DUMPSARENA

CyberSec First Responder (CFR) Exam

CertNexus CFR-410

Version Demo

Total Demo Questions: 20

Total Premium Questions: 207

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and Preparing for Incident Response	65
Topic 2, Performing Threat Analysis and Hunting	55
Topic 3, Collecting and Analyzing Cybersecurity Intelligence	8
Topic 4, Responding to Cybersecurity Incidents	5
Topic 5, Investigating Cybersecurity Incidents	50
Topic 6, Containing, Eradicating, and Recovering from Cybersecurity Incidents	17
Topic 7, Reporting and Communicating Incident Response Findings	5
Topic 8, Mix Questions	2
Total	207

QUESTION NO: 1

A responder is investigating a suspected malicious PowerShell execution on a Windows endpoint. Which of the following artifacts can provide useful evidence of the command and its execution? (Choose two.)

A. PowerShell operational logs

B. Process-creation events

C. Monitor refresh-rate settings

D. Printer spooler configuration

E. Screen-resolution settings

ANSWER: A B

Explanation:

PowerShell operational logs and **process-creation events** can provide useful evidence of malicious PowerShell activity. PowerShell logging can capture script blocks, modules, and operational events depending on organizational configuration. Process-creation telemetry can show that `powershell.exe` was executed, identify the parent process, record the command line, and associate the activity with a user account.

Correlating these sources can help responders determine how PowerShell was launched, what commands were attempted, and whether suspicious child processes or network connections followed. Microsoft documents PowerShell logging capabilities in its PowerShell security overview, and MITRE ATT&CK identifies PowerShell as a commonly abused command and scripting interpreter at T1059.001.

QUESTION NO: 2

Which two options represent the most basic methods for designing a DMZ network firewall? (Choose two.)

A. Software firewall

B. Single firewall

C. Triple firewall

D. Dual firewall

ANSWER: B D

Explanation:

Single firewall and **Dual firewall** are the two fundamental DMZ firewall architectures. A single-firewall design, often called a three-legged or three-homed firewall arrangement, uses one firewall with separate interfaces or security zones for the internet, the DMZ, and the trusted internal network. Firewall policy permits only the specific inbound services that must reach DMZ hosts, such as a public web service, while tightly controlling any traffic between the DMZ and internal systems. This is the simplest common topology because one security device enforces segmentation among all three network areas.

A dual-firewall design places the DMZ between two separate firewalls. The perimeter firewall controls traffic between the internet and the DMZ, while the internal firewall independently controls traffic between the DMZ and the internal network. This layered arrangement provides defense in depth: a compromise of a public-facing DMZ system does not automatically grant the same level of access to the internal network. Both architectures embody the core purpose of a DMZ: isolate externally accessible services from trusted resources and allow only explicitly authorized flows. NIST discusses firewall architectures and policy enforcement in SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy; CISA also describes network segmentation principles in its information security guidance.

QUESTION NO: 3

While planning a vulnerability assessment on a computer network, which of the following is essential? (Choose two.)

A. Identifying exposures

B. Identifying critical assets

C. Establishing scope

D. Running scanning tools

E. Installing antivirus software

ANSWER: B C

Explanation:

Identifying critical assets and **Establishing scope** are essential planning activities for a vulnerability assessment. Identifying critical assets establishes what information systems, applications, data repositories, network segments, and services have the greatest business or mission importance. This lets the assessment team prioritize systems whose compromise would have the most serious effect on confidentiality, integrity, availability, safety, operations, or regulatory obligations. Asset criticality also helps determine the appropriate assessment depth and ensures that significant resources are directed toward the organization's highest-risk environment.

Establishing scope defines the authorized assessment boundary before any testing begins. The scope should document included hosts, networks, applications, cloud resources, interfaces, locations, time windows, assessment methods, points of contact, and any constraints or exclusions. Clear authorization and scope protect both the organization and the assessment team by preventing unintended testing of systems outside the agreed boundary. Together, asset identification and scope provide the context needed to plan a focused, risk-based, and authorized assessment. NIST describes planning as defining assessment scope and identifying relevant targets and information in its Technical Guide to Information Security Testing and Assessment. CISA also emphasizes maintaining an asset inventory to understand and manage organizational cyber risk in its vulnerability-management guidance.

