Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Vulnerability Management: Tools, Challenges and Best Practices

In today's competitive marketplace, companies cannot afford to lose time, money, or integrity due to security incidents. Businesses can suffer immeasurable losses if a data center has a production outage as a result of a worm or virus, a hacker defaces a website, or critical customer information is lost or stolen. The fear of revenue loss should motivate smart businesses to begin taking proactive measures against vulnerabilities. The concept of Vulnerability Management is a critical process that should be followed in l...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
CounterTack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Cathleen Brackin
Version 1.4b (amended August 29, 2002)
GSEC Option 1
October 15th, 2003

Vulnerability Management:
Tools, Challenges and Best Practices

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ABSTRACT 3
DEFINING THE SCOPE OF VULNERABILITY MANAGEMENT 3
STEP 1: ASSET INVENTORY 4
Overview *4*
Challenges *4*
Tools *5*
Best Practices *6*
STEP 2: INFORMATION MANAGEMENT 6
Overview *6*
Challenges *7*
Tools *7*
Best Practices *8*
STEP 3: RISK ASSESSMENT 8
Overview *8*
Tools *9*
Challenges *10*
Best Practices *10*
STEP 4: VULNERABILITY ASSESSMENT 11
Overview *11*
Tools *11*
Challenges *11*
Best Practices *12*
STEP 5: REPORTING AND REMEDIATION TRACKING 12
Tools *12*
Challenges *14*
Best Practices *14*
STEP 6: RESPONSE PLANNING 15
Tools *15*
Challenges *15*
Best Practices *15*
CONCLUSION 16

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

In today's competitive marketplace, companies cannot afford to lose time, money, or integrity due to security incidents. Businesses can suffer immeasurable losses if a data center has a production outage as a result of a worm or virus, a hacker defaces a website, or critical customer information is lost or stolen. The fear of revenue loss should motivate smart businesses to begin taking proactive measures against vulnerabilities. The concept of Vulnerability Management is a critical process that should be followed in large and small organizations as a way to identify, assess and respond to new threats before they become a reality. This paper will outline the key steps to Vulnerability Management, and provide an in-depth look at the tools, challenges and best practices of each part of the VM lifecycle.

Defining the Scope of Vulnerability Management

Vulnerability Management has been defined by the Harris company as "the process of finding, evaluating and remediating vulnerabilities (existing exploitable weaknesses) on servers and workstations. The only way to properly secure a system is to first assess the existing vulnerabilities on each machine, determine the degree of risk for each machine's vulnerability, and then remediate (fix) the vulnerabilities. This process of finding, evaluating and remediating is known as vulnerability management"(Harris "STAT"). This concept expands upon the previous best practices around vulnerability assessment as a standalone process. Vulnerability management provides a holistic solution to security threats by handling vulnerabilities throughout the entire lifecycle. According to a 2002 article in Information Security's online magazine by Al Berg there are 4 steps to Vulnerability Management: 1) inventory your systems, 2) manage the flow of information, 3) assess the information, and 4) plan for response (Berg, sec.1). In order to effectively manage vulnerabilities, organizations must expand upon Mr. Berg's 4 steps. I believe that there are truly 6 crucial pieces to the vulnerability management lifecycle: 1) maintaining an asset inventory, 2) managing information dissemination, 3) assessing risk level of assets and vulnerabilities, 4) performing vulnerability assessments, 5) tracking remediation and report status, and 6) planning for response (see Figure 1). In order for the process to be successful, each participating group has to assist in defining the goals and mission of the VM team and take ownership. Each step of the Vulnerability Management process should be documented and published to the teams who are involved. To gain end user support, it makes sense to provide security awareness training around Vulnerability Management and Response plans. This paper will cover the various tools, challenges and best practices associated with each of these 6 steps.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

