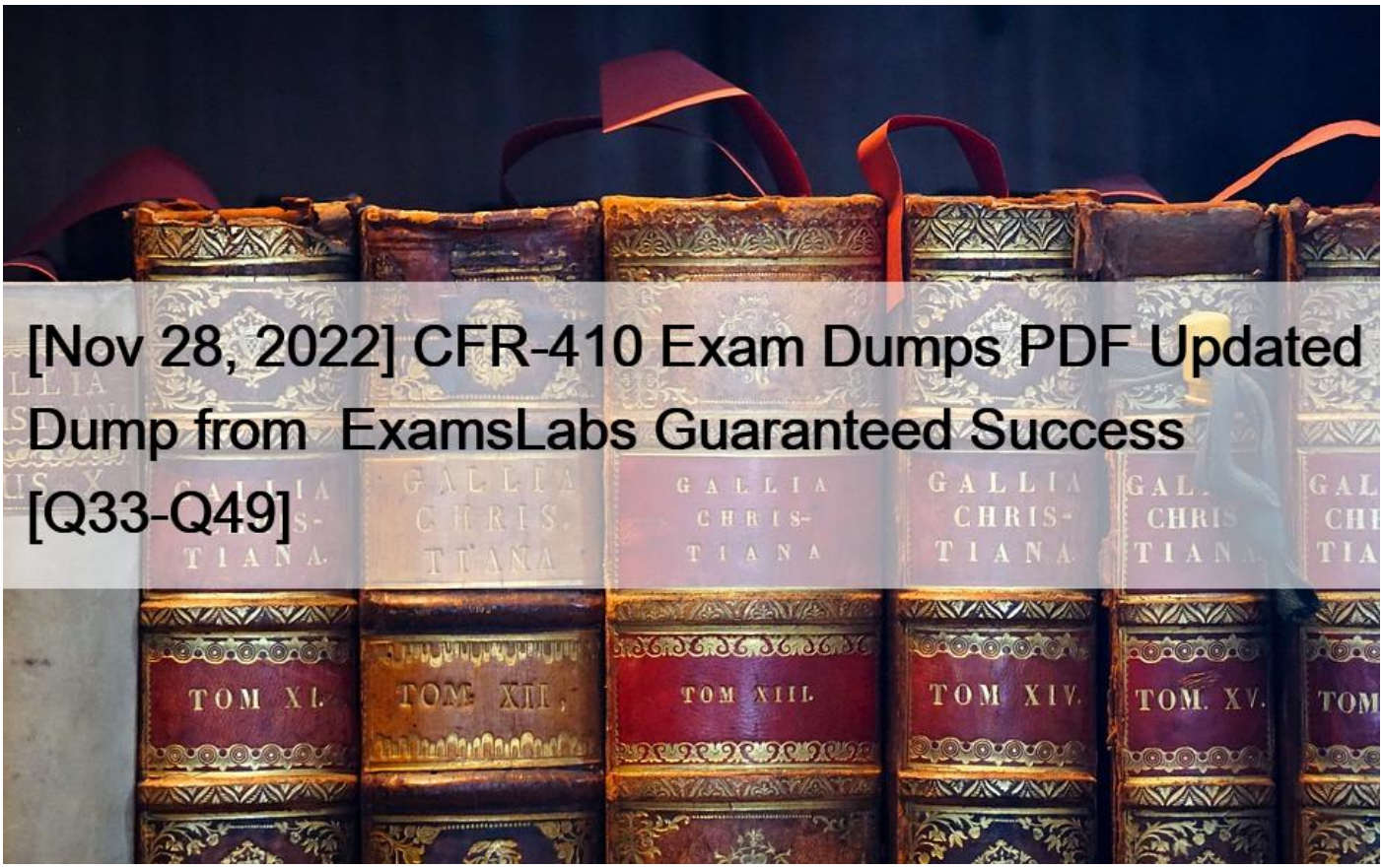
# [Nov 28, 2022 CFR-410 Exam Dumps PDF Updated Dump from ExamsLabs Guaranteed Success [Q33-Q49




[Nov 28, 2022] CFR-410 Exam Dumps PDF Updated Dump from ExamsLabs Guaranteed Success
Pass Your CertNexus Exam with CFR-410 Exam Dumps

