Information Systems Security Fundamentals

Question 1

What is callback security in RADIUS used for?

- It is an extra layer of protection that prevents attackers from using compromised authentication credentials.

Question 2

What are some security issues associated with writing safe program code?

- Security issues associated with writing safe program code incude correct algorithm implementation, correct machine instructions for the algorithm and valid manipulation of data.

Question 3

What are the three approaches recommended by MIST to reduce software responsibilities?

- The three approaches recommended by MIST are to stop vulnerabilities before they occur, find vulnerabilities before they can be exploited and reduce the impact of vulnerabilities by building more resilient architectures.

Question 4

What is a boot sector infector virus?

- A boot sector infector virus infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

Question 5

What is a client/server architecture?

- A client/server architecture is a centralized architecture where one device provides a service (server) and all other devices connected to it are clients.

Question 6

What is a cryptosystem?

- A cryptosystem encompasses all of the necessary componentsfor encryption and decryption to take place.

Question 7

What is a decentralized architecture?

- A decentralized architecture is where there is no centralized entity that controls the communication.

Question 8

What is a Denial of Service (DoS) attack?

- A DoS attack is an attempt to prevent legitimate users from accessing a system or network resource by overwhelming it with traffic or requests.

Question 9

What is a security mechanism?

- A security mechanism is a process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack.

Question 10

What needs to be included in a security policy?

- A security policy needs to address the scope and purpose, IT security requirments, assignment of responsibilities, risk management approach, security awareness and training, general personnel issues and any legal sanctions, integration of security into system development, information classification scheme, contingency and business continuity planning, incident detection and handling processes, and how and when policy is reviewed, and change control to it.

Question 11

What is a security service?

- A security service is a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

Question 12

What is the difference between a tree and a DAG in terms of hierarchical file organization?

- A tree is used in Windows to organise files hierarchically while a directed acyclic graph (DAG) is used in Linux to represent dependencies between files.

Question 13

What can a virus do when attached to an executable program?

- A virus can do anything that the program is permitted to do and executes secretly when the host program is run.

Question 14

What is a virus and how does it spread?

- A virus is a piece of software that infects programs, modifies them to include a copy of the virus, replicates and spreads through network environments.

Question 15

What is an access matrix in DAC?

- An access matrix is a mechanism used to implement DAC. It consists of two dimensions: identified subjects that may attempt data access to the resources and the other dimension lists the objects that may have accessed.

Question 16

What is an attack surface?

- An attack surface consists of the reachable and exploitable vulnerabilities in a system.

Question 17

What is an ICMP attack?

- An ICMP attack is a type of network attack that exploits vulnerabilities in the Internet Control Message Protocol (ICMP) to cause disruption or damage to a target network or system.

Question 18

What is the difference between an APT and other types of attacks?

- APTs differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods.

Question 19

How can attack surfaces be categorized?

- Attack surfaces can be categorized in the following way: Network attack surface: vulnerabilities over an enterprise network, wide-area network or Internet Software attack surface: vulnerabilties in application, utility or operating system code Human attack surface: vulnerabilties created by personnel or outsiders such as social engineering, human error, and trusted outsiders.

Question 20

What are the four fundamental goals of cryptography?

- Confidentiality, Integrity, authentication and non-repudiation

Question 21

What are confusion and diffusion in cryptography?

- Confusion and diffusion are basic operations used in cryptographic algorithms to obscure plain-text messages. Confusion occurs when the relationship between the plain text and the key is complicated, and diffusion occurs when a change in the plain text results in multiple changes spread throughout the cipher text.

Question 22

What is cryptography?

- Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process.

Question 23

What are the two different types of data that must be considered when developing a cryptographic system for the purpose of providing confidentiality?

- Data at rest (stored data) and data in motion (data being transmitted across a network between two systems).

Question 24

What are some defences available to prevent code injection attacks?

