



# Kaspersky Penetration Testing

kaspersky

Ensuring that your IT infrastructure is fully secured against potential cyberattack is an ongoing challenge for any organization, but even more so for large enterprises with perhaps thousands of employees, hundreds of information systems, and multiple locations worldwide.

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls in your corporate network to obtain high privileges in important systems.

## What is Kaspersky Penetration Testing?

Kaspersky's Penetration Testing gives you a greater understanding of security flaws in your infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of your current security measures and suggesting remedial actions and improvements.

The service helps you and your organization to:

- **Identify the weakest points in your network**, so you can make fully informed decisions about where best to focus your attention and budget in order to mitigate future risk.
- **Avoid financial, operational and reputational losses caused by cyber-attacks** by preventing these attacks from ever happening through proactively detecting and fixing vulnerabilities.

## Service Scope and Options

Depending on your needs and your IT infrastructure, you may choose to employ any or all of these services:



### External penetration testing:

Security assessment conducted through the Internet by an 'attacker' with no preliminary knowledge of your system.



### Internal penetration testing:

Scenarios based on an internal attacker, such as a visitor with only physical access to your offices or a contractor with limited systems access.

You can include any part of your IT infrastructure into the scope of penetration testing, but we strongly recommend you consider the whole network or its largest segments, as test results are always more worthwhile when our experts are working under the same conditions as a potential intruder.

# About Kaspersky's Approach to Penetration Testing

## Penetration Testing Results

The Service is designed to reveal security shortcomings which could be exploited to gain unauthorized access to critical network components. These could include:

- Vulnerable network architecture, insufficient network protection
- Vulnerabilities leading to network traffic interception and redirection
- Insufficient authentication and authorization in different services
- Weak user credentials
- Configuration flaws, including excessive user privileges
- Vulnerabilities caused by errors in application code (code injections, path traversal, client-side vulnerabilities, etc.)
- Vulnerabilities caused by usage of outdated hardware and software versions without latest security updates
- Information disclosure

Results are given in a final report including detailed technical information on the testing process, results, vulnerabilities revealed and recommendations for remediation, as well as an executive summary outlining test results and illustrating attack vectors. Videos and presentations for your technical team or top management can also be provided if required.

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky security experts with full regard to your systems' confidentiality, integrity and availability, and in strict adherence to international standards and best practices including:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Web Security Testing Guide
- Common Vulnerability Scoring System (CVSS)

Project team members are experienced professionals with a deep, current practical knowledge of this field, acknowledged as security advisors by industry leaders including Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens and SAP.

## Delivery Options

Depending on the type of security assessment service, your systems specifics and working practices, security assessment services can be provided remotely or onsite. Most services can be performed remotely, and internal penetration testing can even be performed through VPN access, while some services (like wireless networks security assessment) require an onsite presence.

Cyber Threats News: [www.securelist.com](http://www.securelist.com)  
IT Security News: [business.kaspersky.com](http://business.kaspersky.com)  
IT Security for SMB: [kaspersky.com/business](http://kaspersky.com/business)  
IT Security for Enterprise: [kaspersky.com/enterprise](http://kaspersky.com/enterprise)

[www.kaspersky.com](http://www.kaspersky.com)

© 2024 AO Kaspersky Lab.  
Registered trademarks and service marks  
are the property of their respective owners.

#kaspersky  
#bringonthefuture