Securing the Network and Services

Question 1

What are the two main functions of IPsec?

- The main two functions of IPsec are a combined authentication/encryption function called Encapsulating Security Payload (ESP) and a key exchange function.

Question 2

What are the two risk factors consequence categories used in risk analysis?

- The two risk consequence categories used in risk analysis are impact and likelihood.

Question 3

What are the two types of penetration testing?

- The two types of pentration testing are whitebox testing where full information about the target is shared with the testers, and blackbox testing where no information is shared with the testers about the internals of the target.

Question 4

What are the three independent dimensions of a cryptographic system?

- The type of operations used for transforming plaintext to ciphertext, the number of keys used, and the way in which the plaintext is processed are the three independent dimensions of a cryptographic system.

Question 5

What are the types of penetration testing?

- The types of penetration testing are whitebox testing and black testing.

Question 6

What is the ultimate plan for any security practitioner in terms of securing all assets of their organization?

- The ultimate plan is to secure all assets of the organization.

Question 7

What is the World Wide Web, and how does it run over the Internet?

- The world wide web is a client/server application running over the internet and TCP/IP interanets.

Question 8

How are smart cards used in physical access control?

- They are programmed with an ID number and used to control access to physical resources such as parking lots, elevatorsm and office doors.

Question 9

Why are macro and scripting viruses threatening?

- They infect user documents rather than system programs making traditional file system access controls of limited use in preventing their spread, and are much easier to write or modify than traditional executable viruses.

Question 10

What is the role of software developers in addressing the known areas of concern related to insecure software code?

- They should place emphasis on addressing three issues and writing more secure program code.

Question 11

What information is typically logged by a NIDS sensor?

- Timestamp, connection/session ID, event/alert type, rating, network/transport/application, layer protocols, source/destination IP addresses, source/destination TCP or UDP ports or ICMP types and codes, number of bytes transmitted over the connection, and decoded payload data such as application requests and responses.

Question 12

What is the purpose of a firewall?

- To establish a controlled link between a premises network and the Internet and to protect LANs.

Question 13

What is the purpose of logging?

- To provide a record of system activity for security monitoring and analysis.

Question 14

What is the difference between transport mode and tunnel mode in IPsec?

- Transport mode provides protection primarily for upper-layer protocols while tunnel mode provides protection to the entire IP packet.

Question 15

What is UDP and what are some of its characteristics?

- UDP is a transport layer protocol that is lightweight and connectionless, with small packet sizes and no connnection to create and maintain. It provides more control over when data is sent but does not compensate for loss of packet or deliver packets in order, and does not check if the network is busy.

Question 16

What are the privacy issues in biometrics?

- Unauthorized access to biometric data can lead to misuse as it is intrinsic to people and digitally recorded and stored.

Question 17

Name three critical web application security flaws related to insecure software code.

- Unvalidated input, Injection flaws and Cross-site scripting.

Question 18

What is one of the most common failings in software security?

- Unvalidated input

Question 19

What is User Provisioning?

- User provisioning is the process of granting access to new employees. It may include checking management approvals for granting access.

Question 20

What does authentication do in cryptosystems?

- Verifies the claimed identity of system users.

Question 21

How does the security kernel enforce access control?

- When a subject requests access to an object, the security kernel intercepts the request and refers to its rules base or security kernel database to determine access rights. Access rights are set according to the policies an organization has defined. The kernel then allows or denies acces based on the defined access rules and all access requests handled by the system are logged for later tracking and analysis.

Question 22

What are the benefits of implementing IPsec in a firewall or router?

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

Question 23

What is whitebox testing?

- Whitebox testing is a type of testing in which full information about the target is shared with the testers.

Question 24

What are some characteristics of worms?

- Worms are multiplatform, multi-exploit, ultrafast spreading, polymorphic, metamorphic and can exploit zero-day vulnerabilities.