



### Better protect your business by uncovering security weaknesses















The first tactical step you can take to begin the identification process for weaknesses in your IT environment is security penetration testing. Our security professionals use proven techniques and tools to help you evaluate your technical, administrative, and management security controls, and conduct tests against your internet perimeter using real-world attacks techniques – both automated and manual.

- > Review of network, operating system, application, and endpoint security measures
- > Test the ability of network defenders to successfully detect and respond to attacks
- > Identify vulnerabilities that may be getting missed by automated scanning software
- > Understand what can happen if business assets are compromised
- > Comply with industry-driven regulatory requirements for ongoing testing

#### Business Value

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Standardized scalable, repeatable testing
- Knowledge transfer

## Zones Security Penetration Testing

Steps	Professional Level	Enterprise Level	Enterprise + Level
<b>Automated Security Scanning:</b> Commercial scanning tools used to identify potential vulnerabilities			
<b>Report Development and Interpretation:</b> Analyze results and remove false positives			
<b>Network Architecture Review:</b> Review network security design and identify weaknesses			
<b>Manual Exploit Testing:</b> Perform manual in-depth testing techniques to validate weaknesses			
<b>Security Policy Review:</b> Review up to five security policies for gaps in procedures			
<b>Automated Security Re-Scan (within three months):</b> Re-scan identified systems after patches are put in place			
<b>Black Box Testing:</b> Perform system identification without prior knowledge from the client on devices			

## Three Types of Testing

### External Penetration Testing

- > Simulates an external or outside attacker
- > Probes, identifies, and exploits vulnerabilities in systems within scope
- > Attempts to breach the security perimeter of the network boundaries
- > Attempts to gain access to systems within scope, upon breach

### Internal Penetration Testing

- > Simulates an internal attacker, from inside the organization
- > Attempts to escape out of the network boundaries
- > Attempts to gain unauthorized user access to systems within scope and systems connected to network

### Website Application Penetration Testing

- > Designed to meet best practices and industry regulations for application security such as PCI, HIPAA, and Red Flag
- > Assessment looks at the source code, the infrastructure, the operating systems, and the application functionality
- > Attempts to gain unauthorized access to systems connected to the web application