# Free Questions for FC0-U61 by dumpssheet

## Shared by Weeks on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Given the following information:

Table A

| ID | Name |
|---|---|
| 01 | John |
| 02 | Ann |

Table B

| ID | Address | Phone number |
|---|---|---|
| 01 | 5555 John Lane | 555-555-1234 |
| 02 | 7777 Ann Boulevard | 777-777-4321 |

Which of the following is descriptive of both tables?

## Options:

**A-** The database uses a flat file structure.

**B-** The database uses SQL.

**C-** The data most likely exists within a relational database.

**D-** The data is corrupted and is being shown as two sets.

### Answer:

C

### Explanation:

The description that best fits both tables is that the data most likely exists within a relational database. A relational database is a type of database that organizes data into tables, which consist of rows and columns. Each table represents an entity, such as customers, orders, products, etc., and each row represents an instance of that entity, such as customer 01, order 02, product 03, etc. Each column represents an attribute of that entity, such as name, address, phone number, etc. Tables can be related to each other by using common columns, such as ID, which can act as primary keys or foreign keys. A primary key is a column that uniquely identifies each row in a table, such as ID in Table A and Table B. A foreign key is a column that references the primary key of another table, such as ID in Table B referencing ID in Table A. A relational database uses SQL (Structured Query Language) to create, manipulate, and query data in tables. The database does not use a flat file structure, which is another type of database that stores data in plain text files with fixed fields and records. A flat file structure does not support relationships between tables or SQL queries. The data is not corrupted and shown as two sets, but rather separated into two tables for normalization purposes.Normalization is the process of organizing data in tables to reduce redundancy and improve efficiency and integrity.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 6: Database Fundamentals1

## Question 2

**Question Type:** MultipleChoice

A systems administrator is setting up an output device that supports both USB and network capability. Which of the following devices is the administrator most likely installing?

## Options:

**A-** Scanner

**B-** Camera

**C-** SSD

**D-** Printer

## Answer:

D

## Explanation:

The device that the administrator is most likely installing is a printer. A printer is an output device that supports both USB and network capability, meaning that it can be connected to a computer or a network using either a USB cable or a wireless or wired network connection. A printer can produce hard copies of documents, images, or other data on paper or other media. A scanner is an input device that supports both USB and network capability, meaning that it can be connected to a computer or a network using either a USB cable or a wireless or wired network connection. A scanner can capture images or text from paper or other media and convert them into digital data. A camera is an input device that supports both USB and network capability, meaning that it can be connected to a computer

or a network using either a USB cable or a wireless or wired network connection. A camera can capture images or videos and store them as digital data. An SSD stands for Solid State Drive, which is a type of storage device that supports both USB and network capability, meaning that it can be connected to a computer or a network using either a USB cable or a wireless or wired network connection.An SSD uses flash memory chips to store data persistently even when the power is turned off.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 1: IT Fundamentals1

# Question 3

**Question Type:** MultipleChoice

Given the following lines:

```
If child 1 is fed AND child 2 is fed,
  echo "dinner is complete!" and set spouse to satisfied.
else
  echo "please feed the kids!"
```

This is an example of:

## Options:

**A-** a flowchart.

**B-** looping.

**C-** an assembly.

**D-** pseudocode.

## Answer:

D

## Explanation:

The example given is an example of pseudocode. Pseudocode is a way of writing the logic of a program or an algorithm in a simplified and informal language that resembles natural language or code, but does not follow the syntax or rules of a specific programming language. Pseudocode is often used to plan, design, or explain a program or an algorithm before writing the actual code. A flowchart is a way of representing the logic of a program or an algorithm using symbols and arrows that show the sequence of steps and decisions. A flowchart is often used to visualize, analyze, or document a program or an algorithm. Looping is a way of repeating a set of statements or actions in a program or an algorithm until a certain condition is met. Looping is often used to perform iterative tasks, such as counting, searching, or sorting. An assembly is a way of writing the instructions of a program or an algorithm in a low-level language that corresponds to the machine code of a specific processor.An assembly is often used to create programs that run fast and efficiently, but it is difficult to read and write.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 8: Software Development Concepts1

# Question 4

**Question Type:** MultipleChoice

Given this example:

FEB8077911AB12TB

Which of the following is being represented?

## Options:

**A-** MAC address

**B-** String

**C-** Hexadecimal

**D-** Unicode

## Answer:

C

## Explanation:

The example FEB8077911AB12TB is being represented as hexadecimal. Hexadecimal is a number system that uses 16 symbols to represent values from 0 to 15. The symbols are 0-9 for values from 0 to 9, and A-F for values from 10 to 15. Hexadecimal is often used to represent binary data in a more compact and readable form, such as MAC addresses, color codes, or memory addresses. A MAC address is a unique identifier for a network interface card (NIC) that consists of 12 hexadecimal digits separated by colons or dashes. A string is a sequence of characters that can be used to store text or other data types. A string can contain hexadecimal digits, but it can also contain other symbols or characters. Unicode is a standard for encoding characters from different languages and scripts into binary data.Unicode can use hexadecimal digits to represent characters, but it also requires other symbols or codes to indicate the encoding scheme.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 2: IT Concepts and Terminology1

# Question 5

**Question Type:** MultipleChoice

A corporate network just implemented a 60-day password-warning banner. Which of the following is most likely going to happen in 60 days?