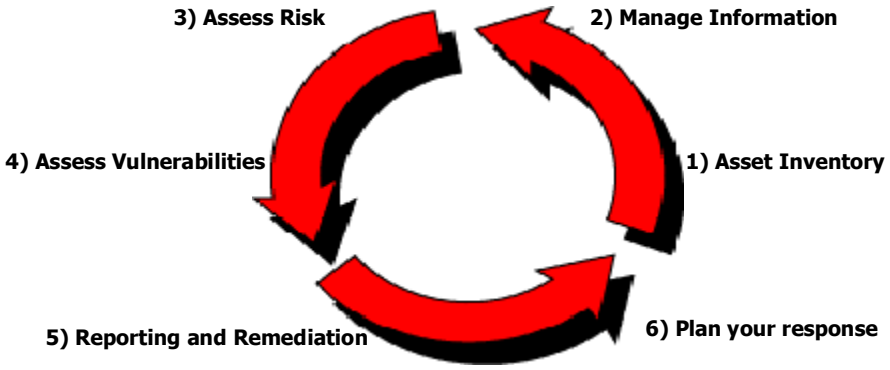

Figure 1 Vulnerability Management Lifecycle

Step 1: Asset Inventory

Overview

Obtaining and maintaining an accurate asset inventory is a goal that many companies never reach. Steve Crutchley of 4FrontSecurity was asked to comment on the asset inventory challenge at this year's RSA Conference. He states there are "many organizations I have counseled [who] lack an effective asset inventory. Without an asset inventory, how are the systems and network engineering groups supposed to sift through security alerts and know which ones apply to them and which can be discarded?" (Gregory, par. 3). Furthermore, businesses should identify a single entity to hold responsible for inventory management to ensure consistency. Companies who are unwilling or unable to manage their networks will end up paying a higher cost in the long run when they cannot quickly find and patch their systems. There are tools for any size company that can help teams track and manage their assets.

Challenges

Managing today's network environment poses many challenges. In addition to the new vulnerabilities that are discovered every day, there are the issues of poor change management, rogue servers, and blurred network boundaries. As organizations merge with and absorb other companies, their networks are typically joined together, but never truly homogenized. The lack of resources, proper tools, and assigned responsibility become the biggest obstacles to maintaining an accurate and up-to-date inventory. These challenges must be handled before an organization takes on the effort of network management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Tools

Countless network management tools exist in today's marketplace. The key to choosing the right one for your organization is to list out the criteria that are important to you and review several products against them. This paper will only provide a brief listing of some of the tools available today, including their pros and cons.

Peregrine (http://www.peregrine.com) offers three products that can be used together to get an accurate picture of your organization's network. Peregrine's AssetCenter is the management piece that will allow any helpdesk or command center quickly view inventory data, and has the added benefit of providing additional details about software licensing and compliance, if you have the Network Discovery and Desktop Inventory pieces installed. In order to maintain a fresh view of the network, however, you must also use Peregrine's Network Discovery and Desktop Inventory. These tools offer an integrated solution that will provide comprehensive network details, physical topology, and desktop configuration and software licensing information viewable from one management interface. Pricing may be too high for smaller companies, and additionally, the desktop solution requires client installs, which could use more resources than are available. Rogue desktop clients also become another issue, since Desktop Inventory will not find them. Overall, this solution seems scalable, and integrated, yet may not provide the flexibility required for ever changing network environments.

Next, LANDesk's Management Suite 7 (http://www.landesk.com/) is a robust network management product that provides asset management, imaging, software distribution, software license monitoring, and remote control features. This tool provides a network discovery component that will identify new hosts on the network and inventory scans that run in the background on clients and report delta information back to the database. Management Suite 7 provides a scalable solution, a backend database that can be exported, and overall, a solid network management tool. This product may be too costly if not being integrated with other help desk and command center functions, and additionally, the desktop client installation may be too time consuming and will not locate rogue desktops.

Latis Networks (http://www.latis.com) StillSecure suite of tools provides network discovery capabilities, and also leverages that data for Vulnerability Management. StillSecure VAM 2.5 (Vulnerability Assessment and Management) products include Desktop VAM, Server VAM, and Remote VAM. These three products can be purchased separately or together, and can provide a holistic view of your network. The VAM product will run automatic or scheduled discovery scans based upon the CIDR blocks that you provide. It will inventory and document new hosts and configure the appropriate vulnerability scans to be run based upon the operating system and services on each host. One of the outstanding features of the VAM products is that they will continuously scan your network for desktops and servers, without installing a client on the network hosts

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

themselves. Additionally, you can utilize the Remote VAM to discover new devices on the perimeter from the outside. Another handy feature is the ability to group inventory by logical business units or system administrator. The only drawback to the VAM products is that it is collecting data about systems for vulnerability assessment and will not collect the amount of necessary data for a robust asset inventory.

