Information Security
Multiple Choice Questions

Cybersecurity Assessment

September 19, 2025

Contents

1 Instructions

- This document contains 100 multiple choice questions on Information Security
- Each question has 4 options (A, B, C, D)
- The correct answers are highlighted in **red bold text**
- Questions are divided into two sets of 50 each

2 First Set - Questions 1-50

2.1 Question 1

Which of the following best defines Information Security?

A) Preventing physical access to data

B) **Securing information that is in a digital format**

C) Creating backups of all files

D) Restricting access to social media accounts

2.2 Question 2

Which of the following is not a part of the CIA triad?

A) Confidentiality

B) Integrity

C) **Accessibility**

D) Availability

2.3 Question 3

Which of the following is a violation of confidentiality?

A) Encrypting sensitive data

B) Deleting critical files

C) **Allowing unauthorized access to sensitive information**

D) Correcting errors in data

2.4 Question 4

Integrity ensures that:

A) Data is protected from unauthorized access

B) **Data is accurate and reliable**

C) Data is available when needed

D) Data is encrypted in transit

2.5 Question 5

The availability aspect of the CIA triad focuses on:

A) Preventing unauthorized access to systems

B) **Ensuring systems are accessible to authorized users**

C) Encrypting sensitive data in transit

D) Detecting unauthorized modifications to files

2.6 Question 6

A DDoS attack affects which aspect of the CIA triad?

A) Confidentiality

B) Integrity

C) **Availability**

D) Accessibility

2.7 Question 7

Which malware type spreads without user intervention?

A) Virus

B) **Worm**

C) Trojan horse

D) Rootkit

2.8 Question 8

Swiss cheese infection refers to:

A) Infecting system files

B) **Scrambling virus code and placing parts randomly in host programs**

C) Encrypting the virus payload

D) Infecting multiple devices simultaneously

2.9 Question 9

The Carbanak malware used in bank attacks provided access to:

A) The bank's database systems

B) **Employee computers used for cash transfer systems**

C) Bank customer accounts

D) ATM systems directly

2.10 Question 10

What attack was used in the Sony data breach of 2011?

A) Malware infection

B) DDoS attack

C) **SQL Injection**

D) Phishing attack

2.11 Question 11

Viruses cannot spread automatically and rely on:

A) Internet connections

B) **User actions, such as opening an email attachment**

C) Exploiting network vulnerabilities

D) Using admin privileges to copy themselves

2.12 Question 12

Polymorphic malware uses:

A) **Constantly changing encryption techniques to avoid detection**

B) Only one method of attack

C) Hardware vulnerabilities to gain access

D) System memory to store data

2.13 Question 13

Metamorphic viruses differ from polymorphic ones because they:

A) Use the same code structure for every attack

B) **Change their internal code without altering the functionality**

C) Cannot replicate on their own

D) Only attack executable files

2.14 Question 14

The ILOVEYOU virus caused damage by:

A) Infecting databases

B) **Overwriting files like JPEGs and MP3s**

C) Sending ransomware demands

D) Destroying operating system files

2.15 Question 15

Which of the following best describes a rootkit?

A) **A type of malware that hides its presence from detection tools**

B) A virus that spreads through emails

C) A Trojan horse that steals login credentials

D) An exploit that corrupts hardware components

2.16 Question 16

Script kiddies are typically:

A) Highly skilled hackers with in-depth system knowledge

B) **Individuals who use automated tools for attacks**

C) Hackers who work for governments

D) Programmers who develop malware

2.17 Question 17

Brokers are attackers who:

A) **Sell vulnerabilities to the highest bidder**

B) Write malicious software for personal use

C) Protect systems from hackers

D) Launch denial-of-service attacks

2.18 Question 18

The Cyber Kill Chain includes all of the following steps except:

A) Reconnaissance

B) Weaponization

C) **Mitigation**

D) Delivery

2.19 Question 19

White hat hackers:

A) Violate systems for financial gain

B) **Perform penetration tests to find vulnerabilities**

C) Cause malicious damage to systems

D) Sell exploits on the black market

2.20 Question 20

Advanced Persistent Threats (APTs) are primarily characterized by:

A) Immediate disruption of services

B) **Long-term, undetected access to sensitive data**

C) Frequent password attacks

D) Use of ransomware

2.21 Question 21

Which of the following security principles ensures that information is available to authorized users at all times?

