TEST
Engineering & Management

Research on Linkage Host Security Protection System Based on Information Security Level Theory

Linjiang Xie[1,*], Feilu Hang[1], Wei Guo[1], Yao Lv[1] and Wei Ou[1]
[1]Information Center, Yunnan Power Grid Co., Ltd, Kunming, Yunnan, China, 650217

Article Info
Volume 83
Page Number: 5513 - 5522
Publication Issue:
July - August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *28 August 2020*

Abstract

With the rapid development of science and technology in China, nowadays people's life and production are inseparable from computers. However, hacker intrusion, virus infection, network crime and important information leakage will seriously affect the information security and host security of our country. Information security level protection (hereinafter referred to as ISLP) is the basic system and strategy of national information security, which requires us to maintain the fundamental guarantee of national information security. ISLP is the embodiment of the will of the state in information security work, which is mainly based on the theory of information security level. At the same time, the evaluation of information system security level protection is a very important work link to carry out the ISLP work, which will better detect and develop the security level compliance evaluation standards. Through the protection requirements of safety level theory, we can provide comprehensive, fair and effective technical support. Therefore, this paper studies the linkage host security protection system based on the information security level theory. Then, this paper develops the detection process. Finally, some suggestions are put forward.

Keywords: *Information Security Level Theory, Linkage, Host Security Protection System;*

1. Introduction

With the rapid development of computer network technology, information and computer network system has become an important guarantee of social development, which has involved the country's political, military, economic and other fields. Computer networks will store, transmit and process a variety of information, including government macro-control policies, business and economic information, high-tech scientific research data and other important information. Therefore, host security is an important factor related to national security and sovereignty, economic development and social stability[1].

Host is the core of information application, which is the operation center and data processing center of application services[2]. At the same time, the host is the direct carrier of sensitive information in the information system, which is the basic platform for the operation of various application systems[3]. Therefore, there are many kinds of attack events and means, including buffer overflow attack, system administrator password attack, malicious code attack, hacker external attack, internal personnel attack and so on[4]. Therefore, we must ensure the security of the host computer, which is the basis of ensuring the security of the entire information system. At the same time, host security is also an important part of the security construction in the hierarchical protection system, which is an urgent task in the current information security guarantee[5].

With the development of information and communication technology, the structure of network information system is becoming more and more complex[6]. The information security problem brought by new technology is becoming more and more serious[7]. Information security classified protection 2.0 standard (hereinafter referred to ISCP

2.0) is the "one center, three protection" network security technology design of the overall idea, which can put forward a comprehensive and detailed criteria for new technologies and key areas. Therefore, ISCP 2.0 standard is a new programmatic and guiding standard for network security construction in China[8].

In ISCP 2.0, security computing environment is an important part of protection, and host security is the core of protection[9]. The main content of host protection is to achieve trusted authentication, identity authentication, access control, human intrusion prevention, data integrity, confidentiality, personal information protection and other security protection measures through technical means, which will realize the comprehensive security protection of host system[10]. In the face of unpredictable network security attacks, we must change passive defense into active immunity[11]. Therefore, on the premise of not destroying software code and business logic, dynamic response to threats is the key to host protection in the era of ISCP 2.0. Through the comprehensive design of ISCP 2.0 standard system, we can realize the host security protection scheme with security immunity and active defense ability, which will comprehensively improve the security performance of host in complex attack environment.

2. Security protection requirements based on information security level theory

2.1. Bibliometric analysis of classified protection of information security

In this paper, the number distribution of classified information security protection documents is obtained by clustering according to the time of papers published, which reflects the research results and popularity of classified protection of information security in China, as shown in Figure 1.

