Peer Mentorship in Live CTF Competitions: The CTF Academy Experience

Pulkit Singh Singaria
Arizona State University
Tempe, AZ, USA
x3ero0@asu.edu

Connor Nelson
Arizona State University
Tempe, AZ, USA
connor.d.nelson@asu.edu

Yan Shoshitaishvili
Arizona State University
Tempe, AZ, USA
yans@asu.edu

Abstract

Capture the Flag (CTF) competitions are a hands-on way to learn cybersecurity, but they are notoriously difficult for beginners to approach. Educational CTF platforms teach the fundamentals of binary exploitation, reverse engineering, web security, and cryptography, but a gap remains between where these platforms end and where live competitions begin. Skills like investigating unfamiliar software and developing working exploits under time pressure are hard to teach from a fixed curriculum.

We present CTF Academy, a near-peer mentoring program that places experienced players (mentors) and learners (mentees) on the same team during live, elite CTF competitions rather than in a classroom. We describe its design, its mentoring and competition workflow, and a model for reproducing it elsewhere. We surveyed mentees and mentors about their confidence, learning, and participation. All 18 responding mentees found the Academy useful to their learning and reported that it increased their participation in CTF events, and 17 of 18 said their confidence in analyzing unfamiliar challenges and software had grown. Beyond technical skills, its main effect was on the *non-technical* barriers, such as intimidation, isolation, and not knowing where to begin, that keep capable learners out of CTFs.

CCS Concepts

• **Applied computing** → **Collaborative learning**.

Keywords

Capture the Flag, Education, Competition, Experience Report

ACM Reference Format:
Pulkit Singh Singaria, Connor Nelson, and Yan Shoshitaishvili. 2027. Peer Mentorship in Live CTF Competitions: The CTF Academy Experience. In *Proceedings of the 58th ACM Technical Symposium on Computer Science Education V.1 (SIGCSE TS 2027), February 17–20, 2027, Sacramento, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3857222.3860195

1 Introduction

Capture the Flag competitions (CTFs) were originally developed by hackers to challenge other expert hackers, giving them a space to test themselves against niche, advanced, and cutting-edge technical concepts. Such "elite" (focused on competition) CTFs are a valuable part of an experienced hacker's toolkit for sharpening real-world technical skills. CTFs provide continual training to think like an attacker, develop zero-day exploits in real-world software [10], or anticipate attacker behavior and become better hackers.

Unfortunately, the same features that make elite CTFs valuable for experts also make them notoriously difficult for novices to approach [33, 34]. To resolve this, educators developed introductory platforms designed to adapt CTFs for *education*, making practical learning challenges more accessible to novices [5, 11, 18, 20, 23, 30]. At face value, these platforms enable practical CTF-style learning while resolving many of the aforementioned accessibility issues plaguing elite CTFs. Over the last several years, the use of "educational" (focused on learning) CTFs has risen in popularity and has been adopted in cybersecurity education curricula worldwide [24].

However, this situation leaves a pedagogical gap: we observe three underlying causes that keep students of educational CTFs from advancing to elite ones. The first cause is *technical*: because educational CTFs primarily optimize learning and accessibility, they rarely explore the cutting-edge concepts and complex scenarios of elite CTFs, where new techniques often appear well before they reach courses and online materials [13]. Nor do they exercise skills such as performing under time pressure [13, 23, 32]. The second is *confidence*: even well-prepared students find elite CTFs intimidating, with ambiguous challenges and little feedback beyond whether a flag is correct [23, 33]. The third is *social*: elite CTFs are team competitions, but educational platforms are largely individual experiences, leaving students without a team or community through which to participate [32].

This paper presents our attempt to bridge this gap between educational and elite CTFs through the creation of the *CTF Academy*, a mentoring program where experienced players of elite CTFs (mentors) are paired with students from educational CTF platforms (mentees) to facilitate the latter's participation in elite CTFs. We carefully designed the CTF Academy to address each of these three causes. Over the course of 20 months, the CTF Academy paired 120 mentees with 22 mentors through their participation in 36 elite CTFs (as well as four practice events).

We carried out two surveys to measure our impact on mentees. Our initial survey, 8 months into the Academy, revealed strong early engagement (14 of 15 responding mentees found the Academy useful to their learning, and 14 of 15 reported that it increased their CTF participation) but lingering hesitancy: only 7 of 15 felt confident competing independently. In our follow-up survey of 18 mentees, 17 reported that CTF Academy increased their confidence in approaching unfamiliar CTF challenges, and 15 credited the CTF Academy with improving their ability to learn new cybersecurity concepts. Throughout our study, 12 mentees "graduated" to join elite CTF teams as elite members in their own right. Our study



This work is licensed under a Creative Commons Attribution 4.0 International License.
SIGCSE TS 2027, Sacramento, CA, USA
© 2027 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-3075-7/2027/02
https://doi.org/10.1145/3857222.3860195

also found an unexpected effect: we allowed our mentees to choose to work primarily collaboratively (with other mentees *and* mentors) or primarily individually (without other mentees, but with a mentor). Collaborative mentees were less confident about competing without the Academy than individual mentees. Finally, we discuss implications of our experience and present a clear roadmap to reproduce the CTF Academy at other institutions.