QUESTION NO: 4

A security analyst suspects that a web server has been compromised and is being used to host a web shell. Which of the following findings would support this conclusion? (Choose two.)

A. An unexpected script in the web root directory

B. A web server process spawning a command shell

C. Regular operating-system patch installation

D. A valid TLS certificate assigned to the website

E. A scheduled backup of the web-server configuration

ANSWER: A B

Explanation:

An unexpected script in the web root directory is a strong indicator of a possible web shell. Attackers commonly upload scripts to a directory served by the web application so that commands can be issued through HTTP or HTTPS requests. Such files may use legitimate-looking names or extensions to avoid detection.

A web server process spawning a command shell is also suspicious because web server processes normally handle web requests rather than launch interactive command interpreters. A process relationship such as a web server process starting `cmd.exe`, `powershell.exe`, or `/bin/sh` can indicate that a web shell is executing operating-system commands. MITRE ATT&CK documents web shells as a method adversaries use to maintain access to compromised servers; see MITRE ATT&CK: Web Shell.

QUESTION NO: 5

An organization stores password hashes for a customer application. Which of the following is the PRIMARY purpose of adding a unique salt to each password before hashing it?

A. Prevent the effective use of precomputed hash tables

B. Encrypt the password for later recovery

C. Reduce the size of the password hash

D. Allow several users to share the same hash value

ANSWER: A

Explanation:

Prevent the effective use of precomputed hash tables is correct because a unique random salt causes identical passwords to produce different stored hash values. This makes rainbow tables and other precomputed password-hash lists far less useful because an attacker would need to generate guesses separately for each salt value.

Salting does not replace the need for a strong password-hashing algorithm with an appropriate work factor, such as Argon2, bcrypt, PBKDF2, or scrypt. NIST recommends using salted, computationally expensive password-verification mechanisms to increase the cost of offline password-guessing attacks; see NIST SP 800-63B.

QUESTION NO: 6

Vulnerability scanners generally classify vulnerabilities by which of the following? (Choose two.)

A. Exploit range

B. Costs

C. Severity level

D. Zero days

E. Threat modeling

ANSWER: A C

Explanation:

Vulnerability scanners generally categorize findings using a severity rating and information about the range in which an exploit can be used. Severity level communicates the expected impact and remediation priority of a finding. Scanner reports commonly map findings to ratings such as critical, high, medium, and low, often using CVSS-derived information. This lets responders focus first on vulnerabilities most likely to cause significant compromise or business harm.

Exploit range describes the scope or reach of exploitation, such as whether an attacker can exploit the vulnerability remotely over a network, from an adjacent network, or only with local access. This closely aligns with the CVSS Attack Vector metric, which expresses the conditions and proximity required for exploitation. Combining severity with exploit range gives incident responders useful context for triage: a serious remotely exploitable vulnerability generally demands more urgent attention than one requiring local access and extensive prerequisites. The CVSS specification describes the severity and attack-vector concepts used in vulnerability assessment. NIST also explains that vulnerability scanning identifies and prioritizes known weaknesses for remediation in its Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 7

During recovery from an incident, which three options should a company focus on? (Choose three.)

A. Evaluating the success of the current incident response plan

B. Ensuring proper notifications have been made

C. Providing details of the breach to media

D. Identifying the responsible parties

E. Restoring system and network connectivity

F. Determining the financial impact of the breach

ANSWER: A B E

Explanation:

Recovery is the phase in which the organization safely returns affected business services to normal operation while completing the essential actions needed to close out the incident responsibly. **Restoring system and network connectivity** is central to recovery: systems should be rebuilt or restored from known-good sources, validated, and returned to service in a controlled manner. Recovery also includes **ensuring proper notifications have been made**. Notifications to internal leadership, customers, partners, insurers, regulators, or other required parties must follow the organization's incident communications procedures and applicable legal or contractual requirements. Finally, **evaluating the success of the current incident response plan** captures whether recovery objectives were met and identifies improvements for future incidents. This evaluation provides practical lessons that can update procedures, recovery capabilities, playbooks, and training. NIST's incident-handling guidance describes recovery as restoring affected systems and validating normal operations, followed by lessons learned that improve the incident-response process. NIST's Cybersecurity Framework likewise emphasizes recovery planning and improvements based on recovery activities. See NIST SP 800-61 Rev. 2 and NIST Cybersecurity Framework.

