Publisher
Vandana Publications
www.vandanapublications.com

International Journal of Engineering and Management Research

2026 Volume 16 Number 3 June

E-ISSN:2250-0758
P-ISSN:2394-6962

Research Article

Cyber Security

Teaching Exploration of Campus Intranet Attack-Defense Competition in Comprehensive Practice for Cyber Security

Ruoqi H[1*], Dongchen Z[2]

DOI:10.31033/IJEMR/16.3.2026.1915

[1*] Huang Ruoqi, Information Technology Center, Wenzhou University, Wenzhou, China.

[2] Zeng Dongchen, Information Technology Center, Wenzhou University, Wenzhou, China.

Driven by the dual demands of advancing the national cyber power strategy and cultivating new engineering cyber security talents, practical teaching of cyber security in universities must break the bottlenecks of traditional models and align with industry's practical talent needs. Regarding the problems of virtual scenarios, monotonous training and one-sided evaluation in the current Comprehensive Practice for Cyber Security, this paper integrates the campus intranet attack-defense competition into professional practical teaching. It takes the university's real systems and intranet environment as the practical arena, and constructs an integrated competition-teaching fusion model featuring pre-competition training, in-competition practice, post-competition review. Based on teaching implementation and questionnaire-based empirical analysis, this paper evaluates students' satisfaction with professional skill enhancement, learning interest and initiative, competition arrangement and assessment methods, and verifies the feasibility and effectiveness of the promoting teaching through competition model. The results show that the campus intranet attack-defense competition effectively remedies the shortcomings of traditional practical teaching, narrows the gap between talent training and job requirements, and provides a reference for the reform of cyber security practical teaching in universities.

Keywords: Attack-Defense Competition, Cyber Security, Promoting Teaching Through Competition

Corresponding Author

Huang Ruoqi, Information Technology Center, Wenzhou University, Wenzhou, China.
Email: ruoqi@wzu.edu.cn

How to Cite this Article

Ruoqi H, Dongchen Z, Teaching Exploration of Campus Intranet Attack-Defense Competition in Comprehensive Practice for Cyber Security. Int J Engg Mgmt Res. 2026;16(3):23-30.
Available From
https://ijemr.vandanapublications.com/index.php/j/article/view/1915

To Browse

Manuscript Received	Review Round 1	Review Round 2	Review Round 3	Accepted
2026-05-02	2026-05-16			2026-06-03

Conflict of Interest	Funding	Ethical Approval	Plagiarism X-checker	Note
None		Yes	5.15	

1. Introduction

Under the strategy of strong cyber power and the requirements for cultivating new engineering talents, the cyber security engineering major increasingly emphasizes the cultivation of practical skills. As a core practical course of the major, the "Comprehensive Practice Course for Cyber security" is a key carrier connecting theoretical teaching and industry needs. At present, the cyber security practice teaching in colleges and universities generally suffers from problems such as virtualized scenarios, monotonous training[1], and one-sided evaluation. The practice platforms are mostly a simulated environments[2], which are disconnected from the real intranet attack and defense scenario. The teaching is mainly based on demonstration and replication, and students lack active exploration and adversarial thinking. The assessment relies on experimental reports, which makes it difficult to quantify practical skills, resulting in a gap between talent cultivation and job requirements. The campus intranet attack and defense practice competition takes the real network environment as the target and integrates core skills such as vulnerability mining, penetration testing, and security hardening, which is highly consistent with the teaching objectives of the comprehensive practice course. This paper deeply embeds the campus intranet attack and defense practice competition into the "Comprehensive Practice Course for Cyber security", constructs an integrated teaching model of "pre-competition training, In-competition practice, Post-competition review". Through teaching practice and questionnaire survey, the ‘competition-promoting teaching’ model indeed improves students' abilities and reforms the curriculum, which could be summarized as a replicable path for practical teaching reform.

2. Current Status of Comprehensive Practice for Cyber Security

The White Paper on Practical Ability of Cyber Security Talents first proposed the practical ability of cyber security talents[3] into four types: "attack and defense practical ability", "vulnerability discovery ability", "engineering development ability" and "combat effectiveness evaluation ability".

It also pointed out that by 2027, China’s cyber security personnel shortage will reach 3.27 million, of which 92% of enterprises believe that they lack cyber security practical talents. This situation puts forward higher requirements for cyber security courses in colleges and universities. The current teaching organization and implementation of comprehensive cyber security practice courses still generally follow the construction logic of traditional experimental courses, which further exacerbates the problems of incompatibility with the goal of practical education in terms of practical scenarios, teaching models and evaluation mechanisms.

Detached from the Real Intranet Environment

The practical scenarios focus on the security deployment requirements of engineering projects or scenarios, involving demand analysis, scheme design and deployment, security strategy optimization,etc. The course relies more on virtual simulation for teaching, its experiments are relatively fixed and differs greatly from the real intranet architecture and system operation logic in the campus. Most of the experimental tasks are based on preset vulnerability points [4], such as the detection and repair of common Web vulnerabilities such as SQL injection and XSS cross-site scripting, and the operation steps are standardized. Therefore, students can only complete the process of vulnerability reproduction, and fail to have the ability to bypass the logic of security devices such as WAF and IPS in the real intranet environment, so they cannot carry out practical training that is close to the real business scenario, such as intranet lateral penetration, boundary protection, and intrusion tracing.

Lack of Confrontation and Initiative in Teaching

The current course mainly adopts the project-driven teaching method [5], and students form project groups and complete teaching objectives and tasks through project implementation. Although the project group improves students' teamwork ability to a certain extent, it may exacerbate the differences in level among members in terms of professional skills. For example, in the intranet lateral penetration training task, the student who is responsible for the initial simulation environment construction can gain a deeper understanding of the network topology.

However, in the subsequent operations involving the use of scanning tools and further privilege escalation using webshells, other members mainly focus on verification, resulting in insufficient cultivation of practical thinking and problem-solving abilities.while the other members mainly perform practical verification for subsequent operations involving scanning tools and further privilege escalation using webshells, resulting in insufficient cultivation of practical thinking and problem-solving ability.

Inadequate to Measure Practical Ability

In terms of the evaluation system, course assessments are mainly based on lab reports, theoretical tests, and presentations, making it difficult to comprehensively measure students' core practical abilities such as the application of relevant tools, vulnerability discovery, and defense design. Furthermore, evaluation results are primarily used for grade determination, failing to provide feedback for optimizing teaching content and improving teaching methods.

3. Teaching Design for Integrating Campus Intranet Attack and Defense Competition into Comprehensive Practical Course

Facing the dual demands of industry and campuses, integrating intranet attack and defense practice competitions into comprehensive practical courses is of paramount necessity. (1) From a talent cultivation perspective: The intranet attack-defense competition breaks down the barriers between theory and practice, stimulating students' initiative and desire for exploration, encouraging them to solidify their theoretical foundation and strengthen their practical skills. Unlike conventional CTF competitions, the training content of attack-defense competitions based on the campus's real internal network highly overlaps with the work content of enterprise penetration testing and security operations positions, shortening students' adaptation period and further identifying, selecting, and cultivating cyber security professionals. (2) From a campus operations perspective: The attack-defense practice based on the campus's real systems allows students to familiarize themselves with campus network security operations processes in advance, and also builds a reserve force for campus network security vulnerability inspection and system reinforcement, achieving a win-win situation for talent cultivation and campus security. (3) From a teaching reform perspective: Integrating competitions into courses can restructure practical teaching content, optimize teaching processes, and improve the evaluation system, promoting the transformation of traditional verification-based practice into comprehensive, adversarial, and combat practice.

The teaching design is carried out in three stages: pre-competition, in-competition, post-competition. Each stage is synchronized with the course teaching progress, so as to truly realize the integration of competitions into the curriculum system and teaching process.

3.1 Pre-competition Training

The pre-competition phase focuses on knowledge preparation and skills training, employing a "dual-instructor team" comprised of full-time university faculty and industry engineers. The university faculty taught theoretical content such as intranet architecture principles, vulnerability causes, and network protection mechanisms, while industry engineers focused on practical tool operation, attack and defense strategies, and industry security standards. The training was structured around four modular training modules,which were progressively increasing difficulty: "Intranet Lateral Penetration Training", "Enterprise Scenario Penetration Training", "Campus Network Comprehensive Penetration Training", and "Enterprise Security Protection Construction".

In addition, a special training session on practical security protocols was launched during pre-competition, clearly defining the operational red lines for real campus intranet competition. Malicious data deletion, malicious system crashes, and traffic flooding were strictly prohibited. An isolated testing network segment was designated to mitigate the risk of intranet competition interfering with normal system status. The entire training utilized existing course resources, allowing students to steadily build the comprehensive capabilities required for real-intranet competition.

