Process for Performing, Evaluating and Documenting Host Vulnerability

Gary L. Conner

GSEC Practical, Version 1.2e

Abstract

An important part of providing security for your organization is awareness of what your exposure is and tracking the security status of your systems over time. The goal of this paper is to provide an outline of the processes involved in identifying and tracking system security that can be adapted to your organization.

Establishing Goals

The ultimate goal of any vulnerability assessment is to find and fix security issues. However, when you have hundreds or even thousands of systems where do you start? Randomly testing systems with no clear goals in mind is a futile exercise at best and can be a very frustrating and demoralizing process.

The first step to setting your goals should be the determination of a starting point based on what's most important to your business. Using the 80/20 rule in this instance is generally a good idea and can get you well one your way to being effective in a short time. Also, having a security policy and security configuration standards for each type of system is a critical part of assessing your security and correcting problems that you find. Using this information while planning and determining your goals will help to keep you on track.

The systems in your organization can be broken down by criticality based on how likely they are to be attacked and how sensitive the data on those systems is. Popular targets for attack are Internet servers, HR databases, customer records and research and development. Having a clear set of goals and knowing where you're most likely to be at risk will help in determining your testing plan.

Now that you have a list of systems to evaluate and have them sorted by importance, it's time to figure out what you're trying to accomplish. Do you just want a baseline that lists the ports open on all of these systems or do you need a complete list of all of the vulnerabilities on every system? The answer to this question will determine what your testing plan looks like. Just remember, always have a plan for where you are going. This will help to keep the testing process on track.

Another thing to account for is the size of the job you're planning. Handing a system administrator several hundred pages of output and telling them to fix everything is not the way to make progress. Keep your projects to a reasonable size and give the people who will be fixing what you find meaningful instructions.

Okay, you know what you want to do and where to do it. Do you start scanning systems now? NO! Before you go any further, get approval from someone in management that has the authority to approve this type of testing. Get this manager to sign an authorization form allowing you to perform the tests. If anyone asks or there are problems, you are covered on two fronts. First, management is aware of what you are doing. Second, management has endorsed what you are doing. With that signed approval, you now have a "get out of jail free card".

Tools

Now that you have a plan and management approval, you need tools. Your test plan will help you to determine which tools you need for which job. One tool does not fit all circumstances; if the only tool you have is a hammer, the whole world looks like a nail. Also, tool selection is directly related to your budget. If you don't have much to spend, there's no reason to plan on using one of the more expensive commercial tools. On the other hand, there are some excellent freeware/shareware tools for the budget conscience.

While there are a lot of free / cheap tools available, two of my favorites are NMAP and NESSUS. These are two of the most comprehensive security testing tools in existence today and the price is right (free!). If you decide to use either of these tools, take the time to learn how they work and how to really get the maximum benefit from them.

If you decide to use commercial assessment tools, there are some excellent products from numerous vendors including Internet Security Systems, Network Associates, Symantec, Cisco and WebTrends to name just a few. All of these companies make excellent tools and any one of them is a worthy addition to a network security toolkit. The same caveat applies to these tools as well; learn how they work and how to use them.

As with any tool, these programs in unskilled hands can have devastating results. Any of these programs can render a system or entire network unusable. When you decide which tools are right for you, learn how to use them on test systems before you test your production environment.

Another aspect to using tools is that none of them are perfect. They all have strengths and weaknesses. Using multiple tools will alleviate some of the gaps but not all of them. There is no substitute for knowing how your systems work. A few minutes at the keyboard looking at what a system is really doing can be more valuable than any scanner if you know what to look for. Which brings up another point, you can't secure what you don't understand. Learn your systems, how they work and what they are being used for; there is no substitute for knowing your environment.

Performing the Assessment

Well, now were ready to start having some fun. We have our tools, we've tested them until we know every detail of their operation and we have the approval of management and the system owners. So what do we do now?

When should we do our tests? That's simple - it depends. Most organizations aren't going to risk having their systems taken down during business hours because of a security scan. After you've completed a few scans, they may become a little less cautious and let you run scans at various times. If you only run your scans on Saturday night from 7pm until midnight, then you may be missing a lot of things. CRON or AT jobs that start and stop services during the week could be missed. This is especially a problem on large corporate networks with a limited staff where you can't touch every system by hand.

Another thing to consider is tuning your tools to meet your security standards and policies. There is no reason for you to test vulnerabilities that you know are there because they have been intentionally left in because of a business need. This only creates extra work when you are sorting through the results of your scans.

