Foreword

This rule-based standard drafting GB / T 1.1-2009 and GB / T 20000.2-2009 given.

Instead of the standard GB / T 28454-2012 "Information technology - Security techniques Intrusion Detection System (IDS) selection, deployment and operation."

Compared with the GB / T 28454-2012, the main changes are as follows:

- structural changes are: Modify the original standard suspension segment as a separate chapter (see 7.1, 7.3.1, 7.4.7.1, 7.4.9.1, 7.5.1, 8.1, 8.3.1, 9.1, 9.4.1, 9.5.1, 9.6.1, A 2.1, A 3.1, A 3.4.2.1, A 3.4.3.1, A 3.4.5.1, A 4.1, A 6.2.1, A 6.2.1, A 7.1);

- technological changes in Appendix B.

This standard ISO / IEC 27039: 2015 and their main differences for the following reasons:

- topic errata, the "operations" changed to "operation" (see English title);

-Standard Structure: Due to the international reference standard in intrusion detection and prevention product safety and other standards no rating, while Standard abbreviations more, to maintain continuity with the old standards, the increase in Chapter 2, "Normative references" and 4 Chapter "Abbreviations";

- Standard section 7.3.1 adds "When the organization has requested level of security aspects of IDPS products, see GB / T 20275 and GB / T 28451"The main consideration protection requirements for IDPS product safety level;

- increase the informative Appendix B.

This modified standard international standards ISO / IEC 27039: 2015 "Information technology - Security techniques intrusion detection and prevention system (IDPS) selection, deployment and operation."

This standard is proposed and managed by the National Information Security Standardization Technical Committee (SAC / TC260).

This standard was drafted: Shandong Province Institute of Standardization, China Information Security Certification Center, Shaanxi Province Network and Information Security Evaluation Center, Beijing Talent Network Security Technology Co., Ltd.

The main drafters: Shuguang, Wang L, Wang Fengjiao, Wei, Wei public, Bin, Yang Fan, Leixiao Feng

This standard supersedes the previous editions are:

—GB / T 28454-2012.

Introduction

Organizations before selecting and deploying intrusion detection and prevention systems (IDPS), not only should know when their network, system or application invasion occurred, is occurring, and how it happened, but also should know what the use of intrusion vulnerability, and to prevent similar intrusion, or what protective measures appropriate risk treatment methods will be implemented in the future (ie, risk mitigation, risk retention, risk avoidance, risk sharing). Organizations should identify and prevent network-based intrusion. In the mid-1990s, the organization began using intrusion detection and prevention systems (IDPS) to meet those needs. With the emergence of a series of IDPS products, IDPS applications continue to expand to meet the growing demand for tissue intrusion detection and prevention capabilities.

To get the maximum benefit from IDPS, the process should be performed by trained and experienced personnel carefully planned and implemented selection, deployment and operation of IDPS. When the process of implementing, IDPS products can help organizations exploit information obtained, and can play an important role in the safety of the entire information and communication technology infrastructure.

This standard provides an effective selection, deployment and operation of IDPS Guide, and the basics of IDPS. This standard applies to consider while outsourcing its intrusion detection capabilities of the organization. Outsourcing the service-level agreements can be found in the IT service management processes based on ISO / IEC 20000 in.

This standard is primarily intended to help:

a) Organization meets the following requirements GB / T 22080-2016 of:
   —The organization shall implement procedures and other controls to quickly detect and respond to security incidents;
   —The organization shall perform the monitoring and review process and other safety hazards and de facto control of security events to identify appropriate attempts.

b) Organizations to achieve security control to meet the following objectives GB / T 22081-2016 of:
   —Detect unauthorized information processing activities;
   —The system should monitor and record information security matters. The operator should use the default log and log information to ensure that the problem is identified system;
   —The organization should comply with all the relevant legal requirements applicable to monitor and record activities;
   —Monitoring system should be used to check the validity of the control implemented to verify compliance access policy model.

The organization should recognize that to meet the above requirements, it is not the

only deploying IDPS and (or) perfect solution. In addition, this standard is not intended to be part of conformity assessment criteria, such as information security management system(ISMS) certification, IDPS service or product certification.

Information technology - Security techniques intrusion detection and prevention system (IDPS) selection, deployment and operation

1 range

This standard provides guidelines to help organizations prepare to deploy intrusion detection and prevention systems (IDPS) of. In particularThis standardDetails IDPS selection, deployment and operation. At the same time standard gives background information to get these guidelines.

2 Normative References

The following documents for the application of this document is essential. All the reference documents date, only the edition is applicable to this document. For undated references, the latest edition (including any amendments) applies to this document.

GB / T 18336 (all parts) IT security evaluation criteria IT security technology (15408 (all parts of ISO / IEC), IDT)

GB / T 20275 Information security technology network intrusion detection system technical requirements and test method for evaluation

GB / T 20985.1-2017 Information technology - Security techniques - Information security incident management - Part 1: Event management principles (ISO / IEC 27035-1: 2006, IDT)

GB / T 22080-2016 Information technology - Security techniques Information Security Management System Requirements (ISO / IEC 27001: 2013, IDT)

GB / T 22081-2016 Information technology - Security techniques - Information security control practice guidelines (ISO / IEC 27002: 2013, IDT)

GB / T 25068.2-XXXX IT Security Network Security Technology: Part 2: Security Network Design and Implementation Guide (ISO / IEC 27033-2: 2012, IDT)

GB / T 25068.3-2010 Information technology - Security techniques - IT network security - Part 3: Wangjiantongxin security gateway security (ISO / IEC 18028-3: 2005, IDT)

GB / T 28451 information security technology network-based intrusion prevention product technical requirements and testing and evaluation approaches

GB / T 29246-2017 Information technology - Security techniques - Information Security Management System Overview and vocabulary (ISO / IEC 27000: 2016, IDT)

GB / T 32920-2016 Information technology security technology industry and inter-

organizational communication information security management (ISO / IEC 27010: 2012, IDT)

ISO / IEC 27033-1: 2009 Information technology - Security Network Security Technology: Part 1: Overview and concepts

3 Terms and Definitions

GB / T 29246-2017 and defining the following terms and definitions apply to this document.

3.1

Attack attack

In the information system, the system and / or destruction of information, disclosure, alteration or loss of function or try to make it contrary to its security policy.

3.2

Attack signature attack signature

Execute an attack of computer activity series or a variant thereof, Usually be determined by examining network traffic or log host, IDPS also be found according to their attacks have occurred.

Note: This can also be called an attack mode.

3.3

Proof attestation

Variables generated public key encryption, can IDPS software programs and devices to identify the identity of its remote party.

Note: See 2.23 remote attestation.

3.4

Bridge bridge

Layer located OSI 2 local area network LAN connected to the other network device using the same protocol.

3.5

Cryptographic hash cryptographic hash value

Assigned to a file and used to test the mathematical value in the latter part of this document, To verify the data contained in the file is not malicious changes.

3.6

Denial of service attacks (Denial-of-Service) attack

DoS

By flooding bandwidth or resources of the target system, a plurality of broken ring system according to unauthorized access to system resources and operating system

functions or delay the loss of availability of authorized users. .

3.7

Distributed denial of service attacks distributed Denial-of-Service attack
DDoS

By flooding the bandwidth or resources of the target system, disruption of multiple systems approach to unauthorized access to system resources or delayed system operation and function, resulting in loss of availability of authorized users.

3.8

DMZ Demilitarized zone
DMZ

Logical or physical network located in the space between the outer border routers and firewalls.

注1: DMZ may be located between the network, if necessary, can be placed under close observation.

注2: They usually contain unsafe area Public Domain Security bastion host.

3.9

(Flaw) exploit exploit

One way has clearly undermine system security vulnerability information defined use.

3.10

Firewall firewall

Disposed between a network environment class barrier. It can be a dedicated device,It may be a combination of several components and technologies. All communications between the network environment must flow through the firewall,Only allowed, authorized communication according to local security policy defined by.

[Quoted from ISO / IEC 27033-1: 2009]

3.11

False false positive

IDPS alarm when there is no case of attack.

3.12

False negative false negative

The case when an attack occurs IDPS no alarm

3.13

Honeypot honeypot

To deceive, disrupt and distract the attacker's decoy system,Prompting the attacker to spend time on some of the information,This information is valuable to look,In fact false,No value to legitimate users.

3.14

Host host

A TCP / IP network protocol (e.g., Internet), the system may be set, or computer addresses.

3.15

Intruder intruder

For the target host, site, network or organization,We are or have been subject to attack or invasion.

3.16

Intrusion intrusion

Unauthorized access to a network or networked systems,That is an information system on intentional or unintentional unauthorized access,Including internal information system for malicious activity or information system resources from unauthorized use.

3.17

IDS intrusion detection

Intrusion detection formal process. The process is generally characterized as follows knowledge acquisition: Abnormal usage patterns, and the vulnerability of the type to be utilized by the way, and when it happened and how it happened.

3.18

Intrusion detection system IDS

IDS

In information systems and networks, a method for identifying some have tried, intrusion is occurring or has occurred, and can be made technology system response.

3.19

IPS intrusion prevention system

IPS

Variant specifically designed to provide a responsiveness active intrusion detection system

3.20

Intrusion detection and prevention system, intrusion detection and prevention system

IDPS

In order to prevent malicious activity and monitoring systems intrusion detection system (IDS) and Intrusion Prevention System IPS software application or device, IDS alarm can only be found on these activities, and the ability to block certain IPS Intrusion detected.

Note: If you need to guard against attacks, IPS will actively deployed in the network. If deployed in the passive mode, it will not provide the above functions, which can provide only an alarm function effectively as conventional as IDS.

3.21

Penetration penetration

Bypass system security, unauthorized acts.

3.22

Upgrade provisioning online

Installation of information technology (IT) equipment the right software, enforce security policies and processes configuration data is loaded.

3.23

Remote Attestation remote attestation

The use of digital certificates to ensure the identity and IDPS software and hardware configuration,And securely transfer the information to a trusted process operations center.

3.24

Response response

Incident response or intrusion response incident response or intrusion response

When the attack or invasion,In order to protect and restore operations information system up and running conditions and the information stored therein taken.

3.25

Router router

Select a path or route through a route protocol mechanisms and algorithms,Network devices to establish and control the data flow between different networks.

注1：Which itself may be based on different network protocols.

注2：Routing information stored in the routing table.

[Quoted from ISO / IEC 27033-1: 2009]

3.26

Server server

Computer system or program provides services to other computers.

3.27

Service Level Agreement Service Level Agreement

SLA

The provisions of technical support contracts or business performance objectives,Including service providers offer to their customers as well as performance measurement of the results of failure.

3.28

Sensor sensor

Information from the system or network to be observed, the collection member IDPS one kind or agent situation data by sensing, monitoring and the like.

Note: also called a monitor.

3.29

Subnet subnet

In certain network, Sharing a part of the public address components.

3.30

Switch switch

Between networked devices, One kind of communication device is provided by means of an internal exchange mechanism Switching technology which is usually implemented in two or three layers of the OSI reference model.

NOTE: The switch is different from other LAN interconnection equipment(Such as a hub), The reason is that technology is used to establish point-switch-connection basis. Ensure that network traffic is visible only to the address of the network equipment, And several connections can co-exist.

[Quoted from ISO / IEC 27033-1: 2009]

3.31

Test access point

Test Access Points

TAP

Typical passive device, It will not install any load on the network packet; When they make the data collected in the network interface is not visible, Also can increase the security level, Here still holding layer 2 switch ports.

Note: TAP also gives the function of multi-port, In this way, without losing the ability to IDPS, You can debug network problems.

3.32

Trojan trojan horse

That masquerades as a benign application software malicious programs.

3.33

Virus virus

One kind of malware with bad intentions can cause potential harm, directly or indirectly, to the user and (or) the user's system

3.34

Virtual Private Network virtual private network

VPN

One kind of a virtual network using tunneling connection, i.e., a logical computer network limited to use of the network resources based on the physical build a network system, establishing a connection through the actual network.

[Cited: GB / T 25068.3-2010]

3.35

Vulnerability vulnerability

It may be one or more assets or control measures using the threat of weakness.

[Cited: GB / T 29246-2017]

4 Abbreviations

The following abbreviations are applicable to this document.

