Global Information Assurance Certification Paper

Concepts and Successes in Vulnerability Management

By

Joseph Shimanek

GIAC Security Essentials Certification (GSEC)

Version 1.4b, Option 1

January 19, 2004

Table of Contents

1 Abstract 1
2 Introduction 1
3 A Case for Vulnerability Management 1
3.1 Nimda 2
3.2 SQL Slammer 2
3.3 A Common Problem 2
4 Modes of Addressing Security 3
5 Vulnerability Management is Proactive Security 4
5.1 Inventory 5
5.2 Assess 5
5.3 Mitigate 6
5.4 Report 7
6 Obstacles of Vulnerability Management 7
7 The Approach to Vulnerability Management 8
7.1 Vulnerability Discovery 9
7.1.1 Network-Based Assessments 9
7.1.2 Host-Based Assessments 9
7.2 Prioritization 10
7.2.1 Confidentiality 10
7.2.2 Integrity 10
7.2.3 Availability 11
7.2.4 Setting Priorities 11
8 Conclusion 12
9 Works Cited 13

1 Abstract

Companies that struggle or fail to identify and manage vulnerabilities are plagued with costly security incidents that are the result of realized threats, such as a worm that has already penetrated defenses and is propagating inside of a company's networks. This problem is aggravated when the response to threats is reactive. Implementing a process that will proactively seek, identify, and eliminate vulnerabilities will greatly improve a company's security posture.

The ideal goal is to remove the vulnerabilities before a hacker, worm, or virus can exploit them. The proactive approach to Vulnerability Management first requires the creation and maintenance of a complete and accurate database of computing assets and the vulnerabilities to which they are subject. Next, the vulnerabilities must be prioritized according to potential impact to the business with corrective action taken first on those with greatest importance. The proactive process must be performed frequently to reduce the window of opportunity for new vulnerabilities to be exploited.

2 Introduction

As networks grow, computing capabilities increase, and software functionality expands, hackers are presented with great opportunity for attacking and exploiting holes in the computing infrastructure. This is evident by the widespread virus and worm outbreaks that propagate throughout the Internet and are prevalent today.

Vulnerability is defined as a weakness in an installed computing component or a missing safeguard in that component.[1] *Vulnerability Management* (VM) is a process of discovering and mitigating vulnerabilities before they can be exploited. According to a whitepaper authored at Visionael Corporation, there are three concepts to successful VM: the approach, the technology, and the people.[2] Poorly implementing any of these VM concepts can render the entire VM process ineffective, while a well-defined approach makes VM efficient and successful.

Focusing on the first concept of VM, the approach, this paper examines some recommendations for addressing VM more successfully. First, it identifies a need for VM by examining some recent threats. Second, it describes the need for addressing security proactively. Third, it presents the basic VM process. Finally, it analyzes the approach to identifying and prioritizing vulnerabilities through the assessment.

3 A Case for Vulnerability Management

Worms, viruses and other security threats propagating freely on the Internet and infiltrating companies are helping to emphasize the need for VM. This section briefly examines two worms, *Nimda* and *SQL Slammer*, to illustrate how the lack of implementing VM can have terrible results.

[1] Krutz and Vines, p.17.
[2] Visionael, "Best Practices for Vulnerability Management".

3.1 Nimda

Nimda, named by reversing the word *admin*, was first identified September 18, 2001. It exploits a known vulnerability in Microsoft's Internet Information Server (IIS). This worm propagates itself through various methods, among which, infected web sites and in e-mail attachments are the most common. According the Symantec Security web site, this worm propagates by mailing itself using addresses in the infected system's address book, searches for available network shares, copies itself to vulnerable IIS servers, and infects local and remote files.[3]

Microsoft posted a security bulletin that provided mitigating strategies as well as a patch that removes the vulnerability on June 18, 2001.[4] This patch was available 3 months prior to the worldwide outbreak. Within a couple days after the worldwide outbreak, the worm spread to 130,000 systems and cost companies an estimated $531 million.[5]

This attack was successful due to the large number of systems on the Internet that were vulnerable because many organizations were either slow to implement a recommended patch or did not know to implement it.

