IDEA GROUP PUBLISHING **ITB12238**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter XVI

Intrusion Detection and Response

David A. Dampier, Mississippi State University, USA

Ambareen Siraj, Mississippi State University, USA

Abstract

This chapter discusses the notion of intrusion detection and introduces concepts associated with intrusion detection and methods used to respond to intrusions. It presents information about different forms of intrusions and how they are recognized. It introduces methods for detecting intrusions and then discusses possible responses to those intrusions. It is hoped that this information will make the readers more aware of the possibility of intrusions and how they might develop a process for detecting and responding to these intrusions.

Introduction

Foremost on any executive's mind is the security, privacy, and protection of the suite of information resources within his or her scope of responsibility. Few would question the potential threat that exists to every business, government, academic, or private computing system today or dismiss this concern as unworthy of attention. CEOs, CIOs, COOs, CFOs, and CKOs[1] are all being asked to provide assurances to the corporate board, stockholders, business partners, government regulators, and other stakeholders that the information assets of the business are reasonably protected. This is not simply an issue of confidentiality — it is an issue of privacy, compliance with the law, protection of key corporate assets, and duty.

In securing one's systems, actions must be taken in three areas — prevention, detection, and response. All three are important and necessary, and no one of them will suffice completely. Simply stated, prevention involves all those actions one must take to attempt to prevent unauthorized access to a system; detection involves those actions taken to discover failures in prevention (realizing that 100% prevention is never possible); and response includes those actions taken by the enterprise after discovering an attack, attempted attack, or damage. Response is generally considered to include recovery measures, but might also include efforts to uncover what has been done to the system in the attack and how it was done. This is what is known as computer forensics. In its 2000 report titled "Enabling Technologies - Cyber Security," the Government Electronic Industry Association (Skinner & REEL, 2000) chose to illustrate these three areas, as depicted in Figure 1.

This chapter focuses on one "point solution" detection technology known as *intrusion detection systems* or IDS. We refer to this as a "technology" rather than a product, because it is a suite of different techniques that can be implemented in a host and IDS functionality exists to various degrees in many products available today from the private sector. The purpose of this chapter is to discuss, at an introductory level, the techniques and capabilities that one should expect to find in a modern intrusion detection system. We wish to make clear, however, that intrusion detection is simply part of an overall

Figure 1. Prevention, detection, and response (Source: Skinner & REEL, 2000)