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.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
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

1877-0509 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
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.

Download English Version:

https://daneshyari.com/en/article/489709

Download Persian Version:

https://daneshyari.com/article/489709

Daneshyari.com