PROFESSIONAL SERVICES

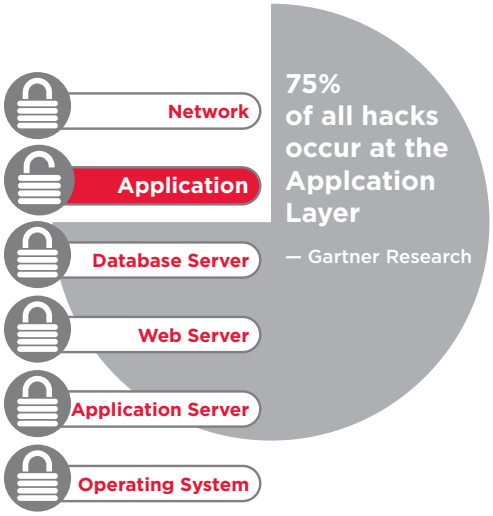
Web Application Vulnerability & Penetration Testing

The Challenge

Now more than ever, Web applications are a critical part of business. Employees, customers and partners prefer to do business online, and expect to be able to access a variety of information and transactions through Web sites and Web services. As a result, Web applications hold a treasure trove of data behind their front ends: credit card numbers, medical records, confidential company financial results, and this list goes on.

Attackers are well-aware of the valuable information accessible through Web applications, and their attempts to get at it are often unwittingly assisted by several important factors. Conscientious organizations carefully product their perimeters with intrusion detection systems and firewalls, but these firewalls must keep ports 80 and 443 (SSL) open to conduct online business. These ports represent open doors to attackers, who have figured out thousands of ways to penetrate Web applications.

Further complicating the security picture, Web applications are often written in high-pressure environments on tight schedules by developers with little or no security training. Once development is complete, the applications are put through QA testing that typically focuses on performance and functionality, rather than security. As a result, an application that emerges from QA with flying colors can still be riddled with exploitable flaws. It's no surprise, then, that Gartner reported that 75% of hacks happen at the application layer.



It is imperative that companies identify and address vulnerabilities in their Web applications. Companies that fail to protect themselves against the threat of web application exploits risk non-compliance with regulations including Sarbanes-Oxley, PCI, HIPAA and others, the loss of confidential data, business interruption, and — perhaps most significantly — damage to their reputation.

Savvis Application Security experts can help companies secure their Web applications

Solution Highlights

- Industry-leading vulnerability scanning tools, updated daily
- Remote scan requires no changes to target web environment
- Reporting includes vulnerability type, severity level, technical explanation, remediation instructions
- Trend analysis to track progress
- Legal and regulatory compliance-focused scans with reports tailored to the language & categorization of each law or regulation
- In-depth penetration testing to verify sever findings by skilled and creative Savvis application security experts

with best-of-breed Web application vulnerability scanning tools, and with their detailed knowledge of the hidden flaws that can cripple the security of a Web application or set of Web services.

Web Application Vulnerability Scan

Savvis Professional Services uses the industry leading Web application vulnerability scanning tool to analyze customer Web sites and Web services. The latest known vulnerabilities and hacker techniques are downloaded on a daily basis, assuring Savvis customers that the checks being performed are as up to date as possible. In addition, the scan requires no changes to the target Web environment as Savvis can run its vulnerability scans remotely with no need to install any server-side software. The scanning software looks for the following vulnerabilities, and much more:

- Parameter Injection
- SQL Injection
- Cross-Site Scripting
- Directory Traversal
- Parameter Overflow
- Buffer Overflow
- Parameter Addition
- Path Manipulation
- Character Encoding
- Site Search
- SSL Strength
- Sensitive Developer Comments
- WebServer/Web Package Identification
- Permissions Assessment
- Brute Force Authentication attacks

Once the vulnerability scan is completed, Savvis delivers an executive summary report to management and a detailed report to the development and quality assurance teams. Both reports list the vulnerabilities found along with the severity levels of each vulnerability.

The detailed report includes an in-depth technical explanation of each vulnerability as well as instructions for remediation. Upon a customer's completion of future versions of their Web application, Savvis can conduct subsequent vulnerability scans and generate trend analysis reports that allow the customer to compare tests and track progress.

Savvis can also conduct vulnerability scans that focus on legal and regulatory compliance for Web applications and Web services. In these types of scans, Savvis runs automated security checks required by specific laws and regulations and produces reports tailored to each law and regulation's language and categorization.

The scanning tool keeps up to date with changing regulations through daily checks for updates to compliance policies and reports.

Web Application Penetration Test

A Web Application Penetration Test builds upon a Web Application Vulnerability Scan.

Savvis security experts manually verify the more severe findings of the scan, devise and launch their own manual attacks against the Web application, and produce real world attack results. Penetration testing not only verifies the existence and exploitability of potential vulnerabilities, but also reveals other vulnerabilities that can only be found by the manual intervention of creative, highly-skilled application security experts.

