Penetration Testing Services
Demonstrate Real-World Risk

The best way to know how intruders will actually approach your network is to simulate a real-world attack under controlled conditions. This documents actual risks posed to your company from the perspective of a motivated attacker.

Rapid7’s Penetration Testing Services team delivers network, application, wireless, social engineering and boutique engagements to demonstrate the security level of your organization’s key systems and infrastructure.

**Leverage offensive security experts to test defenses and uncover issues**

Get an understanding of real-world risks from the attacker’s perspective – Go beyond the limitations of automated scanning to identify the root cause of underlying issues. Our penetration tests simulate real-world attack vectors to provide a point-in-time assessment of vulnerabilities and threats to your network infrastructure and applications.

Quantify and prioritize findings using business-driven criteria – Our post-assessment analysis presents logical groupings of one or more security issues with common causes and resolutions. We provide an actionable findings matrix that can be used as an overarching workflow plan and tracked within your security organization.

Enable your operations team in tracking the remediation effort – Each finding is categorized according to the relative level of risk posed to your organization. The final deliverable also contains the amount of work and resources required to address each finding, hyperlinked references to resources, and detailed remediation information.

Rapid7’s penetration testing services include:

- Internal and external network testing
- Web and mobile application testing
- Wireless network testing
- Social engineering (physical and electronic)
- Boutique engagements, e.g. DDoS, APT, embedded device testing, malware, etc.
“Rapid7 had great expertise. When you hire a person – or a group of individuals – to do a job like this, you want someone who has done extensive penetration testing, who eats, sleeps, and breathes security, who can think like a hacker.”

-Jaya Ayyagari

VP of Software Development, EyeLock Corporation

Why Penetration Testing?

**Uncover security weaknesses**
Learn whether and how your network is exposed to potential attacks.

**Check security controls**
Test if the security measures you’ve put in place are working and effective.

**Test security of new applications**
Conduct a comprehensive security assessment before the roll-out.

Compliance and best practices
Some regulations such as Payment Card Industry Data Security Standard (PCI DSS) require regular penetration tests. Beyond compliance, many best practice frameworks recommend conducting penetration testing.

Contractual obligations
Larger enterprises require a penetration test as part of doing business with them.

Proven penetration testing services and security expertise to meet unique business needs:

**Best practice methodology**
Rapid7 leverages the Open Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), and for application testing, the Open Web Application Security Project (OWASP) as foundation for assessments.

**Comprehensive tools and processes**
Rapid7 uses a combination of proprietary and public tools to gather the most accurate data efficiently.

**Customized services approach**
Support for boutique engagements aligned with specific objectives, technologies, platforms, or threats.

**Risk scoring using the DREAD framework**
Address the top threats that have the greatest potential impact by applying a structured approach.

Learn more about Penetration Testing Services at: www.rapid7.com/services/penetration-testing-services