RMRF Generating value - defeating hackers

Pentest

RMRF – is a Ukrainian team of cybersecurity engineers who specialize in the development of solutions in the field of early cyber threat detection and prevention. Each member of our team has over 10 years of experience in project development in different business areas in Eastern Europe. RMRF's main expertise is providing cyber security services such as digital forensics, penetration testing and the development of deception technology solutions.

Pentest

Pentest (Penetration test) is an assessment of a company's IT security system. During a pentest a real attack by hackers is simulated. The simulated attack includes exploitation of IT infrastructure vulnerabilities, social engineering and exploitation of weaknesses in administrative processes or corporate policy. A pentest is performed by certified specialists in accordance with international standards and methodologies.

Through a pentest an organization receives information about its discovered weaknesses and vulnerabilities. The elimination of the vulnerabilities, combined with the revisions and improvements of business and monitoring processes, helps minimize or avoid potential attacks in the future.

Pentest may be needed in the following cases:

- Organization is a part of critical infrastructure
- Recent attacks on the organization or other members of its industry
- Insider's activity suspicion
- High risk of industrial espionage
- Exclusive requirements to data protection caused by internal and external standards

Pentest results

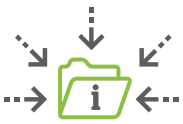
- Assessment of staff proficiency in terms of incident response
- Rationale for improvement of organization's security system
- Revealing of IT system vulnerabilities, which couldn't be detected by automated tools
- Potential threats classification
- Evaluation of potential impact of hackers' attacks on IT infrastructure and business in general
- Guidelines for a prioritized security improvement of IT infrastructure elements and business processes

Pentest process

RMRF

Generating value - defeating hackers

How it works



1 Intelligence gathering

Gathering information about the structure and current capacity of organization's IT system, as well as about all possible penetration paths to the system. It includes:

- Automated data gathering
- Manual data gathering

2 Modeling of threats

- **Information assets analysis.** Those assets include own R&D projects, marketing data, financial, technical and other commercially sensitive information, as well as personal data of the company's employees and customers.
- **Human resources analysis.** Investigation of such factors as organizational structure and hierarchy, level of access to information assets and the level of authority of particular employees, the level of social engineering risk.
- **Business processes analysis.** Examination of critical business processes.
- **Potential threat agents' analysis.** Identifying possible internal (insiders) and external (company's counterparties, organized hackers' groups, single hackers).
- **Threat capabilities analysis.** Includes analysis of tools and communication mechanisms available to potential attackers.
- **Possible motivation modeling.**
- **External information analysis.** Relevant news search about attacks to similar organizations.

3 Vulnerabilities analysis

- Active testing
- Passive testing
- Results validation
- Research of possible exploitations of found vulnerabilitiess

4 Vulnerabilities exploitation

Unauthorized access to the organization's information system bypassing current security restrictions

5 Post-exploitation activities

Determination of attack consequences

6 Reporting and recommendations

Pentest results are formalized including an assessment of the risks of the detected ulnerabilities

Benefits to businesses of conducting a Pentest

Complex security assessment in case of new IT infrastructure implementation or modernization of existing one

Assessment of current security level of existing information IT system

Organization planning in the IT sector

HR policy formalization and improvement

Advantages of RMRF Pentest Services

- Top professionals are hands-on involved with each client.
- Maximum proportion of manual work on the intelligence gathering stage, permitting analysis of all needs and special aspects of a particular organization and discovery of vulnerabilities, which are often invisible to automated tools