Question 11

Not yet answered

Marked out of 2

Flag question

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization. How would you prevent such type of attacks?

Select one:

- a. Hire the people through third-party job agencies who will vet them for you
- b. Conduct thorough background checks before you engage them
- c. Investigate their social networking profiles
- d. It is impossible to block these attacks

Clear my choice

Question 12

Not yet answered

Marked out of 2

Flag question

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

Select one:

- a. Digital signature
- b. Hash value
- c. Digital certificate
- d. Private key

Question 13

Not yet answered

Marked out of 2

Flag question

Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

Select one:

- a. Disconnect the email server from the network
- b. Leave it as it Is and contact the incident response te3m right away
- c. Migrate the connection to the backup email server
- d. Block the connection to the suspicious IP Address from the firewall

Clear my choice

Question 14

Not yet answered

Marked out of 2

Flag question

TCP SYN Flood attack uses the three-way handshake mechanism.
1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism. system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.
This status of client B is called _____

Select one:

- a. xmas-open
- b. half-closed
- c. half open
- d. full-open

Question 15

Not yet answered

Marked out of 2

Flag question

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

Select one:

- a. ACK flag scanning
- b. UDP Scanning
- c. IP Fragment Scanning
- d. Inverse TCP flag scanning

Clear my choice

Question 16

Not yet answered

Marked out of 2

Flag question

Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company. She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture. What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

Select one:

- a. The employee used steganography to hide information in the picture attachments
- b. The Kiley Innovators employee used cryptography to hide the information in the emails sent
- c. The method used by the employee to hide the information was logical watermarking
- d. By using the pictures to hide information, the employee utilized picture fuzzing

Clear my choice

Question 17

Not yet answered

Marked out of 2

Flag question

Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

Select one:

- a. Configure Port Security on the switch
- b. Configure Port Recon on the switch
- c. Configure Switch Mapping
- d. Configure Multiple Recognition on the switch

Clear my choice

Question 18

Not yet answered

Marked out of 2

Flag question

SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

Select one:

- a. A large number of SYN packets appearing on a network with the corresponding reply packets
- b. The source and destination address having the same value
- c. A large number of SYN packets appearing on a network without the corresponding reply packets
- d. The source and destination port numbers having the same value

Question 19

Not yet answered

Marked out of 2

Flag question

During the process of encryption and decryption, what keys are shared?

Select one:

- a. User passwords
- b. Public and private keys
- c. Public keys
- d. Private keys

Clear my choice

Question 20

Not yet answered

Marked out of 2

Flag question

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

Select one:

- a. Data items and vulnerability scanning
- b. Reviewing the firewalls configuration
- c. Source code review
- d. Interviewing employees and network engineers

Question 21

Not yet answered

Marked out of 2

Flag question

What is the main security service a cryptographic hash provides?

Select one:

- a. Message authentication and collision resistance
- b. Integrity and collision resistance
- c. Integrity and ease of computation
- d. Integrity and computational in-feasibility

Clear my choice

Question 22

Not yet answered

Marked out of 2

Flag question

Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

Select one:

- a. External Scanning
- b. Port Scanning
- c. Vulnerability Scanning
- d. Single Scanning

Question 23

Not yet answered

Marked out of 2

Flag question

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database?

Select one:

- a. Jimmy can submit user input that executes an operating system command to compromise a target system
- b. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access
- c. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database
- d. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system

Clear my choice

Question 24

Not yet answered

Marked out of 2

Flag question

Developers at your company are creating a web application which will be available for use by anyone on the Internet. The developers have taken the approach of implementing a Three-Tier Architecture for the web application. The developers are now asking you which network should the Presentation Tier (frontend web server) be placed in?

Select one:

- a. DMZ network
- b. Internal network
- c. isolated vlan network
- d. Mesh network

Question 25

Not yet answered

Marked out of 2

Flag question

The network team has well-established procedures to follow for creating new rules on the firewall. This
includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

Select one:

- a. Monitor all traffic using the firewall rule until a manager can approve it.
- b. Immediately roll back the firewall rule until a manager can approve it
- c. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager
  approval as soon as possible.
- d. Have the network team document the reason why the rule was implemented without prior manager
  approval.

Question 1

Not yet answered

Marked out of 2

Flag question

Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

Select one:

- a. Do not back up either the credit card numbers or then hashes
- b. Hire a security consultant to provide direction.
- c. Encrypt backup tapes that are sent off-site
- d. Back up the hashes of the credit card numbers not the actual credit card numbers

Clear my choice

Question 2

Not yet answered

Marked out of 2

Flag question

Which of the following steps for risk assessment methodology refers to vulnerability identification?

Select one:

- a. Determines if any flaws exist in systems, policies, or procedures
- b. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
- c. Assigns values to risk probabilities; Impact values
- d. Identifies sources of harm to an IT system. (Natural, Human. Environmental)

Question 3

Not yet answered

Marked out of 2

Flag question

Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

Select one:

- a. Dumpster Diving
- b. Scanning
- c. Competitive Intelligence Gathering
- d. Garbage Scooping

Clear my choice

Question 4

Not yet answered

Marked out of 2

Flag question

How do you defend against ARP Spoofing?

Select one:

- a. Place static ARP entries on servers, workstation and routers
- b. Use private VLANS
- c. Use ARPWALL system and block ARP spoofing attacks
- d. All of the above

Question 5

Not yet answered

Marked out of 2

Flag question

These hackers have limited or no training and know how to use only basic techniques or tools.
What kind of hackers are we talking about?

Select one:

- a. Script Kiddies
- b. White-Hat Hackers
- c. Gray-Hat Hacker
- d. Black-Hat Hackers A

Clear my choice

Question 6

Not yet answered

Marked out of 2

Flag question

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

Select one:

- a. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
- b. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography
- c. Symmetric encryption allows the server to securely transmit the session keys out-of-band
- d. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail

Clear my choice

Question 7

Not yet answered

Marked out of 2

Flag question

What are the limitations of Vulnerability scanners?

Select one:

- a. The more vulnerabilities detected, the more tests required
- b. They are highly expensive and require per host scan license
- c. The scanning speed of their scanners are extremely high
- d. There are often better at detecting well-known vulnerabilities than more esoteric (intended) ones

Question 8

Not yet answered

Marked out of 2

Flag question

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

Select one:

- a. Reverse Engineering
- b. Spoofing Identity
- c. Social Engineering
- d. Reverse Psychology

Clear my choice

Question 9

Not yet answered

Marked out of 2

Flag question

This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

Select one:

- a. IP Routing or Packet Dropping
- b. IDS Spoofing or Session Assembly
- c. IP Fragmentation or Session Splicing
- d. IP Splicing or Packet Reassembly

Question 10

Not yet answered

Marked out of 2

Flag question

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail.
What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

Select one:

- a. Integrity
- b. Authentication
- c. Confidentiality
- d. Non-Repudiation

Clear my choice