AIDPS Based IDPS applications Application-Based IDPS

API Application Programming Interface Application Programming Interface

ARP ARP Address Resolution Protocol

CGI Common Gateway Interface Common Gateway Interface

CPU for Central Processing Unit

DMZ Demilitarized Zone Demilitarized Zone

DNS Domain Name System Domain Name System

DDoS Distributed Denial of Service Distributed Denial of Service

DoS Denial of Service Denial of Service

ICMP Internet Control Message Protocol Internet Control Message Protocol

IDS Intrusion Detection System Intrusion Detection System

IDPS intrusion detection and prevention system Intrusion Detection and Prevention Systems

I / O Input / Output Input / output

IODEF Event Object Description Exchange Format Incident Object Description Exchange Format

IP Internet Protocol Internet Protocol

IPS Intrusion Prevention System Intrusion Prevention System

ISIRT Information Security Incident Response Team Information Security Incident Response Team

IT Information Technology Information technology

HIDS Host-based intrusion detection systems Host-based IDS

HIDPS host-based IDPS Host-based IDPS

HIPS Host Intrusion Prevention System Based Host-based IPS

HTTP Hypertext Transfer Protocol Hypertext Transfer Protocol

MAC MAC Media Access Control

MIB MIB Management Information Base

NIDPS network-based IDPS Network-based IDPS

NIPS network-based Intrusion Prevention System Network-based IPS

NOC Network Operations Center Network Operations Center

OSI OSI Open System Interconnection
RID real-time network defense Real-time Intern-network Defence
ROI ROI Return On Investment
SIEM security information and events management Security Information Event Management
SMS Short Message System Short Message System
SLA Service Level Agreement Service Level Agreement
SMTP Simple Mail Transfer Protocol Simple Mail Transfer Protocol
SNMP SNMP Simple Network Management Protocol
SPAN Switch Port Analyzer Switch Port Analyzer
A test access point TAP Test Access Points
TCP Transmission Control Protocol Transport Control Protocol
UDP User Datagram Protocol User Datagram Protocol
VPN Virtual Private Network Virtual Private Network

5 background

The purpose of intrusion detection and prevention systems (IDPS) is a passive monitor, detect and record improper, incorrect, suspicious or unusual activities when these activities may represent intrusion is detected, IDPS an alarm and (or) the automatic response. Responsibilities of full-time IT security personnel are actively reviewed IDPS alarm and associated logs in order to make decisions on the appropriate response. We need to quickly detect when the tissue invasion of organizational information system and an appropriate response, should consider deploying IDPS. Organizations can obtain by deploying IDPS IDPS software and (or) hardware products, it can also be deployed by the IDPS IDPS IDPS outsourcing service providers the ability to fashion.

There are many commercial or open source IDPS products and services, their different techniques and methods. In addition, IDPS is not plug and play technology. So when the organization is ready to deploy IDPS, should at least be familiar with guidelines and information provided by this standard.

Appendix A lists the main foundation of knowledge about the IDPS. This appendix explains the characteristics of different types of IDPS:

—Network-based IDPS (NIDPS), wherein the monitoring devices or a specific network segment network traffic, network and application protocol activity analysis to identify suspicious activity;

—, Wherein a single host and monitoring events occurring in a host wherein, for host-based IDPS (HIDPS) are three basic methods for detecting suspicious activity analysis, i.e., based on feature detection, anomaly detection based on statistical analysis of the detection, the state of the protocol.

Behavior analysis method can be applied network-based and host-based IDPS. This method checks the network traffic and host activities to identify abnormal behavior pose a threat, such as Distributed Denial of Service (DDoS) attack, brute force attacks,

specific forms of malware and policy violations (such as client system providing network services to other systems).

Information host-based intrusion detection and prevention systems (HIDPS) derived from one or more hosts, and web-based information system intrusion detection and prevention (NIDPS) derived from one or more network traffic segments. Methods based on misuse of the information system attacks suffered by modeling for a specific attack signatures, and then scan the system as a whole, the number of attack signatures statistics. This process needs to consider the early acts and activities with intrusion or malicious conduct of specific coding. The method is based on an abnormality detecting intrusion attempts to severely abnormal behavior was found by the method based on such an assumption, these attacks different from normal or legitimate behavior, and the system to recognize the differences detected.

Organization should realize the advantages of the different information from different sources and methods of analysis, drawbacks or limitations which can affect the ability to detect specific attacks, and can affect the installation, the maintenance difficulty IDPS.

6 General

IDPS features and limitations (see Appendix A) shows that, based on the appropriate host tissue (including monitoring application) and a combination of network-based, fully covered to achieve the effect of potential intrusion. IDPS each type has its strengths and limitations, together, they can provide the ability to better security alarm events coverage and analysis.

IDPS combination of different techniques rely on the availability of the associated engine management system alarm Artificial NIDPS and alarms associated HIDPS to the operator in work overload, no other advantages, which is worse than the results from a single IDPS selected the most appropriate output.

In tissue selection, deployment, and operation of IDPS process shown in Figure 1, the subsequent sections of the key steps in this procedure is described in detail.

FIG 1 IDPS selection, deployment and operation

7 select

7.1 Brief introduction

There are many IDPS products and product lines to choose from These products cover a very expensive commercial systems need to support the latest hardware from the free product can be deployed on low-cost to the host. Because too many alternative IDPS products, fromSelect best meets organizational needs IDPS products very difficult. Moreover,There may have limited compatibility between the various IDPS products. Other,Since the potential merger and wide geographic distribution of the organization,The organization may have to use different IDPS,Integration is also a great challenge of these different IDPS.

In the operation of the network traffic in a large,IDPS manufacturer's instructions may not be able to describe how good intrusion detection,As well as the deployment, operation and maintenance of the difficulty of IDPS how much. Manufacturers can point out which attacks can be detected,But at the lack of understanding of an organization's network traffic premise,IDPS describe how effective implementation and to avoid false positives and false negatives are very difficult. IDPS active and independent assessment need responsiveness, and mapped to the tissue requirements. The above process should include deep packet inspection and require recombination, rather than requiring network performance and cost considerations. Therefore rely solely on information supplied by the manufacturer IDPS capacity is not enough,Organization is not recommended to do so.

GB / T 18336 (all parts)IDPS available for evaluation. In this case, compared to the manufacturer's instructions, the document known as the "safety objectives" may comprise IDPS more accurate and reliable performance of the description. The organization should use this document in the selection process.

The following subsections provide a selection process should be organized through the

use of the elements in the IDPS.

7.2 Information Security Risk Assessment

Before selecting IDPS,The organization should perform information security risk assessment, the aim is to identify for the organizationThere may be vulnerabilities specific information system attacks and intrusions (Threat), andConsider the following factors, such as the nature of the information systems and the need to use howProtection information, type of communication system and other operating factors and environmental uses. In the context of organization-specific information system security objectives,By considering these potential threats, the organization can effectively identify and mitigate risks with a cost-effective control.Identified as IDPS control functions provided by the need to provide the foundation.

Note: The information security risk assessment and management GB / T 22080-2016 standardTheme of.

Once installed and IDPS IDPS operable,According to the operating systemshould change and environmental threats, continued implementation of riskEvaluation process,To periodically review the effectiveness of controls.

7.3 Host or network IDPS

7.3.1 Outline

IDPS deployment should be based on organizational risk assessment and asset protection a priority. In selecting IDPS,Research should monitor the situation of the most effectiveMethods. Host-based IDPS (HIDPS)And web-basedIDPS (NIDPS)It can be deployed together. Installation and maintenanceNIDPS care is usually the easiest, soselectIDPS monitoring method,The organization should theNIDPS implemented in phases, and then deploy HIDPS on critical servers.

Each option has its advantages and disadvantages. For example, the external firewall can effectively prevent the need to scan a large number of alarm events, and thereforewhenWhen IDPS deployed outside the external firewall, IDPS can generate a lot of alarmdoes not require careful analysis.

When the organization has requested level of security aspects of IDPS products, see GB / T 20275 and GB / T 28451.

7.3.2 Host-based IDPS (HIDPS)

Select HIDPS need to identify the target host. In view of the full deployment HIDPS on each host organization it is very expensive and can only be deployed HIDPS on critical hosts. So HIDPS deployment should prioritize based on risk analysis and cost-effectiveness considerations. When HIDPS deployed on all or a significant number of host organizations IDPS should be deployed with centralized management and reporting capabilities.

7.3.3 Network-based IDPS (NIDPS)

When deploying NIDPS,The main factor to consider is placed in what position sensor

system,Options include:

—In the external firewall;

—In addition to the external firewall;

—On the main backbone network;

—In key subnet.

7.4 Considerations

7.4.1 System Environment

Organizations should be based on security risk assessment, in order of priority, first determine what assets to protect, and then custom fit IDPS environment. To achieve this goal, the need to collect at least the following information system environment:

—The number and location of the host, the network entry and network topology to the external network connection points described in detail;

—Description of enterprise network management system;

—Each host operating system;

—The number and type of network devices such as routers, bridges, and switches;

—Number and type of servers, and dial-up lines;

—Any network server description, including the type, configuration, application software and versions are running;

—Connected to an external network, comprising a support and a nominal bandwidth protocol;

—And the introduction of a different connection path documents return path, i.e., asymmetric data stream

7.4.2 Security protection

After the technical attributes of the recording system environment, it should identify the security mechanisminstalled. At least the following information:

—Demilitarized zone (the DMZ);

—Firewall and router filtering number, type and position;

—Authentication server;

—Data and communication link encryption;

—Anti-malware or anti-virus package;

—Access control products;

—Professional security hardware such as encryption hardware;

—Virtual private networks (VPNs);

—Any other security mechanisms installed.

7.4.3 IDPS security policy

After identification system and general security environment,Should determineIDPS security policy. SafetyStrategies need to answer at least the following key questions:

—To monitor what information assets;

—Not opened successfully or unsuccessfully closed case what strategy to adopt;

—What type of IDPS needs;

—IDPS can be placed in any position;

—To detect what type of attack;

—What type of information to be recorded;

—When an attack is detected to provide an alarm, or what type of response.

IDPS security policy reflects the target tissue for the IDPS investment. This is the initial step in trying to get the maximum benefit from the IDPS assets.

For a detailed description IDPS security policy goals and objectives, the organization should first identify the risks from internal and external sources. The organization should understand that some manufacturers have IDPS IDPS security policy is defined as a set of rules IDPS used to generate an alarm

Existing organization's security policy should be reviewed to provide for the needs of IDPS template, the template can be clearly defined and based on confidentiality, integrity, availability and security objectives standard anti-repudiation, but also according to more general management objectives such as privacy, responsibility protection and manageability explicitly and regulations.

When the IDPS to detect violations of security policy, the organization should determine how to deal with IDPS. In particular, when the tissue in response to certain types of desired active contrary, should IDPS configured to do so, and the operator should understand the response policy of the organization, so that they can deal with the alarm in a suitable manner. For example, law enforcement agencies may be requested to assist in the investigation of security incidents effectively addressed. Related information (including IDPS logs) may be required to surrender to law enforcement entities to obtain legal evidence.

For additional information related to security event management can be found in GB / T 20985 in.

7.4.4 performance

In selecting IDPS,Performance is another consideration. Should at least answer the followingproblem:

—IDPS how much bandwidth to deal with;

—When operating in a given bandwidth, false positives can be tolerated to what extent;

—Whether IDPS to justify the cost of high-speed or medium-speed or low speed can be satisfied if IDPS;

—What are the limitations IDPS performance because of missed potential consequences of the invasion;

—When deep packet inspection and recombination occurs, what will affect performance.

Sustainable performance is defined,Continuously attack detection capability within a given bandwidth utilization range. In most environments,Hardly tolerate such IDPS:It may be missing or miss attack traffic part of the package. occasionally,When the bandAnd wide(Or) network traffic increases,a lot ofIDPS will no longer be able to effectively and continuously detect intrusion.

Combination of load balancing and adjustments to improve efficiency and performance. E.g:

—We need to organize knowledge about the network and its vulnerability: Every network is different; the organization should be clear what kind of network assets need to be protected, and what kind of attack adjustment features may be associated with these assets. This is usually done through the risk assessment process.

—When IDPS network traffic and is configured to handle a limited number of services, most of IDPS better performance. For example there are many e-commerce business organizations need to monitor all HTTP traffic and adjusting one or more of the IDPS, in order to find the unique features associated with the attack WEB traffic.

—The appropriate load balancing configuration enables signature-based IDPS run faster and more thoroughly, because the need to traverse only optimize a smaller attack signature database for processing, rather than through all the possible attack signature database for processing based IDPS mark.

In IDPS deployment,Load balancing is used to separate the available bandwidth. however,Bandwidth separation may cause problems,Such as additional cost, administrative overhead charges, traffic disorders, copy alarm and false negatives. Moreover,The current technology is about to reach IDPS bit rate G,The result is that the benefit-cost ratio of load balancing may be minimal.

7.4.5 Verification capabilities

IDPS ability to rely on such information supplied by the manufacturer is often not enough. The organization may require manufacturers Annotated,Or give suitableIDPS specific organizational environment and security objectives of the applicability of the demonstration. When the target network expansion,mostIDPS vendors to adjust product experience,Some vendors are committed to supporting the new protocol in the threat environment Standard, platform type and change. The organization should claimIDPS vendors at least answer the following questions:

—IDPS applicability in this particular environment which do hypothesis;

—What are the details of the test to verify the IDPS capabilities statement is executed;

—The operator of IDPS what assumptions;

—IDPS what kind of an interface (e.g., interface type comprising reporting format important physical interfaces, communication protocols, connected with the associated engine);

—What mechanisms or alarm output format, and whether they are well documented (e.g., management information base format, the system log message or Simple Network Management Protocol (SNMP) message (the MIB));

—During working hours, IDPS whether the interface, configuration and customization of shortcut keys with alarm features, and attack signatures;

—IDPS case whether the working time can be configured, to provide this capability characteristic well documented;

—Product development and the ability to adapt to changing system infrastructure of

the organization;

—IDPS products can meet the ever expanding and changing network;

—Whether IDPS provide fail-safe and how the troubleshooting capability, and the ability to integrate these same capabilities on the network link layer;

—IDPS whether the alarm using a private network, or an alarm and monitors whether the same network for transmission;

—Quality assurance, discovered the vulnerability and response aspects of product performance record, how reputable manufacturers.