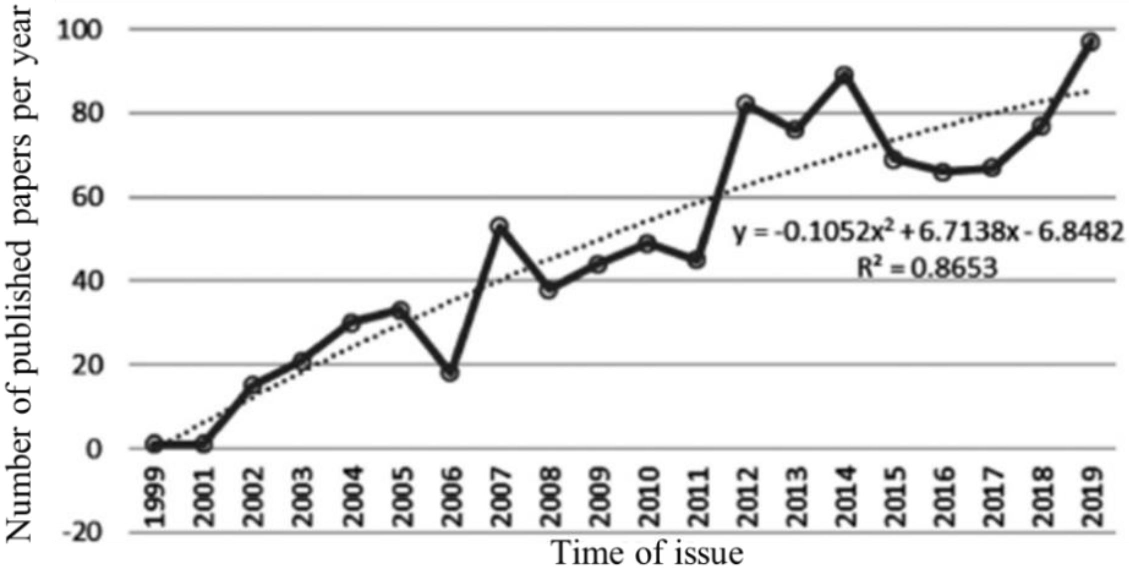

Figure 1. Bibliometric analysis of classified protection of information security.

Through Eviews software, the data is fitted by quadratic function of one variable, and the trend line is shown in Formula 1. With the increasing popularity of research on classified protection of information security, research results are also increasing, which is consistent with the rapid development of information technology and Internet industry.

$$y = -0.1052x^2 + 6.7138x - 6.8482,\ R^2 = 0.8653 \quad (1)$$

2.2. Goals and requirements of host security

For different protection levels of information systems, we should have the basic requirements of host security[12]. Among them, the higher the level, the more security requirements. For the host server in the information system, GB / T 22239-2008 "information security technology basic requirements for classified protection of information system security" can provide basic protection requirements from nine aspects, as shown in Figure 2.

