

Exam Report: 15.2.3 Practice Questions

Date: 5/26/2020 7:26:26 pm
Time Spent: 0:44

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%



Passing Score: 80%

View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Kathy doesn't want to purchase a digital certificate from a public certificate authority, but needs to establish a PKI in her local network. Which of the follow actions should she take?

- ☐ Request a certificate from GoDaddy.
- ➔ ☒ Create a local CA and generate a self-signed certificate.
- ☐ Ensure all HTTP traffic uses port 443.
- ☐ Enable synchronous encryption in her network.

Explanation

Kathy can implement a local PKI by first creating a local CA and generating a self-signed certificate.

Synchronous encryption is not used in a PKI.

Without a certificate, HTTP traffic on port 443 can't be encrypted.

GoDaddy is a public certificate authority.

References

TestOut Ethical Hacker Pro - 15.2 Public Key Infrastructure
[e_pki_eh1.exam.xml Q_PKI_CERT_SIGN_01_EH1]

▼ Question 2: Incorrect

Which of the following is an entity that accepts and validates information contained within a request for a certificate?

- ☐ Certificate management system
- ☐ Validation authority
- ☒ Certificate authority
- ➔ ☐ Registration authority

Explanation

A registration authority (RA) can be used in large enterprise environments to offload client enrollment request processing by handling client verification prior to certificates issue. The RA accepts registrations, validates identity, and approves or denies certificate requests.

A certificate authority (CA) is an entity trusted to issue, store, and revoke digital certificates. Often, the role of a certificate authority is combined with that of RA. But, technically speaking, a CA is the computer that issues the certificate.

A validation authority verifies the validity of a digital certificate.

A certificate management system is software that operates in a PKI environment to create private key/public key pairs and distribute digital certificates.

References

TestOut Ethical Hacker Pro - 15.2 Public Key Infrastructure
[e_pki_eh1.exam.xml Q_PKI_COMPONENT_01_EH1]

▼ Question 3: Incorrect

Which of the following describes a PKI?

- ☐ A protocol that defines secure key exchange.
- ➡ ☐ A security architecture that ensures data connections between entities are validated and secure.
- ☒ An algorithm for encrypting and decrypting data.
- ☐ Software that manages an organization's certificates.

Explanation

A public key infrastructure (PKI) is a security architecture that ensures data connections between entities are validated and secure.

A certificate management system is software that manages an organization's certificates.

PKI is not an algorithm for encrypting and decrypting data.

Secure exchange of keys is provided by many protocols, including RSA, Diffie-Hellman, IKE, and KEA.

References

TestOut Ethical Hacker Pro - 15.2 Public Key Infrastructure
[e_pki_eh1.exam.xml Q_PKI_COMPONENT_02_EH1]

▼ Question 4: Incorrect

Which of the following best describes a certificate authority (CA)?

- ➡ ☐ An entity that issues digital certificates.
- ☒ An entity that provides a service used to verify the validity of a digital certificate.
- ☐ An electronic password that allows a person or organization to exchange data securely over the Internet
- ☐ An entity in a PKI that verifies user requests for a digital certificate.

Explanation

A certificate authority is an entity that issues digital certificates.

A registration authority is an entity in a PKI that verifies user requests for a digital certificate.

A verification authority is an entity that provides a service used to verify the validity of a digital certificate.

A digital certificate is an electronic password that allows a person or organization to securely exchange data over the internet.

References

TestOut Ethical Hacker Pro - 15.2 Public Key Infrastructure
[e_pki_eh1.exam.xml Q_PKI_COMPONENT_03_EH1]

▼ Question 5: Incorrect

Robert, an IT administrator, is working for a newly formed company. He needs a digital certificate to send and receive data securely in a Public Key Infrastructure (PKI). Which of the following requests should he submit?

- ☐ He must send identifying data and the encryption algorithm he will use with his certificate request to a certificate authority (CA).

- ➡ ☐ He must send identifying data with his certificate request to a registration authority (RA).
- ☐ He must send identifying data and a private key request to a validation authority (VA).
- ☒ He must send the MAC and IP addresses with his certificate to a root certificate authority (CA).

Explanation

The registration authority (RA) processes all requests for digital certificates. Registration authorities verify the identifying data before the request is forwarded to the certificate authority (CA) for certificate generation.

An encryption algorithm is not needed for a certificate request.

A validation authority (VA) does not accept certificate requests.

The MAC and IP addresses are not part of the identifying information needed by a registration authority or a certificate authority.

References

TestOut Ethical Hacker Pro - 15.2 Public Key Infrastructure
[e_pki_eh1.exam.xml Q_PKI_WORKS_01_EH1]