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.

Network- and Host-Based Vulnerability Assessments: An Introduction to a Cost Effective and Easy to Use Strategy.

In today's business world, vital company information is accessed, stored, and transferred electronically. The security of this information and the systems storing this information are critical to the reputation and prosperity of companies. Therefore, vulnerability assessments of computer systems are routinely employed by businesses to obtain a complete evaluation of the security risks of the systems under investigation. However, the methods for performing vulnerability assessments are varied and cost prohibitive. The p...

Copyright SANS Institute
Author Retains Full Rights

AD

Network- and Host-Based Vulnerability Assessments:
An Introduction to a Cost Effective and Easy to Use Strategy.

GIAC Security Essentials (GSEC) Practical, Version 1.4b, Option #1.

Author: Ragi Guirguis
Date: June 14, 2003

© SANS Institute 2003, Author retains full rights.

As part of the Information Security Reading Room

Table of Contents

Abstract …….. 1
1. Importance of Vulnerability Assessments …….. 1
2. The Vulnerability Assessment Process …… 3
3. Network-based Versus Host-based Vulnerability Assessments …… 3
3.1. Network-based Vulnerability Assessment Tools …….. 4
3.1.1. Nessus Scanning Features …… 4
3.1.2. Architecture Of Nessus ……... 5
3.1.3. Nessus Security Checks …… 5
3.1.4. Nessus Vulnerability Assessment Reports …….. 6
3.2. Host-based Vulnerability Assessment Tools …… 6
3.2.1. SecurityExpressions Scanning Features …… 6
3.2.2. Architecture of SecurityExpressions …… 7
3.2.3. SecurityExpressions Security Checks ……... 7
3.2.4. Repairing the Vulnerabilities …….. 8
3.2.5. Ad-hoc Queries ……... 8
3.2.6. SecurityExpressions Vulnerability Assessment Reports …… 9
4. Vulnerability Assessment Proposal …… 9
4.1. Outlining and Planning …….. 10
4.2. Hardware Requirements …… 11
4.3. Software Requirements …… 11
4.4. Target System Requirements ……... 11
Conclusion …… 12
APPENDIX A – Acronym List …… 13
REFERENCES …… 15

© SANS Institute 2003, Author retains full rights.

Abstract

In today's business world, vital company information is accessed, stored, and transferred electronically. The security of this information and the systems storing this information are critical to the reputation and prosperity of companies. Therefore, vulnerability assessments of computer systems are routinely employed by businesses to obtain a complete evaluation of the security risks of the systems under investigation. However, the methods for performing vulnerability assessments are varied and cost-prohibitive. The purpose of this research was to investigate a convenient, efficient, and cost-effective method for conducting vulnerability assessments. The results show that a successful method employs the strengths of two software packages, Nessus (Nessus Security Scanner) and SecurityExpressions, running from a mobile laptop computer.

1. Importance of Vulnerability Assessments

The use of digital devices has increased drastically in the last two decades. People rely on microchips embedded in everything from watches to PDAs to pacemakers; technology runs our lives. Nowadays, professionals depend on personal computers and businesses require networks to advance in the competing marketplace. And with this technological advancement, the protection of the information stored on these devices becomes ever more vital.

To be competitive in today's market, businesses use a network of computers linked to the Internet to provide their employees with the fastest and most efficient tools to do their jobs. Not only do employees communicate with each other more effectively, they communicate with their clients – clients that can now be reached worldwide. The benefits of the computer network are astounding; the downfalls, however, can be devastating. No longer is a business just concerned with protecting the physical location where its private information is stored. Technology has now made it possible to store that information electronically, and this information can be made available with the touch of a button. However, the loss, disruption, or release of this information to someone outside the company can lead to public embarrassment, loss of clientele, lawsuits, or possibly bankruptcy. According to a survey conducted in 2002 by the CSI and the FBI, threats of attacks on company computer systems are on the rise and are significantly affecting U.S. corporations, resulting in approximately $US 460 million in financial losses for 40% of the survey respondents[1].

