Vulnerability Assessments: The Pro-active Steps to Secure Your Organization.

Robert Boyce
GSEC version 1.2d

Every business contains an element of risk, ranging from issues of finance to product production. With the world of e-commerce continuing to emerge as the new industry standard businesses are faced with a new risk, the risk of technology.

> Malicious break-ins into corporate computer systems are mounting. A recent FBI study finds 85 percent of respondents detected computer security breaches during the past year. The survey drew responses from 538 security experts in various U.S. corporations and government agencies. Sixty-four percent suffered financial losses due to security breaches, and 186 respondents report a total loss of $378 million (Landergren).

Given this additional risk and increased potential for loss, it is not surprising that most companies on the Internet are spending more and more money finding ways to protect themselves. There is one technique that many companies overlook when developing their security design, the self-administered vulnerability assessment. The practice of conducting a network Vulnerability Assessment (VA) against ones own Enterprise can be very beneficial. It could lead to discovering exposures before potential attackers do, and assist in highlighting the overall security posture of the enterprise.

Along with the immediate benefits there is a lot of preparation that must be put into constructing an effective VA process. Policies and procedures must be created and enforced, there must be strict guidelines outlining the rule of behaviour, and there must be a means of change management detailing all planned activities. Without these components in place there is no way to ensure that the process will be carried out consistently, or even that the process will be carried out at all.

As with any job, having the right tools is essential in obtaining accurate and complete results. When conducting a VA it is important, and very beneficial to use the same tools as the potential attackers. That way it is possible to duplicate the same methodologies and techniques that will be employed when your organization’s systems are being targeted.

By creating a solid policy, executing consistent procedures, and using the right tools, there is no end to the potential advantages that a good VA process will bring to any organization.

VA Policies and Procedures

Every effective security practice is built on a strong foundation of policies and procedures, and the vulnerability assessment process should be no exception. Before beginning to conduct any VA it is important to ensure that the underlying policies relevant to the organization are in place to facilitate the process. These documents will be the principles, outlining the actions to be taken when planning and performing all aspects of the VA each and every time it is conducted.

The policies and procedures will need to encompass existing organizational processes. For example, Change Management. This will ensure that all VA activities have gone through a review process thereby making others in the organization aware of the purpose and scope of the planned VA. There also needs to be a mechanism to manage the resulting VA data. By tying into the existing Issue Management process it is possible to create a method to track issues and distribute the finding to the various system owners for resolution. One last example could include making use of the existing Rule of Behaviour process. This way it is possible to clearly define each individual's roles and responsibilities in the planning, conducting and reporting of the vulnerability assessment.

When developing any procedure it is best practice to start from a high-level and work down towards defining the specific details. These particulars may vary between organizations, but the basic high-level details will usually be the same. Figure 1 illustrates the key concepts involved in performing a vulnerability assessment.

