Risk Management Principles, Plans and Procedures

Question 1

What is the purpose of browser cache in HTTP basic authentication?

- The purpose of browser cache in HTTP basic authentication is to store the user's credentials for a period of time, allowing them to authenticate without having to enter their credentials every time.

Question 2

What is the purpose of covering tracks in the cyber attack process?

- The purpose of covering tracks is to hide or delete any evidence of unauthorized access or malicious activity and ensure continued access without being detected.

Question 3

What is the purpose of detection and recovery controls?

- The purpose of detection and recovery controls is to focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.

Question 4

What is the purpose of DKIM in e-mail?

- The purpose of DKIM is to permit signing domain to claim responsibility for a message in the mail stream.

Question 5

What is the purpose of management controls?

- The purpose of management controls is to focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission.

Question 6

What is the purpose of reconnaissance in the cyber attack process?

- The purpose of reconnaissance is to gather information about the target, such as network layouts, domains, servers, and infrastructure details, to understand how the network works and identify potential entry points.

Question 7

What is the purpose of whitebox testing?

- The purpose of whitebox testing is to confirm the efficacy of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organization's systems

Question 8

What is the security kernel?

- The security kernel is a central point of access control that enforces access control for computer systems. It implements the reference monitor concept.

Question 9

What is the security kernel, and what is its role in access control?

- The security kernel is the central point of access control for computer systems. It enforces access control policies by intercepting access requests from users, checking them against a rules base or security kernel database, and allowing or denying access based on the defined access rules. It also logs all access requests for later tracking and analysis.

Question 10

What are the three security operation principles all access control models are built on?

- The security operation principles are Need to know, Least privilege, and Separation of duties and responsibilities.

Question 11

What are the security requirements for the IoT according to ITU-T Recommendation Y.2066?

- The security requirements for the IoT according to ITU-T Recommendation Y.2066 are communication security, data management security, service provision security, integration of security policies and techniques, mutual authentication and authorization, and security audit.

Question 12

What are the services provided by IPsec?

- The services provided by IPsec include access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality (encryption), and limited traffic flow (confidentiality).

Question 13

How does the strength of an encryption method correlate to the amount of necessary processing power, resources, and time required to break the cryptosystem or to figure out the value of the key?

- The strength of an encryption method correlates to the amount of necessary processing power, resources, and time required to break the cryptosystem or to figure out the value of the key.

Question 14

What is the TCP/IP model?

- The TCP/IP model is a simpler and more streamlined version of the oSI model, with four layers that describe the functions of a network.

Question 15

What are the three categories of security controls?

- The three categories of security controls are management controls, operational controls, and technical controls.

Question 16

What are the three categories of session hijacking attacks?

- The three categories of session hijacking attacks are man-in-the-middle attacks, blind hijack attacks, and session theft attacks.

Question 17

What are the three main types of access control models?

- The three main types of access control models are Discretionary, Mandatory, and Rule-Based.

Question 18

What are the three risk likelihood categories used in risk analysis?

- The three risk likelihood categories used in risk analysis are high, medium, and low.

Question 19

What are the three service models of cloud computing?

- The three service models of cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Question 20

What are the three types of resource records stored in DNS?

- The three types of resource records stored in DNS are Address (A) record, Mail exchange (MX) record, and Name server (NS) record.

Question 21

How does the TLS Handshake Protocol work?

- The TLS Handshake Protocol comprises a series of messages exchanged by the client and server. The exchange has four phases: 1. Establish security capabilities 2. Server authentication and key exchange. 3. Client authentication and key exchange 4. Finish

Question 22

What is the TLS Handshake Protocol, and what is its purpose?

- The TLS Handshake Protocol is the most complex part of TLS. It is used before any application data is transmitted. Its purpose is to allow the server and client to authenticate each other, negotiate encryption and MAC algorithms, and negotiate cryptographic keys to be used. The handshake comprises a series of messages by the client and server, and the exchange has four phases.

Question 23

What are the four protocols defined in TLS?

- The TLS Record Protocol provides basic security services to various higher-layer protocols. Three higher-layer protocols are defined as part of TLS: The Handshake Protocol, the Change Cipher Spec Protocol, and the Alert Protocol. A fourth protocol, the Heartbeat Protocol, is defined in a separate RFC.

Question 24

What are the TLS session and the TLS connection, and how are they related?

- The TLS session is created by the Handshake Protocol and defines a set of cryptographic parameters. It is used to avoid the expensive negotiation of new security parameters for each connection. The TLS connection is a transport layer protocol that provides a suitable type of service. Every connection is associated with one session.

Question 25

What are the top cloud-specific security threats listed by the Cloud Security Alliance?

- The top cloud specific security threats listed by the Cloud Security Alliance are abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, and account or service hijacking.

Question 26

What is the purpose of the Transport layer in the OSI and TCP/IP models?

- The Transport layer is responsible for segmenting messages for transmission and ensuring reliable communication between endpoints.

Question 27

What is the purpose of the Transport layer in the OSI model?

- The Transport layer takes care of segmenting messages for transmission. Both the ICP and the UDP are transport protocols. These protocols use ports for addressing, so receiving systems know which application to pass the traffic to.

Question 28

What is the trigger of a virus?

- The trigger is the event or condition that determines when the payload is activated or delivered, sometimes known as a logic bomb.

Question 29

What are the two basic types of ciphers?

- The two basic types of ciphers are stream ciphers and block ciphers.

Question 30

What are the two components needed to create a risk to an asset?

- The two components needed to create a risk to an asset are a threat and a vulnerability.