2 Background & Related Work

Elite CTF competitions are informal, hands-on settings for hackers to practice technical cybersecurity skills. Large-scale analysis of CTF writeups shows that these challenges span tasks such as web exploitation, password cracking, network compromise, cryptography, reverse engineering, forensics, and pwn-style system exploitation. The same analysis maps CTF challenge topics onto the CSEC2017 cybersecurity curricular guidelines, showing that CTFs exercise skills represented across the CSEC2017 Knowledge Areas, especially data, connection, and system security [28].

Technical Gap. Beginners find CTFs difficult because CTFs often sit near the open-ended end of the cybersecurity exercise spectrum. Prior work contrasts prescriptive exercises, where learners follow step-by-step instructions, with CTF-style activities that provide little guidance on how to proceed and require learners to make independent progress [34]. Other work similarly notes that CTFs can be too difficult for beginners, intentionally ambiguous, and limited in the feedback they provide beyond whether a submitted flag is correct [23, 33]. Studies of beginners working on vulnerability-discovery and binary exploitation exercises show the same problem in more detail. Novices often do not know what to look for, misread online resources, and fail to connect a tool's output to the task in front of them. They often get stuck in unproductive trial-and-error loops without a clear goal [19].

Confidence Gap. Prior work also suggests that the competitive and public nature of CTFs can make them intimidating for novices. CTF assignments and competitions may discourage or alienate some students, especially beginners, when challenges are too difficult or progress is unclear [26, 33]. Nelson and Shoshitaishvili argue that traditional CTF challenges are often designed to be challenging rather than pedagogically effective, which can make them too difficult and intimidating for novice learners [23]. Co-curricular CTF work reaches a similar conclusion that CTFs can be intimidating, but scaffolded, low-risk, and group-based activities with instructional support can help students become less apprehensive about CTF participation [11].

Community Gap. CTF Academy is also motivated by work showing that security learning is often sustained through teams and communities rather than only individual practice [15]. In a review of online vulnerability-discovery exercises, Votipka et al. identify peer learning as part of a learning-conducive environment, arguing that group settings can enable mentoring from senior students, peer brainstorming, and encouragement when learners are stuck [32]. Classroom CTF work likewise reports students working in small groups, dividing tasks, assisting one another, and learning together [11]. More sustained cybersecurity education communities show the same pattern at larger scale: pwn.college uses Discord for asynchronous support, peer mentorship, and collective problem solving, while an IT-security talent program frames student development as a community of practice built around shared activities, CTF team participation, and hands-on knowledge sharing [3, 24]. These results motivate CTF Academy's emphasis on a team-based community where challenge attempts, partial progress, failed approaches, and explanations become shared learning resources.

Several other systems have used mentorship or peer support in cybersecurity education to bridge these gaps, but they focus on educational CTFs, not elite ones. Prior work has studied CTFs as classroom exercises and peer mentoring in cybersecurity education [4, 6, 16, 21, 33]. Mirkovic et al. adapted a novice-oriented Class Capture-the-Flag exercise by forming balanced teams and pairing each team with one or two mentors who helped participants understand and conduct tasks during a controlled workshop CTF [21]. Janeja et al. studied peer mentoring in cybersecurity classes, pairing introductory Information Systems students with students in an upper-level cybersecurity elective through monthly small-group conversations and presentations [16].

CTF Academy combines the elements that prior work has studied separately: hands-on CTF learning, scaffolded support for open-ended security challenges, near-peer mentorship, and team-based learning communities. Unlike general peer-mentoring programs, the mentoring occurs while participants are actively competing in live CTFs. Unlike self-paced platforms, CTF Academy moves peer support into time-bounded external competitions where mentors and mentees work under the same team, solve the same challenges, and share the same community space. To our knowledge, this combination of near-peer mentorship with repeated live external CTF participation has not been previously studied.

3 The CTF Academy

Figure 1 frames CTF Academy along a guidance-independence spectrum. At one end we have tutorials, write-ups, classes, and structured exercises that provide substantial guidance but limit the independent discovery required from learners. At the other end we have elite CTFs and real-world security work that require learners to deal with ambiguity, incomplete information, and little immediate feedback. Weiss et al. describe a similar situation in cybersecurity exercises, contrasting prescriptive step-by-step labs with open-ended CTF-style activities and arguing that students benefit from a middle ground that preserves discovery while still providing sufficient guidance [34].

Design Goals. CTF Academy was designed for learners who had already gained some technical background through educational platforms but who had not yet developed habits for participating in live CTFs. Those platforms provide a structured path through topics such as binary exploitation, reverse engineering, web security, and cryptography. Elite CTFs place the same learners in a different setting where challenges are time-bounded, ambiguous, uneven in difficulty, and solved by teams working in parallel.

