

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

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 3

After a hacker obtained a shell on a Linux box, the hacker then sends the exfiltrated data via Domain Name System (DNS). This is an example of which type of data exfiltration?

- A. Covert channels
- B. File sharing services
- C. Steganography
- D. Rogue service

Answer: A

NEW QUESTION 4

A network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers. Which of the following commands would stop this attack? (Choose two.)

- A. `iptables -A INPUT -p tcp --dport 25 -d x.x.x.x -j ACCEPT`
- B. `iptables -A INPUT -p tcp --sport 25 -d x.x.x.x -j ACCEPT`
- C. `iptables -A INPUT -p tcp --dport 25 -j DROP`
- D. `iptables -A INPUT -p tcp --destination-port 21 -j DROP`
- E. `iptables -A FORWARD -p tcp --dport 6881:6889 -j DROP`

Answer: AC

NEW QUESTION 5

Which of the following is the GREATEST risk of having security information and event management (SIEM) collect computer names with older log entries?

- A. There may be duplicate computer names on the network.
- B. The computer name may not be admissible evidence in court.
- C. Domain Name System (DNS) records may have changed since the log was created.
- D. There may be field name duplication when combining log files.

Answer: D

NEW QUESTION 6

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 7

A common formula used to calculate risk is: + Threats + Vulnerabilities = Risk. Which of the following represents the missing factor in this formula?

- A. Exploits
- B. Security
- C. Asset
- D. Probability

Answer: C

NEW QUESTION 8

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 9

Nmap is a tool most commonly used to:

- A. Map a route for war-driving
- B. Determine who is logged onto a host
- C. Perform network and port scanning
- D. Scan web applications

Answer: C

NEW QUESTION 10

A security administrator needs to review events from different systems located worldwide. Which of the following is MOST important to ensure that logs can be effectively correlated?

- A. Logs should be synchronized to their local time zone.
- B. Logs should be synchronized to a common, predefined time source.
- C. Logs should contain the username of the user performing the action.
- D. Logs should include the physical location of the action performed.

Answer: A

NEW QUESTION 10

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 12

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 16

It was recently discovered that many of an organization's servers were running unauthorized cryptocurrency mining software. Which of the following assets were being targeted in this attack? (Choose two.)

- A. Power resources
- B. Network resources
- C. Disk resources
- D. Computing resources
- E. Financial resources

Answer: AB

NEW QUESTION 20

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: B

Explanation:

The host that owns the IP address sends an ARP reply message with its physical address. Each host machine maintains a table, called ARP cache, used to convert MAC addresses to IP addresses. Since ARP is a stateless protocol, every time a host gets an ARP reply from another host, even though it has not sent an ARP request for that reply, it accepts that ARP entry and updates its ARP cache. The process of updating a target host's ARP cache with a forged entry is referred to as poisoning.

NEW QUESTION 25

A company has noticed a trend of attackers gaining access to corporate mailboxes. Which of the following would be the BEST action to take to plan for this kind of attack in the future?

- A. Scanning email server for vulnerabilities
- B. Conducting security awareness training
- C. Hardening the Microsoft Exchange Server
- D. Auditing account password complexity

Answer: A

NEW QUESTION 27

A security operations center (SOC) analyst observed an unusually high number of login failures on a particular database server. The analyst wants to gather supporting evidence before escalating the observation to management. Which of the following expressions will provide login failure data for 11/24/2015?

- A. `grep 20151124 security_log | grep -c "login failure"`
- B. `grep 20150124 security_log | grep "login_failure"`
- C. `grep 20151124 security_log | grep "login"`
- D. `grep 20151124 security_log | grep -c "login"`

Answer: C

NEW QUESTION 29

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 31

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 36

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 37

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 40

Which of the following describes United States federal government cybersecurity policies and guidelines?

- A. NIST
- B. ANSI
- C. NERC
- D. GDPR

Answer: A

NEW QUESTION 45

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 50

A security engineer is setting up security information and event management (SIEM). Which of the following log sources should the engineer include that will contain indicators of a possible web server compromise? (Choose two.)

- A. NetFlow logs
- B. Web server logs
- C. Domain controller logs
- D. Proxy logs
- E. FTP logs

Answer: BC

NEW QUESTION 52

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 57

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 59

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 61

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 63

Which common source of vulnerability should be addressed to BEST mitigate against URL redirection attacks?

