ExamCertify
Prep Materials and Exams

Eccouncil

112-57

EC-Council Threat Intelligence Essentials (TIE)

v6.0

DEMO QUESTIONS

Sample Q&A Preview

Preview content before purchase

Get Full Version & Premium Features

https://examcertify.co.uk/exam/112-57

Premium Benefits Included

- **Free Updates**
  90 days of exam updates
- **Money Back**
  30-day guarantee policy
- **Instant Access**
  Download immediately
- **24/7 Support**
  Expert assistance anytime

Question 1. (Single Select)

Wesley, a professional hacker, deleted a confidential file in a compromised system using the “/bin/rm/” command to deny access to forensic specialists.

Identify the operating system on which Don has performed the file carving act.

A: Windows
B: Android
C: Mac OS
D: Linux

Answer: D

Explanation:
The command path /bin/rm is a hallmark of UNIX/POSIX-style operating systems, where core userland utilities are commonly stored under directories such as /bin, /sbin, and /usr/bin. The utility rm (remove) is the standard UNIX command used to delete directory entries that reference a file’s data blocks on disk. This layout and command structure do not match Windows, which uses different filesystem conventions (drive letters, backslashes, and Windows-native executables) and does not provide /bin/rm as a native path. Android, while Linux-kernel-based, typically exposes shell utilities through environments like /system/bin (and newer systems may use toybox/busybox variants), not the classic /bin hierarchy expected on general-purpose UNIX systems. Between the remaining options, both Linux and macOS are UNIX-like and can include an rm command; however, in digital forensics training and examination contexts, the explicit reference to /bin/rm is most commonly used to indicate a Linux/UNIX command-line environment on a compromised host. Therefore, the best single-choice answer from the provided options is Linux (D).

Question 2. (Single Select)

Benoy, a security professional at an organization, extracted Apache access log entries to view critical information about all the operations performed on a web server. The Apache access log extracted by Benoy is given below:

“10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458”

Identify the HTTP status code in the Apache access log entry above that indicates the response was successful.

A: +0300
B: 500
C: 1.0
D: 2019

Answer: B

Explanation:
In the Apache Combined/Custom access log format, the value immediately after the quoted request (here, "GET ... HTTP/1.0") is the HTTP status code returned by the server. In the provided entry, that field is 500. From a forensic analysis standpoint, recognizing field positions matters because investigators correlate client IPs, timestamps, requested resources, and server outcomes to reconstruct attack timelines and identify failed exploitation attempts or misconfigurations.
It is important to note that successful HTTP responses are typically in the 2xx range, most commonly 200 (OK), while 3xx indicates redirects, 4xx indicates client-side errors (such as 404 Not Found), and 5xx indicates server-side failures. Specifically, 500 represents an Internal Server Error, meaning the server encountered an unexpected condition and could not fulfill the request successfully.
The other options are not HTTP status codes in this entry: +0300 is the timezone offset in the timestamp, 1.0 is the HTTP protocol version, and 2019 is part of the date. Therefore, the only HTTP status code present—and the correct choice among the options—is 500 (B), even though it reflects an error rather than success.

Question 3. (Single Select)

Andrew, a system administrator, is performing a UEFI boot process. The current phase of the UEFI boot process consists of the initialization code that the system executes after powering on the EFI system. This phase also manages platform reset events and sets up the system so that it can find, validate, install, and run the PEI.

Which of the following UEFI boot phases is the process currently in?

A: Driver execution environment phase
B: Boot device selection phase

C: Pre-EFI initialization phase

D: Security phase

Answer: D

Explanation:

In the UEFI/PI boot architecture, the phase that runs immediately after power-on or reset is the SEC (Security) phase. Digital forensics references include UEFI phases because firmware-level activity can affect the trustworthiness of the platform (e.g., bootkits, persistence, and measured boot artifacts). The SEC phase is responsible for executing the earliest initialization instructions, handling platform reset events, and establishing a minimal, controlled execution environment. Critically, SEC prepares the system so it can locate, verify, and hand off control to the next stage—PEI (Pre-EFI Initialization)—by setting up temporary memory and foundational CPU/chipset state required for PEI modules to execute.

The wording in the question precisely matches SEC responsibilities: “initialization code executed after powering on,” “manages platform reset events,” and “sets up the system so it can find, validate, install, and run the PEI.” By contrast, PEI focuses on discovering and initializing permanent memory and producing the Hand-Off Blocks for DXE; DXE loads drivers and boot services; and BDS selects and launches the boot option. Therefore, the phase described is the Security phase (SEC), which corresponds to option D.

Question 4. (Single Select)

Below is the syntax of a command-line utility that displays active TCP connections and ports on which the computer is listening.

netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Identify the netstat parameter that displays active TCP connections and includes the process ID (PID) for each connection.

A: [-n]

B: [-a]

C: [-o]

D: [-s]

Answer: C

Explanation:

In Windows forensics and incident response, investigators often need to link network activity (remote IPs, ports, connection states) to the responsible process to determine whether traffic is legitimate or associated with malware, unauthorized tools, or data exfiltration. The Windows netstat utility can enumerate current TCP connections and listening ports, but the key flag that enables attribution to a running program is -o. The -o parameter instructs netstat to include the Owning Process ID (PID) with each connection or listening socket. Once the PID is known, examiners can correlate it with process listings (e.g., Task Manager, tasklist, memory forensics output) to identify the executable name, path, user context, and parent process—critical steps in reconstructing attacker behavior and persistence.

The other options do not provide PID mapping: -n shows addresses and ports in numeric form (useful for speed and to avoid DNS lookups), -a displays all connections and listening ports but without PID attribution by itself, and -s shows protocol statistics rather than per-connection ownership. Therefore, the parameter that shows active connections and includes the PID for each is [-o] (Option C).

Question 5. (Single Select)

Jack, a forensic investigator, was appointed to investigate a Windows-based security incident. In this process, he employed an Autopsy tool to recover the deleted files from unallocated space, which helps in gathering potential evidence.

Which of the following functions of Autopsy helped Jack recover the deleted files?

A: Timeline analysis

B: Multimedia

C: Web artifacts

D: Data carving

Answer: D

Explanation:

When a file is deleted on common file systems, the operating system typically removes the directory reference and marks the previously used clusters/blocks as unallocated, but the underlying file content may remain on disk until it is overwritten. Digital forensics procedures emphasize that recovering such deleted content often requires examining unallocated space rather than relying only on file system metadata. Autopsy's "Data Carving" function is specifically intended for this purpose: it scans unallocated space (and

sometimes slack space) for file signatures (headers/footers and internal structure patterns) and reconstructs recoverable files even when the original filename, path, or metadata is missing.
This directly matches the scenario: Jack recovered deleted files from unallocated space, which is the classic use case for carving. The other options in Autopsy support different investigative goals. Timeline analysis correlates timestamps from multiple artifacts to reconstruct sequences of activity, but it does not itself reconstruct deleted file content from raw disk areas. Web artifacts focuses on browser history, downloads, cookies, and related traces. Multimedia helps categorize and analyze media files (e.g., images/videos), but it is not the primary mechanism for recovering deleted data from unallocated space.
Therefore, the Autopsy function that enabled the recovery described is Data carving (D)

Ready for Success?

Get the complete exam package today

https://examcertify.co.uk/exam/112-57

Thank You for Choosing ExamCertify!

Your Success is Our Mission

Special Discount Code

15OFFTODAY

Contact Us

Sales: sales@examcertify.co.uk
Support: support@examcertify.co.uk