Finally, Foundstone's Enterprise, powered by the Foundscan Engine, (http://www.foundstone.com) provides network discovery based upon IP address ranges. When configuring Foundstone Enterprise, users can configure *organizations* that are assigned specific IP ranges. The discovery scans will be run based upon when the organization schedules them to be done. Some critical features offered to users allow them to perform host discovery, services discovery, and DHCP correlation via the Enterprise web interface. Like the Latis product offering, Foundstone will intelligently assess your network for vulnerabilities based upon the network discovery. And, as with Latis, the Foundscan engine will only collect data relevant to vulnerability scanning, falling short of a true asset inventory.

Best Practices

Before undertaking the challenge of a network asset inventory, there are several industry best practices to keep in mind (Raspberry)

- Establish a single point of authority for the inventory
- Get the word out! If the process is being improved or is completely new, end users and support staff will need to know who to notify when something changes.
- Update inventory management systems via change management processes.
- Use an asset numbering scheme and use consistent abbreviations and notations when entering data
- Validate the inventory annually

Step 2: Information Management

Overview

The second step towards true Vulnerability Management is managing the flow of new information into your organization. Currently, there is a constant influx of information about new vulnerabilities, worms, viruses, and threats. This overwhelming amount of data can lead to confusion about where to begin. It is important that part of your VM program involves the use of a Computer Security Incident Response Team (CSIRT). The CSIRT can be made up of staff from various teams who participate as one function of their other jobs, or of staff dedicated entirely to serving the CSIRT function. Although we typically may think

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of the CSIRT as a function that only responds to emergencies, that is not always the case. According to the Carnegie CERT® Coordination Center, the first computer security incident response team, the CSIRT can be responsible for "disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem." (CERT Handbook, p.25). As a filter, the CSIRT can identify which vulnerabilities and threats are serious to your specific organization. For example, they may receive an alert that a new IIS vulnerability has been discovered, however, after Nimda, the company decided to switch to a different web server as the corporate standard. In this scenario, the CSIRT could effectively filter that information from being raised as an advisory to the company.

Challenges

The challenges of information management are typically related to the breadth and depth of the information being gathered and shared, and the methods by which they are shared. It becomes difficult for organizations to manage the flow of new security related information in and out of the company. This responsibility is typically handled by a CSIRT, who can provide oversight to the entire organization's security posture. Some common issues that CSIRTs have to face include the sheer volume of security data, the complexity of the information being disseminated, the multiple sources of new information, and how to best communicate new security vulnerabilities to the general user public. It is also a challenge for the CSIRT to plan for the appropriate resources required to monitor security news and websites, researching the vulnerabilities, and communicating the appropriate alerts to the right audience. One of the other issues faced by CSIRTs is the "helpful end user." Users have access to many of the same resources as the CSIRT team, and, if not properly educated, may react to new threats and vulnerabilities without the guidance of the security team or the CSIRT. This poses a problem to the CSIRT's efforts because they should be the ones to make and communicate the strategy for the organization as a whole. These tasks must be handled efficiently to ensure the appropriate response times and actions from systems administrators, security teams, and the general user public. Organizations should ensure that there is an Incident Response guide and/or policy in place, accessible and clearly communicated. These issues are addressed in the CERT Handbook for Computer Security Incident Response Teams as part of the Incident Handling service under the Announcement Function.

Tools

The tools for information management consist of very simple communication tools such as, email, websites, distribution lists and mailing lists, and security incident policies. Multiple resources exist for CSIRTs to collect data about security news, vulnerabilities, alerts and technical information. There are many websites and mailing lists, free and subscription based, which can keep CSIRTs alerted to new security vulnerabilities and allow them to respond quickly to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

assess the risk to the organization and react. Some of the most well known and responsive security websites are: CERT Coordination Center at www.cert.org, ICAT metabase http://icat.nist.gov/icat.cfm , Security Focus (includes several mailing lists) www.securityfocus.com, Symantec Security Response http://securityresponse.symantec.com/, Packet Storm Security http://packetstormsecurity.nl/, National Infrastructure Protection Center (NIPC) www.nipc.gov, and www.incidents.org . These are just a few examples of the numerous resources available on the internet. CSIRTs can utilize email alerts via distribution list to publish advisories once they've determined that they wish to alert the organization about a new threat or vulnerability. The CSIRT can also maintain a website with the newest vulnerabilities and remediation best practices for general end users. Additionally, organizations can use security policies and guidelines to educate users that they should not independently react to vulnerability issues, but should await direction from management and the CSIRT team.