- Defences available to prevent code injection attacks include blocking assignment of form field values to global variables, using only constant values in include commands and validating variables immediately before use.

Question 25

What is defensive programming, and why is it important?

- Defensive programming is an approach to programming in which programmers validate assumptions about input data and handle all potential failures gracefully and safely. It is important because it helps prevent software vulnerabilities caused by invalid assumptions or errors.

Question 26

What is the potential risk of unencrypted transmission in IP?

- Eavesdropping is possible at any intermediate host during routing.

Question 27

What are some of the threats to access controls?

- Gaining physical access, eavesdropping, bypassing security, exploiting hardware and software, reusing or discarding media, electronic eavesdropping, intercepting communication, accessing networks, exploiting applications.

Question 28

What are some of the activities that cyber criminals engage in?

- Identity theft, theft of financial credentials, coporate espionage, data theft, and data ransoming.

Question 29

What is the difference between DAC and MAC?

- In DAC, the information owner decides who gets to access the system(s), whereas in MAC, access is controlled based on comparing security labels with security clearances.

Question 30

What is the difference between RBAC and ABAC?

- In RBAC, access is controlled based on the roles that users have within the system, while in ABAC, access is controlled based on attributes of the user, the resource to be accessed and current environmental conditions.

Question 31

What is input fuzzing?

- Input fuzzing is a software testing technique that uses randomly generated data as inputs to a program. Its purpose is to determine if the program or function correctly handles abnormal inputs.

Question 32

What is IP source spoofing?

- IP source spoofing is a technique used in network attacks to disguise the true source of a packet by falsifying the source IP address. This can make it more difficult to trace the source of an attack.

Question 33

What is IP spoofing?

- IP spoofing is the act of falsifying the source IP address of a packet to make it appear to come from a different machine or network.

Question 34

What is the main advantage of centralised access control administration?

- It provides a consistent and uniform method of controlling users' access rights.

Question 35

What is the role of management in supporting IT security policy?

- IT security policy must be supported by senior management. A separate IT security officer is needed to provide consistent overall supervision, liaison with senior management, maintenance of IT security objectives, strategies, policies, handle incidents, management of IT security awareness and training programs, and interaction with IT project security officers.

Question 36

Is penetration testing a magic bullet for IT security?

- No, penetration testing is not a magic bullet for IT security.

Question 37

Are the protocols mentioned in the presentation the only ones that exist?

- No, there are many other protocols that exist.

Question 38

What is penetration testing?

- Penetration testing is a method for gaining assurance in the security of an IT system by attempting to breach some or all of the system's security, using the same tools and techniques as an adversary might.

Question 39

What is port knocking?

- Port knocking is a security technique that involves making connection attempts to a series of ports in a certain order to open a port that is otherwise blocked.

Question 40

Why is it important for social engineers to profile their targets?

- Profiling targets allows social engineers to understand their habits, preferences and potential vulnerabilities. This information can be used to craft more effective social engineering attacks that are more likely to be successful in manipulating the target into revealing sensitive information or taking a desired action.

Question 41

Which protocol do many ISPs use for authentication?

- Remote Authentication Dial-In User Service (RADIUS)

Question 42

What are some examples of intrusion?

- Remote root compromise, web server defacement, guessing/cracking passwords, copying databases containing credit card numbers, viewing sensitive data without authorization, running a packet sniffer, distributing pirated software, using an unsecured modem to access internal network, impersonating an executive to get information, and using an unattended workstation.

Question 43

What is the function of security risk management?

- Security risk assessment is needed for each asset in the organization that requires protection. It provides the information necessary to decide what management, operational and technical controls are needed to reduce the risks identified.

Question 44

What are some sources social engineering use to gather information?

- Social engineers use a variety of sources to gather information including social media, public records, company websites, job postings, new articles, and even dumpster diving for physical documents.

Question 45

What are some capabilities of cryptography?

