E COM SECURITY®
SOLUTIONS

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.

What's included?

- Network Vulnerability Scan
- Unauthenticated Web App Scan
- Validation Of Scan Results
- Manual Pen Testing:
  Most Exploitable Findings (Top 10+)
- Manual Pen Testing:
  Any Exploitable Vulnerabilities
- Vertical Escalation
- Horizontal Escalation
- Attack Chains
- Escalation To Adjacent Systems
- Client Side Attacks
- Custom Protocol Attacks
- Limited Phishing
- Escalation To Internal Network
- Findings Report
- Video Evidence
- Post-Test Debrief

For more information

Visit www.ecomsecurity.org to learn how we can help secure your organization.

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. 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. We follow a structured methodology to ensure a thorough test of your entire environment and meet regulatory requirements as PCI DSS, GLBA, HIPAA, SOX, FISMA/NIST.

External Penetration Testing—From the Outside In

Our external penetration testing service includes iterative tests of your environment starting with the most general components working toward the most specific. Our expertise and proven methodology allow us to effectively model attack scenarios that highlight risk from the largest, most complex environments to the most simple. Our 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, we can facilitate an internal penetration test either using the traditional method of deploying consultants to your facility, or testing can be conducted remotely. Using either method you end up with a focused, iterative, manually based security test of your internal network infrastructure.

On-site Penetration Testing—Our expert will report for work as an employee or contractor. Utilizing normal to minimal system access levels based on the simulated role, we iteratively tests all access controls in an attempt to acquire critical data.

Remote Penetration Testing—We will facilitate this by secure remote access connectivity to conduct the penetration test.

Proven Methodology

We 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, we 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— We 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—We 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—our 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—We will inform key security contacts within your organization of specific vulnerability findings and explain the plan of attack for these vulnerable components.

Once Compromised

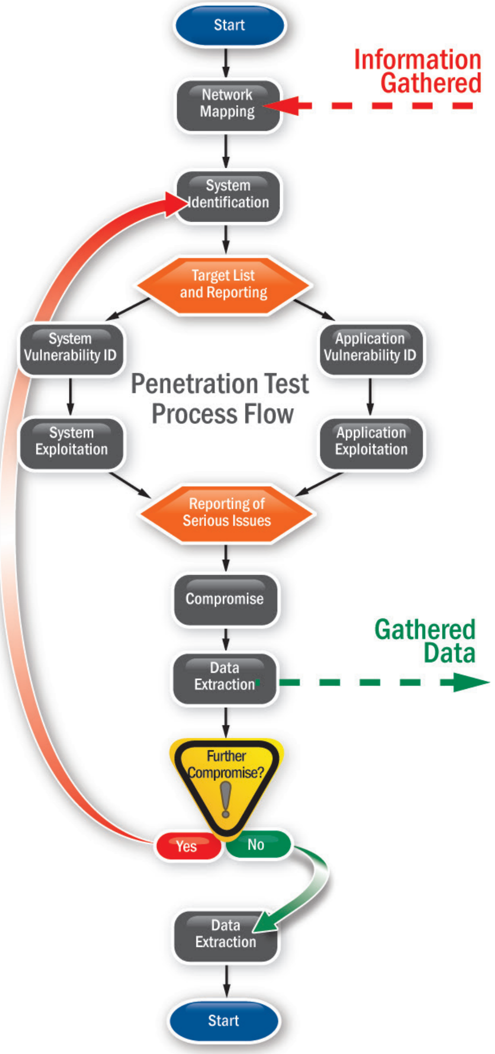
System Compromise—As our experts compromise your environment, they keep you informed so that you can make informed decisions about whether a particular system should undergo additional tests.

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.

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 & 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



E Com Security®
Solutions

MIDDLE EAST ASIA AUSTRALIA EUROPE UNITED STATES OF AMERICA

E Com Security Solutions is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today’s challenging data security and compliance environment, we provide a unique approach with comprehensive solutions that include its customer portal and other proprietary security solutions. We had helped organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers — manage compliance and secure their network infrastructures, data communications and critical information assets. For more information: **https://www.ecomsecurity.org**