarded as a means to mislead people to divulge confidential information. See Workbook ITSF, chapter Attack categories.
D) Incorrect. Spam is a commercial message sent at a large group of recipients.

20 / 20

What tool represents a scanning tool?

A) Nessus

B) John the Ripper

C) Metasploit

D) Ophcrack

A) Correct. Nessus is one of the most well-known tools to scan for vulnerabilities. See Workbook ITSF, chapter Tools.

B) Incorrect. John the Ripper is a tool to brutely force passwords.

C) Incorrect. Metasploit is a hacking toolkit.

D) Incorrect. Ophcrack is a tool to brutely force Windows passwords.

Evaluation

The table below shows the correct answers to the questions in this set of sample questions.

Question	Answer Key
1	B
2	C
3	D
4	C
5	A
6	B
7	D
8	D
9	B
10	D
11	D
12	A
13	A
14	D
15	C
16	C
17	C
18	B
19	C
20	A

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER