**Question 3**

Answer saved

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 4**

Answer saved

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. Interviewing employees and network engineers

○ b. Source code review

○ c. Reviewing the firewalls configuration

◉ d. Data items and vulnerability scanning

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. Identifies sources of harm to an IT system. (Natural, Human. Environmental)

○ d. Assigns values to risk probabilities; Impact values

Clear my choice

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. Digital certificate

○ c. Hash value

○ d. Private key

Clear my choice

Question 7

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 without the corresponding reply packets

○ b. The source and destination port numbers having the same value

○ c. The source and destination address having the same value

○ d. A large number of SYN packets appearing on a network with the corresponding reply packets

Clear my choice

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. Back up the hashes of the credit card numbers not the actual credit card numbers

○ c. Encrypt backup tapes that are sent off-site

◉ d. Hire a security consultant to provide direction.

Clear my choice

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

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. Have the network team document the reason why the rule was implemented without prior manager approval.

○ 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. Immediately roll back the firewall rule until a manager can approve it

Clear my choice

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. Confidentiality

○ b. Integrity

○ c. Authentication

● d. Non-Repudiation

Clear my choice

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

Not yet
answered

Marked out of
2

⚑ Flag
question

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

Select one:

○ a. Private keys

⦿ b. Public keys

○ c. Public and private keys

○ d. User passwords

Clear my choice

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. Mesh network

⦿ d. isolated vlan network

What is the main security service a cryptographic hash provides?

Select one:

○ a. Integrity and collision resistance

○ b. Message authentication and collision resistance

◉ c. Integrity and computational in-feasibility

○ d. Integrity and ease of computation

Clear my choice

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. Vulnerability Scanning

○ c. Single Scanning

○ d. Port Scanning

Clear my choice

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 Switch Mapping

○ b. Configure Port Recon on the switch

◉ c. Configure Port Security on the switch

○ d. Configure Multiple Recognition on the switch

Clear my choice