Password Cracking as a Medium for Introducing Cybersecurity Skills and Student Autonomy

Emily Tanabe*, Cole McCorkendale*, Jens Mache*, Aurelio Puente*, Matthew Chio*, Richard Weiss†
*Lewis & Clark College †The Evergreen State College
{emilytanabe, colem, jmache, apuente, matthewchio}@lclark.edu
{rweiss}@evergreen.edu

***Abstract*—This paper proposes a design for an introductory password cracking exercise that gives students the opportunity to develop foundational cybersecurity skills while increasing their confidence and agency. This exercise aims to educate students about the brittle nature of passwords while increasing students' cybersecurity soft skills, such as collaboration, autonomy, and problem solving. To do so, the exercise uses pedagogical methods such as the Gradual Release of Responsibility model and guiding questions. The exercise is holistic, hands-on, and consists of three scaffolded levels:**

- **Password guessing, intelligence gathering, and spear phishing.**
- **Manually attempting a "credential stuffing" attack on a simple password.**
- **Scripting an automated password cracking tool.**

This exercise will educate students about passwords, how to attack them, and how to choose secure passwords while building foundational cybersecurity skills and keeping less experienced students interested, engaged, and motivated.

***Index Terms*—cybersecurity education, password cracking, student autonomy, intelligence gathering, soft skills, scripting**

I. Introduction

Students unfamiliar with cybersecurity may find intense technical exercises intimidating, which will discourage participation in such exercises or courses. During an undergraduate course in Lewis & Clark College's Computer Science program, many students felt that the main hands-on portion of the class, competing in the National Cyber League's biannual games, was stressful, overwhelming, and difficult. Additionally, employers have increasingly reported a shortage of employees with cybersecurity skills [1], thus educators may assume the best course of action is to teach as many tools and offensive exercises as they are able. However, students should instead be introduced to fundamental cybersecurity habits and soft skills prior to the intense skill building and "hacking tool" training that often serves to confuse less experienced students.

This proposed exercise educates students about password cracking, spear phishing, collaborative work, intelligence gathering, and scripting custom problem-solving tools. Password cracking is used as a medium for introducing students to broader cybersecurity skills, including "soft" skills that are also sought after in the cybersecurity job market [1], [2]. Many security exercises demonstrate how to use a particular tool or explore a particular exploit without explaining its functionality. The proposed scenario contrasts this by giving students practice with more challenging non-technical and soft skills such as persistence, an adversarial mindset, collaboration, and agency, while educating them on the actual steps an attacker will take and what the aforementioned tools do "under the hood" to perform an attack.

Using a holistic approach to cybersecurity education, these fundamental skills are interwoven with the technical content of the exercise. Students are encouraged to build strong cybersecurity habits such as using all available resources, communicating with peers and teammates, using their curiosity to find creative solutions, exploring all options, and cultivating a sense of autonomy and self-driven agency.

This paper is based upon work supported by the National Science Foundation under grant numbers 2216492 and 2216485.

II. Background

A. Gradual Release of Responsibility

The Gradual Release of Responsibility (GRR) model illustrates a pedagogical framework where the responsibility of performing a task gradually shifts from instructor to student [3], [4]. The GRR model is typically broken down into three or four distinct phases, "I do", "We/You do together", and "You do". The "I do" phase is typically an instructor lecture, the "We do" phase is often the instructor modeling an example, and can be expanded to include a "You do together" phase where students work in pairs or groups to complete examples, and the "You do" phase is students practicing a skill independently. For example, the instructor could give a thorough example to students, then give them time to practice with guided questions, and then let them complete the assignment with little instruction or assistance [5].

In many cases, especially in cybersecurity education where hands-on practice is key to developing practical skills, instructors will introduce a topic and then immediately let students practice it independently. Contrasting this to the GRR model, this is a sudden release of responsibility instead of a gradual one. This style of teaching is not necessarily bad and is often exactly what advanced students need to practice their skills in new ways [6]. However, the GRR model should be used at the beginning of courses or for introductory lessons, to help ease students into complex topics. Particularly in the case of cybersecurity, which is itself an extremely technical subject, using GRR can help students remain engaged in exercises without feeling overwhelmed or intimidated. This

Rank	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Score	2105	1265	1235	1185	1140	1130	1105	1080	1060	1045	1025	1025	1015	1005	1005	1005	990	980	935	925	920	910	910	905	890	670	580

Fig. 1. Computer and Network Security Students' Scores in the NCL Individual Game

is particularly useful for encouraging non-technical students to learn cybersecurity skills or for recruiting underrepresented students such as non-male students and BIPOC students for cybersecurity courses.

