Design of the Computer Intrusion Detection System

Hui Liu

Weifang University of science & technology Shouguang City,Shandong Province 262700 China.

Keywords: Intrusion detection; The response module; The system design ; Test

Abstract: From the definition and the invasion of intrusion methods, this paper summarizes the root cause of network security incidents. Then various intrusion detection methods are analyzed. Finally the overall scheme of the intrusion detection system is designed and the intrusion detection system test is completed.

Introduction

In recent years, with the rapid development of modem information and network technology and other interests of the drive, computer and network infrastructure, especially the various official website has become a target for hackers, in recent years because of the aspirations of e-commerce, more intensified the various intrusion growth trend. As a network security protection tool, "firewall" is a major supplementary measures, Intrusion Detection System (Intrusion Detection System, IDS) obtained the swift and violent development.

Invasive definition and the method

The invasion of definition. Anderson in the early 80s, using the concept of "threat" terms, the definition and the invasion of the same meaning. Defines intrusion attempts or threats as unauthorized deliberately try to access information, tampering with information. The system is not reliable, or cannot use.

Invasions Heady gives another definition: refers to the attempt to wipe out the integrity of the resources, confidentiality and usability of collection activities.

Invasion method. 1) Network monitoring

Monitoring network was originally intended to help network administrators to monitor network transmission of data, network fault and the advance of technology, network monitoring, however, it also brought tremendous to Ethernet security hidden danger. Listening is through the network interface set to mix mode, so as to receive after it's all network packets, achieving the goal of peeping in other host communications network.

2) Port scanning

The basic principle of port scanning is scanned by the target system to different port to send packets that have a special place, and record the target response, through the analysis of the relevant information about the target.

The packet types can be subdivided into: TCP, UDP, ICMP scanning scan. TCP scans including: TCP connect () scan, TCP SYN scan, TCP SYN ACK scan, TCP ACK scan, TCP FIN scan, TCP empty scan, TCP Xmax tree scan (the target port sends a set FIN URG PUSH a packet.) ; ICMP scanning include ICMP query request and response message scanning, scanning the ICMP error message; UDP scanning include inaccessible UDP port scanning, etc.

3) Password invasion

Password invasion refers to the attacker using the authorized user account and password to login to the target host, and then attack behavior. Attackers by speculation, listening and decoding users' password for the host or network access, log on to the target system access to resources to install the back door, etc.

4) A Trojan horse

A Trojan horse program is to point to illegal stay in the target system, providing a private program which users want. A Trojan Horse program can be used to steal the target system of sensitive information (such as a user name and password), record users' keyboard operation, until the remote control of the target system. Trojan horse programs generally adopt client/server mode, host to the target system of the program as the server side, receiving the client (in the hacker's host) control command. To take advantage of a Trojan horse program, the key point is how to make a Trojan horse program resides in the target system, which generally requires the use of deception to let users execute a program on the target system or an action to complete the installation of a Trojan horse program. Hackers often after a successful invasion in the target system install a Trojan horse program in order to control the target system for a long time.

Prevention methods: check the system running in the service or open port, if the new service program for running or strange port is open, it should further clarify a new service or a Trojan horse program of normal boot. In order to carry on system boot automatically start every time, Trojan horse program must want to modify the registry entries, so checking the registry can be found, a Trojan horse program has special status and modifies the software to record system to prevent and can prevail against illegal modification.

Intrusion detection technology

The basic structure of the intrusion detection system. Common Intrusion Detection framework (CIDF) (Common Intrusion Detection Frame, Common Intrusion Detection framework) put forward the general model of Intrusion Detection system can be divided into four basic components: the event generator, event analyzer, response unit and the event database, see below（Fig. 1）

