Demand analysis and framework function design of cyber range construction in Colleges and Universities

Zhang Yuehong
Shanghai Technical Institute of Electronics& Information, Shanghai 201411
azhangyuehong@stiei.edu.cn

Abstract: This paper designs the network topology design, node simulation and environment construction, and drives the cyber range in three dimensions according to the teaching and scientific research needs of colleges and Universities: the module based on the classroom, the safety challenge of self-defining schedule, and the dynamic practice based on the team, so as to meet the needs of teaching and scientific research in the construction of cyber range in Colleges and universities.

1. Introduction
Under the increasingly severe situation of cyberspace confrontation, the key is based on network simulation and effect evaluation. The significance of the cyber range constructed by technology becomes more and more important [1]. No matter from the aspects of ensuring national security, maintaining social stability, industrial development and reducing economic losses, the cyber range has broad application prospects and high social and economic benefits [2].

2. Demand analysis
The main functions of network cyber range[3] include: 1) Evaluation and verification of network attack and defense weapons; 2) Scientific experiments and verification of new technologies; 3) Support personnel training and exercise.

Specific to the campus environment, the summary requirements are shown in Table 1:

| Function Module Name       | Objectives to Achieve                                      |
|----------------------------|-----------------------------------------------------------|
| Analog Network             | Provides a mirror image close to the enterprise network in the real environment. |
| Training Scene             | Can run a widely applicable and repeatedly deployable training transaction, which can simulate multiple roles Attack Scenarios |
| Target drone               | Design and generate a new training ground in a simple and easy way. |
| Flow generator             | Generating benign data traffic in the virtual network to optimize training tasks |
| Training Configuration Tool| Configure and generate new training transactions simply, quickly and effectively. |
Task Completion Analysis Report Function  
Able to provide mission completion reports for past training

Integrated Learning Management System  
Can share valid data between the learning management system and the network shooting range; Allow students to independently train in the learning management system, and also can cross to range-based training

Test Tools  
Able to score individual and team activities of students

3. Characteristic analysis
In the aspect of simulating and testing the network environment, the cyber range should provide various types of network equipment and host equipment [4] at the three levels of physical objects, virtual machines and containers to meet the needs of users for different fidelity of equipment simulation, and also provide support for traffic and user behavior simulation.

The cyber range provides a scene-based evaluation model, supports correctness evaluation and quantitative evaluation, and provides customizable analysis rule definitions, allowing users to write analysis rules as needed and use collected data for analysis and evaluation [5]. The cyber range shows the experimental situation based on the analysis results of network topology and collected data.

4. Architecture design and function analysis

4.1. Introduction
The cyber range in the college environments takes requirement determination, task setting, resource allocation, operation deployment, experiment operation, data collection and result evaluation as the business process of the network security experiment to support the whole life cycle of the network security experiment.

4.2. Technical Architecture
This architecture provides an operation-oriented method to test the skills and abilities of individuals and network protection teams through roles and tasks. In this framework, each user can be assigned a learning plan, which provides a unique scoring method for measuring individual proficiency programs and overall progress [6]. The technical framework of the cyber range is shown in Figure 1:

![Cyber range system architecture](image-url)  
Figure 1: Cyber range system architecture
4.2.1. The experimental module based on basic theoretical knowledge

The experimental module based on basic theoretical knowledge covers four levels, as shown in Table 2:

Table 2. Four levels of the experience module

| Course Module                          | Training content                                      |
|----------------------------------------|------------------------------------------------------|
| Basic Course Module                    | Network Foundation                                   |
|                                        | Safety Foundation                                    |
|                                        | Basic Event Response Layer                           |
| Event Response Module                  | Event Response Module                                 |
|                                        | Flow Analysis                                        |
|                                        | Defence in Depth                                     |
|                                        | Event Response Layer (Advanced)                      |
| Industrial Control System module       | Critical Infrastructure                              |
|                                        | Safety of Industrial Control System                  |
|                                        | Safe Operation of Industrial Control System          |
| Advanced Expansion Module              | Malware Analysis/Reverse Engineering                 |
|                                        | Event Response Layer                                 |
|                                        | Penetration testing/vulnerability assessment         |
|                                        | Digital Forensic                                     |
|                                        | Interdepartmental Network Attack and Defence         |

4.2.2. The five subject categories involved in the customized security challenges

The five subject categories involved in the customized security challenges are shown in Table 3:

Table 3. Five subject categories of security challenges

| Category                | Theme               | Description                                                                 |
|-------------------------|---------------------|-----------------------------------------------------------------------------|
| Web Application Security| Application Security| Security and vulnerability of web-based applications                      |
| APP Protection          | Application Security| Traditional network security discipline emphasizes the security of a single system and application Completeness, including privilege escalation and operating System/Application Threats |
| Cryptography            | Encryption and Decryption | Include encryption algorithms, secure communication protocols, digital signatures, and so on |
| Network Security        | Network             | Emphasis is placed on the understanding of OSI model, through packet capture analysis network Network Communication |
| Evidence Collection     | Evidence Collection | Incident response, data collection, forensics data management (chain of custody) |
4.2.3. The content description Based on the dynamic training content of the team

The content description is shown in Table 4:

| Dynamic training          | Content Description                                                                 |
|----------------------------|--------------------------------------------------------------------------------------|
| Attack and Protection      | The machine that obtains and maintains control uses the target vulnerability flag to  |
|                            | indicate                                                                             |
|                            | Control and protect our systems and remove vulnerabilities                            |
|                            | Reinforce the system and patch it                                                   |
| The King of Other Mountains| Similar to flag winning competition                                                 |
|                            | Multiple machines join the system, similar to the game process                      |
| Botnet                     | Role-playing malware analyst and computer forensics analyst                          |
|                            | Team-based and assigned in different work scenarios                                  |
|                            | According to the completion time and the completeness of the plan, points are given  |
| Penetration Test           | Role-playing penetration test engineer                                               |
|                            | Group-based, work in different scenarios                                            |
|                            | According to the completion time and the integrity of the solution, scores are given|

5. Summary

As a training base for security talents, colleges and universities should construct the campus cyber range scientifically and reasonably, which not only meets the basic functions of the cyber range, but also promotes the application effectiveness of the cyber range. This paper puts forward three training latitudes of campus cyber range, that is the basic latitudes based on safety knowledge and practical training, the challenge latitudes based on safety application and the role confrontation latitudes based on team dynamic training. With these three dimensions to jointly drive the training of network shooting range, we will achieve the goal of developing Cyberspace security talents more comprehensively.

References

[1] Fang Binxing, Jia Yan, Li Aiping, Zhang Weizhe. Cyber Ranges : state-of-the-art and research challenges [J]. Journal of Information Security, 2016, 3:1-9.
[2] Li Jianhua. Innovation and Practice of Pluralistic and Multi-level Cyber Security Personnel Training [J]. Information Security Research, 2018, 4 (12): 1073-1082.
[3] Han Weiguo, XU Mingdi. Construction Method of cyberspace-Oriented Network Range [J]. Computer and Mathematical Engineering, 2015, 8: 1465-1470.
[4] Cheng Jing, Lei Jing, Yuan Xuefen. Construction and development of national cyber range [J]. Journal of China Academy of Electronic Sciences, 2014 (5): 446-452.
[5] Li Qiuxiang, Hao Wenjiang, Li Cuicui. Present Situation and Enlightenment of Foreign Network range Technology [J]. Information Network Security, 2014 (9): 63-68.
[6] Jiang X, Wang X, Xu D. Stealthy malware detection and monitoring through VMM-based “out-of-the-box” semantic view reconstruction[J]. Acm Transactions on Information System Security, 2010, 13(2):128-138.