Global Information Assurance Certification Paper

Me? Vulnerable?
An Overview of Self-Vulnerability Assessment Scans

Tom Shimp
SANS Security Essentials GSEC Practical Assignment Version 1.3
March 2002

All businesses have vulnerabilities. For example, a retail outlet has the constant threat of theft. In order to prevent that threat, retail outlets have many different protections such as in store security personnel, closed circuit television monitoring and recording, theft alarm devices installed directly on merchandise, and more. Despite those factors, there are still thieves that successfully get around the system. To prevent further loss, many retailers employ people whose job is to seek out new threats and deterrents to such thefts, while they pose as regular shoppers and shoplifters.

In the same manner, any corporation with computer network systems also has continual threats, many of them are known and published, and many of them have a preventative means to keep them from causing loss or harm. More and more companies are installing firewalls to protect their assets and information. While this is a positive and proactive step, far too many companies feel "safe" and leave their network far too vulnerable beyond the firewall. Peter Loshin makes a noteworthy statement in an article he wrote for Boardwatch Magazine, "A firewall can't filter if an attacker crashes it, and it can't tell you about its own weaknesses [1]." So what is the answer? Like so many other questions in life, there may not be a one simple, clear-cut answer.

We are going to look at a step-by-step plan to complete a comprehensive Vulnerability Assessment of any business or enterprise because if you aren't attacking your own network and identifying its weaknesses, someone else will be glad to do it for you. The steps we are going to go through are these:

1. Determine exactly what it is that you are protecting and the acceptable risks for your company.
2. Present analysis of your protection assessment to management and obtain the proper written permission to execute the Vulnerability Scan.
3. Research and evaluate different vendors and products to determine which one(s) are best suited for the results you are after.
4. Test the product(s) chosen to complete your Vulnerability Scan in a controlled laboratory environment without exposing your entire network to the product.
5. Train personnel that will be completing the actual scan on proper procedures and guidelines as well as on the software itself.
6. Check software links for updates that will ensure that it is scanning for the latest vulnerabilities prior to your network scan.
7. Inform users involved with equipment that is being "scanned" to prevent being mistaken for actual attacks.
8. Execute the scan, making sure that it is monitored throughout the entire process and can be stopped if necessary.
9. Inform users involved with equipment that is being "scanned" when the scan is over so they can be alert.
10. Analyze data generated by the scan and verify its accuracy.
11. Address all serious vulnerabilities immediately and completely.

12. Compare scan results with prior scans and create a database to examine continual or recurring issues.
13. Assign members of the risk management team to examine, address, and correct vulnerabilities that are deemed necessary and manageable.
14. Report findings to management and users as deemed appropriate to develop a better understanding of security vulnerabilities.
15. Step One – Begin again, the threats are continual and must be reviewed on a regular basis.

Early one evening, my sixteen-year-old stepson asked me to show him how to "hack" his own e-mail using SubSeven so he could "see how his friends were doing it." Red flags immediately went up and I knew that what my son really wanted to know was how to get into others' e-mail, and that it wasn't a wise idea. While I explained to him what was wrong with the e-mail attacks, even when done in good playful spirits, I realized that I did not know how to do what he was asking myself. I also knew that if he wanted to, he could easily find his own answers on the Internet. In that split second, a greater insight revealed itself; the thought and the realization came to me abruptly, "If I don't know how hackers do 'it', how am I protecting against 'it' as a computer security specialist?" Sure, we have a well-configured proxy firewall, a network-based intrusion detection system, and so on, but since it is connected to the outside, it still has vulnerabilities!

"Hundreds of new vulnerabilities are being discovered annually, dozens of new patches are being released monthly, and thousands of systems are already behind the security eight ball. Compounding matters, when opening your perimeter for consumers and business partners, system-level security becomes even more critical as it forces an increase in exposure points. Make no mistake, the odds are not in your favor—you have to patch every hole, but an attacker need find only one to get into your environment [2]." So, just as the retail store employs "plain-clothes security personnel" to test their holes, the network environment employs the security professional, whose job it is to seek out the vulnerabilities in the network, expose them, and correct them, before the attacker does the same. Luckily, in today's world of computer security, there are a variety of tools available to the "good guys" to aid in this quest. Unfortunately, the same tools are available and used by the "bad guys" as well. Many of them were even written by the hackers in the first place [3]. These tools can help you complete a comprehensive Vulnerability Assessment (VA) of your company's network system, and if you are on your toes, keep your assets and valuable information secure, because unlike loss in a retail environment, it is not always blatantly obvious when information has been stolen since it does not have to be literally missing to be compromised.