- A. Application
- B. Users
- C. Network infrastructure
- D. Configuration files

Answer: A

NEW QUESTION 67

As part of an organization's regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

- A. Update the latest proxy access list
- B. Monitor the organization's network for suspicious traffic
- C. Monitor the organization's sensitive databases
- D. Update access control list (ACL) rules for network devices

Answer: D

NEW QUESTION 69

A secretary receives an email from a friend with a picture of a kitten in it. The secretary forwards it to the -COMPANYWIDE mailing list and, shortly thereafter, users across the company receive the following message:

"You seem tense. Take a deep breath and relax!"

The incident response team is activated and opens the picture in a virtual machine to test it. After a short analysis, the following code is found in C:

```
\Temp\chill.exe:Powershell.exe -Command "do {(for /L %i in (2,1,254) do shutdown /r /m Error! Hyperlink reference not valid.&gt; /f /t / 0 (/c "You seem tense. Take a deep breath and relax!");Start-Sleep -s 900) } while(1)"
```

Which of the following BEST represents what the attacker was trying to accomplish?

- A. Taunt the user and then trigger a shutdown every 15 minutes.
- B. Taunt the user and then trigger a reboot every 15 minutes.
- C. Taunt the user and then trigger a shutdown every 900 minutes.
- D. Taunt the user and then trigger a reboot every 900 minutes.

Answer: B

NEW QUESTION 72

Which of the following is the FIRST step taken to maintain the chain of custody in a forensic investigation?

- A. Security and evaluating the electronic crime scene.
- B. Transporting the evidence to the forensics lab
- C. Packaging the electronic device
- D. Conducting preliminary interviews

Answer: C

NEW QUESTION 77

In which of the following attack phases would an attacker use Shodan?

- A. Scanning
- B. Reconnaissance
- C. Gaining access
- D. Persistence

Answer: A

NEW QUESTION 78

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

- A. Browser logs
- B. HTTP logs
- C. System logs
- D. Proxy logs

Answer: D

NEW QUESTION 79

An unauthorized network scan may be detected by parsing network sniffer data for:

- A. IP traffic from a single IP address to multiple IP addresses.
- B. IP traffic from a single IP address to a single IP address.
- C. IP traffic from multiple IP addresses to a single IP address.
- D. IP traffic from multiple IP addresses to other networks.

Answer: C

NEW QUESTION 82

An organization recently suffered a breach due to a human resources administrator emailing employee names and Social Security numbers to a distribution list. Which of the following tools would help mitigate this risk from recurring?

- A. Data loss prevention (DLP)
- B. Firewall
- C. Web proxy
- D. File integrity monitoring

Answer: A

NEW QUESTION 83

A cybersecurity expert assigned to be the IT manager of a middle-sized company discovers that there is little endpoint security implementation on the company's systems. Which of the following could be included in an endpoint security solution? (Choose two.)

- A. Web proxy
- B. Network monitoring system
- C. Data loss prevention (DLP)
- D. Anti-malware
- E. Network Address Translation (NAT)

Answer: AB

NEW QUESTION 86

An organization recently suffered a data breach involving a server that had Transmission Control Protocol (TCP) port 1433 inadvertently exposed to the Internet. Which of the following services was vulnerable?

- A. Internet Message Access Protocol (IMAP)
- B. Network Basic Input/Output System (NetBIOS)
- C. Database
- D. Network Time Protocol (NTP)

Answer: C

NEW QUESTION 90

If a hacker is attempting to alter or delete system audit logs, in which of the following attack phases is the hacker involved?

- A. Covering tracks
- B. Expanding access
- C. Gaining persistence
- D. Performing reconnaissance

Answer: A

NEW QUESTION 91

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 95

An incident responder discovers that the CEO logged in from their New York City office and then logged in from a location in Beijing an hour later. The incident responder suspects that the CEO's account has been compromised. Which of the following anomalies MOST likely contributed to the incident responder's suspicion?

- A. Geolocation
- B. False positive
- C. Geovelocity
- D. Advanced persistent threat (APT) activity

Answer: C

NEW QUESTION 99

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 102

While performing routine 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

NEW QUESTION 103

When performing an investigation, a security analyst needs to extract information from text files in a Windows operating system. Which of the following commands should the security analyst use?

- A. findstr
- B. grep
- C. awk
- D. sigverif

Answer: C

NEW QUESTION 108

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 109

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 113

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)