Research on Training Strategies of High-level Practical Skills of Network Security Talents

Xiulan Yin

Shandong College of Electronic Technology, Jinan, 250200, Shandong, China

Keywords: Cyber security threats; Practical skills training; International cooperation and exchange; Network security talents

Abstract: With the acceleration of global digitalization, network security issues have attracted more and more attention. The popularity of various network devices, systems and applications makes the security of cyberspace particularly complicated. A variety of network security threats such as data leakage, malware attacks, APT(Advanced Persistent Threats) and supply chain attacks are constantly emerging, making network security talents a vital resource. However, there is still a huge gap in the current network security education and training system for the cultivation of practical skills. Therefore, this study aims to deeply explore the training strategies of high-level practical skills of network security talents. Through in-depth cooperation with enterprises and research institutions, we provide students with real network environment and scenes, and carry out practical training such as red and blue team drills, penetration tests and emergency response. At the same time, the importance of online learning, continuing education and professional certification in talent training is emphasized. Generally speaking, this study provides a comprehensive, multi-participation, practical-oriented network security personnel training strategy. It is expected to provide useful guidance for educational institutions, enterprises and policy makers in the training of network security talents.

1. Introduction

In the digital age, network security has become the focus of global attention. With the development of technology and digital transformation, and the popularization of various network devices, systems and applications, the security of cyberspace has become more complicated. From data leakage and malware attacks to APT and supply chain attacks, the types and complexity of network security threats are constantly increasing [1]. This puts higher demands on network security talents, which not only requires them to have profound theoretical knowledge, but also requires them to have strong practical ability. However, the current network security education and training system is difficult to meet these requirements [2]. Most educational institutions focus on traditional classroom teaching and theoretical knowledge, but lack practical training in real environment. This leads to many network security practitioners often lack enough experience and skills to deal with real threats. In order to solve this problem, this paper will make an in-depth study on the training strategy of high-level practical skills of network security talents. First of all, this paper analyzes the demand of network security talents and reveals the shortcomings of the existing training model. In particular, educational institutions place too much emphasis on the teaching of theoretical knowledge and neglect the accumulation of practical experience. This has caused a large number of network security practitioners to perform poorly in real scenes and it is difficult to deal with various advanced threats. Secondly, the article puts forward a set of skills training strategies based on actual combat. In addition, the paper also discusses the role of international cooperation and exchange in the cultivation of network security talents. In view of the globalization of cyber threats, it is very important to strengthen international cooperation and share experience and technology to improve the actual combat ability of cyber security talents. We will start with the demand analysis of network security talents, discuss the problems existing in the current training mode, and then put forward a set of skills training strategies based on actual combat, aiming at helping network security talents better cope with the threats in reality [3-4]. Background With the rapid progress of technology, such as cloud computing, IoT(Internet of Things), artificial intelligence and blockchain, enterprises and organizations are facing unprecedented opportunities for digital transformation, however, it also brings huge security risks [5]. In recent years, frequent large-scale data leakage incidents, ransomware attacks and targeted attacks have highlighted the importance of network security. Statistics show that the loss of network security incidents is increasing every year, and the complexity of attacks is also increasing [6]. For example, APT usually involve multi-stage, multi-technology and multi-target attacks, which are often initiated by experienced attackers or state-supported hacker teams. The purpose of these attacks is not only to steal data, but also to destroy infrastructure, affect business or conduct espionage [7]. Faced with this situation, network security talents have become the resources that enterprises and organizations urgently need. However, the current talent market is in short supply, especially high-level network security talents are scarce. Many organizations say that it is difficult for them to find network security experts with practical experience, not only because of the large demand, but also because the existing training system can not meet the practical needs [8]. In order to better understand this problem and find a solution, this paper will deeply discuss the practical skills training strategy of network security talents. We hope that through this research, we can provide valuable guidance and suggestions for educational institutions, enterprises and policy makers, and jointly promote the progress of network security talents training [9].

