Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 57 (2015) 710 – 715

Procedia Computer Science

3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology

Jai Narayan Goel[a,b,*], BM Mehtre[b]

[a]School of Computer and Information Sciences, University of Hyderabad, Hyderabad 500046, India
[b]Center for Information Assurance and Management, Institute for Development and Research in Banking Technology, Hyderabad 500057, India

Abstract

Complexity of systems are increasing day by day. This leads to more and more vulnerabilities in Systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before attacker do. The power of Vulnerability assessment is usually underestimated. While Vulnerability Assessment and Penetration Testing can be used as a cyber-defence technology to provide proactive cyber defence. In this paper we proved Vulnerability Assessment and Penetration Testing (VAPT) as a Cyber defence technology, how we can provide active cyber defence using Vulnerability Assessment and Penetration Testing. We described complete life cycle of Vulnerability Assessment and Penetration Testing on systems or networks and proactive action taken to resolve that vulnerability and stop possible attack. In this paper we have described prevalent Vulnerability assessment techniques and some famous premium/open source VAPT tools. We have described complete process of how to use Vulnerability Assessment and Penetration Testing as a powerful Cyber Defence Technology.

Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

Keywords: Vulnerability Assessment; Penetration Testing; VAPT Tools; Cyber defence; System Security; Cyber defence Technology;

1. Introduction

Use of computers are increasing day by day. System's complexity is increasing. Most of the systems now are connected to Internet. New and complex Software are coming in the market. All these activities are increasing vulnerabilities in systems.

* Corresponding author. Tel.: 91-8332900531
E-mail address: jainarayangoel@gmail.com

Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)
doi:10.1016/j.procs.2015.07.458

A vulnerability is a weakness in the application which can be an implementation bug or a design flaw that allows an attacker to cause harm to the user of the application and get extra privilege[1]. Vulnerability are the potential risk for the system. Attacker uses these vulnerability to exploit the system and get unauthorized access and information.

Vulnerabilities are big flaw in system security and Information assurance. A vulnerability free system can provide more Information Assurance and system security. Though it is almost impossible to have 100% vulnerability free system, but by removing as many vulnerabilities as possible, we can increase system security. The need of Vulnerability Assessment and Penetration Testing is usually underestimated till now. It is just consider as a formality activity and use by very less people. By using regular and efficient Vulnerability Assessment, we can reduce substantial amount of risk to be attacked and have more secured systems.

In this paper we describe Vulnerability Assessment and Penetration Testing as an important Cyber Defence Technology. By using VAPT as a Cyber Defence Technology we can remove vulnerabilities from our system and reduce possibility of cyber-attack. We explained various techniques of Vulnerability Assessment and Penetration Testing. We described complete life cycle of VAPT for proactive defence. This will also provide complete process how to use VAPT as a cyber-defence technology.

Much research have been done by researcher in past in Vulnerability Assessment. Ivan Krsul[2] shows that computer vulnerability information shows important regularities and those can also be detected and possibly visualized. Steven E Noel[3] et al. find out the interdependency of multiple vulnerabilities and exploits in a single network and their effects. Stefan Kals[4] et al. show a web vulnerability scanner tool 'SecuBat' developed by them. Sushil Jajodia[5] and Steven Noel described a Topological Vulnerability Analysis approach. This analyses vulnerability interdependencies and possible attack path into a computer network. Christopher Kruegel[6] et al. present comprehensive study of "Execution after Redirect" Vulnerabilities.

The rest of the paper is organized as follows. Section 2 gives brief introduction of VAPT. Section 3 describes complete life cycle of Vulnerability Assessment and Penetration Testing. In Section 4, we describes various prevalent VAPT techniques. In Section 5 we have listed TOP 15 premium/open source VAPT tools. In section 6 we describe how we can use VAPT as an effective Cyber defence technology. Finally Section 7 concludes the paper and describe future work.

2. Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing is a step by step process. Vulnerability assessment is the process of scanning the system or software or a network to find out the weakness and loophole in that. These loopholes can provide backdoor to attacker to attack the victim. A system may have access control vulnerability, Boundary condition vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities etc.