7.4.6 cost

Cost is not the actual cost of purchasers of IDPS spent. Additional costs include:runAcquisition cost IDPS software system, special subsidies to install and configure the IDPS, personnel training and maintenance costs. Management systems and analyzed the results of the largest costs. IDPS cost effective way to measure the return on investment(ROI)Or analysis of costs and benefits. In this caseunder,groupBased organizations to achieve the cost savings of managing intrusion calculatedROI. The cost of buying and operating IDPS should be required to resolve the alarm personnel costs and indirect costs of false alarms and inappropriate response caused by equilibrium,Such as the inability to determine which part of the information system is compromisedThe reloading information systems.

Benefits include running IDPS:

—Identify defective or misconfigured devices;

—Instant Confirmation configuration;

—Provide an early systemusage statistics.

To make financial decisions about the IDPS,Buyers need to answerQuestion IDPS total cost. to this endShould be analyzedSpend IDPS deployment within the organization. IDPS cost analysis need to answer at least the following questions:

—The initial capital expenditure budget to buy IDPS how much;

—What IDPS operation time period is required, such as the 7 * 24h or less;

—Processing, analysis and reporting of what infrastructure IDPS output is needed, and how much it costs;

—Organization is configured in accordance with its security policy personnel and other resources required for IDPS, whether there is operation, maintenance, update and monitor the IDPS output and alarm response personnel and resources, if not, how to achieve these functions;

—Are there funds for IDPS training;

—What is the scope of the deployment, if HIDPS, how many hosts will be protected.

By remote control to intrusion detection service provider outsourcing IDPS monitoring and maintenance functions for the daily management of cost-sharing,groupIt may be less cost weave.

IDPS is deployed in response to the most expensive part. The main cost includes determining the response mode, setup response team, the development and deployment of response strategies, and training and exercises.

7.4.7 Update

7.4.7.1 General

Most of signature-based IDPS,IDPS value equivalent to only attack signature database for the analysis of the situation. It is often found new vulnerabilities and attacks,Therefore we need to be updatedIDPS attack signature database.Organizations should at leastConsider the following factors:

—Updated timeliness;

—Internal distribution of validity;

—Implementation;

—Affect the system

7.4.7.2 Feature-based IDPS updates timeliness

The current attack signatures to detect known attacks is necessary maintenance.To ensure the attack signatures in real timeUpdate,at leastShould address the following issues:

—When they find or exploit a specific vulnerability, IDPS vendors release updates how fast attack characteristics;

—Notification procedure is reliable;

—Whether the attack signature updates to ensure the authenticity and integrity;

—If the attack to be customized features within the organization, whether they have enough available technology;

—In response to high-risk vulnerabilities immediate or sustained attack, whether written or have the possibility of receiving a custom attack signatures.

7.4.7.3 The effectiveness and implementation of internal distribution

Whether the organization can quickly distribute and implement specific update within a certain time frame all relevant systems.In many cases,shouldModify attack signature updates to include specific IP addresses and ports. Specifically,At least within the enterprise network trust boundariesShould be asked to answer the followingquestion:

—In the case of the manual distribution, the administrator or user whether an attack signature updates within an acceptable time window;

—If you can measure the effectiveness of automatic distribution and installation process;

—Whether they have effective mechanisms for tracking the attack signature updates change the situation.

7.4.7.4 Systemic effects

In order to impact on system performance will minimize the attack signature updates,at leastShould answer the following questions:

—Updated attack signatures would not affect the performance of important services or applications;

—Is it possible to selectively focus updated attack signatures, it is necessary to

avoid conflicts and performance affect service or application.

7.4.8 Alarm Policy

IDPS configuration and operation of the monitoring should be based on organizational strategy. Organization should ensure that at least IDPS can support a specific method of alarm organization's existing infrastructure. Supported alarm properties including e-mail, web pages, text messaging system (SMS), SNMP events And automatically block the attack source.

When data for evidentiary purposes IDPS, Including the burden of proof carried out for internal discipline, need in accordance with Laws and regulations to deal with, management, application or submit IDPS data.

7.4.9 Identity Management

7.4.9.1 General

In the case of human intervention, Identity management is achieved IDPS prove critical infrastructure and remote online upgrade. These capabilities needed to create and use a trusted third party As authority, Despite the poor Different, but its role And often assumed to be a public key infrastructure authority part similar. The ability for seamless, secure, controllable IDPS IDPS data and corporate identity exchange network trust boundary is also very important.

7.4.9.2 Remote Attestation

IDPS can contain millions of lines of code. In such a large code, Hard to find intentional insertion of malicious software, It may allow Xu attacker control IDPS output. therefore, Correct IDPS software and hardware strict access control is very important to identify, And appropriate portions Points based on the identity of the entity to initiate access requests. In the case of unmanned remote attestation instruction is issued, Provide this access control System capacity.

In hardware, Proof verification apparatus to the remote or unmanned running on the device or software by generating a hash value encrypted certificate Identity pieces. The simplest form of identity through an encrypted Hash Values to represent, The encrypted hash value is used to distinguish different software Program or device discovery and change software. In the request the user IDPS, Certificates may be provided to any remote party, In principle There is also the role of the remote party verification, which is IDPS is being used and is not expected to change the software. If the software on IDPS been altered, Generated certificate will reflect the code base IDPS has been changed.

It would IDPS, The purpose is to detect remote attestation IDPS software unauthorized changes. E.g, If the attacker Part has been replaced or modified an IDPS applications with malicious or alternate versions of the operating system IDPS, Hash values do not It will be recognized by the remote service or other software. therefore, Remote party (Such as Network operations center NOC) can be detected by the virus or Trojan destruction IDPS software, And will be able to make a move on that information. Because the proof is

remote,versusCombined with other IDPS IDPS should also know the specific IDPS has been compromised. thereforeinNot repaired before the IDPS,Send them to avoidinformation.

Based on the above reasons,IDPS advised to remote network operation center (NOC)Certificate or report its status, configuration, orHis important information. Proven ability to identify or IDPS IDPS ability to assess the robustness and perform many IDPS configuration and update operations is critical. More clear is,It proved to be remote testingAbility IDPS integrity.After summaryIDPS proof report provides the status of network defense posture review,It is a key part of the overall assessment of the ability of the network situation.

7.4.9.3 Online upgrade

When the remote attestation problems detected IDPS,Require corrective action to alleviate the problem This can allow network operatorsCenter (NOC) has been pushed IDPS identify configuration, software updates and patches to complete. The industry has adopted the term "online upgrade",HanCover for IT equipment (including IDPS)During the installation of the correct software, enforce security policies and load the configuration data. Online's goal is to upgrade as remote processing. Which saves a single physical access to IDPS labor costs,And allow more timely mitigation askquestion,In particular attack signature updates. To be effective,IDPS online upgrade capability from the need to launch operations center safely,ByIDPS safely pull. In the latter case,IDPS should have secure and automatic ability to search new update software vendors from a remote site and download the update has been identified in a timely manner.

7.5 Supplementary IDPS tools

7.5.1 General

The organization should rapidly detect intrusion and reduce the damage caused by the invasion. Tissue should also be appreciated,For achieving these goals,IDPS andIt is not the only and (or) perfect solution. Some network equipment and IT tools provide the ability to IDPS provides. The organization should consider the ability to deploy the equipment and tools to enhance and complement the IDPS.

Examples of these include equipment and tools:

—File Integrity Checker

—Firewall or security gateway

—honey jar

—Network Management Tools

—Security information and events management (SIEM) tool

—HIV / Content Protection Tool

—Vulnerability assessment tools

7.5.2 File Integrity Checker

File integrity checker is to assist IDPS another class of security tools. They use

the message digest of the key file and object code or other cryptographic checksums,Compared with a reference value,Marked difference or change. Since the attacker will often modify the system filesItem,Use Encryption check code in the three stages of the attack is very important. The first stage),They modified the system files targeted for attack(E.g,Placed Trojans). second stage),They tried to leave the back door in the system,so thatCan then re-enter. The final stage),They tried to cover his tracksSo thatThe system responsible may be unaware of the attack.

advantage:

—Determine the vendor-supplied bug patch or other desired change is already applied to system binaries;

—Allow to attack marks for fast, reliable diagnosis, especially for the system has been attacked for forensic examination time;

—Attackers often modify or replace system files, and use technology to preserve file attributes, attributes these documents are periodically reviewed by the system administrator; using a cryptographic checksum code integrity checking tools can still detect any change or modification;

—Modification allows the data file is identified.

Shortcoming:

—During the analysis, the information may require the system startup and shutdown, or at least the verification system

7.5.3 Firewall

Firewall(See alsoGB / T 25068.2)The main responsibility is to restrict access between networks. Simple firewall-based organization can access the source IP address, destination IP address and port number to filterNetwork traffic.E.gOrganizations may only want to takeBy e-mail server(The port number25)orweb server(The port number80)Traffic. however,Application-level Firewall soFiltered to provide more complex application protocol information. When the firewall is located within an enclosed area when,It reducesNIDPS need to check the flow.

While some are trying to stop traffic through the firewall,Most firewall to monitor network information content and launchCapacity warning area is limited. in comparison,NIDPS designed to check the network packet,Constitutes legal and illegal traffic detection and inspectionWhen measured malicious content network packet,Can alarm In many cases,If necessary,NIDPS alarm parameters can be used to change the filtering of the firewall.

When deployed inside the firewall NIDPS,A properly configured firewall can greatly reduce theNIDPS number of check packets. Such NIDPS configuration can greatly improve the accuracy of NIDPS,Because when enteringTraffic will be NIDPScontrolTimeCan eliminateCaused by the scanning activityInternet background noise.

7.5.4 honey jar

Honeypot system is decoy jargon,To deceive, dispersed, and transferred to lure attackers seemingly valuable informationSpend time on, butThis information is actually

fabricated,Without any legal value to the user. The main purpose of the honeypot is closingThere are a threat to the collection of information organization,And lure intruders away fromcritical systems.

Honeypot is not an operating system,But it can lure the attacker to maintain adequate time online information system,So organizationsAssessment intent, skill level and method of operation of the attacker.

Information obtained from the activity analysis honeypot intruder enable organizations to better understand the threats and vulnerabilities of systems,Thereby improvingIDPS into the tissue operations. Information by analyzing action honeypot intruder can be obtained for the organization IDPS strategy, organizational attack signature database and holistic approach to the development of the organization to contribute,The overall approach is to avoid the threat of a known type of attackerIDPS best practices.

In all cases,Only after the organization seek guidance fromlegal advice in,They should use honeypot. From honeypotData can be considered a form of entrapment technology,Therefore required to determine the legality of their data.

Some of the advantages and disadvantages of a honeypot:

advantage:

—An attacker can be transferred to the systemtarget their indestructible;

—Honeypot does not manage authorized activities, a honeypot to be captured any activity is considered to be suspicious;

—Administrators have more time to decide how to respond to an attacker;

—Can more easily and more extensive surveillance operations of the attacker, the monitoring results can be used to improve threat model and system protection;

—Can effectively capture the internal staff on the network snooping.

Shortcoming:

—This device was used to determine the legality bad;

—Once inside the trap system, an attacker could become angry and tried to organize the system more hostile to launch an attack;

—In order to use these systems, administrators and security managers need a high level of proprietary technology.

7.5.5 Network Management Tools

Network management tools with different active and passive detection technology to monitor the availability and performance of network devices. These tools have the information collected by the network topology and memberComeNetwork infrastructure configuration and management functions.

Interconnected network or system management tools and IDPS IDPS alarm can help alert the operator to properly handle and evaluate their impact on the monitoring system

7.5.6 Information security events management (SIEM) tool

SIEMto organizational report uses integrated management and alarm control platform SIEM can collect information from IDPS, firewall, sniffer, etc.,And can reduce

information overload, so that the analyst can manage vast amounts of information. The second and main reason is that the data collection like thisTogether, we can make numerous small single packet and multiple sources associated time under control of the radar,andFor a singleIDPS attack it may become false negatives.

SIEMtool can also be used to process data obtained fromIDPS. usually,SIEMtools are available to performthe following functions:

—Collect and maintain different sources of data security-related events in a centralized database may contain data from one or more of the IDPS, log files from network devices and hosts and event data fromanti-virus tools;

—Further processing of the collected data, in particular to provide further filtering, aggregation and correlation functions;

—Developments related: to detect the mode of non-related security vulnerabilities by establishing a secure and non-secure scenarios related events;

—Filter events: by reducing the level alarm correlation based on the correlation, e.g. IDPS alarmand security patch level;

—Polymerization events: by collecting and normalizing the situation based on source, destination, and time stamp events such as described, to mitigate overflow alarmIDPS;

—Reports related to the police and to provide help to conduct in-depth analysis of the collected data based on alarm, provides a simple interface useful.

The main objective of SIEMtools by providing an automated fashion,The difference between high-threat related alarms and irrelevant or no threatOf false positives. SIEM tool is properly configured to achieve the objectives of this indispensable condition,When planningSIEM tool is introduced,organizationShould consider it as an important task. When used with the systemIDPS,Configuration requires a high level of expertise and considerable workFor the total amount. After proper construction and configuration, SIEMtools provide high value-added,In particular, can provide valuable information,Trigger further processes and activities,Such as event management.

