EyeD
infocomm & security solutions

Vulnerability and Penetrating testing

White Paper

Toa Payoh
Singapore

enquiries@eyed.com.sg
www.eyed.com.sg

Table of Contents

Executive Summary

This paper describes how enterprises can more effectively assess and manage network vulnerabilities and reduce costs related to meeting regulatory requirements. Provides a broad view of the vulnerability, ranging from industry-wide data down to a focused look at different technologies, including Web, mobile etc. The goal of this report is to provide the kind of actionable security that intelligence organizations need to understand the vulnerability as well as best deploy their resources to minimize security risk.

Highlights

A new approach is emerging for detecting and managing vulnerabilities in complex networks. The security provided by annual or quarterly manual vulnerability assessments can now be substantially improved. At the same time vulnerability assessment and management overhead can be reduced and better risk management and vulnerability control can be accomplished.

Vulnerability trends

Understanding technical security risk begins with knowing how and where vulnerabilities occur within an organization. Vulnerabilities can impact every level of enterprise infrastructure from hardware, to network, to software (both old and new). These vulnerabilities are the gateway that malicious actors use to circumvent security protections and steal or alter data, deny access, and compromise critical business processes.

Integration Reduces Risk

While finding vulnerabilities helps organizations understand their exposure, they must also have the ability to quickly mitigate found vulnerabilities to greatly reduce the risk of application exploits. The longer an application remains vulnerable, the more likely it is to be compromised.

EFFECTIVELY MANAGING VULNERABILITIES WITH PENETRATION TESTING

These recent trends in cybercrime make it more critical than ever that organizations acquire a true assessment of their security vulnerabilities so they can identify and address those vulnerabilities associated with their most valuable information assets. Your organization's true vulnerability to threats can be determined only by answering the following questions in regards to each of your identified vulnerabilities:

□ is the vulnerability real, or is it a false positive?

□ Can the vulnerability be exploited?

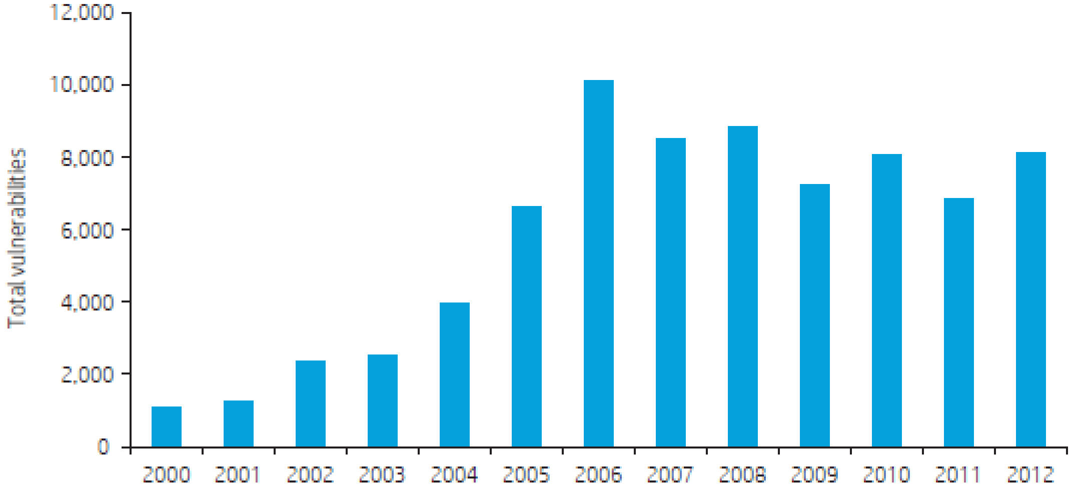
□ Are there any sensitive systems or data exposed by the vulnerability?

Clearly, the answers to these questions will allow you to prioritize your vulnerabilities and structure your security strategy as effectively and efficiently as possible, instead of simply identifying your vulnerabilities and then attempting to address them based only on assumptions about risk. One of the easiest and fastest ways to obtain these answers, both initially, and on an ongoing basis, is to perform a penetration test on your network. A penetration test is an authorized, local attempt to "hack" into a system, to identify exploitable weaknesses, and to reveal what systems and data are at risk. The tester may use several methods to gain entry to the target network, often initially breaking into one relatively low priority section and then leveraging it to attack more sensitive areas. Your organization is probably already running (or considering running) vulnerability scans on your network and/or web applications, and you may wonder what penetration testing offers you that vulnerability scanning does not. It's simple: A vulnerability assessment tells you only what an attacker can potentially do to your environment. A penetration test tells you what an attacker can definitely do to your environment. That's because penetration tests exploit identified vulnerabilities, just as an attacker would. Unlike vulnerability scans, penetration tests leave little doubt as to what an attacker can or cannot do. Penetration tests eliminate the guesswork involved in protecting your network by providing you with the information you need to effectively prioritize your vulnerabilities.

