**Quiz -1**

**Your Answers:**

**Results for question 1.**

1

1 / 1 point

Which term ensures that a system operates as intended, free from both intentional and unintentional unauthorized manipulations?



Privacy

, Not Selected



Availability

, Not Selected



Data confidentiality

, Not Selected

Correct answer:



System integrity

**Results for question 2.**

2

0 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

True

Incorrect answer:

False

Correct Answer:True

**Results for question 3.**

3

1 / 1 point

Which U.S. federal institution focuses on standards, measurement science, and fostering technological advancements in the private sector?



ISO

, Not Selected



ITU-T

, Not Selected



ISOC

, Not Selected

Correct answer:



NIST

**Results for question 4.**

4

1 / 1 point

What ensures that users' identities are genuine and each input stems from a trusted source?



Confidentiality

, Not Selected

Correct answer:



Authenticity



Accountability

, Not Selected



Integrity

, Not Selected

**Results for question 5.**

5

1 / 1 point

A

Correct answer:

digital signature

 can either be data attached to, or a cryptographic transformation of a data unit, enabling the recipient to verify its source and integrity, and safeguarding against counterfeiting.

**Results for question 6.**

6

1 / 1 point

Which type of attacks are aimed at changing system resources or affecting their function?



Release of message content

, Not Selected



Passive

, Not Selected



Traffic analysis

, Not Selected

Correct answer:



Active

**Results for question 7.**

7

1 / 1 point

When designing a security mechanism or algorithm, is it essential to anticipate potential threats to it?

Correct answer:

True

False

**Results for question 8.**

8

0 / 1 point

Are pervasive security methods unrelated to any specific OSI security function or protocol tier?

True

Incorrect answer:

False

Correct Answer:True

**Results for question 9.**

9

1 / 1 point

Is a breach in confidentiality defined as the unauthorized alteration or elimination of data?

True

Correct answer:

False

**Results for question 10.**

10

0 / 1 point

In computer security, three main principles are confidentiality, availability, and

Incorrect answer:

Integrity

Correct Answer:integrity

.

The security goal requiring each entity's actions to be traceable solely to that entity is known as what?



Authenticity

, Not Selected



Integrity

, Not Selected

Correct answer:



Accountability



Privacy

, Not Selected

### Results for question 2.

2

0 / 1 point

Incorrect answer:

Encryption

Correct Answer:encipherment, encryption, cryptography

 involves the application of mathematical procedures to transform data into a scrambled format, which can then be recovered using specific algorithms and keys.

### Results for question 3.

3

1 / 1 point

Is a breach in confidentiality defined as the unauthorized alteration or elimination of data?

True

Correct answer:

False

### Results for question 4.

4

1 / 1 point

What refers to the act of stopping unauthorized resource utilization?



Authentication

, Not Selected

Correct answer:



Access control



Nonrepudiation

, Not Selected



Data confidentiality

, Not Selected

### Results for question 5.

5

1 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

Correct answer:

True

False

### Results for question 6.

6

0 / 1 point

A deliberate action, intending to bypass security measures and breach the system's security guidelines, is termed as

Incorrect answer:

malicious activity

Correct Answer:attack

.

### Results for question 7.

7

1 / 1 point

Besides replay, message modification, and denial of service, active attacks also include

Correct answer:

masquerade

 as a category.

### Results for question 8.

8

1 / 1 point

Is the purpose of data integrity to prevent unauthorized data exposure?

True

Correct answer:

False

### Results for question 9.

9

1 / 1 point

Which type of attacks are aimed at changing system resources or affecting their function?



Release of message content

, Not Selected



Passive

, Not Selected



Traffic analysis

, Not Selected

Correct answer:



Active

### Results for question 10.

10

1 / 1 point

Does data origin authentication shield against copying or altering data units?

True

Correct answer:

False

Did the advent of computers lead to an increased demand for tools to safeguard files and other stored data?

Correct answer:

True

False

### Results for question 2.

2

0 / 1 point

Within network security, the capacity to manage and restrict access to host systems via communication pathways is termed

Incorrect answer:

Network access control

Correct Answer:access control, Access Control

.

### Results for question 3.

3

1 / 1 point

Do users and system administrators often undervalue security investments until a breach happens?

Correct answer:

True

False

### Results for question 4.

4

0 / 1 point

Would you classify patient allergy details as data that has a medium priority for maintaining its accuracy?

Incorrect answer:

True

Correct Answer:False

False

### Results for question 5.

5

1 / 1 point

Which U.S. federal institution focuses on standards, measurement science, and fostering technological advancements in the private sector?



ISOC

, Not Selected

Correct answer:



NIST



ITU-T

, Not Selected



ISO

, Not Selected

### Results for question 6.

6

1 / 1 point

Is the purpose of data integrity to prevent unauthorized data exposure?

True

Correct answer:

False

### Results for question 7.

7

1 / 1 point

When designing a security mechanism or algorithm, is it essential to anticipate potential threats to it?

Correct answer:

True

False

### Results for question 8.

8

1 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

Correct answer:

True

False

### Results for question 9.

9

1 / 1 point

Correct answer:

encryption

 involves the application of mathematical procedures to transform data into a scrambled format, which can then be recovered using specific algorithms and keys.

### Results for question 10.

10

1 / 1 point

A deliberate action, intending to bypass security measures and breach the system's security guidelines, is termed as

Correct answer:

attack

Quiz -2:

1

1 / 1 point

The primary limitation of 3DES is its slow operation in software.

Correct answer:

True

False

**Results for question 2.**

2

1 / 1 point

A device that uses a seemingly random source, often labeled an entropy source, as its input is a \_\_\_\_\_\_\_\_.



PSRN

, Not Selected



PRF

, Not Selected



PRNG

, Not Selected

Correct answer:



TRNG

**Results for question 3.**

3

1 / 1 point

The algorithm responsible for various changes and conversions on the plaintext is the \_\_\_\_\_\_\_\_\_.

Correct answer:



encryption



keystream

, Not Selected



cipher

, Not Selected



codebook

, Not Selected

**Results for question 4.**

4

1 / 1 point

The security of a symmetric block cipher intensifies with the addition of more rounds.

Correct answer:

True

False

**Results for question 5.**

5

0 / 1 point

The composition of a symmetric encryption scheme includes \_\_\_\_\_\_\_\_\_ essential components.

