Network Security

Question 1

What is the difference between a closed policy and an open policy?

- A closed policy assumes that everything is denied by default, while an open policy assumes that everything is allowed by default.

Question 2

What is a file handle used for?

- A file handle is an opaque identifier for a file or folder that is used to perform file operations such as opening, reading, writing, executing, and closing files.

Question 3

What is the main advantage of decentralised access control administration?

- It allows people closer to the resources to control access, which means changes can happen faster.

Question 4

What are some countermeasures for SQL injection attacks?

- Some countermeasures for SQL injection attacks include defensive coding practices, parameterized query insertion, detection using signature-based, anomaly-based, or code analysis techniques, and run-time prevention.

Question 5

What are the four fundamental goals of cryptography?

- The four fundamental goals of cryptography are confidentiality, integrity, authentication, and non-repudiation.

Question 6

What is the purpose of integrity in cryptosystems?

- The purpose of integrity is to ensure that data is not altered without authorization, protect against all forms of alteration, and check if the received message is identical to the sent message.

Question 7

What is a Distributed Denial of Service (DDoS) attack?

- A DDoS attack is similar to a Dos attack but is carried out by multiple compromised systens that are coordinated to flood a target with traffic or requests.

Question 8

What is the difference between a passive and an active attack?

- A passive attack attempts to learn or make use of information from the system but does not affect system resources, while an active attack attempts to alter system resources or affect their operation.

Question 9

What is a peer-to-peer network?

- A peer-to-peer network is an example of a decentralized architecture where devices are connected directly to each other.

Question 10

What is a protocol?

- A protocol is a set of rules or conventions that dictate communication.

Question 11

What is a security attack?

- A security attack is any action that compromises the security of information owned by an organization.

Question 12

What is a security breach?

- A security breach is any event that results in a violation of any of the CIA security tenets.

Question 13

How does a virus spread through a network environment?

- A virus spreads through a network environment by infecting programs and replicating itself to other content.

Question 14

What is a vulnerability?

- A vulnerability is a flaw or weakness in an asset’s design, implementation, or operation and management that could be exploited by sone threat.

Question 15

Give an example of a client/server architecture.

- A website is an example of a client/server architecture.

Question 16

What Is an Access Control Entry (ACE)?

- An ACE is an entry that allows or denies a certain type of access to a file or folder by a user or group.

Question 17

What is a security intrusion?

- An unauthorized act of bypassing the security mechanisms of a system.

Question 18

Who are APT attacks typically attributed to?

- APT attacks are typically attributed to state-sponsored organizations and criminal enterprises.

Question 19

What are the characteristics of an APT?

- APIs are advanced, persistent, and pose a threat to the selected targets.

Question 20

What is intrusion detection?

- It is a hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions.

Question 21

Why is it important to ensure that machine language corresponds to the algorithm?

- It is important to ensure that machine language corresponds to the algorithm to prevent bugs that could be exploited.

Question 22

What is the purpose of providing Internet security?

- It is to protect against various threats and ensure the confidentiality, integrity, and availability of data.

Question 23

What is IT security management?

- IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity. and reliability.

Question 24

What is the aim of activist attacks?

- The aim of their attacks is often to promote and publicize their cause, typically through website defacement, denial of service attacks, and theft and distribution of data that results in negative publicity or compromise of their targets.

Question 25

What are the components of a virus?

- The components of a virus include the infection mechanism, trigger, and payload.

Question 26

What is the concern associated with the dynamic memory allocation?

- The concern associated with dynamic memory allocation is memory leak, which is the steady reduction in memory available on the heap to the point where it is completely exhausted.

Question 27

How did the development of virus creation toolkits in the early 1990s change the development and deployment of naluare?

- The development of virus-creation toolkits in the early 1990s greatly assisted in the development and deployment of malware, allowing even novices to deploy malware through a variety of propagation mechanisms and pauload modules.

Question 28

What are the four possible flags in a TCP packet header?

- The four possible flags in a TCP packet header are SYN (Synchronize), ACK (Acknowledge), FIN (Finished), and RSI (Reset).

Question 29

What are the goals of cryptography?

- The goals of cryptography are to hide information from unauthorized individuals, make obtaining the information too work-intensive or time consuming to be worthwhile to the attacker, and to ensure the integrity and authenticity of the information.

Question 30

What is the intent of APT attacks?

- The intent of APT attacks is to infect the target with sophisticated malware with multiple propagation mechanisms and payloads.

Question 31

What are the IT security management functions?

- The IT security management functions include: (1) determining organizational IT security objectives, strategies, and policies; (2) determining organizational I security requirements; (3) identifying and analyzing security threats to IT assets within the organization: (4) identifying and analyzing risks; (5) specifying appropriate safeguards; (6) monitoring the implementation and operation of safeguards that are necessary to cost-effectively protect the information and services within the organization; (7) developing and implementing a security awareness program: and (8) detecting and reacting to incidents.

Question 32

What is the OSI model?

- The OSI model is a seven-layer model that describes a particular set of functions and behaviours for communication.

Question 33

What is the Ping of Death attack?

- The Ping of Death attack is a Dos attack that involves sending a ping packet that exceeds the maximum size using IP fragmentation. This can cause buffer overflows and crashes in some operating systems.

Question 34

What is the principle of Complete Mediation?

- The principle of Complete Mediation dictates that every access must be checked against the access control mechanism.

Question 35

What is the principle of Compromise Recording?

- The principle of Compromise Recording states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent.

Question 36

What is the principle of Economy of Mechanism?

- The principle of Economy of Mechanism states that security measures embodied in both hardware and software should be as simple and small as possible.

Question 37

What is the principle of Least Common Mechanism?