QUESTION NO: 8

The NIST framework 800-137 breaks down the concept of continuous monitoring into which system of tiers?

A. Tier 1 is information systems, Tier 2 is mission/business processes, and Tier 3 is the organization.

B. Tier 1 is the organization, Tier 2 is mission/business processes, and Tier 3 is information systems.

C. Tier 1 is information systems, Tier 2 is the organization, and Tier 3 is mission/business processes.

D. Tier 1 is the organization, Tier 2 is information systems, and Tier 3 is mission/business processes.

ANSWER: B

Explanation:

The correct tier structure is "Tier 1 is the organization, Tier 2 is mission/business processes, and Tier 3 is information systems." NIST Special Publication 800-137 applies continuous monitoring within the three-tier risk-management hierarchy established by NIST. At the organization tier, leaders establish governance, risk-management strategy, priorities, and organization-wide monitoring requirements. At the mission/business-process tier, those organization-level decisions are translated into requirements and controls that support particular missions, services, and business functions. At the information-system tier, monitoring is performed for individual systems and their components, producing technical security status information such as configuration, vulnerability, control-assessment, and incident data. This bottom tier supplies detailed operational evidence that can be aggregated and used for risk decisions at the business-process and organization levels. The ordering is important because it reflects the flow from enterprise risk governance, through mission execution, to implementation and monitoring of the systems that process, store, or transmit information. NIST describes this hierarchy in NIST SP 800-137, Information Security Continuous Monitoring; the broader three-tier risk-management framework is also defined in NIST SP 800-39.

QUESTION NO: 9

A security operations center is creating alerts for possible data exfiltration. Which of the following network behaviors should be considered suspicious? (Choose two.)

A. A large outbound transfer to an unfamiliar external host

B. Regular outbound connections at consistent intervals

C. Internal DNS queries to an approved resolver

D. Encrypted connections to an approved backup service

E. Normal traffic during established business hours

ANSWER: A B

Explanation:

A large outbound transfer to an unfamiliar external host and **regular outbound connections at consistent intervals** should be considered suspicious. An unexpectedly large transfer can indicate that sensitive data is being copied from the organization to attacker-controlled infrastructure. Regular connections at consistent intervals can indicate beaconing, where malware contacts command-and-control infrastructure on a recurring schedule.

These indicators should be correlated with asset role, user activity, destination reputation, protocol, data volume baselines, and endpoint telemetry before concluding that an incident has occurred. NIST identifies network traffic and flow data as useful sources for detecting and analyzing anomalous communications. See NIST SP 800-92, Guide to Computer Security Log Management and MITRE ATT&CK: Application Layer Protocol.

QUESTION NO: 10

A web server is under a denial of service (DoS) attack. The administrator reviews logs and creates an access control list (ACL) to stop the attack. Which of the following technologies could perform these steps automatically in the future?

A. Intrusion prevention system (IPS)

B. Intrusion detection system (IDS)

C. Blacklisting

D. Whitelisting

ANSWER: A

Explanation:

Intrusion prevention system (IPS) is correct because it is designed to inspect network traffic, recognize malicious activity using signatures, policies, anomalies, or behavioral indicators, and actively take enforcement action. In this scenario, the relevant automated response is identifying traffic consistent with a denial-of-service attack and applying a blocking control, such as dropping offending packets, resetting connections, rate-limiting traffic, or dynamically adding a source address or other indicator to an access control list. This combines the administrator's manual review-and-block workflow into a preventive security control that can respond at network speed.

