APPLICATION SECURITY, INC.

Vulnerability Assessment: The Right Tools to Protect Your Critical Data

White Paper

By Joshua Shaul, Systems Engineering

APPLICATION SECURITY, INC.
www.appsecinc.com
Tel: 1-866-9APPSEC
E-mail: info@appsecinc.com

INTRODUCTION

Over the last several years, Vulnerability Assessment (VA) has become one of the hottest fields within the computer security market. VA tools are designed to detect and report on security holes within various software applications, allowing organizations to take corrective actions before a devastating attack occurs. Due to the reduction in "time to exploit" once a new vulnerability reaches the public domain, and the regulatory pressures imposed on businesses within a variety of verticals, the need for reliable vulnerability assessment has never been greater. Unfortunately, the environment in which software applications are developed today is largely driven by schedule and features, rather then stability or security. This situation has led to corporate networking being ripe with vulnerabilities there for the picking, and the software vendors are doing very little to remedy the situation. Risks to corporate applications are further exacerbated by overburdened and understaffed IT departments.

Successful and well publicized cyber-attacks have now become commonplace; often hitting the affected businesses hard with fines, mandatory external audits, and customers taking their business to someplace where they hope their personal data will be better protected. Securing your assets with a layered approach to security is the only way to win in a world where hackers are everywhere, and software vendors take no liability for the damages that poorly developed products cause.

We've all heard about the need for a Firewall to block access to the network, an IDS or IPS to detect and stop external attacks, and a VPN to protect sensitive communications. These are essential tools in protecting your data, but they fall far short of a complete solution, as external hackers can still access the network through legitimate applications, and insiders continue to operate unfettered. How secure is your money in a bank with no Vault? Vulnerability Assessment inside the perimeter is the next step in proactively protecting your data, but it is a complex marketplace, and there is no single magic bullet or VA tool out there with the breadth to cover your entire network and all the applications within.

VULNERABILITY ASSESSMENT LANDSCAPE

There are two broad categories of vulnerability assessment software, Host-based, and Network-based. Host-based VA tools focus on analyzing issues specific to a single host machine. Typically, these tools load agent software onto the target system that tracks activities and configurations changes, and reports back to a centralized console. Network-based VA tools run on centralized scanner machines, often operate anonymously (requiring no logins), and can scan a range of hosts for vulnerabilities. The remainder of this paper focuses on Network-based VA tools.

NETWORK-BASED OS/NOS VULNERABILITY SCANNING

There are many commercial vulnerability scanning solutions available on the market today. Most of these tools are geared towards scanning Operating Systems and Networking Operating Systems (running on networking appliances) for known vulnerabilities. Some of these tools have included some application specific scanning engines, allowing them to find scan for issues in many networked applications. Running this type of tool is extremely important for any organization. We all run computers, and those computers all run operating systems, and every OS has vulnerabilities that are discovered from time to time. Keeping up to date with patches and maintaining proper operating system configurations is a critical step in preventing attacks both from hackers and insiders.

There are many vendors that provide excellent tools for OS/NOS VA. eEye's Retina, ISS's Internet Scanner, Harris's STAT Scanner, Qualys' QualysGuard, and Symantec's NetRecon are all examples of OS/NOS-centric scanners. Several of these tools have taken the next step to perform simple scans on common applications. Email servers, HTTP servers, FTP servers, DNS servers, and others are good examples of the ubiquitous applications that these VA tools can scan for vulnerabilities. Companies really need to scan these applications to be sure that security holes have been patched.

What these tools leave behind are the large, complex applications that many organizations use to store and manage their most sensitive data. At the heart of almost all of these data storage and processing applications is a relational database (RDB). These databases are critical for business operations. They contain sensitive data about customers, employees, finances, future plans, intellectual property, and lots of other important stuff. The wealth and depth of data managed by the RDB is precisely what makes it such an attractive target for hackers to go after. The RDB management systems, usually from Microsoft, Oracle, IBM, or Sybase are large and extremely complex applications that have been prone to security problems. At the same time, database security is often overlooked. Many organizations fall into the trap of believing that since they have great perimeter security, and they run an OS/NOS VA tool, that the databases are covered. Unfortunately, this is not the case.

