

# Network Penetration Testing



*To ensure that your network infrastructure is secure, you must identify what you're protecting and what you're protecting it from.*

## To Evaluate Your Security Stance, You Must Think Like an Attacker

The most accurate method to evaluate your organization's information security stance is to observe how it stands up against an attack. With Trustwave's penetration testing service, our experts perform a simulated attack on your network to identify faults in your system, but with care to ensure that your network stays online. Our external, internal and wireless penetration testing services follow a structured methodology to ensure a thorough test of your entire environment that includes a detailed report with tactical and strategic recommendations that take your business goals into account.

Every tool used in our penetration testing has been thoroughly tested in Trustwave's labs by staff that have performed numerous information security assessments of organizations in many industries including retail, healthcare, biomedical and pharmaceutical, among others.

## External Penetration Testing – From the Outside In

Our penetration testing service includes iterative tests of your environment starting with the most general components working toward the most specific. Trustwave's expertise and proven methodology allow us to effectively model attack scenarios that highlight risk from the largest, most complex environments to the most simple. Trustwave experts employ a primarily manual process to limit the generic results offered by general vulnerability assessments that use automated scanners and checklist methods.

## Internal Penetration Testing – Addressing Internal Threats

Internal threats can be the most devastating that organizations face today. Internal corporate LAN and WAN environments allow users greater amounts of access, but usually with fewer security controls. The fewer layers of security between a would-be attacker and sensitive data, the greater the risk of compromise. Depending on your needs, a Trustwave expert will report for work as an employee or contractor. Utilizing normal to minimal system access levels based on the simulated role, Trustwave iteratively tests all access controls in an attempt to acquire critical data.

## Testing Wireless Networks

Attackers commonly exploit unsecured wireless networks to gain greater access to a corporate network and compromise data. Trustwave will perform a penetration test of wireless networks using directed attack-based logic to identify the real risks inherent in your wireless infrastructure and what that risk means to sensitive data stored elsewhere. Trustwave tests a varied array of wireless technologies such as 802.11 Wi-Fi, application specific ZigBee, 900MHz networks, legacy FHSS technologies, 5.8GHz networks and others.

## About Trustwave

Trustwave is a leading, global provider of information security and compliance management solutions to large and small businesses and the public sector. Trustwave offers and supports SSL certificates, proprietary security appliances, managed security services and compliance management solutions to help organizations simplify, accelerate and validate their compliance with industry standards and regulations such as PCI DSS, HIPAA, SAS-70, GLBA and ISO 27002 (formerly 17799) among others. Trustwave's clients include financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

[www.trustwave.com](http://www.trustwave.com) 1-888-878-7817



## Trustwave's Proven Methodology

Trustwave's unique approach comprised of both reconnaissance and attack-modeling phases ensure that your network is tested to the full extent with minimal business impact.

**Network Mapping**— Trustwave will scan target network blocks via a list of Internet addresses to create a network map of the target environment.

**System Identification & Classification**— Trustwave then uses specific tools with TCP finger-printing functionality to identify the systems located on the network and classify them by operating system.

### System Tests

**System Vulnerability Identification**—Using automated tools, Trustwave scans each system for potential vulnerabilities. This information will be noted and false positive validation will be performed.

**System Vulnerability Exploitation**— Trustwave will inform key security contacts within your organization of specific vulnerability findings and explain the plan of attack for these vulnerable systems.

### Application Tests

#### Application Architecture Identification

Trustwave will use tools and manual intervention to identify the applications running on each system.

#### Application Exploitation

Again, Trustwave always notifies key security contacts before any exploitation occurs. Trustwave will attempt to exploit each system with a variety of techniques including, among others:

- Input Validation
- Buffer Overflow
- Cross Site Scripting
- URL Manipulation
- SQL Injection
- Hidden Variable Manipulation
- Cookie Modification

**System Compromise**— As our experts compromise your systems, they keep you informed so that you can make informed decisions about whether a particular system should undergo additional tests.

**Data Extraction**— Once our experts compromise a system, they determine whether that system holds critical data and files and download a sample of this data if so.

**Further Compromise**— Once a system has been compromised, its many trust relationships with other assets can lead to further exploitation. Trustwave will launch a new stage of discovery against the environment to identify any trust relationships that will allow further access to a system.

### Report Development & Delivery

From the general to the particular, Trustwave provides a comprehensive report on each layer of your network security along with detailed tactical and strategic recommendations to remediate deficiencies:

- Remote Access Security
- Short Range Wireless Security
- Network Mapping Results
- System and Application Testing Results
- Tactical and Strategic Recommendations

## Why SpiderLabs?

SpiderLabs services and delivery are backed by a full portfolio of information security resources:

### Expertise

The SpiderLabs team consists of some of the top information security professionals in the world. With career experience ranging from corporate information security to security research and federal and local law enforcement, our staff possesses the background and dedication necessary to stay ahead of the technical, legal, and management issues affecting your organization's information security.

### Experience

SpiderLabs has performed hundreds of forensic investigations and application security tests and thousands of ethical hacking exercises for a client list that includes Fortune 500 companies, small to mid-sized businesses, government security agencies and law enforcement agencies.

### Certification

Trustwave is certified by the National Security Agency (NSA), the agency responsible for assessing the US government's information security posture. We are also authorized by all major credit card brands to conduct investigations of compromised merchants and processors.

### Facilities

SpiderLabs maintains the most advanced application and hardware testing facility in the industry.

### Safety

SpiderLabs works closely with clients to ensure that all of its services are performed with strict confidentiality and rigorous legal oversight.

