Penetration Testing

What is penetration testing?

A penetration test, is an authorized simulated attack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

In order to avoid potential misunderstandings, we will first define differences between vulnerability scanning and penetration testing, as the two phrases are commonly interchanged. However, their meaning and implications are very different. A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test (Pen Test) attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing typically includes network penetration testing and application security testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network.

How will we help you with our security assessment approach ?

Ibis Instruments is a company with extensive experience in security testing of different information systems. Our security team has more than 15 years of experience in stress and security testing of different products and the most complex infrastructures. Members of our staff include highly-skilled penetration testers who can test your system defenses and websites for vulnerabilities, carry out exploits in a safe manner and advise on appropriate mitigation measures to ensure that your systems are secure. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tools, tactics and procedures. Our approach is designed to assess your organization’s security before an attacker does.

When should you perform penetration testing?

Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system. Additionally, it should be performed whenever:

- ★ Security system discovers new threats by attackers.
- ★ You add a new network infrastructure.
- ★ You update your system or install new software.
- ★ You relocate your office.
- ★ You set up a new end-user program/policy.

Why should you perform penetration testing?

Penetration testing should be performed whenever you want to:

- ★ Manage the risk properly
- ★ Increase business continuity
- ★ Protect clients, partners and third parties
- ★ Help evaluate security investments
- ★ Protect public relationships and the company's reputation
- ★ Increase security awareness of your staff and associates
- ★ Define adequate protection measures in order to protect critical infrastructure

Our approach

Our approach is tailored to the needs of every single customer. Tools which we use are tools which are accepted as the best tools for penetration testing, as well as custom-made tools for tailored scanning processes. Our approach contains five steps:

• **Defining testing requirements**
These can be at least one of four main drivers for penetration testing such as growing requirements for compliance, the impact of serious security attacks on other similar organizations, the greater number and variety of outsourced services and significant changes to business processes.

• **Agreeing on the testing scope**
The scope of penetration testing needs to be defined prior to the commencement of testing activities. The scope depends on the target environment to be tested and the business purpose for conducting the test. It is also important to determine which systems are 'out of scope' in order to prevent ambiguity, which could result in incomplete coverage or unauthorized testing.

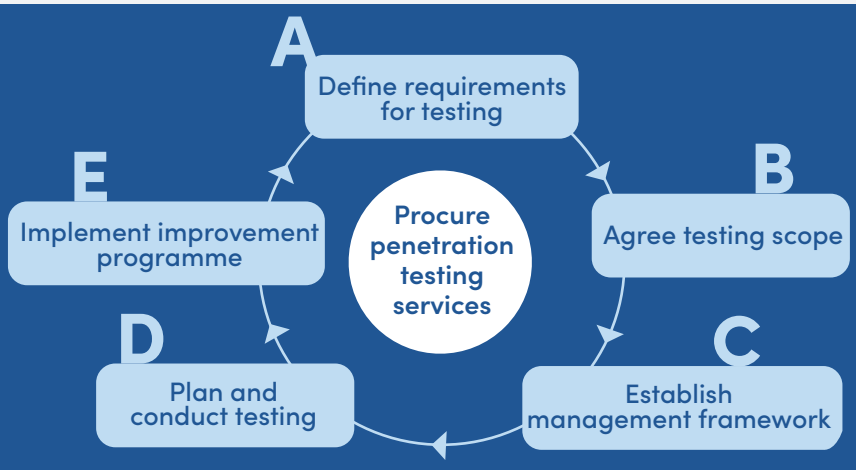
• **Establishing management framework**
An effective framework will provide assurance to the stakeholders that objectives of the penetration test(s) are achieved, contracts with suppliers are signed off and monitored, risks for the organization are kept to a minimum, any changes to the scope of the penetration test are managed quickly and efficiently, and problems are adequately resolved.

• **Planning and conducting the testing**
Within this step, we create and formalize penetration testing tools and steps which will be performed upon customer request. Some of the phases within this step are: planning, contact researching, identifying and exploiting vulnerabilities, reporting the findings and providing proposals for resolving identified vulnerabilities.

• **Implementing the improvement program**
Within this step, in cooperation with the customer, we implement proposals for resolving identified vulnerabilities. The customer can require our consultancy or direct implementation engagement.

In order to provide a more comprehensive approach, we have divided our approach in two levels as per the table below:

	Level 1	Level 2
Purpose	To determine potential vulnerabilities and how to remedy weaknesses in order of priority	To identify the full extent of your exposure to a determined hacker, the data that they could access or damage that they could cause
Outcome	To identify and analyze vulnerabilities so that a proportionate response can be made towards remediation.	This more thorough assessment of your security posture enables you to make more informed decisions about investing in securing your business-critical systems.
Target organization	You are exposed to opportunistic attackers searching the web for easy targets and want to get reassurance beyond a vulnerability scan.	Your application hosts sensitive or personal data or performs a mission-critical role in your business and could be exposed to a targeted attack.
Skill level required	High	Advanced
Emulates a real-life attack	Recreates the early stages of an opportunistic attack, assisting you in keeping off the radar of potential adversaries.	Full emulation of a targeted attack on your web application to extract data or undermine user confidence.
Objective	Agreed to kickoff	Agreed to kickoff
Fixed-price package	✓	✗
Scoping call with consultant	Available	✓
Testing methodology	Threat-driven approach	Threat-driven approach
Vulnerabilty scanning	✓	✓
Can be preformed on-site	✓	✓
Can be preformed remotely	✓	✓
Identification of false positives	✓	✓
Exploation of vulnerabilities	✓	✓
Detailed report	✓	✓
Manual grading of risk and impact	✓	✓



A structured approach to penetration testing

Service Overview

Ibis-Instruments Penetration Testing is tailored to your environment and needs to assess specific aspects of your security program and the security posture of your critical systems, networks and applications.
Our penetration tests use intelligence gained at the front line of incident response to identify gaps in your network infrastructure and configuration that would allow an attacker to access your most critical assets.

Penetration tests offered by Ibis-Instruments are tailored to the specific areas of your network, applications or products, and include:

Internal penetration test

External penetration test

Web application assessment

Mobile device/application assessment

Social engineering assessment

Wireless technology assessment

Perimeter testing

Risk assessment

Ibis Instruments
Measurement & Telecommunication Systems

Ibis Instruments Belgrade
Tošin bunar 272, 11070 Belgrade, Serbia
Office: +381 11 7152 200, Fax: +381 11 7152 201
e-mail: info@ibis-instruments.com
www.ibis-instruments.com

Ibis Instruments Banja Luka (branch office)
Jovana Dučića 37, 78000 Banja Luka
Office: 387 51 223 840, Fax: 387 51 223 841
e-mail: office-bl@ibis-instruments.com
www.ibis-instruments.com

Telecom Instruments Romania
Azur 2 - House F17, 31-33 Emil Racovita Street,
077190 Voluntari, Ilfov, Romania
Office: 4 021 320 3356 , Fax: 40 21 2110884
e-mail: office@telecominstruments.ro
www.telecominstruments.ro

Ibis Instruments DOOEL import-export Skopje
Veljko Vlahović 1-2/2, 1000 Skopje, Macedonia
Office: +389 2 321 5700, Fax: +389 2 321 5700
e-mail: info@ibis-instruments.mk
www.ibis-instruments.com/mk

Telecom Instruments Ltd. Bulgaria
Address: 15, Sveti Naum Blvd., 1421 Sofia, Bulgaria
Office: 359 2 969 1060, Fax: 359 2 969 1080
e-mail: office@telecominstruments.bg
www.telecominstruments.bg