What is a penetration test and what is it for?

The tests or penetration tests are a systematic process to **check the vulnerabilities** of computer applications and networks. Basically, it is a controlled form of hacking whereby a group of people, known as pentesters, perform a scheduled attack on the system in order to find technological weaknesses before the criminals do.

They are also used to ensure compliance with a certain security policy, learn about employee awareness of it, and identify the organization's ability to respond to these incidents.
To reduce the impact on daily operations, these tests are performed outside of business hours or when technology systems are used less. If any issues are discovered, the system owner should be notified.

What types of penetration tests are there?
Broadly speaking, there are four varieties of penetration tests. Each of them focuses on a specific aspect of the organization.

Network penetration test: identifies security problems in the network infrastructure. This **penetration testing** involves scanning the network and wireless services to ensure that the

network design and its individual components are well defined and programmed.

Web Application Penetration Test: Detects security issues in a web application or site. It is essential to monitor the access points to the systems and thus prevent *hackers* from entering them. In this way, data theft or irreparable damage to applications will be avoided.

Wireless penetration test: The purpose of this test is to discover rogue access points and devices, analyze their configurations, and test for vulnerabilities. In addition to studying the network in detail, it is convenient to identify the status of its patches and versions.

Simulated Phishing Test: Provides an independent assessment of *phishing* and discovers the awareness and awareness that employees have about this issue.