

# VULNERABILITY ASSESSMENT AND PENETRATION TEST

A correct security management is based first of all on an appropriate knowledge of the present protection level of the systems. Starting from here, Spike Reply has consolidated its experience in the application of internationally known Vulnerability Assessment and Penetration Testing methodologies, by approaching the problem from different point of views and by meeting all the customers' requirements in these fields.

## AIMS

The Vulnerability Assessment and Penetration Test activities offered by Spike Reply are aimed at providing the customer with a detailed knowledge on the security status of his IT systems.

In particular, through different analysis steps carried out by simulating different intrusion scenarios, the methodologies used by Spike Reply allow for:

- checking that the information on the Customer's network viewable on Internet are minimized;
- checking that it is not possible to obtain unauthorized accesses to systems and information;
- checking if an internal user can access information or obtain privileges for which he is not authorized;
- checking that a Web Application does not contain vulnerabilities that can allow attackers to obtain unauthorized accesses to confidential data, in particular mimicking of other users, privilege escalation, interactive access to target network, attack to application user, Denial of Service.

**VULNERABILITY ASSESSMENT VS PENETRATION TEST.** In order to reach these aims, the Spike Reply methodology uses two different typologies of technical check: Vulnerability Assessment and Penetration Test. These two techniques differ the one from the other both for the results and for the resources required.

A Vulnerability Assessment (VA) activity allows the customer to clearly see the exposure status of its systems to any known vulnerabilities. For this aim, some automatic tools are used which carry out a long series of checks on every system/application to understand their configuration in detail and detect any vulnerability. Checks are carried out very quickly with this software, therefore a very wide perimeter can be tested in a short time providing a very detailed vision. On the other hand, the usage of automatic tools make it impossible to extend the checks beyond the vulnerabilities for which the specific tool has been created and to check the real possibilities an attacker would have to exploit this vulnerability.

In order to provide the Customer with the opportunity to carry out more specific and deeper analysis than those offered by a VA, Spike Reply offers its experience also in the field of Penetration Tests (PT). During a Penetration Test, intrusion simulations are carried out with different attack scenarios and combining manual techniques with automatic tool use. In this way, it is possible to analyze first of all the exposure to vulnerabilities that cannot be checked by automatic software and also to see how –also in cases where the individual vulnerabilities do not cause a real risk situation- their combined exploit can have a strong impact on security.

Moreover, by manually operating on systems and applications, it is also possible to exploit the vulnerabilities that have been found, by completing the attack simulation in order to see the possible consequences in a real situation.

**APPLICATION PARAMETERS.** The general paradigms described above have got very different characteristics according to their application field. Three different fields can be identified:

- infrastructure VAs / PTs: they concern all the checks at wired network, server and client configuration level.
- application VAs/PTs: they concern all the checks carried out on individual applications.
- wireless infrastructure PTs: they concern all the checks which are specific for wireless networks.

## INFRASTRUCTURE VA/PT



The methodology used by Spike Reply for infrastructure VA / PT activity is compliant with the Open Source Security Testing Methodology Manual of ISECOM, the international standard in this field.

The applied methodology is composed of different stages which are represented in the following diagram.



The main stages are:

**HOST IDENTIFICATION.** The network is analyzed in order to define the running systems. Each of them is analyzed through active (by sending requests to the systems) and passive (obtaining information from public servers such as DNS or WHOIS databases) fingerprint techniques in order to determine –in a very precise way- the version of the installed Operative System.

**SERVICE COUNT AND VULNERABILITY IDENTIFICATION.** All the active hosts are examined to identify what ports are open and therefore what services are active. For each detected service, the associated software version is identified, if possible.

This identification allows for the execution of presence tests for the vulnerabilities which could be exploited to obtain an unauthorized access to the systems. The used tests combine manual techniques and automatic tools in order to exploit the speed and completeness of automatic scanning and the efficiency and precision of a qualified expert hacker.

**EFFECTIVE EXPLOIT.** When a complete penetration test is carried out (and in any

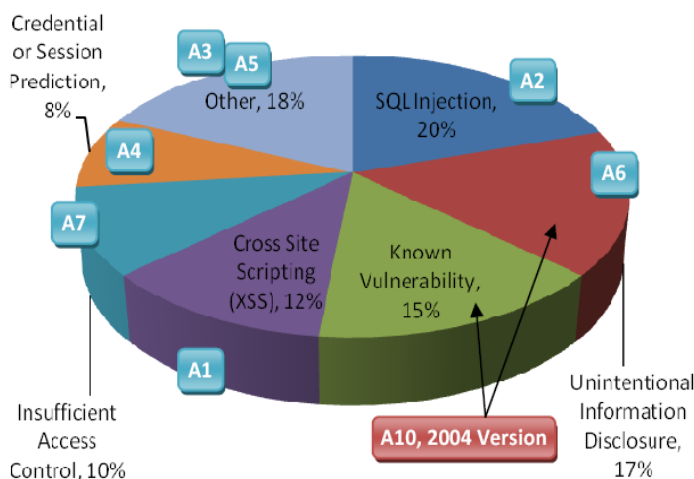
case following a customer's specific request), the vulnerability exploit activity is completed with the aim of understanding the real impacts of a potential intrusion on systems and data.

## APPLICATION VA/PT

The tests on web application play today a very important role within the different technical check activities. The reason for this importance is to be searched in the statistics on attack vehicles: 70% of computer attacks can be carried out thanks to programming errors.

To carry out its Penetration Test activities on web applications, Spike Reply uses an internationally consolidated methodology which is summarized in the Open Web Application Security Project (OWASP), a reference organization for web application security. This analysis is made up of a series of attack attempts involving communication protocols and logics used by final users to interact with the applications (attack to web servers, to the application structure, to authentication and authorization systems, to management interfaces, to client systems and so on). In the specific case of web applications, the attacks are based on manipulations of HTTP packages that are interchanged between users' browsers and web server.

Tests are carried out both anonymously and in "user-mode", using an account created through the usual activation procedures in order to enable the penetration tester to access as authorized user. In this way, it is possible to test the robustness of the authentication and containment systems both for anonymous users and for usual authorized users.



The activity includes the application analysis in terms of architecture and the examination of the configuration of the involved machines, both at operative system and application level.

During the test, particular attention is paid to the vulnerability classes included in the 10 most important vulnerabilities in terms of spreading and impact on the systems that are part of the so-called OWASP Top 10. In this way, it is also possible to have a constant reference to judge the severity of the situations occurred.

## WIRELESS INFRASTRUCTURE

The technical safety check range is completed by the analysis of the wireless network structure. The analysis mainly concern the 802.11 family of networks and the relevant security assessment is aimed at checking the presence of authorized and unauthorized access points and their coverage, as well as their consistency and related vulnerabilities.

The activity is mainly divided into two macro-stages. The first stage is exclusively dedicated to the detection of radio signals in the buildings identified as analysis perimeter and is carried out using hardware and software tools which are specific for any network type. In this way, it is possible to identify what networks are present and to determine if their security levels comply with company policies and relevant best practices and to ensure that no unauthorized networks are present. The second stage is aimed at analyzing the external perimeters in order to see –especially for the most critical networks- if the radio signal level enables connection also in public access zones.

The methodology follows the steps specified in the Open Source Security Testing Methodology Manual (OSSTMM), already used for infrastructural VA and PT activities.



Within the Reply SpA Group, Spike Reply is the company specialized in the field of Security and Personal Data Protection.

Spike Reply developed a comprehensive, integrated and consistent offer, in order to tackle any aspect of risks associated to an information system: from detection of threats and vulnerabilities to the definition, planning and implementation of technology, legal, organization, insurance or risk retention counter-measures.

Spike Reply  
[www.reply.eu](http://www.reply.eu)