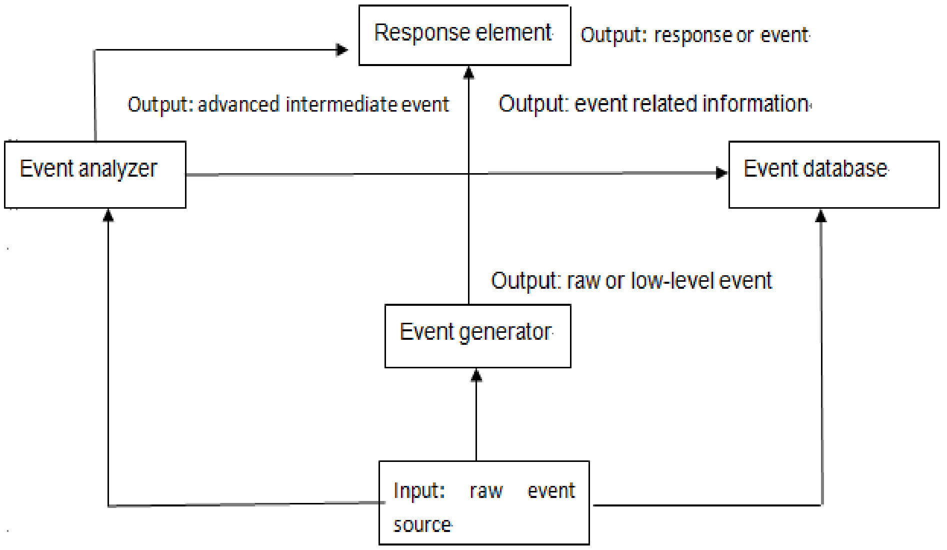
Response element
Output: response or event
Output: advanced intermediate event
Output: event related information
Event analyzer
Event database
Output: raw or low-level event
Event generator
Input: raw event source

Fig. 1 The common intrusion detection framework (common intrusion detection framework (CIDF) architecture

Intrusion detection method. 1) Pattern matching

Pattern matching is part of the traditional intrusion detection method which the most simple. The method to construct the attack characteristic library and to check whether the received data contain features in the library attack, so as to determine whether it is attacked. Its simple algorithm and high accuracy can only detect the known attacks, slightly modifying to know attack which can avoid detection, omission phenomenon which is serious. Model needs to be updated continuously. For large-scale networks, by analyzing a large number of data packets, the speed of this method has become a problem.

2) Protocol analysis

Protocol analysis is intelligent extension of pattern matching. It uses the height of the network protocol regularity rapid detection of attacks. Its remedy some of pattern matching technology is put forward, such as huge amount of calculation and low detection accuracy. In addition, protocol analysis can detect attacks. For example: Suppose an attacker executes the basis of the agreement is fictional BGS, attack illegal variable for must be passed to the BGS type field. If the BGS agreement allows every byte to be blank, it is not be able to find fx00o x00o x00 schema matching, on the contrary, protocol analysis is able to skip the null bytes and sound the alarm on schedule.

3) Expert system

Using expert system based on the rules of the language is known to attack modeling, it put the audit events into semantic expression, inference engine according to the rules and facts. The establishment of the expert system relies on the integration of the knowledge base. Knowledge base completeness depends on the real time and completeness of audit records.

