Using Vulnerability Assessment Tools To Develop an OCTAVE® Risk Profile

Andrew Storms
GIAC GSEC Practical (v1.4b)
December 03, 2003

Abstract

Threats to information technology are ever increasing and many organizations are spending much money and time in attempting to fix security problems. Before one can think about remediation, assets worth protecting and knowing what to protect those assets from must be defined. OCTAVE® characterizes a self-directed methodology for defining an organization's assets and the assets' risks. Critical to OCTAVE® are the tools and processes toward developing asset-based threat profiles. The threat profile includes network risks, also known as vulnerabilities that often times analysis team members are not qualified to assess. Vulnerability assessment tools aid the OCTAVE® analysis team to determine exactly what network-aware technological risks face any certain asset and often times help to further define the asset itself. By applying the results of a vulnerability assessment to an OCTAVE® Risk Profile, many unanswered questions pertaining to the asset and its risks are fulfilled in an autonomous and consistent fashion.

Introduction

Obvious to most is that the economy's reliance on technology is not diminishing and at the same time, the threats to information technology security are ever increasing. By 2002, our economy and national security had become fully dependent upon information technology and the information infrastructure.[1] According to Symantec's latest Internet Security Threat Report, both the number of attacks to networks and the number of vulnerabilities of software is increasing. Of the many data points included in this report, one notes, "For the first six months of 2003, moderate- and high-severity vulnerabilities were the most common. The number of new moderately severe vulnerabilities increased 21% and high severity vulnerabilities increased 6% as compared with the same period in 2002…".[2] According to the strategies as outlined in The National Strategy to Secure Cyberspace, the federal government should show leadership by continuously testing, monitoring and updating security practices while implementing leading-edge training and workforce development.[3]

In an effort to ensure the security of the organization, many corporations look for methods to test and ensure the security of their systems. The Operationally Critical Threat, Asset and Vulnerability Evaluation^{sm} is one method for defining the assets of a corporation and discovering the risks facing said assets. Where OCTAVE ends, is where vulnerability assessment tools pick up the slack.

About OCTAVE®

Typically, security evaluations are performed by specialized consulting firms or inexperienced IT professionals attempting to find their way in the expansive noise of the security industry. Both methods of security evaluations have their own pitfalls. Hiring a security firm means putting your trust into an outsider to understand your company's assets, business practices and strategic direction. Conversely, leaving the security audit to an undirected IT professional often times translates into blind ambition coupled with lack of participation by executives.

The Operationally Critical Threat, Asset and Vulnerability Evaluation^{sm} (OCTAVE®) process defines a self-directed system for an organization to identify

[1] The President's Critical Infrastructure Protection Board. "The National Strategy to Secure Cyberspace." Draft. September 2002. URL: http://www.isalliance.org/draftcyberplan.pdf

[2] Symantec Corporation. "Internet Security Threat Report Vulnerability Trends." September 2003. URL:http://www.symantec.com/press/2003/n031001.html

[3] The President's Critical Infrastructure Protection Board. "The Nation Strategy to Security Cyberspace." Draft. September 2002. URL: http://www.isalliance.org/draftcyberplan.pdf

its assets, the potential threats to its assets and methods for characterizing information protection. Developed thru coordination between Carnegie Mellon Software Engineering Institute and CERT®, OCTAVE® differences itself from other information security assessments by its self-directed nature, ease of flexibility and balance towards technology, risk and business requirements.

A cross-functional analysis team charges an organization thru the three phases of OCTAVE® which are defined in the publication Managing Information Security Risks: The OCTAVE^{sm} Approach. Phase I, Build Asset-Based Threat Profiles, focuses on defining critical assets, the security requirements of each asset and what is currently being done to protect the asset. Phase I concludes with assembling an asset-based threat profile. Phase II, Identify Infrastructure Vulnerabilities, is a review of the information technology infrastructure. Network paths of access and technology vulnerabilities are identified for each asset. Phase III, Develop Security Strategy and Plans, requires the analysis team to finalize risks to critical assets and develop a protection and risk remediation plan.