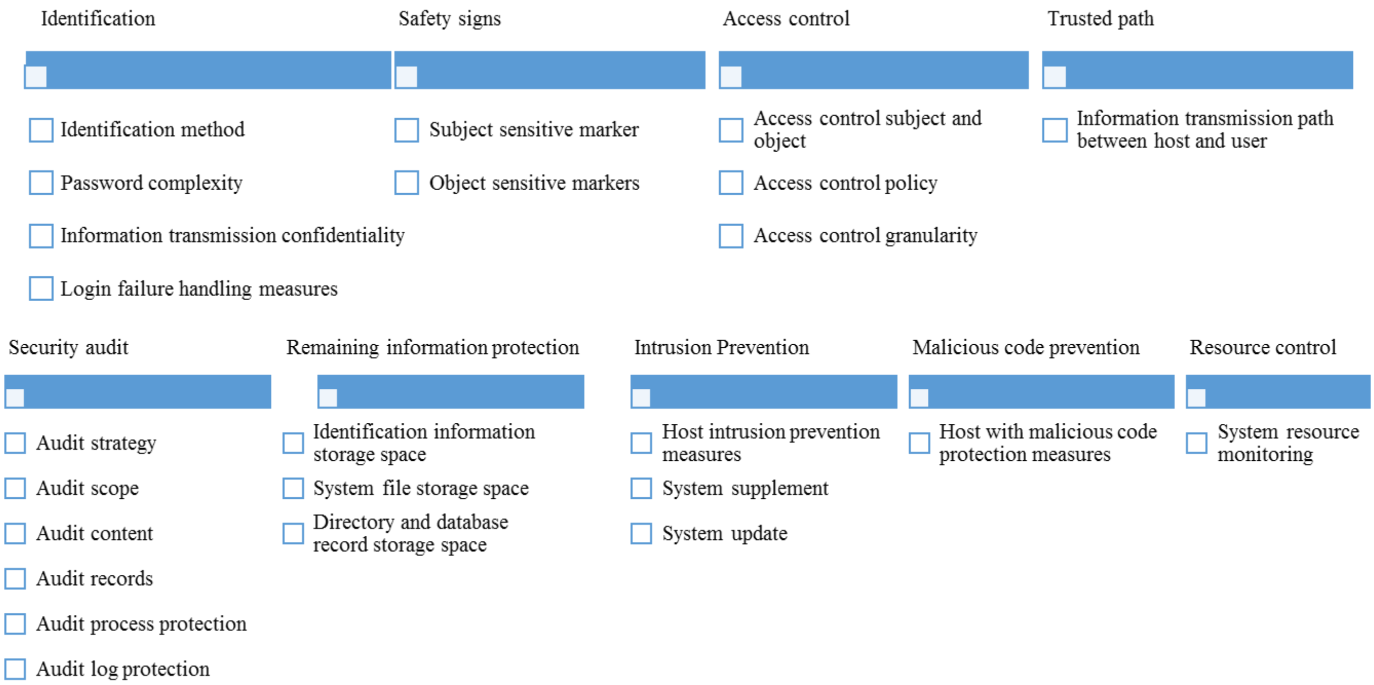
Identification
Safety signs
Access control
Trusted path
□ Identification method
□ Password complexity
□ Information transmission confidentiality
□ Login failure handling measures
□ Subject sensitive marker
□ Object sensitive markers
□ Access control subject and object
□ Access control policy
□ Access control granularity
□ Information transmission path between host and user
Security audit
Remaining information protection
Intrusion Prevention
Malicious code prevention
Resource control
□ Audit strategy
□ Audit scope
□ Audit content
□ Audit records
□ Audit process protection
□ Audit log protection
□ Identification information storage space
□ System file storage space
□ Directory and database record storage space
□ Host intrusion prevention measures
□ System supplement
□ System update
□ Host with malicious code protection measures
□ System resource monitoring

Figure 2. Goals and requirements of host security.

2.3. Host security evaluation method

The technical level of information system level evaluation is mainly divided into five aspects: physical security, host security, network security, application security and data security[13]. Host security evaluation is mainly for the server, terminal / workstation and other computer equipment operating system and database system level security, in which terminal / workstation is desktop and laptop with peripheral devices, and server refers to application, network, web, file and communication servers.

The national standard GB / T 22239-2008 divides the content of host security evaluation into seven control points, including identity authentication, access control, security audit, residual information protection, intrusion prevention, malicious code prevention and resource control[14]. With the decrease of the level of information system, the requirements of host security protection ability are gradually reduced[15]. With the improvement of the corresponding system level, the requirements of protection capability increase step by step[16]. This paper combs out the evaluation implementation process of each level of host security, including the evaluation content, evaluation implementation and evaluation result judgment conditions, which is not applicable to the actual operation of system testing[17]. Therefore, we must sort out the evaluation methods and steps of the tested object according to the basic requirements and evaluation requirements, as shown in Table 1.

Table 1. Host security evaluation method of level 3 information system.

NO.	Control point	Interview	Inspect	Test
1	Identification	√	√	√

2	Access control	√	√	×
3	Security audit	√	√	√
4	Remaining information protection	×	√	×
5	Prevention of human invasion	√	√	×
6	Malicious code prevention	√	√	×
7	Resource control	×	√	√

3. Implementation scheme of host security protection based on information security level theory

3.1. Implementation scheme design of multiple independent protection

From the perspective of working methods, the design of host security protection implementer based on information security level theory mainly considers three methods, namely node protection, channel protection and terminal protection, as shown in Table 2.

Table 2. Principle of three protection methods.