3.2 In-competition Practice

The In-competition phase focuses on practical combat as the core teaching component,

encouraging students to comprehensively apply knowledge and collaborate to get the target, thus strengthening their offensive and defensive thinking and practical abilities. The red team consisted of four students, with each team taking turns playing the roles of attacker, information gatherer, and document writer. This avoided the problem of some students lacking practical experience in traditional project group settings. The blue team consisted of three members of Information and Technology Center. Utilizing the campus's existing firewall and situational awareness platform, they monitored the red team's attack behavior in real time and simultaneously recorded abnormal access logs. Dedicated instructors provided on-site guidance, technical Q&A, and process supervision during the competition. A judging panel of two industry engineers established tiered scoring standards, assigning scores based on vulnerability severity, attack chain integrity, and the steps of vulnerability reproduction. These scores were directly included in the course's practical assessment grade.

To enhance students' enthusiasm for discovering vulnerabilities in target assets and to strengthen the standardization of attack report review, an online management system integrating vulnerability discovery, report submission, and judge review was developed and deployed. A real-time attack and defense competition visualization dashboard was also built, as shown in Figure 1. The data screen dynamically displayed the teams' real-time scores and rankings, the attack situation of campus's systems, and the distribution of effective vulnerabilities, intuitively presenting the overall competition situation and enhancing the sense of realistic combat. At the scoring level, assets were divided into two categories based on their business priority: important assets and general assets. Under the same vulnerability type, important assets received twice the score of general assets, further testing the teams' strategic decision-making capabilities. To address the issue of duplicate reports of the same vulnerability from the same system, the competition added a "priority rights allocation" mechanism. This meant that after the first report of the same vulnerability was verified and becomes effective, the first three teams to submit the report gained priority access to the vulnerability and received corresponding score. Subsequent submissions of the same vulnerability would not be scored repeatedly.

This rule not only reduced the network resource consumption caused by homogeneous repeated scanning attacks, but also incentivized teams to speed up information detection and prioritize the discovery of high-value vulnerabilities.

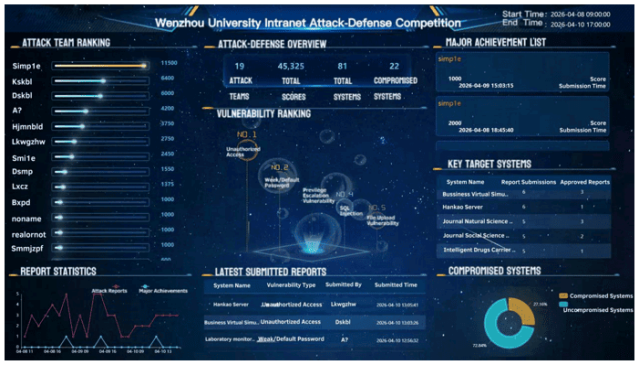

Figure 1: The data screen of campus intranet attack-defense competition online management system

3.3 Post-competition Review

The Post-competition phase focuses on centralized review and self-review process, which is a crucial step in achieving a closed-loop teaching process and optimizing the integration of subsequent practical course content. Centralized review was jointly reviewed by the judging panel and instructors, selected typical successful and unsuccessful penetration tests from the practical exercise. These were then thoroughly analyzed using attack logs retained by the blue team, dissecting the causes of vulnerabilities, shortcomings in defense configurations, and security hardening solutions, while extending and expanding upon theoretical knowledge points from the course. The self-review process, centered on summarizing and solidifying results. Each team comprehensively reviewed the attack and defense process, technical approaches, and shortcomings, independently writing an attack and defense practice report. And then representatives from outstanding teams are selected to share their insights around asset assessment strategies, high-value vulnerability discovery techniques, and key points for report writing.

From the perspective of campus's system, combining vulnerability attack reports and security hardening solutions, targeted vulnerability fix was carried out on the system vulnerabilities exposed during the competition. The effectiveness of vulnerability fix was verified through review,

ensuring the competition results were implemented to serve campus network security operations and maintenance. In terms of teaching reform, teachers identify and address weaknesses in teaching based on common issues reflected in practical reports and course evaluation results. These weaknesses are then adjusted into subsequent course content and training. At the same time, the competition mechanism and scoring rules are optimized to create a complete closed-loop teaching implementation, evaluation feedback, and teaching improvement.

4. Empirical Analysis of Teaching Effectiveness Based on Scale Questionnaire Survey

In order to objectively evaluate the effectiveness of the integrated teaching model of competition and course, a questionnaire was designed around four dimensions: professional skills enhancement, learning interest and initiative, competition arrangements approval, and the rationality of assessment methods. A five-point Likert scale was used for quantitative evaluation, supplemented by open-ended questions to collect suggestions for improvement. The survey participants were students enrolled in the Comprehensive Practice of Cyber security course. The distribution and collection of questionnaires strictly adhered to the principles of anonymity, independence, and voluntariness. A total of 49 valid questionnaires were collected, and the sample structure reflects the overall teaching of the course.

