CSF Assignment

* Theory Questions

Q-1 What is the CIA Triad in information security?

-> The CIA Triad is a fundamental model in information security that consists of three key principles.

- Confidentiality :-
  -> Ensuring that data is accessible only to authorized individuals

- Integrity :-
  -> Ensuring data is accurate, consistent, and not altered by unauthorized users.

- Availability :-
  -> Ensuring that data and services are accessible when needed.

Q-2.

Define a network security model and its key components.

Ans.

A network security model is a framework used to protect a network from cyber threats. Key components include:

- Security Policies :-
  -> Rules defining how data and resources are protected.

- Authentication & Authorization :-
  -> Ensuring only authorized users can access resources.

- Firewalls :-
  -> Filtering and controlling incoming/outgoing network traffic.

- Encryption :-
  -> Protecting data using cryptographic techniques.

Q-3 What are the differences between symmetric and asymmetric cryptography?

Ans.

Feature	Symmetric Cryptography	Asymmetric Cryptography
Key Usage	Uses a single key for encryption & decryption	Uses a pair of public and private keys
Speed	Faster	Slower due to complex computations
Security	Less secure (key must be shared)	More secure (private key remains confidential)
Example Algorithms	AES, DES	RSA, ECC
Use Cases	Encrypting large data, VPNs	Digital signatures, SSL/TLS

Q-4. Explain the concept of a firewall and its role in cybersecurity.

Ans.

A firewall is a network security device or sofware that monitors and controls incoming and outgoing traffic based on predefined ~~sec~~ security rules.

* Roles in cybersecurity :

- Blocks unauthorized access while allowing legitimate communication.
- Prevents malware and attacks ~~form~~ from reaching internal networks.
- Can be implemented as hardware, software, or cloud-based solutions.

Q-5 What is a Trojan horse, and how does it differ from a virus?

Ans.

A Trojan horse is a type of malicious software that appears legitimate but contains harmful code. Unlike viruses, it does not self-replicate.

Feature	Trojan Horse	Virus
Self-Replication	No	Yes
Execution	Needs user to run it	Can spred automatically
Damage	Crates backdoors, steals data	Modifies and corrupts files

Q-6 Describe the purpose of digital signatures in cybersecurity.

Ans.

A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message or document

* Purpose:

- Ensures that the message is not altered (integrity)
- Confirms the sender's identity (authentication).
- Prevents repudiation, meaning the sender cannot deny sending the message.
- Uses public key cryptography (e.g., RSA, DSA).

Q-7. What is WPA2, and why is it more secure than WPA?

Ans.

WPA2 (Wi-Fi Protected Access 2) is a security protocol for wireless networks that improves upon WPA by using:

- AES (Advanced Encryption Standard) instead of the weaker TKIP used in WPA

- Stronger authentication methods such as 802.1X for enterprise security.
- Protection against brute-force attacks and replay attacks.

Q-8 How does a Denial-of-Service (DoS) attack affect a network?

Ans.

A DoS attack overwhelms a network, server, or system with excessive traffic, making it unavailable to legitimate users.

- Effects:
  -> Slows down or crashes services
  -> Disrupts business operations.
  -> Can be amplified in DDoS (Distributed DoS) attacks using multiple compromised devices.

Q-9 What are rogue access points, and how can they be mitigated?

Ans.

A rogue access point is an unauthorized Wi-Fi access point set up within a network, often used for cyberattacks.

* Mitigation strategies:

- Use Wireless Intrusion Detection Systems (WIDS) to detect unauthorized APs.
- Implement MAC address filtering and strong authentication methods.
- Regularly audit network for unauthorized devices.
- Disable unused network ports to prevent unauthorized connections.

Q-10 Explain the role of an intrusion detection system (IDS) in ~~n~~network security.

Ans.

An Intrusion Detection System (IDS) monitors network traffic for suspicious activity or security breaches.

* Roles in security :

- Detects unauthorized access attempts and cyber threats.
- Alerts administrators in real time to mitigate attacks.
- Can be classified as :

-> Network-based IDS (NIDS) :
Monitors network traffic.

-> Host-based IDS (HIDS) :
Monitors system logs and activities on individual devices.

* Practical Questions.

Q-1 How can you open the Command Prompt as an administrator using PowerShell?

Ans.

Start-Process cmd -Verb runAs

Q-2 What command is used to display the version of Windows you are running?

Ans.

winver

Q-3 How can you check your computer's IP address using the commad line?

Ans

ipconfig

Q-4 What is the purpose of the netstat command in Windows?

Ans.

The netstat command displays active network connections, listening ports, and protocol statistics. It is used for network troubleshooting

* Examples :

- netstat -a -> Lists all active connections and listening ports.
- netstat -n -> Shows connections numerically (IP instead of hostnames)
- netstat -ano -> Displays process IDs associated with connections.

Q-5 Which command allows you to list all files and directories in a specific folder?

Ans

dir

Q-6 How can you delete a file using the command line?

Ans.

del filename.extension

Q-7 What command is used to display network configuration details, including MAC address?

Ans

ipconfig /all

Q-8 Explain how to hide and unhide a folder using command-line attributes.

->

attrib +h +s +r foldername

Q-9 How do you open the Windows Firewall settings using a command?

->

firewall.cpl

Q-10 What command is used to check and repair corrupted system files in windows?

->

sfc /scannow