An IPS is typically deployed inline, meaning traffic passes through it and the system can directly prevent detected attacks from reaching the protected web server. Automated prevention is especially valuable during DoS events because high traffic volume can make manual log analysis and ACL updates too slow to protect availability effectively. NIST describes intrusion prevention technologies as capable of monitoring events and attempting to stop detected incidents, while CISA emphasizes implementing protective controls that detect and mitigate denial-of-service activity. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and CISA: Denial-of-Service Attacks.

QUESTION NO: 11

What is the primary purpose of the "information security incident triage and processing function" in the (CSIRT) Computer Security Incident Response Team Services Framework?

A. To analyze and gain an understanding of a confirmed information security incident.

B. To initially review, categorize, prioritize, and process a reported information security incident.

C. To receive and process reports of potential information security incidents from constituents, Information Security Event Management services, or third parties.

D. To accept or receive information about an information security incident, as reported from constituents or third parties.

ANSWER: B

Explanation:

The primary purpose is to initially review, categorize, prioritize, and process a reported information security incident. Triage is the CSIRT's structured first assessment after an incident report enters the response workflow. The team collects enough information to determine the nature of the report, assesses its potential business and technical impact, assigns an appropriate severity and priority, and directs the case into the suitable handling process. This function ensures that urgent, high-impact incidents receive attention and resources quickly while reports with lower urgency are tracked and handled in accordance with established procedures. Effective triage also creates a consistent record of the incident and its initial classification, supporting escalation, coordination, communication, and later analysis. The CSIRT Services Framework distinguishes this initial assessment and routing activity from later, more detailed incident analysis and from the intake function that receives reports. This interpretation aligns with the incident-handling lifecycle described by the CERT Coordination Center and NIST, where analysis and prioritization guide the response effort. See the CERT CSIRT Services Framework and NIST's Computer Security Incident Handling Guide.

QUESTION NO: 12

Senior management has stated that antivirus software must be installed on all employee workstations. Which

of the following does this statement BEST describe?

A. Guideline

B. Procedure

C. Policy

D. Standard

ANSWER: C

Explanation:

Policy is correct because the statement expresses a mandatory, organization-wide management directive: every employee workstation must have antivirus software installed. Security policies communicate leadership's intent, establish required security outcomes, and provide the authority for the organization to implement and enforce security controls. Since the requirement comes from senior management and applies broadly to employee workstations, it functions as a policy-level requirement rather than an implementation task.

A policy need not prescribe the product, configuration settings, deployment method, update interval, or personnel responsible for installation. Those operational details can be established later in supporting documentation and processes. The essential point is that management has set a compulsory security expectation intended to reduce malware risk across the organization. NIST describes policy as management direction for protecting organizational operations and assets, and recognizes that policies establish the foundation for an information security program. See NIST SP 800-12 Rev. 1 and NIST Cybersecurity Framework.

QUESTION NO: 13

According to SANS, when should an incident retrospective be performed?

A. After law enforcement has identified the perpetrators of the attack.

B. Within six months following the end of the incident.

C. No later than two weeks from the end of the incident.

D. Immediately concluding eradication of the root cause

ANSWER: C

Explanation:

No later than two weeks from the end of the incident. is correct. A retrospective, also called a lessons-learned review or post-incident review, is a structured opportunity for the incident-response team and relevant stakeholders to document what occurred, assess the effectiveness of detection, containment, eradication, recovery, communications, and decision-making, and assign improvements to procedures and controls. Performing the review within two weeks preserves critical operational context: timelines, evidence-handling decisions, tool output, communications, and participant recollections are still readily available. This timing also enables the organization to convert findings into tracked remediation activities before the same weaknesses can contribute to another event. The review should produce actionable outcomes, such as updates to playbooks, escalation paths, logging coverage, monitoring rules, training, and incident-response documentation. SANS emphasizes post-incident activity and lessons learned as a core part of the incident-handling lifecycle; the two-week limit supplies a practical window for completing that activity while details remain fresh. See the SANS Incident Handler's Handbook and NIST's guidance on post-incident lessons learned in SP 800-61 Rev. 2.