4.1 Analysis of Reliability and validity

The reliability analysis of the questionnaire is shown in Table 1. The Cronbach's α coefficient is 0.981, which is higher than the confidence standard of 0.8, indicating good internal consistency of the scale. The KMO value is 0.889, and the Bartlett's test of sphericity is significant, indicating that the construct validity of the scale meets the requirements of statistical analysis.

Table 1: Analysis of Reliability

Research Dimension	Number of Items	α Coefficient
Professional Skills Enhancement	3	0.977
Learning Interest and Initiative	3	0.962
Competition Arrangements Approval	4	0.966
Rationality of Assessment Methods	2	0.957
Overall	12	0.981

4.2 Analysis of Variance

Over 30% of students felt they had no or weak foundation in cyber security practical skills and chose to take the "Comprehensive Practice for Cybersecurity Course" to improve their professional abilities and cope with course assessments. Based on the students' prior cyber security practical skills, they were divided into three groups: zero foundation, weak foundation, and good foundation. A one-way ANOVA was used to compare their scores across four research dimensions(professional skills enhancement, learning interest and initiative, etc.). The results are shown in Table 2. No statistically significant differences were found in the scores of students with different practical skills across the four research dimensions ($P>0.05$). This indicates that the integrated teaching and competition model of "pre-competition training - in-competition practice - post-competition review" effectively mitigated the gap in students' original foundations. This teaching model can not only meet the needs of students with a good foundation to deepen their practical skills, but also help students with zero or weak foundations to fill their practical gaps, demonstrating the advantage of adapting to students with different study situations.

Table 2: Analysis of Variance

Prior Cyber Security Practical Skills	Professional Skills Enhancement	Learning Interest and Initiative	Competition Arrangements Approval	Rationality of Assessment Methods
Zero Foundation(n=5)	3.47±1.56	3.53±1.61	3.40±1.64	3.80±1.64
Weak Foundation(n=14)	3.76±1.02	3.93±0.64	4.14±0.58	4.07±0.73
Good Foundation(n=30)	3.91±0.98	3.98±1.05	4.05±1.01	4.07±1.00
F	0.414	0.409	1.115	0.16
P	0.663	0.667	0.337	0.853

4.3 Analysis of Influence Relationship

The four dimensions are positively correlated, and the influence relationship of different dimensions are shown in Table 3. In terms of professional skills enhancement, students generally agree that the attack and defense competition helps in mastering the core knowledge points of the course,

but there is still room for improvement in understanding intranet architecture and applying theoretical knowledge to practical situations. In terms of learning interest and initiative, students generally agree that the competition-course integration model is superior to the traditional one. This model not only effectively stimulates learning interest but also significantly improves teamwork and problem-solving abilities. In terms of competition arrangement approval, students highly approve of the overall arrangement of integrating the competition into the course, especially appreciating the clear and reasonable judging criteria, and strongly hope for continued competitions. In terms of the rationality of the assessment methods, students highly approve of the existing assessment system and generally support the integration of team scores into the course assessment, which indirectly indicates that the competition design aligns with the course requirements, and the process-oriented and practical assessment model conforms to the teaching principles of the comprehensive practice for cyber security.

Table 3: Influence Relationship of Four Dimensions

Research Dimension	Item Settings	Mean	Standard Deviation
Professional Skills Enhancement	Mastery of core course knowledge points (e.g., vulnerability discovering, penetration testing, security hardening, etc.)	3.878	1.033
	Understanding of the architecture of campus intranets and the operational logic of systems	3.796	1.06
	Flexibly applying theoretical knowledge to campus intranet attack-defense competition	3.796	1.099
Learning Interest and Initiative	Campus intranet attack-defense competition have stimulated my interest in learning comprehensive practice for cyber security	3.939	1.029
	Campus intranet attack-defense competition have effectively improved my abilities in teamwork, problem investigation and problem solving	3.857	1.08
	Compared with traditional practical courses, I am more willing to devote time to learning content related to offensive and defensive practices	3.959	1.02
Competition Arrangements Approval	Campus intranet attack-defense competition is highly compatible with comprehensive practice for cyber security	3.939	1.088
	Pre-competition training, in-competition practice and post-competition review are very helpful for my course learning	3.959	1.02
	The evaluation criteria of the intranet attack-defense competition are clear and reasonable	4.082	0.997
	I hope such campus intranet attack-defense competition can be continuously held in subsequent courses	4.061	1.029
Rationality of Assessment Methods	The current course assessment items (including requirement analysis, solution design, deployment and implementation, result analysis of course reports, etc.) are reasonable	4.041	0.978
	It is reasonable to include team scores from campus intranet attack-defense competition in the course assessment.	4.041	1.04

5. Existing Problems and Improvement Strategies

While the competition-course integration model has demonstrated some effectiveness in teaching practice, there is still room for further optimization.

The questionnaire includes open-ended questions addressing the shortcomings of the competition and subsequent optimization efforts. Based on questionnaire feedback and daily campus intranet security management experience, the existing problems are as follows: First, the pre-competition training lacks coverage and detail orientation. Most students lack real cyber security attack and defense experience, and initial participation lacks guidance. Furthermore, students' overall practical foundation is weak, making them prone to abnormal scanning behavior and failing to develop systematic project-based practical skills. Second, the experimental course content is not sufficiently adapted to practical application. Some operations and tools lack universality, making it difficult for students to transfer what they have learned to real applications or system. Third, asset information collection capabilities vary widely. Most students stop at exploiting single web vulnerabilities, lacking chain-based capturing capabilities and failing to fully leverage the practical training value of real systems. Fourth, the computer lab's hardware and software equipment are outdated, affecting the efficiency of penetration testing tools. Fifth, the number of website targets available for attack in the competition is limited. Some systems are out of service, causing students to spend unnecessary time on these target. In addition, the competition is held infrequently, leaving students with a lack of continuous practical opportunities after class.

To address the aforementioned issues, the following improvements will be made to teaching: First, the pre-competition training system will be improved by conducting tiered basic teaching and specialized training in areas such as vulnerability discovery and the use of common penetration tools. Industry experts with extensive practical experience will be invited to provide case studies and on-site guidance to enhance pre-competition training. Second, the content of experimental courses will be appropriately adjusted in collaboration with teachers, focusing on in-depth teaching of practical skills such as Sqlmap and BurpSuite to fully prepare students for the competition. Third, an asset intelligence gathering training program will be added, teaching manual information collection methods combining with campus topology. A project on chain vulnerability discovery will be set up around mainstream architectures such as Tomcat, Nginx, and Windows, guiding students to progress from single-point vulnerabilities to vulnerabilities within the same architecture and origin.

Fourth, the hardware and software configuration of the computer lab will be upgraded, and equipment maintenance will be strengthened. Fifth, a regular equipment inspection and monitoring system will be established to ensure the stable operation of campus targets. The competition plans to be optimized by adopting a short-cycle, high-frequency competition organization to strengthen routine practical training.

6. Conclusion

Integrating campus intranet attack-defense competitions into comprehensive practice for cyber security is an effective way to promote the transformation of practical teaching towards real-world applications or systems. The competition-course integration model constructed in this paper, encompassing pre-competition training, in-competition practice, and post-competition review, has achieved significant results in enhancing students' learning interest, strengthening their practical skills, and optimizing course quality. Conducting campus intranet attack-defense competitions is highly replicable. In the future, the efforts will continue to promote the reform of the real practical teaching system, providing more solid teaching support for cultivating high-quality, practical cyber security talents.

Acknowledgement

This paper was supported by the 2025 Zhejiang Provincial University Laboratory Work Research General Project "Construction of University Cyber security Attack and Defense Laboratory: Platform-Driven, Competition-Led, and Practice-Oriented" (Project No. YB202530) and the Zhejiang Provincial Department of Education General Project "Application of Data Security in University Public Data Platform" (Project No. Y202352109).

References

[1] Chen P, Wang J, Yu H. (2024). Exploration of attack and defense confrontational experimental teaching for information system security protectio. *Computer Education*, (11), 216-220. DOI: 10.16512/j.cnki.jsjjy.2024.11.026.

[2] Zou X, Hu N, & Gu Z. (2024). Current status and prospects of network range research. *Chinese Journal of Network and Information Security*, (05), 1-22. DOI: CNKI:SUN:WXAQ.0.2024-05-001.

[3] Duan, G. (2025). Exploration and practice of a research-driven teaching model for cyberspace security majors in engineering universities. *Journal of Natural Science Education, 2*(5), 51.

[4] Hu W, Liu W, & Li X. (2024). Construction of an innovative teaching system for cybersecurity courses based on practical skills development. *Computer Education*, (02), 85-89. DOI: 10.16512/j.cnki.jsjjy.2024.02.002.

[5] Wang G, Guo N, & Liu J. (2024). Teaching practice of "Network attack and defense technology" integrating OBE and project-driven approach. *China Electric Power Education*, (03), 73-74. DOI: 10.19429/j.cnki.cn11-3776/g4.2024.03.002.