Savvis Compliance Scans

Address the following legal and regulatory initiatives:

- 21CFR11
- Basel II
- California Online Privacy Protection Act
- California SB1386
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- Children's Online Privacy Protection Act (COPPA)
- EU Directive on Data Protection (Directive 1995/46/EC)
- EU Directive on Privacy and Electronic Communications (Directive 2002/58/EC)
- Director of Central Intelligence Directive 6/3 (DCID)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability & Accountability ACT (HIPAA)
- ISO 17799
- Japan Personal Information Protection Act (JPIPA)
- NIST 800-53
- North America Electric Reliability Council (NERC)
- OWASP Top 10
- Payment Card Industry (PCI) Data Security Standard
- Safe Harbor
- Sarbanes-Oxley Act
- UK Data Protection Act

The real world results are also much more compelling than conceptual descriptions. Nothing grabs attention more quickly than a list of customer data extracted through an application vulnerability, or a demonstrated ability to alter any system user's password.

Methodology

There are four key phases to the Web Application Penetration Test:

- Assessment
- Application Vulnerability Scan
- Manual Penetration Test
- Reporting

Assessment

The Savvis team will work in conjunction with your organization to develop a strategy to optimize the effectiveness of the Penetration Test, based on the size and complexity of the different parts of your application and the desired focus of the engagement (e.g., compliance). The team uses the resulting review plan to maximize the relevance of the review results to your organization.

Application Vulnerability Scan

The Savvis team will use the industry leading Web application vulnerability scanning tool to analyze the Web applications and Web services identified by the customer for review.

Manual Penetration Test

In this stage, the Savvis team manually verifies that the more severe vulnerabilities identified by the automated scanner do in fact exist and are exploitable. The team will also use its expertise to devise and manually attack the Web application. For both the manual verification and the newly devised attacks, the Savvis team will attempt to access actual data and functionality to fully demonstrate the significance of each vulnerability.

Reporting

Following the completion of a Web Application Penetration Test, Savvis will deliver an Executive Summary report of the team's findings to management, and a detailed report to the development and quality assurance teams. The results are scored "from the top down" to ensure the most serious security issues are found early on and addressed. Savvis will also meet with the customer's technical team to discuss the results of the review and potential solutions.

Let Savvis Meet the Challenge

Savvis Professional Services provides expert Application Security solutions, delivered by experienced specialists. We pride ourselves in providing a structured approach to strategies, providing consistent methodology and a complete understanding of business requirements.

Savvis has spent many years building our credentials, and today we can offer comprehensive experience in identifying threats, risks and vulnerabilities, and building the counter-measure solutions that companies demand.

Our experts have been at the forefront of designing, securing and supporting risk mitigation for some of the most complex networks in the world, including many Fortune 1000 companies and the United States government. Our team of experts is comprised of senior professionals who have honed their skills through corporate leadership, consulting, investigative branches of the government, law enforcement, and research & development.
Many of Savvis' personnel hold advanced technical degrees, as well as a wide array of industry-recognized certifications including CISSP, CISA, and numerous SANS/GIAC certifications.

Savvis also operates one of ten United States Government NVLAP-accredited, CCEVS-approved, Common Criteria Test Laboratories known as the Common Criteria Testing Lab (CCTL). We have experience in evaluating an array of products from devices, appliances, and general-purpose products, to distributed applications. Our lab is located in a Savvis Internet Data Center with world-class features including secured biometric access on a 24/7 basis, video camera surveillance, raised floors, HVAC temperature control, advanced smoke detection, and advanced fire suppression systems.

Related Services

Application Security solutions from Savvis can be combined with Savvis' security, networking, facilities, server, storage and content distribution service offerings, to provide an IT infrastructure that contributes to a reliable and secure business environment.

Get Ahead

Today, companies face a multitude of tough IT challenges, as well as the need to make information readily accessible to a broad array of public and private users and groups. To meet the challenge, you need a trusted partner with deep IT experience, and Savvis can provide the solutions and expertise you need to fulfill your mission to keep critical information safe and available.

Let Savvis meet the challenge by leveraging our team of highly skilled professionals who have been in the forefront of designing and protecting some of the most complex IT infrastructures in the world.

About Savvis

Savvis, Inc. (NASDAQ:SVVS) is an outsourcing provider of managed computing and network infrastructure for IT applications. By outsourcing to Savvis, enterprises can focus on their core business while Savvis ensures the quality of their IT infrastructure. Leading IT organizations around the world have selected Savvis to help them improve their service levels, reduce capital expense and deal with the rising costs of bandwidth, energy, real estate, staff and expertise. As a pioneer in utility computing, Savvis understands and harnesses the latest advances in technology like virtualization, cloud computing and support process automation.

For more information about Savvis, visit www.savvis.net or call 1.800.SAVVIS.1 (1.800.728.8471).

EMEA
Savvis UK Limited
Tel +44 (0)118 322 6000

ASIA PACIFIC
Savvis Singapore
Company Pte Ltd
Tel +65 6768 8000

JAPAN
Savvis Communications K.K.
Tel +81.3.5214.0151

© 2008 Savvis, Inc. All rights reserved. Savvis® is the registered trademark of Savvis Communications Corporation.
All other trademarks and service marks are the property of their respective owners.