B. National Cyber League

The authors' experience in an undergraduate cybersecurity course informs the design of this exercise. The only prerequisite for the 200-level course (offered in fall semester) is the introductory computer science course, Computer Science 1, meaning many second and third year students take the class. A large portion of the curriculum uses the National Cyber League (NCL) [7] as a framework to introduce, practice, and assess various cybersecurity skills. The NCL's Individual Game was administered as an assessment in the course, to be completed as a take-home midterm over the duration of one weekend. Students were expected to commit 5-10 hours to the assignment. The NCL is an effective tool for cybersecurity education [8], however it can be a controversial issue among students. Many of the student evaluations received from this course mention the NCL, often discussing how they liked the challenge, but found the midterm to be overly time consuming and difficult. One student's comment reflects several students' attitudes, "Using the NCL as a midterm was an interesting idea, but the mixture of low communication, unseen material, and long hours made it a very unpleasant experience for many. Much did not stick in my memory, but what did I found very interesting." Another student asked for more "relevant and introductory work" in order to properly compete in the NCL. Even though many students in CS-211 scored well on the Individual Game, they had ambivalent perspectives about the NCL as a whole. Decreasing student frustration is key to enable better learning environments and retention of information.

Figure 1 shows student scores from the NCL Individual Game. At the end of the individual game, several students were automatically flagged as having used other students' answers, causing them to be disqualified from the leaderboards and NCL scouting reports. Notably, the overall top 4 scores consist of students who copied answers from others. In the assessment, 1000 points across all nine NCL categories was the threshold for a score of 100% on the midterm. The figure shows that most students made the 1000 point goal, but of the 24 who scored above a 90% on the assignment, a quarter of them made the decision to use another student's answer(s). The 6 disqualified scores in the figure are students that refused to complete the assignment as instructed with their given resources. In addition to students who were compelled to plagiarize answers, the scores show two students who scored below a 70% grade, one of which received a failing grade, with a 220 point gap between the lowest two scores and the next highest scoring students. In combination, both groups of students represent a larger issue in cybersecurity education: the common focus on lessons and exercises that require prior experience or skills for success, like the NCL. This focus creates a high barrier of entry that can result in students plagiarizing answers, or failing to progress on their own. The NCL is a great resource for students, and this exercise is not meant to replace or compete with the NCL in any way, merely to supplement its use in classrooms and help prepare students for the competition. The proposed exercise is designed for students who, for any combination of reasons, struggle early on with intensely technical hands-on exercises, with the goal of increasing student engagement, success and autonomy.

III. The Exercise

The proposed exercise would be implemented as part of an existing suite of cybersecurity exercises that run on the cloud-based platform EDURange, created by researchers from Lewis & Clark College and Evergreen State College. EDURange consists of multiple modular activities covering a variety of topics in cybersecurity, with the implementation of guiding questions and telemetry to gather data on student performance, enjoyment, and information retention [9]. Many existing EDURange exercises require knowledge of basic cybersecurity skills like the command-line interface (CLI), networking, and file systems, which can be intimidating to novice students. The exercise consists of three levels, each with their own challenge designed around a specific cybersecurity skill, while following the same simple narrative.

A fairy tale narrative was chosen for three reasons. First, the story provides existing well known characters to lessen the learning curve of becoming familiar with a character's personality traits. Second, the goal is to boost student engagement with a fantasy story and make cybersecurity an approachable topic to novice students. Finally, while using a fairytale narrative, the hope is to encourage creativity throughout the password cracking activities and embrace thinking outside the box. While not everyone is familiar with Snow White, the alternative of generating an entirely new story could detract from the ultimate goal of educating users about password security and cracking. For those unfamiliar with the story, a text summary with links to external resources will be provided.

