Intrusion Detection and Firewalls

Question 1

What are the five layers of the secure IoT framework?

- The five layers of the secure IoT frameworks are perception layer, transport layer, network layer, platform layer and application layer.

Question 2

What are the four components of access control?

- The four components of access control are identification, authentication, authorization and accountability.

Question 3

What are the four deployment models of cloud computing?

- The four deployment models of cloud computing are private, community, public and hybrid.

Question 4

What are the functions of IT security management?

- The functions of IT security management include determining organizational IT security objectives, strategies and policies; identifying and analyzing security threats to IT assets; specifying appropriate safeguards; monitoring the implementation and operation of safeguards; developing and implementing a security awareness program; and detecting and reacting to incidents.

Question 5

What is the goal of a blind SQL injection?

- To allow attackers to infer the data present in a database system even when the system is sufficiently secure to not display any enormous information back to the attacker.

Question 6

What is the goal of blackbox testing?

- To identify ways to acces to an organization’s internal IT assets without sharing any information about the internals of the target with the testers.

Question 7

What is the goal of penetration testing?

- To identify and exploit vulnerabilities in a system to determine whether unauthorized acces or other malicious activity is possible and identify which flaws pose a threat to the application.

Question 8

What is the goal of the baseline approach to security risk assessment?

- To implement agreed controls to provide protection against the most common threats and forms a good base for further security measures.

Question 9

What is the goal of the gaining access phase in the cyber attack process?

- To exploit vulnerabilities in a system and gain unauthorized access or conduct other malicious activities.

Question 10

What is the vulnerability involved in XSS attacks?

- The inclusion of script code in the HTML content.

Question 11

What is the difference between the Internet layer and the Network layer in the TCP/IP model?

- The internet layer is responsible for addressing and routing packets across multiple networks while the network layer is responsible for managing communication within a single network.

Question 12

What are the IoT gateway security functions?

- The IoT gateway security functions include data acquisition and analysis, devices and network management, protocol conversion, and security and privacy protection

Question 13

What is the ISO/IEC 27000 series of standards on IT security techniques?

- The ISO/IEC 27000 series of standards is a set of guidelines for IT security management.

Question 14

What is the main difference between Mandatory Access Control (MAC) and Discrectionary Acess Control (DAC)?

- DAC allows the information owner to decide who gets to access the system(s), while MAC is determined by the sensitivity of the resource (classification label). The system and owner make the decision to allow access.

Question 15

What is the Miral botnet attack?

- The Mirai botnet attack is a DDoS attack that infected cameras, printers, routers, and thousands of other devices with the Mirai botnet malware. It generated an average of 1 Terabit per second, causing widespread disruption to websites and services.

Question 16

What is the Mirai botnet and how did it enable DDoS attacks on a massive scale?

- The Miral botnet is a type of malware that targets Internet of Things (IoT) devices, such as IP CCTV cameras and routers. Once infected, these devices become part of a network of "zombie" hosts that can be controlled remotely by the attacker. This allows the attacker to launch DoS attacks on a massive scale, using thousands or even millions of zombie hosts to flood the target system with traffic. The Mirai botnet was responsible for some of the largest DoS attacks in history, including a 1 terabit per second attack in 2016.

Question 17

What is the most common goal of an SQL injection attack?

- The most common goal of an SQL injection attack is the bulk extraction of data.

Question 18

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

- The Network layer gets messages from one endpoint to another. takes care of addressing and routing. The IP is one protocol that exists at this layer.

Question 19

What is the objective of the NIST cloud computing reference architecture?

- The objective of the NIST cloud computing reference architecture is to provide a technical reference for CSCs to understand, discuss, categorize, and compare cloud services, facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations, and illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model.

Question 20

What should be the basis for developing a firewall access policy?

- The organization's information security risk assessment and policy.

Question 21

What is the OSI model and how many layers does it have?

- The osI (Open Systems Interconnection) model is a conceptual framework for understanding how communication systems operate. It has seven layers.

Question 22

What is the OSI model?

- The OSI model is a conceptual model that describes the layers of communication in a network, with each layer performing a specific set of functions.

Question 23

What is the payload of a virus?

- The payload is what the virus does besides spreading, which may involve damage or benign but noticeable activity.

Question 24

What are the phases of a computer virus?

- The phases of a computer virus include propagation, triggering, delivery, and execution.

Question 25

What is the purpose of the Physical Layer in the OSI model?

- The Physical layer is responsible for managing the physical communications.

Question 26

What is the policy definition phase of access control?

- The policy definition phase of access control determines who has access and what systems resources they can use. It is tied to the authorization phase.

Question 27

What is the policy enforcement phase of access control?

- The policy enforcement phase of access control grants or rejects requests for access based on the authorizations defined in the first phase. It is tied to the identification, authentication, and accountability phases.

Question 28

What algorithms are used for signing S/MIME messages?

- The preferred algorithms used for signing S/MIME messages use either an RSA or a DSA signature of a SHA-256 message hash.

Question 29

What is the primary purpose of HIDS?

- The primary purpose of HIDS is to detect intrusions, log suspicious events, and send alerts.

Question 30

What is the principle behind Attribute-based Access Control (ABAC)?

- The principle behind ABAC is that access is controlled based on attributes of the user, the resource to be accessed, and current environmental conditions.

Question 31

What is the principle behind Role based Access Control (RBAC)?

- The principle behind RBAC is that access is controlled based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

Question 32

What is the principle of Discretionary Access Control (DAC)?

- The principle of DAC dictates that the information owner is the one who decides who gets to access the system(s).

Question 33

What is the process for generating a digital signature in S/MIME?

- The process involves taking the message, mapping it into a fixed-length code of 256 bits using SHA-256, encrypting the digest using RSA and the sender's private RSA key, and attaching the result to the message.

Question 34

What is the purpose of a penetration test?

- The purpose of a penetration test is to evaluate the security of a system by simulating an attack on the system to identify vulnerabilities and weaknesses that can be exploited by attackers.

Question 35

What is the purpose of blackbox testing?

- The purpose of blackbox testing is to identify ways to access an organization's internal IT assets from an external perspective.