Q1

What is identity theft?

Q2

What is the Internet of Things (IoT)?

Q3

What is Big Data?

Q4

Differentiate between personal data and organizational data.

Q5

Mention three things attackers may want to steal.

Q6

Q7

Differentiate between White Hat and Grey Hat attackers.

Q8

Differentiate between Grey Hat and Black Hat attackers.

Q9

What is a Script Kiddie?

Q10

What is a State-Sponsored attacker?

Q11

Mention three types of malware.

Q12

What is Spyware?

Q13

What is Adware?

Q14

What is Ransomware?

Q15

Differentiate between a Virus and a Worm.

Q16

Define Social Engineering.

Q17

What is a Botnet?

Q18

Differentiate between DoS and DDoS attacks.

Q19

What is a security vulnerability?

Q20

What is an exploit?

Q21

Define encryption.

Q22

Draw the basic encryption and decryption process.

Q23

What is a backup and why is it important?

Q24

What is two-factor authentication (2FA)?

Q25

Differentiate between Network Security and Network Forensics.

Q26

Rewrite this table and classify each behavior as **Normal, Suspicious, or Highly Suspicious**. Then identify the main indicator.

Behavior	Classification	Indicator	Reason
A student logs into the LMS at 10:00 AM from a university lab and downloads lecture notes.			
The HR_Manager account accesses employee records and transfers 450 MB to an unknown external IP.			
A workstation contacts a DNS server before opening the university website.			
Network_Admin signs in at 2:20 AM and disables antivirus protection.			
Security logs disappear shortly after a large outbound transfer.			

Q27

Rewrite this table and classify each behavior as **Normal, Suspicious, or Highly Suspicious**.

Behavior	Classification	Indicator	Reason
A lecturer uploads course materials from their office computer.			
Finance_Manager transfers 600 MB of payroll data to an unfamiliar external address.			
A device performs a DNS lookup before opening Gmail.			

Behavior	Classification Indicator Reason
System_Admin logs in at 3:45 AM and stops the IDS service.	
Audit logs are removed after a large file upload.	

Q28

For each situation, identify whether it is a problem of **Confidentiality, Integrity, or Availability**. Explain your reason.

1. An attacker reads private emails exchanged between managers.
2. A student changes marks in the grading system.
3. A hospital website is unavailable due to a server outage.
4. An employee accesses payroll data without authorization.
5. A project document is modified before reaching management.

Q29

For each situation, identify whether it is a problem of **Confidentiality, Integrity, or Availability**.

1. A hacker intercepts customer messages.
2. A database record is accidentally altered.
3. An online banking service becomes unavailable.
4. A nurse accesses unrelated patient records.
5. Source code is modified before deployment.

Q30

Scenario: A student downloads a free application that appears normal but secretly records everything typed on the keyboard.

a. What is the most likely malware type?
b. Which McCumber Cube security principle is affected?
c. What is the data state of the password while it is being typed?
d. Which protection method would reduce the risk most?
e. Explain what happened in two sentences.

Q31

Scenario: A free PDF converter works correctly but secretly sends copies of documents to an external server.

a. What is the most likely malware type?
b. Which McCumber Cube principle is affected?
c. What is the data state while the files are being sent?
d. Which protection method would reduce the risk most?
e. Explain what happened.

Q32

Scenario: A free media player floods the browser with advertisements and prevents normal use.

a. What is the most likely malware type?
b. Which CIA principle is mainly affected?
c. What is the data state of the advertisements while downloading?
d. Which protection method would reduce the risk most?
e. Give advice to the user.

Q33

A company stores customer records in a database.

Use the McCumber Cube to identify:

- Security principle
- Data state
- Protection method

Q34

A university sends student grades by email.

Use the McCumber Cube to identify:

- Security principle
- Data state

- Protection method

Q35

A hospital keeps patient records in a database and wants to prevent unauthorized changes.

Use the McCumber Cube to identify:

- Security principle
- Data state
- Protection method

36- Differentiate between network security and network forensics.
37-What is the function of a switch?
38-What is the function of a router?
39-What is the function of a firewall?
40-What is an Intrusion Detection System (IDS)?
41-What is an Intrusion Prevention System (IPS)?