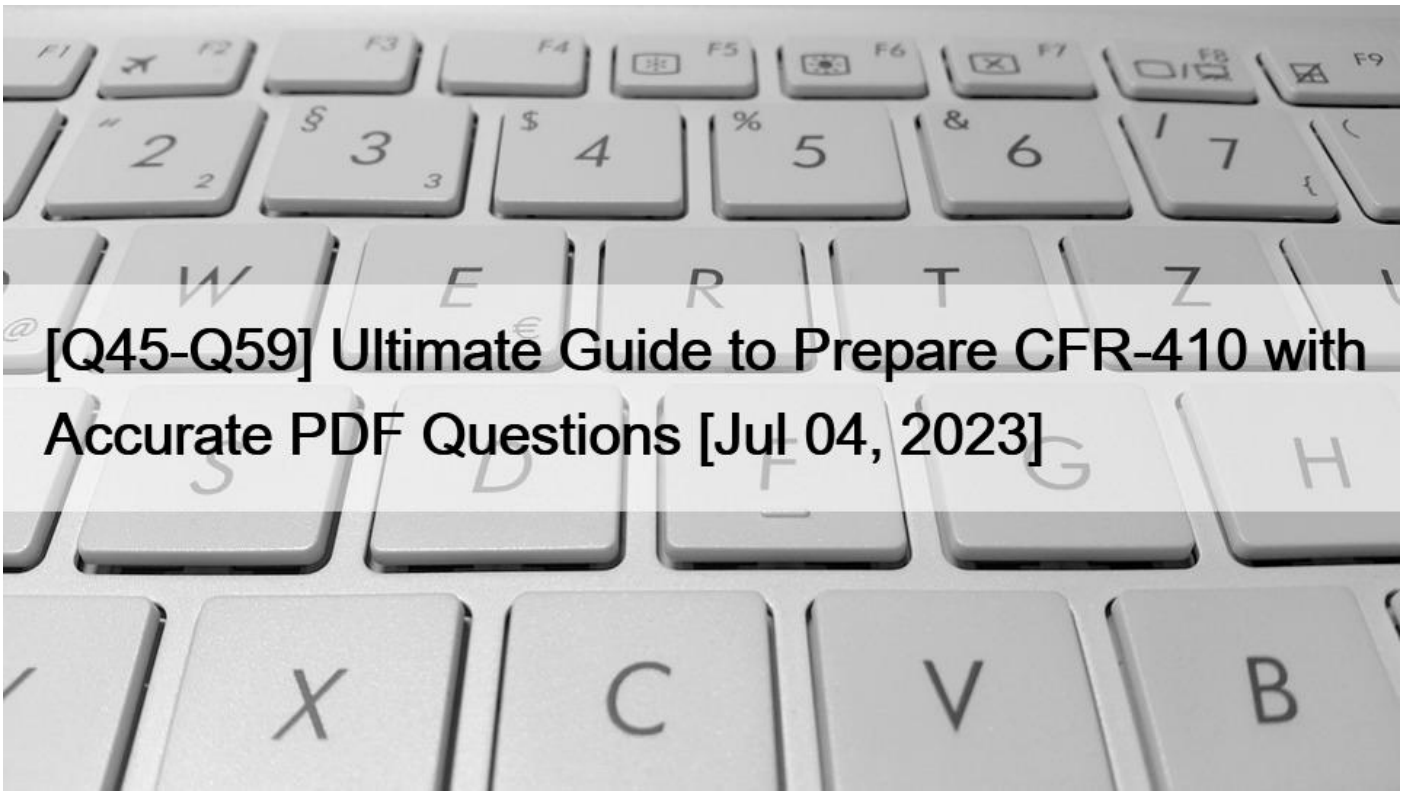
[Q45-Q59 Ultimate Guide to Prepare CFR-410 with Accurate PDF Questions [Jul 04, 2023



Ultimate Guide to Prepare CFR-410 with Accurate PDF Questions [Jul 04, 2023]
Pass CertNexus With DumpsMaterials Exam Dumps

The CFR-410: CyberSec First Responder exam is an essential certification for cybersecurity professionals. It validates the candidate's skills and knowledge in incident response, forensic analysis, and vulnerability management domains. CyberSec First Responder certification is vendor-neutral, globally recognized, and opens up various career opportunities for professionals. It is an excellent investment for cybersecurity professionals who want to advance their careers and stay relevant in the ever-evolving cybersecurity industry.

QUESTION 45

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?
* Intrusion prevention system (IPS)
* Intrusion detection system (IDS)
* Blacklisting
* Whitelisting

QUESTION 46

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?
* Data loss prevention (DLP)
* Firewall
* Web proxy
* File integrity monitoring

QUESTION 47

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?
* Internet Message Access Protocol (IMAP)
* Network Basic Input/Output System (NetBIOS)
* Database
* Network Time Protocol (NTP)

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?
* Cybercriminals
* Hacktivists
* State-sponsored hackers
* Cyberterrorist

QUESTION 49

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:

Tempchill.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?
* Taunt the user and then trigger a shutdown every 15 minutes.
* Taunt the user and then trigger a reboot every 15 minutes.
* Taunt the user and then trigger a shutdown every 900 minutes.
* Taunt the user and then trigger a reboot every 900 minutes.

QUESTION 50

Which of the following, when exposed together, constitutes PII? (Choose two.)
* Full name
* Birth date

* Account balance
* Marital status
* Employment status

QUESTION 51

In which of the following attack phases would an attacker use Shodan?
* Scanning
* Reconnaissance
* Gaining access
* Persistence

QUESTION 52

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?
* Identification
* Preparation
* Recovery
* Containment

QUESTION 53

An attacker intercepts a hash and compares it to pre-computed hashes to crack a password. Which of the following methods has been used?
* Password sniffing
* Brute force attack
* Rainbow tables
* Dictionary attack

QUESTION 54

Which of the following is susceptible to a cache poisoning attack?
* Domain Name System (DNS)
* Secure Shell (SSH)
* Hypertext Transfer Protocol Secure (HTTPS)
* Hypertext Transfer Protocol (HTTP)

QUESTION 55

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?
* Browser logs
* HTTP logs
* System logs
* Proxy logs

QUESTION 56

Organizations considered “covered entities” are required to adhere to which compliance requirement?
* Health Insurance Portability and Accountability Act of 1996 (HIPAA)
* Payment Card Industry Data Security Standard (PCI DSS)
* Sarbanes-Oxley Act (SOX)
* International Organization for Standardization (ISO) 27001

QUESTION 57

Detailed step-by-step instructions to follow during a security incident are considered:
* Policies
* Guidelines
* Procedures
* Standards

QUESTION 58

An unauthorized network scan may be detected by parsing network sniffer data for:
* IP traffic from a single IP address to multiple IP addresses.
* IP traffic from a single IP address to a single IP address.
* IP traffic from multiple IP addresses to a single IP address.
* IP traffic from multiple IP addresses to other networks.

QUESTION 59

Which of the following is a cybersecurity solution for insider threats to strengthen information protection?
* Web proxy
* Data loss prevention (DLP)
* Anti-malware
* Intrusion detection system (IDS)