7.5.7 HIV / Content Protection Tool

HIV / content protection tools for cross traffic and virus-specific sources of information analysis, to provide additional data to supplement the IDPS through.

7.5.8 Vulnerability assessment tools

Vulnerability assessment is an integral part of the risk assessment required,For good security audit/ Compliance checking and monitoring strategy, it is also valuable components. This assessment allows organizations to look for vulnerabilities,And in mostRecommend corrective action in the case to reduce the chance intruders exploit vulnerabilities invasion. therefore,useVulnerability assessment can be greatly reducedIDPS find the number of attacks.

Vulnerability assessment focuses assess the extent of a given host for a given vulnerability is exposed. This assessment process and the implementation of the attack script different. The result is,IDPS to detect vulnerability assessments failure does not mean IDPS can not detect the attack. The opposite of,IDPS detection vulnerability

scanning activity does not mean the same IDPS can properly detect attacks.

Vulnerability assessment tools used to test network host susceptibility to dangerous. Vulnerability assessment tool for use in conjunction with IDPS, Whether in attack or attack detection reaction, they are to checkCheck the validity of IDPS provides a valuable method. Vulnerability assessment toolsIt can be classified based on the host-based or network. By querying the data source host-based vulnerability tools(Such as file content), Configuration details, and other status information,To assess the security of information systems. Allow access to the target host host-based tools,Over a remote connection running on the host. Network-based vulnerability tools are used to scan the host vulnerabilities associated with network services. In order to perform a host or network vulnerability assessment,A certain level managers within the organization should be approved by the test. Use vulnerability assessment tools IDPS is a supplement to, not a substitute, to emphasize this point is very important.

The advantages and disadvantages of using vulnerability assessment tools are:

advantage:

—Vulnerability assessment tools for information system security status file and properly in order to re-establish security baselines rollback after the system change, provides an effective method;

—Regular use of vulnerability assessment tool can reliably identify changes in information systems security declaration;

—The biggest advantage is the vulnerability assessment tool to help identify vulnerabilities;

—It allows an organization known vulnerability and attack data matches to determine whether the attack was successful.

Disadvantages and problems:

—Host-based vulnerability assessment tool is specific platforms and applications, it is generally more expensive in the establishment, management and maintenance than the web-based tools;

—Network-based vulnerability assessment tool is platform-independent, host-based tools are not as good as more targeted;

—Vulnerability assessment is resource consuming activities, activities may be impractical, or the system or network under reduced performance only at the cost of operation, or only the date and time request operation under stringent conditions;

—In many cases, vulnerability assessment is based on weeks, months, or even more random with respect to the continuity of periodic activities, timely detect security problems can be a challenge, and sometimes impossible;

—And IDPS as vulnerability assessment tool is subject to false positives or false negatives, should be carefully analyzed;

—Repeat vulnerability assessment can overlook a lot of anomaly-based IDPS real attack;

—Attack signature updates required;

—The system does not detect unauthorized network-based vulnerability assessment tool host.

Network vulnerability assessment testing should be limited to the target system,Over the entire process should be careful to protect the privacy of any data collected. Data collected by the tool to the vulnerability of sensitive information,An intruder may be used to organize a systemintrusion,It should therefore protect this information.

7.6 Scalability

IDPS before use, into the specific tissue should IDPS scalability. Many IDPS full run at a lower data transmission rate, but when the bandwidth increase, the performance would decrease. As more and more packet loss and treatment failure, IDPS performance degradation, which in turn often leads to false negatives (when the attack produces no alarms) and false positives (generate an alarm when there is no attack) were significantly increased. In other words, many IDPS not suitable for large-scale or widely distributed enterprise network environment.

Scalability is a concern in a wide range of applications NIDPS deployment, but in the case where the host requires high performance, also applies HIDPS.

7.7 Technical Support

Like other systems, like, IDPS require maintenance and support. IDPS is not "plug and play" technology. Many manufacturers to customers to install and configure the IDPS provides expert support. Other manufacturers expect the organization employees to install and configure the IDPS, they only help by phone and e-mail.

Technical support is dependent on the degree of organization and the type of IDPS vendors terms of the contract, combined with specific cases to be implemented. Regardless of the organization's business needs is to monitor custom or legacy systems, or to customize the protocol or format of the report IDPS result, technical support should include at least help manufacturers adjust or debugging IDPS to suit the particular needs of your organization.

Organization appropriate to provide technical support contact information (such as e-mail, phone, online chat, web-based reporting, remote monitoring or response service). Contract terms are usually elaborate on these technical support services and response times. And contract manufacturers should provide sufficient accessibility to these services to support the needs of event processing or other sensitive periods.

7.8 Train

Technology alone is not sufficient intrusion detection system The organization should require qualified technical personnel evaluation, selection, installation, operation and maintenance of IDPS. Qualified personnel requirements IDPS is very high, in many cases, recruiting, hiring, retaining the call of duty to meet the IDPS has a very difficult experience and knowledge of the staff. In response, many organizations decided to IDPS operations outsourced to managed security service providers. This choice presents its own problems and the risk of tissue in training. For example, even in the case of most of its continued function outsourcing, organizations also should be important knowledge about the problem to staff training and operation of IDPS, or it may lose

control of the IDPS. In order to achieve optimal application of IDPS organization that oversees the operation of outsourced employees IDPS IDPS should be familiar with the practices and procedures. This type of training usually get from vendors IDPS products. The organization should be such as IDPS vendors training part of the cost of purchase.

When IDPS vendors do not provide training as part of a package of IDPS, organizations should make the appropriate budget training operating personnel. This training should continue to provide, in order to allow changes to staff turnover and IDPS and its environment.

8 deploy

8.1 General

According to earlier in this standard content, it can only be successful HIDPS or NIDPS deployment in the following ways:

—Based on a comprehensive needs assessment of the risk analysis, including IDPS security requirements;

—Careful selection of IDPS deployment strategy;

—Identify organizational network infrastructure, policies, and resource level consistent solutions;

—Maintenance and operation of IDPS professional training;

—Develop training and exercises procedures to address and respond to IDPS alarm

The two main advantages and limitations of IDPS, IDPS tissue should be considered in conjunction with network-based and host-based IDPS to protect the network across the organization.

8.2 Phased deployment

The organization should consider IDPS phased deployment. This approach can allow employees to gain experience and to determine how much monitoring and maintenance resources required to support IDPS operation. Changes in demand for each IDPS range of resources is very broad, highly dependent on its security systems and environmental organizations.

In a phased deployment, the organization should start from network-based IDPS. NIDPS are usually the easiest to install and maintain the IDPS. The next step is to use to protect critical server-based IDPS host. In addition, in order to implement appropriate functionality and configuration, an organization should use vulnerability assessment tool for periodic testing IDPS and other security mechanisms.

8.3 NIDPS deployment

8.3.1 General

NIDPS HIDPS when used in conjunction with, should ensure that the tissue in a controlled operation, active testing and training environment has been the use of skilled personnel NIDPS. In operation prior to full deployment of NIDPS network, should NIDPS

test sensors at different locations. NIDPS normal position sensor described in FIG. 2 in detail below. When deploying the network sensor, an organization should balance the relationship between deployment and ongoing operational costs and the actual level of protection required.

In addition, especially in the high-speed network environment, the need to observe the extent to IP packet loss, packet loss rate as too high will seriously increase the number does not match the pattern, resulting in increased false positives even underreporting. To be effective, it may need a higher capture rate may provide a suitable network interface card or reducing the packet loss rate as a remedy similar techniques.

In order to monitor the network deployment NIDPS, particularly in the case of using a switch or TAP, data capture method should be considered. When deployed NIDPS, physical separation of tissue used should switch, or the core rather than exchange VLAN similar techniques. Typically, the switch allows only a single Switch Port Analyzer (SPAN) port function at any given time. SPAN port switch also increased CPU usage, and when the CPU has reached the end, SPAN commonly used to stop data replication.

Similarly, when the port used for network debugging, IDPS become non-functional. The organization should open the port to NIDPS function. To deal with this, organization should consider network TAP (test access port), in particular, combined upstream and downstream traffic aggregation TAP. These devices are typically passive devices, any load is not installed on the information packet. When data collection interface so that they are not visible to the network, they also increase the level of security, while still holding the two layers switch ports. TAP also features multiple ports, which can debug network problems without loss IDPS capabilities.

Figure 2 Typical position NIDPS

8.3.2 NIDPS located within the Internet firewall

advantage:

—Identifying from the external network, it has penetrated the boundary attack protection;

—You can help detect errors in firewall configuration policy;

—Monitoring attacks against the DMZ (demilitarized zone) in the system;

—It can be configured from within the organization to detect, attacks against external targets.

Disadvantages:

—Because of its close to the external network is not as strong protection;

—Can not monitor firewall to block (filter out) attacks.

8.3.3 NIDPS located outside the Internet firewall

advantage:

—Allows the number and type of attacks from external networks for file management;

—It can be found not blocked by a firewall (filtered) attacks;

—Reduce the impact of denial of service attacks;

—In the case of cooperation with external to internal firewall of the IDPS, IDPS configured to assess the effectiveness of the firewall.

Disadvantages:

—When the sensor is located outside the boundary of network security, it is subject to attack itself, requiring a reinforcing device invisible;

—A large amount of data generated in this position, so that the collected data IDPS analysis difficult;

—IDPS sensors and interaction management platform may be required to open an additional breach in the firewall, the possibility of external access management console lead.

8.3.4 NIDPS located on an important backbone network

advantage:

—Monitor lot of network traffic, thus increasing the likelihood of attack is detected;

—In the case of IDPS support an important backbone network, denial of service attacks before damage to critical subnets, have the ability to stop them;

—Authorized users in a secure internal organizational boundaries to detect unauthorized activity.

Disadvantages:

—Capture and store sensitive or risk the confidentiality of data;

—IDPS will process large amounts of data;

—Not detected not by attacking the backbone network;

—Not recognize subnet host attacks on the host.

8.3.5 Located in key subnet NIDPS

advantage:

—Monitoring attacks against critical systems, services and resources;

—Allow limited resources to focus on the greatest value of network assets.

Disadvantages:

—Security situation subnets interrelated issues;

—If the alarm is not transmitted on the private network, IDPS key related traffic may increase network load subnet;

—If the configuration is incorrect, IDPS may capture and store sensitive information, and access information in the case where the path is not specified.

8.4 HIDPS deployment

Before HIDPS be operational deployment, the organization should ensure that the operator but active environment familiar with its features and capabilities is protected. IDPS HIDPS particular effectiveness, depending on the operator's ability to distinguish between true and false alarms. This requires the organization's network topology, vulnerabilities, and resolve false alarms and other details related knowledge. Over time, the HIDPS monitored environment, operational experience with normal or substantially can identify the type of activity. Due to constantly monitor HIDPS, organizations should establish a timetable for inspection IDPS output. Way HIDPS operation should greatly reduce the risk of damage to the attacker HIDPS during the attack.

HIDPS full deployment should start from a key server. Once HIDPS routine operations, other servers can also consider the deployment HIDPS. When the host for each specific installation and configuration IDPS, HIDPS install costly and take a long time on all hosts within the tissue. Therefore, organizations should first install HIDPS on critical servers. This method can reduce the overall cost of deployment and allows less experienced personnel to focus on the most important assets of the alarm When this part of HIDPS routine operation, the organization may have to revisit the initial assessment of information security risks and consider installing more HIDPS. The organization should be deployed with centralized management and reporting capabilities HIDPS. These features can greatly reduce the complexity of deploying police from HIDPS be managed in the entire organization. In the case of mass deployment HIDPS, the organization may want to consider outsourcing their HIDPS operation and maintenance to information security management service providers.

8.5 Protection and information security protection IDPS

IDPS database stores all data related to the suspicious activity and attacks in the organization's information infrastructure is security-sensitive. Therefore, the need for data protection, and recommends the following controls:

—Using the check code to confirm the integrity of the stored data;

—IDPS to encrypt stored data;

—Properly configured database, in particular through the use of access control mechanisms;

—Including backup database maintenance procedures, including appropriate technology;

—IDPS system running the database will be sufficiently reinforced to resist penetration;

—IDPS sniffing connected to an Ethernet hub or switch (receive only) cable;

—IDPS management of separate network line.

—Regularly IDPS and connection systems vulnerability assessment and penetration testing.

Log should be stored on separate log host, rather than on the local system Advised to avoid unauthorized modification or deletion IDPS logs, configuration, and wherein the information exchanged between the attack and the collector IDPS sensors.

IDPS log may contain sensitive or private information, it should be protected in storage and transmission. Responsible for analyzing authorized personnel IDPS sensors or collect information from the appropriate protection of such information.

9 operating

9.1 General

Before IDPS operation, the organization should:

—Established process, procedures and mechanisms to ensure organizational vulnerability management process covers IDPS;

—Preparation and GB / T 20985 consistent incident management processes;

—When IDPS alarm, action should be taken of the provisions;

—Identification allows automated and semi-automated responses of condition, as well as how to monitor the results of this type of response to ensure safe and proper implementation of the action;

—Clear and prepare legal considerations.

9.2 IDPS debugging

After IDPS deployment, The organization should determine IDPS alarm features, as well as when and how to use the IDPS alarm features to ensure that the daily adjustment of these characteristics.