So where should you start in assessing the vulnerabilities in your company's network? There are several preliminary steps that must be taken prior to beginning the process. Before approaching your management team with the proposal of a Vulnerability Assessment, load your guns with justification for the scan. The Computer Emergency Response Team (CERT) released reports in February 2002, that show total security

incidents nearly doubled in 2001 compared to the reports from 2000! 52,658 incidents were reported to the CERT in 2001, while only 21,756 such incidents were reported in 2000. The CERT defines security incidents as any related set of security events, be they a large-scale virus outbreak involving thousands of sites over a long period of time, or a much smaller one involving a one time target on one site [4]. L. Taylor of TechnologyEvaluation.com [5] has compiled a great list of probable reasons for your company to do such an assessment.

- Customer Expectations
- Prevent Litigation
- Protecting your revenue stream
- Reducing site outages and performance problems
- Creating secure and seamless information access
- Preventing denial of service attacks
- Taking precautions during acquisitions or mergers
- Customer contractual obligations
- Protect against stock fluctuations
- Mergers and acquisitions
- Testing your Intrusion Detection System
- Cavalier engineers
- Build customer loyalty
- Gain competitive advantage
- Enabling corrective action
- Qualifying for Information Protection Insurance

What are you protecting? What are acceptable risks for your company? As the Internet grows, so do the risks associated with using it. More and more people gaining access to the Internet on a daily basis as the cost of owning or accessing a computer continually falls, and the opportunity for inexpensive or free access is increased. Therefore, new doors are opened to the possibility of attacks every day. The 2000 Computer Security Institute/FBI Computer Crime and Security Survey [9] shows that the cost of security breaches is on the rise. Their statistics show that 70 percent of the 585 respondents in the year 2000 reported computer security breaches. Of these, 273 of the organizations could quantify financial losses at an astonishing total of $265,586,240, a 100 percent increase over the 1999 reports!

Face it; the hackers are out there. They have extensive tools available to allow them to get into very sophisticated systems, that are readily available, and very user friendly. Gone are the days in which the attackers were the system experts and needed extensive knowledge and time to access a system. Today's tools literally do it for them. The means are there, and they are becoming more sophisticated by the day. Attackers use the Internet itself to build better-automated systems that can coordinate massive attacks from multiple sites and they are willing to share with others to continue to increase their capabilities. The reasons for such attacks are as numerous as the attackers and the means.

The attacker may do so out of curiosity and for a challenge, such as my son's desire to hack his friends' e-mail just to be able to say he did. Others may be looking for proprietary information; they may want to launch a Denial of Service Attack just because they can, or because they are protesting a site or product. Whatever the reason or reasons, information, money, politics, or fun, the results can be dangerous and expensive. Therefore, before approaching your management, compile an index that is applicable directly to your company's situation and your company's risk factors. What weaknesses does your infrastructure expose to external attackers or even to internal disgruntled employees?

It is your responsibility to protect your network and your customers. All too often, intruders use "old" methods that have patches or fixes available to attack a system. Consider the February 2000 attacks on Ebay, Amazon, and Yahoo! A thorough Vulnerability Scan would have told the system administrators that they were susceptible to Synfloods in which the attacker sends more traffic than the network can handle. This results in Denial of Service (DOS) for legitimate users. Had the site, employed stateful routers rather than stateless ones, they could have prevented the Synfloods altogether. A good Vulnerability Assessment may have prevented their downtime [5].