3.2 SQL Slammer

The SQL Slammer attack was originally reported on January 25, 2003. SQL Slammer executes code as a result of a buffer overflow due to a flaw in Microsoft SQL Server (MSSQL) and the Microsoft Desktop Engine (MSDE). It actively scans the network for other vulnerable systems, which caused widespread slowness across the Internet.[6]

Microsoft originally reported this vulnerability and issued a patch on October 16, 2002 that fixes the vulnerability exploited by SQL Slammer.[7] This was more than 3 months prior to the worldwide outbreak. The initial estimates of this outbreak placed it at number 9 on the list of all-time most costly attacks, costing between $950 million and $1.2 billion.[8]

Again, this attack was successful due to the large number of systems on the Internet that were vulnerable because many organizations were either slow to implement a recommended patch or did not know to implement it.

3.3 A Common Problem

Nimda and SQL Slammer are just two examples that illustrate a common problem. These threats were only realized on assets that had components (IIS, MSSQL, and MSDE, in this case) that were vulnerable to the attack. Furthermore, patches that

[3] Symantec, "w32.nimda.a@mm".
[4] Microsoft, "Microsoft Security Bulletin MS01-033".
[5] Holbrook, "Nimda: The Cost So Far".
[6] CERT, "CERT Advisory CA-2003-04 MS-SQL Server Worm".
[7] Microsoft, "Microsoft Security Bulletin MS02-061".
[8] Lemos, "Counting the Cost of Slammer".

fixed these vulnerabilities were available before the widespread epidemic. In fact, 3+ months transpired between discovery and worldwide outbreak.

The important point of examining the Nimda and SQL Slammer worms is that proactively identifying vulnerabilities would have identified the problems in IIS, MSSQL, and MSDE before Nimda and SQL Slammer raided the Internet, giving the IT staff time to implement patches. It is also noteworthy that the worms would not have had as many platforms from which to propagate throughout the Internet if companies had proactively identified and repaired the vulnerabilities.

4 Modes of Addressing Security

Companies differ in the way they manage threats. In an online business publication, "The CEO Refresher", Preston G. Smith describes two modes of addressing IT problems: *reactive* (firefighting) and *proactive*.[9] Smith combines the terms, *firefighting* and *reactive* as the same mode. In terms of addressing security, however, they are separate. Expanding upon his idea, there are actually four modes: *firefighting*, *reactive*, *proactive*, and *architecture*.

In the *firefighting* mode one or more vulnerabilities have been exploited. IT administrators (firefighters) are scrambling to pick up the pieces left over after the attack and restore services as fast as possible. Smith explains, "The idea of firefighting is to let a problem fester until it becomes a crisis, and then swoop in and fix it." He further explains that firefighting is popular because of its visibility, so that if the problem is repaired, "the firefighter is the hero."[10] This makes qualifying the value of the IT organization easier, because the work being performed is easily seen and understood.

In the *Reactive* mode, IT administrators are working on stopping and containing an attack that is in progress. Hopefully, damage being caused by the attack is minimized. Much like the firefighting mode, IT administrators are feverishly working on fixing problems that have occurred and impacted the business. Unfortunately, attention is directed at the present attack rather than on identifying other weaknesses that attackers may be actively trying to exploit.

The *Proactive* mode is a good mode under which to operate. It requires a preventative mindset. Smith explains that proactivity is the exercise of taking into account potential problems and taking measures to prevent them from happening.[11] Unfortunately, the work of prevention virtually goes unnoticed. It is difficult to assign value intrinsic to the IT organization that prevents problems that may never be seen. Therefore, the work of prevention is much less glorious.

The *Architecture* mode is a high-value mode under which to operate. This is the scenario where, in a perfect world, developers and architects are building software, computers, and networks that do not have bugs or weaknesses that can be exploited by hackers. Furthermore, this is where IT administrators implement

[9] Smith, "On Being Proactive".
[10] Ibid.
[11] Ibid.

configurations that do not present new weaknesses in the infrastructure. The following graphic illustrates these four ways companies approach security:

