Exploration of Network Security Professional Classroom in Higher Vocational Colleges in the Era of Big Data

Jicheng Chen[*], Hongyou Ge, Long Zhao, Juan Sun

School of Computer and Communication, Jiangsu Vocational College of Electronics and Information, Huaian, China
[*]Corresponding author

Abstract: *With the rapid development of information technology, big data has gradually penetrated into all walks of life, and has had a profound impact on various fields. As higher vocational colleges, the classroom education of network security majors should also keep pace with the times and explore how to better cultivate network security talents in the era of big data. This paper mainly applies the factor analysis method to obtain the important index of network security classroom evaluation, and uses the questionnaire survey method to collect the student satisfaction data. According to the experimental and survey data, 88% of the students are satisfied with the environment of the training room. As to whether the course is combined with the reality, 68% of the students expressed satisfaction and high degree of union, and 30% thought it was general. Therefore, it is necessary to further explore this major.*

Keywords: *big data, higher vocational colleges, network security, professional classroom*

1. Introduction

In the era of big data, network security content is no longer limited to the traditional anti-virus, firewall and other core security technologies, cloud computing security, data security and privacy and many other fields are gradually becoming an important part of network security. Therefore, higher education institutions should timely adjust the curriculum and add the curriculum in these new fields to meet the demand for network security talents in the era of big data.

Network security is one of the important fields in today's society. Mastnetwork security expertise is crucial to protect the important information resources of individuals and organizations. It is proposed that under the background of the accelerated development of educational informatization, adapting to the objective requirements of teaching plan reform in the current era of big data has become an important topic in the development of higher education [1-2]. Some scholars say that in the era of big data, the network security problem of colleges and universities is becoming increasingly serious. Although big data brings us a comfortable life, security issues such as personal information also pose a major threat to our life on campus [3-4]. Another experts point out that the college's safety education is facing a new situation. In the era of data explosion, online data and information are diversifying. Effective identification and use of network information has become a key issue in university campus security [5-6]. In the network security class, students can deeply understand and apply the basic principles, technologies and strategies of network security through theoretical research and practical operation.

This paper first studies big data technology and suggests the importance of network security. Secondly, the teaching of the basic knowledge of computer network security is explored, and the key points and difficulties of the classroom are analyzed. Then, the network security professional classroom is analyzed and designed. Finally, the relevant data and conclusions are obtained through the cultivation of practical skills and the questionnaire survey.

2. Network security major in higher vocational colleges in the era of big data

2.1 Big data technology

In the era of big data, teaching methods should also change. The traditional "farce" teaching method no longer meets the learning needs of students. Therefore, teachers should actively explore new teaching methods, such as project-based learning, flipped classroom, etc., so as to better stimulate students' interest in learning and improve their learning efficiency. In the era of big data, people and things are being digitized. With cloud infrastructure, openness, circulation and sharing of data is possible, but it also poses myriad social risks. In the case of big data and related convenience, students may lose their rational judgment or excessive belief in the emergence of information due to psychological immaturity and low resistance to temptation, which leads to the security risk of students' mobile payment, user data loss, online fraud, malicious virus attacks and other intensification.

Network security technology is a very practical subject, so the practical teaching in the field of network security is particularly important [7-8]. Vocational schools should strengthen practical teaching and improve students' practical skills and innovative awareness by creating an experimental network security environment and holding network security competitions. In the era of big data, network security majors have put forward higher requirements for the quality and performance of teachers. Vocational schools should strengthen teacher training and induction training, train high-quality teachers, and provide a better guarantee for the development of network security. [9-10]. In the era of big data, student skills training is the core of face-to-face cybersecurity education. Higher education institutions should pay attention to cultivating practical skills, innovation ability and teamwork ability. The focus is to train students to better adapt to the demand for network security talents in the era of big data.

2.2 The teaching of basic knowledge

The basic theory of computer network is an important foundation of network security [11-12]. We need to learn the basic principles, structure and communication methods of the network, including the OSI reference model, TCP / IP protocol family, etc. In addition, you also need to understand the common types of threats and attacks on the network, such as denial of service attacks. By learning the basic theory of computer network, students can have a deep understanding of the nature of network security problems, and provide basic support for the subsequent security measures and strategies.

