AAA and Access Control

Question 1

What is the difference between a centralized and decentralized network architecture?

- A centralized network architecture has a single, centralized entity that controls communication, while a decentralized network architecture has no centralized entity and allows devices to communicate directly with each other.

Question 2

What is a denial of service attack?

- A denial of service attack is a type of attack that aims to disrupt the availability of a service or resource by overwhelming it with traffic or other requests.

Question 3

What is a man-in-the-middle attack?

- A man-in-the-middle (MiTM) attack is an attack where an attacker intercepts all communications between two hosts by positioning themselves so that communications between a client and server must flow through them.

Question 4

Is penetration testing an alternative to other IT security measures?

- No, penetration testing is not an alternative to other IT security measures but rather complements them.

Question 5

What is the purpose of reconnaissance and footprinting?

- The purpose of reconnaissance and footprinting is to gather information about a target network, including identifying network layouts, domains, servers, and infrastructure details.

Question 6

What is the purpose of scanning and enumeration?

- The purpose of scanning and enumeration is to find vulnerabilities and entry points in a target network.

Question 7

What is the purpose of gaining access?

- The purpose of gaining access is to break into a network and map the organization's defenses from the inside, creating a battle plan for information to target.

Question 8

What is the purpose of maintaining access?

- The purpose of maintaining access is to continue to access and control the target network, including conducting data exfiltration.

Question 9

What is the purpose of covering tracks?

- The purpose of covering tracks is to hide or delete any evidence of an attacker’s access and actions in the target network.

Question 10

What is whitebox testing?

- Whitebox testing is a type of testing where full information about the target is shared with the testers, allowing them to confirm the efficacy of internal vulnerability assessment and management controls.

Question 11

What is blackbox testing?

- Blackbox testing is a type of testing where no information is shared with the testers about the internals of the target, forcing them to perform the testing from an external perspective.

Question 12

What is access control and what does it prevent?

- Access control is the process of protecting a resource so that it is used only by those allowed to use it. It prevents unauthorized use and puts mitigations in place to protect a resource from a threat

Question 13

What are some operating systems-based DAC policy considerations?

- Access control method, new user registration, and periodic review are some operating systems-based DAC policy considerations.

Question 14

What is accountability in access control?

- Accountability in access control involves audit logs and monitoring to track subject activities with objects to ensure that the person who makes data or system changes can be identified.

Question 15

What is the difference between act-alone malware and coordinated malware?

- Act-alone malware runs on their own and have a specific target, while coordinated malware contributes to a larger scale attack and can cause damage when multiple infected devices are used together.

Question 16

What is active content and what are its potential weaknesses?

- Active content refers to dynamic objects that do something when the user opens a webpage, and its potential weaknesses can be exploited by malware.

Question 17

What is an Access Control List (ACL) in DAC?

- An AcL is a list or a file of users who are given the privilege of access to a system or resource, such as a database. contains a user ID and an associated privilege or set of privileges for that user and that resource.

Question 18

What is an Access Control List (ACL)?

- An ACL is a list or a file of users who are given the privilege of access to a system Or resource. Within the file is a user ID and an associated privilege or set of privileges for that user and that resource.

Question 19

What is an asset in the context of security risk assessment?

- An asset is anything that needs to be protected because it has value to the organization and contributes to the successful attainment of the organization's objectives.

Question 20

How does an attacker hijack a TCP session?

- An attacker can hijack a TCP session by spoofing the client's IP address, determining the correct sequence number that the server is expecting from the client, and injecting data into the session before the client sends its next packet.

Question 21

What is an XSS reflection vulnerability?

- An attacker includes the malicious script content in data supplied to a site.

Question 22

What is an intrusion prevention system (IPS)?

- An extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity. Can be host-based, network-based, or distributed/hybrid. Can use anomaly detection or signature/heuristic detection to identify known malicious behaviour.

Question 23

What is an inband attack?

- An inband attack is an injection attack where code and results are transferred through the same channel.

Question 24

What is an out-of-band attack?

- An out-of-band attack is an injection attack where data is retrieved using a different channel than the one used for injection.

Question 25

What are the two main approaches to IDS analysis?

- Anomaly detection and Signature/Heuristic detection.

Question 26

What are some additional security controls that can be installed?

- Anti-virus software, Host-based Firewalls, IDS or IPS software and Application white listing

Question 27

What are some of the attacks suitable for Anomaly Detection?

- Application layer reconnaissance and attacks, Transport layer reconnaissance and attacks, Network layer reconnaissance and attacks. Unexpected application services, and Policy violations.

Question 28

What should be done during the system planning process?

- Assess risks and plan the system deployment. Secure the underlying operating system and then the key applications. Ensure any critical content is secured. Ensure appropriate network protection mechanisms are used. Ensure appropriate processes are used to maintain security.