A. Level 1

The first level presents students with an information dense website. Students would be introduced to the website as the homepage for Snow White and the Seven Dwarves. Students

play the role of penetration testers hired by Snow White to help secure her webpage from forces of evil that may seek their private data. The site would feature an About page with profiles of each of the dwarves. Here, students would be given a hint that the accounts use particularly insecure usernames and passwords. The dwarves' profiles would list their names and a brief description of themselves. These descriptions would contain information on which all of their credentials would be based.

For example, Dopey would have the easiest password, with his bio mentioning that he "likes to keep things simple" and "often forgets his passwords," so his username is his name in lowercase and his password is "password". Before sending students to work in groups, the instructor would demonstrate Dopey's profile as an easy target for an intelligence based "spear phishing" attack. Given Dopey's simple-minded character design, the instructor would demonstrate the ease with which his username and password can be guessed. After this basic example, students will split into groups to gather intelligence and break into the other employee accounts. This page would also be scripted to give errors when an incorrect login is given, like most login pages. Notably, this login page would tell the user if the username is correct, even if their password is not. There would be no timeout or max attempts, allowing students to try as many times as they need in order to find a working username. Most dwarves' usernames would just be their first name, however, the more secure ones, like Doc, could have more complex usernames. Guessing the username and password would get progressively more difficult, but guiding questions would serve to help students find all the employee profiles. Level 1 as a whole would ideally educate students about the risks of making their passwords simple and based on publicly available personal information. This emphasizes the holistic approach by focusing not only on the character length and use of special characters when choosing a secure password, but also the content of the password and the information that a person shares publicly.

1) Level 1 Learning Objectives: This level aims to give students an example of how social engineering is used in the real world to break less robust security using simple deductions from given information. By allowing students to work in groups, Level 1 also seeks to build collaborative skills and to minimize hints given by the instructor in favor of allowing students to discuss ideas and test their own hypotheses. That said, the instructor would be expected to intervene with a more direct hint if a class or group of students is particularly struggling. One hint that may be necessary to get overwhelmed students started would be to tell them to "just try anything" on the login page, to get an idea of how the error messages look. This approach guides students toward practicing agency and autonomy, allowing them to practice moving beyond receiving instructions to creative problem solving. This level is based on the key idea that the actual skill, guessing the password, is not technically intense, but gives the students the opportunity to practice collaborative exploration with limited instructor guidance.

Additionally, Level 1 models the beginning of the GRR model, as it begins with instructor-led content and moves toward student-collaborative practice. One important goal of the level is to embody the "I do" and "We do" sections of the GRR model

B. Level 2

The second level has a similar login page to the first but with different clues. The narrative would progress with the Dwarves having improved their passwords after their initial breach, but they've discovered that Snow White has also failed to properly secure her account. Here the student acts as a penetration tester, and is asked to find her log in as well. The Dwarves have written a short article on password security in the "about" section, with a section emphasizing the increasing importance of length in passwords as attackers' hardware becomes more advanced. The article also features two short lists: one list of common, easily-guessed usernames (such as "admin"), and one list of similarly common and easily-guessed passwords (such as "password123"). Students would be expected to use the knowledge from the first level and expand upon it to attempt a manual "credential stuffing" attack. Credential stuffing attacks are often performed by an attacker with a stolen credential list, attempting each username and password on such a list until they find a working login.

To begin, students would try each username at the login screen until they get an error telling them that the username is correct. Once they find a working username, they will attempt the commonly used passwords until they find the correct one. These easily guessed credential lists would be relatively long in terms of manually attempting each, with 10-20 usernames and passwords each. Since students would be working in groups, they may work out a way to divide the manual efforts. It should be noted that the usernames and passwords that are used will be real-world common logins rather than ones themed around the narrative, since the goal is to keep Level 2 grounded in real-world password security.

1) Level 2 Learning Objectives: Level 2 aims to reinforce the foundational knowledge of intelligence gathering from Level 1 by allowing them to practice the same skill again while learning new skills required for conducting a credential stuffing attack. This level starts with the instructor giving a definition and an example of what an automated program is doing when conducting such an attack. The dwarves' article on the "about" page will also serve to genuinely educate students on password security. This will demonstrate to students the importance of choosing secure passwords, particularly regarding password length and adding additional characters. Additionally, Level 2 moves students into the "You Do Together" phase of the GRR model which will build students' autonomy while increasing their communication and collaboration skills.