In reality, there are two key points of access to a network – through the computer keyboard at the target system or through the virtual world at a remote system. Ironically, the technology that keeps a business competitive can also be the technology of self-destruction. People may try to obtain private information or disrupt/crash the company systems illegitimately either internally (i.e. – working within the company from a local workstation) or from a remote location. Attacks often occur when the system is not password protected or uses weak passwords for authentications, the system is not configured properly, and/or the system holds software packages containing vulnerabilities that only become evident through a series of specific software commands or actions. Typically, attackers exploit well-known vulnerabilities in software packages;

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the majority of these vulnerabilities can be fixed by using vendor patches – executable files that must be downloaded and installed. Fortunately, company systems can be protected against these attacks by installing and using the appropriate security software that identifies what these vulnerabilities are and where they exist.

Information Technology (IT) professionals can use both network- and host-based vulnerability assessments (VAs) to obtain a complete evaluation of the security risks of the system(s) under investigation. Vulnerability assessments identify and suggest fixes for possible vulnerabilities that attackers might exploit in operating systems or in mail, HTTP, and FTP servers. Moreover, they point out which systems are noncompliant with the company security policies. Performing VAs on company systems provide three key pieces of information necessary for improving their security: 1) it is easier to locate which systems are vulnerable, 2) it identifies what services/components are vulnerable, and 3) it suggests the best method for repairing the vulnerabilities (i.e. – it recommends which patch or software version should be used/applied). Performing this procedure on a regular basis allows IT professionals to find and repair possible security vulnerabilities before attackers find and exploit them.

One recent example of a vulnerability that affected many businesses worldwide was the release of the Sapphire worm, also referred to as the Slammer. The worm (a self-replicating program that spreads itself automatically over the network from one computer to the next) exploded onto the Internet, crippling it on January 25th, 2003 by slowing down organizational network traffic, virtually to a halt. This worm resides in the RAM and propagates via UDP Port 1434 exploiting a buffer overrun vulnerability in Microsoft SQL Servers and MSDE 2000 systems that have not applied the patch. Unfortunately not all users of the software installed the patch, which was released by Microsoft on October 22nd, 2002 under Microsoft Security Bulletin MS02-039[2]. This incident alone was estimated to cause between $US 945 million and $US 1.15 billion in damages[3]. If IT professionals had detected this vulnerability and repaired it when the patch became available, this incident could have been avoided.

Attackers are constantly on the prowl and take advantage of companies that are not vigilant with regards to identifying and repairing security weaknesses, whether the reason is budget cuts, low staffing resources, and/or other company issues. Because software packages will never be free of vulnerabilities due to human error, IT professionals must be aware of the potential damage that these programs can induce. In order to keep up with the attackers, all company systems should be up-to-date with the latest service packs (collection of patches), patches (collection of hotfixes), hotfixes (executable files that fix the code which causes a vulnerability), and ensure that they are compliant with company security policies (i.e. – password strength, file permissions, etc.) to minimize the security holes in them. Therefore, it is important to perform regular VA scans to identify security issues and fix them thus eliminating the damage caused by incidences such as the Sapphire worm.

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

2. The Vulnerability Assessment Process

Securing company systems via VAs involves three continuous steps. First, VAs should be preformed on the target system(s). This step also involves an entry being opened on the company's Change Management system or the like (a database system that tracks changes or issues regarding company systems which helps to ensure that they are resolved over time). Secondly, the issues identified by VAs must be reviewed and responsibilities for fixing them must be assigned to the appropriate individuals. Lastly, the individuals assigned to resolve the issues in the previous step must resolve them in the time allotted. These individuals must also be held accountable for following up with their VAs by reporting to management the conclusions of the actions taken. This entire process must be performed periodically to ensure that company systems are secure against attacks.

Individuals assigned to resolve the issues found by the VAs have a few common techniques for resolving these issues. These techniques are based on the need of the services (i.e. – HTTP, FTP, SMTP, etc.) encompassing the vulnerabilities, and the possibility of them being fixed without affecting the stability of the system or other applications running on it. In other words, if the services causing the vulnerabilities are not needed on the target system, then they must be disabled. On the other hand, if the services causing the vulnerabilities are needed on the target system, then these services must either be upgraded or patched to resolve the vulnerabilities. Conversely, if the patches pose stability risks and/or non-functioning applications on the target system, then management must be informed of the potential risks that these systems present to the organizational network. In that case, management must decide whether the security risk is acceptable or not and must provide written confirmation that it has been informed of the security issues[4]. For example, if a VA indicates that the target system has a Microsoft SQL Server installed with a buffer overrun vulnerability – allowing Sapphire worm attacks – then the individual responsible for resolving this issue has to decide if the SQL server is essential. If the SQL server is not essential, then it must be uninstalled or disabled from the services list. However, if the SQL server is necessary, then this individual has to install the Microsoft patch and test to see if the system is still functioning as desired. If the system is functioning as desired, then another VA should be performed to ensure that the vulnerability has been fixed. Otherwise, if after applying the patch the system is not functioning as desired, then the appropriate management personal must be notified about this issue. If management decides to keep the SQL server, then it must provide a sign-off documentation indicating that it agrees for this system to be kept on the organizational network and that it understands the consequences of it being vulnerable to the Sapphire worm.

3. Network-based Versus Host-based Vulnerability Assessments

Network-based VAs are accomplished through the use of network scanners. Network scanners are able to detect open ports, identify services running on these ports, simulate attacks, and reveal possible vulnerabilities associated with these services. On the other hand, host-based VAs are carried out through host-based scanners. Host-based scanners are able to recognize system-level vulnerabilities including incorrect file

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

permissions, registry permissions, and software configuration errors. Furthermore, they ensure that target systems are compliant with the predefined company security policies. Unlike network-based scanners, an administrator account or an agent is required to be on the target system to allow for the system-level access required.

3.1. Network-based Vulnerability Assessment Tools

Several network-based VA scanners are available on the market today, including SAINT Corporation's SAINT™4, Internet Security Systems' (ISS) Internet Scanner® 7.0, and Nessus Security Scanner (Nessus – latest version 2.0.6a). All three VA scanners are recognized by IT professionals for their scanning speed, configurability, and robustness. Both SAINT™4 and Internet Scanner® 7.0 come with a very high price tag. However, Nessus is an open source VA tool and hence is free. Most IT professionals are skeptical about open source products because they do not provide the same capabilities available in commercial tools. This may be true for some, but this does not apply to Nessus due to the fact that it is as powerful as some of the best commercial VA scanners[5]. In addition, it was the winner of the 2002 Information Security Magazine Excellence award (March 2002), winner of the Network Computing's 7th Annual Well-Connected Award in the Vulnerability Assessment Tool category (May 2001), and was selected as one of the "Top 50 Security Tools" by nmap's users (June 2000)[6]. Furthermore, products such as Vigilante's SecureScan trust the quality and capabilities of Nessus; they combine it with their in-house developed tools and other commercial tools to provide businesses with VA services[7]. For these reasons, the Nessus software package is featured here.

3.1.1. Nessus Scanning Features

Nessus scans target systems based on host name, IP address, subnet, or IP address range. It initially investigates the system by connecting to the target system and simulating various application protocols. For example, if Nessus is checking for web server vulnerabilities, it then pretends to be a web browser by sending HTTP protocols. Similarly, if it was testing for Windows fileserver vulnerabilities, it then pretends to be a Windows client by sending SMB protocols[8]. Next, it does not assume that the services of the target system will be running on their proper IANA assigned port. For example, if the target system is running web servers on ports 21, 80, and 8080, then Nessus will detect that ports 21, 80, and 8080 are open. In spite of this, it will not assume that the target system is running an FTP server on port 21 and web servers on ports 80 and 8080. It will detect that web servers are running on all three ports and will perform the appropriate security checks against them.

All Nessus scans are performed efficiently by sharing the information of each security check with other security checks performed thereafter. For example, if the target system's FTP server does not offer anonymous logins, then anonymous-related security checks will not be performed[6]. This feature permits Nessus to complete VA scans faster, allowing IT professionals to scan an unlimited number of hosts simultaneously.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

However, the number of hosts being scanned at one time will be limited by the power of the hosting system running the Nessus server component.

Some security checks will slow down network traffic, or even cause target systems to crash. For that reason, Nessus has included a "Safe Checks" option that bases the VA only on service banners instead of actually trying to exploit the vulnerabilities. Using this option does not always provide reliable results, but it is useful under certain conditions, especially when scanning production servers that a company cannot afford to have off-line.

3.1.2. Architecture Of Nessus

Nessus features port scanning, OS detection, information gathering, vulnerability scanning, and attack simulation. For some of these features, Nessus uses other open source security tools instead of developing them from scratch. For example, it uses Nmap for OS identification and advanced port scanning, Nikto and Whisker to provide specific Web server and CGI attacks and tests, and Hydra to provide brute force attacks for common services (i.e. – telnet, web, POP3). Nessus must be running under 'root' in order for it to start these programs[6].

Nessus performs all of its functions via client-server architecture. This architecture allows a central server to perform all the attacks on target systems while the client provides a GUI that connects to the server presenting the scanning options and a facility to view and save the results. The server side is POSIX based (i.e. – GNU/Linux, FreeBSD, Solaris, NetBSD, etc.), while the client can either run on MS Windows or Unix (X Windows) platforms. Moreover, Nessus provides the flexibility of using command-line to communicate with the scanning engine to execute VA scans. Furthermore, if OpenSSL is available on the system hosting the Nessus server component, then it will be used to encrypt the communication between the client and server, and for testing SSL services on the target system(s).

3.1.3. Nessus Security Checks

As of June 14th, 2003, Nessus was capable of performing a total of 1,698 security checks, which is competitive with the numbers of high-end commercial network-based vulnerability scanners[9]. Also, Nessus maintains an up-to-date security check database with new security checks added on a daily basis. These security checks are divided into 24 different families covering important security issues including backdoors, denial of service, CGI abuse, gaining shell access remotely, gaining root access remotely, and SMTP problems.

The security checks are written as external plugins, which allows the flexibility of adding new plugins without the need for recompiling the Nessus engine. All plugins are written in a scripting language called NASL. Nessus makes it simpler for IT professionals to write custom security checks and attacks using either NASL or C programming language (C programming language is familiar to the majority of the IT community).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.1.4. Nessus Vulnerability Assessment Reports

Nessus network VA reports are important because they provide a complete overview of the target system's vulnerabilities. They include a list of open ports detected, services associated with these ports, and vulnerabilities associated with these services along with suggested fixes with related CVE identifications and BID identifications to help provide more information about the identified vulnerabilities. Each problem detected by Nessus is categorized into one of four severity levels: high, low, medium, or informational. Furthermore, Nessus categorizes high severity problems as security holes, while medium/low severity problems as warnings and finally informational problems as open ports.

The assessment results can either be exported into different formats such as NSR, Extended NSR, SQL command File, CSV, ASCII text, HTML, XML, and Adobe PDF files, or stored in a central MySQL database. However, only the NSR and Extended NSR formats can be imported by any Nessus client which is not possible with the other formats. Furthermore, the HTML report formats provide two reporting options (available only on POSIX). The first option is a straightforward VA report; the second option provides the same report in addition to pie charts and graphs representing the number and types of vulnerabilities found on the target system. Charts and graphs are significant due to the fact that they are used as visuals aids to emphasize the impact of vulnerabilities on company systems.

3.2. Host-based Vulnerability Assessment Tools

IT professionals use host-based VA tools to standardize security polices and manage system securities including password rules, user rights, policies, file permissions, and registry settings across the organizational network. This process is possible through host-based tools such as Internet Security Systems' (ISS) System Scanner™, Symantec's Enterprise Security Manager™ 5.5, and Pedestal Software Inc.'s SecurityExpressions. All three tools are capable of performing the same basic functions; however, they differ in the way they are deployed throughout the network. Both ISS System Scanner™ and Symantec Enterprise Security Manager™ consume quite some time to deploy because they require an agent to be installed on all target systems to provide the system-level access needed to perform the VA. On the other hand, SecurityExpressions is agent-less and therefore is an easier product for deploying, auditing, and enforcing company security policies and system securities. Another primary feature is that it takes only a few minutes to install and is ready to use straight out of the packaging. It is no surprise that such a powerful tool is being used by more than 1,700 organizations worldwide covering virtually every major industry sector[10]. For these reasons, the SecurityExpressions software package is featured below.

3.2.1. SecurityExpressions Scanning Features

SecurityExpressions VA scans support the MS Windows platforms, Sun Solaris, Linux, IBM AIX, HP-UX, and key Microsoft applications, including Internet Explorer, SQL

As part of the Information Security Reading Room

Server, Outlook, and Office. In addition, it ensures that Microsoft applications and Solaris platforms are up-to-date with the latest patches and hotfixes.

The methods of scanning are quick and virtually trouble free; the software scans target systems using their host names or IP addresses. It has the ability to simultaneously scan and fix up to 200 target systems at once by running separate sub-tasks independently and waiting for network availability. To simplify the scanning process, it offers three different approaches for IT professionals to determine possible target systems on their network: 1) it can use "ping discovery" to send ICMP Echo request packets to systems within an IP range and logs a list of all systems that respond with acknowledgement, 2) it can use the Microsoft's Network Neighborhood utility to list all the domains available and the members within each domain, and 3) it can use LDAP queries to extract machines lists from Active Directory or other LDAP-compliant directories. Moreover, IT professionals can add target systems manually or export them from another list to create a customized target system list. This type of list can be used in batch scans or scheduled batch scans.

3.2.2. Architecture of SecurityExpressions

Unlike most host-based VA scanners, SecurityExpressions utilizes an agent-less architecture. The agent-less architecture is possible because it utilizes MS Windows Networking (NetBIOS - ports 135, 137, 138, 139, 445 and RPC - port 593) to scan and fix target MS Windows systems[11]. Through MS Windows Networking, SecurityExpressions confirms that the currently logged on user can access security functions, including modifying registry keys and altering file permission on target MS Windows systems. However, if the currently logged on user does not have the proper access rights to perform these functions, then a user ID and password must be specified to be used on the target system. On the other hand, the agent-less architecture is possible when scanning target Unix systems through Secure Shell (SSH - port 22), along with an administrative user ID and password on the target system. However, if SSH service is not available on the target Unix system(s), SecurityExpressions supports agents (port 9002) to be installed to provide the necessary access.

The agent-less architecture saves IT professionals valuable time since agents are not required to be installed on each target system under investigation. Also, it saves the time needed for IT professionals to explain to IT system administrators as to why an agent must be installed on their systems.

3.2.3. SecurityExpressions Security Checks

SecurityExpressions performs security checks using a set of security rules outlined in predefined policies. Policies are defined based on the type of OS and the role of the target system (i.e. – sever, workstation, etc.) in the business environment. All polices are written in SIF files to define all rules. These files follow standard INI file format that is used by MS Windows OS and other programs to initialize and/or set parameters. By

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

using this common format, SecurityExpressions provides a lot of flexibility for IT professionals to easily modify and customize polices to meet company polices. This process is simpler to perform through a GUI wizard, which is also provided. Moreover, these SIF files can be further extended and customized using Javascript, Perl, or VBScript code[12].

In case companies do not have their own predefined security policies, SecurityExpressions allows them to test their target systems' security settings against the industries best security practice guidelines. These guidelines are included in a number of SIF files such as SANS Securing Windows NT Security Step-by-Step Guide; NIST Windows 2000 Security Guidelines; NSA Windows 2000 and XP Security Guidelines; Internet Explorer Compliance Checks, MS Word 2000 and Excel 2000 Macros Security settings, sample rules for use with Unix systems, Lockdown for Linux, Lockdown for Solaris (any version 5-9), and recommended security patches for Sun Solaris. Furthermore, SecurityExpressions includes SIF files that scans for missing MS hotfixes and patches, reports weak and easily guessable passwords on Windows systems, and audits installed applications on Windows systems flagging ones that do not meet company standards. In addition to this, Pedestal Software Inc. also provides an online SIF library, which provides up-to-date policy files for all platforms and selected MS applications.

3.2.4. Repairing the Vulnerabilities

Unlike network-based vulnerability scanners, SecurityExpressions repairs the majority of the problems it finds on the target system(s). It repairs the problems that it finds by changing registry settings, executing scripts, or installing patches and hotfixes. This feature empowers IT professionals to quickly lock down company systems from a central location and also ensures that consistent and uniform security settings exist in the organizational network. Fixing and patching the target system(s) is made easy with a click of a button. This process can either be executed one item at a time or in a batch job to automatically correct all deviations. SecurityExpressions retains a complete list of every change made on each target system. In the case of the target system(s) failing due to the changes, it also provides the option for returning to the original settings. This activity is also logged for future reference so that an IT professional can undue their previous changes.

3.2.5. Ad-hoc Queries

SecurityExpressions empowers IT professionals with an option for performing quick queries of specific security settings on target MS Windows systems. The MS Windows Network Neighborhood browser provides a list of systems to scan with the option to add a single system, multiple systems, or domains on which to perform the query. A set of default built-in expressions to find files, groups, registry keys, and users that match specific criteria are built in SecurityExpressions. However, it also provides the flexibility for IT professionals to customize their own expressions using a GUI interface forming a C-like syntax with functions and Boolean operators.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2.6. SecurityExpressions VA Reports

SecurityExpressions offers 13 different types of report packages including: "Host Details" presenting the details of the rules evaluated including compliance and risk of the system scanned, "Compliance List - Problem Sort" providing a list of hosts and their compliance sorted by the number of problems each host comprises, and "Overall Trends" illustrating with the use of charts the historical trends of policy compliance over time. All of these reports can either be exported into MS Word, Excel, HTML, and Adobe PDF formats, or stored in any ODBC compliant database (i.e. – SQL Server, Oracle, DB2, etc.). For each report, SecurityExpressions provides the option of including the type of rule status - NOT OK (the setting is not correct), INFO (issue should be considered), OK (correct setting), and ERROR (an error occurred while evaluating the rule). In particular, these reports provide a complete overview of the possible security weakness and risks that are present on company systems.

4. Vulnerability Assessment Proposal

IT Security professionals face many issues that hinder their efficiency, such as low departmental budgets, low staffing resources and obstacles due to network design (i.e. – firewall implementations). These obstructions can make the process of implementing VAs very difficult to perform and maintain on a regular basis. As a result, I have designed a strategy that overcomes these issues and the obstacles encountered. My approach provides a simple and cost-effective method for performing regular network- and host-based VAs to ensure that all company systems are free of vulnerabilities and are in-line with the business security policies.

To accomplish the goal of securing company systems, it is essential that both network- and host-based VAs to be preformed at the same time. Since network- and host-based VAs do not execute the same security checks on target systems, they do not provide the same VA results. An IT professional cannot depend on only one of these VAs to secure company systems. Both VAs must be used together to gain a comprehensive view of the security risks of all company systems.

This process is best achieved through the use of Nessus and SecurityExpressions software packages on a laptop computer. The laptop makes the VA scanners mobile and therefore provides a solution that is not affected by the limitations encountered by network design (i.e. – internal firewalls). This solution is also efficient and cost-effective because it allows IT security departments to have the required in-house tools to conduct frequent VAs on all company systems.

To illustrate the effectiveness of this solution, take the common example of an internal firewall that exists between the target system(s) and the VA scanners. The presence of this firewall produces several problems. First, the network-based VA scanner will be scanning against the firewall and will provide inaccurate results. The firewall will prevent direct access to all open ports of the target system(s), because it will not have

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

the same ports open as the target system(s). For instance, if ports 80, 21, 22, and 1433 are open on the target system and only ports 80 and 22 are open on the firewall, the network VA scanner will only detect that ports 80 and 22 are open on the target system. It will not detect ports 21 and 1433 because they are blocked by the firewall. As a result, IT professionals can potentially miss extremely critical vulnerabilities of the services running on these ports. Secondly, most host-based vulnerability scanners use ports 5600, 9002, 22, 137, 138, 139, 445, and/or 593 to communicate with the target system(s). If the firewall does not allow communication through these ports, then the host-based VA scanner will not be able to connect to the target system(s). However, since my strategy allows both network- and host-based VAs to be launched from a mobile laptop, IT professionals can directly connect to the target system(s), bypassing any internal firewalls and performing more accurate VAs on them.

Contrary to my proposal, an argument may be made for the permanent placement of the server component of the VA scanner on the same side of the firewall as the target system(s), given that the communication between the VA scanner server component and the client component is allowed through the firewall. However, in most companies this would not work due to the fact that one VA scanner server component will not be able to reach all target systems because of other internal firewall implementations. Thus the same obstacle of network design is encountered. Moreover, placing several VA scanner server components on dedicated systems throughout the organizational network would be logistically difficult with respect to upgrades and system management. Furthermore, if the systems hosting the VA scanner server components are not secure, then internal attackers could possibly hijack the hosting system allowing them to find which company systems are vulnerable and exploit the vulnerabilities found.

My strategy of running both network- and host-based VAs from a laptop overcomes these hurdles. Not only does it include both client and server components of the VA scanner, it eliminates the extra costs of dedicated systems that would be needed for hosting the server component of the VA scanner. As well, since the laptop is not always connected to the network, it eliminates any possibilities of it being hijacked. However, the method for deploying this flexible VA system in any business environment requires careful planning and use of the correct hardware/software combinations.

4.1. Outlining and Planning

In order to deploy a smooth and successful VA system in the business environment, it is imperative for the IT security department to have all related policies and procedures well documented. These documents should state the principles outlining the actions taken when planning and performing all aspects of the network- and host-based VAs each and every time they are conducted. As previously discussed, a Change Management system has to be developed for tracking down issues found by the VAs and to ensure that the issues have been resolved. Without the documentation and the Change Management system in place, there will be no guarantees that the VA process will be carried out consistently, or even carried out at all [4].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.2. Hardware Requirements

Only a few pieces of key hardware are required to get this strategy up and running. First, a laptop, minimum of Pentium III-800 with a minimum of 512M bytes of RAM, is required to install all the software components. The more powerful the laptop, the faster the scanning process will be and the less time it will take the individual in charge of the VAs to audit the target system(s); an average laptop fitting these requirements would cost about $US 600. Second, either a switch and CAT5 cables (approximately $US 60) or a cross over cable (approximately $US 15) must be purchased in order to run VAs on new company system(s) before they are deployed on the network. However, a switch is more ideal if more than one target system needs to be scanned.

4.3. Software Requirements

In order to install the VA scanners, both MS Windows and Linux operating systems must be installed on the laptop first. To simplify and speed up the VA process, both operating systems must coexist on one partition instead of setting up dual partitions. A combination that I have proven works is the Vmware™ Workstation 4 with MS Windows 2000 Professional with Service Pack 3 (5.0.2195) as the host OS, and Red Hat 8.0 as the guest OS. I hardened both operating systems before I installed any other applications and I did not install any firewall software on the laptop as it sometimes interferes with the VA process. On the host OS (e.g. – Windows 2000), SecurityExpressions must be installed along with NessusWX (Nessus MS Windows client). Finally, on the guest OS (e.g. – Red Hat), Nessus must also be installed.

Using this strategy, the only software that must be purchased is the MS Windows OS (approximately $US 320), Vmware™ Workstation (approximately $US 299), and SecurityExpressions, with licenses starting at $US 495 per server and $US 30 per workstation. The other software packages – Red Hat, Nessus, and NessusWX – are open source codes and will not cost a dime.

4.4. Target System Requirements

Nessus and SecurityExpressions need specific requirements of the target systems in order for them to provide accurate VAs. Nessus can scan target systems as long as they are powered and connected to the same network, the ping service is enabled, all required services are running, and no firewall is present. Similarly, SecurityExpressions can scan target systems as long as they are powered and connected to the same network, and no firewall is present. However, it also needs the currently logged-on user to have the correct access rights on the target systems or an administrative user ID and password on them, NetBIOS enabled on MS Windows systems, and OpenSSH installed on Unix based systems. When the requirements for the target system are followed, IT professionals will not encounter any difficulties or obstacles during the VA scanning process.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. Conclusion

Ensuring that company systems are secure and free of vulnerabilities is essential to a business's continued development and growth. Arming IT professionals with the tools and the education to identify and repair the system's vulnerabilities is the best method for securing against attacks. Unfortunately, IT security is a dynamic process in an organizational environment and IT professionals must be ever vigilant. Regular network- and host-based vulnerability assessments of company systems are needed to ensure that these systems are continually free of vulnerabilities and that they are compliant with the business security policies. Therefore, my vulnerability assessment strategy will empower companies to secure and maintain their systems both efficiently and cost-effectively.

