Network Penetration Testing

PT

Penetration Testing

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

For organizations that need an expert assessment of their network security for strategic planning and to fulfill compliance requirements

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure—from the network to the application layer —to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

A Analyze | P Protect | V Validate

For more information about Trustwave's Elements of Compliance and Data Security please visit: www.trustwave.com

Evaluate Your Security Stance, 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 help 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 experts that have performed numerous information security assessments of organizations in the retail, healthcare, biomedical, pharmaceutical and other industries.

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 check-list 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. Depending on your needs, Trustwave can facilitate an internal penetration test either using the traditional method of deploying consultants to your facility, or testing can be conducted remotely using our Remote Penetration Test Appliance. Using either method you end up with a focused, iterative, manually based security test of your internal network infrastructure.

On-site Penetration Testing—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.

Remote Penetration Testing—Trustwave will deliver one of Trustwave's Secure Remote Penetration Testing Appliances to facilitate the remote access needed to conduct the penetration test.

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.

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave® Information Security & Compliance

Why Trustwave's SpiderLabs is the Best Choice

Trustwave's 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.

SpiderLabs℠

Trustwave's Proven Methodology

Trustwave always follows a highly structured methodology to ensure a thorough test of the entire target environment and each layer of your organization's security stance. Our unique approach comprised of both reconnaissance and attack-modeling phases ensures that your network is tested to the full extent with minimal business impact.

Reconnaissance

Moving from the general to the specific, Trustwave will begin by gathering information about your network and systems. The consultant will use this step to gain an understanding of the network topology, design philosophy and security controls present.

Network Mapping— Trustwave will use both technical and non-technical techniques for this purpose. Depending on the network, methods such as layer 2 ARP sweeps, RF profiling, or more traditional methods such as port scanning, may be used.

System Identification & Classification—Trustwave again uses technical and non-technical methods to identify the systems, network components and security devices located on the network, and classifies them.

Network Tests

Low Level Network Testing—Taking a holistic view of your network architecture, Trustwave will gather vital information at this stage that may aid our consultant (or an attacker) in compromising internal systems and applications.

System Tests

Systemic Vulnerability Identification and Development of Attack Paths—Trustwave consultants will use the knowledge of your network to map out potential attack paths and vulnerabilities that may be exploited. At this stage they will collect necessary information and determine a plan for linear and non-linear attacks

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

Once Compromised

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

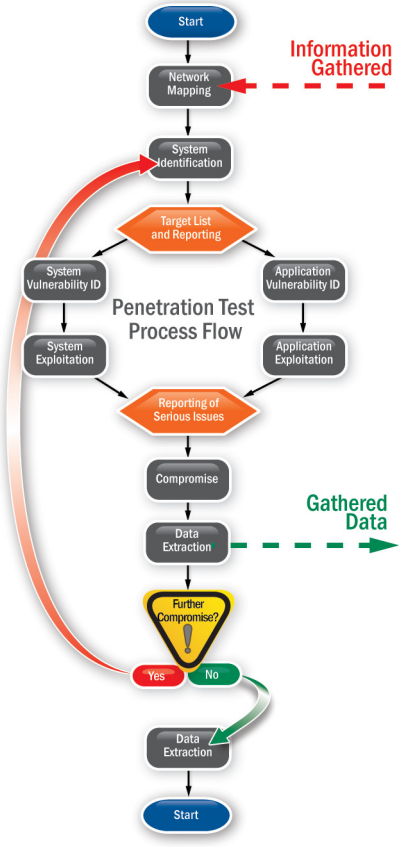
Data Extraction—Once our experts compromise a system, they determine whether that system holds critical data and files and download a sample of this data if so.

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

Upon conclusion of testing, Trustwave provides you with a report detailing results and recommendations on mitigating your network vulnerabilities, including:

- Assessment of design and operating effectiveness of existing controls
- Overall risk level rating
- Identified risks and potential areas of vulnerability
- Security risk mitigation recommendations
- Architectural and procedural recommendations
- Files, passwords or system information obtained during the test



Trustwave Methodology

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave® Information Security & Compliance