## Options:

**A-** Password reset

**B-** Password expiration

**C-** Password reuse

**D-** Password Implementation

## Answer:

B

## Explanation:

The most likely thing that will happen in 60 days after implementing a 60-day password-warning banner is password expiration. A password-warning banner is a message that appears on the screen when a user logs in to a system or network, informing them of how many days are left before their password expires. A password expiration policy is a security measure that requires users to change their passwords periodically, usually every 30 to 90 days. This policy helps to prevent unauthorized access or compromise of passwords by hackers or malicious insiders. Password reset is the process of changing or creating a new password for a user account when the user forgets their password or wants to change it for security reasons. Password reset can be done by the user themselves or by an administrator, depending on the system or network settings. Password reset does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless the user forgets their password or chooses to change it before it expires. Password reuse is the practice of using the same password for multiple user accounts or systems. Password reuse is not recommended as it increases the risk of compromise if one of the accounts or systems is breached by hackers or malicious insiders. Password reuse does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless the user chooses to use their old password for their new password after it expires. Password implementation is not a term used in security, but it may refer to the process of creating or enforcing password policies for user accounts or systems.Password implementation does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless there are changes in the password policies that require users to comply with

them.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts1

# Question 6

**Question Type:** MultipleChoice

The process of determining the source of an issue during troubleshooting is called:

## Options:

**A-** researching.

**B-** sourcing.

**C-** diagnosing.

**D-** triaging.

## Answer:

C

### Explanation:

The process of determining the source of an issue during troubleshooting is called diagnosing. Diagnosing is the third step in the troubleshooting process, after gathering information and determining if anything has changed. Diagnosing involves analyzing the symptoms and possible causes of the problem, testing hypotheses, and identifying the root cause of the problem. Researching is the process of finding relevant information or resources to help solve a problem during troubleshooting. Researching can be done before or after diagnosing, depending on the availability and reliability of the information or resources. Sourcing is not a term used in troubleshooting, but it may refer to the process of finding or obtaining materials or components for a product or service.Triaging is not a term used in troubleshooting, but it may refer to the process of prioritizing problems or tasks based on their urgency or importance.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 2: IT Concepts and Terminology1

## Question 7

**Question Type:** MultipleChoice

A technician travels to a data center to review specifications on a new project. Which of the following is the technician most likely to see pertaining to types of operating systems?

### Options:

**A-** Mobile device OS

**B-** Workstation OS

**C-** Embedded OS

**D-** Hypervisor OS

## Answer:

D

## Explanation:

A hypervisor OS is the most likely type of operating system that a technician would see pertaining to a data center. A hypervisor OS is an operating system that runs on a host machine and allows multiple guest operating systems to run on virtual machines. A hypervisor OS enables efficient utilization of hardware resources, scalability, and isolation of different workloads in a data center. Examples of hypervisor OS include VMware ESXi, Microsoft Hyper-V, and Citrix XenServer. A mobile device OS is an operating system that runs on a smartphone, tablet, or other portable device. A mobile device OS provides features such as touch screen, wireless connectivity, camera, GPS, and app store. Examples of mobile device OS include Android, iOS, and Windows Phone. A workstation OS is an operating system that runs on a desktop or laptop computer. A workstation OS provides features such as graphical user interface, file management, multitasking, and networking. Examples of workstation OS include Windows 10, macOS, and Linux. An embedded OS is an operating system that runs on a special-purpose device or system that performs a specific function. An embedded OS provides features such as real-time performance, low power consumption, and minimal user interface.Examples of embedded OS include Windows Embedded, Linux Embedded, and QNX.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 4: Operating System Fundamentals1

# Question 8

**Question Type:** MultipleChoice

An attacker is using subversive tactics to gain the trust of a target in order to obtain entry to a location or access to confidential information. Which of the following best describes this scenario?

## Options:

**A-** Phishing attack

**B-** Social engineering

**C-** On-path attack

**D-** Eavesdropping

## Answer:

B

## Explanation:

The scenario where an attacker is using subversive tactics to gain the trust of a target in order to obtain entry to a location or access to confidential information is best described as social engineering. Social engineering is a type of attack that exploits human psychology and behavior to manipulate people into performing actions or revealing information that benefits the attacker. Social engineering can take various forms, such as phishing, vishing, baiting, quid pro quo, pretexting, or tailgating. Phishing attack is a type of social engineering attack that involves sending fraudulent emails or messages that appear to come from legitimate sources to trick recipients into clicking on malicious links or attachments, or providing personal or financial information. On-path attack is a type of network attack that involves intercepting or modifying data packets that are transmitted between two parties on a network.Eavesdropping is a type of network attack that involves listening to or capturing data packets that are transmitted between two parties on a network.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts1

# Question 9

**Question Type:** MultipleChoice

Which of the following is most likely to disclose the data collection practices of an application?

### Options:

**A-** README.txt file

**B-** User's guide

**C-** EULA

**D-** Vendor website

## Answer:

C

## Explanation:

The most likely source that will disclose the data collection practices of an application is the EULA. EULA stands for End User License Agreement, which is a legal contract between the software vendor and the user that defines the terms and conditions for using the software. The EULA often includes information about how the software collects, uses, stores, and shares user data, as well as what rights and responsibilities the user has regarding their data. A README.txt file is a text file that accompanies a software package and provides information about how to install, configure, or use the software. A README.txt file may not disclose the data collection practices of an application, unless it is explicitly stated by the vendor. A user's guide is a document that provides instructions and tips on how to use a software application effectively. A user's guide may not disclose the data collection practices of an application, unless it is explicitly stated by the vendor. A vendor website is a web page that provides information about a software vendor and their products or services.A vendor website may disclose the data collection practices of an application, but it may not be as detailed or accessible as the EULA.References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 8: Software Development Concepts1