Chapter 8

Vulnerability Management Tools

Solutions in this chapter:

- The Perfect Tool in a Perfect World
- Evaluating Vulnerability Management Tools
- Commercial Vulnerability Management Tools
- Open Source and Free Vulnerability Management Tools
- Managed Vulnerability Services

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

Numerous tools are available to assist with vulnerability management. However, determining which tool(s) to leverage is not easy, because no one product can address all of the aspects of vulnerability management, as we discussed in Chapter 7. Therefore, when deciding which vulnerability management tool(s) to use, it's important that you understand each tool's capabilities, and how the available tools work with each other. In this chapter, we will discuss what to look for when evaluating vulnerability management tools, as well as discuss some of more popular commercial and open source tools available today.

The Perfect Tool in a Perfect World

To determine what to look for in a vulnerability management tool it helps to think about what the perfect tool would offer. The perfect vulnerability management tool would include capabilities for asset management, vulnerability assessment, configuration management, patch management, remediation, reporting, and monitoring, all working well together, and it would integrate well with third-party technologies.

Ideally, the tool's asset management, vulnerability management, and patch management capabilities would work particularly well together, for three reasons. First, asset management represents the foundation of a vulnerability management program. Without a complete and up-to-date asset inventory, your vulnerability management program will be only marginally effective. Therefore, it's critical that your tools leverage this repository for the list of assets represented within your environment.

Second, you're developing a vulnerability management program, so it would be nice if your vulnerability management tools and auxiliary tools could communicate with one another. A primary example is in your vulnerability assessment (VA) scanner leveraging the asset database to obtain the list of devices that are present within your environment. From that list, the VA scanner knows which assets to assess for security liabilities. VA tools are also helpful in developing system configuration baselines within your environment. You can use these baselines later to identify possible weaknesses and points of exposure within your infrastructure.

And third, patching and configuration management are key elements of the remediation process and, more important, of your vulnerability management plan. Understanding which systems are patched, along with their respective configurations, is one thing; but having this information populated within your asset database and being able to extract this data and use it to make informed security decisions is a capability which all security practitioners wish they had.

Notes from the Underground…

Useful Sites: INFOSEC Mailing Lists, Tools, and Information

Here are some rather useful sites for security tools and security mailing lists:

- Tools and mailing lists: www.securityfocus.com
- Tools: packetstormsecurity.nl
- Mailing list: lists.apple.com/mailman/listinfo/security-announce
- Mailing list archives: seclists.org
- Tools and security advisories: www.frsirt.com/english/index.php
- Tools and security advisories: www.microsoft.com/technet/security/

Evaluating Vulnerability Management Tools

Vendors typically market their tools as the panacea for everything; vulnerability management vendors are no exception. Although some products address multiple areas of the vulnerability management life cycle, others attempt to bridge the gap between vulnerability management tools in an effort to provide synergy among products—for example, integrating patch management tools with vulnerability scanners. In the end, no one vendor or solution provides all of the components necessary to support a vulnerability management program.

Prior to deciding upon a tool, you must understand its capabilities as well as its shortcomings. To aid you in this you should consider the following points when evaluating vulnerability management technologies:

- **Asset management.** Does the technology provide an asset inventory database? If so, can you extend the database schema to support additional fields, such as asset classification? If not, can the technology integrate with other asset management repositories?
- **Coverage.** What's the breadth and platform coverage of the technology? Many technologies can perform operations against the Windows family of products, but you'll need technologies that can operate in a heterogeneous environment and can support a variety of platforms, applications, and infrastructure devices.
- **Aggregation of vulnerability data.** Does the product interoperate with other security technologies? Can the product aggregate data from security technologies such as Internet Security Systems' IIS Scanner, Microsoft's MBSA, Tenable Network Security's Nessus, McAfee's Foundstone, eEye's Retina, and Symantec's BindView bvControl? The ability to aggregate data from multiple and disparate sources is key.

