Proposal to Integrate Capture the Flag (CTF) Training into Our ACM Curriculum

December 5, 2024

Dear Professor,

I hope this message finds you well. I am writing to propose the integration of Capture the Flag (CTF) competitions into our cybersecurity curriculum. Based on extensive research, including findings from ENISA, MIT Lincoln Laboratory, and Adelphi University, CTFs offer hands-on experience, promote engagement, and address crucial industry skill gaps in cybersecurity education.

I. Understanding CTF Competitions

CTF competitions are structured as gamified simulations of cybersecurity scenarios. Participants solve challenges such as cryptography, reverse engineering, web security, and forensics to locate and exploit vulnerabilities. These competitions are often categorized into three formats: Jeopardy-style, Attack-Defense, and hybrid formats. As ENISA highlights, each format develops unique skill sets—ranging from theoretical problem-solving to practical, real-world exploit execution [**?**].

II. Educational Benefits

1. Practical Skill Development

The studies reviewed emphasize the real-world applicability of CTF competitions. According to Leune and Petrilli, students reported a marked increase in self-confidence and practical skills after participating in CTF exercises. For example, they gained hands-on experience with vulnerabilities such as unpatched software, default configurations, and privilege escalation [?]. Similarly, the Lawrence Livermore National Laboratory found that static and dynamic CTF challenges directly mirror real-world security scenarios, preparing participants for industry demands [?].

2. Enhanced Engagement

Gamification significantly boosts motivation and retention in cybersecurity education. Leune et al. argue that the gamified environment addresses disengagement caused by traditional lecture methods. The competitive, interactive nature of CTFs keeps students actively involved while fostering critical thinking and problem-solving skills [?].

3. Teamwork and Communication Skills

As Davis et al. note, team-based CTFs encourage collaboration among participants with diverse expertise, reflecting the interdisciplinary nature of real-world cybersecurity teams [?]. This teamwork develops soft skills such as communication and strategic thinking, essential for professional success.

III. Industry Recognition and Career Advancement

1. Skill Validation and Visibility

CTFs provide tangible evidence of a participant's skills. Success in prestigious competitions like DEF CON's CTF or Carnegie Mellon's picoCTF is often recognized as an indicator of technical competence. These achievements enhance employability and open doors to advanced career opportunities [?, ?].

2. Professional Networking

Participation in global competitions introduces students to industry leaders, potential employers, and peer networks. As ENISA's report highlights, CTFs serve as a bridge between academia and industry, creating pathways for mentorship and collaboration [?].

3. Career Impact

The practical experience gained from CTFs aligns closely with job roles such as penetration testing, OSINT analysis, and incident response. Taylor emphasize that CTFs bridge the gap between theoretical education and industry requirements, addressing critical skills shortages in cybersecurity [?].

IV. Insights from Research

1. Format and Diversity of Challenges

ENISA and Davis et al. discuss how different CTF formats—such as Attack-Defense and Jeopardy—cater to varying skill levels. Jeopardy-style events are ideal for beginners, offering independent challenges, while Attack-Defense models simulate real-time adversarial environments, enhancing defensive and offensive skills [?, ?].

2. Cost-Effectiveness and Accessibility

Taylor identify cost and accessibility as barriers to wider adoption of CTFs. However, open-source platforms like picoCTF provide scalable solutions for educational institutions. By leveraging such resources, we can minimize costs and maximize student participation [?].

3. Long-Term Educational Value

ENISA's report underscores the long-term benefits of integrating CTFs into curricula. Retrospective analysis of events, release of challenge solutions, and detailed write-ups contribute to the broader cybersecurity community by sharing knowledge and fostering continuous learning [?].

V. Proposed Implementation

- **Curriculum Integration**: Incorporate CTFs into ACM's training programs
- **Dedicated CTF Teams**: Establish student teams to participate in national and international competitions.
- **Hosting Events**: Organize local and national CTF events to develop a culture of hands-on learning and collaboration.

- **Resource Utilization**: Leverage open-source platforms like picoCTF, Hack the box and Try hack me to minimize setup costs while providing high-quality challenges.

Conclusion

The research highlights the transformative potential of CTFs in cybersecurity education. By integrating CTFs into our curriculum, we can provide students with practical experience, foster engagement, and enhance their career prospects. This initiative will not only enrich our academic offerings but also establish our institution as a leader in cybersecurity education.

Thank you for considering this proposal.

References

1. Taylor, C., Arias, P., Klopchic, J., Matarazzo, C., & Dube, E. (2021). *CTF: State-of-the-Art and Building the Next Generation.* ASE Conference.

2. Davis, A., Leek, T., Zhivich, M., Gwinnup, K., & Leonard, W. (2021). *The Fun and Future of CTF.* MIT Lincoln Laboratory.

3. Leune, K., & Petrilli, S. (2017). *Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education.* SIGITE.

4. ENISA (2021). *CTF Events: Contemporary Practices and State-of-the-Art.* `https://www.enisa.europa.eu`.

5. DEF CON Official Website. `https://defcon.org/ctf`.

6. Carnegie Mellon University CyLab. *picoCTF.* `https://picoctf.org`.