A) Confidentiality

B) Integrity

C) **Availability**

D) Authenticity

2.22 Question 22

Encryption is primarily used to protect:

A) The availability of data

B) **The confidentiality of data**

C) The integrity of hardware

D) The functionality of software

2.23 Question 23

A macro virus typically infects:

A) Executable files

B) **Document files like Word or Excel**

C) Network configurations

D) Web browsers

2.24 Question 24

The CompTIA Security+ certification focuses on:

A) Ethical hacking

B) Physical security

C) **Foundation-level security skills**

D) Cloud-based security

2.25 Question 25

Confidentiality breaches can result from:

A) Deleting files accidentally

B) **Unauthorized users accessing sensitive information**

C) Failing to back up data

D) Hardware failures

2.26 Question 26

Hashing is a technique used to ensure:

A) Confidentiality

B) **Integrity**

C) Availability

D) Authenticity

2.27 Question 27

Which of the following is not a category of attackers?

A) Hactivists

B) Insiders

C) Brokers

D) **Antivirus developers**

2.28 Question 28

Layering as a security principle refers to:

A) Restricting access based on job roles

B) **Using multiple levels of security controls**

C) Encrypting data at rest and in transit

D) Monitoring network traffic continuously

2.29 Question 29

Phishing attacks primarily target:

A) System vulnerabilities

B) Data encryption methods

C) **Human users through deception**

D) Wireless networks

2.30 Question 30

Which of the following is not a defense principle in cybersecurity?

A) Layering

B) Diversity

C) Limiting

D) **Fragmentation**

2.31 Question 31

A backdoor in malware allows:

A) **Access to the system without the user's knowledge**

B) Infection of other systems automatically

C) The virus to reproduce itself

D) Protection from antivirus software

2.32 Question 32

Ransomware is a type of malware that:

A) Spies on user activity

B) **Demands payment to restore access to files**

C) Infects system boot sectors

D) Corrupts network traffic

2.33 Question 33

Zero-day vulnerabilities refer to:

A) Vulnerabilities that have been publicly known for a long time

B) **Newly discovered vulnerabilities that haven't been patched yet**

C) Vulnerabilities caused by outdated software

D) Network-related vulnerabilities only

2.34 Question 34

A DoS (Denial of Service) attack is designed to:

A) Steal confidential information

B) **Deny legitimate users access to services**

C) Corrupt system files

D) Install spyware on a system

2.35 Question 35

Obscurity as a defense strategy means:

A) **Hiding internal system details from attackers**

B) Limiting the number of security layers

C) Using encryption for all data transmission

D) Simplifying system architecture

2.36 Question 36

Which malware hides its activities by modifying the operating system?

A) Spyware

B) **Rootkit**

C) Adware

D) Worm

2.37 Question 37

Man-in-the-middle attacks involve:

A) Redirecting traffic to an unauthorized server

B) Crashing systems by overloading them

C) **Spying on traffic between two parties**

D) Infecting a system via email attachments

2.38 Question 38

Phishing is often carried out via:

A) Phone calls

B) **Social engineering through email**

C) In-person attacks

D) Keylogging software

2.39 Question 39

VNC (Virtual Network Computing) malware capabilities include:

A) **Remotely viewing and controlling infected systems**

B) Stealing passwords only

C) Disabling antivirus software

D) Encrypting files for ransom

2.40 Question 40

Social engineering attacks rely on:

A) Exploiting software vulnerabilities

B) **Manipulating people into giving up sensitive information**

C) Infecting files with a virus

D) DDoS attacks on servers

2.41 Question 41

A macro virus typically spreads by:

A) Attaching itself to system files

B) **Embedding malicious code in Word or Excel documents**

C) Infecting the system boot sector

D) Spreading via email spam

2.42 Question 42

Firewalls are primarily used to:

