Q) What is the CIA triad of information security?

(a) Confidentiality, Integrity, Availability (b) Encryption, Decryption, Authentication (c) Firewalls, Antivirus, Intrusion Detection (d) Access Control, Logging, Backup

Ans) a

Q) Which type of malware encrypts files and demands ransom to decrypt them?

(a) Worm (b) Trojan (c) Spyware (d) Ransomware

Ans) d

Q) What is a phishing attack?

(a) A brute-force attack targeting passwords (b) A virus that spreads through email attachments (c) A fake website or email designed to steal personal information (d) A denial-of-service attack overwhelming a server with traffic

Ans) c

Q) What is the purpose of a firewall?

(a) To encrypt data at rest and in transit (b) To control the flow of network traffic and block unauthorized access (c) To detect and remove malware from infected systems (d) To back up data regularly in case of system failure

Ans) b

Q) What is social engineering?

(a) The use of technical vulnerabilities to exploit systems (b) The manipulation of people to reveal confidential information or take harmful actions (c) The unauthorized access or use of computer systems or data (d) The disruption or denial of authorized use of computer systems or data

Ans) b

Note - Brute-force attack

A brute force attack is a hacking technique that tries every possible combination of characters until it finds the correct one to gain unauthorized access to a system or data. Imagine it like trying every key on a ring until you find the one that unlocks the door.

- it works using Target Selection, Guessing Game and Trial & Error

Q) What is the most common way to protect against brute-force attacks?

(a) Install antivirus software (b) Use complex passwords with special characters (c) Implement multi-factor authentication (MFA) (d) Update software regularly

Ans) c

Q) What is a vulnerability?

(a) A software bug that can be exploited by attackers (b) Any weakness in a computer system or network that could be used to gain unauthorized access or disrupt operations (c) A piece of malware designed to steal data or cause damage (d) A type of cyber-attack that overwhelms a server with traffic.

Ans) b

Q) What is the purpose of penetration testing?

(a) To identify and exploit vulnerabilities in a computer system or network (b) To install security software and configure security settings (c) To train employees on cybersecurity best practices (d) To simulate a cyber-attack and identify weaknesses in security defenses

Ans) d

Q) What is the importance of data backups in cybersecurity?

(a) To recover data lost due to system failures or accidental deletion (b) To provide temporary storage for data while migrating to a new system (c) To comply with data protection regulations (d) All of the above

Ans) d

Q) Which type of encryption scrambles data in transit for secure communication?

(a) Symmetric encryption (b) Asymmetric encryption c) Hashing d) None of the above

Ans) b

Q) What is the difference between a virus and a worm?

Ans) (a) A virus needs a host program to propagate, while a worm can replicate independently. (b) A virus only targets files, while a worm can attack network devices. (c) A virus is always harmful, while a worm can be harmless. (d) There is no difference between a virus and a worm.

Ans) a

Q) What is a zero-day attack?

(a) An attack that exploits a vulnerability for which there is no known patch (b) An attack that uses social engineering to trick users into giving up their passwords (c) An attack that targets critical infrastructure systems (d) An attack that uses automated bots to launch denial-of-service attacks

Ans) a

Q) Which type of attack targets websites and online services to make them unavailable to users?

(a) Phishing attack (b) Ransomware attack (c) Denial-of-service attack (d) Man-in-the-middle attack

Ans) c

Q) What is the purpose of a secure coding standard?

(a) To ensure that software is written with security in mind (b) To standardize the coding style for improved readability (c) To automate the testing of software for bugs (d) To document the functionalities of the software

Ans) a

Q) What is the difference between an intrusion detection system (IDS) and an intrusion prevention system (IPS)?

Ans) An IDS only detects suspicious activity, while an IPS can also block it.

Q) What is a honeypot in cybersecurity?

(a) A fake website or system designed to lure and trap attackers (b) A secure storage system for sensitive data (c) A tool for encrypting data at rest and in transit (d) A type of malware that steals data silently

Ans) a

Q) What is the importance of data backups in disaster recovery?

(a) To restore data lost due to cyber-attacks (b) To quickly resume operations after a system outage (c) To comply with data retention regulations (d) All of the above

Ans) b

Q) What is a supply chain attack in cybersecurity?

Ans) An attack that targets a third-party vendor to gain access to a target organization.

Q) What is the role of security information and event management (SIEM) in cybersecurity?

Ans) To collect and analyze logs from different security tools.

Q) What is the importance of patch management in cybersecurity?

Ans) To apply security patches to software and systems promptly to fix vulnerabilities.

Q) What is the difference between physical and logical security?

Ans) Physical security protects physical assets like hardware, while logical security protects intangible assets like data.

Q) What is the benefit of using multi-factor authentication (MFA)?

Ans) Adds an extra layer of security compared to password-only authentication

Q) What is a good practice for secure email use?

Ans) Enable spam filtering and be wary of phishing attempts.