After presenting the reasons for a Vulnerability Assessment, you must get written permission to the scan. There are far too many cases of the "good guy" ending up in hot water due to well-intentioned attempts expose deficiencies in a system. One such example was the notorious Randal Schwartz case in 1995. Although this is ancient in terms of the computer world, the results are not to be forgotten. While working as a consultant for Intel of Beaverton, Oregon, he failed to get permission before he tested the network's security. A jury convicted Mr. Schwartz on three felony counts. His sentence was steep and included "5 years' probation, 480 hours community service, and $68,000 in damages" in addition to the lawyer's defense fees that exceeded $170,000 [6]. In addition to the legal ramifications and cost of unauthorized scans, it is unwise to scan networks for vulnerabilities without permission and notification due to the fact that such scans can often cause undesired "side effects," denial of service, and other system failures.

Once permission for the VA has been obtained, you must decide what the goals are for the assessment. Just as there are many of tools for the intruder to use; there are many different tools on the market to perform Vulnerability Assessments for your network. In order to choose the right tool or tools, you must determine exactly what you want to do. Network Scanners are available with a wide array of utensils and functions. In addition to the tradition port scan, scanners can detect common security flaws like configuration errors and Trojans, search for out-of-date operating systems, find and identify devices on a network (whether you knew they were there or not), identify weaknesses and known holes in software, applications, and passwords, and they can simulate attacks. A VA can also help determine if your Intrusion Detection System (IDS) is functioning properly. You cannot protect everything on your system and still allow it to do all necessary

functions as needed in a user-friendly fashion, therefore, it is crucial to determine what information you need to protect and then carefully plan how to do so based on its value to your establishment.

Choosing the right Vulnerability Assessment tools can be a difficult decision. Depending on your objectives, it may even be wise to hire an external company to perform the assessment, much as a financial institution would contract external auditors to perform an evaluation on them. However, considering the extensive tools available to the systems administrator, more and more businesses are conducting their own Vulnerability Scan Assessments by using the same tools the hackers use and/or commercial products that are readily available. So where do you start? The best answer to that question may be to ask, "Where would an intruder start?" After all, aren't you trying to get a "hacker's view" of your system?

Before choosing a product or products to use for your risk management program, you must compare the features, apples-to-apples and oranges-to-oranges. How technically advanced are the people that will be evaluating the assessment? Do they need an easy to use interface such as GUI's or are they comfortable with command line interfaces. How do you want to or need to prioritize the vulnerabilities the scan finds? A vulnerability report can generate hundreds of pages of potential exploits, which may seem unmanageable if you don't know which ones must be addressed immediately and which are of lesser consequence to your particular business. A vulnerability scan is not a one-time shot. It must be done regularly to maintain protection, as new vulnerabilities are continually discovered and exploited. You may discover that some areas of your network need higher protection and more frequent scans than others [3]. How often is the product you are considering updated with new vulnerabilities? Do you want an open-source scanner or a proprietary one? Do you need a product that supports Unix or Windows or both? Which product will use the least of your valuable network resources to perform the scan? What is your budget for the process? Vulnerability scans can be done using everything from freeware to a vendor cost from $695 per server all the way up to $15,000 for 1,000 nodes. A typical cost per server would be $1,000 [9]. After answering these questions, and many more, you can determine the product or products you need.

A good starting point to compare products is by using the Common Vulnerabilities and Exposures (CVE) List by MITRE Corporation. CVE is helping to simplify vulnerabilities by assigning a unique name to each problem and providing a consistent language for the computer security community to use when dealing with those problems. They operate separately from vendors, newsgroups, and advisories to eliminate biases or conflicts of interest. The hacker community is sharing their resources, so should the security community (of course the CVE is available to those trying to do good and those using the information for bad as well, but won't they get it anyway?). The CVE is a good resource for the security professional to evaluate system tools on a level playing field. If a tool is "CVE-compliant, you can immediately determine if a tool tests for the specific vulnerabilities that concern you without poring through the product's documentation [8]."

Seems simple doesn't it. Well, maybe not. Be careful not to let numbers alone be the determining factor in choosing your Vulnerability Assessment Vendor. There are many different ways to list numbers, and statistics are easy to manipulate, so just because one vendor claims to detect twice the vulnerabilities of another, doesn't mean the first necessarily has a more comprehensive product. Vendors may also claim to perform x number of checks when it is operating [3]. However, there is no standardized format of what a "check" is, so what one vendor may consider two checks, another may only consider being one. As more and more vendors adopt the CVE classifications, the easier it should become to compare products.

