Get a *Clue*: A Hands-On Exercise for Password Cracking

Rosemary Arends[1], Raya Deussen[1], Benjamin Green[1], Jodi Rush[1], Jens Mache[1], and Richard Weiss[2]
[1]Lewis & Clark College, Portland, OR, USA
[2]The Evergreen State College, Olympia, WA, USA
{rosemaryarends, rayadeussen, bengreen, jodirush, jmache}@lclark.edu

Abstract— *With the growing threat of cyber attacks, educating students on ethical hacking becomes more and more important. In this paper, we focus on password cracking and (1) analyze exercises from the National Cyber League and EDURange's Treasure Hunt, and (2) describe our design for a new exercise called Clue, which is based on the popular board game of the same name. Our motivation in designing Clue was to bridge the gap in knowledge that beginning students need to compete in the National Cyber League and to complete more open-ended scenarios, like Treasure Hunt. We also aim to provide a more structured activity and keep students engaged with a storyline.*

Keywords: Cybersecurity Education, Password Cracking, Student Engagement, Guidance, Storyline

1. Introduction

In recent years the threat of cyber attacks has become more prevalent in the public spotlight. This influence is due in part to the prevalence and strength of modern cyber attacks. Cybersecurity is a growing field, and it is becoming essential to develop effective methods to educate students. Students need to not only understand the theoretical aspects, but also understand attacks and tools, in order to better defend. The most effective way to do this is to provide students with hands-on activities and labs. Both the National Cyber League Gymnasium (NCL) [4] and EDURange's Treasure Hunt [2] provide students with these types of activities. In this paper, we analyze Treasure Hunt and the password cracking section of the NCL Gymnasium, and offer a design of a new module, Clue, that will focus on providing students of all levels with password cracking experience.

Password cracking is the process of recovering the plaintext password from a password hash. Hashes are the product of a one-way hash function: given an input, you can calculate the output using an encryption algorithm. But given the output, there typically is no way to reliably determine the input. Thus, given the password hash, there is no way to calculate the plaintext password. We can, however, guess a password, hash it with the one-way hash function, and compare the results to the known hash. If the two hashes are the same, we have found a plain-text password. There is a wide range of techniques that can be used to crack passwords, including dictionary attacks, brute force attacks, and rule-based attacks. There are many reliable programs that use these techniques and are valuable tools, such as Hashcat, John the Ripper, and Ophcrack. Most are free downloads and open-source, and are aimed to be educational and help people create better passwords.

1.1 EDURange's Treasure Hunt

EDURange is a NSF-funded education platform designed to introduce students to several aspects of computer security [5, 10, 12, 13, 14]. There are currently six modules available for students to use, and they address analytical abilities as well as skills with various command line tools, such as ssh, nmap, scapy, and strace [1]. The Treasure Hunt module from EDURange is designed to test students' ability to apply the right password cracking tools such as hashcat or John the Ripper, and understand Linux file permissions [1, 2]. Students ssh into an instance where they are provided with 16 user directories, each containing a password. The students are tasked with finding all sixteen passwords through password cracking and utilizing Linux group permissions.

1.2 The National Cyber League

The National Cyber League, or NCL, is an online capture the flag competition that is open twice a year. Thousands of people participate each season, with students paying a fee to gain access to the games and the Gymnasium. The Gym is open throughout the season and this year it contained questions in seven different categories: open source intelligence, cryptography, log analysis, network traffic analysis, password cracking, wireless access exploitation, and enumeration and exploitation [4]. For the purposes of this paper we are going to focus on the password cracking section. There are several parts of the password cracking section, varying in difficulty levels. The password cracking challenges involved dictionary attacks, mask attacks, and rule-based attacks.

ISBN: 1-60132-488-X, CSREA Press ©

Figure 1: Description of brute-force, dictionary, and rule-based attacks.

