**Text 3**

***I. Look through the following text and find information about the ways of classifying exploits.***

An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

There are several methods of classifying exploits. The most common is by how the exploit contacts the vulnerable software. A 'remote exploit' works over a network and exploits the security vulnerability without any prior access to the vulnerable system. A 'local exploit' requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator. Exploits against client applications also exist, usually consisting of modified servers that send an exploit if accessed with client application. Another classification is by the action against vulnerable system: unauthorised data access, code execution, denial of service.

Many exploits are designed to provide superuser level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root.

Normally a single exploit can only take advantage of a specific software vulnerability. Often, when an exploit is published, the vulnerability is fixed through a patch and the exploit becomes obsolete for newer versions of the software. This is the reason why some blackhat hackers do not publish their exploits but keep them private to themselves or other malicious crackers. In computer security, logging (or signing) in and is the process by which individual access to a computer system is controlled by identification of the user in order to obtain credentials to permit access. It is an integral part of computer security. A user can log in to a system to obtain access, and then log on when the access is no longer needed.

To log into a system usually requires: a user name, a unique sequence of characters the user chooses to represent himself or herself with. A user name can be the user's real name, but is more often a short nickname or screen name. The term User ID is also used on some systems. Many websites now use emails in place of the username, which are not publicly available, making password guessing much more difficult (the hackers need to guess the email as well). A password, another sequence of characters which provides the user with a key to the system and is kept secret from others. Logging out may be done explicitly by the user performing some action, such as entering the appropriate command, or clicking a website link labeled as such. It can also be done implicitly, such as by powering the machine off, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period.

Logging out of a computer when leaving it is a common security practice, preventing unauthorized users from tampering with it. There are also people who choose to have a password-protected screensaver to activate after some time of inactivity, requiring the user to log in again to regain access.

***II. Say why some hackers don’t publish their exploits.***

***III. Say where the information presented in the text can be used.***

***IV. Speak on one of the following points to your partner:***

a) methods of classifying exploits;

b) types of exploits;

c) how one can log in;

d) how one can log out.