EXIN

# EXIN Cyber & IT Security

FOUNDATION

Certified by EXIN

## Sample Exam

Edition 202203

# Content

# Introduction

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

This 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 this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for this exam is 60 minutes.

Good luck!

# Sample exam

**1 / 40**
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 / 40**
Currently, several technologies are connected to the Internet, for example smartphones, tablets and IoT. Therefore, the number of public IP addresses will not be enough in the future.

Based on this scenario, which statement is correct?

**A)** IPv4 has an address space of 32-bits, which is enough for the future.
**B)** IPv4 with NAT (Network Address Translation) functionality has enough public IP for the future.
**C)** IPv6 addresses will be enough just working with IPv4 addresses.
**D)** IPv6 has an address space of 128 bits, which is enough for the future.

**3 / 40**
Which IP version **best** anticipates on the exhaustion of public IP addresses in the near future?

**A)** FTP
**B)** HTTP
**C)** S/MIME
**D)** SMTP

**4 / 40**
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.

**5 / 40**
A security analyst needs to perform a forensic analysis on a computer, because this computer was used to steal strategic information from the corporate server which was sold to a competitor.

What is the key component that needs to be analyzed?

**A)** Hardware
**B)** Software
**C)** Firmware
**D)** CPU

**6 / 40**
Which CPU family was developed by Apple?

**A)** A5
**B)** Core i7
**C)** Power8
**D)** Sparc T5

**7 / 40**
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.

**8 / 40**
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

**9 / 40**
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.

**10 / 40**
A software engineer is developing a web application, but the information security manager is worried about the security requirements for this application.

Which assumption made by the software engineer is correct?

**A)** The application server side can trust the information coming from the user.
**B)** The authentication is the only control necessary to ensure the user security.
**C)** The digital certificate ensures the security of the data exchanged between client and server.
**D)** The security misconfiguration will be addressed in the production environment.

**11 / 40**
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.

**12 / 40**
After an analysis, a consultant recommends to the client the implementation of a service directory to centrally manage users and groups.

What is an example of Directory Services that the client will need to implement?

**A)** Data Definition Language (DDL)
**B)** Directory Analysis Procedure (DAP)
**C)** Meta Data Dictionary (MDD)
**D)** Windows Active Directory (AD)

**13 / 40**
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

**14 / 40**
Databases are important to the business, so access and activities must be monitored.

What is the **main** objective of Auditing monitoring?

**A)** Determine and guard the amount of storage needed for log data
**B)** Monitor actions performed by whom, at what time, on which object
**C)** Prevent security incidents by providing logging and audit tables
**D)** Verify the legally prescribed retention and archiving of log data

**15 / 40**
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 private 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.

**16 / 40**
Referring to the well-known substitution ciphers, such as Caesar's Cipher, what is the result of the word "SECURITY" encrypted through the following schema?

SCHEMA:
A = 1, B = R, C = @, D = /, E = T, I = (, R = !, S = 5, T = -, U = &, Y = X

**A)** 5T@&!(-X
**B)** 5T@-!(-@
**C)** ST@&!@-X
**D)** 5E@&!(@X

**17 / 40**
A network administrator sent a message signed with his private key.

Which of the following is correct?

**A)** The origin of this message can be ensured because it was signed with the private key of the sender.
**B)** The origin of this message can be ensured if he uses the algorithm AES before sending this message.
**C)** The origin of this message can be ensured if he uses the algorithm SHA-2 before sending this message.
**D)** The origin of this message cannot be ensured because it was signed with a private key only.

**18 / 40**
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

**19 / 40**
The Public Key Infrastructure (PKI) consists of hardware, software, protocols, procedures, policies and standards to manage the creation, the administration, the distribution and the revocation of the digital certificates and keys.

What is the purpose of a Certificate Revocation List (CRL)?

**A)** CRL presents certificates with an expired validity date only.
**B)** Irreversibly or temporary revoke certificates that are no longer valid or have key compromised.
**C)** Irreversibly revoke certificates that are no longer valid.
**D)** Temporary revoke certificates that are no longer valid.

**20 / 40**
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.

**21 / 40**
A secure channel has been established between two hosts using TLS (Transport Layer Security) version 1.2.

Regarding this TLS, which of the following statements is correct?

