

# Penetration Testing

## Description

During penetration testing engagements, our consultants assume a pre-agreed upon role, usually that of an outside motivated attacker or an internal malicious employee. From this perspective, we use a strict methodology to breach defensive systems and attempt to retrieve a trophy—a resource or piece of critical business information that proves we were able to break into your systems. Once this is complete, we provide a report detailing the techniques we used, the systems we broke into, and, of course, how to fix the flaws.

### BENEFITS:

- *Realize True Security Level*
- *Rationalize Security Investment*
- *Meet Regulatory Requirements*

## Methodology

For penetration tests to be effective, they must be highly customized to every client. Few networks will have the same mix of network devices, workstations, servers and applications. With this in mind, during our penetration tests, we follow a strict methodology defined below:



To provide the most comprehensive penetration test results possible, our consultants work closely with your organization to clearly define the network components to be attacked.

## Deliverables

Upon completion of the engagement, you will receive the following items:

- Executive Summary Risk Matrix
- Detailed Technical Findings with Remediation Steps
- Strategic Next-Step Recommendations

Our executive summary risk matrix assists management with spending security dollars most effectively. We take the guesswork out of the vulnerability remediation process by providing an implementable action plan to immediately begin reducing the risks facing your organization.

### ASSESSMENT

Vulnerability Assessment  
Penetration Testing  
Web Application Testing  
Source Code Review

### REMEDIATION

Vulnerability Remediation  
Policy Development  
Secure System Design  
Procedure Development  
Security Training

### RESPONSE

Incident Response  
Forensics  
Expert Witness Support  
Program Development