Journal of Applied Science and Engineering Innovation, Vol.2 No.6, 2015, pp.230-232
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Overview of Intrusion Detection Systems

Xiaoting Li[1], Jin Meng[1], Haiyan Zhao[1], Jing Zhao[1]
[1]*Department of Network service, Xi'an Communication Institute, Xi'an 710106, China*

Abstract: Detection system as a kind of active means safety protection provides real-time protection to internal attack, exterior attack and misoperation. This paper introduces the concept of the intrusion detection system and its standardization, classification and comparison and explores its development trend.

Keywords Intrusion detection systems; CIDF model; Misuse Detection. Anomaly Detection

INTRODUCTION

Intrusion detection is a reflection of the intrusion behavior (or attempted). It collects information based on the numbers of key points from computer network or computer system and analyzes it to find out if there is a behavior of security strategy or the signs of attack in network or system. The combination of software and hardware is the intrusion detection system (referred to as IDS). Different from other security products, the intrusion detection system needs more intelligence, it must be able to get the analysis of the data and draw the useful results.

STANDARDIZATION OF INTRUSION DETECTION SYSTEM

The intrusion detection system has two international standard, one is common intrusion detection framework(CIDF) proposed by America Defense Advanced Research Projects Agency (DARPA), the other is the intrusion detection working group of IDWG (Intrusion Detection Working Group) proposed by Internet Engineering Task Force(IETF).

CIDF model

The CIDF's main work consists of four parts: the system structure of IDS, communication system, description language and API.

CIDF divide intrusion detection system into four basic components: event generator, event analyzers, response units and event database, as shown in Figure 1.

CIDF calls the data invading detection system an event, which also needs to be analyzed, it can be the network data package based on the intrusion detection system and can also be a information got from the system logs and other ways based on intrusion detection system. As shown in Figure 1, the event generator is designed to obtain the events from the whole computing environment and provide the event to other parts of the system.

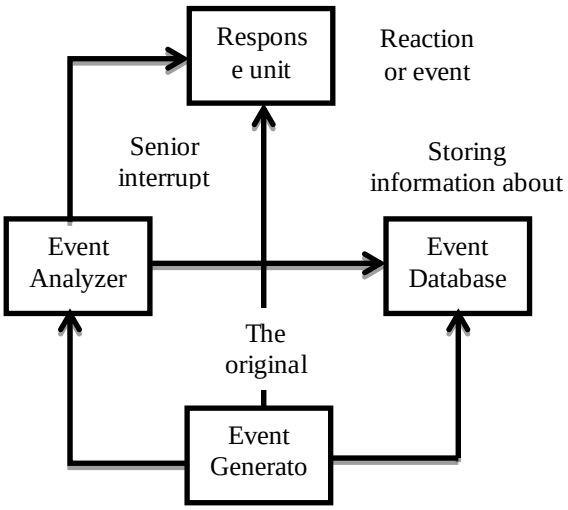

Figure1. Schematic Framework of CIDF

Intrusion Detection Working Group(IDWG)

The intrusion detection working group [4]IDWG is a working group operate under the framework of IETF and composed of IDS product developers who is not interested in CIDF. The IDS system components need to communication with each other, also IDS system from different manufacturers need to communication too. Therefore, it is necessary to define a unified agreement so that each part can communicate according to the standard stipulate by protocol. IDWG has developed a intrusion detection message exchange format (IDMEF), IDMEF adopts the object-oriented thought, using the XML language to describe intrusion detection message. IDWG has also developed intrusion alert protocol (IAP) , which exchange Intrusion Alerts data in intrusion detection systems. The objective of the agreement is transmit sensitive alerts data in the IP network. IAP is an application layer protocol running on top of TCP, its design with reference to HTTP protocol but added many other functions (such as initiate connections from any end, combined with encryption, authentication etc.).

A CLASSIFICATION AND COMPARISON OF INTRUSION DETECTION SYSTEM

According to the input data from intrusion detection system, IDS is usually divided into host based IDS and network IDS; according to the analysis method for detection, it can be divided into Misuse Detection and Anomaly Detection system.

host based IDS and IDS based on Network

Host-based IDS detect and analyze according to the system log and audit records of the host system, discovering attacks through monitoring and analysis of uninterrupted recording system log and audit. Its main purpose is to provide enough analysis after the event in order to prevent further attacks, the response time depends on the periodic inspection intervals, real-time is not as good as the network based IDS.

Based on the network IDS is a network of original data packets as the data source. Network IDS usually uses packet pattern matching or pattern matching based on sequence to define rules, comparing the message which have been listened to the rules while detected, then determine whether there is any abnormal network behavior according to the results of the comparison.

The advantages and disadvantages of the Based on the network and based on IDS is as shown in table 1.

Table 1. Comparison of IDS between the basis of network and the basis of host

Advantages of Network-Based IDS	Advantages of Host-Based IDS
● Real time detection, Response and Warming ● Attack of unsuccessful detection and Malicious attemp ● Independent of operation system ● Low cost ● More difficult for the detector to transfer the data	● Check the successful and failure attacks ● Detect the specific system manner ● Suitable for encryption and exchange environment ● Detection and response on time ● No need for extra hardware ● Low cost

the misuse detection and anomaly detection

Misuse detection type mainly describe intrusion behavior by the mode of attack and attack signature, identifying a system whether there is intrusion activities according to the system intrusion attacks, according to the static known signature collection to intercept network data flow, if it is found that the properties of a data packet matching and a signature sure, then found the intrusion behavior.