A) Encrypt data at rest

B) **Filter traffic based on security rules**

C) Monitor user activity

D) Detect malware infections

2.43 Question 43

The Mirai botnet was used in:

A) Ransomware attacks

B) **DDoS attacks using IoT devices**

C) Phishing campaigns

D) Spyware installation

2.44 Question 44

Behavior-based detection evaluates:

A) The source code of malware

B) **The intended actions of an object before it executes**

C) The network traffic for anomalies

D) The type of encryption used

2.45 Question 45

Signature-based detection relies on:

A) **Comparing file content to known virus signatures**

B) Monitoring for unusual system behavior

C) Blocking encrypted data transmissions

D) Evaluating system configurations

2.46 Question 46

Keylogging malware is designed to:

A) Log network traffic

B) **Record keystrokes on a system**

C) Block access to websites

D) Monitor email attachments

2.47 Question 47

Which type of malware is designed to steal personal information from a system?

A) Adware

B) **Spyware**

C) Ransomware

D) Worm

2.48 Question 48

The CIA triad in information security stands for:

A) Cybersecurity, Integrity, Access

B) **Confidentiality, Integrity, Availability**

C) Control, Innovation, Access

D) Cryptography, Identity, Authorization

2.49 Question 49

Limiting as a security principle means:

A) **Restricting user access to only what they need**

B) Using a single layer of security

C) Encrypting all system data

D) Using the same passwords for all accounts

2.50 Question 50

APT attacks usually focus on:

A) Quick financial gain

B) **Long-term access to sensitive information**

C) Spreading ransomware

D) Creating network outages

3 Second Set - Questions 51-100

3.1 Question 51

Which security principle involves hiding internal system details from attackers?

A) Limiting

B) **Obscurity**

C) Diversity

D) Layering

3.2 Question 52

Diversity in security means:

A) Using multiple layers of the same type of defense

B) **Using different types of defense mechanisms in different layers**

C) Encrypting all data

D) Restricting access to certain files

3.3 Question 53

A Trojan horse is a type of malware that:

A) Replicates itself automatically

B) **Appears as legitimate software but has malicious intent**

C) Infects the boot sector of the system

D) Crashes systems by overloading memory

3.4 Question 54

Ransomware attacks primarily aim to:

A) Spy on user activity

B) Steal sensitive information

C) **Encrypt files and demand payment for decryption**

D) Hijack browsers for click fraud

3.5 Question 55

The primary difference between viruses and worms is:

A) **Worms do not need user interaction to spread**

B) Worms always cause system crashes

C) Viruses cannot cause system damage

D) Worms cannot replicate themselves

3.6 Question 56

Rootkits are designed to:

A) Replicate across systems

B) **Hide the existence of malicious processes from detection**

C) Lock users out of their systems

D) Slow down network performance

3.7 Question 57

Layering as a defense mechanism ensures that:

A) **Multiple types of defenses are in place**

B) Only the simplest defense is used

C) Systems are less vulnerable to zero-day exploits

D) Users have access to all resources

3.8 Question 58

Spyware is designed to:

A) **Monitor user activity and steal sensitive information**

B) Encrypt system files

C) Replicate through email attachments

D) Shut down the system when activated

3.9 Question 59

SQL injection is an attack that targets:

A) Web server vulnerabilities

B) **Database systems**

C) Network infrastructure

D) Authentication mechanisms

3.10 Question 60

A buffer overflow attack involves:

A) Overloading a system with traffic

B) **Exploiting improperly handled memory in software**

C) Sending phishing emails to multiple users

D) Spreading malware through USB drives

3.11 Question 61

Phishing attacks rely on:

A) Exploiting system vulnerabilities

B) **Trickery to make users divulge personal information**

C) Hijacking user sessions

D) Injecting malicious code into websites

3.12 Question 62

Which of the following is an example of social engineering?