Penetration testing is the next step after vulnerability assessment. Penetration testing is to try to exploit the system in authorized manner to find out the possible exploits in the system. In penetration testing, the tester have authority to do penetration testing and he intently exploit the system and find out possible exploits.

3. Life cycle of VAPT

Vulnerability Assessment and Penetration Testing is a total 9 step process[7 8]. These steps are shown in Fig. 1. First of all tester have to decide the scope of the assignment (Black/grey/white box). After deciding the scope, the tester gets information about the operating system, network, and IP address in reconnaissance step. After this tester use various vulnerability assessment technique (explained further) on the testing object to find out vulnerabilities. Then tester analyses the founded vulnerability and make plan for penetration testing. Tester uses this plan to penetrate the victim's system. After penetrating the system, tester increases the privilege in the system. In result analysis step, tester analyses the all results and devise recommendation to resolve the vulnerability from the system. All these activities are documented and sent to management to take suitable action. After these all step, the victim's system and its program get affected and altered. In cleanup step we restore the system in previous state as it was before VAPT process was started.

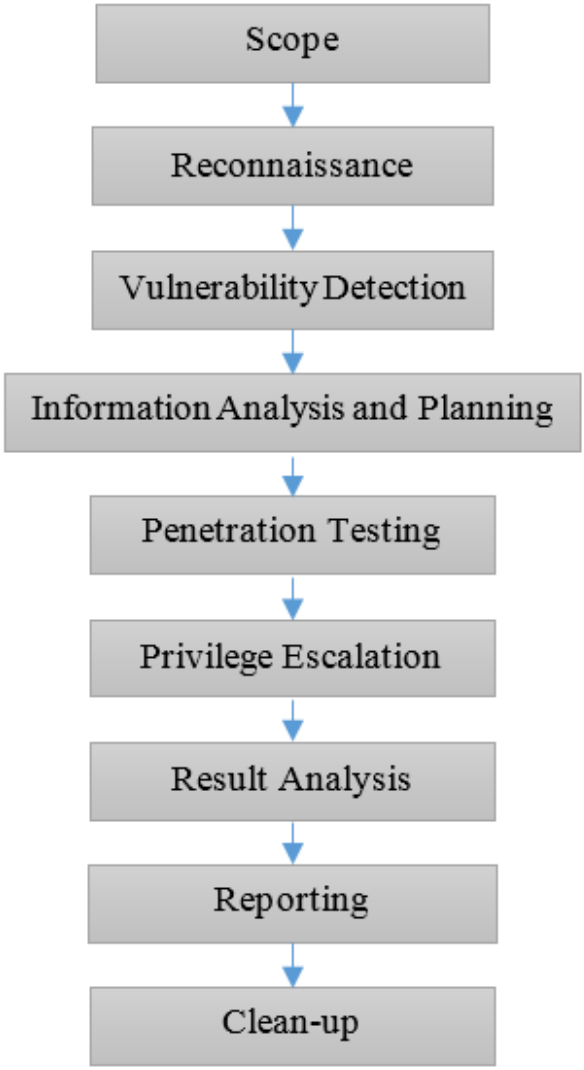

Fig. 1. Vulnerability Assessment and Penetration Testing Life cycle

4. Vulnerability Assessment & penetration testing techniques

4.1. Vulnerability Assessment technique

In this section we described some popular VAPT techniques[9].

4.1.1. Static analysis

In this technique we do not execute any test case or exploit. We analyze the code structure and contents of the system. With this technique we can find out about all type of vulnerabilities. In this technique we do not exploit

system, so there would be no bad effect of this testing on the system. One of the big disadvantage of this technique is that it is quite slow and require many men-hours to perform.

4.1.2. Manual Testing

In this technique, we do not require any tool or any software to find out vulnerabilities. In this tester use his own knowledge and experience to find out the vulnerabilities in the system. This testing can be perform with prepared test plan (Systematic manual testing) or without any test plan (Exploratory manual testing). This technique costs cheaper compare to other techniques, because we do not need to buy any vulnerability assessment tool for this technique.

