Eccouncil 312-49 Mock Exam

Shared by Deleon on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What does the part of the log, ''% SEC-6-IPACCESSLOGP'', extracted from a Cisco router represent?

Options:

A- The system was not able to process the packet because there was not enough room for all of the desired IP header options
B- Immediate action required messages
C- Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available
D- A packet matching the log criteria for the given access list has been detected (TCP or UDP)

Answer:

D

Question 2

Question Type: MultipleChoice

An Expert witness give an opinion if:

Options:

A- The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
B- To define the issues of the case for determination by the finder of fact
C- To stimulate discussion between the consulting expert and the expert witness
D- To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case

Answer:

A

Question 3

Question Type: MultipleChoice

Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

Options:

A- Sector
B- Metadata
C- MFT
D- Slack Space

Answer:

D

Question 4

Question Type: MultipleChoice

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

Options:

A- mysqldump
B- myisamaccess
C- myisamlog
D- myisamchk

Answer:

C

Question 5

Question Type: MultipleChoice

A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be Identified as_____.

Options:

A- Swap space
B- Cluster space
C- Slack space
D- Sector space

Answer:

C

Question 6

Question Type: MultipleChoice

What layer of the OSI model do TCP and UDP utilize?

Options:

A- Data Link
B- Network
C- Transport
D- Session

Answer:

C

Question 7

Question Type: MultipleChoice

Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox

environment.

What type of malware analysis is Edgar performing?

Options:

A- Malware disassembly
B- VirusTotal analysis
C- Static analysis
D- Dynamic malware analysis/behavioral analysis

Answer:

D