What you need to know about OCTAVE®

- OCTAVE® is a process, not a technology one can purchase.
- OCTAVE® requires a cross-functional analysis team to lead the process (executives, managers, workers and IT).
- OCTAVE® was developed thru coordination between CERT and Carnegie Mellon Software Engineering Institute.
- OCTAVE® is self-directed, flexible and focuses on balancing risk with productivity thru tactical operations, strategic direction and technology.

About Vulnerability Assessment Tools

The National American Standard (*T1.523-2001)* defines vulnerability assessment to be "The systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk."[4] Vulnerability assessment tools evaluate network-attached devices (servers, desktops, switches, routers, etc) for vulnerable or potentially vulnerable situations. Most vulnerabilities discovered by these tools result from software flaws, but some tools provide analysts the data necessary to discover design, implementation and configuration vulnerabilities.

[4] Technical Subcommittee on Performance and Signal Processing. "American National Standard for Telecommunications – Telecom Glossary." 2000.
URL: http://www.atis.org/tg2k/_vulnerability_assessment.html

Vulnerability assessment tools are nothing new to Information Technology. Going back to the early 90's, Dan Farmer and Wietse Venema wrote SATAN and authored a paper titled Improving the Security of Your Site by Breaking Into it, in which they discussed the use of SATAN (Security Analysis Tool for Auditing Networks). "Written in shell, perl, expect and C, it [SATAN] examines a remote host or set of hosts and gathers as much information as possible by remotely probing NIS, finger, NFS, ftp and tftp, rexd, and other services."[5]

At that time, SATAN made quite a stir in the industry as people realized it could be used for beneficial or nefarious actions. In today's security industry, the vulnerability assessment market, or know simply as VA, presents a strong product offering of open source and commercial products. Nessus, Internet Security Systems' Proventia™, nCircle Network Security's IP360™ and FoundStone's FoundScan™ are a few of the products available today. See VA Scanners Pinpoint Your Weak Spots (http://www.nwc.com/showitem.jhtml?articleID=15000643) for a more complete list along with independent test results from July of 2003.

Each assessment tool has the same basic concept – scan hosts attached to a network and run a series of tests in an effort to determine which host is vulnerable to a known catalog of vulnerabilities. Vulnerability assessment tools differ themselves from others by speed, feature set and cost to name a few. Of all the vulnerability assessments tools available today, each provides functionality resulting in a more complete asset inspection and asset definition.

What is an Asset-Based Threat Profile?

Developing an OCTAVE® asset-based threat profile requires an enterprise, self-directed view of an organization's assets and the risks threatening these assets. Determining an organization's assets requires proper scope and input from all areas of the organization. An asset is of value to the organization, for example information in electronic or physical form, information systems or a group of people with unique expertise.[6] A threat is an indication of a potential undesirable event.[7] The OCTAVE® approach suggests a method to visibly display assets along with its threats. A visible representation typically shows an asset coupled with access types, the actors involved, the actor's motive and any possible

[5] Farmer, Dan and Venema, Wietse. "Improving the Security of Your Site by Breaking Into It." URL: http://www.fish.com/satan/admin-guide-to-cracking.html
[6] Alberts, Christopher and Dorofee, Audrey. "OCTAVE Threat Profiles". URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf
[7] National Security Telecommunications and Information Systems Security Committee. Index of National Security Telecommunications Information Systems Security Issuances (NSTISSI No. 4014). Ft. Mead, MD: NSTISSC Secretariat, January 1998.

outcome.[8] The threat profile commonly uses vulnerability tools, help from people outside of the OCTAVE® analysis team and may also require outside teams of experts. Commonly, threat profiles reference standard catalogs of practice such as CVE or SANS top 20 listings.

A Possible Threat Profile

	Without IP360
Asset	HR Database
Access	Network
Actor	Employee
Motive	Theft Of Data
Vulnerability	*Unknown*
Outcome	*Unknown*
Catalog Reference	*Unknown*

The threat profile of any given asset may be more detailed as shown and may visibly be displayed differently (OCTAVE® workbooks suggest a tree method; See OCTAVE® Threat Profiles authored by Dorofee and Alberts). The importance of the threat profile is to present the asset with any and all known threats. Further defining the asset, determining the network vulnerabilities, outcome and references to catalogs of an asset is what a VA tool brings to the table for the OCTAVE® process.

