CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

NEW QUESTION 1
The incident response team has completed root cause analysis for an incident. Which of the following actions should be taken in the next phase of the incident response process? (Choose two.)

A. Providing a briefing to management
B. Updating policies and procedures
C. Training staff for future incidents
D. Investigating responsible staff
E. Drafting a recovery plan for the incident

Answer: BE

NEW QUESTION 2
A company website was hacked via the following SQL query: 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 a cross-site scripting (XSS) attack

Answer: C

NEW QUESTION 3
Various logs are collected for a data leakage case to make a forensic analysis. Which of the following are MOST important for log integrity? (Choose two.)

A. Hash value
B. Time stamp
C. Log type
D. Modified date/time
E. Log path

Answer: AB

NEW QUESTION 4
A security investigator has detected an unauthorized insider reviewing files containing company secrets. Which of the following commands could the investigator use to determine which files have been opened by
this user?

A. ls
B. lsof
C. ps
D. netstat

Answer: B

NEW QUESTION 5
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: AC

NEW QUESTION 6
Detailed step-by-step instructions to follow during a security incident are considered:

A. Policies
B. Guidelines
C. Procedures
D. Standards

Answer: C

NEW QUESTION 7
According to company policy, all accounts with administrator privileges should have suffix _ja. While reviewing Windows workstation configurations, a security administrator discovers an account without the suffix in the administrator's group. Which of the following actions should the security administrator take?

A. Review the system log on the affected workstation.
B. Review the security log on a domain controller.
C. Review the system log on a domain controller.
D. Review the security log on the affected workstation.

Answer: B

NEW QUESTION 8
Tcpdump is a tool that can be used to detect which of the following indicators of compromise?

A. Unusual network traffic
B. Unknown open ports
C. Poor network performance
D. Unknown use of protocols

Answer: A

NEW QUESTION 9
An administrator believes that a system on VLAN 12 is Address Resolution Protocol (ARP) poisoning clients on the network. The administrator attaches a system to VLAN 12 and uses Wireshark to capture traffic. After reviewing the capture file, the administrator finds no evidence of ARP poisoning. Which of the following actions should the administrator take next?

A. Clear the ARP cache on their system.
B. Enable port mirroring on the switch.
C. Filter Wireshark to only show ARP traffic.
D. Configure the network adapter to promiscuous mode.

Answer: D

NEW QUESTION 10
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

NEW QUESTION 10
While reviewing some audit logs, an analyst has identified consistent modifications to the sshd_config file for an organization's server. The analyst would like to investigate and compare contents of the current file with archived versions of files that are saved weekly. Which of the following tools will be MOST effective during the investigation?

A. cat * | cut –d ',' –f 2,5,7
B. more * | grep
C. diff
D. sort *

Answer: C

NEW QUESTION 15
A first responder notices a file with a large amount of clipboard information stored in it. Which part of the MITRE ATT&CK matrix has the responder discovered?

A. Collection
B. Discovery
C. Lateral movement
D. Exfiltration

Answer: D

NEW QUESTION 16
A suspicious script was found on a sensitive research system. Subsequent analysis determined that proprietary data would have been deleted from both the local server and backup media immediately following a specific administrator's removal from an employee list that is refreshed each evening. Which of the following BEST describes this scenario?

A. Backdoor
B. Rootkit
C. Time bomb
D. Login bomb

Answer: A

NEW QUESTION 19
A user receives an email about an unfamiliar bank transaction, which includes a link. When clicked, the link redirects the user to a web page that looks exactly like their bank's website and asks them to log in with their username and password. Which type of attack is this?

A. Whaling
B. Smishing
C. Vishing

D. Phishing

Answer: D

NEW QUESTION 21
An incident handler is assigned to initiate an incident response for a complex network that has been affected by malware. Which of the following actions should be taken FIRST?

A. Make an incident response plan.
B. Prepare incident response tools.
C. Isolate devices from the network.
D. Capture network traffic for analysis.

Answer: D

NEW QUESTION 23
Which of the following attacks involves sending a large amount of spoofed User Datagram Protocol (UDP) traffic to a router's broadcast address within a network?

A. Land attack
B. Fraggle attack
C. Smurf attack
D. Teardrop attack

Answer: C

NEW QUESTION 28
After a security breach, a security consultant is hired to perform a vulnerability assessment for a company's web application. Which of the following tools would the consultant use?

A. Nikto
B. Kismet
C. tcpdump
D. Hydra

Answer: A

NEW QUESTION 33
A network administrator has determined that network performance has degraded due to excessive use of social media and Internet streaming services. Which of the following would be effective for limiting access to these types of services, without completely restricting access to a site?

A. Whitelisting
B. Web content filtering
C. Network segmentation
D. Blacklisting

Answer: B

NEW QUESTION 34
A Windows system administrator has received notification from a security analyst regarding new malware that executes under the process name of "armageddon.exe" along with a request to audit all department workstations for its presence. In the absence of GUI-based tools, what command could the administrator execute to complete this task?

A. ps -ef | grep armageddon
B. top | grep armageddon
C. wmic process list brief | find "armageddon.exe"
D. wmic startup list full | find "armageddon.exe"

Answer: C

NEW QUESTION 35
A Linux system administrator found suspicious activity on host IP 192.168.10.121. This host is also establishing a connection to IP 88.143.12.123. Which of the following commands should the administrator use to capture only the traffic between the two hosts?