Most IDPS alarm with configurable properties, It allows various Alarm, include: e-mail, Messaging system, Minute Page and Network Management Protocol trap, And automatically block the attack source. Although many properties to choose from alarm, But in the organization fully understand IDPS installation, And clear Before IDPS behavioral characteristics within the organization's environment Organization should Conservative use them

As mentioned earlier use, SIEM technology may have significant value in the prioritization and mitigation aspects of IDPS alarm, for example, the vulnerability assessment data and alarm system patch level and configuration IDPS compare. In this case, the network traffic analyzer and found that the use of the tool can be further increased value, and allowing for further adjustment of alarm rules.

In some cases, Organization should delay enables the full set alarm feature, until a sufficient time to try operational requirements and alarm possibility to achieve the best balance, and ultimately to allow customization of alarm rules and responsiveness. Then,

the organization can decide what features are unnecessary, which features more helpful than other properties, which properties are most beneficial to the organization.When an alarm and responseWhen features include automatic response to attacks,Especially those that allowWhen IDPS instruct the firewall to block attack traffic source has been discovered,The organization should pay close attention to prevent an attacker use thisIDPS characteristics deny legitimate users access,That is self-inflictedDenial of service attacks. initial,These types ofIDPS characteristics should be placed in the semi-automatic mode,In this mode,,Determined by staffAdvisability IDPS activation response.

9.3 IDPS vulnerability

In terms of sensors in an unsafe manner embodiment IDPS,Like other devices on the network, as it is likely to be attacked. In attackClick to understand the case of its existence,They are more inclined to try and useIDPS any known vulnerabilities. An attacker may attempt to incapacitate the IDPS,Or force it to provide an error message. Other,a lot ofIDPS security vulnerabilities,The sending unencryptedLog files, restricting access control and lack of integrity checks on the log file. In a secure manner embodiment IDPS sensors and control platform is necessary,Processing and shouldPotential weaknesses of IDPS.

9.4 Alarm processing IDPS

9.4.1 General

IDPS generally produce a lot of output. In order to distinguish serious alarm and alarm of some worthless, a comprehensive analysis of the organization should IDPS output. Alarm typically comprises detecting a concise summary of the attack, it should include at least:

—Detecting the time or date to the attack;
—A sensor detects the IP address of an attack;
—Vendor-specific attack name;
—Standard name for the attack (if present);
—Source and destination IP address;
—Source and destination port number;
—For network protocol attacks.

Some IDPS provides a more general method used by the details of the attack. This information allows the operator to assess the severity of the attack, and should contain the following:

—Text description of the attack;
—Attack severity;
—The type of damage caused by the attack;
—Attack of the vulnerability of the type of use;
—Vulnerable to the list of software type and version number of the attacks;
—A list of related patches;
—Public consultation can be used as reference information, containing detailed

information about the attack or vulnerability.

9.4.2 Information Security Incident Response Team (ISIRT)

When an alarm is received, an organization should have appropriate information security incident response team (ISIRT). ISIRT planning organization should establish procedures dealing with security incidents (such as viruses, internal systems misuse, and other types of attacks). Organizational procedures should outline actions when information security incidents to be taken, and to establish a timetable for the training of personnel, and training staff on duty at the information event handling process. For more information security incident reporting and handling are discussed in GB / T 20985 in.

9.4.3 Outsourcing

In addition to IDPS products, some security service providers offer hosted IDPS services, including consulting and operations management center. Many organizations prefer to outsource its main support duties, including the managed security services to the service provider, so they do not have the training and retention of staff with specialized skills. When selecting IDPS products should seriously consider the security services provided by the custodian to determine if economically feasible, and to provide an appropriate level of support to maintain confidentiality. When providing managed security service solutions IDPS vendors have dealings, organizations should ask vendors at least:

—What have confidentiality agreements;

—IDPS monitoring personnel need to have what kind of qualifications;

—Supervisors need to have what kind of qualifications;

—What between the service provider and the organization's internal security personnel liaison and communication protocols are;

—To complement the organization's ability, whether manufacturers to provide emergency response services;

—Whether manufacturers to provide forensic investigation services;

—Whether manufacturers offer service level agreements (SLA);

—What reports are available, whether they can be customized according to the needs of the organization;

—Can custom inspection policy for the organization's environment, or if they have to use a preset default value;

—In order to implement these agreements, with what kind of technical measures;

—Service provider what kind of security personnel diagnostic procedures.

After careful consideration of outsourcing SLA requirements include the following details:

—Regular content of the report (daily, weekly, etc.);

—Response time index;

—When the attack occurred, organizational mechanisms (such as e-mail, pager, SMS systems, multimedia systems, telephones, etc.) communications;

—Event tracking and management procedures;

—Confidentiality and Non-Disclosure Agreement.

advantage:

—Under the same cost, with respect to the service organization to provide their own, managed security service provider may provide a higher level of security;

—Typically takes less cost, faster and more efficient realization of 7 × 24h capacity;

—Since many managed security service provider may access a lot of information from different customers, they are better able to handle suspicious activities and identify attacks;

—The tissue can be reduced effectively IDPS procedures required placement time together, and repeating the time required for all implementation details;

—Although the organization needs to understand IDPS capabilities, but without providing continuous professional training IDPS latest tools and capabilities to employees.

Disadvantages:

—Should monitor and audit the outsourcer to comply organization's security requirements, restrictions and policies;

—May expose sensitive information to a third party organization;

—If not handled carefully, it could cost more than the internal support;

—You can deprive the organization control over sensitive data.

9.5 Response Options

9.5.1 in principle

Many IDPS wide range of support response options that can be divided into active or passive.

9.5.2 Active Response

Active Response actions include automatic detection of the attack when the IDPS taken. Providing active response to intrusion detection systems are also referred to as intrusion prevention system (IPS). Active response further classified as follows:

—Collecting additional information of suspicious attacks;

—Change the system environment, to prevent the attack;

—After the alarms do not require human action, the IPS take preventive measures, and actively rejects communication (or) terminating the communication session.

IDS and IPS have many similar features, such as packet detection, acknowledgment protocol, and attack signature matching state analysis. However, the deployment of each device has a different purpose. IPS representing a combination of protection and intrusion detection capabilities, it detects the attack, followed by a static or dynamic way to prevent attacks.

IDS is a passive device that monitors activity and look for known attack signatures or anomalies. IDS is a bypass device, used to tell what kind of malicious activity has

occurred on the network. Because passive, IDS little chance of leading to a network failure.

On the other hand, IPS certificate-based and rule sets or pre-defined policies that allow or deny access to resources. IPS is a serial device, to monitor traffic and decide whether some packets lost, an unauthorized disconnect connector comprising data, or to allow traffic to pass. In other words, IPS provided by excluding malicious network traffic for the protection of information assets, and continues to allow legitimate activity occurs. IPS are two main types:

—Direct software running on a workstation or server, and can detect and prevent threats to the local host - host-based IPS (HIPS);

—Network-based IPS (NIPS) - standard binding IDPS, IPS and the characteristics of the firewall. Traffic is transferred to the detection engine to determine traffic situations caused by threats. When malicious traffic is detected, an alarm is generated, the malicious traffic is discarded.

As HIDS, HIPS depends on the software installed directly on the protected system, and closely tied to the operating system and services. This allows the system to monitor and call the operating system or interrupt APIs, to stop and record the attack. NIPS binding IDS, IPS and the characteristics of the firewall. Packets may occur within the interface or an external interface, and is transmitted to the detection engine to determine whether the packet is a threat. Upon detecting malicious packets, an alarm, the packet is discarded, the information flow is marked as malicious. This makes the remaining packets arrives at the particular TCP session IPS device and is immediately dropped. Features more sophisticated IPS can prevent individual packets rather than the entire session, they can dynamically reconfigure the firewall rules to route traffic to a honeypot, or a combination of these activities and so on.

HIPS software intercepts all requests to the system of protection. So it should be very reliable, and should not affect the blocking legitimate traffic.

advantage:

—The ability to detect and block attacks;

—Provide active protection;

—By reducing the response to the log of events in claim IDS, improved operational efficiency.

Disadvantages:

—Serial work, thus creating a potential bottleneck and single point of failure;

—IDS is to bring the impact of false positives may be more serious and far-reaching, that is likely to cause a denial of service attack itself;

—Is below the expected traffic load, no significant effect on the flow rate, it should be analyzed for each information packet;

—Active response may be applied to only a subset of the feature set;

—The HIPS software is tightly integrated into the operating system kernel, the future operating system upgrades may cause problems.

9.5.3 Reactive

Passive response providing information to an operator or a predetermined position. They rely on IDPS operator to take follow-up action based on the information provided. Passive response has the following form

—Alarm and notification, usually the screen reported, pop-ups and pager or cell phone information;

—Configure SNMP traps in response to a central management console.

9.6 Considerations legal

9.6.1 General

Criminal investigation after evidence collected information systems may contain sensitive information, employee data or,thus,Responsible should save or process data and full compliance with applicable laws. The organization should ensure that its personnel are aware of this connectionDuties. This section outlines the considerations relating to the legal aspects of IDPS.

9.6.2 Privacy

During normal operation,IDPS system can collect personal information,And it can be used to monitor employee activities. ThisPrivacy and may be subject to applicable regulations. The organization should develop and implement strategies to ensure that any use of IDPS is consistent with relevant privacy and applicable law.

9.6.3 Other legal considerations and guidelines

IDPS implementation and operations may be subject to other legal and regulatory requirements, and deployment approach requires IDPS organization. The implementation and operation of IDPS, should review and deal with legal, regulatory and corporate policy requirements. Legal and regulatory issues are discussed further in GB / T 20985 in.

9.6.4 Obtain evidence

IDPS log can be used for forensics. The organization should be appreciated discovery requests related, andIt should make appropriate storage and processingControl IDPS logs to ensure that this information can accept forensic review. You may also need to file information about the IDPS systems and processes to meet forensic and evidentiary requirements.

附 录 A
(Informative)
Intrusion detection and prevention systems (IDPS): Framework and issues to consider

A.1 Intrusion detection and prevention of the introduction

Although the vulnerability information systems can lead to accidental or intentional use, intrusion and attack, but because of business needs, organizations still use the information system and connect it to the Internet and other networks. Therefore organizations need to protect these information systems.

Advances in technology, the convenience of access to information continues to increase, but new vulnerabilities can arise. At the same time, to exploit these vulnerabilities to attack has also been strengthened. Intruder invaded the continuous improvement of technology and information in their favor are increasingly easy to obtain. It is also important, due to the popularity of computer knowledge, and advanced scripting attack tools available, to attack the necessary technology is weakening. Thus, an attacker can occur without one knows for sure what will be able to bring any harm or attack happening.

A first layer of defense protecting information systems using physical, administrative and technical control, should include identification and authentication, physical and logical access control, auditing, and encryption. Organizations can find a list of recommended control in GB / T 22081-2016 in. However, from an economic standpoint, always protect the integrity of each information systems, services and networks are not possible. For example, for a global use, there is no geographical boundaries, and its internal and external network difference is not obvious, difficult to implement access control mechanisms. In addition, the traditional perimeter defenses are no longer viable, because organizations are more and more trust of employees and business partners remote access. IT environment caused by the complex network configurations, and these configurations are dynamic, including access to multiple access points in an organization's IT systems and services. Accordingly, in order to respond quickly and effectively find invasion requires a second layer of defense. This layer is mainly borne by the Defense intrusion detection and prevention system (IDPS). In addition, the feedback has been deployed IDPS can improve the knowledge of the vulnerability of corporate information systems, and can help improve the overall quality of the organization's information security.

Organizations get IDPS software and (or) hardware product, or service provider deployment by outsourcing to IDPS IDPS IDPS functions, etc. from the market. In any case, the organization should know IDPS is not a Plug and Play device, the effective deployment requires some understanding of the organization of the IDPS.

The effectiveness of each control, organizations need to assess prove IDPS deployment

of the information security risks and IDPS deployment into the information security management process. In addition, the need to consider, once the intruder or attacker eavesdrop on the information contained within the IDPS have been deployed and covering it, the organization will encounter enormous difficulties. These difficulties include how to identify and prove protective measures (such as IDPS) requirements. Organizations and related service systems or security policy statement should be protective measures in order to select the proper management of invasive risk. These protections include:

Eleven reduce the chance of the invasion;

Eleven effective intrusion detection and response that may occur.

Like every control as organizations need to assess the effectiveness of proof IDPS deployment of the information security risk, and into its information security management process. In addition, the need to take into account, in case intruders and attackers from intercepting the information contained in the IDPS deployed and covering it, will face enormous difficulties in the organization.

When organizations consider deploying IDPS, you should know:

Eleven pairs of information systems and (or) the type of network intrusion and attacks;

Eleven generic model IDPS standard mentioned.

A.2 Types of intrusions and attacks

A.2.1 Brief introduction

Information systems and intruder attacker can use the information system and (or) a network configuration of a defect, defects and the implementation (or) the concept of defects, and can be utilized in a user abnormal behavior.