- **Third-party vulnerability references.** Is the product Common Vulnerabilities and Exposures (CVE) compliant? Does it identify the source from which it received its information?
- **Prioritization.** Can the tool prioritize remediation efforts?
- **Remediation policy enforcement.** Does the product provide the capability to designate the selected remediation at varying enforcement levels, from mandatory (required) to forbidden (acceptable risk), via a centralized policy-driven interface?
- **Remediation group management.** Does the tool allow for the grouping of systems to manage remediation and control access to devices?
- **Remediation.** Can you use the product to address vulnerabilities induced by a system misconfiguration as well as vulnerabilities represented by not having the appropriate patch? For example:
    - Patch management, or deploying patches to the operating system or applications
    - Configuration management, or deploying changes to the operating system or application, such as disabling and removing accounts (i.e., accounts with no password, no password expiration, etc.), disabling and removing unnecessary services, and so on
    - The ability to harden services for NetBIOS, anonymous FTP, hosts.equiv, and so on
- **Patch management.** Does the product include or integrate with existing patch management tools?
- **Distributed patch repository.** Does the product provide the capability to load balance and distribute the bandwidth associated for patch distribution to repositories installed in various strategic locations?
- **Patch uninstallation support.** Can the tool report whether a patch was unsuccessful and whether it needs to be reapplied?

- **Workflow.** Does the product have a workflow system that allows you to assign and track issues? Can it auto-assign tickets based on rule sets defined (i.e., vulnerability, owner, asset classification, etc.)? Can it interface with common corporate workflow products such as BMC Software's Remedy and the Hewlett-Packard HP Service Desk?
- **Usability.** Can the tool participate in network services with minimal impact to business operations? Is the user interface intuitive?
- **Reporting.** Does the tool provide reports to determine remediation success rates? Can you use the tool for trending remediation efforts? Is the reporting detailed and customizable?
- **Appliances.** Is the tool software based or appliance based? Appliances often offer performance and reliability advantages. However, software solutions are more affordable and may be able to run on existing hardware, helping to reduce upfront capital expenditures.
- **Agents.** Does the application require agents? Is the application capable of leveraging existing agents on the system? If agents are necessary, can you deploy agents to groups of assets simultaneously, to facilitate ease of deployment? Agents generally provide more information on a particular system, but also increase the system's complexity. An ideal application would allow for the collection of system information with or without the use of agents.
- **Configuration standards.** Does the technology possess predefined security configuration templates that you can use to assess the system? Some products have defined operating system standards and are able to perform reporting based on defined templates to support some regulatory requirements (e.g., Sarbanes-Oxley, HIPAA, and the ISO/IEC 27000 series).
- **Vulnerability research.** Does the vendor have its own vulnerability research team? Does the vendor actively participate in the security community through the identification and release of security vulnerabilities? Does the vendor practice responsible disclosure? Does the

vendor release checks for vulnerabilities it has discovered prior to the OEM remediating the vulnerability? How has the vendor responded to vulnerabilities in its own products?

- **Vulnerability updates.** How frequently does the vendor release updates? How are the updates distributed? Does the distribution mechanism leverage industry-recognized security communications protocols?
- **Interoperability.** Can the application integrate into existing patch management, configuration management, and/or monitoring tools and services?

Note that the items in the preceding list aren't applicable to all vulnerability technologies. We presented a germane list of points that apply to the collection of tools which support a vulnerability management program.

Commercial Vulnerability Management Tools

The vulnerability management space is changing frequently due to mergers, acquisitions, and new partnerships. In the remainder of this section, we will discuss some of the vendors that offer solutions in this space.

eEye Digital Security

www.eEye.com

eEye Digital Security is a leader in vulnerability research. It also develops a suite a tools that can assist you in vulnerability management. The suite consists of the Retina Network Security Scanner (a vulnerability assessment tool), Blink Professional (a host-based security technology), and the REM Security Management Console. The management console provides the centralized management interface for the company's other products. It also handles vulnerability management workflow, asset classification, and threat-level reporting, and it can integrate with CA's UniCenter, IBM's Tivoli, and HP's OpenView.

Symantec (BindView)

www.bindview.com

BindView's Compliance Manager is a software-based solution which allows organizations to evaluate their assets against corporate standards or industry best practices, without the need for agents in most cases. Assets are evaluated against standards and practices based on a pass/fail notion; either an asset is compliant or it's not. Data is then aggregated and assembled to produce reports that the remediation team can leverage to support their efforts, or the internal audit group can use for compliance issues. You also can use the reports generated to support other initiatives.