A. # tcpdump -i eth0 host 88.143.12.123
B. # tcpdump -i eth0 dst 88.143.12.123
C. # tcpdump -i eth0 host 192.168.10.121
D. # tcpdump -i eth0 src 88.143.12.123

Answer: B

NEW QUESTION 39
Which of the following would MOST likely make a Windows workstation on a corporate network vulnerable to remote exploitation?

A. Disabling Windows Updates
B. Disabling Windows Firewall

C. Enabling Remote Registry
D. Enabling Remote Desktop

Answer: D

NEW QUESTION 42
A company help desk is flooded with calls regarding systems experiencing slow performance and certain Internet sites taking a long time to load or not loading at all. The security operations center (SOC) analysts who receive these calls take the following actions:
-Running antivirus scans on the affected user machines
-Checking department membership of affected users
-Checking the host-based intrusion prevention system (HIPS) console for affected user machine alerts
-Checking network monitoring tools for anomalous activities
Which of the following phases of the incident response process match the actions taken?

A. Identification
B. Preparation
C. Recovery
D. Containment

Answer: A

NEW QUESTION 46
During an incident, the following actions have been taken:
-Executing the malware in a sandbox environment
-Reverse engineering the malware
-Conducting a behavior analysis
Based on the steps presented, which of the following incident handling processes has been taken?

A. Containment
B. Eradication
C. Recovery
D. Identification

Answer: A

Explanation:
The "Containment, eradication and recovery" phase is the period in which incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).

NEW QUESTION 51
An automatic vulnerability scan has been performed. Which is the next step of the vulnerability assessment process?

A. Hardening the infrastructure
B. Documenting exceptions
C. Assessing identified exposures
D. Generating reports

Answer: D

NEW QUESTION 55
To minimize vulnerability, which steps should an organization take before deploying a new Internet of Things (IoT) device? (Choose two.)

A. Changing the default password
B. Updating the device firmware
C. Setting up new users
D. Disabling IPv6
E. Enabling the firewall

Answer: BE

NEW QUESTION 56
Which of the following types of attackers would be MOST likely to use multiple zero-day exploits executed against high-value, well-defended targets for the purposes of espionage and sabotage?

A. Cybercriminals
B. Hacktivists
C. State-sponsored hackers
D. Cyberterrorist

Answer: C

NEW QUESTION 60
A security administrator notices a process running on their local workstation called SvrsScEsdKexzCv.exe. The unknown process is MOST likely:

A. Malware
B. A port scanner
C. A system process

D. An application process

Answer: A

NEW QUESTION 65
Malicious code designed to execute in concurrence with a particular event is BEST defined as which of the following?

A. Logic bomb
B. Rootkit
C. Trojan
D. Backdoor

Answer: A

NEW QUESTION 66
An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/ screen) in numerical order?

A. cat | tac
B. more
C. sort –n
D. less

Answer: C

NEW QUESTION 70
Which of the following are part of the hardening phase of the vulnerability assessment process? (Choose two.)

A. Installing patches
B. Updating configurations
C. Documenting exceptions
D. Conducting audits
E. Generating reports

Answer: AB

NEW QUESTION 74
A security analyst has discovered that an application has failed to run. Which of the following is the tool MOST likely used by the analyst for the initial discovery?

A. syslog
B. MSConfig
C. Event Viewer
D. Process Monitor

Answer: C

NEW QUESTION 77
Which of the following are legally compliant forensics applications that will detect an alternative data stream (ADS) or a file with an incorrect file extension? (Choose two.)

A. Disk duplicator
B. EnCase
C. dd
D. Forensic Toolkit (FTK)
E. Write blocker

Answer: BD

NEW QUESTION 79
Which of the following does the command nmap –open 10.10.10.3 do?

A. Execute a scan on a single host, returning only open ports.
B. Execute a scan on a subnet, returning detailed information on open ports.
C. Execute a scan on a subnet, returning all hosts with open ports.
D. Execute a scan on a single host, returning open services.

Answer: D

NEW QUESTION 83
Which of the following is a method of reconnaissance in which a ping is sent to a target with the expectation of receiving a response?

A. Active scanning
B. Passive scanning
C. Network enumeration
D. Application enumeration

Answer: C

NEW QUESTION 87
During which phase of a vulnerability assessment would a security consultant need to document a requirement to retain a legacy device that is no longer supported and cannot be taken offline?

A. Conducting post-assessment tasks
B. Determining scope
C. Identifying critical assets
D. Performing a vulnerability scan

Answer: C

NEW QUESTION 88
Which of the following technologies would reduce the risk of a successful SQL injection attack?

A. Reverse proxy
B. Web application firewall
C. Stateful firewall
D. Web content filtering

Answer: B

NEW QUESTION 89
According to Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

A. 3 months
B. 6 months
C. 1 year
D. 5 years

Answer: C

NEW QUESTION 91
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CFR-410 Practice Exam Features:

* CFR-410 Questions and Answers Updated Frequently

* CFR-410 Practice Questions Verified by Expert Senior Certified Staff

* CFR-410 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CFR-410 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CFR-410 Practice Test Here