The security of the operating system and the database management system is also an important part of the network security. Students must learn common security vulnerabilities and attack methods for operating systems and database management systems, such as software vulnerabilities in the operating system, insufficient authorization controls, and weak passwords. Also, you must understand the appropriate security measures and defense strategies, such as encryption technology, authentication, and access control. By learning the security of the operating system and the operating system and database management system.

Cryptography and secure transmission technology are one of the core contents of network security, [13-14]. Students must understand the basic concepts and principles of cryptography, including symmetric encryption algorithms, asymmetric encryption algorithms, and hash functions. In addition, secure transmission technologies such as digital certificates, public key infrastructure (PKI) and secure socket layer (SSL / TLS) are required. By learning cryptography and secure transmission technologies, protect the confidentiality, integrity and availability of network communication, and prevent information from being intercepted, manipulated or tampered with during transmission.

In the network security professional course, the basic theory of computer network, the security of operating system and database management system, as well as cryptography and security transmission technology are the content that students need to learn [15]. Through theoretical learning and hands-on operation, the students can master the relevant knowledge and skills, and cultivate the ability and awareness to solve the network security problems. Only by understanding and mastering this basic content, can we lay a solid foundation for the effective network security protection and protection.

2.3 Network security professional classroom

The professional cybersecurity course includes a basic set of cybersecurity knowledge. These knowledge includes, but is not limited to, basic knowledge of computer network, operating system security, network protocols and communication, basic knowledge of cryptography, etc. By learning these basic knowledge, students have a comprehensive understanding of the network structure and communication methods, which lays a solid foundation for further study.

In network security courses, students must learn and master various security attacks and defense techniques. Considering network vulnerabilities and weaknesses, students should learn the methods and skills of penetration testing and vulnerability exploration to assess and improve cybersecurity. In addition, students should learn about common types of attacks, such as denial-of-service attacks, malware, and social engineering, as well as corresponding defense strategies and techniques. Practical operation is a very important part of it. Students must use a laboratory environment for a variety of cybersecurity experiments and exercises, such as building virtual networks, simulated attacks and defenses, and real-time monitoring and response. Through practical actions, students can transform theoretical knowledge into practical and applied skills and develop skills and experience to solving cybersecurity problems. Furthermore, special attention should be paid to promoting students' teamwork and innovative thinking. Cybersecurity is a complex area that requires a variety of expertise and skills to respond effectively. Thus, students can conduct group projects and case studies in class to solve practical problems together through collaboration and discussion. At the same time, you will encourage students to think creatively and explore new cyber security technologies and methods to adapt to changing cyber threats. The classroom should also combine practical cases and industry trends to improve students' practical skills and professional knowledge. Cybersecurity industry experts are invited to give lectures and exchanges on the latest security technologies and trends to help students understand the real work environment and needs.

3. The cultivation of practical skills

3.1 The construction of the teaching platform

The education platform is the key to implementing the education. The educational platform is designed to provide a simulated network environment in which students can learn and apply cybersecurity knowledge and technology into practice. This can be achieved either by building a virtualized environment or by using experimental cybersecurity platforms. The teaching platform should include resources for a variety of experiments and exercises, such as configuration and managing experiments, simulated attacks and defense mechanisms, and real-time monitoring and analysis of network traffic. By using this educational platform, students can perform simulation operations in real-world scenarios and develop practical skills. Due to the destructive and offensive nature of network security experiments, using public networks for experiments is obviously inappropriate. Building an experimental LAN environment through a virtualization platform is currently the first choice for network security courses for national higher education organizations. Select open source network vulnerability platforms, such as DVWA, Pikachu, etc. Choose the teaching method of "mutual learning from shallow to deep".

