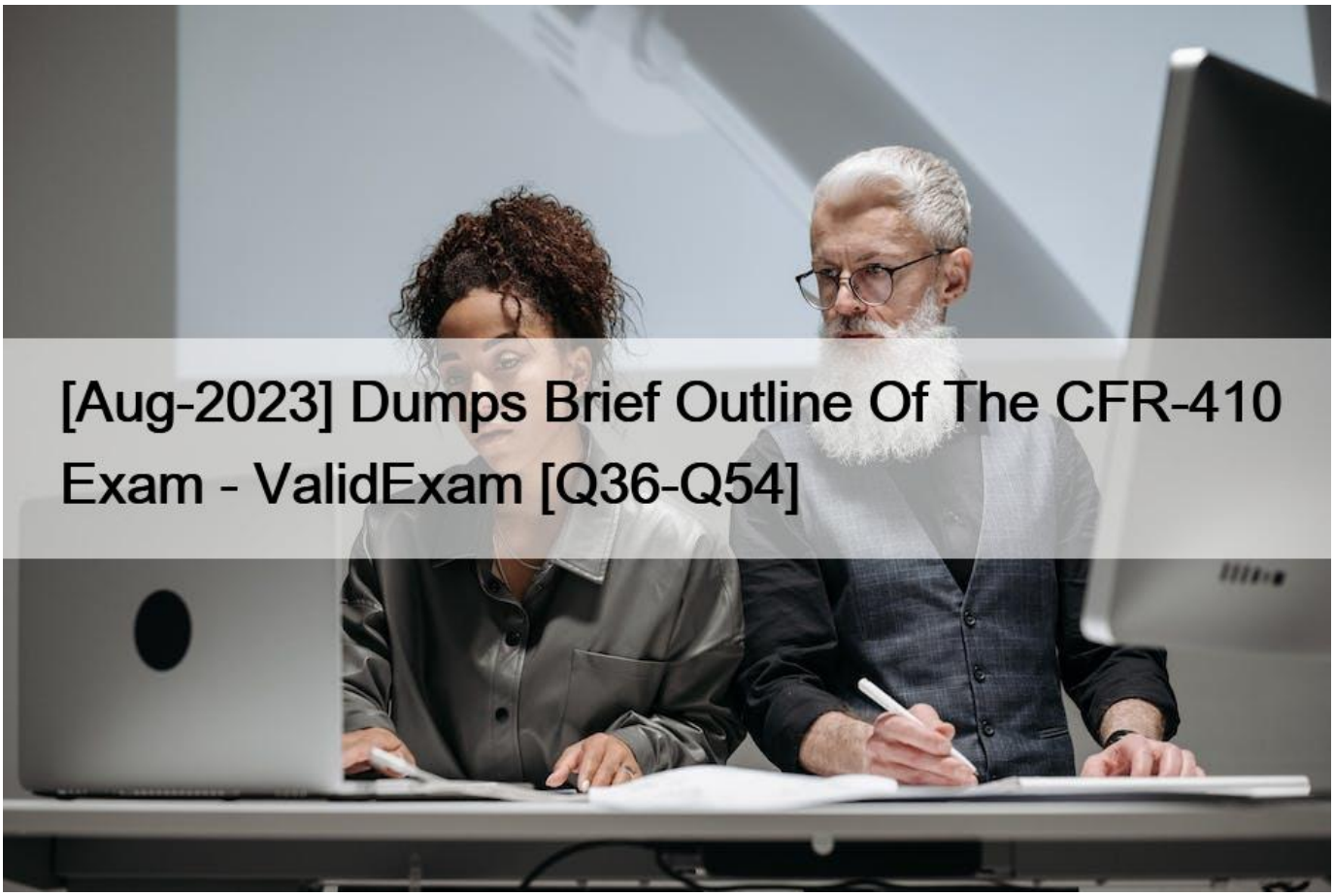
[Aug-2023 Dumps Brief Outline Of The CFR-410 Exam - ValidExam [Q36-Q54



[Aug-2023] Dumps Brief Outline Of The CFR-410 Exam - ValidExam
CFR-410 Training & Certification Get Latest CertNexus Certification

QUESTION 36

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

QUESTION 37

Which of the following does the command nmap -open 10.10.10.3 do?
* Execute a scan on a single host, returning only open ports.
* Execute a scan on a subnet, returning detailed information on open ports.
* Execute a scan on a subnet, returning all hosts with open ports.

* Execute a scan on a single host, returning open services.

QUESTION 38

A security professional discovers a new ransomware strain that disables antivirus on the endpoint during an infection. Which location would be the BEST place for the security professional to find technical information about this malware?
* Threat intelligence feeds
* Computer emergency response team (CERT) press releases
* Vulnerability databases
* Social network sites

QUESTION 39

Malicious code designed to execute in concurrence with a particular event is BEST defined as which of the following?
* Logic bomb
* Rootkit
* Trojan
* Backdoor

QUESTION 40

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?
* tr -d
* uniq -c
* wc -m
* grep -c

QUESTION 41

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.

QUESTION 42

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?
* grep 20151124 security_log | grep -c “login failure”
* grep 20150124 security_log | grep “login_failure”
* grep 20151124 security_log | grep “login”
* grep 20151124 security_log | grep -c “login”

QUESTION 43

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?
* ls
* lsof
* ps
* netstat

QUESTION 44

Which of the following is the GREATEST risk of having security information and event management (SIEM) collect computer names with older log entries?
* There may be duplicate computer names on the network.
* The computer name may not be admissible evidence in court.
* Domain Name System (DNS) records may have changed since the log was created.
* There may be field name duplication when combining log files.

QUESTION 45

If a hacker is attempting to alter or delete system audit logs, in which of the following attack phases is the hacker involved?
* Covering tracks
* Expanding access
* Gaining persistence
* Performing reconnaissance

QUESTION 46

Nmap is a tool most commonly used to:
* Map a route for war-driving
* Determine who is logged onto a host
* Perform network and port scanning
* Scan web applications

QUESTION 47

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 48

After successfully enumerating the target, the hacker determines that the victim is using a firewall. Which of the following techniques would allow the hacker to bypass the intrusion prevention system (IPS)?
* Stealth scanning
* Xmas scanning
* FINS scanning
* Port scanning

QUESTION 49

Which asset would be the MOST desirable for a financially motivated attacker to obtain from a health insurance company?
* Transaction logs
* Intellectual property
* PII/PHI
* Network architecture

QUESTION 50

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 51

Which of the following would MOST likely make a Windows workstation on a corporate network vulnerable to remote exploitation?
* Disabling Windows Updates
* Disabling Windows Firewall
* Enabling Remote Registry
* Enabling Remote Desktop

QUESTION 52

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)

QUESTION 53

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 54

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?
* ps -ef | grep armageddon
* top | grep armageddon
* wmic process list brief | find “armageddon.exe”

* wmic startup list full | find “armageddon.exe”

Certification Training for CFR-410 Exam Dumps Test Engine: https://www.validexam.com/CFR-410-latest-dumps.html]