



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.

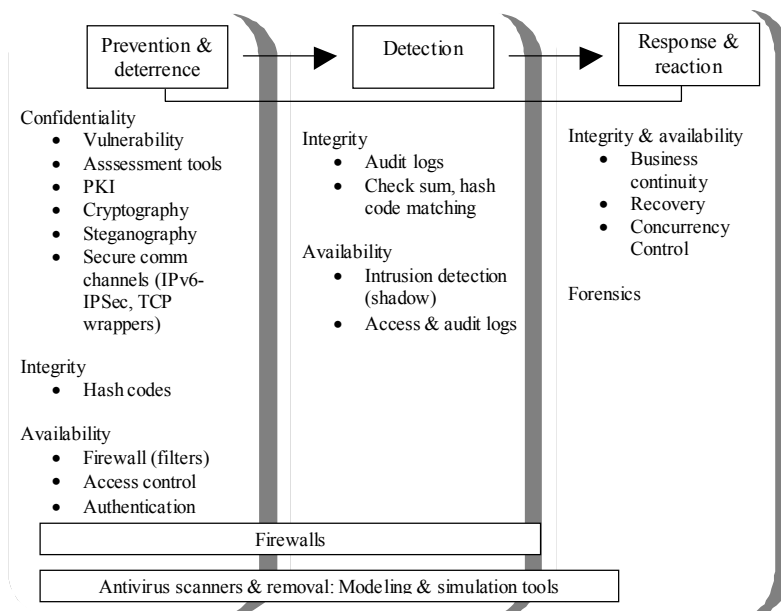
Introduction

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 CKOs¹ 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)



11 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/intrusion-detection-response/18392

Related Content

Management and Control of Intelligent Optical Networks

Dimitrios Pendarakis and Subir Biswas (2002). *Enterprise Networking: Multilayer Switching and Applications* (pp. 31-47).

www.irma-international.org/chapter/management-control-intelligent-optical-networks/18414

An Effectiveness Model for Enterprise Architecture Methodologies

Babak Darvish Rouhani, Mohd Naz'ri Mahrin, Hossein Shirazi, Fatemeh Nikpayand Bitá Darvish Rouhani (2015). *International Journal of Enterprise Information Systems* (pp. 50-64).

www.irma-international.org/article/an-effectiveness-model-for-enterprise-architecture-methodologies/132708

Toward UML-Compliant Semantic Web Services Development

Diana M. Sánchez, César J. Acuña, José María Caverio and Esperanza Marcos (2010). *International Journal of Enterprise Information Systems* (pp. 44-56).

www.irma-international.org/article/toward-uml-compliant-semantic-web/39047

The Creation of a Commercial Software Development Company in a Developing Country for Outsourcing Purposes

Sam Lubbe (2007). *Managing Information Communication Technology Investments in Successful Enterprises* (pp. 126-136).

www.irma-international.org/chapter/creation-commercial-software-development-company/25855

A Fuzzy ANP-Based GRA Approach to Evaluate ERP Packages

Zeki Aya and Ahmet Yücekaya (2019). *International Journal of Enterprise Information Systems* (pp. 45-68).

www.irma-international.org/article/a-fuzzy-anp-based-gra-approach-to-evaluate-erp-packages/220398