3.2 Build a network security experiment environment

The platform is divided into four layers, including the infrastructure layer, the virtualization layer, the experimental platform layer, and the upstream user access layer. We must purchase different types of equipment, such as switches, routers, firewall, VPN, traffic control, user behavior monitoring, and various attack and defense software. Internet-based cloud computing methods have the advantages of dynamic and flexible resource allocation, unified management, and effective reduction of the construction cost of experimental platforms. The cloud platform must monitor and manage various functional components to identify and eliminate errors in a timely manner. The experimental environment includes virtualization technology, network segmentation, virtual network card and virtual machine, enabling students to conduct a variety of network security experiments and exercises. By constructing the experimental environment, students simulate real web scenarios and perform various exercises and safety tests. Platform servers are divided into controlled servers, server nodes, virtual attack machines, virtual targets, etc.

3.3 Penetration testing and offensive and defense drills

Assess network security using vulnerability analysis tools, penetration testing tools, and vulnerability mining techniques, and learn how to manage a variety of attack tools and techniques. With penetration testing and attack and defense training, you will understand the security issues in the network and propose appropriate defense strategies and solutions. At the same time, learning and application of real-time monitoring and response technology, as well as event tracking and forensics methods, improve the ability to deal with cyber threats and security incidents.

3.4 Handling methods for responding to network threats and security incidents

A phishing attack is an attack that uses channels such as email and social media to induce victims to click on malicious links and steal sensitive information. Malware software is a program in which a computer system performs malicious operations. Social engineering attack is a form of attack that uses one's psychological weakness to induce victims to leak sensitive information.

In 2019, a large enterprise suffered a cyber attack. The attacker invaded the internal network of the enterprise through phishing emails and malicious software, and successfully obtained a batch of sensitive data. Immediately after the incident, the company activated the emergency response mechanism and took a series of remedial measures to prevent similar incidents from happening again. People are not aware of the importance of cyber security and lack vigilance against cyber attacks such as phishing emails. Although the enterprise deployed firewall, intrusion detection and other security facilities, but failed to update and upgrade in time, resulting in the absence of security facilities. Lack of perfect security management system and process, for the network security incidents to deal with and response ability is insufficient. All of this leads to the problem. Therefore, it is necessary to carry out regular network security training and knowledge popularization to improve students' awareness of network security and prevention. In the network, it is necessary to regularly check and upgrade security facilities such as firewalls and intrusion detection to ensure their normal functions, establish sound security management systems and processes, and ensure that network security incidents can be quickly handled and responded to.

Handling security incidents requires establishing a security system, including firewalls, intrusion detection and defense systems, real-time monitoring and alarm networks. Students should be trained to enhance their awareness of network security and enhance their ability to detect and respond to network threats. Through developing an emergency plan when time occurs, the response process and responsible persons can be clarified, and it is essential to ensure that they can respond quickly in the event of a safety incident. Moreover, sensitive data should be encrypted to prevent data leakage or forgery, and multi-level security protection systems based on different security levels is necessary to be established to ensure network security.

4. Teaching practice cases

4.1 Instructional objectives

We should understand the functions of Linux common services ssh, telnet, ftp, samba and mysql, and master the login mode and password modification mode of ssh, telnet, ftp, samba and mysql services, and then master the use of the nmap scanning tool and the metasploit platform. Through practice, according to the weak password test results, we can make plans, targeted to complete the weak password reinforcement, forming the logical idea of weak password screening and reinforcement of Linux server. Factor analysis assumes that the X-dimensional random vector satisfies:

$$A = \varepsilon + X\bar{f} = \bar{e} \tag{1}$$

Among them, meet: $E\vec{e}$

$$E\vec{e} = 0, E\vec{e}\vec{e}^{S} = diag(\theta_1^2, \theta_2^2, ..., \theta_X^2) \tag{2}$$

If A satisfies the above formula, the random vector A is said to have the factor structure. It is easy to calculate that:

$$Var(A) = \vec{X}\vec{X}^{s} + \sum \tag{3}$$

The importance index of the different factors can be obtained by the factor score.

Login to the actual combat platform, each group is assigned the same vulnerability target machine, test which weak password vulnerabilities exist in the vulnerability target machine, and reinforce them. According to the principle of homogeneity and heterogeneous, three students are grouped. After the students define the task, they will study independently according to the problem guidance, and make the plan of penetration test and vulnerability reinforcement under the organization of the team leader. This paper uses the nmap tool to scan the target machine service status. Then we crack the weak password using metasploit platform and view the flag under the target machine / root after cracking, and then fill in the vulnerability inspection report. After the reinforcement is completed, the student role is converted to penetration test engineer, and each group conducts penetration test on the reinforced target machine of other groups. The score is given according to the data learning record, attendance, classroom discipline displayed on the training platform. Teacher evaluation Table 1 is as follows:

Table 1: Teacher evaluation form

Evaluation factors	Value
Classroom discipline	3
Data learning	5
Report completion rate	5
Clean workstation	2
Answers to classroom questions	4
Feasibility and thoroughness of the plan	3
The idea and logic of the plan are clear	3
The group presentation represents clear and fluent expression	2

4.2 Implementation effect evaluation

Whether it meets the students' learning needs of courses and the corresponding social post needs of the major is the standard to measure the success of curriculum development, design and implementation. Course feedback investigates students' satisfaction through a questionnaire survey.

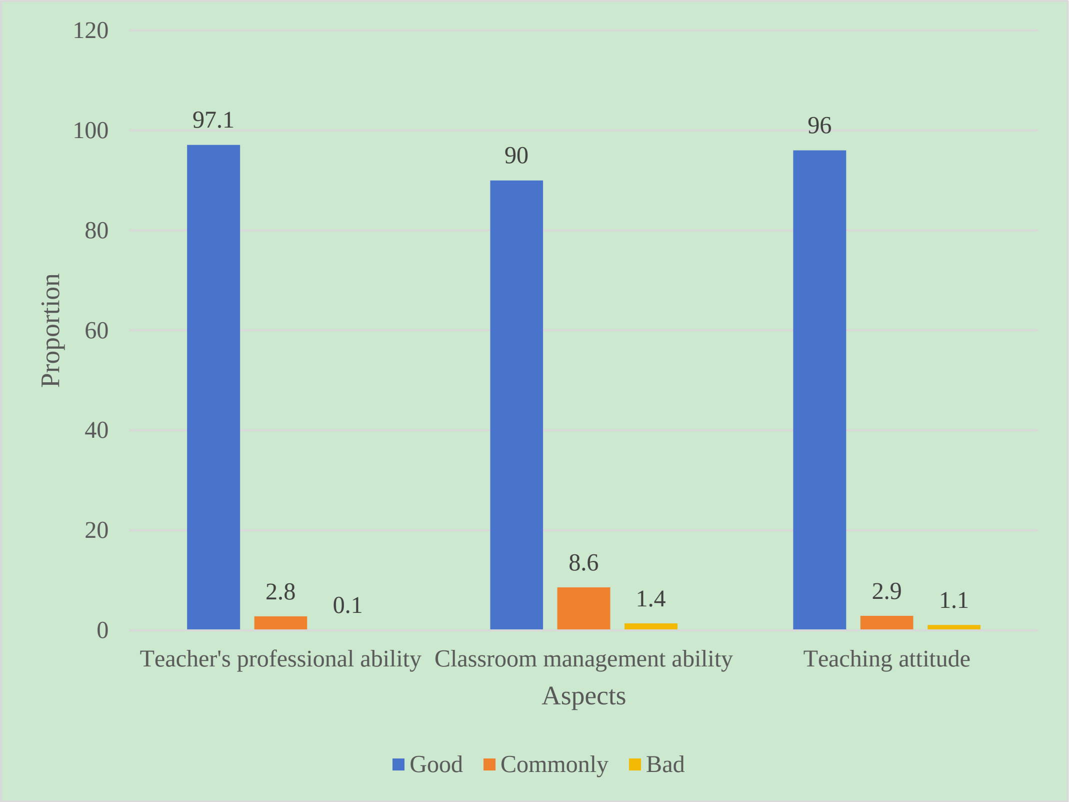

Figure 1: Students' satisfaction with their teachers

As shown in Figure 1, it can be seen from the data that 90%, 96% and 97.1% of students are very positive about management ability, teaching attitude and professional ability, respectively. The data show that students have high satisfaction with teachers. In addition, a small number of students still have a bad attitude towards these three aspects.

