hadengrey
Your Cybersecurity Services Experts

# PENETRATION TESTING SERVICES

**SIMULATE REAL ATTACKS. EXPOSE REAL RISK. STRENGTHEN REAL SECURITY.**

Cyber attackers constantly evolve their techniques to bypass defenses and exploit weaknesses. Automated scans alone cannot replicate real-world attack behavior or uncover complex attack paths.

**Haden Grey's Penetration Testing services simulate real-world attacks to identify exploitable vulnerabilities before adversaries do.** Our expert testers combine manual techniques, advanced tooling, and threat-informed methodologies to uncover security gaps and provide actionable remediation guidance.

Our approach delivers more than findings—we provide context, risk prioritization, and clear recommendations to measurably improve your security posture.

## SERVICE OVERVIEW

Haden Grey delivers comprehensive penetration testing services across networks, applications, cloud, and users. We help organizations:

- Identify exploitable vulnerabilities
- Validate real-world attack paths
- Test detection and response capabilities
- Meet compliance and regulatory requirements
- Reduce breach likelihood
- Strengthen overall security resilience

All testing is conducted with strict rules of engagement, minimal operational disruption, and clear communication throughout the engagement.

## OUR DELIVERY METHODOLOGY

| Plan | Test | Report | Improve |
|---|---|---|---|
| Define scope, objectives, and rules of engagement. | Conduct controlled, expert-led testing. | Deliver clear, prioritized findings. | Support remediation and validation. |

# CORE CAPABILITIES

## 1. External Penetration Testing

***See What Attackers See***

We simulate attacks from an external threat actor perspective.

**Capabilities Include:**

- Internet-facing asset testing
- Perimeter defense evaluation
- Service enumeration and exploitation
- Credential attack simulation
- Exposure validation

**Benefits:**

- Reduced external attack surface
- Early detection of critical flaws
- Improved perimeter security

## 2. Internal Penetration Testing

***Assume Breach. Limit Impact.***

We simulate insider threats or post-compromise scenarios.

**Capabilities Include:**

- Lateral movement testing
- Privilege escalation
- Active Directory attack paths
- Segmentation control validation
- Sensitive data access testing

**Benefits:**

- Reduced blast radius
- Better segmentation validation
- Stronger internal defenses

## 3. Web Application Penetration Testing

***Protect Customer-Facing Systems***

We identify vulnerabilities in web applications and APIs.

**Capabilities Include:**

- OWASP Top 10 testing
- Business logic testing
- Authentication and session testing
- API security testing
- Input validation and injection testing

**Benefits:**

- Reduced app-layer risk
- Protection of customer data
- Safer digital services

## 4. Cloud Penetration Testing

***Test Modern Cloud Environments***

We evaluate cloud security posture and configurations.

**Capabilities Include:**

- Cloud configuration review
- Identity and privilege testing
- Storage exposure validation
- Serverless and container testing
- Multi-cloud assessments

**Benefits:**

- Reduced cloud misconfiguration risk
- Improved cloud governance
- Better identity controls

## 5. Social Engineering Testing

***Test the Human Element***

We assess susceptibility to social attacks.

**Capabilities Include:**

- Phishing simulations
- Vishing (phone-based) testing
- Physical security testing (optional)
- Awareness measurement

**Benefits:**

- Improved user awareness
- Reduced human risk
- Better training insights

## 6. Red Team Exercises (Advanced)

***Simulate Real Adversaries***

We conduct objective-based, stealth-focused engagements.

**Capabilities Include:**

- Threat actor simulation
- Detection evasion techniques
- Multi-stage attack scenarios
- Blue team coordination (purple teaming)

**Benefits:**

- Realistic security validation
- SOC effectiveness testing
- Executive-level insights

## ADVISORY & PRE-TEST SERVICES

- Scoping and risk alignment
- Rules of engagement development
- Compliance-driven testing design
- Threat modeling alignment
- Attack surface review

## COMPLIANCE SUPPORT

Our testing supports regulatory and industry requirements such as:

- PCI DSS
- HIPAA
- SOC 2
- ISO 27001
- GLBA
- NIST-aligned programs

## OUR METHODOLOGY

Haden Grey aligns testing to recognized standards such as:

- OWASP Testing Guide
- NIST SP 800-115
- PTES (Penetration Testing Execution Standard)
- MITRE ATT&CK-informed techniques

## REPORTING & REMEDIATION SUPPORT

Our reporting is clear, actionable, and business-focused.

**Deliverables include:**

- Executive summary
- Technical findings with proof-of-concept
- Risk-based prioritization
- Remediation recommendations
- Optional remediation validation re-test

## BUSINESS OUTCOMES

Organizations partnering with Haden Grey achieve:

- Reduced breach risk
- Validation of security controls
- Clear remediation priorities
- Stronger compliance posture
- Improved detection and response readiness
- Greater confidence in security investments

## WHY HADEN GREY

Clients choose Haden Grey for:

- Deep offensive security expertise
- Highly skilled, certified testers
- Vendor-neutral, unbiased assessments
- Real-world attack simulation
- Clear, actionable reporting
- White-glove client experience
- Practical, risk-based recommendations

HadenGrey.com
Solutions@HadenGrey.com
(303)529-0467