As mentioned, you can evaluate assets against internal standards or to industry best practices. The industry standards included are CIS Level 1 and Level 2 Benchmarks for Windows, Red Hat Linux, BindView's Security Essentials for Sun Solaris, and NetWare. In addition to these standards, the Compliance Manager also provides Report Views for the following regulations and frameworks: ISO 17799, Sarbanes-Oxley based on COBIT, FISMA based on NIST SP 800-53, HIPAA, Basel II, and GLBA.

The Compliance Manager does not include its own workflow capability, but it does provide an interface that allows users to open incidents in Remedy and HP Service Desk. In addition, leveraging its bvControl technology, BindView is capable of delivering patch and configuration management to Windows hosts.

Attachmate (NetIQ)

www.netiq.com

NetIQ's Compliance suite, a combination of NetIQ's Security Manager and Vulnerability Manager tools, brings together vulnerability scanning, patch management, configuration remediation, and reporting. The NetIQ Vulnerability Manager enables users to define and maintain configuration policy templates, vulnerability bulletins, and automated checks via AutoSync technology. It also has the capability to evaluate systems against those policies. Predefined templates are available for Sarbanes-Oxley, HIPAA, and ISO/IEC 27000. These allow you to report and score your information systems against these standards.

The Compliance suite also supports a classification system that allows you to adjust risk scores based upon the asset's classification. The NetIQ suite also looks for common signs of system compromise, such as modified Registry keys and known malicious files, and it has an OEM relationship with Shavlik to provide integrated patch management.

StillSecure

www.stillsecure.com

StillSecure is the manufacturer of VAM, an integrated suite of security products that perform vulnerability management, endpoint compliance monitoring, and intrusion prevention and detection. It also includes a built-in workflow solution (Extensible Vulnerability Repair Workflow) which automatically performs assignment of repairs, scheduling, life cycle tracking, and repair verification, all while maintaining detailed device histories.

VAM interoperates with other third-party scanners too, taking input from Nessus, the ISS Internet Scanner, Harris STAT, and others. Enterprises may want to be wary regarding VAM, because its reporting module is not as well refined as the other vendors' and it relies on third-party information and integration for asset management, patch management, and vulnerability resolution.

McAfee

www.mcafee.com

McAfee's Foundstone Enterprise is an agentless solution that offers asset discovery, inventory, and vulnerability prioritization with threat intelligence, correlation, remediation tracking, and reporting. It integrates with McAfee's IntruSheild network-based intrusion prevention system (IPS), McAfee's Preventsys Compliance Auditor, and other vulnerability and trouble-ticket management systems. One of its more appealing features is its SSH credentialed scans for Red Hat Enterprise, Solaris, AIX, Microsoft Windows, and to the surprise of many, Cisco IOS!

Compliance templates for Sarbanes-Oxley, FISMA, HIPAA, BS7799/ISO17799, and the Payment Card Industry (PCI) standard are included, expediting the preparation of audits. Foundstone Enterprise can also auto-assign tickets, streamlining and simplifying the remediation process.

Open Source and Free Vulnerability Management Tools

The open source community has created some great security tools over the years. However, none of them represents a complete vulnerability management solution. In some cases, though, the open source tools integrate well together, forming a formable foe to the commercial offerings.

In the following sections, we cover open source tools that you can use to support your vulnerability management program.

Asset Management, Workflow, and Knowledgebase

One tool we recommend in this space is Information Resource Manager (IRM), available at http://irm.stackworks.net. IRM is a powerful Web-based asset tracking and trouble-ticket system built for information technology (IT) departments and help desks. All elements are interwoven into a seamless Web application, with a MySQL engine at the back end doing the heavy lifting.

Host Discovery

For host discovery, Nmap (www.insecure.org) is a free, open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw Internet Protocol (IP) packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and versions) they are running, what type of packet filters/firewalls are in use, along with dozens of other characteristics. Nmap runs on most types of computers and both command-line and graphical versions are available.