Incorrect answer:



three

Correct Answer:

five



four

, Not Selected



five

, Not Selected



six

, Not Selected

**Results for question 6.**

6

1 / 1 point

The foundational structure seen in many symmetric block encryption algorithms like DES was initially outlined by \_\_\_\_\_\_\_\_\_ at IBM in 1973.

Correct answer:

Horst Feistel

**Results for question 7.**

7

1 / 1 point

\_\_\_\_\_\_\_\_\_, a stream cipher, is integral to the Secure Sockets Layer/Transport Layer Security standards for browser-server communication and is a component of WEP and WPA protocols.

Correct answer:

RC4

**Results for question 8.**

8

0 / 1 point

An encryption method is considered \_\_\_\_\_\_\_\_\_ when the resources needed to decipher it surpass the value of the information or when the deciphering time outlasts the information's relevance.

Incorrect answer:

secure

Correct Answer:computationally secure

**Results for question 9.**

9

1 / 1 point

Conventional encryption, secret-key, or single-key encryption is synonymous with public-key encryption.

True

Correct answer:

False

**Results for question 10.**

10

0 / 1 point

Before the advent of public-key encryption in the late 1970s, the encryption method universally employed, synonymous with conventional, secret-key, or single-key encryption, was \_\_\_\_\_\_\_\_\_.

Incorrect answer:

symmetric key encryption

Correct Answer:symmetric

1

1 / 1 point

In terms of speed and code size, stream ciphers generally outpace block ciphers.

Correct answer:

True

False

### Results for question 2.

2

1 / 1 point

Encryption algorithms fundamentally lean on two principles: \_\_\_\_\_\_\_\_\_, where each plaintext element is substituted with another, and transposition, which rearranges the plaintext elements.

Correct answer:

substitution

### Results for question 3.

3

1 / 1 point

The security of a symmetric block cipher intensifies with the addition of more rounds.

Correct answer:

True

False

### Results for question 4.

4

1 / 1 point

When the analyst persuades the system to input a specifically crafted message, it opens up the system to a \_\_\_\_\_\_\_\_\_ attack.



known plaintext

, Not Selected

Correct answer:



chosen plaintext



ciphertext only

, Not Selected



chosen ciphertext

, Not Selected

### Results for question 5.

5

1 / 1 point

\_\_\_\_\_\_\_\_\_, a stream cipher, is integral to the Secure Sockets Layer/Transport Layer Security standards for browser-server communication and is a component of WEP and WPA protocols.

Correct answer:

RC4

### Results for question 6.

6

1 / 1 point

The foundational structure seen in many symmetric block encryption algorithms like DES was initially outlined by \_\_\_\_\_\_\_\_\_ at IBM in 1973.

Correct answer:

Horst Feistel

### Results for question 7.

7

0 / 1 point

Three chief cryptographic methods utilized for PRNGs include: Asymmetric ciphers, Hash functions and message authentication codes, and \_\_\_\_\_\_\_\_\_.

Incorrect answer:

Symmetric ciphers

Correct Answer:symmetric block ciphers

### Results for question 8.

8

1 / 1 point

The \_\_\_\_\_\_\_\_\_ mode can operate solely with the encryption function, bypassing the need for decryption.



DKS

, Not Selected



CBC

, Not Selected



ECB

, Not Selected

Correct answer:



CTR

### Results for question 9.

9

1 / 1 point

In the \_\_\_\_\_\_\_\_ mode, a flaw in a block of transmitted ciphertext affects only its corresponding plaintext block.



CBC

, Not Selected



TSR

, Not Selected

Correct answer:



ECB



CTS

, Not Selected

### Results for question 10.

10

1 / 1 point

A characteristic of a good stream cipher is that the ciphertext should exceed the plaintext in length.

True

Correct answer:

False

Quiz -3  
The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very easy to calculate discrete logarithms.

True

Correct answer:

False

**Results for question 2.**

2

1 / 1 point

Private key encryption is used to produce digital signatures which provide an enhanced form of message authentication.

True

Correct answer:

False

**Results for question 3.**

3

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Correct answer:

decryption

**Results for question 4.**

4

1 / 1 point

The most important hash function is \_\_\_\_\_\_\_\_.



OWH

, Not Selected



MAC

, Not Selected

Correct answer:



SHA



ECB

, Not Selected

**Results for question 5.**

5

1 / 1 point

In addition to providing authentication, a message digest also provides data integrity and performs the same function as a frame check sequence.

Correct answer:

True

False

**Results for question 6.**

6

1 / 1 point

Message encryption alone provides a secure form of authentication.

True

Correct answer:

False

**Results for question 7.**

7

1 / 1 point

Bob uses his own private key to encrypt the message. When Alice receives the ciphertext she finds that she can decrypt it with Bob's public key, thus proving that the message must have been encrypted by Bob. No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key. Therefore the entire encrypted message serves as a \_\_\_\_\_\_\_\_\_ .

Correct answer:

digital signature

**Results for question 8.**

8

0 / 1 point

Using an algorithm that is designed to provide only the digital signature function, the \_\_\_\_\_\_\_\_\_ makes use of the SHA-1 and cannot be used for encryption or key exchange.

Incorrect answer:

DSA

Correct Answer:Digital Signature Standard, DSS

**Results for question 9.**

9

1 / 1 point

The key exchange protocol is vulnerable to a man-in-the-middle attack because it does not authenticate the participants.

Correct answer:

True

False

**Results for question 10.**

10

1 / 1 point

As with symmetric encryption, there are two approaches to attacking a secure hash function: brute-force attack and \_\_\_\_\_\_\_\_\_\_\_ .

Correct answer:

cryptanalysis

The purpose of a \_\_\_\_\_\_\_\_\_\_\_ is to produce a "fingerprint" of a file, message, or other block of data.



cipher encryption

, Not Selected



public key

, Not Selected



message authentication

, Not Selected

Correct answer:



hash function

### Results for question 2.

2

0 / 1 point

The \_\_\_\_\_\_\_\_\_\_ approach has two advantages: it provides a digital signature as well as message authentication and it does not require the distribution of keys to communicating parties.

Incorrect answer:

public key

Correct Answer:public-key

### Results for question 3.

3

1 / 1 point

As with symmetric encryption, there are two approaches to attacking a secure hash function: brute-force attack and \_\_\_\_\_\_\_\_\_\_\_ .