2. Analysis of the current situation of network security personnel training

2.1. Training mode under the education system

With the in-depth development of information technology, most colleges and universities have set up network security-related majors and courses. However, there is a gap between academic education and practical skills. Mainly can be described from the following two aspects:

(1) Theoretical orientation

Traditional network security education often attaches importance to theoretical knowledge, such as cryptography, security protocols and network security principles. These basic theoretical knowledge are necessary to cultivate students' thinking ability and theoretical background, but it is difficult to meet the needs of practical work by these alone.

(2) Lack of practical environment

Due to various restrictions, it is difficult for some colleges and universities to provide students with real or simulated network environment for practical training, which leads to students' lack of practical experience.

2.2. Present situation of enterprise and actual combat training center training

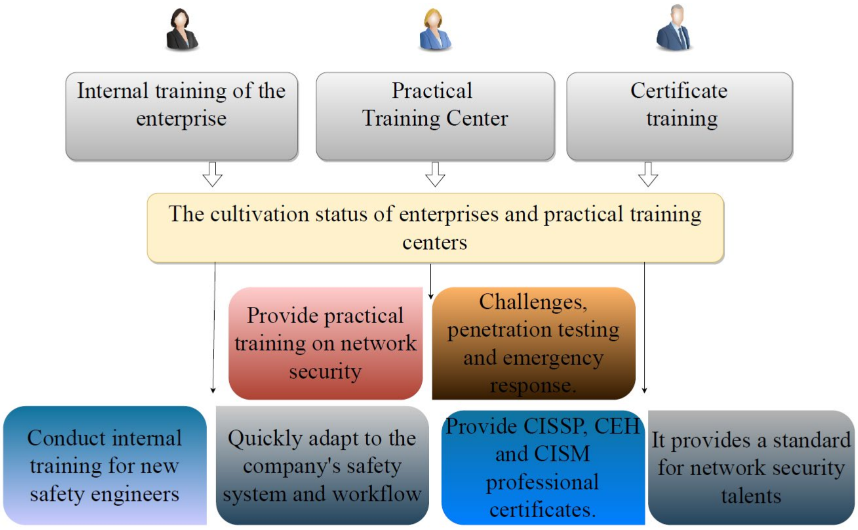
Internal training of the enterprise
Practical Training Center
Certificate training
The cultivation status of enterprises and practical training centers
Provide practical training on network security
Challenges, penetration testing and emergency response.
Conduct internal training for new safety engineers
Quickly adapt to the company's safety system and workflow
Provide CISSP, CEH and CISM professional certificates.
It provides a standard for network security talents

Figure 1 Training status of enterprises and actual combat training centers

With the increasing demand of enterprises for network security, some large companies and training institutions have begun to provide targeted practical training. The training status of enterprises and actual combat training centers is shown in Figure 1.

From the figure 1, it can be found that there are mainly three types of training: first, internal training: large enterprises often have their own safety teams, and they will conduct internal training for newly hired safety engineers to make them quickly adapt to the company's safety system and workflow [10]. Secondly, practical training centers: these centers provide practical training on network security for enterprises or individuals, such as CTF(Capture The Flag) challenge, penetration test and emergency response. Finally, certificate training: professional certificates such as CISSP, CEH and CISM also provide a standard for network security talents to measure and improve their skills.

2.3. Main problems and challenges

Despite the above-mentioned training mode, the training of network security talents still faces some problems and challenges. For example, there is still a gap between the teaching content of colleges and universities and the actual work needs. Especially in some emerging areas of network security, such as cloud security and Internet of Things security. Although some training centers provide actual combat training, limited by cost and resources, the common problems are insufficient practice opportunities and unrealistic scenes. Network security technology and threats are developing rapidly, but the updating of teaching content and training materials often can't keep pace with the times. At present, the evaluation criteria of network security talents are not uniform, and different organizations and institutions may have their own evaluation systems, which has brought obstacles to the flow and development of talents. This is not only the responsibility of educational institutions and enterprises, but also the common responsibility of the whole society, government and relevant institutions. In a word, the cultivation of network security talents is a long-term and systematic project, which requires the joint efforts of all sectors of society. The current situation of training network security talents has a certain foundation, but it still faces many challenges. In order to meet the future security needs, the education and training mode needs to be further innovated and improved.

