MSc Computer Applications - Cyber Security

Internal Assessment Questions & Answers

Course Code: MSC-CA-JULY-2025-SEM-1-CS-IA **Total Questions:** 25

Question 1: Threat Modeling Approaches

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-05

Question: Threat modeling approaches are --

Options: - STRIDE [CORRECT] (CORRECT) - PASTA [CORRECT] (CORRECT) - DREAD [INCORRECT] - RAID [INCORRECT]

Correct Answers: STRIDE, PASTA

Explanation: Both STRIDE and PASTA are established threat modeling methodologies. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and PASTA (Process for Attack Simulation and Threat Analysis) are industry-standard approaches for identifying and analyzing threats in system design.

Question 2: DDoS Attack Type

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-19

Question: Which attack floods servers with traffic?

Options: - Social engineering [INCORRECT] - DDoS [CORRECT] (CORRECT) - MITM [INCORRECT] - Trojan [INCORRECT]

Correct Answer: DDoS (Distributed Denial of Service)

Explanation: DDoS attacks overwhelm servers and networks by flooding them with massive amounts of traffic from multiple sources, making the service unavailable to legitimate users.

Question 3: CIA Triad Definition

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-02

Question: CIA Triad stands for _____

Options: - Control, Integrity, Access [INCORRECT] - Confidentiality, Integrity, Availability [CORRECT] (CORRECT) - Confidential, Internal, Access [INCORRECT] - Cyber, Internet, Attack [INCORRECT]

Correct Answer: Confidentiality, Integrity, Availability

Explanation: The CIA Triad is the fundamental model in cybersecurity: - **Confidentiality:** Data accessible only to authorized persons - **Integrity:** Data accuracy and completeness, not modified by unauthorized persons - **Availability:** Systems and data accessible to authorized users when needed

---

Question 4: Hackivism Definition

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-24

Question: Hacktivism best described as --

Options: - Cyber activism [CORRECT] (CORRECT) - Selling data [INCORRECT] - Protecting systems [INCORRECT] - Development [INCORRECT]

Correct Answer: Cyber activism

Explanation: Hacktivism combines "hacking" and "activism" to describe the use of hacking techniques for political or social purposes, typically to promote social change or protest against organizations.

Question 5: Critical Infrastructure

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-11

Question: Critical infrastructure includes _____

Options: - Social media apps [INCORRECT] - Power & water systems [CORRECT] (CORRECT) - Gaming servers [INCORRECT] - Phones [INCORRECT]

Correct Answer: Power & water systems

Explanation: Critical infrastructure refers to essential systems vital to national security and public health, including power grids, water treatment facilities, transportation networks, and communication systems.

Question 6: CI Attacks and Critical Services

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-18

Question: CI attacks can disrupt power/water.

Options: - True [CORRECT] (CORRECT) - False [INCORRECT]

Correct Answer: True

Explanation: Attacks on critical infrastructure can cause widespread disruption. For example, compromising SCADA systems or grid control systems can lead to power outages or water supply disruptions.

Question 7: Vulnerability Definition

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-04

Question: A vulnerability is _____

Options: - A possible attack [INCORRECT] - A weakness in system [CORRECT] (CORRECT) - An attacker [INCORRECT] - Phishing mail [INCORRECT]

Correct Answer: A weakness in system

Explanation: A vulnerability is a weakness or flaw in a system's security that can be exploited by attackers to gain unauthorized access or cause harm.

Question 8: Common Security Goals

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-01

Question: Which of the following is NOT a common security goal?

Options: - Confidentiality [INCORRECT] - Integrity [INCORRECT] - Availability [INCORRECT] - Profitability [CORRECT] (CORRECT)

Correct Answer: Profitability

Explanation: The three common security goals are Confidentiality, Integrity, and Availability (CIA Triad). Profitability is a business objective, not a security goal.

Question 9: Availability Goal

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-15

Question: Goal of availability _____

Options: - Prevent alteration [INCORRECT] - Ensure accessibility [CORRECT] (CORRECT) - Encrypt data [INCORRECT] - Restrict access [INCORRECT]

Correct Answer: Ensure accessibility

Explanation: Availability ensures that systems, data, and services are accessible to authorized users whenever needed, preventing unauthorized disruptions.

Question 10: Botnets Primary Use

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-06

Question: Botnets are primarily used for --

Options: - Updates [INCORRECT] - Coordinated attacks [CORRECT] (CORRECT) - Backups [INCORRECT] - Authentication [INCORRECT]

Correct Answer: Coordinated attacks

Explanation: Botnets are networks of compromised computers controlled by attackers to perform coordinated malicious activities like DDoS attacks, spam distribution, and large-scale cyber attacks.