Method	Node protection	Channel protection	Terminal protection
Work area	Communication node	Communication channel	Intelligent terminal
Working principle	Intelligent interception	Communication efficiency maintenance	Real time check

Node protection will achieve security protection within the scope, which will match and analyze suspicious packets and programs. By isolating suspicious data directly from the security system, we can ensure the information security within the protection scope of several working equipment. Channel protection can only protect the communication channel, which requires us to ensure that the channel is unobstructed. In the multi information parallel transmission, we must ensure that different information will not interfere with each other[18]. Terminal protection only applies to computers or other portable devices. Through the real-time inspection of firewall and protection software, we can avoid danger and enter the computer to cause information loss[19]. Taking terminal protection as an example, we can carry out technical analysis[20]. In the intelligent terminal, we need to collect the characteristics of Trojan virus and input it into the computer to save. By maintaining real-time connection with protection software and firewall, we default that trojan virus has A feature. When the virus tries to enter the host, its characteristics can show the characteristics highly related to a, as shown in formula 2.

$$A=[A-n;...;A-2;A-1;A;A_1;A_2;...;A_n] \tag{2}$$

Among them, $[A-n,A_n]$ represents the lower limit and upper limit of Trojan virus changes that can be recognized by the computer.

As long as we collect enough samples, we can ensure that the range of computer $[A-n,A_n]$ is wide enough, which will realize intelligent interception of various Trojan viruses. In this way, we can ensure the security of information in the computer.

3.2. Design of layered operation implementation scheme

From the perspective of working mechanism, we can carry out layered operation under the support of node protection, channel protection and terminal protection, which will be better for real-time and instantaneous protection. Under the layered operation mechanism, we can break through the channel, node and terminal respectively, which can destroy or steal computer information. In hierarchical mode, multi-level verification emphasizes the extension of longitudinal security protection. However, the protection effect of the same channel can be improved by multiple channel protection.

Parallel real-time and instantaneous protection means that all programs and files are attempted to be scanned interactively and initially in a single level protection method. After the safety is determined, the system can be released, which is instantaneous protection. At this time, the programs and files that have been put into the computer still need to be processed in real time. Among them, the real-time protection mechanism can be controlled by personnel, which can scan all kinds of information and programs in the computer. Through the assessment, we can confirm whether there is a risk. Through the computer terminal, we can start the firewall, which can be the initial security protection. By isolating dangerous documents and procedures, managers can perform a second scan, which will further improve the protection effect. Layered operation can extend horizontally on the basis of node protection, channel protection and terminal protection, which can not only expand the protection scope, but also carry out vertical extension at a single level, which will enhance the sense and effect of protection level.

3.3. Implementation scheme design of comprehensive scoring

Based on the information security level theory, the feasibility of the scheme needs to be evaluated. Through weight evaluation, problem analysis and processing mode, we can choose the basic method of long-term optimization. By considering the working sensitivity, time and other elements of the scheme, we can score different elements, which will get the ability of components. Among them, the weight ranking is shown in Table 3.

Table 3. First level weight ranking.

Essential factor	Job sensitivity	Scalability	Applicability	Single working time	Other
Ranking	1	2	3	4	5
Weight coefficient	0.50	0.20	0.15	0.10	0.05

According to the score results of the network security classified protection implementation scheme, we can complete the quantitative evaluation. According to the score of different projects, we can analyze the advantages and disadvantages of the scheme. By optimizing the comments, we can keep the items with higher scores. Through continuous evaluation and improvement, we can improve the ability of information security protection.

3.4. Host security protection evaluation process

Host security protection evaluation process is the most important way, which is mainly through inspection and testing two ways of interaction. Inspection and testing is to verify the effectiveness of the security configuration mechanism and operation of the information system manually. Through Tonghe inspection and testing, we can obtain evidence more comprehensively. However, for the large-scale information system with more hosts, we must adopt the method of sampling inspection. By selecting the typical evaluation object host detection, we do not need to check all hosts one by one. The security evaluation items of level 3 host include 7 units and 32 evaluation requirements. In this paper, the on-site inspection content and test flow chart are developed, as shown in Figure 3.

3.5. System workflow design

The design of system workflow needs to refer to the overall process of ISLP evaluation, which will make the overall operation of the system consistent with the evaluation process. For a system under test, the system information that needs to be evaluated is input into the evaluation system. According to the grading standards, we can fill in the applicable levels of the system. When filling in, all hosts in the system that need to be evaluated should be entered, including host IP, host name and host operating system. By judging whether the host level is consistent with the system level, we can clearly indicate the security protection of the host. After the completion of the information entry, the evaluator selects an untested host through the evaluation system, and generates the program according to the evaluation guide book. According to the host's operating system type and security level, the host will automatically select the matching evaluation items from the database evaluation item table. According to this form, the system will generate the work instruction which meets the evaluation standard. The operation instruction is divided into two parts: automatic evaluation and manual evaluation. The automatic evaluation performs relevant operations by calling the evaluation and inspection tools matching with the host, and stores the collected evaluation results into a record file. The evaluation personnel will record the last evaluation system, and the evaluation system will automatically input the content of the record file into the evaluation system. In the manual evaluation part, the evaluation results can be obtained through manual interviews, surveys, etc. According to the criteria, we can judge the evaluation results, which will eventually generate an evaluation report. The actual workflow of the evaluation system is shown in Figure 4.

4. Linkage host security protection system based on ISLP deployment

4.1. Unified host security management

At present, most of the servers still use the single machine management mode, which will have a certain security lag. Therefore, if we want to achieve real and effective security management, we must implement unified centralized management, unified security policy distribution, unified monitoring and collaborative processing for all servers, which will build a healthy server security management system.

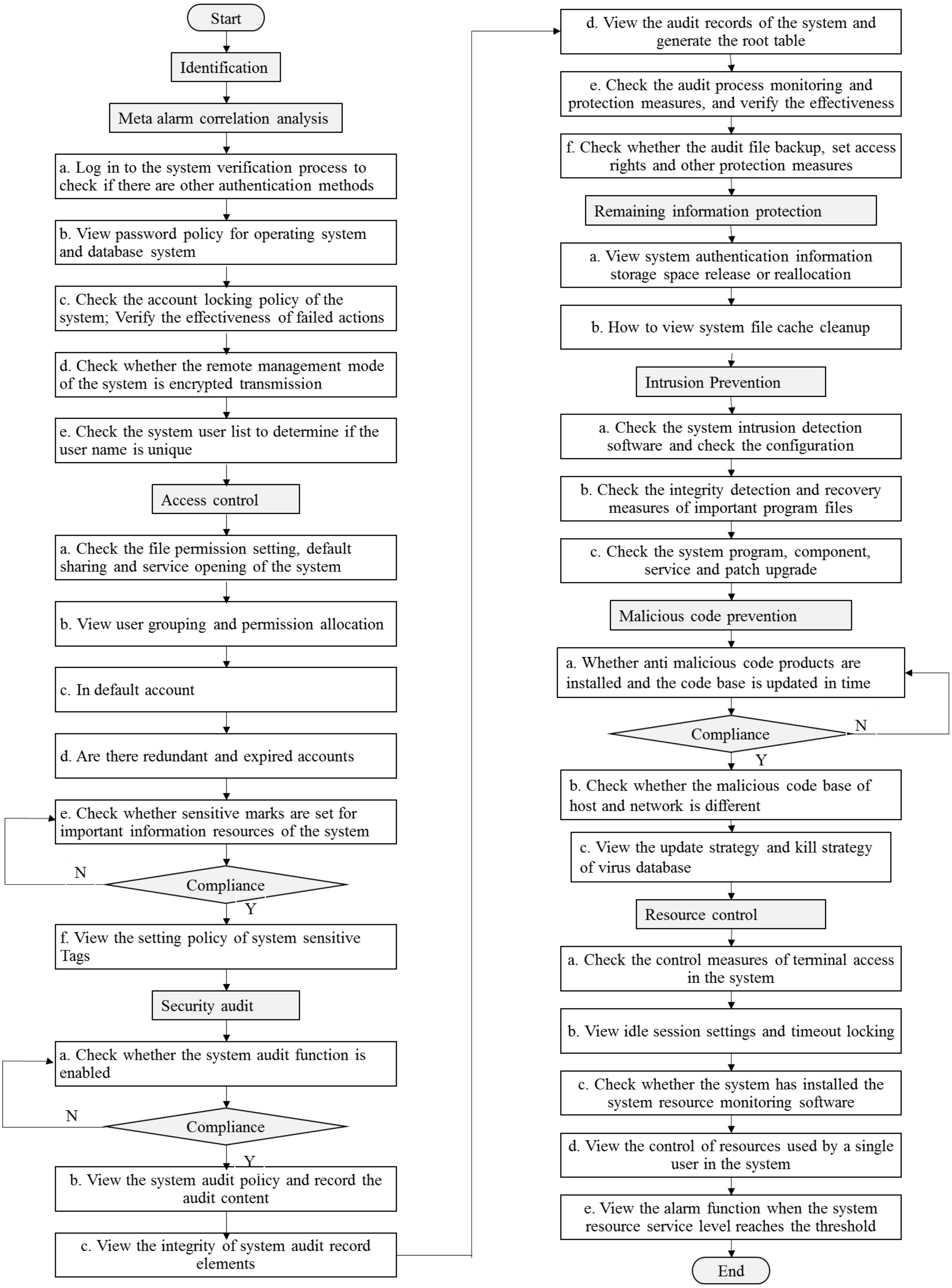
Start
Identification
Meta alarm correlation analysis
a. Log in to the system verification process to check if there are other authentication methods
b. View password policy for operating system and database system
c. Check the account locking policy of the system; Verify the effectiveness of failed actions
d. Check whether the remote management mode of the system is encrypted transmission
e. Check the system user list to determine if the user name is unique
Access control
a. Check the file permission setting, default sharing and service opening of the system
b. View user grouping and permission allocation
c. In default account
d. Are there redundant and expired accounts
e. Check whether sensitive marks are set for important information resources of the system
N
Compliance
Y
f. View the setting policy of system sensitive Tags
Security audit
a. Check whether the system audit function is enabled
N
Compliance
Y
b. View the system audit policy and record the audit content
c. View the integrity of system audit record elements
d. View the audit records of the system and generate the root table
e. Check the audit process monitoring and protection measures, and verify the effectiveness
f. Check whether the audit file backup, set access rights and other protection measures
Remaining information protection
a. View system authentication information storage space release or reallocation
b. How to view system file cache cleanup
Intrusion Prevention
a. Check the system intrusion detection software and check the configuration
b. Check the integrity detection and recovery measures of important program files
c. Check the system program, component, service and patch upgrade
Malicious code prevention
a. Whether anti malicious code products are installed and the code base is updated in time
Compliance
N
Y
b. Check whether the malicious code base of host and network is different
c. View the update strategy and kill strategy of virus database
Resource control
a. Check the control measures of terminal access in the system
b. View idle session settings and timeout locking
c. Check whether the system has installed the system resource monitoring software
d. View the control of resources used by a single user in the system
e. View the alarm function when the system resource service level reaches the threshold
End

Figure 3. Host security protection evaluation process.