A) A brute force attack on passwords

B) **Sending a phishing email to employees**

C) Injecting malware into a database

D) DDoS attacks on servers

3.13 Question 63

State-sponsored attackers are generally motivated by:

A) **Political and strategic goals**

B) Financial gain only

C) Disruption of small businesses

D) Crashing network infrastructure

3.14 Question 64

The primary role of a firewall is to:

A) **Block unauthorized incoming and outgoing traffic**

B) Encrypt all traffic over a network

C) Detect viruses on the system

D) Analyze software vulnerabilities

3.15 Question 65

A denial-of-service (DoS) attack is primarily aimed at:

A) Disabling antivirus software

B) Stealing user credentials

C) **Making a service unavailable to legitimate users**

D) Spreading ransomware

3.16 Question 66

Which attack is most commonly associated with data breaches?

A) **Phishing**

B) Denial of Service

C) Man-in-the-middle

D) Malware injection

3.17 Question 67

Brute force attacks focus on:

A) **Guessing passwords by trying every possible combination**

B) Sending a large amount of data to a server

C) Injecting malicious code into software

D) Gaining access to databases

3.18 Question 68

Authentication is the process of:

A) **Verifying that a user is who they claim to be**

B) Assigning user permissions to data

C) Encrypting sensitive information

D) Monitoring user activities on the network

3.19 Question 69

Encryption ensures the following for data in transit:

A) **Confidentiality**

B) Availability

C) Integrity

D) Usability

3.20 Question 70

Zero-day attacks target:

A) **Unpatched vulnerabilities**

B) Network traffic

C) Encrypted data

D) Updated software

3.21 Question 71

The CIA triad consists of:

A) Cryptography, Integrity, Availability

B) **Confidentiality, Integrity, Availability**

C) Control, Identity, Access

D) Confidentiality, Identity, Authorization

3.22 Question 72

APT attacks are most often associated with:

A) Immediate financial gain

B) **Long-term, undetected access to systems**

C) Disrupting internet services

D) Corrupting hardware components

3.23 Question 73

A virus attaches itself to:

A) Network connections

B) **Files and programs on a system**

C) System firmware

D) User login credentials

3.24 Question 74

Which of the following is a common use of keyloggers?

A) **Capturing passwords and sensitive information**

B) Spreading ransomware

C) Locking users out of their systems

D) Infecting web servers

3.25 Question 75

Spyware is often used to:

A) **Monitor user activities without their knowledge**

B) Encrypt files for ransom

C) Destroy data on hard drives

D) Execute commands on a remote system

3.26 Question 76

Adware typically:

A) **Displays unwanted advertisements to users**

B) Encrypts system files

C) Locks users out of their devices

D) Corrupts network traffic

3.27 Question 77

The primary goal of phishing is to:

A) Infect systems with ransomware

B) **Trick users into providing personal information**

C) Disable firewalls and security systems

D) Steal system resources for cryptocurrency mining

3.28 Question 78

Rootkits are commonly used to:

A) **Hide malicious processes from detection**

B) Encrypt files and demand payment for decryption

C) Destroy system files

D) Spread malware through email attachments

3.29 Question 79

Spam refers to:

A) Malicious software that replicates itself

B) **Unsolicited and often irrelevant emails sent to large numbers of users**

C) Emails containing malicious attachments

D) Software designed to steal information

3.30 Question 80

Firewall rules are primarily designed to:

A) **Block unauthorized access to or from the network**

B) Prevent hardware failures

C) Encrypt data at rest

D) Identify zero-day vulnerabilities

3.31 Question 81

Social engineering relies on:

A) Technical vulnerabilities

B) **Manipulating people into giving up confidential information**

C) Exploiting weak encryption

D) Injecting malware into databases

3.32 Question 82

Hactivists typically attack for:

A) Financial gain

B) Personal vendettas

C) **Ideological reasons**

D) State-sponsored activities

3.33 Question 83

Which of the following is not an example of malware?

A) Trojan horse

B) Spyware

C) Keylogger

D) **Firewall**

3.34 Question 84

Multi-factor authentication (MFA) is designed to:

A) Speed up the login process

B) **Provide stronger security by requiring multiple forms of verification**

C) Replace passwords with PINs

D) Prevent malware from infecting a system

3.35 Question 85

The primary purpose of two-factor authentication (2FA) is to:

A) Simplify the login process

B) **Increase security by requiring two forms of verification**

C) Replace passwords with encryption keys

D) Encrypt all data at rest

3.36 Question 86

Botnets are primarily used for:

A) Spreading malware

B) **Conducting large-scale attacks like DDoS**

C) Encrypting system files

D) Crashing operating systems

3.37 Question 87

Man-in-the-middle attacks intercept:

A) **Communications between two parties**

B) Malicious code in files

C) Phishing emails

D) System logs

3.38 Question 88

SQL injection is primarily used to:

A) **Exploit vulnerabilities in web applications**

B) Attack email servers

C) Corrupt network traffic

D) Infect system files

3.39 Question 89

DDoS attacks typically involve:

A) **Sending excessive traffic to overwhelm systems**

B) Spying on user activity

C) Infecting files with malware

D) Hijacking web servers

3.40 Question 90

Keyloggers are used to:

A) **Capture and record keystrokes made by a user**

B) Encrypt data at rest

C) Inject malware into system files

D) Block access to network resources

3.41 Question 91

Polymorphic malware is designed to:

A) **Change its code to avoid detection**

B) Disable firewalls and antivirus software

C) Encrypt user data for ransom

D) Spread through email attachments

3.42 Question 92

Social engineering attacks target:

A) **Human behavior and decision-making**

B) System vulnerabilities in software

C) Wireless networks

D) Backup systems

3.43 Question 93

Honeypots are:

A) **Systems designed to attract and trap attackers**

B) Antivirus programs that scan for malware

C) Password management tools

D) Backup solutions for sensitive data

3.44 Question 94

Keyloggers often target:

A) **Passwords and sensitive information**

B) Network infrastructure

C) Encrypted files

D) Backup systems

3.45 Question 95

A virus can be classified as:

A) **Self-replicating malware that requires user intervention**

B) Malware that spreads automatically

C) A type of spyware

D) A hidden backdoor in systems

3.46 Question 96

Worms differ from viruses in that:

A) **They do not need user action to spread**

B) They only infect executable files

C) They hide in system root directories

D) They cannot spread across networks

3.47 Question 97

Firewalls are primarily used to:

A) **Monitor and block unauthorized traffic**

B) Encrypt network traffic

C) Store sensitive data

D) Detect keyloggers

3.48 Question 98

Black hat hackers are motivated by:

A) **Financial gain or malicious intent**

B) Exposing vulnerabilities for ethical reasons

C) Protecting corporate data

D) Conducting legal penetration tests

3.49 Question 99

White hat hackers are typically involved in:

A) Developing malware

B) **Exposing vulnerabilities for security improvement**

C) Selling exploits to governments

D) Disabling corporate firewalls

3.50 Question 100

Gray hat hackers are characterized by:

A) **Breaking into systems without permission but not for malicious purposes**

B) Developing viruses and Trojans

C) Only attacking government institutions

D) Working directly for state-sponsored groups

4 Answer Key Summary

4.1 First Set (1-50)

Q	Ans	Q	Ans	Q	Ans
1	B	18	C	35	A
2	C	19	B	36	B
3	C	20	B	37	C
4	B	21	C	38	B
5	B	22	B	39	A
6	C	23	B	40	B
7	B	24	C	41	B
8	B	25	B	42	B
9	B	26	B	43	B
10	C	27	D	44	B
11	B	28	B	45	A
12	A	29	C	46	B
13	B	30	D	47	B
14	B	31	A	48	B
15	A	32	B	49	A
16	B	33	B	50	B
17	A	34	B		

4.2 Second Set (51-100)

Q	Ans	Q	Ans	Q	Ans
51	B	68	A	85	B
52	B	69	A	86	B
53	B	70	A	87	A
54	C	71	B	88	A
55	A	72	B	89	A
56	B	73	B	90	A
57	A	74	A	91	A
58	A	75	A	92	A
59	B	76	A	93	A
60	B	77	B	94	A
61	B	78	A	95	A
62	B	79	B	96	A
63	A	80	A	97	A
64	A	81	B	98	A
65	C	82	C	99	B
66	A	83	D	100	A
67	A	84	B		