C. Level 3

The third level of the exercise would be more difficult, giving students nothing but a command line. After the students

helped to secure Snow White's account, they are tasked with breaking the security in the evil Queen Grimhilde's private network. As a sorceress, the queen is also not very well versed in network security, so the students are given access to a terminal that is logged into a non-administrator account on her network. The terminal is accessed through an unpatched SSH client backdoor which is implied in the narrative, but not required for the students to actually conduct. To complete the level, students would be expected to write a basic automated credential stuffing script to find the root login in Python, a language chosen for its accessibility to beginners. Since this exercise is designed for beginner-level students with varying skill levels, the design includes two levels of difficulty. By the end, students should have a program that is able to test each password with the correct username until the login is correct. It would be beneficial, regardless of the expertise of the class, to include a discussion of the ethics of how students use the knowledge and tools covered in Level 3, focusing students' attention towards the idea of defending against such an attack, and asking them to consider ways they could defend against it.

1) Level 3 Easy Mode: Depending on the prior knowledge and experience of the class, Level 3's easy mode may be best administered following a supplemental lesson from the instructor. The lesson would cover the basics of scripting in Python such as what a script is, how to write one, and a simple example with topics chosen at the instructor's discretion. Students would then be instructed to split into groups and discuss what they think are the necessary elements of an automated credential stuffing attack. This can be done verbally, or by having students write pseudocode. Students would, with instructor assistance, download a password list which could be a moderately sized subset of the RockYou breach password list, or a similar large password list. Students would be guaranteed that the password to the site is in the list somewhere, but it is too long to try by hand. Next, students would be tasked to independently write their attack script. It would be beneficial for the instructor to show and explain the solution on a projector screen in front of the class so that anyone with less experience can follow along while asking questions, regardless of the average student's level of expertise.

2) Level 3 Hard Mode: For advanced students, it would be assumed that their programming skills were advanced enough to be able to write most of the script independently. Similar to easy mode, hard mode would begin with an instructor lecture on automated credential stuffing attacks and other related topics of the instructor's choice. Students would then be asked to break down the integral elements of the script through a discussion with their neighbor or a group discussion. This brief activity would encourage students to start thinking about how they will structure their script and how to break down the problem. In hard mode, students would be independently tasked with writing their script, but encouraged to work with a neighbor if they get stuck.

3) Level 3 Learning Objectives: The third level is designed to emphasize the basics of automated password cracking and scripting tools through heavier instructor led lessons. This would reinforce a holistic approach to password security by blending soft and hard skills through a lesson. Students should gain more confidence in their ability to assess a situation, envision a solution, and begin testing their hypotheses. Level 3 will also help students practice adopting an adversarial mindset when approaching a problem. For students who don't already know how to write basic scripts such as a password cracker, this level serves as a basic introduction to ad-hoc coding and, for some, a first-time introduction to the command-line interface (CLI).

While this level is divided into two different versions depending on the level of the class, instructors should utilize the GRR model regardless of which version they use in their classroom. The overall goal of Level 3 is to give students an introduction to the process of scripting, which will hopefully spark their creativity. Many students may be aware of existing off-the-shelf tools but would not know how to create their own. This knowledge will empower students to better understand the tools they use and spark their creativity when faced with unexpected challenges.

D. Optional Advanced Modules

As an optional final level of the exercise for students who finish early or instructors who wish to challenge their class, a loose range of modules is provided to train students' advanced scripting skills by having them implement more advanced password cracking techniques such as basic dictionary, rule-based, and pattern-matching attacks, in addition to a brief introduction to hash files. These modules would be similar to Level 3's command line design, but the steps students must take in order to find the passwords would increase alongside the difficulty. The expanded narrative could involve students performing more attacks on other fairy tale villains, or perhaps another attack on the evil Queen's network after she has made some security improvements. The narrative for the optional modules could also be entirely foregone at the instructor's discretion since it is intended to discuss real-life applications and add depth to the knowledge and skills from previous levels. Each of the following modules can be selected by the instructor or students depending on their time constraints or other needs.