Using a Vulnerability Assessment Tool To Develop A Threat Profile

In determining the technological threats to an asset, many organizations rely heavily on expensive security professionals or worse, outdated buggy free tools. These tools rarely work "off the download" and in some cases may require a security professional to interpret the data to meet the needs of an OCTAVE® threat profile. Vulnerability assessment tools either aid the analyst or analysis in many ways, just a few are described below.

Vulnerability assessment tools can:

- More clearly define an asset
- Discover technological and network vulnerabilities

[8] Alberts, Christopher and Dorofee, Audrey. Managing Information Security Risks. The OCTAVE approach. Boston, MA: Addison Wesley Professional, 2003

- Provide multi-perspective view points
- Help to properly scope the analysis
- Reference public catalogs
- Highlight design, implementation and configuration vulnerabilities

Discovery Of Technological and Network Vulnerabilities

Searching and discovering vulnerabilities on a network maintains to be the core result and end goal of vulnerability assessment tools. Vulnerability assessment tools reside on a network or set of networks and in an essence attempt to "hack" all network-connected devices. Vulnerabilities or potential vulnerabilities are reported back the analyst. In OCATVE®, analysts can use this initial set of data to begin a list of technological vulnerabilities without having to hire or perform a formal pen-test or similar assessment.

Clearly Define An Asset

In some organizations, it may be apparent that the companies' assets are not well documented. IT personnel and executives may be aware that a large Oracle database is housing the companies financial records, but may have no idea what version of Solaris is installed on that server or what version of Oracle is active. A vulnerability assessment tool, in due course of finding vulnerabilities, typically will also inspect the asset to determine its operating system and patch level. In addition, each application listening on the network will be "fingerprinted" to determine application and version. VA tools perform this work in an effort to more accurately discover vulnerabilities. As a result, an end user of the VA tool also receives an accurate asset inventory. One such example of this side effect is the work done by nmap. Nmap, which is a freely distributed network port mapper, also has the selection to run remote OS detection using TCP/IP fingerprinting options.[9] Nmap's results may show open ports and applications on those ports, but in addition will return a best guess as to the operating system. Defining the asset is an important first step to an OCTAVE® process and a VA tool can aid analysts in discovering assets and more clearly defining those assets.

Multi-Perspective

[9] Fyodor "Remote OS detection via TCP/IP Stack FingerPrinting." June 11, 2002. URL: http://www.insecure.org/nmap/nmap-fingerprinting-article.html

OCTAVE® recommends that from a network point of view, each asset is analyzed from multiple perspectives - including from within the network and from outside the network.[3] Inspection of an asset from many perspectives ensures that different levels of vulnerability risks are discovered. Putting ingress and egress access control lists thru a vulnerability assessment is an important side of effect of testing from different network perspectives.

Some VA tools provide what is known as multi-perspective. Multi-perspective is the ability to inspect an asset from many different points of view. For example, nCircle's multi-perspective capability named DnA or Distributed nCircle Architecture provides the analysis team flexibility to inspect assets from many disparate points of view.[10] Asset inspection from a single end-point is neither efficient nor does it provide a multi-perspective view of an asset. By placing scanners at different logical and physical locations, a VA tool becomes responsible for asset inspection of hosts on its own network and on nearby or distant networks.

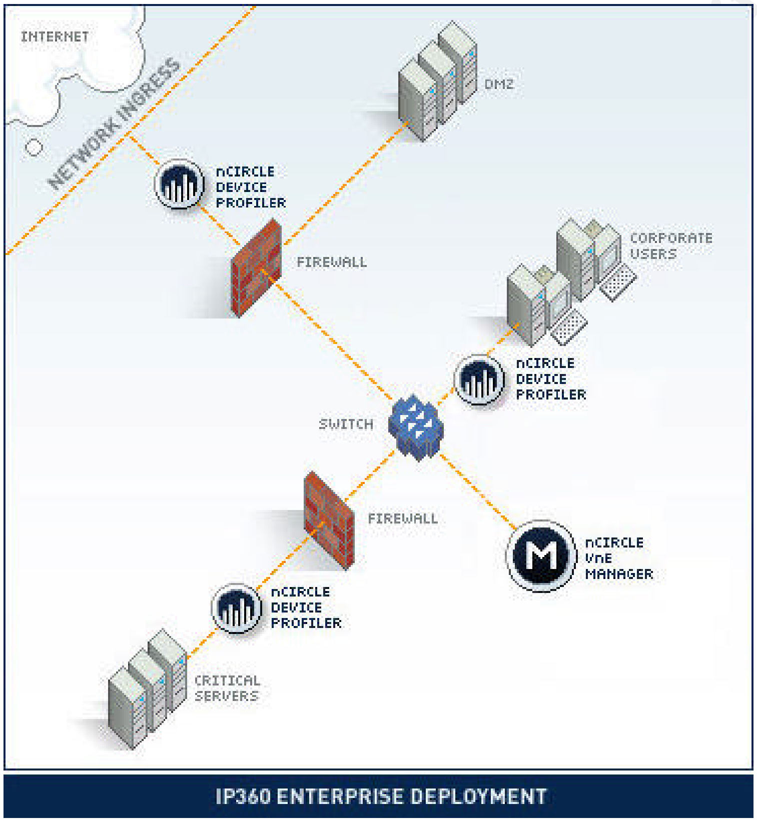


Figure 1 - http://www.ncircle.com/products/deployment.html

[10] URL: http://www.ncircle.com/products/deployment.html

Figure 1 shows a possible VA deployment with 3 scanners. A scanner located in the public network inspects looking inbound, causing inspection traffic to traverse a firewall. Likewise, scanners located on the LAN inspect corporate desktop computers, critical servers and DMZ. Due to the physical and logical position of a scanner, an asset inspection is tied to a perspective. Once a distributed mesh of scanners is created, analysts ensure that inspection traverses ingress and egress policies as well as any access control points that may be present on one or many networks. By distributing the asset inspection to many different points of view, the VA tools provides the OCTAVE® team with multi-perspective data as outlined by OCTAVE®.

Scope

Attempting to manage any security analysis for an entire network presents an unwieldy challenge. OCTAVE® suggests that an analysis should be scoped according to the parameters set forth by the analysis team. Vulnerability assessment tools may also have the same problem of scope, especially if a tool is scanning multiple networks such as in the case of multi-perspective.

Whether vulnerability assessment software is device based, runs from a single node or is multi-perspective, most present a single source for report data and mechanisms to reduce the data into a smaller defined scope - Qualys boasts "centralized reporting" and "easily customizable reports for flexible reporting"[11]; a similar tout by many of its competitors.

To the OCTAVE® team, reducing the dataset which to inspect is significant. Vulnerability assessment tools tout detailed and flexible reporting ranging from diminutive as a single host to an entire network or based on any number of other reporting criteria. No matter the specific reporting criteria, vulnerability assessment tools help the OCTAVE® analysts to scope the analysis at hand.

Reference Public Catalogs

Every security analysis should be benchmarked against a common catalog of practices and based upon the catalog; specific potential outcomes of each threat can be determined. OCTAVE® suggests benchmarking a threat against a common directory such as CVE or lists such as BugTraq or the SANS Top 20. It is within these catalogs and detailed descriptions of vulnerabilities that potential threat outcomes are discussed. Within the vulnerability description, OCTAVE® analysis team members research potential outcomes of a vulnerability, for example: Denial Of Service attack, loss of data and ability to execute arbitrary code on the vulnerable system.

[11] URL: http://www.qualys.com/webservices/qgent/features/

Vulnerability assessment tools typically deliver their own versions of a known vulnerability database. Within these databases of vulnerability information, cross-references are tied to external public catalogs of reference such as CVE and SANS Top 20. The OCTAVE® process suggests benchmarking against public catalogs of references such as CVE and SANS. By utilizing the internal vulnerability databases of these tools, OCTAVE® analysts are automatically given the cross-reference information linking to public security catalogs.

Design, Implementation and Configuration Vulnerabilities

Identification of risk is supplementary to just reporting that a system is running an old version of Apache or is not patched with a specific Microsoft security patch. According to Alberts and Dorofee, technology vulnerabilities can be grouped into the following categories:[12]

- Design Vulnerability
- Implementation Vulnerability
- Configuration Vulnerability

A design vulnerability is inherent in the design or specification of the system's hardware or software.[13] Permitting services such as the "Berkeley R's" to run on a Unix system does not present a threat in itself, however due to the poor authentication methods of rlogin or rexec, these services present a design vulnerability. A flawed software or hardware implementation may manifest itself as an implementation vulnerability.[14] For example, a software programmer may take every effort to ensure the security of credit card transaction software, however the webserver used to transmit credit card numbers from a client to server does not use encryption. The lack of implementing SSL on this webserver would classify as an implementation vulnerability. Finally, configuration vulnerabilities are typically human errors and stem from a system configuration or administration error.[15] The system administrator of a Microsoft SQL server could apply every Microsoft security patch; but leaving the privileged user "sa" account password blank reveals a configuration vulnerability.

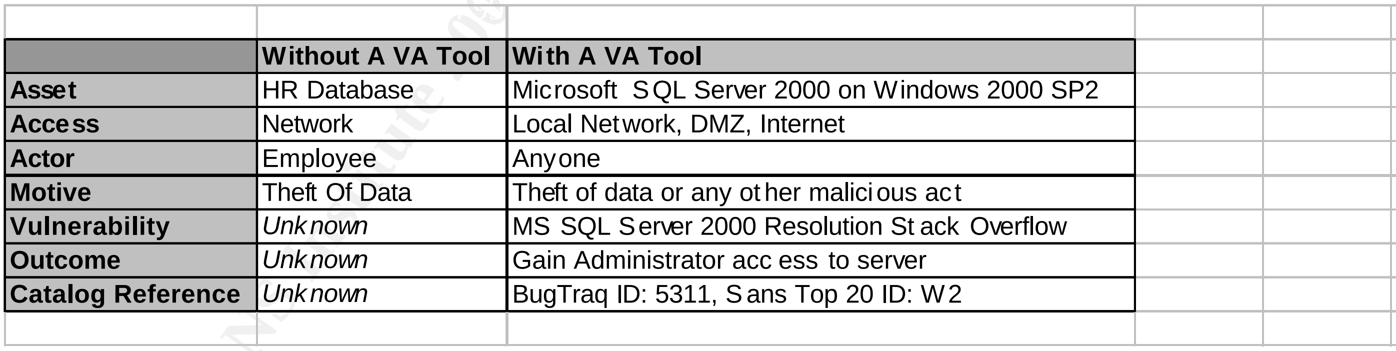
[12] Alberts, Christopher and Dorofee, Audrey. "An Introduction to the OCTAVE Method." January 30, 2001. URL: http://www.cert.org/octave/methodintro.html
[13] Alberts, Christopher and Dorofee, Audrey. "OCTAVE Threat Profiles." URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf
[14] Alberts, Christopher and Dorofee, Audrey. "OCTAVE Threat Profiles." URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf
[15] Alberts, Christopher and Dorofee, Audrey. "OCTAVE Threat Profiles." URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf

Given the autonomous nature of vulnerability assessment tools, it is difficult for any tool to accurately and reliably discover design, implementation and configuration vulnerabilities. However, some VA tools can check for basic configuration vulnerabilities and with further inspection by a human, implementation and design vulnerabilities may become more apparent. One example of a basic configuration check is the Nessus verification of Microsoft SQL Server blank password. Nessus script ID 10673 named "mssql_blank_password" attempts to connect to a SQL server and login under the SA account with a blank password[16]. A successful connection confirms that the SQL server was mis-configured with a blank administrator password, thus constituting a configuration vulnerability.

