Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

https://www.2passeasy.com/dumps/CFR-410/

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
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 3
Which asset would be the MOST desirable for a financially motivated attacker to obtain from a health insurance company?

A. Transaction logs
B. Intellectual property
C. PII/PHI
D. Network architecture

Answer: C

NEW QUESTION 4
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 5
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 6
A Linux administrator is trying to determine the character count on many log files. Which of the following command and flag combinations should the administrator use?

A. tr -d
B. uniq -c
C. wc -m
D. grep -c

Answer: C

NEW QUESTION 7
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 8
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 9
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 10
During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

A. System hardening techniques
B. System optimization techniques
C. Defragmentation techniques
D. Anti-forensic techniques

Answer: D

NEW QUESTION 10
Which of the following are common areas of vulnerabilities in a network switch? (Choose two.)

A. Default port state
B. Default credentials
C. Default protocols
D. Default encryption
E. Default IP address

Answer: AB

NEW QUESTION 13
Recently, a cybersecurity research lab discovered that there is a hacking group focused on hacking into the computers of financial executives in Company A to sell the exfiltrated information to Company B. Which of the following threat motives does this MOST likely represent?

A. Desire for power
B. Association/affiliation
C. Reputation/recognition
D. Desire for financial gain

Answer: D

NEW QUESTION 14
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 16
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 17
Which of the following is a cybersecurity solution for insider threats to strengthen information protection?

A. Web proxy
B. Data loss prevention (DLP)
C. Anti-malware
D. Intrusion detection system (IDS)

Answer: B

NEW QUESTION 19
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 20
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 23
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 28
A security administrator is investigating a compromised host. Which of the following commands could the investigator use to display executing processes in real time?

A. ps
B. top
C. nice
D. pstree

Answer: B

NEW QUESTION 32
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 37
After imaging a disk as part of an investigation, a forensics analyst wants to hash the image using a tool that supports piecewise hashing. Which of the following tools should the analyst use?

A. md5sum
B. sha256sum
C. md5deep
D. hashdeep

Answer: A

NEW QUESTION 38
During a security investigation, a suspicious Linux laptop is found in the server room. The laptop is processing information and indicating network activity. The investigator is preparing to launch an investigation to determine what is happening with this laptop. Which of the following is the MOST appropriate set of Linux commands that should be executed to conduct the investigation?

A. iperf, traceroute, whois, ls, chown, cat
B. iperf, wget, traceroute, dc3dd, ls, whois
C. lsof, chmod, nano, whois, chown, ls
D. lsof, ifconfig, who, ps, ls, tcpdump

Answer: B

NEW QUESTION 43
A company that maintains a public city infrastructure was breached and information about future city projects was leaked. After the post-incident phase of the process has been completed, which of the following would be PRIMARY focus of the incident response team?

A. Restore service and eliminate the business impact.
B. Determine effective policy changes.
C. Inform the company board about the incident.
D. Contact the city police for official investigation.

Answer: B

NEW QUESTION 44
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 48
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 51
An incident at a government agency has occurred and the following actions were taken:
-Users have regained access to email accounts
-Temporary VPN services have been removed
-Host-based intrusion prevention system (HIPS) and antivirus (AV) signatures have been updated
-Temporary email servers have been decommissioned
Which of the following phases of the incident response process match the actions taken?

A. Containment
B. Post-incident
C. Recovery
D. Identification

Answer: A

NEW QUESTION 56
Which of the following characteristics of a web proxy strengthens cybersecurity? (Choose two.)

A. Increases browsing speed
B. Filters unwanted content
C. Limits direct connection to Internet
D. Caches frequently-visited websites
E. Decreases wide area network (WAN) traffic

Answer: AD

NEW QUESTION 58
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 61
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.> /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 64
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 66
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 71
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: AE

NEW QUESTION 73
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 76
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 79
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 83
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 86
Which of the following methods are used by attackers to find new ransomware victims? (Choose two.)

A. Web crawling
B. Distributed denial of service (DDoS) attack
C. Password guessing
D. Phishing
E. Brute force attack

Answer: DE

NEW QUESTION 89
Which of the following data sources could provide indication of a system compromise involving the exfiltration of data to an unauthorized destination?

A. IPS logs
B. DNS logs
C. SQL logs
D. SSL logs

Answer: A

NEW QUESTION 90
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 92
Organizations considered "covered entities" are required to adhere to which compliance requirement?

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Sarbanes-Oxley Act (SOX)
D. International Organization for Standardization (ISO) 27001

Answer: A

NEW QUESTION 97
Which of the following enables security personnel to have the BEST security incident recovery practices?

A. Crisis communication plan
B. Disaster recovery plan
C. Occupant emergency plan
D. Incident response plan

Answer: B

NEW QUESTION 101

An incident response team is concerned with verifying the integrity of security information and event management (SIEM) events after being written to disk. Which of the following represents the BEST option for addressing this concern?

A. Time synchronization
B. Log hashing
C. Source validation
D. Field name consistency

Answer: A

NEW QUESTION 106

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 110

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 111

Which of the following are well-known methods that are used to protect evidence during the forensics process? (Choose three.)

A. Evidence bags
B. Lock box
C. Caution tape
D. Security envelope
E. Secure rooms
F. Faraday boxes

Answer: ACD

NEW QUESTION 112

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 113

......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CFR-410 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CFR-410 Product From:

https://www.2passeasy.com/dumps/CFR-410/

Money Back Guarantee

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