INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume3, Issue6)

Available online at: www.ijarnd.com

Comparison of vulnerability assessments and penetration testing

Jaspreet Kaur

Student, Punjabi University, Patiala, Punjab

ABSTRACT

Web has opened boundless roads of chance by empowering associations to direct business and offer data on a worldwide premise. In any case, it has additionally brought new levels of security concerns and Cyber dangers. It uncovered significant corporate data, mission basic business applications and purchaser's private data to more hazard than some time recently. In any case, security of IT foundation is something that Organizations can't bear to trade off. Vulnerability Assessment and Penetration Testing (VAPT) surveys the viability or inadequacy of the security foundation introduced by the Organizations to stay shielded from the rising Cyber dangers. Consequently, it empowers the Organizations to introduce fixes and embrace required safety efforts to defend themselves from conceivable Cyber assaults.

Keywords: *Vulnerability Assessments, Penetration Testing*

1. INTRODUCTION

The security threats have evolved significantly as it involves all activities that organization, enterprises, and institutions attempt to protect the value and ongoing usability of assets and the integrity and continuity of operations. These attacks or breaches directly or indirectly harm an organization's reputation and result in non-compliances with customer privacy protection laws. As the domain of these has become larger and more sophisticated, security attacks or even worse security breaches have been ever more critical which may result in a loss in business and productivity, the time and labour involved in redeploying infected systems pose a significant expense. The expansion and evolution of Computer, Internet and Web technologies have made society more dependent upon computer network services than ever. There has been a challenge of providing a secure environment; an effective network security strategy that helps to identify threats and then selecting the most effective sets of tools to mitigate them in such a way that any organization will be able to reduce the likelihood of incidents and resultant data loss.

2. VULNERABILITY ASSESSMENT VS. PENETRATION TESTING

Two important vulnerability assessment procedures are vulnerability scanning and penetration testing. Despite the fact that these two activities are often confused, both play an important role in uncovering vulnerabilities. It is not uncommon for some self-appointed "security experts" to claim to perform in-depth penetration testing, while in reality they only conduct less-intensive vulnerability scanning.

3. VULNERABILITY ASSESSMENT

A vulnerability assessment is an automated software search (scan) through a system for any known security weaknesses (vulnerabilities) that then creates a report of those potential exposures. The results of the scans should be compared against baseline scans so that any changes (such as new open ports or added services) will be investigated. Vulnerability scanning should be conducted on existing systems and particularly as new technology equipment is deployed; the new equipment should be scanned immediately and then added to the regular schedule of scans for all equipment. A vulnerability scanner serves to provide a "red flag" to alert personnel of a security issue. A vulnerability scan examines the current security in a passive method. It does not attempt to exploit any weaknesses that it finds; rather, it is intended to only report back what it uncovered. The types of weaknesses that it is searching for include identifying any known vulnerabilities, finding common misconfigurations, and uncovering a lack of security controls. Vulnerability scans are usually performed from inside the security perimeter and are not intended to disrupt the normal operations of the network or devices. These scans are conducted using an automated software package that examines the system for known weaknesses by passively testing the security controls. Because the automated software is conducting the test in a systematic fashion, a technician with only limited security experience could conduct the test. The resulting report, however, should be examined by trained security personnel to identify and correct any problems. There are several commercials as well as open source vulnerability scan software products available for large organizations. In addition, free products that provide users with scans of their local systems are popular. However, the free products may not always provide a comprehensive scan of an entire system. Because of the number of patch updates that should be applied to a wide variety of software, it is easy to overlook patches and leave vulnerabilities exposed. It is recommended that vulnerability scans be conducted on a regular basis (at a minimum once per month) in order to identify problems.

4. PENETRATION TESTING

Unlike a vulnerability scan, penetration testing (sometimes called a "most pent") is designed to actually exploit any weaknesses in systems that are vulnerable. Instead of using automated software, penetration testing relies upon the skill, knowledge, and cunning of the tester. The tester himself is usually an independent contractor not associated with the organization but with very good IT experience and familiarity with the organization's business functions. Testers are typically outside (instead of inside) the security perimeter and may even disrupt the operation of the network or devices (instead of passively probing for a known vulnerability). Vulnerability scan software may indicate a vulnerability was uncovered, yet it provides no indication regarding the risk to that specific organization. If a penetration tester uncovers a vulnerability, he will continue to exploit it to determine how dangerous it can be to the organization. The end product of a penetration test is the penetration test report. The report focuses on what data was compromised, how, and why. The report also details the actual attack method and the value of the data exploited. If requested potential solutions can be provided, but often it is the role of the organization to determine how best to solve the problems. The goals of a penetration test are to actively test all security controls and when possible, bypass those controls, verify that a threat exists, and exploit any vulnerabilities.