QUESTION NO: 14 - (SIMULATION)

What is the correct order of the DFIR phases?

ANSWER: See the explanation for the answer

Explanation:

The correct DFIR phase order is:

1. **Preparation**
2. **Identification**
3. **Containment**
4. **Eradication**
5. **Recovery**
6. **Lessons Learned**

Prepare procedures and resources first; identify and validate the incident; contain its spread; eradicate the root cause and malicious artifacts; restore normal operations; then document findings and improve controls during the lessons-learned phase.

QUESTION NO: 15

Which of the following tools can help to detect suspicious or unauthorized changes to critical system configuration files?

A. Tripwire

B. Logstash

C. Nessus

D. Netcat

E. Ifconfig

ANSWER: A

Explanation:

Tripwire is correct because it is a file integrity monitoring tool designed to establish a trusted baseline for important files, including operating system and application configuration files. It records file attributes and cryptographic checksums, then periodically compares the current state of monitored files with that baseline. When a configuration file is created, modified, deleted, or has relevant attributes changed without authorization, Tripwire can generate an alert or report for investigation. This supports a first responder's need to identify potential indicators of compromise, unauthorized administrative activity, persistence mechanisms, and accidental configuration drift. File integrity monitoring is particularly valuable for critical locations such as system configuration directories, authentication-related files, service definitions, and security-policy files, where unauthorized changes can materially affect a host's security posture. Tripwire's core function and its use of policy-based integrity checking are described in the Tripwire Enterprise product overview. The importance of monitoring files for unauthorized modification is also reflected in NIST's guidance on file integrity checking in NIST SP 800-92, Guide to Computer Security Log Management.

QUESTION NO: 16

The Key Reinstallation Attack (KRACK) vulnerability is specific to which types of devices? (Choose two.)

A. Wireless router

B. Switch

C. Firewall

D. Access point

E. Hub

ANSWER: A D

Explanation:

KRACK targets weaknesses in implementations of the WPA2 four-way handshake, the security process used when Wi-Fi clients associate with a wireless network. Therefore, the affected device types are Wi-Fi infrastructure devices that participate in WPA2-protected wireless communications, including a **Wireless router** and an **Access point**. A wireless router commonly provides the wireless access-point function in addition to routing traffic between the local network and other networks. A standalone access point provides the wireless radio service and likewise participates in the WPA2 handshake with connecting clients. If an affected implementation accepts a replayed handshake message, it can reinstall an already-in-use encryption key and reset associated parameters such as packet counters or nonces. This can undermine the confidentiality and integrity protections expected from the wireless connection. The issue is implementation-dependent, so patching the relevant firmware or software is essential; updating Wi-Fi clients is also important because KRACK affected multiple WPA2-capable implementations. The original research and mitigation information are available from KRACK Attacks and the CISA KRACK vulnerability alert.

QUESTION NO: 17

While performing routing maintenance on a Windows Server, a technician notices several unapproved Windows Updates and that remote access software has been installed. The technician suspects that a malicious actor has gained access to the system. Which of the following steps in the attack process does this activity indicate?

A. Expanding access

B. Covering tracks

C. Scanning

D. Persistence

ANSWER: A

Explanation:

Expanding access is the correct step because the observed changes indicate activity occurring after an attacker has obtained an initial foothold and is working to increase the usefulness, reach, or durability of that compromise. Installing remote-access software gives the actor an additional channel through which to control the server, potentially from outside the organization's normal administration workflow. Unauthorized update activity can also reflect an attempt to alter the system state, introduce components, or make changes that support the attacker's continued operations and broader access.

In incident-response terms, post-compromise activity commonly includes deploying tools and modifying systems so the adversary can access more resources or operate with greater control. The MITRE ATT&CK knowledge base documents software deployment and remote-access tooling as techniques adversaries use after gaining access, including remote access software under Remote Access Software. The related adversary objective is often to extend control beyond the original point of compromise, consistent with the attack-process stage of expanding access. These findings should be treated as indicators requiring immediate containment and forensic preservation.

