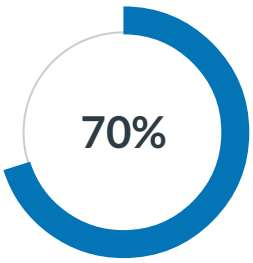
Results

SHASHANK ANSHUMAAN MALKARAM



42
Out of 60 points

42:42
Time for this attempt

Your Answers:

1 1 / 1 point

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

- True
- ✓ False

2 1 / 1 point

important SSL concepts are the SSL session and the SSL _____ .

- ✓ connection

3 1 / 1 point

With a _____ infrastructure, the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns.

- hybrid cloud
- ✓ community cloud
- public cloud

public cloud

private cloud

4 0 / 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 _____ .

✗ Digital Signature

Correct Answer: **digital signature**

5 0 / 1 point

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

✗ Firewall

Correct Answer: **firewall**

6 1 / 1 point

X.509 is based on the use of public-key cryptography and digital signatures.

✓ True

False

7 1 / 1 point

Based on the use of a mathematical construct known as the elliptic curve and offering equal security for a far smaller bit size, _____ has begun to challenge RSA.

RIPE-160

TCB

✓ ECC

DSS

8 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 Computing

Correct Answer: **Cloud**

9 1 / 1 point

The symmetric encryption key for data encrypted by the client and decrypted by the server is a _____.

sequence key

✓ client write key

server write key

master key

10 1 / 1 point

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

✓ True

False

11 1 / 1 point

In the ECB mode of encryption if an attacker reorders the blocks of ciphertext then each block will still decrypt successfully, however, the reordering may alter the meaning of the overall data sequence.

✓ True

False

12 1 / 1 point

The ticket-granting ticket is encrypted with a secret key known only to the authentication server and the ticket-granting server.

✓ True

False

13 1 / 1 point

Unlike traditional publishing environments, the Internet is three-way and vulnerable to attacks on the Web servers.

True

✓ False

14 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.

management server

ticket server

key distribution server

✓ authentication server

15 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.

✗ Public key certificate

Correct Answer: **public-key certificate, certificate**

16 0 / 1 point

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

✗ crypto-analysis attack

Correct Answer: **cryptanalysis**

17 1 / 1 point

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

✓ Replay, masquerade, DOS as a category.

18 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.

✗ Public key infrastructure

Correct Answer: **public-key infrastructure, PKI**

19 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**

20 1 / 1 point

A system that processes input elements sequentially, delivering output for each element, is termed a _____.

✓ ◉ stream cipher

○ block cipher

○ keystream

cryptanalysis

21 0 / 1 point

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

True

✗ False

Correct Answer: **True**

22 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

23 1 / 1 point

In order to solve the problem of minimizing the number of times that a user has to enter a password and the problem of a plaintext transmission of the password, a _____ server is used.

authentication

✓ ticket granting

password ciphering

access code

24 1 / 1 point

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

compression

peer certificate

✓ session identifier

cipher spec

25 0 / 1 point

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

✗ Integrity .

Correct Answer: **integrity**

26 0 / 1 point

Security _____ are third party audits of cloud services.

✗ Assessments

Correct Answer: **assessments**

27 1 / 1 point

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

✓ hash function

message authentication

cipher encryption

public key

28 1 / 1 point

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

✓ True

False

29 1 / 1 point

_____ is a client computer that is attempting to access a network.

PSK

✓ EAP peer

NAC

RAS

30 0 / 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.

✗ Key Distribution center

Correct Answer: **key distribution center, KDC**

31 1 / 1 point

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

✓ True

False

32 1 / 1 point

_____ is organized as three protocols that typically run on top of TCP for secure network communications and are designed to be relatively simple and inexpensive to implement.

✓ SSH

TLS

SSI

SSL

33 0 / 1 point

_____ is an EAP method for mutual authentication and session key derivation using a Pre-Shared Key.

✗ EAP-PSK (EAP-Pre Shared key)

Correct Answer: **EAP-GPSK**

34 1 / 1 point

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

- EAPS
- VLAN
- ✓ DHCP
- IEEE 802.1X

35 0 / 1 point

The _____ property is the "one-way" property and is important if the authentication technique involves the use of a secret value.

✗ Pre-image Resistant

Correct Answer: **preimage resistant**

36 1 / 1 point

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

- CBC
- ✓ CTR
- ECB
- CFB

37 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.

✓ X.509

38 1 / 1 point

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

- chosen ciphertext
- ciphertext only
- known plaintext
- ✓ chosen plaintext

39 0 / 1 point

An attack that seeks to obtain system information without altering its resources is termed a

✗ Passive attack.

Correct Answer: **passive**

40 1 / 1 point

The global organization of national standards bodies that fosters international standardization and collaboration in various spheres is the ✓ ISO.

41 1 / 1 point

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

- True
- ✓ False

42 0 / 1 point

✗ Non -repudation ensures that neither the sender nor the receiver can deny having sent or received a specific message.

Correct Answer: **Nonrepudiation, Non-repudiation, Non repudiation**

43 1 / 1 point

Is there a distinct separation between network security and internet security?

- True
- ✓ False

44 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

45 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

46 1 / 1 point

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

✓ HTTPS

47 1 / 1 point

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

True

✓ False

48 1 / 1 point

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

block cipher

triple DES

computational

✓ brute-force

49 1 / 1 point

Symmetric block ciphers handle _____ of data concurrently.

✓ one block

three blocks

four blocks

two blocks

50 0 / 1 point

The Cloud Security Alliance defines _____ as 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.

✗ Security as a Service (SaaS)

Correct Answer: **Security as a service, Security as a Service, SecaaS**

51 0 / 1 point

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

Correct Answer: **encipherment, encryption, cryptography**

52 1 / 1 point

The key algorithmic ingredients of _____ are the AES encryption algorithm, the CTR mode of operation, and the CMAC authentication algorithm.

✓ CCM

53 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
- ✓ False

54 1 / 1 point

Defending against ciphertext-only attacks is relatively straightforward due to the limited information available to the attacker.

- ✓ True
- False

55 1 / 1 point

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

- PKIX
- X.905
- ✓ X.509

IETF

56 1 / 1 point

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

cloud carrier

cloud auditor

✓ cloud provider

cloud broker

57 1 / 1 point

With each element of the list defining both a key exchange algorithm and a CipherSpec, the list that contains the combination of cryptographic algorithms supported by the client in decreasing order of preference is the _____.

Version

Random

✓ CipherSuite

Session ID

58 1 / 1 point

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets.

✓ True

False

59 0 / 1 point

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

✗ Substitution

Correct Answer: **substitution**

60 1 / 1 point

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

- MAC address
- Ethernet link address
- ISO network address
- ✓ IP address