Chapter XXII
Agents in Security:
A Look at the Use of Agents in Host-Based Monitoring and Protection and Network Intrusion Detection

Theodor Richardson
South University, USA

ABSTRACT

Network Intrusion Detection Systems (NIDS) are designed to differentiate malicious traffic, from normal traffic, on a network system to detect the presence of an attack. Traditionally, the approach around which these systems are designed is based upon an assumption made by Dorothy Denning in 1987, stating that malicious traffic should be statistically differentiable from normal traffic. However, this statement was made regarding host systems and was not meant to be extended without adjustment to network systems. It is therefore necessary to change the granularity of this approach to find statistical anomalies per host as well as on the network as a whole. This approach lends itself well to the use of emergent monitoring agents per host, that have a central aggregation point with a visualization of the network as a whole. This chapter will discuss the structure, training, and deployment of such an agent-based intrusion detection system and analyze its viability in comparison to the more traditional anomaly-based approach to intrusion detection.

INTRODUCTION

In what may seem to be a departure from the rest of this work, let us now deviate from agents and consider instead a networking problem that plagues security experts and network administrators alike; namely, the problem of intrusion on a network of machines. In brief, a network can be considered any number of machines connected together in such a manner that they are able to send signals to each other across the connecting medium in blocks of information called packets. Those of you versed in networking may wish to skip to the next paragraph, but for those of you unfamiliar with this particular venue, this is accomplished via protocols, or sets of formal rules governing how information is structured in an exchange either per packet or

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

across several packets; such rules are necessary to allow machines to communicate regardless of operating system. These protocols are common knowledge and therefore, if someone wishing to send unwanted information on a network had access to the physical media, it would be trivial to structure the information to allow it to be transmitted successfully. Considering the fact that most modern networks are connected to the Internet, the question of anyone having access to the network becomes a very moot point. Sending unwanted information on a network is known as an intrusion.

This goal of detecting intrusions on a network presents a complex problem spanning multiple levels of interaction and varied host behavior. The traditional approach to detecting intrusions is to look at network behavior statistically and attempt to determine significant deviations from the expected behavior of the network as a whole. This type of approach, around which these Network Intrusion Detection Systems (NIDS) are designed, is based upon an assumption made by Dorothy Denning in 1987 stating that malicious traffic should be statistically differentiable from normal traffic; however, this statement was made regarding host systems and was not meant to be extended without adjustment to network systems. While this is viable under certain types of attack, such as a botnet attack or slammer worm, it is insufficient to detect more advanced types of attack that may not trigger a statistical amount of errant traffic. Similarly, network traffic is rarely predictable, meaning there will often be false alarms in such statistically based systems. Even if the traffic is broken into seasonality, or predictable periods of expected activity such as higher traffic during the typical nine to five work day, it is unlikely to produce the desired effect. It is therefore necessary to change the granularity of this approach to find statistical anomalies per host as well as on the network as a whole.

To that end, this chapter proposes the use of emergent agents deployed on each host in the network to find a seasonal baseline of activity for the host itself; these hosts will then report in aggregate to a more traditional NIDS device that will compile a view of the network as a whole and determine if there is suspicious activity present on the network as a whole. This combined approach will provide a comprehensiveness and robustness not currently present in most NIDS systems. This is an example of second emergence, where the emergent behavior is routed back into the system to enhance the emergent result.

The remainder of this chapter is structured to provide an understanding of network intrusion detection systems and how social agents can be applied to this problem. The first section provides an overview of the various approaches to NIDS that currently exist along with a discussion of their relative strengths and weaknesses. The second section presents a formulation of the fundamental problem of determining whether a network has been compromised. The third section describes the methodology used to approach this problem through the use of agent-based monitoring and the socialization. Fourth, the experiments performed to validate the approach are described and Section 5 the final section presents a brief conclusion.

BACKGROUND

Intrusion Detection Systems (IDSs) take many forms and approaches to detection and possibly prevention or recovery, ranging from open source applications such as Snort to extremely expensive dedicated appliances such as Cisco IDS. The fundamental characteristic that defines the two major types of intrusion detection systems is the granularity of the observation: namely, the two types are host-based systems and network-based systems. Both types share many characteristics along with the same fundamental goals but implement them in very different ways.

The essential thing to remember is that there is no silver bullet in security and an IDS of any type should be one line of defense in a multi-tiered strategy. The goal of any such intrusion detection system is to detect anomalous network behavior in an approximation of real time to minimize the damage to the network. Network-based intrusion detection systems (or simply Network Intrusion Detection Systems or NIDS) are used to detect malicious activity across an entire network viewed as a whole. The typical model for this is to have a central aggregation point that collects all traffic sent over

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/agents-security-look-use-agents/19635

Related Content

Autonomous Seller Agent for Multiple Simultaneous English Auctions
Patricia Anthonyand Edwin Law (2012). *International Journal of Agent Technologies and Systems (pp. 1-21).*
www.irma-international.org/article/autonomous-seller-agent-multiple-simultaneous/69522

How Ants Can Efficiently Solve the Generalized Watchman Route Problem
Pawel Paduchand Krzysztof Sapiecha (2013). *Recent Algorithms and Applications in Swarm Intelligence Research (pp. 193-208).*
www.irma-international.org/chapter/ants-can-efficiently-solve-generalized/70647

A Home Agent Initiated Handover Solution for Fine-Grained Offloading in Future Mobile Internet Architectures: Survey and Experimental Evaluation
László Bokor, József Kovácsand Csaba Attila Szabó (2014). *International Journal of Agent Technologies and Systems (pp. 1-27).*
www.irma-international.org/article/a-home-agent-initiated-handover-solution-for-fine-grained-offloading-in-future-mobile-internet-architectures/109600

A Generic Internet Trading Framework for Online Auctions
Dong-Qing Yao, Dong-Qing Qiaoand Haibing Qiao (2007). *Application of Agents and Intelligent Information Technologies (pp. 272-290).*
www.irma-international.org/chapter/generic-internet-trading-framework-online/5117

Multi-Agent Systems Engineering: An Overview and Case Study
Scott A. DeLoachand Madhukar Kumar (2005). *Agent-Oriented Methodologies (pp. 317-340).*
www.irma-international.org/chapter/multi-agent-systems-engineering/5063