ABSTRACT

The development of technology in computer networks has boosted the percentage of cyber-attacks today. Hackers are now able to penetrate even the strongest IDS and firewalls. With the help of anti-forensic techniques, attackers defend themselves, from being tracked by destroying and distorting evidences. To detect and prevent network attacks, the main modus operandi in network forensics is the successful implementation and analysis of attack graph from gathered evidences. This paper conveys the main concepts of attack graphs, requirements for modeling and implementation of graphs. It also contributes the aspect of incorporation of anti-forensic techniques in attack graph which will help in analysis of the diverse possibilities of attack path deviations and thus aids in recommendation of various defense strategies for better security. To the best of our knowledge, this is the first time network anti-forensics has been fully discussed and the attack graphs are employed to analyze the network attacks. The experimental analysis of anti-forensic techniques using attack graphs were conducted in the proposed test-bed which helped to evaluate the model proposed and suggests preventive measures for the improvement of security of the networks.

Keywords: Anti-Forensics, Attack Graphs, Hackers, Network Attacks, Network Forensics

1. INTRODUCTION

Security of the networks has always been a major concern in the current era of technology. As the internet technology advances, cyber-attacks and threats evolve with new multiple phases such as multi-stage and multi-host strategies which are able to penetrate the most powerful firewall and IDS systems (Albanese, Jajodia, Pugliese, & Subrahmanian, 2011). Most of the companies spend large amount of their profit share to maintain a robust security system for the computer networks in their company. But, today’s defensive mechanisms are insufficient to tackle the multi-phase attacks. In order to investigate such kind of attacks and provide preventive and precautionary measures, a wide variety of tools and techniques are developed. Network forensics, the sub-category of digital forensics is trying hard to cope-up with the latest technology attacks. Both offline and live network forensics are needed jointly to trace back the attack path and find the source of the attacks. There are many approaches using various network monitoring tools and network security tools which help in detecting attacks.

DOI: 10.4018/ijdcf.2014010103
and threats. Through forensic investigation of the network traffic and packet capture, one can find the immediate source of the attack (IP address), thus discovering the location of the attacker. But the key area which is unnoticed during the investigation is the mode and the strategy of the attacks. The analysis of the attacks in a deeper way is best recommended to harden the network configuration.

The internet technology and network infrastructure are blessed with evolution of various IDS/IPS systems, powerful network monitoring and security techniques and systems. New approaches, methodologies and algorithms are developed for forensic investigations of network attacks. One of the main approaches is the reverse engineering methodology in which approximate attack path is found out with the help of attack graph algorithms. This approach dates back from the year 2002 where methodologies for generation of attacks graphs were first suggested. Attack graphs are designed to acquire the approximate strategy or modus operandi of an attack or threat. This may work for false negatives and true negatives as well. Using attack graphs, evidence can be detected and analyzed which leads to evidence graph generation. Evidence graph and attack graphs can be combined together to compute the attack strategies thereby estimating the preventive measures and enhancing the network security.

There are few major concerns about forensics. As most of the tools and techniques for forensics and anti-forensics are available open source and are exploited to a great extent, even by the script kiddies. Numerous tutorials are available on internet which provide handful of information about hacking and data theft (Kotenko & Stepanshkin, 2006). Another area is the incorporation of anti-forensics such as data hiding, hiding IP, network steganography, data destruction, obfuscation and log cleaning into attacks to hinder the investigation. One of the key drawbacks of network forensics is that they fail to prove the adequacy and integrity of gathered evidence (W. Wang & Daniels, 2008). The main challenge is in the evidence collection phase. As there are a lot of heterogeneous noisy evidences which need to be filtered. The key research is based on identification of relevant events and evidences of occurred attacks from various piles of evidence. Our research goal is to find out whether the existing evidence is enough for finding the source of attacks using evidence collected from the attack graphs. In the area of digital forensics, some forensic methods could find attackers, some could not. In this paper, we focus on the adequacy of evidence collected from attack graphs for identification of source, less than the amount of information, attackers cannot be found.

The sophisticated multi-staged cyber-attacks are one of the main challenges of network forensics. Since analysis of network attacks are mainly carried out manually which error prone and time consuming (O. Sheyner, Haines, Jha, Lippmann, & Wing, 2002). The analysis has to be made automated and incorporated in current defense mechanisms such as IDS and Firewalls. Intrusion Detection and Intrusion Prevention System (IDS/IPS), firewalls and various network security / monitoring systems are implemented at different nodes of the network. Thus helping in intrusion alerts and blocking attacks. Most of the attacks exploit vulnerabilities of network infrastructure and systems. The recent studies convey that hackers implement robust measures of anti-forensic techniques to conceal their identity and trace out path along with their normal attack strategies. Incorporation of anti-forensic techniques in network attacks, challenges the investigative process as they postulate ambiguity in attack mode and their paths. The key issue deals with differentiation of normal attacks and anti-forensic attacks. One of the methodologies for identification of such kind of attacks is the attack graph reasoning (Albanese et al., 2011).

Attack graph reasoning utilizes reverse engineering techniques used by the investigators for scrutinizing computer attacks in hierarchical way (Anming, Zhuhua, Cong, Jianbin, & Zhong, 2009). This methodology is the main part of the evidence process phase in network forensics. The major advantage of this approach is that one can easily locate the path, vulnerabilities
Age Detection Through Keystroke Dynamics from User Authentication Failures
www.igi-global.com/article/age-detection-through-keystroke-dynamics-from-user-authentication-failures/173780?camid=4v1a