GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 36635-2018

Information security technology - Basic requirements and implementation guide of network security monitoring

信息安全技术 网络安全监测基本要求与实施指南

Issued on: September 17, 2018 **Implemented on: April 01, 2019**

Issued by: State Market Regulatory Administration;
Standardization Administration of PRC.

Table of Contents

Information security technology - Basic requirements and implementation guide of network security monitoring

1 Scope

This standard specifies the basic requirements for network security monitoring, provides a framework for network security monitoring framework and implementation guide.

This standard applies to the implementation of system or network security monitoring, the design-development of network security monitoring products, the provision of network security monitoring services.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/Z 20986-2007 Information security technology - Guidelines for the category and classification of information security incidents

GB/T 25069-2010 Information security technology - Glossary

GB/T 28458-2012 Information security technology - Vulnerability identification and description specification

GB/T 31509-2015 Information security technology - Guide of implementation for information security risk assessment

3 Terms and definitions

The terms and definitions as defined in GB/T 28458-2012 and GB/T 25069-2010 as well as the following terms and definitions apply to this document.

3.1

Network security monitoring

A set of rules, guidelines, practices for managing the security, protecting, distributing assets (including sensitive information) within an organization and its system's intrinsic security, especially those that have an impact on system security and related elements.

[GB/T 25069-2010, definition 2.3.2]

4 Abbreviations

The following abbreviations apply to this document.

FTP: File Transfer Protocol

JDBC: Java Database Connectivity

ODBC: Open Database Connectivity

PCAP: Process Characterization Analysis Package

SFTP: Secure File Transfer Protocol

SNMP: Simple Network Management Protocol

SYSLOG: System Log

TELNET: Teletype Network

WMI: Windows Management Instrumentation

XML: Extensible Markup Language

5 Framework of network security monitoring

5.1 Overview

The framework of network security monitoring is as shown in Figure 1. Through the basic environment of the network or system, use a certain interface mode to collect the relevant data such as logs, to carry out correlated analysis and identification of the security incidents and threat risks, perform visualized display and alarming, store the data generated, to grasp the overall network security posture.

analysis. The collected data mainly includes stream data and packet data, log data and performance data, threat data, strategy data and configuration data, etc.;

c) Storage: Store, by types, the data in the process of network security monitoring. The data types include structured, unstructured or semi-structured;

d) Analysis: Process the collected or stored data according to certain rules or models, discover security incidents, identify security risks. The analysis content mainly includes analysis of information security incidents, operational state analysis, threat analysis, strategy and configuration analysis, etc.

e) Display and alarm: Visualize the results of the analysis in real time and issue alarms according to important levels.

5.3 Classification of monitoring

According to different monitoring objectives, network security monitoring is divided into the following four categories:

a) Monitoring of information security incident: For the incidents that may damage or is damaging the normal operation of the monitoring object or causing the loss of information security, according to the classification and grading requirements of information security incidents, carry out analysis and identification;

b) Monitoring of operation status: Carry out real-time monitoring of the monitoring object's operating status, including network traffic, availability status information of various equipment and system, etc., to judge the information security state of the monitoring object from the operational status;

c) Threat monitoring: Carry out assessment and analysis of the security threats of the monitored objects; discover the information security risks faced by the assets;

d) Monitoring of strategy and configuration: Check and analyze according to the established security policy of the monitoring object and the configuration information of the relevant equipment or system; evaluate its security.

f) Collection of configuration data shall support the acquisition from the operation configuration parameters of the monitoring object. The configuration file as exported from the device or system shall be such as able to be parsed into data of standard format.

6.3 Storage

The storage of network security monitoring data shall:

a) Carry out storage, in a classified and distributed manner, for different types of heterogeneous data (such as standard format logs, metadata, PCAP files, etc.);

b) Pre-process the stored data, including formatting processing, supplementing context information, abnormal data clearing, etc.;

c) Set the retention period of monitoring data;

d) Adopt an encryption mechanism to ensure the confidentiality of important monitoring data;

e) Adopt a verification mechanism to ensure the integrity of important monitoring data;

f) Have backup and recovery capabilities;

g) Set access rights, authorize the use of monitoring data, audit the storage access behavior. The audit log is kept for not less than 6 months;

h) Support distributed storage and original format data storage;

i) The source data is stored for at least 6 months. It shall set the storage period for the analysis data, display and alarm data according to the business needs;

j) Keep up with the unified standard time source.

6.4 Analysis

The analysis of network security monitoring shall include analysis of information security event, analysis of operation status, threat analysis, analysis of strategy and configuration. Each type of analysis shall satisfy:

a) Analysis of information security incident shall support:

1) Identify and verify the behaviors which damage to the monitored object

e) The alarm is graded according to the requirements of 5.2 of GB/Z 20986-2007.

6.6 Protection of self-security

The protection of self-security of network security monitoring shall comply with the following requirements:

a) Encrypted storage of important data;

b) It has the password strength policy, automatic verification of password strength, user login timeout exit mechanism;

c) Monitor its own operation status and support alarms on status abnormality;

d) Monitor sensitive data operation logs and perform log audits on a regular basis;

e) Back up important system information and data to support rapid system recovery;

f) Support automatic synchronization of standard time. It is synchronized at least once a day.

7 Guide for implementation of network security monitoring

7.1 Interface connection

According to the monitoring target and the monitoring object, select the applicable monitoring interface and evaluate the availability of the interface. According to the determined interface type, configure the interface parameters. Use the interface to connect the monitoring object and the collection environment. The specific implementation of the interface connection includes:

a) Use such methods as Netflow protocol and interface, network sniffing mode, to collect stream data and packet data;

b) Use such methods as an SNMP protocol interface, a SYSLOG protocol interface, or a proxy component, to collect log data and performance data;

c) Use the file interface to collect the threat data;

d) Use an SNMP protocol interface, a database access interface, or an offline

b) Provide data storage and access interfaces in the form of documents to satisfy the storage of unstructured data, such as files, pictures, videos, to support fast retrieval;

c) Use distributed data processing technology to convert semi-structured data into structured data, to provide data storage and access interfaces for upper-layer applications, establish fast indexes to improve query performance;

d) Design a system information database to store supporting data for the operation of the network security monitoring environment itself, such as application data including user information, authority control information, system logs, system configuration;

e) Design a meta-database to store data describing source data, data of analysis result, data of presentation and alarm;

f) Design the original database, to store all the collected raw monitoring data;

g) Design a subject database, to store various analysis, display and alarm data which are classified according to the purpose of monitoring. The subject database may be divided into sub-database as needed;

h) Design an asset information base, to store information about all collected objects and software-hardware of network security monitoring environment, such as asset name, type, IP, operating system, usage, business system belonged, engineering, department, security domain, asset supplier, confidentiality value, integrity value, availability value, asset registration time, and other basic attributes. For different types of information assets, it may record the specific security attributes;

i) Design an operation-maintenance service database, to store related data entities such as work order management, duty management, knowledge base;

j) Design statistical report library, to store comprehensive reports such as asset-type report, vulnerability-type report, risk-type report, alarm-type report, daily report, weekly report, monthly report, annual report.

7.4 Analysis

According to the business analysis requirements of the monitoring objects, define the purpose of the analysis, select appropriate data analysis tools and methods, carry out data processing, send the analysis results the display and alarm. The specific implementation of the analysis includes:

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------