Free Questions for ITS-110 by certscare

Shared by Benjamin on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A network administrator is looking to implement best practices for the organization's password policy. Which of the following elements should the administrator include?

Options:

A- Maximum length restriction

B- Password history checks

C- No use of special characters

D- No password expiration

Answer:

B

Question 2

Question Type: MultipleChoice

In order to gain access to a user dashboard via an online portal, an end user must provide their username, a PIN, and a software token code. This process is known as:

Options:

A- Type 1 authentication

B- Type 2 authentication

C- Two-factor authentication

D- Biometric authentication

Answer:

C

Question 3

Question Type: MultipleChoice

Web forms that contain unvalidated fields are vulnerable to which of the following attacks? (Choose two.)

Options:

A- Smurf

B- Ping of death

C- Cross-Site Scripting (XSS)

D- Man-in-the-middle (MITM)

E- SQL Injection (SQLi)

Answer:

C, E

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- URL filtering policies

B- Account lockout policies

C- Software encryption

D- Buffer overflow prevention

Answer:

B

Question 5

Question Type: MultipleChoice

Which of the following attacks would most likely be used to discover users, printers, and other objects within a network?

Options:

A- Distributed Denial of Service (DDoS)

B- SYN flood

C- LDAP Injection

D- Denial of Service (DoS)

Answer:

C

Question 6

Question Type: **MultipleChoice**

A web administrator is concerned about injection attacks. Which of the following mitigation techniques should the web administrator implement?

Options:

A- Configure single sign-on (SSO)

B- Parameter validation

C- Require strong passwords

D- Require two-factor authentication (2FA)

Answer:

B

Question 7

Question Type: MultipleChoice

An IoT developer wants to ensure that data collected from a remotely deployed power station monitoring system is transferred securely to the cloud. Which of the following technologies should the developer consider?

Options:

A- Secure/Multipurpose Internet Mail Extensions (S/MIME)

B- Message-digest 5 (MD5)

C- Blowfish

D- Transport Layer Security (TLS)

Answer:

D

Question 8

Question Type: MultipleChoice

An IoT system administrator discovers that unauthorized users are able to log onto and access data on remote IoT monitoring devices. What should the system administrator do on the remote devices in order to address this issue?

Options:

A- Encrypt all locally stored data

B- Ensure all firmware updates have been applied

C- Change default passwords

D- Implement URL filtering

Answer:

C

Question 9

Question Type: MultipleChoice

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.)

Options:

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 10

Question Type: **MultipleChoice**

An IoT systems integrator has a very old IoT gateway that doesn't offer many security features besides viewing a system configuration page via browser over HTTPS. The systems integrator can't get their modern browser to bring up the page due to a cipher suite mismatch. Which of the following must the integrator perform before the configuration page can be viewed?

Options:

A- Upgrade the browser, as modern browsers have stopped allowing connections to hosts that use only outdated cipher suites.

B- Downgrade the browser, as modern browsers have stopped allowing connections to hosts that use only outdated cipher suites.

C- Upgrade the browser, as older browsers have stopped allowing connections to hosts that use only outdated cipher suites.

D- Downgrade the browser, as modern browsers have continued allowing connections to hosts that use only outdated cipher suites.

Answer:

C

Question 11

Question Type: MultipleChoice

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?

Options:

A- Implement password complexity policies

B- Implement granular role-based access

C- Implement account lockout policies

D- Implement digitally signed firmware updates

Answer:

B