Best Practices

Because the CSIRT will be challenged to consistently and continuously assess the threat level to the organization, they should create their own best practices and collect them from other organizations. Best practices can assist the CSIRT with quickly and effectively disseminating information and providing guidance to users. Some best practices include:

- Use a CSIRT mailing list and allow employees to subscribe to it
- Use a CSIRT website to publish all advisories
- Hold a daily conference call with the correct security teams and lines of business. Review new vulnerabilities, virus activity, malicious activity, and other important security issues
- Create incident response guidelines for employees discouraging them from responding to new security alerts and threats without guidance from CSIRT
- Create a standardized alert format, to provide a consistent "look" for CSIRT communications
- Review the CSIRT handbook for guidelines at http://www.cert.org/archive/pdf/csirt-handbook.pdf

The CSIRT team will handle massive amounts of data regarding new vulnerabilities and should standardize their communications and methodologies to ensure consistency in reporting and handling.

Step 3: Risk Assessment

Overview

In risk management, the 3 objectives are to preserve the confidentiality, integrity, and availability of information systems (Kurtz and Vines, 3). Before an organization can truly mitigate risk, its security team must assign a risk level to new vulnerabilities as they are announced. This exercise is important since

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

organizations have limited resources and time before new vulnerabilities are exploited. Assigning risk levels allows companies to prioritize large amounts of work to a limited resource pool and still minimize the likelihood that a threat will be realized. According to Symantec, "64% of attacks during the first six months of this year were aimed at vulnerabilities less than one year old; most of those--39% percent--targeted security flaws that had been disclosed in the previous six months (Information Week). Risk is determined by four basic elements: the threat, the possible consequences of that threat if realized, the probable frequency of said threat, and the extent of how confident you are that it will happen. (CISSP Prep Guide, p.15). CSIRTs can assess new vulnerabilities by reviewing the four basic elements of risk as it pertains to their organization. These reviews can be time consuming and may require a dedicated resource.

Tools

Security teams can utilize homegrown tools to help assess the level of risk associated with a specific vulnerability. Checklists can simplify the process of asking key questions about the vulnerability and any possible threats. These questions should be defined by an organization's security team and documented for consistency. Appropriate questions will help define the risk level of the associated vulnerability specific to an organization's environment. According to articles on Vulnerability Management, an organization's process for assigning a risk level should include the following as outlined by Al Berg in his article "Feeling Vulnerable?" ("Feeling"):

- How does this vulnerability affect your organization?
    - Do you have that technology in use?
    - If yes, are you running the vulnerable version (or component)?

- What business resources are at risk?
    - Is the resource mission critical?
    - Is it on the internal network, in the DMZ, or on the perimeter?

- Can the vulnerability be exploited remotely?
    - Remote exploits are more dangerous than local exploits

- What's the result of the attack?
    - A defaced web page
    - Loss of confidential information and customer data
    - Production outage as a result of a DoS?

- How common is the platform?
    - Is it well known within the hacker community?
    - Is it highly publicized?

- Are there tools and scripts available?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

    - If there are, they are more likely to be used by script kiddies than if it requires a high skill level.

- Can it be mitigated?
    - What steps have you taken or can you take to mitigate the risk?
    - Have you patched?
    - Is the associated port blocked at the firewalls/routers?

Additionally, there are commercial tools available that provide automated risk analysis solutions, where value of assets can be assigned and correlated with the risk level of the vulnerability such as ArcSight (http://www.arcsight.com/product_info01.htm),

Challenges

One of the biggest challenges of assigning risk to new vulnerabilities is a lack of information. If an organization does not have documented knowledge of its own assets, network design, defense-in-depth strategies, and processes, they will find it difficult to quickly and accurately assess the risk level of the vulnerability. For the smaller organization this data can be fairly easy to collect and document. However, security teams in large enterprises may find the collection of information frustrating because of the diversity of multiple lines of business, multiple departments having overlapping duties, poor discipline around documentation, lack of resources and lack of proper change control. Companies must budget for 'housekeeping' activities such as asset and change management in order to make these activities effective.

Best Practices

The most prepared companies will face the challenge of risk level assignment by having documented information about their environments and established processes for handling new vulnerabilities. Best practices should include:

- Documented processes for reviewing new vulnerabilities as they are announced and management support behind the team that will handle the function (i.e. CSIRT, Risk Management team, etc.)
- Checklists to assist with consistent risk assignment
- Published risk ratings for vulnerabilities and definitions of those risk ratings (i.e. what does a High risk vulnerability mean to the general user public?)
- Accurate and readily available asset inventories (See Step 1: Asset Inventory) (including the asset owners, and patch levels) and network diagrams
- Established and stringent change management process
- Defense-in-Depth documentation: the CSIRT should have a published "matrix" of each security tool deployed in the organization and their respective controls

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- This matrix should include a list of all security tools, and the potential mitigation that they offer, and where they are physically and logically deployed

These best practices can assist CSIRTs and other security teams to best determine the severity of a new vulnerability within their organization.

Step 4: Vulnerability Assessment

Overview

Vulnerability Assessment (VA) is the process of identifying vulnerable assets. The VA team functions as the 'ethical' hacker and attempts to find and fix vulnerabilities before a malicious hacker does. It is crucial for organizations to identify vulnerable systems quickly and accurately.

Tools

There are many VA tools available for organizations to choose. Several freeware utilities and commercial tools provide varying levels of assessment, stability and scalability. Two of the most commonly used freeware tools are nmap and Nessus. Nmap provides a flexible portscanning solution that can be easily configured to the needs of the user. This tool can be used to quickly map out an unknown network environment and attempt to gain further information about assets. This is helpful in attempting to assess large environments because it is fast and easy to use, and can create a good starting point for further investigations. Nessus takes nmap to the next level by providing vulnerability assessment of hosts. Because Nessus is freeware, some large organizations choose not to deploy it. Nessus is flexible enough that you can write your own vulnerability checks using the Nessus scripting language (nasl). In addition to freeware offerings, there are several commercial tools that are widely used. ISS Internet Scanner, Harris STAT, Foundstone's Foundscan, and eEye's Retina are a few of the more popular offerings. Each of these tools offers various levels of features that an organization may need.

Challenges

As we go through the steps of Vulnerability Management, we begin to see some trends. As with many of the other steps, one of the biggest challenges in Vulnerability Assessment is the understanding of *what* to assess. Companies without an accurate asset inventory will spend time and effort attempting to identify active hosts and their respective Operating Systems. Additionally, VA teams will have to deal with scanners that may or may not provide accurate assessments. False positives will always exist, however, users must decide on what percentage of them is acceptable. Security teams will also need to find a tool that causes minimal disruption to the network. Some vulnerability checks are considered dangerous, because they attempt the exploit. It is wise to do testing of any product that you plan on using to ensure that it will not bring down a server. Security teams may also have to observe change windows for

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

scanning. You should always get permission from management to run scans and use a change control system to cover your activities, just in case you cause an outage. Even with a robust scanning tool, it is challenging to find one that not only provides a decent interface for end users, but also provides enough flexibility to write your own scripts and use it in the way that best fits your needs. Additionally, features like reporting, trending, and remediation tracking are key items to look for.

Best Practices

Performing vulnerability assessments can be a time consuming and tedious process. VA teams can look to others in the security community for best practices and formulate their own from experience. Some things to remember:

- Always start with an asset inventory
    - If you don't have one, make one using nmap to scan your network.
- Get permission and change control to run your scans, in case you cause a network disruption.
- Test new checks in a lab to identify any false positives, false negatives, and potential service disruptions.
- Create custom policies by OS or by industry standard (SANS Top 20, Windows Top 10 Vulnerabilities) and specific to your environment
- Identify what scanning methods and operating procedures are best for your company, and document how you choose to proceed in a standard operating procedure.

Step 5: Reporting and Remediation Tracking

Overview

The 5th step in the Vulnerability Management cycle is reporting and remediation. Effective reporting is critical because without it, management and system administrators will not understand the organization's security posture, what remains unfixed, and who should be held responsible. Reporting also gives management something tangible to associate with the vulnerability and a way to measure successes and failures. Remediation tracking brings Vulnerability Management full circle. As the director of Spire Security, Peter Lindstrom, succinctly states, "Vulnerability remediation's time has come. With companies increasingly at risk from unresolved vulnerabilities identified by assessments, remediation is the key to enabling enterprises to quickly 'cover their assets" (Business Wire). If vulnerable hosts are not tracked to remediation, it seems pointless to even find the vulnerabilities. There are a few tools on the market now that include remediation tracking workflow functionality.