Correct answer:

cryptanalysis

### Results for question 4.

4

1 / 1 point

Using an algorithm that is designed to provide only the digital signature function, the \_\_\_\_\_\_\_\_\_ makes use of the SHA-1 and cannot be used for encryption or key exchange.

Correct answer:

DSS

### Results for question 5.

5

1 / 1 point

The most widely accepted and implemented approach to public-key encryption, \_\_\_\_\_\_\_\_\_ is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.

Correct answer:



RSA



CTR

, Not Selected



SHA

, Not Selected



MD5

, Not Selected

### Results for question 6.

6

1 / 1 point

The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very easy to calculate discrete logarithms.

True

Correct answer:

False

### Results for question 7.

7

1 / 1 point

Public key algorithms are useful in the exchange of conventional encryption keys.

Correct answer:

True

False

### Results for question 8.

8

1 / 1 point

If the message includes a \_\_\_\_\_\_\_\_\_ the receiver is assured that the message has not been delayed beyond that normally expected for network transit.



error detection code

, Not Selected



shared key

, Not Selected



sequence number

, Not Selected

Correct answer:



timestamp

### Results for question 9.

9

1 / 1 point

The purpose of the \_\_\_\_\_\_\_\_\_ algorithm is to enable two users to exchange a secret key securely that then can be used for subsequent encryption of messages and depends on the difficulty of computing discrete logarithms for its effectiveness.



DSS

, Not Selected



RSA

, Not Selected



Rivest-Adleman

, Not Selected

Correct answer:



Diffie-Hellman

### Results for question 10.

10

1 / 1 point

\_\_\_\_\_\_\_\_ protects against passive attacks (eavesdropping).

Correct answer:



Encryption



SCR

, Not Selected



Message authentication

, Not Selected



Obfuscation

Quiz -4

\_\_\_\_\_\_\_\_\_\_ is a process where authentication and permission will be passed on from one system to another, usually across multiple enterprises, thereby reducing the number of authentications needed by the user.

Incorrect answer:

SSO

Correct Answer:Federation

**Results for question 2.**

2

1 / 1 point

An \_\_\_\_\_\_\_\_\_\_ manages the creation and maintenance of attributes such as passwords and biometric information.



authorizing agent

, Not Selected

Correct answer:



attribute service



identity provider

, Not Selected



authenticator

, Not Selected

**Results for question 3.**

3

1 / 1 point

Used in most network security applications, the \_\_\_\_\_\_\_\_\_\_ standard has become universally accepted for formatting public-key certificates.



X.905

, Not Selected



PKIX

, Not Selected



IETF

, Not Selected

Correct answer:



X.509

**Results for question 4.**

4

1 / 1 point

The automated key distribution approach provides the flexibility and dynamic characteristics needed to allow a number of users to access a number of servers and for the servers to exchange data with each other.

Correct answer:

True

False

**Results for question 5.**

5

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ knows the passwords of all users and stores these in a centralized database and also shares a unique secret key with each server.



ticket server

, Not Selected



management server

, Not Selected

Correct answer:



authentication server



key distribution server

, Not Selected

**Results for question 6.**

6

0 / 1 point

A \_\_\_\_\_\_\_\_\_ consists of a public key plus a user ID of the key owner, with the whole block signed by a trusted third party which is typically a CA that is trusted by the user community.

Incorrect answer:

Public-key certificate

Correct Answer:public-key certificate, certificate

**Results for question 7.**

7

1 / 1 point

\_\_\_\_\_\_\_\_\_\_ is a centralized, automated approach to provide enterprise wide access to resources by employees and other authorized individuals, with a focus of defining an identity for each user, associating attributes with the identity, and enforcing a means by which a user can verify identity.



PKIX management

, Not Selected



Registration authority

, Not Selected

Correct answer:



Identity management



Federated managing authority

, Not Selected

**Results for question 8.**

8

1 / 1 point

If an opponent captures an unexpired service granting ticket and tries to use it, they will be denied access to the corresponding service.

True

Correct answer:

False

**Results for question 9.**

9

1 / 1 point

The \_\_\_\_\_\_\_\_\_ extension lists policies that the certificate is recognized as supporting, together with optional qualifier information.



policy mappings

, Not Selected

Correct answer:



certificate policies



directory attribute

, Not Selected



authority key identifier

, Not Selected

**Results for question 10.**

10

1 / 1 point

If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

True

Correct answer:

False

The automated key distribution approach provides the flexibility and dynamic characteristics needed to allow a number of users to access a number of servers and for the servers to exchange data with each other.

Correct answer:

True

False

### Results for question 2.

2

0 / 1 point

When two end systems wish to communicate they establish a logical connection and, for the duration of that logical connection, all user data are encrypted with a one-time \_\_\_\_\_\_\_\_\_\_ which is destroyed at the end of the session.

Incorrect answer:

session keys

Correct Answer:session key

### Results for question 3.

3

1 / 1 point

User certificates generated by a CA need special efforts made by the directory to protect them from being forged.

True

Correct answer:

False

### Results for question 4.

4

0 / 1 point

\_\_\_\_\_\_\_\_\_\_ is a process where authentication and permission will be passed on from one system to another, usually across multiple enterprises, thereby reducing the number of authentications needed by the user.

Incorrect answer:

Federation / SSO

Correct Answer:Federation

### Results for question 5.

5

1 / 1 point

Once the authentication server accepts the user as authentic, it creates an encrypted \_\_\_\_\_\_\_\_\_ which is sent back to the client.



access code

, Not Selected

Correct answer:



ticket



password

, Not Selected



key

, Not Selected

### Results for question 6.

6

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is the client's choice for an encryption key to be used to protect this specific application session.

Correct answer:

subkey

### Results for question 7.

7

1 / 1 point

The principal underlying standard for federated identity is the Security Assertion Markup Language (SAML) which defines the exchange of security information between online business partners.

Correct answer:

True

False

### Results for question 8.

8

1 / 1 point

The \_\_\_\_\_\_\_\_\_ extension lists policies that the certificate is recognized as supporting, together with optional qualifier information.



policy mappings

, Not Selected



authority key identifier

, Not Selected

Correct answer:



certificate policies



directory attribute

, Not Selected

### Results for question 9.

9

1 / 1 point

\_\_\_\_\_\_\_\_\_\_ defines a framework for the provision of authentication services by the X.500 directory to its users and defines alternative authentication protocols based on the use of public-key certificates.