**A)** TLS is based on asymmetric key cryptography and operates only on the OSI Transport layer.
**B)** TLS provides data encryption and authentication, and is based on asymmetric key cryptography.
**C)** TLS provides data encryption and authentication, and is based on symmetric key cryptography.
**D)** TLS provides data encryption, is based on symmetric key cryptography and operates only on the transport layer.

**22 / 40**
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.

**23 / 40**
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.

**24 / 40**
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.

**25 / 40**
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.

**26 / 40**
What is an attacker able to do when a single salt value is used for all passwords in a database?

**A)** Add the salt again and get the plaintext values.
**B)** Remove the first characters of the hash to bypass the salts.
**C)** Remove the salt and decrypt the passwords.
**D)** Use the same salt and create a database of passwords and their hash values.

**27 / 40**
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.

**28 / 40**
How many parties (minimum) have a role in an OpenID Connect authentication data flow?

**A)** 2
**B)** 3
**C)** 4
**D)** 5

**29 / 40**
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

**30 / 40**
What is true about the public cloud?

**A)** Parts are used by a single organization and parts are used by a group of organizations.
**B)** It is used by a single organization.
**C)** It is used by a small group of organizations with shared concerns.
**D)** It is used by any organization that wants to use it.

**31 / 40**
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

**32 / 40**
An organization wants to host a web service, but does not want to deal with buying and maintaining hardware or keeping the operating system up-to-date.

What type of service model should they ask for?

**A)** IaaS
**B)** PaaS
**C)** SaaS
**D)** SECaaS

**33 / 40**
There is always a risk when a cloud provider who provides a solution such as SaaS or PaaS goes out of business.

What is this risk for the company who uses this cloud solution?

**A)** Continuity risk
**B)** Jurisdiction risk
**C)** Legal risk
**D)** Storage risk

**34 / 40**
Why would a CEO of a company want to move the key corporate systems to the cloud?

**A)** To decrease the technology cost
**B)** To decrease the leak of sensitive information
**C)** To decrease security vulnerabilities
**D)** To decrease unauthorized access to customer information

**35 / 40**
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

**36 / 40**
There are four main attack categories when it comes to exploiting vulnerabilities.

What is **not** one of the four main attack categories?

**A)** Full penetration
**B)** Information theft or disclosure
**C)** Insider misuse

**37 / 40**
A certain type of attacker knows how to write exploits, uses social engineering to gain information about their target and collects data. The motives of the attacker are unclear and the attacker is not always malicious.

What type of attacker is this?

**A)** Black Hat Hacker
**B)** Gray Hat Hacker
**C)** Hacktivist
**D)** White Hat Hacker

**38 / 40**
What tool represents a scanning tool?

**A)** Nessus
**B)** John the Ripper
**C)** Metasploit
**D)** Ophcrack

**39 / 40**
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

**40 / 40**
A hacker gained access to a web server, using a carefully thought-out step-by-step plan.

Which step did he take immediately after “Penetration and access”?

**A)** Fingerprinting
**B)** Privilege escalation
**C)** Reconnaissance
**D)** Vulnerability assessment

# Answer key

**1 / 40**
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. *Fundamentals of Information Systems Security, Chapter 10: Local Area Networks*
**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 / 40**
Currently, several technologies are connected to the Internet, for example smartphones, tablets and IoT. Therefore, the number of public IP addresses will not be enough in the future.

Based on this scenario, which statement is correct?

**A)** IPv4 has an address space of 32-bits, which is enough for the future.
**B)** IPv4 with NAT (Network Address Translation) functionality has enough public IP for the future.
**C)** IPv6 addresses will be enough just working with IPv4 addresses.
**D)** IPv6 has an address space of 128 bits, which is enough for the future.

**A)** Incorrect. IPv4 has more than 4 billion addresses, but this not enough for the future
**B)** Incorrect. IPv4 has more than 4 billion addresses, but this not enough for the future, even with the use of NAT.
**C)** Incorrect. IPv6 is enough, it's not necessary to use IPv4 addresses.
**D)** Correct. IPv6 has more than 6 * 1023 addresses, which will be enough for the next decades. *Fundamentals of Information Systems Security, Chapter 10: IP Addressing*

**3 / 40**
Which IP version **best** anticipates on the exhaustion of public IP addresses in the near future?

**A)** FTP
**B)** HTTP
**C)** S/MIME
**D)** SMTP

**A)** Incorrect. FTP belongs to the Application Layer.
**B)** Incorrect. HTTP belongs to the Application Layer.
**C)** Correct. S/MIME belongs to the Presentation Layer.
**D)** Incorrect. SMTP belongs to the Application Layer.

