cowbell® PT

Penetration Testing

Uncover hidden vulnerabilities in your applications and networks by simulating real-world attacks, boosting your defenses and fortifying your security.

Key Benefits of GMI Penetration Testing

We utilize active and passive pen testing tactics to uncover more vulnerabilities, enabling effective remediation.

1. Actionable Knowledge is Power

Our hackers leave no stone unturned, providing detailed reports with context, suggested resolutions, and compensating controls. This empowers leadership with risk-based information for guided decision-making.

2. Cost Savings and Avoidance

The average cost of a data breach in the U.S. is $8.19 million. Investing in penetration testing saves money on incident response and potential damages.

3. Compliance and Public Assurance

Our services improve internal processes and security posture while ensuring regulatory compliance, safeguarding customer data, and protecting your brand.

4. Identify and Prioritize Risks

Regular penetration tests help evaluate security and prioritize risks, giving organizations an advantage in anticipating and preventing attacks.

5. Prevent Hackers from Infiltrating Systems

Penetration tests simulate real attacks, revealing security holes and providing the opportunity to remediate weaknesses before actual threats occur.

6. Mature Your Environment

Ongoing improvements in security posture demonstrate to clients your dedication to information security and compliance, enhancing your competitive advantage.

7. Avoid Costly Data Breaches and Loss of Business Operability

Recovering from data breaches can be extremely costly. Regular penetration tests can help prevent financial loss and protect your brand's reputation.

8. Comply with Industry Standards and Regulations

Our tests address compliance obligations mandated by standards like PCI, HIPAA, and ISO 27001, demonstrating due diligence in information security.

Penetration Testing Packages

STANDARD PACKAGE*

✓ Internal and External Network

- Initial Nessus Vulnerability scan utilizing Client PC or server infrastructure
- Black Box network penetration test of up to 20 internal IPs and 3 external IPs utilizing manual scripts, Metasploit and other custom penetration testing tools
- Specialized vulnerability identification for up to 3 servers showing critical missing patches, vulnerable services, directory indexing, improper error, exception management, and information leaks.
- Cursory test of workstations based on common builds for up to 3 samplings

✓ Website

- BurpSuite, manual scripts, and custom penetration testing tools on up to 1 website

ADVANCED PACKAGE

✓ Internal and External Network

- All services included in the standard package for up to 50 internal IPs, 10 external IPs, and 10 servers

✓ Website

- All services included in the standard package for up to 2 websites

✓ External Web Application

- Black Box testing of the external web application
- Application can have up to 1 Login System, 4 API Inputs, 4 Functions, and 4 Roles.
- Utilization of BurpSuite, manual scripts, and custom testing tools
- No code review included

*Testing will be limited based on access provided by the client. GMI prefers jump box access for remote access .

To get started, visit **cowbell.ai** or email **crs@cowbell.ai**.

cowbell®

Resiliency Services