Vulnerability would intruders and attackers access to protected information systems and the information processed or stored, and undermines the confidentiality, integrity and availability of information and information systems. These give the intruder the invasion and attack and attack information systems and networks provide valuable information, and this information can be used by more sophisticated intrusion or attack techniques. The organization should recognize not only outside the organization who will be trying to invade and attack, and that the internal staff may also have such an intention. For example, an authorized user organization's information systems may attempt to gain unauthorized additional privileges. Malicious intrusions and attacks can be used to:

Eleven information gathering, the attacker tries to retrieve details information collected target information system;

Eleven attempt to gain unauthorized system privileges, resources or data;

Eleven compromise the system, system resources may allow the use of further attacks;

Eleven information leakage, intruder attempts to use the protected information (such as passwords, credit card data) with unauthorized means;

Not refuse service (DoS) attack, the attacker tries to target information system

services become slow or suspend their services.

In terms of possible vulnerabilities and intrusion attacks, intrusions and attacks can be divided into:

Eleven host-based;

Eleven-based network;

Eleven based on a combination of methods.

A.2.2 Host-based Intrusion

Host-based Intrusion usually invasive activities that may introduce damaging malicious code (for example, using the attacks, Trojans, worms or viruses), and occur in the following areas:

Eleven application layer (SMTP, DNS) (such as fake e-mail, spam, buffer overflow attacks, race condition attack, middle attack);

Eleven identification system (such as the use of eavesdropping or password guessing attack);

Eleven Web-based services (such as attacks against CGI, ActiveX or JavaScript is);

Eleven system availability (such as denial of service attacks);

Eleven operating system;

Eleven network and application management systems (such as SNMP attack).

A.2.3 Network-based intrusion

Network-based intrusion is generally considered intrusions at the following locations:

Eleven physical layer and data link layer communication protocol and system embodiment thereof (e.g., ARP spoofing, MAC address clone);

Eleven network layer and transport layer communication protocol has been implemented and the system (IP, ICMP, UDP, TCP) (eg IP- spoofing, IP- debris attacks, simultaneous flooding attack, the attack abnormal TCP header information).

A.3 Universal model intrusion detection process

A.3.1 Brief introduction

Software and (or) hardware products combining IDPS through automated monitoring, collection and analysis of information systems or networks of suspicious events, found signs of invasion. Universal model of intrusion detection can be used to define a set of functions. These functions include: the original data sources, the situation detection, analysis, data storage, and response, as a function of these separate components or as part of a larger system embodiment of the package. Figure A.1 way of illustration of these interrelated functions.

图A.1 Universal model Intrusion Detection

A.3.2 Data Sources

Intrusion detection process depends on the success of the detected intrusion attempts data source information. Data sources can be determined as:

Audit data eleven different system resources: audit records contain data messages and status information, the range of very detailed data from the high-level abstraction of information to the display time sequential flow of events. Available sources operating system audit data log files, including system events and activity logs generated by the operating system, such as the audit trail / log. Can be a good source of application information log file system, network services, such as access attempts are also the raw data;

Eleven operating system resource allocation: system monitoring parameters, such as the workload of CPU, memory utilization, the system resource shortage, the input / output rate, the number of active network connections, etc., can help detect intrusion;

Eleven network management logs: network management logs provide a robust level of network devices, device status and state transition information;

Eleven Network Flow. The network flow provides information such as source and destination addresses, and parameters related to the safety of the source and destination ports. Options different communication protocols (such as IP and TCP state flag indicates the source or the route and try to connect confirmation) to IDPS is useful. Because the possibility of collecting data before being manipulated very small, so the OSI model to collect raw data on low-level basis is helpful. If only the higher level of abstraction to collect raw data (such as a proxy server), the information may be lost on the lower level;

Eleven other data sources: other data sources include firewalls, switches and routers, including of course IDPS particular sensor / monitor agent.

The original data source is divided into two categories: host and network. Because in the field of intrusion detection to distinguish the position of the dominant, IDPS is also divided into two types: host-based and network-based. Host-based IDPS can check the audit trail / log, and other data from the host or application. IDPS network mesh network management can check blogs, and data from firewalls, switches, routers, and IDPS sensor Agent.

A.3.3 Detection of events

The purpose of affairs detection is to detect and provide data security-related matters, for analysis.

Detection of affairs may be simple affairs (including part of the event or attack during normal operation) or complex events (including the simple state of affairs is likely to represent a combination of a specific attack). However, the situation or the situation data may not be used as evidence of invasion.

Situation detection function is achieved by monitoring the IDPS member. They can be installed on a network device (such as routers, bridges, firewalls), or on a specific computer (such as application servers, database servers), depending on original data sources to be detected events data.

Since the detection process events generate a lot of events data, the frequency of detected events can affect the overall effectiveness of the IDPS. This situation will also apply to the following analysis.

A.3.4 analysis

A.3.4.1 Brief introduction

The purpose is to analyze the situation analysis of data and processes events detection functionality provided, are trying to find, and the invasion has occurred or is occurring.

In addition to the events detected data, analysis can take advantage of many sources of information or data, including:

Eleven result data previously analyzed and stored by the data storage capabilities of data;

System-from individuals or are expected to show how the knowledge (as known from the task should be carried out and should be completed by an authorized activity) generates information or data;

Individual or system-from undesirable information or knowledge of how to behave in the data (such as from a known attack or known to be harmful actions) generated;

Part other relevant information or data, such as the original suspected attack site, the individual or the attacker position.

There are two general methods of analysis: based on misuse and anomaly-based. Also known as knowledge-based methods misuse based method based anomalies, also known as behavior-based approach.

A.3.4.2 Based on method of misuse

A.3.4.2.1 General

Methods misuse of evidence-based attack detection main aspects of the situation data and knowledge known attacks and unauthorized activities based on accumulation.

Typical methods based on misuse of trying to known attacks on information systems as well as specific attack signatures previously considered to be malicious or intrusive behavior and activities, modeling and coding to include a system scan to detect these information systems attack signatures. Due to minor variations known attack patterns or

known feature called attack, thus sometimes called misuse detection feature-based IDPS.

In commercial products, the most common signature-based attack detection technology is specified for each consistent with the mode of attack or unauthorized activity state of affairs, as an independent attack signatures. However, more complex mechanisms to allow use of a single set of attack signatures to detect unauthorized activities and known attacks.

Note that, when based on the assumption that the situation does not match the data misuse attack signature method based, does not mean that there is intrusion or attack, but does not match some of the data may still contain evidence of invasion or attack, the evidence in feature modeling attack is unknown.

Currently, the method of analysis used widely misused based are:

A.3.4.2.2 Attack signature analysis

This approach may be the most common method of intrusion detection, it expects the information system of any safety-related behavior can produce corresponding audit log entries.

Intrusion scenario may be converted to the audit log sequence or data mode, the data information can be generated in a computer operating system, applications, firewalls, switches and routers, monitors or sensors, or specific IDPS found. Or other sequences may be found in the network attack signatures transport stream. Analysis protocol analysis is a form of network attack signatures particular, it uses the well-defined communication protocol structure. Protocol analysis can handle such packet, frame and connecting elements.

By analysis program, collecting semantic description of known attacks or attacks its features or unified format, and save it in the database. When they find a particular sequence or attack signature matches a predefined intrusion features, such as the audit log, it means have a intrusion attempt.

Attack signature analysis method can be used with a threshold or not the threshold value. If the threshold is not defined, when an attack signature identifying i.e. to generate an alarm. When the defined threshold, an alarm is generated only when the characteristic exceeds a threshold number of attacks. Threshold may be the ratio of the number or other measure of events per unit of time.

The main disadvantage is the need to attack signature analysis methods constantly updated attack signatures in order to discover new vulnerabilities and (or) attack.

A.3.4.2.3 expert system

If misuse is a method based expert system contains rules describing the invasion. If the exception-based method, generating a set of rules for a given time, the recording based on user behavior statistics user's usage behavior. Rules should be constantly updated to accommodate the new description of the invasion or new usage models.

After the audit situation is converted to the fact that its semantic expression, enter the expert system. Intrusion analysis capabilities to use these rules and facts to conclude that in order to detect intrusions or detect suspicious behavior inconsistent.

A.3.4.2.4 State Transition Analysis

This technique is described a series of goals with invasion and transformation, and represent them as state transition diagrams. State and system state are consistent with attack signatures, and includes states associated with these Boolean statements that should be converted to meet the other states.

A.3.4.3 Anomaly-based approach

A.3.4.3.1 General

The observation of the intended use of other conventional profile defined by the normal operation of the observation system or parameters, the method based on the focus on the abnormality of the behavior prediction or conjecture typically found unconventional behavior. A profile is a particular predefined pattern of events, generally a series of events associated with, for comparison purposes stored in a database.

Note that, when based on the assumption that the situation data does not match the attack signature for exception-based representatives of invasion or attack, but some of the data does not match may still contain the normal evidence or unauthorized behavior, the evidence in feature modeling attack is unknown.

At present, the abnormal method of analysis based on the widely used are:

A.3.4.3.2 To identify abnormal behavior

This method is suitable user activity patterns match the attack signature analysis and improper activity matches.

This method of normal or authorized user behavior modeling through a series of tasks that the user through the use of non-statistical techniques are required or authorized to perform on the system. These tasks are described as desired by the user or authorized behavior patterns, such as the right to access to specific files or file types.

Individual behavior found in the audit trail compared to the expected or authorized mode when the expected behavior patterns or licensing mode is not the same, an alarm is generated.

A.3.4.3.3 expert system

(See A.3.4.2.3).

A.3.4.3.4 statistical methods

In the anomaly-based intrusion detection methods, the most commonly used statistical methods.

By a number of different samples to measure the user or system behavior and stored in the configuration file. Combined with the current configuration file on a regular basis has been stored profile, and with the evolution of user behavior to be updated.

Examples of these changes include the number of each session login and logout time, duration, resource utilization, disk storage and processor resources consumed within a

session and a given time.

Profiles can be composed of different types of metrics, these types comprising:

Eleven activity intensity measurement;

Eleven audit record distribution measure;

Eleven classification measurement (e.g. relative frequency log);

Eleven count measurement (e.g., a set of values for a particular user CPU or I / Os).

Abnormal behavior is stored by the profile check to determine, i.e. to determine whether the threshold is exceeded in accordance with the standard deviation of the variable.

A 3.4.3.5 Neural Networks

A neural network is an algorithm used to study the relationship between input and output vectors in a reasonable way to find common rules to obtain new input - output vectors. Intrusion detection, the main purpose neural network learning system within the behavior of characters (such as user daemon). In statistics advantages of using neural network that represents a simple neural network with nonlinear relationships between variables, but also in self-learning neural network and retraining.

A 3.4.4 Combination method

The method of misuse and abnormal based on can be combined to exploit the advantages of each other. IDPS deployment of the hybrid mode to allow intrusion detection based on known attack signatures and unconfirmed mode (such as the number of times a particular user login attempt).

There are also studies underway to explore other ways or methods of detecting intrusion. Petri nets such as applied research, and study of computer immunology, relatively new.

A.3.4.5 Frequency Analysis

A 3.4.5.1 General

Raw data (such as audit trail or log) is usually produced constantly, but they may not always be processed or analyzed by the situation analysis of the situation detection.

The frequency analysis may be:

Eleven continuous;

Eleven periodically;

Eleven specific environment.

A 3.4.5.2 Continuous or near real time

When the situation continues to look for specific data detection occurs, the situation is the situation or activity and provides data, analysis still ongoing.

It should be noted that, in some cases before it is detected and reported, intrusion may be completed, because the time of occurrence of events and may detect and report the

presence of a time interval between the time it is. Time interval can be determined by the parameters such as the data source events, intrusion detection methods or properties, which results in the time between the start and intrusive invasion difference target system

A.3.4.5.3 Periodic or batch processing

If the original data, and (or) the detected data transfer events into a storage medium, or the periodic detection and (or) analysis of the data at the appropriate time will be possible. For example, to detect and analyze IT systems at low load, such as at night or through a bypass auxiliary subsystems.

A.3.4.5.4 Initiated only under certain circumstances

Some analysts may be initiated only under specific circumstances, such as when already identified a wide range of attacks, and are causing serious damage when. In this case, it can be taken to focus on all aspects of the attacks and the consequences of a comprehensive analysis. These ways sometimes called forensic analysis can be used for the purpose of legal proceedings. If there is expected lawsuits, we need to follow the rules of evidence applicable.

A.3.5 data storage

The purpose of data storage function is to store security-related information and make it available for later analysis and (or) reports.

Data storage may include:

-Detected events and other types of necessary data;

-The results of the analysis, including the detected intrusion and suspicious events (later used to coordinate suspicious situation analysis);

-Collection of known attacks and normal behavior profile;

-Once the security alarm sounded, collect and preserve evidence in detail as the original data (e.g., for traceability).

Matters should have the appropriate data retention and data protection strategies, handle a variety of concerns, such as the completion of the analysis, data forensics and evidence preservation, and to prevent security-related information to be tapped.

A.3.6 response

The purpose of the response function is the appropriate analysis results presented to the responsible personnel (such as system administrators, security person in charge). Generally, these results are presented in the form of a graphical user interface on the management console, by other means e-mail, text messaging, telephone and other relevant personnel will be informed of the results is also necessary to enhance and organize a response to the alarm

Passive response function only when an alarm console, and active response capabilities also provide an appropriate response to the invasion. Having an active function in response to intrusion detection systems are also referred to as intrusion

prevention system (IPS). Some active response function by the way, provide corrective or preventive measures to limit the intrusion or minimize the impact:

-Reconfigure intrusion system;

-Lock invasion account;

-Blockade session protocol.