- Some capabilities of cryptography are privacy or confidentiality, integrity, entity authentication or identification, message authentication, signature, access control, certification, timestamping, witnessing, ownership, anonymity and non-repudiation.

Question 46

What are some challenges associated with cyber security?

- Some challenges associated with cyber security include the complexity of security, potential attacks on security features, counter-initiative procedures used to provide services, deciding where to use various security mechanisms, constant monitoring security being too often an afterthought, security mechanisms typically involving more than a particular algorithm or protocol, security being essentially a battle of wits between a penetrator and the designer, little benefit from security investment being perceived until a security failure occurs and strong security being often viewed as an impediment to efficient and user-friendly operation.

Question 47

What are some high-profile API attacks?

- Some high-profile APT attacks include Aurora, RSA, APT1, and Stuxnet.

Question 48

What are the two main types of cryptosystems that enforce confidentiality?

- Symmetric key cryptosystems asymmetric cryptosystems asymmetric cryptosystems.

Question 49

How does TACACS+ differ from RADIUS in terms of transport protocol?

- TACACS+ uses TCP, while RADIUS uses UDP.

Question 50

What is the Transmission Control Protocol (TCP)?

- TCP is a reliable and connection-based transport layer protocol that protects against loss and reordering of packets using sequence numbers, timeouts, and retransmissions.

Question 51

What are some techniques used in API attacks?

- Techniques used in APT attacks range from simple social engineering and spear-phishing emails to sophisticated attack vectors.

Question 52

What is the “To Tell or Not To Tell” block referring to in the context of penetration testing?

- The "To Tell or Not To Tell" block is referring to the decision of whether or not to inform too many people about the penetration test, which may invalidate the test, or not informing anyone, which may result in valuable resources chasing a non existent intruder for too long. It also mentions that elevation procedures make not telling risky.

Question 53

What is the purpose of a penetration test?

- The purpose of a penetration test is to test the security of systems and architectures from the point of view of an attacker (hacker, cracker).

Question 54

What is the purpose of an initial engagement in a penetration test?

- The purpose of an initial engagement is to engage the external team to perform the penetration test.

Question 55

What is the purpose of IT Security Management?

- The purpose of I Security Management is to ensure that critical assets are sufficiently protected in a cost-effective manner.

Question 56

What is the three-way handshake in TCP packet exchange?

- The three way handshake is a process used to initiate a TCP connection, where the initiating system sends a SYN packet to the destination, the destination sends an ACK to acknowledge receipt of the first packet (a combined SYN/ACK packet), and the initiating system sends an ACK packet to acknowledge receipt of the SYN/ACK packet. Data transfer can then begin.

Question 57

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 58

What are the two broad defence approaches to buffer overflow attacks?

- The two broad defence approaches to buffer overflow attacks are compile-time, which harden programs to resist attacks in new programs, and run-time, which detect and abort attacks in existing programs.

Question 59

What is a script-kiddie?

- They are hackers with minimal technical skill who primarily use existing attack toolkits.

Question 60

Who are cyber criminals?

- They are individuals or members of an organized crime group with a goal of financial reward.

Question 61

What is the relative location of security facilities in the TCP/IP protocol stack?

- They are located between the application layer and the network layer.

Question 62

What are the services that various security approaches provide in relation to the TCP/IP protocol stack?

- They provide services such as confidentiality, integrity, authenticity, and non-repudiation.

Question 63

What are some typical privileges included in an ACL in DAC?

- Typical privileges include Read, Write, Update, Execute, Delete, or Rename.

Question 64

What is an application-level gateway?

- Must have proxy code for each application. Tends to be more secure than packet filters

Question 65

What is a botnet and what can It be used for?

- A botnet is a collection of bots capable of acting in a coordinated manner. It can be used for distributed denial-of-service (DoS) attacks, spamming, sniffing traffic, keylogging, spreading new malware, installing advertisement add-ons and browser helper objects (BHOs), attacking IRC chat networks, and manipulating online polls/games.