Penetration Testing

Ethical Hacking Designed to Uncover Vulnerabilities

What is Pen Testing?

Penetration testing is when authorized security professionals test an organization's security by attempting to breach systems in the same way a malicious attacker would. The testing team simulates an attack to document weaknesses an attacker could exploit. The target organization then analyzes and mitigates those weaknesses, often with support from the testing team.

Different types of penetration testing are used to evaluate various systems in different situations. One of the most effective ways to reduce risk to mission-critical systems and data is to conduct regular network and application penetration testing.

RSI Security's penetration testing services simulate real-world cyberattacks against your existing architecture to uncover gaps, vulnerabilities, or entry points that malicious actors could exploit. All tests are conducted within a clearly defined scope, under signed authorization, to ensure full legal and ethical compliance.

Why Do You Need Testing?

One of the most critical challenges for IT departments and leaders across industries is determining whether tools, systems, settings, and configurations are working together effectively to prevent cyberattacks and meet security expectations.

- Penetration and vulnerability testing services help organizations:
- Identify gaps between security tools
- Prioritize potential cybersecurity risks
- Discover backdoors and misconfigurations
- Identify potential attack vectors
- Gain insight into the effectiveness of existing security controls, helping maximize security investments
- Improve incident response by identifying weaknesses before an actual breach occurs

Value of Early Testing

Identify Security Gaps Before Attackers Do

Simulated attacks expose weak points in systems, applications, and networks so they can be addressed proactively.

Support Security and Assessment Readiness

Penetration testing provides technical insight that organizations can use to prepare for regulatory and customer security assessments.

Focus on Real-World Risk

Go beyond checklists — testing highlights which vulnerabilities matter most and how they could be exploited.

Build Trust with Clients and Stakeholders

Demonstrates a mature security posture and provides confidence to customers, partners, and auditors.

Our Network Penetration Testing Services

Network Security Penetration Testing

Internal networks present numerous potential attack paths, including systems, hosts, and network devices. RSI Security's network penetration testing identifies which areas of your environment are most vulnerable to attack.

Firewall Penetration Testing

Firewalls monitor incoming and outgoing traffic to filter and detect malicious activity. External penetration testing helps identify gaps or weaknesses in firewall configurations that could allow unauthorized access.

Web Application Penetration Testing

RSI Security conducts web application penetration testing using either a white-box or black-box approach. Engagements include manual testing and technical review across authentication, authorization, cryptography, input validation, and client-side controls.

Cloud Computing Penetration Testing

Whether you use AWS, Azure, or another cloud provider, we test for misconfigurations, weak access controls, and shared-responsibility risks to help ensure your cloud environment aligns with provider security best practices.

Mobile Penetration Testing

We test mobile applications and devices for security risks related to data leakage, insecure APIs, and insufficient platform controls across iOS, Android, and enterprise mobile environments.

The RSI Security 5-Step Approach
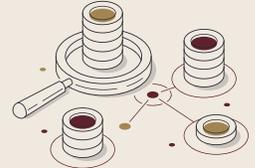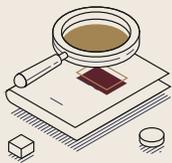
Plan & Prevent	Align with Your Business	Full Transparency	Test	Engagement Support
We prioritize proactive planning, preparation, and prevention—avoiding the pitfalls of reactive, disruptive troubleshooting.	Every technical recommendation is grounded in your business objectives, supporting strategic alignment and informed decision-making.	From engagement kickoff through final delivery, we operate under a strict "No Surprises" approach — clear communication and predictable outcomes.	Our penetration tests are reliable, timely, and cost-efficient, while minimizing impact to daily operations.	You'll receive dedicated tester-led support throughout the engagement, including results walkthroughs and remediation guidance—no generic service, and no getting lost in the shuffle.

RSI Security's penetration testing services are technical security testing activities and do not constitute compliance audits, certifications, or attestation services. Test results may be used by organizations to inform remediation efforts and prepare for independent third-party assessments.

Ready to Take the Next Step?

Penetration testing is essential for identifying and reducing risk across modern IT environments. RSI Security's expert-led penetration testing services help organizations uncover and mitigate vulnerabilities across networks, applications, cloud environments, and more.

858.999.3030 | info@rsisecurity.com | rsisecurity.com