DUMPSQUEEN

Certified Internet of Things Security Practitioner (CIoTSP)

CertNexus ITS-110

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

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: 2

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: 3

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 NO: 4

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: 5

An IoT security architect needs to secure data in motion. Which of the following is a common vulnerability used to exploit unsecure data in motion?

A. External flash access

B. Misconfigured Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

C. Databases and datastores

D. Lack of memory space isolation

ANSWER: B

QUESTION NO: 6

Requiring randomly generated tokens for each connection from an IoT device to the cloud can help mitigate which of the following types of attacks?

A. Malformed URL injection

B. Buffer overflow

C. SSL certificate hijacking

D. Session replay

ANSWER: D

QUESTION NO: 7

A hacker wants to discover login names that may exist on a website. Which of the following responses to the login and password entries would aid in the discovery? (Choose two.)

A. Your login attempt was unsuccessful

B. Invalid password

C. That user does not exist

D. The username and/or password are incorrect

E. Incorrect email/password combination

ANSWER: A C

QUESTION NO: 8

An OT security practitioner wants to implement two-factor authentication (2FA). Which of the following is the least secure method to use for implementation?

A. Out-of-band authentication (OOBA)

B. 2FA over Short Message Service (SMS)

C. Authenticator Apps for smartphones

D. Fast Identity Online (FIDO) Universal 2nd Factor (U2F) USB key

ANSWER: B

QUESTION NO: 9

An IoT system administrator discovers that end users are able to access administrative features on the company's IoT management portal. Which of the following actions should the administrator take to address this issue?

A. Implement password complexity policies

B. Implement granular role-based access

C. Implement account lockout policies

D. Implement digitally signed firmware updates

ANSWER: B

QUESTION NO: 10

An IoT security administrator is concerned about an external attacker using the internal device management local area network (LAN) to compromise his IoT devices. Which of the following countermeasures should the security administrator implement? (Choose three.)

A. Require the use of Password Authentication Protocol (PAP)

B. Create a separate management virtual LAN (VLAN)

C. Ensure that all IoT management servers are running antivirus software

D. Implement 802.1X for authentication

E. Ensure that the Time To Live (TTL) flag for outgoing packets is set to 1

F. Only allow outbound traffic from the management LAN

G. Ensure that all administrators access the management server at specific times

ANSWER: B D G