Research and Design of Intrusion Detection System in Computer Network

Xiaohui ZHANG
Tangshan Industrial Vocational Technical College
Tangshan,Hebei,China

***Abstract*—This paper combines the design of the intrusion detection system based on host and based on network. According to various intrusion detection technology, the paper focus on the mechanism of integration, cooperation, selective of intrusion detection system, so as to achieve the optimization method is introduced to intrusion detection system, put forward a kind of intrusion detection system based on a variety of detection methods and technology, and establish the overall structure of integration, cooperative, selective, so as to achieve the system optimization, and make the network system security really get better effect.**

Keywords: Network security; Intrusion detection system; security technology;

I. INTRODUCTION

With the development of computer network, protection of network information from various attack becomes more and more important. But because the computer network has form of diversity, uneven distribution of the terminal characteristics and network openness, system interconnection, resulting that the computer network is vulnerable to hackers, malicious software and other misconduct attack, network security has increasingly become the key factor restricting the development of the network. With the improvement and development of technology of network security, network security, from the point of view of stereoscopic depth, multi-level defense point, the intrusion detection system and technology is great importance, but because of the intrusion detection technology is not mature enough, and be in the stage of development. Therefore, it is necessary to carry out in-depth comprehensive research on the intrusion detection technology.

Intrusion Detection System (IDS) is an important part of information security architecture, which is a necessary supplement to the firewall, is a kind of active security technology, according to the number of key points to collect information of computer network or computer system and its analysis, monitor the host system or a user activities on the network, find out if there is a breach of security strategy of network or system and the possible intrusion behaviors. Intrusion detection system divided into two types based on host and network accordance with the data source, intrusion detection analysis technology is mainly divided into anomaly detection and misuse intrusion detection.

II. THE DESIGN OF SYSTEM FRAMEWORK

According to the system work and complete tasks in different stages, different system logic is divided into several modules such as shown in Figure 1 below. The system framework is designed training phase and the testing phase, the system analyze training data in the training phase, get the pattern rules, stored in a database (SQL), using the model library test and analyze real-time network data in capture detection stage, results will be presented to the system response module for further processing. The work implement by Control center module scheduling by unified interface.

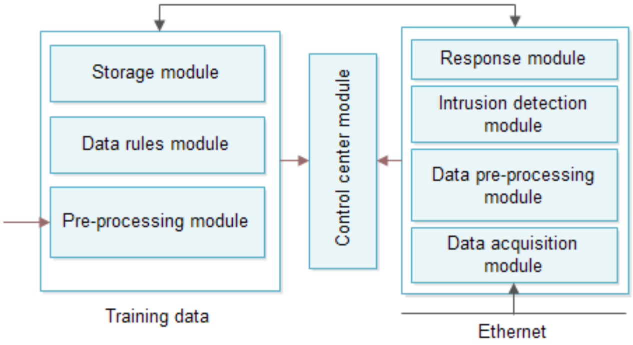

Fig.1 The structure of the network intrusion detection system

(1) Control center

The center is the core of the system model, the control logic of the system is generated by the module. In order to improve the system efficiency, but also upgrades and maintenance for future, the function of the logical system used separate by the control center work, make a general allocation and scheduling. This module defines the general function control interface process, at the same time defined in charge of control function between other internal modules and module work normally. All system functions are from the module defined several categories: data capture class, data preprocessing class, data analysis and response action class. It is realized mainly through the visual system management interface and management of these classes.

(2) Data capture

The detection stage work in data capture system. The logic includes network data packet capturing thread and host system call capture thread. Network packet capture thread takes network data as data source, program introduced Libpcap development package, to achieve real-time capture of network data flows through the network card packet, and packet type according to the captured data, initial corresponding processing operation, complete binary conversion work and initial data storage.

(3) Data storage

Storage system recorded events detects by the system, in order to facilitate the subsequent analysis. Special storage system construction can improve the reaction rate, but it is a very expensive thing. So we choose the existing database systems to build storage system. The existing database systems support SQL query, it to search package makes the analysis system can use common connection. According to the size of the intrusion detection system, storage system also has the very big difference, it may be a single data file storage system, may also be a database system for the large-scale intrusion detection system, and it would be possible to configure a data warehouse that is as its storage system.