Question 11: Attack Motivations

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-21

Question: Motivations for attacks --

Options: - Financial [CORRECT] (CORRECT) - Political [CORRECT] (CORRECT) - Revenge [CORRECT]

(CORRECT) - System updates [INCORRECT]

Correct Answers: Financial, Political, Revenge

Explanation: Attackers are motivated by various factors: - **Financial:** Stealing money, data, or resources for profit - **Political:** Advancing political agendas or ideologies - **Revenge:** Personal grievances or retaliation - System updates is a maintenance activity, not an attack motivation

---

Question 12: Athens Affair Attack Type

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-09

Question: The Athens Affair involved _____

Options: - Banking fraud [INCORRECT] - Telecom wiretapping [CORRECT] (CORRECT) - Crypto theft [INCORRECT] - Malware infection [INCORRECT]

Correct Answer: Telecom wiretapping

Explanation: The Athens Affair (2004-2005) involved illegal wiretapping of high-ranking Greek officials' mobile phones through the Vodafone Greece network, exploiting security vulnerabilities in the telecommunications infrastructure.

Question 13: Athens Affair Discovery

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-23

Question: Cyber espionage is motivated by _____

Options: - Advertising [INCORRECT] - Intelligence gathering [CORRECT] (CORRECT) - Entertainment [INCORRECT] - Education [INCORRECT]

Correct Answer: Intelligence gathering

Explanation: Cyber espionage involves unauthorized access to sensitive information for intelligence purposes, conducted by nation-states, organizations, or groups to gain competitive or strategic advantages.

Question 14: Espionage Signs

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-25

Question: Signs of espionage --

Options: - Data exfiltration [CORRECT] (CORRECT) - Zero-days [INCORRECT] - Long-term infiltration [CORRECT] (CORRECT) - Weak passwords [INCORRECT]

Correct Answers: Data exfiltration, Long-term infiltration

Explanation: Indicators of espionage activities include: - **Data exfiltration:** Unauthorized extraction and transfer of sensitive data - **Long-term infiltration:** Persistent presence in systems over extended periods for continuous intelligence gathering

---

Question 15: Estonia Attack Targets (2007)

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-22

Question: 2007 Estonia attack targeted _____ sites.

Options: - Banking [INCORRECT] - Education Sector [INCORRECT] - Healthcare [INCORRECT] - None of the Mentioned [CORRECT] (CORRECT)

Correct Answer: None of the Mentioned

Explanation: The 2007 Estonia cyberattacks (attributed to Russian actors) primarily targeted government, media, and financial sectors. The attack was broader and not limited to single sector categories listed.

Question 16: Threat Actor Definition

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-16

Question: Threat actor means --

Options: - System patch [INCORRECT] - Person attacking [CORRECT] (CORRECT) - Firewall [INCORRECT] - Antivirus [INCORRECT]

Correct Answer: Person attacking

Explanation: A threat actor is any individual or entity that conducts or attempts cyberattacks, including hackers, criminal organizations, nation-states, insiders, and hacker groups.

Question 17: Botnet Scale

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-14

Question: Botnets can have millions of devices.

Options: - True [CORRECT] (CORRECT) - False [INCORRECT]

Correct Answer: True

Explanation: Modern botnets can compromise millions of devices globally. For example, Mirai botnet infected over 600,000 devices, demonstrating the massive scale possible in coordinated cyberattacks.

Question 18: Threat Modeling Benefits

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-03

Question: Threat modeling helps identify attackers and capabilities.

Options: - True [CORRECT] (CORRECT) - False [INCORRECT]

Correct Answer: True

Explanation: Threat modeling is a systematic process that identifies potential attackers (threat actors), their capabilities, motivations, and methods of attack on a system, enabling better security design and defense strategies.

Question 19: Athens Affair Discovery Method

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-23

Question: Athens Affair found due to unusual logs.

Options: - True [CORRECT] (CORRECT) - False [INCORRECT]

Correct Answer: True

Explanation: The Athens Affair was discovered when Vodafone security team detected unusual system activities and anomalous network logs indicating unauthorized access and wiretapping activities.

Question 20: Common Cyber Threats

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-17

Question: Common cyber threats --

Options: - Malware [CORRECT] (CORRECT) - Phishing [CORRECT] (CORRECT) - Insider threats [CORRECT] (CORRECT) - Floods [INCORRECT]

Correct Answers: Malware, Phishing, Insider threats

Explanation: - **Malware:** Malicious software designed to damage or exploit systems - **Phishing:** Social engineering attacks via deceptive emails/messages - **Insider threats:** Risks from authorized users abusing access privileges - Floods refer to infrastructure attacks, not individual cyber threats

---

Question 21: Payroll System Classification

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA-01-01 (Additional)

Question: Payroll systems are typically classified under which infrastructure category?

Correct Answer: Critical Infrastructure / Sensitive Business Systems

Explanation: Payroll systems handle sensitive employee financial data and are critical for business operations, requiring protection under data security and business continuity frameworks.

Question 22: Defense in Depth Strategy

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA (Related)

Question: Multiple layers of security controls are part of:

Correct Answer: Defense in Depth

Explanation: Defense in Depth is a security strategy using multiple overlapping defenses (firewalls, intrusion detection, authentication, encryption) so that if one layer is compromised, others still provide protection.

Question 23: Zero-Day Vulnerability

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA (Related)

Question: A zero-day vulnerability is:

Correct Answer: An unknown security flaw exploited before vendor awareness or patch availability

Explanation: Zero-day exploits target vulnerabilities unknown to software vendors, making them particularly dangerous as no patches or defenses exist at the time of exploitation.

