PassQueen
a.k.a dumpsqueen.com

# Logical Operations CyberSec First Responder

## Logical Operations CFR-210

**Version Demo**

**Total Demo Questions: 13**

**Total Premium Questions: 133**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Threat and Vulnerability Management | 40 |
| Topic 2, Cyber Incident Response | 66 |
| Topic 3, Security Architecture and Tool Sets | 27 |
| Total | 133 |

QUESTION NO: 1

An attack was performed on a company's web server, disabling the company's website. The incident response team's investigation produced the following:

1. Presence of malicious code installed on employees' workstations.

2. Excessive UDP datagrams sent to a single address.

3. Web server received excessive UDP datagrams from multiple internal hosts.

4. Network experienced high traffic after 3:00 pm.

5. Employee workstations sent large traffic bursts when employees accessed the internal timecard application.

Which of the following BEST describes the attack tool used to perform the attack?

**A.** KeyLogger

**B.** Logic bomb

**C.** Nessus

**D.** Metasploit

**ANSWER: B**

**Explanation:**

Logic bomb is correct because the evidence indicates that malicious code on multiple employee workstations executed when a specific condition occurred: employees accessed the internal timecard application. A logic bomb is code that remains dormant until a defined trigger, such as a particular time, date, user action, or application event, is met. Once triggered, its payload can perform harmful actions, including generating a coordinated UDP flood against a designated target.

Here, the simultaneous large traffic bursts from many internal systems explain why the web server received excessive UDP datagrams from multiple internal hosts and became unavailable. The observation that network traffic increased after 3:00 pm is also consistent with a time-based or event-based activation condition associated with normal timecard use. The malicious code effectively turned compromised employee systems into coordinated traffic generators, producing a denial-of-service condition against the company web server.

The Cybersecurity and Infrastructure Security Agency describes logic bombs as malicious code activated by a specific event or condition. The MITRE ATT&CK technique for event-triggered execution likewise documents adversary code that runs when a designated system or user event occurs. See CISA guidance and MITRE ATT&CK Event Triggered Execution.

**QUESTION NO: 2**

A security analyst for a financial services firm is monitoring blogs and reads about a zero-day vulnerability being exploited by a little-known group of hackers. The analyst wishes to independently validate and corroborate the blog's posting. Whichof the following sources of information will provide the MOST credible supporting threat intelligence in this situation?

**A.** Similar cybersecurity blogs

**B.** Threat intelligence sharing groups

**C.** Computer emergency response team press release

**D.** Internet searches on zero-day exploits

**ANSWER: C**

**Explanation:**

**Computer emergency response team press release** is the most credible supporting source because an established CERT or CSIRT validates reported security events through technical investigation, coordinated vulnerability disclosure, and communication with affected vendors or organizations. A formal press release from such an organization is a primary, authoritative source that can corroborate whether a zero-day is actively being exploited, identify affected products or versions, and provide trusted indicators, mitigations, or response guidance. For a financial-services analyst, using independently verified intelligence is especially important because decisions based on a reported zero-day may lead to urgent actions such as applying emergency mitigations, increasing monitoring, or initiating incident-response procedures. CERT publications are intended to distribute vetted, actionable cybersecurity information to defenders and generally distinguish confirmed facts from preliminary details. This makes an official CERT communication substantially suitable for validating a claim initially encountered in an unverified blog post. The U.S. Cybersecurity and Infrastructure Security Agency describes its role in publishing alerts and advisories for significant cyber threats, while CERT/CC coordinates vulnerability disclosure and provides vulnerability information to organizations and the public. See CISA Cybersecurity Advisories and CERT/CC Vulnerability Notes Database.

## QUESTION NO: 3

Which of the following are legally compliant forensics applications that will detect ADS or a file with an incorrect file extension? (Choose two.)

**A.** Regedit

**B.** EnCase

**C.** dd

**D.** FTK

**E.** Procmon

## ANSWER: B D

**Explanation:**

**EnCase** and **FTK** are purpose-built digital-forensics applications designed to support defensible evidence collection, examination, analysis, and reporting. Both can examine NTFS file-system metadata and enumerate alternate data streams (ADS), which may be used to conceal content outside a file's primary data stream. They also compare a file's apparent extension with its underlying file type or signature, helping an examiner identify files whose names or extensions have been altered to disguise their true content.