Correct answer:

X.509

### Results for question 10.

10

1 / 1 point

Containing the hash code of the other fields encrypted with the CA's private key, the \_\_\_\_\_\_\_\_\_\_ covers all of the other fields of the certificate and includes the signature algorithm identifier.

Correct answer:



signature



extension

, Not Selected



subject unique identifier

, Not Selected



issuer unique identifier

An \_\_\_\_\_\_\_\_\_\_ manages the creation and maintenance of attributes such as passwords and biometric information.



identity provider

, Not Selected



authorizing agent

, Not Selected



authenticator

, Not Selected

Correct answer:



attribute service

### Results for question 2.

2

0 / 1 point

With a principal objective of enabling secure, convenient, and efficient acquisition of public keys, \_\_\_\_\_\_\_\_\_\_ is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

Incorrect answer:

Public key infrastructure

Correct Answer:public-key infrastructure, PKI

### Results for question 3.

3

1 / 1 point

If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

True

Correct answer:

False

### Results for question 4.

4

1 / 1 point

After determining which systems are allowed to communicate with each other and granting permission for the two systems to establish a connection, the \_\_\_\_\_\_\_\_\_ provides a one-time session key for that connection.

Correct answer:

KDC

### Results for question 5.

5

1 / 1 point

Kerberos version 4 requires the use of a(n) \_\_\_\_\_\_\_\_\_\_\_\_.



MAC address

, Not Selected

Correct answer:



IP address



ISO network address

, Not Selected



Ethernet link address

, Not Selected

### Results for question 6.

6

0 / 1 point

The strength of any cryptographic system rests with the \_\_\_\_\_\_\_\_\_ technique, a term that refers to the means of delivering a key to two parties that wish to exchange data without allowing others to see the key.

Incorrect answer:

Key distribution

Correct Answer:key distribution

### Results for question 7.

7

1 / 1 point

If an opponent captures an unexpired service granting ticket and tries to use it, they will be denied access to the corresponding service.

True

Correct answer:

False

### Results for question 8.

8

0 / 1 point

The \_\_\_\_\_\_\_\_\_ extension is used only in certificates for CAs issued by other CAs and allows an issuing CA to indicate that one or more of that issuer's policies can be considered equivalent to another policy used in the subject CA's domain.

Incorrect answer:

Policy mapping

Correct Answer:policy mappings

### Results for question 9.

9

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is the client's choice for an encryption key to be used to protect this specific application session.

Correct answer:

subkey

### Results for question 10.

10

1 / 1 point

The technical deficiencies of Kerberos version 4 are: double encryption, PCBC encryption, session keys, and \_\_\_\_\_\_\_\_\_\_.

Correct answer:

password attacks

Quiz 5

0 / 1 point

An \_\_\_\_\_\_\_\_\_ authenticator is an access point or NAS that requires EAP authentication prior to granting access to a network.

Incorrect answer:

EAP authenticator

Correct Answer:EAP

**Results for question 2.**

2

0 / 1 point

In effect, \_\_\_\_\_\_\_\_ is an operating system in the cloud.



DHCP

, Not Selected



PaaS

, Not Selected



IEEE 802.1X

, Not Selected

Incorrect answer:



IaaS

Correct Answer:

PaaS

**Results for question 3.**

3

0 / 1 point

A \_\_\_\_\_\_\_\_\_ is an entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link.

Incorrect answer:

Supplicant

Correct Answer:supplicant

**Results for question 4.**

4

0 / 1 point

The \_\_\_\_\_\_\_\_\_\_\_ functions as an access control point for users in remote locations connecting to an enterprise’s internal network.

Incorrect answer:

network access server

Correct Answer:Network access server, NAS

**Results for question 5.**

5

1 / 1 point

For many clients, the most devastating impact from a security breach is the loss or leakage of data.

Correct answer:

True

False

**Results for question 6.**

6

1 / 1 point

\_\_\_\_\_\_\_\_\_ is the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers’ on-premise systems.



IaaS

, Not Selected



PaaS

, Not Selected

Correct answer:



SecaaS



SaaS

, Not Selected

**Results for question 7.**

7

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is a person or organization that maintains a business relationship with, and uses service from, cloud providers.

Correct answer:



cloud consumer



cloud auditor

, Not Selected



cloud broker

, Not Selected



cloud carrier

, Not Selected

**Results for question 8.**

8

1 / 1 point

\_\_\_\_\_\_\_\_\_ saves the complexity of software installation, maintenance, upgrades, and patches.



EAP

, Not Selected

Correct answer:



SaaS



IaaS

, Not Selected



DHCP

, Not Selected

**Results for question 9.**

9

1 / 1 point

\_\_\_\_\_\_\_\_\_ defines how the TLS protocol can be encapsulated in EAP messages.

Correct answer:

EAP-TLS

**Results for question 10.**

10

1 / 1 point

Data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Correct answer:

True

False

The threat of data compromise decreases in the cloud.

True

Correct answer:

False

### Results for question 2.

2

1 / 1 point

\_\_\_\_\_\_\_\_\_\_\_ is an umbrella term for managing access to a network.

Correct answer:



NAC



RAS

, Not Selected



ARC

, Not Selected



NAS

, Not Selected

### Results for question 3.

3

1 / 1 point

\_\_\_\_\_\_\_\_\_ is a client computer that is attempting to access a network.



NAC

, Not Selected



RAS

, Not Selected

Correct answer:



EAP peer



PSK

, Not Selected

### Results for question 4.

4

1 / 1 point

The cloud provider in a private cloud infrastructure is responsible for both the infrastructure and the control.

True

Correct answer:

False

### Results for question 5.

5

1 / 1 point

An \_\_\_\_\_\_\_\_\_\_ server is a server computer that negotiates the use of a specific EAP method with an EAP peer, validates the EAP peer’s credentials, and authorizes access to the network.

Correct answer:

authentication

### Results for question 6.

6

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ is an Internet protocol that enables dynamic allocation of IP addresses to hosts.



VLAN

, Not Selected



IEEE 802.1X

, Not Selected

Correct answer:



DHCP



EAPS

, Not Selected

### Results for question 7.

7

1 / 1 point

\_\_\_\_\_\_\_\_\_ saves the complexity of software installation, maintenance, upgrades, and patches.

