3rd International Conference on Management Science and Management Innovation (MSMI 2016)

The Design and Implementation of Campus Network Security Management Service Platform

Li-Xin Li
Information Center, Beijing Jiaotong University, Beijing, China
E-mail: xlli@bjtu.edu.cn

***Abstract*—It is shown in the investigation and study that there are hundreds of application systems in colleges and universities with developers of different professional levels such as extramural specialists, departments or students. Operating environment of application systems are scattered, such as hosting, cloud service or directly placement in office. Since operating environment of numerous application systems in colleges and universities are complicated, it is hard for some unprofessional developers to manage under vulnerability. At present, colleges and universities have deployed safeguards such as firewall and intrusion prevention system to stop hackers from attacking through conventional network layer. However, vulnerabilities in WEB application system are always used by hackers to attack websites. Therefore, a set of security management service platform is urgently needed to enable information security administrators to find and repair security vulnerabilities ahead of attackers with basic information of application system. Combining with reasons above and practical requirements, a campus network security management service platform is designed and developed.**

Keywords- Campus Network; Security;Informationizion

I. INTRODUCTION

With expanding scale of campus network, internet application is playing a more and more important role in management and teaching in schools. However, factors like lacking of uniform norm and standard, difference in application systems between independent departments and huge amount of scattered systems since information construction of colleges and universities make it difficult for schools to manage all systems in a unified manner [1]. Campus network is frequently attacked due to deficiency in management, vulnerabilities in campus network information system, complicated network environment and large amounts of users [2]. Data of Butian vulnerability response platform shows that there were 2868 vulnerabilities in 339 colleges and universities between 2014 and 2015. Vulnerabilities generate potential safety problems in campus network. In order to know condition of all application systems in campus network, colleges and universities integrate and manage related information of application systems in a scientific approach.

Taking a college as an example, there are over 500 information systems distributed on different servers in the campus network of this college, which provide different services to different users. In order to ensure safety of these application systems, information security administrators have to scan vulnerabilities each month so as to find them in time and inform system administrators to fix the vulnerabilities. Therefore, information of application systems such as affiliated institution, person in charge, function of system, contact and situation of vulnerabilities should be collected in time. However, data above is saved in different application systems, namely official automation system, vulnerability scanning system, firewall and EXCEL documents. Manual abstraction, collection and analysis by information security administrators are inefficient and error-prone. Workload of this way is large and makes it hard to find out vulnerabilities in application systems in time. Due to reasons above, campus network security management service platform is designed. This system can integrate heterogeneous data from different application systems, then analyze, visualize, produce report of those data and issue safety notices. The system is trialed online.

II. GENERAL DESIGN OF SYSTEM

A. Main Function Modules of System

According to practical demand of the college, main function modules of campus network security management service platform are management of record information, vulnerability information, extramural access information and security information.

Record information management consists of integration, modification, inquiry, deletion and derivation of record information. Record information is basic information of information system including function of system, IP address, affiliated institution and person in charge for management of information administrators.

Main functions of vulnerability management are integration, inquiry, deletion and analysis on information of two main kinds of vulnerabilities (web vulnerability and system vulnerability) and comprehensive analysis report of vulnerability.

Management module of extramural access information integrates information of extramural access from firewall database to this platform and enables information security administrators to check and revamp situation of extramural access to system servers.

Main functions of security information module are generating comprehensive analysis report and issuing safety notices. This module analyzes vulnerabilities of all application systems and presents situation of vulnerability distribution to users in form of bar charts and pie charts. It also issues notices of safety rectification to systems owners and affiliated institutions according to related record information.

B. *Architecture design of system*

According to functional requirement of campus network security management service platform, this system applies B/S architecture and it is shown in figure 1. Work interface of information security administrators are implemented by browsers, main parts of logic of things are implemented by servers and only few parts are implemented by front-end.

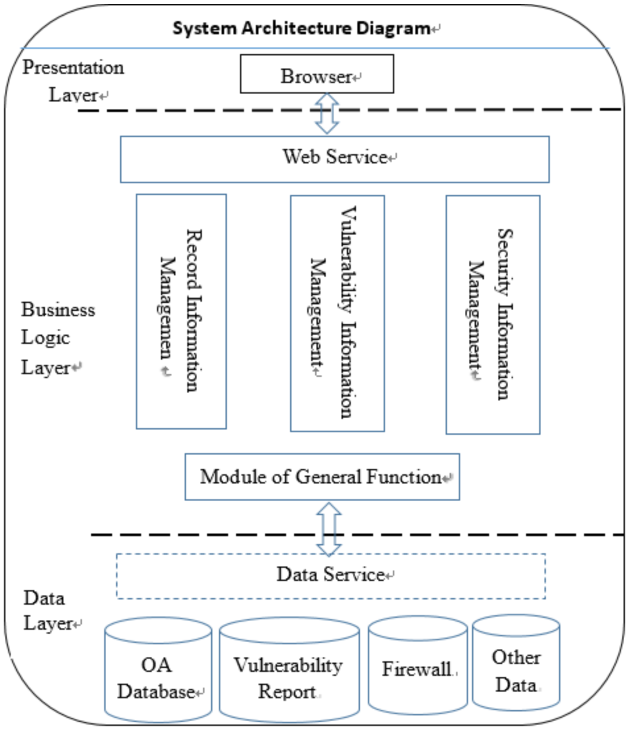
System Architecture Diagram
Presentation Layer
Browser
Web Service
Record Information Managemen
Vulnerability Information Management
Security Information Management
Business Logic Layer
Module of General Function
Data Service
Data Layer
OA Database
Vulnerability Report
Firewall
Other Data

Figure.1. System Architecture Diagram

C. *Module of Record Information Management*

Integration of record information consists of single importing and batch integration. Single importing requires information security administrators to input related information of application systems manually so this method is of low efficiency and aims at application systems not recorded in office automation system. Aiming at those application systems already recorded in office automation system, batch integration is implemented by Excel middleware and takes Excel documents as intermediate medium in data exchange between office automation system and system here. Firstly, record information inputted is judged and be corrected if the result is irregular. Or it will be processed and abstracted needed data to judge whether record information of this application system exists. If there is no similar record information in database, a record will be added to record information table and record information historical table. If there is a similar record, corresponding record in record information table will be updated and a record will be added to record information historical table.

Inquiry function of record information realizes condition query and instant query. Condition query is to combine fields of IP, domain name and import time freely as condition for searching. Instant query is to input anything as condition to search in all fields of target data already found. Through two queries here, users can find data they are interested in quickly and sort it by fields.

Modification and deletion module of record information can modify and delete existing record information. After modification, information will be updated to record information table and a record will be added to record information historical table. When record information is deleted, only information in record information table will be deleted. Record in record information historical table will be kept as data resources for record information statistics later.

Exporting module of record information exports record information needed by users in form of Excel, which helps to data statistics and report of users.

D. *Management of Vulnerability Information*

Module of vulnerability information management consists of integration, inquiry, deletion, analysis of two kinds of vulnerability information and exporting comprehensive analysis report of vulnerability.

Integration of vulnerability information consists of two kinds of vulnerabilities, namely Web application vulnerabilities integration and system vulnerabilities integration. These two kinds of vulnerability information are scanning results of servers and systems respectively from NSFOCUS RSAS. Due to authorization limit, the system cannot gain data directly from database of scanning result. Vulnerability information report in form of Excel based on NSFOCUS RSAS can be applied as intermediate medium in data exchange between campus network security management service platform and NSFOCUS RSAS. Since format and content of Excel from NSFOCUS RSAS cannot be refined according to requirements of users, this platform implements specialized processing on format of documents. Both vulnerability information documents include two worksheets-worksheets of host situation and vulnerability information for system vulnerability information document and worksheets of site overview and risk distribution for Web application vulnerability information document. In integration, system analyzes four worksheets respectively and selects needed data to write into corresponding database table. Firstly, scanning information of vulnerabilities will be read and checked to revamp irregular data for check later and abstract regular one. Then the leak will be judged. If it is new one, the leak will be added into leak database and counter of leak frequency will be initialized as 1, namely find count=1. If not, add one time to counter of leak frequency, namely find_count+1. After update of leak database, ID and IP fields in scanning information of leak will be exported for judging emergence of this kind of leak before in this system. If the result is negative, then a piece of record should be added in distribution chart of application leak. If not, add one time to corresponding leak frequency counters in distribution chart of application leak, namely count+1. Finally, fields of input will be assigned to fields of time for finding the last leak last_find_date.

E. Module of security information management

Main functions of security information module are generating comprehensive analysis report and monthly report as well as issuing security notices and knowledge.

Module function of monthly report generation is as following: The system analyzes leak information of all applications systems in secondary units each month and generates a report. Each monthly report consists of security advisories of all secondary units. Firstly, information security administrators will fill in basic information of monthly report and click button to generate. After collecting basic information of monthly report, the system will put all secondary units in iterator and check whether there is any secondary unit in iterator. If the result is positive, the secondary unit including its host and leak information of hosts will be abstracted to judge whether the amount of host leak is greater than zero. If the amount is greater than zero, leak distribution will be analyzed and a security advisory will be generated. If not, security advisory will not be generated and check the iterator again until there is no secondary unit in it. Then process of monthly report generation is completed. In order to save space, process of generating security advisory is not forming actual documents but saving data for generating security advisory in database, which will be exported to form a security advisory when information security administrators and administrators in secondary units download it.

III. DETAILED DESIGN OF SYSTEM

A. Design of Record Information Module

Record information module includes: basic control-BaseAction.java and DataTableAction.java, data integrated control-InfoUploadAction.java, management control of record information-ArchivalInforMangeDAction.java, management control of record information in secondary units-UserInfoByDepartmentAction.java, basic information entity of users -User, operation interface of basic information entity of users-UserDAO.java and its implementation-UserDAOImpl.java, unique record information entity-UInformation.java, operation interface of unique record information-UInfoDAO.java and its implementation-UInfoDAOImpl.java, historical record information entity-UserInfor.java, operation interface of historical record information-UserInfoDAO.java and its implementation-UserInforDAOImpl.java.

Main methods of data integrated control-InfoUploadAction.java are file uploading- infoUploadFile (), record information integration-saveRecordInfo (row) and record information combination and insertion- operation ().

Main methods of management control of record information-ArchivalInforMangeDAction.java are record information demonstration in secondary units- show (), record information deletion- del () and record information edition- editinit ().

Data integration implemented by record information module is a complex process. Firstly, information security administrators enter import page of record information-importReport.jsp, choose one or more data file (s) need integrating and send order of uploading files- infoUploadFile ()-to data integrated control-InfoUploadAction.java. Data integrated control receives order and reads information, and then it sends field of Excel header and comparison table of database field-uploadChTable.jsp. After filling corresponding tables, security administrators will send order of saving Excel data- saveInfoExcel () to data integrated control which receives order and sends order of reading Excel data- saveRecordInfo(row)-to itself and order of finding conflicting data- uniFind(preAppliDomain, sysIp, sysName)-to UInfoDAO.java. UInfoDAO executes order and send results back to data integrated control which sends page with conflicting data-mergeUniInfo.jsp- to information security administrators. Through click on button labelled “combine or insert”, information security administrators send corresponding data and order to data integrated control which sends corresponding order to UserDAO.java, UInfoDAO.java and UserInfoDAO.java immediately. UserDAO.java, UInfoDAO.java and UserInfoDAO.java save or update data in corresponding database chart and send back result of operation respectively.

B. Design of Leak Information Module

Main functions of module of leak information management are integration, inquiry, deletion, analysis of leak information and generating comprehensive analysis report on leak. Main kinds of leak information module are: leak information integrated control-WebRiskInfoUploadAction.java, leak information operation control-WebInfoOperation-Action.java, leak information analysis control-VulnerStatisticsACtion.java, operation interface of leak database-LeakInfoDAO.java and its implementation-LeakInfoDAOImpl.java, operation interface of leak information in application system-AssociatedTableDAO.java and its implementation-AssociatedTableDAOImpl.java, operation interface of unique record information-UInfoDAO.java and its implementation-UInfoDAOImpl.java, operation interface of extramural access-OffCampusDAO.java and its implementation-OffCampusDAOImpl.java, leak database entity-LeakInfo.java, leak information entity in application system-AssociatedTable.java, unique record information entity-UInformation.java, extramural access entity-OffCampus.java and Excel export tool-ExportExce.java.

Main method of leak information integrated control-WebRiskInfoUploadAction.java-is leak information integration- webInfoUploadFile ().

Methods of leak information operation and control-WebInfoOperationAction.java-are host information loading-webLoad (), leak information editing- editAction (), leak information deletion- dele (), comprehensive information export- exportExcelAction () and detailed host leak information loading- loadWebRiskInfo ().

Main methods of leak information analysis control-VulnerStatisticsACtion.java-are Web leak statistical diagram generating- loadChart () and repeat removing- removeRepeat (IPLeak).

Leak information integration is a process of integrating data from scanning result database of certain scanning system to this platform. Firstly, information security administrators will enter page of Leak information integration-leakimportReport.jsp-to click corresponding button, choose a file to be uploaded and send order of uploading leak file to leak information integrated control-WebRiskInfoUploadAction.java. After reading IP field of files, leak information integrated control will send order of finding user- findUser (IP)-to operation interface of unique record information-UInfoDAO.java-to check whether the IP has been recorded. If it has been recorded, leak information uploading control will send order of updating record information-updateUnInfo (user)-to operation interface of unique record information and update fields of system version as well as system plugin version in uploaded files to corresponding fields in database. Then leak information integrated control will send order of finding all leaks-queryAll ()-to operation interface of database which will send back all leaks after implementation. Leak information integrated control receives all leaks and judges whether there is any leak waiting to be uploaded. If there is no such leak, leak information object-leakInfo- will be generated. Or record-leakInfo-will be abstracted corresponding fields will be updated. With newly generated or updated leak information object-leakInfo, Web leak information integrated control will send order savingOrUpdate (leakInfo) to operation interface of leak database-LeakInfoDAO.java. Newly generated objects will be added and existing objects will be updated. Then Web leak information integrated control will send order-queryByIdAndIp (leakInfoId, user) to operation interface of application system leak information-AssociatedTableDAO.java which implements order and sends all corresponding leak information back to application system. If there is such leak in this application system before, leak information chart of this application system should be updated. Or a record will be added to database. Then all result information will be sent back.