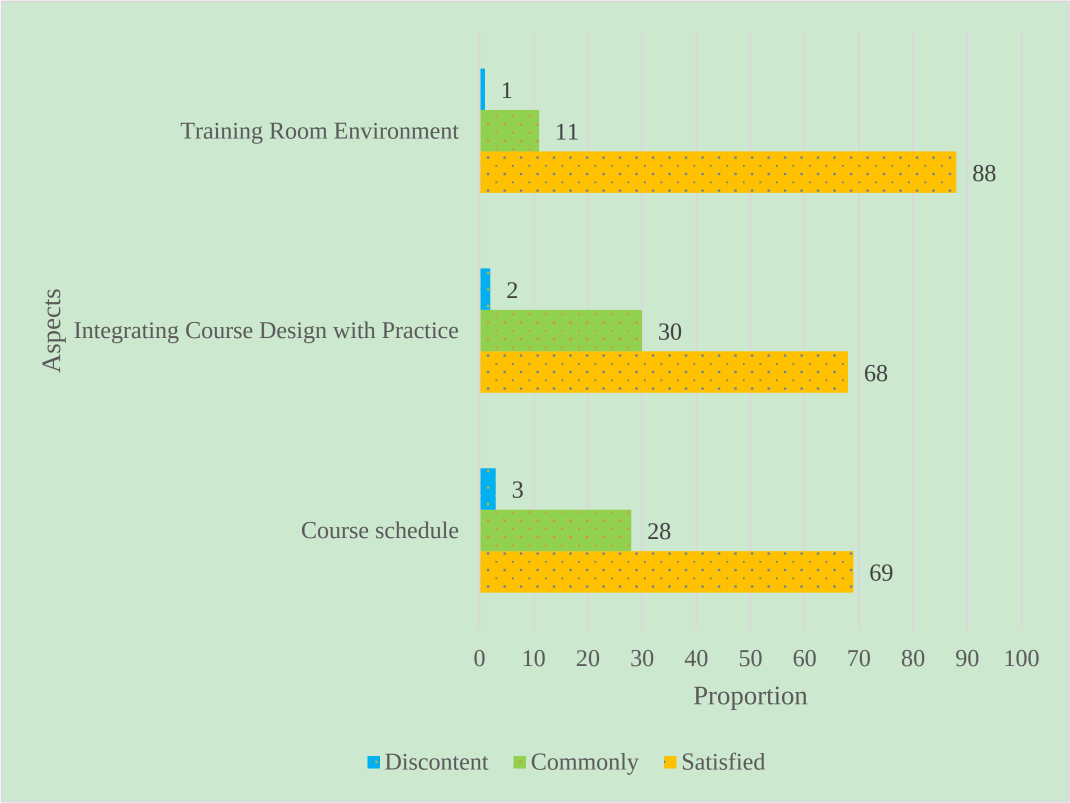

Figure 2: Course teaching and practical training environment satisfaction

As shown in Figure 2, in terms of the course schedule, 69% were satisfied and thought that the progress was reasonable and the acceptance condition was good. However, 28% of the students had a general attitude, thinking that the pace was a little faster and slightly difficult, and some students could not keep up at all. From the feedback of this part of data, although most students can adapt to the teaching rhythm, we found that many students think that the progress is fast, so they need to keep investigating, analyzing and analyze the feedback and make appropriate adjustments in the later teaching.