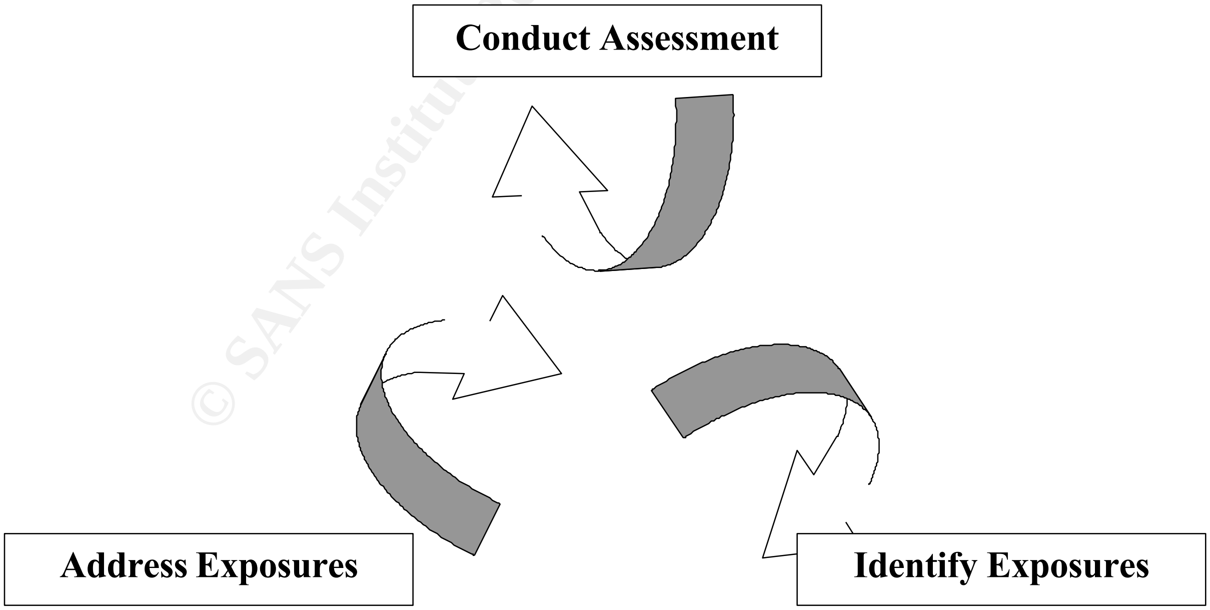

Figure 1

Three phase cyclical vulnerability assessment procedure

Conduct Assessment This phase consists of two main objectives, the planning and performing of the vulnerability assessment. The planning component will include gathering all relevant information, defining the scope of activities, defining roles and responsibilities, and making others aware through the change management process. The method for performing the VA will include interviewing system administrators, reviewing appropriate policies and procedure relating to the systems being assessed and of course the security scanning.

Identify Exposures This phase can include an assortment of tasks. For example, reviewing the resulting data from the assessment phase and tying it into the issue management process so that accountability for the issues are established and the exposures can be resolved. The data can also be stored and reviewed allowing for enterprise wide risk analysis and trending.

Address Exposures This phase tries to resolve the exposures identified in the previous phase. Before any steps are taken to fix the problem an investigation must be conducted to determine if the service that caused the exposure is in fact needed. If the service is needed then the system should be upgraded, or if no upgrade exists management must be informed of the potential risk that system presents. If the services is not needed then it could simply be disabled.

Performing a vulnerability assessment can provide an accurate “point-in-time” representation of the organization’s security posture. However, this is not enough. There must be a mechanism incorporated into the procedures to ensure that the VA process is conducted on a continual basis. This is the only way to really minimize the overall risk.

It is also important to have these policies and procedures reviewed and approved by management. This will help ensure that they become official organizational practices.

Key Benefits

With threats originating from all parts of the globe, as well as from within ones own network, it is now becoming more important for organizations to secure their resources. The benefits that can result from conducting frequent, pro-active vulnerability assessments can be numerous.

The most obvious advantage would be the ability to identify known security exposures before potential attackers do. By completing continual assessments it is easy to identify possible security concerns that may be present on the network, both from an internal and an external perspective. Early detection introduces the opportunity to address the issues before the attackers can exploit the weakness which may cause serious damage to the companies assets and possibly their reputation. No one wants to hear about their security deficiencies on CNN.

Another benefit of conducting routine vulnerability assessments is that it can assist in updating or creating a detailed network map of the enterprise. An organization should have an accurate idea of what systems are present in their environment. However, it is not impossible for someone to connect a new system to the network without informing the right people or going through the correct change management process. If these machines were unofficially connected to the network, chances of them being hardened or secured is probably low. These rogue machines can introduce unwanted and unnecessary risks into the enterprise and need to be dealt with in a timely manner.

During the process of detailing the network map it would be an added value to take things one step further and create an inventory of all the devices on the network. The inventory could consist of the device type, current operating system levels, hardware configurations, application versions, and any other pertinent system information. These statistics will be quite useful for system tracking, but consider adding one additional field in the inventory list, the “vulnerabilities associated” with that device. Now this information becomes very valuable from a security tracking perspective. It becomes possible to not only immediately determine if any existing system has any associated vulnerabilities, but one could also develop focused advisory lists to distribute to the administrators of those systems when new exploits are released.

The self-assessment strategy not only offers an organization a detailed look at some of the potential exposures that may exist, but it can also be used to portrait the overall security posture of the enterprise. The information obtained during the assessment process can be used to trend the level of risk that currently exists on the network. This can be accomplished in a variety of ways. For example, keeping in mind that the VA process is a continual practice, it is possible to maintain an archive of all vulnerabilities associated with any number of systems on the network. This archive will be updated at the completion of each assessment, making it possible to illustrate the number of exposures associated with *y* systems over *x* time.

It is important to recognize that some of the exposures uncovered may actually need to be present for the systems to run correctly, from a business perspective. The services associated with these exposures need to be highlighted so that they will not be identified again during the next assessment. This way it will be possible to accurately develop a risk curve to illustrate how the security posture trends over time. Ideally the risk curve would be reduced, reaching the point where the network security and business requirements reluctantly meet.

