



Penetration Testing

Is Your Perimeter Secure?

Conducting a penetration test is a beneficial first step in discovering the vulnerabilities that may be lurking in your network. Most organizations believe their perimeters are secure, but many do not have the tools or the appropriate skill-set to verify this belief. A perimeter penetration test is a necessary activity to verify that your organization is in fact protecting itself from Internet-based threats. Additionally, many organizations are mandated by federal and trade standards, such as PCI, to perform perimeter penetration tests annually. Furthermore, a perimeter penetration test requires a large amount of knowledge in the areas of software vulnerabilities and network assessment tools. There are also two main methodologies in performing penetration tests. Determining which one is best suited for your organization is a necessary first step.

Black Box or White Box Testing

With black box testing Tevora consultants assume the role of would-be-hackers, with the team possessing minimal prior knowledge of your organization's network or the systems to be tested. In full disclosure testing, or what is more commonly known as white box testing, the Tevora team is given complete information about your target systems, up to and including:

- The types of network devices and their configuration
- The operating systems deployed on servers and workstations as well as their patch level
- The database and Web platforms deployed throughout the network
- Firewall models, along with configurations and detailed diagrams of network connectivity

Black box and white box testing are the opposite ends of the penetration testing spectrum and a third option, partial disclosure is also available.

Tevora's Penetration Testing Services

Comprehensive and all-inclusive, a Tevora penetration test includes:

- Public information collection
- Active host identification
- Network services vulnerability assessment
- Web application vulnerability assessment
- Network services penetration test
- Web application penetration test

Why Tevora?

Tevora consultants will take the time necessary to scrutinize your infrastructure for any weakness or sliver of information that could be used by an attacker to disrupt the confidentiality, availability, or integrity of your organizations network. Our skilled senior consultants have a vast array of knowledge of both zero-day and legacy vulnerabilities and hold industry leading certifications including CISSP, CEH and PCI QSA. We utilize a compilation of commercial, open source and proprietary tools in our testing to ensure you are provided a complete assessment.

Our methodology is risk based and completely frictionless to your organization. We incorporate multiple industry standards into our assessment methodology including NIST 800, ISO 27002 and OSSTMM. The final report includes both details about the activities performed as well as remediation recommendations designed to reduce your organizations risk with regard to identified issues.

Please contact us for more information:
e: info@tevora.com
t: (888) 4-TEVORA