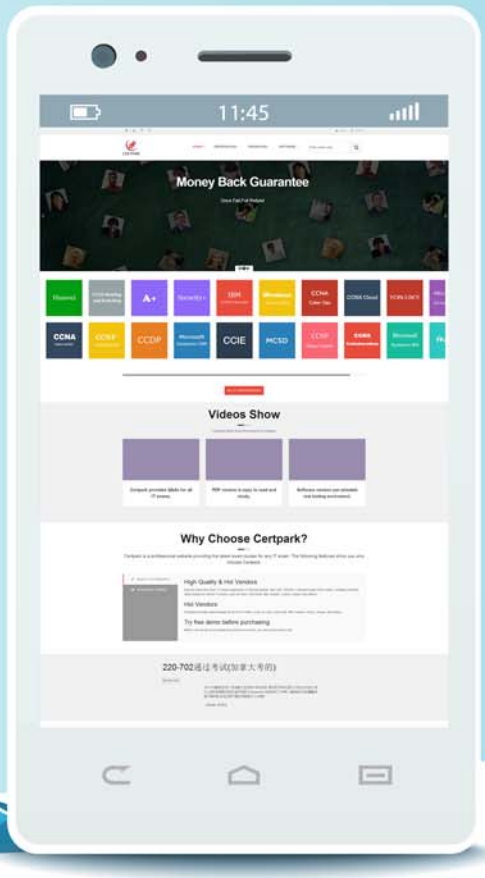
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **CFR-210**

Title : Logical Operations
CyberSec First Responder

Version : Demo

1.An attacker performs reconnaissance on a Chief Executive Officer (CEO) using publicity available resources to gain access to the CEO's office. The attacker was in the CEO's office for less than five minutes, and the attack left no traces in any logs, nor was there any readily identifiable cause for the exploit. The attacker in then able to use numerous credentials belonging to the CEO to conduct avariety of further attacks.
Which of the following types of exploit is described?
A. Pivoting
B. Malicious linking
C. Whaling
D. Keylogging
Answer: C

2.Which of the following is an automated password cracking technique that uses a combination of upper and lower case letters, 0-9 numbers, and special characters?
A. Dictionary attack
B. Password guessing
C. Brute force attack
D. Rainbow tables
Answer: C

3.A zero-day vulnerability is discovered on a company's network. The security analyst conducts a log review, schedules an immediate vulnerability scan, and quarantines the infected system, but cannot determine the root cause of the vulnerability.
Which of the following is a source of information that can be used to identify the cause of the vulnerability?
A. www.virustotal.com
B. Security RSS feeds
C. Security software websites
D. Government websites
Answer: C

4.The Chief Information Officer (CIO) of a company asks the incident responder to update the risk management plan.
Which of the following methods can BEST help the incident responder identify therisks that require in-depth analysis?
A. Qualitative analysis
B. Targeted risk analysis
C. Non-targeted risk analysis
D. Quantitative analysis
Answer: D

5.A security analyst for a financial services firm is monitoring blogs and reads about a zero-day vulnerability being exploited by a little-known group of hackers. The analyst wishes to independently validate and corroborate the blog's posting.

Which of the following sources of information will provide the MOST credible supporting threat intelligence in this situation?

A. Similar cybersecurity blogs

B. Threat intelligence sharing groups

C. Computer emergency response team press release

D. Internet searches on zero-day exploits

Answer: C