DUMPSARENA

Certified Internet of Things Security Practitioner (CIoTSP)

CertNexus ITS-110

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Passwords should be stored…

A. For no more than 30 days.

B. Only in cleartext.

C. As a hash value.

D. Inside a digital certificate.

ANSWER: C

QUESTION NO: 2

The network administrator for an organization has read several recent articles stating that replay attacks are on the rise. Which of the following secure protocols could the administrator implement to prevent replay attacks via remote workers' VPNs? (Choose three.)

A. Internet Protocol Security (IPSec)

B. Enhanced Interior Gateway Routing Protocol (EIGRP)

C. Password Authentication Protocol (PAP)

D. Challenge Handshake Authentication Protocol (CHAP)

E. Simple Network Management Protocol (SNMP)

F. Layer 2 Tunneling Protocol (L2TP)

G. Interior Gateway Routing Protocol (IGRP)

ANSWER: A D F

QUESTION NO: 3

An IoT security administrator wishes to mitigate the risk of falling victim to Distributed Denial of Service (DDoS) attacks. Which of the following mitigation strategies should the security administrator implement? (Choose two.)

A. Block all inbound packets with an internal source IP address

B. Block all inbound packets originating from service ports

C. Enable unused Transmission Control Protocol (TCP) service ports in order to create a honeypot

D. Block the use of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) through his perimeter firewall

E. Require the use of X.509 digital certificates for all incoming requests

ANSWER: D E

QUESTION NO: 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

QUESTION NO: 5

A hacker is sniffing network traffic with plans to intercept user credentials and then use them to log into remote websites. Which of the following attacks could the hacker be attempting? (Choose two.)

A. Masquerading

B. Brute force

C. Directory traversal

D. Session replay

E. Spear phishing

ANSWER: B E

QUESTION NO: 6

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 NO: 7

Which of the following tools or techniques is used by software developers to maintain code, but also used by hackers to maintain control of a compromised system?

A. Disassembler

B. Backdoor

C. Debugger

D. Stack pointer

ANSWER: B

QUESTION NO: 8

You made an online purchase of a smart watch from a software as a service (SaaS) vendor, and filled out an extensive profile that will help you track several fitness variables. The vendor will provide you with customized health insights based on your profile. With which of the following regulations should the company be compliant? (Choose three.)

A. Gramm-Leach-Bliley Act (GLBA)

B. Payment Card Industry Data Security Standard (PCI-DSS)

C. Federal Information Security Management Act (FISMA)

D. Sarbanes-Oxley (SOX)

E. Health Insurance Portability and Accountability Act (HIPAA)

F. Family Educational Rights and Privacy Act (FERPA)

G. Federal Energy Regulatory Commission (FERC)

ANSWER: B E F

QUESTION NO: 9

A hacker enters credentials into a web login page and observes the server's responses. Which of the following attacks is the hacker attempting?

A. Account enumeration

B. Directory traversal

C. Buffer overflow

D. Spear phishing

ANSWER: A

QUESTION NO: 10

An IoT gateway will be brokering data on numerous northbound and southbound interfaces. A security practitioner has the data encrypted while stored on the gateway and encrypted while transmitted across the network. Should this person be concerned with privacy while the data is in use?

A. Yes, because the hash wouldn't protect the integrity of the data.

B. Yes, because the data is vulnerable during processing.

C. No, since the data is already encrypted while at rest and while in motion.

D. No, because the data is inside the CPU's secure region while being used.

ANSWER: B