Tools

The right tools for the right job. That statement is just as true for the VA process as it is in any other situation. When conducting a vulnerability assessment the tool set being used should be very similar to that of the identified adversary. This will ensure that the systems are secure from attacks that are currently being employed out in the wild. Remember new weaknesses are discovered everyday, and new tools to exploit these weaknesses usually follow close behind, so it becomes very important to stay current with security news.

An organization does not need a huge budget to buy loads of commercial security tools, nor do they need a group of techno-geniuses creating custom tools. Many of the tools that attackers use are free open source tools which are available for download from the Internet.

The following list contains just a sample of some very useful and very free tools that can be found on the Internet

Nmap Nmap is a utility for network discovery and/or security auditing. It can be used to scan large networks or single hosts quickly and accurately, determining which hosts are available, what services each host is running and the operating system that is being used.
For more information visit http://www.insecure.org/nmap

Nessus Nessus is a remote security scanner. This software can audit a given network and determine if there are any weaknesses present that may allow attackers to penetrate the defences. It launches predefined exploits, and reports on the degree of success each exploit had.
For more information visit http://www.nessus.org

Whisker Whisker is a CGI web scanner. It scans for known vulnerabilities found in web servers, giving the URL that triggered the event as well, it can determine the type of web server being run. It is easy to update and has many useful features.
For more information visit http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2

Enum Enum is a console-based Win32 information enumeration utility. Using null sessions, enum can retrieve userlists, machine lists, sharelists, namelists, group and member lists, password and LSA policy information. enum is also capable of a rudimentary brute force dictionary attack on individual accounts.
For more information visit http://razor.bindview.com/tools/desc/enum_readme.html

Firewalk Firewalking is a technique that employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks. It can also be used to determine the filter rules in place on a packet forwarding device.

For more information visit *http://www.packetfactory.net/Projects/Firewalk*

Conclusion

Existing controls may be effective, but not sufficiently comprehensive to provide assurance of appropriate and ongoing confidentiality, integrity, and availability of information. Vulnerability assessments are an important mechanism through which organizations can identify potential security exposures and have a process in place to correct any deficiencies. Routine self-assessments provide a good picture of how security is managed and improved over time, and to help identify areas most in need of attention.

Addressing identified security exposures is a good first step, but there is much more to be done. Developing solid policies will ensure that the VA process is completed in line with the organizations requirement each and every time, as well it will give the administrators a consistent base from which to conduct their assessments. Also by seeking management approval it will ensure that the VA process is made a continual and official organizational practice.

Getting the most out of the data that is being collected during the assessment is essential. Creating an inventory of all devices in the enterprise will help with the planning of upgrades and future assessments. This information can also be used to organize a distribution list of future exposures that may affect those systems, another great pro-active step in securing the enterprise.

With the Internet community growing, and the ease at which just about anyone can launch a cyber attack, it is becoming more important to secure potential exposures quickly. Addressing these exposures is becoming a race that is seemingly harder and harder to win, don't let your organization fall behind

References

1. Landergren, Pia. “Hacker Vigilantes Strike Back.” June 20, 2001. URL: http://www.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/index.html.(June 24, 2001)

2. Forristal, Jeff. Shipley, Greg. “Vulnerability Assessment Scanners” January 8, 2001. URL: http://www.networkcomputing.com/1201/1201f1b3.html. (June 25, 2001)

3. “Computer Security Self-Assessment Checklist". June 30, 1998. Massachusetts Institute of Technology.
URL: http://web.mit.edu/security/www/isosec-assess.htm. (June 27, 2001).

4. Brooks, Greg. "Nessus – Get on Board". February 15, 2001. URL: http://www.sans.org/infosecFAQ/audit/nessus2.htm. (June 27, 2001).

5. Fyodor. “The Art of Port Scanning.” September 01, 1997. URL: http://www.insecure.org/nmap/p51-11.txt. (June 27, 2001).

6. "Security Review Checklist". 1997. Rainbow Technologies, InfoSec Services, Spectria Division. URL: http://www.infosec.spectria.com/articles/check-rvw.htm. (June 30, 2001).

7. Winkler, Ira. "Audits, Assessments and Tests (Oh, My): Systems security tests come in three basic flavors. Here's how to make sure you're performing only the test(s) you really need". Information Security. July 2000. URL: http://www.infosecuritymag.com/articles/july00/features4.shtml. (June 30, 2001).