Vulnerability Management is Essential for Effective Security

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

Vulnerability management is the embodiment of continuous process improvement in system security.

In a recent discussion in the Norwich University< http://norwich.edu/ > IS342 (Management of Information Assurance< http://www.mekabay.com/courses/academic/norwich/is342/index.htm >) course in the Bachelor of Science in Computer Security and Information Assurance< http://programs.norwich.edu/business/csia/ >, the class reviewed Rebecca Gurley Bace's< http://www.infidel.net/bios/bacebio.php > chapter 46, "Vulnerability Assessment" from the *Computer Security Handbook*, 5th Edition< http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/ >.

Bace explains that vulnerability management includes several phases:

- Assessing deployed information systems to determine their security status;
- Determining corrective measures
- Managing the appropriate application of the corrections.

The four basic functions of vulnerability management are

- Inventory: identify all systems in the domain of interest, including operating systems, platforms, and topology;
- Focus: determine the data required for assessment and tune vulnerability-assessment tools;
- Assess: run automated and manual tests, evaluate results to judge risk to the systems using security policy and best practices;
- Respond: execute changes as required by assessment and fix specific weaknesses.

Vulnerability assessment (VA) involves gathering sample data, organizing the data, comparing the current status with reference standards, and identifying discrepancies between the current state and recommended standards or goals. An example of a well-known VA tool is the Microsoft Baseline Security Analyzer v2.2 (MBSA< http://www.microsoft.com/download/en/details.aspx?id=7558 >) that "provides a streamlined method to identify missing security updates and common security misconfigurations." The product has been updated over the years to support Windows 7 (32- and 64-bit) and Windows Server 2008 R2 as well as older operating systems back to Windows XP and Windows 2000. It also looks for documented weaknesses in "all versions of… Internet Information Server (IIS) 5.0, 6.0 and 6.1, SQL Server 2000 and 2005, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003 only." Versions of the human interface are available in German, French, and Japanese in addition to English.

For an excellent overview of how a well-design VA tool can support security management, see the extensive set of white papers< http://www.stillsecure.com/library/vam.php > from

StillSecure about their "VAM" product.

VA fits into security management in many ways:

- When systems are first deployed, VA can establish a baseline definition of the security state;
- When security breaches are suspected, VA users can focus on likely attack paths;
- VA may help administrators to see if vulnerabilities have been exploited;
- VA can identify areas where newly reported vulnerabilities should be patched;
- Records of VA scans can be archived and serve for audits or for compliance with certifications.

At a fundamental level, VA systems support *auditability*, which in turn supports incident handling and recovery. VA is an essential part of continuous process improvement for security policies to adapt to the constantly changing threat-and-vulnerability environment.

History and Directory of VA Tools

One of the earliest VA tools was COPS< ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops/ > (Computer Oracle and Password System) developed by Eugene "Spaf" Spafford< http://spaf.cerias.purdue.edu/ > and Dan Farmer< http://www.linkedin.com/in/zenfish > at Purdue University.

In the early 1990s, the Internet Security Scanner (ISS) was the subject of a Computer Emergency Response Team Coordination Center (CERT-CC) Advisory < http://www.cert.org/advisories/CA-1993-14.html > warning of "software that allows automated scanning of TCP/IP networked computers for security vulnerabilities."

Dan Farmer & Wietse Venema< http://www.porcupine.org/wietse/ > developed SATAN< http://www.porcupine.org/satan/ > (Security Administrator Tool for Analyzing Networks) in the early 1990s and posted the code in 1995. For an overview of the tool, see the page< http://www.cerias.purdue.edu/about/history/coast/satan.php > at the Center for Education and Research in Information Assurance and Security (CERIAS).

NESSUS< http://www.tenable.com/products/nessus > from TENABLE Network Security is described by the company as "the world's most widely-deployed vulnerability and configuration assessment product with more than five million downloads to date." The product is freely available for individual, non-commercial use< http://www.tenable.com/products/nessus/nessus-homefeed > and has an evaluation version< http://www.tenable.com/products/nessus-professionalfeed/nessus-evaluation > for use by organizations. The evaluation page includes a chart comparing features of the evaluation version and the professional version, which at the time of this writing (April 2012) costs U$1,500 per year.

NMAP< http://nmap.org/ > (NetMAPper) is a widely used freeware "for Linux, Windows, and Mac OS X." The home page boasts that "Nmap was named "Security Product of the Year" by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in eight movies, including *The Matrix Reloaded*, *Die Hard 4*, and *The Bourne Ultimatum*." [Perhaps other products should consider demonstrating their quality by appearing in popular

movies. Imagine how popular MS Word could become if it appeared in Monty Python movies!]

One of the most useful tools for individual users as well as for network administrators is Steve Gibson's ShieldsUP! service< https://www.grc.com/x/ne.dll?bh0bkyd2 > which provides a quick scan of the first 1056 ports of an individual computer. Ideally, every port will register as "Stealth" (not responding to probes) or at least as "Closed" (not accepting connections).

For links to more products, see the excellent "Alphabetical List of Vulnerability Assessment Products" < http://www.timberlinetechnologies.com/products/vulnerability.html > maintained by Timeberline Technologies< http://www.timberlinetechnologies.com/index.html >.

Concluding Remarks

One of the most important suggestions for effective penetration testing (pen testing) is that vulnerability analysis and vulnerability remediation must precede testing. It's pointless to waste time and money on pen testing if we haven't corrected everything we can find using scanners.

* * *

For study notes on vulnerability assessment, download the IS342 PPTX< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch46_vulnerability_assessment.pptx > *or PDF*< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch46_vulnerability_assessment.pdf > *files.*

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *