Construction and Research of Comprehensive Management Platform for Network Security of China University Information System

Jian-li SUN¹, a

¹Cybersecurity Information Office, Beijing Jiaotong University, Beijing, China

a sjl@pku.org.cn

Keywords: Intelligent campus, Security management, System filing, Level management, Vulnerability scanning, Security notification, Log data.

Abstract. As China moves rapidly toward the country with strong information technology. Colleges and universities, as an important part of the country, are accelerating the realization of a more convenient and fast information-based intelligent campus. The degree of informatization has also become an important stander for measuring the world "Double-First Class" universities. Faced with the increasing information system of colleges and universities, how to achieve unified security management has become an important issue that colleges and universities need to solve urgently. This article based on the information environment of Beijing Jiaotong University and the current operation and maintenance status of information systems. Through the methods and strategies used in daily work, this article combines the information system filing, hierarchical management, system vulnerabilities, web application vulnerabilities, security notice into one single platform. The information system with security risks is notified to the responsible person by SMS or email. This platform has realized a complete process from information system construction, filing, affiliated units, functions, open ports, vulnerability scanning, system operation, system rectification and upgrading. It reducing the switching of security devices from multiple platforms and improving the accuracy of detecting vulnerability.

Overview

With the continuous advancement of education informatization, colleges and universities across the country have established hundreds of application systems such as educational administration, scientific research management, and student management, providing an indispensable support environment for teaching and scientific research. In the face of numerous information systems, how to ensure the safe operation of these information systems and avoid the impact on the teaching and scientific research of the school due to the attack of the information system, especially in some colleges and universities that have been tampered with by the website pages into bad political influence. Occurrence is the primary task of the information supervisors of all universities.

After the implementation of the "Network Security Law of the People's Republic of China" on June 1, 2017, strengthening information system security management is one of the primary tasks of major information departments of universities. Subsequently, the "Network Security Level Protection 2.0 Series of National Standards" was officially released and officially implemented on December 1, 2019. Isobao 2.0 has become the basic national policy, basic system and basic method in the field of cybersecurity in my country. At present, the common problem of information systems in colleges and universities in China is that the number of information systems is large; some systems are built by the user units; the daily operation and maintenance of the system are maintained by themselves or entrusted to others; most systems are developed due to the small application scope and low funding The quality is not high, and the safety aspect is basically not considered during development.

In order to efficiently manage campus information system security, we have developed a set of campus information system security management integrated service platform suitable for the special environment of colleges and universities, System logic diagram (as shown in Figure 1). The system mainly includes subordinate functions:
(1) Information asset management (information system filing): establish information asset ledger for all the opened information systems in the school, including the detailed configuration of the software and hardware of the system, physical location, security protection measures, affiliated departments, maintenance personnel, data backup Situation, etc.

(2) Information system security status record: Establish a security status record for each information system (similar to a security medical record), which mainly contains each vulnerability scan, discovered vulnerabilities and vulnerability processing information.

(3) Vulnerability scanning information processing: according to the set time period (usually set to monthly), the scan results are imported from the vulnerability scanning device automatically or through file import and the current scan is compared with the previous scan to analyze the new Comprehensive analysis of the high-risk vulnerabilities found will verify the vulnerability risk level. For systems with high-risk vulnerabilities (newly discovered vulnerabilities and past vulnerabilities that have not been dealt with in a timely manner), rectification notices are automatically generated and sent to the information system manager by email.

(4) Security notification management: including school-wide security notifications, notifications from all second-level units, network segment analysis and scanning reports, high-risk system warnings, and bug fix reminders.

(5) Information system security status analysis: The system obtains and analyzes the security data (WAF log, IPS log, access volume, etc.) of the security system deployed in the campus network, combined with the system's own vulnerabilities and software equipment, and uses the correlation analysis method for each Information, timely detection of high-risk systems.

(6) Backup management: according to the backup period and the last backup time filled by the person in charge of each filing system, notify the person in charge of each system to back up on time.

(7) Hierarchical protection management: According to the requirements of hierarchical protection, it provides the functions of auxiliary rating, gap analysis and auxiliary evaluation.

At present, the system has been tested in the actual work of the Information Center of Beijing Jiaotong University. After using the system, it not only greatly reduces the workload of safety management personnel, but also realizes the school's comprehensive scientific and efficient management of the information system.

Architecture of Comprehensive Network Security Management Platform

The university information system network security management service platform uses the B/S system structure (as shown in Figure 2). The working interface used by information security administrators, second-level unit administrators and third-level users is implemented through a browser. The main part of the transaction logic is implemented on the server side, and very few are implemented through the front end. ‘This design model greatly simplifies the client computer load,
reduces the workload and cost of system upgrade and maintenance, and reduces the user's total cost.[1]

![System architecture diagram](image)

**Functions of Comprehensive Network Security Management Platform**

Information asset management is mainly to register and backup the information assets existing in the campus network, and realize the management of assets according to the requirements of grade protection evaluation.

Vulnerability management implements the management of the vulnerability database and the management of system vulnerability information of each unit, and provides the discovery and recording of vulnerability information, query of system vulnerability information, discovery of unresolved vulnerabilities and resolved vulnerabilities in the system, and new vulnerability query and audit business.

The backup management mainly realizes the function of the user performing backup on schedule, reminds the user to perform data backup on schedule, and the function of the administrator to view the user backup information. The significance of backup management is to supervise and remind users to back up important systems, information, and data on schedule to avoid serious consequences such as data loss or irreparable system repair.

The campus access information includes the basic information of each server in the campus network and the information about the ports opened by the server. Provide query and modification functions, when necessary, open or close specific ports of the server in time to help administrators maintain campus network security.

The real-time security status of the system uses various graphical representation methods to visually display the security status of the campus network, and vividly and intuitively display the existing and potential security risks in the campus network.

Security bulletin management is a summary notice of the overall security situation of the campus network, including the school-wide safety notice, the notices of each second-level unit, network segment analysis scan report, high-risk system warning and vulnerability repair reminder. By selecting the type of announcement, the administrator can summarize the status of system vulnerabilities, system attacks, and campus network security status in a short period of time, and automatically generate analysis reports, which are finally delivered to the person in charge of each system in the form of a word document In the hands, it plays the role of supervision and reminder. The person in charge of each system can download the document and view it, and manage and maintain the system in charge according to the report content and rectification methods.
Information Asset Management

The main function of the information asset management module is to manage the existing assets of the school. The system can be used to realize the registration of information assets, the inquiry of record information, and the display of corresponding information such as guarantee evaluation.

Users can upload the record information by uploading the excel file. The record information table is an excel form, which can be directly exported from the school's oa system.

After importing the record information, you can view all the record information. Including ip, domain name, system name, etc., you can also export the record information in pdf format.

Click Details to View Detailed Filing Information

(1) Basic information: system name, system IP, system unit, system provider, server location, server type;
(2) Personnel information: office phone, mobile phone and email address of the person in charge of the system and technology;
(3) System software: operating system name, operating system version, database name and version, web service version type, date;
(4) Application software: software name, version, development environment, source, maintenance method;
(5) Backup information: whether there is a backup plan, the amount of backup data, and the contact information of the backup personnel (name, job number, telephone, mobile phone, email)
(6) Maintenance information: maintenance method, maintenance personnel contact information
(7) Protection measures: name and version of anti-virus software, whether anti-tamper software is installed, other security protection measures

Click Vulnerability

Learned about the loopholes of the record server, including the leaked scans of the system and Web applications, in order to understand their security status.

Vulnerability Information (Security Status of Information System) Management

The information security studios of all colleges and universities have deployed their own vulnerability scanning systems, and regularly scan the vulnerabilities of various systems in the campus network to learn about the vulnerabilities in the system and use them to evaluate the security status of the campus network. Therefore, the management of vulnerability information is a very difficult task.

The vulnerability information management module in the security management service platform provides management of system vulnerability information. Assist administrators to obtain and view the vulnerability information of each system, and provide system vulnerability statistics inquiry of each secondary institution, as well as the newly added vulnerability viewing and review business.

The platform can record the vulnerability information in the filed system on the campus network into the database by automatically obtaining vulnerability scanning information or manually importing vulnerability reports. For example, Beijing Jiaotong University discovered server system vulnerabilities through NSFOCUS security device scanning, and regularly imported the data from the completed scanning tasks into the security management service platform for query through the device interface provided by SAFE. In addition, the vulnerability scanning system provided by NSFOCUS can also be used to find vulnerabilities in web applications of the server. After the scanning task is completed, a vulnerability information report can be generated. Vulnerability information can be imported by importing the vulnerability information report in Excel or Xml format.

After integrating various vulnerability information into the security management service platform, the administrator can view the vulnerability information of each system under each secondary unit in the school by selecting the secondary unit; the unit administrator can view the existing in the system belonging to the unit Vulnerability; users can also check the security status of the host responsible for it.
The security management service platform also provides query functions for resolved vulnerabilities and newly discovered vulnerabilities. The user can get detailed information about the name of the vulnerability, the risk level, the time of discovery, the number of vulnerabilities resolved, and the number of newly discovered vulnerabilities in the system through the detailed form.

Although the vulnerability scanning systems deployed by colleges and universities are different, the security management service platform provides a vulnerability library to record all the vulnerability information found by various vulnerability scanning systems.

Vulnerability database management is to manage these vulnerability information. It details the vulnerability name and version number, the vulnerability description and the hazard and vulnerability solutions. For new vulnerabilities in the vulnerability database, the system provides a new vulnerability query function, the administrator can always understand the occurrence of new vulnerabilities and complete the review process of new vulnerabilities through manual verification or automatic review.

Backup Management

This platform can notify the person in charge of each system to make timely backups through the backup period and the time of the last backup filled by the person in charge of the record system, and manage all the record information in a unified manner. The result is clear and more conducive to management.

Open the Management of the Access Server Outside the School

The platform also shows the server management of the school's opening of the off-campus access port, which supports importing port information through files and storing it in the submodule database. When the administrator needs to query the information of the system information, he can directly search and transfer it.

Real-time Information System Network Security Status Management

The platform obtains and analyzes the log data of the security equipment deployed on the campus network to obtain the campus network intrusion log information, the visits of various websites in the campus network, and the website's attacks. And use the HighCharts plug-in to display this information in the form of charts in real time and dynamically.

The bar graph is used to display the visits of mainstream sites on the campus network, which can directly reflect the habits and preferences of school teachers and students to browse the campus website. Combined with the analysis of the attacks on mainstream sites, you can find the security threats in the websites frequently visited by teachers and students. By taking corresponding measures, we should focus on preventing platforms with high security threat coefficients.

By displaying the statistics of the attacked sites on the campus network through a bar graph, you can directly find the most vulnerable sites on the campus network to identify the site objects that need to be protected and prevented.

By analyzing Waf log information, the reason and type of intrusion interception are counted (as shown in Figure 3 and 4). You can discover the most vulnerable types of intrusions on campus networks and which hosts are most likely to be targeted by attackers, thus providing an important basis for formulating network security protection strategies.
Cyber Security Bulletin Management

On the basis of the original complete network security protection system and daily security protection monitoring, adhere to the normalization (routinely once a month) of system vulnerability and web application vulnerability scanning, and conduct regular vulnerability scanning on the information system website of the whole school. This platform adds the logs of each security device, comprehensively evaluates the accuracy of each vulnerability, and improves the quality of reported vulnerabilities. At the same time, combined with the Beijing Jiaotong University SMS platform and e-mail platform, the vulnerable system is directly delivered to the person in charge, making the entire process more intelligent and convenient.

Information Security Bulletin of the Whole School and Secondary Units

The statistical mechanism of server vulnerabilities is based on the vulnerability information obtained from this platform. The total number of vulnerabilities and the number of high-risk vulnerabilities in the second-level unit are the accumulation of the total number of system vulnerabilities and web vulnerabilities marked in the platform and the accumulation of high-risk vulnerabilities under the jurisdiction of the second-level unit. As long as a high-risk vulnerability appears in each server or information system, the vulnerability risk level of the server is high.

The administrator can publish this notice to the second-level unit. At the same time, the second-level unit administrator can also download the security notice of their own unit through the platform download.

The school-wide announcement is mainly about the number of vulnerabilities, high-risk vulnerabilities, and the number of platforms and intrusion information that have not been backed up in each second-level unit in the school, including the number of mainstream website visits and the top ten of the supply statistics and attacks. Top ten statistics.
High-risk Host Security Notice

The platform also has the function of high-risk host security notification, which is mainly divided into web application high-risk host notification and system high-risk host notification. The attack information of web application vulnerabilities comes from website application-level intrusion prevention platforms (WAF and WEB application vulnerability scanning platforms), and the attack information of system vulnerabilities comes from intrusion detection platform data (NSF's remote security assessment platform). Combined with the vulnerability information in the platform in the record, a comprehensive analysis of the vulnerability attack was realized, and finally the alarm information of each record was obtained. Only the servers with a high vulnerability risk level among all the filing servers in the school are displayed.

After selecting the second-level unit option of the platform, it is the detailed information of the vulnerability situation of the second-level unit filing server. The system administrator of the second-level unit can view the detailed analysis process of each filing and the reason for rating.

The analysis process of high-risk host system vulnerabilities is the same as that of web application vulnerabilities, except that the types of attacks and vulnerabilities are different, but the analysis process is the same.

SMS and E-mail Notification

This platform is combined with the SMS platform and email platform independently developed by the Information Center of Beijing Jiaotong University. It can not only send SMS and email notifications at the same time, but also selectively send SMS or email to the person in charge of each filing platform. This function can efficiently and conveniently notify the person in charge of each high-risk vulnerability server, which improves the daily office efficiency.

Information Security Level Protection Management

Since the implementation of the network security level protection system in my country, ‘with the encouragement and leadership of government departments, all sectors of our society have successively put information security level protection on the agenda.'[3] In particular, all the "Network Security Level Protection 2.0 Series National Standards" officially implemented from December 1, 2019 have been officially released. The level protection evaluation process is also carried out in an orderly manner as an evaluation basis for verifying whether the information platform meets the corresponding security protection level.

The safety management service platform provides the rating and rating protection evaluation functions of the information system. The platform's level protection management module is composed of knowledge base management and platform evaluation.

The knowledge base management section records the basic requirements for evaluation at all levels, as well as some safety regulations and evaluation cases. The user can manage the platform he maintains purposefully after fully understanding the evaluation requirements, so that the platform he is responsible for basically meets the evaluation requirements. In addition, users can have a clear understanding of the grade protection evaluation through safety regulations and evaluation cases, and can make a rough assessment of the platform by themselves, and manage the platform according to the requirements of grade protection.

Information system grading part, on-site evaluation implementation and evaluation result analysis:

(1) Information platform grading can be based on the "Level Matrix Table" for information system grading, and can also analyze the information system business functions, and refer to the "Information Platform Security Level Recommendation Form" to determine the security level of the information platform.

(2) The implementation of on-site assessment includes information system asset management, formulation of work plan, determination of assessment plan, and finally collection of data corresponding to the information according to the determined security level, and calculation of
information system satisfaction based on the weight of assessment items and the degree of
conformity of assessment items The degree of the determined level.

(3) Analysis of evaluation results First of all, pie charts and column charts are used to
dynamically visualize the evaluation results, so that the person in charge of information can have an
intuitive understanding of the overall situation of the information information system. The platform
will also dynamically generate a gap analysis report and send it to the platform client for download
by the information system administrator.

Summary
This research plan is based on the information system security management in the special
environment of Chinese universities. Taking Beijing Jiaotong University as an example, it
combines OA, NSFOCUS, Anheng and other professional information system vulnerability
scanning software and information reports. This platform reduces the gap between the various
processes of issuing information system security notifications and improves the speed of processing
information security vulnerabilities each time.

With the continuous acceleration of my country's informatization, the information security of
colleges and universities also needs to be continuously improved. The addition of protective
equipment such as anti-virus walls and IPS will comprehensively strengthen campus network
security protection. However, the lack of compatibility and coordination among many security
equipment makes it difficult to maximize the value of protective equipment. This platform was
developed on this basis, but due to the lack of scientific research data, surveys, personnel, etc., the
platform needs further application and exploration.

Reference
[1] LI Xingquan, Liu Shougui, Design and Implementation of Information Management Platform of
Seismic Equipment on B/S Structure[J], South China Journal of Seismology, 2018, 38(04), 48-53.

[2] Sun Jianli, Li Xinli, etc., Research on Information Platform Recording and Security
Management in College Environment[J]. computer science, 2018, 45(10A):137-141.

[3] Guo Lujie, The Research and Implementation of Leve Protection Auxiliary Assessment System
Based on AHP[D], Beijing Jiaotong University, 2018.