Anomaly detection technology use the statistical method to detect whether there is any abnormal behavior, it uses more statistical analysis techniques than misuse detection. It needs to establish a target system and normal activities model, and then conduct system and the user can judge whether the system appeared the intrusion behavior according to the actual activities of this model. The comparison of anomaly detection and misuse detection as shown in Table 2.

Table 2 Misuse detection and anomaly detection

Analytical Strategies	Anomaly Detection	Misuse Detection
Lack means allowance	Anomaly detection based on machine learning	Misuse Detection based on signals
Lack means ban	Anomaly detection based on contour	Misuse detection based on Strategy

DEVELOPMENT TREND OF INTRUSION DETECTION SYSTEM

With the development of the market demand driven and technology itself, the LDS appears in some new forms, IDS has the following development trend:

1. From the pattern matching techniques to detecting neural networks and data mining, intrusion detection develops in other intelligent direction, especially expert systems with self-learning ability to achieve a knowledge base constantly updated and extended, so the ability to prevent the intrusion detection system will be improved, with a wider range of applications.

2. Introducing the Content recovery and network auditing capabilities. It is the basis of the agreement to restore the contents of the analysis. The behavior on the network is completely recording and restructuring, any behavior on the network cannot escape its monitoring. Network audit recorded all connections in the network event.

3. Improve the approach of large data network. Currently Gigabit intrusion detection system products have emerged, but if the intrusion detection products not only have the attack analysis, along with the contents of the recovery and network auditing capabilities, its storage systems is difficult to fully operate in gigabit environment.

4. firewall linkage function. When intrusion detected attacks, the firewall will be notified automatically, intrusion interception load dynamic rules, called firewall linkage function. Currently this feature is not yet entirely practical, but with the

improvement of detection accuracy of intrusion detection products, and linkage function tends increasingly practical.

5. Research on improvements of intrusion detection system performance. Intrusion detection systems currently exist high false negative rate and false alarm rate, taking effective measures to improve its safety and accuracy is needed.

6. protect intrusion detection systems themselves. Once the intrusion detection system is controlled by intruder, security perimeter of the entire system will be in danger of collapsing the front line. So effective strategies have to be adopted to ensure the absolute safety of intrusion detection systems.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation of China(61179002),Shaanxi Natural Sciences Foundation(2011JM8030).

REFERENCES

BOYER R.S, MOORE J.S. A fast string searching algorithm[J]. Communications of the ACM, 1977, 20:762~772

Denning D E. An intrusion-detection model[J]. IEEE Trans-action on Software Engineering, 1987, SE-13: 222~232

Garfinkel T,Matthews J,Hoff C,et al. Virtual machine contracts for datacenter and cloud computing environments[C] .Proceedings of the 1st Workshop on Automated Control for Datacenters and Clouds, ACM, New York,2009: 25-30.

Hao, Z., & Lib, H. (2014). Study of a weak signal conditioning circuit design method. Journal of applied science and engineering innovation, 1(2), 110-113.

Helman P, Liepins G. E. Statistical Foundations of Audit Trail Analysis for the Detection of Computer Misuse[J].IEEE Transactions on Software Engineering, 1993, 19: 886~901

J.O.Kephart. A biologically inspired immune system for computer[M]. Artificial Life IV:Proceedings of the Fourth International Workshop on the Synthesis and simulation Living Systems, Cambridge: MIT Press, 1994, 130~139

Kantarcioglu M, Clifton C. Privacy-preserving Distributed Miningof Association Rules on Horizontally Partitioned Data, Proc. ofIEEE Transactions on Knowledge and Data Engineering,2004-09:1026-1037.

Kemmerer, Richard A. Computer Security[J]. Encyclopedia of Software Engineering, 1994, 1153~1164

Kumar K, Spafford E. A Pattern Matching Model for Misuse Intrusion Detection[C]. In Proceedings of the 17th National Computer Security Conference, 1994, 11~12

Lu, Y., Li, W., Tian, W., & Zhou, K. (2014). Fuzzy Entropy Thresholding Method Using Adaptive Genetic Algorithm. Journal of Applied Science and Engineering Innovation, 1(1), 1-6.

Marc Norton, Daniel Roelker[EB/0L]. Snort 2.0 rule optimizer. http://www. sourcefire.com2003.2

Marc Norton, Daniel Roelker. Snort 2.0 Hi-performance Muti-rule Inspection[EB/0L]. http://www. sourcefire.com, 2004.4

Michael Armbrust,ArmandoFox,Rean Griffithet.al. A View of Cloud Comput-ing[J]. Communications of the ACM,2010:50-58.

Mukherjee, Briswannath L, Heberlein, Todd, Levitt, Karl N. Network Intrusion Detection[J]. IEEE Network, 1994, 8(3):26~41

NIST [EB] . http://csrc. nist . gov/ groups/ SNS / cloud - comput ing/index. html

Porras P, Kemmerer R. Penetration State Transition Analysis-A Rule Based Intrusition Detection Approach[C]. In Proceedings of the 8th Annual Computer Security Application Conference, 1992, No.11:220~229

Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal etal . Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Comput ing as the 5th Ut ility [J] . Future Generat ion Computer Systems, 2009, 25 (6) : 599- 616.

Sandeep Kumar, Eugene H.Spafford. A Pattern Matching Model for Misuse Intrusion Detection[EB/0L]. http://ftp.cerias.purdue.edu/pub/papers/sandeep-kumar/kumar-spaf-NCS C-paper. pdf