Experiment Design of Information Security Classified Protection based on the Procedure oriented Cultivation

Jian Jiao[1,a], Xingfen Wang[2,b], Xin Chen[3,c], Qiyuan Liu[4,d]

[1] School of Computer, Beijing Information Science & Technology University Beijing, 100101, China

[2] School of Computer, Beijing Information Science & Technology University Beijing, 100101, China

[3] School of Computer, Beijing Information Science & Technology University Beijing, 100101, China

[a]email:jiaojian@bistu.edu.cn, [c]email:chenxin@bistu.edu.cn

Abstract. For the actual situation that it is generally lack of classified protection experiments in the experimental teaching of colleges and universities, analyzing the relevance between each knowledge points and basic knowledge in classified protection, and proposed an experiment construction of classified protection security based on procedure oriented cultivation, planning the classified protection oriented knowledge system for each knowledge point, then, starting with experimental process and effects, implementing the procedure oriented teaching and cultivation of experimental teaching, improved students' comprehensive practical ability.

Introduction

Information security classified protection is a work that protect information and information carrier according to the importance level. In our country, information security classified protection is broadly security work [1] which means Standards, Products, Systems and Information that relate to this work are all comply with the thought of classified protection. With a series of Ministry of public security's information security classified protection policies and measures introduced, classified security protection has become the most important issue in the construction of security field of many departments. The society's demand for classified protection construction and evaluation personnel also showing a growing trend. Personnel training of information security in colleges and universities should have the ability to train the talents.

Procedure oriented teaching and cultivating is the main way [2] to train professional and technical personnel in recent years, especially for some courses that have more knowledge points, such as Software Engineering [3], English Language Teaching [5], in these fields it has a wide range of applications. In the aspect of comprehensive quality cultivating, it also has some relevant attempts [4], but overall, the emphasis of procedure oriented cultivation still remains in the aspect of construction of the curriculum system.

It should be pointed out that there has two aspects we must attach importance to in procedure oriented teaching, the first is the whole teaching come to fully procedure oriented [6], it needs bring all aspects of the whole teaching into procedure oriented teaching links; The second aspect is teaching management and monitoring mechanism, it is referred in literature [7] that procedure oriented teaching management is equal to consider quality management as the core of teaching, it can be seen that the quality of teaching is always the basic of procedure oriented teaching; while in the process of management, monitoring of the teaching process has become an important means, it needs to ensure the completeness of procedure oriented teaching process through the mechanism [8] of monitoring, management, evaluation and feedback.

Analysis on the knowledge system of classified protection

According to macroscopic analyses, information classified protection includes many levels [9], such as Physical security, Network security, Host security, Data security. Physical security is mainly

related to building construction and other engineering fields, security management is mainly reflected in the formulation and implementation of rules and regulations. Combining the characteristics of school teaching and the teaching characteristics of information security, the practice teaching of classified protection is mainly arranged in the four levels of network security, host security, application security and data security.

The refinement of the knowledge system of each protection level in classified security protection has a certain degree of overlap, for example, the aspects of network security, host security and application security all proposed requirements towards system's access control. But in traditional information security teaching process, cryptography access control and other knowledge run through the various stages of certification process of the safety assessment.

Table.1 is a knowledge coverage table designed for classified protection knowledge point, the four rows represent four levels of data security, host security, application security and network security respectively, the eight columns represent structure security, access control and other knowledge points involved in the theory teaching. We can realize through the above analysis that security knowledge points in classified protection need combined with the specific theories to make further division of this kind of knowledge points, in order to construct a complete knowledge system of security information protection.

Table.1. Knowledge coverage table of classified protection

Evaluation layer	Structural security	Access control	Security audit	Backup recovery	Integrity	Confidentiality	Authentication	Residual information protection
Data security	No	No	No	Yes	Yes	Yes	No	No
Host security	No	Yes	Yes	No	No	Yes	Yes	Yes
Application Security	No	Yes	Yes	No	No	No	Yes	Yes
Network security	Yes	Yes	Yes	No	Yes	No	No	No

Note: "Yes" represents "have the knowledge point", "No" represents "None"

The knowledge system of experimental teaching

In the construction of the network security laboratory, schools will go into a misunderstanding, that is, they add only the experimental module of security, and lack of comprehensive understanding of application areas of network security. As for teaching, knowledge points of network security are mostly contain cryptography, network protocol security, operating system security, code security, and many other content; but the teaching content needs to be pointed at the different types of students, for instance, the difficulty should be stayed at a lower level for the students of secondary and higher vocational education, such levels of students are suitable for the work of the security system after sales, it requires students to manager how to configure the switch, router, firewall, IDS, VoIP, wireless and other network equipment's functions that already exists, and learn how to use these devices to organize network in order to achieve the functions and services needed by the user.

For the students of ordinary engineering colleges, a considerable part of the students engaged in the work of system operation and maintenance. It requires these students' master of the network is no longer a separate device, but dynamic operation of a whole. The network is changing constantly, viruses, network attacks, illegal operations may cause fatal damage to the network at any time. Students need to optimize the architecture of this dynamic network, constraints and shaping the traffic, manage the user, prevent and control the virus, defense the attack, etc.

Overall, classified security protection have the highest technical requirements for students. On the one hand, it objectively requires students to have a strong practical ability, on the other hand, it also requires students to have a solid theoretical knowledge. In addition, in order to complete the management of the team, students also need to have a certain ability of analyze, design and

management.

The construction of laboratory

In order to cooperate with the implementation of the whole experimental teaching plan, it has constructed a relatively complete evaluation platform of classified protection, in the construction, it combined with the cloud platform and virtualization technology [10], comprehensively considerate the teaching platform of classified protection-oriented and adopting the three level classified protection as the main experimental target. Through the front end of the web technology to ensure students achieve training work of classified security protection in the virtual platform.

In this network environment (As shown in Fig.1), it deployed security device area, server area, infrastructure area, office area and network management area separately. In each region, the virtual network is built by using simulation host, switch and router run on virtual machine.

Security device area is mainly deployed these contents include the patch used for computer protection and audit, log server and authentication server, etc. This area focus on the inspection of setting and control strategies of network security, and is the core of the whole network security defense system.
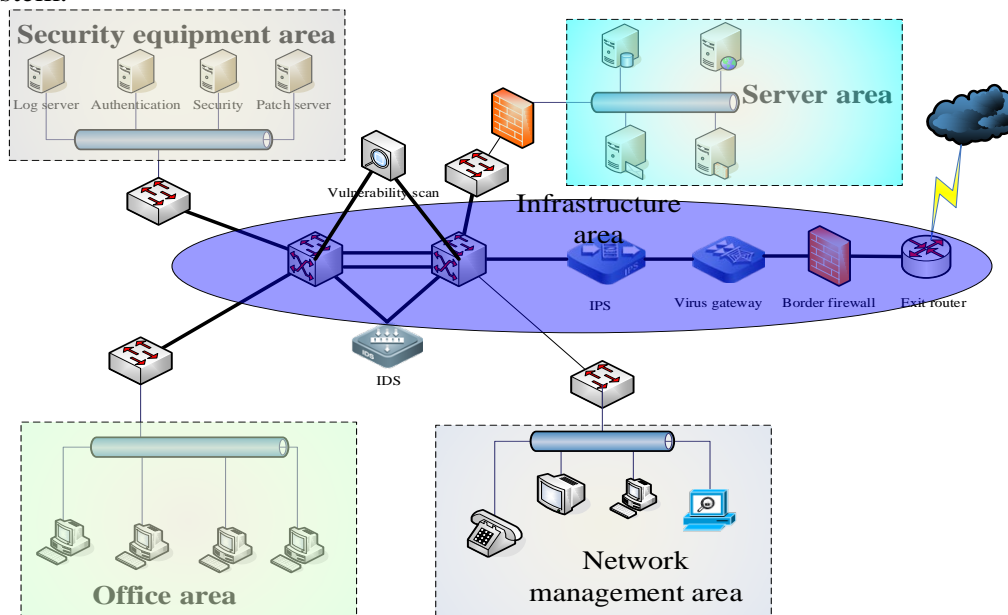

Fig.1. The testing and evaluation laboratory of classified protection

Server area is the core of the whole network's business, and is also the inspection's focus of classified protection, it starts with the field of host and application's security. For network security in classified protection, the infrastructure area is responsible for the main evaluation object; In this area, except the deployment of switches and routers and other equipment, there are also deployment of IPS/FW and antivirus gateway, vulnerability scanning tools and other safety equipment, in order to meet the needs of the three level security protection. Students through the evaluation of the content of these sections, focusing on the implementation of the evaluation of host and application's security.

To ensure the authenticity of the three level network security, the experimental environment is additionally provided with the office area and network management area. Students can achieve the evaluation of the data security, system security, and other test items in the network, they can also complete the actual operation of network management, to further deepen the understanding of the classified security protection.

Procedure oriented training program

On the basis of classified protection experiment courses, we made the experimental program to meet the procedure oriented cultivation, following the knowledge system of classified protection.

The main contents are as follows:

The "procedure oriented" management of experimental process

Managing and monitoring students' experimental process, in other words, is to make standardized management and guidance of the whole process of student from the micro level. In the experimental process, teachers manage and monitor the students' experimental process. The teachers must find the students who have problems in time, support and help them. The main measures include those things: Firstly, previewing and deploying students' experimental knowledge points, understand the preview steps of knowledge points in information security assessment, require students to preview the knowledge which is needed in the specific test items, once the students have problems, the teachers must make an answer. Secondly, making procedure-oriented monitor the of the experiment's process, teachers assess the evaluation scheme and evaluation steps which are developed by students, track the students' evaluation process, record the evaluation time, the test data and evaluation results. Thirdly, making analysis and comments to the evaluation results of students' classified protection, give a comprehensive analysis of the results of the evaluation, and find the students' shortcomings in the evaluation process.

