

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

Safeguarding data is an $\left(\begin{smallmatrix} \text{optional} \\ \text{necessary} \end{smallmatrix} \right) \left(\begin{smallmatrix} \text{proactive} \\ \text{reactive} \end{smallmatrix} \right)$ approach to avoid interrupting customer services even when changes are being modified

The network security system $\left(\begin{smallmatrix} \text{is just a small part} \\ \text{is the global solution} \end{smallmatrix} \right)$ of an organization's information security infrastructure.

Security services are implemented by $\left(\begin{smallmatrix} \text{security mechanisms} \\ \text{security algorithms} \end{smallmatrix} \right)$ according to security $\left(\begin{smallmatrix} \text{protocols} \\ \text{policies} \end{smallmatrix} \right)$.

Security $\left(\begin{smallmatrix} \text{protocols} \\ \text{mechanisms} \end{smallmatrix} \right)$ support the security services and execute specific activities for the protection against attacks.

$\left(\begin{smallmatrix} \text{All} \\ \text{Not all} \end{smallmatrix} \right)$ semi-invasive or invasive attacks are active attacks

$\left(\begin{smallmatrix} \text{All} \\ \text{Not all} \end{smallmatrix} \right)$ the security threats are malicious.

2. Mark the true statements.

- ☐ Network security only concerns the security in the computers at each end of the communication.
- ☐ Securing the network is just as important as securing the computers and encrypting the message.
- ☐ A network security system is a set of hardware devices, that uses and cryptographic algorithms to protect the information and communication systems of a company.
- ☐ All security mechanisms use cryptographic transformations.
- ☐ Security mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service
- ☐ The ability of an attacker is typically determined by his/her skills, traces he/she lefts behind after an attack and the required cost to spend in terms of equipment.



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

Virus

Malicious software propagated through the network.

Worm

Appears as benign programs, but can perform actions that the user did not intend or was not aware of.

Trojan

Software installed without the consent of the user and performs behaviour such as obtaining information about her browsing habits.

Zombies

Self-replication programs that do not require files to propagate.

Spyware

Self-replication programs that use files to infect and propagate.



4. Fill the numbers of correct statements concerning network security threats.

- 1 – Malware is defective software.
- 2 – Scanner refers to a software program that is used by hackers to remotely determine possible vulnerabilities of a given system.
- 3 – A scanning attack is when a malicious party impersonates another device or user on a network.
- 4 – Sometimes, antivirus can have drawbacks and they can impair the performance of a computer.
- 5 – Eradicating a virus means removing the code in the infected file which corresponds to the virus.
- 6 – A firewall is a typical border control mechanism or perimeter defence.
- 7 – Some IDS systems just monitor and alert of an attack, whereas others try to block it.