CTF Academy was designed with the following goals in mind:

- **Ease the transition to open-ended challenges.** CTF Academy gives mentees a setting where they can attempt CTF problems with little built-in guidance while mentors remain available to nudge them toward productive next steps.

- **Build confidence and reduce intimidation.** By playing alongside supportive peers and experienced players, students can build confidence that they are capable of solving difficult problems with enough time, effort, and guidance.
- **Foster a team-based community.** Because CTFs are usually team competitions, the Academy introduces students to collaborative hacking in a team setting, in contrast to the mostly individual learning they experienced on platforms such as pwn.college.

Participants and Recruitment. CTF Academy started off in the Discord [9] community of pwn.college [24], a popular cybersecurity education platform, which gave the program access to a wide variety of learners. We first recruited students who had completed the biggest milestone and had demonstrated technical proficiency in system exploitation, reverse engineering, cryptography, web security, and other courses that the platform offered, but many had limited experience with live competitions. As the program matured, we gradually opened participation to learners earlier in their journey through the platform's milestones. Each new cohort increased the diversity of players in the Academy: our early participants focused more on binary exploitation and reverse engineering, but later cohorts brought in more players drawn to web, cryptography, and miscellaneous challenges.

Eventually, the only durable requirement for joining as a mentee was being interested in playing CTFs. This decision was important because CTF Academy was not structured as a course with grades, prerequisites, or scheduled class meetings. Learners joined from different institutions, time zones, and levels of formal education. The program therefore needed to support both learners who wanted occasional exposure to CTFs and learners who wanted a pathway toward regular team participation.

Mentor Model. Mentors are near-peers who play in the same competitions as the mentees. They are not instructors or teaching assistants, just CTF players who are a little further along in their cybersecurity journey. As more experienced teammates, they model how to approach a challenge, help learners decide what to try next, and share competition practices that are difficult to teach in a self-paced exercise. A mentor may be an undergraduate student, graduate student, or security professional; what matters is their practical CTF skill and willingness to guide less experienced players.

We recruited mentors through three channels. First, we used an existing institutional CTF team as an initial mentor pool. Second, we invited other competitive teams to participate. Third, we published a call for mentors and shared it through social media and community channels. The call explained how the Academy operated and why mentoring could benefit both learners and mentoring teams. For mentees, the benefit was access to experienced teammates in elite competitions and for teams, the benefit was an easy way to meet interested CTF players who might later become good fits for their elite teams.

Competition Workflow. For each event, mentors selected candidate competitions from CTFtime [7]. Selection depended primarily on mentor availability, expected difficulty, event reputation, and category coverage. We generally avoided competitions that were too easy to be useful for mentors or too difficult for newer learners to make progress. In practice, this meant favoring medium-difficulty events or events run by organizers with a strong reputation in the CTF community.

When the Academy and a mentoring team participated in the same CTF, they played under a single team name. This was both pedagogically and operationally important. Pedagogically, mentees could see their work contribute to a real leaderboard position. Operationally, a unified team avoided cross-team collaboration problems that many CTF rules prohibit. Within that team, mentors balanced two roles: they worked on challenges themselves, and they helped mentees who were stuck.

Mentorship happened both synchronously and asynchronously. In-person help was always synchronous and most of the help on Discord was asynchronous because mentors were not always online. Mentees posted details of their approach, commands, traces, partial scripts, or any other artifact in a challenge-specific post on the forum, and mentors responded when they came online. This asynchronous pattern was necessary because the Academy included participants across time zones.

The core mentoring unit was the challenge channel. A channel gave participants a shared place to record observations, avoid duplicated effort, and ask for help without losing the history of the attempt. Mentors tried to keep hints contextual rather than solution-like. A typical interaction might involve helping a learner identify the relevant file, interpret tool output, choose a debugging strategy, or decide whether a result was a dead end. When needed, a mentor could briefly demonstrate a technique, such as using a debugger, writing a small script, or setting up an analysis workflow. The goal was to make the learner's next step possible while preserving the open-ended nature of the challenge.

Collaborative solving also exposed learners to alternative technical approaches. Players may attack the same challenge differently: one might step through a binary in `gdb`, another might automate

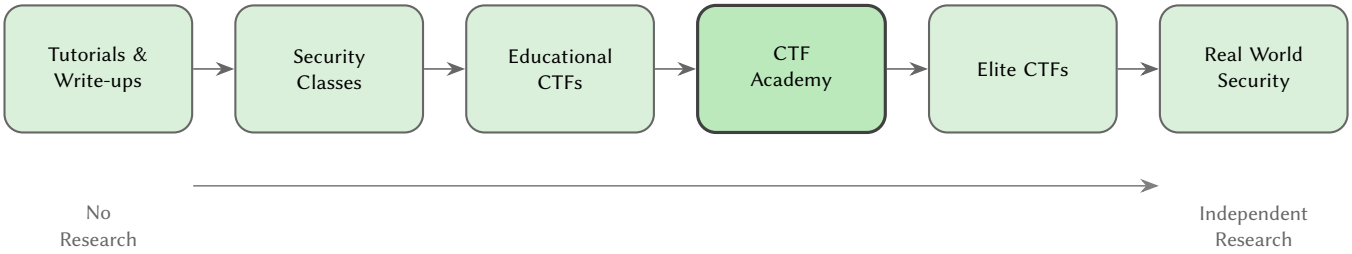


Figure 1: CTF Academy on the learning spectrum from educational security exercises to elite CTFs.

interaction with a script, and a third might use features of IDA Pro [14], Binary Ninja [31], or `angr` [29]. This kind of side-by-side comparison is one reason the Academy emphasizes team participation rather than only individual practice.