These capabilities are important to a legally defensible examination because the tools preserve and present relevant artifact information in a repeatable manner and support documentation of findings for incident-response, investigative, and legal workflows. EnCase describes its forensic platform as supporting acquisition, investigation, and reporting of digital evidence, while FTK provides indexed forensic examination and file analysis capabilities. An examiner should still follow approved evidence-handling procedures, maintain chain-of-custody records, and validate results within the organization's forensic process. See OpenText EnCase Forensic and Exterro FTK Forensic Toolkit.

## QUESTION NO: 4

A DMZ web server has been compromised. During the log review, the incident responder wants to parse all common internal Class A addresses from the log. Which of the following commands should the responder use to accomplish this?

**A.** grep –x"(10.[0-9]+.[0-9]+.[0-9]+)" etc/rc.d/apache2/access.log | output.txt

**B.** grep –x"(192.168.[0.9]+[0-9])" bin/apache2/access.log | output.txt

**C.** grep –v"(10.[0-9]+.[0-9]+.[0-9]+)" /var/log/apache2/access.log > output.txt

**D.** grep –v"(192.168.[0.9]+[0-9]+)" /var/log/apache2/access.log > output.txt

**E.** grep -Eo '10\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' /var/log/apache2/access.log > output.txt

**ANSWER: E**

**Explanation:**

`grep -Eo '10\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' /var/log/apache2/access.log > output.txt` is correct because the private IPv4 range conventionally referred to as the internal Class A range is 10.0.0.0/8. RFC 1918 reserves this entire range for private internets, so an address parser must look for IPv4 values beginning with `10.`. The `-E` switch enables extended regular expressions, allowing the bounded repetition syntax used to match each remaining decimal octet. The `-o` switch is especially appropriate during log review because it outputs only each matched address rather than the full Apache log line, producing a cleaner artifact for later triage, counting, enrichment, or comparison. Shell output redirection with `> output.txt` writes those extracted values into the specified file. In practice, an analyst may further validate octet ranges or deduplicate results, but this command correctly identifies and extracts the common internal Class A-formatted addresses from the access log. The private-address assignment is defined in RFC 1918, and GNU documents the extended-regex and only-matching-text behavior in its grep manual.

## QUESTION NO: 5

An incident responder is investigating a suspected phishing message that appears to have been sent from the company's Chief Executive Officer (CEO). Which of the following information should the responder review to determine whether the sender was spoofed? (Choose two.)

**A.** Email message headers

**B.** Email gateway logs

**C.** Browser history

**D.** DHCP logs

**E.** Printer logs

**ANSWER: A B**

**Explanation:**

**Email message headers** are a primary source for determining how a message was routed and whether the visible sender address is consistent with the sending infrastructure. Headers can contain Received fields, return-path information, sender addresses, originating IP addresses, and authentication results. These details help establish whether the message actually originated from an authorized mail server.

**Email gateway logs** are also useful because they can show the sending host, recipient, delivery time, message identifiers, filtering verdicts, and SPF, DKIM, or DMARC evaluation results. Correlating gateway records with the headers provides stronger evidence of spoofing than relying on the display name or From address alone. CISA provides guidance on phishing at Recognize and Report Phishing, and the Internet Engineering Task Force documents email authentication concepts in RFC 7489: DMARC.

## QUESTION NO: 6

A security analyst suspects that an unauthorized local account was created on a Windows server. Which of the following sources should the analyst review to validate the finding? (Choose two.)

**A.** Windows Security event log

**B.** SAM registry hive

**C.** Browser cache

**D.** Windows Prefetch folder

**E.** DHCP lease database

**ANSWER: A B**

**Explanation:**

**The Windows Security event log** is correct because account-management auditing can record security-relevant events associated with account creation, modification, deletion, group membership changes, and the account responsible for the action. For example, Event ID 4720 may record the creation of a user account when the appropriate auditing policy is enabled. The event details can help establish the time of the change and the account that performed it.

**The SAM registry hive** is also correct because the Security Account Manager database stores local account information on a Windows system. Examination of the SAM hive can help identify local accounts that exist on the host, including suspicious or unexpected accounts that may not be authorized. Correlating the account information with event logs, endpoint telemetry, and administrative records helps determine whether the account was maliciously created. See Microsoft Security Auditing Overview and MITRE ATT&CK: Create Account—Local Account.

