2015 4th International Conference on Software Engineering and Computer Systems (ICSECS), Kuantan, Pahang, Malaysia. August 19-21, 2015

Response option for attacks detected by Intrusion Detection System

Shahid Anwar
Faculty of Computer System and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
shahidanwar.safi@gmail.com

Jasni Muhamad Zain
Faculty of Computer System and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
jasni@ump.edu.my

Mohamad Fadli Zolkipli
Faculty of Computer System and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
fadli@ump.edu.my

Zakira Inayat
Computer Science and Information Technology
University Malaya
Kuala Lumpur, Malaysia
zakirainayat@nwfpuet.edu.pk

Aws Naser Jabir
Faculty of Computer System and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
PCC13011@stdmail.ump.edu.my

Julius Beneoluchi Odili
Faculty of Computer System and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
Odili_julest@yahoo.com

Abstract— **In past decades, we have seen that the increasing speed of the network attacks compromising computer system functionality and degrading network performance. The security of these systems has attracted a lot of research in the field of intrusion detection and response system to reduce the effect of these attacks. Response is a major part of intrusion detection system. Intrusion detection system without a timely response is not considered good even they detect threat and generate alarms. Optimum response is based on the selection of proper response option. In this paper, we categorize the attacks and propose some response option to thwart these attacks.**

Keywords— intrusion; attacks; information security; response option; intrusion detection;

I. INTRODUCTION

In recent years, due to technological advances, society has become more dependent on global networks for their social, business, and educational activities. Due to the explosive use of computer network a number of security issues have been raised in the internet and computer systems. The availability and integrity of computer systems need to be secure from a variety of threats. Annual report from the CERT (Computer Emergency Response Team) indicates a tremendous increase in the number of intrusion each year. According to MYCERT (Malaysian Computer Emergency Response Team) [1] report published in 2014, 43% of 9,986 malicious incidents have involved intrusions during system operational hours. An intrusion [2] is a set of actions that violates the security policies: the confidentiality and integrity of data, and availability of service by exploiting vulnerabilities in the security procedure and implementation of the monitored system by intrusion detection system (IDS). While attacks is a set of action that violate the security policies associated with the IDS itself [3]. It is therefore essential to have an appropriate IDS and intrusion response system (IRS) to detect and respond the potential intrusion and attacks.

An IDSs [2] are the hardware or software systems to automate the identifying and responding process of inappropriate events occurring in a computing system. Based on IDS alerts, IRS continuously monitors system health, so that potential incidents or inappropriate activities can be identified and handled effectively. IRS apply suitable countermeasure for ensuring security of computing environment [4]. The term "Intrusion tolerance " has been defined in [5] as a systems that maintain confidentiality, availability and integrity of computing system regardless of some of its components being compromise. However, the existing IDS have a limited response approach and are inadequate to give the optimum response to the detected intrusion. Therefore, for a good response, response option should be activated according to the nature of attacks and IDS confidence. For instance, all incidents are not malicious in nature, if a person gets access to a different system mistakenly by typing the address of a computer without authorization. However, if the same action is performed by a cyber-criminal, should be malicious as these are highly skilled programmers and can easily exploit the vulnerabilities of computer systems. Therefore, the IRS must be able to understand the malicious activity and choose the response option accordingly.

978-1-4673-6722-6/15/$31.00 ©2015 IEEE