In a report published in January of 2001 [2], Jeff Forristal and Greg Shipley demonstrated that the vulnerability scanners are not an all-in-one solution. They tested seven different platforms including commercial products and open-source products on systems with 17 specific published critical vulnerabilities. Not one of the seven scanners detected all 17 vulnerabilities. Their report stated "In addition to missing a number of major holes, some of the tools presented us with confusing reports, contradictory information and misdiagnosed vulnerabilities." Therefore, it seems that a solid combination of a variety of continually updated tools may be the best defense against a continually growing and mutating attacker.

Although the products are incessantly improving, they aren't there just yet. Forristal and Shipley made the following statement in their report of what the ideal vulnerability scanner would be capable of:

> If we were to build our ideal vulnerability scanner, it would comprise a few fundamental components. First and foremost, it would have an up-to-date database of vulnerability checks. While organizations should have methods in place to monitor new vulnerability announcements, these products should not be months behind on looking for big holes. Second, the scanner would have to be pretty accurate and limited in its susceptibility to flagging false positives. Hunting down a few phantom alerts in a small report is one thing; hunting down hundreds or even thousands of them after a large scan is quite another. On our tiny test LAN, the false reports were annoying. If the ratios we saw hold true on larger networks, this will be a much bigger problem in enterprise environments.
>
> The ideal scanner would have some sort of scalable back end that can store multiple scans and provide some means of performing trend analysis. While products like Internet Scanner let you pull up past scans for comparison, products like eEye's Retina don't appear to have any mechanism for managing

multiple scan sets. Finally, the ideal scanner would contain clear and concise information for fixing any discovered problems. Products like Axent's NetRecon are fairly polished on this end, and Internet Scanner has practically perfected it, but products like SAINT and SARA are severely lacking in providing specific instruction on repairing the identified problems.

So where does one begin in tool assessment? The first scanner to gain notoriety was the Security Administrator's Tool for Analyzing Networks (SATAN) that was released in 1995. It was immediately identified as a powerful tool for the network administrator in defense, but because of its ease of use and availability, it was also deemed a prime tool for malicious intruders [1]. Since then, there have been hundreds of additions to the original tool kit. Lets look below at a small sampling of vendor software and freeware that can be used to protect your environment today.

Symantec NetRecon 3.5 is a network vulnerability assessment tool with root-cause analysis features. This product's claim is that it not only identifies vulnerabilities, but also goes through a systematic response to uncover the sequence it used to expose the vulnerabilities.
Product information can be found at www.symantec.com

HackerShield 2.0 by Binview Development is network-scanning software for Windows NT. Although it requires NT to run, it can scan Unix, NT and Windows workstations for security vulnerabilities.
Product information can be found at http://www.bindview.com

SARA or the Security Auditor's Research Assistant is an open-source product that is designed to work with other software to increase the abilities and performance of both. It is a third generation Unix based security tool that was designed to replace SATAN and SAINT.
Product information can be found at http://www-arc.com/SARA/

SystemScanner by Internet Security Systems detects vulnerabilities at the system level as a part of their total security management platform. It can be used in combination with a variety of other products by ISS for a high level of network security.
Product information can be found at
http:///www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_system.php

Nmap or Network Mapper is another open-source tool available to anyone who can download it. It is a port-scanning tool that successfully scans large networks and supports most operating systems.
Product information can be found at http://www.insecure.org/NMAP/

Nessus is yet another open-source remote security scanner used to audit network and look for weaknesses.
Product information can be found at http://www.nessus.org

Now that you have determined which product or products are the best choices for you, it's time to get down to business. It is important to test the scanner in a controlled laboratory environment prior to doing a full-blown scan on your system. During this step, you are able to train the individuals responsible for completing the scan and identify potential problems prior to introducing them to your network. It would be quite embarrassing and expensive to start a DOS problem when trying to prevent that very same attack in the first place. After a successful test, you are ready to run the scan on your network. In addition, it is important to keep your vulnerability scan from reaching beyond the walls of your own network if you are connected to the Internet since your company could be liable if others are affected. Words of advice to the wise, never, under any circumstance, run a vulnerability scan unattended. Doing so would be jeopardizing your career as a computer security professional. You must be there to stop the scan if unexpected conditions arise.