Correct answer:



SaaS



EAP

, Not Selected



IaaS

, Not Selected



DHCP

, Not Selected

### Results for question 8.

8

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ determines what access should be granted.



authentication server

, Not Selected



access requestor

, Not Selected

Correct answer:



policy server



supplicant

, Not Selected

### Results for question 9.

9

1 / 1 point

There is a decreasing trend in organizations to move information technology operations to a cloud computing infrastructure.

True

Correct answer:

False

### Results for question 10.

10

1 / 1 point

A \_\_\_\_\_\_\_\_\_\_ provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user.

Correct answer:

firewall

## Your Answers:

### Results for question 1.

1

1 / 1 point

Rather than building elaborate authentication protocols at each server, \_\_\_\_\_\_\_\_\_ provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

Correct answer:

Kerberos

### Results for question 2.

2

0 / 1 point

A \_\_\_\_\_\_\_\_\_\_ is a set of managed nodes that share the same Kerberos database which resides on the Kerberos master computer system that is located in a physically secure room.

Incorrect answer:

kerberos realm

Correct Answer:Kerberos realm

### Results for question 3.

3

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ property guarantees that it is impossible to find an alternative message with the same hash value as a given message, thus preventing forgery when an encrypted hash code is used.

Correct answer:

second preimage resistant

### Results for question 4.

4

1 / 1 point

standardized schemes that are becoming increasingly important as part of Web commerce and that focus on security at the transport layer are: SSL/TLS, HTTPS, and \_\_\_\_\_\_\_\_\_.

Correct answer:

SSH

### Results for question 5.

5

0 / 1 point

provides security services between Transport Layer Protocol and applications that use TCP.

Incorrect answer:

TLS

Correct Answer:Secure Socket Layer, SSL

### Results for question 6.

6

1 / 1 point

Using an algorithm that is designed to provide only the digital signature function, the \_\_\_\_\_\_\_\_\_ makes use of the SHA-1 and cannot be used for encryption or key exchange.

Correct answer:

DSS

### Results for question 7.

7

1 / 1 point

In the \_\_\_\_\_\_\_\_ mode, a flaw in a block of transmitted ciphertext affects only its corresponding plaintext block.

Correct answer:



ECB



CBC

, Not Selected



CTS

, Not Selected



TSR

, Not Selected

### Results for question 8.

8

1 / 1 point

The technical deficiencies of Kerberos version 4 are: double encryption, PCBC encryption, session keys, and \_\_\_\_\_\_\_\_\_\_.

Correct answer:

password attacks

### Results for question 9.

9

1 / 1 point

The security goal requiring each entity's actions to be traceable solely to that entity is known as what?



Privacy

, Not Selected

Correct answer:



Accountability



Integrity

, Not Selected



Authenticity

, Not Selected

### Results for question 10.

10

1 / 1 point

\_\_\_\_\_\_\_\_\_ provides secure, remote logon and other secure client/server facilities.



HTTPS

, Not Selected

Correct answer:



SSH



SLP

, Not Selected



TLS

, Not Selected

### Results for question 11.

11

1 / 1 point

A \_\_\_\_\_\_\_\_ is a person, organization, or entity responsible for making a service available to interested parties.



cloud carrier

, Not Selected

Correct answer:



cloud provider



cloud auditor

, Not Selected



cloud broker

, Not Selected

### Results for question 12.

12

0 / 1 point

Reusing keys is a benefit of block ciphers.

True

Incorrect answer:

False

Correct Answer:True

### Results for question 13.

13

1 / 1 point

handshake is complete and the client and server may begin to exchange application layer data after the server sends its finished message in phase \_\_\_\_\_\_\_\_\_ of the Handshake Protocol.

Correct answer:

4

### Results for question 14.

14

1 / 1 point

A session key is destroyed at the end of a session.

Correct answer:

True

False

### Results for question 15.

15

1 / 1 point

Stream ciphers dominate the list of widely utilized symmetric encryption algorithms.

True

Correct answer:

False

### Results for question 16.

16

1 / 1 point

The private key is known only to its owner.

Correct answer:

True

False

### Results for question 17.

17

1 / 1 point

The purpose of the \_\_\_\_\_\_\_\_\_ algorithm is to enable two users to exchange a secret key securely that then can be used for subsequent encryption of messages and depends on the difficulty of computing discrete logarithms for its effectiveness.



DSS

, Not Selected

Correct answer:



Diffie-Hellman



RSA

, Not Selected



Rivest-Adleman

, Not Selected

### Results for question 18.

18

1 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

Correct answer:

True

False

### Results for question 19.

19

1 / 1 point

Public key algorithms are based on mathematical functions rather than on simple operations on bit patterns.

Correct answer:

True

False

### Results for question 20.

20

1 / 1 point

Which organization is globally recognized, oversees Internet infrastructure standards, and houses groups like the IETF and IAB?

Correct answer:



ISOC



FIPS

, Not Selected



ITU-T

, Not Selected



ISO

, Not Selected

### Results for question 21.

21

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ is an Internet protocol that enables dynamic allocation of IP addresses to hosts.



VLAN

, Not Selected



EAPS

, Not Selected



IEEE 802.1X

, Not Selected

Correct answer:



DHCP

### Results for question 22.

22

1 / 1 point

The Data Encryption Standard algorithm incorporates a key size of \_\_\_\_\_\_\_\_\_.



32 bit

, Not Selected

Correct answer:



56 bit



128 bit

, Not Selected



168 bit

, Not Selected

### Results for question 23.

23

1 / 1 point

A cipher that processes fixed-sized chunks of plaintext to yield equally sized blocks of ciphertext is termed a \_\_\_\_\_\_\_\_\_ cipher.

Correct answer:

block

### Results for question 24.

24

1 / 1 point

Cryptographic hash functions generally execute slower in software than conventional encryption algorithms such as DES.

True

Correct answer:

False

### Results for question 25.

25

1 / 1 point

makes use of a pseudorandom function referred to as \_\_\_\_\_\_\_\_\_\_ to expand secrets into blocks of data for purposes of key generation or validation.

Correct answer:

PRF

### Results for question 26.

26

1 / 1 point

A cloud \_\_\_\_\_\_\_\_\_ is an intermediary that provides connectivity and transport of cloud services from CP’s to cloud consumers.

Correct answer:

carrier

### Results for question 27.

27

1 / 1 point

With a \_\_\_\_\_\_\_\_\_ infrastructure, the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.



hybrid cloud

, Not Selected



community cloud

, Not Selected



private cloud

, Not Selected

Correct answer:



public cloud

### Results for question 28.

28

0 / 1 point

Within network security, the capacity to manage and restrict access to host systems via communication pathways is termed

Incorrect answer:

Access control

Correct Answer:access control, Access Control

.

### Results for question 29.

29

1 / 1 point

A characteristic of a good stream cipher is that the ciphertext should exceed the plaintext in length.

True

Correct answer:

False

### Results for question 30.

30

1 / 1 point

An arbitrary byte sequence chosen by the server to identify an active or resumable session state is a \_\_\_\_\_\_\_\_\_.



cipher spec

, Not Selected



peer certificate

, Not Selected

Correct answer:



session identifier



compression

, Not Selected

### Results for question 31.

31

0 / 1 point

\_\_\_\_\_\_\_\_\_ computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Incorrect answer:

cloud

Correct Answer:Cloud

### Results for question 32.

32

0 / 1 point

Diffie-Hellman would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key.

Incorrect answer:

Ephemeral Diffie-Hellman

Correct Answer:Ephemeral

### Results for question 33.

33

1 / 1 point

Which type of attacks are aimed at changing system resources or affecting their function?



Traffic analysis

, Not Selected

Correct answer:



Active



Passive

, Not Selected



Release of message content

, Not Selected

### Results for question 34.

34

1 / 1 point

When the sender and recipient deploy the same key, it's termed \_\_\_\_\_\_\_\_\_ encryption.



asymmetric

, Not Selected

Correct answer:



symmetric



two-key

, Not Selected



public-key

, Not Selected

### Results for question 35.

35

0 / 1 point

The NIST cloud computing reference architecture focuses on the requirements of “what” cloud services provide, not a “how to” design solution and implementation.

True

Incorrect answer:

False

Correct Answer:True

### Results for question 36.

36

1 / 1 point

Does a system component or service's importance correlate with its required availability level?

Correct answer:

True

False

### Results for question 37.

37

1 / 1 point

A \_\_\_\_\_\_\_\_\_\_ indicates the length of time for which a ticket is valid (e.g., eight hours).

Correct answer:

lifetime

### Results for question 38.

38

1 / 1 point

In effect, \_\_\_\_\_\_\_\_ is an operating system in the cloud.



IEEE 802.1X

, Not Selected



DHCP

, Not Selected

Correct answer:



PaaS



IaaS

, Not Selected

### Results for question 39.

39

1 / 1 point

A

Correct answer:

digital signature

 can either be data attached to, or a cryptographic transformation of a data unit, enabling the recipient to verify its source and integrity, and safeguarding against counterfeiting.

### Results for question 40.

40

1 / 1 point

Secure Hash Algorithms with hash value lengths of 256, 384, and 512 bits are collectively known as \_\_\_\_\_\_\_\_\_.

Correct answer:



SHA-2



SHA-1

, Not Selected



SHA-0

, Not Selected



SHA-3

, Not Selected

### Results for question 41.

41

1 / 1 point

Are both viruses and worms categorized as software-based threats?

Correct answer:

True

False

### Results for question 42.

42

1 / 1 point

The \_\_\_\_\_\_\_\_\_ was developed by NIST and published as a federal information processing standard in 1993.

Correct answer:

SHA

### Results for question 43.

43

1 / 1 point

A random value to be repeated to assure that the response is fresh and has not been replayed by an opponent is the \_\_\_\_\_\_\_\_\_\_.

Correct answer:



nonce



option

, Not Selected



realm

, Not Selected



rtime

, Not Selected

### Results for question 44.

44

1 / 1 point

What ensures that users' identities are genuine and each input stems from a trusted source?

Correct answer:



Authenticity



Confidentiality

, Not Selected



Integrity

, Not Selected



Accountability

, Not Selected

### Results for question 45.

45

0 / 1 point

forwarding allows the client to set up a "hijacker" process that will intercept selected application-level traffic and redirect it from an unsecured TCP connection to a secure SSH tunnel.

Incorrect answer:

local

Correct Answer:Local

### Results for question 46.

46

1 / 1 point

The key exchange protocol is vulnerable to a man-in-the-middle attack because it does not authenticate the participants.

Correct answer:

True

False

### Results for question 47.

47

1 / 1 point

The general structure for all symmetric block ciphers is exemplified by the Feistel structure.

Correct answer:

True

False

### Results for question 48.

48

1 / 1 point

In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues that may affect security.

Correct answer:

True

False

### Results for question 49.

49

1 / 1 point

Kerberos relies exclusively on asymmetric encryption and makes use of public key encryption.

True

Correct answer:

False

### Results for question 50.

50

1 / 1 point

refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.

Correct answer:

HTTPS

### Results for question 51.

51

1 / 1 point

The two important aspects of encryption are to verify that the contents of the message have not been altered and that the source is authentic.

True

Correct answer:

False

### Results for question 52.

52

1 / 1 point

The cloud provider in a private cloud infrastructure is responsible for both the infrastructure and the control.

True

Correct answer:

False

### Results for question 53.

53

1 / 1 point

The foundational structure seen in many symmetric block encryption algorithms like DES was initially outlined by \_\_\_\_\_\_\_\_\_ at IBM in 1973.

Correct answer:

Horst Feistel

### Results for question 54.

54

1 / 1 point

Which type of security encompasses measures to address violations related to information transmission?

Correct answer:



Network



Intranet

, Not Selected



Digital

, Not Selected



Computer

, Not Selected

### Results for question 55.

55

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is a key used between entities for the purpose of distributing session keys.



session relay key

, Not Selected



symmetric key

, Not Selected



key distribution center

, Not Selected

Correct answer:



permanent key

### Results for question 56.

56

1 / 1 point

For symmetric encryption, the security relies more on keeping the algorithm undisclosed than the key.

True

Correct answer:

False

### Results for question 57.

57

1 / 1 point

If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

True

Correct answer:

False

### Results for question 58.

58

1 / 1 point

\_\_\_\_\_\_\_\_\_\_\_ includes people, processes, and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, and then granting the correct level of access based on this assured identity.

Correct answer:

IAM

### Results for question 59.

59

1 / 1 point

The principal underlying standard for federated identity is the Security Assertion Markup Language (SAML) which defines the exchange of security information between online business partners.

Correct answer:

True

False

### Results for question 60.

60

1 / 1 point

Microsoft Explorer originated SSL.