Academy-Hosted Events. We used the DOJO [22] to host several events for CTF Academy with the goal of increasing engagement and practice on different kinds of challenges. These events were designed to be less competitive than the elite CTFs but have just enough friendly competition among the mentees to still keep it fun. There were no prizes for coming first other than bragging rights.

Graduated Mentees. During the operation of CTF Academy, a few students started standing out among others. These were the students that showed up consistently, engaged in discussion and solved CTF challenges. We allowed our mentors to choose those well-performing mentees to invite them to their elite CTF team and "graduate" them from the CTF Academy. The mentors described that they were looking for the ability to pursue answers independently without constantly requiring guidance.

LLM Policy of CTF Academy. In the past few years, large language models have become really good at doing security tasks whether that is doing code review to find security bugs or create patches [8]. Consequently, they have also become really good at solving difficult CTF problems [1, 12].

Because of this, we saw many elite CTFs such as DEF CON CTF [2], RITSEC CTF [27], and Kalmar CTF [17] adapting to the rising ability of LLMs by discouraging or sometimes even banning the usage of fully autonomous agentic workflows in these competitions.

We realized that for the purposes of CTF Academy, learning matters more than winning; therefore, we prohibited agentic workflows in the Academy. Use of non-agentic LLMs was still allowed for research purposes.

4 Evaluation

Data and Method. To evaluate the experience of the students as it unfolded, we conducted two short, IRB-exempt surveys: an initial survey in July 2025 and a follow-up survey in July 2026. We invited students to fill out the survey and describe their experiences with CTFs both before and after enrolling in CTF Academy, including their level of confidence, the impact of mentorship on them, and the challenges they faced.

By the time of the follow-up survey, CTF Academy had run for 20 months and participated in 36 elite CTF events, organized four practice events, had 120 mentees, 22 mentors split among two elite CTF teams, solved 444 challenges, and 12 mentees "graduated" to partnered elite CTF teams. In our initial survey, we received 15 responses from mentees and 3 responses from mentors and in our follow-up survey we received 18 responses from mentees and 3 responses from mentors. To complement the survey responses, we also measured event-level participation from Discord challenge threads and Academy-hosted event logs. For elite CTF events, we counted a mentee as active if they sent at least one message in a challenge thread during the event window.

Participation. The same activity logs also show a long-tailed pattern of repeat participation. As shown in Figure 3, many observed participant identities appeared in only one or two counted CTFs, while a smaller recurring group participated across many events.

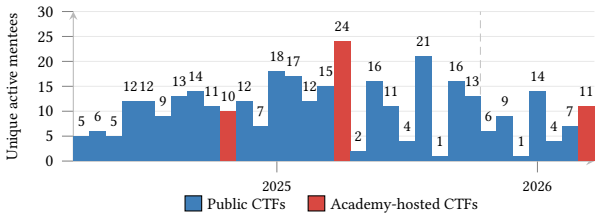


Figure 2: Unique active mentees per CTF event, ordered chronologically.

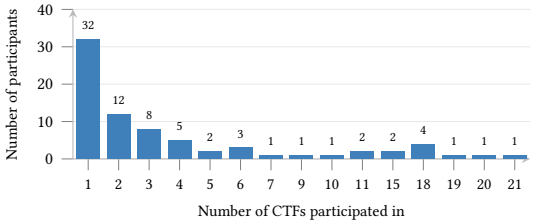


Figure 3: CTF events each participant was active in ($N = 76$ participants).

Technical Preparation. When asked how well pwn.college had prepared them for CTF competitions, 16 of the 18 respondents agreed and the other 2 were neutral. This strong agreement suggests that the players felt well-equipped in core skills like binary exploitation, reverse engineering, web security, and cryptography. However, they felt less prepared to work under time pressure and to navigate unfamiliar challenges independently, and this is backed up by their open-ended responses. 13 of 18 students agreed when asked if the added time pressure in live CTF events helped develop skills that self-paced educational platforms do not.

Usually, during an elite CTF, the goal is to get the flag in the fastest way possible. The right way to solve a challenge may not be the fastest way.

