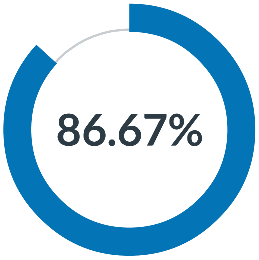
Results

NAVEEN AJAY KARASU



52
Out of 60 points

45:36
Time for this attempt

Your Answers:

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.

✓ Kerberos

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.

✕ kerberos realm

Correct Answer: **Kerberos realm**

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.

✓ second preimage resistant

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 _______.

✓ SSH

5 0 / 1 point

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

✗ TLS

Correct Answer: **Secure Socket Layer, SSL**

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.

✓ DSS

7 1 / 1 point

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

✓ ● ECB

○ CBC

○ CTS

○ TSR

8 1 / 1 point

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

✓ password attacks

9

1 / 1 point

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

○ Privacy

✓ ● Accountability

○ Integrity

○ Authenticity

10

1 / 1 point

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

○ HTTPS

✓ ● SSH

○ SLP

○ TLS

11

1 / 1 point

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

○ cloud carrier

✓ ● cloud provider

○ cloud auditor

○ cloud broker

12

0 / 1 point

Reusing keys is a benefit of block ciphers.

○ True

✗ ● False

Correct Answer: **True**

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.

✓ 4

14 1 / 1 point

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

✓ ● True

○ False

15 1 / 1 point

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

○ True

✓ ● False

16 1 / 1 point

The private key is known only to its owner.

✓ ● True

○ False

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

✓ ● Diffie-Hellman

○ RSA

○ Rivest-Adleman

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?

✓ ● True

○ False

19 1 / 1 point

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

✓ ● True

○ False

20 1 / 1 point

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

✓ ● ISOC

○ FIPS

○ ITU-T

○ ISO

21 1 / 1 point

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

○ VLAN

○ EAPS

○ IEEE 802.1X

✓ ● DHCP

22 1 / 1 point

The Data Encryption Standard algorithm incorporates a key size of _______.

○ 32 bit

✓ ● 56 bit

○ 128 bit

○ 168 bit

23 1 / 1 point

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

✓ block

24 1 / 1 point

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

○ True

✓ ● False

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.

✓ PRF

26 1 / 1 point

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

✓ carrier

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

○ community cloud

○ private cloud

✓ ● public cloud

28 0 / 1 point

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

Correct Answer: **access control, Access Control**

29 1 / 1 point

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

○ True

✓ ● False

30 1 / 1 point

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

○ cipher spec

○ peer certificate

✓ ● session identifier

○ compression

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.

✕ cloud

Correct Answer: **Cloud**

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.

✕ Ephemeral Diffie-Hellman

Correct Answer: **Ephemeral**

33 1 / 1 point

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

○ Traffic analysis

✓ ● Active

○ Passive

○ Release of message content

34 1 / 1 point

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

○ asymmetric

✓ ● symmetric

○ two-key

○ public-key

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

✕ ● False

Correct Answer: **True**

36 1 / 1 point

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

✓ ● True

○ False

37 1 / 1 point

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

✓ lifetime

38 1 / 1 point

In effect, _______ is an operating system in the cloud.

○ IEEE 802.1X

○ DHCP

✓ ● PaaS

○ IaaS

39 1 / 1 point

A ✓ 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.

40 1 / 1 point

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

✓ ● SHA-2

○ SHA-1

○ SHA-0

○ SHA-3

41 1 / 1 point

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

✓ ● True

○ False

42 1 / 1 point

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

✓ SHA

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 ________.

✓ ● nonce

○ option

○ realm

○ rtime

44 1 / 1 point

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

✓ ● Authenticity

○ Confidentiality

○ Integrity

○ Accountability

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.

✗ local

Correct Answer: **Local**

46 1 / 1 point

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

✓ ● True

○ False

47 1 / 1 point

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

✓ ● True

○ False

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.

✓ ● True

○ False

49 1 / 1 point

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

○ True

✓ ● False

50 1 / 1 point

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

✓ HTTPS

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

✓ ● False

52 1 / 1 point

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

○ True

✓ ● False

53 1 / 1 point

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

✓ Horst Feistel

54 1 / 1 point

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

✓ ● Network

○ Intranet

○ Digital

○ Computer

55 1 / 1 point

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

○ session relay key

○ symmetric key

○ key distribution center

✓ ● permanent key

56 1 / 1 point

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

○ True

✓ ● False

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

✓ ● False

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.

✓ IAM

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.

✓ ● True

○ False

60 1 / 1 point

Microsoft Explorer originated SSL.

○ True

✓ ● False