Do your assessments at different times on different days and compare the results. They should be the same; if not, then you have some investigating to do. Contact the system owners and see if they can explain why there are differences. If they can't, then it's time to raise the issue to management or your CIRT depending on what your policies say.

Another suggestion is to only scan one system at a time unless you are looking for something specific. Doing the scans one at a time gives you the opportunity to create a separate file for each system and will make it much simpler to recreate your results and keep a running profile of each of your systems. A directory structure similar to the one in figure 1 works well for this purpose.

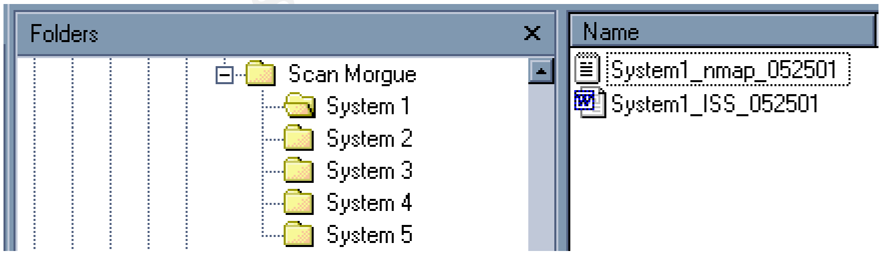


Figure 1

With the scan results stored in this manner, you (or anyone else) should be able to go back and recreate the finding from the scans. This is very important and adds a very high degree of credibility and consistency to your findings.

Evaluating the Results

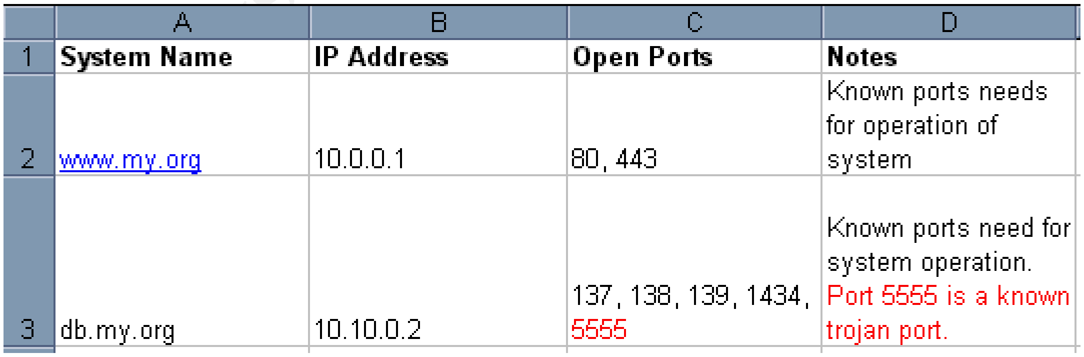
Now that you’ve scanned the systems, what do you do with the results? How do you determine what is important and what’s not? This is where most of the work is and when you need to refer back to the original goals that you set and your security standards.

If you have tuned your scanners to ignore the vulnerabilities you know about and that have been approved by management as “acceptable risk”, it is fairly easy to see what still needs to be fixed and if there are any new vulnerabilities that need to be addressed. These can then be reported to management along with recommendations on what needs to be fixed immediately and what can wait.

Documenting your Findings

One of the keys to performing a successful vulnerability assessment is in documenting your findings. With the number of tools being used and the diversity of the results, this becomes even more important. As I mentioned above, handing a sys admin a pile of paper and telling them to fix everything is not the way to accomplish anything productive. Several reports and formats are usually needed and will allow you to convey the information that is relevant to your environment in a very effective and targeted manner. The samples shown below should provide you with a starting point to develop your own reports and methods for documenting your findings and reporting them to management.

Port Scan Results:
While it is best to keep the results of the scans in separate files, presenting this information as a single report can be very effective. This will allow you to show changes from scan to scan and see trends if a new port starts to show up. Showing changes from the last report in RED will also draw attention to that item. This is illustrated in figure 2 below.

