Vulnerability Management

Joseph Johann

ICTN6823

East Carolina University

Summer 2014

Abstract

With the proliferation of new attack vectors comes the need to be able to identify security vulnerabilities, rate them, and patch them as quickly as possible. This involves a systematic approach to managing this process. In this paper I will define the industry standards for vulnerability management. This includes the methods for identifying vulnerabilities and classifying their risks as well as the individuals involved in the process. I will also define the steps involved in performing a vulnerability assessment and some tools that can facilitate the process. Furthermore I will discuss sources of current vulnerability information and steps that can be taken to protect assets when a patch is not currently available. Finally I will discuss industry regulations that require organizations to have vulnerability assessments performed on a regular basis.

New attacks emerge every day and usually target systems that have known vulnerabilities. Security personnel are in a constant battle to try and stay ahead of the vulnerabilities and keep their systems secure. In order to do this, they need to develop a systematic way of keeping their systems patched as well as developing a method to stay abreast of the latest exploits that are being released. Without managing both sides, a security professional will never be able to defend their systems adequately. With new regulations being passed, it is becoming a requirement to show due diligence when protecting networks. This requires that a vulnerability assessment be performed to identify your asset's vulnerabilities, identify the threats to those assets, analyze the risks, take corrective actions for the threats, and document the results. This cycle of events will be performed usually on a monthly basis as new threats are released. The entire process needs to be managed effectively in order to get effective results that will help the organization stay secure.

The usual trend is for vulnerabilities to be discovered either by the creator of the software or an outsider. The outsider can be a security researcher who discovers the vulnerability through testing also known as a White Hat or a hacker that is actively looking to exploit the software which is also known as a Black Hat. Most reputable security researchers will notify the creator to allow them to fix the issue before going public with it while the hacker will immediately publish or sell exploit code. A zero-day attack consists of a malicious exploit which doesn't have a patch written for it yet. These are the most dangerous threats and rely on additional security measures to protect the assets. Several computer security conferences are held each year where the main intent is to break into systems that have been patched thus discovering new vulnerabilities. Many of these researchers are handsomely rewarded for their efforts. There are organizations such as Microsoft and Adobe that release patches for their vulnerabilities on a set

day each month along with information explaining their details and severities. This allows customers the ability to decide whether the patch should be applied in their environment. The patching of vulnerabilities depends in a large part on the amount of risk the organization is willing to assume. Some organizations choose to avoid the risks by using something else in its place. This isn't always an option. Others accept the risk and don't do anything about it. Another option is to transfer the risk to a third party who then assumes the liability. The most common option is to control the risk by reducing the threat vector and vulnerability exposure. This option requires the most resources but is often the most effective method to employ.

There are several methodologies that can be used to begin a vulnerability assessment. Some people prefer to identify the threats that are commonly known and have been publicly released while others like to perform a vulnerability scan to determine the threats that impact their environment. Either way the end result is to find which vulnerabilities need to be addressed. Security analysts usually perform the scans of the network devices including routers, switches, firewalls, servers, workstations, and printers just to name a few to determine the vulnerabilities in each. This can often be set up on an automated interval. There are several applications that can help to determine vulnerabilities in your systems. The Network Map (NMap) utility is free and can be used to scan assets to determine ports that are listening and then this information can be fed into a script that matches the results against a vulnerability database. NMap scans can achieve good results with less risk of causing havoc to the assets. Another program is Open Vulnerability Assessment System (OpenVAS) which is a freely distributed vulnerability scanner and manager. This utility offers a framework of several services and tools and has a daily updated feed of vulnerabilities from Network Vulnerability Tests. This product can be a great, cost-free solution for organizations looking for a powerful scanner with minimal

costs. One of the leaders in vulnerability scanning is the Nessus program by Tenable Network Security. This was originally a free product until 2005 when it was changed to proprietary. It is used throughout the U.S Department of Defense and by many Fortune 500 companies as a vulnerability, configuration, and compliance scanner. It features high-speed asset discovery, patch and configuration auditing, asset profiling, sensitive data discovery, patch management integration, multi-scanner control, and vulnerability analysis. At a cost of $1500 for a single license, this tool is affordable to all levels of businesses. Finally, one of the most popular vulnerability scanning products is Nexpose by Rapid7. This product has scanning abilities including features such as scheduled scanning and alerting, web application scanning, PCI compliance checking, and integration with Metasploit. The Metasploit application is a penetration testing tool that integrates with Nexpose. While Nexpose discovers the vulnerabilities, Metasploit can be used to attempt to exploit the vulnerabilities to show just how risky they are. The Metasploit application was developed by HD Moore as open source software and was eventually purchased by Rapid7. There are still free open source versions of Metasploit being developed but you will need to purchase a commercial version to integrate with Nexpose. Security teams are usually the personnel responsible for performing the scans. These individuals should be experienced at vulnerability assessments and the software they use. There are often many configurable parameters that can vastly alter the results of your scan. The scanning frequency needs to be determined. Some organizations scan weekly while others scan monthly or quarterly. It really just depends on how often your computer's postures change and the number of assets you are scanning. This process can take up valuable bandwidth especially if performed over a slow WAN link. The time of the scan also needs to be taken into consideration since many users take their computers home at night and would therefore not show

up on the weekly scans. After the scanning is complete you should have a good inventory of your assets along with their associated vulnerabilities.

The 2nd process is to identify the threats that are available. This information can be obtained either through live feeds that go directly into scanning applications or by viewing/downloading them from Internet sites. One of the most popular vulnerability listings is the Common Vulnerabilities and Exposures (CVE) standard which is a dictionary of names for most publicly known IT vulnerabilities. This database is very popular among both private and government organizations and is best viewed through the National Vulnerability Database. Many security organizations follow the latest vulnerabilities being released and try to be the first to release the information on communication channels such as RSS feeds, Twitter, and email listings. As mentioned before, some organizations will release vulnerabilities about their own products on specific days. The live feeds provide the best solution since you don't need to import information or remember to do it each month. The live feeds also give you the fastest results since the existing assets in the vulnerability scanner are automatically matched up with the latest vulnerabilities.

Once the vulnerabilities and threats have been identified, the risk to the organization needs to be determined. Besides security personnel, other IT personnel are usually involved with the evaluation of the risk in discovered vulnerabilities. The impact of the vulnerability to an asset usually requires a product specialist's expertise since the vulnerability often involves the inner workings of the asset. A monthly meeting is usually set up to discuss the latest threats and to determine their risk to the organization. Threats are usually classified as critical, severe, moderate, and low as they relate to the vulnerabilities they affect. Many organizations choose to only patch critical and severe vulnerabilities to reduce the chances of ill effects on the assets.

There are often patches that are not applied due to the issues they can cause with the asset. If that path is taken, it is best to document the reasoning behind it and to determine other controls that are in place to help mitigate the risks. For the patches that are applied, they should be installed on a small group of non-production test computers to see if there are any complications. These computers should have a good cross section of the applications and software installed throughout the network. After successfully testing the patches, a small group of production systems should be chosen to test. These systems are usually within the technology services area where the users are much more technically savvy and can often diagnose any issue that arise. After a successful deployment to this group, a good sample should be taken from different lines of business. The systems chosen should preferably contain standard software for that department as well as a user who is familiar with them and their normal activity. The test users should be told to immediately report back any issues they find. This is process should last about 3-5 days. When this group has successfully been tested, the remainder of the organization should be able to receive the patches although it should still be done in stages so as not to overwhelm departments. It is important to remember that many of the patches cause the systems to reboot so the users need to be made aware of that fact. Also, many organizations patch systems on weekends when users might take their laptops home. It is advisable to instruct those users to manually apply the updates so that they don't fall behind.

After the vulnerabilities have been patched, you will need to document any issues that were discovered. This includes any patches that were unsuccessful or any that couldn't be applied due to compatibility issues with the software. Some major vendors whose software is often incompatible with applications include Adobe's Flash and Reader, Oracle's Java, and Microsoft's .NET framework. It is best to determine the latest versions of these software

packages that are compatible with your line of business (LoB) software and store them with the documentation related to it. Communications with the LoB vendors to determine the latest version of support software is critical. Failure to do so can mean that several versions of patches are not applied thus leaving your environment exposed. The documentation created during these patching cycles should be kept for historical purposes and can also be used to show due diligence to auditors. Although you will probably never achieve 100% patching success it is a best practice to patch all applicable vulnerabilities within 30 days of their release. For the vulnerabilities that cannot be patched, additional steps can be taken to protect the assets. Many times the vulnerable software is obsolete and can simply be uninstalled. This happens a lot when a user installs three web browsers and only one is being patched by the monthly updates. Local firewalls can be installed on some systems which can prevent access to the systems on particular ports or services. Local intrusion protection systems can also detect and stop malicious activity. Antivirus and malware software can also be installed. File integrity monitoring is useful to determine if any changes are made to critical system files. All of these form what is referred to as defense in depth and provide backup protection in case another security measure fails.

Industry regulations also play a part in keeping vulnerabilities patched. The Payment Card Industry Data Security Standard (PCI DSS) requires credit card processors to be able to identify new vulnerabilities in current and new payment applications. They must also be able to verify that they use outside sources for their vulnerability information and that customers are patched in a timely manner. The Gramm-Leach-Bliley Act requires financial institutions to create a comprehensive, written Information Security Program. It requires the institutions to identify possible internal and external threats that could disclose customer information and to test controls, systems, and procedures utilizing an independent 3rd party. The Health Insurance

Portability and Accountability Act (HIPAA) of 1996 emphasizes the protection of the confidentiality, integrity, and availability of electronic protected health information. HIPAA doesn't mandate the use of particular security technologies but instead gives guiding principles for technology choices. HIPAA does require an evaluation and security management of any assets that store, transmit, or create electronic protected health information. With the failure of any of these regulations an organization can face fines, penalties, or even jail time.

Although security management and assessments become more effective the more you do them, there can often be issues that you run into. Goodchild (2013) states that a lack of vision can create issues when performing vulnerability assessments. She recommends brainstorming for ideas on how to best manage vulnerabilities and think like you were going to attack the network yourself. Don't dismiss farfetched ideas too soon. They may be the same ideas that hackers are thinking of. Another point is that getting compliant shouldn't be the main focus of securing your organization. Security and compliance go together but only you know your organization and compliance/regulations are usually just guidelines to get you moving in the right direction. If you have issues with some of the rules you should voice them to the auditors. You should use the audit findings as a baseline for the next set of improvements you make to the network not issues that you didn't uncover. There will always be new requirements coming out that demand more of your security posture. Finally, you should share the findings with the members of your organization or as much as you can. If they don't know the issues you are struggling with you don't ever have a chance of gaining their support and possibly helping with the issues.

There are several areas that can help make a vulnerability assessment easier on you and your staff. First, you should think like someone trying to break into your organization. No one

knows your network better or where the faults lie than the IT staff. Gather information from the experts in each asset area to get their input on the weaknesses in the systems. You should also assign a scope to the vulnerability assessment and determine what testing should be done. If you spend too much time on the vulnerabilities that don't present any risk to the organization you might end up missing one that does. Vulnerability assessment software is great for collecting asset information and the vulnerabilities that exist on them but there also needs to be a human element involved. This involves thinking outside the box and discovering new ways of protecting or eliminating vulnerabilities. By establishing a standard methodology about how you address the vulnerability assessment, you will better be able to manage it. The Open Source Security Testing Methodology Manual (OSSTMM) provides information on establishing a methodology and what should be present. Not all standards fit all organizations so it is sometimes best to take parts of each that best fit your environment. As with all security related functions, having the support of upper management can go a long way in obtaining success in vulnerability management. Make them part of the audience who receives the progress reports from the tests.

There are several resources available to help create a vulnerability management program. The National Institute of Standards and Technology (NIST) has created one of the more popular resources in a document called NIST SP 800-40 which is titled Creating a Patch and Vulnerability Management Program. This document details the creation of a system inventory, the monitoring for vulnerabilities, remediations, and threats, as well as patch and vulnerability management issues. It also discusses the use of security metrics in the process.

There are several reasons to maintain a security vulnerability management program. Compliance is a notable one but standard due diligence should probably be the main factor. The

field of information security was established to protect the information of others from harm just as you would your own information. Being able to manage vulnerabilities is a full time job and it never ends. Compliance only gets more in depth which requires establishing more of a program to manage it. There are several educational organizations which specialize in information security including the SANS Institute, the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC^2). Each provides several certifications related to different aspects of information security. The more knowledge and experience you can gain both in the security field and the general IT field, the better equipped you will be for managing vulnerabilities.

As long as there are individuals who thrive on exploiting weaknesses in information assets, there will always be a need for vulnerability assessments. Those assessments will always need a management system in place to ensure accurate and timely remediation of the issues. With regulatory requirements demanding more and more attention to detail in these processes, organizations have become more dependent on third party vendors to accurately identify risks in their applications as well as on vulnerability assessment programs to report on the security vulnerabilities within networks. Hopefully as the information security industry continues to mature, new more effective ways will be developed to mitigate these issues and reduce the workload currently put on information security professionals.

References

*Zhao, J.J., Truell, A.D., Alexander, M.W., Woosley, S.A. (2011). A Vulnerability Assessment of the U.S. Small Business B2c E-Commerce Network Systems. *The Journal of Research in Business Education*. Vol. 53, No. 1.

*Dinh, T.N., Ying Xuan., Thai, M.T., Pardalos, P.M., Znati, T., On New Approaches of Assessing Network Vulnerability: Hardness and Approximation. *Networking, IEEE/ACM Transactions on*. Vol.20. No.2. pp.609,619, April 2012.

*Chang, E.S., Jain, A.K., Slade, D. M., Tsao, S.L., Managing Cyber Security Vulnerabilities in Large Networks. *Bell Labs Technical Journal*. Vol.4, No.4, pp.252,272, Oct.-Dec. 1999.

*Barrere, M., Badonnel, R., Festor, O. Vulnerability Assessment in Autonomic Networks and Services: A Survey. *Communications Surveys & Tutorials, IEEE*. Vol.16, No.2, pp. 988,1004, Second Quarter 2014.

Goodchild, J. (2013). Security and Vulnerability Assessment: 4 Common Mistakes. Chief Security Officer Magazine. April 2008.

Liu, Simon; Holt, L.; Cheng, B., "A Practical Vulnerability Assessment Program," *IT Professional* , vol.9, no.6, pp.36,42, Nov.-Dec. 2007

Mell, P.; Scarfone, K.; Romanosky, S., "Common Vulnerability Scoring System," *Security & Privacy, IEEE* , vol.4, no.6, pp.85,89, Nov.-Dec. 2006

https://www.qualys.com/docs/hipaa_guide.pdf

http://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

http://www.projectsmart.co.uk/risk-management-options.php

http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0214.pdf