Vulnerability Scanning and Configuration Scanning

Nessus, from Tenable Network Security (www.tennable.com), is a tool for vulnerability scanning and configuration scanning. The Nessus Project was started by Renaud Deraison in 1998 to provide the Internet community with a free, powerful, up-to-date, and easy-to-use remote security scanner. Nessus is the best free network vulnerability scanner available, and the best to run on UNIX at any price. It is constantly updated (more than 11,000 plug-ins are available for as a free feed), but registration and EULA acceptance are required. Key features include remote and local (authenticated) security checks, client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your own plug-ins or understanding the existing ones.

Nessus 3 is now closed source, but it is still free unless you want the very newest plug-ins. If you decide to rely on only Nessus for vulnerability scanning, consider also choosing a product that can manage and schedule scans, such as Tenable Security's Security Center product (www.tenablesecurity.com).

Configuration and Patch Scanning

Microsoft's Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small and medium-size businesses determine their security state in accordance with Microsoft security recommendations, as well as offers specific remediation guidance. Built on the Windows Update Agent and Microsoft Update infrastructure, MBSA ensures consistency with other Microsoft management products including Microsoft Update (MU), Windows Server Update Services (WSUS), Systems Management Server (SMS), and Microsoft Operations Manager (MOM). MBSA on average scans more than 3 million computers each week! For more information, visit www.microsoft.com.

Vulnerability Notification

Advchk (Advisory Check), available at http://advchk.unixgu.ru, reads security advisories so that you don't have to. Advchk gathers security advisories using RSS feeds, compares them to a list of known services, and alerts you if you are vulnerable. Because adding hosts and services by hand would be a boring task, Advchk leverages NMAP for automatic service and version discovery.

Also available in this space is SIGVI (http://sigvi.sourceforge.net). This product is a recent release but could be a promising solution if maintained and developed further. SIGVI downloads vulnerabilities from defined sources, stores them to a database, and then compares them to the products currently installed on the assets (as previously defined in the main application).

The application is flexible in the way that it lets you define your own sources. By default, the application supports the NVD (National Vulnerability Database at http://nvd.nist.gov) format. Periodically, the application will contact the sources, download the vulnerabilities, and store them into the SIGVI database. Those vulnerabilities are then available through the pages of the SIGVI main window.

Security Information Management

Ossim (www.ossim.org) stands for Open Source Security Information Management. Innately a SIM, OSSIM does incorporate several aspects of vulnerability management and over time should become a more comprehensive and complete vulnerability management tool. OSSIM's goal is to provide a comprehensive compilation of tools which, when working together, grant a network/security administrator a detailed view of the network and devices.

Besides getting the best out of open source tools, some of which are described in the following list, OSSIM provides a strong correlation engine, detailed reporting, and incident management tools. Here is a list of open source tools that integrate with OSSIM:

- **Arpwatch.** Used for Media Access Control (MAC) address anomaly detection.
- **P0f.** Used for passive operating system detection and operating system change analysis.

- **Pads.** Used for service anomaly detection.
- **Nessus.** Used for vulnerability assessment and cross-correlation (IDS versus Security Scanner).
- **Snort.** An IDS, used for cross-correlation with Nessus.
- **Spade.** A statistical packet anomaly detection engine, used to gain knowledge about attacks without a signature.
- **Tcptrack.** Used to gather session data information that can provide useful information for attack correlation.
- **Ntop.** A network usage tool that builds an impressive network database from which you can derive aberrant and anomalous behavior.
- **Nagios.** Monitors host and service availability information.
- **Osiris.** A great host-based intrusion detection system (HIDS).

Managed Vulnerability Services

Many organizations have elected to outsource the challenging task of vulnerability management; if not in total, certainly in parts. Outsourcing a vulnerability management program can help you to reduce head count, administrative overhead, and equipment and personnel expenses. However, before you get too excited about the advantages of outsourcing vulnerability management, you need to keep in mind that an effective outsourced solution is going to be based in part on how well you've defined your requirements.

Tired and weary veterans of outsourcing know that clear and concise service-level agreements (SLAs), which have been drafted in conjunction with legal counsel, represent the foundation of all outsourcing relationships and aid in remedying issues that arise during the term of a contract.