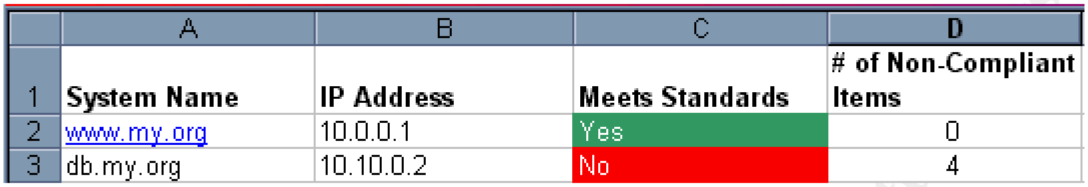


	A	B	C	D
1	**System Name**	**IP Address**	**Open Ports**	**Notes**
2	www.my.org	10.0.0.1	80, 443	Known ports needs for operation of system
3	db.my.org	10.10.0.2	137, 138, 139, 1434, 5555	Known ports need for system operation. Port 5555 is a known trojan port.

Figure 2

Organization Security Profile:

This is another report where you should be providing information about multiple systems. This will allow you to track the security status of your systems at an organizational level and report on compliance to your security standards and policies. Figure 3 shows a sample format for this type of report.



	A	B	C	D
1	**System Name**	**IP Address**	**Meets Standards**	**# of Non-Compliant Items**
2	www.my.org	10.0.0.1	Yes	0
3	db.my.org	10.10.0.2	No	4

Figure 3

System Security Profile:
This is the technical report and should be system specific. Using the reports above to target the critical system and the ones needing the most attention will help to keep the scope of the reporting to a manageable level. This report is for the system administrators that will be correcting the issues that you have identified and will need to be a detailed report.

A system security profile report will need to contain detailed information on each vulnerability that needs to be corrected, what the risks associated with the vulnerabilities are and detailed instructions on how to correct the vulnerability. The report should not contain known vulnerabilities that have been approved by management as an acceptable risk unless they are specifically marked as such and placed into a separate section of the report. Including this information in the main report only serves to complicate and confuse the process of correcting the things that really need to be addressed.

Conclusions

While not the only method for analyzing and improving the security of an organization the methods in this document will be successful if a few guidelines are followed.

- Learn your environment.
- Learn to use the tools that you've selected.
- Set goals.
- Have a plan for achieving your goals.
- Get management approval before beginning testing.
- Keep management informed by providing them with relevant data.
- Show continual progress.

These few guidelines can have a tremendous effect on the success or failure of your efforts, and I strongly suggest that you take them to heart. Expending the effort to analyze your systems only to be shot down when you present the information is counterproductive and highly demoralizing. Or worse, being fired for doing something that you didn't have authorization to do could destroy your career.

Management needs factual and complete data to make good decisions about the risks to the organization. This process will allow you to provide them with data they can us to make decisions concerning the security and the risk levels they are will to accept. Sticking to the facts and making sure your results and conclusions are reproducible lend a level of credibility to your recommendations that you cannot get by using scare tactics. While a good scare will get you a lot of attention, the excitement quickly fades and so does the interest from management. One the other hand, if you are producing valuable information that is fact based, you'll keep the attention of the people making the decisions and go home at night knowing that you made a difference.

References

Wengert, Patrick. "WebTrends Security Analyzer." 16 March 2001.
URL: http://www.sans.org/infosecFAQ/audit/webtrends.htm (26 May 2001)

Scambray, Joel; McClure, Stewart; Kurtz, George. Hacking Exposed, Second Edition. McGraw-Hill Professional Publishing, October 11, 2000.

The MIS corporate Defence Solutions Ltd., Network Security Team. "An overview of Network Security Analysis and Penetration Testing". 1 August 2000.
URL: http://www.mis-cds.com (26 May 2001)

Johnson, John D. "Conducting Risk Analysis to Evaluate Enterprise Security." 5 Nov. 1999. URL: http://securityportal.com/topnews/conduct-risk.html (26 May 2001)

Micksch, Allan. "Information Systems Risk Analysis, Assessment and Management" September 13, 2000
URL: http://www.sans.org/infosecFAQ/policy/risk.htm (26 May 2001)

NESSUS.
URL: http://www.nessus.org (26 May 2001)

Nmap.
URL: http://www.insecure.org/nmap (26 May 2001)

Internet Security Systems. Internet Scanner.
URL: http://www.iss.net/securing_e-business/security_products/security_assessment/internet_scanner/ (26 May 2001)

Network Associates Inc. Cybercop Scanner.

URL: http://www.pgp.com/products/cybercop-scanner (26 May 2001)

Symantec. NetRecon.
URL:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&PID=4495869 (26 May 2001)

Cisco Systems Inc. Cisco Secure Scanner
URL: http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/ (26 May 2001)

WebTrends. WebTrend Security Analyzer.
URL: http://www.webtrends.com/products/wsa/default.htm (26 May 2001)