Vulnerability assessment tools are growing towards the ability to identify every type of vulnerability. Basic design, implementation and configuration vulnerabilities are able to be determined in an autonomous fashion. Nonetheless as these tools mature, they will make efforts to discover and report on all types of vulnerabilities.

The Completed Threat Profile

By applying the information delivered from a vulnerability assessment tool to our sample OCTAVE® Risk Profile, both the assets and risks become clearer and better defined.



	Without A VA Tool	**With A VA Tool**
Asset	HR Database	Microsoft SQL Server 2000 on Windows 2000 SP2
Access	Network	Local Network, DMZ, Internet
Actor	Employee	Anyone
Motive	Theft Of Data	Theft of data or any other malicious act
Vulnerability	*Unknown*	MS SQL Server 2000 Resolution Stack Overflow
Outcome	*Unknown*	Gain Administrator access to server
Catalog Reference	*Unknown*	BugTraq ID: 5311, Sans Top 20 ID: W2

The OCTAVE® Risk Profile can be completed with data from each of the previously discussed methods for using a vulnerability assessment tool within an OCTAVE® analysis. Upon further inspection, the Risk Profile previously presented grows more complete in the following ways:

- Asset is fully defined – Operating System, application, version and patch level are discovered.

[16] URL: http://www.nessus.org/scripts.php

- Possible vulnerabilities are known by the autonomous work performed by the vulnerability assessment tool.
- Access types are now known. Multi-perspective asset inspection expands the access methods.
- Actor is upgraded to anyone because the access method has been expanded.
- Motive is completed from a vulnerability description read about by references to publicly available catalogs of information and practices.
- Outcome – possible outcomes described within the vulnerability information and from publicly referenced catalogs aid the analysts to determine a list of possible outcomes if the asset was compromised.

Conclusion

OCTAVE® presents security professionals with a unique, balanced methodology for addressing security issues within an organization. The United States government recognizes the increased technological threat of information technology and the reality of such threat is confirmed by independent security organizations such as Symantec. Vulnerability assessment tools are a evenhanded solution to put into the tool belt of any OCTAVE analyst. Given the self-directed nature of OCTAVE, it makes sense to invest into an autonomous vulnerability assessment tool to better define an organizations assets and risks. By using a vulnerability assessment tool, OCTAVE analysts can more accurately define a completed asset-based risk profile.

List Of References

The President's Critical Infrastructure Protection Board. "The National Strategy to Secure Cyberspace." Draft. September 2002. URL: http://www.isalliance.org/draftcyberplan.pdf

Symantec Corporation. "Internet Security Threat Report Vulnerability Trends." September 2003. URL:http://www.symantec.com/press/2003/n031001.html

Technical Subcommittee on Performance and Signal Processing. "American National Standard for Telecommunications – Telecom Glossary." 2000. URL: http://www.atis.org/tg2k/_vulnerability_assessment.html

Farmer, Dan and Venema, Wietse. "Improving the Security of Your Site by Breaking Into It." URL: http://www.fish.com/satan/admin-guide-to-cracking.html

Alberts, Christopher and Dorofee, Audrey. "OCTAVE Threat Profiles". URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf

National Security Telecommunications and Information Systems Security Committee. Index of National Security Telecommunications Information Systems Security Issuances (NSTISSI No. 4014). Ft. Mead, MD: NSTISSC Secretariat, January 1998.

Alberts, Christopher and Dorofee, Audrey. Managing Information Security Risks. The OCTAVE approach. Boston, MA: Addison Wesley Professional, 2003

Fyodor "Remote OS detection via TCP/IP Stack FingerPrinting." June 11, 2002. URL: http://www.insecure.org/nmap/nmap-fingerprinting-article.html

URL: http://www.ncircle.com/products/deployment.html

URL: http://www.qualys.com/webservices/qgent/features/

Alberts, Christopher and Dorofee, Audrey. "An Introduction to the OCTAVE Method." January 30, 2001. URL: http://www.cert.org/octave/methodintro.html

URL: http://www.nessus.org/scripts.php