4.1 Some Common Penetration Testing Tools:

- Metasploit Framework
- SATAN
- Core Impact

Table 1: Comparison of vulnerability assessments and penetration testing

Comparison of Vulnerability Assessments and Penetration Testing		
	Vulnerability Assessments	**Penetration Testing**
General Description	Identify vulnerabilities automatically through use of software rather than relying on human skills.	Test to determine if an outside party can penetrate existing organizational defenses both from a technological and social perspective.
Strengths	Runs easily and quickly, enabling ongoing monitoring. Freeware or inexpensive tools available, some of which provide advice on how to fix the identified vulnerability. Excellent method for identifying basic issues.	Simulates actual hacker process to the extent possible. Demonstrates the practical risk of identified vulnerabilities by exploiting the latter to gain entry. Assess effectiveness of user security awareness and training by leveraging social engineering.
Weaknesses	Can create significant amounts of network traffic, slowing overall performance. Easily detected by technology staff. Susceptible to high false positive rate. Often misses new vulnerabilities.	Can result in false positives due to lack of generally accepted testing standards. Requires great expertise. Need to consider legal and regulatory impacts, especially if technology resources are outsourced. Provides a sample and is not intended to identify all vulnerabilities.
Why Perform	Obtain understanding on what's connected to the organization's network. Facilitates the identification of software that is outdated or needs patching. Can identify the most common security threats resulting from configuration management.	Excellent tool to use if organization is trying to determine the effectiveness of security given various levels of efforts by unauthorized individuals (considering that any system can be penetrated with unlimited resources). Serves as a "wake-up" call for organizations that

		have not taken security seriously.
Representative Action Steps	Identify what's on the network, including hosts and open ports. Update assessment tool for technology resources used and latest developments. Scan for compliance with policies and version/patch management issues.	Define and confirm rules of engagement. Identify relevant information through footprinting, scanning, and enumeration. Leverage info gathered to make an informed attempt at the target. After gaining basic access, attempt more significant privileges or rights. Gain access to privileged and sensitive data. Document evidence of access as appropriate.
Typical Findings	Inventory of vulnerabilities. Patch or upgrade systems as required. Tighten configuration management program. Ongoing monitoring of vulnerability alerts and mailing lists to identify evolving threats. Modify security policies as needed.	Poor security monitoring by technology group. Ignorance of user security awareness and responsibilities. Access to privileged and confidential information. Specific vulnerability exploited and how. Poor incident response procedures.
Frequency	Every one to three months, depending on the environment.	Annually.
Popular Tools Used	Nessus, ISS Internet Scanner, CyberCop Scanner, SAINT, and SARA.	Anything needed to gain access, including war dialers, Nmap, Nessus, L0phtcrack, John the Ripper, Dsniff, Hunt, Netcat, RootKit, and many others.

5. REFERENCES

[1] Jianbin Hu, Y.W.C.T.Z.G.F.R.Z.C., 2011. A Novel Framework to Carry out Cloud Penetration Test. I.J. Computer Network and Information Security, pp.1-7.

[2] Jignesh Doshi, B.T., 2015. Comparison of Vulnerability Assessment and. International Journal of Applied Information Systems (IJAIS), 8, pp.51-53.

[3] Aileen G. Bacudio, X.Y.B.-T.B.C.M.J., 2011. An Overview of Penetration Testing.

[4] International Journal of Network Security & Its Applications (IJNSA), 3, p.6. Alharbi, M.A., 2010. Writing a Penetration Testing Report. SANS.

[5] Bode, L.H.a.N., 2006. Network Penetration Testing. Springer.

[6] Mansour A.Alharbi, D.K.L., 2010. Writing a Penetration Testing Report. Global Information Assurance Certification (GIAC).

[7] Michele Fiocca, A.V., 2009. Literature Study of Penetration Testing. Sweden: Project Report for Information Security Course Linköpings universitet.

[8] Shivayogimath, C.N., 2014. AN OVERVIEW OF NETWORK PENETRATION TESTING. IJRET: International Journal of Research in Engineering and Technology.

[9] Shivayogimath, C.N., 2014. AN OVERVIEW OF NETWORK PENETRATION TESTING.