Question 29

What are the key steps in the process of securing an operating system?

- Assessing risks and planning system deployment. Securing the operating system and key applications. Ensuring critical content is secured. Using appropriate network protection mechanisms. Maintaining security through appropriate processes.

Question 30

What does non-repudiation provide in cryptosystem?

- Assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender, and prevents the sender from claiming that they never sent the message in the first place.

Question 31

What is a Cross Site Scripting (XSS) attack?

- Attacks where input provided by one user is subsequently output to another user.

Question 32

What is the difference between authentication and authorization?

- Authentication is the process of verifying a user's identity, while authorization is the process of determining whether a user has permission to access a particular resource or perform a specific action.

Question 33

What are the functions that are involved in access control?

- Authentication, Authorization, and Accountability/Audit.

Question 34

What is the difference between auto spreading malware and user-activated malware?

- Auto-spreading malware runs and looks for other vulnerable machines on the Internet, while user-activated malware is run on a computer only because a user accidentally downloads and executes it.

Question 35

What is the initial critical step in writing more secure program code?

- Awareness of the known areas of concern, such as the critical web application security flaws.

Question 36

What are backdoors and rootkits, and what privileges do they give to attackers?

- Backdoors are secret entry points into a program that allow the attacker to gain access and bypass security access procedures. Rootkits are sets of hidden programs installed on a system to maintain covert access to that system. They give administrator (or root) privileges to the attacker, allowing them to add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand.

Question 37

What are some examples of logical access control solutions?

- Biometrics, Tokens, Passwords and Single Sign on solutions

Question 38

What do browsers do to restrict data access in XSS attacks?

- Browsers impose security checks and restrict data access to pages originating from the same site.

Question 39

What are three errors related to risky resource management in the CWE/SANS list?

- Buffer Copy without Checking Size of Input (Classic Buffer Overflow'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), and Download of Code Without Integrity Check.

Question 40

What is a host-based IPS (HIPS)?

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks. Examples of the types of malicious behaviour addressed by HIPS include modification of system resources, privilege-escalation exploits, buffer-overflow exploits, etc.

Question 41

What is the disadvantage of a packet filtering firewall?

- Cannot prevent attacks that employ application specific vulnerabilities or functions, Limited logging functionality, Do not support advanced user authentication, Vulnerable to attacks on TCP/IP protocol bugs and Improper configuration can lead to breaches.

Question 42

What should be considered during the system planning process regarding users and groups?

- Categories of users on the system, Privileges they have, Types of information they can access and How and where they are defined and authenticated.

Question 43

What is the definition of computer security as given in RFC 4949?

- Computer security is defined as measures that implement and assure security services in a computer system, particularly those that assure access control service.

Question 44

What are the three information security properties that malware can attack?

- Confidentiality, Integrity, and Availability.

Question 45

What are the two services provided by the TLS Record Protocol for TIS connections?

- Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of ILS payloads. The message is compressed before being concatenated with the MAC and encrypted, with a range of ciphers being supported. Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC), which is similar to HMAC.

Question 46

What is a personal firewall?

- Controls traffic between a personal computer or workstation and the Internet or enterprise network. Typically much less complex than server-based or stand-alone firewalls. Primary role is to deny unauthorized remote access.

Question 47

What can be the consequences of a buffer overflow?

- Corruption of program data, unexpected transfer of control, memory access violations, execution of code chosen by the attacker

Question 48

What should be done during application configuration?

- Creating and specifying appropriate data storage areas for application. Making appropriate changes to the application or service default configuration details.

Question 49

Why is cryptography important?

- Cryptography is important because it is an effective way of protecting sensitive information as it is stored on media or transmitted through untrusted network communication paths.

Question 50

What is Discretionary access control (DAC)?

- DAC controls access based on the identity of the requestor and access rules (authorizations) stating what requestors are (or are not) allowed to do.

Question 51

What is data exfiltration in the cyber attack process?

- Data exfiltration is the process of extracting data from the network using tools and techniques to simulate the actions of hackers.

Question 52

What are honeypots?

- Decoy systems designed to lure a potential attacker away from critical systems, collect information about the attacker's activity, and encourage the attacker to stay on the system long enough for administrators to respond.

Question 53

What algorithms are used for encrypting S/MIME messages?

- Default algorithms used for encrypting S/MIME messages are AES and RSA.

Question 54

What are some default items that some applications or services may include?

- Default data, scripts, and user accounts

Question 55

What are some common forms of symmetric key block cipher cryptosystems?

- DES and Triple-DES.

Question 56

What are the three technical mechanisms that can be used for threat mitigation if prevention fails?

- Detection, Identification and Removal