Automation of security scans including verification integration safety in functional automatic tests. Very useful during several iterations of tests.

An example of the stages and areas being tested:

1. Risk assessment

Process of review and analysis of potential risk areas. Given priority is given to possible prevention measures. The result of this stage is the proposal of control points for detection of attack attempts and implementation of mechanisms to minimize the consequences of an attack. Guard memories in this case is a technique called the evaluation model risk (Threat modelling). It allows you to specify the risk level for individual elements indirectly allowing creation methods to reduce its occurrence and use undoubtedly limited resources in the areas most in need comments. Such a model is created based on the NIST 800-30 standard, its result are usually collections of lists and diagrams, its main stages include:

◦ decomposition of the application - it is collected in the inspection process knowledge about the application and its components, functionalities and method of communication.

◦ identification and classification of components - division into resources tangible and uncountable and their weight assessment business.

◦ search for potential vulnerabilities - can be derived from technical, operational or management problems.

◦ search for potential threats - using techniques of scenarios or "trees" of attack, a model describing potential places of attack from the perspective of the burglar is created

◦ creation/development of a strategy of prevention - preparation of control points and reduction procedures for impact of the burglary.

2. Security audition

The procedure for defining security errors in individual applications that make up the attack environment. This can be manual verification of policies, procedures, processes and employees or roles of themselves. The configuration of the system and work environment is taken into account, i.e. the factors for which the technology was chosen or what was the reason for designing the element in this way, and not in another one. On this basis, the tester determines probability of a problem occurring in a given element. It is also one of the few steps allowing to detect problems in the same software life cycle (SDLC) and to make sure that the appropriate policy has been introduced and that it’s understood or to verify the level of competence. Often during this phase of testing the application code is being overviewed. It is possible to check individual lines. This makes possible to find low level mechanisms allowing unintended interaction with the system, which are extremely difficult to find with using other ways. In addition to the problems occurring because of bad intentions, in this case are found: various comments, outdated versions of modules, sharing problems, faulty business logic, incorrect access control, encryption algorithm vulnerabilities, workarounds to facilitate work or various types of malicious code (Trojans, Backdoors). To reduce the workload required to source code reviews of considerable size are used automatic scanners, as a supplement is performed manually review to overcome the limitation of inability the scanner's understanding of the context and dependencies arising from flows between single element of the program.

3. Penetration testing

The test aims to imitate a malicious external attack also known under the name of black box tests. Performed to assess system security. During the test a working version of the application is used and the auditor does not have one in-depth knowledge of how it works. Often, the test group is in possession of a basic account with access. An attempt follows obtain unauthorized access to the system being performed by a qualified specialist the way he would work potential attacker. Stages:

◦ reconnaissance,

◦ gap identification,

◦ using vulnerabilities,

◦ risk analysis,

◦ blurring the tracks.

4. Posture/policy assessment – Posture assessment

The summary of three verifications to value the full picture of the approach for organization security. The components are: risk assessment, test penetration, security scan.

5. Security scanning

It is characterized by the identification of weaknesses in the network and system to which later on, there are proposals on how to reduce risk. This type of scan is performed manually as well as for using automatic tools.

6. Searching for sensitive points – Vulnerability scanning

In this phase, threats are identified that they can actually occur in the tested environment, what is also verified, is effectiveness of using known vulnerabilities in the security systems of single components of the environment, e.g. programs and their concrete versions. This type of scan is realized with help of automated tools that penetrate the environment in the aspect of know areas of vulnerability.