The system overall design

System overall structural framework（Fig. 2）

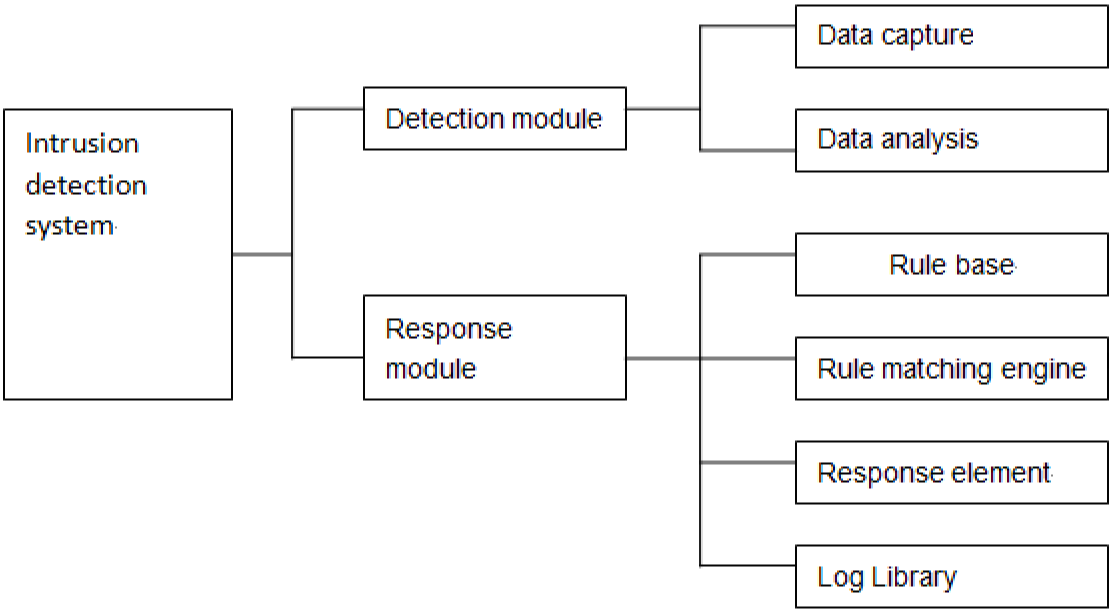

Fig. 2 The system overall structure framework

Response module design implementation. IDS effectively captures the intrusion behavior, which must have a strong intrusion signature database. It is like the public security departments which must have a sound criminal information database. IDS, however, generally with the characteristics of the database are rigid, with the invasion of "face" behaviors often meet strangers. Administrators, therefore, it is necessary to learn how to create to meet the actual needs, the characteristics of the data model, do change should change!

The design of the output module. According to the content of the rule action, invade ignore warning information, warning or warning and deposited in the database. The process is shown in Fig. 3.

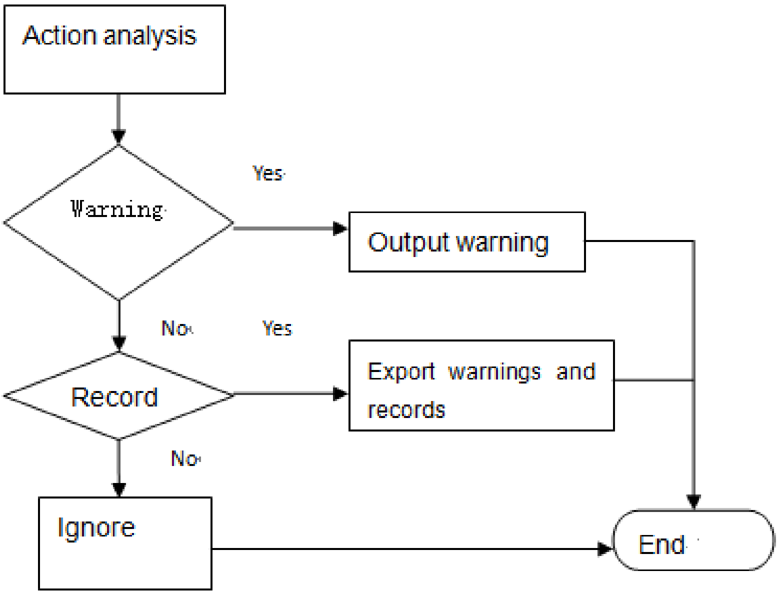

Fig. 3 The response output process

Attack detection test

Scanning is a prelude to hacker attacks, if can timely analyze the scanning intentions which can avoid the hacker's attack in a timely manner. So this test is effective to detect scanning attack behavior is an important step.

Test purpose.

1) Whether the test system can verify the network and host attack.

2) If the test system can output the result of the attack detection.

3) Dynamic rules list whether it supports to add new rules.

The testing process.

1) Using scanning software to scan network or host.

2) Using sniffer software to monitor network, intercept scan packet analysis results.

3) According to the results, write the most appropriate rules, in contrast to snort rules. Check the difference included in the rule base.

4) Open the intrusion detection system to scan test system for testing

5) Again utilize scanning software to scan network or host.

6) Check test

Conclusions

This system based on Windows is a misuse of features (rules) of detection technology architecture of network packet analysis tool to detect intrusive behavior in an effective manner. Ensure users to timely find the invasion, and adopt corresponding measures to effectively guarantee the network security.

References

[1] Zhengjun Tang. Introduction to intrusion detection system technology [M]. Beijing: mechanical industry press, 2004.4.

[2] Jinsong Song. Network intrusion detection [M]. Beijing: National defence industry press, 2004.9.

[3] Wentao Liu. Network security development kit explanation [M]. Beijing: Electronic industry press, 2005.10.

[4] Zhengjun Tang. The design and implementation of network packet analysis tools [M]. Beijing: Electronic industry press, 2002.

[5]Shibin Zhang. Network security technology [M]. Beijing: tsinghua university press, 2004.8, 117:160.