1   # Security aspects

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

- ○ Non-repudiation

- ○ Granularity

- ○ Loss

- ○ Administrative security

Maximum marks: 1

2   # VPNs

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

- ○ Decreased lag

- ○ Protection against packet loss

- ○ Increased lag

- ○ Protection against eavesdropping

Maximum marks: 1

3   # Digital signatures

To create a digital signature, what is needed?
Select one alternative:

- ○ All of them

- ○ Public-key system

- ○ Shared-key system

- ○ Private-key system

Maximum marks: 1

4 **Encryption**

Which of the following standards could be considered the go-to encryption standard of today?
Select one alternative:

◯ AES

◯ WEP

◯ SED

◯ DES

Maximum marks: 1

5 **Security aspects**

In an attack, the adversary changed the number 100,00 to 10000. This type of change can be considered an attack against what security aspect?
Select one alternative:

◯ Confidentiality

◯ Availability

◯ Privacy

◯ Integrity

Maximum marks: 1

6 **Security requirements**

Select the security requirements below that are either not realistic or not verifiable.
Select one or more alternatives:

☐ A system with zero downtime.

☐ A firewall rule that can filter out all harmful traffic.

☐ A system without a loss of confidentiality.

Maximum marks: 2

7   # Malicious code

Pfleeger, Pfleeger, and Margulies (2015) desribes a number of types of malicious code. Match the type of malicious code with the corresponding description.

Note that there are more types than descriptions.   ⌨ Help

Scareware	Rootkit	Dropper	Trapdoor	Virus	Rabbit	Spyware

Program that intercepts and covertly communicates data on the user or the user's

activity. [   ]

Code that causes malicious behavior and propagates copies of itself to other programs. [   ]

Code installed in the most privileged section of an operating system. [   ]

Maximum marks: 2

---

8   # Risk

What is meant by residual risk?
Select one alternative:

○ A risk that is avoided by circumventing the problem.

○ A risk that remains uncovered by security controls.

○ A risk that is mitigated by security controls.

○ A risk that is transferred to e.g. an insurance company.

Maximum marks: 1

---

9   # Assets

Which of the following sentences describe the term asset best from an information security perspective?
Select one alternative:

○ Anything that an organization buys.

○ Anything that an organization sells.

○ Anything that is situated within an organization's premises.

○ Anything that has a value to the organization.

Maximum marks: 1

10 Infosec model

Where in the information security model is the information security policy placed?
Select one alternative:

○ External, informal, administrative security

○ External, formal, administrative security

○ Internal, formal, administrative security

○ Internal, informal, administrative security

Maximum marks: 1

11 Access control

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

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

12 Passwords

Which alternative would provide the best countermeasure against an off-line brute-force attack on a password hash?
Select one alternative:

○ To use the Diffie-Hellman password exchange

○ To use of a firewall

○ To use a strict limit on login failures

○ The use of a long password

Maximum marks: 1

13 **Infosec definition**

How would you define information security? You could use existing definitions or your own definition, as long as it aligns with common definitions.

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | I_x | ⎘ | ⎘ | ↰ | ↱ | ↺ | ≔ | ≔ | Ω | ⊞ | ✎ | Σ | ᴬᴮꟲ▾ | ⤢ |

Words: 0

Maximum marks: 3

14 # ISMS implementation

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

| Format ▾ | B | I | U | x₂ | x² | Iₓ | | | | | | | | | | Ω | | | Σ | | ABC ▾ | | |

Words: 0

Maximum marks: 3

15 IDS, IPS

Describe the concepts: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Also, differentiate the concepts.

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | Iₓ | 📋 | 📋 | ↩ | ↪ | ↺ | ☷ | ☰ | Ω | ▦ | ✎ | Σ | ABC▾ | ⤢ |

Words: 0

Maximum marks: 3

16 Encryption

Explain the difference between stream cipher and block cipher. Also, give an example when each type of cipher could be used.

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | Iₓ | 📋 | 📋 | ↩ | ↪ | ↺ | ☷ | ☰ | Ω | ▦ | ✎ | Σ | ABC▾ | ⤢ |

Words: 0

Maximum marks: 3

17 **MITM**

Man-in-the-Middle (MITM) is a common type of network attack. Give one applied example of a MITM.

Fill in your answer here

| Format ▾ | B *I* U x₂ x² | ... | Ω ⊞ | Σ | ABC▾ | ✕ |

Words: 0

Maximum marks: 2

18 **Session hijacking**

Explain the concept of session hijacking by giving an example of such an attack.

Fill in your answer here

| Format ▾ | B *I* U x₂ x² | ... | Ω ⊞ | Σ | ABC▾ | ✕ |

Words: 0

Maximum marks: 3

19   Penetration testing

What are the disadvantages of penetration testing?

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | Ix | ⎙ ⎙ | ↩ → | ↻ | ⅀ ☰ | Ω ⊞ | ✎ | Σ | ABC▾ | ⤢ |

Words: 0

Maximum marks: 2

20   Authentication

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

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | Ix | ⎙ ⎙ | ↩ → | ↻ | ⅀ ☰ | Ω ⊞ | ✎ | Σ | ABC▾ | ⤢ |

Words: 0

Maximum marks: 3

21 Infosec terms

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

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | I_x | ⌷ ⌷ | ↩ ↪ ↺ | ≔ ⋮≔ | Ω ⊞ | ✎ | Σ | ABC▾ | ⤢ |

Words: 0

Maximum marks: 5

22 Clickjacking

Suggest and describe a technique by which a browser could detect and block clickjacking attacks.

Fill in your answer here

| Format ▾ | B | I | U | x₂ | x² | I_x | ⌷ ⌷ | ↩ ↪ ↺ | ≔ ⋮≔ | Ω ⊞ | ✎ | Σ | ABC▾ | ⤢ |

Words: 0

Maximum marks: 2

23 # Temporal separation

Give an example of the use of temporal separation for security in a computing environment. Also discuss the advantages and disadvantages of such an approach.

Fill in your answer here

| Format ▾ | **B** *I* U x₂ x² | 𝐼ₓ | ⎘ ⎗ | ↶ ↷ ↺ | ≔ ≡ | Ω ▦ | ✎ | Σ | ABC▾ | ⛶ |

Words: 0

Maximum marks: 2

24 # OS security

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

| Format ▾ | **B** *I* U x₂ x² | 𝐼ₓ | ⎘ ⎗ | ↶ ↷ ↺ | ≔ ≡ | Ω ▦ | ✎ | Σ | ABC▾ | ⛶ |

Words: 0

Maximum marks: 2

25   OS security

File access control relates largely to confidentiality. What is the relationship between an access control matrix and the integrity of the objects to which access is being controlled?

Fill in your answer here

Words: 0

Maximum marks: 2