## QUESTION NO: 7

A company website was hacked via the SQL query below:

```
email, passwd, login_id, full_name
FROM members
WHERE email = "attacker@somewhere.com" ; DROP TABLE members;--"
```

Which of the following did the hackers perform?

**A.** Cleared tracks of attacker@somewhere.com entries

**B.** Deleted the entire members table

**C.** Deleted the email, password, and login details

**D.** Performed an XSS attack

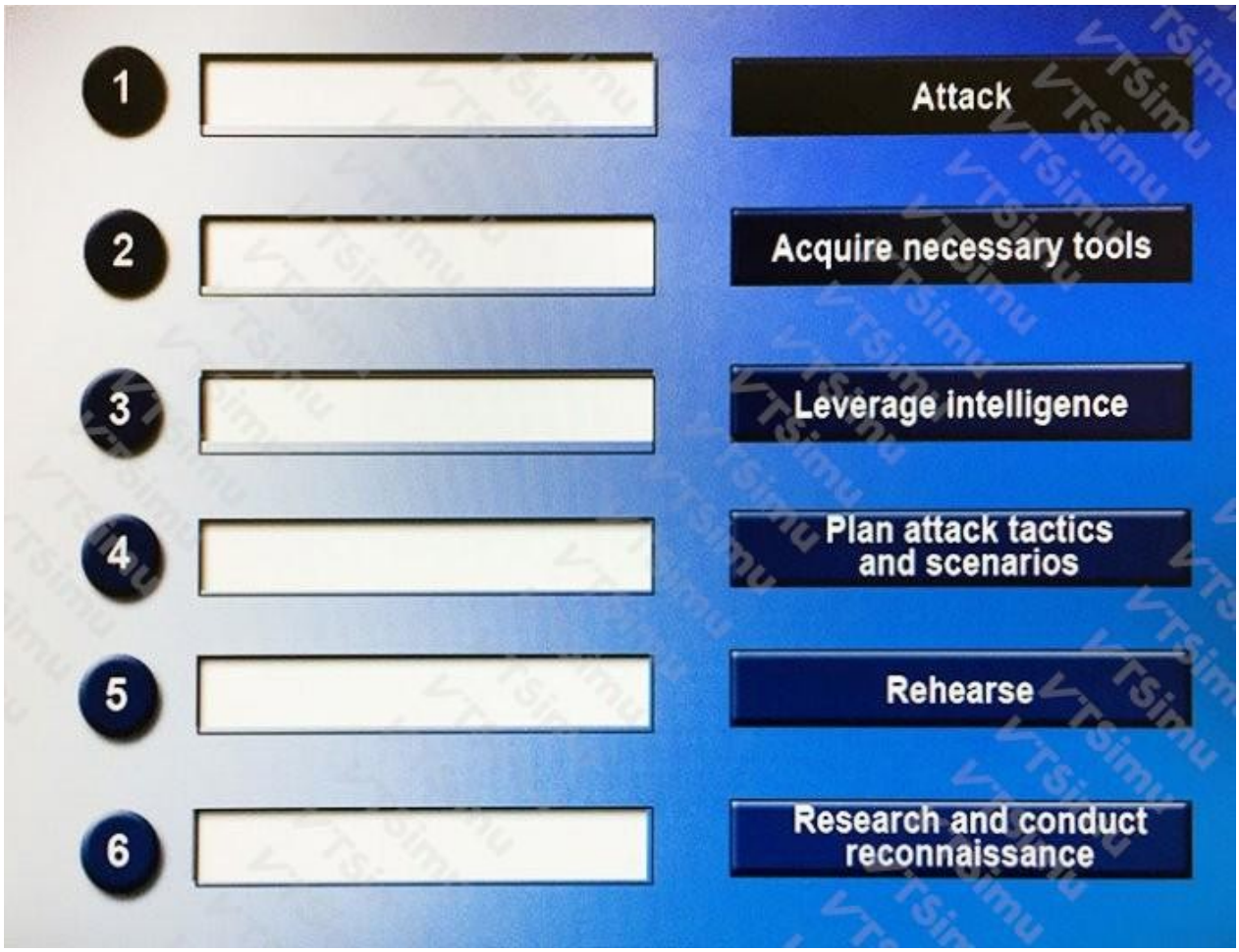
**ANSWER: A**

**Explanation:**

The hackers cleared tracks of `attacker@somewhere.com` entries. The query shown is a SQL `DELETE` operation targeted by a condition that identifies records associated with that email address. A `DELETE FROM` statement removes rows from the specified table, while a `WHERE` clause limits the deletion to rows meeting the stated criterion. In this context, deleting the records tied to the attacker's email address is consistent with an attempt to remove evidence of an account or activity after compromising the site. This is a database-manipulation action delivered through SQL injection; it is not client-side script injection. SQL injection occurs when untrusted input is incorporated into a database query so that the attacker can alter the intended query or execute unauthorized commands. Parameterized queries and appropriate database permissions are important controls because they prevent user input from being interpreted as executable SQL and limit the impact if an application flaw exists. The MySQL reference documents the behavior and syntax of the `DELETE` statement at MySQL DELETE Statement. OWASP also describes SQL injection risks and prevention practices at OWASP SQL Injection Prevention Cheat Sheet.

## QUESTION NO: 8 - (DRAG DROP)

Drag and drop the following steps to perform a successful social engineering attack in the correct order, from first (1) to last (6).


1
2
3
4
5
6
Attack
Acquire necessary tools
Leverage intelligence
Plan attack tactics and scenarios
Rehearse
Research and conduct reconnaissance

**ANSWER:**




**Explanation:**

A successful social-engineering operation follows a preparation-to-execution workflow in which each activity supplies what is needed for the next one. It starts with **Research and conduct reconnaissance**, which establishes an understanding of the target environment, people, organization, processes, and publicly or otherwise legitimately available details relevant to the engagement. The collected material is then processed in the **Leverage intelligence** stage. This means turning raw observations into actionable knowledge that can support a believable, targeted approach.