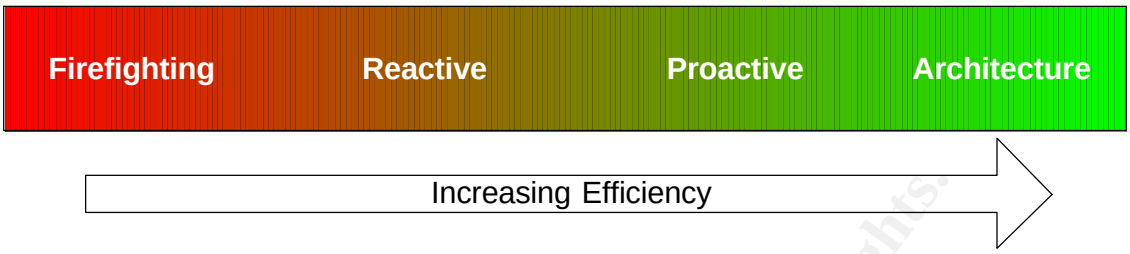

Figure 1 – Methods of Addressing Security

The goal of an IT staff is to move out of the firefighting and reactive modes. Being proactive requires effort. In terms of VM, the approach is vital in moving a company into proactively solving or mitigating threats before they are realized.

5 Vulnerability Management is Proactive Security

Discovering weaknesses and managing them until they are removed or their potential impact is mitigated is Vulnerability Management. Much has been written about the VM process. Authors have presented the steps that comprise VM in different ways; however, they have a common foundation based on the premise that VM is cyclical and consists of four general steps. These steps are: *inventory*, *assess*, *mitigate*, and *report*. The following graphic illustrates these basic steps of the VM cycle:

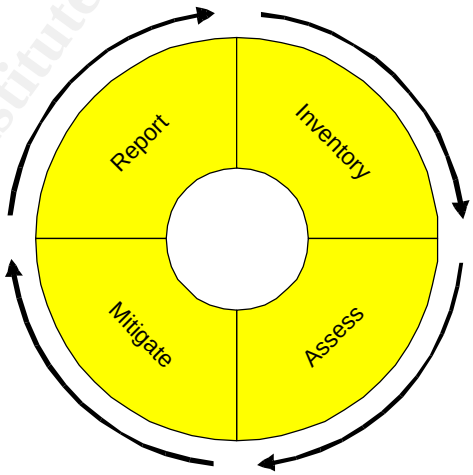

Figure 2 – The Basic Vulnerability Management Cycle

5.1 Inventory

To understand where a company is vulnerable, the IT staff must first know what exists in the computing environment. The first step of the VM process is to identify, or *inventory*, all the components installed in the computing environment. The inventory process must identify the following components:

- A list of the hardware assets; e.g., computers, networks, and other hardware devices.
- A list of the software components; e.g., web servers, operating systems, patches, and other software tools.

There are many tools available to help inventory an infrastructure. It is important to select a tool that is accurate, thorough, and does not negatively impact the normal operations of the business. This is vitally important since the process of taking inventory of the infrastructure must occur frequently and is often very network and disk-intensive.

5.2 Assess

The next step in the VM process is the *assess* phase. This phase focuses on three activities. 1) Build a repository of vulnerability information. 2) Analyze each component from the inventory against the vulnerability repository. 3) Prioritize the list of vulnerable components based on those that pose the greatest risk to the company. The result of these activities is a prioritized list of vulnerable components. The following diagram illustrates this process:

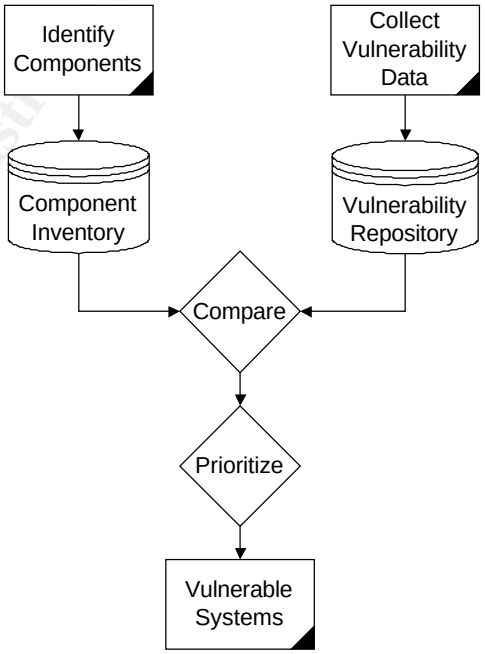

Figure 3 – The Vulnerability Assessment Process

Using the repository of vulnerability data, components (individually or a combination) must be evaluated to determine whether or not they are susceptible to a reported vulnerability. For example, using the information from the vulnerability repository and associating that with the component inventory helps identify systems that are running Windows 2000 with IIS, which are components that are vulnerable to Nimda. However, if the component inventory also indicates that *Microsoft Security Patch Q300972* is installed on some of these systems, then those systems are not vulnerable since the installed patch removes the vulnerability.

This process seems simple enough. Finding information about vulnerabilities is very easy. There are a number of websites that provide detailed information about reported vulnerabilities (there are many more sites that just these):

- http://www.kb.cert.org/vuls
- http://www.securityfocus.com/bid
- http://securityresponse.symantec.com
- http://cve.mitre.org
- http://www.eeye.com/html

In spite of this, compiling a list of vulnerability data can be a huge task depending on the number of vulnerabilities reported. Fortunately, tools exist that build databases of vulnerability information and can perform the assess operation. Generally, they include the most threatening and most current vulnerability information as well as recommendations for mitigation.

There is one additional task that remains in the assess phase. The list of vulnerable systems must be prioritized such that the most critical problems are addressed first. This is where the value of VM starts to be realized. Since there can be many vulnerabilities an organization must address and if IT staff resources are spread thin, then directing IT administrators to the activities that deal with the greatest risk is essential. Solving problems that pose the greatest risk result in the greatest savings for the company.

5.3 Mitigate

The next part of the VM process is where action is taken, in order of highest priority, against vulnerable components. This is called the *mitigate* phase. At this stage, the IT staff will have a prioritized and comprehensive list of vulnerable assets and strategies for mitigating the threats.

There are a number of mitigating strategies. They include, but are not limited to: applying patches that remove the vulnerability, removing or disabling the vulnerable component(s), or eliminating or limiting access to the vulnerable component.

In defining mitigating strategies for a discovered vulnerability, the IT team must verify that the action does not introduce new vulnerabilities, either through untested

patches or configuring changes. The team should work within the bounds of the company's change management policies, regardless of how cumbersome it may be. If there are issues, they need to be communicated back to the management team(s). Furthermore, the status of security activities should be conveyed as well.

5.4 Report

The final step of the VM cycle is to report the activities that have transpired. Reporting provides information to the people who make decisions for the company, including budget for new tools, systems, and headcount. They must see the value VM is to the organization and understand the threats and their impact that could harm the business. As stated earlier, efforts to prevent problems virtually go unnoticed, because they are seldom realized and visible to the masses. Communicating preventative work sheds light on the value of VM. The report will communicate status, issues, and progress of vulnerability assessments as well as highlighting the proactive efforts of the IT staff. A report may include:

- Discovered vulnerabilities
- Mitigation activities
- Issues and obstacles that hinder the progress of the vulnerability assessments
- Qualitative and quantitative cost analyses of realized or potential threats
- Policy violations
- Plans

The report should follow a consistent format and the information contained should be guarded to prevent widespread knowledge about the company's vulnerabilities. The report must be updated and presented regularly.

Companies immune to recent attacks undoubtedly lauded the IT staff's proactive work on identifying and mitigating vulnerabilities before they were realized. The VM report is an excellent vehicle to communicate successes.

6 Obstacles of Vulnerability Management

Vulnerability Management is a simple concept to understand. In practice, however, there are obstacles that complicate it. This section presents 4 obstacles of VM, which are: dynamic security landscapes, complex computing environments, standards that require compliance, and cumbersome change management policies.

The security landscape is highly dynamic. New vulnerabilities are discovered each day. According the CERT Coordination Center, during 2002 there were 4,129 new security vulnerabilities reported. That is an average of more than 11 new vulnerabilities each day! For the first three quarters reported for 2003, there were 2,982 new vulnerabilities reported, which was on pace for results similar to the previous year (fourth quarter metrics for 2003 were not available at the time of the

writing of this paper). Even more telling is the occurrence of realized threats (incidents) reported during those same periods. During the entire 2002-year there were 82,094 security incidents reported. During the first three quarters of 2003, however there were 114,855 incidents reported![12] Keeping information current is extremely taxing for an IT organization that is concerned about vulnerabilities. These metrics demonstrate how easy it is for a company to be simply swamped in data.

While managing vulnerability data can be intimidating, managing the computing environment can be equally frightening. Running a computing environment is a complex operation. There are new computers to install, network configurations to make, new users to add, retiring old hardware and software, removing users that no longer use the computing environment, and the list goes on. With all the changes imposed on a company's infrastructure, problems are bound to emerge. These problems can exhibit themselves as bad configurations and software that has security holes. It is naïve for an IT organization to believe that their computing environment is immune to vulnerabilities and the threat that hackers will exploit them. Supporting this, Andrew S. Tanenbaum stated in his book, Modern Operating Systems that the average operating system "leaks like a sieve."[13]

Knowing that companies are not immune to threats, standards have been adopted that companies must comply to in order to do business. HIPAA, which establishes requirements for the privacy of patient data, is an example of standards the medical industry (and those that do business with them) must comply. There are other standards established by other groups, such as governments, the financial industry, and so forth. Companies often must prove that they comply with standards.

When the company's computing infrastructure is found to be vulnerable or non-compliant to certain security standards, the policies of the company that govern the change management processes need to be flexible enough to allow quick implementation of patches, configuration changes, or whatever is needed to mitigate the problem. Hopefully, these policies do not encumber the process to the point of giving hackers ample opportunity to exploit a vulnerability.

While these obstacles are challenging, they are not insurmountable. It all depends on how the IT organization operates. If VM is a part of the IT operation, then the IT staff is beginning to proactively address security weaknesses before they develop into problems.

7 The Approach to Vulnerability Management

Simply implementing the VM process does not guarantee that the company will operate efficiently. This all depends on the importance placed on the assess phase of the VM cycle. In other words, the approach to VM is as important as the process.

[12] CERT, "CERT/CC Statistics 1988-2003".
[13] Tanenbaum, p.186.

7.1 Vulnerability Discovery

In the *assess* part of the VM cycle, the IT staff focuses on three activities. First, compile a list of potential vulnerabilities. Second, determine which vulnerabilities could impact the business operations by mapping components to known vulnerabilities. Third, prioritize the list of vulnerable components.

Identifying weaknesses in the company's computing infrastructure must occur from two different perspectives. One perspective is from the point-of-view of the network. This is called *network-based assessments*. The other is from the point-of-view of the computer looking at itself. This is called *host-based assessments*.

7.1.1 Network-Based Assessments

Network-based vulnerability assessment provides a quick snapshot of the enterprise. Not only does it provides a quick method of discovering components, but provides a view of vulnerabilities accessible from the network.

Network-based assessment tools operate on a computer that remotely probes or scans network devices, looking for obvious weaknesses. Deeper, more time-consuming testing can be performed, which can actually attempt to exploit discovered components. This is called *penetration testing*. The activities of a network-based assessment are practically identical to that of hackers, except that the reasons drastically differ.

7.1.2 Host-Based Assessments

A host-based assessment provides detailed analysis of installed components and missing safeguards. Host-based assessments operate from the system being analyzed, unlike the network-based assessment, which operates remotely. This means that the host-based assessment occurs using the privileges of a specific user, usually an administrative account, and can find detailed information about components and their vulnerabilities. The difference between host-based assessments versus network-based audits is mostly a matter of privilege.

Using a combination of network and host-based assessments provides the benefits of rapid discovery of vulnerable components and services visible on the network, while being able to analyze each installed component for missing safeguards that may only be visible from the local computer. The data resulting from the audits will be plentiful.

The inventory and assess parts of the VM cycle are the framework on which the entire process functions. If the IT staff does not have an accurate assessment of all installed components and missing safeguards, then the VM cycle is flawed and risks leaving weaknesses exposed to attackers. On the other hand, if the list is comprehensive, then success is within grasp. With the potentially huge list of vulnerable components to address it can be an intimidating task to begin the mitigation process. Therefore, the list of vulnerable components must be prioritized.

7.2 Prioritization

The key to managing vulnerabilities is to prioritize them so that IT administrators can focus on the most critical problems first, the ones that, if realized, would have the greatest impact on the business. Dennis Szerszen explained in "The Next Big Thing", an article about VM that appeared in the September 2003 issue of Information Security Magazine, that companies must assess the value of a vulnerable asset (component) to the business and the likelihood that the vulnerability will be successfully exploited.[14]

To understand the impact an attack perpetrated against a vulnerable component would have, the IT staff must understand the value of what they are protecting about the asset. Shon Harris wrote in his textbook, All-In-One CISSP Certification Exam Guide, that there are three fundamental security objectives: *confidentiality*, *integrity*, and *availability* (CIA). Harris expands this by adding, "All risks, threats, and vulnerabilities are measured in their potential capability to compromise one or all of the CIA principles." [15]

In terms of VM, the principles of confidentiality, integrity, and availability can be used to assign priority to mitigating vulnerable components. This is achieved by applying numeric values for confidentiality, integrity, and availability for each asset.

7.2.1 Confidentiality

Confidentiality is a principle that describes the necessary level of privacy for an asset.[16] For example, publicly disclosing employee names reveals confidential information. However, the value of exposing that information may not be very critical versus publicly revealing credit card numbers from a customer database. Since the confidentiality of credit card numbers may be more important to the business than accidentally publishing a list of employees, the systems that store the credit card numbers would receive a higher confidentiality rating that the systems containing the employee data.

7.2.2 Integrity

The concept of *integrity* addresses how important it is that data (or configurations) stored on an asset is protected from alteration; i.e., accuracy and reliability of the data.[17]

Consider, for example, a situation where two web servers are attacked. If the hacker maliciously modifies the price list of the goods or services published on one of the web servers, the company's e-commerce web server, then this can have disastrous financial results. On the other hand if the hacker defaces the web site on the other web server by writing various slogans on the index page, this may impact the business to a much lesser degree. In both cases, the integrity of each web server

[14] Szerszen, "The Next Big Thing".
[15] Harris, p.62.
[16] ibid, p.63.
[17] ibid, p.63.

was degraded, but which modification impacted the business more? This depends on what is most important to the company; however, they are likely to treat the web server with the price list more critical as it may affect sales. Therefore, that server would receive a higher rating for integrity compared to the other server.

7.2.3 Availability

Availability refers to company assets being accessible to perform their designated function.[18] Interruptions can be caused in many ways, such as Denial of Service attacks (intentional or malicious) or bad configurations (unintentional or accidental). Whatever the cause, IT administrators must determine the affect an outage or unavailability of one or more assets would have to the company. The availability rating of systems that provide services that are critical to the business would be rated higher while systems that are less critical receive a lower availability rating.

7.2.4 Setting Priorities

As vulnerabilities are discovered within the infrastructure, the IT administrators must review the inventory of assets and order them based on priority. The IT team does this by ranking confidentiality, integrity, and availability values for each asset on a scale from 1 to 5 (5 being the most critical). Doing this simplifies determining the most critical vulnerabilities to address first. The scale range by which each asset is rated does not necessarily matter as long as it is consistent for all of the CIA values.

The IT organization must determine actual risk to each affected system's security. The following table, Table 1, outlines how the IT staff can use CIA to determine the priority of critical systems to the business (where the threat, if realized, would impact the company the most):

Description	Confidentiality (1 – 5)	Integrity (1 – 5)	Availability (1 – 5)	Does the Threat Affect This System?
Firewall (Linux)	2	1	5	Y / N
Email Server (Windows 2000)	3.5	3	3	Y / N
e-Commerce Web Server (Apache/Linux)	4	4	5	Y / N
Intranet Web Server (IIS/Windows 2000)	1	2	2	Y / N
Internal File Server (Solaris)	3	4.5	3.5	Y / N

[18] Harris, p.64.

Description	Confidentiality (1 – 5)	Integrity (1 – 5)	Availability (1 – 5)	Does the Threat Affect This System?
Database Server (Oracle/Solaris)	5	5	4	Y / N
Antivirus Server (Windows 2000)	2	4	4.5	Y / N
Database Server (MSSQL)	5	5	4	Y / N

Table 1 – Prioritizing Assets using CIA Values

This table represents several servers. Two servers, in particular, are database servers that have received the highest overall marks for CIA. One server is based on Microsoft SQL Server (MSSQL) while the other is based on Oracle.

What does this mean? Consider the SQL Slammer worm. If a company's intrusion detection software identifies the SQL Slammer worm attempting to scan the network that would put the IT administrators on alert (hopefully). They (or their VM tool) would review the list of critical systems and determine, based on CIA values, the servers to check first. Right away, the Oracle database server can be relegated to the end of the priority list, since SQL Slammer does not affect Oracle. However, each Microsoft-based component will have to be analyzed to see if they are using a local install of MSSQL and MSDE (both vulnerable to SQL Slammer). The systems to be analyzed first would be decided based on the CIA values assigned to the asset.

Rating assets in terms of confidentiality, integrity, and availability and understanding the information about a particular threat, an IT team can quickly prioritize which systems to focus on first. This immediately provides savings for the company since IT administrators are attending to the most important servers to the company, the ones that have the highest impact on the business, and would result in the largest lost if a threat is realized.

8 Conclusion

Companies rely on computers, software, and networks to conduct business. This puts them at risk by exposing weaknesses in the infrastructure that hackers, viruses, and worms can exploit. These threats, when realized, impact the operations of the business.

Viruses and worms have been successfully exploiting vulnerabilities throughout the Internet. Recognizing this problem, companies are seeing the value of proactively identifying the vulnerabilities that plague the infrastructure. Implementing a Vulnerability Management program helps companies proactively address security. These programs are successful when they frequently repeat the 4-step Vulnerability

Management cycle of inventorying the infrastructure, assessing and prioritizing vulnerabilities, mitigating identified vulnerabilities, and reporting results to interested parties. The first two steps of the cycle (inventory and assess) are critical to the entire process. Without an accurate inventory, company assets risk remaining vulnerable. Thorough assessments include prioritizing actions to mitigate the weaknesses.

Prioritization is based on rating assets in terms of confidentiality, integrity, and availability. This ensures that the most pressing security problems are addressed first; the security problems that will impact normal business activities the most. As the company infrastructure continues to grow and since new vulnerabilities are discovered daily, it is vital that the IT staff prioritizes their activities to mitigate each vulnerable component. This makes a company's infrastructure more immune to attacks and results in saving money.

All companies that operate on the internet must assume some risk in order to conduct business. Companies that implement a Vulnerability Management program that focuses on prioritization, reduce their risk imposed by threats.

9 Works Cited

CERT Coordination Center. "CERT Advisory CA-2003-04 MS-SQL Server Worm". January 2003. URL: http://www.cert.org/advisories/CA-2003-04.html (17 December 2003).

CERT Coordination Center. "CERT/CC Statistics 1988-2003". 17 October 2003 URL: http://www.cert.org/stats/cert_stats.html (17 December 2003).

Harris, Shon. All-In-One CISSP Certification Exam Guide. New York: McGraw Hill/Osborne, 2002.

Holbrook, Chris. "Nimda: The Cost So Far". Silicon.com. 20 September 2001 URL: http://www.silicon.com/software/security/0,39024655,11027583,00.htm (05 January 2004).

Krutz, Ronald L. and Vines, Russel Dean. The CISSP Prep Guide. New York, Wiley Computer Publishing, 2001.

Lemos, Robert. "Counting the Cost of Slammer". C/Net News.com. 31 January 2003. URL: http://news.com.com/2100-1001-982955.html (20 December 2004).

Microsoft Corporation. “Microsoft Security Bulletin MS01-033”. TechNet. November 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp (20 December 2003).

Microsoft Corporation. “Microsoft Security Bulletin MS02-061”. TechNet. February 2003 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp (20 December 2003).

Smith, Preston G. “On Being Proactive”. The CEO Refresher. Sept., 2002. URL: http://www.refresher.com/!pgsproactive.html (4 January 2004).

Symantec Corporation. “w32.nimda.a@mm”. Security Response. July 2003. URL: http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html (20 December 2003).

Szerszen, Dennis. “The Next BigThing”. Information Security. Sep. 2003. URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss81_art181,00.html (29 November 2003).

Tanenbaum, Andrew S. Modern Operating Systems. Englewood Cliffs, New Jersey: Prentice Hall, 1992.

Visionael Corp. “Best Practices for Vulnerability Management”. bitpipe IT Research. 1 November 2003. URL: http://www.bitpipe.com/detail/RES/1070381782_523.html (4 January 2004).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS