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.

Demystifying security tools: Should I use commercial or freeware?

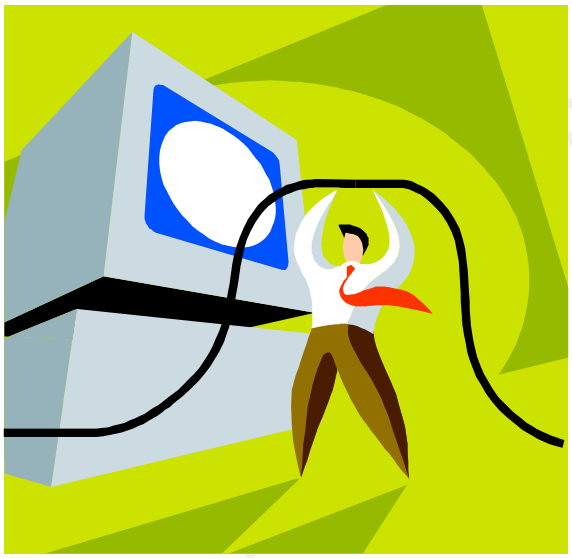
As network security concepts are becoming more advanced, so are the tools used to detect, prevent, and repair security breaches. Many network administrators are unaware of what tools to use, and whether or not to use freeware, commercial, or a combination of both. Determining which security tools to use in the defense against unauthorized access can be intimidating. One realizes that all security tools are not created equal and an "all-in-one" tool does not exist. In this paper, I will touch upon why all network admini...

Copyright SANS Institute

Author Retains Full Rights

AD

Demystifying security tools
Should I use commercial or freeware?



Sang Jin Han
GSEC Practical ver. 1.4b
Option 1

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

Table of Contents

I.0 **Abstract**.....3

2.0 **Baseline security principles**.....4

a. Know thy system
b. Defense in depth
c. Prevention is a must but detection is ideal

3.0 **Using security tools to perform vulnerability assessments on your network** 4

d. Internal assessments
- Identify critical assets via Risk Assessments
- Methodology
- Freeware tools overview
- Commercial tools overview

b. External assessments
- Methodology
- Freeware tools overview
- Commercial tools overview

4.0 **Conclusion**.....14

5.0 **Appendix A - References**.....16

© SANS Institute 2003, Author retains full rights

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

Demystifying security tools
Should I use commercial or freeware?

I.0 Abstract

Security practices within corporations of all sizes tend to be at insufficient priority levels due to numerous reasons. Besides the somewhat excusable reasons such as insufficient funding and unavailable personnel, a growing trend of ignorance is spreading across network administrators leaving them unprepared against hacker attacks. As security concepts are becoming more advanced, so are the tools used to detect, prevent, and repair security breaches. As a result, I notice many network administrators are unaware of what to look for, what tools to use to help identify issues, and whether or not to use freeware, commercial, or the combination of both.

Determining which security tools to use in the defense against unauthorized access can be intimidating. The amount of tools out there are so extensive, you may be left asking which tools should I use? One realization in the topic of security tools is that all security tools are not created equal and an “all-in-one” tool does not exist. With this I must express a disclaimer. The tools and methodology I touch upon here are based on personal opinion and should not be utilized without researching its use to see if it fits your environment. However, I can comfortably say the tools and methodology I talk about are from leading-leading sources. In this paper, I will touch upon why all network administrators need to incorporate security tool usage into their daily practices to help secure their environment. Security tools not only assist in providing defense in depth against unauthorized users but also provides an automated means to identifying security issues; a job that would otherwise be extremely time intensive and prone to human error. In addition, this paper will identify what tools to use in performing vulnerability assessments in various scenarios to give network administrators an idea of what security holes a hacker would most likely target. Since security is not simply running tools against hosts, this paper will also walk you through the methodology used to conduct vulnerability assessments along with the tools used for each step. The idea is to demystify security tools; both commercial and freeware, to show these concepts are not intimidating and imperative they be incorporated as best practices in network administration.

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

2.0 Baseline security principles

In my experience as a security consultant, I've come across a few statements that have become the baseline foundations of my security principles. "Know thy system", "Defense in depth", and "Prevention is a must but detection is ideal" are a few principles I instill no matter what kind of work I perform / recommend and apply to all aspects across the security gambit. "Know thy system" simply says a system administrator should fully know each system in depth to what function it serves, what services and ports are open, and what the level / likelihood of risk is of being compromised. Furthermore, "Defense in depth" talks about how numerous defense mechanisms should be in place (i.e. properly configured routers, firewalls, and intrusion detection systems) to protect a network from unauthorized access by not relying on one security measure but rather multiple to further complicate an attackers attempts. And finally, "Prevention is a must but detection is ideal" talks about how devises such as routers and firewalls *must* be in place to prevent unauthorized access but devises such as intrusion detection systems or log monitoring *ideally* should be in place to detect an unauthorized user if a breach occurs. Understanding these concepts will assist in securing an environment and help mitigate the risk of your network being compromised. Using these principles in conjunction with automated tools and a proven methodology will further harden your environment to acceptable levels of risk. Remember, the goal isn't achieving 100% security since that's impossible, but rather establishing a level of security that will help mitigate the risks.

3.0 Using security tools to perform vulnerability assessments on your network

Securing an environment can be approached in different ways. One of the most common methods to securing an environment is going through a pre-defined checklist or step procedure commonly found by Microsoft or organizations such as the SANS institute. These guides are a great source of information, however; never should be implemented step-by-step since they are meant to be general recommendations and not specific to your organization.

Another method to securing an environment is to perform a vulnerability assessment to identify where the gaps are that need to be addressed. One of the advantages in conducting a vulnerability assessment is the ability to naturally assign priority levels to each issue by assigning a low, medium, or high value. This way, when the assessment is complete, you will be able to prioritize which vulnerability issues need to be resolved immediately and which ones can withstand a comfortable margin of time before being dealt with.

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

With the concept of "defense in depth" in mind, performing either of the above will work but incorporating both practices into one would work even better. Many times I've seen administrators follow a step-by-step procedural guide to secure their environment and then go back and perform a vulnerability assessment to see what was missed or what needs to be hardened further. I feel as though this method is the most optimal since not only will it provide valuable information but will also give you the ability to "know thy system" in the process. With this, let's take a look at the methodology to performing vulnerability assessments and the tools needed to help facilitate the process.

Internal assessments

When performing vulnerability assessments on a network, it is important to approach it with a two-phased perspective, internal and external. Computer systems with internal IP addresses that are normally inaccessible from the internet are going to have different issues then systems that are publicly available. This not only means there will be different vulnerabilities but the approach, or methodology, will also be different. While going through the methodologies, you will notice not all aspects can be performed with an automated tool so I will limit the details on them to stay within the scope of this paper. Let's take a deeper look into each one.

Internal vulnerability assessments

The first step to an internal vulnerability assessment is to conduct an upfront risk assessment to identify the critical assets, the sensitive data they house, and the likelihood of system compromise. Once your critical assets are identified, you can narrow your vulnerability assessments to start with the most critical servers and address the remaining systems as you go. More often, the level of data sensitivity will determine if an asset is critical or not. For example, with the new HIPAA (Health Insurance Portability and Accountability Act) regulations governing health care organizations, any system containing any form of patient data will most likely escalate the asset to critical levels.

Task	Review Activity	Description	Tools
Risk Assessment	Conduct facilitated discussions with key IT and management personnel Create a prioritized list of identified risks utilizing a low, medium, and high ranking scale	Identify key business and security risks facing the IT environment.	N/A

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

Task	Review Activity	Description	Tools
	Create a high-level plan for assessing each area of risk Analysis and report		

Once the target hosts have been identified through the risk assessment, we can now begin the process of going through the framework of an internal security assessment. As you can see from the following matrix, many of the items apart of an internal vulnerability assessment cannot be accomplished with an automated tool. Even though each step is critical in assessing an environment's security posture, I will limit the scope of this paper to activities that have automated tools available; in this case being host-based server testing.

Task	Review Activity	Description
Internal Vulnerability Assessment	Host-based server testing Network-based server testing Firewall review Router review VPN review Intrusion detection system review Network architecture review Review security settings of standard workstation image Review of security administration procedures Assess the strength of physical access controls Analysis and report	Utilize host-based and network-based testing onsite to help identify vulnerabilities in Internal systems. Review network architecture, IT security administration procedures, and workstation security settings.

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

Host-based vulnerability scanners

Host-based vulnerability tools will identify the target operating system's configuration settings and compare them to industry leading best practices to identify the gaps. Any setting below the tool's recommended level will come back as noncompliant and flag it as an issue. Host-based scanners will typically scan for configuration settings in the following categories:

Typical policy checks for host-based scanners	
• Account integrity	• Network Integrity
• Backup Integrity	• Object Integrity
• Disk Quota	• OS Patches
• Encrypted File System	• Password Strength
• File Attributes	• Registry
• File Watch	• Startup Files
• Login Parameters	• System Auditing

Automated tools to perform configuration checks on these categories are available in commercial versions and in freeware but freeware options have limited functionality. Performing internal vulnerability assessments are probably the only time I would recommend using a commercial-grade tool over freeware because a comprehensive solution does not exist in freeware format. You might be able to get away with using numerous freeware tools but the quality and efficiency just isn't worth the effort. Another option is to develop custom scripts to pull configuration settings from your operating system and compare the settings to industry leading sources manually; however, this takes a lot of time and know-how. These custom scripts can be found on the internet but approach them with caution since you don't know who wrote it and what it looks for.

There are obviously numerous companies that make host-based vulnerability scanners but to keep this paper within acceptable limits, I will cover one product in depth and list the others I've had experience with.

Symantec ESM (commercial)

Symantec's Enterprise Security Manager (ESM) is one of industry's leading products for automated security assessment scanning. It does a great job scanning a host operating system to see if its configuration settings are compliant with the industry leading ISO 17799 regulations. ESM can perform assessments on numerous operating systems including, Windows, NetWare, and Unix/Linux.

ESM runs on a manager/agent architecture where a host computer has the ESM manager installed and an agent installed on all target machines under review. The manager is the application that actually initiates the scan whereas the agent

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

collects all the data from the operating system and sends it back to the manager. The manager not only is responsible for initiating the scan but also processes and analyzes the data collected by the agent.

ESM is a great tool because it gives an in-depth view of the target operating system's configuration settings and which ones are noncompliant. It's reporting tool is one of the best I've seen because it's easy to read, gives you a description of the vulnerability, a risk rating, and how to fix the problem. Furthermore, one of the most powerful features of ESM is the ability to create custom policy checks so a system administrator can customize the scans around their environment. The power and effectiveness of ESM makes it a necessity in every organization and apart of everybody's security toolkit.

Along with ESM, other vendors have similar security assessment scanners worth noting from Bindview and Pentasafe.

Custom scripts (commercial / freeware)

An alternative to running manager/agent type host-based vulnerability scanners are custom scripts. Many administrators do not like to install agents on target servers with the fear of interrupting services so an option might be to run custom scripts to pull configuration settings and manually comparing them to industry leading sources to identify gaps. This would be an acceptable option; however, this requires a deep technical ability to not only write the script but also ensure the script is pulling all the critical data from target machines. If you do not have the technical know-how to write custom scripts but prefer to run them over a manager/agent installation, a company called Velosecure (www.velosecure.com) offers custom scripts for sale.

Apart from any internal vulnerability assessment, running only a host-based scanner typically is not enough. Host-based scanners primarily detect non-compliant settings but most likely will not detect mis-configurations or application vulnerabilities. As a result, it is necessary to also run a network based vulnerability scanner internally to see what internal vulnerabilities exist that may be exploitable by unauthorized internal users. With this, let's take a closer look at network-based vulnerability scanners.

Network-based vulnerability scanners

Network-based vulnerability scanning simply means a scan can be initiated from a host machine targeted at an IP address or a range of IP addresses without the need of an agent installation. Host-based vulnerability scanners typically do not focus on system configuration settings but rather mis-configurations or application vulnerabilities. These scanners will try and determine whether or not an authorized user can break in or misuse the system in any way. The great thing about network-based vulnerability scanners is that it can be used from an internal or external perspective. If used externally, it can identify security holes

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

an outside hacker could exploit in order to gain access. If used internally, it can identify security holes an internal unauthorized user could exploit in order to gain access. With the growing number disgruntle employee attacks (i.e. fired system administrators) securing an environment internally is becoming a serious concern. With this, let's take a look at a few network-based vulnerability scanners.

Nessus (freeware)

Nessus, a Linux tool, by far is arguably one of the best all around network-based vulnerability scanners available. Nessus, an open source utility, is a freeware tool that excels in scanning time, flexibility, reporting, comprehensiveness, and customizability. Due to its open source classification, individuals from all over the internet community write vulnerability plug-in code and submit it to Nessus to be included. Not only does this benefit the individual who discovered and wrote the plug-in code but also allows Nessus to have the most up to date and comprehensive vulnerability database around. Nessus follows a low, medium, high, and critical prioritization scheme allowing system administrators address the most severe issues first and the others as follow. One of the gaps to Nessus however is its large number of false-positives; but then again, I'd be impressed if someone showed me a vulnerability scanner that doesn't yield a high number of false positives. In my opinion, Nessus is a must have tool and should be apart of everyone's security toolkit.

ISS Internet Scanner (commercial)

ISS Internet Scanner is also a great network-based vulnerability scanner that performs the same functions as Nessus; however, Nessus is a commercial tool and can be fairly costly to license. Many of my clients will hire us to perform periodic ISS vulnerability scans because it costs too much for their organization to fully own a licensed copy of ISS. One of the positives to ISS is its reporting capabilities, producing a professional easy to follow report written for the business mind. Unlike Nessus where its findings at times seem like are written by 5th graders, ISS produces wording that rarely needs touching up before being released to clients. With this, you may ask why even bother with ISS since Nessus seems to be just as good if not better. Well I agree. I think Nessus is an all around better tool and I wouldn't take any other tool over Nessus. However, it's hard to justify your credibility to clients if you don't have at lease one commercial-grade scanner available. As far as I'm concerned, if you're going to use a vulnerability scanner internally, I think Nessus would be the logical and cheaper choice.

Password auditing tools

With all this talk about host-based and network-based vulnerability scanners, what good is patching up your security holes if you don't have strong passwords to protect your environment in the first place? The absolute first level of security should be implementing an effective password policy over your environment, not

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

only at the server level but also at the user level. If strong passwords are not properly implemented containing a combination of alpha-numeric passwords containing at lease 6 characters in length, then it's just a matter of time before passwords are cracked, allowing total ownership of your system by unauthorized users. Not to mention other critical password policies such as password history, length, age, and expiration, if these are not set to industry leading best practices then the level of risk of an incident increases. With this, a periodic password audit would help mitigate and lower the level of risk.

John the ripper (freeware)
One of my favorite Windows and UNIX password cracking tools is John the ripper, not only because it's free but also because of its effectiveness. John by default will perform a dictionary attack but will also use its own tricks by attaching common characters to the beginning/end of the username and trying those combinations as potential passwords. John also has a brute force option which utilizes all the characters as possible password matches. John is a powerful tool but does not have the ability to decipher if a password is case sensitive or not. In other words, John might be able to crack a password of "edhph" but will not be able to determine if the real password is "edhph", "EdHph", or any other case-sensitive variation. This gap is not an issue with Windows since Windows is a case-insensitive operating system but you can see why this would be an issue in UNIX. Although, I still wouldn't trade John in for any other freeware password cracker.

LC4 (commercial)
LC4, by @stake, is one of the best Windows password auditing tools I have ever come across. It's one of the fastest tools I've use but also one of the most powerful. LC4 gives you numerous options of retrieving encrypted passwords including retrieving them from a local machine, remote machine, from an NT 4.0 emergency repair disk, or by sniffing the local network. LC4 performs four different auditing methods, allowing the administrator to choose depending on its environment or scope. A quick password audit checks for simple passwords that can typical be found in a dictionary. This can be very useful when ran as a preliminary audit to see where your environment stands. Next LC4 offers a common password audit which not only checks for simple passwords typical found in a dictionary but also goes a step further by checking common modifications to dictionary words. And finally, a strong password audit which contains the audit methods of the previous two but also performs a brute force attack that attempts all combinations of standard letters and numbers. If this doesn't satisfy your needs, you can also choose a custom option where you can select a hybrid attack which includes symbols as well as numbers and letters. LC4 is by far one of the most powerful tools ever and a critical asset to any security professional.

When you look at your environment from a security perspective you'll soon realize how many points of risk or weaknesses can be exposed for exploitation

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

from an attacker. A hacker can compromise your network because of a flaw in network architecture or some sort of misconfiguration in your routers and firewalls. However, if an attacker is able to bypass your network architecture, routers, firewalls, or intrusion detection systems, then having your servers hardened makes it just that much tougher for an attacker to get in. The point to this game of security is to make it as tough as you can for an attacker to gain acccess. In my experience, I have never seen a system that has been impenetrable because giving enough time, a hole or vulnerability can be found and exploited to gain access. Security is not about achieving 100% security (since that is impossible) but rather mitigating the risk by putting in place enough defenses that will defend against the time factor. With this, let's take a look at an external vulnerability assessment to help gain a perspective of securing your internal network from unwanted guests.

External Assessments

Conducting an external assessment is just as important then an internal one if not more. Implementing security measures from the external perspective will help identify the vulnerabilities an outside attacker will try to exploit in order to gain unauthorized access. In the game of hacking, the ultimate goal for any hacker is to get root or administrator level access yielding full and totally control over the compromised machine. Once a machine is taken over, a hacker can do anything he/she wants from using it as a data stored (i.e. turning it into a file share to distribute music, movies, porn, etc.) to stealing sensitive private information. You can imagine the repercussions your company would endure if a hacker broke into your systems and stole customer information, credit card numbers, or even sensitive financial data.

Conducting an external assessment is critical to every organization large or small. Any company with publicly accessible computer system such as mail servers or web servers needs to be aware of their external presence. You might be thinking, well I only have a web server publicly available and it contains static information that I don't care if gets compromised. Well in this case the company doesn't care about the web site's content but how about the system's resources (hard drive space, CPU power, etc), website defacement, internal connections to backend databases, or even having a hacker use that machine to attack other machines on the internet. You see, looking at the problem from multiple perspectives shows the importance of securing your external presence no matter how large or small your organization is. With this, this section will go through a few measures to help identify security vulnerabilities an external hacker would try to use in order to gain unauthorized access.

Host detection

One of the first tasks a hacker will perform is some sort of host detection process to identify live hosts in a network. If an attack is directed towards your company,

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

an attacker will try to identify the IP blocks your company owns simply by going to websites such as www.arin.net and typing in your company name. With the IP blocks identified, a hacker will run a series of PingSweeps on the specified range to see which hosts respond back to TCP and/or ICMP ping requests. If a host response back to these types of pings, then an attacker knows a system is publicly available. Another method to identify live hosts is to scan using an SNMP sweep which is effective when system administrators turn TCP and/or ICMP off to prevent pings from occurring. Once hosts have been identified using one of the methods above, the next logical step is to perform port scanning on these hosts to see which services are running. Open ports identified through port scanning typically become the basis of attacks on known vulnerable services such as the http web service, port 80. Let's take a look at a few automated port scanning tools.

Port scanning

Port scanning is one of the easiest measures to perform that yield a great amount of information. In the beginning of this paper I spoke about the concept of "know thy system" where one for the first keys to this concept is to know what ports are open and if there is a business need for that service to be running. When hackers formulate attacks against hosts, they typically target open ports that are know to be more vulnerable then others. For example, hosts running telnet, ftp, or http raise more serious security risks then hosts that have those disabled or filtered from the internet. In addition, certain default installations of the Windows operating system will install by default a web server and NetBIOS. If a publicly available host has an operating system installed with these services without anybody knowing, serious risks can be exposed to your environment. With this, performing periodic port scans on your network is a great way to know what your systems are running and confirm or deny the use of these services.

Nmap (freeware)

Nmap is one of the fastest port scanning tools with multiple uses. Not only can it be used as a traditional port scanning utility but also does OS identification. Nmap can also identify what type of packets filters/firewalls are in use. Nmap is truly effective to a hacker because it has different modes of performing port scans that can evade the detection from intrusion detection systems. Nmap is one of the most popular freeware port scanners available mainly because of its speed, flexibility, portability, and ease of use. Nmap is also a tool that should be apart of everyone's security toolbox.

Solar Winds (commercial)

Solar Winds is a commercial suite of tools bundling a series of effective tools that do network discovery, tools for Cisco routers, fault and performance monitoring, IP address management, and other miscellaneous tools. While Solar Winds has many useful uses it also has tools in its network discovery suite that can perform host identification and port scanning tasks. While you can find multiple freeware

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

tools to perform identical tasks, Solar Winds gives you everything and more in a consolidated suite. As you can see, Solar Winds gives you many additional tools to help manage your network and its performance but if you're needs are limited to this paper, I believe a compilation of freeware tools is enough.

Banner grabbing

Once hosts have been identified and ports scans have been completed, the next step before formulating attacks is to identify what application and its version is running on an open service. This can be done using numerous freeware tools including What's Running (freeware) and netcat (freeware). These tools have the ability to connect to a host machine on a specified port number and retrieve the banner information which typically includes the application maker (i.e. Microsoft, Apache, etc), the version of the running service, and any other information that may assist a hacker in his/her attacks. For example, connecting to an IP address on port 80 (http web service) might yield the host is running Microsoft's IIS version 4.0. This is critical because certain application versions have serious known vulnerabilities if they have not been patched up. Performing banner grabbing on your hosts is an important step to see what information is divulged to potential malicious users. Precautions can been take by altering the banner information to yielding null or misleading information but this step needs to be taken first to fully know thy system.

Network-based vulnerability scanning

Earlier in this paper I spoke about network-based vulnerability scanning using the open source tool Nessus. Without going into more detail about this tool, hackers will often use a network-based vulnerability scanner on a host from the internet to help identify exploitable vulnerabilities. Utilizing this tool against your publicly available hosts will make you more aware of the existing vulnerabilities and also let you see what a hacker would see. This amount of valuable information is critical because you can take what you've learned and apply the appropriate security measures to further secure your environment. In addition, it will pick up any security holes that were missed when you conducted your host-based vulnerability scanning internally. Typically, network-based vulnerability scanning tools such as Nessus will scan a host and try to identifying security vulnerabilities in the following areas:

Typical network-based scanning categories
Sendmail/SMTP security weaknesses, Susceptibility to brute force attacks, Insecure TFTP and FTP implementations, NetBIOS / SMB vulnerabilities, RPC service vulnerabilities, HTTP / CGI vulnerabilities, NIS weaknesses, and

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

Typical network-based scanning categories
IP spoofing / sequence prediction, denial of service and many other attacks. Network and protocol spoofing checks, Source Routed rlogin, rsh and telnet checks, RIP and ARP spoofing checks, IP Forwarding check, Exhaustive DNS checking IP fragmentation, fragmentation and forwarding checks, Internal based addresses check, ICMP netmask and timestamp check, MBONE packet encapsulation check, APPLETALK IP, and IPX encapsulation checks, Reserved bit and Odd protocol checks, Source porting via TCP and UDP checks, TCP and UDP ports filter and Exhaustive ports checks, Custom filter check, Zero length TCP and IP options filter checks, Oversized packet check, and Post-EOL TCP and IP options checks.

Conducting periodic security assessments against your environment from a holistic approach will provide a level of risk that's manageable but also more acceptable. Performing these assessments on a periodic basis not only is best practice but also reasonable in terms of man power and time since tasks can be performed with simple automated tools. It provides you with a wealth of information about your network environment from a non-compliance standpoint but also from the hacker's view. The best thing about these vulnerability assessments is how easy these automated tools are to use, giving you very little reason why you shouldn't implemented this practice into your security strategy immediately. It's a question of are you comfortable with the level of risk without having something similar apart of your security policies and procedures.

