TAGES	EXPLANATION
Black Box Stage	At this stage, no information is requested from the institution to be tested. First of all, the vulnerabilities of the institution's systems that are open to the internet are determined. By exploiting these vulnerabilities to be detected in the said systems, an attempt is made to infiltrate the system through the interfaces of the institution that are open to the internet or not. In this way, the general analysis and vectors of threats that the organization may receive from outside are obtained. The Black Box phase is the closest test phase to a real attack scenario from the outside. The biggest goal is to infiltrate the database in the target system.
Gray Box Stage	Thanks to this test, the danger surface of the system is analyzed by using the gaps of the system by coming as a guest inside the institution. In this way, many processes from the attacker's transition from the institution to the existing system, access to databases, and dominance over applications are handled through this test. The Gray Box stage reveals how successful an attack by a hacker who can physically enter the organization can be. The greatest goal is to take over the entire system, even with limited authority.
White Box Stage	With this test, the security specialist requests a definition of a standard user from the institution where the test is performed, so that as an expert standard user, it is checked whether he has increased his rights on the system and his dominance over databases and all other informatics infrastructure. During these tests, various tools are used, as well as special manual methods, including the necessary techniques to prevent the system from catching the attacker. The White Box stage reveals how effective an internal attack on the organization can be.
Red Box Stage	At the Red Box stage, cyber-weapon-assisted attacks are carried out on previously discovered corporate systems with unique files and methods that have been previously prepared and tested in the lab environment. The main goal at this stage is to examine the vulnerabilities of all steps from the first stage of the attack, such as infiltration, spread, escalation, persistence, and data export, and to identify vulnerability points.