Malicious Software

Question 1

What is the principle of Fail-safe defaults?

- The principle of Fail-safe defaults states that access decisions should be based on permission rather than exclusion-the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.

Question 2

What is a one-time pad?

- A one-time pad is an extremely powerful type of substitution cipher that is made up of truly random values and used only one time.

Question 3

What is the most difficult design issue with sandbox analysis?

- Determining how long to run each interpretation.

Question 4

What are the two default policies of a packet filtering firewall?

- Discard (Deny) and Forward (Permit)

Question 5

What are the four types of Access Control Policies?

- Discretionary access control (DAC), Mandatory access control (MAC), Role-based access control (RBAC), and Attribute-based access control (ABAC).

Question 6

What is DKIM?

- DKIM stands for DomainKeys Identified Mail and is a specification of cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream.

Question 7

What is DNS cache poisoning?

- DNS cache poisoning is when an attacker gives DNS servers false records and gets them cached.

Question 8

What is DNS hijacking?

- DNS hi jacking is when an attacker attempts to change the IP associated with a server maliciously.

Question 9

What is the domain name system (DNS)?

- DNS is an application-layer protocol for mapping domain names to IP addresses.

Question 10

How can DNS cache poisoning be prevented?

- INS Security (DMSSEC) can be deployed to ensure the authenticity and integrity of DNS replies by signing DNS replies at each step of the way using public key cryptography.

Question 11

What is used to enforce message integrity in cryptosystems?

- Encrypted message digests, known as digital signatures created upon transmission of a message.

Question 12

What is the goal of security testing?

- Ensure the previous security configuration steps are correctly implemented. Identify any possible vulnerabilities.

Question 13

What is of particular concern with remotely accessed services such as Web and file transfer services?

- Ensuring that most of the files can only be read, but not written, by the server.

Question 14

How does ESP in tunnel mode encrypt and authenticate the IP packet?

- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.

Question 15

What is ethical hacking?

- Ethical hacking is the practice of testing the security of computer systems and networks using the same tools and techniques as malicious hackers, but with the permission and knowledge of the system owners to identify vulnerabilities and improve security.

Question 16

What are the two approaches to classifying malware?

- Focusing on how they spread or propagate through an information system environment to reach the desired target/s or considering all dimensions of malware in order to classify them.

Question 17

What are the four ways in which an attacker can use malicious code to inflict harm?

- Gaining administrative control of a system and using commands, sending commands directly to a system, using software programs that harm a system or make data unusable, or using legitimate remote administration tools and security probes to identify and exploit security vulnerabilities on a network.

Question 18

How can an attacker exploit a buffer overflow?

- Getting a shell that allows the attacker to execute arbitrary commands with high privileges.

Question 19

What is the difference between Host-Based IDS (HIDS) and Network-Based IDS (NIDS)?

- HIDS monitors a single host while NIDS monitors traffic at selected points on a network.

Question 20

What are the dimensions of malware taxonomy used by NCSC?

- Host dependent or independent, persistent or transient, where it installs itself (persistent malware only), how it is triggered, static or dynamically updated, and act alone or coordinated attack.

Question 21

Why is HTTP basic authentication insecure?

- HTTP basic authentication is insecure because full credentials pass over the wire and data is sent in the clear.

Question 22

What is HTTP basic authentication?

- HIP basic authentication is the most basic authentication method where the authentication is based on the existence of an IP address. It is insecure as full credentials pass over the wire and data is sent in the clear.

Question 23

What is IKE and what is its purpose?

- IKE (Internet Key Exchange) is the key management portion of IPsec and involves the determination and distribution of secret keys.

Question 24

What are some best practices for authentication by knowledge, such as using passwords or passphrases?

- Implement account lockout policies to prevent brute force attacks. Audit logon events to track authentication attempts and identify potential security breaches. Use strong passwords or passphrases that are difficult to guess

Question 25

Name three errors related to insecure interaction between components in the WE/SANS list.

- Improper Neutralization ofSpecial Elements used in an SQL Command ('SQL Injection'), Improper Neutralization of Special Elements used in an 08 Command -('OS-Connand-Injection’) and Improper Neutralization Of Input During Web Page Generation ('Cross site Scripting').

Question 26

What is the difference between inband and out-of-band attacks?

- In inband attacks, data are retrieved and presented directly in application web pages, whereas in out-of-band attacks, data are retrieved using a different channel

Question 27

What is the difference between independent malware and host-dependent malware?

