

Empirical Cases of Competency Measurement and Evaluation for Information Security Trainees

1. Background and Overview

This empirical study was conducted as part of a research project aimed at developing the **Cloud-based Cyber Training Range (K-CR)** and the **Cyber Training Scenario Description Language (K-SDL)**. The main goal of the project is to build an integrated platform for cybersecurity competency development and risk management throughout the entire cycle. In particular, this study focused on **measuring the competency improvement of trainees through practical training**.

The empirical exercise was carried out using the virtual environment of the ITRAINING platform, targeting real-world trainees in information security education programs.

2. Objectives and Methods

The primary objective of the empirical study was to **measure the effectiveness of cybersecurity training**. To this end, identical sets of 30 quiz questions were administered before and after the training, within a limited time, to evaluate changes in performance.

The participants were **77 students (undergraduate and graduate level)**, divided into three groups: Malware (24), Network (28), and Privacy (25).

Additionally, post-training surveys were conducted to gather feedback on usability, functionality, performance, data protection, business feasibility, and overall user experience.

3. Analysis Results

(1) Quiz Evaluation

- **Quiz Topics:** IP and network basics, OS security (Windows/Linux), authentication and encryption, web vulnerabilities, network scanning tools (e.g., Nmap), web logs, firewalls and access control.
- **Improved Areas:** System permission settings, IP address classes, prevention of web directory listing.
- **Areas Requiring Improvement:** File upload vulnerability handling, web shell execution prevention, Linux file permission settings (chmod).

Overall, quiz results showed improvement in most areas, but some critical vulnerabilities still required attention.

(2) Satisfaction Survey

- A notable finding was that some students who showed a **decline in test performance still reported high satisfaction levels**.
 - This highlights the limitations of relying solely on satisfaction scores to measure training effectiveness.
 - **Key feedback from trainees included:**
 - Need for theory-first instruction prior to hands-on practice.
 - Usability issues with VM and platform environments.
 - Lack of contextual explanations for commands (“why this command is used”).
 - Suggestions for step-by-step guidance and hints during exercises.
-

4. Integrated Analysis

Trainees were divided into three groups based on their performance improvement: top 30%, middle 40%, and bottom 30%.

- **Top 30% (23 trainees):** Average improvement of +6.22 points; high satisfaction levels but not the highest in all categories.
- **Middle 40% (31 trainees):** Average improvement of +2.23 points; recorded the highest scores in usability, functionality, and business feasibility.
- **Bottom 30% (23 trainees):** Average decline of -2.30 points; lowest scores in all categories.

The results indicate that the common assumption—“higher performance leads to higher satisfaction”—does not always hold true.

5. Conclusions and Recommendations

From the empirical results, several conclusions and recommendations emerged:

1. Strengthen Pre-training Instruction

- Novice trainees without sufficient prior knowledge tend to experience poor performance when tasks are presented directly.
- A mandatory theory module (approx. 30 minutes) should be provided before hands-on practice.

2. Improve Training Content

- Move beyond simple command-based guides to provide **conceptual explanations** of why commands are used.
- Benchmark the training materials and difficulty adjustment methods from the Network group, which achieved the best outcomes.

3. Enhance Platform and Operations

- Address usability issues in VM environments (e.g., keyboard errors, lack of clipboard support).
- Provide onboarding guides before practice to reduce technical obstacles.
- Revise satisfaction surveys to include improvement-oriented questions such as “Was the theoretical explanation sufficient?”.

6. Final Remarks

This empirical study demonstrated that **quiz performance and satisfaction levels do not always align** in information security training. It also highlighted that pre-training instruction, deeper content design, and platform improvements are key factors to enhance the effectiveness of cybersecurity education.