Overall Experience. The Likert responses in Figure 4 paint a clearer picture of the overall experience of the students with CTF Academy. All 18 participants agreed that the CTF Academy was useful to their learning in one way or another, 15 of 18 reported that CTF Academy had improved their ability to tackle and learn new topics on their own, and 17 of 18 said their confidence in approaching unfamiliar CTF challenges increased because of CTF Academy.

Similarly, 16 of the 18 participants said that they looked forward to upcoming CTFs with CTF Academy, and all 18 reported that CTF Academy had already driven them to participate in more CTFs than they otherwise would.

Skills Beyond CTFs. The participants reported that they had learned a few skills that also helped them outside the context of CTFs, such as collaborating with other people, learning new things quickly, problem-solving ability, research skills, and fast-paced communication with teammates.

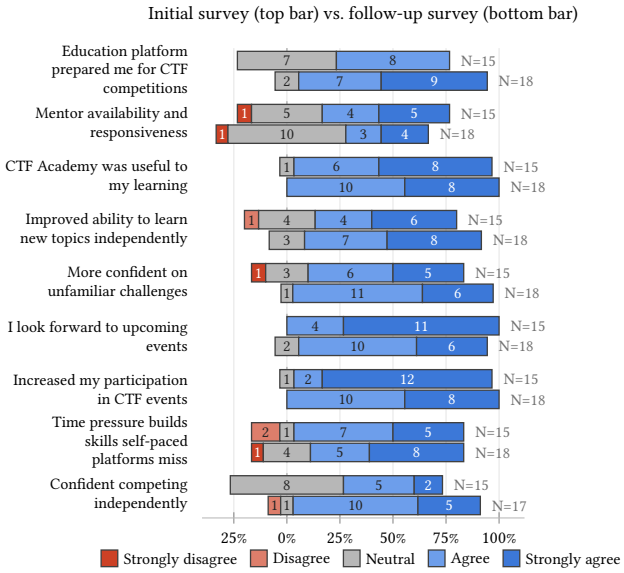


Figure 4: Mentee responses to the Likert statements asked in both survey rounds: the initial survey (top) vs. the follow-up survey (bottom).

> *"General problem-solving ability, improved ability to read documentation, some knowledge about esoteric languages and finding niche stuff on the internet."*

In the follow-up survey, we converted these recurring themes into Likert statements to measure how widely they were shared. 15 of 16 agreed that CTF Academy improved skills that helped them beyond CTFs and 15 of 18 mentees agreed that watching peers and mentors work exposed them to new tools, techniques, and problem-solving approaches that they otherwise did not know about. 15 of 17 agreed that CTF Academy gave them opportunities to practice skills that structured platforms do not usually emphasize, such as working under time pressure, analyzing large and unfamiliar software and quickly recognizing when they were stuck and how to get unstuck.

This transfer also runs upward within the competitive scene itself. Of the 11 mentees to whom the question applied, 7 agreed that the skills they practiced in CTF Academy helped them contribute in elite events such as DEF CON CTF [2], which is considered the "World Championship" of CTFs, and CSAW CTF [25], a prestigious elite event for college hackers.

Confidence and Collaboration. Many students explained that before joining CTF Academy they often felt intimidated and overwhelmed when they hit a roadblock on a challenge. With no teammates or mentors to discuss ideas with, they eventually gave up solving the challenges. Many did not know about CTFs or how to find a team. CTF Academy allowed these players to play CTFs with like-minded people and also helped them feel less intimidated.

Open-ended responses also showed that mentees did not all want the same form of collaboration. Some preferred to solve with others in real time, while others preferred to work alone first and ask for help only when blocked. As a descriptive check, we split mentee responses by the working style they reported preferring. Figure 5 shows that both groups reported increased confidence in tackling unfamiliar CTF challenges, but the individual-working group reported higher confidence about joining other teams and competing without CTF Academy support. This suggests that confidence in skills does not automatically translate to confidence to compete independently.

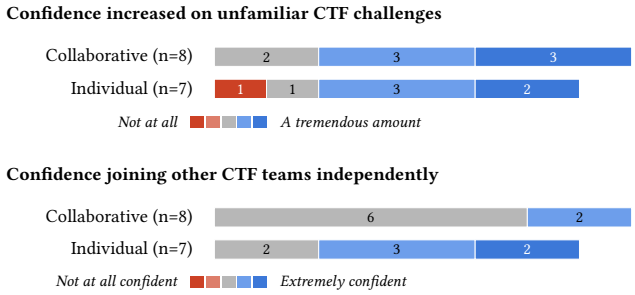


Figure 5: Self-reported confidence by preferred working style. Bars show absolute counts from 2025 mentee respondents who preferred working collaboratively or individually.

Mentor Perspective. Across both survey years, mentors expressed their willingness to continue mentoring. In 2025, however, mentor responses revealed a structural issue: mentors were also active competitors with their own CTF teams, and playing for CTF Academy, a team separate from their own, made them feel disconnected from their normal experience. One mentor described it as "playing for a different team," while another noted that it was "not super clear and ethical to help" when mentors were also playing the same event under a different account. In response, in 2026 we changed the participation model so that mentees played alongside the mentoring team under its team name. This aligned the mentor and mentee experience: for mentees, nothing actually changed, while the mentors could now support learners without feeling separated from their own team's identity.

In 2025, 9 of 15 mentees reported mentor availability and responsiveness, 5 remained neutral, and 1 gave a low rating. In 2026, 7 of 18 mentees reported mentors were available and responsive when needed, 10 were neutral, and 1 strongly disagreed. This was partly because the mentee-to-mentor ratio grew: 59 mentees and 17 mentors in 2025, but 120 and 22 in 2026. It may also be because, as a mentor reported, "It'd be nice if they [reached out] for help or asked questions more frequently."

Academy-Hosted Events. In total, we organized four events, each with its own format. We ran a jeopardy-style Academy CTF, a non-competitive crackmes workshop that introduced mentees to a variety of reverse engineering challenges, an attack-defense CTF, and a second jeopardy-style competition in which mentees designed challenges for one another.

The most notable was a 24-hour attack-defense CTF, which drew 24 unique mentees, the largest spike in Figure 2. Mentees were split into teams of four and had to set up a vulnerable server and their own tooling for monitoring network traffic and exploiting other teams.

> *"[Attack & Defense] CTF was the best. Spent [the] whole night just trying to extinguish different fires and keep our points."*

The survey responses show that mentees agreed that these competitions felt lower pressure and made the Academy feel more like an active community (13 of 16 for both).

5 How to Make Your Own CTF Academy

CTF Academy is intended to be reproducible without requiring the exact institutional context in which it began. The core requirements are a learner community, a pool of experienced CTF players willing to mentor, a shared communication space, and a regular cadence of live CTF participation. Institutions with an existing cybersecurity club or CTF team can start from that community. Institutions without one can recruit from security courses, student organizations, regional CTF groups, or online learning communities.

The most important design choice is to treat the Academy as a mentored team, not as another course. Learners should be able to join because they are interested in CTFs, even if their technical background varies. Mentors should be selected for practical CTF experience and willingness to guide beginners, not for formal instructional roles. This keeps the program close to authentic CTF practice while still making it safer for beginners to ask questions and expose partial progress.

We recommend the following replication process:

(1) **Identify an initial mentor pool.** Start with experienced players from a local CTF team, cybersecurity club, advanced security course, or regional CTF community. A small but reliable mentor group is more useful than a large group that rarely participates.
(2) **Recruit learners around motivation, not only prerequisites.** Prior technical preparation helps, but the program works best when learners are selected for interest in CTF participation and willingness to work with peers.
(3) **Create a shared communication space.** Use a persistent platform such as Discord, Slack, Matrix, or a course-hosted equivalent. Create role-separated spaces for mentors and learners, plus challenge-specific channels during each CTF.
(4) **Pick CTFs deliberately.** Select competitions based on mentor availability, expected difficulty, category coverage, and organizer reputation. Events should be hard enough to expose learners to real CTF practice but not so hard that beginners have no viable path to contribution.
(5) **Play under a rule-compliant team structure.** Before each event, decide whether the Academy and a mentoring team will play under one unified team name. This avoids cross-team collaboration problems and makes it clear which participants may share work.
(6) **Use challenge channels as the mentoring unit.** Ask learners to post observations, failed attempts, scripts, traces, and questions in the channel for the relevant challenge. This gives mentors enough context to provide targeted hints without turning the challenge into a walkthrough.
(7) **Build a path from learner to mentor.** As learners gain experience, invite them to help newer participants. This creates a more sustainable mentoring pool and reinforces the peer-learning model.

Programs adopting this model should also plan for record keeping. At minimum, organizers should track the events played, number of active mentors and learners, challenge solves, mentor availability, and recurring coordination problems.

6 Limitations

As an experience report, our evidence has clear limits. The surveys were voluntary, and only 18 of 120 mentees responded to the follow-up (15 of 59 to the initial survey), so mentees who found CTF Academy engaging were likely overrepresented. Survey outcomes such as confidence are self-reported perceptions, not measurements of skill. Finally, programs adopting the CTF Academy model may see different results depending on their access to elite teams willing to mentor and to an existing learning community to recruit from.

7 Future Work

We observed that mentees and mentors had difficulty connecting with each other. A mentee stuck on a challenge did not always know which mentor to turn to, and available mentors were not always aware that help was needed. We plan to fix this by improving the Academy's structure so that each mentor's areas of expertise are visible to everyone, allowing mentees to know exactly which mentor to ask for help on a specific challenge. We have begun to explore the use of mentor-assistive AI agents to detect confused mentees, but have not yet had promising results in this direction, and more work is needed to determine its feasibility.

8 Conclusion

This paper presented CTF Academy, a near-peer mentoring model that bridges the gap between educational cybersecurity platforms and elite CTF competitions. Rather than softening the competitions to fit beginners, the Academy places experienced players and learners on the same rule-compliant teams in live events, preserving the open-ended nature of the challenges while keeping guidance within reach at the moment a learner gets stuck. Responding mentees reported coming away more confident, many found a community they belong to, and 12 mentees have since graduated to compete with elite teams in their own right.

Acknowledgments

This work would not have been possible without the vibrant enthusiasm of the pwn.college community, the mentoring teams who welcomed our mentees, and the wider CTF community, as well as the generous support of the Department of Defense, including DARPA (HR001124C0362); thank you.

References

[1] Anthropic Frontier Red Team. 2025. Claude Is Competitive with Humans in (Some) Cyber Competitions. https://web.archive.org/web/20261027170140/https://www.anthropic.com/research/cyber-competitions. Online; accessed November 12, 2026.

[2] Benevolent Bureau of Birds. 2026. DEF CON CTF Qualifier 2026. https://web.archive.org/web/20260614042605/https://bbbctf.com/. Online; accessed July 3, 2026.

[3] Levente Buttyán, Márk Félegyházi, and Gábor Pék. 2016. Mentoring Talent in IT Security: A Case Study. In *2016 USENIX Workshop on Advances in Security Education (ASE '16)*. USENIX Association, Austin, TX, USA. https://www.usenix.org/conference/ase16/workshop-program/presentation/buttyan

[4] Martin Carlisle, Michael Chiaramonte, and David Caswell. 2015. Using CTFs for an Undergraduate Cyber Education. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '15)*. USENIX Association, Washington, D.C., USA. https://www.usenix.org/conference/3gse15/summit-program/presentation/carlisle

[5] Peter Chapman, Jonathan Burket, and David Brumley. 2014. PicoCTF: A Game-Based Computer Security Competition for High School Students. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '14)*. USENIX Association, San Diego, CA, USA. https://www.usenix.org/conference/3gse14/summit-program/presentation/chapman

[6] Stephen V. Cole. 2022. Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class. In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1* (Dublin, Ireland) *(ITiCSE '22)*. Association for Computing Machinery, New York, NY, USA, 470–476. doi:10.1145/3502718.3524806

[7] CTFtime. 2026. CTFtime: All about CTF (Capture The Flag). https://web.archive.org/web/20260621175624/https://ctftime.org/. Online; accessed July 3, 2026.

[8] DARPA. 2025. AI Cyber Challenge (AIxCC). https://web.archive.org/web/20260624234851/https://aicyberchallenge.com/. Online; accessed July 3, 2026.

[9] Discord. 2026. Discord. https://web.archive.org/web/20260703200305/https://discord.com/. Online; accessed July 3, 2026.

[10] Chris Eagle and John L. Clark. 2004. Capture-the-Flag: Learning Computer Security Under Fire. In *Proceedings of the Sixth Workshop on Education in Computer Security (WECS6)*. Naval Postgraduate School, Monterey, CA, USA. doi:10.21236/ADA435319

[11] Margaret Ellis, Liesl Baum, Kimberly Filer, and Stephen H. Edwards. 2021. Experience Report: Exploring the Use of CTF-based Co-Curricular Instruction to Increase Student Comfort and Success in Computing. In *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1* (Virtual Event, Germany) *(ITiCSE '21)*. Association for Computing Machinery, New York, NY, USA, 303–309. doi:10.1145/3430665.3456376

[12] Wil Gibbs. 2025. All You Need Is MCP – LLMs Solving a DEF CON CTF Finals Challenge. https://web.archive.org/web/20260424050515/https://wilgibbs.com/blog/defcon-finals-mcp/. Online; accessed July 3, 2026.

[13] Pratham Gupta, Aditya Gabani, Connor Nelson, and Yan Shoshitaishvili. 2025. CTF Archive: Capture, Curate, Learn Forever. arXiv:2512.01233 [cs.CR] https://arxiv.org/abs/2512.01233

[14] Hex-Rays. 2026. IDA Pro. https://web.archive.org/web/20260627220752/https://hex-rays.com/ida-pro. Online; accessed July 3, 2026.

[15] Emma Hogan, Alejandro Cuevas Villalba, Hanan Hibshi, and Nicolas Christin. 2025. Observations of Highly Successful, Distributed Teams in a K-12 Online Security Competition. In *Proceedings of the 25th Koli Calling International Conference on Computing Education Research* (Koli, Finland) *(Koli Calling '25)*. Association for Computing Machinery, New York, NY, USA, 13 pages. doi:10.1145/3769994.3770022

[16] Vandana P. Janeja, Abu Zaher Md Faridee, Aryya Gangopadhyay, Carolyn Seaman, and Amy Everhart. 2018. Enhancing Interest in Cybersecurity Careers: A Peer Mentoring Perspective. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (Baltimore, MD, USA) *(SIGCSE '18)*. Association for Computing Machinery, New York, NY, USA, 384–389. doi:10.1145/3159450.3159563

[17] Kalmarunionen. 2026. KalmarCTF 2026. https://web.archive.org/web/20260407214809/https://kalmarc.tf/. Online; accessed July 3, 2026.

[18] Kees Leune and Salvatore J. Petrilli. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (Rochester, New York, USA) *(SIGITE '17)*. Association for Computing Machinery, New York, NY, USA, 47–52. doi:10.1145/3125659.3125686

[19] James Mattei, Christopher Pellegrini, Matthew Soto, Marina Sanusi Bohuk, and Daniel Votipka. 2025. "I'm trying to learn... and I'm shooting myself in the foot": Beginners' Struggles When Solving Binary Exploitation Exercises. In *Proceedings of the 34th USENIX Security Symposium (USENIX Security '25)*. USENIX Association, Seattle, WA, USA, 2867–2886. https://www.usenix.org/conference/usenixsecurity25/presentation/mattei

[20] Jelena Mirkovic and Peter A. H. Peterson. 2014. Class Capture-the-Flag Exercises. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '14)*. USENIX Association, San Diego, CA, USA. https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic

[21] Jelena Mirkovic, Aimee Tabor, Simon Woo, and Portia Pusey. 2015. Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '15)*. USENIX Association, Washington, D.C., USA. https://www.usenix.org/conference/3gse15/summit-program/presentation/mirkovic

[22] Connor Nelson and Yan Shoshitaishvili. 2024. DOJO: Applied Cybersecurity Education in the Browser. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (Portland, OR, USA) *(SIGCSE '24)*. Association for Computing Machinery, New York, NY, USA, 930–936. doi:10.1145/3626252.3630836

[23] Connor Nelson and Yan Shoshitaishvili. 2024. PWN The Learning Curve: Education-First CTF Challenges. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (Portland, OR, USA) *(SIGCSE '24)*. Association for Computing Machinery, New York, NY, USA, 937–943. doi:10.1145/3626252.3630912

[24] Connor Nelson, Robert Wasinger, Adam Doupé, and Yan Shoshitaishvili. 2026. Open Cybersecurity Education: Five Years of pwn.college. In *Proceedings of the 57th ACM Technical Symposium on Computer Science Education V. 1* (St. Louis, MO, USA) *(SIGCSE TS '26)*. Association for Computing Machinery, New York, NY, USA, 743–749. doi:10.1145/3770762.3772636

[25] NYU OSIRIS Lab. 2026. CSAW Capture the Flag. https://web.archive.org/web/20260513191920/https://www.csaw.io/ctf. Online; accessed July 3, 2026.

[26] Kentrell Owens, Alexander Fulton, Luke Jones, and Martin Carlisle. 2019. picoBoo!: How to Avoid Scaring Students Away in a CTF Competition. In *Colloquium for Information Systems Security Education (CISSE)*. Las Vegas, NV, USA. https://kentrell.net/static/papers/Pico_paper_CISSE_journal.pdf

[27] RITSEC. 2026. RITSEC CTF 2026. https://web.archive.org/web/20260316055121/http://ctf.ritsec.club/. Online; accessed July 3, 2026.

[28] Valdemar Švábenský, Pavel Čeleda, Jan Vykopal, and Silvia Brišáková. 2021. Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. *Computers & Security* 102 (2021), 102154. doi:10.1016/j.cose.2020.102154

[29] The angr Project. 2026. angr: A Powerful and User-Friendly Binary Analysis Platform. https://web.archive.org/web/20260621204928/https://angr.io/. Online; accessed July 3, 2026.

[30] Erik Trickel, Francesco Disperati, Eric Gustafson, Faezeh Kalantari, Mike Mabey, Naveen Tiwari, Yeganeh Safaei, Adam Doupé, and Giovanni Vigna. 2017. Shell We Play A Game? CTF-as-a-service for Security Education. In *2017 USENIX Workshop on Advances in Security Education (ASE '17)*. USENIX Association, Vancouver, BC, Canada. https://www.usenix.org/conference/ase17/workshop-program/presentation/trickel

[31] Vector 35. 2026. Binary Ninja: An Interactive Disassembler, Decompiler, and Binary Analysis Platform. https://web.archive.org/web/20260630113024/https://binary.ninja/. Online; accessed July 3, 2026.

[32] Daniel Votipka, Eric Zhang, and Michelle L. Mazurek. 2021. HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1268–1285. doi:10.1109/SP40001.2021.00092

[33] Jan Vykopal, Valdemar Švábenský, and Ee-Chien Chang. 2020. Benefits and Pitfalls of Using Capture the Flag Games in University Courses. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Portland, OR, USA) *(SIGCSE '20)*. Association for Computing Machinery, New York, NY, USA, 752–758. doi:10.1145/3328778.3366893

[34] Richard Weiss, Franklyn Turbak, Jens Mache, Erik Nilsen, and Michael E. Locasto. 2016. Finding the Balance Between Guidance and Independence in Cybersecurity Exercises. In *2016 USENIX Workshop on Advances in Security Education (ASE '16)*. USENIX Association, Austin, TX, USA. https://www.usenix.org/conference/ase16/workshop-program/presentation/weiss