## CertNexus CFR-410 Exam Syllabus Topics:

TopicDetailsTopic 1- Identify and conduct vulnerability assessment processes- Identify applicable compliance, standards, frameworks, and best practices for privacyTopic 2- Implement system security measures in accordance with established procedures- Determine tactics, techniques, and procedures (TTPs) of intrusion setsTopic 3- Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks- Correlate incident data and create reportsTopic 4- Establish relationships between internal teams and external groups like law enforcement agencies and vendors- Identify and evaluate vulnerabilities and threat actorsTopic 5- Provide advice and input for disaster recovery, contingency- Implement specific cybersecurity countermeasures for systems and applications

**NO.33** 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.)

* Web proxy

* Network monitoring system
* Data loss prevention (DLP)
* Anti-malware
* Network Address Translation (NAT)

**NO.34** 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?
* # tcpdump -i eth0 host 88.143.12.123
* # tcpdump -i eth0 dst 88.143.12.123
* # tcpdump -i eth0 host 192.168.10.121
* # tcpdump -i eth0 src 88.143.12.123

**NO.35** Which of the following enables security personnel to have the BEST security incident recovery practices?
* Crisis communication plan
* Disaster recovery plan
* Occupant emergency plan
* Incident response plan

**NO.36** 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?
* Logs should be synchronized to their local time zone.
* Logs should be synchronized to a common, predefined time source.
* Logs should contain the username of the user performing the action.
* Logs should include the physical location of the action performed.

Section: (none)

Explanation

**NO.37** An incident responder was asked to analyze malicious traffic. Which of the following tools would be BEST for this?
* Hex editor
* tcpdump
* Wireshark
* Snort

**NO.38** An administrator investigating intermittent network communication problems has identified an excessive amount of traffic from an external-facing host to an unknown location on the Internet. Which of the following BEST describes what is occurring?
* The network is experiencing a denial of service (DoS) attack.
* A malicious user is exporting sensitive data.
* Rogue hardware has been installed.
* An administrator has misconfigured a web proxy.

**NO.39** 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?
* Update the latest proxy access list
* Monitor the organization’s network for suspicious traffic
* Monitor the organization’s sensitive databases
* Update access control list (ACL) rules for network devices

**NO.40** 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?
* iperf, traceroute, whois, ls, chown, cat
* iperf, wget, traceroute, dc3dd, ls, whois
* lsof, chmod, nano, whois, chown, ls
* lsof, ifconfig, who, ps, ls, tcpdump

**NO.41** 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.)
* Disk duplicator
* EnCase
* dd
* Forensic Toolkit (FTK)
* Write blocker

**NO.42** During a malware-driven distributed denial of service attack, a security researcher found excessive requests to a name server referring to the same domain name and host name encoded in hexadecimal. The malware author used which type of command and control?
* Internet Relay Chat (IRC)
* Dnscat2
* Custom channel
* File Transfer Protocol (FTP)

**NO.43** Which of the following, when exposed together, constitutes PII? (Choose two.)
* Full name
* Birth date
* Account balance
* Marital status
* Employment status

**NO.44** Which of the following methods are used by attackers to find new ransomware victims? (Choose two.)
* Web crawling
* Distributed denial of service (DDoS) attack
* Password guessing
* Phishing
* Brute force attack

**NO.45** 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.)
* Providing a briefing to management
* Updating policies and procedures
* Training staff for future incidents
* Investigating responsible staff
* Drafting a recovery plan for the incident

**NO.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

**NO.47** A security analyst is required to collect detailed network traffic on a virtual machine. Which of the following tools could the analyst use?
* nbtstat
* WinDump
* fport
* netstat

**NO.48** 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?
* Backdoor
* Rootkit
* Time bomb
* Login bomb

**NO.49** Which of the following are common areas of vulnerabilities in a network switch? (Choose two.)
* Default port state
* Default credentials
* Default protocols
* Default encryption
* Default IP address

**New Real CFR-410 Exam Dumps Questions:**
https://www.examslabs.com/CertNexus/CertNexus-Certification/best-CFR-410-exam-dumps.html]