Software and Web application security

Question 1

What is a distributed denial-of-service (DDoS) attack and how does it differ from a traditional DoS attack?

- A DDoS attack is a type of attack that uses multiple hosts to amplify the attack. Instead of overwhelming the target system with traffic or data from a single source, a DDoS attack uses a network of intermediary hosts to generate enough traffic to disrupt entire networks or server farms. This makes DDoS attacks much more difficult to detect and mitigate than traditional DoS attacks.

Question 2

What is the difference between a DoS attack and a DDoS attack?

- A DoS attack attempts to overwhelm a network connection for a targeted host through a more powerful host, while a DDoS attack uses multiple intermediary hosts to generate enough traffic to disrupt server farms or a whole network segment and possibly beyond.

Queston 3

What is a network?

- A network is a set of technologies that connects computers, allowing communication and collaboration of computers and devices connected together.

Question 4

What is a chroot jail?

- It restricts the server's view of the file system to just a specified portion, confining a process by mapping the root of the file system to show some other directory.

Question 5

What is IT security management, and what questions does it answer?

- IT security management is a formal process of protecting critical assets in a cost-effective manner. It answers the questions of what assets need to be protected, how are those assets threatened and what can be done to counter those threats.

Question 6

What was the 2014 Heartbleed OpenSSL bug, and what caused it?

- It was a vulnerability that allowed attackers to access sensitive information and it was caused by a failure to check the validity of a binary input value.

Question 7

What is logical access control?

- Logical access control involves deciding which users can get into a system, monitoring what each user does on that system, and restraining or influencing a user's behaviour on that system.

Question 8

What is a Mandatory access control (MAC)?

- MAC controls access based on comparing security labels with security clearances.

Question 9

What are the limitations of host-based behaviour-blocking software?

- Malicious code can cause harm before it has been detected and blocked.

Question 10

What is malware and how can it be prevented?

- Malware is any software designed to harm or exploit a computer system or network. It can be prevented by using antivirus and anti-malware software, keeping software and operating systems up to date, avoiding suspicious downloads and links, and using strong passwords.

Question 11

What are the different types of payloads that malware can carry out?

- Malware payloads can include system corruption, attack agents (bots), remote control facility, information theft (keyloggers and spyware), phishing, stealthing (backdoor and rootkit).

Question 12

What is the purpose of MIME?

- MIME is an extension to the old RFC 822 specification for mail format and provides a number of new header fields that define information about the body of the message.

Question 13

What are the two errors related to porous defenses in the CWE/SAMS list?

- Missing Authentication for Critical Function and Missing Authorization.

Question 14

What are the key components of security maintenance?

- Monitoring and analyzing logging information. Performing regular backups. Recovering from security compromises. Regularly testing system security. Patching and updating critical software. Monitoring and revising configuration as needed.

Question 15

Which access control principle do most of the common operating systems on the market today rely on?

- Most of the common operating systems on the market today (Windows, Macintosh, UNIX, and others) rely on DAC principles for access and operation.

Question 17

What should be considered when evaluating human threat sources in security risk assessment?

- Motivation, capability, resources, probability of attack, and deterrance should be considered when evaluating human threat sources.

Question 18

What is MIST's definition of cloud computing?

- MIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Question 19

What is Non-Discretionary Access Control?

- Non-Discretionary Access Control is an access control model in which access rules are closely managed by security administrators, not system owners or ordinary users.

Question 20

What is packet sniffing?

- Packet sniffing is a technique used to capture and monitor network traffic, even those not meant for the listener, by setting the network interface card into promiscuous mode.

Question 21

What are some key components of Linus/Unix security?

- Patch management. Application and service configuration. Users, groups, and permissions. Chroot jail.

Question 22

How does penetration testing help in ensuring system security?

- Pentration testing helps in identifying vulnerabilities in the system that can be exploited by attackers, and helps in determining the effectiveness of security measures in place.

Question 23

What is penetration testing?

- Penetrating testing is a method of testing the security of IT systems by attempting to breach the security of the system, using the same tools and techniques as an adversary might.

Question 24

What is the difference between persistent malware and transient malware?

- Persistent malware is installed in persistent storage while transient malware is installed in volatile memory such as RAM.

Question 25

What is phishing and how does it exploit social engineering?

- Phishing is a type of information theft that exploits social engineering by masquerading as communication from a trusted source to trick the user into revealing sensitive information such a s login credentials. It can be done through spam emails, fake websites or spear-phishing.

Question 26

What is phishing and how can it be prevented?

- Phishing is a type of social engineering attack where attacks attempt to trick users into divulging sensitive information such as login credentials or financial data. It can be prevented by educating users on how to identify and avoid phishing emails, using spam filters and anti-phishing software, and implementing multi-factor authentication.

Question 27

What is the difference between physical and logical access control?

- Physical access control restricts access to physical resources such as doors, elevators, and parking lots using smart cardsm or similar technologies. Logical access control, on the other hand, focuses on managing access to computer systems and applications, monitoring user activity, and restraining user behaviour.

Question 28

What are the four elements of prevention for malware?

- Policy, Awareness, Vulnerability mitigation, and Threat mitigation

Question 29

What is the ideal solution to the threat of malware?

- Prevention

Question 30

Why is privileged access necessary for mainitng access in the cyber attack process?

- Privileged access is necessary for maintaining access becaue it allows the attackers to move freely within the environment and gain control over the network.

Question 31

What is ransomware and what tactics does it use to pressure vicitms to pay the ransom?

- Ransomware is malware that encrypts a large number of files and demands a ransom payment in Bitcoin to recover them. It may threaten to publish sensitive personal information or permanently destroy the encryption key after a short period of time to increase the pressure on the victim to pay up.

Question 32

What is Role-based access control (RBAC)?

- RBAC controls access based on the roles that users have within the system and on rules statign what accesses are allowed to users in given roles.

Question 33

How does Role-based access control (RBAC) work?

- RBAC uses specific rules that indicate what can and cannot happen between a subject anf an object, and before a subject can access an object in a certain circumstance, it must meet a set of predefined rules.

Question 34

What is risk?

- Risk is the potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.

Question 35

What is RSA?

- RSA (Rivest-Shamir-Aldleman) is a public key cryptosystem.

Question 36

What is sandbox analysis?

- Running potentially malicious code in an emulated sandbox or on a virtual machine.

Question 37

What are the functions provided by S/MIME?

- S/MIME provides the ability to sign and /or encrypt e-mail messages.

Question 38

What is S/MIME?

- S/MIME stands for Secure/Multipurpose Internet Mail Extension and is a security enhancement to the MIME Internet e-mail format.

Question 39

What is the difference between scanning and enumeration in the cyber attack process?

- Scanning involves identifying entry points by scanning the organization’s networks while enumeration involves actively counting vulnerabilities and assessing potential attacks and threats to the target system.

Question 40

In which type of web applications are XSS attacks commonly seen?

- Scripted web applications

Question 41

What is second-order injection?

- Second-order injection is a type of injection attack where a malicious user could rely on data alreay present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself.

Question 42

What is the first critical step in securing a system?

- Securing the base operating system

Question 43

What is a major security concern when augmenting or replacing on-premises systems with cloud computing?

- Security is a major concern when augmenting or replacing on-premises systems with cloud services.

Question 44

What is the final step in the process of initially securing the base operating system?

- Security testing

Question 45

What should be done following the initial hardening of the system?

- Security testing

Question 46

What are the three logical components of an Intrusion Detection System (IDS)?

- Sensors, Analysers and User Interface

Question 47

What are the three components of MIDS?

- Sensors, Management servers and Management consoles

Question 48

What is the difference between session hijacking and session theft attacks?

- Session hijacking involves an attacker taking control of or modifying any communications between two hosts whereas session theft attacks involve an attacker creating new sessions or utilizing old sessions without intercepting or injecting data into existing communications.

Question 49

What is session hijacking?

- Session hijacking is an attack where an attacker takes control of where an attacker takes control of or modifies any communications between two hosts.

Question 50

What is session hijack?

- Session hijacking is an attack where an attacker takes control of where an attacker takes control of or modifies any communications between two hosts. This can be anything from a Telnet session, a domain name lookup to a local user’s keystrokes.

Question 51

What is a circuit-level gateway?

- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host. Relays TCP segments from one connection to the other without examining contents. Typically used when inside users are trusted.

Question 52

What is the advantage of a packet filtering firewall?

- Simplicity, Typically transparent to users and are very fast.

Question 53

What is social engineering and how can it be prevented?

- Social engineering is the use of deception or manipulation to gain access to sensitive information or systems. It can be prevented by educating users on how to identify and avoid social engineering tactics, implementing security protocols such as multi-factor authentication, and conducting regular security awareness training.