2. Analysis of existing cybersecurity exercises

From playing both Treasure Hunt and the NCL Gymnasium, we note several aspects of each that we found effective and ineffective. A valuable learning objective of both were the skill sets required to complete each. While we believe that password cracking is an important area for cybersecurity students to learn, a drawback of both the NCL Gym and Treasure Hunt is their reliance on the user having been pre-exposed to the tools and skills needed to crack passwords. Specifically, Treasure Hunt challenges are divided into 16 users, where the students are required to determine which tools and techniques to use for each of the passwords [2]. Despite being numbered 1 through 16, the tasks are not ordered according to difficulty, thus allowing the user to bounce around between tasks as they attempt to complete them all. While this allows the student the freedom to try accessing different folders in any order, it can also be quite overwhelming, especially for beginning students who have little to no experience with many of the tools and techniques needed. We saw this same reliance on users' knowledge of these tools in the NCL Gym. While those tasks were labeled based on difficulty, there was little guidance for students to follow in terms of developing an understanding of how to crack passwords. Thus, we felt there was a need for an exercise to fill in that gap.

When designing this exercise, we were attracted to the structure of Treasure Hunt. Hints and other files were stored in the directories, and could be reached using the command-line. This format worked well on the EDURange platform, allowing students to sign-in and access this exercise without needing to necessarily store any of the information on their computer. On the other hand, we preferred the type of questions asked in the NCL Gym. These questions more directly assessed students' knowledge of tools to crack passwords. While we liked the overall structure of Treasure Hunt and the assessment in the NCL Gymnasium, neither had a structured storyline. This feature is one that students say that they like, and also appealed to us. Another EDURange module, Total Recon, has a storyline that is integrated with solving the problems in the exercise [10], and we took a similar approach. We chose the game *Clue*, and the movie it inspired, to base our storyline of off.

The NCL Gym addressed student engagement differently by using a point system, rewarding users for answering questions correctly. While this can be an effective system, for the purpose of our module, we wanted to focus less on getting the right answer and more on learning the skills. Therefore, in creating a new module, Clue, our goal was to bridge the gap between a beginner's knowledge and the knowledge needed to fully engage with the NCL Gymnasium as well as EDURange's Treasure Hunt.

3. Our new exercise Clue

3.1 Introduction to the *Clue* board game

Clue is a multi-player murder mystery board game as well as a 1985 film starring Tim Curry. The goal of the game is to discover who murdered Mr. Boddy in what room and with what weapon. Players gather clues from other players as they move around the board and visit various rooms to ultimately deduce the details of the murder. The movie follows a similar storyline, with all the characters gathering for a dinner party. Again, Mr. Boddy is murdered and everyone tries to determine who the murderer is. Our module will have students gather clues as they crack passwords to move from room to room and finally discover who killed Mr. Boddy [11].

3.2 Structure of our new exercise

In our module, we aim to create a space for students to learn and practice important password cracking skills through a more guided approach than given in the NCL and Treasure Hunt. To help keep students engaged, we have created a password cracking tutorial based off *Clue*. The students follow a storyline and are given the role of a detective trying to solve the murder. Throughout this module, students must use different password cracking skills to obtain the passwords corresponding to the provided hashes, which are then used to unlock the next room. Rooms are associated

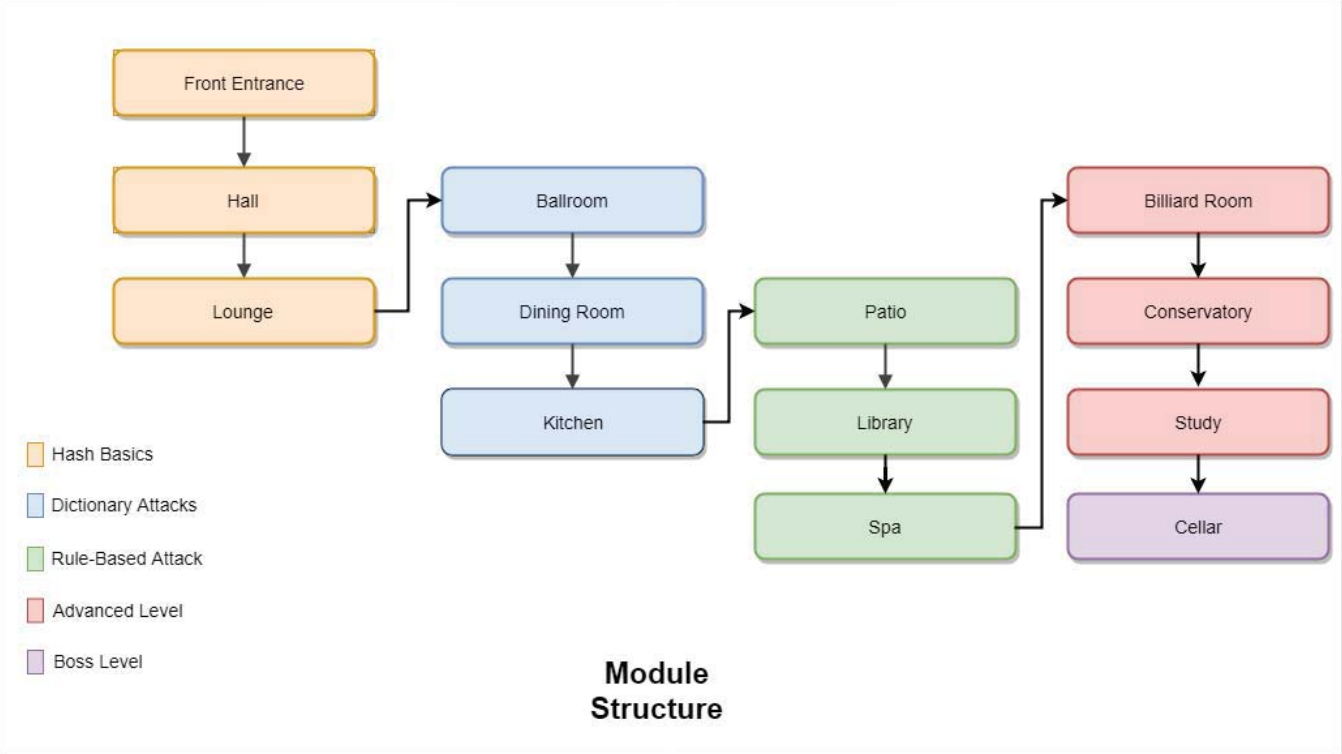

Figure 2: Exercise structure showing room paths and types of password cracking challenges in each room.

with users, each protected with a password that students will need to discover to proceed. As they move forward, the challenges increase in difficulty and students are required to understand how more difficult passwords are cracked and more efficient ways to crack them, see Figure 2.

4. Discussion

While the NCL and Treasure Hunt provide little instruction, we provide challenges that begin structured with clear hints, and get progressively harder with less guidance. As students complete this module, they will learn more about the different techniques for cracking passwords and become more comfortable with using available tools, as well as develop a greater understanding of password security.

	Treasure Hunt	NCL	Clue
Self-driven navigation	x	x	
Necessary pre-existing skills/understanding	x	x	x
Linear progression of difficulty		x	x
Use of the command line	x		x
Guidance for beginning students			x
Useful as practice for advanced students	x	x	x
Engaging storyline			x
Engagement using point system		x	

Table 1: A Comparison of Treasure Hunt, the NCL, and our new exercise

When designing a multi-level game or exercise, one has to choose the mechanism by which players progress from one level to the next. This could be implemented as a single user logging in to different hosts or a player finding secrets on the same host. EDURange has both of these (SSH Inception and Treasure Hunt), so we had two models for our design. SSH Inception utilizes several virtual machines to provide different hosts for players to SSH into. Students will first SSH into one machine, and then use nmap and other tools to locate subsequent hosts and SSH into those machines. This requires the use of many virtual machines. Treasure Hunt, however, uses only one virtual machine with files and directories that are protected or hidden in different ways. We chose to use the structure of Treasure Hunt, since Clue contains many password protected directories that would translate into thirteen virtual machines had we used the structure of SSH Inception. Mirroring the structure of Treasure Hunt, we choose the names of the rooms to be the usernames, with the corresponding passwords students are required to crack to proceed, see Figure 3. We also included an optional hint file in each difficult room to help guide students in case they get stuck, much like how the NCL offered hints and solutions.