5. Conclusion

The teaching content of network security major is to cultivate students' comprehensive quality through their practical operation ability, application skills and analysis to solving problems. Therefore, in the context of big data era, higher vocational colleges must strengthen the construction of network security professional curriculum system. In the teaching of network security, teachers enable computer and Internet to realize data sharing through multimedia technology, providing students with colorful, real and reliable learning opportunities. The teaching mode is mainly based on students, supplemented by teachers. The training goal of the network security major in higher vocational colleges is to solve the problem-solving ability when college students encounter problems in the learning process, and to provide students with a good and efficient learning environment. Students need to learn in the process, constantly innovate and improve.

References

[1] SeukGue Hong, HyungBin Seo, MyungKeun Yoon: Data Auditing for Intelligent Network Security Monitoring. IEEE Commun. Mag. 2023, 61(3): 74-79.

[2] Ranganathan Mavureddi Dhanasekaran, Jing Ping, German Peinado Gomez: End-to-End Network Slicing Security Across Standards Organizations. IEEE Commun. Stand. Mag. 2023, 7(1): 40-47.

[3] Aanjanadevi, S. Aanjankumar, K. R. Ramela, V. Palanisamy: Face Attribute Convolutional Neural Network System for Data Security with Improved Crypto Biometrics. Comput. Syst. Sci. Eng. 2023, 45(3): 2351-2362.

[4] Junfeng Sun, Chenghai Li, Yafei Song, Peng Ni, Jian Wang: Network Security Situation Prediction

Based on TCAN-BiGRU Optimized by SSA and IQPSO. Comput. Syst. Sci. Eng. 2023, 47(1): 993-1021.

[5] Nandita Pattnaik, Shujun Li, Jason R. C. Nurse: A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. ACM Comput. Surv. 2023, 55(9): 1-180.

[6] Benyamin MazhariSefat, Soodeh Hosseini: Social network security using genetic algorithm. Evol. Syst. 2023, 14(2): 175-190.

[7] Minh-Nam Pham, Duy-Hung Ha, Tran Trung Duy, Le-Tien Thuong: Security-reliability tradeoff of MIMO TAS/SC networks using harvest-to-jam cooperative jamming methods with random jammer location. ICT Express2023, 9(1): 63-68.

[8] Pavol Sokol, Richard Stana, Andrej Gajdos, Patrik Pekarc ̌k: Network security situation awareness forecasting based on statistical approach and neural networks. Log. J. IGPL 2023, 31(2): 352-374.

[9] Durga, Periyasamy Sudhakar: Implementing RSA algorithm for network security using dual prime secure protocol in crypt analysis. Int. J. Adv. Intell. Paradigms 2023, 24(3/4): 355-368.

[10] Sabrine Ennaji, Nabil El Akkad, Khalid Haddouch: i-2NIDS Novel Intelligent Intrusion Detection Approach for a Strong Network Security. Int. J. Inf. Secur. Priv. 2023, 17(1): 1-17.

[11] Umesh K. Raut, L. K. Vishwamitra: Seek-and-destroy algorithm for optimal resource allocation and security analysis in software-defined vehicular networks. Int. J. Pervasive Comput. Commun. 2023, 19(1): 97-123.

[12] Elmehdi Illi, Marwa K. Qaraqe, Faissal El Bouanani, Saif M. Al-Kuwari: On the Physical-Layer Security of a Dual-Hop UAV-Based Network in the Presence of Per-Hop Eavesdropping and Imperfect CSI. IEEE Internet Things J. 2023, 10(9): 7850-7867.

[13] Shalli Rani, Himanshi Babbar, Gautam Srivastava, Thippa Reddy Gadekallu, Gaurav Dhiman: Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain. IEEE Internet Things J. 2023, 10(7): 6074-6081.

[14] Abdelwahab Boualouache, Bouziane Brik, Sidi-Mohammed Senouci, Thomas Engel: On-Demand Security Framework for 5GB Vehicular Networks. IEEE Internet Things Mag. 2023, 6(2): 26-31.

[15] Somia Sahraoui, Nabil Henni: SAMP-RPL: secure and adaptive multipath RPL for enhanced security and reliability in heterogeneous IoT-connected low power and lossy networks. J. Ambient Intell. Humaniz. Comput. 2023, 14(1): 409-429.