



CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 2

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?

- A. The network is experiencing a denial of service (DoS) attack.
- B. A malicious user is exporting sensitive data.
- C. Rogue hardware has been installed.
- D. An administrator has misconfigured a web proxy.

Answer: B

NEW QUESTION 3

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?

- A. Threat intelligence feeds
- B. Computer emergency response team (CERT) press releases
- C. Vulnerability databases
- D. Social network sites

Answer: A

NEW QUESTION 4

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 5

During which of the following attack phases might a request sent to port 1433 over a whole company network be seen within a log?

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

Answer: B

NEW QUESTION 6

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 7

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 8

A government organization responsible for critical infrastructure is being attacked and files on the server been deleted. Which of the following are the most immediate communications that should be made regarding the incident? (Choose two.)

- A. Notifying law enforcement
- B. Notifying the media
- C. Notifying a national compute emergency response team (CERT) or cybersecurity incident response team (CSIRT)
- D. Notifying the relevant vendor
- E. Notifying a mitigation expert

Answer: CE

NEW QUESTION 9

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 10

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 10

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 11

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 13

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 15

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 20

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 24

An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/ screen) in numerical order?

- A. cat | tac
- B. more
- C. sort –n
- D. less

Answer: C

NEW QUESTION 29

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 31

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 32

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 34

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 38

Which of the following is susceptible to a cache poisoning attack?

- A. Domain Name System (DNS)
- B. Secure Shell (SSH)
- C. Hypertext Transfer Protocol Secure (HTTPS)
- D. Hypertext Transfer Protocol (HTTP)

Answer: A

NEW QUESTION 43

An incident responder was asked to analyze malicious traffic. Which of the following tools would be BEST for this?

- A. Hex editor
- B. tcpdump
- C. Wireshark
- D. Snort

Answer: C

NEW QUESTION 46

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 47

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 48

.....

Relate Links

100% Pass Your CFR-410 Exam with Exam Bible Prep Materials

<https://www.exambible.com/CFR-410-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>