Question 24: SCADA Systems

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA (Related)

Question: SCADA systems are used in:

Correct Answer: Industrial Control Systems for critical infrastructure

Explanation: SCADA (Supervisory Control and Data Acquisition) systems monitor and control industrial processes in power plants, water treatment, manufacturing, and other critical infrastructure.

Question 25: Social Engineering

Question ID: MSC-CA-JULY-2025-SEM-1-CS-IA (Related)

Question: Social engineering attacks primarily exploit:

Correct Answer: Human psychology and trust

Explanation: Social engineering attacks manipulate people into divulging confidential information or performing security-breaching actions, exploiting human psychology rather than technical vulnerabilities.

Summary Statistics

| Category | Count | |----------|-------| | Total Questions | 25 | | Multiple Choice | 20 | | True/False | 4 | | Multiple Select | 3 | | Coverage Topics | Threat Modeling, DDoS, CIA Triad, Botnets, Espionage, Critical Infrastructure, Cyber Attacks, Threat Actors |

Key Takeaways

1. **Threat Modeling:** Essential for identifying security risks early 2. **CIA Triad:** Foundation of all security objectives 3. **Attack Types:** Diverse methods including DDoS, phishing, malware, and espionage 4. **Infrastructure Protection:** Critical systems require special attention 5. **Threat Actors:** Various motivations from financial to political 6. **Defense Strategy:** Multiple layers and continuous monitoring required

---

Document Version: 1.0 **Date:** December 11, 2025 **Course:** MSc Computer Applications - Cyber Security

Institution: Symbiosis Online University

Part 2

MSc CA - Information Security & Cybersecurity

Internal Assessment - Complete Q&A Guide

SECTION 15: Multilateral Security

Question: STATE True/False: Multilateral security considers all parties' interests.

Answer: **TRUE** [CORRECT]

SECTION 16: Information Technology Act, 2000

Question: The Information Technology Act, 2000 in India primarily deals with:

Answer: **Digital signatures, cybercrimes & electronic records** [CORRECT]

SECTION 17: Copyright Protection

Question: Copyright protects _____.

Answer: **Expression of ideas** [CORRECT]

Explanation: Copyright protects the original expression of ideas (creative works, software, written content, etc.), not the ideas themselves.

SECTION 18: Software Patenting

Question: Software patenting protects:

Answer: **Novel software inventions** [CORRECT]

SECTION 19: Security Policies

Question: Security policies define _____.

Answer: **What is allowed** [CORRECT]

Explanation: Security policies establish rules and guidelines defining what is permitted within an organization's security framework.

SECTION 20: Computer Misuse Legislation

Question: Computer misuse legislation aims to prevent:

Answer: **Misuse of systems** [CORRECT]

SECTION 21: Cyber Laws

Question: STATE True/False: Cyber laws regulate online activities.

Answer: **TRUE** [CORRECT]

SECTION 22: Privacy Control

Question: Privacy ensures control over one's personal _____.

Answer: **Data** [CORRECT]

Explanation: Privacy is about maintaining control over personal data and preventing unauthorized access or misuse of one's information.

SECTION 23: Data Protection

Question: Data protection involves:

Answer: **Safeguarding personal data** [CORRECT]

Explanation: Data protection involves implementing measures and policies to secure and protect personal data from unauthorized access, breaches, and misuse.

SECTION 24: Management of Malicious Intent

Question: Management of malicious intent involves:

Answer: **Identifying threats** [CORRECT]

Explanation: Proper threat management requires proactive identification, detection, and analysis of security threats and malicious activities.

SECTION 26: Network Security Focus

Question: Network security focuses on:

Answer: **Protecting data in transit** [CORRECT]

Explanation: Network security primarily ensures the confidentiality, integrity, and availability of data as it moves

across networks and communication channels.

Summary of Key Concepts

Security Fundamentals - **Data Protection:** Safeguarding sensitive information from unauthorized access - **Privacy:** Control over personal data and information - **Encryption:** Method to ensure confidentiality

Legal Framework - **IT Act 2000:** India's primary law for digital crimes and electronic records - **Copyright:** Protects expression of creative ideas - **Patents:** Protect novel software inventions - **Computer Misuse Laws:** Prevent unauthorized system access

Security Practices - **Security Policies:** Define what is permitted (allow/deny rules) - **Threat Identification:** Core of malicious intent management - **Network Security:** Focus on data protection in transit - **Multilateral Security:** Considers interests of all stakeholders

---

Study Tips for MSc CA

1. **Understand the distinction** between ideas (not protected) and expression of ideas (protected by copyright) 2. **Remember IT Act 2000** covers digital signatures, cybercrimes, and electronic records 3. **Security vs Privacy:** Security is about protection; Privacy is about control 4. **Policies define the rules** - what's allowed and what's not 5. **Threat management** is proactive - focus on identification 6. **Network security** protects data while it travels across networks

---

Document Version: Complete Internal Assessment Q&A Guide **Created:** December 26, 2025 **Course:** MSc CA - Cybersecurity and Information Security **Institution:** Symbiosis Online University