Information provided in response function can help organize reasonable authority to assess the severity of the invasion, and decided to implement appropriate countermeasures. Organizations need to ensure that, to assess the severity of the invasion and Strategies to be implemented to be consistent with the information security policies and procedures of the organization.

In Chapter 13 GB / T 22081-2016, the organization can find a list of recommended control, including reporting information security events, responsibilities and procedures to recover from system failures and correct security vulnerabilities in. GB / T 20985Also provide useful information on the management of information security incidents.

A.4 IDPS type

A.4.1 Brief introduction

As described above, there are three types of IDPS: IDPS based feature, based IDPS abnormal state IDPS protocol analysis. Most IDPS using a variety of detection methods (either alone or integrated) to provide a broader and more accurate detection. Detection major categories as follows:

Identifying the event based on the feature detection means known threat signatures events will be observed compared. This is very effective in detecting known threats, but many variants to detect known threats and unknown threats largely ineffective. Based on the feature detection and tracking can not know the state of the complex communication, it can not detect most attacks include a plurality of events.

, It is defined based on a comparison of normal activity and detection of abnormalities observed events, to identify significant deviations. The typical method of forming the monitoring activity profile over time profile. Then, IDPS and the characteristics of the current active profile associated with a threshold value. Anomaly detection method can be very effective in detecting previously unknown threats based. FAQ anomaly detection of malicious activity based on the configuration file is accidentally included the establishment of the configuration file is not adequately reflect the complexity of real-world computing activities, and produce many false positives.

State protocol analysis, refers preset profiles (the profile of each active protocol as benign state protocol generally accepted to be defined) are compared to identify events with the observed deviations. Unlike anomaly-based detection (using a specific host or network configuration file), depending on the general state protocol analysis profile supplier development, the configuration file specifies how a particular protocol should be used and not how to use. It is able to understand and track the status of the protocol state has the concept, which enables it to detect many other methods can not

detect the attack. Problem state protocol analysis include the development of complete and accurate protocol model is often very difficult or impossible, is very resource intensive, and can not detect the attack is not contrary to accepted protocol behavior characteristics.

IDPS Other types include:

-Application-based IDPS (AIDPS), which is a special type of HIDPS HIDPS and has similar properties.

Generally speaking IDPS can achieve the following functions:

-Monitor and analyze system events and user behavior;

-Identifying a known attack patterns corresponding system events;

-Identify statistically different from normal activity patterns of activity;

-When an attack is detected, appropriate to remind employees through reasonable manner;

-In measuring performance analysis engine coding security policies;

-Allow non-security professionals to perform important security monitoring;

-Increase the perceived risk and the ability to find the attacker's punishment;

-Many other security devices to identify problems could not be prevented;

-Coordination of other safety equipment (such as firewalls) to deal with the situation;

-Verify, List and describe threats to the organization's information network system;

-Provide information about the invasion of valuable information that support event handling, damage assessment, restoration work and legal activities specific environment.

IDPS should understand the limitations of the main limitations include:

-Can not detect new attacks, we can not capture the majority of new variant of the attack;

-Irreparable sources of error and noise;

-The process is difficult to effectively switched network;

-Difficult to scale to a very large or distributed network;

-Difficult to determine the physical and (or) the position of the intruder based IDPS virtual output;

-Difficult to use NMS to integrate different IDPS products;

-Irreparable security policy and (or) security mechanisms (such as firewalls, identification and authentication, link encryption, access control mechanisms and virus detection and removal) defects in infrastructure protection or missing;

-It can not detect, report or respond quickly to the specific type of attack;

-Despite the ability to identify DoS attacks, but can slow down the most DoS attacks;

-Detecting new attacks can not attack or existing variants (which only applies feature-based IDPS, unavailable for anomaly of IDPS);

-In the case of human intervention, we can not attack a detailed analysis;

-Can not make up significant deficiencies in the organization's security strategy, policy or security architecture;

-You can not make up for the security flaws network protocol;

-Usually, IDPS output may contain a significant error rate, especially false

positives, we need to spend a lot of time and resources to solve;

-It may be disabled as part of the attack sequence;

-They could be exploited by attackers to generate false positives, in order to distract attention from the main attack;

-It may produce a large amount of audit information, which may take up additional local storage system;

-Based IDPS alarm automatically block may cause security and availability issues;

-It requires advanced technology and systems knowledge in order to effectively use the IDPS.

A.4.2 Host-based IDPS (HIDPS)

HIDPS present within one computer and provide protection for this particular machine. This allows the computer's operating system to check HIDPS log data (e.g., audit trails / logs), and other local data. HIDPS also analyze developments occur within the application using the operating system or application log files.

Operating system audit trails HIDPS generally used by the operating system kernel (core) is produced, and therefore in more detail than the system log and better protected. However, these systems are shorter than log audit trails and easy to understand.

Some HIDPS designed to support IDPS management and centralized reporting infrastructure, which can allow a single management console to track multiple hosts. Other HIDPS generating a message for compatibility with the network management system format.

And NIDPS different, HIDPS could sense the result of an attempt to attack, because it can directly access and monitor data files and system processes attacks are usually targeted. For example, HIDPS allow detection of attacks from the mission-critical server keyboard.

HIDPS intended to be used:

-The specific user identity associated with suspicious activity;

-Observe and track changes in user behavior;

-Establish baseline system security status, and track the change from baseline;

-Management operating system auditing, logging mechanism and generated data;

-When data is encrypted or non-encrypted form for transmission and storage, application layer provides logging and surveillance;

-Observation data changes caused by the attack;

-Present in the system monitoring high-speed network and the encrypted network;

-Detect network-based attacks IDPS can not be found.

HIDPS should understand the unique limitations. The main limitations include:

-Specific DoS attacks can cause HIDPS ineffective;

-HIDPS may consume host resources, including the required host audit log data storage;

-Because of the large number of installations (at least one per host), you may require complex installation and maintenance;

-In stealth mode can not be used, because the host is typically addressed by a higher network layer;

-It does not recognize attacks against other hosts or networks.

A.4.3 Network-based IDPS (NIDPS)

NIDPS flow monitoring leads to a host system in the network. Typically, NIDPS by the host or a series of single use sensor located in a network different compositions. These cells were analyzed by the local traffic and report attacks the central management console to monitor network traffic. Because the sensor is particularly useful as IDPS member, so they are less likely to be protected against attack. Many such sensors higher network layer are not visible (i.e. is designed to run in "stealth" mode), to make it more difficult for an attacker to determine their presence and location. .

And HIDPS response time is directly related to the frequency of the polling interval by providing intrusion suspicious (e.g., DoS attacks) information occurs, NIDPS allows real-time or near real-time detection and response.

NIDPS with unique functional properties, its capacity is as follows:

-And the higher level of the sensor network protocol (layer 3 and above usually) hidden in a "stealth mode";

-Using a single sensor monitoring the flow of a plurality of hosts on the same network segment;

-Many hosts to identify the impact of distributed attacks.

NIDPS should understand the unique limitations. The main limitations include:

-Can not handle encrypted network traffic;

-You may require more bandwidth than HIDPS and faster processing capabilities, because should NIDPS performance equivalent to the capacity of the flow to maximize the performance of the deployment of the network segment;

-NIDPS many features provided may be provided to require special techniques in modern switch-based network is available (e.g., sensor networks, it needs to connect to a particular network switch port to all other ports mapping data);

-Because of issues related to the application layer protocol decoding (e.g., HTTP, SMTP), and some may NIDPS processing network layer (IP) or transport layer (TCP / UDP) data packet segment difficulties attack;

-Usually we can not observe whether the attack was successful.

A.5 Architecture

IDPS can be achieved in different ways.

In smaller organizations, or to protect the well-defined and relatively independent system, a single IDPS may be a good solution.

In the considerable and complex support network infrastructure, environmental systems and applications, a single IDPS may not be sufficient or can not meet the requirements of intrusion detection. To meet these requirements, may require multiple IDPS, IDPS is customized for each subsystem or component has been defined. In this environment, a

plurality of subsystems or components may attack against. In another case, an attacker may be configured for a particular component or subsystem, or subsystems rather than vulnerability member itself. In order to detect attacks such cases, correlate and analyze data from different IDPS of events.

IDPS target architecture is based on an efficient and effective way to achieve intrusion detection features. In this context, about the two key architectural considerations are:

-And a plurality of interconnected IDPS associated manner;

-IDPS centralized or distributed architecture task.

Example of a layered intrusion detection architecture shown in Figure A.2.

图A.2 Layered intrusion detection architecture

In Figure A.2, the output member and associated plurality of analysis are further aggregated, to obtain a higher level of analysis and correlation. In any multi-tier application infrastructure, there may be more than one location to operational requirements.

In the centralized architecture, and sensor means detecting the situation may simply collect raw data and sends it to the individual components for further analysis and correlation. Although this method is simple design, but it may not scale well, and may apply only to smaller environments.

More scalable solution IDPS perform certain tasks in the dispersion member, the goal is to reduce as early as possible in this process the raw data, and sends the relevant matters to the next layer member. Chain member may further analyze and correlate events data, only the relevant alarm or transmitted to the final situation, i.e., the core

member. Such a system may have some very complex task. For example, this requires indicated by attacking the central member and find the correct manner of giving the alarm, and to configure the filter member associated analysis and correlation.

A.6 IDPS management

A.6.1 Brief introduction

In the enterprise network infrastructure, management, intrusion detection and prevention systems are efficient and effective deployment of their critical. IDPS order to make more efficient management subsystem should provide sufficient functionality. This section discusses various aspects of IDPS management.

A.6.2 Configuration Management

A.6.2.1 General

Configuration management provides several features for controlling, entity identification (IDPS part of those entities), and provide the data collected therefrom For the purpose of intrusion detection, configuration management, including management and detection of the corresponding response mechanism

A.6.2.2 Detection

Configuring detection function including the sequence of events and developments violation of security policy and setting standards. This may also include a description of misuse mode and normal user behavior.

A.6.2.3 Response function

Management response function determines the behavior of the security alarm system This includes controlling in response to a variety of mechanisms, such as an audible alarm to notify the administrator, and (or) the security personnel and the session termination. IDPS should also be protected against unauthorized initialization response. If an attacker found a way to cheat the system to respond to the invasion does not exist, it is possible to install than no IDPS cause more damage, depending on the configuration response. Response Management Event Management program should be consistent with the organization.

A.6.2.4 Security Management Services

Security service management includes IDPS as part of the security services management. It contains control user certificates, confidentiality, integrity, and access control services. According to the user's credentials, access may be limited, to restrict access to information on the security situation on the configuration parameters, as well as an audit trail.

A.6.2.5 Integration with other management systems

IDPS receiving network management system and should be managed under the protection

of the environment, and management system (or) the safety management system security interface, or management of these systems to become an integral part. This is the realization of some type of detection (e.g., the access log) function and some type of response may be necessary. Choice is important not to separate or implemented IDPS because IDPS management functions should be integrated with other system management functions.

A.6.2.6 Security management operations

A.6.2.6.1 General

Security should protect the management operations to prevent intruders from accessing information or IDPS IDPS control of resources. IDPS security management, including authentication, integrity, confidentiality and availability management services.

Administrative privileges to run IDPS system should be (compared to other management systems that require security policy) are configured according to the required high security level security policy. Host IDPS sensors usually run an operating system privileged mode, therefore prejudice the administration of privilege could result in a very wide range of security vulnerabilities and possible damage to all hosts running IDPS agents. Based IDPS, especially host-based IDPS, the consequences of administrative privileges are often overlooked security vulnerabilities, and attacks most commercial products with executable instructions to monitor the host response options.

Monitor developments detectors and sensors to ensure proper operation and function of IDPS essential for success. The events detector information from the sensors is transmitted to the detection analysis. Failure to maintain these devices continues to monitor the safety function may lead to erroneous sensor, such as sensor failure and a central system (and thus the entire organization) are not aware of this technical failure. Therefore, the central system will not send an alarm or reading to still believe that everything good central administrator.

A.6.2.6.2 Differentiate

Before performing management operations on the managed entity should be appropriate for identifying and authenticating. Management entity may be a user or system entity.

A.6.2.6.3 Integrity

It should protect the integrity of management operations to prevent attacks. Not in an unauthorized manner insert, delete, or change management operations.

A.6.2.6.4 Confidentiality

Management should protect the confidentiality of operations in order to avoid attacks. No unauthorized manner inappropriate to speculate any intention of management operations.

A.6.2.6.5 Availability

For network infrastructure, IDPS itself or surveillance target attack should not affect the availability of managed services. For example, when a denial of service attack occurs, it should be feasible IDPS management. Even IDPS fails, it should be possible to manage the IDPS. IDPS and its management should be incorporated into business continuity planning process.

A.6.3 Management Model

Control and management is essential for the successful implementation of intrusion detection, especially in a distributed environment using a large number of intrusion detection component. Figure A.3 provides an example of a tiered management model, this model is perfect for large organizations. In some cases, the centralized control means that a single point of failure, in some circumstances may not accept this situation. It will also give attackers a single point of attack. This could give the attacker the opportunity to delay attack detection, and prevents the administrator to take appropriate action.