**4 / 40**
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 ?'. 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 ?'. 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 ? Tell ’. The host with the correct IP address will answer with its hardware address. *Fundamentals of Information Systems Security, Chapter 3: IP Address Spoofing*
**D)** Incorrect. ARP is used to broadcast the question ‘who has ?'. The host with the correct IP address will answer with its hardware (MAC) address.

**5 / 40**
A security analyst needs to perform a forensic analysis on a computer, because this computer was used to steal strategic information from the corporate server which was sold to a competitor.

What is the key component that needs to be analyzed?

**A)** Hardware
**B)** Software
**C)** Firmware
**D)** CPU

**A)** Incorrect. The correct option is the software, not the hardware
**B)** Correct. He needs to analyze the operating system looking for evidence of stolen information.
**C)** Incorrect. The correct option is the software, not the firmware
**D)** Incorrect. The correct option is the software, not the CPU

**6 / 40**
Which CPU family was developed by Apple?

**A)** A5
**B)** Core i7
**C)** Power8
**D)** Sparc T5

**A)** Correct. A5 was developed by Apple.
**B)** Incorrect. Core i7 is a particular series of Intel processors.
**C)** Incorrect. Power8 was developed by IBM.
**D)** Incorrect. Sparc T5 was developed by Oracle (formerly SUN Microsystems).

**7 / 40**
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. *Fundamentals of Information Systems Security, Chapter 6: Configuration Management*

**8 / 40**
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. *Fundamentals of Information Systems Security, Chapter 7: How to Verify Security Controls*

**9 / 40**
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.
**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.

**10 / 40**
A software engineer is developing a web application, but the information security manager is worried about the security requirements for this application.

Which assumption made by the software engineer is correct?

**A)** The application server side can trust the information coming from the user.
**B)** The authentication is the only control necessary to ensure the user security.
**C)** The digital certificate ensures the security of the data exchanged between client and server.
**D)** The security misconfiguration will be addressed in the production environment.

**A)** Incorrect. The user input data is not reliable, all security controls must be done on the server side.
**B)** Incorrect. Authorization and session management are other key controls to ensure the user security.
**C)** Correct. The digital certificate (protocol HTTPS) ensures the traffic is secure.
**D)** Incorrect. Security misconfiguration should be addressed in the QA environment.

**11 / 40**
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.
**C)** Incorrect. A foreign key can also link to a primary key in other tables.
**D)** Incorrect. A record represents a relationship between columns.

**12 / 40**
After an analysis, a consultant recommends to the client the implementation of a service directory to centrally manage users and groups.

What is an example of Directory Services that the client will need to implement?

**A)** Data Definition Language (DDL)
**B)** Directory Analysis Procedure (DAP)
**C)** Meta Data Dictionary (MDD)
**D)** Windows Active Directory (AD)

**A)** Incorrect. Data Definition Language (DDL) describes a data model in a database.
**B)** Incorrect. DAP stands for Directory Access Protocol.
**C)** Incorrect. A Meta Data Dictionary does not exist, only a Data Dictionary or Meta Data in databases.
**D)** Correct. AD is an example of a directory services, based on X.500.

**13 / 40**
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.

**14 / 40**
Databases are important to the business, so access and activities must be monitored.

What is the **main** objective of Auditing monitoring?

**A)** Determine and guard the amount of storage needed for log data
**B)** Monitor actions performed by whom, at what time, on which object
**C)** Prevent security incidents by providing logging and audit tables
**D)** Verify the legally prescribed retention and archiving of log data

**A)** Incorrect. Determining the minimal or maximum amount of log data remains a challenge.
**B)** Correct. Auditing monitoring can follow up on security incidents that have occurred. *Fundamentals of Information Systems Security, Chapter 5: Policies and Procedures for Accountability*
**C)** Incorrect. Auditing monitoring is a reactive measure and cannot prevent security incidents.
**D)** Incorrect. Auditing monitoring can only verify conformation to legal terms.

**15 / 40**
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 private 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.
**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.
**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.
**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. *Fundamentals of Information Systems Security, Chapter 9: Digital Signatures and Hash Functions*

**16 / 40**
Referring to the well-known substitution ciphers, such as Caesar's Cipher, what is the result of the word "SECURITY" encrypted through the following schema?