Our module is an engaging way for students to learn and practice necessary skills for cracking passwords. There are many different techniques and programs available to use as tools for this topic, so we chose to highlight a limited

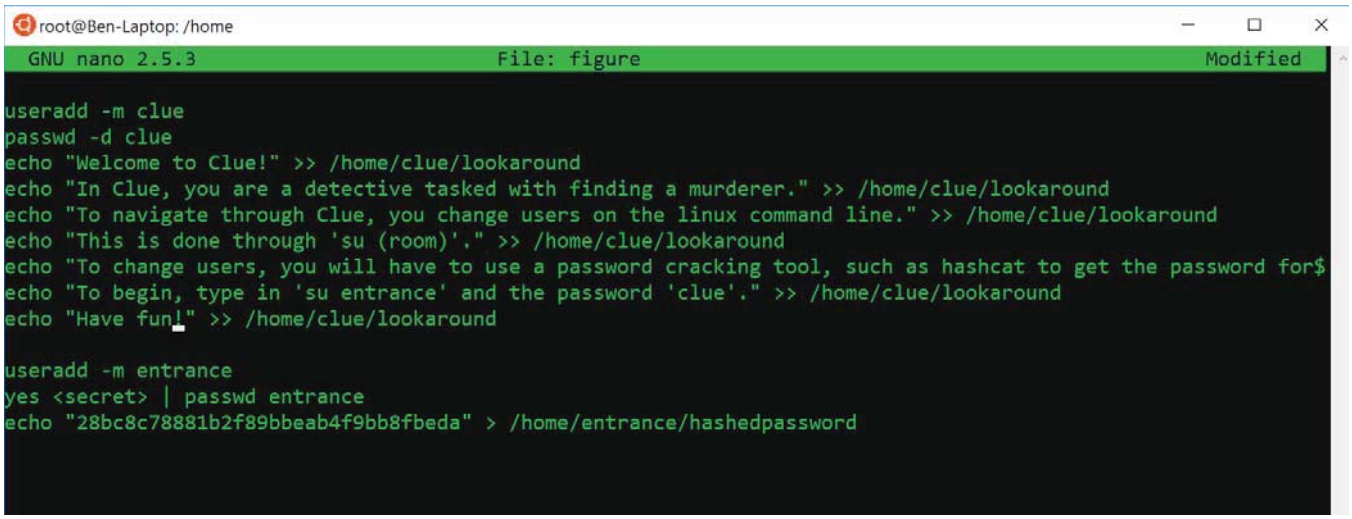

Figure 3: A sample of bash code used to set up a room in our exercise.

selection. As students navigate through this module, they are expected to use password cracking programs like hashcat and John the Ripper to perform brute-force, rule-based and dictionary attacks. The process of reversing hashes to passwords can be very challenging, so we hope to introduce each new concept with reasonable instruction as to which tools should be used while maintaining enough ambiguity to keep each step self-driven. With the completion of each step, students will become more comfortable with generating commands for each tool and come to recognize the format of different hashing methods.

5. Related Work

In addition to the NCL Gymnasium and Treasure Hunt, other cybersecurity education platforms include the NICE Challenge Project and DETERLab. The NICE Challenge Project is a web platform where students are provided virtual machines to solve various challenges in accordance with the NICE Cybersecurity Workforce Framework. There are a variety of public challenges for students to complete, in addition to teachers being able to upload their own content [9].

DETERLab is another education and research module created by the University of Southern California that focuses on providing a platform to teach cybersecurity [7]. It provides users with realistic settings to practice cybersecurity exercises on a variety of topics, including man-in-the-middle attacks, code injection attacks, and worm modeling. DETERLab is currently used in 103 institutions in a variety of classes to further cybersecurity education [8].

