1. Modify the following texts so that the statements are true.

E-mail (spoofing / ~~sniffing~~) involves sending messages from a bogus e-mail address or faking the e-mail address of another user.

Denial of Service attacks (~~destroy~~ / do not destroy) or (~~steal~~ / do not steal) data as some other types or attacks do.

The objective of (volume-based / protocol) DDoS attacks is to sature the bandwith of the network

Social engineering attacks (refers / does not refer) to a technological manipulation of computer hardware or software vulnerabilities and (requires / does not require) much in the way of technical skills.
(Signature-based / Heuristic approach) virus detection can identify new viruses or variants of existing viruses by looking for known malicious code, or (slight / major) variations of such code, in files.

---

2. Mark the true statements.

- ☐ A DoS attack is a deliberate action that keeps a computer or network from functioning as intended (for example, preventing users from being able to log onto the network).
- ☐ Adware is considered an ilegitimate alternative offered to consumers who do not wish to pay for software.
- ☐ A spyware infestation does not generate unwanted CPU activity, disk usage, or network traffic
- ☐ A computer program that performs an action that intentionally damages a system or data is named malicious code
- ☐ A spoofing attack is when a malicious party impersonates another device or user on a network.
- ☐ Zero-day attacks are discovered in few minutes

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. Assign the terms from the left column to the corresponding on the right.

Confidentiality	Assuring the identity of the communicating entities.
Data integrity	Prevention of unauthorized use of a resource.
Availability	Protection of information from disclosure to unauthorized entities.
Authentication	Having timely access to information.
Access control	Protection of data against creation, alteration, deletion, duplication or reordering by unauthorized entities.

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Fill the numbers of correct statements.

1 – Non repudiation allows an individual to maintain the right to control what information about him is collected, how it is used and who uses it.

2 – Traffic padding is a mechanism that inserts bits into gaps in a data stream to frustrate traffic analysis attempts.

3 – Data privacy refers to the protection of information from disclosure to unauthorized entities.

4 – Notarization is a mechanism that uses a trusted third party to assure certain properties of a data exchange.

5 – A semi-invasive attack can tamper with the attacked device but do not make direct electrical contact with the chip's surface.

6 – Node replication and spoofing are examples or passive attacks.

7 – A way to crash a system is by putting more data into a buffer than the buffer is able to hold.

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.