SCHEMA:
A = 1, B = R, C = @, D = /, E = T, I = (, R = !, S = 5, T = -, U = &, Y = X

**A)** 5T@&!(-X
**B)** 5T@-!(-@
**C)** ST@&!@-X
**D)** 5E@&!(@X

**A)** Correct. Involve the simple process of substituting one character for another, based upon a crypto variable. *Fundamentals of Information Systems Security, Chapter 9: Types of Ciphers*
**B)** Incorrect. Because U = & and Y = X.
**C)** Incorrect. Because I = ( and S = 5.
**D)** Incorrect. Because E = T and T = -.

**17 / 40**
A network administrator sent a message signed with his private key.

Which of the following is correct?

**A)** The origin of this message can be ensured because it was signed with the private key of the sender.
**B)** The origin of this message can be ensured if he uses the algorithm AES before sending this message.
**C)** The origin of this message can be ensured if he uses the algorithm SHA-2 before sending this message.
**D)** The origin of this message cannot be ensured because it was signed with a private key only.

**A)** Correct. We can ensure that the message is reliable because it was signed with a private key, which ensures non-repudiation. *Fundamentals of Information Systems Security, Chapter 9: Digital Signatures and Hash Functions*
**B)** Incorrect. It's not necessary to use a symmetric encryption to ensure non-repudiation.
**C)** Incorrect. It's not necessary to use other hash functions because the message integrity is guaranteed by the private key.
**D)** Incorrect. The message was signed with a private key, which ensures non-repudiation.

**18 / 40**
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, hashing is also 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. *Fundamentals of Information Systems Security, Chapter 9: Symmetric and Asymmetric Key Cryptography and Digital Signatures and Hash Functions*

**19 / 40**
The Public Key Infrastructure (PKI) consists of hardware, software, protocols, procedures, policies and standards to manage the creation, the administration, the distribution and the revocation of the digital certificates and keys.

What is the purpose of a Certificate Revocation List (CRL)?

**A)** CRL presents certificates with an expired validity date only.
**B)** Irreversibly or temporary revoke certificates that are no longer valid or have key compromised.
**C)** Irreversibly revoke certificates that are no longer valid.
**D)** Temporary revoke certificates that are no longer valid.

**A)** Incorrect. The CRL presents all the certificates that are no longer valid, based on incidents with the certificate or an expired validity date.
**B)** Correct. The CRL is responsible for revoking certificates that are no longer valid, irreversibly if a private key has been compromised or the validity date is expired and temporary if a user is unsure if the private key was lost or compromised. *Fundamentals of Information Systems Security, Chapter 9: Cryptographic Applications and Uses in Information System Security*
**C)** Incorrect. The CRL is responsible to revoke certificates that are no longer valid, irreversibly or temporary.
**D)** Incorrect. The CRL is responsible to revoke certificates that are no longer valid, irreversibly or temporary.

**20 / 40**
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. *Fundamentals of Information Systems Security, Chapter 9: Cryptographic Applications and Uses in Information System Security*
**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.

**21 / 40**
A secure channel has been established between two hosts using TLS (Transport Layer Security) version 1.2.

Regarding this TLS, which of the following statements is correct?

**A)** TLS is based on asymmetric key cryptography and operates only on the OSI Transport layer.
**B)** TLS provides data encryption and authentication, and is based on asymmetric key cryptography.
**C)** TLS provides data encryption and authentication, and is based on symmetric key cryptography.
**D)** TLS provides data encryption, is based on symmetric key cryptography and operates only on the transport layer.

**A)** Incorrect. TLS operates on the OSI Transport, Session, Presentation and Application layer.
**B)** Correct. TLS is a protocol that protects the communication, such as HTTPS, SMTP and other, and is based on an asymmetric key. *Fundamentals of Information Systems Security, Chapter 10: The OSI Reference Model*
**C)** Incorrect. TLS is based on asymmetric key cryptography.
**D)** Incorrect. TLS is based on an asymmetric key and operates on the OSI Transport, Session, Presentation and Application layer.

**22 / 40**
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. *Fundamentals of Information Systems Security, Chapter 9: Principles of Certificates and Key Management*

**23 / 40**
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. *Fundamentals of Information Systems Security, Chapter Centralized and Decentralized Access Control*

**24 / 40**
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. *Fundamentals of Information Systems Security, Chapter 5: Processes and Requirements for Authentication*
**B)** Incorrect. That a biometric method like swipe 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.