QUESTION NO: 18

Which two answer options correctly highlight the difference between static and dynamic binary analysis techniques? (Choose two.)

A. Dynamic analysis tells everything the program can do. and static analysis tells exactly what the program does when it is executed in a given environment and with a particular input.

B. Static analysis tells everything the program can do. and dynamic analysis tells exactly what the program does when it is executed in a given environment and with a particular input.

C. Dynamic analysis examines the binary without executing it, while static analysis executes the program and observes its behavior.

D. Static analysis examines the binary without executing it. while dynamic analysis executes the program and observes its behavior.

ANSWER: B D

Explanation:

"Static analysis tells everything the program can do. and dynamic analysis tells exactly what the program does when it is executed in a given environment and with a particular input." correctly states the core distinction. Static binary analysis inspects a file without running it. Analysts can examine file headers, strings, imports, embedded resources, control flow, and disassembled or decompiled instructions to identify possible capabilities and execution paths. This provides broad visibility into behavior the program may be capable of performing.

"Static analysis examines the binary without executing it. while dynamic analysis executes the program and observes its behavior." is also correct because dynamic analysis requires controlled execution, commonly in an isolated sandbox or virtual machine. This lets an analyst observe behaviors actually triggered under the chosen operating system, configuration, network conditions, and supplied inputs, such as process creation, file changes, registry modifications, and network connections. Static and dynamic analysis are complementary: static techniques identify potential functionality, while dynamic techniques validate and observe behavior manifested during a specific run. NIST describes malware analysis as including both examination of malware code and observation of its effects during execution; see NIST SP 800-83 Rev. 1. Additional practical guidance on safely analyzing suspicious files in isolated environments is available from CISA.

QUESTION NO: 19

When tracing an attack to the point of origin, which of the following items is critical data to map layer 2 switching?

A. DNS cache

B. ARP cache

C. CAM table

D. NAT table

ANSWER: C

Explanation:

CAM table is critical because it records the Layer 2 forwarding information a switch uses to associate learned source MAC addresses with specific physical switch interfaces (and, where applicable, VLANs). During incident investigation, an analyst can take a MAC address observed in packet captures, endpoint records, or other network telemetry and look it up in the switch's CAM table—also called its forwarding database—to identify the port through which that device is connected. The investigator can then trace that port to a wall jack, wireless access point uplink, downstream switch, or directly attached endpoint, progressively following the path toward the originating system.

This information is particularly valuable when an attacker has moved within a local network or when the apparent source IP address alone does not identify a physical network location. Switch forwarding entries represent the actual Layer 2 association needed to map Ethernet traffic to infrastructure ports at the relevant point in time. Cisco describes the MAC address table as the table used by a switch to map MAC addresses to switch ports and forward frames accordingly. Preserving these entries promptly is important because dynamic entries can age out or change as devices move or network topology changes. See Cisco's Layer 2 switching documentation and Cisco's MAC address table overview.

QUESTION NO: 20

During which phase of the incident response process should an organization develop policies and procedures for incident handling?

A. Containment

B. Preparation

C. Identification

D. Recovery

ANSWER: B

Explanation:

Preparation is the phase in which an organization establishes and maintains its incident-response capability before a security incident occurs. This includes creating incident-response policies, plans, and standard operating procedures; defining incident categories and escalation paths; assigning roles and responsibilities; establishing communication and reporting requirements; and ensuring personnel have appropriate training, tools, and access. Preparation also involves maintaining relevant asset information, logging capabilities, forensic resources, and relationships with internal stakeholders or external service providers. Documenting these elements in advance enables responders to act consistently, quickly, and with appropriate authority when an incident is identified. The incident response lifecycle described by NIST explicitly identifies preparation as the foundational activity that supports the later detection, analysis, containment, eradication, recovery, and post-incident improvement activities. CertNexus CFR concepts likewise emphasize having documented processes and organizational readiness prior to an event, rather than attempting to design response procedures during active incident handling. See NIST's Computer Security Incident Handling Guide (SP 800-61 Rev. 2) and NIST's Cybersecurity Framework resources.