- The principle of Least Common Mechanism states that in systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized.

Question 38

What is the principle of Least Privilege?

- The principle of Least Privilege states that every process and every user of the system should operate using the least set of privileges necessary to perform the task.

Question 39

What is the principle of Open Design?

- The principle of Open Design states that the design of a security mechanism should be open rather than secret.

Question 40

What is the principle of Psychological Acceptability?

- The principle of Psychological Acceptability states that user interfaces should be well designed and intuitive, and all security related settings should adhere to what an ordinary user might expect.

Question 41

What is the principle of Separation of Privilege?

- The principle of Separation of Privilege dictates that multiple conditions should be required to achieve access to restricted resources or have a program perform some action.

Question 42

What is the principle of Work Factor?

- The principle of Work Factor states that the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.

Question 43

What is the purpose of authentication in cryptosystems?

- The purpose of authentication is to verify the claimed identity of system users.

Question 44

What is the purpose of follow up in a penetration test?

- The purpose of follow-up is to verify that any vulnerabilities found during the penetration test have been remediated and to retest the systems and applications to ensure that they are secure.

Question 45

What is the purpose of non-repudiation in cryptosystems?

- The purpose of non repudiation is to provide assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender and prevent the sender from claiming that they never sent the message in the first place.

Question 46

What is the purpose of reporting in a penetration test?

- The purpose of reporting is to document the results of the penetration test and provide recommendations for remediation of any vulnerabilities found.

Question 47

What is the purpose of scoping in a penetration test?

- The purpose of scoping is to def ine the scope of the penetration test, including the systems and applications that will be tested and the types of tests that will be performed.

Question 48

What is the purpose of testing in a penetration test?

- The purpose of testing is to perform the penetration test and attempt to identify vulnerabilities in the systems and applications being tested.

Question 49

What needs to be examined when addressing an organization's IT security?

- The role and importance systems in the organization of IT to be examined.

Question 50

How can a sender make it difficult to trace a packet back to an attacker in IP?

- The sender can spoof the source address, making it difficult to trace the packet back to the attacker.

Question 51

What is the Smurf IP attack?

- The Smurf IP attack is a Dos attack that involves sending ping requests to a broadcast address using a spoofed source address. This causes all hosts on the network to reply to the spoofed address, overwhelming it with traffic.

Question 52

What are the three categories of vulnerabilities?

- The three categories of vulnerabilities are corrupted (loss of integrity), leaky (loss of confidentiality), and unavailable or very slow (loss of availability).

Question 53

What are the three concepts that form the CIA triad?

- The three concepts are confidentiality, integrity, and availability.

Question 54

What are the three questions that IT Security Management seeks to answer?

- The three questions are: (1) What assets need to be protected? (2) How are those assets threatened? (3) What can be done to counter those threats?

Question 55

What are the two types of data that need to be considered when developing a cryptographic system for confidentiality?

- The two types of data are data at rest and data in motion.

Question 56

What is the typical pattern of a penetration test engagement?

- The typical pattern of a penetration test engagement is initial engagement, scoping, testing, reporting, and follow-up. There should be a severity rating for any issues found.

Question 57

What is the underground economy in relation to malware?

- The underground economy involves the sale of attack kits, access to compromised hosts, and stolen information.

Question 58

What Is an example of threats on a typical network?

- These can include malware, viruses, phishing, denial of service attacks, and unauthorized access.

Question 59

What are some approaches to providing Internet security?

- They include using firewalls, encryption, intrusion detection/ prevention systems, virtual private networks, and secure sockets layer/transport layer security.

Question 60

What is the User Datagram Protocol (UDP)?

- UDP is a lightweight and connectionless transport layer protocol that provides more control over when data is sent but does not compensate for loss of packets or deliver packets in order.

Question 61

How can XSS attacks be prevented?

- XSS attacks can be prevented by examining any user supplied input and removing or escaping any dangerous code to block its execution.

Question 62

What is an example of an attack kit?

- Zeus and Angler are examples of attack kits.

Question 63

How does NIST 808-83 define naluare?

- "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, Or availability of the victim data, applications, or operating system or otherwise annoying or disrupting the victim."

Question 64

How does NCSC define malware?

- "A term that includes viruses. trojans, worms or any code or content that could have an adverse impact on organisations or individuals."

Question 65

What is a blind hijack attack?

- A blind hi jack attack is an attack where an attacker injects data such as malicious commands into communications, but cannot see the response to that data.

Question 66

What is a blind SQL injection attack?

- A blind SQL injection attack is a type of inferential attack that allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker.

Question 67

What is a buffer overflow attack?

- A buffer overflow attack occurs when a program tries to store more data in a buffer than it can hold, causing the excess data to overflow into adjacent memory spaces and potentially allowing an attacker to execute malicious code.

Question 68

What is a Caesar cipher?

- A Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Question 69

What is a denial-of-service (Dos) attack and how does it work?

- A DoS attack is a type of cyber attack that aims to prevent legitimate users from accessing a system. This is typically done by flooding the target system with traffic or data, overwhelming its resources and causing it to crash or become unresponsive. This can be accomplished through a variety of techniques, including sending large numbers of packets to the target system, using IP source spoofing to hide the attacker's identity, or exploiting vulnerabilities in the system's software or hardware.

Question 70

What is the purpose of a firewall in network security?

- A firewall is used to monitor and control incoming and outgoing network traffic based on predetermined security rules.

Question 71

What does a low interaction honeypot emulate?

- A particular IT service or system well enough to provide a realistic initial interaction.

Question 72

What is port scanning and what are some common scanning techniques?

- Port scanning is an essential step in the reconnaissance phase. Some common scanning techniques include ping scans, connect scans, SIN scans, and FIN scans.