Tools

Most tools provide some level of reporting, even if very basic. The goal for most large organizations, however, is to find a tool with the capability to provide meaningful reporting that can be customized for the audience. CSIRTs should

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

be able to provide high-level dashboard type reports to senior management and detailed host reports to system administrators. Some tools with good reporting functionality include Foundstone's Enterprise Manager (Figure 2) and Latis' Still Secure (Figure 3).

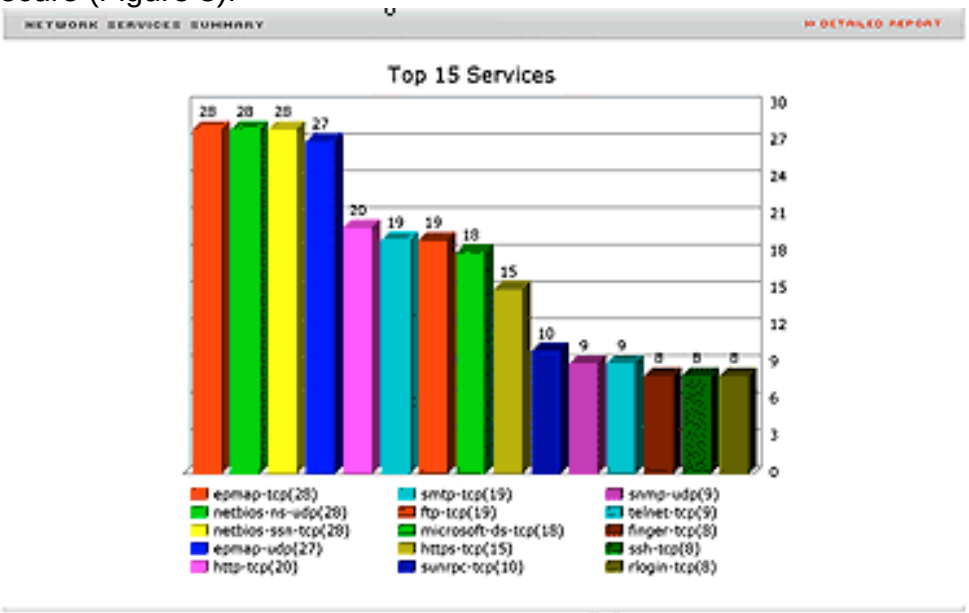

Figure 2 Foundstone Reporting

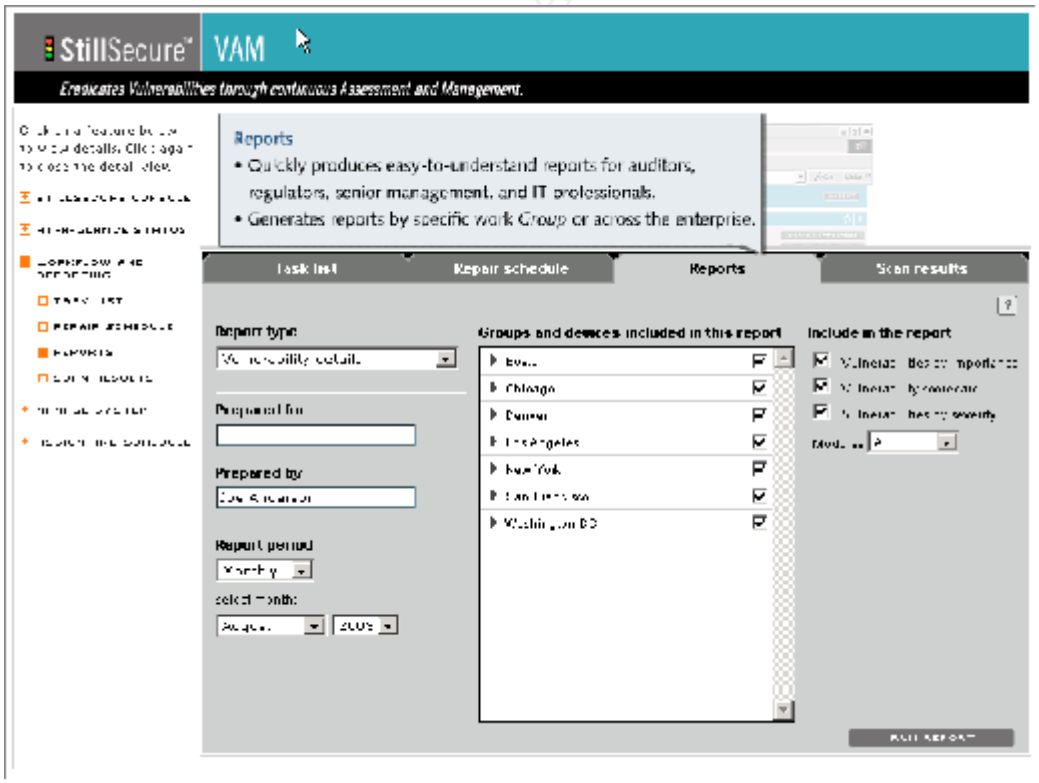

Figure 3 Latis Reporting

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Each of these products provides reporting features that can be customized to the user's needs. Foundstone offers several canned reports including a customizable Executive Dashboard, a long-term trend report, and reports customized for specific regions, operating systems, services, and vulnerabilities. The Still Secure product provides an Executive Status report, vulnerability details, vulnerability frequency and a SANS/FBI Top 20 report. Foundstone and Latis also provide remediation tracking and workflow systems. The Foundstone product allows users to assign vulnerabilities to specific system administrators and track them to remediation via tickets. Latis' Vulnerability Repair Workflow system automatically assigns vulnerabilities to the responsible party, sends notifications when new ones are found, and performs validation scans when the task is marked repaired.

Challenges

The challenges of reporting and remediation tracking are fairly universal. Without the proper information at the beginning of your program, it is difficult to bring vulnerability management full circle. Many organizations, especially those with little or no documentation, will have problems connecting the right people to the right assets that require fixing. Reporting and remediation are also key to holding lines of business and departments accountable for patching and fixing vulnerable hosts. Customized reporting is required to allow organizations to target specific audiences with minimal effort. Remediation efforts can be greatly reduced by following a few best practices.

Best Practices

Because remediation tracking and reporting can become time consuming, organizations can use these best practices to achieve maximum effectiveness.

- Make sure the tool you use has a method of notifying the asset owners that they have vulnerabilities to be fixed. Otherwise, your team may become bogged down with sending out emails or posting results.
- Meet with management and lines of business to agree upon the types of reporting they want to see, and what you'll be able to offer.
