KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **ITS-110**

Title : Certified Internet of Things Security Practitioner(CIoTSP)

Version : DEMO

1.An IoT manufacturer wants to ensure that their web-enabled cameras are secured against brute force password attacks.
Which of the following technologies or protocols could they implement?
A. URL filtering policies
B. Account lockout policies
C. Software encryption
D. Buffer overflow prevention
Answer: B

2.Which of the following methods or technologies is most likely to be used in order to mitigate brute force attacks?
A. Account lockout policy
B. Automated security logging
C. Role-based access control
D. Secure password recovery
Answer: A
Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/account-lockout-policy#:~:text=Account%20lockout%20policies%20are%20used,twice%2C%20but%20not %20numerous%20times

3.An IoT service collects massive amounts of data and the developer is encrypting the data, forcing administrative users to authenticate and be authorized. The data is being disposed of properly and on a timely basis. However, which of the following countermeasures is the developer most likely overlooking?
A. That private data can never be fully destroyed.
B. The best practice to only collect critical data and nothing more.
C. That data isn't valuable unless it's used as evidence for crime committed.
D. That data is only valuable as perceived by the beholder.
Answer: B

4.Accompany collects and stores sensitive data from thousands of IoT devices. The company's IoT security administrator is concerned about attacks that compromise confidentiality.
Which of the following attacks is the security administrator concerned about? (Choose two.)
A. Salami
B. Aggregation
C. Data diddling
D. Denial of Service (DoS)
E. Inference
Answer: B,E

5.A DevOps engineer wants to provide secure network services to an IoT/cloud solution.
Which of the following countermeasures should be implemented to mitigate network attacks that can render a network useless?
A. Network firewall

B. Denial of Service (DoS)/Distributed Denial of Service (DDoS) mitigation
C. Web application firewall (WAF)
D. Deep Packet Inspection (DPI)
Answer: B
Explanation:
Reference: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/#:~:text=A%20distributed%20denial%2Dof%2Dservice,a%20flood%20of%20Internet %20traffic