Taking the penetration test in classified protection as an example, according to the requirement of procedure oriented experiment, a series of steps are needed in the course of the experiment:

Step.1, in the aspect of experiment learning, students need to study penetration testing in classified protection, submit learning notes and experiment problems online. Teachers need to assess the students' experimental condition, thus determine whether the students can participate in the experiment; and giving a certain score assessment for students' review.

Step.2, in the experiment, teachers need to give a feasible evaluation for the test scheme which is submitted by students, and ask the students to fill in the content of the test in accordance with the existing test document, including test points, test cases and the specific implementation steps. Teachers must promptly point out the errors of the test report and correct the deficiencies in students' tests.

Step.3, after the experiment, students need to fill in the form of the penetration test results, submit the penetration test report and rectification opinions according to the requirements of classified protection.

The "procedure oriented" management of experimental results

The core of the security assessment of classified protection is the need for students to complete a larger network of security evaluation work through teamwork. It has higher difficulty for students, so it is necessary to do "procedure oriented" management of student's experimental results, combined with the aforementioned experimental teaching system, we should do "procedure oriented" management to experimental teaching effect according to different stages. The main steps include:

Step.1, evaluation for the operation's teaching effect of evaluation tools. Master of evaluation tools is the basic ability in classified protection evaluation, so in order to determine the effect of students' ability to use the evaluation tool, to make a reasonable assessment in in the experiment for students' using process of tools and effects is needed.

Step.2, the process evaluation of students' ability to use the whole knowledge in evaluation experiment. Each evaluation item needed in information security assessment requires students to develop a reasonable evaluation program, and make the use of evaluation data to do effective evaluation. For example, the classified protection evaluation of structure security in network security. The results of this experiment require to realize the students' independent use of knowledge, including using the content of network topology, the principle of computer network, network engineering and firewall technology to analysis the security issues of structure in the network, and to develop evaluation items. In order to ensure the students' learning effect, the experiment needs to record the contents and results of the students in each stage of the evaluation, and analyze the students' learning effect in the whole process. Teachers can understand the performance of the students in the assessment process of classified protection according to the

student's discussion record, it is helpful for teachers to evaluate the design of the experiment and the information of the students' feedback after the experiment.

Conclusion

The experiment in the teaching of information security has always been an important part in the cultivation of students, in view of the request of student's ability in current classified protection evaluation of information security, training of technical personnel in respect of classified protection is the trend of the times. As classified protection is a course that emphasizes practice, the knowledge points involved are more complex, and the request of ability to use knowledge is relatively high. Therefore, it is suitable to use the method of procedure oriented training to reform the experiment system and the experiment teaching, and improve the comprehensive quality of the students in the field of information security.

Acknowledgement

References

[1] Standards of the people's Republic of China GB17859-1999 Computer information system security grading criteria [Z]. National Technical Supervision Bureau, 2001.1.

[2] Yanping Zhou. The introduction of procedure-oriented work to the teaching methods of training professional talents of multimedia [J]. Chai- Chi _ New concept of success. 2014.3.

[3] Fen Yuan. Practice and Research on the Software Technology Curriculum System of Higher Vocational College Based on Working Process [J]. Modern computer (Professional edition), 2014.5: 56-59.

[4] Xiangjun Fei, Chunlan Wang. The procedure-oriented reform of teaching and management in Colleges and Universities Based on the comprehensive quality training [J]. Contemporary educational theory and Practice, 2014 (6) 12:89-91.

[5] Yan Zhu, Lei Qin. Process teaching method based on interactive network technology -- a new approach to college English Writing Teaching [J]. Journal of Chifeng University (Natural Science Edition), 2013(29) 10:258-262.

[6] Zhengyu Zhu and so on. A discussion teaching mode based on the whole process management [J]. Computer Education. 2013.3:80-84.

[7] Hongwei Yan. Practice and conception of process-oriented teaching assessment and management in Colleges and Universities [J]. Science and Technology Innovation Herald, 2013.25:111-112.

[8] Jie Zeng. The implementation of process management and goal management in teaching quality monitor of Higher Vocational Colleges [J]. Industry and Technology Forum, 2015 (14) 7:209-211.

[9] National standard of the people's Republic of China. GB/TXXXX-XXXX Information security technology and information system security classified protection, implementation guide [Z]. National Technical Supervision Bureau. 2007.

[10] Xiaolei Guo. Educational Reform Research of Computer Basic Courses Based on Cloud Computing Environment [J]. Computer development and Application, 2012 (10) :45-47.