C. *Design of security information module*

Main kinds of security information module are: monthly report management and control-JournalManageAction.java, security notice control-SafetyJournalAction.java, operation interface of host leak distribution information-IpLeakDAO.java and its implementation-IpLeakDAOImpl.java, operation interface of basic information of monthly report-JournalDAO.java and its implementation-JournalDAOImpl.java, operation interface of security notice-SafetyJournalDAO.java and its implementation-SafetyJournalDAOImpl.java, host leak distribution information entity-IpLeak.java, basic information of monthly report-Journal.java, security notice entity-SafetyJournal.java and security information entity-SafetyInfo.java.

Main methods of monthly report management and control are monthly report uploading- show (), security notice reading- showUnited (), monthly leak detail reading-showIpLeakDetails (), monthly report adding- add (), monthly report updating- update (), monthly report publishing- publish () and monthly report deletion- delete ().

Main methods of security notice control-SafetyJournalAction.java-are: reading security notice of secondary unit administrator- showJournal (), security notice downloading- download (), security notice data gaining-getSafetyNotification (safetyJournal, type) and security notice template gaining- getDataMap (safetyNotifications, safetyJournal).

When security notice is generated in security information module, information security administrators will fill in information related to notice and send order of generating notice- add ()-to notice management and control which send order of generating notice- save(journal)-to operation interface of basic information of notice after receiving order. Then operation interface of basic information of notice saves information related to notice generation in corresponding chart in database and send information back to notice management and control. Then notice management and control will send order of finding ID of newly found leak-findNewIds (ip, journal), finding ID of existing leak-findOldIds(ip, journal) and finding ID of leak having been solved- findSolvedIds(ip, journal) to operation interface of application system leak information-AssociatedTableDAO.java which receives order and sends back three kinds of ID. Notice management and control receives information and sends order of updating application system leak information- update (associatedTable) - to operation interface of application system leak information, order of saving security notice of secondary unit- save (safetyJournal) - to operation interface of security notice-SafetyJournalDAO.java and order of saving leak distribution- save (ipLeak) - to operation interface of host leak distribution information. Security notice will be generated and sent back to users after data being saved or updated in corresponding charts in database.

IV. IMPLEMENTATION OF SYSTEM

JAVA programming language with good portability is applied to background development of this system. Hardware environment in system development is IntelCore 3.2 GHZ CPU, 4GB RAM and software environment is JDK1.8, Tomcat 8.0, Mysql 5.6.

The system has been completed and put into use online.

V. CONCLUSION

Although campus network develops quickly nowadays, there is no uniform norm and standard since information construction of colleges and universities. Application systems are purchased or developed by departments dependently and maintained by users. Huge amount of scattered application systems of campus network makes it hard for colleges and universities to manage efficiently. Deficiency in management and potential security problems of Web system lead to frequent attack of campus network.

Development of campus network security management platform enables uniform management of record information of application system inside colleges and universities and health situation of website. It also helps security managers to find and solve security problems before attackers to protect talent cultivation and scientific innovation in colleges and universities.

REFERENCES

[1] Huangqiongzhen, “Survey and Analysis on Usage of Campus Educational Resources”, China Educational Technology,vol.4, pp. 75 -80, 2010.

[2] Fu Xiaolong, Chen Huaichu,Wang Yingxue et al., “Framework of Web Informaion Gate Facing Campus Network”, Education Informationization, vol.11, pp. 35-37, 2002.

[3] Zhang Sanqiu, Book of Distance Education and Campus Network Construction in China, Changchun: Yinsheng Audio Video Press, 2003, pp.10-15.

[4] Wang Yunwu, “Summary of China Digital Campus Constrution”, Modern Distance Education Study, vol.4, pp. 39-50, 2011.

[5] Zuo Li, “Era of Digital Campus 2.0”, China Education Network, vol.4, pp. 8-9, 2008.

[6] Gu Hongzhou, Jiang Chunran, Zhang Lingling et al, “Survey on Domestic and Foreign Network Education Platform”, Available: http://www.Kejizhifu.com.