Overview

Symantec Application Penetration Tests evaluate the security of an organization’s applications against security best-practice criteria. By simulating real-world, application-level attacks, the tests provide insight into the ability of an organization’s application to resist attacks from unauthorized users and to help prevent misuse by valid users.

Symantec has proven methodologies to provide a wide range of application penetration tests to address specific business needs including, but not limited to; testing an organization’s existing Web-based applications, testing application security before the release of new software or a major software upgrade, and testing the security of third-party commercial applications. As part of the testing, Symantec application security consultants gather and review available information about the customer’s software design, the interaction of the application’s components, and security architecture. These tests can be used to validate the effective implementation of role-based access controls; confirm that external users, such as partners and affiliations, are secure; help satisfy the requirements of an organization’s formal operational risk management program; and allow organizations to demonstrate due diligence through independent validation.

Testing can be performed onsite, or remotely via the Internet depending on the desired approach. Consultants assess a variety of attack vectors including data validation, session management, access controls, use of cryptography, and use of third-party components, among others.

After identifying and testing existing security controls, Symantec security consultants deliver a written report that provides prioritized remediation guidance for application security vulnerabilities that they have identified and validated. This report serves as a roadmap to prioritize application security issues that require immediate and longer-term strategic attention. In-depth knowledge transfer assists customers in understanding their application security strengths and weaknesses and best practices for their remediation.

Key Features

• Simulate real-world attacks to identify vulnerabilities and threats to applications and products

• Deliver an action plan including prioritized recommendations for mitigating risks to applications

• Provide best practices for relevant security architecture components

• Identify specific areas of security strengths and weaknesses in an application’s security architecture

• Inform organizations of where in the application to focus security efforts and development resources to avoid attacks on, or failures within, an application

• Provide in-depth knowledge transfer illustrating specific vulnerabilities identified and best practices for remediation
Key Benefits

• Reduce patching efforts by identifying vulnerabilities in applications and products prior to deployment

• Reduce the security risks associated with applications and help demonstrate due diligence

• Incorporated within a suite of services that provide organizations with a programmatic approach to significantly improve their ability to design, develop, test, and maintain the security of applications

Types of Penetration Tests

Symantec offers various types of Application Penetration Tests, based on customers’ business needs. These include:

• Web Application Penetration Test – Evaluates an organization’s application built with Web-based technologies, including frameworks such as J2EE or .Net (for example, assessing the organization’s eStore through its Web site or its internal human resources systems).

• Commercial Product Test – Tests the security of a product – including an embedded application or appliance – that the organization plans to sell in the marketplace. The test can be conducted in either an informed (“white box”) or blind (“black box”) scenario. In an informed test, the customer provides Symantec with access to developers, product documentation, and other resources as necessary, which facilitates greater depth of analysis. Examples of commercial products tested by Symantec include: mobile phones, wireless handheld devices, networking and security devices, printers, cable boxes, voting applications, mainframe operating systems, wireless cards, online gaming systems, cryptographic accelerators, databases, application servers, and business intelligence and reporting applications.

• Client/Server Application Penetration Test – Provides an internal test of a client/server application that resides on the organization’s network or is shared between the organization and one or more business partners.

• Third-Party Product Test – Tests the security of off-the-shelf products – including an embedded application or appliance – that organizations have purchased or are considering purchasing for use in their environment.
More information

Visit our Web site
http://ses.symantec.com/secureapps

To speak with a Symantec Security Consulting Services specialist in the US
Call toll-free 800 745 6054

To speak with a Symantec Security Consulting Services specialist outside the US
Symantec has operations in 40 countries. For specific country offices and contact numbers, visit our Web site.

About Symantec
Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec’s Norton brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
www.symantec.com