**25 / 40**
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. *Fundamentals of Information Systems Security, Chapter 5: Processes and Requirements for Authentication*
**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.

**26 / 40**
What is an attacker able to do when a single salt value is used for all passwords in a database?

**A)** Add the salt again and get the plaintext values.
**B)** Remove the first characters of the hash to bypass the salts.
**C)** Remove the salt and decrypt the passwords.
**D)** Use the same salt and create a database of passwords and their hash values.

**A)** Incorrect. The salt and plaintext password are combined and hashed. Adding the salt again gives nonsense data that cannot be used. The problem is that an attacker can generate a database with passwords and their salted hash values (a so called rainbow table) and look up every hash value from the password database in the rainbow table. With randomized salts, the attacker would have to attack each hash value separately.
**B)** Incorrect. Removing the first characters of the hash turns the hash into nonsense. The problem is that an attacker can generate a database with passwords and their salted hash values (a so called rainbow table) and look up every hash value from the password database in the rainbow table. With randomized salts, the attacker would have to attack each hash value separately.
**C)** Incorrect. Once the salt is hashed it can't be removed. The problem is that an attacker can generate a database with passwords and their salted hash values (a so called rainbow table) and look up every hash value from the password database in the rainbow table. With randomized salts, the attacker would have to attack each hash value separately.
**D)** Correct. An attacker can generate a database with passwords and their salted hash-values (a so called rainbow table) and look up every hash-value from the password database in the rainbow table. With randomized salts, the attacker would have to attack each hash-value separately.

**27 / 40**
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 the necessary information only.
**D)** Incorrect. 'Need to know' means that users should have access to only the information that is needed to perform their tasks.

**28 / 40**
How many parties (minimum) have a role in an OpenID Connect authentication data flow?

**A)** 2
**B)** 3
**C)** 4
**D)** 5

**A)** Incorrect. There's at least the user (web browser), the website to logon to, and the OpenID provider - 3.
**B)** Correct. There's at least the user (web browser), the website to logon to, and the OpenID provider - 3.
**C)** Incorrect. There's at least the user (web browser), the website to logon to, and the OpenID provider - 3.
**D)** Incorrect. There's at least the user (web browser), the website to logon to, and the OpenID provider - 3.

**29 / 40**
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. *Fundamentals of Information Systems Security, Chapter 5: Centralized and Decentralized Access Controls*
**D)** Incorrect. In a public cloud resources are shared with other parties.

**30 / 40**
What is true about the public cloud?

**A)** Parts are used by a single organization and parts are used by a group of organizations.
**B)** It is used by a single organization.
**C)** It is used by a small group of organizations with shared concerns.
**D)** It is used by any organization that wants to use it.

**A)** Incorrect. This is a hybrid cloud.
**B)** Incorrect. This is a private cloud.
**C)** Incorrect. This is a community cloud.
**D)** Correct. This is a public cloud. *Fundamentals of Information Systems Security, Chapter 5: Centralized and Decentralized Access Controls*

**31 / 40**
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, with which the organization has a relationship.
**D)** Incorrect. IDaaS provides services for both internal and external users.

**32 / 40**
An organization wants to host a web service, but does not want to deal with buying and maintaining hardware or keeping the operating system up-to-date.

What type of service model should they ask for?

**A)** IaaS
**B)** PaaS
**C)** SaaS
**D)** SECaaS

**A)** Incorrect. Infrastructure as a Service would require the organization to maintain the operating system.
**B)** Correct. Platform as a Service gives a platform where the organization only has to manage their web service.
**C)** Incorrect. Software as a Service would not allow the organization to create their own web service.
**D)** Incorrect. SECurity as a Service would not allow the organization to host any web service.

**33 / 40**
There is always a risk when a cloud provider who provides a solution such as SaaS or PaaS goes out of business.

What is this risk for the company who uses this cloud solution?

**A)** Continuity risk
**B)** Jurisdiction risk
**C)** Legal risk
**D)** Storage risk

**A)** Correct. When the company goes out of business all information is lost (data stored in the cloud, etc).
**B)** Incorrect. Where is the data stored? Is it stored in the country (region) where the company is located or not? This information should be provided by the service provider.
**C)** Incorrect. This can be read in the EULA.
**D)** Incorrect. This is a risk for the provider not the company that uses the cloud.