1) Hashes: As an easier topic to introduce, hashes may be a suitable choice for classes who are doing the optional module(s) on a different day from the rest, giving them a chance to warm up. Depending on whether students are familiar with the topic, the instructor could elect to give a lecture on hashes, what they are used for, the different types, and the encryption methods that have already been cracked. As a short activity, students could be given different types of hashes, beginning with known ones that are easy to crack with a simple internet search, and moving on to more complex ones that require tools to solve. This would serve as a segue into the next module, should the instructor choose to administer it.

2) Off-The-Shelf Tools: The instructor would give a short demonstration of decrypting a hash file with an off-the-shelf

tool such as John the Ripper and host a discussion on how robust tools like John are used to do everything the students' scripts did, and more. Depending on the interest and investment of the students, the module could go further and give more examples of ways that John can be used to break various types of security. The instructor could choose other tools such as ophcrack or hashcat to discuss with the class as well. This would serve as a discussion to give students real-world context for the software and skills covered in the knowledge. Given the ease of access to these tools, this discussion would add to the holistic approach of teaching both technical and non-technical students.

3) Scripting Dictionary and Rule-Based Attacks: Students would first be faced with a list of passwords with a common pattern between them, such as an English word and a number, and would be asked to write a script to generate passwords with this pattern. As a dictionary to read from for these passwords, students could be given a short subset of an English dictionary as a text file. After this, the instructor would discuss rule-based attacks and how they work with the students, then ask them to rewrite their previous script in the form of a rule-based attack, where the given rule is to append permutations of a number at the end of each word on the list. Students could be asked to expand upon their program's rules in order to generate different types of passwords, such as uppercase, lowercase, capital first letter, or staggered capitalization.

IV. Discussion and Related Work

While password cracking as an exercise is not new [7], [10]–[13], through the GRR model and a holistic approach, the designed exercise is a novel instructional tool. Password cracking is a useful skill and is widely taught in cybersecurity courses. National competitions like the National Cyber League have entire sections dedicated to the use of password cracking tools [7]. The NSA recommends GenCyber's password cracking lesson found through the CLARK center, which is similar to the NCL in that it focuses mainly on tools, in this case, John the Ripper [13]. The US Cyber Range, built by Virginia Tech, includes a password cracking exercise [14]. Wang et al developed several labs, including a password cracking lab, to increase the presence of IT security education for undergraduates [15]. The proposed exercise is not even the first time EDURange has incorporated password cracking into their scenarios. Two other exercises, Treasure Hunt [12] and Clue [12] have used password cracking as part of their topics. The Treasure Hunt scenario involves more skills than password cracking, including understanding and manipulating Linux permissions. The main password cracking skill is using hashcat and John the Ripper in a command-line setting. Both scenarios are geared towards intermediate or advanced students who have some computer science experience.

Additionally, the Clue scenario, which was never fully incorporated into EDURange uses the premise of the Clue board game and has students logging into different Linux user accounts through various password cracking skills. The Clue scenario also takes place in a command-line interface (CLI)

	NCL	CLARK	Treasure Hunt	Clue	Our Exercise
Doesn't require previous skills					x
Use of command line	x	x	x	x	x
Guidance for beginner students		x		x	x
Gradual Release of Responsibility					x
Introduction to scripting					x

Fig. 2. Comparison of the proposed exercise to password cracking exercises from the NCL [7], GenCyber's password cracking lesson found through the CLARK center [13], Treasure Hunt [12], and Clue [12].

and introduces students to various kinds of password cracking, including brute force attacks, dictionary attacks, and rule-based attacks. Unfortunately, this exercise was never classroom tested, so there is no data to indicate how students would respond to such an exercise. While the Clue exercise may seem similar to the proposed exercise due to their shared topic, they differ in three key areas. The Clue exercise exists entirely on the CLI while the proposed exercise has a web interface in addition to the CLI. The Clue exercise does not educate students about social engineering or scripting in addition to education about password cracking. Finally, the Clue exercise is designed to be almost entirely self driven from the students' perspective, while the proposed exercise includes an intentional breakdown of related topics between instructor-led segments, student group work, and student independent work.

