Chapter 58
Intrusion Prevention System

Bijaya Kumar Panda
GITA, India

Manoranjan Pradhan
GITA, India

Sateesh Kumar Pradhan
Utkal University, India

ABSTRACT

In the last decade, there is a rapid growth in the use of Internet by the organization for information sharing. As information is very vital to the organizations, it should be preserved and insulated from any unauthorized access or alternation. In last few years, attacks on the computer infrastructures have increased exponentially. Several information security techniques are available now a days like firewalls, anti-virus software and Intrusion prevention systems (IPSs), which are important tools for protecting an organization from intrusions. Now most attacks are impossible to defend with firewalls and anti-virus software alone. Without an IPS, such attacks are difficult to detect and prevent. This chapter presents different definitions of intrusion prevention system with meaningful explanation; compare network IPS with Host IPS, common and the advanced detection methods, common IPS components, coverage of attacks by IPS and criteria to select right IPS. Finally, this chapter concludes with an analysis of the challenges that still remain to be resolved.

INTRODUCTION

In the last decade, there is rapid growth of communication networks through computers and Internet. The numbers of Internet users are also rapidly increasing for business applications, other online applications and services. With the rapid growth of internet communication and availability of tools to intrude the network, network security has become indispensable. Security threat comes not only from external intruder but also from internal misuse.

Security and protection of computer networks and their resources is one of the most important IT activities today. Most organizations no longer take for granted that their deployed networks and appli-

DOI: 10.4018/978-1-5225-9866-4.ch058

cations are secure and therefore use all kind of protection tools and products. But, even after installing various protection mechanisms, performing continuous monitoring of security logs, and running extensive penetration tests, network and hosting security personnel spend considerable time chasing incidents, preventing penetrations or solving problems after intrusions and damages. More or less everybody has already realized that the "secure the perimeter" approach does not prevent the tide of incidents, intrusions and damages, because current techniques and products do not provide effective solutions. Over the last several years, the trends and styles of intrusions have been changing (CERT, 2007). Intrusion profiles have enhanced from simple methods like tracing passwords, social engineering attacks (Bishop, 2005), and exploiting simple software vulnerabilities to more sophisticated methods, like exploiting protocol flaws, defacing web servers, installing snifter programs, denial of service attacks, distributed denial–of–service attacks, or developing command and control networks using compromised computer to launch attacks. CERT Coordination Center confirmed in the "Recent CERT/CC Experiences Vulnerability Report" (CERT, 2008) that there has been significant exponential increase in discovered vulnerabilities: 171 in 1997 to 7236 in 2007. This increase in vulnerabilities and intrusion profiles has also dramatically increased the number of security incidents in past few years. These statistics show an alarming situation in which expertise of intruders is increasing, complexity of network and system administration is increasing, ability to react fast enough is declining significantly and along this, vendors continue to produce software with inherent vulnerabilities. In addition to direct attacks and penetrations by humans (hackers or insiders), one of the additional rising problems in today's networks is the existence of malicious bots and bot networks (Security, 2007). Most botnets are created to conduct malicious actions such as conducting Denial of Service (DoS) attacks, stealing user identities, installing keyboard loggers to record keystrokes, or generating e-mail spam.

The network security is to protect the networks and their services from unauthorized modification, destruction or disclosure. It is the process of preventing and detecting unauthorized access to data or resources across the network. It involves all activities that organization, enterprises and institutions undertake to protect the value of asset and the integrity and the continuity of operation. The security strategy requires identifying threats and then choosing the most effective set of tools to combat them. The security risks to be managed are unauthorized access to data and unauthorized use of system resource.

Current security policies do not sufficiently guard data stored in an information system against privileged users. Intruders who have gained super-user privileges can perform malicious operations and disable many resources in the information system. Many other mechanisms and technologies like firewalls, encryption, authorization, vulnerability checking and access control policies can offer security but they are still susceptible for attacks from hackers who take advantage of system flaws and social engineering tricks. In addition, computer systems with no connection to public networks remain vulnerable to disgruntled employees who misuse their privileges.

These observations result in the fact that much more emphasis has to be placed on Intrusion Detection and prevention System (IDPS) to protect the system from intruders

BACKGROUND

Stallings & Brown (2008)defined computer security that deals with computer related assets that are subjected to a variety of threats and for which various measures are taken to protect those assets.