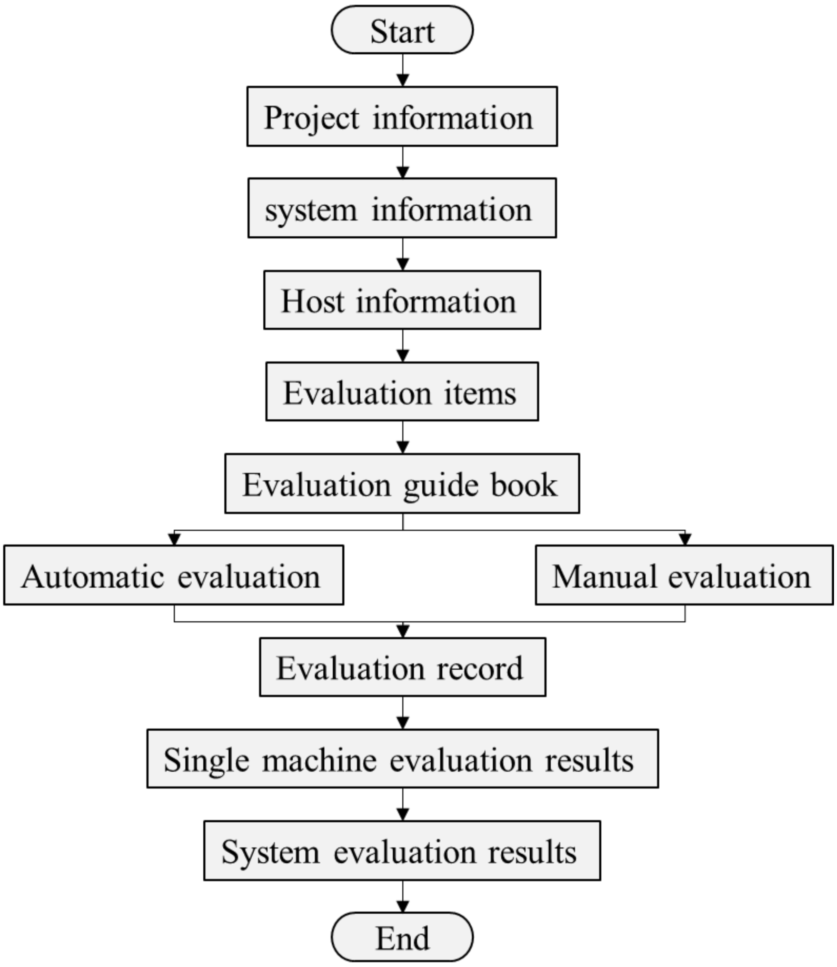

Figure 4. The actual workflow of the evaluation system.

4.2. Identification

Identity authentication is the "gate" of host security, which is the basic condition to obtain host system resources. The existing host operating system still uses single password authentication to identify the user's identity, which is vulnerable to dictionary attacks and other attacks. Therefore, we need to manage the identity of host users. According to the user's identity and role assignment permissions, we can carry out different authentication. At the same time, we need to adopt strong authentication mode for host users, such as double factor authentication. Through the legal USB-Key, at the same time, we need to enter the correct server operating system password + USB-Key password, in order to successfully log in to the server. Through the double factor authentication, we can bind the user identity with USB-Key, which will effectively prevent the occurrence of user identity forgery. When remote maintenance is carried out on the host, we need to use plaintext mode for operation as small as possible, such as Telnet, mstsc and so on.

4.3. Safety signs

Through the security identification of the subject and object in the server system, we can formulate different access control rules, which will strictly control the user behavior. In this way, we can ensure that the user's behavior is monitored by the security policy, which will ensure the security and confidentiality of the server data in an all-round way. At the same time, through the full path name, we can mark the important objects in the server system. By setting user or process on file / directory, we can enforce access control rules. In the server sensitive file or directory operation behavior, we must carry out strict access control, which will prevent the user data from being tampered, deleted, inserted and so on.

4.4. Access control

By identifying the identity of the access server, we can effectively prevent unauthorized users from accessing the server. Through the trusted interconnection mechanism, we can realize the effective control of access. The host administrator shall specify the access to the server system. Only after passing the authentication test can the user communicate with the server. At the same time, the host should provide remote access and implement connection restriction. Through the establishment of trusted access list, we can allow access to services for trusted addresses. At the same time, we need to limit illegal address connections.

4.5. Security audit

For the controlled server, we should formulate detailed audit strategies according to the audit requirements, including user login, resource access, process startup, etc. For the collected audit information, we should carry out detailed classified audit query, including user ID query, operation type query, operation result query, etc. At the same time, only the security auditor can modify or delete the audit log, which requires us to backup the audit log in time.

4.6. System reinforcement and intrusion prevention

We need to establish a unified patch management and anti-virus system for the whole network, which will timely distribute the vulnerability patches and upgrade the virus library to the host. At the same time, the host system should also install and deploy malicious code protection system. By upgrading the malicious code base in time, we can regularly scan and remove viruses, Trojans, backdoors, webpages and other malicious programs.

4.7. Clear the log

The attacker will usually clear the log before exiting the target system, which will leave traces of deletion. Once the log is cleared, it is difficult for the administrator to find the attacker's intrusion behavior. Therefore, we should take measures to protect audit records, such as building log server. By transferring the logs to the log server in real time, we can use third-party operating system hardening software, which will implement strong access control on log files. In this way, the attacker can obtain the administrator's permission in time and have no right to delete the log record.

5. Conclusion

It is necessary and feasible to design the implementation scheme of network security level protection based on information security. In this paper, three feasible measures are put forward, which are multi independent protection scheme design, layered operation implementation scheme design and comprehensive score implementation scheme design. Through different protection technologies and different protection mechanisms, this paper provides effective help for host security protection.

References

[1] Ao Jianxun. A real-time malware detection model. Information security and communication security, 2011,09 (10): 76-78.

[2] Zhang Yu. Computer virus prevention based on registry configuration [J]. Journal of Zhengzhou Institute of light industry, 2011,26 (4): 82-84.

[3] Chen Rui, Chen zemao, Wang Hao. Research on industrial control network threat modeling based on attack graph [J]. Information network security, 2018, 18 (10): 70-77.

[4] Chi Shuiming, Zhou Suhang. Research on DDoS attack defense technology [J]. Information network security, 2012, (05): 27 – 31.

[5] Fan Guangyuan, Xin Yang. Analysis and design of firewall Audit Scheme [J].

Information network security, 2012, (03): 81 – 84.

[6] Fang Xin, Wan Yang, Wen Xia, et al. Research on DDoS attack method in network intrusion detection system based on protocol analysis technology [J]. Information network security, 2012, (04): 36 – 38.

[7] Gao Kunlun. Constructing system network security immune system based on trusted computing technology [J]. Engineering Science and technology, 2017, 49 (2) 28-35.

[8] Guo min, Zeng Yingming, Yao Jinli, et al. Software behavior security analysis based on big data samples [J]. Information network security, 2017, 17 (9): 153-156.

[9] Huang Huajun, Wang Yaojun, Jiang Liqing. Research on network color fishing defense technology [J]. Information network security, 2012, (04): 30 – 35.

[10] Huang Jianhui, Shen Changxiang. Design of TPCM active defense trusted server platform [J]. Journal of Zhengzhou University, 2019, 51 (3): 1-6.

[11] Liang Hong, Liu Jianan, Li Yong. Analysis and prevention of "flame" virus [J]. Information network security, 2012, (08): 157-159.

[12] Lin Cong, Hei Xiali. Analysis of Trojan horse camouflage and kill free technology [J]. Computer and modernization, 2009, (1): 25-27.

[13] Lin Cong, heixiali. Analysis of Trojan horse implantation and hiding technology [J]. Information security and communication security, 2008, (7): 53-55.

[14] Ning bin, Cao Wenping. Research on intrusion detection system [J]. South China financial computer, 2010, (4): 97-99.

[15] Shen Changxiang. Building a clean cyberspace with active immune trusted computing network security line [J]. Information security research, 2018, 4 (4): 282-302.

[16] Shen Chengdong, song Bomin. Research on detection technology based on malicious code [J]. Network security technology and application, 2012, (4): 9-11.

[17] Tian Xiuxia. Teaching reform of information security specialty driven by innovation practice project [J]. Computer education, 2015 (23): 30-33.

[18] Wang Wei, Shen Xudong. Case based anomaly detection algorithm for migration time series [J]. Information network security, 2019, 19 (3): 11-18.

[19] Wang Xiaolong, Liu Guanghui. Analysis of hacker attack technology and Defense Technology in computer network [J]. Digital technology and application, 2011, (10): 214-214.

[20] Xu Fu. Computer terminal immune model based on trusted root [J]. Acta electronica Sinica, 2016,44 (3): 653-657.