NOTE

One mistake people often make is to believe that business risk is transferred when you outsource a portion of your security program, such as vulnerability management. However, risk is not transferable. Organizations remain responsible, even when their operations are completely outsourced, although they may shift the financial liability to the third party. With that said, it's critical to assess a provider's financial stability when considering outsourcing.

When leveraging a third party to support all or part of your vulnerability management program you should consider the following:

- **Escalation procedures.** Ensure that escalation procedures exist and communication processes are defined. Also ensure that ownership is well documented and agreed upon in writing by both parties.
- **Data access.** Ensure that you have access to the data that the outsourcer is collecting. Many times an outsourcer will collect data from your assets, but won't provide you with access to the data. You could use this data to better ascertain risk within your environment, and it could help you to make appropriate risk-based decisions. If the outsourcer doesn't allow you access to your data, you should think twice before signing the contract. Also, it is important that you understand how the outsourcer shares your data within its own organization. Is your data privy to everyone who works for the outsourcer?
- **The toolset.** Before selecting a vendor, you should confirm which products the vendor uses, and why. There may be a conflict between the vendor's tools and yours, or the vendor may simply be using inferior technology to support your operations.

- **Metrics.** How will the provider be evaluated/measured? It is important that you ensure that these metrics are clearly defined. Depending on the level of service the outsourcer is providing, the metrics used to evaluate the outsourcer may be different; for example, if the provider is providing path management, how long does the provider have before it must patch all of the assets it manages? You should define, understand, and clearly agree upon these metrics up front.

Summary

In Chapter 7, we discussed the methodology behind vulnerability management. In this chapter, we discussed what an ideal vulnerability tool features, although we know and understand why such a tool doesn't exist. However, as we discussed, some vendors are getting close to delivering complete solutions in this comparatively new discipline in information security.

We briefly discussed some of the players, but gave no suggestions regarding the pros and cons of the tools because there is no one tool that fits all the requirements of an organization. Although the open source community has a wealth of great tools available, there isn't one tool that supports all of the facets of vulnerability management; rather, there are bits and pieces scattered among many authors.

To close out the chapter, we discussed some of the pros and cons of leveraging an outsourcer to manage parts of a vulnerability management program. It's conceivable, and many organizations do it, but it's imperative to put in place some serious guidelines and detailed service-level agreements beforehand to ensure that no one becomes disappointed with the delivery of the service.

Solutions Fast Track

The Perfect Tool in a Perfect World

☑ The perfect vulnerability management tool would include asset management, vulnerability assessment, configuration management, patch management, remediation, reporting, and monitoring capabilities.

☑ All of these components interoperate, pushing and pulling data as each task is performed.

Evaluating Vulnerability Management Tools

☑ No one vendor has a solution or set of technologies that completely addresses all aspects of the vulnerability management life cycle.

☑ Several key questions can assist you in evaluating vulnerability management tools and, hopefully, in identifying gaps in terms of capabilities.

Commercial Vulnerability Management Tools

☑ The vulnerability management market is changing frequently due to mergers, acquisitions, and alliances. Numerous vendors provide tools in this space, so you must identify your needs prior to evaluating technologies.

Open Source and Free Vulnerability Management Tools

☑ The open source community has created some great security tools.

☑ No one tool provides a complete vulnerability management solution.

☑ It may not require much effort to create interoperability between open source vulnerability management tools.

Managed Vulnerability Services

☑ Set some serious guidelines and detailed service-level agreements to ensure that no one becomes disappointed with the delivery of a service.

☑ Before selecting a vendor, confirm which products the vendor is using and how the information is distributed to interested parties.

☑ Ensure that you have access to the raw data.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: How do I decide which tool to use?

A: Demo the technology first. Most vendors provide trial-ware offerings of their products. Even if it's an appliance-based solution, most vendors are usually willing to provide you with a loaner unit. Managed vulnerability providers also allow for interactive demonstrations.

Q: Should I seriously consider an open source solution?

A: That depends on your aversion to technology. If you're looking for creative technologies and novel intellectual property, and you are seeking to fill a gap within your vulnerability management program, you should definitely consider open source. If your organization is taking the creation of a vulnerability management program seriously (i.e., you have a budget), you should look into a combination of commercial tools and open source tools.