The vulnerability arms race—total disclosures in 2012 increased 19 percent from 2011

The total number of new vulnerabilities reported during 2012 (8,137) increased by roughly 19 percent from the number of vulnerabilities disclosed in 2011 (6,844), but remained 19 percent lower than the number reported at the peak in 2006. This continued oscillation in the number of reported vulnerabilities demonstrates that the struggle between organizations and the attackers bent on compromising them rages on with no clear victor (see Figure 1)

Figure 1. Disclosed vulnerabilities measured by OSVDB, 2000–2012



ERP Penetration Testing approach

As it has been said before, there are many problems existing in different areas of ERP systems. Security problems exist in Implementation and Development processes, but the main difference is in the approach to how you conduct the security assessment of those applications.

Approach Differences

This section discusses penetration testing and security assessment of business applications. There are some major differences in testing business applications versus testing typical corporate environments. Here are the main differences:

- ✓ *A deep knowledge of a system assessed is required to even begin*

It is extremely difficult to understand all the features and business processes of every ERP system because it is changed from company to company. It can be much harder than typical penetration tests due to the huge amount of overall technical information and very little security-related information the tester needs to have mastery of. The tester needs to understand business system processes and look at every vulnerability risk while taking into consideration real business risks.

- ✓ *ERP systems are critical and great care must be taken not to cause outages to avoid the high costs of downtime*

Proof of Concept exploits are too dangerous to use, for example. Memory vulnerabilities need a lot of testing and are risky, too. Brute forcing a password for the system with account lockouts after a certain number of unsuccessful logon attempts can have serious impacts such as: locking out individuals engaged in closing a monthly financial period; causing the company to undergo significant monetary losses; and damaging the relationship between the client and the tester.

- ✓ *Gaining OS level shell access is not the goal of ERP penetration testing*

The goal is to access critical DATA and to identify the impact on business process. ERP penetration testing customers expect to see business risks explained in reporting rather than OS level vulnerabilities. Gaining access to CFO's ERP account and showing how to create unauthorized money transfers demonstrates more risk.

ISS X-Force™ Penetration Testing Service

Internet Security Systems introduced the ***Internet Scanner™*** application, the industry's first penetration testing solution, in 1994. Today, ISS' ***X-Force™ Penetration Testing Service*** provides the premier attack simulation and analysis service available. This powerful combination of ISS' X-Force security intelligence, research and development and ISS' highly experienced, business-driven consultants provides customers with the timely, accurate testing and reporting they need to make knowledgeable information protection decisions.

IBM Security AppScan Scanner

IBM Security AppScan delivers security capabilities that allow enterprises to not only identify vulnerabilities, but to reduce overall application risk. The IBM Security AppScan portfolio includes white box (advanced static) and black box (dynamic) analysis—as well as run-time analysis that keeps current with the latest threats and produces precise, actionable results. IBM Security AppScan helps organizations manage risk throughout the application lifecycle and enables them to drive application security within EyeD Solution. Security AppScan service integration tests web application vulnerabilities and the latest Web 2.0 technologies, including AJAX based applications. Administrators can manage reporting and policy creation and enforcement through the EyeD Solution.

Cenzic Hailstorm Scanner

Cenzic's scanning solution can scan websites and web applications in the enterprise to see how vulnerable they are to possible attack. Hailstorm scans against several default policy templates, and the results make it easy to see the overall status of the application, the number of URLs discovered, the forms discovered, and an overall site map. Hailstorm can also detect a link to an outside site, which other utilities can overlook. It can run different types of reports, for instance, a technician report or an executive report. Similar to the IBM Security AppScan, administrators can manage reporting and policy creation and enforcement through the Eyed Solution.

QualysGuard WAS

One of the challenges of dynamic application security testing (DAST) is successfully authenticating the application during a scan. Built on Qualys's powerful SaaS platform, QualysGuard Web Application Scanning (WAS) 2.1 can perform authenticated web application scans and even complex authentication with multi-step login processes like client certificates to identify vulnerabilities. QualysGuard uses the power and scalability of the cloud to accurately discover, catalog, and scan large numbers of web apps to provide a high level of protection. QualysGuard WAS 2.1 identifies OWASP Top Ten web application vulnerabilities as well as emerging threats such as Slowloris. This automated solution reduces the complexity and cost of web application scanning.

WhiteHat Sentinel

In addition to the vulnerability scanner integration, EyeD (version 11.1 and later) provides context that helps administrators understand attack methods, which better enables them to defend against attacks. And session-based enforcement and reporting gives security analysts an in-depth understanding of attack execution by user. For example, Eyed will not only report that a SQL injection attack occurred on the website and the user name that executed it, but it will also associate the application user name with the session and specific violations.

With Violation Correlation, EyeD administrators can make multiple violations appear as a single group according to a common rule or criteria. For example, multiple attacks that are coming from the same source IP address can be correlated into a single incident. Administrators can also define a blacklist or whitelist based on IP address geo-location information.

The EyeD Solution includes a deployment wizard to secure virtual servers and dynamic reports that offers endless reporting scenarios. For instance, an administrator can receive a report of the top attacked URL of an enterprise's websites. And when there are application issues and web pages are rendering slowly, virtual server CPU statistics show the CPU utilization per virtual server so operators can troubleshoot performance and capacity issues.

IBM iSeries (formerly AS/400)

IBM introduced the AS/400 in 1988 as its computing system for small- and medium-sized companies. Today, the Power Systems product line ranges from small servers with a single processor to the high-end mainframe-class POWER7 Model 795, which can have up to 256 processors. The iSeries Access for Windows, previously called "Client Access Express for Windows" in V5R1 and earlier OS/400 releases, offers an all-inclusive client solution for accessing and using resources from your Windows desktop over a TCP/IP connection. It includes 5250 emulation, access to DB2 Universal Database™ (UDB) for iSeries through its Data Transfer function, and utilizes iSeries NetServer for working with the OS/400 integrated file system (IFS) and printers. It also includes iSeries Navigator, the OS/400 GUI, for administering iSeries and AS/400 servers.

Additionally, SessionWall-3 is particularly useful if you want to gain access to a mainframe or AS400 computer system. The telnet session with a mainframe often looks like binary traffic. SessionWall-3 can do on-the-fly translation from EBCDIC to ASCII. This makes AS400 and mainframe systems that use telnet vulnerable in a shared media environment. Without this translation capability, you would have to perform an extra step to read the EBCDIC traffic on the file on a UNIX system.

We suggest creating a list of roles and the AS/400 access required for each role. Create a group profile for each role with the appropriate access, then assign the group profile to users when created or when a user's role changes on the team. Team members may temporarily require higher levels of access to accomplish the goals of a specific project, like a Domino server upgrade or to install new software.

JD Edwards Enterprise Security

JD Edwards EnterpriseOne is an integrated application suite of comprehensive enterprise resource planning software that combines business value, standards-based technology, and deep industry experience into a business solution with a low total cost of ownership. A collection of prebuilt Business Intelligence (BI) applications available as modules for JD Edwards EnterpriseOne provide organizations the ability to implement and integrate more quickly, with less risk, and at a fraction of the cost required for building traditional BI solutions. JD Edwards EnterpriseOne provides organizations with the ability to transform information into business actions and enjoy a strategic advantage over less-nimble competitors.

Providing prudent security to utility processes is essential. Oracle Security Technology is unsurpassed in the industry, providing for JDE as follows:

- ✓ Secure meters and data by enhancing AMI security and comprehensive meter data security.

- ✓ The ability to help streamline customer and employee care by implementing user, role and password management as well as enabling next-generation consumer energy portals.
- ✓ An agile architecture for compliance which helps reduce time and cost and aids in rapid adjustment to new regulations and mandates.

This design is also insecure. If an attacker has access to the client workstation they can sniff the transmission of the password from the JDE user during authentication process in MS SQL. In older versions of MSSQL it can be easily done by Cain and Abel. In new versions it can be done by hooking API of JDE frontend during authentication. After acquiring the password the attacker can then directly connect to database with DBA access. This provides full access to all data, bypassing any restrictions. JDE security guides mention that access to the JDE.INI must be secured by file restrictions but it doesn't help from this attacks.

Preventing JDE Access Bypass:

1) The user types in their username (Ex. APPUSER) and password (Ex. APPASSWORD) on the frontend.

2) The frontend application tries to connect to the JD Edwards Database server on the SQL port using username JDE and its password which is read from configuration file JDE.INI (Password reads from "SECURITY", "Password", "JDE") this password is by default – JDE).

3) The frontend application check APPUSER's password in database table F98OWSEC and if it is ok APPUSER authenticates and Frontend draw a GUI by analyzing APPUSERS role in database.

What to Look for in a Penetration Testing Service Provider

Many companies offer penetration testing services, but the best choice is a provider who offers focus on the entire threat spectrum, including highly researched vulnerability and threat intellectual capital and tools. Look for a robust penetration testing methodology, preferably one that provides a multi-layer approach that identifies and leverages small cracks that springboard into identifying major cracks not found by typical security tools. Make sure the final deliverable report provides business value, as security recommendations should be based on the client's business objectives and the appropriateness of security measures per exposure. Lastly, use a provider that has a proven track record of finding known and new threats and whose recommendations provide a holistic approach to security.

A final note: reconsider before using a penetration testing service provider who merely runs a security audit or scanning tool and delivers a report on that one tool's results. While an individual tool provides some value as a standalone assessment device, it can never replace the human mind to creatively apply new methods and techniques to break and bypass standard security systems, much like an intruder would.

Conclusion

A penetration test from a trusted provider offers an excellent means by which an organization can baseline its current security posture, identify threats and weaknesses, and start implementing remediation strategies. By identifying risk exposures and highlighting what resources are needed to correct them, penetration tests provide not only the basis for a security action plan, but also the compelling events, due diligence and partner interface protocols necessary to establish information security as a key corporate initiative.

Security is a never-ending battle. The bad guys advance, organizations counter, bad guys cross over—and so the cat and mouse game continues. The need to properly secure web applications is absolute. Knowing what vulnerabilities exist within an application can help organizations contain possible points of exposure. EyeD offers unprecedented application protection by integrating with many market-leading vulnerability scanners to provide a complete vulnerability scan and remediate solution.