Once that intelligence is available, **Plan attack tactics and scenarios** defines the intended pretext, communication path, timing, objective, and likely interaction flow. The plan determines what resources will actually be required, so **Acquire necessary tools** follows planning. The operation can then be **Rehearsed** to validate the scenario, refine messaging and procedures, and ensure the planned activity can be carried out consistently. Finally, **Attack** is the execution stage, where the prepared and rehearsed scenario is conducted. This ordered progression reflects the broader reconnaissance, planning, preparation, and execution concepts used in social-engineering security awareness and testing methodologies. See the CISA phishing guidance for discussion of how targeted social-engineering activity relies on information about intended victims, and the MITRE ATT&CK phishing technique reference for related adversary tradecraft context.

## QUESTION NO: 9

A network administrator has been asked to configure a new network. It is the company's policy to segregate network functions using different Virtual LANs (VLANs). On which of the following is this configuration MOST likely to occur?

**A.** Network switch

**B.** Virtual Machine

**C.** Virtual Private Network

**D.** Network firewall

**ANSWER: A**

**Explanation:**

Network switch is correct because VLANs are a Layer 2 network-segmentation capability normally configured on managed switches. A switch assigns its physical access ports, and in some cases logical interfaces, to particular VLANs. Devices connected to ports in one VLAN form a separate broadcast domain from devices in another VLAN, even when they use the same switching infrastructure. This allows an organization to separate functions such as user workstations, servers, voice endpoints, management interfaces, and guest devices according to its security and operational policy.

Switch links between network devices can also carry traffic for multiple VLANs by using VLAN tagging, commonly IEEE 802.1Q. This permits VLAN separation to extend across the switched network while retaining the VLAN identity of each frame. Communication between VLANs requires intentional Layer 3 routing and can then be governed by security policy, helping enforce the required segregation. Cisco's overview of virtual LANs describes VLANs as logical network partitions implemented through switching, while the IEEE 802.1Q standard defines bridged-network VLAN operation and tagging.

## QUESTION NO: 10

An incident responder is preparing to power down a compromised server that may contain active malware. Which of the following volatile evidence should be collected before the system is shut down? (Choose two.)