A vulnerability scan is done in three simple steps [3]. The first of these may appear as innocent communication between two computers. However, in this step the would-be attacker is gaining invaluable knowledge about your system. In this discovery step, the intruder uses the Ping utility to uncover which devices are operating on your network by sending Internet Control Message Protocol (ICMP) packets to the system and waiting for a response. By doing this, the intruder can detect and create a "map of live hosts" to be targeted.

The second step for the intruder is a port scan. In this step, the attacker "identifies ports in listening mode as well as those that may have exploitable active services." During the port scan it is also possible to identify the operating system on the targets as well as any service packs or kernel releases that have been installed. Note though, that just because a listening port has been found, it does not mean that it is vulnerable. Attackers often have to send a variety of distorted packets to coax the target to give up the desired information.

Finally, the scanner dissects and scrutinizes the data to generate a potential vulnerabilities report to the would-be intruder. Hopefully, that is you. Ideally, the scan should be checking for a variety of things. Again, L. Taylor [4] tells us things that a worthwhile scan should try to do such as try to retrieve your routing table, try to obtain ICMP netmasks, search for IRC servers, look for SSH configuration information, and search for password files. It should search out known "vulnerabilities associated with file transfer protocols, hardware peripherals, hacker Trojans and backdoors, SMTP and messaging problems, network file system vulnerabilities, website and CGI holes." Further, premier scans should also check for things such as "denial of service attacks, Intrusion Detection System functionality, and UDP ports."

"The most important step in scanning your networks for vulnerabilities is interpreting the results," notes Loshin. Since different vendors provide differing result formats, it is important that you have chosen one that is useful to you. You may choose to have graphs and visual reporting, numerical data summaries, or detailed results for individual systems [1]. Whatever the format, it is important to assess the following. What vulnerabilities or holes were found? Which of those are most crucial to your systems functions? Did the assessment tool you used already repair some of the problems found? What problems still exist? Who is responsible for repairing those issues? This is where the value of a risk management team may come into play. Problems can be properly divided among the team and addressed in a timely responsible manner.

In short, knowing that a vulnerability exists is not enough to protect your network since a vulnerability scanner cannot tell you if your network has already been targeted or even if it has already been overcome. Steps must be taken to ensure the vulnerability is eliminated and furthermore, prevented from reoccurring. When used in combination with an effective IDS and firewall, scanners can greatly increase your odds of beating the intruders and maintaining a safe and secure network for your enterprise and those associated with it.

References:

1. Loshin, Pete. "Network Vulnerability Scanning – Keeping Your Networks Buttoned Up." Boardwatch Magazine, October, 2000. URL: http://www.program.intel.com/SOLUTIONS/shared/en/resource/insight/indtrends/vulnerability.html
2. Forristal, Jeff. Shipley, Greg. "Vulnerability Assessment Scanners." January 8, 2001. URL: http://www.networkcomputing.com/1201/1201f1b3.html
3. Conry-Murray, Andrew. "Vulnerability Assessment Tools – A vulnerability scan takes a hacker's-eye view of your network." Network Magazine, April 5, 2001. URL: http://lanmag.com/article/NMG20010321S0005
4. "CERT/CC Statistics 1998-2001." February 2002. URL: http://www.cert.org/stats/cert_stats.html
5. Taylor, L. "The Whys and Hows of a Security Vulnerability Assessment." URL: http://www.intranetjournal.com/articles/200010/SE_10_18_00A.html
6. Kaybay, M. E. "Unauthorized Vulnerability Scans." URL: http://www.net-security.org/text/articles/nwf/scans.shtml
7. Computer Security Institute, 2000 CSI/FBI Computer Crime Security Survey, Computer Security Issues and Trends, Vol. VI, No. 1 (Spring 2000).
8. Merkow, Mark. "An Ounce of Prevention CVE: Helping Make the Internet a safer place for us all." November 5, 1999. URL: http://www.ecommerce.internet.com/news/insights/outlook/article/0,,10535233131,00.html
9. Haber, Lynn. "New Tools To Assess Security." URL: http://networking.earthweb.com/netsecur/article/o,,12084_731581,00.html