(4) Rule description

The module uses a rule description language to describe the attack signature and corresponding countermeasures, the language take example by the Snort language grammar. At the same time, the system uses a very flexible, efficient, simple rules of storage, easy to use fast pattern matching detection module, for improving the overall efficiency of IDS play a very important role. System design rules analysis processing algorithm flow is as shown in figure 2:

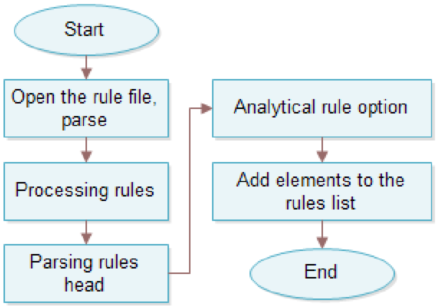

Fig.2 The process of rules analysis processing algorithm

```
//NIDS main rule list
typedef struct_ RuleListNode
{
RuleHeadNode *rhnptr; / / rule head
RuleOptNode *ronptr; // rule option
Int active_ flag; / / rule activation marker
Int rule_ num; // rule number
Int Ron num; // the number of rules options
Char *ron_name; //name rule option
Struct-uleListNode *next;
} RuleListNode;
The rules of //NIDS head
Typedef struct RuleHeadNode
{
Int type; / * head type rules (rule action) * /
Int proto; // protocol type
IpAddrSet *sip; / * source ip*/
IpAddrSet *dip; / * to ip*/
U_int16_t sort; // source port
U_int16_t d}ort; // destination port
} RuleHeadNode;
```

III. The Design of Intrusion Detection Module

A. *Protocol decoding*

Purpose of protocol decoding is to get the IDS right intrusion detection. It decode correctly and accurately the TCP/IP protocol, and turn into another kind of code form or data structure that is convenience for intrusion detection.

B. *The protocol analysis module*

The protocol analysis module is mainly the features of network against shown by the specific attacks. Protocol analysis using high order of the network, and combine high speed packet capture, protocol analysis and command parsing, to rapidly detect a whether attack exists.

Protocol analysis package process and protocol stack is as shown in following figure 3.

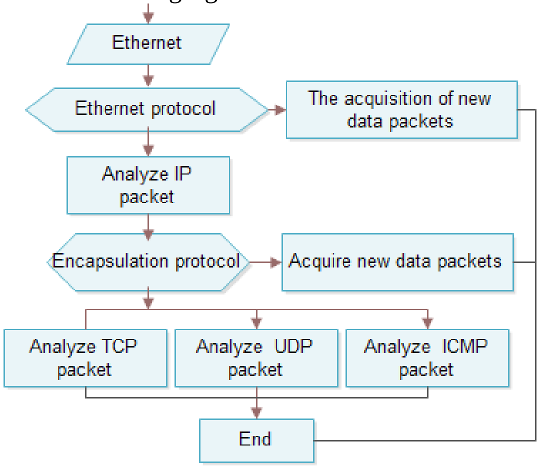

Fig.3 Procedure of protocol analysis

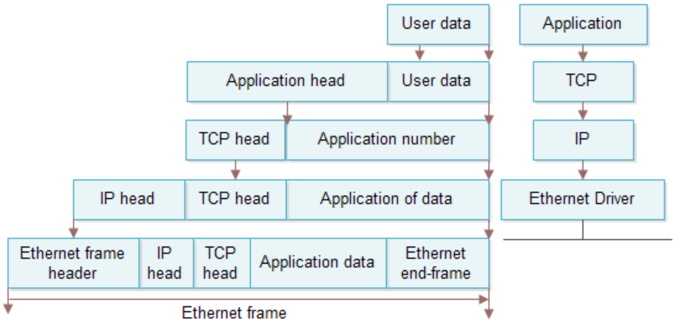

Fig.4 The encapsulation process of the protocol stack

C. *The data preprocessing module*

In the training phase, the data processing module mainly completes the preprocessing of the network training unlabeled data , training data will be numerical value, remove redundant attributes and data storage, as well as to preprocess operations for host the training data, such as data conversion, filter etc..