True

Correct answer:

False

1

1 / 1 point

In addition to providing authentication, a message digest also provides data integrity and performs the same function as a frame check sequence.

Correct answer:

True

False

### Results for question 2.

2

1 / 1 point

Besides replay, message modification, and denial of service, active attacks also include

Correct answer:

masquerade

 as a category.

### Results for question 3.

3

1 / 1 point

Security \_\_\_\_\_\_\_\_\_\_ are third party audits of cloud services.

Correct answer:

assessments

### Results for question 4.

4

1 / 1 point

The cloud provider in a private cloud infrastructure is responsible for both the infrastructure and the control.

True

Correct answer:

False

### Results for question 5.

5

1 / 1 point

The most widely accepted and implemented approach to public-key encryption, \_\_\_\_\_\_\_\_\_ is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.

Correct answer:



RSA



CTR

, Not Selected



MD5

, Not Selected



SHA

, Not Selected

### Results for question 6.

6

1 / 1 point

The NIST cloud computing reference architecture focuses on the requirements of “what” cloud services provide, not a “how to” design solution and implementation.

Correct answer:

True

False

### Results for question 7.

7

1 / 1 point

Encryption in version 4 makes use of a nonstandard mode of DES known as \_\_\_\_\_\_\_\_\_\_\_.



KDC

, Not Selected



CBC

, Not Selected



PKI

, Not Selected

Correct answer:



PCBC

### Results for question 8.

8

1 / 1 point

Which service tackles security concerns raised by denial-of-service incidents?



Integrity

, Not Selected

Correct answer:



Availability



Routing control

, Not Selected



Event detection

, Not Selected

### Results for question 9.

9

1 / 1 point

The shared master secret is a one-time 48-byte value generated for a session by means of secure key exchange.

Correct answer:

True

False

### Results for question 10.

10

1 / 1 point

In the \_\_\_\_\_\_\_\_ mode, a flaw in a block of transmitted ciphertext affects only its corresponding plaintext block.

Correct answer:



ECB



TSR

, Not Selected



CBC

, Not Selected



CTS

, Not Selected

### Results for question 11.

11

1 / 1 point

A \_\_\_\_\_\_\_\_ is a person, organization, or entity responsible for making a service available to interested parties.

Correct answer:



cloud provider



cloud carrier

, Not Selected



cloud broker

, Not Selected



cloud auditor

, Not Selected

### Results for question 12.

12

1 / 1 point

It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). A hash function with this property is referred to as \_\_\_\_\_\_\_\_\_\_.



preimage resistant

, Not Selected



weak collision resistant

, Not Selected



one-way

, Not Selected

Correct answer:



collision resistant

### Results for question 13.

13

1 / 1 point

EAPOL operates at the network layers and makes use of an IEEE 802 LAN, such as Ethernet or Wi-Fi, at the link level.

Correct answer:

True

False

### Results for question 14.

14

1 / 1 point

The final message in phase 2, and one that is always required, is the \_\_\_\_\_\_\_\_\_\_\_ message, which is sent by the server to indicate the end of the server hello and associated messages.



finished

, Not Selected

Correct answer:



server\_done



goodbye

, Not Selected



no\_certificate

, Not Selected

### Results for question 15.

15

1 / 1 point

A PRNG utilizes a consistent value, known as the \_\_\_\_\_\_\_\_\_, to generate a bit sequence through a set algorithm.

Correct answer:

seed

### Results for question 16.

16

0 / 1 point

A method that exhaustively tries every conceivable key to decode ciphertext is known as the \_\_\_\_\_\_\_\_\_ approach.



brute-force

, Not Selected

Incorrect answer:



block cipher

Correct Answer:

brute-force



computational

, Not Selected



triple DES

, Not Selected

### Results for question 17.

17

1 / 1 point

The two important aspects of encryption are to verify that the contents of the message have not been altered and that the source is authentic.

True

Correct answer:

False

### Results for question 18.

18

0 / 1 point

In computer security, three main principles are confidentiality, availability, and

Incorrect answer:

Integrity

Correct Answer:integrity

.

### Results for question 19.

19

1 / 1 point

Access requestors are also referred to as clients.

Correct answer:

True

False

### Results for question 20.

20

1 / 1 point

The transformed and often unreadable output from an encryption process is called ciphertext.

Correct answer:

True

False

### Results for question 21.

21

1 / 1 point

Once the authentication server accepts the user as authentic, it creates an encrypted \_\_\_\_\_\_\_\_\_ which is sent back to the client.



access code

, Not Selected



key

, Not Selected



password

, Not Selected

Correct answer:



ticket

### Results for question 22.

22

1 / 1 point

Are pervasive security methods unrelated to any specific OSI security function or protocol tier?

Correct answer:

True

False

### Results for question 23.

23

1 / 1 point

\_\_\_\_\_\_\_\_\_ defines how the TLS protocol can be encapsulated in EAP messages.

Correct answer:

EAP-TLS

### Results for question 24.

24

1 / 1 point

A \_\_\_\_\_\_\_\_\_\_ is a set of managed nodes that share the same Kerberos database which resides on the Kerberos master computer system that is located in a physically secure room.

Correct answer:

Kerberos realm

### Results for question 25.

25

1 / 1 point

The purpose of a \_\_\_\_\_\_\_\_\_\_\_ is to produce a "fingerprint" of a file, message, or other block of data.



cipher encryption

, Not Selected



message authentication

, Not Selected



public key

, Not Selected

Correct answer:



hash function

### Results for question 26.

26

1 / 1 point

A Pseudorandom Function takes as input:



an identifying label

, Not Selected



a secret value

, Not Selected

Correct answer:



all of the above



a seed value

, Not Selected

### Results for question 27.

27

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ property guarantees that it is impossible to find an alternative message with the same hash value as a given message, thus preventing forgery when an encrypted hash code is used.

Correct answer:

second preimage resistant

### Results for question 28.

28

1 / 1 point

Which term means that systems operate in a timely manner without denying service to valid users?



Data confidentiality

, Not Selected



System integrity

, Not Selected



Integrity

, Not Selected

Correct answer:



Availability

### Results for question 29.

29

1 / 1 point

Microsoft Explorer originated SSL.

True

Correct answer:

False

### Results for question 30.

30

1 / 1 point

Kerberos relies exclusively on asymmetric encryption and makes use of public key encryption.

True

Correct answer:

False

### Results for question 31.

31

1 / 1 point

Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement.