3. Practical skills training strategy

3.1. Scene-based simulated actual combat training

In skill training, scene simulation is an effective method, which enables students to experience real attack and defense situations in a relatively safe environment.

3.1.1. Attack and defense simulation

This chapter is divided into red team and blue team for drills: the red team simulates attackers and attacks specific targets, while the blue team is responsible for defense. This kind of drill can help students understand the real scenes of attack and defense, and improve strategies according to feedback. Finally, the purple team drills: the red team cooperates with the blue team to analyze and solve security problems together and cultivate the ability of cross-team cooperation. In the real working environment, pure theoretical knowledge is far from enough. In order to make up for this defect, educational institutions need to strengthen cooperation with enterprises and research institutions and provide more practical training opportunities. Red and blue team drills, penetration tests and emergency response are all practical methods worth popularizing.

3.1.2. Testing and emergency response in real environment

Conduct penetration test and emergency response drill, the contents are as follows.

Penetration test: simulate real attack behavior, identify and repair security vulnerabilities under authorization.

Emergency response drill: simulate security incidents and train students how to quickly identify, respond and recover.

3.2. Teaching mode of combining curriculum with actual combat

The course of pure theory is difficult to meet the actual needs, so the teaching mode needs to be reformed in three steps, as shown in Figure 2.

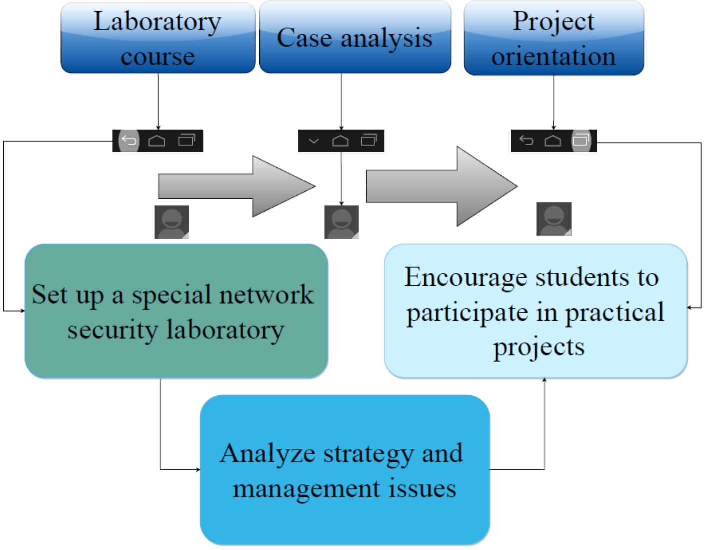
Laboratory course
Case analysis
Project orientation
Set up a special network security laboratory
Encourage students to participate in practical projects
Analyze strategy and management issues

Figure 2 Teaching mode reform

The main reform contents of teaching mode reform can be divided into:

Laboratory course: Set up a special network security laboratory for students to practice in the experimental environment, such as building a security environment, analyzing malware, conducting penetration testing, etc.

Case analysis: Combining with real security incidents, analyze the technical, strategic and management issues behind them to help students form a comprehensive perspective.

Project orientation: encourage students to participate in practical projects, such as open source security tool development, security product evaluation, security consultation, etc.

3.3. Continuous skill upgrading and certificate system

The field of network security is changing rapidly, which requires practitioners to continue to learn and improve. For example, Coursera, Udemy and Pluralsight provide a wealth of network security courses for practitioners to learn at any time. Certificates such as CISSP, CEH and CISM are not only the symbol of practitioners' skills, but also the motivation for them to continue learning. Conduct skills assessment regularly, give specific feedback and suggestions to practitioners, and help them to define their development direction.

3.4. Cooperative training mode between enterprises and universities

In order to bridge the gap between education and industry, enterprises and universities need to cooperate more closely. Internship and training can be carried out, and enterprises provide internship and training opportunities for students to study and practice in a real environment. At the same time, build a laboratory, and enterprises can cooperate with universities to build a network security laboratory to jointly develop technologies and solve practical problems. You can also hold lectures and seminars, and invite experts from enterprises to give lectures and seminars in colleges and universities to share the latest technology and experience.

3.5. International cooperation and exchange absorb the latest external practical experience and skills

Facing the threat of global network security, international cooperation has become particularly important. Academic exchanges can be conducted, scholars and students are encouraged to participate in international conferences and seminars, and exchange and cooperate with foreign counterparts. Carry out project cooperation, cooperate with foreign research institutions and enterprises, and carry out joint research and development and project implementation. Conduct study abroad and training, and encourage students to go to foreign universities and research institutions for short-term or long-term study and training. Through the above analysis, it can be seen that the high-level practical skills training strategy needs multi-party cooperation, continuous innovation and improvement in combination with practical needs, in order to cultivate network security talents with real practical ability.

4. Conclusions

Network security has become the core issue in today's digital age. Facing the increasingly complex security threats, it is essential to have network security talents with high-level practical skills. However, from the above research, we can see that there are still gaps between theory and practice, education and industry, and domestic and international in the current talent training system. First of all, the education system often focuses on theoretical knowledge in the field of network security, but ignores the cultivation of practical skills. Secondly, the rapid evolution of network security technologies and threats requires practitioners to constantly update their knowledge and skills. This means that talent training can not only stay in the school education stage, but should become a continuous and lifelong process. Online learning platform, professional certificate and skill evaluation can provide practitioners with channels and motivation for continuous learning. In addition, international cooperation and exchange is also the key to improve the level of personnel training. Facing the threat of globalization, we need to jump out of national boundaries and cooperate with foreign counterparts to jointly develop technologies and share experiences. Finally, in order to cultivate network security talents with real practical ability, we need a comprehensive, multi-party participation and practical-oriented training strategy. It is hoped that this study can provide valuable reference for relevant institutions and jointly promote the progress of network security personnel training.

References

[1] Beurana R, Vykopal J, Belajova D,et al.Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms[J].Computers & Security, 2023, 24(9):9-14.

[2] Mallah R A, Badu-Marfo G, Farooq B.Cybersecurity Threats in Connected and Automated Vehicles based Federated Learning Systems[J]. 2021, 26(8):10-16.

[3] Chou T, Hempenius N.An Assessment of Practical Hands-On Lab Activities in Network Security Management[J]. International Journal of Technical Research & Science, 2020, 11(6):21-26.

[4] Makeri Y A.The Effectiveness of Cybersecurity Compliance in a Corporate Organization in Nigeria[J].International Journal on Recent and Innovation Trends in Computing and Communication, 2019, 7(6):16-19.

[5] Dinham P.CISCO, VICTORIA UNI PARTNER ON SECURITY SKILLS TRAINING[J]. Exchange, 2019, 16(AUG.19):2-3.

[6] Ali A, Vaish A.CYBER SECURITY AND THE INTERNET OF THINGS: VULNERABILITY, THREATS AND ATTACKS[J].International Journal of Technical Research & Science, 2021, 19(7):10-13.

[7] Haney J M, Lutters W G.Cybersecurity advocates: discovering the characteristics and skills of an emergent role[J].Information and Computer Security, 2021, 22(11):10-17.

[8] Graham C M, Lu Y.Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements[J].Journal of Computer Information Systems, 2023, 63(4):937-949.

[9] Huang J D.Problem-Based Cybersecurity Lab with Knowledge Graph as Guidance[J].Journal of Artificial Intelligence Technology (English), 2022, 2(2):55-61.

[10] Mashiane T, Kritzinger E.Identifying Behavioral Constructs in Relation to User Cybersecurity Behavior[J].Eurasian Journal of Social Sciences, 2021, 9(5):12-16.