The proposed exercise is novel in these specific ways:

- The levels range in difficulty and complexity so that it isn't too intimidating to approach, yet still keep students of all skill levels engaged
- A scaffolded set of levels using the GRR model of education to increase learning productivity through guidance and release
- A holistic approach is taken to demonstrate core aspects of cybersecurity (intelligence gathering and scripting) alongside the main technical skill (password cracking)
- Students build their soft skills through collaboration, critical thinking, problem solving, and student agency

The Mountrouidou 2018 [11] paper discusses the importance of cybersecurity education for all majors as part of a liberal arts first-year general education course. Their paper reviews students' perceptions of and performance in a cybersecurity introductory course where a majority of students had no experience in computer science. They found that students gained a deeper understanding of cybersecurity and its importance in their lives, especially through the hands-on exercises conducted in the classroom. They note that students particularly enjoyed their password cracking exercise, which

was structured in a similar manner to the proposed exercise. The Mountrouidou exercise began with students guessing easy passwords, then built into them looking for encrypted passwords and hashes and using tools to decrypt them. The authors describe student enjoyment of the password exercise had to do with its simplicity. Student comments mention that the exercise was, "just cracking a password and finding a solution to a problem." The proposed exercise expands on this idea by recognizing that students may find passwords a very simple and relatable security topic, but it gives them the opportunity to practice their problem-solving skills. The authors also discuss how some of their students felt left out of the course because of their lack of computer science experience, something they hope to fix in future courses. The proposed exercise hopes to avoid this issue, as it is designed for total novices as well as more advanced students.

The Crick 2020 [2] paper describes current challenges in Cybersecurity education, specifically within UK computer science programs. In their description of the pedagogic principles they deem necessary for cybersecurity education, they mention the need to embed soft skills into cybersecurity courses. According to the authors, an "ideal assignment in cybersecurity mixes the academic and human skills, preferably inseparably." The proposed exercise aims to do just this, by designing the exercise to intentionally build students' soft skills. The authors list their key human skills as problem solving, communication, analytical thinking, collaboration, and attention to detail. The exercise gives students beginner technical problems to apply these human skills.

V. Limitations

The previous discussion has focused on the benefits of the exercise and the ways in which it builds off previous literature. This section will detail the limitations of the exercise.

Firstly, the exercise is designed to appeal to beginner students, which comes with the tradeoff of lacking in appeal for advanced students. While this exercise is still recommended for more advanced students because of the soft skills it introduces, a student who is already familiar with password cracking may find this exercise boring or beneath their skill level.

Because the exercise is meant for beginner students, it doesn't focus on tools. This is a pro and a con for the exercise, as it allows students to build confidence in ad-hoc coding, creative problem solving, and understanding what goes on "beneath the hood" in other tools. However, it is acknowledged that some students may be frustrated with having to perform the task "by hand" when tools have already been developed. It is suggested that instructors lean into such reasoning and transparently explain to students how building a tool by hand can be beneficial.

Level 1 was originally intended to educate students about social engineering, but unfortunately implementing this aspect would be too difficult and cumbersome for the purposes of this exercise. Level 1's introduction to spear phishing allows students to understand how bad actors may maliciously utilize publicly available information, but does not explore how to counteract an intentional manipulation in real time. For further advanced or modified modules, exploring call transcripts or email exchanges as examples of social engineering attacks could expose students to the tactics, language, and methods bad actors may use.

While offensive exercises are increasingly common in cybersecurity courses, there is something to be said about the ethical considerations of framing a malicious attack against an "evil" person. The exercise's narrative uses the fairy-tale plot of Snow White and the Seven Dwarves and frames one of the levels around trying to break into the Evil Queen's root account to access her malicious files. While obviously not based in reality, it's possible that without proper framing and discussion students may take it upon themselves to hack other actors they perceive as "evil", so it's important to have a conversation with students about how they will be using the skills taught in this exercise.

Lastly, the proposed exercise is simply a design, it has not yet been tested in a classroom setting. However, two of the main authors who designed the exercise are students and have taken the course that this exercise is intended for. Using their perspective, they reflected on what they felt was missing from the course, and they developed this exercise.