4.1.3. Automated Testing

In automated testing technique we use automated vulnerability testing tools to find out vulnerabilities in the system. These tools execute all the test cases to find out vulnerabilities. This reduce the men-hours and time required to perform testing. Because of tool repeated testing can also be perform very easily.

Automated testing provide better accuracy than what other techniques provide. It takes very less time and same test cases can be used for future operations. But tools increase cost of testing. A single tools is not capable to find out all type of vulnerabilities. So this increase the total cost to perform vulnerability assessment.

4.1.4. Fuzz testing

This is also known as fuzzing. In this we inputs invalid or any Random Data into system and then look for crashes and failure. This is like robustness testing. This technique can be applied with very less human interaction. This technique can be used to find out zero day vulnerability.

4.2. Penetration testing techniques

4.1.5. Black box testing

In this technique, the tester do not have any prior knowledge of the network architecture or systems of the testing network. Usually black box testing is perform from external network to internal network. Tester have to use his expertise and skills to perform this testing.

4.1.6. Grey box testing

In this technique, the tester have some partial knowledge of the testing network. Tester do not have knowledge of complete network architecture, but he know some basic information of testing network and system configuration. Actually Grey box testing is the combination of both the other techniques. This can be perform from internal or external network.

4.1.7. White box testing

Tester have complete knowledge of the network configuration of the testing network and the system configuration of the testing network/system. Usually this testing is perform from the internal network. White box testing require deep understanding of the testing network or system and gives better results.

5. Vulnerability Assessment and Penetration Testing Tools

There are many open source/premium VAPT tools[10] available in the market. Every tool have its expertise and limitation. In Table 1 we have listed Top 15 VAPT tools, their usage and the operating system on which they are compatible. These make VAPT process fast and more accurate to assess and exploit vulnerability.

Table 1. Top 15 VAPT tools.

NO.	Name	License	Type	Operating System
1	Metasploit	Proprietary	Vulnerability scanner and exploit	Cross-platform
2	Nessus	Proprietary	Vulnerability scanner	Cross-platform
3	Kali Linux	GPL	Collection of various tools	Linux
4	Burp Suite	Proprietary	web vulnerability scanner	Cross-platform
5	w3af	GPL	web vulnerability scanner	Cross-platform
6	OpenVAS	GPL	Vulnerability scanner	Cross-platform
7	Paros proxy	GPL	web vulnerability scanner	Cross-platform
8	Core Impact	Proprietary	Vulnerability scanner and exploit	Windows
9	Nexpose	Proprietary	Entire vulnerability management lifecycle	Linux, Windows
10	GFI LanGuard	Proprietary	Vulnerability scanner	Windows
11	Acunetix WVS	Proprietary	web vulnerability scanner	Windows
12	QualysGuard	Proprietary	Vulnerability scanner	Cross-platform
13	MBSA	Freeware	Vulnerability scanner	Windows
14	AppScan	Proprietary	web vulnerability scanner	Windows
15	Canvas	Proprietary	Vulnerability scanner and exploit	Cross-platform

6. VAPT as a Cyber defence technology

In this section we will show how we can consider vulnerability analysis as a cyber-defence technology. What usually attacker do is he reconnaissance the victim's network and get information about victim's network. After getting information, attacker perform vulnerability assessment on the victim's network/system and get vulnerability list. This is shown in Fig. 2.