**34 / 40**
Why would a CEO of a company want to move the key corporate systems to the cloud?

**A)** To decrease the technology cost
**B)** To decrease the leak of sensitive information
**C)** To decrease security vulnerabilities
**D)** To decrease unauthorized access to customer information

**A)** Correct. Moving to the Cloud will decrease the cost of the technology. *Fundamentals of Information Systems Security, Chapter 5: Centralized and Decentralized Access Controls*
**B)** Incorrect. A leak of sensitive information is a risk when moving to the cloud.
**C)** Incorrect. Uncontrolled security vulnerabilities is a risk when moving to the cloud.
**D)** Incorrect. Unauthorized access to customer information is a risk when moving to the cloud.

**35 / 40**
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. *Fundamentals of Information Systems Security, Chapter 11: The Main Types of Malware*
**D)** Incorrect. Spam is a commercial message sent at a large group of recipients.

**36 / 40**
There are four main attack categories when it comes to exploiting vulnerabilities.

What is **not** one of the four main attack categories?

**A)** Full penetration
**B)** Information theft or disclosure
**C)** Insider misuse

**A)** Incorrect. This is one of the main attack categories.
**B)** Incorrect. This is one of the main attack categories.
**C)** Correct. This is a source of attack but not one of the main attack categories. The missing category is Denial of Service.

**37 / 40**
A certain type of attacker knows how to write exploits, uses social engineering to gain information about their target and collects data. The motives of the attacker are unclear and the attacker is not always malicious.

What type of attacker is this?

**A)** Black Hat Hacker
**B)** Gray Hat Hacker
**C)** Hacktivist
**D)** White Hat Hacker

**A)** Incorrect. The black hat hacker wants to gain something out of the hack: money, status, etc.
**B)** Correct. The gray hat hacker is not always malicious and the motivation is sometimes unclear. Sometimes the gray hat hacker just hacks for the fun of it and sometimes he wants to show a company that there are leaks in their systems. Still the gray hat is not hired (or ethical) like the white hat hacker. *EXIN Ethical Hacking Foundation*
**C)** Incorrect. The hacktivist attacks systems from a political kind of view.
**D)** Incorrect. Motivation of the white hat hacker are always clear.

**38 / 40**
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. *EXIN Ethical Hacking Foundation*
**B)** Incorrect. John the Ripper is a tool to brutally force passwords.
**C)** Incorrect. Metasploit is a hacking toolkit.
**D)** Incorrect. Ophcrack is a tool to brutally force Windows passwords.

**39 / 40**
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. *EXIN Ethical Hacking Foundation*
**C)** Incorrect. Erasing tracks is essential to hide system breaches.
**D)** Incorrect. Erasing tracks is essential to hide system breaches.

**40 / 40**
A hacker gained access to a web server, using a carefully thought-out step-by-step plan.

Which step did he take immediately after “Penetration and access”?

**A)** Fingerprinting
**B)** Privilege escalation
**C)** Reconnaissance
**D)** Vulnerability assessment

**A)** Incorrect. Identifying the operating system and detecting specific versions of applications or protocols is done before entering the system of application.
**B)** Correct. After entering the system or application, he gains administrative access. *EXIN Ethical Hacking Foundation*
**C)** Incorrect. This is the first step: gathering preliminary information.
**D)** Incorrect. Identifying and exploiting any vulnerabilities is done before entering the system of application.

# Evaluation

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

| Question | Answer | Question | Answer |
|---|---|---|---|
| **1** | B | **21** | B |
| **2** | D | **22** | D |
| **3** | C | **23** | D |
| **4** | C | **24** | A |
| **5** | B | **25** | A |
| **6** | A | **26** | D |
| **7** | C | **27** | C |
| **8** | D | **28** | B |
| **9** | A | **29** | C |
| **10** | C | **30** | D |
| **11** | B | **31** | C |
| **12** | D | **32** | B |
| **13** | D | **33** | A |
| **14** | B | **34** | A |
| **15** | D | **35** | C |
| **16** | A | **36** | C |
| **17** | A | **37** | B |
| **18** | D | **38** | A |
| **19** | B | **39** | B |
| **20** | B | **40** | B |

Driving Professional Growth

## Contact EXIN

www.exin.com