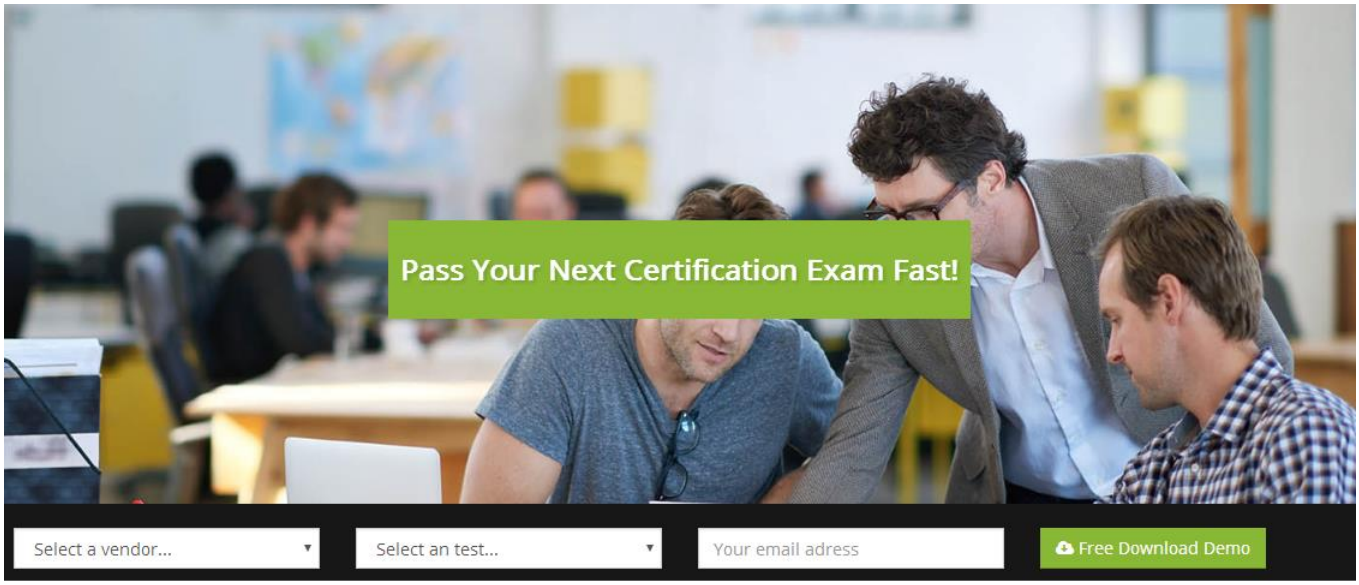
ITPassLeader



Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.itpassleader.com

High-praise Exam Dumps Questions grant you success by high pass rate - ITPassLeader

Exam : **CFR-210**

Title : Logical Operations CyberSec First Responder

Vendor : Logical Operations

Version : DEMO

NO.1 A malicious attacker has compromised a database by implementing a Python-based script that will automatically establish an SSH connection daily between the hours of 2:00am and 5:00am.
Which of the following is the MOST common motive for the attack vector that was used?
A. Pivoting
B. Persistence/maintaining access
C. Exfiltration
D. Lateral movement
Answer: D

NO.2 An incident responder notices many entries in an apache access log file that contain semicolons.
Which of the following attacks is MOST likely being attempted?
A. SQL injection
B. Remote file inclusion
C. Account brute force
D. Cross-site scripting
Answer: A

NO.3 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. Cyber incident response plan
Answer: D

NO.4 A suspicious laptop is found in a datacenter. The laptop is on and processing data, although there is no application open on the screen.
Which of the following BEST describes a Windows tool and technique that an investigator should use to analyze the laptop's RAM for working applications?
A. Net start and Network analysis
B. Regedit and Registry analysis
C. Task manager and Application analysis
D. Volatility and Memory analysis
Answer: B

NO.5 A DMZ web server has been compromised. During the log review, the incident responder wants to parse all common internal Class A addresses from the log.
Which of the following commands should the responder use to accomplish this?
A. grep -x"(10.[0-9]+.[0-9]+.[0-9]+)" etc/rc.d/apache2/access.log I output.txt
B. grep -x"(192.168.[0.9]+[0-9])" bin/apache2/access.log I output.txt
C. grep -v"(10.[0-9]+.[0-9]+.[0-9]+)" /var/log/apache2/access.log > output.txt
D. grep -v"(192.168.[0.9]+[0-9]+)" /var/log/apache2/access.log > output.txt
Answer: C

NO.6 A high-level government official uses anonymous bank accounts to transfer a requested amount of funds to individuals in another country.

These individuals are known for defacing government websites and exfiltrating sensitive data.
Which of the following BEST describes the involved threat actors?
A. State-sponsored hackers
B. Gray hat hackers
C. Hacktivists
D. Cyber terrorists
Answer: D

NO.7 Which of the following technologies is used as mitigation to XSS attacks?
A. Intrusion prevention
B. Proxy filtering
C. Web application firewall
D. Intrusion detection
Answer: C

NO.8 Which of the following is the reason that out-of-band communication is used during a security incident?
A. The SMTP server may be compromised.
B. The incident response systems may be busy.
C. Other communication methods are unreliable.
D. An attacker could be monitoring network traffic.
Answer: C

NO.9 Which of the following are legally compliant forensics applications that will detect ADS or a file with an incorrect file extension? (Choose two.)
A. Regedit
B. EnCase
C. dd
D. FTK
E. Procmon
Answer: A,C

NO.10 Which of the following describes pivoting?
A. Copying captured data to a hacker's system
B. Performing IP packet inspection
C. Generating excessive network traffic
D. Accessing another system from a compromised system
Answer: D