SECURITY TESTING

Test the security of your organization with the insight of a real attacker using an arsenal of offensive methods!

Offensive security methods can be useful in providing a realistic assessment of an organization's protections. The CENSUS Security Testing Services examine all components of an IT infrastructure against publicly known but also previously undisclosed (0-day) vulnerabilities and attack vectors, without causing any disruption to the target organization's processes.

CENSUS offers Security Testing Services as both independent and combined security testing modules, based on field best practices. A list of these services is provided below.

TIGER TEAM

Tiger Team testing is the ultimate way to realize an asymmetric attack against an organization. The Tiger Team targets the core business of the client institution, testing all layers of the organization's security architecture. It also makes every effort to remain undetected and shares information about the attack only with upper management. Payment on this service is required only in the case where the Team has successfully seized one or more of the designated targets.

PENETRATION TESTING

Penetration testing is the process of testing an IT infrastructure for security vulnerabilities in a controlled manner. The process varies according to the degree of knowledge provided by the client (Black Box testing, White Box testing, Gray Box testing, etc.); a mixture of these degrees of knowledge is useful for evaluating the effects of both insider and outsider attacks. Providing more knowledge may also shorten the time required to assess a system. The threat agents, exploitable vulnerabilities, impact vectors and, ultimately, the maximum risk paths identified through penetration testing can be used to extend and enhance an organization's risk assessment reports.

WEB APPLICATION TESTING

Web applications are the most common entry point of an organization's security perimeter. The Web Application Testing module evaluates web applications via a rigorous security assessment process. This process examines all functions of a Web Application (and their effects to a user's browser), all layers of the Web Application stack (from the application itself to the underlying operating system) and all tiers of the Web Application architecture (from the front-facing web server and load balancer to the back-end database and application server).

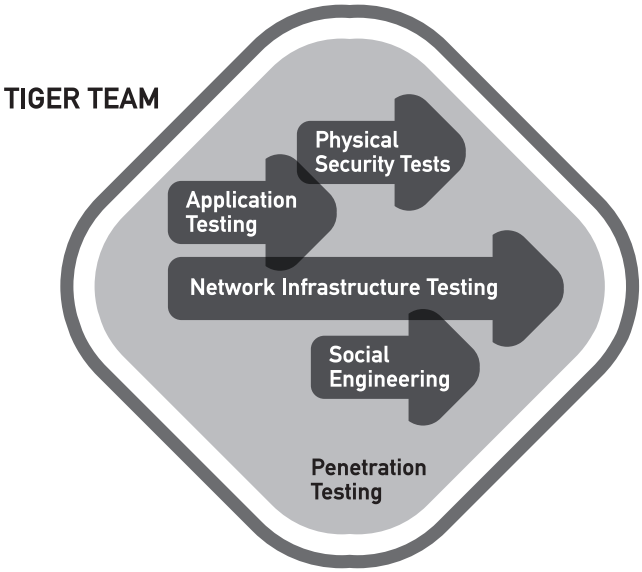
MOBILE APP TESTING

The Mobile App Testing Services assess the security of mobile applications and related (web or other) services. This security testing module combines a black box (or white box if code is available) assessment of the app code, live security testing of the app & related server APIs, and release testing of the app bundle.

NETWORK INFRASTRUCTURE TESTING

Network Infrastructure Testing examines all measures and controls used to implement security policies in an organization's network architecture, in order to assess the level of protection they provide. These include:

- **Network Firewalls:** Firewall-bypassing methodologies are used in order to ensure that the implemented rules offer maximum protection.
- **Routers and Wireless Access Points:** The routing infrastructure of the client's network is tested for security vulnerabilities, malfunctions and misconfigurations.
- **Intrusion Detection / Prevention Systems:** Polymorphic and metamorphic techniques among others, are used to assess the quality of the detection engines found in the client's infrastructure. Intrusion preventions systems are tested using a wide variety of payloads. Finally, the Intrusion Detection and Prevention systems themselves are examined for vulnerabilities.



SOCIAL ENGINEERING

Social Engineering tests the security awareness of the target organization's personnel. Social Engineering attacks are performed through both remote channels (landline/mobile telephones, VoIP, e-mail, "snail" mail) and local means. This module extends security testing to the human factor, exploiting the personnel's knowledge, privileges and habits.

PHYSICAL SECURITY TESTING

To assist in the holistic assessment of an organization's security, CENSUS offers a Physical Security Testing module. Within this module, the reliability and integrity of physical security controls, such as access authorization mechanisms for restricted zones, is evaluated. Physical Security Testing also tests the effectiveness of the implemented physical controls in terms of:

- Protecting sensitive information
- Protecting physical assets
- Collecting sufficient evidence that may later be used for the prosecution of intruders

For more information about the CENSUS Security Testing Services please visit our website at **www.census-labs.com**

CENSUS
IT Security Works

Stadiou 33, 10559,
Athens, Greece
T. +30 2110 128 355
F. +30 2310 947 234

I. Gkoura 16, 54352,
Thessaloniki, Greece
T. +30 2310 947 233
F. +30 2310 947 234

E. info@census-labs.com
www.census-labs.com