CertNexus

ITS-110
Certified Internet of Things Security Practitioner (CIoTSP)

Latest Version: 6.0

Question: 1

An IoT systems administrator wants to ensure that all data stored on remote IoT gateways is unreadable. Which of the following technologies is the administrator most likely to implement?

A. Secure Hypertext Transmission Protocol (HTTPS)
B. Internet Protocol Security (IPSec)
C. Triple Data Encryption Standard (3DES)
D. Message Digest 5 (MD5)

Answer: B

Question: 2

In designing the campus of an IoT device manufacturer, a security consultant was hired to recommend best practices for deterring criminal behavior. Which of the following approaches would he have used to meet his client's needs?

A. Crime Prevention Through Environmental Design (CPTED)
B. British Standard 7799 part 3 (BS 7799-3)
C. International Organization for Standardization 17799 (ISO 17799)
D. National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Answer: A

Question: 3

An IoT security administrator is concerned that someone could physically connect to his network and scan for vulnerable devices. Which of the following solutions should he install to prevent this kind of attack?

A. Media Access Control (MAC)
B. Network Access Control (NAC)
C. Host Intrusion Detection System (HIDS)
D. Network Intrusion Detection System (NIDS)

Answer: D

Question: 4

Which of the following is one way to implement countermeasures on an IoT gateway to ensure physical security?

A. Add tamper detection to the enclosure
B. Limit physical access to ports when possible
C. Allow quick administrator access for mitigation
D. Implement features in software instead of hardware

Answer: B

Question: 5

Which of the following methods or technologies is most likely to be used to protect an IoT portal against protocol fuzzing?

A. Secure Hypertext Transfer Protocol (HTTPS)
B. Public Key Infrastructure (PKI)
C. Next-Generation Firewall (NGFW)
D. Hash-based Message Authentication Code (HMAC)

Answer: C

Question: 6

A manufacturer wants to ensure that user account information is isolated from physical attacks by storing credentials off-device. Which of the following methods or technologies best satisfies this requirement?

A. Role-Based Access Control (RBAC)
B. Password Authentication Protocol (PAP)
C. Remote Authentication Dial-In User Service (RADIUS)

D. Border Gateway Protocol (BGP)

Answer: C

Question: 7

An IoT device which allows unprotected shell access via console ports is most vulnerable to which of the following risks?

A. Directory harvesting
B. Rainbow table attacks
C. Malware installation
D. Buffer overflow

Answer: C

Question: 8

An embedded developer is about to release an IoT gateway. Which of the following precautions must be taken to minimize attacks due to physical access?

A. Allow access only to the software
B. Remove all unneeded physical ports
C. Install a firewall on network ports
D. Allow easy access to components

Answer: B

Question: 9

You work for an IoT software-as-a-service (SaaS) provider. Your boss has asked you to research a way to effectively dispose of stored sensitive customer dat

a. Which of the following methods should you recommend to your boss?
A. Crypto-shredding
B. Degaussing

C. Overwriting
D. Physical destruction

Answer: D

Question: 10

A user grants an IoT manufacturer consent to store personally identifiable information (PII). According to the General Data Protection Regulation (GDPR), when is an organization required to delete this data?

A. Within ninety days after collection, unless required for a legal proceeding
B. Within thirty days of a user's written request
C. Within seven days of being transferred to secure, long-term storage
D. Within sixty days after collection, unless encrypted

Answer: B