- Independent malware is a complete program that can run on its Own once installed on a compromised machine and executed, whereas host-dependent nature requires a host program to run.

Question 28

What are the two types of monitoring software used in perimeter scaring approaches?

- Ingress monitors and egress monitors.

Question 29

What are the steps involved in the system security planning process?

- Initiation, Development, Implementation, Maintenance

Question 30

What is a network-based IPS (NIPS)?

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections. Makes use of signature and anomaly detection. Methods used to identify malicious packets include protocol anomaly, signature-based detection, heuristic-based detection, and stateful protocol analysis.

Question 31

What are the three categories in which the errors in the CWE/SANS list are grouped?

- Insecure interaction between components, risky resource management, and porous defenses.

Question 32

What are some ways to secure the base operating system?

- Installing and patching the operating system, Removing unnecessary services, applications, and protocols. Configuring users, groups, and permissions, Configuring resource controls. Configuring resource controls. Testing the controls.

Question 33

How can IPsec be used to enhance electronic commerce security?

- IPsec can be used to secure remote access over the Internet, establish extranet and intranet connectivity with partners, and enhance electronic commerce security.

Question 34

What is the scope of IPsec?

- IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

Question 35

What is the purpose of IPsec?

- IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet.

Question 36

Why is sandbox analysis useful for malware detection?

- It allows the code to execute in a controlled environment where its behaviour can be closely monitored without threatening the security of a real system.

Question 37

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

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

Question 38

What is the consequence of insufficient checking and validation of data and error codes in programs?

- It can lead to critical web application security flaws.

Question 39

What is the purpose of Distributed or Hybrid IDS?

- It combines information from multiple sensors, both host and network-based, to better identify and respond to intrusion activity.

Question 40

What is a drive by download attack?

- It exploits browser and plugin vulnerabilities to download and install malware on the system without the user's knowledge or consent.

Question 41

What is a boot sector infector virus?

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

Question 42

What is host-based behaviour-blocking software?

- It integrates with the operating system of a host computer and monitors program behaviour in real time for malicious action.

Question 43

What is Signature Detection?

- Te involves matching a large collection of known patterns of malicious data against data stored on a system or in transit over a network.

Question 44

What is Rule based Heuristic Identification?

- It involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses.

Question 45

What is the Advanced Encryption Standard (AES)?

- It is a block cipher that works on128-bit blocks and can have one of three key sizes of 128, 192, or 256 bits. It is now the most widely used symmetric key algorithm.

Question 46

What is the CWE/SANS Top 25 Most Dangerous Software Errors list?

- It is a list of poor programming practices that are the cause of the majority of cyber attacks.

Question 47

What is defensive programming?

- It is a programming practice that requires programmers to validate program assumptions and handle potential failures safely and gracefully.

Question 48

What does a high interaction honeypot entail?

- It is a real system with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers, and may occupy an attacker for an extended period.

Question 49

What is a Denial-of-Service attack?

- It is a type of attack that attempts to prevent legitimate users from accessing a system.

Question 50

What is a polymorphic virus?

- It is a virus that mutates with every infection.

Question 51

What is buffer overflow?

- It is a vulnerability that occurs when a program allocates insufficient space for input, causing data to overwrite adjacent memory locations.

Question 52

What is clickjacking?

- It is a vulnerability used by an attacker to collect an infected user's clicks and trick them into performing unintended actions.

Question 53

What is security by design?

- It is an approach to software development that emphasizes designing software with security in mind.

Question 54

What is the infection mechanism of a virus?

- It is the means by which a virus spreads or propagates, also referred to as the infection vector.

Question 55

What is Single Sign-On (SSO)?

- It is the process of signing on to a computer or network once, and using identification and authorization credentials to access all computers and systems where authorized.

Question 56

What is the payload of a virus?

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

Question 57

What is the danger in failure to validate input interpretation?

- It may result in an exploitable vulnerability.

Question 58

What is malvertising?

- It places malware on websites without actually compromising them, by paying for advertisements that incorporate malware.

Question 59

What is the importance of the WE/SANS Top 25 Most Dangerous Software Errors list?

- It provides a consensus view on the poor programming practices that cause the majority of cyber attacks and serves as a reference for developers to write more secure program code.

Question 60

What is the disadvantage of SPA?

- It requires high resource usage.