Design and Implementation of Intrusion Detection System

Tai-ping Mo and Jian-hua Wang

School of Electronic Engineering & Automation,
Guilin Univ. of Electronic Tech., Guilin 541004, China
{mtp,wjh}@guet.edu.com

Abstract. This paper have a research on intrusion detection technology , by analyzing the composition and implementation of intrusion, we designed a network intrusion detection system model: network packet capture - analysis of data package - key elements of the data packet matches with the rule base - causing alarm. under VC++6.0 and Access 2000 environment, we designed and implemented a network intrusion detection system. The experiment result show the system can detect both known intrusions and the new intrusion. What's more it can notify users to deal with problems immediately.

Keywords: intrusion detection, rules base, invasion.

1 Introduction

Since James P. Anderson detail the concept of intrusion detection for the first time in his book "Computer security threat monitoring and surveillance"[4] in 1980. The intrusion detection system has made a significant progress. As more and more companies began to turn their business to network, network security has become an unavoidable problem. With the maturity of the attacker skills, the complication and diversity of attack tools and techniques, the simple firewall technology has been unable to meet our needs. At the same time, network environment has become more complex. Hardware equipment, software systems need to constantly upgrade and worker's carelessness could cause a major security risk. Intrusion Detection System is in accordance with a certain degree of security policy, through software, hardware, network, the status of the system to found all kinds of attack attempts, aggressive behaviors or attack results, so as to ensure the network resources confidentiality, integrity and availability.

Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS) are the most popular IDS, and the appliance of them are most widely. Network intrusion detection system is more common so this paper has design and implement it. Network intrusion detection technology is a kind of dynamic secure technology, and it is an important part in the security protection system. Firewall is a static security and defense technology well as network intrusion detection system is dynamic. It can detect network intrusion events and processes and make real-time response. Working with network firewall, NIDS become the core of network security equipment.

M. Ma (Ed.): Communication Systems and Information Technology, LNEE 100, pp. 303–308.
springerlink.com

2 IDS and NIDS

IDS is a combination of software and hardware and have function of intrusion detection. Through Collecting and analyzing some key points of computer network or computer system, IDS can discover whether the network or system have violation or attack. The data will be analyzed, then useful results can be obtained.

The main function of IDS include: Monitor and analyze users' and systems' activities, Verificate system's configuration and vulnerability, Assess critical resources of system and data integrity of the files, Identify of the known attacks, Statistic and analysis of abnormal behavior and Manage the log of the operating system.

IDS always contains information collection and data analysis. IDS Can be divided into host-based and network-based. Among them, host-based intrusion detecting systems (HIDS) are often through selecting system log, application log as data source, or through other means (such as calls of the monitoring system) to gather information from the host; Data source of network intrusion detecting system (NIDS) is packets on the network, NIDS often set a NIC of one machine into promiscuous mode, monitor data packets and make judgments.

In the shared network, NIDS monitor communications and do data collection, analysis of suspicious phenomenon. Fig. 1 illustrates the principle of it's implementation. Compared with HIDS, NIDS is transparent to the invaders. There is two kinds of NIDS's operation, one is running on the target host to monitor the communications of its own information, the other is runing on a separate machine to monitor all network communication and information devices, such as the Hub, router. NIDS including packet capture, protocol decoding and matching modules. It is always run at real-time status to detect possible intrusions any time. NIDS has high detection speed, better for hiding, wide field of vision, less use of resource of monitor and many other advantages.

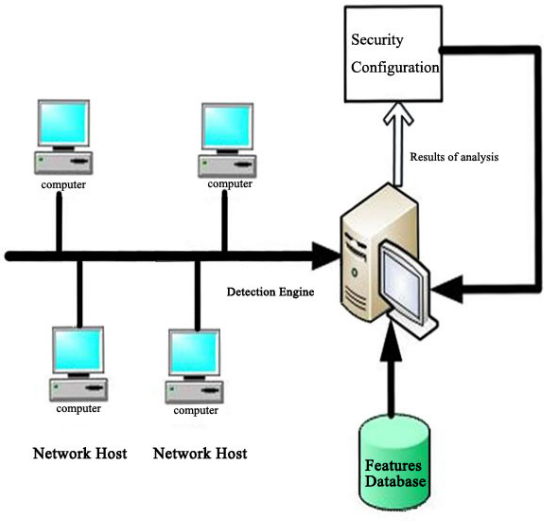

Fig. 1. Implementation principle of network intrusion detection system(NIDS).