Evaluation and Demonstration of the Usage of a Virtual Honeynet for Monitoring and Recording Online Attacks

Rajiv J. C. Ponweera[1], Ravindra Koggalage[2], Narada Wickramage[3]
Department of Computing, Informatics Institute of Technology, Sri Lanka
rajivjcp@yahoo.com[1], Koggalage@iit.ac.lk[2], narada@iics.ac.lk[3]

Abstract – **Even though the Internet has revolutionized our perception of global communications and business, it is also feared as one of the stealthiest threats to both individuals and organizations alike. The threats posed vary from simple port scans to the distribution of viruses, worms and the deployment of distributed denial of service attacks by malicious Hackers, also known as Blackhats. This project addresses the above problem domain and strives to provide a reliable mechanism to gather information of suspected and ongoing attacks through the implementation of a virtual honeynet. The acquired information could be used to build enhanced security measures against Blackhat attacks.**

I INTRODUCTION

The development of the Internet has revolutionized our perception of global communications. It has given birth to eCommerce and eBusinesses, both flourishing phenomena in the twenty first century. The technology which surrounds the Internet is both diverse and ever enhancing. However, the Internet is not without its drawbacks or weaknesses. The very same resource which provides inexhaustible assistance through connectivity and information is also feared as one of the stealthiest threats to both individuals and organizations alike. This is because of the existence of hackers who illegitimately attack or retrieve sensitive information from other Internet users. These individuals vary in skill and age ranging from predominantly teenaged novices known as 'Script Kiddies' [1,2] to mature and experienced 'Blackhats' [3,4]. The attacks initiated by Hackers include simple Port Scans [5], coordinated Denial of Service attacks (DoS), creation of Botnets and deployment of Distributed Denial of Service attacks (DDoS) [6,7], spreading of worms [8], viruses and malware, spamming, phishing [9,10] and the exploitation of known vulnerabilities of unpatched web applications [11,12] to gain sensitive information from victims.

II THE PROPOSED SYSTEM

In order to implement effective counter measures against Hackers and to thwart or prevent such attacks, it is essential to have a reliable mechanism to gather information of suspected and ongoing attacks. In answer to the above problem, this paper proposes the implementation of a customized Honeynet, which closely monitors various attacks so as to obtain detailed insight into various hacking methods and strategies. According to Lance Spitzner, a honeypot could be defined as a "*security resource whose value lies in being probed, attacked, or compromised"* [13]. It could be implemented to address a wide range of issues from intrusion detection to research. A Honeynet is a network of individual Honeypots which cooperate with each other to capture data efficiently. A Honeynet may be a physical implementation where all connected nodes are actual computers which run actual services or it could be a virtual network, which is simulated on a single computer and executes simulated Web based applications [14].

III THE AIMS

The main aim of this project is to develop and deploy a virtual honeynet, which offers simulated Web based applications in order to demonstrate and evaluate its suitability to monitor, record and analyze malicious activity. This mechanism would no doubt assist us to gain a better understanding of the methods and strategies used by hackers to compromise computer systems. The virtual honeynet consists of a collection of low-interaction honeypots. This essentially means that the applications running on the honeypots are simulations as opposed to being installed software. Furthermore, due to time constraints, the honeynet deals with the simulation of Web applications and the identification of attacks against popular Web servers only. Certainly, future enhancements could be made to simulate other applications and aspects of the honeypots. The Honeynet is capable of capturing, analyzing and recording incoming packets. Since Honeynets are not intended for any production purposes, the majority of traffic seen on the Honeynet is considered to be malicious. The system is also able to interact with attackers in a timely manner, by generating appropriate responses to the received requests. Since the applications are simulated, there is no real risk of compromise. Thus this paper presents an effective mechanism to study the strategies used by attackers in a secure environment. It is hoped that this paper would contribute towards the ultimate goal of honeynet technology, which is the identification of the physical location of attackers, so that law enforcement authorities could arrest the attackers, based on the data captured by the honeynet.

1-4244-1152-1/07/$25.00 ©2007 IEEE.