4.0 Conclusion

Simply put, the goal of this paper was to show how easy it is to incorporate the use of automated tools and vulnerability assessments into your security practice by making you more aware of the process holistically. This by no means is meant to be a focused framework but rather a high-level foundation to be used as a baseline standard to be built upon and personalized towards your environment. By following the guidelines set forth in this paper you will be achieving the three baseline principles to security, which are (1) Know thy system, (2) Defense in depth, and (3) Prevention is a must but detection is idea.

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

Following these three principles can only help further secure your environment and help mitigate the risk. In addition, by providing effective inexpensive automated tools, the excuse of cost is no longer a factor and should be active within your organization.

Upon review of this paper you might be left asking yourself so which tools should I use? None of the tools in this paper should be used as a single solution to your needs. In other words, don't just use nmap to do port scans; rather use multiple port scanning tools to verify results or gather information one scanner doesn't produce. Use the tools I've outlined in this paper as a foundation and test other similar tools to see which yield the best results for your environment. The idea to tool usage is to utilize a set of tools that's "best of breed" meaning utilizing a compilation of tools that best meet your needs.

In my experience I've seen organizations that cannot adopt the policies I've talked about in this paper for numerous reasons. Some organization's security policy restricts the use of open source applications or maybe there's not budget to purchase somewhat expensive commercial tools. While these reasons are absolutely valid, it's still unacceptable not to perform some variation of what I propose. Considering this, there are managed services your organization can purchase where a 3rd party firm will perform periodic (usually quarterly) vulnerability scans and provide you with a report as a deliverable. This will yield similar results while staying with any limitations your organization has towards open source tools.

To this end, security is an ever changing topic with new vulnerabilities and more sophisticated attacks coming out on a daily basis. Having a dynamic and scalable security policy in your organization is step one in a series of procedures that need to be in place in order to achieve a manageable level of risk you're comfortable dealing with. The topics covered in this paper are achievable with the benefit of time and cost on its side. In many instances, security vulnerabilities are a matter of one's unawareness and can be avoided or properly managed as long as you are equipped with good information and a set of best of breed tools.

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

5.0 Appendix A - References

1. Scambrary, Joel. McClure, Stuart. Kurtz, George. (2001) **Hacking Exposed Second Edition.** Osborne / McGraw-Hill.

2. SANS Institute (2002) **1.1 SANS Security Essentials I: Networking Concepts.** The SANS Institute.

3. Armstrong, Illena. Condon, Ron. "Vulnerability Testing - Keeping a tight ship." February 2003. http://www.scmagazine.com/artframe_art_feature2.html

4. Taschek, John. "White Hat Tools Turn IT Administrators Into White Hat Hackers." February 11, 2002. http://www.eweek.com/article2/0,3959,35320,00.asp

5. Piepers, Eric. "Cost-effective Information Security (Information Security from a business perspective)." June 6, 2001. http://www.sans.org/rr/audit/cost-effective.php

6. Coffee, Peter. "Security Roundtable." March 25, 2002. http://www.eweek.com/article2/0,3959,43769,00.asp

7. Disabatino, Jennifer. "Multiple Web sites defaced in hacking spree." February 16, 2001. http://archive.infoworld.com/articles/hn/xml/01/02/16/010216hnspree.xml

8. Radcliff, Deborah. "Calculating e-risk." February 12, 2001. http://www.itworld.com/Man/3872/CWSTO57529/

9. Shipley, Greg. "The High Price of Vulnerability." February 19, 2001. http://www.networkcomputing.com/1204/1204colshipley.html

10. AZZARA, CAREY. "QUANTIFYING INFOSECURITY." September 2001. http://www.infosecuritymag.com/articles/september01/columns_secmarket.shtml

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

Last Updated: February 11th, 2016

Upcoming SANS Training

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

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced