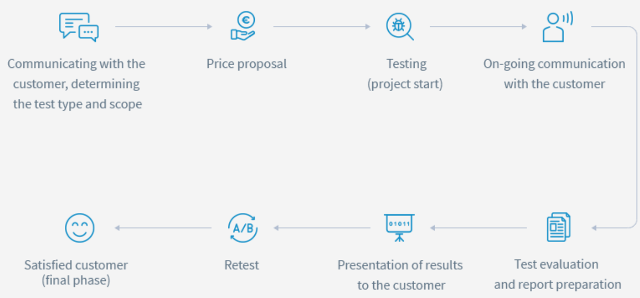
WIRELESS NETWORK (WIFI) PENETRATION TEST

Many companies make use wireless (WiFi) networks, which are often the target of attacks because a successful attack on WiFi devices can provide direct access to the internal network.

While these networks bring many benefits, an unprotected or poorly configured network can lead to unauthorized use and possible security risks such as data leakage.



GENERAL SERVICE OVERVIEW

The wireless network (WiFi) penetration test/audit is designed to assess the security of your wireless network that may be compromised due to incorrect configuration or implementations.

The penetration test results in a report that contains the identified vulnerabilities that are assigned a risk and recommendations on how to remove them.

The penetration test can be performed using the BLACK BOX (no information about the tested environment), GRAY BOX (partial information about the test environment) or WHITE BOX (full information about the tested environment, including configuration files of devices / settings) method.

The cost of the penetration test depends on the depth of the tests, the size and complexity of the tested infrastructure. The price is determined after customer consultation, which determines the scope, type of test and other requirements from the customer.

DETAILED OVERVIEW OF THE SERVICE AND METHODOLOGY

For the penetration test, we use methodologies such as the Open Source Security Testing Methodology Manual (OSSTMM), NIST800-115, the Information Systems Security Assessment Framework (ISSAF), and especially our internally developed methodology that simulates a real attack. Our experts are holders of the Offensive Security Wireless Professional (OSWP) certification.

Penetration tests for wireless networks usually include:

- Identification of all WiFi access points throughout a facility
    - Hidden SSID
    - Rogue WiFi access points
    - Unauthorized wireless networks with access to a corporate network
- WEP/WPA/WPA2 Preshared Key brute force attacks
- Attack on WPA/WPA2 enterprise
- Attack on WiFi Protected Setup (WPS)
- Identification of weak authentication (e.g. MAC filtering)

- Identification and exploitation of vulnerable services (HTTP, SNMP, Telnet, SSH, etc.) of WiFi routers
- "Man in the middle" attack (MitM) on end users connected to the WiFi network
- Bypassing of the captive portal
- Attempt to bypass guest and corporate WiFi segmentation
- Network flow analysis
- Setting up a rogue WiFi access point/Evil twin attack
- Exfiltration of data to the Internet using WiFi network (firewall bypass)
- Evaluation of WiFi router configuration
- KRACK attack
- Evaluation of physical access to WiFi routers