ARICOMA

Penetration Tests

We perform simulations of cyber attacks on systems, applications and entire infrastructure. You can choose specific penetration tests for specific applications and systems from our range.

Application Pentests

- Web
- Mobile
- Desktop
- API

Infrastructure Pentests

- Internal
- External
- Stress/DoS tests
- Wi-Fi networks
- IoT

Configuration Tests

- Operating systems
- Cloud

Specialized Tests and Services

- ATM
- RFID
- Reverse Engineering
- Phishing
- Source Code Review
- Advanced White-Box
- Computer Forensics

Social Engineering Tests

Red Team Operations

With Red Teaming exercises, **you test your ability to detect an attack and respond correctly** through your processes and security specialists. We also offer a service that simulates phishing attacks using social engineering.

Application Pentests

Web
When testing applications, our goal is to detect vulnerabilities that may compromise their confidentiality, integrity or availability. Within the framework of application security, we not only deal with common attacks exploiting typical vulnerabilities, but also focus on the design or architecture of the application.

Mobile
When testing mobile applications, we look for security flaws and weaknesses in their implementation, both on the application side and on the server side. For business applications, we analyse potential risks and look for secure solutions for the use of mobile devices in the corporate environment. For mobile phones, we perform forensic analysis of devices that have been targeted by hacker attacks. We also test IoT applications and systems to verify that they are secure. We draw on all our experience to help create a more secure mobile world.

Desktop
For desktop applications, we decompile them to the source code level, and make any necessary modifications. We identify security risks, sensitive data or other flaws in the authorization or transmission between the client application and the server.

API
We conduct API penetration tests to check for any weaknesses in the service delivery interface. With APIs, we test different types of interfaces, the most common being REST and SOAP. We use the relevant parts of the OWASP methodology for testing web applications and also our own methodology, which is based on our experience testing API services, PSD2 and others. .

Infrastructure Pentests

Internal
When conducting pentests on internal infrastructure, we map the company's internal network, identify active network elements and verify their security. We attempt to crack selected systems and compromise the company's domain by escalating privileges from a regular user to a domain administrator. They also include tests from a normal user's workstation.

External
When conducting pentests on external infrastructure, we primarily aim to discover all available network services, components and enumerate them in detail. Collecting public information about a company's network infrastructure is crucial for an attacker. For this purpose, we use both automated and our own proprietary tools and methodologies.

Stress
Attackers often damage companies' websites by simply making key web applications inaccessible. The longer a web application is unavailable to users, the greater the losses. As part of Denial of Service, we test selected services to ensure that these situations do not occur and that critical web applications continue to function under unexpectedly high load.

IoT
Our main focus when testing the Internet of Things (IoT) is to determine how easy a target the devices are. What information can be extracted from them, and how to detect vulnerabilities that can be exploited to gain unauthorized access or steal data.

Configuration Tests

Operating Systems
In operating systems, we check the security level of individual configuration elements. We also offer to implement recommendations that we issue based on the results of our tests, eliminating the weaknesses found and increasing your defenses in the event of a sudden real attack.

Cloud
Business infrastructures, web applications and other internet services are now largely hosted in the cloud. Configuring these services, whether native or third-party, plays a key role in security. Configuration flaws can lead to the loss of company data and client trust, so we're ready to help you configure your cloud environment securely. We currently specialize in AWS, MS Azure and MS 365 services.

Social Engineering Tests
Social engineering is an act by which a social engineer attempts to get his target to perform an action that may not be in the best interests of the subject. Employees are considered to be the weakest link of security in a company. This means an attacker can use social engineering to breach even the most secure perimeters. Social engineers use attacks such as vishing, phishing, or physical infiltration through impersonation. Our goal is to examine your company's security using these methods and then propose the best solution to eliminate the risks found.

Red Team Operations
Standard pentesting methods detect various types of vulnerabilities, but do not test the ability to detect, respond to, and recover from a cyber attack. Red Team Operations, also known as Red Teaming, is derived from the term Red Team, which refers to a team of experienced ethical hackers who execute an attack using the same sophisticated means as real attackers. Red Teaming therefore faithfully simulates attack threats using the latest technologies and tactics, and also provides information on a company's readiness to detect, eliminate and remediate these attacks.

Wifi Networks
Penetration tests on Wi-Fi technologies simulate an attack on access to an organization's internal network via a Wi-Fi wireless signal. After gaining access, we check the quality of traffic filtering between the Wi-Fi client network segment and the rest of the internal networks. Our tests also include analysis of the configuration of the client-side wireless network connection.

NFC / RFID
In a corporate environment, RFID or NFC technology is most often used in the form of entry cards to control physical access to a building, but there are many other applications. During the analysis, we check the security of the solution in place and its ability to prevent unauthorized access to the building, the theft of data stored on the card or the modification of its content. For RFID technologies, we replicate publicly known attacks on specific types of cards and also undertake our own research into possible vulnerabilities and potential attack vectors.

Our main services

- Social Engineering Tests
- Application Pentests
- Source Code Review
- Cloud service pentests
- Infrastructure Pentests
- Configuration Tests
- Wi-Fi network pentests
- Mobile device pentests
- Red Teaming

Specialized tests and services

ATM
We'll scan for ATM vulnerabilities within a week. Our comprehensive analysis includes physical access methods, privilege escalation, operating system and application tests. However, we can only focus on pentesting infrastructure, integration services and management, reverse analysis of software, or security analysis of source code.

Reverse Engineering
In reverse engineering, we reverse-engineer the functionality of the applications being tested, without access to or knowledge of their source code, to verify their resilience to potential real-world attacks. When analyzing the code, we use our experience from penetration tests of desktop clients.

Phishing
We test companies' resilience to ransomware attacks. During the review, we analyse existing situations, including a system resilience test. The result is a report with recommendations for appropriate solutions.

Codebashing
If you develop applications, we offer solutions for application security education and evangelism through Codabashing. This enables security and development teams to create and maintain a secure development culture. Using communication tools, gamification, peer challenges and ongoing assessments, Codebashing helps you eliminate software vulnerabilities in your source code.

Computer Forensics
The goal of computer forensics is to examine digital media and data in order to identify, preserve, recover, analyze, and then present facts and findings. The findings can subsequently be used as evidence in computer crime trials as well as in civil proceedings.

Advanced White-box
This is a combination of penetration testing and secure code review or other assessment services. The goal of advanced white-box is to comprehensively verify the security of applications under development by simulating hacker attacks, automated code analysis, manual code reviews and audits.

hackingLab

We have set up a community project where we share know-how and build an attractive platform for regular meetings that move our members forward.

We deliberately bypass the logic of the products and systems being tested. We hack their processes and seek vulnerabilities, implementation and security flaws.

Join the IoT device security testing program
We will analyze your devices and describe the security vulnerabilities found in a detailed report with suggestions for remediation.

Let us know if you are
- an IoT and smart technology manufacturer
- a dealer who wants to offer your clients quality service
- a user who is unsure about the quality of security of the product you have purchased

For more information about HackingLab, the community and collaboration opportunities, visit hackinglab.cz.