IJCSMA
Madhavi Dhingra, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 230-234 **ISSN: 2321-8363**
Impact Factor: 5.515

Vulnerability Assessment Policies and Tools in Enterprise Networks

Madhavi Dhingra
Amity University Madhya Pradesh, Gwalior
madhavi.dhingra@gmail.com

Abstract: Vulnerability assessment takes a wide-range of network issues into consideration and identifies weaknesses that need correction, including misconfigurations and policy non-compliance vulnerabilities that a patch management system alone cannot address. It provides a comprehensive picture of all systems, services and devices that can breach a network, as well as a complete, prioritized list of vulnerabilities that need to be addressed. Remediation is the follow-up stage after vulnerabilities have been accurately identified. The two work hand-in-hand and form a complimentary process. This paper examines how vulnerability assessments are currently performed by following VA policies and procedures. It also discusses about the current vulnerability tools that are being used by the enterprises.

Keywords: Vulnerability Assessment, Network Security, Vulnerability

I. Introduction

A new approach is emerging for detecting and managing vulnerabilities in complex networks. The security gave by yearly or quarterly manual defenceless-ness evaluations can now be considerably made strides. In the meantime weakness appraisal and administration overhead can be decreased and better hazard administration and powerlessness control can be proficient. Today's business system foundation is quickly changing with new servers, administrations, associations, and ports included frequently, once in a while every day, and with a constant inflow of tablets, stockpiling media and remote gadgets. With the developing number of vulnerabilities and endeavours connected with the persistent advancement of IT base, associations now require more successive powerlessness evaluations. These appraisals should normally be performed with the most recent of weakness learning and ability. In this way security costs have been rising when general spending plans have not. The ordinary border guard systems that review activity, for example, antivirus, firewalls, and IPS/IDS are presently typical and even the normal programmer or bot expect their nearness and is persistently re-designing their assaults to keep away from them. To adjust, system security heads with significant resources or having high perceivability (counting numerous little organizations and nearby government substances) are currently receiving the VA/VM instruments that have for some time been utilized just by the biggest enterprises and governments. In light of these elements, the computerization of the VA/VM procedure to lessen the exertion required for every test and to expand the recurrence of tests has turned into a practical method for dealing with the inexorably complex issues of keeping a system secure. Similarly as with the choice to mechanize any business capacity, it must be founded on regardless of whether a computerized arrangement can play out the occupation in a more productive, successful and ideally speedier path than by manual means.

When examining vulnerability scanning as an automated service, three important factors must be taken into consideration.

1. The ability of the solution to provide accurate and complete vulnerability assessment
2. Analysis and representation of assessment data as meaningful information
3. Tracking and reporting the effectiveness of mitigation efforts.

II. 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.

- **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 are not needed then it could simply be disabled.**

III. Tools

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. New weaknesses are discovered every day, 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.**
- **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.**
- **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.**
- **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**

IV. Conclusion

Vulnerability assessments are an essential component through which associations can recognize potential security exposures and have a procedure set up to rectify any lacks. Routine self-appraisals give a decent picture of how security is overseen and enhanced after some time, and to recognize territories most needing consideration. Tending to recognized security exposures is a decent initial step, yet there is a great deal more to be finished. 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. Making a stock of all gadgets in the undertaking will help with the arranging of redesigns and future evaluations. This data can likewise be utilized to sort out a circulation rundown of future exposures that may influence those frameworks, another extraordinary proactive stride in securing the venture. With the

Internet people group developing, and the simplicity at which pretty much anybody can dispatch a digital assault, it is turning out to be more essential to secure potential exposures rapidly.

References

1. Forristal, Jeff. Shipley, Greg. “Vulnerability Assessment Scanners” January 8, 2001. URL: http://www.networkcomputing.com/1201/1201f1b3.html. (June 25, 2001)
2. “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).
3. Brooks, Greg. "Nessus – Get on Board". February 15, 2001. URL: http://www.sans.org /infosecFAQ /audit/nessus2.htm. (June 27, 2001).
4. Fyodor. “The Art of Port Scanning.” September 01, 1997. URL: http://www.insecure.org/nmap/p51-11.txt. (June 27, 2001).
5. "Security Review Checklist". 1997. Rainbow Technologies, InfoSec Services, Spectria Division. URL: http://www.infosec.spectria.com/articles/check-rvw.htm. (June 30, 2001).
6. 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