

1 We can deal with harm in several ways. What is the best description of deterring harm?
Select one alternative:

- ☐ Made another target more attractive.
- ☐ Made the impact less severe.
- ☐ Made an attack impossible (blocked).
- ☐ Made an attack harder but not impossible.

Maximum marks: 1

2 Which of the following is an established security aspect?
Select one alternative:

- ☐ Non-repudiation
- ☐ Administrative security
- ☐ Loss
- ☐ Granularity

Maximum marks: 1

3 What is the benefit of using a Virtual Private Network?
Select one alternative:

- ☐ Protection against packet loss
- ☐ Increased lag
- ☐ Decreased lag
- ☐ Protection against eavesdropping

Maximum marks: 1

4 Which alternative would provide the best countermeasure against an on-line attack (active authentication) against a username and a password?

Select one alternative:

- ☐ To use a strict limit on login failures
- ☐ The use of a long password
- ☐ To use the Diffie-Hellman password exchange
- ☐ To use of a firewall

Maximum marks: 1

5 Which of the following sentences describe the term asset best from an information security perspective?

Select one alternative:

- ☐ Anything that has a value to the organization.
- ☐ Anything that an organization buys.
- ☐ Anything that an organization sells.
- ☐ Anything that is situated within an organization's premises.

Maximum marks: 1

6 Where in the information security model could algorithms for securing a harddrive be placed?

Select one alternative:

- ☐ Administrative security
- ☐ Physical security
- ☐ Network security
- ☐ Computer security

Maximum marks: 1

7 Access control is an essential aspect of information security. An operating system often manages the access control. Access control is often described using the terms:

Note that there are more types than descriptions.

 [Help](#)

Subjects	Topics	Secrecy-based	Accountability	Identifications
Items	Objects	Access-based	Role-based	Identities

are the entities that can access objects (often the human user).

are things on which an action can be performed such as, e.g., files, programs, and hardware devices.

There are many models for how to implement access control in practice, and one example is

access control.

Maximum marks: 2

8 Which of the below-mentioned protocol(s) is susceptible to sniffing?

Select one alternative:

- ☐ All of them
- ☐ HTTP
- ☐ SMTP
- ☐ Ethernet

Maximum marks: 1

9 Select the outdated encryption algorithm among the acronyms below.

Select one alternative:

- ☐ TCP
- ☐ DES
- ☐ AES
- ☐ SED

Maximum marks: 1

10

According to the CIA Triad, which of the below-mentioned security aspects is not considered in the triad?

Select one alternative:

☐

Authenticity

☐

Integrity

☐

Availability

☐

Confidentiality

Maximum marks: 1

11

(XML injection, Malicious code injection, SQL injection, HTML injection) is a code injecting method used for attacking the database of a website.

Maximum marks: 1

12

Which of the following is not a wireless attack?

Select one alternative:

☐

Wireless hijacking

☐

Eavesdropping

☐

MAC spoofing

☐

Phising

Maximum marks: 1

13

Assume you encounter a search box on a web page that can take an input of 200 characters. You insert 300 characters and the remote system crashes. Usually, this type of behaviour is because of limited

(local memory, storage, buffer, cloud).

Maximum marks: 1

14

Imagine you are using an internet service provider (ISP) who you don't trust. What could you use to hide your browsing activity?

Select one alternative:

☐

The incognito mode on the browser

☐

A firewall

☐

A virtual private network

☐

Anti spyware software

☐

An antivirus software

Maximum marks: 1

15 Describe what penetration testing is and what type of skills are required to perform such penetration testing.

Fill in your answer here

Maximum marks: 3

16 Imagine that you have been appointed responsible for the implementation of information security in an organization. Provide three key factors you deem necessary in order to succeed with such a task. Motivate your answer.

Fill in your answer here

Maximum marks: 3

21 Authentication mechanisms can be divided into three categories. Describe these three categories.

Fill in your answer here

Maximum marks: 3

22 Define the terms: vulnerability, threat, harm and security controls. Also, relate the terms to each other by giving an applied example.

Fill in your answer here

Maximum marks: 5

25 Why should the directory of one user not be generally accessible to other users (not even for read-only access)?

Fill in your answer here

Maximum marks: 2

26 In the context of software security, such as OS security, eight design principles were formulated more than 40 years ago. Despite the relative age, they remain valid even today. Describe any four of these design principles.
Fill in your answer here

Maximum marks: 4