6. Future Work

We will use Clue in the undergraduate cybersecurity course at our college to help engage students in practicing password cracking. We believe Clue will be an important first step for beginning cybersecurity students and will prepare them for completing Treasure Hunt and the password cracking section of the NCL.

We plan to integrate Clue into the EDURange platform. Our module will be available for students and instructors to use in classes in the near future.

7. Conclusion

Cybersecurity is a constantly evolving and growing field of study. It is becoming increasingly crucial to develop effective methods to educate and familiarize students with the many aspects of cybersecurity. Both EDURange's Treasure Hunt and the NCL are effective educational frameworks for allowing students to develop their skills with various tools and concepts. However, both of these rely on the assumption that students have certain background knowledge and skills, making these modules very challenging to beginning students. In this paper, we described our design for a module that would allow beginning students to gain experience with password cracking. This additional structure will help guide students with no experience through password cracking problems and tools. The module also provides experienced students with questions to test their skills. The plan is that cybersecurity classes will be able to use the Clue exercise to provide a structured and engaging way for students of a variety of levels to gain experience and familiarity with password cracking.

8. Acknowledgements

This work was partially supported by National Science Foundation grants 1723705, 1723714, 1516100 and 1516730. We would also like to thank the John S. Rogers Science Research Program and the James F. and Marion L. Miller Foundation.

References

[1] *EDURange Student Manual*. PDF. EDURange, March 6, 2017.

[2] "EDURange | Scenarios | Treasure Hunt." EDURange | Welcome. Accessed May 14, 2018. https://edurange.org/scenarios.html

[3] "EDURange | Welcome." EDURange | Welcome. Accessed May 14, 2018. https://edurange.org

[4] "NCL Gymnasium." NCL | National Cyber League | Ethical Hacking and Cyber Security. Accessed May 14, 2018. https://www.nationalcyberleague.org/ncl-gymnasiums

[5] Weiss, R., F. Turbak, J. Mache and M. E. Locasto, "Cybersecurity Education and Assessment in EDURange," in IEEE Security & Privacy, vol. 15, no. 3, pp. 90-95, 2017.

[6] Marechal, Simon. "Advances in Password Cracking" *Computer Virology 4*, no. 1 (2008) 73-81.

[7] Benzel, Terry. "The Science of Cyber Security Experimentation: The DETER Project" USC Information Sciences Institute (2012).

[8] "Education" The DETER Project. Accessed May 15, 2018. https://deter-project.org/deterlab_education

[9] "NICE Challenge Project - The Workforce Experience Before the Workforce" NICE Challenge Project. Accessed May 16, 2018. https://nice-challenge.com

[10] Weiss, R., J. Mache, and M. Locasto. "The EDURange Framework and a Movie-themed Exercise in Network Reconnaissance." *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, 2017. Accessed May 17, 2018. https://www.usenix.org/system/files/conference/ase17/ase17_paper_weiss.pdf

[11] "Clue | Board Game." BoardGameGeek. Accessed June 15, 2018. https://boardgamegeek.com/boardgame/1294/clue

[12] Weiss, R., Turbak, F., Mache, J., Nilsen, E., AND Locasto, M. "Finding the balance between guidance and independence in cybersecurity exercises." In USENIX Workshop on Advances in Security Education (2016).

[13] R. Weiss, M. Locasto, J. Mache, "A Reflective Approach to Assessing Student Performance in Cybersecurity Exercises", Proceedings of the 47th ACM Technical Symposium on Computer Science Education (SIGCSE), 2016

[14] S. Boesen, R. Weiss, M. Locasto, J. Sullivan, J. Mache, E. Nilsen, "EDURange: Meeting the Pedagogical Challenges of Student Participation in Cybertraining Environments", Proceedings of the 7th Workshop on Cyber Security Experimentation and Test (CSET at USENIX), 2014