- Get management support on remediation timeframes and consequences of not remediating hosts.
- Focus on the highest risk vulnerabilities by ranking them by the vulnerability risk rating and an asset risk rating.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Step 6: Response Planning

While steps 1 through 5 are crucial, they mean nothing if there is no response plan to react to new vulnerabilities. In large enterprises, there may be so many hosts to assess and so little time before an exploit is created for a new vulnerability, it is important to be prepared. For instance, when the Microsoft vulnerability MS03-023 was announced, organizations with response plans (or small networks) could quickly respond and patch their environments. However, any larger organizations without a response plan in place were ambushed before they could effectively patch their networks. MS Blaster worm began spreading in the wild about 26 days after the MS03-026 vulnerability was announced. For those companies on top of their game, this was ample time to work on preventative measures. Others, who did not complete patching in time, experienced network slow downs and outages due to MS Blaster and its variants which cost companies money in resource hours and production capability.

Tools

The best tools for response planning are documentation, education and practice. CSIRTs and security teams that have no documentation of a response plan will be lost when it comes time to react. When the lines of business and core remediation teams are not educated, they may not understand what is expected of them during an incident. And when faced with an emergency situation, teams may forget what they're supposed to do, or who should be performing which functions. Additional resources for response planning can be found in the CERT CSIRT Handbook

Challenges

CSIRT teams will face multiple challenges when attempting to organize a response plan. They may face issues getting the appropriate communications out to the right people and getting the right people focused on the most appropriate tasks. Security managers may also find that holding people accountable for remediation is difficult. Rogue machines, laptops, and remote users will also come to light in an emergency response situation. Often times, in a response situation, teams will incidentally duplicate work. It is the CSIRT that should outline beforehand who will be responsible for specific duties. For example, who will research the vulnerability, which team should perform the network assessment, who can test any scanning tools or patches, which team is the best to create any necessary scripting, and who will handle walking end users through patching. These situations can be avoided if preplanning is done.

Best Practices

CSIRTs should take the lead in vulnerability response. Best practices include:

- Establish a documented, widely published plan that the CSIRT and other critical staff will understand and follow

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- In the event of an incident, establish multiple bridge calls, if necessary, one for CSIRT, one for Technical Staff (S.A.'s, Engineers, Security Staff), and one for End Users to call in for support, to avoid cross-topics.
- Provide quick and accurate information dissemination to technical staff and general user populations.
- Make sure that any relevant help desks are notified and briefed on how to handle specific issues.
- Have critical information at the fingertips of the staff that require it, including up-to-date lists with key contacts from each Line of Business and within security.
- The CSIRT team and the Vulnerability Assessment function should have easy access to any network/infrastructure information to be able to quickly react to enterprise-wide threats.

Conclusion

As vulnerabilities are discovered at an ever increasing rate and exploits are created with record speed, corporations must position themselves to react immediately and effectively to protect themselves. In order to effectively manage vulnerability response and remediation, it is important for security teams to establish their vulnerability management lifecycle. This lifecycle should consist of five steps: creating and managing an asset inventory, managing information flow, assessing the risk of vulnerabilities and assets, assessing the network for vulnerabilities, reporting and remediating vulnerabilities, and planning vulnerability response. Asset inventory is a crucial first step so that a security team knows where to begin assessments and who to contact when there is an issue. CSIRT teams should aim for effective management of information so that the correct information is delivered to audiences in a timely manner. Determining risk levels of new vulnerabilities allows companies to prioritize work and put resources on the most immediate tasks. Network vulnerability assessment allows security teams to identify which hosts are vulnerable to various issues. Reporting and remediation tracking provide management visibility to security issues and accountability for unmitigated risk. Finally, security groups must outline, test, and publish their plan for responding to new high risk vulnerabilities. These steps can help organizations reduce the revenue and resources spent on fighting vulnerabilities in their environment. As Carl Banzhof summarizes in his article "Strategies to Protect against Network Security Vulnerabilities", organizations can "address their current vulnerability exposures and prepare an adequate defense by proactively defining and executing a plan that follows […] best practices and leverages the latest automated technologies that make the plan repeatable" ("Strategies").

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Works Cited

Banzhof, Carl. "Strategies to protect against network security vulnerabilities." Information World 17 Apr. 2003. 23 Sep. 2003. <http://www.computerworld.com/securitytopics/security/story/0,10801,80426,00.html>.

Berg Al. "Feeling Vulnerable?" Information Security Magazine Feb. 2002. 21 Sep. 2003. <http://infosecuritymag.techtarget.com/2002/feb/features_vulnerable.shtml>.

Gregory, Peter. "Is an asset inventory in your company's future?" 22 May 2003. 2 Oct. 2003. <http://www.computerworld.com/securitytopics/security/story/0,10801,81442,00.html>.

Harris STAT. Vulnerability Management. Harris Corporation. 23 Sep. 2003. <http://www.statonline.com/solutions/vuln_mgmt.asp>.

Krutz, Ronald and Vines, Russell Dean. The CISSP Prep Guide. NY, Wiley and Sons, 2001.

Raspberry, John. "What to Maintain." Maintenance Technology. May 2000. PCA Consulting. 23 Sep. 2003. <http://www.pcaconsulting.com/articles/WhatToMaintain.pdf>.

"Spire Security Report Identifies Vulnerability Remediation as Most Effective Solution for Reducing Risk Across the Enterprise." Business Wire 15 Jul. 2003. 1 Oct. 2003. <http://quickstart.clari.net/qs_se/webnews/wed/aj/Btx-citadel-security.RNCN_DIF.html>.

"Symantec: Viruses Are Becoming Faster And More Complex." Information Week 1 Oct 2003. 8 Oct 2003. <http://www.informationweek.com/story/showArticle.jhtml?articleID=15201000>.

West-Brown, Moira J. et. al. Handbook for Computer Security Incident Response Teams (CSIRTS). 2nd ed. Apr. 2003. 15 Aug. 2003. CERT/CC. <http://www.cert.org/archive/pdf/csirt-handbook.pdf>.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced