

Penetration Testing



When you think it's all over, hackers start a new shift...

Penetration testing simulates real-world attacks and examines the functionality of the security mechanisms during normal common operation. Attacks can be conducted secretly or openly from the internal IS infrastructure, or from the external environment, focusing on a concrete object or all accessible systems, based on the given conditions.

The strength of RAC penetration testing lies in the highly professional approach and skilled background of our specialized and reputable company, and in the selection and application of independent multi-platform and highly specialized testing toolsets and best practices. For our work, we mainly use the *QualysGuard®*, a proven technology for penetration testing, which has the largest knowledge base of vulnerability signatures in the industry and is updated on a daily basis. RAC always concentrates on using a systematic approach to its work and delivering solutions and services based on international standards for ISMS and QMS.

We perform hacker attack simulations on your systems, including security control and safeguard recommendations.

Basic proposal of penetration tests

RAC is prepared to perform testing done according to individual customer's requests and conditions using these basic tests:

Testing from external environment
• footprinting and network discovery
• classical penetration testing
• hidden penetration testing
Testing from internal environment
• testing inside LAN / WAN / DMZ network
- systems inaccessible from Internet
- intranet systems verification
• host-based testing
- local vulnerabilities testing
- domain policy testing
Wireless wi-fi networks testing
• wi-fi networks monitoring
• wi-fi traffic analysis
• penetration testing of access points
• penetration testing of VPN access points
Continuous security and penetration testing
• RAC CISS service
Continuous vulnerability management
• RAC QGVM service

RAC competitive advantages

RAC ISSEC: methodology for practical security examinations in all phases of the ISMS lifecycle

RAC CISS: service for continuous, proactive security screening of Internet connections

RAC QGVM: design, implementation and support of vulnerability management process based on the QualysGuard® technology

Primary objectives of penetration testing

- ♦ footprinting and network discovery of target Internet domain or IP range and identification of accessible systems
- ♦ a complex penetration testing of all accessible servers, firewalls and other network appliances and their vulnerabilities
- ♦ countermeasure recommendation for discovered weaknesses and vulnerabilities

Hidden penetration testing

- ♦ conducted secretly and silently only (without informing IT administrators or outsourced company for network administrations)
- ♦ probes the readiness and functionality of internal response protection mechanisms

Testing from internal environment

- ♦ detailed testing of the systems inaccessible from the Internet (DMZ, WAN, LAN) or security intranet systems verification
- ♦ optional host-based testing of vulnerabilities and security of domain policy setting (only for some OS systems)

Wireless wi-fi networks testing

- ♦ wi-fi segment monitoring and identification of the accessible wi-fi systems
- ♦ wi-fi networks accessibility outside the organization perimeter
- ♦ detailed and complex testing of all detectable AP/VPN access points