**A.** A memory image

**B.** Active network connections

**C.** Archived backup tapes

**D.** Printed asset inventory reports

**E.** Network rack labels

**ANSWER: A B**

**Explanation:**

**A memory image** should be collected because RAM can contain running processes, injected code, decrypted malware content, command-line arguments, credentials, encryption keys, and network artifacts that may be lost when the system is powered off. Memory acquisition should be performed as early as practical when it can be done safely and according to the organization's incident-handling procedures.

**Active network connections** should also be collected because they can identify current remote endpoints, listening ports, connection states, and potentially the process responsible for suspicious communication. This evidence can help identify command-and-control infrastructure, lateral movement, or data-exfiltration channels. NIST discusses collection of volatile data in SP 800-86, and MITRE ATT&CK documents collection of system network connection information under System Network Connections Discovery.

## QUESTION NO: 11

A cloud security analyst receives an alert indicating that a user account authenticated from two geographically distant locations within a short period. Which of the following logs should the analyst review to investigate the activity? (Choose two.)

**A.** Identity provider sign-in logs

**B.** Cloud audit logs

**C.** Printer logs

**D.** BIOS event logs

**E.** DHCP lease logs from an unrelated office

**ANSWER: A B**

**Explanation:**

**Identity provider sign-in logs** are essential because they record authentication events, source IP addresses, device information, timestamps, geolocation details, authentication methods, and conditional-access decisions. These records help determine whether the apparent impossible-travel activity resulted from credential theft, VPN use, mobile networks, or inaccurate geolocation.

**Cloud audit logs** should also be reviewed because they show actions performed after authentication, such as mailbox-rule changes, file access, role assignments, virtual-machine modifications, or creation of access keys. Correlating sign-in activity with audit events helps determine whether the account was used to access data or change cloud resources. Microsoft documents sign-in reporting in Microsoft Entra sign-in logs and audit reporting in Audit search.

## QUESTION NO: 12

A security analyst receives an unfamiliar executable from an email gateway and must conduct initial static triage without executing the file. Which of the following actions should the analyst perform? (Choose two.)

**A.** Calculate the file hash

**B.** Extract readable strings from the file

**C.** Open the file on a production workstation

**D.** Run the executable with administrator privileges

**E.** Disable endpoint protection before analysis

**ANSWER: A B**

**Explanation:**

**Calculate the file hash** is correct because a cryptographic hash provides a consistent identifier for the submitted file. The analyst can use the hash to search internal threat-intelligence platforms, endpoint telemetry, malware repositories, and vendor intelligence sources for prior detections or reputation information. Hashing also supports evidence tracking and helps confirm that the examined file remains unchanged.

**Extract readable strings from the file** is also correct because embedded strings can reveal useful static indicators without executing the program. Relevant strings may include domains, IP addresses, file paths, registry locations, mutex names, command-line arguments, error messages, or suspicious PowerShell commands. The analyst should treat strings as leads for additional analysis because malware may encrypt, encode, or omit meaningful readable content. See MITRE ATT&CK: Obfuscated Files or Information and CISA Malware guidance.

## QUESTION NO: 13

The incident response team needs to track which user last connected to a specific Windows domain controller. Which of the following is the BEST way to identify that specific user?

**A.** Check Systems Event Log on the user's computer

**B.** Check Systems Event Log on the domain controller

**C.** Check Security Log on the user's computer

**D.** Check SecurityLog on the domain controller

**ANSWER: D**

**Explanation:**

Checking the SecurityLog on the domain controller is the best method because a domain controller records security-auditing events for authentication activity that it processes. In an Active Directory domain, the domain controller is the authoritative system for domain account authentication and authorization activity. Its Security log can contain events such as successful account logons, Kerberos authentication-service ticket requests, and NTLM authentication events, depending on the authentication protocol and configured audit policy. These records include useful incident-response details, including the account name, time of the event, source workstation or network address where available, logon type, and authentication process. Investigators can sort the relevant Security log events by time and correlate the account and source information to establish which user most recently authenticated to or connected with that specific domain controller. This approach also preserves the investigation's focus on evidence maintained by the system being examined rather than relying on a potentially unavailable or altered endpoint. Microsoft documents that Advanced Audit Policy can record account logon events on domain controllers, while Windows Security auditing records logon-related activity in the Security event log. See Microsoft's Audit account logon events documentation and Microsoft's Event 4624 documentation.