1

IDS

What word would best describe how an intrusion detection system operates?
Select one alternative:

○ proactive

○ reactive

○ inductive

○ reductive

Maximum marks: 1

2

Services

What could be considered a best mitigation practice for services that are not being used on devices?
Select one alternative:

○ Enable

○ Limit

○ Disable

○ Monitor

Maximum marks: 1

3

VPNs

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

○ Increased lag

○ Increased confidentiality

○ Increased availability

○ Decreased lag

Maximum marks: 1

4 Passwords

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

Select one alternative:

○ The use of a long password

○ To use of a firewall

○ To use the Diffie-Hellman password exchange

○ To use a strict limit on login failures

Maximum marks: 1

5 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 is situated within an organization’s premises.

○ Anything that has a value to the organization.

○ Anything that an organization sells.

Maximum marks: 1

6 Infosec model

Where in the information security model would an information security policy be placed?

Select one alternative:

○ Physical security

○ Administrative security

○ Network security

○ Computer security

Maximum marks: 1

7

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

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

□ 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

Sniffing

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

Select one alternative:

○ TCP

○ HTTP

○ UDP

○ All of them

Maximum marks: 1

9

Encryption

What type of cryptographic algorithms are DES and 3DES?

Select one alternative:

○ Assymetric

○ Caesar

○ Symmetric

○ Vigenère

Maximum marks: 1

10

Security aspects

According to the CIA Triad, which of the below-mentioned security aspects is considered in the triad?
Select one alternative:

○ Authenticity

○ Availability

○ Accountability

○ Auditability

Maximum marks: 1

11

Web security

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

Maximum marks: 1

12

Network security

Which of the following is not a wireless attack?
Select one alternative:

○ Wireless hijacking

○ Rootkit

○ MAC spoofing

○ Eavesdropping

Maximum marks: 1

13

Program security

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 □ (cloud, storage, local memory, buffer).

Maximum marks: 1

14 General information security

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:

○ Anti spyware software

○ An antivirus software

○ A firewall

○ The incognito mode on the browser

○ A virtual private network

Maximum marks: 1

15 Integrity

List at least three kinds of damage a company could suffer when the integrity of a program or company data is compromised.

Fill in your answer here

Format

Words: 0

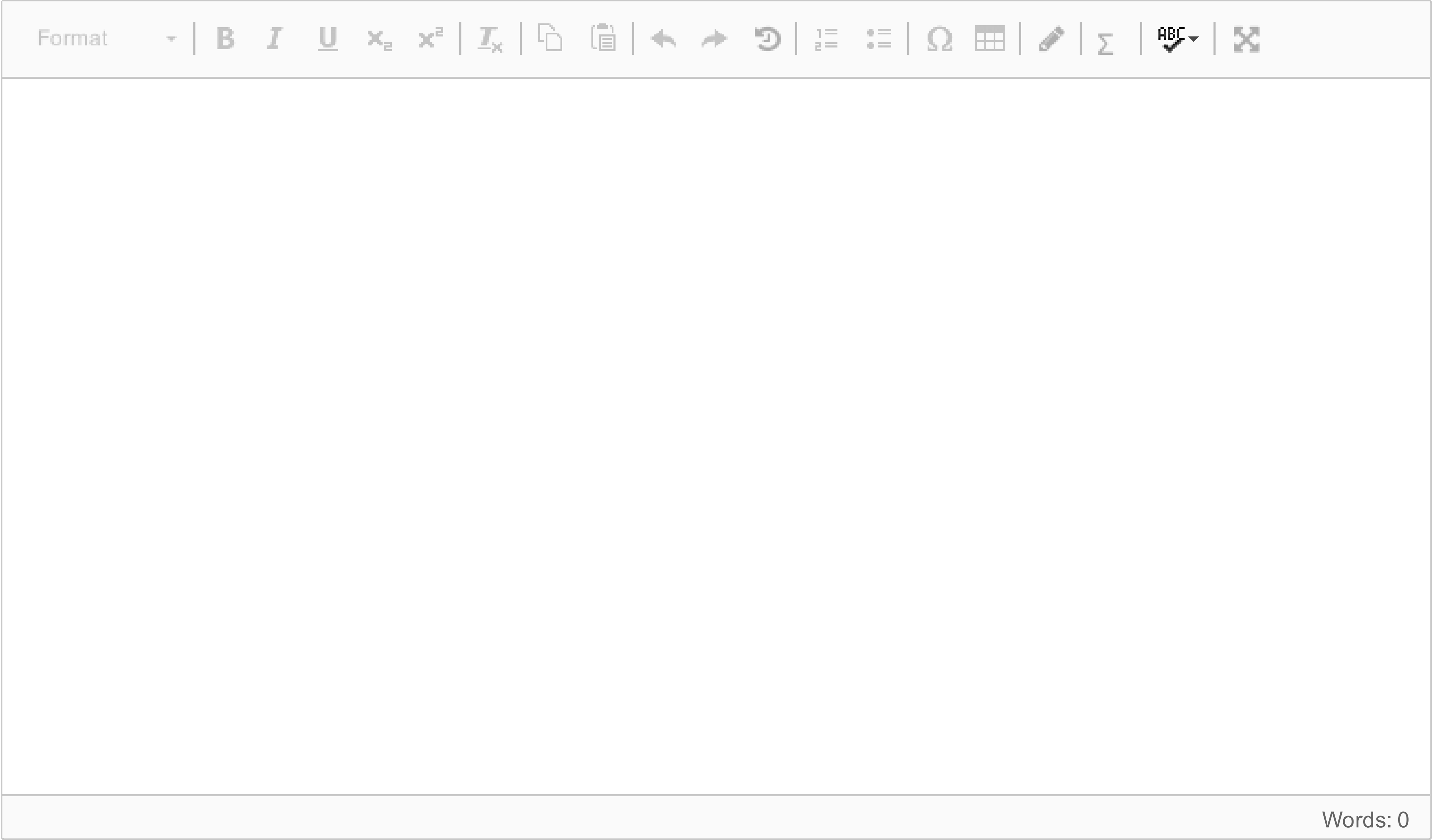
Maximum marks: 3

16

Practical security

Describe two examples of vulnerabilities of cars for which car manufacturers have instituted controls. Tell whether you think these controls are effective, somewhat effective, or ineffective. Motivate your answer.

Fill in your answer here



Maximum marks: 3

17 IDS, IPS

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

Fill in your answer here

Format

Words: 0

Maximum marks: 3

18 Program security

Describe three reasons why penetrate-and-patch is a misguided strategy.

Fill in your answer here

Format

Words: 0

Maximum marks: 3

19 General infosec

Consider a program that allows a surgeon in one city to assist in an operation on a patient in another city via an Internet connection. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?

Fill in your answer here

Format

Words: 0

Maximum marks: 4

20 Passwords

Explain the concept of salt, and exemplify how it can be used.

Fill in your answer here

Format

Words: 0

Maximum marks: 3

21 Authentication

List three reasons why people might be reluctant to use biometrics for authentication. Also give examples of how to counter those objections?

Fill in your answer here

Format

Words: 0

Maximum marks: 3

22 Infosec terms

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

Format

Words: 0

Maximum marks: 5

23 Authentication

Are computer-to-computer authentications subject to the weakness of replay? Motivate why or why not.

Fill in your answer here

Format

Words: 0

Maximum marks: 2

24 OS security

Describe by giving an applied example of how passwords are stored by the operating system of your personal computer?

Fill in your answer here

Format

Words: 0

Maximum marks: 2

25 OS security

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

Format

Words: 0

Maximum marks: 4