NETWORK-BASED DATABASE VULNERABILITY SCANNING

The only way for a business to protect its most critical data from both outside hackers, and unscrupulous insiders is to ensure that the database is properly configured, patched, and locked down. Many organizations have implemented a manual process of reviewing database security, but this method is slow, difficult, and often inaccurate and ineffective. A database assessment on two separate databases either by the same person or by two different assessors can produce varied results. This inconsistency calls into question the reliability of manual assessments, and makes it difficult at best to verify if a database has been hardened according to corporate standard. A much better approach is to run a specialized VA tool for databases, one with the specific low-level knowledge of every commonly used database server. Similar to a OS/NOS VA scanner, a database VA scanner will find security holes and configuration problems in the database, and then present the user with a report detailing the issues found and recommended fixes. It has become critical for organizations to add database-specific VA to their existing security infrastructure.

Several of the OS/NOS scanners mentioned earlier have begun to address databases in their scanning products. However, because of the complexity of database applications, and the near flood of vulnerabilities that are regularly discovered, these tools fall far short of offering any meaningful protection for the database. For example, while an OS/NOS scanner may have a dozen checks for one or two types of databases, a database scanner will have literally thousands of checks for several database platforms.

APPDETECTIVE: AWARD WINNING VULNERABILITY ASSESSMENT FOR DATABASES

AppDetective from Application Security is an award winning product designed specifically for scanning databases. AppDetective was designed by leading experts in the field of database security, with the intention of building the most thorough, accurate, and easy to use DB security tool on the market. All commonly used database servers are supported, with a depth of analysis unparalleled in any other DB scanning solution. Supported databases include Oracle, Microsoft SQL Server and MSDE, Sybase, IBM DB2, MySQL, and Lotus Notes/Domino.

AppDetective is able to intelligently inventory all of these applications on the network, often uncovering databases that were previously unknown or unaccounted for. Having an accurate inventory of databases on the network is a critical aspect of vulnerability management, as it is impossible to manage risk on an unknown application. If the Slammer worm taught us anything, it was that unknown databases can be found and exploited with devastating results.

With a complete list of applications, organizations can begin to assess the security posture of their databases by running non-intrusive penetration tests to determine what kind of damage can be done by a hacker without a legitimate database login. These tests often discover serious holes, such as blank, default, or easily guessed passwords or vulnerability to a buffer overflow that would allow an attacker to easily steal accounts or even take complete control of the system.

Next, AppDetective digs in deeper by performing a complete security audit on the databases. This involves logging into the application and thoroughly analyzing the patch level, configuration settings, and password strengths. The security audit allows an organization to determine their susceptibility to internal attack and misuse, the most important but most overlooked area in the data security world. This depth of analysis can only be provided by a specialized database scanner.

AppDetective also includes an intuitive reporting engine, allowing users to easily create attractive reports on the vast amount of data that the tool collects during its scans. A large number of report templates are built into the tool, along with many choices of output format, from Crystal Reports, to HTML, to raw text or XML, allowing AppDetective to stand-alone or easily integrate into an existing reporting infrastructure. Actionable reports allow for easy communication of the database assessment across the organization, and can also be used to demonstrate due diligence efforts to external auditors.

APPDETECTIVE: BEYOND VULNERABILITY ASSESSMENT

Identifying missing patches, weak passwords, and insecure configuration settings is the main purpose for using AppDetective, however there is much more that the tool can do for an organization then simply find vulnerabilities. AppDetective can be configured to perform configuration policy compliance scans, automatically determining if applications are configured properly, and calling out exactly which settings violate the policy. Configuration policies will vary from group to group; AppDetective has the flexibility to support any configuration desired.

AppDetective also offers assistance in correcting the issues that it finds. With a click of the 'Fix it' button, AppDetective will automatically generate remediation scripts for any problems that can be fixed through a configuration change. These scripts can be automatically run against the database, or can be output for review and manual application. This allows organizations to not only easily detect problem areas, but to immediately correct those problems without requiring any expertise in the art of database administration.

Recently added to the AppDetective product, Application Security's AppIntegrity tool offers organizations an intuitive GUI for performing baselining on a database. This allows an organization to baseline a known good configuration, then easily detect and roll back any changes made to the configuration tools. By integrating this feature into AppDetective, Application Security offers our customers broad security related functionality in a single, affordable package.

