VULNERABILITY SCAN

If your company has not yet been subjected to a penetration test, a scan is a good starting point for improving the security of assets in your infrastructure.

Such scan is performed by automated tools that collect information about your infrastructure components, and compare them to databases of known vulnerabilities. These vulnerabilities are not exploited during the test.

Regular scans are one of the recommended measures that lead to continuous security.

Upon scan completion, you will receive a clear vulnerability report along with an estimation of the technical risk. For each identified vulnerability, you'll receive a specific action that needs to be applied to fix the problem.

A test carried out from the external environment focuses on all systems and applications accessible from the Internet, verifying if they are adequately secured against intrusion into your organization's internal network.

The security of internal systems should not be neglected, and a test from the internal environment is as important as a test from the external environment (from the Internet). An internal environment scan identifies and classifies the vulnerabilities of your organization's internal assets.

The cost of an infrastructure security scan depends on the number of scanned devices and the frequency of service delivery.

Advantages versus penetration testing:

- Cheaper
- Shorter waiting time for results (a penetration test takes much longer)
- Results are available immediately after tests have been completed

Disadvantages over penetration testing:

- Reveals only known vulnerabilities
- More prone to false positives
- Not possible to verify if currently implemented security mechanisms cannot prevent an exploitation
- Not possible to verify the real technical risk, as vulnerabilities are not exploited