D. *The system response module*

Response is response actions when the intrusion detection system detect intrusion behavior. The response of the intrusion detection system is divided into two types of active response and passive response. Analysis of response technology: response of intrusion detection system is divided into two types of active response and passive response. In active response, intrusion detection system should be able to automatically (or under the control of the user) blocking or influence the attack, and then change the attack process. In a passive attack, intrusion detection system simply reporting and recording the detected problem.

E. The communication between modules

In this module, we mainly use socket communication mechanism and multi thread technology between processes. Communication diagram between modules is shown in Figure 5.

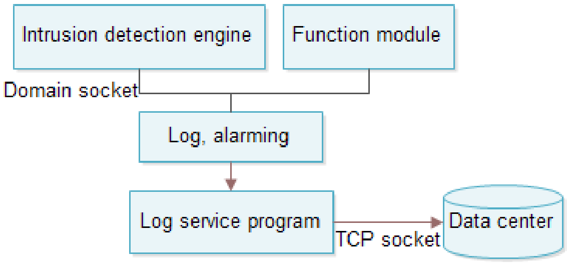

Fig.5 The communication principle between modules

IV. The Work Flow of System

The system can run under the WinXP platform, and provides a friendly user interface for system administrators. The user set the initial value to determine the system working mode. When the system runs, can library function call message mapping mechanism of concrete, so as to complete a series of specific operation. If the current packet conforms to a detection rules specify conditions, mode response system can according to the rules defined and output (Output) initialization definition module, log and report with operation. The concrete work flow chart is as shown in figure 6.

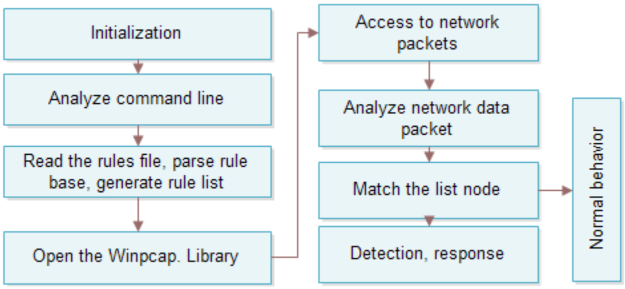
Initialization
Analyze command line
Read the rules file, parse rule base, generate rule list
Open the Winpcap. Library
Access to network packets
Analyze network data packet
Match the list node
Detection, response
Normal behavior

Fig.6 The work flow chart of the system

V. Conclusions

Intrusion detection system is an important safety assistant system, it is an important part of the PPDR model. Intrusion detection is as a proactive security protection technology, provides real-time protection to internal attack, exterior attack and misoperation, which intercept and is response to the intrusion before the network system is endangered. Starting from the three-dimensional depth of network security, multi-level defense point, intrusion detection has attracted high attention. Therefore, this research mainly aims to establish the information security assurance for the enterprise to provide theoretical and technical support system.

Reference

[1] Zhang Wen. Design and Realization of dynamic password identity authentication system [J]. Micro computer information, 2005.3

[2] Huang Zhan, Cao Wangxi. Application of dynamic password technology in network security [J]. Computing technology and automation, Volume 22, 2003 11

[3] Qian YuE. Study on the technology of firewall [J]. Journal of Simao Normal College, Vol. 21, 2005.3

[4] Peng Zhuofeng, Application of firewall technology [J]. popular science, 2004 4 period

[5] Jing Su Liu Yuejun. Design and implementation of packet filtering firewall [J]. Journal of Anyang Normal University, 2003.5

[6] Qi Lanlan Sun Lechang. Firewall technology and information security [J]. Anhui electronic information, Journal of Career Technical College, Vol. 3 2004 5