DEFENSE IN DEPTH: AN INTEGRATED APPROACH TO DATA SECURITY

When implementing a security strategy it is critical to select the proper mix of tools, technologies and usage policy in order to protect valuable assets. Network perimeter security tools such as Firewalls and Intrusion Detection / Prevention Systems form the first line of defense for your data. Next, focus on hardening operating systems and business critical applications by running Vulnerability Assessment tools and following up, or apply the configuration to a similar database. In the past, this type of functionality was only available in stand-alone on the results. A layered approach is required here, with a mix of OS/NOS scanners and Database scanners to fully uncover all security holes and configuration problems. In addition to scanning for vulnerabilities, organizations should effectively monitor user activity, scan for attacks in real-time, and potentially protect critical data at rest through encryption.

Adhering to the layered defense model, Application Security's suite of tools effectively mitigate threats by applying sensible protections where they are most critically needed, at the heart of an organizations data storage systems – the relational database. By incorporating proper database and web application security techniques and tools with effective perimeter defenses, organizations can be assured that private information will remain private, allowing for unhindered growth and profitability.

COMPLETE DATABASE PROTECTION FROM APPLICATION SECURITY, INC.

Application Security has engineered a suite of software tools that offer an effective layered protection mechanism for web applications and databases. When deployed properly, these tools will discover applications and databases, determine if they are vulnerable to either external or internal attack, monitor them for an attack and for misuse, and finally protect the confidentiality of the most critical data at rest with strong encryption.

AppDetective

AppDetective and AppDetective for Web Applications perform discovery scanning, penetration testing, and security auditing on any web application, nearly every modern RDBMS, and for several middleware products including Lotus Domino, BEA Weblogics, and IBM Websphere. Updated monthly, AppDetective is aware of all known vulnerabilities in these systems with specific checks built-in to address each. This allows organizations to quickly ascertain the reliability of their critical systems, then initiate remediation, following the steps recommended by AppDetective.

AppDetective for Web Applications

When working with web applications, AppDetective performs a web crawl and a penetration test. When issues are found, built-in utilities can be used to 'debug' the application code to eliminate the vulnerability. This allows organizations to implement security during application development instead of trying to bolt it on afterwards. This saves tremendous amounts of time, as no complete systems need to be sent back to engineering for redesign when glaring security holes are found during final production testing. AppDetective can also be used by Quality Assurance teams to prove that applications do not have potentially damaging or embarrassing weaknesses before they are released to market.

AppRadar

AppRadar represents a revolutionary step forward in database security tools. Combining real-time intrusion detection and auditing, AppRadar ensures that nothing happens within the database without a DBA or Security Officer knowing about it. The latest in an award winning suite of tools from Application Security, AppRadar was built by experienced security professionals, with the most intimate knowledge of detecting and exploiting database vulnerabilities. Centrally managed from the AppSecInc Console, AppRadar can simultaneously protect an unlimited number of MS SQL and Oracle databases.

DbEncrypt

For those systems that contain the most critical or highly regulated data, steps need to be taken to protect data while it is at rest, stored within the database. Application Security's award winning DbEncrypt product is designed to protect data at rest utilizing strong encryption built upon a robust key management mechanism. Simply encrypting data within a database is not sufficient, user access must be carefully managed, and encryption keys need to be very well protected, as a failure in either category could lead to catastrophic loss of data. DbEncrypt handles these issues properly and transparently, allowing existing applications to continue to work unmodified, handling all user access and encryption/decryption operations silently in the background. DbEncrypt should be the last layer of defense, providing the assurance that even if all other security systems fail, stolen data will provide the thief with nothing more then undecipherable gibberish.

AppSecInc Console

The AppSecInc Console is a web-based centralized management system for the AppDetective and AppRadar products. The console enforces role-based separation of duties through a built-in access control mechanism that designates three distinct privilege levels: administrator, user, and viewer. This mechanism allows enterprises to assign separate security and database administrators, while allowing for a convenient management portal for viewing generated reports. With the AppSecInc Console, security administration can be done remotely with confidence. All Console communications are protected with SSL,

allowing administrators to access the tool from anywhere with an internet connection, ensuring that security issues can always be detected and addressed.

ABOUT APPLICATION SECURITY, INC.

AppSecInc is the leading provider of database security solutions for the enterprise. AppSecInc products proactively secure enterprise applications at more than 200 organizations around the world by discovering, assessing, and protecting the database against rapidly changing security threats. By securing data at its source, we enable organizations to more confidently extend their business with customers, partners and suppliers. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business. Please contact us at 1-866-927-7732 to learn more, or visit us on the web at www.appsecinc.com.