Correct answer:

True

False

### Results for question 32.

32

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ approach is vulnerable to man-in-the-middle attacks.



Ephemeral Diffie-Hellman

, Not Selected

Correct answer:



Anonymous Diffie-Hellman



Fixed Diffie-Hellman

, Not Selected



Fortezza

, Not Selected

### Results for question 33.

33

1 / 1 point

Message encryption alone provides a secure form of authentication.

True

Correct answer:

False

### Results for question 34.

34

1 / 1 point

Are both viruses and worms categorized as software-based threats?

Correct answer:

True

False

### Results for question 35.

35

1 / 1 point

The foundational structure seen in many symmetric block encryption algorithms like DES was initially outlined by \_\_\_\_\_\_\_\_\_ at IBM in 1973.

Correct answer:

Horst Feistel

### Results for question 36.

36

1 / 1 point

The \_\_\_\_\_\_\_\_\_ mode employs a counter equivalent to the size of a plaintext block.



CFB

, Not Selected

Correct answer:



CTR



ECB

, Not Selected



CBC

, Not Selected

### Results for question 37.

37

1 / 1 point

Public key cryptography is \_\_\_\_\_\_\_\_\_\_.



one key

, Not Selected



symmetric

, Not Selected

Correct answer:



asymmetric



bit patterned

, Not Selected

### Results for question 38.

38

1 / 1 point

Which organization is globally recognized, oversees Internet infrastructure standards, and houses groups like the IETF and IAB?



ITU-T

, Not Selected



FIPS

, Not Selected

Correct answer:



ISOC



ISO

, Not Selected

### Results for question 39.

39

1 / 1 point

The strength of any cryptographic system rests with the \_\_\_\_\_\_\_\_\_ technique, a term that refers to the means of delivering a key to two parties that wish to exchange data without allowing others to see the key.

Correct answer:

key distribution

### Results for question 40.

40

1 / 1 point

Sessions are used to avoid the expensive negotiation of new security parameters for each connection that shares security parameters.

Correct answer:

True

False

### Results for question 41.

41

0 / 1 point

When there's an interruption in accessing or using an information system, it's known as a loss of

Incorrect answer:

Availability

Correct Answer:availability

.

### Results for question 42.

42

1 / 1 point

When two end systems wish to communicate they establish a logical connection and, for the duration of that logical connection, all user data are encrypted with a one-time \_\_\_\_\_\_\_\_\_\_ which is destroyed at the end of the session.

Correct answer:

session key

### Results for question 43.

43

1 / 1 point

higher-layer protocols defined as part of SSL and used in the management of SSL exchanges are: The Handshake Protocol, The Change Cipher Spec Protocol, and the \_\_\_\_\_\_\_\_\_\_ Protocol.

Correct answer:

Alert

### Results for question 44.

44

1 / 1 point

An \_\_\_\_\_\_\_\_\_\_ manages the creation and maintenance of attributes such as passwords and biometric information.



identity provider

, Not Selected



authorizing agent

, Not Selected



authenticator

, Not Selected

Correct answer:



attribute service

### Results for question 45.

45

1 / 1 point

What category of mechanisms are designed to maintain the consistency of individual data units or data streams?



Event detection

, Not Selected



Authentication exchange

, Not Selected



Trusted functionality

, Not Selected

Correct answer:



Data integrity

### Results for question 46.

46

1 / 1 point

Which U.S. federal institution focuses on standards, measurement science, and fostering technological advancements in the private sector?

Correct answer:



NIST



ITU-T

, Not Selected



ISO

, Not Selected



ISOC

, Not Selected

### Results for question 47.

47

1 / 1 point

\_\_\_\_\_\_\_\_\_ Protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm along with cryptographic keys to be used to protect data sent in an SSL Record.

Correct answer:

Handshake

### Results for question 48.

48

1 / 1 point

Server authentication occurs at the transport layer, based on the server possessing a public/private key pair.

Correct answer:

True

False

### Results for question 49.

49

1 / 1 point

A random value to be repeated to assure that the response is fresh and has not been replayed by an opponent is the \_\_\_\_\_\_\_\_\_\_.



rtime

, Not Selected



option

, Not Selected

Correct answer:



nonce



realm

, Not Selected

### Results for question 50.

50

1 / 1 point

The \_\_\_\_\_\_\_\_\_ is used to convey SSL-related alerts to the peer entity.



Handshake Protocol

, Not Selected

Correct answer:



Alert Protocol



Change Cipher Spec Protocol

, Not Selected



SSL Record Protocol

, Not Selected

### Results for question 51.

51

1 / 1 point

The foundation of AES is the Feistel framework.

True

Correct answer:

False

### Results for question 52.

52

1 / 1 point

Cryptographic hash functions generally execute slower in software than conventional encryption algorithms such as DES.

True

Correct answer:

False

### Results for question 53.

53

1 / 1 point

A \_\_\_\_\_\_\_\_\_\_ provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user.

Correct answer:

firewall

### Results for question 54.

54

1 / 1 point

After determining which systems are allowed to communicate with each other and granting permission for the two systems to establish a connection, the \_\_\_\_\_\_\_\_\_ provides a one-time session key for that connection.

Correct answer:

KDC

### Results for question 55.

55

1 / 1 point

The threat of data compromise decreases in the cloud.

True

Correct answer:

False

### Results for question 56.

56

1 / 1 point

Kerberos version 4 requires the use of a(n) \_\_\_\_\_\_\_\_\_\_\_\_.



Ethernet link address

, Not Selected

Correct answer:



IP address



MAC address

, Not Selected



ISO network address

, Not Selected

### Results for question 57.

57

1 / 1 point

Three chief cryptographic methods utilized for PRNGs include: Asymmetric ciphers, Hash functions and message authentication codes, and \_\_\_\_\_\_\_\_\_.

Correct answer:

symmetric block ciphers

### Results for question 58.

58

1 / 1 point

The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.

Correct answer:

True

False

### Results for question 59.

59

1 / 1 point

An encryption method is considered \_\_\_\_\_\_\_\_\_ when the resources needed to decipher it surpass the value of the information or when the deciphering time outlasts the information's relevance.

Correct answer:

computationally secure

### Results for question 60.

60

1 / 1 point

Two prerequisites for the safe application of symmetric encryption are: secure acquisition of the secret key by both sender and receiver, and a robust \_\_\_\_\_\_\_\_\_.

Correct answer:

encryption algorithm