图A.3 Intrusion Detection Management Model

In addition to using the hierarchical model in many collections, you may also use other appropriate management relationship collection:

-Many to many: multiple management consoles can manage multiple distributed agents;

-To-many: one Management Console can manage multiple distributed agents;

-One: one Management Console can manage an agent.

A.7 Implementation and deployment issues

A.7.1 Brief introduction

When decisions need to deploy IDPS, there are many important issues and considerations. All IDPS not identical, therefore, enterprises in the deployment IDPS evaluate, should consider the requirements of enterprises according to their IT risk management and security policies.

A.7.2 effectiveness

When deploying IDPS to be evaluated, an important consideration is the efficiency. Evaluation of IDPS efficiency standards are:

-Accuracy: When the IDPS activities mistaken attack (such as false positives) or IDPS to attack mistaken for legitimate activities (such as false negatives), the error will occur. Any type of failure to the total number of events detected ratio will significantly affect the availability of IDPS. The ratio of false positives and false negatives may be an important security policy parameters, and may indicate the implementation of analytical bias.

-Performance: Performance IDPS is to speed the collection, storage and processing audit events. If IDPS poor performance can not be detected in real time. On the other hand the performance of the network load IDPS may arise.

-Comprehensiveness: When IDPS can not detect the attack, there will be no comprehensive. This measure is more difficult to assess the evaluation index compared with other, because comprehensive understanding of assault or abuse of the privileges is not possible.

-Fault Tolerance: IDPS itself should be resistant to attack, especially denial of service attacks, and should be designed according to this target. This is particularly important because most IDPS runs on top of commercial operating systems or hardware, it is known here vulnerable.

-Timeliness: IDPS must be performed as soon as possible and send its analysis report to the person in charge of security response can be made before extensive damage caused, the same should also prevent the attacker from corrupting data, data source or IDPS itself.

A.7.3 Feature

When deploying IDPS, another important consideration is the functionality of the previous section discussed. The following will discuss some of the functional aspects of content:

-Use encryption or exchange environment, host-based IDPS well suited for encryption and exchange environment. Because host-based systems deployed on a variety of host companies, they can overcome the deployment challenges faced by network-based IDPS in exchange and encryption environment.

-Detecting an attack, the source network-based data allow the time of the attack by providing data to detect malicious and suspicious attacks (such as denial of service attacks) to detect and respond to real-time, and also provides a more rapid response and notification. Network-based IDPS can detect a host-based systems miss attacks. Many able to identify them by looking up the IP header when denial of service attacks and fragmented packet transmitted in the network based only.

-Comprehensive analysis of host-based and network-based data, both the host and the use of some of IDPS network data sources to the integrated member hosts and networks. As discussed in 6.1, network-based and host-based IDPS solutions have their own unique

advantages and strengths, can complement each other. Therefore, host-based and network-based intrusion detection technology can be integrated analysis, in order to create a more powerful defense information systems.

A.7.4 IDPS deployment and operations personnel

IDPS organization selected may be the most advanced, and between subsystems and IDPS with the organization's IT systems, services and (or) network can be well integrated. However, most features should be manually operated by personnel with the trained and understand intrusion detection, IT security (including network security), and the IT organization (including network topology and configuration).

Intrusion detection process including the installation of IDPS and have the human resources have the following capabilities:

-Custom IDPS have to be able to find and deploy IT environments IDPS-related matters;

-When the alarm disappears, explain what IDPS to express;

-In response to the IDPS look real alarm, develop policies and procedures;

-Correct the cause of the vulnerability of the success of the invasion.

These labor intensive operations beyond the scope of IDPS installed intrusion detection process and should be an integral part of.

Analysis analyze data collected by the sensor to detect signs of unauthorized or suspicious activities or events, these signs may indicate that the probe is / scan the network intrusion has occurred or malicious attack is in progress. If there is no manual input, configuration, and interpret the output adjustment support IDPS, automated part will not be able to run.

When the IDPS is properly configured, it provides information should be carefully analyzed to understand intrusions occur in the network. IDPS requires intensive interaction of people, not know what to wait for the network to reject packets that do not want. IDPS requires skilled personnel to understand when the output IDPS be regarded as merely false positives (legitimate activities were as invasion) or false negatives (the invasion activity occurred, but was identified as non-invasive).

Response functions include manual and automated tools. For example, most of the current IDPS to points according to a predefined alarm criterion Alarm severityClass, rarely point out what should be done when an alarm occurs. Because of today's most IDPS produce a lot of false positives, and in most cases the first level of response would involve quite inexperienced operators, leading to further aggravate the situation. Even if the operator has the honor organizations both knowledge and experience, they can not know how to respond to each of the detected intrusions properly. On the other hand, the situation in the tense period of rapid expansion, the rapid response of the IDPS is very important to the police. For these and other reasons, to provide the operator through careful consideration, to an overview of the specific types of IDPS guide alarm should take steps to deal with extremely important. If these guidelines are not available, then the response of the IDPS alarm may be inadequate, disorganized or overreaction. Totally dependent automatic response mechanism is unwise.

By pattern matching the payload of known vulnerabilities or by malicious bytecode

feature, IDPS may detect a zero day exploit, in this unusual situation, personnel should be coordinated with the appropriate vendor has to be aware of an unknown the new vulnerability has been discovered and the vulnerability is attacking an organization's network.

A.7.5 Other implementation considerations

When considering the implementation, operation, and when the integration selection IDPS, there are other important features as follows:

-User interface;

-The layout of the sensor network, the sensor network can be placed on a flexible support to a range of detection and response strategies, such as the detection of an attack attempt external firewall;

-System fault tolerance, system integrity is the most important concern, is an example of denial of service attacks. If possible, the communication between the IDPS appropriate sensors, monitors and network managers being independently monitored outside the network. This will improve the safety and availability;

-IDPS assurance;

-Ease of use, such as ease of use;

-IDPS of scalability;

-Interoperability with other security products;

-Vendor support level and quality;

-Management, IDPS Plug and Play devices are not typically required to analyze and interpret the art IDPS output;

-Hardware and software requirements;

-Documents;

-Costs, in addition to software, hardware and installation costs, as well as education, training, operation and maintenance costs.

A.8 Intrusion detection problem

A.8.1 Intrusion detection and privacy

Privacy has become a problem of the use of IDPS. When looking for hidden malicious and suspicious content specific attack signatures or pattern recognition or intrusion detection network transmission requirements analysis and (or) operating system audit trail.

Network traffic or the situation of data collection may contain some personal data, that data relating to a specific person. Hardware or IP address may be an example of the above data. Therefore, intrusion detection could be monitoring their behavior and user tools. If the intrusion detection is used to detect the "internal" intruders, ie the organization employees should consider their impact.

If you use intrusion detection, we should consider three principles reflect the privacy challenges:

-Intrusion detection system must meet the protected object or data;

-Data collection (network packets, audit logs) must be fully satisfied the purpose of protection;

-Should develop and apply policy that covers the privacy of personal information collected IDPS claimed.

The first aspect as a means of intrusion detection tool does not require supervision and employee behavior.

The second aspect should be pointed out that only the collection and analysis of data necessary to identify the attack. The attack signatures events data and IDPS of comparison, the data are no longer needed should be deleted or show signs of attack data, show signs of attack by security-related data should be stored. However, in some cases deleted data may be inappropriate, the situation may need to archive data for subsequent inspection, as for traceability attacker or for future forensic analysis. Some data may at first appear to be benign. After further analysis, it may prove to be related to an attack. Later, data collection may also prove relevant to attack. In any case, it should strengthen the protection of data in order to avoid access a variety of purposes, including privacy. The action taken should be consistent with the organization's security policy.

Data should be stored in accordance with the policy for some time, and then safely destroyed to protect the privacy of all parties. This time to the forensics and law enforcement a lot of time to investigate, and in the future may be subject to unauthorized access to the system, do not leave sensitive data no longer needed.

The third aspect implies the need for a global privacy policy basis and (or) any law applicable to sensitive personal information protection and privacy of personal information management organization.

Currently, there are few specialized intrusion detection associated with legal and regulatory requirements. Expect the law or regulations provide adequate protection for the privacy of individuals, while allowing IDPS and related events log collection and use enough data to identify potentially devastating invasion. Some countries have regulations contain enough standard, and the use of personal data related purposes. Some countries have regulations on the protection of personal data of staff, and staff involved in their personal data privacy rights regulations. In addition, different national regulations and treaties on cross-border data flows may affect the intrusion detection and privacy.

If the legal and regulatory requirements to monitor staff activities, such as logs and events through specific IDPS sensor / Monitor Agent, then it should clearly inform employees and contractors, and confirmed before the operation starts. This can be achieved by signing the form of employment contract terms, specific files or electronic notice.

A.8.2 Invasion of shared data

Sharing data and invasion IDPS experience for all organizations are actively using the IDPS is beneficial. For example, a similar invasion by many other organizations were analyzed, so that a number of organizations for early warning of invasion is possible, or

the invasion of a new information will be useful for many other organizations. IDPS use of empirical information may help other organizations to improve their IDPS operation.

However, it is recognized that most organizations already affecting their IT systems thereby affecting the invasion of public knowledge of its business operations to be universal consensus. These small public knowledge to be misleading, the impact of large business, such as profitability, stock prices. Based on this, the organization, the most appropriate approach is to participate in cooperation programs, thereby purifying the use of information sources and IDPS invasion, making it anonymous. These programs collect anonymous knowledge is the foundation for community service IDPS database information in the above. This database should be used for intrusion detection:

-Coordination vulnerability configuration, invasion and use details of these types of configuration instructions;

-Processing large amounts of information on a sample of the invasion, in order to make the right statement on the invasion of the prerequisites in terms of the type of impact, traces the difficulties, remedial measures;

-If both types of distinct traces were observed, then the storage of data on invasive type of technology, and share major difference between the two;

-Ensure trace information is downloaded to support the invasion of new structured format described;

-When they find new vulnerabilities, update rules and (or) change the parameters;

-Can be extracted automatically generate new rules may identify a new invasion (e.g., signature, parameters, etc.).

IDPS modern database may be likened to a virus detection system, the latter typically having a network-based automatic update function.

Intrusion intrusion event database is not the database, which stores information about the attack case evidence.

In GB / T 32920-2016 details the considerations to share event information. Data model, format and secure exchange protocol has been developed and standardized in the IETF to facilitate automatic exchange of data intrusion. International standards, including RFC5070 event automation Object Description Exchange Format (IODEF), RFC6545 real-time network defense (RID) and RFC6546 transmission of real-time network defense.

附 录 B
(Informative)
GB / T 28454-XXXX with GB / T 28454-2012 technical differences

1, modified for the intrusion detection system IDS IDPS intrusion detection and prevention system, an intrusion prevention system IPS into the standard range;

2, to modify the standard range;

3, modified normative references cited references prepared (see 2) according to the standard content;

4, part of the term no longer follow the GB / T 28454-2012 term preparation ideas, not adopted in the definition 25069-2010 GB / T, but directly using the definition of the international standard, modifying some of the terms, including "attack", "denial of service", "demilitarized zone", "intruder" "invasion", "router", "switch", "Trojan horse", according to international standards variations, modifications, some of the terms, including "attack signatures", " password hash "," firewall "," host "," intrusion detection system "," intrusion prevention system "," online upgrade "," probe "," test access point ", an increase of some terms, including" distributed denial of service attack "," intrusion detection and prevention systems, "" virus, "" virtual private network "," vulnerability "of terms and definitions (see 3);

5, an increase of some abbreviations, including AIDPS, DMZ, DDoS, DoS, IDPS, I / O, ICDEF, HIDPS, SIEM, VPN, delete abbreviations NIDS, SIM (see 4);

6, IDPS selection considerations, add, delete, and modify some of the issues (see 7.4);

7, SIEM modification function, associated with an increase of the situation, the situation was filtered, the polymerization events (see 7.5.6);

8, due to the increased intrusion prevention system, modify "When organizations have security requirements to register aspects of IDS products, see GB / T 20275" to "When the organization has requested level of security aspects of IDPS products, see GB / T 20275 and GB / T 28451 "(see 9.3.1).;

9, the modified classification IDPS, IDPS and explanations given three types (see A 4.1);

10, increased data sharing case relevant international standards (see A 8.2).

references

[1] ISO / IEC 15408 (all parts) security evaluation criteria IT Information Technology Security Technology
[2] GB / T 25068.4-2010 Information technology - Security techniques - IT network security: Part 4: remote access security
[3] ISO / IEC 18028-5information Technology Security techniques - IT network security: Part 5: useCross-network communication security virtual private network
[4] ISO / IEC 20000(All parts) information Technology Service Management
[5] ISO / IEC 27033-1: 2009 Information technology - Security Network Security Technology: Part 1: Overview of concepts and
[6] ISO / IEC 27033-2: 2012 Information technology - Security Network Security Technology: Part 2: Security Network Design and Implementation Guide
[7] ISO / IEC 27035: 2011 Information technology - Security techniques - Information security incident management
[8] ISO / IEC 27001 Information technology - Security techniques Information Security Management System Requirements
[9] ISO / IEC 27002 Information technology - Security techniques - Information security Control Practices Guide