VI. Conclusion and Future Work

The design of this exercise was focused on contributing beginner-friendly cybersecurity exercises to the EDURange platform with an emphasis on fundamental soft skills. The aim was to lower the barrier of entry to cybersecurity training exercises. Through the use of the Gradual Release of Responsibility (GRR) educational model, narrative, and guiding questions, the exercise was designed to construct a healthy learning environment for students. Additionally, as more was learned about the process and challenges of designing for cybersecurity education, it was remarkable how few offensive security exercises at an undergraduate level considered soft skills; thus, the proposed exercise explores new ways to incorporate creativity, autonomy, password/security education, teamwork, problem solving, and critical thinking.

Future work will focus on fully implementing the exercise into the EDURange platform. This will include creating the exercise framework and instructor directions, as well as writing guiding questions and milestones to track students as they complete each step. Future work also includes expanding on ideas for the supplemental modules to make the exercise more interesting for advanced students and including more complex levels of optional exercises. The future plan for EDURange includes a focus on designing a machine learning hint system that uses reinforcement learning to understand student performance and give hints to help students' progress flow better.

References

[1] R. Flores, A. Siami Namin, N. Tavakoli, S. Siami-Namini, and K. S. Jones, "Using experiential learning to teach and learn digital forensics: Educator and student perspectives," *Computers and*

Education Open, vol. 2, p. 100045, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666557321000161

[2] T. Crick, J. H. Davenport, P. Hanna, A. Irons, and T. Prickett, "Overcoming the challenges of teaching cybersecurity in uk computer science degree programmes," in *2020 IEEE Frontiers in Education Conference (FIE)*, 2020, pp. 1–9.

[3] S. Webb, D. Massey, M. Goggans, and K. Flajole, "Thirty-five years of the gradual release of responsibility: Scaffolding toward complex and responsive teaching," *The Reading Teacher*, vol. 73, no. 1, pp. 75–83, 2019. [Online]. Available: https://ila.onlinelibrary.wiley.com/doi/abs/10.1002/trtr.1799

[4] P. Pearson and M. Gallagher, "The instruction of reading comprehension," *Contemporary Educational Psychology*, vol. 8, 07 1983.

[5] D. Fisher and N. Frey, *Better Learning through structured teaching;a framework for the gradual release of responsibility*. Association for Supervision Curriculum Development, 2021.

[6] N. Maynes, L. Julien-Schultz, and C. Dunn, "Modeling and the gradual release of responsibility: What does it look like in the classroom?" *Brock Education: a Journal of Educational Research and Practice*, vol. 19, 2010.

[7] The national cyber league. [Online]. Available: https://nationalcyberleague.org/

[8] D. Zeichick, "Successfully incorporating a cyber security competition into an intro to computer security course," *J. Comput. Sci. Coll.*, vol. 38, no. 1, p. 58–67, nov 2022.

[9] R. Weiss, F. Turbak, J. Mache, and M. E. Locasto, "Cybersecurity education and assessment in edurange," *IEEE Security & Privacy*, vol. 15, no. 03, pp. 90–95, may 2017.

[10] R. Snyder, "Ethical hacking and password cracking: A pattern for individualized security exercises," in *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, ser. InfoSecCD '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 13–18. [Online]. Available: https://doi.org/10.1145/1231047.1231051

[11] X. Mountrouidou, X. Li, and Q. Burke, "Cybersecurity in liberal arts general education curriculum," in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, ser. ITiCSE 2018. New York, NY, USA: Association for Computing Machinery, 2018, p. 182–187. [Online]. Available: https://doi-org.library.lcproxy.org/10.1145/3197091.3197110

[12] R. Arends, R. Deussen, B. Green, J. Rush, J. Mache, and R. Weiss, "Get a clue: A hands-on exercise for password cracking," in *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2018, pp. 117–121.

[13] GenCyber. (2023) Gencyber lesson plan password design and cracking. [Online]. Available: https://clark.center/details/jouypo1/923400e6-02de-450e-9912-417471cd1b9a

[14] M. Vogel. (2023) Lesson/laboratory exercise 7: Password cracking. [Online]. Available: https://www.uscyberrange.org/courseware/laboratory-exercise-7-password-cracking

[15] X. Wang, Y. Bai, and G. C. Hembroff, "Hands-on exercises for it security education," in *Proceedings of the 16th Annual Conference on Information Technology Education*, ser. SIGITE '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 161–166. [Online]. Available: https://doi.org/10.1145/2808006.2808023