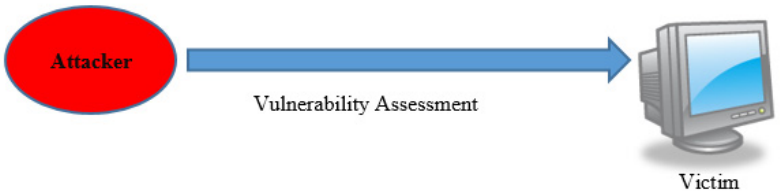

Fig. 2. Vulnerability Assessment by attacker

After getting the vulnerability list of the victim, the attacker make a plan for the possible attack. With that list attacker exploit the victim's network or system and compromise his system security and information. This is shown in Fig. 3. But if Victim removes all the vulnerabilities from his system, the attacker would not be able to exploit the victim's network/system. By applying VAPT technique user can find out the vulnerabilities those can result in various severe attacks like - DDoS attack, RA flooding, ARP poisoning etc. After finding out the vulnerabilities user can apply countermeasures[11 12] against them. To make the system vulnerability free, Administrator should find out vulnerabilities in his own system/network. The administrator should apply complete vulnerability and penetration testing cycle on the system/network. When the administrator would get the list of available vulnerability in his system, he should remove those vulnerabilities. To remove the vulnerabilities, the administrator should apply the necessary patches, updates, install necessary software and other requisite. In this way administrator would remove all vulnerabilities from his system/network.

Fig. 3. Attacker exploiting victim's system

Now if the attacker would do vulnerability assessment of the victim's system/network, he would not find any open vulnerability in the victim's system/network. In absence of open vulnerabilities in the system, the attacker would not able to exploit victim's system/network. So by using Vulnerability Assessment and Penetration Testing as a cyber- defence technology administrator can be able to save his resources and critical information and can achieve proactive cyber defence.

7. Conclusion and Future Work

In this paper we explained how Vulnerability Assessment and Penetration Testing can be used as an effective cyber defence technology. We described why VAPT should be made a compulsory activity for cyber defence. We explained complete life cycle of VAPT, prevalent VAPT techniques and top 15 vulnerability assessment tools. This paper provide complete overview of Vulnerability Assessment and Penetration Testing, and its use as a cyber-defence technology. This paper clearly explain necessity to increase use of VAPT for complete system security. This paper would be very helpful for future researchers to get complete knowledge of VAPT process, tools, techniques and its use as a cyber-defence technology. It would be helpful to develop new VAPT techniques and tools. This paper state VAPT as a powerful Cyber defence technology. Compulsory VAPT testing can stop cyber-attack cases and provide strengthen system security.

References

1. Owasp category: Vulnerability. 2015. URL: https://www.owasp.org/index.php/Vulnerability. Last Accessed: JAN 2015.
2. Krsul, I.. Computer vulnerability analysis: Thesis proposal 1997;.
3. Noel, S.E., O'Berry, B., Hutchinson, C., Jajodia, S., Keuthan, L.M., Nguyen, A.. Combinatorial analysis of network security. In: AeroSense 2002. International Society for Optics and Photonics; 2002, p. 140–149.
4. Kals, S., Kirda, E., Kruegel, C., Jovanovic, N.. Secubat: a web vulnerability scanner. In: Proceedings of the 15th international conference on World Wide Web. ACM; 2006, p. 247–256.
5. Jajodia, S., Noel, S.. Topological vulnerability analysis. In: Cyber Situational Awareness. Springer; 2010, p. 139–154.
6. Doupe´, A., Boe, B., Kruegel, C., Vigna, G.. Fear the ear: discovering and mitigating execution after redirect vulnerabilities. In: Proceedings of the 18th ACM conference on Computer and communications security. ACM; 2011, p. 251–262.
7. Vulnerability assessment and penetration testing (vapt). 2015. URL: http://memorize.com/vulnerability-assessment-and-penetration-te Last Accessed: JAN 2015.
8. Nist, usaid mission site vulnerability assessment and remediation. 2015. URL: http://www.nist.gov. Last Accessed: JAN 2015.
9. Shah, S., Mehtre, B.M.. An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques 2014;:1–23.
10. Sectools.org: Top 125 network security tools. 2015. URL: http://sectools.org/. Last Accessed: JAN 2015.
11. Tripathi, N., Mehtre, B.M. Analysis of various arp poisoning mitigation techniques: A comparison. In: Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on. IEEE; 2014, p. 125–132.
12. Goel, J.N., Mehtre, B.M.. Dynamic ipv6 activation based defense for ipv6 router advertisement flooding (dos) attack. In: Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. Dec 18-20, 2014, p. 628–632.