© SANS Institute 2003, Author retains full rights.

APPENDIX A – Acronym List

ASCII	American Standard Code for Information Interchange
BID	Bugtraq ID
CGI	Common Gateway Interface
CSI	Computer Security Institute
CSV	Comma Separated Values
CVE	Common Vulnerabilities and Exposures
DB2	Database 2
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
GUI	Graphical User Interface
GNU	GNU's not UNIX
HP-UX	Hewlett Packard -Unix
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
IBM-AIX	International Business Machines – Advanced Interactive eXecutive
ICMP	Internet Control Message Protocol
INI	Initialization
IP	Internet Protocol
ISS	Internet Security Systems
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MS	Microsoft
MSDE	Microsoft SQL Server Desktop Engine
NASL	Nessus Attack Scripting Language
NetBIOS	Network Basic Input Output System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSR	Nessus Scan Report
ODBC	Open DataBase Connectivity
OS	Operating System
PDA	Personal Digital Assistant
PDF	Portable Document Format
POP3	Post Office Protocol V.3
POSIX	Portable Operating System Interface for UNIX
RAM	Random Access Memory
RPC	Remote Procedure Call
SANS	SysAdmin, Audit, Network, Security
SIF	Security Information File

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

SMB	Server/Session Message Block
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
UDP	User Datagram Protocol
VA	Vulnerability Assessment
XML	Extensible Markup Language

© SANS Institute 2003, Author retains full rights.

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

REFERENCES:

[1] Richardson, Robert. "CSI/FBI 2002 Computer Crime and Security Survey." April 7th, 2002. Computer Security Institute. URL: http://www.gocsi.com/press/20020407.html (June 14th, 2003)

[2] ADVISOR NETWORK. "Protect Your Machines Against the W32.Slammer Worm." January 29th, 2003. (Doc # 11819) URL: http://dotnetadvisor.net/doc/11819 (June 14th, 2003)

[3] Surmacz, Jon. "METRICS: 20,000 Digital Attacks Hit in January." February 20th, 2003. CSO Online. URL: http://www.csoonline.com.au/index.php?taxid=14&id=1806476717&e=1 (June 14th, 2003)

[4] Boyce, Robert. "Vulnerability Assessments: The Pro-active Steps to Secure Your Organization." July 12th, 2001. SANS Reading Room. URL: http://www.sans.org/rr/threats/steps.php (June 14th, 2003)

[5] Andress, Mandy. "Network scanners pinpoint problems." February 4th, 2002. NetworkWorlFusion. URL: http://www.nwfusion.com/reviews/2002/0204bgrev.html (June 14th, 2003)

[6] Deraison, Ranuad. "Nessus Data Sheet." February 26th, 2003. Nessus. URL: http://www.nessus.org/doc/datasheet.pdf (June 14th, 2003)

[7] Andress, Mandy. "Vulnerability-assessment services on the rise." February 4th, 2002. NetworkWorlFusion. URL: http://www.nwfusion.com/reviews/2002/0204bgside.html (June 14th, 2003)

[8] Van Den Berg, Richard and Van Der Kooij, Hugo. "Nessus F.A.Q." January 11th, 2002. Nessus. URL: http://www.nessus.org/doc/faq.html (June 14th, 2003)

[9] Nessus. "Nessus Plugins families." 2003. URL: http://cgi.nessus.org/plugins/dump.php3?viewby=family (June 14th, 2003)

[10] Pedestal Software Inc. "Customers." PedestalSoftware.Com URL: http://www.pedestalsoftware.com/customers/ (June 14th, 2003)

[11] Kessler, Gary. "Test Center - SecurityExpressions". February 2002. Information Security Magazine. URL: http://www.infosecuritymag.com/2002/feb/testcenter.shtml (June 14th, 2003)

[12] Kessler, Gary. "SecurityExpressions: Centralized Policy Security Management for Windows NT and Windows 2000 ". November 2001. GaryKessler.net. URL: http://www.garykessler.net/library/securityexpressions.html (June 14th, 2003)

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

Last Updated: June 19th, 2013

Upcoming SANS Training

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

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**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**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 Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**